ESTUDIO DE LA TECNOLOGÍA WI – FI, PARA ACCESO INALÁMBRICO A REDES DE COMUNICACIONES ELECTRÓNICAS DE ÁMBITO REDUCIDO

CRISTIAN CAMILO BARRIOS ZARANTE
YANIRA ULIANOVA CARRASCAL VILLALBA

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
FACULTAD DE CIENCIAS DE INGENIERÍA
DEPARTAMENTO DE INGENIERÍA ELECTRÓNICA Y ELÉCTRICA
CARTAGENA DE INDIAS D.T. Y C.
2005

ESTUDIO DE LA TECNOLOGÍA WI – FI, PARA ACCESO INALÁMBRICO A REDES DE COMUNICACIONES ELECTRÓNICAS DE ÁMBITO REDUCIDO

CRISTIAN CAMILO BARRIOS ZARANTE
YANIRA ULIANOVA CARRASCAL VILLALBA

Monografía para optar al titulo de
Ingeniero Electrónico

Director
Gonzalo López Vergara
Magíster en Telemática

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
FACULTAD DE CIENCIAS DE INGENIERÍA
DEPARTAMENTO DE INGENIERÍA ELECTRÓNICA Y ELÉCTRICA
CARTAGENA DE INDIAS D.T. Y C.
2005

Cartagena de Indias D. T. y C, Noviembre de 2005

Señores:

Comité Evaluador

Departamento de Ingeniería Eléctrica y Electrónica

La Ciudad

Respetados Señores

Tengo el agrado de presentar a su consideración el trabajo de grado del cual me desempeño como director de la monografía titulada **"ESTUDIO DE LA TECNOLOGÍA WI – FI, PARA ACCESO INALÁMBRICO A REDES DE COMUNICACIONES ELECTRÓNICAS DE ÁMBITO REDUCIDO"** desarrollada por los estudiantes CRISTIAN CAMILO BARRIOS ZARANTE Y YANIRA ULIANOVA CARRASCAL VILLALBA, como requisito para obtener el titulo de ingenieros electrónicos.

Atentamente

Gonzalo López Vergara MSC

Cartagena de Indias D. T. y C, Noviembre de 2005

Señores:

Comité Evaluador

Departamento de Ingeniería Eléctrica y Electrónica

La Ciudad

Respetados Señores

Con mucha atención nos dirigimos a ustedes para presentar la monografía titulada: **"ESTUDIO DE LA TECNOLOGÍA WI – FI, PARA ACCESO INALÁMBRICO A REDES DE COMUNICACIONES ELECTRÓNICAS DE ÁMBITO REDUCIDO"** para su estudio y evaluación como requisito fundamental para obtener el titulo de Ingeniero Electrónico.

En espera que esta cumpla con las normas pertinentes establecidas por la institución nos despedimos

Atentamente

---------- ----------

Cristian Camilo Barrios Zarante **Yanira Carrascal Villalba**

Nota de aceptación

Firma del jurado

Firma del jurado

Cartagena de Indias D. T. y C, Diciembre de 2005

Dedico el fruto de mi esfuerzo a mis padres, mis hermanos y abuelos, quienes con su esfuerzo, amor y dedicación me ayudaron a seguir el camino del éxito.

A mis amigos, profesores y todas aquellas personas que de una u otra manera me tendieron la mano en los momentos difíciles.

Pero principalmente a Dios, quien siempre confió en mis capacidades y me dio la bendición de poder cristalizar uno de mis sueños.

Cristian Camilo Barrios Zarante

Esta dedicatoria va dirigida al Señor Supremo que me dio la fuerza necesaria para salir adelante, que mantuvo en mi corazón el deseo de superación para lograr alcanzar esta meta tan anhelada. Gracias le doy a Dios por mis padres y hermanos que siempre creyeron en mí y me apoyaron en todo momento. Gracias les doy a Dios por mi esposo porque ha sido el soporte y el pilar que faltaba en mi vida y que ayudo a sortear todos los malos momentos que se me presentaron, por su amor y dedicación y por creer en mi. Gracias le doy a Dios por mis familiares y amigos que me brindaron su apoyo incondicional y todo su cariño.

Que Dios lo bendiga.

Yanira Ulianova Carrascal Villalba

Agradecemos a nuestras familias, nuestros profesores y demás personas que nos apoyaron en todo momento y nos guiaron hacia metas exitosas como esta; especialmente a nuestros padres y nuestro director Gonzalo López Vergara.

AUTORIZACIÓN

Cartagena de Indias, Noviembre de 2005

Yo **Cristian Camilo Barrios Zarante**, identificado con número de cédula 73.187.895 de la ciudad de Cartagena, autorizo a la Universidad Tecnológica de Bolívar para hacer uso de mi trabajo de grado y publicarlo en el catálogo online de la Biblioteca.

_____

CRISTIAN CAMILO BARRIOS ZARANTE

AUTORIZACIÓN

Cartagena de Indias, Noviembre de 2005

Yo **Yanira Ulianova Carrascal Villalba**, identificado con número de cédula 22.808.533 de la ciudad de Cartagena, autorizo a la Universidad Tecnológica de Bolívar para hacer uso de mi trabajo de grado y publicarlo en el catálogo online de la Biblioteca.

_____

YANIRA ULIANOVA CARRACAL VILLABA

TABLA DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

El desarrollo del sector de las comunicaciones ha permitido un uso mas eficiente de la infraestructura de redes y el desarrollo de aplicaciones y contenido enriquecido, los cuales demandan mas ancho de banda y facilidades de conexión, de tal forma que el usuario final pueda tener acceso a estas nuevas aplicaciones y contenidos con menos tiempos de descarga, costos mas apropiados y sin inconvenientes de infraestructura.

La fiebre tecnológica se ha encaminado hacia tendencias inalámbricas. Paisajes cableados, emblemáticos de las telecomunicaciones durante décadas, dejan paso a escenarios donde las tecnologías inalámbricas surgen como alternativa a considerar. Las tecnologías de redes inalámbricas habilitan a través de señales de radio la conexión entre un dispositivo de cómputo y un sistema central de información. Así, un computador puede acceder a los recursos de una red empresarial, como a la opción de navegar en Internet.

En la exposición de las redes Wi – Fi[1], se definirán ciertos temas, entre los que se encuentran; la descripción histórica y/o evolución del estándar IEEE 802.11[2], topologías y funcionamiento de los dispositivos, velocidad contra modulación, seguridad inalámbrica, y algunos casos de estudio para la puesta en práctica de una red inalámbrica.

[1] Wi Fi: Wireless Fidelity.
[2] IEEE: Institute of Electrical and Electronics Engineers.

1 GENERALIDADES

1.1 ANTECEDENTES

El origen de las LAN[3] inalámbricas se remonta a la publicación en 1979 de los resultados de un experimento realizado por ingenieros de IBM[4] en Suiza, consistente en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados, publicados por el IEEE, pueden considerarse como el punto de partida en la línea evolutiva de esta tecnología.

En mayo de 1985, y tras cuatro años de estudios, la agencia federal del Gobierno de Estados Unidos encargada de regular y administrar en materia de telecomunicaciones, asignó las bandas ISM[5] 902-928 MHz, 2,400-2,4835 GHz, 5,725-5,850 GHz para uso en las redes inalámbricas basadas en Espectro Ensanchado. En la figura 1 podemos observar las bandas de frecuencia ISM.

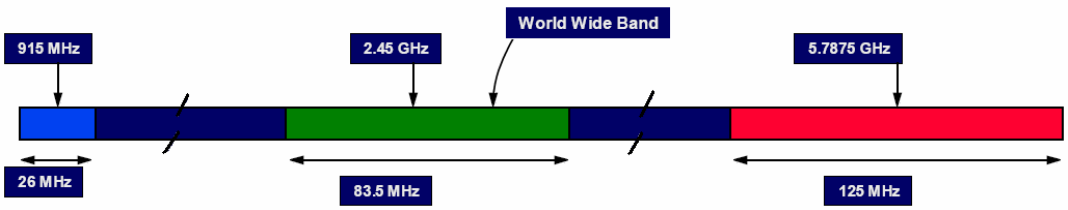


Figura 1: Bandas ISM utilizadas por las redes inalámbricas.

[3] LAN: Local Area Networks.
[4] IBM: International Business Machines Corporation.
[5] ISM: Industrial, Scientific and Medical.

La asignación de estas bandas de frecuencias propició una mayor actividad en el seno de la industria y ese respaldo hizo que las WLAN empezaran a dejar ya el entorno del laboratorio para iniciar el camino hacia el mercado.

Desde 1985 hasta 1990 se siguió trabajando más en la fase de desarrollo, hasta que en mayo de 1991 se publicaron varios trabajos referentes a WLAN operativas que superaban la velocidad de 1 Mbit/s, el mínimo establecido por el IEEE 802 para que la red sea considerada realmente una LAN, con aplicación empresarial.

La historia de las WLAN es bastante reciente, de poco más de una década. En 1989, en el seno de IEEE 802, se forma el comité IEEE 802.11, que empieza a trabajar para tratar de generar una norma para las WLAN, pero no es hasta 1994 cuando aparece el primer borrador, y habría que esperar hasta el año 1999 para dar por finalizada la norma.

En junio del año 1997 el IEEE ratificó el estándar para WLAN IEEE 802.11, que alcanzaba una velocidad de 2 Mbit/s, con una modulación de señal de espectro expandido por secuencia directa DSSS, aunque también contempla la opción de espectro expandido por salto de frecuencia FH. El 802.11 es una red local inalámbrica que usa la transmisión por radio en la banda de 2.4 Hz, o infrarroja, con regímenes binarios de 1 a 2 Mbit/s.

Un poco más tarde, en el año 1999, se aprobó el estándar 802.11b, una extensión del 802.11 para WLAN empresariales, con una velocidades de hasta 11 Mbit/s y

un alcance de 100 m, que al igual de 802.11, también emplea la banda de ISM de 2.4 GHz, utilizando la modulación DSSS.

El IEEE ratificó en julio de 1999 el estándar en 802.11a, que con la codificación OFDM[6] alcanza una velocidad de hasta 54 Mbit/s en la banda de 5 GHz, con un alcance limitado a 50 m.

El IEEE también ha aprobado en el año 2003 en el estándar 802.11g, compatible con el 802.11b, capaz de alcanzar una velocidad doble, es decir hasta 22 Mbit/s o llegar, incluso a 54 Mbit/s, para competir con los otros estándares que prometen velocidades mucho más elevadas pero que son incompatibles con los equipos 802.11b ya instalados.

En el 2004 fue aprobado el estándar IEEE 802.11i, para seguridad en redes Wi Fi. Este abre la posibilidad de que Wi Fi pueda ser ampliamente utilizado en entornos corporativos sin amenazar la seguridad de los sistemas.

Existen multitud de estándares definidos o en proceso de definición para redes inalámbricas 802.11 por la IEEE y que se pueden ser observados en la tabla 1.

[6] OFDM: Orthogonal Frequency Division Multiplexing.

ESTANDAR	GRUPOS DE TRABAJO
802.11	Especificaciones de la capa física y MAC para las LANs inalámbricas. Provee una velocidad de 1 o 2 Mbps de transmisión en la banda de 2.4 GHz.
802.11a	Estándar de comunicación en la banda de los 5 Ghz.
802.11b	Estándar de comunicación en la banda de los 2.4 Ghz.
802.11c	Especifica métodos para la conmutación inalámbrica, define las características que necesitan los APs para actuar como puentes (bridges).
802.11e	Estándar sobre la introducción del QoS en la comunicación entre PAs y TRs. Actúa como árbitro de la comunicación. Los servicio de QoS y de soporte multimedia son críticos en el ambiente de las redes inalámbricas del hogar donde voz, video y audio deben ser entregadas. Esto provee un ingrediente esencial para conquistar el mercado del cliente residencial.
802.11f	Estándar que define una práctica recomendada de uso sobre el intercambio de información entre el AP y el TR en el momento del registro a la red y la información que intercambian los APs para permitir la interportabilidad entre puntos de acceso de distintos fabricantes.
802.11g	Estándar que permite la comunicación en la banda de los 2.4 Ghz.
802.11h	Estándar que sobrepasa al 802.11a al permitir la asignación dinámica de canales para permitir la coexistencia de éste con el HyperLAN. Además define el TPC[7] según el cual la potencia de transmisión se adecua a la distancia a la que se encuentra el destinatario de la comunicación.
802.11i	Estándar que define la encriptación y la autentificación para complementar completar y mejorar el WEP. Es un estándar que mejorará la seguridad de las comunicaciones mediante el uso del TKIP[8]. Agrega el protocolo de seguridad AES[9] al estándar inalámbrico 802.11.
802.11m	Estándar propuesto para el mantenimiento de las redes inalámbricas.

Tabla 1: Algunos estándares definidos o en proceso de aprobación de la familia IEEE 802.11.

[7] TPC: Transmit Power Control.
[8] TKIP: Temporal Key Integrity Protocol.
[9] AES: Advanced Encryption Standard.

1.2 CLASIFICACIÓN DE LAS REDES INALAMBRICAS

Antes de situarnos dentro del mundo inalámbrico, lo más conveniente es clasificar las diferentes variantes que podemos encontrar: redes inalámbricas personales, de consumo y 802.11 (Wi – Fi).

1.2.1 Redes inalámbricas personales

Dentro del ámbito de estas redes podemos integrar a dos principales actores:

a) En primer lugar están las redes que usan el intercambio de información mediante infrarrojos. Estas redes son muy limitadas dado su corto alcance, la necesidad de visión sin obstáculos entre los dispositivos que se comunican y su baja velocidad (hasta 115 kbps). Se encuentran principalmente en computadores portátiles, PDAs[10], teléfonos móviles y algunas impresoras.

b) En segundo lugar el Bluetooth, estándar de comunicación entre pequeños dispositivos de uso personal, como pueden ser los PDAs, teléfonos móviles y computador portátil. Opera dentro de la banda de los 2.4 Ghz.

1.2.2 Redes inalámbricas de consumo

a) Redes CDMA[11] y GSM[12] . Son los estándares que usa la telefonía móvil empleados alrededor de todo el mundo en sus diferentes variantes.

[10] PDAs: Agendas electrónicas personales.
[11] CDMA: Code Division Multiple Access, estándar de telefonía móvil Estadounidense.

b) IEEE 802.16[13] son redes que pretenden complementar a las anteriores estableciendo redes inalámbricas metropolitanas en la banda de entre los 2 y los 11 Ghz.

1.2.3 Redes inalámbricas 802.11 - Wi Fi

Desde la aprobación definitiva en 1999 del estándar 802.11 proliferaron los estándares, como suele pasar siempre que un estándar aparece y los grandes fabricantes se interesan por él, aparecen diferentes aproximaciones al mismo lo que genera una incipiente confusión. Al hablar de Wi Fi nos referimos de igual modo a IEEE 802.11, pues estas redes se basan en este conjunto de estándares.

1.2.3.1 IEEE 802.11b

Es la primera extensión del 802.11 para WLAN, con una velocidad de 11 Mbps estandarizada por el IEEE y una velocidad de 22 Mbps por el desdoblamiento de la velocidad que ofrecen algunos fabricantes pero sin la estandarización del IEEE. Opera dentro de la frecuencia de los 2.4 Ghz.

Adolece de varios de los inconvenientes como son la falta de QoS[14], además de otros problemas como la masificación de la frecuencia en la que transmite y recibe, pues en los 2.4 Ghz funcionan teléfonos inalámbricos, teclados y ratones

[12] GSM: Group Special Mobile, Sistema Global para Comunicaciones Móviles, estándar de telefonía móvil Europeo.
[13] 802.16: Estándar conocido en el mundo de las comunicaciones como Wi – Max.
[14] QoS: Posibilidades de aseguro de Calidad de Servicio.

inalámbricos, hornos microondas, dispositivos Bluetooth, etc., lo cual puede provocar interferencias.

