Material desarrollado a partir de los “Proyectos de Innovación e Investigación Educativa de los años 2002 y 2003”.

WIRELESS
Redes Inalámbricas
WIFI
WLAN

Última modificación: 07-01-07

Ignacio Pérez López de Luzuriaga

Índice:

PRÁCTICAS:

ANEXOS:

¿Qué es Wireless?

Las redes inalámbricas, WLAN o Wireless como son más conocidas, son un nuevo tipo de redes surgidas por la necesidad de aumentar la movilidad de los trabajadores de una empresa sin los impedimentos actuales de continuos cambios en el cableado de datos de dicha empresa.

Se terminó el tener que “recablear” una oficina por la llegada de nuevos usuarios, o el tener que “tirar” 30 puntos de red nuevos en una sala porque la semana que viene se va ha realizar una demostración esporádica.

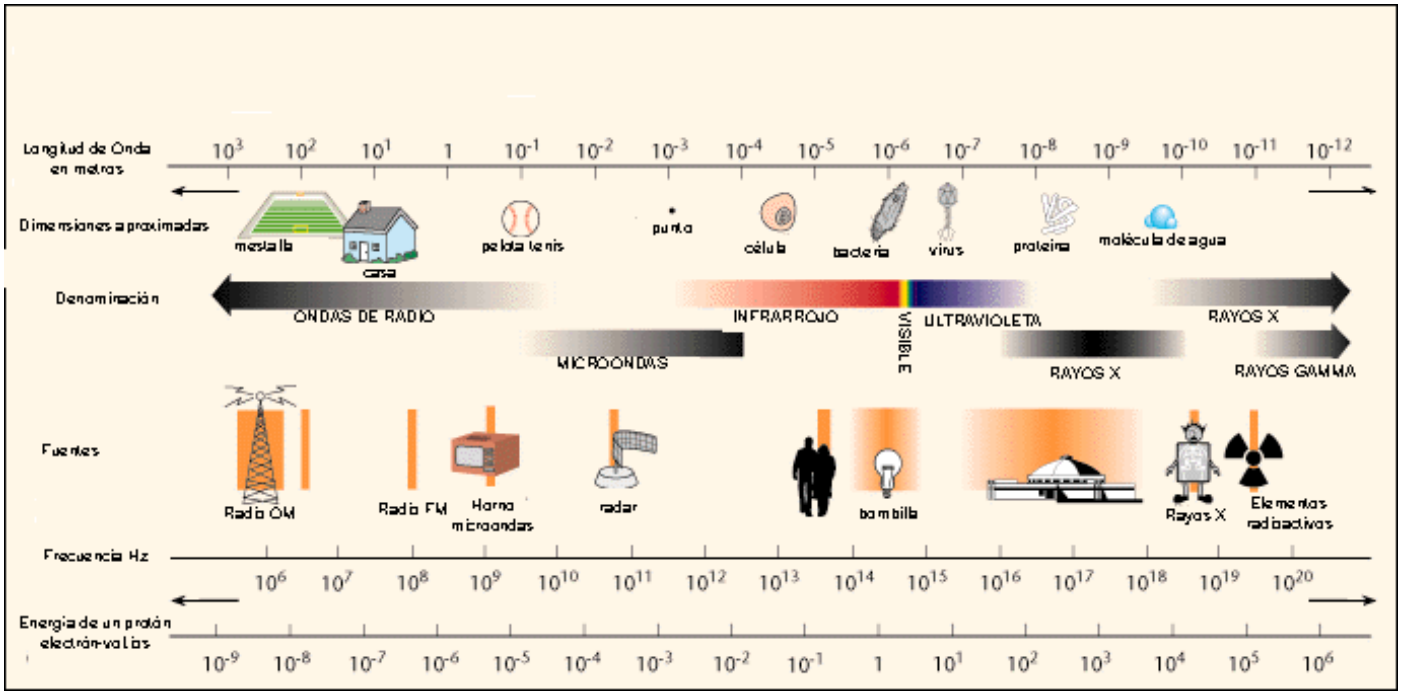
Se evitará el tener que realizar el tendido de cables en paredes de edificios históricos (bibliotecas, edificios gubernamentales, iglesias, etc.

O el tener que cablear un Instituto en el cual se cambia continuamente la ubicación de las aulas de informática por problemas de espacio.

Gracias a esta nueva tecnología, conseguimos que los usuarios sean completamente autónomos y sobre todo móviles, ya que no existen cables que nos obliguen a permanecer conectados físicamente a la red. Utilizamos el aire como medio de transmisión. Todo ello basándonos en el nuevo estándar el **IEEE802.11**.

Utilizamos principalmente el rango de frecuencias de 2,4 GHz:

Representación del espectro radioeléctrico:



Estándar Wireless IEEE802.11

Este estándar desarrollado por el Instituto de Ingeniería Eléctrica y Electrónica IEEE 802.11, describe las normas a seguir por cualquier fabricante de dispositivos Wireless para que puedan ser compatibles entre si.

Los más importantes estándares son:

- **IEEE802.11a:** hasta 54 Mbps (megabits por segundo) de ancho de banda disponible, trabajando en la frecuencia de 5GHz.
- **IEEE802.11b:** hasta 11 Mbps. Este es el más usual y el más utilizado, y sobre el que trabajaremos en nuestras pruebas trabajando en la frecuencia de 2,4GHz.
- **IEEE802.11g:** hasta 54 Mbps, trabajando en la frecuencia de 2,4 GHz como 802.11a.
- **IEEE802.11n:** futuro estándar hasta 600 Mbps, trabajando en las frecuencias de 2,4 GHz y 5 GHZ. Actualmente existen productos "preN", pero se espera la aprobación del estándar a mediados del 2007. Se basa en MIMO (Multiple Input Multiple Output), utilizar varias frecuencias y con varias antenas a la vez para aumentar el alcance y el ancho de banda.

Al ser un estándar mundial, muchos fabricantes de hardware están creando equipos Wireless para poder conectar ordenadores, y van mucho más allá, utilizando Wireless para otras aplicaciones como pueden ser: servidores de impresión o cámaras web. Un mundo lleno de posibilidades.

Estos fabricantes ha formado el Wireless Ethernet Compatibility Alliance (WECA o Wi-Fi Alliance), (WIFI) para identificar los productos Wireless compatibles, lo cual es cierto si cumplen la norma 802.11b.

Se habla de que la importancia de este estándar eclipsará a la tercera generación de telefonía móvil (3G, UMTS) en cuanto a la transferencia de datos y acceso a Internet.

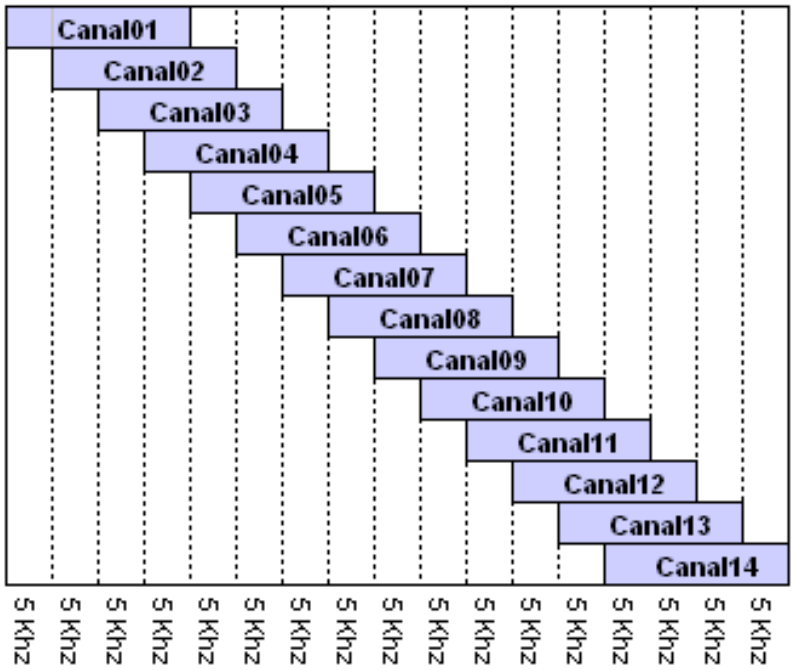
Características IEEE802.11

A mediados de los años 80, el FCC (Federal Communications Comission) asignó las bandas **ISM** (Industrial, Scientific and Medical) 902-928 MHz, 2,4-2,4835 GHz, 5,725-5,85 GHz a las redes inalámbricas.

Las bandas ISM son bandas de frecuencias para uso comercial y sin licencia (son las utilizadas por los teléfonos inalámbricos domésticos DECT, los microondas, o los dispositivos BlueTooth, por ejemplo).

Cada uno de los 14 canales asignados al IEEE 802.11 tiene un ancho de banda de 22 Mhz, y la gama de frecuencias disponible va de los 2.412 GHz hasta los

2.484 GHz. En este espacio es dividido por el IEEE 802.11 en 14 canales, solapándose los canales adyacentes.



Canal	Frecuencia
1	2.412 MHz
2	2.417 MHz
3	2.422 MHz
4	2.427 MHz
5	2.432 MHz
6	2.437 MHz
7	2.442 MHz
8	2.447 MHz
9	2.452 MHz
10	2.457 MHz
11	2.462 MHz
12	2.467 MHz
13	2.472 MHz
14	2.484 MHz

Sobre el cuadro nacional de atribución de frecuencias, tenemos esta tabla publicada en el BOE de marzo del 2002, donde se puede ver como los rangos de frecuencias wireless (a, b o g) se encuentran dentro del rango de “aplicaciones Industriales, Científicas y Médicas – MCI”. Por lo tanto son de libre uso para todos los usuarios.

Notas UN (Utilización Nacional) del Cuadro Nacional de Atribución de Frecuencias (CNAF)
BOE número 70 del Viernes 22 de marzo 2002, página 11812.

UN - 51

Bandas de frecuencias designadas para aplicaciones industriales, científicas, y médicas (ICM).

- 2400 a 2500 MHz (frecuencia central 2450 MHz)
- 5725 a 5875 MHz (frecuencia central 5800 MHz)
- 24,00 a 24,25 GHz (frecuencia central 24,125 GHz)
- 61,00 a 61,50 GHz (frecuencia central 61,250 GHz)

Los servicios de radiocomunicaciones que funcionen en las citadas bandas deberán aceptar la interferencia perjudicial resultante de estas aplicaciones.

Los equipos ICM que funcionen en estas bandas estarán sujetos a las medidas prácticas que adopte la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información si fuera necesario para que las radiaciones fuera de banda de estos equipos sean mínimas, sin perjuicio de lo establecido en el Real Decreto 444/1994 de 11 de marzo sobre requisitos de protección relativos a compatibilidad electromagnética.

La utilización de estas frecuencias para las aplicaciones indicadas se considera uso común.

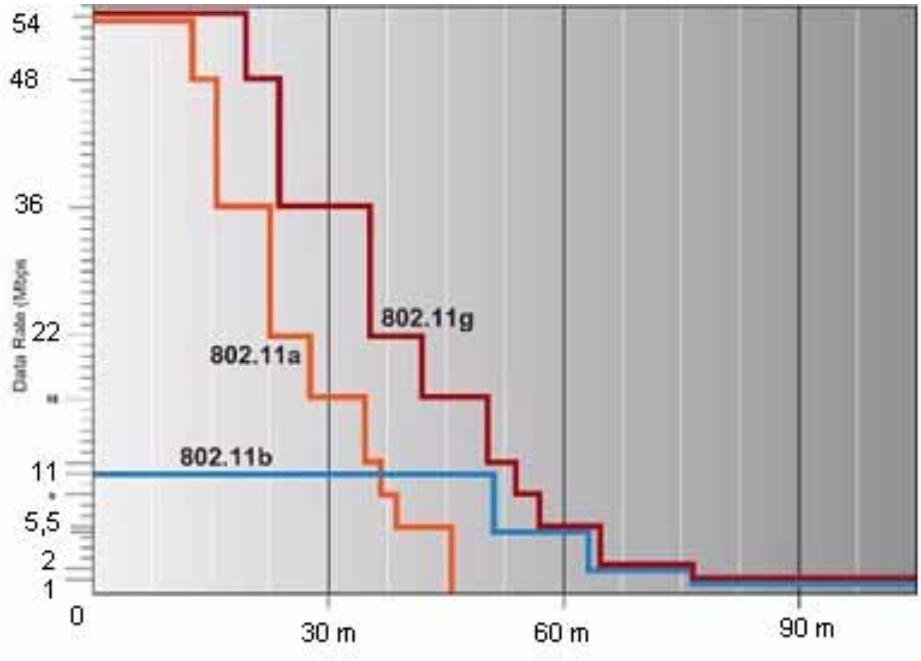
Alcance:

Las distancias tipo para estos dispositivos Wireless 802.11b (a partir de ahora sólo Wireless), son de 100 metros para “espacios cerrados” y hasta 400 metros en “espacios abiertos”.

El alcance depende principalmente de la potencia de emisión de los equipos, dato que nos suele suministrar el fabricante en mWatios o en dB, y de los "objetos a atravesar", no es lo mismo una oficina con paredes de pladur, a un edificio antiguo con paredes gruesas de piedra.

