

# 8

## Unidad

# Despliegue de redes inalámbricas



### Y estudiaremos:

- Los diversos elementos de interconexión disponibles en redes inalámbricas.
- Los diferentes protocolos que utilizan las redes inalámbricas, así como la seguridad que usan para protegerse.
- Las opciones de configuración más importantes de estos dispositivos.
- La configuración con los clientes móviles.

### En esta unidad aprenderemos a:

- Diferenciar los diferentes tipos de redes inalámbricas.
- Utilizar Bluetooth dentro de redes WPAN.
- Emplear Wi-Fi dentro de redes de WLAN.
- Instalar un punto de acceso inalámbrico dentro de una red local.
- Establecer un mecanismo de seguridad para las comunicaciones inalámbricas.
- Utilizar diversos tipos de dispositivos y adaptadores inalámbricos para comprobar la cobertura.
- Montar un encaminador inalámbrico con conexión a red pública y servicios inalámbricos de red local.
- Configurar y probar el encaminador desde los ordenadores de la red local.



CEO

En el CEO dispones del documento *SMR\_SER\_08\_Historia.pdf*, que contiene una breve reseña histórica de las redes inalámbricas que se describen en la unidad.

## 1. Redes inalámbricas



### Importante

En 2016 se espera que el 80% de acceso a Internet se realice con dispositivos móviles, y solo en China habrá 800 millones de internautas móviles.

En la actualidad, cualquier ordenador o dispositivo móvil, como un smartphone o una tablet (e incluso electrodomésticos como un smartTV o una nevera), dispone de elementos de hardware que le permiten conectarse y comunicarse con otros, ya sea por cable o mediante sistemas inalámbricos. A pesar de que estos últimos son algo más caros y lentos, se han impuesto de manera paulatina gracias a la sensación de libertad que les confiere su gran movilidad. De hecho, a menudo constituyen la única solución, ya que puede resultar costoso, o incluso problemático, llevar el cable a determinadas zonas (por el coste o por prohibición de obras para el cableado si el edificio está protegido). Para estas situaciones y, en especial, aquellas en las que se deberá trabajar en diversos lugares, las redes inalámbricas son en la actualidad la mejor solución para equipos móviles y portátiles, así como PDA, tablets y smartphones.

Estas redes inalámbricas (wireless network o simplemente wireless) cada vez tienen mayor presencia y un mayor número de funciones, aplicables en ámbitos muy diversos:

- **En el hogar**, con aplicaciones domésticas que la controlan o la parte de la telefonía inalámbrica DECT o sobre VoIP, que se explicará en la Unidad 9.
- **En la empresa**, con mensáfonos de todo tipo para localizarnos o para emitir la señal de televisión (actualmente en formato digital a través de la TDT).
- **En telefonía**, con todas las tecnologías xG vistas en la Unidad 1. Por su importancia vamos a ver sus fortalezas, pero también sus debilidades (Tabla 8.1):

Ventajas	Inconvenientes
Montaje rápido al no tener que cablear toda la instalación, lo que conlleva un menor coste de mantenimiento a la larga.	Mayor coste de implantación, ya que los dispositivos emisores/receptores, como antenas, suelen ser más caros.
Facilitan la movilidad por no depender de un cable. Al mismo tiempo, contribuyen a aumentar la productividad al facilitar el trabajo en equipo desde distintos lugares.	Varía según el clima: con mal tiempo bajan las prestaciones. Por tanto, tienen menor velocidad que las tecnologías cableadas. Mayor tasa de error en la transmisión, ya que, al compartir el medio, e incluso la frecuencia de transmisión, pueden sufrirse interferencias externas entre tecnologías, como microondas.
Son más accesibles, ya que ayudan a salvar los obstáculos o barreras del entorno, e incluso suelen integrar varias tecnologías en el mismo dispositivo, permitiendo elegir su uso.	Menor seguridad al utilizar el aire como medio compartido para propagarse, por lo que los esfuerzos de seguridad son mayores para proteger adecuadamente nuestra información.

Tabla 8.1. Pros y contras de las tecnologías inalámbricas frente a las cableadas.

La tecnología inalámbrica se encuentra en todos los tipos de redes y, según el área que abarcan, las podemos agrupar en cuatro categorías.

Las dos primeras de mayor alcance (hasta miles de kilómetros) utilizan bandas de frecuencias altas. Cada gobierno las asigna bajo licencia (concesión para su explotación) a los operadores de telecomunicaciones, que pujan por ellas durante largos períodos de tiempo por grandes cantidades de dinero. Esto supone una barrera de entrada que limita su explotación solo a grandes empresas (ver Unidad 1). En este primer grupo encontramos:

- **Redes de área ancha inalámbricas (WWAN):**
  - Las tecnologías vía satélite (vSAT).
  - Todas las redes móviles GSM/EGPRS (2G), UMTS (3G), HSDPA/HSUPA (3.5G) o LTE/SAE (4G).
  - MBWA (IEEE 802.20), en fase de estudio y desarrollo.
- **Redes de área metropolitana inalámbricas (WMAN):**
  - WiMax 2 o móvil (IEEE 802.16) (ver Unidad 1).
  - MMDS/LMDS (ver Unidad 1).
  - ETSI HiperMAN & HiperAccess. Es una tecnología europea que surgió como competidora de las anteriores, pero no ha llegado a explotarse comercialmente.

Las siguientes dos categorías están englobadas dentro las bandas ISM (Industrial, Scientific and Medical), utilizados para usos industriales, científicos y médicos. Estas bandas de 2,4 GHz y 5 GHz están reservadas internacionalmente para uso no comercial de radiofrecuencia electromagnética en las áreas industrial, científica y médica. De este modo, los gobiernos no pueden explotarlas ni licenciarlas. Esto ha facilitado la expansión de este tipo de redes. En estas dos categorías encontramos:

- **Redes de área local inalámbricas (WLAN):**

- **Wi-Fi** (IEEE 802.11). Es el estándar más utilizado para la interconexión de este tipo de redes, por lo que se va a explicar en detalle en esta unidad.
- **ETSI HiperLAN2.** Es una tecnología europea que surgió como competidora de Wi-Fi. Utiliza la banda de frecuencia de 5 GHz con velocidades máximas de 54 Mbps, pero no ha conseguido una gran implantación.

- **Redes de área personal inalámbricas (WPAN):**

- **Bluetooth** (IEEE 802.15.1). Convertida en el estándar del sector, se halla en todo tipo de dispositivos de uso personal. La versión 4 puede alcanzar velocidades de transmisión de hasta 24 Mbps en condiciones óptimas.
- **HomeRF** (también conocida como Homero), más centrada en los hogares digitales, se basa en las normas de los teléfonos DECT y los teléfonos Wi-Fi para interconectar todos los dispositivos y formar una única red de voz y datos. La versión 2 puede llegar hasta velocidades de transmisión de 10 Mbps.
- **Infrarrojos** (irDA), la primera en aparecer, en 1993. Trabaja en el espectro de infrarrojos. Aunque se ha quedado estancada en los últimos años, puede llegar hasta velocidades de transmisión de 4 Mbps.
- **Zigbee** (IEEE 802.15.4), de las últimas en aparecer para cubrir un hueco en la gama baja (de coste más bajo) de estas tecnologías. Al tener una pila de protocolo básico, forma un red en malla, un factor de forma reducida, baja velocidad de datos (de hasta 250 kbps), pero sobre todo una duración muy larga de la batería, que le da una autonomía de hasta cinco años.
- **Otras tecnologías** englobadas dentro de las WPAN serían: ETSI HiperPAN, RFID, TAG y televía y UWB, entre otras.

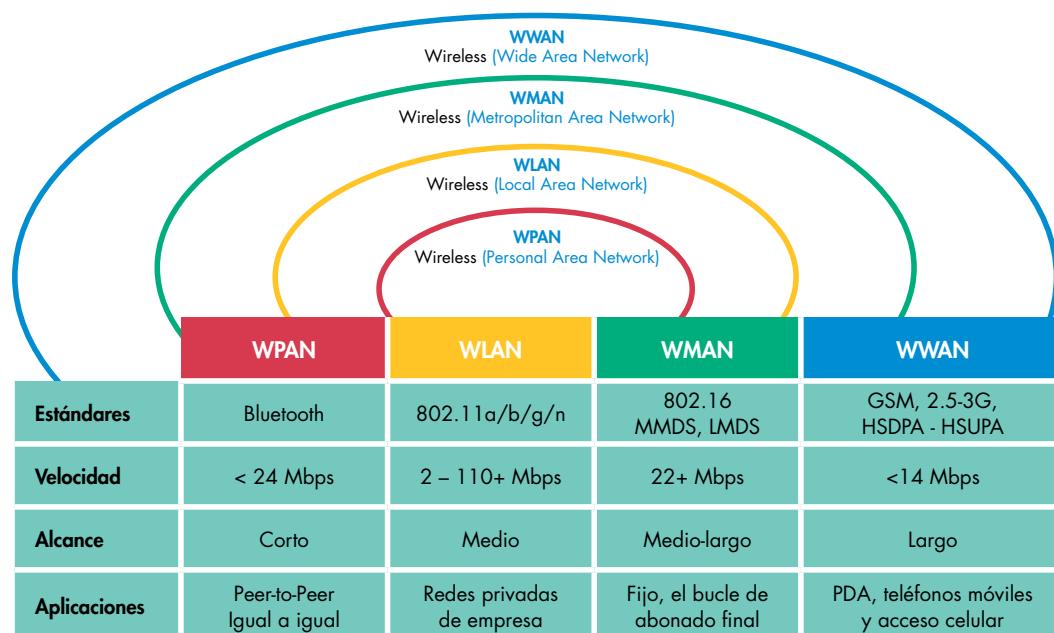


Fig. 8.1. Ámbito de actuación de las diferentes tecnologías inalámbricas.



### Importante

La tecnología DECT es un estándar abierto desarrollado por la ETSI. Sin embargo, sus especificaciones están ocultas y solo se muestran a aquellos fabricantes que se comprometen a no revelarlas. A diferencia de las tecnologías WLAN y WPAN comentadas, no utiliza la banda ISM para evitar interferencias de estas frecuencias, ya tan colapsadas. En EMEA utiliza la banda 1,88-1,9 GHz, y en Norteamérica utiliza la banda 1,92-1,93 para ser compatible con el estándar de Telecomunicaciones inalámbrica personales (PWT, Personal Wireless Telecommunications).



### Claves y consejos

Las limitaciones físicas de las redes inalámbricas están implícitas en las **leyes de la radio dinámica**:

- Un aumento de la velocidad equivale a una disminución del alcance de la transmisión.
- Un aumento de la potencia equivale a incrementar el alcance o cobertura, pero reduce la vida de la batería.
- Un aumento de la frecuencia de radio equivale a un aumento de la velocidad, pero una disminución del alcance.



### Actividades

1. Investiga sobre las otras tecnologías WPAN que no se han desarrollado en la teoría, como son ETSI HiperPAN, RFID, TAG o Televía, UWB. E incluso busca alguno que no aparezca en esta sección.
2. Haz una tabla con la versión más actual, la velocidad máxima y la autonomía de las baterías de todas las tecnologías WPAN.



### Actividades

3. Haz una lista de todos tus dispositivos Bluetooth que utilices habitualmente.
4. Busca tres dispositivos Bluetooth con los que pudieras realizar el Caso práctico 2. ¿Cuál te comprarías? ¿Por qué? ¿Ya tienes alguno tuyo en casa?
5. Investiga para qué sirve el programa BlueScanner de Aruba Labs para Windows y/o el BTScanner para GNU/Linux. Descárgatelo y prueba a utilizarlos.

## 1.1. Redes inalámbricas personales (WPAN)

Las redes de área personal inalámbricas surgieron a raíz del interés de un grupo de trabajo (IEEE 802.15) para desarrollar un sistema que permitiese comunicar directamente entre sí dispositivos móviles de uso personal a distancias cortas, de igual a igual (P2P, Peer To Peer) y sin que fuese precisa una infraestructura intermedia.

