Bab 1. Pengenalan Wireless LAN

Kita akan mendiskusikan tentang pangsa pasar wireless LAN, gambaran masa lalu, sekarang dan masa depan dari wireless LAN, serta pengenalan wireless LAN standar pemerintah. Kemudian kita akan mendiskusikan beberapa aplikasi yang sesuai untuk wireless LAN. Menurut pengalaman dari cerita dan evolusi dari teknologi wireless LAN merupakan bagian yang penting dari prinsip dasar wireless LAN. Suatu pemahaman dari mana wireless LAN datang dan aplikasinya serta organisasinya yang dapat membantu perkembangan teknologi yang memungkinkan anda untuk mengaplikasikan wireless LAN yang lebih baik ke dalam organisasimu atau kebutuhan klien

1.1 Pangsa Pasar Wireless LAN

Pangsa pasar wireless LAN sepertinya berkembang sama halnya dengan fashion pada kebanyakan industri jaringan, dimulai dengan mengadopsi awal menggunakan teknologi apapun yang telah tersedia. Pemasaran telah dipindahkan kedalam pertumbuhan yang cepat, di mana standard populer menyediakan katalisator. Perbedaan yang besar antara pemasaran jaringan secara keseluruhan dan pemasaran wireless LAN menjadi meningkat. wireless LAN memberikan fleksibilitas dalam implementasinya dan tidak heran mereka pindah dengan cepat ke sektor pasar yang lainnya.

1.2 Sejarah Wireless LAN

Penyebaran jaringan nirkabel, seperti kebanyakan teknologi, seperti turun temurun dibawah naungan dari militer. Militer perlu suatu kemudahan, yang mudah diterapkan, dan metode keamanan pertukaran data dalam suatu lingkungan peperangan.

Ketika biaya teknologi nirkabel merosot dan mutu meningkat, itu menjadi penghematan biaya untuk perusahaan-perusahaan yang dapat menggabungkan bagian nirkabel ke dalam jaringan mereka. Teknologi nirkabel menawarkan suatu

jalan yang murah untuk kampus untuk menghubungkan bangunan satu sama lain tanpa pemasangan kabel fiber atau tembaga.

1.3 Standarisasi Wireless LAN

Karena wireless LAN mengirim menggunakan frekuensi radio, wireless LAN diatur oleh jenis hukum yang sama dan digunakan untuk mengatur hal-hal seperti AM/FM radio. Federal Communications Commission (FCC) mengatur penggunaan alat dari wireless LAN. Dalam pemasaran wireless LAN sekarang, menerima beberapa standard operasional dan syarat dalam Amerika Serikat yang diciptakan dan dirawat oleh *Institute of Electrical Electronic Engineers (IEEE)*.

Beberapa Standar wireless LAN :

IEEE 802.11 – standar asli wireless LAN menetapkan tingkat perpindahan data yang paling lambat dalam teknologi transmisi light-based dan RF.

IEEE 802.11b – menggambarkan tentang beberapa transfer data yang lebih cepat dan lebih bersifat terbatas dalam lingkup teknologi transmisi.

IEEE 802.11a – gambaran tentang pengiriman data lebih cepat dibandingkan (tetapi kurang sesuai dengan) IEEE 802.11b, dan menggunakan 5 GHZ frekuensi band UNII.

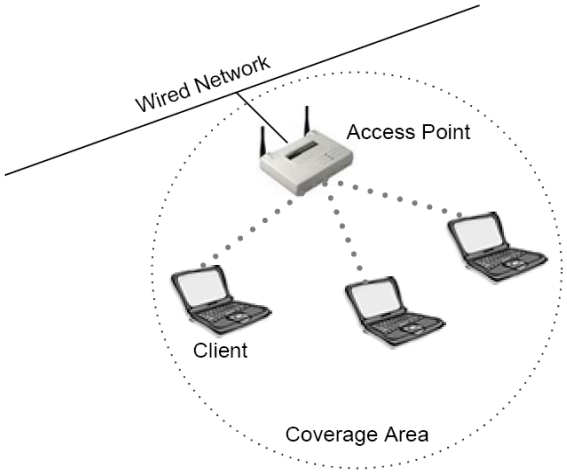
IEEE 802.11g – syarat yang paling terbaru berdasar pada 802.11 standard yang menguraikan transfer data sama dengan cepatnya seperti IEEE 802.11a, dan sesuai dengan 802.11b yang memungkinkan untuk lebih murah.

1.4 Aplikasi Wireless LAN

1.4.1 Akses Role

Wireless LAN kebanyakan menyebar dalam suatu lapisan akses, maksudnya mereka digunakan sebagai suatu titik masukan ke dalam suatu kabel jaringan. Di masa lalu, akses telah digambarkan sebagai dial-up, ADSI, kabel/telegram, selular, Ethernet, Token Ring, Frame Relay, ATM, dan lain lain. wireless cara sederhana yang lain untuk para user dalam mengakses jaringan tersebut. Wireless LAN adalah lapisan jaringan Data-Link seperti cara akses semuanya hanya mendaftar saja. Dalam kaitan dengan kecepatan, jaringan nirkabel tidaklah tepat diterapkan dalam distributor atau sebagai inti dalam

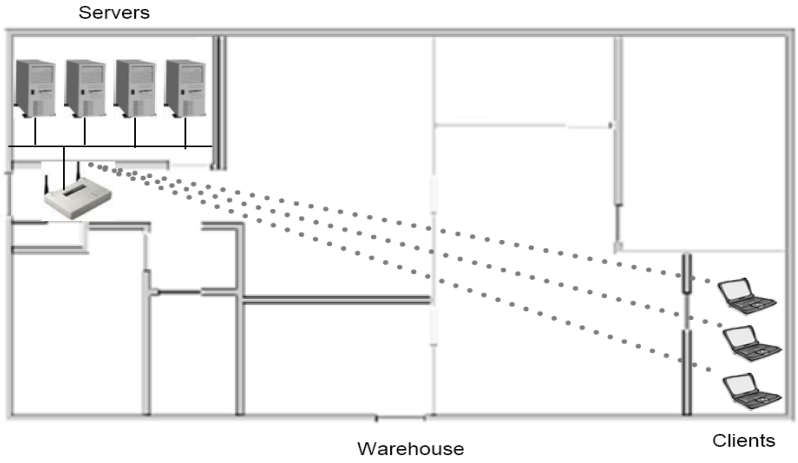
jaringan. Tentu saja, dalam jaringan kecil, mungkin tidak ada perbedaan antara inti, Distribusi, atau Lapisan akses dari jaringan tersebut. Lapisan inti dari suatu jaringan harus sangat stabil dan sangat cepat, mampu menangani suatu jumlah yang luar biasa dengan sedikit kesulitan dan pengalaman tidak ada penurunan waktu. Lapisan distribusi suatu jaringan harus cepat, fleksibel, dan dapat diandalkan. Wireless LAN tidak secara khusus dibutuhkan sebagai suatu solusi perusahaan. Gambar 1.1 menggambarkan klien dengan cepat memperoleh akses dalam suatu kabel jaringan melalui hubungan suatu alat koneksi (point access).



Gambar 1.1. Akses role dari wireless LAN

1.4.2 Perluasan Jaringan

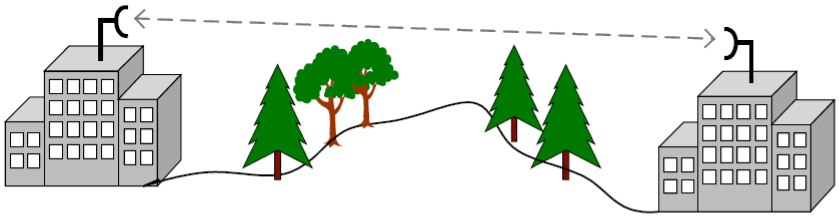
Jaringan nirkabel dapat bertindak sebagai suatu perluasan dari suatu kabel jaringan. Ada kemungkinan masalah dimana memperluas jaringan akan memerlukan tambahan kabel dalam instalasinya dan menjadi kendala dalam pembiayaannya. Wireless LAN dapat dengan mudah digunakan untuk menyediakan konektivitas dalam suatu gedung yang merupakan area yang jauh, digambarkan dalam denah dalam gambar 1.2. Karena hanya sedikit diperlukan pemasangan kabel untuk memasangan wireless LAN, biaya instalasi dan pembelian ethernet dengan sepenuhnya dihapuskan.



Gambar 1.2. Perluasan Jaringan

1.4.3 Menghubungkan Gedung Satu dengan yang lain

Terdapat 2 perbedaan bentuk dari konektivitas antar gedung. Pertama disebut Point-to-Point (PTP), dan yang kedua disebut Point-to-Multipoint (PTMP). Point-to-point adalah koneksi nirkabel hanya antar dua bangunan, seperti gambar 1.3. Koneksi PTP hampir selalu menggunakan semi-directional atau highly-directional antenna pada masing-masing akhir dari link.



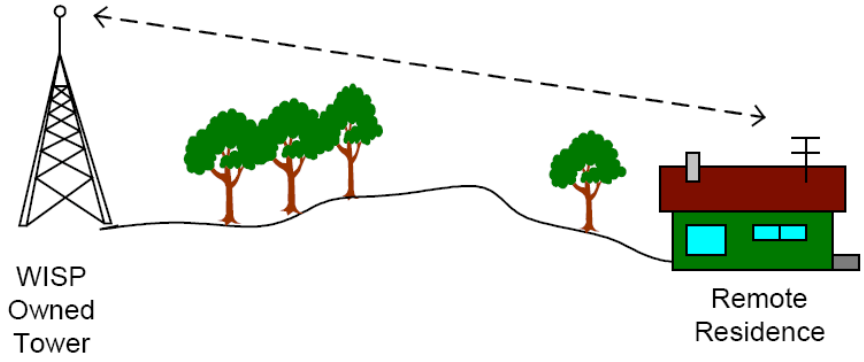
Gambar 1.3. Koneksi antar gedung

Point-to-multipoint (PTMP) adalah koneksi nirkabel tiga atau lebih dari beberapa gedung, bentuk penerapannya adalah “hub and spoke” atau star topologi, dimana salah satu gedung sebagai titik pusat dari jaringan (server).

1.4.4 Pengiriman Data Bermil-mil

Wireless Internet Service Providers (WISPs) sekarang mengambil keuntungan dari kemajuan terbaru dalam teknologi nirkabel untuk mengirim data bermil-mil untuk melayani pelanggan mereka. WISP mempunyai tantangan yang unik bagi mereka. Hanya provider xDSL mempunyai permasalahan lebih

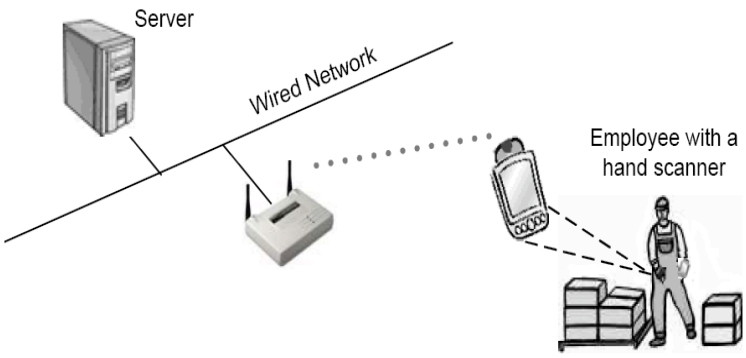
jauh pada jarak yang jauh yaitu 18.000 kaki (5,7 km) dari kantor pusat dan kabel provider mempunyai persoalan dengan kabel yang sedang dipakai bersamaan oleh user, WISP mempunyai masalah dengan atap, pohon, kilat, pegunungan, menara dan banyak lagi hambatan dalam konektivitas.



Gambar 1.4. Layanan Data yang jauh

1.4.5 Mobilitas

Sebagai suatu solusi lapisan akses, wireless LAN tidak dapat digantikan dengan kabel LAN dalam kondisi kecepatan data (100BaseTx tiap 100Mbps versus IEEE 802.11a tiap 54Mbps). Wireless LAN melakukan penawaran dalam peningkatan suatu mobilitas (seperti pada gambar 1.5) sebagai awal perdagangan untuk kecepatan dan mutu layanan.

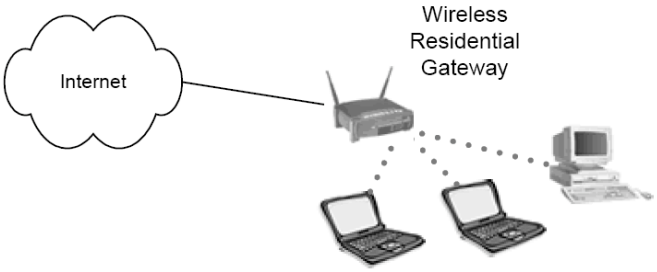


Gambar 1.5. Mobilitas

1.4.6 Small Office – Home Office

Bentuk jenis ini juga digunakan oleh banyak perusahaan yang hanya mempunyai beberapa karyawan. Dalam perusahaan ini mempunyai kebutuhan

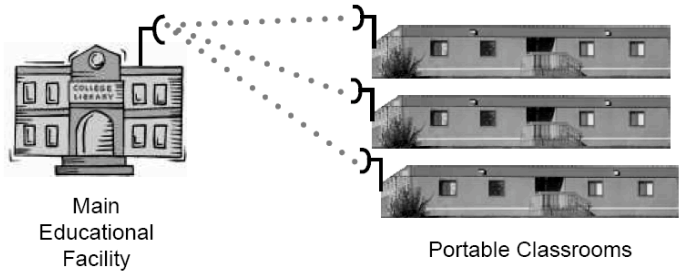
untuk membagi informasi antar para pemakai dan koneksi internet tunggal untuk efisiensi dan peningkatan produktivitas. Untuk aplikasi ini -small office-home office, atau SOHO- wireless LAN sangat mudah dan solusi yang efektif.



Gambar 1.6. SOHO wireless LAN

1.4.7 Mobile Offices

Suatu contoh sederhana dalam menghubungkan kelas dengan cepat yang konektivitasnya menggunakan wireless LAN yang digambarkan dalam gambar 1.7. Ruang kantor sementara juga memanfaatkan jaringan dengan wireless LAN. Ketika perusahaan berkembang, mereka sering mencari kekurangan dari ruang kantor mereka, dan butuh untuk sedikit pekerjaan untuk berpindah ke lokasi yang berdekatan, seperti suatu kantor bersebelahan atau suatu kantor pada lantai yang berbeda tetapi masih satu gedung.



Gambar 1.7. Suatu sekolah dengan kelas yang mobilitas

1.5 Kesimpulan

Teknologi wireless telah ada sejak dulu yang secara sederhana diimplementasikan di dunia militer. Kepopuleran dan level teknologi yang digunakan dalam wireless Lan bertumbuh dengan sangat pesat. Manufactur telah menciptakan a myriad of solutions untuk berbagai kebutuhan kita akan jaringan wireless. Kenyamanan, pupolaritas,

penyediaan, dan harga dari perangkat keras wireless LAN menyediakan kita semua dengan banyak solusi yang berbeda.

Dengan laju perkembangan teknologi wireless, manufaktur, dan perangkat keras yang sangat pesat, aturan dari organisasi seperti FCC, IEEE, WECA, dan WLANA akan menjadi semakin penting untuk pembersihan gangguan operasi antar solusi. Hukum-hukum tersebut ditetapkan oleh organisasi yang mengaturnya seperti FCC bersama-sama dengan organisasi pendukung lainnya seperti IEEE, WLANA, dan WECA yang akan menjadi tumpuan bagi industri wireless LAN dan menyediakan path yang umum bagi industri wireless LAN untuk bertumbuh dan berkembang.

1.6 SOAL

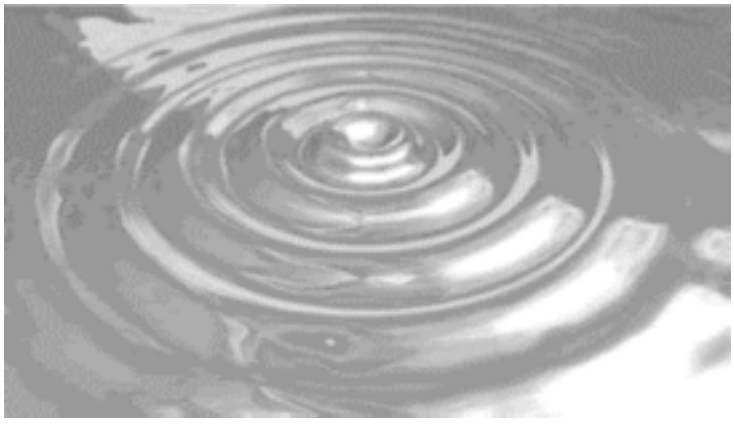
1. Apa nama badan internasional yang mengatur tentang penggunaan alat – alat wireless dan penggunaan radio AM/FM ?
2. Sebutkan standar wireless LAN yang telah dikeluarkan oleh IEEE ?
3. Jelaskan masing –masing sdari standar wireless menurut sola no. 3 ?
4. Sebutkan beberapa aplikasi dari Wireless LAN ?
5. Apa yang dimaksud dengan SOHO Wireless LAN ?

Bab 2. Dasar Frekuensi Radio

Untuk mengerti aspek wireless dari LAN wireless, seorang administrator harus memiliki dasar yang kuat tentang pokok teori radio frekuensi(RF). Pada bagian ini kita akan membahas properti dari radiasi RF dan bagaimana sifatnya pada situasi tertentu dapat mempengaruhi performance dari LAN wireless. Antenna akan dikenalkan untuk membuat pengertian yang baik untuk kegunaan dan propertinya. Kita akan mendiskusikan hubungan matematika yang ada pada RF circuit dan mengapa hal itu penting,sebagaimana menunjukkan pentingnya penghitungan matematika pada RF. Untuk administrator wireless LAN , mengerti konsep dari RF penting untuk implementasi, expansi, maintenance, dan permasalahan dari jaringan wirelesss.

2.1 Frekuensi Radio

Frekuensi Radio adalah sinyal arus berfrekuensi tinggi yang berubah-ubah yang melewati konduktor tembaga yang panjang dan kemudian diradiasikan ke udara melalui sebuah antenna. Sebuah antenna mentranformasikan sinyal kabel ke sinyal wireless dan sebaliknya. Ketika sinyal AC berfrekuensi tinggi diradiasikan ke udara,akan membentuk gelombang radio. Gelombang radio tersebut berpindah dari sumber (antenna) pada sebuah garis lurus semuanya bersamaan.



Gambar 2.1. Batu Jatuh di Air

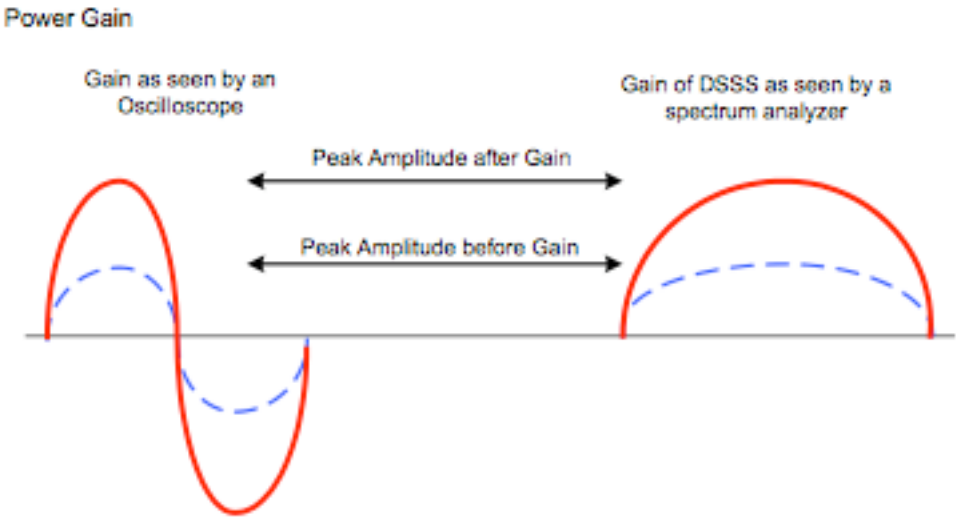
Jika anda dapat membayangkan menjatuhkan batu ke dalam kolam dan melihat titik pusat riak air yang mengalir dari titik dimana batu membentur air (seperti ditunjukkan Gambar 2.1), kemudian anda mempunyai ide bagaimana RF bekerja

seperti dipancarkan dari antenna. Mengerti tingkah laku dari panyebaran gelombang RF adalah bagian penting untuk mengerti mengapa dan bagaimana wireless LAN berfungsi. Tanpa dasar pengetahuan tersebut,seorang administrator tidak mampu menentukan lokasi instalasi dari perlengkapan dan tidak akan mengerti bagaimana memecahkan masalah wireless LAN.

2.1.1 Sifat RF

RF kadang disebut kaca dan asap karena RF terlihat bekerja tidak teratur dan tidak konsisten pada kenyataanya. Barang kecil seperti konektor tidak terlalu kecil atau tipis yang tidak cocok pada garis dapat menyebebkan sifat yang tidak teratur dan hasil yang tidak diinginkan. Pada sesi berikut mendiskripsikan type tersebut dan bagaimana dapat terjadi pada gelombang radio seperti pengirimnya.

2.1.2 Gain



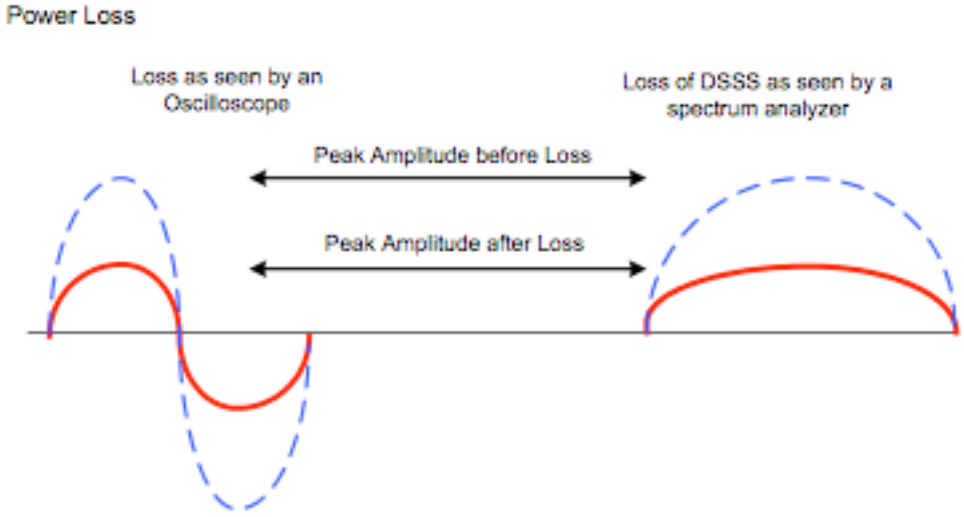
Gambar 2.2. Power Gain

Ilustrasi gain pada Gambar 2.2, adalah waktu yang digunakan untuk mendiskripsikan peningkatan pada sinyal RF amplitudo. Gain biasanya adalah proses yang aktif.; berarti bahwa sumber tenaga , seperti RF amplifier , digunakan untuk menguatkan sinyal atau sebuah high-gain antenna digunakan memfocuskan beamwidth dari sinyal untuk meningkatkan amplitudo sinyalnya.

Tetapi proses yang pasif bisa juga menyebabkan Gain. Contohnya, refleksi sinyal RF dapat berkombinasi dengan sinyal utama untuk meningkatkan tegangan sinyal utama.

Meningkatkan tegangan mungkin memiliki dampak positif dan negatif. Khususnya,tenaga yang banyak adalah lebih baik, tetapi merupakan kasus ,seperti saat transmitter meradiasikan tenaga sangat tertutup ke tenaga output yang terbatas, dimana penambahan tenaga akan menyebabkan masalah yang serius.

2.1.3 Power Loss



Gambar 2.3. Power Loss

Loss menggambarkan sebuah penurunan kekuatan sinyal (Gambar 2.3). Banyak cara yang dapat menyebabkan kerusakan sinyal, baik ketika sinyal masih dalam kabel seperti sinyal AC yang berfrekuensi tinggi dan ketika sinyal dipancarkan seperti gelombang radio melalui udara dengan antenna. Resistansi dari kabel dan konektor menyebabkan kerusakan karena perubahan sinyal AC terlalu panas. Impedance yang tidak seimbang pada kabel dan konektor dapat mengakibatkan power direfleksikan kembali ke sumber, yang mana dapat menyebabkan degradasi sinyal. Secara langsung objek dipancarkan oleh transmisi gelombang dapat menyerap, memantulkan, atau merusak sinyal RF. Kerusakan dapat dimasukkan dengan sengaja ke sirkuit dengan sebuah RF attenuator. RF attenuator adalah resistor yang akurat yang merubah AC berfrekuensi tinggi ke panas sehingga mengurangi amplitudo sinyal pada titik dalam sirkuit.

Ada banyak sebab yang mempengaruhi sinyal RF antara pengirim dan penerima. Karena gain atau loss sesuai untuk implementasi wireless LAN, hal itu harus dapat ditentukan . Sesi pada bagian ini tentang matematika RF akan mendiskusikan loss dan gain yang sesuai dan bagaimana untuk menghitung dan mengimbanginya.

Menjadi ukuran dan penyeimbang untuk loss pada koneksi RF atau sirkuit adalah penting karena radio memiliki penerima threshold yang sensitiv. Threshold yang sensitiv didefinisikan sebagai titik yang mana radio dapat membedakan dengan jelas sebuah sinyal dari noise background. Karena keterbatasan penerima yang sensitiv, letak transmitting harus memancarkan sinyal dengan amplitudo yang cukup untuk dapat dikenal oleh penerima. Jika kerusakan terjadi antara pengirim dan penerima , masalah tersebut harus dikoreksi oleh object yang berpindah mengakibatkan loss atau dengan meningkatkan kekuatan transmisi.

2.1.4 Refleksi

Refleksi diilistrusikan pada Gambar 2.4, terjadi ketika pemancar gelombang elektromagnetik mengenai object yang memiliki dimensi yang sangat besar ketika dibandingkan dengan lamanya gelombang dari pemancar gelombang. Refleksi terjadi pada permukaan bumi, bangunan ,tembok, dan panghalang yang lain. Jika permukaan lembut, refleksi sinyal mungkin tertinggal utuh, pendapat itu adalah beberapa loss karena penyerapan dan penyerapan sinyal.

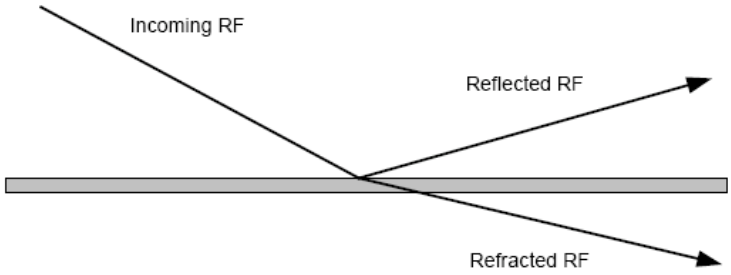
Sinyal RF dapat menyebabkan masalah yang serius pada wireless LAN. Pemantulan pada sinyal utama dari banyak object pada area pengirim diteruskan ke multipath. Multipath dapat memiliki dampak negativ yang parah pada LAN wireless, seperti penurunan atau pembatalan sinyal utama dan mengakibatkan lubang atau celah pada RF area. Permukaan seperti danau, atap logam, pintu logam, dan lainnya dapat mengakibatkan refleksi yang parah, dan multipath.

Gambar 2.4. Pemantulan (Reflection)

Refleksi pada magnitudo tersebut tidak pernah menguntungkan dan secara khusus membutuhkan fungsi khusus(antenna diversity) dengan wireless LAN hardware untuk mengimbanginya. Baik multipath maupun antenna diversity didiskusikan lebih jauh pada bagian 9.

2.1.5 Pembiasan (Refraksi)

Pembiasan digambarkan sebagai pembelokan gelombang radio yang melewati medium yang memiliki kepadatan yang berbeda. Seperti gelombang RF yang melewati medium yang lebih padat gelombang akan akan cenderung melewati arah yang lain, seperti diilustrasikan pada Gambar 2.5.



Gambar 2.5. Pembiasan

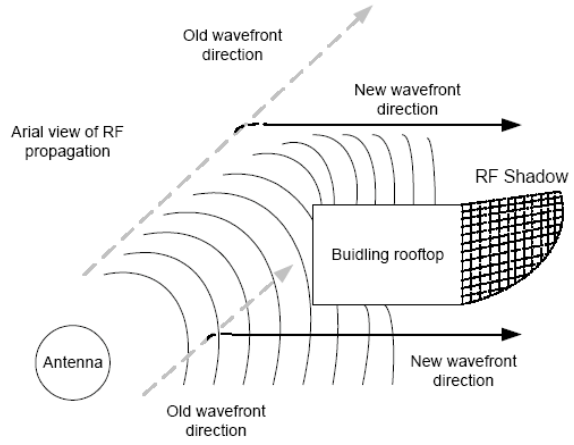
Pemantulan dapat mengakibatkan masalah untuk RF pada area yang luas. Seperti perubahan kondisi atmosfer, gelombang RF mungkin berubah arah, mengalihkan jalannya sinyal dari target yang dikehendaki.

2.1.6 Difraksi

Difraksi terjadi ketika garis edar radio antara pengirim dan penerima dihambat oleh permukaan yang tajam atau dengan kata lain kasar. Pada frekuensi

tinggi, difraksi, seperti refleksi, tergantung pada ukuran objek yang menghambat dan amplitudo, fase, dan polarisasi dari gelombang pada titik difraksi.

Difraksi secara umum dibingungkan dan disalah artikan dengan refraksi. Perhatian seharusnya tidak membingungkan jangka waktunya. Difraksi didiskripsikan sebuah gelombang membelok melalui medium. Pada contoh diatas seperti batu pada kolam, sekarang menganggap menancapkan tongkat melewati permukaan air disamping dimana batu mengenai air. Seperti kocakan air mengenai tongkat, itu akan diblok ke derajat yang kecil, tetapi ke derajat yang besar, ripple akan dipancarkan disekitar ranting. Ilustrasi tersebut menunjukan bagaimana difraksi dengan rintangan pada garis edarnya, tergantung pada permukaan hambatan. Jika object lebih besar atau tidak rata , gelombang mungkin tidak dipancarkan, tetapi mungkin diblok.

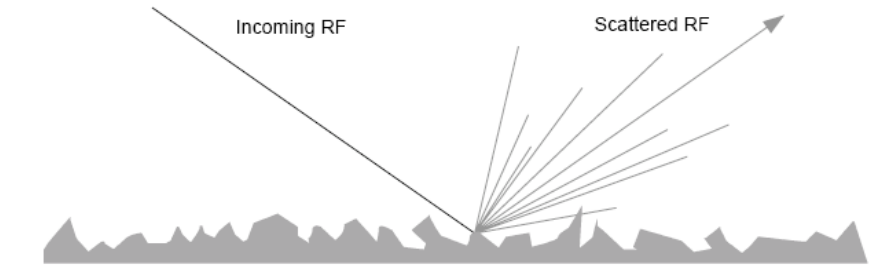


Gambar 2.6. Difraksi

Difraksi adalah gelombang yang pelan pada titik dimana permukaan gelombang mengenai hambatan,ketika tumpuan dari permukaan gelombang menopang penyebaran pada kecepatan yang sama. Difraksi adalah effect dari putaran gelombang, atau belokan,disekitar hambatan. Seperti contoh yang lain ,menganggap mesin blowing sebuaharus yang kuat dari asap. Asap itu akan mengalir lurus sampai hambatan dibuka pada bagiannya. Memperkenalkan blok kayu yang luas ke energi asap akan menyebabkan asap menggulung disekitar pojok dari blok menyebabkan degradasi yang menyolok pada kecepatan asap pada titik dan perubahan signifikan pada arahnya

2.1.7 Scattering

Penyebaran terjadi ketika medium dimana gelombang merambat mengandung object yang kecil dibandingkan dengan panjang sinyal gelombang, dan jumlah object perunit volume sangat besar. Gelombang tersebar dihasilkan dari perrmukaan kasar, benda kecil,atau oleh ketidak normalan path sinyal, seperti terlihat pada Gambar 2.7



Gambar 2.7. Scattering

Beberapa contoh diluar ruangan yang menyebabkan penyebaran pada sistem komunikasi mobile termasuk foliage, rambu lalu lintas,dan lamppost. Penyebaran dapat terjadi dalam 2 cara utama.

Pertama, penyebaran terjadi ketika gelombang merambat melalui permukaan kasar dan terpantul ke segala arah secara simultan. Penyebaran tipe ini memicu banyak pemantulan amplitudo kecil dan merusak sinyal RF utama. Dissipasi sinyal RF bisa terjadi ketika gelombang ketika gelombang RF dipantulkan oleh pasir, bebatuan atau permukaan tidak rata lainnya. Ketika penyebaran terjadi dengan cara ini ,degradasi sinyal RF bisa signifikan pada titik komunikasi intermettenly dissporing atau menyebabkan kehilangan sinyal secara total.

Kedua, penyebaran dapat terjadi ketika gelombang sinyal merambat melalui partikel-partikel dalam medium seperti debu. Dalam kasus ini, bukanya terpantul oleh permukaan kasar,gelombang RF secara individual terpantul pada partikel-partikel yang sangat kecil.

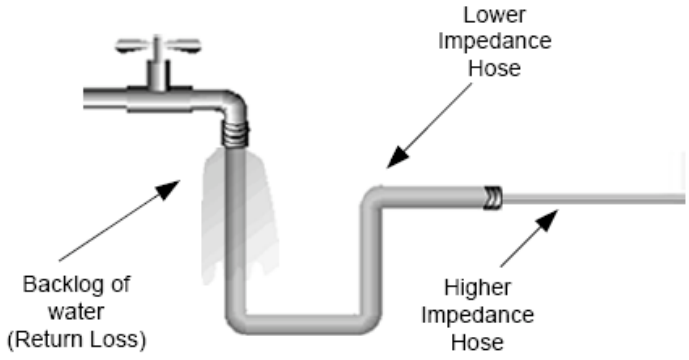
2.1.8 Penyerapan (Absorption)

Penyerapan terjadi ketika sinyal RF merambat objek dan terserap dalam material objek dengan cara tidak menembusnya, memantul, atau mengitari objek

2.2 Rasio Tegangan Gelombang Berdiri (VSWR)

VSWR terjadi ketika terdapat impedalisi yang tidak cocok (hambatan arus dalam satuan ohm) antara alat dalam sistem RF. Ketidakcocokan dalam kontes ini, berarti bahwa satu alat mempunyai impedasi yang lebih tinggi atau lebih rendah daripada alat yang terhubung padanya. VSWR disebabkan oleh sinyal RF yang terpantul pada titik ketidakcocokan impedansi dalam path dalam empat sinyal. VSWR menyebabkan kehilangan kembalian, yang didefinisikan sebagai kehilangan energi maju melalui sebuah sistem yang disebabkan beberapa dayanya terpantulkan dan kembali ke pengirim. Jika impedasi pada ujung koneksi tidak cocok, kemudian tenaga tertransmisi maksimal tidak akan diterima pada antenna, ketika bagian sinyal RF terpantul kembali kepengirim, levelo sinyal pada line berbeda, bukannya menjadi tetap. Perbedaan ini merupakan indikator VSWR.

Sebagai ilustrasi VSWR, bayangkan air mengalir melalui dua selang. Selama dua selang mempunyai diameter yang sama air mngalir dengan normal. Jika selang terhubung pada faucet yanfg secara signifikan lebih besar dari selang lainnya akan terjadi tekanan balikpada faucet dan bahkan pada koneksi antara dua selang. Tekanan balik berdiri mengilustrasikan VSWR, seperti terlihat pada Gambar 2.8. dalam contoh ini anda dapat melihat bahwa back pressure mempunyai effek negative dan tidak secara dekat sebanyak air dialirkan keselang yang kedua dibandingkan dengan selang yang cocok disambungkan secara benar.



Gambar 2.8. VSWR

2.2.1 Pengaturan VSWR

VSWR merupakan rasio, jadi ia diekspresikan sebagai hubungan antara dua angka. Nilai khusus VSWR adalah 1,5 : 1. dua angka berelasi dengan rasio ketidakcocokan impedasi disbanding dengan impedasi yang cocok sempurna.

Angka kedua selalu satu, mempresentasikan ketidakcocokan yang sempurna, sedangkan angka pertama bias berbeda. Semakin rndah angka pertma (mendekati satu), semakin baik kecocokan impedansi yang dimiliki system anda. Sebagai contoh VSWR dengan rasio 1,1 : 1 loebih baik daripada 1,4 : 1. pengukuran VSWR 1 : 1 menunjukkan kecocokan impedansi yang sempurna dan tidak ada tegangan gelombang berdiri akan muncul dalam path sinyal.

2.2.2 Efek VSWR

VSWR yang berlebihan dapat menyebabkan masalah yang serius dalam sirkuit RF. Sebagian besar, hasilnya menuru dalam amplitude dalam sinyal RF terkirim. Bagaimanapun, beberapa transmitter tidak akan terlindungi terhadap daya selama diterima atau dikembalikan ke sirkuit output transmitter, tenaga yang terpantul bias membakar elektronik transmitter. Efek VSWR terjadi ketika sirkuit transmitter terbakar, level output daya tidak stabil dan pengamanan daya berbeda secara signifikan dari tenaga yang diharapkan. Metode pembandingan VSWR dal;am sirkuit termasuk penggunaan yang benar dari alat yang benar. Koneksi keras diantra kabel dan konektor, penggunaan perangkat yang impedensinya cocok dan penggunaan alat berkualitas tinggi dengan laporan kaligrasi ketika dibutuhkan semuanya merupakan pengukuran preventatif terhadap VSWR. VSWR dapat diukur dengan instrumen berakularasi tinggi seperti SWR meter, tetapi pengukuran ini masih dalam ruang lingkup text ini dan merupakan tugas kerja dari adminnetwork.

2.2.3 Solusi VSWR

Untuk mencegah efek negatif VSWR sangatlah penting bahwa semua kabel, konektor dan alat-alat mempunayi impedensi yang semirip mungkin. Jangan gunakan kabel 75 ohm dengan alat 50 ohm, sebagai contoh. Kebanyakan alat-alat wireless LAN mempunyai impedansi 50 ohm, tetapi tetap disarankan agar anda tetap mengecek setiap alat sebelum pemasangan, hanya untuk menyakinkan. Setiap alat transmiter ke antenna harus mempunyai impedensi sesama mimpin, termasuka kabel, konektor, antenna, amplifiyer, antenuators, sirkuit output transmitor, dan sirkuit imput penarima.

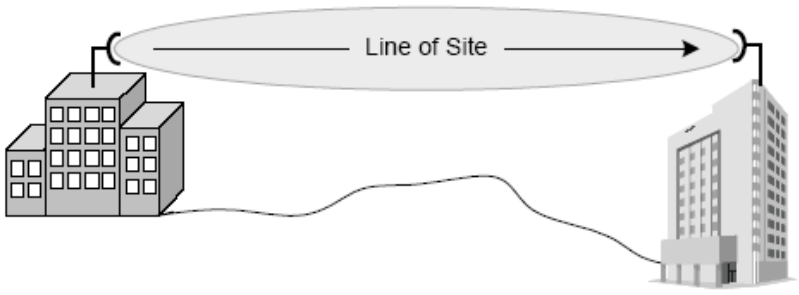
2.3 Prinsip Antenna

Bukan maksud kami mengajarkan teori antenna pada buku ini, tetapi untuk menjelaskan bebearap prinsip antenna yang secara langsung berhubungan penggunaan Wireless LAN. Tidak penting bagi Wairless LAN untuk secara detail untuk memahami desain antenna untuk mengadmintrasi network. Sepasang point utama yang penting untuk dimengerti untuk antenna adalah:

1. Antenna menkonversi energi listrik gelombang ke gelombang RF. Dalam kasus antenna pentramisi, atau gelombang RF ke energi elektik dalam kasus antenna penerima.
2. Dimensi fisik antenna seperti panjangnya berhubungan langsung dengan frekuensi dimana antennanya dapat menghambat gelombang atau menerima gelomang terhambat. Beberapa point penting dalam memahami pengadmintrasian werless LAN bebas lisensi adalah garis panjang, efek zona fresnel (baca : fra-nel) dan penapaian antenna, dalam melalui beamwidth terfokus. Point ini akan didiskusikan dalam bagian ini.

2.3.1 Garis Pandang

Dengan cahaya tampak, visual LOSD (yang lebih sederhana dikenal sebagai LOS) didefinisikan sebagai garis lurus dalam objek dalam pandangan (transmiter) kemata pengamat. LOS merupakan garis lurus karena gelombang cahaya bisa berubah-ubah karena refraksi, defraksi, dan refleksi dengan cara yang sama dengan RF refreksi. Gambar 2.9 mengilustrasikan LOS. RF bekerja mirip dengan cahaya tampak pada wireless LAN dengan satu pengecualian: RF LOS dapat juga dipengaruhi oleh pengeblokkan zona Fresnel.

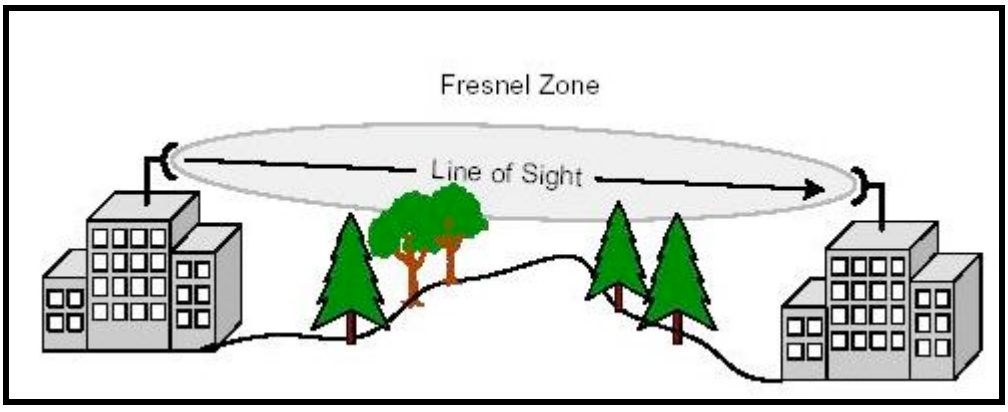


Gambar 2.9. Line of Site

Bayangkan jika anda melihat kearah sebuah pipa sepanjang dua kaki kemudian obstruksi mengeblok dalam pipa. Ilustrasi sederhana ini menunjukkan bagaimana RF bekerja ketika benda mengeblok zona Fresnel, kecuali bahwa dengan pipa itu anda dapat melihat ujung lainnya pada beberapa derajat. Dengan RF kemampuan yang sama terbatasnya untuk melihat translasi kekoneksi yang korup atau yang rusak, RF LOS penting karena RF tidak sama seperti cahaya tampak berkerja.

2.3.2 Daerah Fresnel (Fresnel Zone)

Sebuah keputusan ketika merencanakan atau memperbaiki RF LAN adalah zona Fresnel. Zona Fresnel menepati beberapa seri dari area berbentuk elips konsentrik disekitar jalan LOS seperti terlihat Gambar 2.10. Zona Fresnel penting dalam entergritas RF link karena dapat memperbaiki area disekeliling LOS yang dapat memngenali interferensi sinyal RF jika terblok. Objek dalam zona Fesnel seperti pohon, bukit, dan bangunan dapat menyebarkan atau dapat memantulakn sinyal utama keluar dari penerima, mengubah RF LOS. Objek-objek ini juga dapat menyerap atau menyebarkan sinyal RF utama menyebabkan degradasi atau kehilangan sinyal.



Gambar 2.10. Fresnel Zone

Radius fresnel zone dari titik terluarnya dapat dihitung dengan menggunakan rumus.

$$r = 43.3 \times \sqrt{\frac{d}{4f}}$$

Dimana d adalah jarak link dalam ukuran mil, f adalah frekuensi dalam besaran GHz, dan hasilnya adalah r dalam ukuran feet.

2.3.3 Obstruction

Mempertimbangkan pentingnya jarak jangkauan fresnel zone, oleh karena itu penting juga mengukur derajat yang dapat di-blok oleh fresnel zone. Sebuah Rf sinyal, ketika secara partial di-blok akan membelok mengelilingi sebuah penghambat beberapa derajat, beberapa halangan fresnel zone dapat terjadi tanpa adanya gangguan link yang berarti. Secara khusus, 20-40% gangguan fresnel zone memasukkan sedikit tanpa adanya campur tangan kedalam link. Hal tersebut selalu menimbulkan kesan error/salah pada sudut conservative yang membolehkan tidak lebih dari 20% gangguan pada fresnel zone. Lebih jelasnya, jika pohon atau objek lain adalah sumber dari gangguan, kemungkinan perlu mempertimbangkan design sebuah link yang didasarkan pada 0% gangguan. Jika lebih dari 20% fresnel zone dari sebuah RF link yang dimaksud telah ter-blok, atau jika sebuah aktif link menjadi ter-blok oleh bangunan baru atau pohon yang tumbuh, biasanya dengan menaikkan ketinggian antenna akan mengurangi masalah.

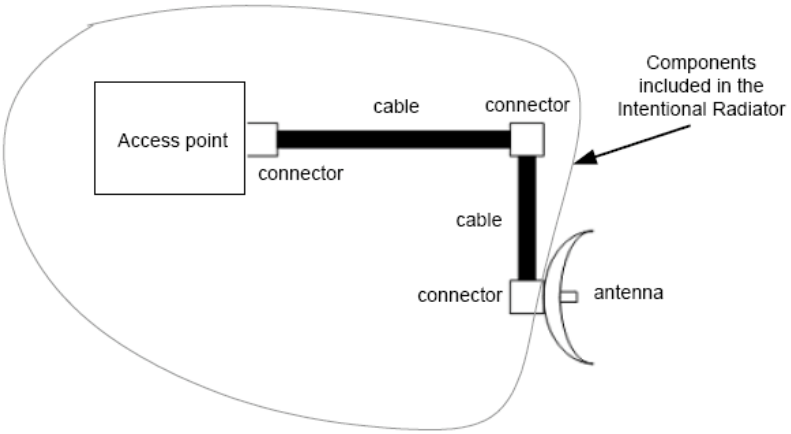
Sebuah pertanyaan yang umum ditanyakan tentang fresnel zone adalah ketika menggunakan peralatan indoor wireless LAN seperti PC cards dan access point, yaitu tentang bagaimana gangguan pada fresnel zone mampu mempengaruhi instalasi indoor. Pada sebagian besar instalasi indoor, RF sinyal mampu menyambung jalur, memantulkan, dan membelok mengelilingi dinding, perabotan, dan gangguan yang lain. Fresnel zone dikatakan tidak melanggar batas kecuali jika secara partial atau penuh sinyal ter-blok. Ini adalah sebuah kasus yang kadang kala terjadi, tetapi jarang diperhatikan oleh sebagian besar pengguna wireless mobile. Di lingkungan mobile, fresnel zone secara terus-menerus berubah sehingga pengguna secara normal membebaskan hal tersebut dan berpikir bahwa coverage yang mereka tempati jelek, tanpa berpikir kenapa coverage area yang tersebut menjadi tidak bagus.

2.3.4 Antenna Gain (Penguatan Antena)

Sebuah element antenna yang secara tipikal tidak diasosiasikan dengan amplifier dan filter disebut passive device. Tidak ada proses pengkondisian, penguatan, atau manipulasi sinyal oleh element antenna itu sendiri. Sebuah antenna dapat mempengaruhi proses penguatan (amplification) dari bentuk fisiknya. Proses pengguatan antenna merupakan hasil dari proses pemusatan(focusing) radiasi RF kedalam sebuah penguat beam, yang hanya sebagai bulb dari flashlight yang dapat difokuskan kedalam penguat beam yang membuat sebuah sumber menyerupai lampu penerang yang mengirimkan lampu selanjutnya. Focusing radiasi diukur dengan cara beamwidth, dari derajat horizontal dan vertical. Contohnya, sebuah omni-directional antenna memiliki 360 derajat horizontal beamwidth. Dengan membatasi 360 derajat beamwidth kedalam beam yang difokuskan kembali, katakanlah sebesar 3 derajat, pada daya yang sama gelombang RF akan diradiasikan kembali. Hal ini tergantung bentuk design dari antenna, patch, panel, dan yagi (yang kesemuanya termasuk kedalam jenis semi-derectional antenna). Higly-directional antenna meggunakan teori ini selangkah lebih maju dengan cara memfokus kedua beamwidth baik horizontal maupun vertical secara kuat untuk memaksimalkan jarak penyebaran gelombang pada low daya (daya kecil).

2.3.5 Intentional Radiator

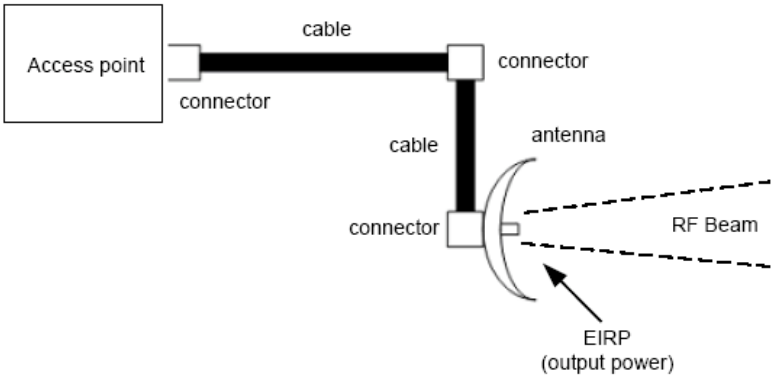
Sebagaimana yang telah didefinisikan oleh Federal Comunication Commision (FCC), intentional radiator adalah sebuah peralatan RF yang secara khusus di-design untuk meng-generate dan me-radiasi sinyal RF. Dalam istilah hardware, intentional radiator meliputi peralatan RF dan semua pengkabelan juga konektor-konektor pendukung tetapi tidak termasuk antenna, sebagaimana diilustrasikan pada Gambar 2.11 dibawah ini



Gambar 2.11. Intentional Radiator

2.3.6 Equivalent Isotropically Radiated Daya (EIRP)

EIRP adalah sebuah daya yang secara actual di pancarkan oleh element antenna, sebagaimana ditunjukkan pada Gambar 2.12. Konsep ini adalah penting karena telah diatur oleh FCC dan telah digunakan untuk perhitungan apakah sebuah wireless link atau bukan telah aktif. EIRP menerima account sebuah gain dari antenna



Gambar 2.12. EIRP

Jika sebuah stasiun transmisi menggunakan antenna sebesar 10 dBi (yang memperkuat sinyal sebesar 10-fold) dan intentional radiator memberikan daya sebesar 100 miliwatt. Maka EIRP-nya adalah sebesar 1000 mW atau 1 watt. FCC telah mengatur keduanya, meliputi kekuatan output pada internasional radiator dan element antenna. Kegagalan menggunakan aturan FCC yang berkenaan dengan

kekuatan output dapat menjadi persoalan administrator atau organisasi untuk kemudian melegalkan segala aksi untuk menjadikan semuanya menjadi baik

2.3.7 Rumus Matematika Frekuensi Radio

Ada 4 bagian penting dari pengkalkulasian daya pada wireless LAN, yaitu sebagai berikut :

- Daya (kekuatan) pada peralatan transmisi
- Loss dan gain dari peralatan penghubung antara peralatan transmisi dan antenna, seperti kabel, konektor, amplifier, attenuator, dan splitters.
- Daya (kekuatan) pada konektor terakhir sebelum sinyal RF masuk pada antenna (intentional Radiator).
- Daya pada element antenna (EIRP)

Bagian ini akan didiskusikan dalam contoh-contoh perhitungan pada sesi forthcoming. Setiap bagian ini akan membantu untuk menentukan link-link RF yang aktif tanpa melebihi daya yang telah dibatasi oleh FCC. Setiap factor tersebut harus dilakukan pada account ketika akan merencanakan sebuah wireless LAN, dan seluruh factor tersebut telah direlasikan secara matematik. Sedangkan pada bagian pendukung menjelaskan satuan-satuan ukuran yang digunakan pada perhitungan output daya ketika akan meng-konfigurasi peralatan-peralatan LAN.

2.4 Unit Of Measure (Satuan Ukur)

Ada beberapa standart satuan ukuran yang telah lazim dipakai oleh administrator wireless network karena lebih efektif dalam hal implementasi dan troble shooting (penanganan error) pada wireless LAN. Kita akan mendiskusikan tentang hal tersebut secara detil, beserta contoh penggunaanya. Kemudian kita akan menggunakan beberapa contoh permasalahan matematis-nya sehingga anda akan memahami sepenuhya apa saja yang diperlukan sebagai bagian dari perintah-perintah CWNA’s job.

2.4.1 Watts (W)

Satuan dasar dari daya adalah watt. Watt didefinisikan sebagai satu ampere(A) arus pada satu volt(V). Sebuah contoh untuk memahami satuan ini

adalah, kita bayangkan sebuah kebun yang dilalui oleh aliran air. Tekanan air dapat direpresentasikan dengan tegangan (voltage) dalam circuit elektrik. Aliran air yang melewati kebun tersebut dapat direpresentasikan dengan dengan ampere (arus). Sehingga dapat diumpamakan watt adalah hasil yang didapatkan dari penjumlahan besarnya tekanan dan banyaknya air yang melewati kebun. Satu watt sebanding dengan satu ampere dikalikan dengan satu volt.

Pengkhususan untuk 120 watt plug-in night-light kira-kira 7 watt. Pada malam hari yang terang, daya 7 watt ini akan tampak 50 mil (83 km) dari segala arah, dan jika kita dapat menyandikan informasi sedemikian rupa, seperti dengan menggunakan kode morse, kita akan mendapatkan sebuah wireless link yang telah terbentuk. Perlu diingat bahwa kita hanya memperhatikan proses penerimaan dan pengiriman data, dan bukan proses pencahayaan pada penerima dengan menggunakan energi RF sebagaimana kita akan menerangi sebuah ruangan dengan lampu. Anda dapat melihat secara relative sedikit daya yang diperlukan untuk untuk membentuk sebuah RF link dengan jarak yang besar. FCC hanya membolehkan 4 watt daya untuk diradiasikan dari sebuah antenna pada proses koneksi point-to-multipoint wireless LAN dengan menggunakan unlicensed 2,4 GHz peralatan spread spectrum. 4 watt kelihatannya bukan sebuah daya yang amat besar, tetapi lebih dari cukup untuk mengirim sinyal data RF secara jelas pada jarak bermil-mil.

2.4.2 Miliwatts

Pada saat proses implementasi wireless LAN, level daya yang sama-sama rendah sebesar 1 miliwatt (1/1000 watt, disingkat denganmW) dapat digunakan pada area yang kecil, dan level daya pada sebuah single-wireless LAN segment jarang sekali diatas 100 mW – cukup untuk komunikasi dengan jarak setengah mil (0.83 km) pada kondisi optimum. Secara umum access point memiliki kemampuan meradiasi daya 30-100 mW, tergantung pada manufacturer (pembuatnya). Hal ini hanya terjadi pada kasus point-to-point outdoors conection antara beberapa bangunan dimana level daya yang digunakan diatas 100 mW. Sebagian besar level daya yang dikerahkan oleh administrator akan menjadi mW atau dBm. Kedua satuan ukuran ini merepresentasikan sejumlah daya yang

absolute dan keduanya merupakan ukuran standart yang digunakan dalam industry.

2.4.3 Decibel

Saat penerima sangat sensitive terhadap sinyal RF (Radio Frequency), kemungkinan sinyal tersebut mampu membawa daya sekitar 0.000000001 watt. Lebih jelasnya maksud nilai tersebut adalah nilai yang sangat kecil untuk layperson dan akan ditolak atau tidak akan dibaca. Decibel diperuntukkan untuk mempresentasikan angka yang dibuat lebih mudah dipahami dan dimengerti. Decibel berdasarkan pada hubungan logaritmik dari pangukuran daya secara linier:Watts. Pada RF, logaritmik adalah eksponen dari angka 10 yang dipangkatkan untuk mencapai nilai yang diinginkan.

Jika kita memberikan angka 1000 dan ingin menemukan logaritmik (log), kita temukan log 1000=3 karena 10^3 = 1000. catatan bahwa logaritmik 3 adalah eksponensial. Hal yang penting sebagai catatan tentang logaritmik adalah logaritmik dari negative adalah nol atau tidak didefinisikan.

```
Log(-100)          = undefined!
Log(0)             = undefined!
```

Pada skala linier watt kita dapat menggambari titik-titik dari absolute daya. Ukuran dari absolute daya menunjuk pada ukuran daya dalam relasi beberapa referensi yang telah ditentukan. Pada sebagian besar skala linier (watt, derajat Kelvin, mil/jam), referensi telah ditentukan pada nol (zero), yang biasanya mendeskripsikan kekurangan dari sesuatu yang telah diukur: zero watts = no daya (tidak ada daya), zero derajat Kelvin = no thermal energy (tidak ada energi), zero MPH = no movement (tidak ada perpindahan). Pada skala logaritmik, sebuah referensi tidak dapat menjadi zero (nol) karena log dari zero tidak ada (tidak didefinisikan). Decibel adalah sebuah unit ukuran relative yang tidak sama dengan ukuran absolute dari miliwatt.

2.4.4 Gain And Loss Measurements (Pengukuran Penguatan dan Pelemahan)

Gain dan loss pada daya diukur dalam decibel, bukan dalam watt, karena gain dan loss adalah sebuah konsep relative dan decibel sendiri adalah suatu ukuran yang relative. Gain dan loss dalam system RF ditunjukkan oleh ukuran absolute daya (e.g. setengah dari daya-nya). Kehilangan setengah dari daya dalam sebuah system maka bersamaan dengan itu akan hilang 3 desibel. Jika sebuah system kehilangan setengah dari daya-nya (-3 dB), kemudian kehilangan setengah daya lagi (-3 dB), maka total kehilangan dari system sebesar ¾ dari daya original ½ dari kondisi awal, sehingga menjadi ¼(½ of ½). Lebih jelasnya, tidak ada ukuran absolute/mutlak pada watt yang dapat mengukur asymmetrical loss dengan jalan yang berarti, tetapi decibel mampu melakukannya.

Sebagai referensi yang cepat dan mudah, ada beberapa angka yang direlasikan untuk gain dan loss dan seorang administrator seharusnya sudah akrab dengan angka-angka ini. Angka-angka tersebut adalah sebagai berikut :

-3 dB = ½ daya dalam mW
+3 dB = *2 daya dalam mW
-10 dB = 1/10 daya dalam mW
+10 dB = *10 daya dalam mW

Kami menyebut referensi yang cepat ini sebagai 10's dan 3's dari RF math. Pada saat menghitung gain dan loss pada daya, keduanya hampir selalu dibagi dengan 10 atau 3. Nilai-nilai ini memberikan kemudahan bagi administrator untuk melakukan perhitungan loss dan gain pada RF secara cepat dan mudah dengan akurasi yang lumayan tanpa menggunakan kalkulator. Pada sebuah kasus dimana dengan menggunakan cara ini tidak mungkin dapat dilakukan, maka ada beberapa rumus pengkonversi yang dapat dilihat dibawah, yang dapat dilakukan untuk melakukan perhitungan ini.

Berikut ini adalah persamaan umum untuk mengkonversi mW ke dBm :

$$P_{dbm} = 10 \log P_{mW}$$

Persamaan ini dapat dimanipulasi untuk membalik pengkonversian, yaitu mengkonversi dBm ke mW :

$$Pmw = Log^{-1}(Pdbm /10) \quad Pmw = 10(Pdbm /10)$$

Note : Log^{-1} merupakan inverse logarithma (invers log).

Point lainnya yang juga penting adalah bahwa gain dan loss merupakan additive (tambahan). Jika access point dikoneksikan pada sebuah kabel yang telah loss sebesar -2 dB dan konektor loss sebesar -1 dB, maka keseluruhan dari loss akan ditambahkan dan hasil total dari loss adalah -3 dB. Kita akan sambung beberapa perhitungan RF pada sesi selanjutnya untuk mmberikan gambaran yang baik tentang bagaimana merelasikan ankga-angka tersebut dalam praktek nyata.

2.4.5 dBm

Reference point yang berkenaan dengan skala logaritmik dB untuk skala linier watt adalah :

1 mW = 0 dBm

Dimana m dalam dBm secara sederhana merujuk pada skala decibel dan skala watt yang kira-kira dapat menggunakan aturan sebagai berikut :

+dB akan mengalikan dua nilai watt :

(10 mW + 3 dB = 20 mW)

Demikian juga, -3 akan membagi dua nilai watt :

(100 mW – 3 dB 50 mW)

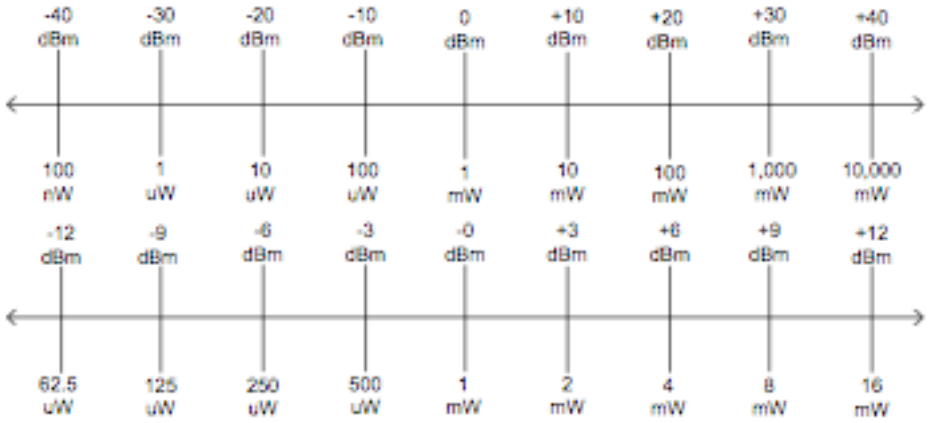
+10 dB akan meningkatkan nilai watt sebesar sepuluh kali lipat:

(10 mW + 10dB = 100 mW)

Sebaliknya, -10 akan mengurangi nilai watt sampai sepersepuluh dari nilai tersebut.

(300 mW – 10dB = 30 mW)

Aturan-aturan ini akan memberikan perhitungan yang cepat dari miliwatt daya level ketika diberikan daya level, gain, dan loss dalam dBm dan dB. Gambar 2.13 memberikan sebuah reference point yang selalu sama, tetapi level daya dapat berpindah kesalah satu arah dari reference point yang tergantung pada apa yang mereka representasikan pada daya, gain atau loss.



Gambar 2.13. Tabel Power Level

Grafik atas pada **gambar 2.13**, gain dan loss sebesar 10 dB ditunjukkan pada setiap penambahan. Perlu diperhatikan bahwa gain sebesar +10 dB dari reference point sebesar 1 mW memindahkan daya sampai +10 dBm (10 mW). Sebaliknya, perlu diperhatikan juga bahwa loss sebesar -10 dB memindahkan daya sebesar -10 dBm (100 microwatts). Pada grafik bawah juga menggunakan prinsip yang sama. Kedua grafik merepresentasikan maksud yang sama, kecuali yang satu dilakukan penambahan pada gain dan loss sebesar 3 dB dan yang satu lagi sebesar 10 dB. Dipisahkan menjadi dua grafik untuk kemudahan dalam pembacaan. Dengan menggunakan grafik diatas, maka akan lebih mudah melakukan konversi dBm dan mW pada level daya.

Contoh:

+43 dBm dibagi dengan 10 dan 3 sehingga menjadi +10+10+10+10+3. Dari reference point, gambar grafik menunjukkan bahwa dilakukan perkalian nilai miliwatt (dimulai dari reference point) sebuah factor dari perkalian sepuluh

sebanyak empat kali dan factor dari perkalian 2 sebanyak satu kali dan hasilnya adalah sebagai berikut :

```
1 mW x 10 = 10 mW
10 mW x 10 = 100 mW
100 mW x 10 = 1,000 mW
1,000 mW x 10 = 10,000 mW
10,000 mW x 2 = 20,000 mW = 20 watt
```

Sehingga kita dapat melihat bahwa daya sebesar +43 dbm sama dengan 20 watt. Contoh lain dengan ukuran daya negative, misalkan diberikan nilai reference point sebesar -26 dBm.

Pada contoh ini kita tahu bahwa -26 dBm sama dengan -10-10-3-3. Dari reference point, gambar grafik menunjukkan bahwa dilakukan pembagian pada nilai miliwatt (dimulai pada reference point) oleh factor dari 10 sebanyak dua kali dan factor dari 2 sebanyak dua kali dan hasilnya adalah sebagai berikut :

```
1 mW / 10 = 100 uW
100 uW / 10 = 10 uW
10 uW / 2 = 5 uW
5 uW/ 2 = 2.5 uW
```

Sehingga dapat dilihat bahwa daya sebesar -26 dBm sama dengan 2.5 microwatt.

2.4.6 dBi

Sebagaimana yang telah dibahas sebelumnya, gain dan loss diukur dalam decibel. Ketika dilakukan paengukuran gain pada antenna, satuan decibel direpresentasikan dengan dBi. Satuan ukuran dBi ditujukan hanya untuk gain pada antenna. Huruf “i” kepanjangan dari “isotropic”, yang mengartikan perubahan pada daya yang telah direferensikan untuk isotropic radiator. Isotropic radiator adalah sebuah teori transmitter ideal yang menghasilkan manfaat pada output field electromagnetic di segala arah dengan intensitas yang sama, dan pada effisiensi

100 %, dalam space 3-dimensi. Salah satu contoh dari isotropic radiator adalah matahari. Pikirkan bahwa dBi telah direferensikan untuk penyempurnaan. Ukuran dBi digunakan dalam perhitungan RF pada tata cara yang sama seperti dB. Satuan dBi adalah relative.

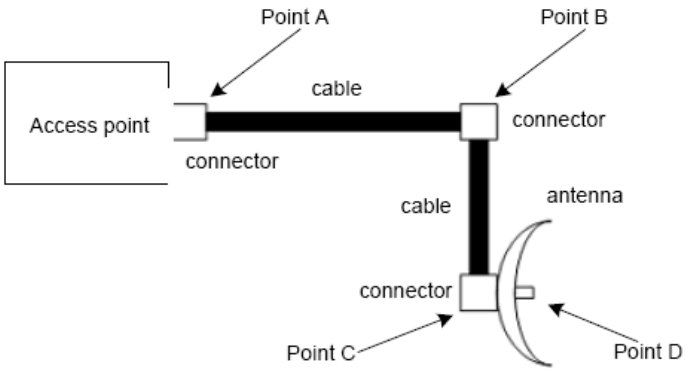
Dengan menganggap sebuah antenna sebesar 10 dBi dengan daya yang digunakan sebesar 1 watt. Sehingga EIRP adalah (daya output pada element antenna)?

1 W + 10 dBi (meningkat 10 kali lipat) = 10 W

Perhitungan ini bekerja pada cara yang sama seperti yang dapat dilihat pada gain yang diukur dalam dBi. Gain sebesar 10 dBi dikalikan dengan daya input pada antenna dengan factor. Antenna yang tidak berfungsi secara normal tidak dapat menurunkan sinyal, sehingga nilai dBi-nya selalu positif. Seperti halnya dB, dBi merupakan satuan ukuran yang relative yang dapat ditambah atau dikurangi dari satuan decibel yang lainnya. Sebagai contoh, jika sebuah sinyal RF direduksi sebesar 3 dB berjalan melewati copper cabel kemudian ditransmisikan oleh sebuah antenna dengan gain 5 dBi, maka hasilnya dari keseluruhan gain adalah +2 dB.

Contoh

Pemberian RF circuit pada Gambar 2.14, menentukan daya pada semua titik sasaran dalam miliwatt.



	Access Point	Point A	Point B	Point C	Point D
	100 mW	-3 dB	-3 dB	-3 dB	+12 dBi
=	100 mW	÷2	÷2	÷2	(x2 x2 x2 x2)
=	100 mW	÷2	÷2	÷2	x16
=	50 mW		÷2	÷2	x16
=	25 mW			÷2	x16
=	12.5 mW				x16
=	200 mW				

Gambar 2.14. Contoh Konfigurasi WLAN

2.4.7 Pengukuran Akurat

Meskipun teknik ini bermanfaat dan cocok pada semua situasi, ada beberapa masalah ketika rentetan angka yang telah ditetapkan tidak tersedia. Pada saat inilah digunakan rumus yang merupakan metode terbaik untuk melakukan perhitungan RF. Selama decibel merupakan satuan ukuran daya yang relative, perubahan dalam level daya menjadi implicit (tidak secara langsung). Jika level daya diberika dalam dBm, maka merubah kedalam dB akan lebih sederhana perhitungannya :

Daya awal = 20 dBm

Daya akhir = 33 dBm

Perubahan daya, Δ**P = 33-20 = +30 dB**, karena nilai yang dihasilkan adalah positif maka menandakan bahwa terjadi peningkatan pada daya.

Jika level daya diberikan pada miliwatt, prosesnya dapat lebih komplek lagi :

Daya awal (P*f*) = 130 mW

Daya akhir (P*i*) = 5,2 W

Perubahan daya,

$$\Delta P = 10 \text{ Log } (Pf / Pi)$$
$$= 10 \text{ Log } (5.2 \text{ mW} / 130 \text{ mW})$$
$$= 10 \text{ Log } 40$$
$$= 10 * 1.6$$
$$= 16 \text{ dB}$$

2.5 Kesimpulan

Frekuensi Radio adalah sinyal arus berfrekuensi tinggi yang berubah-ubah yang melewati konduktor tembaga yang panjang dan kemudian diradiasikan ke udara melalui sebuah antenna. Mengerti tingkah laku dari panyebaran gelombang RF adalah bagian penting untuk mengerti mengapa dan bagaimana wireless LAN berfungsi. Tanpa dasar pengetahuan tersebut,seorang administrator tidak mampu menentukan lokasi instalasi dari perlengkapan dan tidak akan mengerti bagaimana memecahkan masalah wireless LAN. Sifat dari RF atu Frekuensi Radio terdiri atas *Gain, Power Loss,* Refleksi / Pemantulan, Pembiasan, Difraksi, *Scattering*, dan Penyerapan. VSWR terjadi ketika terdapat impedalisi yang tidak cocok (hambatan arus dalam satuan ohm) antara alat dalam sistem RF. VSWR disebabkan oleh sinyal RF yang terpantul pada titik ketidakcocokan impedansi dalam path dalam empat sinyal. VSWR menyebabkan kehilangan kembalian, yang didefinisikan sebagai kehilangan energi maju melalui sebuah sistem yang disebabkan beberapa dayanya terpantulkan dan kembali ke pengirim. Antenna adalah media yang esensial dalam komunikasi Wireless untuk menghubungkan *Point* yang satu dengan yang lain. Hal yang penting di mengerti untuk antenna adalah Antenna menkonversi energi listrik gelombang ke gelombang RF. Dalam kasus antenna pentramisi, atau gelombang RF ke energi elektik dalam kasus antenna penerima. Dan, Dimensi fisik antenna seperti panjangnya berhubungan langsung dengan frekuensi dimana antennanya dapat menghambat gelombang atau menerima gelomang terhambat. Beberapa point penting dalam memahami pengadmintrasian werless LAN bebas lisensi adalah garis panjang, efek zona fresnel dan penapaian antenna, dalam melalui beamwidth terfokus.

