REDES LOCALES

TEMA 7

REDES LOCALES INALÁMBRICAS

- ✗ Decidir cuándo es necesario instalar una red inalámbrica.
- ✗ Definir los estándares de las redes inalámbricas.
- ✗ Identificar la arquitectura de las WLAN.
- ✗ Enumerar los cifrados de comunicación de los dispositivos inalámbricos.
- ✗ Tomar conciencia de la importancia de la seguridad en las redes inalámbricas.
- ✗ Planificar e instalar redes inalámbricas locales.
- ✗ Enumerar los diferentes dispositivos inalámbricos.

Contenidos

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, tablets o móviles; la improvisación de una red para una feria, congreso o incluso en una situación de emergencia o catástrofe; o la dotación de acceso a Internet a cuantos usuarios lo requieran en una biblioteca, cafetería, hotel, aeropuerto, plaza, etc. En estos casos será necesario el uso de tecnologías de red inalámbricas.

Hasta no hace mucho, 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 los dispositivos se produce mediante ondas electromagnéticas.

1.1. Clasificación.

Las redes inalámbricas se extienden a todos los ámbitos de las redes, desde el personal hasta el más extenso o mundial. Según el **alcance** las redes inalámbricas se clasifican en:

- **Redes inalámbricas de ámbito personal (WPAN):** interconectan dispositivos en el entorno más próximo de un usuario (pocos metros). Tecnologías: bluetooth e infrarrojos (IrDA).
- **Redes inalámbricas de ámbito local (WLAN):** interconectan dispositivos en un local, piso, planta, edificio o campus. Tecnologías: WiFi.
- **Redes inalámbricas de ámbito metropolitano (WMAN):** interconectan dispositivos y redes en un barrio, pueblo o ciudad. Tecnología: WiMax.
- **Redes inalámbricas de ámbito extenso (WWAN):** interconectan dispositivos y redes en toda una región, país o conjunto de países. Tecnología: UMTS, GPRS, 3G, 4G,…

En este tema nos centraremos en las redes inalámbricas de ámbito local, atendiendo a sus características, dispositivos asociados y opciones de configuración más frecuentes para garantizar un buen funcionamiento y su seguridad.

2. Introducción a las WLAN.

A continuación, veremos las principales características de las WLAN, así como sus principales ventajas e inconvenientes.

2.1. Características.

Las principales características de las WLAN son las siguientes:

- **Naturaleza de la señal:** las redes inalámbricas utilizan señales electromagnéticas para transmitir datos.

- **Medio o canal:** las redes inalámbricas no utilizan cables de ningún tipo, sino que las señales se propagan por el espacio y son capaces de atravesar una gran variedad de materiales.

- **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 onda**, la **potencia de la emisión**, la tecnología de **modulación** y el tipo y **sensibilidad** de las antenas determinarán el alcance (o **cobertura**) de los dispositivos de la red.

- **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, solo 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, ya que en una

zona y WLAN determinadas, hasta que no finaliza una transmisión, no se puede iniciar otra.

Otros factores que influyen en la velocidad son el ruido, las interferencias y las pérdidas de intensidad, ya que si son intensas las señales que se envían son más robustas, pero ocupan mayor espacio y, por tanto, la velocidad de transmisión disminuye.

- **Movilidad:** las WLAN permiten la existencia de dispositivos móviles. Como no necesitan cables, los dispositivos no están obligados a permanecer en una zona concreta, por lo que pueden moverse libremente por toda la zona de cobertura de la WLAN.

- **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 básicos (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 las 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.

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 hub. Esto no ocurre en las redes cableadas basadas en switches.

- 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.

2.3. Situación actual de las WLAN.

Hoy en día encontramos WLAN en casi todas las partes: en nuestros hogares, en oficinas, en centros educativos, en hoteles, etc. También existen proyectos para compartir el acceso a Internet en espacios públicos como calles, plazas, etc. En algunas ciudades se pretende dotar de puntos de acceso inalámbrico a cada uno de los

semáforos de la ciudad. Pero también hay iniciativas privadas, como Fon, que permite que los usuarios particulares puedan compartir su conexión a Internet a través de su WiFi. Existe, sin embargo, una polémica legal respecto a Fon y proyectos similares surgida de que, actualmente, en algunos países como España no es legar compartir la conexión a Internet a través de WiFi fuera del domicilio concreto para el que el particular o empresa ha contratado ellos servicios del ISP, salvo que el contrato firmado con el ISP así lo permita o que el titular del contrato se registre como un operador de telecomunicaciones y pague los correspondientes gravámenes de la CMT (Comisión de Mercado de Telecomunicaciones).

