9. Capítulo 9: LAN Inalámbrica

Como su nombre lo indica, una LAN inalámbrica es aquella que hace uso de un medio de transmisión inalámbrico, como es el aire. En los últimos años se ha extendido el uso de las redes LAN's inalámbricas como complemento indispensable de las redes cableadas con el fin de satisfacer necesidades de movilidad, traslado, trabajo en red ad hoc y para dar cobertura en lugares difíciles de cablear. Una vez superados los problemas de alto precio, baja velocidad de transmisión, seguridad y necesidad de licencia para transmitir en el espectro radioeléctrico, el uso de las LAN inalámbricas se ha difundido rápidamente.

9.1. LAN Inalámbrica: Usos

Normalmente se indican tres áreas de aplicación para las redes LAN inalámbricas:

1. Ampliación de redes LAN cableadas
2. Acceso nómada
3. Redes ad hoc
4. Interconexión de edificios

Ampliación de Redes LAN Cableadas

Ante la necesidad de extender una LAN cableada, la mejor decisión en un gran número de situaciones es implementar una LAN inalámbrica. Un ejemplo es un edificio de gran superficie que es ocupado por una planta de fabricación, una planta comercial y un depósito, y al que se debe agregar una oficina independiente pero que debe estar conectada a la LAN del edificio por necesidades de trabajo en red. Otro ejemplo son los edificios históricos con insuficiente cable instalado de par trenzado donde está prohibido hacer más perforaciones para agregar nuevo cableado. Otro ejemplo de mención son pequeñas oficinas donde la instalación y el mantenimiento de una LAN cableada no resultan económicos. En todos los casos nombrados una LAN inalámbrica puede ofrecer una alternativa más efectiva y atractiva. En la mayoría de las situaciones, la institución ya posee una LAN cableada con servidores y algunas estaciones de trabajo de escritorio; en este caso, LAN inalámbrica es una ampliación o extensión de la LAN existente.

En la Figura 9.1.1 se muestra una configuración sencilla de LAN inalámbrica, típica en muchos entornos. En la parte inferior de dicha figura hay una LAN troncal cableada de 100 Mbps que conecta servidores, estaciones de trabajo y uno o más puentes o routers que comunican con otras redes. En dicha figura hay un módulo de control (CM) que tiene las funciones de:

- Interfaz ente la LAN inalámbrica y la LAN troncal cableada: actúa como puente o router para la conexión física y lógica.

- Con los sistemas finales: tiene instalado un software de control de acceso como, por ejemplo, un esquema de sondeo o uno de paso de testigo, para regular el acceso de los sistemas finales. En la Figura 9.1.1 los sistemas finales son los que están dentro del rectángulo.

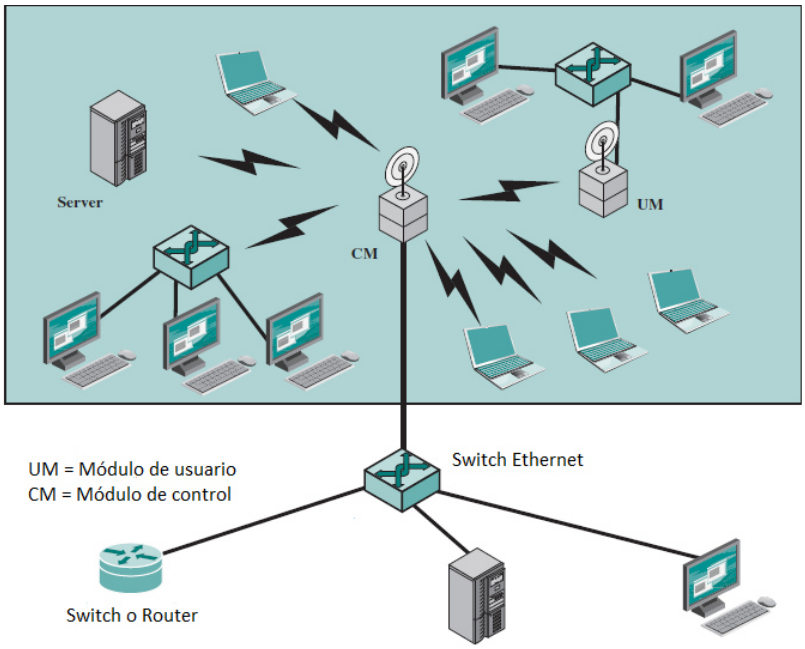

Figura 9.1.1: Red LAN inalámbrica de celda única

Debe destacarse que los sistemas finales de la LAN inalámbrica son elementos independientes como estaciones de trabajo, servidores, switches y, además, pueden ser uno o más módulos de usuario (UM) que controlan, a su vez, redes LAN cableadas que también forman parte de la LAN inalámbrica. La configuración mostrada en la Figura 9.9.1 se denomina LAN inalámbrica de celda única, porque todos los sistemas finales inalámbricos se encuentran en el dominio de un único módulo de control.

Otra configuración común es una LAN inalámbrica de celdas múltiples como se muestra en la Figura 9.1.2. En este caso existen varios módulos de control interconectados por una LAN cableada. Cada módulo de control da servicio a varios sistemas finales inalámbricos dentro de su rango de transmisión. Este es el caso de la LAN de infrarrojos cuya transmisión está limitada a una sola habitación, por lo que se necesita una celda en cada habitación de un edifico donde hay varias oficinas con soporte inalámbrico.

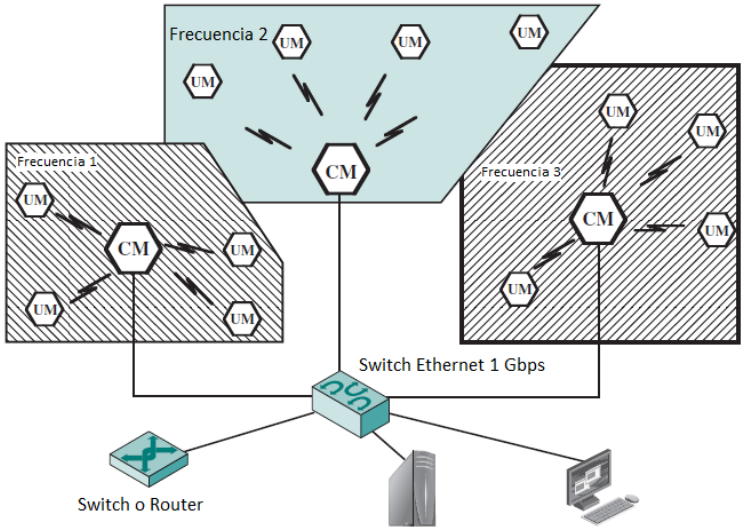

Figura 9.1.2: Red LAN Inalámbrica de celdas múltiples

Acceso nómada

El acceso nómada proporciona un enlace inalámbrico entre un switch de una LAN y un terminal de datos móvil equipado con una antena, como una notebook. Un ejemplo de la utilidad de este tipo de conexiones es posibilitar a un empleado que vuelve de un viaje la transferencia de datos desde un computador personal portátil a un servidor en la oficina. El acceso nómada resulta útil también en un entorno amplio, como un campus universitario o un centro financiero de un grupo de edificios. En ambos casos, los usuarios se pueden desplazar con sus computadores portátiles y pueden desear conectarse con los servidores de una LAN inalámbrica desde distintos lugares. Inclusive en nuestra FACET, alumnos, docentes, investigadores y cuerpo no docente tienen la posibilidad de conectarse en forma inalámbrica con sus celulares y de esta forma acceder a internet.

Red ad hoc

Una red ad hoc es una red entre iguales (sin servidor central) establecida temporalmente para satisfacer alguna necesidad inmediata. Por ejemplo, un grupo de empleados, cada uno con su notebook, puede reunirse para una cita de negocios o para una conferencia, conectando entre sí sus dispositivos en una red temporal sólo durante la reunión.

En la Figura 9.2.1 se sugieren las diferencias entre una LAN inalámbrica ad hoc y una LAN inalámbrica que proporciona ampliaciones de LAN y acceso nómada. En el segundo caso, la LAN inalámbrica presenta una infraestructura estacionaria consistente en una o más celdas con un módulo de control para cada una; dentro de cada celda pueden existir varios sistemas finales estacionarios. Las estaciones nómadas se pueden desplazar de una celda a otra. Por el contrario, en una red LAN ad hoc no existe infraestructura; más aún, muchas estaciones localizadas en el mismo dominio se pueden auto configurar dinámicamente para formar una red temporalmente.

9.2. Requisitos de las LAN Inalámbricas

Una LAN inalámbrica debe cumplir los mismos requisitos típicos de cualquier otra red LAN, incluyendo alta capacidad, cobertura de pequeñas distancias, conectividad total entre las estaciones conectadas y capacidad de difusión. Además, existe un conjunto de necesidades específicas para entornos de LAN inalámbricas. Entre las más importantes se encuentran las siguientes:

- Rendimiento: el protocolo de control de acceso al medio debería hacer un uso tan eficiente como fuera posible del medio aéreo para maximizar la capacidad de utilización del mismo.

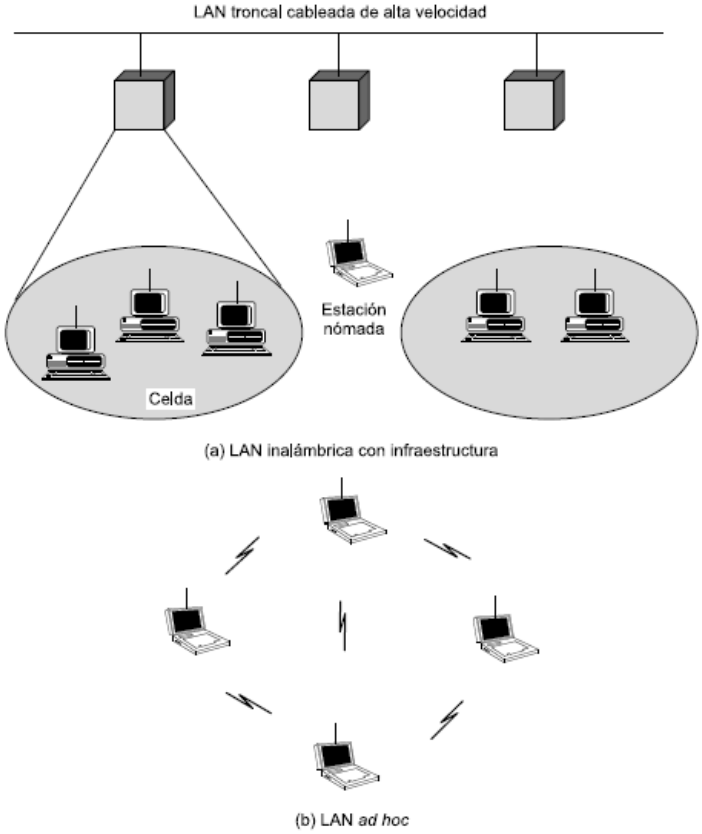

Figura 9.2.1: Configuración de redes inalámbricas

- Número de estaciones: las LAN inalámbricas pueden necesitar dar soporte a cientos de estaciones mediante el uso de varias celdas.

