# LAS TECNOLOGÍAS WIFI Y WIMAX

# INTRODUCCIÓN

## INTRODUCCIÓN

En los últimos años, las telecomunicaciones han experimentado un gran avance impulsadas, entre otros, por la evolución de las comunicaciones vía radio. Tecnologías como GSM, DECT, LMDS, UMTS han generado grandes expectativas de nuevos servicios entre la población.

Actualmente, la expansión de la tecnología Wi-Fi, acrónimo de Wireless Fidelity (fiabilidad sin hilos), se está produciendo con bastante mundialmente. La causa radica|rae en el hecho que la tecnología Wi-Fi posibilita el acceso móvil de lado ancha a Internet a un coste muy asequible.

Posteriormente ha aparecido la tecnología WiMAX, acrónimo de Worldwide Interoperability for Microwave Access (interoperabilidad a nivel mundial por los accesos de microondas) que también ha supuesto un avance|anticipo importante con respecto al panorama de las tecnologías sin hilos. WiMAX puede trabajar según diferentes configuraciones, y ofrecer enlaces punto a punto de lado ancha como una alternativa a soluciones de cable o DSL.

El objeto de este documento es presentar de forma clara y entenedora en que consisten el Wi-Fi y el WiMAX, qué servicios pueden aportar, cuál es la situación actual, tanto desde del punto de vista técnico, como desde el punto de vista de despliegue, qué experiencias hay de ámbito nacional e internacional, y finalmente cuál sería la metodología óptima para la implantación de una red basada en soluciones Wi-Fi o WiMAX en un municipio.

# REGULACIÓN DEL ESPECTRO

## REGULACIÓN DEL ESPECTRO

Las bandas de frecuencia utilizadas mayoritariamente por las redes sin hilos y especialmente por los equipos Wi-Fi son las de 2,4 y 5 GHz, que están clasificadas como uso común compartido. La caracterización como uso común permite que diversos operadores o usuarios puedan utilizar de forma simultánea estas frecuencias, de acuerdo con unas normas establecidas por la regulación para mitigar las posibles interferencias entre emisiones.

Para la operación en estas bandas dentro de las limitaciones establecidas en la legislación española, no se exige disponer de licencia de uso del espectro, a diferencia de otra bandas de frecuencia.

En todo caso, el hecho de que no sea necesario disponer de licencia para operar no implica que la utilización de esta banda no esté sujeta a condiciones específicas. Hay límites sobre la potencia que se puede radiar y los protocolos de comunicaciones que se pueden utilizar con el fin de garantizar el uso común de estas frecuencias del espectro radioeléctrico.

La mayoría de estas condiciones de utilización emanan de la regulación que fija el Ministerio de Industria para el uso del dominio público radioeléctrico. El Cuadro Nacional de Atribución de Frecuencia (CNAF) recoge las condiciones de utilización del espectro en el Estado español por el que hace a atribución de uso para las frecuencias, las potencias de emisión y los protocolos que hay que utilizar en cada banda.

La limitación de potencias máximas de emisión está orientada a buscar un equilibrio entre la cobertura de los puntos de acceso y las posibles interferencias entre emisores. En el caso de las bandas de uso común del espectro, la regulación limita la potencia máxima que se puede utilizar en esta banda en 100 mW (20 dBm) de potencia isótropa radiada equivaliendo (PIRE)[1] en la mayoría de los países y así se recoge en el caso español a la nota UN-85 del CNAF actualmente vigente. Esta potencia es diversos órdenes de magnitud inferior a las limitaciones que se establecen para usos privativos, hecho que se debe a la necesidad que se puedan reutilizar frecuencias en ubicaciones próximas entre sí.

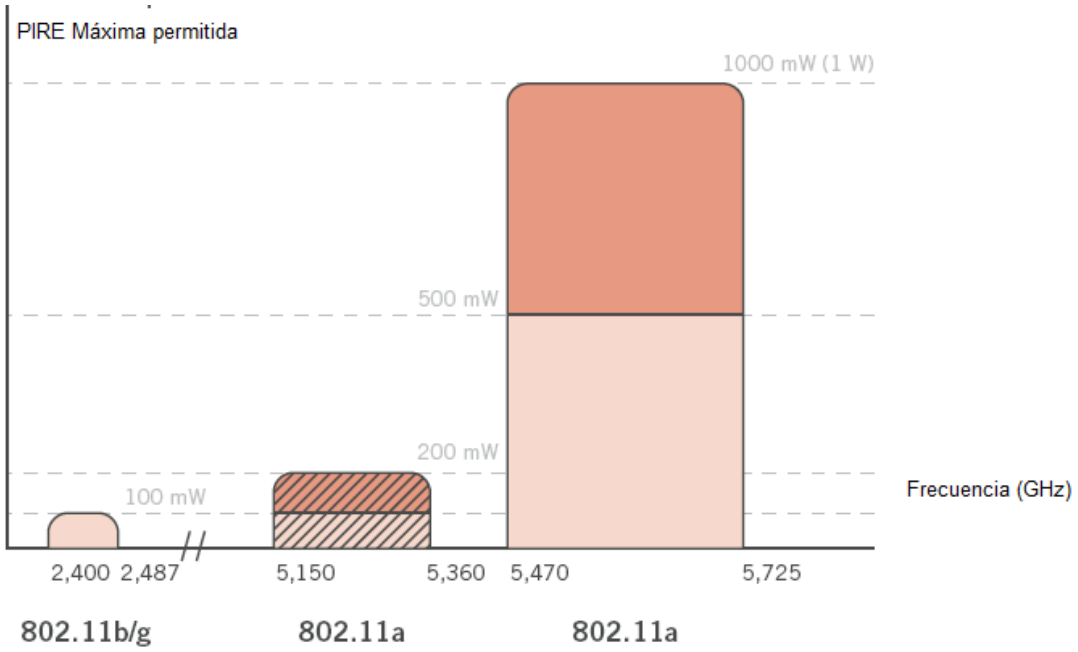
Con respecto al uso de Wi-Fi en la banda de 5 GHz, las potencias permitidas en éstas bandas varían en cada país, incluso dentro de la Comunidad Europea y son dependientes de diversos factores, como el uso en interiores, exteriores o la implantación de mecanismos de control de potencias.

En el caso español, las condiciones de uso compartido de la banda de 5 GHz se concreta en la nota UN-128 del CNAF. La PIRE máxima está restringida a 200 mW entre los 5,15 y 5,360 GHz y en 1 W en la banda comprendida entre los 5,470 y 5,725 GHz, siempre que se utilicen técnicas de control de potencia, soportadas por los puntos de acceso que se comercializan habitualmente. El uso de la banda entre 5,15 GHz y 5,25 GHz está reducido a instalaciones interiores.

En la figura siguiente se resumen las bandas de frecuencia y potencias máximas permitidas para cada banda del espectro utilizado Wi-Fi.

---

[1] La PIRE incluye tanto la potencia de emisión como la ganancia de la antena utilizada (en términos logarítmicos, PIRE= Potencia Radiada + Ganancia) y la regulación establece las limitaciones de potencia en la dirección de máxima radiación, por|para lo cual en la práctica no es posible aumentar el alcance de la emisión utilizando antenas de más ganancia respetando la legislación.




Por el hecho de ser una banda de uso común, la banda de frecuencia de 2,4 GHz es compartida por las redes Wi-Fi y por otras tecnologías (Bluetooth[2], Home RF[3], hornos microondas...) cosa que incrementa la posibilidad de congestión en esta banda. Por este motivo se decidió utilizar también la banda de los 5 GHz por|para aplicaciones de redes Wi-Fi. De alguna manera se puede decir que la banda de 2,4GHz es de uso común para propósito general y la de 5Ghz de uso común más orientada estrictamente a redes. La importancia de esta diferenciación es primordial ya que una gran cantidad de elementos de diferentes redes que operan en una misma frecuencia comporta una caída importante del rendimiento de éstos.

Los estándares no establecen limitación en el número de usuarios simultáneos conectados a un punto de acceso, pero las pruebas efectuadas por los fabricantes de los equipos han mostrado que a partir de aproximadamente 200 usuarios conectados el rendimiento del sistema baja notablemente a causa de las limitaciones de la electrónica de los equipos. Vale a decir que ésta cifra depende mucho del comportamiento de los usuarios; es decir, del tipo de tráfico que generan, de las aplicaciones que utilicen, etc.

En cualquier caso, la conclusión es que dimensionando el número de puntos de acceso en una red lo que hay que garantizar es no sólo la cobertura radioeléctrica del territorio (a través de las antenas conectadas al punto de acceso) sino la capacidad, es decir, el número de usuarios simultáneos conectados que se prevén, ya que como más usuarios conectados más disminuye la velocidad efectiva de transmisión de cada uno.

[2] Bluetooth es una tecnología que posibilita la conexión sin hilos de corto alcance de voz y datos entre PC, portátiles, agendas electrónicas, teléfonos móviles, impresoras, escáneres, cámaras digitales y otros dispositivos domésticos, a la frecuencia de uso común de 2,4 GHz.

