Redes locales y metropolitanas sin hilos

PID_00265433

Antonio Satué Villar

Tiempo mínimo de dedicación recomendado: 4 horas

Universitat Oberta de Catalunya

Antonio Satué Villar

Doctor ingeniero en Telecomunicación por la Universidad Politécnica de Cataluña, en el año 2007. Desde el año 1994 es profesor de la Escuela Universitaria Politécnica de Mataró y secretario académico desde el año 2009. Su línea de investigación se centra principalmente en el ámbito del reconocimiento de locutor y las aplicaciones biométricas. En este sentido, participa en distintos proyectos de ámbito nacional y europeo.

La revisión de este recurso de aprendizaje UOC ha sido coordinada por el profesor: Ferran Adelantado Freixer (2019)

Segunda edición: septiembre 2019

Av. Tibidabo, 39-43, 08035 Barcelona
Realización editorial: FUOC

Índice

Introducción

En el módulo anterior hemos hablado de las redes sin hilos de tipo personal (de corto alcance). En éste aumentamos el radio de acción de las redes y nos moveremos en coberturas de tipo local y de tipo metropolitano.

Las redes locales sin hilos son aquellas que permiten dar servicio a distancias a un centenar de metros aproximadamente (un piso, una planta de un edificio, una nave industrial, unas calles...). Comentaremos las diferentes tecnologías y nos detendremos en la 802.11, que es la dominante en el sector y la que presenta un ritmo más elevado de actualizaciones.

Las redes metropolitanas inalámbricas permiten dar servicios a distancias de un kilómetro aproximadamente. Así, podremos dar cobertura en un barrio, en un pueblo o en una urbanización, entre otros. Aquí comentaremos las tecnologías basadas en el estándar 802.16, que es el referente en este tipo de redes. Aun así, hoy en día su uso decae puesto que se usan redes de gran alcance para dar solución a necesidades de alcance medio (alcance metropolitano).

Objetivos

Los contenidos de este módulo deben permitir a los estudiantes:

1. Comparar las redes de infrarrojos y las láser.

2. Describir la arquitectura de red 802.11 y las funciones de sus elementos.

3. Diferenciar los mecanismos de transmisión coordinado y distribuido en redes 802.11.

4. Describir el mecanismo de ahorro de potencia en redes 802.11.

5. Describir los mecanismos para dar calidad de servicio en redes 802.11.

6. Describir los mecanismos de seguridad en redes 802.11.

7. Diferenciar LMDS y el estándar 802.16.

8. Enumerar los perfiles que define el estándar 802.16.

9. Describir los tipos de calidad de servicio que ofrece el estándar 802.16.

10. Diferenciar las topologías de red del estándar 802.16.

11. Describir los aspectos que deben tenerse en cuenta antes de adquirir productos 802.16.

1. Introducción

En este módulo hablaremos de las redes locales y metropolitanas sin hilos. Es decir, redes con un alcance de hasta unos cuantos kilómetros. Las principales ventajas de estas redes sin hilos con respecto a las cableadas son:

- Permiten movilidad (más o menos).
- Son flexibles, ideales para instalaciones temporales.
- Son fáciles de instalar.
- Permiten su integración con sistemas cableados.
- Son adecuadas para instalaciones en edificios de alto valor histórico donde hay restricciones a las obras que se hacen en el interior.
- Son adecuadas en grandes naves industriales donde las canaladuras de cableado pueden dificultar el paso de maquinaria.
- Pueden ser una vía alternativa en la red cableada, como sistema de seguridad.

También hay algunos inconvenientes:

- Precio elevado, aunque cada vez hay menos diferencias.
- Poca velocidad, aunque hay tecnologías sin hilos que pueden competir con las técnicas cableadas de gran velocidad.
- Sensibles a hornos microondas (los 2,4 GHz son capturados óptimamente por el agua) o cambios de humedad.

1.1. Clasificación

A continuación comentaremos las tecnologías que permiten implantar redes locales sin hilos:

1) Infrarrojos

Los primeros experimentos se hicieron en Suiza en 1979.

El diseño es simple (económico), ya que los receptores sólo detectan la amplitud de la señal. La detección de frecuencia y/o fase es compleja. El dispositivo

emisor es el LED (*light emiting diode*), que emite luz que se propaga por el medio. El receptor es un fotodiodo PIN, que recibe los pulsos de luz y los transforma en señales que pueda entender el ordenador (bits).

Utilizan rayos infrarrojos (longitud de onda aproximada: 870 nm), o sea, frecuencias muy elevadas que no sufren congestión. Por contra, comparten espectro con los fluorescentes (éstos reducen la relación señal-ruido en el enlace).

Necesitan visión directa entre nodos y la distancia se limita a 10-25 m. Eso hace que:

- No admitan vibraciones.
- No puedan atravesar paredes. Eso también puede ser positivo, ya que tenemos muy controlada la información (los datos están confinados en la trayectoria).
- Les afecte la lluvia pero todavía más la niebla (perturba la visión).

Observación

Las paredes pueden servir para provocar reflexiones deseadas. Los vidrios pueden atravesarse en ciertos casos.

2) Espectro ensanchado

Estas técnicas se basan en distribuir los datos en un margen frecuencial de banda ancha (típicamente en torno a los 2,4 GHz o bien a los 900 MHz) mediante un código de expansión que sólo es conocido por el receptor. Estas frecuencias se corresponden con la banda ISM (*industrial scientifical medicine*), en la que no se requiere licencia para emitir. La banda ISM tiene una tercera zona en torno a los 5,8 GHz, pero tenemos interferencias de ratones sin hilos, microondas, mandos a distancia...

En España, la banda ancha ISM está especificada en la norma UN-51: 2,45 GHz, 5,8 GHz, 24 GHz y 61 GHz. En la banda ancha ISM:

– No debemos interferir (hay límites de potencia de emisión).
– No podemos solicitar protección frente a servicios autorizados de más categoría.

La norma UN-51...

... especifica genéricamente la banda ISM. Pero hay otras bandas que también son de uso común:

- **UN-85**: redes sin hilos a 2,4 GHz.
- **UN-109**: vídeo de corto alcance a 2,4 GHz.
- **UN-115**: uso de bandas estrechas (434 MHz, 868 MHz...).
- **UN-128**: redes sin hilos a 5,8 GHz.
- **UN-129**: uso de la banda de 2,4 GHz.
- **UN-130**: uso de la banda de 5,8 GHz.

Las técnicas de espectro ensanchado son de dos tipos:

– ***Frequency hopping* (FHSS):** cambia de frecuencia de una manera seudoaleatoria (PN) sólo conocida por emisor y receptor.

– ***Direct sequence* (DSSS):** la información se multiplica por una secuencia seudoaleatoria conocida por emisor y receptor.

En estas frecuencias se pueden atravesar obstáculos. Estas técnicas son la base de los sistemas actuales de redes locales sin hilos.

3) Láser

No es una tecnología específica, sino que es una extensión de los infrarrojos pero para distancias mayores.

Tiene las propiedades de los infrarrojos pero con más ventajas:

- Distancias mayores (hasta 5 km)
- Velocidades mayores (hasta 2,5 Gbps)

Algunas aplicaciones son:

- Conexión de edificios
- En puentes, para transmitir datos provenientes de cámaras de tráfico
- Enlaces en aeropuertos

WEB

En aeiwireless.com y lightpointe.com podemos encontrar información de productos láser.

El inconveniente principal es el precio. Por ejemplo, en diciembre del 2006 los elementos necesarios para hacer un enlace punto a punto de 1 km láser a 1 Gbps tenían un coste aproximado de 15.000 euros.

2. Estándar 802.11

En 1990 el IEEE creó el grupo de trabajo 802. En Europa, el ETSI creó en 1991 el comité RES10 para definir también sus estándares propios.

Los estándares del ETSI se llaman *hiper-LAN (high performance radio LAN*) y son:

- **Hiper-LAN/1**
  Es un estándar de 1996 que obtiene 23 Mbps trabajando a 5,8 GHz. Ha tenido poca aceptación por parte de los fabricantes.

- **Hiper-LAN/2**
  Este estándar, del año 2000, obtiene 54 Mbps trabajando a 5,8 GHz. Ha tenido más aceptación que hiper-LAN/1, pero aún así su uso es muy minoritario frente a los estándares del IEEE.

  Hay otros estándares, com hiper-LAN/3 (*hiperaccess*) e hiper-LAN/4 (*hiperlink*), pero no han tenido mucho éxito de mercado.

Observación

Las velocidades de las que hablamos son brutas (incluyen las redundancias, bits de control...). Las velocidades útiles son menores.

Los estándares del IEEE son los que realmente han llegado al mercado, y son los que estudiaremos en este capítulo. Del ETSI sólo hay algunos productos hiper-LAN/2 y hay un estándar 802 (el 802.11h) que los quiere hacer compatibles con los productos 802 que trabajan en la misma frecuencia (5,8 GHz).

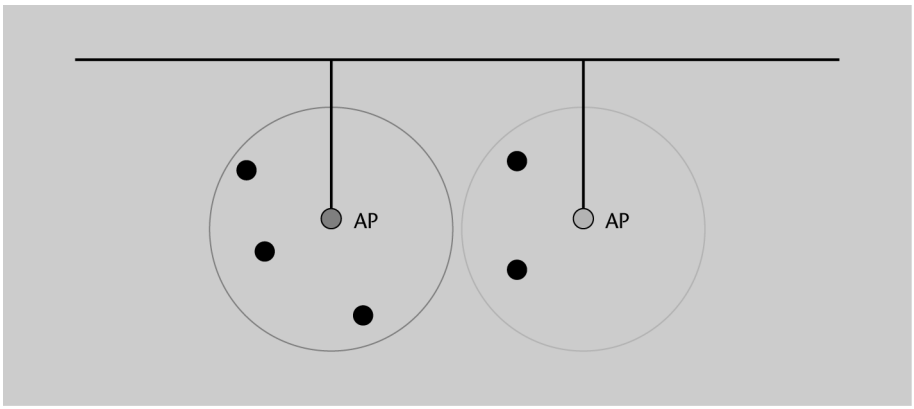
El objetivo del grupo de trabajo 802.11 del IEEE es definir un conjunto de protocolos de acceso al medio (MAC) que puedan trabajar independientemente de la capa física (por ejemplo, con el estándar Ethernet 802.3). El primer estándar se creó en junio de 1997.

2.1. Arquitectura

La arquitectura 802.11 consta de estaciones (figura siguiente), y una de ellas puede hacer funciones de AP (*access point*). Un AP es una estación que permite el acceso a otras redes.

Una BSS (*basic service set*) es el conjunto de estaciones conectadas a un mismo AP. Un ESS (*extended service set*) es el conjunto de BSS interconectadas. Dependiendo de la necesidad se pueden definir coberturas disjuntas (para cubrir más área) o solapadas (para mejorar el servicio en un área). Si queremos que varios AP formen parte de la misma red, les pondremos el mismo **SSID** (identificador de ESS o *service set identifier*). La medida de seguridad más básica cuando un usuario quiere acceder a una red es mirar su SSID.