Se caracterizan por disponer de una cobertura relativamente pequeña (hasta unos 10 metros), si bien con antenas específicas se puede ampliar, ya que la potencia con que transmiten es muy baja (Tabla 8.2).

Alcance estimado	Potencia máxima de salida	Clase de Bluetooth
Hasta 1 metro	1 mW (0 dBm)	3
Hasta 10 metros	2,5 mW (4 dBm)	2
Hasta 100 metros	100 mW (20 dBm)	1

Tabla 8.2. Clases de potencia de las interfaces Bluetooth según su alcance.



### Caso práctico 1

#### Compartir un archivo a través de Bluetooth

■ Duración: ④ 5-10 min ■ Dificultad: ④ fácil

**Objetivo:** comprobar la facilidad con que se pueden compartir todo tipos de archivos en distancias cortas con la tecnología Bluetooth.

**Descripción:** a través de Bluetooth, vamos a compartir una captura de pantalla o una foto que hagamos al compañero con quien vamos a realizar la actividad en pareja. En este ejemplo vamos a utilizar un smartphone con Android 2.3 (Gingerbread) y una tablet con Android 4.0 (Ice Cream Sandwich), aunque puede servir cualquier otro dispositivo equivalente.

#### Desarrollo:

Para activar la tecnología Bluetooth en los dispositivos seguiremos estos pasos:

1. Desbloquea los terminales Android (o, según el caso, iOS, Blackberry o Windows Phone).
2. Accede a *Ajustes > Conexiones inalámbricas y redes > Bluetooth > Activar*. Esto mismo se puede realizar directamente desde el escritorio, si se dispone del widget que da acceso a *Activar/desactivar Wi-Fi, Bluetooth, GPS, Sincronización y Pantalla*.

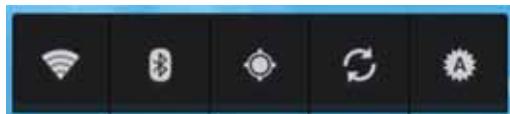


Fig. 8.2. Widget de Android 4.0 (ICS).

3. Activa la visibilidad de los dos dispositivos Bluetooth, entrando en *Ajustes* en 2.3 o haciendo clic sobre el nombre en la versión 4.0.

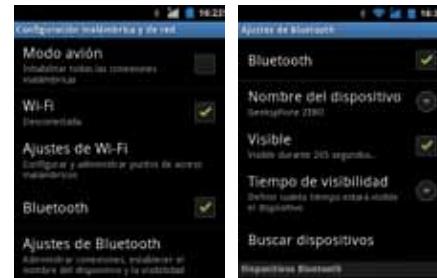


Fig. 8.3. Activación de Bluetooth desde Android 2.3 (Gingerbread).

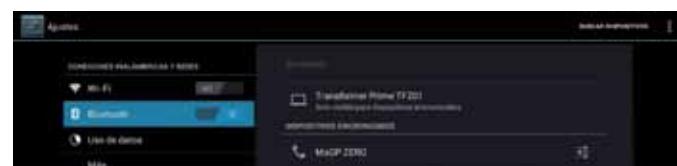


Fig. 8.4. Activación de Bluetooth de Android 4.0 (ICS).

4. Haz la foto o captura. A continuación, accede a *Galería > Elegir imagen > Compartir > Bluetooth* (Fig. 8.5) > *Elegir dispositivo a enviar*.
5. Acepta la petición de envío desde el otro dispositivo.
6. Finalizará con éxito el envío y recepción de la imagen elegida.

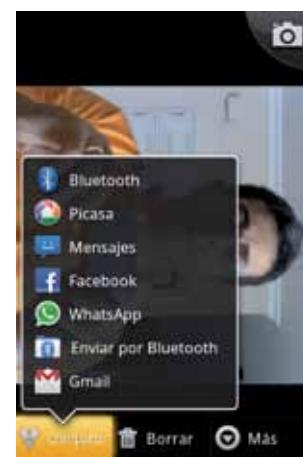


Fig. 8.5. Opciones para compartir la imagen de la Galería desde Android.



## Caso práctico 2

### Activación de Bluetooth en Windows 7

■ Duración: ⑤ 5-10 min ■ Dificultad: ☺ fácil

**Objetivo:** ver cómo organiza y gestiona Windows 7 la utilización estándar del protocolo Bluetooth según su implementación.

**Descripción:** vamos a comprobar la evolución de Windows XP a Windows 7 en cuanto a Bluetooth.

#### Desarrollo:

Partimos de la premisa de tener un ordenador, notebook o netbook con Windows 7, que no suelen llevar Bluetooth. Y al mismo tiempo, contamos con un dispositivo Bluetooth (por ejemplo, por USB) que nos permite activarlo en este sistema operativo.

1. Enciende el equipo y pincha el dispositivo USB en una ranura libre. Por plug-and-play (P&P), debería reconocerlo y utilizar los controladores implementados por Microsoft (cada fabricante suele implementar sus propios controladores para sacar el máximo partido del dispositivo Bluetooth), ya que es bastante básico el que viene de serie con Windows.
2. En el icono *Bluetooth* que habrá aparecido en la barra inferior junto al reloj, haz clic y, en el menú desplegable (Fig. 8.6), elige *Mostrar dispositivos Bluetooth*.



Fig. 8.6. Menú contextual de las opciones del ícono de Bluetooth en Windows 7.

3. Accede a *Panel de control > Hardware y sonido > Dispositivos e impresoras > Dispositivos Bluetooth*. Como es lógico, aún no tendrás ningún dispositivo enlazado.
4. Como hemos visto en el caso anterior, si tenemos activado el Bluetooth de nuestro smartphone, podremos hacer clic en *Agregar dispositivo* (Fig. 8.6 o Fig. 8.7).



Fig. 8.7. Dispositivos Bluetooth en Windows.

5. Bluetooth utiliza tres tipos de emparejamiento (Fig. 8.8): el más actual y seguro es el emparejamiento simple seguro (SSP); dependiendo de cuál sea el dispositivo a conectar, se utilizará uno u otro. Si eliges la primera opción, Windows 7 generará un valor que habrá que introducir en el dispositivo para conseguir enlazarlo con el otro equipo permanentemente de manera más segura (Fig. 8.9).

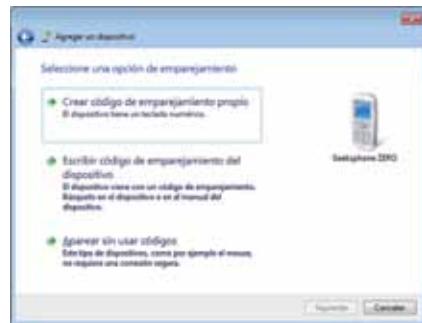


Fig. 8.8. Opciones de emparejamiento.



Fig. 8.9. Código de emparejamiento generado por el Bluetooth en Windows 7 para agregar un nuevo dispositivo.

6. Una vez emparejados ambos equipos, confiarán uno en el otro cada vez que se vuelvan a detectar. Así, se podrán enviar y recibir archivos en un sentido u otro utilizando los protocolos OBEX FTP u OBEX OPP, dependiendo de sus capacidades. Prueba a enviar la foto o captura del Caso práctico 1 a tu equipo en Windows 7.
7. Una última opción que nos permite Bluetooth en Windows 7 es crear una red de área personal (PAN) mediante clave USB para conectar ambos equipos. Ambos dispositivos Bluetooth tendrán una dirección MAC propia a la que se le asociará una dirección IP para crear esa red.
8. Desde el smartphone deberás activar el anclaje USB. Esto te permitirá compartir la conexión de datos del móvil (3G o Wi-Fi) con el equipo que tengas conectado para que puedas conectarte a Internet a través de él.
9. Prueba a navegar desde tu Windows 7 (desconecta el cable Ethernet que estés utilizando) para comprobar que, efectivamente, es otra opción a tener en cuenta en el futuro, cuando nos encontraremos sin conexión para dicho equipo.

**Web**

Las empresas que dan soporte a la tecnología Wi-Fi poseen su propio sitio web:

<http://www.wi-fi.org>.



**Fig. 8.10.** Logotipo de la alianza de empresas que dan soporte a Wi-Fi.

## 1.2. Redes Wi-Fi (WLAN)

Wi-Fi es una tecnología de redes de área local inalámbricas (WLAN) de paquetes no guiados basados en la transmisión de la señal por ondas electromagnéticas de radio en torno a los 2,4 GHz o los 5 GHz. Aunque al principio el ancho de banda era sensiblemente menor con respecto a las redes guiadas que utilizan cableado, actualmente, con la **versión n** hasta 600 Mbps (pero, sobre todo, con la **ac** a 1 Gbps) esta diferencia ya es inapreciable en instalaciones profesionales. Su implantación prolifera de forma significativa gracias a la disminución de los costes de los componentes, a los estándares en que se basan y a la producción de los mismos a gran escala. Las WLAN no surgen para sustituir a las LAN, sino más bien para complementarlas, ya que permiten tanto a los usuarios como a los dispositivos mantenerse conectados y disfrutar de plena libertad de movimientos, siempre conviviendo en armonía ambas tecnologías y pudiendo compartir entre ambas todo tipo de información. Sin embargo, no se han resuelto por completo los problemas de seguridad: los algoritmos de protección que van apareciendo se vuelven ineficaces cada vez que se aumenta el cómputo de cálculo de los equipos, tal como se verá a lo largo de esta unidad. Los primeros algoritmos de cifrado pudieron romperse con bastante facilidad, si bien de un tiempo a esta parte se han desarrollado otros mucho más fiables y robustos.

Por todo lo comentado, esta tecnología de red inalámbrica resulta imprescindible para cualquier empresa del siglo XXI. Sin ella, la Internet móvil que se agrega como herramientas de trabajo, los smartphones y tablets sería imposible.

Inconvenientes	Ventajas
Ancho de banda inferior.	Disminución de costes.
Pueden sufrir interferencias entre distintos aparatos.	Fácil instalación (no requiere cableado).
Requiere un mayor mantenimiento.	Reducción del tiempo de implantación.
Menor seguridad.	Mayor flexibilidad para ampliar o modificar la red.
Cobertura o distancia de conexión limitada.	Permite total movilidad de los clientes (roaming).

**Tabla 8.3.** Ventajas e inconvenientes de la tecnología inalámbrica frente a la cableada.

Antes de proceder al diseño de una red Wi-Fi, habrá que realizar un estudio para establecer los espacios físicos que se requieren cubrir, el tipo de cobertura que se dará y la funcionalidad deseada, así como los canales y los identificadores de red que se utilizarán. Además, conviene tener en cuenta los obstáculos, los materiales existentes, la cantidad de usuarios a los que se debe dar servicio, etc.

De cara a su **implantación**, y a la hora de adquirir el hardware Wi-Fi, hay que considerar los factores siguientes:

- **Alta disponibilidad:** la conexión inalámbrica tiene que estar en servicio en todo momento, todos los días del año, siendo un servicio 24x7.
- **Arquitectura abierta:** todos sus elementos siguen los estándares existentes, de modo que los dispositivos suministrados por fabricantes distintos funcionan correctamente entre sí, siempre que estén certificados por la asociación Wi-Fi.
- **Escalabilidad:** permite disponer de diversos puntos de acceso (PA o AP, Access Point) en una misma red para proporcionar un mayor ancho de banda. A partir de una configuración mínima de un AP, la tecnología permite su ampliación para llegar a cubrir las nuevas necesidades o requerimientos de la empresa, pudiendo ampliar tanto el espacio físico a cubrir como el ancho de banda a suministrar en cada zona.
- **Manejabilidad:** todos los elementos implicados en las redes inalámbricas han de ser de fácil configuración y manejo, como por ejemplo, oprimiendo un simple botón en cada dispositivo a conectar e introduciendo un PIN (entre enrutador/PA y/o equipo o impresora Wi-Fi o cualquier otro), como lo permite la tecnología WPS (parecida al emparejamiento en Bluetooth).

