

# Capítulo 5.

## Descripción de IEEE802.11

### **5.1 Introducción.**

El propósito de este estándar es el de proveer conectividad inalámbrica a maquinaria, equipo, o estaciones. Éstas pueden ser portátiles, o pueden estar montadas en vehículos dentro de un área local. La conexión debe ser a una tasa de transmisión muy elevada. En las primeras versiones de éste estándar se especificaban 1 o 2 Mbps, en las versiones subsecuentes de las cuales se hablará más adelante en este capítulo se llega a los 11 Mbps en el caso de la versión IEEE802.11g. Las siguientes redes inalámbricas llamadas Hiper redes llegan a obtener velocidades de 54 Mbps.

Las redes inalámbricas tienen características fundamentales que las hacen diferir mucho de las tradicionales LANs alámbricas, para conectarse entre ellas se tienen que utilizar otro tipo de elementos, para interconectarlas se utiliza un portal, el cual será explicado más adelante. En redes alámbricas, la dirección destino es equivalente a la dirección física, en redes inalámbricas, la dirección destino es una estación que no siempre es una locación fija.

Los medios físicos que utiliza IEEE802.11:

- Utilizan un medio que no tiene fronteras más que hasta donde el transceptor utilizado pueda cubrir.
- Están desprotegidas de señales externas.
- Se comunican por un medio que es mucho menos confiable que en las alámbricas.
- Tienen topologías dinámicas.
- Carecen de conectividad completa.
- Tienen propiedades de propagación asimétricas y que cambian con el tiempo.

Debido a las limitaciones en los alcances de los transceptores, WLANs están diseñadas para cubrir zonas geográficamente razonables, actualmente se diseñan para cubrir bloques de edificios.

Un aspecto importante a considerar cuando se diseñó este estándar fue que tenía que servir a unidades portátiles, y unidades móviles. Una unidad portátil es aquella que se mueve de un lugar a otro, pero permanece fija mientras envía y recibe información. Una unidad móvil es la que mientras está recibiendo o enviando información está en constante movimiento. Por razones técnicas, no es suficiente considerar a las unidades portátiles, esto debido a que por la propagación, incluso una unidad portátil se ve como una unidad móvil debido a las condiciones de propagación. [3]

## 5.2 Componentes de la Arquitectura de IEEE802.11.

La arquitectura consiste en varios componentes que interactúan para proveer una LAN inalámbrica que soporta movilidad transparente para las capas superiores.

### 5.2.1 Basic Service Set (BSS) o Juego Básico de Servicio.

El BSS es el bloque básico del estándar. En la figura 5.1 se muestran dos BSSs, cada uno tiene dos estaciones que son miembros de cada BSS.

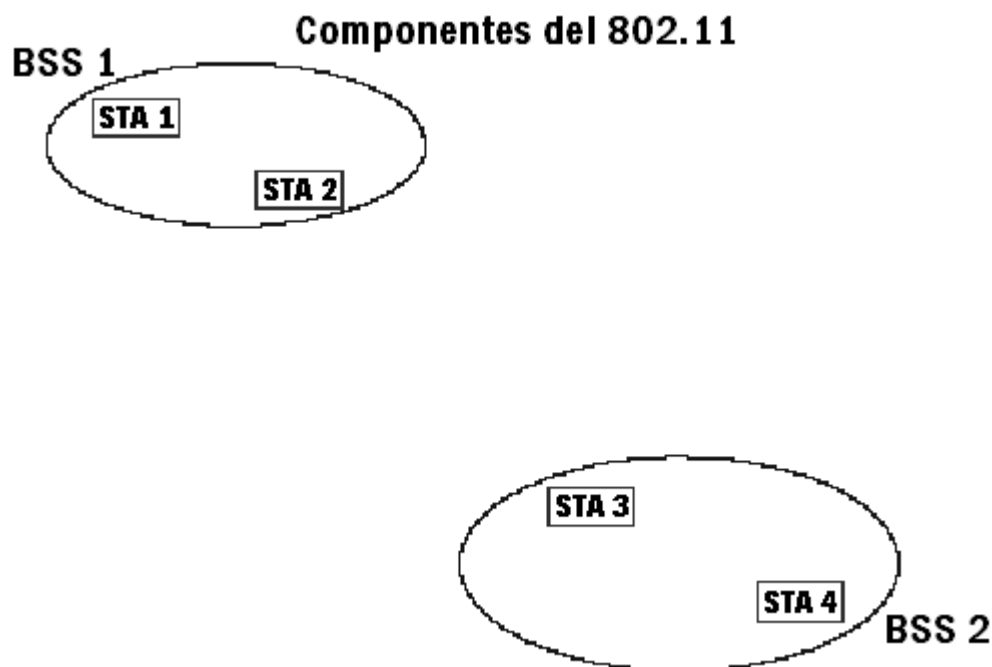


Figura 5.1. Basic Service Set. [3]

