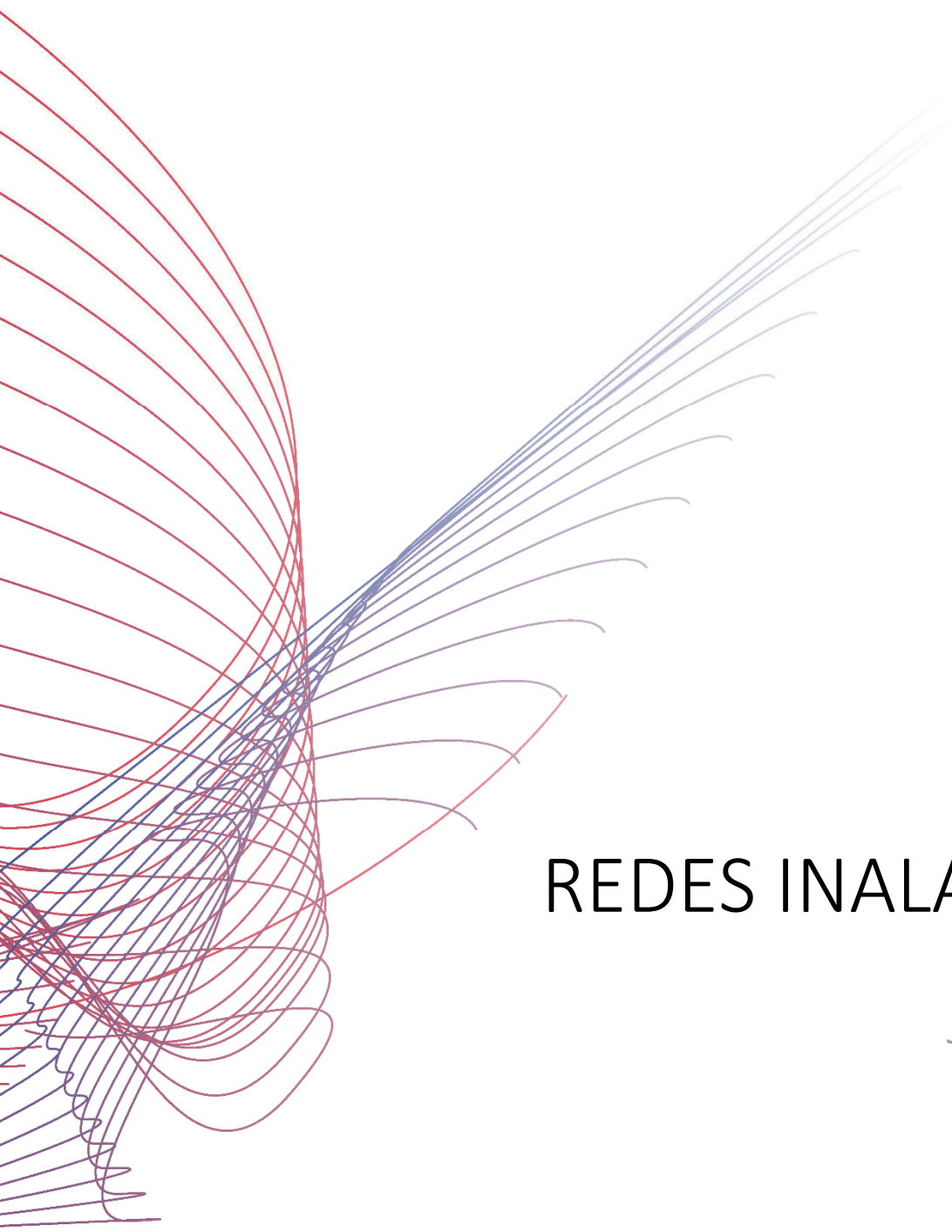
en cs de sk es

TECH pedia



REDES INALÁMBRICAS

JORDI SALAZAR

Título: Redes Inalámbricas
Autor: Jordi Salazar
Publicado por: České vysoké učení technické v Praze
Fakulta elektrotechnická
Dirección de contacto: Technická 2, Praha 6, Czech Republic
Número de teléfono: +420 224352084
Print: (only electronic form)
Número de páginas: 40
Edición: Versión de prueba

TechPedia
European Virtual Learning Platform for
Electrical and Information Engineering

http://www.techpedia.eu

Erasmus+

El presente proyecto ha sido financiado con el apoyo de la Comisión Europea.
Esta publicación (comunicación) es responsabilidad exclusiva de su autor. La Comisión no es responsable del uso que pueda hacerse de la información aquí difundida.

NOTAS EXPLICATIVAS

	Definición
	Interesante
	Nota
	Ejemplo
	Resumen
	Ventajas
	Desventajas

ANOTACIÓN

Este módulo proporciona una introducción a las redes inalámbricas en general y a las redes inalámbricas de área local en particular. Describe y explica lo que son las diferentes tecnologías inalámbricas, sus principales características, problemas de seguridad, ventajas, desventajas y usos o aplicaciones.

OBJETIVOS

Conocer las diferencias de arquitectura existentes en varias redes inalámbricas. Aprender sobre aspectos de seguridad de las redes inalámbricas. Conocer los pros y los contras de las redes inalámbricas.

LITERATURA

[1] William Stallings, Wireless Communications and Networks, Second Edition, Pearson Prentice Hall, Upper Saddle River, NJ, 2005. ISBN 0-13-191835-4.

[2] B. Ciubotaru, G.M. Muntean, *Advanced Network Programming. Principles and Techniques*, Springer-Verlag London, 2013. ISBN 978-1-4471-5292-7.

[3] K. Sharma, N. Dhir, "A study of wireless networks: WLANs, WPANs, WMANs, and WWANs with comparison", *International Journal of Computer Science and Information Technologies*, vol. 5 (6), pp. 7810-7813, 2014.

[4] K. Pothuganti, A. Chitneni, "A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi", *Advance in Electronic and Electric Engineering*, vol. 4 (6), pp. 655-662, 2014.

[5] "An introduction to Wi-Fi", Rabbit product manual, Digi International Inc., 2007-2008. (www.rabbit.com)

[6] IEEE Standards Association web site (http://standards.ieee.org/index.html).

Indice

1 Introducción a las redes inalámbricas

Este módulo proporciona una introducción a las redes inalámbricas en general y a las redes de área local en particular. Describe y explica lo que las diferentes tecnologías inalámbricas son, sus principales características, problemas de seguridad, ventajas, desventajas y usos o aplicaciones.

Las **redes inalámbricas** son redes que utilizan ondas de radio para conectar los dispositivos, sin la necesidad de utilizar cables de ningún tipo.

Los dispositivos que comúnmente utilizan las redes inalámbricas incluyen ordenadores portátiles, ordenadores de escritorio, netbooks, asistentes digitales personales (PDA), teléfonos móviles, tablets y dispositivos localizadores. Las redes inalámbricas funcionan de manera similar a las redes cableadas, sin embargo, las redes inalámbricas deben convertir las señales de información en una forma adecuada para la transmisión a través del medio de aire.

Las redes inalámbricas sirven a muchos propósitos. En algunos casos se utilizan en sustitución a las redes cableadas, mientras que en otros casos se utilizan para proporcionar acceso a datos corporativos desde ubicaciones remotas.

La infraestructura inalámbrica puede ser construida a muy bajo coste en comparación con las alternativas cableadas tradicionales. Pero el ahorro de dinero justifica muy parcialmente la construcción de redes inalámbricas. Si a la gente de una comunidad local se le proporciona un acceso más barato y más fácil a la información, se beneficiarán directamente de lo que Internet tiene para ofrecer. El tiempo y el esfuerzo ahorrado al tener acceso a la red mundial de información se traduce en riqueza a escala local, ya que se puede hacer más trabajo en menos tiempo y con menos esfuerzo.

Las redes inalámbricas permiten a los dispositivos remotos que se conecten sin dificultad, independientemente que estos dispositivos estén a unos metros o a varios kilómetros de distancia. Todo ello sin necesidad de romper paredes para pasar cables o instalar conectores. Esto ha hecho que el uso de esta tecnología sea muy popular, extendiéndose muy rápidamente.

Existen muchas tecnologías diferentes que difieren en la frecuencia de transmisión utilizada, la velocidad y el alcance de sus transmisiones.

Por otro lado, hay algunas cuestiones relacionadas con la regulación legal del espectro electromagnético. Las ondas electromagnéticas se transmiten a través de muchos dispositivos, pero son propensas a la interferencia. Por esta razón, todos los países necesitan regulaciones que definan los rangos de frecuencia y potencia de transmisión permitidos para cada tecnología.

Además, las ondas electromagnéticas no se pueden confinar fácilmente a un área geográfica limitada. Por esta razón, un hacker puede escuchar fácilmente a una red si los datos transmitidos no están codificados. Por lo tanto, se deben tomar todas las medidas necesarias para garantizar la privacidad de los datos transmitidos a través de redes inalámbricas.

2 Tecnologías inalámbricas

Las redes inalámbricas se pueden clasificar en cuatro grupos específicos según el área de aplicación y el alcance de la señal [1-3]: redes inalámbricas de área personal (*Wireless Personal-Area Networks* - WPAN), redes inalámbricas de área local (*Wireless Local-Area Networks* - WLAN), redes inalámbricas de área metropolitana (*Wireless Metropolitan-Area Networks* - WMAN), y redes inalámbricas de área amplia (*Wireless Wide-Area Networks* - WWAN). La Figura 1 ilustra estas cuatro categorías.

