Tema 11: Redes locales inalámbricas

1. Introducción a las redes Inalámbricas

Existen situaciones en las que resulta imposible o inviable utilizar cables para conectarse a la red.

Este es el caso, por ejemplo, de la conexión de dispositivos con movilidad a la red, como portátiles, móviles o tablets; la improvisación de una red para uso puntual en una feria o congreso, en una biblioteca, cafetería, hotel, aeropuerto, plaza, etc.

Hasta no hace tanto los dispositivos debían conectarse físicamente a la red, sin embargo hoy en día la red es capaz de llegar hasta los propios dispositivos.

Una red inalámbrica es aquella en la que los distintos equipos se interconectan entre sí sin necesidad de cables. La comunicación entre dispositivos inalámbricos se produce mediante ondas electromagnéticas.

1.1. Clasificación de las redes inalámbricas

Según su alcance las redes inalámbricas se clasifican del siguiente modo:

- Redes inalámbricas de ámbito personal (WPAN o wireless personal area networks): interconectan dispositivos en el entorno próximo de un usuario (pocos metros).

  Tecnologías: Bluetooth e infrarrojos (IrDA).

- Redes inalámbricas de ámbito local (WLAN o wireless local area networks): interconectan dispositivos en un local, piso, planta, edificio o campus.

  Tecnologías: WiFi.

1.1. Clasificación de las redes inalámbricas

- Redes inalámbricas de ámbito metropolitano (WMAN o wireless metropolitan area networks): interconectan dispositivos y redes en un barrio, pueblo o ciudad.

  Tecnologías: WiFi, WiMax.

- Redes inalámbricas de ámbito extenso (WWAN o wireless wide area networks): interconectan dispositivos y redes en toda una región, país o conjunto de países.

  Tecnologías: UMTS, GPRS, 3G, 4G...

En este capítulo nos centrarnos en las redes inalámbricas de ámbito local: sus características, dispositivos asociados y opciones de configuración más frecuentes.

2. WLANs
2.1. Características

Medio (naturaleza de la señal): las redes inalámbricas utilizan señales electromagnéticas para transmitir los datos. No requieren de ningún medio para ser transportadas y pueden atravesar materiales como el aire, paredes, puertas, muebles, etc...

Antenas: todos los dispositivos inalámbricos deberán disponer de ellas.

Alcance: las WLAN tienen un alcance limitado. A medida que las señales electromagnéticas atraviesan un determinado material (incluido el aire), su intensidad disminuye. El tipo de ondas, la potencia de emisión, la tecnología de modulación y el tipo y sensibilidad de las antenas determinarán el alcance (o cobertura) de los dispositivos de la red.

2.1. Características

Capacidad: las WLAN tienen una capacidad limitada. No pueden existir a la vez dos señales que utilicen el mismo tipo de ondas en una misma zona, ya que se mezclarían y no podrían interpretarse. Por esta razón, en una zona y momento determinados, sólo puede emitir un único dispositivo de la WLAN (o de otras WLAN con el mismo tipo de ondas).

Velocidad de transmisión: las WLAN tienen una velocidad de transmisión limitada. El hecho de que su capacidad sea limitada también afecta a la velocidad.

Otros factores que influyen en la velocidad son el ruido, las interferencias.

Movilidad: las WLAN permiten a los dispositivos móviles moverse libremente por toda la zona de cobertura de la WLAN.

2.1. Características

Escalabilidad: las redes inalámbricas son fácilmente escalables. La escalabilidad es la capacidad de crecer si la red lo necesita. Ampliar una WLAN es tan fácil como añadir más puntos de acceso allá donde se necesiten.

Requerimientos de seguridad: las redes inalámbricas requieren de protocolos de seguridad para proteger la información y el acceso a la red.

Cualquier persona lo suficientemente cercana a la WLAN y con un dispositivo inalámbrico con suficiente sensibilidad podría intentar acceder a la WLAN o a la información que viaja a través de ella. Para evitar que estas acciones tengan lugar tendremos que dotar a la WLAN de sistemas de seguridad: autenticación y cifrado.

2.2. Ventajas e inconvenientes respecto a las LAN cableadas

Principales ventajas:

— **Permiten la movilidad de usuarios y dispositivos:** los usuarios pueden desplazarse con sus dispositivos inalámbricos a lo largo de toda la zona de cobertura de la WLAN sin perder la conexión.

— **Menor coste:** el hecho de necesitar muy pocos cables, o incluso ninguno si la red es pequeña, junto con el bajo coste de los componentes de la WLAN hacen que la instalación resulte muy económica.

— **Menor tiempo de instalación:** es más rápida porque no se tienen que instalar cables. canalizaciones, rosetas, etc.

2.2. Ventajas e inconvenientes respecto a las LAN cableadas

Principales inconvenientes:

— Sensibilidad a las interferencias electromagnéticas y a la presencia de otras WLAN: la presencia de interferencias electromagnéticas y de otras WLAN que operen con frecuencias próximas a las de la nuestra puede influir negativamente en el rendimiento de la misma.

— Si en una zona aumenta el número de dispositivos, el rendimiento en dicha zona disminuye: en una misma zona e instante solo puede existir una transmisión para nuestra WLAN, pues sería como si todos los dispositivos de la zona estuvieran conectados a un mismo cable o hub. Esto no ocurre en las redes cableadas basadas en switches.

2.2. Ventajas e inconvenientes respecto a las LAN cableadas

Principales inconvenientes:

— Velocidades de transmisión generalmente inferiores: aunque cada vez surgen tecnologías más veloces, todavía no se ha llegado a igualar la velocidad que ofrecen los medios cableados.

— Mayores requerimientos de seguridad: dado que no hace falta acceder físicamente a las WLAN para atacarlas, necesitan mayor seguridad. Esto supone una mayor complejidad de instalación y requiere más atención que las redes cableadas.

3. Estándares WLAN. Estándares IEEE 802.11

Existen varios protocolos y estándares para las redes locales inalámbricas, sin embargo, los más utilizados son los IEEE 802.11.

(El IEEE es el Instituto de Ingenieros Eléctricos y Electrónicos de EE.UU.)

Podemos verlos en la siguiente tabla:

3. Estándares WLAN. Estándares IEEE 802.11

Protocolo IEEE	Banda de frecuencias (GHz)	Velocidad máxima de transmisión	Compatibilidad con versiones anteriores
802.11 (original)	2,4	2 Mb/s	-
802.11a	5,7	54 Mb/s	-
802.11b	2,4	11 Mb/s	-
802.11g	2,4	54 Mb/s	802.11b
802.11n	2,4 y 5,7	600 Mb/s	802.11a/b/g
802.11ac	5,7 (compatible con 2,4)	1,3 Gb/s	802.11a/b/g/n
802.11ad	60 (compatible con 2,4 y 5,7)	7 Gb/s (a corta distancia)	802.11a/b/g/n/ac

3. Estándares WLAN. Estándares IEEE 802.11

Compatibilidad entre estándares

Todos los estándares IEEE 802.11 son compatibles con sus predecesores que operan en la misma banda de frecuencias.

Sin embargo, cuando un dispositivo opera con una tecnología predecesora, toda la red se adapta a esa tecnología, lo que provoca que el rendimiento de la red disminuya considerablemente.

3. Estándares WLAN. Estándares IEEE 802.11

Certificación WiFi

La WiFi Alliance es una organización internacional sin ánimo de lucro que se encarga de certificar si los productos de los fabricantes cumplen con los estándares IEEE 802.11.

Cuando un dispositivo cumple con un estándar IEEE 802.11, la Wi-Fi Alliance le otorga un certificado.

El fabricante puede entonces poner el sello WiFi CERTIFIED™.

El certificado WiFi garantiza la fidelidad a los estándares y, por lo tanto, que los productos de los distintos fabricantes sean compatibles entre sí.

4. Infraestructura inalámbrica

El estándar IEEE 802.11 define una infraestructura de red que establece las bases de funcionamiento de las WLAN.

Para ello define un conjunto de componentes físicos y lógicos, dos modos de operación y toda una colección de protocolos y especificaciones agrupados en dos capas, la física y la de enlace, de la pila de protocolos OSI.

El estándar IEEE 802.11, además, guarda compatibilidad en todo momento con las redes de área local IEEE 802.3 (Ethernet) de tal forma que una red WLAN se puede integrar dentro de una LAN Ethernet convencional.

4.1. Componentes físicos: las estaciones

En una red inalámbrica, una estación es cualquier dispositivo que implementa el estándar IEEE 802.11.