- Conexión a la LAN troncal: en la mayoría de los casos es necesaria la interconexión con estaciones situadas en una LAN troncal cableada. En el caso de LAN inalámbricas con infraestructura, esto se consigue fácilmente a través del uso de módulos de control que conectan con ambos tipos de LAN. También puede ser necesario dar soporte a usuarios móviles y redes inalámbricas ad hoc.

- Área de servicio: una superficie de cobertura para una red LAN inalámbrica tiene un diámetro típico de entre 100 y 300 metros.

- Consumo de batería: los usuarios móviles utilizan estaciones de trabajo con batería que necesitan tener una larga vida cuando se usan con adaptadores sin cable. Esto sugiere que resulta inapropiado un protocolo MAC que requiera que las estaciones móviles supervisen constantemente el enlace con los puntos de acceso o realicen comunicaciones frecuentes con una estación base.

- Robustez en la transmisión y seguridad: a menos que exista un diseño apropiado, una LAN inalámbrica está expuesta a sufrir interferencias y escuchas. El diseño de una LAN inalámbrica debe permitir transmisiones confiables incluso en entornos ruidosos y debe ofrecer cierto nivel de seguridad contra escuchas.

- Funcionamiento de redes cercanas: a medida que crece el uso de las LAN inalámbricas, es probable que dos o más de estas redes operen en la misma o en alguna zona en que sea posible la interferencia entre ellas. Estas interferencias pueden frustrar el normal funcionamiento del algoritmo MAC y pueden permitir accesos no autorizados a una LAN particular.

- Funcionamiento sin licencia: los usuarios podrían preferir adquirir y trabajar sobre LAN inalámbricas que no precisan de una licencia para la banda de frecuencia usada por la red.

- Traspasos/Itinerancias: el protocolo MAC usado en LAN inalámbricas debería permitir a las estaciones móviles desplazarse de una celda a otra.

- Configuración dinámica: los aspectos de direccionamiento MAC y de gestión de red de la LAN deberían permitir la inserción, eliminación y traslado dinámicos y automáticos de sistemas finales sin afectar a otros usuarios.

9.3. Tecnología de LAN Inalámbrica

Las LAN inalámbricas se clasifican generalmente de acuerdo con la técnica de transmisión usada. Todas las LAN actuales se encuentran dentro de una de las siguientes categorías:

- LAN de infrarrojos (IR). Una celda individual en una LAN IR está limitada a una sola habitación dado que la luz infrarroja no es capaz de atravesar muros opacos.

- LAN de espectro expandido. Este tipo de LAN hace uso de tecnologías de transmisión de espectro expandido. En la mayoría de los casos estas LAN operan en las bandas ISM (industria, ciencia y medicina), de modo que no se necesita licencia FCC para su utilización en los Estados Unidos.

- Microondas de banda estrecha. Estas LAN operan en el rango de las microondas, pero no hacen uso de espectro ensanchado. Algunos de estos productos operan a frecuencias para las que es necesario licencia FCC, mientras que otras lo hacen en alguna de las bandas ISM.

En la Tabla 9.3.1 se resumen algunas de las características principales de estas tres tecnologías.

Tabla 9.3.1: Comparación de tecnologías inalámbricas

	Infrarrojos		**Espectro expandido**		**Radio**
	Infrarrojos difusos	**Infrarrojos de haz directo**	**Salto de frecuencia**	**Secuencia directa**	**Microondas de banda estrecha**
Velocidad [Mbps]	1 - 4	1 - 10	1 - 3	2 - 50	10 -20
Movilidad	Estacionario/ móvil	Estacionario con línea de vista	Móvil	Estacionario/móvil	
Alcance [m]	15 - 60	25	30 - 100	30 - 250	10 - 40
Detectabilidad	Despreciable		Pequeña		Alguna
Longitud de onda/frecuencia	λ: 800 – 900 nm		902 - 928 MHz 2,4 -2,4835 GHz 5,725 - 5,85 GHz		902 - 928 MHz 5,2 - 5,775 GHz 18,825-19,205 GHz
Técnica de modulación	ASK		FSK	QPSK	FS/QPSK
Potencia radiada			< 1 W		25 mW
Método de acceso	CSMA	Anillo con paso de testigo, CSMA	CSMA		Reserva ALOHA, CSMA
Necesidad de licencia	No		No		Sí, a menos que sea ISM

9.3.1. Redes LAN de Infrarrojos

Los dos espectros más usados para las LAN inalámbricas son el ocupado por las microondas de radio (espectro expandido) y transmisión en banda estrecha e infrarrojos.

Ventajas del Infrarrojo sobre Microondas

- Espectro ilimitado. El espectro de infrarrojos es virtualmente ilimitado, lo que ofrece la posibilidad de alcanzar velocidades de datos extremadamente altas.

- No está regulado su uso. El espectro de infrarrojos no se encuentra regulado a nivel internacional, es decir, es de uso libre. Esto no es así para las microondas.

- Reflexión difusa. Tiene algunas de las propiedades de la luz visible como es la difusión difusa en objetos de color, siendo así posible utilizar la reflexión en el techo para proporcionar cobertura de señal a toda una habitación.

- No atraviesa muros u objetos opacos. Esta característica presenta dos ventajas: es más fácil preservar la seguridad de la información que las microondas y en cada habitación de un edificio puede funcionar una instalación de infrarrojos aislada sin interferencias, posibilitando así la construcción de redes LAN con infrarrojos muy grandes.

- Equipos de bajo costo. Al usar modulación de amplitud, los detectores de infrarrojos solo deben detectar la amplitud de las señales ópticas (pulsos de señal), mientras que la mayoría de los receptores de microondas precisan detectar la frecuencia o la fase.

Desventajas del Infrarrojo

- Radiación de luz externa a la red. La luz solar como la artificial contiene radiación de infrarrojos que se manifiesta como en forma de ruido en el receptor, lo que obliga a utilizar transmisiones de alta potencia, lo que limita el alcance de la señal. Sin embargo, los incrementos de potencia de la señal deben ser limitados por dos factores: posibles daños en los ojos y consumo excesivo de potencia.

Técnicas de Transmisión en Infrarrojos

Existen tres técnicas alternativas que se usan comúnmente para la transmisión infrarroja de datos: direccional, omnidireccional, o bien, reflejada por el techo.

- Transmisión direccional. Se usan para construir enlaces punto a punto. El alcance del enlace puede llegar hasta una distancia de varios kilómetros, dependiendo de la potencia de emisión y el grado de enfoque. Si bien, este tipo de enlaces no se usa para la implementación de LAN inalámbricas, sí se puede usar para interconectar dos LAN que está en dos edificios mediante el uso de puentes o routers entre los que haya una línea de vista.

- Configuración omnidireccional. Para este tipo de configuración es necesario la existencia de una estación base que se encuentra en la línea de vista de todas las estaciones que conforman la LAN. Generalmente, esta estación se ubica en el techo que, al reflejar la señal, actúa como repetidor multipunto. Por otro lado, el transceptor de cada estación emite un haz direccional que apunta a la estación base localizada en el techo.

- Configuración de difusión. En este caso, todos los transmisores de infrarrojos están enfocados hacia un punto en un techo reflectante. La radiación infrarroja que llega al techo es reflejada omnidireccionalmente y recogida por todos los receptores de la zona.

9.3.2. Redes de Espectro Expandido

Las LAN inalámbricas de mayor aplicación en la actualidad son las que utilizan técnicas de espectro expandido.

Configuración

Exceptuando el caso de oficinas de espacio reducido, una LAN inalámbrica de espectro expandido hace uso de una disposición de celdas múltiples como la ilustrada en la Figura 9.1.2. Para evitar interferencias entre las celdas adyacentes, se utilizan diferentes frecuencias dentro de la misma banda.

Dentro de cada celda puede usarse una topología basada en un concentrador, o bien, una entre pares o peer to peer. En una topología basada en un concentrador, como

la indicada en la Figura 9.2.1(a), éste suele ubicarse en el techo y conectarse a una LAN cableada troncal para proporcionar conectividad entre las estaciones conectadas a las diversas redes locales, ya sea cableadas o inalámbricas pertenecientes a otras celdas. El concentrador puede también controlar el acceso actuando como un repetidor multipunto. En este caso, todas las estaciones de la celda transmiten únicamente hacia el concentrador y reciben exclusivamente de él. Alternativamente, y con independencia del mecanismo de control de acceso, cada estación puede difundir usando una antena omnidireccional, de tal forma que le resto de las estaciones de la celda pueden recibir la transmisión. Esto último se corresponde con una configuración lógica en bus.

Otra función del concentrador es el traspaso automático de las estaciones móviles. En cualquier instante, una serie de estaciones se encuentran asignadas a un concentrador dado de acuerdo con un criterio de proximidad. En el momento en que el concentrador detecta que una señal se debilita, traspasa la estación automáticamente al concentrador adyacente más próximo.

En una topología entre iguales no existe concentrador alguno (Figura 9.2.1(b)), utilizándose algoritmos MAC como CSMA para controlar el acceso. Esta topología es apropiada para redes LAN ad-hoc. Por último, la mayoría de las LAN de espectro expandido operan en la banda ISM, no necesitando contar con licencia.

9.3.3. Redes LAN de Microondas de Banda Estrecha

El término microondas de banda estrecha se refiere al uso de una banda de frecuencias de microondas de radio para la transmisión de la señal, siendo esta banda relativamente estrecha, con un ancho suficiente para contener la señal. Las LAN de Microondas de banda estrecha pueden operar en bandas que requieren licencia y otras que no.

- Banda estrecha con licencia. Generalmente, un esquema de banda estrecha hace uso de una configuración en celdas como la mostrada por la Figura 9.1.2. Las celdas adyacentes utilizan bandas de frecuencias no solapadas dentro de una banda de 18 GHz. Una ventaja de las LAN de banda estrecha con licencia es que garantizan una comunicación ausente de interferencias.

- Banda estrecha sin licencia. Utilizan la banda de los 5,8 GHz destinada a ISM (sigla que identifica al sector conformado por la industria, la ciencia y la medicina).