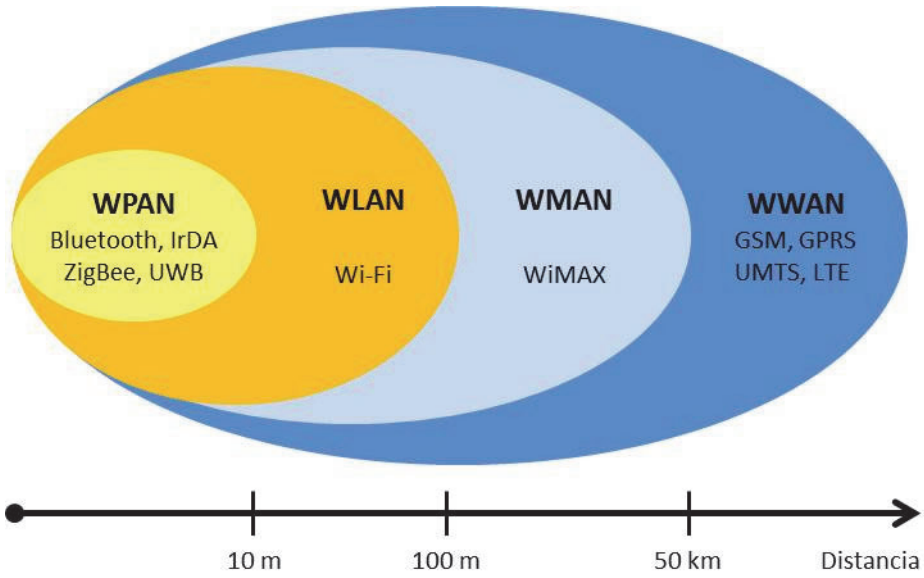


Fig. 1.1 Clasificación de las redes inalámbricas

Además, las redes inalámbricas pueden dividirse también en dos grandes segmentos: de corto y de largo alcance. Inalámbrica de corto alcance se refiere a las redes confinadas en un área limitada. Esto se aplica a las redes de área local (LAN), como edificios corporativos, los campus escolares y universitarios, fábricas o casas, así como a las redes de área personal (PAN) donde los ordenadores portátiles necesitan estar muy cerca entre sí para comunicarse. Estas redes suelen operar sobre un espectro sin licencia y reservado para uso industrial, científica y médica (banda ISM). Las frecuencias disponibles difieren de país a país. Las bandas de frecuencia más comunes son la de 2,4 GHz y la de 5 GHz, que están disponibles en la mayor parte del mundo. La disponibilidad de estas bandas de frecuencias permite a los usuarios operar con redes inalámbricas sin necesidad de obtener una licencia, y además sin cargo alguno. Al no requerirse una licencia para su uso, ello ha facilitado la expansión de este tipo de redes.

En las redes de largo alcance, la conectividad es típicamente proporcionada por las empresas que comercializan la conectividad inalámbrica como un servicio. Estas redes abarcan grandes áreas, tales como un área metropolitana (WMAN), un estado o provincia, o un país entero. El objetivo de las redes de largo alcance es proporcionar cobertura inalámbrica a nivel mundial. La red de largo alcance más

común es la red inalámbrica de área amplia (WWAN). Cuando se requiere verdadera cobertura global, también están disponibles las redes de satélites.

2.1 Redes inalámbricas de área personal (WPAN)

Las redes inalámbricas de área personal se basan en el estándar IEEE 802.15 [3-4]. Las redes inalámbricas permiten la comunicación en un rango de distancias muy corto, unos 10 metros. A diferencia de otras redes inalámbricas, una conexión realizada a través de una WPAN implica, por lo general, poca o ninguna infraestructura o conectividad directa fuera del enlace establecido. Esto permite soluciones pequeñas, eficientes en energía y de bajo coste que pueden ser implementadas en una amplia gama de dispositivos, como por ejemplo teléfonos inteligentes, PDAs, entre otros.

Este tipo de redes se caracterizan por su bajo consumo de energía y también una baja velocidad de transmisión. Se basan en tecnologías como Bluetooth, IrDA, ZigBee o UWB. Desde un punto de vista de aplicación, Bluetooth está destinado a un ratón, un teclado, un manos libres; IrDA está pensado para enlaces punto a punto entre dos dispositivos para la transferencia de datos simples y sincronización de archivos; ZigBee está diseñado para redes inalámbricas fiables para el seguimiento y control de procesos, mientras que UWB está orientado a enlaces multimedia de gran ancho de banda.

La **velocidad de transmisión** (*bit rate* del inglés) es el número de bits transferidos o recibidos por unidad de tiempo (Unidades: bps o bit/s)

Un **Módem** es un dispositivo que permite a un ordenador transmitir y recibir datos

Bluetooth

Bluetooth pertenece al estándar IEEE 802.15.1. Originalmente Bluetooth fue diseñado para comunicaciones omnidireccionales (punto a multipunto), de bajo consumo de energía, corto alcance y con dispositivos baratos, reemplazando el uso de cables y conectando los dispositivos a través de una conexión ad hoc por radio. Hoy en día los desarrolladores están diseñando componentes y sistemas habilitados para Bluetooth para una gama de aplicaciones adicionales. Los dispositivos que incorporan esta tecnología se clasifican en tres grupos diferentes según su alcance máximo: Clase 1, Clase 2 y Clase 3, donde el rango es de unos 100 metros, 10 metros y 1 metro, respectivamente. El uso de la banda de 2,4 GHz, permite que dos dispositivos dentro del rango de cobertura de cada uno puedan compartir hasta 720 Kbps de velocidad de transferencia. La clase 2 es la más utilizada.

Una red Bluetooth también se denomina picored (*piconet*), y se compone de hasta 8 dispositivos activos en una relación maestro-esclavo (*master-slave*). El primer dispositivo de Bluetooth en la picored es el maestro y todos los demás dispositivos son esclavos que se comunican con el maestro. Una picored típicamente tiene un alcance de 10 metros, aunque se puede llegar a rangos de hasta 100 metros en circunstancias ideales. Para garantizar la seguridad, cada enlace se codifica y protege contra escuchas e interferencias. Dos picoredes pueden conectarse para

formar una red dispersa (*scatternet*). Un dispositivo Bluetooth puede participar en varias picoredes al mismo tiempo, permitiendo así la posibilidad de que la información pudiera fluir más allá de la zona de cobertura de una única picored. En una red dispersa, un dispositivo podría ser un esclavo en varias de las picoredes, pero actuar como maestro en sólo una de ellas.

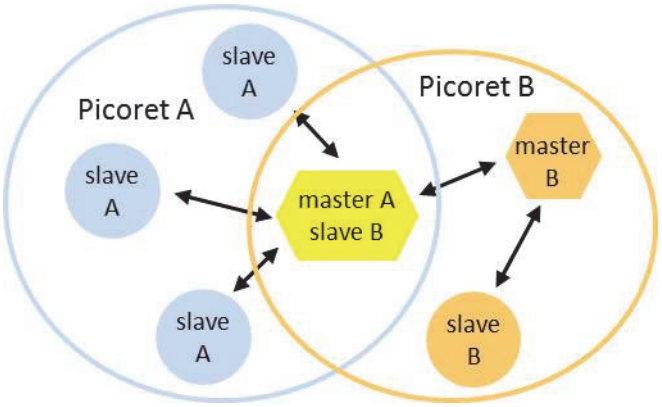


Fig. 1.2 Red dispersa Bluetooth formada de dos picoredes. El maestro de la picored A es un esclavo en la picored B.

IrDA

La Asociación de Datos por Infrarrojos (*Infrared Data Association* - IrDA) especifica un conjunto completo de estándares para comunicaciones por infrarrojos. IrDA se refiere a ese conjunto de normas y se utiliza para proporcionar conectividad inalámbrica a los dispositivos que normalmente utilizan cables para la conectividad. IrDA es un estándar de transmisión de datos ad-hoc de bajo consumo de energía, bajo coste, unidireccional (punto a punto), cono de ángulo estrecho (<30º), diseñado para operar con distancias de hasta 1 metro y a velocidades de 9600 bps a 4 Mbps (actualmente), 16 Mbps (en desarrollo). Algunos de los dispositivos que utilizan IrDA son portátiles, PDAs, impresoras y cámaras.

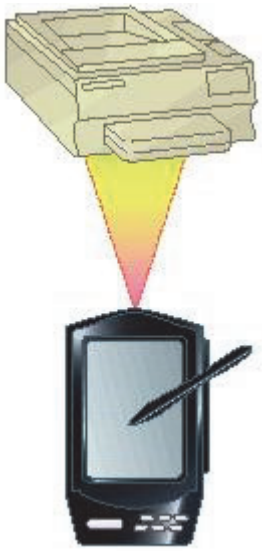


Fig. 2 . Comunicación IrDA entre una PDA y una impresora (punto a punto)

ZigBee

ZigBee está basado en el estándar IEEE 802.15.4 que fue desarrollado como un estándar global abierto para abordar las necesidades de fácil aplicación, alta fiabilidad, bajo costo, bajo consumo y bajas velocidades de transmisión de datos en redes de dispositivos inalámbricos. ZigBee opera en las bandas sin licencia 2.4 GHz, 900 MHz y 868 MHz con una velocidad de transmisión máxima de 250 Kbps, lo suficiente para satisfacer las necesidades de un sensor y de automatización usando redes inalámbricas.