Figura 1. Arquitectura 802.11



2.2. Acceso al medio

Hay tres opciones para la capa física: DSSS, FHSS e infrarrojos. Los estándares 802.11 permiten que una red de área local sin hilos interactúe con redes cableadas o sin hilos del mismo tipo.

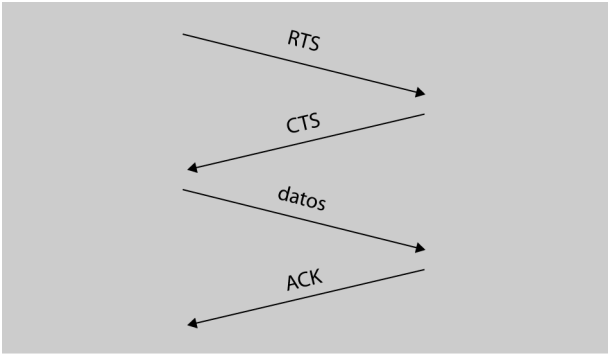
Cuando varias estaciones quieren acceder al medio se utiliza la técnica CSMA/CA para resolver las colisiones.

CSMA (*carrier-sense multiple access*): el mecanismo *carrier-sense* determina si la energía de señal en un determinado ancho de banda supera un cierto umbral.

> Si la energía es inferior al umbral, eso quiere decir que nadie está transmitiendo. En este caso, enviamos una trama. Si la energía es superior al umbral, esperamos un tiempo de retraso (*backoff*) y lo volvemos a intentar.

CA (*colision avoidance*): la estación destino confirma cada trama que recibe (eso lo hace enviando un ACK inmediatamente después de cada trama recibida). Si el emisor no recibe el ACK, se retransmitirá la trama.

> En redes fijas se hace CD (*colision detection*) porque, después de enviar, el transmisor puede escuchar el medio. Ahora no lo podemos hacer, porque el margen dinámico de las señales en el aire es grande (podemos tener dispositivos ocultos para el transmisor pero no para el punto de acceso).



Para soportar servicios que admitan poco retraso, se establecen niveles de prioridad. Así, los servicios que admiten poco retraso tienen un tiempo más bajo de *backoff*.

Mecanismo CSMA/CA del 802.11

Hay dos modos de transmisión:

- DCF (*distributed coordination function*). Viene por defecto.
- PCF (*point coordination function*). Hay un Access Point, que hace *pollings* a las estaciones (tareas de coordinación). Se tiene que configurar.

Observación

En una misma red podemos usar los dos modos alternativamente.

Manera de transmitir en un canal:

1) Miramos el canal.

2) Si está ocupado, lo monitorizamos hasta que esté libre.

3) Cuando esté libre, hay tres tiempos de espera diferentes (tres prioridades):

– DIFS (*distributed inter-frame space*). Para el modo DCF.
– PIFS (*point inter-frame space*). Para el modo PCF.
– SIFS (*short inter-frame space*). Lo utilizan las estaciones que deben enviar un ACK (tienen prioridad).

DIFS > PIFS > SIFS

El estándar define los siguientes tiempos de espera (en microsegundos)

Estándar	SIFS	PIFS	DIFS	Ranura**
802.11	10	30	50	20
802.11b	10	30	50	20
802.11a	16	25	34	9
802.11g	10	19 / 30*	28 / 50*	9 / 20*

* Si tenemos estaciones tipo 802.11b (b y g son compatibles).
** Cuando alguien colisiona, espera cierto número de ranuras.

En el apartado 2.5 hablaremos de los distintos estándares (b, a, g).

4) Después se establece una contención (*backoff*), que es esperar un número de ranuras de forma aleatoria. Si alguien tiene un número grande de éstas, en posteriores intentos se le priorizará.

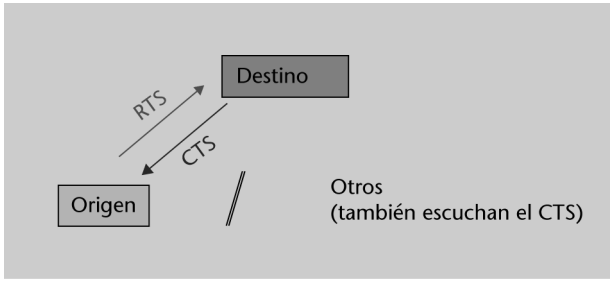
– Un *backoff* alto es bueno para evitar colisiones, pero puede ser que el canal esté libre y todas las estaciones en *backoff*.
– Más adelante veremos que este *backoff* nos permite especificar diferentes QoS.

5) Si dos estaciones transmiten al mismo tiempo, no recibirán el ACK, y cuando vuelvan a probar el número aleatorio será de 0 a 4, y después de 0 a 15, etc. de forma exponencial, ya que con el paso del tiempo tenemos más estaciones que lo pueden intentar (figura siguiente).

Figura 2. Tiempo de contención

Es preciso un RTS/CTS, ya que podemos tener estaciones que no se vean entre ellas.

Figura 3. Mecanismo RTS/CTS



- Cuando una estación quiere transmitir, envía un RTS con un tiempo de reserva del canal.
- Cuando el punto de acceso recibe el RTS, envía un CTS con el mismo tiempo de reserva, para que lo escuchen todas las estaciones (figura anterior).
- Mientras que una estación tiene el canal reservado, las demás, aunque lo vean libre, no pueden transmitir.

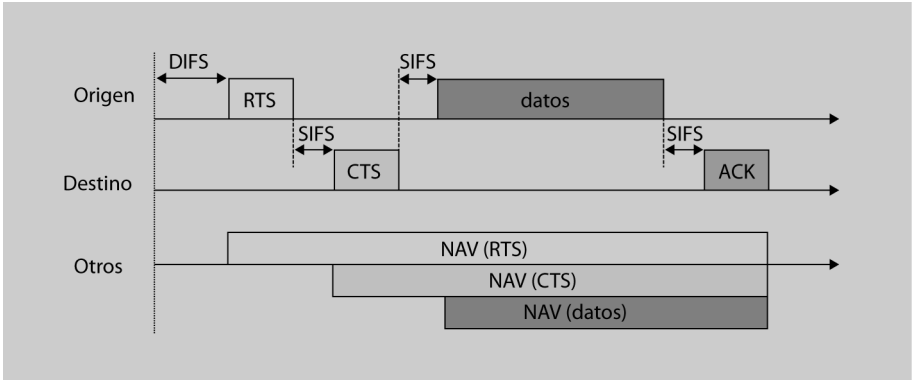
Respecto a la conveniencia del mecanismo RTS/CTS, debe tenerse en cuenta que:

- Para pocos usuarios, RTS/CTS ralentiza. Para muchas máquinas, mejor ponerlo.
- RTS/CTS va bien para paquetes grandes. Ese tamaño de paquete a partir del cual utilizamos RTS/CTS depende del número de estaciones. Así, por ejemplo, podríamos decir que para diez estaciones, todos los paquetes superiores a 3.000 bits hay que enviarlos en modo RTS/CTS. Eso es configurable.

Ya se ha comentado que dentro del RTS se inserta la información de cuánto tiempo tendrá ocupado el canal (mensaje NAV, *network allocation vector*).

En la figura siguiente tenemos un ejemplo:

Figura 4. Ejemplo



- Si no hay colisiones, estamos deteriorando el rendimiento (*throughput*).

– Aunque haya un tercer terminal que no escuche la transmisión del nodo origen, puede conocer que el canal será ocupado si escucha la respuesta del nodo destino.

El sistema tiene un mecanismo para fragmentar paquetes, que deberemos activar (podemos configurar a partir de qué tamaño) si la BER (tasa de error de bit) es muy alta. Así, si hay algún error, sólo se retransmite el fragmento afectado. La siguiente expresión nos dice la tasa de error por paquete (PER) en función de su tamaño (*N*) y la BER.

$$\text{PER} = 1 - (1 - \text{BER})^N$$

Por ejemplo,

PER	*N* = 200	*N* = 2.000
BER = 10^{-4}	2%	20%
BER = 10^{-5}	0,2%	2%

Fijémonos en que el modo DCF no garantiza un retraso máximo ni un ancho de banda mínimo.

El modo PCF gestiona el punto de acceso con *pollings* en las estaciones cada cierto tiempo. El inconveniente es que, si una estación no tiene nada que transmitir, perdemos ancho de banda.

Observación

Suele ser habitual una combinación de los dos modos DCF y PCF.

El coordinador divide el tiempo en periodos DCF y periodos PCF:

- En el PCF, las estaciones ponen el NAV en el máximo valor. Sólo responden si son sondeables (hay que configurarlo) y cuando le enviamos un paquete de permiso de transmisión.
- El coordinador utiliza el PIFS.
- Cuando ha acabado, envía un CFend (*colision free end*).
- El coordinador puede enviar cuatro tipos de tramas:

– Datos (*unicast*, *multicast* o *broadcast*). El receptor debe enviar un ACK.

– Sondeo a una estación. La estación debe enviar una trama, aunque esté vacía (trama NULL).

– Datos y sondeo.

– CFend.

Sincronización

Cada estación tiene su reloj, pero entre ellos se sincronizan con el *beacon* (aproximadamente, cada 100-200 ms):

- Si es red con infraestructura, lo emite el AP.
- Si es *ad hoc*, lo intentan las estaciones. Cuando una lo consigue, las otras anulan los envíos.

2.3. Ahorro de potencia

El estándar incluye un protocolo que permite dejar el móvil en estado de reposo; con eso reducimos el consumo sin perder las comunicaciones. Este proceso es configurable y básicamente consiste en desconectar la recepción de vez en cuando:

- La estación se conecta periódicamente para ver si tiene datos para recibir.
- La estación puede estar despierta o dormida.
- Es necesaria la colaboración de los emisores para guardar los datos de las estaciones dormidas.
- Para recibir, todas las estaciones se despiertan al mismo tiempo.
- Las estaciones que tienen datos para transmitir envían una lista de las estaciones para las que tienen datos en cola (estarán despiertas hasta recibirlas; las otras estarán dormidas).
- Redes con infraestructura: en el *beacon* se envía la lista de receptores (TIM, *traffic indication map*). En tramas *broadcast* tenemos la DTIM (*delivery TIM*) para que todos estén despiertos. Este proceso lo hace el AP.
- Redes *ad hoc*: cada estación debe guardar sus datos en las estaciones que están dormidas. Hay momentos en los que envían tramas ATIM (*adhoc TIM*) y los receptores contestan con ACK ATIM (y se quedan despiertos).