[3] Home RF es una tecnología para la interconexión sin hilos de PC, periféricos, teléfonos móviles, y otros aparatos de consumo, a la frecuencia de uso común de 2,4 GHz.

# TECNOLOGÍA WIFI

Una red Wi-Fi es una red de comunicaciones de datos y, por lo tanto, permite conectar servidores, PC, impresoras, etc., con la particularidad de alcanzarlo sin necesidad de cableado.

De manera purista vale a decir que el acrónimo Wi-Fi se utiliza para identificar los productos que incorporan cualquier variando de la tecnología sin hilos de los estándares IEEE 802.11, que permiten la creación de redes de área local sin hilos conocidas como WLAN4, y que son plenamente compatibles con los de cualquier otro fabricante que utilice estos estándares.

Las características generales de funcionamiento de una red Wi-Fi son las mismas que las de una red con cableado. La particularidad es que el Wi-Fi utiliza el aire como medio de transmisión.

Los componentes básicos de una red Wi-Fi son:

- El punto de acceso (AP): es la unión entre las redes con cableado y la red Wi-Fi, o entre diversas zonas cubiertas por redes Wi-Fi, que actúa entonces como repetidor de la señal entre estas zonas (celdas).
- Unas o más antenas conectadas al punto de acceso.
- Un terminal Wi-Fi. Éste puede tener forma de dispositivo externo Wi-Fi, que se instala en el PC del usuario, o bien puede encontrarse ya integrado, como sucede habitualmente con los ordenadores portátiles. Adicionalmente se pueden encontrar otros terminales con capacidad de comunicación, como agendas electrónicas (PDA) y teléfonos móviles, que disponen de accesorios (internos o externos) para conectarse a redes Wi-Fi.

A continuación se presentan algunos de los aspectos más relevantes para analizar las redes Wi-Fi: el alcance y el rendimiento, la calidad de servicio, la seguridad, la movilidad y el estado de la estandarización de cara a mejoras futuras.

## *1.1. Arquitectura de redes Wi-Fi*

En un principio, las redes sin hilos fueron concebidas para la creación de redes de área local de empresa. La arquitectura de éstas es, pues, bastante sencilla. Con el tiempo, sin embargo, su uso ha evolucionado hacia redes de área extendida, principalmente en núcleos urbanos. Eso es debido al hecho de que la arquitectura, a pesar de ser sencilla, es muy fácilmente escalable.

### 1.1.1 Elementos de una red Wi-Fi

Los elementos que forman una red Wi-Fi son los siguientes:

- Punto de acceso (AP): Es el dispositivo que gestiona la información transmitida y la hace llegar a destino. Asimismo, proporciona la unión entre la red Wi-Fi y la red fija.

- Antena: Las antenas son los elementos que envían al aire señales en forma de ondas electromagnéticas que contienen la información dirigida en el dispositivo de destino; y a la vez, captan del aire las señales de las cuales se extraerá la información que llega de otro dispositivo.

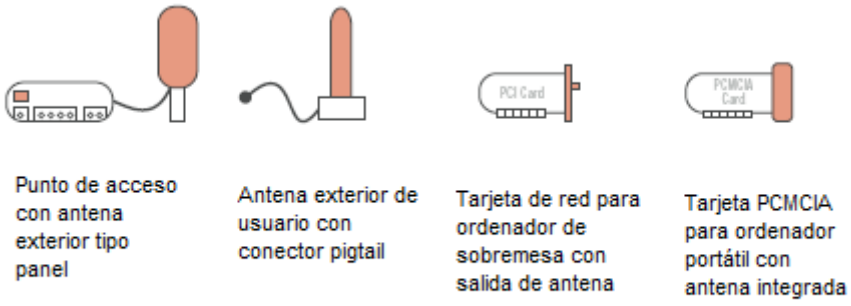
Cada tipo de antena tiene unas propiedades geométricas que hacen que dirija la energía electromagnética en unas ciertas direcciones del espacio. Las antenas omnidireccionales emiten en todas direcciones mientras que las antenas sectoriales o otros de más direccionales todavía, como las antenas parabólicas, reducen progresivamente el sector angular hacia el cual emiten. Concentrando la energía enviada (o captada), se pueden obtener comunicaciones entre antenas además distancia. Una antena omnidireccional, en cambio, ofrece una superficie de cobertura más extendida.

Determinar el tipo y número de antenas que hay que utilizar para dar cobertura a un área es una tarea que hace falta llevar a cabo para cada situación concreta en la definición del proyecto, en función de la morfología de los territorios y de las ciudades y de la frecuencia de la señal para emitir.

- Dispositivo externo Wi-Fi: La tarjeta Wi-Fi es una tarjeta de red de área local (CHAL) que cumple la certificación Wi-Fi y permite por lo tanto la conexión de un terminal de usuario en una red 802.11. Hay tarjetas diferentes para cada subestándar (a, b o gr), pero también hay mixtas. Estos dispositivos externos pueden conectarse a ranuras PCI o PCMCIA o en puertos USB. Las principales diferencias entre este tipo de tarjetas y una tarjeta Ethernet convencional son el cifrado de datos, el identificador de red Wi-Fi (ESSID), el canal y el ajuste de velocidad.

- Antena de usuario y conector pigtail: La antena de usuario proporciona la cobertura necesaria a un usuario para el acceso a la red Wi-Fi. El conector pigtail es un tipo de cable que conecta y adapta la tarjeta Wi-Fi y la antena del usuario. Hay que decir que el pigtail no es un elemento estándar, depende del fabricante de la tarjeta. En ciertos casos la tarjeta Wi-Fi trae integrada la antena de usuario, como es el caso de las tarjetas para portátiles, PDA, etc. Si es así, entonces no es necesaria otra antena externa.

En la Figura 3-1 se muestran los elementos mencionados de la arquitectura de una red Wi-Fi.




### 1.1.2 Topología de una red Wi-Fi

En las redes Wi-Fi podemos encontrar dos tipos de topologías:

- **Redes sin infraestructura**. Las redes Wi-Fi sin infraestructura no necesitan un sistema fijo que interconecte algunos elementos de la arquitectura. Son redes que no han tenido un importante éxito comercial. Los ejemplos más habituales

que podemos encontrar son las redes ad hoc, (o Peer-to-Peer) y las redes pescadas|trilladas o MESH, en inglés. Las primeras consisten en un grupo de terminales que se comunican cada uno directamente con los otros a través de las señales de radio sin utilizar ninguno punto de acceso. Los terminales de esta red Wi-Fi que quieran comunicarse entre sí tienen que utilizar el mismo canal radio y configurar un identificador específico de Wi-Fi (nombrado ESSI) en modo ad hoc. Las configuraciones ad hoc son comunicaciones de tipo punto a punto. Un ejemplo de red ad hoc sería la comunicación directa entre dos ordenadores mediante señales de radio.

En cambio, las redes tipos MESH utilizan puntos de acceso que trabajan con diferentes canales de frecuencia. Por una parte, ofrecen cobertura a los terminales portátiles, y por|para la otra, se comunican entre sí formando una red pescada|trillada que les permite cubrir grandes superficies sin necesidad de un cableado previo.

- **Red en modo infraestructura**. Una red en modo infraestructura trabaja utilizando puntos de acceso. Presenta una eficiencia superior a la red ad hoc, ya que este modo gestiona y transporta cada paquete de información en su destino, mejorando la velocidad del conjunto. En este modo de funcionamiento, la tarjeta de red se configura automáticamente para utilizar el mismo canal radio que utiliza el punto de acceso más próximo de la red. En una red en modo infraestructura, los puntos de acceso pueden trabajar como interconexión entre dos redes. En esta topología se encontrarían dos posibilidades: la primera consiste a que el punto de acceso actúe como interconexión entre la red Wi-Fi y otra red sobre cables, como una red de área local, un acceso ADSL, etc. El segundo escenario consiste que el punto de acceso actúe como interconexión entre dos puntos de acceso que dan acceso Wi-Fi a usuarios ubicados en zonas diferentes.

  Un ejemplo de red en modo infraestructura sería una red municipal que cubriera el núcleo urbano para dar conexión a la Intranet del ayuntamiento.

## *1.2. Estándares Wi-Fi*

La creación de los estándares que han dado lugar al Wi-Fi es una tarea llevada a cabo por el International Electrical and Electronic Engineers (Asociación Internacional de Ingenieros Electrónicos y de Telecomunicaciones), conocido por las siglas IEEE. Este organismo es una asociación profesional que se encarga de la publicación de artículos, realización de conferencias y redacción de estándares, como el muy popular Ethernet.

