ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE TECNOLOGÍA

DISEÑO E IMPLEMENTACIÓN DE UNA RED INALÁMBRICA PARA LA OFICINA DE PROFESORES DE LA ESFOT

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGO EN ELECTRÓNICA Y TELECOMUNICACIONES

GARY GABRIEL TERAN BRAVO
RONALD HUMBERTO DAVILA PEÑALOZA

DIRECTOR: ING. ALCÍVAR COSTALES

Quito, Octubre 2005

DECLARACIÓN

Nosotros, GARY GABRIEL TERAN BRAVO Y RONALD HUMBERTO DAVILA PEÑALOZA, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

GARY GABRIEL TERAN BRAVO

RONALD HUMBERTO DAVILA PEÑALOZA

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por el Sr. GARY GABRIEL TERAN BRAVO Y EL Sr. RONALD HUMBERTO DAVILA PEÑALOZA que tiene como titulo **Diseño e Implementación de una Red Inalámbrica para la oficina de Profesores de la ESFOT**; bajo mi supervisión.

_____

Ing. ALCIVAR COSTALES
DIRECTOR DE PROYECTO

INDICE

RESUMEN

Mediante el presente proyecto se ha permitido que las oficinas de los profesores de la ESFOT cuenten con un sistema de comunicación de red inalámbrica la misma que ha sido instalada mediante un Access point y adaptadores PCI o tarjetas de red inalámbricas, con dicha red se obtiene grandes ventajas como son las de poder compartir recursos e información teniendo la posibilidad de movilizarse dentro de una área establecida.

En el cápitulo uno se explica todo lo que tiene que ver con redes de computadoras tanto cableada como inalámbrica, pero haciendo hincapié a estas últimas ya que en si nuestro proyecto se basa en este tipo de red.

En el cápitulo II se explica todo lo que tiene que ver con los dispositivos que van a ser usados en la construcción de la red inalámbrica, como son el Access Point, tarjetas de red inalámbrica PCI entre otros, aquí se estudia las ventajas y desventajas que cada uno de estos tiene.

En el cápitulo III se realizan las configuraciones de cada uno de los dispositivos a utilizar y se realizan las respectivas pruebas para que la red quede funcionando de la mejor manera.

PRESENTACION

Al finalizar este proyecto se podrá demostrar lo versátil, de tener una red inalámbrica, el pro y el contra frente a una red que es cableada.

Con la utilización de equipos de última tecnología podemos llegar a alcanzar un nivel superior en cuanto a administración, seguridad, rendimiento, y principalmente que la ubicación de un computador no esta limitado a estar fijo, cerca de un punto de red ya que ésta presenta la ventaja de poder poner un computador en cualquier sitio del área de cobertura.

También con esta aplicación podemos compartir a más de información otros tipos de dispositivos como son impresoras, scanner, mediante el uso de servidores poder mantener una base de datos que se encuentren en el servidor y no necesariamente en todos los computadores.

CAPITULO I

REDES DE COMUNICACION

1.1 REDES INALÁMBRICAS

Debido al crecimiento de la computación móvil y los PDA's (Personal Digital Assistants), se ha dado un gran impulso a las redes inalámbricas, las cuales tienen muchos usos. Uno de ellos es en los computadores portátiles.

Las desventajas actuales de la computación móvil se basan en que son más lentas que otros medios de transmisión (1 - 54 Mbps) y además la tasa de errores es más alta. Las tecnologías que tenemos entre éstas son: Microondas, infrarrojos, celulares y Wireless.

1.1.1 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 el uso de cables de interconexión. También existen redes inalámbricas de voz, pero éstas no son el objeto de este proyecto.

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 le 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 intercomunicarse.

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 y hasta 1Gbps. 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.

1.1.1.1 TIPOS DE REDES INALÁMBRICAS DE DATOS

Las comunicaciones inalámbricas 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.

WPAN	WLAN	WMAN	CELULAR
<10 metros	**Edificio Campus**	**Ciudad**	**Región Global**
Bluetooth	*WI-FI,*	*LMDS*	*2,5G*
802.15	*Homero*	*MMDS*	3G
IrDA	*HiperLAN*	*802.16*	

Tipo de redes inalámbricas

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

1.1.2 REDES INALÁMBRICAS DE ÁREA PERSONAL

Se ha venido a llamar redes inalámbricas de área personal, WPAN *{Wireless Personal Área 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. Éste es el caso de la tecnología Bluetooth o de IEEE 802.15; que es una de las tecnologías de redes inalámbricas de área personal más conocidas.

1.1.3 REDES INALÁMBRICAS DE ÁREA LOCAL

Se llama redes inalámbricas de área local, WLAN *(Wireless Local Área 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: Wi-Fi; Home RF; HiperLAN; HiSWAN OpenAir.

1.1.4 REDES INALÁMBRICAS DE ÁREA METROPOLITANA

Se llama redes inalámbricas de área metropolitana, WMAN *(Wireless Metropolitan Área 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.

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 compartido entre todos los usuarios del sistema.

1.1.5 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 División Múltiple Access,* 'Acceso Múltiple por División de Código').

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.

Característica	Wi-Fi	HiperLAN	HomeRF
Normalización	*alto*	*alto*	*bajo*
Regulación	*alto*	*medio*	*alto*
Tecnología	*medio*	*alto*	*alto*
Servicios	*bajo*	*alto*	*medio*
Precios	*alto*	*bajo*	*bajo*

1.2 LA REGULACION

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.

ESTÁNDAR	ÁREA	FRECUENCIA	POTENCIAMÁXIMA
802.11, 11by11g	*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*	*10mW/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*
HiperiAN/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*

Distintas regulaciones de las bandas de 2,4 y 5 GHz

Aunque no se necesite licencia de uso, los equipos que funcionan en la banda de 2,4 GHz sí 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.

1.3 WI-FI

1.3.1 INTRODUCCIÓN

Ciertamente, se puede construir una red Wi-Fi sin saber cómo funciona; no obstante, si se comprende su funcionamiento, se estará en una mejor disposición para entender qué está pasando cuando algo no va como se espera. Por otro lado, también ayuda a entender mejor las características de los distintos equipos Wi-Fi y cuáles son las posibilidades reales.

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.

Wi-Fi hace referencia al estándar IEEE 802.11b y 802.11g. Las redes inalámbricas Wi-Fi que se instalan hoy en día son de este tipo por lo que, aunque muchos de los principios de funcionamiento que vamos a describir aquí son válidos para distintos miembros de la familia IEEE 802.11, evidentemente nos centraremos en 802.11g.

1.3.2 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 Eléctrica! 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 ínterconnection).*

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.

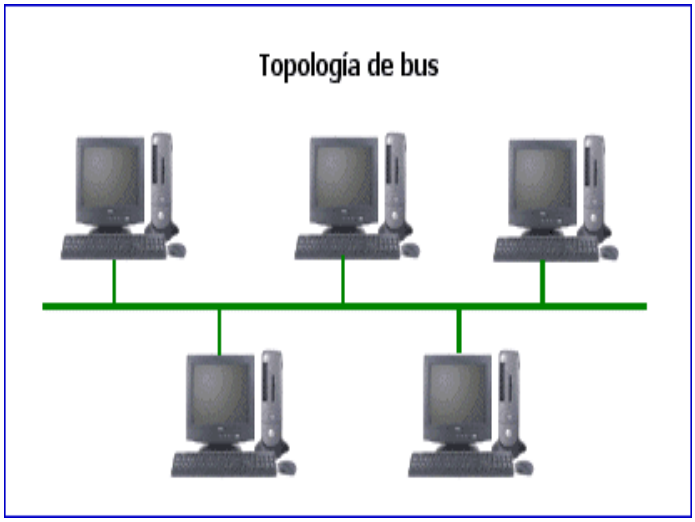
1.3.3 LAS REDES DE CABLE

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 Múltiple Access with Colusión 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.



1.3.4 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 *(High-Level LAN Interfeces)*	
802.2	Control lógico del enlace, LLC *(Logical LJnk Controf)*	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 asosíncronas	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 *(Wireless Personal Área Network)*	
802.16	Acceso inalámbrico de banda ancha, BWA *(Broadband Wireless Access)*	

Tabla 1.1. Grupos de trabajo del comité de normalización IEEE 802

El mayor inconveniente de los sistemas inalámbricos definidos originalmente por 802.11 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 (principalmente liderados por empresas como Lucent y Harris). Por otro lado, aparecieron tres nuevas versiones de la norma 802.11:

- **IEEE 802.11b,** 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 802.11a.** Esta norma se diferencia de 802.11b 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 División 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. El mayor inconveniente es que la tecnología de semiconductores para 5 GHz no está suficientemente desarrollada todavía.

- **IEEE 802.1 lg.** 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.

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 *(Interaccess Point Protocol,* IAPP)	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
802.11Í	Mejoras para seguridad y autentificación	Activo
5GSG	Globalizactón de los 5 GHz Grupo de estudio junto con ETSI/BRAN *(European Telecommunications Standands Institute/Broadband Radio Área Network,* 'Instituto Europeo de Normalización en Telecomunicaciones/Redes Vía Radio de Banda Ancha') y MMAC *(Mobile Multimedia Access Communication,* 'Comunicaciones Multimedia de Acceso Móvil') de Japón para promover la interoperatividad entre 802.11a, ETSI HiperLAN/2 y MMAC	Activo

Tabla 1.2. Grupos de trabajo y de estudio relacionados con IEEE 802.11

1.3.5 LAS MEJORAS

En el interés de disponer de unos estándares inalámbricos lo antes posible, al desarrollar sus normas, el IEEE no se paró a 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 802.11e (Calidad de servicio).** Este grupo trabaja en los aspectos relacionados con la calidad de servicio (QoS o *Quality of Services*). 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, vídeo, 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 802.11h (Gestión del espectro).** Este grupo de trabajo pretende conseguir una mejora de la norma 802.11a en cuanto a la gestión del espectro radioeléctrico. Este punto es una de las desventajas que tiene IEEE 802.11a 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').

1.4 EL NACIMIENTO DE WI-FI

El problema principal que pretende resolver la normalización es la compatibilidad. No obstante, como hemos visto, existen distintos estándares que definen distintos tipos de

redes inalámbricas. Esta variedad produce confusión en el mercado y descoordinación en los fabricantes. Para resolver este problema, los principales vendedores de soluciones inalámbricas (3Com, Aironet, Intersil, Lucent Technologies, Nokia y Symbol Technologies) crearon en 1999 una asociación conocida como WECA *(Wireless Ethernet Compability Alliance,* 'Alianza de Compatibilidad Ethernet Inalámbrica'). El objetivo de esta asociación fue crear una marca que permitiese fomentar más fácilmente la tecnología inalámbrica y asegurase la compatibilidad de equipos.

De esta forma, desde abril de 2000, WECA certifica la interoperatividad de equipos según la norma IEEE 802.11b bajo la marca Wi-Fi *(Wireless Fidelity,* 'Fidelidad Inalámbrica'). Esto quiere decir que el usuario tiene la garantía de que todos los equipos que tengan el sello Wi-Fi pueden trabajar juntos sin problemas independientemente del fabricante de cada uno de ellos.

1.4.1 COMPATIBILIDAD ENTRE WI-FI Y ETHERNET

La norma IEEE 802.11 fue diseñada para sustituir a las capas física y MAC de la norma 802.3 (Ethernet). Esto quiere decir que, en lo único en que se diferencia una red Wi-Fi de una red Ethernet, es en la forma en cómo los ordenadores y terminales en general acceden a la red; el resto es idéntico. Por tanto, una red local inalámbrica 802.11 es completamente compatible con todos los servicios de las redes locales de cable 802.3 *(Ethernet).*

1.4.2 QUÉ ES UN PROTOCOLO

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 normalizados 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.

1.4.3 EL MODELO OSI

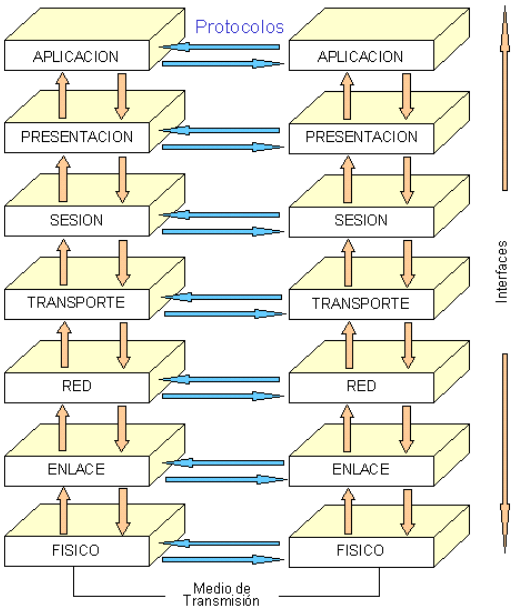
Una característica común a todas las comunicaciones actuales de ordenadores es el hecho de que todas ellas estructuran el proceso de comunicación en distintos niveles o capas. Cada capa se encarga de realizar una tarea distinta y perfectamente coordinada con el resto de capas. Por ejemplo, hay capas 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 llamante, 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 permitiese estructurar las

comunicaciones en siete capas. A este modelo lo llamó OSI *(Open Systems ínterconnection,* 'Interconexión de Sistemas Abiertos').

Las capas del modelo OSI son las siguientes:



1. **Capa física.** Esta capa define las propiedades físicas de los componentes (frecuencias de radio utilizadas, cómo se transmiten las señales, etc.).

2. **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.

3. **Capa de red.** Esta capa define cómo organizar las cosas para que distintas comunicaciones puedan hacer uso de una infraestructura común, una red.

4. **Capa de transporte.** Esta capa define las características de la entrega de los datos.

5. **Capa de sesión.** Aquí se describe cómo se agrupan los datos relacionados con una misma función.

6. **Capa de presentación.** Nos define cómo es representada la información transmitida.

7. **Capa de aplicación.** Define cómo interactúan los datos con las aplicaciones específicas.

1.4.4 CÓMO FUNCIONA WI-FI

Una red Wi-Fi puede estar formada por dos ordenadores o por miles de ellos. Para que un ordenador pueda comunicarse de forma inalámbrica, necesita que se le instale un adaptador de red.