ZigBee también sirve para la creación de redes inalámbricas más grandes que no exijan una gran cantidad de transmisión de datos. En una red ZigBee pueden participar dos tipos diferentes de dispositivos: dispositivos de funcionalidad completa (*Full Function Device* - FFD) y dispositivos de funcionalidad reducida (*Reduced Function Device* - RFD). Los FFDs pueden operar en tres modos distintos, como coordinador de la WPAN, coordinador o dispositivo. El RFD se diseñó sólo para aplicaciones muy simples, como la de un interruptor de luz. ZigBee soporta tres topologías de red diferentes: estrella, malla, y árbol, mostradas en la Figura 1.4. En la topología en estrella, la comunicación se establece entre los dispositivos y un controlador central único, denominado coordinador de la WPAN. En la topología de malla, cualquier dispositivo puede comunicarse con cualquier otro dispositivo, siempre y cuando estén uno en el rango del otro. La red en árbol es un caso especial de una red en malla en la que la mayoría de los dispositivos son FFDs y un RFD puede conectarse a la red como un nodo hoja en el extremo de una rama. Cualquiera de los FFD puede actuar como router y proporcionar servicios de sincronización a otros dispositivos y routers. El coordinador de la WPAN será uno de estos routers.

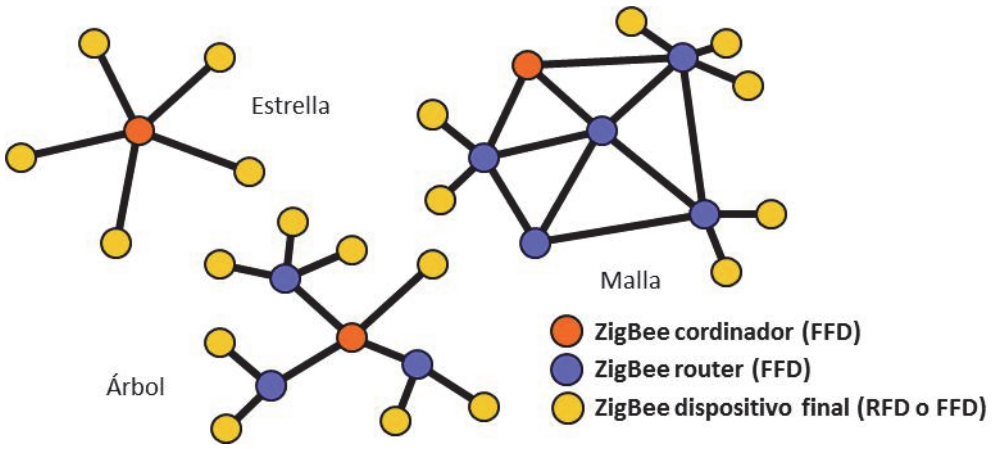


Figure 1.4 Diagrama de la estructura de una red ZigBee

UWB

Basado en el estándar IEEE 802.15.3, la tecnología UWB ha atraído recientemente mucha atención como una red inalámbrica para comunicaciones de alta velocidad y corto alcance en interiores. UWB sirve a un propósito muy diferente que las otras tecnologías ya mencionadas en este apartado. UWB permite la transmisión de grandes archivos de datos a altas velocidades en distancias cortas. La tecnología

UWB ofrece una velocidad de transmisión de datos de más de 110 Mbps hasta 480 Mbps a distancias de hasta unos pocos metros capaz de satisfacer a la mayoría de las aplicaciones multimedia como pueda ser el audio y video en las redes del hogar, y también puede actuar como un sustituto inalámbrico del cable de buses serie de alta velocidad tales como el USB 2.0 y IEEE 1394. En América, las frecuencias para UWB están asignadas en la banda de 3,1 GHz a 10,6 GHz. Sin embargo, en Europa, las frecuencias incluyen dos bandas: de 3,4 GHz a 4,8 GHz y de 6 GHz a 8,5 GHz.

Las comunicaciones UWB transmiten información mediante la emisión de pulsos de muy corta duración y de gran ancho de banda, ver Figura 1.5, lo que permite utilizar modulación por posición o tiempo de pulso. La información también puede ser modulada en señales UWB (pulsos) mediante la codificación de la polaridad del pulso, su amplitud y/o mediante el uso de pulsos ortogonales. Los pulsos de UWB se pueden enviar de forma esporádica a relativamente bajas velocidades de transmisión para soportar la modulación por posición o tiempo de pulso, pero también se pueden enviar a tasas de hasta el inverso del ancho de banda de pulso UWB.

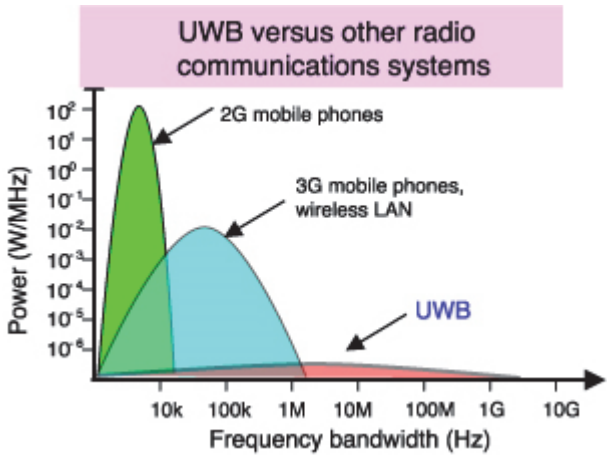


Figure 1.5 Utilización del ancho de banda frecuencial y consumo de energía por la tecnología UWB.

2.2 Redes inalámbricas de área local (WLAN)

Las redes inalámbricas de área local (WLAN) están diseñadas para proporcionar acceso inalámbrico en zonas con un rango típico de hasta 100 metros y se utilizan sobre todo en el hogar, la escuela, una sala de ordenadores, o entornos de oficina (Figura 1.6). Esto proporciona a los usuarios la capacidad de moverse dentro de un área de cobertura local y permanecer conectado a la red [2, 5]. Las WLAN se basan en el estándar 802.11 del IEEE y son comercializadas bajo la marca Wi-Fi. Debido a la competencia, otros estándares como HIPERLAN nunca recibieron tanta aplicación comercial. El estándar IEEE 802.11 fue más sencillo de implementar y se hizo más rápido con el mercado. La familia completa de este estándar se revisará con más detalle en el apartado 4.

El IEEE 802.11 comprende toda una familia de diferentes estándares para redes inalámbricas de área local. El IEEE 802.11b fue el primer estándar aceptado, admitiendo hasta 11 Mbps en la banda frecuencial sin licencia de 2,4 GHz. Posteriormente, el estándar IEEE 802.11g fue diseñado como el sucesor del IEEE 802.11b con un mayor ancho de banda. Un punto de acceso IEEE 802.11g soportará clientes 802.11b y 802.11g. Del mismo modo, un ordenador portátil con una tarjeta IEEE 802.11g será capaz de acceder a los puntos de acceso 802.11b existentes, así como a los nuevos puntos de acceso 802.11g. Esto se debe a las redes LAN inalámbricas basadas en 802.11g utilizan la misma banda de 2,4 GHz que utiliza el 802.11b. La velocidad de transferencia máxima para el enlace inalámbrico IEEE 802.11g es de 54 Mbps, pero se ve reducida automáticamente cuando la señal de radio es débil o cuando se detecta una interferencia.

Figure 1.6 Esquema de una WLAN en el hogar

2.3 Redes inalámbricas de área metropolitana (WMAN)

Las redes inalámbricas de área metropolitana (WMAN) forman el tercer grupo de redes inalámbricas. Las WMAN se basan en el estándar IEEE 802.16, a menudo denominado WiMAX (*Worldwide Interoperability for Microwave Access*). WiMAX es una tecnología de comunicaciones con arquitectura punto a multipunto orientada a proporcionar una alta velocidad de transmisión de datos a través de redes inalámbricas de área metropolitana [1-3]. Esto permite que las redes inalámbricas LAN más pequeñas puedan ser interconectadas por WiMAX creando una gran WMAN. Consecuentemente, la creación de redes entre ciudades puede lograrse sin la necesidad de cableado costoso.

WiMAX es similar a Wi-Fi, pero proporciona cobertura a distancias mayores. Mientras que Wi-Fi está destinado a proporcionar cobertura en áreas relativamente pequeñas, como en oficinas o *hot spots*, WiMAX opera en dos bandas de frecuencia, una mezcla de banda con licencia y banda sin licencia, de 2 GHz a 11 GHz y de 10 GHz a 66 GHz, pudiendo alcanzar velocidades de transmisión próximas a 70 Mbps en una distancia de 50 km a miles de usuarios desde una única estación base, tal como se representa en la Figura 1.7. Al poder operar en dos bandas de frecuencia, WiMAX puede trabajar con y sin línea de visión directa. En el rango de frecuencias de 2 a 11GHz se trabaja sin línea de visión directa, donde un equipo dentro de un edificio se comunica con una torre/antena exterior del edificio. Las transmisiones a baja frecuencia no son fácilmente perturbadas por obstáculos físicos. Por el contrario, las transmisiones a mayor frecuencia se utilizan en aplicaciones con línea de visión directa. Esto permite a las torres/antenas poder comunicarse entre sí en distancias mayores.