El círculo en el cual están contenidas las estaciones se debe considerar como la zona de cobertura de cada BSS, al salir de éstas zonas teóricas, la comunicación no puede ser mantenida. La asociación entre una estación y un BSS es dinámica. Puede estar encendida, apagada, entrar a zona de cobertura, salir de zona de cobertura. Para convertirse en miembro de una infraestructura BSS, una estación debe asociarse. Éstas asociaciones son

dinámicas e involucran el uso de un Servicio de Sistema de Distribución o DSS, que se describirá a continuación.

### 5.2.2 Conceptos de un Sistema de Distribución.

Las limitaciones físicas determinan la distancia de estación a estación que puede ser soportada. Para algunas redes ésta distancia es suficiente; sin embargo, para otras redes, una cobertura mayor es requerida. En lugar de existir independientemente, una BSS puede también formar parte de una red que está construida con múltiples BSSs. Para interconectar estos elementos se utiliza un sistema de distribución o DS. El DS da soporte a dispositivos móviles al proveer los servicios lógicos necesarios para manejar direccionamiento y la integración de múltiples BSSs.

Un Punto de acceso o Access Point (AP) es una estación que provee acceso al DS al dar servicios de DS y actuar como una estación. En la figura 5.2 se muestra como se integran el DS y el AP a la arquitectura.

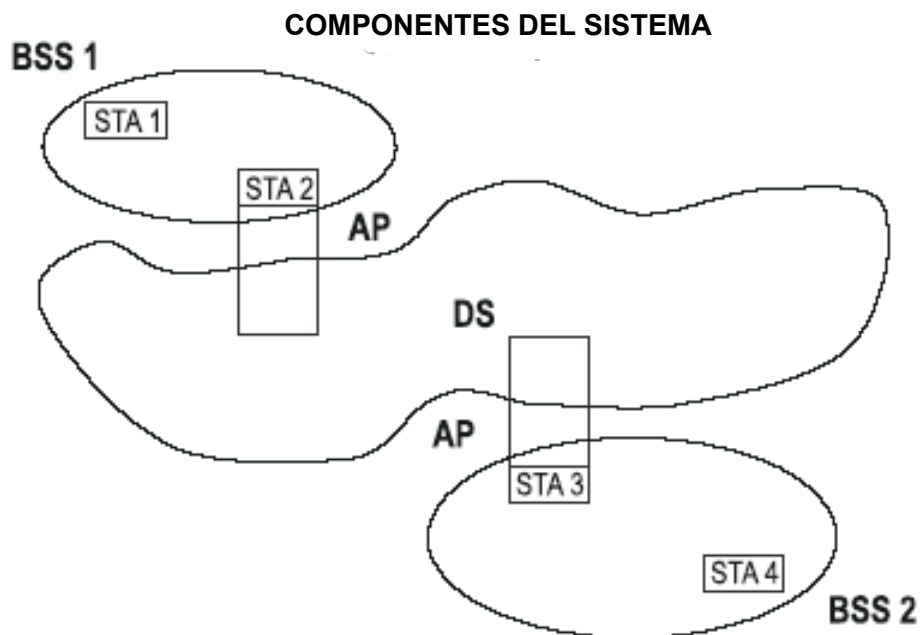


Figura 5.2. Sistema de Distribución. [3]

La información fluye entre DS y BSS vía un AP. Es importante agregar que un AP es también una estación, por lo que son entidades que pueden ser direccionadas. Las direcciones dependiendo si son enviadas por el medio inalámbrico o si son enviadas por el medio del DS pueden ser diferentes.

### 5.2.3 Juego de Servicio Extendido (ESS).

El DS y los BSSs permiten a IEEE802.11 crear una red inalámbrica de tamaño y complejidad arbitraria. A éste tipo de red se le conoce como ESS (Ver figura 5.3).