Un **adaptador de red** es un equipo de radio (con transmisor, receptor y antena) que puede ser insertado o conectado a un ordenador, PDA o cualquier otro equipo que forme parte de la red (impresoras, etc.).

De forma general, a los equipos que forman parte de una red inalámbrica se les conoce como **terminales.**

Aparte de los adaptadores de red, las redes Wi-Fi pueden disponer también de unos equipos que reciben el nombre de **puntos de acceso** (AP o *Access Points*). Un punto de acceso es como una estación base utilizada para gestionar las comunicaciones entre los distintos terminales. Los puntos de acceso funcionan de forma autónoma, sin necesidad de ser conectados directamente a ningún ordenador.

Tanto a los terminales como a los puntos de acceso se les conoce por el nombre general de **estación.**

Las estaciones se comunican entre sí gracias a que utilizan la misma banda de frecuencias y a que internamente tienen instalados el mismo conjunto de protocolos. Aunque los protocolos que utiliza Wi-Fi están basados en las siete capas del modelo de referencia OSI, el estándar IEEE 802.11b sólo define las dos primeras capas (física y enlace); el resto de las capas son idénticas a las empleadas en las redes locales

cableadas e Internet y se conoce con el nombre de conjuntos de protocolos IP *{Internet Protocol* o 'Protocolo Internet').

Los diferentes estándar, incluido IEEE 802.11, permiten que aparezcan nuevas versiones de ese mismo estándar simplemente modificando una de las capas. Esto facilita no sólo la evolución de los estándares, sino que un mismo equipo pueda ser compatible con distintas versiones de un estándar.

1.4.4.1 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** *{Médium 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.

1.5 ESPECTRO EXPANDIDO

La tecnología básica en la que se basa el funcionamiento de los sistemas inalámbricos es el sistema conocido como espectro expandido *(spread spectrum*). 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.

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 11 Mbps. Esta nueva DSSS está recogida en la norma IEEE 802.11b. Por esta razón, al 802.11b 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 que 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 de radio), por lo que pueden transmitir o recibir, pero no ambas cosas simultáneamente.

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

1.5.1 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*). 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 Frecuency-Shift Keying,* 'Modulación Gausiana por Salto de Frecuencia')
- CCK *(Complemen tary 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 demodular la información. Los sistemas FHSS son más complicados de sincronizar que los sistemas DSSS. En el primer caso hay que sincronizar tiempo y frecuencia y en el segundo, sólo el tiempo.

1.6 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:

- **Autentificación.** 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.

- **Desautentíficación.** Cancela una autentificación 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.
- **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 transfieren 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.

SERVICIOS MAC	**DEFINICIÓN**	**TIPO DE ESTACION**
Autentificación	Comprueba la identidad de una estación y la autoriza para asociarse	Terminales y puntos de acceso
Desautentificación	*Cancela una autentificación 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-Fiyno Wi-Fi*	*Puntos de acceso*

Servicios de la capa MAC

1.7 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 802.11a).

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.

CARACTERISTICA	**802.11a**	**802.11b**	**802.11g**	**HIPERLAN2**
Regulador	*IEEE (USA)*	*IEEE (USA)*	*IEEE (USA)*	*ETSI (Europa)*
Banda de frecuencia	*5GHz*	*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, 12,9y6*	*11,5,5, 2y1*	*54, 36, 33, 24, 22, 12, 11, 9, 6, 5.5, 2y1*	*54, 36, 27, 18, 12,9y6*
Número de canales sin sobre posición	*8*	*3*	*3*	*8*
Ancho de banda en un área	*432 Mbps (8x54)*	*33 Mbps (3x11)*	*162Mbps (3x54)*	*432Mbps (8x54)*
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*

Comparación de las tecnologías inalámbricas principales

Actualmente existen dos grupos de trabajo, IEEE 802.11h 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.

1.8 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 sí 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 o 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 loable 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.

1.8.1 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.

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.

Ahorro de costos. Diseñar e instalar una red cableada puede llegar a alcanzar un alto costo, no solamente económico, sino en tiempo y molestias. En entornos domésticos y en determinados entornos empresariales donde no se dispone de una red cableada porque su instalación presenta problemas, la instalación de una red inalámbrica permite ahorrar costos 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.

1.8.2 INCONVENIENTES

Evidentemente, como todo en la vida, no todo son ventajas, las redes inalámbricas también tienen algunos puntos negativos al compararlas 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 costo 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, incluída 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.

Incertidumbre tecnológica. La tecnología que actualmente se está instalando y que ha adquirido una mayor popularidad es la conocida como Wi-Fi (IEEE 802.1 Ib). 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.

1.9 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, 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.

1.9.1 LAS REDES INALÁMBRICAS WI-FI ADMITEN TRES TIPOS DE CONFIGURACIONES:

1. **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.

2. **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.

3. **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.

1.10 NECESIDAD DE LOS PUNTOS DE ACCESO

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.

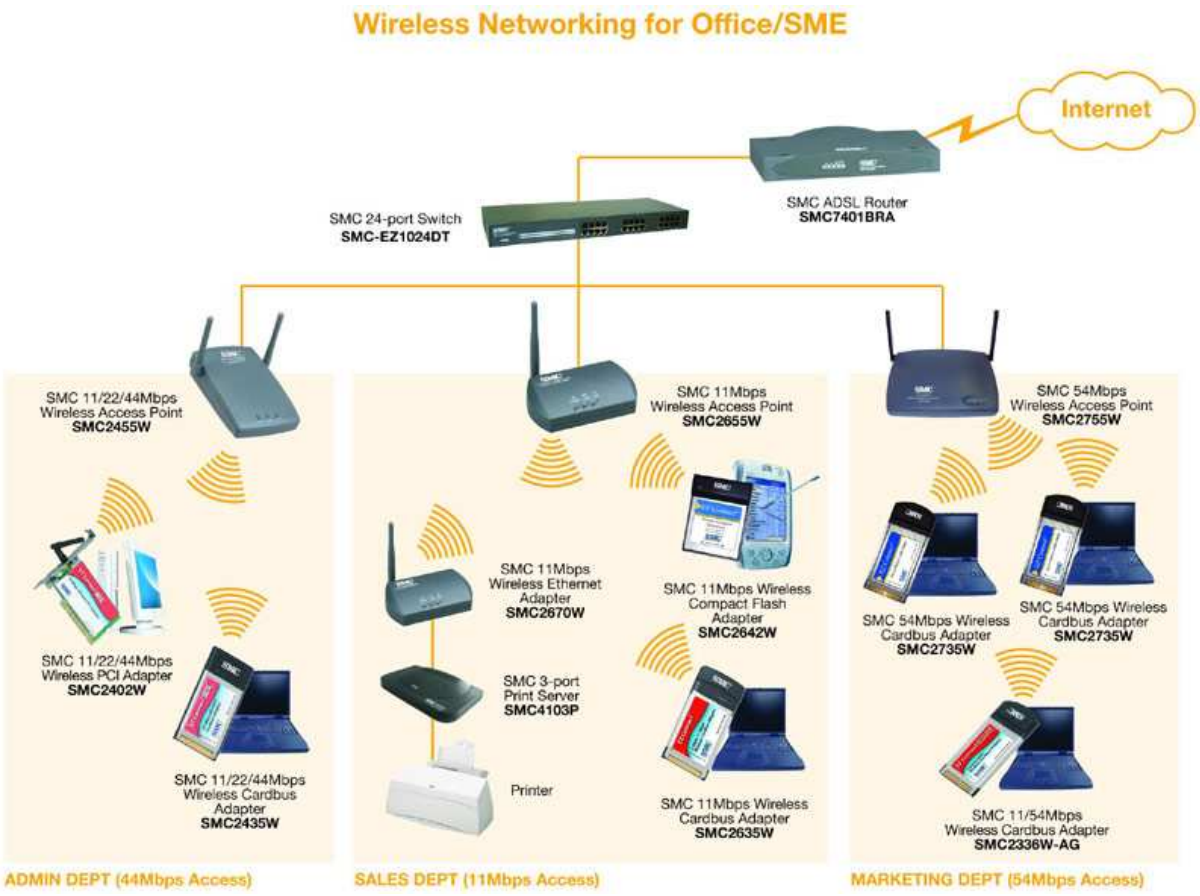
- El punto de acceso permite compartir el acceso a Internet entre todos sus terminales. Esto permite compartir un acceso de banda ancha entre todos los terminales que forman la red, sean dos o cientos de ellos.

- El punto de acceso permite crear redes con un mayor número de terminales y también 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.

1.10.1 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 sí a través de una red que, generalmente, suele ser una red cableada Ethernet. Esta conexión sirve 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.

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**
54 Mbps	*50 metros*	*100 metros*
11Mbps	*50 metros*	*270 metros*
5,5Mbps	*80 metros*	*380 metros*
2Mbps	*130 metros*	*430 metros*
1 Mbps	*160 metros*	*540 metros*

Relación entre distancia y velocidad con las tarjetas Wi-Fi (en ambientes ideales)

1.11 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 2,4 GHz (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 baja 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.

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.

1.11.1 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 tele vigilancia, 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 moviendo el Terminal.

1.11.2 PÉRDIDAS 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.

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.

CAPITULO II

DISEÑO DEL SISTEMA DE COMUNICACIÓN CON RED INALÁMBRICA

2.1 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 describir las características más importantes de los distintos componentes de una red inalámbrica.

2.1.1 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:

2.1.1.1. 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 mejor integración con el resto de equipos. Los líderes de este tipo de equipamiento son Cisco, 3Com, Agere/Orinoco (antiguamente conocidos como Lucent) y Nokia.

2.1.1.2. 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, 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 las cuales 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 darles 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.

Por último, los equipos Wi-Fi tienen la ventaja de que tienen la garantía de ínterfuncionar 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 aparece a la hora de mantener

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 este caso, si los puntos de acceso son de distintos fabricantes, 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 sí pueden proceder de fabricantes distintos sin problemas.

2.1.2 CARACTERÍSTICAS DE LOS PUNTOS DE ACCESO

Los puntos de acceso son realmente unas pequeñas cajas de las que sobresalen 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, en 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 y 802.11g 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

2.1.3 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, son 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 al 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.

2.1.4 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 10/100Base-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 seguridad 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.

2.1.4.1 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. En cualquier caso, siempre es buena idea asegurarse de que el punto de acceso es compatible con nuestro sistema operativo.

2.1.5 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. Ésta suele venir integrada dentro del propio adaptador sin que externamente 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.

2.1.5.1 TIPOS DE ADAPTADORES DE RED

Al igual que desde hace tiempo viene siendo normal encontrar ordenadores que incluyen de fábrica un puerto Ethernet RJ45, 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. 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 sí 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.

- **Unidades 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. 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.

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.

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'.

Es cierto que también se les conoce como *PocketPC* (PC de bolsillo) o como *HandHeldPC* (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. No obstante, un PDA puede utilizarse también como herramienta de comunicación: permite acceder a Internet, ver páginas *web,* gestionar correos electrónicos, etc. En definitiva, un PDA es un pequeño ordenador de gran utilidad debido precisamente a su pequeño tamaño.

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.

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)*. 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.

BRIDGES

Un *bridge* ('puente') es un dispositivo que interconecta dos redes. Una vez interconectadas, los equipos de una red pueden ver y comunicarse con los equipos de la otra red como si todos formaran parte de la misma red. La mayoría de los puntos de acceso hacen las funciones de *bridges* al poder interconectar una red local cableada con la red inalámbrica. Esto hace posible que los ordenadores de la red inalámbrica utilicen las impresoras de la red cableada o accedan a los archivos de cualquiera de sus ordenadores.

No obstante, existe un equipo conocido como *bridge* inalámbrico *{Wireless Bridge)* que es algo distinto de un punto de acceso. Un *bridge* inalámbrico interconecta dos redes remotas (cableadas o no) mediante una conexión inalámbrica. Estas dos redes pueden ser interconectadas también mediante cable, pero los *bridges* inalámbricos evitan la necesidad de tener que instalar o alquilar el cable.

La solución inalámbrica requiere de dos equipos *bridges* inalámbricos, uno en cada extremo. En cualquier caso, estos equipos pueden ser utilizados para extender el área de cobertura de una red inalámbrica, sobre todo cuando se trata de interconectar zonas localizadas en edificios distintos o que no tienen una visibilidad directa para poder

utilizar antenas externas direccionales.

EL *SOFTWARE*

Para instalar y hacer funcionar una red inalámbrica, no hace falta más que el *software* que viene incluido con el propio equipamiento. Es posible que haga falta acceder a la *web* del fabricante de algún adaptador de terminal para bajarse el controlador de dispositivo necesario para nuestro sistema operativo. Por tanto, la necesidad del *software* no viene para hacer funcionar la red, sino para conseguir unas características de gestión más adecuada a nuestras necesidades.

En el mercado existe una variedad de *software* muy útil para analizar y gestionar la red inalámbrica. Entre otras cosas, este *software* sirve para identificar posibles huecos en la seguridad de la red o para identificar redes activas en el entorno. Esto quiere decir que el *software* sirve tanto para piratear las redes de otros como para asegurar la nuestra.

INSTALAR UNA RED CON PUNTOS DE ACCESO

A las redes inalámbricas Wi-Fi con puntos de acceso se les conoce con el nombre de modo infraestructura o modo BSS.

La utilización de puntos de acceso es conveniente cuando se pretende crear una red permanente, aunque sea con pocos terminales, cuando se desea disponer de una amplia área de cobertura o crear una red inalámbrica con muchos usuarios. Dicho de otra forma, salvo que se vaya a realizar una comunicación esporádica entre dos o más ordenadores o se disponga de muy poco presupuesto se empleara en ese caso el modo ad hoc, el modo normal de configuración de las redes inalámbricas Wi-Fi es con puntos de acceso.

Una ventaja adicional de las redes con puntos de acceso es que se disfruta de ciertas características de gestión de red de las que carece completamente el modo *ad hoc* sin puntos de acceso.

