Facultad de Ciencias Sociales y de la Comunicación

Diplomatura en Gestión y Administración Pública

Asignatura de:

Redes de datos

Tema XI:

Redes inalámbricas

(Transparencias de clase)

DEPARTAMENTO DE LENGUAJES Y SISTEMAS INFORMÁTICOS

curso 2008/2009

Profesor: Manuel Fernández Barcell

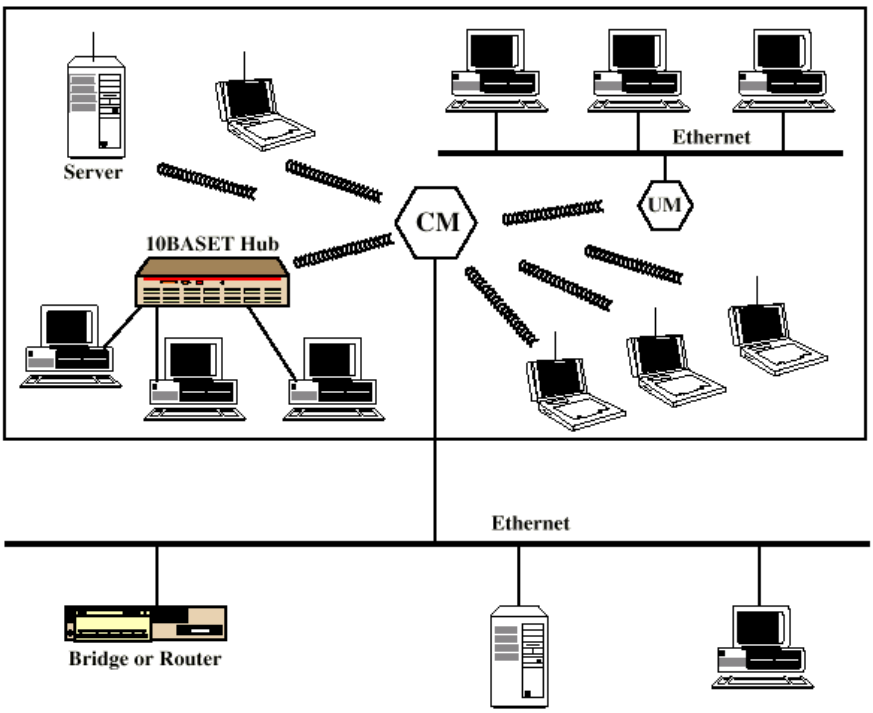
e-mail: manuel.barcell@uca.es

Índice

1 Redes inalámbricas

Son una alternativas a las redes cableadas para satisfacer necesidades de movilidad, traslado, trabajos en red *ad hoc* y coberturas en lugares difíciles de cablear.

Una red inalámbrica evita el coste de la instalación del cableado y facilitan las tareas de traslado y otras modificaciones de la estructura de red. Ejemplos: edificios de gran superficie, como plantas de fabricación, plantas comerciales y almacenes, edificios históricos.



1.1 Clasificación de redes inalámbricas

Lo primero que tenemos que hacer antes que nada es situarnos dentro del mundo inalámbrico. Para ello vamos a hacer una primera clasificación que nos centre ante las diferentes variantes que podemos encontrarnos:

- Redes inalámbricas personales
  - Infrarrojos
  - BlueTooth
- Redes inalámbricas 802.11 Las redes inalámbricas básicamente se diferencian de las redes conocidas hasta ahora por el enfoque que toman de los niveles más bajos de la pila OSI, el nivel físico y el nivel de enlace, los cuales se definen por el 802.11 del IEEE (Organismo de estandarización internacional).
- Redes inalámbricas de consumo
  - Redes CDMA (estándar de telefonía móvil estadounidense), GSM (estándar de telefonía móvil europeo y asiático), GPRS, UMTS, HSDPA. Son los estándares que usa la telefonía móvil empleados alrededor de todo el mundo en sus diferentes variantes. Vea http://www.gsmworld.com .
  - Redes WIMax (802.16e) son redes que pretenden complementar a las anteriores estableciendo redes inalámbricas metropolitanas (MAN) en la banda de entre los 2 y los 11 Ghz. Extiende su capacidad a radios que cubran importantes distancias (50 Km). Una de sus principales ventajas es la complementariedad con las redes Wifi (802.11)

con lo que los dispositivos que se utilizan habitualmente en cualquier equipo (tarjetas e incluso NAPs en compañías) pueden ser usadas en estas redes. La 802.16 usa frecuencias desde los 2 GHz a los 11 GHz para la creación de redes metropolitanas (MAN) funcionando como una extensión de las líneas ADSL o cable. Por ejemplo, basta conectar una línea ADSL a un transmisor 802.16 para que este ofrezca cobertura de banda rápida para 1000 residencias en una área. Su uso puede también extenderse a empresas, y el mismo ejemplo podría ofrecer servicios de alta velocidad hasta a 60 empresas en la misma área.. http://www.wirelessman.org/

1.2 Redes personales PAN (*Personal Area Network*)

Dentro del ámbito de estas redes podemos integrar a dos principales actores:

- En primer lugar la redes de **infrarrojos**. Estas redes se usan para el intercambio de información mediante infrarrojos. Estas redes son muy limitadas dado su cortísimo alcance, necesidad de visión sin obstáculos entre los dispositivos que se comunican y su baja velocidad (hasta 115 kbps). Se encuentran principalmente en ordenadores portátiles, PDAs (Agendas electrónicas personales), teléfonos móviles y algunas impresoras. Sobre esta tecnología ya la comentamos en el tema de Medio.
- En segundo lugar el **Bluetooth**, estándar de comunicación entre pequeños dispositivos de uso personal, como pueden ser los PDAs, teléfonos móviles de nueva generación y algún que otro ordenador portátil. (http://www.bluetooth.com).

1.2.1 Tecnología BlueTooth

Es una especificación para la industria informática y de las telecomunicaciones que describe un método de conectividad móvil universal con el cual se pueden interconectar dispositivos como teléfonos móviles, asistentes personales digitales PDA, ordenadores y muchos otros dispositivos. Utilizando una conexión inalámbrica de corto alcance.

Bluetooth es la tecnología que posibilita la conexión de dispositivos diferentes, un sistema que además está promovido por Ericsson (Suecia) y Nokia (Finlandia), dos países escandinavos.

Origen del nombre Bluetooth

En el siglo X, el rey Harald II de Dinamarca, apodado 'Diente azul' (Bluetooth) a causa de una enfermedad que le daba esta coloración a su dentadura, reunificó bajo su reinado a numerosos pequeños reinos que existían en Dinamarca y Noruega y que funcionaban con reglas distintas.

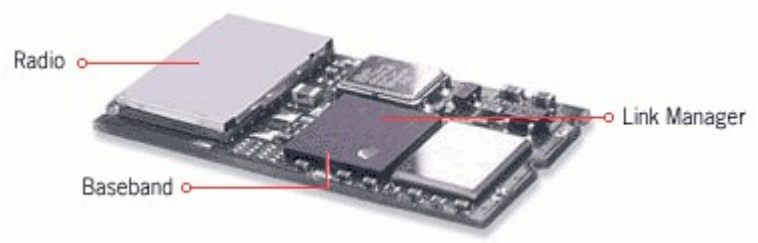
Banda de frecuencia

Emiten a 1 Mb en la banda de frecuencia de 2,4 GHz. La distancia operativa será de 10 metros.

