



**UNIVERSIDAD AUTÓNOMA DEL ESTADO DE  
HIDALGO**

---

---

**INSTITUTO DE CIENCIAS BÁSICAS E  
INGENIERÍA**

**“NUEVA TECNOLOGÍA PARA REDES  
INALÁMBRICAS Wi-Fi”**

**MONOGRAFÍA**

**QUE PARA OBTENER EL TÍTULO DE**

**INGENIERO EN ELECTRÓNICA Y  
TELECOMUNICACIONES**

**P R E S E N T A**

**GÓMEZ GARCÍA JUAN CARLOS**

**Asesor de Monografía: M. en C. EVA JEANINE LEZAMA ESTRADA**

**PACHUCA, HIDALGO**

**MAYO 2006**

# **AGRADECIMIENTOS**

## **A mi Padre**

Gracias a su esfuerzo, a su confianza que en mí depositó y a su total apoyo que me ha ayudado a salir adelante en las buenas y en las malas. Gracias a eso ha hecho de mí la persona que soy ahora.

## **A mi Asesora**

M. en C. Eva Jeanine, gracias por su apoyo y paciencia durante la elaboración de este trabajo, gracias a su valioso tiempo que invirtió en asesorarme, gracias por ser la maestra que apoya a sus alumnos y nunca los deja, gracias maestra por ser como es.

## **A mi Universidad**

Universidad Autónoma del Estado de Hidalgo, agracias a esta gloriosa institución que me albergó durante nueve semestres y me dio la educación superior que ahora tengo.

## **A mis Maestros**

Gracias a todos ellos por compartir su tiempo, sus consejos y sus grandes conocimientos con mis compañeros y en especial con migo y así ser los ingenieros que ahora somos.

## **JUSTIFICACIÓN**

Esta investigación ha sido realizada con el afán de conocer un poco más acerca de las redes inalámbricas pero en especial esta enfocada a la tecnología para redes inalámbricas llamada Wi-Fi, ya que difícilmente se encuentra a personas o bien empresas que ocupen una red inalámbrica eficiente y de alta calidad.

Hoy en día existen personas y empresas que tienen la necesidad de transmitir información inalámbrica, pero eso no lo es todo si no que también quieren o bien necesitan que esa transmisión sea de buena velocidad y además con calidad, Wi-Fi ha llegado a satisfacer esas necesidades.

Con este trabajo se conocerá a fondo lo que es Wi-Fi, desde lo más básico hasta sus aplicaciones más complejas y así poder llevar acabo una comunicación inalámbrica de la mejor calidad y de la más alta tecnología en cuanto a comunicaciones inalámbricas se refiere.

## **OBJETIVO GENERAL**

Mostrar la tecnología Wi-Fi con sus aplicaciones actuales y futuras, así como su desarrollo y sus elementos que la componen con el propósito de que esta tecnología sea conocida y utilizada por las personas interesadas en las comunicaciones en especial en las redes inalámbricas de tipo Lan.

# INTRODUCCIÓN

La necesidad de comunicación ha llevado a descubrir nuevos mundos tecnológicamente hablando, todo comenzó a finales del siglo XIX con la invención del primer teléfono alámbrico que funcionaba analógicamente.

Con el paso del tiempo la tecnología fue avanzando rápidamente y aquellos inventos analógicos y alámbricos se convirtieron en grandes inventos funcionales, digitales e inalámbricos como lo son los teléfonos celulares y las PC's que a partir de mediados del siglo pasado se fueron actualizando estrepitosamente debido a que estos aparatos o dispositivos se fueron tornando cada vez más comunes entre las personas, casas, empresas etc.

La comunicación inalámbrica se fue desarrollando con la necesidad de comunicar dispositivos que por el tipo de uso es imposible comunicarse alámbricamente como son teléfonos, computadoras (portátiles, y en algunos casos de mesa) y los más recientes PDA, estas comunicaciones inalámbricas se ha llevado acabo por tecnologías como láser, infrarrojo y radio principalmente, las cuales ya existen desde hace varios años pero con implementación comercial hasta hace pocos años.

Hoy en día las tecnologías inalámbricas son muy variadas como son GSM, GPRS, UMTS, LDSM, Bluetooth, WI-FI (tecnología de la cual habla este trabajo), principalmente.

En el capítulo uno trataremos acerca de las redes inalámbricas y algunos tipos de redes inalámbricas que existen.

En el capítulo dos hablaremos de que es Wi-Fi, como surgió y como funciona. Así como también vamos a describir los principios generales y protocolos en los que se basa el funcionamiento del estándar IEEE 802.11. Como ya sabemos, esta familia de estándares

tiene miembros diversos con diferencias tecnológicas. Por ello, vamos a empezar por presentar a la familia para luego centrarnos en su funcionamiento interno.

En el capítulo tres trataremos sobre cómo instalar una red, vamos a describir las características más importantes de los distintos componentes de una red inalámbrica. En este capítulo vamos a tratar fundamentalmente los adaptadores de red y los puntos de acceso,

En el capítulo 4 vamos a hablar de cómo conectar una red de tipo Wi-Fi a Internet así como también cómo tener mejor conexión por medio de antenas de estructura básica.

En el capítulo 5 vamos a hablar básicamente de cuáles son las aplicaciones básicas y más comunes de Wi-Fi en la actualidad y además cuáles pueden o tal vez van a ser las futuras aplicaciones.

# ÍNDICE

## CAPÍTULO 1

### COMO HAN EVOLUCIONADO LAS REDES INALÁMBRICAS 5

1.1 REDES INALÁMBRICAS DE DATOS.....	6
1.2 TIPOS DE REDES INALÁMBRICAS DE DATOS.....	7
1.3 REDES INALÁMBRICAS DE ÁREA PERSONAL.....	9
1.3.1 Infrarrojo.....	10
1.3.2 Bluetooth.....	12
1.3.3 DECT.....	14
1.4 REDES INALÁMBRICAS ÁREA LOCAL.....	15
1.4.1 HiperLAN.....	16
1.4.2 HomeRF.....	17
1.4.3 Wi-Fi.....	18
1.5 REDES INALÁMBRICAS DE ÁREA METROPOLITANA.....	19
1.5.1 LMDS.....	20
1.5.2 WIMAX.....	20
1.6 REDES INALÁMBRICAS GLOBALES.....	22
1.6.1 GSM.....	23
1.6.2 2,5G.....	23
1.6.3 CDMA.....	26
1.6.4 3G.....	26
1.7 LA LUCHA TECNOLÓGICA.....	29
1.8 REGULACIÓN.....	30

## CAPÍTULO 2

### PROTOCOLOS Y ESTÁNDARES UTILIZADOS EN Wi-Fi 32

2.1 PROTOCOLOS.....	32
2.1.1 Protocolos de IEEE 802.11.....	34
2.2 El modelo OSI.....	36
2.3 LA EVOLUCIÓN DE IEEE 802.....	38
2.3.1 Las redes de cable.....	39
2.3.2 Las redes inalámbricas.....	40
2.3.3 Las capas de IEEE 802.....	43
2.4 LA CAPA FÍSICA.....	44
2.4.1 Espectro expandido.....	45
2.4.2 Hedy Lamarr y George Antheil.....	47
2.4.3 FHSS.....	47
2.4.4 DSSS.....	50

2.4.5 OFDM.....	51
2.4.6 Modulación de la señal.....	52
2.5 MAC. El CONTROL DE ACCESO AL MEDIO.....	53
2.5.1 Evitar las colisiones.....	54
2.5.2 Los servicios.....	56
2.5.3La gestión.....	58
2.5.4 El flujo de datos.....	59
2.6 LA ESTRUCTURA DE RED.....	60
2.7 HIPERLAN FRENTE A 802.11 a.....	61

## CAPÍTULO 3

<b>EQUIPO BÁSICO PARA UNA RED Wi-Fi</b>	<b>64</b>
3.1 POR QUE INSTALAR UNA RED INALÁMBRICA .....	64
3.1.1 Ventajas.....	65
3.1.2 inconvenientes.....	67
3.1.3 Qué hacer .....	68
3.2 QUÉ POSIBILIDADES TENEMOS.....	70
3.2.1 Las distintas configuraciones de red.....	70
3.3 NECESIDAD DE LOS PUNTOS DE ACCESO.....	72
3.4 CREAR UNA RED EXTENSA.....	73
3.5 SOBRE EL ALCANCE .....	75
3.5.1 Interferencias.....	76
3.5.2 Pérdida de propagación.....	77
3.6 EL EQUIPAMIENTO NECESARIO.....	78
3.6.1 Elegir un punto de acceso.....	78
3.6.2 Características de los puntos de acceso.....	81
3.6.2.1 La radio.....	82
3.6.2.2 Los puertos.....	83
3.6.2.3 Gestión del punto de acceso.....	84
3.6.3 Adaptadores inalámbricos de red.....	84
3.6.4 Tipos de adaptadores de red.....	85
3.6.4.1 Tarjetas PCMCIA.....	86
3.6.4.2 Adaptadores PCI e ISA.....	88
3.6.4.3 Adaptadores USB.....	90
3.6.4.4 Adaptadores para PDA .....	92
3.6.4.5 Compatibilidad con los sistemas operativos.....	94

## CAPÍTULO 4

### CONEXIÓN A PORTAL INTERNET CON ELEMENTO BÁSICO DE TRANSMISIÓN 96

4.1 LA CONEXIÓN A INTERNET.....	96
4.2 EL ACCESO A INTERNET.....	97
4.2.1 Ancho de banda.....	97
4.2.2 El proveedor de acceso.....	98
4.3 EL ACCESO DE BANDA ANCHA.....	99
4.3.1 Las ventajas de la banda ancha.....	101
4.3.2 Acceso mediante ADSL.....	101
4.3.3 Acceso mediante módem cable.....	103
4.3.4 Acceso por satélite.....	104
4.3.5 Acceso vía radio LMDS.....	105
4.3.6 Acceso mediante circuitos de datos.....	106
4.4 LA CONEXIÓN DE WI-FI CON INTERNET.....	107
4.4.1 Instalar la conexión entre Wi-Fi e Internet.....	108
4.4.2 Configurar la conexión en el punto de acceso.....	109
4.4.3 Comprobar el acceso a Internet.....	110
4.5 LA CONFIGURACIÓN DE UN ROUTER.....	111
4.5.1 Las distintas direcciones IP.....	111
4.6 DHCP.....	114
4.7 NAT.....	115
4.7.1 El problema con ciertas aplicaciones.....	117
4.7.2 Reenvío de puerto.....	118
4.8 DMZ.....	119
4.8.1 Filtros.....	120
4.8.2 Máscara de subred.....	121
4.9 DNS.....	123
4.10 Colocar una antena externa.....	125
4.10.1 Sobre las antenas.....	126
4.10.1 Sobre las antenas.....	128
4.10.1.1 La ganancia.....	127
4.10.1.2 La relación señal/ruido.....	128
4.10.1.3 Patrón de radiación y apertura del haz.....	128
4.10.1.4 Polarización.....	130
4.10.2 Tipos de antenas.....	130
4.10.3 Los conectores y cables de antena.....	133
4.10.3.1 Tipos de conectores.....	134
4.10.3.2 El cable.....	136
4.10.3.3 El adaptador o pigtail.....	138
4.10.4 Calcular el alcance.....	139
4.10.4.1 Pérdida de propagación.....	140
4.10.4.2 Pérdidas y ganancias.....	140
4.10.5 Elegir una antena.....	143

4.10.6 Dónde situar la antena.....	143
4.10.6.1 Sintonizar la antena.....	145
4.10.7 Construir una antena.....	146
4.10.7.1 Principios básicos.....	147
4.10.7.2 Una antena con una lata .....	148
4.10.7.3 Una antena con un bote de Pringles .....	151

## **CAPÍTULO 5**

### **APLICACIONES DE LAS REDES Wi-Fi 157**

5.1 APLICACIONES.....	157
5.1.1 Aplicaciones en la empresa.....	159
5.2 COMUNIDADES INALÁMBRICAS.....	160
5.2.1 Organizaciones de las comunidades inalámbricas.....	161
5.3 REDES COMERCIALES DE ACCESO PÚBLICO INALÁMBRICO.....	162
5.4 ENLACE PUNTO A PUNTO.....	165
5.5 TELEVIGILANCIA.....	166
5.6 WI-FI EN EL COCHE.....	170
5.7 TELEFONÍA WI-FI.....	172
5.7.1 Recibir llamadas en el terminal Wi-Fi.....	174
5.7.2 Teléfonos Wi-Fi.....	174
5.8 EL HOGAR DIGITAL.....	175

### **CONCLUSIONES 178**

### **GLOSARIO 179**

### **BIBLIOGRAFÍA 206**

## CAPÍTULO 1

### COMO HAN EVOLUCIONADO LAS REDES INALÁMBRICAS

Se llama comunicación inalámbrica a aquella que se lleva a cabo sin el uso de cables de interconexión entre los participantes; por ejemplo, una comunicación con teléfono móvil es inalámbrica, mientras que una comunicación con teléfono fijo tradicional no lo es.

No cabe duda de que la tecnología inalámbrica está ocupando rápidamente las preferencias de todo tipo de usuarios. La telefonía móvil está cada vez más cerca de convertirse en un sistema de comunicación personal universal en el mundo, los teléfonos inalámbricos de casa son cada vez más comunes en detrimento de los incómodos teléfonos con cables enrollados y, desde hace poco, los ordenadores están también liberándose de sus ataduras. Cada vez son más los hogares, los cafés, las pequeñas empresas, los aeropuertos o las grandes compañías en los que se dispone de redes inalámbricas de ordenadores.

Aunque las tecnologías que hacen posible las comunicaciones inalámbricas (láser, infrarrojo y radio, principalmente) existen desde hace muchos años, su implantación comercial no ha sido posible hasta fechas recientes. El primer servicio que se liberó del cable fue la telefonía, la transmisión de voz. La telefonía móvil apareció en los años setenta y poco a poco se ha ido desarrollando hasta superar a la telefonía fija en el número de líneas; por ejemplo, en Europa existía a finales de 2002 una penetración de telefonía fija de 50 líneas por cada 100 habitantes mientras que la telefonía móvil llegaba a las 80 líneas.

La revolución de los ordenadores personales y el espectacular desarrollo de Internet están haciendo que la informática sea tan común en la vida diaria como lo es el teléfono. Tenemos ordenadores de sobremesa, portátiles o los más recientes PDA (Personal Digital Assistant, 'Asistentes Digitales Personales') o TabletPC. Por otro lado, también tenemos la informática en todo tipo de útiles diarios: desde el coche o la calefacción de

casa hasta los juguetes de los niños. Todos estos dispositivos son susceptibles de comunicarse entre sí y, aunque pueden hacerlo por los sistemas de cables tradicionales, su mayor potencial se alcanza a través de las comunicaciones inalámbricas. (<http://www.maestrosdelWeb.com/editorial/redeswlan/>, agosto 2005)

## **1.1 REDES INALÁMBRICAS DE DATOS**

Una red inalámbrica de datos no es más que un conjunto de ordenadores, o de cualquier otro dispositivo informático, comunicados entre sí mediante soluciones que no requieran del uso de cables de interconexión.

Aunque se puede llegar a pensar que las redes inalámbricas están orientadas a dar solución a las necesidades de comunicaciones de las empresas, dado su bajo costo, cada vez más forman parte del equipamiento de comunicaciones de los hogares.

Para disponer de una red inalámbrica, sólo hace falta instalar una tarjeta de red inalámbrica en los ordenadores involucrados, hacer una pequeña configuración y listo. Esto quiere decir que instalar una red inalámbrica es un proceso mucho más rápido y flexible que instalar una red cableada. Piense lo que supone no tener que instalar cables por los suelos y paredes de la oficina o la casa. Además, las redes inalámbricas les permiten a sus usuarios moverse libremente sin perder la comunicación.

Una vez instalada la red inalámbrica, su utilización es prácticamente idéntica a la de una red cableada. Los ordenadores que forman parte de la red pueden comunicarse entre sí y compartir toda clase de recursos. Se pueden compartir archivos, directorios, impresoras, disqueteras o, incluso el acceso a otras redes, como puede ser Internet. Para el usuario, en general, no hay diferencia entre estar conectado a una red cableada o a una red inalámbrica. De la misma forma, al igual que ocurre con las redes cableadas, una red inalámbrica puede estar formada por tan sólo dos ordenadores o por miles de ellos.

Por todo lo anterior, las soluciones inalámbricas están poco a poco ocupando un lugar más destacado dentro del panorama de las posibilidades que tienen dos equipos informáticos de comunicarse.

No obstante, hoy por hoy, las soluciones inalámbricas tienen también algunos inconvenientes: tienen un menor ancho de banda (velocidad de transmisión) y, en general, son más caras que las soluciones con cable. El ancho de banda de las soluciones inalámbricas actuales se encuentra entre los 11 y los 54 Mbps (aunque ya existen algunas soluciones propietarias a 100 Mbps), mientras que las redes de cable alcanzan los 100 Mbps. En cuanto al precio, aunque, en general, son algo más caras, en muchas ocasiones resultan no sólo más baratas que su alternativa cableada, sino que se muestran como la solución más conveniente.

*(<http://www.maestrosdelWeb.com/editorial/redeswlan/>, agosto 2005)*

## **1.2 TIPOS DE REDES INALÁMBRICAS DE DATOS**

Cuando anteriormente hemos hablado de las redes inalámbricas de datos, realmente nos hemos estado refiriendo a las redes de área local inalámbricas. Sin embargo, a poco que hayamos leído algún que otro artículo al respecto o participado en alguna conversación, rápidamente vienen a nuestra mente siglas como Wi-Fi, Bluetooth, UMTS, etc. Estas siglas, al igual que otras existentes, hacen referencia a distintos tipos de redes o de tecnologías inalámbricas. Para saber bien por dónde nos movemos, vamos a paramos un momento a diferenciar los distintos tipos de redes inalámbricas que existen.

Las comunicaciones inalámbricas, como cualquier otra cosa en esta vida, pueden clasificarse de distintas formas dependiendo del criterio al que se atienda. En este caso, vamos a clasificar los sistemas de comunicaciones inalámbricas de acuerdo con su alcance. Se llama alcance a la distancia máxima a la que pueden situarse las dos partes de la comunicación inalámbrica.

*(<http://www.redaragon.com/informatica/wireless/redwireless.asp>, agosto 2005)*

WPAN	WLAN		WMAN	CELULAR	
<10 metros	Edificio	Campus	Ciudad	Región	Global
<i>Bluetooth</i>	<i>Wi-Fi</i>		<i>LMDS</i>	<i>2,5G</i>	
<i>802.15</i>	<i>HomeRF</i>		<i>MMDS</i>	<i>3G</i>	
<i>IrDA</i>	<i>HiperLAN</i>		<i>WiMAX</i>		

*Tabla 1.1 tipos de redes inalámbricas*  
([www.htmlWeb.net/redes/topologia/topologia\\_1.html](http://www.htmlWeb.net/redes/topologia/topologia_1.html), agosto 2005)

Las comunicaciones inalámbricas se dividen en los siguientes grupos de acuerdo con su alcance:

- Las redes inalámbricas de área personal o WPAN (Wireless Personal Área Network) cubren distancias inferiores a los 10 metros. Estas soluciones están pensadas para interconectar los distintos dispositivos de un usuario (por ejemplo, el ordenador con la impresora). Éste es el caso de la tecnología Bluetooth o de IEEE 802.15.
- Las redes inalámbricas de área local o WLAN (Wireless Local Área Network) cubren distancias de unos cientos de metros. Estas redes están pensadas para crear un entorno de red local entre ordenadores o terminales situados en un mismo edificio o grupo de edificios. Éste es el caso de Wi-Fi o HomeRF, por ejemplo.
- Las redes inalámbricas de área metropolitana o WMAN (Wireless Metropolitan Area Network) pretenden cubrir el área de una ciudad o entorno metropolitano. Los protocolos LMDS (Local Multipoint Distribution Service, 'Servicio Local de Distribución Multipunto') o WiMAX (World Wide Interoperability for Microwave Access, 'Interoperatividad Mundial para Accesos de Microondas') ofrecen soluciones de este tipo.
- Por último, tenemos las redes globales con posibilidad de cubrir toda una región (país o grupo de países). Estas redes se basan en la tecnología celular y han aparecido como evolución de las redes de comunicaciones de voz. Éste es el caso de las redes de telefonía móvil conocidas como 2,5G o 3G. En comunicaciones móviles de voz se les llama 1G (primera generación) a los sistemas analógicos

(tipo NMT o AWS), 2G a los digitales (tipo GSM o CDMA), 2,5G a los digitales con soporte para datos a alta velocidad (tipo GPRS, IS-95B o EDGE, Enhanced Data for GSM Evolution) y 3G o tercera generación a los nuevos sistemas de telefonía celular con capacidad de gran ancho de banda. Este último es el caso de UMTS (Universal Mobile Telecommunications Service, 'Servicio Universal de Telecomunicaciones Móviles') o CDMA-2000 (Code División Multiple Access, 'Acceso Múltiple por División de Código'), por ejemplo.

(<http://www.redaragon.com/informatica/wireless/redwireless.asp> , agosto 2005)

### **1.3 REDES INALÁMBRICAS DE ÁREA PERSONAL**

Se ha venido a llamar redes inalámbricas de área personal, WPAN (Wireless Personal Area Networks), a aquellas redes que tienen un área de cobertura de varios metros (del orden de 10 metros). La finalidad de estas redes es comunicar cualquier dispositivo personal (ordenador, terminal móvil, PDA, etc.) con sus periféricos, así como permitir una comunicación directa a corta distancia entre estos dispositivos.

Hoy en día se dispone de una variedad de dispositivos personales: al ordenador se ha unido el teléfono móvil y, más recientemente, el PDA. Tradicionalmente, la comunicación de estos dispositivos con sus periféricos se ha hecho utilizando el cable. No obstante, tener pequeños dispositivos repletos de cables alrededor no resulta muy cómodo, por lo que la comunicación inalámbrica supone un gran avance en cuanto a versatilidad y comodidad.

Impresoras, auriculares, módem, escáner, micrófonos, teclados, todos estos dispositivos pueden intercomunicarse con su terminal vía radio evitando tener que conectar cables para cada uno de ellos. ([www.htmlWeb.net/redes/topologia/topologia\\_1.htm](http://www.htmlWeb.net/redes/topologia/topologia_1.htm) , agosto 2005)

### 1.3.1 Infrarrojo

La luz infrarrojo es un tipo de radiación electromagnética invisible para el ojo humano. Los sistemas de comunicaciones con infrarrojo se basan en la emisión y recepción de haces de luz infrarroja. La mayoría de los mandos a distancia de los aparatos domésticos (televisión, vídeo, equipos de música, etc.) utilizan comunicación por infrarrojo. Por otro lado, la mayoría de las famosas PDA (Agendas Electrónicas Personales), algunos modelos de teléfonos móviles y muchos ordenadores portátiles incluyen un dispositivo infrarrojo como medio de comunicación entre ellos.

*(<http://es.wikipedia.org/wiki/Infrarrojo>, agosto 2005)*

Los sistemas de comunicaciones de infrarrojo pueden ser divididos en dos categorías:

- **Infrarrojo de haz directo.** Esta comunicación necesita una visibilidad directa sin obstáculos entre ambos terminales.
- **Infrarrojo de haz difuso.** En este caso el haz tiene suficiente potencia como para alcanzar el destino mediante múltiples reflexiones en los obstáculos intermedios. En este caso no se necesita visibilidad directa entre terminales.

Las ventajas que ofrecen las comunicaciones de infrarrojo es que no están reguladas, son de bajo costo e inmunes a interferencias de los sistemas de radio de alta frecuencia. Sus principales inconvenientes son su corto alcance, el hecho de que no puedan traspasar objetos y que no son utilizables en el exterior debido a que agentes naturales como la lluvia o la niebla les producen grandes interferencias.

El estándar original IEEE 802.11 (antecesor de Wi-Fi) contemplaba el uso de infrarrojos, pero nunca llegó a desarrollarse debido principalmente a los inconvenientes mencionados. No obstante, no cabe duda de que los sistemas infrarrojos son de los más eficaces sistemas de comunicaciones punto a punto para corta distancia. De hecho, es el sistema utilizado, no sólo por millones de mandos a distancia, sino por millones de

ordenadores portátiles, PDA, teléfonos móviles y otros equipos electrónicos de todo el mundo.

IRDA (Infrared Data Association) es una asociación que tiene como objetivo crear y promover el uso de sistemas de comunicaciones por infrarrojo. Actualmente tiene creados dos estándares:

- **IrDA-Control.** Es un protocolo de baja velocidad optimizado para ser utilizado en los dispositivos de control remoto inalámbricos. Éste es el caso de dispositivos como los mandos a distancia, ratones de ordenador o joysticks.
- **IrDA-Data.** Es un protocolo orientado a crear redes de datos de corto alcance. Está diseñado para trabajar a distancias menores de 1 metro y a velocidades que van desde los 9,6 Kbps hasta los 16 Mbps. Existe una versión que extiende el alcance a 2 metros, con un alto coste de consumo energético, y otra que reduce el alcance a 30 cm., reduciendo el consumo energético a la décima parte. Existen también varios protocolos opcionales que habilitan el protocolo IrDA-Data para ser utilizado en aplicaciones específicas. Éste es el caso de IrCOMM (Infrared Serial/parallel Port, Emulation, 'Emulador infrarrojo de Puerto Serie/Paralelo'), IrTran-P (Infrared Digital Image Transfer, 'Transferencia de Imagen Digital con Infrarrojo'), IrLAN (Infrared Local Area Network Connectivity, 'Conectividad de Red de Área Local con Infrarrojo') o IrMC (Infrared Mobile Communications, 'Comunicaciones Móviles con Infrarrojo')

La tecnología de infrarrojos parece que ha encontrado su nicho en las comunicaciones a muy corto alcance. Esto convierte a IRDA en compatible con tecnologías como Bluetooth. Además, IRDA ofrece la ventaja adicional de la seguridad, ya que las emisiones de haces infrarrojos se quedan en un entorno mucho más privado que las propagaciones de ondas de radio.

*(espanol.geocities.com/revista\_infrarrojo/index.htm, agosto 2005)*



*Figura 1.1 Dispositivos infrarrojos*

*(espanol.geocities.com/revista\_infrarrojo/index.htm, agosto 2005)*

### **1.3.2 Bluetooth**

La iniciativa Bluetooth se inició a principios de 1998 con un SIG (Grupo de Interés Especial) promovido por Ericsson, IBM, Intel, Nokia y Toshiba bajo el codename "Bluetooth" pero se hizo público hasta el 20 de Mayo del mismo año. Al transcurso de 2 meses, la primera especificación Bluetooth 1.0 fue liberada y en la actualidad se está trabajando en Bluetooth 2.0 con la colaboración de 3Com, Ericsson, IBM, Intel, Lucent Technologies, Microsoft, Motorola, Nokia y Toshiba. Como se puede apreciar, el número de compañías interesadas en el proyecto casi se ha duplicado y actualmente el SIG cuenta con 1883 miembros.

Bluetooth es una tecnología orientada a la conectividad inalámbrica entre dispositivos; estos dispositivos pueden ser computadoras de escritorio, PDAs, teléfonos móviles y en fin, las posibilidades pueden considerarse infinitas.

La tecnología Bluetooth revoluciona el mercado de la conectividad personal ya que es un estándar libre, proveyendo interconectividad entre cualquier tipo de dispositivo que cumpla con las especificaciones inalámbricas Bluetooth.

A diferencia de otros estándares inalámbricos, la especificación Bluetooth incluye dos capas, la capa de enlace y la de aplicación para los desarrolladores de productos que soportan datos, voz, y aplicaciones de contenido centralizado.

Los dispositivos de radio que soportan la tecnología no requieren de licencia y deben tener un espectro de 2.4 Ghz para asegurar la compatibilidad en todo el mundo. Estos dispositivos usan spread spectrum, frequency hopping, y full-duplex signal a más de 1600 hops/sec. Además se pueden establecer y mantener mas de seis conexiones simultáneas.

Cada dispositivo Bluetooth esta equipado con un transceiver que transmite y recibe a una frecuencia de 2.4 Ghz, la cuál está disponible en todo el mundo y como se menciona anteriormente en este documento, no requiere de ninguna licencia. Además de los canales de datos, están disponibles 3 canales de voz a 64kbs. Cada dispositivo tiene una dirección única de 48 bits basada en el estándar de la IEEE 802.11 para redes de área local inalámbricas, que le permite formar temporalmente parte de una piconet. Las conexiones son uno a uno, con un rango máximo de 10 metros, aunque mediante el uso de repetidores se puede lograr un alcance de hasta 100 metros con algo de distorsión. El ancho de banda que se alcanza entre los dispositivos "bluetooth enabled" se espera en 1Mbps.

Bluetooth utiliza la técnica FHSS (Frequency Hopping Spread Specowm, 'Espectro Expandido por Salto de Frecuencia') en la banda de frecuencias de 2,4 GHz. Puede establecer comunicaciones asimétricas donde la velocidad máxima en una dirección es de 721 Kbps y 57,6 Kbps en la otra o comunicaciones simétricas de 432,6 Kbps en ambas direcciones. Por otro lado, puede transmitir tanto voz como datos.

A pesar de la aparente complementariedad de bluetooth con Wi-Fi, lo cierto es que esta última tecnología está evolucionando mucho más rápidamente que la primera. Teniendo en cuenta que Wi-Fi tiene un ancho de banda mucho mayor que Bluetooth, que goza de un alcance bastante mayor y que poco a poco está consiguiendo equipararse en precios,

existe una cierta incertidumbre en cuanto al futuro de Bluetooth.

(<http://www.Webopedia.com/TERM/P/piconet.html>, Julio 2005)



*Figura 1.2 Dispositivos Bluetooth*

(<http://vig.pearsoned.com/samplechapter/0130661066.pdf>, julio2005 )

### 1.3.3 DECT

El estándar DECT (Digital Enhanced Cordless Telecommunications, 'Telecomunicaciones Digitales Inalámbricas Mejoradas') existe desde 1992 promulgado por ETSI (European Telecommunications Standards Institute, 'Instituto Europeo de Normalización en Telecomunicaciones'). El objetivo de DECT es facilitar las comunicaciones inalámbricas entre terminales telefónicos (teléfonos inalámbricos y centralitas inalámbricas).

DECT trabaja en la banda de frecuencias de 1,9 GHz y utiliza la técnica TDMA (Time Division Multiple Access, 'Acceso Múltiple por División de Tiempo'). La velocidad máxima actual a la que trabaja DECT es de 2 Mbps, aunque existe una propuesta de ETSI para aumentar esta velocidad hasta los 20 Mbps y conseguir alcances de hasta 17 kilómetros.



*Figura 1.3 Dispositivos DECT  
(espanol.geocities.com/revista\_DECT/index.htm, agosto 2005)*

A pesar de que, técnicamente, DECT podría ser un competidor de Bluetooth o, incluso, de otros sistemas inalámbricos de mayor alcance, el hecho de que trabaje en la banda de 1,9 GHz (utilizada en Europa para esta tecnología pero con barreras reguladas en Norteamérica y otras partes del mundo) y que esté muy orientada a voz le pone grandes limitaciones para competir con esas otras tecnologías.

*(en.wikipedia.org/wiki/DECT, agosto 2005)*

## **1.4 REDES INALÁMBRICAS ÁREA LOCAL**

Se llama redes inalámbricas de área local, WLAN (Wireless Local Area Networks), a aquellas redes que tienen una cobertura de unos cientos de metros. Estas redes están pensadas para crear un entorno de red local entre ordenadores o terminales situados en un mismo edificio o grupo de edificios. En el mercado existen distintas tecnologías que dan respuesta a esta necesidad. Entre estas tecnologías se encuentran las siguientes:

HiperLAN

HomeRF

Wi-Fi

HISWAN

OpenAir

*([www.htmlWeb.net/redes/topologia/topologia\\_1.html](http://www.htmlWeb.net/redes/topologia/topologia_1.html), agosto 2005)*

### 1.4.1 HiperLAN

HiperLAN (High-Performance Radio Local Area Network, 'Red de Área Local de Radio de Alto Rendimiento') es el resultado de los trabajos de ETSI (European Telecommunications Standards Institute, 'Instituto Europeo de Normalización en Telecomunicaciones') para conseguir un estándar de red de área local inalámbrica vía radio. La primera versión de este estándar, HiperLAN/I, publicada en 1996, trabajaba en la banda de frecuencias de 5 GHz y alcanzaba velocidades de hasta 24 Mbps.

En 1997 ETSI reconoció que HiperLAN/1 no estaba resultando viable comercialmente y creó un proyecto llamado BRAN (Broadband Radio Access Network, 'Red de Acceso Radio de Banda Ancha'). El resultado se obtuvo en febrero de 2000 con HiperLAN/2. Este estándar está diseñado para ofrecer accesos inalámbricos de alta velocidad a redes ATM (Asynchronous Transfer Mode, 'Modo de Transferencia Asíncrono'), a redes celulares de tercera generación, Firewire IEEE 1394 y redes IP.

HiperLAN2 ofrece velocidades de transmisión de 54 Mbps utilizando el sistema OFDM (Orthogonal Frequency Division Multiplying, 'Multiplexado Ortogonal por División de Frecuencia'). Las frecuencias utilizadas son de 5,25 a 5,35 GHz para sistemas de interior a 200 mW de potencia y de 5,47 a 5,725 GHz para sistemas de exterior a 1 000 mW de potencia.

En 1999 se creó una asociación, HiperLAN2 Global Forum, formada por Nokia, Tenovis, Del, Ericsson, Telia y Texas Instrumen para promover el uso de este estándar. A pesar de ello, este sistema sigue sin alcanzar el éxito comercial deseado.

([www.hiperlan2.com/presdocs/site/whitepaper.pdf](http://www.hiperlan2.com/presdocs/site/whitepaper.pdf), agosto 2005)

### 1.4.2 HomeRF

En 1998 se creó un grupo de trabajo bajo el nombre HomeRF (Home Radio Frequency, 'Radiofrecuencia del Hogar') con el objetivo de desarrollar y promover un sistema de red inalámbrica para el hogar. Aunque el grupo de trabajo lo formaron inicialmente Compaq, HP, IBM, Intel y Microsoft, posteriormente se le han ido uniendo más miembros hasta casi alcanzar los 100 a finales de 2000. Actualmente cuentan con menos miembros debido a la proliferación de otras tecnologías.

HomeRF es una tecnología similar a la de Bluetooth, su nombre completo es Home Radio Frequency, proporciona interconexión entre productos electrónicos de consumo dentro del hogar. Utiliza también la misma banda de 2,4 GHz, pero no interfiere con ella gracias al método de salto de frecuencia (protocolo de acceso inalámbrico compartido), que en este caso es de 50 saltos por segundo, en vez del Direct Sequence empleado en otras tecnologías. Asimismo, la potencia de los transmisores es de sólo 100 mW. Las principales aplicaciones que encuentra HomeRF son la conexión inalámbrica de un PC a otros dispositivos electrónicos de consumo, como vídeos, electrodomésticos, juguetes avanzados, impresoras, centralitas, teléfonos inalámbricos, etc., con un rango de distancia que alcanza hasta los 50 metros. Al igual que Bluetooth, HomeRF utiliza el salto de frecuencia para evitar interferencias, admite la comunicación de datos hasta 2 Mbits/s y permite conectar hasta un total de 127 dispositivos. Soporta comunicación de voz y datos, admitiendo hasta seis conversaciones. El grupo de trabajo HRFWG formado en marzo de 1998 y que ahora cuenta con más de cien compañías, ha desarrollado el protocolo SWAP (Shared Wireless Access Protocol), basado en el estándar IEEE 802.11 para datos y en DECT para voz, que se usará en esta aplicación. SWAP puede soportar todo tipo de servicios enfocados a la transmisión de datos TCP/IP, así como protocolos para voz, tipo DECT/GAP, en redes domésticas. Por cierto, HomeRF, como Bluetooth, utiliza el sistema FUSS.

*(<http://cek.bitacoras.com/archivos/2004/06/03/homerf/>, octubre 2005)*



*Figura 1.4 PDA con Dispositivos inalámbricos  
(<http://cek.bitacoras.com/archivos/2004/06/03/homerf/>, octubre 2005)*

### 1.4.3 Wi-Fi

Durante bastantes años, las redes inalámbricas de ordenadores se llevaban a cabo utilizando soluciones particulares de cada fabricante. Estas soluciones, llamadas propietarias, tenían el gran inconveniente de no permitir interconectar equipos de distintos fabricantes. Cada fabricante desarrollaba su propia solución y la comercializaba por su cuenta. Para el cliente, esto suponía tener que trabajar siempre con el mismo fabricante, y, por tanto, estar sometido siempre a las limitadas soluciones que un solo fabricante puede ofrecer.

La única forma de resolver este problema es desarrollar un sistema normalizado que acepten los fabricantes como sistema común. Idealmente, son los organismos internacionales de normalización quienes realizan este trabajo con la ayuda de los propios interesados. No obstante, en muchas ocasiones una de las empresas o asociación de empresas ha sido la que ha logrado imponer su sistema en el mercado. Éste es el caso, por ejemplo, del sistema VHS de video o del sistema GSM de comunicaciones móviles.

En el caso de las redes locales inalámbricas, el sistema que se está imponiendo es el normalizado por IEEE con el nombre 802.11b. A esta norma se la conoce más habitualmente como Wi-Fi o Wireless Fidelity ('Fidelidad Inalámbrica').

Con el sistema Wi-Fi se pueden establecer comunicaciones a una velocidad máxima de 11 Mbps, alcanzándose distancias de hasta varios cientos de metros. No obstante, versiones más recientes de esta tecnología permiten alcanzar los 22, 54 y hasta los 100 Mbps. ([www.wikipedia.org](http://www.wikipedia.org) agosto 2005)



*Figura 1.5 Ordenador TabletPC con conexión inalámbrica Wi-Fi*  
([www.wikipedia.org](http://www.wikipedia.org) agosto 2005)

## **1.5 REDES INALÁMBRICAS DE ÁREA METROPOLITANA**

Se llama redes inalámbricas de área metropolitana, WMAN (Wireless Metropolitan Area Networks), a aquellas redes que tienen una cobertura desde unos cientos de metros hasta varios kilómetros. El objetivo es poder cubrir el área de una ciudad o entorno metropolitano. Los protocolos LMDS (Local Multipoint Distribution Service, 'Servicio Local de Distribución Multipunto') o WiMAX (WorldWide Interoperability for Microwave Access, 'Interoperatividad mundial para accesos de microondas') ofrecen soluciones de este tipo.

Existen dos topologías básicas: sistemas que facilitan una comunicación punto a punto a alta velocidad entre dos emplazamientos fijos y sistemas que permiten crear una red punto-multipunto entre emplazamientos fijos. En este último caso el ancho de banda utilizado es comparado entre todos los usuarios del sistema.

*([www.htmlWeb.net/redes/topologia/topologia\\_1.html](http://www.htmlWeb.net/redes/topologia/topologia_1.html) ,agosto 2005)*

### **1.5.1 LMDS**

LMDS es una tecnología inalámbrica vía radio para comunicación entre puntos fijos. Esto quiere decir que no es una tecnología pensada para ser utilizada por Wireless en movimiento. El rango de frecuencias utilizado varía entre 2 y 40 GHz dependiendo de la regulación del país en el que se utilice.

LMDS utiliza un transmisor central emitiendo su señal sobre un radio de hasta 5 kilómetros. Las antenas de los receptores se sitúan generalmente en los techos de los edificios para procurar una visibilidad directa con el transmisor central.

Un inconveniente de los sistemas LMDS es que no existe un estándar que asegure la compatibilidad de los equipos de distintos fabricantes. En cualquier caso, en general, las soluciones LMDS no están teniendo una buena aceptación comercial.

*([www.wikipedia.org](http://www.wikipedia.org) agosto 2005)*

### **1.5.2 WIMAX**

WiMAX (WorldWide Interoperability for Microwave Access, 'Interoperatividad Mundial para Accesos de Microondas') es una organización sin ánimo de lucro creada en abril de 2002 por fabricantes y suministradores de equipos inalámbricos. WiMAX tiene hoy en día (agosto 2005) cerca de 70 miembros, entre los que se encuentran Intel, Nokia y Fujitsu.

El objetivo de WIMAX es promover el uso de las tecnologías IEEE 802.16a y ETSI HiperMAN y asegurar su interoperatividad. Estas tecnologías permiten crear redes inalámbricas metropolitanas de banda ancha.

Tanto el IEEE norteamericano como el ETSI europeo han estado trabajando en los últimos años en la definición de un estándar de red inalámbrica metropolitana. Los primeros resultados fueron la definición de dos protocolos punto-multipunto (IEEE 802.16 y ETSI HiperAccess) que operan a frecuencias superiores a 11 GHz. Estas frecuencias tienen el inconveniente de necesitar visibilidad directa, por lo que obstáculos, como edificios o árboles, limitan grandemente su aplicación. Por este motivo, ambas organizaciones han desarrollado nuevos estándares que operan en la banda de 2 a 11 GHz. El resultado son un par de protocolos, IEEE 802.16a y ETSI HiperMAN, que tienen la particularidad de poder interoperar entre sí.

Desde el punto de vista de la cobertura, una estación base típica WIMAX (802.16a/HiperMAN) tiene un alcance de hasta 50 kilómetros. Aunque la cobertura típica suele ser menor de 10 kilómetros. Por otro lado, desde el punto de vista del servicio, una estación base puede ofrecer servicio a más de 60 empresas (a 2Mbps) y cientos de hogares (a 256 Kbps) simultáneamente. Todo esto convierte a WIMAX en una tecnología de banda ancha alternativa a XDSL o el cable. De hecho, también se la conoce como WDSL (Wireless DSL, 'DSL inalámbrico').

Para garantizar la conectividad, aún en las peores condiciones, WiMAX considera la utilización de distintos tipos de modulaciones, pudiendo aumentar el alcance a costa de bajar la velocidad de conexión. Por otro lado, aunque actualmente se está trabajando a velocidades de hasta 72 Mbps, se espera poder aumentar esta velocidad en un futuro.

([www.wikipedia.org](http://www.wikipedia.org) agosto 2005)

## 1.6 REDES INALÁMBRICAS GLOBALES

Los sistemas inalámbricos de cobertura global que existen son los sistemas de telefonía móvil. Los primeros sistemas de telefonía móvil fueron sistemas analógicos con muy pocas prestaciones para transmitir datos. Hasta finales de los años ochenta no aparecieron los primeros sistemas digitales con posibilidades de transmitir datos. A estos sistemas se les ha conocido como sistemas de telefonía celular de segunda generación (2G). Éste es el caso de la tecnología europea GSM (Global System for Mobile Communications, 'Sistema Global para Comunicaciones Móviles') y de la norteamericana CDMA (Code Division Multiple Access, 'Acceso Múltiple por División de Código').

TECNOLOGÍA	DESCRIPCIÓN
AMPS	Advanced Mobile Phone System ( <i>Sistema de Telefonía Móvil Avanzada</i> ). Desarrollado por los laboratorios Bell en los años setenta. Su primer uso comercial no se produjo hasta 1983 en Estados Unidos. Opera en la banda de los 800 MHz.
C-Netz	Antiguo sistema de telefonía celular utilizado en Alemania y Austria. Opera en la banda de 450 MHz.
Comvik	Sistema lanzado en 1981 en Suecia por la empresa Comvik Network.
N-AMPS	Narrowband Advanced Mobile Phone System ( <i>Sistema de Telefonía Móvil de Banda Estrecha</i> ). Desarrollado por Motorola como paso intermedio entre la tecnología analógica y digital. Opera en la banda de 800 MHz y tiene tres veces más capacidad que AMPS.
NMT	Nordic Mobile Telephones ( <i>Teléfonos Móviles Nórdicos</i> ). Desarrollado por Ericsson y Nokia para operar en los países nórdicos. Este sistema lo instaló Telefónica en España a finales de los años ochenta. La primera versión trabajaba en la banda de 450 MHz. Posteriormente se desarrolló una versión en 900 MHz.
NTT	Nippon Telegraph and Telephone ( <i>Teléfonos y Telégrafos de Japón</i> ). Sistema de telefonía móvil analógica utilizado en Japón. Tuvo una nueva versión de mayor capacidad conocido como HICAP.
RC2000	Radiocom 2000. Sistema analógico francés lanzado en noviembre de 1985.
TACS	Total Access Communications System ( <i>Sistema de Comunicaciones de Acceso Total</i> ). Desarrollado por Motorola. Es un sistema similar a AMPS que fue utilizado por primera vez en el Reino Unido en 1985. En Japón se utilizó con el nombre JTAC. Opera en la banda de 900 MHz.

Tabla 1.2 Tecnologías celulares analógicas (1G) existentes en el mundo ([www.htmlWeb.net/redes/topologia/topologia\\_1.html](http://www.htmlWeb.net/redes/topologia/topologia_1.html) agosto 2005)

### 1.6.1 GSM

GSM es una tecnología estandarizado por el CEPT (Conference European Posts and Telecommunications, 'Conferencia de Correos y Telecomunicaciones Europeas') a finales de los años ochenta. Su comercialización se llevó a cabo en Europa durante los primeros años de la década de los noventa y rápidamente alcanzó una cobertura global con cientos de millones de usuarios. Hoy en día es el sistema 2G más extendido. GSM puede transmitir datos a 13 Kbps sin necesidad de utilizar módem. Para conectar un ordenador o PDA a un teléfono GSM sólo hace falta un cable adaptador y el software apropiado. Un modo especial de transmisión de datos que admite GSM es el envío y recepción de mensajes cortos de texto (hasta 160 caracteres) mediante el servicio SMS (Short Message Service, 'Servicio de Mensajes Cortos') desde el propio terminal de telefonía móvil. Estos mensajes pueden intercambiarse tanto con otros terminales móviles, como con terminales de telefonía fija e Internet.

*([www.htmlWeb.net/redes/topologia/topologia\\_1.html](http://www.htmlWeb.net/redes/topologia/topologia_1.html) agosto 2005)*

### 1.6.2 2,5G

Aunque los sistemas 2G tienen ciertas capacidades de transmisión de datos, fundamentalmente se trata de un sistema que da soporte a servicios de voz. Para ofrecer servicios de datos, se ha pensado en una nueva generación de redes celulares, la tercera generación o 3G. No obstante, mientras se desarrolla convenientemente la tecnología para poder ofrecer servicios 3G, se ha creado una ampliación de la tecnología 2G a la que se ha llamado 2,5G. Esta tecnología de transición añade nuevas capacidades de transmisión de datos a la infraestructura de red celular existente.

*([www.htmlWeb.net/redes/topologia/topologia\\_1.html](http://www.htmlWeb.net/redes/topologia/topologia_1.html) agosto 2005)*

TECNOLOGÍA	DESCRIPCIÓN
CDMA (IS-95)	Code Division Multiple Access ( <i>Acceso Múltiple por División de Código</i> ). Sistema digital desarrollado por Qualcomm. Utiliza las mismas frecuencias que el sistema AMPS y, de hecho, son sistemas compatibles.
CT-2 y CT-3	Cordless telephone ( <i>telefonía inalámbrica</i> ). Es la segunda y tercera versión del estándar de telefonía inalámbrica precursora de DECT.
D-AMPS (IS-54)	Digital AMPS ( <i>AMPS digital</i> ). Versión digital del estándar AMPS analógico. Emplea las mismas frecuencias que su antecesor analógico (800 MHz).
DCS 1800	Digital Cordless Standard ( <i>Estándar Inalámbrico Digital</i> ). Es una versión de GSM que opera en la banda de 1.800 MHz.
DECT	Digital European Cordless Standard ( <i>Estándar Inalámbrico Digital Europeo</i> ). Es una evolución de CT-3. Permite transmitir datos a 32 Kbps. Existen terminales que pueden funcionar indistintamente en DECT y GSM.
GSM	Global System for Mobile Communications ( <i>Sistema Global de Comunicaciones Móviles</i> ). Sistema digital europeo utilizado tanto en Europa como en el resto del mundo. Opera en la banda de 900 MHz.
PCS	Personal Communications Service ( <i>Servicio de Comunicaciones Personales</i> ). Es la versión de GSM utilizada en Estados Unidos. Opera en la banda de 1.900 MHz.
Inmarsat	International Maritime Satellite System ( <i>Sistema Internacional de Comunicaciones Marítimas por Satélite</i> ). Permite comunicaciones móviles desde cualquier parte del mundo gracias a los satélites geoestacionarios que componen el sistema.
PDC	Personal Digital Cellular ( <i>Celular Digital Personal</i> ). Es un estándar japonés que utiliza el sistema TDMA y funciona en las bandas de 800 y 1.500 MHz.
PHS	Personal Handy System ( <i>Sistema Personal Manejable</i> ). Sistema japonés que permite transmitir datos a alta velocidad.
TDMA	Time Division Multiple Access ( <i>Acceso Múltiple por División en el Tiempo</i> ). Tecnología en el que se han basado los primeros sistemas digitales de telefonía: DAMP y GSM.