9.4. IEEE 802.11: Arquitectura y Servicios

En 1990, el comité IEEE 802 formó un nuevo grupo de trabajo, IEEE 802.11, específicamente dedicado a las WLAN, con el objetivo de desarrollar un protocolo con especificaciones para la capa MAC y la capa física. Desde ese momento, la demanda de WLAN, a diferentes frecuencias y las tasas de datos, ha explotado. Manteniendo el ritmo de esta demanda, el grupo de trabajo IEEE 802.11 ha emitido una lista de estándares en constante expansión. La Tabla 9.4.1 define brevemente los términos clave utilizados en el estándar IEEE 802.11:

Tabla 9.4.1: Terminología 802.11

Denominación	Descripción
Punto de Acceso (AP)	Cualquier entidad que tenga la funcionalidad de una estación y proporcione acceso al sistema de distribución en forma inalámbrica a las estaciones asociadas.
Conjunto Básico de Servicios (BSS)	Conjunto de estaciones controladas por una sola función de coordinación que compiten por el mismo medio compartido.
Función de coordinación	Función lógica que determina cuándo una estación funcionando dentro de un BSS tiene permiso para transmitir y puede recibir PDU.
Sistema de Distribución (DS)	Sistema que interconecta un conjunto de BSS y LAN y, al integrarlos en la comunicación, crea un ESS.
Conjunto Extendido de Servicios (ESS)	Conjunto de uno o más BSS interconectados y LAN integradas que aparece como un único BSS en la capa LLC de cualquier estación asociada a uno de tales BSS.
Unidad de Datos del Protocolo MAC (MPDU)	Unidad de datos que intercambian las entidades MAC paritarias usando los servicios de la capa física.
Unidad de Datos del Servicio MAC (MSDU)	Información entregada como una unidad entre usuarios MAC.
Estación	Cualquier dispositivo que contenga capas físicas y MAC compatibles con IEEE 802.11

La alianza wifi

Aunque los productos 802.11 se basan en los mismos estándares, siempre hay un preocuparse si los productos de diferentes proveedores interoperarán con éxito. Para satisfacer esta preocupación, la Wireless Ethernet Compatibility Alliance (WECA), un Consorcio de la industria, se formó en 1999. Esta organización, posteriormente renombrada Wi-Fi (Wireless Fidelity) Alliance, creó un conjunto de pruebas para certificar la interoperabilidad para productos 802.11.

9.4.1. Arquitectura

En la Figura 9.4.1.1 se ilustra el modelo desarrollado por el grupo de trabajo IEEE 802.11. El componente elemental de una LAN inalámbrica es un Conjunto Básico de Servicios o BSS (Basic Service Set) consistente en un número de estaciones que ejecutan el mismo protocolo MAC y compiten por el acceso al mismo medio inalámbrico compartido. Un BSS puede funcionar aisladamente, o bien, estar conectado a un Sistema Troncal de Distribución o DS (Distribution System) a través de un Punto de Acceso o AP (Access Point) que efectúa las funciones de puente. Éste último tiene las mismas funciones que las del Módulo de Control (CM) definido en la sección anterior.

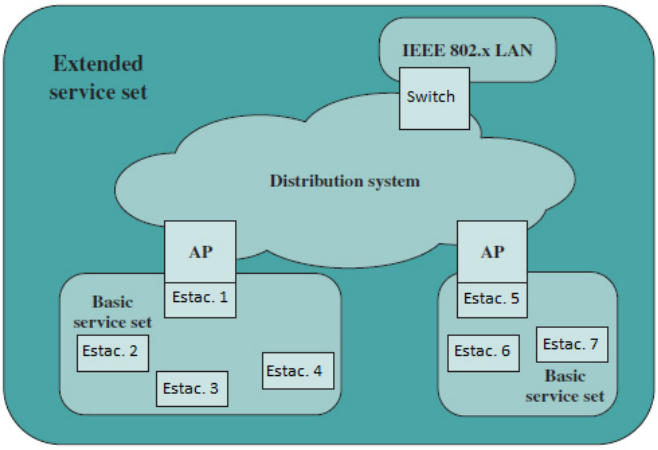

Figura 9.4.1.1: Arquitectura 802.11

El protocolo MAC puede estar completamente distribuido, o bien, estar controlado por una función central de coordinación ubicada en el punto de acceso. Generalmente, el BSS se corresponde con lo que en la bibliografía es referido como celda. Por otro lado, el DS puede ser un switch, una red cableada tradicional o una red inalámbrica.

La configuración más simple posible es la mostrada en la Figura 9.4.1.1, en la que cada estación pertenece a un BSS aislado. Esto es, cada estación se encuentra dentro de un conjunto de estaciones que pertenecen al mismo BSS. Es igualmente posible que exista un solapamiento entre dos BSS, de manera que una estación podría formar parte de más de un BSS. Además, la asociación entre una estación y un BSS es dinámica, puesto que una estación puede apagarse, salirse de la distancia máxima permitida o incorporarse de nuevo.

Un Conjunto Extendido de Servicios o ESS (Extended Service Set) consiste en dos o más BSS interconectados mediante un DS. Este último es, por lo general, una LAN cableada troncal, aunque puede tratarse de cualquier red de comunicaciones. El conjunto extendido de servicios (ESS) aparece a nivel de control de enlace lógico (LLC) como única red LAN lógica.

En la Figura 9.4.1.1 se indica que un AP se implementa formando parte de una estación. Ésta funciona como estación propiamente dicha y, además, contiene el hardware y software del AP que proporciona el acceso al DS a través de los servicios de distribución. La integración de una arquitectura 802.11 con una red cableada tradicional se realiza a través de un switch o router que, además, debe contener el software que conecta lógicamente a la LAN cableada con el DS.

9.4.2. Servicios

La normativa IEEE 802.11 define nueve servicios que deben ser proporcionados por una red inalámbrica para proporcionar una funcionalidad equivalente a la inherente a una LAN cableada tradicional. En la Tabla 9.4.2 se enumeran estos servicios y se indican dos formas de categorizarlos.

Tabla 9.4.2.1: Servicios 802.11

Servicio	Proveedor	Usado para dar soporte a:
Asociación	Sistema de distribución	Entrega de MSDU
Autenticación	Estación	Acceso a la LAN y seguridad
Fin de la autenticación	Estación	Acceso a la LAN y seguridad
Disociación	Sistema de distribución	Entrega de MSDU
Distribución	Sistema de distribución	Entrega de MSDU
Integración	Sistema de distribución	Entrega de MSDU
Entrega de MSDU	Estación	Entrega de MSDU
Privacidad	Estación	Acceso a la LAN y seguridad
Reasociación	Sistema de distribución	Entrega de MSDU

Descripción de los servicios detallados en la Tabla 9.4.2.1

1. El proveedor de estos servicios puede ser tanto la estación como el DS. Los servicios de la estación son implementados en cada estación IEEE 802.11, incluyendo la estación que constituye el AP. Los servicios de distribución son proporcionados entre BSS diferentes y deben ser implementados en un AP o en cualquier otro dispositivo de propósito específico conectado al sistema de distribución.

2. Tres de los servicios enumerados se emplean para controlar el acceso a una LAN IEEE 802.11 y para proporcionar confidencialidad. Los seis servicios restantes dan soporte a la entrega de Unidades de Datos de Servicio MAC o MSDU (MAC Service Data Units) entre estaciones. Una MSDU es un bloque de datos que el usuario MAC le pasa a la capa MAC, generalmente en la forma de una PDU LLC. Si una MSDU es demasiado grande para ser transmitida en una sola trama MAC, puede ser fragmentada y transmitida en una serie de tramas. La fragmentación se discutirá en la sección Control de Acceso al Medio.

Siguiendo el documento IEEE 802.11, a continuación, se discutirá los servicios de acuerdo con un orden que clarifica el funcionamiento de una red ESS IEEE 802.11. La entrega de MSDU, que constituye el servicio básico, ya ha sido mencionada.

Distribución de Mensajes dentro de un DS

Los dos servicios implicados en la distribución de mensajes dentro de un DS son la distribución y la integración.

- Servicio de distribución. Es el servicio primario utilizado por las estaciones para intercambiar tramas MAC cuando la trama debe atravesar el DS para pasar a una estación en un BSS a otra estación en un BSS diferente. Por ejemplo, considerando la Figura 9.4.1.1, supóngase que una trama es transmitida desde la estación 2 (EST2) hasta la estación 7 (EST7). La trama se envía desde la estación EST2 hasta la estación EST1, que es el AP para este BSS. A continuación, el AP entrega la trama al DS, que se encarga de encaminarla hasta el AP asociado a la estación EST5 en el BSS de destino. La estación EST5 recibe la trama y la retransmite a la estación EST7. Las cuestiones acerca de cómo se transporta el mensaje a través del DS caen fuera del alcance del estándar IEEE 802.11.

Si las dos estaciones que establecen la comunicación se encuentran dentro del mismo BSS, entonces el servicio de distribución pasa, lógicamente, a través del AP de dicho BSS.

- Servicio de integración. Permite la transferencia de datos entre una estación situada en una LAN IEEE 802.11 y otra estación en una LAN IEEE 802.x que se encuentre integrada con la primera. El término integrada hace referencia a una LAN cableada que esté físicamente conectada con el DS y cuyas estaciones puedan conectarse de forma lógica a una LAN IEEE 802.11 a través del servicio de integración. Este servicio es el encargado de llevar a cabo la traducción de direcciones y cualquier otra conversión lógica requerida para el intercambio de datos.

Servicios Relacionados con la Asociación

El principal objetivo de la capa MAC es la transferencia de MSDU entre entidades MAC. Esta tarea es desempeñada por el servicio de distribución. Para que este servicio pueda llevar a cabo sus funciones, necesita disponer de información acerca de las estaciones que se encuentran dentro del ESS. Esta información está proporcionada por los servicios relacionados con la asociación. Antes de que el servicio de distribución pueda entregar o aceptar datos de una estación, ésta debe estar asociada. Antes de explorar la noción de asociación es necesario describir el concepto de movilidad. El estándar define tres tipos de transiciones basadas en la movilidad:

- Sin transición. Una estación de este tipo es estacionaria o se desplaza únicamente dentro del rango de comunicación directa de las estaciones conectadas a un único BSS.

- Transición BSS. Se define como el desplazamiento de una estación desde un BSS hasta otro BSS destino ubicado en el mismo ESS. En este caso, la entrega de datos a la estación necesita que la función de direccionamiento sea capaz de reconocer la nueva localización de la estación.

- Transición ESS. Se define como el desplazamiento de una estación desde un BSS ubicado en un determinado ESS hasta otro BSS perteneciente a un ESS diferente del primero. Esta situación se soporta únicamente debido a que la estación tiene libertad para moverse. Sin embargo, el mantenimiento de conexiones de capas altas sustentadas sobre IEEE 802.11 no puede garantizarse. De hecho, es probable que se produzca una interrupción del servicio.

Para entregar un mensaje dentro de un DS, el servicio de distribución necesita conocer dónde se encuentra ubicada la estación destino. Específicamente, el DS necesita conocer la identidad del AP al que el mensaje deberá ser entregado con el fin de que tal mensaje alcance la estación destino. Para satisfacer este requisito, una estación debe mantener una asociación con el AP dentro de su BSS actual. Existen tres servicios vinculados con este requisito:

- Asociación. Establece una asociación inicial entre una estación y un AP. La identidad y dirección de una estación debe conocerse antes de que la misma pueda transmitir o recibir tramas en una LAN inalámbrica. Para ello, una estación debe

establecer una asociación con un AP perteneciente a un BSS particular. A partir de entonces, el AP puede comunicar esta información a otros AP dentro del ESS con el objeto de facilitar el ruteo y la entrega de tramas.

- Reasociación. Permite que una asociación previamente establecida sea transferida desde un AP hasta otro, haciendo así posible que una estación móvil pueda desplazarse desde un BSS hasta otro.