2.4 Ghz. (Banda ISM). Potencia del transmisor: 1 mW para 10 m, 100 mW para 100 m. Tecnología: Espectro Expandido (Secuencia Directa y Saltos en Frecuencia). Canales máximos de voz: 3 por piconet. Canales máximos de datos: 7 por piconet. Velocidad de datos: hasta 721 kbit/s por piconet. Rango esperado del sistema: 10 metros (40 pies). Número de dispositivos: 8 por piconet y hasta 10 piconets. Alimentación: 2,7 voltios. Consumo de potencia: desde 30 uA a 30 mA transmitiendo. Tamaño del módulo: 0,5 pulgadas cuadradas (9x9 mm). Interferencia: Bluetooth minimiza la interferencia potencial al emplear saltos rápidos en frecuencia +/-1600 veces/segundo.

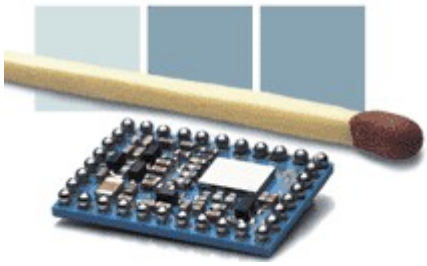
La solución sin cables

Frente a otras tecnologías en uso, como es la de infrarrojos -promovida por la IrDA- o la tecnología DECT, Bluetooth cuenta con el apoyo de la industria de Informática y de Telecomunicaciones, lo que garantiza su éxito. En la actualidad hay fabricantes que incorporan el interfaz IrDA en sus teléfonos, como Ericsson, Motorola y Nokia, pero su uso resulta frustrante para muchos usuarios que tratan sin éxito de descargar información desde sus PCs o PDAs hasta sus teléfonos móviles, o viceversa.



Los dispositivos que incorporan Bluetooth se reconocen y se hablan de la misma forma que lo hace un ordenador con su impresora; el canal permanece abierto y no requiere la intervención directa y constante del usuario cada vez que se quiere enviar algo.

El bajo precio que se espera que alcancen estos productos (en torno a 5 dólares, frente a los 20 o 30 actuales), hará que su inclusión en cualquier dispositivo suponga un bajo coste para el fabricante y el usuario, dando algunas estimaciones una cifra superior a los 1.000 millones de unidades en el año 2005.



Funcionamiento técnico

Cada dispositivo Bluetooth está equipado con un microchip (*transceiver*) que transmite y recibe en la frecuencia de 2.45 GHz. (2,402 hasta 2,480 en salos de 1 Mhz.). Esta tecnología está disponible en todo el mundo (con algunas variaciones de ancho de banda en diferentes países, como pasa en España, Francia y Japón) y no necesita licencia. Además de los canales de datos, están habilitados tres canales de voz a 64 kbit/s.

Cada dispositivo tiene una dirección única de 48 bits, basada en el estándar IEEE 802.11 para LAN inalámbricas, que le permite formar, temporalmente, parte de una piconet, es decir, una pequeña red (célula) que establece automáticamente los terminales

Bluetooth para comunicarse entre sí

Las conexiones son uno a uno con un rango máximo de diez metros, aunque utilizando amplificadores se puede llegar hasta los 100 metros, pero en ese caso se introduce alguna distorsión. Los datos se pueden intercambiar a velocidades de hasta 1 Mbit/s.

Un esquema de '*hop*' (saltos de frecuencia aleatorios) permite a los dispositivos comunicarse incluso en áreas donde existe una gran interferencia electromagnética. La tecnología Bluetooth provee además de mecanismos de cifrado (con longitud de la clave de hasta 64 bits) y autenticación, para controlar la conexión y evitar que cualquier dispositivo no autorizado pueda acceder a los datos o modificarlos. El manejo de la clave se realiza a nivel de la capa de aplicación.

Seguridad sin interferencias

Bluetooth se ha diseñado para operar en un ambiente multiusuario. Los dispositivos pueden habilitarse para comunicarse entre sí e intercambiar datos de una forma transparente al usuario. Hasta ocho usuarios o dispositivos pueden formar una piconet y hasta diez piconets pueden coexistir en la misma área de cobertura. Dado que cada enlace es codificado y protegido contra interferencia y pérdida de enlace, Bluetooth puede considerarse como una red inalámbrica de corto alcance muy segura.

En cuanto a interferencias con otros aparatos, hay que tener cuidado con los que operan en la misma banda. Al igual que está prohibido el uso de teléfonos móviles en los aviones, se puede impedir el uso de cualquier otro dispositivo que incorpore un chip Bluetooth, ya que podría interferir con los elementos de navegación.

El problema es que esta tecnología ha sido diseñada para mantener una comunicación continua, incluso en movimiento, y si el dispositivo Bluetooth se encuentra, por ejemplo, dentro de un maletín puede ocurrir que ni el usuario, por descuido, ni la tripulación de la nave, perciban que se está utilizando.

El protocolo banda base que utiliza Bluetooth combina las técnicas de conmutación de circuitos y de paquetes para asegurar que los paquetes llegan en orden. La velocidad para un canal asimétrico de datos puede llegar a 721 kbit/s en un sentido y 57,6 kbit/s en el otro, o 432,6 kbit/s en ambos sentidos si el enlace es simétrico.

Un aspecto importante, dado lo reducido del chip (ya que va a ir incorporado en dispositivos portátiles y alimentado con baterías) es que tenga un consumo de potencia muy reducido (hasta un 97% menos que un teléfono móvil). Si los dispositivos Bluetooth no intercambian datos establecen el modelo de 'espera' para ahorrar energía, quedando a la escucha de mensajes.

Aplicaciones de Bluetooth

La aplicación de la tecnología Bluetooth en la telefonía móvil han sido los kit Manos Libres portátiles. Estos dispositivos se acoplan a la oreja y se conectan con el móvil de forma inalámbrica, evitando así los incómodos cables

La marca sueca, además, ha desarrollado el producto Bluetooth Home Base, un aparato que permite usar el teléfono portátil como si fuera un terminal inalámbrico digital, es decir, realizar llamadas utilizando indistintamente la línea fija o móvil con un sólo aparato y de forma inalámbrica.

Bluetooth se puede incorporar a mandos a distancia, posibilita el uso de un teléfono móvil como si fuera un inalámbrico, sirve para abrir puertas, conectar electrodomésticos, pasar ficheros MP3 del móvil al PC, permite conectar cámaras de vigilancia, y por supuesto, todo tipo de dispositivos a Internet, formando puntos de acceso. Conectar el ratón, una impresora o un escáner al PC, disponer de un kit Manos Libres para el teléfono móvil sin necesidad de cable, sincronizar dispositivos de una manera totalmente automatizada, como que la agenda del terminal móvil y la del PC estén actualizadas al intercambiar información cada vez que uno de los aparatos entra en el área de influencia del otro, ya es posible con Bluetooth.