**Vocabulario**

**Itinerancia o roaming.** Posibilidad de que un usuario móvil cambie de cobertura entre diferentes estaciones base sin reconnectarse.

**WPS.** Siglas en inglés de Wi-Fi Protected Setup. Se trata de la definición de varios mecanismos para facilitar la configuración de una red WLAN segura con WPA2, con la mínima intervención del usuario.

**WPA2.** Siglas de Wi-Fi Protected Access 2. Es la tecnología más avanzada para proteger las redes Wi-Fi. Mejora algunos problemas de la primera versión.

### 1.3. Redes de área metropolitana inalámbricas (WMAN)

Las tecnologías para MAN inalámbrica (WMAN), como WiMaX o MMDS/LMDS, se tratan en detalle en la Unidad 1. Sin embargo, es interesante volver a incidir en la tecnología 802.16, con la aparición de la versión 2, más orientada a la conexión de telefonía móvil, debido a la gran expansión que está teniendo, tanto en las empresas como en ámbitos domésticos, para dar servicio de Internet mediante subcontratas promovidas por ayuntamientos o compañías operadoras de telecomunicaciones. Sin embargo, aunque se parece a la norma 802.11 utilizada en las WLAN, no son idénticas, aunque sí resultan compatibles (Tabla 8.4).

	802.11 – Wi-Fi	802.16 – WiMaX
Rango	<ul style="list-style-type: none"> <li>Optimizado para los usuarios dentro de un radio de 100 m.</li> <li>Se puede cambiar al punto de acceso la antena de mayor potencia para una mayor cobertura.</li> </ul>	<ul style="list-style-type: none"> <li>Optimizado para tamaño de celda típico de 7 a 10 km.</li> <li>Hasta 50 km de autonomía.</li> <li>Ningún problema en modo oculto.</li> </ul>
Cobertura	<ul style="list-style-type: none"> <li>Optimizada para espacios interiores.</li> </ul>	<ul style="list-style-type: none"> <li>Optimizada para espacios exteriores.</li> </ul>
Escalabilidad (ancho de banda del canal)	<ul style="list-style-type: none"> <li>De tamaño fijo, a 20 MHz.</li> </ul>	<ul style="list-style-type: none"> <li>De tamaño variable, desde un mínimo de 1,5 MHz hasta un máximo de 20 MHz.</li> <li>Dispone de la reutilización de frecuencias de uso.</li> <li>Permite la configuración de la celda para proveedores de servicios comerciales.</li> </ul>
Bit rate o tasa de velocidad	<ul style="list-style-type: none"> <li>Permite transmitir hasta un máximo de 5,5 bps/Hz (hasta 110 Mbps dentro de un canal de 20 MHz).</li> </ul>	<ul style="list-style-type: none"> <li>Posibilita transmitir hasta un máximo de 5 bps/Hz (hasta 100 Mbps dentro de un canal de 20 MHz).</li> </ul>

Tabla 8.4. Comparativa de las diferencias entre las normas 802.11 y la 802.16.

### 1.4. Redes de área ancha inalámbricas (WWAN)

Las tecnologías para WAN inalámbrica (WWAN) vistas también con más detalle en la primera unidad de este libro, como GSM/EGPRS, UMTS, HSPA+ o LTE/SAE, constituyen otra opción a la hora de realizar despliegues de redes inalámbricas entre dos puntos muy distantes que sobrepasan los límites físicos de las anteriores, si bien siempre resultará más económico emplear WPAN, WLAN o WMAN, que emplean bandas de frecuencias libres sin costes para su utilización. No hay que olvidar que las licencias para telefonía móvil son limitadas, y el gobierno de cada país las cede a través de concesiones a operadores de telecomunicaciones para que realicen una explotación comercial de las mismas. En España, las empresas que disponen de estas licencias para su explotación son los denominados **operadores móviles** (OM): Movistar, Vodafone, Yoigo y Orange. También se puede contratar este servicio a través de operadores móviles virtuales (OMV), que utilizan la infraestructura de las anteriores, ya que no tienen permiso para instalar antenas propias, teniendo que subcontratarlas a los OM.

Por último, existen unos servicios de **geoposicionamiento**, denominados genéricamente «sistemas globales de navegación por satélite» (GNSS), como el norteamericano GPS, y en un futuro cercano el Galileo de la Unión Europea. Estos sistemas permiten diversos usos civiles y militares. Así, marca la posición donde se realiza un fotografía o se emplea para navegadores de posición de aviones, barcos y vehículos terrestres.



#### Vocabulario

**Bit rate.** Tasa de velocidad binaria, que indica la velocidad a la que se transmiten los bits vía radio o cable.

**Calidad del servicio (QoS).** Son tecnologías orientadas a trabajos en tiempo real, como la transmisión de voz (VoIP) o vídeo, que permiten disponer de los recursos necesarios para garantizar la transmisión de esa información en un tiempo dado.



#### Actividades

6. Compara los costes de un servicio de telefonía móvil para crear una WWAN entre dos delegaciones de una empresa situadas en el mismo país, pero tan distantes que las demás tecnologías no sean válidas.

7. Investiga sobre cuál es el coste de la licencia que pagan los operadores móviles a los gobiernos para poder hacer uso de estas bandas de frecuencia de la telefonía móvil.

8. Profundiza un poco más sobre los sistemas de satélites de geoposicionamiento mencionados. ¿Cuándo empezaran a funcionar? ¿Cuántos satélites hacen falta para que el sistema funcione en todo el planeta? ¿Qué otros usos se les puede dar?

9. Ayudándote del documento adjunto *SMR\_SER\_08\_Canales\_por\_Paises.pdf*, averigua qué canales puedes utilizar tu país. ¿Cuáles son los que más usas en tu casa y en el instituto? Compáralos con los que han anotado tus compañeros.

## 2. Estándares de conexión



CEO

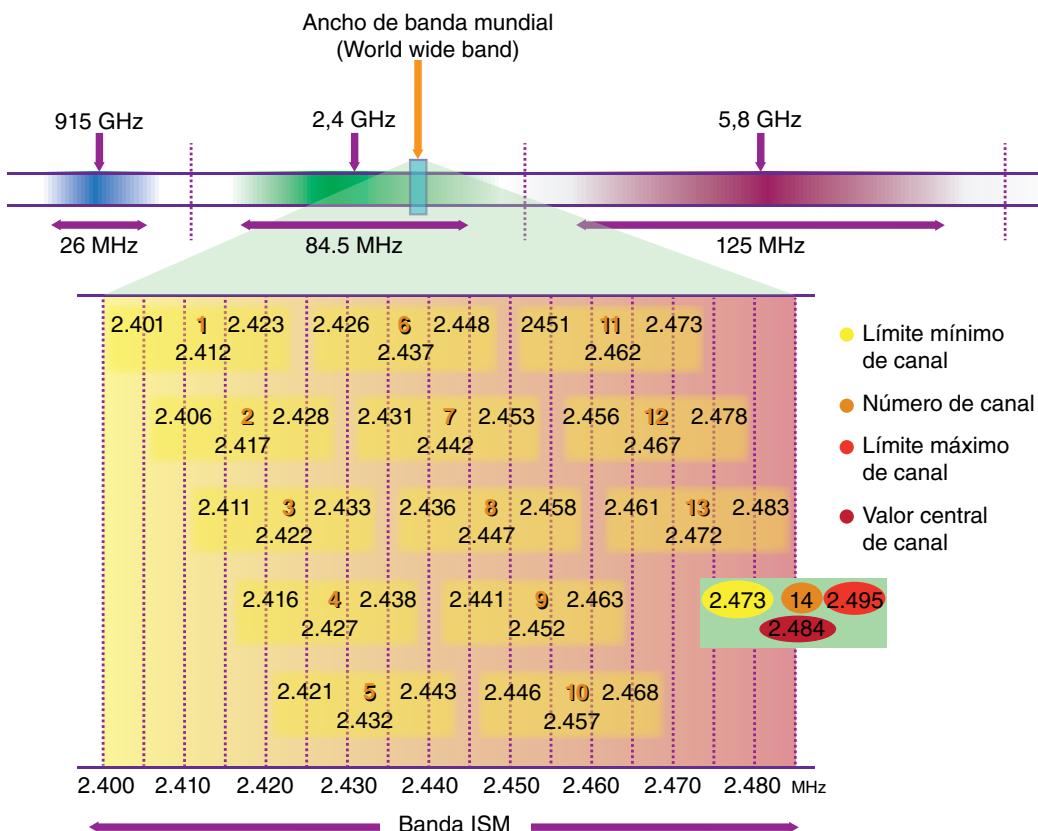
En el CEO se ha incluido el documento *SMR\_SER\_08\_Canales\_por\_Paises.pdf*, que contiene una tabla con los canales que pueden utilizarse en diversos países.

En el CEO también encontrarás el documento *SMR\_SER\_08\_Estandares\_Wi-Fi.pdf*, que incluye una tabla con todos los estándares publicados sobre la norma 802.11.



**Fig. 8.12.** Sello de certificación para un producto que soporta el estándar Wi-Fi.

La organización de las tecnologías WLAN con soporte Wi-Fi que ha llevado a la estandarización de los diferentes grupos de trabajo ha sido la IEEE, aunque no es la única que los respalda. De hecho, se ha desarrollado a partir de los dos rangos de frecuencias libres ISM: 2,4 GHz y 5 GHz.



**Fig. 8.11.** Esquema de canales disponibles para la banda de frecuencias ISM de 2,4 GHz.

Aunque los primeros sistemas, propuestos en 1997, funcionaban con velocidades de transmisión de 1 o 2 Mbps, a partir de 2013 empezarán a estar disponibles para ser comercializados los primeros que soporten la versión **ac** de hasta 1 Gbps (Tabla 8.5).

Estándar IEEE	Especificaciones WLAN
802.11a	De 54 Mbps en la banda de 5 GHz (no utilizada en Europa).
802.11b	De hasta 11 Mbps en la banda de 2,4 GHz.
802.11g	De hasta 54 Mbps en la banda de 2,4 GHz.
802.11n	De hasta 600 Mbps en la banda de 2,4 GHz y 5 GHz.
802.11ac	De hasta 1 Gbps en la banda de 5 GHz.

**Tabla 8.5.** Relación de estándares publicados con el estándar IEEE 802.11 para Wi-Fi.

También hay que comentar que no todas ellas son compatibles. La versión 802.11a solo se entiende con la 802.11n y la 802.11ac, ya que todas ellas trabajan en la frecuencia de los 5 GHz, mientras que todas las demás también son compatibles, pero solo en la banda de los 2,4 GHz.



**Fig. 8.13.** Logotipo con todas las versiones soportadas por Wi-Fi.



### Caso práctico 3

#### Activar el dispositivo Wi-Fi integrado de tu smartphone

■ Duración: ④ 15 min ■ Dificultad: ② fácil

**Objetivo:** instalar herramientas útiles para detectar la calidad de la señal Wi-Fi en nuestro teléfono móvil.

**Descripción:** vamos a activar el Wi-Fi de nuestro smartphone e instalar apps que nos ayuden a informarnos mejor de la señal que recibimos de las diferentes redes inalámbricas.

#### Desarrollo:

##### Activación del interfaz Wi-Fi

1. Desbloquea los terminales Android (iOS, Blackberry, Windows Phone).
2. Accede a Ajustes > Conexiones inalámbricas y redes > Wi-Fi > Activar (Figs. 8.2 y 8.3 del Caso práctico 1). Esto mismo se puede realizar directamente desde el escritorio si se dispone del widget que da acceso a activar y desactivar Wi-Fi, Bluetooth, GPS, sincronización y pantalla (Fig. 8.4).
3. En caso de no tener ninguna red guardada, tendremos que entrar en la opción de ajustes de Wi-Fi, elegir una de las redes Wi-Fi que nuestra estación detecte (si no aparece ninguna, pero conocemos los datos de alguna, la podemos añadir manualmente). En caso de no haber accedido nunca a ninguna red, si no está abierta, seguramente nos pedirá una clave que deberemos conocer para poder acceder.