Una estación puede ser **un ordenador, una tablet, un móvil, un punto de acceso, un dispositivo multifunción, etc.**

Las estaciones se conectan a la red inalámbrica mediante una tarjeta o adaptador de red inalámbrico, ya sea este interno, una tarjeta PCI, un USB, etc.

4.1. Componentes físicos: las estaciones

Puntos de acceso (AP)

Un punto de acceso (Access Point o AP) es una estación especializada que dispone de dos interfaces de red distintas: una por cable y otra inalámbrica.

Los puntos de acceso anuncian una WLAN, es decir, hacen público un nombre de red a la cual se pueden conectar otras estaciones.

Por una parte ejercen de puente entre los dispositivos inalámbricos y la red cableada: las estaciones conectadas a la WLAN a través del AP podrán acceder a la LAN.

4.1. Componentes físicos: las estaciones

Puntos de acceso (AP)

Pero también ejercen de intermediario en el proceso de comunicación entre estaciones inalámbricas:

1. cuando un dispositivo de la WLAN quiere enviar información a otro de la WLAN o de la LAN, envía la información al AP
2. y éste la reenvía hacia el dispositivo destino correspondiente basándose en su dirección física o MAC.

El funcionamiento de un AP es un híbrido entre un hub y un switch.

4.1. Componentes físicos: las estaciones

Dispositivos multifunción

Las WLAN domésticas y de oficina no suelen tener una extensión demasiado grande y generalmente es un único punto de acceso el que da cobertura a toda la casa o empresa.

Por ello existen dispositivos que integran en su interior las funciones de router, switch y punto de acceso: son los dispositivos multifunción o **routers inalámbricos**.

Puede que, además, incorporen también un MODEM (ADSL, fibra...) si conectan directamente con Internet.

4.1. Componentes físicos: las estaciones

Dispositivos multifunción

También los móviles tienen la función de crear una red WiFi para permitir conectar a otros aparatos a Internet a través de su red de datos.

En este caso también actuarían como dispositivos multifunción (serían routers inalámbrico).

Y también los ordenadores si tienen LAN cableada y una tarjeta inalámbrica pueden hacer de dispositivo multifunción y crear una WiFi que permita la conexión de dispositivos inalámbricos a la red local.

4.2. Componentes lógicos

Conjunto de servicios (SS o *Service Set*)

Es el equivalente a una LAN pero en inalámbrico.

Toda red inalámbrica con un único AP o con múltiples AP, tiene un nombre que la identifica: el identificador del conjunto de servicios (SSID).

El SSID es un nombre compuesto por 32 dígitos alfanuméricos como máximo y es el que utilizan los usuarios para identificarse y conectarse a la red.

Generalmente los dispositivos que ofrecen conexión a una red inalámbrica publican su SSID para que las distintas estaciones los puedan reconocer con un simple escaneo de redes disponibles al alcance. Sin embargo, como veremos más adelante, el SSID también se puede ocultar.

4.2. Componentes lógicos

- Cuando una red inalámbrica tiene un único AP se denomina **BSS** (*Basic Service Set* o conjunto básico de servicios).

Cada conjunto básico de servicios posee un identificador único en la red local: el **BSSID**, que es un número binario de 48 bits, que es normalmente la dirección MAC del AP.

- Cuando una red inalámbrica tiene múltiples AP (para ampliar o mejorar su cobertura) se denomina **ESS** (*Extended Service Set* o conjunto básico de servicios).

En este caso habrá varios BSSIDs, uno por cada punto de acceso.

Cuando el SSID identifica un ESS se denomina **ESSID** (identificador del ESS).

5. Nivel físico
5.1. Señales electromagnéticas

Una señal electromagnética es un conjunto de ondas electromagnéticas cuyas propiedades físicas les permiten ser portadoras de información.

Sus características son:

— Frecuencia: número de ciclos o perturbaciones completas por unidad de tiempo. Se mide en hercios (Hz) o sus derivados (KHz, MHz, GHz). Un hercio corresponde a un ciclo por segundo.

— Longitud de onda: distancia que es capaz de recorrer la onda en el vacío en un ciclo o perturbación completa. Es inversa a la frecuencia.

— Energía: la energía asociada a una onda electromagnética.

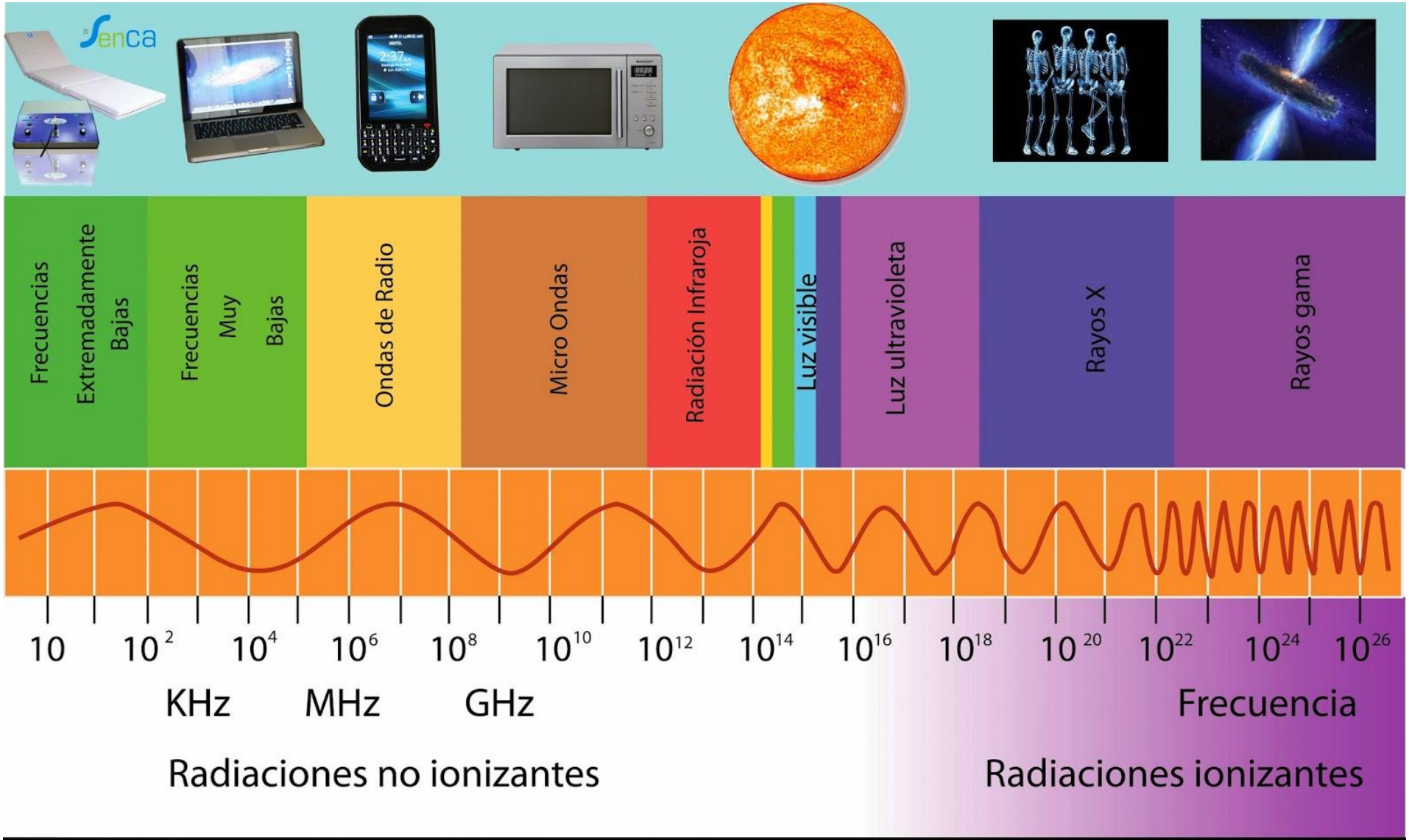
5.2. El espectro electromagnético

Las ondas electromagnéticas se clasifican en función de las propiedades descritas en el apartado anterior.