Práctica 1

3. Estándares WLAN.

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

3.1. Estándares IEEE 802.11

El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) desarrolla y publica especificaciones y estándares para las redes locales inalámbricas en su sección 802.11. Los estándares tecnológicos más importantes de esta familia se resumen en la siguiente tabla:

TABLE 1: IEEE 802.11 COMMON WIFI STANDARDS BREAKDOWN

Standard	Frequency Band	Bandwidth	Modulation Scheme	Channel Arch.	Maximum Data Rate	Range	Max Transmit Power
802.11	2.4 GHz	20 MHz	BPSK to 256-QAM	DSSS, FHSS	2 Mbps	20 m	100 mW
b	2.4 GHz	21 MHz	BPSK to 256-QAM	CCK, DSSS	11 Mbps	35 m	100 mW
a	5 GHz	22 MHz	BPSK to 256-QAM	OFDM	54 Mbps	35 m	100 mW
g	2.4 GHz	23 MHz	BPSK to 256-QAM	DSSS, OFDM	54 Mbps	70 m	100 mW
n	2.4 GHz, 5 GHz	24 MHz and 40 MHz	BPSK to 256-QAM	OFDM	600 Mbps	70 m	100 mW
ac	5 GHz	20, 40, 80, 80+80= 160 MHz	BPSK to 256-QAM	OFDM	6.93 Gbps	35 m	160 mW
ad	60 GHz	2.16 GHz	BPSK to 64-QAM	SC, OFDM	6.76 Gbps	10 m	10 mW
af	54-790 MHz	6, 7, and 8 MHz	BPSK to 256-QAM	SC, OFDM	26.7 Mbps	>1km ?	100 mW
ah	900 MHz	1, 2, 4, 8, and 16 MHz	BPSK to 256-QAM	SC, OFDM	40 Mbps	1 km	100 mW

3.2. 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.

3.3. 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 WiFi 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. Arquitectura IEEE 802.11

El estándar IEEE 802.11 define una arquitectura de red que establece las bases del 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 o **PHY** y la de control de acceso al medio o **MAC**. Estas capas regulan los aspectos de las capas físicas y de enlace, respectivamente, de la pila de protocolos OSI.

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

4.1. Componentes físicos: las estaciones (STA).

Una estación (STA) es cualquier dispositivo que implementa el estándar IEEE 802.11. Puede referirse a un ordenador, un portátil, un dispositivo móvil, un punto de acceso, un dispositivo multifunción, etc.

Las estaciones utilizan **adaptadores de red inalámbricos** para conectarse a la WLAN, como tarjetas o adaptadores USB.

Unos tipos especiales de estaciones son los puntos de acceso inalámbricos y los dispositivos multifunción.

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.

Las principales **funciones de los AP** son las siguientes:

- Publicar una WLAN: un punto de acceso publica una WLAN para que pueda conectarse a ella el resto de estaciones.

- Definir los parámetros de acceso a la WLAN: cualquier estación que desee conectarse a la WLAN mediante el AP deberá conocer los parámetros de acceso a ella.

- Ejercer de puente entre los dispositivos inalámbricos y la red cableada: las estaciones conectadas a la WLAN a través del AP podrán acceder a los recursos de la LAN según se les haya autorizado dentro de la misma.

- Ejercer de intermediario en el proceso de comunicación: cuando un dispositivo de la WLAN quiere enviar información a otro de la WLAN o de la LAN, envía la información al AP y este 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.

Dispositivos multifunción.

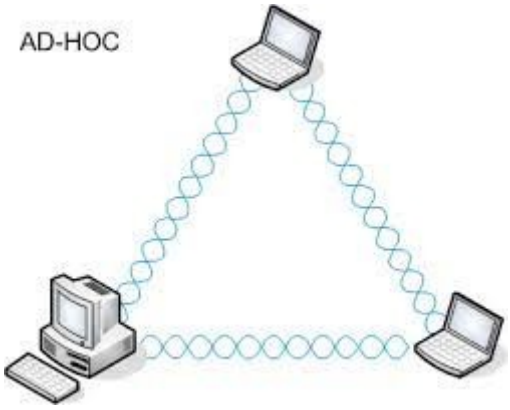
Las WLAN domésticas y de las pymes no suelen tener una extensión demasiado grande y generalmente es un único punto de acceso el que da cobertura a toda la casa o empresa. Los ISP suelen ofrecer a sus clientes dispositivos que integran en su interior las funciones de router, switch, módem y punto de acceso: son los dispositivos multifunción.

4.2. Modos de operación y tipos de redes.

El estándar IEEE 802.11 define dos modos de operación para las estaciones: *ad hoc* y en infraestructura. A su vez, estos modos definen dos tipos de redes totalmente distintas.