En el futuro Bluetooth permitirá la automatización del hogar, la lectura de contadores o para subir al autobús o al metro y sentarnos mientras el billete nos es facturado a nuestro monedero electrónico. Si, además de Bluetooth, el teléfono móvil integra un lector de código de barras se podrá pagar la compra en el hipermercado enviando desde el móvil directamente a la caja la información de los productos que se van cargando en el carrito. Confirmar una reserva de un vuelo y obtener la tarjeta de embarque, simplemente, con entrar en el recinto del aeropuerto, también será posible con esta tecnología. Si tuviéramos encendido el móvil, éste se comunicaría con el ordenador del aeropuerto, daría nuestra identificación y confirmaría la plaza. Estos datos se transmitirían a nuestro teléfono y servirían para realizar el embarque sin necesidad de soportar ninguna cola ni

solicitar ningún papel. Un ejecutivo al llegar a su puesto de trabajo y conectarse con la red local podrá recibir en su portátil todos los mensajes que tiene en su buzón de correo.

Su teléfono móvil, dotado con un dispositivo Bluetooth, le servirá para acceder a determinadas zonas sin necesidad de tarjeta de identificación; o al entrar al ascensor, automáticamente, subirle a la planta en la que trabaja, si es que no establece ninguna indicación en contra. También los coches en el futuro incorporarán un chip de Bluetooth que permitirá un control telemático de su funcionamiento.

En medicina, Bluetooth se podrá utilizar para la monitorización de los enfermos sin necesidad de que el paciente soporte cables conectados al cuerpo.

1.3 Redes WLAN

1.3.1 Tecnologías de las LAN inalámbricas

De los tres rangos de frecuencias tradicionales: Microondas, Onda Radio, e Infrarrojos, para la transmisión en redes locales se utilizan los siguientes:

- LAN de infrarrojos (IR) 1-2 Mb
  - Difusos (*diffuse*)
  - Haz directo (*Line of sight*, LOS)
- LAN de espectro expandido (1- 20 Mb)
- Microondas de banda estrecha (10- 20 Mb)

1.3.2 Introducción a WIFI (Fuentes: Víctor de la Nuez y Ander Otxoa Gilo)

La primera pregunta que se suele hacer es ¿Qué es ésto del *Wireless*? ¿Qué implica? ¿Qué ventajas tiene?

Wireless es un término que significa "SIN CABLES", y que designa a todos aquellos aparatos que, en su funcionamiento no requieren la conexión física entre él y otro.

Hablando más claro: el mando de la TV es *wireless*. Lo que ocurre, es que el término wireless se ha asociado a las comunicaciones 802.11b que son de las que estamos hablando. Es más correcto decir "tarjetas WIFI (*wireless fidelity*)" que "tarjetas *wireless*".

La tecnología de redes inalámbricas ofrece movilidad y una instalación sencilla, además permite la fácil ampliación una red. Es decir, que podemos estar moviéndonos por nuestra empresa / calle / parque / cafetería / aeropuerto, sin perder la conectividad con Internet. Esto es algo que actualmente está tomando gran importancia.¿Quién no ha tenido que enviar un correo electrónico urgente a alguien, y en ese momento no tienes acceso a Internet?

Dispositivos WIFI

Sea cual sea el estándar que elijamos vamos a disponer principalmente de dos tipos de dispositivos:

Punto de acceso *(Access Point*) (PA):

Son los encargados de recibir la información de las diferentes tarjetas inalámbricas de las que conste la red bien para su centralización o bien para su encaminamiento.

Se suele abreviar como PA. Piensa en ellos como un concentrador (HUB) de red normal: a él se conectan los equipos y es él quien reparte los paquetes. En WIFI es algo similar. Es un dispositivo que 'gestiona', los paquetes lanzados por otras estaciones inalámbricas, haciéndolas llegar a su destino. Además el punto de acceso, da conectividad a una red cableada, por lo que la red inalámbrica puede acceder a otros equipos que estuvieran en una red cableada.

Tarjetas WIFI (TR):

Las más conocidas son las que vienen en formato PCMCIA, para portátiles, aunque también las hay en formato PCI, en CompactFlash, Smart Card y similares. Son equivalentes a una tarjeta de red normal, sólo que sin cables. Su configuración a nivel de IP es EXACTAMENTE igual que una Ethernet.

Las diferencias más importantes entre una WIFI y una Ethernet, (a parte de que las primeras no llevan cable...) son: El cifrado de datos, el ESSID, el Canal, y el ajuste de velocidad. Hablaré de todas ellas un poco más adelante.

A parte de las tarjetas, existen más aparatos: Bridges, Router, Gateways.... pero no es habitual encontrarlos en la aplicación que nos interesa ahora.

Ethernet Converters

Los Ethernet Converters son aparatos que en esencia, son lo mismo que las tarjetas mencionadas anteriormente, salvo que se conectan al PC por medio de cable Ethernet (cable de red), lo que supone una enorme ventaja: no es necesario instalar ningún tipo de Driver en el PC... es más, no es necesario conectar un PC: valen MAC, impresoras de red, autómatas... en el mundo PC la ausencia de drivers supone que equipos basados en sistemas operativos no soportados generalmente por equipos WiFi (Linux, QNX, Solaris, etc...) no tendrán problema.

Algunos puntos de acceso incorporan una característica que hace las veces de Ethernet Converter y es el 'Modo Cliente'.

Antenas:

Actualmente ya hay fabricantes que ofrecen antenas que aumentan la capacidad de TX/RX (transmisión y recepción) de los dispositivos *wireless*.

Dentro de los PAs (actualmente ya se puede comenzar a aplicar también a los TRs) se puede modificar enormemente la capacidad de transmisión/recepción, gracias al uso de antenas especiales. Entre los modelos y variantes de antenas, se pueden distinguir 2 grandes familias:

- Las antenas Direccionales y
- Las antenas Omnidireccionales.

Las antenas Direccionales envían la información a una cierta zona de cobertura, a un ángulo determinado, por lo cual su alcance es mayor, sin embargo fuera de la zona de cobertura no se escucha nada, no se puede establecer comunicación entre los interlocutores.

Las antenas Omnidireccionales envían la información teóricamente a los 360 grados por lo que es posible establecer comunicación independientemente del punto en el que se esté., pero sólo sobre el plano perpendicular de la antena. En contrapartida el alcance de estas antenas es menor que el de las antenas direccionales. Dentro del grupo de antenas direccionales, tenemos las de Rejilla o *Grid*, las *Yagi*, las parabólicas, las "*Pringles*" y las de Panel. Las omnidireccionales suelen ser una simple varilla vertical.

Hay que decir que cuanta más alta sea la ganancia de la antena, mayores distancias podremos cubrir con una antena, y con mejor calidad podremos captar señales que pudieran llegarnos muy débilmente.

Para que te sirva de referencia, te pongo algunas distancias conseguidas con antenas:

- **Antena de Parrilla de 24dB de ganancia**: 70,5 km (El enlace entre Gran Canaria y Tenerife se hizo con ésta antena.)