El IEEE dispone de una extensa familia de estándares correspondientes a las redes de área local, la 802. Dentro de esta familia se encuentran iniciativas bien diferentes, separadas esencialmente por el alcance que se pretende obtener. Así, la subfamilia 802.15.4, más conocida como ZigBee, está dedicada a la estandarización de protocolos orientados a redes de sensores, donde el bajo consumo y la alta variabilidad de la topología son fundamentales. El Bluetooth (802.15.1), por contra, está orientado en las redes personales, donde los diferentes accesorios que un individuo puede llevar encima o en su entorno inmediato (pocos metros) se han de interconectar. Algunos ejemplos son el teléfono móvil con el equipo de sonido del coche, o el móvil con el micrófono sin hilos. Por otra parte, el 802.16, más conocido como WiMAX, busca dar un alcance de hasta el vigésimo de kilómetros, con capacidades de centenares de Mbps.

Lógicamente, la complejidad, coste y consumo del sistema son muy superiores a los casos anteriores.

Para el caso concreto de las redes sin hilos de alcance reducido, con coberturas de menos de 100 metros y capacidades de unos pocos Mbps (es decir, para el nicho entre WiMAX y ZigBee o Bluetooth), se creó la subfamilia de estándares nombrada 802.11, popularmente conocida como Wi-Fi.

Las redes Wi-Fi cumplen los estándares genéricos aplicables a las XAL5 cableadas (Ethernet o equivalentes) pero necesitan una normativa específica adicional que defina el uso de los recursos radioeléctricos y la manera o el orden en qué cada uno de los dispositivos en red envía la información a los otros.

Los estándares del IEEE no se configuran nunca de manera cerrada, es decir que se van mejorando mientras es posible, por eso a lo largo del tiempo van apareciendo nuevos sub estándares que implementan mejoras o variantes sobre algún aspecto. La nomenclatura que se sigue en estos casos consiste a ir añadiendo letras minúsculas detrás del número 802.11, que es el del estándar principal.

En cuanto a velocidad de transmisión de datos y de banda de frecuencia de uso, que de hecho son los dos parámetros principales del sistema, se han definido hasta ahora los subestándares siguientes:

### 1.2.1 Limitaciones tecnológicas de la familia 802.11

Independientemente de la banda de frecuencia en que trabajan, todos los estándares de la subfamilia 802.11 comparten algunas limitaciones que es conveniente conocer antes de tomar una decisión sobre coberturas, alcance o velocidades que se pueden alcanzar.

Estas limitaciones son cinco:

- **Alcance**: Aunque comercialmente se habla típicamente de un alcance de hasta 100 metros, este dato depende, en primer lugar, de la ubicación y de la presencia de obstáculos en el camino entre el punto de acceso y el terminal, y en segundo lugar, de las condiciones meteorológicas y de las interferencias. Así, en espacio abierto, con buenas condiciones meteorológicas y antenas exteriores de los terminales, este alcance puede ser bastante superior. Sin embargo, en el interior de un edificio, donde las paredes representan un obstáculo muy importante, la distancia será notablemente inferior. Asimismo, si hay otros redes Wi-Fi próximas, o sencillamente otras fuentes de interferencias, es también mucho probable que las distancias disminuyan.
- **Anchura de banda**: Nominalmente, los diferentes estándares pueden alcanzar, físicamente (es decir, en el canal aéreo, descontando cualquier ineficiencia que puedan introducir los protocolos superiores), las velocidades mencionadas en la mesa|tabla presentada a el apartado anterior. Ahora bien, a causa del efecto de los protocolos necesarios para transportar la información de usuario sobre el canal aéreo, la velocidad útil es mucho menor. Además, en función de las condiciones del entorno y, por lo tanto, de la calidad de cada comunicación entre un terminal y el punto de acceso, la anchura de lado de esta comunicación se adapta, con el fin de utilizar codificaciones más robustas ante interferencias y/o errores. Es por eso que a veces nos encontremos con una conexión con el punto de acceso de 11 Mbps, otros en 5 Mbps, en 2 Mbps o, incluso, en 1 Mbps.

- **Calidad de servicio**: No todo el tráfico tiene la misma importancia desde el punto de vista de cada usuario. Así, se puede considerar que una llamada de VoIP tendría que tener prioridad sobre una transferencia de ficheros. Los protocolos más extendidos de Wi-Fi, como|cómo ahora b y gr, no incluyen ningún mecanismo para priorizar un tipo de tráfico sobre uno otro, lo cual resulta muy perjudicial cuando se mezclan flujos de tráfico con requerimientos muy diferentes, como voz y datos. La consecuencia es que Wi-Fi es poco adecuado para transportar tráfico exigente en términos de calidad, como VoIP, no tanto para que no funcione adecuadamente, como porque no se puede garantizar cuándo y en qué condiciones funcionará. El 802.11e, como se vea después, introduce mejoras en este aspecto.
- **Seguridad**: En un principio, las redes Wi-Fi no presentaban mecanismos de seguridad muy sofisticados, ya que el énfasis se puso en cómo transmitir datos sobre el aire, que era un desafío tecnológico más urgente. Con el éxito de esta tecnología, sin embargo, y la publicación de las debilidades de los mecanismos de seguridad originales, se hizo necesario introducir mejoras en este aspecto. De hecho, la falta de seguridad de éstas redes, a pesar de que muy exagerada en la mente de la opinión pública, es uno de los suyos grandes detractores. Como veamos, el 802.11i resuelve la mayoría de las debilidades originales, hasta el punto de hacerlas comparables en seguridad en las redes fijas.
- **Movilidad**: Popularmente, se considera que las redes Wi-Fi son móviles, ya que no hay que conectarse desde una ubicación fija para acceder a los servicios que nos ofrece, y además se puede ir caminando y navegando por Internet o leyendo el correo electrónico al mismo tiempo. Estrictamente hablando, eso se considera itinerancia, y no movilidad. De hecho, no es posible utilizar una red Wi-Fi desde un vehículo en movimiento a velocidad normal, por razones físicas asociadas a la velocidad. Además, incluso cuando nos movemos a baja velocidad (caminando), a causa del escaso alcance de cobertura de un punto de acceso, rápidamente tenemos que establecer conexión con otro punto de acceso, la cual cosa implica "saltar" del uno al otro. También en este aspecto el estándar presenta deficiencias que pueden hacer que perdamos brevemente la conexión e incluso hayamos de volver a conectarnos manualmente. Para compensar ambas restricciones, están desarrollando nuevos estándares, y es de esperar que pronto se dispondrá de productos en|a el mercado.

A continuación se expondrán brevemente las características más destacadas de cada tecnología, con el fin de poder hacer una elección adecuada, en función de cada necesidad.

### 1.2.2 Aspectos tecnológicos de 802.11b: Wi-Fi para las masas

Este estándar define la creación de redes sin hilos a la frecuencia de 2.4 GHz, con una tipología de modulación que permite alcanzar velocidades de transmisión "en el aire" de hasta en 11 Mbps, cosa que supone una velocidad efectiva para los usuarios de aproximadamente 5.5 Mbps. Hasta hace poco era la tecnología más extendida, pero ahora ha sido sustituida por 802.11g, que ofrece las mismas ventajas (banda de uso libre, simplicidad de funcionamiento ...), pero con más anchura de lado, y que, además, es compatible con b, lo cual permite mezclar dispositivos de ambos tipos en la misma red.

### 1.2.3 Aspectos tecnológicos de 802.11a: la primera mejora de velocidad

Este estándar define la creación de redes sin hilos a la frecuencia de 5 GHz. La información de un usuario se transmite modulando digitalmente una señal de la banda de 5 GHz con los datos del usuario. La modulación que se utiliza en este están-

dar difiere de la del 802.11b, y es especialmente útil en entornos donde pueden aparecer grandes interferencias, por ejemplo, en transmisiones móviles en trenes. En cambio, es incompatible con 802.11b, ya que trabaja en otra frecuencia.
El estándar 802.11a permite alcanzar velocidades de transmisión máximas de hasta 54 Mbps, cosa que supone una velocidad efectiva de aproximadamente 36 Mbps.

### 1.2.4 Aspectos tecnológicos de 802.11g: el estándar de hoy en día

Este estándar mejora el 802.11b, ya que trabaja igualmente a la frecuencia de 2.4 GHz, pero varía la modulación (en este caso es idéntica a la de 802.11a) hasta alcanzar igualmente velocidades de transmisión máximas de hasta 54 Mbps, cosa que supone una velocidad efectiva de aproximadamente 36 Mbps. Su capacidad de trabajar conjuntamente con el equipamiento 802.11b lo hace doblemente interesante, porque permite mantener el equipamiento anterior y migrar lentamente al nuevo estándar.

### 1.2.5 Aspectos tecnológicos de 802.11n: anchura de lado equivalente a Fast Ethernet

El objetivo del nuevo estándar 802.11n es mejorar todavía más el alcance y sobre todo la anchura de lado de las redes Wi-Fi, de manera que sea comparable a las redes de área local fijas. Cómo hoy en día eso es sinónimo de Ethernet, la velocidad que se pretendía alcanzar como|cómo a mínimo eran 100 Mbps. Se tiene que decir que este estándar todavía se encuentra en proceso de finalización, y por lo tanto, aunque ya se conocen las características principales, encara allí ha espacio para modificaciones. Es por eso que no se pueden dar datos definitivos sobre velocidad que, en todo caso, con certeza, se moverán en torno a los 100 Mbps.