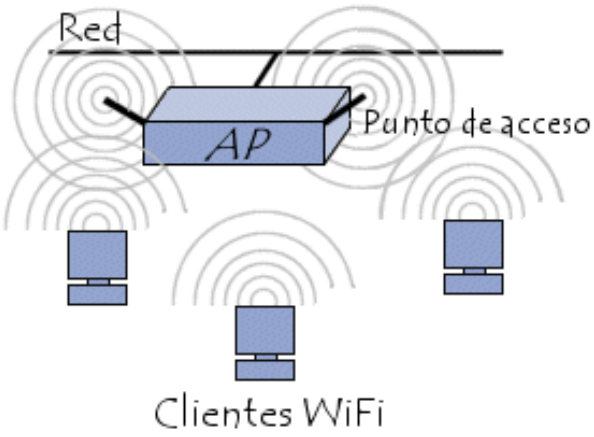
Redes *ad hoc.*

Las redes *ad hoc* son aquellas donde diferentes estaciones establecen enlaces inalámbricos directos entre sí para comunicarse mutuamente. Estas redes se suelen crear y utilizar de forma puntual, cuando dos o más usuarios se encuentran fortuitamente y quieren compartir algún recurso en un momento dado.



Redes en infraestructura.

Las redes en infraestructura son aquellas donde las distintas estaciones se conectan a la WLAN a través de un AP. En zonas muy amplias, pueden existir varios AP para una misma WLAN.



4.3. Componentes lógicos.

Conjunto básico de servicios (BSS).

El término *conjunto básico de servicios (BSS)* hace referencia al conjunto de estaciones (STA) enlazadas entre sí mediante una conexión inalámbrica y al conjunto de servicios que comparten, como el método de codificación de la información, la forma de autenticarse, el modo de cifrar los datos, etc. El BSS es el bloque básico de construcción de las WLAN 802.11.

BSS independientes (IBSS).

Un BSS independiente (IBSS) lo forma un conjunto de estaciones que se interconectan entre sí directamente, de igual a igual. Se trata del BSS formado por las redes *ad hoc*.

BSS en las redes en infraestructura.

En las redes en infraestructura los BSS los crean y definen los propios AP. El resto de estaciones se asocian a él para beneficiarse de sus servicios.

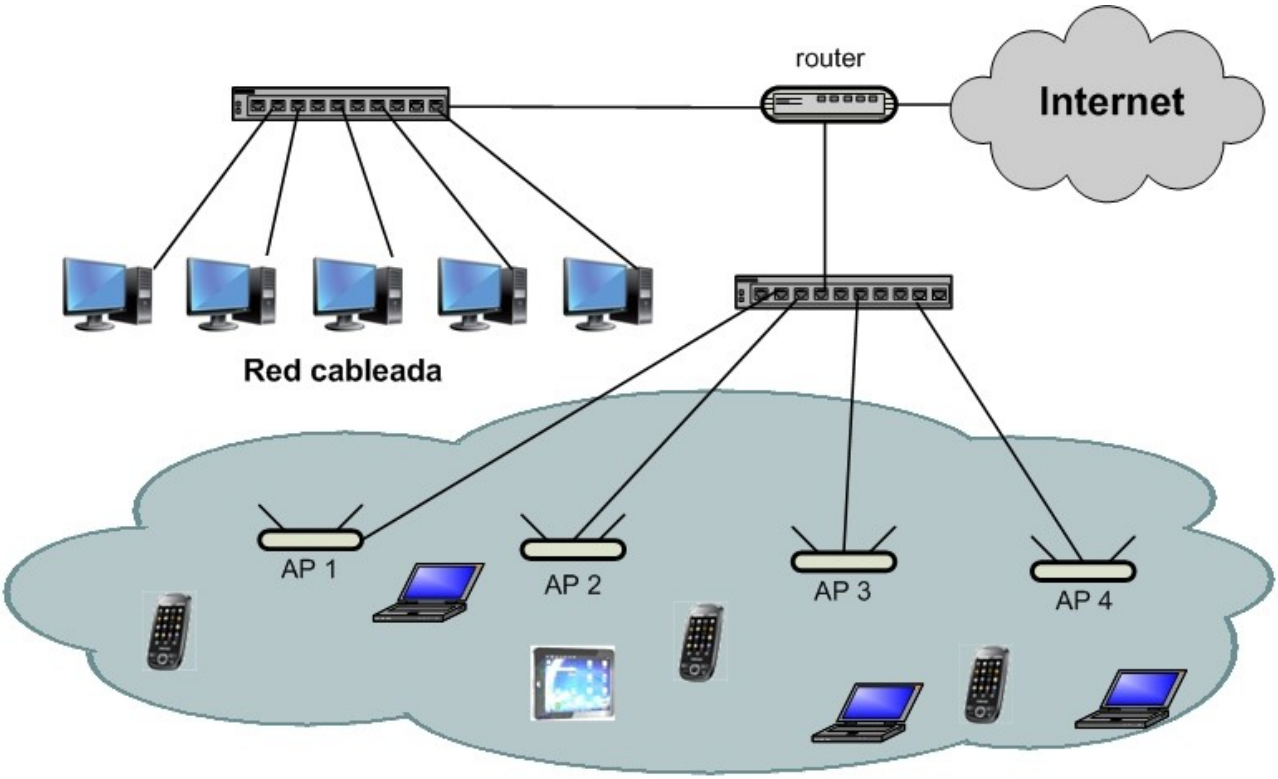
Identificador del BSS (BSSID).