.

Por la legislación española, no podemos emitir con más de 100mW, por eso las antenas "caseras" no están permitidas ya que no están homologadas, pero para pruebas nos sirven perfectamente. En la sección de antenas haremos una pequeña introducción de ellas.



Gráfica con la relación entre la distancia y el ancho de banda disponible en cada caso.

mW y dBm

dBm es la potencia de radio expresada en dB referida a 1mW. En España la potencia máxima permitida de emisión para la banda ISM (2,4GHz) es de **100mW** (20dB). Si bien en julio de 2003 se ha aumentado la potencia para la frecuencia de 5GHz hasta 1W (30dB) debido a la baja penetración de esta frecuencia.

Esta potencia de emisión es el resultado de sumar la potencia de salida de la tarjeta WIFI, con la ganancia de la antena y teniendo en cuenta las perdidas del cable y conectores.

Para convertir mW a dBm, tenemos que multiplicar por 10 el logaritmo de la potencia expresada en mW. Por ejemplo, si la potencia máxima son 100mW:

10 x log 100mW = 20 dBm

La potencia máxima legal de emisión es de 100mW o 20 dBm.

La mayoría de los dispositivos Wireless emiten en un rango de 20 a 50mW:

10 x log 50mW = 17 dBm

Lo que quiere decir que podemos utilizar una antena de hasta 3 dBm máximo para estar dentro de la legalidad.

En el Anexo 1, disponemos de una tabla para la conversión rápida de dB a mW.

Direcciones MAC

Antes de entrar en detalle sobre el material disponible para montar una red WLAN, tenemos que conocer que son las direcciones MAC.

Toda dispositivo que se conecta a una red (Tarjeta Adaptadora de Red), independientemente del medio que utilicemos (cable, aire, medio de la capa 1 – Física – del modelo OSI de 7 capas), dispone de un identificador llamado **dirección MAC**.

Este identificador "trabaja" en la capa 2 – Enlace de Datos – del modelo OSI, y es un identificador exclusivo para cada dispositivo.

Esta MAC está formada por 48 bits de los cuales los 24 primeros identifican al fabricante, y los 24 siguientes son el número de serie/referencia que el fabricante le ha asignado a la NIC.

Por ello se supone que no existen dos NIC con la misma MAC, **o no deben de existir**, aunque en el mercado existen tarjetas de red a las cuales se le pueden cambiar la MAC, esto hay que tenerlo en cuenta para no considerar inexpugnable un filtrado por MAC como medida de seguridad.

La forma de representar la dirección MAC es en hexadecimal: **3A-F5-CD-98-33-B1**

En toda trama de información que circula por una red, independientemente del medio sobre el que se transporte, habrá sido encapsulada en la capa de Enlace con una MAC destino y una MAC origen, lo que permite que esta trama llegue al dispositivo con la MAC destino coincidente.

Si disponemos de un programa que ponga la NIC en modo promiscuo, que acepte todos las tramas de información aunque no sea él la MAC destino, estaremos hablando de un **Sniffer**, un programa para buscar redes, capturar tramas y poderlas estudiar. En nuestro caso, utilizaremos el NetStumbler como herramienta para escanear las redes Wireless.

Dispositivos WLAN

Actualmente se dispone de multitud de dispositivos para conseguir un acceso a una red Wireless, dependiendo del dispositivo desde el que realicemos la conexión. Un equipo conectado a una red se denomina host.

Acceso desde un ordenador portátil o Tablet PC:

Si el portátil o tablet PC no está equipado con procesadores en los que ya está integrado el adaptador wireless, disponemos de ranuras PCMCIA donde conectar las tarjetas del mismo nombre.

Hay PCMCIA con conector para poder añadir una antena exterior de mayor ganancia o sin él (lo más usual).

Acceso desde un ordenador de sobremesa:

En este caso disponemos de varias soluciones dependiendo de nuestras necesidades. Existen **tarjetas PCI** para pinchar en el interior del equipo, las cuales pueden disponer de una pequeña antena exterior.

O bien tarjetas **PCI puente** donde se puede insertar la tarjeta PCMCIA Wireless que se utiliza en los portátiles, de esta manera una misma tarjeta PCMCA puede tener dos usos.

Si no deseamos tener que abrir el ordenador para pinchar la tarjeta, podemos utilizar adaptadores Wireless **USB.** Estos tienen la ventaja de poder mover el adaptador para conseguir una mejor señal, ya que podemos utilizar un cable USB más largo.

La última novedad en cuanto a dispositivos Wireless son los Stick de memoria USB que a su vez son adaptadores Wireless, como el de la figura.

Acceso desde una PDA o un PocketPC:

El acceso Wireless de este tipo de dispositivo depende mucho del fabricante, ya que viene siendo habitual el que este acceso lo incorporen de fábrica. En caso contrario podemos disponer de adaptadores Wireless en formato *CompactFlash (CF)* como la que se muestra o bien *SecureDigital (SD).*

El único inconveniente de este tipo de adaptadores wireless es que por regla general su potencia es menor que el de una PCMCIA de un portátil (por ejemplo), esto

es lógico ya que para poder emitir con mayor potencia debemos consumir mucha más batería del dispositivo. Un bien preciado en este tipo de equipos.

Estos equipos con los adaptadores Wireless correspondientes se conectarán a los "Puntos de Acceso / Access Point" APs. Los APs realizan la función de proporcionar un canal de comunicación válido donde los clientes Wireless pueden establecer una conexión.

Debido a su construcción lo habitual es que los APs dispongan de un conector para la red cableada del edificio, por lo que servirán de interface entre la red inalámbrica y la cableada.

Puntos de Acceso APs:

Existen multitud de fabricantes, y cada uno de ellos proporciona unas características básicas y otras más avanzadas a sus equipos como un valor añadido:

- Firewall integrado.
- Switch 4 puertos incorporado.
- Función de bridge entre edificios.
- Función de repetidor.
- Potencia de emisión variable.
- DHCP, etc.

Para que realicen su función deben utilizar un canal de frecuencia donde trabajarán, configurable por el usuario. De esta manera cualquier dispositivo cliente Wireless detectará que en ese canal existe un AP e intentará conectarse con él siempre que:

- El usuario conozca el Identificador del Canal (**SSID**).
- No sea un canal cifrado.
- No requiera autentificación con login y contraseña.

En resumen, nos podremos conectar con un AP que no tenga ningún tipo de filtrado ni autentificación.

La mayoría de los puntos de acceso del mercado proporcionan un servidor de DHCP para que asigne automáticamente direcciones IPs a los equipos que se conectan, de esta manera el usuario no tiene que conocer los datos técnicos de conexión a la red de la empresa, es algo transparente al usuario. La dirección de la puerta de enlace, y de los DNS también se proporciona para que el host cliente esté completamente configurado y operativo.

Existen otros dispositivos como son los servidores de impresión inalámbricos, o las cámaras inalámbricas, pero solamente son aplicaciones de wireless, no son dispositivos que permitan crear redes WLAN.

Diseño de las redes WLAN, topologías

Las redes inalámbricas pueden construirse sin o con Punto de Acceso (AP), esto es lo que nos determina si es una “Ad-Hoc” o una “Infraestructura”.

Ad-Hoc:

Red *peer to peer*.

Al igual que las redes cableadas ethernet, en las cuales compartimos el medio (cable) y se pueden realizar varias “conversaciones” a la vez entre distintos Host, el medio de las redes WLAN (aire) dispone de un identificador único para cada una de esas “conversaciones” simultaneas que se pueden realizar, es una dirección MAC (48 bits).

En el caso de las redes Ad-Hoc, este número MAC es generado por el adaptador inalámbrico que crea “la conversación”, y es un identificador MAC aleatorio.

Cuando un adaptador wireless es activado, primero pasa a un estado de “escucha”, en el cual, durante unos 6 segundos está buscando por todos los canales alguna “conversación” activa. Si encuentra alguno, le indicará al usuario a cual se quiere conectar.

En el supuesto de que no se pueda conectar a otro Host que ya estuviera activo, pasa a “crear la conversación”, para que otros equipos se puedan conectar a él.

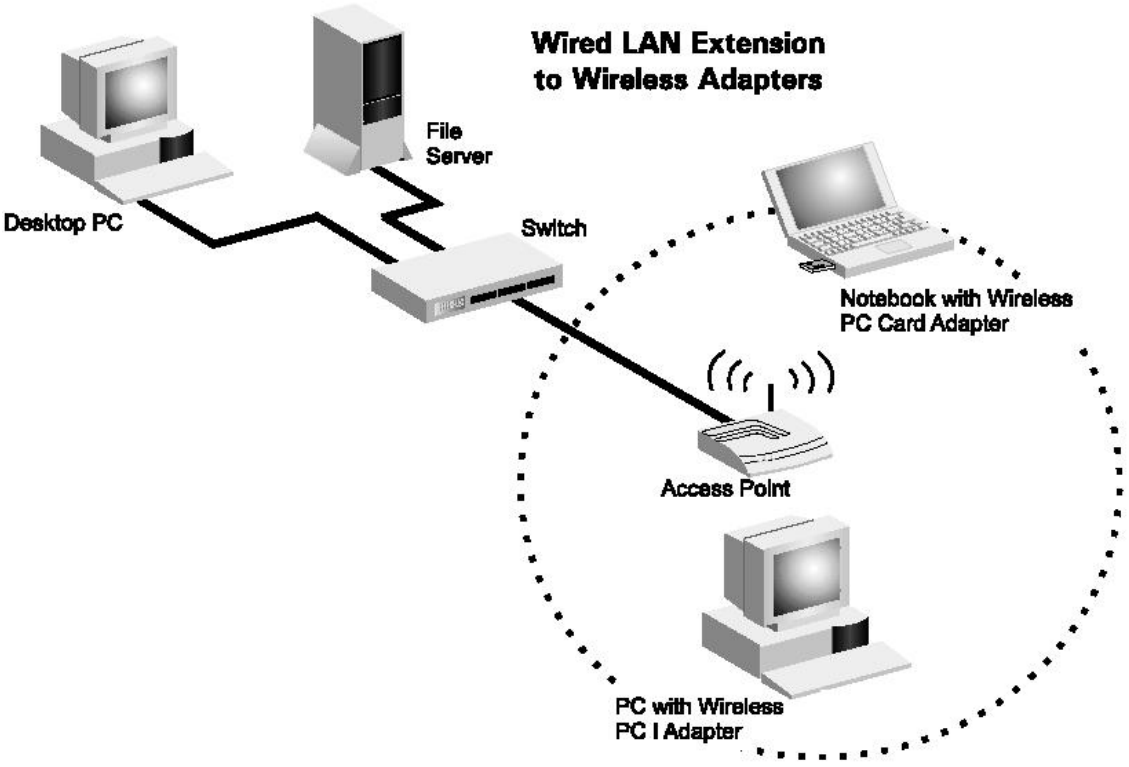
BSSID:

Para una determinada WLAN con topología Adhoc, todos los equipos conectados a ella (Host) deben de ser configurados con el mismo Identificador de Servicio Básico (Basic Service Set, BSSID)

El modo Ad-hoc como máximo puede soportar 256 usuarios, pero es algo inviable ya que sería una red inalámbrica que no funcionará correctamente. Cuando se necesita un número elevado de usuarios debemos de utilizar una topología:

Infraestructura:

Del mismo modo, como en las redes ethernet, en las cuales se dispone de un Hub o concentrador para “unir” todos los Host, ahora disponemos de los Puntos de Acceso (AP), los cuales se encargan de “crear esa conversación” para que se puedan conectar el resto de Host inalámbricos que están dentro de su área de cobertura.



Ahora la MAC que identifica a esta “conversación” es la MAC del AP (MAC real wireless), un dato que puede ser observado con cualquier programa Sniffer Wireless.

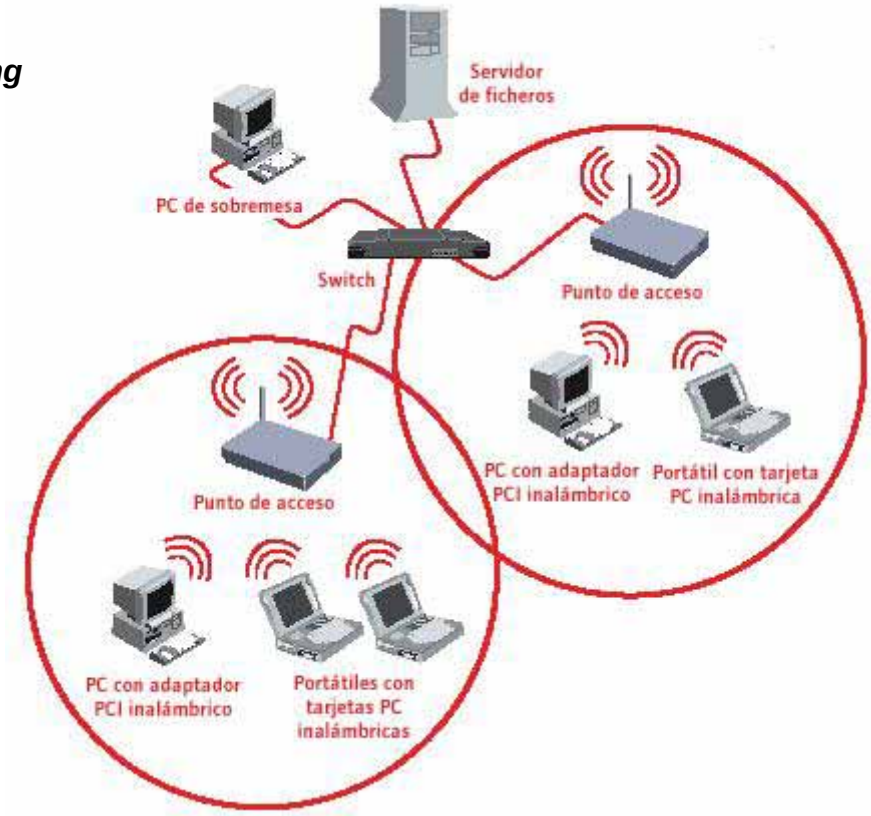
ESSID:

Una configuración en Infraestructura debe configurarse como un Extended Service Set (ESSID). Los usuarios con el mismo ESSID se pueden desplazar libremente entre varios APs mientras el servicio continua (roaming).