En el mercado ha aparecido recientemente una alternativa a los puntos de acceso que

consiste en crear una red en modo *ad hoc* e instalar un *software* especial en uno de los ordenadores de la red. Este *software* hace las funciones de punto de acceso *software.* La única ventaja que tiene esta opción es que nos ahorramos el costo de un punto de acceso, pero, a cambio, nos condena a un ordenador a estar ocupado con esta tarea.

2.2 EN QUÉ CONSISTEN LOS ACCESS POINT

Como ya hemos visto, un punto de acceso es un equipo que funciona en las redes inalámbricas Wi-Fi como si fuera una estación base central que sirve de intermediario de todas las comunicaciones entre los ordenadores de la red. Los ordenadores que se conectan vía radio a los puntos de acceso necesitan disponer de un adaptador de red.

Otras de las ventajas de los puntos de acceso es que permite interconectar la red inalámbrica con una red local cableada e Internet. Para ello, los puntos de acceso disponen de equipos de radio y antena para comunicarse con sus ordenadores inalámbricos y de puertos Ethernet (10/100 BaseT, RJ45) para comunicarse con la red cableada.

En las redes con puntos de acceso no se producen comunicaciones directas entre ordenadores (aunque estén uno junto al otro), sino que todas ellas pasan por el punto de acceso. Por tanto, el punto de acceso es el equipo del que dependen todas las comunicaciones y desde el que se puede gestionar toda la red.

Cada punto de acceso dispone de un área de cobertura. Un área de cobertura es la zona dentro de la cual cualquier ordenador puede comunicarse con el punto de acceso de forma inalámbrica. El mayor o menor tamaño del área de cobertura depende de distintos factores, como son:

- Localización del punto de acceso
- Obstáculos entre el punto de acceso y el ordenador
- Interferencias radioeléctricas
- Tipos de antenas utilizadas

Si se sitúan distintos puntos de acceso complementando sus coberturas, se puede llegar a crear una red local inalámbrica con un área de servicio tan extensa como se desee.

2.2.1 DÓNDE COLOCAR LOS PUNTOS DE ACCESO.

Si lo que se pretende cubrir es una pequeña área, una casa o una pequeña oficina, lo más probable es que baste con colocar un solo punto de acceso en el lugar más céntrico y alto posible. A veces, el lugar viene dado por el sitio donde se encuentra el acceso a Internet (ADSL, módem cable o línea telefónica). Se complica cuando lo que se pretende cubrir es una gran oficina, una zona empresarial, un campus universitario o todo un vecindario. En estos casos hay que estudiar muy bien dónde se van a colocar los puntos de acceso.

La colocación de los puntos de acceso tiene una gran base técnica, pero también tiene un gran componente artístico. Esto se debe a que cualquier cosa del entorno (muebles, estanterías, paredes, fenómenos atmosféricos, metales, árboles, etc.) puede afectar a la propagación de las ondas electromagnéticas y, generalmente, no es posible realizar un estudio teórico de la propagación de las ondas en nuestro entorno. Por ello, teniendo presente lo que afecta a la propagación, la colocación de los puntos de acceso suele basarse en el método de prueba y error.

El método de prueba y error consiste en realizar una inspección previa, decidir los lugares de los puntos de acceso basados en esta primera inspección, hacer pruebas de cobertura con la ayuda de un ordenador portátil y recolocar los puntos de acceso hasta situarlos en su posición idónea.

En cualquier caso, antes de proceder a instalar los puntos de acceso, es necesario tener claro el área que se desea cubrir y cuántos usuarios simultáneos habrá en cada área. Un área muy congestionada puede necesitar más de un punto de acceso.

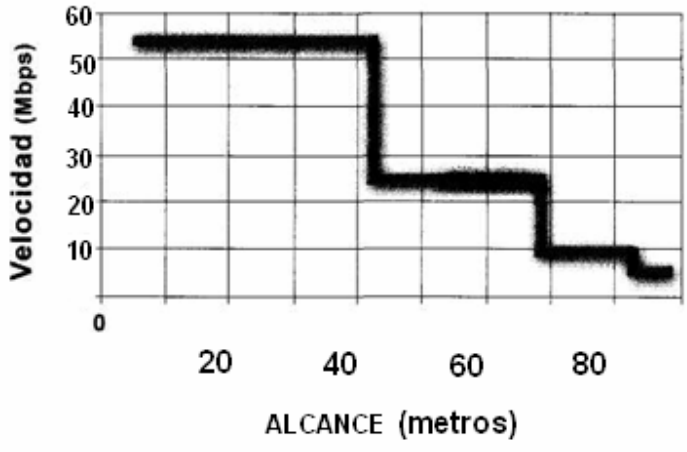
2.2.2 SOBRE LA COBERTURA

Ya sabemos que la cobertura de un punto de acceso puede variar entre los 30 y los 300 metros dependiendo de las condiciones de visibilidad entre emisor y receptor y de las

posibles interferencias que se puedan producir en la zona. En los espacios abiertos se consiguen los mayores alcances, mientras que en los lugares de interior con paredes y muebles se consiguen alcances muy reducidos. Esto quiere decir que los puntos de acceso no se pueden colocar con el único criterio del alcance teórico.

Por otro lado, la potencia de transmisión de un punto de acceso varía entre los 100 mW (límite máximo de acuerdo con la regulación europea) y 1 W (límite máximo de acuerdo con la regulación norteamericana). Evidentemente, a más potencia, mayor es el alcance. No obstante, no siempre interesa que un solo punto de acceso tenga una gran cobertura. Si lo que se pretende cubrir es, por ejemplo, una pequeña oficina o una sala de reuniones, el disponer de una cobertura mucho mayor (llegando a la calle o a las oficinas vecinas) no tiene ningún interés y, sin embargo, se aumenta el riesgo de seguridad de la red. Por otro lado, cuando se intenta cubrir un área donde se concentran muchos usuarios, a menor cobertura de cada punto de acceso, más puntos de acceso serán necesarios para cubrir la misma área y mayor será el ancho de banda total disponible (11 Mbps por cada punto de acceso).

Por tanto, aunque un equipo pueda tener un gran alcance, siempre hay que configurarlo para que ofrezca la cobertura necesaria.



Cobertura típica en el interior de una oficina

2.2.3 SOBRE LA COEXISTENCIA DE PUNTOS DE ACCESO

Típicamente, cada canal del protocolo DSSS de Wi-Fi necesita 22 MHz de ancho de banda (aunque esto puede variar); no obstante, tiene asignado 25 MHz por canal para minimizar las interferencias entre canales. Como la banda de 2,4 GHz en la que trabaja Wi-Fi tiene un ancho de banda total de 80 MHz, esto quiere decir que en una misma zona sólo pueden coexistir tres canales (tres puntos de acceso) sin que haya interferencia entre canales.

Por otro lado, cada punto de acceso facilita un ancho de banda de 11 Mbps. Al situar dos o tres puntos de acceso juntos, se consigue aumentar el ancho de banda disponible a 22 ó 33 Mbps. En este caso, cada usuario sólo podrá disponer de un máximo de 11 Mbps, pero el ancho de banda total disponible para compartir entre todos los usuarios será de 22 ó 33 Mbps.

2.2.4 SOBRE EL ANCHO DE BANDA

El ancho de banda de que dispone cada punto de acceso Wi-Fi es de 11 Mbps a 54 Mbps. Si en un momento dado coinciden varias comunicaciones simultáneas a través del mismo punto de acceso, los 11 o 54 Mbps se repartirán entre todas ellas. Por tanto, dependiendo del número de usuarios simultáneos, el ancho de banda de cada comunicación puede ser inferior o bastante inferior a 11 o 54 Mbps.

A pesar de lo anterior, tampoco es real decir que el ancho de banda de cada ordenador es el resultado de dividir 11 o 54Mbps por el número de ordenadores. La realidad es que cada ordenador no está transmitiendo y recibiendo datos de forma continúa. Evidentemente, depende de la aplicación que se le dé, pero lo normal es que navegar por páginas *web,* explorar el directorio de un disco duro remoto o utilizar una aplicación a distancia suele tener momentos de transmisión de datos entre grandes silencios de comunicación. Esto hace que se consiga un gran aprovechamiento del ancho de banda común. Con 11 o 54Mbps pueden trabajar decenas de usuarios en condiciones normales sin que se noten grandes retardos, salvo en momentos puntuales.

En cualquier caso, si en la zona de cobertura de un punto de acceso se notan grandes retardos y se comprueba que no es debido a interferencias, siempre se puede añadir un nuevo punto de acceso.

2.3 EL ACCESO A INTERNET

La red Internet es una red 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.

2.3.1 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 (RJ45). 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.

2.3.2 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').

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 queda listo para utilizar el acceso a Internet.

2.3.3 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 DSL/cable.

Si el ordenador puede acceder a Internet desde el módem DSL/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 (RJ45): 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 (RJ45) no cruzado para conectar el módem ADSL/cable con el punto de acceso.

2.4 COLOCAR UNA ANTENA EXTERNA

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, la señal 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.

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.

2.4.1 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.

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).

2.4.2 La Relación Señal a ruido.- Uno de los mayores inconvenientes de los sistemas de radio es que, cuando se emite, no solo se emiten los datos, sino que, mezclados con los datos también, se emiten ruidos. De la misma forma, cuando se recibe, no solo se reciben los datos, sino que también se recibe ruido. Este hecho inevitable, incluso en los sistemas digitales se corrige utilizando técnicas especiales de modulación, filtrado, auto correlación, etc. En cualquier caso una transmisión se recibirá mejor cuanto mas potente sea la señal de los datos en comparación con los ruidos.

2.4.3 Patrón de radiación y Apertura del Haz.- Es un grafico 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 la antena. Las

antenas omnidireccionales emiten en todas direcciones y tienen menor alcance que las antenas direccionales.

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.

2.4.4 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:

1. Vertical. Cuando el campo eléctrico generado por la antena es vertical con respecto al horizonte terrestre (va de arriba abajo).

2. Horizontal. Cuando el campo eléctrico generado por la antena es paralelo al horizonte terrestre.

3. 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).

4. 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.

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

2.5 SEGURIDAD

Las comunicaciones inalámbricas tienen un inconveniente particular: carece de barreras físicas. Por tanto, cualquier persona, con unos conocimientos mínimos sobre seguridad y con una tarjeta Wi-Fi instalada en su ordenador puede, potencialmente, acceder a un punto de acceso de una red inalámbrica. No obstante, fundamentalmente, lo que hace que esto sea cierto es que muy pocos usuarios se toman en serio las medidas de seguridad. Por ejemplo, suele ser común que un usuario instale una red Wi-Fi sin modificar la configuración que trae el sistema por defecto. Si un intruso desea entrar en un sistema, lo primero que comprobará es si todavía tiene la configuración inicial.

Por tanto, independientemente de que las redes inalámbricas sean más o menos seguras, lo que sí es cierto es que vienen provistas de medidas de seguridad para evitar que personas ajenas puedan hacer uso de la red. Estas medidas son lo suficientemente buenas como para que la inmensa mayoría de las personas que tenemos a nuestro alrededor no puedan entrar en la red.

La única manera de conseguir seguridad es manteniendo unas técnicas de protección adecuadas. Hay que ser conscientes de que ninguna técnica de protección es eficaz al cien por ciento. Siempre existe riesgo aunque sea pequeño. No obstante, a más barreras de seguridad, menor será el riesgo.

En un principio, las barreras de seguridad básicas que pueden tenerse en cuenta para cada uno de los riesgos son las siguientes:

- Pérdida del equipo. Tomar las precauciones mínimas para evitar en lo posible la pérdida o robo del equipo. No dejar grabados en el equipo los nombres de usuario y contraseña, ni tampoco dejar estos datos escritos en papeles que estén permanentemente con el equipo.

- Infección por un virus. Utilizar software antivirus. Los ataques exteriores se pueden presentar bajo tres formas: virus, gusanos y caballos de Troya. Un virus es un

programa diseñado para autorreplicarse y ejecutarse sin el conocimiento del usuario. Un gusano es un programa que está pensado para autorreplicarse y difundirse por el mayor número de equipos posibles. Un caballo de Troya es un programa que aparenta ser un programa útil, pero que, realmente, se dedica a recoger información o a facilitar que el intruso tenga acceso a ese ordenador o a la red en la que se encuentra.

- Uso equivocado por personas autorizadas (intencionado o accidental). Para estos casos es fundamental implantar una política de seguridad donde se defina cuáles son los puntos importantes que se deben tener en cuenta en relación con la seguridad.

- Uso fraudulento por personas no autorizadas. A pesar de que los problemas de seguridad es un tema que tienen en mente la mayoría de los usuarios, muchas veces no se le dedica una mínima atención. Por ejemplo, es habitual dejar configurados los productos en su configuración por defecto. Si hay algo que conocen los intrusos es la configuración por defecto de los equipos. Por ello, es recomendable cambiar las claves de acceso y activar las medidas de seguridad no configuradas por defecto. En el caso de WEP, por defecto, viene deshabilitado en muchos equipos. Conviene habilitarlo, así como cambiar la identificación SSID. Otra medida interesante en redes inalámbricas, desde el punto de vista de la seguridad, es que, si se dispone de router con DHCP (Dynamic Host Control Protocol, 'Protocolo de Control Dinámico del Hosf), conviene tenerlo deshabilitado y asignar las direcciones IP de forma manual. Resulta también altamente recomendable la instalación de firewall.

CAPITULO III

PRUEBAS Y VERIFICACION DEL FUNCIONAMIENTO DE LA RED INALÁMBRICA.

Como se ha comentado anteriormente, en las redes pequeñas hay poco que analizar: se coloca el punto de acceso en el lugar más cómodo y se comprueba si cubre las expectativas. En el peor de los casos, bastará con hacer un par de intentos de colocación antes de llegar a la disposición óptima.

En general, el proceso de instalación de una red inalámbrica se compone de los siguientes pasos:

- Realizar un análisis previo.
- Configurar los ordenadores.
- Configurar e instalar los puntos de acceso.
- Instalar las conexiones entre los puntos de acceso.
- Configurar el acceso a Internet.

