



ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 28 MARZO 2010

“REDES INALAMBRICAS: WIRELESS”

AUTORÍA M^a.TERESA GARZÓN PÉREZ
TEMÁTICA NNTT, INFORMATICA, REDES DE ORDENADORES
ETAPA ESO, FP

Resumen

Convivimos hoy en día con las redes inalámbricas (wíreles). Están en universidades, aeropuertos, bibliotecas...Raro es la zona de la ciudad por la que pasemos con un dispositivo wireless, y no encontremos alguna red inalámbrica a nuestro alcance. En este artículo trataremos de estudiar los estándares mas empleados, los dispositivos de los que se compone una red inalámbrica, las diferentes topologías y los mecanismos de seguridad con los que cuentan.

Palabras clave

Wireles.

Red de ordenadores inalámbrica.

Wi-Fi

Punto de acceso

Antena

1. CONCEPTO DE WIRELESS

Wireless significa “sin cables”, y designa a todos aquellos dispositivos que, para su funcionamiento, no requieren la conexión física entre él y otro aparato.

El término Wireless se ha asociado a las comunicaciones 802.11b, un estándar para redes de ordenadores inalámbricas que transmiten por ondas de radio: WLAN (“*Wireless Local Area Network*”, red de área local inalámbrica).



ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 N° 28 MARZO 2010

2. ESTANDARES

Las tecnologías de redes inalámbricas se basan en el estándar 802.11, creado en 1997 por el *IEEE (Institute of Electrical and Electronics Engineers)*. Desafortunadamente, el estándar 802.11 solo soportaba un ancho de banda máximo de 2 [Mbps](#), demasiado lento para la mayoría de las aplicaciones. Por esta razón salieron otras versiones de este estándar. Entre las más empleadas están las siguientes versiones del estándar 802.11:

- **802.11b**

IEEE amplió el estándar original 802.11 en Julio de 1999, creando la especificaciones del *802.11b*. 802.11b suporta un ancho de banda (velocidad) de hasta 11 Mbps, comparable a la tradicional [Ethernet](#), con 11-15 canales de emisión (depende del país).

802.11b usa la misma frecuencia de ondas de radio (2.4 [GHz](#)) que el estándar original 802.11 .

Los vendedores a menudo prefieren utilizar estas frecuencias para reducir sus costes de producción. Al no estar regulada, 802.11b puede producir interferencias con hornos microondas, teléfonos móviles, y otros aparatos que vayan a la misma frecuencia del rango de 2.4 GHz . Sin embargo, instalando la red inalámbrica 802.11b a una distancia razonable de estos dispositivos, las interferencias pueden evitarse fácilmente.

- Ventajas de 802.11b: bajo coste; el rango de señal es bueno.
- Inconvenientes de 802.11b: baja velocidad máxima; se pueden producir interferencias con algunos electrodomésticos.

- **802.11g**

En 2002 y 2003, las redes WLAN empezaron a soportar un Nuevo estándar emergente en el mercado llamado *802.11g*, que pretendía combinar lo mejor de sus predecesores 802.11a y



ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 N° 28 MARZO 2010

802.11b. 802.11g soporta un ancho de banda de hasta 54 Mbps, y usa la frecuencia de 2.4 Ghz. 802.11g es compatible con802.11b, lo que significa que los puntos de acceso 802.11g funcionan con los adaptadores de red 802.y viceversa.

- Ventajas de 802.11g: alta velocidad máxima; buen rango de señal y no es fácil de interferir.
- Inconvenientes de 802.11g: mas caro que 802.11b; puede producir interferencias con algunos electrodomésticos.

Tabla de estándares de la familia 802.11:

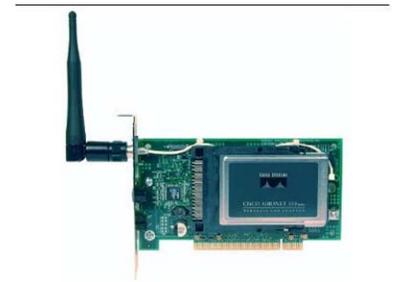
Protocolo	Año	Frecuencia de operación	Velocidad máxima
802.11	1997	2.4-2.5 GHz	2 Mbit/s
802.11a	1999	5.15-5.35/5.47-5.725/5.725-5.875 GHz	54 Mbit/s
802.11b	1999	2.4-2.5 GHz	11 Mbit/s
802.11g	2003	2.4-2.5 GHz	54 Mbit/s
802.11n	2008	2.4 GHz o 5 GHz	540 Mbit/s

Estos estándares tienen el inconveniente de que funcionan en la frecuencia 2,4 GHz, en la que también funcionan teléfonos inalámbricos, teclados y ratones inalámbricos, hornos microondas, dispositivos Bluetooth..., lo cual puede provocar interferencias.