Tabla 1.3 Algunas Tecnologías celulares digitales (2G) existentes en el mundo. ([www.htmlWeb.net/redes/topologia/topologia\\_1.html](http://www.htmlWeb.net/redes/topologia/topologia_1.html), agosto 2005)

Existen distintas tecnologías 2,5G:

- **GPRS** (General Packet Radio Service, Servicio General de Radio Paquetes). Esta tecnología añade a las redes GSM datos la posibilidad de transmitir paquetes de datos. Utiliza la misma infraestructura GSM para enviar la voz y añade una infraestructura de red que permite utilizar un conjunto de protocolos para la transmisión de paquetes de datos. La tecnología GPRS permite transmitir datos a velocidades de hasta 171 Kbps. Esta tecnología se ha implementado

fundamentalmente en Europa, aunque se está expandiendo a aquellas otras regiones con sistemas GSM.

- **EDGE** (Enhanced Data Rates for GSM Evolution, 'Velocidades Mejoradas de Datos para la Evolución de GSM'). Se trata de una variación de la tecnología GPRS que permite alcanzar velocidades de transmisión de datos de hasta 384 Kbps. Para conseguir esto, se utiliza parte del canal de voz.
- **IS-95B**. Esta tecnología añade la capacidad de transmitir datos a 64 Kbps a las redes CDMA (IS-95A). Esta tecnología se ha implementado principalmente en Corea, Japón y Norteamérica.
- **IMode**. Esta tecnología desarrollada en Japón es complementaria de las redes CDMA. Permite entregar correo electrónico y navegar por los servicios ofrecidos por los proveedores de información. La velocidad de transmisión es de 9,6 Kbps.

([www.htmlWeb.net/redes/topologia/topologia\\_1.html](http://www.htmlWeb.net/redes/topologia/topologia_1.html), agosto 2005)

TECNOLOGÍA	DESCRIPCIÓN
WCDMA	Wideband CDMA, 'CDMA de Banda Ancha', desarrollada en Japón por NTT DoCoMo. Es la base tecnológica en la que sustentan las tecnologías 3G asociadas a IMT2000.
UMTS	Universal Mobile Telecommunications System, 'Sistema Universal de Telecomunicaciones Móviles'. Es el estándar europeo creado como evolución de la arquitectura GSM. Basada en WCDMA, ofrece servicios de voz, fax, mensajes multimedia, así como servicios de datos a velocidades de hasta 2 Mbps.
CDMA-2000	Evolución del estándar americano CDMAOne. Las empresas coreanas SK Telecom, LG Telecom y KT Freetel la convirtieron en la primera tecnología 3G que ve el mercado al comercializarla a finales del año 2000. Esta primera versión, CDMA-2000-1x, permite transmitir datos a 300 Kbps.
TD-SCDMA	Time Division-Synchronous Code Division Multiple Access, 'División de Tiempo-Acceso Múltiple Síncrono por División de Código'. Desarrollada por Siemens y CATT, es una combinación de las técnicas TDMA y CDMA. Su mayor ventaja es que permite interoperar con las redes 2G.

Tabla 1.4 Algunas Tecnologías celulares 3G existentes en el mundo.  
([www.htmlWeb.net/redes/topologia/topologia\\_1.html](http://www.htmlWeb.net/redes/topologia/topologia_1.html), agosto 2005)

### 1.6.3 CDMA

CDMA es una tecnología desarrollada por la empresa Qualcomm. El gran mérito de esta tecnología es que supone una nueva forma de establecer comunicaciones inalámbricas multiusuario con un aprovechamiento de la capacidad seis veces mejor que TDMA. CDMA estuvo hasta en 1988, aunque, posteriormente, con la ayuda de AT&T, Motorola y otros fabricantes, se desarrolló una nueva versión dual (analógica y digital) a la que se llamó IS-95, y que ha sido la que se ha instalado en distintos países. La primera implantación de la tecnología CDMA tuvo lugar en Hong Kong en 1995. CDMA también ofrece el servicio SMS de mensajes cortos. ([www.wikipedia.org](http://www.wikipedia.org) agosto 2005)

### 1.6.4 3G

En el paso de las redes celulares analógicas a las digitales, cada una de las tres regiones importantes desde el punto de vista del desarrollo tecnológico de la tecnología celular (Europa, Norteamérica y Asia) tomaron caminos distintos. De hecho, incluso dentro de cada región ha habido sus variaciones. En cualquier caso, es evidente que lo ideal sería que la tercera generación (3G) se afrontara con el objetivo de conseguir un sistema global común. No obstante, conseguir esto es extremadamente complicado debido a los distintos intereses económicos, políticos y regulatorios que tiene cada parte.

Se puede decir que la tecnología celular de tercera generación comenzó en 1985 cuando la UIT (Unión Internacional de Telecomunicaciones, conocida en inglés por ITU, International Telecommunications Union) anunció su iniciativa de crear un nuevo sistema de comunicaciones móviles al que llamó FPLMTS (Future Public Land Mobile Telecommunications System, 'Futuro Sistema Público de Telecomunicaciones Móviles Terrestres'). Esta iniciativa se concretó en 1996 con la creación de IMT2000 (International Mobile Communications, 'Comunicaciones Móviles Internacionales'). El número 2000 se le puso porque se esperaba que la nueva tecnología estuviera lista para

la primera década del nuevo milenio y porque la banda de frecuencia asignada era 2GHz (2000 MHz).

El objetivo de W2000 es definir un marco dentro del cual puedan coexistir distintas tecnologías 3G, asegurándose la interoperatividad de servicios (roaming, portabilidad, multimedia, etc.). De hecho, IMT2000 pretende ir más allá de un acuerdo entre tecnologías celulares. La visión es disponer de un sistema universal de comunicaciones que cubra todo tipo de redes: con cables y sin cables, terrestres y satelitales.



*Figura 1.6 Teléfonos de tercera generación  
([www.wikipedia.org](http://www.wikipedia.org) agosto 2005)*

Después de muchas luchas entre todos los grupos de intereses, finalmente se llegó a un acuerdo de tecnología única en marzo de 1999. Esta tecnología se basa en una base única, conocida como WCDMA (Wideband CDMA, 'CDMA de Banda Ancha', desarrollada en Japón por NTT DoCoMo), sobre la que se desarrollan tres modos opcionales:

- **UMTS** (Universal Mobile Telecommunications System, 'Sistema Universal de Telecomunicaciones Móviles'). Es el estándar europeo creado como evolución de la arquitectura GSM MAP basada en WCDMA. Ofrece servicios de voz, fax, mensajes multimedia, así como servicios de datos a velocidades de hasta 2 Mbps.

- **CDMA-2000.** Es una evolución del estándar americano CDMAOne. La particularidad de esta tecnología es que, a finales del año 2000, se convirtió en la primera tecnología 3G que ve el mercado. Los primeros en comercializarla fueron las empresas coreanas SK Telecom, LG Telecom y KT Freetel. Esta primera versión, CDMA-2000-1 x, permite transmitir datos a 300 Kbps.
- **TD-SCDMA** (Time Division-Synchronous Code Division Multiple Access, 'División de Tiempo-Acceso Múltiple Síncrono por División de Código'). Es una combinación de las técnicas TDMA y CDMA. Esta tecnología ha sido desarrollada por Siemens y CATT, academia china para la tecnología de las telecomunicaciones. Su mayor ventaja es que permite interoperar con las redes 2G.

Desde el punto de vista de la transmisión de datos, la tercera generación define tres modalidades de transmisión: 144 Kbps para usuarios de mucha movilidad, 384 Kbps para usuarios con movilidad limitada (de a pie) y 2 Mbps para usuarios sin movilidad.

([www.wikipedia.org](http://www.wikipedia.org), agosto 2005)

CARACTERÍSTICA	UMTS	TD-SCDMA	CDMA 2000
Método de acceso	CDMA	TDMA/CDMA	CDMA
Ancho de banda del canal	5 MHz	5 MHz	3x1,25 MHz
Velocidad de chip	3,84 Mchip/s		
Longitud de trama	10 mseg	10 mseg	20 mseg
Factor de expansión	4-512	1-16	4-256
Modulación	QPSK		
Codificación del canal	Convolutional, turbo codificado		

Tabla 1.5 Comparación de las Tecnologías 3G  
([www.wikipedia.org](http://www.wikipedia.org), agosto 2005)

## 1.7 LA LUCHA TECNOLÓGICA

Como hemos visto anteriormente, existen muchas tecnologías distintas de comunicaciones inalámbricas. Muchas de estas tecnologías son complementarias (éste es el caso de Bluetooth, Wi-Fi o UMTS), pero otras dan respuesta a una misma necesidad y, por tanto, compiten entre ellas por ser las preferidas del mercado. En el caso de las tecnologías de redes de área local inalámbricas, la competencia se centra en Wi-Fi, HiperLAN, HomeRF y las nuevas versiones tecnológicas de cada una de ellas.

Para que una tecnología esté lista para ser adoptada por el mercado, es necesario que tenga suficientemente desarrolladas estas cinco características:

- Normalización
- Regulación
- Tecnología
- Servicios
- Precios

En el caso de las redes locales inalámbricas, la tecnología que tiene mejor posicionamiento en estos cinco puntos es Wi-Fi. Sobre todo, tiene el mejor posicionamiento en el apartado precios, lo cual está resultando determinante para que el mercado acepte esta tecnología frente a sus competidores.

Claro que el mercado de las comunicaciones inalámbricas de datos se acaba de despertar ahora, por lo que Wi-Fi sólo lleva ganada la primera batalla de lo que, seguro, será una dura guerra.

(<http://www.redaragon.com/informatica/wireless/redwireless.asp>, agosto 2005)

Característica	Wi-Fi	HiperLAN	HomeRF
Normalización	<i>alto</i>	<i>alto</i>	<i>bajo</i>
Regulación	<i>alto</i>	<i>medio</i>	<i>alto</i>
Tecnología	<i>medio</i>	<i>alto</i>	<i>alto</i>
Servicios	<i>bajo</i>	<i>alto</i>	<i>medio</i>
Precios	<i>alto</i>	<i>bajo</i>	<i>bajo</i>

Tabla 1.6 Nivel de aceptación al mercado de las distintas de redes locales inalámbricas. (<http://www.redaragon.com/informatica/wireless/redwireless.asp>, agosto 2005)

## 1.8 REGULACIÓN

Uno de los aspectos más importantes para el desarrollo de una tecnología es la regulación. En cada país existe un organismo que se encarga de regular el uso del espectro radioeléctrico. Si dos dispositivos intentasen utilizar la misma frecuencia al mismo tiempo y en el mismo lugar, ninguno de los dos funcionaría. Esto quiere decir que, para que funcionen los equipos de radio, es necesario regular el uso de las bandas de frecuencias. El espectro radioeléctrico es único y se considera un bien social.

El regulador del espectro radioeléctrico se asegura que cada servicio que utiliza dicho espectro (televisión, radio, policía, ambulancia, telefonía móvil, etc.) lo pueda hacer con las mejores garantías y sin que existan interferencias entre ellos. Por este motivo, la mayoría de las bandas de frecuencia no pueden ser utilizadas a menos que se disponga de una licencia (éste es el caso de la telefonía móvil, las emisoras de radio o de televisión, por ejemplo). Sin embargo, existen bandas de frecuencias para las que no se necesita licencia de uso. Éste es el caso de la banda de 2,4 GHz y de 5 GHz.

El hecho de que no se necesite licencia para el uso de estas frecuencias ha favorecido tremendamente la implantación de la tecnología inalámbrica. No obstante, no se está exento de problemas ya que estas bandas de frecuencias son utilizadas no sólo por la tecnología de redes locales inalámbricas, sino que tecnologías como Dect o Bluetooth utilizan también los 2,4 GHz pudiendo producirse problemas de interferencias.

Aunque no se necesite licencia de uso, los equipos que funcionan en la banda de 2,4 GHz si deben cumplir una serie de características. Una de estas características es la potencia máxima de emisión (1.000 mW). Otras de las características hacen referencia a las técnicas de modulación y retransmisión utilizada.

(<http://www.redaragon.com/informatica/wireless/redwireless.asp,agosto> 2005)

ESTÁNDAR	ÁREA	FRECUENCIA	POTENCIA MÁXIMA
802.11, 11b y 11g	Norteamérica	2,4-2,4835 GHz	1.000 mW
	Europa	2,4-2,4835 GHz	100 mW
	Francia	2,4465-2,4835 GHz	100 mW
	España	2,445-2,475 GHz	100 mW
	Japón	2,471-2,497 GHz	10 mW/MHz
802.11a	Norteamérica	5,15-5,25 GHz	50 mW
		5,25-5,35 GHz	250 mW
		5,725-5,825 GHz	1.000 mW
HiperLAN/2	Europa	5,15-5,25 GHz	200 mW
		5,25-5,35 GHz	200 mW
		5,47-5,725 GHz	1.000 mW
HiSWAN	Japón	5,15-5,35 GHz	200 mW

Tabla 1.7 distintas regulaciones de las bandas de 2.4 y 5 GHz  
(<http://www.redaragon.com/informatica/wireless/redwireless.asp,agosto> 2005)

## CAPÍTULO 2

### PROTOCOLOS Y ESTÁNDARES UTILIZADOS EN Wi-Fi

#### 2.1 PROTOCOLOS

Cuando una persona pretende comunicarse con otra, lo primero que hace es llamar su atención ("perdone", "oye, Paco", etc.); luego, comprueba que la otra persona le atiende, para, a continuación, transmitirle la información que desea. Durante la comunicación, lo normal es que la persona que habla se asegure de que la que escucha está entendiendo lo que le dice. Para ello, espera recibir gestos de asentimiento o palabras de asimilación. Si el que habla no recibe estos mensajes, interpretará que lo que dice no es entendido y lo volverá a repetir. Finalmente, mediante mensajes preestablecidos, se da por concluida la comunicación ("adiós", "hasta luego", etc.).

Pues bien, la transmisión de datos entre ordenadores también requiere llevar a cabo estos mismos procedimientos. En cualquier comunicación, bien sea entre personas o entre máquinas, siempre hacen falta una serie de normas que regulen dicho proceso. En el caso de las comunicaciones entre personas, las normas las establece la sociedad y son apocadas por cada persona de acuerdo con la educación que haya recibido; en el caso de las máquinas, las normas las establecen los organismos de normalización (IEEE, ETSI, UIT, etc.) y son aplicadas por los ordenadores de acuerdo con el protocolo o conjunto de protocolos que se está utilizando.

Obviamente, aunque existen grandes similitudes de procedimientos, la diferencia fundamental entre personas y máquinas es que las personas están dotadas de inteligencia y pueden adaptarse fácilmente a situaciones imprevistas, además de tener inventiva y capacidad de resolver situaciones nuevas. Los ordenadores, sin embargo, deben tener

protocolos muy estrictos, que tengan previstos todos los posibles casos que se puedan presentar en una comunicación, sin dejar nada al azar.

En definitiva, un protocolo no es más que un conjunto de reglas que emplean dos equipos informáticos para dialogar entre sí, de forma que puedan establecer y mantener una comunicación sin errores.

Para que los protocolos puedan llevar a cabo sus objetivos, necesitan añadir ciertos datos de control a la información original a transmitir. Estos datos adicionales son incluidos por el terminal emisor y suprimidos por el terminal receptor antes de entregar la información al destino.

En un principio, cada fabricante establecía los procedimientos de comunicación de sus propios equipos, siendo casi imposible conectar equipos de fabricantes distintos. Con la expansión de la informática, se hizo evidente que era necesario disponer de protocolos que permitiesen la interconexión de equipos independientemente de quién los fabricase. Con esta idea, a lo largo de los años han ido apareciendo distintos protocolos normalizados, cada uno de ellos dedicados a distintas aplicaciones o cubriendo distintas necesidades. Muchos de estos protocolos normalizados han surgido a partir de los protocolos desarrollados por empresas u organismos concretos (caso de TCP/IP para interconexión de redes Internet), mientras que otros han sido desarrollados por los organismos de normalización (Wi-Fi).

De forma práctica, los protocolos de comunicación son unos programas que se instalan tanto en el terminal origen, como en el destino de la comunicación. Parte de estos programas residen en el propio hardware del equipo, otra parte puede venir incorporada en el sistema operativo y la restante debe ser instalada por el usuario en el momento de configurar el equipo. ([www.sc.ehu.es/scWebci/WIFI/wifi-cc-tt.html](http://www.sc.ehu.es/scWebci/WIFI/wifi-cc-tt.html), septiembre 2005)

### **2.1.1 Protocolos de IEEE 802.11**

#### 802.11

La versión original del estándar IEEE 802.11 publicada en 1997 especifica dos velocidades de transmisión teóricas de 1 y 2 mega bit por segundo (Mbit/s) que se transmiten por señales infrarrojas (IR) en la banda ISM a 2,4 GHz. IR sigue siendo parte del estándar, pero no hay implementaciones disponibles.

El estándar original también define el protocolo CSMA/CA (Multiple acceso por detección de portadora evitando colisiones) como método de acceso. Una parte importante de la velocidad de transmisión teórica se utiliza en las necesidades de esta codificación para mejorar la calidad de la transmisión bajo condiciones ambientales diversas.

Una de las mayores debilidades de este estándar fue que dejaba mucha libertad de implementación a los proveedores de equipos, lo cual se tradujo en dificultades de interoperabilidad entre equipos de diferentes marcas. Estas y otras debilidades fueron corregidas en el estándar 802.11b, que fue el primero de esta familia en alcanzar amplia aceptación entre los consumidores.

#### 802.11b

La revisión 802.11b del estándar original fue ratificada en 1999. 802.11b tiene una velocidad máxima de transmisión de 11 Mbit/s y utiliza el mismo método de acceso CSMA/CA definido en el estándar original. Debido al espacio ocupado por la codificación del protocolo CSMA/CA, en la práctica, la velocidad máxima de transmisión con este estándar es de aproximadamente 5.9 Mbit/s sobre TCP y 7.1 Mbit/s sobre UDP.

#### 802.11a

La revisión 802.11a al estándar original fue ratificada en 1999. El estándar 802.11a utiliza el mismo juego de protocolos de base que el estándar original, opera en la banda

de 5 GHz y utiliza 52 subportadoras orthogonal frequency-division multiplexing (OFDM) con una velocidad máxima de 54 Mbit/s, lo que lo hace un estándar práctico para redes inalámbricas con velocidades reales de aproximadamente 20 Mbit/s. La velocidad de datos se reduce a 48, 36, 24, 18, 12, 9 o 6 Mbit/s en caso necesario. 802.11a tiene 12 canales no solapados, 8 para red inalámbrica y 4 para conexiones punto a punto. No puede interoperar con equipos del estándar 802.11b, excepto si se dispone de equipos que implementen ambos estándares.

Dado que la banda de 2,4 GHz tiene gran uso, el utilizar la banda de 5 GHz representa una ventaja del estándar 802.11a, dado que se presentan menos interferencias. Sin embargo, la utilización de esta banda también tiene sus desventajas, dado que restringe el uso de los equipos 802.11a a únicamente puntos en línea de vista, con lo que se hace necesario la instalación de un mayor número de puntos de acceso; Esto significa también que los equipos que trabajan con este estándar no pueden penetrar tan lejos como los del estándar 802.11b dado que sus ondas son más fácilmente absorbidas.

#### 802.11g

En Junio de 2003, se ratificó un tercer estándar de modulación: 802.11g. Éste utiliza la banda de 2.4 GHz (al igual que el estándar 802.11b) pero opera a una velocidad teórica máxima de 54 Mbit/s, o cerca de 24.7 Mbit/s de velocidad real de transferencia, similar a la del estándar 802.11a. Es compatible con el estándar b y utiliza las mismas frecuencias. Buena parte del proceso de diseño del estándar lo tomó el hacer compatibles los dos estándares. Sin embargo, en redes bajo el estándar b la presencia de nodos bajo el estándar g reduce significativamente la velocidad de transmisión.

Los equipos que trabajan bajo el estándar 802.11g llegaron al mercado muy rápidamente, incluso antes de su ratificación. Esto se debió en parte a que para construir equipos bajo este nuevo estándar se podían adaptar los ya diseñados para el estándar b.

## 802.11n

En enero de 2004, la IEEE anunció la formación de un grupo de trabajo 802.11 para desarrollar una nueva revisión del estándar 802.11. la velocidad real de transmisión podría llegar a los 500 Mbps (lo que significa que las velocidades teóricas de transmisión serían aún mayores), y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y cerca de 40 veces más rápida que una red bajo el estándar 802.11b. También se espera que el alcance de operación de las redes aumente con este nuevo estándar. Existen también otras propuestas alternativas que podrán ser consideradas y se espera que el estándar sea completado hacia finales de 2006.

*([http://es.wikipedia.org/wiki/IEEE\\_802.11](http://es.wikipedia.org/wiki/IEEE_802.11), septiembre 2005)*

## 2.2 El modelo OSI

Una característica común a todas las comunicaciones actuales de ordenadores es el hecho de que todas ellas estructuran el proceso de comunicación en distintos niveles o capas. Cada capa se encarga de realizar una tarea distinta y perfectamente coordinada con el resto de capas. Por ejemplo, hay capas que se encargan de poner en contacto dos terminales (nivel de enlace), otras se encargan de detectar posibles bloqueos o fallos en la línea (nivel de transporte) y otras, de identificar al terminal flamante, pedir las claves de acceso, etc. (nivel de sesión).

La ventaja de hacer una división por capas es que cada una de ellas puede ser normalizada de forma independiente. No obstante, finalmente, la comunicación se lleva a cabo gracias al buen funcionamiento de todas las capas.

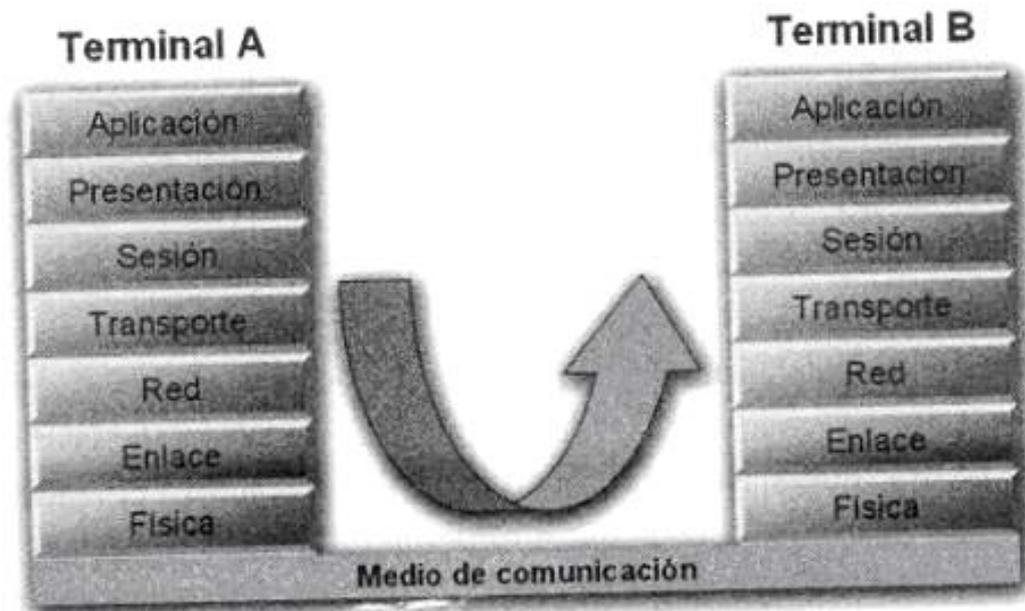
La Organización Internacional de Normalización, ISO (International Standards Organization), propuso un modelo de referencia que permite estructurar las comunicaciones en siete capas. A este modelo lo llamó OSI (Open Systems Interconnection, 'Interconexión de Sistemas Abiertos').

Las capas del modelo OSI son las siguientes:

- **Capa Física.** Esta capa define las propiedades físicas de los componentes (frecuencias de radio utilizadas, cómo se transmiten las señales, etc.).
- **Capa de enlace.** Esta capa define cómo se organizan los datos que se transmiten, cómo se forman los grupos de datos (paquetes, tramas, etc.) y cómo se asegura que los datos llegan al destino sin errores.
- **Capa de red.** Esta capa define cómo organizar las cosas para que distintas comunicaciones puedan hacer uso de una infraestructura común, una red. Por ejemplo, aquí están definidos cómo se identifican los terminales (numeración) o cómo se enrutan los datos.
- **Capa de transporte.** Esta capa define las características de la entrega de los datos.
- **Capa de sesión.** Aquí se describe cómo se agrupan los datos relacionados con una misma función.
- **Capa de presentación.** Nos define cómo es representada la información transmitida.
- **Capa de aplicación.** Define cómo interactúan los datos con las aplicaciones específicas.

Los modelos como OSI pretenden definir todos y cada uno de los factores que intervienen en una comunicación de una red abierta; sin embargo, no todas las comunicaciones de datos son iguales; por ejemplo, existen comunicaciones en las que no hace falta definir una determinada capa (por ejemplo, en las comunicaciones directas entre dos ordenadores no es necesario que exista un nivel de red). En cualquier caso, de todos los procedimientos definidos por OSI, los que siempre están presentes en cualquier tipo de comunicación son aquellos que están incluidos dentro de las capas físicas y de enlace.

*([www.geocities.com/txmetsb/el\\_modelo\\_de\\_referencia\\_osi.htm](http://www.geocities.com/txmetsb/el_modelo_de_referencia_osi.htm), septiembre 2005)*



*Figura 2.1 Esquema de comunicación con el modelo OSI.  
([www.geocities.com/txmetsb/el\\_modelo\\_de\\_referencia\\_osi.htm](http://www.geocities.com/txmetsb/el_modelo_de_referencia_osi.htm), septiembre 2005.)*

### **2.3 LA EVOLUCIÓN DE IEEE 802**

Uno de los factores más importantes para que una tecnología sea aceptada es la normalización, el hecho de que la tecnología esté perfectamente definida para que los distintos fabricantes de equipos, componentes o software puedan hacer su trabajo con la seguridad de ser aceptados por el mercado. El organismo de normalización que más ha avanzado en la definición de normas de redes de área local es el IEEE (Institute of Electrical and Electronics Engineers, 'Instituto de Ingenieros Eléctricos y Electrónicos').

El IEEE empezó a tratar el tema de la normalización de redes locales y metropolitanas en 1980. Para ello creó un grupo de trabajo al que llamó 802. La norma IEEE 802 fue aprobada en 1990. Esta norma sentaba las bases para el establecimiento de redes de área local y redes metropolitanas basadas en el modelo de interconexión de sistemas abiertos conocido como OSI (Open Systems Interconnection).

El modelo OSI se basa en estructurar el proceso de comunicación en siete partes independientes a las que llama capas (física, enlace, red, transporte, sesión, presentación y aplicación). La mayoría de las redes públicas y privadas de comunicaciones utilizan el modelo OSI como modelo de referencia. ([http://es.wikipedia.org/wiki/IEEE\\_802.11](http://es.wikipedia.org/wiki/IEEE_802.11), septiembre 2005)

### 2.3.1 Las redes de cable

De las siete capas del sistema OSI, la norma IEEE 802 define exclusivamente los temas relacionados con las dos primeras capas: las capas física y de enlace. Uno de los temas que se definen en estas dos capas son las técnicas de acceso. Las técnicas de acceso definen cómo cada terminal puede hacer uso del medio de comunicación común. Las primeras técnicas de acceso que definió el IEEE se pensaron para las redes de cable. De esta forma, empezaron a surgir los primeros miembros de la familia 802:

- **IEEE 802.3** define una tecnología conocida como CSMA/CD (Carrier Sense Multiple Access with Collision Detection, 'Acceso Múltiple por Detección de Portadora con Detección de Colisión'). A esta norma se la conoce más comúnmente por el nombre Ethernet. No obstante, aunque ambas están basadas en CSMA/CD, IEEE 802.3 es un estándar, mientras que Ethernet es un protocolo inventado por Bob Metcalfe y comercializado por Xerox en 1973.
- **IEEE 802.4** define una tecnología conocida como token bus o red de área local en bus con paso de testigo.
- **IEEE 802.5** define una tecnología conocida como token ring o red de área local en anillo con paso de testigo.

([http://es.wikipedia.org/wiki/IEEE\\_802.11](http://es.wikipedia.org/wiki/IEEE_802.11), septiembre 2005)



*Figura 2.2 Redes de cable*  
([http://es.wikipedia.org/wiki/IEEE\\_802.11](http://es.wikipedia.org/wiki/IEEE_802.11), septiembre 2005)

### 2.3.2 Las redes inalámbricas

En 1997 el IEEE añadió un nuevo miembro a la familia 802 que se ocupa de definir las redes de área local inalámbricas, Este nuevo miembro es el 802.11.

La primera norma 802.11 utilizaba infrarrojos como medio de transmisión. Esta norma nunca tuvo una buena aceptación en el mercado. Posteriormente, salieron otras dos normas 802.11 basadas en el uso de radiofrecuencia en la banda de 2,4 GHz. Ambas se diferencian en el método de transmisión de radio utilizado. Una utiliza el sistema FHSS (Frequency Hopping Spread Spectrum, 'Difusión por Salto de Frecuencia') y la otra, el sistema DSSS (Direct Sequence Spread Spectrum, 'Difusión por Secuencia Directa').

ESTÁNDAR	GRUPOS DE TRABAJO	ESTADO
802.0	Comité ejecutivo patrocinador, SEC	
802.1	Interfaces de red de área local de alto nivel ( <i>High-Level LAN Interfaces</i> )	
802.2	Control lógico del enlace, LLC ( <i>Logical Link Control</i> )	Inactivo
802.3	CSMA/CD (Ethernet)	
802.4	Token Bus	Inactivo
802.5	Token Ring	Inactivo
802.6	MAN (red de área metropolitana)	Inactivo
802.7	Emisión (Grupo técnico de recomendación)	Inactivo
802.8	Fibra óptica (Grupo técnico de recomendación)	Disuelto
802.9	Redes de área local isosincronas	Inactivo
802.10	Seguridad de interoperación de redes de área local	Inactivo
802.11	Redes de área local inalámbricas	
802.12	Prioridad de demanda	Inactivo
802.14	Red de cable de comunicaciones de banda ancha	Disuelto
802.15	Redes personales inalámbricas, WPAN ( <i>Wireless Personal Area Network</i> )	
802.16	Acceso inalámbrico de banda ancha, BWA ( <i>Broadband Wireless Access</i> )	

*Tabla 2.1 Grupos de trabajo del comité de normalización IEEE 802  
([http://es.wikipedia.org/wiki/IEEE\\_802.11](http://es.wikipedia.org/wiki/IEEE_802.11) ,septiembre 2005)*

1

es que trabajaban a velocidades de 1 y 2 Mbps. Esto, unido al alto coste inicial de los equipos, hizo que la tecnología inalámbrica no se desarrollase hasta 1999. En ese año aparecieron semiconductores de tecnología de radio de 2,4 GHz mucho más baratos. Por otro lado, aparecieron tres nuevas versiones de la norma 802.11:

- IEEE 802.11 b, que subía la velocidad de transmisión a los 11 Mbps. Por este motivo se la conoció también como 802.11 HR (High Rate, Alta Velocidad').
- IEEE 802.11 a. Esta norma se diferencia de 802.11 b en el hecho de que no utiliza la banda de los 2,4 GHz, sino la de los 5 GHz y que utiliza una técnica de transmisión conocida como OFDM (Orthogonal Frequency Division Multiplexing, 'Multiplexación Ortogonal por División de Frecuencia'). La gran ventaja es que se consiguen velocidades de 54 Mbps; llegándose a alcanzar los 72 y 108 Mbps con versiones propietarias de esta tecnología (p.e. Netgear). El

mayor inconveniente es que la tecnología de semiconductores para 5 GHz no está suficientemente desarrollada todavía.

- IEEE 802.11g. Esta norma surgió en el año 2001 con la idea de aumentar la velocidad sin renunciar a las ventajas de la banda de los 2,4 GHz. Esta norma permite transmitir datos a 54 Mbps. En cualquier caso, existen versiones propietarias de esta tecnología que llega a los 100 Mbps (p.e. US Robotics).

ESTÁNDAR	GRUPOS DE TRABAJO	ESTADO
802.11 (1997)	Especificaciones de la capa física y MAC de las redes de área local inalámbricas (infrarrojo y radio 2,4 GHz)	Completo
802.11a (1999)	Especificaciones de la capa física y MAC de las redes de área local inalámbricas (radio 5 GHz)	Completo
802.11b (1999)	Especificaciones de la capa física y MAC de las redes de área local inalámbricas de rango de velocidad de 5,5 a 11 Mbps (radio 2,4 GHz)	Completo
802.11c	Pasarela MAC entre redes	Completo
802.11e	Calidad de servicio para aplicaciones avanzadas (voz, vídeo, etc.)	Activo
802.11f (2000)	Interoperatividad entre puntos de acceso de distintos fabricantes ( <i>Interaccess Point Protocol, IAPP</i> )	Activo
802.11g (2002)	Especificaciones para redes inalámbricas de alta velocidad (54 Mbps) en la banda de 2,4 GHz	Activo
802.11h	Mejoras para la selección dinámica de canal y control de potencia de transmisión	Activo
802.11i	Mejoras para seguridad y autenticación	Activo
5GSG	Globalización de los 5 GHz Grupo de estudio junto con ETSI/BRAN ( <i>European Telecommunications Standards Institute/Broadband Radio Area Network</i> , 'Instituto Europeo de Normalización en Telecomunicaciones/Redes Vía Radio de Banda Ancha') y MMAC ( <i>Mobile Multimedia Access Communication</i> , 'Comunicaciones Multimedia de Acceso Móvil') de Japón para promover la interoperatividad entre 802.11a, ETSI HiperLAN/2 y MMAC	Activo

*Tabla 2.2 Grupos de trabajo y de estudio relacionados IEEE 802.11  
([http://es.wikipedia.org/wiki/IEEE\\_802.11](http://es.wikipedia.org/wiki/IEEE_802.11) ,septiembre 2005)*

En el interés de disponer de unos estándares inalámbricos lo antes posible, al desarrollar sus normas, el IEEE no se preocupó por considerar determinadas características (como la calidad de servicio, seguridad, utilización del espectro, etc.) que hubiesen producido un estándar más robusto. Para resolver este problema, el IEEE ha creado posteriormente unos grupos de trabajo para desarrollar estándares que resuelvan estos problemas y que puedan ser añadidos fácilmente al protocolo principal. Estos grupos son los siguientes:

- IEEE 802.11 e (Calidad de servicio). Este grupo trabaja en los aspectos relacionados con la calidad de servicio (QoS o Quality of Services, en inglés). En el mundo de las redes de datos, calidad de servicio significa poder dar más prioridad de transmisión a unos paquetes de datos que a otros, dependiendo de la naturaleza de la información (voz, video, imágenes, etc.). Por ejemplo, la información de voz necesita ser transmitida en tiempo real, mientras que la información de datos originada por una transferencia de archivo da igual que llegue medio segundo antes o después.
- IEEE 802.11b (Gestión del espectro). Este grupo de trabajo pretende conseguir una mejora de la norma 802.11 en cuanto a la gestión del espectro radioeléctrico. Este punto es una de las desventajas que tiene IEEE 802.11 la frente a su competidor europeo HiperLAN/2 (que también opera en la banda de 5 GHz).
- IEEE 802.11i (Seguridad). El sistema de seguridad que utiliza 802.11 está basado en el sistema WEP. Este sistema ha sido fuertemente criticado debido a su debilidad. Este grupo de trabajo pretende sacar un nuevo sistema mucho más seguro que sustituya a WEP. El sistema sobre el que se está trabajando se conoce como TKIP (Temporal Key Integrity Protocol, 'Protocolo de Integridad de Clave Temporal').

*([http://es.wikipedia.org/wiki/IEEE\\_802.11](http://es.wikipedia.org/wiki/IEEE_802.11), septiembre 2005)*

### **2.3.3 Las capas de IEEE 802**

La norma IEEE 802 define exclusivamente los temas relacionados con las dos primeras capas del sistema OSI: las capas física y la de enlace. De hecho, a la capa de enlace la divide en dos, por lo que el resultado son tres capas:

- **PHY** (Physical Layer, 'Capa Física') es la capa que se ocupa de definir los métodos por los que se difunde la señal.

- **MAC** (Medium Access Control, 'Control de Acceso al Medio') es la capa que se ocupa del control de acceso al medio físico. En el caso de Wi-Fi el medio físico es el espectro radioeléctrico. La capa MAC es un conjunto de protocolos que controlan cómo los distintos dispositivos comparten el uso de este espectro radioeléctrico.
- **LLC** (Logical Link Control) es la capa que se ocupa del control del enlace lógico. Define cómo pueden acceder múltiples usuarios a la capa MAC.

([http://es.wikipedia.org/wiki/IEEE\\_802.11](http://es.wikipedia.org/wiki/IEEE_802.11), septiembre 2005)

MODELO OSI		PROTOS	PROTOS
7	Aplicación	IP	HTTP, FTP, SMTP
6	Presentación		DNS, LDAP
5	Sesión		
4	Transporte		UDP, TCP
3	Red		ICMP, RSVP
2	Enlace	IEEE 802	LLC, MAC
1	Físico		Físico

Tabla 2.3 Relación de los protocolos de red local.

([http://es.wikipedia.org/wiki/IEEE\\_802.11](http://es.wikipedia.org/wiki/IEEE_802.11), septiembre 2005)

## 2.4 LA CAPA FÍSICA

Como hemos visto, la capa física se ocupa de definir los métodos por los que se difunde la señal. Para hacer esto, la capa física de IEEE 802,11 se divide en dos subcapas: lo que se conoce como PLCP (Physical Layer Convergence Procedure, 'Procedimiento de Convergencia de la Capa Física') y PMD (Physical Medium Dependent, 'Dependiente del Medio Físico'). PLCP se encarga de convertir los datos a un formato compatible con el medio físico. Por ejemplo, este formato es distinto si se trata de un medio físico de infrarrojos o de radio, mientras que PMD es el que se encarga de la difusión de la serial.

Por cierto, aunque las especificaciones originales de IEEE 802.11 contemplan la opción de utilizar infrarrojos como medio de transmisión, no obstante, nunca ha llegado a

desarrollarse este sistema debido principalmente al corto alcance que ofrece y a que no es utilizable en el exterior debido a las interferencias producidas por agentes naturales como la lluvia o la niebla. ([http://es.wikipedia.org/wiki/IEEE\\_802.11](http://es.wikipedia.org/wiki/IEEE_802.11) ,septiembre 2005)

### **2.4.1 Espectro expandido**

En cuanto a la utilización del medio radioeléctrico, la tecnología básica en la que se basa el funcionamiento de los sistemas inalámbricos es el sistema conocido como espectro expandido (spread spectrum en inglés). Este sistema consiste en que el ancho de banda real utilizado en la transmisión es superior al estrictamente necesario para la transmisión de la información. Lo que se consigue con esto es un sistema muy resistente a las interferencias de otras fuentes de radio, resistente a los efectos de eco (multipath) y que puede coexistir con otros sistemas de radiofrecuencia sin verse afectado y sin influir en su actividad. Estas ventajas hacen que la tecnología de espectro expandido sea la más adecuada en las bandas de frecuencia para las que no se necesita licencia.

Existen distintas técnicas de espectro expandido, entre las que se encuentra la tecnología CDMA utilizada en la tercera generación de telefonía móvil. No obstante, IEEE 802.11 contempla sólo dos técnicas distintas de espectro expandido:

- **FHSS** (Frequency Hopping Spread Spectrum, 'Espectro Expandido por Salto de Frecuencia'), con la que se consiguen velocidades de transmisión de 1 Mbps.
- **DSSS** (Direct Sequence Spread Spectrum, 'Espectro Expandido por Secuencia Directa'), con la que se consiguen velocidades de transmisión de 2 Mbps. En versiones posteriores de este sistema se han conseguido velocidades superiores.

Dependiendo de la velocidad a la que se van a transmitir los datos, la norma IEEE 802.11 utiliza una técnica u otra.

En 1999 el IEEE sacó una nueva versión de DSSS que permite transmitir datos a 11Mbps. Esta nueva DSSS está recogida en la norma IEEE 802.11 b. Por esta razón, al 802.11 b también se le conoce como 802.11 DSSS o 802.11 HR (High Rate, 'Alta Velocidad').

A pesar de esto, en la práctica, la velocidad de 11 Mbps no es totalmente real debido a distintas razones:

- Las interferencias y ruidos hacen que la velocidad real baje
- El propio protocolo consigue menos rendimiento en sistemas cableados
- Las conexiones a los puntos de acceso son un cuello de botella

Por otro lado, la mayoría de las tarjetas inalámbricas de las estaciones son semidúplex (sólo contienen un equipamiento radio), por lo que pueden transmitir o recibir, pero no ambas cosas simultáneamente.

([http://es.wikipedia.org/wiki/IEEE\\_802.11](http://es.wikipedia.org/wiki/IEEE_802.11), septiembre 2005)

MODELO ISO	MODELO 802.11	TÉCNICAS DE DIFUSIÓN DE 802.11				
Capa de enlace	LLC					
	MAC					
Capa física	PLCP	DSSS 802.11	FHSS 802.11	Infrarrojos 802.11	DSSS-HR 802.11b	OFDM 802.11a
	PMD					

*Tabla 2.4 Capa física y de enlace del estándar IEEE 802.11*  
([http://es.wikipedia.org/wiki/IEEE\\_802.11](http://es.wikipedia.org/wiki/IEEE_802.11), septiembre 2005)

Además de las técnicas de difusión comentadas anteriormente, con la nueva versión IEEE 802.11 a salió una nueva técnica conocida como OFDM (Orthogonal Frequency Division Multiplexing, 'Multiplexación Ortogonal por División de Frecuencias') con la que se consigue velocidades de transmisión de hasta 54 y 100 Mbps.

([http://es.wikipedia.org/wiki/IEEE\\_802.11](http://es.wikipedia.org/wiki/IEEE_802.11), septiembre 2005)

### 2.4.2 Hedy Lamarr y George Antheil

Curiosamente, la patente de las técnicas de espectro expandido no la registraron los militares norteamericanos ni ninguna universidad o empresa afamada, sino la actriz austriaca Hedy Lamarr (su nombre original era Hedwig Eva Maria Kiesler, 1913-2000) y el músico norteamericano George Antheil (1900-1959). Ambos desarrollaron la idea en tiempos de la segunda guerra mundial de un sistema secreto de comunicaciones. Esta idea la patentaron en 1942. La idea se basaba en que, en vez de realizar una transmisión utilizando siempre la misma frecuencia, se utilizaran distintas frecuencias preestablecidas y hacer cambiar la frecuencia utilizada cada corto tiempo para evitar ser interceptados.

El problema de la idea de Lamarr y Antheil es que no había tecnología suficiente para ponerla en práctica. Aunque los militares norteamericanos le dieron uso en la década de los sesenta, no ha sido hasta los años noventa, en la era de la tecnología de radio digital, cuando se le ha dado un uso comercial a este sistema. Desgraciadamente, la parte de Lamar y Antheil expiraba en 1959, por lo que no ha podido repercutirles económicamente.

Lamar fue una actriz muy conocida en los años cuarenta y cincuenta, sobretodo, obtuvo mucha notoriedad en la película Ecstasy (1933) con su escena de 10 minutos en la que aparecía nadando desnuda. Por su parte, Antheil escribía música ultramoderna en los años veinte Todas personas adelantadas a su tiempo.

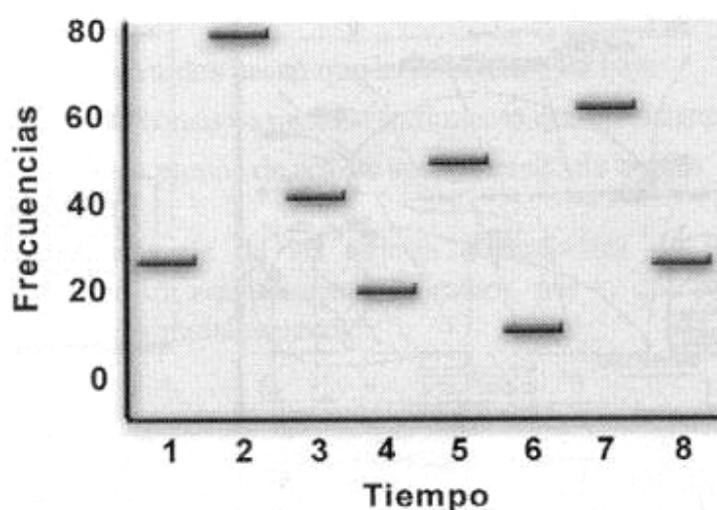
*([http://es.wikipedia.org/wiki/IEEE\\_802.11](http://es.wikipedia.org/wiki/IEEE_802.11), septiembre 2005)*

### 2.4.3 FHSS

La técnica FHSS (Frequency Hopping Spread Spectrum, 'Espectro Expandido por Salto de Frecuencia') consiste en dividir la banda de frecuencias en una serie de canales e ir transmitiendo la información saltando de un canal a otro de acuerdo con un patrón de

saltos (spreading code o hopping code) conocido tanto por el emisor como por el receptor. El tiempo máximo que se debe permanecer en cada frecuencia está regulado en 400 mseg.

El inconveniente de FHSS es que tiene la necesidad de sincronizar el emisor y el receptor en la frecuencia a utilizar en cada momento. Este problema fue resuelto por los ingenieros de Sylvania Electronic Systems a finales de los años cincuenta.



*Figura 2.3 Sistema FHSS*

*([www.arcelect.com/DSSS\\_FHSS-Spead\\_spectrum.htm](http://www.arcelect.com/DSSS_FHSS-Spead_spectrum.htm), septiembre 2005)*

El estándar IEEE 802.11 definió en 1997 que cada canal de FHSS tuviera un ancho de banda de 1 MHz dentro de la banda de frecuencias de 2,4 GHz. El ancho de banda total disponible y, por tanto, el número total de canales disponibles varía de acuerdo con el marco regulatorio de cada país o área geográfica. En cualquier caso, siempre existen tres juegos de secuencias de saltos.

La técnica FHSS reduce las interferencias porque, en el peor de los casos, la interferencia afectara exclusivamente a uno de los saltos de frecuencia, liberándose a interferencia al saltar a otra frecuencia distinta. El resultado es que el número de bits erróneo es extremadamente bajo.

Otra de las ventajas de FHSS es que permite que coexistan varias comunicaciones en la misma banda de frecuencia. Para ello, cada comunicación debe tener un patrón de saltos con distinta secuencia.

A pesar de que el estándar original IEEE 802.11 incluía el sistema FHSS, no existe ninguna instalación real que utilice este sistema. La razón es que la velocidad máxima que se consigue con la técnica FHSS es de unos 3 Mbps (aunque solo este normalizada la velocidad de 1 Mbps). No obstante, es posible que en un futuro se consigan velocidades superiores, se habla de hasta 15 Mbps.