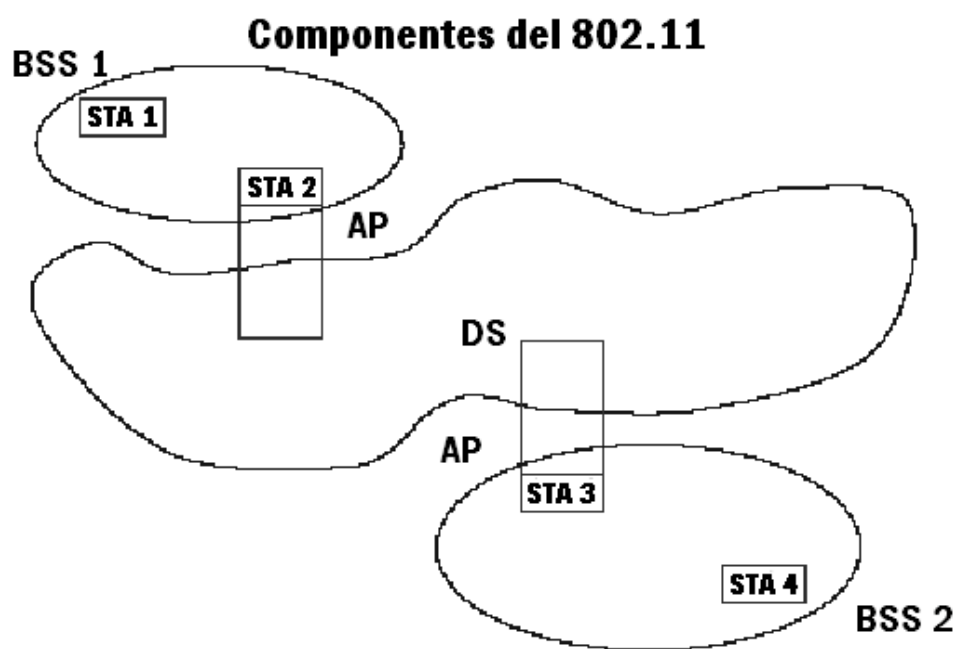


Figura 5.3. Extended Service Set. [3]

El concepto clave es que la red ESS es apreciada de la misma manera para las capas superiores que una red IBSS (Juego de servicio básico independiente), estaciones dentro del ESS se pueden comunicar y estaciones móviles se pueden mover de un BSS a otro, dentro del mismo ESS, de forma transparente para las capas superiores. Al utilizar ESS las BSSs pueden traslaparse un poco para dar una cobertura continua en un rango específico. Debido a que el medio es inalámbrico y el medio cambia continuamente, especificar áreas de

cobertura bien definidas simplemente no es posible. Las características de propagación son dinámicas e impredecibles. Un pequeño cambio en la posición o dirección puede resultar en grandes cambios en el nivel de la señal que se recibe. Al igual que en telefonía celular, el área de cobertura que se presenta en los esquemas es simplemente teórica, en realidad el área de cobertura varía mucho.

#### 5.2.4 Portal para la Integración con redes alámbricas.

Para integrar el IEEE802.11 con la tradicional LAN, se presenta un componente adicional a la arquitectura: El Portal.

Un portal es un punto lógico en donde MSDUs de una LAN alámbrica se comunica con el DS de la WLAN. Toda la información que entra de otras redes entra por este punto. Es posible que un portal ofrezca las funciones de un AP, éste sería el caso cuando un DS es implementado por componentes de la LAN. En la figura 5.4 se muestra la arquitectura completa del sistema. [3]