2.6 SOAL

1. Sebutkan beberapa macam sifat dari Frekuensi Radio ?
2. Apakah pengertian dari *Intentional Radiator* ? (Jelaskan beserta gambar)
3. Sebutkan enpat bagian penting dari *Radio Frequency Mathematics* ?
4. Berapa *Zone Fresnel* yang dapat dihasilkan apabila diketahui dua Antenna Wireless LAN berjarak 0.4 mil dengan menggunakan frekuensi 1600 Mhz ?
5. Berapa perubahan daya apabila diketahui daya akhir yang dihasilkan empat kali dari daya awalnya ?

Bab 3. Teknologi Spread Spectrum

Dalam rangka untuk menjalankan dan menyelesaikan wireless Lan dengan baik, mengerti teknologi spread spectrum dan mengimplementasikannya dengan baik merupakan suatu keharusan. Dalam bagian ini, akan membahas apa teknologi spread spectrum dan bagaimana kegunaan menurut petunjuk FCC. Kita akan membedakan dan membandingkan dua bagian utama teknologi spread spectrum dan membahas, di dalamnya, bagaimana tekhnologi spread spectrum di implementasikan dalam wireless Lan.

3.1 Memperkenalkan Spread Spectrum

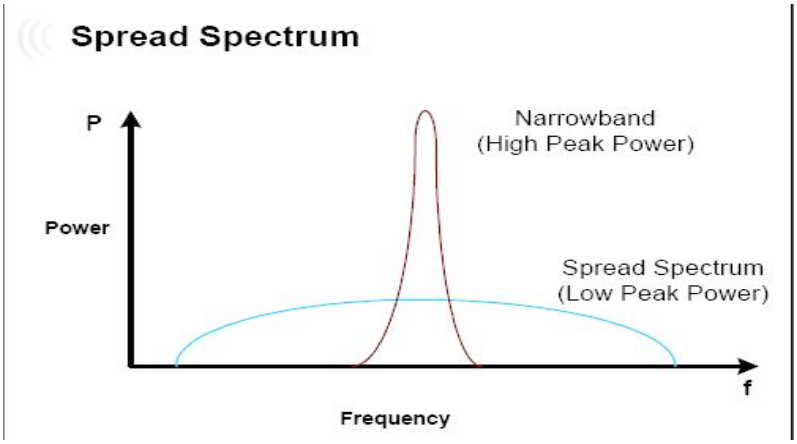
Spread spectrum adalah sebuah teknologi komunikasi yang memberikan karakter kepada lebar bandwidth dan low peak power. Spread spectrum komunikasi digunakan berbagai macam modulasi teknologi dalam wireless Lan dan memiliki banyak keuntungan, membatasi komunikasi narrow band. Gangguan yang sedikit akan mempengaruhi komunikasi pada spread spectrum dibandingkan pada komunikasi narrow band. Karena alasan ini, spread spectrum telah lama disangkutkan dengan militer. Dalam rangka membahas spread spectrum apa yang pertama kita harus tetapkan pada suatu referensi dengan membahas konsep pengiriman narrow band.

3.1.1 Mengirimkan Narrow Bandz

Suatu pengiriman narrow band adalah teknologi komunikasi yang hanya cukup digunakan dari frekwensi spectrum untuk membawa data sinyal, dan tidak lebih. Misi FCC untuk menjaga penggunaan frekwensi sebanyak mungkin, hanya membagi-bagikan apa yang diperlukan untuk melakukan pekerjaan. Spread spectrum bertentangan dengan misi karena menggunakan banyak band frekwensi yang lebih luas dibandingkan keperluan untuk mengirimkan informasi. Ini membawa kita kepada kebutuhan yang pertama pada suatu sinyal untuk spread spectrum. Suatu sinyal merupakan suatu sinyal spread spectrum ketika bandwidth lebih luas dari pada apa yang diperlukan untuk mengirimkan informasi.

Gambar 3.1 menjelaskan perbedaan diantara narrow band dan transmisi spread spectrum. Catatan bahwa satu karakteristik dari narrow band merupakan

high peak power. Power yang lebih diperlukan untuk mengirimkan suatu transmisi ketika penggunaan range frekwensi lebih kecil. Dalam urutan untuk sinyal narrow band untuk jadi diterima, mereka harus mengeluarkan tingkatan level atas dari noise, memanggil noise floor, dengan jumlah yamg significant. Sebab band menjadi narrow, high peak power memastikan resepsi error-free suatu sinyal narrow band.



Gambar 3.1. Narrow Band vs Spread Spectrum

Suatu argumentasi bertentangan dengan transmisi narrow band selain dari pada itu juga memerlukan narrow band untuk mengirimkan sinyal narrow band bisa jadi mengganggu atau mengalami gangguan campur tangan denagn mudah. Gangguan menjadi intensional yang menaklukkan transmisi menggunakan sinyal yang tak dikehendak imengirimkan pada band yang sama. Sebab band menjadi narrow, sinyal narrow band yang lain, termasuk noise, dengan sepenuhnya menghapus informasi dengan menaklukkan transmisi narrow band, seperti kereta lewat tengah menundukkan suatu ketenangan.

3.1.2 Teknologi Spread Spectrum

Teknologi spread spectrum mengijinkan kita untuk mengambil dengan jumlah informasi yang sama dengan sebelumnya yang akan dikirimkan dengan menggunakan sinyal pengangkut narrow band dan menyebarnya ke luar dengan frekwensi jarak yang lebih besar. Sebagai contoh, kita boleh menggunakan 1 MHz pada 10 Watt denagn narrow band, tetapi 20 MHz pada 100 mW dengan spread spectrum. Dengan penggunaan spectrum frekwentasi yang lebih luas, kita

mengurangi kemungkinan data yang akan rusak. Narrow band mengganggu usaha suatu sinyal spread spectrum yang akan mungkin dirintangi berdasarkan atas bagian kecil dari informasi sinyal narrow band dengan frekwensi jarak. Kebanyakan data digital akan diterima dengan error-free. Sekarang ini spread spectrum RF radio manapun dapat memancarkan kembali dengan jumlah yamg kecil dari kerugian data dalam kaitan dengan gangguan narrow band.

Selagi spread spectrum band secara relative luas, peak power dari sinyal merupakan quite low. Ini menjadi kebutuhan yang kedua untuk suatu sinyal untuk jadi dipertimbangkan spread spectrum. Karena suatu sinyal untuk dipertimbangkan spread spectrum, harus menggunakan low power. Dua karakteristik dari spread spectrum ini (penggunaan band frekwensi luas dan sangat low power) membuat kebanyakan penerima seolah-olah merupakan suatu sinyal noise. Noise adalah suatu band luas sinyal low power, tetapi berbeda dengan noise yang tak dikehendaki. Lagipula, Sejak kebanyakan radio penerima akan memandang sinyal spread spectrum sebagai noise, penerima ini tidak akan mencoba ke demodulate atau menginterpretasikan, menciptakan kurang lebih pengamanan komunikasi.

3.2 Penggunaan Spread Spectrum

Keamanan ini tidak bisa dipisahkan untuk menarik militer di dalam teknologi spread spectrum melalui tahun1950 dan tahun1960. Oleh karena itu noise seperti karakteristik, spread spectrum bisa dikirim di bawah noses lawan dengan menggunakan teknik komunikasi klasik. Keamanan hampir semua dijamin. Secara alami, keamanan komunikasi yang dirasakan hanya valid asalkan tidak ada yang menggunakan teknologi lain. Jika kelompok yang lain akan menggunakan teknologi yang sama, komunikasi spread spectrum ini bisa ditemukan, jika tidak diinterupsi dan dikodekan.

Di dalam tahun 1980, FCC menerapkan satu set aturan yang membuat teknologi spread spectrum untuk masyarakat dan memberikan harapan kepada penyelidikan dan riset ke dalam commercialisasi tentang teknologi spread spectrum. Meskipun demikian pada mulanya sekilas mungkin kelihatan bahwa militer telah kehilangan keuntungan, padahal itu tidak pernah. Band yang digunakan oleh militer berbeda dari band yang digunakan oleh masyarakat. Juga, militer menggunakan modulasi yang sangat berbeda dengan teknik encoding untuk memastikan bahwa komunikasi spread spectrum jauh

lebih sulit untuk menginterupsi dibanding mereka yang dari general public. Sejak tahun 1980, riset telah dimulai, spread spectrum telah digunakan dalam telepon cordless, global positioning systems (GPS), digital cellular telephony (CDMA), personal communications system (PCS), dan sekarang wireless local area networks (wireless Lan). Penggemar radio amatir kini mulai mengadakan percobaan dengan teknologi spread spectrum untuk banyak dipertimbangkan meraka yang mempunyai permasalahan.

Sebagai tambahan terhadap wireless Lan (WLan), wireless personal area networks (WPANs), wireless metropolitan area networks (WMANs), and wireless wide area networks (WWANs) adalah juga mengambil keuntungan dari teknologi spread spectrum. WPANs dengan menggunakan teknologi Bluetooth untuk mengambil keuntungan dari kebutuhan yang sangat low power untuk mengijinkan jaringan Wireless di dalam jarak yang sangat pendek. WWANs dan WMANs dapat menggunakan keuntungan antenna yang directional yang tinggi untuk membuat long-distance, high-speed RF yang menghungkan dengan low power.

3.2.1 Wireless Local Area Networks

Wireleess Lan, WMANs, dan WWANs menggunakan spread spectrum yang sama dengan cara yang berbeda. Sebagai contoh suatu wireless LAN mungkin bisa digunakan dalam bangunan untuk menyediakan penghubung para mobile, atau jembatan mungkin bisa digunakan untuk menyediakan building-to-building penghubung ke seberang suatu kampus. Ini adalah penggunaan yang spesifik dari teknologi spread spectrum yang tepat di dalam uraian suatu Local Area Network (LAN).

Penggunaan yang umum dari teknologi spread spectrum yaitu suatu kombinasi dari Wireless 802.11 yang memenuhi Lan dan 802.15 peralatan yang memenuhi Bluetooth. Dua teknologi ini sudah megcepture bagian pasar yang luar biasa, jadi merupakan ironis bahwa keduanya berfungsi dengan banyak cara yang berbeda, permainan di dalam FCC dengan aturan yang sama, tetapi sangat bertentangan satu sama lain. Riset pantas dipertimbangkan, waktu, dan sumber daya termasuk dalam pembuatan teknologi ini pada waktu yang sama.

3.2.2 Wireless Personal Area Networks

Bluetooth, paling populer dari teknologi WPAN yang ditetapkan oleh standart IEEE 802.15. Peraturan FCC mengenai penggunaan spread spectrum, mengijinkan untuk berbeda tipe dari implementasi spread spectrum. Beberapa format dari spread spectrum memperkenalkan konsep frekwensi hopping, yang mengirim dan menerima system hop dari frekwensi ke frekwensi di dalam band frekwensi yang mengirimkan data, Bluetooth hop kira-kira 1600 kali per detik sedang teknologi HomeRF (luas band teknologi WLAN) hop kira-kira 50 kali per detik. Kedua teknologi ini saling bertukar dari standart 802.11 WLAN, yang mana hop 5-10 kali per detik.

Masing teknologi ini mempunyai kegunaan yang berbeda di dalam pasar, tetapi semua tergolong dalam peraturan FCC. Sebagai contoh, ciri 802.11 frekwensi hopping WLAN boleh jadi diterapkan di lingkungan rumah dalam kaitan dengan pembatasan lower output power oleh FCC

3.2.3 Wireless Metropolitan Area Networks

Penggunaan spread spectrum lain, seperti link wireless yang mengilingi keseluruhan kota besar yang menggunakan high-power link point-to-point untuk membuat suatu jaringan, dalam mengenal sebagai Wireless Metropolitan Area Networks, atau WMANs. Menghubungkan banyak link point-to-point Wireless ke suatu jaringan ke seberang area yang geografisnya sangat besar dengan mempertimbangkan WMAN, tetapi masih menggunakan teknologi yang sama sebagai WMAN. Perbedaan WLAN dan WMAN, WMANs menggunakan frekwensi yang diizinkan sebagai ganti frekwensi yan tidak diizinkan dengan menggunakan WLan. Alasan untuk perbedaan ini bahwa organisasi menerapkan jaringan yang akan mengontrol jarak frekwensi di mana WMAN sedang diterapkan dan tidak perlu khawatir jika orang lain menerapkan jaringan yang bertentangan. Faktor yang sama berlaku pada WWANs.

3.3 FCC Specification

Meskipun ada implementasi yang berbeada dari teknologi spread spectrum, hanya dua jenis yang ditetapkan oleh FCC. Hukum menetapkan spread spectrum di dalam judul 47 melalui kongress dengan judul ”Telegraf, Telepon, dan Radiotelegraphs.” Hukum menyediakan basis untuk peraturan dan implementasi oleh FCC.Peraturan FCC

dapat ditemukan di dalam kode Peraturan Pemerintah pusat (CFR). Wireless LAN diuraikan di dalam peraturan ini.Peraturan FCC ini uraikan dua teknologi spread spectrum yaitu DSSS dan FHSS.

3.3.1 Frequency Hopping Spread Spectrum (FHSS)

Frekwensi hopping spread spectrum adalah suatu teknik yang menggunakan kecepatan frekwensi spread spectrum yang lebih dari 83 MHz. Kecepatan frekwensi mengacu pada kemampuan radio untuk merubah frekwensi transmisi di dalam RF band frekwensi yang dapat di pakai. Dalam frekwensi hopping wireless Lan, bagian yang dapat dipakai dari 2.4 GHz ISM band adalah 83.5 MHz, per peraturan FCC dan standart IEEE 802.11.

3.3.1.1 How FHSS Works ?

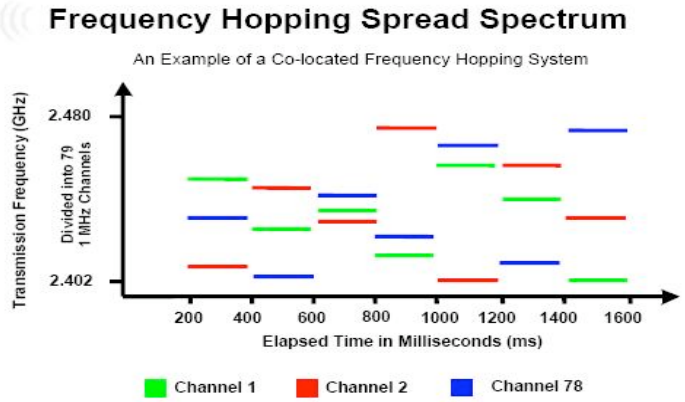
Dalam sistem frekwensi hopping, merubah frekwensi, atau hop, menurut urutan pseudorandom. Urutan pseudorandom adalah daftar beberapa frekwensi yang akan hop pada interval waktu yang ditetapkan sebelum mengulanginya. Pemancar menggunkan urutan hop untuk memilih frekwensi transmisinya. Pengngkut akan tinggal pada frekwensi tertentu untuk waktu yang ditetapkan (dikenal sebagai dwell time), dan kemudian menggunakan sejumlah waktu kecil untuk hop kepada frekwensi yang berikutnya (hop time).

Gambar 3.2 menunjukkan frekwensi hopping sistem menggunakan urutan hop frekwensi 5 MHz band. Di dalam contoh ini, urutannya adalah

1. 2.449 GHz
2. 2.452 GHz
3. 2.448 GHz
4. 2.450 GHz
5. 2.451 GHz

Ketika radio telah memancarkan informasi pada 2.451 GHz, radio akan mengulangi urutan hop, start lagi ke 2.449 GHz. Proses mengulang urutan selanjutnya sampai informasi diterima dengan sepenuhnya. Penerima radio disamakan ke pemancar hop radio dalam rangka menerima frekwensi yang

sesuai di proper time. Sinyal kemudian di demodulated dan digunakan oleh komputer yang menerima.



Gambar 3.2. Single FHSS

3.3.1.2 Effects Of Narrow Band Interference

Frekwensi hopping adalah suatu metoda data pengiriman di mana transmisi dan sistem menerima hop sepanjang pola frekwensi dapat diulang bersama-sama.

Dengan semua teknologi spread spectrum, frekwensi hopping sistem bersifat resistant tetapi tidak kebal untuk gangguan campur tangan narrow band. Di dalam contoh gambar 3.2, jika sinyal akan bertentangan dengan frekwensi sinyal hopping, pada 2.451 GHz hanya bagian dari sinyal spread spectrum yang hilang. Sisa dari sinyal spread spectrum akan tetap utuh, dan data yang hilang akan dipancarkan kembali. Pada kenyataannya, sinyal spread spectrum yang bertentangan boleh menduduki megahertz dari bandwidth. Sejak frekwensi hopping band selesai lebar 83 MHz, bahkan sinyal yang bertentangan akan menyebabkan sedikit penurunan dari sinyal spread spectrum.

3.3.1.3 Frequency Hopping Systems

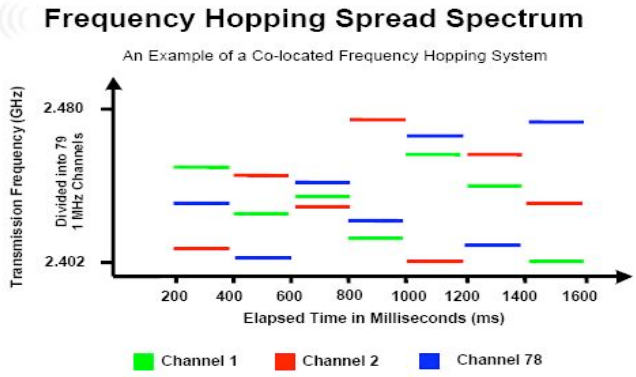
Adalah menjadi pekerjaan dari IEEE untuk menciptakan standart operasi dalam membatasi peraturan yang diciptakan oleh FCC. IEEE dan standart OpenAir mengenai sistem FHSS menguraikan:

- what frequency bands may be used (frekwensi band apa yang boleh digunakan)
- hop seguences
- dwell time
- data rates

Standart IEEE 802.11 menetapkan tingkat data1 Mbps dan 2 Mbps dan OpenAir (standart yang diciptakan oleh almarhum dalam wireless LAN bentuk interoperasi) menetapkan tingkat data 800 jbps dan 1.6 Mbps. Dalam rangka untuk sistem frekwensi hopping untuk 802.11 atau OpenAir, ia must beroperasi dalam 2.4 GHz ISM band (yang mana telah di definisikan oleh FCC dari 2.400 GHz ke 2.5000 GHz). Keduanya standart mengenai operasi dalam jarak 2.4000 GHz ke 2.4835 GHz. Sejak Wireless LAN Interoperability Forum (WLIF) tidak lagi mendukung standart yang di luar, system IEEE akan memenuhi untuk system FHSS dalam buku ini.

3.3.1.4 Channels

Suatu sistem frekwensi hopping akan beroperasi menggunakan pol suatu channel. Sistem frekwensi hopping secara khusus menggunakan hop standart 26 atau subnet daripadanya. Beberapa sistem frekwensi hopping mengijinkan hop menggunakan pola. Dan yang lain mengijinkan sinkronisasi antar sistem dengan menghapus collisions dalam menempatkan lokasinya. Meskipun mungkin untuk mempunyai sebanyak 79 poin-poin akses yang disamakan, dengan banyak sistem ini, masing-masing frekwensi hopping radio akan memerlukan sinkronisasi dengan semua dalam urutan tidak untuk bertentangan dengan frekwensi hopping radio yang lain dalam area. Harga system seperti itu menjadi penghalang dan biasanya tidak dipertimbangkan pada sustu pilihan. Jika radio tidak disamakan untuk digunakan, Kemudian 26 sistem dapat dilokasikan dalam Wireless LAN, jumlah ini dianggap sebagai maksimum dalam Wireless LAN medium-traffic. Lebih dari 15 sistem frekwensi hopping dilokasikan dalam lokasi yang bertentangan pada tingkat collisions itu akan mulai mengurangi kumpulan keluaran dari Wireless LAN



Gambar 3.3. Co-located FHSS

3.3.1.5 Dwell Time

Ketika mendiskusikan system frekwensi hopping, Kita sedang mendiskusikan sistem yang harus memancarkan pada frekwensi yang ditetapkan untuk sementara waktu, Kemudian hop pada suatu frekwensi yang berbeda unutk melanjutkan pemancaran. Ketika sistem frekwensi hopping memancarkan pada frekwensi, harus melakukan sejumlah waktu yang ditetapkan. Wkatu ini akan memanggil dwell time. Sekali ketika dwell time berakhir, system tombolke frekwensi yang berbeda dan mulai unutuk memancarkan lagi. Suatu sistem frekwensi hopping memancarkan dua frekwensi,2.401 GHz dan 2.402 GHz. Sistem akan memancarkan pada frekwensi 2.401 GHz untuk durasi dari dwell time-100 miliseconds (ms), sebagai contoh. Setelah 100 ms radio harus berubah pemancarkan frekwensi pada 2.402 GHz dan mengirimkan informasi pada frekwensi untuk 100 ms.

3.3.2 Direct Sequence Spread Spectrum (DSSS)

Direect Sequence Spread Spectrum sangat dikenal luas dan merupakan tipe spread spektrum yang paling banyak digunakan, digunakan oleh aplikasi yang sangat popular, mudah penggunaan dan memiliki rate data yang tinggi. DSSS merupakan sebuah metode pengiriman data dimana pengiriman dan penerimaan data berada pada range frekuensi 22 MHz. Chanel yang lebih lebar akan membuat peralatan dapat mengirim informasi lebih tinggi daripada system FHSS

3.3.2.1 Bagaimana DSSS Bekerja

DSSS menggabungkan sebuah data sinyal pada station pengiriman dengan kecepatan bit sequence yang tinggi dimana direferensikan sebagai chipping code atau penguatan prosesor. Sebuah prosesor yang tinggi akan menambah resistansi sinyal untuk saling berinteferensi. Proses dari direct sequence dimulai dengan sebuah carier dimodulasikan dengan kode sequence. Angka pada chips dalam kode akan menentukan bagaimana penyebaran terjadi dan angka dari chips serta kecepatan dari kode akan menentukan kecepata data.

3.3.2.2 Direct Sequence Systems

Dalam ISM band 2.4 GHz, IEEE telah menjelaskan bahwa penggunaan DSSS pada rate data 1 atau 2 Mbps dibawah standar 802.11. Peralatan IEEE 802.11b beroperasi pada 5.5 atau 11 Mbps yang akan mampu berkomunikasi dengan peralatan 802.11 yang beroperasi pada 1 atau 2 Mbps hal ini dikarenakan tipe 802.11 b menyediakan kemampuan untuk berkomunikasi dengan versi sebelumnya.

3.3.2.3 Channels

Tidak seperti frekuensi hoping system yang menggunakan rangkaian lompatan untuk mendefinisikan chanel-chanel, direct system menggunakan definisi chanel yang lebih konvensional. Masing-masing chanel merupakan band yang saling berdekatan dengan lebar frekuensi 22 MHz dan 1 MHz frekuensi carier digunakan hanya sebagai FHSS. Chanel 1 beroperasi dari 2.401 GHz – 2.423 GHz dan chanel 2 operates dari 2.406 – 2.429.

3.3.3 Akibat dari Narrow Band Interfence

Seperti sistem frekuensi hop, direct sequence system selalu resistan. Sebuah sinyal DSSS akan lebih suspek daripada FHSS karena band DSSS sangat kecil

(dengan lebar 22 MHz 79 MHz yang digunakan FHSS) dan informasi dikirim melalui simultan band. Dengan FHSS, frekuensi akan sulit dan lebar frekuensi akan mengalami interferensi.

3.3.4 Akibat Aturan FCC terhadap DSSS

Hanya karena sistem FHSS, FCC menggunakan regulasi bahwa sistem DSSS menggunakan 1 w untuk point to multipoint. Keluaran maksimum yang berdiri sendiri dari channel yang dipilih, artinya channel yang disetujui, daya keluaran yang sama. Regulasi ini mengaplikasikan spread spectrum antara 2.4 GHz ISM band dan naik 5 GHz UNII band.

3.3.5 Perbandingan FHSS dan DSSS

Antara teknologi FHSS dan DSSS memiliki kelebihan dan kekurangan, dan hal itu urusan dari administrator Wireless LAN untuk memberikan tiap kelebihan dan kekurangan ketika memutuskan bagaimana mengimplementasikan Wireless LAN. Pada bagian ini akan membahas beberapa faktor yang seharusnya didiskusikan ketika membandingkan teknologi yang akan diimplementasikan pada perusahaan kita, yaitu

- Narrowband interference
- Co-Location
- Cost
- Equipment Compability & Availability
- Data rate & Thoughput
- Security
- Standards Support

3.4 Narrowband Interference

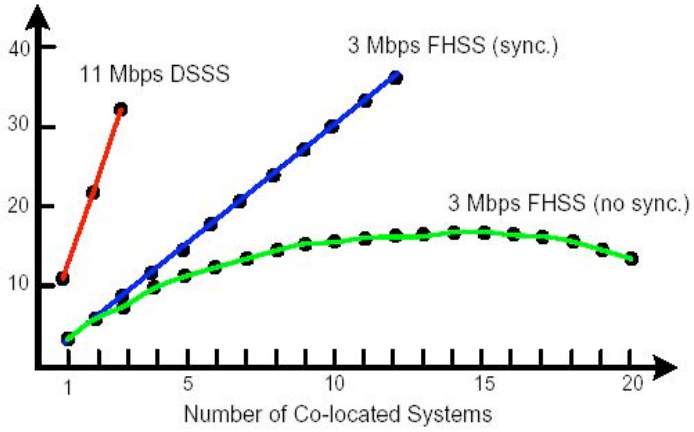
Salah satu kegunaan system FHSS adalah resistensi yang besar untuk narrowband interference. System DSSS mungkin diakibatkan oleh Narrowband interference dan pada system FHSS karena menggunakan 22 MHz dibandingkan dengan 79 MHz FHSS.

3.4.1 Cost

Ketika mengimplementasikan jaringan wireless LAN, kegunaan dari sistem DSSS mungkin lebih murah dari pada sistem FHSS. Biaya untuk mengimplementasikan sebuah direct sequence system sangat sulit. Sejak sistem frekuensi hop yang jelek.

3.4.2 Co-Location

Sebuah kegunaan dari FHSS dari DSSS adalah kemampuan yang lebih pada sistem frekuensi hop untuk di-co-located ke direct sequence system. Sejak sistem frekuensi hop disebut frekuensi yang jelek dan menggunakan 79 channel diskrit, yang mana memiliki c-location maksimum terhadap 3 access point.



Gambar 3.4. Perbandingan Co-location

Bagaimanapun, ketika dihitung biaya hardware pada sistem FHSS untuk mendapatkan sistem DSSS secara keseluruhan, kegunaan akan cepat hilang. Karena sistem DSSS memiliki 3 co-located access point, secara keseluruhan konfigurasi ini akan menjadi

```
3 access point x 11 Mbps = 33 Mbps
```

atau secara kasaran 50 % dari bandwith rate, sistem DSSS secara keseluruhan

```
33 Mbps / 2 = 16.5 Mbps.
```

Home RF2.0 menggunakan lebar band frekuensi hoping teknologi untuk mencapai 10 Mbps kecepatan data.,dimana kira-kira pada putaran 5 Mbps keluaran yang sebenarnya.

Penangkap membandingkan Home RF2.0 ke 802.11 atau 802.11b system aplles ke apples. Perbedaannya ialah HomeRF batas keluaran powernya (125 mW) dibandingkan dengan 802.11 sistem (1 watt).

Ketika wireless frame dipancarkan , sinyal akan berhenti antara data frame untuk mengontrol sinyal dan perintah over head lainnya.Dengan frekuensi system hoping ini "interframe spacing " lebih panjang daripada menggunakan direct sequence system, menyebabkan kecepatan data yang dikirim melambat. Sebagai tambahan ketika system frekuensi hoping dalam proses perubahan frekuensi pemancar , tidak ada data yang terkirim.ini menyebabkan lebih banyak kehilangan output, meskipun hanya sebagian kecil. Beberapa wireless LAN system menggunakan phisycal layer protocol dalam beberapa macamnya untuk meningkatkan output.Cara kerja metode ini menguntungkan keluarannya setinggi 80 % dari keceptana transfer data, tetapi juga mengakibatkan pengorbanan antar kemampuan pengoperasiannya.

3.4.3 Keamanan

Kelebaran toute dan mitos bahwa frekuensi system hoping tidak dapat dipisahkan keamanannya dengan direct sequences system. Fakta utama mitos ini tidak membuktikan bahwa FHSS radio hanya dibuat oleh beberapa perusahaan kecil saja. Dari beberapa perusahaan ini semuanya mematuhi standard seperti 802.11 atau OpenAir dalam usaha menjual produknya lebih efektif. Kedua kebanyakan perusahaan menggunakan standar dari hop sequences, yang umumnya digabungkan dengan daftar pre-determined , diprodusi dengan standar organisasi (IEEE atau WLIF). Kedua macam bentuk itu membuat kode hop sequences relative sederhana.

Alasan lain yang membuat hop sequences sangat sederhana ialah banayak channel yang di siarkan sangat bersih dengan beberapa pemancar.Juga MAC address yang dipancarkan access point dapat dilihat setiap pemancar(dengan indikasi buatan dari pabrik radio). Beberapa perusahaan memperbolehkan

administrator lebih fleksibel dlam mendefinisikan sendiri bentuk hopping.Walaupun kejadian ini biasanya level keamanannya tidak ada sejak alat canggih seperti spectrum analyzer dan laptop computer dapat digunakan untuk jalur bentuk hopping dari FHSS radio dalam detik.

3.4.4 Standard Support (Dukungan Standar)

Dalam diskusi sebelumnya , DSSS mempunyai lebar gain yang harus diberikan untuk biaya rendah, kecepatan tinggi, WECA's Wi-Fi standar operasioanal , dan banyak factor lainnya.Pasar akan mengijinkan hanya kecepatan perubahan industri yang harus diberikan, DSSS system lebih cepat seperti 802.11g baru dan 802.11 a wireless LAN hardware .WECA's baru mengoperasikan WiFi5 standar untuk 5GHz DSSS system operasi pada UNII band yang membantu pergerakan industri pada direksi yang sama. Standar baru FHSS system terdapat HomeRf2.0 dan 802.15 (mendukung WPAN's seperti Bluetooth), tetapi tidak untuk advancing FHSS system pada enterprise. Semua standar itu dan teknologinya akan dibicarakan didepan pada bab 6.

3.5 Kesimpulan

Spread spectrum adalah sebuah teknologi komunikasi yang memberikan karakter kepada lebar bandwidth dan low peak power. Spread spectrum komunikasi digunakan berbagai macam modulasi teknologi dalam wireless Lan dan memiliki banyak keuntungan yaitu membatasi komunikasi *Narrow Band.* Suatu pengiriman narrow band adalah teknologi komunikasi yang hanya cukup digunakan dari frekwensi spectrum untuk membawa data sinyal, dan tidak lebih. Penerapan dari aplikasi komunikasi Wireless diantaranya wireless personal area networks (WPANs), wireless metropolitan area networks (WMANs), and wireless wide area networks (WWANs). Teknologi Spread Spektrum terbagi atas FHSS (Frequency Hoping Spread Spectrum) dan DSSS (Direct Sequence Spread Spectrum).

3.6 SOAL

1. Apakah yang dimaksud dengan pengiriman sinyal *Narrow Band* ?
2. Jelaskan tentang pengertian FHSS ?
3. Jelaskan tentang pengertian DSSS ?
4. Sebutkan dalam apa saja perbedaan antara FHSS dengan DSSS ?
5. Bagaimana prinsip kerja dari DSSS ?

Bab 4. Perangkat untuk Infrastruktur

Pada bab dari buku ini kita akan banyak membahas bagian hadware wireless LAN. Seperti yang disebutkan pada bab sebelumnya, kita dapat memilih sebuah keperluan dasar untuk jaringan wireless SOHO (Small Office Home Office) dibawah 400 dolar, termasuk sebuah Accesss Point, kartu wireless PC, dan mungkin sebuah USB client. Meskipun dengan tipe perlengkapan ini kita tidak mempunyai pengalaman dengan setiap bagian yang dicakup pada bab ini, kita akan memiliki ide bagus bagaimana mengkomunikasikan beberapa peralatan tersebut dengan kata lain bekerja menggunakan teknologi RF (Frekuensi Radio).

Pada bagian ini meliputi kategori berbeda dari perlengkapan infrastruktur jaringan wireless dan beberapa variasi didalam tiap kategori. Dengan membaca sendiri bagian ini, kita dapat lebih jelas mencerna implementasi terkini jaringan wireless, walaupun sederhana kita alan tahu semua perbedaan macam-macam perlengkapan wireless LAN yang kita punyai. Hal ini akan membantu kita dalam membuat atau menambahkan ke sebuah jaringan wireless. Materi hardware ini pembangunan secara fisik tiap wireless LAN.

Pada umumnya, kita akan melingkupi tiap tipe hardware pada bagian ini pada cara yang sama menurut topik dibawah ini :

- Mendefinisikan dan peranan hardware pada jaringan
- Pilihan umum yang mungkin termasuk dengan hardware
- Bagaimana memasang dan mengkonfigurasikan hardware

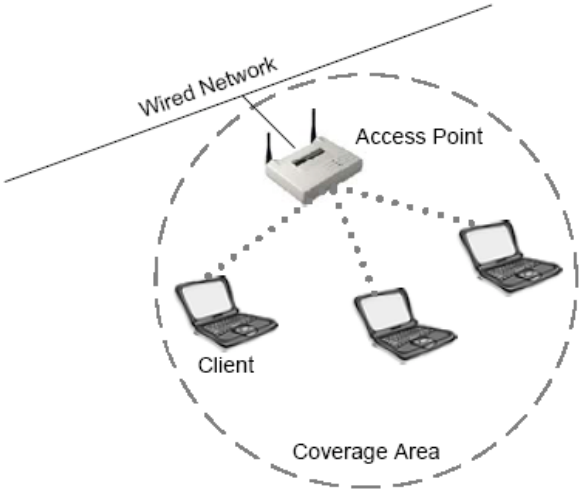
Tujuan dari bab ini adalah membuat kita mengerti akan kebutuhan hardware yang kita perlukan untuk banyak konfigurasi bermacam-macam wireless LAN.

4.1 Access Point

Dasar kedua kartu wireless PC, accesss point/AT, kemungkinan peralatan paling umum untuk Wireless LAN yang mana kita akan bekerja sebagai administrator Wireless LAN. Seperti nama disarankan, accesss point menyediakan client dengan sebuah point untuk mengakses ke dalam sebuah jaringan. Sebuah accesss point adalah sebuah peralatan *half duplex* dengan kecerdasan yang sesuai untuk kecanggihan switch

Ethernet. Gambar 4.1 menunjukkan sebuah contoh dari sebuah accesss point, dimana Gambar 4.2 mengilustrasikan dimana sebuah accesss digunakan pada sebuah wireless LAN.

Gambar 4.1. Access Point



Gambar 4.2. Installasi AP di Jaringan

4.1.1 Mode Access Point

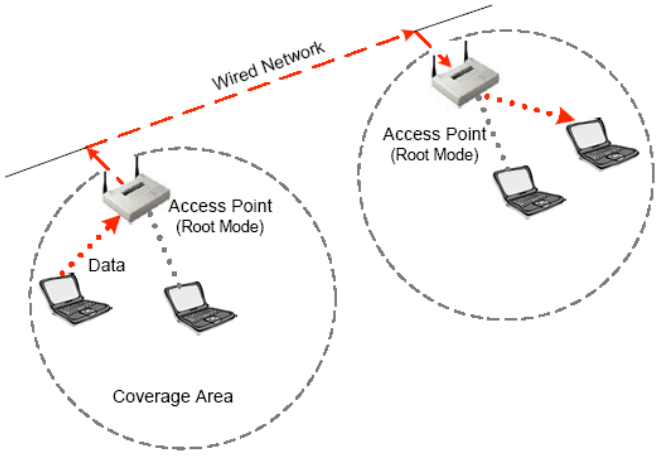
Accesss point berkomunikasi dengan wireless clientnya, dengan jaringan kabel dan dengan accesss point lainnya. Ada 3 macam model pada accesss point yang akan dikonfigurasikan:

- Root Mode
- Repeater Mode
- Bridge Mode

Tiap model akan digambarkan dibawah ini

4.1.1.1 Root Mode

Root Mode digunakan ketika accesss point dikoneksikan ke sebuah tulang punggung kabel (wired backbone) sepanjang interface kabel (biasanya Ethernet)/ kebanyakan accesss point mendukung model lebih dari model root hadir dikonfigurasikan secara default. Ketika sebuah accesss ponit dikoneksikan ke segment kabel sepanjang port Ethernetnya, normalnya itu (accesss point) akan dikonfigurasikan sebagai mode root. Ketika dalam mode root, accesss point terkoneksi pada sistem distribusi kabel yang sama dapat berkomunikasi satu sama lain melalui segment kabel. Accesss point dapat berkomunikasi satu sama lain ke fungsi koordinat penjelajahan sama seperti pengassosiasian kembali. Wireless client dapat berkomunikasi dengan wiress client lainnya pada lokasi yang cellnya berbeda sepanjang access point masing-masing ke seberang segment kabel, seperti yang ditunjukkan Gambar 4.3

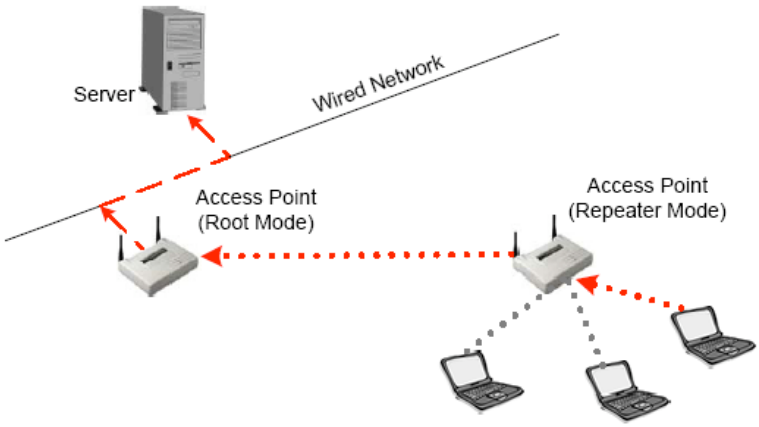


Gambar 4.3. Root Mode

4.1.1.2 Repeater Mode

Dalam mode pengulangan, accesss point memiliki kemampuan untuk mendukung sebuah koneksi wireless upstream (hulu) kedalam jaringan kabel lebih dari koneksi normal kabel. Seperti yang kita lihat pada Gambar 4.4, satu accesss point melayani sebagai accesss point root dan lainnya melayani

sebagai sebuah wireless repeater. Acess point dalam mode repeter terkoneksikan ke client sebagai accesss point dan terkoneksikan ke accesss point upstream root sebagai client itu sendiri. Menggunakan accesss point dalam mode repeater adalah tidak disarankan jika tidak benar-benar dibutuhkan karena cell disekitar tiap accesss point pada skenario ini harus tumpang tindih minimal 50 %. Konfigurasi ini mengurangi secara drastis jangkauan pada tiap client yang apat konek ke accesss point repeater. Tambahan, accesss point repeater berkomunikasi dengan client sama baiknya pada accesss point upstream melalui koneksi wireless, mengurangi throughput pada wireless segment. Pengguna dapat membebankan pada koneksi wireless akan mengalami throughput/keluaran yang rendah dan meningkatnya keterpendaman pada skenario ini. Pada dasarnya untuk port Ethernet kabel dapat dihentikan ketika dalam mode repeater.

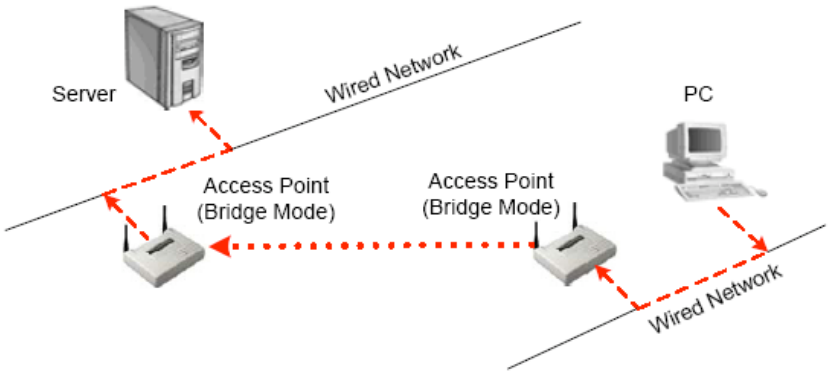


Gambar 4.4. Repeater Mode

4.1.1.3 Bridge Mode

Pada model jembatan, accesss point bertindak tepatnya sebagai jembatan wireless, yang mana akan didiskusikan nanti pada bagian ini. Kenyataannya, mereka menjadi jembatan wireless ketika dikonfigurasikan pada cara ini. Hanya sebagian kecil accesss point di pasaran yang memiliki fungsi jembatan, yang mana ciri khasnya ditambahkan biaya tertentu untuk perlengkapan. Kita akan menjelaskan singkat bagaimana fungsi jembatan wireless, tetapi kita dapat melihat dari Gambar 4.5 bahwa client tidak diasosiasikan ke jembatan,

tetapi sedikit, jembatan digunakan untuk sambungan dua atau lebih segment kabel bersama sama wireless.



Gambar 4.5. Bridge Mode

4.2 Fixed atau Detachable Antenna

Tergantung kebutuhan organisasi atau client, kita memerlukan pilihan antara memiliki accesss point dengan antenna tetap (artinya tidak dapat berpindah-pindah) atau antenna berpindah. Sebuah accesss point dengan antenna berpindah memberikan kita kemampuan untuk menyertakan sebuah antenna berbeda untuk accesss point yang digunakan apapun panjang kabel yang kita butuhkan. Sebagai contoh, jika kita memerlukan untuk memasang accesss point didalamnya dan memberikan koneiksi dengan user luar ke dalam jaringan. Kita dapat menertakan sebuah kabel dan sebuah antenna luar ruangan langsung ke accesss point dan hanya memasang antenna luar.

Access point dapat dikirimkan dengan atau tanpa antenna berbeda. Antenna wireless LAN berbeda digunakan dari bermacam-macam antenna dengan bermacam-macam input pada satu penerima dalam rangka menyample sinyal dari seluruh tiap antenna. Inti sample/contoh dua antenna adalah untuk mengambil input sinyal dari antenna yang menerima penerimaan sinyal terbaik. Dua antenna mungkin dapat memiliki perbedaan penerimaan sinyal karena sebuah gejala yang disebut multipath, yang mana akan dibicarakan secara detail pada Bab 9.

4.3 Kemampuan Penyaringan Tingkat Lanjut

MAC atau protokol kemampuan penyaringan dapat dimasukkan pada sebuah accesss point. Penyaringan biasanya digunakan untuk melihat keluar penyusup pada

jaringan wireless LAN kita. Seperti sebuah persyaratan dasar keamanan (dicakup dalam Bab 10 – Keamanan), sebuah accesss point dapat dikonfigurasikan untuk menyaring keluar peralatan yang tidak terdaftar pada daftar Penyaring MAC accesss point yang mana dikendalikan administrator.

Protokol penyaringan mengijinkan administrator untuk memutuskan dan mengontrol protokol yang mana yang digunakan melalui koneksi wireless. Sebagai contoh, jika seorang administrator hanya mengharapkan menyediakan akses protokol http melalui koneksi wireless jadi user dapat menjelajah web dan mencek emailnya melalui email, kemudian mensetting sebuah protokol http akan mencegah semua tipe protokol lainnya ke segment dari jaringan.

4.4 Kartu Radio (modular) Berpindah

Beberapa manufaktur mengijinkan kita menambah atau mengurangi radio ke dan dari slot PCMIA yang dibangun pada accesss point. Beberapa accesss point dapat memiliki slots PCMIA untuk fungsi spesial. Mempunyai dua slot radio dalam sebuah accesss point mengijinkan satu kartu radio untuk bertindak sebagai sebuah accesss point sementara kartu radio lainnya bertindak sebagai jembatan (pada kebanyakan kasus sebuah backbone wireless). Kegunaan sedikit banyak ketidaksamaan adalah untuk digunakan tiap kartu radio sebagai sebuah accesss point yang berdiri sendiri (independent). Memiliki tiap kartu bertindak sebagai accesss point independent mengijinkan seorang administrator untuk mengakomodasikan keduanya seperti banyak user pada ruang fisik yang sama tanpa pembelian sebuah accesss point kedua, yang lebih jauh lagi pada pengurangan biaya. Ketika accesss point dikonfigurasikan pada cara ini, tiap kartu radio harus dikonfigurasikan pada sebuah channel yang tidak tumpang tindih (non-overlapping), diharapkan idealnya channel 1 dan 11.

4.5 Variabel Output Power

Variabel output power mengijinjan administrator untuk mengontrol power (dalam miliwatts) dari accesss point yang digunakan untuk mengirim data itu sendiri. Mengontrol output power menjadi penting dalam beberapa situasi dimana jarak node

tidak dapat menentukan letaknya accesss point. Itu juga dapat sederhana menjadi sebuah kemewahan mengijinkanmu mengontrol area yang dicakup accesss point. Seperti output power yang ditingkatkan pada accesss point, client akan dapat bergerak lebih jauh dari accesss point tanpa kehilangan konektivitas. Fitur inijuga dapat membantu keamanan dengan mengijinkan untuk ukuran cell frekuensi radio sehingga penyusup tidak dapat untuk jaringan dari luar dinding bangunan.

Alternatif fitur output variabel power adalah digunakan untuk output accesss point yang tetap. Dengan sebuah output tetap dari akses point, ukuran kreatif seperti amplifier, attenuator, panjang kabel atau penambahan ketinggian antenna yang akan diimplementasikan. Kedua pengendalian keluaran power dari accesss point dan antenna juga dianggap operasi penting didalam aturan petunjuk FCC. Kita akan membicarakan item ini pada Bab 5, antenna dan aksesorisnya

4.6 Berbagai Macam Tipe Sambungan Kabel

Pilihan sambungan untuk sebuah accesss point dapat termasuk sebuah sambungan 10baseTx, 10/100baseTx,100baseTx, 100baseFx, token ring, atau lainnya. Karena sebuah accesss point pada sepanjang peralatan umumnya yang mana mengkomunikasikan client dengan jaringan kabel backbone, administrator harus mengerti bagaimana untuk sepantasnya mengkoneksikan akses point ke dalam jaringan kabel. Desain jaringan sepantasnya dan konektisitas akan membantu mencegah akses point menjadi sebuah bottleneck dan akan memberikan hasil sejauh problem kecil pada tidakberfungsinya peralatan.

Menggunakan sebuah pertimbangan standar, terbatas untuk akses point digunakan dalam sebuah perusahaan wireless LAN. Jika pada kasus ini akses point dialokasikan 150 meter dari pengkabelan terdekat, jalankan sebuah kategori 5 kabel ethernet untuk accesss point kemungkinan tidak bekerja. Pada skenario ini akan ada sebuah masalah karena Etheernet melalui kabel kategori 5 hanya khusus untuk 100 meter. Pada kasus ini, pembelian sebuah konektor 100baseFx dan jalankan fiber dari lemari pengkabelan ke akses point dipasang lokasi mendahului waktu akan megkonfigurasikan ke fungsi yang seharusnya dan lebih mudah.

4.7 Konfigurasi dan Management

Metode atau metode yang digunakan untuk konfigurasi dan mengatur akses point akan berbeda pada tiap buatan pabrik. Kebanyakan merek menawarkan paling tidak console, telnet, USB atau sebuah web server built-in untuk akses browser, dan beberapa akses point akan memiliki configurasi pilihan dan management software. Konfigurasi akses point dari pabrik dengan sebuah alamat IP selama inisialisasi konfigurasi. Jika administrator memerlukan mereset peralatan ke setingan awal pabrik, biasanya berupa tombol reset hardware pada luar unit/alat untuk tujuan ini.

Bermacam-macam fitur ditemukan dalam akses point. Bagaimanapun, satuhal adalah konstan, beberapa fitur akses point yang dimiliki, beberapa biaya akses point.sebagai contoh, beberapa akses point SOHO akan memiliki WEP, filter MAC dan bahkan sebuah web server built-in. Jika fitur seperti melihat asosiasi kabel, dukungan 802.1x/EAP, dukungan VPN, fungsi routing, protokol Inter-accesssPoint, dan kebutuhan dukungan RADIUS, yang diharapkan dalam pembayaran yang lebih untuk sebuah accesss point level perusahaan.

Tiap fitur yang standard pada Wi-Fi menurut akses point kadang berbeda pada penerapannya. Sebagai contoh, dua merek berbeda dari sebuah accesss point SOHO mungkin menawarkan filter MAC, tapi hanya salah satu dari keduanya yang akan menawarkan filtering MAC dimana kita dapat dengan tegas mengijinkan dan dengan jelas menolak stasiun, lebih dari satu atau lainnya. Beberapa accesss point mendukung full-duplex 10/100 koneksi pengkabelan dimana lainnya hanya menawarkan koneksitas 10baseT half duplex pada sisi pengkabelan.

Mengerti fitur apa yang diharapkan pada sebuah SOHO, jangkauan menengah, level accesss point perusahaan adalah bagian penting dari menjadi seorang administrator jaringan wireless. Daftar dibawah ini dengan tidak menjelaskan secara lengkap karena pabrik meluncurkan sering fitur baru pada tiap level. Pada daftar ini berarti menyediakan sebuah ide dimana untuk memulai mencari sebuah daftar akses point yang sesuai. Pada daftar ini dibuat atas tiap awal lainya dengan level SOHO access point, berarti bahwa setiap level yang lebih tinggi termasuk fitur dari layer dibawahnya.

4.7.1 Small Office, Home Office (SOHO)

- Penyaringan MAC
- WEP (64 atau 128 bit)

- Konfigurasi Interface USB atau console
- Interface konfigurasi built-in server sederhana
- Aplikasi konfigurasi pilihan sederhana

4.7.2 Perusahaan

- Aplikasi konfigurasi pilihan tingkat lanjut
- Interface konfigurasi web server built-in tingkat lanjut
- Akses Telnet
- Management SNMP
- 802.1x/EAP
- RADIUS client
- VPN client dan server
- Routing (static/dinamic)
- Fungsi Repeater
- Fungsi jembatan

Menggunakan panduan manual awal yang cepat akan mendukung informasi yang lebih spesifik dari tiap merek. Beberapa fungsi, seperti memiliki yang dilakukan untuk keamanan seperti dukungan terhadap RADIUS dan dukungan VPN, diduskusikan pada bagian selanjutnya. Beberapa fungsi termasuk bagian sebelum kebutuhan untuk membaca buku ini,seperti telnet, USB dan web server. Topik lainnya, seperti sebuah routing dicakup dalam buku ini.

Seperti seorang administrator wireless LAN, kita harus tahu lingkunganmu, mencari produk yang cocok membangun dan keamanan yang diperlukan dan membandingkan fitur antara 3-4 dan membuat produk untuk untuk segment pasar. Proses evaluasi ini niscaya akan memakan banyak waktu, tetapi waktu yang dihabiskan mempelajari tentang perbedaan produk pada pasar sangat berguna. Kemungkinan sumber terbaik untuk belajar tentang tiap persaingan merek dalam sebuah pasar tertentu pada tiap website pembuatnya. Ketika memilih sebuah accesss point, pastikan untuk mendapatkan dukungan account pembuatnya, sebagai tambahan fitur dan harga.

4.7.3 Mounting / Cara Kerja Pemasangan

- Gunakan duty zip ties untuk memasang accesss point ke kolom atau sorotan.
- Jangan tutupi cahaya akses point ketika memasang accesss point dengan zip ties
- Pasang akses point terbalik sehingga lampu indikator dapat terlihat dari lantai
- Beri nama accesss point

Ketika pemasangan sorotan, salah satunya menggunakan langsung zip ties atau mungkin pemasangan 2x4 ke sorotan dengan penjepit dengan pemasangan akses point kepadanya. Jangan lupa untuk memasang antenna dengan cara yang sama sepertisurvey yang spesifik pada situs.

Beberapa akses point dapat datang dengan pemasangan lubang slide dan lainya akan memiliki perlengkapan terpisah atau frame yang akan memasangnya. Beberapa ajangan diterapkan dengan switch untuk memasangnya. Beberapa jangan lakukan sesuai dengan desain yang digunakan untuk dipasang.

4.8 Tipe Wireless Bridges

Sebuah wireless bridge mendukung konektivitas antara 2 segment LAN kabel dan digunakan point to point atau konfigurasi point to multipoint. Sebuah wireless bridges adalah peralatan yang mempunyai kemampuan half duplex hanya dari layar 2 wireless konektivitas. Gambar 4.6 menggambarkan sebuah contoh dari sebuah wireless bridge, ketika diilustrasikan pada Gambar 4.8 dimana sebuah wireless bridge digunakan pada sebuah wireless LAN.

Gambar 4.6. Wireless Bridge

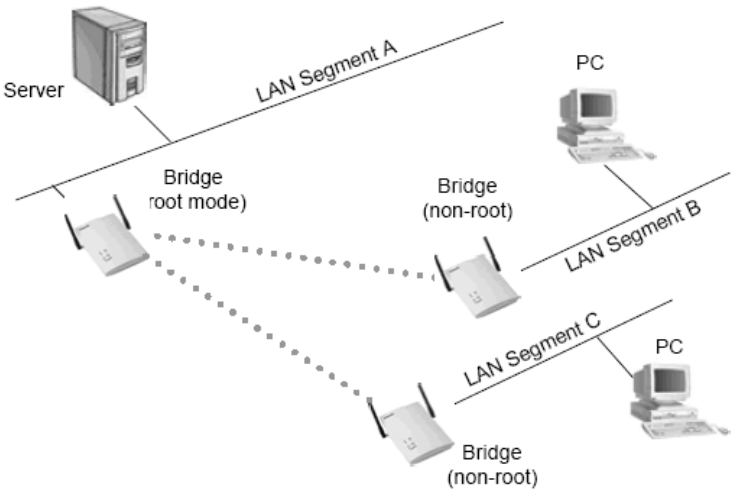
4.8.1 Wireless Bridges Mode

Wireless Bridges berkomunikasi dengan dengan wireless bridge lainnya pada salah satu dari 4 tipe:

- Root mode
- Non-root Mode
- Access point Mode
- Repeater Mode

4.8.1.1 Root Mode

Satu jembatan pada tiap grup bridge harus di set sebagai root bridge. Sebuah root bridge dapat hanya berkomunikasi dengan yang bukan root bridge dan peralatan clientnya dan tidak dapat diasosiasikan dengan root bridge. Gambar 4.7 diilustrasikan sebuah root bridge berkomunikasi dengan yang bukan root bridge.



Gambar 4.7. Komunikasi Root Mode

4.8.1.2 Non-root Mode

Wireless bridge pada anggapan tipe root mode, bersifat wireless, ke wireless bridges yang ada mode root. Beberapa pabrik wireless mendukung konektivitas ke tipe yang bukan root bridge ketika bride pada tipe akses point. Mode ini biasanya sebuah tipe spesial dimana bridge bertindak sebagai sebuah accesss point dan sebagai sebuah bridge simultan. Peralatan client diasosiasikan untuk accesss point (atau bridge pada tipe accesss point) dan bridge berkomunikasi ke bridge. Ketika menggunakan Protokol Spanning Treee, semua yang bukan root bridge harus terkoneksi dengan root bridge.

4.8.1.3 Opsi Umum

Pilihan hardware dan software pada wireless bridge umumnya mirip dengan access poit untuk tujuan tujuan sebagai berikut:

1. Fixed atau detachable antennas
2. Kemampuan filter handal
3. Removable(modular)radio card
4. Variable output power
5. Berbagai variasi jenis dari konektifitas non wireless

4.8.1.4 Fixed atau Detachable Antenna

Antenna Wireless bridge bisa hadir dalam bentuk yang tetap ataupun bisa dipisah-pisah dan juga bisa ada dengan atau tanpa keanekaragaman. Sering kali keaekaragaman tidak diperhatikan ketika mengkonfigurasi sebuah wireless bridge dikarenakan baik bridge(satu pada masing-masing akhir link)akan bersifat ststis, dan lingkungan di sekitar wirelsess bridge cenderung tidak berubah terlalu sering. Untuk alasan itulah multipath tidak mengkhususkan access point dan mobile users.

Detachable antenna adalah layanan tertentu pada wireless bridge yang menguntungkan karena detachable antenna memberikan kemampuan untuk memasanag bridge pada indoor ruangan dan menjalankan kabel outdoor untuk menghubungkan antenna. Pada sebagian besar kasus antenna semi-directioal dan detachable digunakan dengan wireless bridge. Jalan alternative untuk menghubungkan detachable antenna dengan wireless bridge dan pemasangan bridge inddor adalah dengan memasang wireless bridge outdor tepat di atas atap wireless bridge indoor.

Pada tahun 1926 the Electric Power Club dan The Associated Manufacturers of Electrical Supplies memerger pekerjaan mereka dan membentuk the National Electrical Manufacturers Associateions(NEMA). Walapun demikian kepemimpinan mereka kembali lagi lebih dari 75 tahun, dari dahuku hingga sekarang NEMA telah memfokuskan untuk memberlakukan standart terhadap peralatan listrik, pembelaan atas nama industri dan analisa ekonomi. Diantara hal-hal lan NEMA mengkhususkan pada standarisasi piranti yang digunakan di setiap industri untuk melindungi isinya dari efek negative dari pengaruh kondisi cuaca sekitar

4.8.1.5 Kemampuan Filter Yang Handal

Filter MAC ataupun filter protocol mungkin dibentuk dalam wireless bridge. Untuk system keamanan dasarnya administrator bisa mengkovigurasi sebuah wireless bridge untuk memperbolehkan atau tidak akses jaringan pada peralatan tertetu berdasarkan MAC address mereka.

Sebagian besar wireless bridge menawarkan layanan protocol filtering. Protokol filtering merupakan penggunaan di layer3-7 yang membolehkan transfer atau tidak paket tertentu atau datagrans berdasarkan layer 3 protokol, layer 4port atau bahkan layer 7applikasi. Protokol filter digunakan untuk membatsi penggunaan wireless LAN. Sebagai contoh seorang administrator bisa mencegah sekelompok user dari menggunakan aplikasi bandwith-intensive berdasarkan pada port atau protocol yang digunaakan untuk aolikasi itu sendiri.

4.8.1.6 Removable (modular) Radio Cards

Mempunyai kemampuan untuk membentuk wireless backbone menggunakan satau atau dua slot radio card yang didapat di beberapa bridge untuk mengurangi jumlah dari peralatan kita 4 menjadi 2 ketika ada konektifitas client dan fungsioality bridge. Fungsi ini akan membutuhkan access point dan bridge pada kedua ujung link. Beberapa wireless bridge menunjukkan fungsi yang sama menggunakan gelombag radio tunggal. Ketika masih menunjukkan pekerjaan yang sama, konfigurasi ini memberikan troughput yang lebih sedikitdaripada apabila memisahkan gelombang radio yang digunakan untuk access point dan fungs bridge.

4.8.1.7 Variabel Output Power

Layanan ini memungkinkan administrator untuk mengontrol output power(mw) yang seharusnya dimiliki oleh bridge untuk mengirimkankan RF sinyalnya. Fungsi ini sangat bermanfaat ketika harus melakukan survey ke luar kantor karena system ini memperbolehkan surveyor untuk mengontrol fleksibilitas dari mengontrol output power tanpa menambh\ah atau mengurangi amplifier,attenuator,dan panjang kabel dari rangkaian selama pemeriksaaan. Apabila digunaka secara bersamaan dengan amplifier, variable output dari bridge dapat berguna untuk jarak jauh dan mengurangi jumlah waktu yang dibutuhkan untuk mendapatkan frequesi yang benar. Sebagai contonya power

dari bridge cukup kuat untuk membuat link dan cukup lemah untuk tetap berkomunikasi dengan aturan tetap dari FCC.

4.8.1.8 Berbagai Macam Koneksi dengan Koneksi tanpa Wireless

Pilihan konketifitas dari wireless bridge bis termasuk dalam 10 baseeTX, 10/100baseTx, 100base Tx, atau 100 base FX. Selalu berusaha untuk mengeluarkan koneksi full-duplex ke segmet kabel dengan tujuan memperbesar output dar wireless btidge. Hal ini penting keteika menyiapkan pembelian wireless bridge untuk andil dalam permasalahan tertentu seperti jarak dari wiring closet terdekat dengan tujuan mengkhususkan konektifitas dari wireless bridge.

4.8.1.9 Konfigurasi dan Management

Wireless bridge memiliki banyak kesamaan konfigurasi dengan acess poin:konsol,telnet,HTTP,SNMP atau konfigurasi dan management umum. Banyak bridge yang support Power over Ethernet(PoE) sebagaimana dibahas pada bab5. ketika wireless bridge diimplementasikan, pengecekan troughput seharusnya dilakuka sesuai dengan pertauran untuk mengkonfirmsikan bahwa link tidak hilag karena ada bagian peralatan yang dipndah atau antenna yang diganti.

Wireless bridge biasanya ada dari pabrik dengan default IP address dan dapat diakses melalui metode yang disebutkan di atsa untuk konfigurasi awal. Umumnya selalu ada tombol reset di luar item untuk mereset unit dan mengeset kembali ke setingan awal dari pabrik.

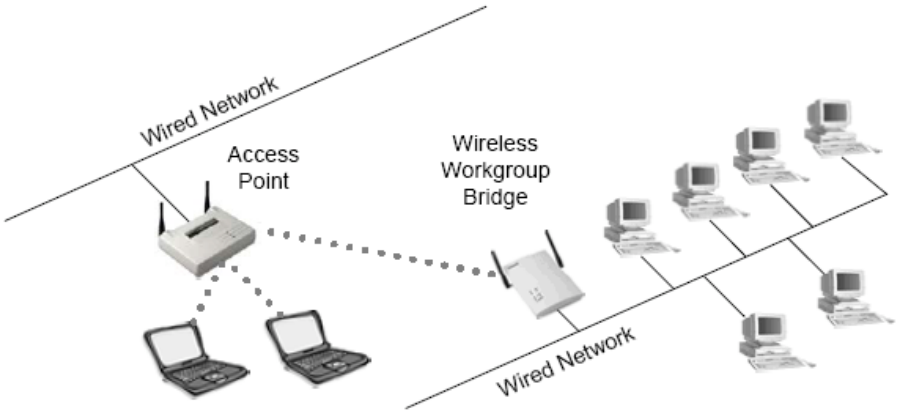
4.9 Wireless Group Bridges

Yang hamper sama dan emmbingungkan jika dibandingkan dengan wireless bridge adalah wireless workgroup bridge. Perbedaan yang paling besar diantara bridge dan workgroup bridge adalah bahwa workgroup bridge adalah piranti untuk client.

Wireless workgroup bisa untuk mengumpulkan banyak peralatan wired LAN client dalam satu gabungan client wireless LAN.

Pada table asosiasi access point, workgroup bridge akan tampak pada table sebagai peralatan single client. MAC address dari peralatan workgroup bridge tidak akan bisa dilihat di access point. Workgroup bridge umumnya berguna di linkungan dengan ruang kelas mobile, kantor mobile, atau bahkan bangunan kampus secara remote dimana sekelompok kecil dari user membutuhkan akses ke jaringan utama. Bridge dapat digunakan untuk jenis fungsi ini , tetapi apabila terdapat accesss point daripada bridge pada site pusat, maka dengan menggunakan workgroup bridge akan menghindarkan administrator untuk membeli bridge tambahan untuk site pusat. Gambar 4.8 menunjukkan contoh dari wireless workgroup bridge sementara Gambar 4.9 mengilustrasikan dimana penggunaannya dalam konteks wireless LAN.

Gambar 4.8. Wireless Workgroup Bridge



Gambar 4.9. Contoh Aplikasi Wireless Workgroup Bridge

Dalam suatu lingkup indoor dimana sekelompok user secara fisik dipisahkan dari main body pengguna jaringan, workgroup bridge dapat secara ideal menghubungkan

semua group kembali ke jaringan utama secara wireless. Sebagai tambahan workgroup bridge bisa mempunyai pemfilter protocol yang memperbolehkan administrator untuk mengontrol lalu lintas data melalui wireless link

4.9.1 Opsi Umum

Karena wireless workgroup bridge adalah jenis dari bridge maka banyak opsi yang bisa nada temukan dalam sebuah bridge--pemfilteran MAC dan protocol, antenna fix dan detacable, variable power output, dan berbagai jenis konektifitas tanpa wireless—juga ditemukan pada workgroup bridge. Ada batasan mengenai jumlah stasiun yang mungkin menggunakan workgroup bridge dari segment selain wireless. Jumlahnya berada pada range 8 sampai 128 tergatung pada pabrikan. Menggunakan lebih dari 30 client melalui segment wireless akan menyebabkan throughput drop sampai point dimana user merasa bahwa link wireless begitu lambat dan tdak cukup untuk menyelesaikan pekerjaan mereka.

4.9.2 Konfigurasi dan Management

Method yang digunakan untuk mengakses, mengkonfigurasi dan mengatur wireless workgroup bridge mirip dengan wireless bridge:console, telnet, HTTP,SNMP support atau software konfigurasi dan management umum. Workgroup bridge dikonfigurasi untuk alamat IP yang default dari pabrikan tetapi dapat dirubah dengan mengakses unit melalui port konsol, web browser, telnet atau aplikasi software umum lain. Administrator bisa mereset peralatan ke setingan default dari pabrik dengan menggunakan tombol reset pada hardware

4.10 Wireless LAN Client Devices

Peralatan client dalam tujuan diskusi ini akan mencakup beberapa peralatan wireless LAN dimana akses point (AP) dikenali sebagai client dalam suatu jaringan. Peralatan ini mencakup:

1. PCMCIA dan Compact Flash(CF)
2. Ethernet dan Serial Converter

3. USB Adapter
4. PCI dan ISA Adapter

Client dari wireless LAN adalah pengguna akhir dari system jaringan seperti desktop,laptop atau computer PDA yang membutuhkan konektifitas wireless dengan infrastruktur jaringan wireless. Peralatan client wireless LAN yang tertera diatas memberikan konektifitas untuk client wireless LAN. Hal ini penting untuk mengetahui bahwa pihak pabrikan hanya membuat radio card(card pemancar gelombang radio) dalam 2 format fisik yaitu PCMCIA dan Compact Flash(CF). Semua radio card diciptakan pihak pabrikan dalam format card ini dan kemudian dihubungkan ke adapter seperti PCI, ISA, USB dsb.

4.10.1 PCMCIA dan Compact Flash Cards

Sebagian besar komponen di beberapa jaringan wireless adalah PCMCIA card. Lebih lanjut PCMCIA card umumnya dikenal dengan "PC card", peralatan ini digunakan di notebook(laptop) dan PDA. PC card adalah komponen yang menyediakan koneksi antara peralatan client dan jaringan. PC card memberikan pelayanan sebagai modular radio di access point, bridge, workgroup bridge, USB adapter, PCI & ISA adapter, bahkan point server**.** Gambar 4.10 menunjukkan contoh dari PCMCIA card.

Gambar 4.10. Contoh PCMCIA Card

Antenna pada PC card berbeda-beda untuk masing-masing pabrikan. Kita harus memperhatikan bahwa beberapa pabrikan menggunakan antenna yang sama sementara pabrikan lain menggunakan model yang benar-benar berbeda. Beberapa diantaranya kecil dan pipih sementara bentuk lainnya dapat dipisahkan dan terhubung dengan PC card melalui kabel pendek. Beberapa PC Card dikemas

dengan banyak antenna dan bahkan aksesoris untuk memasang antenna detachable(dapat dipisahkan) pada laptop atau desktop dengan Velcro.

Ada 2 pabrikan utama dari chipset radio yang membuat "jantungnya" 802.11 b PC dan CF card yang terkenal:**Agere System** (awalnya Lucent Techologies) dan **intersil.** Atheros adalah chipset produk masal pertama untuk standar 802.11a yang menggunakan frekwensi bands 5 GHz UNII. Pabrikan ini menjual chipset mereka pada pabrikan PC card dan CF radio card (perusahaan pembuatan hardware wireless LAN) yang menggunakan gelombang radio pada produk mereka.

Compact Flash card yang lebih umum dikenal dengan "CF card" mempunyai fungsi yang sangat mirip dengan wireless PC Card tetapi CF card lebih kecil dan khusus digunakan pada PDA. Wireless PC Card membutuhkan power yang sangat kecil dan seukuran dengan ukuran matchbook.

4.10.2 Wireless Ethernet dan Serial Converter

Ethernet dan serial converter digunakan dengan berbagai peralatan yang menggunakan Ethernet dan 9 pin serial port dengan tujuan untuk mengkonversi koneksi jaringan menjadi koneksi wireless LAN. Ketika anda menggunakan converter wireless Ethernet maka anda akan menghubungkan gelombang radio wireless LAN dengan peralatan kable kategori 5 secara eksternal. Penggunaan yang paling umum dari converter wireless Ethernet adalah sebagai penghubung Ethernet based print server dengan jaringan wireless.

Peralatan serial dianggap sebagai peralatan warisan(peralatan kuno) dan sangat jarang digunakan pada personal computer. Serial converter khususnya digunakan pada perlatan lama yang menggunakan port serial untuk konektifitaas jaringan seperti terminal, peralatan telemetri dan serial printer. Sering kali pabrikan akan menjual perlatan client yang mencakup baik serial maupun Ethernet converter dalam satu paket yang sama.

Peralatan converter Ethernet dan serial ini pada umunya tidak ditemui pada PC card radio. Sebagai gantinya PC card yang harus dibeli secara terpisah dan diinstall pada slot PCMCIA di converter. Jenis converter Ethernet tertentu memperbolehkan administrator untuk mengkonversi sejumlah besar node-node yang terhubung dengan kael menjadi wireless dalam periode yang singkat.

Konfigurasi dari converter Ethernet dan serial ada berbagai macam. dalam sebagian besar kasus konsol akses tersedia melalui 9 pin serial port. Gambar 4.11 menunjukkan contoh dari converter Ethernet dan serial.

Gambar 4.11. Contoh Wireless Ethernet dan Serial Converter

4.10.3 USB Adapter

USB client menjadi begitu popular dikarenakan konektifitasnya yang sangat sederhana. USB client compatible dengan peralatan *plug n play,* dan tidak membutuhkan tambahan power lain selain USB port yang memang sudah ada pada computer. Beberapa USB client menggunakan mode modular yang merupakan piranti removable radio card sedangkan yang lainnya mempunyai internal card yang sudah fixed sehingga tidak bisa dipindah tanpa membuka casingnya. Ketika membeli peralatan USB client yakinlah bahwa anda mengetahui apakah USB adapater ada atau tidak pada PC Card Radio. Pada contoh kasus ketika USB adapter membutuhkan PC card, mode ini yang direkomendasikan walaupun tidak selalu membutuhkan PC card, anda seharusnya menggunakan perlatan dari vendor yang sama baik untuk adapter dan PC card**.** Gambar 4.12 menunjukkan contoh dari USB client.