([www.arcelect.com/DSSS\\_FHSS-Speed\\_spectrum.htm](http://www.arcelect.com/DSSS_FHSS-Speed_spectrum.htm), septiembre 2005)

ÁREA GEOGRÁFICA	SECUENCIAS DE SALTO	NÚMERO DE CANALES
Norteamérica (2,4 – 2,4835 GHz) Europa (2,4 – 2,4835 GHz)	Secuencia 1: 0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75 Secuencia 2: 1, 4, 7, 10, 13, 16, 19, 22, 25, 28, 31, 34, 37, 40, 43, 46, 49, 52, 55, 58, 61, 64, 67, 70, 73, 76 Secuencia 3: 2, 5, 8, 11, 14, 17, 20, 23, 26, 29, 32, 35, 38, 41, 44, 47, 50, 53, 56, 59, 62, 65, 68, 72, 74, 77	79
España (2,445 – 2,475 GHz)	Secuencia 1: 0, 3, 6, 9, 12, 15, 18, 21, 24 Secuencia 2: 1, 4, 7, 10, 13, 16, 19, 22, 25 Secuencia 3: 2, 5, 8, 11, 14, 17, 20, 23, 26	27
Francia (2,4465 – 2,4835 GHz.)	Secuencia 1: 0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30 Secuencia 2: 1, 4, 7, 10, 13, 16, 19, 22, 25, 28, 31 Secuencia 3: 2, 5, 8, 11, 14, 17, 20, 23, 26, 29, 32	35
Japón (2,471 – 2,497 GHz)	Secuencia 1: 6, 9, 12, 15 Secuencia 2: 7, 10, 13, 16 Secuencia 3: 8, 11, 14, 17	23

Tabla 2.5 Secuencias de salto de frecuencia de IEEE 802.11 en distintas áreas geográficas.  
([www.arcelect.com/DSSS\\_FHSS-Speed\\_spectrum.htm](http://www.arcelect.com/DSSS_FHSS-Speed_spectrum.htm), septiembre 2005)

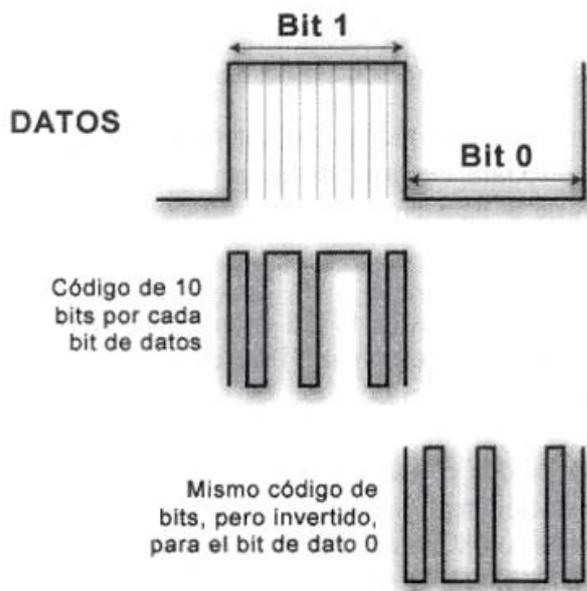
## 2.4.4 DSSS

La técnica DSSS se basa en sustituir cada bit de información por una secuencia de bits conocida como chip o código de chips (chipping code, en inglés). Estos códigos de chips permiten a los receptores eliminar por filtrado las señales que no utilizan la misma secuencia de bits. Entre las señales que son eliminadas se encuentra el ruido y las interferencias.

El código de chips permite al receptor identificar los datos como pertenecientes a un emisor determinado. El emisor genera el código de chips y, sólo los receptores que conocen dicho código pueden descifrar los datos. Por tanto, en teoría, DSSS permite que varios sistemas puedan funcionar en paralelo; cada receptor filtrara exclusivamente los datos que se corresponden con su código de chips. Por otro lado, cuanto más largo es el código de chips, más resistente será el sistema a las interferencias y mayor número de sistemas podrán coexistir simultáneamente. La norma IEEE 802.11 recoge que la longitud mínima del código de chips debe ser de 11.

En la práctica, la coexistencia de sistemas no se consigue por el uso de distintos códigos de chips, sino por el uso de distintas bandas de frecuencias. Un sistema DSSS de 11 Mbps (IEEE 802.11b) necesita un ancho de banda de 22 MHz, siendo la distancia mínima entre portadoras de 30 MHz. Como el ancho de banda disponible en la banda de 2,4 GHz (en el área regulada por el FCC) es de 83,5 MHz, sólo es posible la coexistencia de tres sistemas DSSS en el mismo lugar.

*([www.arcelect.com/DSSS\\_FHSS-Speed\\_spectrum.htm](http://www.arcelect.com/DSSS_FHSS-Speed_spectrum.htm), septiembre 2005)*



*Figura 2.4 Principios del sistema DSSS*  
([www.arcelect.com/DSSS\\_FHSS-Spead\\_spectrum.htm](http://www.arcelect.com/DSSS_FHSS-Spead_spectrum.htm), septiembre 2005)

## 2.4.5 OFDM

OFDM (Orthogonal Frequency Division Multiplexing, 'Multiplexación Ortogonal Por División de Frecuencias') es la técnica de gestión de frecuencias utilizada por IEEE 802.11 a. Esta técnica divide el ancho de banda en subcanales más pequeños que operan en paralelo. De esta forma se consigue llegar a velocidades de transmisión hasta 54Mbps (100 Mbps con soluciones propietarias).

La técnica OFDM fue patentada por Bell Labs en 1970 y está basada en un proceso matemático llamado FFT (Fast Fourier Transform, 'Transformada Rápida de Fourier'). OFDM divide la frecuencia portadora en 52 subportadoras solapadas. 48 de estas subportadoras son utilizadas para transmitir datos y las otras cuatro para poder alinear las frecuencias en el receptor. Este sistema consigue un uso muy eficiente del espectro radioeléctrico.

OFDM puede transmitir datos a distintas velocidades, utilizando distintas técnicas de modulación en cada una de ellas. Las velocidades normalizadas que admite OFDM son 6, 9, 12, 18, 24, 36, 48 y 54 Mbps.

Una de las ventajas de OFDM es que consigue una alta resistencia a las interferencias producidas por las ondas reflejadas en los objetos del entorno (eco o multipath). Estas ondas llegan al receptor con distinta amplitud y a distinto tiempo que la señal principal produciendo interferencias. Estas interferencias son un problema a velocidades superiores a 4Mbps; por este motivo, se utilizan técnicas (OFDM) que mitiguen este efecto.

([www.iss.rwth-aachen.de/Projekte/Theo/OFDM/www\\_ofdm.html](http://www.iss.rwth-aachen.de/Projekte/Theo/OFDM/www_ofdm.html), septiembre 2005)

VELOCIDAD	TÉCNICA DE MODULACIÓN	BITS POR SEÑAL
6 Mbps	BPSK	1
9 Mbps	BPSK	1
12 Mbps	QPSK	2
18 Mbps	QPSK	2
24 Mbps	QAM-16 (BPSK)	4
36 Mbps	QAM-16 (BPSK)	4
48 Mbps	QAM-64 (QPSK)	6
54 Mbps	QAM-64 (QPSK)	6

*Tabla 2.6 Técnicas de modulación utilizadas por el IEEE 802.11a.*  
([www.iss.rwth-aachen.de/Projekte/Theo/OFDM/www\\_ofdm.html](http://www.iss.rwth-aachen.de/Projekte/Theo/OFDM/www_ofdm.html), septiembre 2005)

#### 2.4.6 Modulación de la señal

Para poder transmitir la señal vía radio, hace falta definir un método de difusión de la señal y un método de modulación de la señal. La modulación consiste en modificar una señal pura de radio para incorporarle la información a transmitir. La señal base a modular recibe el nombre de portadora (carrier en inglés). Lo que se le cambia a la portadora para modularla es su amplitud, frecuencia, fase o una combinación de éstas. Mientras mayor es la velocidad de transmisión, más complejo es el sistema de modulación. Las técnicas de modulación utilizadas en IEEE 802.11 son las siguientes:

- BPSK (Binary Phase-shift keying, modulación binaria por salto de fase)
- QPSK (Quadrature Phase-Shift Keying, modulación por salto de fase en cuadratura)
- GFSP (Gaussian frequency-Shift Keying, modulación Gaussiana por salto de frecuencia)
- CCK (Complementary Code Keying, modulación de código complementario)

Una vez emitida la señal modulada, el receptor tiene que recibir la señal, sincronizar el código de difusión y remodular la información. Los sistemas FHSS son más complicados de sincronizar que los sistemas DSSS. En el primer caso hay que sincronizar el tiempo y frecuencia y en el segundo solo el tiempo. ([www.teleco.com.br/es/es\\_ieee802.asp](http://www.teleco.com.br/es/es_ieee802.asp), septiembre 2005)

## **2.5 MAC. EL CONTROL DE ACCESO AL MEDIO**

La capa MAC define los procedimientos que hacen posible que los distintos dispositivos compartan el uso de este espectro radioeléctrico. Mientras que las distintas versiones del estándar 802.11 utilizan distintos sistemas para difundir su señal (su capa física es distinta), la capa MAC es la misma para todas ellas.

Es interesante también el hecho de que la capa MAC sea muy similar a la utilizada por la red Ethernet. Ambas utilizan la técnica conocida como CSMA (Carrier Sense Multiple Access, 'Acceso Múltiple por Detección de Portadora'). No obstante, la versión cableada (Ethernet) utiliza la tecnología CD (Collision Detection, 'Detección de Colisión'), mientras que la versión inalámbrica utiliza la tecnología CA (Collision Avoidance, 'Evitación de Colisión'). Una colisión se produce cuando dos terminales intentan hacer uso del medio físico simultáneamente. La tecnología CD detecta que se ha producido una colisión y retransmite los datos, mientras que la tecnología CA dispone de procedimientos para evitar que se produzcan colisiones.

La razón de que haya dos sistemas es que, cuando el medio es un cable, un terminal puede transmitir y recibir al mismo tiempo, por lo que puede detectar las colisiones. Por el contrario, en el medio radioeléctrico una terminal no puede transmitir y recibir al mismo tiempo por el mismo canal (la transmisión dejaría opaca a la recepción), por lo que, al no poder detectar las posibles colisiones, no hay más remedio que disponer de una técnica que las evite. ([www.teleco.com.br/es/es\\_ieee802.asp](http://www.teleco.com.br/es/es_ieee802.asp), septiembre 2005)

### 2.5.1 Evitar las colisiones

Entre la capa MAC y la capa física se intercambian tres tipos de paquetes de datos: de control, de gestión y de información.

MAC tiene dos funciones distintas para coordinar la transferencia de datos:

- **PCF** (Point Coordination Function, 'Función de Coordinación del Punto') facilita un sistema para poder transmitir el tráfico que es sensible a los retardos y que requiere un tratamiento especial evitando las demoras. A la estación que hace uso de esta función se le llama coordinador del punto, PC (Point Coordinator). El PC emite una señal guía con la duración del periodo de tiempo que necesita disponer del medio. Las estaciones que reciben este serial no emiten durante ese tiempo.
- **DCF** (Distributed Coordination Function, 'Función de Coordinación Distribuida') facilita un sistema que permite compartir el medio físico (radioeléctrico, infrarrojos, etc.) entre todas las estaciones de la red. Para ello, DCF define los mecanismos que le permiten a las estaciones negociar el acceso al medio físico, así como los mecanismos que aseguran la entrega de los datos a las estaciones. A través de DCF se transmiten los datos que no son sensibles a los retardos.

La función DCF se encuentra con un problema y es que una de las diferencias de los medios cableados frente a los inalámbricos es que en estos últimos es mucho más complicado detectar las colisiones. Dos estaciones que no se ven entre sí pueden iniciar una comunicación simultáneamente sin percatarse de la colisión. DFC dispone de una función para impedir la colisión que evita este problema.

Los mecanismos CSMA/CA de detección de la colisión consisten en comprobar si el medio está en uso antes de empezar a transmitir. Si el medio está en uso, se espera un tiempo antes de volver a hacer la comprobación. El tiempo que espera cada estación tiene una duración aleatoria (generada por cada estación entre un tiempo mínimo y un máximo) para evitar que haya colisiones sucesivas indefinidas.

La función DCF contempla un mecanismo físico y otro lógico de detección de colisión. Al mecanismo físico se le conoce como CCA (Clear Channel Assessment, 'Valoración de la Disponibilidad del Canal'). Por ejemplo, cuando hablamos de un medio radioeléctrico, este mecanismo puede consistir en comprobar si en el medio existe cualquier señal DSSS o cualquier otra señal con un nivel de energía superior a un umbral.

El mecanismo físico de detección de colisión es muy eficiente, pero no es eficaz cuando dos estaciones de una misma red que no se ven entre ellas emiten al mismo tiempo. Esto se conoce con el nombre de problema del nodo oculto. Para evitar estos casos, se dispone del sistema lógico de detección de colisión. Este sistema consiste en intercambiar la información del uso del medio a través de tramas de control. A estas tramas de control se las conoce como RTS (Request to Send, 'Solicitud para Enviar') y CTS (Clear to Send, 'Listo para Enviar'). Como esta información de control añade más datos de control a la transmisión en detrimento de los datos de información (baja el rendimiento del protocolo), en aquellos casos en los que se disponga de un medio físico con poca probabilidad de colisiones se puede deshabilitar el mecanismo de detección de colisión, o habilitarlo exclusivamente para aquellos paquetes de datos que tengan un tamaño superior a uno determinado.

Cuando una estación de una red va a transmitir información, primero envía una trama RTS al punto de acceso donde facilita información del destinatario de la transmisión, el remitente y el tiempo que ocupará dicha transmisión. El punto de acceso responde con una trama CTS que reciben todas las estaciones que están en el área de cobertura del punto de acceso. En esta trama CTS se incluye el tiempo de ocupación del medio; por tanto, las estaciones saben el tiempo que estará ocupado el medio y no intentar hacer ninguna transmisión hasta que dicho tiempo no haya pasado.

Por cierto, cuando el destinatario ha recibido toda la información, emite una trama ACK (Acknowledgment, 'Conocimiento') para indicarle al emisor que todo está bien. Si el emisor no recibe la trama ACK que espera, aguardará un tiempo antes de dar la transmisión por errónea y volver a hacer el envío.

*(www.teleco.com.br/es/es\_ieee802.asp, septiembre 2005)*

## 2.5.2 Los servicios

Como hemos visto, las redes inalámbricas IEEE 802.11 están formadas por terminales y puntos de acceso y ambos reciben el nombre de estaciones. La capa MAC define cómo las estaciones acceden al medio mediante lo que llama servicios de estaciones. De la misma forma, define cómo los puntos de acceso gestionan la comunicación mediante lo que llama servicios de distribución.

Los servicios de estación de la capa MAC son los siguientes:

- **Autenticación.** Comprueba la identidad de una estación y la autoriza para asociarse. En una red cableada lo que identifica a un terminal como parte de la red es el hecho de estar conectado físicamente a ella. En una red inalámbrica no existe la conexión física, por lo que, para saber si un terminal forma o no parte de la red, hay que comprobar su identidad antes de autorizar su asociación con el resto de la red.

- **Desautenticación.** Cancela una autenticación existente. Este servicio da por concluida la conexión cuando una estación pretende desconectarse de la red.
- **Privacidad.** Evita el acceso no autorizado a los datos gracias al uso del algoritmo WEP (Wired Equivalency Protocol, 'Protocolo de Equivalencia con Red Cableada'). Este algoritmo pretende emular el nivel de seguridad que se tiene en las redes cableadas.
- **Entrega de datos.** Facilita la transferencia de datos entre estaciones.

Por su lado, los servicios de distribución son estos otros:

- **Asociación.** Para que un terminal pueda comunicarse con otros terminales a través de un punto de acceso, debe primero estar asociado a dicho punto de acceso. Asociación significa asignación del terminal al punto de acceso haciendo que éste sea el responsable de la distribución de datos a, y desde, dicho terminal. En las redes con más de un punto de acceso, un terminal sólo puede estar asociada a un punto de acceso simultáneamente.
- **Desasociación.** Cancela una asociación existente, bien porque el terminal sale del área de cobertura del punto de acceso, o porque el punto de acceso termina la conexión.
- **Reasociación.** Transfiere una asociación entre dos puntos de acceso. Cuando un terminal se mueve del área de cobertura de un punto de acceso a la de otro, su asociación pasa a depender de este último.
- **Distribución.** Cuando se refieren datos de un terminal a otro, el servicio de distribución se asegura de que los datos alcanzan su destino.
- **Integración.** Facilita la transferencia de datos entre la red inalámbrica IEEE 802.11 y cualquier otra red (por ejemplo, Internet o Ethernet).

Los puntos de acceso utilizan tanto los servicios de estaciones como los servicios de distribución, mientras que los terminales sólo utilizan los servicios de estaciones.  
([www.teleco.com.br/es/es\\_ieee802.asp](http://www.teleco.com.br/es/es_ieee802.asp), septiembre 2005)

SERVICIO MAC	DEFINICIÓN	TIPO DE ESTACIÓN
Autenticación	Comprueba la identidad de una estación y la autoriza para asociarse	Terminales y puntos de acceso
Desautenticación	Cancela una autenticación existente	Terminales y puntos de acceso
Asociación	Asigna el terminal al punto de acceso	Puntos de acceso
Desasociación	Cancela una asociación existente	Puntos de acceso
Reasociación	Transfiere una asociación entre dos puntos de acceso	Puntos de acceso
Privacidad	Evita el acceso no autorizado a los datos gracias al uso del algoritmo WEP	Terminales y puntos de acceso
Distribución	Asegura la transferencia de datos entre estaciones de distintos puntos de acceso	Puntos de acceso
Entrega de datos	Facilita la transferencia de datos entre estaciones	Terminales y puntos de acceso
Integración	Facilita la transferencia de datos entre redes Wi-Fi y no Wi-Fi	Puntos de acceso

*Tabla 2.7 Servicios de la capa MAC  
(www.teleco.com.br/es/es\_ieee802.asp, septiembre 2005)*

### 2.5.3 La gestión

Tanto la capa física como la capa MAC están divididas en capacidades de gestión y de transferencia de datos. Lo que se conoce como PLME (PHY Layer Management Entity, 'Entidad de Gestión de la Capa Física') es quien se encarga de la gestión de la capa física, mientras que lo que se conoce como MLNE (AMC Layer Management Entity, 'Entidad de Gestión de la Capa MAC') es quien se encarga de la gestión de la capa MAC. PLME y MLME intercambian información a través de MIB (Management Information Base, 'Base de Datos de la Información de Gestión'). Ésta es una base de datos de las características físicas (velocidad de transmisión, niveles de potencia, tipo de antena, etc.) de las estaciones. (www.teleco.com.br/es/es\_ieee802.asp, septiembre 2005)

### 2.5.4 El flujo de datos

Los datos que se van a transmitir por el medio radioeléctrico proceden de las capas superiores (formato IP) y se pasan a la capa LLC (Logical Link Control, 'Control Lógico del Enlace'). La capa LLC le pasa estos datos a la capa MAC, quien, a su vez, se los pasa a la capa física para su emisión.



*Figura 2.5 Interfaz de la capa MAC y Física  
(www.teleco.com.br/es/es\_ieee802.asp, septiembre 2005)*

Los paquetes de datos que se intercambian entre las capas LLC y MAC se conocen como MSDU (MAC Service Data Unit, 'Unidad de Datos del Servicio MAC'), mientras que los paquetes de datos que se intercambian entre las capas MAC y física reciben el nombre de MPDU (MAC protocol data unit, 'Unidad de Datos del Protocolo MAC'). En la capa física, quien recibe estos datos es PLCP, quien es responsable de convertir los datos MPDU a un formato compatible con el medio físico.

*(www.teleco.com.br/es/es\_ieee802.asp, septiembre 2005)*

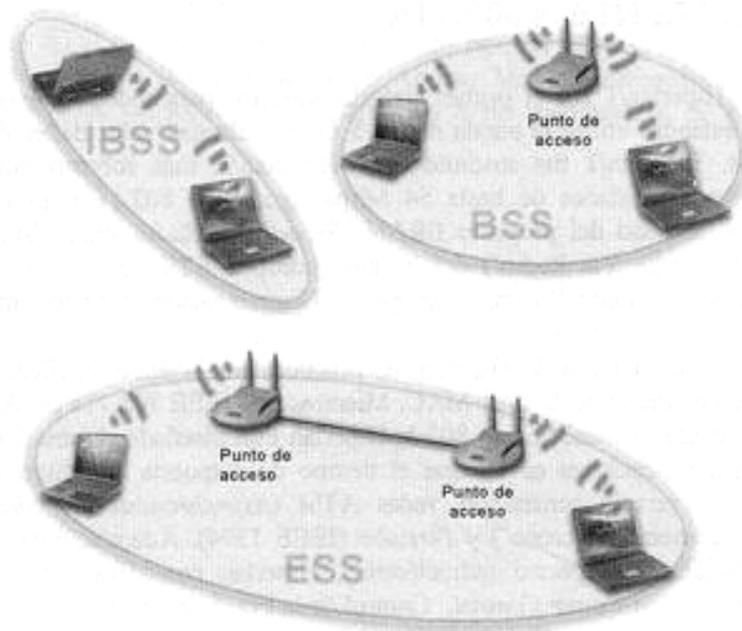
## 2.6 LA ESTRUCTURA DE RED

La topología de una red es la arquitectura de la red, la estructura jerárquica que hace posible la interconexión de los equipos. IEEE 802.11 y, por tanto, Wi-Fi, contempla tres topologías distintas:

- **IBSS** (Independent Basic Service Set, 'Conjunto de Servicios Básicos Independientes'). Esta modalidad está pensada para permitir exclusivamente comunicaciones directas entre los distintos terminales que forman la red. En este caso no existe ningún terminal principal que coordine al grupo, no existe punto de acceso. Todas las comunicaciones son directas entre dos o más terminales del grupo. A esta modalidad se la conoce también como ad hoc, independiente o de igual a igual (peer-to-peer en inglés).
- **BSS** (Basic Service Set, 'Conjunto de Servicios Básicos'). En esta modalidad se añade un equipo llamado punto de acceso (AP o Access Point en inglés) que realiza las funciones de coordinación centralizada de la comunicación entre los distintos terminales de la red. Los puntos de acceso tienen funciones de buffer (memoria de almacenamiento intermedio) y de gateway (pasarela) con otras redes. A los equipos que hacen de pasarelas con otras redes externas se les conoce como portales. A la modalidad BSS también se la conoce como modo infraestructura.
- **ESS** (Extended Service Set, 'Conjunto de Servicios Extendido'). Esta modalidad permite crear una red inalámbrica formada por más de un punto de acceso. De esta forma se puede extender el área de cobertura de la red, quedando constituida por un conjunto de celdas pegadas unas a otras. Una red ESS está formada por múltiples redes BSS.

En las modalidades BSS y ESS todas las comunicaciones pasan por los puntos de acceso. Aunque dos terminales estén situados uno junto al otro, la comunicación entre ellos pasará por el punto de acceso al que estén asociados, Esto quiere decir que un

terminar no puede estar configurado para funcionar en la modalidad ad hoc (IBSS) y de infraestructura (BSS) a la vez. ([http://es.wikipedia.org/wiki/IEEE\\_802.11](http://es.wikipedia.org/wiki/IEEE_802.11), septiembre 2005)



*Figura 2.6 Estructuras de redes Wi-Fi*  
([http://es.wikipedia.org/wiki/IEEE\\_802.11](http://es.wikipedia.org/wiki/IEEE_802.11), septiembre 2005)

## 2.7 HIPERLAN FRENTE A 802.11 a

HiperLan/1 fue el primer estándar europeo para redes de área local inalámbricas. Este estándar utiliza la banda de los 5 GHz y alcanza velocidades de transmisión de 24 Mbps. Hiperlan/1 fue sustituido por Hiperlan/2, más robusto que el anterior y que permite velocidades de hasta 54 Mbps (igual que 802.11 a). El estándar Hiperlan es responsabilidad del proyecto BRAN (Broadband Radio Area Network, 'Red Local de Banda Ancha Vía Radio') del instituto europeo ETSI (European Telecommunications Standards Institute, 'Instituto Europeo de Normalización en Telecomunicaciones').

La capa física de Hiperlan es prácticamente idéntica a IEEE 802.11a. La mayor diferencia radica en la capa MAC. Mientras que IEEE 802.11a pretende ser simplemente una versión inalámbrica de 802.3, Hiperlan está diseñado de una forma más ambiciosa: soporta aplicaciones en las que el tiempo de respuesta es crítico, define interfaces de redes de tercera generación, redes ATM (Asynchronous Transfer Mode, 'Modo de Transferencia Asíncrono') y Firewire (IEEE 1394). Además, para conseguir una mejor utilización del espectro radioeléctrico, Hiperlan considera características como TPC (Transmission Power Control, 'Control de la Potencia de Transmisión') o DFS (Dynamic Frequency Selection, 'Selección Dinámica de Frecuencia').

CARACTERÍSTICA	802.11a	802.11b	802.11g	HiperLAN2
Regulador	IEEE (USA)	IEEE (USA)	IEEE (USA)	ETSI (Europa)
Banda de frecuencia	5 GHz	2,4 GHz	2,4 GHz	5 GHz
Modulación	OFDM	DSSS	OFDM	OFDM
Velocidad máxima	54 Mbps	11 Mbps	54 Mbps	54 Mbps
Rango de velocidades (Mbps)	54, 48, 36, 24, 18, 12, 9 y 6	11, 5,5, 2 y 1	54, 36, 33, 24, 22, 12, 11, 9, 6, 5,5, 2 y 1	54, 36, 27, 18, 12, 9 y 6
Número de canales sin superposición	8	3	3	8
Ancho de banda en un área	432 Mbps (8 x 54)	33 Mbps (3 x 11)	162 Mbps (3 x 54)	432 Mbps (8 x 54)
Usuarios en un área	512	192	192	512
Eficiencia por canal (throughput)	18 Mbps	6 Mbps	12 Mbps	31 Mbps
Compatibilidad	Wi-Fi5	Wi-Fi	Wi-Fi	
A destacar	Alta velocidad y número de usuarios	Buen alcance y consumo de potencia	Compatible con 802.11b y más alcance que 11a	Integrado en sistemas 3G (UMTS) y soporta QoS

*Tabla 2.8 Comparación de las tecnologías inalámbricas principales.*  
([http://es.wikipedia.org/wiki/IEEE\\_802.11](http://es.wikipedia.org/wiki/IEEE_802.11), septiembre 2005)

Actualmente existen dos grupos de trabajo, IEEE 802.11 h y 5GSG, para considerar las compatibilidades entre Hiperlan y IEEE 802.11a. Estos grupos de trabajo esperan poder promover un nuevo estándar en la banda de 5 GHz que sea compatible no sólo para el IEEE y ETSI, sino también para el Consejo japonés MMAC (Mobile Multimedia Access

Communication, 'Comunicación de Acceso Móvil Multimedia'). Un aspecto importante que debe conseguir es la adaptación a las regulaciones de Norteamérica, Europa y Japón. ([http://es.wikipedia.org/wiki/IEEE\\_802.11](http://es.wikipedia.org/wiki/IEEE_802.11), septiembre 2005)

## CAPÍTULO 3

### EQUIPO BÁSICO PARA UNA RED Wi-Fi

#### 3.1 POR QUÉ INSTALAR UNA RED INALÁMBRICA

Las redes inalámbricas hacen exactamente el mismo trabajo que realizan las redes cableadas: interconectan ordenadores y otros dispositivos informáticos (impresoras, módem, etc.) para permitirles compartir recursos. Las redes locales permiten interconectar desde dos ordenadores hasta cientos de ellos situados en un entorno donde la distancia máxima de un extremo a otro de la red suele ser de algunos cientos de metros. Esto quiere decir que las redes de área local se limitan generalmente al ámbito de un edificio. No obstante, distintas redes locales situadas en distintos edificios (edificios que pueden estar situados en distintas ciudades) pueden interconectarse entre si formando un único entorno de red.

En resumen, las ventajas que ofrece una red de área local, sea cableada o Inalámbrica, son las siguientes:

- Permite compartir periféricos: impresoras, escáneres, etc.
- Permite compartir los servicios de comunicaciones (ADSL, módem cable, RDSI, etc.)
- Permite compartir la información contenida en cada ordenador.
- Permite compartir aplicaciones.

A partir de aquí, la pregunta sería si la red local que nos interesa instalar debe ser cableada o inalámbrica. Muchos usuarios responden a esta cuestión simplemente decidiéndose a instalar la última tecnología del mercado y la última tecnología es la inalámbrica. La inquietud de disponer de la tecnología más moderna es viable y no cabe

duda de que las redes inalámbricas ofrecen una mayor comodidad de uso o una mayor facilidad de instalación, pero toda tecnología tiene sus propias limitaciones. Por tanto, creo que es interesante pararse a analizar un poco las ventajas y posibles inconvenientes que tiene la tecnología inalámbrica.

(<http://www.mailxmail.com/informatica/wifi/capitulo1.htm>, octubre 2005)

### 3.1.1 Ventajas

Las principales ventajas que ofrecen las redes inalámbricas frente a las redes cableadas son las siguientes:

- **Movilidad.** La libertad de movimientos es uno de los beneficios más evidentes de las redes inalámbricas. Un ordenador o cualquier otro dispositivo (por ejemplo, una
- PDA o una Webcam) pueden situarse en cualquier punto dentro del área de cobertura de la red sin tener que depender de si es posible o no hacer llegar un cable hasta ese sitio. Ya no es necesario estar atado a un cable para navegar por Internet, imprimir un documento o acceder a la información de nuestra red local corporativa o familiar. En la empresa se puede acceder a los recursos compartidos desde cualquier lugar de ella, hacer presentaciones en la sala de reuniones, acceder a archivos, etc., sin tener que tender cables por mitad de la sala o depender de si el cable de red es o no suficientemente largo.
- **Desplazamiento.** Con un ordenador portátil o PDA no sólo se puede acceder a Internet o a cualquier otro recurso de la red local desde cualquier parte de la oficina o de la casa, sino que nos podemos desplazar sin perder la comunicación. Esto no sólo da cierta comodidad, sino que facilita el trabajo en determinadas tareas, como, por ejemplo, la de aquellos empleados cuyo trabajo les lleva a moverse por todo el edificio.

- **Flexibilidad.** Las redes inalámbricas no sólo nos permiten estar conectados mientras nos desplazamos con un ordenador portátil, sino que también nos permiten colocar un ordenador de sobremesa en cualquier lugar sin tener que hacer el más mínimo cambio en la configuración de la red. A veces, extender una red cableada no es una tarea fácil ni barata. Piense en edificios antiguos o en áreas apartadas. En muchas ocasiones acabamos colocando peligrosos cables por el suelo para evitar tener que hacer la obra de poner enchufes de red más cercanos. Las redes inalámbricas evitan todos estos problemas. Resulta también especialmente indicado para aquellos lugares en los que se necesitan accesos esporádicos. Si en un momento dado existe la necesidad de que varias personas se conecten a la red en la sala de reuniones, la conexión inalámbrica evita llenar el suelo de cables. En sitio a donde pueda haber invitados que necesiten conexión a Internet (centros de formación, hoteles, cafés, entornos de negocio o empresariales) las redes inalámbricas suponen una alternativa mucho más viable que las redes Cableadas.
- **Ahorro de costes.** Diseñar e instalar una red cableada puede llegar a alcanzar un alto coste, no solamente económico, sino en tiempo y molestias. En entornos domésticos y ni determinados entornos empresariales donde no se dispone de una red cableada porque su instalación presenta problemas, la instalación de una red inalámbrica permite ahorrar costes al permitir compartir recursos: acceso a Internet, Impresoras, etc.
- **Escalabilidad.** Se le llama escalabilidad a la facilidad de expandir la red después de su instalación inicial. Conectar un nuevo ordenador cuando se dispone de una red inalámbrica es algo tan sencillo como instalarle una tarjeta y listo. Con las redes cableadas esto mismo requiere instalar un nuevo cableado o, lo que es peor, esperar hasta que el nuevo cableado quede instalado.

*(<http://www.mailxmail.com/informatica/wifi/capitulo1.htm>, octubre 2005)*

### 3.1.2 inconvenientes

Evidentemente, como todo en la vida, no todo son ventajas, las redes inalámbricas también tienen algunos puntos negativos en su comparativa con las redes de cable. Los principales inconvenientes de las redes inalámbricas son los siguientes:

- **Menor ancho de banda.** Las redes de cable actuales trabajan a 100 Mbps, mientras que las redes inalámbricas Wi-Fi lo hacen a 11 Mbps. Es cierto que existen estándares que alcanzan los 54 Mbps y soluciones propietarias que llegan a 100 Mbps, pero estos estándares están en los comienzos de su comercialización y tienen un precio superior al de los actuales equipos Wi-Fi.
- **Mayor inversión inicial.** Para la mayoría de las configuraciones de red local, el coste de los equipos de red inalámbricos es superior al de los equipos de red cableada.
- **Seguridad.** Las redes inalámbricas tienen la particularidad de no necesitar un medio físico para funcionar (podría funcionar incluso en el vacío). Esto fundamentalmente es una ventaja, pero se convierte en un inconveniente cuando pensamos que cualquier persona con un ordenador portátil sólo necesita estar dentro del área de cobertura de la red para poder intentar acceder a ella. Como el área de cobertura no está definida por paredes o por ningún otro medio físico, a los posibles intrusos no les hace falta estar dentro de un edificio o estar conectado a un cable además, el sistema de seguridad que incorporan las redes Wi-Fi no es de los más fiables. A pesar de esto, también es cierto que ofrece una seguridad válida para la inmensa mayoría de las aplicaciones y que ya hay disponible un nuevo sistema de seguridad (WPA) que hace a Wi-Fi mucho más confiable.
- **Interferencias.** Las redes inalámbricas funcionan utilizando el medio radioeléctrico en la banda de 2,4 GHz. Esta banda de frecuencias no requiere de licencia administrativa para ser utilizada por lo que muchos equipos del mercado, como teléfonos inalámbricos, microondas, etc., utilizan esta misma banda de frecuencias. Además, todas las redes Wi-Fi funcionan en la misma banda de

Frecuencias, incluida la de los vecinos. Este hecho hace que no se tenga la garantía de que nuestro entorno radioeléctrico esté completamente limpio para que nuestra red inalámbrica funcione a su más alto rendimiento. Cuantos mayores sean las interferencias producidas por otros equipos, menor será el rendimiento de nuestra red. No obstante el hecho de tener probabilidades de sufrir interferencias no quiere decir que se tengan. La mayoría de las redes inalámbricas funcionan perfectamente sin mayores problemas en este sentido.

- **Incertidumbre tecnológica.** La tecnología que actualmente se está instalando y que ha adquirido una mayor popularidad es la conocida como Wi-Fi (IEEE802.11b). Sin embargo, ya existen tecnologías que ofrecen una mayor velocidad de transmisión y unos mayores niveles de seguridad. Es posible que, cuando se popularice esta nueva tecnología, se deje de comercializar la actual o, simplemente, se deje de prestar tanto apoyo a la actual. Lo cierto es que las leyes del mercado vienen también marcadas por las necesidades de los clientes y aunque existe esta incógnita, los fabricantes no querrán perder el tirón que ha supuesto Wi-Fi y harán todo lo posible para que los nuevos dispositivos sean compatibles con los actuales. La historia nos ha dado muchos ejemplos similares. (<http://www.mailxmail.com/informatica/wifi/capitulo1.htm>, octubre 2005)

### 3.1.3 Qué hacer

Después de ver las ventajas y los inconvenientes, cualquiera puede sacar sus propias conclusiones; no obstante, hagamos un par de apreciaciones.

La tecnología inalámbrica en los hogares es un caso especial. Es raro encontrar una casa que tenga preinstalada una red cableada de datos. Sin embargo, aun contando con una única impresora, una única conexión a Internet (vía ADSL o cable, por ejemplo), un único grabador de CD o un único escáner, cada vez es más normal disponer de más de un ordenador en casa. Para poder compartir estos recursos, se puede instalar una rígida

red cableada tendiendo cables a través de las paredes o configurar una red inalámbrica. Es cierto que esta última solución es más cara que la primera, pero también es más flexible, escalable, fácil de instalar y, además, permite movilidad. ¿Por qué estar encerrado en una habitación si hace un día estupendo y se está mejor en el salón, en el patio o en el parque enfrente de casa? Por otro lado, el problema de la seguridad no es altamente preocupante en la informática del hogar.

El caso de las empresas puede ser similar al anterior, pero también nos encontramos con un punto adicional. Las redes cableadas son un problema en aquellas empresas donde existe la posibilidad de cambiar la disposición de los puestos de trabajo. Sin embargo, para una red inalámbrica no supone ningún problema el cambiar un ordenador de sitio.

El hecho de instalar una red inalámbrica no quiere decir que toda la red tenga que ser inalámbrica. Las redes Wi-Fi son completamente compatibles con las redes locales cableadas Ethernet. Por tanto, la parte inalámbrica puede ser un complemento de la parte cableada. Se puede cablear lo que sea fácil cablear y dejar a Wi-Fi que resuelva la extensión de la red a aquellas áreas más difícilmente cableables. Por otro lado, también se puede disponer de una red de cable para unos usuarios y una red inalámbrica paralela para aquellos otros que por la labor que desempeñan necesitan disfrutar de la ventaja de la movilidad.

Por último, las redes inalámbricas son ideales, por ejemplo, si se necesita disponer de conexión a red en lugares abiertos (por ejemplo, un campus universitario), en sitios Públicos (centros comerciales, redes vecinales, servicios municipales etc.) o sitios cerrados pero disponiendo de movilidad (almacenes, salas de reuniones, etc.).

*(<http://www.mailxmail.com/informatica/wifi/capitulo1.htm>, ,octubre 2005)*

## 3.2 QUE POSIBILIDADES TENEMOS

Anteriormente hemos dado los puntos más importantes para confirmar que, efectivamente, necesitamos una red inalámbrica. Ahora toca analizar qué tipo de red es la que le viene mejor a nuestras necesidades. Una red puede comunicar un par de ordenadores o a cientos de ellos, podemos tener a todos los ordenadores concentrados ni una pequeña zona o dispersos por una gran área, dentro de un edificio, en vanos edificios o en el exterior.

Las decisiones que hay que tomar a este respecto son las siguientes:

- Cuál será la configuración de la red, si se necesitaran instalar puntos de acceso y cuántos serán necesarios.
- Qué tarjeta o dispositivos inalámbricos instalaremos en cada ordenador, PDA o cualquier otro equipo informático que necesitemos conectar.
- Qué tipo de antenas necesitaremos para poder cubrir todo el área por la que necesitamos disponer del servicio.
- Cómo conectaremos nuestra red inalámbrica a la red local cableada y a Internet.

*(<http://www.mailxmail.com/informatica/wifi/capitulo1.htm>, octubre 2005)*

### 3.2.1 Las distintas configuraciones de red

Las redes inalámbricas, al igual que las redes cableadas, sirven para interconectar no sólo ordenadores, sino también cualquier otro tipo de equipo informático al que se le pueda instalar un dispositivo inalámbrico. Éste es el caso, por ejemplo, de las agendas electrónicas PDA (como las Palm Pilot de 3Com), las impresoras o las cámaras Web. A pesar de ello, no cabe duda de que el uso fundamental que se le da a una red inalámbrica es la interconexión de ordenadores. De hecho, en esta monografía hablamos

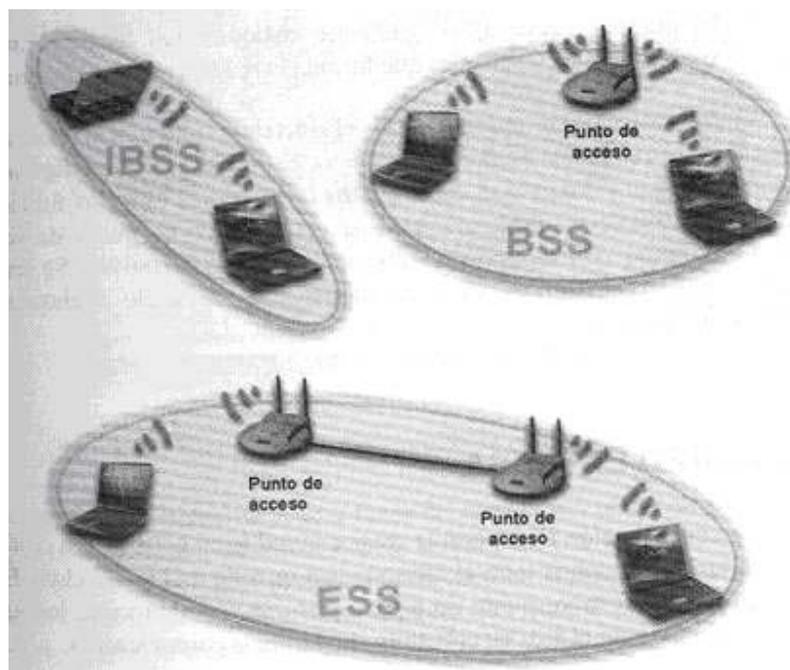
frecuentemente de red de ordenadores, aunque evidentemente nos referimos a ordenadores o cualquier otro equipo susceptible de ser conectados a la red.

Las redes inalámbricas Wi-Fi admiten tres tipos de configuraciones:

- **Modo ad hoc o IBSS.** Es una configuración en la cual sólo se necesita disponer de tarjetas o dispositivos inalámbricos Wi-Fi en cada ordenador. Los ordenadores se comunican unos con otros directamente, sin necesidad de que existan puntos de acceso intermedios.
- **Modo infraestructura o BSS.** En esta configuración, además de las tarjetas Wi-Fi en los ordenadores, se necesita disponer de un equipo conocido como punto de acceso. El punto de acceso lleva a cabo una coordinación centralizada de la comunicación entre los distintos terminales de la red.
- **Modo ESS.** Esta configuración permite unir distintos puntos de acceso para crear una red inalámbrica con una amplia cobertura. Una red ESS está formada por múltiples redes BSS. Las distintas redes BSS se pueden poner pegadas unas a otras para conseguir tener una continuidad de servicio en toda la red ESS.

Desde el punto de vista de los terminales, las configuraciones BSS y ESS son la misma. Por otro lado, un terminal no puede estar configurado en modo ad hoc e infraestructura a la vez; lo que sí se puede es configurar el terminal de distinta forma dependiendo de lo que interese en cada momento.

*(<http://www.mailxmail.com/informatica/wifi/capitulo1.htm>, octubre 2005)*



*Figura 3.1 Configuraciones de redes Wi-Fi*  
 (<http://www.mailxmail.com/informatica/wifi/capitulo1.htm>, octubre 2005)

### 3.3 NECESIDAD DE LOS PUNTOS DE ACCECO

Las comunicaciones ad hoc son muy fáciles de configurar y resultan muy interesantes cuando se necesita establecer una comunicación temporal entre dos equipos. Por otro lado, el modo infraestructura es el más adecuado para crear redes permanentes, aunque sean de tan sólo dos terminales. Las razones que nos llevan a esta conclusión son varias:

- El modo infraestructura ofrece un mayor alcance que en la modalidad ad hoc. Los terminales no tienen por qué estar dentro del área de cobertura el uno del otro; al tener un punto de acceso intermedio pueden, al menos, duplicar su distancia.
- El punto de acceso permite compartir el acceso a Internet entre todos sus terminales. Esto permite compartir un acceso de banda ancha (por ejemplo,

ADSL o cable) entre todos los terminales que forman la red, sean dos o cientos de ellos.

- El punto de acceso permite crear redes con un mayor número de terminales.
- El punto de acceso ofrece características de gestión de la comunicación que no ofrece el modo ad hoc.
- El punto de acceso, al igual que cualquier red local, permite compartir los recursos de los terminales que forman la red (archivos, impresoras, etc.)

Recientemente ha aparecido en el mercado una alternativa al modo ad hoc conocida como software de punto de acceso. Esto consiste en configurar los ordenadores en modo ad hoc y hacer que uno de estos ordenadores haga las funciones de punto de acceso instalándole un programa especial, el software de punto de acceso. Ya se han hecho programas de este tipo para distintos sistemas operativos. Se ha dado el caso de usuarios que recuperan un viejo ordenador para dedicarlo exclusivamente a trabajar como punto de acceso. (<http://www.mailxmail.com/informatica/wifi/capitulo1.htm>, octubre 2005)

### **3.4 CREAR UNA RED EXTENSA**

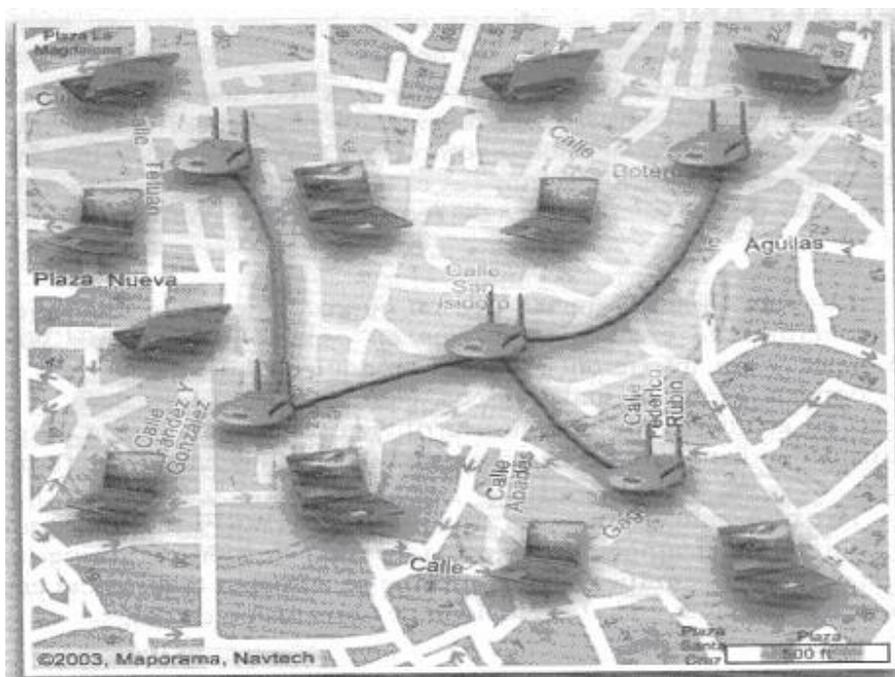
La configuración ESS permite crear una red local inalámbrica con una extensa área de cobertura. Para cubrir toda el área, se disponen de múltiples celdas BSS, cada una de las cuales cuenta con su punto de acceso. En esta configuración, los terminales pueden desplazarse por toda el área de cobertura sin perder la comunicación.

La configuración ESS resulta interesante cuando se necesita cubrir una gran área de oficinas, oficinas localizadas en distintas plantas, un espacio público o lugares con una alta concentración de terminales donde un solo punto de acceso resulta escaso.

Los distintos puntos de acceso que forman una red ESS se interconectan entre si a través de una red que, generalmente, suele ser una red cableada Ethernet. Esta conexión sino

también para que los terminales inalámbricos puedan comunicarse con los terminales de la red cableada.

Para que funcionen las redes ESS, deben configurarse los distintos puntos de acceso como miembros de una misma red. Esto implica que todos deben tener el mismo nombre de red y la misma configuración de seguridad, aunque funcionando en distintos canales de radio. Esto último es importante porque, de otro modo, los puntos de acceso se interferirían unos a otros impidiendo la comunicación con sus terminales.



*Figura 3.2 Con la configuración ESS se puede cubrir toda la ciudad.*  
(<http://www.mailxmail.com/informatica/wifi/capitulo1.htm>, octubre 2005)

Cuando un terminal se mueve fuera del alcance del punto de acceso con el que está asociado originalmente, automáticamente se reasocia con un nuevo punto de acceso con el que tenga cobertura. Esta reasociación la hace el terminal automáticamente, sin que el usuario tenga que hacer nada. Desde el punto de vista del usuario, la conexión a una red ESS es idéntica a la conexión a una red BSS. La única diferencia es que se dispone de una mayor cobertura.

VELOCIDAD	DISTANCIA EN INTERIOR	DISTANCIA EN EXTERIOR
11 Mbps	50 metros	270 metros
5,5 Mbps	80 metros	380 metros
2 Mbps	130 metros	430 metros
1 Mbps	160 metros	540 metros

*Tabla 3.1 relación entre las distancia y velocidad con las tarjetas Wi-Fi (en condiciones ideales).*

*(<http://www.mailxmail.com/informatica/wifi/capitulo1.htm>, octubre 2005)*

### 3.5 SOBRE EL ALCANCE

Cuando nos decidimos a instalar una red inalámbrica, generalmente se parte de unas necesidades de cobertura. Pretendemos tener cobertura en toda la oficina, la casa, el entorno empresarial o el pueblo completo. Quiere esto decir que uno de los factores más importante de las redes inalámbricas es la cobertura. La cobertura de la red depende tanto del alcance de los adaptadores de red (las tarjetas Wi-Fi), como del de los puntos de acceso.

Los fabricantes anuncian que un punto de acceso o una tarjeta Wi-Fi llega a tener una cobertura de cientos de metros en espacio abierto con visibilidad directa entre terminales y sin interferencias de otros equipos que trabajen en la banda de 2,4GHz (microondas, teléfonos inalámbricos, etc.). Esto es cierto, pero, si se instala el punto de acceso en el interior de una casa u oficina, el alcance puede reducirse a unos 25 a 50 metros dependiendo de los obstáculos que haya en la habitación (armarios, mesas, etc.).

Por otro lado, la mayoría de los equipos Wi-Fi vienen equipados con un sistema que bala automáticamente la velocidad de transmisión conforme la señal de radio se va debilitando. Esto significa que, conforme se aumenta la distancia entre emisor y receptor, se puede ir disminuyendo la velocidad de transmisión de datos.