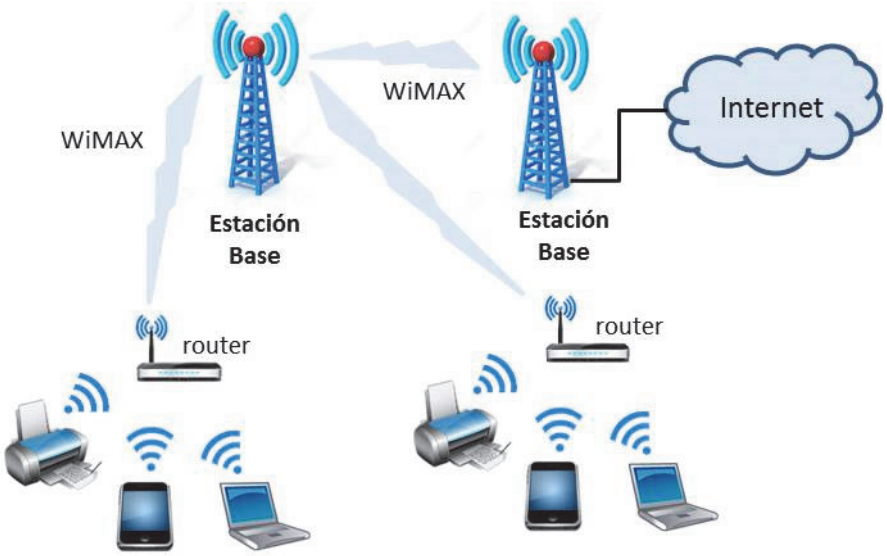


Figure 1.7 Diagrama de una red WiMAX

2.4 Redes inalámbricas de área amplia (WWAN)

Las redes inalámbricas de área amplia se extienden más allá de los 50 kilómetros y suelen utilizar frecuencias con licencia. Este tipo de redes se pueden mantener en grandes áreas, tales como ciudades o países, a través de los múltiples sistemas de satélites o ubicaciones con antena atendidos por un proveedor de servicios de Internet. Existen principalmente dos tecnologías disponibles: la telefonía móvil y los satélites [1-3].

Red de telefonía móvil

En la red de telefonía móvil, el área de cobertura se divide en celdas. Un transmisor de celda o estación base, en el centro de la celda, está diseñado para servir a una celda individual. Los dispositivos móviles están conectados a una estación base y estas últimas a una central de conmutación de telefonía móvil que une el teléfono móvil y la red cableada de telefonía. El sistema pretende hacer un uso eficiente de los canales disponibles mediante el uso de transmisores de baja potencia para permitir la reutilización de frecuencias a distancias mucho más pequeñas.

Las diferentes generaciones de telefonía móvil se han desarrollado desde principios de 1980. La primera generación, 1G, era analógica y fue concebida y diseñada exclusivamente para las llamadas de voz casi sin consideración de servicios de datos, con una velocidad de hasta 2,4 kbps. La segunda generación, 2G, está basada en tecnología digital y la infraestructura de red (GSM), permitiendo mensajes de texto con una velocidad de datos de hasta 64 Kbps. La generación 2.5G se sitúa entre la 2G y la 3G. También se la conoce como 2G + GPRS. Se trata de una versión mejorada de 2G, con una velocidad de hasta 144 Kbps. La generación 3G fue introducida en el año 2000, con una velocidad de datos de hasta 2 Mbps. La 3.5G es una versión mejorada de la 3G que utiliza HSDPA para acelerar las transferencias de datos hasta 14 Mbps. Por último, la cuarta generación, 4G, es capaz de proporcionar velocidades de hasta 1 Gbps y cualquier tipo de servicio en cualquier momento de acuerdo con las necesidades del usuario, en cualquier lugar. La generación 5G se espera para el año 2020.

Satélite

Las comunicaciones inalámbricas también pueden llevarse a cabo a través de satélites. Debido a su gran altura, las transmisiones por satélite pueden cubrir una amplia área sobre la superficie de la tierra. Esto puede ser muy útil para los usuarios que se encuentran en zonas remotas o islas donde no hay cables submarinos en servicio. En estos casos, se necesitan teléfonos vía satélite.

Cada satélite está equipado con varios transpondedores los cuales constan de un transceptor y una antena. La señal entrante se amplifica y luego es retransmitida en una frecuencia diferente.

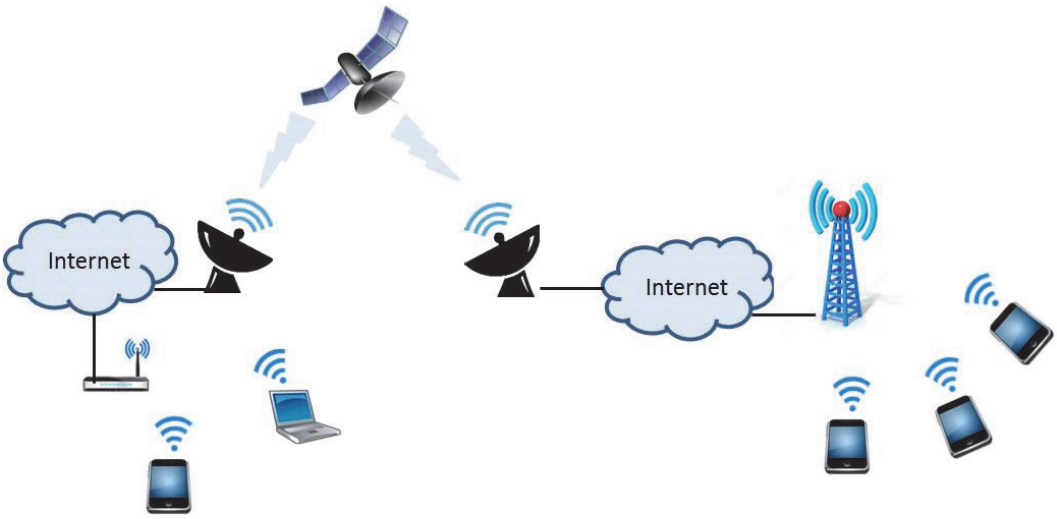


Figure 1.8 Redes de telefonía móvil y de satélite

3 Arquitectura de red

3.1 Términos y terminología

En esta sección se definen diversos términos utilizados en una arquitectura de red inalámbrica. Sin embargo, no todas las entradas de una arquitectura genérica existen en todas las tecnologías y su funcionalidad exacta puede ser diferente.

La arquitectura lógica del estándar 802.11 contiene varios componentes principales: la estación (STA), el punto de acceso inalámbrico (AP), el conjunto independiente de servicios básicos (IBSS), el conjunto de servicios básicos (BSS), la red de distribución (DS), y el conjunto de servicios extendidos (ESS). Algunos de los componentes de la arquitectura lógica 802,11 corresponden directamente a dispositivos de hardware, tales como estaciones y puntos de acceso inalámbricos. La estación contiene una tarjeta de adaptador, tarjeta PC o un dispositivo integrado para poder proporcionar conectividad inalámbrica. Las funciones del punto de acceso inalámbrico son servir como un puente entre las estaciones y la red troncal existente para el acceso a la red.

Una **estación (*Station* - STA)** podría ser un PC, un ordenador portátil, una PDA, un teléfono o cualquier dispositivo que tenga la capacidad de interferir en el medio inalámbrico.

Un **punto de acceso (*Access Point* - AP)**, a veces también llamado **estación base (BS),** es un dispositivo que permite a los dispositivos inalámbricos que se conecten a una red cableada mediante Wi-Fi, o estándares relacionados.

Un **conjunto de servicios básicos (*Basic Service Set* - BSS)** consiste en un punto de acceso, junto con todas las estaciones asociadas. El punto de acceso actúa como un maestro para controlar las estaciones dentro de ese BSS. El BSS más simple se compone de un AP y una STA.

Un **conjunto de servicios extendidos (*Extended Service Set* - ESS)** es un conjunto de uno o más conjuntos interconectados de servicios básicos (BSS) que aparecen como un solo BSS a la capa de control de enlace lógico de cualquier estación asociada con una de esas BSS.

Cuando todas las estaciones en el conjunto de servicios básicos son estaciones móviles y no hay conexión a una red cableada, el BSS se denomina **BSS independiente (*Independent Basic Service Set* - IBSS).** Un IBSS es una red ad hoc que no contiene puntos de acceso, lo que significa que no pueden conectarse a cualquier otro conjunto de servicios básicos.

Un **sistema de distribución (DS)** es el mecanismo por el cual diferentes puntos de acceso pueden intercambiar tramas entre sí o bien con las redes cableadas, si las hubiera. El sistema de distribución no es necesariamente una red y el estándar IEEE 802.11 no especifica ninguna tecnología en particular para el DS. En casi todos los productos comerciales se utiliza Ethernet por cable como la tecnología de red troncal.

Figure 1.9 Con junto de servicios básicos (BSS) e Independiente (IBSS).

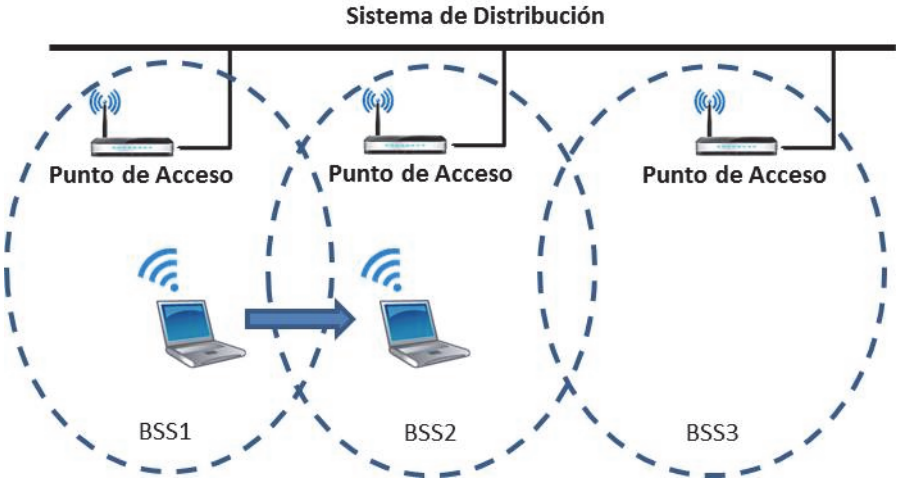


Figure 1.10 Conjunto de servicios extendidos (ESS) y soporte a la movilidad.