- **Antena de Parrilla de 19dB de ganancia**: 54 km entre dos antenas iguales.
- **Antena OmniDireccional de 8dB de ganancia**: 25 km de distancia, al otro extremo había una de 19dB grid.A 10km el enlace era a 11Mbps, y a esa misma distancia conectamos entre 2 Omnis a 2Mbps.

El Pigtail

El Pigtail, o rabo de cerdo, no es más que un pequeño cable, que sirve de adaptación entre la tarjeta WIFI y la antena o el cable que vaya hacia la antena. Este *Pigtail* tiene 2 conectores: el propietario de cada tarjeta en un extremo, y por el otro un conector N estándar en la mayoría de los casos. El *pigtail* depende del fabricante de la tarjeta, por lo que no es una cosa estándar, aunque es verdad que el más conocido es el compatible con las tarjetas AVAYA y ORINOCO. El uso de este cable es IMPRESCINDIBLE para conectar una antena a la tarjeta, salvo en algunos modelos de antenas diseñadas expresamente para usar en interiores, que ya vienen con ese conector de serie.

información sobre antenas:

- http://www.34t.com/unique/WiFiAntenas.asp
- http://www.ciudadwireless.com/index.php
- http://www.cablematic.com/

Funcionamiento de los dispositivos

Vamos a referirnos principalmente al 802.11g, por ser el probable vencedor de la guerra de estándares abierta hoy en día, aunque lo explicado será fácilmente extrapolable a los demás teniendo en cuenta las características propias de cada uno.

Todos los estándares aseguran su funcionamiento mediante la utilización de dos factores, cuando estamos conectados a una red mediante un cable, sea del tipo que sea, disponemos de una velocidad fija y constante. Sin embargo cuando estamos hablando de redes inalámbricas aparece un factor añadido que puede afectar a la velocidad de transmisión, que es la distancia entre los interlocutores.

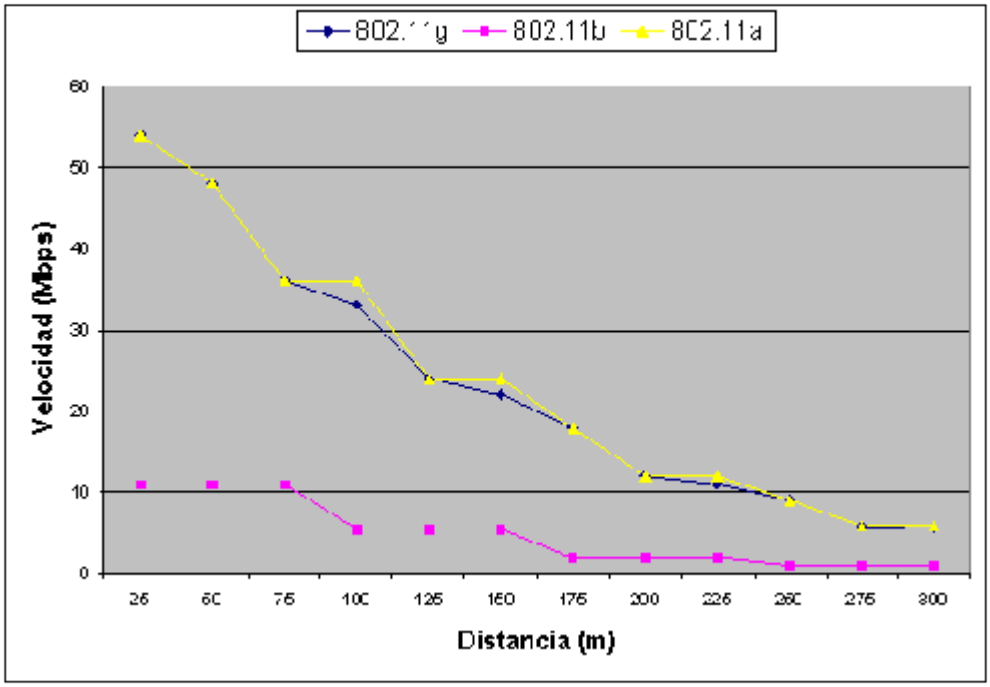
Así pues cuando un TR se conecta a un PA se ve afectado principalmente por los siguientes parámetros:

- Velocidad máxima del PA (normalmente en 802.11g será de 54Mbps)
- Distancia al PA (a mayor distancia menor velocidad)
- Elementos intermedios entre el TR y el PA (las paredes, campos magnéticos o eléctricos u otros elementos interpuestos entre el PA y el TR modifican la velocidad de transmisión a la baja)
- Saturación del espectro e interferencias (cuantos más usuarios inalámbricos haya en las cercanías más colisiones habrá en las transmisiones por lo que la velocidad se reducirá, esto también es aplicable para las interferencias.)

Normalmente los fabricantes de PAs presentan un alcance teórico de los mismos que suele andar alrededor de los 300 metros. Esto obviamente es sólo alcanzable en condiciones de laboratorio, pues realmente en condiciones objetivas el rango de alcance de una conexión varía (y siempre a menos) por la infinidad de condiciones que le afectan.

Cuando ponemos un TR cerca de un PA disponemos de la velocidad máxima teórica del PA, 54 Mbps por ejemplo, y conforme nos vamos alejando del PA, tanto él mismo como el TR van disminuyendo la velocidad de la transmisión/recepción para acomodarse a las condiciones puntuales del momento y la distancia.

Así pues, se podría decir que en condiciones de laboratorio y a modo de ejemplo teórico, la transmisión entre dispositivos 802.11 podría ser como sigue:



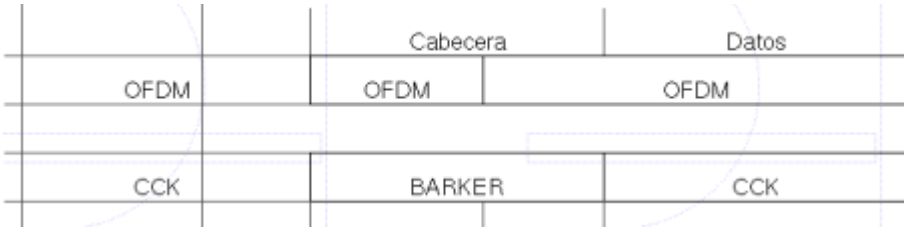
Velocidad vs Modulación

Cuando transmitimos información entre dos dispositivos inalámbricos, la información viaja entre ellos en forma de tramas. Estas tramas son básicamente secuencias de bits. Las secuencias de bits están divididas en dos zonas diferenciadas, la primera es la cabecera y la segunda los datos que verdaderamente se quieren transmitir.

La cabecera es necesaria por razones de gestión de los datos que se envían. Dependiendo de la forma en la que se module la cabecera (o preámbulo), podemos encontrarnos con diferentes tipos de tramas, como son:

- Barker. (RTS / CTS)
- CCK. Complementary Code Keying
- PBCC. Packet Binary Convolutional Coding
- OFDM. Orthogonal Frequency-Division Multiplexing

Una representación gráfica de las tramas más importantes:



Como podemos ver la cabecera en el caso de la codificación OFDM es más pequeña. A menor tamaño de cabecera menor *overhead* en la transmisión, es decir, menor tráfico de bits de gestión luego mayor sitio para mandar bits de datos. Lo que repercutirá positivamente en el rendimiento de la red.