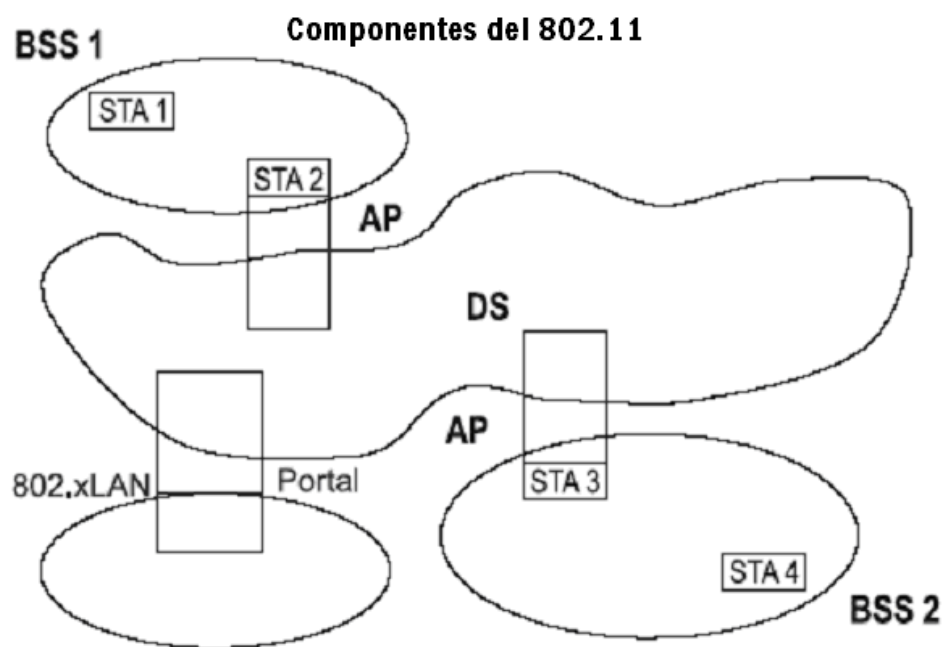


Figura 5.4. Arquitectura Completa del IEEE802.11. [3]

### **5.3 Servicios de la Arquitectura.**

Los servicios se dividen en dos grupos: los servicios que son parte de cada estación, y los servicios que son parte de un DS. Los servicios que tienen que ofrecer las estaciones son los siguientes:

- Autenticación.
- Deautenticación.
- Privacía.
- Entrega de MSDU .

Los que tiene que entregar el sistema de distribución:

- Asociación.
- Disociación.
- Distribución.
- Integración.
- Reasociación.

### **5.4 Tipos de Movilidad.**

- Sin transición. Éste tipo de movilidad tiene dos subclases:
  - Estática. Sin movimiento.
  - Movimiento Local. El movimiento es dentro del rango físico de las estaciones que están involucradas en la comunicación.
- Transición entre BSS. Se cambia de BSS pero se mantiene dentro del mismo ESS.
- Transición entre ESS. Se cambia de un BSS de un ESS a otro BSS de otro ESS, el servicio solo se garantiza con estaciones móviles, pero mantener la conexión con las capas superiores no se garantiza. Es probable que se pierda la conexión. [3]

## **5.5 Autenticación.**

En LANs alámbricas la seguridad física se puede utilizar para prevenir accesos no autorizados. En el caso de las WLANs esto es impráctico debido a que la cobertura no tiene fronteras específicas. IEEE802.11 provee la habilidad de controlar el acceso mediante un servicio de autenticación. Este servicio se utiliza por todas las estaciones para establecer su identidad con las estaciones que se estará en comunicación. Si no se establece cierto nivel de autenticación entre las estaciones la asociación no ocurrirá. La autenticación es un servicio de estación. El estándar soporta varios procesos de autenticación, entre estos se encuentra la autenticación a nivel de enlace entre estaciones. La autenticación del estándar está definida para llegar a lo especificado para un enlace alámbrico. Otro tipo de autenticación es el de clave compartida. En éste tipo la identidad es demostrada por el conocimiento de una clave compartida, secreta, y encriptada WEP.

Debido a que el proceso de autenticación puede consumir mucho tiempo, el servicio de autenticación puede ser invocado independientemente del servicio de asociación. Si la autenticación se deja para el momento de la reasociación, este proceso puede impactar la velocidad con la cual la estación se reasocia. La preautenticación como se le conoce a éste proceso hace que el servicio de autenticación salga del proceso de tiempo de reasociación crítico.

### **5.5.1 Autenticación de Sistema Abierto.**

Éste es el mecanismo de autenticación más simple disponible. Esencialmente es un algoritmo de autenticación nulo. Cualquier estación que solicite autenticación con este algoritmo puede ser autenticada si en la estación receptora está bajo la autenticación de sistema abierto. Esta autenticación involucra una secuencia de dos pasos. El primer paso



en la secuencia es la obtención de la identidad y la solicitud de autenticación. El segundo paso es el resultado de la autenticación.

#### **5.5.2 Autenticación de Clave compartida.**

Esta autenticación soporta estaciones que conocen la clave y aquellas que no la conocen. Esto es obtenido debido a que no siempre se tiene que transmitir la clave, se requiere para esto el mecanismo de privacidad WEP. La clave secreta compartida se le envía a los usuarios mediante un canal seguro. Durante la autenticación tanto la solicitud de la clave y la respuesta encriptada son transmitidos. Lo que facilita el descubrimiento de la secuencia pseudo aleatoria de la clave, por lo que se tiene que evitar enviar ésta clave en los segmentos subsiguientes. [3]

#### **5.6 Privacidad.**

En una LAN, solo las estaciones que se encuentran físicamente conectadas al cable pueden escuchar el tráfico. Con las WLAN cualquier estación capacitada puede escuchar el tráfico que tengo en su rango. Por lo que si no existe la privacidad, la seguridad de este tipo de redes seria muy baja. El servicio de privacidad, que es un servicio de cada estación, permite encriptar el contenido de mensajes. El estándar especifica un algoritmo de privacidad, WEP, cuyo objetivo es el de satisfacer la privacidad equivalente a las LAN tradicionales. El algoritmo no está diseñado para proveer al usuario con alta seguridad, simplemente emular lo que una LAN daría de privacidad al usuario.