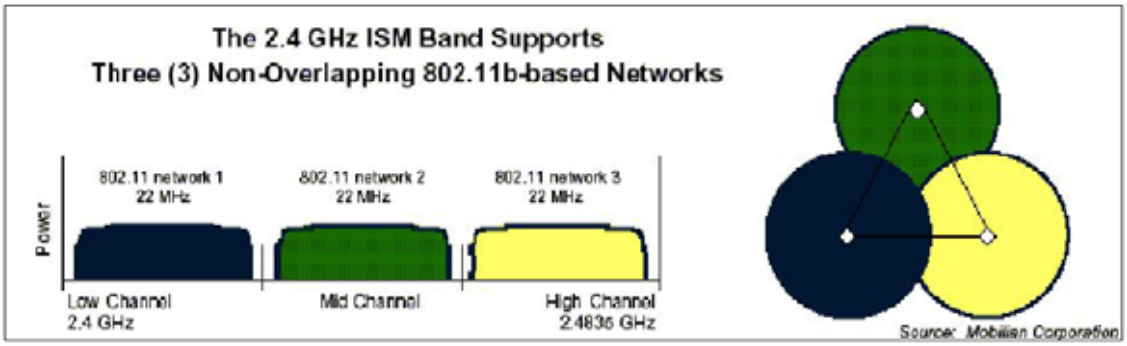
El modo Infraestructura, como máximo puede soportar 2048 usuarios, pero a igual que en el caso Ad-hod es inviable el montar una red con un número tan alto de usuarios sobre el mismo AP. Lo ideal es utilizar celdas de cobertura inalámbricas más pequeñas con más APs, como se hace en la telefonía celular, donde existe el término de “picocélula”, celdas de cobertura telefónica muy pequeñas para poder situar muchas más antenas donde la densidad de usuarios es muy elevada, como por ejemplo en los campos de fútbol.

Dependiendo del tipo de uso del ancho de banda que se necesite, se estudiará el número de AP necesarios para conseguir una total cobertura del edificio, teniendo en cuenta otros factores como la redundancia ante la caída de uno de los APs, para que esa zona este también cubierta por otro próximo. Un tema cada vez más importante en las redes empresariales donde la disponibilidad tiene que ser de 7x24.

Roaming



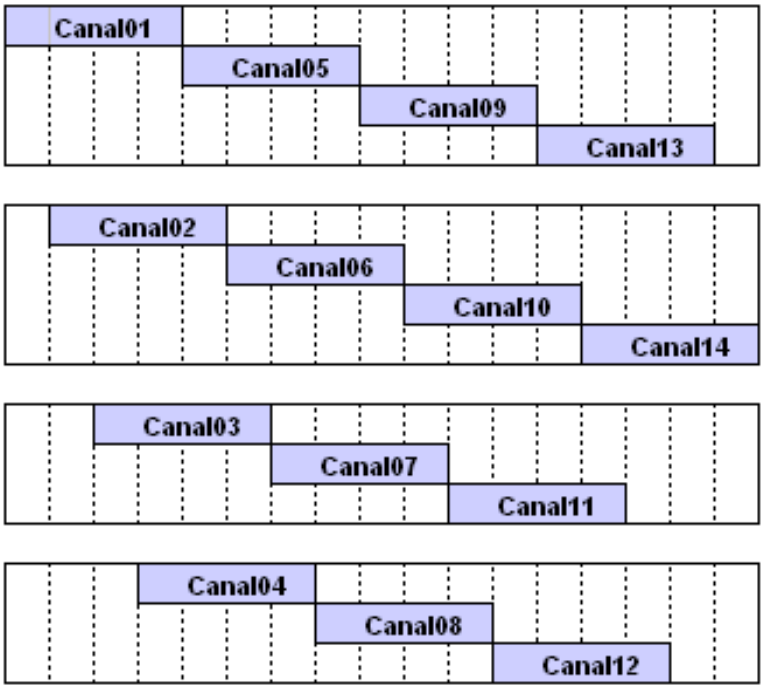
Unas de las utilidades más interesantes de esta tecnología inalámbrica, es la posibilidad de realizar roaming entre los APs de la empresa, con lo que al igual que la tecnología celular, no perdemos cobertura y podemos movernos desde el campo de cobertura de un AP a otro sin problemas, para ello debemos configurar los APs para que trabajen en distintos canales de frecuencia para que no se produzcan problemas de funcionamiento / interferencias en las zonas donde existe cobertura de más de un AP.



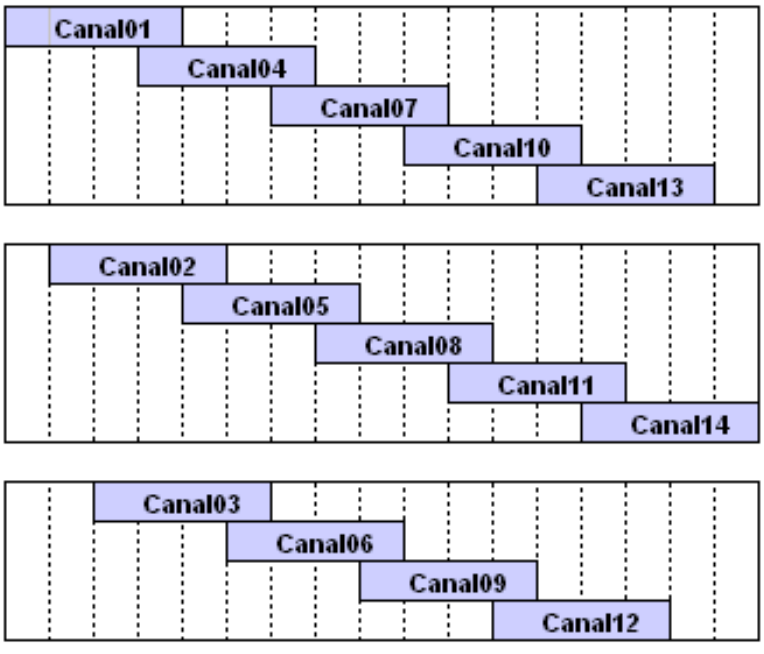
Evitar interferencias entre APs

Como ya comentamos anteriormente, cada uno de los 14 canales asignados al IEEE 802.11 tiene un ancho de banda de 22 Mhz, y la gama de frecuencias disponible va de los 2.412 GHz hasta los 2.484 GHz. En este espacio esta dividido en 14 canales, solapándose los canales adyacentes.

Como resultado solo tenemos las siguientes combinaciones de canales enteros en los que colocar los APs para que no se hagan interferencias de unos a otros :



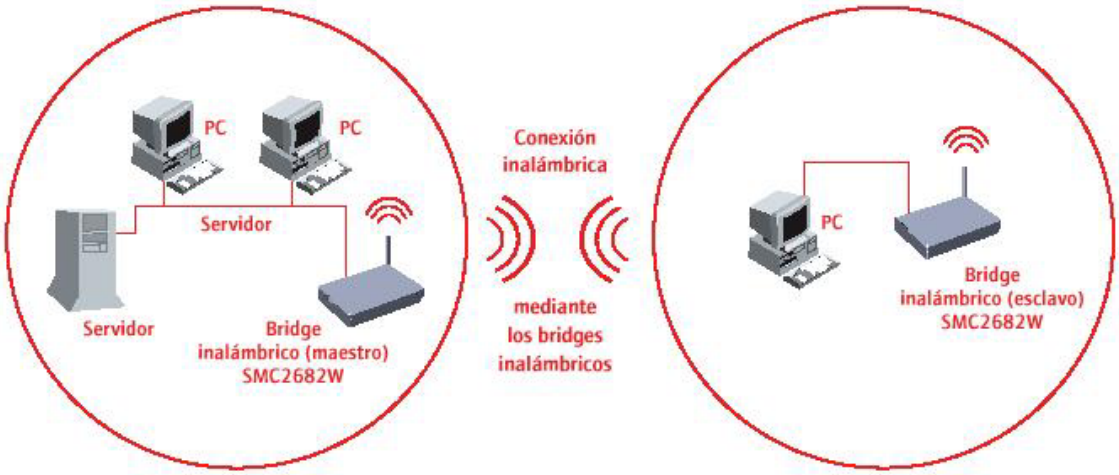
O en caso de que necesitemos más canales utilizar el mínimo solapamiento :



(Más información: dwl900AP_config_Basica.pdf)

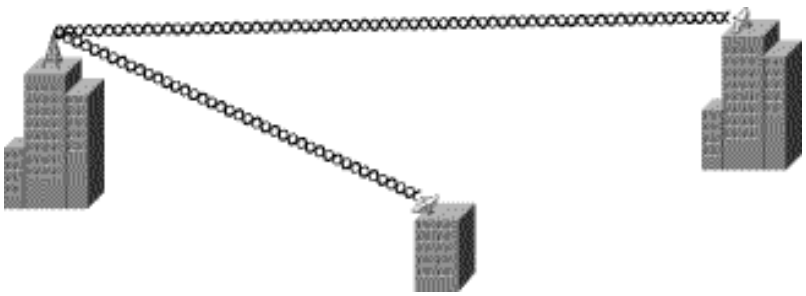
Funcionamiento especial de un AP, Bridge

Un AP puede ser configurado como **puente de dos redes**:



Es el típico ejemplo de la unión de dos redes situadas en dos edificios diferentes.

O bien como **multipuente** *(multibridge)*, unir varias redes a un AP:



Para ello tenemos que indicarle al AP que cambie su modo de trabajo, todo ello desde el programa de configuración del AP, que actualmente tiende a ser desde un navegador. Al configurar el AP que trabaje en modo Bridge, tenemos que indicarle cuál el la MAC del AP contra el que va ha establecer el Bridge. Para ello dispondremos de alguna opción del menú donde "vea" las MACs de los otros APs (normalmente esta opción se denomina "Site Survey", *sondeo del lugar*).

Otro modo de operación es el de **repetidor**, lo que permite extender aun más la WLAN siendo esto completamente transparente para el usuario. El usuario no ve dos APs, sino la MAC y el Canal del AP "original".
Si bien, el ancho de banda en este modo de trabajo se ve reducido a la mitad.

Y uno de los usos más comunes es el utilizar el AP como **cliente wireless**, es decir como si se tratara de un adaptador PCI, PCMCIA o USB, proporcionando acceso a una WLAN. De esta manera podemos situarlo hasta 100 metros de distancia de nuestro PC (por ejemplo en el tejado).

¿22 megas, 108 megas?

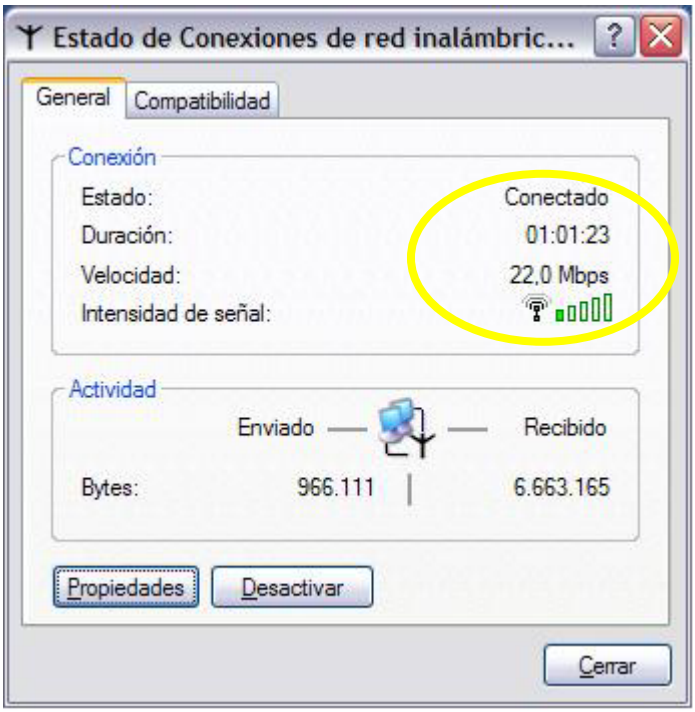
Debido a que el espectro de frecuencias que utilizaremos en wireless (2,4GHz), está muy saturada de otros dispositivos/interferencias, para conseguir una comunicación confiable entre dispositivos WIFI, se han utilizado varias técnicas:

- *Utilización de la secuencia de Backer, por la cuál un bit de información a transmitir se codifica en 11 bits, para que cuando lleguen a destino sea fácilmente reconstruible la información aunque perdamos parte de esos bits por interferencias.*
- *Uso de la técnica de espectro Ensanchado por Salto de Frecuencia (FHSS) para dar servicio a 1 y 2 Mbps.*
- *Uso de la técnica de espectro Ensanchado por Secuencia Directa (DSSS), con las modulaciones DBPSK y DQPSK, para 1 y 2 Mbps. Según 802.11b, modulando con PBCC, conseguiremos los 5,5 y 11 Mbps.*

Todo dispositivo compatible WIFI o IEEE802.11b, podrá conectarse hasta 11 Mbps; pero varios fabricantes, utilizando la misma técnica de modulación PBCC, y codificaciones propietarias, están llegando a los **22 Mbps** (802.11b) y **108 Mbps** (802.11g), no estándar.