Gambar 4.12. Contoh USB Client

4.10.4 PCI dan ISA Adapter

PCI dan ISA wireless diinstal di dalam desktop atau pada computer server. Peralatan PCI wireless compatible dengan piranti *plug n play* tetapi bisa juga hanya berupa PCI card yang "kosong" dan membutuhkan PC Card untuk dimasukkan pada slot PCMCIA bersamaan dengan PCI card yang diinstal pada computer. Wireless ISA card tampaknya tidak compatible dengan piranti *plug n play* dan akan membutuhkan konfigurasi manual baik melalui software maupun pada operating system. Karena operating system tidak bisa mengkonfigurasi piranti ISA yang tidak compatible dengan piranti *plug n play*, administrator harus memastikan bahwa settingan adapter dengan operating systemnya cocok. Pabrikan secara khusus mempunyai driver yang terpisah untuk adapter PCI atau ISA dan PC card akan dimasukkan pada masing-masing piranti tersebut. Sama halnya dengan USB adapter PCI direkomendasikan untuk menggunakan peralatan dari vendor yang sama untuk PCI/ISA adapter dan PC card. Gambar 4.13 menunjukkan contoh dari PCI adapter dengan PC card yang sudah dimasukkan.

Gambar 4.13. Contoh PCI Adapter

4.10.5 Konfigurasi dan Management

Ada 2 step untuk menginstall peralatan client wireless LAN.

1. install drivernya
2. install utilities pembuat wireless(manufacturer's wireless utilities)

4.10.6 Instalasi Driver

Drivernya termasuk untuk card diinstall dengan cara yang sama dengan penginstallan jenis PC hardware yang lain. Sebagian besar peralatannya(selain ISA adapter) compatible dengan peralatan *plug n play* yang berarti bahwa ketika peralatan client pertama kali diinstall , pengguna akan diminta untuk memasukkan CD atau disk yang berisi software driver ke dalam mesin. Langkah khusus untuk instalasi akan sangat beragam untuk pabrikan yang berbeda. Yakinlah untuk mengikuti instruksi manual merek khusus hardware anda.

Ketika membeli peralatan client, yakinlah bahwa drivernya termasuk dalam operating system yang akan kita install. Converter serial dan Ethernet tidak membutuhkan driver khusus untuk bekerja namun demikian wireless LAN client tetap bisa diinstall dan digunakan.

4.11 Manufacture Utilities

Beberapa pabrikan menawarkan fungsilitas yang penuh dan yang lainnya menyediakan sebagian besar fungsi dasar untuk koneksitisitas. Fungsionalitas yang lengkap meliputi hal-hal berikut:

1. Site Survey Tools
2. Spectrum analyzer
3. Peralatan monitoring power dan speed
4. Profile Configuration utilities
5. Link status monitor dengan link testing fungsionality

4.11.1 Site Survey Tools

Peralatan site survey bisa dikategorikan beberapa item yan berbeda yang memperbolehkan user untuk menemukan jaringan , mengidetifikasi MAC address dari akses point, menghitung kekuatan sinyal dan perbandingan sinyal dengan noise juga memonitor interfering semua akses point pada waktu yang sama selama site survey

4.11.2 Spectrum Analyzer

Software penganalisa spectrum mempunyai banyak kegunaan secara praktis termasuk menemukan sumber interferensi dan channel wireless LAN yang terjadi overlapping(tumpang tindih) dalam wilayah sekitar wireless LAN anda.

4.11.3 Power Output and Speed Configuration

Peralatan monitoring power dan speed berguna untuk mengetahui link wireless mana yang bisa berfungsi pada periode waktu tertentu. Sebagai contohnya, apabila seorang user berencana untuk menransfer data dalam jumlah yang besar dari server ke laptop, mereka tidak perlu memulai proses transfer sampai koneksi wireless ke jaringan sebesar 11 Mbps sebagai ganti dari 1 Mbps. Mengetahui lokasi dari point dimana troughtputnya naik/turun sangat berharga untuk meningkatkan produktifitas user.

4.11.4 Profile Configuration Utilities

Utility konfigurasi profile akan sangat mempermudah pekerjaan administrasi ketika berubah dari satu jaringan wireless ke jaringan wireless yang lain. Sebagai ganti dari penggantian secara manual konfigurasi dari semua settingan client wireless setiap kali kita berganti jaringan maka user bisa mengkonfigurasi profile untuk masing-masing jaringan wireless selama konfigurasi awal dari peralatan client sehingga lebih bisa menghemat waktu nantinya.

4.11.5 Link Status Monitor Utilities

Fungsi memonitor status link memudahkan user untuk melihat paket error/kesalahaan. Transmisi yang berhasil, kecepatan koneksi, kelangsungan link, dan parameter berharga lainnya. Biasanya ada suatu fungsi untuk melakukan pengetesan konektifitas real-time link untuk demikian sebagai contohnya seorang administrator akan bisa melihat bagaimana kestabilan wireless link selama keberadaan dari interferensi yang hebat dari RF(Radio Frequency) atau blockade sinyal.

Kemampuan umum

Parameter dari kegunaan yang ditawarkan oleh pabrikan tercantum dalam parameter berikut yang masing-masingnya dijelaskan secara detail di buku ini.

1. Infrastruktur mode/Ad Hoc mode
2. SSID (a.k.a nama jaringan)
3. Channel (jika dalam mode ad hoc)
4. WEP Keys
5. Tipe authentication (Open System, Shared Key)

4.12 Wireless Residental Gateways

Wireless residental gateways adalah peralatan yang didesain untuk menghubungkan sejumlah kecil titik wireless ke satu peralatan untuk Layer 2 (wireless dan non wireless) dan konektifitas layer 3 ke internet atau ke jaringan lain. Pihak pabrikan telah memulai untuk mengkombinasikan peran access point dan gateways ke dalam satu peralatan. Wireless residential gateways biasanya termasuk dalam hub atau switch built in sebagaimana konfigursi penuh,Wi-Fi memenuhi access point. Port WAN pada suatu wireless residential gateways adalah Internet yang dihadapkan dengan port Ethernet yang dihubungkan dengan Internet melalui salah satu dari yang berikut ini:

1. Cable modem
2. xDSL modem
3. Analog modem
4. Satellite modem

4.12.1 Opsi Umum

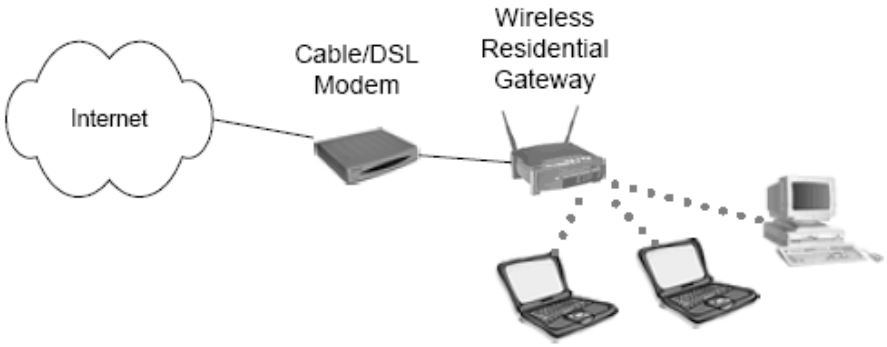
Karena wireless residential gateways menjadi popular di telecommuters dan di bisnis keci, pabrikan telah memulai untuk menambahkan feature yang lebih banyak pada peralatan ini untuk membantu produktifitas dan keamanannya. Opsi umum dimana wireless residential gateways termasuk didalamnya adalah sebagai berikut:

1. Point to Point Protokol over Ethernet(PPPoE)

2. Network Address Translation(NAT)
3. Port Address Transalation(PAT)
4. Ethernet switching
5. Virtual Server
6. Print Serving
7. Fail-over routing
8. Virtual Private Networks(VPNs)
9. Dynamics Host Configuration Protocol(DHCP) Server dan Client
10. Configuration Firewall

Perbedaan kemampuan array membuat rumah dan kantor kecil menjadikannya dalam peralatan single secara utuh yang mudah dikonfiguarasi dan mengatasi sebagian besar kebutuhan bisnis. Residential gateways menjadi popular untuk beberapa waktu tertentu, tetapi sekarang ini dengan kepopuleran ekstrim dari peralatan wireless 802.11b, wireless akan ditambahkan sebagai tamabahan feature. Wireless residential gateways mempunyai semua yang diinginkan dalam seleksi konfiguarasi akses point dari SOHO klas seperti halnya WEP, MAC Filter, seleksi channel, dan SSID.

Gambar 4.14. Contoh Wireless Residential Gateway



Gambar 4.15. Contoh Wireless Residential Gateway

4.12.2 Konfigurasi dan Manajemen

Mengkonfigurasi dan menginstall wireless residential gateways umumnya meliputi browing ke built-in HTTP server lewat salah satu built in port Ethernet dan merubah settingan konfigurasi user untuk memenuhi kebutuhan tertentu anda. Konfigurasi ini meliputi perubahan ISP.LAN atau settingan VPN. Konfigurasi dan monitoring umumnya sama caranya yaitu dengan melibatkan interface browser. Beberapa unit wireless residential gateways mendukung console, telnet, dan konektifitas USB untuk manajement dan konfigurasi. Menu berdasarkan teks khususnya disediakan oleh port console dan telnet session kurang mudah digunakan dibandingkan dengan interface browser tetapi cukup untuk melakukan konfigurasi. Fungsi statistics yang memungkinkan untuk dipantau adalah up-time, dynamics IP address, konektifitas VPN dan asosiasi client. Settingan ini biasanya ditandai dengan baik atau dijelaskan untuk pengguna non teknikal dan perkantoran

Ketika anda memutuskan untuk menginstall wireless residential gateways di rumah atau untuk kepentingan bisnis, waspadalah bahwa ISP anda tidak akan memberikan technical support untuk mendapatkan piranti anda terhubung dengan internet keculai mereka secara khusus meyebutkan bahwa ISP anda bisa memberikannya. ISP biasanya hanya support pada hardware yang anda beli atau yang telah diinstal. Kekurangan service ini dapat secara khusus meresahkan user non teknis yang harus mengkonfigurasi IP address yang benar dan menyeting gateway yang benar pula sehingga bisa mengakses internet. Usaha yang bisa anda lakukan dalam menginstall peraltan ini adalah dengan membaca manual yang ada pada peralatan tersebut atau pada seseorang yang baru saja sukses menginstal unit

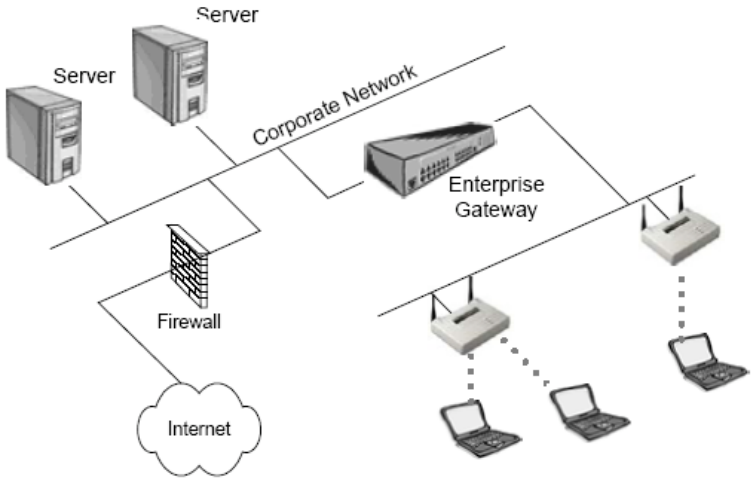
yang sama dan bisa memberi petunjuk yang benar.wireless residential gateways saat ini begitu umum dimana masing-masing individu yang menganggap diri mereka sendiri user nonteknis telah mendapatkan pengalaman yang significant untuk menginstall dan mengkonfigurasinya.

4.13 Enterprise Wireless Gateways

Enterprise Wireless Gateways adalah piranti yang memberikan autensifikasi khusus dan konektifitas untuk wireless client. Enterprise Wireless Gateways cocok untuk lingkungan skala besar wireless LAN dimana memberikan banyak servise wireless LAN yang bisa di atur seperti rate limiting, Quality of Service(QoS), dan profile management.

Hal ini penting bahwasanya piranti enterprise wireless gateway membutuhkan CPU yang kuat dan interface fast Ethernet karena mungkin akan support banyak access point, yang semuanya akan mengirim lalu lintas data ke dan melalui enterprise wireless gateway. Unit enterprise wireless gateway biasanya support berbagai varietas dari teknologi WLAN dan WPAN seperti standar peralatan 802.11,Bluetooth,HomeRF,dan masih banyak lagi. Enterprise Wireless Gateway support SNMP dan mengijinkan pelebaran atau upgrade profile user enterprise secara simulatan. Peralatan ini dapat dikonfigurasi untuk hot fail-over(ketika diinstall sepaket), support RADIUS, LDAP, autentikasi database Windows NT, dan enkripsi data menggunakan tipe jaringan VPN standart industri. Gambar 4.16 menunjukkan contoh dari enterprise wireless gateway sementara Gambar 4.17 menunjukkan ketika enterprise wireless gateway diinstal pada suatu jaringan.

Gambar 4.16. Contoh Enterprise Wireless Gateway



Gambar 4.17. Contoh Aplikasi Enterprise Wireless Gateway

Teknologi autentifikasi yang disatukan dalam enterprise wireless gateway seringkali dibangun pada access point dengan level yang lebih canggih. Sebagai contohnya , konektifitas VPN dan 802.1x/EAP yang didukung pada banyak merk dari enterprise level access point.

Enterprise wireless gateways mempunyai banyak fasilitas seperti Role-Based Access Control(RBAC) yang tidak ditemukan di beberapa access point. RBAC memperbolehkan administrator untuk menempatkan akses wireless pada level tertentu pada posisi job yang tertentu pula pada sebuah perusahaan. Apabila orang yang melakukan pekerjaan tersebut diganti, maka orang yang baru secara otomatis mendapatkan hak atas system jaringan yang sama sebagai orang pengganti. Mempunyai kemampuan untuk membatasi akses wireless user untuk bekerja sama memanfaatkan sumber daya sebagai bagian dari "peran" bisa merupakan layanan keamanan yang berguna.

Kelas pelayanan didukung secara khusus, dan seorang administrator dapat menempatkan level pelayanan pada user atau peran tertentu. Sebagai contohnya account guest mungkin bisa menggunakan jaringan wireless sekitar 500 kbps sementara administrator bisa mencapai 2 Mbps.

Pada beberapa kasus Mobile IP didukung oleh enterprise wireless gateway, memperbolehkan user untuk menjelajahi sampai batas layer 3. Penjelajahan user bahkan bisa didefinisikan sebagai bagian dari kebijakan enterprise wireless gateway, memperolehkan user untuk menjelajah pada temapt-tempat yang hanya diperbolehkan oleh administrator. Beberapa enterprise wireless gateway mendukung pengantrian paket

dan prioritasi, user tracking, dan bahkan pengontrolan tanggal/waktu untuk menentukan kapan user bisa mengakses jaringan wireless.

Pencegahan MAC Spoofing dan pembukuan sessi yang lengkap juga termasuk feature yang ditawarkan dan bertujuan untuk mengamankan wireless LAN. Ada banyak feature yang sangat beragam dan berbeda significant diantara pabrikan. Enterprise wireless gateways secara menyeluruh kami rekomendasikan bahwa administrator aka mengambil kelas training manufacturer sebelum membuat pembelian sehingga dengan demikian penyebaran dari enterprise wireless gateway akan maju sedikit demi sedikit.

Seorang konsultan menempatkan diri mereka sendiri pada suatu situasi yang harus memberikan solusi keamanan untuk penyebaran wireless LAN dengan banyak access point yang tidak mendukung feature keamanan. akan mengert bahwa enterprise wireless gateway adalah solusi yang bagus untuk masalah mereka . Enterprise wireless gateway sangat mahal, tetapi mempunyai sejumlah solusi management dan keamanan sehingga harga bukan masalah utamanya.

4.13.1 Konfigurasi dan management

Enterprise wireless gateway dipasang pada path data utama di segment yang hanya melewatkan akses point seperti pada gambar yang terlihat di 4.19. enterprise wireless gateway dikonfiguarsi melalui port console (menggunakan CLI) ,telnet, internal HTTP atau server HTTPS dsb, Management secara tersentrall pada peralatan kita adalah salah satu keuntungan besar penggunaan enterprise wireless gateway. Seorang administrator dari single console dapat secara mudah mengatur penyebaran jaringan wireless menggunakan hanya sedikit peralatan central sebgai ganti dari akses point yang sangat banyak.

Enterprise wireless gateway umumnya diupgrade dengan penggunaan TFTP dengan cara yang sama pada banyak switch dan router yang ada di pasaran dewasa ini. Konfigurasi backup dapat secara sering diotomasi sehingga demikian seorang administrator tidak akan menghabiskan waktu management tambahan untuk mebackup atau proses recover dari file konfigurasi yang hilang. Enterprise wireless gateways sebagian besar dibuat dengan tanda 1U atau 2 U yang bisa dipaskan dengan data saat ini pada design utama kita.

4.14 Kesimpulan

Pada umumnya yang perlu diperhatikan dalam penggunaan perangkat komunikasi Wireless meliputi pendefinisan dan peranan hardware pada jaringan, memilih hardware dan pemasangan dan pengkonfigurasian hardware. Perangkat yang paling umu dalam komunikasi Wireless adala Access Point. Sebuah accesss point adalah sebuah peralatan *half duplex* dengan kecerdasan yang sesuai untuk kecanggihan switch Ethernet. Yang mode nya terdiri atas Root Mode, Repeater Mode dan Bridge Mode. Pemasangan dari perangkat Access Point bergantung pada kebutuhan jaringan. Termasuk juga pemasangan Antenna pada Access Point. Untuk mengkomunikasikan client dengan jaringan kabel backbone, harus mengerti bagaimana untuk sepantasnya mengkoneksikan akses point ke dalam jaringan kabel.

4.15 SOAL

1. Sebutkan dan jelaskan beberapa mode dari Access Point ?
2. Sebutkan beberapa tahapan yang perlu diperhatikan dalam proses pemasangan perangkat Wireless (Access Point) ?
3. Sebutkan beberapa macam dari Wireless Client Device ?
4. Jelaskan mengenai perangkat Wireless Residential Gateways, berikut dengan gambar ?
5. Jelaskan mengenai perangkat Enterprise Wireless Gateways, berikut dengan gambar ?

Bab 5. Antenna dan Aksesoris

Pada bab sebelumnya, kita membahas bagian-bagian dari peralatan wireless LAN yang sangat banyak yang ada di pasaran saat ini untuk membuat wireless LAN sederhana dan rumit. Pada bab ini, kita akan membahas element dasar dari peralatan yang akan membuat access point, bridge, kartu pc dan peralatan komunikasi wireless lainnya : antennas.

Antenna adalah yang sering digunakan untuk meningkatkan jangkauan dari system wireless LAN, namun pilihan antenna yang sesuai juga dapat menambah keamanan dari wireless LAN anda. Pilihan antenna yang tepat dan posisi antenna dapat mengurangi kebocoran sinyal dari batasan anda, dan membuat pemotongan sinyal amat sulit. Pada bab ini, kami akan menjelaskan pola pemancaran sinar dari design antenna yang berbeda, dan bagaimana posisi antenna user membuat penerimaan sinyal yang berbeda.

Ada 3 kategori umum yang membagi antenna wireless LAN : omni directional, semi-directional, dan highly-directional. Kami akan membahas attribute dari tiap kedalaman group ini, sebagaimana metode yang tepat untuk meng-install tiap jenis antenna. Kami juga akan menjelaskan polarisasi, pengumpulan pola, penggunaan yang tepat, dan mengalamatkan item yang begitu banyak berbeda yang digunakan untuk mengkoneksikan antenna ke hardware wireless LAN lain.

Mulai dari sekarang, kami akan membahas teori RF dan beberapa kategori umum dari peralatan wireless LAN yang akan digunakan administrator pada dasar harian. Pengetahuan ini merupakan dasar yang bagus, namun ini hanyalah bernilai kecil tanpa pengetahuan pekerjaan yang padat tentang antenna, yang mana adalah alat yang sebenarnya mengirim dan menerima sinyal RF.

Bab ini akan meliputi aksesori LAN seperti :

- ❒ Amplifiers RF
- ❒ RF attenuators
- ❒ Lightning arretors
- ❒ Konektor RF
- ❒ Kabel RF
- ❒ Pemisah Rf
- ❒ Pigtails

Pengetahuan tentang penggunaan alat, spesifikasi, dan efek pada penguat sinyal RF adalah penting untuk bisa membangun wireless LAN yang berfungsi.

Power of Ethernet (PoE) telah menjadi factor penting pada jaringan wireless saat ini mengembangkan produk baru dan standar baru. Teknologi PoE akan dibahas bersama dengan peralatan PoW yang berbeda tipe yang bisa digunakan untuk mengirim power pada alat PoE yang enabled.

5.1 Antenna RF

Antenna RF adalah peralatan yang digunakan untuk menkonversikan sinyal frekuensi tinggi(RF) pada garis transmisi (kabel atau waveguide) ke gelombang siaran di udara. Medan elektrik dipancarkan dari antenna yang disebut beams atau lobes. Dibawah ini adalah 3 kategori umum dari antenna RF, yaitu :

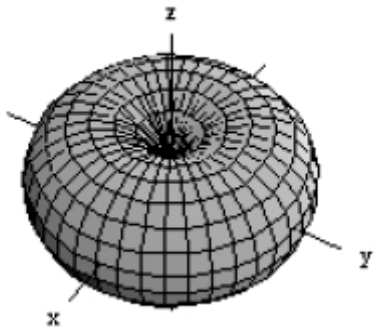
- ❒ Omni – directional
- ❒ Semi – directional
- ❒ Highly – directional

Tiap kategori mempunyai bermacam-macam tipe antenna, masing-masing mempunyai karakteristik RF yang berbeda dan penggunaan yang tepat. Ketika penambahan antenna meningkat, lingkup area menyempit sehingga antenna high-gain menawarkan lingkup area lebih luas daripada antenna low-gain pada level masukan (input) yang sama. Setelah mempelajari bagian ini, Anda akan mengerti antenna mana dan berapa jumlah yang terbaik sesuai kebutuhan anda dan kenapa.

5.1.1 Antenna Omni – directional (Dipole)

Antenna wireless LNn yang paling umum adalah antenna dipole. Sederhana dalam design, antenna dipole merupakan peralatan standar pada kebanyakan access point. Dipole adalah antenna omni-directional, karena ia memancarkan energinya secara bersamaan pada semua arah sekitar porosnya. Antenna directional memusatkan energinya dalam bentuk kerucut, dikenal dengan “beam”. Dipole mempunyai element pemancaran hanya 1 inchi panjangnya yang melakukan fungsi yang sama dengan antenna “rabbit ears” pada seperangkat televise. Antenna dipole yang digunakan dengan wireless LAN lebih kecil karena

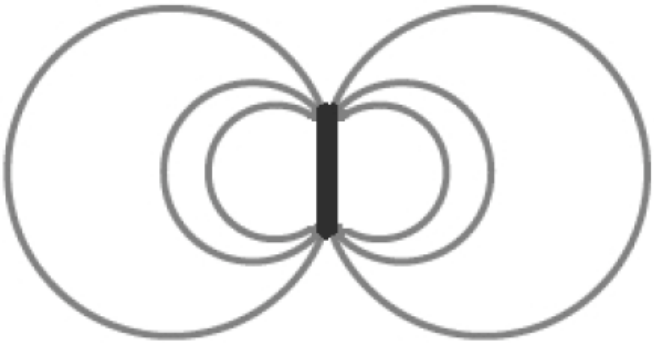
frekuensi wireless LAN dalam 2,4 GHz spectrum microwave sebagai ganti dari 100 Mhz spectrum TV. Bila frekuensinya meninggi, wavelength dan antennanya menjadi kecil.



Gambar 5.1 Energi Radiasi Dipole

Gambar 5.1 menunjukkan bahwa energi radiasi dipole di pusatkan pada daerah yang tampak seperti sebuah donat, dengan dipole secara vertical melalui "lubang" dari "donat". Sinyal dari antenna omni-directional memancar dalam 360 derajat horizontal beam. Bila antenna memancar pada semua arah secara bersamaan (membentuk sebuah bulatan), ini disebut radiator isotropic. Matahari adalah contoh yang bagus dari radiator isotropic. Kita tidak bisa membuat isotropic radiator, yang mana secara teori merujuk pada antenna, meski demikian, prakteknya antenna semua mempunyai beberapa tipe gain over dari isotropic radiator. Semakin tinggi nilai gain-nya (penambahan), semakin keras kita menekan donat menjadi datar hingga ia mulai kelihatan seperti pancake, yang pada kasus dengan antenna yang mempunyai nilai gain sangat tinggi.

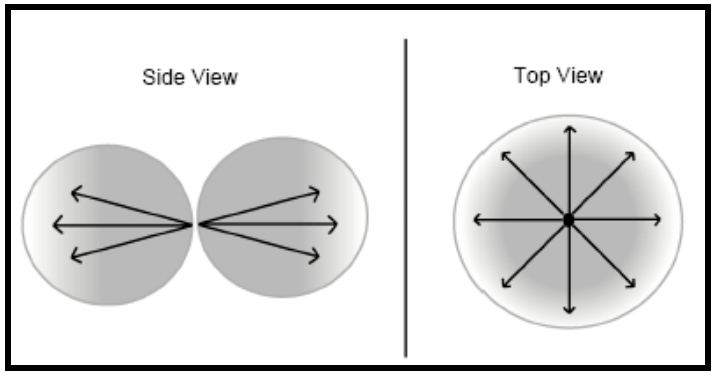
Pancaran dipole secara bersamaan pada semua arah mengelilingi porosnya, tapi tidak memancar bersama dengan panjang kabelnya, layaknya pola donat. Perhatikan tampak samping dari pancaran dipole ketika ia memancarkan gelombang pada **gambar. 5.2**. gambar ini juga mengilustrasikan bahwa antenna dipole membentuk pola pancaran bila dilihat dari atas disamping antenna vertical.



Gambar. 5.2. Pola pancaran dari Antenna Vertikal

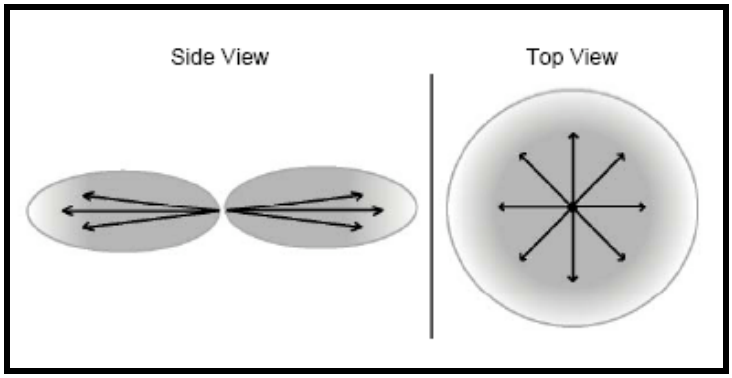
Bila antenna dipole ditempatkan di tengah-tengah satu lantai dari banyak bangunan, kebanyakan energinya akan di pancarkan terus pada lantai tersebut, dengan beberapa bagian penting kecil yang dikirim ke lantai atas dan bawah access point. **Gambar 5. 3** menunjukkan contoh dari beberapa tipe yang berbeda dari antenna omni-directional. **Gambar 5.4** menunjukkan contoh dua-dimensi dari tampak atas dan tampak samping antenna dipole

Gambar 5. 3 Tipe dari Antenna Omni-Directional



Gambar 5.4. Lingkup Area Antenna Omni-Directional

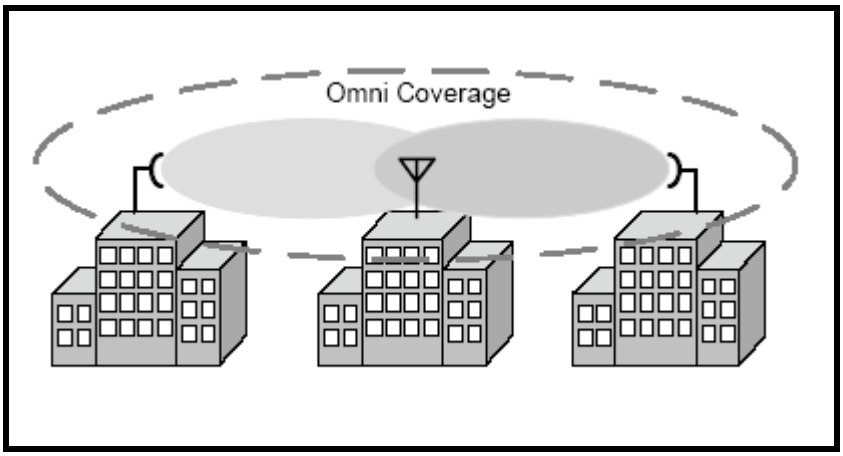
Antenna high-gain omni-directional menawarkan jangkauan yang lebih horizontal, namun jangkauan yang vertical dikurangi, seperti tampak **pada gambar 5.5.** karakteristik ini bisa menjadi pertimbangan penting ketika memasang antenna omni high-gain dalam ruangan pada langit-langit. Bila langit-langitnya terlalu tinggi, jangkauannya bisa tidak mencapai lantai, dimana user berada.



Gambar 5.5 Lingkup Area Antenna high-gain omni-directional

Kegunaan

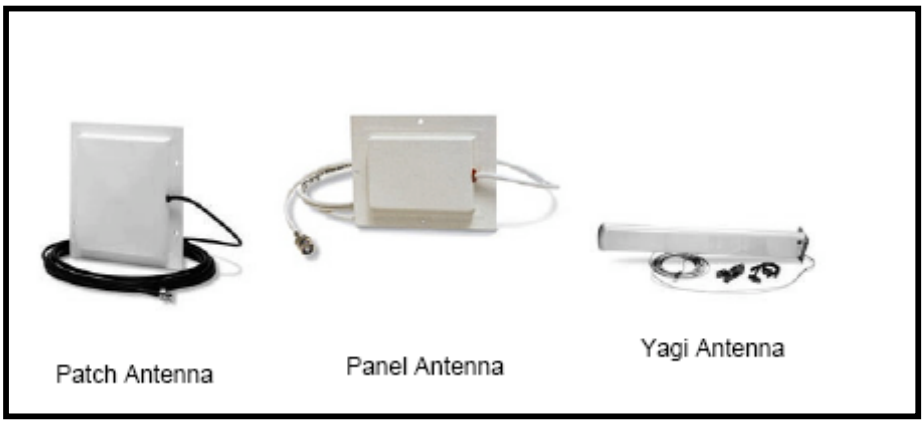
Antenna omni-directional digunkan ketika melingkupi semua arah sekitar poros horizontal dari antenna dibutuhkan. Antenna omni-directional sangat efektif dimana jangkauan besar dibutuhkan disekitar titik pusat. Sebagai contohnya, menempatkan antenna omni-directional di tengan-tengah sebuah ruangan terbuka dan besar akan melengkapi lingkupan yang bagus. Antenna omni-directional umumnya digunakan untuk design point-to-multipoint dengan bentuk bintang (Lihat **gambar 5. 6).** Penggunaan di luar ruangan, antenna omni-directional harus diletakkan di atas dari struktur (misalnya bangunan) pada pertengahan lingkup area. Contohnya, pada sebuah kampus, antenna bisa saja ditempatkan di pusat kampus untuk lingkup area yang terbesar. Ketika digunakan di dalam ruangan, antenna harus ditempatkan di tengah bangunan atau lingkup area yang diinginkan, dekat dengan langit-langit, untuk jangkauan yang optimum. Antenna omni-directional memancarkan jangkauan area yang besar pada pola lingkaran dan cocok untuk warehouse atau tradeshows dimana lingkupnya biasanya dari satu sudut bangunan ke sudut bangunan lain.



Gambar 5.6 Sambungan point-to-multipoint

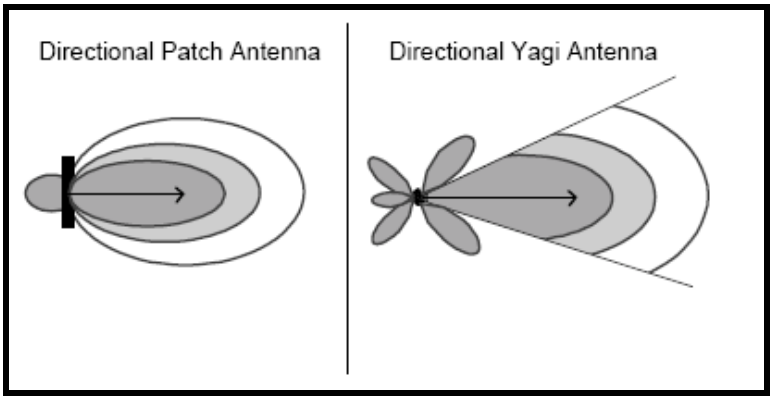
5.1.2 Antenna semi-directional

Antenna semi-directional terdiri dari bermacam-macam bentuk dan jenis. Beberapa tipe antenna semi-directional yang sering digunakan bersama wireless LAN adalah antenna Patch, Panel dan Yagi (dibaca "YAH-gee"). Semua antenna tersebut umumnya berbentuk datar dan dirancang untuk dinding gunung. Tiap tipe mempunyai karekteristik jangkauan yang berbeda. **Gambar 5.7** menunjukkan beberapa contoh dari antenna semi-directional.



Gambar 5.7 Contoh antenna semi-directional

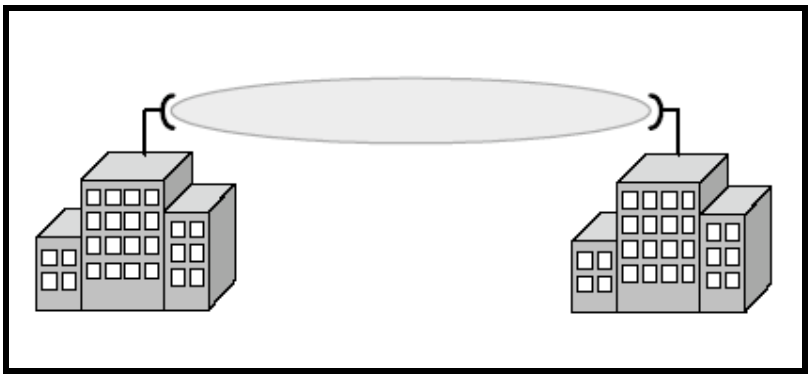
Antenna tersebut merubah energi dari pemancar lebih ke satu arah khusus daripada kearah yang sama., pola lingkaran yang umum dengan antenna omni-directional. Antenna semi-directional sering memancarkan pada bentuk hemispherical atau pola lingkup silinder seperti bisa dilihat pada **gambar 5.8.**



Gambar 5.8 Jangkauan Antenna Semi-Directional

Kegunaan

Antenna semi-directional idealnya cocok untuk jembatan dengan jarak pendek atau rata-rata. Sebagai contoh, dua bangunan kantor yang bersebrangan jalan satu sama lain dan perlu membagi koneksi jaringan akan menjadi scenario yang bagus untuk mengimplementasikan antenna semi-directional. Pada ruang tertutup yang luas, bila pemancar harus diletakkan di sudut atau pada bagian belakang bangunan, koridor, atau ruangan besar, antenna semi-directional akan menjadi pilihan yang baik untuk menyediakan jangkauan yang tepat. **Gambar 5.9** menggambarkan hubungan antara dua bangunan yang menggunakan antenna semi-directional.



Gambar 5.9. Hubungan Point-to-Point Menggunakan Antenna Semi-Directional

Seringkali, sebelum penelitian di tempat tertutup, para insinyur akan secara terus-menerus berpikir pada bagaimana cara terbaik untuk meletakkan antenna omni-directional. Pada beberapa kasus, antenna semi-directional menyediakan

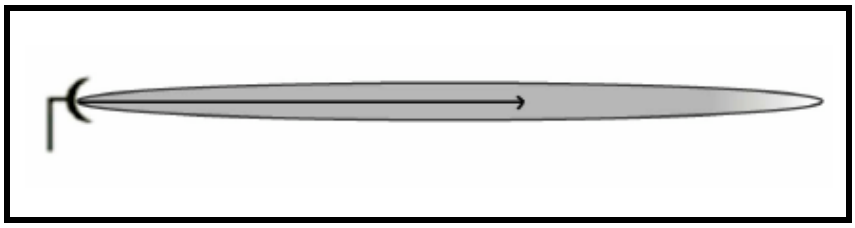
jangkauan yang amat sangat luas sehingga mereka bisa menyingkirkan kebutuhan pada multiple access point dalam bangunan. Sebagai contoh, pada gang yang panjang, beberapa access point dengan antenna omni-directional mungkin digunakan atau mungkin hanya satu atau dua accecc point dengan penempatan antenna semi-directional yang sepantasnya – menghemat sejumlah uang pelanggan secara signifikan. Pada beberapa kasus, antenna semi-directional mempunyai bagian belakang dan samping yang berbentuk bola yang, bila digunakan secara efektif, akan mengurangi kebutuhan akan penambahan access point lebih jauh. Secara spesifik, antenna Yagi sangat cocok untuk sinyal yang menjangkaun jalan kecil atau jalur di tempat duduk pada warehouse, palang jalan, toko retail atau fasilitas manufaktur.

5.1.3 Antenna highly-directional

Dari namanya sudah bisa ditebak, antenna highly-directional memancarkan sinyal sinyal terbatas dari tipe antenna apapun dan mempunyai gain terbesar dari ketiga group antenna. Antenna highly-directional secara khusus berbentuk cekung, peralatan berbentuk piringan, seperti bisa dilihat pada **gambar 5.10** dan **5.11**. antenna ini cocok untuk jarak jauh, hubungan wireless poin-to-point. Beberapa model ditujukan pada parabolic dishes karena mereka menyerupai piringan satelit kecil. Yang lainnya disebut antenna grid karena design mereka yang bolong untuk pengisian angin.

Gambar 5.10 Contoh Antenna Highly-Directional Berbentuk Parabola

Gambar 5.11 Contoh Antenna Highly-Directional Berbentuk Grid



Gambar 5.12 Pola Radiasi Antenna Highly-Directional

Kegunaan

Antenna high-gain tidak mempunyai jangkauan area yang peralatan klien bisa digunakan. Antenna ini digunakan untuk hubungan komunikasi point-to-point dan bisa memancarkan pada jarak hingga 25mil (42km). Kemampuan antenna highly-directional adalah bisa menghubungkan dua bangunana yang tepisah beberapa mil satu sama lain dan tidak punya hambatan jarak penglihatan diantara mereka. Ditambah pula, antenna ini bisa ditujukan secara langsung satu sama lain melalui bangunan dengan tujuan untuk "meledak" melalui sebuah hambatan. Susunan ini bisa digunakan dengan tujuan untuk mendapatkan sambungan jaringan ke tempat yang tdak bisa dilewati kabel dan dimana jaringan wireless normal tidak bisa bekerja.

Note : antenna higly-directional mempunyai beamwidth yang sangat terbatas dan harus ditujukan secara akurat satu sama lain.

5.1.4 Konsep antenna RF

Ada beberapa konsep yang merupakan pengetahuan penting ketika mengimplementasikan solusi yang membutuhkan antenna RF. Diantaranya yang akan dibahas adalah:

- Peng-kutuban (Polarization)

- Gain
- Beamwidth
- Free space path loss

Daftar diatas tidak didasari sebuah daftar yang luas dari semua konsep antenna RF, tapi lebih pada seperangkat kebutuhan fundamental yang membolehkan administrator untuk mengerti bagaimana fungsi peralatan wireless LAN disekeliling perantara wireless. Pengertian utuh dari dasar antenna secara kegunaan adalah kunci untuk memindahkan kedepan dalam mempelajari konsep RF lebih lanjut.

Mengetahui dimana antenna ditempatkan , bagaimana posisi mereka, seberapa jauh kekuatan mereka memancar, jarak kekuatan pancaran, dan seberapa banyak kekuatan tersebut dapat diterima oleh receiver, seringkali, merupakan bagian pekerjaan administrator yang paling rumit.

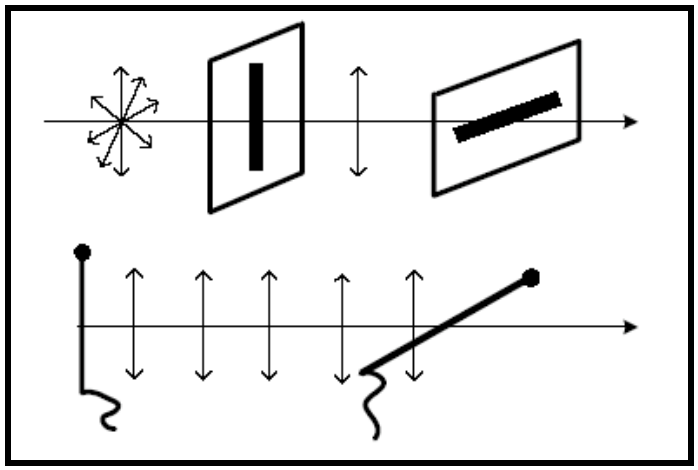
5.2 Polarization

Gelombang radion sebenarnya terdiri dari dua bagian, satu electric dan satunya lagi magnetic. Dua bagian ini tersusun secara vertical satu sama lain.Gabungan dari dua bagian ini disebut dengan bagian electro-magnetic. Energi ditransfer dari dan ke bagian lain satu sama lain, pada prosesnya dikenal sebagai “oscillation”. dataran yang parallel dengan elemen antenna merupakan “dataran-E” sementara dataran yang secara vertical dengan elemen antenna adalah “dataran-H”. Mula-mula kami tertarik dengan bidang electric sejak posisi dan arahnya yang menunjuk pada permukaan bumi (tanah) menentukan gelombang kutub

Peng-kutuban adalah orientasi fisik dari antenna pada posisi horizontal dan vertical. Bagian electric paralle dengan element pancaran (elemen antenna merupakan bagian logam dari antenna yang melakukan pekerjaan memancar) jadi, bila antennanya vertical, maka kutubnya vertical

- Kutub horizontal – bagian electric parallel dengan tanah
- Kutub vertical – bagian electric vertical dengan tanah.

Kutub vertical , yang biasanya digunakan pada wireless LAN, adalah vertical dengan dataran bumi. Perhatikan antenna rangkap menacap secara vertical dari banyak access point – antenna tersebut secara vertical mengkutub pada posisi ini – kutub horizontal parallel dengan bumi. **Gambar 5.13** mengilustrasikan efek pengkutuban dapat terjadi ketika antenna tidak lurus secara benar. Antenna yang tidak ter-kutub-kan pada cara yang sama tidak akan bisa berkomunikasi satu sama lain secara efektif.



Gambar 5.13 Peng-kutub-an (Polarization)

Cara penggunaan :

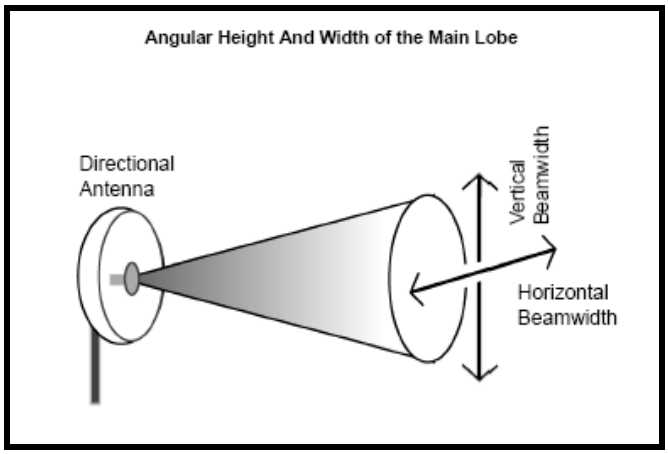
Pembuat antenna untuk kartu PCMCIA menghadapi masalah serius. Tidak mudah untuk membentuk antenna menjadi papan sirkuit kecil didalam sampul plastic yang menancap pada kartu PCMCIA. Jarang dilakukan membangun antenna dalam kartu PCMCIA yang menyediakan jangkauna memuaskan, terutama ketika client sedang bepergian. Pengkutuban kartu PCMCIA dan bahwa access point seringkali tidak sama, yang karenanya merubah laptop pada posisi berbeda hanya untuk meningkatkan penerimaan. PDA, yang biasanya menyesuaikan secara vertical dengan kartu PCMCIA, secara normal mempertunjukkan penerimaan yang baik. Luar, antenna paten yang dibingkai dengan Velcro pada computer laptop secara vertical hampir selalu menunjukkan peningkatan yang bagus melalui gigitan-antenna termasuk dengan hampir kebanyakan kartu PCMCIA. Pada area dimana terdapat sejumlah besar pengguna kartu PCMCIA, sering disarankan untuk menyesuaiakn antenna access point secara horizontal untuk penerimaan yang lebih baik.

5.3 Gain

Antenna gain dispesifikasikan pada dBi, maksudnya decibel ditujukan pada radiator isotropic. Radiator isotropic adalah bulatan yang memancarkan kekuatan secara sama pada semua arah secara simulatan. Kami tidak mempunyai kemampuan untuk membuat radiator isotropic, tapi sebagai gantinya kami dapat membuat antenna omni-directional seperti dipole yang memancarkan kekuatan 360 derajat secara horizontal, tapi bukan 360 derajat secara vertical. Pemancaran sinar sinyal RF pada cara ini memberi kita pola lingkaran. Semakin kita meng-horizontal-kan secara paksa donut ini, semakin menyenangkan jadinya, lebih membentuk sebuah bentuk pancake ketika gain-nya sangat tinggi. Antenna mempunyai gain pasif, yang artinya mereka tidak menaikkan kekuatan yang menjadi masukannya, tapi agak berbentuk bidang pancaran untuk memperpanjang atau memperpendek jarak gelombang akan menyebarluas. Semakin tinggi gain antenna-nya, semakin jauh gelombangnya akan berjalan, pusatkan gelombang keluarannya secara ketat sehingga akan lebih banyak kekuatan yang dikirim ke tujuan (antenna penerima) pada jarak jauh.

5.4 Beamwidth

Seperti telah dijelaskan sebelumnya, terbatas, atau memfokuskan sinar antenna meningkatkan gain antenna (ukuran dalam dBi). Beamwidth (pelebaran sinar) antenna artinya seperti kedengarannya : “width = lebar” dari sinar sinyal RF yang dipancarkan antenna**. Gambar 5.14** mengilustrasikan jangka waktu beamwidth .



Gambar 5.14 Beamwidth Antenna

Terdapat dua vector untuk dipertimbangkan ketika membahas beamwidth antenna secara vertical dan horizontal. Beamwidth vertical ditentukan pada derajat dan terletak secara vertical pada permukaan bumi. Beamwidth horizontal ditentukan pada derajat dan terletak secara parallel pada permukaan bumi. Beamwidth sangat penting untuk anda ketahui karena tiap tipe antenna mempunyai spesifikasi beamwidth yang berbeda. Table dibawah dapat digunakan sebagai paduan referensi cepat untuk beamwidth.

Tabel 5.1 Antenna Bandwith

Tipe antenna	**Beamwidth horizontal (dalam derajat)**	**Beamwidth vertical (dalam derajat)**
Omni-directional	360	Jarak antara 7-80
Patch / panel	Jarak antara 30-180	Jarak antara 6-90
Yagi	Jarak antara 30-78	Jarak antara 14-64
Tatanan parabolic	Jarak antara 4-25	Jarak antara 4-21

Memilih antenna dengan luas yang tepat atau beamwidth yang terbatas adalah penting untuk mempunyai pola jangkauan RF yang diinginkan. Sebagai contoh, bayangkan lorong panjang dalam sebuah rumah sakit. Ada kamar di kedua sisi lorong tersebut, dan sebagai ganti menggunakan beberapa access point dengan antenna omni, anda telah memutuskan untuk menggunakan access point tunggal dengan antenna semi-directional seperti antenna patch (tambalan).

Access point dan patch antenna ditempatkan pada ujung lorong menghadap sebuah lorong. Untuk melengkapi jangkauan pada lantai atas dan bawah lantai tersebut antenna patch dapat dipilih dengan beamwidth vertical besar secara signifikan contohnya 60-90 derajat. Setelah beberapa percobaan , anda dapat menemukan bahwa pilihan anda pada patch antenna dengan 80 derajat beamwidth vertical melakukan pekerjaan dengan baik.

Saat ini keperluan beamwidth horizontal harus diputuskan . melalui panjang lorong, percobaan bisa memperlihatkan antenna high-gain harus digunakan dengan tujuan jangkauan sinyal yang cukup pada akhir yang berlawanan. Mempunyai gain yang tinggi, beamwidth horizontal dari antenna patch secara signifikan terbatas seperti ruangan pada tiap sisi lorong yang tidak memiliki jangkuan yang cukup. Ditambah pula, antenna high-gain tidak memiliki beamwidth vertical yang cukup besar untuk menutupi lantai atas dan bawahnya. Pada kasus ini, anda bisa memutuskan menggunakan dua antenna patch – satu pada ujung lorong berhadapan satu sama lain. Keduanya akan rendah nilai gain-nya dengan lebar beamwidth horizontal dan vertical seakan-akan tiap sisi ruangan pada lorong telingkpi bersama dengan lantai bawah dan atasnya. Melaui gain rendah, antenna mungkin hanya bisa menutupi sebagian (mungkin setengah) dari luas lorong.

Seperti bisa anda lihat dari contoh ini, pemilihan yang cocok dari beamwidth untuk mendapatkan pola jangkauan yang benar sangat penting dan sepertinya menentukan berapa banyak hardware (seperti access point) yang perlu dibeli untuk peng-install-an.

5.5 Free Space Path Loss

Free space path loss (atau hanya Path Loss) ditujukan pada kehilangan yang diakibatkan oleh sinyal RF yang harus dibayar karena perbesaran pada “penyebaran sinyal” yang mana secara alami meluas pada depan gelombang. Semakin lebar bagian depan gelombang, semakin sedikit kekuatan yang dapat disokong ke dalam antenna penerima. Seperti halnya pneyebarluasan sinyal pemancar, kekuatannya meningkat pada taraf kebalikannya sebanding dengan jarak yang dijalaninya dan sebanding dengan kelebaran sinyal. Level kekuatannya menjadi factor yang sangat penting ketika hubungan yang terus-menerus menjadi pertimbangan.

Persamaan Path loss merupakan salah satu pondasi dari perhitungan anggaran belanja sebuah sambungan. Path loss mempersembahkan sumber tunggal terbesar dalam system wireless. Dibawah ini adalah rumus untuk Path Loss.

$$PathLoss = 20LOG_{10}[\frac{4\prod d}{}] \{dB\}$$

Rumus PathLoss

Note: Anda tidak akan bisa mencoba rumus Path Loss pada tugas CWNA, namun ini disediakan sebagai refernsi administrative anda.

5.6 Peraturan 6 dB

Penyelidikan terturup pada persamaan Path loss menghasilkan hubungan yang tidak berguna berkaitan dengan hal hubungan anggaran belanja. Tiap 6 dB meningkatkan EIRP setara dengan 2 kali jarak. Sebaliknya, pengurangan 6 dB pada EIRP berarti memotong jaraknya hingga setengah. Dibawah ini adalah table yag memberi Anda perkiraan secara kasar dari Path Loss untuk memberi jarak anara pemancar dan penerima pada 2,4 GHz.

Tabel 5.2. Tabel Perbandingan Jarak dan Loss

Jarak	Loss (dalam 6dB)
100 meters	80.23
200 meters	86.25
500 meters	94.21
1000 meters	100.23
2000 meters	106.25
5000 meters	114.21
10000 meters	120.23

5.7 Instalasi Antenna

Sangatlah penting untuk memiliki installasi antenna yang benar dalam wirelsess LAN. Installasi yangtidak tepat dapat membawa pada kerusakan atau kehancuran dari peraltan anda dan juga dapat membawa pada kerugian seseorang. Pekerjaan yang baik dari system wireless LAN sama pentingnya dengan keselamatan seseorang, yang dicapai melalui penempatan yang benar, pemasangan, pengarahan dan penyesuaian. Pada bagian ini kita akan meliputi :

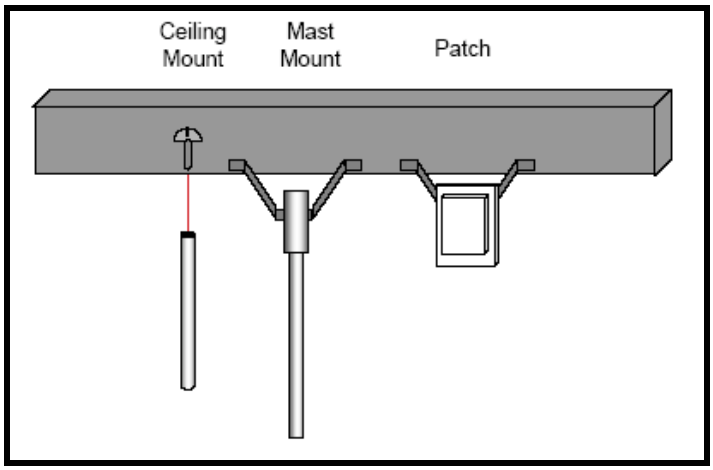
- Penempatan (placement)
- Pemasangan (mounting)
- Penggunaan yang tepat (appropriate use)
- Pengarahan (orientation)
- Penyesuaian (alignment)
- Keamanan (safety)
- Pemeliharaan (maintenance)

5.7.1 Penempatan (placement)

Memasang antenna omni-directional berkaitan dengan access point didekat pertengahan dari jangkauan area yang diinginkan dimanapun berada. Menempatkan antenna setinggi mungkin untuk meningkatkan jangkauan area, berhati-hati bahwa user meletakkan sesuatu dibawah antenna masih dapat menerima. Terutama ketika menggunakan omni antenna high-gain. Antenna diluar ruangan harus dipasang diatas rintangan seperti pepohonan dan bangunan seakan-akan tidak ada objek yang melanggar batas Zone Fresnel

5.7.2 Pemasangan (mounted)

Sekali anda telah menghitung betapa pentingnya kekuatan output, gain, dan jarak yang anda perlukan untuk memancarkan sinyal RF, dan telah memilih antenna yang tepat untuk pekerjaan tersebut, anda harus memasang antenna tersebut. Terdapat beberapa pilihan untuk memasang antenna didalam maupun diluar ruangan.



Gambar 5.15. Pemasangan antenna

Pilihan pemasangan antenna

- Pemasangan pada langit-langit – biasanya tergantung di palang pada bawah langit-langit.
- Pemasangan pada dinding – memaksa sinyal pergi dari permukaan vertical
- Pemasangan pillar(tiang penyangga) – memasang sama rata pada permukaan vertical
- Dataran tanah – didudukkan datar pada tanah
- Pemasangan tiang layar – antenna dipasang pada ujungnya
- Pemasangan penyambungan – pemasangan pada tiang layar yang bisa dipindah-pindah.
- Pemasangan pada cerobong asap / semrong lampu – berbagai jenis hardware yang membolehkan antenna dipasang pada cerobong asap / semrong lampu.
- Penyanggah tiang – antenna didudukkan diatas penyanggah.

Tidak ada jawaban sempurna untuk dimana memasanag antenna secara tepat. Anda akan belajar pada bab 11 (Dasar Meninjau Tempat) bahwa penempatan yang disarankan dan memasang antenna akan menjadi bagian dari meninjau tempat yang tepat. Tidak ada pengganti untuk dalam-masa-latihan –pekerjaan, yaitu dimana anda seringnya belajar bagaimana memasang antenna wireless LAN menggunakan berbagai jenis tipe hardware pemasang. Tiap tipe dari pemasang

akan ada bersama dengan instruksi (petunjuk) dari pabrik tentang bagaimana meng-install dan mengamankannya. Terdapat berbagai jenis yang berbeda dari tiap tipe pemasang karena tiap pabrik memiliki cara tersendiri dalam merancang alat pemasang.

Beberapa hal yang perlu diingat dalam memasang antenna adalah :

- Seringkali penopang yang dikirimkan dengan antenna tidak bisa bekerja untuk situasi tertentu. Memodifikasi penopang atau merakit ulang penopang mungkin diperlukan.
- Jangan menggantung antenna dengan kabelnya dan pastikan pemasangannya kokoh dan aman. Kabelnya bisa putus dan goyangnya kabel bisa menghasilkan pergerakan pada pusatnya.
- Sesungguhnya bagaimana antenna dipasang harus dispesifikasikan untuk tiap antenna pada laopran tinjauan tempat.

Memasang dengan ilmu keindahan

Antenna biasanya tidak kelihatan dan harus disembunyikan. Beberapa pabrik membuat langit-langit untuk menyisipkan antenna. Ketika keindahan penting, antenn patch atau panel mungkin lebih digunakan daripada antenna omni. Jika mungkin, antenna harus disembunyikan untuk menghidari kerusakan oleh anak-anak dan juga oleh orang dewasa yang secara sengaja merusak komponenya.

5.7.3 Penggunaan yang tepat (appropriate use)

Gunakan antenna untuk dalam ruangan(indoor antenna) di dalam bangunan dan antenna untuk luar ruangan(outdoor antenna) diluar bangunan kecuali area dalam ruangan secara signifikan sangat besar untuk membenarkan penggunaan antenna untuk luar ruangan (outdoor antenna). Antenna untuk luar ruangan (outdoor antenna) paling sering disegel untuk mencegah air memasuki daerah element antenna dan dibuat dari plastic untuk menahan perubahan panas dan dingin yang ekstrim. Antenna untuk dalam ruangan (indoor antenna) tidak dibuat untuk penggunaan di luar ruangan dan umumnya tidak bisa menahan elemennya.

5.7.4 Orientation

Orientasi antenna membutuhkan pengkutuban, yang telah dibahas sebelumnya sebagai pemilik dampak berpengaruh pada penerimaan sinyal. Bila antenna diarahkan dengan bagian electric parallel dengan permukaan bumi, maka client (jika antenna dipasangn pada access point) juga harus mempunyai pengarahan yang sama untuk penerimaan ang maksimum. Kebalikannya juga berlaku dengan keduanya memiliki bagian electric yang diarahkan secara vertical dengan permukaan tanah. Keluaran dari jembatan penguhubung akan secara drastic berkurang bila tiap akhir hubungan tidak memiliki orientasi antenna yang sama.

5.7.5 Penyesuaian (Alignment)

Penyesuaian antenna terkadang kritis dan lain waktu tidak. Beberapa antenna mempunyai beamwidth horizontal dan vertical yang sangat lebar sehingga memungkinkan administrator untuk membidik dua antenna pada lingkungan jembatan bangunan-ke-bangunan pada tiap arah umum lain dan mendapatkan penerimaan yang hapir sempurna. Penyesuaian (alignment) lebih penting ketika mengimplementasikan hubungan jarak jauh menggunakan antenna highly-directional. Jembatan wireless dating dengan software penyesuaian (alignment) yang membantu administrator mengoptimalkan penyesuaian antenna untuk penerimaan yang terbaik, yang mengurangi paket yang hilang dan perhitungan berulang yang tinggi ketika kekuatan sinyal membesar.

Ketika menggunakan access point dengan antenna omni-directional atau semi-directional, penyesuaian (alignment) yang tepat biasanya adalah masalah menutupi area yang tepat seperti client wireless bisa berhubungan pada tempat dimana hubungan diharapkan.

5.7.5 Keamanan

Antenna RF, seperti peralatan listrik lainnya, bisa menjadi berbahaya untuk diimplemetasikan dan dioperasikan. Petunjuk dibawah ini harus dipelajari kapanpun anda atau salah satu dari perkumpulan anda meng-install atau dengan kata lain bekerja dengan antenna RF.

Ikuti petunjuknya

Secara hati-hati ikuti instruksi yang disediakan semua antenna. mengikuti semua instruksi yang disediakan akan mencegah kerusakan oleh antenna dan kerusakan perorangan. Kebanyakan pencegahan keaman yang ditemukan pada petunjuk pabrik antenna masuk akal.

Jangan disentuh ketika powernya masih terpasang

Jangan pernah menyentuh antenna high-gain dengan bagian tubuh anda yang mana saja atau tunjuklah melalui badan anda ketika ia memancar. FCC membolehkan kekuatan RF dalam jumlah yang sangat tinggi untuk dipancarkan pada band bebas yang di-license ketika mengkonfigurasi hubungan point-to-point. Meletakkan bagian tubuh anda yang mana saja didepan antenna highly-directional 2.4 GHz yang sedang memancar pada kekuatan tinggi akan sama dengan meletakkan tubuh anda pada oven microwave.

Installer professional

Untuk kebanyakan peng-installan antenna di tempat tinggi, pertimbangkan menggunakan installer professional. Pemanjat professional dan installer dilatih dalam pemanjatan tepat yang aman, dan akan bisa meng-install dengan lebih baik dan mengamankan antenna wireless LAN anda jika dipasang di ujung, menara, atau tipe bangunan tinggi lainnya.

Hambatan logam

Jauhkan antenna dari hambatan logam seperti pemanas dan saluran air-conditioning. Penyangga langit-langit yang besar, susunan bangunan super, dan aliran kabel power utama. Tipe hambatan metal ini menciptakan sejumlah jalan kecil yang signifikan. Dan, sejak tipe hambatan logam ini memantulkan bagian sinyal RF yang besar, jika sinyalnya di siarkan pada kekuatan penuh, sinyal yang dipantulkan akan bisa berbahaya untuk orang yang melihat.

Garis kekuatan (Power lines)

Menara antenna harus diletakkan pada jarak aman dari power lines terdekat. Jarak aman yang disarankan adalah dua kali tinggi antenna. Berhubung antenna wireless LAN umumnya kecil, pada prakteknya saran ini biasanya tidak digunakan. Bukanlah hal yang bagus mempunyai antenna wireless LAN didekat sumber power karena arus listrik pendek antara sumber kekuatan (power) dan wireless LAB bisa berbahaya untuk personil yang berkerja pada wireless LAN dan bisa menghancurkan peralatan wireless LAN.

Pasak (grounding rods)

Gunakan pasak khusus dan ikuti Kode Listrik Nasional (National Electrical Code) dan kode listrik local untuk antenna outdoor yang tepat dan pasak menara. Pasak harus secara umum mempunyai kurang 5 ohms dari permukaan tanah. Resistansi yang disarankan adalah 2 ohms atau kurang. Pasak dapat mencegah kerusakan pada peralatan wireless LAN dan mungkin juga menyelamatkan hidup siapapun yang memanjat menara bila menara tidak disoroti cahaya.

5.7.6 Pemeliharaan (maintenance)

Untuk mencegah embun memasuki kabel antenna, segel semua kabel konektor luar menggunanakan produk komersial seperti coax compatible electrical tape atau coax-seal. Embun yang telah memasuki konektor dan kabel sangat sulit dihilangkan . biasanya lebih hemat untuk mengganti kable dan konektornya daripada menghilangkan embun tersebut. Konektor dan kabel dengan sejumlah air didalamnya akan membuat sinyal RF tidak menentu dan bisa menyebabkan penurunan sinyal secara signifikan karena kehadiran sebuah air akan merubah impedansi kabel, dan karennya merubah VSWR.

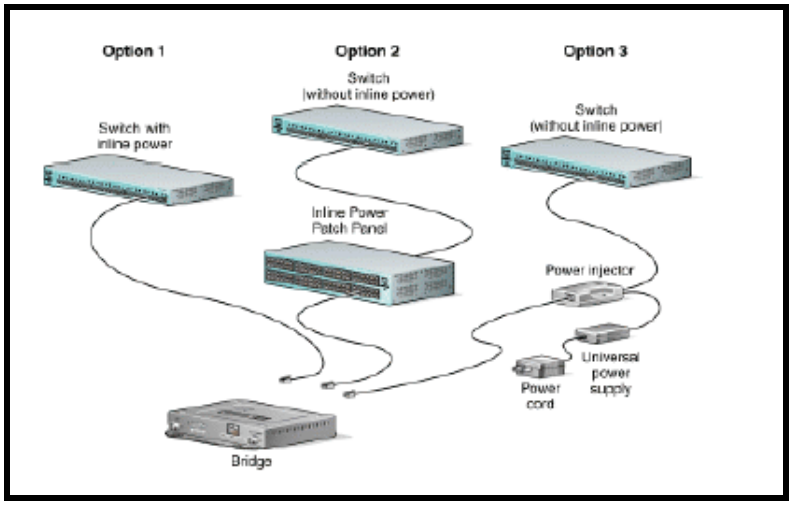
Ketika menginstall kabel RF diluar ruangan, pastikan untuk memasang konektor saling menghadap dan gunakan lem pada kabel sehingga air akan langsung menjauh dari titik dimana embun tampaknya akan memasuki konektor. Cek segel secara teratur. Segel pada material terkadang dapat mengering ketika terkena matahari dalam jangka waktu yang lama dan mungkin perlu menggantinya dari waktu ke waktu.

5.8 Peralatan Power over Ethernet (PoE)

Power Over Ethernet (PoE) adalah metode yang mengirim voltase DC pada access point, jembatan wireless, atau jembatan wireless workgroup melalui kabel Ethernet Cat5 dengan tujuan memberi daya pada unit. PoE digunakan ketika penyiman AC power tidak tersedia dimana peralatan infrastruktur wireless LAN harusnya berada, kabel Ethernet digunakan untuk membawa baik data dan power dari sebuah unit.

Mempertimbangkan warehouse dimana access point perlu untuk dipasang pada langit-langit sebuah bangunan. Biaya kerja yang akan berpengaruh untuk memasang jalur listrik melaui langit-langit bangunan untuk memperkuat access point perlu dipertimbangkan . Mempekerjakan seorang ahli listrik untuk melakukan tipe pekerjaan ini akan menghabiskan banyak uang dan waktu.

Ingatlah bahwa kabel Ethernet hanya bisa membawa data sejauh 100 meter dan, untuk jarak lebih dari 100 meter, PoE bukanlah solusi yang bagus. **Gambar 5.16** menggambarkan bagaimana peralatan POE akan menyediakan power ke aeccess point.



Gambar 5.16 Pemasangan PoE

Seringkali tempat terbaik untuk memasang access point atau jembatan untuk konektivitas RF tidak memiliki sumber AC power. Makanya, PoE bisa merupakan penolong yang hebat untuk mengimplementasi jaringan wireless dengan rancangan yang baik . beberapa pabrik membolehkan hanya untuk PoE untuk memperkuat peralatan meraka, bukan AC power standar.

5.8.1 Pilihan Umum PoE

Peralatan PoE tersedia dalam beberapa tipe

- Single-port DC voltage injectors
- Multi-port DC volatage injectors
- Ethernet switches yang dirancang untuk memasukkan voltase DC pada tiap port pada bagian tertentu dari pin.

Meskipun konfigurasi dan manajemen secara umum tidak penting untk peralatan PoE, ada beberapa protes yang harus diwaspadaiketika anda mulai mengimplementasikan PoE.

Pertama, tidak ada standar industri dalam mengimplementasi PoE. Artinya bahwa pabrik dari peralatan PoE tidak mempunyai kerjasama dan setuju tentang bagaimana peralatan ini harus berhubungan dengan peralatan lain. Bila anda menggunakan peralatan wirelss seperti access point dan akan di power-in dengan PoE, sangat disarankan agar anda membeli peralatan PoE dari pabrik yang sama dengan access point. Saran ini juga berlaku pada semua peralatan manapun ketika mempertimbangakan ingin di-power-in dengan PoE.

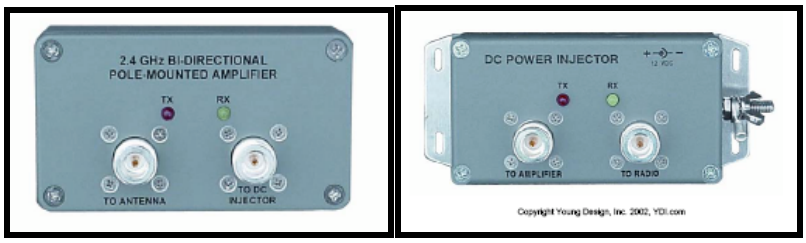
Kedua, dan sama dengan sifat dari protes pertama, adalah bahwa output voltase dibutuhkan untuk memperkuat peralatan wireless LAN yang berbeda dari pabrik ke pabrik. Protes ini adalah alasan lain untuk menggunakan peralatan dari penjual (pabrik) yang sama ketika menggunakan PoE. Ketika ragu, Tanya pada pabriknya atau penjualnya tempat dimana peralatan tersebut dibeli.

Akhirnya, pin yang tidak terpakai digunakan untuk membawa arus listrik melalui Enthernet bukanlah hal yang standar. Satu pabrik bisa saja membawa power pada pin 4 dan 5, padahal yang lainnya membawa power pda pin7 dan 8. bila anda mengkoneksikan kabel dengan membawa power pada pin4 dan 5 untuk access point yang tidak menerima power pada pin tersebut, maka aceess pont tidak akan dialiri arus

5.8.1.1 Pengalir single-port volatase DC (Single-port DC voltage Injectors)

Access point dan jembatan yang secara khusus wajib menggunakan PoE termasuk single-port DC voltage injetors intuk mengaliri unit. Lihat **gambar 5.17** dibawah untuk contoh dari single-port DC voltage injetors, Injector

single-port ini diterima ketika digunakan dengan sejumlah kecil peralatan wireless infrasctructure, tapi secara cepat menjadi beban, membuat berantakan mengabeli lemari, ketika membangun jaringan wireless menengah atau besar.



Gambar 5.17 Sebuah injector single-port

5.8.1.2 Injector multi-port DC voltage

Beberapa pabrik menawarkan injector multi-port termasuk model port-4, 6 atau 12. model ini mungkin lebih ekonomis atau cocok untuk pemasangan dimana banyak peralatan harus dialiri listrik melaui kabel Cat5 menghasilkan dalam lemari pengkabelan tunggal atau dari satu switch. Injector multi-port DC voltage secara khusus ,mengoperasikan dengan cara yang tepat sama seperti rekannyam single-port. **Lihat gambar 5.19** untuk contoh dari injector PoE multi-port . Sebuah injector multi-port DC voltage tampak seperti switch Ethernet dengan dua kalo seperti banyak port. Injector multi-port DC voltage adalah peralatan pass-through dimana anda berhubungan dengan switch Ethernet (atau hub) ke port masukan, dan kemudian menghubungkan peralatan PoE client ke peralatan output, keduanya melaui kabel Cat5. injector PoE menghubungkan ke sumber AC power pada ruang pengkabelan. Injector multi-port ini cocok untuk installasi jaringan wireless ukuran sedang dimana 50 access point keatas dibutuhkan, namun pada perusahaan besar, bahkan injector multi-port DC voltage terpadat. Dikombinasikan dengan hub ethrenet atau switche bisa menjadi cluttered ketika dipasang pada lemari pengkabelan.

5.8.1.3 Swicth Ethernert Active

Langkah selanjutnya untuk pemasangan pada perusahaan besar dari access point adalah implementasi switches etehrnet active. Peralatan ini menyatukan injeksi DC voltage pada switch Ethernet sendiri memperbolehkan sejumlah besar peraltan PoE tanpa hardware tambahan di jaringan. Lihat **gambar 5.20** untuk contoh dari switch Active Ethernet. Lemari pengkabelan

tidak akan mempunyai hardware tambahan lain daripada switches Ethernet yang telah ada untuk sebuah jaringan non-PoE. Beberapa pabrik membuat switches ini dalam berbagai konfigurasi yang berbeda (sejumlah port). Pada banyak switch active Ethernet, switch dapat secara otomatis merasakan peralatan client PoE pada sebuah jaringan. Bila switchnya tidak mendeteksi peralatan PoE pada sambungan tersebut, DC voltage-nya tidak diaktifkan pada port tersebut.