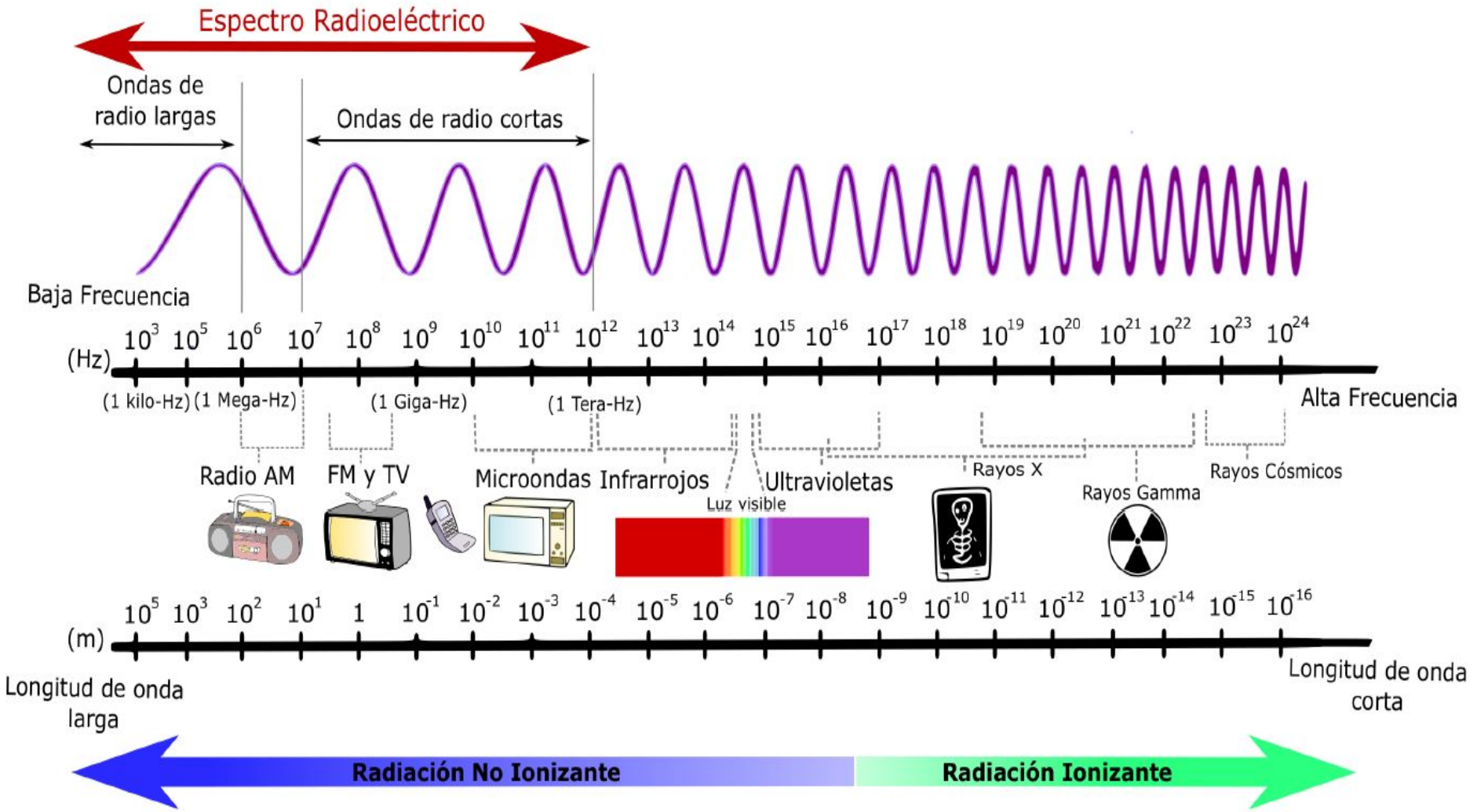
El conjunto de todas las tipologías de radiación electromagnética recibe el nombre de espectro electromagnético.

Las siguientes figuras resumen los distintos tipos de radiación electromagnética que existen y el nombre que reciben:

5.2. El espectro electromagnético



5.2. El espectro electromagnético



5.3. El espectro radioeléctrico

Para impedir que distintas señales electromagnéticas puedan solaparse o interferir unas con otras, existe una regulación sobre su emisión.

La Unión Internacional de Telecomunicaciones (ITU) regula las emisiones a nivel mundial y el Instituto Europeo de Estándares de Telecomunicaciones (ETSI), a nivel europeo.

Cada país posee además su propia regulación, que se adapta a las internacionales y las completa.

5.3. El espectro radioeléctrico

Estas organizaciones dividen el espectro electromagnético en rangos de frecuencias llamadas bandas.

Cada banda, a su vez, se puede dividir en más bandas, según lo que se necesite.

Las comunicaciones inalámbricas se encuentran dentro de un rango de frecuencias llamado espectro radioeléctrico o bandas de radiofrecuencia, que se corresponde con un rango que oscila entre los 300 Hz y los 300 GHZ.

En general, para poder emitir en una determinada frecuencia hace falta disponer de una licencia.

Sin embargo cada país puede reservar una parte para su uso sin licencia, siempre y cuando no se superen los niveles de potencia delimitados. Es el caso de las WiFis

5.4. Potencia de emisión

La potencia de emisión es la intensidad con que se emiten las señales electromagnéticas desde una antena. Normalmente se mide en milivatios (mW).

La potencia permite aumentar el alcance. Sin embargo es importante recordar que en cada país existe una potencia máxima de emisión. En España la potencia máxima de emisión sin licencia es de 100mW.

También nos puede interesar lo contrario, es decir, disminuir la potencia de emisión por cuestiones de seguridad. De esta manera se puede limitar el alcance de la WLAN para evitar que nuestras comunicaciones salgan de nuestro edificio y puedan ser interceptadas y analizadas por personas ajenas a la organización.

5.5. Atenuación y dispersión

La atenuación es la pérdida de intensidad de una señal electromagnética a lo largo de su paso a través de un medio (incluido el aire) debido a que parte de sus ondas son absorbidas por el propio medio en forma de calor.

La dispersión se produce cuando las ondas que forman la señal no se propagan todas en la misma dirección, sino que se separan, de tal modo que a medida que la señal avanza su intensidad disminuye.

La atenuación y la dispersión producen una pérdida de intensidad de la señal a lo largo de su recorrido. Las ondas de las WLAN atraviesan mejor el aire que la madera, mejor la madera que los ladrillos y mejor los ladrillos que el cemento.

5.6. Interferencias y ruido

Se denomina interferencia a cualquier perturbación electromagnética no deseada que afecta a la señal electromagnética.

A nivel de las WLAN el origen de las interferencias es diverso, pudiendo provenir desde de las señales procedentes de otras WLAN hasta de emisiones de ondas próximas en frecuencia producidas por ejemplo por un microondas de cocina.

Cuando existen interferencias es importante, siempre que sea posible, detectar la fuente para poder solucionar el problema.

Existe una radiación electromagnética de base, generalmente de poca intensidad, que es inevitable. A este tipo de interferencias se las conoce como ruido.

5.7. RSSI, SNR y pérdida de la señal

El **indicador de fuerza de señal recibida (RSSI)** indica con qué potencia se recibe la señal.

El RSSI se mide en dBm y suele tener valor negativo.

La razón señal-ruido (SNR) indica la diferencia entre la potencia de la señal y la del ruido. **La SNR se mide en dB** (decibelios).

La calidad de la señal determinará que se pueda establecer la conexión, así como la velocidad de la misma.

Se dice que se ha perdido la señal cuando ya no es posible interpretarla debido a que se ha atenuado o dispersado.

5.8. Modulación

La modulación es la técnica que permite transmitir información a través de las bandas del espectro radioeléctrico mediante la modificación de las ondas que viajan por esas bandas.

A cada una de las bandas utilizadas en el proceso de modulación se las conoce como bandas portadoras de la información.

Las tecnologías de modulación están en constante desarrollo.

Cuanta más información se pueda transmitir en un tiempo menor y con una menor pérdida, mayor será la velocidad de la transmisión de datos en la WLAN.

Las tecnologías de modulación más usadas en las WLAN son: FHSS, DSSS, OFDM...

5.8. Modulación

Modulación en los estándares IEEE 802.11	
Estándar IEEE	Modulación
802.11 (original)	FHSS/DSSS
802.11a	OFDM
802.11b	DSSS
802.11g	OFDM/DSSS
802.11n	OFDM+MIMO

5.8. Modulación

Tecnología de múltiple entrada-múltiple salida (MIMO)

Esta tecnología utiliza múltiples antenas para la emisión y la recepción de la señal.

Puede operar en varias frecuencias a la vez y ofrece mayor alcance, robustez y velocidad que los métodos convencionales.

MIMO es la base tecnológica del estándar IEEE 802.11n, que puede operar a 2,4 GHZ, a 5,7 GHZ o en ambas frecuencias a la vez y llegar a velocidades de transmisión de hasta 600 Mbps.

5.8. Modulación

Velocidad de transmisión

Cuando dos dispositivos inalámbricos quieren intercambiar información entre ellos, deben negociar en primer lugar qué tipo de modulación van a utilizar.