La solución utilizada en 802.11n consiste a reducir las ineficiencias, pero sobre todo a aprovechar lo que en principio es una gran desventaja de los sistemas sin hilos: las interferencias provocadas por las reflexiones de la señal en paredes, edificios, etc., que hacen que lleguen diversas copias de la misma señal ligeramente distorsionadas y retrasadas en el receptor. La gran innovación del 802.11n es el uso de más de una antena en cada punto de acceso y en cada terminal, de manera que se puedan aprovechar los "rebotes" y combinarlos para obtener uno señal mejor. Al mismo tiempo, se puede enviar más de una señal a la vez (diversas antenas). Combinando ambos efectos, se consigue una transmisión más eficaz y más robusta, y en definitiva, más anchura de lado para el usuario. Esta técnica se llama MIMO (Multiple-input, Multipleoutput).

Se prevé que este estándar pronto saldrá al mercado, ahora bien, ya se pueden encontrar al mercado productos preestándar de algunos fabricantes. Básicamente, estos productos son versiones propietarias que implementan la técnica MIMO, pero que no necesariamente serán compatibles con el futuro estándar. Además, lógicamente están en muchas ocasiones incompatibles entre sí, ya que cada despliegue se liga a un único fabricante. También hay problemas de compatibilidad con los productos b y gr (incluso del mismo fabricante), con los cuales el 802.11n tendría que ser compatible. No hay que confundir estos productos anteriores al 802.11n con otras soluciones, también propietarias de cada fabricante, que ofrecen velocidades similares basadas en modificaciones de 802.11g. Normalmente tienen el apelativo "Turbo-g" o similar. La manera de conseguir las anchuras de lado anunciadas (típicamente 108 Mbps) es juntando dos canales gr "normales" para una única comunicación. Evidentemente, si bien la velocidad es el doble, la capacidad total de la celda se reduce a la mitad.

### 1.2.6 Aspectos tecnológicos de 802.11e: calidad de servicio en redes Wi-Fi

Como se ha indicado, uno de los grandes problemas de las redes Wi-Fi es que no proveen ningún mecanismo para dar prioridad a ciertos tipos de tráfico sobre otros (calidad de servicio). Eso es especialmente grave si se mezclan voz y datos en la misma red sin hilos. El nuevo estándar 802.11e da respuesta a este problema. Hace falta evaluar qué necesidad real, para un uso concreto, tenemos de mecanismos de éste estilo. Claro está que son convenientes en el caso de querer dar VoIP de buena calidad, todo y que hay despliegues con tecnología 802.11g que ofrecen el servicio sencillamente dimensionando la red para que haya capacidad excedente sobradamente, y por lo tanto, no haya nunca "atascos". En la mayoría de escenarios, sin embargo, la necesidad de QoS es más difícil de justificar.

### 1.2.7 Aspectos tecnológicos de 802.11i: seguridad en redes Wi-Fi

Éste es uno de los aspectos más importantes para la popularización definitiva de las redes Wi-Fi. Todas las tecnologías radio son vulnerables a priori por el hecho de utilizar el aire como medio de transmisión (ya que en principio es un medio accesible a todo el mundo, que quiera escuchar nuestras comunicaciones), por eso hay que imponer estrictas medidas de seguridad a la hora de implementar estas redes.

En termas generales, los requerimientos de seguridad en una red de comunicaciones son los siguientes:

- Autenticación: La garantía de que el servicio se ofrece únicamente a los usuarios autorizados y que el servicio es ofrecido por a quien dice ofrecerlo.

- Confidencialidad: La garantía de que sólo los usuarios autorizados pueden acceder al contenido de la información enviada. Implica la implantación de mecanismos de cifrado de la información que se transmite por la red.

- Integridad: La garantía de que la información no pueda ser alterada ni cambiada en el transcurso de su transmisión por una red.

- Disponibilidad: La garantía de que la información es accesible para los usuarios autorizados de forma sencilla y en cualquier momento.

En particular, la tecnología Wi-Fi tradicional (es decir, los estándares b, gr y a) provee actualmente seguridad mediante dos atributos: la confidencialidad y la autentificación.

Con respecto a la confidencialidad:

- **WEP**: es un sistema de cifrado estándar propuesto por el comité 802.11, que comprime y cifra los datos que se transmiten a través de las ondas de radio. Este sistema es vulnerable, ya que es sencillo obtener la manera cómo han sido cifrados los datos. La clave está fija (no cambia nunca) y es la misma para todos los usuarios de una red. WEP es soportado por la mayoría de fabricantes de productos Wi-Fi.

Con respecto a la autenticación:

- Autenticación abierta: Es el mecanismo de autenticación por defecto que permite que cualquier dispositivo pueda obtener acceso a la red y los datos se transmiten sin ningún tipo de cifrado.

- Autenticación de clavo compartida: Es un mecanismo de autenticación que utiliza la clave WEP de la red para autenticar al cliente. El proceso consiste en el envío por parte del punto de acceso de un texto que posteriormente el cliente cifra con la clave de red y lo devuelve al punto de acceso. Si este proceso se resuelve satisfactoriamente, se inicia el mismo proceso en sentido inverso. De esta manera se produce una autenticación mutua. Este sistema es vulnerable, ya que es sencillo obtener la clave de cifrado, el algoritmo no se considera seguro.

- Autenticación por dirección MAC: Es un mecanismo de autenticación basado en listas de control de acceso que contienen las direcciones físicas de los equipos (direcciones MAC7). Cada punto de acceso establece las direcciones que son válidas por autenticar un cliente en su red. Este sistema también es vulnerable ya que es sencillo capturar las direcciones permitidas por un punto de acceso concreto.

Con respecto a los mecanismos de autenticación, dos son las mejoras principales: en primer lugar, la inclusión de un servidor de autenticación externo. Hoy día RADIUS (Remote Access Dial-In User Service) es el estándar en redes fijas, y 802.11i prevé la interconexión de un servidor de este tipo. En segundo lugar, la introducción de un mecanismo más seguro de autenticación sobre el canal aéreo, basada en claves más seguras y que cambian periódicamente. El problema reside en cómo obtener la primera clave.

Aparte de eso, durante el proceso de autenticación, los interlocutores intercambian toda la información sobre las claves que utilizarán para el cifrado (y que serán diferentes de las hechas servir para la autenticación) y los algoritmos de cifrado escogidos. Esta información viaja, lógicamente, encriptada sobre el canal.
Con respecto a los mecanismos de cifradoe, las mejoras propuestas son:

- WPA (Wi-Fi Protected Access, también conocido como TKIP): Sistema de cifrado creado para eliminar las principales debilidades de seguridad de las redes sin hilos y de WEP. Se trata de un paso intermedio para sistemas que todavía no son totalmente compatibles con 802.11i, ya que se puede implementar con una sencilla actualización del software de los productos b y gr. Hace un proceso de encriptación más fuerte que WEP, pero las claves de cifrado son estáticas, cosa que lo hace todavía vulnerable.

- WPA2: Utiliza un nuevo sistema de cifrado, nombrado AES, considerado el más seguro conocido actualmente en cualquier tipo de red (con o sin hilos). Además, la clave cambia en cada sesión, y es diferente para cada usuario.

El problema más grave que encara se mantiene, a pesar de las mejoras mencionadas, es como conseguir la primera clave, nombrada llave maestra, que se utilizará para la autentificación inicial, y que permitirá conseguir todas las claves subsiguientes. El estándar aconseja hacer servir IPSec, pero eso sólo traslada el problema un paso más lejos, ya que la misma pregunta se puede hacer para la conexión inicial IPSec. En cualquier caso, la introducción de uno mecanismo de gestión de clavos, que permite actualizarlas para cada sesión mediante el servidor externo (típicamente RADIUS), es un gran paso adelante.

El 802.11i se puede considerar el paso que lleva las redes sin hilos al mismo estándar de seguridad que las redes fijas. Como serie de mecanismos transversales a la tecnología de transporte utilizadas, no se encontrarán productos en el mercado bajo esta denominación.

Lo que pasará es que los productos de otros estándares, como 802.11n o 802.11g, incorporarán los mecanismos del 802.11i, y serán compatibles. Como última reflexión, sin embargo, vale a decir que siempre está la posibilidad de incorporar medidas de seguridad en redes Wi-Fi a nivel de aplicación. Es decir, siempre es posible utilizar software especializado que cifre los datos del usuario y que las transmita a través de una conexión segura, como por ejemplo usando redes privadas virtuales (VPN), o las posibilidades de los navegadores actuales (SSL, HTTPS). Es por eso que si bien las redes Wi-Fi no se consideraban segura en los inicios, es justo decir que había mecanismos de más alto nivel para compensar estas deficiencias, de la misma manera que se utilizaban en redes fijas.