Cada fabricante asegura estos nuevos anchos de banda entre sus propios dispositivos, pero no entre dispositivos de otros fabricantes, con los que interactuará a los ancho de banda estándar (11, 54, etc).

(Más info.: D-Link 2003 - Wireless Scenarios.ppt)



Seguridad

La seguridad es uno de los temas más cuestionados en el tema de las redes inalámbricas. Los posibles futuros usuarios es lo que primero se plantean, sobre todo si la aplicación de esa red WLAN va a ser de uso empresarial.

El disponer de una red inalámbrica significa que se deben de tomar LAS MISMAS MEDIDAS que si la red es cableada:

- Autentificar las conexiones con login y password.
- No compartir recursos innecesarios en la red.
- Securizar las partes críticas de la red informática de la empresa.

E independientemente de si se dispone de una WLAN en la empresa o no, actualmente se deben de tomar una serie de medidas de prevención como son:

- Realizar escaneos buscando posibles Puntos de Acceso no autorizados por el personal de informática. Esto empieza a ocurrir en las empresas, donde Departamentos instalan puntos de acceso para poder desplazarse con comodidad dentro de su recinto, pero no están securizados.

Por todo lo anterior, y viendo que existen herramientas tan potentes como es el Netstrumbler, debemos conocer los sistemas de protección más básicos que podemos aplicar a nuestra red inalámbrica.

NETSTUMBLER.COM

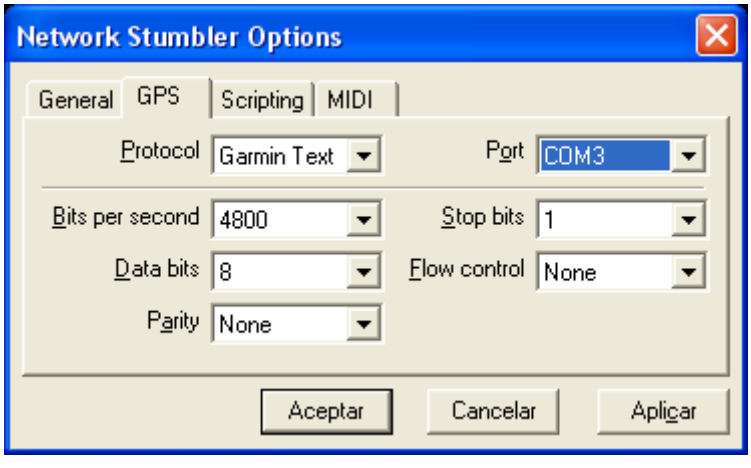
Netstumbler:

Uno de los sniffers más conocidos de la red, principalmente porque funciona bajo Windows y es de muy fácil uso. No es el mejor, pero si el más extendido lo que hace que sea una de las herramientas más comunes de los usuarios inalámbricos. Nosotros la utilizamos para comprobar la cobertura de nuestra red, comprobar las ganancias de las antenas, comprobar cuantos APs están operativos, etc.

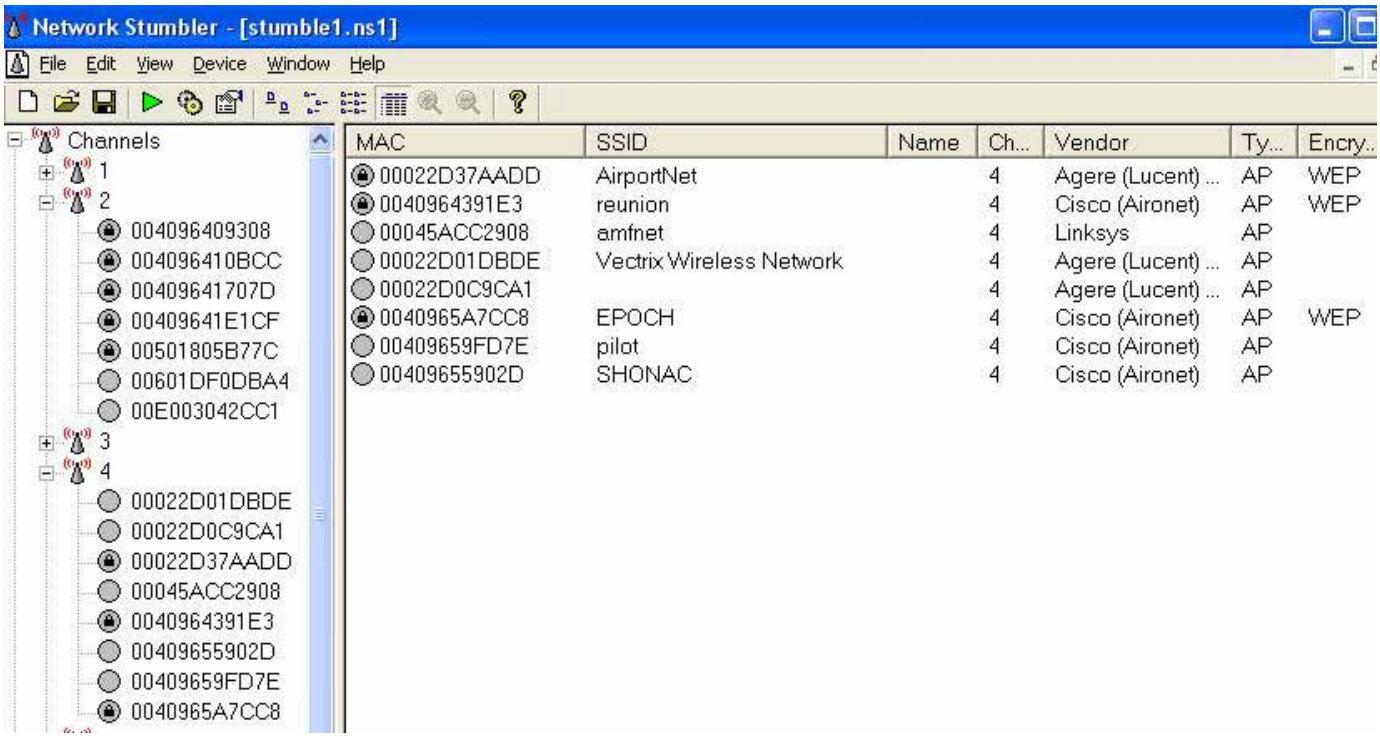
En resumen, es una herramienta que tiene lo que necesita cualquier técnico para obtener información sobre la red a estudio. Pero ahí reside el problema, cualquier usuario puede obtener información sobre la red inalámbrica que hemos instalado, y si es necesario debemos conocer como securizarla.

El desplazarse por la localidad con una antena buscando redes operativas es de lo más usual. En el mercado existen:

- Antenas con soportes de imán para poderlas colocar en el coche, como la de la figura anterior.
- Programas que junto con un GPS te muestran las coordenadas de localización del AP.
- Si ese mismo programa lo soporta, es posible que marque sobre un plano digitalizado la localización exacta de la red escaneada.

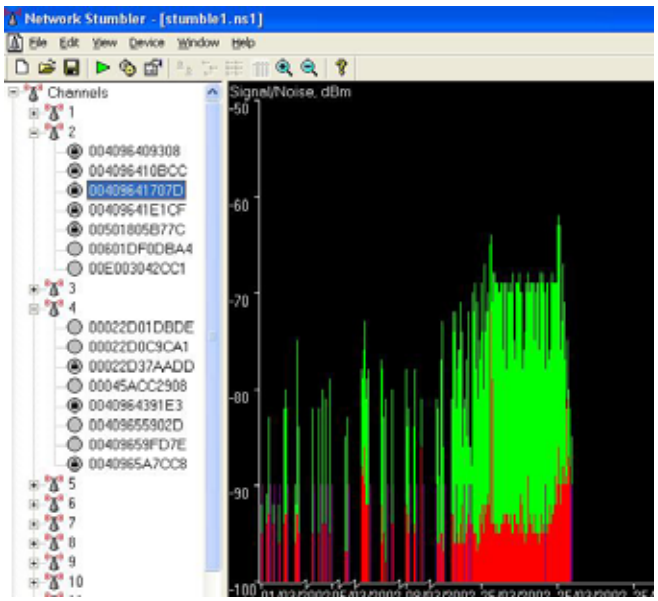


Veamos algunos ejemplos reales de lo que puede encontrarse con el Netstrumbler si se desplaza por una localidad con varias redes WLAN operativas:



Como podemos observar, estamos obteniendo valiosa información de la red de estas empresas:

- MAC de sus APs.
- Canales de emisión por defecto.
- Si el canal está o no encriptado, indicando que la encriptación “es sólo WEP”.
- Y si conectamos un GPS al portátil, nos dará la información exacta de donde nos encontramos para poder situar la “red a estudio” en un mapa.



Y como información gráfica me puede mostrar la potencia de la señal recibida en dB, y los niveles de señal-ruido:

A continuación haremos un repaso por las distintas técnicas de seguridad más conocidas:

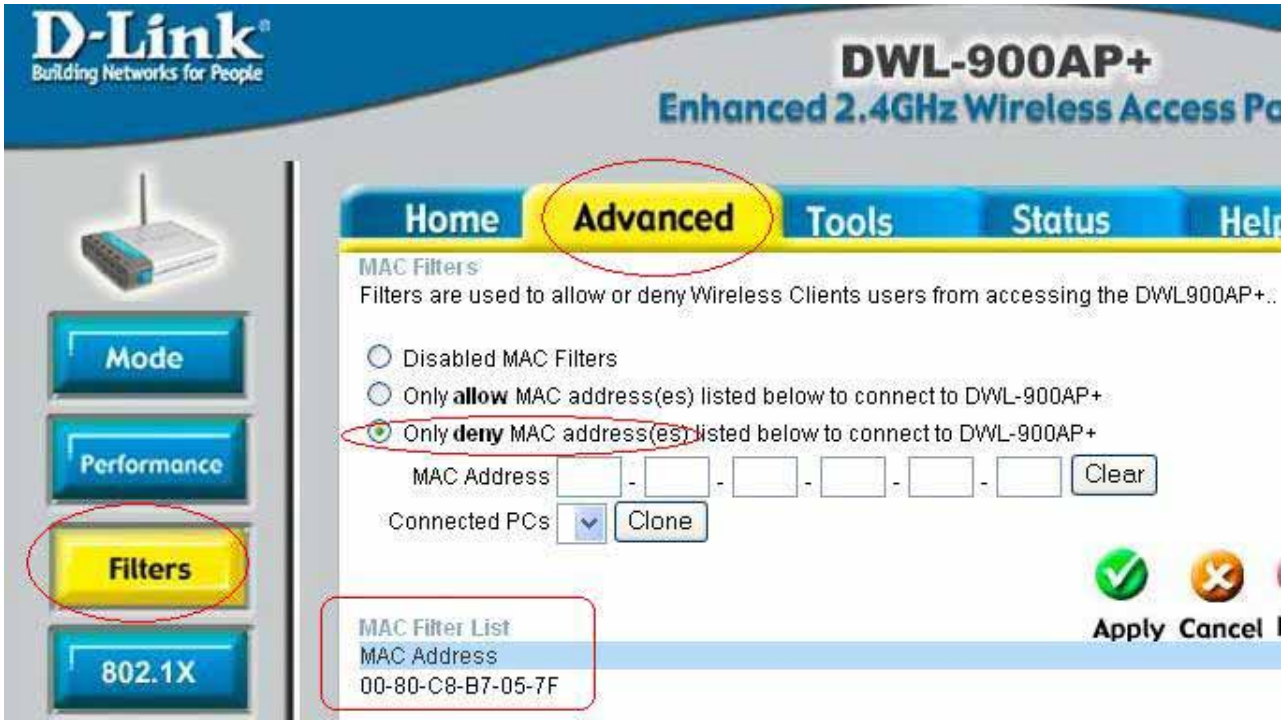
1.- Uso de filtrado por MAC:

Este tipo de seguridad lo proporciona cualquier Punto de Acceso. Es un sistema muy básico pero también efectivo, aunque se puede saltar como luego se muestra.