3.1 ANÁLISIS PREVIO

El análisis previo supone simplemente definir las necesidades, analizar el terreno, estudiar los posibles inconvenientes y calcular los recursos. El tener una idea clara de estos conceptos ayudará grandemente a obtener una red adecuada y eficaz.

Los pasos a dar son los siguientes:

3.1.1. **Determinar las necesidades.** Se parte de que se conoce exactamente el área que se pretende cubrir y los usuarios de la red.

3.1.2. **Hacer un esquema de cobertura.** Dibujar un diagrama donde se especifiquen las áreas a cubrir y las necesidades en cada área.

3.1.3. **Decidir las áreas de movilidad.** Habrá áreas en las que baste tener servicio, mientras que en otras se necesitará garantizar además que el servicio no se corte

cuando se desplace el usuario. Tenemos, por tanto, que determinar las áreas con uno y otro tipo de movilidades. Es posible que este último aspecto afecte a la distribución de los puntos de acceso. Las opciones son las siguientes:

3.1.4. **Lugares Con Cobertura.** Son aquellas zonas que tienen que estar cubiertas porque hay usuarios que necesitan conectarse a la red desde allí. Incluso puede haber zonas que necesitan estar cubiertas muy esporádicamente. En este caso, pueden disponerse de puntos de acceso que ocasionalmente puedan estar situadas en lugares distintos.

Lugares por los que se pueda desplazar (roaming). Son las zonas por las que se desplazan los usuarios haciendo uso de la conexión. Estas áreas deben garantizar una continuidad del servicio aunque los usuarios estén en movimiento. Éste sería el caso, por ejemplo, de un almacén donde se hace inventario.

Estudiar la cobertura real. Una vez descritas las necesidades, se puede hacer una comprobación práctica de la cobertura. Se instala una tarjeta Wi-Fi en un ordenador portátil, se va situando el punto de acceso y la portátil en distintos sitios y se va comprobando el nivel de señal dentro de las áreas a cubrir. Esto nos da una idea de los mejores lugares donde situar los puntos de acceso. Para cada localización se debe comprobar tanto el alcance, como la respuesta (velocidad máxima conseguida). Para comprobar el alcance, basta con desplazarse y ver que la conexión sigue establecida. Para comprobar la calidad de respuesta, se pueden realizar transferencias de archivos y ver la velocidad de transmisión de datos. En las zonas con interferencias se notará que la velocidad de transferencia puede llegar a ser realmente baja. Por cierto, la mayoría de los equipos Wi-Fi incluyen un *software* de utilidades que permiten verificar la calidad de la señal (fuerza de la señal, ruidos, velocidad de transmisión, etc.). Este *software* puede resultar muy útil para estudiar la cobertura real. Hay que tener siempre en cuenta que, en general, el mejor punto para colocar un punto de acceso será el centro de la habitación en una posición elevada. En las habitaciones repletas de obstáculos, como muebles, librerías, estantes, archivadores, etc., se consiguen coberturas inferiores

que en las habitaciones abiertas. Hay que evitar esconder el punto de acceso dentro de los típicos cubículos separadores de las oficinas, en armarios o ponerlos cerca de objetos de metal. Recuerde que algunos armarios de oficinas y mesas son de metal.

3.1.5. **Identificar interferencias.** El entorno radioeléctrico está sujeto a la presencia de interferencias. Las interferencias pueden bajar el rendimiento del sistema; por ello, es importante identificar las posibles fuentes de interferencias. Generalmente, estas fuentes proceden de dispositivos como hornos microondas, teléfonos inalámbricos, dispositivos *bluetooth,* motores (de ascensores, por ejemplo) o alarmas. El impacto de estas fuentes de interferencia se puede comprobar haciendo pruebas de transferencia con los dispositivos encendidos y apagados. Se puede utilizar el *software* de utilidad que acompaña al equipo Wi-Fi para comprobar las interferencias. En los lugares con interferencias donde no se puede eliminar la fuente y sea necesaria la cobertura, se pueden colocar puntos de acceso adicionales.

3.1.6. **Hacer una instalación de prueba.** Llegados a este punto, se tiene una idea muy clara de las condiciones del entorno. No obstante, antes de lanzarse a instalar todos los puntos de acceso, conviene hacer una primera instalación de prueba donde sólo se conecten unos cuantos usuarios. Esto puede ayudar a detectar posibles problemas de desplazamiento *(roaming)* o de congestión por interferencias.

3.1.7. **Realizar la comprobación final.** Una vez hechas todas las comprobaciones anteriores, se contará con todos los datos necesarios para hacer la instalación: localización de los puntos de acceso, identificación de zonas muertas, modelo de funcionamiento del roaming, fuentes de interferencias y número y localización de los usuarios. Basta con echarle un último vistazo a todo antes de decidir la instalación.

3.2 CONFIGURAR LOS ORDENADORES

Cualquier ordenador que se desee conectar de forma inalámbrica a una red con puntos de acceso necesita disponer de un adaptador de red (tarjeta Wi-Fi) y configurarse adecuadamente para que el adaptador se entienda con el punto de acceso de la red

deseada.

El proceso de instalación de estos dispositivos es idéntico tanto para la configuración de redes inalámbricas en modo *ad hoc*, como para el modo infraestructura (con puntos de acceso).

En cuanto a lo que hay que configurar desde el ordenador, hay que llevar a cabo dos tipos de configuraciones:

3.2.1 CONFIGURAR EL ADAPTADOR DE RED

Los adaptadores de red se configuran con una aplicación que viene en el CD incluido con el equipo. Los parámetros a configurar son los siguientes:

- **Tipo de red.** En este caso, el tipo de red que hay que configurar es el BSS, también conocido como infraestructura o con puntos de acceso.

- **Nombre de red.** El nombre de red debe ser el mismo que el configurado en el punto de acceso, incluidos los caracteres en mayúscula y minúscula. Al parámetro nombre de red también se le conoce como *Network Name* ('Nombre de Red') o *SSID (Service Set Identifier,* 'Identificador del Conjunto de Servicios'). Muchas aplicaciones de configuración de adaptadores de red ofrecen la posibilidad de realizar una búsqueda automática de todas las redes del entorno que son recibidas por el adaptador en ese momento. En este caso, sólo habría que escoger un nombre de red de la lista.

- **Canal.** En este caso no es necesario configurar el canal porque el adaptador lo tomará automáticamente del punto de acceso.

- **Seguridad.** Es importante que los parámetros de seguridad que aquí se configuren sean los mismos que los configurados anteriormente en el punto de acceso. Si se tiene dudas, simplemente se dejan deshabilitados los parámetros de seguridad.

Hay que tener en cuenta que un ordenador puede tener guardadas distintas

configuraciones de red, distintos perfiles. Esto es especialmente útil cuando un mismo ordenador se conecta a distintas redes. En estos casos no es necesario introducir todos los parámetros cada vez que se cambia de red, sino, simplemente, elegir el perfil correspondiente.

3.2.2 Instalación de la Red Inalámbrica con Access Point.

Primeramente se proceda a conectar las tarjetas inalámbricas (adaptadores de red) en el interior de las computadoras debido que se tratan de adaptadores PCI, PCMIA o ISA; una vez que se fija dicha tarjeta se procede al encendido de la computadora y al momento que se inicia Windows, automáticamente aparece en la pantalla un asistente

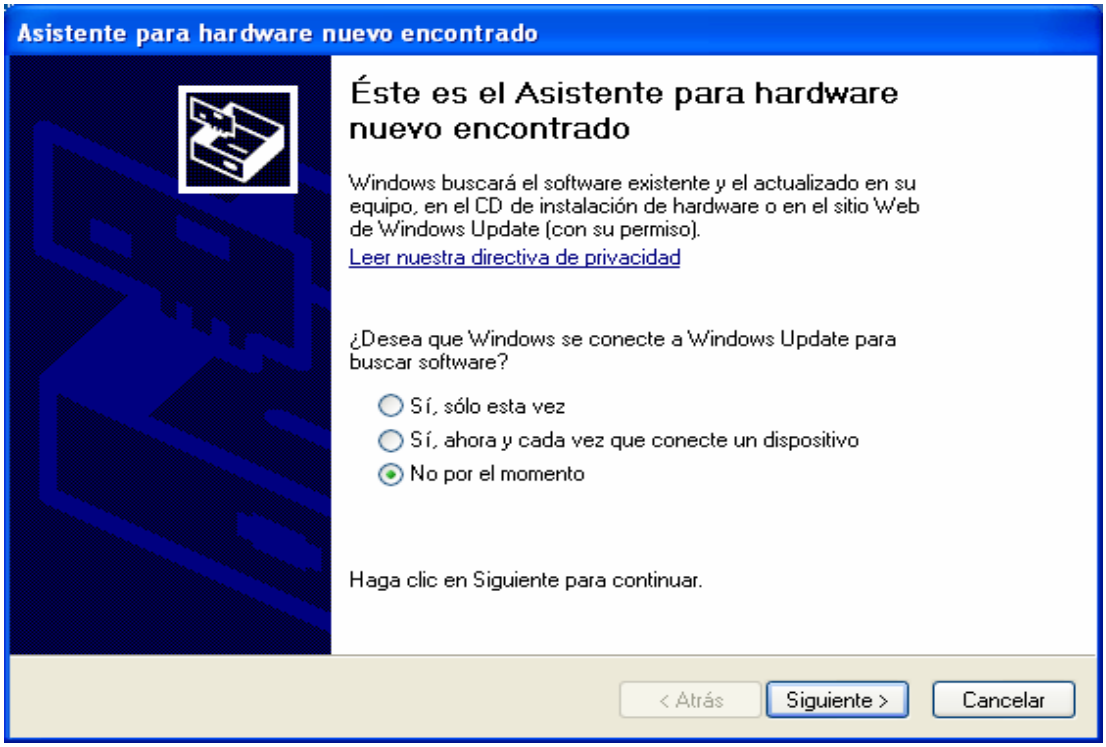


Fig.: 3.1

Se escoge dicha opción debido a que no es necesario que Windows se conecte a Windows Update ya que no se necesita actualizar.

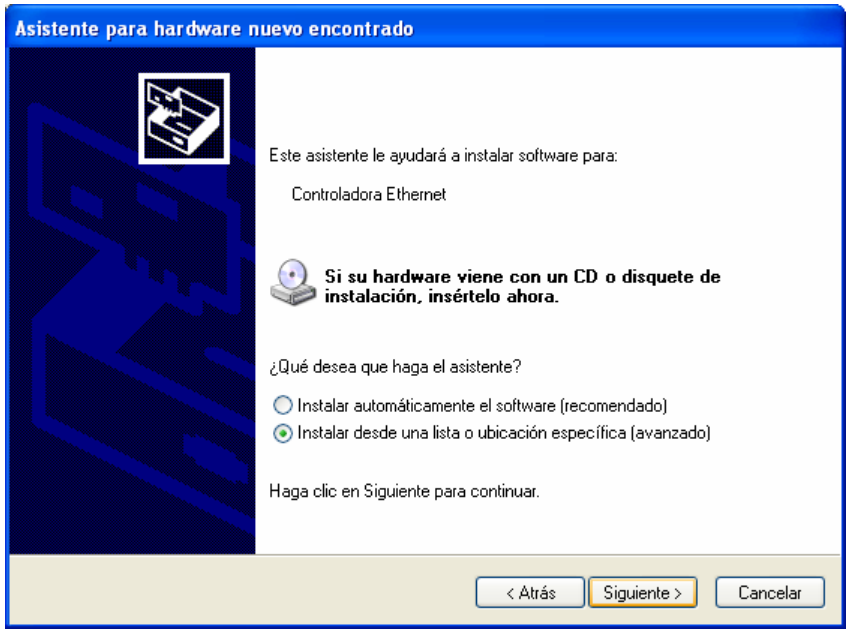


fig. 3.2

Como se observa en el la fig. 3.2 se debe insertar el CD que viene con la tarjeta; luego se procede a examinar en la unidad “E” del computador que es donde se encuentra el CD con los respectivos drivers para que la tarjeta quede instalada.

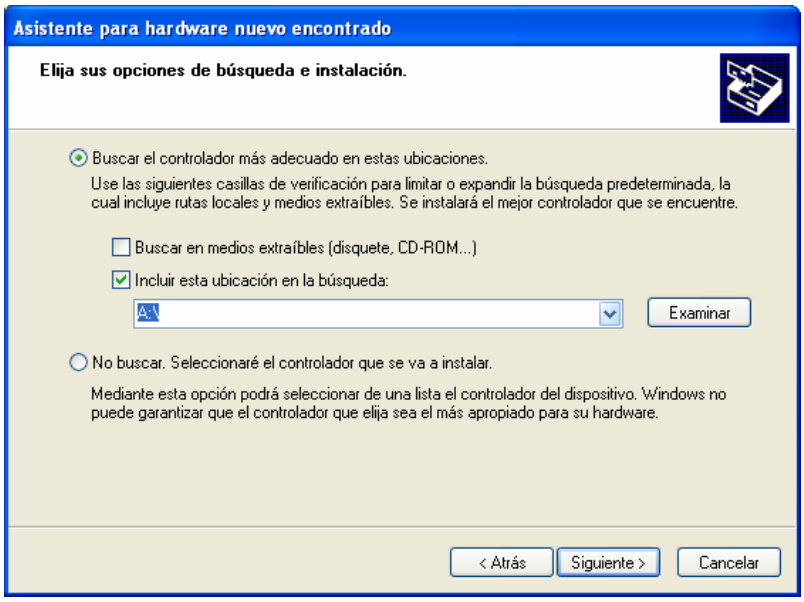


fig. 3.3

Luego de haber escogido la unidad E se hace clic en siguiente para que comience a buscar automáticamente los drivers de instalación.