## *1.3. Itinerancia y movilidad*

Una de las utilidades más interesantes de la tecnología sin hilos es la posibilidad de cambiar de red sin necesidad de modificar la configuración del sistema, es decir, ofrecer Itinerancia (roaming) entre los diferentes puntos de acceso. Esta característica permite que el usuario pueda moverse por el territorio sin tener que hacer ninguna modificación en su PC de la misma manera que en el entorno a la telefonía móvil, es decir que no se pierde la cobertura y que se permite la movilidad entre diferentes islas Wi-Fi.

A fin de que la red permita itinerancia se tienen que configurar los puntos de acceso para que trabajen en diferentes canales de frecuencia, de manera que no se produzcan problemas de funcionamiento en aquellas zonas en que se crucen las coberturas de diferentes puntos de acceso, y el usuario "salte" de manera transparente de uno al otro.

Para la interconexión de puntos de acceso de diferentes fabricantes creando una única red por la cual los usuarios puedan moverse libremente, se ha aprobado recientemente el estándar 802.11f que, entre otros aspectos, define el registro de un punto de acceso dentro de una red y el intercambio de información con el otros puntos de acceso para permitir la funcionalidad mencionada.

Aun así, el problema más grave de la itinerancia entre islas Wi-Fi de diferentes propietarios deriva de la falta de estándares (de jure o de facto) sobre intercambio de información de autentificación.

En las redes de telefonía móvil, por ejemplo, se han establecido mecanismos para el intercambio de información sobre el estado del contrato y del crédito de un usuario que quiere conectarse desde la red de un competidor (en el extranjero, por ejemplo). En las redes Wi- Fi, estos acuerdos, a estas alturas, se hacen de una manera más ad hoc, lo cual dificulta en cierta manera la itinerancia internacional. Sin embargo, los operadores más grandes de redes Wi-Fi han llegado a acuerdos de iItinerancia de ámbito, incluso, mundial.

La movilidad pura, es decir, el hecho de poder mantener una comunicación en movimiento sin interrupciones a velocidades elevadas, es todavía un objetivo lejano de la subfamilia 802.11.

Actualmente, un nuevo estándar está en preparación, el 802.11p, que se ocupará precisamente de las comunicaciones en vehículos.

## *1.4. Futuras evoluciones de la tecnología Wi-Fi*

Los resultados más inmediatos, desde el punto de vista del usuario, serán sin duda la aparición de productos que implementan el estándar 802.11e y que, por lo tanto, dan la posibilidad de proveer de calidad de servicio a ciertos tipos de tráfico, especialmente la VoIP. Eso podría convertir la VoIP en una alternativa viable para dar cobertura a entornos rurales o de difícil acceso sin necesidad de desplegar infraestructura fija. Evidentemente, sólo como solución en el acceso más inmediato al usuario, ya que el Wi-Fi no está pensado como red de transporte, aunque hay iniciativas que han conseguido despliegues de gran alcance mediante esta tecnología.

El siguiente paso en esta evolución será la finalización del estándar 802.11n, y la aparición de productos que lo implementan. Si alcanzan el rendimiento que todo el mundo espera, éstos productos pondrán al mismo tiempo las redes de área local basadas en tecnología sin hilos y las más tradicionales basadas en FastEthernet, y abrirán la puerta a despliegues alternativos, completamente desprovistos de cableado, en entornos de oficinas y otras redes corporativas de pequeña dimensión.

Más a largo plazo se encuentran los trabajos, que acban de empezar, para alcanzar la movilidad en vehículos (802.11p), mecanismos más rápidos (y estandarizados) de itinerancia entre puntos de acceso (802.11r) y para simplificar la interoperación de redes Wi-Fi con otras tecnologías (802.11u). Este último estándar es particularmente importante para escenarios donde se quieran combinar redes Wi-Fi con redes de telefonía móvil, salto de la una en la otra sin tener que cortar la comunicación. Otras iniciativas destacadas son las de mejorar los mecanismos de gestión de las redes Wi-Fi (802.11v) y simplificar la creación de redes “mesh”, en las cuales los nodos actúan de repetidores los unos de los otros, y simplifican el despliegue de redes de alcance importante y con redundancia sin necesidad de puntos de acceso adicionales (802.11s).

# TECNOLOGÍA WIMAX

# TECNOLOGÍA WIMAX

La tecnología estandarizada por el IEEE bajo el apelativo 802.16, por lo común conocida como WiMAX, es considerada el hermano mayor del Wi-Fi. Eso responde al hecho que el WiMAX promete más alcance, más anchura de lado y más potencia que el Wi-Fi, acompañadas de más funcionalidad en términos, especialmente, de calidad de servicio y seguridad. Sin embargo, la publicidad que ha rodeado WiMAX ha creado unas expectativas que la tecnología no puede cumplir, como se explique a continuación. Todo ofrece un panorama similar a lo que va rodear la aparición del UMTS hace unos años, con la diferencia que los inversores no son tan proclives a comprometer grandes cantidades de dinero antes de haber comprobado las auténticas posibilidades de esta nueva tecnología.

La primera diferencia importante entre el Wi-Fi y el WiMAX radica en los diferentes ámbitos de aplicación para los cuales fueron diseñadas. El Wi-Fi surgió como una tecnología para cubrir los últimos metros del acceso y permitir al usuario librarse de la tiranía de los hilos en entornos de oficina o al hogar. La funcionalidad deseada era una anchura de lado comparable a la de las conexiones de lado ancha fijas disponibles (es decir, unos pocos Mbps) y un servicio best-effort (sin garantías de calidad), igual que las ubicuas redes Ethernet de área local en las cuales complementaba. Asimismo y como a consecuencia de el uso en lo que estaba destinada la tecnología, preferentemente surgieron productos para funcionar en la banda no regulada de frecuencia entorno en los 2,4 GHz, aunque también hay la posibilidad de utilizar la banda de los 5 GHz.

El WiMAX, por contra, fue diseñado como alternativa para dos grandes aplicaciones, las dos propias de operadores de telecomunicaciones, y no de usuarios finales. Por una parte, el WiMAX está destinado a ser la evolución del LMDS y el MMDS para la implementación de radioenlaces punto a punto. De la otra, el WiMAX es una tecnología adecuada para dar un servicio de acceso fijo; es decir, puede utilizarse como competidor o sustituto de la red de acceso fija (DSL y cable) en determinados entornos, especialmente en entornos rurales, donde el despliegue de soluciones de cable es muy costoso y los radioenlaces punto-multipunto se presentan como una alternativa flexible y más barata. Lógicamente, si las aplicaciones están orientadas a operadores de telecomunicaciones, no tiene sentido utilizar bandas de frecuencias no reguladas y por lo tanto susceptibles de interferencias. Es también por eso que el estándar incluye mecanismos de seguridad y QoS, ya que éstos son requisitos obligatorios para un servicio que quiere ser de categoría comercial.

Vista su orientación como servicio de distribución y de backhaul (conexión de redes entre sí), el alcance era un parámetro importando para el WiMAX. Originalmente, se utilizaron frecuencias elevadas, que permitían coberturas de decenas de kilómetros (10-66 GHz). El precio que hace falta pagar es que estas frecuencias necesitan una visión directa entre el emisor y el(s) receptor(s), así como equipamientos mayores y pesados, adecuados para ubicaciones fijas, pero no para ser transportados en laptops o PDA.

El WiMAX, por su parte, introdujo mejoras para el soporte de la movilidad (y no sólo de la itinerancia), a velocidades de hasta 120 km/h. También introdujo la posibilidad de complementar las redes “mesh” y mejoró el uso en interiores de edificios. En definitiva, evoluciones que permitieron al WiMAX promocionarse también como alternativa en las redes móviles convencionales en términos de ubicuidad, alcance y funcionalidad, como las redes de telefonía móvil 2G y 3G. Eso comporta, sin embargo, un desplaza-

miento hacia bandas de frecuencias más bajas (2-11 GHz), que permiten las transmisiones sin visión

### 1.4.1 Topologías de redes WiMAX

Las topologías propias de una red WiMAX pueden ser:

- **De distribución**: análogo a las redes de infraestructura Wi-Fi. La estación base ocupa el rol del punto de acceso y centraliza el acceso de los usuarios distribuidos por la celda en la red fija y a la salida hacia Internet. Además, se ocupa de gestionar el canal y distribuir los recursos en función de las necesidades de calidad de cada usuario.
- Malladas: análogo a las redes ad hoc, permiten la comunicación directamente entre estaciones móviles sin necesidad de pasar por una estación base. La gestión de los recursos es entonces distribuida. Un inconveniente de esta última característica es que, por razones de compatibilidad en los sistemas de gestión, a menudo todos los equipos han de ser del mismo fabricante.