		802.11a		802.11b		802.11g	
Velocidad nominal	Portadora	Obligatorio	Opcional	Obligatorio	Opcional	Obligatorio	Opcional
1	única			Barker		Barker	
2	única			Barker		Barker	
5.5	única			CCK	PBCC	CCK	PBCC
6	múltiple	OFDM				OFDM	CCK-OFDM
9	múltiple		OFDM				OFDM, CCK-OFDM
11	única			CCK	PBCC	CCK	PBCC
12	múltiple	OFDM				OFDM	CCK-OFDM
18	múltiple		OFDM				OFDM, CCK-OFDM
22	única						
24	múltiple	OFDM				OFDM	CCK-OFDM
33	única						
36	múltiple		OFDM				OFDM, CCK-OFDM
48	múltiple		OFDM				OFDM, CCK-OFDM
54	múltiple		OFDM				OFDM, CCK-OFDM

Ya a primera vista podemos ver que el estándar 802.11g es una unión de los estándares 802.11 a y b. Contiene todos y cada uno de los tipos de modulación que éstos usan, con la salvedad de que [a] opera en la banda de los 5 Ghz, mientras que los otros dos operan en la del los 2,4 Ghz.

Cuando tenemos una red inalámbrica en la que todos los dispositivos son tipo a o todos de tipo b no hay problemas en las comunicaciones. Cada AP tipo a tendrá sólo TRs tipo a y los APs tipo b tendrán sólo TRs tipo b. Se seleccionará la mejor modulación y se transmitirá. Si la comunicación óptima no es posible debido a una excesiva distancia entre los dispositivos o por diferentes tipos de interferencias se va disminuyendo la velocidad hasta que se encuentre la primera en la que la comunicación es posible.

En el caso de dispositivos AP 802.11g normalmente estaremos usando la modulación OFDM, modulación que es la óptima para este estándar.

Si por un casual un dispositivo 802.11b quisiera hablar con otro dispositivo 802.11g, este último debería aplicar una modulación compatible con el estándar b, cosa que es capaz de hacer. Sin embargo el dispositivo b no puede escuchar las transmisiones de los otros dispositivos g que hablan con su *partner* pues éstos usan una modulación que él no es capaz de entender. Si un dispositivo b comenzase a hablar a la vez que un dispositivo g se producirían colisiones que impedirían la transmisión, no por que interfieran ya que usan diferente modulación sino porque el AP normalmente sólo será capaz de hablar con un dispositivo a la vez.

Para evitar las colisiones, los equipos b usan la modulación Barker con TRS/CTS (*Request To Send / Clear To Send*), que básicamente significa que deben pedir permiso al AP para transmitir.

Topologías y modos de funcionamiento de los dispositivos

Es conveniente el hacer una división entre la topología y el modo de funcionamiento de los dispositivos WiFi. Con topología nos referimos a la disposición lógica (aunque la disposición física también se pueda ver influida) de los dispositivos, mientras que el modo de funcionamiento de los mismos es el modo de actuación de cada dispositivo dentro de la topología escogida.

En el mundo *Wireless* existen dos topologías básicas:

- **AD-HOC**: Una red "Ad Hoc" consiste en un grupo de ordenadores que se comunican cada uno directamente con los otros a través de las señales de radio sin usar un punto de acceso. Las configuraciones "Ad Hoc" son comunicaciones de tipo punto-a-punto. Los ordenadores de la red inalámbrica que quieren comunicarse entre ellos necesitan configurar el mis-

mo canal y ESSID en modo "Ad Hoc". Ahora puede surgir una pregunta: ¿Qué es el ESSID?, pues es un identificador de red inalámbrica. Es algo así como el nombre de la red, pero a nivel WIFI.

- **INFRASTRUCTURE**: Esta es la forma de trabajar de los puntos de acceso. Si queremos conectar nuestra tarjeta a uno de ellos, debemos configurar nuestra tarjeta en este modo de trabajo. Sólo decir que esta forma de funcionamiento es bastante más eficaz que AD HOC, en las que los paquetes "se lanzan al aire, con la esperanza de que lleguen al destino..", mientras que *Infrastructure* gestiona y se encarga de llevar cada paquete a su sitio. Se nota además el incremento de velocidad con respecto a AD HOC.

Todos los dispositivos, independientemente de que sean TRs o PAs tienen dos modos de funcionamiento. Tomemos el modo Infraestructura como ejemplo:

- Modo *Managed*, es el modo en el que el TR se conecta al AP para que éste último le sirva de concentrador. El TR sólo se comunica con el AP.
- Modo *Master*. Este modo es el modo en el que trabaja el PA, pero en el que también pueden entrar los TRs si se dispone del firmware apropiado o de un ordenador que sea capaz de realizar la funcionalidad requerida.

Estos modos de funcionamiento nos sugieren que básicamente los dispositivos WiFi son todos iguales, siendo los que funcionan como APs realmente TRs a los que se les ha añadido cierta funcionalidad extra vía firmware o vía SW. Para realizar este papel se pueden emplear máquinas antiguas 80486 sin disco duro y bajo una distribución especial de linux llamada LINUXAP/OPENAP.

Modos de funcionamiento

Los puntos de acceso inalámbricos (Access Points) pueden funcionar en tres tipos de modo diferentes: Maestro (Root), Repetidos (Repeater) y puente (Bridge).

Modo Root:

Este es el modo mas común donde múltiples usuarios acceden al punto de acceso al mismo tiempo. En modo maestro, usuarios con portátiles y PDA’s pueden acceder a Internet a través de un solo Access Point compartiendo la conexión.

Hay que aclarar que existe una diferencia entre un usuario móvil y un usuario “roaming”. Un usuario móvil se mantiene conectado al mismo punto de acceso. Un usuario “roaming” se mueve del área de cobertura de una Access Point (llamado celda) a otro Access Point distinto. Precisamente el término “roaming” significa la capacidad de moverse de una zona de cobertura a otra.

Modo Repeater:

El modo repetidor se utiliza cuando quieres extender tu señal mas allá de los limites actuales. Necesitas emplazar el punto de acceso en modo repetidor dentro del área de un punto de acceso en modo Root. Con esto la señal del AP maestro se extenderá con igual fuerza por medio de este AP repetidor mejorando el alcance.

Modo Bridge:

Como especifica el nombre, hacemos un puente inalámbrico entre dispositivos. Dos puntos de acceso en modo “bridge” solo hablarán entre ellos. Este tipo de conexión es útil cuando estás conectando dos edificios o localizaciones separadas donde instalar cableado no resulta fácil o económicamente viable.

Para preparar un puente inalámbrico necesitarás dos puntos de acceso y dos antenas direccionales.

Mesh Networks

Los inicios de las redes acopladas son, como no, militares. Inicialmente se usaron para comunicarse con aquellas unidades de militares que aún estando lejos de las zonas de cobertura de sus mandos estaban lo suficientemente cerca entre si como para formar una cadena a través de la cual se pudiese ir pasando los mensajes hasta llegar a su destino (los mandos).