3. DISPOSITIVOS DE UNA RED INALÁMBRICA

3.1. Tarjeta inalámbrica

Es la tarjeta de red instalada en nuestro ordenador que sirve de interfaz entre este y el resto de la red. Reciben y transmiten la información hacia su destino desde el ordenador en el que estemos trabajando a través de una pequeña antena en el caso de ordenadores de sobremesa o mediante conectores PCMCIA o USB si trabajamos con un portátil. La velocidad de transmisión/recepción de datos es variable dependiendo del fabricante y de los estándares que cumpla.



3.2. Punto de Acceso (PA o WAP: Wireless Access Point)

Un punto de acceso inalámbrico (WAP) es un dispositivo que permite a los dispositivos de comunicación inalámbrica conectarse a una red inalámbrica mediante Wi-Fi, Bluetooth u otro estándar. El WAP usualmente se conecta a una red cableada, y puede transmitir datos entre los dispositivos inalámbricos (tales como computadoras o impresoras) y dispositivos cableado de la red cableada.

El punto de acceso recibe la información de los diferentes interfaces de red bien para su centralización o bien para su encaminamiento. El punto de acceso complementa a los hubs, switches o routers, si bien los PA pueden sustituir a estos últimos pues muchos de ellos ya incorporan su funcionalidad. La velocidad de transmisión/recepción de un punto de acceso es variable, en función del fabricante y los estándares que cumpla.

Cuando una interfaz de red se conecta a un punto de acceso se ve afectada principalmente por los siguientes parámetros:

- Velocidad máxima del punto de acceso (normalmente en 802.11g será de 54 Mbps)
- Distancia al punto de acceso (a mayor distancia menor velocidad).
- Elementos intermedios entre ambos (las paredes, muros, campos magnéticos o eléctricos u otros elementos interpuestos modifican la velocidad de transmisión a la baja).
- Saturación del espectro e interferencias: cuantos mas usuarios inalámbricos haya en las cercanías mas colisiones habrá en las transmisiones por lo que la velocidad se reducirá.

Normalmente el alcance de un punto de acceso esta alrededor de los 300 metros, aunque se suele ver reducido por la infinidad de condiciones que le afectan.

Existen distintos modos en que puede configurarse un punto de acceso:

- **Modo Punto de Acceso:** es el modo normal en que trabajan los puntos de acceso y equivale aun switch en Ethernet. Tendremos que configurar el punto de acceso en nuestra red dándole una dirección IP, máscara de red, puerta de enlace y si va a actuar como servidor DHCP o no. Y habrá que configurar la red wireless que se va a crear: el SSID, el canal y el modo de seguridad (WEP o WPA). Todos los equipos que tengan el mismo SSID (y el protocolo TCP/IP bien configurado) y estén dentro de la cobertura del punto de acceso entrarán a formar parte de la

red. El punto de acceso tiene un puerto Ethernet que tendremos que conectar a nuestra red Ethernet.

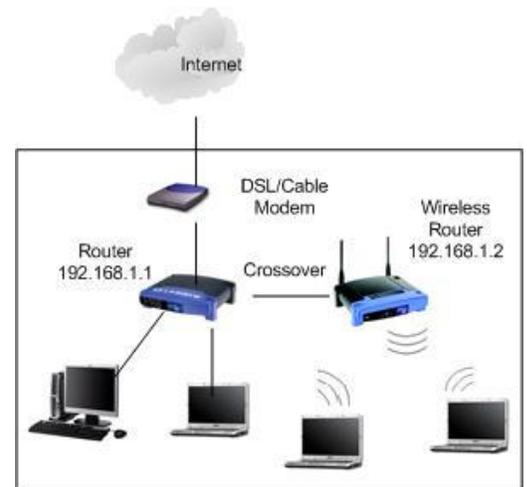
- **Modo Cliente:** actúa de forma similar a una tarjeta de red Wifi. Así tendremos que configurar el punto de acceso igual que se configura una tarjeta de red wifi: SSID, canal, modo de seguridad, TCP/IP), pero además tendremos que darle la dirección MAC del punto de acceso al que se conectará.
- **Modo Bridge:** este modo es para unir dos redes,. Los dos puntos de acceso tendrán que configurarse en modo bridge. Cada bridge puede tener una configuración diferente wifi, pero lo normal es que se ponga la misma (SSID, el canal y el modo de seguridad) para que si un ordenador pasa de la zona de cobertura de un bridge a la del otro, siga perteneciendo a la red. Cada bridge tendrá que tener la dirección MAC del otro.
- **Modo Repetidor:** si un punto de acceso (PA) no tiene suficiente cobertura para llegar con suficiente señal a una zona, se puede poner entre medias otro PA en modo repetidor del anterior PA. En el repetidor tendremos que dar la dirección MAC del que está en modo punto de acceso. También tendremos que poner el SSID, WEP y canal que tenga el PA.