## *1.5. Estándares WiMAX*

Como el WiMAX es un estándar más reciente que el Wi-Fi, el número y la complejidad de los estándares que lo componen es muy menor que en el caso precedente. Básicamente, actualmente sólo hay dos estándares a tener en cuenta: el IEEE 802.16-2004 y el IEEE 802.16e-2005.

Originalmente, el estándar 802.16 se finalizó el año 2001 y comprendía las funcionalidades básicas del WiMAX. Trabajaba en la banda de los 10 en los 66 GHz, que exigía visibilidad directa para la comunicación. Con canales muy anchos (hasta 28 MHz) y modulaciones eficientes, el estándar permitía capacidades teóricas de hasta 134 Mbps. El año 2003 se va publicar un estándar complementario, el 802.16a, que básicamente extendía el estándar original para bandas de frecuencias más bajas, que permitían la comunicación sin visibilidad directa, mejoraba la cobertura dentro de edificios y permitía establecer redes donde los mismos terminales WiMAX actúan como repetidores (mesh networks). El estándar 802.16d, más conocido como en 802.16-2004, unificaba ambos estándares en uno de sol, y además, incorporaba algunas correcciones sobre los estándares originales. Éste es el estándar de referencia actualmente, y para el cual empiezan a aparecer los primeros equipos. Con posterioridad se diseñó el estándar 802.16e, que incluía soporte para la movilidad con velocidades de hasta 120 km/h, así como soporte para la itinerancia, en la banda de frecuencias más inferior de las utilizadas por WiMAX. Este estándar ha pasado a ser conocido como 802.16e-2005.

Esta enorme flexibilidad en términos de bandas de frecuencia, anchuras de lado por|para canal, velocidades, etc. sólo se consiguió mediante un estándar de gran complejidad y con un gran número de parámetros y configuraciones posibles, muchas incompatibles entre sí. Además, aunque fuera técnicamente posible trabajar en este rango de frecuencias y anchuras de lado, la regulación de los diferentes países no necesariamente lo permite. Así, se han asignado segmentos del espectro para usos compatibles con la tecnología 802.16-2004 en las bandas de 3,5 GHz y 5,8 GHz. En cuanto al 802.16e, encara está a debate el rango de frecuencias que se le asignarán, aunque parece que bandas en los 2,3 y 2,5 GHz son las más probables (ambas regu-

ladas). En todos los casos, las anchuras de lado por canal permitidas son más reducidas de lo que el estándar permite, con valores que oscilan entre los 3,5 y los 10 MHz como máximo en realidad.

Como consecuencia de este doble requisito regulatorio y técnico, el IEEE acordó definir un número de configuraciones que fueron implementadas por todos los fabricantes y que aseguraron la interoperabilidad entre los productos.

Como se puede observar, son valores que están lejos de los máximos teóricos que constaban en la figura anterior. Sin embargo, los fabricantes son libres de implementar también otras configuraciones permitidas por el estándar. Así pues, para aquellos operadores que disponen de suficiente espectro asignado y del equipamiento adecuado, es posible superar estos valores. Además, estos valores se entienden por cada sector. De manera que si una antena tiene la capacidad de radiar en diferentes direcciones sin provocar interferencias consigo misma, estos valores se multiplicarán por el número de sectores en que radie la antena.

### 1.5.1 IEEE 802.16-2004: WiMAX para redes fijas y nómadas con calidad de servicio y seguridad

Como en el caso del Wi-Fi, el WiMAX define sólo los niveles más bajos de la tecnología, ombrados nivel físico y de enlace de datos, y deja todos los aspectos más próximos a los servicios y aplicaciones que se quieran utilizar en manos del mercado. Las diferencias que dan pie al mayor alcance de WiMAX y a su soporte de mecanismos de calidad de servicio, siempre con respecto al Wi-Fi, se encuentran en los orígenes y características de estos dos niveles.

Físicamente, el WiMAX utiliza una modulación conocida como OFDM, que permite un uso más eficiente del espectro que no el Wi-Fi (el 802.11a es la única variante de Wi-Fi que utiliza OFDM), y por lo tanto permite extraer más velocidad de la misma anchura de lado.

Sin embargo, hay todo un número de mejoras en el ámbito físico de WiMAX que introducen una mayor robustez ante errores, interferencias, etc. que en el caso del Wi-Fi. Estos mecanismos son básicamente de dos tipos:

- Forward Error Correction: La introducción de cierta redundancia en la información emitida, de manera que si hay pérdidas debidas, por ejemplo, a la meteorología, la información en recepción pueda ser reconstruida correctamente.
- Adaptive Modulation: El hecho de que la modulación utilizada se adapte automáticamente a las condiciones del canal. Wi-Fi también dispone de esta característica, que hace que la velocidad de transmisión varíe en función de la distancia, la lluvia, etc. En el caso de WiMAX, el número de modulaciones alternativas (y por lo tanto, de velocidades de transmisión) es de nuevo, más del doble que el Wi-Fi.

Por encima de estos mecanismos, el WiMAX introduce un sistema de reparto de las posibilidades de transmisión totalmente diferente al Wi-Fi, que es lo que permite que algunos flujos de datos tengan más prioridad y mejores garantías de calidad que otros.Básicamente, antes de transmitir o de recibir información con un determinado nivel de calidad, cada estación tiene que solicitar a la estación base los recursos (anchura de lado, retrasos máximos permisibles, etc.) que necesita para la aplicación a que vaya destinada la conexión. Como en el caso del 802.11e, recae sobre la estación base, y fuera de la especificación del estándar, definir los mecanismos por los cuales

se decide cuándo aceptar una nueva conexión y como decidir la manera de repartir los recursos, naturalmente limitados.

Lo que sí que especifica el estándar son las cuatro clases de servicio que el WiMAX soporta::

- Unsolicited Grant-Real Time: transmisión a intervalos regulares y garantizada por parto de la estación. Es el servicio de máxima calidad y está pensado para aplicaciones de voz y vídeo en tiempo real, como telefonía y videoconferencia.
- Real Time Polling: muy similar al HCCA de 802.11e. Aunque también da garantías de calidad, la transferencia ya no se hace en intervalos tan regulares como en la clase anterior y, por lo tanto, es más adecuado para transmisión de vídeo no interactivo, como ver televisión.
- Variable BitRate- Non Real Time: se garantiza una velocidad durante toda la transmisión, pero no una transmisión constante. Adecuado para servicios de datos donde se quiera asegurar una transmisión rápida y con un caudal garantizado.
- Variable Bit Rate - Best Effort: el servicio tradicional sin garantías de ningún tipo, más que suficiente, por ejemplo, para navegar por Internet.

Estas capacidades, junto en los mecanismos de robustez del WiMAX, permiten ofrecer, potencialmente, un servicio de alta calidad y de categoría profesional en operadores de telecomunicaciones. Ahora bien, la gestión de los mecanismos de calidad de servicio introduce uno nuevo elemento de complejidad en estas redes, que dificulta su despliegue y el uso para usuarios no profesionales.

Otra característica destacada del WiMAX es que incorpora en el mismo estándar los mecanismos de seguridad necesarios, ya que, como ya se ha explicado, es una tecnología destinada al uso de operadores de telecomunicaciones, que requieren esta funcionalidad. Podemos decir que el Wi-Fi en su estándar 802.11e incorporó muchos de los mecanismos que WiMAX implementa "de serie", y utiliza prácticamente los mismos mecanismos y algoritmos. Así pues, el WiMAX incorpora:

- Encriptación de los datos utilizando el algoritmo AES, igual que WPA2 del 802.11i.
- Autenticación entre la estación base y el usuario basada en certificados digitales X.509, para evitar suplantaciones de personalidad por parte tanto de la estación base como del usuario.
- Autenticación de cada mensaje donde se intercambia una nueva clave mediante una firma digital, para evitar que estos mensajes puedan ser interceptados y modificados.
- Llaves de encriptación y autenticación que se renuevan periódicamente, para evitar ataques basados en almacenar y repetir mensajes válidos y para evitar que se puedan romper estas claves.

Así pues, la seguridad en WiMAX es comparable a la conseguida por el Wi-Fi con las mejoras introducidas con el estándar 802.11i, y comparable a las de cualquier red fija adecuadamente protegida.

Los productos con certificación 100% WiMAX llevan poco tiempo en el mercado. Hay que prestar- allí atención, ya que algunos fabricantes sacaron en el mercado productos llamados "pre- WiMAX". Estos productos seguían las directrices generales de lo que se esperaba que fuera el estándar WiMAX, pero no necesariamente son compatibles, ni proporcionan la misma funcionalidad o rendimiento. Entonces

hay que evaluar esmeradamente la conveniencia de atarse a una línea de productos y a un fabricante que probablemente sean incompatibles con los futuros desarrollos del estándar WiMAX. Dicho esto, hay un gran número de productos y despliegues en el mercado basados en tecnología pre-WiMAX, especialmente como sustituto de LMDS que han dado resultados muy satisfactorios.