Cada conjunto básico de servicios posee un identificador único en la red local: el BSSID, que es un número binario de 48 bits. En las redes en infraestructura el BSSID es la dirección MAC del AP. En las redes *ad hoc*, el BSSID es un número generado al azar.

Conjunto extendido de servicios (ESS).

Cuando la extensión a cubrir por la red inalámbrica en infraestructura es muy amplia, es necesario instalar más de un AP para dar cobertura a toda la zona. En este caso, aunque cada AP tendrá su propio BSS, pueden configurarse para ofrecer un servicio

común y presentarse todos ellos como una misma WLAN. En este caso los distintos BSS forman un conjunto extendido de servicios (ESS).



Sistema de distribución.

El sistema de distribución (DS) es aquel que permite interconectar los diversos BSS que forma una red local inalámbrica para formar un ESS. Generalmente hace referencia a la red local cableada.

Nombre de la WLAN (SSID).

Toda red inalámbrica, ya sea *ad hoc* o en infraestructura, con un único AP o con múltiples AP, tiene un nombre que la identifica: el identificador del conjunto de servicios (SSID).

El SSID es el 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.

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

Práctica 3

5. Subcapa PHY.

En los estándares IEEE 802.11 se distingue entre la capa física (PHY) y la capa de control de acceso al medio (MAC).

5.1. Señales electromagnéticas.

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

Una onda electromagnética altera los campos eléctrico y magnético a su alrededor haciéndolos crecer y decrecer en intensidad de forma periódica y tiene las siguientes **propiedades**:

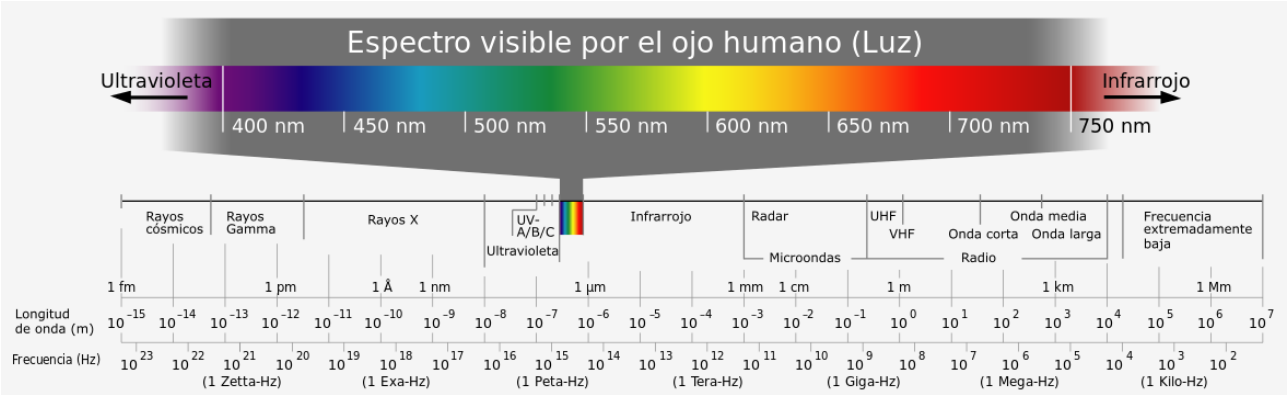
- **Frecuencia (F):** número de ciclos o perturbaciones completas por unidad de tiempo. Se mide en hercios (Hz) o sus derivados (MHz, KHz, GHz). Un hercio corresponde a un ciclo por segundo.

- **Longitud de onda (λ):** distancia que es capaz de recorrer la onda en el vacío en un ciclo o perturbación completa. La velocidad de las ondas electromagnéticas en el vacío es la misma para todos los tipos de onda, como por ejemplo, la de la luz. Por consiguiente, a mayor frecuencia, menor longitud de onda y viceversa.

- **Energía (E):** la energía asociada a una onda electromagnética depende de la frecuencia. A mayor frecuencia, mayor energía.

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*. La siguiente figura resume los distintos tipos de radiación electromagnética que existen y el nombre que reciben:



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.