Seperti Anda lihat pada gambar, sebuah switch Active Ethernet tampak tidak ada bedanya dengan switch Ethernet umumnya. Satu-satunya perbedaan adalah ditambahkannya kemampuan bagian dalam dari mensuplai DC voltage pada tiap port.

5.8.2 PoE Compatibility

Peralatan yang bukan termasuk "PoE Compatibility" dapat dikonversikan pada Power-over-Ethernet dengan cara DC "picker" atau "tap". Terkadang ini disebut Active Ethernet "splitter". Peralatan ini mengambil DC voltage yang telah di-injeksi-kan ke dalam kabel CAT5 oleh injector dan membuat nya available untuk peralatan melalui tuas power DC biasa.

Dengan tujuan untuk menggunakan Power-over-Ethernet satu dari 2 kombinas peralatan ini dibutuhkan :

```
(Injector) + (peralatan kompatibel dengan PoE)
atau
(Injector) + (peralatan yang tidak kompatibel  dengan PoE ) + (Picker)
```

5.8.3 Types dari Injector

Ada 2 type basic dari Injector yang tersedia,*passive* dan *fault protected.* Setiap type yang tersedia memiliki berbagai tingkatan tegangan dan port.

Passive injector menempatkan tegangan DC menjadi kabel CAT5. Pelatan-peraltan ini menyediakan tidak adanya short-circuit atau proteksi terhadap arus yang berlebih.

Fault protected injector menyediakan monitoring fault secara berkesinambungan dan proteksi untuk mendekteksi adanya short circuit dan kondisi arus yang berlebih di kabel CAT5.

5.8.4 Types dari Picker/Taps

2 basic tipe dari picker dan tap adalah : passive dan regulated. Passive tap, secara sederhana membawa tegangan dari CAT5 dan menyalurkannya ke dalam peralatan untuk menyambungkan ke koneksi. Oleh karena itu, jika injector meng-inject48 VDC (Volts of Direct Current) , maka 48 VDC akan tetap diproduksi di output dari passive tap.

Regulated tap membawa tegangan ke CAT5 kabel dan mengkonversikannya ke tegangan yang lain. Beberapa tegangan regulated yang tersedia (5 VDC, 6 VDC, & 12 VDC) mengijinkan variety yang lebar dari peralatan non-PoE yang dikuatkan melewati kabel CAT5.

5.8.5 Tegangan dan Standart Pinout

Meskipun IEEE bekerja pada standartnya seperti 802.3af untuk PoE, sebuah definisi standard belum dikenalkan. Pada sekarang ini, vendor peraltan yang berbeda menggunakan tegangan PoE yang berbeda dan konfigurasi pin CAT5 untuk menyediakan power DC. Oleh karena itu , sangat penting untuk menyeleksi peralatan PoE yang yang cocok untuk setiap peralatan yang anda rencanakan untuk menguatkan melewati kabel CAT5. IEEE mempunyai standarisasi pada penggunaan 48 VDC sebagai tegangan PoE yang di-inject-kan. Penggunaan dari tegangan yang sangat tinggi akan mengurangi arus yang mengalir melewati kabel CAT5 dan maka akan menaikkan beban dan menaikkan batas panjang dari kabel CAT5. Dimana maksimum panjang kabel belum merupakan pertimbangan yang utama , beberapa vendor telah memilih 24 VDC dan juga 12 VDC sebagai tegangan injeksi.

5.8.6 Fault Protection

Tujuan utama dari fault protection adalah melindungi kabel, peralatan , dan power supply dalam suatu kesalahan atau terjadinya short-circuit. Selama operasi normal, sebuah kesalahan mungkin tidak akan pernah terjadi dalam kabel CAT5. Bagaimanapun juga, ada banyak cara sebuah fault akan dikenalkan ke dalam kabel CAT5, meliputi beberapa contoh di bawah ini:

- Peralatan attached akan sangat tidak compatible dengan PoE dan tidak mempunyai non-standard atau koneksi defective bahwa short-circuit konduktor PoE. Sekarang ini, kebanyakn dari peralatan non-PoE tidak mempunyai koneksi pada pin PoE.
- Pemasangan kabel CAT5 yang tidak tepat. Memotong atau crushed kabel CAT5, dimana insulasi pada satu atau lebih konduktor akan menyebabkan kontak dengan beberapa atau material konduktor lainnya.

Selama kondisi fault , circuit fault-protection mematikan tegangan DC yang di-inject-kan ke dalam kabel. Operasi sirkuit fault-protection varies dari model ke model. Beberapa model secara bersambungan me-monitor kabel dan menyimpan kembali power secara otomatis , ketika sekali fault di pindahkan. Beberapa model laninnya harus secara manually di-reset dengan menekan tombol reset atau memutar power.

5.9 5.9 Wireless LAN Accessoris

Ketika waktu berjalan untuk mengkoneksikan semua peralatan wireless LAN anda secara bersama-sama, anda akan memerlukan untuk mem-purchase kabel yang sesuai dan aksesoris yang akan memaksimalkan throughput anda , meminimalkan loss-sinyal anda , dan yang paling penting mengijinkan anda untuk membuat koneksi secara tepat. Dalam section ini akan mendiskusikan beberapa type dari aksesoris dan dimana mereka akan fit ke dalam design wireless LAN. Berikut ini adalah tipe2 aksesoris yang akan didiskusikan dalam section ini :

- RF Amplifier
- RF Attenuator
- Lighting Arrestors
- RF Connectors
- RF Cables
- RF Splitters

Setiap dari peralatan ini adalah sangat penting untuk membangun wireless LAN secara sukses. Beberapa item yang digunakan lebih dari yang lain , ada beberapa item yang wajib , dimana yang lainnya adalah optional. Ini seperti bahwasanya seorang

administrator harus akan menginstall dan menggunakan semua dari item beberapa kali ketika mengimplementasi dan mengatur sebuah wireless LAN.

5.9.1 RF Amplifier

Sebagai namanya yang disarankan , sebuah RF Amplifier akan digunakan untuk amplify atau menaikkan amplitude dari sebuah sinyal RF. Kenaikkan positif dalam power biasa disebut GAIN dan diukur dalam +dBi. Sebuah amplifier akan digunakan ketika mengganti kerugian untuk loss yang terjadi oleh sinyal RF , meskipun kaitan jarak antara antenna atau panjang dari kabel dari peralatan infrastruktur wireless ke antenna itu sendiri. Kebanyakan RF Amplifier digunakan dengan wireless LAN yang dikuatkan dengan menggunakan tegangan DC yang diberikan kepada kabel RF dengan injector DC di dekat sumber dari sinyal RF (seperti access point atau bridge)

Kadang-kadang tegangan DC digunakan untuk menguatkan RF amplifier yang disebut “phantom voltage” karena RF amplifier kelihatan seperti power up secara magic. Injector DC dikuatkan menggunakan tegangan AC dari wall outlet , jadi akan kelihatan seperti di lokasikan di wiring-closet. Pada scenario ini , kabel RF membawa kedua-duanya yaitu sinyal RF frekuensi tinggi dan tegangan DC yang diperlukan untuk menguatkan in-line amplifier , dimana in-turn, boosts amplitude sinyal RF. Gambar dibawah ini depicts both sebuah RF amplifier dan DC power injector

Gambar 5.18. RF Amplifier

RF amplifier dibagi menjadi 2 tipe yaitu unidirectional dan bi-directional. Unidirectional amplifier compensate untuk sinyal loss incurred over long kabel RF dengan menaikkan level dari sinyal sebelum akan di-inject-kan ke dalam antenna transmitting. Amplifier bidirectional menaikkan sensitifitas secara efektif dari receiving-antenna dengan mengeraskan sinyal yang diterima sebelum diberikan ke access-point, bridge,atau client device. Amplifier bidirectional seharusnya diletakkan sedekat mungkin dengan antenna sehingga akan memungkinkan penggantian kerugian secara efektif untuk kabel yang loss antara antenna dan receiver (access-pint atau bridge) untuk penerimaan sinyal. Kebanyakan amplifier digunakan dengan wireless-LAN yang bi-directional.

5.9.2 Common Options

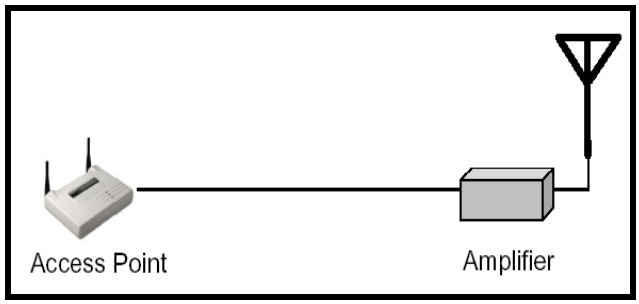
Sebelum anda mendapatkan ide untuk memutuskan amplifier mana yang anda beli , ada baiknya anda harus tahu kebutuhan dari spesifikasi amplifier itu sendiri. Sekali anda sudah mengetahui dari spesifikasi tersebut, misalnya impedansi (ohms), gain (dB), respon frekuensi (range dalam GHz), VSWR, input (mW atau dBm) dan output (mW atau dBm), maka anda sudah siap dalam memilih RF Amplifier.

Respon frekuensi adalah spesifikasi pertama yang harus anda putuskan terlebih dulu. Jika wireless-LAN menggunakan spectrum frekuensi 5GHz, sebuah amplifier akan bekerja hanya pada 2.4 GHz spectrum frekuensi yang tidak bekerja. Menentukan seberapa besar gain, input, dan power output adalah diperlukan dengan menampilkan kalkulasi dari RF yang diperlukan. Amplifier seharusnya sesuai dengan impedansi dengan semua keperluan hardware dari wireless-LAN antara transmitter dan antenna. Secara umum, komponen wireless-LAN mempunyai impedansi 50 ohms, tapi bagaimanapun juga akan sangat baik jika memeriksa impedansi dari setiap komponen dari wireless-LAN.

Amplifier seharusnya disambungkan ke dalam jaringan , jadi amplifier akan dipilih dengan beberapa konektor yang sama sebagai kabel dan/ antenna untuk amplifier akan disambungkan. Secara typically, RF Amplifier akan mempunyai sifat yang sama dengan SMA atau konektor N-Type. Konektor SMA dan N-Type melakukan dengan baik dan digunakan secara luas.

5.9.3 Configuration & Management

RF amplifier yang digunakan dengan wireless-LAN di-instalasi secara seri dengan path dari sinyal utama seperti terlihat pada **Gambar 5.19**. Amplifier secara typicallydisusun ke permukaan yang solid menggunakan sekrup melalui piringan dari amplifier.



Gambar 5.19. RF Amplifier dengan Access Point

5.9.4 Syarat-syarat Khusus

FCC CFR menyatakan bahwa setiap sistem yang diguanakn dalam ISM dan UNII harus bersertifikasi sebagai sistem yang lengkap dan diberikan nomor sertifikat oleh FCC. Keterangan ini akan disertai oleh sertifikat yang akan mendaftar keperluan berbagai peralatan dan pengenal FCC mereka aka diijinkan untuk menggunakan sistem wireless-LAN yang khusus. Semua bagian dari wireless-LAN setup yang digunakan akan dilist di dalam sertifikat. Memahami keperluan ini akan menjadikan krusial ketika menyetujui dengan amplifier. Sebuah ”sistem” yang didefinisikan sebagai perlatan transmitting, pengkabelan, konektor, amplifier, attenuator,splitter dan antenna. Perusahaan memperoleh persetujuan FCC atau ”sertifikasi” atas hardware mereka yang dijual ke end-user atas perlatan radio dan antenna dan menggunakan mereka sebagai suatu sistem tanpa melakukan konfirmasi dengan FCC untuk testing dan sertifikasi. Ketika peralatan tambahan seperti amplifier ditambahkan ke dalam sistem, sertifikasi perusahaan tidak akan lama diterapkan dan user harus memperoleh sertifikasi atas sistem mereka. Ini akan menghabiskna biaya sebesar $12,000 tiap sistem. Jawaban untuk permasalahan ini adalah menjual sistem yang telah bersertifikasi FCC dari vendor yang bereputasi yang menyediakan kebutuhan jaringan wireless.

CFR 15.204 tidak memperbolehkan amplifier dipasarkan atau dijual ketika tidak merupakan bagian dari sistem yang bersertifikasi. FCC memelihara database dari sistem yang bersertifikasi dan perusahaan yang memegang sertifikasi ini. Database ini dapat anda cari pada alamatweb:http://gullfoss2.fcc.gov/cgi-bin /ws.exe/prod/oet/forms/reports/Search_Form.hts & ?form=Generic_Search

FCC memelihara website ini dengan sangat cermat sekali dan selalu beredar. Update dilakukan setidaknya seminggu sekali. End-user dapat dikenakan denda untuk pelanggaran aturan FCC sementara mereka menggunakan peralatannya. Pelanggaran FCC sekali denda berkisar antara $27,500 - $1,200,000. FCC biasanya mengijinkan pelanggar waktu (10 hari) untuk mengoreksi masalahnya dan melaporkan ke FCC bagaimana pelanggaran tersebut telah diperbaiki.Ini bukan hal yang tidak biasa untuk FCC dalam meng-audit Wireless ISP untuk mencari pelanggaran sistem bersertifikasi.

Banyak perusahaan tidak memproduksi amplifier yang digunakan dengan sistem mereka. Untuk alasan ini, perusahaan yang memproduksi amplifier (tpi bukan unutk hardware wireless-LAN) yang mendapatkan sertifikasi FCC ke dalam sistem wireless-LAN menggunakan amplifier mereka dan beberapa hardware wireless-LAN dari perusahaan lainnya secara bersamaan. Hati-hati dalam tipe apakah amplifier yang anda beli, beberapa amplifier menyebabkan FCC hanya untuk sistem yang bersertifikasi agar dapat menggunakan DSSS channel 2-10 daripada 1-11 seperti sistem yang tidak teramplifier. Berkaitan dengan bagaimana sinyal RF di diperkuat dan mengeluarkan ke dalam spektrum frekuensi RF yang terlisensi dimluar dari ISM dan UNII

FCC CFR 15.203 menyatakan bahwa installer yang bertaggung jawab unutk menyakinkan bahwa radiator intentional yang digunakan dengan antenna yang disahkan. Antenna dibuat supaya mereka dapat diperbaiki, tapi dipasang ke non-certified radiator intentional.

Satu pertanyaan bahwa kita ingin mengalamatkan yang berkaitan CFR 15.204 bahwa satu antenna dari perusahaan tidak dapat digunakan dengan raiator intentional perusahaan lainnya (bridge, PC Card, atau access-point) tanpa sertifikasi FCC sebagai sistem. Peraturan ini secara langsung mempengaruhi indivudual yang ingin menyambungkan sebuah antenna Pringles ke PC Card untuk tujuan dari pengendalian perang.

Ketika membeli RF Amplifier untuk digunakan sebagai bagian dari wireless-LAN , tanyalah bagian dari dokumentasi sertifikasi FCC untuk sebuah amplifier sebelum anda membelinya. Ada 2 kelas perubahan yang dapat dibuat ke dalam sertifikasi FCC. Kelas pertama adalah kelas yang saya rubah. Tipe ini, perubahan dapat dibuat oleh perusahaan yang menginginkan perubahan dokumen yang tidak mempengaruhi negatif pada perkembangan RF atau density sinyal (kenaikkan interferensi dengan sistem lain di dalam lingkungan anda) dengan catatan pada sertifikat FCC dan menulis sebuah sinopsis tentang bagaimana perubahan dapat dilibatkan dan kenapa hal tersebut tidak mempunyai pengaruh negatif. Kelas kedua adalah perubahan yang mempunyai pengaruh negatif terhadap perkembangan RF atau density sinyal dan membutuhkan bahwa sistem harus di resertifikasi kembali oleh FCC

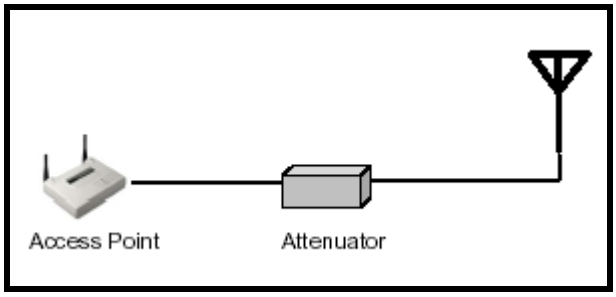
5.9.5 RF Attenuator

RF Attenuator adalah peralatan yang menyebabkan loss (dalam dB) dapat diukur secara teliti dalam sebuah sinyal RF. Sementara sebuah amplifier akan menaikkan sinyal RF , maka sebuah attenuator akan mengurangi hal itu. Mengapa anda perlu atau menginginkan untuk mengurangi sinyal RF ? Pikirkan sebuah kasus dimana acess-point memiliki ouput sebesar 100mW, dan antenna yang tersedia hanyalah omni-directional dengan gain sebesar +20 dBi. Menggunakan peralatan ini secara bersamaan dapat melanggar aturan FCC unutk power output, jadi attenuator dapat ditambahkan untuk mengurangi sinyal RF yang turun sebesar 30mW sebelum memasuki antenna. Konfigurasi ini meletakkan output power dalam parameter FCC. **Gambar 5.20** menampilkan sebuah contoh dari fixed-loss RF attenuator dengan konektor BNC (kiri) dan konektor SMA(kanan). Gambar 5.25 menampilkan contoh dari RF step attenuator.

Gambar 5.20 RF attenuator dengan konektor BNC

5.9.6 Common Options

RF attenuator tersedia untuk fixed-loss atau variabel loss. Seperti variabel amplifier, variabel attenuator mengijinkan administrator untuk mengkonfigurasi banyaknya loss yang disebabkan dalam sinyal RF dengan tepat. Variabel RF attenuator tidak digunakan dalam sistem wireless-LAN yang berkaitan dengan peraturan FCC pada sistem tersertifikasi. Secara tipically, digunakan di tempat survey supaya untuk menentukan antenna gain, keperluan amplifier, dll.



Gambar 5.21 Attenuator dengan Access Point

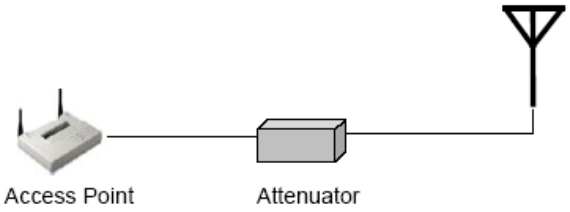
Pemilihan macam dari attenuator yang dibutuhkan , perhatikan item yang sama ketika pemilihan RF amplifier (lihat atas). Tipe dari attenuator (fixed atau variabel loss) , impedansi, rating (input, power, loss, dan respon frekuensi) dan tipe konektor seharusnya dapat dijadikan bagian dari proses pengambilan keputusan.

5.9.7 Konfigurasi dan Management

Gambar 5.22 dibawah menunjukkan bahwa peletakkan dalam wireless-LAN yang sesuai untuk sebuah RF attenuator , dimana dipasang secara seri dengan path sinyal utama. Yakinlah, attenuator coaxial akan disambungkan secara langsung di antara 2 point koneksi antara transmitter dan antenna. Sebagai contoh, antenna coaxial mungkin akan disambungkan secara langsung pada output dari access-point, pada input ke antenna, atau dari manapun di antara 2 point jika kabel RF yang multiple digunakan.

Konfigurasi dari RF attenuator tidak wajib dilakukan kecuali variabel attenuator sedang digunakan, dalam kasus ini jumlah dari pelemahan yang

dikonfigurasikan berdasarkan pada kalkulasi RF. Instruksi dari konfigurasi untuk setiap bagian dari attenuator akan dimasukkan ke dalam user manual buatan perusahaan. Untuk mengulangi pernyataan tersebut, anda akan seperti tidak melihat sistem yang bertanda dari FCC yang mempunyai variabel attenuator.



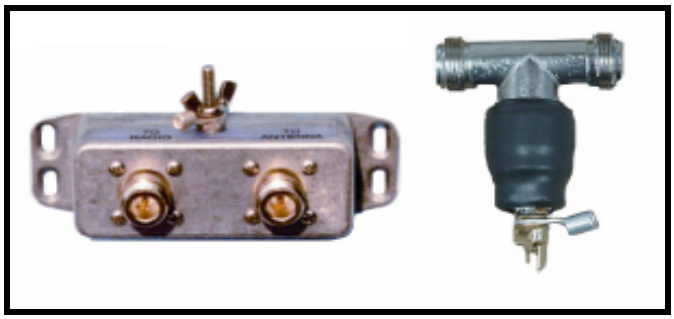
Gambar 5.22 Peletakkan dalam wireless-LAN sebuah RF attenuator

5.9.8 Lighting Arrestors

Sebuah lighting arrestor digunakan untuk melangsir arus transient ke dalam tanah yang disebabkan karena petir. Lighting arrestor digunakan untuk melindungi hardware wireless-LAN anda seperti access-point, bridges, dan kelompok dari bridge yang tercantum ke line transmisi Lighting arrestor dapat melangsir gelombang secara tidak langsung dari 5000 Amperes hingga 50 volts. Fungsi dari lighting arrestor (tergantung tipenya)adalah sebagai berikut :

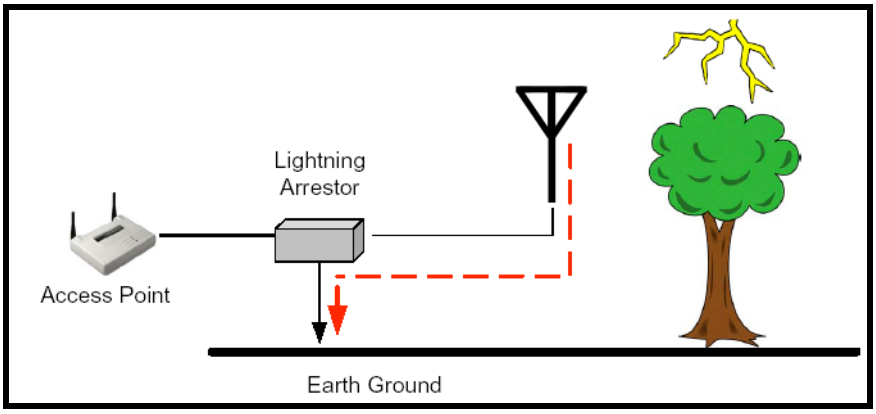
1. Petir menyambar object yang dekat.
2. Arus transient yang di induksikan ke dalam antenna atau Line transmisi coaxial.
3. Lighting arrestor mengenali arus ini dan secara cepat mengurai udara secara internal untuk menyebabkan hubungan pendek secara langsung ke tanah.

Gambar 5.23 menunjukkan beberapa tipe dari lighting arrestor. Pertama pada sebelah kanan , melangsir arus transient ke tanah dengan karakteristik fisik dari lighting arrestor itu sendiri selama mengijinkan sinyal RF yang cocok untuk melewatkannya.



Gambar 5.23 Contoh Ligthning Arrestor

Gambar 5.24 menunjukkan bagaimana lighting arrestor yang di-install ke wireless-LAN. Ketika objek terkena oleh petir elektrik yang dibangun di sekitar objek hanya untuk sesaat. Ketika petir berhenti untuk menginduksi elektrik ke objek, bangunan menjadi roboh. Ketika bangunan roboh, akan menginduksi arus tinggi dalam jumlah yang banyak ke objek terdekat, dimana dalam kasus ini, kemungkinannya adalah wireless-LAN anda atau line transmisi coaxial. Petir dibuang sebagai pulsa DC tapi lalu menyebabkan komponen AC terjadi resonansi sebesar 1 GHz, Tapi bagaimanapun juga, kebanyakan dari power tersebut dibuang dari DC ke 10 MHz.



Gambar 5.24 Installasi Lightning Dalam Jaringan

5.9.9 Common Options

Ada beberapa opsi pada lighting arrestor, dan biaya yang berkisar antara $50-$150 untuk setiap merk-nya. Tapi bagaimanapun juga, ada beberapa atribut yang harus dipertimbangkan untuk lighting arrestor dalam pembelian:

- Harus sesuai dengan standar IEEE <8µs

- Reusable
- Gas tube breakdown voltage
- Tipe konektor
- Respon frekuensi
- Impedansi
- Insertion loss
- VSWR rating
- Garansi

5.9.10 IEEE standart

Kebanyakan dari lighting arrestor dapat untuk memicu ke tanah dalam waktu kurang dari 2μs tapi IEEE menspesifikasikan bahwa proses ini dapat terjadi dalam waktu kurang dari 8μs. Ini sangat penting bahwa lighting arrestor yang anda pilih setidaknya sesuai dengan standar IEEE.

5.9.11 Reusable Unit

Beberapa lighting arrestor dapat digunakan kembali setelah adanya sambaran petir, tetapi ada juga yang tidak. Ini akan membutuhkan biaya yang efektif untuk memiliki sebuah arrestor yang dapat digunakan dalam beberapa kali. Beberapa model reusable unit, mempunyai elemen tube gas yang dapat diganti sehingga lebih murah dalam menggantinya daripada sepenuhnya lighting arrestor. Model lainnya mempunyai karakteristik fisik yang mengijinkan lighting arrestor untuk melakukan pekerjaannya secara tepat dalam beberapa kali pemakaian tanpa harus mengganti bagian-bagiannya.

5.9.12 Voltage Breakdown

Beberapa lighting arrestor support dalam pelewatan tegangan DC untuk penggunaan dalam powering RF amplifier dan lainnya tidak. Lighting arrestor harus dapat melewatkan tegangan DC yang digunakan dalam powering RF amplifier jika anda menginginkan untuk meletakkan RF amplifier lebih dekat ke arah antenna daripada ke lighting arrestor. Gas tube breakdown voltage (tegangan

yang terjadi ketika adanya pemendekan arus dari arrestor ke dalam tanah) harus lebig tinggi daripada tegangan yang disyaratkan untuk mengoperasikan in-line RF amplifier. Hal ini disarankan bahwa anda meletakkan lighting arrestor sebagai komponen terakhir dalam line RF transmission sebelum antenna sehingga lighting arrestor dapat melindungi amplifier dan attenuator sejalan dengan bridge atau access-point anda.

5.10 Tipe Konektor

Yakinkan bahwa tipe konektor dari lighting arrestor yang anda pilih cocok dengan kabel yang anda rencanakan untuk anda gunakan dalam wireless-LAN anda. Jika mereka tidak cocok satu sama lain, lalu adapter juga harus digunakan , menyisipi lebih banyak loss ke dalam RF sirkuit dan itu yang perlu.

5.10.1 Respon Frekuensi

Spesifikasi respon frekuensi dari lighting arrestor setidaknya harus sebesar frekuensi yang digunakan dalam wireless-Lan. Sebagai contoh, jika anda menggunakan hanya 2.4 GHz wireless-LAN, maka lighitng arrestor yang dispesifikasikan untuk digunakan adalah sebesar lebih dari 3 GHz, dan itu yang terbaik.

5.10.2 Impedansi

Impedansi dari arrestor harus cocok dengan semua peralatan yang ada dalam sirkuit yang terletak di antara transmitter dan antenna. Impedansi yang ada dalam kebanyak wireless-LAN adalah sebesar 50 Ohms.

5.10.3 Insertion Loss

Insertion loss harus dalam keadaan yang benar-benar rendah (mungkin sekirat 0.1 dB) sehingga tidak menyebabkan amplitudo sinyal RF yang tinggi berkurang sebagaimana sinyal melewati arrestor.

5.10.4 VSWR Rating

VSWR rating dari lighting arrestor yang memiliki kualitas yang baik adalah sebesar 1.1:1 tapi beberapa malah lebih tinggi sebesar 1.5:1. Perbandingan ratio yang rendah dari peralatan, yang baik, dapat merefleksikan menurunnya tegangan utama dari sinyal RF.

5.10.5 Garansi

Tanpa memperhatikan kualitas dari lighting arrestor , maka unit dapat berfungsi tidak baik. Carilah perusahaan yang menawarkan garansi yang bagus dalam lighting arrestornya. Beberapa perusahaan menawarkan impian yang tinggi ”No Matter What” tipe dari garansi.

5.10.6 Konfigurasi dan Pemeliharaan

Tidak ada konfigurasi yang diperlukan untuk lighting arrestor . Lighting arrestor di-install secara seri dengan path sinyal RF utama, dan koneksi grounding yang harus disalurkan ke dalam tanah yang diukur dengan resitansi sebesar 5 Ohms atau kurang dari itu. Direkomendasikan bahwa anda melakukan test ke sebuah koneksi tanah dengan tester koneksi yang sesuai sebelum anda memutuskan bahwa installasi dari lighting arrestor berhasil dengan baik. Buat sebuah point,sejalan dengan tugas pemeliharaan secara periodik, untuk mengecek resistansi dari tanah dan tube gas buangan secara teratur.

5.11 RF Splitter

RF Splitter adalah perlatan yang mempunyai konektor single input dan konektor multipel output. RF splitter digunakan untuk tujuan membagi sinyal single menjadi sinyal RF multiple independent. Kegunaan dari RF splitter dalam keseharian dari implementasi wireless-LAN tidak direkomendasikan. Kadangkala 2 120 derajat panel antenna atau 2 90 derajat panel antenna mungkin akan di kombinasikan dengan sebuah splitter dan kabel yang cukup panjang ketika antenna berada pada posisi yang berlawanan. Konfigurasi ini akan memproduksi bi-directional coverage area , maka akan sangat ideal untuk menutupi area sepanjang sungai atau jalan raya. Back-to-back 90 derajat panel mungkin akan dipisahkan sebesar 10 inches atau sebanyak 40 inches

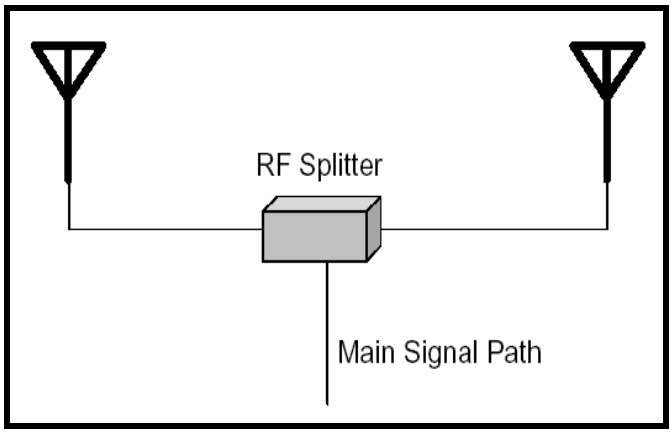
pada tiap sisi dari tiang atau towernya.Tiap panel dari konfigurasi mempunyai mechanical down tilt.Resultan gain dari tiap radiasi utama yang di kurangi dengan 3-4 dB dalam konfigurasi ini.

Ketika menginstall RF splitter, konektor input harus selalu berada di atas permukaaan dari sinyal RF. Output konektor disebut ”taps”, di hubungkan ke tujuan dari sinyal RF(antenna) . Gambar 5.29 menunjukkan 2 contoh dari RF splitter. Gambar 2.30 mengilustrasikan bagaimana RF splitter dapat di gunakan dalam instalasi wireless-LAN.

Splitter dapat digunakan untuk menyimpan track dari power output dalam link wireless-LAN. Dengan menyertakan power meter ke salah satu output dari splitter dan RF antenna pada salah satu sisinya, maka seorang administrator dapat memoinitor secara aktif output setiap saat. Dalam skenario ini, power meter, antenna dan splitter harus mempunyai impedansi yang sama..Meskipun bukan praktek yang biasanya, memindahkan power meter dari satu output splitter dan menggantikannya dengan 50 Ohm beban yang tidak penting, yang akan mengijinkan administrator untuk memindahkan power meter dari satu conecction point ke yang lainnya melalui wireless-LAN sementara juga memebuat pengukuran power output.

Power splitter , peralatan yang belum dapat digunakan sebagai bagina dari wireless-LAN. Tetaplah ingat bahwasanya splitter HARUS merupakan bagian dar sistem yang bersertifikasi jika ingin digunakan dalam wireless-LAN anda.

Gambar 5.25 Contoh RF Splitter



Gambar 5.26 Installasi RF Splitter Dalam Jaringan

5.11.1 Memilih RF Splitter

Di bawah ini, terdapat beberapa hal yang harus dipertimbangkan ketika memilih sebuah RF Spiltter :

- Insertion loss
- Respon frekuensi
- Impedansi
- VSWR Rating
- High isolation Impedansi
- Power Ratings
- Tipe konektor
- Report Kalibrasi
- Mounting
- DC voltage passing

5.11.1.1 Insertion loss

Insertion loss yang rendah (loss yang didatangkan hanya dengan mengenalkan item ke dalam sirkuit) adalh penting karena secara sederhana meletakkan splitter dalam RF sirkuit yang dapat menyebabkan penurunan amplitudo sinyal RF secara berarti. Insertion loss dari 0.5 dB

5.11.1.2 Respon Frekuensi

Spesifkasi respon frekunsi dari splitter setidaknya setinggi dari frekuensi yang digunakan dalam wireless-LAN anda. Sebagai contoh,, jika anda menggunakan hanya dengan 2.4 GHz wireless-LAN , sebuah splitter dimana di spesifikasikan untuk digunakan di atas 3 GHz akan jauh lebih baik.

5.11.1.3 Impedansi

Impedansi dari splitter , dimana biasanya 50 Ohms dalam kebanyakan wireless-LAN, seharusnya cocok dengan semua peralatan di dalam sirkuit di antara transmitter dan antenna.

5.11.1.4 VSWR Rating

Sebagaimana peralatan RF lainnya, VSWR rating seharusnya mendekati 1:1. Tipe dari VSWR rating pada RF splitter adalah < 1.5:1. VSWR rating yang rendah pada splitter akan jauh lebih kritis daripada peralatan lainnya pada RF sistem karena refleksi power RF pada splitter akan di refleksikan dalam berbagai arah di dalam splitter, mempengaruhi sinyal input splitter dan seluruh sinyal output splitter.

5.11.1.5 High Isolation Impedansi

High isolation impedansi antara port pada RF splitter sangatlah penting untuk beberapa alasan. Pertama, beban pada salah satu port output seharusnya tidak mempengaruhi power output pada port output splitter lainnya. Yang kedua,, sinyal yang datang ke port output dari splitter seharusnya di arahkan ke port input daripada ke port output lainnya. Persyaratan ini di selesaikan melalui impedansi yang tinggi antara output konektor. Typical isolation adalah sebesar 20dB atau lebih di antara portnya.

5.11.1.6 Power Rating

Splitter yang di rata-rata untuk maksimum power input, dimana yang berarti bahwasanya anda di ijinkan dalam sejumlah power yang anda dapat

kerjakan ke dalam splitter anda. Pelebihan perusahaan dalam hal power rating akan menghasilkan kerusakan pada RF splitter.

5.11.1.7 Tipe Konektor

Secara umum, RF splitter mempunyai konektor N-type dan SMA. Ini sangat pentign untuk membeli sebuah splitter dengan tipe konektor yang sama dengan kabel yang kita gunakan. Melakukan pemotongan pada adapter konektor , akan mengurangi sinyal amplitudo RF. Pengetahuan ini, sangatlah penting ketika menggunaksan splitter yang sudah terpotong sinyal amplitudonya dalam sistem RF.

5.11.1.8 Report Kalibrasi

Semua RF splitter harusnya dengan report kalibrasi yang menunjukkan adanya insertion loss, respon frekuensi, melalui loss pada tiap konektor , dll. Mempunyai splitter yang telah di kalibrasi sekali dalam setahun adalah tidak mudah dikerjakan maka akan sangat penting bahwa administrator mengetahui sebelum instalasi awal apakah splitter sesuai dengan spesifikasi perusahaannya atau tidak. Kalibrasi yang berlanjut membutuhkan wireless-LAN yang off-line untuk perode waktu yang lama, dan mungkin tidak praktis dalam beberapa situasi.

5.11.1.9 Mounting

Mounting sebuah RF splitter biasanya sebuah masalah dalam meletakkan sekrup melalui piringan ke dalam permukaan apapun , dimana anda ingin splitter tersebut di-mounted. Beberapa model dengan hardware pole-mounting menggunakan baut ”U”, piringan mounting dan ukuran standar dari mur. Berdasarkan pada perusahaannya, splitter seharusnya tahan terhadap air, ini berarti dapat saja di lakukan mounting di luar dari pole tanpa takut akan air, dimana hal ini akan menyebabkan permasalahan. Ketika ini merupakan suatu permasalahan, yakinlah untuk menyegel koneksi kabelnya dan gunakan simpulan drip.

5.11.1.10 DC Voltage Passing

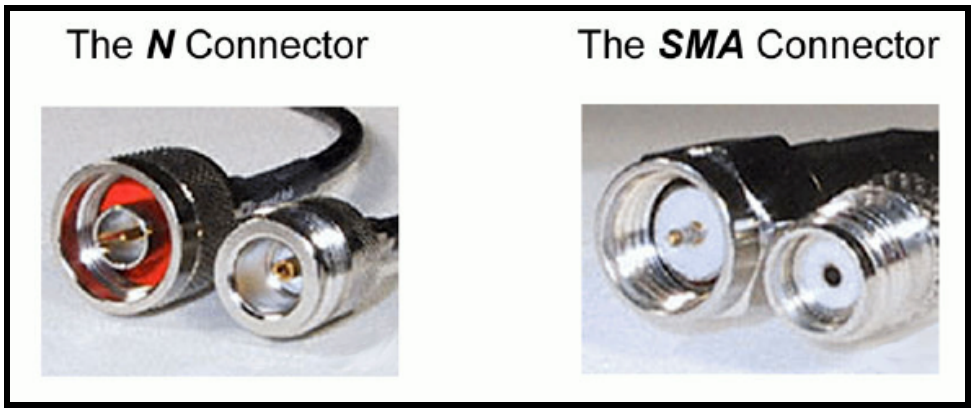
Beberapa RF splitter mempunyai pilihan untuk melewati tegangan DC yang di syaratkan untuk semua port output secara paralel. Ciri ini sangat membantu ketika terdapat RF amplifier, dimana power internal sirkuitnya dengan tegangan DC dari injektor tegangan DC dalam wiring-closet, dilokasikan pada output di tiap port splitternya

5.12 RF Connectors

RF connector adalah tipe spesifik dari peralatan koneksi yang digunakan untuk menghubungkan kabel ke peralatan atau peralatan ke peralatan. Secara tradisional,konektor N, F, SMA, BNC, & TNC (atau turunannya) telah digunakn pada wireless-Lan.

Pada taun 1994, FCC dan DOC (sekarang Industry Canada) memberi aturan bahwa konektor yang digunakan dengan peralatan wireless-LAN seharusnya disesuaikan di antara beberapa perusahaan. Untuk alasan ini, berbagai macam tipe konektor yang muncul , seperti :

- N-type
- Reverse polarity N-type
- Reverse threaded N-type



Gambar 5.27. Contoh Konektor Tipe N dan SMA

5.12.1 Memilih RF Connector

Ada 5 hal yang harus dipertimbangkan ketika membeli dan meng-install konektor RF, dan mereka adalah sama dalam kriteria untuk memilih RF amplifier dan attenuator.

1. RF connector harusnya sesuai dengan impedansi dengan semua komponen wireless-LAN (biasanya 50 Ohms). Ini bukannya suatu permasalahan sejak ketika anda membeli konektor dengan impedansi yang berbeda, mereka tidak akan cocok jika bersama-sama karena ukuran dari pin-center-nya.
2. Kenali seberapa banyak insertion loss dari tiap konektor yang di sisipkan ke dalam path sinyal. Jumlah dari loss akan menyebabkan faktor ke dalam kalkulasi dari kekuatan sinyal yang anda inginkan dan juga jarak yang dibolehkan.
3. Kenali kenaikan batas frekuensi (respon frekuensi) yang di spesifikasikan untuk tiap konektor. Point ini akan sangat penting sebesar 5GHz wirelessLan menjadi lebih dan lebih. Beberapa konektor yang di hitung hanya sebesar 3 GHz, dimana ini baik di gunakan dengan 2.4 GHz wirelessLan, tapi akan tidak berjalan dengan baikuntuk 5GHz wirelessLan. Beberapa konektor yang di hitung hanya diatas 1 GHz dan akan sama sekali tidak berjalan dengan baik dengan wirelessLan, yang di legalkan hanya 900MHz wirelessLan.
4. Hati-hati dengan kualitas konektor yang buruk. Pertama, selalu pertimabngkan dari perusahaan yang bereputasi. Kedua,, belilah hanya konektor dengan kualitas tinggi yang dibuat oleh perusahaan yang terkenal. Bagian dari pembelian ini akan membantu anda untuk mengurangi permasalahan dengan sinyal RF yang sporadik, VSWR dan koneksi yang buruk.
5. Yakinlah bahwa anda mengetahui tipe dari konektor(N,F,SMA,dll) yang anda butuhkan dan jenis kelamin dari konektor itu sendiri. Konektor mempunyai 2 jenis kelamin, yaitu male dan female. Konektor male mempunyai pin center, sedangkan konektor female mempunyai receptable center.

5.13 RF Cables

Pada beberapa cara yang sama yang harus anda pilih, kabel yang sesuai untuk infrastrukture backbone wired 10Gbps, anda harus memilih kabel yang sesuai untuk menghubungkan antenna ke access-point atau wireless-bridge. Dibawah ini ada beberapa kriteria yang harus di pertimbangkan dalam memilih kabel yang cocok untuk jaringan wireless anda.

- Kabel mengenalkan loss ke dalam wirelessLAN, jadi yakinlah panjang pendek kabel sangat dibutuhkan
- Rencanakan untuk membeli kabel yang pre-cut length dengan konektor pre-installed. Meminimalkan kemungkinan terburuk antara konektor dan kabel. Perusahaan yang profesioanl mempraktekkan bahwa hampir selalu superior untuk kabel manufactured oleh individual yang tidak terlatih.
- Carilah kabel lowest loss yang tersedia pada keterangan range harga. **Tabel 5.3** mengilustrasikan loss yang dikenali dengan menambahkan kabel pada wirelessLAN.
- Belilah kabel yang mempunyai impedansi yang sama dengan semua komponen wireless LAN anda.
- Respon frekuensi dari kabel , seharusnya di pertimbangkan sebagai factor pengambilan keputusan yang sangat utama dalam pembelian. Dengan 2.4 GHz wirelessLAN, kabel yang di hitung setidaknya 2.5 GHz. . Dengan 5 GHz wirelessLAN, kabel yang di hitung setidaknya 6 GHz.
- Satu hal yang diperlukan untuk pemanjangankabel ketika access-pint dan remote antenna jauh terpisah (seperti instalasi outdoor). Pada kasus ini, berhati-hatilah bahwa konektor dapat drop ~0.25dB dan kabel dapat loss secara berarti. Penggunaan kabel Cat5 secara lama, kadang dapat mengualng situasi dengan mengijinkan access-point dipindah mendekati antenna. Kabel RG-58 harusnya tidak pernah dipakai untuk perpanjangan kabel yang berkaitan dengan respon frekuensi yang buruk. LMR, Heliax, atau kabel high-frekuensi lainnya seharusnya diguankan untuk perluasan.

Jika FCC mengeluarkan perintah pada wirelessLAN anda (dimana, mereka menginginkan untuk melakukannya setiap saat) , mereka akan mengambil catan tentang

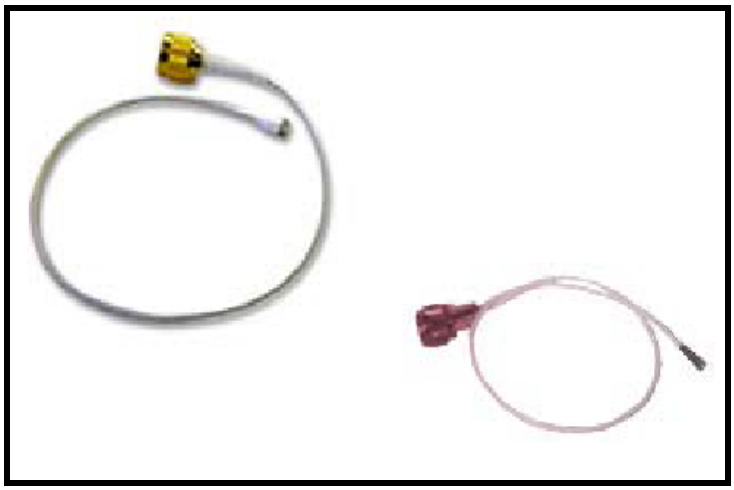
perusahaan, nomor model,panjang dan tipe dari konektor pada kabel RF anda. Bagian dari informasi ini, seharusnya di dokumentasikan dalam sistem FCC anda.

Tabel 5.3.. Coaxial cable attenuation ratings (dalam dB/foot pada X MHz)

LMR CABLE	30	50	150	220	450	900	1500	1800	2000	2500
100A	3.9	5.1	8.9	10.9	15.8	22.8	30.1	33.2	35.2	39.8
195	2.0	2.6	4.4	5.4	7.8	11.1	14.5	16.0	16.9	19.0
200	1.8	2.3	4.0	4.8	7.0	9.9	12.9	14.2	15.0	16.9
240	1.3	1.7	3.0	3.7	5.3	7.6	9.9	10.9	11.5	12.9
300	1.1	1.4	2.4	2.9	4.2	6.1	7.9	8.7	9.2	10.4
400	0.7	0.9	1.5	1.9	2.7	3.9	5.1	5.7	6.0	6.8
400UF	0.8	1.1	1.7	2.2	3.1	4.5	5.9	6.6	6.9	7.8
500	0.54	.70	1.2	1.5	2.2	3.1	4.1	4.6	4.8	5.5
600	0.42	.55	1.0	1.2	1.7	2.5	3.3	3.7	3.9	4.4
600UF	0.48	.63	1.15	1.4	2.0	2.9	3.8	4.3	4.5	5.1
900	0.29	0.37	0.66	0.80	1.17	1.70	2.24	2.48	2.63	2.98
1200	0.21	0.27	0.48	0.59	0.89	1.3	1.7	1.9	2.0	2.3
1700	0.15	0.19	0.35	0.43	0.63	0.94	1.3	1.4	1.5	1.7

5.13.1 5.13.1 RF ”Pigtail” Adapter Cable

Kabel Pigtail adapter di gunakan untuk menghubungkan kabel yang mempunyai konektor standar-industri ke peralatan wirelessLAN. Pigtail di gunakan untuk adaptasi konektor pemilik ke konektor standar industri seperti N-tipe dan konektor SMA.Akhir dari kabel pigtail adalah konektor pemilik , sementara akhir lainnya berada pada konektor standar industri.



Gambar 5.28 Contoh RF Pigtail Adapter

Peraturan DOC dan FCC (United States Federal Communications Commission) pada 23 Juni 1994, menyatakan bahwa konektor yang di buat setelah 23 June 1994, harus di buat sesuai konektor antenna pemilik. Aturan tahun 1994 akan mengecilkan penggunaan amplifier, antenna high-gain atau sarana lainnya dalam menaikkan radias RF secara berarti. Aturan ini akan mengecilkan untuk sistem ”home brew” dimana di lakukan instalasi oleh user yang kurang pengalaman dan tidak menuruti aturan FCC dalam penggunaan ISM band.

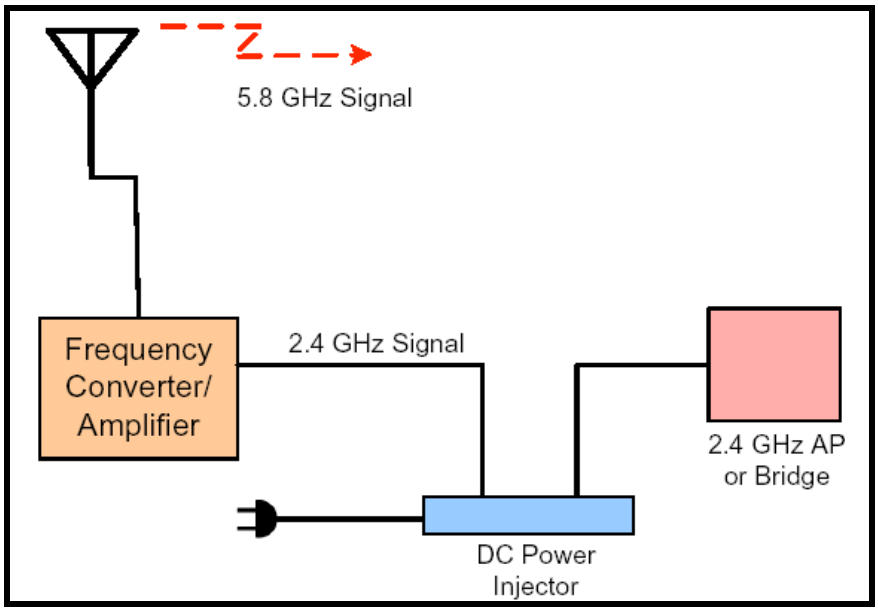
Sejak aturan itu di buat, konsumer harus menaati konektor pemilik dari pengusaha pabrik untuk menghubungkan konektor standar industri. Ulang tahun ketiga pengusaha telah memulai kebiasaan dalam membaut kabel adapter (disebut pigtail) dan menjualnya murah di pasaran. Tetapi tetaplah ingat, bahwasanya FCC CFR 15.204 tidak mengijinkan sistem ”home brew”sama sekali. Semua sistem haruslah bersertifikasi, dan sistem di definisikan sebagai sebuah radiator intentional, an antenna dan semuanya yang berada di antaranya. Individu ini menggunakan security seperti Netstumber dengan Pringles can antenna adalah pelanggran dalam aturan FCC. Ini telah di sebutkan untuk menjawab pertanyaan yang selalu sama dan sebagai contoh dari bagaimana pertaturan di tejemahkan oleh FCC. Pigtail atau antenna yang di gunakan dengan wireless LAN di ISM atau UNII bands harus menjadi bagian dari sistem yang tersertifikasi dan terdokumentasi oleh FCC.

5.14 Frequency Converter

Frekuensi converter digunakan untuk menkonversi 1 range frekuensi ke lainnya untuk tujuan menghilangkan frekuensi bands. Kira-kira banyak perusahaan yang di lokasikan pada multi-tenant office building mempunyai wirelss LAN. Tiap dari perusahaan tersebut menginginkan konektivitas wireless building-to-building dengan buildingnext door karena tiap perusahaan mempunyai kantor di dalam gedung yang berdekatan. Ini sangat mudah untuk melihat hanya ada 3 perusahaan yang akan menggunakan wirelss LAN building-to-building bridging berkaitan dengan nomor yang terbatas dari non-overlapping channels. Dalam kasus ini, frekunesi konverter diterapkan bahwa akan menggunakan peralatan 2.4 GHz, tapi akan mengkonversi frekuensi tersebut ke band yang padat (seperti 5.8 GHz diatas UNII band) untuk segmen wireless bridge.

Gambar 5.29 Contoh Frekuensi Konverter.

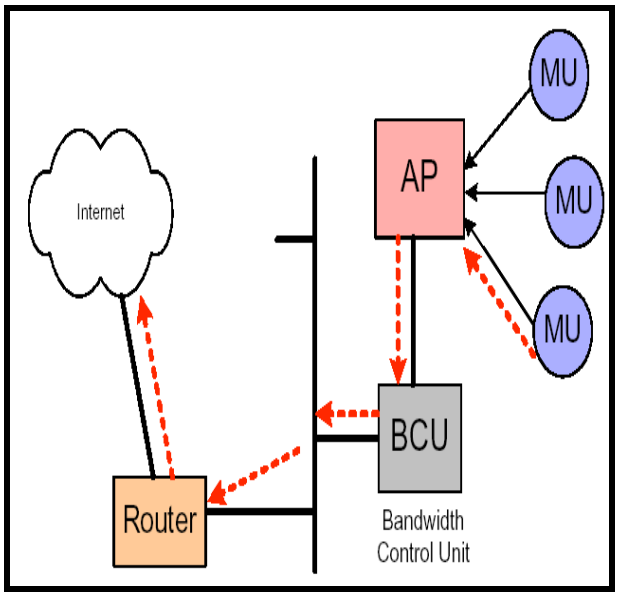
Antenna dan kabel harus di gunakan ketika menggunakan frekuensi konverter berkaitan dengan antenna dan kabel yang mempunyai respon frekuensi yang terbatas, tapi itu akan merupakan alasan ekonomi pada area yang padat. Alternatif yang dapat menggantikan semua hardware wireless LAN dengan hardware 5 GHz yang baru. **Gambar 5.30** menggambarkan bagaimana frekuensi konverter di install ke dalam konfigurasi wireless LAN.



Gambar 5.30. Penggunaan Frekuensi Konverter

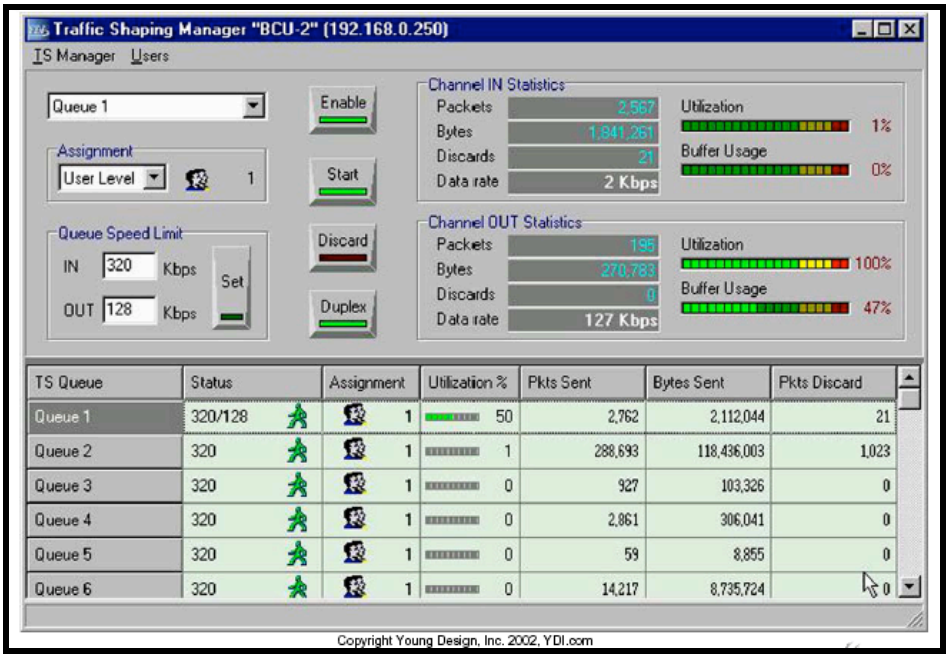
5.15 Bandwidth Control Units

Wireless LAN adalah medium shared dengan throughput yang low jika di bandingkan dengan teknologi wireless yang sekarang. Untuk alas an ni, bandwidth pada wireless harus di konservasi dan di lindungi, terutama pada lingkungan luar seperti yang kita temukan pada Wireless Internet Service Provider (WISPs) bandwidth harusnya di control dalam berbagai cara yang mana tiap user mempunyai kepercayaan dan pengalaman konektivitas yang konsisten dan mendapatkan sesuai dengan apa yang mereka bayarkan. Dengan instalasi wireless LAN indoor , maka ini bukan sesuatu yang biasa untuk menggunakan Bandwidth Control Units (BCU) karena banyak user yang menginginkan untuk mempunyai pengalaman yang sama sebagaimana yang mereka dapat pada wired LAN. Sesederhana ini , tidak mugkin di kerjakan dengan mudah berdasarkan perbedaan bandwidth yang ekstrim. Tapi, bagaimanapun juga administrator berusaha untuk memberikan indoor LAN kepada user sebanyak bandwidth dengan tidak melebihi beban dari access-point. Dalam wireless LAN, BCU diletakkan antara access-point atau bridge dan jaringan, sebagaimana **gambar 5.31**



Gambar 5.31 Using a bandwidth control unit

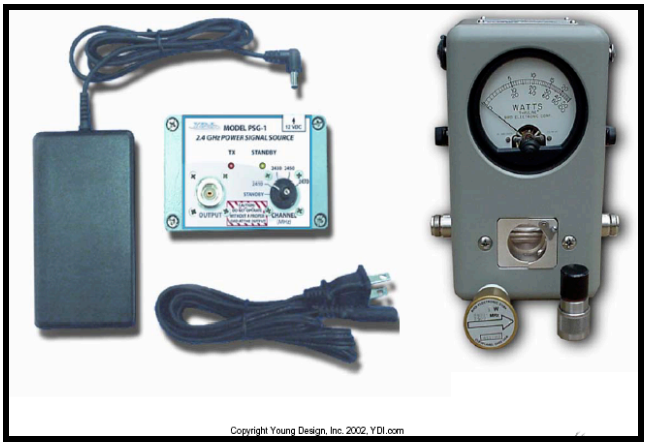
Tipe BCU bekerja dengan mem-filter pada MAC address supaya untuk men-drop tiap user ke dalam antrian pre-assigned. Tiap antrian mempunyai keterangan properties seperti bandwidth upstream dan dowmstream. Multiple user mungkin akan di masukkan ke dalam satu antrian yang sama. Ini mengijinkan untuk control bandwidth secara presisi dan menghitung per user. BCU di kelola melalui berbagai software packages, seperti yang ada pada bawah ini...



Gambar 5.32 Aplikasi manager untuk BCU

5.16 Test Kits

Ada beberapa macam test kits yang beredar di pasaran. Salah satu yang sangat berharga dari tipe test kits pada industry wireless LAN adalah yang digunakan untuk mengetes kabel dan konektor. Kit terdiri dari sinyal RF generator dan through-line power meter. Sinyal generator yang di belokkan secara langsung ke power meter untuk mendapatkan pengukuran baseline. Ketika meletakkan kabel dan konektor di antara sinyal generator dan power meter , ini dapat di tentukan jika merek sesuia dengan spesifikasi perusahaan dan jika mereka intermittent. Konektor pada kabel dapat menjadi usang dan loose membuat sesuatu menjadi buruk atau koneksi intermittent yang buruk. Mereka juga akan mengambil tes di air, dimana tingkat kerusakan dari karakteristik RF. Ini sangat penting untuk mengetes kabel dan konektor sebelum di sebarkan.



Gambar 5.33 Contoh dari tes kit

5.17 Kesimpulan

Antenna adalah yang sering digunakan untuk meningkatkan jangkauan dari system wireless LAN. Pilihan antenna yang tepat dan posisi antenna dapat mengurangi kebocoran sinyal dari batasan anda, dan membuat pemotongan sinyal amat sulit. Ada 3 kategori umum yang membagi antenna wireless LAN : omni directional, semi-

directional, dan highly-directional. Kami akan membahas attribute dari tiap kedalaman group ini, sebagaimana metode yang tepat untuk meng-install tiap jenis antenna. Kami juga akan menjelaskan polarisasi, pengumpulan pola, penggunaan yang tepat, dan mengalamatkan item yang begitu banyak berbeda yang digunakan untuk mengkoneksikan antenna ke hardware wireless LAN lain. Dalam komunikasi Wireless aksesori jaringan yang digunakan meliputi Amplifiers RF, RF attenuators, Lightning arretors, Konektor RF, Kabel RF, Pemisah Rfdan Pigtails.

5.18 SOAL

1. Sebutkan tiga kategori umum dari perangkat Antenna Wireless LAN ?
2. Jelaskan pengertian mengenai antenna *Omni Directional* beserta gambar ?
3. Hal – hal apa saja yang perlu diperhatikan dalam pemilihan RF Splitter ?
4. Hal – hal apa saja yang perlu diperhatikan dalam pemilihan RF Connector ?
5. Apakah kegunaan dari Frequency Converter ?

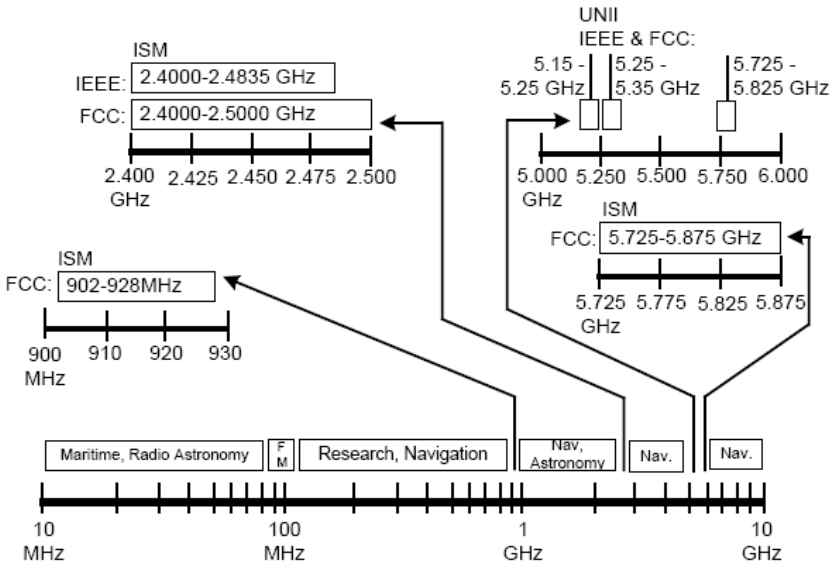
Bab 6. Organisasi Wireless LAN Standart

6.1 FCC (Federal Communications Commisions)

Federal Communications Commission (FCC) adalah agen pemerintah US yang langsung bertanggung jawab pada konggres. FCC didirikan oleh Communication Act pada tahun 1934, yang mengatur komunikasi menggunakan radio, televisi, kawat, satelit dan kabel. Aturan FCC meliputi tidak hanya 50 negara bagian dan District of Columbia tetapi juga Puerto Rico, Guam dan Kepuluan Virgin.

6.2 6ISM dan UNII Band

FCC membuat batasan peraturan dimana frekuensi wireless LAN dapat menggunakan output power untuk masing-masing frekuensi band. FCC telah membagi bahwa untuk wireless yang digunakan oleh Industrial, Scientific dan Medical (ISM) menggunakan license free. Band ISM terletak pada lokasi mulai 902 MHz, 2,4 MHz dan 5,8 GHz dan bermacam-macam lebarnya dari 26MHz sampai 150 MHz.



Gambar 6.1. Perbandingan ISM dan UNII Band

6.3 Keuntungan dan Kerugian Band License-Free

Ketika mengimplementasikan beberapa sistem wireless pada band license-free maka tidak ada persyaratan ketentuan tentang bandwidth dan power dari FCC. Batasan

transmisi power ada tapi tidak ada prosedur untuk harus menerima ijin untuk mentransmit pada power tertentu

Seperti kebebasan dari membawa license tetapi juga ada faktor kerugiannya yaitu semua orang juga mempunyai hak yang sama dalam menggunakan frekuensi sehingga akan menyebabkan interferensi. Cara mengatasinya, dua sistem yang bersaing tidak perlu menggunakan channel yang sama atau bahkan tidak menggunakan spread spectrum yang sama.

6.4 Industrial Scientific Medical (ISM) Band

Ada 3 license-free ISM band FCC telah menetapkan bahwa wireless LAN boleh digunakan. Mereka adalah 900 MHz, 2,4 GHz dan 5,8 GHz.

6.4.1 900 MHz ISM Band

Band 900 MGz didefinisikan sebagai range frekuensi dari 902 HGz sampai 928 MHz. Dalam band ini sebagai tambahan didefinisikan sebagai 915 MHz +- 13 MHz.

.

6.4.2 2,4 GHz Band

Band ini digunakan oleh semua 802.11, 802.11b dan compliant 802.11g. Band 2.4 GHz dibatasi oleh 2,4GHz dan 2.5 GHz seperti yang didefinisikan oleh FCC.

6.4.3 5,8 GHz Band

Band ini juga disebut 5 GHz ISM band dan dibatasi oleh 5.725 dan 5.875. Frekuensi band ini tidak banyak digunakan oleh peralatan wireless LAN sehingga cenderung menimbulkan kebingungan. Band ini juga overlap dengan bagian dari license-free yang lain.

6.5 6Unilicensed National Information Infrastructure (UNII) Band

5 GHz UNII band terbuat dari 3 bagian yang terpisah 100 MHz lebarnya. Ketiga bagian itu disebut lower, middle dan upper band. Dalam masing-masing ketiga band ini

ada 4 non-overlapping channel OFDM yang masing-masing dipisahkan oleh 5 MHz.. Karena access point kebanyakan digunakan di indoors, band ini akan memperbolehkan 8 non-overlapping access point menggunakan kedua lower dan middle UNII band.

6.5.1 Lower Band

Lower band dibatasi oleh 5.15 GHz dan 5.25 GHz dan ditentukan oleh FCC untuk mempunyai maximum output power 50 mW. Ketika diimplementasikan 802.11a compliant devices, the IEEE telah menyebutkan bahwa maximum output hanya 40mW (80%).

6.5.2 Middle Band

Middle band dibatasi oleh 5.25 GHz dan 5.35 GHz dan ditentukan pada 250mW output oleh FCC. Power output telah disebutkan oleh IEEE untuk middle UNII band adalah 200 mW.

6.5.3 Upper Band

Upper band digunakan untuk link outdoor dan dibatasi oleh FCC sampai 1 watt sebagai ouput power.

6.6 Aturan Output Power

FCC melaksanakan peraturan tertentu berdasarkan radiasi power oleh elemen antenna tergantung pada apakah implementasinya adalah point-to-multipoint atau point-to-point. Istilah yang digunakan untuk power yang diradiasikan oleh anten adalah *Equivalent Isotropically Radiated Power* (EIRP).

6.6.1 Point-to-Multipoint (PtMP)

Link PtMP mempunyai central point koneksi dan dua atau lebih non-central koneksi. Link PtMP dasarnya dikonfigurasikan sebagai topologi star. Koneksi central bisa menggunakan antenna omnidireksional. Berdasarkan susunan dari link PtMP, FCC membatasi EIRP sampai 4 Watts baik untuk 2.4 GHz ISM band dan upper 5 GHz UNII band.

Tabel 6.1 Point-to-Multi Point Power Limit

Power at Antenna (dBm)	Antenna Gain (dBi)	EIRP (dBm)	EIRP (watts)
30	6	36	4
27	9	36	4
24	12	36	4
21	15	36	4
18	18	36	4
15	21	36	4
12	24	36	4

6.6.2 Point-to-Point (PtP)

Link PtP termasuk single directional transmitting antenna dan single directional receiving antenna. Koneksi ini biasanya digunakan untuk building-to-building atau link yang mirip dan harus ada oleh peraturan yang khusus.

Tabel 6.2 Point-to-Point Power Limit

Power at Antenna (dBm)	Max Antenna Gain (dBi)	EIRP (dBm)	EIRP (watts)
30	6	36	4
29	9	38	6.3
28	12	40	10
27	15	42	16
26	18	44	25
25	21	46	39.8
24	24	48	63
23	27	50	100
22	30	52	158

Informasi yang spesifik yang terdapat di **Tabel 6.2** tidaklah dicakup di ujian CWNA. Informasi disajikan sebagai sumber daya untuk tugas yang administratif. Fcc mempunyai suatu aturan yang berbeda untuk PtP hubungkan di UNII band yang bagian atas. Alat UNII Point-To-Point yang yang ditetapkan yang beroperasi dalam 5.725 - 5.825 regu GHz boleh mempekerjakan antenna pemancar dengan keuntungan yang directional sampai ke 23 dBi tanpa bersesuaian pengurangan di daya keluaran puncak pemancar. Untuk ditetapkan, pemancar UNII point-to-point yang mempekerjakan suatu antenna terarah memperoleh lebih besar dari 23 dBi, suatu 1 pengurangan dB di pemancar puncak

menggerakkan untuk masing-masing 1 dBi dari antenna lebih dari 23 dBi diperlukan. Berpesan bahwa oleh mempunyai;nikmati suatu daya keluaran yang maksimum dari + 30 dBm di radiator yang disengaja, dan mempunyai maksimum 23 bati antenna dBi di depan pengurangan apapun di daya keluaran pemancar diperlukan, ini mengijinkan ini 5 sistem GHz UNII untuk mempunyai suatu keluaran dari 200 Watts EIRP.

6.7 Institute of Electrical and Electronics Engineers

Institute of Electrical and Electronics Engineers (IEEE) adalah pembuat kunci yang baku untuk kebanyakan berbagai hal berhubungan dengan teknologi informasi di Amerika Serikat. IEEE menciptakan standard nya di dalam hukum yang diciptakan oleh FCC. Pokok-Pokok IEEE banyak teknologi baku seperti Public Key Cryptography (IEEE 1363), Firewire (IEEE 1394), Ethernet (IEEE 802.3), dan Wireless Lan (IEEE 802.11).

Itu menjadi bagian dari misi dari IEEE untuk dikembangkan standard untuk operasi LAN wireless di dalam kerangka dari peraturan dan aturan FCC itu. Berikut adalah empat standard IEEE yang utama untuk Lan wireless yang adalah salah satu digunakan atau di format draft

- 802.11
- 802.11b
- 802.11a
- 802.11g

6.7.1 IEEE 802.11

Standard 802.11 adalah standard yang pertama gambarkan pengoperasian Wireless LAN. Standard ini yang dimasukkan semua teknologi transmisi yang yang tersedia yang mencakup Direct Sequence Spread Spectrum (DSSS), Hopping Spread Spectrum frekwensi (FHSS), dan inframerah.

Penguasaan pasar LAN yang inframerah wireless adalah sungguh kecil dan teknologi adalah sangat dibatasi dengan kemampuannya. Dalam kaitan dengan ketiadaan ketenaran dari inframerah teknologi di pasar LAN wireless, IR akan tersebut, tetapi tidak tercakup secara detil dalam buku ini.

Standard IEEE 802.11 menguraikan sistem DSSS yang beroperasi pada 1 Mbps dan 2 Mbps saja. Jika suatu sistem DSSS beroperasi pada daftar biaya pengiriman barang-barang data yang lain juga, seperti 1 Mbps, 2 Mbps, dan 11 Mbps, kemudian dapat tetap suatu sistem 802.11-compliant. Jika, bagaimanapun, sistem sedang beroperasi bagaimanapun juga selain dari 1 atau 2 Mbps, kemudian sistem adalah 802.11-compliant oleh karena kemampuannya mempekerjakan pada 1 & 2 Mbps. Itu bukanlah yang beroperasi dalam suatu gaya 802.11-compliant dan tidak bisa diharapkan untuk berkomunikasi dengan alat 802.11-compliant yang lain.

IEEE 802.11 adalah salah satu dari dua standard yang menguraikan pengoperasian frekwensi yang meloncat sistem LAN wireless. Jika suatu pengurus LAN wireless menghadapi suatu frekwensi yang meloncat sistem, kemudian kemungkinan untuk salah satu suatu sistem atau 802.11-compliant OpenAir yang memenuhi (yang dibahas di bawah). Standart 802.11 menguraikan penggunaan dari sistem FHSS pada 1 dan 2 Mbps. Ada sistem FHSS banyak orang di pasar yang meluas kemampuan ini dengan menawarkan gaya kepemilikan yang beroperasi pada 3-10 Mbps, hanya sebagai dari DSSS, jika sistem sedang beroperasi pada kecepatan selain dari aku & 2 Mbps, itu tidak bisa diharapkan untuk secara otomatis berkomunikasi dengan alat 802.11-compliant yang lain.