- Disociación. Constituye una notificación, ya sea, de una estación o de un AP, de que una asociación existente deja de tener validez. Una estación debería proporcionar este aviso antes de abandonar un ESS o apagarse. No obstante, las funciones de gestión MAC incluyen mecanismos para protegerse frente a estaciones que desaparezcan sin emitir esta notificación.

Servicios de Acceso y Privacidad

Existen dos características de una LAN cableada que son inherentes a una LAN inalámbrica:

1. Para poder transmitir en una LAN cableada, una estación debe estar físicamente conectada a la misma. Sin embargo, en el caso de una LAN inalámbrica, cualquier estación situada dentro de una celda junto con otros dispositivos de la red puede transmitir. Existe, en cierto sentido, una forma de autenticación en el contexto de una red cableada: se precisa una acción positiva y presumiblemente observable para conectar una estación a una LAN cableada.

2. Análogamente, para poder recibir una transmisión desde una estación que forma parte de una LAN cableada, la estación receptora debe igualmente estar conectada al medio. Sin embargo, en el caso de una LAN inalámbrica cualquier estación dentro de una celda puede recibir. De esta forma, una LAN cableada proporciona cierto grado de privacidad, limitando la recepción de datos únicamente a aquellas estaciones conectadas a la LAN.

El estándar IEEE 802.11 define tres servicios que proporcionan estas dos características a una LAN inalámbrica:

- Autenticación. Es utilizada para que una estación pueda comunicar su identidad a otras estaciones. En una LAN cableada se asume, por lo general, que el acceso a una conexión física lleva aparejado la potestad de conectar a la LAN. Esta hipótesis no es válida en un entorno inalámbrico, en el que la conectividad se adquiere simplemente poseyendo una antena que se encuentre sintonizada adecuadamente. El servicio de autenticación es utilizado por las estaciones para establecer su identidad con otras con las que se desee comunicar. El estándar IEEE 802.11 da soporte a varios esquemas autenticación y permite que la funcionalidad de los mismos pueda extenderse. El estándar no impone ningún esquema de autenticación concreto, que podría ir desde algún procedimiento relativamente inseguro hasta esquemas de cifrado de llave pública. Sin embargo, el estándar IEEE 802.11 precisa de una autenticación correcta y aceptada mutuamente antes de que una estación pueda establecer una asociación con un AP.

- Fin de la autenticación. Este servicio es invocado siempre que se vaya a dar por finalizada una autenticación existente.

- Privacidad. Se utiliza para asegurar que los contenidos de los mensajes no sean leídos por alguien diferente al receptor legítimo. El estándar incluye el uso opcional de mecanismos de cifrado para asegurar la privacidad.

9.5. Control de Acceso al Medio en IEEE 802.11

La capa MAC de IEEE 802.11 cubre tres aspectos funcionales: la entrega confiable de datos, el control de acceso y la seguridad.

9.5.1. Entrega Confiable de Datos

Al igual que cualquier otra red inalámbrica, una LAN inalámbrica que utilice las capas física y MAC especificadas en el estándar IEEE 802.11 está sujeta a una considerable falta de confiabilidad. El ruido, las interferencias y otras perturbaciones repercuten en la pérdida de un número significativo de tramas. Incluso, disponiendo de códigos correctores errores, es posible que muchas tramas MAC no sean recibidas apropiadamente. Se puede hacer frente a esta situación con mecanismos que proporcionen confiabilidad en capas más altas, como TCP. Sin embargo, los temporizadores utilizados para la retransmisión en capas superiores son, por lo general, del orden de segundos. Es, por tanto, más eficiente abordar el problema de los errores en el nivel MAC. Con esta finalidad, el estándar IEEE 802.11 incluye un protocolo de intercambio de tramas. Cuando una estación recibe una trama de datos de otra estación, devuelve una trama de confirmación (ACK) a la estación origen. Si la fuente no recibe la confirmación en un intervalo corto de tiempo, ya sea porque la trama de datos resultó dañada, o porque la trama ACK de retorno fue la que se dañó, la fuente retransmite la trama.

De esta forma, el mecanismo básico de transferencia de datos IEEE 802.11 implica un intercambio de dos tramas. Para mejorar aún más la confiabilidad, es posible utilizar un intercambio de cuatro tramas. En este esquema, la fuente emite inicialmente una trama de solicitud para enviar RTS (Request To Send) que es un pedido para enviar datos un hacia un destino. La estación destino responde con una trama de permiso para enviar CTS (Clear to Send). Tras recibir la trama CTS, la fuente emite la trama de datos y el destino responde con una confirmación (ACK). La trama RTS alerta a todas las estaciones que se encuentran dentro del rango de recepción de la fuente de que una transmisión está en curso. El resto de las estaciones se abstiene de transmitir con el objeto de evitar que se produzca una colisión entre dos tramas transmitidas al mismo tiempo. Análogamente, la trama alerta a todas las estaciones que están en el rango de recepción del destino de que se va a producir un intercambio. Aunque la parte RTS/CTS del protocolo de intercambio es una función que es provista por la capa MAC, es posible deshabilitarla.

9.5.2. Control de Acceso

El grupo de trabajo IEEE 802.11 ha considerado dos tipos de propuestas para algoritmos MAC: protocolos de acceso distribuido y de acceso centralizado.

- Protocolos de Acceso Distribuido. De la misma forma que en el caso de una LAN de difusión como Ethernet, la decisión para transmitir se distribuye sobre todas las

estaciones usando un mecanismo de detección de portadora. Este esquema de transmisión es apropiado en el caso de una red ad-hoc de estaciones pares, aunque puede ser también interesante para otras configuraciones de LAN inalámbricas cuyas transmisiones sean del tipo de ráfagas.

- Protocolos de Acceso Centralizado. Imponen una regulación de la transmisión por una autoridad central que toma las decisiones. Este esquema centralizado es más apropiado para configuraciones en las que una serie de estaciones inalámbricas se interconectan entre sí y, además, con una estación base que actúa como router hacia una LAN troncal cablead a. También es especialmente útil cuando parte de los datos tiene algún requisito de tiempo real o alta prioridad.

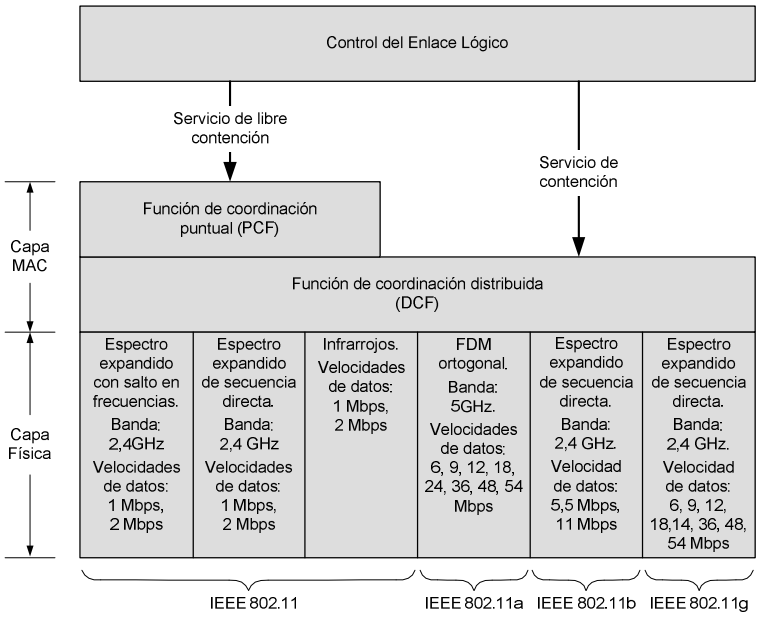

Figura 9.5.2.1: Arquitectura de protocolos 802.11

La propuesta de IEEE 802.11 es un algoritmo MAC denominado DFWMAC (Distributed Foundation Wireless MAC) que proporciona un mecanismo de control de acceso distribuido sobre el que se ubica un control centralizado opcional. En la figura 9.5.2.1 se ilustra esta arquitectura. La subcapa MAC inferior es la Función de Coordinación Distribuida o DCF (Ditributed Coordination Function). La DCF utiliza un algoritmo de contención para proporcionar acceso a la totalidad del tráfico. El tráfico asincrónico ordinario hace uso directamente de la DCF. La Función de Coordinación Puntual o PCF (Point Coordination Function) es un algoritmo MAC centralizado usado para ofrecer un servicio libre de contención. La PCF se ubica justo por encima de DCF y utiliza las características de ésta para asegurar el acceso para sus usuarios. A continuación, se estudian estas dos subcapas.

Función de Coordinación Distribuida

La subcapa DCF hace uso de un sencillo algoritmo CSMA (Carrier Sense Multiple Access). Una estación escucha el medio cuando dispone de una trama para transmitir. Si el medio esta libre, la estación puede transmitir; en otro caso, la estación debe

esperar antes de transmitir hasta que se complete la transmisión en curso. La DCF no incluye una función de detección de colisiones (como CSMA/CD) porque esta no resulta práctica en una red inalámbrica. El rango dinámico del nivel de las señales en el medio inalámbrico es muy grande; esto es: una estación que transmite no puede distinguir de manera efectiva si una señal entrante muy débil colisiona o no con su propia transmisión, simplemente porque el nivel de la señal entrante es de un nivel extremadamente bajo respecto del de la señal emitida.

Para asegurar un funcionamiento adecuado y equitativo de este algoritmo, la DCF incluye un conjunto de retardos que se ordenan de acuerdo con un esquema de prioridades. Se comenzará considerando un retardo simple denominado Espacio entre Tramas o IFS (InterFrame Space).

De hecho, existen tres valores diferentes para el IFS, pero el algoritmo se explica mejor ignorando inicialmente este detalle. Usando un IFS, las reglas de acceso CSMA son las siguientes (Figura 9.5.2.2):

1. Una estación que dispone de una trama lista para ser transmitida sondea el medio. Si este se encuentra libre, la estación espera para verificar si el medio permanece libre durante una cantidad de tiempo igual al IFS. Si es así la estación puede transmitir inmediatamente.

2. Si el medio está ocupado (ya sea porque la estación lo encuentra inicialmente así o porque este hecho sucede durante el tiempo de espera IFS), la estación pospone la transmisión y continúa monitorizando el medio hasta que la transmisión en curso finalice.

3. Una vez que la transmisión actual haya terminado, la estación espera otro IFS. Si el medio permanece libre durante ese periodo, la estación espera durante una cantidad aleatoria de tiempo y vuelve a sondear el medio de nuevo. Si el medio continúa libre, la estación puede transmitir. Si, por el contrario, el medio queda ocupado durante el periodo de espera, el temporizador de espera se detiene, comenzando de nuevo cuando el medio quede libre.