Estas organizaciones dividen el espectro electromagnético en rangos de frecuencias, a los que llama ***bandas***. Cada banda, a su vez, se puede dividir en más bandas, según lo 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.

5.4. Las bandas ISM.

En general, para poder emitir una determinada frecuencia hace falta disponer de una licencia. Sin embargo, la regulación internacional define en el espectro radioeléctrico un conjunto de bandas para usos industriales, científicos y médicos llamadas **bandas ISM** *(industrial, cientific and medical)* de entre las cuales cada país puede reservar una parte para su uso sin licencia, siempre y cuando no se superen los niveles de potencia delimitados.

Las WLAN utilizan las siguientes bandas ISM para operar (si la legislación del país lo permite):

Estándares IEEE 802.11	Banda ISM
Legacy (original), b y g	2,4 GHz
a	5,7 GHz
n	2,4 GHz + 5,7 GHz

5.5. 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 milésima parte de un vatio) o decibelios respecto a un milivatio (dBm).

La potencia permite combatir los efectos de la atenuación, la dispersión, el ruido y algunas de las interferencias, de modo que determina el alcance de la antena: a mayor potencia, mayor será su alcance. Sin embargo, es importante recordar que en cada país existe una potencia máxima de emisión para las bandas ISM.

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.

Práctica 4

5.6. 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 la intensidad de la señal a lo largo de su recorrido. La permeabilidad de cada material para la radiación electromagnética es distinta en función del tipo de onda y del propio material. Las ondas de las WLAN atraviesan mejor el aire que la madera, mejor la madera que los ladrillos y mejor los ladrillos que los cementos.

5.7. Interferencias y ruido.

Se denomina interferencia a cualquier perturbación electromagnética no deseada que afecta a la señal electromagnética en transmisión, a su emisión o a su recepción.

A niveles 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.

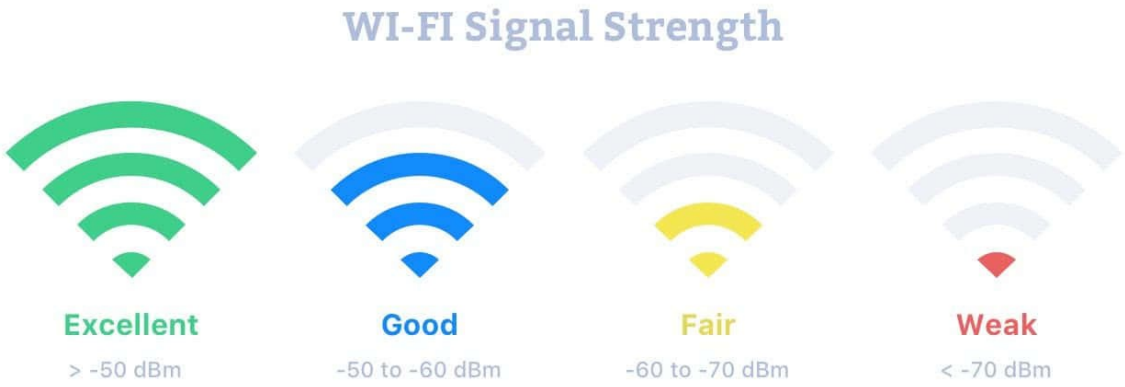
Existe una radiación electromagnética de base, generalmente de poca intensidad, que es inevitable y su comportamiento es totalmente aleatorio e imprevisible. A este tipo de interferencias se las conoce como **ruido**.

5.8. 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. Sin embargo, lo más importante no es el RSSI, sino que la potencia recibida sea suficientemente mayor que el ruido ambiental.

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

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.



Práctica 5

5.9. 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.

5.10. Velocidad de transmisión.

Cuando dos dispositivos inalámbricos quieren intercambiar información entre ellos, deben negociar en primer lugar qué tipo de modulación van a utilizar. La modulación determinará la velocidad y robustez de la trasmisión.

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

IEEE Standard	Year Adopted	Frequency	Max. Data Rate	Max. Range
802.11a	1999	5 GHz	54 Mbps	400 ft.
802.11b	1999	2.4 GHz	11 Mbps	450 ft.
802.11g	2003	2.4 GHz	54 Mbps	450 ft.
802.11n	2009	2.4/5 GHz	600 Mbps	825 ft.
802.11ac	2014	5 GHz	1 Gbps	1,000 ft.
802.11ac Wave 2	2015	5 GHz	3.47 Gbps	10 m.
802.11ad	2016	60 GHz	7 Gbps	30 ft.
802.11af	2014	2.4/5 GHz	26.7 Mbps – 568.9 Mbps (depending on channel)	1,000 m.
802.11ah	2016	2.4/5 GHz	347 Mbps	1,000 m.
802.11ax	2019 (expected)	2.4/5 GHz	10 Gbps	1,000 ft.
802.11ay	late 2019 (expected)	60 GHz	100 Gbps	300-500 m.
802.11az	2021 (expected)	60 GHz	Device tracking refresh rate 0.1-0.5 Hz	Accuracy <1m to <0.1m

5.11. Canales.

Ya sabemos que las redes WiFi operan en las bandas ISM de 2,4 GHz y 5 GHz, 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.