Las redes *Mesh*, o redes acopladas, para definirlas de una forma sencilla, son aquellas redes en las que se mezclan las dos topologías de las redes inalámbricas. Básicamente son redes con topología de infraestructura, pero que permiten unirse a la red a dispositivos que a pesar de estar

fuera del rango de cobertura de los PA están dentro del rango de cobertura de algún TR que directamente o indirectamente está dentro del rango de cobertura del PA.

También permiten que los TRs se comuniquen independientemente del PA entre sí. Esto quiere decir que los dispositivos que actúan como TR pueden no mandar directamente sus paquetes al PA sino que pueden pasárselos a otros TRs para que lleguen a su destino.

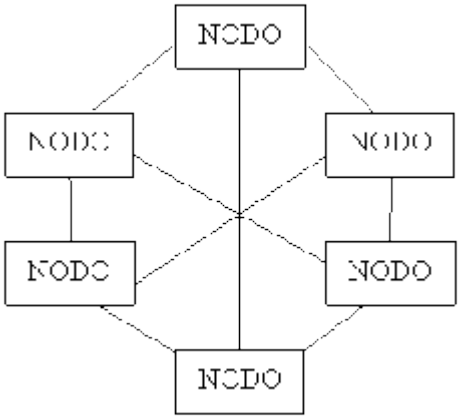
Para que esto sea posible es necesario el contar con un protocolo de enrutamiento que permita transmitir la información hasta su destino con el mínimo número de saltos (Hops en inglés) o con un número que aún no siendo el mínimo sea suficientemente bueno.

Es tolerante a fallos, pues la caída de un solo nodo no implica la caída de toda la red.

Antiguamente no se usaba porque el cableado necesario para establecer la conexión entre todos los nodos era imposible de instalar y de mantener. Hoy en día con la aparición de las redes inalámbricas este problema desaparece y nos permite disfrutar de sus grandes posibilidades y beneficios.

Hoy por hoy uno de los principales fabricantes de SW y HW para redes acopladas es LocustWorld. http://www.locustworld.com.

A modo de ejemplo de muestra una red acoplada formada por seis nodos. Se puede ver que cada nodo establece una comunicación con todos los demás nodos. Si este gráfico ya comienza a ser complicado, imagine si el número de nodos fuese de varios cientos.



Seguridad en las comunicaciones inalambricas

La seguridad es una de los temas más importantes cuando se habla de redes inalámbricas. Desde el nacimiento de éstas, se ha intentado el disponer de protocolos que garanticen las comunicaciones, pero han sufrido de escaso éxito. Por ello es conveniente el seguir puntual y escrupulosamente una serie de pasos que nos permitan disponer del grado máximo de seguridad del que seamos capaces de asegurar.

Terminología

Para poder entender la forma de implementar mejor la seguridad en una red inalambrica, es necesario comprender primero ciertos elementos:

- WEP. Significa *Wired Equivalet Privacy*, y fue introducido para intentar asegurar la autenticación, protección de las tramas y confidencialidad en la comunicación entre los dispositivos inalámbricos. Puede ser WEP64 (40 bits reales) WEP128 (104 bits reales) y algunas marcas están introduciendo el WEP256. Este protocolo no es 100% seguro, que hay software dedicado a violar este cifrado, aunque requiere tiempo. Es INSEGURO debido a su arquitectura, por lo que el aumentar los tamaños de las claves de cifrado sólo aumenta el tiempo necesario para romperlo. Se puede habilitar o deshabilitar WEP y especificar una clave de cifrado. Todas las estaciones que necesiten comunicarse deben usar la misma clave para generar la llave de cifrado.
- WPA: es la versión mejorada de WEP. Su nivel de seguridad es mucho más alto. Para WPA, se requiere el cifrado con el protocolo TKIP. El protocolo TKIP sustituye a WEP con un algoritmo de cifrado nuevo más seguro que el algoritmo de WEP que, sin embargo,

utiliza las utilidades de cálculo de los dispositivos inalámbricos existentes para realizar las operaciones de cifrado.

- OSA vs SKA. OSA (*Open System Authentication*), cualquier interlocutor es válido para establecer una comunicación con el AP. SKA (*Shared Key Authentication*) es el método mediante el cual ambos dispositivos disponen de la misma clave de cifrado, entonces, el dispositivo TR pide al AP autenticarse. El AP le envía una trama al TR, que si éste a su vez devuelve correctamente codificada, le permite establecer comunicación.
- ACL. Significa *Access Control List*, y es el método mediante el cual sólo se permite unirse a la red a aquellas direcciones MAC que estén dadas de alta en una lista de direcciones permitidas.
- CNAC. Significa *Closed Network Access Control*. Impide que los dispositivos que quieran unirse a la red lo hagan si no conocen previamente el SSID de la misma.
- SSID. Significa *Service Set IDentifier*, y es una cadena de 32 caracteres máximo que identifica a cada red inalámbrica. Los TRs deben conocer el nombre de la red para poder unirse a ella.

AUTENTICACIÓN CENTRALIZADA

Pero la seguridad depende de mucho más que la sola cifra. Es necesario disponer de un sólido mecanismo de autenticación que, además de garantizar la identidad de los usuarios y estaciones de trabajo, ayude a escalar sin temores los entornos inalámbricos 802. La nueva norma 802.1X ayuda en la tarea proporcionando un mecanismo estándar para autenticar centralmente estaciones y usuarios, simplificando así el soporte de cientos o miles de puestos. 802.1X será además lo suficientemente flexible para soportar distintos algoritmos de autenticación, y, como estándar abierto , facilitará a los fabricantes el desarrollo de innovaciones y mejoras complementarias. Básicamente, 802.1X se apoya en el protocolo de autenticación EAP (*Extensible Authentication Protocol*), vinculándolo al medio físico de la red. Para ello, los mensajes EAP son encapsulados en mensajes 802.1X, creando lo que se conoce como EAP *over* LAN.

ESQUEMA FUNCIONAL

La autenticación 802.1X para WLAN se basa entres componentes principales: el solicitante (generalmente el software cliente), el autenticador (el punto de acceso) y el servidor de autenticación (por lo general, pero no necesariamente, un servidor RADIUS -*Remote Authentication Dial-InUser Service*).Cuando un puesto cliente intenta conectar con el punto de acceso, éste le detecta y activa su puerto para proceder a la autenticación, al tiempo que le desautoriza a que transmita ningún tipo de tráfico salvo el relacionado con 802.x. El cliente entonces, utilizando EAP, envía un mensaje de inicio al punto de acceso, que, al recibirlo ,devuelve un mensaje de petición de identidad. El cliente le remite acto seguido un mensaje de respuesta con su identidad, que será pasado al servidor de autenticación. El resultado es un paquete de aceptación o rechazo que el servidor envía al punto de acceso, que, nada más recibirlo ,vuelve a autorizar al puerto del cliente a que comience la transmisión. Con este simple esquema centralizado de funcionamiento, 802.1X tiene el potencial de simplificar la gestión de la seguridad de grandes despliegues inalámbricos. Pero hay que recodar que la autenticación no es la única pieza del puzzle de la seguridad de los entornos 802.11. Su utilización requiere obviamente la presencia de un algoritmo de autenticación y de un sistema de cifrado de datos. Juntos, los tres componentes ofrecen a los administradores de redes un modo efectivo de proporcionar servicios de red móviles, flexibles, gestionables y escalables .