Para asegurar que el proceso de espera mantenga la estabilidad, se utiliza una espera exponencial binaria que proporciona una forma de manejar cargas elevadas de tráfico. Los intentos repetidos y fallidos de transmitir se traducen en períodos de espera cada vez mayores, hecho éste que ayuda a reducir la carga. En el caso de que este mecanismo no existiera, se podría dar la siguiente situación: dos o más estaciones intentan transmitir al mismo tiempo, produciendo una colisión. Luego ambas intentan retransmitir inmediatamente, causando una nueva colisión. El esquema anterior se refina para permitir que la DCF proporcione un acceso basado en prioridades. Para ello se utiliza un mecanismo simple basado en el uso de tres valores para IFS:

- SIFS (IFS corto, short IFS): es el IFS más pequeño y se utiliza para todas las acciones de respuestas inmediatas, tal como se explica más adelante.

- PIFS (IFS de la función de coordinación puntual, Punctual Coordination Function IFS): se trata de un IFS de tamaño medio, utilizado por el controlador central en el esquema PCF cuando emite un sondeo.

- DIFS (IFS de la función de coordinación distribuida, Distributed Coordination Function IFS): constituye el IFS más grande y se usa como un retardo mínimo para las tramas que compiten por el acceso al medio.

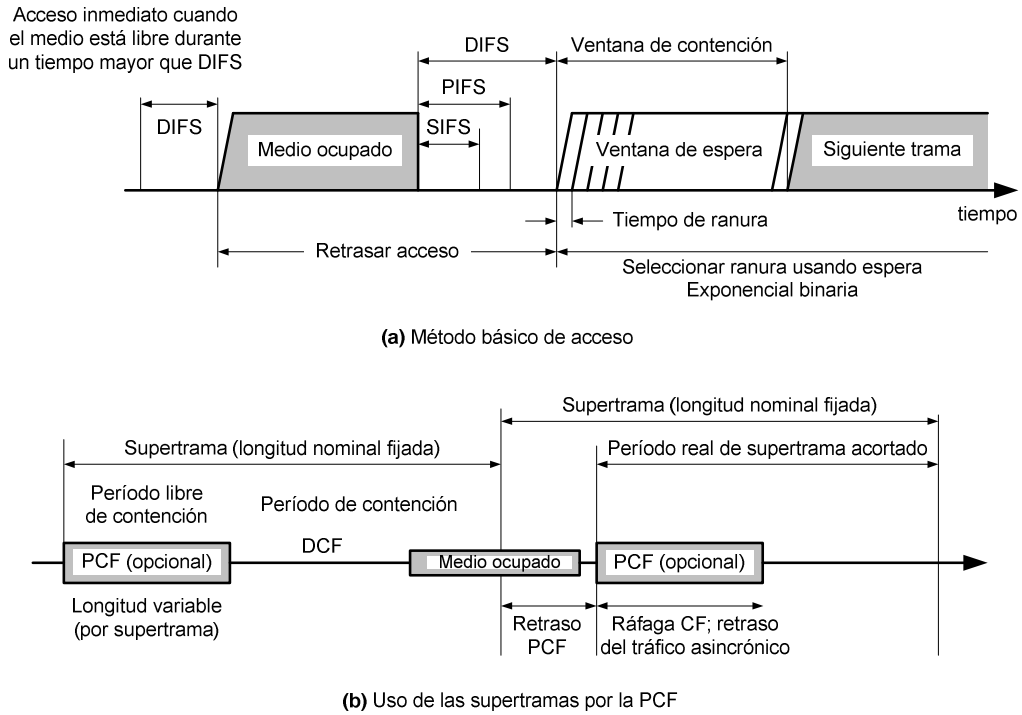

Figura 9.5.2.2: Esquema temporal de eventos MAC 802.11

La Figura 9.5.2.2(a) ilustra el uso de estos valores de tiempo. Considérese primero el caso del SIFS. Cualquier estación que utilice un SIFS para determinar la ocasión de transmitir tiene, en efecto, la prioridad más alta, dado que siempre ganará el acceso antes de que cualquier otra estación que espere una cantidad de tiempo igual a un PIFS o a un DIFS. El uso de SIFS se produce en las siguientes circunstancias:

- Confirmación (ACK). Cuando una estación recibe una trama dirigida exclusivamente a ella (es decir, sin difusión ni multidifusión), ésta responde con una trama ACK tras esperar únicamente un espacio de tiempo igual a un SIFS. Esto tiene dos efectos deseables. En primer lugar, dado que no se utiliza detección de colisiones, la probabilidad de las colisiones es mayor que con CSMA/CD, de forma que la confirmación a nivel MAC proporciona un mecanismo eficiente de recuperación ante colisiones. En segundo lugar, el SIFS puede ser utilizado para proporcionar una entrega eficiente de una PDU correspondiente a un protocolo de nivel LLC que requiera varias tramas MAC.

- Permiso para enviar (CTS). Una estación puede asegurar que su trama de datos se enviará satisfactoriamente si primero emite una pequeña trama de solicitud para enviar (RTS). La estación a quién va dirigida la trama RTS debería responder inmediatamente con una trama CTS si se encuentra preparada para recibir. El resto de las estaciones reciben la trama RTS y se abstienen de usar el medio.

- Respuesta a sondeo (poll response): este punto es explicado posteriormente en la discusión PCF.

El siguiente intervalo IFS en longitud es el PIFS. Éste es utilizado por el controlador central para emisión de sondeos y tiene prioridad sobre el tráfico de contención normal. Obsérvese, sin embargo, que las tramas transmitidas utilizando IFS tienen prioridad sobre un sondeo PCF.

Finalmente, el intervalo DIFS se utiliza para el tráfico ordinario asincrónico.

Función de Coordinación Puntual

PCF es un método de acceso alternativo implementado sobre DCF, cuya función consiste en un sondeo realizado por un elemento central de sondeos (coordinador puntual). El coordinador puntal hace uso de un PIFS cuando emite un sondeo. Dado que un PIFS es más pequeño que un DIFS, el coordinador puntual puede adueñarse del medio y bloquear todo el tráfico asincrónico mientras se emite un sondeo y recibe la respuesta.

Como caso extremo puede considerarse el siguiente escenario posible. Una red inalámbrica se configura de tal manera que una serie de estaciones con tráfico sensible a los retardos se controla por medio del coordinador puntual, mientras que el resto del tráfico compite por el acceso usando CSMA. El coordinador puntual podría emitir consultas a todas las estaciones configuradas para sondeo siguiendo un esquema de turno rotatorio. Cuando se emite un sondeo, la estación consultada puede responder utilizando un SIFS. Si el coordinador puntual recibe una respuesta, entonces emite un nuevo sondeo usando un PIFS. Si no se recibe respuesta alguna durante el tiempo correspondiente al turno, el coordinador emite un sondeo.

Si la disciplina expuesta en el párrafo anterior fuese implementada, el coordinador puntual podría bloquear todo el tráfico asincrónico si más que emitir repetidamente sondeos. Para prevenir la ocurrencia de este hecho se define un intervalo conocido como supertrama. Durante la primera parte de este intervalo, el coordinador puntual emite sondeos a todas las estaciones configuradas para el sondeo siguiendo un esquema de turno rotatorio. A continuación, el coordinador espera un tiempo igual a lo que reste de la supertrama, permitiendo así la existencia de un período de contención asincrónico.

En la Figura 9.5.2.2(b) se ilustra el uso de la supertrama. Al principio de una supertrama, el coordinador puntual puede hacerse con el control opcionalmente y emitir sondeos durante un período de tiempo dado. Este intervalo varía debido al tamaño variable que pueden tener las tramas de respuesta de las estaciones. El tiempo restante de la supertrama queda disponible para el acceso competitivo. Al final del intervalo de supertrama, el coordinador puntual compite por el acceso al medio usando un PIFS. Si el medio se encuentra disponible, el coordinador gana el acceso inmediatamente, siguiendo a continuación una supertrama completa. Sin embargo, el medio puede estar ocupado al final de la supertrama. En este caso, el coordinador puntual debe esperar hasta que el medio quede libre para conseguir el acceso, lo que se traducirá en un período de supertrama más corto para el siguiente ciclo.

9.5.3. Trama MAC

En la Figura 9.5.3.1 se muestra el formato de una trama IEEE 802.11. Este formato general se utiliza para todas las tramas de datos y de control, aunque no todos los campos se utilizan en todos los contextos. Los campos son los siguientes:

- Control de trama (*Frame Control*). Indica el tipo de trama (control, gestión o datos) y proporciona información de control. La información de control indica si la trama proviene o va destinada a un DS, y contiene información de control y relativa a la privacidad.

- ID de duración/conexión (*Duration/ID*). Si se utiliza como un campo de duración, indica el tiempo (en microsegundos) que el canal será reservado para una transmisión satisfactoria de una trama MAC. En algunas tramas de control, este campo contiene el identificador de una asociación o de una conexión.

- Direcciones (*Address 1..4*). El número y significado de los campos direcciones dependen del contexto. Los tipos de direcciones son de la fuente, el destino, la estación transmisora y la estación receptora.

- Control de secuencia (*Sequence Control*): contiene un sub-campo de 4 bits (número de fragmento) utilizado para la fragmentación y el re-ensamblado, y un número de secuencia de 11 bits utilizado para numerar las tramas enviadas entre un transmisor dado y un receptor.

- Cuerpo de la trama (*Body Frame*): contiene una MSDU completa o un fragmento de la misma. La MSDU es una unidad de datos del protocolo LLC o información de control MAC.

- Secuencia de comprobación de trama (*Frame Check Sequence*): se trata de una comprobación de redundancia cíclica de 32 bits.

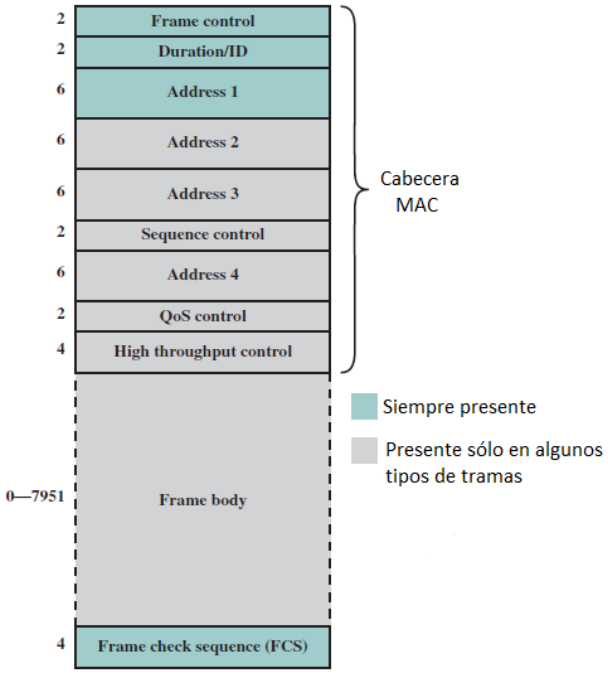

Figura 9.5.3.1: Trama MAC 802.11

A continuación, examinaremos los tres tipos de tramas MAC:

Tramas de control

Las tramas de control prestan servicio a la entrega fiable de tramas de datos. Existen seis subtipos de tramas de control:

- Sondeo de ahorro de energía (PS-Poll, Power Save-Poll): esta trama es enviada por cualquier estación hacia la estación que contiene el punto de acceso (AP). Su objetivo es solicitar al AP que transmita una trama destinada a esta estación que ha sido almacenada en una memoria temporal debido a que la estación se encontraba en modo de ahorro de energía.
- Solicitud para enviar (RTS): se trata de la primera trama en el protocolo de cuatro pasos discutido cuando se trató la entrega fiable de datos al principio de esta sección. La estación que envía este mensaje está alertando a un posible destino, así como al resto de las estaciones dentro del rango de recepción, de que pretende enviar una trama de datos a dicho destino.
- Permiso para enviar (CTS): se trata de la segunda trama en el protocolo de cuatro pasos. Es enviada por la estación de destino hacia la fuente para concederle permiso para emitir una trama de datos.
- Confirmación: proporciona una confirmación del destino hacia la fuente, indicando que los datos, información de gestión o sondeo de ahorro de energía previos han sido recibidos correctamente.
- Fin de periodo libre de contención: anuncia el final de un periodo libre de contenciones que forma parte de la función de coordinación puntual.