2.4. Calidad de servicio

Antes hemos visto que la ventana de *backoff* nos puede servir para definir calidades de servicio. Básicamente hay tres tipos de actuaciones que pueden hacerse:

1) Actuaciones sobre la ventana de *backoff*:

– Podemos variar los límites de la ventana de *backoff* (dar valores pequeños al usuario más prioritario). Así, cada usuario tiene un CWmín (valor mínimo de la ventana) y un CWmáx (valor máximo de la ventana).

– Podemos variar los límites de la ventana sólo en caso de colisión. Así, asignamos un parámetro *P* a cada usuario de manera que el tamaño de la ventana en el intento $n + 1$ dependerá del tamaño en el intento n según la expresión:

$$\text{CWmáx}\ (n + 1) = 2 \cdot P \cdot \text{CWmáx}\ (n)$$

Daremos valores pequeños de *P* a los usuarios más prioritarios.

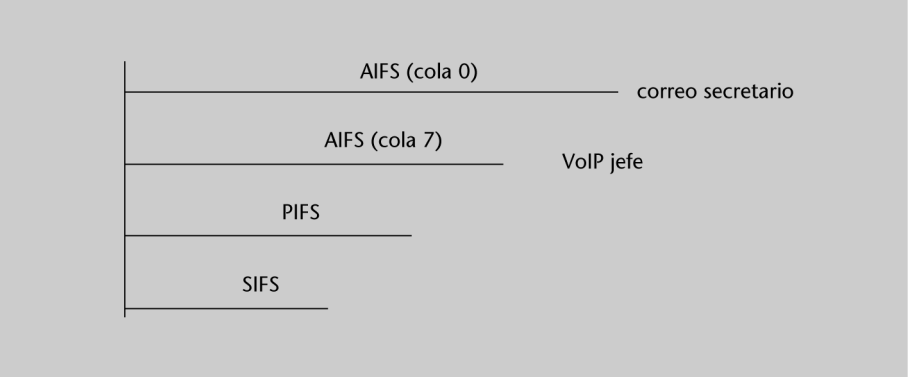
2) Actuaciones sobre el DIFS: modificaremos el DIFS de manera que el nuevo DIFS será el antiguo DIFS más un parámetro *Ri*, donde *Ri* es pequeño para usuarios prioritarios.

3) Actuaciones sobre los instantes PCF: podemos ranurar los instantes PCF (en los que el AP coordina) de manera que priorice a ciertos usuarios.

Hay un grupo de trabajo dentro del 802.11 que en el año 2004 definió un estándar de calidad de servicio llamado **802.11e** (o *extended DCF*), que consiste en lo siguiente:

- Cada estación tiene ocho colas para ordenar su tráfico (figura siguiente). A cada categoría definimos unos AIFS (*arbitration inter frame space*) y después unas ventanas de *backoff* (con su CWmín y CWmáx). Si el AIFS es grande, eso quiere decir que la prioridad es pequeña.

Figura 5. Colas de tráfico



- Cuando una estación accede al canal, puede transmitir varios paquetes consecutivos durante un tiempo TXOP (*transmission opportunities*). Cada cola tiene su TXOP límite.

- Define el HCF (*hybrid coordination function*) de manera que, si alternamos DCF y PCF, en el DCF el punto de acceso puede poner información en el momento que quiera.

2.5. Estándares 802.11

La tabla siguiente muestra los primeros estándares 802.11 más importantes. Actualmente, una buena parte de los productos en el mercado europeo son 802.11g.

Estándar	Año	Tecnología y banda	Velocidad
802.11	1997	Infrarrojo	1 o 2 Mbps
		FHSS 2,4 GHz	
		DSSS 2,4 GHz	
802.11b	1999	DSSS 2,4 GHz	11 Mbps
802.11a	1999	OFDM 5,8 GHz	6-54 Mbps
802.11g	2003	OFDM 2,4 GHz	54 Mbps

La modulación OFDM (*orthogonal FDM*) consiste en repartir los datos en un gran número de portadoras de baja velocidad moduladas individualmente, y permite buena eficiencia espectral y resistencia a los efectos de la propagación multicamino.

Hay que tener presente que a distancias máximas se utilizará la velocidad mínima (y más robusta ante errores).

Hoy en día, Wi-Fi abarca todos los estándares 802.11. Quien supera el protocolo de pruebas Wi-Fi (determinado por la Wi-Fi Alliance) puede llamarse *Wi-Fi*.

Las notas UN-85 y UN-128 del CNAF (Cuadro Nacional de Atribución de Frecuencias) determinan las condiciones de uso de las bandas Wi-Fi:

a) UN-85

- De 2.400 a 2.483,5 MHz.
- Potencia hasta 100 mW PIRE.
- Aplicaciones de interiores (o exteriores de corto alcance).

PIRE

PIRE es la potencia que radiaría una antena omnidireccional para dar el mismo nivel de potencia en el punto de estudio que la antena que tenemos instalada.

b) UN-128

- de 5.150 a 5.350 MHz:
  - Sólo en interiores.
  - Potencia entre 30 mW y 200 mW, dependiendo de si hay control de potencia (TPC) y/o selección dinámica de frecuencia (DFS).
- de 5.470 a 5.725 MHz:
  - Interiores y exteriores.
  - Potencia hasta 1 W PIRE (con TPC y DFS).

En 2,4 GHz hay más interferencias que en 5,8 GHz. En cambio, cuanta más frecuencia, es necesaria la visión directa. Por eso se permite emitir con más potencia a 5,8 GHz.

El estándar 802.11 define trece canales separados 5 MHz en la banda de 2,4 GHz. Un canal 802.11b tiene un ancho de 11 MHz a derecha e izquierda de la frecuencia central (total: **22 MHz**). Por lo tanto, en un mismo espacio sólo podremos tener tres canales sin solapamiento.

Según lo anterior, en una misma área podemos tener sin problemas **3 x 11 Mbps**, seleccionando los canales 1, 6 y 11 (este último viene por defecto). Con cierto solapamiento podríamos tener cinco canales (1, 4, 7, 10, 13). Observamos que con tres canales podemos hacer una estructura "celular" para que dos BSS con la misma frecuencia no se toquen.

En cambio, el estándar 802.11a define ocho canales de 25 MHz (pueden convivir diferentes operadores en una misma área). En los 25 MHz, y gracias a OFDM (dividimos la banda en 64 portadoras ortogonales –en el máximo de una *sinc*, las otras valen 0–, de las que sólo utilizamos 52) podemos transmitir 54 Mbps.

La arquitectura básica de estos sistemas consta de tres elementos:

- Clientes
- Puntos de acceso (AP)
- Servidor de seguridad (donde están los datos de los clientes)

La velocidad debe repartirse entre las estaciones conectadas a un mismo AP. Por ejemplo, un AP de 54 Mbps tiene que repartir esta velocidad entre los usuarios que se conecten.

Hay que ir con cuidado, ya que la velocidad real es normalmente un 50% de la velocidad teórica. Además, la velocidad máxima sólo se da cerca del AP. Si nos alejamos, el sistema la va reduciendo.

En la siguiente tabla comparamos las prestaciones de los estándares b, a y g:

	802.11b	**802.11a**	**802.11g**
Cobertura	X		X
Consumo eléctrico	X		X
Número de AP en un área		X	
Velocidad		X	X
Interferencias		X	
Compatibilidad con 802.11b			X

En las siguientes líneas haremos una rápida descripción de las modulaciones que utilizan estos estándares:

802.11: tiene dos versiones, la DSSS (1 y 2 Mbps) y el FHSS (1 y 2 Mbps). La FHSS está obsoleta. La DSSS funciona como el 802.11b de 1 Mbps y 2 Mbps que comentamos a continuación.

802.11b: tiene dos versiones, la DSSS (1, 2, 5,5 y 11 Mbps) y la FHSS (1 y 2 Mbps). La FHSS está obsoleta. La DSSS se comporta de manera diferente dependiendo de la velocidad:

sps

sps significa *samples per second* o muestras por segundo.

- **1 Mbps**: convierte cada bit en una secuencia de Barker de 11 bits (0 = 10111010000; 1 = 01000101111). Utiliza DBPSK [1 Msps con 1 bit/símbolo].

- **2 Mbps**: convierte cada bit en una secuencia de Barker de 11 bits. Utiliza DQPSK (1 Msps con 2 bits/símbolo).

- **5,5 Mbps**: cogemos los datos en bloques de 4 bits:

– Con los dos últimos bits, seleccionamos un código CCK de 8 bits (CCK, *complementary code keying*).
– Con los dos primeros bits, seleccionamos una de les cuatro posibles fases para transmitirlo con DQPSK (1.375 Msps con 4 bits/símbolo).

- **11 Mbps**: cogemos los datos en bloques de 8 bits:

– Con los seis últimos bits, seleccionamos un código CCK de 8 bits (tenemos un total de 64 códigos de 8 bits).
– Con los dos primeros bits, seleccionamos una de les cuatro posibles fases para transmitirlo con DQPSK (1.375 Msps con 8 bits/símbolo).

802.11a: aplica OFDM sobre cada canal de 20 MHz y lo divide en cuarenta y ocho portadoras (decimos que el símbolo OFDM es de 48 bits). Se comporta de manera diferente dependiendo de la velocidad:

- **6 Mbps**: cada grupo de 24 bits se convierte en un símbolo OFDM de 48 bits. En cada uno de estos canales se aplica BPSK.

– BPSK también se utiliza para obtener 9 Mbps.

- **12 Mbps**: cada grupo de 48 bits se convierte en dos símbolos OFDM de 48 bits. En cada portadora, por lo tanto, tenemos 2 bits a los que aplicamos QPSK.

– QPSK también se utiliza para obtener 18 Mbps.

- **24 Mbps**: cada grupo de 96 bits se convierte en cuatro símbolos OFDM de 48 bits. En cada portadora, por lo tanto, tenemos 4 bits a los que aplicamos 16QAM.

– 16QAM también se utiliza para obtener 36 ó 48 Mbps. Para los 54 Mbps se utiliza 64QAM.

A partir del 2009 se produjo un salto importante en las prestaciones de estas redes, que multiplicaron las velocidades. La tabla siguiente recoge algunas de ellas.

Estándar	Año	Banda	Velocidad
802.11n	2009	2,4 GHz / 5 GHz	450 Mbps
802.11ad	2012	60 GHz	7 Gbps
802.11ac	2014	5-6 GHz	1300 Mbps
802.11ax	2019	2,4 GHz / 5 GHz	10 Gbps

En los subapartados siguientes nos centraremos en 802.11n y 802.11ac, puesto que son los estándares que han penetrado más en el mercado.

2.6. Estándar 802.11n

Los estándares 802.11b y 802.11g sólo permiten 3 canales sin solapamientos, y esto limita la velocidad máxima que se puede dar en un mismo recinto. Por este motivo, desde abril del 2008, el CNAF define 19 canales de 16,6 MHz, separados 20 MHz (pueden convivir diferentes operadores en una misma área). FCC define 23 y Japón, 15. Podemos usar los 19 canales sin interferencias.