3.3. Router inalámbrico (wifi)

Un router o enrutador es un dispositivo electrónico que se usa para conectar dos o más ordenadores u otros dispositivos electrónicos entre ellos y a Internet a través de señales de radio y/o cables.

Permite a varios ordenadores comunicarse entre ellos y salir a Internet al mismo tiempo. Usualmente el router inalámbrico se conecta a Internet por cable y a los ordenadores por ondas mediante una antena de radio.

Los routers domésticos o para pequeñas empresas, suelen tener un puerto de entrada (de Internet) y 4 puertos de salida, que pueden ser conectados a otros ordenadores por cable, además de los dispositivos wireless que se conectan a través de su antena por ondas.



3.4. Antenas

Una **antena** es un dispositivo diseñado con el objetivo de emitir o recibir ondas electromagnéticas hacia el espacio libre. Una antena transmisora transforma voltajes en ondas electromagnéticas, y una receptora realiza la función inversa.

La antena puede modificar enormemente la capacidad de transmisión/recepción de un punto de acceso o una tarjeta de red.

Existe una gran diversidad de tipos de antenas, dependiendo del uso a que van a ser destinadas. Se pueden clasificar en:

- **Antenas Direccionales:** envían la información a una cierta zona de cobertura, con un ángulo o dirección determinada, por lo que su alcance es mayor, sin embargo, fuera de la zona de cobertura no se recibe la señal y no se puede establecer comunicación entre los interlocutores.
- **Antenas Omnidireccionales:** envían la señal teóricamente a los 360 grados, por lo que es posible establecer comunicación independientemente del punto en el que se este. En contrapartida, su alcance es menor que el de las direccionales.



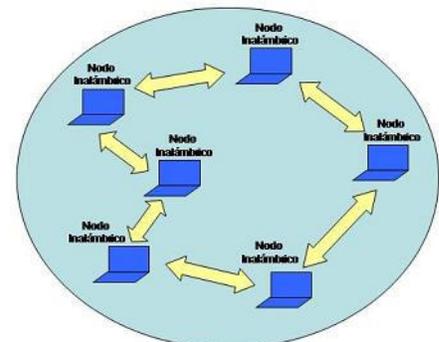
Otra clasificación de las antenas es:

- Antenas Interiores: están diseñadas para interiores de edificios, pero dan un mal resultado si se utilizan en exteriores.
- Antenas exteriores: están preparadas para dar un buen resultado en el exterior: Sirven para comunicar dos edificios, por ejemplo.

4. TOPOLOGIA

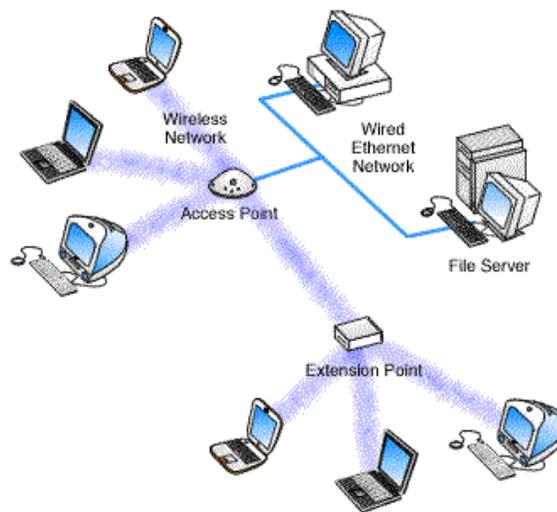
En las redes inalámbricas existen dos topologías básicas:

- **Topología Punto a Punto (Ad-Hoc):** cada dispositivo se puede comunicar con todos los demás. Cada nodo forma parte de una red *Peer to Peer* o *de igual a igual*, para lo cual sólo se necesita disponer de un SSID igual para todos los nodos y no sobrepasar un número razonable de dispositivos que hagan bajar el rendimiento. A más dispersión geográfica de cada nodo, mas dispositivos pueden



formar parte de la red, aunque algunos no lleguen a verse entre sí.