- CF-End + CF-Ack: confirmación de la trama CF-End. Esta trama finaliza el periodo libre de contención y libera a las estaciones de las restricciones asociadas con este periodo.

Tramas de datos

Existen ocho subtipos de tramas de datos, organizados en dos grupos. Los primeros cuatro subtipos definen tramas que transportan datos de una capa superior desde la estación origen hasta la estación de destino. Las cuatro tramas de transporte de datos son las siguientes:

- Datos: se trata de la trama de datos más simple. Puede ser utilizada tanto en el periodo de contención como en el periodo libre de contención.
- Datos + CF-Ack: únicamente puede ser enviada durante el periodo libre de contención. Además de transportar datos, esta trama confirma la recepción de otros previamente recibidos.
- Datos + CF-Poll: se utiliza por parte de un coordinador puntual para entregar datos a una estación móvil y para solicitar que ésta envíe una trama de datos que puede haber sido almacenada temporalmente.
- Datos + CF-Ack + CF-Poll: combina en una sola trama las funciones de las tramas Datos + CF-Ack y Datos + CF-Poll.

Los cuatro subtipos restantes de tramas de datos no transportan, en realidad, datos del usuario. La trama conocida como función nula (Null Function) no transporta datos, sondeos o confirmaciones. Se utiliza para transportar el bit de gestión de energía en el campo de control de una trama destinada al AP, indicando así que la estación va a entrar en un estado de operación de baja energía. Las tres tramas restantes (CF-Ack, CF-Poll y CF-Ack + CF-Poll) poseen la misma funcionalidad que los subtipos de tramas de datos correspondientes que se han comentado en la lista anterior (Datos + CF-Ack, Datos + CF-Poll, Datos + CF-Ack + CF-Poll), pero sin transportar datos.

Tramas de gestión

Las tramas de gestión se utilizan para gestionar las comunicaciones entre las estaciones y los puntos de acceso. Las funciones que cubren incluyen la gestión de las asociaciones (solicitud, respuesta, reasociación, disociación y autenticación).

9.5.4. Seguridad

Debido a la naturaleza del medio de transmisión de las redes inalámbricas (el aire), estas son especialmente vulnerables a problemas de seguridad. Mientras que, en las redes cableadas, el acceso necesariamente requiere de un cable físico para de conexión a la red, en una red inalámbrica, los paquetes de información viajan libremente en forma de ondas de radio.

Debido a la naturaleza insegura del medio utilizado, las características de seguridad en las redes inalámbricas se basan especialmente en el control de acceso a la red y en garantizar la privacidad de las comunicaciones.

9.5.4.1.WEP (Wired Equivalent Privacy - Privacidad Equivalente al Cableado)

Es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite.

La idea del WEP es proporcionar a las redes inalámbricas la "privacidad de un cable". El algoritmo WEP se basa en *RC4*[1] y utiliza una clave que deben conocer tanto los clientes como los puntos de acceso (habitualmente se utiliza más de una clave), junto con un vector de iniciación (IV)[2] generado de forma pseudoaleatorio para realizar la encriptación de los datos. Una vez cifrado el texto, además de éste hay que enviar el IV y el checksum, este último independiente de la clave. Para dificultar los ataques al protocolo, el IV se cambia periódicamente. Los tamaños de clave utilizado son 40 y 104 bits, los cuales sumados a los 24 bits del IV, conforman la clave de cifrado de tamaño 64 y 128 bits respectivamente. Además, indicar que estas claves pueden estar en formato decimal, en hexadecimal o en ASCII, en cuyo caso la clave se suele obtener mediante un generador a partir del texto introducido.

El principal problema con la implementación del algoritmo anteriormente descrito es el tamaño de los vectores de iniciación. A pesar de que se pueden generar muchos vectores, la cantidad de tramas que pasan a través de un punto de acceso es muy grande, lo que hace que rápidamente se encuentren dos mensajes con el mismo vector de iniciación, y por lo tanto sea fácil hacerse con la clave. Por lo tanto, es inseguro debido a su implementación. Aumentar los tamaños de las claves de cifrado sólo aumenta el tiempo necesario para romperlo.

9.5.4.2.WPA (Wi-Fi Protected Access, Acceso Protegido Wi-Fi)

El sistema nace para corregir las deficiencias del sistema anterior WEP. WPA implementa la mayoría del estándar IEEE 802.11i, y fue creado como una medida intermedia para ocupar el lugar de WEP mientras 802.11i era finalizado. Por un lado, corrige las deficiencias de encriptación de WEP mediante TKIP, y por otra, utiliza un método de autenticación para el acceso a la red (EAP).

Tipos de WPA

WPA fue diseñado para utilizar un servidor de autenticación (normalmente un servidor RADIUS), que distribuye claves diferentes a cada usuario (a través del protocolo 802.1x); sin embargo, también se puede utilizar en un modo menos seguro de clave pre-compartida (PSK - PreShared Key).

[1] Dentro de la criptografía RC4 o ARC4 es el sistema de cifrado de flujo "stream cipher" más utilizado y se usa en algunos de los protocolos más populares como Transport Layer Security (TLS/SSL) (para proteger el tráfico de Internet) y Wired Equivalent Privacy (WEP)

[2] En criptografía, un vector de inicialización (conocido por sus siglas en inglés IV) es un bloque de bits que es requerido para permitir un cifrado en flujo o un cifrado por bloques, en uno de los modos de cifrado, con un resultado independiente de otros cifrados producidos por la misma clave

La alianza Wi-Fi llama a la versión de clave pre-compartida WPA-Personal y a la versión con autenticación 802.1x/EAP como WPA-Enterprise.

WPA-Personal (WPA-PSK)

Es el sistema más simple de control de acceso WPA, a efectos prácticos tiene la misma dificultad de configuración que WEP, una clave común compartida, sin embargo, la gestión dinámica de claves aumenta notoriamente su nivel de seguridad. PSK se corresponde con las iniciales de Pre-Shared Key y viene a significar clave compartida previamente, es decir, a efectos del cliente basa su seguridad en una contraseña compartida.

WPA-PSK usa una clave de acceso de una longitud entre 8 y 63 caracteres, que es la clave compartida. Al igual que ocurría con WEP, esta clave hay que introducirla en cada una de las estaciones y puntos de acceso de la red inalámbrica. Cualquier estación que se identifique con esta contraseña, tiene acceso a la red.

Las características de WPA-PSK lo definen como el sistema, actualmente, más adecuado para redes de pequeñas oficinas o domésticas, la configuración es muy simple, la seguridad es aceptable y no necesita ningún componente adicional.

Debilidades de WPA-PSK:

La principal debilidad de WPA-PSK es la clave compartida entre estaciones. Cuando un sistema basa su seguridad en una contraseña siempre es susceptible de sufrir un ataque de fuera bruta, es decir ir comprobando contraseñas, aunque dada la longitud de la contraseña y si está bien elegida no debería plantear mayores problemas. Debemos pensar que hay un momento de debilidad cuando la estación establece el diálogo de autenticación. Este diálogo va cifrado con las claves compartidas, y si se entienden entonces se garantiza el acceso y se inicia el uso de claves dinámicas. La debilidad consiste en que conocemos el contenido del paquete de autenticación y conocemos su valor cifrado. Ahora lo que queda es, mediante un proceso de ataque de diccionario o de fuerza bruta, intentar determinar la contraseña.

WPA-Empresarial (WPA-EAP)

En redes corporativas resultan imprescindibles otros mecanismos de control de acceso más versátiles y fáciles de mantener como por ejemplo los usuarios de un sistema identificados con nombre/contraseña o la posesión de un certificado digital. Evidentemente el hardware de un punto de acceso no tiene la capacidad para almacenar y procesar toda esta información por lo que es necesario recurrir a otros elementos de la red cableada para que comprueben unas credenciales. Ahora bien, parece complicado que un cliente se pueda validar ante un componente de la red por cable si todavía no tenemos acceso a la red, parece el problema del huevo y la gallina. En este punto es donde entra en juego el IEEE 802.1X, que describimos a continuación, para permitir el tráfico de validación entre un cliente y una máquina de la red local (RADIUS). Una vez que se ha validado a un cliente es cuando WPA inicia TKIP para utilizar claves dinámicas.

Los clientes WPA tienen que estar configurados para utilizar un sistema concreto de validación que es completamente independiente del punto de acceso. Los sistemas de validación WPA pueden ser, entre otros, EAP-TLS, PEAP, EAP-TTLS

TKIP (Temporary Key Integrity Protocol, Protocolo de Integridad de Claves Temporales)

Utilizado por WPA para mejorar la encriptación, TKIP es también llamado hashing de Clave WEP. WPA incluye mecanismos del estándar emergente 802.11i para mejorar el cifrado de datos inalámbricos. WPA tiene TKIP, que utiliza el mismo algoritmo que WEP, pero construye claves en una forma diferente. TKIP es una solución temporal que soluciona el problema de reutilización de clave de WEP. WEP utiliza periódicamente la misma clave para cifrar los datos. El proceso de TKIP comienza con una clave temporal de 128 bits que es compartida entre los clientes y los Access Point. TKIP combina la clave temporal con la dirección MAC del cliente. Luego agrega un vector de inicialización relativamente largo, de 16 octetos, para producir la clave que cifrará los datos. Este procedimiento asegura que cada estación utilice diferentes "streams" claves para cifrar los datos. El hashing de clave WEP protege a los Vectores de Inicialización (IV's) débiles para que no sean expuestos haciendo hashing del IV por cada paquete.

TKIP utiliza el RC4 para realizar el cifrado, que es lo mismo que el WEP. Sin embargo, una gran diferencia con el WEP es que el TKIP cambia las claves temporales cada 10.000 paquetes. Esto proporciona un método de distribución dinámico, lo que mejora significativamente la seguridad de la red.

EAP (Extensible Authentication Protocol, Protocolo de Autenticación Extensible)

El estándar 802.1X utiliza EAP para la autenticación de usuarios. En realidad, EAP actúa como intermediario entre un solicitante y un motor de validación (RADIUS) permitiendo la comunicación entre ambos.