3.2 Arquitecturas

Existen dos modos para configurar la arquitectura de una red inalámbrica: ad hoc e infraestructura [1-2]. En el modo ad hoc, los dispositivos transmiten directamente punto a punto, mientras que en el modo infraestructura, los dispositivos se comunican a través de un punto de acceso que sirve de puente a otras redes.

Modo Ad hoc

Cuando se utiliza el modo ad hoc, todos los dispositivos de la red inalámbrica se comunican directamente entre sí, de igual a igual, en el modo de comunicación punto a punto. La red no tiene ninguna estructura o puntos fijos. No se requiere ningún punto de acceso para la comunicación entre dispositivos.

El modo ad hoc es el más adecuado para un pequeño grupo de dispositivos que se encuentren presentes físicamente en estrecha proximidad entre sí. El rendimiento de la red sufre si el número de dispositivos aumenta. En este modo, las desconexiones al azar de dispositivos pueden ocurrir con frecuencia y, también, la gestión de la red puede resultar una tarea difícil para su. El modo ad hoc tiene otra limitación y es sin la instalación de pasarelas especiales, las redes en modo ad hoc no pueden conectarse con una red de área local cableada y en consecuencia no puede acceder a Internet.

Sin embargo, el modo ad hoc funciona bien en un entorno pequeño siendo la forma más fácil y menos costosa de configurar una red inalámbrica.

Modo Infraestructura

La otra arquitectura de red inalámbrica es el modo de infraestructura. En este modo, todos los dispositivos están conectados a la red inalámbrica con la ayuda de un punto de acceso (AP). Los puntos de acceso inalámbricos son generalmente routers o switches que pasan los datos de la red inalámbrica a datos en una Ethernet cableada, actuando como un puente entre la LAN cableada y los dispositivos inalámbricos. La conexión de varios puntos de acceso a través de una red troncal Ethernet por cable puede extender aún más la cobertura de la red inalámbrica permitiendo que un dispositivo móvil se salga fuera del rango de cobertura de un punto de acceso y entre en el rango de otro. Consecuentemente, los clientes inalámbricos pueden moverse libremente del dominio de un punto de acceso a otro y seguir manteniendo la conexión de red sin cortes.

El modo de infraestructura ofrece una mayor seguridad, facilidad de gestión, y mucha más escalabilidad y estabilidad. Sin embargo, el modo de infraestructura incurre en un costo adicional debido al despliegue de puntos de acceso.

Identificador del Conjunto de Servicios Extendidos (ESSID)

El identificador del conjunto de servicios extendidos (ESSID) es uno de los dos tipos de identificadores del conjunto de servicios (SSID). En una red inalámbrica ad hoc sin puntos de acceso se utiliza el identificador del conjunto de servicios

básicos (BSSID). En una red inalámbrica de infraestructura, que incluye un punto de acceso, se utiliza el ESSID aunque a menudo se refiere al mismo como SSID.

El **identificador del conjunto de servicios** (***service set identifier*** **- SSID)** es una clave alfanumérica de hasta un máximo de 32 caracteres que identifica a una red inalámbrica de área local.

Algunos vendedores se refieren a la SSID como el nombre de la red. Para que los dispositivos inalámbricos en una red puedan comunicarse entre sí, es necesario que todos ellos se configuraren con el mismo SSID.

4 El estándar IEEE 802.11

El estándar IEEE 802.11 es un conjunto especificaciones de control de acceso al medio (MAC) y de la capa física (PHY) para la implementación de redes inalámbricas de área local en las bandas de frecuencias 2,4 GHz, 5 GHz, y 60 GHz [1-2].

Estas especificaciones son creadas y mantenidas por el grupo de trabajo IEEE 802.11. La versión base del estándar fue lanzado en 1997, y ha tenido modificaciones posteriores. El estándar y las enmiendas constituyen la base de los productos para redes inalámbricas que utilizan la marca Wi-Fi.

4.1 El protocolo 802.11

El comité del estándar IEEE 802 define dos capas separadas para la capa de enlace de datos del modelo de referencia OSI, la subcapa de control de enlace lógico (*Logical Link Control* - LLC) y la subcapa de control de acceso al medio (*Media Access Control* - MAC). El estándar IEEE 802.11 define las especificaciones para la capa física y la capa de control de acceso al medio que se comunica por arriba con la capa de control de enlace lógico, tal y como se muestra en la Figura 1.11.

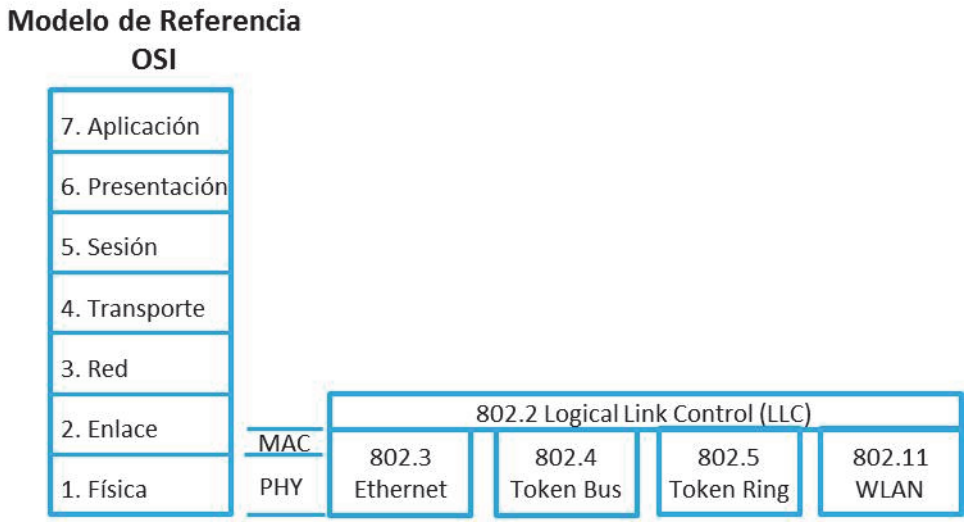


Figure 1.11El estándar IEEE 802.11 y el modelo de referencia OSI

Todos los componentes de la arquitectura 802.11 pertenecen a cualquiera de las dos capas, la subcapa de control de acceso al medio de la capa de enlace de datos o bien de la capa física (*Physical* - PHY).

4.2 802.11 La trama MAC

La trama MAC del estándar IEEE 802.11 que se muestra en la Figura 1.12 consta de una cabecera MAC, un cuerpo de la trama y una secuencia de verificación de la trama (FCS). El formato de la trama MAC comprende un conjunto de nueve campos que se producen en un orden fijo en todas las tramas.

Campo Control de Trama

El Campo de Control de Trama, ver Figure 1.12, contiene información de control utilizada para definir el tipo de trama MAC 802.11 y proporcionar la información necesaria a los siguientes campos para entender cómo procesar la trama MAC.

Una descripción de cada subcampo del campo de control de trama es la siguiente:

- ***Protocol Version*** proporciona la versión actual del protocolo 802.11 utilizado. Las estaciones receptoras utilizan este valor para determinar si es soportada la versión del protocolo de la trama recibida.

- ***Type and Subtype*** determina la función de la trama. Hay tres tipos de tramas diferentes: de control, de datos y de gestión. Existen varios subtipos para cada tipo de trama. Cada subtipo determina la función específica que debe llevar a cabo el tipo de trama asociada.

- ***To DS and From DS*** indica si la trama se dirige o sale del DS (sistema de distribución), y sólo se utiliza en las tramas de tipo de datos de las STA asociadas con un AP.

- ***More Fragments*** indica si hay más fragmentos de la trama, ya sea de tipo datos o de gestión.

- ***Retry*** indica si la trama está siendo retransmitida, ya sea de tipo datos o de gestión.

- ***Power Management*** indica si la STA que envía está en modo activo o en el modo de ahorro de energía.

- ***More Data*** indica a un STA que se encuentra en el modo de ahorro de energía que el AP tiene más tramas para enviar. También se utiliza en los APs para indicar que existen tramas adicionales de difusión/multidifusión.

- ***WEP*** indica si se utilizan cifrado y autenticación en trama. Se puede configurar para todas las tramas de datos y de gestión que tienen el subtipo establecido en autenticación.

- ***Order*** indica que todas las tramas de datos recibidas deben ser procesadas en orden.

Campo Duración/ID

Este campo es utilizado en todas las tramas de tipo control, excepto en las del subtipo *Power Save* (PS) *Poll*, para indicar la duración restante necesaria hasta recibir la próxima transmisión de trama. Cuando se trata del subtipo PS *Poll*, el campo contiene la identidad de asociación (AID) de la STA que transmite la trama.

Campos de Dirección

Dependiendo del tipo de trama, los cuatro campos de dirección contendrán una combinación de los siguientes tipos de dirección:

- ***BSS Identifier (BSSID)*** identifica unívocamente a cada BSS. Cuando la trama es de una STA en una infraestructura BSS, el BSSID es la dirección MAC del AP. Cuando la trama es de una STA perteneciente a una IBSS, el BSSID es una dirección MAC administrada localmente generada aleatoriamente por la STA que inició la IBSS.
- ***Destination Address (DA)*** indica la dirección MAC del destino final que debe recibir la trama.
- ***Source Address (SA)*** indica la dirección MAC de la fuente original que inicialmente creó y transmitió la trama.
- ***Receiver Address (RA)*** indica la dirección MAC de la próxima STA que debe recibir la trama.
- ***Transmitter Address (TA)*** indica la dirección MAC de la STA que transmitió la trama.