En el lado positivo está su rápida adopción por parte de una gran comunidad de usuarios debido principalmente a unos muy bajos precios de sus dispositivos, la gratuidad de la banda que usa y su disponibilidad gratuita alrededor de todo el mundo.

1.2.3.2 IEEE 802.11a

Fue la segunda aproximación a las WN[15] y llega a alcanzar velocidades de hasta 54 Mbps. Esta variante opera dentro del rango de los 5 Ghz dentro de los estándares del IEEE y hasta 72 y 108 Mbps con tecnologías de desdoblamiento de la velocidad ofrecidas por diferentes fabricantes, pero no están estandarizadas por el IEEE.

Sus principales ventajas son su velocidad, la base instalada de dispositivos de este tipo, la gratuidad de la frecuencia que usa y la ausencia de interferencias en la misma.

Sus principales desventajas son su incompatibilidad con los estándares 802.11b y 802.11g, y la no incorporación a la misma de QoS.

[15] WN: Wireless Networks.

1.2.3.3 IEEE 802.11g

Es la tercera aproximación a las WN, y se basa en la compatibilidad con los dispositivos 802.11b y en el ofrecer unas velocidades de hasta 54 Mbps. Existen versiones propietarias[16] de esta tecnología que ofrecen velocidades de 100 Mbps, pero no estandarizadas por la IEEE. Funciona dentro de la frecuencia de 2.4 Ghz.

Dispone de las mismas ventajas e inconvenientes que el 802.11b.

En la figura 2, se puede observar el ámbito y/o cobertura de los diferentes estándares inalámbricos.

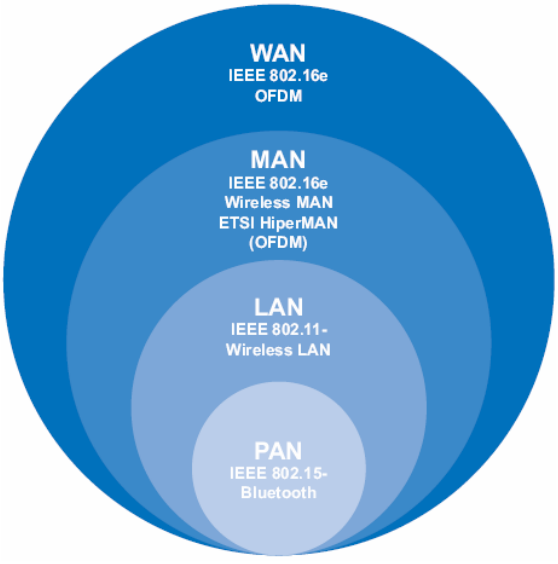


Figura 2[17]: Cobertura de los diferentes estándares inalámbricos.

[16] Por ejemplo US Robotics.
[17] Figura tomada de [4].

2 TECNOLOGIA WI FI

2.1 TOPOLOGÍAS DE RED

Al hablar de topología nos referimos a la disposición lógica de los dispositivos. A los equipos conectados a una red inalámbrica los denominamos estaciones móviles. La estructura básica de una red inalámbrica la denominamos BSS[18]. Puede pensarse en un BSS como la mínima estructura en la cual se pueden organizar un grupo de estaciones móviles que se comunican entre si. En el mundo Wireless existen dos topologías básicas; la topología Infraestructura y la topología Independiente.

2.1.1 Topología Infraestructura

En este caso, cada BSS esta organizado alrededor de una estación que puede permitir el acceso a una red mayor, por ejemplo, a una LAN cableada.

Esta estación recibe el nombre de punto de acceso[19]. El punto de acceso sirve para encaminar las tramas hacia una red convencional o hacia otras redes distintas. Para poder establecerse la comunicación, todos los nodos deben estar dentro de la zona de cobertura del AP. El esquema de esta topología se encuentra ilustrado en la figura 3.

[18] BSS: Basic Service Set.
[19] En Ingles: Access Point o AP.

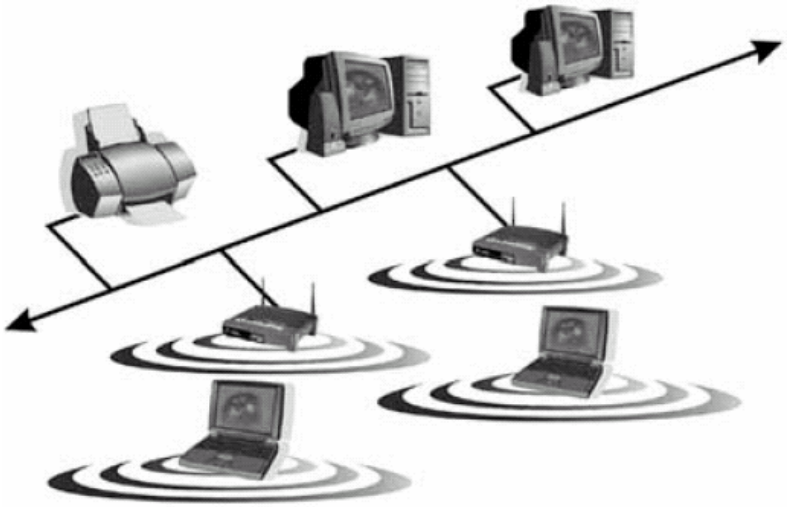


Figura 3[20]: Topología Infraestructura.

Los BSS de redes infraestructura se pueden agrupar formando una entidad mayor conocida como ESS[21]. Un ESS es simplemente una red conformada por un conjunto de BSS donde la conectividad entre BSS esta dada gracias a las funciones de puente de los puntos de acceso. El medio por el cual están conectados los puntos de acceso se denomina DS[22]. En la figura 4 se observa el conjunto de servicio extendido.

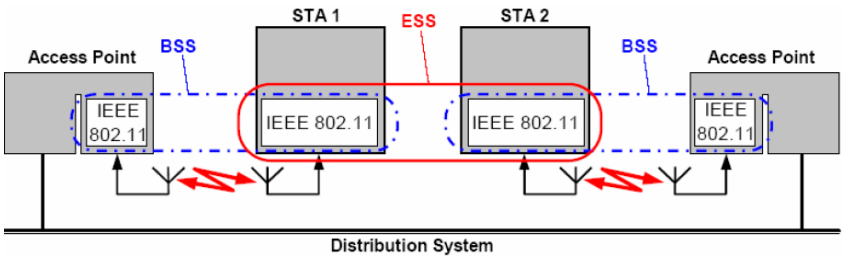


Figura 4[23]: Conjunto de servicio extendido.

[20] Figura tomada de [8].
[21] ESS: Extended Service Set.
[22] DS: Distribution System.
[23] Figura tomada de [11].

2.1.2 Topología Independiente

Son redes formadas por un solo BSS, denominado IBSS[24], que no se estructuran alrededor de ninguna estación con funciones particulares, sino que distribuyen las tareas de coordinación entre si, tal y como se observa en la figura 5.

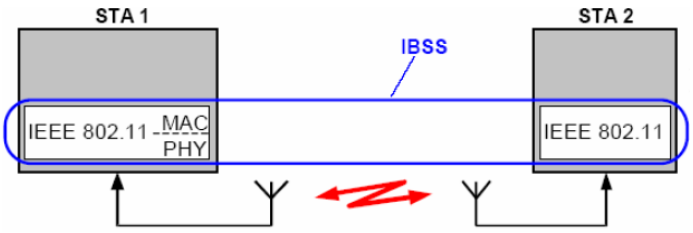


Figura 5[25]: Conjunto de servicio básico independiente.

Cada dispositivo se puede comunicar con todos los demás de forma directa, como se aprecia en la figura 6. A más dispersión geográfica de cada nodo más dispositivos pueden formar parte de la red, aunque algunos no lleguen a verse entre si, lo que conlleva a que el radio de cobertura sea limitado.

Figura 6[26]: Topología Ad-Hoc.

[24] IBSS: Independent BSS.
[25] Figura tomada de [11].

2.2 ENSANCHAMIENTO DE ESPECTRO[27]

Es una técnica por la cual la una señal transmitida de pequeño ancho de banda es extendida a lo largo de una banda más amplia. Este ensanchamiento, trae como beneficio una mayor resistencia a la interferencia de señales no deseadas. Existen fundamentalmente tres formas de espectro ensanchado: Saltos en Frecuencia[28], Secuencia Directa [29] y División en frecuencia ortogonal[30].

2.2.1 Saltos en Frecuencia

En saltos en frecuencia se divide el espectro disponible en una serie de sub-bandas o canales. Las transmisiones se realizan en diferentes canales en diferentes momentos. La clave esta en que la secuencia de saltos de canales es conocida, no solo por el transmisor que la genera, sino también por el receptor, por lo que este puede seguir la secuencia y demodular la señal recibidos en cada canal. Si un receptor no conoce la secuencia de saltos, no podrá comprender la señal recibida.

La figura 7 muestra un esquema de FH, además de demostrar el por que de la resistencia a la interferencia de banda angosta. Aun si es muy elevada la potencia de la señal interferente, esta podrá afectar a unos pocos canales a la vez, por lo que no lograra interrumpir la comunicación completa.

[26] Figura tomada de [8].
[27] En Ingles: Spread Spectrum SS.
[28] En Ingles: Frequency Hopping FH.
[29] En Ingles: Direct Sequence DS.
[30] En Ingles: Orthogonal Frequency Division Multiplexing OFDM.

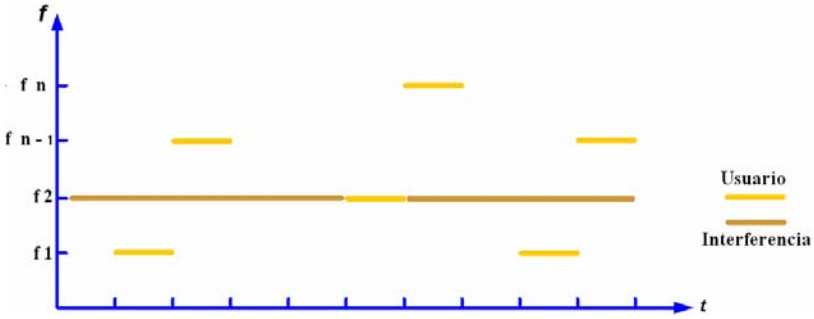


Figura 7: Saltos en frecuencia.

2.2.2 Secuencia Directa

En secuencia directa lo que se hace es modificar la señal a enviar multiplicándola por otra señal de mucha mayor frecuencia, conocida como secuencia de ensanchado. Una de las razones por las cuales se utiliza esta forma de ensanchamiento de espectro es su resistencia a la interferencia de banda angosta, esto se debe a la existencia de un proceso de demodulación en el receptor, siendo este equivalente al de modulación, por ende la señal interferente se ve ensanchada en el receptor y su potencia efectiva disminuida al expandirse el espectro. El esquema de secuencia directa se puede apreciar en la figura 8.

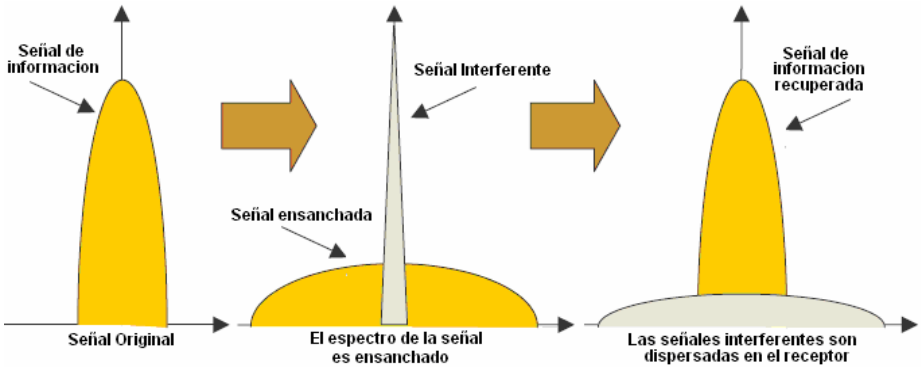


Figura 8: Envió y recepción de una señal ensanchada con secuencia directa.

2.2.3 División en frecuencia ortogonal

Los sistemas de transmisión OFDM se caracterizan por separar la información a transmitir en varios subconjuntos de menor tamaño, enviando símbolos simultáneamente en cada canal. De esta manera se consigue: alta eficiencia espectral, resistencia a las interferencias de banda estrecha y evitar la distorsión multitrayecto.

La distorsión multitrayecto genera una alta ISI[31]. En un escenario de estas características, con una sola portadora, los procedimientos habituales para eliminar la ISI son ineficaces. Supongamos un flujo original de datos, con una tasa de transmisión r. Si lo dividimos en N subconjuntos de datos, la nueva tasa de transmisión pasara a ser r_n = r/N. Cada uno de estos nuevos flujos es transmitido por separado en diferentes portadoras, de forma que la nueva tasa r_n puede ser suficientemente baja como para que la distorsión multitrayecto sea eliminada con comodidad.

Para maximizar la eficiencia espectral, tendremos que escoger subportadoras muy cercanas entre si. Con una adecuada conformación de la forma de pulso, podemos conseguir que aunque los espectros de las subportadoras moduladas se solapen, lo hagan de tal manera que a determinadas frecuencias, las contribuciones de cada subportadora sean nulas para las demás. Esto se debe a

[31] ISI: Inter Symbol Interference.

la ortogonalidad de los canales, la señal de un canal no interfiere con la de los canales adyacentes porque el máximo del espectro de un canal coincide con los ceros en amplitud de los canales linderos. Lo mencionado anteriormente puede ser observado en la figura 9.

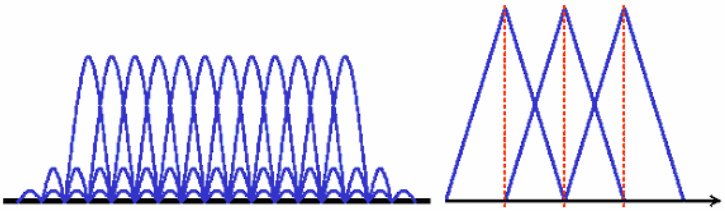


Figura 9: Espectro y ortogonalidad de OFDM.

En la tabla 2 se pueden apreciar los sistemas de modulación utilizados por 802.11.

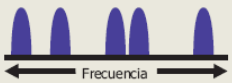
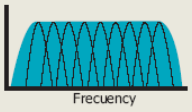
Banda Angosta	FHSS	DSSS	OFDM
■ Señal angosta ■ Alta amplitud ■ Baja frecuencia	■ Transmite los datos en portadoras que cambian o saltan de frecuencia en funcion del tiempo	■ Banda angosta dispersa sobre un amplio espectro ■ Baja amplitud	■ Transmite señales simultaneas de alta elocidad ■ Divide el espectro en varios sub-portadoras
Ventajas ■ Larga distancia ■ NLOS, no requiere LOS y viaja a traves de obstaculos	Ventajas ■ Alta tolerancia a interferencia ■ Alta seguridad contra intercepcion de señal	Ventajas ■ Alta velocidad ■ Mas resistente contra interferencia que banda angosta	Ventajas ■ Alta eficiencia espectral ■ Alta velocidad de transmision ■ No requiere retransmision de datos
Desventajas ■ Baja velocidad ■ 9600 bps ■ Sujeto a interferencia	Desventajas ■ Baja/Media velocidad ■ Dificyultad en P MP ■ Dificil de sincronizar en Larga distancia	Desventajas ■ Ciertas afectaciones por ruido y multitrayectoria ■ Proximo a su limite de velocidad	Desventajas ■ Costo ■ Requiere mayor capacidad de procesamiento
			

Tabla 2[32]: Comparación entre los sistemas de modulación utilizados por 802.11 y banda angosta.