#### **5.7 Formatos de Segmentos o Frames.**

Todas las estaciones deben ser capaces de construir segmentos para transmisión y decodificar segmentos cuando se reciben. Cada segmento está compuesto de los siguientes componentes básicos:



- El campo de Duración contiene la identidad de asociación de la estación que transmitió el segmento.
- Los campos para direcciones contienen al identificador del BSS, dirección de la fuente, dirección del destino, dirección de la estación transmisora, y la dirección de la estación receptora. Algunos segmentos pueden no tener todos estos elementos.
- Campo para Control de secuencia. Este campo de 16 bits en longitud consiste de dos subcampos: el número de secuencia y el número de fragmento. [3]

### **5.8 Método de Acceso Secuencia Directa Espectro Extendido (DSSS) para la capa física.**

El sistema de RF LAN está dirigido a la banda de los 2.4 GHz diseñada para aplicaciones ISM. El sistema DSSS provee LAN inalámbricas tanto de 1 y 2 Mbps de capacidad de carga de información. En los Estados Unidos se definió que el sistema debe dar una ganancia mínima de 10 dB. El sistema utiliza modulaciones en banda base de DBPSK y DQPSK para dar tasas de datos de 1 Mbps y 2 Mbps, respectivamente. [3]

El DSSS PHY consiste de las próximas funciones de protocolo:

- a) Una función de convergencia para la capa física, que adopte las capacidades del sistema dependiente del medio (PMD). Ésta función es soportada por un procedimiento de convergencia de la capa física (PLCP), que define un método para mapear las unidades de datos del protocolo MAC (MPDUs) a segmentos, de modo que pueden ser transmitidos y recibidos por el sistema.
- b) Un sistema PMD, cuya función define las características, y el método de transmisión y recepción de datos a través del WM entre dos o más estaciones.

El DSSS PHY contiene tres entidades funcionales: la función PMD, la PLCP, y la función de administración de capas.

#### 5.8.1 La subcapa PLCP.

Para permitir que IEEE802.11 MAC opere con una mínima dependencia en la subcapa PMD, se define esta subcapa. En esta capa los MPDUs se convierten de y a PPDUs. Durante la transmisión, un MPDU debe convertirse mediante una cabecera y un preámbulo PLCP para crear un PPDDU. En el receptor, se procesan la cabecera y el preámbulo para realizar la demodulación y entregar el MPDU. En la Figura 5.7 se muestra la composición de un segmento PLCP.

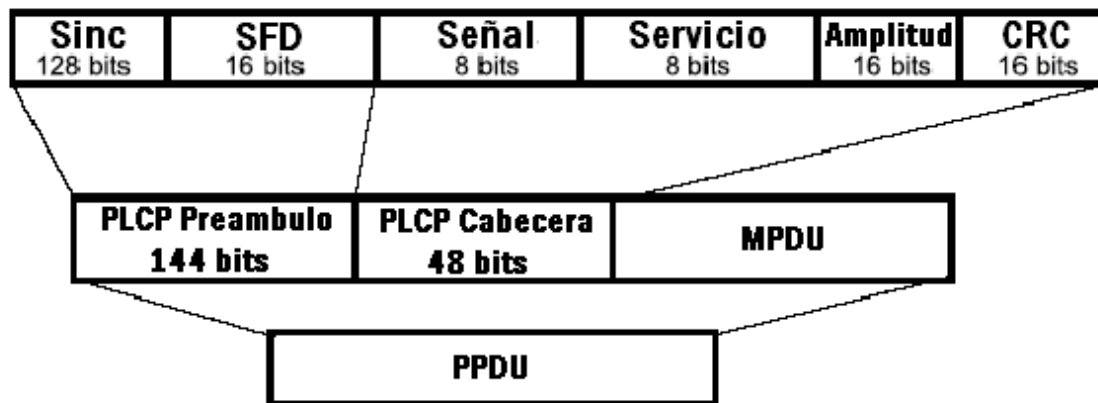


Figura 5.7. Protocolo de Convergencia de la Capa Física. [3]

#### 5.8.2 Subcapa PMD.

Esta subcapa provee de un medio para enviar y recibir datos entre dos o más estaciones. Esta capa PMD recibe la información de la capa PLCP y provee los medios necesarios para su transmisión y recepción del medio. La función resulta en flujo de datos, información de temporizador, y parámetros de la señal asociado recibida que son entregados a la subcapa PLCP. La ubicación de esta capa se muestra en la figura 5.8.