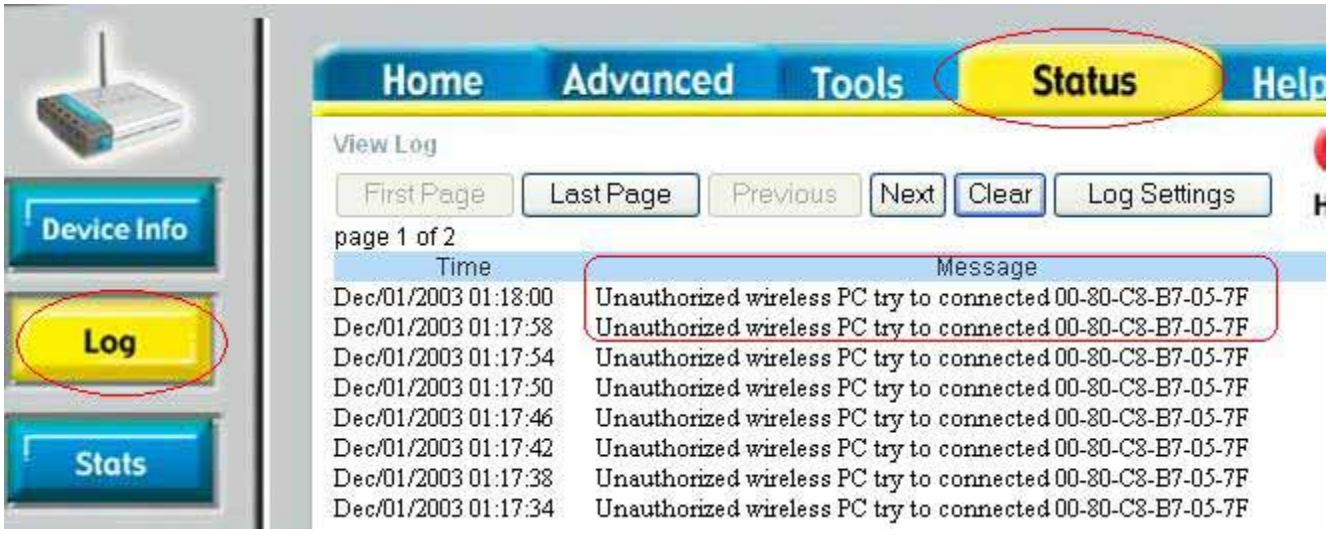
Podemos configurar el AP para que permita o impida el acceso a determinadas MACs, y ya sabemos que “oficialmente” no pueden existir dos tarjetas con la misma MAC.

Vemos un ejemplo, vamos a impedir que el usuario 00-80-C8-B7-05-7F pueda conectarse a una red WLAN.

Para ello configuramos el AP (normalmente mediante un navegador web):



En el momento que el usuario filtrado intenta conectarse, queda reflejado en el LOG para un futuro estudio y el usuario no se puede conectar:

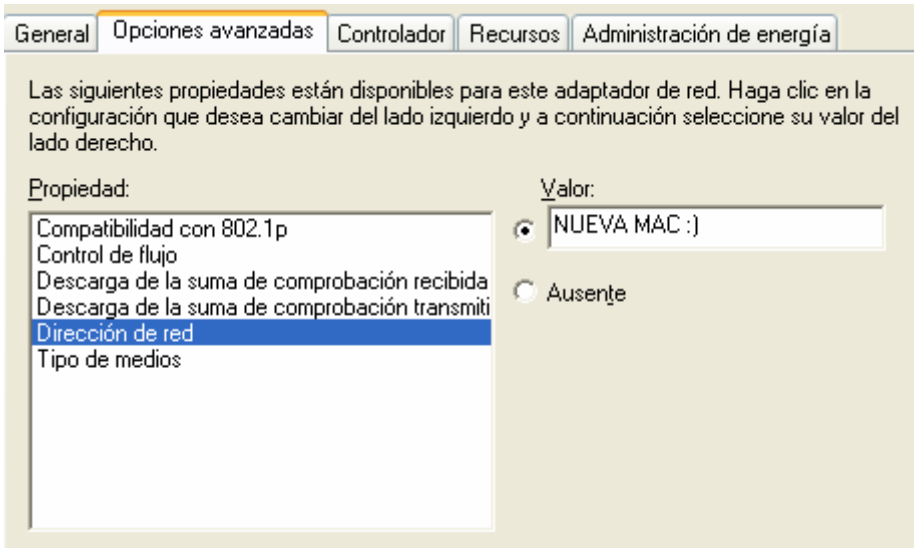


El usuario sigue detectando que hay una o más redes disponibles, pero no puede conectarse, ni conociendo los datos de la red (SSID, IP, puerta de enlace, etc.).

Esta medida de seguridad interesante, pero no efectiva; impedirá el acceso a usuarios poco experimentados, pero si realmente el "estudioso de la red" pretende entrar, no tiene más que modificar la MAC de su adaptador Wireless.

Primero necesitaría el conocer una MAC válida del sistema (que esté autorizada a entrar en ese AP), para ello sólo tiene que estar *esnifeando* (capturando paquetes) la red durante un pequeño tiempo, hasta que decodifique alguna trama en la que se pueda ver la MAC origen. Existen multitud de programas para realizar esta didáctica práctica, incluso para Pocket PC.

Segundo ir a las propiedades avanzadas de la tarjeta y escribir la nueva MAC:



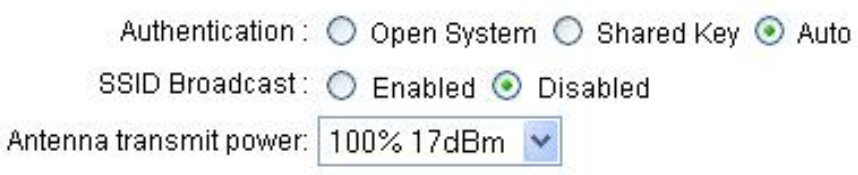
A partir de ahora, y cuando el usuario de la "MAC original" no esté operativo, nosotros podremos suplantarle, ya que somos una MAC válida.

Por lo tanto este sistema de protección es sólo uno más de los que tenemos que tener activos en nuestra red, pero no el único.

2.- Identificador de la red inalámbrica, el SSID:

Definido en el 802.11, el procedimiento SSID (Service Set Identifier) incluye un identificador único en la cabecera de los mensajes que actúa como contraseña cuando un dispositivo quiere conectarse al sistema. Como nuestro sniffer puede capturarlo en alguna trama aunque su publicación esté desactivada, esto incorpora poca seguridad, pero al igual que la anterior es otra a añadir.

Para desactivar la publicación del SSID en el AP, lo tendremos que seleccionar desde la configuración del AP en Broadcast SSID.



3.- Regulación de la potencia a emitir:

Esta facilidad también está incluida en la mayoría de dispositivos Wireless. Como se puede observar en la figura anterior, podemos regular la potencia de nuestro AP para conseguir una cobertura en el interior del edificio, pero nos interesa que esa cobertura no se extienda innecesariamente a zonas donde no debemos tener usuarios.

De esta manera, si alguien quiere snifear nuestra red tendrá que aproximarse demasiado al edificio, y no lo podrá hace desde el parque de enfrente sentado tranquilamente en un banco.

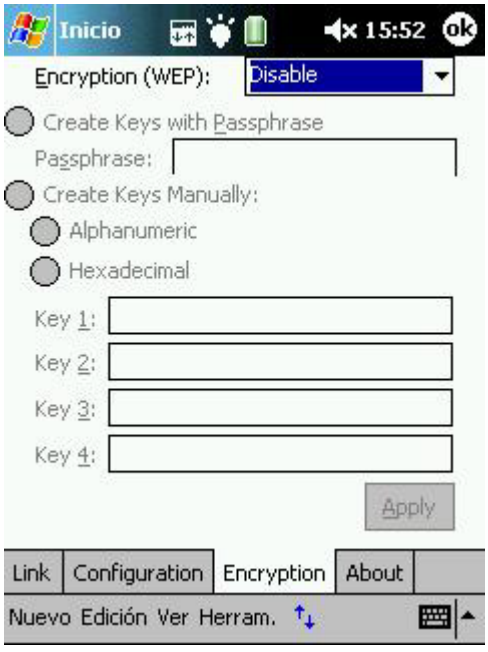
Al igual que las medidas de seguridad anteriores, es una medida que no garantiza nada pero ayuda.

4.- Uso de protocolos de encriptación WEP:

Wired Equivalent Privacy, Privacidad equivalente a redes cableadas. Utiliza un algoritmo de encriptación RC4, y claves de cifrado de 64, 128 y 256 bits; pero en realidad las utiliza de 40, 104 y 152 respectivamente, el resto (overhead), no es información significativa para el cifrado. Nota: el 256 bits no es estándar y no todos los dispositivos lo aceptan.

Todos los sistemas en los que está implementado suelen ser compatibles, pero antes de realizar su implantación es mejor asegurarse.

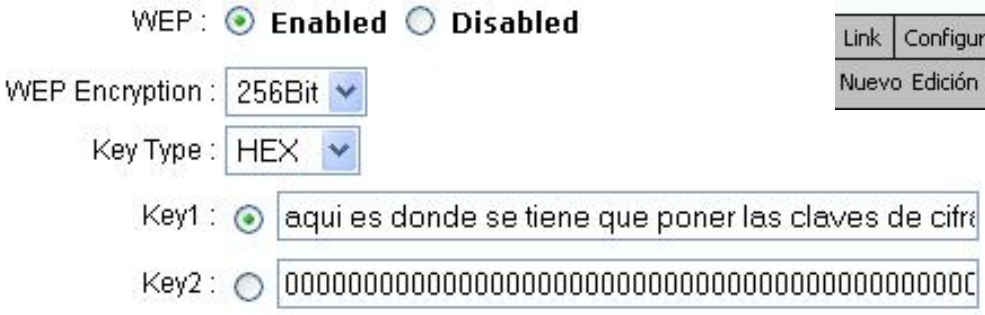
Utiliza una clave de cifrado asignada por el administrador tanto a los PCs como a los puntos de acceso. El cifrado es simétrico con la misma clave tanto para cifrado como para descifrado, por lo que para alcanzar un nivel aceptable de seguridad las claves deben ser cambiadas con relativa frecuencia en todos los dispositivos por el administrador, por ello el WEP tiene los días contados y han surgido otros protocolos de encriptación mucho mejores como el WAP.



Al igual que los anteriores, si un “usuario inquieto” captura la suficiente cantidad de paquetes y tiene las herramientas necesarias (AirSonrt + WEPcrack), puede descifrar las claves introducidas.

El WEP de 64 bits puede ser desencriptado sin problemas, y no todos los dispositivos Wireless soportan encriptaciones mayores.
(Más información: airsnort.ppt)

Pero es otra medida de seguridad que podemos sumar a las anteriores, para ello debemos configurar si queremos cifrado a 64, 128 o 256 y establecer la contraseña correspondiente en ambos:



Para facilitar la tarea de cambiar de clave de cifrado, hay dispositivos que permiten el introducir texto como clave.

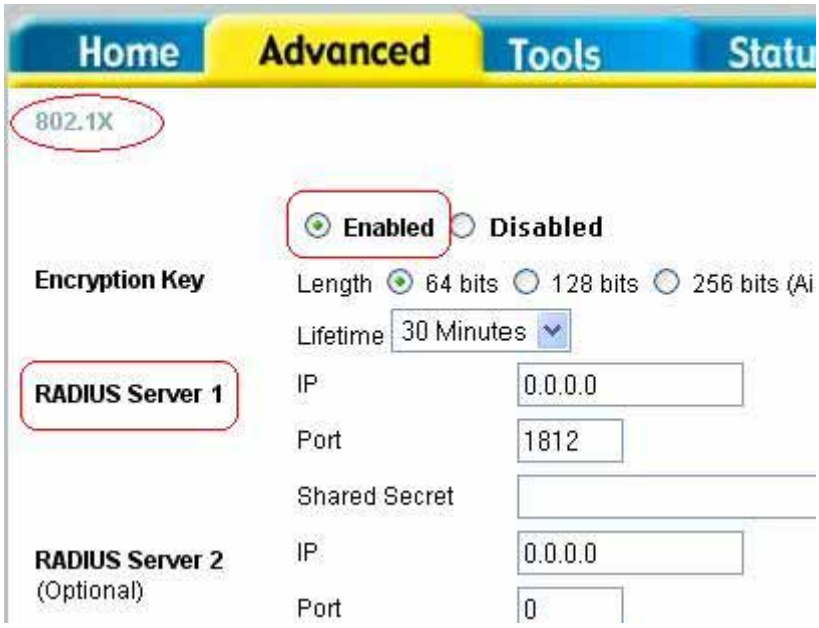
5.- Crear una VPN:

Montar una red privada virtual entre el origen y el destino. Utilizando una VPN se proporciona un túnel seguro independientemente del camino por el que circule la información, incluido Internet. Ya existen APs en el mercado que lo soportan, pero no es lo normal, sólo los de la gama medio-alta.