Para finalizar, se tiene que decir que todavía no han salido al mercado tarjetas PCMCIA para ordenadores portátiles, y muy menos portátiles con dispositivos WiMAX integrados, como sí que sucede en el caso de Wi-Fi. A pesar de una evidente reducción en dimensión y precio de los receptores WiMAX, todavía son más caros y más aparatosos que en el caso de Wi-Fi, lo cual los hace poco adecuados como tecnología móvil o incluso para soluciones en Itinerancia. Es ésta una razón más que decanta WiMAX hacia un uso más adecuado como tecnología de backhaul que no para el acceso final del usuario.

### 1.5.2 IEEE 802.16e: movilidad para WiMAX

Introducir movilidad en WiMAX, como ya se ha explicado, implicaba diversas modificaciones de el estándar:

- Trabajar.. en frecuencias más bajas, que permiten una mejor penetración en edificios y vehículos.

- Introducir una modulación diferente, nombrada SOFDMA, que permite adaptar parcelas del espectro a las condiciones exactas de cada usuario, que ahora serán mucho más diferentes que en el caso fijo, a causa de la velocidad. Vale a decir que esta modulación es incompatible con la utilizada por 802.16-2004, y por lo tanto el despliegue de una de las tecnologías implica el abandono de la otra, excepto que se hagan servir equipos duales, de muy elevado coste.

- Aplicar técnicas de emisión y recepción basadas en sistemas de múltiples antenas, que permiten aprovechar las reflexiones de la señal en paredes, árboles, etc. Tal como se ha explicado para el estándar 802.11n, se pueden transformar estas reflexiones, que en principio provocan interferencias, en una fuente adicional de información para reconstruir mejor la señal original, y obtener así un sistema más eficiente y más robusto. 802.16e introduce entonces el uso de más de una antena en cada punto de acceso y en cada terminal, de manera que se puedan aprovechar las reflexiones y combinarlas para obtener uno señal mejor. Al mismo tiempo, se puede enviar más de una señal a la vez (diversas antenas). Combinando ambos efectos, se consigue una transmisión más eficaz y más robusta, lo cual es crucial en entornos móviles. Esta técnica se llama MIMO (Multiple-input, Multiple-output), y en el caso de WiMAX se combina con AAS (Adaptive Antenna System). Esta segunda mejora permite no sólo combinar los señales de diversas antenas, sino que las características de emisión de cada antena se adaptan a las condiciones de potencia y ruido de cada receptor individual, y mejoran todavía más la recepción.

Adicionalmente, 802.16e introduce mecanismos que eran innecesarios en 802.16-2004, como la posibilidad para un receptor en movimiento de desligarse de la antena de la qual recibía la información y conectarse a otra de más próxima en algunos milisegundos, a medida que se desplaza. Ésta técnica, habitual en redes celulares y que nos permite mantener una conversación mientras estamos caminando o en el coche, se llama traspaso o handoff, y hay de diversos tipos. El estándar prevé todos los tipos de traspaso, y pone en WiMAX a la vez con las redes de telefonía móvil en este aspecto. Aun así, inicialmente, los equipos que saldrán al mercado sólo tendrán que so-

portar el llamado hard handoff; es decir, que podrá pasar hasta más de uno segundo entre el abandono de una antena y la conexión en la siguiente, lo cual puede dar pie a degradaciones apreciables de la comunicación, especialmente para servicios de voz. Para datos no sería prácticamente apreciable.

La gran ventaja del 802.16e es la posibilidad de mantener comunicaciones en movimiento hasta a120 km/h, aunque, cómo se ha explicado, los primeros productos que saldrán al mercado no tendrán toda la funcionalidad prevista al estándar. En este orden de cosas, las configuraciones obligatorias para productos 802.16e se aprobaron en febrero del 2006, y nada más se dispone de los primeros productos en el mercado que cumplen el estándar. Hay, como en apartados anteriores, productos propietarios de diversos fabricantes, que proponen soluciones para movilidad compatibles con WiMAX. Ahora bien, estas "soluciones" son adaptaciones de los sistemas de telefonía móvil 3G en entornos WiMAX, y no soluciones WiMAX compatibles con el estándar.

## *1.6. Futuras evoluciones de la tecnología WiMAX*

El estándar WiMAX no prevé para el futuro inmediato modificaciones de la talla de las convertidas en Wi-Fi. Así, los trabajos de estandarización en curso son de cariz más técnico, para corregir o aumentar funcionalidades ya existentes. De esta manera, el futuro estándar 802.16g se ocupa de los procedimientos y servicios de gestión de una red WiMAX.

802.16k estudia mecanismos de bridging y 802.16j, mecanismos de repetidores múltiples, ambos como complemento a las topologías de malla ya introducidas en 802.16a. Los trabajos hacia 802.16h buscan facilitar la coexistencia de diversas redes WiMAX en una misma área geográfica utilizando espectro libre, dónde por lo tanto ha posibilitado de interferencias entre las diferentes redes.

# GESTIÓN DE REDES

# GESTIÓN DE REDES WI-FI/WIMAX

Para suministrar servicios sobre cualquier red es necesario desplegar recursos adicionales a las tecnologías de telecomunicación que permiten conectar el equipo terminal con el punto de acceso al servicio donde se suministra éste y gestionar los accesos y las prestaciones de la red. Estos recursos adicionales permiten llevar a cabo las tareas siguientes que son clave para soportar el conjunto de procesos que facilitan la gestión y la explotación de la red y el servicio:

- Control de accesos: Agrupa todas las acciones encaminadas a.. facilitar o denegar el acceso a la red a los usuarios, junto con la aplicación de políticas de asignación de anchura de lado y calidad de servicio que se proporciona a cada uno.

- Gestión de contratación y facturación: Conjunto de facilidades que permiten que el usuario contrate, o actívese para utilizar el servicio, así como las reglas y los mecanismos utilizados parar tarificar y facturar el uso del servicio cuando el modelo de negocio prevé el pago de contraprestaciones económicas por parte de los usuarios.

- Gestión de quiebras y prestaciones: Actividades encaminadas a garantizar que la red suministra una calidad de servicio adecuada.

Estas tareas se tienen que desarrollar independientemente de la tecnología que se haga servir. Es decir, sea Wi-Fi o WiMAX, habrá que encontrar herramientas para desarrollar éstas mismas funciones. Aun así, como la experiencia con redes públicas Wi-Fi es mucho superior a la de redes WiMAX, esta discusión se centrará mucho en ejemplos aplicables en Wi-Fi, pero que son de aplicación directa a WiMAX en la mayoría de los casos, en utilizarse herramientas y procedimientos similares.

No siempre es necesario disponer de herramientas para llevar a cabo estas actividades, ya que los modelos de explotación más sencillos de estas redes, basados en un uso libre, gratuito y sin garantizaba de calidad de servicio, no hacen uso normalmente de estas capacidades. Así, por ejemplo, en el modelo de provisión de servicio más habitual de las comunidades sin hilos, todos los usuarios potenciales pueden acceder de forma gratuita al servicio sin hacer un registro previo y, por lo tanto, no se controlan los accesos ni es necesario soportar la contratación y facturación del servicio. En la mayoría de los modelos es necesario disponer de todas o al menos una parte de estas capacidades para suministrar el servicio.

Teniendo en cuenta esta necesidad, la disponibilidad, el coste, y la complejidad de instalación y uso de estos componentes son factores importantes para evaluar la viabilidad económica y técnica de despliegue y operación de este tipo de redes.

En general, el mecanismo de autentificación más utilizado en las redes públicas Wi-Fi, es el uso de identificador (login) y clave (password), proporcionados por el usuario a través de un portal cautivo que se presenta cuando éste intenta conectarse. El resto de mecanismos se utilizan en el contexto de redes privadas, donde los usuarios pertenecen a grupos reducidos y conocidos con antelación.

## *2.1. Estándares de autentificación y autorización*

Para soportar los servicios de autentificación, autorización y control de utilización de recursos (en terminología anglosajona, AAA, Authetication, Authorization & Accounting), los estándares 802.11 no incluyen estos servicios y dejan abierta la selección del modelo y el mecanismo para utilizar. El estándar aplicado de forma universal por la gran mayoría de proveedores de servicios es RADIUS (Remote Access Dial-In User Service).

Los productos que implementan RADIUS disponen de acceso a bases de datos de usuarios configurables mediante APIO accesibles para las aplicaciones de contratación y facturación y facilidades para controlar los tiempos acumulados de uso de la red, expiración de periodos contratados y, de forma más limitada, recogida y gestión de volúmenes de tráfico intercambiados.