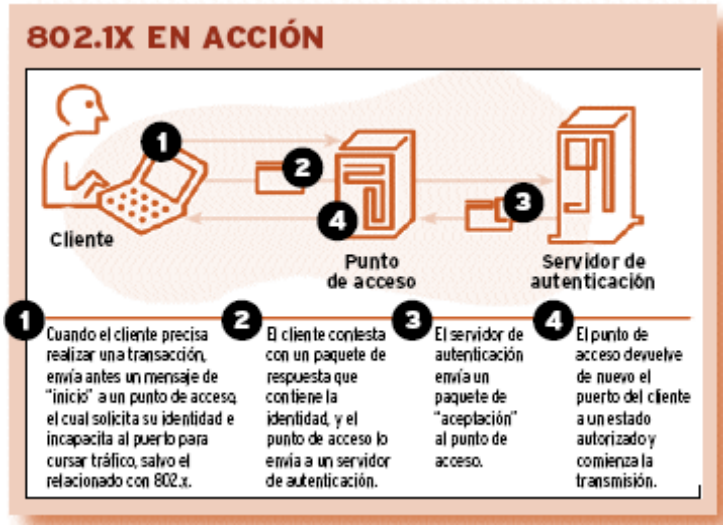
Pasos para asegurar una red inalámbrica

En primer lugar hay que situarse dentro de lo que seguridad significa en el mundo informático.

Se dice que una red es segura cuando casi nadie puede entrar la misma o los métodos de entrada son tan costosos que casi nadie puede llevarlos a cabo. Casi nadie puede significar que es segura en un 99.99%, por ello debemos desechar la idea de que los sistemas informáticos son seguros al 100%. No es cierto.

Un sistema es seguro cuando tiene la protección adecuada al valor de la información que contiene o que puede llegar a contener.

Una vez situados vamos a ver los pasos que podemos seguir para introducir una seguridad razonablemente alta a nuestra red *inalámbrica*. Debemos tener en cuenta que cuando trabajamos con una red convencional cableada disponemos de un extra de seguridad, pues para conectarse a la misma normalmente hay que acceder al cable por el que circula la red o a los dispositivos físicos



de comunicación de la misma. En nuestro caso no, de hecho vamos a estar desperdigando la información hacia los cuatro vientos con todo lo que esto conlleva.

- Paso 1, debemos activar el WEP. Parece obvio, pero no lo es, muchas redes inalámbricas, bien por desconocimiento de los encargados o por desidia de los mismos no tienen el WEP activado. Esto viene a ser como si el/la cajero/a de nuestro banco se dedicase a difundir por la radio los datos de nuestras cuentas cuando vamos a hacer una operación en el mismo. WEP no es completamente seguro, pero es mejor que nada.
- Paso 2, debemos seleccionar una clave de cifrado para el WEP lo suficientemente difícil como para que nadie sea capaz de adivinarla. No debemos usar fechas de cumpleaños ni números de teléfono, o bien hacerlo cambiando (por ejemplo) los ceros por “oes”.
- Paso 3, uso del OSA. Esto es debido a que en la autenticación mediante el SKA, se puede comprometer la clave WEP, que nos expondría a mayores amenazas. Además el uso del SKA nos obliga a acceder físicamente a los dispositivos para poder introducir en su configuración la clave. Es bastante molesto en instalaciones grandes, pero es mucho mejor que difundir a los cuatro vientos la clave. Algunos dispositivos OSA permiten el cambiar la clave cada cierto tiempo de forma automática, lo cual añade un extra de seguridad pues no da tiempo a los posibles intrusos a recoger la suficiente información de la clave como para exponer la seguridad del sistema.
- Paso 4, desactivar el DHCP y activar el ACL. Debemos asignar las direcciones IP manualmente y sólo a las direcciones MAC conocidas. De esta forma no permitiremos que se incluyan nuevos dispositivos a nuestra red. En cualquier caso existen técnicas de *sniffing* de las direcciones MAC que podrían permitir a alguien el descubrir direcciones MAC válidas si estuviese el suficiente tiempo escuchando las transmisiones.
- Paso 5, Cambiar el SSID y modificar su intervalo de difusión. Cada casa comercial preconfigura el suyo en sus dispositivos, por ello es muy fácil descubrirlo. Debemos cambiarlo por uno lo suficientemente grande y difícil como para que nadie lo adivine. Así mismo debemos modificar a la baja la frecuencia de *broadcast* del SSID, deteniendo su difusión a ser posible.
- Paso 6, hacer uso de VPNs. Las Redes Privadas Virtuales nos dan un extra de seguridad que nos va a permitir la comunicación entre nuestros dispositivos con una gran seguridad. Si es posible añadir el protocolo IPSec.
- Paso 7, aislar el segmento de red formado por los dispositivos inalámbricos de nuestra red convencional. Es aconsejable montar un cortafuegos que filtre el tráfico entre los dos segmentos de red.

Actualmente el IEEE está trabajando en la definición del estándar 802.11i que permita disponer de sistemas de comunicación entre dispositivos *inalámbiricos* realmente seguros.

Otros conceptos a tener en cuenta son:

PS Mode: Se puede habilitar la función de ahorro de energía (*Power Saving*) para ahorrar batería

en los portátiles cuando no se esté usando la red.

Channel: Cuando un grupo de ordenadores se conectan a través de radio como una red inalámbrica independiente (Ad Hoc), todas las estaciones deben usar el mismo canal de radio. Aunque si te conectas a una red a través de un punto de acceso (modo infraestructura), entonces la tarjeta de red se configura automáticamente para usar el mismo canal que usa el punto de acceso más cercano.

Tx Rate: es la velocidad del enlace. Por defecto se ajusta automáticamente en función de la calidad de la señal, aunque se puede forzar a mano. Es recomendable dejarla automática, ya que forzarla a niveles superiores no significa aumentar la velocidad de la red.

Los cables:

Son un factor crítico a la hora de montar una estación cliente o un nodo. Los cables, TODOS, tienen pérdidas, sólo que unos tienen más que otros. Generalmente se recomienda el uso del cable LMR400 que, aunque existen otras alternativas, sigue siendo el cable ideal para este uso. Del cable depende que la señal llegue correctamente desde la tarjeta a la antena, y viceversa, y es recomendable usar siempre el mínimo cable posible, independientemente de que el cable sea muy bueno. ¿por qué?, evidentemente cuanto menos cable usemos, menores pérdidas de señal habrán.