- **Topología Infraestructura:** existe un nodo central (punto de acceso Wi-Fi) que sirve de enlace para todos los demás (tarjetas de red Wi-Fi). Este nodo sirve para encaminar las tramas hacia una red convencional o hacia otras redes distintas. Para poder establecerse la comunicación, todos los nodos deben estar dentro de la zona de cobertura del punto de acceso.



5. SEGURIDAD EN REDES INALÁMBRICAS

Los mensajes de difusión de las redes inalámbricas se transmiten por ondas de radio, lo que los hace más susceptibles, frente a las redes cableadas, de ser captados con relativa facilidad.

La seguridad de la red es extremadamente importante, especialmente para las aplicaciones o programas que almacenan información valiosa.



ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 N° 28 MARZO 2010

5.1. SSID

SSID (Service Set Identifier) es un código Identificador de red inalámbrica, similar al nombre de la red pero a nivel Wi-Fi. Este código consiste en un máximo de 32 caracteres alfanuméricos. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID.

Este identificador puede ser pública (broadcast) o privada. Cuando es privada no se muestra al buscar redes inalámbricas desde mi PC. Pero para poder hacer la SSID privada tiene que tener el punto de acceso esta opción.

5.2. CANAL

La frecuencia libre que comprende la banda de 2,4 Ghz utilizada por los dispositivos wireless está subdividida en canales, que varían de acuerdo a las leyes de los diferentes países que los regulan.

El estándar IEEE define una separación mínima entre canales de 5 Mhz, por lo que, empezando de 2.412 Ghz. tendremos los siguientes canales:

- Canal 01: 2.412 Ghz
- Canal 02: 2.417 Ghz.
- Canal 03: 2.422 Ghz.
- Canal 04: 2.427 Ghz.
- Canal 05: 2.432 Ghz.
- Canal 06: 2.437 Ghz.
- Canal 07: 2.442 Ghz.
- Canal 08: 2.447 Ghz.
- Canal 09: 2.452 Ghz.
- Canal 10: 2.457 Ghz.
- Canal 11: 2.462 Ghz.
- Canal 12: 2.467 Ghz.
- Canal 13: 2.472 Ghz.
- Canal 14: 2.484 Ghz.

Cada canal necesita un ancho de banda de 22 Mhz para transmitir la información, por lo que se produce un inevitable solapamiento de varios canales contiguos. Para evitar interferencias en presencia de varios puntos de acceso cercanos, estos deberían estar en canales no solapables, que podrían ser:

- 2, 7 y 12
- 3, 8 y 13
- 4, 9 y 14
- 1, 8 y 14.



ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 N° 28 MARZO 2010

El número de canales disponibles de ser usados para dar servicio Wireless Lan según el estándar 802.11b varia entre países. Así pues en España a día de hoy se pueden utilizar hasta 13 canales los mismos que en toda la comunidad europea. Sin embargo el número de canales disponibles en USA son 11.

Si bien según **el estándar 802.11b sólo se dispone de hasta 3 canales** para trabajar simultáneamente sin solapamiento, es posible llegar a utilizar hasta 4 con un análisis de cobertura in situ de forma que la interferencia entre ellos sea pequeña.

Cuando se trabaja con 3 canales radio, los 3 canales sin solapamiento utilizados son el 1-6-11 (3 Mhz libres entre canales).

5.3. WEP

WEP son las siglas de *Wired Equivalent Privacy (Privacidad Equivalente a Cableado)*. Es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite. Fue introducido para intentar asegurar la autenticación, protección de las tramas y confidencialidad en la comunicación en los dispositivos inalámbricos. Proporciona un cifrado a nivel 2, basado en el algoritmo de cifrado RC4 que utiliza claves de 64 bits (WEP64, con 40 bits reales), de 128 bits (con 104 bits reales) o de 256 bits (WEP 256). Presentado en 1999, el sistema WEP fue pensado para proporcionar una confidencialidad comparable a la de una red tradicional cableada.

Consiste en una contraseña de unos bytes prefijados según el tipo de WEP (WEP64, WEP128 o WEP256) que encripta las tramas. El sistema WEP ralentiza la transmisión y recepción de dato ya que tiene que encriptarlos y desencriptarlos al enviar/recibir. El retardo es mayor cuanto mayor es la clave WEP (cuantos mas bits tenga).