Para más información acerca de los tipos de dirección y del contenido de los campos de dirección en el encabezado MAC 802.11, consulte el estándar IEEE 802.11 en la Web del IEEE [6].

Control de Secuencia

El campo de control de secuencia está formado por dos subcampos, el número de fragmento y el número de secuencia, tal y como se muestra en la Figura 1.12.

A continuación se describe cada uno de los subcampos anteriores:

- ***Sequence Numbe*****r** indica el número de secuencia de cada trama. El número de secuencia es el mismo para cada trama enviada en una trama fragmentada; de lo contrario, el número de secuencia se incrementa en uno hasta llegar a 4095, volviéndose a empezar desde cero.
- ***Fragment Number*** indica el número de fragmento en una trama fragmentada. El valor inicial se establece en 0 y luego se incrementa en uno para cada uno de los fragmentos de trama enviados.

Cuerpo de la Trama

El cuerpo trama contiene los datos o la información incluida en cualquier trama del tipo de gestión o de datos.

Secuencia de Verificación de Trama

La STA transmisora utiliza una verificación de redundancia cíclica (*cyclic redundancy check* - CRC) sobre todos los campos de la cabecera MAC y el cuerpo de la trama para generar el valor de FCS. La STA receptora utiliza el mismo cálculo de CRC para determinar su propio valor del campo FCS y verificar si se produjeron errores en la trama durante la transmisión.

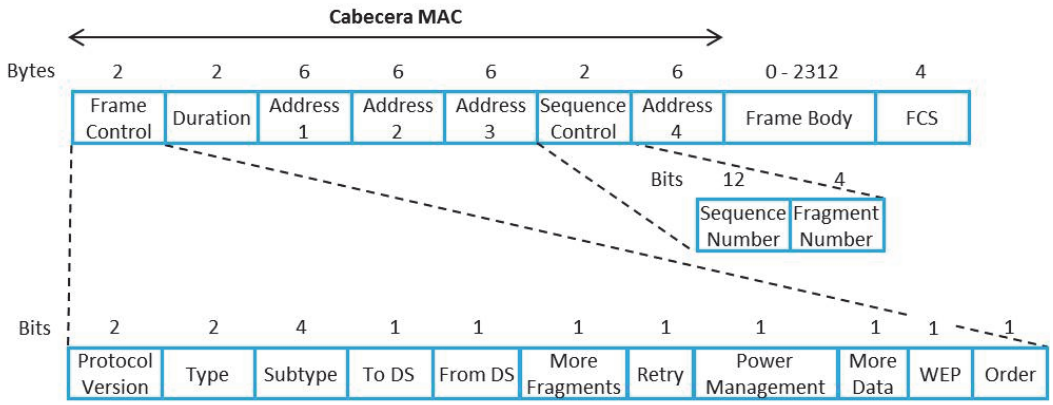


Figure 1.12 Formato de trama MAC en el estándar 802.11. Se detallan los campos de control de trama y de control de secuencia.

4.3 Capa Física PHY

En la capa física (PHY), el estándar IEEE 802.11 define una serie de esquemas de codificación y transmisión para las comunicaciones inalámbricas, los esquemas de transmisión más comunes son Espectro Ensanchado por Salto de Frecuencia (*Frequency Hopping Spread Spectrum* - FHSS), Espectro Ensanchado por Secuencia Directa (*Direct Sequence Spread Spectrum* - DSSS) y Multiplexación por División de Frecuencias Ortogonales (*Orthogonal Frequency Division Multiplexing* - OFDM). La figura 1.13 muestra los estándares 802.11, 802.11b, 802.11a, 802.11g, 802.11n y 802.11ac que existen en la capa PHY. Estos estándares se describen en los siguientes apartados.

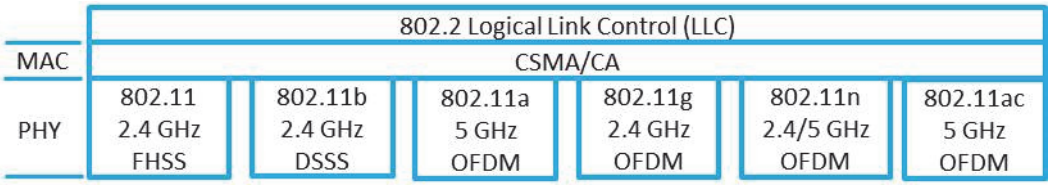


Figure 1.13 Estándares IEEE 802.11en la capa física PHY

IEEE 802.11

La velocidad de transmisión para el estándar IEEE 802.11 original es de 2 Mbps utilizando el esquema de transmisión FHSS y la banda de frecuencia ISM que opera en el rango de frecuencia de 2,4 GHz a 2,5 GHz. Sin embargo, bajo condiciones menos ideales, se utiliza una velocidad de transmisión menor, de 1 Mbps.

802.11b

La principal mejora de IEEE 802.11 por IEEE 802.11b es la estandarización de la capa física para soportar velocidades de transmisión más altas. El estándar IEEE 802.11b admite dos velocidades adicionales, 5.5 Mbps y 11 Mbps, utilizando la banda de frecuencia de 2,4 GHz. Se utiliza el esquema de transmisión DSSS con el fin de proporcionar velocidades de transmisión más altas. La velocidad de 11 Mbps es alcanzable bajo condiciones ideales. Si no se cumplen las condiciones ideales, se utilizan las velocidades más lentas de 5,5 Mbps, 2 Mbps y 1 Mbps.

Es importante señalar que 802.11b utiliza la misma banda de frecuencia que utilizan los hornos de microondas, teléfonos inalámbricos, monitores de bebés, cámaras de vídeo inalámbricas y los dispositivos Bluetooth.

802.11a

El estándar IEEE 802.11a puede operar a una velocidad de hasta 54 Mbps y utiliza la banda de frecuencia de 5 GHz. En lugar de DSSS, este estándar utiliza OFDM, lo que permite que los datos sean transmitidos por subportadoras en paralelo, proporcionando una mayor resistencia a las interferencias y una mayor velocidad

de transmisión. Esta tecnología, con mayor velocidad, permite a la red inalámbrica un mejor comportamiento en aplicaciones de vídeo y conferencia.

Al no utilizar las mismas frecuencias que otros dispositivos (como teléfonos inalámbricos que funcionan en la banda de frecuencia de 2,4 GHz), OFDM y IEEE 802.11a proporcionan una mayor velocidad de transferencia y una señal más limpia, con muchas menos interferencias. La velocidad de bits de 54 Mbps es alcanzable bajo condiciones ideales. Si no se cumplen las condiciones ideales, se utilizan las velocidades más lentas de 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps y 6 Mbps.

802.11g

El estándar IEEE 802.11g puede operar a una velocidad de hasta 54 Mbps, pero utiliza la banda de frecuencia de 2,4 GHz y OFDM. 802.11g también es compatible con 802.11b, y puede operar a las velocidades de bits 802.11by utilizar DSSS. Adaptadores de red inalámbrica 802.11g pueden conectarse a un punto de acceso inalámbrico 802.11b, y adaptadores de red inalámbrica 802.11b pueden conectarse a un punto de acceso inalámbrico 802.11g. Por lo tanto, 802.11g proporciona una ruta de migración para redes 802.11b a una tecnología estándar compatible en frecuencia pero con una velocidad de transmisión más alta. Los adaptadores existentes de red inalámbrica 802.11b no se pueden actualizar a 802.11g mediante una actualización del firmware del adaptador, deben ser reemplazados. A diferencia de la migración de 802.11b a 802.11a (en la que todos los adaptadores de red, tanto en los clientes inalámbricos como en los puntos de acceso inalámbricos deben ser reemplazados al mismo tiempo), la migración de 802.11b a 802.11g se puede hacer de forma incremental.

Al igual que 802.11a, 802.11g utiliza 54 Mbps en condiciones ideales y las velocidades más lentas de 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps y 6 Mbps en condiciones menos ideales.

802.11n

El estándar IEEE 802.11n tiene como objetivo mejorar la distancia (hasta 250 m) y la velocidad de transmisión de las dos normas anteriores, 802.11a y 802.11g, con un aumento significativo de la velocidad máxima de datos en bruto de 54 Mbps a 600 Mbps en condiciones ideales añadiendo la tecnología de múltiple entrada múltiple salida y canales de 40 MHz, de mayor ancho de banda. Esta tecnología, denominada MIMO (*Multiple Input Multiple Output*), utiliza múltiples señales inalámbricas y antenas en el transmisor y el receptor. El estándar puede funcionar en las bandas de frecuencia de 2,4 GHz o 5 GHz.

802.11ac

El estándar 802.11ac, una actualización de 802.11n, ofrece un alcance similar, pero aumenta la velocidad de transmisión. Funciona en la banda de 5 GHz e incorpora la tecnología de formación de haz, banda ancha y múltiples antenas para ofrecer

velocidades de datos teóricas de hasta 1,3 Gbps, más del doble que las tasas de pico de 600 Mbps alcanzadas con el estándar 802.11n.