El proceso de validación está conformado por tres elementos, un solicitante que quiere ser validado mediante unas credenciales, un punto de acceso y un sistema de validación situado en la parte cableada de la red. Para conectarse a la red, el solicitante se identifica mediante unas credenciales que pueden ser un certificado digital, una pareja nombre/usuario u otros datos. Junto con las credenciales, el cliente solicitante tiene que añadir también qué sistema de validación tiene que utilizar. En general EAP actúa de esta forma, recibe una solicitud de validación y la remite a otro sistema que sepa cómo resolverla y que formará parte de la red cableada. De esta forma vemos como el sistema EAP permite un cierto tráfico de datos con la red local para permitir la validación de un solicitante. El punto de acceso rechaza todas las tramas que no estén validadas, que provengan de un cliente que no se he identificado, salvo aquéllas que sean una solicitud de validación. Estos paquetes EAP que circulan por la red local se denominan EAPOL (EAP over LAN). Una vez validado, el punto de acceso admite todo el tráfico del cliente.

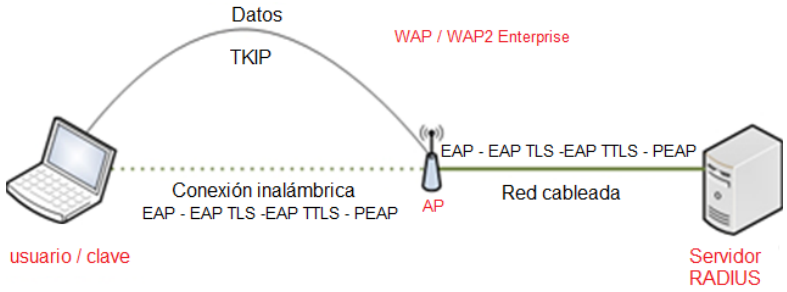

Figura 9.5.4.2.1: Autenticación y encriptación WPA/WPA2 Enterprise

El sistema de autenticación puede ser un servidor RADIUS situado en la red local. Los pasos que sigue el sistema de autenticación 802.1X son:

- ✓ El cliente envía un mensaje de inicio EAP que inicia un intercambio de mensajes para permitir autenticar al cliente.
- ✓ El punto de acceso responde con un mensaje de solicitud de identidad EAP para solicitar las credenciales del cliente.
- ✓ El cliente envía un paquete respuesta EAP que contiene las credenciales de validación y que es remitido al servidor de validación en la red local, ajeno al punto de acceso.
- ✓ El servidor de validación analiza las credenciales y el sistema de validación solicitado y determina si autoriza o no el acceso. En este punto tendrán que coincidir las configuraciones del cliente y del servidor, las credenciales tienen que coincidir con el tipo de datos que espera el servidor.
- ✓ El servidor puede aceptar o rechazar la validación y le envía la respuesta al punto de acceso.
- ✓ El punto de acceso devuelve un paquete EAP de acceso o de rechazo al cliente.
- ✓ Si el servidor de autenticación acepta al cliente, el punto de acceso modifica el estado del puerto de ese cliente como autorizado para permitir las comunicaciones.

Existen múltiples tipos de EAP, algunos son estándares y otros son soluciones propietarias de empresas. Entre los tipos de EAP podemos citar:

EAP-TLS

Es un sistema de autenticación fuerte basado en certificados digitales, tanto del cliente como del servidor, es decir, requiere una configuración PKI (Public Key Infraestructure) en ambos extremos. TLS (Transport Layer Security) es el nuevo estándar que sustituye a SSL (Secure Socket Layer).

EAP-TTLS

El sistema de autenticación se basa en una identificación de un usuario y contraseña que se transmiten cifrados mediante TLS, para evitar su transmisión en texto limpio. Es decir, se crea un túnel mediante TLS para transmitir el nombre de usuario y la contraseña. A diferencia de EAP-TLS sólo requiere un certificado de servidor.

PEAP

El significado de PEAP se corresponde con Protected EAP y consiste en un mecanismo de validación similar a EAP-TTLS, basado en usuario y contraseña también protegidos.

AES

El estándar de cifrado (encriptación) avanzado AES, Advanced Encryption Standard (AES), es uno de los algoritmos más seguros y más utilizados hoy en día disponible para uso público. Está clasificado por la Agencia de Seguridad Nacional, National Security Agency (NSA), de los Estados Unidos para la seguridad más alta de información secreta “Top Secret”. Su historia de éxito comenzó 1997, cuando el Instituto Nacional de Estándares y Tecnología, National Institute of Standards and Technology (NIST), anunció la búsqueda de un sucesor para el estándar de cifrado DES. Un algoritmo llamado "Rijndael", desarrollado por los criptólogos belgas Joan Daemen y Vincent Rijmen, fue destacado en seguridad, así como en el rendimiento y la flexibilidad. Este algoritmo le gano a varios competidores, y fue oficialmente presentado como el nuevo estándar de cifrado AES en el 2001 y se transformó en estándar efectivo en el 2002. El algoritmo se basa en varias sustituciones, permutaciones y transformaciones lineales, ejecutadas en bloques de datos de 16 bytes - por lo que se le llama blockcipher. Estas operaciones se repiten varias veces, llamadas "rondas". En cada ronda, un único “roundkey” se calcula de la clave de encriptación, y es incorporado en los cálculos. Basado en esta estructura de bloque de AES, el cambio de un solo bit, ya sea en la clave, o en los bloques de texto simple y claro, resulta en un bloque de texto cifrado/encriptado completamente diferente - una clara ventaja sobre cifrados de flujo tradicionales. La diferencia entre AES-128, AES-192 y AES-256, es la longitud de la clave: 128, 192 o 256 bits, todos profundamente mejorados en comparación con la clave DES de 56 bits. A modo de ejemplo: Descifrar una clave de 128 bits AES con una supercomputadora estándar del momento, llevaría más tiempo que la presunta edad del universo. Por lo tanto, sigue siendo el estándar AES de cifrado preferido por los gobiernos, los bancos y los sistemas de alta seguridad de todo el mundo.

9.6. Capa Física

La capa física del estándar IEEE 802.11 ha sido definida en cuatro etapas. La primera parte fue publicada en 1997. Dos partes adicionales se publicaron en 1999 y, finalmente, una más reciente apareció en 2002. La primera de ellas, llamada simplemente IEEE 802.11, incluye la capa MAC y tres especificaciones de la capa física, dos en la banda de los 2,4 GHz y una en los infrarrojos, todas ellas operando a 1 y 2 Mbps. IEEE 802.11a

funciona en la banda de los 5 GHz a velocidades de datos de hasta 54 Mbps. IEEE 802.11b funciona en la banda de los 2,4 GHz a 5,5 y 11 Mbps. IEEE 802.11g amplía la norma IEEE802.11b a velocidades de datos más altas. Las velocidades de transmisión de datos de todas las versiones de IEEE 802.11x se muestran en la Tabla 9.6.1.

Tabla 9.6.1: Evolución estándar 802.11

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

IEEE 802.11a

La especificación IEEE 802.11a hace uso de la banda de los 5 GHz. Al contrario que en el caso de las especificaciones en la banda de los 2,4 GHZ, en IEEE 802.11a no se emplea un esquema de espectro expandido, sino multiplexación por división de frecuencia ortogonal (OFDM, Orthogonal Frequency Division Multiplexing). OFDM, también conocido como modulación multiportadora, utiliza varias señales portadoras con frecuencias diferentes, enviando algunos de los bits totales por cada canal. Se trata de un esquema similar a FDM. Sin embargo, en el caso de OFDM todos los subcanales están dedicados a una única fuente de datos.

Las velocidades de datos posibles en IEEE 802.11a son 6, 9, 12, 18, 24, 36, 48 y 54 Mbps. El sistema utiliza hasta 52 subportadoras que se modulan usando BPSK, QPSK, QAM-16 o QAM-64, en función de la velocidad requerida. El espaciado entre frecuencias subportadoras es de 0,3125 MHz. Un código a una tasa de 1/2, 2/3 o 3/4 proporciona corrección de errores hacia delante.

IEEE 802.11b

IEEE 802.11b es una extensión del esquema IEEE 802.11 DS-SS, proporcionando velocidades de datos de 5,5 y 11 Mbps. La tasa de minibits es de 11 MHz, la misma que el esquema DS-SS original, proporcionando así el mismo ancho de banda ocupado. Para conseguir una velocidad de datos mayor en el mismo ancho de banda y con

la misma tasa de minibits se utiliza un esquema de modulación conocido como modulación por código complementario (CCK, Complementary Code Keying). El esquema de modulación CCK es bastante complejo y no será examinado aquí en detalle.

IEEE 802.11g

IEEE 802.11g es una extensión de IEEE 802.11b a mayor velocidad. Este esquema combina toda una gama de técnicas de codificación del medio físico utilizadas en 802.11a y 802.11b para proporcionar servicio a diversas velocidades de datos.

IEEE 802.11n

Con el aumento de la demanda de WLAN, el comité 802.11 buscó formas de aumentar el rendimiento de datos y la capacidad general de las redes 802.11. El objetivo de este esfuerzo es no solo aumentar la tasa de bits de las antenas de transmisión, sino para aumentar el rendimiento efectivo de la red. El incremento del rendimiento efectivo implica mirar no solo el esquema de codificación de la señal, sino también la arquitectura de la antena y la estructura de trama MAC. El resultado de estos esfuerzos es un paquete de mejoras y mejoras incorporadas en IEEE 802.11n. Esta norma es definida para operar tanto en las bandas de 2.4 GHz como en las de 5 GHz y, por lo tanto, puede ser compatible con 802.11a o 802.11b / g.

IEEE 802.11n incorpora cambios en tres áreas generales: uso de MIMO, mejoras en la transmisión de radio y mejoras MAC. Examinamos brevemente cada uno de estos.

La arquitectura de antena de entrada múltiple y salida múltiple (MIMO) es la más importante de las mejoras proporcionadas por 802.11n. En un esquema MIMO, el transmisor emplea múltiples antenas. El flujo de datos de origen es dividido en "n" subgrupos de flujo de datos, una para cada una de las "n" antenas de transmisión. Cada subgrupo de flujo de datos es la entrada a las antenas de transmisión (entradas múltiples). En el extremo receptor, "m" antenas reciben las transmisiones de las "n" antenas de origen a través de una combinación de transmisión de línea de visión y trayectoria múltiple. Las salidas de la "m" antenas receptoras (salida múltiple) se combinan. Con muchas matemáticas complejas, el resultado es una señal de recepción mucho mejor que la que se puede lograr con una sola antena o canales de frecuencia múltiple. 802.11n define varias combinaciones diferentes para el número de transmisores y el número de receptores, de 2 x 1 a 4 x 4. La figura 9.6.2 muestra un modelo SISO (*Single In – Single Out*), y dos modelos MIMO (*Multiple In – Multiple Out*). Cada transmisor o receptor adicional en el sistema aumenta la SNR (relación señal-ruido).