En condiciones óptimas (SNR excelente) se elegirá aquella modulación que ofrezca mayor velocidad de transmisión; pero cuando haya pérdida de señal se pueden negociar nuevos parámetros o incluso cambiar el tipo de modulación para ganar robustez, lo que conllevará siempre velocidades de transmisión más bajas.

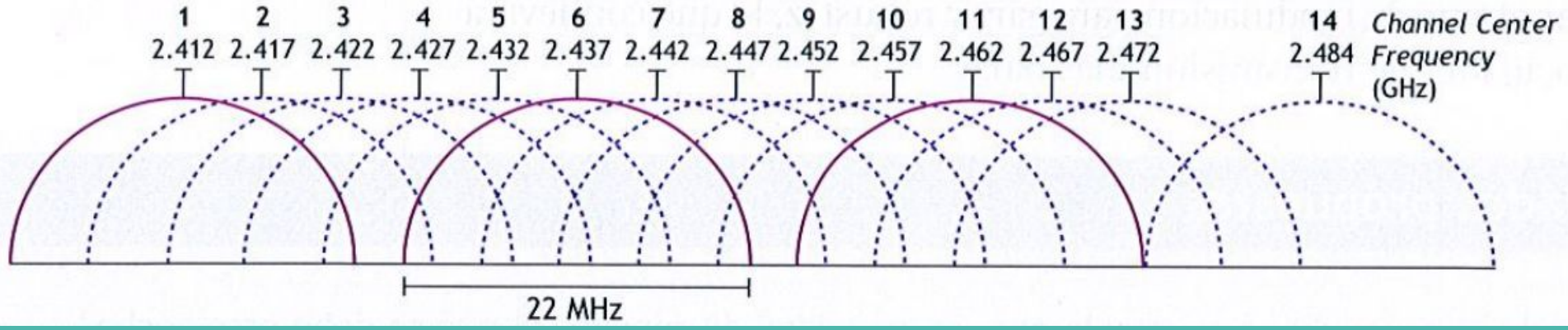
Estándar IEEE	Velocidades (Mbps)
802.11 (original)	1,2
802.11a	6, 9, 12, 18, 24, 36, 48, 54
802.11b	5,5, 11
802.11g	6, 9, 12, 18, 24, 36, 48, 54
802.11n	15, 30, 45, 60, 90, 120, 135, 150, 180, 270, 300...

5.9. Canales

Ya sabemos que las redes WiFi operan en las bandas de 2,4GHz y 5GHz, pero estas bandas son muy anchas y pueden permitir la coexistencia de varias redes WiFi en una misma zona.

Que las redes se interfieran o no entre sí dependerá de los canales que utilicen.

En el ámbito de las redes WiFi, un canal es el rango de frecuencias que utiliza una red WiFi para operar. Se caracteriza por tener una frecuencia central y un ancho de banda.



5.9. Canales

Redes WiFi b y g

Los estándares IEEE 802.11 b y g utilizan frecuencias dentro de la banda de 2,4GHz y necesitan un ancho de banda de 22MHz para funcionar.

El IEEE ha definido 13 canales consecutivos en el rango de frecuencias de 2,401GHz a 2,483GHz, separados entre sí por 5MHz, así como un canal superior (el 14) con centro en los 2,484GHz.

Como se puede observar, los diferentes canales se encuentran solapados entre sí.

Cuando dos redes distintas operan en canales solapados, su rendimiento disminuye considerablemente.

5.9. Canales

Canal	Frecuencia central (GHz)	Rango de frecuencias (GHz)
1	2,412	2,401 - 2,423
2	2,417	2,406 - 2,428
3	2,422	2,411 - 2,433
4	2,427	2,416 - 2,438
5	2,432	2,421 - 2,443
6	2,437	2,426 - 2,448
7	2,442	2,431 - 2,453
8	2,447	2,436 - 2,458
9	2,452	2,441 - 2,463
10	2,457	2,446 - 2,468
11	2,462	2,451 - 2,473
12	2,467	2,456 - 2,478
13	2,472	2,461 - 2,483
14	2,484	2,473 - 2,495

5.9. Canales

Los usuarios domésticos no suelen tener conocimientos sobre canales y solapamientos.

Normalmente instalan los routers WiFi sin modificar la configuración de fábrica de su canal de emisión, con lo que es fácil que se produzcan solapamientos entre las redes WiFi de las zonas urbanas.

¡Vosotros no sois usuarios domésticos!

Redes WIFI a

Estas redes también operan por canales distribuidos en la banda de 5GHz, concretamente dentro del rango de 4,915 GHz a 5,825 GHz.

Cada canal puede ocupar un ancho de banda de 10, 20 o 40 MHz. El número de canales disponibles también varía según el país.

5.10. Antenas

Una antena no es más que un hilo de material conductor a través del cual se pueden generar señales electromagnéticas a partir de señales eléctricas y/o generar señales eléctricas cuando sobre él inciden señales electromagnéticas.

Las principales características de las antenas, que es necesario conocer para poder compararlas, son las siguientes:

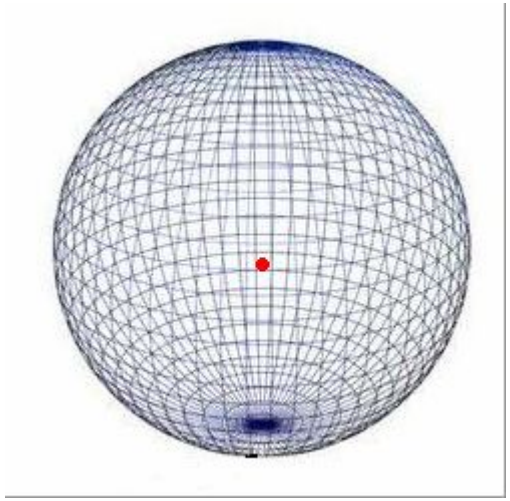
Direccionalidad

La direccionalidad hace referencia al modo de radiar de la antena, es decir, a la potencia que se alcanza en cada dirección del espacio durante la emisión.

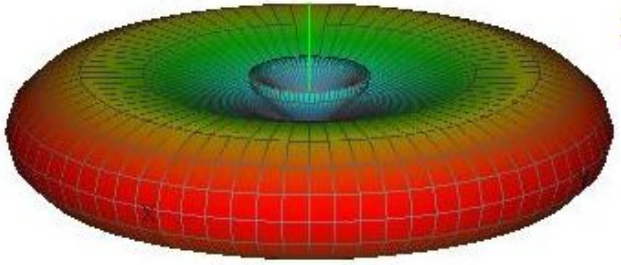
5.10. Antenas

Según su **direccionalidad** las antenas se clasifican en:

— Antenas **isotrópicas**: emiten con la misma intensidad hacia todas las direcciones del espacio (la zona de cobertura tiene forma esférica).



— Antenas **omnidireccionales**: emiten con la misma intensidad hacia todas las direcciones de un plano del espacio.



5.10. Antenas

— Antenas **sectoriales**: emiten con mayor intensidad hacia una región concreta del espacio, donde generalmente se logra mayor alcance que con una antena omnidireccional. Son habituales en las redes metropolitanas.

— Antenas **direccionales**: emiten con mayor intensidad hacia una dirección concreta del espacio, en la cual pueden lograr mayor alcance que las antenas omnidireccionales. Se utilizan habitualmente para conectar puntos de la WLAN lejanos entre sí y en las redes inalámbricas metropolitanas.

5.10. Antenas

Ganancia

La ganancia es el incremento de potencia que aporta una antena direccional o sectorial en la dirección de máxima radiación respecto a una antena modelo.

Se mide en **dBi** cuando se utiliza como modelo una antena isotrópica teórica (decibelios respecto a una antena isotrópica) y en **dBd** cuando el modelo es una antena omnidireccional real (decibelios respecto a un dipolo).

Cuando un dBi o dBd es igual a cero, significa que no hay ganancia respecto al modelo; valores superiores indican que hay un incremento de potencia **en esa dirección** respecto a la antena modelo y valores negativos señalan que hay pérdida de potencia.

6. Subcapa MAC en 802.11
6.1. Direccionamiento físico (dirección MAC)

Cada estación inalámbrica tiene una dirección física (dirección MAC) que la identifica de forma única en todo el mundo.

Esta tiene la misma estructura y formato que la dirección MAC del protocolo Ethernet y ambas pueden coexistir en la misma red.

No puede haber una dirección MAC inalámbrica que coincida con una física. Los fabricantes están obligados a que sean únicas.