5 Seguridad

Las redes inalámbricas en general no son tan seguras como las redes cableadas. Las redes cableadas, desde un punto de vista muy simple, envían datos entre dos puntos, A y B, que están conectados por un cable de red. Sin embargo, las redes inalámbricas transmiten los datos en todas las direcciones a cualquier dispositivo que pueda estar escuchando, dentro de un rango limitado. Una red cableada puede ser protegida en sus extremos, por ejemplo, restringiendo el acceso físico e instalando cortafuegos. Una red inalámbrica con las mismas medidas sigue siendo vulnerable a escuchas. Por lo tanto, las redes inalámbricas requieren un esfuerzo más centrado para mantener la seguridad.

5.1 Comunicaciones seguras

La seguridad en las comunicaciones se describe a menudo en términos de tres elementos: autenticación, confidencialidad e integridad [1].

La **autenticación** garantiza que los nodos son quién y lo que dicen ser.

La autenticación se basa normalmente en demostrar el conocimiento de un secreto compartido, como la pareja nombre de usuario y contraseña. En sistemas más complejos, la posesión del secreto compartido puede demostrarse probando la posesión de una señal de que sea más difícil de robar o falsificar, como un certificado o una tarjeta inteligente.

La **confidencialidad** asegura que los intrusos no pueden leer el tráfico de red.

Típicamente, la confidencialidad se protege mediante el cifrado del contenido del mensaje. El cifrado aplica un conocido método reversible de transformación (denominado algoritmo de cifrado o encriptación) al contenido del mensaje original (denominado texto plano), codificándolo u ocultándolo para crear el texto cifrado. Sólo los que saben cómo revertir el proceso (descifrar el mensaje) pueden recuperar el texto original. Las formas más comunes de cifrado son a través de transformaciones matemáticas que utilizan una variable llamada clave como parte de sus manipulaciones. El receptor debe conocer tanto el método correcto como el valor de la clave que se utilizó con el fin de ser capaz de descifrar el mensaje. Para esquemas de cifrado comerciales, el método será de conocimiento público. La protección del secreto de la clave se vuelve crucial.

La **integridad** asegura que los mensajes son entregados sin alteración.

En el contexto de seguridad de las comunicaciones, la integridad se refiere a la capacidad de asegurarse de que el mensaje recibido no ha sido alterado de manera alguna y que es idéntico al mensaje que se envió. Los bytes de la secuencia de verificación de trama (*Frame Check Sequence* - FCS) son un ejemplo de comprobación de integridad, pero no se consideran seguros. Los bytes de FCS no se calculan sobre el mensaje de texto plano y luego protegiendo mediante encriptación toda la trama. En su lugar, se calculan sobre el texto cifrado, utilizando un método conocido, y se envían como texto plano, sin cifrar. Los bytes de FCS ayudan a identificar los paquetes que han sido alterados por accidente durante el transporte. Un atacante, sin embargo, podría volver a calcular los FCS ordinarios (por ejemplo, para ocultar la alteración deliberada de un paquete que capturado y retransmitido). Lo más difícil para un atacante es volver a calcular correctamente la secuencia de verificación de integridad o la función hash de seguridad, que es la prueba más fiable de la integridad del mensaje.

El concepto de integridad a veces se extiende para incluir la verificación de que la fuente del mensaje es la misma que la fuente indicada. Las marcas de tiempo y números de secuencia de mensajes pueden proteger contra "ataques por repetición"

pero, de nuevo, no se consideran seguros a menos que estén protegidos por encriptación.

La seguridad es siempre relativa, nunca absoluta. Para cada defensa, hay (o pronto habrá) un ataque exitoso. Para cada ataque, hay (o pronto habrá) una defensa exitosa. Sólo se trata de tiempo y esfuerzo. Cuanto mejor sea la defensa, más tiempo y esfuerzo que se necesita para romperla.

La defensa adecuada es aquella que está equilibrada y que coincide con el número esperado de ataques. El equilibrio es importante en dos sentidos. En primer lugar, el eslabón más débil debe ser lo suficientemente seguro. En segundo lugar, los elementos pasivos de autenticación, cifrado y comprobación de integridad deben ser respaldados por elementos activos tales como el seguimiento y la búsqueda de los intentos de ataques, el mantenimiento de una disciplina en seguridad, y así sucesivamente. La defensa adecuada es aquella en la que una ataque requiere sólo un poco más de tiempo y esfuerzo por parte de los atacantes de lo que están dispuestos a invertir. Las medidas de seguridad imponen costes y restricciones sobre el defensor. Al igual que cualquier otra decisión empresarial, estos equilibrios se deben hacer con los ojos abiertos.

5.2 Confidencialidad y Encriptación

La confidencialidad (impidiendo el acceso no autorizado a los contenidos de un mensaje) se logra mediante la protección del contenido de los datos con el cifrado. El cifrado es opcional en las WLAN, pero sin él, cualquier dispositivo compatible con el estándar dentro del alcance de la red puede leer todo su tráfico.

Principalmente ha habido tres métodos de encriptación para hacer seguras las redes WLAN. Desde finales de 1990, los algoritmos de seguridad Wi-Fi han sufrido múltiples actualizaciones con una pura y simple depreciación de los algoritmos más antiguos y una sustancial revisión de los algoritmos más recientes. En orden cronológico de aparición, estos son:

- WEP (*Wired Equivalent Privacy*)
- WPA (*Wi-Fi Protected Access*)
- WPA2 (*Wi-Fi Protected Access, version 2*)

WEP

WEP fue ratificado como estándar de seguridad Wi-Fi en septiembre de 1999. Las primeras versiones de WEP no eran particularmente fuertes, incluso para el momento en que fueron lanzados, porque las restricciones estadounidenses a la exportación de diversas tecnologías criptográficas llevaron a los fabricantes a restringir sus dispositivos con sólo 64 bits de cifrado. Cuando se levantaron las restricciones, se incrementó a 128 bits. A pesar de la introducción de la encriptación WEP de 256 bits, 128 bits sigue siendo una de las implementaciones más comunes.

A pesar de las revisiones del algoritmo y un aumento del tamaño de la clave, con el tiempo fueron descubiertos numerosos fallos de seguridad en el estándar WEP y, con una potencia de cálculo de los ordenadores cada vez mayor, se hizo más y más fácil explotarlos. Desde 2001 ya circulaban las gestas de la prueba de concepto y antes de 2005 el FBI hizo una demostración pública (en un esfuerzo por aumentar la conciencia de las debilidades de WEP) en la que rompían las contraseñas WEP en minutos utilizando software de libre distribución.

A pesar de varias mejoras, soluciones temporales y otros intentos para reforzar el sistema WEP, éste sigue siendo altamente vulnerable y los sistemas que se basan en WEP deberían ser actualizados o, si las actualizaciones de seguridad no son una opción, reemplazados. Wi-Fi Alliance retiró oficialmente WEP en 2004.

WPA

Para hacer frente a las vulnerabilidades de WEP, el grupo comercial Wi-Fi Alliance estableció WPA a principios de 2003. La configuración WPA más común es WPA-PSK (*Pre-Shared Key*). Las claves utilizadas por WPA son de 256 bits, un aumento significativo con respecto las claves de 64 bits y 128 bits utilizados en el sistema WEP.

Algunos de los cambios significativos implementados con WPA incluyeron comprobaciones de integridad del mensaje (para determinar si un atacante había capturado o alterado paquetes transmitidos entre el punto de acceso y el cliente) y el protocolo de integridad de clave temporal (*Temporal Key Integrity Protocol* - TKIP). TKIP utiliza un sistema de claves por paquete que era radicalmente más segura que la clave fija utilizada en el sistema WEP. TKIP fue reemplazado más tarde por el *Advanced Encryption Standard* (AES).

A pesar de que WPA era una mejora significativa sobre WEP, el fantasma de WEP atormentaba a WPA. TKIP, un componente central de WPA, fue diseñado para ser fácilmente ampliado a través de actualizaciones de firmware en los dispositivos WEP existentes. Como tal, tuvo que reciclar ciertos elementos utilizados en el sistema WEP que, en última instancia, también fueron explotados.

WPA, al igual que su predecesor WEP, se ha demostrado a través de ambas manifestaciones públicas a prueba de concepto y aplicadas a ser vulnerable a la intrusión. Curiosamente el proceso por el cual WPA se suele romper no es por un ataque directo contra el algoritmo WPA (aunque este tipo de ataques se han demostrado con éxito), sino por los ataques contra un sistema complementario que se puso en marcha con la instalación de WPA, la configuración protegida de Wi-Fi (WPS), diseñada para hacer más fácil la conexión de dispositivos a los puntos de acceso actuales.

WPA2

A partir de 2006, WPA fue sustituido oficialmente por WPA2. Uno de los cambios más significativos entre WPA y WPA2 fue el uso obligatorio de los algoritmos AES y la introducción de CCMP (*Counter Cipher Mode with Block Chaining Message Authentication Code Protocol*) como un reemplazo de TKIP (aún se conserva en WPA2 como un sistema de reserva y para interoperabilidad con WPA).

En la actualidad, la principal vulnerabilidad de seguridad para el sistema WPA2 real es una de oscura y requiere que el atacante ya tenga acceso a la red Wi-Fi protegida con el fin de tener acceso a ciertas claves para luego poder perpetuar un ataque en contra de los otros dispositivos en la red. Como tal, las implicaciones en seguridad de estas vulnerabilidades de WPA2 se limitan casi exclusivamente a las redes a nivel de empresa y merecen poca o ninguna consideración práctica en materia de seguridad de red doméstica.