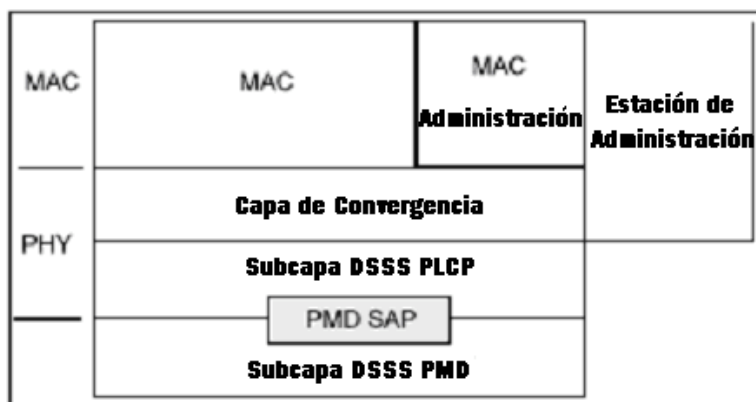


Figura 5.8. Physical Medium Dependent. [3]

### 5.8.3 Entidad de administración de la capa física (PLME).

La PLME realiza la administración de las funciones de la capa física locales en conjunto con la entidad de administración de la capa MAC.

### 5.8.4 Especificaciones de Operaciones PMD.

*Rango de Frecuencias de Operación.*

El DSSS PHY debe operar en el rango de frecuencias de 2.4 GHz a 2.4835 GHz en los Estados Unidos, y en Europa de 2.471 a 2.497 GHz.

*Número de canales en operación.*

La tabla 5.1 muestra el número de canal y su frecuencia de operación; después del número de canal aparece los organismos que soportan ese canal.

CHNL_ID	Frecuencia	Dominio Regulatorio					
		X'10'	X'20'	X'30'	X'31'	X'32'	X'40'
		FCC	IC	ETSI	España	Francia	MKK
1	2412 MHz	X	X	X	-	-	-
2	2417 MHz	X	X	X	-	-	-
3	2422 MHz	X	X	X	-	-	-
4	2427 MHz	X	X	X	-	-	-

5	2432 MHz	X	X	X	-	-	-
6	2437 MHz	X	X	X	-	-	-
7	2442 MHz	X	X	X	-	-	-
8	2447 MHz	X	X	X	-	-	-
9	2452 MHz	X	X	X	-	-	-
10	2457 MHz	X	X	X	X	X	-
11	2462 MHz	X	X	X	X	X	-
12	2467 MHz	-	-	X	-	X	-
13	2472 MHz	-	-	X	-	X	-
14	2484 MHz	-	-	-	-	-	X

Tabla 5.1. Número de canal y frecuencia de operación. [3]

En un sistema con múltiples células, con traslapes o adyacentes utilizando diferentes canales pueden permanecer sin interferencia, siempre y cuando exista un mínimo de 30 MHz de separación entre las frecuencias centrales de los canales.

*Modulación y tasa de transmisión de canales.*

Dos formatos de modulación y tasas de transmisión están especificados: una tasa de acceso básico y un tasa de acceso mejorada. La primera debe estar basada en 1 Mbps DBPSK. La segunda en 2 Mbps DQPSK. A continuación en la tabla 5.2 se muestran los cambios de fase para ambas.

Bit de Entrada	Cambio de Fase
0	0
1	□
Patrón de Dibit.	Cambio de Fase.
00	0

01	$\pi/2$
10	$\pi$
11	$3\pi/2$ ( $-\pi/2$ )

Tabla 5.2. Cambios de fase. [3]

### *Control de Potencia.*

Está definido el máximo nivel de potencia de transmisión para el sistema. En Europa el ETSI definió 100 mW (EIRP), en Estados Unidos la FCC definió 100 mW. Siendo el mínimo no menos de 1 mW.