En los 16,6 MHz, y gracias a OFDM, somos capaces de transmitir 54 Mbps. Las velocidades pueden ser 6, 9, 12, 18, 24, 36, 48 o 54 Mbps dependiendo de la calidad del enlace de radio.

De este modo:

- Con el estándar *b*, en una misma sala podemos desplegar como máximo 3 AP (3 × 11 = 33 Mbps).
- Con el estándar *g*, en una misma sala podemos desplegar como máximo 3 AP (3 × 54 = 162 Mbps).
- Con el estándar *a*, en una misma sala podemos desplegar como máximo 19 AP (19 × 54 = 1.026 Mbps), y esto ya nos permite hacer planificaciones de red más complejas.

El estándar 802.11n permitirá todavía mayores velocidades, concretamente hasta 600 Mbps. Este estándar se publicó en septiembre del 2009, y ya hay productos que siguen un borrador (p. ej., Buffalo WLI-CB-G300N da 300 Mbps o el *router* Linksys WRT300N). En la figura, tenéis la etiqueta que indica que un producto sigue este borrador.

Símbolo de un producto pre-802.11n

Las características del 802.11n son las siguientes:

- **Usa un OFDM mejorado**.

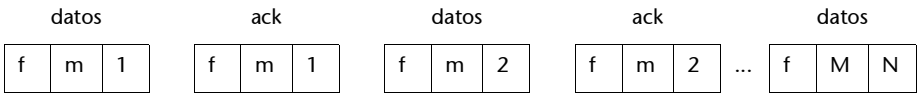
- **Utiliza *Spatial Multiplexing***: transmitimos la información por distintas antenas (donde había un solo flujo de bits que se transmitían por una única antena, ahora tendremos hasta 4 flujos que se transmitirán por 4 antenas, aumentando la velocidad). Esto también incrementa el consumo de potencia y por este motivo, 802.11n tiene un mecanismo de ahorro de potencia que hace que usemos más de un flujo sólo cuando sea necesario.

- **Utiliza MIMO**: el receptor tiene hasta cuatro antenas y combina las informaciones. Aunque utilicemos una sola antena transmisora nos beneficiamos de la diversidad, ya que el único flujo transmitido puede ser recibido por las cuatro antenas receptoras (y el alcance podría ser mayor).

- **Los canales no son de 20 MHz, sino de 40 MHz**: esto nos permite ganar velocidad, ya que optimizamos el espacio. Por ejemplo, si sobre 20 MHz tenemos 65 Mbps, sobre 40 MHz se consiguen 135 Mbps (que es un poco más del doble).

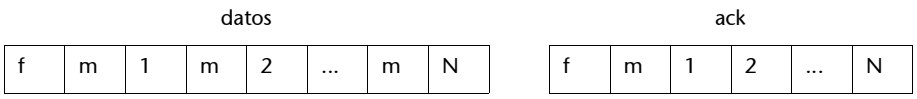
- **No transmitimos paquete a paquete, sino bloque a bloque (con un solo ACK por bloque, lo que nos permite ganar velocidad)**: como veremos en el gráfico siguiente, con esta estrategia mejoramos la velocidad. De este modo, por ejemplo, si sin usar esta estrategia tenemos 54 Mbps (como puede ser el caso del 802.11g), usándola llegamos a 65 Mbps.

Antes:



f: cabecera física; m: cabecera MAC

Ahora:



f: cabecera física; m: cabecera MAC

- **Menor tiempo de espera (menor *Inter-frame spacing IFS*)**: con esto, conseguimos una mejora aproximada de un 10%. Por ejemplo, si sobre 40 MHz

tenemos 135 Mbps usando el intervalo de guardia normal, si usamos el intervalo reducido conseguimos 150 Mbps.

- **Modo Greenfield**: este modo mejora la eficiencia cuando sólo hay dispositivos *n* (eliminamos el soporte a dispositivos *a*, *b* y *g*).

- **Funciona a 2,4 GHz y 5 GHz**: o sea, aprovecha los 3 canales de 2,4 GHz y los 19 canales de 5 GHz.

Velocidad:

- En 802.11a/g teníamos 54 Mbps sobre 20 MHz. Es decir, sobre 40 MHz teóricamente tendríamos 108 Mbps, aunque en realidad son 135 Mbps porque aprovechamos espacios de guarda.

- Conseguimos unos 15 Mbps suplementarios por las mejoras que incorpora el 802.11n. De este modo, tenemos 150 Mbps por cada antena transmisora. En un caso extremo, podríamos tener 22 canales a 150 Mbps en una sola sala.

- Este valor se debe multiplicar por el número de antenas transmisoras (el mínimo que fija la Wi-Fi Alliance para considerarse 802.11n es 2). Con 4 antenas, salen los 600 Mbps.

En la tabla siguiente tenemos una visión de conjunto de las velocidades (en Mbps) que se han comentado anteriormente:

802.11g	6	9	12	18	24	36	48	**54**
802.11n 1 flujo BW = 20 MHz	6,5	13	19,5	26	39	52	58,5	**65**
802.11n 1 flujo BW = 40 MHz	13,5	27	40,5	54	81	108	121,5	**135**
802.11n 1 flujo BW = 40 MHz IFS pequeño	15	30	45	60	90	120	135	**150**
802.11n 2 flujos BW = 20 MHz	13	26	39	52	78	104	117	**130**
802.11n 2 flujos BW = 40 MHz	27	54	81	108	162	216	243	**270**
802.11n 2 flujos BW = 40 MHz IFS pequeño	30	60	90	120	180	240	270	**300**
802.11n 3 flujos BW = 20 MHz	19,5	39	58,5	78	117	156	175,5	**195**

802.11n 3 flujos BW = 40 MHz	40,5	81	121,5	162	243	324	364,5	**405**
802.11n 3 flujos BW = 40 MHz IFS pequeño	45	90	135	180	270	360	405	**450**
802.11n 4 flujos BW = 20 MHz	26	52	78	104	156	208	234	**260**
802.11n 4 flujos BW= 40 MHz	54	108	162	216	324	432	486	**540**
802.11n 4 flujos BW = 40 MHz IFS pequeño	60	120	180	240	360	480	540	**600**

La complejidad de los procesos técnicos que incorpora 802.11n ha dado lugar al concepto de **MCS** (*Modulation Coding Scheme*). Estas siglas incluyen conceptos como la modulación, el número de flujos espaciales y la velocidad de los datos en cada flujo. Hay que negociar en cada momento cuál es el MCS óptimo en función de las condiciones del enlace.

El borrador de 802.11n especifica 77 MCS diferentes. 8 de éstos (MCS-0 a MCS-7) son obligatorios para los clientes y 16 (MCS-0 a MCS-15) para los puntos de acceso. La máxima velocidad (600 Mbps) se consigue con el MCS-31 usando modulación 64QAM en un canal de 40 MHz, con 4 flujos de datos y trabajando con un espacio de guarda (EG) pequeño (EG = 400 ns). El estándar también especifica un espacio de guarda mayor (EG = 800 ns), en el que las velocidades son un poco inferiores.

La tabla siguiente muestra las velocidades que se pueden conseguir con los MCS-0 a MCS-15 sobre un canal de 40 MHz.

Sobre un canal de 20 MHz las velocidades serían un poco inferiores a la mitad.

Canal	Flujos	Modulación	Bits por portadora	Velocidad (EG = 800)	Velocidad (EG = 400)
MCS-0	1	BPSK	1	13,5 Mbps	15 Mbps
MCS-1	1	QPSK	2	27 Mbps	30 Mbps
MCS-2	1	QPSK	2	40,5 Mbps	45 Mbps
MCS-3	1	16QAM	4	54 Mbps	60 Mbps
MCS-4	1	16QAM	4	81 Mbps	90 Mbps
MCS-5	1	64QAM	6	108 Mbps	120 Mbps
MCS-6	1	64QAM	6	121,5 Mbps	135 Mbps
MCS-7	1	64QAM	6	135 Mbps	150 Mbps
MCS-8	2	BPSK	1	27 Mbps	30 Mbps
MCS-9	2	QPSK	2	54 Mbps	60 Mbps
MCS-10	2	QPSK	2	81 Mbps	90 Mbps
MCS-11	2	16QAM	4	108 Mbps	120 Mbps
MCS-12	2	16QAM	4	162 Mbps	180 Mbps

MCS-13	2	64QAM	6	216 Mbps	240 Mbps
MCS-14	2	64QAM	6	243 Mbps	270 Mbps
MCS-15	2	64QAM	6	270 Mbps	300 Mbps

Hay dos tipos de soluciones:

- La más clásica consiste en poner puntos de acceso "normales" como el Buffalo AG300NH o el Buffalo G300N Nfinity. Los usuarios requerirán PCMCIA del tipo *n* (por ejemplo, la WL12-CB-G300N) o USB del tipo n (por ejemplo, la UC-G300N).

- Usar unos equipos que ya integran distintos puntos de acceso. Por ejemplo, el Xirrus XS4 integra 4 AP o el Xirrus XS8 integra 8 AP. Además, hay que añadir la PCMCIA o USB de los usuarios. Estos productos compactos permiten dar soluciones rápidas a instalaciones con muchos requerimientos de capacidad.

Consideraciones cuando se hacen diseños con 802.11n:

- Si usamos todos los canales disponibles, podemos llegar a tener 4 Gbps (27 canales de 150 Mbps). Por lo tanto, es importante que la red fija tenga, al menos, un puerto Gigabit (se recomienda un par).

- Puede trabajar en dos bandas: 2,4 GHz y 5 GHz. Es decir, hay que proteger las dos bandas (por ejemplo, con sensores de actividad en las dos bandas, para detectar posibles interferencias o accesos no deseados).

- En un nivel de propagación, la banda de los 5 GHz es más complicada. Por lo tanto, los cálculos de cobertura se deben hacer a 5 GHz.

- Se recomienda usar seguridad WPA2. WEP es muy simple y fácilmente descifrable, y WPA también es descifrable (con un poco más de tiempo). En sistemas que funcionan a velocidades elevadas, como este, es peligroso usar sistemas que no cambien las claves, ya que circulan muchos paquetes por segundo y, por lo tanto, un posible intruso dispone de mucha información para averiguar las claves.

2.7. Estándar 802.11ac

802.11ac es una mejora de 802.11n. 802.11ac está diseñado para funcionar solo en la banda de 5 GHz. Esto evita la banda de 2,4 GHz, llena de aparatos y dispositivos (Bluetooth en general y hornos microondas) que provocarían interferencias.

Un dispositivo 802.11ac tiene que soportar todos los modos obligatorios de 802.11a y 802.11n. Así, un punto de acceso 802.11ac se puede comunicar con

dispositivos 802.11a y 802.11n. Del mismo modo, un dispositivo 802.11ac se puede comunicar con un punto de acceso 802.11a o 802.11n.