Redes WiFi b y g

Los estándares IEEE 802.11 b y g utilizan frecuencias dentro de la banda ISM de 2,4 GHz y necesitan un ancho de banda de 22 MHz para funcionar. El IEEE ha definido 13 canales consecutivos en el rango de frecuencias de 2,401 GHz a 2,483 GHz, separados entre sí por 5 MHz, así como un canal superior con centro en los 2,484 GHz.

Identificador de Canal	Frecuencia en MHz	Dominios Reguladores				
		América (-A)	EMEA (-E)	Israel (-I)	China (-C)	Japón (-J)
1	2412	×	×	—		×
2	2417	×	×	—	×	×
3	2422	×	×	×	×	×
4	2427	×	×	×	×	×
5	2432	×	×	×	×	×
6	2437	×	×	×	×	×
7	2442	×	×	×	×	×
8	2447	×	×	×	×	×
9	2452	×	×	×	×	×
10	2457	×	×	—	×	×
11	2462	×	×	—	×	×
12	2467	—	×	—	—	×
13	2472	—	×	—	—	×
14	2484	—	—	—	—	×

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

Como se puede observar, los diferentes canales se encuentran solapados entre sí. Cuando dos redes distintas operan en canales solapados, su rendimiento disminuye considerablemente.

Cuando deben coexistir diferentes redes WiFi en una misma zona, es importante tener en cuenta los canales a utilizar. Se deben elegir siempre canales sin solapamiento.

Así pues, si una red WiFi g opera en el canal 1, la siguiente deberá operar en el 6, la siguiente en el 11 y la siguiente aún podría operar en el 14, siempre y cuando estos canales sean de uso público en nuestro país.

Los 14 canales no están disponibles en todos los países, sino que cada país determina qué canales permite utilizar. La tabla anterior muestra los canales permitidos en algunos países o continentes.

Redes WiFi a

Estas redes operan por canales distribuidos en la banda ISM de 5 GHz, 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 varía en cada país.

Redes WiFi n

Las redes WiFi n pueden operar en la banda ISM de 2,4 GHz, en la de 5 GHz o en las dos a la vez.

Para cada una de estas bandas se utiliza la división en canales definida en los estándares anteriores y hará falta que el administrador de la red determine qué canal utilizar.

Sin embargo, hay una diferencia respecto a los estándares anteriores y es que el ancho de banda que se utiliza en las redes n para la banda de 2,4 GHz es de 40 MHz en lugar de 22 MHz, por lo que la cantidad de canales simultáneos sin solapamiento para estas redes en esta banda es menor.

Práctica 7

6. Subcapa MAC.

En este apartado se detallan las características más importantes de la subcapa de control de acceso al medio (MAC) del estándar IEEE 802.11.

6.1. Direccionamiento físico (dirección MAC).

Cada estación inalámbrica tiene una dirección física 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.

6.2. Publicación del SSID y búsqueda de redes.

Si queremos conectarnos desde un dispositivo inalámbrico a una red inalámbrica o a otro dispositivo inalámbrico, tenemos que tener configurados debidamente los parámetros de conexión a la red (el SSID y los parámetros básicos de acceso que se hayan establecido para la red inalámbrica en cuestión). La publicación del SSID suele estar habilitada por defecto en las redes WiFi.

Generalmente, aquellas estaciones que ofrecen un BSS (los puntos de acceso en las redes en infraestructura o cualquier estación en las redes *ad hoc*) se configuran para hacer pública la presencia de la red junto con sus características básicas de acceso (como son su SSID, tipo, canal, el procedimiento de autenticación, etc). Esta publicación se realiza mediante tramas de gestión específicas.

La funcionalidad anterior se completa con la función de **búsqueda de redes inalámbricas al alcance**, que poseen las mayoría de los dispositivos inalámbricos. Mediante esta función pueden capturar las tramas de gestión que contienen el nombre (SSID) y las características básicas de acceso de todas las redes IEEE 802.11 al alcance del dispositivo y mostrárselas al usuario. Con el listado resultante lo más habitual es que el usuario pueda seleccionar la red a la que desea conectarse y que su programa gestor de conexiones WiFi autoconfigure un perfil de red con las opciones básicas de acceso a la red seleccionada.