Cuando la potencia de transmisión es mayor a 100 mW se puede establecer control de potencia. Dicho control de potencia puede tener un máximo de 4 niveles de potencia. Por lo menos, un radio capaz de transmitir más de 100 mW debe ser capaz de reducir su potencia a 100 mW o menos. [3]

## **5.9 IEEE802.11a.**

Entre los cambios realizados con esta actualización se definió el protocolo para la banda de los 5 GHz. Para esta banda se especificó un sistema OFDM. Dicho sistema se explica a continuación.

### **5.9.1 OFDM PHY.**

El sistema está diseñado para los rangos de frecuencia de 5.15-5.25, 5.25-5.35, y 5.725-5.825 GHz. El sistema OFDM provee una WLAN con capacidades de comunicación de 6,9,12,18,24,36,48 y 54 Mbps. Ser capaz de comunicarse a 6,12 y 24 Mbps es obligatorio

para este estándar. El sistema utiliza 52 subportadoras que son moduladas utilizando BPSK o QPSK, 16 QAM o 64 QAM. Se utiliza una codificación convolucional con una tasa de codificación de 1/2, 2/3 y 3/4.

Este sistema contiene las mismas subcapas definidas para DSSS PHY. [20] Las diferencias entre estos sistemas se indican a continuación.

### 5.9.2 OFDM PLCP.

Este subclausula provee el proceso de convergencia en la cual PSDUs son convertidos de y a PPDU. Igual que en el caso de DSSS PLCP se le agrega un preámbulo y cabecera para la creación de los PPDU. Estos igualmente sirven en el receptor para ayudar en la demodulación y entregar el PSDU. El formato de un PPDU se muestra en la figura 5.9.

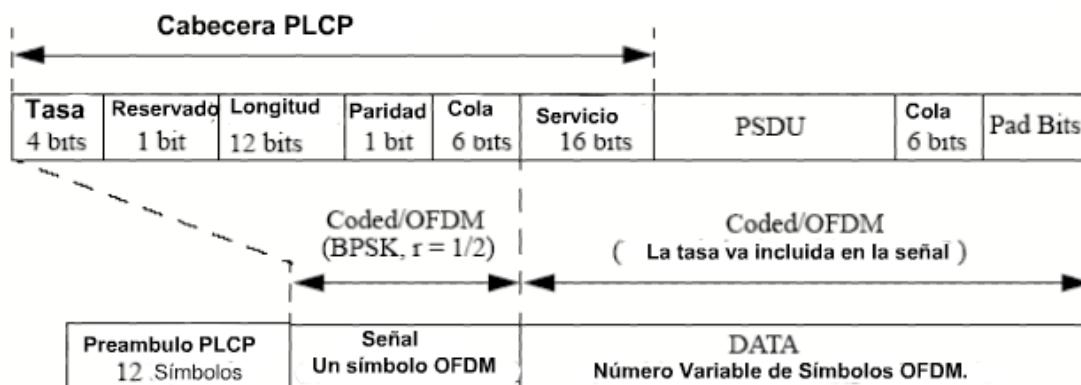


Figura 5.9. Orthogonal Frequency Division Multiplexing PLCP. [20]

Un aspecto muy importante especificado es que algunos parámetros varían dependiendo de la velocidad deseada. Estos parámetros se muestran en la tabla 5.3.

Tasa de dato (Mbits/s)	Modulación	Tasa de codificación	Bits codificados	Bits codificado por símbolo	Bits de datos por símbolo OFDM



				<b>OFDM</b>	
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	96	48
18	QPSK	3/4	2	96	72
24	16-QAM	1/2	4	192	96
36	16-QAM	3/4	4	192	144
48	64-QAM	2/3	6	288	192
54	64-QAM	3/4	6	288	216

Tabla 5.3. Parámetros dependientes de la velocidad. [20]

Este sistema cuenta con 48 subportadoras de datos, 4 subportadoras piloto, llegando a un total de 52 subportadoras. Además el espaciamiento entre cada una es de 0.3125 MHz.

#### **5.9.2.1 Canales.**

Los canales para este sistema están espaciados 5 MHz sus frecuencias centrales empezando en los 5 GHz llegando hasta los 6 obteniendo 200 canales.

#### **5.9.2.2 Potencia de Transmisión.**

La máxima potencia de transmisión depende de la banda de frecuencia utilizada, para la banda de 5.15-5.25 es de 40 mW, de 5.25-5.35 de 200 mW, de 5.725-5.825 de 800 mW. [20]

### **5.9.3 OFDM PMD.**

Las características de esta subcapa es la misma que en el caso de DSSS que se explicó anteriormente. En este caso se pueden considerar dos tipos de interacciones:

- Servicios que soportan interacciones Peer a Peer.