802.11 produk memenuhi beroperasi dengan keras di 2.4 regu GHz ISM antara 2.4000 dan 2.4835 GHz. Inframerah, juga yang dicakup oleh 802.11, adalah light-based technology dan tidak jatuh masuk ke 2.4 regu GHz ISM.

6.7.2 IEEE 802.11b

Meskipun demikian, standard 802.11 adalah sukses dalam membiarkan DSSS seperti halnya sistem FHSS ke interoperate, teknologi telah membesar standard. Segera setelah implementasi dan persetujuan dari 802.11, Lan DSSS wireless sedang menukarkan data pada sampai ke 11 Mbps. Tetapi, standard terus-menerus, dengan tak ada hentinya untuk memandu pengoperasian alat seperti itu, disana menjadi permasalahan meskipun demikian standard 802.11 adalah sukses dalam membiarkan DSSS seperti halnya sistem FHSS ke interoperate, teknologi telah membesar standard. Segera setelah implementasi dan persetujuan dari 802.11, Lan DSSS wireless sedang menukarkan data pada sampai ke 11 Mbps.

Tetapi, standard terus-menerus: dengan tak ada hentinya untuk memandu pengoperasian alat seperti itu, disana menjadi permasalahan.

IEEE 802.11b, dikenal sebagai " High-Rate" dan Wi-Fi, specifies direct sequencing (DSSS) sistem yang beroperasi pada 1, 2, 5.5 dan 11 Mbps. 802.1 standard lb tidak menguraikan sistem FHSS yang manapun, dan 802.11b-compliant alat adalah juga 802.1 1-compliant dengan tak hadir, maksud mereka adalah mundur dapat dipertukarkan dan kedua-duanya dukungan 2 dan 1 data Mbps daftar biaya pengiriman barang-barang. Kecocokan yang mundur adalah sangat penting sebab itu mengijinkan suatu LAN wireless untuk diupgrade tanpa ongkos menggantikan perangkat keras inti. Ini murah menonjolkan, bersama-sama dengan data yang tinggi menilai, telah buat 802.1 perangkat keras lb-compliant yang sangat populer.

Data yang tinggi tingkat alat 802.11b-compliant adalah hasil dari menggunakan suatu teknik persandian yang berbeda. Meskipun demikian sistem masih suatu mengarahkan sistem peruntunan, cara chip adalah coded (CCK dibanding/bukannya Barker Code) bersama dengan cara informasi diatur (QPSK pada 2, 5.5, & 11 BPSK dan Mbps pada 1 Mbps) mempertimbangkan suatu lebih besar jumlah data untuk ditransfer di batasan waktu yang sama. 802.11b produk memenuhi beroperasi hanya di 2.4 GHz bands ISM antara 2.4000 dan 2.4835 GHz. persandian dan Modulasi adalah dibahas lebih lanjut di Bab 8 (MAC & Physical Layers).

6.7.3 IEEE 802.11a

Standard IEEE 802.11a menguraikan operasi alat LAN wireless di 5 GHz UNII bands. Operasi di UNII bands yang secara otomatis membuat 802.11a alat tidak cocok/bertentangan dengan semua alat yang lain mentaati yang lain 802.11 rangkaian dari standard. Alasan untuk ketidakcocokan ini adalah sederhana:: sistem yang menggunakan 5 frekwensi GHz tidak akan berkomunikasi dengan sistem yang menggunakan 2.4 frekwensi GHz.

Menggunakan UNIT bands, kebanyakan alat bisa mencapai daftar biaya pengiriman barang-barang data dari 6, 9. 12, 18, 24. 36. 48, dan 54 Mbps. Sebagian dari alat yang memanfaatkan UNII bands sudah mencapai daftar biaya pengiriman barang-barang data dari 108 Mbps dengan menggunakan teknologi

kepemilikan, seperti tingkat tarip yang menggandakan. Daftar biaya pengiriman barang-barang yang paling tinggi dari sebagian dari alat ini adalah hasil dari teknologi lebih baru tidak yang ditetapkan oleh standard 802.11a. IEEE 802.11a menetapkan daftar biaya pengiriman barang-barang data dari saja 6. 12, dan 24 Mbps. Suatu alat LAN wireless harus mendukung sedikitnya daftar biaya pengiriman barang-barang data ini di UNII bands untuk 802.11a-compliant. Tingkat tarip data yang maksimum yang ditetapkan oleh standard 802.11a adalah 54 Mbps.

6.7.4 IEEE 802.11g

802.11g menyediakan yang sama kecepatan maksimum dari 802.11a, menggabungkan dengan kecocokan mundur untuk alat 802.11b. Kecocokan yang mundur ini akan membuat Lan upgrading wireless yang sederhana dan murah. Karena teknologi 802.11g adalah baru, 802.1 alat 1g waktu itu belum yang tersedia mulai dari ini menulis.

IEEE 802.11g menetapkan operasi di 2.4 GHz ISM hand. Untuk mencapai daftar biaya pengiriman barang-barang data yang lebih tinggi menemukan di 802.11a, 802.11g alat memenuhi menggunakan Orthogonal Frequency Division Multiplexing (OFDM) teknologi modulasi. Alat ini dapat secara otomatis tombol ke modulasi QPSK untuk tujuan berkomunikasi dengan 802.11b yang lebih lambat dan 802.11 alat yang yang compatable. Dengan semua keuntungan yang nyata, penggunaan dari penuh sesak 802.11g's 2.4 GHz band bisa membuktikan untuk menjadi kerugian.

Mulai dari penulisan ini, standard 802.11g telah disetujui sebagai standard, hanyalah spesifikasi standard masih di draft membentuk. Spesifikasi akhir untuk 802.11g diharapkan di pertengahan untuk akhir-akhirnya 2002.

6.8 Major Organizations

Sedangkan FCC dan IEEE bertanggung jawab atas penjelasan standard dan hukum sebagai mereka berlaku bagi/meminta kepada Lan wireless di Amerika Serikat, ada beberapa organisasi yang lain, baik dalam U.S. dan di negara-negara yang lain, yang

berperan untuk pendidikan dan pertumbuhan di pasar LAN wireless. Di bagian ini, kita akan memperhatikan sebanyak tiga organisasi ini:

- Wireless Ethernet Compatibility Alliance (WECA)
- European Telecommunications Standards Institute (ETSI)
- Wireless LAN Association (WLANA)

6.8.1 Wireless Ethernet Compatibility Alliance

Wireless Ethernet Compatibility Alliance (WECA) mempromosikan dan menguji untuk interoperabilas LAN wireless dari alat 802.11b dan 802.11a. MISI WECA's adalah untuk menjamin interoperabilas dari Wi-Fi (IEEE 802.11) produk dan untuk mempromosikan Wi-Fi ketika standard LAN global wireless ke seberang semua segmen pasar. Sebagai suatu pengurus, anda harus memecahkan konflik antar alat LAN wireless yang diakibatkan oleh gangguan campur tangan, ketidakcocokan, atau permasalahan yang lain.

Ketika suatu produk temu persyaratan interoperabilas seperti diuraikan di acuan test WECA's, WECA mewujudkan produk adalah suatu sertifikasi dari intero0perabilas, yang mengijinkan penjual untuk gunakan logo Wi-Fi di mengiklankan dan pengemasan untuk produk yang bersertifikat. Segel Wi-Fi dari persetujuan meyakinkan pemakai akhir dari interoperabilas dengan alat LAN wireless yang juga membawa logo Wi-Fi.

Antar WECA's daftar cek interoperabilas adalah penggunaan dari kunci WEP 40-bit. Yang catat bahwa 40 dan 64-bit adalah sama hal. Suatu 40-bit "rahasia" kunci adalah concatenated dengan suatu Initialization Vector 24-bit (IV) untuk menjangkau 64-bits. Di cara yang sama, 104 dan 128-bit menyetem adalah sama. WECA tidak menetapkan interoperabilas dari kunci 128-bit; karenanya, tidak ada kecocokan diharapkan untuk diharapkan antara penjual yang mempertunjukkan segel Wi-Fi ketika menggunakan 128-bit kunci WEP. Meskipun demikian, banyak sistem 128-bit dari penjual yang berbeda adalah interoperable.

Ada banyak orang lain faktor di samping penggunaan dari kunci WEP 40-bit yang diperlukan untuk temu ukuran-ukuran WECA's, faktor meliputi dukungan dari pemecahan menjadi kepingan, gaya PSP, pemeriksaan SSID meminta dan orang yang lain. Sebagian dari topik ini akan dibahas di bab yang kemudiannya.

6.8.2 European Telecommunications Standards Institute.

European Telecommunications Standards Institute (ETSI) mencarter dengan memproduksi standard komunikasi untuk Europe dengan cara yang sama bahwa IEEE adalah untuk Amerika Serikat. Etsi yang baku telah mendirikan, HiPerLAN/2 sebagai contoh, secara langsung bersaing melawan terhadap standard yang diciptakan oleh IEEE seperti 802.11a. Telah ada banyak diskusi tentang ETSI dan IEEE mempersatukan di teknologi tertentu yang wireless, tetapi tidak ada apapun mempunyai materialized mulai dari penulisan ini. Usaha ini adalah dikenal sebagai "5UP" prakarsa untuk "5 GHz Unified Protocol". IEEE'S mencoba pada interoperabilas dengan standard ETSI's Hiper LAN/2 adalah standard 802.11h baru yang mendatang.

HIPERLAN asli ETSI's yang baku untuk Hiper LAN/1 wireless, yang digelari, daftar biaya pengiriman barang-barang yang didukung dari sampai ke 24 Mbps yang menggunakan teknologi DSSS dengan bidang kira-kira 150 kaki (45.7 meter). HiperLAN/1 menggunakan menurunkan dan UNII band pertengahan, seperti halnya HiperLAN/2, 802.11a dan standard 802.11h yang baru. Standard HiperLAN/2 yang baru mendukung daftar biaya pengiriman barang-barang dari sampai ke 54 Mbps dan penggunaan adalah semua sebanyak tiga UNII band.

Standard HIPERLAN/2 ETSI's mempunyai lapisan pemusatan yang yang dapat bertukar tempat, mendukung untuk QoS, dan mendukung DES dan 3DES encryption. Lapisan pemusatan yang didukung adalah ATM, Ethernet, PPP, Fire Wire dan 3G. Kesadaran QoS didukung meliputi 802.1p, RSVP dan DiffServ-FC.

6.8.3 Wireless LAN Association

Misi Wireless LAN Association's adalah untuk mendidik dan menaikkan kesadaran konsumen mengenai ketersediaan dan penggunaan dari Lan wireless dan untuk mempromosikan industri LAN wireless secara umum. Wireless LAN Association (WLANA) adalah suatu sumber daya yang bidang pendidikan bagi mereka yang mencari cara belajar lebih banyak tentang Lan wireless. WLANA dapat juga membantu jika anda sedang mencari suatu layanan atau produk LAN spesifik yang wireless.

WLANA mempunyai mitra banyak orang di dalam industri yang menyokong isi kepada direktori WLANA dari informasi. Itu adalah direktori ini, bersama dengan banyak kasus dan laporan resmi belajari bahwa WLANA menyediakan, itu

menawarkan anda informasi yang berharga untuk membuat keputusan tentang implementasi LAN wireless.

6.9 Competing Technologies

Ada beberapa teknologi yang bersaing dengan 802.11 keluarga dari standard. Sebagai kebutuhan bisnis dan teknologi meningkatkan, akan ada melanjut untuk standar baru diciptakan untuk mendukung pasar seperti halnya penemuan yang baru yang memandu perusahaan yang membelanjakan. Lain standard dan teknologi LAN wireless yang digunakan meliputi:

- HomeRF
- Bluetooth
- Infrared
- OpenAir

6.9.1 HomeRF

Homerf beroperasi di 2.4 frekwensi penggunaan dan GHz band yang meloncat teknologi. HomeRF alat meloncat pada sekitar 50 loncatan saban sekitar detik 5 sampai 20 kali lebih cepat dari kebanyakan alat HISS 802,11-compliant. Versi yang baru tentang HomeRF, HomeRF 2.0 gunakan yang baru "band yang lebar" frekwensi yang meloncat aturan yang disetujui oleh FCC, dan adalah yang pertama untuk melakukannya. Ini adalah kata bahwa IEEE belum diadopsi frekwensi yang band lebar/luas yang meloncat aturan ke dalam 802.11 rangkaian dari standard. Adalah mengingat bahwa aturan ini, menerapkan setelah 08/31/00, meliputi:

- Maximum of 5 MHz wide carrier frequencies
- Minimum of 15 hops in a sequence
- Maximum of 125 mW of output power

Sebab HomeRF mengijinkan suatu peningkatan di atas yang terdahulu 1 frekwensi pengangkut MHz yang lebar dan fleksibilitas dalam menerapkan kurang dari yang sebelumnya memerlukan 75 loncatan, satu kekuatan berpikir meloncat

frekwensi band yang lebar itu akan sungguh populer antar penjual dan korporasi mirip. Ini, bagaimanapun, bukanlah kasus. Sebagai menguntungkan sebagai yang hasilnya 10 tingkat tarip data Mbps adalah itu tidak menaungi kerugian dari 125 mW dari daya keluaran, penggunaan batas yang dari frekwensi band lebar yang meloncat alat kepada mendekati cakupan dari 150-300 kaki (46-92 meter). Hasil ini membatasi penggunaan dari frekwensi wideband yang meloncat alat terutama kepada lingkungan SOHO.

HomeRF unit gunakan Shared Wireless Access Protocol (SWAP) protokol, yang mana adalah suatu kombinasi dari CSMA (used in local area networks) dan TDMA (used in cellular phones) protokol. SWAP adalah suatu bastar dari 802.11 dan standard DECT dan dikembangkan oleh kelompok kerja HomeRF. HomeRF alat adalah satu-satunya alat sekarang ini di pasar yang diikuti frekwensi wideband yang meloncat aturan. HomeRF alat dipertimbangkan lebih menjamin/mengamankan dibanding 802.11 produk yang menggunakan WEP oleh karena garis vektor initialisasi 32-bit (IV) HomeRF penggunaan (berlawanan dengan IV 24-bit 802.11's). Apalagi, HomeRF telah menetapkan bagaimana IV diharapkan untuk terpilih selama encryption, sedangkan 802.11 tidak, sisa-sisa 802.11 membuka untuk serangan dalam kaitan dengan implementasi yang lemah.

Beberapa liputan yang terutama sekali menarik tentang HomeRF 2.0 adalah:

- 50 hops per second
- Uses 2.4 GHz ISM band
- Meets FCC regulations for spread spectrum technologies
- 10 Mbps data rate with fallback to 5 Mbps, 1.6 Mbps and 0.8 Mbps
- Backwards compatible with OpenAir standard
- Simultaneous host/client and peer/peer topology
- Built-in security measures against eavesdropping and denial of service
- Support for prioritized streaming media sessions and toll-quality two-way voice connections
- Enhanced roaming capabilities

6.9.2 Bluetooth

Bluetooth adalah frekwensi lain yang meloncat teknologi yang beroperasi di 2.4 GHz ISM band. Loncatan tingkat alat Bluetooth akan berbuat 1600 loncatan

per detik (sekitar 625us tinggal waktu), sehingga mempunyai dengan sangat lebih banyak ongkos exploitasi dibanding frekwensi 802.11-compliant yang meloncat sistem. Tingkat tarip loncatan yang tinggi juga memberi pembalasan teknologi yang lebih besar ke suara gaduh regu palsu yang sempit. Bluetooth sistem tidaklah dirancang untuk throughput yang tinggi, tetapi lebih untuk penggunaan yang sederhana, tenaga yang rendah, dan cakupan yang singkat (WPANS). IEEE 802.15 yang baru draft untuk WPANs meliputi spesifikasi untuk Bluetooth.

Suatu kerugian yang utama dari menggunakan teknologi Bluetooth adalah bahwa itu sepenuhnya mengganggu lain hingga 2.4 GHz jaringan. Loncatan yang tinggi tingkat Bluetooth di atas keseluruhan yang dapat dipakai 2.4 GHz band membuat isyarat Bluetooth nampak bagi semua sistem yang lain sebagai band semua suara gaduh atau semua band gangguan campur tangan. Bluetooth juga mempengaruhi sistem FHSS yang lain. All-Band gangguan campur tangan, seperti nama menyiratkan, mengganggu isyarat di atas cakupan dari frekwensi yang bisa gunakan keseluruhannya, menyumbangkan isyarat yang utama sia-sia. Gangguan campur tangan yang disajikan oleh LAN wireless bertentangan dengan Bluetooth tidak berdampak pada alat Bluetooth ketika Bluetooth berdampak pada 802.11 LAN wireless. Sekarang umum untuk plakat untuk menjulang di area LAN wireless yang dibaca "No Bluetooth" di cetakan yang menyolok.

Bluetooth alat beroperasi di tiga kelas tenaga: 1 mW, 2.5 mW, dan 100 mW. Sekarang ini ada sedikit bila ada implementasi dari Class 3 (100 mW) alat Bluetooth, sehingga data cakupan tidaklah siap tersedia bagaimanapun, Class 2 (2.5 mW) alat Bluetooth mempunyai suatu cakupan yang maksimum dari 33 kaki (10 meter). Secara alami, jika diperluas bergerak diinginkan, penggunaan dari antenna terarah adalah suatu kemungkinan pemecahan, meskipun kebanyakan alat Bluetooth adalah alat yang gesit (mobile).

6.10 Infrared Data Association (IrDA)

IrDA bukanlah suatu standard Bluetooth, HomeRF dan 802.11 rangkaian dari standard melainkan, IrDA adalah suatu organisasi. yang ditemukan pada bulan Juni dari 1993, IrDA adalah suatu organisasi dibiayai anggota piagam siapa adalah "untuk menciptakan suatu interoperable murah, low-cost, low-power, half-duplex, standard

interkoneksi data yang serial yang mendukung suatu gedung tanpa lift point-to-point model pemakai yang adalah dapat menyesuaikan diri suatu cakupan luas dari alat komputer. "Inframerah transmisi data dikenal dengan paling untuk penggunaannya di kalkulator, pencetak, beberapa yang building-to-building dan ruang di jaringan komputer dan sekarang di komputer handheld.

6.10.1 Infrared

Inframerah (IR) adalah suatu teknologi transmisi didasarkan cahaya dan tidaklah tersebar teknologi spektrum tersebar spektrum adalah semua radiasi RF penggunaan. IR alat dapat mencapai suatu data yang maksimum tingkat 4 Mbps dari dekat mencakup, hanyalah suatu teknologi didasarkan cahaya, lain sumber cahaya dapat bertentangan dengan transmisi IR. Data yang khas tingkat suatu alat IR akan berbuat 115 kbps, yang mana adalah baik untuk menukarkan data antara alat handheld. Suatu keuntungan yang penting tentang jaringan IR adalah bahwa mereka tidak bertentangan dengan tersebar jaringan RF spektrum. Karena alasan ini keduanya adalah komplementer dan kaleng dengan mudah digunakan bersama-sama.

6.10.2 Security

Keamanan dari alat IR adalah dengan tak terpisahkan sempurna untuk dua pertimbangan yang utama. yang pertama IR tidak bisa bepergian meskipun demikian dinding pada kuasa yang rendah seperti itu (2 mW maksimum) dan detik, suatu pemasang telinga atau mencincang harus secara langsung menginterupsi cahaya untuk tujuan akses keuntungan informasi ditransfer. Jaringan tunggal yang memerlukan connectivas wireless harus dijamin keamanan bermanfaat bagi dari jaringan dan. Dengan komputer dan PDAs, IR digunakan untuk connectivas point-to-point pada cakupan yang sangat pendek sehingga keamanan akan hampir tidak relevan di kejadian ini.

6.10.3 Stability

Meskipun demikian IR tidak akan menerobos dinding, itu akan memantul langit-langit dan dinding, yang membantu di networking kamar tunggal. Inframerah adalah diganggu oleh isyarat yang electromagnetis, yang mempromosikan stabilitas dari suatu sistem IR. Menyiarkan alat IR ada tersedia dan dapat menjulang di langit-langit. Suatu IR menyiarkan alat (yang mana adalah dapat disamakan kepada suatu antenna RF) akan memancarkan informasi dan pengangkut IR di segala jurusan sedemikian sehingga isyarat ini dapat diambil oleh klien IR yang dekat. Karena pertimbangan konsumsi tenaga, IR siaran adalah secara normal diterapkan di atau ke dalam rumah. Point-To-Point pemancar IR dapat digunakan keluar rumah dan mempunyai suatu cakupan yang maksimum dari sekitar 3280 kaki (1 km), tetapi cakupan ini mungkin dipendekkan oleh kehadiran dari cahaya matahari. Cahaya matahari adalah kira-kira 60% inframerah cahaya, yang sungguh melemahkan isyarat IR siaran. Di hari yang cerah ketika memindahkan data antara PDAs atau komputer laptop, dua alat mungkin telah untuk memegang semakin dekat bersama-sama untuk baiknya perpindahan data IR.

6.11 Wireless LAN Interoperability Forum (WLIF)

Standard OpenAir adalah suatu standard yang diciptakan oleh Wireless LAN Interoperability Forum, di mana sistem LAN banyak orang wireless diciptakan untuk mematuhi sebagai suatu alternatif untuk 802.11 diluar ketetapan Dua kecepatan - 800 kbps dan 1.6 Mbps diluar dan 802.11 sistem tidaklah dapat dipertukarkan dan tidak akan interoperate. Karena sekarang ini beberapa lini produk namun yang tersedia yang mematuhi standard OpenAir, adalah penting bahwa pengurus LAN wireless mengetahui bahwa OpenAir ada, bagaimanapun, OpenAir adalah dengan cepat dukungan kehilangan antar penjual dan tidak ada produksi baru dibuat itu mematuhi standard ini. Diluar adalah usaha yang pertama pada standardisasi dan interoperabilas antar Lan wireless. Diluar dipusatkan Di alat FHSS beroperasi hanya pada dua kecepatan.

6.12 Kesimpulan

Federal Communications Commission (FCC) adalah agen pemerintah US yang langsung bertanggung jawab pada konggres. FCC didirikan oleh Communication Act pada tahun 1934, yang mengatur komunikasi menggunakan radio, televisi, kawat, satelit dan kabel. FCC membuat batasan peraturan dimana frekuensi wireless LAN dapat menggunakan output power untuk masing-masing frekuensi band. FCC telah membagi bahwa untuk wireless yang digunakan oleh Industrial, Scientific dan Medical (ISM) menggunakan license free. Band ISM terletak pada lokasi mulai 902 MHz, 2,4 MHz dan 5,8 GHz dan bermacam-macam lebarnya dari 26MHz sampai 150 MHz. Seperti kebebasan dari membawa license tetapi juga ada faktor kerugiannya yaitu semua orang juga mempunyai hak yang sama dalam menggunakan frekuensi sehingga akan menyebabkan interferensi. Cara mengatasinya, dua sistem yang bersaing tidak perlu menggunakan channel yang sama atau bahkan tidak menggunakan spread spectrum yang sama.

6.13 SOAL

1. Jelaskan secara singkat mengenai FCC ?
2. Jelaskan perbedaan antara standar dari ISM dan UNII dari segi pengelompokan bandwidth ?
3. Apa yang anda ketahui tentang IEEE ?
4. Jelaskan secara singkat mengenai IrDa ?
5. Sebutkan pembagian kelas dari Bluetooth ?

Bab 7. Arsitektur Jaringan

Pada bab ini akan membahas beberapa konsep kunci yang ditemukan pada 802.11 arsitektur jaringan. Kebanyakan topiknya didefinisikan secara langsung pada standar 802.11, dan diperlukan untuk implementasi dari 802.11-compliant hardware. Pada bab ini, kita akan memeriksa proses dimana klien tersambung ke sebuah access point, syarat-syarat untuk mengatur wireless Lan, dan bagaimana manajemen power disempurnakan dalam peralatan wireless LAN untuk klien.

Tanpa suatu pemahaman yang jelas dari prinsip yang dibahas pada bab ini, akan menjadi sangat sulit sekali untuk mendesain,mengadminister,atau memperbaiki suatu wireless LAN. Bab ini membahas beberapa langkah-langkah dasar yang terpenting dari desain dan administrasi wireless LAN. Saat anda mengadministrasi wireless LAN, pemahaman dari konsep-konsep ini akan memenuhi anda untuk secara cerdik memanage kerja secara hari perhari.

7.1 Menempatkan Sebuah Wireless LAN

Saat anda meng-install,mengkonfigurasi, dan akhirnya memulai suatu peralatan wireless LAN klien sebagai suatu USB klien atau kartu PCMCIA, klien secara otomatis "mendengar" untuk melihat apakah ada suatu wireless LAN didalam range. Klien juga menemukan jika dapat berhubungan dengan wireless LAN tersebut. Proses "mendengar" disebut juga dengan *scanning.* Scanning terjadi sebelum proses lainnya, dikarenakan scanning adalah bagaimana klien menemukan network.

Ada dua tipe scanning : pasif scanning dan aktif scanning. Di dalam menemukan sebuah access point, pemancar klien mengikuti sebuah jejak *breadcumbs* kiri oleh access point. Breadcrumbs ini disebut juga *Service Set Identifiers* (SSID) dan rambu-rambu. Tool ini melayani sebagai sebuah titik tengah untuk sebuah pemancar klien untuk mencari suatu dan semua access point.

7.1.1 7.1.1 Service Set Identifier

Service set identifier (SSID) adalah sebuah nilai unique, case sensitive, alphanumeric dari 2-31 panjang karakter yang digunakan oleh wireless LAN sebagai sebuah nama network. Penanganan nama ini digunakan untuk men-segmentasi jaringan, sebagai ukuran security yang bersifat sementara, dan di

dalam proses penggabungan sebuah network. Administrator mengkonfigurasi SSID (kadang disebut dengan ESSID) di dalam setiap access point. Beberapa klien mempunyai kemampuan untuk menggunakan nilai SSID apapun bahkan hanya satu yang secara manual ditetapkan oleh administrator. Jika klien menjelajahi secara berlapis diantara suatu grup dari access point, maka kliennya dan seluruh access point harus dikonfigurasi dengan memasangkan SSIDnya. Hal yang terpenting dari sebuah SSID adalah SSID harus sesuai secara tepat antara access point dan klien. Jangan membingungkan SSID (ESSID) dengan BSSID. Basic Service Set Idenfier (BSSID) adalah suatu 6-byte heksa desimal mengidentifikasi access point dimana susunan mula-mula atau telah di-relay, mengingat SSID dan ESSID adalah hal-hal yang dapat ditukarkan yang menunjukkan nama jaringan atau identifier.

7.1.2 7.1.2 Beacons

Beacons (kependekan untuk beacon management frame) adalah frame pendek yang dikirim dari access point ke pemancar (Mode Infrastruktur) atau pemancar ke pemancar (Mode ad Hoc) yang digunakan mengorganisir dan mensinkronkan wireless pada LAN wireless itu. Beacon mempunyai beberapa fungsi, mencakup berikut

7.1.2.1.1.1.1.1 7.1.2.1 Time Synchronization

Beacon mensinkronkan klien melalui suatu time-stamp di saat transmisi yang tepat. Ketika klien menerima beacon, merubah clock sendiri untuk merefleksikan clock dari access point. Sekali ketika perubahan ini terbentuk, dua clock disinkronkan. Sinkronisasi clock unit komunikasi akan memastikan bahwa semua fungsi time-sensitive, seperti hopping dalam sistem FHSS, dilakukan tanpa kesalahan. Beacon juga berisi interval beacon, yang menginformasikan stasiun bagaimana sering untuk harapkan beacon.

7.1.2.1.1.1.1.2 7.1.2.2 FH atau Ds Parameter Sets

Beacon berisi informasi yang secara rinci menghubungkan teknologi spread spectrum sistem yang sedang digunakan. Sebagai contoh, di dalam

sistem FHSS, hop dan dwell parameter waktu dan ihop squence tercakup di dalam. Di dalam sistem DSSS, beacon berisi informasi saluran

7.1.3 7.1.3 SSID Information

Stasiun singgah beacon untuk SSID dari jaringan gabungan. Ketika informasi ini ditemukan, stasiun meneliti alamat MAC di mana autentifikasi memulai dan mengirimkan beacon meminta menghubungkan access point. Jika suatu stasiun mulai menerima apapun SSID, kemudian setasiun akan mencoba untuk bergabung dengan jaringan melalui access point yang pertama yang mengirimkan beacon atau dengan kekuatan sinyal yang paling kuat jika ada berbagai multipel access point.

7.1.4 7.1.4 Traffic Indication Map(TIM)

TIM digunakan sebagai indikator yang mana stasiun yang tidak bekerja mempunyai paket yang dientrikan Access point. Informasi ini dilewati pada setiap beacon ke semua stasiun yang berhubungkan. Selagi tidak bekerja, Sinkronisasi stasiun menggerakkan receivernya, membaca untuk beacon, memeriksa TIM untuk melihat jika terdaftarkan, kemudian, jika tidak terdaftarkan, meghentikan penerimanya.

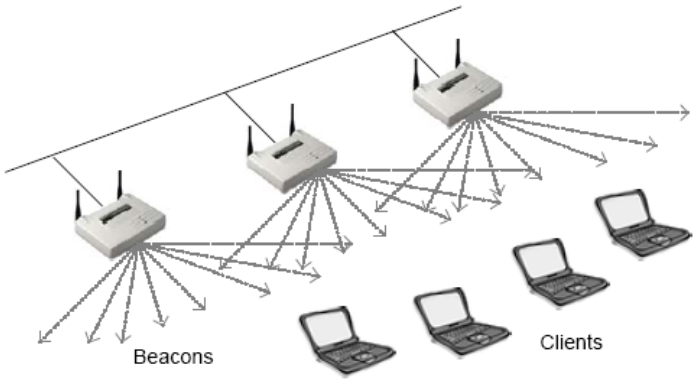
7.2 Supported Rates

Dengan jaringan wireless, ada banyak kecepatan didukung tergantung pada standard dari perangkat keras yang digunakan. Sebagai contoh, suatu 802.11b kecepatan 11, 5.5, 2,& 1 Mbps. kemampuan informasi ini dilewatkan beacon untuk menginformasikan stasiun kecepatan berapa yang didukung pada access point. Ada informasi yang banyak yang dilewatkan dalam beacon, tetapi daftar meliputi segalanya ini bisa menjadi pertimbangan yang penting dari suatu pandangan poin adiministrasi.

7.3 Passive scanning

Passive scanning adalah proses melacak beacon pada masing-masing saluran untuk suatu periode waktu yang spesifik setelah stasiun diinisialisasi beacon ini dikirim

oleh access point (model infrastruktur) atau stasiun klien (moded ad hoc), dan karakteristik katalok scanning station tentang stasiun atau access point berdasar pada beacon ini. Stasiun mencari suatu jaringan yang melacak beacon sampai dilacak oleh beacon yang terdaftarkan pada SSID dari jaringan untuk bergabung. Stasiun kemudian mencoba untuk bergabung dengan jaringan melalui access point yang mengirim beacon. Passive scanning digambarkan dalam **gambar 7.1**.



Gambar 7.1. Passive Scanning

Di dalam konfigurasinya di mana ada berbagai access point, SSID dari jaringan stasiun yang bergabung kemungkinan broadcast dengan lebih dari satu access point ini. Dalam situasi ini, stasiun akan mencoba untuk bergabung dengan jaringan melalui access point dengan kekuatan sinyal yang paling kuat dan rata-rata bit yang paling rendah.

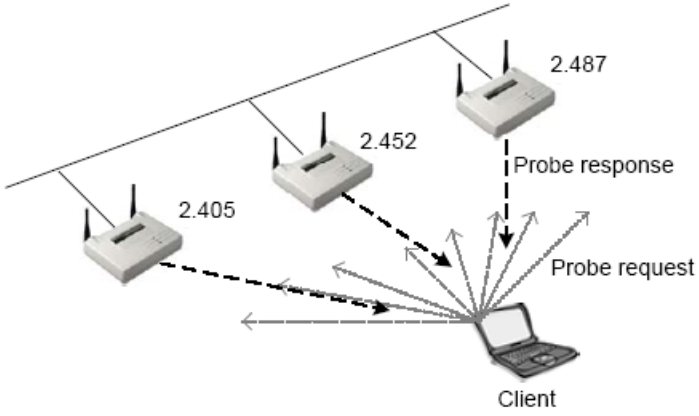
Stasiun melanjut passive scanning bahkan setelah menghubungkan access point. Passive scanning menyinpan waktu yang menghubungkan kembali ke jaringan jika klien diputus (disassociated) dari access point yang mana klien sekarang ini dihubungkan. Dengan pengonrolan daftar access point yang tersedia dan karakteristiknya(saluran, kekuatan sinyal, SSID, dll), stasiun dapat dengan cepat menempatkan access point yang terbaik yang koneksinya diputus untuk alasan tertentu.

Stasiun akan menjelajahi dari satu access point ke yang lain setelah sinyal radio dari access point di mana stasiun dihubungkan sampai kepada suatu kekuatan sinyal tingkat rendah tertentu. Penjelajahan diterapkan sedemikian sehingga stasiun dapat tinggal bertahan dihubungkan ke jaringan. Stasiun menggunakan informasi yang diperoleh lewat pasive scanning untuk menempatkan access point terbaik yang berikutnya (atau jaringan ad hoc) untuk menggunakan konektifitas kembali ke jaringan

itu. Karena alasan ini, tumpang-tindih antara sel access point pada umumnya ditetapkan kira-kira 20-30%. Tumpang-tindih ini membiarkan stasiun untuk secara tanpa lapisan menjelajahi antara access point selagi pemutusan dan penggubungan kembali tanpa pengetahuan pemakai.

Sebab kepekaan threshold pada beberapa radio tidak bekerja dengan baik, kadang-kadang administrator akan lihat suatu radio berkait dengan suatu access point sampai sinyal diputus dalam kaitan dengan kekuatan sinyal yang rendah sebagai ganti penjelajahan bagi access point yang mempunyai sinyal lebih baik. Situasi seperti ini adalah masalah yang dikenal dengan beberapa hardware dan harus dilaporkan ke pembuat jika anda mengalami masalah ini.

7.4 Active Scanning



Gambar 7.2. Active Scanning

Active scanning melibatkan pengiriman dari suatu request pemeriksaan (probe) frame dari suatu pemancar wireless. Pemancar mengirim probe frame jika mereka secara aktif mencari suatu jaringan untuk digabungkan. Probe frame akan berisi baik SSID dari jaringan yang mereka ingin gabungkan atau suatu SSID broadcast. Jika suatu request probe di kirim dengan menspasifikasi suatu SSID, maka hanya access point yang melayani SSID tersebut akan merespon dengan suatu frame respon probe. Jika suatu frame request probe dikirim dengan suatu SSID broadcast, maka semua access point didalam jangkauan akan merespon dengan suatu frame respon probe, dimana dapat dilihat pada **gambar 7.2**

Hal yang pokok dari probing dalam penggunaan ini adalah untuk menempatkan access point melalui pemancar yang dapat menempel ke suatu jaringan. Sekali sebuah access point dengan access point yang benar dapat ditemukan, pemancar meng-inisiasi langkah autentifikasi dan hubungan dari penggabungan jaringan melalui access point tersebut. Informasinya dilewatkan dari access point ke pemancar dalam frame respon probe hamper sama dengan beacons tersebut. Frame respon probe berbeda dari beacons hanya dalam dimana mereka tidak *time-stamped* dan keduanya tidak meliputi sebuah Traffic Indication Map (TIM).

Kekuatan sinyal dari frame respon probe dimana PC Card menerima bantuan kembali menentukan access point dengan dimana PC Card akan berusaha untuk berhubungan. Pemancar secara umum memilih access point dengan sinyal terkuat dan bit error rate (BER) yang terendah. BER adalah rasio dari paket-aket yang rusak ke paket yang bagus secara khusus ditetapkan oleh rasio Sinyal-ke-Noise dari sinyal. Jika puncak dari sebuah RF sinyal adalah di suatu tempat yang dekat dengan dasar noise, penerima akan membingungkan data sinyal dengan noise

7.5 Autentifikasi & Penggabungan

Proses dari menghubungkan ke wireless LAN terdiri dari dua dub proses yang terpisah. Sub-proses ini selalu terjadi dalam permintaan yang sama, dan disebut dengan *autentifikasi* dan *penggabungan(assosiasi)*. Untuk contoh, jika kita berbicara tentang sebuah wireless PC card dihubungkan ke wireless LAN, kita umpamakan bahwa PC card telah di-autentifikasi oleh dan telah di-assosiasikan dengan access point tertentu. Ingatlah bahwa saat kita berbicara tentang assosiasi, kita berbicara tentang konektivitas Layer 2, dan autentifikasi menyinggung secara umum ke PC card radio, tidak kepada user. Pemahaman langkah yang terhubung dalam mendapatkan sebuah klien terhubung ke sebuah access point adalah penting untuk keamanan, troubleshooting, dan manajemen dari sebuah wireless LAN.

7.5.1 Autentifikasi

Langkah pertama dalam hubungan ke wireless LAN adalah autentifikasi. Autentifikasi adlah proses melalui dimana sebuah wireless node (PC Card, USB Client, dsb) mempunyai identitas tersendiri yang diperiksa oleh jaringan (biasanya

access point) ke node yang berusaha untuk terhubung. Pemeriksaan ini terjadi saat access point yang ke klien terhubung memeriksa apakah klien tersebut memang klien yang disebut. Untuk menempatkan di tempat yang lain, access point merespon ke sebuah klien merequest untuk terhubung dengan memeriksa identitas klien sebelum ada hubungan yang terjadi. Kadang-kadang proses autentifikasi adalah null, yang berarti bahwa meskipun keduanya klien dan access pointharus memproses melalui proses ini agar dapat berasosiasi, disana tidak ada identitas khusus untuk berasosiasi. Ini adalah kasus saat access point baru dan PC Card dipasang di dalam konfigurasi default. Kita akan mendiskusikan dua tipe autentifikasi proses pada setelah bab ini.

Klien memulai proses autentifikasi dengan mengirim sebuah frame request autentifikasi ke access point (dalam Mode Infrastruktur). Access point akan melakukan keduanya baik menerima atau menolak request ini, sesudah itu memberitahukan pemancar dari keputusan ini dengan frame respon autentifikasi. Proses autentifikasi dapat diselesaikan pada access point, atau access point mungkin terlewati sepanjang responsibilitas ini ke sebuah hulu server autentifikasi seperti RADIUS. RADIUS server akan melakukan autentifikasi berdasarkan sebuah daftar dari criteria, dan kemudian mengembalikan hasilnya ke access point jadi access point tersebut dapat mengembalikan hasilnya ke pemancar klien.

7.5.2 Penggabungan (Assosiasi)

Sekali sebuah klien wireless telah terautentifikasi, klien tersebut kemudian berasosiasi dengan access point. *Terasosiasi* adalah sebuah kondisi pada saat sebuah klien diijinkan untuk melewatkan data melalui sebuah access point. Jika PC Card anda terasosiasi ke sebuah access point, anda berarti terhubung ke access point, dan juga jaringan.

Proses untuk menjadi terasosiasi adalah sebagai berikut. Saat suatu klien ingin terhubung, klien mengirimkan sebuah request autentifikasi ke access point dan menerima kembali sebuah authentification response. Setelah autentifikasi telah selesai, pemancar mengirim sebuah association request frame ke access point yang menjawab ke klien dfengan sebuah association response frame baik membolehkan atau tidak mengijinkan berasosiasi.

7.6 Status Pengesahan& Asosiasi

Proses asosiasi dan pengesahan yang lengkap mempunyai tiga status beda:

1. Unauthenticated and unassociated
2. Authenticated and unassociated
3. Authenticated and associated

7.6.1 Unauthenticated and Unassociated

Di dalam awal menyatakan,wireless node dengan komplet diputus dari jaringan dan tidak mampu untuk lewat frame melalui access point. Access point menyimpan tabel status koneksi klien dikenal sebagai tabel asosiasi. Adalah penting untuk mencatat vendor yang berbeda mengacu pada status yang unauthenticated dan unassociated dalam access pointnya tabel asosiasi dengan cara yang berbeda. Tabe ini akan secara khas menunjukkan "unauthenticated" untuk klien manapun yang belum menyelesaikan proses pengesahan atau telah mencoba pengesahan dan gagal.

7.6.2 Authenticated and Unassociated

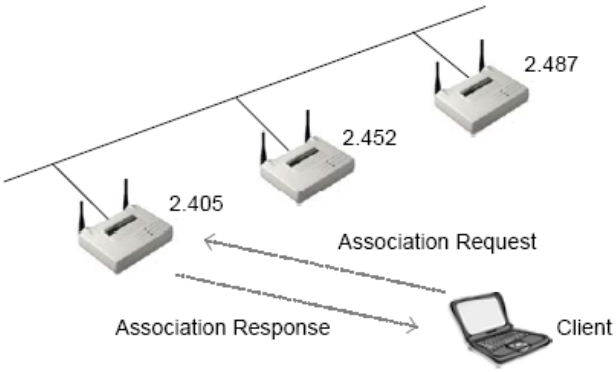
Di dalam status detik ini, klien wireless telah lewat proses pengesahan, tetapi waktu itu belum dihubungkan dengan access point. Klien waktu itu belum diijinkan untuk mengirimkan atau menerima data melalui access point. Tabel asosiasi access point akan secara khas menunjukkan "authenticated." Sebab klien lewat langkah pengesahan dan dengan seketika berproses ke dalam langkah asosiasi dengan cepat (seperseribu detik), jarang ditemui "authenticated" melangkah pada access point. Adalah jauh lebih mungkin akan ditemui "unauthenticated" atau "associated"- yang mana dibawa sampai akhir langkah.

7.6.3 Authenticated and Associated

Di dalam status akhir ini, wireless node dengan komplet dihubungkan ke jaringan dan mampu mengirimkan dan menerima data melalui access point yang mana nodet dihubungkan. **Gambar 7.3** menggambarkan suatu klien yang terhubung dengan suatu access point. Kita mungkin akan meihat "associated" di dalam tabel asosiasi access point yang menandakan bahwa klien ini secara penuh dihubungkan dan diberi hak untuk lewat lalu lintas melalui access point.

Sepertinya anda dapat menyimpulkan dari uraian dari tiap tiga status ini, mengedepan ukuran keamanan jaringan wireless akan diterapkan di titik di mana klien sedang mencoba untuk membuktikan keaslian.

7.7 Authentication Methods



Gambar 7.3 Association

Standard IEEE 802.1 1 menetapkan dua metoda pengesahan: *Open System authentication* dan *Share Key authentication*. Yang lebih sederhana dan juga semakin menjamin kedua metode adalah *Open System authentication*. Untuk suatu klien untuk menjadi authenticated, klien harus melewati rangkaian dengan access point. Rangkaian ini bervariasi tergantung pada proses pengesahan yang digunakan. Di bawah ini, kita akan mendiskusikan masing-masing proses pengesahan yang ditetapkan oleh standar 802.1 1, bagaimana bekerja, dan mengapa digunakan.

7.7.1 Open System Authentication

Open system authentication adalah suatu metoda pengesahan null dan ditetapkan oleh IEEE 802.1 1 seperti default yang ditentukan di dalam peralatan LAN Wireless. Penggunaan metoda pengesahan ini, suatu stasiun dapat berhubungan dengan access point manapun yang menggunakan Open system authentication berdasarkan hanya pada SSID. SSID harus sesuai pada kedua klien dan access point sebelum suatu klien diijinkan untuk melengkapi proses pengesahan. Penggunaan SSID yang berkenaan dengan keamanan akan dibahas di Bab 10 (Keamanan). Proses Open Sysytem authentication digunakan secara

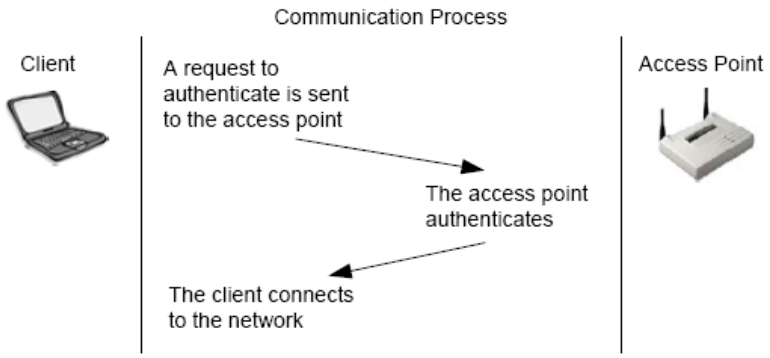
efektif dalam keduanya menjamin/mengamankan dan lingkungan yang tidak menjamin.

7.7.2 Open System Authentication Process

Proses Open System Authentication terjadi sebagai berikut:

- Wireless klien membuat suatu permintaan untuk berhubungan kepada access point
- Access point membuktikan keaslian klien dan mengirimkan suatu hal tanggapan positif klien menjadi terhubung

Langkah-Langkah ini dapat dilihat di **Gambar 7.4**.



Gambar 7.4 Sistem Autentikasi Open

Autentifikasi Open System adalah suatu proses yang sangat sederhana. Sebagai wireless LAN administrator, anda mempunyai pilihan untuk menggunakan WEP (wired equivalent privacy) enkripsi dengan autentifikasi Open System. Jika WEP digunakan dengan proses autentifikasi Open System, maka masih tidak ada verifikasi dari kunci WEP dalam setiap sisi dari koneksi selama autentifikasi. Lebih baik, WEP key digunakan hanya untuk pen-enkripsian data sekali saat klien terautentifikasi dan terasosiasi. Autentifikasi Open System digunakan dalam beberapa skenario, tetapi ada dua alasan utama untuk menggunakannya. Pertama, Autentifikasi Open System dipertimbangkan lebih amanam dari dua metode autentifikasi yang tersedia untuk alasan sebagai berikut. Dua, Autentifikasi Open System mudah untuk dikonfigurasi karena tidak membutuhkan konfigurasi sama sekali. Semua 802.11-compliant wireless LAN

hardware dikonfigurasi untuk menggunakan autentifikasi Open System secara default, membuatnya mudah untuk memulai membangun dan menghubungkan jaringan wireless LAN anda dengan benar.

7.7.3 Shared Key Authentication

Pengesahan shared key adalah suatu metoda authentification yang memerlukan penggunaan WEP. WEP encryption menggunakan kunci yang dimasukkan (pada umumnya oleh administrator) ke dalam kedua-duanya klien dan access point. Kunci ini harus [tanding/ temu] timbal balik untuk WEP untuk bekerja dengan baik. Kunci Yang bersama Pengesahan menggunakan WEP menyetem di (dalam) dua pertunjukan, ketika kita akan menguraikan di sini.

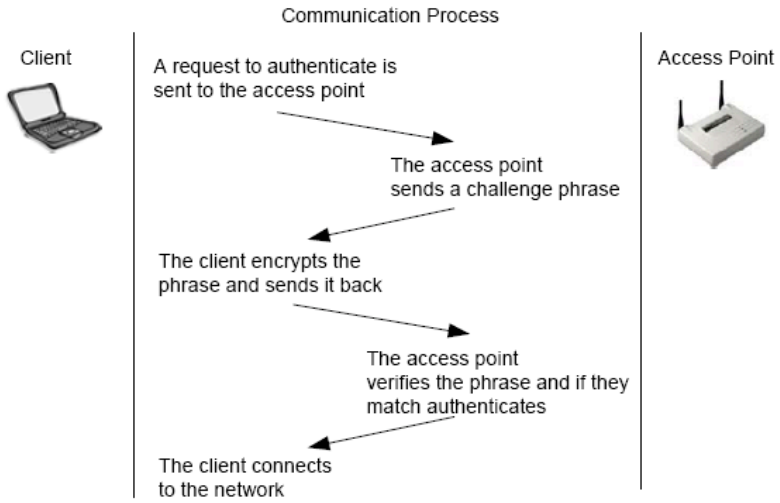
7.7.4 Shared Key Authentication Process

Proses pengesahan yang menggunakan Shared Key authentication terjadi sebagai berikut:

1. Suatu klien meminta asosiasi kepada suatu access point- langkah ini menjadi sama halnya itu sistem terbuka Pengesahan.
2. Akses Titik mengeluarkan suatu tantangan kepada klien- tantangan ini secara acak dihasilkan text datar, yang mana adalah dikirim dari access point klien bebas dari bahaya/kecurigaan
3. Klien bereaksi terhadap tantangan- klien menjawab dengan mengenkripsi tantangan teks menggunakan WEP klien menyetem dan mengirimkannya kembali ke access point
4. Access point bereaksi terhadap tanggapan klien- Access point de-enkripsi tanggapan yang di-enkripsi klien untuk memverifikasi yang tantangan teks adalah penggunaan di-enkripsi adalah mempertemukan suatu kunci WEP menyetel.

Melalui proses ini , access point menentukan ya atau tidaknya klien mempunyai WEP kunci yang benar. Jika WEP kunci klien benar, access point akan menjawab secara positif dan membuktikan keaslian klien itu. Jika WEP kunci klien tidak benar, access point akan menjawab secara negatif, dan tidak

membuktikan keaslian klien, meninggalkan klien yang tidak dibuktikan keasliannya dan tidak dihubungkan.



Gambar 7.5 Proses Shared Key

Itu akan nampak bahwa Proses Shared Key authentication jadi lebih menjamin dibandingkan dengan Open System Authentication, tetapi seperti anda akan segera lihat, ini bukan. Melainkan, Bagi Shared Key authentication membuka pintu untuk calon hackers. Adalah penting untuk memahami kedua kemungkinan bahwa WEP digunakan. WEP key dapat digunakan sepanjang Proses Shared Key authentication untuk memverifikasi suatu identitas klien, tetapi dapat juga digunakan untuk enkripsi dari data payload mengirimkan dengan klien melalui access point. WEP penggunaan jenis ini adalah dibahas lebih lanjut di dalam Bab 10 (Keamanan).

7.7.5 Authentication Security

Shared Key authentication tidaklah dipertimbangkan menjamin sebab access point memancarkan tantangan teks bebas dari bahaya/kecurigaan dan menerima teks tantangan yang sama yang encrypted dengan WEP kunci. Skenario ini mengijinkan suatu hacker menggunakan suatu sniffer untuk lihat kedua-duanya plaintext menghadapi tantangan dan tantangan yang dienkripsi.Setelah kedua-duanya nilai-nilai ini, suatu hacker bisa menggunakan suatu program cracking sederhana untuk memperoleh WEP kunci. Sekali ketika WEP kunci diperoleh,

hacker bisa men-dekripsi lalu lintas yang terenkripsi. Adalah untuk alasan ini bahwa Open System Authentication dipertimbangkan lebih menjamin dibanding Shared Key authentication.

Adalah penting bagi administrator wireless jaringan untuk memahami bahwa bukan Open System maupun Share Key authentication tipe keamanan, dan untuk alasan ini suatu solusi keamanan LAN wireless solusi, di atas dan di luar standard 802.11 yang ditetapkan, adalah perlu dan penting.

7.7.6 Shared Secrets & Certificates

Shared Secrets adalah teks atau angka-angka yang biasanya dikenal sebagai kunci WEP. Sertifikat adalah metoda identifikasi pemakai yang lain menggunakan dengan wireless. Sama halnya dengan kunci WEP, sertifikat (yang mana dokumen telah disahkan) ditempatkan pada mesin klien sebelum waktu yang ditetapkan. Penempatan ini juga dikerjakan ketika berbagai keinginan pemakai untuk membuktikan keaslian ke jaringan wireless, mekanisme pengesahan telah pada tempatnya pada stasiun klien. Kedua metoda ini sudah menurut sejarah diterapkan di dalam suatu pertunjukan manual, tetapi ada aplikasi yang tersedia hari ini itu mengijinkan otomasi dari proses ini.

7.8 Emerging Wireless Security Solutions

Ada banyak protokol dan solusi keamanan pengesahan baru pada pasaran hari ini, mencakup VPN dan 802.Ix yang menggunakan Extensible Authentication Protocol (EAP). Banyak dari solusi keamanan ini melibatkan pengesahan melalui server pengesahan ke hulu dari accesssa point selagi memelihara klien yang menunggu sepanjang tahap pengesahan. Windows XP mempunyai pendukungan asli untuk 802.11, 802.Ix, dan EAP. Manufaktur Cisco dan LAN wireless juga mendukung standard ini. Karena alasan ini,untuk melihat bahwa 802.Ix dan solusi pengesahan EAP adalah suatu solusi umum dalam keamanan pasar LAN wireless.

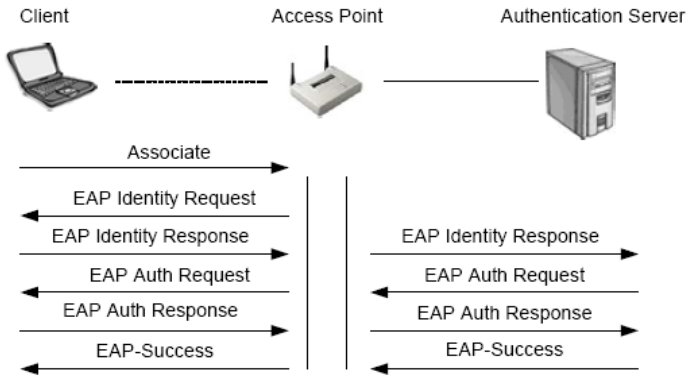
7.8.1 802.1x and EAP

802.Ix (kontrol akses jaringan port-based) standard secara relatif baru, dan alat yang mendukungnya mempunyai kemampuan untuk mengijinkan sekedar

koneksi ke dalam jaringan pada layer 2 hanya jika pengesahan pemakai sukses. Protokol ini bekerja baik untuk access point yang membutuhkan kemampuan untuk memelihara para pemakai yang memutuskan jaringan jika mereka tidak mendukung pada jaringan. EAP adalah, suatu protokol layer 2 yang menggantikan PAP atau CHAP dibawah PPP yang bekerja area jaringan lokal. EAP mengijinkan plug-ins manapun akhir dari suatu link dengan banyak metoda pengesahan dapat digunakan. Di masa lalu, PAP dan CHAP telah digunakan untuk pengesahan pemakaian, dan keduanya menggunakan password. Kebutuhan akan suatu yang lebih kuat. Alternatif yang lebih fleksibel harus jelas dengan jaringan wireless karena implementasi yang lebih bervariasi penuh dengan wireless dibanding dengan jaringan kawat.

Secara khas, pengesahan pemakaian terpenuhi menggunakan Remote Authentication Dial-In user Service (RADIUS) server dan beberapa bentuk database pemakai (Native RADIUS. NDS, Direktori Aktif, LDAP, dll.). Proses dalam autentifikasi menggunakan EAP ditunjukkan di dalam Gambar 7.6. Standar 802.11i yang baru meliputi mendukun untuk 802.Ix, EAP, AAA, pengesahan timbal balik, dan key generation, tidak satupun tercakup pada yang asli standard 802.11. " AAA" adalah singkatan dari *authentication*(mengidentifikasi siapa kita), *authorization*(menghubungkan dengan mengijinkan kita untuk melaksanakan tugas tertentu pada jaringan), dan *accounting* (menunjukkan apa yang telah dilakukan dan mana yang dipunya pada jaringan).

Di dalam model standard 802. Ix, autentifikasi jaringan terdiri dari tiga potongan: pemohon, authenticator, dan server autentifikasi.



Gambar 7.6 802.1x and EAP

Sebab keamanan LAN wireless penting dan tipe autentifikasi EAP menyediakan rata-rata pengamanan koneksi LAN wirelesst-vendor dengan cepat mengembangkan dan menambahkan tipe autentifikasi EAP kepada access point LAN wireless. Mengetahui jenis EAP yang sedang digunakan adalah penting di dalam pemahaman karakteristik dari metoda autentifikasi seperti kata sandi, key generation, mutusl authentication, dan protokol. Sebagian dari tipe autentifikasi EAP meliputi:

7.8.1.1 EAP-MD-5 Challenge.

Yang apaling jenis autentifikasi EAPl, ini sangat utama menyalin perlindungan password CHAP pada suatu LAN wireless. EAP-MD5 menghadirkan semacam tingkat dasar EAP mendukung antar 802.Ix.

7.8.1.2 EAP-CISCO Wireless.

Disebut LEAP (Lightweight Extensible Authentication Protokol), Jenis autentifikasi EAP ini digunakan terutama semata dalam Cisco LAN wireless access point. LEAP menyediakan keamanan, enkripsi transmisi data menggunakan dinamis WEP keys yang dihasilkan, dan mendukung mutual authentication.

7.8.1.3 EAP-TLS (Transport Layer Security).

EAP-TLS menyediakan certificate-based,mutual autentifikasi klien dan jaringan. EAP-TLS bersandar pada sertifikat client-side dan server-side untuk melaksanakan autentifikasi, penggunaan yang dinamis menghasilkan pemakai dan WEP keys session-based membagikan untuk mengamankan jaringan. Windows XP meliputi suatu klien EAP-TLS, dan EAP-TLS juga mendukung Windows 2000.

7.8.1.4 EAP-TTLS.

Funk Software dan Certicom sudah bersama-sama mengembangkan *EAP-TTLS* (Tunneled Transport Layer Security). EAP-TTLS adalah suatu

perluasan EAP-TLS, yang menyediakan certificate-based, mutual autentifikasi jaringan dan klien. Tidak sama dengan EAP-TLS, bagaimanapun, EAP-TTLS memerlukan hanya sertifikat server-side, menghapuskan kebutuhan untuk mengatur sertifikat untuk masing-masing klien LAN wireless.

Sebagai tambahan, EAP-TTLS mendukung password protokol, maka kita dapat menyebarkannya melawan sistem autentifikasimu (seperti Aktive Directory atau NDS). EAP-TTLS dengan aman menerobos klien autentifikasi di dalam arsip TLS, memastikan bahwa sisa pemakai tanpa nama ke eavesdroppers pada the wireless link. Pemakai dihasilkan secara dinamis dan WEP kunci session-based dibagi-bagikan untuk menjamin koneksi.

EAP-SRP (Secure Remote Password), SRP adalah suatu autentikasiberbasis password dan protokol key-exchange. Ini memecahkan permasalahan dalam klien yang membuktikan keaslian ke server dengan aman dalam keadaan dimana pemakai dari perangkat lunak klien harus menghafal suatu rahasia kecil (seperti suatu kata sandi) dan tidak membawa informasi rahasia lain. Server membawa suatu pemeriksa untuk masing-masing pemakai, yang mana mengijinkan server untuk membuktikan keaslian klien. Bagaimanapun, jika pemeriksa disepakati, penyerang tidak akan diijinkan untuk menyamar klien. Sebagai tambahan, SRP menukar suatu rahasia yang kuat sebagai byproduct dari autentikasi yang sukses, yang mana memungkinkan kedua pihak untuk komunikasi dengan aman.

EAP-SIM (GSM). EAP-SIM adalah suatu mekanisme untuk mobile IP jaringan mengakses pendaftaran dan autentikasi pembangkitan key menggunakan GSM Subscriber Identity Module(SIM). Dasar pemikiran untuk . yang menggunakan GSM SIM dengan mobile IP akan pengungkitan GSM otorisasi infrastruktur yang ada dengan user yang ada mendasarkan dan SIM kartu saluran distribusi yang ada. Dengan penggunaan SIM kunci pertukaran, tidak ada asosiasi keamanan yang lain yang dikonfigurasi terlebih dahulu di samping SIM kartu diperlukan pada mobile node. Gagasannya bukanlah untuk menggunakan teknologi GSM radio akses, tetapi untuk menggunakan GSM SIM otorisasi dengan mobile IP pada layer manapun, sebagai contoh pada akses jaringan wireless LAN.

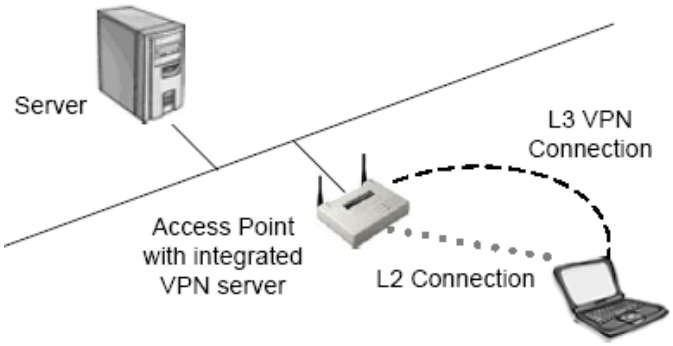
Ada kemungkinan bahwa daftar autentikasi jenis EAP akan tumbuh ketika semakin banyak penjual masuk wireless LAN keamanan pasar, dan sampai pasar memilih suatu standard.

Jenis EAP pengesahan yang berbeda tidaklah tercakup pada ujian CWNA, tetapi pemahaman apa EAP adalah dan bagaimana digunakan di dalam umum adalah suatu unsur kunci di (dalam) menjadi efektif sebagai wireless network administrator

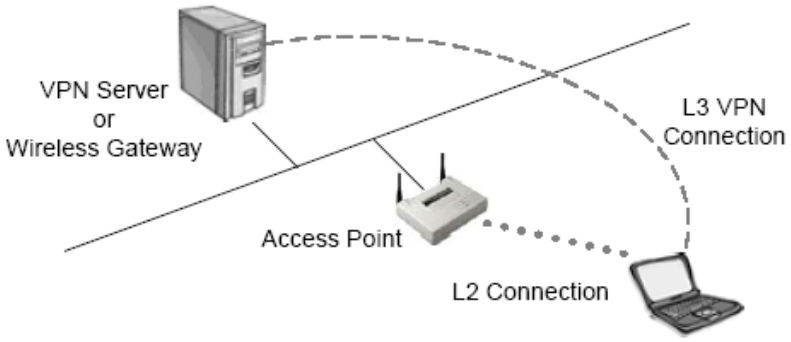
7.9 VPN Solutions

Teknologi VPN menyediakan rata-rata untuk dengan aman memancarkan data antar network-devices (di) atas suatu data pinjaman mengangkut medium. Biasanya digunakan untuk menghubungkan remote jaringan atau komputer bagi suatu server perusahaan via Internet. Bagaimanapun, VPN adalah juga suatu solusi untuk melindungi data pada suatu jaringan wireless. VPN bekerja dengan pedoman menciptakan suatu tunnel di atas sekali suatu protokol seperti IP. Lalu lintas di dalam tunnel terenkripsi, dan secara total terisolasi seperti dapat dilihat di **gambar 7.7** dan **gambar 7.8**. VPN teknologi menyediakan tiga tingkatan keamanan: pengesahan pemakai, encryption, dan pengesahan data.

- Autentikasi pemakai memastikan bahwa hanya memberi hak para pemakai (pada atas suatu alat yang spesifik) bisa menghubungkan, mengirimkan, dan menerima data melalui jaringan wireless.
- Enkripsi menawarkan perlindungan tambahan ketika memastikan bahwa sekalipun transmisi diinterupsi, mereka tidak bisa dikodekan tanpa usaha dan waktu penting.
- Data Pengesahan memastikan integritas data pada jaringan wireless, menjamin bahwa semua lalu lintas adalah dari alat dibuktikan keasliannya saja.



Gambar 7.7 Accesss Point Terintegrasi dengan VPN Server



Gambar 7.8 Access Point dengan external VPN Server

Menerapkan VPN teknologi untuk menjamin suatu jaringan wireless memerlukan suatu pendekatan berbeda dibanding ketika digunakan pada jaringan wired untuk pertimbangan berikut

- Yang tidak bisa dipisahkan fungsi repeater dari wireless access points secara otomatis ke depan lalu lintas antar pemancar wireless LAN yang berkomunikasi bersama-sama dan itu nampak pada jaringan wireless yang sama.
- Cakupan dari jaringan wireless akan mungkin meluas di luar secara fisik batasan-batasan dari suatu rumah atau kantor, memberi pengganggu rata-rata untuk berkompromi jaringan.

Kesenangan dan scalabilas dengan mana solusi wireless LAN dapat menyebar membuat mereka solusi ideal untuk banyak lingkungan berbeda. Sebagai hasilnya, implementasi VPN keamanan akan bertukar-tukar berdasar pada kebutuhan dari tiap

jenis lingkungan. Sebagai contoh, suatu hacker dengan suatu wireless sniffer, jika ia memperoleh WEP kunci, bisa memecahkan kode paket di dalam waktu riil. Dengan suatu VPN solusi, paket tidak akan hanya dienkripsi, tetapi juga dilewatkan pada tempat tertentu. Lapisan tambahan keamanan menyediakan banyak manfaat di tingkatan akses.

Suatu catatan penting di sini adalah bahwa tidak semua VPN membiarkan para pemakai wireless menjelajahi antar subnets atau jaringan tanpa " mematahkan" jalan amannya, dan tidak semua VPN akan mengijinkan koneksi aplikasi dan pengangkutan untuk tinggal dibentuk selama penjelajahan. Blok tumbang yang lain menjadi sistem operasi- apa yang sistem operasi atau sistem lakukan klien yang mobile harus menjalankan dalam rangka mendapatkan perlindungan suatu wireless VPN.

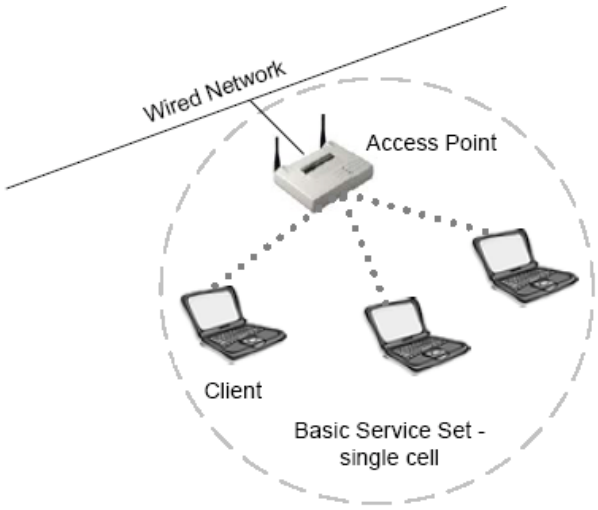
7.10 Service Sets

Service Sets adalah suatu istilah yang digunakan untuk menguraikan komponen dasar suatu operasional LAN wireless. Dengan kata lain, ada tiga cara untuk mengatur suatu LAN wireless, dan masing-masing cara memerlukan suatu perangkat keras yang berbeda . Ketiga cara konfigurasi LAN wireless adalah:

- Basic service set
- Extended service set
- Independent basic service set

7.10.1 Basic Service Set (BSS)

Ketika access point dihubungkan suatu jaringan kabel dan satu set stasiun wireless, konfigurasi jaringan dikenal sebagai basic service set (BSS). BSS terdiri dari hanya satu access point dan satu atau lebih klien wireless, seperti ditunjukkan di dalam Gambar 7.9. BSS menggunkan model infrastruktur- suatu model yang memerlukan penggunaan dari suatu access point dan di mana semua lalu lintas wireless menyilang. Transmisi yang diijinkan tidak secara langsung client-to-client.

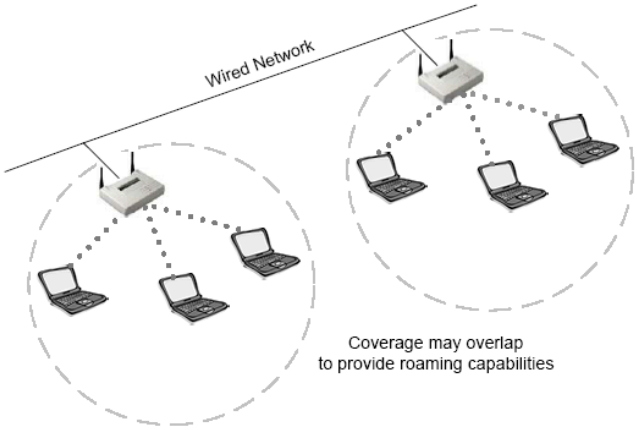


Gambar 7.9 Basic Service Set

Masing-Masing klien wireless harus menggunakan access point untuk berkomunikasi dengan klien wireless lainnya atau manapun host pada jaringan itu. BSS meliput singel cell, atau RF area, di sekitar access point dengan data yang bermacam-macam nilai zone (lingkaran-lingkaran konsentris) tentang kecepatan data berbeda. yang diukur di dalam Mbps. Kecepatan data dalam lingkaran-lingkaran konsentris ini akan tergantung pada teknologi yang sedang digunakan. Jika BSS terdiri dari peralatan 802.1 Ib, kemudian lingkaran-lingkaran konsentris akan membuat kecepatan data 11, 5.5, 2, dan 1 Mbps. Suatu BSS mempunyai satu SSID unik.

7.10.2 Extended Service Set (ESS)

Extended Service Set (ESS) digambarkan sebagai dua atau lebih layanan dasar menetapkan hubungan oleh suatu sistem distribusi secara umum, seperti ditunjukkan dalam **Gambar 7.10.** System distribusi dapat dimanapun Kabel, Wireless, LAN, WAN, atau metoda konektivitas jaringan yang lain. ESS harus punya sedikitnya 2 access point yang beroperasi dalam model infrastruktur. Sama suatu BSS, semua paket di dalam ESS harus pergi melalui salah satu dari access point.

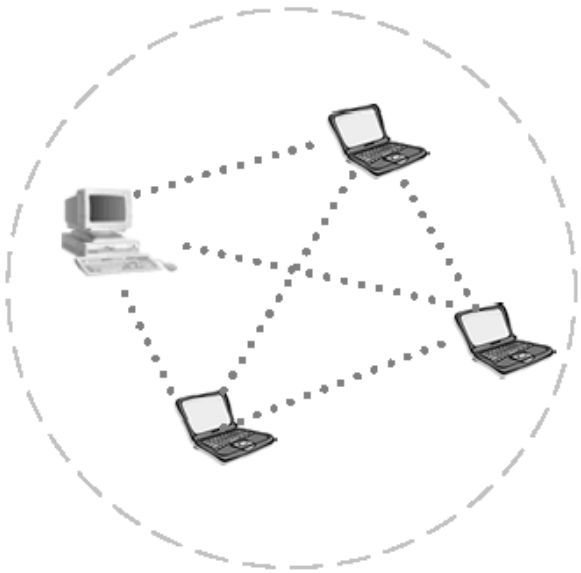


Gambar 7.10 Extended Service Set

Karakteristik yang lain dari ESS, sesuai standar 802.11, adalah bahwa ESS meliputi berbagai sel, mengijinkan-tetapi tidak memerlukan-kemampuan menjelajah dan tidak memerlukan SSID yang sama di dalam kedua layanan dasar.