[32] Tabla tomada de [4].

3 ARQUITECTURA DE LA CAPA FÍSICA Y CAPA MAC DE WI - FI

Las redes inalámbricas básicamente se diferencian de las redes conocidas hasta ahora por el enfoque que toman de los niveles más bajos de la pila OSI, el nivel físico y el nivel de enlace, los cuales se definen por el IEEE 802.11.

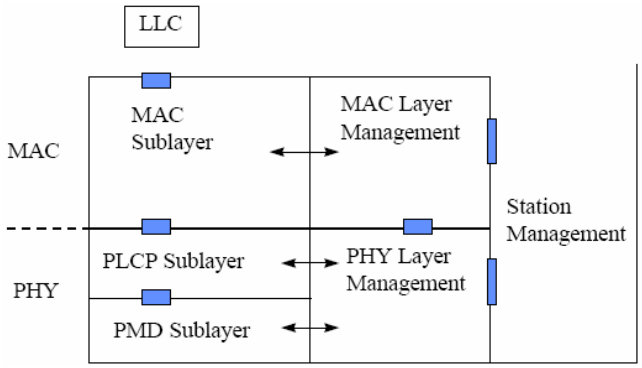


Figura 10: Capa física y Capa MAC de 802.11.

La capa más baja es la física, en la figura10. Esta es la capa lógica encargada de definir los detalles físicos de la red, como ser potencia transmitida, esquema de modulación, etc.

Sobre la capa física, se ubica la capa de control de acceso al medio MAC. Esta es la capa que permite la coordinación en el uso del medio de transmisión común entre todas las estaciones que desean comunicarse.

3.1 CAPA FISICA DE 802.11

La capa física de los estándares 802.11 esta dividida en dos sub-capas: Physical Layer Convergence Procedure y Physical Medium Dependent.

- Physical Layer Convergence Procedure: Esta sub-capa permite la integración de la capa MAC[33] con la capa física, mediante la añadidura de un preámbulo que depende del esquema de modulación particular que sea utilizado.

- Physical Medium Dependent: Esta sub-capa se encarga, en cambio, de poner los bits en el aire, es decir, es la capa de radiofrecuencia propiamente dicha, que especifica, entre otras cosas, el esquema de modulación y velocidad de transmisión.

Cuando transmitimos información entre dos dispositivos inalámbricos, la información viaja entre ellos en forma de tramas. Estas tramas son básicamente secuencias de bits.

Las secuencias de bits están divididas en dos zonas diferenciadas, la primera es la cabecera y la segunda los datos que se quieren transmitir.

La cabecera es necesaria por razones de gestión de los datos que se envían. Dependiendo de la forma en la que se module la cabecera (o preámbulo), podemos encontrarnos con diferentes tipos de tramas, estas serán descritas para el 802.11 Original, y para sus tres principales variantes: 802.11a, b y g.

[33] MAC: Medium access control.

3.1.1 Estándar IEEE 802.11 Original

El estándar 802.11 original, tal como fue publicado en 1997, determina el uso de dos formas de transmisión con uso de espectro ensanchado diferentes: Frequency Hopping (Saltos en Frecuencia) y Direct Sequence (Secuencia Directa).

3.1.1.1 802.11 Saltos en Frecuencia

El estándar 802.11 original utiliza las bandas ISM alrededor de 2.4 GHz. El esquema de FH divide las bandas en canales de 1 MHz cada uno: los saltos en frecuencia se producen entre estos canales.

En el caso de FH la trama es como se aprecia en la figura 11.

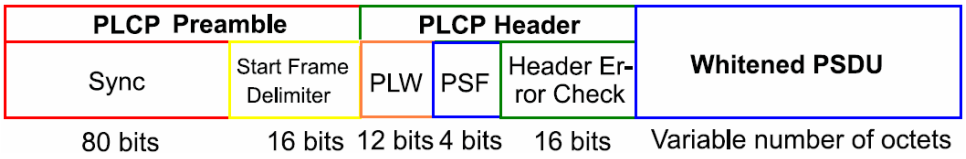


Figura 11[34]: Formato de la trama de PLCP[35].

3.1.1.1.1 El Preámbulo

Permite la sincronización entre la estación móvil transmisora y la receptora. Esta conformado por dos campos:

[34] Figura tomada de [1].
[35] PLCP: Physical Layer Convergence Procedure.

a) SYNC: Permite la sincronización. Es una secuencia de 80 ceros y unos alternados. El receptor escucha el canal en busca de esta secuencia. Cuando la encuentra, toma el sincronismo de esta secuencia, al tiempo que sabe que se encuentra en la parte inicial de una nueva trama.

b) Start Frame Delimiter[36]: Marca el comienzo de la trama, permitiendo al receptor reconocer que, a partir de esa posición, viene información útil. El patrón utilizado es: 0000 1100 1011 1101.

3.1.1.1.2 La Cabecera

Contiene parámetros específicos de la capa física, permitiendo una interpretación adecuada de la trama de datos que sigue. Esta formada por tres campos:

a) PLW: PSDU Length Word. Indica la longitud de la PSDU.

b) PSF: PLCP Signalling Field. Indica la velocidad de transmisión en pasos de 500 Kbps. Se encuentran definidos en la IEEE 802.11 los esquemas de modulación para 1 y 2 Mbps. La tabla 3, presenta la codificación de estos cuatro bits.

c) Header Error Check: Debido a la importancia de la cabecera, se envía a continuación de la misma este campo de Cheksum[37] o CRC, que permite detectar errores que se hayan producido durante la transición de la trama.

[36] En Español: Delimitador de trama de inicio.
[37] Checksum (SUMmation CHECK). Suma de chequeo: Esquema simple de detección de errores, donde cada mensaje transmitido es acompañado con un valor numérico basado en el número de grupo de bits del mensaje.

Bit	Parameter name	Parameter values	Description
0	Reserved	Default = 0	Reserved
1:3	PLCP_BITRATE	b1 b2 b3 = Data Rate 0 0 0 = 1.0 Mbit/s, 0 0 1 = 1.5 Mbit/s, 0 1 0 = 2.0 Mbit/s, 0 1 1 = 2.5 Mbit/s, 1 0 0 = 3.0 Mbit/s, 1 0 1 = 3.5 Mbit/s, 1 1 0 = 4.0 Mbit/s, 1 1 1 = 4.5 Mbit/s	This field indicates the data rate of the whitened PSDU from 1 Mbit/s to 4.5 Mbit/s in 0.5 Mbit/s increments.

Tabla 3: Descripción de los bits de PSF[38].

3.1.1.1.3 Trama Física

La trama física[39] es transmitida a continuación de la cabecera.

3.1.1.2 802.11 Secuencia Directa

En el esquema DS cada bit de la secuencia de datos a ser transmitida es codificado como una secuencia de unos y ceros (habitualmente denominados chips) transmitidos a mayor velocidad. Se utilizan secuencias de ensanchado, conocidas como secuencias de Barker, de 11 chips de longitud. De esta manera:

- Si se desea transmitir un 1, se envían los siguientes 11 chips: 01001000111.
- Si se desea transmitir un 0, se envían los siguientes 11 chips: 10110111000. En la figura 12 se puede ver un esquema del proceso de ensanchamiento.

[38] Figura tomada de [1].
[39] En Ingles: Physical Layer Service Data Unit – PSDU.

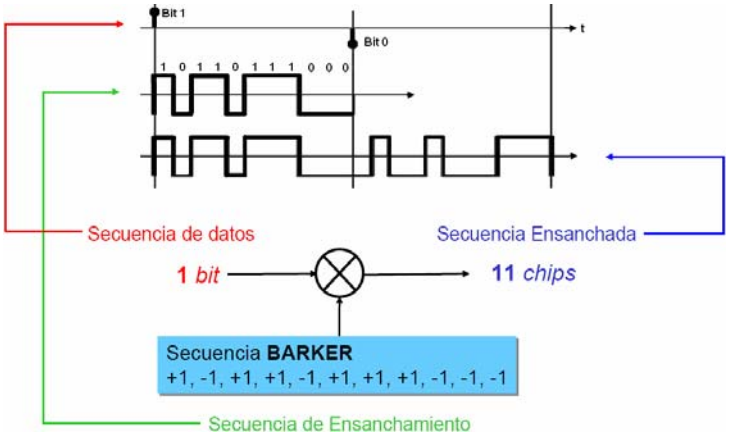


Figura 12[40]: Ensanchado mediante secuencia Barker.

Al igual que en el caso de FH, se dividen las bandas alrededor de 2.4 GHz en varios canales, pero en este caso los canales son de 5 MHz cada uno.

Los chips son transmitidos utilizando sistemas de modulación diferencial de la fase, es decir, sistemas en los cuales los bits son codificados como la diferencia de fase entre dos símbolos consecutivos.

Los sistemas de modulación especificados en el estándar IEEE 802.11 para su uso con DS son: DBPSK[41] y DQPSK[42].

a) DBPSK: Codifica 1 chip por símbolo, de acuerdo a si la diferencia de fase respecto del símbolo anterior es 0º o 180º.

Esta modulación se utiliza cuando se transmite a 1 Mbps, esto se puede clarificar en la figura 13.

[40] Figura tomada de [11].
[41] DBPSK: Differential Binary Phase Keying.
[42] DQPSK: Differential Quad Phase Shift Keying.

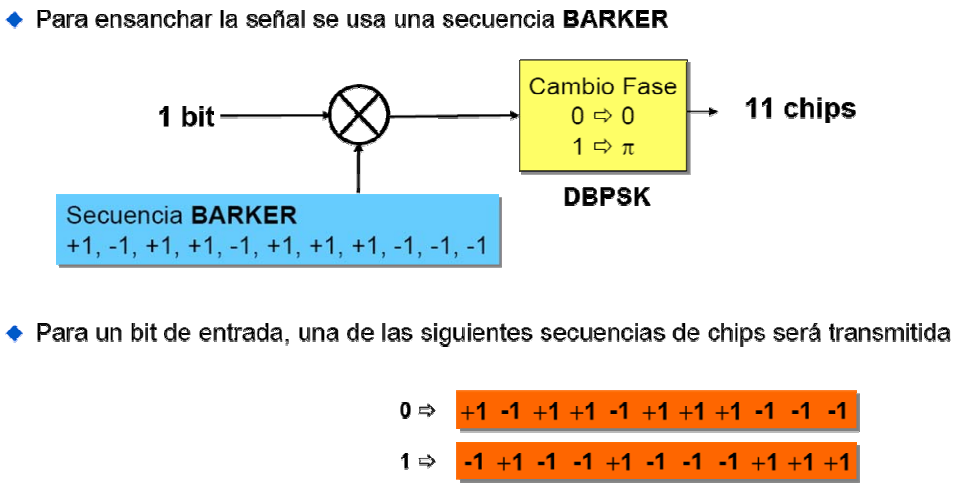


Figura 13[43]: Ensanchamiento y modulación para 1 Mbps.

b) DQPSK: Codifica 2 chips por símbolo, de acuerdo a si la diferencia de fase respecto del símbolo anterior es de 0º, 90º, 180º o 270º. Esta modulación se utiliza cuando se transmite a 2 Mbps, lo cual se puede observar en la figura 14.

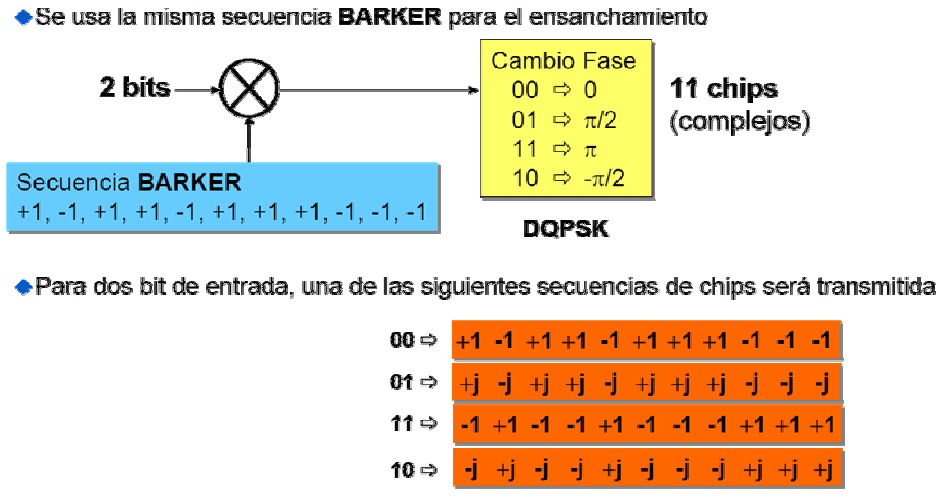


Figura 14[44]: Ensanchamiento y modulación para 2 Mbps.

[43] Figura tomada de [11].

Es importante remarcar la distinción que se hace entre bits, chips y símbolos:

a) Bits: Son aquellos ceros y unos correspondientes a la secuencia de datos que se desea enviar.

b) Chips: Son los ceros y unos correspondientes a secuencia ensanchada. En el caso de IEEE 802.11 hay 11 chips por cada bit.

c) Símbolos: Son aquellas señales que son verdaderamente transmitidas en el canal de radiofrecuencia. Dicho de otra manera, los símbolos codifican los bits para ser transmitidos por el medio físico. En la nomenclatura de transmisión se le llama a cada símbolo por segundo baudio.

En el caso de Secuencia Directa, la capa de convergencia PLCP[45] agrega bits en el principio de la trama de la manera en que se muestra en la figura 15.

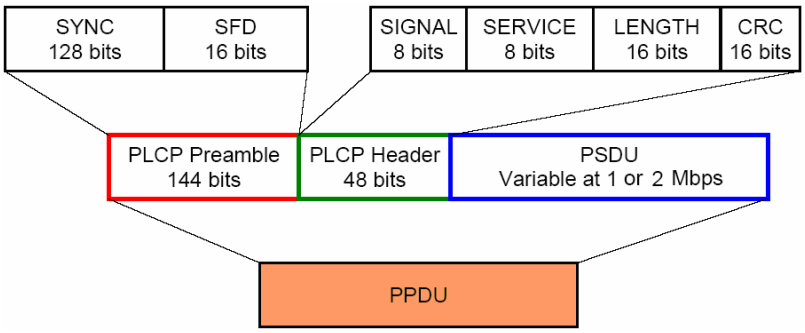


Figura 15[46]: Esquema del formato de la PPDU en secuencia directa[47].

[44] Figura tomada de [11].
[45] PLCP: Physical Layer Convergence Procedure.
[46] Figura tomada de [1].
[47] PPDU: PLCP protocol data unit.

3.1.1.2.1 El Preámbulo

Al igual en el caso de Frequency Hopping, el preámbulo permite la sincronización entre la estación móvil de la transmisora y la receptora y esta conformado por dos campos:

a) SYNC: Permite la sincronización propiamente dicha. Es una secuencia de 128 unos. Si bien parece difícil recuperar el sincronismo a través de una secuencia de todos unos, hay que recordar que estos unos son desordenados justo con el resto de la trama.

b) Start Frame Delimiter: Al igual que en el caso de FH, marca el comienzo de la trama, permitiendo al receptor reconocer que, a partir de esa posición, viene información útil. El patrón utilizado es: 0000 0101 1100 1111.