Además de la distancia, en el entorno existen otros factores que pueden afectar a la cobertura, como son las interferencias (naturales y artificiales) o las pérdidas de propagación debido a los obstáculos. De hecho, muchas de estas condiciones del entorno son cambiantes, por lo que en una posición puede haber cobertura en un momento dado y no haberla unos minutos más tarde. Por ejemplo, puede que no tenga cobertura en la cocina cuando tenga puesto el microondas, pero si el resto del tiempo, o puede que no tenga cobertura en una zona del patio cuando en primavera los árboles la dejan completamente en sombra radioeléctrica, pero si el resto del año.

La conclusión es que, a poco que se complique la visibilidad entre los terminales (por distancia, por los obstáculos o por las interferencias), la única manera de saber exactamente si existe cobertura entre ellos es Instalando los equipos y haciendo una prueba real de cobertura.

*(<http://www.mailxmail.com/informatica/wifi/capitulo1.htm>, octubre 2005)*

### **3.5.1 Interferencias**

Dado que 802.11b utiliza la banda de 2,4 GHz y que estas frecuencias se encuentran en una banda abierta para usos industriales, científicos y médicos para los que no se necesita licencia, existe el riesgo de coincidir en el uso de la frecuencia con otros sistemas como los microondas, teléfonos inalámbricos, sistemas de televigilancia, dispositivos bluetooth o, incluso, otras redes inalámbricas. Estos otros usos pueden producir interferencias en las señales de radio de nuestra red. Una interferencia consiste en la presencia no deseada de señales radioeléctricas que interrumpen el normal funcionamiento del sistema.

Para evitar que una interferencia pueda cortar la comunicación, cuando el equipo Wi-Fi (protocolo MAC) detecta la presencia de una señal de interferencia, automáticamente entra en un periodo de espera en la idea de que, pasado dicho periodo, habrá pasado la

interferencia. Evidentemente, esto hace que el servicio se degrade, pero no se interrumpe.

Desde el punto de vista del usuario, es imposible evitar las interferencias esporádicas, pero lo que sí se puede evitar son las interferencias constantes o periódicas. El sistema consiste en hacer pruebas de recepción de señal en la zona bajo sospecha. Estas pruebas pueden realizarse a distintas horas del día. A veces ocurre que las interferencias sólo se producen a la hora de la comida (microondas). Muchas de estas interferencias pueden evitarse sencillamente situando el punto de acceso en otro lugar, o movimiento el terminal.

*(<http://www.mailxmail.com/informatica/wifi/capitulo1.htm>, octubre 2005)*

### **3.5.2 Pérdida de propagación**

Desde el momento que una señal de radio sale del equipo transmisor empieza a perder potencia por el simple hecho de propagarse. Conforme aumenta la distancia desde el emisor, las pérdidas de señal van en aumento. Esta pérdida de señal es mayor también cuanto mayor es la frecuencia radioeléctrica a la que se emite. Por tanto, a mayor frecuencia, menor es el alcance de la señal.

Por otro lado, generalmente no existe una línea de visión directa entre el transmisor y el receptor. Los obstáculos (como las paredes, los árboles, los muebles o los cristales) que impiden dicha visibilidad directa afectan grandemente a la pérdida de señal.

Otros de los factores que afectan negativamente a la propagación de la señal son los ecos producidos por el rebote de la señal en los obstáculos (paredes, muebles, etc.). El rebote produce que la señal pueda tomar distintos caminos para llegar hasta el receptor. Al final, lo que el receptor recibe no es una única señal, sino una señal principal y una combinación de señales iguales (ecos) que le llegan a distinto tiempo y con distinta potencia. A esto se le llama efecto eco. Este efecto puede producir graves interferencias que llegan a degradar fuertemente la recepción de la señal. El efecto eco es más

perjudicial cuanto mayor es la potencia del eco y mayor su retardo con respecto a la señal principal.

Algunos equipos Wi-Fi disponen de sistemas como la diversidad de antenas (tienen dos antenas), el filtrado de la señal o software de filtrado que ayudan a resolver este problema.

*(<http://www.mailxmail.com/informatica/wifi/capitulo1.html>, octubre 2005)*

### **3.6 EL EQUIPAMIENTO NECESARIO**

La mayoría de las redes inalámbricas que hay en el mercado (sean Wi-Fi o de otro tipo) funcionan de una manera similar: tienen unas estaciones base (puntos de acceso) que coordinan las comunicaciones y unas tarjetas de red (adaptadores de red) que se instalan en los ordenadores y que les permiten formar parte de la red.

Adicionalmente, existen antenas que permiten aumentar el alcance de los equipos Wi-Fi, así como software especializado que permite facilitar la labor de gestión y mantenimiento de la red inalámbrica.

Antes de describir cómo instalar una red, vamos a dedicar unas páginas a describir las características más importantes de los distintos componentes de una red inalámbrica. En este capítulo vamos a tratar fundamentalmente los adaptadores de red y los puntos de acceso; las antenas externas serán tratadas en un capítulo aparte.

*(<http://www.microsoft.com/formacion/redinalambrica.msp>, octubre 2005)*

#### **3.6.1 Elegir un punto de acceso**

El punto de acceso es el centro de las comunicaciones de la mayoría de las redes inalámbricas. El punto de acceso no sólo es el medio de intercomunicación de todos los

terminales inalámbricos, sino que también es el puente de interconexión con la red fija e Internet.

Existen dos categorías de puntos de acceso:

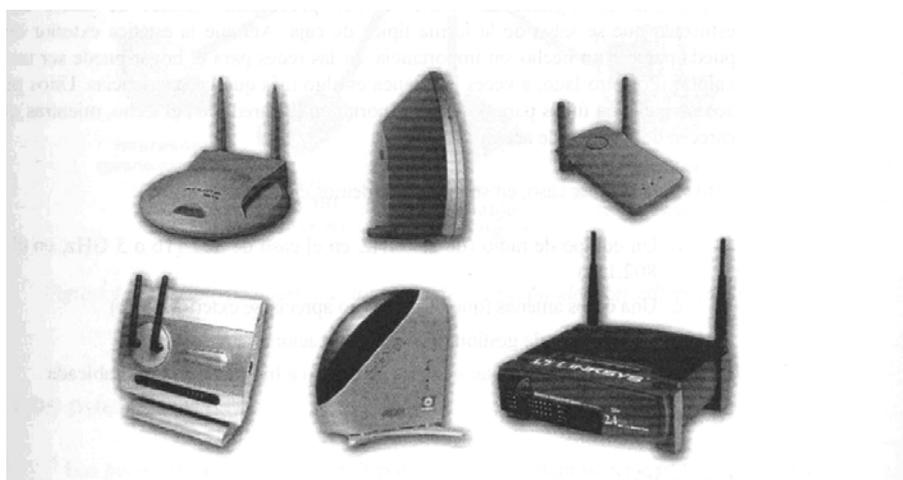
- Puntos de accesos profesionales, diseñados para crear redes corporativas de tamaño medio o grande. Éstos suelen ser los más caros, pero incluyen mejores características (aunque sean particulares del fabricante), como son mejoras en la seguridad y una más perfecta integración con el resto de equipos. Los líderes de este tipo de equipamiento son Cisco, 3Com, Agere/Orinoco (antiguamente conocidos como Lucent) y Nokia.
- Puntos de acceso económicos dirigidos a cubrir las necesidades de los usuarios de pequeñas oficinas o del hogar. Estos puntos de acceso ofrecen exactamente los mismos servicios que los anteriores, con la misma cobertura y las mismas velocidades. La diferencia se nota cuando se dispone de un gran número de usuarios. En estos casos, los puntos de acceso profesionales ofrecen mejores resultados, eso sí, multiplicando el precio por cuatro o cinco. Los que más puntos de acceso de tipo económico venden son Intel, 3Com, D-Link, Agere/Orinoco, NetGear Proxim y Linksys.

Aparte de lo anterior, cada equipo tiene sus propias características externas. Por ejemplo, algo que diferencia claramente a unos puntos de acceso de otros es el número y tipo de puertos exteriores que ofrece. Existen puntos de acceso que disponen hasta de un puerto de impresora (con su servidor de impresión), mientras que otros se limitan a ofrecer una conexión para red cableada o Internet.

Por otro lado, es habitual que los puntos de acceso se utilicen también como pasarela de conexión con otras redes (por ejemplo, con Internet). Desde este punto de vista, es importante que se tengan en cuenta dos cosas: la primera es que nos fijemos en las características de router del punto de acceso: DHCP, NAT o propiedades de firewall son

características que nos ayudarán en la configuración y manejo de las comunicaciones con Internet o con otras redes.

En el entorno corporativo suelen coexistir una red inalámbrica, para darle movilidad a los usuarios que la necesitan, junto con una red cableada, para darle conectividad al resto de usuarios. Generalmente, las redes corporativas utilizan el protocolo TCP/IP; no obstante, hay que tener en cuenta que en el mercado existen otros protocolos como SPX/IPX, NetBIOS, LANtastic, etc. Por tanto, conviene comprobar que el punto de acceso que se va a comprar sea compatible con el protocolo de red cableada con el que se va a conectar.



*Figura 3.3 modelos de puntos de acceso (no están a la misma escala)*  
([www.superwarehouse.com/Wireless\\_\\_\\_Access\\_Point/c3/2154](http://www.superwarehouse.com/Wireless___Access_Point/c3/2154), octubre 2005)

Por último, los equipos Wi-Fi tienen la ventaja de que tienen la garantía de funcionar sin problemas de acuerdo con la norma IEEE 802.11b. Esto es así, sin duda, en relación con los adaptadores de red; sin embargo, existe cierta incompatibilidad en relación con los puntos de acceso. La incompatibilidad en servicio una comunicación cuando un usuario pasa del área de cobertura de un punto de acceso al de otro (a esto se le llama roaming en inglés). En este caso, si los puntos de acceso son de distinto fabricante, es muy posible que se corte la comunicación. La comunicación se podrá volver a establecer con el nuevo punto de acceso, pero no se habrá producido una

transferencia sin interrupciones, que es de lo que se trata. Para evitar este problema, es recomendable que los puntos de acceso vecinos sean del mismo fabricante. Además, cuando todos los dispositivos son del mismo fabricante, es posible utilizar alguna característica adicional propietaria del fabricante. Se puede valorar si esto merece la pena.

En cualquier caso, el IEEE está trabajando para solucionar este problema (grupo de trabajo IEEE 802.11f). Por cierto, esto no tiene nada que ver con las tarjetas inalámbricas que se conectan a los ordenadores; estas últimas si pueden proceder de fabricantes distintos sin problemas.

*(www.superwarehouse.com/Wireless\_\_\_Access\_Point/c3/2154,octubre 2005)*

### **3.6.2 Características de los puntos de acceso**

Los puntos de acceso son realmente unas pequeñas cajas de las que sobre salen una o dos antenas. Algunos fabricantes se han preocupado incluso de darles una forma estilizada que se salga de la forma típica de caja. Aunque la estética exterior de la caja pueda parecer un hecho sin importancia, ni las redes para el hogar puede ser un punto a valorar. Por otro lado, a veces la estética es algo más que las apariencias. Unos puntos de acceso incluyen útiles para poderlos soportar en la pared o en el techo, mientras que otros carecen de este tipo de accesorios.

En cualquier caso, en su interior podemos encontrar lo mismo:

- Un equipo de radio (de 2,4 GHz, en el caso de 802.11b o 5 GHz, en el caso de 802.11a)
- Una o dos antenas (que pueden o no apreciarse exteriormente)
- Un software de gestión de las comunicaciones
- Puertos para conectar el punto de acceso a Internet o a la red cableada

*(www.superwarehouse.com/Wireless\_\_\_Access\_Point/c3/2154,octubre 2005)*

### 3.6.2.1 La radio

El objetivo principal de los puntos de acceso es comunicarse con los terminales vía radio. Por tanto, lo principal de los puntos de acceso es su equipamiento de radio. Este equipamiento viene integrado en un conjunto de chips electrónicos conocidos como chipsets. Aunque en el mercado existen muchos fabricantes de puntos de acceso, muchos menos los que fabrican chipsets. Dos de los principales fabricantes de chipsets Wi-Fi son Lucent e Intersil.

Desde el punto de vista del usuario, el funcionamiento de los distintos chipsets es idéntico. Además, entre ellos deben ser compatibles. No obstante, la teoría de la compatibilidad trae sorpresas a veces, por lo que resulta recomendable comprar equipos (puntos de acceso y tarjetas inalámbricas) que utilicen chipsets del mismo fabricante.

La única forma de estar seguros de esto es comprar todo el equipamiento del mismo fabricante. Esto puede ser un contrasentido desde el punto de vista de la compatibilidad de la marca Wi-Fi, pero tiene sus ventajas prácticas.

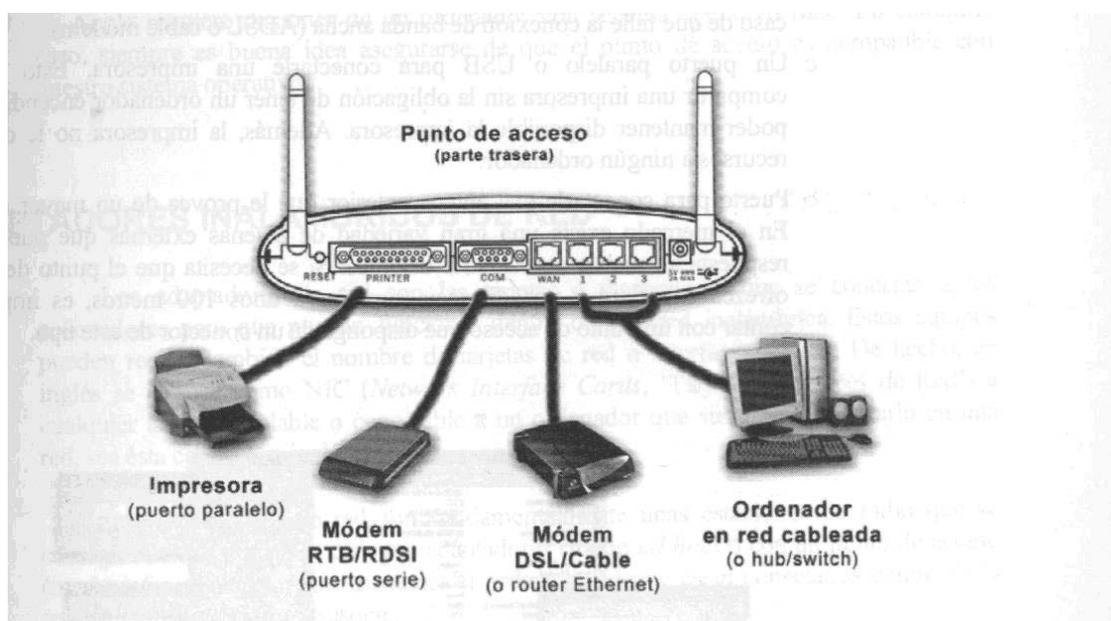


Figura 3.4 Ejemplo de puertos de un punto de acceso (modelo SpeedStream 2623).

([www.superwarehouse.com/Wireless\\_\\_Access\\_Point/c3/2154](http://www.superwarehouse.com/Wireless__Access_Point/c3/2154), octubre 2005)

### 3.6.2.2 Los puertos

Los puntos de acceso necesitan disponer de puertos para poderse conectar con una red local cableada y con Internet. Para conseguir esto, los puntos de acceso suelen traer uno o más puertos 10/100 Base-T (RJ-45). No obstante, las posibilidades de conectividad de los puntos de acceso no acaban aquí dependiendo del modelo, nos podemos encontrar con los siguientes puertos:

- Un puerto especial para conectarse a un hub o switch de red de área local Ethernet ( uplink port)
- Disponer internamente de un hub, por lo que ofrecen de dos a cuatro puertos exteriores para conectarles los equipos de red Ethernet de que disponga el usuario. Esto es ideal para el hogar o la pequeña oficina ya que evita la necesidad de disponer de un hub o switch independiente. En cualquier caso, si se necesitase de más de cuatro puertos, siempre se puede comprar otro hub y conectarlo al punto de acceso para extender la red.
- Un puerto serie RS-232 para que se le pueda conectar un módem de red telefónica (RTB o RDSI). Esta conexión a Internet a 56 Kbps o 64 Kbps puede ser utilizada como acceso principal a Internet o como acceso de segunda en el caso de que falle la conexión de banda ancha (ADSL o cable módem).
- Un puerto paralelo o USB para conectarle una impresora. Esto permite compartir una impresora sin la obligación de tener un ordenador encendido para poder mantener disponible la impresora. Además, la impresora no le ocuparía recursos a ningún ordenador.
- Puerto para conectarle una antena exterior que le provea de un mayor alcance. En el mercado existe una gran variedad de antenas externas que pueden dar respuesta a muchas necesidades distintas. Si se necesita que el punto de acceso ofrezca cobertura a una distancia superior a unos 100 metros, es importante contar con un punto de acceso que disponga de un conector de este tipo.

*([www.superwarehouse.com/Wireless\\_\\_\\_Access\\_Point/c3/2154](http://www.superwarehouse.com/Wireless___Access_Point/c3/2154), octubre 2005)*

### 3.6.2.3 Gestión del punto de acceso

Los puntos de acceso ofrecen determinadas características que son configurables, como son las opciones de seguridad o de gestión de la red. La mayoría permiten llevar a cabo esta configuración a través de una interfaz basada en páginas Web. Para hacer uso de esto, sólo se necesita instalar el software que incluye el punto de acceso.

No obstante, es importante saber que algunos puntos de acceso no utilizan una interfaz Web, sino que requieren de la introducción directa de líneas comandos (lo que se conoce como CLI, Command Line Interface, 'Interfaz de Línea de Comandos') o, incluso, requieren de un sistema operativo particular. Por ejemplo, Airport Base Station de Apple requiere disponer de un ordenador con sistema operativo Mac. En cualquier caso, siempre es buena idea asegurarse de que el punto de acceso es compatible con nuestro sistema operativo.

*([www.superwarehouse.com/Wireless\\_\\_\\_Access\\_Point/c3/2154](http://www.superwarehouse.com/Wireless___Access_Point/c3/2154), octubre 2005)*

### 3.6.3 Adaptadores inalámbricos de red

Los adaptadores de red son las tarjetas o dispositivos que se conectan a los ordenadores para que puedan funcionar dentro de una red inalámbrica. Estos equipos pueden recibir también el nombre de tarjetas de red o interfaces de red. De hecho, en inglés se conoce como NIC (Network Interface Cards, 'Tarjetas Interfaces de Red') a cualquier tarjeta instalable o conectable a un ordenador que sirve para integrarlo en una red, sea ésta cableada o inalámbrica.

Los adaptadores de red son fundamentalmente unas estaciones de radio que se encargan de comunicarse con otros adaptadores (modo ad hoc) o con un punto de acceso (modo infraestructura) para mantener al ordenador al que están conectados dentro de la red inalámbrica a la que se asocie.

Como todos los equipos de radio, los adaptadores de red necesitan una antena. Esta suele venir integrada dentro del propio adaptador sin que extremadamente se note. Algunos adaptadores, sin embargo, permiten identificar claramente su antena. En cualquier caso, la mayoría de los adaptadores incluyen un conector para poder disponer una antena externa. Este tipo de antenas aumentan grandemente el alcance del adaptador.

*(www.superinventos.com/wifi.htm, octubre 2005)*

### **3.6.4 Tipos de adaptadores de red**

Al igual que desde hace tiempo viene siendo normal encontrar ordenadores que incluyen de fábrica un puerto Ethernet RJ-45, recientemente están apareciendo en el mercado algunos ordenadores portátiles que ya tienen Integrado un adaptador de red Wi-Fi. No obstante, éstos son todavía excepciones, lo normal es que el adaptador de red sea un equipo independiente que haya que instalar o conectar al ordenador o PDA.

Actualmente existen los siguientes tipos de adaptadores inalámbricos de red:

- **Tarjetas PCMCIA.** Éstas son tarjetas que tienen un tamaño similar al de una tarjeta de crédito (realmente como un 30% más larga) y que se insertan en los puertos PCMCIA (PC card) de tipo II que suelen incorporar la mayoría de los ordenadores portátiles. Se pueden encontrar tarjetas PCMCIA de Wi-Fi desde 300 pesos (y el precio sigue bajando). Los ordenadores de sobremesa no suelen contar con puertos PCMCIA.
- **Tarjetas PCI o ISA.** Los ordenadores de sobremesa no suelen disponer de ranuras PCMCIA. De lo que si disponen son de ranuras PCI o ISA donde se pueden instalar todo tipo de tarjetas de periféricos, entre las que están las tarjetas Wi-Fi. No obstante, lo cierto es que no es fácil encontrar en el mercado este tipo de tarjetas Wi-Fi. La solución alternativa consiste en instalar tarjetas conversoras de PCI o ISA a PCMCIA. Estos conversores son tarjetas PCI o ISA que se insertan en una ranura interna del ordenador y que ofrecen un puerto PCMCIA al

exterior. El precio de estos adaptadores es de unos 400 pesos. Evidentemente, adicionalmente haría falta disponer de la tarjeta PCMCIA.

- **Unidades USB.** Se trata de unidades inalámbricas que se conectan al ordenador (portátil o sobremesa) mediante un puerto USB. Estas unidades son más propias de los ordenadores de sobremesa, ya que evitan tener que instalar en su interior un adaptador de tarjeta PCMCIA. No obstante, son válidas para todo tipo de ordenadores Si el ordenador ya tiene ocupados todos sus puertos USB (por ejemplo, porque se está utilizando para el teclado, la impresora, etc.), en el mercado existen multiplicadores de puertos USB que permiten sacar cuatro puertos de donde había uno (cuestan sobre unos 100 o 200 pesos).

*(www.superinventos.com/wifi.htm, octubre 2005)*



*Figura 3.5 Distintos tipos de adaptadores de red PCMCIA.*

*(www.superinventos.com/wifi.htm, octubre 2005)*

#### **3.6.4.1 Tarjetas PCMCIA**

Uno de los problemas que tenían antiguamente los ordenadores portátiles era que difícilmente podían ampliarse en sus prestaciones. Para instalarle una tarjeta de red o un módem a un ordenador de sobremesa, bastaba con añadir en su interior la tarjeta correspondiente (ISA, PCI, etc.). El interior de los portátiles, sin embargo, estuvo completamente cerrado hasta que aparecieron unos puertos especiales conocidos como PCMCIA (Personal Computer Memory Card International Association, 'Asociación

Internacional de Tarjetas de Memoria para Ordenadores Portátiles'). En inglés se la conoce más coloquialmente como PC Card (tarjeta de PC).

Los puertos PCMCIA son una especie de ranura en la que se pueden insertar unas tarjetas del tamaño de una de crédito. Estas tarjetas quedan insertadas en el interior de la ranura, por lo que el ordenador portátil no pierde su integridad y fácil portabilidad. En el mercado existen muchos tipos de tarjetas PCMCIA: módem, tarjetas de red Ethernet, discos duros, etc.

Las tarjetas PCMCIA las crearon en 1989 una asociación de fabricantes de equipos con el propósito inicial de desarrollar una norma hardware y software para tarjetas de memoria intercambiables (de ahí su nombre). No obstante, la idea fue tan buena que se ha utilizado para todo tipo de periféricos.

Todas las tarjetas PCMCIA tienen un ancho de 54 milímetros, siendo su largo variable, pero con un mínimo de 85,6 milímetros. El hecho de ser variable se debe a que algunas tarjetas necesitan sobresalir hacia el exterior para mostrar algún tipo de conector, una antena o, simplemente, porque necesitan más espacio.

En cuanto al grosor de las tarjetas existen tres tipos: las tarjetas tipo I con un grosor de 3,3 milímetros (utilizadas, por ejemplo, para ampliaciones de memoria), las de tipo II con un grosor de 5 milímetros (son las habituales en los adaptadores de red inalámbricos) y las de tipo III con un grosor de 10,5 milímetros (utilizadas, por ejemplo, por los discos duros).

Por una razón exclusivamente de espacio, cada tarjeta requiere su propio tipo de ranura en el ordenador. Esto quiere decir que una ranura de tipo III admite cualquier tipo de tarjeta, mientras que una ranura de tipo I sólo admite tarjetas de este tipo. El tamaño más habitual de las tarjetas es el de tipo II.

Aparte del tamaño y del peso; otra de las características que aportan las tarjetas PCMCIA es su bajo consumo de energía y ser resistentes a los golpes típicos de los dispositivos móviles.

Por cierto, los adaptadores Wi-Fi PCMCIA suelen ser de tipo II (con bus de 32 bits tipo CardBus) y la mayoría de los ordenadores portátiles incluyen una o dos ranuras PCMCIA de este tipo. Si tiene un ordenador muy antiguo, será mejor que compruebe si admite este tipo de tarjetas antes de comprar el adaptador.

*(www.superinventos.com/wifi.htm, octubre 2005)*

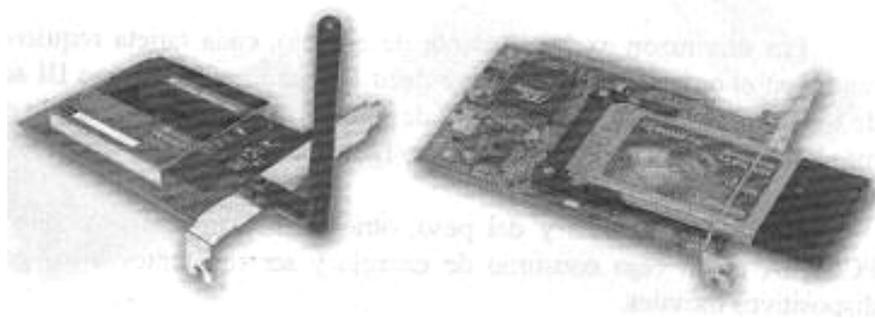
#### **3.6.4.2 Adaptadores PCI e ISA**

Los ordenadores de sobremesa no suelen incluir ranuras PCMCIA. Estos ordenadores suelen disponer de suficiente espacio interior como para admitir la instalación de nuevos periféricos a base de tarjetas tipo PCI (Peripheral Components Interconnect, 'Interconexión de Componentes Periféricos') o ISA (Industry Standard Architecture, 'Arquitectura Normalizada de la industria'). Este tipo de tarjetas es más barata que las tarjetas PCMCIA, aunque también son mayores en tamaño y de instalación algo más compleja (entre otras cosas, hay que abrir el ordenador). Lo curioso en este caso es que difícilmente se encuentran en el mercado adaptadores inalámbricos de red de tipo PCI e ISA. El motivo quizás sea que las mayores prestaciones de las redes inalámbricas se consiguen con un ordenador portátil (por aquello de la movilidad), así que el mayor mercado de adaptadores de red está hoy por hoy en el de las tarjetas PCMCIA, siendo relativamente pequeño el de las tarjetas PCI e ISA.

¿Cómo se conectan entonces los ordenadores de sobremesa a las redes inalámbricas? Pues con adaptadores USB o utilizando una tarjeta convertora de PCI e ISA a PCMCIA.

Una tarjeta convertora de PCI e ISA a PCMCIA es una tarjeta que se instala en el interior del ordenador en una de las ranuras PCI e ISA disponibles y que ofrece al

exterior una ranura PCMCIA (generalmente de tipo II o III). Dicho de otra manera, este conversor le añade una ranura PCMCIA al ordenador.



*Figura 3.6 Adaptador de red PCI y conversor PCI a PCMCIA.  
(www.superinventos.com/wifi.htm, octubre 2005)*

Las tarjetas conversoras de este tipo suelen ser baratas, pero a este precio hay que añadirle el precio de la propia tarjeta PCMCIA, por lo que la conexión a la red inalámbrica del ordenador de sobremesa pasa a ser algo más cara que la del ordenador portátil.

El mayor inconveniente que presentan los dispositivos PCI e ISA es que requieren ser instalados en el interior del ordenador. Por tanto, hay que abrir el ordenador. Adicionalmente, incluso los que anuncian ser Plug&Play (tipo conectar y funcionar) finalmente requieren que se les instale el software de los controladores (por eso algunos los llaman Plug&Play, Conectar y rezar).

Por cierto, si se tiene un ordenador que dispone tanto de ranuras PCI como ISA, siempre es más aconsejable utilizar las de tipo PCI. Éstas suelen dar menos problemas de instalación y requieren menos recursos del sistema. No hay más que pensar que ISA es un estándar de principios de los años ochenta, mientras que PCI es de principios de los años noventa (1993, exactamente). PCI fue desarrollado por Intel como competidor al que poco antes se había convertido en el primer estándar de bus local, el estándar VESA (Video Electronics Standard Association, 'Asociación para la Normalización de la

Electrónica de Video') La principal novedad que trajo PCI fue el ser el primer sistema que permitía lo que se vino a llamar Plug&Play (conectar y funcionar).

Por cierto, ISA, también conocido como bus AT, puede transmitir información a una velocidad máxima de 16 MBps, mientras que PCI puede llegar a 528 Mbps. ([www.superinventos.com/wifi.htm](http://www.superinventos.com/wifi.htm), octubre 2005)

### **3.6.4.3 Adaptadores USB**

USB (Universal Serial Bus, 'Bus Serie Universal') es un nuevo puerto de comunicaciones que se diseñó para poder mejorar la forma en cómo los periféricos se conectaban a los ordenadores. Hasta que apareció USB en 1993, las únicas posibilidades de conectar un periférico a un ordenador eran mediante el puerto serie o el puerto paralelo (además del puerto del teclado/ratón y el puerto de juego). El inconveniente mayor con estos puertos es que sólo se podían conseguir velocidades de transmisión de 115 Kbps. Adicionalmente, los ordenadores sólo disponían de un puerto paralelo y dos series, con lo que el número de dispositivos a conectar se reducía a tres; además, son puertos que no le permiten al ordenador reconocer automáticamente el dispositivo que tienen conectado, ni alimentarlos a través del propio puerto.

USB vino a traer las siguientes ventajas:

- No hace falta apagar el ordenador para conectar o desconectar un periférico USB.
- El ordenador reconoce automáticamente los periféricos que se conectan mediante USB. Si es preciso, instalan automáticamente los controladores necesarios para hacerlo funcionar adecuadamente.
- Ofrecen una alta velocidad de transferencia de datos: hasta 12 Mbps.

- Permite conectar hasta 127 dispositivos USB. Incluso, aunque el ordenador disponga de un solo puerto, basta con instalar un multiplicador de puertos (un hub) para disponer de más puertos USB.
- Ofrece alimentación eléctrica a los periféricos a través del propio conector USB (Hasta 500 mA)
- Los periféricos USB pueden apagarse automáticamente cuando detectan que no se están utilizando.
- Los periféricos USB se instalan automáticamente, sin necesidad de abrir el ordenador.



*Figura 3.7 Adaptador de red USB  
([www.superinventos.com/wifi.htm](http://www.superinventos.com/wifi.htm), octubre 2005)*

Todo lo anterior ha hecho que los periféricos USB hayan ido desplazando poco a poco al resto de periféricos del mercado, hasta el punto de que ya existen ordenadores que no disponen de puertos serie ni paralelo, sino sólo puertos USB. Hoy en prácticamente todos los tipos de periféricos ofrecen la posibilidad de ser conectados ordenador a través de un puerto USB: impresoras, módem, escáneres, cámaras, discos duros, etc. El caso de los adaptadores de red inalámbricos no iba a ser menos.

Desde el punto de vista de los adaptadores de red inalámbrica, USB ofrece la ventaja de poder compartir el adaptador entre diferentes ordenadores según se necesite. Como

instalar el adaptador es tan fácil como conectarlo al puerto USB, si un ordenador necesita conectarse a la red, se le enchufa el adaptador y listo. Cuando no lo necesite, con desenchufarlo del puerto USB se tiene bastante.

Otras de las ventajas es que el adaptador puede reorientarse con respecto al punto de acceso para buscar una mejor cobertura, sin tener que mover el ordenador.

El único inconveniente de los adaptadores USB es que son dispositivos externos al ordenador. No quedan integrados dentro de él como lo hacen los adaptadores PCMCIA, PCI o ISA. (*www.superinventos.com/wifi.html, octubre 2005*)

#### **3.6.4.4 Adaptadores para PDA**

Un PDA es un pequeño ordenador que cabe en la palma de la mano; de hecho, en inglés también se les conoce como PalmPC, literalmente, 'PC de la palma de la mano', y el PDA más vendido es el Palm Pilot de 3Com. Es cierto que también se les conoce como PocketPC (PC de bolsillo) o como HandHeld PC (PC de mano).

Debido a su pequeño tamaño, los PDA pueden llevarse siempre encima, por lo que suelen incluir aplicaciones que, de alguna manera, son asistentes personales de su usuario: agenda de direcciones, agenda de actividades, lista de tareas, juegos, etc. No obstante, un PDA puede utilizarse también como herramienta de comunicación: permite acceder a Internet, ver páginas Web, gestionar correo electrónico, etc. De hecho, las nuevas PDA incluyen versiones reducidas de programas de gestión tan conocidos como Microsoft Word, Excel, etc. En definitiva, un PDA es un pequeño ordenador de gran utilidad debido precisamente a su pequeño tamaño.

Habitualmente, un PDA se conecta a Internet a través de un ordenador personal. Los correos se escriben en el PDA, pero no se transmiten (o reciben) hasta que no se conectan mediante un cable (o infrarrojos) al ordenador personal con el que se ha

asociado previamente. También existe la posibilidad de conectarle un módem especial al PDA y acceder directamente a Internet a través de un proveedor de acceso (vía Llamada telefónica). En este sentido, han aparecido más recientemente en el mercado equipos PDA que incluyen en su interior un terminal móvil, o teléfonos móviles que incluyen en su interior las capacidades de los PDA.

Cualquiera de las soluciones anteriores tiene un inconveniente y es que no permite que el PDA esté conectado a Internet permanentemente, al menos, sin pagar unas altas tarifas por las llamadas telefónicas (del móvil o del fijo). Por otro lado, salvo en el caso del PDA con móvil (con alto coste en Llamadas), el PDA siempre estará conectado por cable para intercambiar sus datos con el ordenador asociado o conectarse a Internet. Pues bien, las redes inalámbricas le ofrecen al PDA la posibilidad de liberarse de las ataduras del cable.



*Figura 3.8 Adaptador de red para PDA  
(www.superinventos.com/wifi.html, octubre 2005)*

En el mercado existen módulos adaptadores de red inalámbrica para los principales modelos de PDA: 3Com, Compaq, HP, Casio, etc. A la hora de comprar uno de estos dispositivos, es conveniente asegurarse de que es el adecuado para el modelo concreto

de PDA de que se dispone. Estos módulos suelen ser tarjetas de tipo Compact Flash con una pequeña antena exterior. (*www.superinventos.com/wifi.html, octubre 2005*)

#### **3.6.4.5 Compatibilidad con los sistemas operativos**

Los adaptadores de red, como el resto de periféricos, para su correcto funcionamiento necesitan instalar un pequeño software que se conoce como controlador de dispositivo (driver en inglés). Este software es específico de cada sistema operativo y se instala, de forma automática o manual, cuando se instala el adaptador o cuando se conecta al ordenador por primera vez.

Los sistemas operativos suelen disponer de los controladores de dispositivos de los periféricos más comunes del mercado. En muchos casos, es suficiente conectar el adaptador al ordenador y automáticamente se instala todo lo necesario. Sin embargo, en otras ocasiones, el sistema operativo no dispone del controlador adecuado. Para estos casos, el fabricante suele incluir un CD con el adaptador que contiene los controladores para los principales sistemas operativos. Incluso puede incluir un programa instalador del controlador. Si no se dispusiese de este CD, también se puede acceder a la página Web del fabricante del equipo para intentar conseguirlo.

El inconveniente es que no todos los adaptadores disponen del controlador necesario para todos los sistemas operativos. La mayoría incluyen el controlador para Windows, pero son muchos menos los que lo incluyen para Linux o Mac OS. Esto quiere decir que es importante asegurarse de que el controlador que se va a comprar es compatible con el sistema operativo del ordenador en el que se va a instalar. Esto es más importante aún si se dispone de Linux o Mac OS. Los que peor lo tienen son los usuarios de Mac. Estos últimos pueden buscar en las marcas Agere/Orinoco o Proxim.

(*www.superinventos.com/wifi.html, octubre 2005*)



*Figura 3.9 Equipos Wi-Fi bridge*  
([www.superinventos.com/wifi.html](http://www.superinventos.com/wifi.html), octubre 2005)

## **CAPÍTULO 4**

### **CONEXIÓN A PORTAL INTERNET CON ELEMENTO BÁSICO DE TRANSMISIÓN**

#### **4.1 LA CONEXIÓN A INTERNET**

Dicen los expertos que en un futuro próximo la mayor parte de nuestra información estará en Internet. Esto nos permitirá disponer de la información independientemente de donde nos encontremos: en casa, en la oficina, de visita profesional o personal o de vacaciones. Siempre podremos acceder a nuestras bases de datos, catálogo de fotos, documentos, libros o aplicaciones.

Pues bien, las redes inalámbricas permiten que todos los dispositivos conectados a la red puedan compartir una única conexión a Internet. Evidentemente, esto no significa que todos los usuarios tengan que ver las mismas páginas Web. Cada usuario puede navegar por sus propias páginas, leer su correo o hacer cualquier otro uso de Internet. Lo que si es cierto es que el ancho de banda de la conexión será compartido entre todos los usuarios. Por tanto, es posible que en algunos momentos la conexión vaya algo más lenta de lo habitual, pero en general, la navegación será bastante buena. Si no lo fuera, siempre se puede contratar una velocidad mayor de acceso a Internet o contratar más de una línea de acceso.

La inmensa mayoría de los modelos de punto de acceso ya tienen integrada la posibilidad de compartir una conexión a Internet (o a cualquier otra red). Esto es posible porque el punto de acceso tiene integrada la función de router. El router es un equipo que hace de intermediario entre Internet y cada uno de los ordenadores de la red privada (en este caso inalámbrica).

Evidentemente, para compartir un acceso a Internet, lo primero es disponer del acceso. Las empresas que facilitan los servicios de acceso a Internet se conocen con el nombre de proveedores de acceso (o por su acrónimo en inglés, ISP, Internet Service Provider).

Aunque existen puntos de acceso que permiten compartir el acceso a Internet de baja velocidad (56 Kbps), lo más recomendable es disponer de un acceso de banda ancha: ADSL, módem cable, satélite, etc.

([www.adsl.com](http://www.adsl.com), noviembre 2005)

## **4.2 EL ACCESO A INTERNET**

La red Internet es una " global interconectada con prácticamente todos los tipos de redes públicas de telecomunicaciones existentes en la actualidad. Esto quiere decir que cualquier persona que tenga acceso a una red de comunicaciones (red telefónica, red de móviles, RDSI, satélites, etc.) podrá tener acceso a través de ésta a la red Internet.

La red pública más extendida es la red telefónica básica. Esto hace que la mayoría de los usuarios de Internet utilicen esta red como su acceso habitual. No obstante, existen otros caminos de acceso a Internet que son utilizados fundamentalmente por aquellos usuarios que necesitan un acceso a más alta velocidad (banda ancha) o que están situados en unos emplazamientos sin cobertura telefónica. ([www.adsl.com](http://www.adsl.com), noviembre 2005)

### **4.2.1 Ancho de banda**

Un término que se utiliza frecuentemente cuando se habla del acceso a Internet es el de banda ancha o banda estrecha. Cuando se habla de comunicación digital, la palabra ancho de banda hace referencia a la velocidad con la que se transmiten los datos entre dos puntos (los bits por segundo). El ancho de banda de acceso a Internet es la velocidad con la que se está conectado con esta red. El estar conectado a Internet con banda estrecha

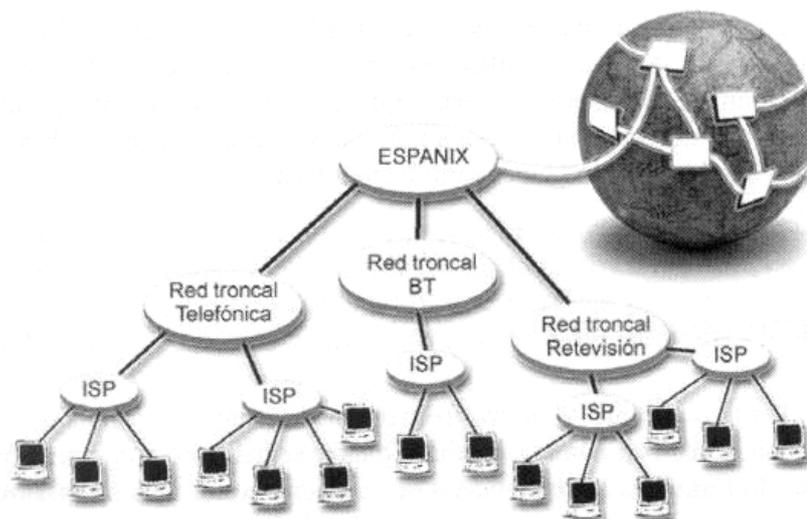
significa estar conectado a baja velocidad y el hacerlo con banda ancha significa disponer de alta velocidad.

Realmente, la frontera entre la banda ancha y estrecha no está claramente definida. No obstante, se entiende que la velocidad que se puede alcanzar utilizando un canal telefónico o RDSI es banda estrecha y las velocidades superiores son banda ancha. En este sentido la frontera entre ambas bandas se encuentra en 64 Kbps. Igual o menor es banda estrecha, superior es banda ancha. En la práctica, la banda ancha empieza en 128Kbps ya que no existe comercializada ninguna conexión superior a 64 y menor a 128Kbps. ([www.adsl.com](http://www.adsl.com), noviembre 2005)

#### **4.2.2 El proveedor de acceso**

Un proveedor de acceso, también conocido como ISP (Internet Service Provider, 'Proveedor del Servicio Internet'), es un intermediario que facilita el acceso a Internet a las personas o empresas interesadas. Los proveedores de acceso suelen ofrecer a sus clientes la posibilidad de acceder a Internet por cualquiera de los sistemas siguientes:

- **Baja velocidad (banda estrecha)**, mediante un módem de red telefónica básica o de RDSI. Para ello, le facilitan al cliente un nombre de usuario y clave y una lista de números telefónicos de acceso para que el cliente elija el número que le venga mejor dependiendo de dónde se encuentre.
- **Alta velocidad (banda ancha)**, mediante circuito dedicado. En este caso, dependiendo del tipo de proveedor de acceso de que se trate, puede ofrecer un tipo de solución tecnológica u otra: ADSL, módem cable, circuito Frame Relay, solución por satélite, etc. En cada caso, el proveedor de accesos suele facilitarle al usuario el equipamiento necesario.



*Figura 4.1 Visión simplificada de la red de acceso a Internet  
([www.adsl.com](http://www.adsl.com), noviembre 2005)*

Por otro lado, como toda conexión a Internet requiere una configuración en el ordenador del usuario, el proveedor de acceso siempre tiene que proporcionar al usuario todos los parámetros necesarios para realizar esta configuración.

([www.adsl.com](http://www.adsl.com), noviembre 2005)

### 4.3 EL ACCESO DE BANDA ANCHA

El estar conectado a Internet con banda ancha quiere decir que se dispone de un gran ancho de banda o, lo que es lo mismo, que se está conectado a Internet a alta velocidad. En la práctica, esto significa disponer de una conexión igual o superior a 128 Kbps.

El acceso a Internet mediante banda ancha y a bajo coste es un servicio relativamente reciente. De hecho, aunque las redes de televisión por cable ofrecían esta posibilidad desde hace tiempo, la introducción masiva de este tipo de accesos ha venido de la mano del servicio ADSL.

Los servicios de acceso a Internet en banda ancha más comunes son los siguientes:

- Acceso mediante ADSL
- Acceso mediante módem cable
- Acceso vía satélite
- Acceso vía radio LMDS
- Acceso vía circuito dedicado de datos

Por cierto, cuando se accede a Internet por línea telefónica o RDSI, es necesario disponer de la línea y luego contactar con un proveedor de acceso a Internet. Sin embargo, cuando se accede a Internet con banda ancha, el propio proveedor del servicio de banda ancha facilita el acceso a Internet, cuentas de correo e, incluso, espacio para la creación de páginas Web. Esto quiere decir que en estos casos no hace falta contratar con ningún otro proveedor de acceso a Internet. ([www.adsl.com](http://www.adsl.com), noviembre 2005)

CARACTERÍSTICA	TIPO DE ACCESO				
	Línea telefónica	Línea RDSI	ADSL	Cable módem	LMDS
Velocidad máxima	56K	64/128K	2M	2M	2M
Tipo de tarificación	Por tiempo	Por tiempo	Fijo al mes	Fijo al mes	Fijo al mes
Red soporte	RTB	RDSI	RTB/RDSI	TVcable	Radio
Tipo de medio	Compartido	Compartido	Dedicado	Compartido	Compartido
Tipo de módem	56K	RDSI	ADSL	Cable	LMDS
Equipo especial			Filtro	Filtro	E. radio
Seguridad	Baja	Baja	Alta	Media	Media
Eficiencia	Baja	Baja	Alta	Media	Media
Web hosting	Sí	Sí	Sí	No	No
Usuario/clave de acceso	Sí	Sí	No	No	No
Siempre conectado	No	No	Sí	Sí	Sí
Banda ancha	No	No	Sí	Sí	Sí

NOTAS:

- El equipamiento especial suele ser facilitado por el proveedor del servicio de acceso.
- RTB significa línea telefónica básica o línea telefónica normal.

Tabla 4.1 Comparación de las distintas formas de acceso a Internet  
([www.adsl.com](http://www.adsl.com), noviembre 2005)

### 4.3.1 Las ventajas de la banda ancha

La posibilidad de acceder a Internet con banda ancha está haciendo que surjan servicios que se aprovechen de la alta velocidad. Por ejemplo, la posibilidad de incorporar vídeo está dando paso a popularizar aplicaciones como televigilancia, teleformación o videoconferencia. Ver una imagen del negocio, una panorámica de la habitación donde están los niños (en la guardería o en casa) o celebrar una reunión familiar sin movernos de casa siempre ha sido posible, pero ahora está a nuestro alcance por muy pocos pesos.

Las ventajas principales de los servicios de acceso a Internet con banda ancha son las siguientes:

- **Alta velocidad.** Ofrece una velocidad de acceso a Internet de hasta 2 Mbps.
- **Siempre conectado.** No hace falta perder tiempo estableciendo la conexión. La conexión de banda ancha está siempre activa y funcionando.
- **Voz y datos simultáneamente.** Funciona de forma completamente independiente al servicio telefónico.
- **Tarifa plana.** Ofrece la posibilidad de disponer del servicio de acceso a Internet las 24 horas al día por un bajo precio fijo mensual.

*(adslinternautas.org , noviembre 2005)*

### 4.3.2 Acceso mediante ADSL

ADSL son las siglas de una nueva tecnología pensada para poder transmitir datos a alta velocidad (banda ancha) a través de los bucles de abonado de las líneas telefónicas. El bucle de abonado es el par de hilos de cobre que va desde la casa del usuario hasta la central telefónica y que se suele utilizar para disponer del servicio telefónico o de fax.

Aunque la tecnología ADSL permite velocidades de hasta 8 Mbps, la velocidad real que puede conseguir el usuario depende de la distancia del domicilio del usuario a la central telefónica del proveedor del servicio ADSL.

El significado de las siglas ADSL es Asymmetric Digital Subscriber Line, o 'Línea de Abonado Digital Asimétrica'. La letra A de asimétrico significa que no emplea el mismo ancho de banda para subir (transmisión usuario-red) que para bajar información (transmisión red-usuario). En la práctica, esto quiere decir que la mayoría de los recursos de la conexión se emplean en la bajada de información, como suele ser habitual en el uso de Internet.