7.10.3 Independent Basic Service Set (IBSS).

Independent Basic Service Set juga dikenal sebagai suatu jaringan *ad hoc* Suatu IBSS tidak punya access point atau akses lain untuk suatu sistem distribusi, tetapi menutupi singel cell dan mempunyai satu SSID, seperti ditunjukkan dalam **Gambar 7.11.** Klien di dalam suatu IBSS mengubah tanggung jawab pengiriman beacon karena tidak ada access point untuk melaksanakan tugas ini**.**

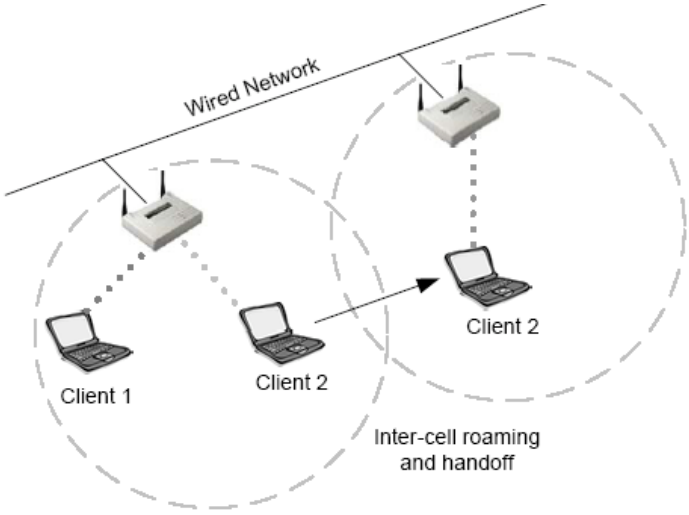


Gambar 7.11 Independent Basic Service Set

Dalam rangka memancarkan data yang ada di luar suatu IBSS, salah satu klien di dalam IBSS harus bertindak sebagai suatu pintu gerbang, atau penerus, menggunakan suatu perangkat lunak solusi untuk tujuan ini. Di dalam suatu IBSS, buatan klien mengarahkan koneksi untuk satu sama lain ketika pemancaran data, dan untuk alasan ini, suatu IBSS adalah sering dikenal sebagai suatu jaringan peer-to-peer.

Roaming adalah kemampuan atau proses dari suatu klien wireless untuk pindah secara tanpa kelim dari satu sel (atau BSS) ke yang lain tanpa jaringan kehilangan connectivas. Access points menyampaikan klien mulai dari satu ke yang lain dengan cara yang adalah tak kelihatan kepada klien, memastikan hubungan tak putus-putus. **Gambar 7.12** menggambarkan suatu klien yang menjelajahi dari satu BSS ke BSS lain.

Ketika area manapun di dalam bangunan adalah di dalam cakupan resepsi lebih dari satu access point pemenuhan sel tumpang-tindih. Overlap coverage areas adalah suatu atribut penting menyangkut susunan wireless LAN, sebab itu memungkinkan roaming tanpa kelim antar sel yang overlap. Roaming mengijinkan para pemakai mobile dengan pemancar portabel untuk pindah dengan bebas antara sel yang overlap,secara konstan memelihara koneksi jaringan mereka.



Gambar 7.12 Roaming di ESS

Ketika roaming tanpa kelim, suatu sesi pekerjaan dapat dimaintain saat bergerak dari satu sel ke yang lain. Berbagai access point dapat menyediakan pemenuhan wireless roaming untuk suatu keseluruhan bangunan atau kampus

Ketika coverage area dua atau lebih access point tumpang-tindih, pemancar di dalam area overlap dapat menetapkan kemungkinan terbaik koneksi dengan satu dari access point saat berlangsung secara terus-menerus mencari-cari access point yang terbaik. Dalam rangka memperkecil kerugian paket selama peralihan, yang yang "tua" dan " baru" access point-access point komunikasi untuk mengkoordinir proses roaming. Fungsi ini adalah serupa kepada suatu handover telepon selular , dengan dua perbedaan utama:

- Pada sistem suatu packet-based LAN , transisi dari sel ke sel mungkin dilakukan antar transmisi paket, sebagai lawan teleponi jika transisi boleh terjadi selama suatu percakapan telepon.
- Pada suatu sistem suara, suatu pemutusan hubungan temporer tidak boleh mempengaruhi percakapan, saat di suatu lingkungan packet-based itu dengan mantap mengurangi performa dikarenakan lapisan atas protokol kemudian memancarkan kembali data itu.

7.11 Standar

Standar 802.11 tidak menggambarkan bagaimana roaming harus dilakukan, tetapi menggambarkan dasar membangun blok. Blok bangunan ini meliputi aktif & pasif scanning dan suatu proses reasosiasi. Proses asosiasi kembali terjadi ketika pemancar wireless menjelajahi dari access point satu ke yang lain, menjadi terhubung dengan access point yang baru.

Standard 802.11 mengijinkan suatu klien untuk menjelajahi antar berbagai access point-access point yang beroperasi pada saluran sama atau terpisah. Sebagai contoh, tiap-tiap 100 m, suatu access point mungkin memancarkan suatu rambu isyarat yang meliputi suatu perangko waktu untuk sinkronisasi klien, suatu lalu lintas indikasi peta, suatu indikasi dari tingkat tarip data didukung, dan parameter lain. Roaming klien menggunakan rambu untuk mengukur kekuatan koneksi yang ada pada mereka ke access point. Jika koneksi lemah, pemancar penjelajah dapat mencoba untuk berhubungan sendiri dengan suatu access point baru.

Untuk memenuhi kebutuhan komunikasi mobile radio, 802.11b standar harus untuk bersikap toleran terhadap koneksi yang sedang mati dan berhubungan kembali. Usaha standard untuk memastikan gangguan minimum ke penyerahan data, dan menyediakan beberapa macam untuk caching dan menyampaikan pesan antar BSS.

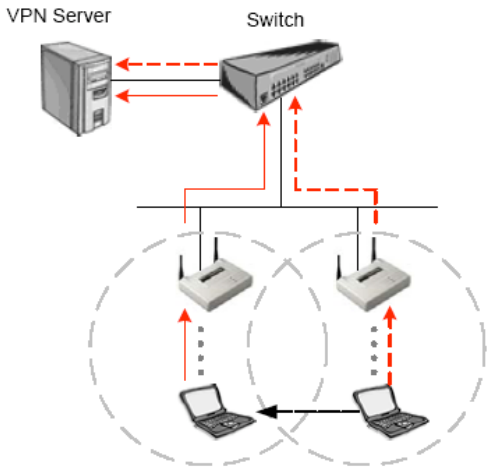
Implementasi tertentu beberapa yang lebih tinggi lapisan protokol seperti TCP/IP mungkin lebih sedikit bersikap toleran. Sebagai contoh, di dalam suatu jaringan di mana DHCP digunakan untuk menugaskan IP alamat, suatu roaming node boleh hilang koneksi nya ketika pindah ke seberang batasan-batasan sel. Node kemudian harus re-establish koneksi ketika masuk BSS atau sel yang berikutnya. Solusi perangkat lunak tersedia untuk masalah masalah tertentu ini.

Salah satu solusi adalah mobile IP. Mobile IP adalah suatu Internet Engineering Task Force (IETF) Request for Comment (RFC) (# 2002) itu didokumentasikan untuk kepentingan menjelaskan bagaimana cara terbaik mempunyai para pemakai korset mobile menghubungkan kepada Internet saat bergerak antar poin-poin koneksi. Ini terpenuhi dengan menggunakan agen rumah dan agen asing. Dua pekerjaan ini bersama-sama untuk meyakinkan bahwa lalu lintas yang diperuntukkan ke mobile node menjangkau dimanapun juga dihubungkan. Suatu agen rumah atau agen asing bisa merupakan suatu komputer, suatu penerus, atau alat serupa lain yang adalah mampu untuk menjalankan mobile IP protokol. Ada beberapa surat protes penegakan hukum di (dalam) banyak solusi mobile IP yang harus dengan singkat ditujukan di dalam teks ini sedemikian hingga pemakai memahami apa yang harus dicari di (dalam) suatu solusi mobile IP.

IP Pertama, mobile tidak mengijinkan agen kemampuan dan alat mobile pada [atas] jaringan untuk_ berbagi informasi status tentang masing-masing sesi yang suatu alat mobile telah menetapkan. Alat-Alat ini bahwa aplikasi tidak bisa tetap berlaku selama periode ketika alat yang mobile tidak bisa dicapai. Ketika alat yang mobile menyertakan kembali kepada jaringan, mungkin ada suatu kebutuhan untuk menyapu bersih sesi aplikasi rusak, batang kayu di dalam lagi, re-authenticate, start kembali aplikasi, dan masuk kembalinya hilang data (lagi suatu kerugian produktivitas, belum lagi suatu usabilas kegagalan). Ke dua, " ketekunan sesi" berarti lebih dari menyampaikan paket [bagi/kepada] suatu penempatan baru pemakai. Jika kita tidak mempunyai ketekunan sesi aplikasi dan pengangkutan, solusi pecah;roboh. Mengapa? Ketika suatu protokol pengangkutan tidak bisa komunikasi ke panutan nya, dasar

protokol,sepertiTCP, berasumsi bahwa gangguan layanan adalah dalam kaitan dengan jaringan buntu. Ketika ini terjadi, protokol ini mengundurkan diri, mengurangi capaian dan secepatnya mengakhiri koneksi .Satu-Satunya cara untuk memecahkan masalah ini akan mempunyai node mobile menyebar dengan suatu perangkat lunak solusi yang berlaku atas nama alat yang mobile ketika itu tak dapat dicapai.

Batasan-batasan. Proses ini adalah tanpa kelim kepada lapisan 3. Bagaimanapun, jika suatu terowongan dibangun ke access point atau memusatkan VPN server dan suatu lapisan 3 batas silang, suatu mekanisme beberapa sesama harus disediakan untuk mempertahankan jalur hidup ketika batas silang.

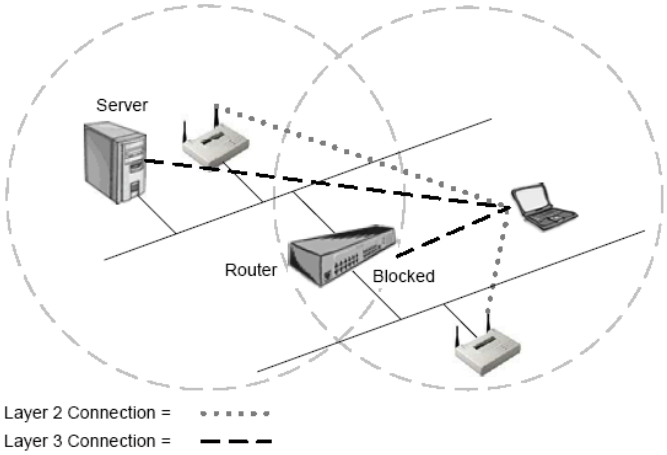


Gambar 7.13 Roaming dengan VPN Tunnels

7.12 Layer 2 & 3 Boundaries

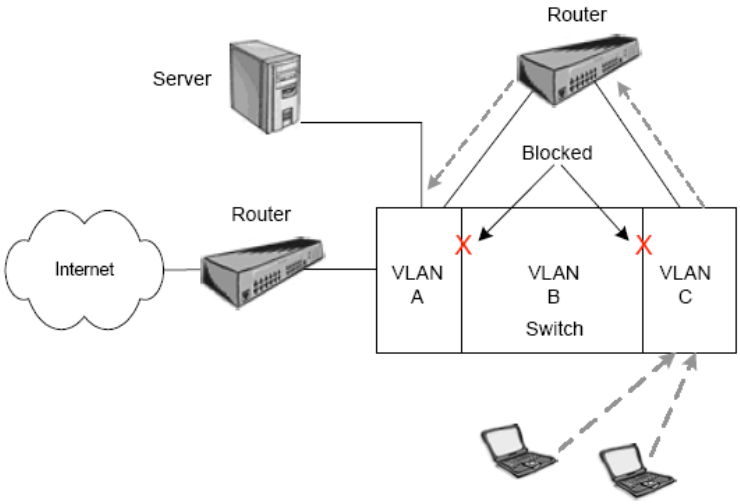
Suatu batasan teknologi yang ada adalah jaringan wired itu adalah sering terbagi-pagi untuk cara penanganannya. Perusahaan dengan berbagai bangunan, seperti rumah sakit atau bisnis besar, sering menerapkan suatu LAN pada setiap bangunan dan kemudian menghubungkan LAN ini dengan router atau switch-routers. Lapisan 3 segmentasi mempunyai dua keuntungan utama. Pertama, berisi siaran yang secara efektif, dan detik/second itu mengijinkan akses mengendalikan antar segmen pada jaringan itu. Segmentasi jenis ini dapat juga dilaksanakan pada lapisan 2 penggunaan VLAN pada tombol. VLAN yang sering dilihat floor-by-floor diterapkan di dalam multi-floor bangunan kantor atau untuk masing-masing bangunan yang remote di dalam suatu kampus untuk pertimbangan yang sama itu. Segmen pada lapisan 2 di dalam segmen performa ini jaringan dengan sepenuhnya seolah-olah berbagai jaringan sedang diterapkan. Ketika penggunaan router seperti figur dilihat di **gambar 7.14**, para

pemakai harus mempunyai suatu metoda penjelajahan(roaming) ke seberang batasan-batasan penerus tanpa kehilangan koneksi lapisan 3 mereka. Koneksi Lapisan 2 masih di-maintain oleh access point-access point, tetapi sejak IP subnet telah berubah saat penjelajahan, koneksi ke server, sebagai contoh, akan jadi rusak. Tanpa subnet-roaming kemampuan (seperti dengan penggunaan suatu IP solusi mobile atau menggunakan DHCP), wireless LAN access point-access point harus semua dihubungkan ke subnet tunggal (alias. " suatu jaringan flat/kempes"). Work-Around ini bisa dilakukan putus bicara fleksibilitas manajemen jaringan, tetapi pelanggan mungkin berkeinginan membuat biaya ini jika mereka merasa bahwa nilai dari sistem akhir cukup tinggi.



Gambar 7.14 Roaming across Layer 3 boundaries

Banyak lingkungan jaringan (e.g., multi-building campus, multi-floored high rises, atau older atau historical building) tidak bisa mengambil solusi single subnet sebagai pilihan praktis. Arsitektur Kabel berselisih dengan teknologi LAN wireless baru-baru ini. Access point tidak bisa menyampaikan suatu sesi ketika suatu alat remote pindah melewati batasan router sebab persimpangan rute merubah alamat IP klien. Sysytem Wired tidak lagi mengetahui di mana untuk mengirimkan pesan itu. Ketika suatu pergerakan alat menyertakan kembali ke jaringan, semua aplikasi hilang dan para pemakai wajib login lagi, re-authenticate, menampung diri mereka di dalam aplikasi, dan membangun ulang data hilang. Jenis masalah yang sama terjadi ketika menggunakan VLAN. Tombol lihat para pemakai sebagai penjelajah melewati batasan-batasan VLAN.



Gambar 7.15 Roaming Across VLan

Suatu solusi hardware pada masalah ini akan menyebar semua access point pada Single VLAN yang menggunakan suatu flat subnet IP untuk semua access point sehingga tidak ada perubahan alamat IP untuk penjelajahan para pemakai dan suatu solusi mobile IP yang diperlukan. Para pemakai kemudian yang ditetapkan sebagai kelompok kembali ke jaringan menggunakan suatu firewall, suatu router, suatu gateway, dan lain lain. Solusi Ini sulit untuk menerapkan di dalam banyak kejadian, tetapi berlaku umum seperti " standard" metodologi. Ada banyak lagi kejadian lainnya di mana suatu perusahaan harus membatalkan penggunaan suatu LAN wireless semuanya sebab solusi seperti itu tidak praktis.

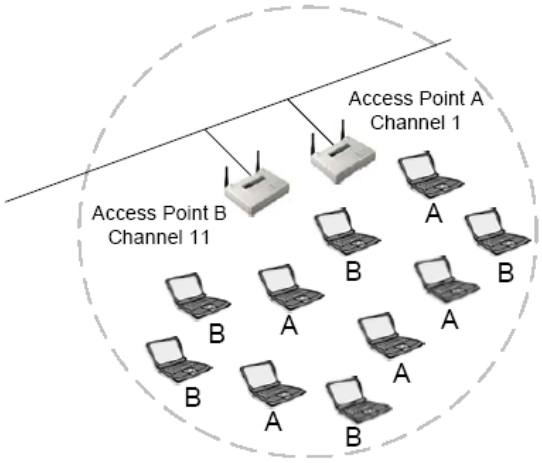
Sama dengan semua access point pada subnet tunggal, para mobile user masih menghadapi permasalahan pemenuhan. Jika seorang pemakai pindah dari batasaa, ke dalam suatu lubang pemenuhan, atau sederhananya memenjarakan alat untuk memperpanjang hidup baterei, semua aplikasi hilang dan para pemakai di dalam situasi ini lagi juga dipaksa untuk membukukan lagi dan menemukan jalan kembali di mana mereka berhenti.

Ada beberapa solusi layer 3 pada pasar mulai dari ini penulisan. Satu solusi seperti itu adalah suatu access point telah dibangun di dalam server VPN dan melaksanakan routing penuh, termasuk yang merouting protokol seperti RIP. Solusi yang lain diterapkan pada satu rangkaian server menggunakan Mobile IP standard (RFC 2002). Banyak dari solusi perangkat lunak diterapkan di alam sedikitnya cara yang sama.

7.13 Load Balancing

Area terlampau banyak dengan banyak para pemakai dan lalu lintas lebat memuat per unit memerlukan suatu struktur multi-cell. Di dalam suatu struktur multi-cell, beberapa access point " illuminate" area yang sama yang menciptakan suatu area pemenuhan umum, yang mana meningkatkan kumpulan throughput. Stasiun di dalam area pemenuhan yang umum yang secara otomatis berhubungan dengan access point itu adalah lebih sedikit terisi dan menyediakan mutu sinyal yang terbaik.

Seperti digambarkan di dalam **Gambar 7.16**, stasiun yang sama dibagi antara access point dalam rangka sama-sama berbagi beban antara semua access point. Efisiensi dimaksimalkan



Gambar 7.16 Load Balancing

7.14 Fitur Manajemen Power

Klien wireless beroperasi di dalam salah satu dari dua gaya manajemen power yang ditetapkan oleh IEEE 802.11 standar. Mode manajemen power ini adalah mode aktif, dimana biasanya disebut called continuous aware mode (CAM) dan power save, yang mana biasanya disebut po\w save polling (PSP) mode. Memelihara power menggunakan suatu mode power-saving terutama bagi para pemakai mobil yang laptops atau PDAS berjalan pada baterei. Memperpanjang hidup baterei ini mengijinkan pemakai untuk tetap bangun dan menjalankan lebih panjang tanpa suatupengisian ulang. Wireless LAN cards dapat menarik suatu jumlah penting power dari baterei saat di dalam CAM yang mana mengapa penyimpanan power fitur adalah tercakup di standard 802.11 .

7.14.1 Continuous aware mode

Continuous aware mode menjadi pengaturan selama yang mana klien wireless menggunakan power penuh, tidak " tidur," dan secara konstan di (dalam) komunikasi reguler dengan access point. Suatu komputer yang tinggal bertahan diisi ke dalam suatu ARUS BOLAK-BALIK menggerakkan saluran [yang] secara terus-menerus seperti suatu server atau desktop harus di-set untuk CAM. Di bawah keadaan ini, tidak ada alasan untuk mempunyai PC Card memelihara power.

7.14.2 Power Save Polling

Penggunaan mode power save polling(PSP) mengijinkan suatu klien wireless untuk " tidur." Dengan tidur, berarti bahwa klien yang benar-benar mati powernya untuk jumlah waktu sangat pendek, barangkali suatu pecahan kecil suatu detik. Tidur ini adalah cukup waktu untuk menyimpan suatu penting jumlah power pada klien wireless dalam putaran, power yang disimpan oleh klien wireless memungkinkan suatu laptop komputer pemakai, sebagai contoh, untuk bekerja untuk suatu periode waktu yang lebih panjang pada baterei, membuat pemakai lebih produktif. Ketika menggunakan PSP, klien wireless bertindak dengan cara yang berbeda di dalam ketetapan layanan dasar dan ketetapan layanan dasar mandiri. Satu persamaan di dalam perilaku dari suatu BSS ke suatu IBSS mengirimkan dan menerima rambu. Proses yang beroperasi selama mode PSP, di keduanya BSS dan IBSS, diuraikan di bawah. Ingatlah bahwa proses ini terjadi berulang kali per detik. Fakta itu mengijinkan wireless LAN anda untuk memelihara hubungannya, tetapi juga menyebabkan suatu jumlah ongkos exploitasi tambahan. Seorang administrator perlu mempertimbangkan ongkos exploitasi ini dalam perencanaan untuk kebutuhan dari para pemakai wireless LAN.

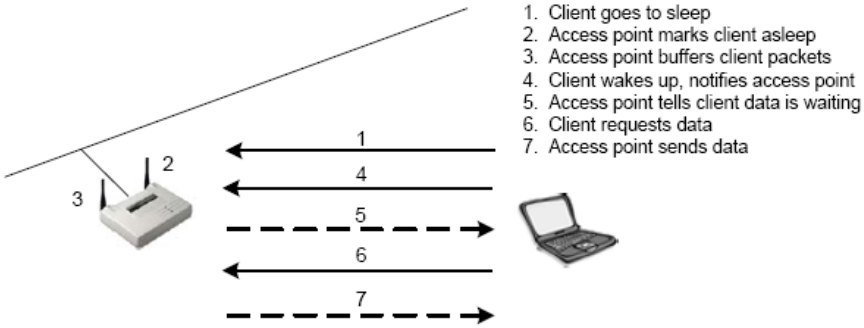
7.14.3 PSP in an Independent Basic Service Set

Power menyimpan proses komunikasi di dalam suatu IBSS adalah sangat berbeda dibanding ketika power menyimpan mode yang digunakan di dalam suatu BSS. Suatu IBSS tidak berisi suatu access point, maka tidak ada alat ke paket buffer. Oleh karena itu, tiap-tiap stasiun harus menunjukkan paket buffer dirinya sendiri kepada semua stasiun yang lain di dalam Jaringan Ad Hoc. Stasiun mengubah pengiriman beacon pada suatu jaringan IBSS dengan menggunakan metoda bervariasi, masing-masing tergantung pada pabrik.

Kapan stasiun menggunakan power saving mode, ada masa waktu menghubungi] suatu jendela ATIM , selama masing-masing stasiun secara penuh terjaga dan siap untuk menerima frame data. *Ad hoc traffic indication message(ATIM)* adalah fram*e* unicast yang digunakan oleh stasiun untuk memberitahu stasiun lain yang ada datanya diperuntukkan kepada stasion itu dan stasion itu tinggal bertahan terjaga cukup panjang untuk menerima itu. ATIM dan beacon kedua-duanya dikirim sepanjang jendela ATIM. Proses yang diikuti oleh stasiun dalam rangka melewati lalu lintas adalah:

Stasiun disinkronkan melalui beacon sehingga bekerja sebelum jendela ATIM mulai.

Jendela ATIM mulai, stasiun mengirimkan beacon dan kemudian stasiun mengirimkan frame ATIM yang memberitahu stasiun yang tentang lalu lintas buffer. Stasiun yang menerima frame ATIM sepanjang jendela ATIM menerima frame data. Jika tidak ada frame ATIM, stasiun kembali untuk istirahat. Jendela ATIM menutup, dan stasiun mulai mentransmisikan frame data. Setelah frame data yang menerima, stasiun kembali untuk istirahat menunggu jendela ATIM yang berikutnya. Proses PSP Ini untuk suatu IBSS digambarkan di dalam **Gambar 7.17.**



Gambar 7.17. PSP Mode in an IBSS

Sebagai administrator LAN wireless, kita harus mengetahui apa yang mempengaruhi fitur manajemen power yang berakibat pada performance, hidup baterei, lalu lintas bradcast LAN, dan lain lain Di contohkan di atas, efek bisa menjadi penting

7.15 Kesimpulan

Ada beberapa langkah-langkah dasar yang terpenting dari desain dan administrasi wireless LAN. Dalam mengadministrasi wireless LAN, pemahaman dari konsep-konsep ini akan membantu dalam me manage jaringan Wireless LAN. Salah satu diantaranya adalah menempatkan perangkat Wireless LAN. Proses "mendengar" antara perangkat yang dipasang disebut juga dengan proses *scanning.* Scanning terjadi sebelum proses lainnya, dikarenakan scanning adalah bagaimana klien menemukan network. Ada dua tipe scanning : pasif scanning dan aktif scanning. Setelah proses scanning maka selanjutnya adalah proses autentifikasi dan penggabungan antara perangkat tersebut. Teknologi VPN menyediakan rata-rata untuk dengan aman memancarkan data antar network-devices (di) atas suatu data pinjaman mengangkut medium. Biasanya digunakan untuk menghubungkan remote jaringan atau komputer bagi suatu server perusahaan via Internet.

7.16 SOAL

1. Jelaskan secara singkat mengenai SSID (Service Set Identifier) dan Beacons ?
2. Jelaskan secara singkat tentang Passive Scanning dan Active Scanning ?

3. Sebutkan tiga status yang berbeda dalam proses asosiasi dan pengesahan ?
4. Sebutkan dan jelaskan tiga cara konfigurasi wireless LAN ?
5. Sebutkan tiga tingkatan keamanan dalam teknologi VPN ?

Bab 8. Layer MAC dan Phisik

8.1 Sasaran

- Mengerti dan memahami konsep-konsep seputar penyusunan wireless LAN berikut :
    - Perbedaaan antara wireless LAN dan penyusunan Ethernet
    - Protocol layer 3 yang didukung oleh wireless LAN
- Menentukan mode operasi yang terlibat pada pergerakan trafik data melewati wireless LAN
    - Fungsi koordinasi terdistribusi (Distributed Coordination Function DCF)
    - Fungsi koordinasi titik (Point Coordination Function PCF)
    - CSMA/CA dibandingkan dengan CSMA/CD
    - Pembagian ruang
    - RTS/CTS
    - Seleksi rata-rata dinamis
    - Coding dan modulasi

Kami menyebutkan dibagian awal buku ini bagaimana kebanyakan teknologi di semua wireless LAN itu adalah sama, tetapi dari pendekatan pabrikan dan penggunaan ditunjukkan bahwa teknologi tersebut berbeda. Pada bab ini kita akan mendiskusikan beberapa dari karakteristik layer fisik dan MAC dari wireless LAN yang sangat umum dipakai pada semua produk wireless LAN, berkenaan dengan pabrikan. Kita akan menjelaskan perbedaan antara pembagian-pembagian Ethernet dan wireless LAN dan bagaimana wireless LAN menghindarkan tabrakan. Kita akan melewati bagaimana pemancar wireless LAN berkomunikasi dengan pemancar yang lain pada keadaan yang normal, kemudian bagaimana penanganan tabrakan terjadi pada wireless LAN.

Hal ini sangat penting untuk anda sebagai administrator wireless LAN untuk mengetahui tingakatan ini secara detail yang pada keperluannya mampu untuk mengkonfgurasi secara benar dan mengatur sebuah access point, sebaik sebagaimana mendiagnosa dan menangani permasalahan yang sangat umum pada wireless LAN.

8.2 Bagaimana wireless LAN berkomunikasi

Pada tujuannya, untuk mengerti bagaimana mengkonfigurasi dan mengatur sebuah wireless LAN, seorang administrator harus mengerti hal-hal yang berkaitan dengan komunikasi yang dikonfigurasi pada alat dan bagaimana melaksanakan hal-hal tersebut. Pada tujuannya untuk memperkirakan keluaran melewati wireless LAN, salah satunya harus mengerti dampak dari hal-hal ini dan penanganan tabrakan pada system keluaran. Pada bagian ini akan disampaikan sebuah dasar pengertian dari berbagai macam hal-hal yang bisa dikonfigurasi dan dampaknya pada kecepatan jaringan.

8.3 Perbandingan Frame Wireless LAN dengan Susunan Ethernet

Sekali sebuah wireless client bergabung dalam sebuah jaringan, client dan sisa dari jaringan akan berkomunikasi dengan bergerak pada susunan melalui jaringan, pada hampir semua cara yang sama sebagimana jaringan IEEE 802 yang lain. Untuk menjernihkan kesalahpahaman yang umum, wireless LAN tidak menggunakan susunan Ethernet 802.3. syarat wireless Ethernet adalah bagaimana agak terjadi kesalahan penomeran. Susunan Wireless LAN mengandung lebih banyak informasi dari pada susunan pada Ethernet yang umum. Struktur yang serbenarnya dari susunan wireless LAN dibandingkan dengan susunan Ethernet adalah melewati bidang dari ujian CWNA sebaik pekerjaan seorang administrator wireless LAN.

Beberapa hal untuk kita sadari bahwa banyak sekali tipe dari susunan IEEE 802, tetapi hanya ada satu tipe untuk susunan wireless. Dengan susunan Ethernet 802.3, sekali dipilih oleh administrator jaringan, tipe susunan yang sama dipakai untuk mengirim semua data melewati kabel sebagaimana dengan wireless. Susunan wireless semuanya dikonfigurasi dengan format frame yang sama secara keseluruhan. Ethernet 802.3 mempunyai ukuran susunan maksimum 1518 bytes sebelum pembagian yang diperlukan secara standar, tapi bisa naik menjadi 9000 bytes (ditujukan sebagai “susunan jumbo”). Susunan yang lebih besar dari 1518 bytes akan dibagi untuk memenuhi standar. Susunan wireless LAN mempunyai ukuran maksimum susunan sebesar 2346 bytes sebelum standar 802.11 membutuhkan pembagian. Bagaimanapun, susunan wireless dibagi secara umum pada 1518 byte dengan access point sesuai pada transfer data antara media Ethernet kabel (802.3) dan wireless (802.11).

Sebuah pokok persoalan yang sering didiskusikan adalah preamble dan header dari susunan wireless. Ada sedikit bagian dari informasi yang penting untuk diketahui –

terutama jika anda akan melakukan analisa protocol wireless. Preamble (sebuah rangakaian 1 dan 0 yang digunakan untuk sinkronisasi pada awal dari tiap susunan) selalu dikirimkan pada kecepatan 1Mbps untuk menyediakan data rate yang umum yang semua penerima bisa mengartikan. Ada dua jenis panjang dari preamble (yang biasa di namakan PLCP preamble) – panjang (128 bits) dan pendek (56 bits). Sangat penting sekali untuk menandai pada setiap akhir dari hubungan wireless menggunakan tipe preamble yang sama. Standar 802.11b membutuhkan dukungan dari preamble yang panjang dan menyediakan pilihan untuk preamble yang pendek yang pada tujuannya untuk memperbaiki efisiensi jaringan ketika mengirimkan traffic tipe yang khusus misalkan VoIP. Setelah preamble dikirim, header (yang biasa dinamakan PLCP header) dikirim. Untuk preamble yang panjang, pramble dan header keduanya dikirim pada kecepatan 1 Mbps. Untuk preamble yang pendek, preamble dikirim pada pada kecepatan 1 Mbps dan header dikirim pada kecepatan 2 Mbps. Data rate atau "DR" menempati header menentukan rata-rata pada data yang akan ditransmisikan. Setelah mengirim header, pengirim kemudian akan mengganti data rate pada dimanapun header ditentukan. Dasar pemikiran yang sama dipergunakan pada mercu suar, yang juga mengirimkan pada kecepatan 1 Mbps untuk alasan yang sama.

Ada tiga kategori yang berbeda dari susunan yang dihasilkan antara batas-batas dari format frame ini secara keseluruhan. Tiga kategori susunan ini dan tipe dari setiap kategori adalah :

- Management Frame
    - Association request frame
    - Association response frame
    - Reassociation request frame
    - Reassociation response frame
    - Probe request frame
    - Probe response frame
    - Beacon frame
    - ATIM frame
    - Disassociation frame
    - Authentication frame
    - Deauthentication frame

- Control Frame
    - Request to send (RTS)
    - Clear to send (CTS)
    - Acknowledgement (ACK)
    - Power-Save Poll
    - Contention-Free End (CF End)
    - CF End + CF Ack
- Data Frame

Tipe tertentu dari susunan (yang disebutkan diatas) menggunakan bidang tertentu antara tipe susunan keseluruhan dari susunan wireless. Apa yang administrator wireless LAN perlu ketahui adalah bahwa wireless LAN mendukung secara praktis semua protocol-protokol layer 3-7 – IP, IPX, NetBEUI, AppleTalk, RIP, DNS, FTP, etc. perbedaan utama dari susunan Ethernet 802.3 diimplementasikan pada Media Access Control (MAC) sub layer dari Layer Data Link dan semua layer fisik. Protocol-protokol layer atas secara mudah betul-betul dipertimbangkan alat-alat yang penting oleh layer 2 susunan wireless.

8.4 Penanganan Tabrakan (Collision Handling)

Sejak frekwensi radio dipakai sebagai sebuah medium yang di pakai secara umum., wireless LAN harus berhubungan dengan kemungkinan tabrakan mirip dengan wired Lan traditional juga. Perbedaannya adalah bahwa, pada wireless LAN, tidak ada hal yang menunjukkan melalui pemancar pengiriman mana yang ditentukan bahwa sebenarnya terjadi tabrakan. Hal ini sangat tidak mungkin untuk mendeteksi sebuah tabrakan pada sebuah wireless LAN. Untuk alasan ini, wireless Lan, memakai protokol Carrier Sense Multiple Access / *Collision Avoidance*, yang juga dikenal sebagi CSMA/CA. CSMA/CA adalah sesuatu yang mempunyai kemiripan dengan protocol CSMA/CD, yang sangat terkenal pada jaringan Ethernet.

Perbedaan yang besar antara CSMA/CA dan CSMA/CD adalah bahwa CSMA/CA menghindari tabrakan dan menggunakan acknowledgements (ACKs) dari pada mengambil keputusan untuk menggunakan medium ketika tabrakan terjadi. Penggunaan acknowledgement, atau ACKs, bekerja dengan cara yang sederhana. Ketika sebuah

pemancar wireless mengirim sebuah paket, pemancar penerima mengirimkan kembali sebuah ACK sekali yang biasanya pemancar menerima paket. Jika pemancar pengirim tidak menerima sebuah ACK, pemancar pengirim menganggap bahwa terjadi tabrakan dan mengirimkan data kembali.

CSMA/CA, menambahkan sejumlah besar data control yang dipakai di wireless Lan, menyebabkan kelebihan yang menggunakan kira-kira 50% bandwidth yang ada pada wireless LAN. Kelebihan ini, ditambah dengan penambahan kelebihan dari protocol seperti RTS/CTS yang mempertinggi penghindaran tabrakan, bertanggung jawab untuk keluaran yang sebenarnya dari kira-kira 5.0-5.5 Mbps pada sebuah tipe wireless LAN 802.11b yang dirata-rata pada 11 Mbps. CSMA/CD juga menghasilkan kelebihan, tapi hanya sekitar 30% pada sebuah penggunaan jaringan rata-rata. Ketika sebuah jaringan Ethernet menjadi padat, CSMA/CD bisa menyebabkan kelebihan sampai 70%, ketika kepadatan sebuah jaringan wireless menunjukkan beberapa angka keluaran sekitar 50%-55%.

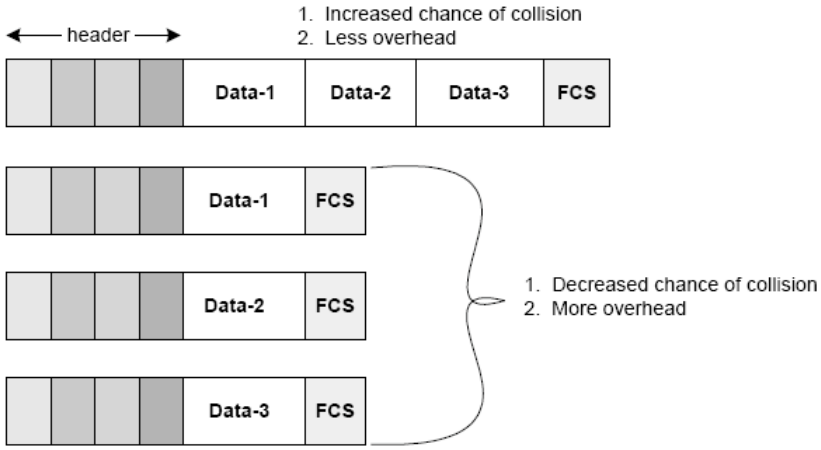
Protocol CSMA/CA menghindari kemungkinan dari tabrakan diantara pemancar yang dibagi pada medium dengan menggunakan sebuah waktu kembali acak (random back of time) jika fisik pemancar atau pengertian logika mekanik menunjukkan sebuah medium yang sibuk. Periode waktu secara cepat mengikuti medium yang sibuk adalah ketika kemungkinan yang tinggi dari tabrakan terjadi, terutama pada pamakaian yang tinggi. Pada saat ini, banyak pemancar menunggu medium pada saat idle dan akan berusaha memancarkan kembali pada saat yang sama. Sekali jika medium mengalami idle, sebuah waktu kembali acak menunda sebuah pemancar untuk mengirimkan sebuah susunan (frame), memperkecil kemungkinan bahwa pemancar akan bertabrakan.

8.5 Fragmentation

Pembagian paket-paket menjadi bagian yang lebih pendek menambah batasan protocol dan mengurangi effisiensi protocol (menurunkan keluaran jaringan) ketika tidak ada error yang diamati, tetapi mengurangi waktu yang terbuang pada pengiriman kembali jika error terjadi. Paket-paket yang besar mempunyai kemungkinan yang besar untuk tabrakan pada jaringan; oleh karena itu, sebuah metode untuk mengubah ukuran potongan paket sangat diperlukan. Standar IEEE 802.11 menyediakan dukungan untuk memecah-mecah.

Dengan mengurangi panjang dari setiap paket, kemungkinan gangguan selama pengiriman paket bisa dikurang, sebagaimana diilustrasikan pada figure 8.1. ada timbal balik yang harus dibuat antara rata-rata error paket yang rendah yang dicapai dengan menggunakan paket-paket pendek, dan peningkatan kelebihan dari susunan yang lebih Pada jaringan karena pemotongan. Setiap potong membutuhkan header-header dan ACK sendiri, jadi pendekatan dari pemotongan tingkatan juga merupakan sebuah pendekatan dari sejumlah kelebihan dengan paket yang diasosiasikan dengan setiap paket yang dikirimkan.

Pemancar tidak pernah memecah-mecah pancaran yang berulang dan menyiarkan susunan-susunan, tetapi hanya satu kesatuan pancaran dengan tujuan untuk memperkenalkan kelebihan yang tidak diperlukan pada jaringan. Menemukan pengaturan pemotongan untuk memaksimalkan keluaran pada jaringan pada sebuah jaringan 802.11 adalah sebuah bagian yang penting dari pengaturan sebuah wireless LAN. Tetap pada pikiran bahwa sebuah susunan 1518 byte adalah susunan terbesar yang bisa melintasi bagian wireless LAN tanpa melalui pemotongan.



Gambar 8.1 Fragmentation

Salah satu cara untuk menggunakan pemotongan untuk memperbaiki keluaran jaringan pada beberapa waktu dari error-error paket yang berat adalah untuk mengawasi rata-rata error paket pada jarigan dan mengatur tingkatan pemotongan secara manual. Sebagaima sebuah latihan yang direkomendasikan, anda harus mengawasi jaringan pada keluaran setiap waktu pada suatu hari untuk melihat apa akibat dari dampak

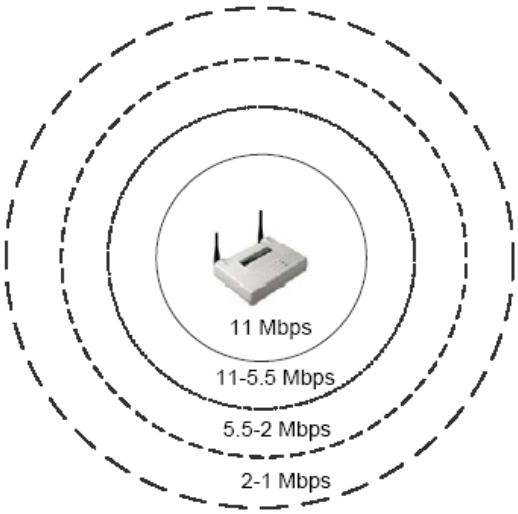
pengaturan pemotongan yang akan dilakukan pada beberapa waktu. Metode yang lain untuk pengaturan adalah untuk menkonfigurasi permulaan pemotongan.

Jika jaringan anda adalah terbiasa dengan sebuah rata-rata error paket yang tinggi (paket-peket cacat), naikkan permulaan pemotongan pada pemancar client dan atau access point (tergantunga pada unit-unit mana pengaturan yang dipakai pada peralatan anda yang khusus). Dimulai dengan nilai maksimum dan berangsur-angsur menurunkan ukuran permulaan pemotongan sampai sebuah perbaikan muncul. Jika pemotongan digunakan, jaringan akan terbiasa dengan perubahan kecepatan karena mendatangkan kelebihan dengan pemotongan. Suatu waktu perubahan ini dapat diterima dengan tujuan untuk melawan keluaran tertinggi karena sebuah penurunan pada error-error paket dan pengurutan pada mengiriman sinyal kembali.

8.6 Dynamic Rate Shifting / DRS

Seleksi rata-rata yang dapat berubah (Adaptive <atau otomatis> Rate Selection / ARS) dan pengangkatan rata-rata secara dinamis (Dynamic Rate Shifting / DRS) kedua-duanya adalah syarat yang digunakan untuk menggambarkan metode dari pengaturan kecepatan secara dinamis pada client-client wireless LAN. Pengaturan kecepatan ini terjadi sebagaimana jarak antara client dan access point meningkat atau sebagai peningkatan ganguan. Hal ini sangat penting sekali bagi administrator jairngan untuk mengerti bagaimana fungsi ini bekerja dengan tujuan untuk merencanakan keluaran jaringan, ukuran bagian terkecil, keluaran-keluaran tenaga dari access point dan pemancar, serta keamanan.

Pancaran system spectrum yang moderen didesain untuk membuat lompatan-lompatan yang berlainan yang hanya untuk menentukan rata-rata data, yang semisal 1,2,5.5, dan 11 Mbps. Sebagaimana jarak meningkat antara access point dan sebuah pemancar, panjang sinyal akan menurun pada suatu titik ketika rata-rata data sekarang tidak bisa diatur. Ketika penurunan kekuatan sinyal terjadi, unit pengiriman akan menjatuhkan rata-rata data pada rata-rata data berikutnya yang ditentukan secara rendah, katakan saja dari 11 Mbps menjadi 5.5 Mbps atau dari 2 Mbps menjadi 1 Mbps. **gambar 8.2** mengilistrasikan bahwa, sebagaimana jarak dari access point meningkat rata-rata data akan menurun.



Gambar 8.2 Dynamic Rate Shifting

Sebuah system wireless LAN tidak akan pernah menjatuhkan kecepatan dari 11 Mbps menjadi 10 Mbps, sebagai contoh, sejak 10 Mbps adalah bukan rata-rata data yang ditentukan. Metode dari pembuatan lompatan-lompatan yang berbeda tersebut biasanya dinamakan ARS atau DRS, tergantung dari pabrikannya. FHSS dan DSSS keduanya menggunakan DRS, dan IEEE 802.11, IEEE 802.11b, HomeRF dan standar OpenAir menggunakan metode tersebut.

8.7 Distributed Coordination Function / DCF

Fungsi koordinasi terdistribusi (DCF) adalah sebuah metode akses yang ditentukan pada standar 802.11 yang membolehkan semua pemancar pada sebuah wireless LAN untuk menghadapi akses pada media transmisi yang dibagikan (RF) menggunakan protocol CSMA/CA. Pada hal ini, media transmisi adalah sebuah bagian dari berkas frekwensi radio yang digunakan wireless LAN untuk mengirim data. Bagian-bagian pembetulan dasar (Basic Service Sets / BSS), bagian-bagian pembetulan yang luas (Extended Service Sets / ESS), dan bagian-bagian pembetulan dasar yang berdiri sendiri (Independent Basic Service Sets / IBSS) semunya bisa menggunakan mode DCF. Access point pada bagian-bagian pembetulan ini bertindak dengan cara yang sama sebagaimana dasar IEEE 802.3 kabel yang terhubung untuk mengirimkan datanya, dan DCF adalah mode dimana access point mengirimkan datanya.

8.8 Point Coordination Function

Fungsi koordinasi titik (Point Coordination Function / PCF) adalah sebuah mode pengiriman yang menyediakan pengiriman susunan bebas isi (contention-free) . pada sebuah wireless LAN dengan menggunakan mekanisme polling. PCF mempunyai keuntungan dari memberikan jaminan untuk mengetahui sejumlah hal yang tersembunyi jadi bahwa aplikasi-aplikasi membutuhkan QoS (suara atau gambar untuk contoh) yang bisa digunakan. Ketika menggunakan PCF, access point pada sebuah wireless LAN membentuk polling. Karena alasan ini, sebuah ad hoc jaringan tidak bisa memakai PCF, karena sebuah ad hoc jaringan tidak mempunyai access point untuk melakukan polling.

8.8.1 Proses PCF

Pertama kali, sebuah pemancar wireless harus memberitahukan access point bahwa pemancar mampu untuk menjawab mengambil pertanyaan, kemudian access point menanyakan, atau mengambil pertanyaan, setiap pemancar wireless untuk melihat apakah pemancar perlu untuk mengirimkan sebuah susunan data melalui jaringan. PCF, melalui polling, menghasilkan sejumlah penting kelebihan pada sebuah wireless LAN.

Ketika menggunakan PCF, hanya satu access point yang harus menyala pada setiap saluran non-overlaping untuk menghindari kecepatan degradasi karena gangguan co-channel.CF bisa digunakan tanpa PCF, tapi PCF tidak bisa digunakan tanpa DCF. Kita akan menjelaskan bagaimana dua mode co-exist ini sebagaimana kita mendiskusikan penempatan susunan. DCF adalah mudah berubah karena desainnya yang contention-based, begitu juga PCF, dengan desain, membatasi penggunaan secara bebas pada jaringan wireless dengan menambahkan penambahan kelebihan dari susunan-susunan poling.

8.9 Interframe Spacing

Penempatan dalam susunan tidak kedengaran seperti sesuatu yang bagi seorang administrator perlu ketahui. Bagaimanapun, jika anda tidak mengerti tipe dari penempatan dalam susunan, secara efektif anda tidak akan bisa memahami RTS/CTS, yang sangat membantu anda untuk mengatasi permasalahan, atau DCF dan PCF, yang secara manual terkonfigrasi pada access point. Fungsi-fungsi ini keduanya terintegrasi

pada proses komunikasi terus-menerus pada sebuah wireless LAN. Pertama, kita akan mendefinisikan setiap tipe dari susuna-susunan dalam ruang (InterFrame Space / IFS), dan kemudian kita akan menjelaskan bagaimana setiap tipe bekerja pada wireless LAN.

Sebagaimana kita sudah kita pelajari ketika kita membahas tentang beacons, semua pemancar pada sebuah wireless LAN adalah sinkronisasi waktu (time-sincronized). Semua pemancar pada sebuah wireless LAN sangat efektif "menandai" waktu pada sinkronisasi satu dengan yang lain. Penyususan adalah syarat kita menggunakan untuk menunjukkan stadarisasi ruang waktu yang digunakan pada semua wireless LAN 802.11.

8.9.1 Tiga Tipe Dari Spacing

Diantaranya ada tiga interval penempatan utama (penempatan penyusunan): SIFS, DIFS, and PIFS. Setip tipe penyusunan tersebut digunakan oleh wireless LAN yang juga untuk mengirimkan tipe pesan tertentu melewati jaringan atan untuk mengatur interval selama pemancar mana yang dihadapi untuk media pengiriman. **tabel 8.1** mengilustrasikan waktu yang sebenarnya dimana tempat penyusunan diambil untuk tiap tipe dari teknologi 802.11.

Tabel 8.1 . Interframe Spacing

IFS	**DSSS**	**FHSS**	**Diffused Infrared**
SIFS	10 uS	28 uS	7 uS
PIFS	30 uS	78 uS	15 uS
DIFS	50 uS	128 uS	23 uS

Penempatan penyusunan diuukur pada microsecond dan digunakan untuk menunda sebuah akses pemancar ke media dan untuk menyediakan tingkatan prioritas yang bermacam-macam. Pada sebuah jaringan wireless, semuanya disinkronisasi dan semua pemancar dan access point menggunakan setandar sejumlah waktu (ruang) untuk membentuk bermacam-macam tugas. Setiap titik mengetahui penempatan ini dan menggunakannya secara tepat. Sebuah bagian ruang standar ditentukan untuk DSSS, FHSS, dan Infrared yang sebagaimana anda lihat pada **tabel 8.1**. dengan menggunakan ruang ini, setiap titik mengetahui dan ketika hal ini harus membentuk sebuah aksi tertentu pada sebuah jaringan.

8.9.1.1.1.1.1.1 8.9.1.1 Sort Interframe Space (SIFS)

SIFS adalah ruang antar susunan terpendek yang ditentukan. SIFS adalah ruang waktu sebelum dan sesudah dimana tipe-tipe pesan-pesan berikut dikirim. Dibawah ini adalah sebuah daftar yang tidak lengkap.

- RTS – Request-to-Send Frame, digunakan untuk menyediakan media oleh pemancar.
- CTS – Clear-to-Send Frame, digunakan sebagai sebuah tanggapan oleh access point pada susunan RTS yang dihasilkan oleh sebuah pemancar dengan tujuan untuk meyakinkan semua pemancar sudah menghentikan pancaran.
- ACK – Acknowledgement Frame digunakan untuk memberitahukan pengiriman pemancar-pemancar yang datanya datang pada format yang mudah di baca pada pemancar penerima

SIFS menyediakan prioritas tingkatan tertinggi pada sebuah wireless LAN. Alasan untuk SIFS menggunakan prioritas tertinggi adalah bahwa pemancar-pemancar secara konstan mendengarkan media (indra pembawa / carrier sense) menunggu sebuah media yang kosong. Sekali media telah kosong, setiap pemancar harus menunggu sejumlah waktu yang diberikan sebelum melakukan proses dengan sebuah pengiriman. Lama waktu dari pemancar yang harus menunggu ditentukan oleh fungsi yang diperlukan oleh pemancar untuk membentuknya. Setiap fungsi pada sebuah jaringan wireless jatuh pada kategori sebuah penempatan. Tugas yang merupakan prioritas tertinggi jatuh pada kategori SIFS. Jika sebuah pemancar hanya harus menunggu sebuah periode waktu yang pendek setelah media sudah kosong untuk melakukan transmisinya, hal tersebut akan mempunyai prioritas melampaui pemancar untuk menuggu pada periode waktu yang lama. SIFS digunakan untuk fungsi yang membutuhkan periode waktu yang sangat pendek, serta belum memerlukan prioritas yang tinggi dengan tujuan untuk menyelesaikan sasaran.

8.9.1.1.1.1.2 8.9.1.2 Point Coordination Function Interframe Space (PIFS)

Sebuah PIFS ruang antar susunan bukan merupakan jalur terpendek maupun jalur terpanjang ruang antar susunan yang ditentukan, jadi hal ini mendapatkan prioritas yand lebih dari pada DIFS dan kurang dari SIFS. Access point menggunakan sebuah ruang antar susunan PIFS hanya ketika jaringan pada mode fungsi koordinasi titik, yang secara manual dikonfigurasi oleh administrator. PIFS mempunyai durasi yang lebih pendek dari pada DIFS (lihat **tabel 8.1.**), jadi access point hanya akan mencari kendali dari media sebelum pemancar-pemancar yang lain berhadapan pada mode fungsi koordinasi terdistribusi (DCF). PCF hanya bekerja dengan DCF, tidak sebagai mode operasional yang berdiri sendiri maka, sekali access point telah selesai melakukan polling, pemancar-pemacar yang lain akan melanjutkan untuk menghadapi madia pengiriman dengan menggunakan mode DCF.

8.9.1.1.1.1.3 8.9.1.3 Distributed Coordination Function Interframe Space (DIFS)

DIFS adalah ruang antar susunan yang paling panjang yang ditentukan dan digunakan secara default pada semua 802.11-pamancar-pemancar yang menggunakan fungsi koordinasi terdistribusi. Setiap pamancar pada jaringan yang menggunakan mode DCF dibutuhkan untuk menunggu sampai DIFS sudah habis masa waktunya sebelum semua pemancar berhadapan pada jaringan. Semua pemancar berpoerasi menurut DCF yang menggunakan DIFS untuk mengirimkan susunan datanya dan mengatur susunan-susunan. Ruangang ini membuat pengiriman susunan ini mempunyai prioritas yang rendah dari pada pengiriman-pengiriman yang berdasarkan PCF. Meskipun semua pemancar menggap media tersebut bersih dan berubah-ubah memulai mengirimkan secara terus-menerus setelah DIFS (yang dapat menyebabkan tabrakan), setiap pemancar menggunakan sebuah algoritma memutar kembali secara acak untuk menentukan berapa lama waktu untuk menunggu sebelum mengirimkan data tersebut.

Periode waktu yang secara langsung mengikuti DIFS ditunjukkan sebagai periode perkiraan (contention period / CP). Semua pemancar pada mode DCF menggunakan algoritma memutar kembali secara acak selama periode perkiraan. Selama proses pemutaran kembali secara acak, sebuah pemancar memilih sebuh angka acak dan mengalikannya dengan lubang waktu

untuk mendapatkan panjang dari waktu tunggu. Pemancar-pemancar menghitung lubang waktu ini satu-persatu, membantuk sebuah penilaian saluran yang bersih clear channe assessment (CCA) setelah setiap lubang waktu untuk melihat apakah medianya sedang sibuk. Kapanpun waktu memutar kembali pada pemancar telah berakhir telebih dahulu, pemancar tersebut mengerjakan sebuah CCA, dan menyediakan media yang kosong, dan kemudian memulai pengiriman.

Sekali pemancar yang pertama telah memulai pengiriman semua pemancar-pemancar memperkirakan bahwa media tersebut sedang sibuk, dan mengingat sejumlah sisa waktu mundur acaknya dari CP yang sebelumnya. Beberapa sisa waktu ini digunakan pada penggantian pengambilan nomer acak yang lain selama CP yang berikutnya. Proses ini menjamin akses yang baik pada media diantara semua pemancar.

Sekali periode mundur secara acak berakhir, pemancar pengirim mengirimkan datanya dan menerima kembali ACK dari pemancar penerima. Semua proses ini kemudian akan berulang-ulang. Karena dengan alasan bahwa kebanyakan pemancar-pemancar akan memilih nomer-nomer acak yang berbeda, menghilangkan tabrakan-tabrakan. Bagaimanapun, hal ini sangat penting untuk diingat bahwa tabrakan-tabrakan sering terjadi pada wireless Lan, tapi hal tersebut tidak bisa dideteksi secara langsung. Tabrakan bisa dianggap bahwa ack tidak diterima kembali dari pemancar tujuan.

8.9.2 Lubang Waktu

Sebuah lubang waktu, dimana yang diprogram sebelumnya pada radio pada mode yang sama sebagai SIFS, PIFS, dan susunan waktu DIFS, adalah standar periode waktu pada sebuah jaringan wireless. Lobang waktu digunakan pada metode yang sama sebagai waktu kedua yang digunakan. Sebuah node wireless menandai lubang waktu seperti sebuah detik-detik tanda waktu. Lubang waktu ini ditentukan oleh teknologi wireless LAN yang digunakan.

- Celah waktu FHSS = 50μS
- Celah waktu DSSS = 20μS
- Celah waktu Infrared = 8μS

Dengan catatan sebagai berikut

PIFS = SIFS + 1 lubang waktu

DIFS = PIFS + 1 lubang waktu

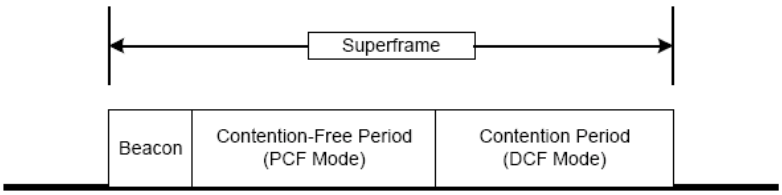
Dengan catatan yang lain juga bahwa FHSS telah tercatat sebagai lubang waktu yang lama, waktu DIFS, waktu PIFS dari pada DSSS. Waktu lama ini termasuk pada FHSS yang berlebih, yang menurunkan keluaran.

8.9.3 Proses Komunikasi

Setelah anda paham dengan proses PIFS yang dijelaskan diatas, hal tersebut sebagai pemikiran bahwa access point akan selalu mengatur media, sejak access point tidak harus menunggu DIFS, tetapi dilakukan oleh pemancar. Hal ini akan menjadi benar, kecuali dari keberadaan apa yang dsebut dengan sebuah susunan super, sebuah susunan super adalah sebuah periode waktu, dan hal tersebut mengandung tiga bagian :

1. Beacon
2. Contention Free Period (CFP)
3. Contention Period

Sebuah diagram dari susuan super (superframe) ditunjukkan pada **Gambar 8.3**. tujuan dari superframe adalah untuk memberikan ketenangan, co-existence yang baik antara client-client mode PCF dan DCF pada jaringan, memberikan QoS pada beberapa, tetapi tidak pada yang lain.



Gambar 8.3 Superframe

Dan juga, perlu diingant bahwa PIFS, dan karena superframe, hanya terjadi ketika

1. Jaringan pada mode fungsi koordinasi titik
2. Access point telah dikonfigurasi untuk melakukan polling
3. Client-client wireless telah dikonfigurasi untuk memberitahukan pada access point bahwa mereka telah siap dipolling.

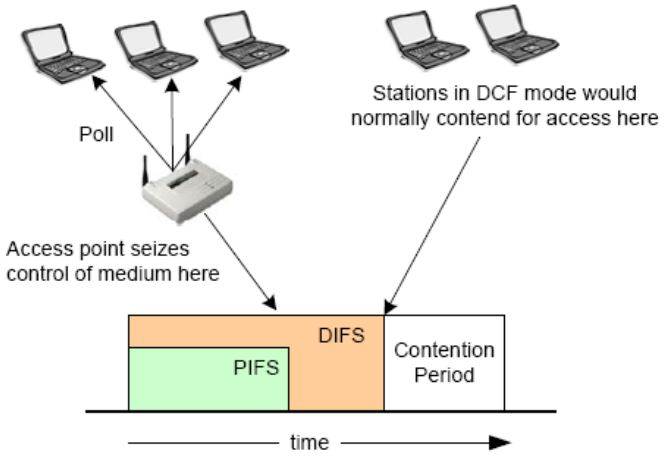
Karena itu, jika kita mengawali dari sebuah titik awal hipotetik pada sebuah jaringan yang mempunyai access point yang telah dikonfigurasi pada mode PCF, dan beberapa client-client dikonfigurasi untuk polling, prosesnya ditunjukkan sebagai berikut.

1. access point memancarkan sebuah beacon.
2. selama dengan anggapan pada periode yang bebes, access point mempolling pemancar-pemancar untuk melihat apakah ada pemancar yang perlu untuk mengirim data.
3. jika pemancar perlu untuk mengirimkan data, maka akan mengirimkan satu susunan pada access point yang pada tanggapannya untuk polling access point.
4. jika sebuah pemancar tidak merasa perlu untuk mengirimkan data, maka akan kembali pada sebuah susunan yang null pada access point yang pada tanggapannya untuk polling access point.
5. polling akan berlanjut melalui anggapan periode yang bebas.
6. sekali periode yang bebas dinyatakan berakhir dan awal periode dinyatakan, access point tidak bisa melakukan poll pada pemancar. Selama periode yang dinyatakan, pemancar menggunakan mode DCF untuk menghadapi media dan access point yang menggunakan mode DCF.
7. superframe berakhir dengan seketika pada CP, dan superframe yang baru akan berawal dengan CFP berikutnya.

Berpikir pada CFP seperti menggunakan sebuah “kebijakan akses yang diatur” dan CP seperti menggunakan sebuah “kebijakan akses secara acak”. Selama CFP, access point adalah pengaturan yang lengkanp dari semua fungsi-

fungsi pada jaringan wireless, dimana selama CP, pemancar-pemancar memperkirakan dan mengacak pengaturan tambahan melalui media. Access point menggunakan PIFS, yang lebih pendek dari pada DIFS, dengan tujuan untuk menangkap media sebelum ada client yang menggunakan mode DCF melakukannya. Sejak access point menangkap media dan mulai melakukan pengiriman polling selama CFP, client-client DCF merasakan media yang sibuk dan menunggu untuk mengirim. Setelah CFP dan CP berlangsung, selama dimana semua pamancar-pemancar menggunakan mode DCF bisa menghadapi media dan access point beralih pada mode DCF.

Gambar 8.4 mengilustrasikan sebuah waktu tempuh yang pendek untuk sebuah wireless LAN menggunakan mode DCF dan PCF.



Gambar 8.4 Waktu tempuh mode DCF/PCF

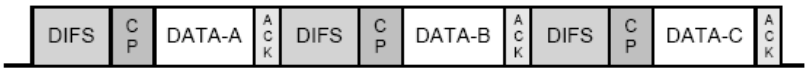
Prosesnya sederhana ketika sebuah wireless LAN hanya pada mode DCF, karena tidak ada polling dan, karena itu, tidak ada superframe. Proses ini ditunjukkan sebagai berikut :

1. pemancar menunggu DIFS sampai batas waktu
2. selama CP, yang secara cepat mengikuti DIFS, pemancar-pemancar memperkirakan waktu kembali acaknya berdasar pada sebuah angka yang acak dikalikan dengan lubang waktu.
3. pemancar-pemancar menandai waktu acaknya dengan setiap melewati lubang waktu, mengecek media (CCA) pada akhir setiap lubang waktu.

Pemancar akan dengan waktu terpendek akan dapat menguasai media terlebih dahulu.

4. sebuah pemancar mengirimkan datanya.
5. pemancar penerima menerima data dan mengunggu sebuah SIFS sebelum mengembalikan sebuah ACK kembali ke pemancar yang mengirimkan datanya.
6. pemancar pengirim menerima ACK dan proses dimulai dari awal dengan sebuah DIFS yang baru.

Gambar 8.5 mengilustrasikan sebuah garis waktu untuk sebuah wireless LAN mode DCF. Tatap dalam pikiran bahwa garis waktu ini adalah sepanjang beberapa milidetik. Dan proses keseluruhannya terjadi berkali-kali setiap detik.



Gambar 8.5 Garis waktu DCF

8.10 Request to Send/ Clear to Send (RTS/CTS)

Ada 2 jenis mekanisme pembawa yang digunakan dalam jaringan wireless. Yang pertama adalah *physical carrier sense*. Fungsi dari physical carrier sense adalah mengecek kekuatan sinyal, disebut Received Sinyal Strength Indicator (RSSI), pada RF pembawa sinyal untuk melihat apakah ada sesuatu yang sedang dipancarkan. Yang kedua adalah, *virtual carrier sense.* Virtual carrier sense bekerja dengan menggunakan bagian yang disebut Network Allocator Vector (NAV), yang berperan seperti waktu pada station. Jika station akan mem-broadcast tujuannya untuk menggunakan jaringan, station akan mengirim frame ke station tujuan, yang akan mengeset bagian NAV pada semua station memeriksa frame dalam bentuk kebutuhan waktu untuk melengkapi transmisinya, juga mengembalikan frame ACK. Pada yang demikian, station manapun dapat menyediakan penggunaan jaringan untuk waktu tertentu. Virtual carrier sense diimplementasikan dengan protokol RTS/CTS.

Protokol RTS/CTS adalah perluasan dari protokol CSMA/CA. sebagai administrator wireless LAN, kita dapat memanfaatkan penggunaan protokol untuk

menyelesaikan masalah seperti Hidden Node (dibahas pada bab 9, Troubleshooting). Menggunakan RTS/CTS mengijinkan station untuk mem-broadcast tujuannya untuk mengirim data melalui jaringan.

Seperti yang bisa dibayangkan berdasar deskrips diatas, RTS/CTS akan menyebabkan masalah khusus jaringan. Untuk alasan ini, RTS/CTS dimatikan secara default pada wireles LAN. Jika kita telah berpengalaman dengan sekumpulan collision/tabrakan yang tidak biasa pada wireless LAN kita (ditunjukkan dengan semakin lambat dan sedikitnya througput) menggunakan RTS/CTS dapat meningkatkan aliran lalu lintas pada jaringan dengan mengurangi jumlah coallision/tabrakan. Menggunakan RTS/CTS tidak seharusnya digunakan sembarangan. RTS/CTS harus dikonfigurasi setelah mempelajari benar-benar collision pada jaringan, throughput, kelambatan, dll

---

.

Beberapa perusahaan tidak mengijinkan administrator untuk mengubah setting station RTS/CTS (dan setting-setting lainnya), kecuali mereka memperoleh password khusus dari perusahaan. Secara default, administrator tidak diijinkan mengakses fitur pada software station driver. Normalnya, tidak akan mudah mendapatkan password tersebut. Perusahaan biasanya akan memberikan seminar mengenai produk mereka pada administarator selama 1-2 hari sebelum mereka mengijinkan administrator untuk mengisi paperwork untuk memperoleh password yang dibutuhkan.

Proses hansdshake mempunyai 4 cara handshake menggunakan RTS/CTS. Pendeknya, station transmisi mem-broadcast RTS, diikuti dengan reply CTS dari station penerima, keduanya bersama-sama menuju akses point. Selanjutnya, station transmisi mengirim data sisanya melalui akses point menuju station penerima, yang secara langsung dijawab dengan frame acknowledgment, atau ACK. Proses ini digunakan untuk tiap frame yang dikirim melalui jaringan wireless.

8.10.1 Konfigurasi RTS/CTS

Ada 3 setting yang utama pada access point dan node untuk RTS/CTS :

- Off (mati)
- On (nyala)

- On with threshold (nyala dengan threshold)

Ketika RTS/CTS dinyalakan (on), tiap paket yang berjalan dalam jaringan wireless diadakan dan dibersihkan antara node utama pentransmisi dan penerima untuk melakukan transmisi, membentuk kumpulan yang berlebih dan menghasilkan throughput yang kurang. Secara umum, RTS/CTS seharusnya hanya digunakan untuk mendiagnosis masalah jaringan dan hanya jika ada paket yang sangat besar yang mengalir melalui jaringan wireless, yang jarang terjadi.

Sedang, setting "On with threshold" mengijinkan administrator untuk mengontrol paket mana (ukuran yang tepat disebut threshold) yang diadakan dan dibersihkan untuk dikirim oleh station, karena collision / tabrakan mempengaruhi paket yang lebih besar daripada yang lebih kecil. Kita bisa mengeset nilai threshold untuk bekerja hanya ketika node akan mengirim paket melalui ukuran yang tepat. Setting ini mengijinkan kita untuk meng-costumize setting RTS/CTS pada lalu lintas data jaringan dan mengoptimalkan throughput wireless LAN kita ketika mencegah suatu masalah seperti Hidden Node.

8.11 Modulasi

Modulasi, fungsi layer physical, merupakan proses dimana transceiver radio mempersiapkan sinyal digital didalam NIC untuk transmisi melalui gelombang udara. Modulasi adalah proses menambahkan data dengan carrier dengan merubah ampitudo frekuensi, atau fase dari arrier pada pengontrol setelah mengetahui banyak perbedaan dari bermacam-macam modulasi yang digunakan wireless LAN akan sangat berguna ketika berusaha membangun jaringan piece-by-piece yang compatible.

Diatas menunjukkan detail dari modulasi dan jenis spreading code digunakan dengan frekuensi hopping dan direct sequence wireless LAN pada band ISM 2.4 GHz. Differential Binary Phase Shift Keting (DBPSK), Differential Quadrature Phase Shift Keying (DQPSK), dan Gaussian Frequency Shift Keying (GFSK) adalah jenis-jenis modulasi yang digunakan oleh produk 802.11 dan 802.11b yang dipasarkan saat ini. Barker code dan Complimentary Code Keying (CCK) adalah jenis dari spreading code yang digunakan pada 802.11 dan 802.11b wireless LAN.

Karena kecepatan transmisi lebih tinggi dikhususkan (seperti ketika system menggunakan DRS), tehnik modulasi berubah agar menghasilkan data throughput yang lebih. Sebagai contoh, 802.11g dan 802.11a melakukan pengkususan peralatan wireless LAN menggunakan Orthogonal Frequency Division Multiplexing (OFDM), mengijinkan kecepatan sampai 54 Mbps, yang peningkatannya mencapai 11 Mbps ditetapkan oleh 802.11.b Gambar 8.10 menunjukkan jenia modulasi yang digunakan untuk jaringan 802.11a. Standard 802.11g menyediakan kemampuan backward dengan mendukung CCK coding dan bahkan mendukung Packet Binary Convolution Coding (PBCC) sebagai pilihan. Bluetooth dan HomeRF adalah dua-duanya tehnologi FHSS yang menggunakan tehnologi modulasi GFSK pada band ISM 2.4 GHz.

OFDM (Orthogonal Frequancy Division Multiplexing) adalah tehnik komunikasi yang membagi channel komunikasi ke jumlah dari space frequency band yang sama. Subcarrier membawa bagian dari informasi usere yang ditransmisikan pada tiap band. Tiap subcarrier adalah orthogonal (tidak tergantung satu sama lain) dengan tiap subcarrier lainnya, yang merupakan perbedaaan OFDM dengan frequency umum yang biasa digunakan, yaitu FDM (Frequency Division Multiplexing).

8.12 Kesimpulan

Sasaran yang ingin dicapai dalam bagian ini adalah mengerti dan memahami konsep-konsep seputar penyusunan wireless LAN dan Menentukan mode operasi yang terlibat pada pergerakan trafik data melewati wireless LAN. Sekali sebuah wireless client bergabung dalam sebuah jaringan, client dan sisa dari jaringan akan berkomunikasi dengan bergerak pada susunan melalui jaringan. Ada tiga kategori yang berbeda dari susunan yang dihasilkan antara batas-batas dari format frame ini secara keseluruhan. Tiga kategori susunan ini dan tipe dari setiap kategori adalah :Management Frame, Control Frame dan Data Frame. Untuk menangani tabrakan (Collision Handling) dalah dengan menggunakan protokol Carrier Sense Multiple Access / *Collision Avoidance*, yang juga dikenal sebagi CSMA/CA. Pembagian paket-paket menjadi bagian yang lebih pendek menambah batasan protocol dan mengurangi effisiensi protocol (menurunkan keluaran jaringan) ketika tidak ada error yang diamati, tetapi mengurangi waktu yang terbuang pada pengiriman kembali jika error terjadi. Seleksi rata-rata yang dapat berubah (Adaptive <atau otomatis> Rate Selection / ARS) dan

pengangkatan rata-rata secara dinamis (Dynamic Rate Shifting / DRS) kedua-duanya adalah syarat yang digunakan untuk menggambarkan metode dari pengaturan kecepatan secara dinamis pada client-client wireless LAN.

8.13 SOAL

1. Sebutkan tiga kategori dari susunan yang dihasilkan antara batas – batas dari format frame secara keseluruhan berikut dengan contohnya ?
2. Apa protokol yang digunakan untuk menangani tabrakan antar paket dalam komunikasi Wireless ?
3. Apa pengertian Distributed Coordination Function ?
4. Jelaskan secara singkat mengenai proses Point Coordination Function ?
5. Sebutkan dan jelaskan secara singkat tiga tipe dari Interframe Spacing ?