Dentro de WEP hay varios tipos de protección:

- OSA (*Open System Authentication*): cualquier interlocutor es válido para establecer una comunicación con el punto de acceso (AP).
- SKA (*Shared Key Authentication*): en este método ambos dispositivos disponen de la misma clave de encriptación. El dispositivo punto de acceso (AP) pide a la tarjeta de red (TR) autenticarse. El AP le envía un trama al TR, y si este la devuelve correctamente codificada, le permite establecer la comunicación.

Problemas de WEP:

- Claves estáticas, fácilmente descifrables.
- Únicamente cifra las tramas de datos.
- Autentica dispositivos, no usuarios.
- ICV (Integrity Check Value) fácil de simular.



ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 N° 28 MARZO 2010

5.4. WPA

WPA son las siglas de Wi-Fi Protected Access (*Acceso protegido Wi-Fi*). WPA es un sistema para proteger las redes inalámbricas, creado para corregir las deficiencias del sistema previo [WEP](#) (*Wired Equivalent Privacy - Privacidad Equivalente a Cableado*). Los investigadores han encontrado varias debilidades en el algoritmo WEP (tales como la reutilización del vector de inicialización (IV), del cual se derivan ataques estadísticos que permiten recuperar la clave WEP, entre otros). WPA implementa la mayoría del estándar IEEE 802.11i, y fue creado como una medida intermedia para ocupar el lugar de WEP mientras 802.11i era finalizado. WPA fue creado por "The Wi-Fi Alliance" (La Alianza Wi-Fi).

WPA adopta la autenticación de usuarios mediante el uso de un servidor, donde se almacenan las credenciales y contraseñas de los usuarios de la red. Para no obligar al uso de tal servidor para el despliegue de redes, WPA permite la autenticación mediante clave compartida ([PSK], Pre-Shared Key), que de un modo similar al WEP, requiere introducir la misma clave en todos los equipos de la red.

6. CONCLUSIONES

6.1. Ventajas e inconvenientes de las redes inalámbricas

Entre las **ventajas** con las que cuenta la tecnología inalámbrica están su bajo coste, la facilidad de instalación, su movilidad y escalabilidad.

- **Movilidad:** Las redes inalámbricas pueden proveer a los usuarios de una LAN acceso a la información en tiempo real en cualquier lugar dentro de la organización. Esta movilidad implica una productividad y servicio que no son posibles con una red cableada.
- **Simplicidad y rapidez de instalación:** la instalación de una red inalámbrica es rápida y fácil, ya que elimina la necesidad de tirar cables a través de paredes y techos.
- **Flexibilidad en la instalación:** la tecnología inalámbrica permite a la red ir donde la cableada no puede ir.
- **Costo de propiedad reducido:** mientras que la inversión inicial requerida para una red inalámbrica puede ser más alta que el costo en hardware de una LAN cableada, la inversión de toda la instalación y el costo del ciclo de vida puede ser significativamente inferior. Los beneficios y costos a largo plazo son superiores en ambientes dinámicos que requieren acciones y movimientos frecuentes.



ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 N° 28 MARZO 2010

- Escalabilidad: los sistemas WLAN pueden ser configurados en una variedad de topologías para satisfacer las necesidades de las instalaciones y aplicaciones específicas. Las configuraciones son muy fáciles de cambiar y además es muy fácil la incorporación de nuevos usuarios a la red.

Los principales **inconvenientes** de las redes inalámbricas son su baja velocidad máxima y que algunos dispositivos electrodomésticos pueden provocar interferencias en la red con una banda de frecuencias no regulada.

7. BIBLIOGRAFÍA

- Carballar Falcón, J. A. (2004). *Wi-fi. Cómo Construir Una Red Inalámbrica, 2ª Edición*. Editorial Ra-ma.
- Andreu / Pellejero / Lesta. (2006). *Fundamentos y aplicaciones de seguridad en redes wlan*. Marcombo, Ediciones Técnicas.
- Gómez López, J. (2008). *Guía de campo de Wi-Fi*. Editorial Ra-ma
- Roldán Martínez, D. (2004). *Comunicaciones inalámbricas. Un enfoque aplicado*. Editorial Ra-ma

Autoría

- Nombre y Apellidos: M. TERESA GARZÓN PÉREZ
- Centro, localidad, provincia: IES ANTONIO GALA, PALMA DEL RÍO, CÓRDOBA
- E-mail: teresa.garzon.ext@juntadeandalucia.es, maitegp99@gmail.com