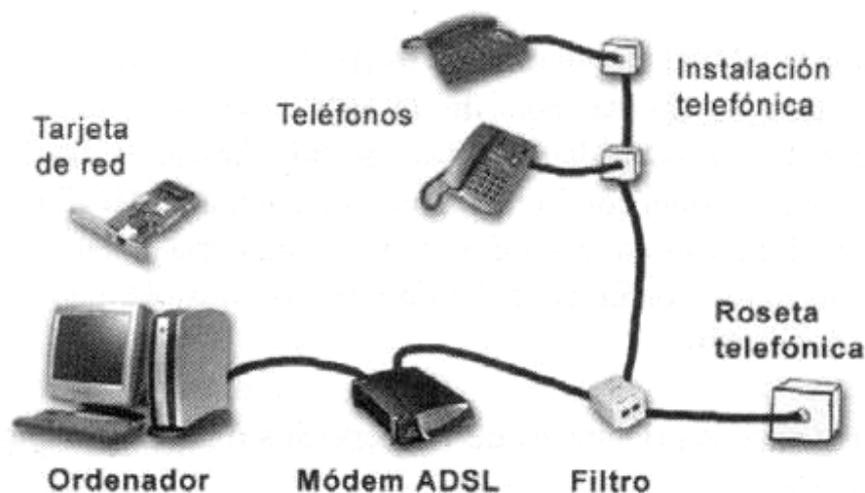


Figura 4.2 Instalación de un acceso ADSL  
(*adslinternautas.org*, noviembre 2005)

Los proveedores de los servicios ADSL pueden comercializar estos servicios de distintas formas: ofrecer tarifa plana con precios dependientes de la velocidad máxima contratada, ofrecer velocidad máxima con cuota mensual más cargo por volumen de tráfico, ofrecer cuota mensual más cargo por tiempo, etc.

Hay que tener en cuenta que las limitaciones de velocidades se fijan en las instalaciones del proveedor, no en el equipo del usuario. Por tanto, en general, un usuario podría cambiar la velocidad contratada sin cambiar su equipamiento, incluso, sin modificar su configuración.

Para instalar el servicio ADSL, se necesita disponer de un filtro (splitter o microfiltros) y un módem ADSL (ATU-R, ADSL Terminal Unit-Remote). Este módem ADSL ofrece

una salida de red Ethernet. Esto quiere decir que cualquier ordenador (que disponga de una tarjeta de red Ethernet) o punto de acceso Wi-Fi puede conectarse directamente al módem ADSL. (*adslinternautas.org*, noviembre 2005)

### 4.3.3 Acceso mediante módem cable

El módem cable es un dispositivo, módem, que permite el acceso a Internet una alta velocidad a través de las redes de televisión por cable. El sistema permite velocidades de hasta 40 Mbps, aunque por razones técnicas y comerciales, los proveedores suelen limitar este acceso a velocidades por debajo de 2 Mbps. Evidentemente, este servicio es propio de empresas de televisión por cable y como se puede suponer, la recepción de los canales de televisión no se ve afectada por la existencia del módem cable.

Es importante destacar que algunos operadores de cable no cuentan con un sistema de cable bidireccional, por lo que, en estos casos, el usuario necesita disponer además de una línea telefónica. La información usuario-Internet sube por la línea telefónica, mientras que la información Internet-usuario baja por la red de cable a alta velocidad. En este caso, al sistema se le conoce como TRI (Telephony Return Interface, 'Interfaz de Retorno Telefónico'). Las redes de televisión digital por satélite o por radio suelen utilizar este sistema.

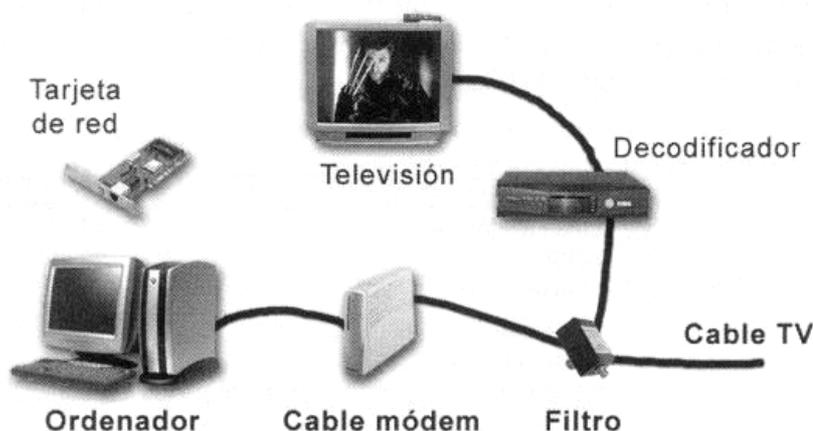


Figura 4.3 Instalación de un acceso por cable modem.  
([www.intercable.net](http://www.intercable.net), noviembre 2005)

TIPO DE INFORMACIÓN	TAMAÑO TÍPICO
Mensaje de correo electrónico	2,2 KB
Documento de 20 páginas	44 KB
Imagen gráfica	330 KB
Un minuto de audio	475 KB
Un minuto de vídeo	2.400 KB

Tabla 4.2 Tamaño de las informaciones

[www.intercable.net](http://www.intercable.net), noviembre 2005)

#### 4.3.4 Acceso por satélite

Si se vive en un lugar remoto donde no se tiene acceso a la mayor parte de las nuevas tecnologías, pero se necesita de una conexión a Internet a alta velocidad, la solución apropiada es la conexión por satélite. La conexión por satélite sólo necesita tener una vista despejada hacia el cielo del sur (o del norte, si se encuentra en el hemisferio sur).

El satélite puede ofrecer velocidades de hasta 400 Kbps sin necesidad de disponer de línea telefónica, o velocidades incluso mayores para aquellos sistemas que se apoyan en el uso de la línea telefónica para la transmisión usuario-Internet.

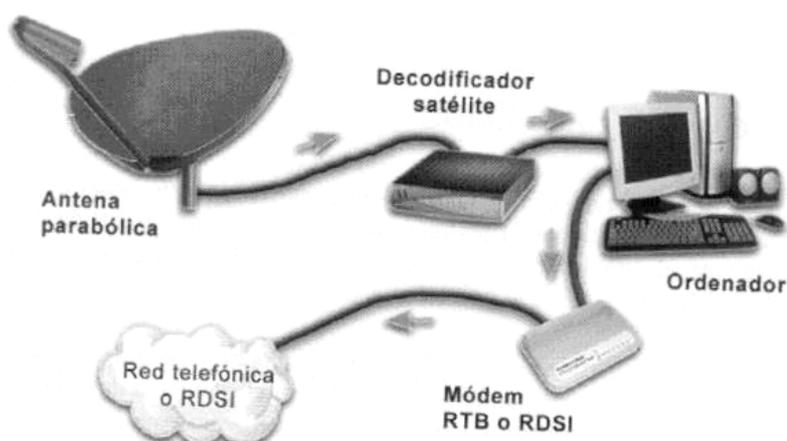


Figura 4.4 Instalación de un acceso por satélite

[www.intercable.net](http://www.intercable.net), noviembre 2005)

El usuario necesita disponer de una antena parabólica, un módem especial (decodificador) para este tipo de conexiones y el software correspondiente. Todo este equipamiento suele ser proporcionado por el proveedor del servicio.

Existen tres proveedores típicos de este tipo de servicios: las operadoras de telecomunicaciones, las empresas de televisión por satélite y las empresas especializadas en este tipo de conexión para Internet (*adslinternautas.org*, noviembre 2005)

MODO DE ACCESO	VELOCIDAD DE TRANSMISIÓN	TIEMPO NECESARIO
Módem sobre GSM	9.600 bps	1 h 56' 30"
Red telefónica básica	56 Kbps	2' 26"
Acceso básico RDSI	64 Kbps	2' 8"
Dos canales de RDSI	128 Kbps	1' 4"
ADSL 256 Kbps	256 Kbps	32"
ADSL 512 Kbps	512 Kbps	16"
UMTS 1 Mbps	1 Mbps	8"
ADSL 2 Mbps	2 Mbps	4"
ADSL máximo	8 Mbps	1"
VDSL 55 Mbps	55 Mbps	0,1"
Circuito dedicado	155 Mbps	0,05"

*Tabla 4.3 Comparación de tiempos y de tecnologías*

*[www.intercable.net](http://www.intercable.net), noviembre 2005)*

#### **4.3.5 Acceso vía radio LMDS**

La tecnología LMDS (Local Multipoint Distribution Service o 'Servicio Local de Distribución Multipunto') permite un acceso a Internet de banda ancha (hasta 8 Mbps) mediante el establecimiento de un enlace de radio bidireccional. Por el mismo enlace pueden facilitarse servicio de telefonía, datos y vídeo.

La particularidad de LMDS es que el enlace de radio tiene que tener una visibilidad directa entre la antena parabólica a instalar en el domicilio del usuario y la estación base

del operador del servicio. La estación base puede tener un alcance de hasta 7 kilómetros para un servicio sin restricciones o hasta 20 Km. con un menor ancho de banda. Una única estación base puede gestionar las comunicaciones de más de 4.000 usuarios.

*(adslinternautas.org , noviembre 2005)*

#### **4.3.6 Acceso mediante circuitos de datos**

Otras de las posibilidades de acceder a Internet es mediante circuitos de datos. En este caso hemos llamado circuito de datos a las líneas punto a punto y a los circuitos de las redes públicas de transmisión de datos. Esta solución suele ser adecuada para organizaciones que desean ofrecer información a la red o para aquellas empresas que desean conectar una red de área local (o Intranet) a Internet.

- **Acceso mediante circuitos punto a punto.** A este tipo de circuitos también se les conoce como circuitos dedicados o circuitos alquilados. Un circuito punto a punto es una línea dedicada exclusivamente a mantener una conexión entre dos ordenadores. Estos circuitos se alquilan generalmente a las compañías telefónicas, encargándose éstas de utilizar el medio más adecuado en cada caso para su constitución (por ejemplo, fibra óptica, par de hilos telefónicos, microondas, etc.). Una conexión de este tipo suele tener una velocidad de transmisión de entre 64 Kbps y 2 Mbps, aunque también son normales velocidades superiores, pudiéndose llegar a los 622 Mbps. Los circuitos punto a punto no tienen tiempo de establecimiento de conexión, no tienen una limitación de velocidad y no comparten el acceso con otros usuarios, por lo que resulta ser el medio más rápido y eficaz de conectarse a Internet pero también es el más caro, por lo que en ocasiones puede convertirse en un lujo innecesario. En general, este tipo de conexiones es propio de grandes organizaciones o de pequeñas empresas relacionadas con Internet.

- **Mediante una red pública de transmisión de datos** (Frame Relay, IP, etc.). Ésta es una solución intermedia entre el acceso por línea conmutada (línea telefónica o RDSI) y línea punto a punto. Estas redes tienen tiempos de establecimiento de conexión muy cortos, ofreciendo además un bajo índice de error a un precio inferior al de un circuito punto a punto. En este caso la velocidad máxima suele ser de hasta 512 Kbps. Dado el coste del equipamiento de usuario necesario, esta solución suele ser más apropiada para empresas que para usuarios particulares.

*(adslinternautas.org , noviembre 2005)*

#### **4.4 LA CONEXIÓN DE WI-FI CON INTERNET**

La conexión de una red inalámbrica Wi-Fi con Internet se lleva a cabo a través del punto de acceso. En el mercado existen distintos modelos de puntos de acceso con distintas características. No obstante, las facilidades que puede presentar un punto de acceso para su conexión a Internet son las siguientes:

- Disponer de un puerto 10/100Base-T (RJ-45 o Ethernet, también conocido como uplink port) por donde poder conectarse al modem ADSL, al módem cable o al hub o switch de la red local cableada que ya está conectada a Internet.
- Disponer internamente de la funcionalidad hub. Esto facilitaría de dos a cuatro puertos exteriores 10/100Base-T (RJ-45 o Ethernet) por donde poder conectarse a la red local cableada con conexión a Internet, o al módem ADSL/cable. Adicionalmente, esta funcionalidad de hub permitiría crear una pequeña red local cableada de dos a cuatro ordenadores. Si se necesitase de más de cuatro puertos, siempre se puede utilizar otro hub o switch y conectarlo al punto de acceso para extender la red cableada.
- Un puerto serie RS-232 a donde se le puede conectar un módem tradicional de red telefónica (V90 a 56 Kbps). Esta conexión a Internet a baja velocidad podría ser utilizada como acceso principal a Internet o como acceso secundario de

seguridad en el caso de que falle la conexión principal de banda ancha (ADSL o módem cable).

- Disponer internamente de un módem V90 (56 Kbps) de línea telefónica. En este caso, el punto de acceso muestra al exterior un conector RJ-11 (el conector telefónico al que se enchufan los teléfonos normales) que hay que conectar a la línea telefónica. Igual que en el caso anterior, esta conexión a Internet de baja velocidad podría ser utilizada como acceso secundario a Internet.

Esto quiere decir que la conexión de una red Wi-Fi a Internet pasa, generalmente, por conectar el punto de acceso a una red cableada que ya dispone de acceso a Internet o por conectarlo a un módem ADSL o módem cable.

Aparte de llevar a cabo esta conexión, y configurarla adecuadamente, existen puntos de acceso que incluyen la funcionalidad de router. Esto quiere decir que el punto de acceso podría ser configurado, por ejemplo, con unas mejores medidas de seguridad (configuración de filtros), para compartir más de una dirección IP pública entre sus usuarios, para permitir que uno de sus ordenadores sea un servidor Web, para resolver el problema de acceso a determinadas aplicaciones de Internet, etc.

([www.intercable.net](http://www.intercable.net), noviembre 2005)

#### **4.4.1 Instalar la conexión entre Wi-Fi e Internet**

Las interconexiones entre un punto de acceso Wi-Fi y un módem ADSL/Cable pueden diferir levemente de unos fabricantes a otros; no obstante, los conceptos básicos son los mismos.

La interconexión de la red Wi-Fi con el módem ADSL/cable consiste en interconectar ambos equipos mediante un cable 10/100Base-T (RJ-45). Para ello, primeramente hay que comprobar que tanto la red Wi-Fi como la conexión ADSL/cable están instaladas y funcionando correctamente de forma independiente.

Si la conexión ADSL/cable está funcionando conectada directamente a un ordenador, el trabajo consiste en sustituir el ordenador por el punto de acceso. Esto supone configurar el punto de acceso con los mismos parámetros con los que está configurado el ordenador y cambiar la conexión del cable del ordenador al punto de acceso.

Hay que tener presente que estas desconexiones y conexiones son mucho más seguras si se hacen habiendo apagado previamente los equipos a los que hay que desconectar o conectar los cables. ([www.intercable.net](http://www.intercable.net), noviembre 2005)

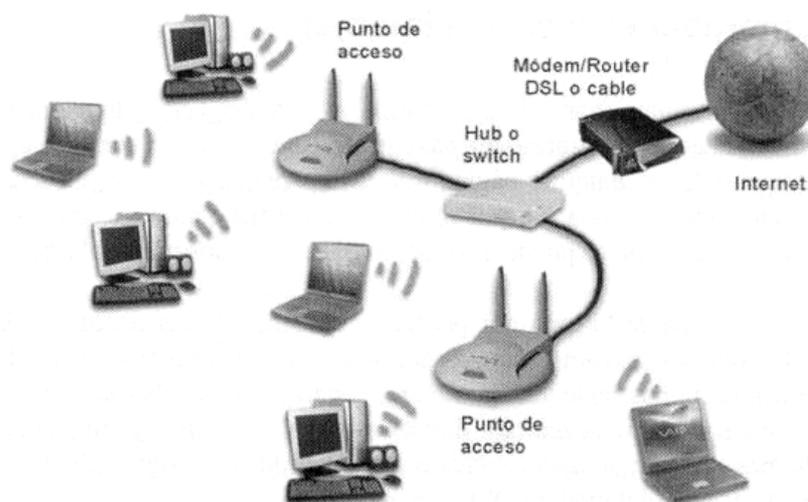


Figura 4.5 Conexión a Internet con banda ancha

([www.intercable.net](http://www.intercable.net), noviembre 2005)

#### 4.4.2 Configurar la conexión en el punto de acceso

Para configurar el punto de acceso, se debe ejecutar el software de utilidad que acompaña a los equipos Wi-Fi (suele venir en un CD). Este software permite verificar las conexiones, modificar las configuraciones y, en general, gestionar las comunicaciones de la unidad Wi-Fi. Cada fabricante llama a este software de una manera. Por ejemplo, Sony lo llama Wireless Palette ('Paleta Inalámbrica') y Orinoco lo llama Client Manager ('Gestor del Cliente').

Por cierto, es siempre una buena idea acceder al Web del fabricante de los dispositivos Wi-Fi para comprobar si existe una versión más moderna de los controladores, firmware y software de utilidad de estos dispositivos Wi-Fi. Si así fuera, es recomendable instalar las versiones más modernas de la Web antes que las versiones más antiguas del CD.

Cuando se pone en marcha el software de configuración del punto de acceso, y una vez introducida la identificación del punto de acceso y su clave, habrá que buscar la opción de configuración del puerto Ethernet. Generalmente, se muestra un menú donde simplemente hay que elegir la opción general utilizada (ADSL, módem cable, red de área local o conexión local), o bien, se muestran las opciones a configurar (números IP, etc.). Para terminar, se sale del programa de configuración aceptando los cambios. Esto hará que la nueva configuración se transmita al punto de acceso y todo quede listo para utilizar el acceso a Internet. ([www.intercable.net](http://www.intercable.net), noviembre 2005)

#### **4.4.3 Comprobar el acceso a Internet**

Para comprobar si el acceso a Internet está funcionando correctamente, simplemente hay que abrir un navegador (Internet Explorer, por ejemplo) y ver si se puede acceder a cualquier página Web. Si las páginas Web se pueden ver sin problemas, perfecto, esto funciona. Si, por el contrario, se tiene como respuesta el famoso mensaje de que la página no se puede mostrar, entonces tenemos un problema.

Antes de darlo todo por perdido, conviene intentar acceder a distintas páginas. Es posible que nos hayamos equivocado a la hora de introducir el nombre de la página. Si aun así, seguimos teniendo problemas, debemos comprobar la conexión a Internet desde ese ordenador conectándolo directamente al módem ADSL/cable. Si no funciona, debemos configurar dicha conexión en el ordenador siguiendo las instrucciones de la guía de usuario del módem ADSL/cable.

Si el ordenador puede acceder a Internet desde el módem ADSL/cable pero no desde la conexión inalámbrica y, por otro lado, la conexión inalámbrica de este ordenador funciona adecuadamente, sólo nos quedan dos puntos por comprobar: o el cable de conexión entre el punto de acceso y el módem no es el correcto o no está bien conectado, o el punto de acceso no está bien configurado. Compruebe todos estos términos.

En cuanto al cable, existen dos tipos de cables Ethernet categoría 5 (RJ-45): cruzado y no cruzado. Los cables de tipo no cruzados no suelen tener ningún tipo de marca mientras que los de tipo cruzado suelen tener una marca especial, por ejemplo, una marca negra donde se puede leer Crossover, Xover o similar. Asegúrese que está utilizando un cable Ethernet categoría 5 (RJ-45) no cruzado para conectar el módem ADSL/cable con el punto de acceso.

Por último, si tiene alguna duda en la configuración del punto de acceso, consulte el manual de usuario del equipo. ([www.intercable.net](http://www.intercable.net), noviembre 2005)

## **4.5 LA CONFIGURACIÓN DE UN ROUTER**

Un router es un equipo que sirve de intermediario entre los ordenadores de una red local (inalámbrica o cableada) y una red exterior (típicamente Internet). Esto es precisamente lo que hacen los puntos de acceso, por lo que es habitual que estos equipos ofrezcan determinadas funcionalidades de los routers. ([www.intercable.net](http://www.intercable.net), noviembre 2005)

### **4.5.1 Las distintas direcciones IP**

Todos los ordenadores o equipos que forman parte de una red local tienen que disponer de una dirección IP. Esta dirección IP es la que identifica al ordenador para todas sus

comunicaciones. A las direcciones IP que utilizan los equipos de una red local se las conoce como dirección IP privada.

Las direcciones IP privadas tienen la misma apariencia que las direcciones IP de Internet. A estas últimas se las conoce como direcciones IP públicas. En ambos casos, las direcciones IP están formadas por una cadena de cuatro cifras separadas por un punto. Cada una de esas cifras puede tomar un valor entre 0 y 255. Por ejemplo, 10.13.163.1 es una dirección IP. Sin embargo, aunque ambos tipos de direcciones tengan la misma apariencia, se trata de direcciones independientes. Las direcciones IP privadas son asignadas arbitrariamente por el administrador o usuario de la red local, mientras que las direcciones IP públicas son asignadas por las autoridades de Internet (por IANA).

Las direcciones IP privadas están reguladas por el documento RFC 1918 (<ftp://ftp.ufl.edu/net/rfc>). En este documento se define que, para que una dirección IP privada sea compatible con Internet debe estar dentro de los siguientes rangos:

Clase A. 1 0.0.0.0 a 10.255.255.255

Clase B. 172.16.0.0 a 172.31.255.255

Clase C. 192.168.0.0 a 192.168.255.255

Estas direcciones no son reconocidas por la red Internet. Esto quiere decir que ningún paquete de datos que tenga una de estas direcciones como identificación origen o destino puede progresar dentro de Internet. Esta particularidad impide que las direcciones IP privadas sean visibles directamente desde Internet. Por tanto, el administrador de una red de área local es libre de utilizar cualquiera de estas direcciones dentro de su red.

Cuando una red local está conectada a Internet, su router es el que se encarga de traducir las direcciones IP privadas a públicas, y viceversa, para que se pueda llevar a cabo la comunicación. El sistema que hace esto se conoce como NAT (Network Address Translation o 'Traducción de Direcciones de Red'). Por tanto, un router debe tener una

dirección IP privada (IP LAN) que lo identifique dentro de la red local y una dirección IP pública (IP WAN) que lo identifique en Internet.

Por último, el router tiene que saber a qué dirección de Internet tiene que enviar toda la información que salga de la red local. Esta dirección coincide con la dirección IP del router del proveedor de acceso (IP router remoto).

Por tanto, tenemos las siguientes direcciones configuradas en un router:

- **IP interna del router**, también conocida como dirección privada del router o IP LAN. Es la dirección IP que identifica al router dentro de la red local. Desde el punto de vista de los ordenadores de la red, la dirección IP interna del router es su puerta de enlace con Internet. Generalmente, la dirección interna del router suele ser la primera dirección IP del rango de direcciones privadas. Por ejemplo, 172.26.0.1 o 192.168.0.101.
- **IP externa del router**, también conocida como dirección IP pública del router o dirección IP WAN. Es la dirección IP con la que se puede acceder al router desde Internet. No obstante, suele ser normal que el router esté configurado con unos filtros para que, aun conociendo esta dirección, nadie ajeno pueda acceder a este equipo. Esta dirección suele coincidir con la dirección IP pública facilitada por el proveedor de acceso.
- **IP Router remoto**. Es la dirección IP del router de la red del proveedor de acceso a Internet (ISP). Este valor puede generarse automáticamente.

Aparte de las direcciones anteriores configuradas en el router, existen las direcciones IP de los ordenadores conectados al router. Estas direcciones se configuran en cada ordenador, aunque también pueden asignarse automáticamente a través de la facilidad DHCP. En este caso, el router debe tener habilitado el servicio DHCP.

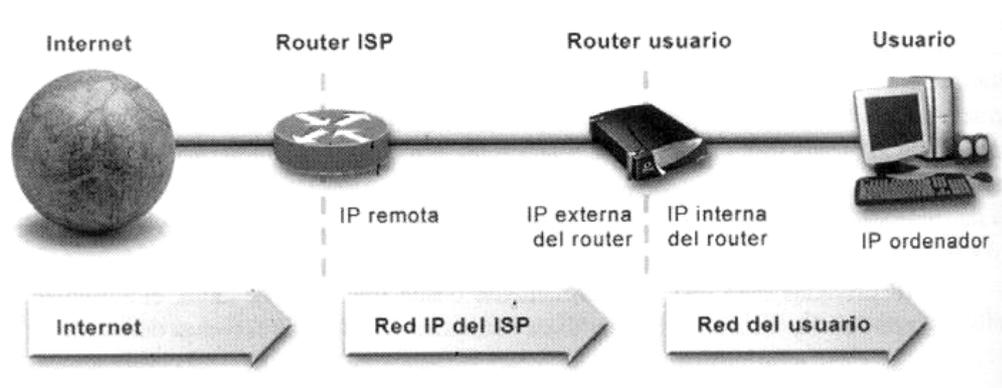


Figura 4.6 Las distintas direcciones IP de una conexión DSL

([www.intercable.net](http://www.intercable.net), noviembre 2005)

Ordenador	Router (LAN)	Router (WAN)	Router remoto
IP privada del ordenador p.e. 192.168.0.2 ó 3, 4, ...	IP privada p.e. 192.168.0.1	IP pública	(IP pública AND máscara)+2

Tabla 4.4 Configuración de direcciones IP

([www.intercable.net](http://www.intercable.net), noviembre 2005)

## 4.6 DHCP

Hemos visto que los ordenadores de una red de área local conectados a un router disponen de direcciones IP privadas. Estas direcciones IP privadas deben configurarse en cada uno de los ordenadores de la red local. Como este trabajo de configuración puede ser tedioso e, incluso, dar lugar a confusión conforme la red va adquiriendo un tamaño mayor, se pensó en un modo de asignar esta dirección IP privada a cada ordenador de forma automática. El sistema que hace esto se conoce como DHCP (Dynamic Host Configuration Protocol o 'Protocolo de Configuración Dinámica del Host').

La técnica DHCP le permite al router asignar direcciones IP de forma automática a los ordenadores conectados a él. Estas direcciones pueden ser públicas (que forman parte de Internet) o privadas (invisibles a Internet). En cualquier caso, a este modo de asignar

direcciones se le conoce como direccionamiento dinámico. En caso contrario, estaríamos hablando de direccionamiento estático.

Para utilizar este modo de asignación de direcciones, hay que habilitar el modo DHCP, tanto en el router, como en cada ordenador de la red. En caso contrario, habría que configurarle a cada ordenador su dirección IP correspondiente. Esta dirección IP sería utilizada sólo y exclusivamente por cada ordenador; por ello, se la conoce como dirección IP estática o dirección IP fija.

Por cierto, DHCP asigna las direcciones IP en el momento en el que se enciende el ordenador. Un mismo ordenador puede tener distintas direcciones IP cada vez que se enciende. No obstante, si interesase, DHCP puede configurarse para que le asigne siempre la misma dirección IP a un mismo ordenador. En caso contrario, lo hará de forma aleatoria.

Por último, DHCP puede utilizarse también para asignar las direcciones de los DNS. Esto evitaría tener que asignar estas direcciones en cada ordenador.

(<http://www.bandaanchoa.st/foros.php?temid=781904>, diciembre 2005)

## **4.7 NAT**

Tradicionalmente, todo ordenador (o cualquier otro equipo) conectado a Internet necesita disponer de una dirección IP en exclusiva. Esta dirección IP es la que identifica a este ordenador dentro de la red Internet. En el sistema de numeración IP actual (IPv4) sólo existen unos 4.300 millones de números IP posibles. Esta escasez de números IP ha llevado a buscar un método que permita ahorrar números IP hasta que se implante la nueva versión del protocolo IP conocida como IPv6. Esta nueva versión aportará, entre otras cosas, una cantidad de números IP exageradamente superior a la actual.

La única forma de ahorrar números IP es haciendo que varios ordenadores (o equipos en general) utilicen la misma dirección IP pública en sus conexiones con Internet. La tecnología que permite hacer esto se conoce con el nombre de NAT (Network Address Translation o 'Traducción de Direcciones de Red').

La funcionalidad NAT suele estar incluida dentro del router de la red local. El router se conecta a Internet utilizando una única dirección IP (IP pública) y permite, mediante NAT, que todos los ordenadores de la red local puedan hacer un uso simultáneo de dicha conexión.

Aplicación	Protocolos y puertos
Servidor FTP	In TCP 21
Servidor POP3	In TCP 110
Servidor SMTP	In TCP 25
Servidor Telnet	In TCP 23
Servidor Web	In TCP 80
NetMeeting	TCP 1503, TCP 1720
mIRC	TCP 1080, TCP 113
Aim Talk	Out TCP 4099, In TCP 5190
Go2Call	In UDP 2090 y 2091, In TCP 2090
Internet Phone	Out UDP 22555
Napster	Out TCP 6699, In TCP 6699
Quick time 4 Server	In TCP 6970, In UDP 6970 - 7000
Real Audio	Out TCP 7070, In UDP 6970 - 7170
Delta Force	Out UDP 3568, In TCP 3100 3999, Out TCP 3100 3999, In UDP 3100 3999, Out UDP 3100 3999
Fighter Age II	In TCP 50000 - 50100, In UDP 50000 - 50100
Quake II	In UDP 27910
CarbonCopy 32 (host)	In TCP 1680, In UDP 1023-1679
Laplink (host)	In TCP 1547
PCAnywhere (host)	In TCP 5631, In UDP 5632, In UDP 22
Windows 2000 Terminal Server	In TCP 3389, In UDP 3389

Puede conseguir más información sobre aplicaciones y puertos en [http://practicallynetworked.com/sharing/app\\_port\\_list.htm](http://practicallynetworked.com/sharing/app_port_list.htm).

*Tabla 4.5 Ejemplos de aplicaciones y puertos asociados*

(<http://www.bandaancha.st/foros.php?temid=781904>, diciembre 2005)

NAT se aprovecha de que en las cabeceras de los paquetes que se comunican entre ordenador y servidor siempre va la identificación de la dirección de origen, puerto de origen, dirección de destino y puerto de destino. Las direcciones son los números IP de

los equipos origen y destino y los puertos son unos números que sirven para identificar cada una de las comunicaciones simultáneas que puede tener un mismo equipo.

Lo que hace el router que tiene implementado NAT es que cambia las direcciones IP origen internas de cada ordenador por la dirección IP pública de que dispone. Para Internet todas las comunicaciones procedentes de esa red local provienen del mismo equipo, el router. Para poder identificar el tráfico de cada ordenador de la red, se utiliza el número de puerto. El router se encarga de hacer la conversión del número del puerto para poder identificar a cada equipo. Esto lo hace mediante NAPT (Network Address Port Translation o 'Traducción del Puerto de Dirección de Red').

(<http://www.bandaancha.st/foros.php?temid=781904,diciembre> 2005)

Preámbulo	Dirección IP destino	Dirección IP origen	Tipo de trama	Datos	PAD (opcional)	Chequeo de error	Extensión (opcional)
8 bytes	6 bytes	6 bytes	2 bytes	De 46 a 1500 bytes		4 bytes	

*Tabla 4.6 Esquema de un paquete de datos Ethernet*

(<http://www.bandaancha.st/foros.php?temid=781904,diciembre> 2005)

#### 4.7.1 El problema con ciertas aplicaciones

El router que tiene NAT activado realiza una conversión de las direcciones IP y puertos analizando exclusivamente la cabecera de los paquetes. La cabecera es donde se supone que deben estar las direcciones IP y puertos origen y destino de la comunicación. La problemática surge cuando se tienen aplicaciones de Internet como, por ejemplo, NetMeeting, que incluyen información de la dirección IP dentro del área de datos del paquete. En este caso, estas direcciones IP no son analizadas ni traducidas por el router, por lo que estas comunicaciones acaban perdiéndose.

La forma ideal de arreglar este problema es hacer que NAT analice también la parte de datos y traduzca las direcciones que aquí aparezcan. Pero esto no es sencillo hacerlo.

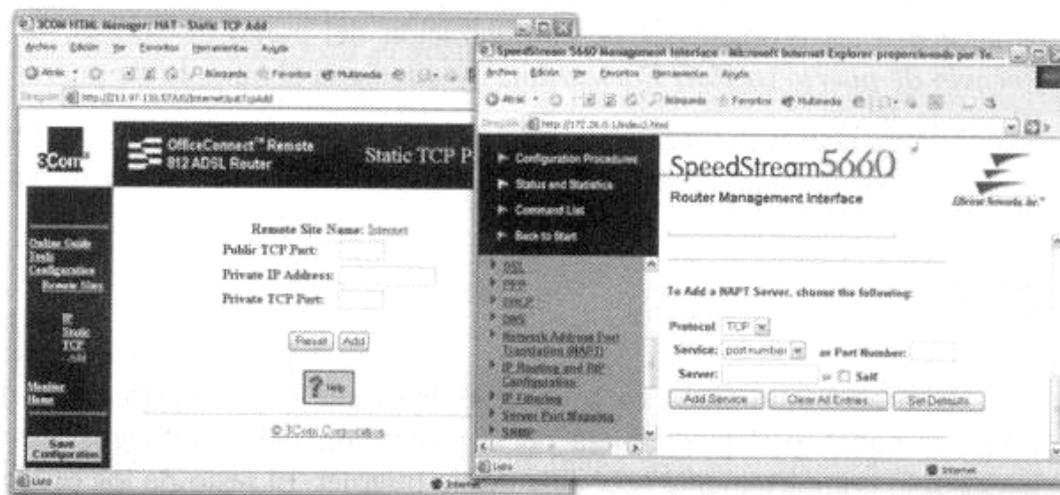


Figura 4.7 Configuración NAT el router Efficient SS 5660 y 3Com 812  
(<http://www.bandaancha.st/foros.php?temid=781904>, diciembre 2005)

La solución alternativa se basa en que cada aplicación de Internet suele utilizar siempre el mismo número de puerto. Por ejemplo, un servicio Web suele utilizar el puerto 80, Telnet el 23 o el correo POP3 el 110. La solución consiste en decirle al router (NAT) que todas las comunicaciones que vengan de Internet utilizando un número concreto de puerto las dirija a un ordenador concreto dentro de la red local. De esta forma podemos tener un servidor Web en uno de los ordenadores de la red local o establecer una comunicación de NetMeeting. La característica que permite configurar esto se llama reenvío de puerto.

(<http://www.bandaancha.st/foros.php?temid=781904>, diciembre 2005)

#### 4.7.2 Reenvío de puerto

La característica de reenvío de puerto (Port Forwarding en inglés) permite, al igual que DMZ, que un ordenador de la red pueda hacer las funciones de servidor. Al reenvío de puerto también se le conoce como servidor virtual (Virtual Server). La diferencia con DMZ es que el reenvío de puerto abre a Internet uno o más puertos, pudiendo

redireccionar cada puerto a ordenadores distintos de la red. Esto permite facilitar un acceso limitado a múltiples ordenadores. Por ejemplo, se puede abrir el puerto 20 y 21 a un ordenador para convertirlo en un servidor FTP, el puerto 25 y 110 a otro para convertirlo en servidor de correo, etc.

Los ordenadores a los que se les van a reenviar todas las llamadas a un puerto deben disponer de una dirección IP privada fija. Quiere esto decir que no pueden estar configurados para obtener una dirección IP automáticamente del servidor DHCP del punto de acceso. Es válida cualquier dirección dentro del rango de IP privadas. Como puerta de enlace debe especificarse la dirección IP privada del router.

La configuración de la característica de reenvío de puerto es similar a la de DMZ: se accede a las propiedades de configuración del punto de acceso, se busca la opción Reenvío de puerto (o Port Forwarding) y se asigna el número de puerto a cada dirección IP que se desee. (<http://www.bandaancho.st/foros.php?temid=781904,diciembre> 2005)

## 4.8 DMZ

Este acrónimo significa zona desmilitarizada (Demilitarized Zone). Un ordenador DMZ es aquél que queda fuera de la protección del cortafuegos (firewall) de la red, haciéndolo completamente accesible desde Internet. El resto de los ordenadores no DMZ permanecen protegidos detrás del cortafuego.

El ordenador DMZ debe disponer de una dirección IP privada fija, mientras que el resto, si se desea, pueden disfrutar de las ventajas del direccionamiento dinámico que ofrece el servidor DHCP del punto de acceso. De la misma forma, la dirección IP privada del punto de acceso debe estar configurada en el ordenador DMZ como su puerta de enlace (gateway).

Para configurar el ordenador DMZ en el punto de acceso, simplemente se accede a su configuración, se elige la opción DMZ Host, o similar, y se le especifica el número IP privado del ordenador DMZ.

(<http://www.bandaanchoa.st/foros.php?temid=781904,diciembre> 2005)

#### **4.8.1 Filtros**

Un cortafuego (firewall) evita que desde fuera de la red se pueda acceder indiscriminadamente a los ordenadores protegidos por el cortafuegos. Otra de las posibilidades del cortafuegos es impedir que determinados ordenadores de la red local puedan acceder al exterior. Algunos puntos de acceso ofrecen la posibilidad de filtrar tanto el tráfico de salida como el de entrada a la red. Además, este filtrado puede restringirse a determinados ordenadores, a determinados contenidos o a determinados servicios.

Un tipo de filtro que puede ser interesante configurar es el que impide a determinados ordenadores de la red acceder a Internet. Las limitaciones pueden hacerse tanto a ordenadores identificados por su dirección IP, como a ordenadores identificados por su dirección MAC. La dirección MAC identifica al adaptador de red y no es modificable por el usuario, por lo que resulta más segura que la dirección IP.

Otro tipo de filtro posible es el que se conoce como filtro de contenidos (Content filters). Los filtros de contenidos impiden la utilización de servicios (páginas Web, correos electrónicos o chats) que contengan determinadas palabras. Esto se utiliza fundamentalmente para impedir el acceso a servicios con contenido de sexo, juegos, etc. Por ejemplo, se puede configurar el filtro con palabras como casino, sexo, viagra porno, etc. A veces, estos filtros pueden configurarse para estar activos a determinadas horas o para determinados ordenadores.

(<http://www.bandaanchoa.st/foros.php?temid=781904,diciembre> 2005)

#### 4.8.2 Máscara de subred

La máscara de subred es una forma de poder definir e identificar redes secundarias (subredes) dentro de una red mayor. Mediante este procedimiento se puede determinar fácilmente a qué subred pertenece una dirección IP.

Una dirección IP puede descomponerse en dos partes: la parte que identifica a la red, dirección de red, y la parte que identifica al nodo dentro de esa red. Se le llama nodo a cualquier ordenador o equipo (router, host, cámaras IP, etc.) conectado a Internet y que tiene una dirección IP propia.

Una dirección IP (IPv4) contiene 32 bits (cuatro cifras de 8 bits cada una). Si una red local va a tener un máximo de 256 usuarios, sólo necesita 8 bits ( $2^8 = 256$ ) para identificar al ordenador de cada usuario. El resto de bits, 24, son bits que identifican a la red (la dirección de red).

Número de usuarios	Máscara en decimal	Máscara en hexadecimal	Bits de la máscara	Ejemplo de rango direcciones válidas
1 + el router	255.255.255.252	FFFFFFFC	30	x.x.x.1 / x.x.x.2
5 + el router	255.255.255.248	FFFFFFF8	29	x.x.x.1 / x.x.x.6
13 + el router	255.255.255.240	FFFFFFF0	28	x.x.x.1 / x.x.x.14
29 + el router	255.255.255.224	FFFFFFE0	27	x.x.x.1 / x.x.x.30
61 + el router	255.255.255.192	FFFFFFC0	26	x.x.x.1 / x.x.x.62
125 + el router	255.255.255.128	FFFFFF80	25	x.x.x.1 / x.x.x.126
253 + el router	255.255.255.000	FFFFFF00	24	x.x.x.1 / x.x.x.254

*Tabla 4.7 Máscaras típicas de subredes*

(<http://www.bandaancho.st/foros.php?temid=781904,diciembre> 2005)

En este ejemplo, los equipos que intervienen en el enrutamiento de los paquetes de datos de la red local no necesitan analizar los 32 bits de la dirección de cada paquete para saber cuál es su destino; con analizar 8 bits, sería suficiente. Si tenemos en cuenta que cada paquete sólo contiene unos cientos de bytes, podemos suponer la gran cantidad de trabajo que se ahorran los equipos al no tener que analizar los bits de la dirección de red.

Los bits de la dirección de red se configuran mediante lo que se conoce como máscara de red o máscara de subred.

Si la dirección IP 150.215.017.009 fuese una de las direcciones del ejemplo de red anterior, la cifra que identifica al nodo es 009; el resto, 150.215.017, es la dirección de red. Si escribimos esto en binario, la dirección IP del ejemplo sería la siguiente:

100101 10.1 10 101 1 1.00010001.0000100 1

La parte que identifica a la red sería la siguiente:

100101 1 0.1 10101 1 1.00010001 (150.215.017)

y la parte que identifica al nodo sería esta otra:

00001001 (009)

La máscara de subred es un número binario formado por tantos unos como bits tenga la dirección de red y tantos ceros como bits tenga la identificación del nodo. En el ejemplo, la máscara de subred sería:

11111111.11111111.11111111.00000000 o lo que es lo mismo 255.255.255.0

Esta forma de representar la máscara permite averiguar la dirección de la red y del nodo simplemente haciendo una operación Y lógica (and) con el número de la máscara y la dirección IP. Este tipo de operaciones son extremadamente sencillas de realizar para cualquier equipo electrónico.

(<http://www.bandaancha.st/foros.php?temid=781904>, diciembre 2005)

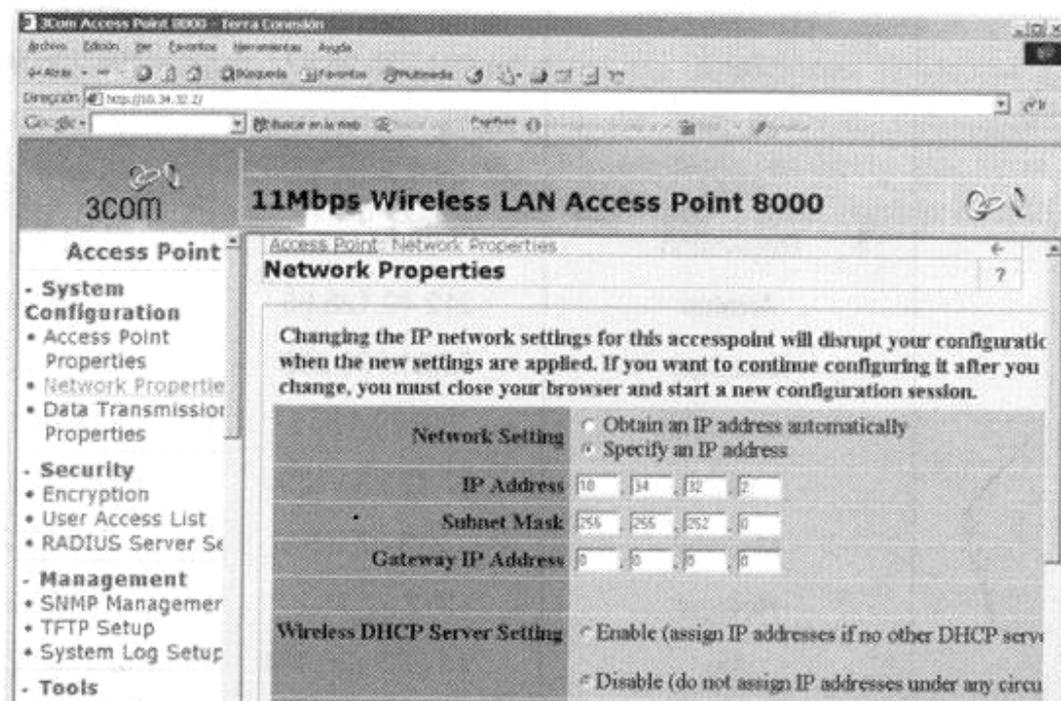


Figura 4.8 Configuración de la máscara de subred

(<http://www.bandaancha.st/foros.php?temid=781904>, diciembre 2005)

## 4.9 DNS

Las siglas DNS significan Sistema de Nombres de Dominio y provienen del inglés Domain Name Server. Lo que hace el sistema de nombres de dominio es traducir los nombres de dominio (de la forma `www.telefonica.mx`) a direcciones IP (de la forma `194.224.55.24`). Esta traducción la llevan a cabo los servidores DNS. Cuando se configura un DNS lo que se introduce es la dirección IP del servidor DNS que va a realizar la traducción.

Como se sabe, los equipos de la red Internet no entienden de nombres de dominio, lo único que entienden es de direcciones IP. Los nombres de dominio fueron creados para que a las personas nos fuese más fácil el uso de Internet. Por tanto, cuando una persona introduce un nombre de dominio en su navegador, lo primero que hace el navegador es averiguar a qué dirección IP le corresponde. A continuación el navegador establece la

comunicación con esa dirección IP. Las bases de datos que relacionan nombres de dominios y direcciones IP se encuentran en los DNS.

Proveedor de acceso	DNS primario	DNS secundario
Telefónica de España	194.179.1.100	194.179.1.101
Telefónica Data	194.224.52.36	194.224.52.37
Terra	194.235.96.87	194.235.96.88
Jazztel	212.106.192.250	212.106.192.251
Uni2	62.36.193.72	62.36.220.75
Retevisión	62.81.0.1	62.81.16.197
Arrakis	212.49.128.65	212.49.128.66
Eresmas	62.81.160.250	62.81.16.197
Supercable	212.79.128.3	212.79.128.
Ono	62.42.230.135	62.42.230.136
Madritel	213.37.2.5	213.37.2.6
Retecal	212.22.34.2	212.22.34.7
Alo	213.250.128.144	213.250.128.150
Able	212.97.163.3	212.97.163.4

*Tabla 4.8 Ejemplos de servidores de nombres de dominio*

(<http://www.bandaanchoa.st/foros.php?temid=781904>, diciembre 2005)

Dado que el número de nombres de dominios de toda la red Internet es muy grande, sería imposible que un solo servidor DNS pudiera atender todas las peticiones.

En Internet existen un gran número de servidores DNS estructurados de forma jerárquico. Cada una de las partes que componen un nombre de dominio se corresponde con un nivel jerárquico distinto. Por ejemplo, en mi dominio telefonica.mx, es se corresponde con el primer nivel jerárquico, telefónica con el segundo y mi dominio con el tercero. Cada nivel tiene asociado un servidor DNS que sabe cómo resolver todos los niveles inferiores.

Cuando un usuario intenta acceder a una dirección de Internet (por ejemplo, mi dominio telefonica.mx), su programa (por ejemplo, su programa navegador) le hace una petición

a su servidor DNS del número IP asociado. Generalmente éste no sabrá la respuesta, así que le preguntará al servidor DNS de primer nivel (el servidor que gestiona los es) por el DNS asociado con el nombre de dominio telefonica.mx. Posteriormente le preguntará a éste por el DNS asociado con el dominio midominio.telefonica.mx. Este último DNS será quien facilite el número IP buscado. En total, el tiempo necesario para resolver un nombre de dominio suele ser muy pequeño (menor de 200 ms).

Al configurar el DNS, siempre se introducen dos DNS (primario y secundario). En realidad, con un solo DNS sería suficiente. No obstante, se introducen dos para evitar quedamos sin poder trabajar en el caso de que el primero de ellos falle.

En principio, cada usuario debe configurar las direcciones IP de los DNS que le facilita su proveedor de servicio. Haciéndolo de esta manera, conseguirá la mayor velocidad de resolución de las direcciones IP. No obstante, es cierto que sería igualmente válido configurar cualquier otro DNS de otro proveedor siempre que no tenga limitaciones de acceso. (<http://www.bandaanchoa.st/foros.php?temid=781904,diciembre> 2005)

#### **4.10 Colocar una antena externa**

Una antena es un dispositivo que permite la emisión y recepción de ondas electromagnéticas (ondas de radio). Esto quiere decir que las antenas convierten las señales eléctricas en ondas electromagnéticas, y viceversa.

Todos los equipos Wi-Fi ya incorporan sus propias antenas. No obstante, cuando se desea disponer de una red de mayor alcance o cobertura a veces, resulta conveniente sustituir la antena incorporada en el equipo Wi-Fi por otra exterior con mayor ganancia. El obtener un buen resultado en la colocación de antenas exteriores depende no sólo del conocimiento técnico que se tenga de los distintos tipos de antenas y de cómo instalarlos, sino que, además, hará falta un cierto componente de experiencia y saber hacer.

La razón para que no existan unas reglas absolutas para el diseño y localización de antenas es que son muchas variables las que afectan a la propagación de la señal electromagnética. Además, con las redes inalámbricas nos enfrentamos a usuarios móviles y condiciones ambientales cambiantes. Lo que esto significa de forma práctica es que el problema de la colocación de una antena exterior requiere de una cierta experimentación hasta encontrar la mejor solución.

La mayoría de las antenas que incorporan los equipos Wi-Fi son antenas internas. Esto quiere decir que son antenas que vienen incluidas dentro de la unidad del punto de acceso o del adaptador de red (tarjeta PCMCIA o dispositivo USB). Las antenas internas ofrecen la gran ventaja de la comodidad al formar parte del propio dispositivo, pero tienen el inconveniente del alcance. Si se necesita aumentar el alcance sin instalar nuevos puntos de acceso, la mejor solución es colocar una antena externa. Con una buena antena externa, el serial Wi-Fi de un punto de acceso puede llegar a superar los 15 kilómetros de alcance siempre que no haya obstáculos, como edificios o árboles, y que la antena esté bien colocada.