Bab 9. Troubleshooting Instalasi

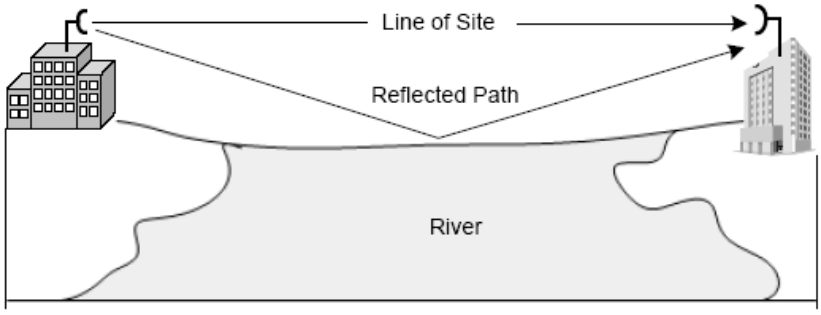
Seperti jaringan tradisional wired yang mempunyai tantangan selama implementasi, Wireless LAN juga mempunyai gambaran mereka sendiri tentang tantangan, sebagian besar berhadapan dengan perilaku dari sinyal RF. Di bab ini, kita akan mendiskusikan rintangan yang semakin umum ke implementasi yang sukses dari suatu Wireless LAN, dan bagaimana cara troubleshoot nya. Ada metoda yang berbeda dari menemukan ketika tantangan ada, ini dan masing-masing dari tantangan yang dibahas mempunyai perbaikan nya dan workarounds.

Tantangan untuk menerapkan semua Wireless LAN yang dibahas di sini dianggap sebagai oleh banyak orang sebagai permasalahan yang dapat terjadi di dalam manapun instalasi Wireless LAN, dan, oleh karena itu, dapat dihindarkan oleh perencanaan saksama dan hanya sedang sadar bahwa permasalahan ini dapat dan akan terjadi.

9.1 Multipath

Jika anda akan mengingat dari Bab 2, RF Fundamentals, ada dua jenis garis arah (LOS). Pertama,, ada LOS visuil, yang mana mata manusia lihat. Los visuil adalah test pertama dan paling dasar. jika kita dapat melihat penerima RF dari titik instalasi dari pemancar RF, kemudian anda mempunyai garis arah visuil. Ke dua, dan berbeda dari LOS yang visuil, garis arah RF. RF LOS adalah apa yang alat RF mu dapat " lihat".

Multipath digambarkan sebagai komposisi dari suatu salinan sinyal yang utama yang lebih atau medan disebabkan oleh pemantulan dari object penerima dan pemancar. Penundaan pada saat tertentu bahwa sinyal yang utama tiba bahwa sinyal terakhir dicerminkan yang datang dikenal sebagai penundaan secara menyebar.



Gambar 9.1 Multipath

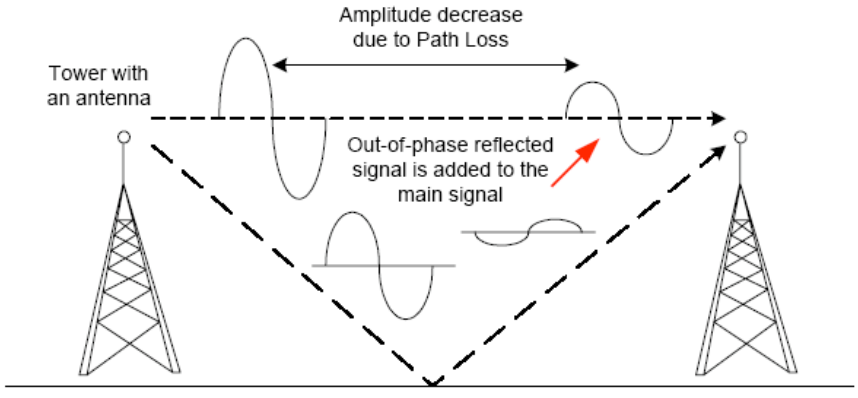
9.1.1 Effects of Multipath

Multipath dapat menyebabkan beberapa kondisi-kondisi yang berbeda, semua dari yang dapat mempengaruhi transmisi dari sinyal RF dengan cara yang berbeda. Kondisi-Kondisi meliputi:

- Sinyal Amplitude yang dikurangi (downfade)
- Korupsi
- Nulling Sinyal
- Amplitude yang ditingkatkan (upfade)

9.1.1.1 Sinyal Amplitude

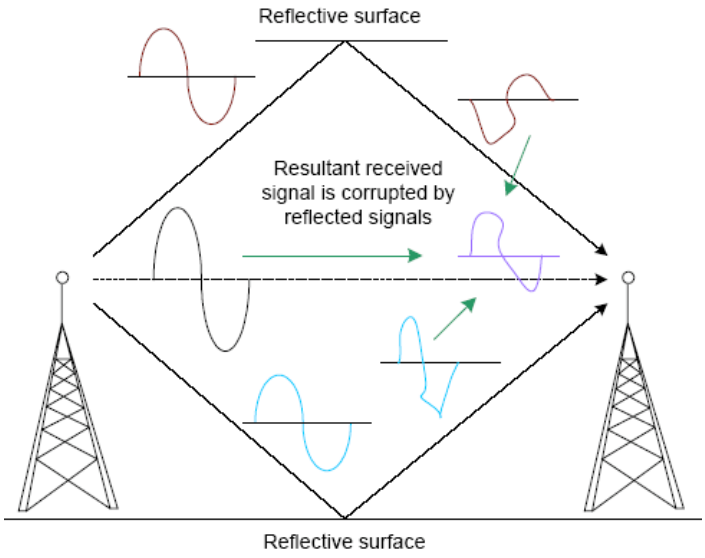
Ketika suatu gelombang RF tiba di penerima, banyak gelombang pantul yang tiba dalam waktu yang sama dari arah yang berbeda. Kombinasi dari amplitudo gelombang ini adalah adiptip RF terhadap gelombang yang utama. Gelombang yang dicerminkan, jika tak satu fase dengan gelombang utama, dapat menyebabkan amplitudo sinyal akan dikurangi di penerima, seperti digambarkan di **Gambar 9.2**. Kejadian ini adalah biasanya dikenal sebagai downfade dan harus dipertimbangkan dengan seksama ketika pelaksanaan suatu survei penglihatan dan antenna pemilihan yang sesuai.



Gambar 9.2 Downfade

9.1.1.2 Korupsi

Sinyal yang hilang dalam kaitannya dengan multipath dapat terjadi sebagai hasil yang sama dari gejala yang menyebabkan amplitudo yang berkurang, tetapi untuk tingkat yang lebih besar. Kapan gelombang pantul tiba dengan tidak satu fase penerima dengan gelombang yang utama, seperti digambarkan di **Gambar 9.3**, mereka dapat menyebabkan gelombang tersbut berkurang di amplitudo nya. Pengurangan amplitudo sedemikian hingga penerima cukup sensitif untuk mendeteksi banyaknya informasi dari gelombang yang diteruskan, tetapi tidak semua.



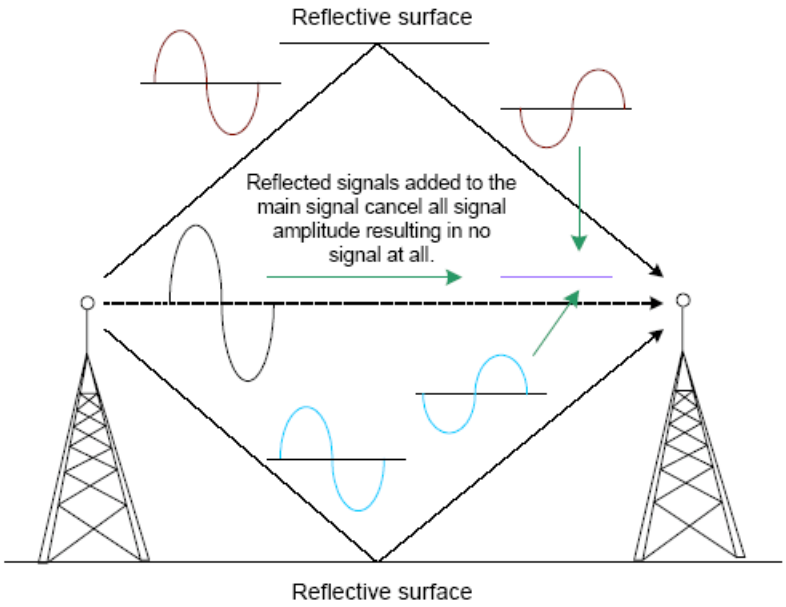
Gambar 9.3 RF Signal Corruption

Dalam . beberapa kasus, sinyal untuk menyiarkan perbandingan (SNR) secara umum sangatlah rendah, di mana sinyal itu sendiri sangat dekat. Penerima tidak mampu dengan jelas menerjemahkan sinyal informasi, menyebabkan data yang diterima tersebut hanya ada yang hilang. Korupsi dari data ini akan menugaskan pemancar untuk mengirimkan kembali data, meningkatkan i dan mengurangi throughput di wireless LAN.

9.1.1.3 Nulling

Kondisi yang dikenal sebagai kondisi Nulling batal terjadi ketika satu atau lebih gelombang pantul tiba di penerima out-of phase dengan gelombang

yang utama dengan amplitudonya. Seperti digambarkan di **Gambar 9.4**, kapan gelombang pantul menuju out-of phase dengan gelombang yang utama di penerima, kondisi dapat membatalkan atau "null" keseluruhan dalam sinyal RF, mencakup gelombang yang utama.



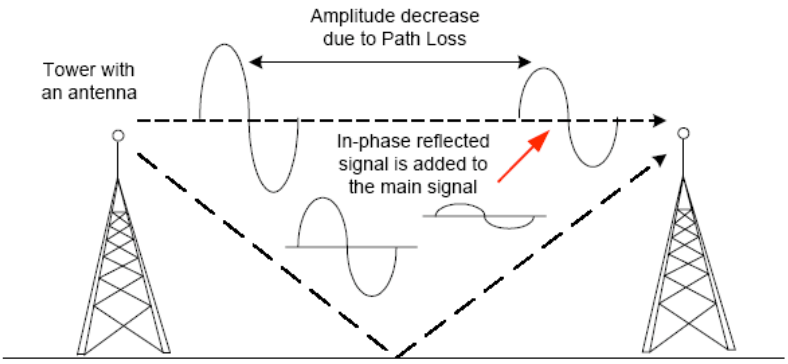
Gambar 9.4 RF Signal Nulling

Ketika Nulling terjadi, melakukan transimisi ulang tidak akan menyelesaikan masalah. Transmitter, Receiver, dan obyek harus dipindahkan. Terkadang satu atau lebih diantaranya harus di relokasi untuk menghindari efek dari Nulling.

9.1.1.4 Sinyal Amplitude yang ditingkatkan.

Kondisi –kondisi mulitpath dapat juga menyebabkan amplitudo sinyal dapat bertambah meskipun tidak adanya gelombang pantul. Upfade adalah istilah yang digunakan untuk menjelaskan. ketika multipath menyebabkan sinyal RF menjadi semakin kuat. Upfade, sebagai digambarkan di **Gambar 9.5**. terjadi pada sinyal yang dipantulkan yang datang di penerima dengan sinyal utama. Sama halnya dengan sinyal yang berkurang / turun, semua gelombang ini aditip pada sinyal utama. Selain itu multipath tidak menyebabkan sinyal yang menjangkau penerima lebih kuat daripada yang

dipancarkan sinyal ketika sinyal meninggalkan alat pemancar. Jika multipath terjadi demikian maka dapat membuat aditip pada sinyal utama, total sinyal yang menjangkau penerima akan menjadi lebih kuat dari sinyal yang terjadi tanpa adanya multipath.



Gambar 9.5 Upfade

penting memahami bahwa sinyal RF yang diterima dapat tidak lebih besar daripada sinyal yang ditransmisikan pada *free space* (istilah ini sering disebut sebagai *path loss*). *Parh loss* merupakan akibat dari hilangnya amplitudo pada sinyal pada saat ditransmisikan pada ruang terbuka.

Path loss disebabkan oleh dua faktor, yang pertama yaitu jarak antara pemancar dan penerima, dan yang kedua adalah ukuran dari celah yang diperoleh.

9.1.2 Troubleshooting Multipath

Suatu tahap di atau gelombang RF tak sefase tidak bisa dilihat, sehingga kita harus melihat efek dari multipath untuk tujuan mendeteksi kejadian nya. Ketika melakukan suatu kalkulasi anggaran mata rantai, untuk tujuan menemukan betapa banyak keluaran tenaga anda akan harus mempunyai suatu mata rantai yang sukses antara lokasi, anda mungkin mengkalkulasi suatu tingkatan daya keluaran yang perlu bekerja, tetapi tidak. Kejadian seperti itu adalah satu arah untuk menentukan multipath itu sedang terjadi.

Metoda lain yang umum dari menemukan multipath adalah untuk men/cari lubang pemenuhan RF dalam suatu survei lokasi (dibahas di Bab 11). Lubang ini

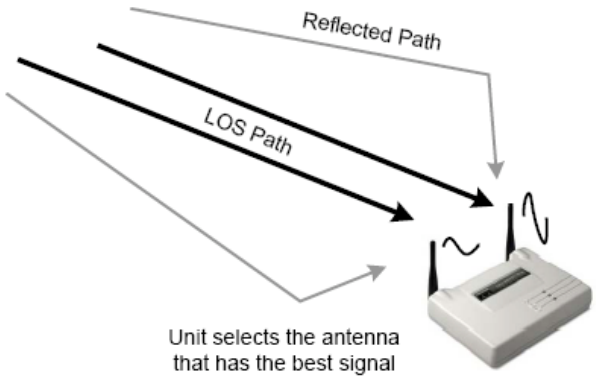
diciptakan baik melalui ketiadaan pemenuhan dan oleh multipath pemantulan yang batalkan sinyal yang utama. Pemahaman sumber dari multipath adalah rumit untuk menghapuskan barang kepunyaan nya. Multipath adalah disebabkan oleh dicerminkan ombak RF, sehingga rintangan yang dengan mudah cerminkan ombak RF, seperti metal buta,, badan tentang air, dan atap metal, harus dipindahkan dari atau dihindarkan di alur sinyal jika mungkin.. Prosedur ini boleh meliputi bergerakkan pemancaran, dan antenna penerima. Multipath paling umum adalah masalah wireless LAN. Pengurus dan installers berhadapan dengan multipath sehari-hari.

Bahkan para pemakai wireless LAN sebab mereka sering mengalami permasalahan dengan multipath. Para pemakai boleh menjelajahi ke dalam suatu area dengan multipath yang tinggi, tidak mengetahui mengapa sinyal RF mereka telah turun.

Solusi untuk Multipath Antenna dipikirkan untuk tujuan penyeimbangan multipath. Dengan menggunakan berbagai antenna, masukan, dan penerima untuk tujuan mengganti kerugian untuk kondisi-kondisi yang menyebabkan multipath. Ada empat jenis, yang mana salah satunya sebagian besar digunakan di wireless Lan. Seperti diuraikan dibawah :

- Diversity antenna - tidak aktif.
  - Antenna Multiple dengan single input.
  - Jarang digunakan.
- Menswitch Diversity.
  - Antenna Multiple di berbagai penerima.
  - Penerima Switches berdasakanr pada kekuatan sinyal.
- Switching Diversity antenna - aktip..
  - Used oleh kebanyakan pabrikan WLAN.
  - Antenna Multiple di berbagai input penerima yang tunggal.
  - Sinyal diterima sampai hanya satu antenna pada waktu yang sama.
- Diversity tahap.
  - Paten dari teknologi.
  - Tahap *adjust* dari sinyal untuk tujuan memelihara mutu sinyal.
- Diversity transmisi.
  - Used oleh kebanyakan pabrikan WLAN.

- Transmits ke luar dari antenna digunakan untuk resepsi.
- Dapat mengubah antenna untuk transmisi secara beranting.
- Unit A dapat memancarkan atau menerima, tetapi bukan kedua-duanya secara bersamaan.



Gambar 9.6 Antenna Diversity

Keaneka ragaman antenna terdiri dari yang berikut karakteristik yang bekerja sama untuk mengganti kerugian untuk barang kepunyaan dari multipath:

1) Keaneka ragaman antenna gunakan berbagai antenna di berbagai masukan untuk membawa suatu sinyal ke penerima yang tunggal.
2) Sinyal RF yang datang diterima sampai satu antenna pada waktu yang sama. Menerima radio adalah secara konstan sampling sinyal yang berikutnya dari antenna kedua-duanya untuk menentukan sinyal yang menjadi suatu mutu yang lebih tinggi. Menerima radio kemudian pilih untuk menerima sinyal mutu yang lebih tinggi.
3) Radio memancarkan sinyal yang berikutnya nya ke luar dari antenna yang adalah terakhir digunakan untuk menerima suatu sinyal yang datang sebab diterima sinyal adalah suatu sinyal mutu yang lebih tinggi dibanding dari antenna yang lain. Jika radio memancarkan kembali suatu sinyal, akan mengubah antenna sampai suatu transmisi yang sukses dibuat.
4) Akhirnya, masing-masing antenna dapat digunakan untuk memancarkan atau menerima, tetapi bukan kedua-duanya pada waktu yang sama. Hanya satu antenna mungkin digunakan pada waktu yang sama, dan antenna itu

boleh hanya memancarkan atau menerima, tetapi bukan kedua-duanya, di setiap sekejap/saat tertentu.

Kebanyakan access point di wireless Lan masa kini dibangun dengan antenna yang rangkap untuk persisnya tujuan ini: untuk mengganti kerugian untuk menurunkan multipath terhadap mutu sinyal dan throughput.

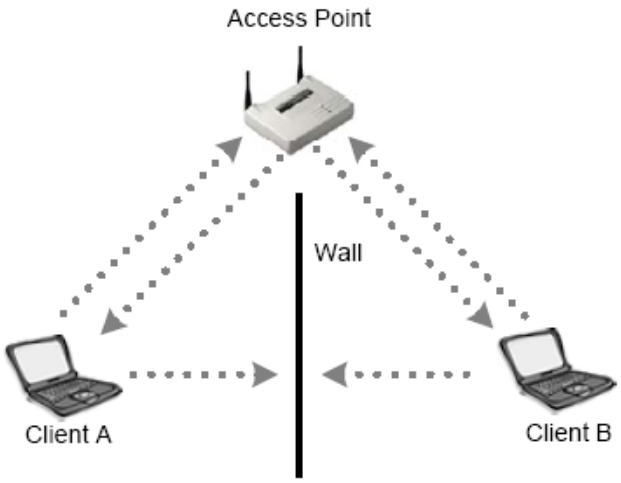
9.2 Node Tersembunyi

Berbagai protokol akses yang buka peluang alat komputasi networked untuk berbagi suatu medium, seperti Ethernet, sungguh baik dikembangkan dan dipahami. Bagaimanapun sifat alami medium yang wireless membuat metoda tradisional dari berbagi suatu koneksi yang umum yang lebih sulit..

Pendeteksian benturan telah menyebabkan permasalahan banyak orang di networking yang wired, dan bahkan lebih-lebih untuk jaringan yang wireless. Benturan terjadi ketika dua atau lebih berbagi suatu medium komunikasi memancarkan data secara serempak. Sinyal keduanya merusak satu sama lain dan hasilnya adalah suatu kelompok fragmen paket yang yang tak terbaca. Benturan telah selalu suatu masalah untuk jaringan komputer, dan protokol paling sederhana sering tidak mengalahkan masalah ini. Protokol yang lebih rumit seperti CSMA/CA dan CSMA/CD memeriksa saluran sebelum memancarkan data. CSMA/CD adalah Ethernet protokol yang digunakan dan melibatkan pemeriksaan voltase di kawat sebelum pemancaran. Bagaimanapun, proses adalah dengan sangat lebih sulit untuk sistem yang wireless karena benturan adalah tidak bisa mendeteksi. Suatu kondisi yang dikenal sebagai masalah Node yang tersembunyi telah dikenali di sistem yang wireless dan adalah disebabkan oleh permasalahan di pendeteksian transmisi.

Node tersembunyi adalah suatu situasi yang ditemui dengan Wireless LAN di mana sedikitnya satu node mampu mendeteksi satu atau lebih Node yang lain yang dihubungkan Wireless LAN. Di situasi ini, suatu Node dapat lihat access point, tetapi tidak bisa lihat bahwa ada klien lain juga menghubungkan untuk yang sama access point dalam kaitan dengan rintangan beberapa atau sejumlah besar jarak antara gambar telanjang. Situasi ini menyebabkan masalah di akses medium yang berbagi, menyebabkan benturan antara transmisi node. Benturan ini dapat mengakibatkan

dengan mantap penurunkan throughput di Wireless LAN, seperti digambarkan di **Gambar 9.7**.



Gambar 9.7 Hidden Node

Gambar 9.7 menggambarkan suatu dinding dengan suatu access point yang duduk dalam puncak. Di sisi masing-masing dari dinding adalah suatu setasiun wireless. Setasiun wireless ini tidak bisa dengar transmisi satu sama lain, tetapi keduanya mendengar transmisi dari access point itu. Jika A setasiun sedang memancarkan suatu bingka access point, dan setasiun B tidak bisa dengar transmisi, setasiun ini B berasumsi bahwa medium harus jelas dan dapat mulai suatu transmisi tentang mengakui nya access point. Access point akan, dalam posisi ini, jadilah menerima transmisi yang sudah dimulai pada dua poin-poin dan di sana akan merupakan suatu benturan. Benturan akan transmisi kembali oleh keduanya A setasiun & B, dan lagi, karena mereka tidak bisa dengar satu sama lain, mereka akan memancarkan sesuka hati berpikir medium harus jelas. Akan ada mungkin jadilah benturan yang lain. Masalah ini diperburuk dengan Node banyak orang yang aktip di Wireless LAN yang tidak bisa dengar satu sama lain.

9.2.1 Trubleshooting Hidden Node

Gejala yang utama dari suatu Node yang tersembunyi diturunkan pangkat throughput di atas Wireless LAN. Banyak kali anda akan menemukan bahwa anda mempunyai suatu menyembunyikan Node dengan tatap muka keluhan dari para

pemakai yang dihubungkan kepada Wireless LAN untuk mendeteksi suatu melempem yang tidak biasa dari jaringan itu. Throughput mungkin dikurangi sampai 40% karena suatu masalah node tersembunyi. Karena Wireless LAN gunakan protokol CSMA/CA, mereka telah mempunyai suatu mendekati ongkos exploitasi dari 50%, tetapi, selama suatu masalah node yang tersembunyi, itu adalah mungkin untuk menghilangkan hampir separuh dari throughput pada sistem.

Sebab sifat alami suatu Wireless LAN meningkatkan mobilitas, anda boleh menghadapi suatu node yang tersembunyi pada setiap waktu, di samping suatu sempurna perancangan Wireless LAN mu. Jika seorang pemakai memindahkan komputer nya ke suatu konferensi ruang, kantor yang lain, atau ke dalam suatu data tinggal, penempatan yang baru dari node itu dapat berpotensi tersembunyi dari sisa node yang dihubungkan ke Wireless LAN.

Untuk secara proaktif troubleshoot suatu node tersembunyi, anda harus menguji untuk throughput diturunkan pangkat dan juga temukan banyak tempat yang potensial untuk suatu node yang tersembunyi sampai mungkin.

9.2.2 Solusi untuk Hidden Node

Once anda sudah melakukan troubleshooting dan menemukan bahwa ada suatu menyembunyikan masalah node, masalah node(s) harus ditempatkan; terletak. Temuan node(s) akan meliputi suatu manual mencari-cari node yang boleh jadi tidak terjangkau dari seikat yang utama tentang node. Proses ini adalah pada umumnya mencoba-coba paling baik. Sekali ketika node ini ditempatkan; terletak, ada beberapa perbaikan dan workarounds untuk masalah.

- Gunakan RTS/CTS.
- Meningkatkan power ke node.
- Mencabut rintangan.
- Pindah node

9.2.2.1 Gunakan RTS/CTS.

Protokol RTS/CTS tidaklah perlu suatu solusi untuk masalah node tersembunyi. Sebagai gantinya, ini merupakan suatu metoda dari mengurangi

dampak hal negatif yang node yang tersembunyi berakibat pada jaringan. node yang tersembunyi menyebabkan benturan yang berlebihan, yang mempunyai suatu dampak sungguh merugikan di jaringan throughput. Rts/Cts (request-to-send/clear-to-send) protokol melibatkan pengiriman paket kecil (RTS) kepada penerima yang diharapkan untuk membisikkan nya untuk mengembalikan suatu paket (CTS) pembukaan hutan medium untuk transmisi data sebelum mengirimkan muatan penghasil untung data. Proses ini menginformasikan manapun setasiun yang dekat yang data akan dikirim, selama menunda transmisinya (dan dengan demikian menghindarkan benturan). Kedua-Duanya RTS dan CTS berisi panjang transmisi data yang segera terjadi sedemikian sehingga setasiun mendengar-dengar salah satu bingkai CTS atau RTS mengetahui berapa lama transmisi akan mengambil dan ketika mereka dapat start untuk memancarkan lagi.

Ada tiga pengaturan untuk RTS/CTS di kebanyakan klien dan poin-poin akses: Terpasang, Off, dan On dengan Threshold. Pengurus jaringan harus dengan tangan mengatur RTS/CTS yang menentukan. Pengaturan Off adalah kelalaian untuk tujuan mengurangi ongkos exploitasi jaringan tak perlu disebabkan oleh protokol RTS/CTS. Menunjuk secara langsung ukuran paket yang akan mencetuskan

Penggunaan dari protokol RTS/CTS. Sejak node yang tersembunyi menyebabkan benturan, dan benturan sebagian besar mempengaruhi paket yang lebih besar, anda mungkin mampu diperdaya tersembunyi masalah node dengan menggunakan ambang pintu ukuran paket menentukan untuk RTS/CTS. Apa yang ini menentukan sangat utama mengerjakan adalah access point memancarkan semua paket yang adalah lebih besar di ukuran dibanding "x" menggunakan RTS/CTS dan untuk memancarkan semua paket yang lain tanpa RTS CTS. Jika node tersembunyi hanya mempunyai; nikmati suatu dampak throughput pada jaringan, kemudian mengaktipkan RTS CTS mungkin dapat menimbulkan efek yang merugikan pada throughput nya.

Usaha dengan menggunakan RTS/CTS di "On" sebagai test untuk melihat jika throughput terpengaruh. Jika RTS/CTS meningkatkan throughput, kemudian anda hampir bisa dipastikan menetapkan menyembunyikan masalah node. Anda akan menghadapi ongkos tambahan ketika menggunakan

RTS/CTS, tetapi throughput keseluruhan akan meningkat ketika masalah node yang tersembunyi terjadi.

9.2.2.2 MeningkatKan Power ke Nodes

Meningkatkan power (yang diukur milliwatts) dari node dapat memecahkan masalah node tersembunyi dengan mengijinkan sel disekitar masing-masing node untuk meningkatkan ukuran, mencakup semua node yang lain. Maka node yang tersembunyi adalah tidak lagi tersembunyi. Sebab Wireless LAN gunakan protokol CSMA/CA, node akan menunggu giliran mereka sebelum memberitahukan access pointnya.

9.2.2.3 Mencabut Obstacles

Meningkatkan power di node yang bergerak tidak akan bekerja, sebagai contoh, satu node yang tersembunyi terdapat dinding yang dapat mencegah komunikasi dengan node yang lain. Sangatlah sulit untuk menghilangakn obstacle, akan tetapi menghilangkan obstacle merupakan salah satu metode unutk mengatasi node yang tersembunyi. Metode ini dipakai berdasakan pada survei lokasi.

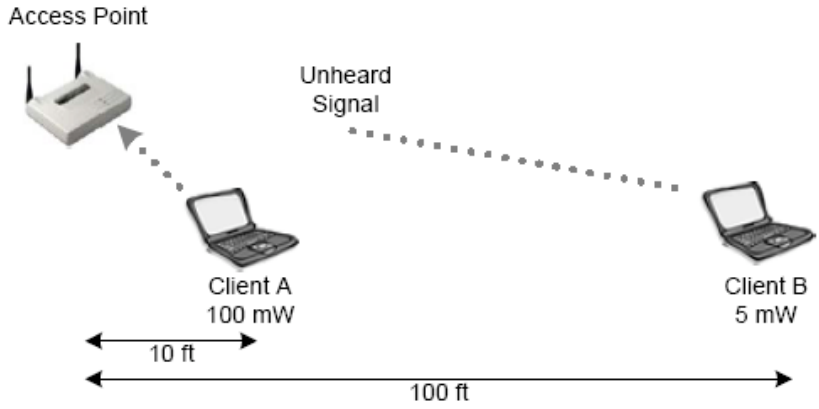
9.2.2.4 Memindahkan Node

Metoda yang lain dari memecahkan masalah node yang tersembunyi yaitu dengan memindahkan node. Jika anda telah menemukan masalah node yang tersembunyi merupakan akibat dari user yang berpindah, anda mungkin akan memaksa user tersebut untuk berpindah lagi. Alternatif yang lain yaitu dengan menggunakan access point tambahan.

9.3 Near/Far

Masalah Near/Far pada implementasi Wireless LAN diakibatkan oleh skenario di mana ada berbagai (a) node klien yang dekat pada access point dan (b) mempunyai power yang tinggi; dan kemudian sedikitnya satu klien yang (a) banyak lebih jauh dari

access point dibanding node klien yang tersebut diatas, dan (b) menggunakan sangat sedikit pancaran power dibanding node klien yang lain. Hasil dari situasi jenis ini adalah bahwa klien yang mana lebih jauh dari access point dan menggunakan lebih sedikit power, seperti digambarkan di **Gambar 9.8.**



Gambar 9.8 Near/Far

9.3.1 Troubleshooting Near/Far.

Troubleshooting masalah near/far adalah umumnya sederhana seperti pada disain jaringan, penempatan dari stasiun di jaringan yang wireless, dan daya keluaran transmisi dari tiap node. Langkah-langkah ini akan memberi administrator kunci rahasia seperti apa mungkin berlangsung dengan stasiun yang mempunyai permasalahan koneksi. Karena near/far mencegah suatu node dari yang berkomunikasi, administrator perlu memeriksa jika stasiun mempunyai pengarah dengan baik untuk wireless card dan telah dihubungkan dengan access point.

Yang berikutnya adalah penggunaan dari wireless sniffer. Wireless sniffer akan mengambil transmisi dari semua stasiun yang mendengar. Satu metoda yang sederhana dari menemukan node sinyal siapa yang tidak sedang terdengar oleh access point adalah untuk jaringan yang mencari stasiun dengan sinyal yang dalam hubungan dengan node dan access point dekat access point. Menggunakan metoda ini, harusnya tidak terlalu memakan waktu untuk menempatkan node seperti itu, tergantung pada ukuran dari jaringan dan kompleksitas yang dibangun dan

membandingkan kekuatan sinyalnya untuk dari itu node yang dekat access point dapat memecahkan masalah near/far secara wajar dengan cepat.

9.3.2 Solusi Untuk Near/Far

Walaupun masalah near/far dapat melemahkan sinyal RF, near/far adalah suatu masalah secara relatif mudah untuk berbagai situasi. Dengan memahami bahwa protokol CSMA/CA dapat memecahkan sebagian besar masalah near/far dengan tidak ada intervensi . Jika suatu node dapat mendengar node yang lain yang memancarkan, maka akan menghentikan transmisi itu sendiri. Di bawah adalah daftar perbaikan yang mudah diterapkan.

- Peningkatan pergerakan dari satu node ke node yang remote (node yang lain)
- Pengurangan daya dari node lokal
- Gerakkan node yang remote yang semakin dekat ke access point

9.4 Throughput Sistem

Throughput di suatu Wireless LAN didasarkan banyak faktor. Sebagai contoh, jumlah dan jenis gangguan berdampak pada jumlah data yang dapat dengan sukses dipancarkan. Solusi keamanan diterapkan, seperti Wired Equivalent Privacy (WEP- di Bab 10, Wireless LAN Security.

Jarak yang lebih besar antara penerima dan pemancar akan menyebabkan throughput berkurang sebab peningkatan jumlah kesalahan akan menciptakan kebutuhan transmisi itu kembali. Sistem spread spectrum modern diatur untuk membuat lompatan secara terpisah untuk ditetapkan (I, 2, 5.5, dan 11 Mbps).

Pembatasan perangkat keras akan juga mendikte tingkat tarip data. Jika suatu alat IEEE 802.11 sedang memberitahukan suatu alat IEEE 802.11b, tingkat tarip data ia dapat tidak lebih daripada 2 Mbps, di samping kemampuan 802.11b alat untuk komunikasi kan pada 11 Mbps. Dengan selalu berhubungan, throughput yang nyata akan jadilah lebih sedikit 50%, atau 1 Mbps.

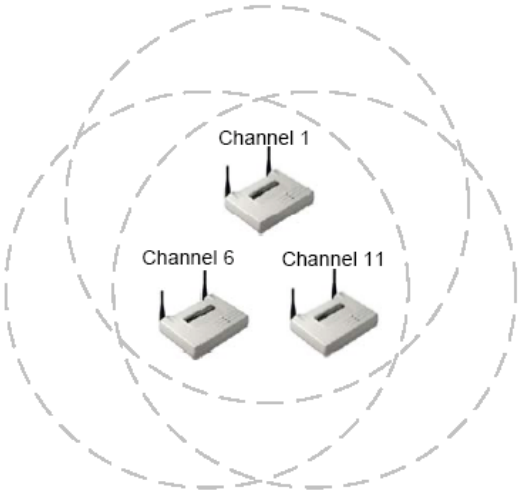
Jenis teknologi spread spectrum, DSSS atau FHSS, akan membedakan di throughput untuk dua pertimbangan yang spesifik. Pertama adalah data rate.. FHSS memenuhi salah satu standard OpenAir dan dapat memancarkan pada 800 kbps atau 1.6

Mbps, atau standard IEEE 802.11, yang mengijinkan untuk memancarkan pada 1 Mbps atau 2 Mbps. Sekarang ini, sistem DSSS mematuhi salah satu standard IEEE 802.11 atau standard 802.11b, mendukung data rate dari 1, 2, 5 5, & 11 Mbps.

Faktor lain yang membatasi throughput dari Wireless LAN meliputi protokol pada lapisan Data Link), dan paket ukuran. Paket yang lebih besar akan mengakibatkan throughput yang lebih.

9.4.1 Co-Location Throughput (Teori Vs Kenyataan)

Co-Location adalah teknik pada wireless LAN yang digunakan untuk menyediakan lebih banyak bidang dan throughput ke pemakai, dikombinasikan dengan peraturan FCC. 3 saluran ini dapat digunakan untuk co-locate berbagai access point dengan menggunakan 802.11b , seperti dapat dilihat di **Gambar 9.9**.

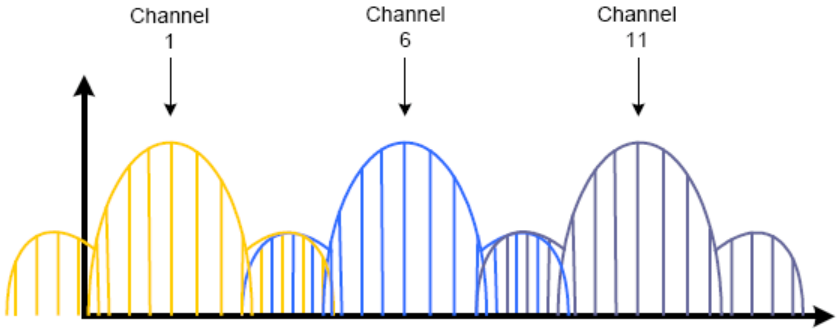


Gambar 9.9 Co-location throughput

Ketika co-locating sangat direkomendasikan bahwa anda:

- Gunakan teknologi spread spectrum yang sama untuk semua access point.
- Gunakan vendor yang sama untuk semua access point.

9.4.2 Kenyataan: Apa yang Terjadi



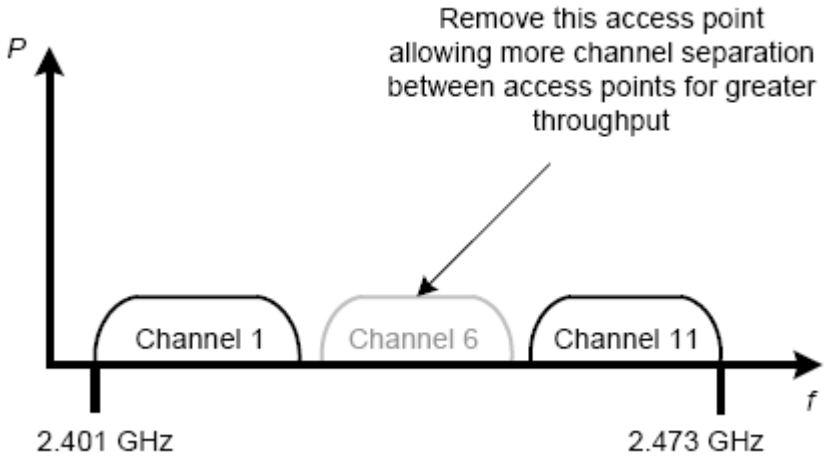
Gambar 9.10 DSSS Over Lap

Jika kita melakukan co-locate dengan tiga access point, lebih baik kita menerapkan co-location menggunakan hardware dengan merek yang sama untuk ketiga accses point. Hal ini telah ditengarai bahwa pada banyak lab yang menggunakan peralatan dari vendor yang berbeda memiliki efek negatif pada throughput dari salah satu atau lebih access point. Efek negative ini bisa saja dikarenakan perbedaan power output dan kedekatan antar accses point, tetapi juga bisa disebabkan oleh banyak faktor lainnya.

9.4.3 Solusi Untuk Permasalahan Throughput Co-location

9.4.3.1 Gunakan Dua Access Point

Salah satu pilihan, yang merupakan cara termudah adalah menggunakan channel 1 dan 11 dengan dua access point, seperti yang digambarkan pada **gambar 9.11**. Menggunakan hanya dua channel akan memastikan bahwa kita tidak mendapatkan overlap antara channel-channel yang dikarenakan kedekatan antara kedua sitem ini, lagipula tidak ada efek yang merugikan pada throughput masing-masing access point.



Gambar 9.11. Menggunakan dua access point

Sebagai perbandingan dua access point berjalan pada kapasitas maksimum yaitu 5,5 Mbps (dari kemampuan terbaik yang bisa diharapkan dari semua access point), memberikan total kapasitas hingga 11 Mbps dari jumlah throughput keduanya, sementara tiga access point menjalankan kapasitas mendekati 4 Mbps tiap access point (berkurang karena overlap channel sesungguhnya) sehingga menghasilkan total throughput hanya 12 Mbps. Untuk beberapa tujuan, bandwith ekstra sebesar 1 Mbps mungkin masih berguna, tetapi didalam sebuah lingkungan kecil, hal ini mungkin tidak praktis. Jangan lupa bahwa skenario ini hanya digunakan untuk access point yang ditempatkan pada ruang fisik yang sama untuk melayani basis klien yang sama, tetapi menggunakan channel yang berbeda. Konfigurasi ini tidak dapat diaplikasikan untuk pemakaian kembali channel, dimana channel yang berbeda secara bergantian menyebar pada suatu area untuk menghindari gangguan antar channel.

9.4.3.2 Gunakan peralatan 802.11a

Pilihan kedua, kita bisa menggunakan peralatan 802.11a yang beroperasi dengan frekuensi UNII 5 Ghz. Frekuensi UNII 5 GHz yang lebih luas daripada frekuensi ISM 2,4 GHz, memiliki tiga band yang dapat digunakan, dan tiap band memungkinkan untuk empat channel non-overlapping. Dengan menggunakan perpaduan peralatan 802.11b dan 802.11a, maka makin banyak

sistem yang bisa ditempatkan (co-located) dalam ruang yang sama tanpa takut adanya gangguan antar sistem. Dengan dua(atau tiga) sistem 802.11b yang ditempatkan pada tempat yang sama dan sampai 8 sistem 802.11a yang dapat ditempatkan pada tempat yang sama, maka berpotensi menghasilkan throughput yang sangat besar dalam ruang fisik yang sama. Alasan mengapa hanya digunakan 8 dari 12 access point yang memungkinkan dari 802.11a, adalah bahwa hanya band lower dan middle (dengan masing-masing 4 channel) yang dapat digunakan untuk indoor. Yang mana indoor adalah tempat bagi kebanyakan access point, yang secara normal hanya memungkinkan hingga 8 akses point apabila menggunakan peralatan 802.11a.

9.4.3.3 Keterangan mengenai peralatan 802.11a

Peralatan 802.11a sekarang hanya tersedia pada beberapa vendor saja, dan ia lebih mahal daripada peralatan yang menggunakan frekuensi 2,4 Ghz. Meskipun begitu frekuensi 5 GHz memiliki keuntungan pada lebih banyaknya channel yang tidak overlap daripada frekuensi 2,4 GHz (8 vs 3), memungkinkan kita untuk menerapkan penempatan akses point pada tempat yng sama lebih banyak

Yang harus diingat adalah meskipun frekuensi 2,4 GHz memungkinkan peralatan yang lebih murah, tetapi frekuensi ini lebih ramai, yang berarti kita akan dihadapkan pada masalah gangguan dari jaringan wireless terdekat lainnya. Ingat alat 802.11a dan alat 802.11b tidak kompatibel. Peralatan ini tidak melihat, mendengar atau berkomunikasi antara satu dengan lainnya dikarenakan penggunaan frekuensi yang berbeda dan perbedaan teknik modulasi.

9.4.3.4 Kesimpulan Solusi

Kenapa channel non-overlapping bisa sampai overlap? Banyak jawaban untuk pertanyaan ini; meskipun begitu, tampaknya penyebab yang paling besar adalah akses point ditempatkan terlalu dekat dengan akses point lainnya. Dengan memisahkan akses point pada jarak yang lebih jauh, overlap antar non-overlaping channel bisa dikurangi. Melihat konfigurasi ini pada sebuah

spectrum analyzer, kita bisa melihat bahwa untuk seperempat penempatan channel lebih dekat, memerlukan pemisahan channel lebih dari 3 MHz; meskipun kita agar sebagai administrator bisa melakukan hal itu, kita harus melakukan suatu tindakan.

Kita bisa memisahkan secara fisik dengan penempatan yang lebih jauh atau kita menggunakan channel yang berselisih lebih besar dari 3 MHz. Selain itu tampaknya penggunaan peralatan dari vendor yang berbeda juga menimbulkan perubahan. Mengguanakn peralatan dari vendor yang sama ternyata mengurangi overlapping daripada menggunakan peralatan dari vendor yang berbeda-beda. Fenomena ini disebabkan karena ketidak akuratan dalam radio, atau hanya karena penerapan hardware masing-masing vendor tidak diketahui.

9.5 Tipe-tipe Gangguan

Dikarenakan perilaku yang tidak dapat diprediksi pada teknologi RF, Kita harus mengetahui macam-macam gangguan RF yang mungkin mengganggu pada saat implementasi dan pengelolaan sebuah jaringan wireless. Narrowband, all-band, berkurangnya sinyal RF, dan penempatan maupun gangguan antar channel merupakan sumber masalah yang umum terjadi pada saat penerapan sebuah jaringan wireless. Pada bagian ini, kita akan membicarakan tipe-tipe gangguan ini, bagaimana akibatnya terhadap jaringan wireless, bagaimana mendeteksinya, dan pada beberapa kasus bagaimana cara mengatasinya.

9.5.1 Narrowband

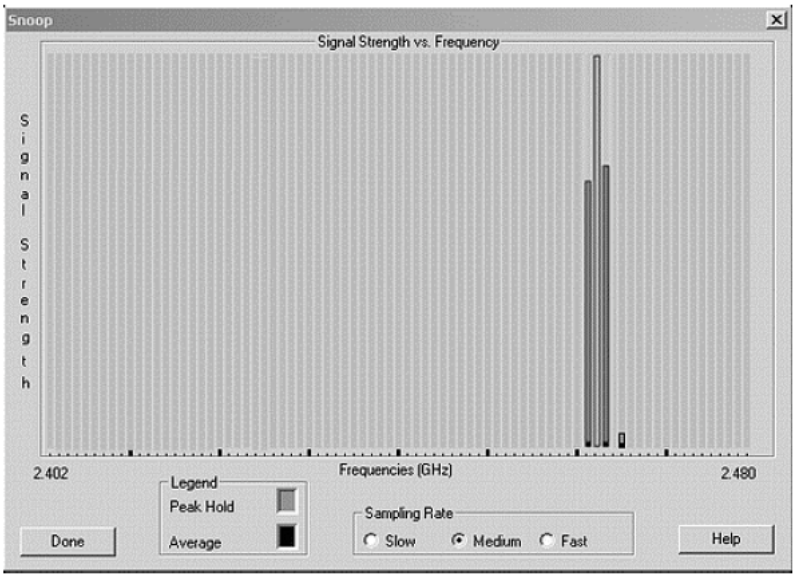
Narrowband RF pada dasarnya merupakan kebalikan dari teknologi spread spectrum. Sinyal Narrowband, bergantung pada power output, lebar frekuensi dalam spectrum, dan konsistensi, bisa mengganggu atau bahkan merusak sinyal RF yang dikeluarkan dari sebuah peralatan berteknologi spread spectrum sebagai contoh akses point. Meskipun begitu, sesuai namanya, sinyal narrowband tidak mengganggu sinyal RF pada keseluruhan band. Sehingga apabila sinyal narrowband menggangu sinyal pada channel 3, maka kita sebagai contoh gunakan channel 11, dimana kita tidak mengalami gangguan sama sekali. Sepertinya hanya

sebagian kecil saja pada channel yang diberikan yang mungkin terganggu oleh sinyal narrowband. Biasanya, hanya satu frekuensi pembawa(penambahan 1MHz dari sebuah channel 22MHz 802.11b) yang akan terganggu karena gangguan narrowband. Dihadapkan gangguan seperti ini, teknologi spread spectrum akan dapat mengatasi permasalahan ini tanpa tambahan administrasi atau konfigurasi.

Gambar 9.12. Spectrum Analyzer

Untuk mengidentifikasi gangguan narrowband, kita membutuhkan sebuah spectrum analyzer, sperti yang ditunjukkan **gambar 9.12**. Spectrum analyzer digunakan untuk mendeteksi dan mengukur sinyal narrowband RF. Bahkan alat ini bisa dibawa dengan mudah, spectrum analyzer digital dapat diperoleh dengan biaya mendekati $4000. Harga ini mungkin terlalu mahal untuk mendeteksi sumber gangguan narrowband, tetapi apabila sumber itu sungguh mengganggu jaringan mu, harga tersebut mungkin layak.

Sebagai alternatif, beberapa vendor jaringan wireless telah menerapkan sebuah software spectrum analyzer pada software driver nya. Software ini menggunakan kartu PCMCIA FHSS untuk memindai bagian yang bisa digunakan dari 2,4 GHz band ISM untuk sinyal RF. Software ini menampilkan secara grafik semua sinyal RF antara 2,400GHz dan 2,4835GHz, yang memberikan cara untuk seorang administrator ”melihat ” RF pada area tersebut, satu contoh tampilan visual yang disediakan spectrum analyzer ini tergambar pada **gambar 9.13**.



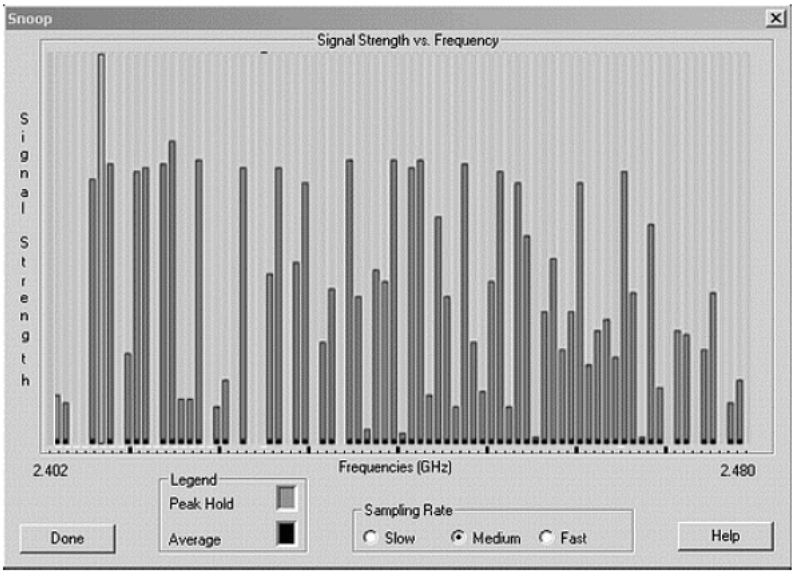
Gambar 9.13. Tampilan Visual Spectrum Analyzer

Dalam rangka untuk mengatasi gangguan narrowband RF, pertama anda harus menemukan dimana gangguan itu berasal dengan menggunakan spectrum analyzer. Semakin anda berjalan mendekati sumber sinyal RF, maka sinyal RF pada display spectrum analyzer akan tampak membesar pada amplitudonya (ukuran). Ketika sinyal RF pada layar mencapai puncak, maka kita telah mendeteksi sumbernya. Pada tahap ini anda bisa meningkirkan sumber, menutupnya, atau gunakan pengetahuan anda sebagai administrator jaringan wireless untuk mengkonfigurasi jaringan wireless anda agar dapat mengatasi secara efisien gangguan narrowband. Tentu saja terdapat beberapa pilihan untuk kategori penyelesaian terakhir, seperti mengganti channel, mengganti teknologi spread spectrum (DSSS menjadi FHSS atau 802.11b menjadi 802.11a), dan solusi lainnya yang akan kita bicarakan pada bagian selanjutnya.

9.5.2 Gangguan All-band

Gangguan All-band adalah semua sinyal yang mengganggu band RF dari akhir spectrum hingga bagian lainnya. Gangguan all-band tidak berarti hanya mengganggu keseluruhan band ISM 2,4 GHz, tetapi lebih merupakan istilah yang digunakan pada semua kasus dimana gangguan mencakup keseluruhan range yang akan kau gunakan, tanpa memperhatikan frekuensi. Teknologi seperti Bluetooth (yang berlompatan pada keseluruhan 2,4 GHz band ISM lebih dari sekali dalam

satu detik) bisa saja dan biasanya, secara signifikan mengganggu sinyal RF 802.11. Bluetooth bisa disebut sebagai gangguan all-band untuk jaringan wireless 802.11. **Gambar 9.14** menunjukkan contoh gambaran sebuah spectrum analyzer merekam gangguan all-band.



Gambar 9.14. Spectrum Analyzer merekam gangguan all-band

Sumber gangguan all-band yang mungkin didapatkan dalam rumah maupun kantor adalah sebuah oven microwave. Oven microwave tipe lama yang memiliki power yang tinggi bisa membocorkan power sebanyak satu watt kepada spectrum RF. Satu watt bukan merupakan kebocoran yang banyak untuk sebuah oven microwave 1000 watt, tetapi mempertimbangkan fakta bahwa satu watt merupakan power yang cukup besar untuk sebuah akses point biasa, anda bisa melihat bahwa hal ini menimbulkan akibat yang signifikan.Memang tidak disebutkan oven microwave akan memancarkan power kepada keseluruhan band 2,4 GHz, tetapi itu mungkin saja, tergantung pada tipe dan kondisi oven microwave tersebut. Sebuah spectrum analyzer bisa mendeteksi permasalahan semacam ini.

Ketika gangguan all-band terjadi, solusi terbaik adalah berganti teknologi, contohnya dari 802.11b (yang menggunakan band ISM 2,4GHz) menjadi 802.11a (yang menggunakan band UNII 5GHz). Jika mengganti teknologi tidak memungkinkan karena biaya atau masalah penerapan, solusi terbaik lainnya

adalah temukan sumber gangguan dan singkirkan, jika memungkinkan. Menemukan sumber gangguan all-band lebih sulit daripada menemukan sumber gangguan narrowband karena anda tidak hanya mengawasi satu sinyal pada spectrum analyzer. Padahal, anda mengawasi suatu jangkauan sinyal, dengan amplitudo yang bervariasi. Anda sepertinya memerlukan antenna highly directional untuk mendeteksi sumber gangguan all-band.

9.5.3 Cuaca

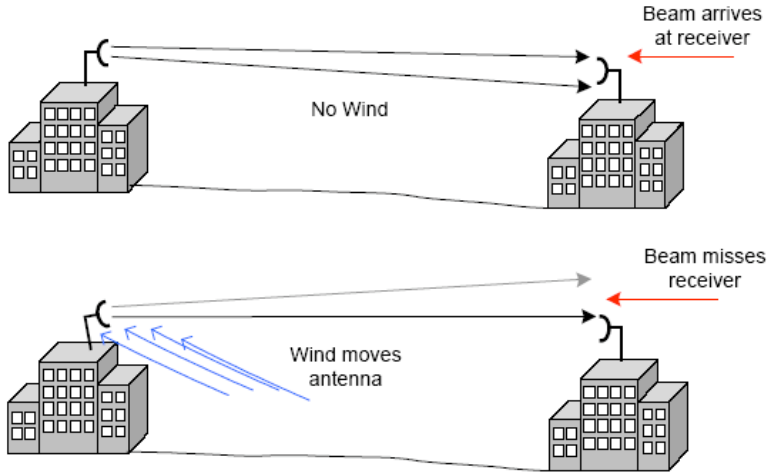
Beberapa kondisi cuaca yang merugikan bisa berpengaruh pada performa jaringan wireless. Biasanya kejadian cuaca umum seperti hujan, hujan es, salju, atau kabut tidak memiliki akibat merugikan bagi jaringan wireless. Meskipun begitu, kejadian ekstrim pada angin, kabut, dan mungkin asbut bisa menyebabkan penurunan atau bahkan downtime pada jaringan wireless anda. Sebuah radome bisa digunakan untuk melindungi antenna dari unsur tersebut. Jika digunakan, radome memiliki lubang kering untuk mengeringkan pengembunan. Antenna yagi tanpa radome akan menjadi rentan terhadap hujan, dimana tetes hujan akan berkumpul dan akan menurunkan performa. Tetes air sebenarnya akan membuat tiap element terlihat lebih panjang daripada aslinya. Kumpulan es pada element yang terbuka bisa menyebabkan efek detuning seperti halnya hujan; meskipun hal ini akan bertahan lama. Radome juga bisa melindungi sebuah antenna dari benda jatuh seperti es yang jatuh dari pucuk pohon.

Sinyal 2,4 GHz bisa berkurang sampai 0,05 dB/km (0,08dB/mil) dikarenakan hujan yang sangat deras (4 inci/jam). Kabut tebal menimbulkan pengurangan sampai 0,02 dB/km(0,03 dB/mil). Pada 5,8GHz, hujan deras menghasilkan pengurangan sampai 0,5dB/km (0,8dB/mil). Dan kabut tebal sampai 0,07 dB/km (0,11 dB/mil). Meskipun hujan sendiri tidak menyebabkan masalah perambatan yang besar, tetapi hujan akan terkumpul diatas daun dari pepohonan dan menghasilkan pengurangan hingga ia menguap.

9.5.4 Angin

Angin tidak mempengaruhi gelombang radio atau sebuah sinyal RF, tetapi ia bisa mempengaruhi posisi dan penempatan antenna outdoor. Sebagai contoh,

misalkan sebuah hubungan wireless point-to-point yang menghubungkan dua gedung sejauh 12 mil(20km). Apabila dihitung kelengkungan bumi, dan tiap antenna hanya memiliki beamwidth vertikal dan horisontal sebesar 5 derajat, maka penempatan tiap antenna haruslah tepat. Sebuah angin yang kuat bisa dengan mudah menggerakkan satu atau kedua antenna, cukup untuk mengurangi sinyal antara kedua antenna. Efek ini disebut ”antenna wind loading”, dan digambarkan pada **gambar 9.15**.



Gambar 9.15 Antenna Wind Loading

Kejadian cuaca ekstrim yang mirip seperti tornado atau badai harus juga dipertimbangkan. Jika anda menerapkan sebuah jaringan wireless di lokasi geografik dimana badai atau tornado sering terjadi, anda harus menyertakan hal itu dalam perhitungan ketika melakukan seting terhadap semua tipe jaringan wireless outdoor. Pada kondisi cuaca seperti ini, mengamankan antenna, kabel, adalah sangat penting.

9.5.5 Stratifikasi

Ketika terdapat kabut yang sangat tebal atau bahkan kabut asap (seperti pada sebuah lembah), udara di sekitar kabut menjadi diam dan mulai terpisah-pisah menjadi lapisan-lapisan. Bukan karena kabut itu sendiri yang menyebabkan difraksi pada sinyal RF, tetapi lapisan-lapisan udara diantara kabut. Ketika sinyal

RF menembus lapisan ini, ia akan dibelokan seperti bagaimana cahaya dibelokkan ketika bergerak dari udara ke air.

9.5.6 Petir

Petir bisa mempengaruhi jaringan wireless melalui dua cara. Pertama, petir bisa menyambar komponen jaringan wireless seperti antenna atau mungkin menyambar benda terdekat. Petir yang menyambar benda terdekat bisa merusak komponen jaringan wireless anda jika komponen ini tidak dilindungi oleh lightning arrestor. Cara kedua sebuah petir bisa mempengaruhi jaringan wireless adalah dengan mengumpulkan udara dimana gelombang RF berjalan setelah menyambar sebuah benda diantara pemancar dan penerima. Pengaruh dari petir ini hampir sama dengan cara Cahaya Utara Aurora Borealis menimbulkan masalah bagi transmisi RF televisi dan radio.

9.5.7 Gangguan Co-channel yang berdekatan

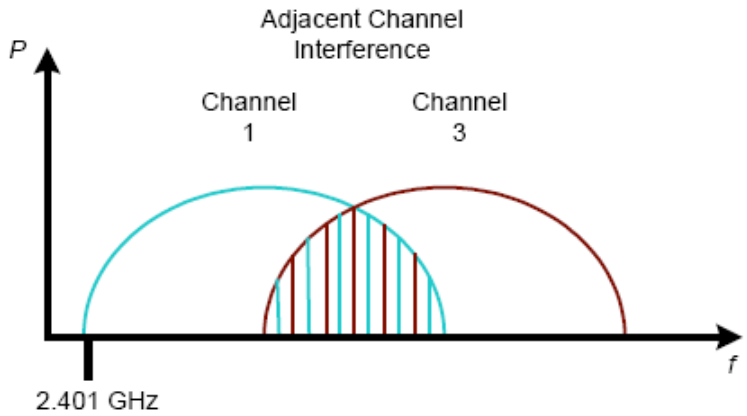
Memiliki pemahaman yang kuat mengenai penggunaan channel dalam jaringan wireless adalah sangat penting bagi seorang administrator jaringan wireless. Sebagai seorang konsultan jaringan wireless, anda pasti menemukan banyak jaringan yang mempunyai banyak akses point, semuanya dikonfigurasi untuk channel yang sama. Pada situasi seperti ini, pembicaraan dengan administrator jaringan yang menginstall akses point tersebut akan mengungkapkan bahwa ia pikir penting bagi semua akses point dan klien berada pada channel yang sama, agar jaringan wireless dapat bekerja semestinya. Konfigurasi ini sangat umum, dan biasanya tidak tepat. Bagian ini akan membangun pengetahuan anda tentang bagaimana penggunaan channel; menjelaskan bagaimana banyak akses poin menggunakan channel yang beragam akan menimbulkan akibat merugikan pada jaringan.

9.5.8 Gangguan Channel yang berdekatan

Channel yang berdekatan adalah channel didalam band RF yang dalam artian bersebelahan. Sebagai contoh, channel 1 berdekatan dengan channel 2, yang berdekatan dengan channel 3 dan seterusnya. Channel yang berdekatan ini saling

tumpang tindih atau overlap dikarenakan tiap channel memiliki lebar 22 MHz sedangkan jarak antar frekuensi tengah hanya 5 MHz.Gangguan channel yang berdekatan terjadi ketika dua atau lebih akses point menggunakan channel yang overlap dan terletak berdekatan hingga sel cakupan secara fisik overlap. Gangguan channel yang berdekatan bisa menurunkan throughput dalam sebuah jaringan wireless.

Hal ini khususnya penting untuk memperhatikan gangguan channel yang berdekatan, ketika penempatan akses point bersama dilakukan untuk mendapatkan throughput yang lebih tinggi dalam area tersebut.Akses point yang dipasang bersama pada channel non-overlapping bisa mengalami gangguan channel berdekatan jika pemisahan diantara channel yang digunakan tidak cukup jauh, saperti yang ditunjukkan pada **gambar 9.16**



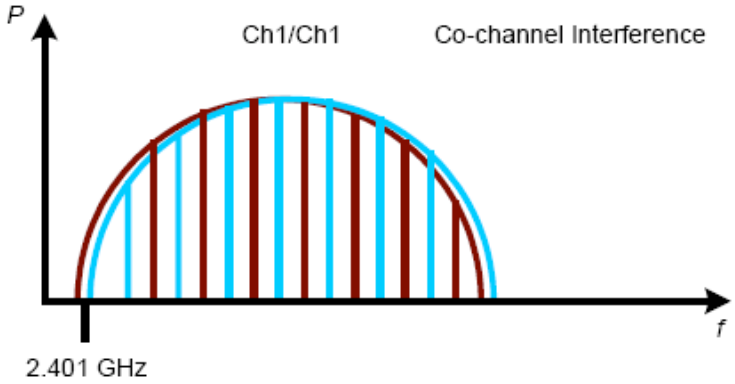
Gambar 9.16 Gangguan pada Channel

Dalam rangka menemukan permasalahan gangguan channel berdekatan, sebuah spectrum analyzer akan dibutuhkan. Spectrum analyzer akan menunjukkan bagaimana channel yang digunakan saling tumpang tindih atau overlap.

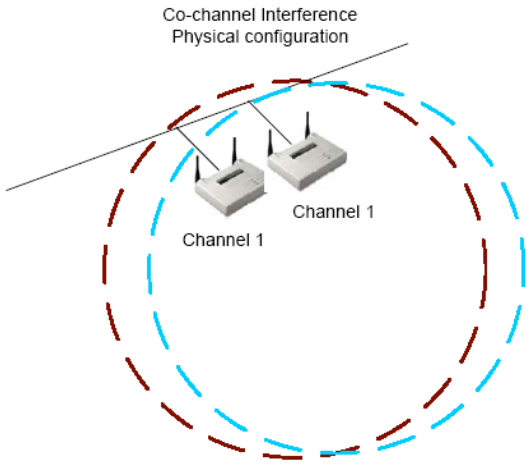
Hanya ada dua solusi untuk permasalahan ini. Yang pertama pindahkan akses point pada channel berdekatan pada jarak yang cukup jauh dari akses point lainnya sehingga cakupan sel tidak overlap, atau turunkan power pada tiap akses point agar cakupan sel tidak overlap. Solusi kedua adalah gunakan channel yang tidak akan overlap. Sebagai contoh , menggunakan channel 1 dan 11 dalam sistem DSSS akan menyelesaikan permasalahan.

9.5.9 Gangguan Co-Channel

Untuk menggambarkan gangguan co-channel, anggap ada satu gedung, dengan jaringan wireless pada tiap lantainya, dan masing-masing jaringan wireless menggunakan channel 1. Jangkauan sinyal akses point , atau sel, tampaknya akan overlap pada situasi seperti ini. Karena tiap akses point berada pada channel yang sama, mereka akan saling mengganggu satu sama lain. Tipe gangguan ini disebut gangguan co-channel.



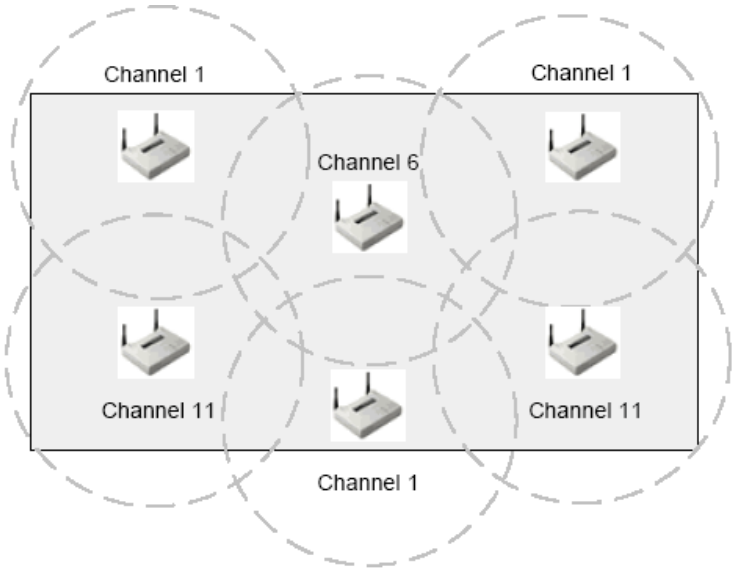
Gambar 9.17. Gangguan Co-Channel



Gambar 9.18. Gangguan Co-Channel pada Jaringan

Dalam rangka mendeteksi gangguan co-channel, sebuah sniffer jaringan wireless akan diperlukan.Sniffer ini akan menampilkan paket yang datang dari tiap jaringan wireless yang menggunakan channel apa saja. Sebagai tambahan, ia akan

menunjukkan sinyal kekuatan dari tiap paket jaringan wireless, memberikan anda sebuah ide bagaimana jaringan wireless saling mengganggu dengan lainnya.



Gambar 9.19. Penggunaan Channel Kembali

Terdapat dua solusi untuk gangguan ini, pertama channel non-overlapping yang berbeda untuk tiap jaringan wireless, dan yang kedua menjauhkan antar jaringan wireless agar jangkauannya tidak overlap. Solusi ini merupakan penyelesaian yang sama pada gangguan channel berdekatan.

Pada situasi dimana roaming dibutuhkan, satu teknik yang disebut daur ulang channel, dapat digunakan yang bertujuan meringankan gangguan co-channel dan channel berdekatan sementara mengijinkan user untuk berkelana pada channel yang berdekatan. Daur ulang channel merupakan penempatan sel yang tidak overlapping secara bersebelahan sehingga membentuk cakupan dimana tidak ada sel yang menyentuh sel yang lain pada channel tersebut.

9.6 Pertimbangan Jangkauan

Ketika mempertimbangkan untuk menempatkan hardware jaringan wireless, jangkauan komunikasi unit tersebut tentu harus masuk perhitungan. Biasanya, tiga hal akan mempengaruhi jangkauan hubungan RF: power transmisi, jenis antenna dan lokasi, dan lingkungan. Jangkauan komunikasi maksimum dari hubungan jaringan wireless

dicapai ketika, pada suatu jarak tertentu , hubungan menjadi tidak stabil tetapi tidak hilang atau putus.

9.6.1 Power Transmisi

Output power dari radio transmisi memiliki dampak pada jangkauan hubungan. Output power yang semakin tinggi akan menyebabkan sinyal dikirimkan hingga jarak yang lebih jauh, menghasilkan jangkauan yang lebih luas. Sebaliknya menurunkan output power akan mengurangi jangkauan.

9.6.2 Tipe Antenna

Jenis antenna yang digunakan mempengaruhi jangkauan dengan memusatkan energy RF kedalam pancaran yang lebih sempit akan memancarkannya lebih jauh (seperti yang dilakukan antenna parabolic dish); atau dengan memancarkannya ke segala arah(seperti yang dilakukan antenna omni-directional), mengurangi jangkauan komunikasi.

9.6.3 Lingkungan

Lingkungan yang berisik dan tidak stabil bisa menyebabkan jangkauan hubungan jaringan wireless berkurang. Tingkat error paket dari sebuah hubungan RF akan lebih besar pada batasan jangkauan dikarenakan sebuah sinyal noise kecil.Tentu saja menambah gangguan secara efektif menaikkan noise, mengurangi kemungkinan mempertahankan hubungan yang solid.

Jangkauan hubungan RF bisa juga dipengaruhi oleh frekuensi transmisi. Meskipun biasanya tidak mendapatkan perhatian dalam menerapkan jaringan wireless, frekuensi mungkin menjadi pertimbangan ketika merencanakan sebuah bridge link. Sebagai contoh, sebuah sistem 2,4 GHz akan mampu mencapai lebih jauh pada output power yang sama dari pada sistem 5 GHz. Kenyataan yang sama berlaku untuk sistem 900 MHz yang lebih tua; ia akan mencapai jarak lebih jauh daripada sistem 2,4 GHz pada output power yang sama. Semua band ini digunakan dalam jaringan wireless, tetapi sistem 2,4 GHz tampaknya yang paling umum dipakai.

9.7 Kesimpulan

Ada berbagai permasalahan yang sering dihadapi dalam implementasi Wireless LAN, yaitu diantaranya Mulitpath, Hidden Node (Node yang tersembunyi), Near/Far, masalah Throughput. Sedanngkan ada beberapa tipe –tipe gangguan pada jaringan wireless, seperti contoh gangguan Narrowband, gangguan All-Band, gangguan cuaca, gangguan angin, stratifikasi, gangguan petir, dan gangguan channel yang saling berdekatan. Yang perlu diperhatikan pada jaringan wireless untuk menghindari dan menghadapi permasalah sperti diatas adalah dengan mendesain secara cermat terhadap jaringan wireless yang akan dibuat. Termasuk diantaranya adalah pemilihan tempat / lokasi, perangkat yang digunakan, user yang akan memakai jaringan tersebut, dan perawatan jaringan itu sendiri.

9.8 SOAL

1. Apa yang anda ketahui tentang Multipath dan efek apa yang dapat diakibatkan oleh Multipath ?
2. Bagaimana cara mengatasi node yang tersembunyi pada jaringan wireless ?
3. Solusi apa yang dapat digunakan untuk mengatasi masalah Near/Far pada jaringan Wireless ?
4. Apa yang dapat dilakukan untuk dapat mengatasi masalah Throughput Co-Location Access Point ?
5. Sebutkan beberapa tipe gangguan pada jaringan wireless ? (5)

Bab 10. Keamanan Wireless LAN

10.1 WEP (Wired Equivalent Privacy)

WEP merupakan suatu algoritma enkripsi yang digunakan oleh shared key pada proses autentikasi untuk memeriksa user dan untuk meng-enkripsi data yang dilewatkan pada segment jaringan wireless pada LAN.

WEP digunakan pada standar IEEE 802.11. WEP juga merupakan algoritma sederhana yang menggunakan pseudo-random number generator (PRNG) dan RC4 stream cipher. RC4 stream cipher digunakan untuk decrypt dan encrypt.

10.1.1 Alasan memilih WEP

WEP merupakan sistem keamanan yang lemah. Namun WEP dipilih karena telah memenuhi standar dari 802.11 yakni

- Exportable
- Reasonably strong
- Self-Synchronizing
- Computationally Efficient
- Optional

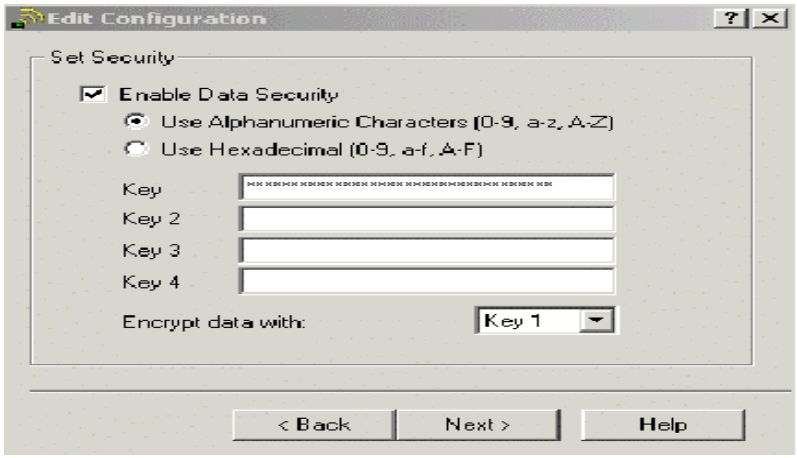
WEP dimaksudkan untuk tujuan keamanan yakni kerahasiaan data, mengatur hak akses dan integritas data. Selain WEP terdapat standar lain yakni standar 802.1x yakni EAP atau VPN.