6.3. Establecimiento del enlace.

Una vez configurado un perfil de acceso a una red inalámbrica, podremos indicar al dispositivo que inicie una conexión. En ese preciso instante se iniciará un intercambio de tramas de gestión para intentar establecer un enlace entre los dos dispositivos (estación con punto de acceso, en las redes en infraestructura, o estación con estación, en las redes *ad hoc*) que finalizará con la aceptación o el rechazo de este enlace por parte del otro dispositivo. Durante el establecimiento del enlace se producen dos procesos fundamentales: la **sincronización** y la **autenticación**.

Sincronización: consiste en determinar la velocidad de transmisión de datos de la conexión y, por consiguiente, el tipo de modulación y sus parámetros.

Autenticación: es el procedimiento mediante el cual una estación comprueba la identidad de los dispositivos que quieren conectarse a ella y, en función del resultado, autoriza o rechaza el establecimiento del enlace.

6.4. Ocultación del SSID

Aunque el comportamiento por defecto de las estaciones suele ser publicar el SSID de la WLAN ofertada, también se pueden configurar para que no lo publiquen. En ese caso decimos que el SSID está **oculto**.

La ocultación del SSID no es garantía de seguridad. Puede ser útil, aunque nadie podrá ver nuestra red mediante una simple búsqueda de redes disponibles al alcance, sí que es posible detectar su presencia utilizando programas como Acrylic Wi-Fi Professional que permiten detectar el SSID de redes con el SSID oculto.

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 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, el estándar IEEE 802.11 aborda el problema desde dos perspectivas diferentes: 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 y comporta siempre, como mínimo, el envío de una trama de solicitud de autenticación desde el dispositivo que desea conectarse a la red.

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 tanto, todo el mundo podrá conectarse.

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. 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 puedan entrar en la WLAN.

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. Para que la asociación se lleve a término, primero se deberá establecer un enlace con el punto inalámbrico y posteriormente se deberá comprobar si la dirección MAC del dispositivo existe o no en las listas de direcciones MAC autorizadas o no autorizadas.

Los filtros MAC actúan en un segundo nivel, ya que se ejecutan después del establecimiento del enlace con el punto de acceso y, para ello, ya debe haberse establecido un primer mecanismo de autenticación.

IEEE 802.x y el protocolo ampliable de autenticación

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 concretos, 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 o universitarios.

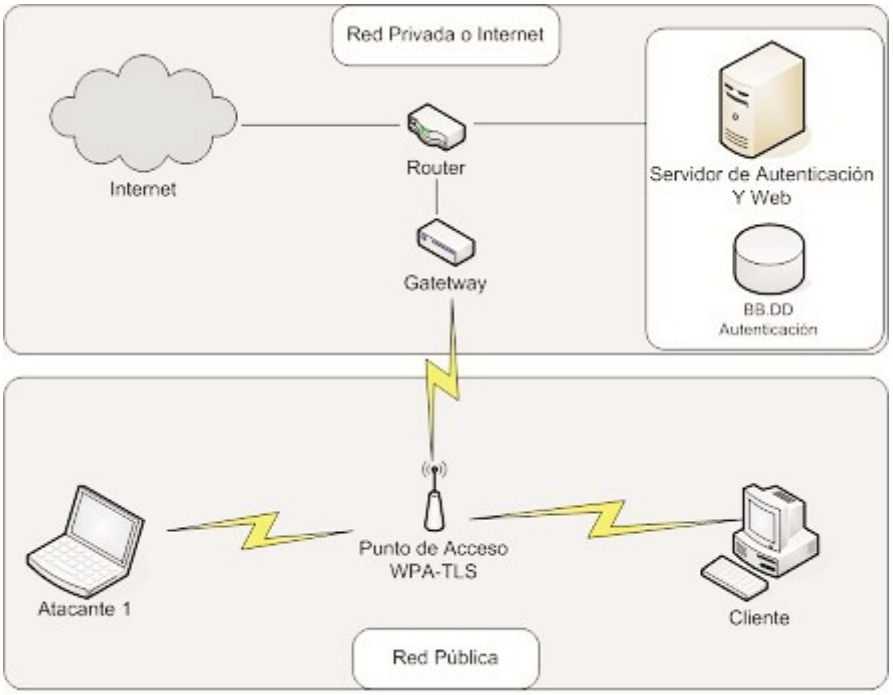
El estándar IEEE 802.x ofrece una solución a este problema, tanto para redes cableadas (IEEE 802.3 o Ethernet) como inalámbricas (IEEE 802.11).

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, independientemente de que además se utilice o no una clave compartida para acceder a la red.