6.2. Tramas en 802.11

Tipos de trama

El estándar distingue tres tipos de tramas:

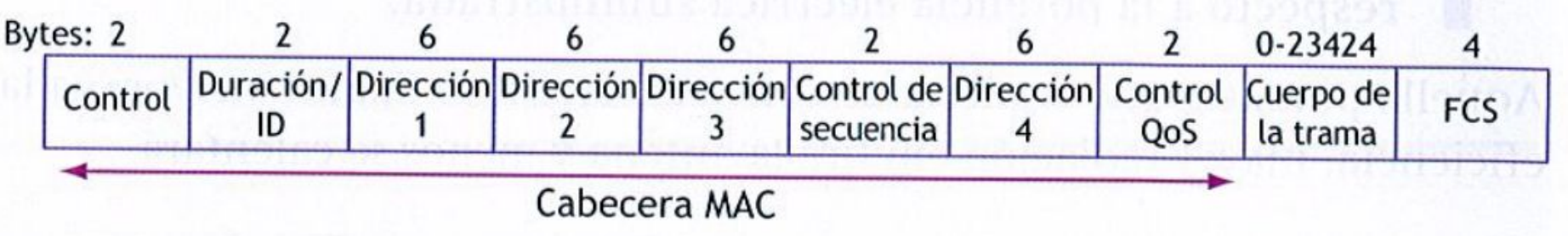
— De datos: contienen los datos a transmitir de las capas superiores.

— De control: permiten ejercer un control sobre las transmisiones en curso o pendientes de iniciar. A lo largo del capítulo veremos algunos ejemplos, como las tramas ACK, RTS o CTS.

— De gestión: permiten establecer y gestionar las conexiones inalámbricas, como por ejemplo la publicación del SSID, las solicitudes y confirmaciones de asociación o las tramas implicadas en el proceso de autenticación.

6.2. Tramas en 802.11

Formato de las tramas



— Campos de la cabecera:

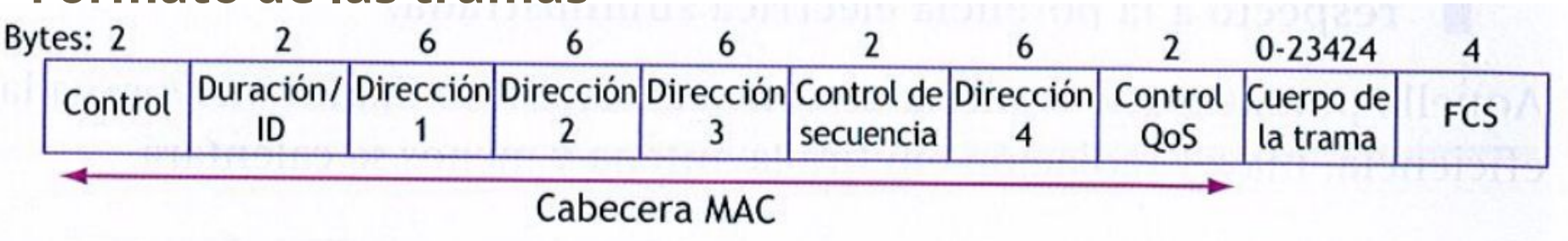
Control: permite indicar, entre otras cosas, el tipo de trama.

Duración/ID: varía su significado en función del tipo de trama.

Direcciones 1, 2, 3 y 4: permiten identificar el BSSID, la estación origen, la estación destino, la estación que está transmitiendo y la estación que está recibiendo (estas dos últimas no son necesariamente el origen y el destino, sino que pueden ser puntos de acceso intermedios). El significado de cada campo varía en función del tipo de trama.

6.2. Tramas en 802.11

Formato de las tramas



— **Campos de la cabecera:**

Control de secuencia: permite identificar cada trama para poder así confirmar su recepción. ¡Como si fuera el TCP!

Control de la QoS *(quality of service):* permite indicar la calidad de servicio necesaria en la transmisión.

— **Cuerpo:** contiene los datos a transmitir de los niveles superiores.

— **FCS** *(frame checksum):* es un código de detección de errores de 32 bits

6.3 Acuse de recibo (ACK)

En las redes IEEE 802.11. en general, se debe confirmara la estación origen la recepción de la trama mediante el envío de una trama especial llamada ACK.

Si la estación que envió la trama no recibe el ACK en un margen de tiempo determinado, considerará que se ha producido una colisión y reenviará la trama de nuevo.

¡Como si fuera TCP!

6.4. Control de acceso al medio

En las redes IEEE 802.11 se utilizan los protocolos CSMA/CA y RTS/CTS:

— **CSMA/CA:** cuando una estación quiere emitir, primero debe analizar el medio para comprobar si ya hay alguna transmisión en curso (protocolo CSMA, acceso múltiple con escucha de la portadora).

Si el medio está ocupado, espera un tiempo aleatorio y vuelve a consultar; mientras que, si está libre, en lugar de emitir directamente (como se haría en el CSMA/CD), se espera un tiempo definido para permitir que se envíe la trama de confirmación (ACK) de la transmisión anterior y evitar así que se produzcan colisiones con ella (protocolo CA, prevención de colisiones).

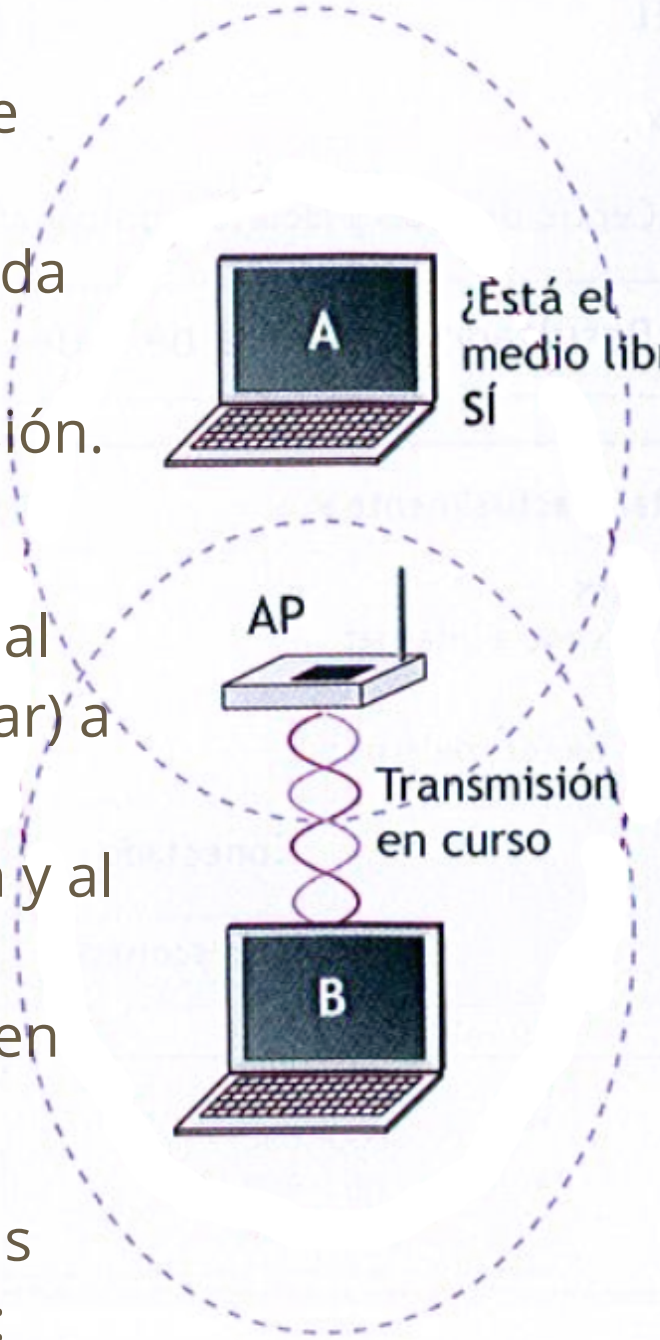
Pasado ese tiempo vuelve a escuchar y si el medio está libre, envía

6.4. Control de acceso al medio

— **RTS/CTS:** cuando una estación (A) quiere enviar datos a otra estación (B), antes de hacerlo envía a B una trama especial llamada RTS (*request to send* o solicitud de envío) indicándole que desea iniciar una transmisión.

Entonces, si B no está ocupada y detecta el canal como libre, enviará una trama especial llamada CTS (*clear to send* o libre para enviar) a toda su zona de cobertura, indicando a la estación A que puede iniciar la transmisión y al resto de estaciones que deben detener su actividad hasta que finalice la transmisión en curso.