La evolución de RADIUS pasa por la implantación del protocolo DIAMETER que potencia la flexibilidad de RADIUS en la gestión de perfiles de usuario para gestionar las cualidades de servicio ofertas. Ofrece más robustez y flexibilidad en el control de los recursos. En el contexto actual de los servicios prestados por las redes públicas Wi-Fi, DIAMETER no ha sustituido encara a RADIUS en las iniciativas existentes, si bien es posible que en un futuro las redes evolucionen hacia el uso de DIAMETER, especialmente para la aplicación de modelos de facturación para uso en la transmisión de voz sobre IP o una gestión más sofisticada de las cualidades de servicio ofertas a los clientes. IMS tiene en cuenta también la utilización de DIAMETER en redes móviles adelantadas, por lo cual se prevé que en un futuro sea posible coordinar la validación de los usuarios sobre diferentes tecnologías de red.

## *2.2. Productos de autentificación y autorización*

Para llevar a cabo las funciones descritas, actualmente se dispone tanto software comercial como de software libre. Dentro del software comercial, el más extendido es Bluesocket (www.bluesocket.com). Con respecto a software libre, NoCat (www.nocat.net) es un producto de Linux, que se utiliza extensamente como software de gestión de accesos bajo el modelo de portal cautivo. Aunque no dispone de capacidades tan adelantadas como los productos comerciales, es una buena alternativa para la construcción del control de accesos en este tipo de redes públicas, soportando el estándar RADIUS, gestión de calidad de servicio segmentada por usuarios y grupos y apoyo|soporte a SSL. FreeRadius (www.freeradius.org) es otra iniciativa de desarrollo de software libre de autentificación y autorización. En el contexto de herramientas de software libre destacan también LANRoamer, Wireless Heartbeat (http://www.river.com/tools/authhb/), y Firstspot (www.patronsoft.com), basados en portal cautivo.

## *2.3. Contratación y facturación*

Los mecanismos de contratación y facturación del servicio facilitan la interacción con el usuario para que éste se dé de alta al servicio y abone el importe establecido para el uso de los servicios.

La aplicación de las redes Wi-Fi para mercado residencial como infraestructura de acceso de banda ancha utiliza los mecanismos habituales de contratación y facturación establecidos para las redes fijas: contratación del servicio por vía telefónica, web o en persona y facturación mediante una cuenta corriente con pagos mensuales.

En el caso de redes WIFI/WIMAX orientadas a un uso itinerante y ocasional de la red, como es el caso del despliegue en vías públicas, es necesario disponer de un sistema de contratación y facturación de uso sencillo y rápido, que faciliten la contratación y el uso en el momento, con el fin de incentivar la utilización. Así pues, las soluciones identificadas para contratar y facturar el servicio para uso itinerante, difieren de las soluciones utilizadas en redes fijas y de telefonía a causa de la necesidad de soportar el uso ocasional de las redes sin que haya una relación estable ni previa entre el usuario potencial y el proveedor de servicio. Las alternativas en este campo son:

- **Sistemas de prepago**: Consisten a hacer efectivo y por adelantado el pago de los servicios de donde se van descontando los consumos realizados por el usuario. Una vez agota el crédito disponible no puede disfrutar de servicio hasta que no efectúa uno nuevo prepago.
- **Micropago basado en SMS**: Se obtiene una contraseña para conectarse a la red durante un breve periodo de tiempo a cambio de enviar un SMS premium a un número contratado por el proveedor de la red Wi-Fi.
- **Prepago vía web**: Cuando un usuario intenta acceder a la red, se le presenta una página con las condiciones del servicio y un acceso para contratarlo. La contratación se lleva a cabo mediante un prepago basado en tarjeta de crédito, por eso el cliente tiene que suministrar su identidad y sus datos de tarjeta.
- **Prepago en ubicación de la red**: En este caso el pago se lleva a cabo presencialmente en la ubicación donde se encuentra disponible el servicio. Es el caso de los cibercafés que disponen de redes Wi-Fi, o los hoteles que suministran este servicio de pago.
- **Empaquetamiento con otros servicios**: El usuario adquiere el derecho para utilizar la red mediante la contratación de otros servicios. Muchas veces se presenta éste empaquetamiento como "Wi-Fi gratuito", al conceptuarse como un servicio suplementario al servicio principal que se comercializa.
- **Pago basado en exposición a publicidad**: Igual que el empaquetamiento de servicios, en este caso el servicio es presentado al cliente como "gratuito", si bien el modelo de financiación se basa al exponerlo a publicidad contextual (pop-ups y bàners).

El modelo más extendido para usuarios ocasionales es el basado en tarjetas de prepago. Este modelo es uno de los que más crecimiento ha tenido en los últimos años como modo de suscripción con pago regular para usuarios residenciales.

Con respecto a la generación de facturas, la mayoría de los modelos no necesitan abordar este problema de cara al usuario final, al basarse en pago gratuito o prepago.Sí que es necesario en el pago por suscripción, que se resuelve mediante soluciones ad hoc o integración en la facturación de otros servicios, cuando el acceso Wi-Fi se empaqueta con otros productos.

## *2.4. Gestión de incidencias y prestaciones*

Para suministrar una adecuada calidad de servicio a los usuarios es necesario llevar a término actividades de mantenimiento preventivo que permitan detectar situaciones de pérdida o disminución de servicio y de mantenimiento correctivo que permitan resolver los problemas que afecten al servicio proporcionado a los usuarios, como la avería en puntos de acceso.

Para llevar a cabo estas actividades se utilizan herramientas de monitorización y configuración que permiten supervisar el estado de los puntos de acceso remotamente, mostrando problemas detectados de congestiones, averías, etc. Estas herramientas se comunican con los puntos de acceso mediante pruebas sencillas de operatividad en los casos más básicos (por ejemplo, intentos de conexión o pings), o accediendo vía SNMP (protocolo normalizado de gestión) a los parámetros más relevantes de operatividad que se almacenan y se gestionan en tiempo real en los mismos puntos de acceso.

Además del software de monitorización y gestión remota, los operadores que hagan despliegues comerciales con extensión geográfica importante, tienen que disponer de herramientas que permitan llevar a cabo la atención a los usuarios para gestionar reclamaciones e incidencias de servicio, que se soportan mediante centros de atención al cliente en las iniciativas con más ámbito y con pequeñas herramientas realizadas ad hoc en otros.

# CONCLUSIONES

# CONCLUSIONES

Las redes sin hilos basadas en los estándares 802.11x y 802.16 llamadas Wi-Fi y WiMAX, respectivamente, representan una novedad sustancial en el panorama de las telecomunicaciones, ya que amplían lo que tradicionalmente eran tecnologías restringidas sólo en|a el ámbito de empresa hacia el mundo de las tecnologías de redes públicas. La causa de esta nueva característica hay que verla no sólo en el hecho de que el Wi-Fi elimina los cables, sino también en la sencillez de instalación, la flexibilidad, el bajo coste y la gran anchura de lado que proporciona al usuario. A todas estas facilidades se les ha añadido la nueva tecnología WiMAX que permite dotar de enlaces con más capacidad y calidad de servicio, y es el complemento ideal en algunos despliegues municipales que no disponen de soluciones de lado ancha fija.

A través de las tecnologías Wi-Fi y WiMAX se puede dar solución a múltiples problemáticas en el entorno a un municipio: establecimiento de redes locales en el interior de edificios, interconexión entre edificios, servicio de acceso para los trabajadores municipales móviles itinerantes que se desplazan por la vía pública, y finalmente conexión de los ciudadanos en la red, ya sea para acceder a los servicios telemáticos municipales o a Internet. Se espera en los próximos años un crecimiento sostenido de los ordenadores portátiles y de bolsillo, de tal manera que se puede garantizar un número muy importante de usuarios con posibilidad de conectarse a las redes públicas Wi-Fi.

Aun así, si bien el Wi-Fi ya ha demostrado ser una tecnología versátil que se puede adaptar a muchas de las necesidades que puede tener un ayuntamiento o un municipio, sufre todavía ciertas limitaciones que hay que considerar: el hecho de trabajar en bandas de frecuencia abiertas y de uso no privativo, y también una seguridad de las comunicaciones encara en proceso de mejora. El WiMAX se presenta como una tecnología con más recorrido, todavía no está tan extendida como la Wi-Fi, pero ya ha sido diseñada para poder dar solución a los principales retos tecnológicos de las redes sin hilos de alta capacidad.

Estas dos características hacen que en algunas topologías de configuración las ventajas de las redes sin hilos puedan disminuir a medida que se van añadiendo nuevos usuarios.

Es por eso que en primera instancia esta tecnología parece más indicada sobre todo para proyectos de complejidad media y baja, y en entornos geográficamente limitados.

Configuraciones más complejas son también posibles pero exigen una planificación y operación significativamente más importante y, por lo tanto, una inversión más elevada.

En cualquier caso, la implantación de redes sin hilos en el entorno municipal implica el cumplimiento de una serie de requisitos que hagan estos sistemas plenamente sólidos: la existencia de un proyecto técnico solvente, un modelo de negocio contrastado, la adecuación a las normativas y el establecimiento del mantenimiento y la gestión oportunos para hacer una herramienta económicamente sostenible y socialmente rentable.