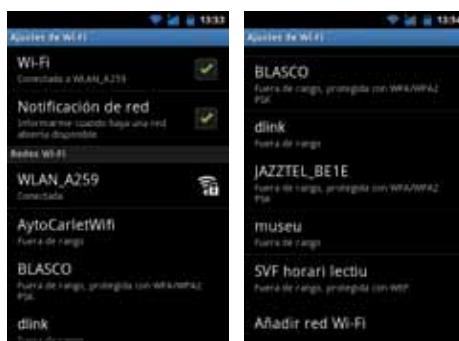


Fig. 8.14. Ajustes WiFi en Android 2.3.

#### Instalación de apps relacionadas con la interfaz Wi-Fi

1. Accede al Market de aplicaciones (en el caso de Android es Google Play).
2. Busca e instala las apps llamadas inSSIDer, Wifi Analyzer o WiFi Finder.
3. Abre inSSIDer y observa las tres opciones de Networks, 2,4 GHz y 5 GHz.
4. Abre Wifi Analyzer y comprueba las cinco opciones de gráfico de canales, gráfico de tiempo, puntuación de canales, lista de AP y medidor de señal (Fig. 8.15).



Fig. 8.15. Información de WiFi.

5. Abre WiFi Finder y observa las opciones de que dispone (Fig. 8.16). Finalmente, con toda la información obtenida podemos decidir ajustar y mejorar nuestro punto de acceso (sobre todo, el canal a utilizar).



Fig. 8.16. Información de WiFi.

A

**Vocabulario**

**Onda electromagnética.** Perturbación en el campo eléctrico y magnético que se desplaza en el espacio.

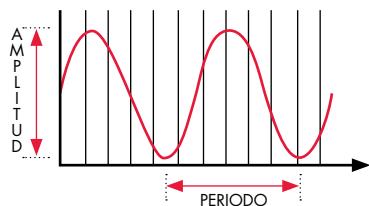


Fig. 8.17. Forma de una onda electromagnética. Esta depende de la amplitud y la frecuencia, que es la inversa del periodo.

$$F = 1/P \text{ o } P = 1/F$$

**Importante**

Si los fabricantes expresan la ganancia (potencia) de sus antenas en dBi, para obtener el dBd hay que aplicar esta fórmula aproximada:

$$G_{\text{dBd}} = G_{\text{dBi}} - 2,15$$

Consulta esta página para realizar cálculos sobre antenas y distancias:

[http://www.zero13wireless.net/wireless/calculos/webcalculo/distancia\\_antenas.html](http://www.zero13wireless.net/wireless/calculos/webcalculo/distancia_antenas.html).

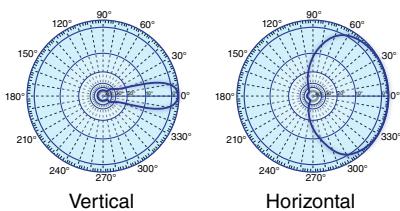


Fig. 8.20. Cobertura de las ondas electromagnéticas en una antena direccional.

## 3. Elementos inalámbricos

Tal como se hizo con los elementos de interconexión para intranets cableadas, es necesario conocer los dispositivos que harán de conversores entre ambos medios (el inalámbrico y el cableado), ya que deben disponer de una interfaz para cada uno.

### 3.1. Antenas

Las antenas constituyen la parte fundamental de los dispositivos inalámbricos, puesto que se encargan de enviar o recibir las ondas electromagnéticas con los datos.

Según la forma de señal que cubren, pueden clasificarse en tres tipos:

- **Omnidireccionales** (Fig. 8.18). Radian la señal en todas direcciones. En realidad, lo hacen según un diagrama en forma de toro. A medida que aumenta la ganancia de este tipo de antenas pueden lograrse conexiones a mayores distancias, si bien la potencia se concentra cada vez más en el eje horizontal.

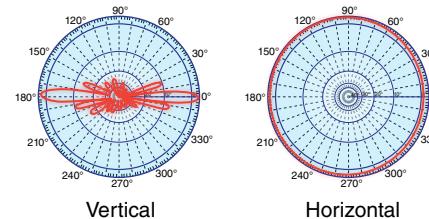


Fig. 8.18. Área de cobertura de las ondas electromagnéticas en una antena omnidireccional.

- **Direccionales o bidireccionales** (Fig. 8.19). Concentran la señal en una sola dirección (o en dos direcciones, en las bidireccionales) y cubren cierto ángulo alrededor de la dirección a la que se apunta. Cuanto mayor sea la ganancia de la antena, menor será el ángulo de radiación, con lo que resultará más difícil apuntar al otro extremo y mantener una conexión estable.

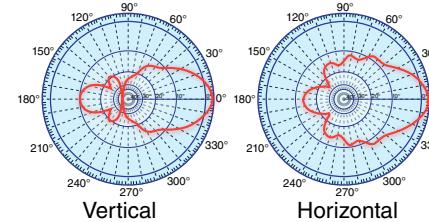


Fig. 8.19. Cobertura de las ondas electromagnéticas en una antena direccional.

- **Sectoriales** (Fig. 8.20). Es un tipo mixto, que intenta juntar lo mejor de los anteriores. Por una parte, emite una señal más amplia que una direccional, pero menor que la omnidireccional. En cuanto a la intensidad (alcance) es mayor que la omnidireccional, pero algo menor que la direccional.

Las características más importantes que deben valorarse a la hora de elegir las antenas son las siguientes:

- El **alcance o intensidad**, es decir, la distancia física en línea recta entre dos puntos.
- Las **dimensiones**, imprescindibles para saber si cabe en la ubicación donde necesita colocarse.
- Los **rangos de temperaturas** que soporta en funcionamiento, sabiendo si es apta para interior o exterior.
- El tipo de **polarización** (vertical u horizontal).
- La **frecuencia de trabajo** (para Wi-Fi de la banda 2,4 GHz oscila entre 2.400 y 2.485 MHz).
- La **ganancia o potencia**, expresada en dBi (fabricantes) o en dBd (reales).
- Los **ángulos de recepción** del ancho de banda, tanto horizontal como vertical (Horizontal or Vertical Beam Bandwidth).



### Caso práctico 4

#### Construir una antena Pringles para redes Wi-Fi

■ Duración: ④ 30 min ■ Dificultad: ② media

**Objetivo:** ampliar la ganancia (potencia) de nuestra estación Wi-Fi de manera que, en lugar de dar cobertura a unos pocos metros, podamos alcanzar cientos de metros.

**Descripción:** vamos a construir una antena casera Wi-Fi a partir de una lata de Pringles u otra de forma similar.

#### Desarrollo:

##### Obtención de los materiales necesarios

Compra todos los elementos que van a hacer falta: una lata larga de patatas Pringles (aunque valdría cualquier otra), unos centímetros de espiga de cobre de grosor de 4 mm de diámetro, un conector N-Hembra aéreo o de chasis.

##### Realizar los cálculos del diseño de la antena

1. Halla la longitud óptima. Esta sería de  $3/4 Lg$  (Tabla 8.6) o mayor. Esto dependerá de la altura (diámetro) de la lata o bote (en nuestro caso, una Pringles larga).
2. La espiga central del conector N-Hembra se prolongará con cobre de una sola fibra de unos 4 mm de diámetro y de largo  $Lo/4$ . El valor de  $Lo$  depende únicamente de la frecuencia nominal. En nuestro caso, para Wi-Fi 2,4 GHz, estos serán:  $Lo = 122 \text{ mm} @ 2,45 \text{ GHz}$ , por lo que  $Lo/4 = 31 \text{ mm}$ .

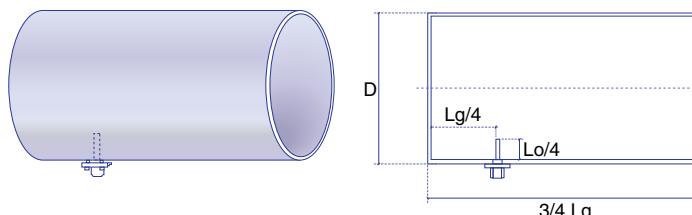


Fig. 8.21. Esquema de construcción de una antena casera.

3. El valor de  $Lg$  depende del diámetro del cilindro:

Diámetro interior del cilindro <i>D/mm</i>	Longitud onda estacionaria <i>Lg/mm</i>	Separación trasera <i>Lg/4</i>
90	202,7	51
95	186,7	47
100	175,7	44
105	167,6	42
110	161,5	40

Tabla 8.6. Valores para la construcción de la antena casera (@ 2,45 GHz).

#### Construcción de la antena

1. Suelda la espiga de cobre de longitud  $Lo/4$  sobre el conector N-Hembra.
2. Haz el agujero en la lata en la posición  $Lg/4$  (Fig 8.21 y Tabla 8.6)
3. Enrosca el conector N-Hembra a la lata.

#### Conexión de la antena

1. Ya solo queda conectar la antena casera Wi-Fi a la tarjeta de la estación o a un punto de acceso, para lo que necesitas un pigtail. Puedes optar por comprarla o por construirla tú mismo.
2. Una vez construida la antena y el pigtail, prueba si el equipo ahora consigue llegar a puntos de acceso más lejanos que antes no aparecían; los que sí estaban accesibles antes deben aparecer con mejor calidad de señal.



#### Web

Si optas por construir un pigtail, en la página siguiente se explican los pasos a realizar:

<http://www.jnewton.uphero.com/praredes/p01i/p01i.html>.



#### Vocabulario

**Pigtail.** Latiguillo de cable coaxial para radiofrecuencia que se utiliza para realizar la conexión de una antena Wi-Fi.



#### Actividades

10. Averigua de qué tipo es la antena de la tarjeta inalámbrica o del AP o enrutador Wi-Fi del grupo que estés utilizando. Si en casa tienes alguna, míralo también.
11. Busca algunos modelos comerciales de antenas direccionales y omnidireccionales. Anota sus características y precios para compararlos con los valores obtenidos por el resto de compañeros de la clase.
12. Existen modelos artesanales de antenas caseras construidos con latas de conserva o cazuelas. Busca imágenes o vídeos de alguna de ellas. ¿Te atreverías a construir alguna?

### 3.2. Adaptadores inalámbricos

Se trata de tarjetas inalámbricas integradas en todos los dispositivos inalámbricos denominadas estaciones, como son los clientes móviles, por ejemplo notebook, netbook, smartphones, tablets o ultrabooks, sin olvidar clientes fijos, como ordenadores de sobremesa, que pueden tener diferentes maneras de conectarse (PCI, PCMCIA y USB), y hasta los elementos de interconexión inalámbricos (puntos de acceso, puentes y enruteadores Wi-Fi) que los llevan incrustados.



#### ¿Sabías que...?

Las distribuciones de GNU/Linux disponen del paquete Herramientas inalámbricas para Linux (Wireless tools for Linux). Se trata de un proyecto de fuente abierta patrocinado por HP desde 1996 que ha mejorado gracias a contribuciones anónimas de diversos programadores. Las órdenes que la componen son las siguientes:

- iwconfig
- iwlist
- iwspy
- iwpriv
- ifrename

La página web oficial del proyecto en inglés es:

[http://www.hpl.hp.com/personal/Jean\\_Tourrilhes/Linux/Tools.html](http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html).



#### Caso práctico 5

##### Configuración de la tarjeta inalámbrica

■ Duración: ④ 10 min ■ Dificultad: ☺ fácil

**Objetivo:** conocer los pasos necesarios para configurar los parámetros TCP/IP. Realizaremos la configuración básica TCP/IP manual o automática por DHCP tanto en Windows como en Ubuntu GNU/Linux de forma gráfica.

**Material y herramientas:** ordenador del aula o propio con la tarjeta de red inalámbrica.

##### Desarrollo:

Nos proponemos conocer las posibilidades de las redes inalámbricas tanto en GNU/Linux como en Windows.