Este protocolo permite evitar los problemas derivados de los nodos ocultos (ver figura):



7. Seguridad en las WLAN

En las WLAN la red y su información quedan expuestas a cualquier persona con un dispositivo inalámbrico con suficiente sensibilidad como para capturar las transmisiones o interaccionar con la red.

A un posible atacante no le será necesario entrar físicamente en la empresa para escuchar las comunicaciones inalámbricas que se produzcan o tratar de conectarse a la propia red, tan solo le hará falta encontrar un punto donde la calidad de la señal sea suficientemente buena como para poder llevar a cabo esas acciones.

Para intentar dotar a las redes de un nivel de seguridad equivalente al de una red cableada, se usan dos técnicas: la autenticación y el cifrado.

7.1. Autenticación

La autenticación es el procedimiento mediante el cual los dispositivos que desean acceder a la red se identifican ante ella y esta decide autorizar o denegar el acceso solicitado.

La autenticación previene los accesos no autorizados a la red.

Este procedimiento se lleva a cabo mediante tramas de gestión.

A continuación se describen los distintos tipos de autenticación utilizados en las redes IEEE 802.11:

Sistema abierto (open system)

La autenticación de sistema abierto es aquella en la que no se comprueba la identidad del dispositivo que desea conectarse a la red, sino que simplemente se autorizan todos los accesos. Por lo tanto, todo el mundo podrá conectarse a la red.

7.1. Autenticación

Clave compartida (PSK)

La autenticación de clave previamente compartida (PSK, *preshared key*) se basa en el hecho de que, para poder autorizar el acceso de una estación, esta debe demostrar que conoce una clave determinada que previamente se habrá introducido en el punto de acceso.

Es decir, es como una contraseña.

Solo se les autorizará el acceso a la red a los dispositivos que acrediten conocer la clave compartida.

Es importante destacar que este tipo de autenticación no discrimina a los usuarios que pueden entrar en la WLAN.

Este es el método más utilizado en las WiFis.

7.1. Autenticación

Filtros MAC

Los filtros MAC actúan a nivel de la asociación de un dispositivo a un punto de acceso inalámbrico.

En los puntos de acceso se pueden crear listas de direcciones MAC que determinen cuáles se han de autorizar y cuáles rechazar cuando envíen solicitudes de asociación.

Se deberá comprobar si la dirección MAC del dispositivo existe o no en las lista de direcciones MAC autorizadas o no autorizadas.

Se puede aceptar sólo a los autorizados y descartar el resto o descartar a los no autorizados y aceptar a todos los demás.

Los filtros MAC pueden coexistir con otras autenticaciones como la clave compartida.

7.1. Autenticación. IEEE 802.1x

IEEE 802.1x y protocolo ampliable de autenticación (EAP)

El problema de las claves compartidas está en que todo usuario con acceso a la red conoce la clave, por lo que, si se le quiere retirar el acceso a un usuario o grupo de usuarios o si la clave es descubierta por personas no autorizadas, se debe cambiar la clave y comunicarla a todos los usuarios de la red para que la cambien en sus dispositivos, procedimiento que suele ser lento e inseguro.

Este problema es especialmente preocupante en entornos empresariales o con muchos usuarios, como en los centros docentes y universitarios, además de poco adecuado para hoteles, hospitales, etc.

7.1. Autenticación. IEEE 802.1x

La solución que da el estándar **IEEE 802.1x** consiste en que **cada usuario tiene sus propias credenciales de acceso a la red** (por ejemplo, un nombre de usuario y una contraseña, un certificado digital, etc.) y se autentica con ellas.

Se define una arquitectura de autenticación basada en el modelo cliente-servidor con tres componentes básicos:

— **Dispositivos suplicantes:** son aquellos dispositivos cliente que desean acceder a la red y que deben ser autenticados para ganar dicho acceso.

— **Servidor de autenticación:** equipo que almacena una base de datos con las credenciales de los clientes autorizados a acceder a la red. Normalmente se trata de un servidor RADIUS o, más recientemente, DIAMETER.

7.1. Autenticación. IEEE 802.1x

Las credenciales pueden ser desde simples nombres de usuario y contraseñas hasta certificados digitales firmados por entidades de confianza.

— **Dispositivos autenticadores:** son aquellos a los que se conectan los dispositivos clientes para acceder a la red. En las redes inalámbricas son los puntos de acceso.

Los dispositivos autenticadores gestionan el procedimiento de autenticación entre los suplicantes y el servidor de autenticación, haciendo de puente entre ellos.

7.1. Autenticación. IEEE 802.1x

El estándar define el protocolo EAP (*extensible authentication protocol* o protocolo de autenticación ampliable) como base para el procedimiento de autenticación entre cliente y servidor.

Existen multitud de soluciones disponibles en el mercado para llevar a cabo este procedimiento, entre las cuales destacan los siguientes:

— **EAP-TLS** (*EAP transport layer security* o EAP con seguridad en la capa de transporte)

— **EAP-TTLS** (*EAP tunneled TLS* o EAP con túneles para TLS)

— **PEAP** (*protected EAP* o EAP protegido)

— **LEAP** (*lightweight EAP* o EAP ligero)

7.1. Autenticación

Portales cautivos

Los portales cautivos regulan el acceso a la red a nivel de aplicación, interceptando todo el tráfico dirigido al protocolo HTTP.

Este es el portal que solemos encontrar en el acceso WiFi de un hotel, camping, aeropuerto, etc.

Consiste en una especie de Proxy que filtra todo el tráfico de la WLAN, por la que solo puede navegar el usuario que introduce unas credenciales que previamente ha solicitado al propietario de la red.

Mientras el usuario no se autentique, el Proxy redirige todos los intentos de navegación hacia el portal cautivo, al tiempo que muestra al usuario la pantalla para que se autentique.

7.1. Autenticación

Ejemplo de portal cautivo:

7.1. Autenticación

Portales cautivos

Normalmente estas credenciales se conceden durante un período limitado de tiempo por el que el usuario puede tener que pagar.

Transcurrido este tiempo, el usuario deberá volver a pagar para mantener su acceso a la red.

Para que esto funcione, el usuario llega a acceder a un punto de acceso, obtiene una dirección IP por DHCP y navega hasta el portal que le cautiva, que no le deja hacer nada más mientras no se autentique.

Por lo tanto, este sistema de autenticación y control del tráfico de la red funciona a nivel de aplicación por encima del IEEE 802.11

7.2. Cifrado

El cifrado es el procedimiento mediante el cual se protege la información transmitida para que no pueda ser interpretada por aquellas personas que no son sus destinatarias.

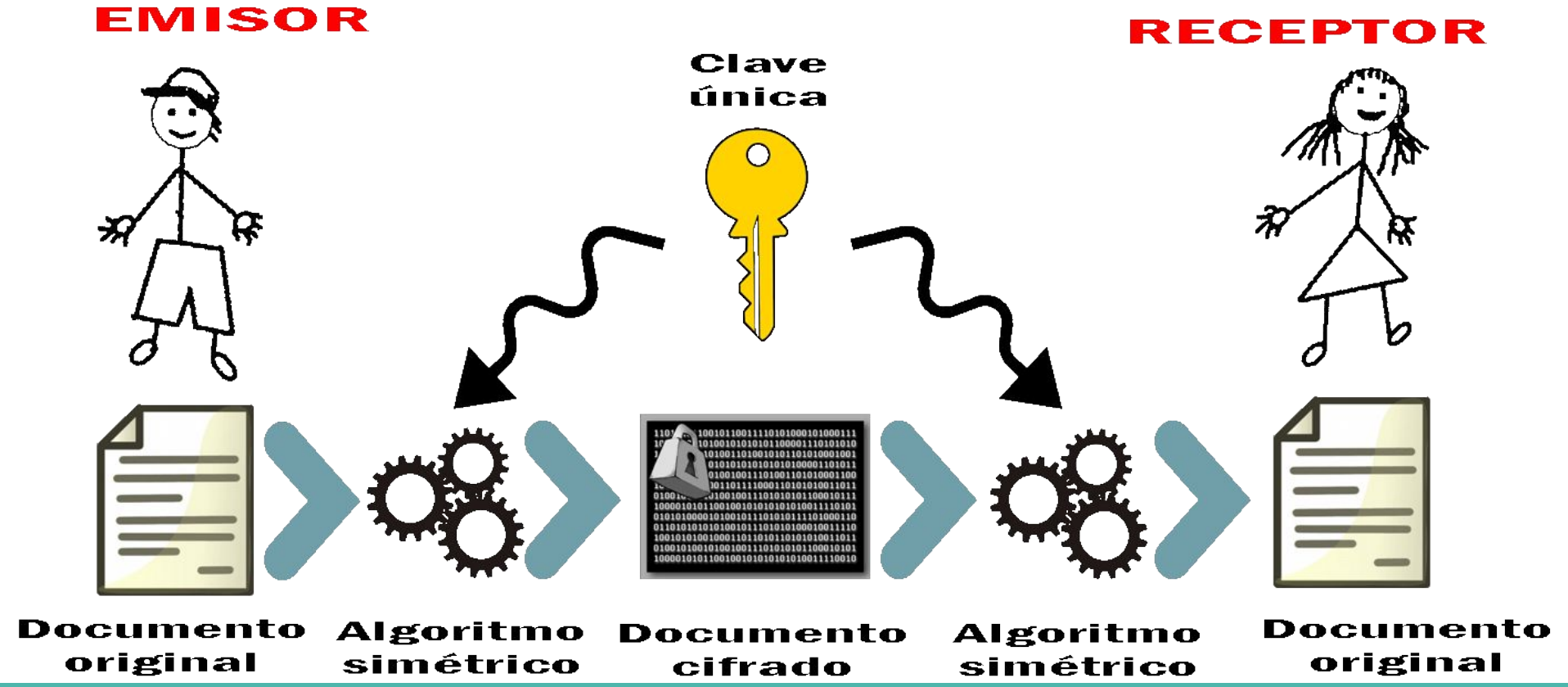
La forma de proteger la información es estableciendo unos códigos que solo conocen el emisor y el receptor de la información.