Voy a poner un ejemplo, para dejarlo algo más claro:

Supongamos que tenemos una tarjeta AVAYA, que tiene una salida de 15dBm, o lo que es lo mismo, 30mW (pulsa aquí para saber más sobre esta equivalencia), y tenemos que poner la antena en la azotea de nuestro edificio. Supongamos que necesitamos usar 25 metros de cable y que tenemos a elegir los siguientes:

Cable	Pérdida (dB/100Mts)
RG-58	81dB
RG-213	41dB
RG-216	136dB
LMR-400	22dB

La elección es clara: el cable LMR400 tiene menos pérdidas de señal, pero... ¿qué quiere decir esto? Supongamos que usamos el cable RG-58 para unir nuestra tarjeta con la antena, a 25 metros de distancia. Si la tarjeta 'emite' a 15 dBm, y este cable tiene 20dB de pérdida, a los 25 metros está claro que la seña simplemente apenas llegará, ya que la pérdida que introducen los mismos conectores harán que esos restantes 5dBm se vean reducidos.

Con el cable LMR-400, las pérdidas para esa distancia serían de 5,5dB, con lo que a nuestra antena llegan 9,5dB de señal, ya bastante poco de por sí. No hablemos ya del RG-216... ;-)

También es verdad que existen cables aún mejores que el LMR400, pero su elevado coste, el coste de los conectores necesarios, su peso, la dificultad de conseguirlos, hacen que se descarte rápidamente. Ya me cuesta bastante conseguir el LMR400, y la verdad, para la inmensa mayoría de las instalaciones es más que suficiente.

Los conectores:

Son otro de los quebraderos de cabeza del personal. Básicamente se van a usar los conectores N para las antenas (salvo marcas raras), tanto en macho como hembra. Son conectores relativamente fáciles de localizar, y de ellos depende la calidad de un buen enlace. Una mala soldadura, un conector de baja calidad, puede introducir una cantidad importante de pérdidas que hagan imposible establecer un enlace. Recuerda que los conectores también tienen pérdidas, no por el conector en sí, sino por el enlace entre el cable y el conector: el estaño, mala sujeción, mala calidad de ambos. etc. No se decirte de cuánto es la pérdida realmente, pero yo siendo pesimista, siempre le pongo 0,5dB de pérdida por conector, aunque en documentos como éste, pone que la pérdida es de 0,25dB por cada conector.

El conector más importante y también, más caro, es el famoso conector MC, de las AVAYA y ORINOCO. Este conector tiene un tamaño realmente ridículo, el diámetro de este conector es de 2 milímetros! y de largo, no llega a 1 centímetro.

1.3.3 Versiones de WI-FI

IEEE 802.11: Especificaciones para 1-2 Mbps en la banda de los 2.4GHz. usando salto de frecuencias (FHSS) o secuencia directa (DSSS).

Wi-Fi (*Wireless Fidelity):* Termino registrado promulgado por la WECA para certificar productos IEEE 802.11b capaces de interoperar con los de otros fabricantes.

IEEE 802.11a

802.11a: Fue la primera aproximación a las redes inalámbricas y llega a alcanzar velocidades de hasta 54 Mbps dentro de los estándares del IEEE y hasta 72 y 108 Mbps con tecnologías de desdoblamiento de la velocidad ofrecidas por diferentes fabricantes, pero que no están (a día de hoy) estandarizadas por el IEEE. Esta variante opera dentro del rango de los 5 Ghz. Inicialmente se soportan hasta 64 usuarios por Punto de Acceso, la velocidad de 802.11a se degrada más rápido a medida que aumenta la distancia.

Sus principales ventajas son su velocidad, la base instalada de dispositivos de este tipo, la gratuidad de la frecuencia que usa y la ausencia de interferencias en la misma. Velocidad máxima: 54 Mbps (disminuye al aumentar la distancia). Alcance: 90 metros.

Sus principales desventajas son su incompatibilidad con los estándares 802.11b y g, la no incorporación a la misma de QoS (posibilidades de aseguro de Calidad de Servicio, lo que en principio impediría ofrecer transmisión de voz y contenidos multimedia *online*), la no disponibilidad de esta frecuencia en Europa dado que esta frecuencia está reservada a la HyperLAN2 (Ver http://www.hiperlan2.com) y la parcial disponibilidad de la misma en Japón.

El hecho de no estar disponible en Europa prácticamente la descarta de nuestras posibilidades de elección para instalaciones en este continente. Usa OFDM.

IEEE 802.11b

Es la segunda aproximación de las redes inalámbricas. Alcanza una velocidad de 11 Mbps estandarizada por el IEEE y una velocidad de 22 Mbps por el desdoblamiento de la velocidad que ofrecen algunos fabricantes pero sin la estandarización (a día de hoy) del IEEE.

Opera dentro de la frecuencia de los 2.4 Ghz. Inicialmente se soportan hasta 32 usuarios por PA. Es la más difundida. Trabaja en la misma banda de frecuencias (2,4 gigahertz) de Bluetooth y dispositivos electrónicos como teléfonos inalámbricos y hornos microondas; eso la hace vulnerable a la interferencia. En el lado positivo está su rápida adopción por parte de una gran comunidad de usuarios debido principalmente a unos muy bajos precios de sus dispositivos, la gratuidad de la banda que usa y su disponibilidad gratuita alrededor de todo el mundo. Está estandarizado por el IEEE. Usa DSSS

Velocidad máxima: 11 megabits por segundo (Mbps). Esta velocidad disminuye a medida que aumenta la distancia. Alcance: 90 metros.

IEEE 802.11g

Velocidad máxima: 54 Mbps (disminuye al aumentar la distancia).

Alcance: 90 metros.

Características: trabaja en la misma banda de frecuencias de la versión original de Wi-Fi, pero ofrece cinco veces más velocidad. Aunque eso la hace más susceptible a la interferencia que la versión ‘a’, tiene la ventaja de que es compatible con los equipos Wi-Fi antiguos. Usa DSSS y OFDM

A modo de resumen:

- IEEE 802.11: Especificaciones para 1-2 Mbps en la banda de los 2.4GHz. usando salto de frecuencias (FHSS) o secuencia directa (DSSS).
- IEEE 802.11b: Extensión de 802.11 para proporcionar 11 Mbps usando DSSS.
- Wi-Fi (Wireless Fidelity): Termino registrado promulgado por la WECA para certificar productos IEEE 802.11b capaces de inter-operar con los de otros fabricantes.
- IEEE 802.11a: Extensión de 802.11 para proporcionar 54 Mbps usando OFDM.
- IEEE 802.11g: Extensión de 802.11 para proporcionar 20-54 Mbps usando DSSS y OFDM. Es compatible hacia atrás con 802.11b. Tiene mayor alcance y menor consumo de potencia que 802.11a.

Información sobre todos los estándares en:

- http://standards.ieee.org/getieee802/portfolio.html

Wlana Wireless LAN Association

- http://www.wlana.org/
- http://www.wi-fi.org/

Mas información en:

- http://www.riskinformatica.com
- http://www.redlibre.net/index.php
- http://www.sincables.net/
- http://www.apdirectory.com/
- http://standards.ieee.org/wireless/

2 Cuestiones

1. Nombra las tres tecnologías de las LAN inalámbricas
2. Clasificación de las redes inalámbricas.
3. Tecnologías usadas en las redes PAN
4. Qué alcance tienen las distintas normas wi-fi?
5. ¿Qué velocidad de transmisión máxima tienen las redes wi-fi?
6. Nombra las dos topologías básicas de las redes wi-fi
7. Haz un esquema de una red wi-fi, indicando los componentes necesarios y sus funciones.