- Importancia local, interacciones de subcapa a subcapa. [20]

### **5.10 IEEE802.11g.**

Para esta actualización aparecen algunos cambios en el formato de los segmentos, así como a la subcapa MAC a los cuales no nos adentraremos en éste capítulo, si desea conocer a fondo estos cambios dirigirse directamente al estándar.

#### **5.10.1 Especificación PHY de Tasa Expandida (ERP).**

Esta cláusula se agrega para esta actualización del estándar para la banda de los 2.4 GHz. Con el ERP se añaden a las ya existentes 1,2,5.5, y 11 Mbps las tasas de transmisión de: 6,9,12,18,24,36,48 y 54 Mbps. De estas nuevas tasas de transmisión tienen que ser obligatorias hasta los 24 Mbps. Se incorporan 2 modulaciones ERP-PBCC con tasas de transmisión de 22 y 33 Mbps. Se agrega una modulación opcional conocida como DSSS-OFDM con tasas de transmisión hasta los 54 Mbps.

Toda la porción de radio para sistemas ERP cumplen con las especificaciones para sistemas OFDM que se introdujo en la actualización IEEE802.11a, solo que para la banda de los 2.4 GHz. Este sistema puede decodificar los PLCPs de los sistemas anteriores.

Un ERP BSS es capaz de operar en cualquier combinación de los disponibles modos de ERP y modos No ERP.

Es importante recalcar que la banda de los 2.4 GHz es un medio compartido, y la coexistencia con otros dispositivos que estén diseñados para los sistemas anteriores es muy importante para mantener el sistema con un rendimiento óptimo. Las modulaciones introducidas en ésta actualización (ERP-OFDM, ERP-PBCC y DSSS-OFDM) están diseñadas para coexistir con las estaciones diseñadas para HR DSSS y para DSSS. La coexistencia es obtenida por varios métodos, incluyendo detección de portadora virtual, detección de portadora, protocolos para evitar colisiones y fragmentación de MSDUs. En la

tabla 5.4 se muestra la modulación que se utiliza dependiendo de la tasa de transmisión requerida.

El sistema ERP PHY al igual que los anteriores se divide en su PLCP y también su PMD. Ambos sistemas tienen las mismas funciones que los explicados anteriormente.

Modulación.	Tasa de Transmisión (Mbps).
ERP-DSSS	1 y 2
ERP-CCK	5.5 y 11
ERP-OFDM	6,9,12,18,24,36,48 y 54
ERP-PBCC	5.5, 11,22 y 33
DSSS-OFDM	6,9,12,18,24,36,48 y 54.

Tabla 5.4. Modulación y tasa de transmisión. [22]

#### **5.10.2 Subcapa PLCP.**

Una estación ERP debe soportar tres diferentes cabeceras y preámbulos. El primero es el preámbulo largo. Este PPDU provee interoperabilidad con los sistemas HR DSSS cuando se utilizan las tasas de transmisión de 1, 2, 5.5, y 11 Mbps; todas las tasas cuando se utiliza ya sea DSSS-OFDM o ERP-PBCC. El segundo es el preámbulo corto, éste soporta tasas de 2, 5.5 y 11 Mbps, así como DSSS-OFDM y ERP-PBCC. El tercero es el preámbulo ERP-OFDM para soportar las tasas de modulación DSSS-OFDM.

Para conocer el formato de las cabeceras referirse al IEEE802.11g. [22]

#### **5.10.3 Especificaciones de Operación ERP-PBCC.**

Estos modos adicionales proveen al sistema la habilidad de alcanzar las velocidades de 22 y 33 Mbps siendo completamente compatibles con los sistemas anteriores. Se especifican 4 opcionales formatos de modulación y tasas de transmisión de datos para ERP. Estos deben estar basados en PBCC.

#### **5.10.4 Especificaciones de Operación DSSS-OFDM.**

Este modo de operación opcional da la habilidad de ser completamente compatible sin necesidad de coordinación adicional. Se reutilizan los preámbulos especificados para HR DSSS. Los cambios en su mayoría se encuentran en el formato de los PSDU.

Al no ser el objetivo de ésta tesis describir completamente los diferentes estándares estudiados, de requerir mayores referencias de los cambios introducidos referirse directamente a los estándares que están disponibles de la IEEE. [22]

Para este punto de la tesis ya se estudiaron las WLAN y los sistemas celulares, con este estudio ya se puede pasar a la investigación de la interconexión entre estos dos tipos de sistemas. Además de manejar el problema de interferencia entre el sistema Bluetooth y los sistemas IEEE802.11