La mayoría de los puntos de acceso y de los adaptadores de red admiten que se les conecte una antena externa. Existen antenas externas tanto para interiores como para exteriores de edificios y su coste varía entre los 800 y los 2000 pesos.

(<http://www.bandaanchoa.st/foros.php?temid=781904>, diciembre 2005)

#### **4.10.1 Sobre las antenas**

Una antena es un dispositivo (generalmente formado por una o más varillas) destinado a la radiación y/o captación de ondas radioeléctricas. La antena de un equipo emisor radia las ondas radioeléctricas, mientras que la antena de un equipo receptor las capta. Un mismo equipo de radio, y su antena, puede ser utilizado tanto para transmitir como para recibir. Por cierto, a esto se le llama transceiver (transmitter-receiver, 'transmisor-receptor').

Una comunicación en la que la información fluye en ambas direcciones recibe el nombre de bidireccional. No obstante, cuando la transmisión y recepción no se efectúa simultáneamente, sino alternativamente, se obtiene lo que se conoce como comunicación semidúplex (half-duplex en inglés). Las comunicaciones Wi-Fi son bidireccionales semidúplex.

En el mercado existen muchos tipos de antenas que pueden funcionar bien en los entornos Wi-Fi. No obstante, antes de lanzarse a comprar, conviene tener claro algunos conceptos generales que nos ayudan a comprender mejor las características de los distintos tipos de antena.

(<http://www.bandaancha.st/foros.php?temid=781904,diciembre> 2005)

#### **4.10.1.1 La ganancia**

Una característica importante en las antenas es su ganancia. La ganancia viene a ser el grado de amplificación de la señal. En el caso de las antenas, la ganancia representa la relación entre la intensidad de campo que produce dicha antena en un punto determinado y la intensidad de campo que produce una antena omnidireccional (llamada isotrópica) en el mismo punto y en las mismas condiciones. Una antena es mejor cuanto mayor es su ganancia.

El valor de la ganancia de una antena se mide en decibelios (dB). El decibelio es una unidad que se calcula como el logaritmo de una relación de valores. No obstante, como para calcular la ganancia de una antena se toma como referencia a la antena isotrópica, el valor de la ganancia se representa en dBi (decibelios en relación a la antena isotrópica).

Las antenas de los puntos de acceso suelen ser antenas verticales omnidireccionales. Estas antenas tienen una ganancia bastante mayor que las antenas que vienen incluidas en los adaptadores de red, pero bastante menor que una antena externa direccional. Las

antenas direccionales concentran la energía radiada en una sola dirección, por lo que consiguen que la energía radioeléctrica llegue bastante más lejos (mayor alcance, aunque en una sola dirección).

(<http://www.bandaanchoa.st/foros.php?temid=781904,diciembre> 2005)

#### **4.10.1.2 La relación señal/ruido**

Uno de los mayores inconvenientes de los sistemas de radio es que, cuando se emite, no sólo se emiten los datos, sino que, mezclado con los datos también, se emiten ruidos. De la misma forma, cuando se recibe, no sólo se reciben los datos, sino que también se reciben ruidos. Este hecho inevitable, incluso en los sistemas digitales, se corrige utilizando técnicas especiales de modulación, filtrado, autocorrelación, etc. En cualquier caso, una transmisión se recibirá mejor cuanto más potente sea la señal de los datos en comparación con los ruidos. Al resultado de dividir el valor de la fuerza de la señal de los datos por el valor de la fuerza del ruido se le conoce como relación señal/ruido (S/N ratio o signal-to-noise ratio en inglés). Evidentemente, cuanto mayor sea este valor, mejor será la comunicación.

El valor de la relación señal/ruido se expresa generalmente en decibelios (dB). El valor de decibelios tiene una escala exponencial. Esto quiere decir que, por ejemplo, 10 dB indica que la señal tiene 10 veces más potencia que el ruido, mientras que 20 dB indica, no 20 veces, sino 100 veces más potencia.

#### **4.10.1.3 Patrón de radiación y apertura del haz**

El patrón de radiación (radiation pattern) es un gráfico o diagrama polar sobre el que se representa la fuerza de los campos electromagnéticos radiados por una antena. La forma del patrón de radiación depende del modelo de antena. Las antenas omnidireccionales emiten en todas direcciones y tienen menor alcance que las antenas direccionales. El

patrón de radiación puede ser representado en dos planos perpendiculares conocidos como azimut y elevación.

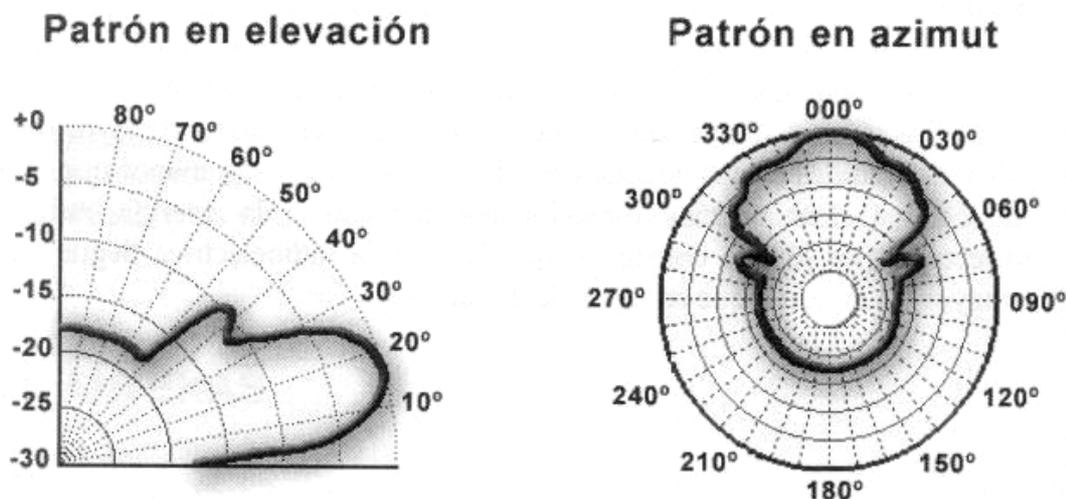


Figura 4.9 Ejemplo de patrón de radiación de una antena

(<http://www.bandaancha.st/foros.php?temid=781904,diciembre> 2005)

Los modelos de antenas comerciales suelen publicar sus patrones de radiación entre sus características.

Otro valor que está relacionado con el modelo de radiación es la apertura del haz. Este valor se expresa en grados y viene a representar la separación angular entre los dos puntos del lóbulo principal del patrón de radiación donde el valor de la energía electromagnética es la mitad de la original (-3 dB). La apertura del haz se suele representar, aunque no siempre, sobre el plano horizontal.

(<http://www.bandaancha.st/foros.php?temid=781904,diciembre> 2005)

#### 4.10.1.4 Polarización

La polarización de una antena describe la orientación de los campos electromagnéticos que irradia o recibe la antena. Las formas de polarización más comunes son las siguientes:

- **Vertical.** Cuando el campo eléctrico generado por la antena es vertical con respecto al horizonte terrestre (va de arriba abajo).
- **Horizontal.** Cuando el campo eléctrico generado por la antena es paralelo al horizonte terrestre.
- **Circular.** Cuando el campo eléctrico generado por la antena va rotando de vertical a horizontal, y viceversa, creando movimientos circulares en todas direcciones. La polarización circular puede ser dextrógira (rotación a favor de las agujas del reloj, conocida también como CCW) y levógira (rotación en contra de las agujas del reloj, conocida también como CW).
- **Elíptica.** Cuando el campo eléctrico se mueve como en la polarización circular pero con desigual fuerza en las distintas direcciones. Generalmente, este tipo de polarización no suele ser intencionado.

Idealmente, la polarización de las antenas de ambos extremos de la comunicación debe ser la misma para minimizar la pérdida de ganancia.

(<http://www.bandaancha.st/foros.php?temid=781904,diciembre> 2005)

#### 4.10.2 Tipos de antenas

En el mercado existen tantos tipos de antenas como ha permitido la imaginación: yagui, de panel, parabólica de disco, parabólica de rejilla, de techo, patch, dipolo, planas, compactas, móviles, sectoriales, espiral, guía-onda, anular, etc. No obstante, todos estos tipos de antenas pueden agruparse en dos tipos primarios: omnidireccional y direccional.



Figura 4.10 Distintos tipos de antenas

(<http://www.bandaanchoa.st/foros.php?temid=781904>, diciembre 2005)

Las antenas omnidireccionales son aquellas que radian en todas direcciones y también pueden captar la señal procedente de todas direcciones. Por el contrario, las antenas direccionales concentran su radiación en una dirección y solo pueden captar la señal procedente de esa dirección. Las antenas direccionales tienen un mayor alcance (y ganancia) que las primeras a costa de concentrarse en una sola dirección.

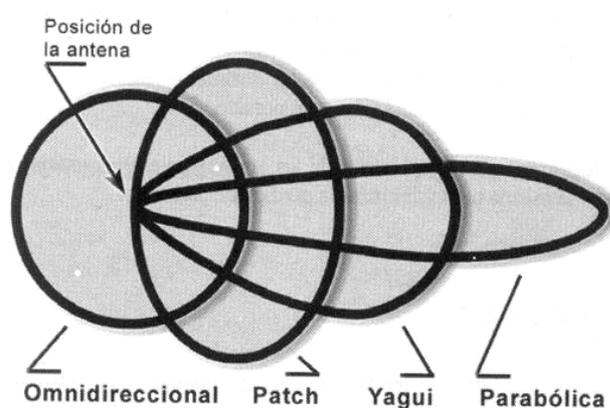


Figura 4.11 Lóbulo principal de propagación de la señal en distintas antenas (simplificación)

(<http://www.bandaanchoa.st/foros.php?temid=781904>, diciembre 2005)

En el caso de los equipos Wi-Fi, se suelen utilizar los tipos de antenas omnidireccionales para interiores y los tipos direccionales para exteriores.

Las antenas más habituales son las conocidas como dipolo. Un dipolo emite su señal haciendo que la energía se propague paralela al dipolo y perpendicular al suelo (polarización vertical). Si se girase la antena 90 grados, se obtendría una antena de polarización horizontal. Ambos modelos son posibles. Para cada caso particular un modelo puede funcionar mejor que el otro.

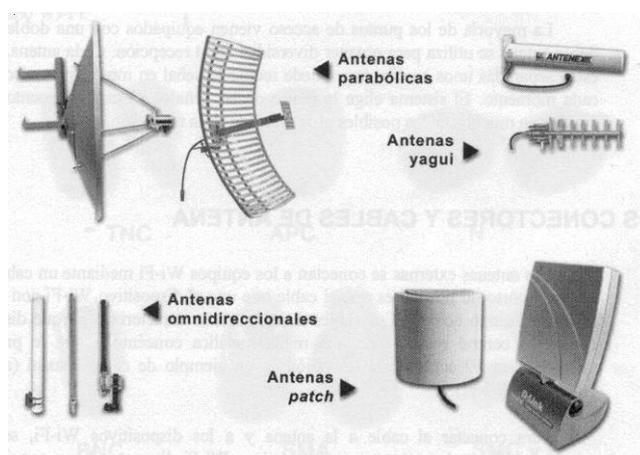


Figura 4.12 Tipos de antenas más comunes

(<http://www.bandaanchoa.st/foros.php?temid=781904,diciembre> 2005)

Las antenas direccionales concentran la energía en una sola dirección consiguiendo obtener incrementar el alcance. Cuanto más direccional es una antena, mayor es su alcance. Existen muy distintos modelos de antenas direccionales entre los que destacan los siguientes:

- La antena **yagui** es una antena direccional con una apertura de haz de entre 15 y 60 grados. Su ganancia varía entre los 6 y los 21 dBi. Estas antenas suelen venir montadas en el interior de una cobertura cilíndrica.
- La antena de panel tipo **patch** (parche) es una antena plana para ser montada en la pared. Esta antena emite energía siguiendo un modelo semiesférico. Tienen

ganancias de entre 12 y 22 dBi. Su mayor inconveniente es que, al ser plana, puede sufrir por la fuerza del viento si se sitúan en el exterior

- La antena **parabólica** es una antena que tiene forma de disco cóncavo con la que se consigue unos haces muy direccionales. Es muy útil para comunicaciones punto a punto y se pueden conseguir ganancias de hasta 27 dBi. En el mercado existen distintas configuraciones de antenas parabólicas: redondas, mayadas, cuadradas, etc.
- Además de las anteriores, existen otros diferentes tipos de antenas (dipolos, reflectores, etc.) que pueden ser utilizadas en las instalaciones Wi-Fi. En cualquier caso, siempre es conveniente asegurarse que la antena está construida para funcionar en la banda de 2,4 GHz.

La mayoría de los puntos de acceso vienen equipados con una doble antena. Esta doble antena se utiliza para obtener diversidad en la recepción. Cada antena, aunque sólo estén separadas unos centímetros, puede recibir la señal en muy distintas condiciones en cada momento. El sistema elige la mejor de las señales en cada momento evitando de esta forma muchos de los posibles problemas de mala recepción.

(<http://www.bandaanchoa.st/foros.php?temid=781904,diciembre> 2005)

#### **4.10.3 Los conectores y cables de antena**

Las antenas externas se conectan a los equipos Wi-Fi mediante un cable. Salvo que sea muy corto, lo normal es que el cable que une el dispositivo Wi-Fi con la antena sea un cable de tipo coaxial. Los cables de este tipo se caracterizan porque disponen de un conductor central rodeado de una malla metálica concéntrica que le protege de las interferencias. El cable de la televisión es un ejemplo de cable coaxial (aunque no es válido para Wi-Fi).

Para conectar el cable a la antena y a los dispositivos Wi-Fi, se utilizan los conectores. Tanto la antena como los equipos Wi-Fi disponen de un conector donde se deben enchufar sus correspondientes conectores de los extremos del cable. Para poder llevar a cabo esta operación, existen unos conectores conocidos como de tipo macho y otros como de tipo hembra. Sólo los conectores de distinto sexo pueden conectarse entre sí. Por ejemplo, en la antena suele haber un conector de tipo hembra y en el cable, uno de tipo macho. Esto permite conectar el cable a la antena.

Tanto el cable, como cada conector, añaden pérdidas a la señal de radio. Para evitar estas pérdidas, aparte de utilizar cables y conectores de calidad, hay que procurar utilizar un cable lo más corto posible y el número de conectores imprescindibles. Esto último quiere decir que hay que evitar utilizar conectores para extender la longitud del cable o para adaptar tipos de cables o conectores.

(<http://www.bandaanchoa.st/foros.php?temid=781904,diciembre> 2005)

#### **4.10.3.1 Tipos de conectores**

La utilización de los conectores parece muy sencilla, pero todo se complica por el hecho de que no existe una regulación que especifique cómo deben ser los conectores. Esto trae consigo que existan muchos modelos distintos de conectores, algunos muy extendidos y otros específicos de un fabricante (conectores propietarios). Por ejemplo, Cisco y LinkSys utilizan conectores TNC; los equipos Intel tienen conectores BNC y Avaya y Orinoco utilizan conectores de diseño propio. El hecho se agrava si tenemos en cuenta que el tipo de conector de la antena suele ser distinto del tipo de conector del equipo Wi-Fi.



*Figura 4.13 Tipo de conectores (no están a la misma escala)*  
 (<http://www.bandaancho.st/foros.php?temid=781904>, diciembre 2005)

La mayoría de los equipos Wi-Fi (adaptadores de red y puntos de acceso) disponen de un conector para enchufar una antena externa. Esto es así porque la FCC (el regulador norteamericano de comunicaciones) exige que todos estos equipos vengan equipados con un conector. No obstante, lo cierto es que, a veces, existe cierta dificultad para encontrar el conector. Lo mismo hay que levantar algún pequeño tapón de plástico o similar.

Los tipos de conectores más comunes son los siguientes:

- **N.** Navy (marina). Es el conector más habitual en las antenas de 2,4 GHz. Trabaja bien con frecuencias de hasta 10 GHz. Es un conector de tipo rosca. Estos conectores tienen un tamaño apreciable y, a veces, se confunden con los conectores de UHF. La gran diferencia es que estos últimos no son aptos para la frecuencia de 2,4 GHz.
- **BNC.** Bayonet Navy Connector (conector tipo bayoneta de la marina). Es un conector barato utilizado en las redes Ethernet del tipo 10Base2. Es un tipo de conector muy común, pero poco apto para trabajar en la frecuencia de 2,4 GHz.

- **TNC.** Threaded BNC (conector BNC roscado). Es una versión roscada del conector BNC. Este tipo de conector es apto para frecuencias de hasta 12 GHz.
- **SMA.** Sub-Miniature Connect (conector subminiatura). Son unos conectores muy pequeños, van roscados y trabajan adecuadamente con frecuencias de hasta 18 GHz.
- **SMC.** Se trata de una versión todavía más pequeña de los conectores tipo SMA. Son aptos para frecuencias de hasta 10 GHz. Su mayor inconveniente es que sólo son utilizables con cables muy finos (con alta pérdida). El conector SMB es una versión del SMC con la ventaja de que se conecta y desconecta más fácilmente.
- **APC-7.** Amphenol Precision Connector (conector Amphenol de precisión). Se trata de un conector con muy poca pérdida, y muy caro, fabricado por la empresa Amphenol. Tiene la particularidad de que no tiene sexo.

(<http://www.bandaancha.st/foros.php?temid=781904,diciembre> 2005)

#### 4.10.3.2 El cable

El motivo principal por el que se utiliza una antena externa no es alejar la antena del equipo Wi-Fi, sino poder conseguir aumentar el alcance de este equipo. Esto quiere decir que, para instalar una antena externa, no se debe pensar en unir la antena con el equipo Wi-Fi con un largo cable, sino todo lo contrario. El cable introduce pérdidas en la señal que van desde los 0,05 a 1 dB por metro y a precios desde 10 a 500 pesos por metro (dependiendo de la calidad del cable). Por tanto, a menor longitud del cable, menores pérdidas.

Por otro lado, el cable tiene soldado un conector en cada extremo. Como los conectores pueden encontrarse en cualquier tienda especializada, cualquier aficionado podría fácilmente fabricarse un cable con sus respectivos conectores. Sin embargo, es recomendable comprar el cable completo con sus conectores ya puestos. La razón es que el soldar conectores a cables es un arte y una ciencia que requiere contar con experiencia para obtener resultados óptimos.

Para comprar el cable, hay que asegurarse que sea óptimo para la frecuencia de 2,4 GHz. Un cable puede ser muy apropiado para ser utilizado en aplicaciones de televisión y video y no ser adecuado para Wi-Fi. Elegir el cable adecuado es casi tan importante como elegir la antena adecuada. Todos los cables introducen pérdidas, pero unos introducen más pérdidas que otros.

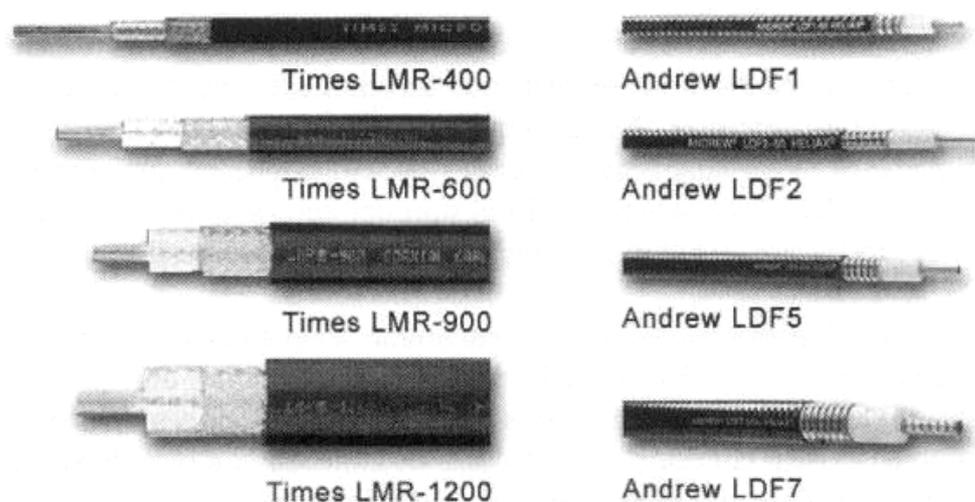


Figura 4.14 Ejemplos de cables LMR y Heliax (no están en la misma escala)

(<http://www.bandaancha.st/foros.php?temid=781904,diciembre> 2005)

Quizás, los cables mas utilizados en las frecuencias de Wi-Fi sean los de tipo LMR. Estos son unos cables fabricados por Times Microwave System ([www.timesmicrowave.com](http://www.timesmicrowave.com)). Una alternativa son los cables Heliax fabricados por Andrew Corporation ([www.andrew.com](http://www.andrew.com)). Estos son unos cables que introducen muy poca pérdida a la señal pero a cambio de un alto coste. Por dar una última referencia, también puede interesarse por los cables fabricados por Belden ([www.belden.com](http://www.belden.com)).

TIPO DE CABLE	PÉRDIDA 802.11b (2,4 GHz) dB/100m	PÉRDIDA 802.11a (5,3 GHz) dB/100m
LMR-200	54,2	82,4
LMR-240	41,5	63,6
LMR-400	21,7	33,7
LMR-600	14,2	22,6
LMR-900	9,58	15,1
LMR-1200	7,27	11,7
LMR-1700	5,51	
RG-58	105,6	169,2
RG-8X	75,8	134,2
RG-213/214	49,9	93,8
9913	25,3	45,3
3/8" LDF	19,4	26,6
1/2" LDF	12,8	21,6
7/8" LDF	7,5	12,5
1 1/4" LDF	5,6	9,2
1 5/8" LDF	4,6	8,2

*Tabla 4.9 Perdidas en distintos tipos de cables*

(<http://www.bandaanchoa.st/foros.php?temid=781904,diciembre> 2005)

#### 4.10.3.3 El adaptador o pigtail

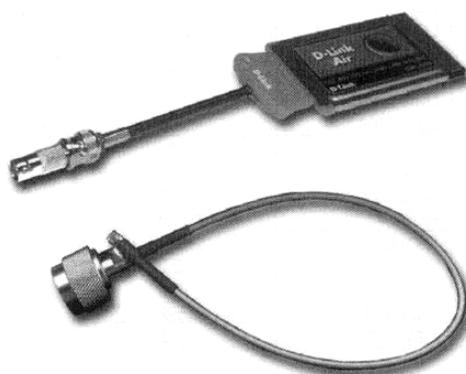
A diferencia de las antenas, los adaptadores de red Wi-Fi no suelen disponer de un conector tipo N. Esto quiere decir que no se puede conectar directamente el cable de la antena (con conector N) al equipo Wi-Fi (con conector distinto, posiblemente propietario). Por tanto, para permitir la conexión, es imprescindible conseguir un adaptador del conector tipo N al del tipo del equipo Wi-Fi. A estos adaptadores se les conoce mejor por su término en inglés: pigtail (literalmente, trenza).

En el mercado se pueden encontrar adaptadores de conectores para distintos modelos de equipos Wi-Fi. De hecho, existen fabricantes de equipos Wi-Fi que también fabrican antenas externas. En estos casos, el propio fabricante tiene resuelta la conexión. También existen conectores adaptadores de conector N a otro tipo de conector. Si se tiene suerte, es posible que se encuentre el adaptador adecuado para el equipo Wi-Fi de que se dispone.

Si no se encuentra en el mercado el adaptador adecuado, la única solución que queda es fabricarse un adaptador. Generalmente, la fabricación de un adaptador consiste en utilizar un cable con conector N en un extremo y conectarlo al equipo Wi-Fi por el otro extremo soldándolo directamente en su contacto correspondiente. Para ello, es necesario abrir el equipo Wi-Fi, identificar las conexiones de la antena externa y realizar la soldadura sacando el cable por el sitio que se vea más adecuado.

Antes de lanzarse a fabricar un adaptador, conviene saber que realizar esta operación no sólo deja al equipo Wi-Fi sin garantía, sino que se tiene el riesgo de producirle daños irreparables al equipo. Esta operación sólo debe ser realizada por personal especializado.

(<http://www.bandaanchoa.st/foros.php?temid=781904>, diciembre 2005)



*Figura 4.15 Pigtail comercial (abajo) y fabricado (arriba)*

(<http://www.bandaanchoa.st/foros.php?temid=781904>, diciembre 2005)

#### **4.10.4 Calcular el alcance**

¿Cuál puede ser el alcance de un equipo Wi-Fi? Ésta es una pregunta cuya mejor respuesta viene de la experimentación. Hacemos la instalación y comprobamos con un ordenador portátil la calidad de la señal a distintas distancias. No obstante, existen alternativas teóricas a esta práctica: por un lado, existen distintas Web en Internet que ofrecen utilidades de cálculo; por otro, podemos hacer un cálculo teórico manual si se dispone de las características técnicas de los cables, conectores y antenas.

En cuanto al cálculo teórico, aunque el alcance de una antena depende también de factores como los obstáculos o las interferencias, lo que se suele hacer es realizar el cálculo suponiendo unas condiciones ideales y, posteriormente, estimar unas pérdidas adicionales por falta de condiciones ideales.

(<http://www.bandaancha.st/foros.php?temid=781904>, diciembre 2005)

#### **4.10.4.1 Pérdida de propagación**

La pérdida de propagación es la cantidad de serial necesaria para llegar de un extremo a otro de la transmisión. Dicho de otra forma, es la cantidad de señal que se pierde al atravesar un espacio.

Las señales electromagnéticas se propagan por el medio a la velocidad de la luz. Incluso tienen la habilidad de poder traspasar paredes, techos, puerta o cualquier otro obstáculo. Además, pueden colarse por los pequeños agujeros gracias a un fenómeno conocido como difracción. En cualquier caso, unos obstáculos los pasa más fácilmente que otros.

El hacer un cálculo teórico del alcance de una señal, considerando todos los posibles obstáculos, resulta algo complicado teniendo en cuenta la finalidad a la que se dedican estos cálculos. Por ello, generalmente se lleva a cabo el cálculo en espacio abierto sin obstáculos.

(<http://www.bandaancha.st/foros.php?temid=781904>, diciembre 2005)

#### **4.10.4.2 Pérdidas y ganancias**

Aparte de las pérdidas de propagación, en una instalación de radio existen distintos dispositivos que producen pérdidas o aportan ganancias a la señal. El cálculo teórico del alcance de una transmisión se basa en sumar los factores de la instalación que aportan ganancias y restar los que producen pérdidas. Al final, obtendremos un nivel de señal. El

que este nivel de señal sea suficiente para una buena recepción depende del equipo receptor.

CARACTERÍSTICA	VALOR
Ganancia de una antena	De 6 a 24 dB
Pérdida del cable	De 0,05 a 1dB por metro
Pérdida del conector	0,25 dB por conector
Pérdida de propagación	$20\log_{10}(D) + 20\log_{10}(F) + 32,4$

Tabla 4.10 Valores típicos en el cálculo del alcance

(<http://www.bandaancho.st/foros.php?temid=781904>, diciembre 2005)

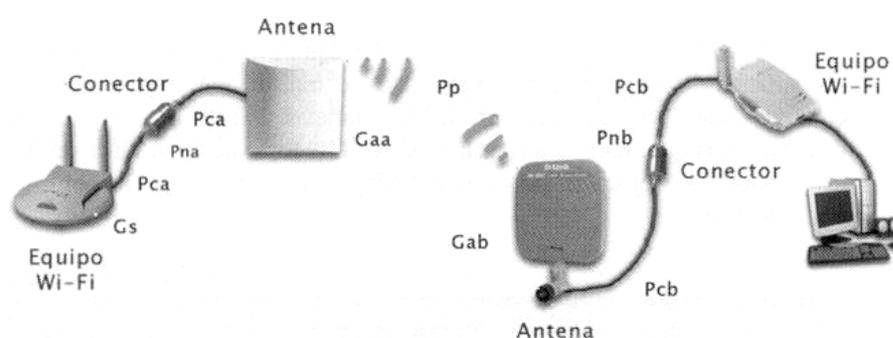


Figura 4.16 Factores que intervienen en el alcance (configuración más amplia)

(<http://www.bandaancho.st/foros.php?temid=781904>, diciembre 2005)

En una comunicación Wi-Fi extremo a extremo contamos con los siguientes factores:

- **Gs.** Ganancia de salida. Es la potencia con la que sale la señal del equipo de radio transmisor.
- **Pca.** Pérdida del cable del extremo transmisor. Hay que contar las pérdidas de todos los cables que intervienen en la instalación, incluido el cable adaptador (pigtail), si lo hubiera. Dependiendo de la calidad del cable, las pérdidas pueden variar entre los 0,05 y 1 dB por metro. Si no se utilizase una antena exterior, no se utilizaría cable de antena y, por tanto, no se consideraría esta pérdida.
- **Pna.** Pérdida de los conectores del extremo transmisor. Hay que contar las pérdidas de todos los conectores. Generalmente se considera una pérdida de 0,25

dB por conector. De la misma forma, si no se utilizase una antena exterior, no se utilizarían conectores para la antena y, por tanto, no se consideraría esta pérdida.

- **Gaa.** Ganancia de la antena del extremo transmisor. Este valor depende del modelo de antena que se utilice. Esta ganancia varía habitualmente entre los 6 y los 24 dB.
- **Pp.** Pérdida de propagación.
- **Gab.** Ganancia de la antena del extremo receptor.
- **Pnb.** Pérdida de los conectores del extremo receptor.
- **Pcb.** Pérdida del cable del extremo receptor.

Esto quiere decir que el nivel de señal que le llega al equipo de radio receptor es el siguiente:

$$S = G_s - P_{ca} - P_{na} + G_{aa} - P_p + G_{ab} - P_{nb} - P_{cb}$$

Si se desea tener en cuenta las condiciones ambientales, se pueden estimar unas pérdidas adicionales de 20 dB.

Dependiendo de las características del equipo receptor, este nivel de señal puede ser suficiente para una u otra velocidad de transmisión o para no hacer posible la comunicación. Por ejemplo, un de las tarjetas Wi-Fi de Orinoco indica en sus características que, para una transmisión de 11 Mbps, necesita un nivel de señal de -82 dBm; para 5,5 Mbps, -87 dBm; para 2 Mbps, -91 dBm y para 1 Mbps, le es suficiente con -94 dBm. (<http://www.bandaancha.st/foros.php?temid=781904,diciembre> 2005)

MODELO	POTENCIA EMISIÓN	SENSIBILIDAD DEL RECEPTOR			
		11 Mbps	5,5 Mbps	2 Mbps	1 Mbps
3Com	15 dBm	-76 dBm	-80 dBm	-80 dBm	-80 dBm
Edimax	14 dBm	-80 dBm	-83 dBm	-86 dBm	-86 dBm
Linksys	19 dBm				
Orinoco	15 dBm	-83 dBm	-87 dBm	-91 dBm	-94 dBm
SpeedStream	15 dBm	-76 dBm	-80 dBm	-80 dBm	-80 dBm
US Robotics	13 dBm	-76 dBm	-80 dBm	-80 dBm	-80 dBm

Tabla 4.11 Potencia de emisión y sensibilidad del receptor de algunos equipos Wi-Fi

(<http://www.bandaancha.st/foros.php?temid=781904,diciembre> 2005)

#### 4.10.5 Elegir una antena

Una vez vistos los conceptos generales relacionados con la tecnología de las antenas, ya podemos decidirnos a elegir la más adecuada para resolver nuestras necesidades. No obstante, antes de seguir adelante, repasemos rápidamente los conceptos más importantes que hay que tener en cuenta a la hora de elegir una antena:

- **Frecuencia.** Hay que estar seguros que la antena elegida trabaja en la banda de frecuencias de 2,4 GHz. Recordar que 802.11b y 802.11g trabajan en esta frecuencia, mientras que 802.11a trabaja en 5 GHz.
- **Tipo de antena.** Cuando se va a buscar una antena, no hay que fiarse excesivamente del nombre del tipo de la antena. Los distintos fabricantes suelen utilizar distintos nombres de tipos de antenas. Por ello, lo importante es fijarse que la antena elegida dispone de las características de direccionalidad y ganancia que se necesitan.
- **Polarización.** Es importante asegurarse de que la polarización de las distintas antenas es la misma (horizontal o vertical).
- **Ganancia.** La ganancia es uno de los parámetros fundamentales de una antena. No obstante, hay que tener en cuenta que la ganancia real de una antena depende también de los cables y conectores que se utilicen.
- **Conectores.** Los conectores introducen pérdidas. Por este motivo, hay que procurar utilizar el menor número de conectores posible. Internet no utiliza adaptadores o dispositivos similares. De la misma forma, el cable también introduce pérdidas, por lo que se deben evitar los excedentes de cable.

(<http://www.bandaanchoa.st/foros.php?temid=781904,diciembre> 2005)

#### 4.10.6 Dónde situar la antena

La tecnología Wi-Fi tiene dos retos desde el punto de vista de la transmisión de radio: el primero es que utiliza un espectro de frecuencias que es utilizado también por otros

muchos dispositivos (como los teléfonos inalámbricos, microondas, etc.) y el segundo es que la regulación limita la potencia máxima con la que un equipo Wi-Fi puede emitir la señal. Esto quiere decir que no solamente nos enfrentamos a utilizar una banda de frecuencias muy sucia (desde el punto de vista radioeléctrico) y, por tanto, donde se pueden producir muchas interferencias, sino que, además, no se puede amplificar la señal para mejorar el alcance.

Por otro lado, es importante elegir un buen lugar para situar la antena. El interior de un cajón, bajo una mesa, detrás de un mueble archivador, entre pilas de papeles, al lado de un microondas, al lado de superficies metálicas o en una estantería repleta de libros no son buenos lugares.

Las interferencias las producen generalmente otros equipos que están funcionando en los alrededores de nuestra instalación Wi-Fi. Los hornos microondas, motores de los ascensores, sistemas de alarmas, teléfonos inalámbricos u otros equipos Wi-Fi instalados en la colonia pueden producir interferencias. Los problemas de interferencias suelen afectar a la comunicación de forma intermitente. Quiere esto decir que, si la comunicación funciona bien salvo en determinados momentos, lo más probable es que estemos sufriendo interferencias. Por ejemplo, si nos falla la comunicación a la hora del almuerzo, es posible que la fuente de interferencias esté en un microondas cercano.

En los espacios abiertos existen circunstancias que pueden degradar transmisiones: un elevado grado de humedad, niebla, lluvia, humo o, simplemente, hojas de los árboles.

Los CD de utilidades que acompañan a algunos equipos Wi-Fi incluyen programa que permite hacer un seguimiento del ruido durante las últimas 24 horas. Esto permite comprobar si las interferencias se producen principalmente a una hora para poder ayudarnos a buscar la fuente de las interferencias.

(<http://www.bandaancho.st/foros.php?temid=781904,diciembre> 2005)

#### 4.10.6.1 Sintonizar la antena

Una vez decidido el sitio donde colocar la antena, es necesario hacer pruebas para asegurarse de que se coloca en la mejor posición posible y, en las antenas direccionales, en la mejor orientación.

Sintonizar una antena no es algo complejo, pero será mucho más fácil dos personas en este trabajo. Una persona se encarga de colocar la antena en diferentes posiciones u orientaciones mientras la otra se encarga de comprobar en el ordenador (mediante el programa de utilidad que viene en el equipo Wi-Fi) los niveles de recepción de la señal para cada posición de la antena. Comprobando estos niveles se podrá determinar cuál es la mejor posición y orientación para la antena.

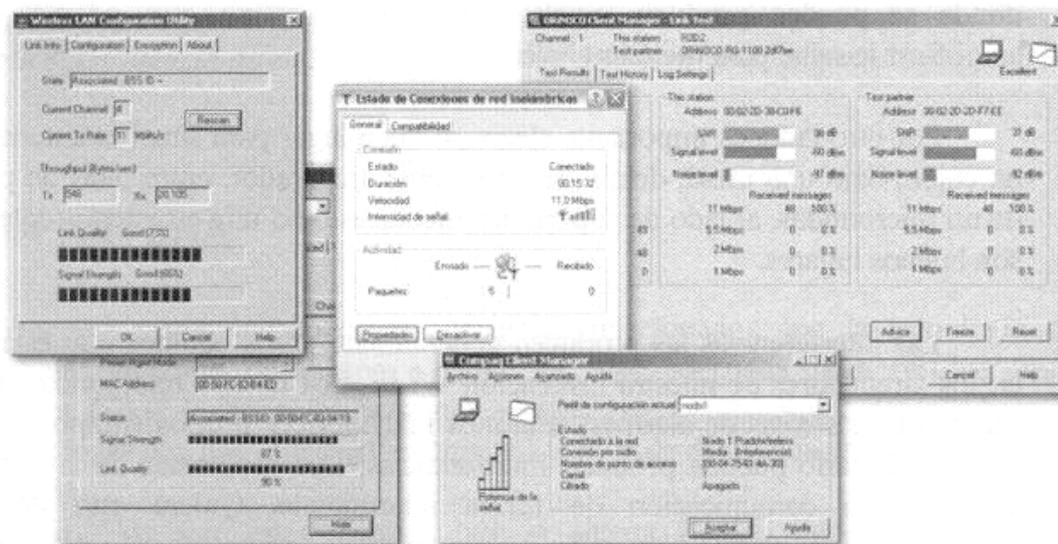


Figura 4.17 Distinto software de utilidades de medición de niveles de recepción  
<http://www.bandaancho.st/foros.php?temid=781904,diciembre> 2005)

#### 4.10.7 Construir una antena

Existen usuarios que disfrutan construyendo con sus propias manos todo aquello que es factible construir. En el caso de las redes inalámbricas, mientras que construir un punto de acceso o un adaptador de red es algo complicado, construir una antena sí es abordable.

En cualquier caso, construir una antena, o hacer modificaciones en antenas existentes no dedicadas a Wi-Fi, requiere disponer de conocimientos específicos, tanto de la técnica como de la regulación. Una soldadura mal hecha o no hacer del todo bien un cálculo pueden hacer que la antena no funcione como se espera o, incluso, que se esté incumpliendo la regulación de emisiones radioeléctricas.



*Figura 4.18 Distintos modelos de antenas caseras*

*(<http://www.bandaanchoa.st/foros.php?temid=781904,diciembre> 2005)*

A donde queremos llegar con esto es que, independientemente de que se sigan las instrucciones de este capítulo o de alguna página de Internet, en determinadas circunstancias una antena casera podría llegar a dañar el equipo Wi-Fi, incumplir la ley

de emisiones radioeléctricas, interferir los teléfonos inalámbricos de los vecinos o produce daños en la salud. No se sabe, nadie ha experimentado todos estos factores con estas antenas caseras y sacando conclusiones. Por tanto, sepa que está actuando bajo su propia responsabilidad.

(<http://www.bandaancha.st/foros.php?temid=781904,diciembre> 2005)

#### 4.10.7.1 Principios básicos

Como ya sabemos, las ondas radioeléctricas tienen forma senoidal. Esto quiere decir que la onda va aumentando y disminuyendo su amplitud de forma cíclica. La onda tiene al final de cada ciclo la misma amplitud y tendencia que tenía al principio. El tiempo que tarda la onda en completar cada ciclo se conoce como periodo. Por otro lado, la distancia que recorre la señal en un ciclo se conoce como longitud de onda.

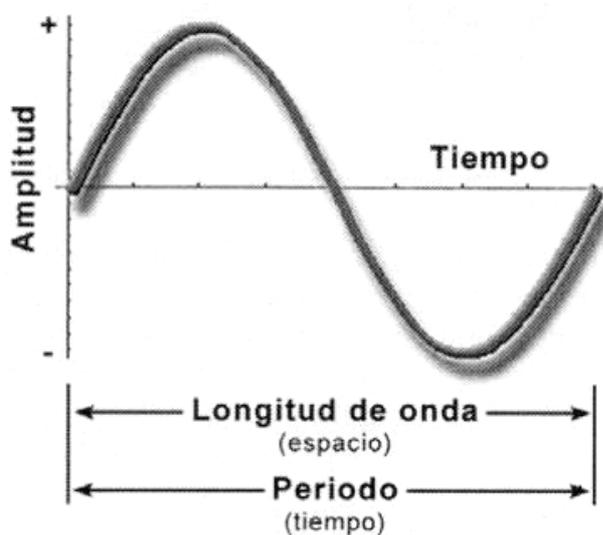


Figura 4.19 Forma de una onda de radiofrecuencia (senoidal)

(<http://www.bandaancha.st/foros.php?temid=781904,diciembre> 2005)

El hercio es una unidad de medida que significa el número de ciclos que completa una onda en un segundo. Una frecuencia de 10 Hz significa que la onda completa 10 ciclos en un segundo. Esto quiere decir que tarda una décima de segundo en completar cada ciclo. Por tanto, el periodo es de 0,1 segundo.

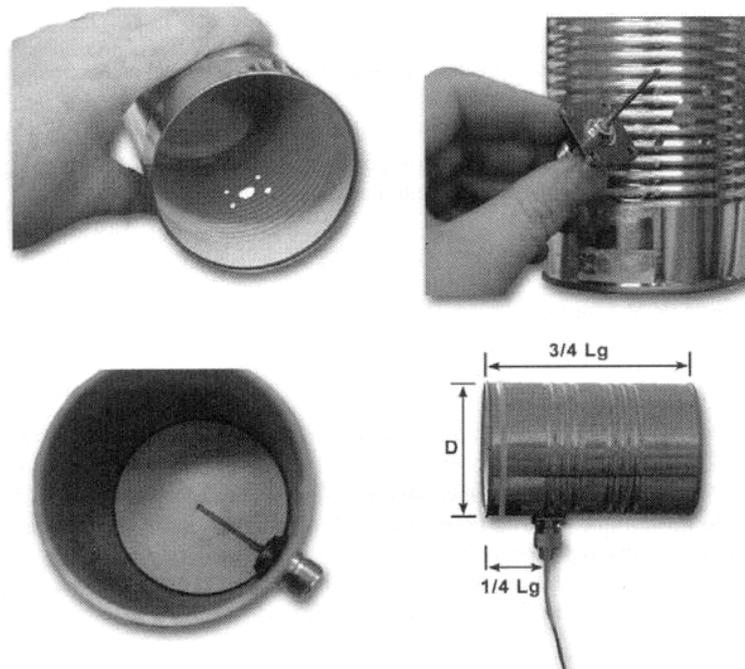
(<http://www.bandaancha.st/foros.php?temid=781904>, diciembre 2005)

#### **4.10.7.2 Una antena con una lata**

El modelo de antena guía-ondas que vamos a explicar a continuación ha sido desarrollado por Gregory Rehm del Bellingham Technical College.

Esta antena consiste básicamente en un cilindro cerrado por un extremo en el que se le coloca el conector en el que termina el cable de la antena. Como cilindro cerrado puede utilizarse una lata de comestible, un tubo de aire acondicionado fabricarlo directamente. Lo importante es que tenga un diámetro entre 9 y 11 cm. y que las paredes sean lisas.

Lo que se consigue es una antena direccional con una mayor ganancia que la antena omnidireccional que viene incluida en los equipos Wi-Fi. Por cierto, si se utilizase una lata, es importante eliminar los posibles restos de rebabas que pudiesen quedar en el lado abierto.



*Figura 4.20 Fabricación de una antena externa con una lata.*

*([www.turnpoint.net](http://www.turnpoint.net), diciembre 2005)*

La longitud de la lata ( $3/4$  de la longitud de onda,  $L_g$ ) y la posición del conector ( $1/4$  de la longitud de onda desde la base) depende de la frecuencia a la que se trabaje (en el ejemplo, 2,46 GHz) y del diámetro interior de la lata. Aunque estas distancias no tienen que ser exactas, es aconsejable que sean lo más aproximadas posibles a las indicadas en la tabla adjunta.

Diámetro del cilindro (mm)	Longitud de onda estacionaria (mm)	_ Longitud de onda (mm)	_ Longitud de onda (mm)
90	201	50	151
92	194	48	145
94	188	47	141
96	183	46	137
98	178	45	134
100	174	44	131
102	171	43	128
104	168	42	126
106	165	41	124
108	163	41	122
110	160	40	120

*Tabla 4.12 Medidas del cilindro en función de su diámetro interior (calculado para una frecuencia de 2,46 GHz)*

*([www.turnpoint.net](http://www.turnpoint.net), diciembre 2005)*

Si desea hacer sus propios cálculos, utilice la fórmula siguiente:

$$(1/L-g)^2 = F/300)^2 - (1/1,706*D)^2$$

Donde Lg es la longitud de onda estacionaria dentro de la lata en milímetros; F, la frecuencia en GHz y D, el diámetro interior de la lata en milímetros.

El conector tipo N debe situarse en el lateral a una distancia de \_ Lg del fondo de la lata (le llamamos fondo al lado tapado). Al conector se le debe prolongar la espiga central con un trozo de cable de cobre de 30 mm de longitud. Este cable debe soldarse al conector.

La longitud del cable de cobre depende también de la frecuencia. Se puede calcular con la siguiente fórmula:

$$\text{Longitud} = \text{onda de señal al aire} = (300/F)$$

Donde F es la frecuencia en GHz y la longitud queda expresada en milímetros.

El conector N se debe pegar a la lata asegurándose de que no queda ningún hueco y que la superficie interior queda lisa. Si se desea, también se puede fijar el conector a la lata mediante sus tornillos. En este caso, es importante que los tornillos tengan la cabeza hacia adentro para evitar protuberancias en el interior. Además, es mejor si se sella la unión del conector a la lata mediante silicón o elemento similar.

Por último, se debe hacer un pequeño agujero en el fondo de la lata para evacuar la posible agua que se condense en el interior. A ser posible, la lata debe ir tapada con su tapa de plástico. Esta tapa debe ser resistente a las microondas.

Para saber si una tapa es resistente a las microondas, se puede hacer la prueba de meter la tapa en el interior de un horno microondas (ya sabe que los microondas trabajan en la misma banda de frecuencias que Wi-Fi) durante un par de minutos y comprobar que no se calienta ni se deforma. Si se decide a hacer esta prueba, no se olvide de introducir también un vaso con agua junto con la tapa para evitar posibles sobrecalentamientos.

Una vez construida la antena, puede probarla uniéndola al equipo Wi-Fi (punto de acceso o adaptador de red) mediante su cable correspondiente. Si el equipo Wi-Fi tiene un conector especial de antena exterior, es posible que tenga que comprobar o construirse el adaptador correspondiente (pigtail) que convierta dicho conector en un tipo N.

([www.turnpoint.net](http://www.turnpoint.net), diciembre 2005)

#### **4.10.7.3 Una antena con un bote de Pringles**

La antena que más ha llamado la atención entre los usuarios de redes Wi-Fi ha sido la construida con un bote de patatas Pringles. El primer modelo que se le viene a la cabeza a la mayoría de los usuarios que piensan en construir una antena es el del bote de Pringles. Si se para un poco a buscar por Internet, comprobará que existen muchas direcciones que hacen referencia a este modelo de antena.

Hasta donde se ha podido averiguar, el inventor de esta antena es Andrew Clapp, aunque, posteriormente, han aparecido distintas versiones de este modelo. Quizás la más famosa sea la versión de Rob Flickenger, administrador de la red de O'Reilly.

Hay que tener en cuenta que lo importante de una antena son sus medidas. Por tanto, realmente da igual hacer este modelo con un bote de patatas fritas Pringles o con cualquier otro bote, siempre que tenga las mismas medidas. La casualidad ha hecho que los botes de Pringles tengan las medidas apropiadas (aunque no ideales). Se trata de un bote de 73 milímetros de diámetro y 230 milímetros de largo.

Dependiendo de lo cuidadoso que se sea, con una antena de este tipo se puede Negar a alcanzar los 12 dB de ganancia y cubrir distancias de más de 1 kilómetro. Hay quien dice que ha conseguido varios kilómetros. No obstante, como se ha visto en capítulos anteriores, el alcance no depende sólo de la antena, sino que influyen también otros factores como la climatología, el entorno, las posibles interferencias, etc. En cualquier caso, conforme aumenta la distancia entre un extremo y otro de la comunicación, baja la velocidad de transmisión. Los 11 Mbps sólo se mantienen durante las primeras decenas de metros. En cualquier caso, no está nada mal para una antena cuyos componentes no cuestan más de 80 pesos.

Por cierto, como la construcción de este tipo de antenas no suele ser muy precisa (ya de por sí las herramientas que utilizamos no lo son), se puede dar por bueno haber construido una antena con 9 dB de ganancia y que alcance los 400-500 metros transmitiendo en el rango bajo de las velocidades de Wi-Fi.