Uno de los objetivos del 802.11ac es disponer de mucha velocidad. Esto lo hace de varias maneras:

- Con más anchura de banda del canal, para pasar de los 40 MHz del 802.11n a los 80 MHz o 160 MHz del 802.11ac.

- Con modulaciones más eficientes, para pasar del 64QAM del 802.11n al 256QAM del 802.11ac.

- Con un uso de MIMO (entrada múltiple salida múltiple) más intensivo, para pasar de los 4 flujos del 802.11n a los 8 flujos del 802.11ac.

Con todo esto, mientras que un sistema 802.11n típico puede gestionar 300 Mbps, un 802.11ac de 80MHz puede gestionar 870 Mbps, cifra que se puede duplicar con un ancho de banda de 160 MHz. Claramente, mejora la velocidad y también la eficiencia espectral.

2.8. Escucha del canal

Cada BSS transmite paquetes *beacon* con información de red. La escucha puede ser pasiva o activa:

- **Escucha pasiva** (escucha de *beacons*):

Cuando detectamos un *beacon* con el SSID que queremos, negociamos la incorporación.

- **Escucha activa** (los terminales siempre escogen la mejor EB):

– Los terminales envían un *probe* con el SSID deseado a las EB que lo escuchen.
– Las EB que han escuchado envían un *probe response*. Si no hay respuesta, formamos una nueva BSS con el SSID (por si se es el primero).
– El terminal envía un *association request* a la mejor.
– La EB seleccionada lo confirma (*association response*).
– Se informa al antiguo punto de acceso por el sistema de distribución cableado.

Observamos que en una itinerancia o *roaming*, es el terminal el que decide cuándo un punto de acceso no da suficiente calidad.

Hay un *inter-access point protocol* (IAPP) que quiere mejorar la comunicación entre AP:

– para informar a otros AP de la presencia de un nuevo AP.
– para informar a un AP de que asociemos a un cliente suyo.

En lugar de anunciarlo a todos los AP, lo anunciamos al *AP manager*. Así, será este *manager* quien recibirá las confirmaciones de todos los AP.

2.9. Seguridad

Cuando hablamos de seguridad, hay dos aspectos que debemos abordar: la **autenticación** y el **cifrado**.

1) Autenticación (control de accesos):

- Con clave compartida (*shared key authentication*): todas las estaciones de un BSS la han conocido por un canal seguro (normalmente, de forma manual). No es seguro, porque cifra una respuesta conocida.
- Sistema abierto (*open system authentication*): no hay contraseña y sólo se indica la intención de acceder. Es el más sencillo (y más inseguro).

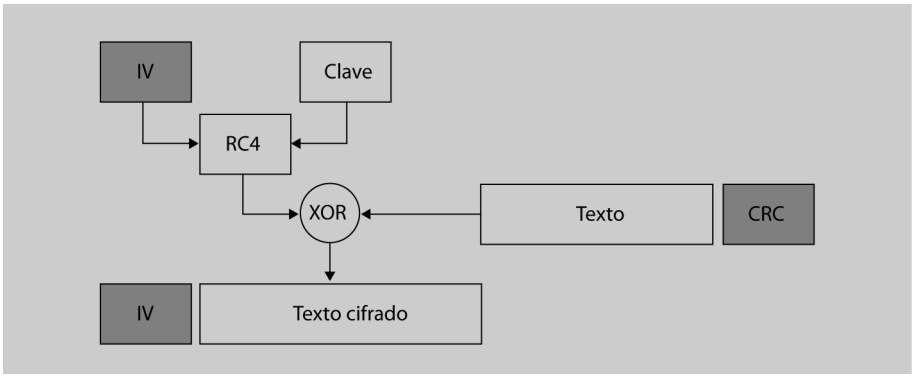
También se puede autenticar utilizando la dirección de dispositivo (MAC). El AP tendrá una lista con las MAC permitidas. Pero alguien nos puede escuchar la MAC.

2) Cifrado (hay que tener en cuenta que, por defecto, no se cifra):

El método de cifrado más básico es el WEP, que comentamos a continuación. WEP (*wired equivalent privacy*) hace un cifrado de 64 bits (estándar) o de 128 bits. Cuantos más bits mejor, pero no se puede aumentar más, porque, si incrementamos la longitud, hacen falta más CPU. En WEP:

- La clave es estática y simétrica (por lo tanto, no hay gestión de claves).
- Se cifra con RC4 (algoritmo criptográfico simétrico).
- Se protege la integridad de los datos (MIC, *message integrity code*) con CRC-32 (el cifrado pretende evitar que se vean los datos; la integridad pretende evitar que se cambien los datos durante el camino).

Figura 6. Cifrado WEP



En la figura anterior tenemos la estructura de cifrado en WEP. Las claves WEP son de 40 + 24 bits o 104 + 24 bits, donde los 24 bits son el vector de inicialización (IV). La

clave debe ser conocida por todos. Se puede poner manualmente o se puede generar automáticamente. El CRC es independiente de la clave y del IV.

Los mecanismos de seguridad de WEP son muy simples (e inseguros). El WEP+ (WPA, *wireless protected area*), que es compatible con WEP y apareció en noviembre del 2002, incorpora:

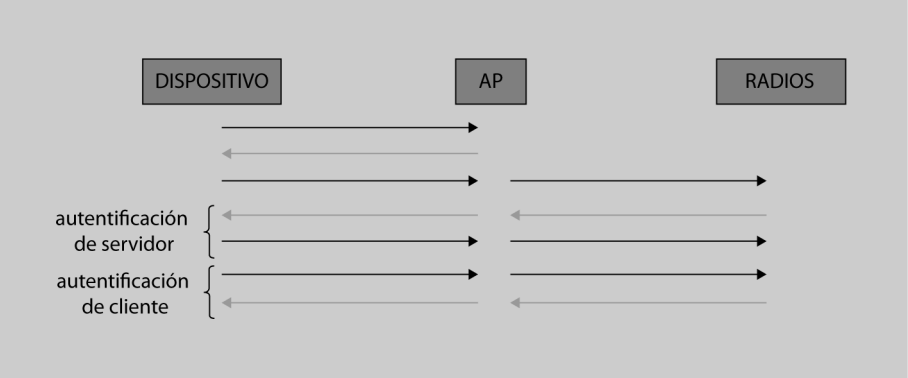
a) Autenticación con 802.1x + EAP

– Puede utilizarse un servidor RADIUS como servidor de autenticación (todos los AP piden el inicio de sesión-contraseña, *login-password*, a este servidor; antes poníamos la contraseña en todos los AP).

La comunicación entre servidor y AP se hace con protocolos EAP (*extensible authentication protocol*). Algunos protocolos EAP existentes son TLS, TTLS, LEAP y PEAP.

– La autenticación (ver figura siguiente) es recíproca entre cliente y servidor (y al revés)

Figura 7. Autenticación 802.1x



Si no disponemos de servidor, también podemos introducir unas claves (PSK, *pre-shared key*) en cada elemento.

b) Claves dinámicas (en WEP eran estáticas; conocer una implica conocerlas todas), **gestionadas con el protocolo de recálculo de claves TKIP** (*temporal key integrity protocol*):

– La primera clave es el punto de partida para las siguientes.

– Seguimos cifrando con RC4 y una clave de 128 bits.

– Mecanismo de integridad MIC (también llamado *Michael*) con claves de 64 bits. Si hay dos errores en un segundo, borra las claves, se disocia y reasocia (supone un ataque).

También se pueden añadir otros mecanismos de seguridad en red, como podría ser una contraseña para acceder a ciertos servicios, etc.

El **802.11i** (también llamado *WPA2*), aprobado en junio del 2004, se diferencia de WPA en lo siguiente:

– WPA2 utiliza AES (*advanced encryption standard*) para cifrar, en lugar de RC4. Las claves pueden ser de 128, 192 ó 256 bits.

– WPA2 utiliza un mecanismo de integridad de tipo CCMP.

En la siguiente tabla podemos ver de manera esquemática las características de los tres estándares de seguridad:

	WEP	**WPA**	**WPA2 o 802.11i**
Autenticación	Muy básica	802.1x + EAP	802.1x + EAP
Gestión de claves	No hay (claves estáticas)	EAP	EAP
Cifrado	RC4	RC4	AES
Integridad	CRC-32	Michael	CCMP

Hay que ser conscientes de que la seguridad total no existe, pero deben aplicarse algunos de los mecanismos de seguridad. Todavía hoy en día hay un porcentaje muy alto de redes que no aplican ninguna protección.

2.10. Aplicaciones

Las aplicaciones de las redes locales sin hilos son múltiples:

- Enlace entre diferentes plantas de un edificio con puntos de acceso (modo infraestructura). Tenemos una gran cobertura y es útil cuando el tráfico se origina o finaliza en redes externas a las que está conectado el AP.
- Redes sin hilos independientes en una misma área física (modo *ad hoc*). La cobertura no es muy grande (es determinada por la distancia máxima entre dos equipos) y es útil cuando hay muchas transacciones internas.
- Enlace entre edificios.
- Etc.

En las aplicaciones hay que tener en cuenta que el número de usuarios que puede soportar un punto de acceso depende del tráfico esperado por usuario. A continuación hay algunas recomendaciones:

- En una planta industrial en la que se trabaje con lectores de códigos de barras, hay que prever unos 25 kbps/usuario.
- En un centro de formación en el que cada alumno deba acceder a una intranet para ver la documentación en línea, hay que prever unos 300 kbps/usuario.

- En una oficina en que a menudo se realicen transferencias de archivos, hay que prever 1 Mbps/usuario.

Si solapamos AP para descongestionar cierta área, hay que separarles 2-3 metros a causa de sus filtros no ideales.

El aislamiento teórico entre canales es infinito, pero en la práctica es de unos 60 dB. Por ejemplo, si un AP emite 20 dBm en el canal 1, podría ser que un AP próximo reciba 20 dBm – 60 dB por su canal 11.

Hoy en día, las tecnologías de redes locales sin hilos tienen muchas ventajas para las empresas:

- Permiten que el personal no tenga un lugar físico asignado, cosa que facilita el trabajo en empresas donde el personal se mueve de sede.
- Reducen los problemas con los conectores, cables...
- Permiten el acceso a todos los recursos (impresoras...).
- Las reuniones son más eficaces (todo el mundo puede mostrar sus informaciones...).
- Podemos estar con conexión permanente al correo electrónico.
- Como hay un estándar, si un equipo se estropea es fácilmente sustituible.
- Los dispositivos son *Plug* & *Play*.
- Acceso a la red en lugares públicos como aeropuertos, hoteles...
- Permite la comunicación de datos entre elementos móviles (lectores de códigos de barras en un almacén, pedidos en la cocina en un restaurante...).
- Facilita la instalación de cámaras de seguridad.