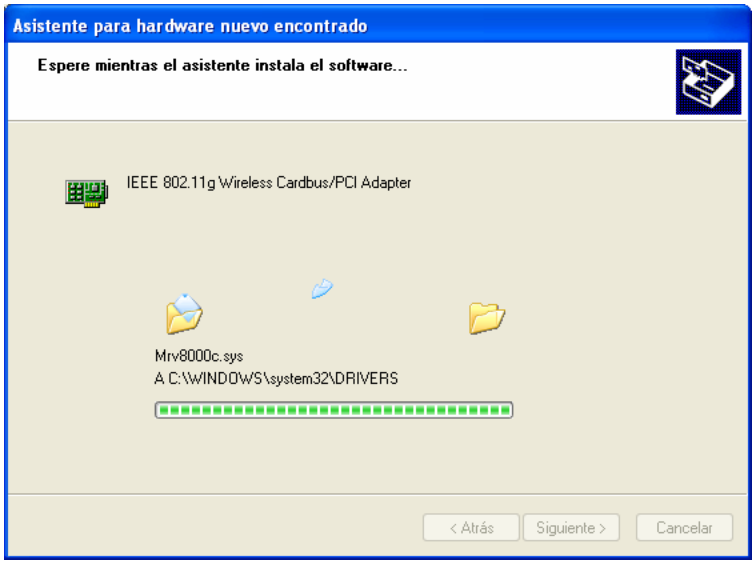


Fig. 3.4

Como se observa los drivers de la tarjeta inalámbrica se están instalando y guardando en el disco duro.

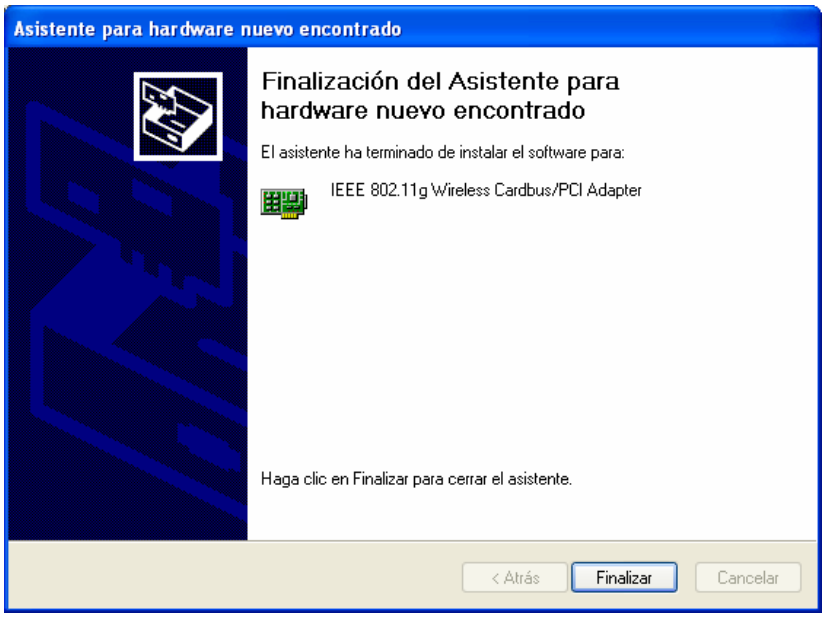


Fig. 3.5

En esta última parte del asistente se puede observar que los controladores de la tarjeta inalámbrica ya han sido instalados, solamente tenemos que hacer clic en finalizar para que concluya definitivamente la instalación.

Luego en el escritorio va aparecer el siguiente mensaje como se muestra

Fig. 3.6

Aparece el mensaje “conexiones de red inalámbrica no esta conectado” esto se debe a que falta por configurar los parámetros del Access point y los protocolos TCP/IP.

3.2.3 Configurar el protocolo TCP/IP.

La operación de configurar el protocolo TCP/IP y el adaptador de red hay que repetirla con cada ordenador que se desee conectar al punto de acceso.

Cualquier ordenador con un adaptador Wi-Fi que tenga configurados correctamente los parámetros anteriores y que esté dentro del área de cobertura radioeléctrica de cualquier punto de acceso de la red formará parte de ella y, por tanto, podrá compartir sus recursos y tener acceso a los recursos (configurados como compartidos) del resto de ordenadores. Esto quiere decir que, para añadir nuevos ordenadores a la red, simplemente hay que copiar los parámetros de cualquiera de los ordenadores ya conectados y configurárselos al nuevo ordenador.

Por cierto, un mismo ordenador puede tener guardadas distintas configuraciones de red, distintos perfiles. Esto es especialmente útil para aquellos casos en los que un mismo ordenador se conecta a distintas redes. En estos casos no es necesario introducir todos los parámetros cada vez que se cambia de red, sino, simplemente, elegir el perfil correspondiente.

Configurar el protocolo TCP/IP en un ordenador suele suponer configurarle una dirección IP, una máscara de subred, una puerta de enlace y un servidor DNS. No obstante, en el

caso de los puntos de acceso, todas estas configuraciones suelen sustituirse por configurar cada ordenador para que obtenga las direcciones IP de forma automática. El punto de acceso ya se encarga de pasarle a cada ordenador los datos necesarios para establecer la comunicación.

La forma de configurar el ordenador automáticamente para obtener las direcciones IP depende del sistema operativo de que se dispone. Por cierto, si no sabe el sistema operativo de un ordenador, puede averiguarlo haciendo clic en *Inicio, Panel de control* y *Sistema.*

Fig. 3.7

Los pasos a dar para cada sistema operativo Windows son los siguientes:

- Con **Windows 95/98** haremos clic con el botón derecho sobre el icono *Entorno de red.* Posteriormente, seleccionamos la opción *Propiedades.* La ventana que nos aparece nos indica los componentes de red que están instalados. Hacemos doble clic sobre el componente *TCP/IP* (o bien, lo marcamos y hacemos clic sobre el botón *Propiedades). A* continuación, en la ficha *Dirección IP,* seleccionamos *Obtener una dirección automáticamente.* En la ficha *Configuración Wins* señalamos la opción *Usar DHCP para resolución WINS.* En la ficha *Puerta de enlace* no debe haber ninguna puerta de enlace configurada. Por último, cerramos todas las ventanas pulsando los botones *Aceptar.* Al finalizar, habrá que apagar y encender el ordenador.

- Con **Windows 2000/Me** haremos clic con el botón derecho sobre el icono *Mis sitios de red.* A continuación, seleccionamos la opción *Propiedades.* En la ventana que nos aparece presionamos el botón *Propiedades.* En la lista de componentes marcamos el componente *Protocolo Internet (TCP/IP) y* presionamos el botón *Propiedades.* Una vez que hemos llegado a la ventana de *Propiedades de protocolo Internet,* marcamos la opción *Obtener la dirección IP automáticamente.* Hay que verificar también que está marcada la opción *Obtener la dirección del servidor DNS automáticamente.* Para terminar, simplemente se cierran todas las ventanas pulsando *Aceptar.*

- Con **Windows NT** pulsamos *Inicio;* a continuación, elegimos *Configuración y* elegimos la opción *Panel de control.* Aquí debemos localizar el icono *Red* y hacer doble clic sobre él. Nos aparecerá una ventana titulada *Red.* Seleccionamos la ficha *Protocolos.* En la lista de protocolos de red debe aparecer *Protocolo TCP/IP.* Lo seleccionamos y pulsamos el botón *Propiedades.* Nos aparecerá una nueva ventana donde seleccionamos la ficha *Dirección IP.* Marcamos la opción *Obtener la dirección IP de un servidor DHCP.* Para terminar, cierre todas las ventanas pulsando *Aceptar.*

- Con **Windows XP** hay que hacer clic en *Inicio, Configuración, Conexiones de red.* A continuación se hace clic con el botón derecho sobre *Conexión de área local* y se elige *Propiedades.* También se puede llegar aquí eligiendo *Cambiar la configuración de esta conexión* en la ficha *Tareas de red.* Se continúa haciendo clic sobre *Protocolo Internet (TCP/IP)* y, luego, sobre el botón *Propiedades.* Se marca la opción *Obtener una dirección IP automáticamente.* Hay que verificar también que está marcada la opción *Obtener la dirección del servidor DNS automáticamente.* Para terminar, cierre todas las ventanas pulsando *Aceptar.*

Aunque, generalmente, se configure el protocolo TCP/IP del ordenador para obtener automáticamente las direcciones IP del punto de acceso, si se desea, también podrían configurarse unos datos concretos. En este caso, los datos serían los siguientes:

Número IP del ordenador: Cualquier número, siempre que esté dentro del rango de numeración de la red local inalámbrica. Eso sí, cada ordenador debe disponer de un número IP distinto. Por ejemplo, si el número IP del punto de acceso es el

192.168.1.1, a los ordenadores se les podría asignar los números 192.168.1.x, donde x es cualquier número entre 2 y 255.

Para nuestro caso nosotros vamos a tener las siguientes direcciones IP de los computadores.

192.168.1.3 Pc3

192.168.1.4 Pc4

192.168.1.5 Pc5

192.168.1.6 Pc6

Máscara de subred: Generalmente, se suele utilizar como máscara de subred el número 255.255.255.0. Este número es válido para redes que dispongan de menos de 255 terminales.

Puerta de enlace: Aquí habría que indicar el número IP del punto de acceso. Para nuestros casos la dirección del punto de acceso del Access Point es la 192.168.1.21

DNS: Lo normal es introducir aquí la dirección IP del punto de acceso. Ya que el punto de acceso sabrá asignar el DNS adecuado. No obstante, si se está conectado a Internet y se conoce la dirección de los DNS, podría configurarse directamente en este campo. El DNS que utilizamos fue el 192.188.57.242.

Los pasos a seguir para la configuración del protocolo TCP/IP son los siguientes:

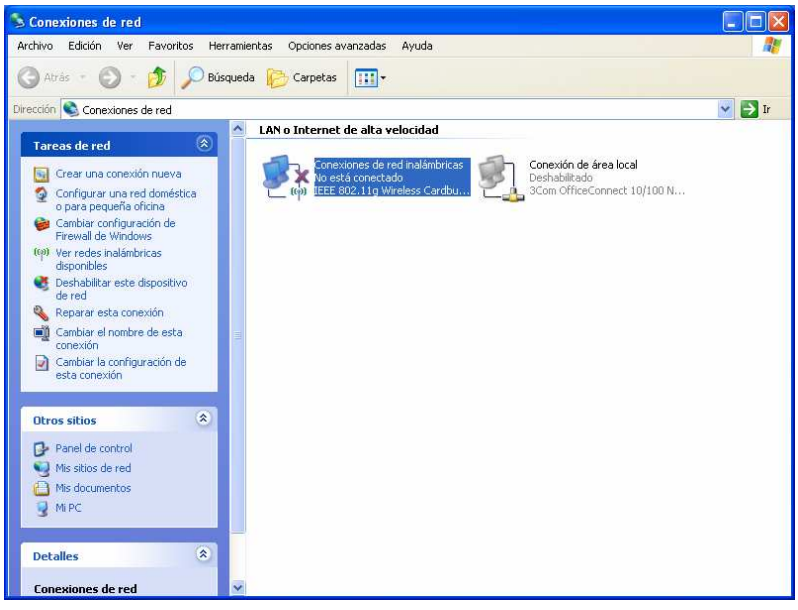


Fig. 3.8

Hacemos doble click en el icono de conexiones de red para que nos aparezca la pantalla con las conexiones de red disponible.

Hacemos clic derecho en conexiones de red inalámbrica y escogemos la opción propiedades. Luego nos aparecerá la siguiente pantalla en la cual escogemos la opción indicada “Protocolo Internet (TCP/IP)” y hacemos clic en propiedades.

Fig. 3.9

En la pantalla propiedades debemos configurar los parámetros que se muestran en la figura

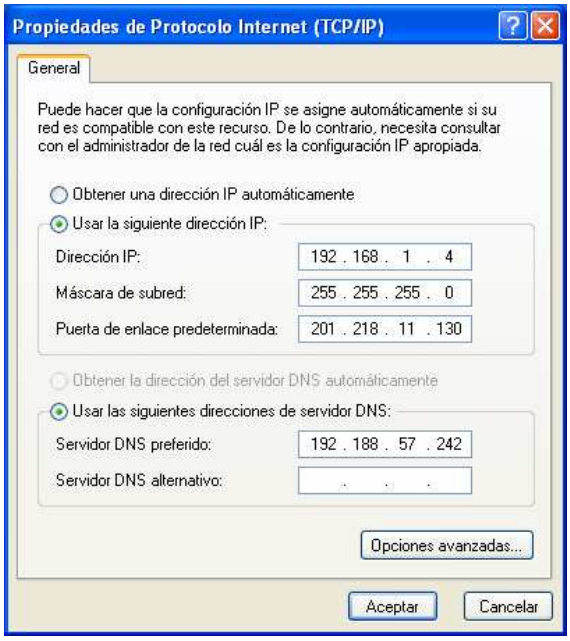


Fig. 3.10

3.2.4 CONFIGURAR EL PUNTO DE ACCESO

Una vez que se dispone del punto de acceso, antes de colocarlo en su lugar definitivo, es conveniente proceder a su configuración. La mayoría de los fabricantes ya facilitan el punto de acceso con una configuración por defecto. Esta configuración suele ser adecuada para una red con un solo punto de acceso. En este caso, el fabricante facilita los valores (fundamentalmente el nombre de red y las características de seguridad) con los que hay que configurar los adaptadores de red de los ordenadores de los usuarios de la red.

Si se desea configurar unos valores propios o se tiene la necesidad de realizar algún tipo de configuración especial, entonces será necesario modificar la configuración. La forma de configurar un punto de acceso depende del fabricante o, incluso, del modelo del equipo. Por ello, siempre es recomendable atender a las instrucciones del manual de usuario del equipo.
En cualquier caso, los pasos a dar son los siguientes:

3.2.4.1 Establecer una conexión entre un ordenador y el punto de acceso. Esta conexión se puede llevar a cabo de dos formas:

A *Vía inalámbrica*. En este caso se debe configurar el adaptador de red del ordenador con el nombre de red (SSID) especificado en el manual de usuario del punto de acceso el cual en nuestro caso fue **LINKSYS**.

B *Vía cable.* En el caso de llevarse a cabo la conexión vía cable, se tienen tres posibilidades: cable Ethernet 10/lOOBaseT a conectar en puertos RJ45 del ordenador y del punto de acceso el cual consta de cuatro puertos, cable USB o cable específico del equipo a conectar al puerto serie del ordenador.