(Más información: VPNs.doc)

6.- Utilizar el estándar 802.1x:

Nuevo estándar con el que permitimos autenticar al usuario entrante a nuestra WLAN. El autenticador no tiene por que ser una máquina inteligente, por lo que pequeños APs podrán utilizar este estándar 802.1x. Es el conocido “Portal Cautivo”, como el NoCat en Linux o los RADIUS y los TACACS+LDAP.



7.- Utilizar el nuevo WPA (Wi-Fi Protected Access):

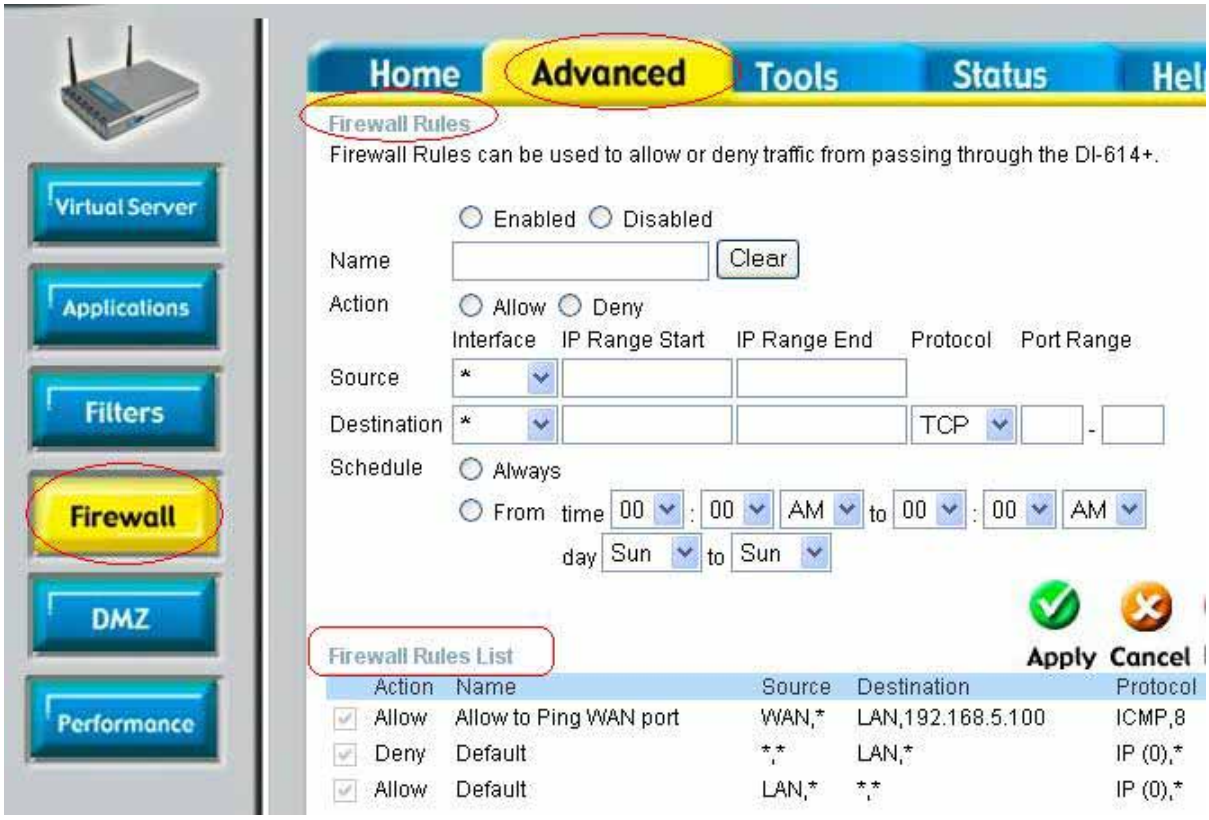
Mucho más fiable que el WEP siempre que no se utilicen claves inferiores a 20 caracteres los cuales estén contenidas en un diccionario, ya que es susceptible de este tipo de ataques. Este problema puntual no es, una indicación de la debilidad de WPA. Únicamente es un recordatorio de la necesidad de utilizar claves convenientemente largas y que incluyan caracteres especiales.

En la nueva protección WPA la cadena ASCII que se introduce sirve de semilla para una clave en constante rotación, de forma que cada paquete de información lleva una clave completamente diferente a los anteriores.

La autenticación se basa en el estándar 802.1x que define un protocolo de autenticación por puerto, considerando cada frecuencia de radio como un puerto en el caso de las WLAN.
(Más información: wpa+eap-tls+freeradius-jornadas-telematicas-2005.pdf)

8.- Funciones de Firewall:

Si el AP dispone de ellas activarlas, para cerrar determinados puertos que impidan posibles ataques a nuestra WLAN, si no dispone de un firewall integrado, montar uno.



E incluso, si el equipo lo soporta, puede disponer de facilidades para crear una zona DMZ (desmiritalizada) donde colocaríamos los equipos que deben de servir en la WLAN:

Como resumen, la mejor solución es utilizar varios de los anteriores para poner más trabas a los usuarios que no tienen autorización, si bien, el impedir el acceso por completo es difícil.

Antenas

Las antenas son dispositivos utilizados para recoger o radiar ondas electromagnéticas. Aumentan la zona de influencia/cobertura de nuestras tarjetas inalámbricas de manera que en lugar de dar cobertura a unos pocos metros, podemos alcanzar cientos de metros sin problemas.

Se han realizado pruebas de campo y se han establecido comunicación entre dispositivos wireless a más de 75 Km. (con antenas parabólicas utilizando una antena Biquad como LNB).

Sobre la polémica de si las antenas son perjudiciales para la salud, únicamente hay que tener en cuenta que los teléfonos móviles usuales emiten con 500mW de potencia, y normalmente no nos ponemos una antena wireless de 100mW junto a la cabeza ni en el bolsillo de la camisa o pantalón.

Si bien la polémica está servida, cumpliendo la ley de potencia máxima de emisión de 100mW (o 1000mW para 802.11a), estamos legalmente seguros de la salubridad de la instalación.

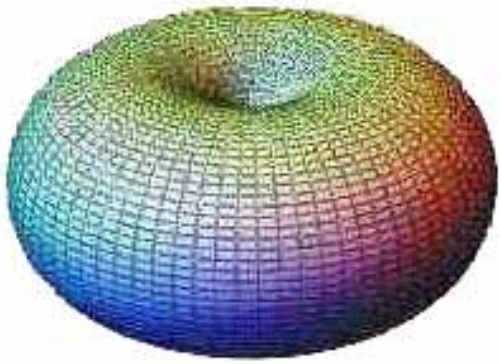
Las antenas “caseras” son útiles para realizar pruebas, pero no pueden ser las antenas permanentes de una instalación al no estar homologadas.

Tenemos que aclarar que una antena nunca funciona como amplificador. Nunca emitiremos mas potencia que la que le entreguemos a la antena. Lo que si existen son antenas que concentren parte de esa potencia en una dirección determinada pudiendo alcanzar una mayor distancia.

Tipos de antena

Básicamente disponemos de dos tipos:

- **Omnidireccionales:** las cuales dan cobertura con un diagrama de radiación teórico de una esfera, aunque en la práctica es un diagrama de radiación circular (360º), ya que una antena no puede emitir en su vertical.



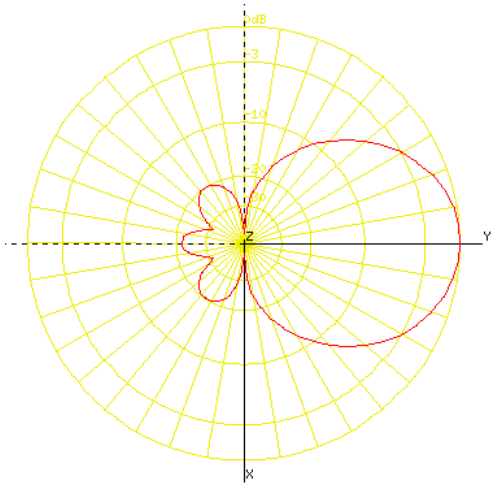
Se supone que dan servicio por igual independientemente de su colocación, pero debido a que las frecuencias en las que estamos trabajando son próximas a microondas, los diagramas no son circulares, son óvalos.

- **Direccionales:** son directivas y solo emiten/reciben con un ancho de haz

definido por la construcción de la antena.

Diagrama de radiación de una antena unidireccional – sectorial.

En estos diagramas se pueden apreciar los lóbulos de radiación (lobes).



f = 2457 MHz maxgain = 14.48 dBi vgain = -8.74 dBi

La ganancia de una antena viene dada en decibelios isotrópicos (dBi). Es la ganancia de energía en comparación con una antena isotrópica ideal la cual irradia en todas direcciones con la misma potencia.

Algunas antenas dan su ganancia expresada en dBd, que es la ganancia comparada con una antena dipolo. En este caso hay que sumar 2,14 para obtener la ganancia correspondiente en dBi.

Una antena tiene más ganancia contra más directiva es, ya que concentra toda la potencia en una dirección.

La energía irradiada por la antena EIRP se expresa en dBm, y se obtiene:

EIRP (dBm) = Energía del transmisor (dBm) – pérdidas del cable (dB) + ganancia de la antena (dBi)

Effective Isotropic Radiated Power (EIRP)

La ganancia de la antena es la misma para la transmisión que para la recepción.

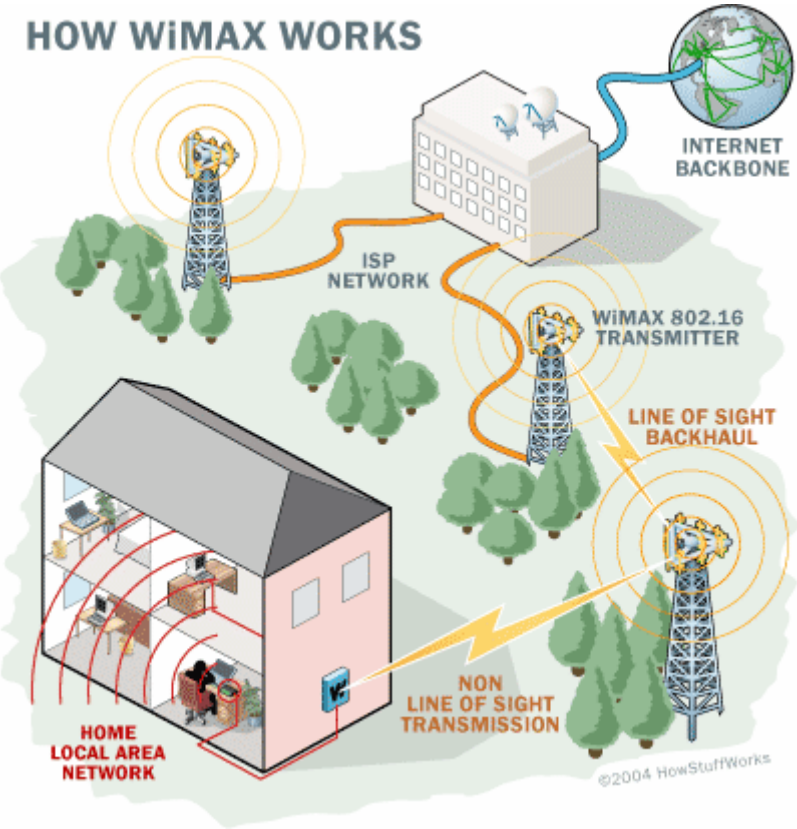
(Más información: Wireless LAN Technical Training - Basic Antenna Theory.ppt)

WiMax, más allá de WiFi

Resumen:

WiMax (Worldwide Interoperability for Microwave Access) es el nombre con el que se conoce la norma 802.16a, un estándar inalámbrico aprobado en el **WiMax Forum,** que ofrece un mayor ancho de banda y alcance que la familia de estándares WiFi, compuesta por el 802.11a, 802.11b y 802.11g.

Como decimos, la diferencia entre estas dos tecnologías inalámbricas son su alcance y ancho de banda. Mientras que WiFi está pensado para oficinas o dar cobertura a zonas relativamente pequeñas, WiMax ofrece tasas de transferencia de 70Mbps a distancias de hasta 50 kilómetros de una estación base. Por comparación, la tasa de transferencia de WiFi es de 11mbps y la distancia de hasta 350 metros en zonas abiertas.

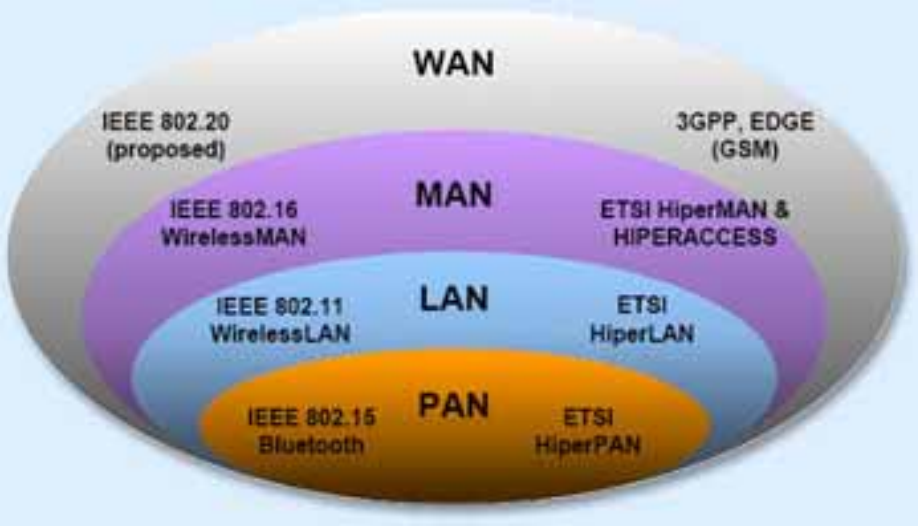


Los **backhaul** (red de retorno) conectan redes de datos, redes de telefonía celular y constituyen una estructura fundamental de las redes de comunicación. Usado para interconectar redes entre sí utilizando diferentes tipos de tecnologías alámbricas o inalámbricas.