3.1.1.2.2 La Cabecera

La cabecera contiene parámetros específicos de la capa física. En el caso de DS, esta formada por cuatro campos:

a) Signal: Identifica la tasa de transmisión de la trama MAC. Si bien hay ocho bits, solo hay dos tasas de transmisión especificas: 1 Mbps, denotada por los bits 0000 1010 y 2 Mbps, denotada por los bits 0001 0100.

b) Service: Suelen agregarse campos que, si bien no tienen uso al momento de publicarse el estándar, podrían ser utilizados en el futuro. Se le deja en todo ceros.

c) Length: Es la longitud de la PSDU.

d) CRC: Se incluye un CRC para proteger el header de posibles errores durante la transmisión.

3.1.2 Estándar IEEE 802.11b HR/DSSS

El estándar IEEE 802.11 fue modificado en 1999 para permitir aumentar las velocidades de transmisión. Dado que hacia 1999 ya existía capacidad instalada de equipos que respetaban la norma tal como había sido generada dos años antes, se realizo una extensión que sea compatible hacia atrás, de manera de reducir los costos de instalación de nuevos equipos y aumentar las posibilidades de inserción.

Al realizar la actualización del estándar se opto en cambio por realizar una extensión de Direct Sequence, dando como resultado lo que se conoce como HR/DSSS[48], que permite transmitir a 1, 2, 5.5 y 11 Mbps. Las dos primeras tasas de transmisión son implementadas exactamente de la misma forma en que fue especificado DS en el estándar original. La extensión de 1999 especifica como

[48] HR/DSSS: High Rate Direct Sequence Spread Spectrum.

alcanzar las dos tasas mayores: 5.5 y 11 Mbps. Por eso existen dos tipos de tramas a nivel de convergencia:

a) Trama larga: Es exactamente igual a la trama de 802.11 DS y es incorporada por compatibilidad hacia atrás.

b) Trama corta: Solo puede utilizarse si todas las estaciones móviles la reconocen[49] y esta diseñada para ser mas eficiente.

3.1.2.1 Formato de Trama Larga

La trama larga es igual en estructura a la presentada en la figura 20. Sin embargo, algunos de los campos son interpretados de manera ligeramente diferentes para poder incorporar las nuevas especificaciones,

La estructura de la trama larga se puede apreciar en la figura 16.

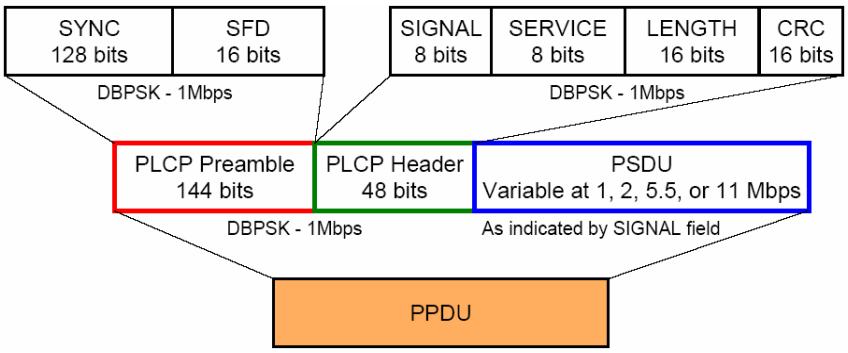


Figura 16[50]: Formato largo de la PPDU.

[49] Es decir, si todas las estaciones móviles han sido diseñadas luego de la elaboración del estándar 802.11b.
[50] Figura tomada de [2].

En particular cambiaron los siguientes campos de la cabecera:

a) Signal: Agrega dos identificadores nuevos para las dos nuevas velocidades: 00110111 para 5.5 Mbps y 01101110 para 11 Mbps.

b) Service: Se le agrega funcionalidad a este campo que antes no la tenía.

El bit 2 de este campo sirve para determinar si la frecuencia de transmisión y la tasa de símbolos fueron derivadas del mismo reloj.

El bit 3 permite determinar si se utiliza CCK o PBCC en la trama MAC.

El bit 7 permite agregar un bit al campo Length en caso que los bits dispuestos originalmente para el mismo no alcancen. El resto de los bits sigue sin uso.

3.1.2.2 Formato de Trama Corta

La figura 17 muestra la estructura de la trama corta.

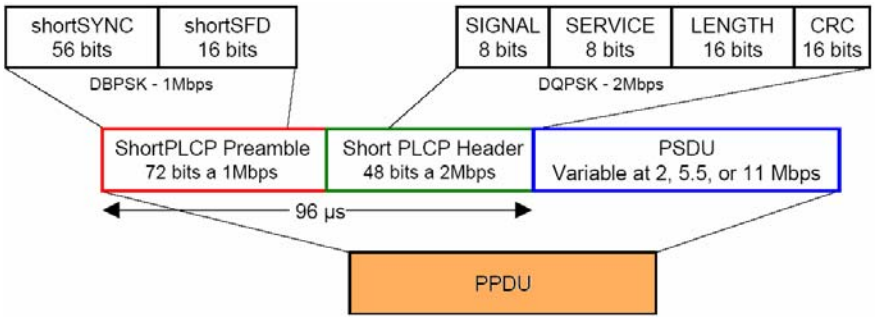


Figura 17[51]: Formato corto de la PPDU.

[51] Figura tomada de [2].

Si se la compara con la figura 16 (formato largo de la PPDU), es fácil notar cuales son las principales diferencias entre la trama corta y la larga:

- El campo de sincronización es mas corto, 56 bits contra 128 bits.
- El Start Frame Delimiter es igual en ambas tramas, pero los bits tienen el orden invertido. Esto permite identificar unívocamente a la trama como corta.
- La cabecera se envía a 2 Mbps, utilizando DQPSK, en vez de enviarla a 1 Mbps usando DBPSK.

3.1.3 Estándar IEEE 802.11a OFDM

Al mismo tiempo que se extendió el estándar 802.11 DS, también se agrego una nueva forma de acceso al medio físico que permite velocidades de transmisión de datos mucho más altas, de 6 a 54 Mbps: 802.11a. Sin embargo, al tomarse un camino completamente diferente al de FH y DS en el estándar original, se decidió utilizar una banda de frecuencias completamente distinta de manera que no haya problemas de convivencia de redes de diferentes estándares. La banda de frecuencias ISM elegida es aquella que se encuentra alrededor de los 5 GHz.

La elección de una banda de frecuencias facilita la convivencia espacial de redes respetando diferentes estándares, también implica impedimento para la escalabilidad de redes 802.11 ya instaladas que puedan ser actualizadas

progresivamente a una red 802.11a. OFDM[52] es la forma de compartir el medio elegido para 802.11a. Las redes 802.11a utiliza 52 subportadoras, entre los 5.15 - 5.825 GHz. El espaciado entre ellas es de 312,5 KHz.

Una representación grafica de la estructura de la trama PLCP se encuentra en la figura 18. En el caso de 802.11a, la subcapa de convergencia agrega no solo bits al comienzo de la trama, sino también al final.

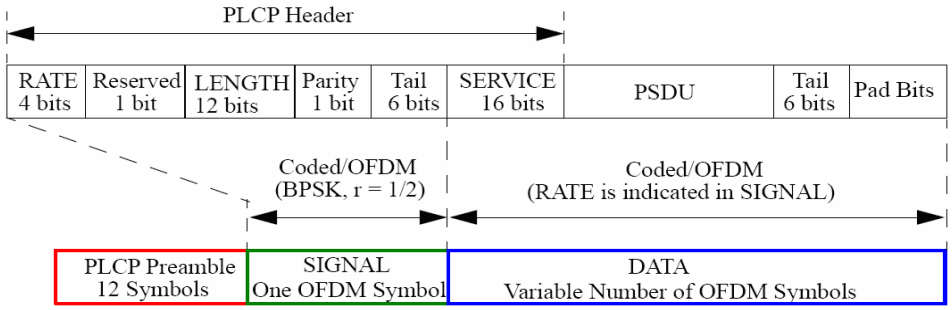


Figura 18[53]: Formato de la PPDU en OFDM.

3.1.3.1 El Preámbulo

El preámbulo esta conformado por una secuencia corta entrenamiento de 10 símbolos y dos secuencias largas de entrenamiento de 2 símbolos. Las secuencias cortas de entrenamiento permiten la detección de la señal, el control de la ganancia de la antena receptora y el ajuste grueso de sincronismo, entre otras cosas. Las secuencias largas permiten un ajuste fino del sincronismo y otros parámetros de recepción.

[52] OFDM: Orthogonal Frequency Division Multiplexing.
[53] Figura tomada de [3].

3.1.3.2 La Cabecera

La mayor parte de la cabecera PLCP es siempre enviada con el esquema de modulación BPSK y con un código convolucional. El header esta conformado por varios campos:

a) Rate: Especifica la tasa de transmisión.

b) Reserved: Un bit sin con uso reservado para futuras aplicaciones.

c) Length: Especifica el numero bytes de la trama de datos PSDU que viene a continuación de la cabecera PLCP.

d) Parity Bit: Es un bit de paridad de los bits anteriores, utilizado para detectar errores en el header.

e) Tail: Son seis bits necesarios para terminar el código convolucional.

f) Service: Los bits 0 – 6 son utilizados para el sincronismo en el receptor, los bits 7 – 15 se dejan para aplicaciones futuras.

3.1.3.3 Terminador

En 802.11a es necesaria la cola para poder terminar limpiamente el código convolucional. Para ello se ubican los primeros seis bits de la cola, marcados como Tail en la figura 18. El resto de los bits, marcados como Pad, son necesarios

para completar la trama, dado que OFDM solo puede transmitir múltiplos de bloques de bits de longitud dada.

3.1.4 Estándar IEEE 802.11g

Debido al impedimento de las redes 802.11a de no permitir la escalabilidad, convino realizar una nueva actualización del estándar, conocida como 802.11g, que permita la transmisión a velocidades tan altas como 802.11a, pero en la misma banda de frecuencia que HR/DSSS (802.11b) y DS (802.11 Original) de manera de aprovechar la base de equipos ya instalados. El estándar define tres tipos de capas PLCP diferentes. Esta diversidad se debe a la necesidad de compatibilidad hacia atrás con 802.11b. Los tres tipos de trama son:

3.1.4.1 Con preámbulo y cabeceras largas

Es exactamente igual a las tramas con preámbulo y cabeceras largas especificadas en 802.11b, salvo pequeñas diferencias hechas para acomodar algunas especificaciones del nuevo estándar. Este tipo de tramas es compatible con HR/DSS a 1, 2, 5.5 y 11 Mbps y con los esquemas opcionales DSSS/OFDM y ERP/PBCC.

3.1.4.2 Con preámbulo y cabeceras cortas

Es exactamente igual a las tramas con preámbulos y cabeceras cortas especificadas en 802.11b, salvo pequeñas diferencias hechas para acomodar

algunas especificaciones del nuevo estándar. Este tipo de tramas es compatible con HR/DSSS a 2, 5.5 y 11 Mbps y con los esquemas opcionales DSSS/OFDM y ERP/PBCC.

3.1.4.3 Con preámbulo, cabecera y terminador específicos

Es exactamente igual a las tramas especificadas en 802.11a, salvo con algunas modificaciones menores.

Habiendo descrito la trama, sistemas de modulación y velocidades permitidas por los estándares 802.11 original, a, b y g, podemos realizar un compendio de los mismos en la tabla 4.

		802.11b @2.4 GHz		802.11g @2.4 GHz		802.11a @5.2 GHz	
Rate, Mbps	Single/Multi Carrier	Mandatory	Optional	Mandatory	Optional	Mandatory	Optional
1	Single	Barker		Barker			
2	Single	Barker		Barker			
5.5	Single	CCK	PBCC	CCK	PBCC		
6	Multi			OFDM	CCK-OFDM	OFDM	
9	Multi				OFDM, CCK-OFDM		OFDM
11	Single	CCK	PBCC	CCK	PBCC		
12	Multi			OFDM	CCK-OFDM	OFDM	
18	Multi				OFDM, CCK-OFDM		OFDM
22	Single				PBCC		
24	Multi			OFDM	CCK-OFDM	OFDM	
33	Single				PBCC		
36	Multi				OFDM, CCK-OFDM		OFDM
48	Multi				OFDM, CCK-OFDM		OFDM
54	Multi				OFDM, CCK-OFDM		OFDM

Tabla 4[54]: Velocidad vs. Modulación de los principales estándares 802.11.

[54] Tabla tomada de [7].

3.2 CAPA CONTROL DE ACCESO AL MEDIO DE 802.11

3.2.1 El Acknowledgement

En las comunicaciones inalámbricas no existe garantía de una transmisión confiable en el medio, debido a las posibles interferencias, pues se utilizan bandas ISM, además de la atenuación variable de la señal si se esta en movimiento. Por esto se necesito diseñar un sistema que ofreciera al transmisor la manera de saber si el receptor había obtenido el mensaje enviado sin errores. La forma básica de lograr esto es exigiendo al receptor que le comunique la recepción correcta al transmisor enviando una trama de ACK; como se muestra en la figura 19. La trama de ACK también puede ser corrompida en el trayecto del receptor al transmisor del mensaje original, de manera que este último puede no enterarse de la transmisión correcta de su mensaje. Este problema se soluciona obligando al transmisor a tomar nota del tiempo desde que envió el mensaje, si pasado una cantidad de tiempo máxima no ha recibido ACK, asume que la trama no fue recibida correctamente y vuelve a enviarla.

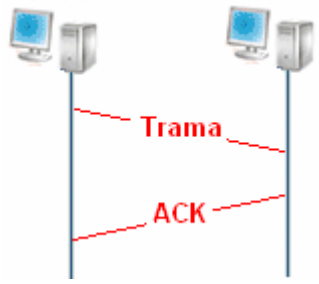


Figura 19: Confirmación de recepción correcta de la trama.

3.2.2 Las Colisiones

Para comprender mejor el fenómeno de las colisiones observemos la figura 20, donde dos estaciones móviles A y C desean comunicarse con una tercera estación móvil B. Cada una comienza a transmitir independiente de la otra. Al llegar los mensajes a la estación B, estos colisionan, de manera que la estación B no puede entender ninguno de los dos mensajes.

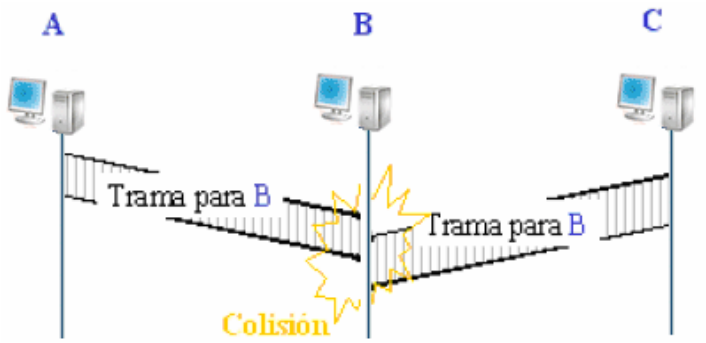


Figura 20: Colisión en la transmisión.

Existen fundamentalmente dos formas de soluciones este problema: Control Centralizado y Control Distribuido**.**

3.2.2.1 Control Centralizado

Una estación toma el control del medio y distribuye el tiempo destinado para transmisión entre todas las estaciones presentes de manera que no haya colisiones. El estándar IEEE 802.11 llama a esta solución PCF[55].

[55] PCF: Point Coordination Function.

3.2.2.2 Control Distribuido

Las estaciones transmiten de forma independiente, pero implementan estrategias para evitar las colisiones. IEEE 802.11 denomina este sistema como DCF[56]. Este modo de acceso se basa fundamentalmente en CSMA/CA. De las dos alternativas para acceso al medio especificadas por IEEE 802.11 la mas usada es DCF.