3.2.4.2 Tenemos dos alternativas dependiendo del modelo del punto de acceso:

A *Mediante una aplicación de configuración.* Esto supone ejecutar una aplicación específica de configuración que viene incluida en el CD que acompaña al punto de

acceso. Esta aplicación suele localizarse en el directorio principal del CD bajo el nombre ***setup***.

B *Mediante el servidor* web *del punto de acceso.* En este caso el punto de acceso incluye un servidor *web* al cual se accede desde el ordenador del usuario mediante cualquier navegador de Internet (Internet Explorer o Netscape). Previamente hay que configurar el ordenador para que obtenga la dirección IP de forma automática e introducir en el navegador de Internet la dirección (URL) que se indica en el manual de usuario del punto de acceso (una dirección IP que suele empezar por 192.168.x.x) y que en nuestro equipo vino con la dirección **IP 192.168.1.1** Esto llevará a una ventana donde se solicita el nombre de usuario y clave para entrar en el menú de configuración. Estos datos pueden ser modificados por el administrador de la red, pero, por defecto, el fabricante ofrece un nombre de usuario y clave para permitirle al administrador entrar la primera vez. Estos datos por defecto suelen consistir en dejar el nombre de usuario en blanco e introducir la clave ***admin.***

Esta fue la opción que escogimos para la configuración de nuestro punto de acceso como se muestra en las siguientes figuras.

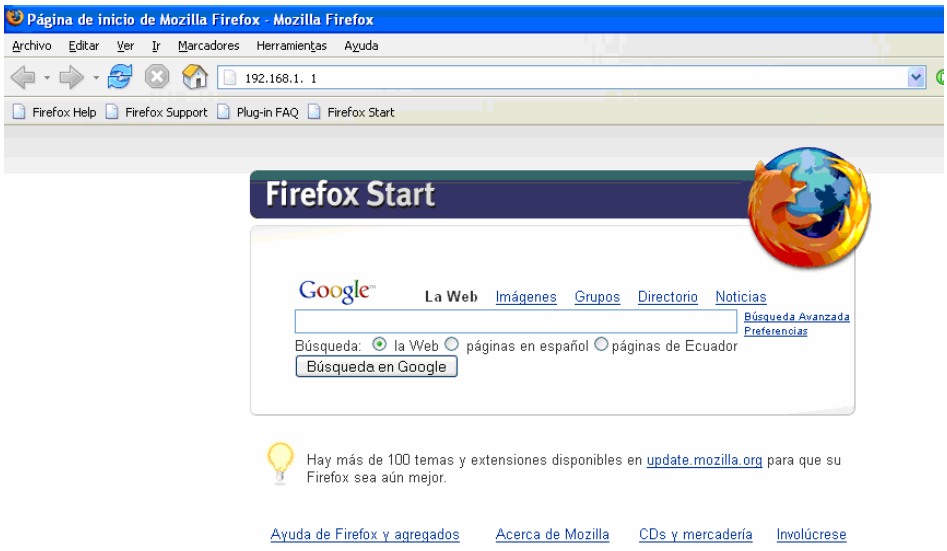


Fig. 3.11

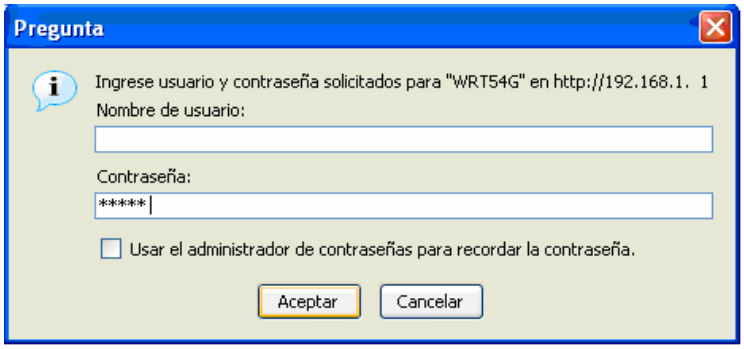


Fig. 3.12

Esta ventana aparece con los campos para llenar tanto el nombre de usuario como la contraseña. Para el Access Point Linksys por default viene sin nombre de usuario y como contraseña es la palabra “admin.” Cuyo detalle lo indica la tabla 3.1.

MODELO	URL	USUARIO	CLAVE
LinksysAP Router/switch	***http://192.168.1.1***		***admin***
SpeedStream 2623	*http://192.168.254.2*		*admin*
3Com Homeconnect	*http://192.168.2.1*		*admin*
3Com Officeconnect	*http://192.168.1.1*		*admin*
Adaptec Ultra Wireless	*http://192.168.8.1*	*admin*	
Otros	*http://192.168.1.250*		*public*

Tabla 3.1. Ejemplos de URL, usuario y clave para acceder a distintos puntos de acceso

3.2.4.3. Seguir las instrucciones del programa de configuración o moverse por las páginas web del punto de acceso para llevar a cabo los cambios de configuración deseados.

Un punto importante es que, salvo que se utilice un cable específico, para conectar el ordenador al punto de acceso, es necesario que el ordenador esté configurado convenientemente. Esto supone que el ordenador esté configurado para obtener la dirección IP de forma automática.

3.2.5 Propiedades configurables en el punto de acceso

Existen modelos de puntos de acceso que solamente son puntos de acceso de red local

inalámbrica. Sin embargo, es habitual encontrar modelos de puntos de acceso que, además, incluyen en su interior un *router,* un *switch* o un módem DSL. Por este motivo, las propiedades que son configurables en cada modelo de punto de acceso pueden variar dependiendo de todo lo que sea capaz de hacer. En cualquier caso, las propiedades principales propias de las funciones de punto de acceso son las siguientes:

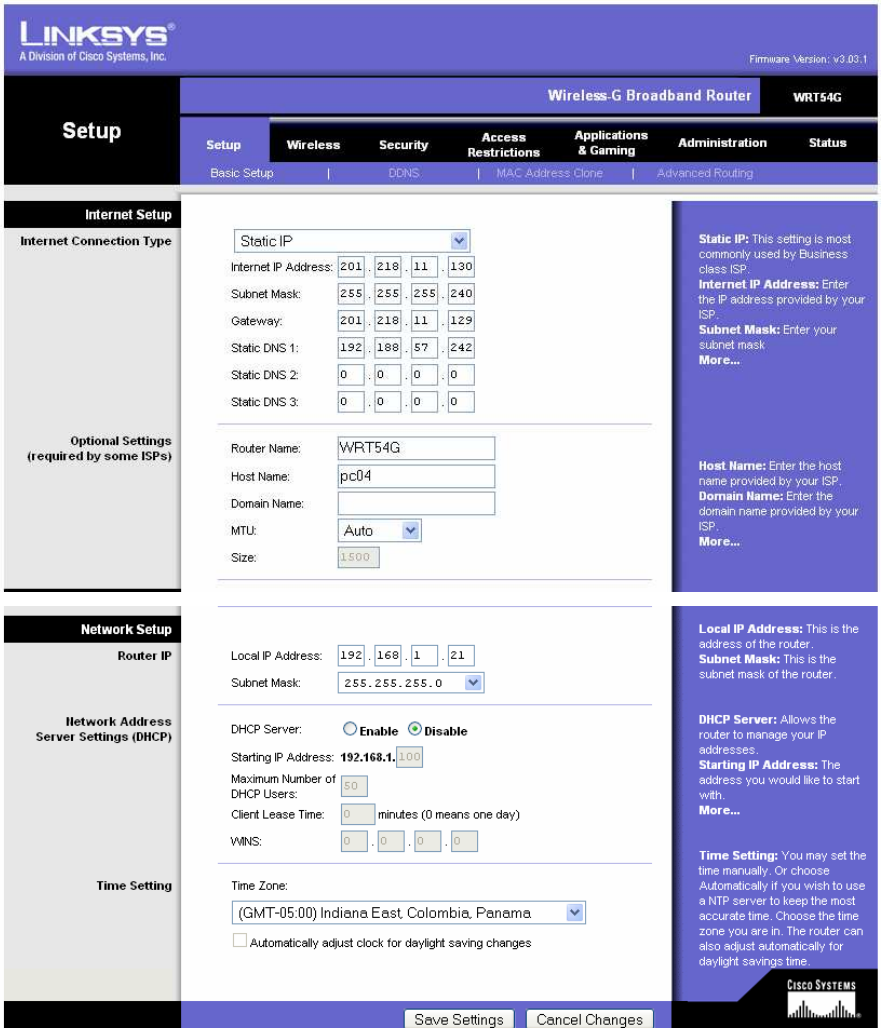


Fig. 3.13

Como podemos observar en la figura anterior luego de ingresar la clave nos aparece esta ventana en la cual podemos configurar los parámetros del Access Point.

Siempre que se haga un cambio en la configuración del Access Point debemos guardar los cambios para que estos surjan efecto.

Los Access Points nos dan algunas facilidades que nos permiten configurar las redes inalámbricas de acuerdo a nuestras necesidades.

Setup, Wíreless, Security, Access Restrictions, Administration and Status.

Fig. 3.14

3.2.6 Parámetros:

3.2.6.1. **Nombre de red (Network name***).* Al nombre de red se le conoce también como *SSID (Service Set Identifier,* 'Identificador del Conjunto de Servicios')- Los puntos de acceso suelen incluir un nombre de red por defecto. No obstante, es recomendable sustituir este nombre por cualquier otro que se considere adecuado. Por cierto, este nombre de red debe ser el que se configure en cada ordenador. Es importante recordar que en los nombres de red se diferencian las letras mayúsculas de las minúsculas.

3.2.6.2. **Canal (Channel)**. Aquí se deberá introducir el número de canal que se considere apropiado. Hay que tener en cuenta que, aunque el sistema me permita elegir cualquier canal, existen limitaciones regulatorias para el uso de los canales dependiendo del área geográfica en que nos encontremos.

3.2.6.3. **Seguridad (Security)**. Los equipos Wi-Fi disponen de determinadas características de seguridad que pueden ser configuradas en el punto de acceso y en los adaptadores de cada ordenador que forme parte de la red. Es importante que los parámetros de seguridad que aquí se configuren sean los mismos que los que se configuren en cada ordenador. La primera vez que se configura un punto de acceso conviene dejar deshabilitados los parámetros WEP de seguridad. Una vez comprobado que la red funciona adecuadamente, se puede proceder a configurar las características de seguridad. Para utilizar el cifrado WEP, hay que habilitar esta característica, elegir un tipo de cifrado *(WEP type)* e introducir una clave de cifrado *(WEPKey).* Sólo existen dos tipos de cifrado: 64 bits y 128 bits. El tipo de 128 bits ofrece un mayor nivel de seguridad, pero también es cierto que hace bajar levemente el rendimiento. En cuanto a la clave de

cifrado, se trata de una palabra clave que puede incluir caracteres alfabéticos o numéricos. El sistema puede mantener hasta cuatro claves, de las cuales sólo una estará activa. Periódicamente debe cambiarse la clave activa para aumentar la seguridad del sistema. Algunos sistemas incluyen una utilidad que permite generar claves de cifrado a partir de una frase *(passphrase).* Es más fácil recordar la frase que la clave. Adicionalmente, los puntos de acceso ofrecen distintas características que ayudan a gestionar la red. Algunas de estas características son las siguientes:

3.2.6.4. **Bajada automática de velocidad {Auto rate fall back)**. Esta característica permite que, cuando empeoren las condiciones de difusión de la señal radioeléctrica, el sistema pueda bajar la velocidad de transmisión para mantener la comunicación abierta.

3.2.6.5. **Selección de los ordenadores autorizados (Authorised MAC address)**. Algunos puntos de acceso incluyen la facilidad adicional de incluir una lista de los ordenadores autorizados (lista de direcciones MAC) al conectarse al punto de acceso. Esta característica es interesante cuando se desea incrementar la seguridad de la red, pero no resulta práctica cuando se desea disponer de una red inalámbrica abierta a nuevos usuarios. En este caso, tener seleccionada esta opción forzaría a cambiar la configuración del punto de acceso cada vez que se desea conectar un nuevo equipo. Las direcciones MAC son unos números únicos que cada fabricante asigna a todos sus dispositivos inalámbricos. Este número identifica al dispositivo de forma inequívoca (incluidos los adaptadores de red de los ordenadores). Las direcciones MAC están formadas por 12 caracteres alfanuméricos (por ejemplo, 12-AB-56-78-90-FE).

3.2.6.6. **Emitir el nombre de red (Broadcast SSID to associate)**. Los puntos de acceso emiten generalmente su nombre de red (SSID) para permitirle a los posibles usuarios que puedan asociarse a la red con facilidad. No obstante, si se desea aumentar la seguridad de la red, puede deshabilitarse esta opción. Esto hará que sólo puedan conectarse a la red aquellos usuarios que conozcan su nombre.

3.2.6.7. **Clave de acceso (Password)**. El punto de acceso dispone de una clave para impedir el acceso a sus funciones de configuración. El fabricante configura a todos sus

equipos con una misma clave de acceso*,* pero el usuario debe cambiar esta clave para aumentar la seguridad de su equipo.

3.2.6.8. **Habilitar la red inalámbrica (Enable Wireless Networking)***.* Algunos equipos permiten que su función de punto de acceso pueda ser habilitada o deshabilitada. Esto es útil, fundamentalmente, cuando el punto de acceso dispone también de las funciones de *router* o *switch.* En algún caso podría ser interesante mantener sus funciones de *router* y deshabilitar sus funciones de punto de acceso.

3.2.7 Sobre la selección de canal

Las redes Wi-Fi disponen de 11 canales de 11 Mbps cada uno. Cada canal viene identificado por un número del 1 al 11 y, por defecto, la mayoría de los puntos de acceso ya vienen configurados con un determinado canal. No obstante, el número de canal que va a utilizar cada punto de acceso es configurable. Esto es así porque, de otra forma, los puntos de acceso vecinos que vengan configurados con el mismo canal por defecto se interferirían unos a otros.

Cuando se colocan varios puntos de acceso para cubrir un área de cobertura de una misma red, debe procurarse que el área de solapamiento sea mínima y, además, configurar diferentes canales en cada uno de ellos.