10.1.2 WEP Keys

WEP keys diimplementasikan pada client dan infrastrukturnya digunakan pada Wireless LAN. WEP keys ini merupakan alphanumeric character string yang memiliki dua fungsi pada Wireless LAN. Pertama, WEP keys ini dapat digunakan untuk verifikasi identitas pada authenticating station. Kedua, WEP keys dapat digunakan untuk data encryption.

WEP keys terdiri atas dua tipe, yakni tipe 64-bit dan tipe 128-bit. Untuk memasuki static WEP keys melalui client atau infrastruktur seperti bridge atau access point adalah muda.

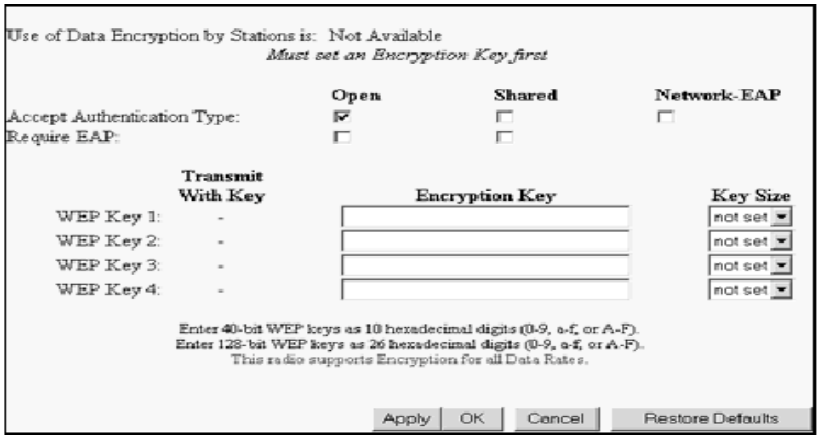
Berikut pada **gambar 10.1** menunjukkan konfigurasi program untuk memasuki WEP keys. Terkadang tampilan untuk memasuki WEP keys berupa checkbox yang menyeleksi 40-bit atau 128-bit WEP. Terkadang tampilannya bukan checkbox, oleh karena itu administrator harus mengetahui berapa banyak karakter yang ditanyakan. Pada umumnya software client akan mengijinkan untuk memasukkan WEP keys baik berupa format alphanumeric (ASCII) ataupun hexadecimal (HEX)



Gambar 10.1 Memasuki WEP keys melalui client device

10.1.3 Static WEP Keys

Untuk mengimplementasikan static WEP keys ini kita harus mengatur secara manual WEP key pada access point dan dihubungkan ke client. Pada **gambar 10.2** ini untuk memasuki WEP keys melalui infrastruktur.



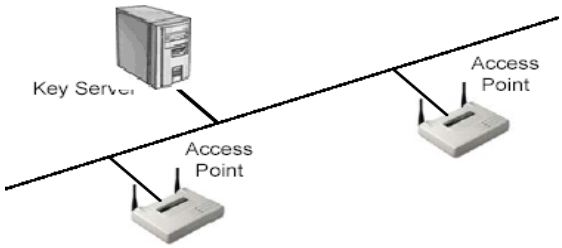
Gambar 10.2 Memasuki WEP keys melalui infrastruktur

10.1.4 Centralized Encryption Key Servers

Centralized encryption key servers ini digunakan atas dasar alasan-alasan berikut:

- centralized key generation
- centralized key distribution
- ongoing key rotation
- reduced key management overhead

Beberapa nomor dari device yang berbeda dapat bertindak sebagai Centralized key server. Berikut ini gambar Centralized Encryption Key Servers:



Gambar 10.3. Centralized Encryption Key Servers

10.1.5 WEP Usage

Ketika WEP diinisialisasi, paket data akan dikirimkan dengan menggunakan WEP untuk meng-encrypt. Namun paket header data yang berisi MAC address tidak mengalami proses encrypt. Semua layer 3 yang berisi source dan destination mengalami encrypt.

10.1.6 Advanced Encryption Standard (AES)

AES merupakan pengganti algoritma RC4 yang digunakan pada WEP. AES menggunakan algoritma Rijndale.

10.2 Filtering

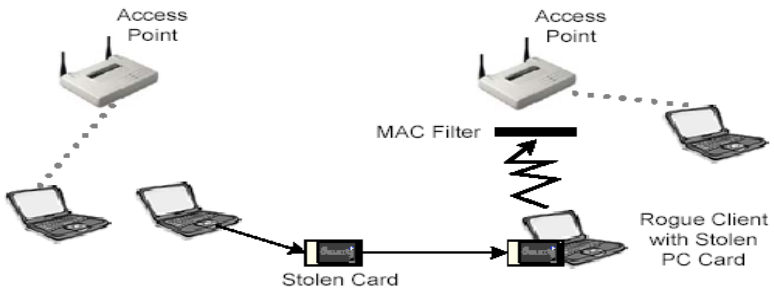
Merupakan mekanisme keamanan dasar yang digunakan untuk mendukung WEP dan atau AES. Filtering memiliki arti menutup semua hubungan yang tidak diijinkan

dan membuka semua hubungan yang diijinkan. Filtering terdiri dari tiga tipe dasar yang dapat diimplementasikan pada WLAN, yakni:

- SSID Filtering
- MAC Address Filtering
- Protocol Filtering

SSID Filtering merupakan metode penyaringan/ filtering yang bersifat elementer dan hanya digunakan untuk mengontrol hak akses. SSID merupakan nama dari jaringan.

MAC Address Filtering merupakan metoda filtering untuk membatasi hak akses dari MAC Address yang bersangkutan. Berikut ini adalah gambar yang menunjukkan illustrasi MAC filters:

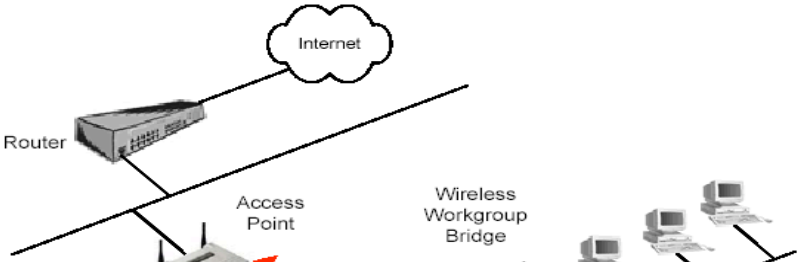


Gambar 10.4. Illustrasi MAC Filters

MAC filters ini juga merupakan metode sistem keamanan yang baik dalam WLAN, karena peka terhadap jenis gangguan seperti:

- Pencurian pc card dalam MAC filter dari suatu access point
- Sniffing terhadap WLAN

Protocol Filtering merupakan metoda yang memungkinkan WLAN dapat menyaring paket-paket yang melalui jaringan dari layer 2 hingga layer 7. Berikut illustrasi dari protocol filtering:



Gambar 10.5. Illustrasi dari protocol filtering

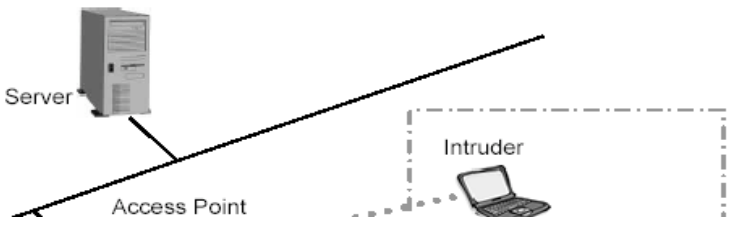
10.3 Attack On Wireless LAN

Seorang hacker dapat melakukan beberapa tindakan yang tujuannya adalah untuk memperoleh hak akses secara paksa dari suatu WLAN. Beberapa metoda yang digunakan hackerantara lain:

- Passive attack (eavesdropping)
- Active attack
- Jamming attack
- Man in the middle attack

10.3.1 Passive attack

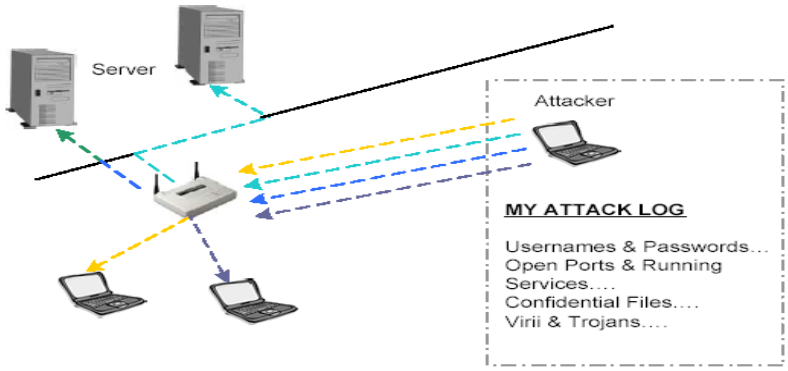
Eavesdroping merupakan penyerangan ke WLAN yang paling sederhana dan efektif. Metode ini tanpa meninggalkan jejak dari hacker itu sendiri. Berikut contoh illustrasi dari Passive attack:



Gambar 10.6. Illustrasi dari Passive attack

10.3.2 Active attack

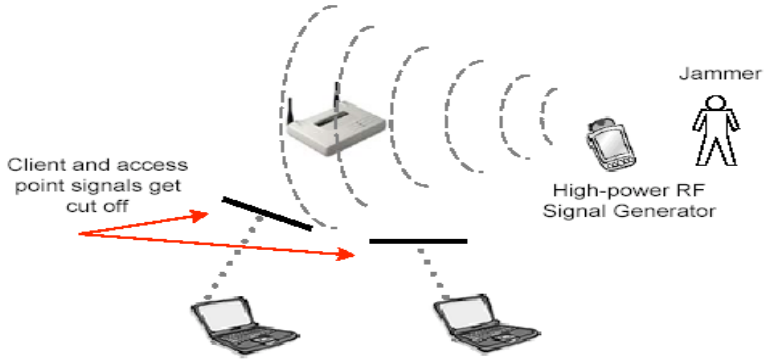
Merupakan metode hacking yang memungkinkan seseorang mendapat hak akses yang digunakan untuk tujuan merusak. Dengan metode ini memungkinkan hacker dapat mengacak-acak data pada jaringan. Berikut contoh illustrasi dari Active attack:



Gambar 10.7. Illustrasi dari Active attack

10.3.3 Jamming attack

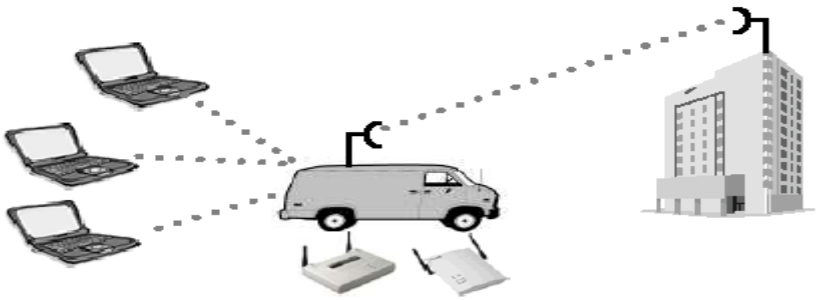
Merupakan metode yang dapat mematikan supply tegangan pada suatu jaringan. Contohnya:



Gambar 10.8. Illustrasi dari Jamming attack

10.3.4 Man in the middle attack

Metode yang juga dikenal dengan istilah membajak. Berikut contoh illustrasinya:



Gambar 10.9. Illustrasi dari Man in Middle attack

10.4 Emerging Security Solution

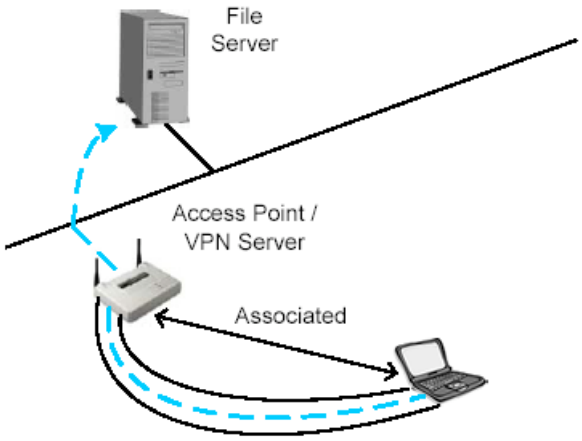
Karena WLAN tingkat keamanannya rendah, dan karena mekanisme keamanan WEP pada end-to-end buruk. Maka digunakan standar IEEE 802.1x.

10.4.1 WEP Key Management

Dengan menggunakan WEP sebagai sistem keamanan maka akan dengan mudahnya hacker menembus sistem keamanan tersebut. Solusinya adalah dengan memberi WEP key untuk setiap paketnya.

10.4.2 Wireless VPN

Merupakan salah satu teknologi yang berguna dalam keamanan koneksi pada Wireless LAN. Software yang digunakan untuk membangun VPN antara lain PPTP dan IP Sec. Berikut illustrasi VPN:



Gambar 10.10. Illustrasi VPN

10.5 Key Hopping Technologies

Merupakan teknologi yang memberikan solusi atas kelemahan WEP.

10.5.1 Temporal Key Integrity Protocol (TKIP)

Merupakan protokol yang membantu meningkatkan kerja dari WEP. TKIP digunakan untuk inisialisasi vektor (IV) dan menangani paket pasif yang mengalami proses snooping.

10.5.2 Solusi yang bedasarkan AES

Solusi yang didasarkan AES mungkin akan menggantikan WEP yang mengunakan RC4, tetapi sementara solusi seperti TKIP sedang diterapkan. Walaupun sekarang ini dipasaran tidak ada produk yang menggunakan AES, tetapi tetapi beberapa penjual telah memiliki produk ini hanya tinggal menunggu keputusan release nya saja. AES memiliki tinjauan yang luas sehungga sangat effisien bagi harware dan software. Konsep 802.11i adalah konsep untuk penggunaan AES, dan merupakan sebuah pertimbangan bagi pemain industri Wierless LAN. AES sepertinya merupakan sebuah penyeleseian standart.

Teknik perubahan enkripsi data merupakan sebuah solusi yang penting, AES akan menbuat dampak penting pada sistem keamanan WLAN, tetapi masih ada solusi yang msih bisa diimplementasikan pada jaringan enterprise, contohnya memusatkan encryption key server untuk mengotomatisasi handling out key. Jika radio cart pelanggan hilang, dengan AES enkripsi didalamnya, hal ini tidak akan berpengaruh, karena pencurinnya tidak bisa mengakses jaringan.

10.6 Wireless Gateway

Residential wireless gateway sekarang tersedia dengan teknologi VPN, seperti NAT, DHCP, PPPoE, WEP, MAC Filter dan bahkan sebuah built in firewall. Device ini cocok untuk kantor kecil atau lingkungan rumah dengan beberapa komputer dan jaringan ke internet. Biaya dari unit ini sangat tergantung pada servis yang ditawarkan. Beberapa dari unit hi-n bahkan mempunya static routing dan RIP v2.

Enterprise Wireless gateway adalah sebuah adaptasi spesial dari VPN dan server authehtikasi untuk jaringan wireless. Sebuah enterprise gateway berada dalam segmen jaringan kabel antara akses point dan jaringan wired akstrim. Sesuai namanya, sebuah gateway mengontrol akses dari wireless Lan ke jaringan wired, sehingga ketika seorang hacker mendapatkan akses ke segmen wireless, gateway akan melindungi sistem distribusi jaringan wired dari serangan.

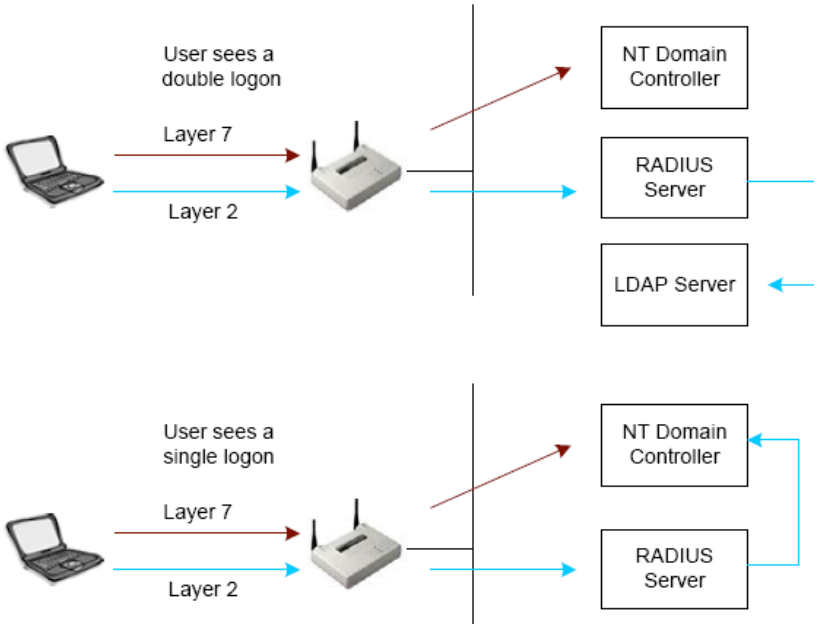
Sebuah contoh dari waktu yang tepat untuk membangun sebuah enterprise wireless line gateway mungkin dapat dilihat pada situasi berikut. Anggaplah sebuah rumah sakit mempunyai 40 akses point dalam gedungnya. Investasi mereka pada akses point cukup penting, sehingga jika akses point tidak mendukung ukuran keamanan, rumah sakit bisa dalam keadaan yang sulit/bahaya dan harus mengganti semua akses point mereka. Malahan, rumah sakit dapat membangun sebuah wireless line gateway.

Gateway ini dapat terhubung antara core switch dan distribution switch (yang terhubung pada akses point) dan dapat berfungsi sebagai sebuah authentikasi dan VPN server pada jaringan yang terhubung dengan semua wireless LAN client. Malahan daripada membangun seluruh akses point baru satu (atau lebih tergantung dari kebutuhan jaringan) gateway device dapat di install dibelakang semua akses point sebagai sebuah group. Kegunaan dari tipe gateway ini adalah untuk menyediakan keamanan untuk kepentingan sebuah akses point yang tidak aman. Sebagian besar

entreprise wireless gateway mendukung sebuah array dari protokol VPN seperti PPTP, IP Sec, L2TP, Sertificate, dan bahkan QoS berdasarkan profile.

10.7 802.1x and Extensible Authentication Protocol

Standart 802.1x menyediakan spesifikasi untuk akses control jaringan port-based. Akses kontrol port-based sebenarnya – dan masih – digunakan dengan eterneth switch. Ketika sebuah user mencoba untuk terhubung ke port ethernet, port kemudian menempatkan koneksi user pada bloked mode untuk menunggu verifikasi dari identitas user dengan sebuah sistem authentikasi back end.



Gambar 10.11. 2-Logon Processor

Protokol 802.1x telah dipergunakan pada banyak sistem wireless LAN dan hampir menjadi sebuah latihan standart pada banyak vendor. Ketika dikombinasikan dengan Extensible Authentication Protocol (IEP), 802.1x dapat menyediakan sebuah lingkungan yang fleksibel dan sangat aman berdasarkan berbagai macam skema authentikasi yang digunakan sekarang.

IEP, yang dulunya didefinisikan untuk point to point protokol (ppp), adalah sebuah protocol untuk bernegosiasi dengan metode authentikasi. IEP diterangkan pada RFC 2284 dan mendefinisikan karakteristik dari metode authentikasi termasuk informasi user yang dibutuhkan (pasword, sertifikat, dll), protokol yang digunakan

(MD5, TLS, GSM, OTP, dll), dukungan dari igeneration, dan dukungan dari mutu authentikasi. Mungkin terdapat beberapa tipe EAP yang berada dipasar sejak IEEE dan pelaku industri membuat persetujuan pada setiap single type,atau beberapa tipe lain untuk menciptakan sebuah standart.

10.8 Corporate Security Police

Sebuah perusahaan seharusnya memiliki sebuah hubungan dengan security police yang menunjukan resiko yang unik yang ditunjukkan WLAN terhadap suatu jaringan. Contoh, dari sebuah ukuran sel yang tidak tepat yang memperkenankan hacker untuk mengambil keuntungan akses jaringan pada area parkir adalah contoh yang sangat bagus dari sebuah item yang seharusnya termasuk dalam beberapa hubungan security police. Hal lain yang perlu diperhatikan dalam security police adalah pasword yang baik, WEP yang bagus keamanan secara fisik penggunaan solusi keamanan yan bagus dan keteraturan perlengkapan hardware pada wireless LAN. Semua itu jauh dari sempurna mengingat solusi keamanan yang akan mengalami perubahan diantara organisasi-organisasi. Luasnya pembahasan security policy pada wireless LAN akan bergantung pada perlengkapan securitas dari organisasi seperti halnya luas dari daerah wireless LAN pada suatu jaringan.

10.8.1 Keep Sensitive Informatio Private

Beberapa hal yang seharusnya diketahui hanya oleh administrator jaringan pada level yang tepat adalah :

1. Username dan password dari access point dan bridge
2. SNMP strings
3. WEP keys
4. Daftar MAC address

Point penting untuk menjaga informasi ini hanya ditangan orang yang terpercaya. Kemampuan individual seperti administrator jaringan sangat penting karena seorang hacker akan sangat mudah mengunakan bagian informasi tersebut untuk mengambil keuntungan pada akses jaringan.

10.8.2 Physical Security

Walaupun saat physical security menggunakan jaringan wired tradisional sangat penting tapi akan lebih penting lagi perusahaan yang menggunakan teknologi wireless LAN. Untuk alasan yang telah dibahas diawal seseorang yang memiliki sebuah wireless PC card (dan mungkin sebuah antenna) tidak dapat berada dalam gedung yang sama, seperti halnya suatu jaringan mengambil keuntungan akses pada jaringan yang lain. Bahkan software pendeteksi gangguanpun tak sepenuhnya cukup untuk mencegah hacker wireless LAN untuk melakukan pencurian informasi sensitif/penting. Serangan pasif tidak meninggalkan jejak, karena tidak adanya koneksi yang dibuat. Sekarang semua itu merupakan kebutuhab pasaran yang dapat menunjukkan network card dengan mode yang menjanjikan, mengakses data tanpa membuat koneksi.

10.8.3 Inventaris Peralatan Wireless LAN dan Security Audits

Sebagai bagian dari physical security policy, semua peralatan Wireless LAN seharusnya secara teratur dicatat disahkan dan mencegah penggunaan peralatan WLAN yang tidak sah untuk mengakses organization's network. Jika jaringan terlalu besar dan berisi sejulah peralatan Wireless yang penting, maka inventori peralatan secara berkala sangat tidak praktis. Jika masalahnya seperti ini, penyeleseian kemanan Wireless LAN sangat penting untuk diimplementasikan, yang tidak berdasar pada hardware tetapi berdasar pada username dan password atau beberapa tipe yang bukan hardware-based peneleseian keamanan.

10.8.4 Menggunakan penyeleseian keamanan tingkat lanjut

Organisasi yang menerapkan WLAN seharusnya mengambil keuntungan dari mekanisme keamanan yang lebih maju yang sudah tersedia dipasaran saat ini. Ini juga diperlukan suatu kebijakan keamanan yang mengimplementasikan tentang segala sesuatu yang mengedepankan mekanisme keamanan secara menyeluruh. Karena ini merupakan teknologi baru, hak milik, dan sering juga digunakan dalam kombinasi dengan protokol keamanan yang lain, mereka harus mendokumentasikannya, sehingga jika terjadi suatu pelanggaran keamanan,

network administrator dapat menentukan dimana dan bagaiman pelanggaran itu terjadi.

10.9 Publik Wireless Network

Ini sangat mutlak bahwa mereka (corporate users) dengan informasi yang sensitif pada komputer mereka akankah terhubung dengan publik wireless LAN. Ini seharusnya menjadi masalah bagi kebijakan peusahaan bahwa semua pengguna wireless berjalan di keduanya, yaitu sofware firewall pribadi dan antiviral sofware pada labtop mereka. Kebayakan publik wireles network hanya memiliki sedikit atau bahkan tanpa pengamanan pada saat membuat hubungan/konektifitas sederhana bagi pengguna dan mengurangi jumlah pendukung teknis diperlukan.

10.9.1 Limited dan Tracked Access

Kebanyakan perusahaan LAN memiliki beberapa metode dalam membatasi tracking akses pengguna pada LAN. Secara khusus, sistem pendukung servis authentikasi, Authorisasi, dan Laporan dipekerjakan. Tindakan pengamanan yang sama ini seharusnya didokumentasikan dan diterapkan sebagai bagian dari keamanan Wierless LAN. AAA servis akan menizinkan perusahaan untuk menempatkan penggunaan yag tepat ke kelas user tertentu. Pengunjung (misalnya) hanya boleh mengakses internet, sedangkan karyawan diperbolehkan mengakses data-data departemen dan juga mengakses intenet.

10.10 Rekomendasi keamanan

Sebagai ringkasan pada bab ini , di bawah adalah beberaparekomendasi untuk pengamanan wireless LAN.

10.10.1WEP

Jangan semata-mata hanya percaya pada WEP, tidak perduli sebaaik-baiknya kamu mengimplementasikan sebuah solusi keamaan wireless LAN end to end. Suatu peralatan wireless LAN dilindungi hanya dengan WEP hal itu bukan suatu jaminan. Ketika menggunakan WEP, jangan menggunakan WEP keys yang

dihubungkan ke SSID atau ke organisasi. Membuat WEP keys sangat sulit untuk di ingat di dibawa keluar. Pada banyak kasus, WEP key dapat dengan mudah ditebak hanya dengan melihat SSID atau nama dari organisasi.

10.10.2Cell Cizing

Dalam rangka mengurangi kesempatan *eavesdropping*, administrator harus yakin bahwa cell size dari aksess point adalah tepat. Mayoritas hackers mencari penempatan di mana sangat kecil energi dan waktu harus dihabiskan untuk memperoleh akses ke dalam jaringan tersebut. Karena alasan ini, adalah penting untuk tidak mempunyai access point yang memancarkan sinyal yang kuat yang meluas keluar daearh organisasi/perusahan kecuali jika perlu. Beberapa enterprise-level access point mengizinkan menkonfigurasi power output, yang mana secara efektif mengendalikan ukuran dari RF cell disekitar access point. Jika pembajak berada diarea perusahaan tidak dapat mendeteksi jaringanmu, kemudian jaringanmu tidak akan terbajak.

10.10.3User Authentication

Sejak user authentication adalah sebuah wireless LAN paling lemah, dan standart 802.11 tidak menetapkan metode apapun dari user authentikasi, ini sangat penting bahwa administrator secepat mengimplementasikan user-based authentikasi pada saat instalasi infrastruktur wireless LAN. User authentiksi harus berdasar pada rencana device-independent seperti, username dan password, biometric, smart card, sistem token-based, atau beberapa tipe yang lain dari alat keamanan yang mengidentifikasi user, bukan pada hardware. Solusi yang kamu terapkan seharusnya didukung authentikasi bi-direcsional antara server authentikasi dan wireless client.

10.10.4Security Need

Memilihlah suatu solusi keamanan yang sesuai dengan anggaran dan kebutuhan organisasimu, keduanya untuk hari ni dan seterusnya. Wireless LAN memperoleh popularitas yang sangat cepat karena kemudahannya dalam pengimplementasian. Ini berarti bahwa wireless LAN yang dimulai dari sebuah

access point dan 5 buah client dapat tumbuh dengan cepat menjadi 15 accesss point dan 300 client. Mekanisme keamanan yang sama bekerja dengan baik untuk satu accses point tidak akan bisa diterima, atau dijamin untuk 300 user. Sebuah organisasi bisa membuang uang untuk solusi keamanan yang akan tumbuh dan berkembang dengan cepat seperti perkembangan wireless LAN. Pada banyak kasus, organisasi sudah memiliki keamanan ditempatnya seperti sistem deteksi gangguan, firewall, dan RADIUS server. Ketika memutuskan pada sebuah solusi wireless LAN, maka peralatan yang ada menjadi pengaruh yang sangat penting dalam penurunan biaya.

10.10.5Use additional security tool

Mengambil keuntungan dari teknologi yang ada tersedia, seperti VPNs, firewalls, intrusion detection systems (IDS), standart dan protokol seperti 802.1x dan EAP, dan client authentication dengan RADIUS dapat membantu membuat solusi wireless diatas dan melebihi standart 802.11 yang dibutuhkan. Biaya dan waktu untuk mengimplementasikan solusi ini sangat dianjurkan dari SOHO solution dan solusi perusahaan besar.

10.10.6Monitoring for Rogue Hardware

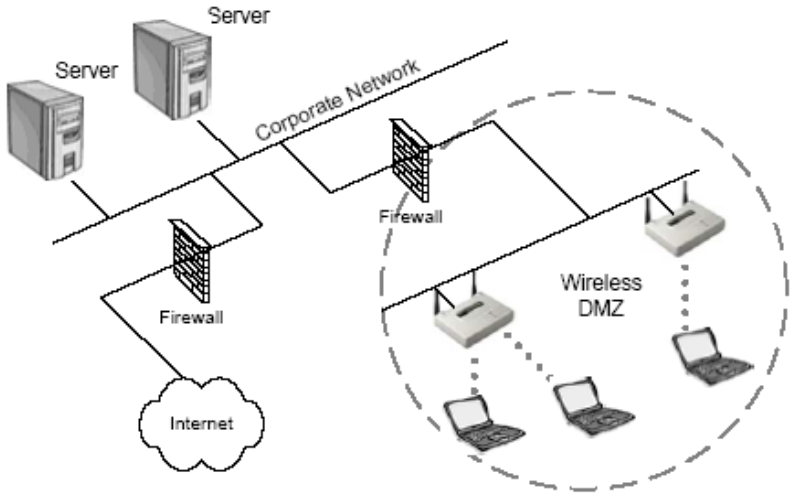
Untuk mengetahui penjahat accsess point, access point regular sesi penemuan seharusnya dijadwal tetapi tidak diumumkan. Dengan aktif menemukan dan memindahkan penjahat access point akan seperti menjauhkan hacker dan mengizinkan administrator untuk merawat control jaringan dan keamanan. Pemeriksaan keamanan secara regular harus dilakukan untuk menempatkan configurasi access point yan salah, dapat menjadi resiko keamanan. Tugas ini bisa dilakukan selagi mengawasi jaringan dari kejahatan penjahat access point adalah bagian dari suatu keamanan reguler yang rutin. Kini, konfigurasiharus dibandingkan denga konfigurasi yang lama dalam rangka untuk melihat jika hacker telah meng konfigurasi ulang access point. Penguncian access harus diterapkan dan dimonitor bertujuan untuk menemukan semua access yang tidak beraturan pada segmen wireless. Type pengawasan ini bahkan dapat membantu menemukan hilangnya atau tercurinya peralatan wireless client.

10.10.7Switches, not hub

Petunjuk sederhana yang lain untuk mengikuti selalu menghubungkan accsess point ke switch malahan ke hub. Hub adalah peralatan broadcast, jadi setiap paket yang diterima oleh hub akan dikirimkan ke semua port hub yang lain. Jika access point terhubung dengan hub, kemudian setiap paket dikirim melalui segmen wired akan di broadcast menyeberangi segmen wireless. Kemampuan ini memberi informasi tambahan kepada hacker seperti password dan ip address.

10.10.8Wireless DMZ

Ide yang lain untuk menerapkan keamanan untuk segmen wireless LANadalah menciptakam WDMZ. Membuat WDMZ ini menggunakan firewall atau router biayanya dapat bergantung pada level implementasi. WDMZS biasanya diterapkan di medium dan large-scale LAN deployments. Karena pada dasarnya access point adalah alat yang tidak aman dan tidak dipercaya, mereka harus terpisah dari segmen jaringan lain oleh perlatan firewall. Dapat digambarkan pada **gambar 10.12** dibawah ini.



Gambar 10.12 Wireless DMZ

10.10.9Firmware & Software Updates

Updete-lah firmware dan driver pada access point dan wireless card anda. Merupakan keputusan yang tepat untuk menggunakan firmware dan driver terbaru pada access point dan wireless card anda. Perusahaan-perusahaan sangat biasa mengalami kesulitan untuk mengetahui isu, security hole dan mengaktifkan fitur baru dengan melakukan update tersebut

10.11 Kesimpulan

Untuk mengatasi masalah keamanan dalam jaringan wireless digunakan WEP. WEP (Wireless Equivalent Privacy) merupakan algoritma enkripsi yang digunakan oleh shared key pada proses autentikasi untuk memeriksa user dan untuk meng-enkripsi data yang dilewatkan pada segment jaringan wireless pada LAN. WEP dimaksudkan untuk tujuan keamanan yakni kerahasiaan data, mengatur hak akses dan integritas data. Selain WEP terdapat standar lain yakni standar 802.1x yakni EAP atau VPN. Standar yang banyak digunakan adalah WEP meskipun merupakan keamanan yang lemah. Ada beberapa alasan mengapa WEP dipilih karena memenuhi standar 802.11, yaitu Exportable, Reasonably strong, Self-Synchronizing, Computationally Efficient, Optional. Sedangak Filtering adalah sisitem keamanan yang digunakan unutk mendukung dari sistim WEP. Dan yang terpenting dalam keamanan jaringan wireless adalah melakukan update terhadap software perangkat yang digunakan.

10.12 SOAL

1. Apa yang anda ketahui tentang Wired Equivalent Privacy ?
2. Jelaskan mengenai konsep Filtering pada sistim keamanan jaringan wireless yang mendukung WEP ?
3. Sebutkan dan jelaskan secara singkat serangan pada jaringan wireless ?
4. Sebutkan dua software yang digunakan untuk membangun VPN ?
5. Sebutkan solusi yang dapat digunakan untuk lebih meningkatkan keamanan pada jaringan wireless ?

Bab 11. Site Survey

Survey site Radio Frekuensi (RF) adalah peta untuk keberhasilan implementasi jaringan wireless. Survey site tidak terlalu susah dan tekniknya cepat. Survey site sangat penting dalam implementasi jaringan wireless. survey site digunakan untuk mendefinisikan kontur cakupan radio frekuensi dari sumber radio frekuensi (access point/bridge) dalam banyak fasilitas. site survey digunakan untuk mengetahui cakupan radio frekuensi yang dibutuhkan.

11.1 Persiapan untuk survey site meliputi:

11.1.1 Pengumpulan informasi

11.1.2 Pembuatan keputusan :

Beberapa topik yang mungkin dibutuhkan sebagai pertanyaan manajemen jaringan sebelum survey site :

11.1.2.1 Analisa fasilitas

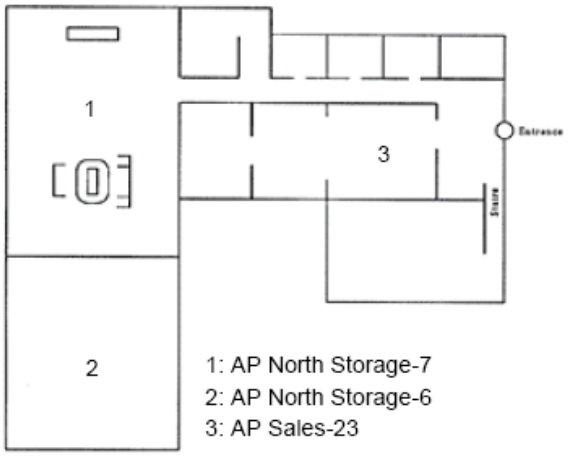
Jenis fasilitas di rumah sakit yang memiliki peralatan radiologi, di real estate dengan kantor sebanyak 25 agen dalam hal ini keamanan sangat penting dimana cakupannya hanya 1 atau 2 central access point dan kebutuhan bandwith akan disebutkan sejak access internet atau transfer file.

11.1.2.2 Menampilkan Jaringan

Apakah jaringan telah siap? ,pertanyaan yang biasanya ada pada administrator jaringan adalah sebagai berikut:

- Sistem operasi jaringan apa yang digunakan.
- Berapa banyak penggunanya yang membutuhkan access secara bersama - sama ke jaringan wireless.
- Berapa besar kebutuhan bandwith dalam jaringan
- Protokol apa yang digunakan dalam wireless LAN
- Kanal den teknologi spread spectrum apa yang saat ini digunakan
- Pengukuran keamanan wireless LAN apa yang ada dilokasi

- Dimana point koneksi wired LAN diletakkan
- Apakah client menggunakana wireless LAN dalam sebuah organisasi



Gambar 11.1. Naming Conventions

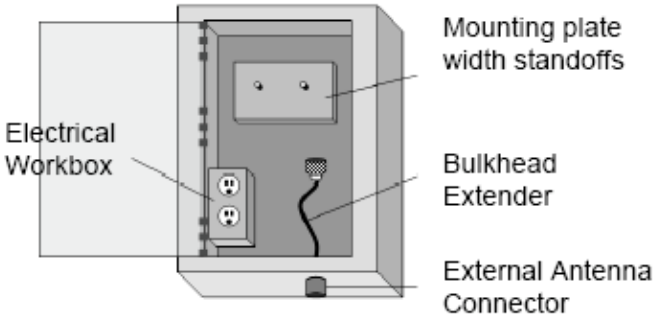
11.1.2.3 Penggunaan Area dan Tower

Apakah Wireless LAN digunakan untuk indoor,outdoor atau kedua-duanya?...

Wireless LAN menggunakan tipe outdoor dalam banyak situasi dan potensi rintangan dalam instalasi dan perbaikan wireless LAN.

Tipe tower apa yang digunakan?...

- *Apakah butuh perijinan*
- *Apakah butuh struktur engineer*



Gambar 11.2. NEMA Enclosure

11.1.2.4 Tujuan dan Kebutuhan Bisnis

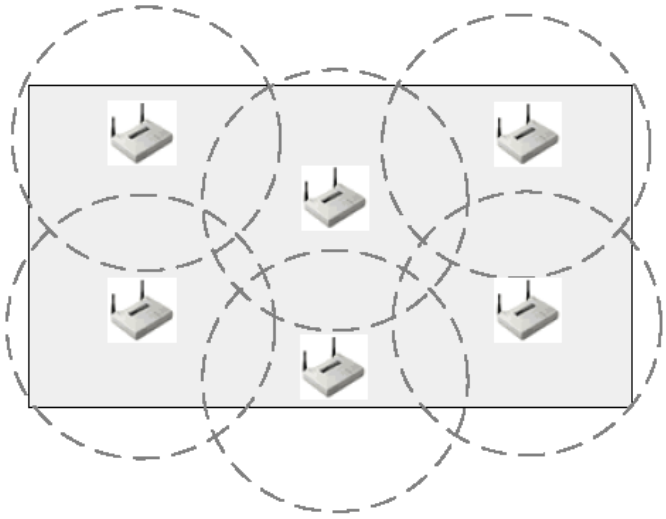
Apakah tujuan dari wireless LAN?...

Site surveyor harus memiliki pengetahuan darimana jaringan yang akan digunakan dan untuk tujuan apa. dengan mengetahui bagaimana effect jaringan wireless untuk tujuan bisnis, site surveyor akan dapat membuatnya lebih baik. site surveyor harus mengetahui kebutuhan bisnis untuk efisiensi survey site

11.1.2.5 Kebutuhan Bandwidth dan Roaming

Apakah dibutuhkan bandwith dan roaming?...

Dengan implementasi teknologi dan penggunaannya saat survey site sebagai contoh jika client di perumahan hanya menggunakan wireless LAN sebagai tujuan untuk scanning data dari box label dan mengirim data ke server maka bandwith yang dibutuhkan sangat kecil. pengumpulan data hanya membutuhkan 2 MBPS.



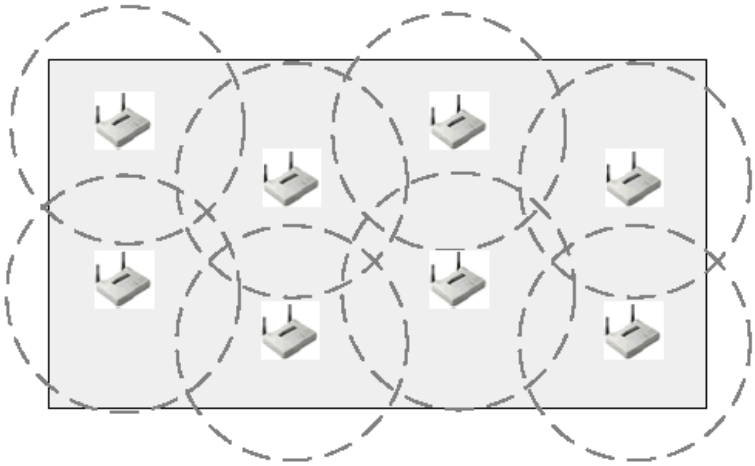
Gambar 11.3. 2 Mbps Data Rate

Berapa banyak pengguna?...

Dengan memahami berapa banyak pengguna yang akan dialokasikan dibutuhkan untuk menghitung besar data throughput masing-masing pengguna.

Tipe aplikasi apa yang akan digunakan wireless LAN?...

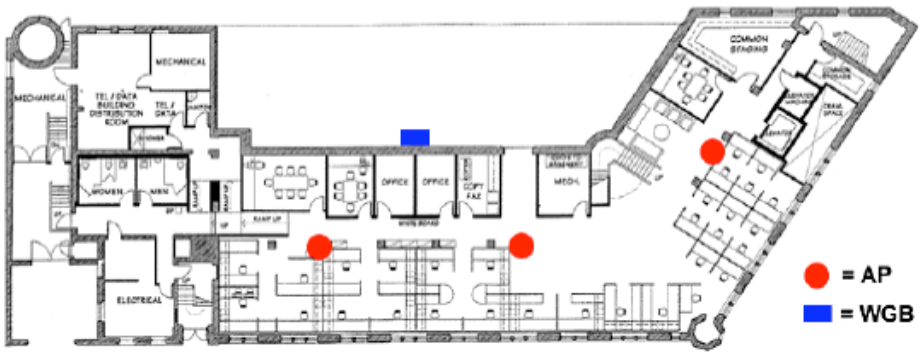
Jaringan digunakan hanya untuk transmit data non-time sensitive atau data time sensitive seperti suara atau video. Aplikasi bandwitdh besar seperti suara atau video membuthkan throughput yang lebih besar tiap pengguna.



Gambar 11.4. 5.5 Mbps Data Rate

11.1.2.6 Sumber yang Digunakan

Sumber yang digunakan berdasarkan pada budget project, waktu pengalokasian project, dan apakah administrator pernah ditraining tentang jaringan wireless.



Gambar 11.5. Contoh Blueprint Jaringan Wireless

11.1.2.7 Kebutuhan Keamanan

Level keamanan jaringan apa yang dibutuhkan?....

Diskusi dengan pelanggan akan menyediakan informasi untuk solusi pelanggan oleh designer.

11.2 Persiapan Latihan

- Apakah pelanggan bergerak menggunakan fasilitas seperti komputer portable atau desktop
- Berapa jauh koneksi yang dibutuhkan oleh pelanggan
- Level akses apa yang dibutuhkan pelanggan untuk sensitivitas data dalam jaringan, apakah membutuhkan keamanan, dan tipe keamanan seperti apa yang dibutuhkan
- Apakah pelanggan dapat mengambil laptop nya ketika card wireless LAN nya dicuri
- Apakah pelanggan menggunakan intensive bandwidth, sensitive time, atau aplikasi connection oriented.
- Berapa sering pelanggan melakukan perpindahan
- Apakah pelanggan memiliki akses internet
- Apakah perangkat pelanggan sering dirubah untuk event khusus yang dapat mengganggu kerja wireless LAN
- Siapa yang biasanya mendukung pelanggan dalam pengadaan jaringan, dan apakah mereka berkualitas untuk mendukung pelanggan wireless
- Jika pelanggan bergerak, tipe peralatan mobile computing apa yang mereka gunakan
- Berapa sering dan berapa jauh pelanggan bekerja dengan laptop tanpa daya AC

11.3 Persiapan Check List

- Dokumentasi sumber daya
- Dokumentasi survey site wireless LAN
- Pemetaan topologi
- Pertemuan dengan administrator jaringan

- Pertemuan dengan manager building
- Pertemuan dengan security officer
- Akses ke semua area fasilitas yang diakibatkan oleh wireless LAN
- Akses ke wiring closet
- Akses ke roof
- Rencana konstruksi masa depan

11.4 Peralatan Survey Site

- Access Point

  Digunakan selama survey site dengan power output yang bervariasi dan konektor antenna ekstenal.
- PC Card
- Laptop dan PDA
- Paper
- Spectrum analyzer

11.5 Menganalisis Jaringan (Sniffer)

Sniffer adalah perangkat yang digunakan untuk mencari wireless Lan lain yang telah ada pada suatu area. Bekerja dengan mengambil paket yang dipancarkan oleh Wireless lan tersebut lalu memuat data informasi terperinci mengenai wireless Lan yang telah ada pada area tersebut.

11.5.1 Kit check survey site

Perangkat yang termasuk dalam kit site survey

- Laptop dan/atau PDA.
- Wireless PC card dengan drivernya & software utility yang dibutuhkan.
- Bridge atau accsess Point jika dibutuhkan.
- Baterei kemasan & DC-TO-AC konvertor.
- Software utility site survey (dibuka dari laptop atau PDA).
- Alat tulis menulis.

- Cetak biru & diagram jaringan.
- Antenna dalam dan luar ruangan.
- Kabel & connectors.
- Teropong dan radio dua arah.
- Payung dan/atau perlengkapan hujan.
- Hardware atau software khusus seperti sniffer dan spectrum analyzer.
- Peralatan, selotip dan perlengkapan lain untuk perpindahan hardware sementara.
- pengamanan dan tempat sebagai isi hardware untuk computer rumah, peralatan, dan keamanan dokumen selama survei dan perjalanan dari lokasi survey.
- Kamera digital untuk mengambil gambar dari tempat tertentu di dalam suatu fasilitas.
- Pengisi baterei.
- Attenuator antenna .
- Roda untuk pengukuran.
- Tas travel atau cara lain untuk mengangkut peralatan & dokumentasi.

11.5.2 Mengadakan Survey Site

Mensurveilah ditempat dengan toolkit yang lengkap, berjalan beberapa miles sepanjang;seluruh client's fasilitas umum. RF site survey adalah 10% survey dan 90% berjalan, gunakan sepatu yang nyaman saat dilokasi yang besar.

11.5.2.1 Survey indoor

Untuk survey dalam ruang, menempatkan dan merekam materi pada suatu copy, cetakbiru atau suatu gambar menyangkut fasilitas itu.

11.5.2.2 Survey outdoor

Sebelum memulai, perhatikan hal – hal berikut ini :

- Siapa yang akan memasang dan memindahkan accsess point pada tempat – tempat yang tinggi.

- Apakah ada seseorang yang mau memindahkan pohon yang menghalangi pemasangan sesuai zona freznel.
- Jika diperlukan tower baru, apakah izinnya sudah siap.
- Apakah diperlukan izin untuk pemasangan antenna pada tower.
- Apakah bangunan memerlukan kode plenum rate untuk peralatan yang digunakan

11.5.3 Pengumpulan Informasi RF

Informasi yang perlu dikumpulkan

- Range dan pola cakupan
- Data rate yang dinilai
- Dokumentasi
- Tes menyeluruh dan perencanaan kapasitas
- Sumber interferensi
- Kabel koneksi data dan power AC yang dibutuhkan
- Penempatan antenna diluar ruang
- Pemeriksaan dadakan

11.5.4 Laporan Site Survey

Setelah secara menyeluruh mendokumentasikan fasilitas pelanggan, perlu disediakan data untuk menyiapkan suatu laporan yang tepat untuk klien itu. Laporan akan bertindak sebagai peta untuk implementasi menyangkut Wireless LAN dan dokumentasi sebagai acuan kedepan untuk pengurus dan teknisi jaringan.

Laporan lokasi adalah puncak dari semua usaha sampai sekarang, dan mungkin membutuhkan harian atau bahkan mingguan untuk melengkapi laporan. Mungkin saja diperlukan untuk mengunjungi lokasi untuk mengumpulkan lebih banyak data atau untuk mengkonfirmasikan sebagian dari penemuan awal. Beberapa lebih banyak percakapan mungkin diperlukan untuk membuat keputusan dan sebagian dari orang dengan yang tidak dapat ditemukan manakala berada ditempat lokasi.

- Format laporan

- Tujuan bisnis dan laporan lokasi survey
- Metodologi
- Cakupan area RF
- Keseluruhan
- Interference
- Masalah area
- Gambar

11.5.5 Laporan Tambahan

Untuk memberitahu pelanggan tentang pelayanan terbaik. Diperlukan tambahan data berupa Potongan informasi tambahan yang menjadi anggota dalam lokasi mensurvei laporan adalah penemuan gangguan interferensi, type peralatan yang diperlukan, dan usul penempatan peralatan.

11.6 Kesimpulan

Dalam membangun jaringan wireless, hal yang perlu diperhatikan adalah melakukan survei letak / lokasi, atau yang lebih dikenal sebagai Survey Site.RF (Radio Frequency). Hal ini penting dilakukan karena merupakan peta untuk keberhasilan implementasi jaringan wireless. Dan menentukan cakupan frekuensi dari sumber (access point). Persiapannya meliputi pengumpulan informasi, pembuatan keputusan, persiapan check list, mempersiapkan peralatan survey site, dan melakukan analisa terhadap jaringan.

11.7 SOAL

1. Desain dan gambarkan jaringan wireless indoor pada sebuah ruangan.. User yang akan menggunakan koneksi wireless berkisar 50 – 100 orang. ?
2. Berikan rincian harga dan keterangan secara detail dari soal nomor 1 ?
3. Apa saja yang diperlukan dalam pengumpulan informasi RF ?
4. Sebutkan peralatan yang dibutuhkan untuk melakukan survey site pada jaringan wireless ?

5. Sebutkan beberapa hal yang perlu diperhatikan dalam melakukan survei jaringan wireless outdoor ?

Kunci Jawaban

Bab 1.

1. Federal Communications Commission (FCC)
2. IEEE 802.11

   IEEE 802.11b

   IEEE 802.11a

   IEEE 802.11g
3. IEEE 802.11 :

   Standar asli wireless LAN menetapkan tingkat perpindahan data yang paling lambat dalam teknologi transmisi light-based dan RF.

   IEEE 802.11b :

   Menggambarkan tentang beberapa transfer data yang lebih cepat dan lebih bersifat terbatas dalam lingkup teknologi transmisi.

   IEEE 802.11a :

   Gambaran tentang pengiriman data lebih cepat dibandingkan (tetapi kurang sesuai dengan) IEEE 802.11b, dan menggunakan 5 GHZ frekuensi band UNII.

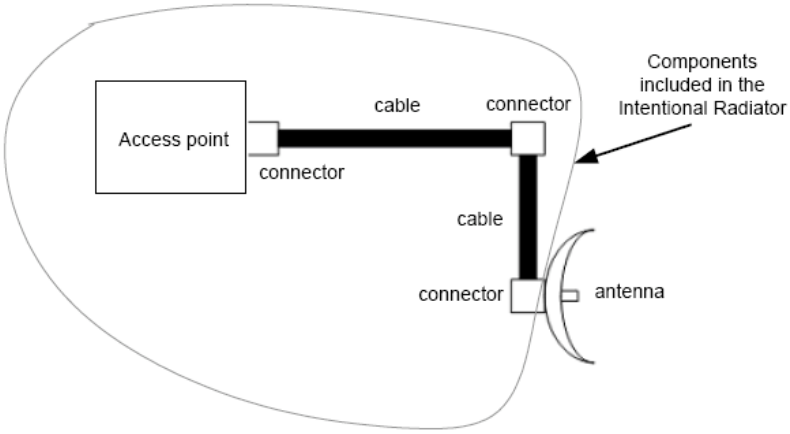
   IEEE 802.11g :

   Syarat yang paling terbaru berdasar pada 802.11 standard yang menguraikan transfer data sama dengan cepatnya seperti IEEE 802.11a, dan sesuai dengan 802.11b yang memungkinkan untuk lebih murah.
4. Akses Role, Perluasan Jaringan, Menghubungkan Gedung Satu dengan yang lain, Pengiriman Data Bermil-mil, Mobilitas, Small Office – Home Office, Mobile Offices.
5. Small Office – Home Office, merupakan salah satu aplikasi dari wireless LAN yang banyak digunakan oleh perusahaan dan efisiensi untuk pengunaan internet tunggal dan peningkatan produktifitas.

Bab 2.

1. Gain, Power Loss, Refleksi, Pembiasan, Difraksi, Scattering, Penyerapan (Absorpsi).

2. Sebuah peralatan RF yang secara khusus di-design untuk meng-generate dan me-radiasi sinyal RF. Dalam istilah hardware, intentional radiator meliputi peralatan RF dan semua pengkabelan juga konektor-konektor pendukung tetapi tidak termasuk antenna



3. - Daya (kekuatan) pada peralatan transmisi
   - Loss dan gain dari peralatan penghubung antara peralatan transmisi dan antenna, seperti kabel, konektor, amplifier, attenuator, dan splitters.
   - Daya (kekuatan) pada konektor terakhir sebelum sinyal RF masuk pada antenna (intentional Radiator).
   - Daya pada element antenna (EIRP)

4. 10.825 feet.
5. 6.021 db.

Bab 3.

1. Teknologi komunikasi yang hanya cukup digunakan dari frekwensi spectrum untuk membawa data sinyal, dan tidak lebih. Misi FCC untuk menjaga penggunaan frekwensi sebanyak mungkin, hanya membagi-bagikan apa yang diperlukan untuk melakukan pekerjaan.
2. Teknik yang menggunakan kecepatan frekwensi spread spectrum yang lebih dari 83 MHz. Kecepatan frekwensi mengacu pada kemampuan radio untuk merubah frekwensi transmisi di dalam RF band frekwensi yang dapat di pakai.
3. Merupakan sebuah metode pengiriman data dimana pengiriman dan penerimaan data berada pada range frekuensi 22 MHz. Chanel yang lebih lebar akan

membuat peralatan dapat mengirim informasi lebih tinggi daripada system FHSS.

4. Narrowband interference

   Co-Location

   Cost

   Equipment Compability & Availability

   Data rate & Thoughput

   Security

   Standards Support

5. DSSS menggabungkan sebuah data sinyal pada station pengiriman dengan kecepatan bit sequence yang tinggi dimana direferensikan sebagai chipping code atau penguatan prosesor. Sebuah prosesor yang tinggi akan menambah resistansi sinyal untuk saling berinteferensi. Proses dari direct sequence dimulai dengan sebuah carier dimodulasikan dengan kode sequence. Angka pada chips dalam kode akan menentukan bagaimana penyebaran terjadi dan angka dari chips serta kecepatan dari kode akan menentukan kecepata data.

Bab 4.

1. Root Mode

   Root Mode digunakan ketika accesss point dikoneksikan ke sebuah tulang punggung kabel (wired backbone) sepanjang interface kabel (biasanya Ethernet)/ kebanyakan accesss point mendukung model lebih dari model root hadir dikonfigurasikan secara default.

   Repeater Mode

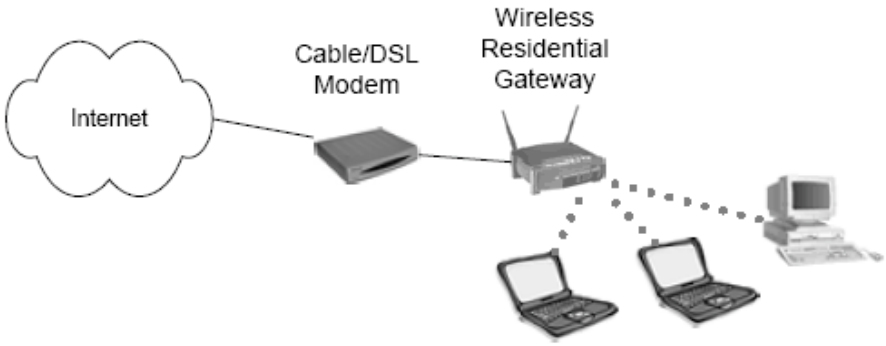
   Dalam mode pengulangan, access point memiliki kemampuan untuk mendukung sebuah koneksi wireless upstream (hulu) kedalam jaringan kabel lebih dari koneksi normal kabel. Satu access point melayani sebagai access point root dan lainnya melayani sebagai sebuah wireless repeater.

   Bridge Mode

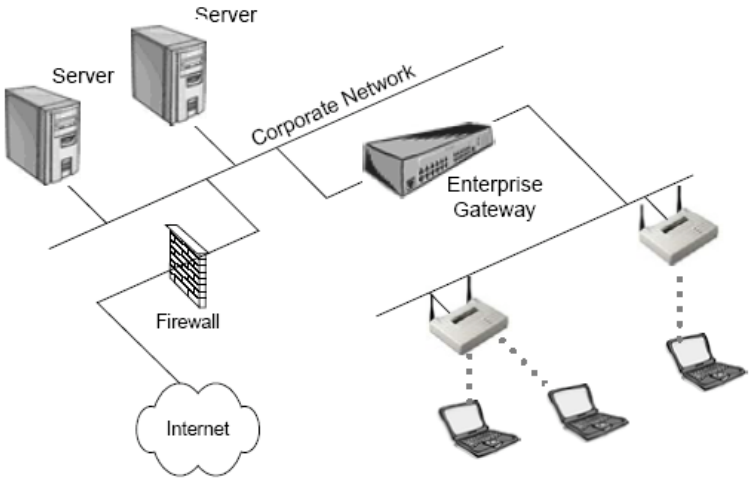
   Pada model jembatan, acces point bertindak tepatnya sebagai jembatan wireless, yang mana akan didiskusikan nanti pada bagian ini. Kenyataannya, mereka menjadi jembatan wireless ketika dikonfigurasikan pada cara ini. Hanya sebagian kecil acces point di pasaran yang memiliki fungsi jembatan,

yang mana ciri khasnya ditambahkan biaya tertentu untuk perlengkapan. Kita akan menjelaskan singkat bagaimana fungsi jembatan wireless.

2. - Gunakan duty zip ties untuk memasang access point ke kolom atau sorotan.
   - Jangan tutupi cahaya akses point ketika memasang access point dengan zip ties
   - Pasang access point terbalik sehingga lampu indikator dapat terlihat dari lantai
   - Beri nama access point
3. - PCMCIA dan Compact Flash(CF)
   - Ethernet dan Serial Converter
   - USB Adapter
   - PCI dan ISA Adapter
4. Peralatan yang didesain untuk menghubungkan sejumlah kecil titik wireless ke satu peralatan untuk Layer 2 (wireless dan non wireless) dan konektifitas layer 3 ke internet atau ke jaringan lain.

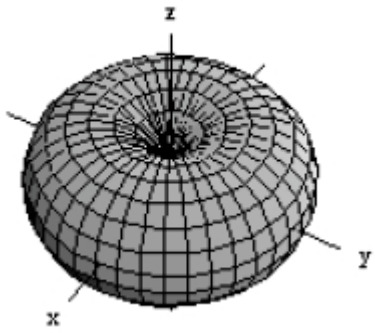


5. Piranti yang memberikan autensifikasi khusus dan konektifitas untuk wireless client. Enterprise Wireless Gateways cocok untuk lingkungan skala besar wireless LAN dimana memberikan banyak servise wireless LAN yang bisa di atur seperti rate limiting, Quality of Service(QoS), dan profile management.



Bab 5.

1. - Omni – directional
   - Semi – directional
   - Highly – directional
2. - Antenna memancarkan energinya secara bersamaan pada semua arah sekitar porosnya. Antenna directional memusatkan energinya dalam bentuk kerucut, dikenal dengan “beam”. Antenna omni-directional digunakan ketika melingkupi semua arah sekitar poros horizontal dari antenna dibutuhkan. Antenna omni-directional sangat efektif dimana jangkauan besar dibutuhkan disekitar titik pusat.



3. Insertion loss, Respon frekuensi, Impedansi, VSWR Rating, High isolation, Impedansi, Power Ratings, Tipe konektor, Report Kalibrasi, Mounting, DC voltage passing
4. - RF connector harusnya sesuai dengan impedansi dengan semua komponen wireless-LAN (biasanya 50 Ohms). Ini bukannya suatu permasalahan sejak ketika anda membeli konektor dengan impedansi yang berbeda, mereka tidak akan cocok jika bersama-sama karena ukuran dari pin-center-nya.
   - Kenali seberapa banyak insertion loss dari tiap konektor yang di sisipkan ke dalam path sinyal. Jumlah dari loss akan menyebabkan faktor ke dalam kalkulasi dari kekuatan sinyal yang anda inginkan dan juga jarak yang dibolehkan.
   - Kenali kenaikan batas frekuensi (respon frekuensi) yang di spesifikasikan untuk tiap konektor. Point ini akan sangat penting sebesar 5GHz wirelessLan menjadi lebih dan lebih. Beberapa konektor yang di hitung hanya sebesar 3 GHz, dimana ini baik di gunakan dengan 2.4 GHz wirelessLan, tapi akan tidak berjalan dengan baikuntuk 5GHz wirelessLan. Beberapa konektor yang di hitung hanya diatas 1 GHz dan akan sama sekali tidak berjalan dengan baik dengan wirelessLan, yang di legalkan hanya 900MHz wirelessLan.
   - Hati-hati dengan kualitas konektor yang buruk. Pertama, selalu pertimabngkan dari perusahaan yang bereputasi. Kedua,, belilah hanya konektor dengan kualitas tinggi yang dibuat oleh perusahaan yang terkenal. Bagian dari pembelian ini akan membantu anda untuk mengurangi permasalahan dengan sinyal RF yang sporadik, VSWR dan koneksi yang buruk.
   - Yakinlah bahwa anda mengetahui tipe dari konektor(N,F,SMA,dll) yang anda butuhkan dan jenis kelamin dari konektor itu sendiri. Konektor mempunyai 2 jenis kelamin, yaitu male dan female. Konektor male mempunyai pin center, sedangkan konektor female mempunyai receptable center.
5. Untuk menkonversi 1 range frekuensi ke lainnya untuk tujuan menghilangkan frekuensi bands.

Bab 6.

1. Federal Communications Commission (FCC) adalah agen pemerintah US yang langsung bertanggung jawab pada konggres. FCC didirikan oleh

Communication Act pada tahun 1934, yang mengatur komunikasi menggunakan radio, televisi, kawat, satelit dan kabel.

2. - ISM Band
   - 900 MHz ISM Band
   - 2,4 GHz ISM Band
   - 5,8 GHz. ISM Band

   - UNII Band
   - Lower Band
   - Middle Band
   - Upper Band

3. Institute of Electrical and Electronics Engineers (IEEE) adalah pembuat kunci yang baku untuk kebanyakan berbagai hal berhubungan dengan teknologi informasi di Amerika Serikat. IEEE menciptakan standard nya di dalam hukum yang diciptakan oleh FCC. Pokok-Pokok IEEE banyak teknologi baku seperti Public Key Cryptography (IEEE 1363), Firewire (IEEE 1394), Ethernet (IEEE 802.3), dan Wireless Lan (IEEE 802.11).
4. IrDA adalah suatu organisasi untuk menciptakan suatu interoperable murah, low-cost, low-power, half-duplex, standard interkoneksi data yang serial yang mendukung suatu gedung tanpa lift point-to-point model pemakai yang dapat menyesuaikan diri suatu cakupan luas.
5. - Class 1 → 1 mW
   - Class 2 → 2.5 mW
   - Class 3 → 100 mW

Bab 7.

1. - SSID → sebuah nilai unique, case sensitive, alphanumeric dari 2-31 panjang karakter yang digunakan oleh wireless LAN sebagai sebuah nama network.
   - Beacons → adalah frame pendek yang dikirim dari access point ke pemancar (Mode Infrastruktur) atau pemancar ke pemancar (Mode ad Hoc) yang digunakan mengorganisir dan mensinkronkan wireless pada LAN wireless itu.
2. - Passive Scanning → proses melacak beacon pada masing-masing saluran untuk suatu periode waktu yang spesifik setelah stasiun diinisialisasi beacon ini

dikirim oleh access point (model infrastruktur) atau stasiun klien (moded ad hoc

- Active Scanning → Active scanning melibatkan pengiriman dari suatu request pemeriksaan (probe) frame dari suatu pemancar wireless. Pemancar mengirim probe frame jika mereka secara aktif mencari suatu jaringan untuk digabungkan. Probe frame akan berisi baik SSID dari jaringan yang mereka ingin gabungkan atau suatu SSID broadcast.

3. - Unauthenticated and unassociated
   - Authenticated and unassociated
   - Authenticated and associated
4. - Basic service set → BSS terdiri dari hanya satu access point dan satu atau lebih klien wireless.
   - Extended Service Set → sebagai dua atau lebih layanan dasar menetapkan hubungan oleh suatu sistem distribusi secara umum.
   - Independent basic service set →
5. Pengesahan pemakai, Encryption, dan Pengesahan data.

Bab 8.

1. - Management Frame → Association request frame, Association response frame, Reassociation request frame, Reassociation response frame, Probe request frame, Probe response frame, Beacon frame, ATIM frame, Disassociation frame, Authentication frame, Deauthentication frame
   - Control Frame → Request to send (RTS), Clear to send (CTS), Acknowledgement (ACK), Power-Save Poll, Contention-Free End (CF End), CF End + CF Ack
   - Data Frame
2. Carrier Sense Multiple Access / *Collision Avoidance* CSMA/CA
3. Distributed Coordination Function → sebuah metode akses yang ditentukan pada standar 802.11 yang membolehkan semua pemancar pada sebuah wireless LAN untuk menghadapi akses pada media transmisi yang dibagikan (RF) menggunakan protocol CSMA/CA.

4. Sebuah mode pengiriman yang menyediakan pengiriman susunan bebas isi (contention-free) . pada sebuah wireless LAN dengan menggunakan mekanisme polling. PCF mempunyai keuntungan dari memberikan jaminan untuk mengetahui sejumlah hal yang tersembunyi jadi bahwa aplikasi-aplikasi membutuhkan QoS (suara atau gambar untuk contoh) yang bisa digunakan. Ketika menggunakan PCF, access point pada sebuah wireless LAN membentuk polling. Karena alasan ini, sebuah ad hoc jaringan tidak bisa memakai PCF, karena sebuah ad hoc jaringan tidak mempunyai access point untuk melakukan polling.
5. - Sort Interframe Space (SIFS) adalah ruang antar susunan terpendek yang ditentukan. SIFS adalah ruang waktu sebelum dan sesudah dimana tipe-tipe pesan-pesan berikut dikirim.

   - Point Coordination Function Interframe Space (PIFS) merupakan ruang antar susunan bukan merupakan jalur terpendek maupun jalur terpanjang ruang antar susunan yang ditentukan, jadi hal ini mendapatkan prioritas yand lebih dari pada DIFS dan kurang dari SIFS. Access point menggunakan sebuah ruang antar susunan PIFS hanya ketika jaringan pada mode fungsi koordinasi titik, yang secara manual dikonfigurasi oleh administrator. PIFS mempunyai durasi yang lebih pendek dari pada DIFS.

   - Distributed Coordination Function Interframe Space (DIFS) adalah ruang antar susunan yang paling panjang yang ditentukan dan digunakan secara default pada semua 802.11-pamancar-pemancar yang menggunakan fungsi koordinasi terdistribusi.

Bab 9.

1. Multipath digambarkan sebagai komposisi dari suatu salinan sinyal yang utama yang lebih atau medan disebabkan oleh pemantulan dari object penerima dan pemancar. Penundaan pada saat tertentu bahwa sinyal yang utama tiba bahwa sinyal terakhir dicerminkan yang datang dikenal sebagai penundaan secara menyebar. Efek yang dapat ditimbulkan antara lain : Sinyal Amplitude yang dikurangi (downfade), Korupsi, Nulling Sinyal, dan Amplitude yang ditingkatkan (upfade).

2. Solusi yang dapat digunakan untuk mengatasi Node yang tersembunyi yaitu dengan menggunakan RTS/CTS, meningkatkan power ke node, mencabut rintangan dan pindah node
3. - Meningkatkan mobilitas ke node yang lain
   - Pengurangan daya dari node lokal
   - Gerakkan node semakin dekat ke access point
4. - Gunakan Dua Access Point
   - Gunakan peralatan 802.11a
5. Gangguan Narrow band, Gangguan Allband, Cuaca, Angin, Stratifikasi, Petir dan Gangguan Channel yang berdekatan.

Bab 10.

1. WEP merupakan suatu algoritma enkripsi yang digunakan oleh shared key pada proses autentikasi untuk memeriksa user dan untuk meng-enkripsi data yang dilewatkan pada segment jaringan wireless pada LAN.
2. Merupakan mekanisme keamanan dasar yang digunakan untuk mendukung WEP dan atau AES. Filtering memiliki arti menutup semua hubungan yang tidak diijinkan dan membuka semua hubungan yang diijinkan. Filtering terdiri dari tiga tipe dasar yang dapat diimplementasikan pada WLAN, yakni SSID Filtering, MAC Address Filtering dan Protocol Filtering.
3. * Passive Attack → Eavesdroping merupakan penyerangan ke WLAN yang paling sederhana dan efektif. Metode ini tanpa meninggalkan jejak dari hacker itu sendiri.

   * Active Attack → Merupakan metode hacking yang memungkinkan seseorang mendapat hak akses yang digunakan untuk tujuan merusak. Dengan metode ini memungkinkan hacker dapat mengacak-acak data pada jaringan.

   * Jamming Attack → Merupakan metode yang dapat mematikan supply tegangan pada suatu jaringan

   * Man in the Middle Attack → Metode yang juga dikenal dengan istilah membajak.
4. PPTP dan IP Sec
5. - WEP
   - Cell Cizing

- User Autentification
- Menggunakan software Security tambahan
- Monitoring Hardware
- Menggunakan Switch (bukan Hub)
- Wireless DMZ
- Software update

Bab 11.

1. ----------
2. **----------**
3. - Range dan pola cakupan
   - Data rate yang dinilai
   - Dokumentasi
   - Tes menyeluruh dan perencanaan kapasitas
   - Sumber interferensi
   - Kabel koneksi data dan power AC yang dibutuhkan
   - Penempatan antenna diluar ruang
   - Pemeriksaan dadakan
4. - Access Point
   - PC Card
   - Laptop dan PDA
   - Paper
   - Spectrum Analyzer
5 - Siapa yang akan memasang dan memindahkan accsess point pada tempat – tempat yang tinggi
   - Apakah ada seseorang yang mau memindahkan pohon yang menghalangi pemasangan sesuai zona freznel.
   - Jika diperlukan tower baru, apakah izinnya sudah siap.
   - Apakah diperlukan izin untuk pemasangan antenna pada tower.
   - Apakah bangunan memerlukan kode plenum rate untuk peralatan yang digunakan

Daftar Pustaka

1. Certified Wireless Network Administraror. Official Study Guide, Exam PWO-100, Objective-by-Objective coverage of the CWNA certification exam.
2. http://wikipedia.com

Buku ini ditulis oleh mahasiswa D4 Telekomunikasi PENS-ITS
Dan disupervisi oleh :

Sritrusta Sukaridhoto