3.2.3 CSMA/CA

Una de las estrategias utilizadas para disminuir la posibilidad de colisión se denomina CSMA/CA[57]. Antes de transmitir datos, la estación móvil A, para el caso anterior, envía un tono piloto para avisar que desea transmitir. Luego de enviar el piloto, la estación A espera un tiempo prudencial para que todas las estaciones oigan el piloto. Este tiempo esta determinado por el máximo retraso de comunicación entre las estaciones de una misma red. Toda estación móvil, por ejemplo C en el caso anterior, debe oír el canal antes de enviar una trama a B. Si la estación móvil C detecta el piloto enviado por A (Carrier Sense), no envía nada a B, evitando de esta manera la colisión (Collision Avoidance). Dado que C seguirá teniendo información para enviar a B, espera un tiempo (Backoff time) que considere suficiente antes de intentar transmitir nuevamente. Por lo anterior CSMA/CA se le suele llamar "escucha antes de hablar". Lo anterior se puede comprender mejor al apreciar la figura 21.

[56] DCF: Distributed Coordination Function.
[57] CSMA/CA: Carrier Sense Multiple Access with Collision Avoidance.

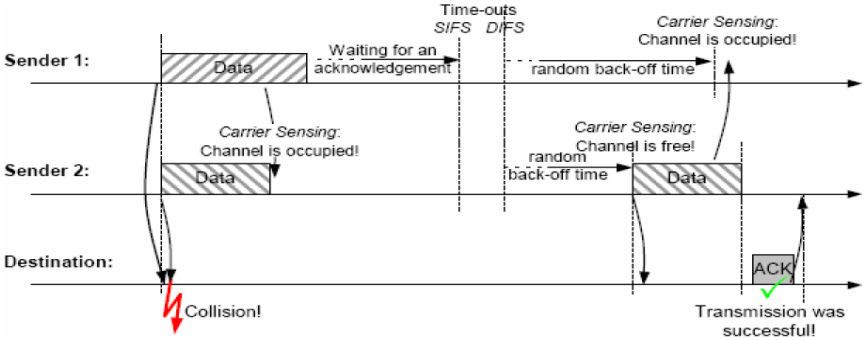


Figura 21[58]: Coordinación del medio mediante CSMA/CA.

3.2.3.1 Problema del Nodo Oculto

Un problema característico de las comunicaciones inalámbricas que no se presenta en las redes cableadas, es el del nodo oculto. Observemos por ejemplo la figura 22. La estación B esta tanto en el área de cobertura de A como de C. Sin embargo, ni la estación móvil A esta en el área de cobertura de C, ni C se encuentra en el área de cobertura de A. Si A desea transmitir un mensaje a B, enviara un tono piloto para notificar al resto de las estaciones móviles en la red de su intención, dado que C no esta en su área de cobertura, esta no escuda el tono piloto enviado por A y esta puede decidirse a transmitir un mensaje a B al mismo tiempo que A, produciéndose una colisión, haciendo fallar a CSMA/CA.

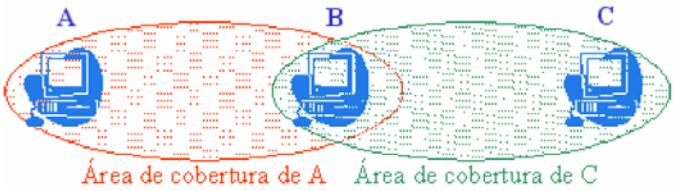


Figura 22: Problema del nodo oculto.

[58] Figura tomada de [11].

En resumen se tendrá un receptor que puede escuchar dos transmisores, pero estos no se pueden escuchar entre sí, entonces no se realizaría el mecanismo de tiempo de espera aleatorio, puesto que un transmisor nunca capta la portadora del otro, resultando en muchas colisiones. 802.11 MAC lo soluciona utilizando dos tramas de control:

- Request to Send (RTS) que uno de los posibles transmisores manda al receptor.

- Clear to Send (CTS) que el receptor responde afirmativamente al RTS dando permiso al transmisor para transmitir. En el proceso de RTS/CTS se observa en la figura 23, en el mismo podemos encontrar la señal de acuso de recibo ACK.

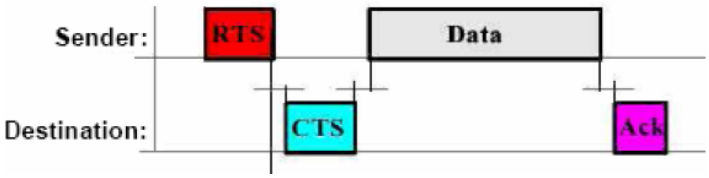


Figura 23[59]. Tramas de control RTS/CTS.

3.2.4 Trama MAC

La figura 24 muestra la estructura de una trama en la capa de control de acceso al medio. Una trama MAC esta compuesta de tres partes: la cabecera, el cuerpo

[59] Figura tomada de [11].

principal de datos y un CRC de 32 bits que permite detectar la presencia de errores en la trama.

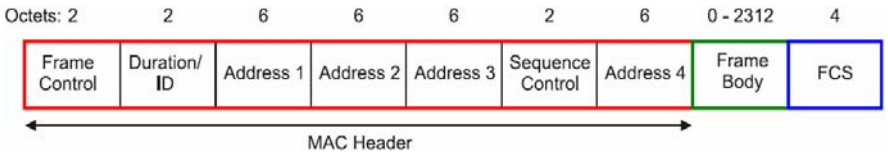


Figura 24[60]: Formato de la trama MAC.

3.2.4.1 La Cabecera

Es necesaria por razones de gestión de los datos que se envían.

3.2.4.1.1 Frame Control

La figura 25 muestra la estructura del primer campo de la cabecera, el Frame Control. Los sub-campos del frame control son los siguientes:

a) Protocol Version: Esta previsto para incorporar futuras versiones del protocolo MAC.

b) Type: Distingue tres clases de tramas diferentes: de control, de datos y de administración.

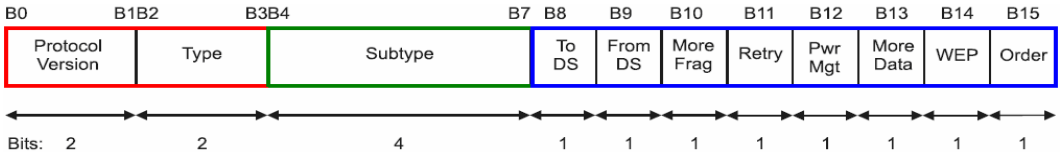


Figura 25[61]: Campo de control de trama.

[60] Figura tomada de [1].

c) Subtype: Identifica diferentes mensajes dentro de un mismo tipo. Type y Subtype combinados identifican el tipo de trama.

d) TO DS y FROM DS: Distingue si las tramas van hacia o vienen del Distribution System. La tabla 5 presenta el significado de estos bits.

To/From DS values	Meaning
To DS = 0 From DS = 0	A data frame direct from one STA to another STA within the same IBSS, as well as all management and control type frames.
To DS = 1 From DS = 0	Data frame destined for the DS.
To DS = 0 From DS = 1	Data frame exiting the DS.
To DS = 1 From DS = 1	Wireless distribution system (WDS) frame being distributed from one AP to another AP.

Tabla 5[62]: Combinaciones To/From DS en las tramas de datos.

e) More Fragments: Este bit es fijado en 1 si la trama es un fragmento más de una ráfaga de fragmentos correspondiente a una sola trama de una superior.

f) Retry: Este bit es fijado en 1 si la trama esta siendo retransmitida.

g) Power Management: Estaciones móviles necesitan guardar energía para no gastar la batería. Si el bit es fijado en 1, la estación transmisora esta indicando que pasara a un modo de conservación de batería inmediatamente después de transmitir.

[61] Figura tomada de [1].
[62] Tabla tomada de [1].

h) More Data: Los AP guardan un buffer las tramas con destino a las estaciones móviles que se encuentran en el modo de ahorro de batería. Un AP puede fijar este bit en 1 para avisar a una estación en ahorro de batería que hay al menos una trama más para transmitir.

i) WEP: Indica si la trama de datos ha sido encriptada.

j) Order: Si este bit es fijado en 1, la transmisión y la recepción de tramas debe realizarse en orden. Si este bit es 0, se permite la entrega de tramas fuera de orden.

3.2.4.1.2 Duration Field

El segundo campo en la cabecera es el Duration Field. Este campo tiene varias aplicaciones, de acuerdo al valor de los dos bits más significativos, esto se explica a continuación:

a) NAV: Si el bit mas significativo es 0 (Bit 15). Corresponde al número de microsegundos que el medio va a ser ocupado. Las estaciones no trasmiten mientras su temporizador NAV sea mayor que 0.

b) CFP[63]: Si el bit 14 es cero y el bit 15 es 1. Son periodos en los cuales las estaciones no compiten por el acceso al medio.

[63] CFP: Contention Free Period.

c) PS - Poll[64] Frames: Si el bit 14 y el bit 15 son fijados en 0. Cuando las estaciones salen del modo de conservación de energía, solicitan mediante una trama PS - Poll al punto de acceso que le envíen todas las tramas que hayan sido guardadas para ellas. En la tabla 6 se puede observa cada uno de estos casos.

Bit 15	Bit 14	Bits 13–0	Usage
0	0–32 767		Duration
1	0	0	Fixed value within frames transmitted during the CFP
1	0	1–16 383	Reserved
1	1	0	Reserved
1	1	1–2 007	AID in PS-Poll frames
1	1	2 008–16 383	Reserved

Tabla 6[65]: Codificación del campo de duración.

3.2.4.1.3 Campos de Address

El estándar 802.11 usa direcciones de 48 bits que son comunes a todo el grupo de estándares 802. Existen básicamente dos tipos de direcciones 802 MAC:

a) Individuales: Son utilizadas en Unicast, en estas direcciones el primer bit enviado al medio es cero.

b) Grupales: Pueden ser de dos tipos Multicast y Broadcast.

- Multicast: Dirigida a un grupo particular de estaciones móviles, en este caso el primer bit enviado al medio es 1.

[64] PS – Poll: Power - Save Poll.
[65] Tabla tomada de [1].

- Broadcast: Dirigida a todas las estaciones móviles, en este caso todos los bits son 1.

Existen diferentes tipos de direcciones en la arquitectura 802.11, entre las que se encuentran:

- Destination Address DA: La dirección MAC de la estación móvil que va a pasar la trama a una capa superior.
- Source Address SA: La dirección MAC de la estación móvil donde se origino la trama.
- Receiver Address RA: La dirección MAA de la estación que va a recibir la trama procesada.
- Transmiter Address TA: La dirección MAC de la estación que debe transmitir la trama hacia su destino.

Un ejemplo se puede observar en la figura 26. La estación A desea enviar un mensaje a la estación C que no se encuentra en una red Wi Fi. En este caso, A necesitara de los servicios del punto de acceso B que sirve como puente entre las dos redes. Entonces A envía el mensaje a B, en donde se coloca ella misma tanto como transmisora (TA) como generadora (SA). El mensaje va dirigido finalmente a

C, que figura como destino (DA), pero primero debe ser recibido por el punto de acceso B, que figura como receptor (RA).

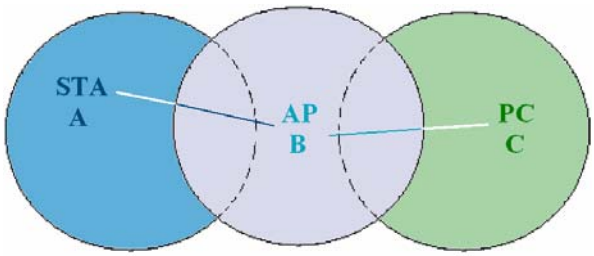


Figura 26: Esquema de direccionamiento MAC.

3.2.4.1.4 Sequence Control

La figura 27 muestra la estructura del campo de control de secuencia, el cual esta constituido por dos sub-campos:

a) Sequence Number: Es el número de secuencia de trama antes de fragmentar. Este se mantiene constante en todas las retransmisiones. Se cuenta desde 0.

b) Fragment Number: Es el número de fragmento y permite reconstruir el mensaje original en el destino.

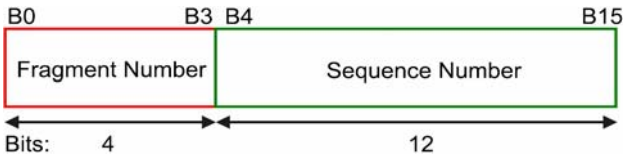


Figura 27[66]: Campo de control de secuencia.

[66] Figura tomada de [1].

3.2.5 Autenticación

Autenticación es el proceso por el cual una estación le demuestra a otra su identidad. Uno de los usos de la autenticación es la limitación del acceso a una red a estaciones no deseadas. La autenticación tiene mas sentido en redes de infraestructura, cuando el proceso de autenticación se realiza hacia los puntos de acceso, pues estos suelen estar bajo el control de administradores de red, que se encargaran de la función de seguridad.

Existen dos formas de autenticación en el estándar 802.11 original:

- Open System[67].
- Shared - Key System[68].

3.2.5.1 Open System

La estación móvil le envía una trama, consignando su propio MAC Address, al AP. El AP puede contestar con aceptación o elegir no contestar, de tal modo que solo las estaciones móviles permitidas tienen acceso a la red.

3.2.5.2 Shared - Key System

En este sistema todas las estaciones móviles autorizadas comparten una clave secreta. El proceso de autenticación se realiza de la siguiente manera.

[67] En Español: Sistema Abierto.
[68] En Español: Sistema de clave compartida.

- La STA[69] envía al AP un mensaje comunicándole su MAC address.
- El AP le contesta a la STA con un texto de 128 bytes generado al azar, conocido como texto de desafió.
- La STA debe responder al AP con el mismo texto pero esta vez encriptado utilizando la clave compartida.
- El AP verifica que el texto haya sido encriptado correctamente, si este es adecuado le envía una trama concediéndole acceso a la red.

Entre los problemas de este sistema se encuentra la necesidad de distribuir de manera segura la clave a todas las estaciones móviles autorizadas.

3.2.6 Asociación

Luego de autenticarse, una estación debe asociarse con la nueva red para poder comunicarse a través de la misma. La asociación permite ubicar la estación móvil en una BSS determinada y así poder rutear las tramas destinadas a ella a través del punto de acceso adecuado. Al asociarse, el AP le otorga a la estación móvil una Identificación de asociación única AID[70]. EL punto de acceso utiliza este identificador para señalar una cola de mensajes que reserva para guardar aquellas tramas que le llegan al AP con destino a esa estación móvil.

[69] STA: Estación.
[70] AID: Association ID.

Para poder entender la necesidad de asociación observemos la figura 28. En esta figura se presenta una estación móvil que se mueve de un BSS a otro dentro de la misma red, llamada ESS. Es posible que mientras se movía del BSS 1 al BSS2, hayan llegado mensajes para el AP1 que provienen, por ejemplo, desde fuera de la red inalámbrica. El AP1 guarda todos los mensajes en una cola asociada con la estación móvil e identificada a través de la AID. La única manera que la estación móvil no pierda estos mensajes es que el AP1 los envié al AP2 para que este a su vez se los transmite a la estación móvil.

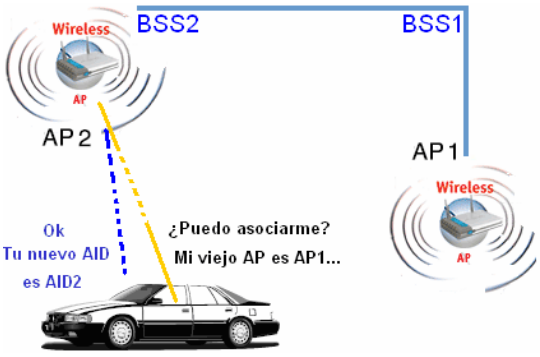


Figura 28: Proceso de asociación.