Cada número de canal Wi-Fi se corresponde con una frecuencia determinada. Los números consecutivos representan también frecuencias consecutivas. Por tanto, mientras más diferencia haya entre los números de canal, mayor diferencia habrá entre sus frecuencias. En una red con múltiples puntos de acceso es interesante tener en cuenta este detalle para intentar configurar a los puntos de acceso vecinos, no solamente con canales distintos (cosa imprescindible), sino que sus frecuencias estén lo más lejanas posible.

En teoría, con tan sólo tres frecuencias se podría cubrir cualquier área, por grande que ésta fuera, sin dejar zonas en sombra. Para ello, basta con imaginarse que cada punto de acceso dispone de un área de cobertura hexagonal (lo que también se conoce como célula). Como se dispone de 11 canales, una buena elección de canales sería el 1, 6 y

11. Esto nos dejaría una distancia de cuatro canales intermedios.

En la asignación de canales a los puntos de acceso, hay que tener en cuenta que la propagación de las señales de radio se efectúa tanto horizontal como verticalmente. Esto quiere decir que, si tenemos dos plantas de un edificio cubiertas por distintos puntos de acceso, habría que comprobar que no se producen interferencias entre plantas.

CANA	Frecuenci (MHz)	FCC (USA)	ETSI (Europa)	España	Francia	Japón
1	2412	X				X
2	2417	X				X
3	2422	X	X			X
4	2427	X	X			X
5	2432	X	X			X
6	2437	X	X			X
7	2442	X	X			X
8	2447	X	X			X
9	2452	X	X			X
10	2457	X	X	X	X	X
11	2462	X	X	X	X	X
12	2467		X		X	X
13	2472		X		X	X
14	2484					X

Tabla 3.2 Regulación de canales y frecuencias en distintos países

La teoría anterior no es del todo aplicable a países como España o Francia donde la regulación sólo permite la utilización de un número muy reducido de canales (dos en el caso de España, el 10 y 11, y cuatro en el caso de Francia, del 10 al 13). En estos casos, la única solución consiste en permitir zonas de sombra entre los puntos de acceso. El inconveniente es que, no sólo se impedirá el desplazamiento sin interrupción del servicio, sino que el número de usuarios que pueden coexistir en un mismo área será bastante menor. Estos inconvenientes desaparecerán con la nueva tecnología de 5 GHz.

3.2.8 Conexión con la red local cableada e Internet

Cuando se desea conectar un punto de acceso a una red local cableada o a Internet, los parámetros que hay que configurarle son los mismos que hay que configurarle a

cualquier ordenador que forma parte de la red cableada. Para ello, las utilidades de configuración del punto de acceso dan la opción de configurar estos parámetros.

Una posibilidad muy común es configurar el punto de acceso para que obtenga las direcciones IP de su conexión con la red local cableada o con el proveedor de acceso a Internet (ISP) de una forma automática. Para ello, el punto de acceso ofrece una opción con el nombre *Obtener una dirección IP automáticamente* o similar. Si las opciones le aparecen en inglés, el equivalente sería *Obtain an IP automatically* o similar.

Si hubiese que configurar los datos manualmente, los parámetros a configurar son los siguientes:

Dirección IP *{IP Address).* Es la dirección IP del punto de acceso como componente de la red local cableada o la que el proveedor de acceso a Internet ha facilitado.

Máscara de subred *(Subnet Mask).* Es la máscara de la red local cableada o la que facilite el proveedor de acceso a Internet. Un número de máscara muy común es el 255.255.255.0.

Puerta de enlace *(Gateway).* Es el número IP del equipo al que el punto de acceso tiene que enviarle los datos con destino a Internet o red local cableada.

Servidor DNS *(DNS Server).* Son las direcciones IP de los DNS (servidor de nombres de dominio). Este dato lo facilita el proveedor de acceso a Internet.
Interconexión de los puntos de acceso

La interconexión entre los distintos puntos de acceso que forman una red inalámbrica suele realizarse mediante la conexión de cada uno de ellos con una red local cableada (idealmente Ethernet). Lo que sí es interesante es considerar que dicha conexión supone tener que disponer de cables que permitan enlazar los puntos de acceso con el *router, switch* o *hub* de Ethernet.

3.3. Pruebas básicas

3.3.1 Comprobar el funcionamiento

Bueno, una vez instalado todo lo instalable, sólo queda comprobar si funciona. Para ello se puede empezar por probar las comunicaciones entre dos de los ordenadores. Poco a poco se pueden ir conectando uno a uno el resto de usuarios hasta comprobar que todo funciona correctamente.

Para poder ver las direcciones IP de la red instalada y para poder hacer alguna pruebas podemos habilitar la acción ejecutar. La ruta para esto es la siguiente; Inicio/Ejecutar luego en la ventana ejecutar se introduce la palabra cmd damos clic en aceptar.

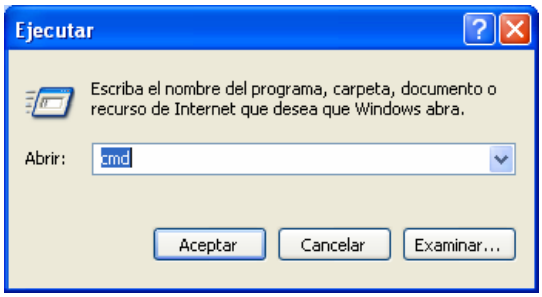


Fig. 3.15

Una vez que estamos en la ventana de comandos se introduce la palabra ***ipconfig*** con la cual vamos ha poder observar la dirección IP del terminal, mascara de red y la puerta de enlace que se encuentra en funcionamiento en ese instante.

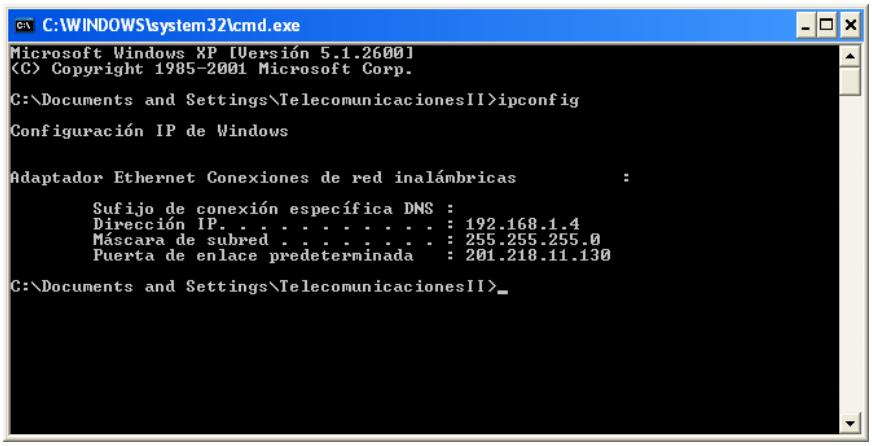


Fig. 3.16

Hacemos una prueba básica con el comando ping mas la dirección de la computadora,

con esto lo que se esta haciendo es enviar un paquete de datos hasta dicha computadora y retornarlos con esto lo que se logra es ver si existe conexión entre dichas computadoras.

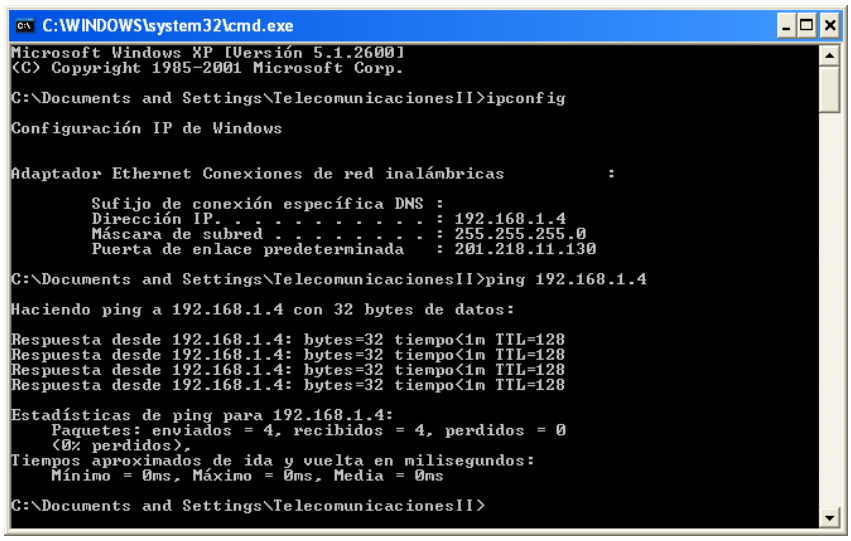


Fig. 3.17

Este tipo de pruebas se la realiza para cada una de las computadoras para ver si existe comunicación entre ellas.

En la equina inferior derecha de la barra de tareas podemos hacer clic sobre el icono de conexión de red inalámbrica para ver el status de la misma.

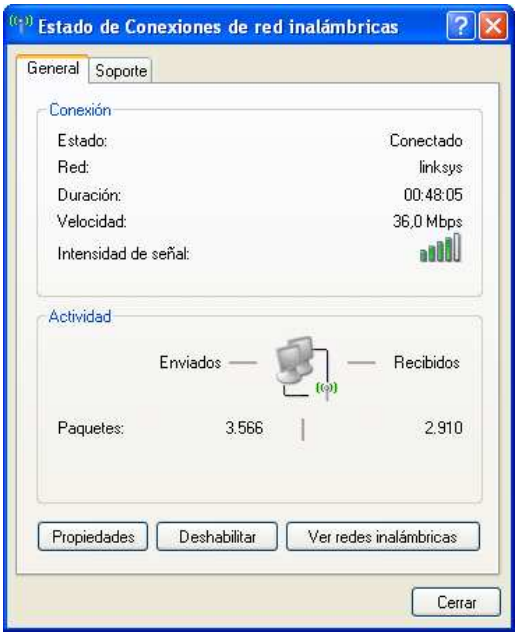


Fig. 3.18

En esta figura podemos ver que cantidad de paquetes se están enviando y recibiendo en ese instante de tiempo.

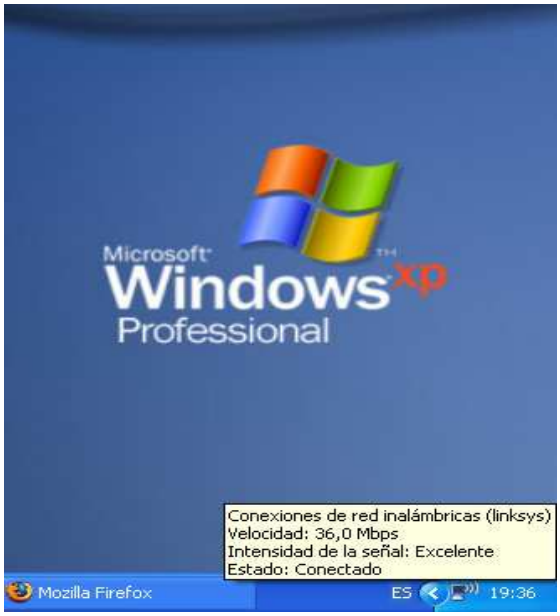


Fig. 3.19

Cuando queremos ver si existe conexión en una red únicamente acercamos el Mouse en la esquina inferior derecha en conexiones de red inalámbricas (linksys) y nos debe indicar que el estado esta conectado.

La mayoría de los adaptadores de red incluyen un *software* de utilidades que permite comprobar si el adaptador está recibiendo o no señales de otros equipos Wi-Fi (punto de acceso o adaptador), así como la calidad de dichas señales. La mejor forma de comprobar el funcionamiento de una red Wi-Fi es utilizando estas aplicaciones.

El sistema operativo Windows XP incluye aplicaciones propias tanto para la instalación de los dispositivos Wi-Fi como para su monitorización.

Si no se dispone de una de estas aplicaciones, se pueden probar las comunicaciones abriendo el *Explorador de Windows* desde uno de los ordenadores y comprobar si se pueden ver los recursos que se han compartido en los otros ordenadores. Es posible que, para hacer esto, tenga que hacer clic sobre la opción *Entorno de red, Toda la red* y sobre el grupo de trabajo que haya definido. Si el ordenador remoto tiene definido un nombre de usuario y clave de acceso para acceder a sus recursos, tendrá que introducirlos.

Recuerde que, para compartir recursos en un ordenador, se debe abrir el *Explorador*

de Windows, buscar el recurso a compartir (el archivo, la carpeta, etc.) y hacer clic sobre él con el botón derecho del ratón (el botón secundario). Aparecerá una lista de opciones donde podremos ver una con el nombre *Compartir.* Haciendo clic sobre esta opción, veremos una ventana con todas las opciones de comparación.

Si se conoce el número IP del punto de acceso, se puede comprobar que un ordenador está en comunicación con el punto de acceso abriendo un navegador de Internet (Internet Explorer, por ejemplo) e introduciendo este número como dirección. Si se obtiene cualquier respuesta distinta de *página no encontrada,* es que funciona la conexión. Incluso, todavía sería más fiable la utilización del comando *ping.* Abra una ventana del DOS desde Windows y teclee *ping* seguido del número IP del punto de acceso (por ejemplo, *ping 192.168.1.1);* si aparece una línea que empieza por ***respuesta desde****,* es que la conexión funciona. Si la línea empieza por ***Request timed out****,* es que no funciona.

3.4 GESTIÓN DE LA RED

Existen aplicaciones que permiten vigilar y gestionar el funcionamiento de la red. De hecho, existen dos tipos de aplicaciones: las que se instalan en las estaciones, aplicaciones cliente, y las que instala el administrador para vigilar la red, aplicaciones de red. La mayoría de estos programas se basan en el protocolo SNMP *{Simple Network Management Protocol,* 'Protocolo Simple de Gestión de Red'). Un ejemplo de estas aplicaciones es HP Openview.

Las aplicaciones clientes están relacionadas con la tarjeta de red inalámbrica de que se disponga. Suele ser el propio proveedor del adaptador de red el que facilita la aplicación. Estas aplicaciones facilitan información sobre la calidad de la señal, el estado de la conexión, SSID, WEP, etc. Las aplicaciones cliente permiten definir distintos perfiles para que el usuario pueda utilizar la misma tarjeta en distintas redes.