Portales cautivos

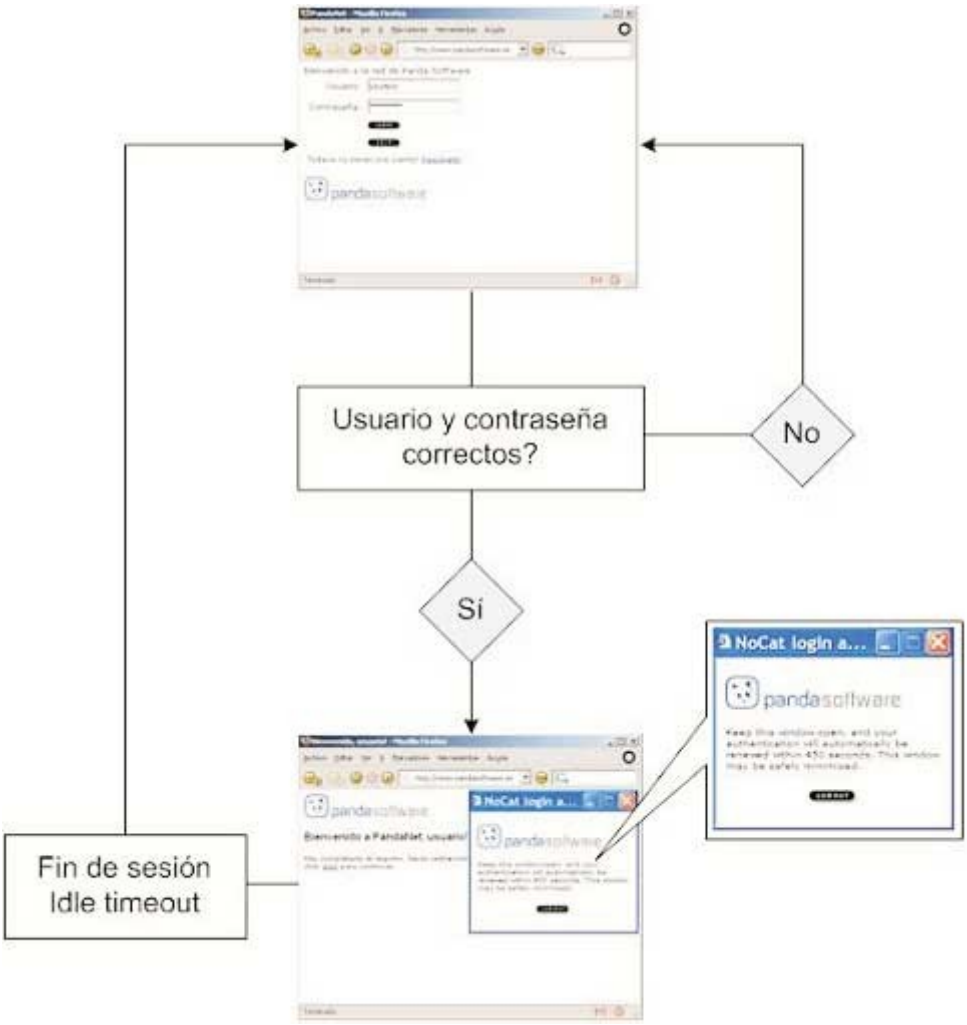
Los portales cautivos regulan el acceso a la red a nivel de aplicación, interceptando todo el tráfico dirigido al protocolo HTTP.

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

Normalmente estas credenciales se conceden durante un tiempo limitado. Transcurrido este tiempo, el usuario tendrá que volver a autenticarse para seguir utilizando la red.



7.2. 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 información, sí se puede evitar que la puedan interpretar aquellas personas no autorizadas para hacerlo.

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. Sin embargo, existen dos métodos de cifrado de clave simétrica con propiedades muy distintas:

- **Cifrado de clave estática:** es aquel que la clave no cambia. Fue el primero en ser usado por las redes IEEE 802.11 en su algoritmo de seguridad WEP, pero como veremos, presenta graves problemas de seguridad, ya que al no cambiar la clave es fácil descifrarla en un tiempo relativamente corto.

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

7.3. El estándar IEEE 802.11i y las certificaciones WPA y WPA2.

A medida que se fueron descubriendo las vulnerabilidades del protocolo WEP (original del IEEE 802.11), el IEEE y los distintos fabricantes empezaron a buscar soluciones más seguras.

Certificación WPA

Mientras el IEEE trabaja en la elaboración de un nuevo estándar de seguridad para las redes inalámbricas,los distintos fabricantes acordaron un estándar intermedio de seguridad llamado WPA *(WiFi protected access* o acceso WiFi protegido) que incorporaba mejoras como el uso del protocolo de cifrado de claves dinámicas TKIP (*protocolo de integridad de claves temporales)* y el sistema de autenticación IEEE 802.11x en las redes empresariales.

Este estándar llegó a la WiFi Alliance y esta decidió emitir certificados WPA a aquellos productos fieles al estándar desarrollado por los fabricantes.

Práctica 9