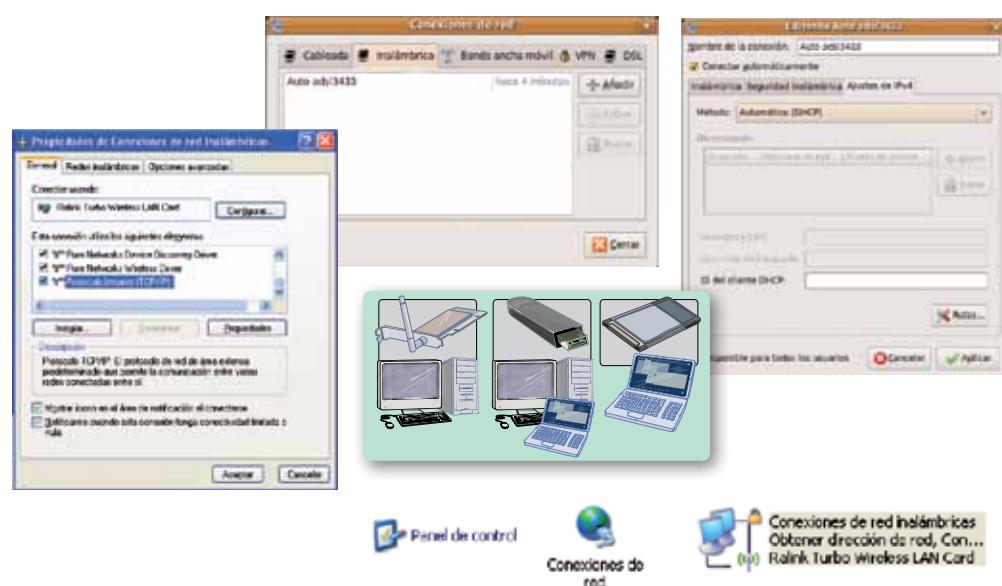
##### Activación de la interfaz inalámbrica (wlan0) en Ubuntu GNU/Linux (Fig. 8.22)

1. Accede al menú principal del sistema y activa la opción **Conexiones de red**.
2. En la pestaña *Inalámbrica* puedes añadir una nueva conexión o editar alguna.
3. Finalmente, en la pestaña *Ajuste de IP v4*, indica si asignarás los valores de manera manual o dejarás que lo haga el servidor DHCP.

##### Utilización de la interfaz inalámbrica (WLAN0) desde la consola en Ubuntu GNU/Linux

1. Comprueba con qué tarjetas contamos en nuestro equipo que sean Ethernet:  

```
raul@ubuntu:~$ lspci | grep Ethernet
```



**Fig. 8.22.** Diferentes modelos de adaptadores Wi-Fi, que varían según el perfil del dispositivo a utilizar, junto con las opciones de configuración IP v4 tanto en Windows como en GNU/Linux.

(Continúa)



## Caso práctico 5

(Continuación)

02:05.0 Ethernet controller: Realtek Semiconductor Co., Ltd. RTL-8110SC/8169SC Gigabit Ethernet (rev 10)  
02:00.0 Network controller: Realtek Semiconductor Co., Ltd. RTL8187SE Wireless LAN Controller (rev 22)

- Abre un terminal y utiliza los comandos iwconfig para cambiar o consultar sobre la interfaz inalámbrica:

```
raul@ubuntu:~$ iwconfig wlan0
wlan0 IEEE 802.11abgn ESSID:"WLAN _ 16" Mode:Managed
Frequency:2.422 GHz Access Point: 00:1A:2B:19:6D:6C
Bit Rate=54 Mb/s Tx-Power=15 dBm Retry min limit:7 RTS thr:off
Fragment thr=2352 B Power Management:off Link Quality=
100/100
Signal level:-45 dBm Noise level=-89 dBm
Rx invalid nwid: 0 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries: 0 Invalid misc: 0 Missed beacon:0
```

- Desde la consola utiliza el comando iwlist para consultar la interfaz inalámbrica:

```
raul@ubuntu:~$ iwlist wlan0 scanning
wlan0 Scan completed :
Cell 01 - Address: 00:1A:2B:19:6D:6C
      ESSID:"WLAN _ 16"
      Mode: Master
      Channel: 3
      Frequency: 2.422 GHz (Channel 3)
      Quality=92/100 Signal level:-46 dBm
      Noise level=-83 dB
      Encryption key: on
      Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s; 6 Mb/s
                  9 Mb/s; 12 Mb/s; 18 Mb/s; 24Mb/s; 36 Mb/s
                  48 Mb/s; 54 Mb/s
      Extra:tsf=00000008f04cb187
      Extra: Last beacon: 44ms ago
```

## Activación de la interfaz inalámbrica en Windows 7

- Dirígete a *Inicio > Panel de control > Redes e Internet > Centro de redes y recursos compartidos* (también puedes acceder hasta aquí escribiendo «redes» en el recuadro de *Ejecutar* desde el botón de *Inicio*).
- Haz doble clic sobre *Conexión red inalámbrica > Propiedades*.
- Selecciona *Protocolo Internet (TCP/IP)* y edita las propiedades.
- Al igual que en el primer apartado de este caso práctico, has de decidir si prefieres asignar los valores de manera manual o si dejas que se ocupe de ello el servidor DHCP.

## Utilización de la interfaz inalámbrica desde Windows 7

- Haz clic en el icono de señal Wi-Fi que hay junto al reloj.
- Elije con qué red quieras conectarte. En el ejemplo la red es JAZZTEL\_BE1E; si fuese la primera vez, habría que autenticarse con la clave correspondiente.
- Desde esta misma ventana desplegable, abre el *Centro de redes y recursos compartidos de Windows 7*.
- Windows 7 te pedirá que le indiques a qué tipo de red inalámbrica has accedido (si es una red pública, una red de trabajo o una red doméstica).
- Podrías abrir un navegador y comprobar que tenemos conexión a Internet.



## Actividades

- Consigue el manual electrónico del adaptador Wi-Fi que utilices. Averigua qué estándares de conexión soporta.
- Analiza la información que muestra la ejecución de la orden iwconfig wlan0.
- Analiza la información que muestra la ejecución de la orden iwlist wlan0 scanning.
- Estudia para qué sirven el resto de órdenes del paquete Herramientas inalámbricas para Linux (Wireless tools for Linux).



Fig. 8.23. Opciones del ícono rápido para redes Wi-Fi de Windows 7.

## A

**Vocabulario**

**Puntos de acceso públicos, Zona Wi-Fi o Hotspots.** Son espacios comunes de aeropuertos, hoteles, zonas públicas, etc., que se habilitan para permitir la conexión, mediante validación (con tarjetas identificativas, normalmente) con tecnología Wi-Fi. Esto permite al usuario la conexión, por ejemplo, a la web o al correo.

## @

**Web**

Algunas comunidades de usuarios, como Fon <http://www.fon.com/es>, comparten el ancho de banda de sus conexiones privadas con el objetivo de crear una red Wi-Fi universal y unificada.

**3.3. Puntos de acceso**

Las redes Wi-Fi tienen una topología sin organización, con uno o varios dispositivos emisores y receptores denominados «puntos de acceso» (AP), conectados a una red troncal. Se trata de un elemento clave dentro de estas redes, ya que dirige el tráfico y permite o no la circulación de los datos.

Los puntos de acceso se crearon para adaptar la señal al medio y dar cobertura, si bien al mismo tiempo realizan la función de concentrador inalámbrico, ya que transmiten las tramas recibidas a través de cable u ondas de radio. De ahí que todos dispongan al menos de una conexión RJ45.



Fig. 8.24. Diferentes modelos de puntos de acceso según sus características.



Fig. 8.25. Puentes inalámbricos en modo punto a punto.

En la actualidad se distinguen cuatro tipos de puntos de acceso:

- Para **redes de alto rendimiento**, como empresas, que requieren el mayor ancho de banda posible en cada momento.
- Para **redes de entornos de radiofrecuencia (RF) complicados**, como almacenes o zonas de producción en fábricas.
- Para **redes de interior**, muy indicados a la hora de cubrir los espacios interiores de edificios de oficinas.
- Para **redes malladas**, donde todos los elementos inalámbricos están interconectados siguiendo una topología de malla en que cualquier nodo sirve como repetidor o destino de la información.

**3.4. Puentes inalámbricos**

Se trata de los mismos puntos de acceso vistos en el apartado anterior, aunque configurados para funcionar como puentes (ver la diferencia en <http://www.support.dlink.com/emulators/dap1555>), con la idea de unir dos segmentos de red en una o más sedes de una misma organización. El administrador de la red indica en qué modo ha de funcionar de acuerdo con las necesidades de cada momento.



Fig. 8.26. Puentes inalámbricos en modo punto a múltiples puntos.

Para conseguirlo, se le puede indicar que trabaje en **modo punto a punto** (Fig. 8.25) o en **modo punto a múltiples puntos**, (Fig. 8.26). En ambos casos, solo puede existir un puente principal o raíz (root bridge) que se encargará de encaminar el tráfico, mientras que los otros tendrán la función de no-raíz (non-root bridge). Esta característica es muy importante en el modo punto a múltiples puntos, pues resulta imposible que los puentes no-raíz se comuniquen directamente. Deben dirigir los paquetes y establecer la comunicación con el puente raíz, que encauzará la información según el destino solicitado hacia su red o hacia otro puente.

### 3.5. Routers inalámbricos

En la actualidad, debido a la demanda de este tipo de dispositivos, los fabricantes de routers les han añadido un adaptador Wi-Fi para que puedan funcionar también como puntos de acceso. Basta con disponer de una conexión para acceder, mediante un navegador y la IP correspondiente, al panel de opciones y configurar la parte específica del acceso inalámbrico.

Por lo general, la configuración se lleva a cabo tras introducir el nombre de usuario y la contraseña correspondiente. A partir de ese momento, y según el fabricante (existen versiones emuladoras en sus webs), podremos obtener información del aparato y configurar todos los parámetros.

De forma genérica, dicha configuración contempla los aspectos de configuración WAN, LAN y WLAN, y convierte el router en un elemento de interconexión híbrido que realiza también las funciones de punto de acceso.



#### Caso práctico 6

##### Configuración inalámbrica del router

**Duración:** ④ 10 min    **Dificultad:** ② fácil

**Objetivo:** acceder a la configuración vía web del router inalámbrico.

##### Material y herramientas:

- Ordenador de trabajo.
- Router Wi-Fi del grupo.

**Utilidades:** navegador web, software original o emulación (<http://ui.linksys.com>).

##### Desarrollo:

1. En primer lugar, tendrás que recurrir al manual para averiguar el nombre del usuario administrador y su contraseña por defecto, así como la IP asignada.
2. Una vez dentro, dirígete al menú Wireless y, dentro del apartado Configuración básica, verás las diferentes opciones de la configuración manual. Los modelos más modernos incorporan otro modo de configuración automática denominada Protected Setup.



Fig. 8.27. Configuración automática o manual de un enrutador Linksys WTR160N vía web.

## 4. Modos de conexión

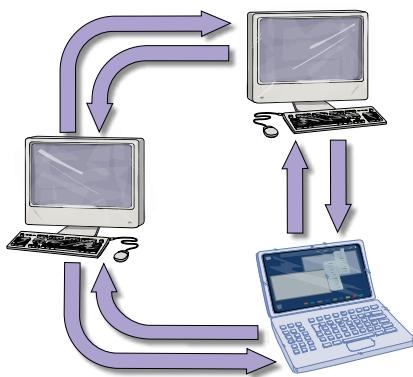


Fig. 8.28. Modo punto a punto.

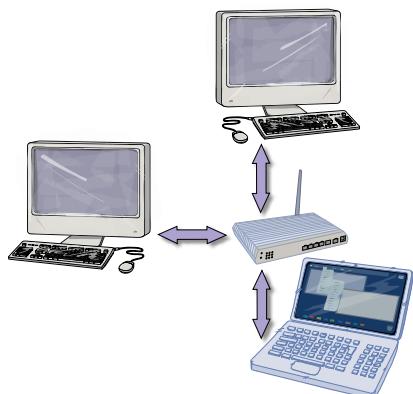


Fig. 8.29. Modo infraestructura.

