Wi-Fi e IEEE 802.11

Las conexiones inalámbricas de tipo Radio LAN (RLAN) encontraron estándares adecuados gracias a los trabajos de los grupos IEEE 802.11.

1. Presentación

En 1997 el grupo de trabajo 802.11 estandariza, después de varios años de trabajo, la definición de redes de tipo Wireless LAN, que se retocó en 1999. Como en el caso de 802.3, estas especificaciones cubren las capas Física y Conexión de datos del modelo OSI. Esta última está dividida en dos subcapas: *Medium Access Control* (MAC), para el acceso al soporte de transmisión, y *Logical Link Control* (LLC), para el control de la transmisión.

En la capa Física, 802.11 define tres modos de transmisión. El primero está basado en la difusión infrarroja, que finalmente no se utilizará en las implementaciones de estas especificaciones. Las otras dos tecnologías utilizan la transmisión por radio. Finalmente, una sola, denominada *Direct Sequence Spread Spectrum* (DSSS), se implementará.

Las especificaciones 802.11 interesan tanto a algunos fabricantes que en 1999 forman la asociación *Wireless Ethernet Compatibility Alliance* (WECA). Su objetivo no es solamente promover este nuevo estándar, sino también certificar dispositivos con el fin de garantizar su buen funcionamiento. El certificado *Wireless Fidelity* (Wi-Fi), patente de interoperabilidad, se otorga después de algunas pruebas. Finalmente, este organismo se rebautiza como Wi-Fi Alliance.

Después de las pruebas de compatibilidad, el fabricante del hardware puede etiquetar las cajas con el siguiente logotipo, siempre que respete los estándares exigidos.

Logo Wi-Fi

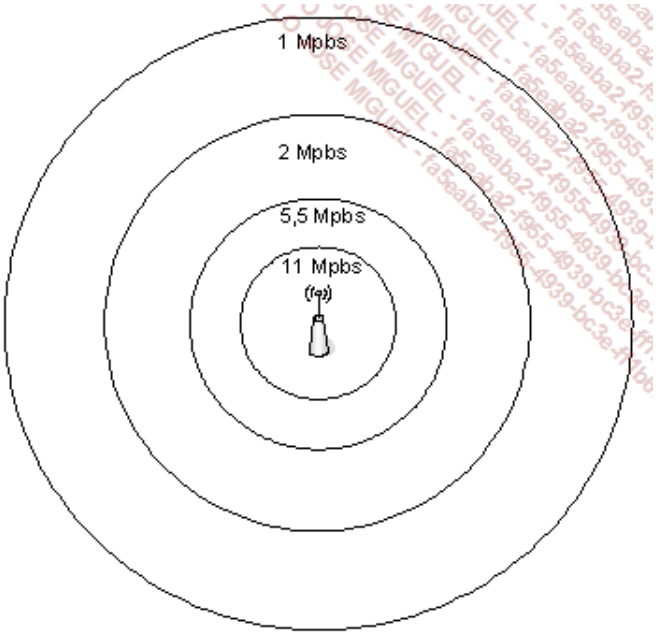
El estándar Wi-Fi permite la conectividad a distancias que superan algunas decenas de metros. La utilización de antenas permite alcanzar varios centenares de metros.

2. Normas de la capa Física

Hay muchas especificaciones que se han basado en la 802.11 original, de las cuales tres definen el uso de la capa física.

a. 802.11b

Esta norma, publicada en septiembre de 1999, aumenta la velocidad máxima de transmisión a 11 Mbps, con velocidades que pueden llegar a 5,5, 2 y 1 Mbps. La frecuencia de trabajo es de 2,4 GHz.



Rangos de velocidad disponibles (802.11b)

A partir de ahora, la red tiene un nombre, el SSID (*Service Set IDentifier*).

b. 802.11a

Como 802.11b, la norma 802.11a se publicó en septiembre de 1999. Pero, en cambio, su capa Física puede trabajar a 5 GHz. La transmisión máxima es de 54 Mbps. Como en la anterior, las velocidades pueden ser a 48, 36, 24, 18, 12, 9 y 6 Mbps.

A causa del cambio de frecuencia, las antenas 802.11a son incompatibles con las de 802.11b.

c. 802.11g

Este estándar, ratificado en junio de 2003, es el sucesor del 802.11b. También utiliza la banda de los 2,4 GHz y permite velocidades de 54 Mbps. Las velocidades posibles son las mismas que en 802.11a, es decir, 48, 36, 24, 18, 12, 9 y 6 Mbps.

d. 802.11n

La especificación 802.11g sigue siendo, desde 2003, la más explotada comercialmente. IEEE ha finalizado la evolución 802.11n en septiembre de 2009.

Después de las versiones 1.0 y 1.1, el grupo de trabajo de IEEE adoptó, en marzo de 2007, la versión 2.0 del borrador, que se acerca al estándar definitivo. En términos de capacidad, 802.11n en versión borrador incluía ya la calidad del servicio (QoS - *Quality of Service*), WMM (*Wi-Fi MultiMedia*) para las aplicaciones de VoIP (*Voice over IP*) y el *streaming*.

Las evoluciones que se tenían que definir eran importantes, ya que se trataba de mejorar a la vez, considerablemente, la velocidad y la cobertura de radio. Se pusieron en marcha varios procedimientos y fue difícil garantizar sus definiciones en el ámbito del estándar.

En primer lugar, se realizó un trabajo sobre la señal (capa Física). Este avance permitió prever una velocidad de 65 Mbps en lugar de los 54 Mbps de las especificaciones anteriores.

La segunda mejora en las transmisiones la han realizado una serie de técnicas relativas a la tecnología MIMO (*Multiple Input Multiple Output*). Por multiplexado espacial, se pueden tratar simultáneamente hasta 4 flujos en lugar de uno solo. Utilizando más antenas de recepción que flujos, es posible recibir señales de varios caminos.

La específicación 802.11n utiliza bandas de frecuencia de 2,4 y 5 GHz. Con esta última, es posible duplicar la longitud del canal, lo que permite ganar aún más velocidad. La velocidad máxima de la versión final de 802.11n es de 200 Mbps. Las técnicas utilizadas permiten en teoría alcanzar los 540 Mbps.

El alcance en interiores es de 50 metros y de 125 metros en exteriores.

e. 802.11ac

802.11ac se normalizó en enero de 2014. Utiliza la banda de frecuencia de 5 GHz a 6 GHz y puede llegar a 7 Gbps de velocidad gracias a los diferentes mecanismos utilizados.

Esta norma garantiza una compatibilidad ascendente con la 802.11n en la banda de frecuencia de los 5 GHz.

Se basa en un modo de funcionamiento **MIMO** (*Multiple Input, Multiple Output*), en el que se utilizan varias antenas de emisión y de recepción, que permiten multiplicar la capacidad y aumentar así el ancho de banda. También se caracteriza por el modo de codificación OFDM (*Orthogonal Frequency Division Multiplexing*) y OFDMA (*Orthogonal Frequency Division Multiple Access*).

El iPad Air 2 de Apple y la Surface Pro 3 de Microsoft implementan esta norma Wi-Fi.

iPad Air 2

Surface Pro 3 que implementa la norma 802.11ac

3. Hardware

La elección del hardware Wi-Fi requiere, en primer lugar, asegurarse de su compatibilidad con la norma de la capa Física.

a. La tarjeta de red

Una adaptador Wi-Fi está compuesto por un chip conectado a una antena. Está integrado al equipo informático, ordenador portátil, PDA... o incluido en una tarjeta periférica.

En el caso de una solución integrada, la antena también lo está. Por ejemplo, en un ordenador portátil se coloca a lo largo de la pantalla. Los fabricantes también pueden adoptar la tecnología Intel Centrino, que incluye Wi-Fi en una solución integral.

Hay muchos modelos de tarjetas Wi-Fi que permiten incorporar esta función a un ordenador. Existen los formatos PC Card/PCMCIA, Compact Flash, PCI o USB.

Tipos de tarjetas Wi-Fi

b. El equipo de infraestructura

Se utilizan principalmente dos dispositivos. Su objetivo es la interconexión de la red Wi-Fi a la red cableada Ethernet, lo que se denomina sistema de distribución (DS - *Distribution System*).

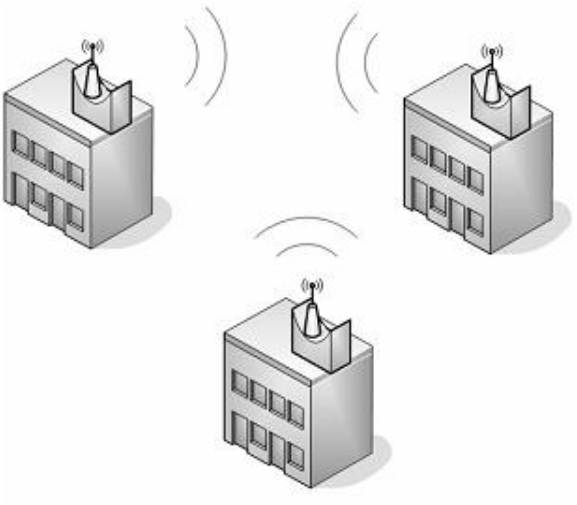
Punto de acceso

El punto de acceso (AP - *Access Point*) es el principal componente de la infraestructura de una red Wi-Fi. Como concentrador, centraliza todas las comunicaciones de los equipos que están asociados.

Concentradores Wi-Fi

Puente

La función principal de un puente (*bridge*) Wi-Fi es interconectar dos redes cableadas Ethernet a través de la interfaz inalámbrica. Los puentes Wi-Fi ofrecen una solución de bajo presupuesto para conectar las redes Ethernet de diferentes edificios, sin tener que recurrir a la fibra óptica, que, por supuesto, es más rápida.



Los puentes Wi-Fi permiten la conexión entre edificios

c. Los dispositivos Wi-Fi

Los terminales Wi-Fi más frecuentes siguen siendo los ordenadores, sobre todo los portátiles, y los dispositivos móviles, como los asistentes personales (PDA). En las oficinas, otros dispositivos se comunican ya por Wi-Fi: videoproyectores, impresoras, cámaras…

A nivel industrial o en almacenes, los lectores de código de barras, que hace mucho que son inalámbricos, han adoptado el estándar Wi-Fi.

Dispositivos Wi-Fi

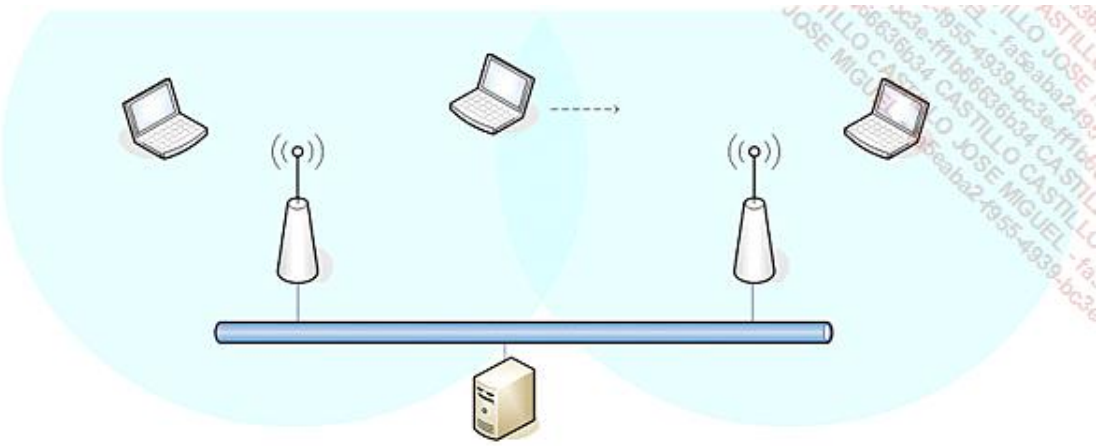
El éxito de la telefonía IP (VoIP) ha llevado a los fabricantes a ofrecer soluciones inalámbricas sobre la red Wi-Fi (VoWi-Fi). Estas recurren actualmente a funcionamientos propietarios, por ejemplo para la itinerancia, miestras se esperan los estándares.

4. Arquitectura

La primera arquitectura definida en la norma 802.11 permite una comunicación de igual a igual entre al menos dos equipos. Se denomina *Independent Basic Service Set* (IBSS), y se utiliza para crear redes *ad hoc*.

La segunda arquitectura requiere un punto de acceso. En este caso *Basic Service Set* (BSS) actúa como administrador para las estaciones periféricas que se le asocian. Todas las comunicaciones deben pasar por él.

Una red de mayor amplitud, con varios puntos de acceso, se llama *Extended Service Set* (ESS). Este tipo de red permite el desplazamiento por el interior de la empresa, asociándose sucesivamente a los puntos de acceso más cercanos y sin producir cortes de comunicación. Esta capacidad es la itinerancia o *roaming*.



Wi-Fi e itinerancia

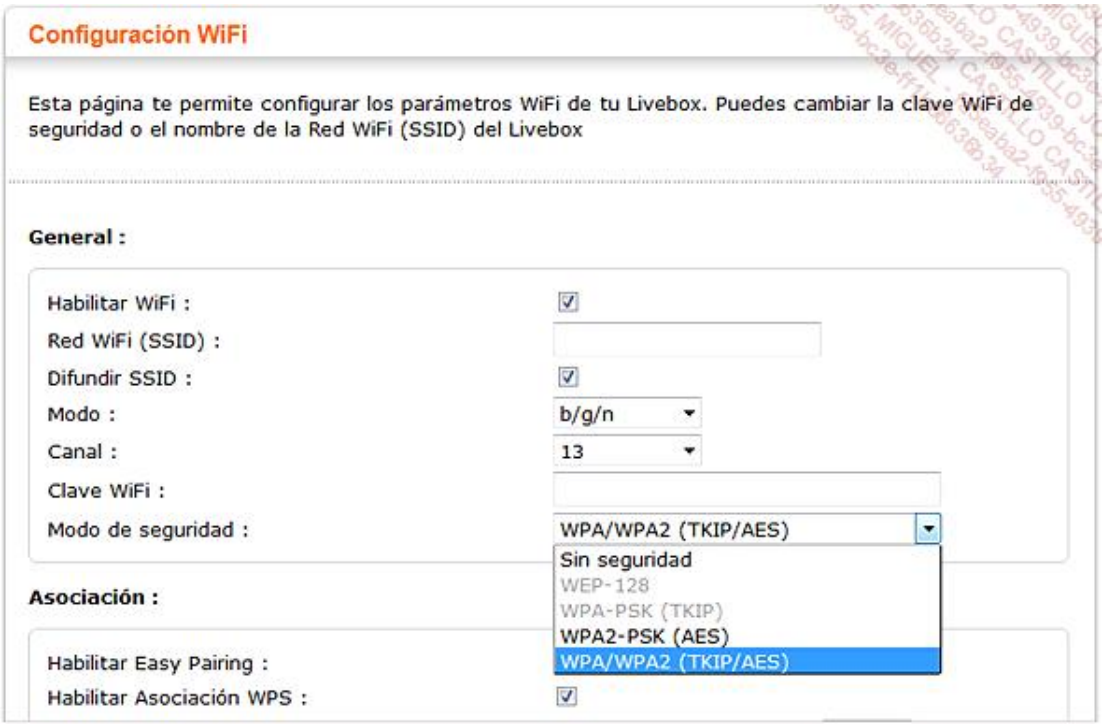
5. Seguridad

a. WPA

El Wi-Fi Protected Access se finalizó en 2003 en respuesta a las numerosas vulnerabilidades de WEP (*Wired Equivalent Privacy*). WPA implementa la mayor parte de las funcionalidades descritas en la norma 802.11i que se había completado totalmente en esa época.

El diseño del protocolo se basa en la utilización de un servidor de autenticación basado en 802.1X que es necesario para la distribución de claves para cada uno de los usuarios.

Existe una implementación más básica para particulares y pymes, que es la utilización de una clave compartida (*Pre-Shared Key* o PSK).



Ejemplo de elección de seguridad Wi-Fi en un router ADSL.

WPA se basa normalmente en el protocolo TKIP (*Temporal Key Integrity Protocol*), que utiliza claves más largas que las claves WEP. Este protocolo TKIP permite el intercambio dinámico de las claves.

Existen dos variantes de WPA (v1 o v2):

- WPA-personal.
- WPA-empresa.

El WPA-personal no necesita servidor de autenticación; cada equipo se autentica directamente con el punto de acceso a través de una clave de 256 bits.

La versión para empresas se basa en la utilización de un servicio RADIUS (*Remote Dial In User Services*) y se apoya necesariamente en un cifrado AES (*Advanced Encryption Standard*).

De este modo, WPA garantiza no solamente la autenticación, sino también el cifrado. Igualmente protege la integridad de las tramas firmándolas. Así, es casi imposible realizar ataques de modificación de las tramas y de su CRC (*Cyclic Redundancy Check*) como con WEP. Ofrece igualmente un mecanismo para contar tramas que impide la repetición por parte de los atacantes.

El algoritmo utilizado por la identificación de los mensajes es el MIC (*Message Integrity Code*), llamado también «Mickeal».

b. WPA2

Se trata de la versión del protocolo que respeta escrupulosamente la norma IEEE 802.11i.

El cifrado se implementa a través del protocolo AES.

Desde 2006, es obligatoria la compatibilidad WPA2 para los equipos certificados Wi-Fi.

6. Utilización

En primer lugar se debe considerar esta tecnología como la versión inalámbrica de Ethernet. Se presenta como la respuesta a las exigencias de movilidad dentro de las empresas. Más allá del uso administrativo, que se traduce en un equipo colocado en una mesa, Wi-Fi permite una verdadera itinerancia.

Otra utilización importante es la extensión de la red en la empresa. Llevar la red local allí donde aún no está disponible es, a partir de ahora, mucho más fácil que teniendo que llevar el cable. Además de la facilidad y rapidez de la implementación, el coste representa un criterio de elección importante.

Un *Hot-Spot* permite un acceso a Internet a través de la tecnología Wi-Fi. También se le conoce con el nombre de Acceso Público a Internet (API).

7. Encabezado de trama Wi-Fi

La capa *Medium Access Control* (MAC), capa inferior base de la Conexión de datos, constituye el núcleo de Wi-Fi.

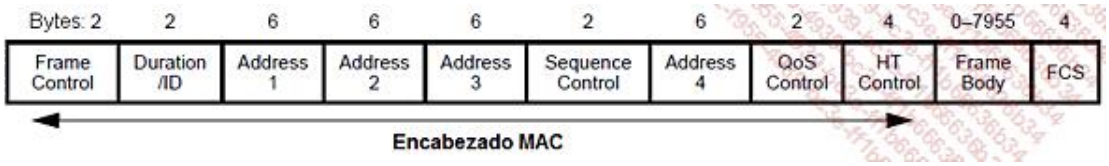
Esta capa debe administrar los canales de comunicación o, más bien, la ausencia de canales de comunicación físicos, caracterizados por una frecuencia de radio. Este canal debe compartirse entre los distintos nodos de la red. Cada uno posee su propia dirección MAC, como en Ethernet.

El mecanismo de gestión de los soportes de comunicación no puede utilizar la detección de colisiones, impensable en una red inalámbrica. Por ello se utiliza una solución que evita las tramas de tipo CSMA/CA.

La gestión de la división del ancho de banda no es, ni mucho menos, la única utilización de la capa MAC. Antes de emitir datos hacia un punto de acceso, un equipo debe conectarse a *Basic Service Set* (BSS), la red del equipo administrador. Pero antes será necesario un proceso de asociación, y antes de eso, puede que el punto de acceso pida la autentificación del equipo.

También pueden presentarse otras problemáticas a este nivel. Se gestionan la fragmentación/defragmentación de las tramas transmitidas, así como la administración de la capacidad para comunicar a distintas velocidades. Tampoco se deben olvidar los controles de error y el ahorro de energía. La seguridad también se puede administrar en la capa MAC.

El encabezado de trama Wi-Fi es claramente más complejo que su par Ethernet. El cuerpo de la trama tiene un tamaño máximo de 7956 bytes. Se observa que se reservan cuatro campos para las direcciones MAC. Esto permite el uso de las direcciones fuente y destino, y de puntos de acceso como intermediarios.



Construcción de un encabezado de trama Wi-Fi

El proyecto de enmienda 802.11n draft, entre otras cosas, ha dado como resultado algunas modificaciones en la capa MAC, tanto en el formato del encabezado como en su contenido. Se ha añadido un campo destinado a la

calidad del servicio (QoS - *Quality of Service*) después de la Dirección 4.