Para poder hacer esto, la estación móvil tiene que asociarse al BSS2, es decir, informarle al AP2 que viene de BSS1 y que estaba asociado con un numero dado de AID (llamémosle AID1) y pedirle autorización para asociarse. Si el AP2 acepta la asociación, le da un nuevo AID (llamémosle AID2) a la estación y le pide al AP1 que le envié cualquier mensaje que sea destinado a la estación móvil con AID1. Una vez recibimos los mensajes, el AP2 los ubica en la cola correspondiente al AID2 y continua con sus otras tareas. Este proceso se conoce como reasociación,

y se produce cuando la estación detecta mayor nivel de señal en otro AP de la red diferente al que está asociado, o cuando una estación se mueve del área de cobertura de un AP a otro.

3.2.7 Roaming

La movilidad es una de las características principales de las redes inalámbricas. Se define roaming como la capacidad de una estación móvil de desplazarse físicamente sin perder comunicación. Es gracias al proceso de reasociación que la estación pueda seguir formando parte de la red. Básicamente el proceso de roaming se produce por:

- La estación detecta otro AP que transmite a mayor velocidad.
- La potencia de transmisión de un AP excede considerablemente la actual.
- El rendimiento de su BSS cae considerablemente, aumentando la pérdida de datos.
- El AP cesa la transmisión.

Los protocolos de Roaming no están definidos en el estándar 802.11. Cada fabricante utiliza sus propios métodos.

4 SEGURIDAD EN REDES 802.11

El acceso sin necesidad de cables, la razón que hace tan populares a las redes inalámbricas, es a la vez el problema más grande de este tipo de redes en cuanto a seguridad se refiere. Es muy común encontrar redes en las que el acceso a Internet se protege adecuadamente con un firewall[71] bien configurado, pero al interior de la red existen puntos de acceso inalámbrico totalmente desprotegidos e irradiando señal hacia el exterior. Tal es el caso de la figura 29, donde una persona desde el exterior capta la señal del punto de acceso, empleando la red para tomar datos del número de tarjeta de crédito, enviar troyanos[72] y lanzar ataques a la Internet desde la propia red. Un punto de acceso inalámbrico mal configurado se convierte en una puerta trasera que vulnera por completo la seguridad informática de la compañía.

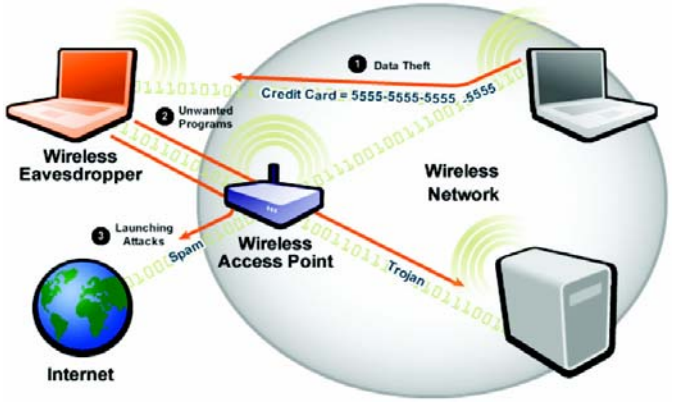


Figura 29[73]: Acceso no autorizado a una red inalámbrica.

[71] Sistema diseñado para prevenir el acceso no autorizado a intrusos desde el Internet.
[72] Virus informático o programa malicioso capaz de alojarse en computadoras y permitir el acceso a usuarios externos, con el fin de socavar la información.
[73] Figura tomada de www.mcafee.com.

Dentro del mundo Wireless, existen dos prácticas bien conocidas para localizar redes inalámbricas que se han extendido rápidamente entre algunas comunidades de usuarios de esta tecnología sobre todo con el ánimo de conseguir acceso gratuito a Internet, estas son el Warchalking y el WarDriving.

El warchalking, consiste en caminar por la calle con un computador portátil dotado de una tarjeta WLAN, buscando la señal de un PA. Cuando se encuentra uno, se pinta con tiza un símbolo especial en la acera o en un muro, indicando la presencia del PA y si tiene configurado algún tipo de seguridad.

En la figura 30 podemos observar el modo de información utilizado por el Warchalking.

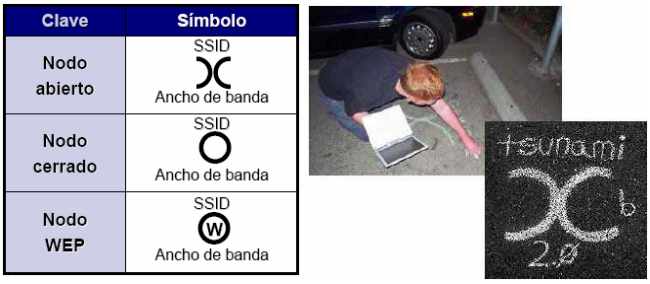


Figura 30. Warchalking y su simbología.

El WarDriving es un método usado para la detección de redes inalámbricas desde un automóvil, con un computador portátil. Para la identificación de las redes es necesario usar una TR Wi-Fi, una antena, un GPS para localizar los puntos de acceso en un mapa, y software para detección de redes inalámbricas.

Al haber observado lo vulnerables que pueden llegar a ser las redes inalámbricas, es conveniente presentar varios métodos para lograr la configuración segura; cada método logra un nivel[74] diferente de seguridad y presenta ciertas ventajas y desventajas.

4.1 Filtrado de Direcciones MAC

Este método consiste en la creación de una tabla de datos en cada uno de los puntos de acceso a la red inalámbrica. Dicha tabla contiene las direcciones MAC de las tarjetas de red inalámbricas que se pueden conectar al punto de acceso. Como toda tarjeta de red posee una dirección MAC única, se logra autenticar el equipo.

Este método tiene como ventaja su sencillez, por lo cual se puede usar para redes caseras o pequeñas. Sin embargo, posee muchas desventajas que lo hacen impráctico para uso en redes medianas o grandes, tomando como principal el que las direcciones MAC viajan sin cifrar por el aire.

4.2 Wired Equivalent Privacy.

Sistema de cifrado incluido en el estándar 802.11 como protocolo para redes Wireless que permite encriptar la información que se transmite. Proporciona encriptación a nivel 2. Este utiliza claves de 64bits, de 128bits o de 256 bits.

[74] Un sistema es seguro cuando tiene la protección adecuada al valor de la información que contiene o que puede llegar a contener, dependiendo de la información que manejemos debemos emplear distintos niveles de seguridad.

Es inseguro debido a su arquitectura, por lo que el aumentar los tamaños de las claves de encriptación sólo aumenta el tiempo necesario para romperlo. Entre los inconvenientes de WEP se encuentra que no ofrece servicio de autenticación. El cliente no puede autenticar a la red, ni al contrario; basta con que el equipo móvil y el punto de acceso compartan la clave WEP para que la comunicación pueda llevarse a cabo.

4.3 Las VPN

Una red privada virtual VPN[75] emplea tecnologías de cifrado para crear un canal virtual privado sobre una red de uso público. Las VPN resultan especialmente atractivas para proteger redes inalámbricas, debido a que funcionan sobre cualquier tipo de hardware inalámbrico y superan las limitaciones de WEP. Los servidores de VPN se encargan de autenticar y autorizar a los clientes inalámbricos, y de cifrar todo el tráfico desde y hacia dichos clientes. Un esquema de una VPN se puede observar en la figura 31.

Figura 31: Estructura de una VPN para acceso inalámbrico seguro.

[75] VPN: Virtual Private Network.

4.4 WI-FI Protected Access

WPA es un estándar propuesto por los miembros de la Wi-Fi Alliance en colaboración con la IEEE. Este estándar busca subsanar los problemas de WEP, mejorando el cifrado de los datos y ofreciendo un mecanismo de autenticación. Para solucionar el problema de cifrado de los datos, WPA propone un nuevo protocolo para cifrado, conocido como TKIP[76]. Este protocolo se encarga de cambiar la clave compartida entre punto de acceso y cliente cada cierto tiempo, para evitar ataques que permitan revelar la clave.

4.5 Estándar IEEE 802.11i

Abre paso a la posibilidad de que Wi Fi pueda ser ampliamente utilizado en entornos corporativos sin amenazar la seguridad de los sistemas. Entre los impulsores de la norma existe la expectativa de que este estándar haga pasar a segundo plano la importancia de tecnologías de redes privadas virtuales que se venían utilizando para brindar una adecuada seguridad a los enlaces inalámbricos en entornos sensibles. El estándar provee seguridad a nivel de la capa 2 de red. Varios de los conceptos de 802.11i ya estaban implementados en la norma conocida como WPA de tal modo que la Wi Fi Alliance certificará a los equipos que cumplan adecuadamente la norma 802.11i como WPA2 compatibles. Esto se debe a que WPA se baso en los borradores de 802.11i.

[76] TKIP: Temporary Key Integrity Protocol.

5 CASOS DE ESTUDIO

Dentro de la puesta en práctica de las redes inalámbricas se han incluido tres casos de estudio que pueden representar un alto número de los escenarios de uso de esta tecnología: Redes SOHO[77], Comunitarias, Hot – Spots y Servicio VIP, y Corporativas.

5.1 Redes SOHO

Este viene siendo y es hoy por hoy uno de los escenarios más comunes de esta tecnología. Hasta hace bien poco los usuarios caseros de computadores, bien por uso particular bien por uso profesional del computador y por ende de Internet, estaban atados a las zonas de la casa/local donde tenían las tomas telefónicas o bien los módems ADSL/DSL/CABLE. El mover los computadores a otra localización dentro de la casa / pequeño negocio era prácticamente imposible o muy costoso. Gracias a la tecnología inalámbrica actual, esto es posible solucionarlo de una manera muy fácil y nos va a permitir disponer de los computadores en la situación que queramos dentro del hogar.

Vamos a tomar como ejemplo una casa con tres computadores, dos de ellos de sobremesa y uno portátil. Esta configuración es una configuración estándar que representa bastante bien un amplio espectro de los hogares medios, en los cuales

[77] SOHO: Small Office- Home Office.

uno de los computadores se ha quedado tecnológicamente desfasado pero aún se quiere aprovechar, se ha comprado un segundo computador de sobremesa más potente y se tiene uno portátil bien por necesidades particulares o bien porque el trabajo de uno de los integrantes de la familia lo provee. Suponemos que disponemos bien de una conexión telefónica o bien un ADSL/DSL/CABLE para conectarnos a Internet.

La lista de elementos que vamos a necesitar para implantar la red es muy corta.

- 1 tarjeta PCI Wi-Fi 802.11b.
- 1 tarjeta USB Wi-Fi 802.11b.
- 1 tarjeta PCMCIA Wi-Fi 802.11b.
- 1 PA Router Wi-Fi 802.11b.

La configuración más normal será la de configurar el computador más tecnológicamente atrasado con la tarjeta Wi-Fi PCI, poniendo la USB Wi-Fi al computador más moderno y dejando la PCMCIA Wi-Fi para el computador portátil.

Lo preferible sería ponerle a los dos computadores de sobremesa TR USB Wi-Fi, pero si no disponemos de puerto USB o no tenemos ninguno libre en el computador antiguo habrá que ponerle tarjeta PCI Wi-Fi. En el caso de conectar tarjetas USB Wi-Fi, debemos tener en cuenta que el USB 1.1 sólo permite

transferir datos a una velocidad máxima de 12 Mbps por lo que si le conectamos una tarjeta USB Wi-Fi 802.11g con una velocidad máxima de 54 Mbps no conseguiremos aumentar la velocidad. Para conectar este tipo de tarjetas es necesario disponer de conectores USB 2.0.

El PA Router será el encargado de conectarnos a Internet. Hay algunas unidades que llevan un MODEM 56K V90 integrado por lo que no es necesario comprar un MODEM adicional. En cualquier caso usar un MODEM para conectarse a Internet debería de ser la última de nuestras opciones, pues es muy recomendable el contratar las ya baratas soluciones ADSL / DSL / CABLE de cualquier proveedor que nos la ofrezca. Es caso del ADSL, por ejemplo y del DSL y CABLE por extensión, los routers disponen de una entrada WAN a la cual enchufar el MODEM sea del tipo que sea. Para este caso, supongamos una salida a Internet mediante ADSL 256 Kbps.

El PA Router distribuirá la señal entre los tres computadores, que ahora podremos poner en cualquier sitio. La configuración normal será que el joven de la casa disponga del más potente para jugar en su habitación, y los padres del tecnológicamente desfasado pero seguro para almacenar su documentación y navegar por Internet en su despacho y el computador portátil se reservaría para hacer en casa cosas del trabajo y poco más. El esquema de esta red se puede observar en la figura 32.

Dado que tenemos tres adaptadores recibiendo información desde Internet, y dada la conexión ADSL con 256 Kbps de bajada, en el peor momento punta tendremos 256 Kbps/3 = 85.32 Kbps para cada uno, el cual parece un ancho de banda razonable, es más, dadas las características de los tres aparatos es altamente improbable que los tres estén conectados al mismo tiempo, y en ese caso de los tres conectados, es poco probable que estén los tres recibiendo información al máximo de su velocidad al mismo tiempo.

Figura 32: Esquema de conexión de tres computadores en el hogar.

Para realizar este tipo de red es deseable usar un tipo de conexión 802.11b que nos va a permitir conectarnos a Internet sin ningún problema además de transferir archivos entre las máquinas y compartir recursos sin ningún problema de velocidad.

5.2 Redes Comunitarias

Este escenario en el que nos vamos a mover difiere en ciertos aspectos del que acabamos de describir. Contrariamente a lo que se puede pensar en un primer momento no nos encontramos ante un sobredimensionamiento del caso anterior.

Para describir este escenario vamos a suponer que una comunidad de propietarios de un edificio, desea conectarse a Internet, a la vez que quiere disponer de una página Web que muestre información a los vecinos sobre reuniones, pagos de comunidad, etc. Partamos de un edificio que dispone de 15 vecinos. Todos se han puesto de acuerdo y quieren alquilar a un proveedor de Internet por cable un acceso de 10 Mbps, el cual es demasiado caro para una sola persona pero perfectamente asumible pagándolo entre toda la comunidad. Un esquema de esta red se puede apreciar en la figura 33.

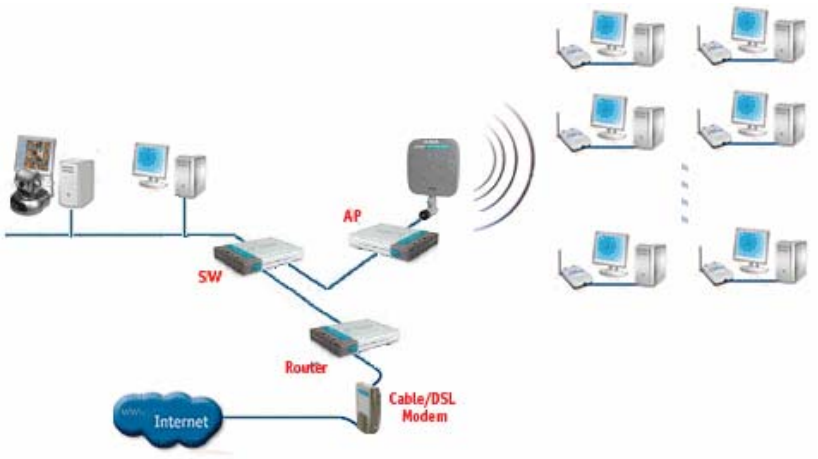


Figura 33: Esquema de conexión de un grupo computadores de una comunidad de vecinos.

Cada vecino va a disponer de un computador en su casa (máximo dos) desde los cuales se les dará servicio de conexión a Internet. Esto hace un total de en el peor de los casos 30 computadores conectados simultáneamente a Internet. Para empezar vamos a describir la infraestructura necesaria:

- Vamos a necesitar bien de un Router estándar con un punto de acceso o bien de un PA Router. En cualquier caso debería poder disponer de una toma a la que conectar una antena adicional o bien que la antena del mismo sea desmontable. El protocolo seleccionado para el PA será el 802.11g. Sea cual sea la elección, conectaremos al Router un computador que será el encargado de realizar la gestión de todo el sistema. No es necesario que sea muy potente, pero si al menos lo suficiente como para poder instalar el Servidor Web + Correo electrónico, gestión de las comunicaciones y poco más.

- Si fuese necesario, necesitaríamos una antena con un cable que sea capaz de ubicar a la misma en el centro del edificio o en la parte más alta del mismo. Debemos tener en cuenta que cuanto más largo sea el cable de conexión a la antena mas atenuación de la señal emitida / recibida tendremos.

- Cada vecino ya dispone al menos de un computador, al cual conectará una TR 802.11g. No es conveniente hoy por hoy el mezclar tarjetas

802.11b con PA 802.11g pues provoca que éstos bajen su rendimiento de forma apreciable.

Haciendo cuentas tenemos:

- 10 Mbps/30 computadores = 350 Kbps velocidad que es bastante buena para una conexión a Internet en el peor de los casos.

- 10 Mbps/15 computadores = 700 Kbps velocidad que es muy buena para una conexión a Internet en el mejor de los casos.

En el tramo que hay entre el TR y el PA, nuestro PA va a ser capaz de repartir sus 54 Mbps entre los 30 computadores de los vecinos, lo cual hace un total de 1.8 Mbps disponibles en el peor caso para cada computador. Dado que en el peor de los casos cada computador dispone sólo de 350 Kbps para acceder a Internet, 1.8 Mbps son más que suficientes. De hecho, esta infraestructura nos permitiría teóricamente aumentar el ancho de banda de nuestra conexión por cable a Internet hasta llegar a los 54 Mbps.

Desde el punto de vista de los usuarios y manteniendo un mínimo de 128 Kbps de velocidad de acceso a Internet para cada uno, y dada la conexión de 10 Mbps, teóricamente podríamos dar servicio a alrededor de 80 computadores/usuarios simultáneos como máximo, pero en el tramo de comunicación entre el TR y el PA, la velocidad sería de 691 Kbps con 80 usuarios. Dado que esta velocidad no está

soportada, tendríamos que subir hasta 1 Mbps lo que nos llevaría a su vez a dar servicio a 56 usuarios simultáneos como máximo.

Cada vecino puede conectarse a Internet a una velocidad razonable, pero esto sólo es teoría pues dado que el estándar 802.11g de momento no dispone QoS, por lo que no podemos asegurar que un solo vecino no se "coma" todo el ancho de banda, dejando al resto "parado". Para resolver este problema vamos a tener que recurrir a un sistema de gestión de comunicaciones y más concretamente del ancho de banda.

Respecto a la seguridad, es la misma que siempre, prestando especial atención al tema de que cada vecino sólo debe tener dos máquinas dadas de alta en la lista de direcciones MAC del PA.

5.3 Redes Hot – Spots y Servicios VIP

Hot-spots corresponde con la creación de redes de comunicaciones electrónicas inalámbricas para la prestación de servicios, fundamentalmente acceso a Internet, en ubicaciones específicas donde se concentra un gran número de potenciales clientes, en lugares de tránsito o vía pública. Las redes hot – spots tienen una infraestructura similar a la comunitaria, estas varían en que mientras una busca obtener un bien o servicio, la otra se interesa en obtener rentabilidad a partir de un negocio. En este modelo de negocio se cobra directamente al cliente por la

prestación del servicio. Este modelo se ha convertido en el uso de la tecnología Wi-Fi más popular. Típicamente este tipo de puntos de servicio se localizan en aeropuertos, estaciones de tren, centros comerciales, hoteles, metro, centros de convenciones, cafés o restaurantes. Los *hot-spots* se dirigieron inicialmente al uso por parte de viajeros de negocios, aunque cada vez más se está extendiendo su uso a la población en general. Los terminales a través de los cuales el usuario se conecta a la WLAN son el ordenador portátil, PDA o teléfono móvil. En los *hot-spots* se ofrece servicio de acceso a Internet, para actividades del tipo mensajería, navegación *Web* o juegos en red.

Las redes de servicio VIP constituye una variante del modelo hot - spots donde asociado a un entorno delimitado y de gran tránsito, un agente presta esta funcionalidad de forma “gratuita” o al menos por la que no se paga directamente. Nos encontramos ante un servicio de valor añadido a través del cual un agente no prestador de servicios de telecomunicaciones, como serían los aeropuertos, estaciones de tren, hoteles o centros de convenciones ofrece de forma adicional al servicio contratado la posibilidad de disponer de acceso a Internet de alta velocidad en salas de espera VIP, vagones de primera clase o de negocios, cafés o restaurantes selectos. El retorno de la inversión se espera conseguir a través de la diferenciación que ofrece esta nueva capacidad y no por una remuneración directa por el servicio. Asimismo, la entidad que pone a disposición de sus clientes

este servicio puede utilizarlo para transmitir información en relación a su negocio o servicios publicitarios.

5.4 Redes Corporativas

Este tercer caso vamos a enfocarlo desde un punto de vista diferente.

El primer caso estudiado estaba enfocado al intercambio de archivos y a compartir recursos entre un conjunto muy limitado de computadores/usuarios con un acceso a Internet restringido entre 56 y 256 Kbps.

En el segundo nos basamos casi exclusivamente en el acceso a Internet y la gestión del ancho de banda del mismo, teniendo muy pocos recursos o ninguno compartidos entre los participantes de la red.

Este tercer caso vamos a enfocarlo como un escenario en el que vamos a compartir recursos, impresoras, servidores, espacios de almacenamiento y acceso a Internet. Este acceso no va a ser para todos los computadores y aunque el ancho de banda va a ser mayor que en el primer caso no va a llegar a ser tan grande como en el segundo.

Tendremos una infraestructura de sistemas internos muy grande, a la cual se dirigirá la mayoría de las comunicaciones. El acceso a Internet no será muy amplio, basándose sobre todo en el uso del correo electrónico.

Vamos a suponer una empresa en la que disponemos de por ejemplo 50 computadores repartidos por diferentes plantas y con un área física a cubrir mayor que en los casos anteriores. La seguridad dentro de las comunicaciones será un aspecto crítico. Se aconseja el uso de VPNs.

Dispondremos de una infraestructura básica de comunicaciones "tradicional" mediante el uso de una red Ethernet 100, a la que conectaremos PA Routers 802.11g.

Hay que tener en cuenta que tratándose de una empresa, podríamos llegar a tener puntos con una gran demanda de ancho de banda y otros con muy poca. Corresponde investigar cuáles pueden ser los puntos donde haya más concentración de máquinas, como pueden ser las zonas de reuniones, zonas de gran concentración de trabajadores, etc.

Desde el punto de vista de la seguridad, las antenas deben ser colocarlas en lugares "centrales" del edificio, donde el radio de alcance de la señal no exceda demasiado del edificio físico en el que se encuentre. En cualquier caso, siempre o casi siempre tendremos cobertura inalámbrica fuera de nuestro edificio. Por ello hay que seguir las normas de seguridad escrupulosamente.

Otro uso bastante práctico puede ser el unir dos redes empresariales lejanas entre si. Para ello se puede disponer de dos antenas direccionales especialmente

preparadas para tal evento y dos puntos de acceso normales, como se percibe en la figura 34.

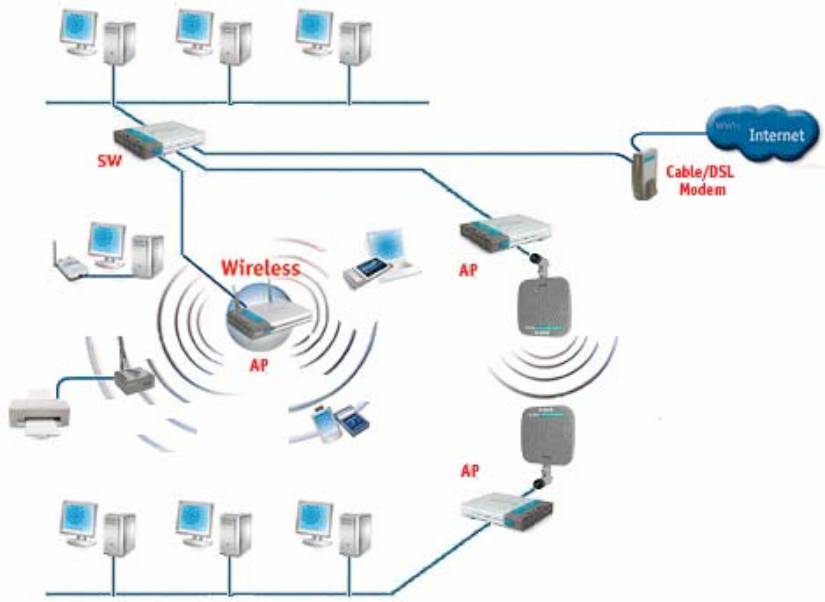


Figura 34: Esquema de conexión de una red de tipo empresarial.

Se configuran los puntos de acceso para que sólo sea posible la comunicación entre ellos y se enfocan las antenas entre si.

Para que esta comunicación sea posible es necesario que el PA Wi-Fi cumpla el estándar 802.11c, que define las características que necesitan los APs para actuar como puentes[78] (bridges).

[78] Interconectan segmentos de red, haciendo el cambio de tramas entre las redes de acuerdo con una tabla de direcciones que dice en que segmento está ubicada una dirección MAC

6 DISPOSITIVOS WI FI

Sea cual sea el estándar que elijamos vamos a disponer principalmente de dos tipos de dispositivos: Las tarjetas de red TR y los puntos de acceso PA.

6.1 Dispositivos Tarjetas de red

Serán los que tengamos integrados en nuestro computador, o bien conectados mediante un conector PCMCIA[79] ó USB[80] si estamos en un portátil o en una abertura PCI[81] si estamos en un computador de escritorio. Reciben y envían la información hacia su destino desde el computador en el que se este trabajando. La velocidad de transmisión / recepción es variable dependiendo del fabricante y de los estándares que cumpla. En la figura 35 se puede apreciar una TR PCMCIA.

Figura 35: Tarjeta PCMCIA Wi – Fi.

[79] PCMCIA: Personal Computer Memory Card International Association.
[80] USB: Universal Serial Bus.
[81] PCI: Interconexión de Componente Periférico.

6.2 Dispositivos Puntos de Acceso

Son los encargados de recibir la información de los diferentes TR que tenga la red, bien sea para su centralización o para su enrutamiento. Complementan a los Hubs, Switches o Routers[82]. En la figura 36 se observa el grafico de un PA.

Figura 36: Punto de acceso Wi – Fi.

La velocidad de transmisión / recepción es variable, las diferentes velocidades que alcanzan varían según el fabricante y los estándares que cumpla.

6.3 Velocidad Vs. Distancia

Todos los estándares aseguran su funcionamiento mediante el manejo de dos factores, la velocidad y la distancia. Cuando estamos conectados a una red mediante un cable, sea del tipo que sea, disponemos de una velocidad fija y constante. Sin embargo cuando estamos hablando de redes inalámbricas aparece un factor añadido que puede afectar a la velocidad de transmisión, que es la distancia entre los interlocutores.

[82] El PA puede sustituir a los últimos, pues muchos de ellos ya incorporan su funcionalidad.

Así pues cuando un TR se conecta a un PA se ve afectado principalmente por los siguientes parámetros: velocidad máxima del PA, distancia al PA (a mayor distancia menor velocidad) y los elementos intermedios entre el TR y el PA (las paredes, campos magnéticos o eléctricos u otros elementos interpuestos entre el PA y el TR modifican la velocidad de transmisión).

Normalmente los fabricantes de PAs presentan un alcance teórico de los mismos, algo que sólo es alcanzable en condiciones de laboratorio, pues en condiciones reales el rango de alcance de una conexión varía[83]. Cuando ponemos un TR cerca de un PA disponemos de la velocidad máxima teórica del PA, y conforme nos vamos alejando del PA, tanto él mismo como la TR van disminuyendo la velocidad de la transmisión/recepción para acomodarse a las condiciones puntuales del momento y la distancia. Cuando la distancia del punto de acceso aumenta, productos basados en IEEE 802.11 proporcionan una tasa de transferencia de datos reducida para mantener la conectividad.

La norma IEEE 802.11g tiene las mismas características de propagación de la 802.11b, porque transmite en la misma banda de frecuencia de 2.4 GHz. Como los productos 802.11b y 802.11g comparten las mismas características de propagación, las aplicaciones proporcionan el mismo rango máximo a la misma proporción de rata de datos. Como las señales de radio a 5 GHz no se propagan

[83] El alcance de los PA varía siempre hacia menos debido a la infinidad de condiciones que los afectan.

también como las señales de 2.4 GHz, el estándar 802.11a está limitado en comparación con el rango de 802.11b y 802.11g.

La figura 37 ilustra la rata de datos esperada para cada tecnología a diferentes distancias.

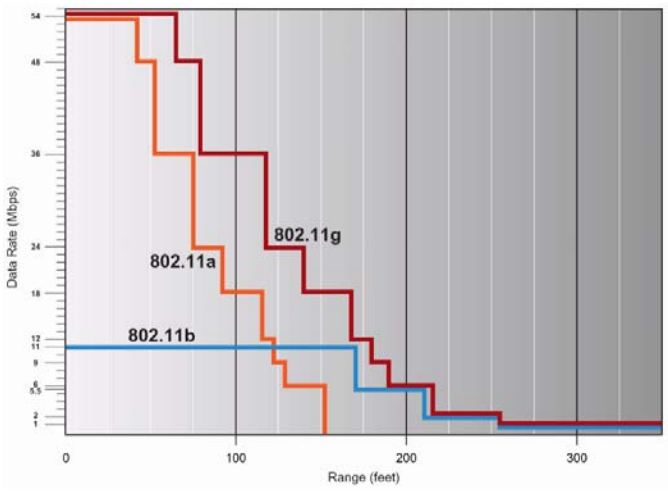


Figura 37: Velocidad esperada de los estándares 802.11a, 802.11b, y 802.11g al variar la distancia del punto de acceso[84].

Actualmente hay fabricantes que ofrecen antenas que aumentan la capacidad de TX/RX[85] de los dispositivos Inalámbricos.

6.4 Antenas

Dentro de los PA se puede modificar enormemente la capacidad de TX/RX gracias al uso de antenas especiales. Estas antenas se pueden dividir en tres grupos: direccionales, omnidireccionales y sectoriales.

[84] Figura tomada de [5].
[85] TX/RX: Transmisión y Recepción.

Las dimensiones de una antena son inversamente proporcionales a su frecuencia de operación, en otras palabras a frecuencias más altas, mas pequeñas son las dimensiones físicas de una antena.

Una buena antena con las características apropiadas es un elemento crítico para el alto rendimiento de una red inalámbrica en las distintas configuraciones que se puedan presentar. Una antena es un componente esencial, dado que provee ganancia y direccionalidad adicional a la señal Wi-Fi. La ganancia es una medida del aumento de potencia que puede alcanzar un punto objetivo, mientras que la direccionalidad es la modalidad y precisión con que la señal puede llegar al punto objetivo. La energía irradiada puede llegar al punto objetivo cubriendo toda un área a sus alrededores o solamente el objetivo con más o menos precisión. Una buena analogía de una antena es el reflector de una linterna. La función del reflector es el de concentrar e intensificar el rayo de luz en una dirección particular, de modo similar que la parábola reflectora de una antena concentra y localiza la señal de radiofrecuencia.