Las redes inalámbricas IEEE 802.11 disponen de dos modos de conexión para trabajar (mode network), pero son incompatibles entre sí:

- **Modo punto a punto o ad hoc (IBSS):** se establece entre dos clientes que pueden comunicarse directamente con tarjetas WLAN compatibles sin necesidad de elementos de interconexión inalámbricos. Se trata de un servicio básico entre iguales semejante al uso de un cable cruzado.
- **Modo infraestructura (BSS):** es la configuración construida en torno a un punto de acceso activo, que gestiona todo el tráfico y ejerce como puerta de enlace entre la red inalámbrica, y otra cableada, que puede o no estar conectada a Internet. Se diferencia del modo anterior en que los clientes inalámbricos no pueden comunicarse directamente entre sí.

También existe la posibilidad de crear un **conjunto extendido (ESS)** uniendo dos o más BSS entre sí para extender redes sin cables, en cuyo caso uno actuará como maestro (root) y el resto como esclavos (no root). De este modo, los servicios que ofrecen cada uno de los puntos de acceso a los clientes se unen para permitir la movilidad entre diferentes zonas, si bien parte del tráfico inalámbrico será utilizado para el envío de tramas de control entre los AP.

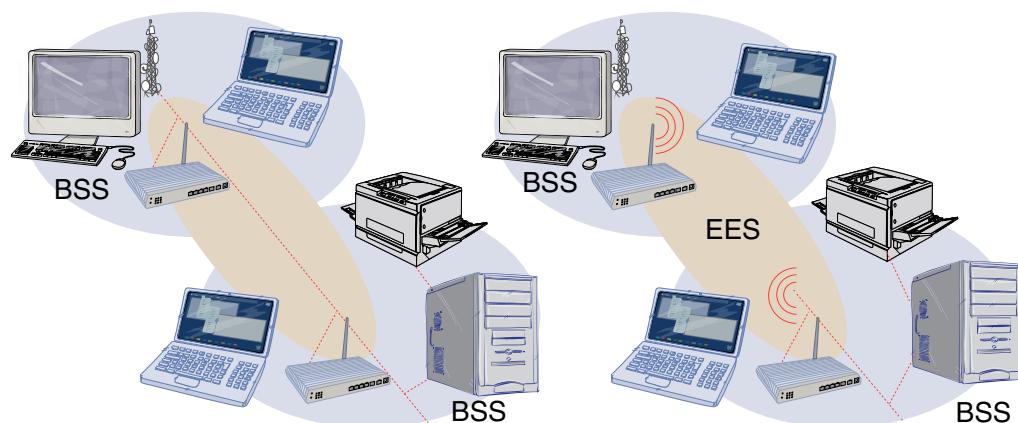


Fig. 8.30. A la izquierda, dos BSS diferentes. A la derecha, un ESS.

Existe un tercer modo, que consiste en la fusión de los dos anteriores para constituir **redes malladas** (mesh networks). En un principio, se ideó para aplicarse en países en vías de desarrollo, ya que no disponen de tantos puntos de acceso. En estos casos, un nodo puede comunicarse con cualquier otro, tal como se lleva a cabo en el modo punto a punto, pero también como repetidor o punto de acceso para propagar la información, al igual que en el modo infraestructura.

Las redes malladas se desarrollaron como parte del proyecto «un portátil por niño» (OLPC) del MIT con el fin de crear una infraestructura económica y robusta para los alumnos de escuelas de países en vías de desarrollo. Más información en la web <http://www-static.laptop.org/es/>.

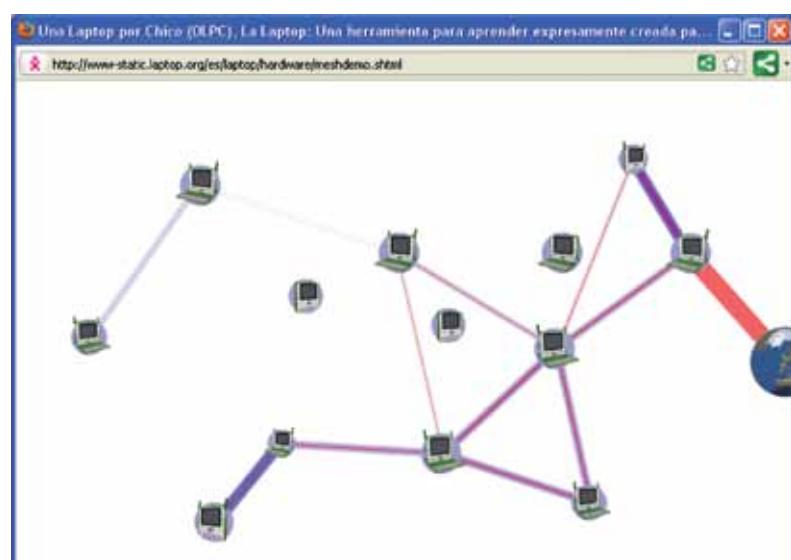


Fig. 8.31. Modo de funcionamiento de una red mallada con equipos del proyecto OLPC. Puede verse una demostración en <http://www-static.laptop.org/es/laptop/hardware/meshdemo.shtml>.

## 5. Identificadores de servicio

Todo elemento de interconexión inalámbrico siempre ha de tener al menos un **servicio de identificación (SSID)**, que consta de un valor alfanumérico de hasta 32 caracteres —una especie de nombre de red—, que debe utilizarse en todos los paquetes que se transmitan, ya que en caso de solapamiento de zonas permite diferenciar el tráfico de los clientes.

En **modo punto a punto**, más básico, recibe el nombre de BSSID, ya que está relacionado con la MAC de las propias tarjetas inalámbricas, mientras que en el **modo infraestructura** se denomina ESSID, de extendido (ver *Claves y consejos*).

El funcionamiento de un cliente activo en una WLAN es el siguiente: el dispositivo escucha o escanea la red y, cuando localiza algún punto compatible con la tarjeta, intenta conectarse de alguna de estas dos formas:

- **Activa:** el cliente envía un mensaje de conexión que contiene el SSID de la red a la que pretende unirse (puede que esté oculto como medida de seguridad en el PA que está configurado para no difundirlo). Si existe algún PA con el mismo SSID, le reenvía una respuesta de aceptación, y el cliente se asocia y autentica en la red.

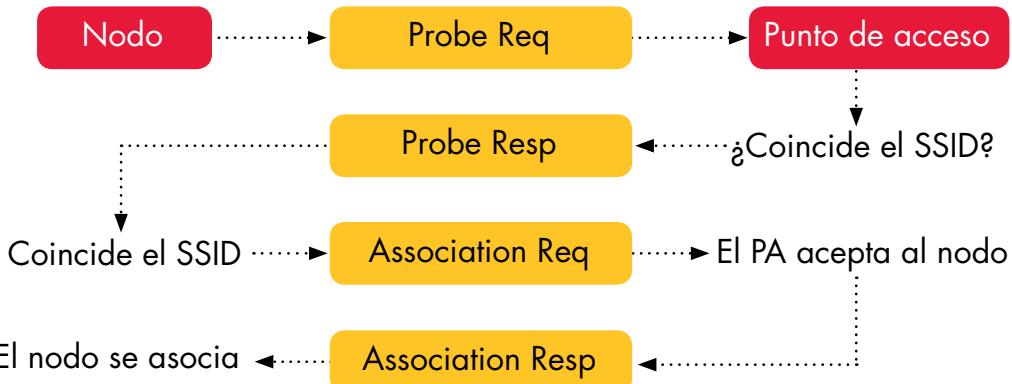


Fig. 8.32. Modo de funcionamiento del descubrimiento activo.

- **Pasiva:** el cliente se limita a escanear en busca de unas tramas de administración de balizas, llamadas «beacons», emitidas por el PA cada cierto tiempo y que contienen básicamente el SSID de la red. Una vez obtenida la baliza, el cliente intentará unirse a la red usando el SSID. Si el proceso se completa, este se asociará y autenticará.

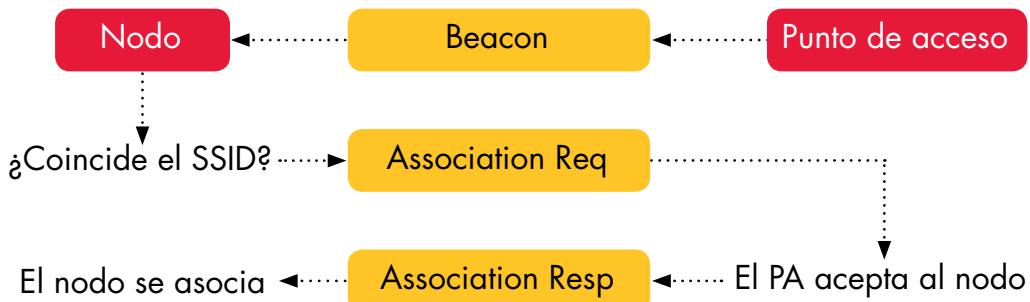


Fig. 8.33. Modo de funcionamiento del descubrimiento pasivo.

### Claves y consejos

Los identificadores son del tipo case-sensitive, es decir, distinguen entre mayúsculas y minúsculas. Por lo tanto, no será el mismo SSID «empresa» que «EMPRESA». A la hora de escribir la cadena alfanumérica, habrá que prestar mucha atención, pues de lo contrario, no se logrará la conexión.



### ¿Sabías que...?

Puedes modificar la cadena alfanumérica vía web desde el campo *Network Name (SSID)* de la configuración manual de un router Linksys WTR160N.

## 6. Seguridad en redes inalámbricas

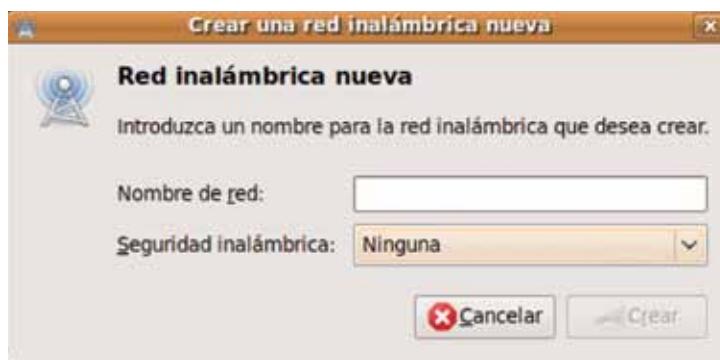


**Fig. 8.34.** Ejemplo de punto de acceso libre de zonas Wi-Fi municipales.

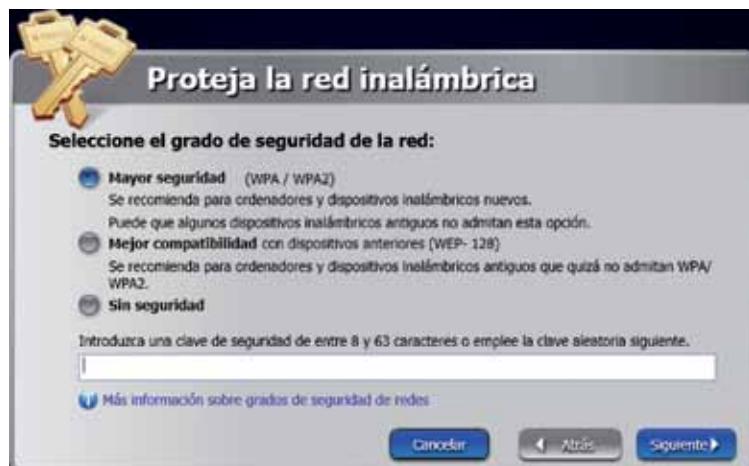
Tal como se comentó en la introducción a esta unidad, la seguridad es uno de los puntos débiles de las WLAN. Al utilizar el aire como medio de transmisión para enviar datos a través de las ondas de radio, cualquier persona puede captarlas. Los recursos empleados para proteger la red dependerán del valor de la información manejada, si bien, por lo general, deberá permitir la autenticación, confidencialidad e integridad de los datos transmitidos.