Un ejemplo de backhaul lo tenemos en los saltos de microondas que se utilizan para conectar las estaciones bases celulares con el nodo principal de esta red.

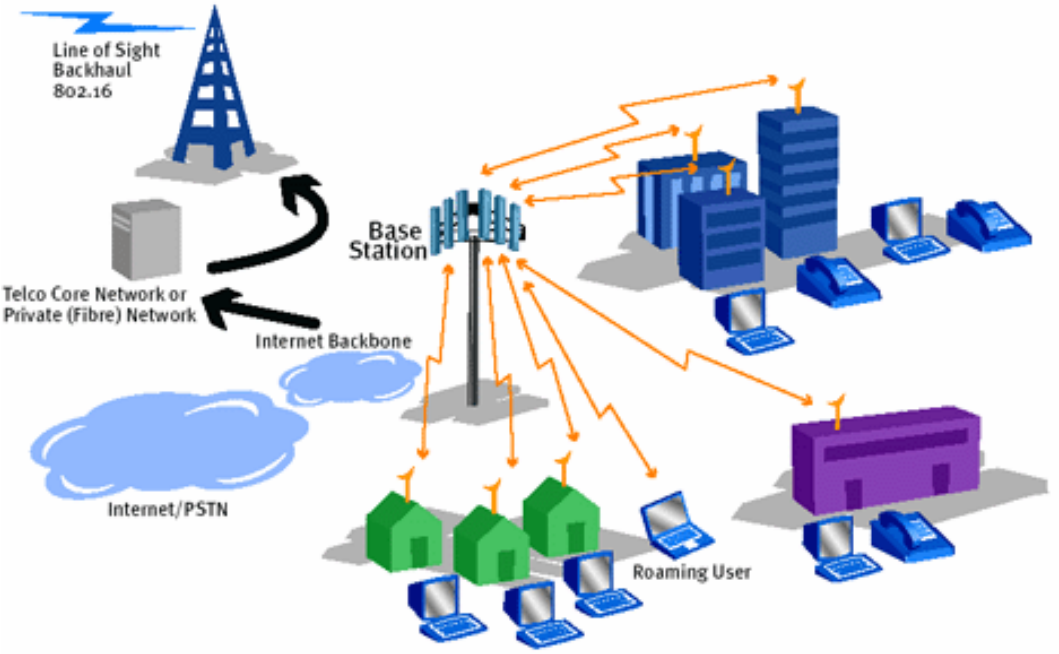
Más información:

WiMAX (del inglés ***W**orldwide **I**nteroperability for **M**icrowave **A**ccess*, Interoperabilidad Mundial para Acceso por Microondas) es un estándar de transmisión inalámbrica de datos (**802.16e**) diseñado para ser utilizado en el área metropolitana o MAN proporcionando accesos concurrentes en áreas de hasta 50 kilómetros de radio y a velocidades de hasta 70 Mbps, utilizando tecnología portátil LMDS.



Integra la familia de estándares IEEE 802.16 y el estándar HyperMAN del organismo de estandarización europeo ETSI. El estándar inicial 802.16 se encontraba en la banda de frecuencias de 10-66 GHz y requería torres LOS (antenas con visión directa entre ellas). La nueva versión 802.16a, ratificada en marzo de 2003, utiliza una banda del espectro más estrecha y baja, de 2-11 GHz, facilitando su regulación. Además, como ventaja añadida, no requiere de torres LOS sino únicamente del despliegue de estaciones base (BS) formadas por antenas emisoras/receptoras con capacidad de dar servicio a unas 200 estaciones suscriptoras (SS) que pueden dar cobertura y servicio a edificios completos. Su instalación es muy sencilla y rápida (culminando el proceso en dos horas) y su precio competitivo en comparación con otras tecnologías de acceso inalámbrico como Wi-Fi: entre 5.000 euros y 25.000 euros.

Esta tecnología de acceso transforma las señales de voz y datos en ondas de radio dentro de la citada banda de frecuencias. Está basada en OFDM, y con 256 subportadoras puede cubrir un área de 48 kilómetros permitiendo la conexión sin línea vista, es decir, con obstáculos interpuestos, con capacidad para transmitir datos a una tasa de hasta 75 Mbps con una eficiencia espectral de 5.0 bps/Hz y dará soporte para miles de usuarios con una escalabilidad de canales de 1,5 MHz a 20 MHz. Este estándar soporta niveles de servicio (SLAs) y calidad de servicio (QoS).



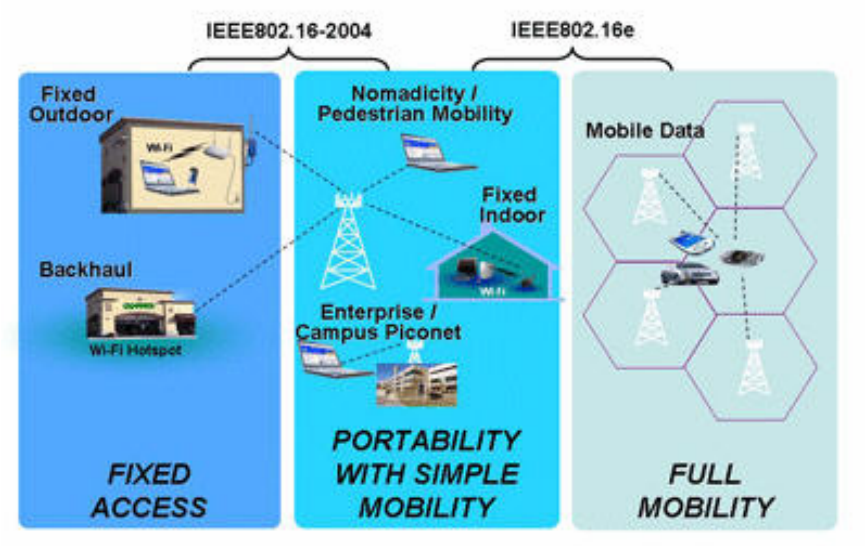
WiMAX se sitúa en un rango intermedio de cobertura entre las demás tecnologías de acceso de corto alcance y ofrece velocidades de banda ancha para un área metropolitana.

Iberbanda

Equipos receptores de cliente

Anchura de haz-elevación y azimuth: 18 grados.
Ganancia: 17,5 dBi.
Tamaño (altura, anchura, profundidad): 260x260x60mm.
Peso: 3 Kg.
Mástil: En caso de no poder reutilizar mástiles existentes, se instala un mástil de 6cm . de diámetro y altura máxima de 2m.
Cableado: Un solo cable coaxial idéntico al utilizado en las instalaciones de antena de televisión con sección de 11mm.

El pasado 7 de diciembre de 2005, el IEEE aprobó el estándar del **WiMAX MÓVIL**, el 802.16e, que permite utilizar este sistema de comunicaciones inalámbricas con terminales en movimiento. Muchos fabricantes de hardware y operadores estaban esperando a esta decisión para empezar a desplegar redes de wimax. Ahora ya pueden hacerlo.



Lo que ocurría en la práctica es que pocos se atrevían a invertir en wimax bajo el único estándar aprobado hasta ahora, el 802.16d, que sólo sirve para aquellos terminales que están en un punto fijo. Ahora ya saben qué especificaciones técnicas debe tener el hardware del wimax móvil, que es mucho más jugoso económicamente, con lo que es posible diseñar infraestructuras mixtas fijo-móvil.

PRÁCTICAS:

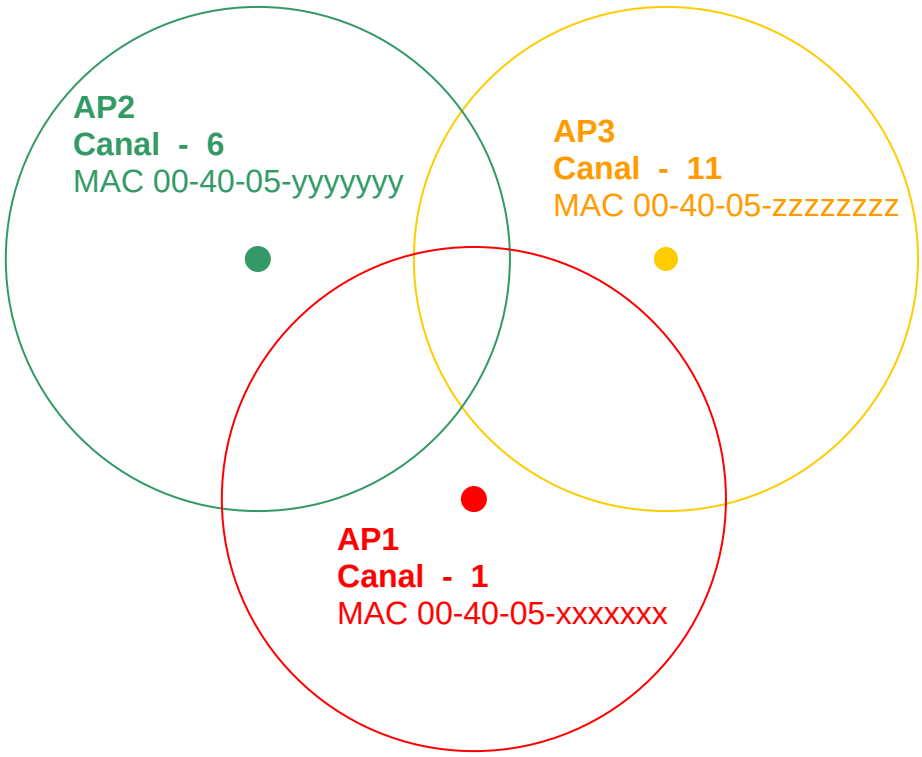
Primera práctica: cobertura de un AP.

Segunda Práctica: redes Ad-Hoc (Sin AP, Peer to Peer).

Tercera Práctica: redes Infraestructura (Con AP).

Cuarta Práctica: roaming entre APs.

Realizamos el siguiente montaje con tres APs dentro de la misma aula:



ANEXO 1: Tabla de conversión rápida de dB a mW.

dBm	mw
0dBm	1mW
1dBm	1.25mW
2dBm	1.56mW
3dBm	2mW
4dBm	2.5mW
5dBm	3.12mW
6dBm	4mW
7dBm	5mW
8dBm	6.25mW
9dBm	8mW
10dBm	10mW
11dBm	12.5mW
12dBm	16mW
13dBm	20mW
14dBm	25mW
15dBm	32mW

dBm	mw
16dBm	40mW
17dBm	50mW
18dBm	64mW
19dBm	80mW
20dBm	100mW
21dBm	128mW
22dBm	160mW
23dBm	200mW
24dBm	256mW
25dBm	320mW
26dBm	400mW
27dBm	512mW
28dBm	640mW
29dBm	800mW
30dBm	1000mW

ANEXO 2: Fabricación de antenas

Las antenas se pueden fabricar con bastante facilidad, como es el típico ejemplo de las antenas hechas con botes de una conocida marca de patatas fritas.

Pero son antenas que no están homologadas, no conocemos su diagrama de radiación ni la potencia con que se emite. Muy interesantes para hacer pruebas, pero no se pueden utilizar para dar servicio continuo.

Cables y conectores:

Existen en el mercado un gran número de conectores distintos para wireless:
SMA, tipo N, C, MCX, etc. Y luego tener en cuenta si son male, female, reverse, ... nosotros utilizaremos los N por ser unos conectores estándar de fácil adquisición y los SMA porque por su pequeño tamaño son muy manejables con cables coaxiales finos.

Los cables que unen los APs con la antena deben de ser de baja pérdida para evitar una pérdida excesiva de señal. Estos suelen ser gruesos, llamados de media pulgada.

Los cables que unen los APs (o las tarjetas wireless) con el cable de baja pérdida de 50 ohmios que llega hasta la antena se denomina “Pig Tail” (siempre se venden enrollados), y no suelen exceder de medio metro. Este cable nos sirve para poder conectar nuestro dispositivo Wireless (PCMCIA, AP, USB con la antena).