Además de MIMO, 802.11n realiza una serie de cambios en el esquema de transmisión de radio para aumentar la capacidad. La más importante de estas técnicas, conocida como enlace de canales, combina dos canales de 20 MHz para crear un canal de 40 MHz. Usando OFDM, esto permite el doble de subcanales, duplicando la velocidad de transmisión.

Finalmente, 802.11n proporciona algunas mejoras de MAC. El cambio más significativo es agregar múltiples tramas MAC en un solo bloque para la transmisión. Una

vez que una estación adquiere el medio para la transmisión, puede transmitir paquetes largos sin demoras significativas entre transmisiones. El receptor envía un solo bloque de "acknowledgement" (confirmación de recepción). El encabezado físico asociado con la transmisión se envía solo al comienzo de la trama "agregada", en lugar de un encabezado físico por cada trama. La agregación de tramas resulta una significativa mejora en el uso de la capacidad de transmisión.

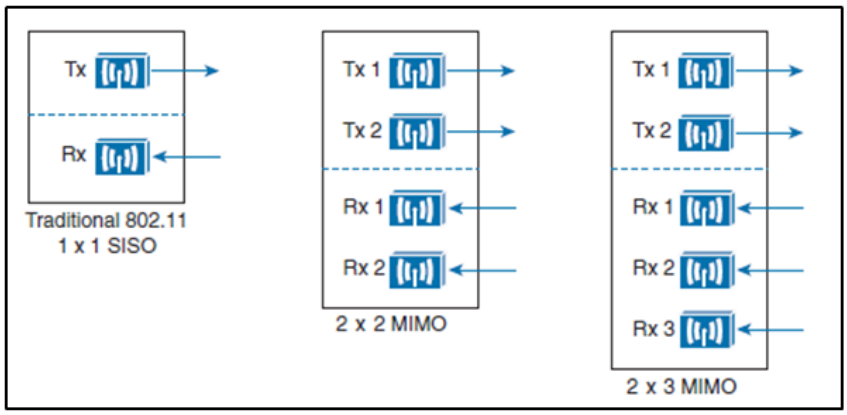

Figura 9.6.2: Modos de transmisión SISO y MIMO

9.7. Gigabit WI-FI

Así como ha habido una necesidad de extender el estándar de Ethernet a velocidades en gigabit por segundo rango, existe el mismo requisito para Wi-Fi. En consecuencia, IEEE 802.11 ha introducido recientemente dos nuevos estándares, 802.11ac y 802.11ad, que proporcionan redes Wi-Fi que funcionan a más de 1 Gbps. Se van a analizar estos dos estándares.

IEEE 802.11ac

IEEE 802.11ac opera en la banda de 5 GHz, al igual que 802.11a y 802.11n. Es diseñado para proporcionar una evolución fluida desde 802.11n. El nuevo estándar logra velocidades de datos mucho más altas que 802.11n mediante mejoras en tres áreas (Figura 9.7.1):

- Ancho de banda: el ancho de banda máximo de 802.11n es de 40 MHz; el máximo ancho de banda de 802.11ac es de 160 MHz.
- Codificación de señal: 802.11n usa 64 QAM con OFDM, y 802.11ac usa 256 QAM con OFDM. Por lo tanto, se codifican más bits por símbolo. Ambos esquemas usan la corrección de errores hacia adelante con una tasa de código de 5/6 (relación de bits de datos a bits totales).
- MIMO: con 802.11n, puede manejar antenas con un máximo de 4 canales de entrada y 4 canales de salida. 802.11ac aumenta esto a 8 * 8.

Podemos cuantificar estas mejoras utilizando la siguiente fórmula, que produce la velocidad de datos de la capa física en bps:

[(número subportadoras de datos) x (número de flujos en el espacio) x (bit de datos por sub-portadora)] / (Tiempo por símbolo OFDM en segundos)

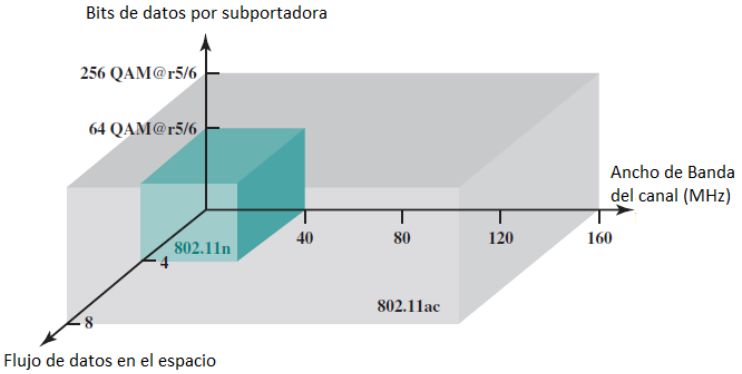

Figura 9.7.1: Factores de perfomance en 802.11

Usando esta ecuación tenemos lo siguiente:

$$802.11n: \frac{108 \times 4 \times (5/6 \times \log_2 64)}{3.6 \times 10^{-6}} = 600 \times 10^6 \text{ bps} = 600\,\text{Mbps}$$

$$802.11ac: \frac{468 \times 8 \times (5/6 \times \log_2 256)}{3.6 \times 10^{-6}} = 6937 \times 10^6 \text{ bps} = 6.937\,\text{Gbps}$$

Aumentar el ancho de banda del canal en un factor de 4 aproximadamente cuadruplica la tasa de datos La potencia de transmisión ahora debe también incrementarse en 4 veces (igual al número de subportadoras), lo que trae como consecuencia en una ligera reducción del alcance de la señal. Pasar de 64 QAM a 256 QAM aumenta la velocidad de datos en un factor de 1,33. Sin embargo, 256 QAM es más sensible a ruido y, por lo tanto, es más efectivo a distancias más cortas. Finalmente, la velocidad es directamente proporcional al número de flujos de datos en el espacio. Por supuesto, más flujos en el espacio requiere más antenas, lo que aumenta el costo del dispositivo suscriptor.

Otros dos cambios que van de 802.11n a 802.11ac son dignos de mención. 802.11ac incluye la opción de MIMO multiusuario (MU-MIMO). Esto significa que, en el enlace descendente, el transmisor puede usar sus recursos de antena para transmitir múltiples tramas a diferentes estaciones, todo al mismo tiempo y sobre el mismo espectro de frecuencias. Por lo tanto, cada antena de un AP MU-MIMO puede simultáneamente comunicarse con un dispositivo de antena única diferente, como un teléfono inteligente o una tableta. Esto permite que el AP entregue significativamente más datos en diferentes ambientes.

Otra diferencia es que 802.11ac requiere que cada transmisión 802.11ac sea enviada como una trama agregada A-MPDU. Brevemente, este requisito se impone para garantizar un uso eficiente del canal.

IEEE 802.11ad

IEEE 802.11ad es una versión de 802.11 que opera en la banda de frecuencia de 60 GHz. Esta la banda ofrece el potencial de un ancho de banda de canal mucho más amplio que la banda de 5 GHz, permitiendo altas velocidades de datos con codificación de señal relativamente simple y características de antena.

Pocos dispositivos funcionan en la banda de 60 GHz, lo que significa las comunicaciones experimentarán menos interferencia que en las otras bandas utilizadas por 802.11. Sin embargo, a 60 GHz, 802.11ad está operando en el rango de milímetros, lo cual implica que existan algunas características de propagación indeseables:

1. La pérdida de energía en el espacio libre aumenta con el cuadrado de la frecuencia; por lo tanto, las pérdidas son mucho mayores en este rango que en los rangos utilizados para sistemas de microondas.
2. Las pérdidas por trayectos múltiples pueden ser bastante altas. La reflexión ocurre cuando una señal electromagnética encuentra una superficie que es grande en relación con la longitud de onda de la señal; la dispersión ocurre si el tamaño de un obstáculo está en el orden de la longitud de onda de la señal o menos; la difracción ocurre cuando el frente de onda se encuentra con el borde de un obstáculo que es grande en comparación con la longitud de onda.
3. Las señales de ondas milimétricas generalmente no penetran objetos sólidos.

Por estas razones, es probable que 802.11ad sea útil solo dentro de una habitación individual. Puede soportar altas velocidades de datos y, por ejemplo, podría transmitir fácilmente video de alta definición sin comprimir. Con estas características, es adecuada para aplicaciones como la sustitución cables en un sistema de entretenimiento doméstico o transmisión de películas de alta definición desde tu celular a tu televisor.

Hay dos diferencias notables entre 802.11ac y 802.11ad. Mientras 802.11ac admite una configuración de antena MIMO, 802.11ad está diseñado para antena de única operación. Y 802.11ad tiene un gran ancho de banda de canal de 2160 MHz.

Tabla 9.7.2: Modulación y esquema de codificación 802.11ad

Capa Física	Codificación	Modulación	Tasa de bits bruta
Control (CPHY)	1/2 LDPC, 32 × spreading	π/2-DBPSK	27.5 Mbps
Single carrier (SCPHY)	1/2 LDPC 1/2 LDPC, 5/8 LDPC 3/4 LDPC 13/16 LDPC	π/2-BPSK π/2-QPSK π/2-16 QAM	385 Mbps to 4.62 Gbps
OFDM (OFDMPHY)	1/2 LDPC 5/8 LDPC 3/4 LDPC 13/16 LDPC	OFDM-OQPSK OFDM-QPSK OFDM-16 QAM OFDM-64 QAM	693 Mbps to 6.76 Gbps
Low-power single carrier (LPSCPHY)	RS(224,208) + Block Code(16/12/9/8,8)	π/2-BPSK π/2-QPSK	636 Mbps to 2.5 Gbps

IEEE 802.11ad define cuatro esquemas de codificación y modulación de capa física (Tabla 9.7.2). Cada tipo tiene un propósito distinto y admite un rango diferente de velocidades de datos:

- Control PHY (CPHY) es el codificado más robusto (y, en consecuencia, modo de rendimiento más bajo), con una tasa de código de solo la mitad. Su propósito es exclusivamente para transmitir mensajes del canal de control.
- PHY de una sola portadora (SCPHY) utiliza el potente codificado "código de verificación baja densidad (LDPC), para una corrección robusta de errores hacia adelante y proporciona tres opciones de modulación.
- OFDM PHY (OFDMPHY) emplea modulación multiportadora, que puede proporcionar densidades de modulación más altas y, por lo tanto, un mayor rendimiento de datos comparando con las opciones de la portadora única
- La portadora única de baja potencia (LPSCPHY) emplea la modulación de portadora única para minimizar el consumo de energía. Usa codificación "Reed – Solomon" o "Bloques Hamming", los cuales requieren menos energía que LDPC, a expensas de una corrección de errores menos robusta. Los pequeños dispositivos alimentados por batería podrían beneficiarse del ahorro de energía adicional.

La técnica de codificación de corrección de errores LDPC que es común a la CPHY, SCPHY y OFDMPHY se basa en una longitud de palabra de código común de 672 bits que transportan 336, 504, 420 o 546 bits de carga útil para lograr una tasa de código de 1/2, 3/4, 5/8 o 13/16, según sea necesario.