A grandes rasgos, existen tres niveles de seguridad:

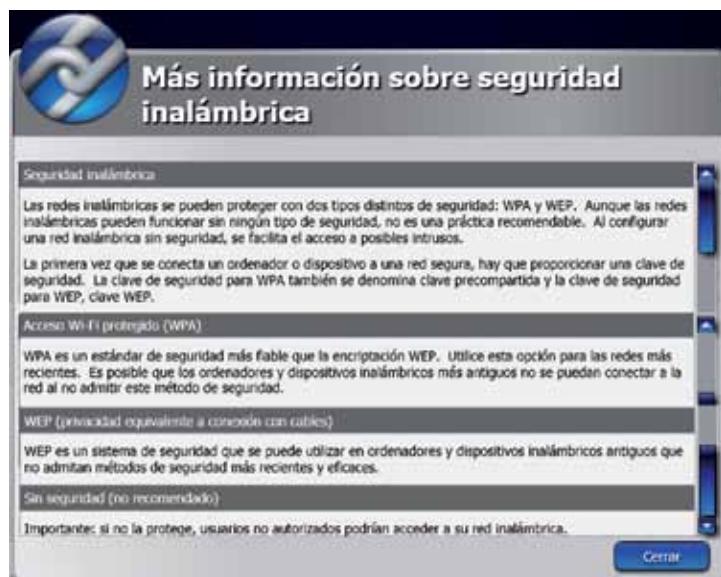
- **Cero (no recomendable):** suele aplicarse cuando se considera que la información transmitida no es importante. Se da en los **sistemas abiertos** sin seguridad que permiten un acceso WLAN gratuito a Internet.
- **Básica (configuración por defecto):** los elementos de interconexión suelen estar pre-configurados con algoritmos básicos de cifrado fáciles de romper. Se acepta solo en el caso de usuarios domésticos y/o aplicaciones no críticas. Equivaldría a una red cableada sin cifrar. Se da en los sistemas WEP y WPA personales.
- **Avanzada:** habitual en aquellos casos en que debe manejarse información muy importante. Habrá que dedicar el mayor número de recursos posibles para su protección. Se emplea en los sistemas WPA profesionales, ya que se considera inadmisible que una persona ajena a una organización determinada pueda acceder a documentación confidencial.



**Fig. 8.35.** Ventana para crear una nueva conexión inalámbrica abierta sin seguridad.



**Fig. 8.36.** Configuración de la seguridad del router WiFi desde LELA (Linksys Easy Link Advisor).



**Fig. 8.37.** Recomendaciones de Linksys en relación con el tipo de sistema de seguridad que puede seleccionarse en función del uso.

## 6.2. Privacidad equivalente a cableado (WEP)

Suele ser la opción por defecto suministrada por los fabricantes para preconfigurar los routers, ya que es compatible con todos los dispositivos y estándares Wi-Fi existentes. Utiliza solo una clave única compartida (PSK) de seguridad (Tabla 8.7) para cifrar todas las comunicaciones entre los dispositivos, que deben conocerla. De hecho, baraja los paquetes de la comunicación entre los AP y los clientes para cifrar tanto las transmisiones unicast como las multicast. Sin embargo, resulta bastante sencillo obtener una gran cantidad de paquetes y romper el cifrado mediante métodos de fuerza bruta para obtener la clave de seguridad de la WLAN. Como puede verse, la seguridad que ofrecen los sistemas WEP es muy básica.



### ¿Sabías que...?

La clave o frase de paso WEP, una vez introducida, se transmite codificada en Base64, un sistema de numeración posicional que utiliza los rangos de caracteres A-Z, a-z y 0-9.

Protocolo	Año de aparición	Algoritmo de encriptación	Clave secreta	Vector de inicialización	Integración de claves
WEP	1999	RC4	De 40 o 104 bits	24 bits	Ninguna
WPA	2001	RC4	64 bits o 128 bits	48 bits	EAP
WPA2	2005	AES	128 bits	48 bits	EAP

Tabla 8.7. Los diferentes protocolos de seguridad WLAN.

## 6.3. Acceso protegido Wi-Fi (WPA/WPA2)

Tanto WPA como WPA2 pueden considerarse variantes mejoradas de WEP que aumentan la seguridad de una clave compartida única con claves dinámicas (TKIP) y protegen las identidades de los usuarios o las máquinas mediante la autenticación con clave compartida (PSK), diversos certificados (PKI), como DNI-e, OpenID, etc., y servidores de autenticación RADIUS (802.1X), con los que utilizar diferentes versiones del Protocolo de Autenticación Extensible (EAP), como EAP-MD5, EAP-OTP, EAP-SIM, EAP-TLS (PKI), LEAP (Cisco), PEAP, etc. Asimismo, se han incorporado algunas mejoras, como el cambio del algoritmo de encriptación RC4 por AES en los sistemas WPA2 (ver Unidad 4). Aunque todas estas medidas han mejorado el grado de seguridad de las redes inalámbricas, también son vulnerables a ataques por fuerza bruta, si bien se requiere una gran potencia de cálculo para llevarlos a cabo.

Este mecanismo de seguridad tiene dos modos o variantes:

- WPA y WPA2 Personal, cuando se utiliza una clave compartida.
- WPA y WPA2 Empresarial (Enterprise), cuando hay autenticación 802.1x.

En este último, el AP ha de conocer la IP y el puerto en que está escuchando el servidor de autenticación RADIUS de la organización.

Ninguna
WEP 40/128-bit Key
Frase de paso WEP de 128 bits
LEAP
WEP dinámica (802.1x)
WPA y WPA2 personal
WPA y WPA2 enterprise

Fig. 8.38. Opciones de seguridad inalámbrica disponibles en GNU/Linux.

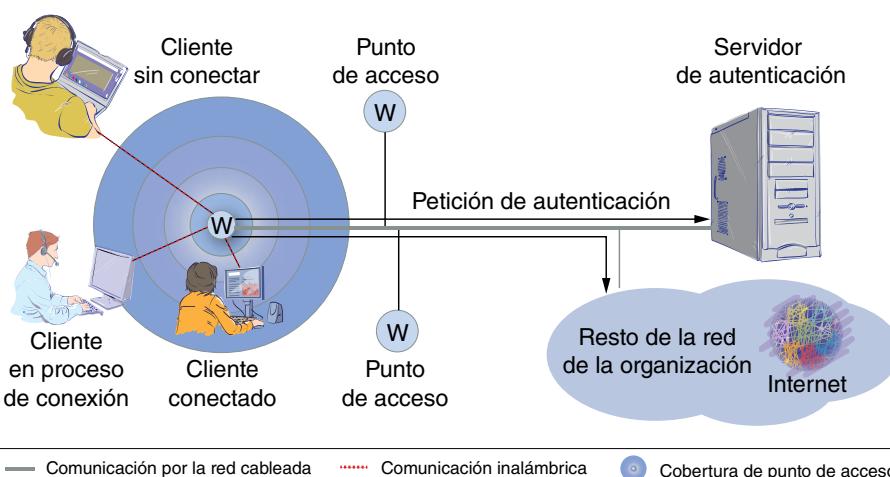


Fig. 8.39. Esquema de una WLAN, así como la cobertura ofrecida por un AP a los clientes móviles y la validación de los mismos sobre un servidor de autenticación.



## Vocabulario

### Dirección física de una interfaz de red (MAC)

Secuencia de seis pares de dígitos hexadecimales separados por dos puntos que identifica de forma única una interfaz (AA:BB:CC:DD:EE:FF).

Estos seis pares, a su vez, están agrupados en dos campos. El primero (AA: BB:CC) indica el fabricante de la tarjeta y el segundo (DD:EE:FF), un número de control de fabricación.

## 7. Direcciones MAC

El uso de las direcciones físicas de una interfaz de red (MAC) constituye una técnica sencilla y muy interesante a la hora de aumentar la seguridad de acceso a una intranet a través de conexiones inalámbricas. Basta con activar el cortafuegos básico que pueden tener los enruteadores con función de AP y aceptar o denegar las direcciones físicas MAC de la interfaz. Teniendo en cuenta que no pueden existir dos tarjetas con la misma MAC física, se pueden crear dos tipos de listas de acceso:

- Listas negras o de denegación (prevent):** comparan las MAC entrantes y, si corresponden con las consignadas, se deniega la conexión.
- Listas blancas o de aceptación (permit):** se emplean de la manera contraria.

Pese a tratarse de una solución muy robusta, cabe la posibilidad de engaño, ya que existen algunas herramientas de software que pueden cambiar este valor. No obstante, se puede detectar una suplantación de MAC.



### Caso práctico 7

#### Cambiar la MAC por software

■ Duración: ④ 20 min ■ Dificultad: ☺ media

**Objetivo:** saber qué dirección física tiene tu equipo y saber cómo cambiarla por software. Averiguar los parámetros básicos (dirección IP, máscara de red, puerta de enlace y direcciones IP de los servidores DNS) que utiliza tu ordenador.

#### Material y herramientas:

- Ordenador del aula con la tarjeta de red inalámbrica.
- Elementos de interconexión (punto de acceso o router inalámbrico) del grupo o el aula.

#### Utilidades:

- En Ubuntu, habrá que modificar el archivo /etc/network/interfaces.
- En Windows, se modificará el valor en la sección Propiedades avanzadas de la tarjeta inalámbrica.

#### Consideraciones previas:

Pese a existir un único valor físico MAC en cada tarjeta, hay herramientas de software que permiten modificarlo.

#### Desarrollo:

##### 1. En Ubuntu GNU/Linux:

En primer lugar, puedes ver el valor real de tu MAC ejecutando las órdenes ifconfig o iwconfig.

Si quieras cambiar temporalmente de MAC para esta sesión, ejecuta las siguientes órdenes parando el servicio de red, sustituyendo el valor por 00:11:22:33:44:55 y reiniciando el servicio:

```
$ sudo /etc/init.d/networking stop
$ sudo ifconfig wlan0 hw ether 00:11:22:33:44:55
$ sudo /etc/init.d/networking start
```

Si, por el contrario, quieras que se mantenga siempre este nuevo valor, edita el archivo de configuración /etc/network/interfaces y añade una entrada con el parámetro y el nuevo valor (HWADDR= 00:11:22:33:44:55).

##### 2. En Windows:

En primer lugar, puedes ver el valor real de la MAC ejecutando la orden ipconfig /all.

A continuación, ve a las opciones avanzadas de las propiedades de la tarjeta de red inalámbrica, selecciona el parámetro relacionado con la MAC (para este ejercicio, Local Administration MAC Network Address) y pon el valor 001122334455 o cualquier otro que quieras. Acepta los cambios.

Si vuelves a ejecutar la orden ipconfig/all, verás cómo se ha modificado correctamente el valor.

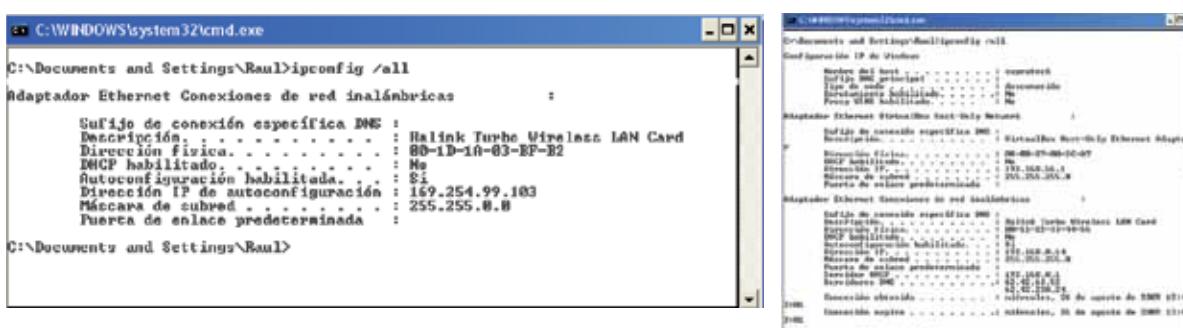


Fig. 8.40. Cambio del valor de la MAC en Windows.