El cifrado protege la información que viaja por la red.

Aunque no se puede impedir la captura de la información, si se puede evitar que la puedan interpretar aquellas personas no autorizadas a hacerlo.

7.2. Cifrado

El cifrado que se utiliza para proteger la información en los enlaces inalámbricos IEEE 802.11 es un cifrado de clave simétrica, es decir, se utiliza la misma clave para cifrar que para descifrar el mensaje.



7.2. Cifrado

— **Cifrado de clave estática:** es aquel en que la clave no cambia. Fue el primero utilizado en las redes IEEE 802.11 en su algoritmo de seguridad WEP, pero, como veremos más adelante, presenta graves problemas de seguridad, ya que al no cambiarla clave es fácil descifrarla en un tiempo relativamente breve.

— **Cifrado de clave dinámica:** es aquel en que la clave va cambiando de forma automática cada cierto tiempo. El tiempo de cambio, además, es mucho menor al que se requeriría para descifrar la clave. De esta forma se solucionan la mayoría de los problemas del cifrado de clave estática.

Son ejemplos de cifrado de clave dinámica los algoritmos TKIP y AES.

7.2.1. Cifrado WEP

El estándar original IEEE 802.11 de 1997 incorporaba un procedimiento de seguridad llamado WEP *(Wired Equivalent Privacy* o privacidad equivalente a la del cable).

Este procedimiento se basa en la utilización de un algoritmo de cifrado de clave estática combinado con un método de autenticación de **clave compartida**, donde **la clave de autenticación es la misma que la de cifrado**.

La clave la establece el administrador de la red al configurarla y los usuarios para poder conectarse ella deben conocerla e introducirla manualmente en los parámetros de conexión a la red de sus dispositivos.

7.2.1. Cifrado WEP

El estándar define tres niveles de seguridad basándose en la longitud de la clave: a mayor longitud, mayor seguridad.

Las claves pueden ser de 40, 104 o 232 bits, aunque a menudo se expresan en hexadecimal (10, 26 o 48 dígitos). Las claves deben tener exactamente la longitud indicada, ni un dígito más ni uno menos.

Pero no tardaron mucho en surgir algoritmos y programas que logran descodificar las claves WEP en un tiempo más que asequible a través del análisis de grandes volúmenes de tráfico inalámbrico.

Hoy en día el método WEP es completamente inseguro y su uso para proteger una red WiFi está totalmente desaconsejado.

7.2.2. WPA y WPA2

Tras el fracaso del WEP se creó un nuevo estándar de seguridad llamado WPA *(WiFi Protected Access* o acceso WiFi protegido) que incorpora mejoras como el uso del protocolo de cifrado de claves dinámicas TKIP *(temporal key integrity protocol* o protocolo de integridad de claves temporales) y el sistema de autenticación IEEE 802.1x en las redes empresariales (ya visto).

El TKIP es mucho más seguro porque cambia constantemente las claves de encriptación.

Posteriormente se introducía un nuevo algoritmo de cifrado de claves dinámicas llamado AES (*Advanced Encryption System* o sistema de encriptación avanzado), más seguro aún que el TKIP.

7.2.2. WPA y WPA2

WPA2 es en realidad una especie de versión definitiva del WPA.

Como era tan urgente crear un nuevo protocolo que fuera mejor que el WEP, los fabricantes crearon el WPA de manera poco coordinada e incompleta.

WPA2 es el estándar completo, el que incluye todos los mecanismos de seguridad y el que se debería utilizar siempre que no tengamos que integrar en la WiFi dispositivos que sólo soporten WPA.

Para resumir, podemos establecer esta serie de combinaciones de autenticación y cifrado:

7.2.2. WPA y WPA2

Denominación	Autenticación	Cifrado	Seguridad
WEP	Clave compartida	RC4 (obsoleto)	
WPA-PSK (TKIP)	Clave compartida (EAP)	TKIP	
WPA-PSK (AES)	Clave compartida (EAP)	AES	
WPA2-PSK (TKIP)	Clave compartida (EAP)	TKIP	
WPA2-PSK (AES)	Clave compartida (EAP)	AES	
WPA2-Empresarial	IEEE 802.11i (RADIUS)	AES/CCMP	

8. Planificación celular de las WLANs

La planificación celular hace referencia a la ubicación física que daremos a cada uno de los puntos de acceso de la(s) WLAN, así como a los canales que utilizarán cada uno de ellos.

Solapamiento de canales

Al instalar un punto de acceso es importante que su zona de cobertura no se solape con la zona de cobertura de otro punto de acceso, ya que se interferirían.

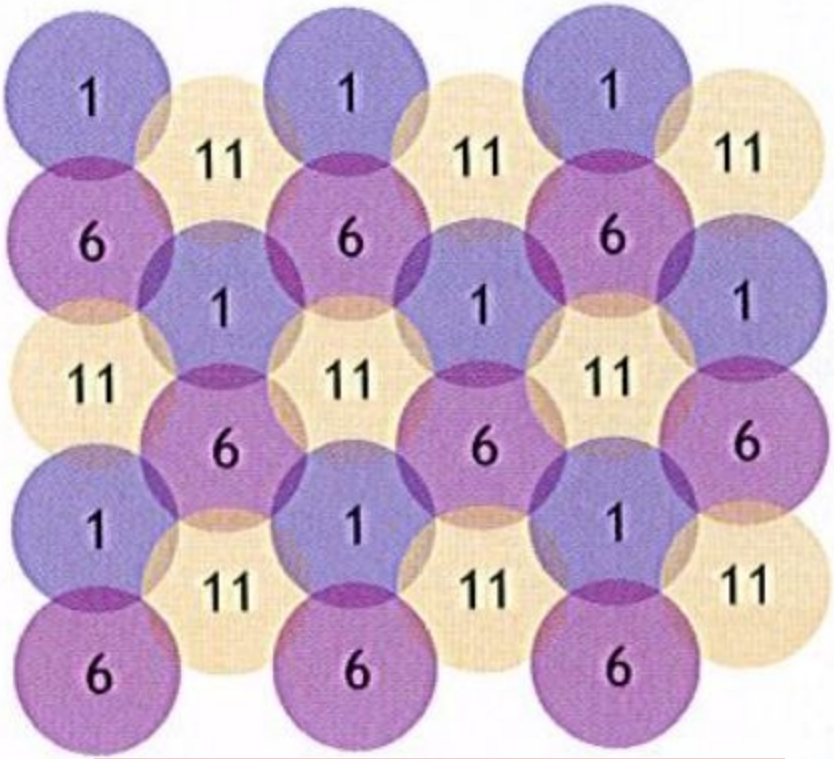
Distribución de canales y celdas para evitar interferencias

Para dar cobertura con una misma WLAN a toda una planta de un edificio, lo más importante a tener en cuenta es que cada celda tenga asignado un canal que no interfiera con el de sus celdas adyacentes.