Las aplicaciones de red ofrecen herramientas tanto para el seguimiento como para la gestión de la red. La mayoría de los puntos de acceso vienen acompañados de un *software* de este tipo.

3.4.1 Medir la velocidad

La velocidad máxima a la que transmite Wi-Fi es de 54 Mbps; no obstante, esta velocidad puede ser menor dependiendo de la distancia entre emisor y receptor y de las condiciones del entorno. También hay diferencias si los equipos se encuentran en el interior de un edificio o en el exterior en espacio abierto. La transmisión en el exterior suele ser de mayor calidad porque existen menos interferencias y menos equipos intentando competir por el uso del espectro radioeléctrico.

A pesar de lo anterior, la percepción de la velocidad es algo relativo. 1 Mbps es una buena velocidad para la mayoría de las aplicaciones que tenemos hoy en día; no obstante, se percibirá como lenta si se pretende transmitir un archivo de gran tamaño o acceder al directorio de un ordenador remoto, pero en el resto de casos es una velocidad suficiente.

Si desea comprobar la velocidad a la que está haciendo uso de la red, la mayoría de las aplicaciones cliente de las tarjetas Wi-Fi permite comprobar este dato, además de otros como la relación señal/ruido, nivel de recepción de la señal recibida, etc.

3.4.2 QUÉ HACER EN CASO DE PROBLEMAS

Si, después de hacer todo el trabajo de instalación y configuración en uno de los ordenadores, no es posible ver los recursos compartidos por el resto de ordenadores, no se desespere, a veces las instalaciones requieren una segunda pasada.

Lo primero que hay que hacer es comprobar lo evidente: comprobar que todos los dispositivos están encendidos, funcionando y bien conectados. Si hubiese una antena exterior, se deberá comprobar que está conectada. Las tarjetas PCMCIA *(PC Card)* o unidades USB deben estar insertadas o conectadas al ordenador. Se pueden mover estas conexiones para comprobar que están firmemente conectadas.

3.4.3 Otras causas:

Se debe situar los ordenadores más cerca del punto de acceso evitando que haya obstáculos en medio. Una vez establecida la conexión en estas condiciones, se podrán ir separando los ordenadores hasta situarlos en la localización deseada.

Se deben comprobar las luces de las unidades Wi-Fi (adaptadores de red y puntos de acceso) para comprobar si están funcionando como indican los manuales de usuario de los equipos. Quizás esto nos de una pista de lo que está funcionando mal.

La mayoría del *hardware* (impresoras, equipos Wi-Fi, etc.) dispone de una utilidad que permite comprobar de forma local que dicho *hardware* está operativo. Si se dispone de dicha utilidad, se debe hacer la comprobación.

Apague y encienda ambos ordenadores. Algunas veces los propios registros de Windows o de los controladores no funcionan adecuadamente inmediatamente después de ser instalados y necesitan que se re arranque el ordenador.

Comprobar que el *software* de utilidad que venía con la unidad Wi-Fi está instalado y funcionando correctamente.

Desconecte y vuelva a conectar su unidad Wi-Fi. Esto hará que se reinicie esta unidad. A veces es necesario este tipo de reinicio aunque la unidad haya estado funcionando bien durante mucho tiempo.

Comprobar que los parámetros de la comunicación (tipo de red, SSID y canal) están configurados adecuadamente en ambos equipos. Cuando en una configuración de red se va a permitir *roaming* (desplazamiento con servicio entre puntos de acceso), las tarjetas Wi-Fi de los ordenadores deben configurarse para que adopten automáticamente los valores de configuración de SSID y canal del punto de acceso. Si fuese éste el caso, comprobar que está configurado correctamente.

Comprobar que los parámetros de seguridad están configurados en los mismos valores

en ambos equipos.
Comprobar que el nombre de un ordenador es distinto al nombre del otro y que no coinciden con el nombre del grupo de trabajo.

Comprobar que las direcciones TCP/IP son distintas en todos los ordenadores, o bien, que los ordenadores están configurados para obtener las direcciones IP de forma automática.

Comprobar que los adaptadores de red están instalados correctamente en el ordenador. Se puede comprobar esto haciendo clic con el botón derecho del ratón sobre *Mi PC,* luego sobre *Propiedades* y *Gestor de dispositivos* y comprobar que la unidad Wi-Fi se encuentra en la lista de *hardware* conectado al ordenador y que no tiene ningún signo de exclamación sobre él. El signo de exclamación indicaría que existe algún conflicto con este *hardware.* Si fuese éste el caso, desinstale la unidad (a través de *Añadir/Quitar hardware* del *Panel de Control)* e instálelo de nuevo.

Si ninguna de las comprobaciones anteriores nos ha sacado de dudas, aunque sea poco probable, lo mismo estamos ante un fallo de *hardware.* El fallo puede estar en el ordenador, el punto de acceso o en la tarjeta Wi-Fi (el adaptador de red). Por ejemplo, si otros ordenadores consiguen funcionar bien con el punto de acceso, se puede probar a intercambiar las tarjetas Wi-Fi. Si la conexión funciona con esta nueva tarjeta Wi-Fi, es posible que la tarjeta Wi-Fi anterior esté estropeada. Si la tarjeta Wi-Fi funciona bien con el nuevo ordenador, es posible que el ordenador anterior tenga algún problema. Si lo que no funciona es el punto de acceso, se puede intercambiar este equipo por otro y hacer una comprobación similar a la anterior.

A veces, lo que está estropeado no son los circuitos electrónicos de un dispositivo, sino los conectores o los cables. Esto se puede comprobar intercambiando los cables o los dispositivos. Aunque Wi-Fi sea inalámbrico, existen dispositivos que se conectan a los ordenadores o equipos de red *{switches, hubs, routers,* etc.) utilizando cables.

Si ha llegado hasta aquí sin resolver el problema, le quedan todavía las siguientes opciones:

3.4.4 Si la conexión es mala

Si se puede establecer una conexión, pero esta conexión tiene muy mala calidad, podemos hacer las siguientes comprobaciones:

Intentar enviar o recibir un archivo. Si se puede acceder a dicho archivo, pero la comunicación va extremadamente lenta (nunca se termina de completar la transmisión), comprobar las posibles fuentes de interferencias o si existe un número muy elevado de usuarios conectados en un solo punto de acceso.

Si a veces funcionan bien las comunicaciones y otras veces no, comprobar si los fallos coinciden con la circunstancia de haber muchos usuarios conectados a la red. Es posible que en esas circunstancias se tengan sobrecargados los puntos de acceso. En estos casos se pueden instalar puntos de acceso adicionales al lado del anterior o comprobar si, reposicionando el punto de acceso, se consigue mejorar la respuesta.

3.5 POR QUE EMPLEAR WI-FI

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 edifico 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 la 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, telerreunión, teleformación, retransmisión de eventos, recepción de televisión, radio, acceso a disco duro virtual, interconexión de redes, teleasistencia, teletrabajo, trabajo en grupo, etc.

Conclusiones:

- Pudimos observar que una manera fácil y conveniente de interconectarse entre dos computadoras es de manera inalámbrica con el empleo de puntos de accesos y tarjetas inalámbricas.

- Se comprobó que las redes inalámbricas alcanzan velocidades relativamente altas, siempre y cuando se encuentre dentro del área de cobertura, por tal motivo en la actualidad este tipo de redes están siendo bastante empleadas tanto por su facilidad de instalación como por los costos.

- La instalación de las redes inalámbricas es sumamente fácil y rápida, con la cual se evita el cableado cuyo trabajo es mucho más complejo y costoso.

Recomendaciones.

- Al momento de la instalación del Access point se debe tratar que exista línea de vista o que existan pocas interferencias entre el Access Point y el Terminal (laptop, PC u otros dispositivos).
- Se debe tratar de que el Access point como las tarjetas inalámbricas sean de la misma marca, aunque todo esto este normalizado se debe evitar el uso de diferentes marcas por posibles problemas futuros.
- Evitar que en el área donde se encuentra funcionando la red inalámbrica existan otras redes inalámbricas porque pueden causar interferencias entre ellas, esto puede causar una deficiente comunicación.
- Tratar de que la distancia máxima entre el Access point y el Terminal no excedan las que indica el fabricante (50 metros sin línea de vista y 100 metros con línea de vista), para evitar la perdida del enlace y disminución de la velocidad.
- Evitar el mal uso, manipulación inadecuada del los equipos para poder mantener el buen funcionamiento.

Bibliografía:

CASTRO, Antonio Ricardo, Teleinformática Aplicada, Editorial Mc Graw Hill, Vol. I

DOWNES, Kevin, Manual para solución de problemas de Interconectividad, Editorial Prentice Hall, Vol. II

Presuman Soller. Ingeniería del Software un enfoque Practico

Ruble David. Análisis y Diseño de Sistemas. Cliente – Servidor con GUI. Editorial Prentice Hall Hispanoamérica. S.A. 1997. México

SHAUGHNESSY, Tom, manual de Cisco, Editorial Mc Graw Hill

Steve McConnell. Desarrollo y Gestión de Proyectos Informáticos

TANENBAUM, Andrew, Redes de Computadoras, Editorial Prentice Hall

http://www.educar.org/educadores/iguerrero/AdmonCC Centro de Computo del Centro Universitario del Sur

www.wirelessethernet.org/certified_products.asp

http://standards.ieee.org/.

http://standards.ieee.org/getieee802/ 802.11.htm

www.ethereal.com freebase.sourceforge.net

www. ecommwireless.com

www.kismetwireless.net

www. netstumbler.com

www.sniffer.com

www. wildpackets.com

ANEXOS

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 lOBaseT. lOOBaseT 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. lOBaseT 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 Eléctrica! and Electronics Engineers, 'Instituto de Ingenieros Eléctricos y Electrónicos'). Entre estos estándares se encuentra 802.1 Ib, que es en el que se basa Wi-Fi.

ACCESO TELEFÓNICO. Establecer una comunicación vía módem utilizando una línea de red telefónica básica. También se le conoce por el término inglés dial-up.

ACTIVE X. Tecnología desarrollada por Microsoft para incluir aplicaciones en las páginas HTML.

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 Abonado Digital Asimétrica'.
Tecnología pensada para poder transmitir datos a alta velocidad a través del bucle de abonado de la Mnea 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 bits 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, 'Interfaz 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 en las páginas web.

ATENUACIÓN. Es la reducción o pérdida de potencia de la señal.

ATM. Asynchronous Transfer Mode, 'Modo de Transferencia Asincrono'. 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, vídeo, 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 más habitual de verificar la identidad es mediante un nombre de usuario y clave.

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.

BANDA 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.

BANDWIDTH. 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 unidad 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 10 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.

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.

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 Interface, '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 que se lleva a cabo por medio de la voz.

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.

CLIENTE/SERVIDOR. 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 compartición 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 on-line.

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.

CSMA/CA. Carrier Sense Múltiple Access with Collision 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 Múltiple 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.

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 Hosf. 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.

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 Ñame System, 'Sistema de Nombres de Dominio'. Este sistema es el encargado de traducir los nombres de dominio (como law.columbia.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 802.1 Ib (Wi-Fi) para transmitir datos a alta velocidad (11 Mbps).

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 Standares 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.

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 lOOBaseT y se basa en la norma IEEE 802.3u.

FHSS. Frequency Hopping Spread Spectrum, 'Espectro Expandido por Salto de Frecuencia'. Es una técnica de modulación utilizada tanto por los sistemas IEEE 802.11 como Bluetooth. Transmite datos a baja velocidad (I Mbps) por lo que en la versión 802.11b se sustituyó por el sistema DSSS para poder transmitir datos a alta velocidad (11 Mbps).

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.

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.

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 Área 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.

HOMEPNA. Home Phoneline 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.

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 ANSÍ (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 Protocot). 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. IP 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 Medecine, '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/OSI, 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 Telecommunications Union-Telecommunications Standard Sector, 'Unión Internacional de Telecomunicaciones-Sector de Normalización de Telecomunicaciones'. Antes CCITT.

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 instrucciones Java en las páginas HTML.

KBPS. Kilobits 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).

L2TP. Layer 2 TunnelingProtocol, 'Protocolo de Tunelado de Capa 2'. Es un protocolo del IETF utilizado para crear redes privadas virtuales.

LAN. Local Área Network, 'Red de Área Local'.

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.

MAC. Médium 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.

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 señales 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 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, se le llama demodulación.
MULTIMEDIA. Sistema que integra sonido, textos e imágenes (fijas o en movimiento) en un único soporte.

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

NIC. NetworkInterface 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.

OFDM. Orthogonal Frequency División Multiplexing, 'Multiplexado Ortogonal por 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 Ínterconnect, 'Interconexión de Sistemas Abiertos'. Se trata de una serie de protocolos normalizados por la Organización Internacional para la Normalización, ISO.

PAQUETE. Es cada uno de los trozos en los que un protocolo de comunicaciones divide el flujo de información para transmitirlo por la red.

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 Architecturé).

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).

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 sí.

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 sí. 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).

RED. Conjunto de ordenadores interconectados entre sí. 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).

RELACIÓN 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.

RJ11. Es el nombre que recibe el conector de los equipos telefónicos (teléfonos, fax, módem, etc.). Este conector permite utilizar hasta cuatro hilos.

RJ45. Es el nombre que recibe un conector estándar que se utiliza habitualmente en el cableado de las redes locales Ethernet lOBaseT y lOOBaseT. 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.

SERVIDOR. Se trata de un software que permite ofrecer servicios remotos a 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.

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 segundos, 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.

TRANSCEIVER. Transmiter-Receiver, 'Transmisor-Receptor'. Es un equipo de radio que

puede tanto transmitir como recibir.

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.

VAPORWARE. Software anunciado pero no disponible.

VIRUS. Es un programa que tiene la característica de autorreproducirse (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 Prívate 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).

WAN. Wide Área 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 Compability 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 asegurase 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 WECA 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 802.1 Ib.

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 Área 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 IEE 802.1 li 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.

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.