## 8. Filtrado de tráfico

Al tratar las medidas de seguridad que pueden tomarse para los elementos de interconexión como los cortafuegos y los proxy-caché, conviene mencionar también el filtrado de paquetes del tráfico que circula por el router o el AP. Basta con efectuar un bloqueo sobre los servicios que no se quieran activos (POP3, FTP, etc.). Según el firmware cargado, se podrán realizar operaciones más complejas, como ajustar los días y las horas en que se permite el acceso o bloquear páginas web según el dominio o la palabra clave que contengan (Fig. 8.41).



### Actividades

17. Estudia qué medidas de seguridad Wi-Fi (Fig. 8.42) puedes aplicar y cuáles no en una instalación diseñada por ti. Justifica la respuesta con ejemplos.

Fig. 8.41. Filtrado de tráfico desde la consola de administración web del enrutador inalámbrico.

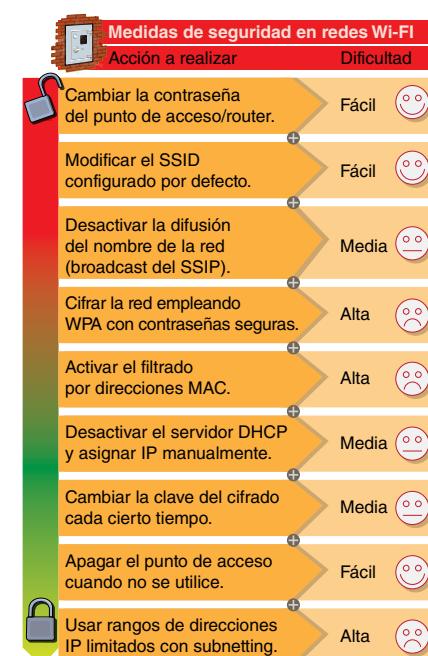
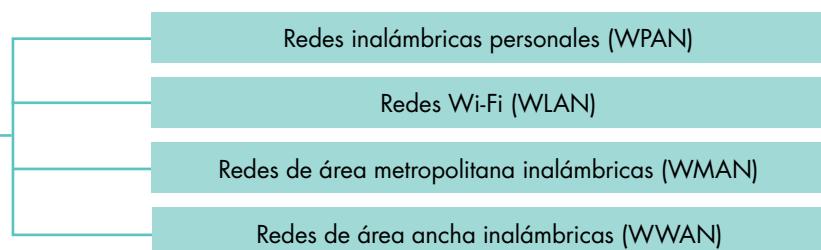


Fig. 8.42. Diferentes medidas de seguridad en redes Wi-Fi dependiendo de su dificultad.



## Síntesis

### Redes inalámbricas

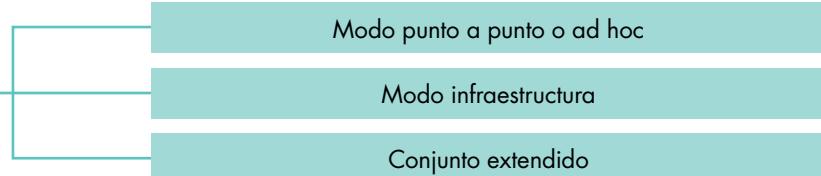


### Estándares de conexión

### Elementos inalámbricos

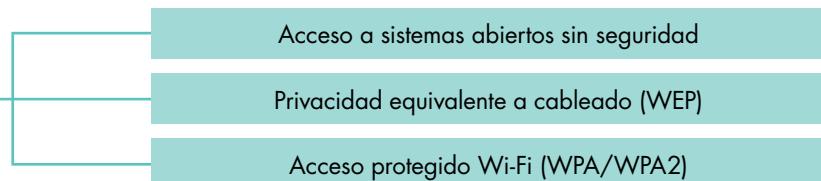


### Modos de conexión

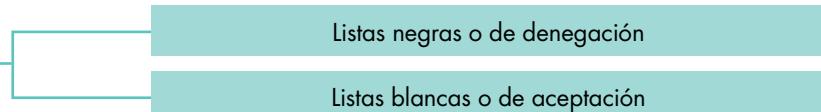


### Identificadores de servicio

### Seguridad en redes inalámbricas



### Direcciones MAC



### Filtrado de tráfico



## Test de repaso

- 1.** ¿Cuántos grupos de redes inalámbricas existen?
  - Dos: las WLAN y las WPAN.
  - Tres: las dos anteriores y las WMAN.
  - Cuatro: las tres anteriores y las WWAN.
  - Ninguna de las anteriores es cierta.
- 2.** ¿Qué tecnologías se utilizan en las WPAN?
  - WiMaX, Wi-Fi y Bluetooth.
  - irDA, HomeRF y Bluetooth.
  - 802.11 a/b/g y n.
  - Ninguna de las anteriores es cierta.
- 3.** ¿Cuál de las siguientes características no es propia de la Wi-Fi?
  - Menor seguridad.
  - Fácil instalación.
  - Mayor flexibilidad.
  - Todas las anteriores son ciertas.
- 4.** ¿Qué regula el estándar 802.11e?
  - La seguridad.
  - La calidad del servicio.
  - Los canales por países.
  - Todas las anteriores son ciertas.
- 5.** ¿Cuántos tipos de antenas existen?
  - Uno: la direccional.
  - Dos: la direccional y la omnidireccional.
  - Tres: las dos anteriores y la hegadireccional.
  - Ninguna de las anteriores es cierta.
- 6.** ¿Qué orden utilizarías para ver la configuración de la tarjeta de red inalámbrica en Linux?
  - Ipconfig.
  - Iwconfig.
  - Wificonfig.
  - Todas las anteriores son ciertas.
- 7.** ¿Qué diferencia existe entre un AP y un puente?
  - Ninguna: son lo mismo tanto por lo que respecta al hardware como al software y poseen la misma configuración.
  - El AP solo puede comunicarse con clientes, mientras que los puentes inalámbricos se comunican entre ellos.
  - Los puentes inalámbricos solo pueden comunicarse con clientes, mientras que los AP se comunican entre ellos.
  - Ninguna de las anteriores es cierta.
- 8.** ¿Cuántos puentes de tipo root pueden existir?
  - En una misma red inalámbrica, solo uno.
  - No hay limitación en el número de puentes root.
  - En conexiones multipunto, habrá más de uno.
  - Ninguna de las anteriores es cierta.
- 9.** La configuración de la parte wireless de los routers inalámbricos siempre es:
  - Automática.
  - Manual.
  - Dependiendo del modelo, pueden ser ambas.
  - Ninguna de las anteriores es cierta.
- 10.** ¿Qué modos de conexión existen?
  - Modo punto a punto o ad hoc.
  - Modo infraestructura.
  - Modo en forma de red mallada.
  - Todas las anteriores son ciertas.
- 11.** ¿Cuántos modos para buscar SSID existen?
  - Uno: el modo pasivo.
  - Dos: el modo pasivo y el activo.
  - Tres: el pasivo, el activo y el dormido.
  - Ninguna de las anteriores es cierta.
- 12.** ¿Cuántos niveles de seguridad Wi-Fi hay?
  - Tres: ninguno, básico y avanzado.
  - Dos: básico y avanzado
  - No hay ninguno.
  - Ninguna de las anteriores es cierta.
- 13.** ¿Qué protocolo de seguridad Wi-Fi es más seguro?
  - WPA-WPA2 empresarial.
  - WPA-WPA2 personal.
  - WEP.
  - Ninguna de las anteriores es cierta.
- 14.** ¿Qué otras medidas se pueden llevar a cabo para mejorar la seguridad, además de las que se han citado en el ejercicio anterior?
  - Una buena opción para mejorar la seguridad consiste en realizar un filtrado de MAC.
  - Una buena opción para mejorar la seguridad consiste en llevar a cabo un filtrado de tráfico.
  - Una buena opción para mejorar la seguridad consiste en crear redes privadas virtuales.
  - Todas las anteriores son ciertas.

Soluciones: 1 c, 2 b, 3 a, 4 b, 5 d, 6 b, 7 b, 8 a, 9 c, 10 d, 11 b, 12 a, 13 a, 14 d.



## Comprueba tu aprendizaje

**Despliega redes inalámbricas seguras justificando la configuración elegida y describiendo los procedimientos de implantación.**

1. Elabora un glosario con el resto de la clase en el que aparezcan los términos más importantes y publicadlos en la wiki o Moodle.
2. Haz una tabla comparativa entre las diferentes tecnologías WPAN comentadas. Indica las versiones y las velocidades soportadas en cada una de ellas para ver la evolución de las mismas.
3. Analiza la tabla de ventajas e inconvenientes de las redes Wi-Fi (WLAN). ¿Añadirías o eliminarías algo? Justifica la respuesta.
4. Averigua las relaciones que establecen los organismos internacionales o nacionales entre sí y con los estándares de conexión que se han comentado en la unidad. Cita las fuentes utilizadas.
5. Copia esta tabla y relaciona en tu cuaderno los estándares con sus frecuencias de trabajo.

802.11a	2,4 GHz
802.11b	
802.11g	5 GHz
802.11j	
802.11n	

6. Entre las propiedades de la onda electromagnética figuran la amplitud y el periodo.
  - a) ¿Recuerdas la fórmula física para convertir el periodo en frecuencia?
  - b) ¿Por qué crees que la banda de frecuencias de los 5 GHz tiene más canales de transmisión que la de 2,4 GHz?

Consulta el documento del CEO SMR\_SER\_08\_Canales \_por\_Paises.pdf para contestar y justificar la respuesta.

7. Explica qué diferencia existe entre las antenas direccionales y omnidireccionales.
8. Compara los precios de los tipos de adaptadores inalámbricos existentes en el mercado. Si el gerente de una empresa te pidiera que instalases este tipo de dispositivos en cien ordenadores, ¿cuál elegirías? Confeciona un presupuesto y justifica tu elección.

9. Prueba las diferentes órdenes del paquete llamado Herramientas inalámbricas para GNU/Linux y explica para qué sirve cada una. Justifica tu respuesta y da un ejemplo de uso.

10. Analiza la configuración de la intranet del aula y el instituto. Para ello, te proponemos que realices en tu cuaderno una tabla parecida a la que te mostramos como ejemplo. Copia esta tabla en tu cuaderno e indica cuántos elementos inalámbricos existen.

Elemento	Aula	Instituto
Antenas		
Adaptadores		
Puntos de acceso		
Puentes		
Routers		

11. Analiza todas las opciones de filtrado de MAC y de filtrado de tráfico de tu enrutador Wi-Fi del grupo.
12. Desde el punto de vista de la interconexión, ¿qué tipos de redes privadas virtuales existen?
13. Busca en Internet el vídeo más ilustrativo y de mayor calidad relacionado con lo que se ha estudiado en la unidad. Sube el enlace a la wiki de esta actividad y explica por qué lo has elegido.
14. Reorganiza la Figura 8.42 según el nivel de dificultad. Opina si estás de acuerdo con la dificultad asignada a cada una de las tareas.
15. Piensa qué reglas de filtrado crearías para la empresa donde te van a contratar. Teniendo en cuenta su horario laboral, explica qué finalidad persigue, según tus criterios, cada regla.
16. ¿Qué hecho histórico, de los comentados en esta unidad, consideras más importante? Razona y justifica la respuesta aportando datos de alguna fuente nueva que hayas encontrado en la red. Busca un hecho acaecido en los últimos años que esté relacionado con esta unidad y no aparezca en el documento.
17. Propón un último ejercicio para el examen justificando su enunciado y razonando su respuesta. Indica también las fuentes web consultadas o la página del libro donde se halla la solución. Consulta al profesor el formato que debe tener.