Por desgracia, la misma vulnerabilidad causante del mayor agujero en la armadura WPA, el vector de ataque a través de la configuración protegida de Wi-Fi (WPS), persiste en los puntos de acceso WPA2 actuales. Aunque para irrumpir en una red protegida con WPA/WPA2 utilizando esta vulnerabilidad sean necesarias de 2-14 horas de esfuerzo sostenido con un ordenador actual, todavía es una preocupación legítima de seguridad y WPS debería ser desactivada (y, si fuese posible, el firmware del acceso punto debería ser reprogramado con una distribución que ni siquiera admitiese WPS por lo que el vector de ataque se eliminaría por completo).

La siguiente es una lista básica de clasificación de los métodos actuales de seguridad Wi-Fi, ordenados de mejor a peor:

1. WPA2 + AES
2. WPA + AES
3. WPA + TKIP/AES (TKIP aparece como método alternativo)
4. WPA + TKIP
5. WEP
6. Red abierta (ningún tipo de seguridad)

Idealmente, se desactivará la configuración protegida de Wi-Fi (WPS) y se pondrá el nivel de seguridad a WPA2 + AES. Todo lo demás en la lista está por debajo de lo ideal.

6 Ventajas y desventajas

Las redes inalámbricas tienen una serie de beneficios clave frente a las redes cableadas como la movilidad, la rentabilidad y la capacidad de adaptación, pero también algunas desventajas como la seguridad. A continuación, se enumeran las principales ventajas y desventajas de una red inalámbrica frente a una red cableada.

La siguiente lista resume algunos de los beneficios de las redes inalámbricas:

Aumento de la eficiencia

La mejora en las comunicaciones de datos conduce a una transferencia más rápida de información dentro de las empresas y entre los socios y clientes. Por ejemplo, los vendedores pueden comprobar de forma remota los niveles de existencias y precios durante sus ventas.

Mejor cobertura y movilidad

Los cables atan a uno a un lugar. Conectarse de manera inalámbrica significa que uno tiene la libertad de cambiar su ubicación sin perder la conexión, sin la necesidad de cables o adaptadores adicionales para acceder a las redes de la oficina.

Flexibilidad

Los trabajadores de oficinas con redes inalámbricas pueden conectarse en red sin sentarse en equipos dedicados y pueden también seguir siendo productivos fuera de la oficina. Esto puede conducir a nuevos estilos de trabajo, como el trabajo en el domicilio o el acceso directo a datos corporativos mientras uno se encuentra en las oficinas o instalaciones de un cliente.

Ahorro de costes

Las redes inalámbricas pueden resultar más fáciles y baratas de instalar, especialmente en edificios catalogados o donde el propietario no va a permitir la instalación de cables. La ausencia de cableado hace bajar costos. Esto se consigue mediante una combinación de factores: el costo relativamente bajo de los routers inalámbricos, la no necesidad de hacer regatas, perforar y empotrar cables dentro de las paredes u otros métodos que sean necesarios para realizar conexiones físicas. Además, no se hace necesario el mantenimiento del cableado.

Adaptabilidad

Integración rápida y fácil de los dispositivos en la red, y una alta flexibilidad al modificar una instalación.

Nuevas oportunidades/aplicaciones

Las comunicaciones inalámbricas podrían permitir ofrecer nuevos productos o servicios. Por ejemplo, muchas salas de embarque de aeropuertos, estaciones de tren, hoteles, cafés y restaurantes proporcionan conexión Wi-Fi a través de *hot spots*, permitiendo que los usuarios conecten su equipo a sus oficinas durante el viaje.

Existen también ciertas desventajas asociadas con el uso de redes inalámbricas.

Seguridad

La transmisión inalámbrica es más vulnerable a los ataques de usuarios no autorizados, es por ello que se debe prestar una especial atención a la seguridad.

Problemas de instalación

Se pueden sufrir interferencias si existen otras redes inalámbricas en el mismo edificio o bien cuando otras fuentes de señales de radio están presentes. Esto podría conducir a una mala comunicación o, en casos extremos, a la pérdida de la comunicación inalámbrica por completo

Cobertura

En algunos edificios conseguir una cobertura consistente puede ser difícil, lo que conlleva la existencia de puntos negros donde no hay cobertura. Por ejemplo, en las estructuras construidas a base de materiales de refuerzo de acero, puede que resulte difícil recibir las señales vía radio.

Velocidad de transmisión

La transmisión inalámbrica puede ser más lenta y menos eficiente que las redes cableadas. En las grandes redes inalámbricas, por lo general, la red troncal será cableada en vez de inalámbrica.

7 Aplicaciones

La implantación de la comunicación inalámbrica en sistemas embebidos sigue creciendo. Forrester Research, una compañía que se centra en las implicaciones empresariales de los cambios tecnológicos, ha informado que en unos pocos años hasta el 95% de los dispositivos utilizados para acceder a Internet serán los dispositivos distintos a un PC y que utilizan en su lugar un sistema embebido.

Existen multitud de aplicaciones para dispositivos embebidos con conectividad Wi-Fi:

- Aplicaciones de control y proceso industrial donde las conexiones cableadas son demasiado costosas o un inconveniente, por ejemplo, maquinaria en continuo movimiento.
- Aplicaciones de emergencia que requieran configuración inmediata y transitoria, como situaciones en el campo de batalla o de catástrofe.
- Aplicaciones móviles, tales como el seguimiento de bienes materiales.
- Cámaras de vigilancia (tal vez no desea que sean vistas, los cables son difíciles de ocultar).
- En mercados verticales como la medicina, la educación, y la fabricación.
- La comunicación con otros dispositivos Wi-Fi, como pueda ser un ordenador portátil o una PDA.
- Aplicaciones Máquina a Máquina (M2M).

Con referencia a la última, el término máquina a máquina (*Machine to Machine* - M2M) se refiere a las tecnologías que permiten tanto a los sistemas inalámbricos como a los cableados poder comunicarse con otros dispositivos del mismo tipo. Otra característica de la comunicación M2M es que esta interconexión permite la comunicación automatizada entre máquinas remotas y una o más capas de las aplicaciones de gestión centralizadas. Estos sistemas proporcionan el seguimiento y control en tiempo real, sin la necesidad de intervención humana.

Las interconexiones inalámbricas M2M se pueden dividir en dos grandes grupos: de corto alcance y de área amplia. En las de área amplia, la tecnología predominante utiliza módulos embebidos de telefonía móvil para conectar dispositivos remotos a los servidores de Internet o de aplicaciones. Un módulo de telefonía móvil incluye muchas de las mismas características que se pueden encontrar en un teléfono móvil, incluyendo voz y comunicación de datos, y es ideal para aplicaciones embebidas.

Las aplicaciones M2M se encuentran dentro de una amplia gama de industrias, por ejemplo: la lectura automática de medidores (*Automatic Meter Reading* - AMR), las máquinas expendedoras, los puntos de ventas (*Point of Sales* - POS), el transporte y la logística (gestión de flotas), la salud, la seguridad y muchas otras aplicaciones.

Según ABI Research, una empresa de investigación tecnológica y de asesoramiento, se prevé que para el año 2020 más de 30 mil millones de dispositivos estarán conectados de forma inalámbrica en el Internet de las Cosas (*Internet of Things*).

8 Conclusiones

Las tecnologías de redes inalámbricas conectan, sin el uso de cables, nuestros dispositivos de alta tecnología a una red de alta velocidad o a otro dispositivo. En el pasado, los cables tenían que ser instalados de una habitación a otra o de un piso a otro, el precio de configuración de la red era alto, y el tiempo para configurar una red cableada era muy superior con respecto a una red inalámbrica, entre otras cosas.

Hoy en día la configuración de red inalámbrica es muy fácil de hacer, y hay una enorme cantidad de productos inalámbricos para elegir, además de un montón de recursos disponibles de ayuda con la instalación y la configuración de la red inalámbrica, si fuera necesario.

Se puede elegir entre diferentes tecnologías aquella que mejor se adapte a los requisitos de la aplicación y al alcance, desde unos pocos metros hasta varios kilómetros. Sin duda, las redes inalámbricas ofrecen nuevas oportunidades para soluciones industriales, pero deben implementarse con especial atención a la seguridad.

Comparación entre diferentes tipos de redes inalámbricas

Tipo de red	Nombre	Estándar	Banda de frecuencia	Rango nominal	Máxima Velocidad. Transmis.
WPAN	Bluetooth	IEEE 802.15.1	2.4 GHz	10 m:	720 Kbps
	IrDA	IrDA	Ventana Infrarrojo 850-900 nm longitud de onda	1 m	16 Mbps
	ZigBee	IEEE 802.15.4	868 MHz, 900 MHz, 2.4 GHz	10 m	250 Kbps
	UWB	IEEE 802.15.3	3.1-10.6 GHz (USA) 3.4-4.8 GHz & 6-8.5 GHz (Europa)	10 m	480 Mbps
WLAN	Wi-Fi	IEEE 802.11	2.4 / 5 GHz	100 m	1 Mbps
		IEEE 802.11ª	5 GHz	100 m	48 Mbps
		IEEE 802.11b	2.4 GHz	100 m	11 Mbps
		IEEE 802.11g	2.4 GHz	100 m	54 Mbps
		IEEE 802.11n	2.4 / 5 GHz	250 m	600 Mbps
		IEEE 802.11ac	5 GHz	250 m	1.3 Gbps
WMAN	WiMAX	IEEE 802.16	2-11 GHz y10-66 GHz	50 km	70 Mbps
WWAN	Móvil	AMPS, GSM, GPRS, UMTS, HSDPA, LTE	700 MHz, 850 MHz, 900 MHz, 1800 MHz, 1900 MHz, 2100 MHz, 2600 MHz	> 50 km	1 Gbps
	Satélite	DVB-S2	3-30 GHz	> 50 km	60 Mbps