A pesar de trabajar en bandas libres, se puede hacer negocio con estos sistemas, ofreciendo al usuario una determinada calidad de servicio.

También hay que destacar las comunidades sin hilos o *wireless*, grupos que tienen como objetivo compartir las conexiones sin hilos. Hay muchos lugares donde estos espacios están indicados con una rotulación especial.

Fon

Cabe destacar el movimiento Fon (comunidad mundial, tipo "planeta WiFi"): http://es.fon.com.

Las redes sin hilos aparecen como respuesta a la necesidad de tener conexión a red en cualquier lugar. Como en casi todas partes hay red eléctrica, ¿se puede aprovechar ésta para acceder a redes de datos? La respuesta es afirmativa, con la tecnología PLC (*power line communication*).

PLC

Hay productos y experiencias con PLC. Podemos encontrar más información en www.ovislinkcorp.es

3. Redes metropolitanas sin hilos

En el apartado anterior hemos hablado de las redes de alcance local. En este apartado hablaremos de las redes metropolitanas sin hilos, las cuales dan cobertura a distancias de unos cuantos kilómetros, que pueden corresponder a una ciudad o metrópoli, y de ahí viene su nombre.

Inicialmente, estas redes se hacían con la tecnología LMDS (no había estándares), pero poco después el estándar 802.16 se impuso a LMDS y, ya en los últimos años, 802.16 ha sido desplazado por la implantación de otros sistemas de comunicaciones móviles que, al dirigirse a un público más amplio, ofrecen una mejor relación calidad-precio.

3.1. LMDS (*local multipoint distribution service*)

LMDS es una tecnología de comunicaciones sin hilos de banda ancha que trabaja en 26-28 GHz. Trabajar a frecuencias tan elevadas permite disponer de mucha banda frecuencial (mucha capacidad), pero tenemos un alcance menor (ya sabemos por el módulo "Comunicaciones sin hilos" que, cuanta más frecuencia, más pérdidas). También hay un LMDS a frecuencias más bajas (3,5 GHz), llamado *WLL* (*wireless local loop*).

El significado de LMDS es:

L [*local*]: poco alcance debido a las elevadas frecuencias.
M [*multipoint*]: punto a multipunto (punto a punto de abonado a base).
D [*distribution*]: distribución de señales.
S [*service*]: servicio.

A grandes rasgos, un sistema LMDS es un conjunto de estaciones base interconectadas entre ellas que dan servicio *full-duplex* a unas ubicaciones de usuario que tienen visión directa.

Como las estaciones base dan cobertura a zonas muy delimitadas, es una tecnología muy útil para servicios interactivos (vídeo por encargo, videoconferencia...) en lugares donde haya una alta densidad de usuarios (hasta 80.000 abonados por base). También es de gran utilidad para canales locales de televisión que adapten programación y publicidad a las características del público al que dan servicio.

Como se ha comentado anteriormente, en 26-28 GHz tenemos mucha capacidad pero hay inconvenientes:

- Las ondas no atraviesan obstáculos, y se necesita visión directa (3-5 km). Cuanta más frecuencia, tendremos menos alcance.

  El alcance también depende de la disponibilidad del enlace deseada. Por ejemplo, a 26-28 GHz podemos llegar a 14 km con una disponibilidad del 99,9%, pero sólo podemos llegar a 2,5 km si la disponibilidad deseada es del 99,999%.

- Cuando llueve, hay que aumentar la potencia de transmisión de las bases (vimos en el módulo 1 que a estas frecuencias las gotas de agua son un obstáculo).
- También hay que considerar la humedad atmosférica.

Disponibilidad

Disponibilidad es el porcentaje de tiempo en el que el enlace funciona correctamente. Por ejemplo, una disponibilidad del 99,9% equivale a 8 horas/año de inactividad del enlace.

Por ejemplo, en 26-28 GHz, por un enlace con un 99,99% de disponibilidad podemos llegar a 5 km en un área seca como la ciudad de Denver, pero sólo a 3 km en una ciudad húmeda como Miami.

En el año 2001, el Estado español otorgó licencias de LMDS en las bandas de 26 GHz y 3,5 GHz. Los operadores que disponían de licencia a 3,5 GHz no podían dar mucho ancho de banda pero el alcance era mayor (requerían menos estaciones base y, por lo tanto, los servicios eran más económicos). Los operadores de 26 GHz podían ofrecer un gran ancho de banda pero requerían más estaciones base (y esta inversión la repercutían en las tarifas).

La Ley de Servicios de la Sociedad de la Información (LSSI) representó un gran impulso para la tecnología LMDS. Esta ley, de junio del 2002, preveía que todos los ciudadanos pudieran acceder a Internet (hasta entonces, sólo la telefonía era un servicio universal). Las 200.000 líneas que disponían del servicio TRAC (telefonía rural de acceso celular) no podían disfrutar de éste, por lo cual el Gobierno encargó a Telefónica que pusiera en marcha un plan para proporcionar este servicio. La mayor parte de las líneas TRAC se sustituyeron por enlaces LMDS (y, de manera más minoritaria, con acceso mediante redes de gran alcance como GSM/GPRS y mediante satélite).

Por ejemplo, la operadora Neo dio el servicio TRAC en Castilla-León y la operadora Iberbanda lo hizo en las provincias de Lérida y Tarragona.

Operadores

Podemos ver las webs de algunos de estos operadores: neo.es, iberbanda.es, basacom.com.

TRAC

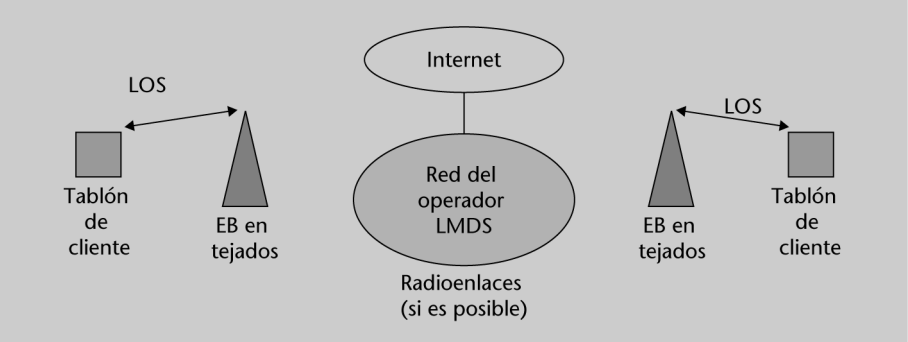
TRAC es un servicio para dar telefonía a los lugares dónde no está justificado económicamente llegar con cables telefónicos (por ejemplo una casa rural aislada, donde el pueblo más próximo esté a 10 km).

Una empresa o particular que quiera contratar LMDS debe hacer lo siguiente:

1) Escoger operadora.
2) Ver si su población tiene cobertura (en las webs de las operadoras lo suelen decir).
3) Ver si su empresa tiene visión directa con la estación base LMDS. Eso lo hacen unos técnicos que se desplazan a la empresa para verificarlo.
4) Conseguir un permiso de instalación del propietario del edificio.

Como vemos en la figura siguiente, el abonado se conecta con su equipo de usuario a la estación base de la operadora (que debe tener en visión directa). Las distintas estaciones base de la operadora están conectadas a la red global (Internet). La instalación es muy rápida y eso hace que sea una tecnología muy adecuada cuando queremos contratar ancho de banda para acontecimientos especiales (*ciber-parties*, traspaso de datos en empresas...).

Figura 8. Arquitectura LMDS



3.2. Estándar 802.16

La norma IEEE 802.16 *(wireless metropolitan area networks*), publicada en diciembre del 2001, sirvió para fomentar la operatibilidad entre los sistemas LMDS, ya que define un estándar para redes metropolitanas (LMDS era una tecnología propietaria, no un estándar).

En el 2001...

... antes de la aparición de los estándares, se creó el fórum WiMAX (www.wimaxforum.org).

En las frecuencias del 802.16 (entre 10 GHz y 66 GHz), es necesaria visión directa. En enero del 2003 apareció el 802.16a, que trabajaba entre 2 y 11 GHz. Como la frecuencia es menor, a veces podemos tener cobertura con visión directa parcial. Este estándar también se llama *WiMAX* (o **802-16-2004**).

En noviembre del 2005 apareció el 802.16e (o **802.16-2005**), que trabaja entre 2 y 6 GHz y permite movilidad de terminales hasta 150 km/h.

WiMAX está pensado para reducir el vacío –*gap*– digital que limita la difusión de información de banda ancha en zonas de baja densidad. Wi-Fi no podía hacer eso porque, entre otras cosas:

- Tiene un acceso al medio poco eficiente (en Wi-Fi, si un usuario quiere transmitir mientras lo hace otro, debe esperarse). No permite calidad de servicio (a no ser que se desarrolle el 802.11e).
- Sólo está pensado para bandas libres (nos pueden interferir).
- Ámbito reducido (local).

Veremos las **principales características de WiMAX**, que lo hacen apropiado para una red metropolitana:

- **Modulación adaptativa**. Si el canal tiene un buen comportamiento (pocas pérdidas), la velocidad aumenta porque utilizamos una modulación que lleva más bits en cada símbolo. Por ejemplo, si la relación señal-ruido (SNR) es de 6 dB, utilizamos BPSK, pero si la SNR llega a 9 dB, entonces utilizamos QPSK.

- **Banda frecuencial**. Se puede trabajar en banda libre a 5,4 GHz, pero con poca potencia (poca cobertura) y con visión directa. Pero también hay una banda licenciada en 3,5 GHz donde no es imprescindible la visión directa.

- **Elementos**. De manera similar a las unidades de abonado y a los puntos de acceso Wi-Fi, aquí tenemos estaciones base (BS o BSU, *Base Station Unit*) y unidades de usuario (CPE o SU, *Subscriber Unit*). En realidad, podríamos decir que hay tres tipos de productos:

– BSU (estación base)
– CPE *outdoor*
– CPE *indoor* (que puede ser de sobremesa o tipo USB)

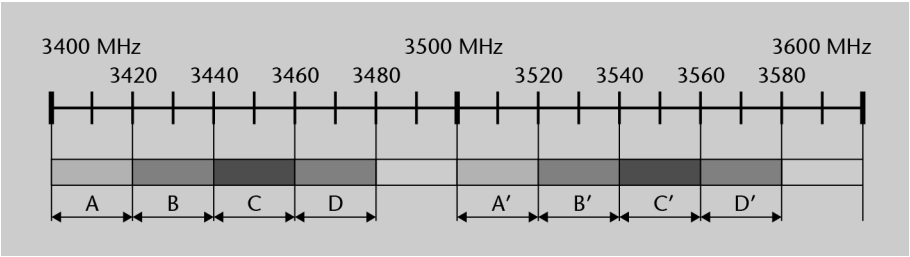
Las ganancias típicas de las BSU y los CPE son entre 16 y 24 dB. Habitualmente, si un CPE tiene mucha ganancia deberá ser grande, lo que puede no interesar en los CPE *indoor*.