Tabla de atenuación de cable coaxial para varias frecuencias en dB/ 100 m:

Tipo de Cable	144 MHz	220 MHz	450 MHz	915 MHz	1.2 GHz	2.4 GHz	5.8 GHz
RG-58	20.3	24.3	34.8	54.1	69.2	105.6	169.2
RG-8X	15.4	19.7	28.2	42.0	52.8	75.8	134.2
LMR-240	9.8	12.1	17.4	24.9	30.2	42.3	66.9
RG-213/214	9.2	11.5	17.1	26.2	33.1	49.9	93.8
9913	5.2	6.2	9.2	13.8	17.1	25.3	45.3
LMR-400	4.9	5.9	8.9	12.8	15.7	22.3	35.4
CNT-400 (C2FP)	5.0	6.0	8.8	12.7	16.2	22	40.2
3/8" LDF	4.3	5.2	7.5	11.2	13.8	19.4	26.6
LMR-600	3.1	3.9	5.6	8.2	10.2	14.4	23.9
1/2" LDF	2.8	3.6	4.9	7.2	8.9	12.8	21.6
7/8" LDF	1.5	2.1	2.7	3.9	4.9	7.5	12.5
1 1/4" LDF	1.1	1.4	2.0	3.0	3.6	5.6	9.2
1 5/8" LDF	0.92	1.1	1.7	2.5	3.1	4.6	8.2

Nosotros utilizaremos para los pig tail el RG58 y el RG213 (un poco más grueso este último que el primero).

El cable que utilizamos para unir el AP central con nuestra antena exterior del tejado del edificio del Cossío es un LMR-400, con una pérdida de 0,22dB por metro.

Existe una página muy interesante en la que podemos realizar todos los cálculos necesarios para las antenas: http://www.swisswireless.org/wlan_calc_en.html,

Teoría básica de antenas:

Partimos de que **Lambda** es la longitud de onda y viene definida por:

Lambda = velocidad de la luz / frecuencia

La frecuencia media en 802.11b es:

F= (2.484.000.000 + 2.412.000.000) / 2 = 2.448.000.000 Hz

Por lo que :

Lambda = 300.000.000 / 2.448.000.000 = 0,12254 m = **122,84 mm**

Lambda /2 = 61,42 mm

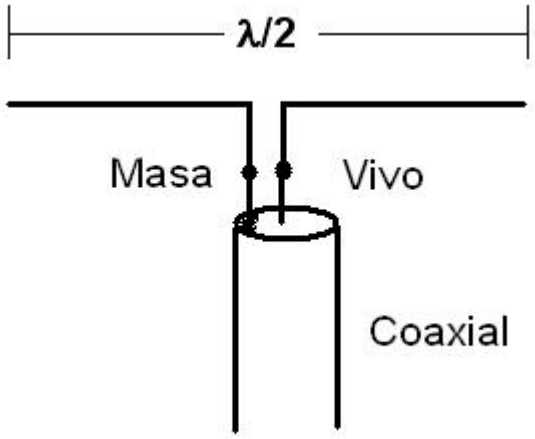
Lambda /4 = 30,71 mm

Lambda /8n = 15,35 mm

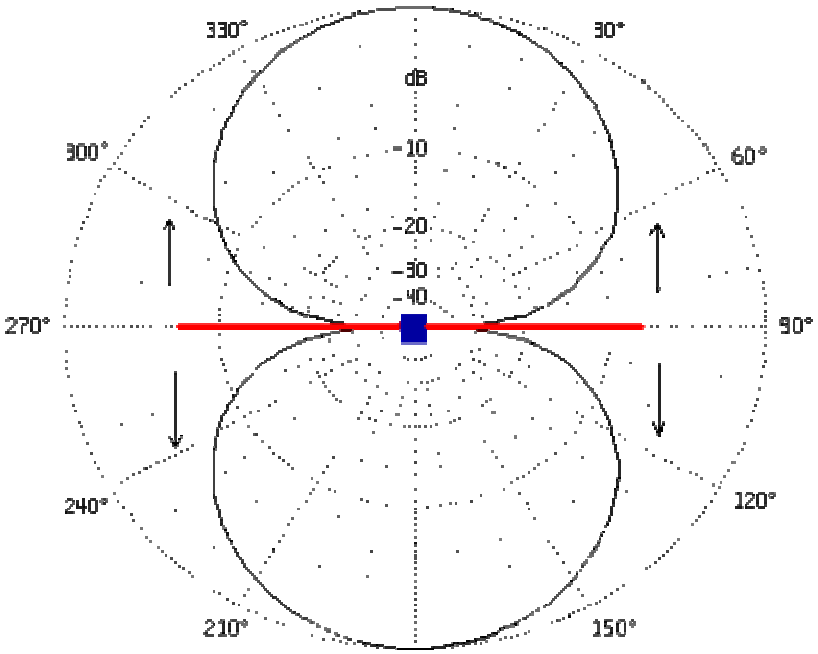
Dipolo:

La antena Dipolo es la más sencilla de todas la antenas, consta de un hilo conductor de cobre de tamaño de media longitud de onda (λ /2), cortado por la mitad donde se conecta el coaxial que viene del transmisor:

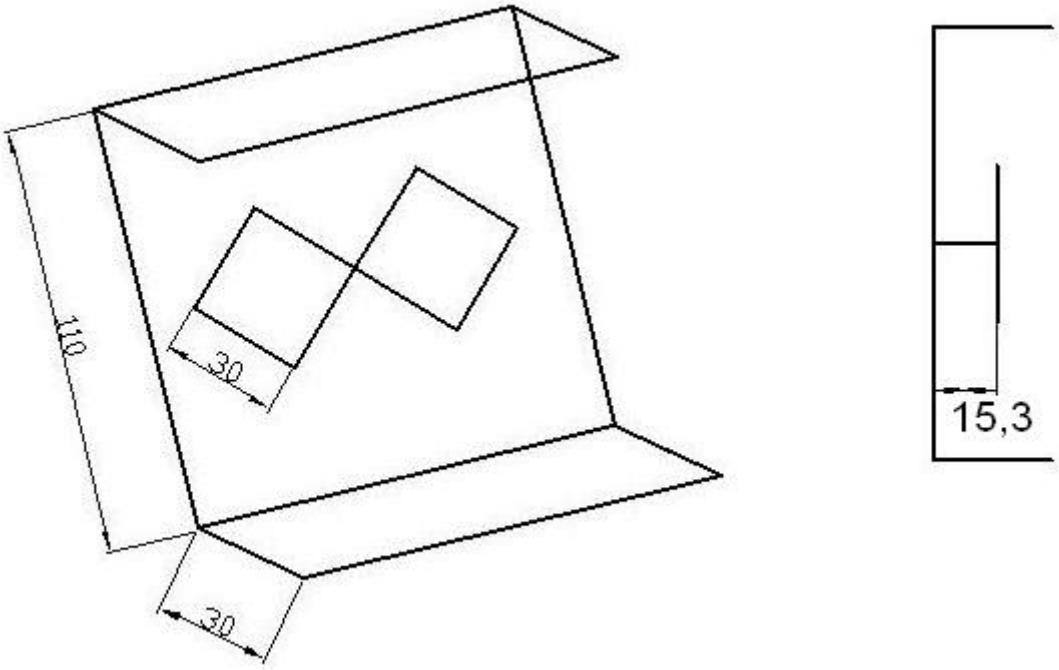
Por la tanto, a cada lado del coaxial tenemos **Lambda** /4 y soldamos el vivo y la malla del cable a cada uno de los hilos del dipolo.



Siendo su diagrama de radiación:



Partiendo de esto, teniendo en cuenta el plano de tierra que lo tendremos como deflector, podemos realizar el diseño de una antena direccional del tipo Biquad:



Siendo:

Lambda /4 = 30,71 mm
Lambda /8n = 15,35 mm

Construcción de la Biquad:

Esta antena fue inicialmente desarrollada por Trevol Marshall http://www.trevormarshall.com/biquad.htm. Y hemos hecho alguna modificación como nos indicó Toni de MataróWireless http://www.antenaswireless.net/ durante el taller de antenas Wireless que se realizó durante riojaparty 2003.

Utilizamos los siguientes materiales:

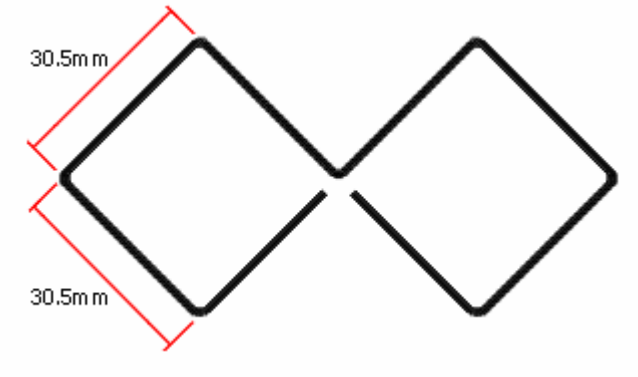
- 1 placa de cobre de circuito impreso (de fibra preferentemente) de 130x180mm
- 50cm de cable de cobre de 1,5mm
- 1 Conector N hembra chasis de rosca
- 50cm de estaño
- soldador
- sierra de calar
- broca del 12
- taladro

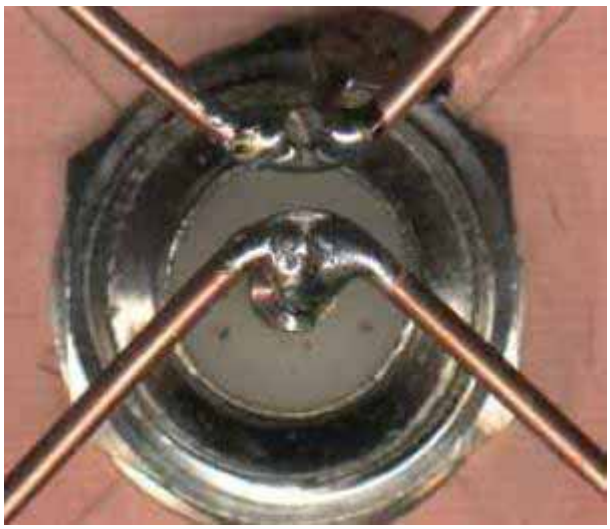
El material más novedoso a utilizar son estos conectores N, nosotros utilizaremos el macho de la izquierda encajándolo en el medio de la placa de 110x110 mm.

Nos ponemos manos a la obra para hacer nuestras primeras antenas:

Tenemos que soldar el conector N a la placa para una buena conexión de la tierra (malla del coaxial), como se muestra en la figura:

Y del mismo modo, soldar cuidadosamente la antena Biquad al conector N de la manera que se ve en esta fotografía:



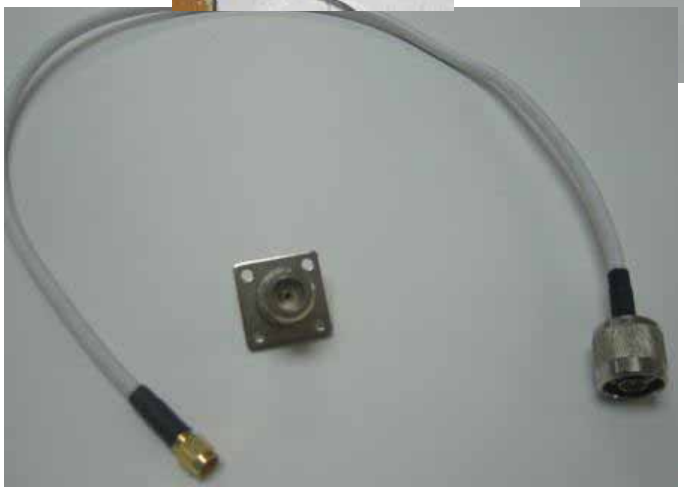


Finalmente obtenemos este resultado:

Necesitamos construir los pig-tail, los cables que conectaran las tarjetas con las antenas. Para hacer distintas pruebas, utilizaremos pig-tail comprados y haremos los otros con cable RG58 (de elevada pérdida) y con el RG213 de mejor calidad.

Cable RG213 grueso, conector N y SMA. Hacemos los pig-tail de un metro. Y los alternamos con las antenas. Podemos comprobar que la diferencia de pérdidas entre un pig-tail con un cable de peor pérdida y el otro no son apreciables con cables de tan poca longitud.

Esto deberá ser tenido en cuenta cuando se desee instalar varios metros de cable, con un metro la diferencia en el rendimiento no es apreciable.



Analizando los resultados con el netstrumbler, llegamos a las siguientes conclusiones:

- La ganancia de las Biquad construidas es de unos 8 dB aproximadamente.
- Utilizando pig-tail cortos (de un metro como los nuestros), no hay diferencia apreciable entre utilizar un cable RG58 y uno RG213.

Anexo 3: Wardriving.

Con esta palabra tan de moda en el mundo inalámbrico, estamos describiendo el entretenimiento de usuarios Wireless cuando buscan redes inalámbricas por las localidades.

Utilizando sniffers (olfateadores de red), capturan tramas de datos inalámbricos y los estudian, para determinar la localización de redes abiertas.

Una red se dice que está abierta cuando no dispone de ningún tipo de sistema de seguridad como los expuestos en esta memoria. Para que el resto de los usuarios estén informados sobre la existencia de este tipo de redes se suelen realizar "pintadas" en las paredes y en el suelo, dando información sobre si la red está abierta, si está cifrada, etc.

La simbología a utilizar es esta: