Redes de Comunicaciones Móviles: 802.11

Jose Antonio Molina Jiménez <*jamjcorreo@gmail.com*>
Guillermo J. De Ignacio Marí <*gdeignacio@gmail.com*>
Vicente J. Ferrer Dalmau <*vf.dalmau@gmail.com*>

11 de diciembre de 2007

Resumen

En el presente trabajo se muestra una visión de por qué, cómo y dónde se ha asentado la tecnología WiFi, centrándonos en el estándar americano 802.11

Índice general

Capítulo 1

Introducción

En este capítulo se explica el **por qué** de la rápida expansión de la tecnología WiFi.

1.1. Introducción

A lo largo de la historia de la humanidad una de las necesidades más importantes que se nos han planteado se han referido a las diferentes formas de relacionarnos con nuestros semejantes. Desde la simple comunicación gestual y verbal, pasando por las redes analógicas, hasta las comunicaciones digitales actuales, las comunicaciones han discurrido por múltiples etapas. Una fase más en el proceso evolutivo de estas tecnologías son las redes inalámbricas. Cuándo se habla de redes inalámbricas podemos distinguir dos grandes tipos: las redes inalámbricas que necesitan una línea de visión directa y sin elementos que bloqueen la señal, por ejemplo las señales de infrarrojos (IR), y las que no necesitan de una línea de visión directa, como son las señales de radiofrecuencia (FR) para la transmisión de información. Ejemplos típicos de este tipo de tecnología son los mandos a distancia para el televisor o algunos modelos de teclados inalámbricos para ordenadores. Típicamente este tipo de redes necesita de un funcionamiento próximo entre los componentes que la forman para su correcta operatividad. Uno de los motivos es la limitada capacidad en potencia de los dispositivos de transmisión regulada por los gobiernos para evitar problemas de interferencias y otros aspectos específicos de cada estado. Otro factor limitante es la frecuencia de operación (normalmente medida en Hz) a la que trabajan estos dispositivos. Algunas señales, como las señales de radio, los rayos-X o los RF son capaces de traspasar objetos sólidos mientras que otras, como las señales infrarrojas, no. Dentro del grupo de las primeras se encuentran las redes inalámbricas que nos ocupan: las redes definidas por la especificación IEEE 802.11 normalmente conocidas por "*WIFI*" (Wireless Fidelity). Este tipo de redes han supuesto una auténtica revolución en determinados ámbitos de la comunicación permitiendo desplegar muy rápidamente redes de carácter local (WLAN) sin necesidad de grandes infraestructuras y dotando de movilidad al usuario. De hecho, son su velocidad y alcance (unos 100-150 metros en hardware asequible) los que las convierten en una fórmula perfecta para el acceso a Internet sin cables. Actualmente existen varios subtipos de variantes que nos permiten diferentes tipos de velocidades y rangos de alcance, como son el 802.11a, b ,g y el novedoso n.

A pesar de estas grandes ventajas, las redes inalámbricas también tienen una serie de inconvenientes derivados principalmente de la naturaleza del medio por el que discurren. En primer lugar hay que decir que las redes inalámbricas no sustituyen a las redes fijas, simplemente las complementan, proporcionando flexibilidad y facilidad al usuario. Hay que tener en cuenta que las centrales de datos, es decir, los servidores normalmente no se mueven y que por tanto estos pueden estar conectados a un red cableada. Otra consideración refiere a las velocidades que se pueden alcanzar con las redes inalámbricas. A pesar de que algunos estados están intentando aumentar el rango de frecuencias libres para poder operar, al final las redes inalámbricas siempre están condicionadas a velocidades inferiores

a las redes cableadas. Las redes inalámbricas tienen que superar problemas de carácter físico como son la longitud de la onda o la frecuencia. Cuanto mayor es la frecuencia, de menor alcance se dispone y más sensible se es a las interferencias. Otro aspecto a considerar es el de la seguridad. Una de las supuestas ventajas de las redes cableadas concierne a la mayor seguridad de estas. La única forma de acceder a la información que se trasmite es mediante la conexión física al cable. En cambió en el caso de las redes inalámbricas la señal se propaga en múltiples direcciones hasta el rango de alcance de la señal lo que provoca que cualquiera que esté dentro del rango de la misma pueda acceder también a la información. A lo largo del tiempo se han ido desarrollando una serie de sistemas de protección y autentificación que como veremos, permiten dotar a las redes inalámbricas de cierto nivel de confianza.

1.2. Historia

La historia de las redes inalámbricas no podría contarse sin unos grandes pioneros como **Hedy Lamarr** y **George Antheil,** creadores del *spread spectrum*, elemento clave para el desarrollo de las redes inalámbricas actuales. Hedy fue una actriz austriaca que triunfó en Europa antes de llegar a Hollywood a finales de la década de los 30. Nacida en 9 de noviembre en Viena, Austria, su nombre real era **Hedwig Eva Maria Kiesler** hija de un poderoso banquero austriaco. Inició, aunque no completó, unos estudios en ingeniería que dejaría por su pasión, la interpretación. Debido a unos escándalos con una serie de filmes que protagonizó tuvo que alejarse de las pantallas por un tiempo. Su padre la obligó a casarse con un industrial alemán pro-nazi, que la mantuvo prácticamente secuestrada durante cuatro años hasta que la joven escapó de su marido huyendo primero París, luego a Londres y finalmente a los Estados Unidos. En aquella época, uno de los problemas mas graves a los que se enfrentaban los militares era la fragilidad de las comunicaciones por radio. Por un lado, el enemigo podía escuchar los canales utilizados por sus tropas, lo que les permitía, además de enterarse de sus comunicaciones, triangular el origen de la transmisión y así localizar al emisor. Además, el enemigo, en el momento en que detectaba una transmisión, podía enviar una señal parásita en ese mismo canal, lo que interfería y anulaba la transmisión. Este problema era especialmente grave en el caso de los espías, que cada vez que enviaban una transmisión no solo estaban delatando su posición, sino que las interferencias enemigas podían hacer su trabajo inútil. Además, el problema de la fragilidad de las comunicaciones por radió también tenía paralizados los proyectos para crear misiles y torpedos teledirigidos, ya que la facilidad para interferir las señales de radio hacía a estas armas totalmente inviables. Una vez en Estados Unidos, además de retomar su carrera como actriz, empezaría a trabajar en una solución para el problema de las comunicaciones por radio; para ello, inventó unos equipos de radio que iba cambiando de canal continuamente, con lo que al enemigo le resultaba imposible seguir la señal. En el aparato diseñado por Hedy conjuntamente con su amigo, el compositor George Antheil, el cambio de frecuencias seguía un patrón fijo que estaba grabado en un tambor; tanto el transmisor como el receptor debían conocer este patrón y estar adecuadamente sincronizados. Hedy patentaría este aparato en 1941, bajo el nombre de "*sistema de comunicaciones secreto*"; sería la patente número 2.292.387.

Muchos se podrán preguntar los motivos que pueden relacionar esta patente con las redes inalámbricas actuales, pues bien, en los años 90 del pasado siglo, los ingenieros que trabajaban en el desarrollo de las redes informáticas inalámbricas se encontraron con el problema de evitar que los equipos que integraban la red se interferíeran entre si. El problema estaba claro, si dos aparatos emiten a la vez por el mismo canal, sus señales se interfieren y a los receptores no les llega nada; la solución obvia es hacer que los equipos estén escuchando el canal y emitan únicamente cuando no hay nadie mas emitiendo, pero esto tiene un problema: ¿Que pasa si dos equipos empiezan a emitir simultaneamente? Este problema es muy real, ya que los equipos informáticos funcionan a unas velocidades muy altas, de manera que en las milésimas de segundo que tarda una señal de radio en recorrer la distancia que le separa de alguno de sus compañeros de la red, este último tiene tiempo de comprobar el canal y realizar su propia emisión. En general, se observó que los esquemas basados en regular el tráfico para evitar que varios aparatos emitieran a la vez eran muy ineficientes. En este punto, se puso sobre la

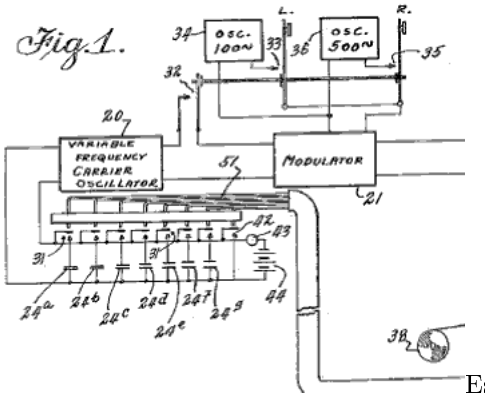


Figura 1.1: Esquema de la patente original.

mesa la invención de Hedy Lamarr; en este caso, la idea era que los equipos, en lugar de utilizar un único canal, utilizarían un rango de canales de radio, y a la hora de transmitir elegirían uno de ellos al azar, e irían cambiando de frecuencia también de forma aleatoria. Por supuesto, seguía existiendo el problema de que dos aparatos emitieran a la vez por el mismo canal en el mismo momento, pero se observó que las probabilidades de que esto ocurriera eran muy bajas, con lo que las pérdidas de datos derivadas eran lo bastante pequeñas como para ser manejadas mediante un protocolo convencional de detección y corrección de errores. El único problema que tenía esta tecnología era la necesidad de que el receptor pudiera escuchar simultáneamente en todos los canales utilizados, algo que en aquel momento ya era perfectamente posible (cuando Hedy inventó su aparato no lo era), pero con un coste mucho mas elevado de lo que los compradores estarían dispuestos a pagar, así que la idea tuvo que quedarse en el congelador hasta los primeros años del presente siglo, en que la tecnología ya se había abaratado lo suficiente como para que el cambio aleatorio de frecuencia se pudiera utilizar en equipos comerciales. Otra de las bases sobre las que se asienta la tecnología 802.11 fueron desarrolladas por Nikola Tesla en sus trabajos sobre las tecnologías inalámbricas y de radio. En concreto y más recientemente el estandar *Wi-Fi* fue inventada por **NCR Corporation/AT&T** en 1991 por **Vic Hayes** para sistemas bancarios. Los primeros sistemas comerciales fueron comercializados bajo el nombre de *WaveLan* con velocidades de 1Mbps/2Mbps . Su inventor Vic Hayes se retiro de la empresa (la cual más tarde pasó a llamarse Lucen Tecnologies) poco antes de que la misma, debido a razones de mercado, abandonara el mercado de las redes inalámbricas a principios del 2004. Actualmente la marca comercial *Wi-Fi* referente al estandar 802.11 es propiedad de la *Wi-Fi Alliance*. En 1999 un grupo de empresas: 3Com, Aironet (ahora llamada Cisco), Intersil, Lucent, Nokia y Symbol Technoligies decidieron unirse para crear el *WECA* o alianza de compatibilidad para redes ethernet inalámbricas gistrando la marca comercial Wi-Fi. Las funciones de esta alianza eran las de realizar tests, certificar interoperatibilidad de los productos y promover la tecnología. En el 2003 WECA se renombró a si misma como *Wi-Fi Alliance* y tiene su sede central en Austin, Texas. Hoy día esta alianza cuenta con unos 260 miembros y controla la certificación de productos Wi-fi lo que garántiza a los compradores que sus productos funcionarán correctamente en sus redes. La autoridad mundial en estandarización de redes LAN wireless es el Wireless Local Area Networks Standards Working Group, IEEE 802.11 . Desde 1990, fecha en que se constituyo el comité de estudio del estándar, el proyecto 802.11 no ha parado de evolucionar. En 1991 el comité seleccionó el protocolo *DFWMAC* (distributed foundation wireless media access control) propuesto por AT&T y un conjunto de empresas más como la base para el desarrollo de un estándar para redes inalámbricas

Son dos los estándares que han llenado (y siguen haciéndolo a día de hoy) el mercado de las comunicaciones inalámbricas bajo la tecnología 802.11: los formatos b y g. EL sistema 802.11b opera en la banda de frecuencias de los 2.4 Gh con una capacidad de unos 11Mbps máximos teóricos. Estandariza-

do en 1999 tiene un alcance aproximado de unos 100 metros en interiores y unos 300 en exteriores. Si bién este estandar es más que suficiente para la navegación por internet y comunicaciones básicas, pronto se reveló como insuficiente conforme las redes fueron necesitando de más ancho de banda, así surgió el estandar 802.11a. Este era capaz de un ancho de banda de unos 54Mbps y operaba en el rango de frecuencias de los 5Ghz. Este hecho provocó que su alcance fuera mucho más corto y bastante más caro que su predecesor, por lo que nunca llegó a adoptarse masivamente. De nuevo apareció un nuevo formato: se adoptó en estandar 802.11g a princios del 2003. Este permitía las mismas tasas máximas teóricas de conexión pero con un mayor alcance (al operar en los 2.4Ghz) y coste más bajo.

Aún así, dadas las crecientes necesidades de las redes actuales, en enero del 2004 el IEEE decidió preparar un grupo de trabajo para crear un nuevo estandar para las redes inalámbricas: el 802.11n, el cual promete mejoras sustanciales en las redes inalámbricas del futuro mediante el uso del *MIMO* o multiple- entrada, multiple-salida que se basa en el uso de varios receptores y antenas de emisión para crear la red.

Hoy día la tecnología inalámbrica sigue evolucionando hacia soluciones cada vez más potentes, ŕapidas y versátiles, en este campo están despegando tecnologías como Wimax que representan todo un desafío para las redes inalámbricas del futuro y que probablemente supongan auténticas revoluciones en el mundo de las comunicaciones.

1.3. Órganos certificadores y consorcios

Wifi Alliance

En el ámbito de las tecnologías relacionadas con el estandar 802.11 el consorcio que aglutina a la inmensa mayoría de fabricantes es la alianza WiFi. Esta alianza se creó en 1999 para conseguir un cierto grado de estandarización de los productos que seguian el protocolo. El papel de esta organización (sin ánimo de lucro, como ellos mismos la definen) ha sido, y es, fundamental en el desarrollo de la tecnología, ya que por un lado ha conseguido un excelente nivel de interoperatividad entre los fabricantes y sus dispositivos y por otro, este mismo hecho ha permitido una gran popularización de la tecnología que a su vez, al acceder a las masas, ha conseguido unos precios muy buenos. Actualmente la alianza dispone de unos 250 miembros, entre los que se encuentran la inmensa mayoría de los más importantes agentes en el mundo de la informática y las comunicaciones, como **Microsoft, Intel, apple** computers, **Dell, Sony, Nokia** y un largo etc. Esta alianza de empresas también se encarga de certificar los dispositivos inalámbricos. En el año 2000 se habían certificado ya unos 3000 productos. Sus certificados se fundamentan en varias categorías:

- Productos Wifi basados en los estandares de radio del **IEEE 802.11a/b/g** en formato de transmisón simple, doble o multibanda.
- **WPA / WPA2** para usuarios empresariales o domésticos.
- **EAP**, protocolo sobre el que se basa el sistemas de autentificación 802.1x
- **WMM**, soporte para el uso de contenidos multimedia en redes inalámbricas.

Estas certificaciones se realizan en varios laboratorios,ente los que se destacan: ADT Corporation (Taiwan), Allion Computers Inc (Taiwan), AT4 Wireless (España), Cetecom Inc. (USA) SGS group (Japón).

El protocolo **IEEE 802.11** es un estándar de protocolo de comunicaciones de la rama 802.x (los cuales definen la tecnología de redes de área local) que define el uso de los dos niveles más bajos de la

arquitectura **OSI** (capas física y de enlace de datos). Podemos ir viendo como se han ido aprobando los estándares en los últimos años. Si hablamos del estándar original, que data de 1997, era el IEEE 802.11, que tenía velocidades de 1 hasta 2 Mbps y trabajaba en la banda de frecuencia de 2,4 GHz. Actualmente ya no se fabrican productos sobre este estándar. Éste protocolo se conoce ahora como **802.11legacy.** Más adelante, en 1999, y como primera modificación, apareció el **IEEE 802.11b**, en cuya especificación tenía velocidades de 5 hasta 11 Mbps y que también trabajaba en la frecuencia de 2,4 GHz. Además, también se aprobó el IEEE 802.11a, que en este caso su especificación era sobre una frecuencia de 5 GHz que alcanzaba los 54 Mbps y que resultaba incompatible con los productos de la b.En 2003 se incorporó un estándar a la velocidad de la a y que era compatible con b. Éste se llamó **IEEE 802.11g.** En la actualidad la mayoría de productos son de la especificación b y g. Actualmente hay un paso más, con el IEEE 802.11n, que con él sube el límite teórico a 600 Mbps y que se espera que se apruebe a finales de 2007 o principios de 2008. Veamos ahora cada uno de estos protocolos:

802.11legacy

Es la versión original del estándar IEEE 802.11. Fue publicado en 1997 y en él se especifican las velocidades de 1 y 2 Mbps (teóricos), que se transmiten por señales IR (infrarrojas) en la banda **ISM** (Industrial, Scientific and Medical) a 2,4 GHz. Como método de acceso utiliza el protocolo **CSMA/CA** (Carrier Sense Multiple Access With Collission Avoidance) para evitar colisiones entre los paquetes de datos, que también se define en el estándar original. Debido a las necesidades de esta codificación para mejorar la calidad de la transmisión se utilizaba una parte importante de la velocidad de transmisión teórica en ello, lo cual hizo que se dificultara la interoperabilidad entre equipos de diferentes marcas. Ello se corrigió en el siguiente estándar.

802.11b

Este protocolo se aprobó en 1999 y como ya se ha comentado, tiene una velocidad máxima de transmisión de hasta 11 Mbps y funciona en la banda de frecuencia de 2,4 GHz. En 802.11b se utiliza el mismo método de acceso (CSMA/CA) que se define en el estándar original, y debido al hecho de la codificación de este protocolo, en la práctica, las velocidades máximas de transmisión no son de 11 Mbps, sino aproximadamente 5.9 Mbps sobre TCP (Transmission Control Protocol) y 7.1 sobre **UDP** (User Datagram Protocol).

802.11a

Este protocolo fue el otro que se aprobó en 1999, junto con el b. En él la velocidad máxima teórica aumentaba hasta los 54 Mbps, y funciona en la banda de frecuencia de 5 GHz. En este caso, puede ser práctico para redes inalámbricas con velocidades reales de aproximadamente 20 Mbps. Utiliza el mismo juego de protocolos de base que el estándar original y utiliza 52 subportadoras **OFDM** (Orthogonal Frequency-Division Multiplexing). La velocidad de datos se reduce a 48, 36, 24, 18, 12, 9 o 6 Mbps en caso necesario.802.11a tiene 12 canales no solapados (8 para red inalámbrica y 4 para conexiones punto a punto), y como ya se ha comentado, no puede haber interoperabilidad con equipos del estándar 802.11b (a menos que se disponga de equipos que implementen ambos estándares). El que se utilice la banda de 5 GHz supone una ventaja para el 802.11a ya que presentan menos interferencias (hay que recordar que en 2,4 GHz es la misma banda utilizada por los teléfonos inalámbricos y los hornos microondas, entre otros aparatos). Aunque por otro lado tiene la desventaja de que restringe el uso de los equipos a únicamente puntos en línea de vista (lo cual equivale a una mayor instalación de puntos de acceso), y dichos equipos no pueden penetrar tan lejos como los del estándar 802.11b, ya que sus ondas son más fácilmente absorbidas.

802.11g

Se ratificó este tercer estándar de modulación en 2003, utilizando la banda de frecuencia de 2,4 GHz (al igual que lo hace el 802.11b) pero operando a una velocidad teórica máxima de 54 Mbps,

o cercanos a los 24.7 Mbps de velocidad real de transferencia (similar a 802.11a). Éste estándar es compatible con 802.11b y utiliza las mismas frecuencias. Es más, buena parte de proceso de diseño del estándar lo tomó el hacer compatibles los dos estándares. Eso si, la presencia de nodos de estándar b, reduce significativamente la velocidad de transmisión.

802.11n

Hace pocos días, a finales de enero de 2007, se aprobó el borrador del estándar 802.11n, mientras que se espera que a finales de 2007 o a principios de 2008, se ratifique finalmente. La velocidad marcada en el borrador es de hasta 300 Mbps, pero se prevé que la versión final marque los 600 Mbps como velocidad máxima posible. Las principales características promocionales del 802.11n son:

- *MIMO (Multi-In, Multi-Out)* generando canales de tráfico simultáneos entre las diferentes antenas de los productos 802.11n, permitiendo mayor alcance de operación.
- *Canales de 20 y 40 MHz* (Lo que permite incrementar enormemente la velocidad)
- *El uso de las bandas de 2,4 y 5 GHz simultáneamente.*

Capítulo 2

Tecnología y seguridad

En este capítulo se muestra **cómo** funciona la tecnología WiFi.

2.1. Aspectos tecnológicos

Capa MAC

Tres servicios son proporcionados por la subcapa MAC en IEEE 802.11. Estos servicios son los siguientes:

1. Servicio de datos asíncronos
2. Servicios de seguridad
3. Ordenamiento de MSDU[1]

Todos estos servicios utilizan unidades de información llamadas frames; cada frame consiste en los siguientes componentes básicos:

- Un encabezado MAC, que consiste en información acerca del control de frames, la duración, la dirección y el control de las secuencias
- Un cuerpo de frames de longitud variable, que contiene información específica del tipo de frame. Por ejemplo, en los frames de datos, esto contendría datos de la capa superior. Los tipos de frames son los siguientes:
  - Frames de datos.
  - Frames de control: organizan el tráfico porporcionando indicaciones sobre el estado de los paquetes; ejemplos de esto son las señales como la solicitud para enviar (RTS), despejado para enviar (CTS) y confirmación (ACK).
  - Frames de administración: proporcionan información de administración y no se envían a las capas superiores.
- Una secuencia de verificación de frames (FCS), que contiene una verificación de redundancia cíclica (CRC) IEEE de 32 bits.

[1] MAC Service Data Unit, corresponde a la unidad de datos recibidos por la subcapa LLC.

Para transmitir estos frames es necesario que el dispositivo tenga acceso al medio, lo que se puede realizar de dos formas:

1. El método de acceso fundamental del MAC IEEE 802.11, acceso múltiple con detección de portadora y colisión evitable (CSMA/CA), se denomina Función de Coordinación Distribuida (DCF) tanto en configuraciones de red ad hoc como de infraestructura.
2. También puede incorporar un método de acceso opcional, denominado Función de Coordinación de Punto (PCF), que crea un acceso libre de contención (CF). La PCF sólo puede utilizarse en configuraciones de red de infraestructura.

Una vez conseguido el acceso al medio es necesario saber el estado del mismo, es decir detectar las portadoras físicas y virtuales; lo cual se consigue mediante una serie de funciones. Cuando alguna de estas funciones indica un medio ocupado, el medio se considera ocupado. Si el medio no está ocupado, se considerará inactivo. Un mecanismo de detección de portadora físico es proporcionado por la PHY[2]

Los detalles de la detección de portadora física se proporcionan en las especificaciones individuales de la PHY. El MAC proporciona un mecanismo de detección de portadora virtual. Este mecanismo se denomina vector de adjudicación de la red (NAV). El NAV mantiene una predicción del tráfico futuro en el medio, basado en la información del campo de duración de los frames. La información respecto a la duración también está disponible en los encabezados MAC de todos los frames enviados.

Confirmaciones del nivel de la MAC

La recepción de algunos frames requiere que la estación receptora responda con una confirmación, en general un frame ACK, si la Secuencia de Verificación de Frames (FCS) del frame recibido es correcta. Esta técnica se conoce como confirmación positiva. La falta de recepción de un frame ACK esperado indica a la estación de origen que ha ocurrido un error. Puede ser posible que la estación de destino haya recibido el frame correctamente y que el error haya ocurrido en la entrega del frame ACK. Para el iniciador del intercambio de frames, estas dos condiciones son indistinguibles entre sí.

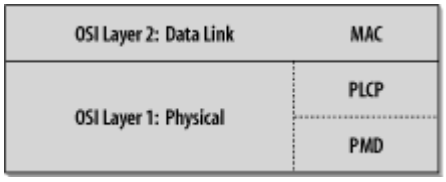
Confirmaciones del nivel de la MAC

El intervalo entre frames se denomina espacio interframe (IFS). Cada intervalo IFS se define como el tiempo desde el último bit del frame anterior al primer bit del preámbulo del frame subsiguiente, como se aprecia en la interfaz aérea. Cuatro IFSs diferentes se definen para proporcionar niveles de prioridad para un acceso al medio inalámbrico. Los IFSs se enumeran en orden, desde el más corto al más largo:

1. **SIFS** es el espacio interframe corto.
2. **PIFS**[3] empleado por el controlador centralizado en el esquema PCF[4] cuándo realiza sondeos.
3. **DIFS**[5] es el espacio interframe DCF
4. **EIFS** es el espacio interframe extendido.

Capa Física

[2] PHY es una abrebiatura para la capa física com se verá más adelante.
[3] Función de coordinación puntual IFS.
[4] Point Coordination Function, control de acceso al medio centralizado.
[5] Función de coordinación distribuida IFS.

Figura 2.1: 

Uno de los componentes más importantes del estandar 802.11 es la capa física, la cual es abreviada usualmente como PHY. Como se puede observar en la figura 1.1, está formada por 2 partes o subcapas: *the Physical Layer Convergence Procedure* ***(PLCP) o capa física de convergencia*** y la *Physical Medium Dependent* ***(PMD)*** o **capa dependiente del medio**. El PLCP realiza las funciones de conexión entre la capa mac y las trasmisiones en el aire. El PMD se encarga de transmitir la información que le llega de la capa PCLD y la transmite por el aire mediante la antena del dispositivo. La capa fisica también dispone de una función llamada ***CCA*** *(clear channel assessment)* que le indica a la capa MAC cuando se detecta una señal

1. **Modulación y velocidades de datos del canal**

Se especifican cuatro formatos de modulación y velocidades de datos para la PHY. La velocidad de acceso básico se basará en la modulación de afinación de desplazamiento de fase binaria diferencial (DBPSK) de 1 Mbps. La velocidad de acceso mejorada se basa en una afinación de desplazamiento de fase de cuadratura diferencial (DQPSK) de 2 Mbps. La especificación de secuencia directa extendida define dos velocidades de datos adicionales. Las velocidades de acceso de Alta Velocidad se basan en el sistema de modulación de la Codificación de Código Complementario (CCK) para 5,5 Mbps y 11 Mbps. La codificación de circunvolución binaria de paquetes (PBCC) opcional también se proporciona para un desempeño mejorado de hasta 22 Mbps. La Codificación de Código Complementario (CCK) se utiliza para incrementar la velocidad de datos pico de 802.11b de 2 a 11 Mbps, a la vez que se utiliza la modulación DQPSK. Hace esto incrementando en primer lugar la velocidad de reloj de datos de 1 Mbps a 1,375 Mbps, y luego tomando los datos en bloques de 8 bits (8*1,375 = 11). Seis de los ocho bits se utilizan para escoger 1 de 64 códigos complementarios, que tienen cada uno ocho chips de largo y se cronometran en 11 MHz. Los otros 2 bits se combinan con el código del modulador DQPSK.
.

Modulación 802.11b

Esta extensión del sistema DSSS se basa en las capacidades de velocidades de datos del estándar 802.11 original, para proporcionar tasas de datos con una carga de 5,5 Mbps y 11 Mbps. Las primeras velocidades de 1 Mbps y 2 Mbps aún se soportan. Para proporcionar las velocidades más altas, se emplea la codificación de código complementario (CCK) de 8 chips como sistema de modulación. La velocidad de chipping es de 11 MHz, que es igual a la del sistema DSSS, proporcionando así el mismo ancho de banda del canal ocupado. La PHY de Alta Velocidad básica utiliza el mismo preámbulo PLCP que la PHY DSSS, por lo cual ambas PHYs pueden co-existir en el mismo BSS.
Además de proporcionar extensiones de más alta velocidad al sistema DSSS, una cantidad de funciones opcionales permiten mejorar el desempeño del sistema LAN de frecuencia de radio. Se han definido las siguientes funciones opcionales:

• Un modo opcional puede reemplazar la modulación CCK por la codificación de circunvolución binaria de paquetes (HR/DSSS/PBCC). Esta extensión opcional también se aplica a 802.11g, que puede operar a velocidades de hasta 54 Mbps.

• Un modo opcional puede permitir que un throughput de datos a las velocidades más altas de 2, 5'5 y 11 Mbps se incremente significativamente utilizando un preámbulo PLCP más corto. Este modo se denomina HR/DSSS/corto, o HR/DSSS/PBCC/corto. Este modo de preámbulo corto puede

coexistir con DSSS, HR/DSSS, o HR/DSSS/PBCC bajo circunstancias limitadas, como en diferentes canales. La extensión de IEEE 802.11a a 802.11 incluye una función similar, denominada secuencia de capacitación corta o larga.

• Una capacidad opcional para la agilidad del canal permite que una implementación supere dificultades inherentes a las asignaciones de canal estáticas. Esta opción puede utilizarse para implementar sistemas que cumplen con IEEE 802.11 que sean interoperables con modulaciones tanto FH como DS.

2.1.1. Especificación de PHY IEEE 802.11a

Los productos que cumplen con el estándar 802.11a permitirán a las WLANs lograr velocidades de datos tan altas como 54 Mbps. Los dispositivos IEEE 802.11a operan en el rango de frecuencia de 5 GHz. Es desde esta frecuencia más alta que el estándar obtiene parte de su rendimiento. El resto proviene de la combinación de las técnicas de codificación y modulación utilizadas. El protocolo 802.11a se desplazó a una frecuencia más amplia (5 GHz) en parte para obtener velocidades más altas, pero también para evitar problemas de interferencia en la banda más poblada de los 2,4 GHz. Además de las WLANs 802.11b, las LANs HomeRF, los dispositivos Bluetooth, los teléfonos inalámbricos e incluso los hornos a microondas operan todos en la banda de los 2,4 GHz.

Los beneficios de utilizar el espectro de 5 GHz son contrarrestados por la falta de compatibilidad con la generación de LANs 802.11b, porque las frecuencias no coinciden. Muchos fabricantes están tratando este problema fabricando productos de modo dual que realmente contienen dos radios, una que opera en el rango de los 2,4 GHz, y una que opera en el rango de los 5 GHz. Multiplexado por división de frecuencia ortogonal (OFDM). El estándar IEEE 802.11a utiliza multiplexado por división de frecuencia ortogonal, una técnica que divide un canal de comunicaciones en una cierta cantidad de bandas de frecuencia que se encuentran separadas por el mismo espacio. OFDM utiliza múltiples subportadoras, que son 52, separadas por 312,5 KHz. Los datos se envían por 48 portadoras simultáneamente, donde cada subportadora transporta una porción de los datos del usuario. Cuatro subportadoras se utilizan como pilotos. Las subportadoras son ortogonales (independientes) entre sí.

El tiempo para transmitir cada bit se incrementa en proporción a la cantidad de portadoras. Esto hace al sistema menos sensible a la interferencia multiruta, una fuente importante de distorsión

2.1.2. Especificación de PHY IEEE 802.11g

IEEE 802.11a proporciona velocidades de hasta 54 Mbps. El problema más importante de 802.11a, que se especificó al mismo tiempo que 802.11b, es que utiliza la banda de frecuencia de 5 GHz en lugar de la de 2,4 GHz. Esto impide la compatibilidad con productos anteriores y representa un bloqueo considerable a la difusión de su implementación. El grupo de trabajo IEEE 802.11 aprobó mas tarde el estándar IEEE 802.11g. Proporciona la misma velocidad máxima que 802.11a, que es de 54 Mbps, pero opera en el mismo espectro de 2,4 GHz que los otros estándares de WLAN existentes. Existe una interoperabilidad entre todas las velocidades, por lo cual no es necesario actualizar toda la WLAN al desplazarse a velocidades más elevadas

El IEEE seleccionó a OFDM, la misma tecnología utilizada en las redes 802.11a, como base para el estándar de la red 802.11g. La forma de onda OFDM multiportadora es superior en casi cada aspecto a la forma de onda CCK de portadora única utilizada en 802.11b. Ofrece velocidades mucho más altas, un mayor alcance y una mejor tolerancia de ecos multiruta, que son comunes en las aplicaciones del interior de los edificios. El estándar 802.11g requiere el uso de OFDM para velocidades de datos rápidas (mayores que 20 Mbps), así como compatibilidad con la codificación CCK 802.11b. Aunque la arquitectura híbrida no es tan eficiente como OFDM pura, es atractiva. Incluso aunque los dispositivos 802.11b de legado no podrán decodificar la carga de paquetes de estos frames, pueden "detectarlos" en la red. Los nuevos frames pueden coexistir con 802.11b, de manera similar a la forma en la cual 802.11b puede coexistir con sistemas 802.11 más antiguos de 2 Mbps. La especificación OFDM pura, que

utiliza un preámbulo/encabezado basado en OFDM más eficiente, no tiene las mismas características. Los dispositivos 802.11b no detectarán los frames 802.11g, y viceversa. Aprovechando los elementos RTS/CTS de IEEE 802.11, en el cual los access points que hablan ambos lenguajes pueden regular las transmisiones, los dos pueden coexistir pacíficamente.

2.1.3. Especificaciones de PHY de FHSS e Infrarrojo (IR)

El Espectro Expandido de Salto de Frecuencia (FHSS) y el Infrarrojo (IR) son dos de las diversas especificaciones de PHY disponibles. IR y FHSS no se utilizan ampliamente hoy en día. DSSS y OFDM son las tecnologías más comunes actualmente en uso. El estándar 802.11 define un conjunto de canales FH espaciados de manera pareja a lo largo de la banda de 2,4 GHz. La cantidad de canales, como ocurre con DSSS, depende de la geografía. Puede haber hasta 79 canales en Norteamérica y en la mayor parte de Europa, y 23 canales en Japón. El rango de frecuencia exacta varía levemente según la ubicación.
El PMD FHSS transmite PPDUs saltando de canal a canal, de acuerdo a una secuencia de salto pseudoaleatoria particular que distribuye uniformemente la señal a través de la banda de frecuencia operativa. Una vez que la secuencia de saltos se configura en un AP, las estaciones se sincronizarán automáticamente según la secuencia de salto correcta. Tres conjuntos de secuencias de salto válidas están definidas.
El PMD utiliza una modulación de codificación de desplazamiento de frecuencia de Gauss (GFSK) de dos niveles para transmitir a 1 Mbps. Un seno de modulación GFSK de cuatro niveles se utiliza para transmitir a 2 Mbps. Las estaciones que operan a 2 Mbps también deben poder operar a 1 Mbps.

2.1.4. PHY infrarroja (IR)

La PHY IR utiliza luz casi visible en el rango de los 850 nm a los 950 nm para la señalización. Esto es similar al uso espectral de dispositivos comunes entre los consumidores tales como controles remotos infrarrojos, así como otro equipamiento de comunicaciones de datos, como los dispositivos de la Asociación de Datos Infrarrojos (IrDA). A diferencia de muchos otros dispositivos infrarrojos, la PHY IR no está dirigida.
Esto significa que el receptor y el transmisor no tienen que estar dirigidos uno al otro y no necesitan una línea de visión clara. Esto permite construir con más facilidad un sistema WLAN inalámbrico. Un par de dispositivos infrarrojos que cumplan con las normas podrían comunicarse en un entorno típico a un rango de alrededor de 10 m. Este estándar permite receptores más sensibles, que pueden incrementar el rango hasta en 20 m.
La PHY IR se basa tanto en energía infrarroja reflejada como en energía infrarroja de línea de visión para las comunicaciones. La mayoría de los diseños anticipan que toda la energía del receptor sea energía reflejada. Esta forma de transmisión basada en la energía infrarroja se denomina transmisión infrarroja difusa.
La PHY IR operará sólo en entornos de interiores. La radiación infrarroja no pasa a través de las paredes, y se ve significativamente atenuada al pasar a través de la mayoría de las ventanas que dan al exterior. Esta característica puede utilizarse para "contener" una PHY IR en una única habitación física, como un aula o una sala de conferencias. Diferentes LANs que utilizan la PHY IR pueden operar en salas adyacentes separadas sólo por una pared, sin interferencia y sin la posibilidad de que ocurra una escucha no deseada. Actualmente no existe ninguna restricción regulatoria respecto a la adjudicación de frecuencia o a la adjudicación de ancho de banda sobre las emisiones infrarrojas. El emisor, en general, un diodo electroluminiscente, LED, y el detector, en general, un diodo PIN, utilizados para las comunicaciones infrarrojas son de relativamente bajo costo en las longitudes de onda infrarrojas especificadas en la PHY IR y en las frecuencias operativas eléctricas requeridas por esta PHY.

2.1.5. Tecnologías inalámbricas

Las WLAN sólo son uno de los usos del espectro RF. La Figura 1 ilustra las relaciones de velocidad "distancia frente a datos" que existen en las diferentes tecnologías inalámbricas. La tabla 1.1 enumera las distintas bandas de radiofrecuencias, junto con el nombre de las ondas transmitidas en cada banda y los usos típicos. Multitud de diferentes y complejas tecnologías abarrotan el espectro de frecuencias.

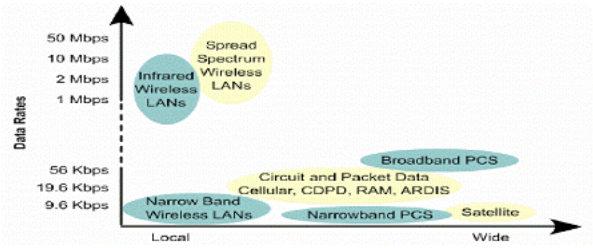


Figura 2. Velocidades A continuación se muestran las diferentes frecuencias y su relación con su longitud de onda y su banda ITU:

Nombre	Abreviatura inglesa	Banda ITU	Frecuencias	Longitud de onda
			Inferior a 3 Hz	>100.000 km
Extra baja frecuencia	ELF	1	3-30 Hz	100.000 km – 10.000 km
Super baja frecuencia	SLF	2	30-300 Hz	10.000 km – 1000 km
Ultra baja frecuencia	ULF	3	300–3000 Hz	1000 km – 100 km
Muy baja frecuencia	VLF	4	3–30 kHz	100 km – 10 km
Baja frecuencia	LF	5	30–300 kHz	10 km – 1 km
Media frecuencia	MF	6	300–3000 kHz	1 km – 100 m
Alta frecuencia	HF	7	3–30 MHz	100 m – 10 m
Muy alta frecuencia	VHF	8	30–300 MHz	10 m – 1 m
Ultra alta frecuencia	UHF	9	300–3000 MHz	1 m – 100 mm
Super alta frecuencia	SHF	10	3-30 GH	100 mm – 10 mm
Extra alta frecuencia	EHF	11	30-300 GHz	10 mm – 1 mm
			Por encima de los 300 GHz	<1 mm

La Administración de servicios generales de Estados Unidos define la radio de la siguiente forma:

- Telecomunicación por modulación y radiación de ondas electromagnéticas.
- Transmisor, receptor o transceptor utilizado para la comunicación mediante ondas electromagnéticas.
- Término general aplicado al uso de ondas de radio.

Las tecnologías inalámbricas están compuestas de muchos parámetros variables, como muestra la tabla 1.2. Algunas tecnologías proporcionan comunicaciones de una sola dirección, mientras que otras ofrecen comunicaciones simultáneas en dos direcciones. Algunas operan a niveles de energía bajos, y otras operan a niveles de energía altos. Algunas son digitales y otras analógicas. Algunas operan a distancias cortas, y otras operan sobre distancias largas (incluso entre continentes).El coste de las distintas tecnologías inalámbricas puede variar desde unos cuantos € hasta millones.
Las tecnologías inalámbricas llevan entre nosotros muchos años. La televisión, la radio AM, FM, la TV por satélite, los teléfonos móviles, los dispositivos de control remoto, los radares, los sistemas de alarma y los teléfonos inalámbricos son algunas de las cosas completamente integradas en nuestra vida cotidiana. Algunas de las tecnologías beneficiosas que dependen de la tecnología inalámbrica son los sistemas de rada meteorológicos, los rayos X, los MRI, los hornos microondas y el GPS (Posicionamiento Global por Satélite).La tecnología inalámbrica rodea a la humanidad a diario, en los negocios y en la vida personal.

Frecuencia	Baja (Hz) a alta (Ghz)
Ancho de banda	Banda estrecha a banda ancha
Diálogo	Unidireccional a dúplex
Intervalo de señal	Corto(<30,5 m) a largo (miles de kilometros)
Tipo de señal	Digital o analógica
Ruta de la señal	Directa o reflexiva
Aplicaciones	Fija o móvil
Cobertura	Área local o amplia
Velocidad de datos	Baja (10 kbps) a alta (>10 Mbps)
Coste	Barato (<50 €) a cara (>miles de €)
Nivel de energía	Bajo(<1MW) a alto (>100000 W)

2.1.6. Tecnologías inalámbricas: digital y celular

Estas dos tecnologías se remontan a la década de 1940, cuando empezó la telefonía móvil comercial. La revolución inalámbrica empezó después de que aparecieran los microprocesadores económicos y la conmutación digital, y el clima regulador cambio para requerir un menor control sobre el equipo de transmisión de radio. La siguiente lista describe estas tecnologías:

- Terrestre: Esta categoría incluye los microondas y los infrarrojos, entre otros. El coste es relativamente bajo, y normalmente se necesita una línea visual.
- Tecnologías celulares móviles.
  - Primera generación (AMPS, CDPD). Estos sistemas principalmente analógicos utilizan señales eléctricas continuas para la transmisión y recepción de información, con velocidades de hasta 14,4 kbps.
  - Segunda generación (PCS). Estos sistemas digitales tienen varias ventajas, incluyendo una mejor cobertura, más llamadas por canal, menor interferencia por ruido y la posiblidad de añadir nuevas características y funciones, como la mensajería corta. Las velocidades pueden ser de hasta 64 kbps.
  - Tercera generación (WCDMA/IMT2000, CDMA2000). 3G es una tecnología móvil de banda ancha. Además de voz y datos, 3G envía audio y video a los dispositivos inalámbricos en cualquier parte del mundo. Las dos tecnologías 3G en competencia son CDMA de banda ancha y CDMA2000. Las velocidades pueden alcanzar los 2 Mbps.
- Otras tecnologías inalámbricas digitales
  - LMDS y MMDS. LMDS opera en 28 Ghz y ofrece una cobertura de línea de visión a distancias de hasta 5 Km, con velocidades que pueden alcanzar los 155 Mbps. Por termino medio, las velocidades son de aproximadamente 38 Mbps. MMDS opera de 2 a 3Ghz, con velocidades de transferencia que pueden llegar a los 27 Mbps, a distancias de hasta 48,2 Km. MMDS requiere licencia FCC.
  - OFDM. OFDM opera dentro del espectro U-NII y es utilizada por 802.11a. El espectro está localizado en 5,15 a 5,35 Ghz y en 5,725 a 5,825 Ghz. Las velocidades de transferencia pueden llegar a 54 Mbps.
  - DSSS y FHSS. DSSS y FHSS son tecnologías de espectro disperso utilizadas por las WLAN, incluyendo las 802.11b, y que operan a 11 Mbps. La cobertura de la línea de visión esta disponible hasta los 40 km.
- Satelite: Además de para entregar la señal de TV, los satelites tambien pueden servir a los usuarios de voz móviles y a los usuarios remotos que suelen estar lejos de los hilos o cables. El coste de los servicios por satelite es alto. Algunos tipos de satelites son LEO,MEO y GEO.

2.1.7. Legislación Wireless en España

La legislación de Wireless en España para el nivel de señal en transmisión es de 100mW para la frecuencia de 2,4 GHz y 1W para la frecuencia de 5,4 GHz. Esto quiere decir que si se emplean amplificadores que superen estas cantidades se estará incumpliendo esta normativa.
Podríamos definir las redes Wireless como un estándar desarrollado por la IEEE (Institute of Electrical and Electronic Engineers) que permite conectar dispositivos mediante una frecuencia de 2,4 Ghz o 5 GHz, con drivers que permiten comunicarse a través de los protocolos actuales de comunicación (TCP / IP), disponiendo cada dispositivo de una dirección única a nivel de Hardware (MAC address), y con una potencia de transmisión que va desde los 10-20 mW a los 100 mW (según la FCC / CEPT o la legislación de cada país).

2.1.8. Frecuencia en la que opera

Es un sistema de transmisión de datos inalambrico que utiliza la frecuencia 2'4 Ghz, que estaba libre de regulaciones y usos comerciales. Es una frecuencia cercana a la de los hornos microondas y de los telefonos inalámbricos domésticos.

2.1.9. Requisitos para tener una WIFI

La red WIFI tiene la ventaja de una fácil y rápida instalación sin los incovenientes de las incompatibilidades de dispositivos típicos de una red alámbrica. Una red en el hogar o en la empresa puede interconectar diversos dispositivos sin la necesidad de cableado y de una forma muy sencilla.
Dispositivos wireless:

- Punto de acceso (AP/PA): Se trata de un dispositivo que ejerce básicamente funciones de Puente entre una red Ethernet cableada con una red Wireless sin cables. Su configuración permite interconectar en muchos casos varios Puntos de Acceso para cubrir una zona amplia, pudiendo por si sólo proporcionar la configuración TCP / IP mediante un servicio DHCP. Se suele configurar en un único canal y admite la encriptación WEP, pudiendo enlazar un gran número de equipos entre ellos.
- Ordenadores de sobremesa : hay diversos dispositivos WIFI que se conectan a los ordenadores de sobremesa. Uno de los más comunes es el adaptador WIFI PCI.
- Ordenadores portátiles: por su movilidad son los que más provecho le sacan a este tipo de red.
- Dispositivos PDA

2.1.10. Resumen

- IEEE 802.11 especifica estándares para las WLANs. MAC y capa física (PHY) son servicios que han sido normalizados, utilizando los estándares 802.11 a, b, y g.
- La función principal de los adaptadores de clientes es transferir los paquetes de datos a través de la infraestructura inalámbrica. La instalación, la configuración y el monitoreo de las placas de interfaz de red (NICs) inalámbricas son siempre importantes.

2.2. Seguridad

2.2.1. Vulnerabilidades

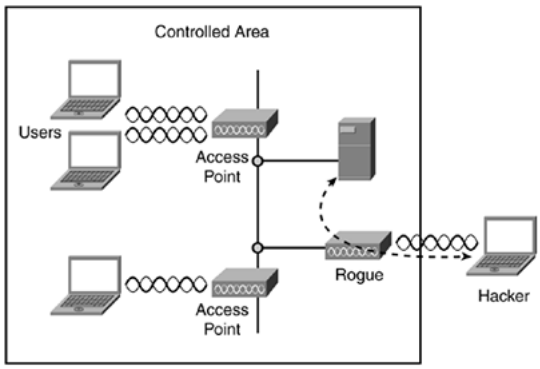
A continuación se muestran algunos de los problemas más comunes que presentan las redes inalámbricas desde el punto de vista de la seguridad.

2.2.1.1. Monitorización del tráfico

Uno de los posibles problemas de las redes inalámbricas consiste en la posibilidad de que un experimentado hacker o incluso un eventual sujeto pueda monitorizar los paquetes de una red inalámbrica mediante programas como *AirMagnet* o *AiroPeek*. Además este proceso puede ser llevado a cabo físicamente desde el exterior de la propia empresa siempre que se encuentre dentro del rango de la señal. Evidentemente esto supone que una cantidad enorme de información sensible puede ser visible por personas no autorizadas. Por tanto un elemento básico de seguridad consiste en la utilización de algún sistema de encriptación. Aún así existen métodos para obtener el acceso a la información cifrada, por ejemplo mediante los ataques de diccionario, que consiste en tener una base de datos con información de contraseñas para ir comparando con las posibles de la red analizada.

2.2.1.2. Accesos no autorizados

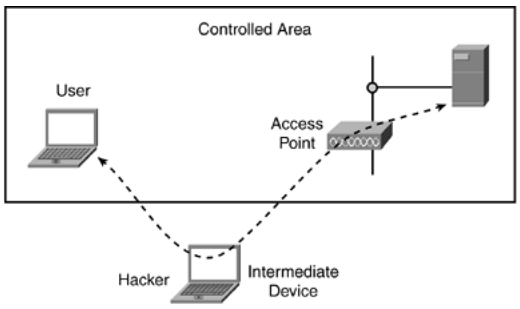
De igual forma que en el caso de la monitorización, usuarios no autorizados pueden acceder a una red corporativa desde fuera de las instalaciones de la misma. Sin las debidas medidas de protección cualquier persona puede acceder a la red de una empresa simplemente asociándose a cualquiera de los puntos de acceso disponibles, normalmente el más cercano al usuario. También existe la posibilidad de que un usuario de la red corporativa introduzca puntos de acceso desprotegidos (Rogue AP) en la red permitiendo, sin saberlo (o intencionadamente) el acceso al sistema. Hay que tener en cuenta que este problema puede afectar a redes tanto inalámbricas como cableadas.



Para poder evitar esta situación, es necesaria un proceso de identificación mutua, es decir que tanto el cliente como el servidor tienen que identificarse mutuamente.

2.2.1.3. Ataques del tipo Man-in-the-Middle

Si bien el uso de sistemas de encriptación aumentan la seguridad de las redes inalámbricas, todavía es posible encontrar vulnerabilidades basándose en el funcionamiento de las mismas. El problema del Man-in-the-Middle o literalmente "hombre en medio", consiste en la inserción de un dispositivo ficticio entre los usuarios y la red para tomar control del sistema. Por ejemplo, un caso típico de este tipo de problemas consiste en explotar el ARP, es decir el protocolo de resolución de direcciones que todas las redes TCP/IP utilizan.



Para entender como funciona esto veamos los mecanismos sobre los que se asienta el protocolo ARP. En una red local cada dispositivo de red o NIC tiene un identificador único llamado MAC. La MAC no es más que un número que sirve para identificar inequívocamente cada elemento de la red local. Por otra parte, dentro de redes más grandes cada dispositivo dispone de una dirección ip, que no es más que otro número identificativo. Para poder relacionar a ambos se creó el protocolo ARP o protocolo de resolución de direcciones. Cuando el tráfico ip llega a una red de área local cada paquete ip tiene que ser adaptado para que pueda ser correctamente redirigido en el interior de la red. En esta situación pueden ocurrir dos cosas:

- el router (o cualesquiera otro dispositivo de entrada a la red local) tiene guardado la dirección ip que orresponde a la dirección MAC y así envia el paquete al destino adecuado
- el dispositivo de entrada a la red local no dispone de esa información. En tal caso se procede a realizar un broadcasting por la red preguntando que máquina tiene la ip correspondiente.

Este proceso se realiza mediante la transmisión de una petición de ARP. Cuando una máquina determina que la ip solicitada es la suya simplemente responde con una respuesta ARP. De esta forma cuando el router recibe la respuesta este tiene la dirección MAC y la ip de la máquina que respondió guardando esta información en una cache. Cada máquina de la red mantiene su propia caché de ARP conteniendo las parejas ip-MAC. Desgraciadamente este protocolo es excesivamente sencillo ya que cualquier máquina puede responder a las peticiones del router sin ser necesariamente el auténtico destinatario de la información, es más, aún cuando no se ha realizado ninguna petición de ARP por parte del router una máquina que envía una respuesta provoca que las estradas de la caché de ARP se actualicen. Es decir, si una máquina malintencionada quiere realizar un ataque sólo tiene que enviar la respuesta de ARP al router para introducirse en el sistema. Si además al mismo tiempo envía otra señal a la máquina que se pretende suplantar para actualizar su caché con entradas falsas sobre el router ya tenemos un man in the middle. A continuación se muestran algunos de los tipos de ataques más comunes de tipo man-in-the-midle:

- ARP Poisoning (o ARP Spoofing)

  Es un ataque de MITM para redes ethernet, que permite al atacante capturar el tráfico que pasa por la LAN y también detenerlo (una denegación de servicio o DoS). El ataque consiste en enviar algunos mensajes ARP falsos. Estos frames ethernet contienen las direcciones MAC manipuladas según la conveniencia del atacante. Estos mensajes confunden a los dispositivos de red (principalmente a los switchs). Como resultado los frames de las víctimas son enviados al atacante o a un destino no válido en el caso de una "DoS". Este ataque puede ser prevenido/limitado utilizando entradas estáticas en las tablas ARP de los Hosts, usar Secure ARP, o usando tecnologías de seguridad en capa de acceso como port security (o seguridad por puertos que se verá más adelante), 802.1x, NAC Network Admission Control o NAP Network Access Protection. Hay algunas herramientas que permiten detectar este tipo de ataque (por ejemplo el arpwatch), estas escuchan el tráfico ARP que transita por la red LAN y alertan ante cambios sospechosos.

- Port Stealing (robo de puerto)

  En este ataque el atacante envía muchos frames ethernet (paquetes de capa 2), con la dirección MAC de la víctima como origen, y como destino su propia dirección MAC. Esto hace que el switch crea que la víctima está conectada en el puerto del atacante (de ahí el nombre de esta técnica). Cuando el atacante recibe un paquete destinado a la víctima, este genera un ARP request preguntando por la MAC asociada a la IP de la víctima. Cuando la víctima responde el switch vuelve a conocer en donde está ubicada realmente la víctima, es entonces cuando el atacante reenvía el paquete recibido (intacto o modificado, dependiendo de los intereses del atacante). Luego vuelve a robar el puerto y espera por el próximo paquete con destino a la víctima. Esta técnica degrada la conectividad de la víctima notablemente y es fácilmente detectable por los IDS.

- DNS spoofing

  El protocolo DNS Domain Name System convierte nombres en direcciones IP (por ej.: www.google.com a 64.233.161.147) y también la resolución inversa. Este ataque utiliza respuestas falsas a las peticiones de resolución DNS (los request) enviadas por una víctima. Hay dos métodos en los que puede basarse el atacante: DNS ID Spoofing y Cache poisoning (envenenamiento de la cache). El método ID Spoofing se basa en obtener el ID de las peticiones de resolución, el atacante puede lograr esto a través de algún ataque de sniffing, como por ejemplo desbordar la tabla ARP MAC Flooding de los switchs para ponerlos en un modo conocido como failopen (esto los transforma en un HUB). Siendo capaz de escuchar los ID de las peticiones, el atacante intenta responder a estas antes que el servidor real, logrando de esta forma engañar a la víctima y llevarla así al destino que desee. El método Cache poisoning es similar al anterior, salvo que se dirige a los servidores de cache de DNS, redirigiendo así a todos sus clientes al host que indique el atacante. Dado que existe este ataque se vuelve muy importante que los servidores de caché de DNS hagan sus consultas utilizando ID aleatorios. Los IDS son capaces de detectar este tipo de ataque y una medida de prevención podría ser cargar el archivo lmhost (en windows) y /etc/hosts (en linux), para los dominios corporativos.

- DHCP Spoofing

  Las requerimientos de DHCP son hechos con frames de tipo broadcast, ya que deben ser escuchados por todos los dispositivos dentro de la red local. Si un atacante responde antes que el verdadero servidor, este puede pasarle información errónea a la víctima, como por ejemplo puede decirle que la puerta de enlace es él. Para algunos servidores de DHCP suele ser bastante sencillo responder antes que él, debido a que muchos verifican si no hay otro dispositivo en la red con la dirección que van a entregar; mientras el servidor real comprueba, el atacante tiene tiempo valioso en el que puede responder antes. Los IDS detectan este ataque debido a que se producen múltiples respuestas para una única solicitud.

- Denegación de servicio. (DoS)

  El fin de esta vulnerabilidad no es introducirse en la red sino dejarla totalmente inoperativa, es por tanto uno de los más graves problemas de este tipo de redes si bien no exclusiva de ellas. El impacto de un ataque de este tipo dependerá como es natural de las circunstancias del atacado. En el caso de un usuario doméstico este tipo de ataque no supondrá más que una molestia pero en el caso de una empresa podemos estar hablando de millones en pérdidas económicas. Una forma de ataque de tipo DoS consiste en el método de la fuerza bruta. El proceso consiste en enviar una gran cantidad de paquetes utilizando todos los recursos de la red, obligando a esta a apagarse. También es posible enviar paquetes basura, esto es, sin ninguna utilidad pero que obligan al servidor a procesar una gran cantidad de paquetes lo que normalmente supone una disminución del ancho de banda disponible para los usuarios legítimos o bien directamente la caida del sistema.

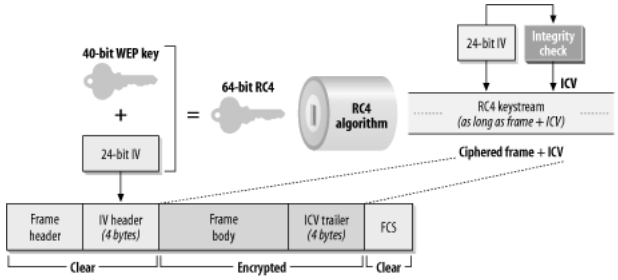
2.3. WEP

2.3.1. Funcionamiento

Este acrónimo refiere, literalmente a *seguridad equivalente a un sistema cableado* (*wired equivalent privacy*), y es uno de los protocolos sobre las redes inalámbricas 802.11 que más se ha utilizado a pesar de ser un sistema de seguridad que está claramente superado. De hecho es muy fácil romper la seguridad en este tipo de redes. Aún así, para entornos domésticos en los que la seguridad no sea un requisito imperativo puede ser un sistema sencillo y simple de obtener un grado aceptable de seguridad.
El modo de funcionamiento de WEP se aplica sobre la capa MAC del sistema. En primer lugar se genera una semilla.
Ésta está formada por dos elementos:

- la clave que proporciona el usuario (Key) que normalmente se introduce como una cadena de caracteres o de valores hexadecimales Esta clave ha de estar presente tanto en el receptor como en el emisor por lo que es necesario introducirla manualmente en los mismos.
- un vector de 24 bits (IV, o vector de inicialización) generado aleatoriamente que además puede cambiar en cada frame. Las semillas más habituales son de 64 bits o de 128 bits (algunos vendedores lo llaman WEP2).

Una vez generada la semilla es suministrada a un generador de números pseudoaleatorios formando una cadena de longitud igual al payload del frame más una parte de comprobación de la integridad de los datos de 32 bits (ICV). Este proceso se lleva a cabo mediante un algoritmo de cifrado llamado RC4. Finalmente se combinan la clave de cifrado generada (keystream) con el payload/ICV mediante una operación xor. Dado que para poder desencriptar es necesario disponer de los bits de IV, éstos son transmitidos sin encriptar en el propio frame



2.3.2. Problemas

Por un lado, las claves de usuario son estáticas lo que implica que todos y cada uno de los usuarios tienen que usar la misma clave. Este hecho suele provocar que las claves no se cambién durante meses o incluso años, facilitando su obtención. Por otra parte el hecho de que el IV se transmita sin encriptar y de que se pueda repetir cada cierto tiempo, además de que el algoritmo que genera este vector presenta ciertos caracteres de predictibilidad , hace que sea un sistema perfecto para romper por la fuerza bruta.
Algunos de los tipos de ataques son:

- Ataques pasivos basados en el análisis de paquetes para intentar descifrar el tráfico.
- Ataques activos basados en la introducción de paquetes.
- Ataques activos basados en el ataque/engaño al punto de acceso
- Ataques de diccionario.
- *etc.*

El ISAAC (Internet Security, Applications, Authentication and Cryptography) hizo un estudio minucioso acerca de los problemas y debilidades de WEP llegando a las siguientes conclusiones generales:

1. El manejo de las claves es una fuente constante de problemas. Para empezar el hecho de tener que distribuir la misma clave a todos los usuarios implica que este proceso se tiene que realizar un mismo día en un momento determinado, teniéndose que cambiar de nuevo si un usuario abandona la empresa o lugar en donde se utilicen la red WEP. Las claves que se distribuyen por todo el sistema y que se guardan con esmero tienden a ser publicas con el tiempo. Los ataques de Sniffing se basan sólo en obtener la clave WEP que es cambiada infrecuentemente.

2. Una longitud de claves de 64 o 128 bits no es hoy en día suficiente para garantizar un buen nivel de seguidad.

3. Los algoritmos de cifrado son vulnerables al análisis si se utiliza frecuentemente los mismos keystreams. Dos frames que usan el mismo IV usaran casi con toda probabilidad la misma key y por tanto el mismo keystream.

4. El cambio infrecuente de las claves permite a los atacantes usar las técnicas de ataque por diccionario

5. WEP utiliza CRC para garantizar la integridad de los frames enviados. Aunque el CRC es encriptado por el algoritmo de RC4, los CRC no son criptográficamente seguros.

2.3.3. Variantes

Existen algunas variantes que básicamente se basan en intentar mejorar el IV, por ejemplo aumentándolo en tamaño. Así tenemos:

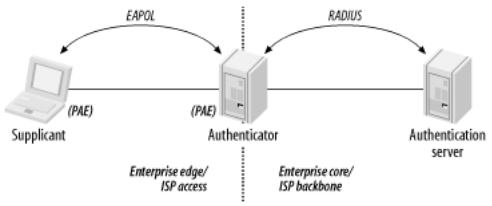
- WEP2: se trata del mismo sistema en esencia y sus únicas diferencias consisten en un mayor tamaño del IV y una protección de encriptación de 128 bits.

- WEP+: consiste en una variante propietaria de la empresa Lucent Technologies que se basa en la eliminación de los IV "debiles". Para ser efectivo debe de utilizarse tanto en el emisor como en el receptor. Dado que es una tecnología propietaria no existen muchos fabricantes que lo integren y por tanto no presenta de una gran disponibilidad.

2.4. 802.1X

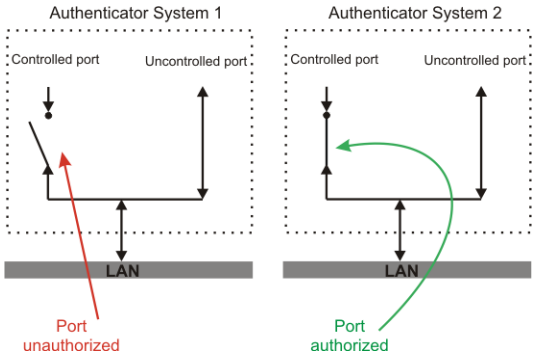
2.4.1. Funcionamiento

El IEEE 802.1X es un estándar de la IEEE basado en el control de acceso a redes mediante puertos y es parte de la familia de protocolos 802.1. El protocolo utiliza un framework de autentificación (EAP) que permite a un usuario ser identificado por una unidad central de control. De forma simplificada se puede decir que este protocolo es simplemente un estándar para hacer pasar EAP sobre redes cableadas o inalámbricas.

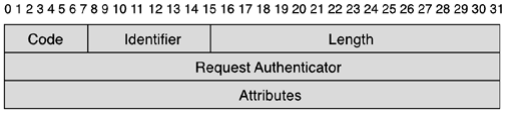


El estándar define tres entidades, el supplicant o cliente que busca acceso a los diferentes recursos de la red, el Authentificator (en adelante "AT" para abreviar) que se encarga de controlar el acceso a la red y por último del Authentification sever, que se encarga del proceso de autentificación. Tanto el cliente como el AT son elementos de tipo PAE (Port Authentication Entities), es decir literalmente, entidades de autentificación del puerto. Los cuales pueden estar en estado de autorización o desautorización. El proceso de autentificación se lleva acabo entre el cliente y el servidor de autentificación siendo la función del AT la de puente entre los dos. Así tenemos que entre el cliente y el AT se usa el protocolo EAP sobre redes inalámbricas o EAPOW (EAPOL, para redes cableadas) y entre el AT y el servidor de autentificación se utiliza el protocolo RADIUS, también conocido como EAP sobre RADIUS.

El concepto de puerto es importante en el protocolo 802.1x ya que basa su funcionamiento en los mismos. Un puerto no es más que una entidad virtual con la que debe tratar el AT o autentificador. Existen dos puertos virtuales, los puertos controlados y los no controlados. Antes de que se produzca la autentificación el único tráfico permitido es el EAPOW (EAPOL, para redes cableadas) mediante el puerto no controlado. Cuando se produce la autentificación por el servidor se habilita o autoriza el puerto controlado permitiéndose acceso a los recursos de la red.



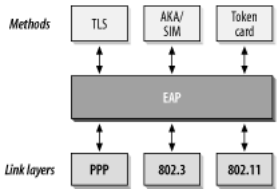
El protocolo RADIUS definido formalmente en [RFC2865] y creado por la empresa Livingston Enterprises, significa literalmente Remote Authentication Dial In User Service, es decir servicio de usuario de autentificación remoto y es un protocolo de tipo AAA (authentication, authorization and accounting), es decir, realiza tres acciones: autentificación, autorización y recuento para aplicaciones de acceso a redes. Esta pensado para situaciones locales y con roaming. RADIUS usa como sistema de transporte UPD y es considerado como un servicio de tipo no orientado a la conexión con una estructura cliente / servidor, donde el cliente suele ser el AT o un NAS (servidor de acceso a la red) y el servidor, el propio servidor RADIUS.



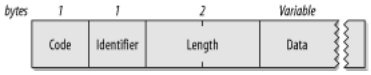
Como hemos dicho el servidor RADIUS realiza tres acciones básicas: autentificaciones, autorizaciones y recuentos. Una vez que el cliente ha proporcionado sus datos de identificación, como contraseñas y nombres de usuario u otras, para las autentificaciones pueden utilizarse un gran número de sistemas diferentes que dependerán en gran medida de lo que implemente el fabricante, ejemplos pueden ser CHAP, UNIX login etc. El proceso de autorización se realiza junto con el de autenticación, si la contraseña se encuentra en la base de datos el servidor RADIUS devuelve un mensaje de aceptación con un conjunto de parejas atributo / valor sobre la sesión iniciada, como pueda ser ip, tipo de protocolo etc. Finalmente el recuento puede realzarse de forma independiente a la autorización y autntificación. Las funciones de recuento pueden monitorizar diferentes aspectos como intervalos de tiempo de sesiones, número de paquetes etc.

Dado que el protocolo 802.1X basa su funcionamiento en EAP (Extensible Authentication Protocol), es necesario explicar el funcionamiento del mismo. EAP está formalmente especificado en el [RFC

2284] y fue inicialmente desarrollado para ser usado con PPP (Point-to-Point Protocol), un protocolo de acceso a redes mediante modems telefónicos, que también es usado por algunos ISP para la autentificación en DSL y cable modems bajo la forma de PPP sobre ethernet. PPP usado como sistema de acceso a redes mediante modems telefónicos permite la autentificación de los usuarios a través del uso de un doblete nombre_usuario / contraseña. Este sistema básico de autentificación era insuficiente en los entornos empresariales, máxime cuando comenzó a ser utilizado en acceso DSL, surgiendo EAP. En general, EAP es una forma de encapsular los diferentes tipos de sistemas de autentificación. Además EAP puede funcionar sobre cualquier tipo de protocolo de la capa de enlace como PPP o en nuestro caso el 802.11 de las redes inalámbricas.



Paquete Eap



Así pues, el protocolo 802.1X, no es más que un protocolo que encapsula a otro, el EAP. En terminos generales el proceso de funcionamiento del sistema 802.1x es el siguiente:

1. El cliente envía un mensaje de inicio tan pronto como el AT detecta que el enlace está activo (por ejemplo, el cliente se asocia a un punto de acceso) provocando una serie de mensajes para verificar la autenticidad del cliente.

2. El punto de acceso, esto es el AT, responde con un mensaje de petición de identidad.

3. El cliente envía una respuesta indicando la información de identidad para el servidor de autentificación. El AT envía esta información al servidor de autentificación

4. El servidor de autentificación utiliza un algorismo para verificar la identidad del cliente. Este proceso se puede realizar mediante el uso de certificados o cualquier otro sistema de autentificación de EAP.

5. El servidor de autentificación enviará un mensaje de éxito o rechazo al AT.

6. El AT envía al cliente un mensaje de éxito o rechazo al cliente, permitiéndole tener o no acceso a la red modificando el estado del cliente a autorizado.

2.4.2. WPA/WPA2

Funcionamiento

Su nombre proviene del acrónimo WPA, Wireless Protected Access (acceso inalámbrico protegido) y tiene su origen en los problemas detectados en el anterior sistema de seguridad creado para las redes inalámbricas. La idea era crear un sistema de seguridad que hiciera de puente entre WEP y el 802.11i (WPA2), el cual estaba aun por llegar. Para ello utiliza el protocolo TKIP (Temporal Key Integrity Protocol) y mecanismos 802.1x. La combinación de estos dos sistemas proporciona una encriptación dínámica y un proceso de autentificación mutuo. Así pues, WPA involucra dos aspectos: un sistema de encriptación mediante TKIP y un proceso de autentificación mediante 802.1x.

Cuadro 2.1: Modos de funcionamiento de WPA/WPA2

	WPA	WPA2
Modo Enterprise	Autentificación: 802.1x / EAP Encriptación: TKIP / MIC	Autentificación: 802.1x / EAP Encriptación: AES-CCMP
Modo Personal	Autentificación: PSK Encriptación: TKIP / MIC	Autentificación: PSK Encriptación: AES-CCMP

El proceso de encriptación es similar al realizado en WEP, pero contiene varias aspectos diferenciados. Para empezar, si bien TKIP usa el algoritmo RC4 proporcionado por RSA Security para encriptar el cuerpo del frame así como el CRC[6] antes de la transmisión, en este caso se utilizan IV[7] de 48 bits, lo que reduce significativamente la reutilización y por tanto la posibilidad de que un hacker recoja suficiente información para romper la encriptación. Por otro lado y a diferencia de WEP, WPA automáticamente genera nuevas llaves de encriptación únicas para cada uno de los clientes lo que evita que la misma clave se utilice durante semanas, meses o incluso años, cómo pasaba con WEP. Por último WPA implementa lo que se conoce como MIC (message integrity code o en español código de integridad del mensaje) introducido por TKIP al final de cada mensaje de texto plano. Recordemos que WEP introduce unos bits de comprobación de integridad (ICV) en el payload del paquete. Desgraciadamente es relativamente fácil, a pesar de que los bits de ICV también se encriptan, modificarlos sin que el receptor lo detecte. Para evitarlo se hace uso del MIC (8 bytes, Message Integrity Check también conocido cómo Michael), un sistema de comprobación de la integridad de los mensajes, que se instala justo antes del ICV.

Para el proceso de autentificación WPA y WPA2 usan una combinación de sistemas abiertos y 802.1x. El funcionamiento es igual al ya comentado en el apartado del 802.1x. Inicialmente el cliente se autentifica con el punto de acceso o AT, el cual le autoriza a enviarle paquetes. Acto seguido WPA realiza la autentificación a nivel de usuario haciendo uso de 801.1x. WPA sirve de interfaz para un servidor de autentificación como RADIUS o LDAP. En caso de que no se disponga de un servidor de autentificación se puede usar el modo con PSK. Una vez se ha verificado la autenticidad del usuario el servidor de autentificación crea un pareja de claves maestras (PMK) que se distribuyen entre el punto de acceso y el cliente y que se utilizarán durante la sesión del usuario. La distribución de las claves se realizará mediante los algoritmos de encriptación correspondientes TKIP o AES con las que se protegerá el tráfico entre el cliente y el punto de acceso.

WPA2 fue lazado en septiembre de 2004 por la Wi-Fi Alliance. WPA2 es la versión certificada que cumple completamente el estándar 802.11i ratificado en junio de 2004. Análogamente a WPA presenta dos vertientes: la autentificación y la encriptación de datos. Para el primer elemento utiliza 802.1x / EAP o bien PSK. Para la encriptación se utiliza un algoritmo que mejora a TKIP, el algoritmo AES. Cada uno de los sistemas puede funcionar de dos formas diferentes en función de los recursos y necesidades, el modo personal, pensado para pequeñas empresas o usuarios domésticos y el modo empresarial. En la tabla 2.1 se muestran las dos posibilidades.

En el modo empresarial (enterprise) el sistema trabaja asignando a cada usuario una única clave de identificación, lo que proporciona un alto nivel de seguridad. Para la autentificación el sistema utiliza el ya comentado 802.1x y para la encriptación el algoritmo AES. Para el funcionamiento en la versión personal, se utiliza una clave compartida (PSK) introducida manualmente por el usuario tanto en el punto de acceso como en las máquinas cliente, utilizándose para la encriptación TKIP o AES. En este sentido las diferencias con WEP se basan en el algoritmo de cifrado de los datos.

[6] Códigos cíclicos también denominados CRC (Códigos de Redundancia Cíclica) o códigos polinómicos.
[7] Vector de inicialización.

Problemas

Desgraciadamente WPA no está exento de problemas. Los más importantes siguen siendo los DoS (ataques de denegación de servicio). Si alguien envía dos paquetes consecutivos en el mismo intervalo de tiempo usando una clave incorrecta el punto de acceso elimina todas las conexiones de los usuarios durante un minuto. Este mecanismo de defensa utilizado para evitar accesos no autorizados a la red puede ser un grave problema.

2.4.3. Otras medidas

Otras medidas que se pueden utilizar en conjunción con los diferentes sistemas de seguridad son:

Filtrado de direcciones MAC: aunque no es una práctica que implique un aumento elevado en la seguridad del sistema, es un extra que añade un nivel más de seguridad de cara a posibles atacantes casuales y es en todo caso recomendable, si bien no supondrá ningún impedimento para hackers profesionales ya que hoy día es muy fácil modificar las dirección MAC de un dispositivo.

Ocultación del nombre de la red (ESSID): de nuevo, es una medida más que es aconsejable tomar a la hora de implementar una política de seguridad a nuestra red inalámbrica, pero, y de forma equivalente al caso anterior, en ningún caso supone graves complicaciones para hackers experimentados.

Capítulo 3

Aplicaciones y perspectiva de futuro

En este capítulo se muestra **dónde** se aplica la tecnología WiFi actualmente y dónde podría aplicarse en un futuro cercano.

3.1. Aplicaciones

Los primeros entornos que adoptaron la tecnología inalámbrica se hallaban inmersos en mercados verticales. Estos usuarios estaban más preocupados por la movilidad que por los estándares o el throughput (productividad). Sin embargo la tendencia ha ido cambiando y, hoy en día, los usuarios se están orientando más hacia los mercados denominados horizontales dónde la movilidad no es tan relevante cómo la interoperabilidad y la productividad. Con los productos WLAN 802.11a, 802.11b y 802.11g, la movilidad y el roaming[1] no tienen que ser sacrificados para ganar en productividad e interoperabilidad. Sin embargo, elegir la tecnología WLAN correcta es decisivo y dependerá de la aplicación concreta y de la infraestructura de que dispongamos.

Los dispositivos WLAN se encuentran en el mercado desde hace una década pero, en los últimos años, la tecnología se ha popularizado gracias a un conjunto de claves que se explican detenidamente a continuación.

3.1.1. Claves del desarrollo

1. La IEEE garantiza la compatibilidad entre equipos de diferentes fabricantes. Anteriormente los dispositivos de diferentes fabricantes presentaban problemas a la hora de su interoperación, lo que hacía que las redes se construyesen en base a soluciones mono-fabricante lo que limitaba su uso y ampliación dramáticamente.

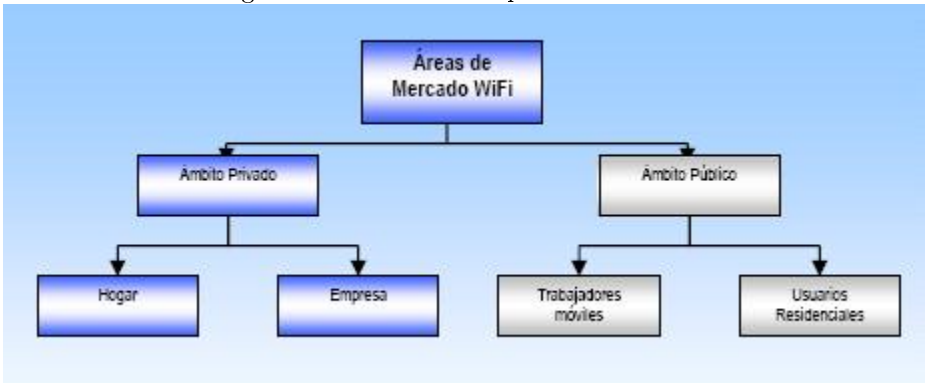
2. Los precios de este tipo de equipamientos se han reducido drásticamente, siendo en muchos casos más interesante una solución WLAN que una solución cableada o "wired". En edificios con alto valor histórico, sin infraestructura de red cableada o dónde la movilidad es un valor añadido, la solución WLAN puede superar a la solución cableada o incluso ser la única alternativa viable.

3. Fabricantes de ordenadores y PDAs comienzan a incluir de serie la tecnología WiFi. Esto provoca que WiFi se haya convertido en una buena alternativa para la interconexión de dispositivos. Fabricantes cómo INTEL incorporan esta tecnología de forma habitual.

4. Los dispositivos de comunicaciones móviles comienzan a incluir WiFi de serie, lo que abre una gran incógnita respecto al desarrollo que WiFi puede llegar a alcanzar. Si los teléfonos móviles

[1] La itinerancia (en inglés, y popularmente, roaming) es un concepto utilizado en comunicaciones inalámbricas que está relacionado con la capacidad de un dispositivo para moverse de una zona de cobertura a otra.

Figura 3.1: Ámbitos de aplicación de WiFi



llegan a utilizar WiFi para las conexiones de banda ancha, las previsiones de uso de WiFi pueden verse sobrepasadas en gran medida.

5. El hecho de utilizar una banda de frecuencias considerada "libre", ha abierto expectativas en el uso de WiFi cómo un método viable para desarrollar servicios de acceso a Internet en lugares públicos.

3.1.2. Oportunidades para las pymes

Las PYMES (pequeñas y medianas empresas) pueden beneficiarse de la tecnología WiFi en dos ámbitos:

1. Cómo usuarios.
2. Cómo proveedores de servicios .

Son muchas las aplicaciones de WiFi, y únicamente la imaginación pone límites a la innumerable lista de aplicaciones posibles. Las PYMES relacionadas con el mundo de las tecnologías de la información y las telecomunicaciones podrán beneficiarse de la tecnología WiFi desde la doble vertiente de usuarios y proveedores de soluciones. El resto de PYMES se beneficiaran fundamentalmente como usuarios WiFi. A continuación se describen diversos ámbitos de aplicación de las tecnologías WiFi. En cada aplicación se muestran los usuarios y los proveedores de la tecnología.

3.1.3. Aplicaciones

La figura 3.1 refleja los ámbitos de aplicación de la tecnología WiFi.

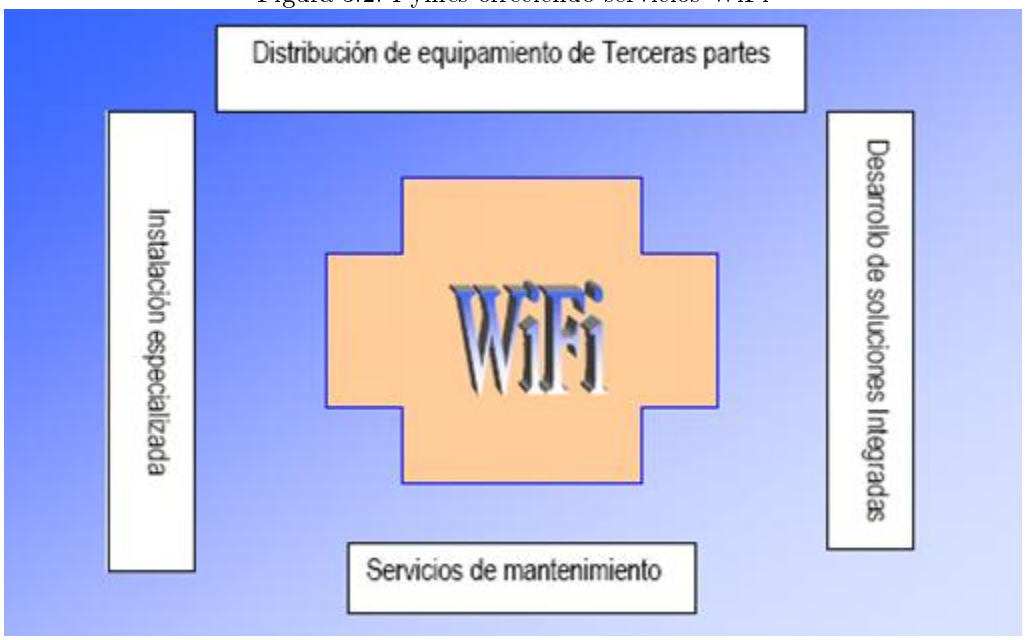
Cómo ya se ha indicado, inicialmente WiFi fue ideado para aplicarse como LAN inalámbrica dentro de un ámbito privado, tanto para hogares cómo para empresas. El desarrollo posterior ha abierto expectativas en cuánto a su aplicación en entornos públicos.

Las PYMES, actuando como proveedoras de esta tecnología pueden adoptar distintos perfiles en la cadena de valor[2].

Una red pública WiFi para el acceso a Internet recibe el nombre de **PWLAN** (Public Wireless LAN); la compañía proveedora de servicios de conxión a Internet se conoce cómo **WIPS** (Wireless Internet Service Provider). Los lugares desde dónde se presta el servicio se denominan **hot spots** públicos y suelen ocupar lugares estratégicos cómo son aeropuertos, hoteles, estaciones de ferrocarril, restaurantes y otras ubicaciones con una densidad de personas considerable. Su mercado objetivo es

[2]La cadena de valor categoriza las actividades que producen valor añadido en una organización. Se dividen en dos tipos de actividades, primarias y secundarias.

Figura 3.2: Pymes ofreciendo servicios WiFi



el formado por los denominados **trabajadores móviles**, es decir, aquellos empleados que pasan gran tiempo fuera de su oficina y que utilizan Internet cómo parte de su trabajo diario. El tendencia en el desarrollo de hot spots públicos va creciendo en el mundo aunque la viabilidad comercial de estas iniciativas aún no está completamente demostrada. Podemos encontrar hot spots gratuitos, dónde la entidad que gestiona el espacio decide desplegar una infraestructura WiFi y ofrecer el servicio cómo un servicio de valor añadido a su oferta empresarial (si no se trata de una entidad pública o sin ánimo de lucro). Es el caso de ciertas cafeterías, hoteles, bibliotecas y universidades. En otras ocasiones es un WISP quién presta el servicio bajo una modalidad de pago. Cómo ejemplo de desarrollo de hot spots se proponen las siguientes direcciones:

- *http://www.austinwirelesscity.org*
- *http://www.afitel.com/afitel/DesktopDefault.aspx*

Centrándonos en el uso privado de WiFi, en los siguientes apartados se muestran ciertas aplicaciones frecuentes.

3.1.3.1. Aplicaciones en el hogar

WiFi aparece en el hogar cómo alternativa al "home networking"; su utilización permite la interconexión de diferentes dispositivos de forma inalámbrica bajo un mismo estándar y de una forma sencilla y económica. A medida que el acceso a Internet de banda ancha se ha popularizado, el hogar se ha convertido en un espacio de ocio y trabajo. Por tal motivo el acceso a Internet se ha hecho más necesario y la necesidad de un acceso compartido entre varios ordenadores de forma simultánea se ha convertido en una necesidad. Para resolver lo anterior muchos los fabricantes de dispositivos han integrado en un único equipo un punto de acceso WiFi, un módem ADSL/cable y un router. Así pues, la plataforma de "hogar digital" se basa actualmente en WiFi cómo uno de los medios de interconexión de dispositivos.

Cada día son más los hogares que disponen de multitud de dispositivos que deben ser compartidos cómo es el caso de impresoras, discos duros y un largo etcétera. El acceso a contenidos digitales

se ha convertido en algo muy común: música, vídeo y fotografías están muy presentes en nuestros hogares. Diversos fabricantes están desarrollando nuevos equipos relacionados con el ocio con WiFi cómo estándar. Es el caso de los nuevos equipos de música que, además de características estándar cómo reproducción de DVDs, rádio, y otras, son capaces de conectarse a otras fuentes de audio codificado en MP3, tanto en una red local cómo a servidores de Internet a través de un acceso de banda ancha.

Actualmente las consolas de videojuegos son otros dispositivos que participan en la red local. Su conexión a Internet es ya una realidad y los videojuegos que utilizan características en red son cada día más demandados. Además de las videoconsolas otros dispositivos y electrodomésticos han dado el salto para utilizar tecnologias de red lo que ha propiciado una serie de nuevos entornos:

1. Juegos multijugador en red, utilizando vídeoconsolas (además de ordenadores).
2. Descarga de juegos a la carta.
3. Contratación de juegos "on line".
4. La televisión digital interactiva precisa de un canal de retorno para sus aplicaciones, WiFi se presenta cómo una alternativa sin hilos. En los próximos años aparecerán en el mercado equipos set top box WiFi que permitirán, desde un punto cercano al televisor, realizar este tipo de comunicaciones interactivas.
5. Modelos híbridos de televisión. Están apareciendo dispositivos híbridos que ofrecen contenidos vía satélite o mediante televisión digital terrestre en combinación con una conexión inalámbrica a Internet, ya sea vía ADSL o mediante cable. Este tipo de servicio permite el uso de aplicaciones interactivas, acceso a contenidos multimedia, así cómo servicios de vídeo por demanda accedidos a través de conexiones de banda ancha.
6. Distribución vídeo y audio digital internamente en el hogar. Los estándares IEEE802.11 utilizados en algunos equipos comerciales, permiten unas velocidades cercanas a los 54 Mbps, haciendo posible la distribución de señales de audio y vídeo digital con niveles de calidad más que aceptables.

Los operadores de telecomunicaciones que pretendan potenciar el desarrollo del nuevo consumo digital, deberán promover soluciones atractivas en el campo de las redes de acceso local con un soporte total para los requisitos básicos de movilidad, facilidad de conexión de los dispositivos, economía e interoperabilidad del estándar.

Aproximadamente un 51 % de los hogares "digitales", entendiéndose cómo tales aquellos con una conexión a Internet de banda ancha, que consumen contenidos digitales de forma habitual, están interesados en conectar la televisión a contenidos multimedia locales y de Internet. Del 51 % anterior, un 7 % ya ha realizado la conexión con sus contenidos locales. En los hogares españoles cada día se dispone de un mayor equipamiento digital. Así nos encontramos con una tasa de PCs que se aproxima al 40 %, lo que supone aproximadamente unos 6,5 millones de hogares con uno o más ordenadores.

El acceso a Internet en los hogares españoles ha experimentado un crecimiento considerable durante los últimos años, consiguiéndose un nivel en torno al 30 %. En cuanto al tipo de conexión, la banda ancha ha ganado el terreno a las conexiones RTB. De entre los hogares conectados a Internet con más de un ordenador (el 26 % del total de hogares) la mayoría, un76 %, disponen únicamente de un ordenador. Sin embargo, la renovación del parque de ordenadores, así cómo la necesidad de compartir la conexión a Internet ha provocado que las necesidades de conectividad en el hogar hayan aumentado. En cuánto al tipo de red utilizada un 57 % utiliza ethernet y sólo un 6 % utiliza WiFi. Es importante resaltar la falta de información sobre este tipo de tecnologías de conectividad LAN, ya que el 13 % de los encuestados no ha sido capaz de clarificar la tecnología que usaba. En cuánto a la cuantificación de la banda ancha en España el número de hogares conectados supera el millón trescientos mil, frente a las empresas que alcanzan un total de seiscientas mil, a finales del 2003. En una situación de mercado dónde el hogar digital es cada día una realidad más fehaciente y dónde la conexión a Internet de banda

Figura 3.3: Clientes, proveedores y dispositivos WiFi

Clientes potenciales:	Hogares del mercado residencial con uso de tecnología digital y banda ancha
Proveedores:	PYMES especializadas en el desarrollo e integración de soluciones para el hogar digital.
Dispositivos:	Ordenadores, tarjetas PCMCIAs, Adaptadores USB, Modems Routers, GAteWay Media Placer, vídeoconsolas, equipos HiFi,.

Figura 3.4: Redes ciudadanas

Clientes potenciales:	Jóvenes aficionados a la informática y telecomunicaciones, dentro y fuera del ámbito universitario
Proveedores:	PYMES la distribución y venta de equipamiento WiFi
Dispositivos:	Ordenadores, Antenas, routers, Puntos de Acceso, Bridges, tarjetas PCMCIAs, Adaptadores USB,...

ancha se ha desarrollado por encima de las conexiones tradicionales, las aplicaciones de conectividad WiFi en el hogar suponen un importante mercado actualmente y previsiblemente en los próximos años.

Redes ciudadanas

Estas iniciativas tratan de crear una oferta de acceso a Internet, proporcionando acceso a los ciudadanos. En España es muy poco probable que se desarrolle, dado que una red estable y de calidad precisa de unas inversiones y unos servicios de mantenimiento considerables. Compatibilizarlo con un coste cero para los usuarios parece bastante complicado. Las experiencias hasta el momento dentro de este campo han sido incapaces de establecer un verdadero modelo de negocio que haga viable su explotación.

Son diversas las iniciativas en marcha actualmente, que recuerdan a los primeros radioaficionados de la banda del 27 Mhz. Cómo ejemplo, estos grupos utilizaban la radio de forma gratuita y libre, pero tuvieron que ser los operadores de telecomunicaciones los que desarrollaron el servicio de telefonía móvil que conocemos hoy en día. Éstos poseían capacidad financiera suficiente cómo para desarrollar un modelo de negocio sostenible y ofrecer un servicio al usuario final con suficientes garantías en términos de calidad de servicio.

3.1.3.2. Wifi en la empresa

WiFi aparece cómo una *extensión inalámbrica* de las redes de área local en las empresas. En la empresa, una solución de red basada en WiFi presenta una serie de ventajas e inconvenientes. Las ventajas son claras:

1. Movilidad de los equipos.
2. Ausencia de cableado.
3. Libertad en los cambios organizativos.

Figura 3.5: WiFi en la empresa

Figura 3.6: WiFi en la empresa

Clientes potenciales:	Empresas con equipamiento informático y LANs.
Proveedores:	PYMES la distribución y venta de equipamiento WiFi
Dispositivos:	Ordenadores, tarjetas PCMCIAs, Adaptadores USB, Puntos de Acceso, MODEM router Cables/ADSL, VPNs ...

4. Acceso a la red independientemente del puesto de trabajo .

Si el tráfico es medianamente alto la *solución cableada* es superior, dado que en un punto de acceso se concentran, en general, las comunicaciones de todos los usuarios y el caudal se reparte entre los usuarios simultáneamente. No obstante, la aparición de dispositivos como el 802.11g, así como dispositivos "duales" 802.11 b y g, modifican este escenario permitiendo alcanzar velocidades del orden de 50 Mbps. La *solución mixta* wireless-cableado es en muchos casos la más adecuada para una empresa, dado que parte de la LAN se despliega de forma cableada y la WLAN es un complemento a la red ya existente. En general las empresas disponían de una red cableada con anterioridad.

Paralelamente, diversos fabricantes están promoviendo soluciones IP para las redes empresariales. En muchas ocasiones, estas soluciones integran las comunicaciones de voz y datos sobre la misma plataforma. La solución de red que se plantea es completamente IP, la PABX[3] tradicional desaparece físicamente y pasa a ser sustituída por una aplicación software y un equipamiento de conexión a las líneas de voz tradicional. Otras veces, este equipamiento es remoto y es ofrecido cómo una solución desde la red. WiFi aparece cómo un complemento inalámbrico para este entorno, se ofrecen conexiones de datos así como de voz IP sobre WiFi. Los terminales inalámbricos de voz de la empresa pasan a ser WiFi y a integrarse en la red local.

Las empresas en España se han modernizado en los últimos años y la gran mayoría ha adoptado al ordenador cómo una herramienta imprescindible. Estas empresas normalmente disponen de su propia red informática, pudiendo contar con varias sedes e incluso con teletrabajadores; este tipo de empresas son las más propicias para la expansión total de WiFi.

Investigando sobre áreas de aplicabilidad y posibles negocios dónde puede utilizarse WiFi, queda claro que, hoy por hoy, la aplicación de la tecnología WiFi no tiene unos límites definidos, todo lo que

[3] Un PBX o PABX (siglas en inglés de Private Branch Exchange y Private Automatic Branch Exchange para PABX) es una central telefónica pertenciente a una empresa.

Figura 3.7: WiFi en el teletrabajo

Clientes potenciales:	Empresas con teletrabajadores, y teletrabajadores autónomos
Proveedores:	PYMES la distribución y venta de equipamiento WiFi
Dispositivos:	Ordenadores, tarjetas PCMCIAs, Adaptadores USB, Puntos de Acceso, MODEM router Cables/ADSL, VPNs ...

implique relacionar diferentes dispositivos dentro de un mismo ámbito de trabajo, es un campo dónde la tecnología WiFi puede ser una muy buena opción.

Wifi en el teletrabajo

El teletrabajo cómo ya se ha mencionado es otro de los entornos de aplicación de WiFi. Un teletrabajador es una persona que desarrolla gran parte de su trabajo externamente a la oficina, y en muchas ocasiones desde su propio domicilio. Cómo equipamiento tecnológico, el teletrabajador precisa disponer de una conexión de datos, típicamente de banda ancha, un ordenador y un conjunto de aplicaciones informáticas que le permitan estar conectado remotamente a su oficina (probablemente utilice WiFi internamente en su domicilio). En general se utiliza una VPN (Virtual Private Network) que facilita al teletrabajador la conexión remota a las aplicaciones ofimáticas de su empresa, de forma equivalente a hallarse en la oficina y con todas las garantías de seguridad exigibles.

WiFi en los hoteles

Los hoteles y algunas empresas de restauración aparecen como potenciales consumidores de la tecnología WiFi. En el caso de los hoteles, WiFi aparece cómo un servicio de valor añadido que puede ofrecerse a los clientes, posibilitando la conexión a Internet inalámbrica desde las habitaciones y otros espacios comunes. Se trata de un servicio que cada día se incorpora más a la oferta hotelera, y que puede llegar a ser diferenciador a la hora de decidirse por un hotel en concreto. Normalmente directivos de empresas y otros profesionales similares eligen hoteles con conexión a Internet y a ser posible con WiFi. Los hoteles turísticos, destinados a otro tipo de público más general, tendrán igualmente que incorporar en su oferta la conexión a Internet, así cómo otras aplicaciones y dispositivos orientados al ocio y al entretenimiento.

WiFi aparece cómo una alternativa de conexión inalámbrica que permite la creación de una red sin necesidad de obras ni molestas canalizaciones. Son muchas las cadenas hoteleras que ya disponen de WiFi en todos sus hoteles.

WiFi y las empresas de seguridad

WiFi tiene otros ámbitos de aplicación adicionales a la conexión de ordenadores a Internet o a la LAN de la empresa. En el sector de seguridad, WiFi permite la interconexión inalámbrica de dispositivos de seguridad cómo sensores remotos y cámaras de vídeovigilancia. Ante la creciente demanda en el sector, las empresas de seguridad comienzan paulatinamente a desarrollar ofertas de vídeovigilancia a través de conexiones de banda ancha.

WiFi en almacenes de distribución y grandes superficies

Dispositivos cómo las PDAs, o tablet PCs, dotados de aplicaciones de gestión del almacén, son elementos muy útiles a la hora de realizar la supervisión de stocks e inventarios. La conectividad

Figura 3.8: WiFi y las empresas de seguridad

Clientes potenciales:	Empresas con necesidad de videovigilancia
Proveedores:	PYMES la distribución y venta de equipamiento WiFi
Dispositivos:	Webcam WiFi, Puntos de Acceso, MODEM router Cables/ADSL, VPNs ...

inalámbrica permite realizar cualquier operación de acceso a bases de datos, contabilidad, pedidos y facturación desde cualquier punto del almacén sin la necesidad de una molesta conexión cableada.

WiFi en la interconexión de entornos

Muchas empresas han realizado la interconexión de distintos edificios cercanos utilizando la tecnología WiFi, cómo una alternativa a la contratación de servicios tradicionales de telecomunicaciones. Para ello la empresa debe disponer de su propio servicio de mantenimiento de la infraestructura informática y de telecomunicaciones. Estas tipo de interconexiones precisan de antenas direccionales con una alta ganancia así cómo visión directa entre los edificios. Las distancias alcanzables (dentro de los límites de potencia máxima permitida) rondan los 70 metros.

Este tipo de enlaces punto a punto o punto multipunto permiten la creación de conexiones inalámbricas de bajo coste y con un ancho de banda importante. Su aplicación se centra en:

1. Entornos urbanos interconectando edificios, cómo las diferentes sedes de una empresa.
2. Entornos urbanos mediante la creación de una red de acceso inalámbrica punto multipunto para un entorno residencial. Un ejemplo típico son las redes desplegadas por operadores WISP (Wireless Internet Service Providers).
3. Entornos rurales mediante la interconexión de poblaciones punto a punto. Poblaciones o edificios alejados de los núcleos urbanos cómo por ejemplo hoteles rurales, restaurantes y balnearios pueden beneficiarse de este tipo de soluciones.
4. Entornos rurales creando una red de acceso inalámbrica de ámbito local y compartido punto multipunto. Existe un gran interés por parte de las comunidades autónomas para promover el desarrollo de la banda ancha en entornos rurales. Una de las alternativas que se baraja actualmente es la combinación de una conexión a Internet vía satélite con distribución local mediante WiFi.

3.1.3.3. Recintos portuarios y aeroportuarios

Este tipo de lugares son muy adecuados para la utilización de la tecnología WiFi. En algunos de estos entornos, las aplicaciones se orientan al despliegue de PWLAN operadas por alguna compañía WISP, no obstante también se han desarrollado infraestructuras de uso interno para las diversas compañías que operan en estos ambientes. Podemos destacar las siguientes aplicaciones:

1. Carga de combustible: algunos aeropuertos instalan en los camiones cisterna dispositivos WiFi que se conectan de forma inalámbrica a la red permitiendo contabilizar de forma on line cada una de las operaciones de carga de combustible así cómo posibles incidencias.

2. Movimiento de contenedores: los recintos portuarios están muy interesados en registrar los movimientos y emplazamientos de los contenedores de mercancias, ya que la localización y su tiempo de permanencia son dos factores cruciales. Las gruas pueden dotarse de terminales WiFi que permiten la conexión en tiempo real con los servidores y aplicaciones informáticas de gestión de carga del recinto.

3. Los buques, al atracar en un puerto, pueden disponer fácilmente de servicios de conexión a la LAN portuaria, Internet o incluso VPN todo ello sin necesidad de cableado.

3.1.3.4. Ámbitos hospitalarios

Son ya muchos los informes que han demostrado la no interferencia de los equipos WiFi con los instrumentos médicos, materializándose la posibilidad de incorporar dispositivos WiFi en estos entornos. Se citan a continuación y a modo de ejemplo algunas de sus aplicaciones:

1. La tecnología WiFi en equipos instrumentales hace posible su movilidad, localización y uso compartido así cómo la conexión directa de los mismos con elementos de gestión médica permitiendo una mejor integración de las pruebas clínicas en la historia clínica del paciente.

2. El uso de terminales portátiles tipo tablet PC permiten al personal clínico la interacción directa con la historia clínica del paciente tanto para su consulta cómo para la actualización e incorporación de nuevos resultados.

3.1.3.5. Universidad

Es creciente la aparición de campus universitarios con cobertura WiFi. Esta cobertura alcanza elementos comunes como cafeterias, bibliotecas, ciertas salas y laboratorios, así cómo zonas exteriores. En todas ellas los alumnos con ordenadores portátiles, PDAs y otros terminales pueden consultar prácticas y ejercicios así cómo acceder a aplicaciones de e-learning. En definitiva, a las mismas aplicaciones a las que el alumno puede acceder desde una conexión cableada se suma un acceso inalámbrico. La interconexión de edificios del campus es otra de las aplicaciones de WiFi, cómo ya se ha indicado anteriormente.

3.1.3.6. Ámbitos públicos

La aparición de las PWLAN (Public Wireless Local Area Network) representa una oportunidad de negocio tanto para fabricantes cómo para empresas interesadas en desarrollar servicios de acceso a Internet en lugares de uso público. En este sentido opiniones encontradas, por una lado existen aquellas que auguran un enorme éxito basándose en la creciente necesidad de acceso a Internet mediante banda ancha para ciertos trabajadores cuyas empresas estarían dispuestas a pagar casi cualquier precio. También se espera que Wifi se despliegue de forma masiva en cafeterías, restaurantes y locales similares.

El contrapunto lo constituyen aquellas opiniones que descalifican totalmente este tipo de iniciativas y consideran que las PWLAN son una exageración más, cómo tantas otras dentro del e-business. Piensan que este negocio no evolucionará y se quedará en meras especulaciones. En este extremo hay que situar a las empresas proveedoras de acceso a Internet a las que no les entusiasma en absoluto este tipo de redes ya que en estas zonas, los clientes probablemente se darían de baja de los servicios que puedan tener contratados con ellas.

Volviendo al ámbito empresarial, ya se vió que la utilización de WiFi es algo más que habitual en estos últimos años. Lo que supone realmente una novedad es la aparición de los llamados hot spots, zonas de cobertura WiFi dentro de espacios públicos dónde un prestador de servicios facilita la conexión a Internet a través de dispositivos WiFi. Estos dispositivos pueden ser tanto PDAs como PCs portátiles.

3.1.3.7. Otros ámbitos de aplicación WiFi

La imaginación es la única que puede poner límites a las aplicaciones que hagan uso de dispositivos WiFi, conjuntamente el mercado fija el grado de interés, y por ende, de éxito. A continuación se muestran algunas aplicaciones adicionales a las descritas en secciones anteriores:

1. Medios de pago: la nueva normativa europea exigirá que la utilización de las tarjetas de crédito o débito en restaurantes, cafeterías, almacenes y otros establecimientos se realice siempre en presencia del cliente. Por esta razón, en breve los terminales punto de venta deberán adoptar características de movilidad que permitan acatar la normativa. Los equipos terminales punto de venta dotados de WiFi podrían ser un campo muy interesante a corto y medio plazo.

2. Distribución Multimedia: el despliegue de la banda ancha en comercios, restaurantes y, en general, espacios públicos, invita al desarrollo de aplicaciones dónde existe una distribución de contenido multimedia tal cómo publicidad, noticias y videoclips. WiFi es una alternativa para la conexión de pantallas y otro equipamiento multimedia.

3. Transporte Público: ya son una realidad las aplicaciones de transporte público que implican conectividad vía WiFi, cómo por ejemplo en el metro y el autobús.

3.2. Futuro

Si hablamos de un posible futuro para la tecnología WiFi, hay que tener en cuenta que actualmente nos dirigimos hacia una **convergencia** tecnológica. Todo pasa por la obtención de un términal único que permita al usuario final acceder a toda una gama de servicios de forma transparente, aprovechando las ventajas que ofrecen las distintas redes tanto fijas cómo móviles. Uno de los objetivos dentro de esta tendencia pretende conseguir una unión de los distintos tipos de redes de telecomunicaciones que conocemos actualmente (fijas, de datos y móviles) hacia un único modelo basado en el protocolo IP.

Por otro lado, la existencia de diversas plataformas tecnológicas en el ámbito de las tecnologías de la información y las comunicaciones (mayoritariamente de carácter propietario), genera una necesidad de integración e interoperabilidad entre ellas. Es en este escenario dónde el desarrollo de software intermedio (**middleware**) cobra un papel clave debido a la diversidad de plataformas y sistemas operativos existentes, especialmente en el caso de los terminales.

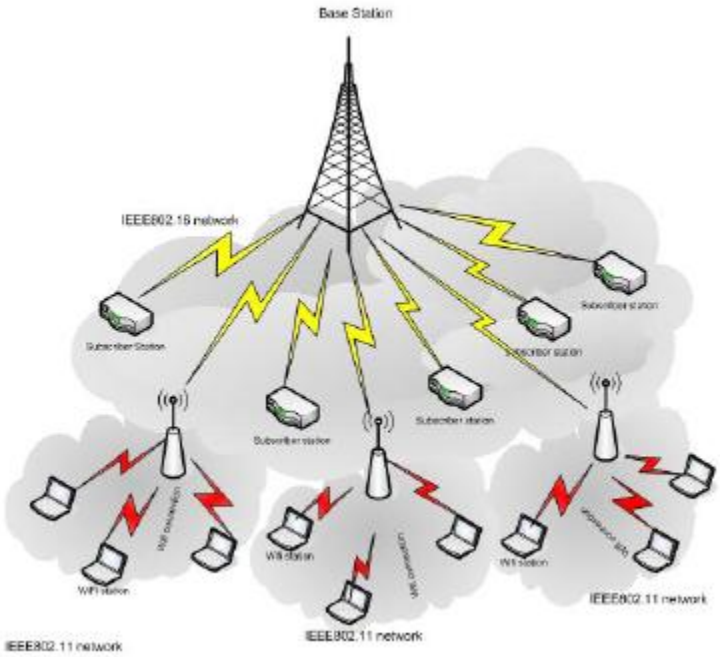
La base dónde se sustentará esta tendencia la encontramos en las conexiones de **banda ancha**, un elemento clave que se espera que finalmente acabe con la dicotomía WAN-LAN. Desde un punto de vista tecnológico, las redes de banda ancha vienen soportadas por tecnologías de naturaleza muy diversa, con prestaciones técnicas, costes y aplicaciones que varían sensiblemente de unas a otras. En cuánto a las *tecnologías cableadas*, las tecnologías más extendidas actualmente son ADSL y cable. De cara al futuro se prevé que los accesos cableados proporcionen mayores velocidades. En todo caso, se vislumbra una tendencia hacia una mayor demanda de *accesos inalámbricos* mediante diferentes tipos de terminales móviles.

En el **entorno doméstico**, ya mencionamos el llamado hogar digital. Previsiblemente, se piensa que en el futuro se dispondrá de una mayor gama de aplicaciones de domótica, seguridad, comunicaciones y aplicaciones audiovisuales. La evolución de la electrónica ha hecho posible que numerosos dispositivos domésticos que tradicionalmente carecían de capacidades de cómputo puedan ser dotados de nuevas funcionalidades. Estos dispositivos por otra parte, no viven aislados sino que tienden a interconectarse formando redes domésticas. A modo de ejemplo se pueden citar diferentes tecnologías que permiten esta interconexión cómo Bluetooth, CEBus, HAVi, HomePNA, HomeRF, LONWORKS y UPnP.

En un futuro más lejano se prevé una introducción de las tecnologías UWB (IEEE 802.15.x) en el entorno doméstico y WiMAX (IEEE 802.16e) en las comunicaciones inalámbricas a alta velocidad en el **ámbito metropolitano**.

Centrándose en la **tecnología WiFi** hay que citar el nuevo estándar IEEE 802.11n. Se hace referencia a velocidades máximas de hasta 300 Mbps sobre las bandas de frecuencia de 2,4 GHz y 5

Figura 3.9: Arquitectura de integración de WMAN y WLAN



GHz simultáneamente. Gracias al nuevo estándar, el WiFi del futuro implicará una mayor capacidad de transmisión, lo cual, dadas las comunicaciones actuales grandes y sus requerimientos, mejorará la proliferación de las redes inalámbricas.

De otra parte, los ya mencionados *hot spots* parece que actualmente estan marcando el camino a seguir en los próximos años.

No hay que olvidar tampoco las organizaciones que promueven las tecnologias inalámbricas. Cómo ejemplo más relevante hay que citar la WiFi Alliance, que certifica la interoperabilidad de los productos basados en la especificación IEEE 802.11. Actualmente son más de 300 las compañías de todo el mundo que se hallan implicadas y la cantidad sigue creciendo. Otras asociaciones que promueven el desarrollo de estas tecnologías son WLANA (Wireless LAN Association), FCC (Federal Communications Commission), ETSI (European Telecommunications Standards Institute) y UL (Underwriters Laboratories Inc).

Cómo conclusión, de cara a un futuro próximo, las tecnologías inalámbricas encabezadas por WiFi parece que acabarán por dominar el sector integrando las distintas tecnologias que conocemos actualmente basándose para ello en el protocolo IP.

Bibliografía

[INT01] http://www.intel.com/standards/case/case_802_11.htm (Intel.com, Intel Standards)

[WIL01] http://www.wilcorpinc.com/wifi_history.htm (Wilcopinc.com, What´s WIFI)

[SAF01] http://0proquest.safaribooksonline.com.llull.uib.es/1587201119/pref01#X2ludGVybm FsX1NlY3Rpb25 Db250ZW50P3htbGlkPTE1ODcyMDExMTkvY2gwOGxldjFzZWMy (Safary books)

[SAF02] http://0proquest.safaribooksonline.com.llull.uib.es/1587051176/pref01#X2ludGVy bmFsX1RvYz94bWxp ZD0xNTg3MDUxMTc2L2NoMDI= (Safary Books)

[MER01] http://www.cs.umd.edu/~waa/wireless.html (Universidad de Maryland, vulnerabilidades del 802.11)

[WEP01] http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html (Seguridad en WEP)

[SCN01] http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci787174,00.html (Searchnetworking.com, el protocolo 802.1x)

[WIP01] http://www.wi-fiplanet.com/tutorials/article.php/1041171 (Wi.Fi planet, Protocolo 802.1x)

[WIP02] http://www.wi-fiplanet.com/tutorials/article.php/2148721 (Wi.Fi planet, Mejoras en la seguridad de WPA)

[NWO01] http://www.networkworld.com/research/2002/0506whatisit.html (NetworkWorld.com, La tecnología inalámbrica)

[SOU01] http://open1x.sourceforge.net/ (Sourceforge, implementación libre del 802.1x)

[UNT01] http://www.untruth.org/~josh/security/radius/radius-auth.html (Unthuth.com, analisis del protocolo RADIUS)

[RFC01] http://www.ietf.org/rfc/rfc2865.txt (rfc2865)

[LDP01] http://tldp.org/HOWTO/html_single/8021X-HOWTO/#p8021x (Linux documentation project, protocolo 802.1x)

[MIC01] http://www.microsoft.com/windowsxp/using/networking/expert/bowman_03july28.mspx (Microsoft, redes inalambricas en windows)

[WIO01] http://www.wi-fi.org/files/uploaded_files/wp_9_WPA-WPA2%20Implementation_2-27-05.pdf (Wi-Fi.org, implementación del estandar WPA2)

[NWO02] http://www.networkworld.com/columnists/2006/091106-wireless-security.html (Networkworld.com, seguridad en redes inalámbricas)

[OPE01] http://www.openxtra.co.uk/articles/wpa-vs-80211i.php (Openxtra.com.uk, comparación entre wpa y wpa2)

[WIK01] http://en.wikipedia.org/wiki/Wi-Fi_Alliance (Wikipedia)

[WIK02] http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access (Wikipedia)

[WIK03] http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy (Wikipedia)

[WIK04] http://en.wikipedia.org/wiki/RADIUS (Wikipedia)

[WIK05] http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access (Wikipedia)

[WIK06] http://en.wikipedia.org/wiki/Wireless#History http://en.wikipedia.org/wiki/802.1x (Wikipedia)

[GOO01] http://www.google.com/patents?vid=USPAT2292387&id=R4BYAAAAEBAJ (Patentes en google)

[HED01] http://www.alohacriticon.com/elcriticon/article128.html (Hedy Lamarr. Biografia y fotos)

[INV01] http://www.inventions.org/culture/female/lamarr.html (Inventions.org, Lamarr)

[CIS01] Libro de Fundamentos de redes inalambricas Ed. Cisco Press.

[CIS02] Curso cisco.netacad.com - curso de wíreless.

[WIF01] Wi-Fi Handbook: Building 802.11b Wireless Networks.

[WIF02] Hotspot Networks: WiFi for Public Access Locations. (Professional Telecom)

[IEEE01] http://0ieeexplore.ieee.org.llull.uib.es/iel5/10227/32603/01524793.pdf?tp=&arnumber=1524793&isnumber=32603 (Optimal pricing for broadband wireless Internet access service. Ieeexplore)

[IEEE02] http://0ieeexplore.ieee.org.llull.uib.es/iel5/9145/29024/01307700.pdf?tp=&arnumber=1307700&isnumber=29024 (Performance evaluation of the security in wireless local area networks (WiFi). Ieeexplore)

[IEEE03] http://0ieeexplore.ieee.org.llull.uib.es/iel5/4135322/4037316/04135353.pdf?tp=&arnumber=4135353&isnumber=4037316 (Improving Accuracy of WiFi Positioning System by Using Geographical Information System (GIS). Ieeexplore)

[IEEE04] http://0ieeexplore.ieee.org.llull.uib.es/iel5/4085644/4037317/04085653.pdf?tp=&arnumber=4085653&isnumber=4037317 (Tutorial 2: Emerging Wireless Standards for WRAN, WiFi, WiMedia and ZigBee. Ieeexplore)

[IEEE05] http://0ieeexplore.ieee.org.llull.uib.es/iel5/4054516/4054517/04055012.pdf?tp=&arnumber=4055012&isnumber=4054517 (Wifi Broadband Networks for Wide Rural and Remote Areas. Ieeexplore)

[IEEE06] http://0ieeexplore.ieee.org.llull.uib.es/iel5/4014788/4014789/04014887.pdf?tp=&arnumber=4014887&isnumber=4014789 (Radio-over-Fiber Architecture for Simultaneous Feeding of 5.5 and 41 GHz WiFi or WiMAX Access Networks. Ieeexplore)

[IEEE07] http://0ieeexplore.ieee.org.llull.uib.es/iel5/9502/30141/01383419.pdf?tp=&arnumber=1383419&isnumber=30141 (Rural/Remote WiFi Wireless Broadband System. Ieeexplore)

[IEEE08] http://0ieeexplore.ieee.org.llull.uib.es/iel5/7693/4027759/04027785.pdf?tp= &arnumber=4027785&isnumber=4027759 (A MAC-Layer Retransmission Algorithm Designed for the Physical-Layer Characteristics of Clustered Sensor Networks. Ieeexplore)

[IEEE09] http://0ieeexplore.ieee.org.llull.uib.es/iel5/4234/33685/01603368.pdf?tp= &arnumber=1603368&isnumber=33685 (Stabilizing TCP performance over bursty wireless links through the combined use of link-layer techniques. Ieeexplore)

[IEEE10] http://0ieeexplore.ieee.org.llull.uib.es/iel5/2188/21252/00986237.pdf?tp= &arnumber=986237&isnumber=21252 (Networking gets personal. Ieeexplore)

[SIN01] http://0www.blackwellsynergy.com.llull.uib.es/doi/pdf/10.1111/j.1467-9310.2005.00369.x (Synergy: Analysing disruptive potential: the case of wireless local area network and mobile communications network companies)

[SAF03] 802.11 Wireless Networks: The Definitive Guide