Las potencias típicas de transmisión son 20-30 dBm.

Las sensibilidades (potencia recibida mínima necesaria para funcionar) suelen ser de unos –90 dBm, pero con niveles tan pequeños de potencia recibida la velocidad también es pequeña. Con –70 dBm, normalmente tendremos máxima velocidad.

A la hora de seleccionar un elemento, debemos tener en cuenta la frecuencia de trabajo. En España, el Cuadro Nacional de Atribución de Frecuencias (CNAF) define dos normas.

1) UN-107 (3400-3600 MHz): enlaces punto a punto en todo el territorio nacional otorgados por concurso (son las cuatro licencias actuales).



2) UN-128 (5470-5725 MHz): enlaces interiores y exteriores hasta 1W PIRE, sin licencia pero con necesidad de constituirse como operador ante la Comisión del Mercado de las Telecomunicaciones (CMT).

A corto plazo esto cambiará, ya que el Estado está pensando en habilitar una nueva banda en torno a los 2,6 GHz.

- **Perfiles**. Se definen cinco:

SC

En SC hay que transmitir los símbolos consecutivamente. En OFDM cada símbolo va en una portadora.

– SC (*single carrier*): entre 10 y 66 GHz, con licencia y visión directa (LOS) para hacer enlaces punto a punto (PaP).

– SCa: entre 2 y 11 GHz, con licencia y LOS para hacer enlaces PaP.

– OFDM: utiliza FFT de 256 puntos para tener enlaces punto-multipunto (PmP) con licencia sin necesidad de visión directa (NLOS).

OFDMA

OFDMA es un OFDM que mejora la transmisión en entornos ruidosos, gracias a la creación de subcanales en las portadoras.

– OFDMA: utiliza FFT de hasta 2.048 puntos para tener enlaces punto-multipunto (PmP) con licencia sin necesidad de visión directa (NLOS).

– HUMAN: abarca los tres perfiles anteriores pero en banda libre.

- **Antenas**. Puede utilizar antenas adaptativas que controlan el haz en la dirección de las CPE.

- **Diversidad**. En recepción utiliza diversidad MRC (ver el módulo 1). En transmisión también utiliza dos antenas (si en el instante *t* se transmite la información *X* en la antena 1 e Y en la antena 2, en el instante *t + 1* se transmite Y en la antena 1 y *X* en la 2).

- **Selección dinámica de frecuencia (DFS)**. Si detecta interferencias, tiene que cambiar de frecuencia (obligatorio si se trabaja en banda libre, para evitar interferir los radares).

- **Permite calidad de servicio (QoS)**. Cada trama es para un CPE. Como WiMAX está orientado a la conexión, permite QoS. Los enlaces ascendente y descendente pueden ser asimétricos, pero en la misma trama (en modo TDD). Se definen cinco tipos de QoS:

Observación

En un servicio orientado a la conexión, es posible garantizar recursos a las conexiones.

– UGS (*unsolicited grant service*): cada usuario tiene su ranura reservada. Tendremos velocidad fija y no deberemos pedir el canal. Una aplicación es la voz sobre IP sin suprimir silencios (VoIP).

– rtPS (*real-time polling service*): en este caso el usuario va diciendo lo que necesita y la red se lo concede (dentro de unos límites). Es de utilidad, por ejemplo, en televisión por IP.

– nrtPS (*non real-time polling service*): los datos pueden tener cierto retraso. Por ejemplo, si hacemos transferencia de archivos (FTP).

– BE (*best effort*): es el caso de navegación por Internet.

– ertPS (*extended real-time polling service*) [sólo en el 802.16-2005]: no hace una reserva continua de tráfico, sino que toma lo mejor de UGS y de rtPS.

Es ideal para tráfico en tiempo real con velocidad variable (VolP) y supresión de silencios.

Topologías de red

- **PaP.** Podemos conseguir enlaces punto a punto entre 20 Mbps y 300 Mbps a distancias de 2 km (visión directa). Una aplicación de esta topología es alimentar enlaces PmP.

- **PmP**. En enlaces punto a multipunto disponemos de antenas sectoriales en la BS (en el enlace ascendente) donde cada sector apunta a una unidad de usuario. Las unidades de usuario disponen de antenas directivas.

- **Mesh**. Como su nombre indica, en una estructura mallada hay varias BS cubriendo una zona, de manera tal que la comunicación entre un CPE y una BS lejana se puede hacer mediante saltos entre BS intermedias.

Si nos planteamos la compra de equipos 802.16, hay que fijarse en lo siguiente:

- **Temperatura de trabajo de los equipos**. Que sea adecuada a la temperatura del lugar donde los queremos ubicar.

- **Suministro eléctrico**. Valorar si la alimentación se hace sobre el mismo cable de datos (PoE, *power over Ethernet*) y si la fuente de alimentación es de buena calidad.

- **Indicador de alineación**. Verificar que las antenas disponen de indicadores acústicos para indicar que el enlace está alineado. A veces los indicadores visuales no son adecuados (especialmente si hay mucha luz exterior).

- **Inclinaciones**. Verificar que la antena dispone de PAN (posibilidad de cambiar su orientación a derecha e izquierda) y TILT (ídem en vertical y horizontal). Ésta última es especialmente interesante en enlaces largos, ya que, por efecto de la curvatura terrestre, a partir de 14 km ya se tiene que inclinar hacia abajo.

- **Garantía**. Es un valor añadido que los equipos sean de tipo *carrier class*. Eso significa que son equipos robustos (admiten ampliaciones, disponen de fuentes de alimentación redundantes...) y son utilizados habitualmente por los mismos operadores.

- **Geometría del enlace**. Se recomienda dejar libre el 60% del radio de la primera zona de Fresnel (ver el apartado 5.2 del módulo didáctico 1). Si hay obstáculos por el camino, nos veremos obligados a elevar las antenas.

En los últimos años, los precios de las estaciones base están en torno a los 3.000 euros o por encima. Las principales aplicaciones son enlaces fijos punto a punto (conexión entre dos pueblos pequeños próximos) y enlaces fijos pun-

to a multipunto (Internet rural). Observamos que no es un sistema pensado para multipunto a punto (conexión de cámaras de seguridad a un centro de control). Una aplicación muy interesante es para despliegues de emergencia (en caso de una catástrofe, las infraestructuras permanentes se suelen dañar o colapsar; con WiMAX se podría crear una red para los servicios de emergencia de manera muy rápida).

De manera paralela, está el estándar 802.20 (o MBWA, *mobile broadband wireless access*). Éste está impulsado por la compañía Qualcomm y promete movilidad de terminales de hasta 250 km/h trabajando a 2,4 GHz.

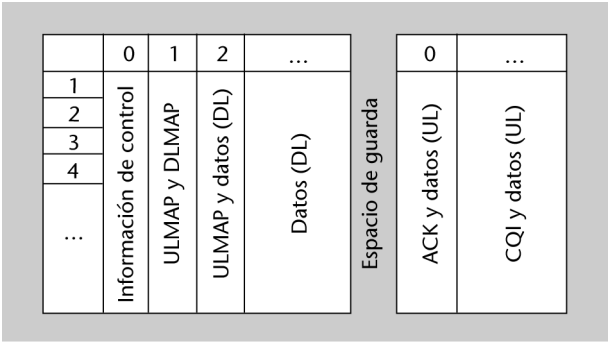
La certificación de los productos WiMAX está resultando bastante lenta. De eso se encarga el consorcio WiMAX, que al estilo de Wi-Fi certificará qué productos cumplen el estándar.

En diciembre del 2006 no había productos 802.16e certificados, pero ya había productos en el mercado. Por ejemplo, en Japón había enlaces en funcionamiento.

El estándar 802.16e (WiMAX en movilidad) ofrece 63 Mbps en el enlace descendente (DL) y 28 Mbps en el ascendente (UL) sobre 10 MHz. La latencia es inferior a 50 ms. Puede trabajar en anchos de banda entre 1,25 y 20 MHz, y usa OFDM.

Los recursos están disponibles en símbolos OFDM en el dominio del tiempo y en subportadoras en el dominio de la frecuencia. Estos recursos se organizan en subcanales para colocar a los distintos usuarios.

A modo de ejemplo, veamos en la figura siguiente la trama OFDMA para el modo TDD.



Observemos cómo en la trama se diferencia la parte del enlace descendente (a la izquierda) y la del enlace ascendente (a la derecha), separadas por un espacio de guardia. En los símbolos 1 y 2 de la subtrama descendente, tenemos el ULMAP y el DLMAP. En estos campos, se describe la disposición de los subcanales que vendrán a continuación. En distintos puntos de la subtrama ascendente, tenemos el CQI y el ACK. En estos campos, el móvil informa de la calidad del enlace y da los ACK del HARQ.

A partir de diciembre del 2007, se inició la certificación de productos por parte del WiMAX Forum.

Hemos hablado de 802.16a (802.16-2004) y 802.16e (802.16-2005) por separado. En el año 2009 apareció el 802.16-2009, que engloba los dos estándares.

El desarrollo del estándar 802.16m quiere competir con el 802.20 dando más velocidades a los enlaces. De manera simplificada, podríamos decir que en redes WiMAX el 802.16m es la evolución del 802.16e, del mismo modo que en redes Wi-Fi el 802.11n es la evolución del 802.11g.

Actividades

1. Una pequeña empresa situada en una población de 20.000 habitantes dispone de una oficina donde trabajan ocho personas conectadas en red. La oficina dispone de una línea ADSL mediante la que acceden a Internet (básicamente para consultar el correo electrónico) desde cualquiera de las máquinas.

Esta empresa ha alquilado un local situado a 100 metros, en una planta baja, y en la misma calle. En este local trabajarán tres personas y tendrán contratada una línea telefónica sólo para voz. Se quiere que las tres personas puedan trabajar en red (que se vean sus máquinas entre ellas), pero también se quiere que vean a las personas de la otra oficina. También deben poder acceder a Internet, aprovechando la línea de la sede central.

No se quiere hacer ninguna instalación permanente en el local alquilado, y se valora la conveniencia de que los tres ordenadores de sobremesa se interconecten mediante tarjetas sin hilos con un punto de acceso.

Os pedimos que propongáis una solución al problema planteado e indiquéis el porqué de las decisiones que toméis, los equipos que hay que comprar y su importe. No incluyáis los gastos de ingeniería (valorad sólo el coste del material).

Ejercicios de autoevaluación

1. El estándar IEEE 802.11 de redes locales sin hilos ha escogido la técnica CSMA/CA para resolver las colisiones. Explicad brevemente en qué consiste esta técnica y justificad por qué no se puede aplicar la técnica CSMA/CD que utiliza Ethernet.