*Figura 4.21 Distintas vistas de la fabricación de una antena Pringles  
([www.oreillynet.com/lcs/ weblog/Mewlwgl4481](http://www.oreillynet.com/lcs/ weblog/Mewlwgl4481), diciembre 2005)*

Los materiales que se necesitan para construir esta antena son los siguientes:

- Un bote de papas Pringles de cualquier sabor. Se necesita tanto el bote (vacío) como su tapa de plástico. Si no se dispone de uno de estos botes, también valdría cualquier otro bote que tenga un diámetro de 73 milímetros y una longitud de 230 milímetros.
- Un disco de plástico de 73 milímetros de diámetro exterior (el diámetro interior del bote de Pringles). Vale la tapa de cualquier otro bote de Pringles o cualquier otra tapa.
- Un conector de antena. Generalmente se suele utilizar un conector hembra tipo N. Aquí se conectará el cable que une la antena con el equipo Wi-Fi.
- Varilla roscada de 3 milímetros de diámetro. Harán falta menos de 15 centímetros.
- Dos tuercas de nailon que rosquen en la varilla roscada.
- Cinco arandelas de 25 milímetros de diámetro exterior, 1,5 milímetros de espesor y con un diámetro interior suficiente para poderlas meter en la varilla roscada (algo más de 3 mm).

- Tubo de aluminio de unos 6 milímetros de diámetros. Harán falta menos de 16 centímetros de tubo.
- Cable de cobre grueso de un solo hilo. Bastará con menos de 40 milímetros de longitud.

Para construir la antena, lo primero es cortar el tubo de aluminio haciendo cuatro trozos de 31 milímetros de largo. A continuación cortamos la varilla roscada a una longitud de 143 milímetros. La longitud de la varilla debe ser suficiente para albergar cinco arandelas (de 1,5 mm de espesor), cuatro tubos de aluminio (de 31 mm de largo) y las dos tuercas de los extremos.

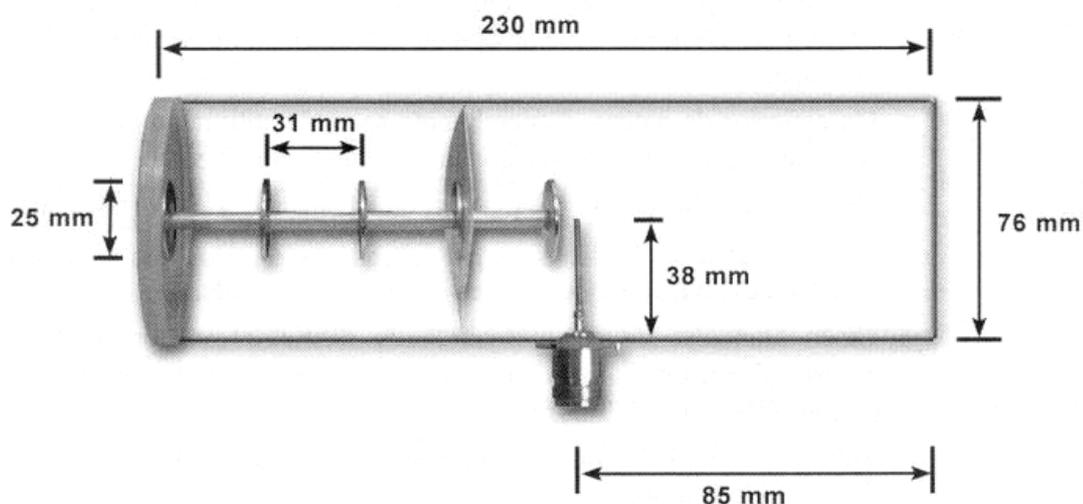
Por cierto, una vez montada la antena, las arandelas actúan como amplificadores de la señal. Lo que hace que esta antena sea apta para Wi-Fi es la distancia entre las arandelas (la longitud de los tubos de aluminio). Esta distancia está relacionada con la frecuencia por la siguiente fórmula (simplificada para este caso):

$$L = 75 / F$$

Donde L es la longitud de los tubos de aluminio (un cuarto de longitud de onda) en milímetros y F, la frecuencia en GHz.

Si hacemos estos cálculos para la frecuencia menor de Wi-Fi (2,412 GHz, la del canal 1) y la mayor (2,462 GHz, la del canal 2), vemos que la longitud de los tubos podría variar entre los 31,1 y los 30,46 milímetros. Como, en cualquier caso, las herramientas domésticas no tienen la precisión suficiente como para afinar estas medidas, nos podemos quedar con los 31 milímetros.

Las siguientes dos piezas que tenemos que preparar son la tapa del bote de Pringles, a la que hay que hacerle un agujero en el centro para que pase la varilla roscada, y el disco de plástico, al que hay que cortar con un diámetro exterior de 73 milímetros y hacerle un agujero en el centro de unos 6 milímetros para que quepa el tubo de aluminio.



*Figura 4.22 Esquema de construcción de una antena Pringles  
(www.oreillynet.com/lcs/ weblog/Mewlwlgl4481, diciembre 2005)*

A continuación debemos ensamblar el tubo formando la pieza de la imagen. Consiste en poner una tuerca en un extremo de la varilla e ir introduciendo por el otro extremo el resto de las piezas en el siguiente orden: tapa del bote, arandela, tubo, arandela, tubo, arandela, tubo con el disco de plástico, arandela, tubo, arandela; y cerramos el montaje con una tuerca. Si es necesario, limamos el resto de varilla que nos haya sobrado.

Vamos con el bote. El cable de cobre debe soldarse al conector y el conector debe fijarse en la pared del bote. El resultado debe ser que el cable de cobre llegue justo al centro del bote. Como hay distintos modelos de conectores, es posible que la longitud del cable de cobre pueda variar de unos modelos a otros. En general, estará en torno a los 27 milímetros de longitud.

El cable de cobre debe estar recto y bien soldado al conector. Para fijar el conector al bote, deben hacerse unos agujeros en un lateral de forma que el cable de cobre quede justo delante de la varilla sin tocarla. Esto supone situar el conector a unos 85 milímetros de la base del bote.

Por último, montamos la varilla en el bote, conectamos el conector al equipo Wi-Fi mediante un cable adecuado y listo.

*(www.oreilynet.com/es/Weblog/Mew/wlgl4481, diciembre 2005)*

## CAPÍTULO 5

### APLICACIONES DE LAS REDES Wi-Fi

#### 5.1 APLICACIONES

La popularización de la tecnología inalámbrica está suponiendo un creciente interés por parte de los usuarios y de las empresas proveedoras en buscar soluciones alternativas más fáciles de implantar a las necesidades de comunicaciones existentes o a las nuevas necesidades que puedan surgir.

Se puede decir que las aplicaciones de las redes inalámbricas se pueden dividir en tres campos:

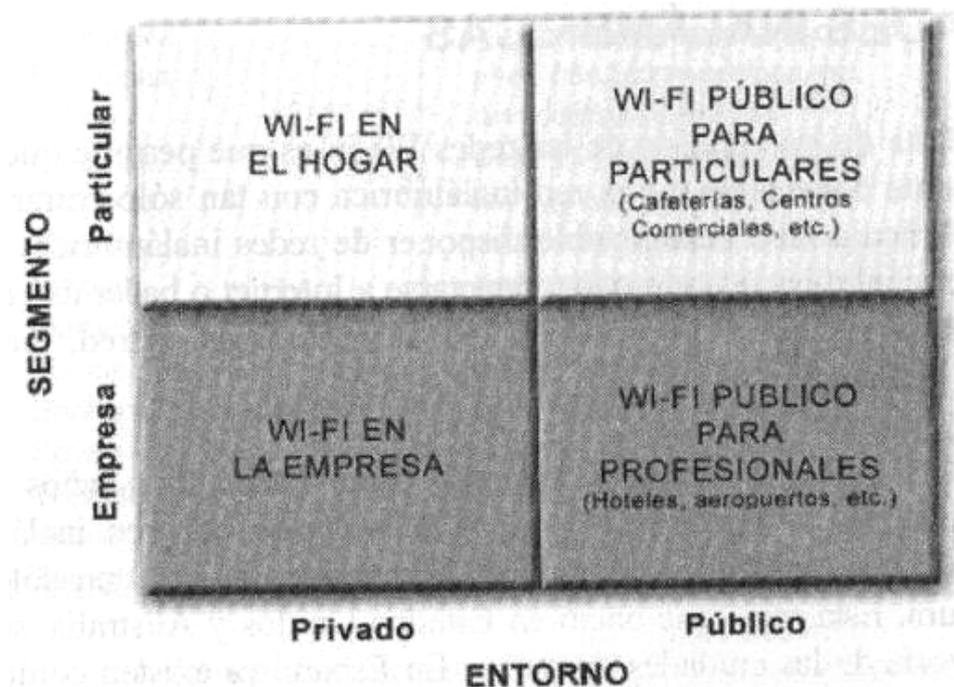
- Aplicaciones relacionadas con la facilidad de comunicar dispositivos portátiles. Si se dispone de un ordenador portátil o PDA, éstos pueden disponer de conexión con el resto de la red local o con Internet sin necesidad de tener que estar atados a un conector de red. Es más, se puede disfrutar de estos servicios aunque se permanezca en movimiento.
- Aplicaciones relacionadas con la facilidad de configuración y reorganización. Las redes de área local cableadas son complicadas de instalar por la necesidad que tienen de disponer un conector al lado de cada ordenador. Incluso reorganizar una red cableada puede ser todo un problema si la nueva disposición no coincide con los lugares donde hay red. Las redes inalámbricas son fáciles de instalar y no tienen necesidad de modificación cuando los ordenadores se cambian de sitio.
- Aplicaciones relacionadas con su facilidad de establecer comunicación punto a punto vía radio. Cablear una red local dentro de un edificio puede ser una tarea abordable, pero interconectar las redes de dos edificios o comunicar dos ordenadores distantes es muy complicado de hacer por los propios medios vía

cable. Resolver esto vía inalámbrica no supone mucho problema. La única limitación es que, si la distancia es grande, debemos contar con visibilidad directa entre los extremos.

Aparte de lo anterior, la existencia de los servicios de acceso a Internet con banda ancha y la popularización de las redes inalámbricas está llevando a un creciente interés por parte de las empresas proveedoras en ofrecer servicios y aplicaciones basados en el hecho de que los usuarios pueden disponer de un dispositivo inalámbrico en cualquier lugar y con una alta velocidad de acceso hacia y desde Internet. Esto le da un valor añadido importante a los servicios de banda ancha como juegos multimedia videoconferencias, televigilancia, visitas virtuales, telereunión, teleformación, retransmisión de eventos, recepción de televisión, radio, acceso a disco duro virtual interconexión de redes, teleasistencia, teletrabajo, trabajo en grupo, etc.

Un campo de aplicación que todavía no está muy extendido es el del control de los dispositivos del hogar desde el ordenador. Programar la calefacción, controlar el dispositivo de riego o poner en marcha el microondas desde el ordenador no es abordable si hay que llenar la casa de agujeros por los que poner los cables; sin embargo, es mucho más asimilable si lo único que hay que hacer es conectar unos dispositivos inalámbricos a cada aparato, para, a continuación, poder controlarlos, tanto desde el ordenador de casa como desde cualquier parte del mundo a través de Internet. Desde este punto de vista, hacer televigilancia del hogar o poner en marcha o apagar cualquier aparato puede que se convierta en habitual dentro de un tiempo.

(<http://www.unincca.edu.co/boletin/indice.html> , enero 2006)



*Figura 5.1 Área de aplicación Wi-Fi*  
(<http://www.unincca.edu.co/boletin/indice.html>, enero 2006)

### 5.1.1 Aplicaciones en la empresa

Las redes inalámbricas son aplicables en cualquier campo de la industria donde exista la necesidad de utilizar un dispositivo informático, tener movilidad y permanecer en contacto en tiempo real con recursos informáticos de dentro o fuera de la empresa.

Las redes inalámbricas son especialmente útiles cuando los empleados necesitan acceder a la información desde distintos sitios o mantener una cierta movilidad. Éste sería el caso, por ejemplo, de médicos, enfermeras, inspectores, agentes, vendedores, personal de mantenimiento, personal de almacén, atención al cliente, personal de exposición, etc.

Para ver las ventajas de las redes inalámbricas, simplemente hay que pensar en la alternativa actual: utilizar formularios en papel, copiar del papel al ordenador, manejar información impresa no actualizada, tener que moverse para conseguir acceder a la

información de la empresa, etc. Esto trae consigo la duplicación del trabajo, aumentar los tiempos de respuesta, introducir errores de interpretación de la escritura manual, manejar información no actualizada, perder tiempo en desplazamientos innecesarios, etc.

Un ordenador portátil o PDA con conexión inalámbrica puede mejorar grandemente el rendimiento y eficacia de muchos puestos de trabajo: facilita la movilidad, elimina el papeleo, disminuye los errores, reduce los costes de gestión, acerca la empresa al trabajador, aumenta la eficiencia. (<http://www.unincca.edu.co/boletin/indice.html>, enero 2006)

## **5.2 COMUNIDADES INALÁMBRICAS**

Una de las ventajas de las redes Wi-Fi es que permite que cualquier usuario pueda fácilmente conectarse a una red inalámbrica con tan sólo entrar en su área de cobertura. Esta particularidad hace posible disponer de redes inalámbricas públicas a las que puede acceder cualquier usuario para conectarse a Internet o hacer uso de cualquier otro servicio que ofrezca (uso de impresoras, uso de programas en red, juegos, almacenamiento de información, etc.).

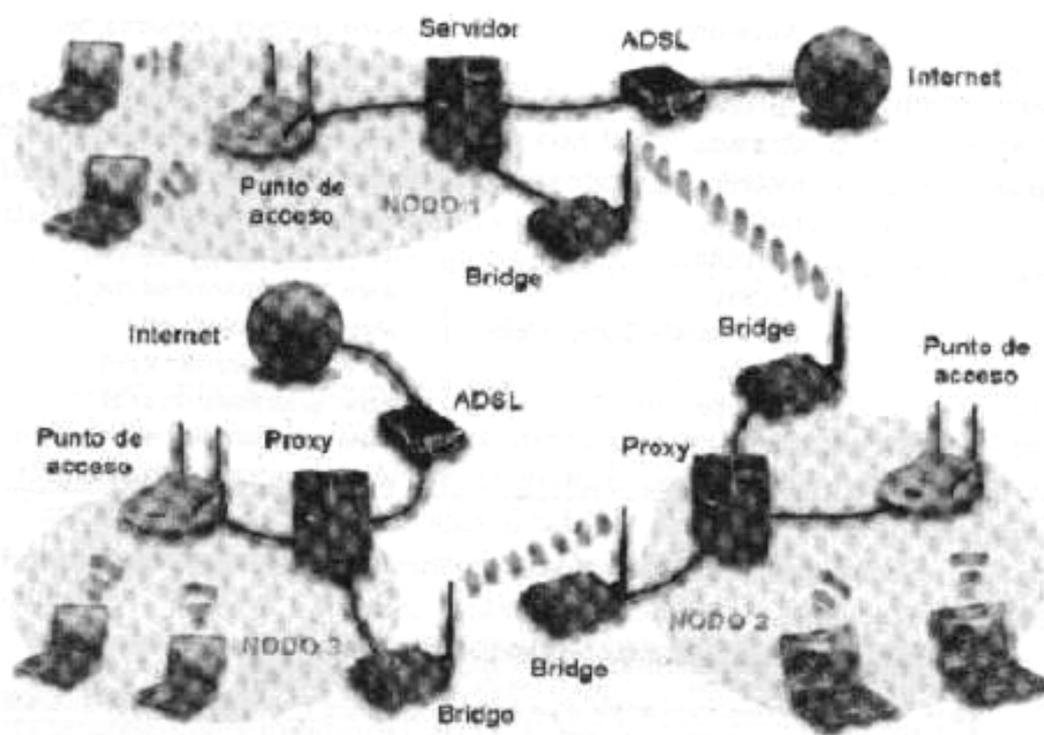
La facilidad anterior permitió que hace unos años un grupo de jóvenes pertenecientes a movimientos ciudadanos crease una red inalámbrica pública a la que podía acceder cualquier persona de forma gratuita con tan sólo situarse en su área de cobertura. Esta idea, que nació en Estados Unidos y Australia, se propagó rápidamente a la mayoría de las ciudades europeas.

Las comunidades inalámbricas están formadas por voluntarios que, en algunos casos, cuentan con el apoyo de algunas empresas o instituciones. Las empresas suelen ser distribuidores informáticos que donan equipos o los venden con grandes descuentos. (<http://www.unincca.edu.co/boletin/indice.html>, enero 2006)

### 5.2.1 Organizaciones de las comunidades inalámbricas

Técnicamente, una comunidad inalámbrica es una red de redes inalámbricas interconectadas entre sí para crear una red única con cobertura, generalmente, metropolitana o regional, pero que podría llegar a tener alcance nacional o internacional.

Cada red está gestionada por un administrador de red y está formada por los ordenadores o dispositivos Wi-Fi de los usuarios, uno o más puntos de acceso y los equipos y enlaces necesarios para hacer funcionar la red y las interconexiones de la red con el resto de la comunidad. A cada punto de acceso se le conoce con el nombre general de nodo.



*Figura 5.2 Esquema de comunidad Wi-Fi.*  
(<http://www.unincca.edu.co/boletin/indice.html>, enero 2006)

Para que toda la comunidad funcione de forma interconectada, es imprescindible que exista un acuerdo en el uso de las direcciones IP. Cada red inalámbrica, cada administrador, necesita su propio rango de direcciones IP para poder asignar direcciones

a sus usuarios. Por otro lado, la comunidad necesita determinadas direcciones IP para los elementos de red (servidores DNS, routers, etc.). Además, no puede haber dos direcciones repetidas. La gran ventaja es que no se utilizan IP públicas de Internet, sino IP privadas. Las direcciones IP privadas pueden ser utilizadas por los administradores de red con total libertad, sin que las instituciones que gestionan la numeración de Internet tengan que intervenir.

(<http://www.unincca.edu.co/boletin/indice.htm>, enero 2006)



Figura 5.3 Segmentación del mercado de acceso libre.  
(<http://www.unincca.edu.co/boletin/indice.html>, enero 2006)

### 5.3 REDES COMERCIALES DE ACCESO PÚBLICO INALÁMBRICO

Una comunidad inalámbrica puede convertirse, con la configuración adecuada, en una red inalámbrica de acceso público que ofrezca una serie de servicios comerciales. Quizás, el principal de los servicios sea el acceso a Internet desde lugares públicos (cafeterías, aeropuertos, etc.), pero este servicio se puede complementar con otros como uso de impresoras, uso de programas ni red, juegos, almacenamiento de información,

A las redes inalámbricas que ofrecen sus servicios al público se las conoce como redes inalámbricas de acceso público, PWLAN (Public Wireless Local Area Network, 'Red Pública Inalámbrica de Área Local') o, simplemente, hot-.spot (punto caliente en inglés).

Las redes comerciales de acceso público inalámbrico sitúan sus puntos de acceso en aquellos lugares donde existe una gran asistencia de público con tiempo suficiente para conectarse a Internet para realizar cualquier tarea profesional o personal. Estos lugares suelen ser hoteles, centros de convenciones, aeropuertos, campus universitarios, centros comerciales, cafeterías, restaurantes, etc. En estos lugares les ofrecen a sus usuarios la facilidad de acceder a Internet desde su propio ordenador (previamente dotado con una tarjeta Wi-Fi). Los proveedores de este servicio suelen cobrar una cuota mensual fija, una tarifa por uso o ambas cosas, ofreciendo la posibilidad de hacer uso de su servicio desde cualquier punto de su red.

PAIS	EMPRESA	OBJETIVOS
<i>Alemania</i>	<i>Lobox</i>	<i>Hoteles</i>
<i>Reino Unido</i>	<i>BT</i>	<i>Aeropuertos</i>
<i>Austria</i>	<i>Connect One</i>	<i>Hoteles</i>
<i>Italia</i>	<i>Megabeam</i>	<i>Hoteles y aeropuertos</i>
<i>Suecia</i>	<i>Telia</i>	<i>Hoteles y aeropuertos</i>
<i>España</i>	<i>Telefónica</i>	<i>Hoteles, aeropuertos, centros comerciales, etc.</i>
<i>España</i>	<i>Kubi Wireless</i>	<i>Hoteles y aeropuertos</i>
<i>España</i>	<i>Afitel</i>	<i>Ciudad de Zamora</i>
<i>USA</i>	<i>Cometa, Wayport</i>	<i>Hoteles y aeropuertos</i>

*Tabla 5.1 Ejemplos de WISP.*  
(<http://www.unincca.edu.co/boletin/indice.html>, enero 2006)

Los usuarios principales de este tipo de servicios son dos: Personas de negocios que se desplazan continuamente y tienen necesidad de mantener acceso a Internet (desde los hoteles, aeropuertos, etc.) y el gran público que aprovecha su estancia en un lugar público (cafetera, centro comercial, etc.) para pasar un tiempo de ocio. Los servicios de acceso público inalámbrico son vistos como una oportunidad de negocio tanto por los operadores de telecomunicaciones de red fija y móviles, como por empresas

independientes. Al proveedor de este tipo de servicios se le conoce por el término general de WISP (Wireless Internet Service Provider, 'Proveedores de Acceso Inalámbrico a Internet'). Éste es el caso de Tmobile en Estados Unidos, Telia HomeRun en Europa o Telefónica, Kubi Wireless y Wireless&Satellite Networks. No obstante, donde más se está desarrollando este mercado es en Japón y Corea. En estos países existe un gran número de WISP y, curiosamente, utilizados en gran medida por los usuarios de PDA.

(<http://www.unincca.edu.co/boletin/indice.html>, enero 2006)

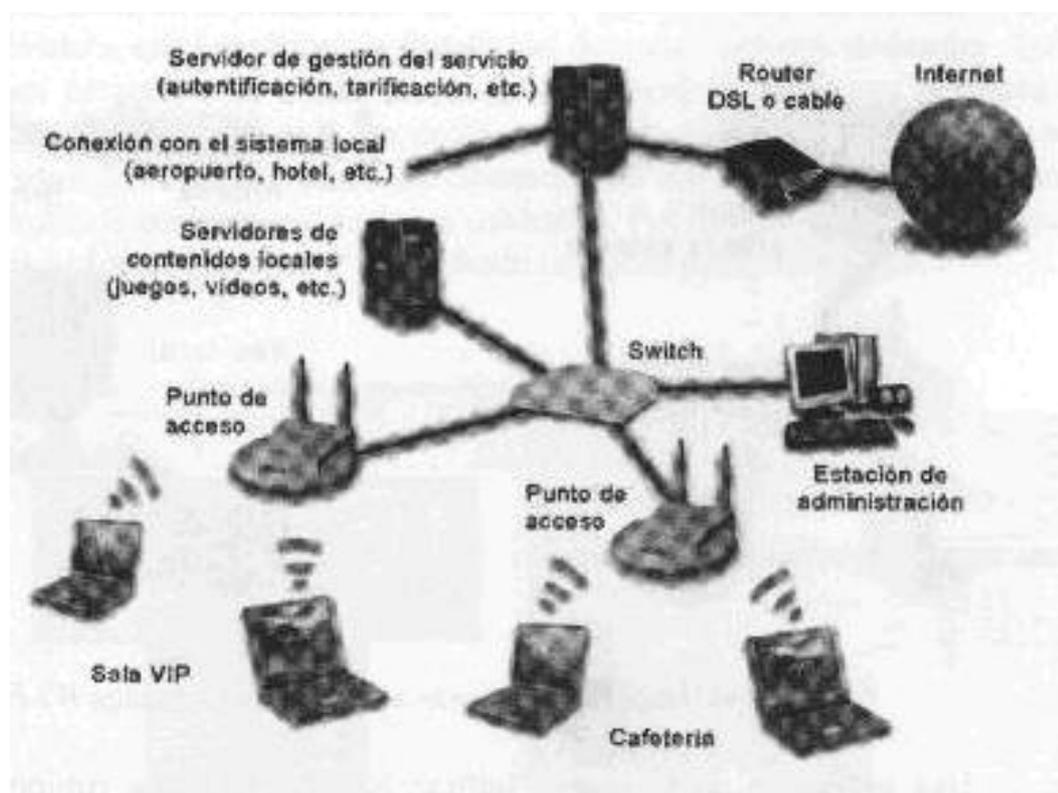
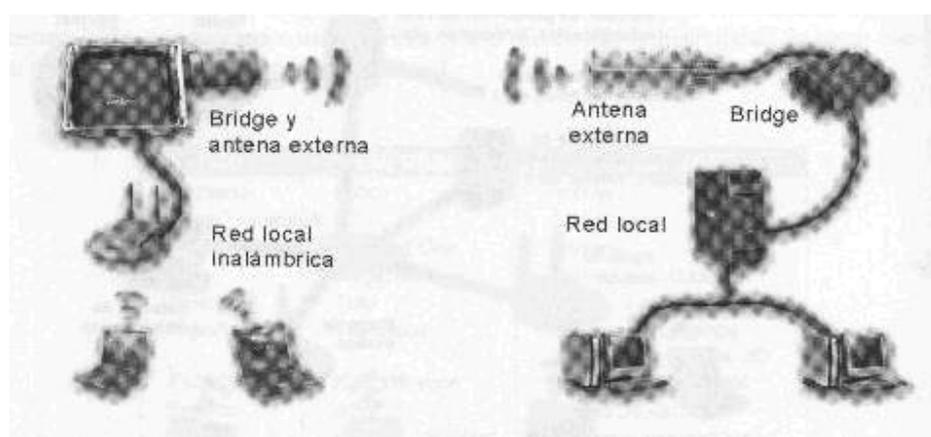


Figura 5.4 estructura de una red inalámbrica de acceso público.  
(<http://www.unincca.edu.co/boletin/indice.html>, enero 2006)

## 5.4 ENLACE PUNTO A PUNTO

Aunque el estándar Wi-Fi es utilizado habitualmente para crear redes locales inalámbricas, también puede utilizarse para crear un enlace de comunicación entre dos puntos. Esta facilidad sirve, por ejemplo, para interconectar dos edificios de una forma fácil, rápida y barata. Tradicionalmente, para establecer una comunicación entre dos puntos que no estuviesen situados en un mismo entorno privado, sólo existía la alternativa de recurrir a un operador de telecomunicaciones. Esto supone pagar una cuota de alta y una tarifa mensual más o menos elevada. Con Wi-Fi se puede establecer esta misma conexión (hasta 11 Mbps) con un único coste de compra de los equipos (e instalación si es el caso). Posteriormente, no hay que hacer ningún pago mensual, salvo los posibles trabajos de mantenimiento, si los hubiera.

Aunque se puede establecer una comunicación punto a punto utilizando puntos de acceso o tarjetas de red, en el mercado existen unos equipos Wi-Fi especialmente pensados para este trabajo. A estos equipos se les conoce con el nombre de wireless bridge ('puente inalámbrico'). Un bridge inalámbrico interconecta dos ordenadores o dos redes remotas (cableadas o no) mediante una conexión inalámbrica. Una conexión inalámbrica requiere de dos equipos bridges inalámbricos, uno en cada extremo.



*Figura 5.5 enlace punto a punto con un bridge Wi-Fi.  
(<http://www.unincca.edu.co/boletin/indice.html>, enero 2006)*

Una aplicación en la que se utilizan habitualmente los equipos bridge es en la interconexión de puntos de acceso para crear una red extensa inalámbrica que cubra todo un campus, zona empresarial, vecindario o ciudad. Los equipos bridge pueden establecer enlaces punto a punto o punto a multipunto.

Un par de equipos bridge complementados con antenas direccionales y una buena instalación puede llegar a establecer enlaces de más de 10 kilómetros. En algún caso, para eliminar al máximo las pérdidas del cable y conectores, se instala el bridge en una caja estanca pegada a la antena. Hay que tener en cuenta que cada 3 dB de pérdida supone disminuir la potencia a la mitad.

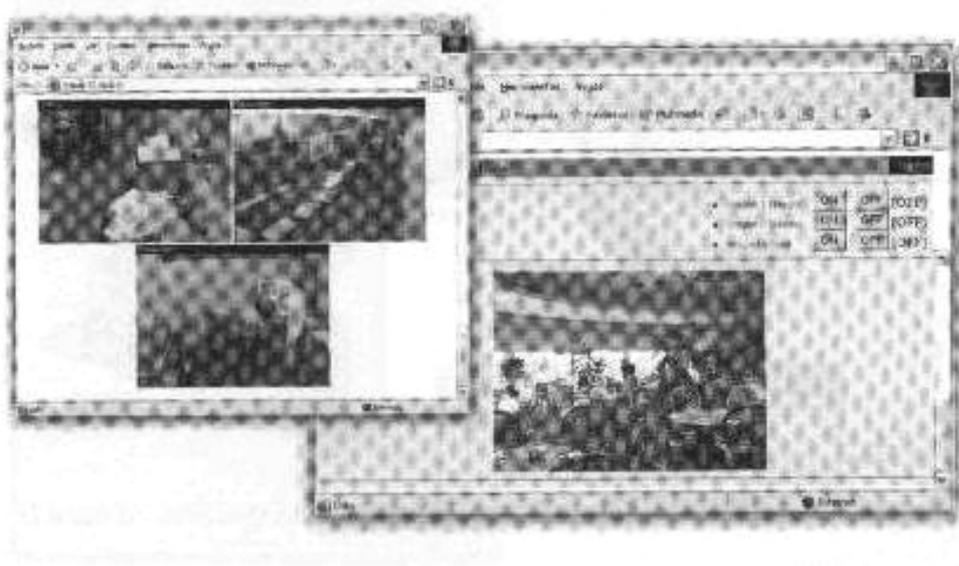
Por si tiene curiosidad, el récord del mundo de distancia alcanzada con un enlace Wi-Fi lo tiene, por ahora, la Asociación Canana de Redes Inalámbricas ([www.acri.ws](http://www.acri.ws)), quienes consiguieron establecer un enlace a 1 Mbps entre dos de las Islas Canarias, cubriendo una distancia de 70,5 Km. El evento tuvo lugar el 3 de agosto de 2002 a las 16:30 horas durante FICIT (Fiesta Canaria de Informática y Telecomunicaciones), Se utilizó una antena de rejilla de 24 dB sin amplificador. Se conectó el Mirador de los Campitos en Santa Cruz de Tenerife con la montaña de Gáldar en Gran Canarias.

Curiosamente, este mismo equipo de personas (Alejandro Cámara, José Padilla, Eric Gibaud, Víctor de la Nuez, Williams de la Nuez y Rubén Delgado) ya se habían hecho un mes antes con el récord de España al cubrir la distancia de 54 Km. (<http://www.unincca.edu.co/boletin/indice.html>, enero 2006)

## **5.5 TELEVIGILANCIA**

La televigilancia consiste en poder ver desde un lugar lo que está ocurriendo en otro lugar mediante la transmisión de video y audio. Tradicionalmente, la televigilancia se ha llevado a cabo mediante la instalación de Caros circuitos dedicados. Internet y las soluciones de acceso de banda ancha (DSL o módem cable) nos permiten establecer soluciones de televigilancia a un Coste muy bajo. Además, la tecnología inalámbrica

permite situar los dispositivos de televigilancia (las cámaras) de una forma fácil y rápida, sin depender de costosas instalaciones cableadas. Por otro lado, Internet ofrece la ventaja de que las imágenes pueden ser vistas desde cualquier parte del mundo.



*Figura 5.6 imágenes de televigilancia con cámaras Wi-Fi.  
(www.dti2.net/televigilancia.asp, enero 2006)*

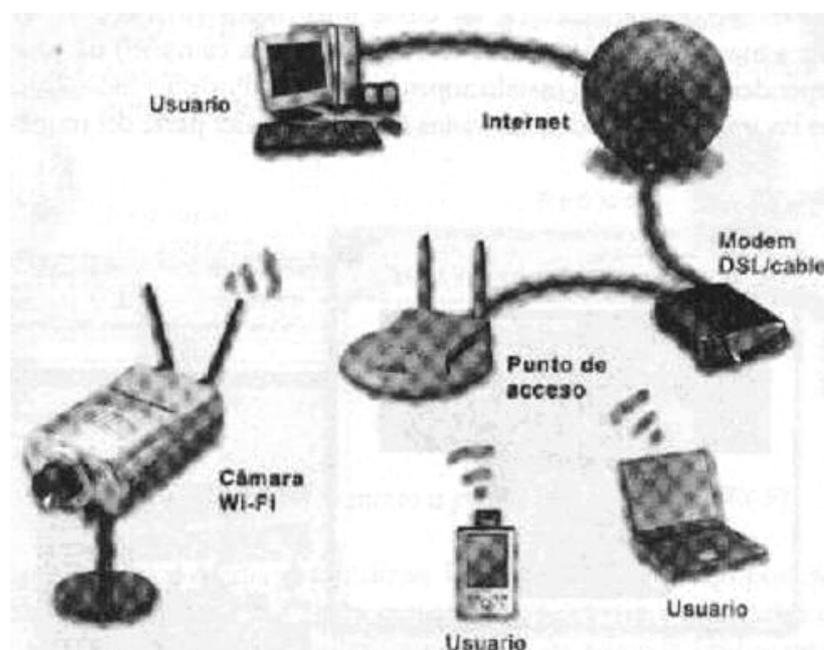
En el mercado existen cámaras inalámbricas Wi-Fi que permiten situar la cámara en cualquier lugar, con la sola necesidad de disponer un enchufe de alimentación eléctrica o, en su defecto, de una batería. La señal de video se transmite vía Wi-Fi hasta la red local o Internet.

Hay que tener claro que estas soluciones de televigilancia sólo ofrecen la posibilidad de ver imágenes de forma remota. En ningún caso, esta simple retransmisión de imágenes sustituye a los múltiples servicios de vigilancia y asistencia de las empresas profesionales de este sector.

Las cámaras inalámbricas suelen disponer de un servidor Web interno al que se puede acceder tanto para la configuración de la cámara como para ver su imagen. La cámara se configura como cualquier otro dispositivo inalámbrico (a excepción de las propiedades

de video que son propias de este dispositivo). Si se dispone de varias cámaras, existen aplicaciones (como IPView) que permiten gestionarlas simultáneamente e, incluso, realizar grabaciones de las imágenes.

Para determinadas aplicaciones resulta más conveniente llevar la imagen de la cámara a un servidor desde donde se ofrece al público. También existen empresas en Internet que, por un módico precio, colocan en sus servidores las imágenes de video recogidas por las cámaras Web de sus clientes.



*Figura 5.7 sistemas de televidencia mediante cámara IP  
(www.dti2.net/televidencia.asp, enero 2006)*

En cualquier caso, la televidencia a través de Internet resulta una buena solución de supervisión de instalaciones y dependencias tanto para el uso particular (supervisión de los niños, vigilancia de la casa, etc.) como para la pequeña empresa y profesionales (supervisión de instalaciones, tiendas, almacén, despacho, teletrabajadores, etc.). Además, estos sistemas permiten ser combinados con el envío de mensajes de correo electrónico o llamadas al teléfono móvil en el caso de dispararse alguna alarma.

Como conclusión, podemos ver a continuación algunas de las aplicaciones de los sistemas de televigilancia por Internet:

- **Residencial.** Permite supervisar el estado del hogar o de la segunda residencia.
- **Guarderías.** Los padres autorizados pueden ver a sus hijos en la guardería.
- **Personas mayores.** Permite estar en contacto directo con las personas mayores que vivan solas.
- **Comunidad.** Permite que cualquier vecino pueda ver las instalaciones comunes para supervisar el juego de los niños o el aparcamiento del coche.
- **Industrial.** Control de almacenes solitarios, verificación de alarmas, etc.
- **Construcciones y proyectos.** Permite que los clientes puedan ver el estado de la construcción o el proyecto sin tener que desplazarse.
- **Vigilancia.** Para ver y vigilar a distancia distintos centros desde una oficina central.

Por último, las cámaras inalámbricas tienen la posibilidad de ser instaladas sobre personas o equipos en movimiento. Esto las hace ideales para cámaras subjetivas en la retransmisión o grabación de imágenes deportivas o de aventura.

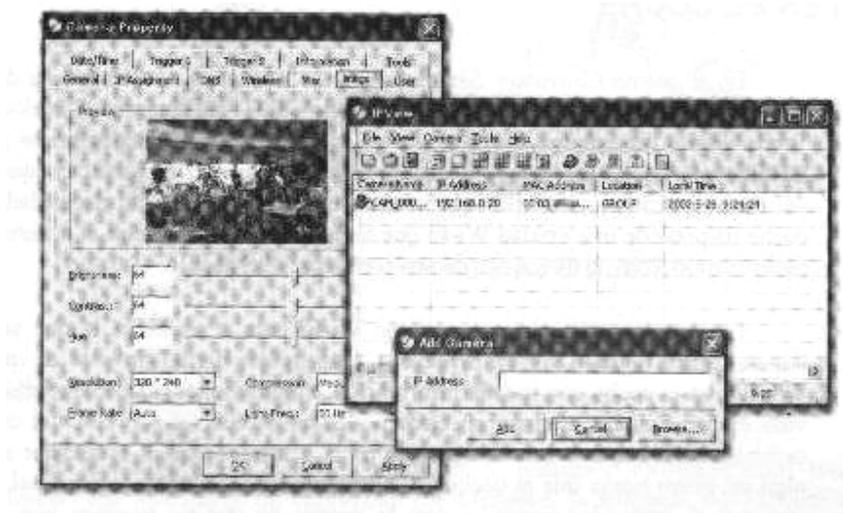


Figura 5.8 Aplicaciones IPview para gestionar varias cámaras.  
([www.dti2.net/televigilancia.asp](http://www.dti2.net/televigilancia.asp), enero 2006)

## 5.6 WI-FI EN EL COCHE

En el último Consumer Electronics Show ('Muestra de Electrónica de Consumo'), que tuvo lugar en Las Vegas en enero de 2003, las empresas Linksys y Zadiant Technologies presentaron una serie de aplicaciones de redes inalámbricas para el coche.

La aplicación que más llamó la atención fue la posibilidad de cargar el equipo de música del coche con la música MP3 que se tiene en el PC de casa sin necesidad de cables. El coche dispone de una unidad Wi-Fi que le permite conectarse con el ordenador de casa y hacer la transferencia de música de una forma rápida y fácil.

Otra de las aplicaciones que tiene Wi-Fi para el coche es la que se ha venido a llamar maleta digital (Digital Briefcase). Una maleta digital consiste en que se lleva un servidor en el coche con toda la información y aplicaciones que necesitamos para nuestra vida diaria. Cuando estamos en casa, podemos acceder al servidor del coche desde el ordenador del hogar y cuando estamos en la oficina, desde el ordenador del trabajo. Es algo así como pensar que el coche es una herramienta informática personal, más personal aún que el ordenador portátil y con la ventaja de que no tenemos que cargar con él.

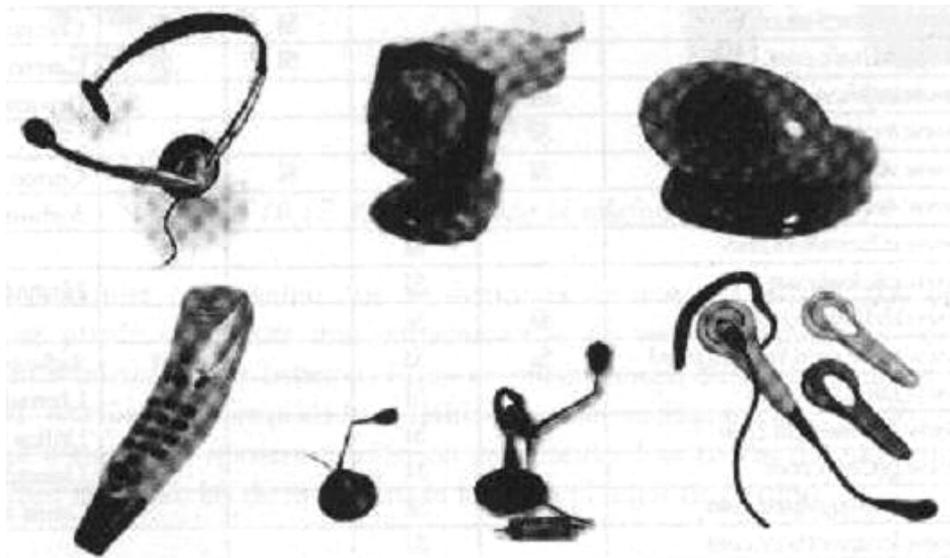
Obviamente, el inconveniente de este tipo de aplicaciones es que se necesitaría estar siempre a una distancia del coche inferior a los 100 metros. En las grandes ciudades esto no es posible muchas veces ni siquiera en la casa.

Por otro lado, el disponer de Wi-Fi en el coche hace posible que se pueda acceder a Internet desde él. Bastaría con acercarse a un punto Wi-Fi público (conocidos en inglés como hot-spot) para poder leer el correo electrónico, acceder a las noticias o bajarse la música o vídeo para el resto del trayecto. Uno de los sitios propicios para este tipo de actividades son las gasolineras, áreas de descanso de las autopistas o aparcamientos públicos.

Yendo un poco mas allá, hay quien habla de aprovechar este enlace entre el coche e Internet para poder tener el coche vigilado y localizado. Una cámara en el interior y un sistema GPS pueden complementar el equipamiento para permitir un sistema de vigilancia y localización del vehículo.

Ciertamente, todo lo anterior no estará disponible en el mercado hasta el año 2004 o 2005. Empresas como DaimlerChrysler, Fiat, 3Com, Linksys, Zadiant o Awa están trabajando en estos temas.

*(es.wikipedia.org/wiki/Gíreles, enero 2006)*



*Figura 5.9 distintos equipos de telefonía y videoconferencia por Internet.  
(es.wikipedia.org/wiki/Gíreles, enero 2006)*

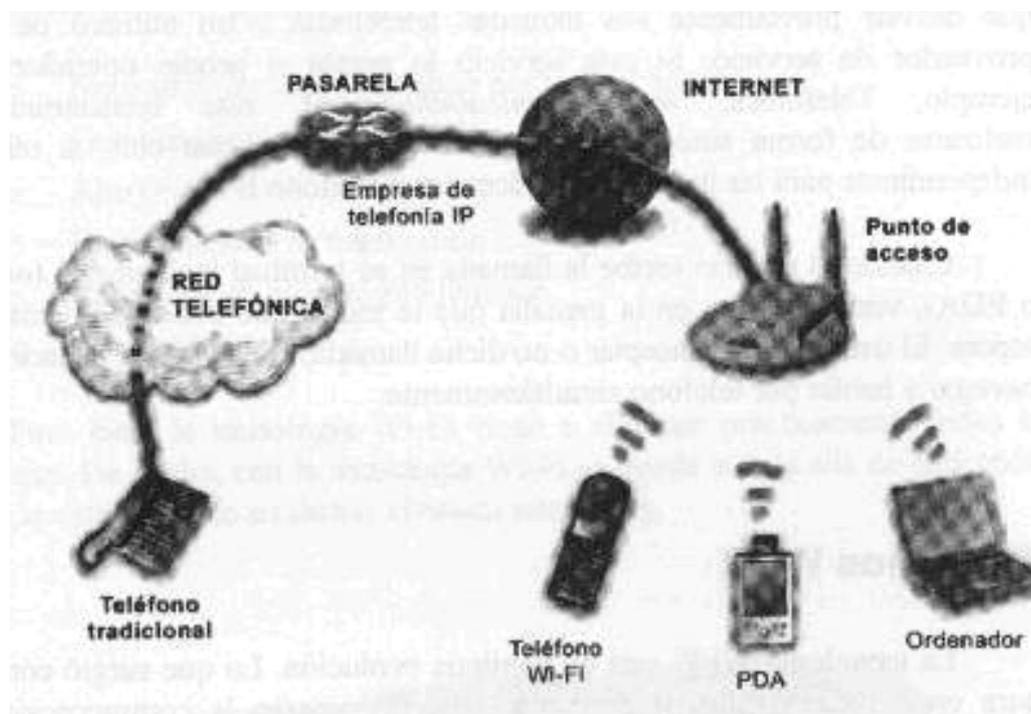
## 5.7 TELEFONÍA WI-FI

La telefonía Wi-Fi permite establecer y mantener conversaciones telefónicas utilizando sus facilidades de movilidad. En definitiva, la telefonía Wi-Fi viene a ser la unión de las redes inalámbricas y de la telefonía IP.

La telefonía Wi-Fi puede tener su campo principal de aplicación en las empresas y sectores como la educación, salud, fabricación o almacenamiento, donde la movilidad de los trabajadores es un factor importante. La ventaja que ofrece la telefonía Wi-Fi frente las comunicaciones inalámbricas de voz actuales (Dect) es que permite integrar la facilidad de transmisión de voz con la de datos y video. Adicionalmente, la existencia de lugares de acceso público Wi-Fi (hot-spot) permite disponer de un servicio telefónico inalámbrico de bajo coste desde lugares públicos.

Para poder hacer uso de esta tecnología, se espera disponer tanto de terminales telefónicos específicos, como de terminales multipropósitos: PDA y ordenadores portátiles. Los terminales basados en PDA pueden resultar muy interesantes, ya que permiten integrar las funciones de telefonía, video y datos en un solo terminal de reducido tamaño.

Los retos que tienen que vencerse en la actualidad para la introducción de este servicio son tres, fundamentalmente: la calidad de audio en una red abierta llena de interferencias y retardos, que actualmente no está garantizada la continuidad del servicio cuando se desplaza el usuario y la falta de seguridad de las comunicaciones Wi-Fi. A pesar de lo anterior, para todas las pegas anteriores, existen soluciones que harán que este servicio sea posible con todas las garantías a corto o medio plazo.



*Figura 5.10 estructura de la telefonía por Internet.  
(peoplecall.typepad.com, enero 2006)*

En cualquier caso, salvo que se disponga de una red Wi-Fi muy congestionada, siempre se puede establecer una comunicación de voz utilizando los servicios de las empresas de telefonía por Internet. Estas empresas hacen de intermediarios entre Internet y la red telefónica permitiendo establecer una comunicación telefónica desde un ordenador a cualquier número telefónico del mundo. Las tarifas de estas empresas suelen ser algo más altas que las de una llamada local en el lugar de destino.

En el mundo existen muchas empresas de telefonía por Internet. Generalmente, suelen utilizar el sistema de prepago, de forma que el usuario sólo tiene que recargar su cuenta con la cantidad que estime oportuna y podrá hablar hasta que se le agote el saldo.

*(peoplecall.typepad.com, enero 2006)*

### **5.7.1 Recibir llamadas en el terminal Wi-Fi**

Cuando se dispone de un terminal inalámbrico Wi-Fi desde donde se pretende realizar las comunicaciones telefónicas, esto implica disponer de la posibilidad tanto de realizar llamadas como de recibirlas. Ya hemos visto que, para realizar las llamadas, se necesita disponer de los servicios de una empresa intermediaria que transfiera la llamada de Internet a la red telefónica, pero qué pasa cuando lo que se pretende es recibir las llamadas telefónicas ni el terminal inalámbrico.

Para solucionar este problema, algunos fabricantes han desarrollado un sistema que convierte las llamadas telefónicas en datos IP que puedan ser remitidos al PC del usuario (o al teléfono IP) por un proveedor de servicio. Para que esto funcione, el usuario tiene que desviar previamente sus llamadas telefónicas a un número de teléfono de su proveedor de servicio. Si este servicio lo presta el propio operador telefónico (por ejemplo, Telefónica, [www.telefonicaonline.com](http://www.telefonicaonline.com)), este reencaminamiento podría realizarse de forma automática. También se puede contar con un número telefónico independiente para las llamadas al ordenador o teléfono IP.

Cuando el usuario recibe la llamada en su terminal inalámbrico (ordenador portátil o PDA), verá un icono en la pantalla que le indica que tiene una llamada telefónica en espera. El usuario puede aceptar o no dicha llamada. De hecho, el usuario podría, incluso, navegar y hablar por teléfono simultáneamente.

*(peoplecall.typepad.com, enero 2006)*

### **5.7.2 Teléfonos Wi-Fi**

La tecnología Wi-Fi está en continua evolución. Lo que surgió como una solución para crear redes locales inalámbricas que permitieran la comunicación de datos está evolucionando hacia un sistema inalámbrico que da soporte a cualquier necesidad de comunicación: datos, voz, imagen, etc.