8. Planificación celular de las WLANs

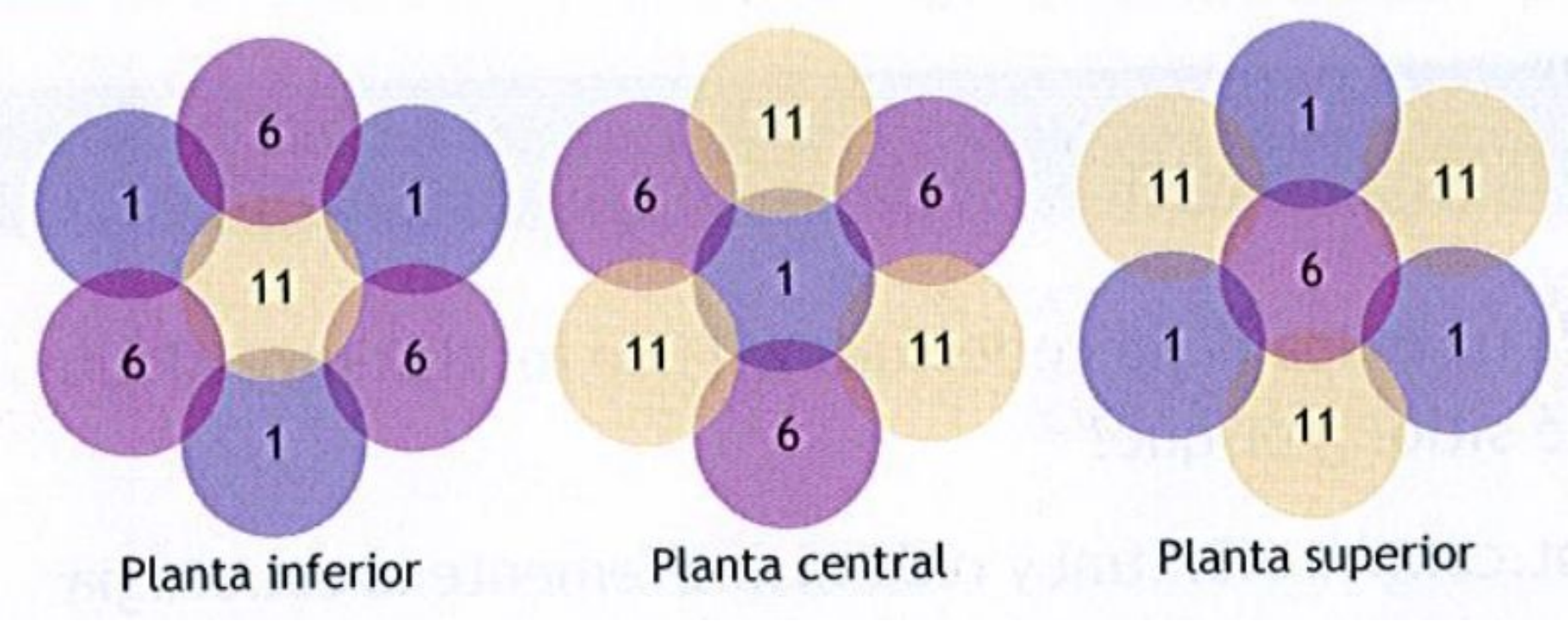
Como ya vimos los canales de la banda de 2,4GHz que no se solapan son el 1, el 6 y el 11. El 14 tampoco se solaparía, pero no es legal utilizarlo en España.

Cuando queremos dar cobertura a más de una planta de un mismo edificio, tendremos que tener cuidado para que las celdas de una planta determinada no interfieran con las de las plantas superior e inferior.



Posible distribución de canales para evitar interferencias en una planta.

8. Planificación celular de las WLANs



Posible distribución de canales y celdas para evitar interferencias entre varias plantas.

8. Planificación celular de las WLANs

Uso de antenas sectoriales y direccionales

En algunos casos nos puede interesar el uso de antenas sectoriales o direccionales para lograr un mayor alcance en una región concreta del espacio.

Ubicación de los puntos de acceso

Se deben tener en cuenta los siguientes aspectos:

— Las paredes de hormigón o ladrillo reducen notablemente la cobertura de los puntos de acceso. Las paredes de cartón yeso (como el pladur), madera o cristal son más permeables.

8. Planificación celular de las WLANs

— Se debe evitar, la presencia de dispositivos que utilicen la banda de frecuencias de 2,4 GHz, como microondas, dispositivos bluetooth, etc.

— Se deben ubicar en lugares elevados a fin de evitar la interferencia generada por el movimiento de las personas o por la presencia de obstáculos diversos (muebles, sillas, electrodomésticos, aparatos electrónicos, etc.).

— En aquellos lugares donde sea difícil hacer llegar el suministro eléctrico, puede considerarse la opción de proporcionar la electricidad directamente a través del propio cableado UTP (**POE**).

8. Planificación celular de las WLANs

— Es aconsejable, antes de fijar el AP, realizar medidas de la señal que se obtiene al situarlo en un determinado punto e ir reubicándolo hasta obtener la mejor.

Existen diferentes programas para realizar estas medidas. Estas aplicaciones reciben el nombre de *site survey tools.* Kismet, NetStumbler, Vistumbler o WiFi Analyzer serían buenos ejemplos.

— Se recomienda aprovechar las medidas anteriores para generar planos de la cobertura WiFi de cada AP, ya que nos pueden ser útiles para detectar zonas de poca cobertura o con solapamientos.

8. Planificación celular de las WLANs

Modos de funcionamiento de los AP

Los AP suelen soportar distintos modos de funcionamiento:

— **Modo raíz:** es el modo de funcionamiento habitual.

El AP publica un BSS, que puede pertenecer a un ESS más amplio, al que pueden conectarse los dispositivos inalámbricos al alcance.

Cuando varios AP operan de este modo en una misma zona, deberán utilizar canales diferentes para no interferirse.

Este es el modo que se utiliza en las redes WiFi con *roaming* (el ***roaming*** es la capacidad de desplazarse sin perder cobertura entre las celdas de una WiFi).

8. Planificación celular de las WLANs

Modos de funcionamiento de los AP

— **Modo puente inalámbrico:** el AP no publica un BSSID sino que se conecta a uno ya existente de otro AP para hacer de puente entre la red cableada a la que está conectado por cable y la red a la que está conectado inalámbricamente.

— **Modo repetidor:** de este modo el AP tampoco publica un BSSID, sino que se conecta a uno ya existente de otro AP y repite todos los mensajes que le llegan que pertenecen a ese BSS.

Los repetidores permiten ahorrar costes en cableado, ya que no es necesario hacer llegar la red cableada hasta ellos.

9. Instalación y configuración de los AP

Instalación

En la instalación de estos dispositivos hay que tener en cuenta que se les debe hacer llegar tanto la red cableada como la alimentación eléctrica.

Hay que recordar que podemos hacer llegar la alimentación eléctrica a través del propio cable Ethernet utilizando en un extremo un adaptador POE, para la entrada de corriente eléctrica al cable de red, y en el otro un AP con tecnología POE, o bien un separador o splitter POE que separe la red de la corriente antes de llegar al AP.

9. Instalación y configuración de los AP

Configuración

Los AP suelen ser elementos de la red configurables a través de un pequeño servidor web accesible en su IP. Suele tener un login con usuario y contraseña (que debe cambiarse y no dejar la que viene de fábrica, como es lógico por seguridad)

Los AP vienen configurados con una dirección IP y una máscara por defecto que suelen indicarse en la documentación técnica del AP.

9. Instalación y configuración de los AP

Configuración por WPS

El WPS (WiFi protected setup) es un estándar creado por la WiFi Alliance que permite la configuración automática de los parámetros de acceso a las redes WiFi.

Mediante este estándar, el AP y el dispositivo a conectar intercambian una serie de mensajes previos a la asociación que permiten autenticar y autoconfigurar el dispositivo con todos los parámetros de la red, incluyendo las claves compartidas.

Hay cuatro métodos básicos de configuración:

9. Instalación y configuración de los AP

— PBC *(push button configuration):* este método se basa en la existencia de un botón especial en el AP que al ser pulsado permite que se asocie automáticamente un dispositivo que está a la espera de establecer una conexión.

9. Instalación y configuración de los AP

— PIN *(personal identification number):* en este caso debe introducirse en el dispositivo que desea conectarse al AP un número secreto (el PIN), que previamente se ha configurado en el AP.

— NFC *(near field communications):* los dispositivos más cercanos al AP se autoconfiguran y asocian automáticamente.

— USB (universal serial bus): utiliza un lápiz USB para transferir los datos de acceso desde el AP hasta el dispositivo a conectar.