2. LMDS es una tecnología sin hilos que facilita el acceso a otras redes. El bucle telefónico de abonado tradicional también nos permite el acceso a otras redes. ¿Qué ventajas tiene un acceso LMDS con respecto a un acceso de bucle telefónico tradicional desde el punto de vista de operador?

3. ¿Cuáles son los pasos que debe seguir un empresario o un particular que quiera contratar el servicio LMDS con una de las operadoras que lo ofrecen en España?

4. El primer estándar LMDS (802.16) funciona en la banda de los 10-66 GHz. Una nueva versión de este estándar (802.16a) funciona en la banda de los 2-6 GHz. Explicad las principales ventajas de este nuevo estándar con respecto al primer estándar.

5. Explicad cómo funciona el ahorro de potencia en las redes locales sin hilos (WLAN) configuradas con infraestructura, e indicad qué es y qué papel tiene el TIM *(traffic indication map)* en este proceso de ahorro de potencia.

6. En uno entorno de interiores se dispone de un punto de acceso Wi-Fi. Como se prevé un aumento del número de usuarios, se decide poner otro punto de acceso en el mismo lugar (sintonizado en otro canal) para doblar la capacidad. ¿Por qué motivo es recomendable separar unos cuantos metros estos dos puntos de acceso?

7. En España las condiciones de uso de las bandas libres de 2,4 GHz y 5,8 GHz están descritas en las normas UN-85 y UN-128, respectivamente. En el caso de la primera, la potencia máxima son 100 mW, mientras que, en el caso de la segunda, la potencia puede llegar a 1 W, con ciertas restricciones. ¿Por qué motivos el Estado permite que en la banda de 5,8 GHz se emita con más potencia que en la de 2,4 GHz?

8. ¿Qué es una red 802.16 con topología *mesh*?

Solucionario

1. El CSMA determina si la energía de señal en un determinado ancho de banda supera cierto umbral. Si la energía es inferior al umbral, el transmisor podrá enviar datos (antes enviará una trama o *frame*). Si no, esperará un tiempo aleatorio. El CA hace que la estación destino devuelva un ACK después de cada trama recibida (si no lo devuelve, se retransmite). Ethernet utiliza CD (*colision detection*), ya que después de enviar puede escuchar el medio y ver si ha habido colisión. Ahora no podemos escuchar el medio, ya que en el aire el margen dinámico de las señales es grande.

2. Algunas de las ventajas son:
– LMDS tiene más ancho de banda y, por tanto, permite ubicar más información.
– LMDS permite fácilmente conexiones asimétricas, que son adecuadas para servicios interactivos.
– LMDS tiene un tiempo de despliegue más pequeño (no hace falta cablear) y requiere menos inversión.

3. Para contratar LMDS, primero debe comprobarse si alguna empresa con licencia LMDS ofrece cobertura. En caso afirmativo, deben acudir unos técnicos de la empresa para verificar que la cobertura es correcta (verificar que hay visión directa con la estación LMDS) y tener permiso para instalar la antena que nos comunicará con la estación base de ellos.

4. El primer estándar trabaja a unas frecuencias tan elevadas que es necesaria visión directa. Eso obliga a que emisor y receptor estén en posiciones fijas (típicamente, en tejados de edificios). Con el nuevo estándar, se permite cierto movimiento de emisor y/o receptor (la visión directa no es del todo necesaria) y además se puede tener más alcance (cuanta menos frecuencia, menos pérdidas de propagación).

5. Este ahorro de potencia se basa en el hecho de que las estaciones pueden estar despiertas o dormidas. Cada cierto tiempo, todas se despiertan a la vez (se necesita sincronización) y el punto de acceso (hablamos de la configuración con infraestructura) envía en el *beacon* una lista de los receptores para los que tiene información. Esta lista es el TIM y los receptores que figuren en ella no podrán volverse a dormir hasta recibir la información que el punto de acceso tiene para ellos.

6. Se recomienda separar los puntos de acceso porque los filtros no son ideales, y se colaría información no deseada. Cuando decimos que un punto de acceso emite en cierto canal, debe tenerse presente que también tiene ciertas emisiones en los canales adyacentes. Así, si un punto de acceso emite en el canal 1 y otro punto de acceso emite en el canal 2, si están muy próximos, el primero recibirá por el canal 1 una parte de la información que el otro punto de acceso está emitiendo por el canal 2, ya que al lado tiene un emisor en el canal 2 que le está introduciendo interferencias de canal adyacente. Dejando una separación, el efecto queda bastante reducido, ya que con la distancia estas interferencias quedan rápidamente atenuadas.

7. El principal motivo es el de que a altas frecuencias la propagación es más difícil, y para llegar a cierta distancia, hace falta más potencia si lo hacemos a 5,8 GHz que si lo hacemos a 2,4 GHz. Otro motivo es que en la banda de 5,8 GHz hay menos servicios en funcionamiento y, por lo tanto, podemos emitir a más potencia sin que otros servicios se vean afectados. Cabe decir que sólo se permite emitir a 1 W si utilizamos técnicas de control de potencia y selección dinámica de frecuencia (es decir, garantizamos un uso racional del espectro).

8. Una red 802.16 con topología *mesh* es aquélla en la que para ir de un punto a otro no hay un camino preestablecido, sino que podemos ir dando saltos entre varias estaciones.

Glosario

ACK *f* Conformidad o reconocimiento positivo.

AES *m* Servicio de cifrado adelantado.

AIFS *m* Tiempo variable que permite asignar prioridades en el estándar 802.11.

AP *m* Punto de acceso.

ATIM *f* Lista de receptores para los cuales tenemos datos para enviar, en redes *ad hoc* dentro del estándar 802.11.

BE *m* Lo mejor posible.
en best effort

BER *f* Tasa de error de bit.

best effort *m* Véase **BE**.

BPSK *f* Modulación de fase de dos estados.

BS *f* Estación base.

BSS *m* Conjunto de estaciones base conectadas a un mismo punto de acceso en WiMAX.

CA *f* Prevención de colisiones en accesos multiusuario.

CCK *m* Tipo de código complementario que, entre otros, se utiliza en el estándar 802.11.

CD *f* Detección de colisiones en accesos multiusuario.

CFend *m* Final del periodo libre de colisiones en el estándar 802.11.

clear to send *f* Véase **CTS**.

CNAF *m* Cuadro Nacional de Atribución de Frecuencias en el Estado español.

CPE *f* Unidad de usuario en WiMAX.

CSMA *m* Mecanismo que determina la energía de señal dentro de cierto ancho de banda.

CTS *f* Respuesta que da un equipo a otro equipo que le ha comunicado que está preparado para transmitir.
en clear to send

DCF *f* Función de coordinación distribuida en el estándar 802.11.

DECT *m* Estándar de tercera generación de telefonía sin hilos.

DFS *f* Selección dinámica de frecuencia.

DIFS *m* Tiempo de espera que utiliza el estándar 802.11 cuando trabaja en modo distribuido.

DQPSK *f* Modulación QPSK que codifica la diferencia de fase entre estados.

DSSS *m* Sistema de espectro ensanchado de secuencia directa.

DTIM *f* Lista de receptores para los que tenemos datos para enviar, en tramas *broadcast* dentro del estándar 802.11.

EAP *m* Uno de los protocolos que permite la comunicación entre un punto de acceso y un servidor de autenticación en redes 802.11.

ESS *m* Conjunto de BSS interconectadas en el estándar 802.11.

ETSI *m* Instituto de Estándares Europeos de Telecomunicaciones.

FHSS *m* Sistema de espectro ampliado que usa saltos en frecuencia.

GSM/GPRS *m* Estándar de telefonía móvil de segunda generación que permite transmisión de datos.

HCF *m* Modo de coordinación híbrido que se usa en el estándar 802.11 para combinar los modos centralizado y distribuido.

IEEE *m* Instituto de Estándares Electrónicos a escala internacional.

ISM *f* Banda frecuencial pensada para aplicaciones industriales, médicas y científicas en que no se necesita licencia para emitir, bajo ciertas condiciones.

LAN *f* Red de área local.

LED *m* Diodo emisor de luz.

LMDS *f* Tecnología de comunicaciones local de punto a multipunto.

LSSI *f* Ley de Servicios de la Sociedad de la Información.

MAC *f* Capa de acceso al medio.

MBWA *m Mobile broadband wireless access* (estándar 802.20).

MIC *m* Mecanismo que permite proteger la integridad de los datos.

MRC *f* Combinación de máxima ganancia (combinación óptima de señales).

NAV *m* Mensaje que, en el estándar 802.11, nos indica el tiempo que el canal estará ocupado.

OFDM/OFDMA *f* Técnica de modulación (OFDM) o acceso (OFDMA) por división en frecuencia donde la señal se transmite simultáneamente en diversas frecuencias ortogonales entre ellas.

PaP *m* Punto a punto.

PCF *f* Función de coordinación centralizada en el estándar 802.11.

PER *f* Tasa de error de paquete.

PIFS *m* Tiempo de Espera que utiliza el estándar 802.11 cuando trabaja en modo centralizado.

PIRE *f* Potencia isotrópica radiada equivaliente.

PLC *f* Tecnología que permite comunicaciones de datos mediante la red eléctrica.

PmP *m* Punto a multipunto.

PoE *m* Sistema para suministrar energía eléctrica a dispositivos sobre el mismo cable de datos.
en power over Ethernet

power over Ethernet *m* Véase **PoE**.

QoS *f* Calidad de servicio.

QPSK *f* Modulación de fase en cuadratura.

request to send *f* Véase **RTS**.

rtPS *f* Petición de recursos en tiempo real.

RTS *f* Petición de transmisión de un equipo.
en request to send

SC *f* Portadora única.

SIFS *m* Tiempo de espera que, en el estándar 802.11, utilizan las estaciones que quieren enviar un ACK.

SNR *f* Relación señal-ruido.

SSID *m* Identificador de un ESS.

TDD *m* Duplexado en tiempo.

TIM *f* Lista de receptores para los cuales tenemos datos para enviar, dentro del estándar 802.11.

TPC *m* Control de potencia.

TRAC *f* Telefonía rural de acceso celular.

TXOP *m* Tiempo durante el que una estación puede transmitir datos al canal, en el estándar 802.11.

UGS *f* Reserva de recursos prefijada.

UN *f* Nota la aplicación dentro del CNAF.

WEP *m* Es uno de los primeros mecanismos de seguridad del estándar 802.11.

WLAN *f* Red de área local sin hilos.

WLL *m* Bucle de abonado vía radio.

WPA *m* Mecanismo de seguridad en el estándar 802.11 posterior al WEP.

Bibliografía

Huidobro, J. M. (2002). *Comunicaciones móviles*. Madrid: Paraninfo.

Sendín Escalona, A. (2004). *Fundamentos de los sistemas de comunicaciones móviles*. Madrid: McGraw Hill.