En este sentido, ya se ha anunciado la aparición, dentro de este año 2003, de terminales telefónicos inalámbricos de tecnología Wi-Fi. Estos terminales permiten recibir y realizar llamadas telefónicas de voz siempre que se esté dentro del área de cobertura de una red Wi-Fi (dentro de la empresa, en la casa o conectado a alguna red Wi-Fi pública). Para evitar tener que llevar encima dos terminales distintos (uno Wi-Fi y otro de telefonía móvil), algunos fabricantes ya han prometido que ofrecerán terminales multimodos (GSM, Wi-Fi y PCS). Esto posibilitará que, con un solo terminal, se pueda utilizar Wi-Fi cuando se esté dentro del área de cobertura Wi-Fi y GSM o PCS cuando se esté fuera del área de cobertura Wi-Fi.

Los teléfonos Wi-Fi, al igual que los teléfonos IP o la telefonía por ordenador, necesitan que se contrate los servicios de una empresa de telefonía por Internet. Estas empresas pueden ofrecer incluso un número telefónico exclusivo para las comunicaciones de voz sobre IP.

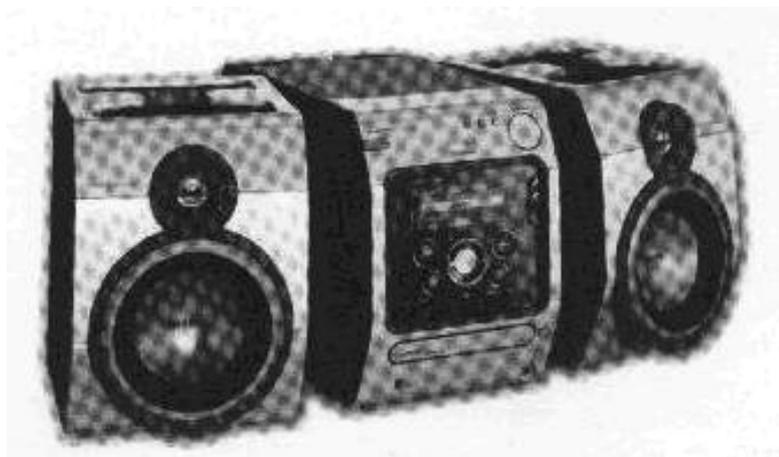
*(www.circo.com, enero 2006)*

## **5.8 EL HOGAR DIGITAL**

Desde hace algunos años se viene hablando insistentemente de la domótica o, lo que es lo mismo, de la automatización del hogar. Cada nuevo desarrollo tecnológico produce inmediatamente que se desarrolle la imaginación para verle una aplicación al hogar. No obstante, su implantación real siempre se ha visto frenada por toda una serie de limitaciones, entre las que se encuentran las siguientes:

- Necesidad de nuevo cableado por todo el hogar
- Complicación en su instalación
- Alto coste
- Baja velocidad de transmisión
- Capacidad de crecimiento limitada
- Compatibilidad

Pues bien, la tecnología Wi-Fi viene a eliminar prácticamente todas las barreras anteriores. De hecho, con la tecnología Wi-Fi se puede ir más allá de la domótica y crear lo que se está viniendo en llamar vivienda inteligente.



*Figura 5.11 Equipo de música por internet a través de Wi-Fi.  
(www.circo.com, enero 2006)*

Una vivienda inteligente consta de tres tipos de redes interconectadas:

- **Red doméstica** o de automatización que interconecta los dispositivos eléctricos del hogar, puntos de luz, calefacción, riego, conmutadores, sistemas de seguridad, etc.
- **Red de entretenimiento** para interconectar la recepción de televisión, películas, radio, juegos, etc.
- **Red de datos** para la interconexión de ordenadores y dispositivos informáticos (impresoras, escáneres, etc.).

El mercado está avanzando en esta idea. De hecho, ya se tiene desarrollado lo que se conoce como pasarela residencial (residencial gateway). Éste es un dispositivo único que hace de interfaz entre el exterior y cada una de las subredes del hogar (domótica, entretenimiento y datos). Los organismos de normalización están realizando un gran

esfuerzo con el objeto de conseguir un estándar común de trabajo que permita desarrollar esta Industria.

Una de las iniciativas de normalización más relevante es la que se conoce como OSGI (Open Services Gateway Initiative, 'Iniciativa de Pasarela de Servicios Abierta').

Ésta es una alianza, establecida en 1999, de las empresas más importantes del sector de las telecomunicaciones, microelectrónica y fabricantes de equipos de consumo con el objetivo de conseguir un estándar capaz de comunicarse con prácticamente cualquier tipo de aparato eléctrico electrónico del hogar.

Por otro lado, en relación con el entretenimiento, en el mercado ya existen soluciones que permiten recibir música, películas o canales de televisión por Internet. Este tipo de recepción garantiza una buena calidad de recepción al no verse sometidas a las limitaciones de las recepciones tradicionales de radiofrecuencia. (*www.circo.com, enero 2006*)

## CONCLUSIONES

Como ya vimos en este trabajo las redes inalámbricas son o pueden llegar a ser de gran importancia para industrias, escuelas, o incluso en nuestro propio hogar.

Wi-Fi es una tecnología ya conocida en Europa ya que de ahí nace, y no tiene mucho tiempo que surgió esta tecnología por lo que su uso puede llegar a durar un buen tiempo, y poco a poco puede ir entrando a nuestro país ya que es una buena tecnología en lo que a redes inalámbricas nos referimos ya que esta tecnología viene a desplazar a otras que son de menor calidad, y como vimos su uso es muy extenso lo cual nos ayuda a que tengamos mayores implementaciones.

Como ya se vio es relativamente fácil el crear una red inalámbrica Wi-Fi, porque seguiríamos teniendo las ventajas de la velocidad (en algunos casos) que nos brinda una red cableada y expandiríamos las posibilidades con la parte inalámbrica, en este trabajo se observó que este tipo de redes pueden llegar a ser más eficientes que cualquier red.

Y si se quiere tener una red inalámbrica de un costo no muy caro y de muy buenas cualidades la tecnología Wi-Fi tiene eso.

## GLOSARIO

**100BASET.** Es el estándar de la red Ethernet que permite velocidades de transmisión de 100 Mbps. Este estándar es también compatible con el estándar anterior 10BaseT. 100BaseT se basa en la norma IEEE 802.3u y se le conoce comúnmente como Fast Ethernet o Ethernet rápido.

**10BASET.** Es el estándar de la red Ethernet que permite velocidades de transmisión de 10 Mbps. 10BaseT se basa en la norma IEEE 802.3.

**802.11.** Conjunto de estándares de red de área local inalámbrica definidos por el IEEE (Institute of Electrical and Electronics Engineers, 'Instituto de Ingenieros Eléctricos y Electrónicos'). Entre estos estándares se encuentra 802.11b, que es en el que se basa Wi-Fi.

### A

**ACCESO TELEFÓNICO.** Establecer una comunicación vía módem utilizando una línea de red telefónica básica. También se le conoce por el término inglés dial-up.

**ACTIVIE X.** Tecnología desarrollada por Microsoft para incluir aplicaciones en las páginas HTML.

**AD HOC.** Véase Modo ad hoc.

**ADDRESS.** Dirección. Véase Dirección.

**ADMINISTRADOR.** Persona responsable del mantenimiento y/o gestión de una red corporativa, red de área local (cableada o inalámbrica) o de un servidor de red.

**ADSL.** Asymmetric Digital Subscriber Line, 'Línea de Abandono Digital Asimétrica'. Tecnología pensada para poder transmitir datos a alta velocidad a través del bucle de abonado de la línea telefónica. El bucle de abonado es el cable de Cobre que va desde la casa del usuario hasta la central telefónica.

**ANCHO DE BANDA.** Es la cantidad de datos que puede circular en un medio por unidad de tiempo. Generalmente se mide en bit por segundos. También puede hacer referencia a un rango de frecuencias.

**AP.** Access point, 'Punto de Acceso'. Véase Punto de acceso.

**API.** Application Program Interface 'Interface entre Programas'. Interfaz que permite la comunicación entre programas, redes y bases de datos.

**APLICACIÓN.** Software que realiza una función particular para el usuario.

**ARP.** Address Resolution Protocol, 'Protocolo de Resolución de Direcciones'. Se trata de un protocolo usado para averiguar la dirección del enlace correspondiente a la dirección IP.

**ASCII.** American Standard Code for Information Exchange 'Código Normalizado Americano para el intercambio de Información'. Se trata de un código que le asigna a cada letra, número o signo empleado por los ordenadores una determinada combinación de ceros y unos. Éste es el código más ampliamente utilizado por todos los ordenadores a escala internacional.

**ASP.** Active Server Pages, 'Páginas de Servidor Activo' Lenguaje de programación creado por Microsoft para permitir aumentar la interactividad con las páginas Web.

**ATENUACION.** Es la reducción o pérdida de potencia de la señal.

**ATM.** Asynchronous transfer mode, 'Modo de Transferencia Asíncrono'. Es una Tecnología de transmisión de datos a alta velocidad, la cual posee la característica de poder transmitir diferentes tipos de información, incluyendo voz, datos, fax, video, audio e imágenes

**AUP.** Acceptable Use Policy, 'Política de Uso Aceptable'. Se refiere a las normas que deben cumplir todos los usuarios que hacen uso de una red.

**AUTENTIFICAR.** Verificar la identidad. La forma mas habitual de verificar la identidad es mediante un nombre de usuario y clave.

## **B**

**BANDA ANCHA.** Hace referencia a las comunicaciones que transmiten datos a alta velocidad. Éste es un término relativo; sin embargo, se suele considerar banda ancha a cualquier comunicación Con velocidad superior a 64 Kbps.

**RANDA DE FRECUENCIAS.** Es un rango de frecuencias del Espectro radioeléctrico. El espectro radioeléctrico está dividido en bandas de frecuencias que Regulatoriamente son utilizadas para distintas finalidades.

**BANDUWITH.** Ancho de banda Véase Ancho de banda.

**BASE DE DATOS.** Cualquier conjunto de información almacenada en cualquier formato. Generalmente, el término se aplica a textos o información gráfica almacenada en un ordenador y accesible de forma sistemática. La información de una base de datos suele estar dividida en registros y éstos, en campos.

**BIT.** La utilidad más pequeña de información. Un bit puede tomar el valor 0 o el valor 1. Los ordenadores internamente, sólo pueden manejar este tipo de información.

**BITS POR SEGUNDO.** Unidad de medida de la velocidad de transmisión de datos por un medio. Indica el número de bits en un segundo que son transmitidos por ese medio.

**BLUETOOTH.** Es una tecnología inalámbrica que permite intercomunicar equipos a una distancia de varios metros (menos de 100 metros). Al contrario que otras tecnologías como Wi-Fi, la tecnología Bluetooth no está pensada para soportar redes de ordenadores, sino, más bien, para comunicar un ordenador o cualquier otro dispositivo con sus periféricos: un teléfono móvil con su auricular, una PDA con su ordenador, un ordenador con su impresora, etc.

**BPS.** Bits por segundo. Véase Bits por segundo.

**BRIDGE.** Puente. Es un dispositivo que interconecta dos redes que utilizan el mismo protocolo haciéndolas funcionar como si se tratara de una sola red. Los puntos de acceso hacen la función de bridge.

**BROADBAND.** Banda ancha. Véase Banda ancha.

**BROWSER.** Navegador. Véase Navegador.

**BSS.** Basic Service Set, 'Conjunto de Servicios Básicos'. Es una de las modalidades de comunicación en las que se pueden configurar los terminales de una red Wi-Fi. En este caso, la red inalámbrica dispone de un equipo (punto de acceso) que se encarga de gestionar las comunicaciones (internas y externas) de todos los dispositivos que forman la red. Este modo de conexión también es conocido como modo infraestructura.

**BYTE.** Una unidad de información formada por 8 bits.

## C

**CABLE COAXIAL.** Es un cable que tiene un conductor Central rodeado de una malla metálica concéntrica que le protege de las interferencias. El cable de la televisión es un ejemplo de cable coaxial.

**CANAL.** La banda de frecuencias en la que trabaja una red inalámbrica se divide en canales. Por cada Canal se puede establecer una comunicación.

**CCK.** Complementary Code Keying, 'Salto de Código Complementario'. Es una técnica de modulación utilizada en Wi-Fi junto con las técnicas de espectro distribuido.

**CERTIFICADO.** Es una información adjunta a una página Web y que garantiza la fuente de dicha información. Los certificados son publicados por compañías independientes dedicadas a la certificación.

**CGI.** Common Gateway Interfece, 'Interfaz de Pasarela Común'. Es un estándar que describe cómo un navegador Web intercambia información con un servidor Web. Esto le permite al servidor leer información introducida por el usuario en una página Web, procesarla y mostrarle los resultados posteriormente.

**CHAT.** Hablar. Sistema de conversación de múltiples participantes en tiempo real. Generalmente, la conversación se lleva a cabo en modo texto, aunque también existen los voicechat de voz.

**CLAVE.** Véase Contraseña.

**CLIENTE.** Es un software que trabaja en el ordenador local para poder hacer uso de algún servicio del ordenador remoto. El software del ordenador remoto que permite ese uso recibe el nombre de servidor. También puede hacer referencia al propio ordenador o dispositivo local que depende del ordenador o dispositivo remoto (llamado servidor). En

las redes Wi-Fi, cliente puede hacer referencia a los dispositivos (ordenadores, PDA, etc.) conectados a la red a través de un punto de acceso.

**CLIENTEISERVIDOR.** Es un sistema mediante el Cual las aplicaciones quedan divididas en dos partes: la parte residente en el ordenador del usuario, el cliente, y la parte residente en un ordenador central compartido, el servidor. El cliente se encarga de hacer de interfaz con el usuario. El servidor se encarga de gestionar la comparación de las aplicaciones, informaciones y periféricos entre los distintos clientes. El sistema cliente/servidor es utilizado tanto en redes de área local como en servicios online.

**CONTRASEÑA.** Es una palabra secreta o secuencia de caracteres que se utiliza para confirmar la identidad de un usuario. Para que sea eficaz, la contraseña debe ser conocida exclusivamente por el usuario y por el proveedor del servicio.

**CORTAFUEGOS.** Es un dispositivo de seguridad (hardware o software) que controla los accesos a una red local desde el exterior (típicamente, Internet).

**CRACKER.** Persona que intenta romper las protecciones de los programas informáticos comerciales para hacer copias ilegales.

**CRC.** Cyclic Redundancy Check, 'Comprobación Cíclica de Redundancia'. Son unos datos adicionales que se adjuntan al final de la información para poder comprobar fácilmente que no ha habido errores en la transmisión. Los datos CRC son el resultado de hacer determinadas operaciones matemáticas con la información original. Como las operaciones son las mismas en origen y en destino, si el resultado no es el mismo, es que hay error en la transmisión.

**CSMAICA.** Carrier Sense Multiple Access with Collicion Avoidance, 'Acceso Múltiple por Detección de Portadora con Evitación de Colisión'. Es el sistema que emplea Wi-Fi para negociar las comunicaciones entre los distintos dispositivos. Este sistema evita que

dos dispositivos puedan intentar hacer uso del medio simultáneamente (evita la colisión).

**CSMA/CD.** Carrier Sense Multiple Access with Collision Detection, 'Acceso Múltiple por Detección de Portadora con Detección de Colisión'. Es el sistema que emplean las redes Ethernet para negociar las comunicaciones entre los distintos dispositivos. Este sistema detecta que dos dispositivos han intentado hacer uso del medio simultáneamente (detecta la colisión) y hace que cada uno lo intente de nuevo en tiempos distintos.

## D

**DAEMON.** En los sistemas UNIX, se le da este nombre al software servidor. Este software está siempre funcionando en segundo plano esperando a que una aplicación cliente solicite sus servicios.

**DECIBELIO.** Es una unidad que mide la relación entre dos valores. Por ejemplo, la relación entre la señal y el ruido o la ganancia se miden en decibelios. Esta unidad se representa por las letras dB y utiliza una escala logarítmica.

**DHCP.** Dynamic Host Configuration Protocol, 'Protocolo de Configuración Dinámica del Host'. Es un protocolo que permite que un servidor asigne dinámicamente las direcciones IP a los ordenadores clientes conforme éstos las van necesitando. La mayoría de los routers (incluso los incluidos en los puntos de acceso) incluyen la Función de servidor DHCP.

**DIAL-UP.** Véase Acceso telefónico.

**DIRECCIÓN.** Cada ordenador conectado a Internet dispone de una dirección que lo identifica. Esta dirección puede estar dada en forma numérica (dirección IP) o alfanumérica (nombre de dominio).

**DIRECCIÓN IP.** Es una cadena numérica que identifica a los ordenadores conectados a Internet. Un ejemplo de una dirección IP es 128.56.78.2.

**DIRECCIÓN MAC.** Es un número único que asignan los fabricantes a los dispositivos de red (adaptadores de red y puntos de acceso). Este número es permanente y viene grabado en el propio dispositivo para permitir identificarlo de forma inequívoca. Las direcciones MAC están formadas por 12 caracteres alfanuméricos (por ejemplo, 12-AB-56-78-90-FE)

**DIVERSIDAD DE ANTENA.** Es una técnica que consiste en añadirle una segunda antena al equipo receptor de radio para conseguir mejorar la calidad de la recepción.

**DNS.** Domain Name System, 'Sistema de Nombres de Dominio'. Este sistema es el encargado de traducir los nombres de dominio (como law.columhiu.edu) de los ordenadores conectados a Internet en direcciones IP (como 128.56.78.2).

**DOWNLOAD.** Se puede traducir como bajar o, menos literalmente, como traer o descargar. Cuando un usuario copia un archivo de un ordenador remoto a su propio ordenador, se dice que el archivo ha sido bajado (downloaded).

**DSL.** Digital Subscriber Line, 'Línea Digital de Abonado'. Es el término genérico que hace referencia a la familia de tecnologías que utilizan la línea telefónica para transmitir datos a alta velocidad. ADSL, SDSL o HDLS son algunas de estas tecnologías. También se utiliza el término xDSL para hacer referencia a esta familia de tecnologías.

**DSSS.** Direct Sequence Spread Spectrum, 'Espectro Expandido por Secuencia Directa'. Es la técnica de modulación utilizada por los sistemas IEEE 802.11b (Wi-Fi) para transmitir datos a alta velocidad (11 Mbps).

## E

**ENLACE.** Ruta de comunicación entre dos nodos de una red.

**ESTACIÓN BASE.** Es el nombre general que reciben los equipos de una red inalámbrica que se encargan de gestionar las comunicaciones de los dispositivos que forman la red.

**ETHERNET.** Es un tipo particular de red de área local. Tiene la particularidad de utilizar el mismo protocolo de comunicaciones que Internet (TCP/IP).

**ETSI.** European Telecommunications Standards Institute, 'Instituto Europeo de Normas de Telecomunicaciones Creado en marzo de 1989 y con sede en Sophia-Antipolis, cerca de Niza.

**ESPECTRO EXPANDIDO.** Es un sistema de difusión de las señales radioeléctricas. Este sistema utiliza un ancho de banda mayor al estrictamente necesario a cambio de conseguir reducir la vulnerabilidad a las interferencias y garantizar la coexistencia con otras transmisiones.

**ESS.** Extended Service Set, 'Conjunto de Servicios Extendido'. Es una de las modalidades en las que se puede configurar una red local inalámbrica Wi-Fi. Reciben este nombre las redes inalámbricas que están formadas por más de un punto de acceso.

## F

**FAQ.** Frequently-Asked Question, 'Preguntas Frecuentes'. Normalmente estas siglas se refieren a una lista de las preguntas más frecuentes sobre un tema y sus respuestas correspondientes. Muchos servicios en Internet ofrecen una FAQ con el objetivo de orientar a sus nuevos usuarios o de ofrecer información adicional sobre un tema.

**FAST ETHERNET.** Es como se conoce comúnmente al estándar de la red Ethernet que permite velocidades de transmisión de 100 Mbps. A este estándar se le conoce como 100BaseT y se basa en la norma IEEE802.3u.

**FHSS.** Frequency Spread Spectrum, 'Espectro Expandido por Salto de Frecuencia'. Es una técnica de modulación utilizada tanto por los sistemas IEEE802.11 como Bluetooth. Transmite datos a baja velocidad (1 Mbps) por lo que en la versión 802.11b se sustituyó por el sistema DSSS para poder transmitir datos a alta velocidad (11 Mbps).

**FIREWALL.** Véase Cortafuegos.

**FIRMWARE.** Es un código de programa que se graba en las unidades de hardware de los equipos. A través del firmware los fabricantes consiguen actualizar el hardware sin cambiar un chip. Estos códigos se guardan en unos chips de memoria conocidos como PROM. Estos chips tienen la particularidad de que no se borran cuando no tienen alimentación eléctrica y pueden ser reprogramados.

**FTP.** File Transfer Protocol, 'Protocolo de Transferencia de Archivos'. Es un protocolo de Internet que permite transferir archivos de un ordenador a otro.

## G

**GATEWAY.** Pasarela. Es un sistema informático que transfiere datos entre dos aplicaciones o redes incompatibles entre sí. El gateway adapta el formato de los datos de una aplicación a otra o de una red a otra. Se utiliza generalmente para interconectar dos redes distintas o para hacer que una aplicación entienda los datos generados por otra aplicación distinta.

**GNU.** Es un tipo de software que puede ser copiado y distribuido libremente. De la misma forma, también puede ser copiado, distribuido o utilizado todo o parte de su código fuente, con la condición de que el software producido también sea de tipo GNU.

**GUILTWARE.** Se le aplica este nombre a aquel software de tipo freeware que contiene un mensaje en el que se cuenta lo mucho que ha trabajado y sufrido el autor para realizar el programa y lo bien que le vendría una pequeña aportación económica. El nombre viene del inglés *guilt*, 'culpabilidad', y hace referencia a los sentimientos de culpabilidad que crea en el usuario si no atiende a la petición del autor.

**GURÚ.** Experto.

## H

**HACKER.** Persona que se dedica a entrar ilegalmente en sistemas y redes de ordenadores para robar, modificar o borrar información.

**HIPERENLACE.** Es un bloque de texto o imagen que señala a otro recurso de la red, generalmente otra página Web.

**HIPERLAN.** High-performance Radio Local Area Network, 'Red de Área Local de Radio de Alto Rendimiento'. Es un estándar de red de área local inalámbrica definido por ETSI (Instituto Europeo de Normalización en Telecomunicaciones) que permite transmitir datos hasta 54 Mbps trabajando en la banda de 5 GHz.

**HIT.** Es un sistema para medir la carga de trabajo de un servidor. Se le llama hit a la transmisión de cada elemento de una página Web. Si una página Web consiste en un texto HTML, una imagen y un sonido, el servidor recibe tres hits cada vez que alguien accede a esta página.

**HOMEFNA.** Home Phonenumber Networking Alliance, 'Alianza de Red Doméstica sobre Líneas Telefónicas'. Es el nombre que recibe el grupo que creó las especificaciones que permiten crear una red local de datos utilizando la infraestructura telefónica del hogar. La red de datos utiliza los mismos cables telefónicos que los teléfonos, fax o los módem DSL.

**HOMERF.** Home Radio Frequency, 'Radio Frecuencia del Hogar'. Es una tecnología de red de área local inalámbrica que en su día fue promovida por Intel (además de otros). Existen tres versiones en el mercado que alcanzan los 1,6, 10 y 40 Mbps, respectivamente. En cualquier caso, HomeRF ha quedado hoy en día en el olvido debido al auge de Wi-Fi.

**HOST.** Es cualquier ordenador o dispositivo conectado a una red TCP/IP.

**HTML.** HyperText Markup Language 'Lenguaje de Diseño de Hipertextos'. Se trata de un formato especial de archivos sobre el que está basada la estructura del servicio WWW (World Wide Web).

**HTTP.** Hypertext Transfer Protocol, 'Protocolo de Transporte de Hipertexto'. Es el protocolo que se utiliza en Internet para transferir la información Web.

**HUB.** Es un dispositivo utilizado en las redes de área local para interconectar los ordenadores o equipos de red. Éste es un dispositivo pasivo que se limita a recoger la información de un puerto y retransmitirla por el resto de puertos sin hacer ningún tipo de análisis de ella.

## I

**IAB.** Internet Architecture Board, 'Consejo de la Arquitectura Internet'. Es una organización existente dentro de la Sociedad Internet (ISOC) que se encarga, entre otras cosas, de aprobar las normas de Internet.

**IBSS.** Independent Basic Service Set, 'Conjunto de Servicios Básicos Independientes'. Es una de las modalidades de comunicación en las que se pueden configurar los terminales de una red Wi-Fi. En este caso, la red inalámbrica no dispone de punto de acceso, llevándose a cabo las comunicaciones de forma directa entre los distintos terminales que forman la red. Este modo de conexión también es conocido como modo ad hoc, modo independiente o de igual a igual peer-to-peer en inglés).

**IEEE.** Institute of Electrical and Electronics Engineers, 'Instituto de ingenieros Eléctricos y Electrónicos'. Es una asociación mundial de ingenieros de este sector. El IEEE forma también el comité de normalización que recomienda al ANSI (órgano estadounidense de normalización) sobre los estándares de tecnologías de Redes de área local.

**INTERNET.** Es un conjunto de redes, de ámbito mundial, conectadas entre sí mediante el protocolo IP (Internet Protocol). A través de Internet se puede acceder a servicios como WWW, transferencia de archivos, acceso remoto, correo electrónico o noticias, entre otros.

**INTRANET.** Son redes corporativas que utilizan el mismo protocolo que Internet. Estas redes conectan a los ordenadores de la empresa y ofrecen a sus usuarios (empleados de la empresa) acceder a servidores Web (o de otro tipo) con información corporativa, documentación, bases de datos, acceso remoto, etc.

**IP.** Internet Protocol, 'Protocolo Internet'. Es el protocolo de nivel de red utilizado tanto por Internet como por la mayoría de las redes de área local cableadas e inalámbricas. Mediante el protocolo IP, cualquier paquete puede viajar a través de las distintas redes de Internet hasta llegar a su destino final. LP es la clave del funcionamiento de Internet.

**IPSec.** Es un protocolo de redes privadas virtuales que, aunque forma parte de la recomendación IPv6, es ampliamente utilizado en las redes IPv4 actuales.

**ISM.** Industrial, Scientific and Medicine, 'Industrial, Científica y Médica'. Estas siglas hacen referencia a la banda de frecuencias radioeléctricas reservadas a aplicaciones de este tipo. Ésta es la banda de frecuencias en las que actúa Wi-Fi.

**ISO.** International Standard Organization, 'Organización internacional para la Normalización'. Esta organización ha definido los protocolos de comunicaciones conocidos como ISO/OST, utilizado por las redes públicas de conmutación de paquetes.

**ISP.** Internet Service Provider, 'Proveedor de Acceso a Internet'. Es cualquier empresa que facilite el acceso a Internet a sus clientes o usuarios. Estos usuarios pueden ser personas particulares u otras empresas.

**ITU-TSS.** International Telecommunication. Union-Telecommunications Standard Sector, 'Unión internacional de Telecomunicaciones-Sector de Normalización de Telecomunicaciones'. Antes CCITT.

## **J**

**JAVA.** Es un lenguaje de programación utilizado en Internet. Java permite que distintos usuarios de Internet con distintos sistemas operativos en sus ordenadores puedan acceder de la misma manera a las aplicaciones de las páginas Web.

**JAVASCRIPT.** Lenguaje script desarrollado por Netscape para permitir la inclusión de Instituciones Java en las páginas HTML.

## **K**

**KBPS.** Kilo bits por segundo. Es una unidad de medida de la velocidad de transferencia de datos. Un kilobit por segundo significa que se transfieren 1.024 bits cada segundo. Un bit es la unidad más pequeña de información (un 0 o un 1).

## **L**

**L2TP.** Layer 2 tunneling Protocol, 'Protocolo de Tunelado de Capa 2': Es un protocolo del IETF utilizado para Crear redes privadas virtuales.

**LAN.** Local Area Network, 'Red de Área Local'. Véase Red de área local.

**LINK.** Enlace. Véase Enlace.

**LINUX.** Es una versión del sistema operativo Unix desarrollada por el sueco Linus Torvalds. La característica de este sistema operativo es que es distribuido de forma completamente gratuita.

## **M**

**MAC.** Medium Access Control, 'Control de Acceso al Medio'. Es un conjunto de protocolos de las redes inalámbricas que controla cómo los distintos dispositivos se comparten el uso del espectro radioeléctrico.

**MAC ADDRESS.** Dirección MAC. Véase Dirección MAC,

**MÁSCARA DE SUBRED.** Es un número de 32 bits utilizado para identificar la parte de la dirección IP que identifica a la red y la parte que identifica al ordenador o equipo de red.

**MBPS.** Megabits por segundo. Es una unidad de medida de la velocidad de transferencia de datos. Un megabit por segundo significa que se transfieren 1.048.576 (1.024 x 1.024) bits cada segundo. Un bit es la unidad más pequeña de información (un 0 o un 1).

**MÓDEM.** Es un equipo que se conecta al ordenador para poder transmitir datos por un medio de transmisión analógico. En el caso de las líneas telefónicas, el módem convierte las señales digitales propias del ordenador en seriales analógicas, aptas para ser transmitidas por una línea telefónica. Los módem utilizados habitualmente en las líneas telefónicas suelen ofrecer una velocidad de transmisión de hasta 56 Kbits por segundo.

**MODO AD HOC.** Se refiere a las redes inalámbricas Wi-Fi que no disponen de punto de acceso. En este caso, las comunicaciones se llevan a cabo directamente entre los distintos terminales que forman la red. Este modo de conexión también es conocido como modo IBSS, modo independiente o de igual a igual (peer-to-peer en inglés).

**MODO BSS.** Véase Modo infraestructura.

**MODO DE IGUAL A IGUAL.** Véase Modo ad hoc

**MODO IBSS.** Véase Modo ad hoc.

**MODO INFRAESTRUCTURA.** Se refiere a las redes inalámbricas Wi-Fi que disponen de un equipo central, conocido como punto de acceso, que se encarga de gestionar las comunicaciones (internas y externas) de todos los dispositivos que forman la red. Este modo de conexión también es conocido como modo BSS.

**MODULACIÓN.** Se llama modulación al hecho de distorsionar una señal eléctrica o radioeléctrica para que contenga la información a transmitir. Al proceso contrario, extraer la información de una señal modulada, de le llama demodulación.

**MULTIMEDIA.** Sistema que integra sonido, textos e imágenes (fijas o en movimiento) En un único soporte

## N

**NAGWARE.** Se refiere a los programas shareware que están continuamente solicitándole al usuario que debe registrarse. Nag significa regañar en inglés.

**NAVEGADOR.** Programa que permite acceder a los recursos Web de Internet. Adicionalmente, un navegador puede utilizarse también para acceder a otros recursos, como correo electrónico, grupos de noticias, etc. Internet Explorer y Netscape son los dos navegadores más conocidos.

**NAT.** Network Address Translation, 'Traducción de Direcciones de Red' Es un estándar que le permite a las redes locales conectadas a Internet utilizar su propio sistema de numeración IP privado compartiendo los números IP públicos. Los usuarios de la red pueden acceder a Internet a través del router, pero el resto de usuarios de Internet no pueden acceder directamente a los ordenadores de la red local.

**NIC.** Network Interface Card, 'Tarjeta Interfaz de Red'. Es la tarjeta de red que necesita cualquier equipo para conectarse a una red de área local (cableada o inalámbrica).

**NODO.** En general se le llama nodo a cualquier ordenador conectado a una red.

**O**

**OFDM.** Orthogonal Frequency Division Multiplexing 'Multiplexado Ortogonal par División de Frecuencia'. Es una técnica de modulación utilizada por las redes de área local inalámbrica de alta velocidad (IEEE 802.11a y HiperLAN2). Permite transmitir datos de hasta 54 Mbps.

**OFF-LINE.** Significa estar desconectado. Trabajar off-line en Internet quiere decir que se está trabajando estando desconectado de la red. Lo opuesto sería trabajar on-line, o trabajar conectado a la red.

**ON-LINE.** Significa estar conectado. Trabajar on-line en Internet quiere decir que se está trabajando estando conectado a la red. Lo opuesto sería trabajar off-line, o trabajar mientras se está desconectado de la red.

**OSI.** Open Systems Interconnet, 'Interconexión de Sistemas Abiertos'. Se trata de una serie de protocolos normalizados por la Organización internacional para la Normalización, TSO.

**P**

**PACKET.** Véase Paquete.

**PAQUETE.** Es cada uno de los trozos en los que un protocolo de comunicaciones divide el flujo de información para transmitirlo por la red.

**PASSWORD.** Véase Contraseña.

**PCI.** Peripheral Component Interconnect, 'Interconexión de Componentes Periféricos'.

Son unas especificaciones creadas por Intel y que definen un sistema de bus local que permite conectar al PC hasta 10 tarjetas de periféricos. El estándar PCI ha venido a reemplazar al antiguo estándar ISA (Industry Standard Architecture).

**PCMCIA.** Personal Computer Memory Card International Association, 'Asociación Internacional de Tarjetas de Memoria para Ordenadores Personales'. Se trata de una asociación de fabricantes de equipos que en 1989 sacó al mercado un tipo de puerto y de dispositivo de pequeño tamaño que permite que se le puedan instalar todo tipo de periféricos a los ordenadores personales. En un principio se dedicaron sólo a ampliar la memoria, de ahí su nombre. Tanto el puerto como los dispositivos reciben también el nombre de PCMCIA. En inglés se la conoce más coloquialmente como PC Card (tarjeta de PC).

**PEER-TO-PEER.** Véase Modo ad hoc.

**POP.** Post Office Protocol, 'Protocolo de Oficina de Correos'. Se trata de un protocolo que permite a los usuarios de ordenadores personales acceder a un host y transferir a su ordenador todo el correo dirigido a ellos (recoger el correo). Existen diferentes versiones del programa POP y no todas ellas son compatibles entre si.

**PORT.** Véase Puerto.

**PPTP.** Point to Point Tunneling Protocol, 'Protocolo de Tunelado Punto a Punto'. Es un protocolo de red privada virtual incluido en los sistemas operativos Windows.

**PROTOCOLO.** Es un conjunto de normas que indican cómo deben actuar los ordenadores para comunicarse entre si. Los protocolos definen desde para qué se va a usar cada hilo de un Conector hasta el formato de los mensajes que se intercambian los ordenadores.

**PUERTO.** Puede tener dos significados. Por un lado, puede tratarse de un número que identifica una aplicación particular de Internet. Cuando un ordenador envía un paquete a otro, el paquete contiene la información de la aplicación que está intentando comunicarse con el ordenador remoto. Esta identificación se hace mediante un número de puerto (port number). Por otro lado, también se conoce como puerto al conector físico que utilizan los ordenadores para comunicarse con el exterior (puerto de impresora, puerto serie, etc.).

**PUNTO DE ACCESO.** Es el equipo de la red inalámbrica que se encarga de gestionar las comunicaciones de todos los dispositivos que forman la red. El punto de acceso no sólo se utiliza para controlar las comunicaciones internas de la red. Sino que también hace de puente en las comunicaciones con las redes externas (redes cableadas e Internet).

## R

**RED.** Conjunto de ordenadores interconectados entre si. También puede hacer referencia a la infraestructura que permite la interconexión de estos ordenadores.

**RED DE ÁREA LOCAL.** Es una red de datos que interconecta ordenadores situados en el entorno de un edificio o de las oficinas de una empresa dentro de ese edificio. Una red local permite a sus usuarios compartir información y recursos de la red, como impresoras o líneas de comunicaciones (acceso a Internet).

**RELACION SEÑAL RUIDO.** En una comunicación de radio es el resultado de dividir el valor de la fuerza de la señal de los datos por el valor de la fuerza del ruido. Generalmente se expresa en decibelios (dB) y se utiliza como indicativo de la calidad de la comunicación. Cuanto mayor sea este valor, mejor será la comunicación.

**RF.** Radiofrecuencia.

**RJ-11.** Es el nombre que recibe el conector de los equipos telefónicos (teléfonos, fax; modem, etc.). Este conector permite utilizar hasta cuatro hilos.

**RJ-45.** Es el nombre que recibe un conector estándar que se utiliza habitualmente en el cableado de las redes locales Ethernet 10BaseT y 100BaseT. Tiene la misma forma que el conector RJ11, con la salvedad de que es de un tamaño algo mayor. lo que le permite Utilizar hasta ocho hilos.

**ROAMING.** Se conoce por este nombre a la posibilidad que tienen los equipos inalámbricos de desplazarse dentro del área de cobertura de una red inalámbrica sin perder la conexión.

**ROUTER.** Es un sistema utilizado para transferir datos entre dos redes que utilizan un mismo protocolo. Un router puede ser un dispositivo software, hardware o una combinación de ambos. Los puntos de acceso, generalmente, hacen las funciones de router. A este equipo también se le conoce en español por el nombre de enrutador.

## S

**SERVER.** Véase Servidor.

**SERVIDOR.** Se trata de un software que permite ofrecer servicios remotos sus usuarios. También puede recibir el nombre de servidor el propio ordenador donde está instalado el software servidor. El ordenador de los usuarios Contacta con el servidor gracias a otro software llamado cliente.

**SHAREWARE.** Se refiere al software que es distribuido de forma gratuita y sin ningún tipo de restricción. Después de un periodo de prueba, en el caso de que el usuario decida

continuar utilizándolo, se compromete a pagar al autor del software una cierta cantidad (generalmente pequeña).

**SISTEMA OPERATIVO.** Es el software que hace que los ordenadores puedan funcionar. Es el encargado de gestionar y operar todos los recursos hardware y software de que disponga el ordenador. Los programas informáticos están diseñados para funcionar con un sistema operativo particular. Mac OS, Windows XP o Linux son ejemplos de sistemas operativos.

**SMTP.** Simple Mail Transfer Protocol, 'Protocolo Simple de Transferencia de Correo'. Se trata del protocolo en el que se basa el servicio de correo electrónico en Internet. Este protocolo define el formato que deben tener los mensajes y cómo éstos deben ser transferidos.

**S/N.** Signal to Noise Ratio, 'Relación Señal/Ruido'. Véase Relación señal ruido.

**SNIFFER.** 'Husmeador'. Es una herramienta que utilizan los administradores de red o los piratas informáticos para interceptar los paquetes de datos de las redes cableadas o inalámbricas. Sniffer puede ser tanto software como hardware.

**SNR.** Signal To Noise Ratio, 'Relación Señal Ruido.. Véase Relación señal ruido.

**SPAM.** Se refiere a los mensajes de correo electrónico que se reciben sin ser solicitados y que tienen un objetivo comercial o, simplemente una clara intención de molestar. También es aplicable a los mensajes enviados a los grupos de noticias y que no están relacionados con el tema del grupo. Los spam suelen ser anuncios publicitarios.

**SPREAD SPECTRUM.** Espectro expandido. Véase Espectro expandido.

**SSID.** Service Set Identifier, 'identificador del Conjunto de Servicios'. Es el parámetro que identifica la red inalámbrica. También se le conoce como nombre de red.

**SSL.** Secure Sockets Layer,'Capa de Conexión Segura'. Protocolo desarrollado por Netscape para codificar la comunicación entre un navegador Web y un servidor. SSL garantiza la privacidad, autenticidad e integridad de la información intercambiada.

## T

**TCP/IP.** Transmission Control Protocol/Internet Protocol,'Protocolo de Control de Transmisión/Protocolo Internet'. Normas técnicas de actuación que fijan el interfuncionamiento de las redes que forman parte de Internet.

**TELNET.** Es una aplicación de Internet que permite el acceso remoto a otros ordenadores de la red y trabajar como si se fuese un usuario local. Mediante Telnet se puede tener acceso a todas las facilidades del ordenador remoto.

**THROUGHPUT.** Se refiere a la cantidad real de información que puede transmitirse en un enlace. Es una forma de conocer la eficiencia del enlace. Este valor suele medirse en bits por segundo, bps.

**TIME OUT.** Se dice que ha ocurrido un time out (tiempo límite) cuando dos ordenadores están manteniendo una comunicación y uno, por cualquier razón, no responde. Después de un cierto tiempo (time out), la comunicación se corta. Esta idea de plazo de tiempo se aplica también a cualquier otro proceso que disponga de un tiempo máximo de respuesta.

**TRINSCIVER.** Transmitter-Receiver, 'Transmisor-Receptor'. Es un equipo de radio que puede tanto transmitir como recibir.

## U

**UIT.** Unión Internacional de Telecomunicaciones.

**UNIX.** Es un sistema operativo multitarea y multiprogramación.

**UPLINK.** Enlace de subida. Suele hacer referencia al puerto donde se pueden conectar otros hubs o switches para extender la red.

**UPLOAD.** Se puede traducir como subir. Cuando un usuario copia un archivo de su ordenador a un ordenador remoto, se dice que el archivo ha sido subido (Uploaded).

**URL.** Uniform Resource Locators, 'Localizador Universal de Recursos'. Es la forma particular que se tiene en Internet de especificar las direcciones de sus distintos recursos. Un URL es una dirección.

**USB.** Universal Serial Bus, 'Bus Serie Universal'. Interfaz serie del ordenador que permite conectar hasta 127 dispositivos (impresoras, adaptadores de red, escáneres, monitores, etc.) a una velocidad de 1,5 o 12 Mbps. Además, tiene la particularidad de que no es necesario apagar el ordenador para conectar o desconectar los dispositivos.

## V

**VAPORWARE.** Software anunciado pero no disponible.

**VIRUS.** Es un programa que tiene la característica de auto reproducirse (pasar de unos ordenadores a otros). Los virus pueden ser malignos si causan efectos destructivos en los ordenadores que va contaminando, o benignos, si no van causando daños.

**VoIP.** Voice over IP, 'Voz sobre IP'. Es una tecnología que permite la transmisión de voz sobre la redes de datos IP. Es la base de las comunicaciones de voz entre ordenadores. Aplicaciones como NetMeeting o Net2Phone se basan sobre esta tecnología.

**VPN.** Virtual Private Network, 'Red Privada Virtual'. Hace referencia a las soluciones que permite crear redes completamente privadas en cuanto a seguridad y confidencialidad utilizando para ello infraestructuras no seguras (como Internet o redes inalámbricas).

## W

**WAN.** Wide Area Network, 'Red de Área Extensa'. Recibe este nombre la red formada por la interconexión de distintas redes de área local situadas en distintos edificios. También recibe este nombre el puerto del punto de acceso donde se debe conectar la conexión con la red de área local cableada (Ethernet).

**WEB HOSTING.** Alojamiento Web. Es el nombre del servicio que consiste en dar alojamiento en un ordenador a los servicios Web de otras empresas o entidades.

**WEBCAM.** Hace referencia a las cámaras de vídeo que pueden ser conectadas a un ordenador para establecer una videoconferencia o retransmitir un evento.

**WECA.** Wireless Ethernet Compatibility Alliance, 'Alianza de Compatibilidad Ethernet Inalámbrica'. Es una asociación de fabricantes de equipos de red creada en 1999 con el objetivo de fomentar la tecnología inalámbrica y asegurarse la compatibilidad de equipos.

**WECA** es la creadora de la marca Wi-Fi y es quien certifica los equipos con esta marca.

**WEP.** Wired Equivalency Protocol, 'Protocolo de Equivalencia con Red Cableada'. Es el sistema de cifrado de datos que incorporan las redes Wi-Fi. El sistema WEP surgió con

la idea de ofrecerle a las redes inalámbricas un estado de seguridad similar al que tienen las redes cableadas.

**WI-FI.** Wireless Fidelity, 'Fidelidad Inalámbrica'. Es una marca creada por la asociación VYTCA con el objetivo de fomentar la tecnología inalámbrica y asegurarse la compatibilidad de equipos. Todos los equipos con la marca Wi-Fi son compatibles entre sí y utilizan la tecnología inalámbrica definida por el IEEE en su estándar 802.11b.

**WiMAX.** Worldwide Interoperability for Microwave Access, 'Interoperatividad mundial para accesos de microondas'. Organización sin ánimo de lucro creada por fabricantes y suministradores de equipos inalámbricos para promover el uso de las tecnologías de redes inalámbricas metropolitanas de banda ancha IEEE 802.16a y ETSI HiperMAN, así como, asegurar su interoperatividad.

**WINDOWS.** Windows hace referencia a la familia de sistemas operativos de Microsoft. Algunos de estos sistemas son Windows 95, Windows XP o Windows CE.

**WLAN.** Wireless Local Area Network, 'Red de Área Local Inalámbrica'. Es el acrónimo con el que se hace referencia a las redes de área local inalámbricas. Las redes Wi-Fi son un ejemplo de este tipo de redes.

**WORLD WIDE WEB.** Es un servicio de Internet basado fundamentalmente en la presentación de información en forma de documentos multimedia, los cuales pueden contener enlaces directos con otros documentos World Wide Web.

**WPA.** Wi-Fi Protected Access, 'Acceso Wi-Fi Protegido'. Son unas especificaciones de seguridad basadas en el estándar IEEE 802.11i que incrementa fuertemente el nivel de protección de datos y de control de acceso de las redes Wi-Fi. Las facilidades de seguridad ofrecidas por WPA pueden implantarse en las redes Wi-Fi existentes mediante una instalación de software.

**WWW.** Véase World Wide Web.

## **Z**

**ZIP.** Es un sistema de compresión del tamaño de los archivos. Hacer zip a un archivo es comprimirlo mediante programas como Winzip, Pkzip, Easyzip o similar.

---

**BIBLIOGRAFÍA**

<http://www.maestrosdelWeb.com/editorial/redeswlan/>  
<http://cek.bitacoras.com/archivos/2004/06/03/homerf/>  
<http://www.redaragon.com/informatica/wireless/redwireless.asp>  
<http://www.Webopedia.com/TERM/P/piconet.html>  
<http://www.mailxmail.com/informatica/wifi/capitulo1.htm>  
<http://www.microsoft.com/formacion/redinalambrica.msp>  
<http://www.bandaancha.st/foros.php?temid=781904>  
[http://bcnWeb2.bcn.es:8885/www\\_bcn/owa/monta\\_e.tramit?p\\_trami](http://bcnWeb2.bcn.es:8885/www_bcn/owa/monta_e.tramit?p_trami)  
<http://www.emb.cl/gerencia/noticia.mv?id=20060124x1>  
<http://www.adslayuda.com/foro-viewtopic-t-60863.html>  
<http://www.unincca.edu.co/boletin/indice.htm>  
[espanol.geocities.com/revista\\_infrarrojo/index.htm](http://espanol.geocities.com/revista_infrarrojo/index.htm)  
[peoplecall.typepad.com](http://peoplecall.typepad.com)  
[www.hiperlan2.com/presdocs/site/whitepaper.pdf](http://www.hiperlan2.com/presdocs/site/whitepaper.pdf)  
[www.htmlWeb.net/redes/topologia/topologia\\_1.html](http://www.htmlWeb.net/redes/topologia/topologia_1.html)  
[www.wikipedia.org](http://www.wikipedia.org)  
[www.geocities.com/txmetsb/el\\_modelo\\_de\\_referencia\\_osi.htm](http://www.geocities.com/txmetsb/el_modelo_de_referencia_osi.htm)  
[www.sc.ehu.es/scWebci/WIFI/wifi-cc-tt.htm](http://www.sc.ehu.es/scWebci/WIFI/wifi-cc-tt.htm)  
[www.arcelect.com/DSSS\\_FHSS-Spead\\_spectrum.htm](http://www.arcelect.com/DSSS_FHSS-Spead_spectrum.htm)  
[www.iss.rwth-aachen.de/Projekte/Theo/OFDM/www\\_ofdm.html](http://www.iss.rwth-aachen.de/Projekte/Theo/OFDM/www_ofdm.html)  
[www.teleco.com.br/es/es\\_ieee802.asp](http://www.teleco.com.br/es/es_ieee802.asp)  
[www.superwarehouse.com/Wireless\\_\\_\\_Access\\_Point/c3/2154](http://www.superwarehouse.com/Wireless___Access_Point/c3/2154)  
[www.superinventos.com/wifi.htm](http://www.superinventos.com/wifi.htm)  
[www.wirelesslan.com](http://www.wirelesslan.com)  
[www.dti2.net/televigilancia.asp](http://www.dti2.net/televigilancia.asp)  
[www.circo.com](http://www.circo.com)

Hacking Wireless: Seguridad De Redes Inalámbricas

[Andrew A. Vladimirov](#)

Edit. Anaya Multimedia

Manual De Redes Inalámbricas

[Neil Reid](#)

Edit. Mcgraw-Hill Interamericana

Redes Wireless 802.11

[Matthew S. Gast](#)

Edit. Anaya Multimedia

Fundamentos De Seguridad En Redes: Aplicaciones Estándares

[William Stallings](#)

Edit. Prentice May

Redes De Computadoras, Internet E Interredes

[Douglas E. Comer](#)

Edit. Prentice Hall