6.4.1 Antenas Direccionales

Orientan la señal en una dirección muy determinada con un haz estrecho pero de largo alcance. Una antena direccional actúa de forma parecida a un foco que emite un haz de luz concreto y estrecho pero de forma intensa (más alcance).

Las antenas Direccionales "envían" la información a una cierta zona de cobertura, a un ángulo determinado, por lo cual su alcance es mayor, sin embargo fuera de la zona de cobertura no se "escucha" nada, no se puede establecer comunicación entre los interlocutores.

El alcance de una antena direccional viene determinado por una combinación de los dBi de ganancia de la antena, la potencia de emisión del punto de acceso emisor y la sensibilidad de recepción del punto de acceso receptor.

Las antenas direccionales vienen en muchas formas y estilos. Una antena es muy diferente de los otros componentes que forman parte de un sistema Wi-Fi, como lo es un amplificador, dado a que es un componente pasivo y no agrega ninguna potencia adicional a la señal recibida. Una antena direccional logra un aumento de ganancia concentrando o redirigiendo la energía recibida del transmisor de una dirección a otra.

El proceso de redistribuir la energía recibida, tiene el efecto de proveer mas energía en una dirección privilegiada y menos en todas las direcciones restantes, una antena direccional y el modo en que radia se puede apreciar en la figura 38. De este modo la ganancia de una antena direccional aumenta a medida que el ángulo de radiación o de cobertura disminuye, pero al mismo tiempo permite que la señal radiada cubra distancias más grandes pero en áreas precisas.

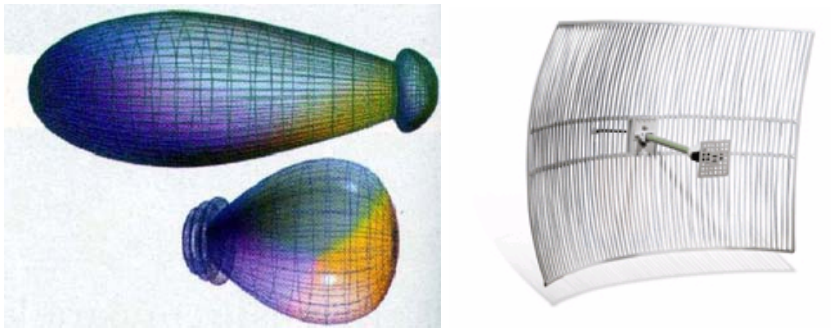


Figura 38: Gráfico de una antena direccional y de su patrón de radiación[86].

Las antenas direccionales incluyes antenas de tipo Yagi, paneles y parabólicas. Las antenas parabólicas son las mas precisas para focalizar la energía de la señal de radiofrecuencia en un ángulo muy pequeño y por consiguiente se instalan en pares donde las dos parábolas están enfrentadas una a la otra de modo altamente preciso, caso contrario una pequeña desviación podría resultar en la perdida de energía y hacer que el enlace sea completamente inoperante. La capacidad de poder dirigir su señal en una dirección vuelve a las antenas direccionales ideales para transmitir hacia sectores reducidos como: Clientes de un PA o para la interconexión LAN – LAN, es decir, para unir dos puntos a largas distancias.

6.4.2 Antenas Omnidireccionales

Orientan la señal en todas direcciones con un haz amplio pero de corto alcance. Si una antena direccional sería como un foco, una antena omnidireccional sería como una bombilla emitiendo luz en todas direcciones pero con una intensidad menor que la de un foco, es decir, con menor alcance. Las antenas

[86] Figura tomada de [6].

Omnidireccionales "envían" la información teóricamente a los 360 grados por lo que es posible establecer comunicación independientemente del punto en el que se esté. En contrapartida el alcance de estas antenas es menor que el de las antenas direccionales. Una antena omnidireccional y el modo en que radia se puede apreciar en la figura 39. El alcance de una antena omnidireccional viene determinado por la potencia de emisión del punto de acceso emisor y la sensibilidad de recepción del punto de acceso receptor.

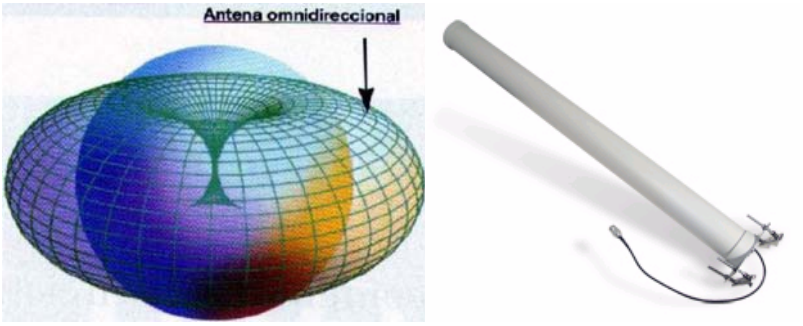


Figura 39: Grafico de una antena omnidireccional y de su patrón de radiación [87].

Las antenas de tipo omnidireccional son perfectas para APs, es decir, para dar señal extensa en los alrededores

6.4.3 Antenas Sectoriales

Son la mezcla de las antenas direccionales y las omnidireccionales. Las antenas sectoriales emiten un haz más amplio que una direccional pero no tan amplio como una omnidireccional. La intensidad (alcance) de la antena sectorial es mayor

[87] Figura tomada de [6].

que la omnidireccional pero algo menor que la direccional. Siguiendo con el ejemplo de la luz, una antena sectorial sería como un foco de gran apertura, es decir, con un haz de luz más ancho de lo normal. Las antenas tipo panel plano ofrecen menos direccionamiento cubriendo ángulos en el rango de 180° a 5° grados ya sea en la dirección vertical como horizontal.

Para tener una cobertura de 360º (como una antena omnidireccional) y un largo alcance (como una antena direccional) deberemos instalar o tres antenas sectoriales de 120º ó 4 antenas sectoriales de 80º. Las antenas sectoriales se suelen utilizan cuando se necesita un balance de las dos cosas, es decir, llegar a largas distancias y a la vez, a un área extensa. Las antenas sectoriales suelen ser más costosas que las antenas direccionales u omnidireccionales. Una antena sectorial y una comparación entre el patrón de radiación de las antenas direccionales, omnidireccionales y sectoriales se puede apreciar en la figura 40.

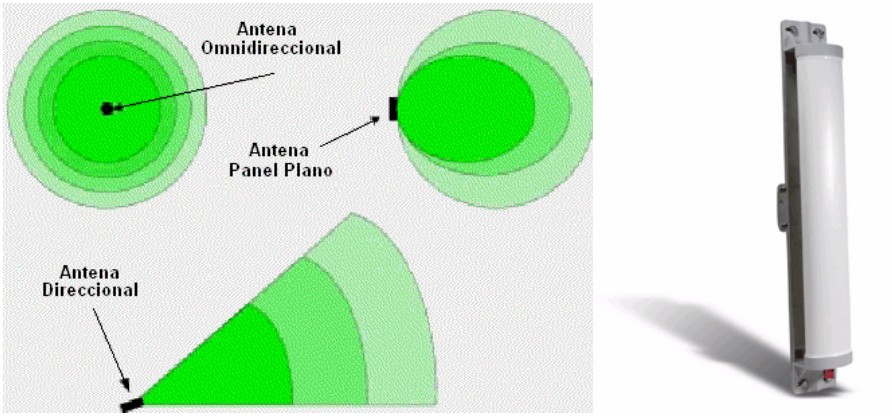


Figura 40: Antena Sectorial y Patrón de radiación de las antenas direccionales, omnidireccionales y sectoriales.

6.4.4 Apertura Vertical y Apertura Horizontal

La apertura es cuanto se "abre" el haz de la antena. El haz emitido o recibido por una antena tiene una abertura determinada verticalmente y otra horizontalmente. En lo que respecta a la apertura horizontal, una antena omnidireccional trabajará horizontalmente en todas direcciones, es decir, su apertura será de 360º. Una antena direccional oscilará entre los 4º y los 40º y una antena sectorial oscilará entre los 90º y los 180º.La apertura vertical debe ser tenida en cuenta si existe mucho desnivel entre los puntos a unir inalámbricamente. Si el desnivel es importante, la antena deberá tener mucha apertura vertical. Por lo general las antenas, a más ganancia menos apertura vertical. En las antenas direccionales, por lo general, suelen tener las mismas aperturas verticales y horizontales.

6.5 Consejos Prácticos

Una red de área local inalámbrica tiene los siguientes requerimientos básicos: cobertura completa en el área determinada y capacidad suficiente para soportar el tráfico. Estos requerimientos se cumplen a través de la ubicación adecuada de los AP y la asignación adecuada de canales.

Tanto los AP como las estaciones transmiten en diferentes frecuencias llamadas canales. El estándar define 14 canales: Europa 13 y EEUU 11 por regulaciones.

Las interferencias pueden ser:

- Co-canales: al transmitir simultáneamente sobre el mismo canal.

- Inter-canales: al transmitir sobre canales adyacentes

Tanto la interferencia de co-canales como inter-canales pueden limitar con severidad la capacidad de la WLAN. Por eso es conveniente espaciar lo máximo posible los AP, asegurando cobertura completa del área, o hacer un uso alternado de los canales como se observa en la figura 41.

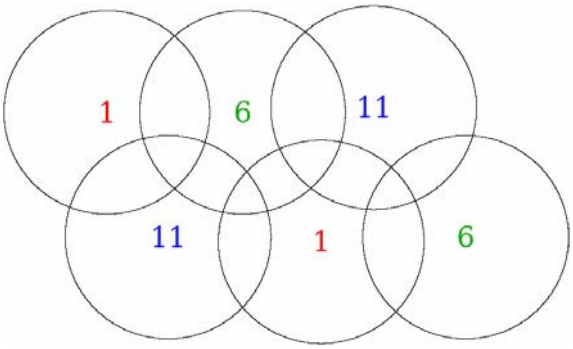


Figura 41: Asignación de canales sin interferencias.

Para el diseño deben de considerarse las áreas de servicio con distintas densidades de usuarios. En general las densidades son bajas, si es alta se pueden utilizar varios AP con distintos canales para cubrir la misma área.

Para la buena implementación de una red Wi – Fi se recomienda el siguiente procedimiento de diseño:

- Obtener planos del lugar y planos de la red Ethernet. Recorrer el lugar.

- Establecer densidades máximas de usuarios.
- Ubicar inicialmente los AP.
- Ajustar las ubicaciones de los AP basados en mediciones de intensidad de señal.
- Construir un mapa de cobertura.
- Asignar canales de frecuencia a los AP basado en el mapa de cobertura.
- Análisis y mediciones del rendimiento.
- Evitar mezclas de AP, pues esta complica la estimación de celdas y la actualización del software.
- Si se desea mayor cobertura en vez de utilizar un AP con amplificador de potencia es mejor distribuir y utilizar varios con baja potencia.
- Por seguridad tratar de ocultar las antenas externas. De lo posible tratar que el área de cobertura de las antenas sea de lo posible igual al área física por cubrir.

CONCLUSIONES

Wi-Fi puede jugar un papel importante como tecnología de transición que permita llevar acceso de banda ancha a zonas geográficas rurales que quedan fuera de la cobertura de las tecnologías de acceso de banda ancha más extendidas. En estas zonas, los operadores no encuentran viabilidad económica para realizar el despliegue de tecnologías de acceso de banda ancha (ADSL, cable,…).

Por sus características y nivel de desarrollo, las soluciones basadas en el estándar 802.11b son las que actualmente poseen una mayor utilización, y se prevé hacia el futuro un aumento en el uso de soluciones basadas en 802.11g, principalmente por efectos de compatibilidad.

Aunque la norma 802.11i promete impulsar el desarrollo de productos inalámbricos y promover las instalaciones WLAN, la seguridad de las redes WLAN en la empresa debe regirse por políticas de seguridad actualizadas que satisfagan las demandas exclusivas del lugar de trabajo móvil.

La familia de estándares 802.11 desarrollados para redes de área local se ve complementada con análogos desarrollos para entornos más amplios, esto es, tecnología inalámbrica también para redes de área metropolitana o MAN. En esta línea merece la pena destacar el recientemente respaldado por la industria 802.16 WMAN, especificación aprobada por el IEEE, que funcionando entre las bandas

de 2 y 11 GHz, proporcionará una capacidad de hasta 70 Mbps para la transmisión de voz, datos y vídeo en un rango de casi 50 Km. Se trata de una solución inalámbrica para la red de acceso que opera tanto en bandas reguladas, como libres. En la estandarización debe considerarse la importancia de converger hacia un estándar único que de ser posible cubriera el ámbito de las WLAN y WMAN.

Idealmente todas las empresas deberían seguir los estándares del IEEE para de esa forma asegurar la interoperabilidad de los dispositivos vendidos con los dispositivos de otros fabricantes. Lo mejor es comprar dispositivos estandarizados por el IEEE, pues es la única forma que tenemos de que los dispositivos que compramos hoy funcionen mañana.

BIBLIOGRAFIA

[1] ANSI/IEEE Std 802.11, 1999 Edition (R2003). Information technology Telecommunications and information exchange between systems— Local and metropolitan area networks— Specific requirements— Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[2] ANSI/IEEE Std 802.11b, 1999 Edition (R2003). Supplement to IEEE Standard for Information technology— Telecommunications and information exchange between systems— Local and metropolitan area networks— Specific requirements— Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Higher-Speed Physical Layer Extension in the 2.4 GHz Band.

[3] ANSI/IEEE Std 802.11a, 1999 Edition. Supplement to IEEE Standard for Information technology— Telecommunications and information exchange between systems— Local and metropolitan area networks— Specific requirements— Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Higher-Speed Physical Layer in the 5 GHz Band.

[4] Principales estándares Inalámbricos. Jalercom S.A. de C.V.

[5] WHITE PAPER IEEE 802.11g. The New Mainstream Wireless LAN Standard. Broadcom Corporation. 2003.

[6] GARAIZAR, Sagarminaga Pablo. Seguridad En Redes Inalámbricas 802.11 a/b/g. Protección y vulnerabilidades.

[7] CARNEY, William. IEEE 802.11g. New Draft Standard Clarifies Future of Wireless LAN. Wireless Networking Business Unit, Texas Instruments Incorporated. 2002.

[8] SMITH, Raymond J. WiFi Home Networking. McGraw-Hill. 2003.

[9] FIERENS, Pablo. Control de Acceso al Medio en 802.11: Introducción. Instituto Tecnológico de Buenos Aires.

[10] Authentication and Privacy. ANSI / IEEE Standard 802.11, 1999 Edition. http://standards.ieee.org/getieee802/download/802.11-1999. PDF, 59-68 pp.

[11] VALCÁRCEL, Sergio. Wireless LANs. Rohde&Schwarz. Abril de 2005.

[12] MARTINEZ, Javier Enrique. Wi Fi como solución de campo de acceso LAN, para prestar servicio de Internet y aplicaciones, dentro de la Universidad Tecnológica de Bolívar. Universidad Tecnológica de Bolívar. 2004.

[13] MADRID, Juan. Seguridad en redes inalámbricas 802.11. Universidad Icesi.

[14] CARBALLAR, José Antonio. Wi Fi, como construir una red inalámbrica. Alfaomega grupo Editor, S.A. de C.V. 2004.

Sitios Web

- www.icamericas.net. Configuraciones y usos de la tecnología Wi – Fi.
- www.observatorio.red.es. WI-FI, análisis, diagnóstico y políticas públicas.
- www.tecnun.es. Conexión a la red Wi – Fi.
- www.monografias.com. WLAN y Bluetooth
- www.leytelecomunicaciones.gov.co. Proyecto Normativo de Telecomunicaciones.
- www.crt.gov.co. Promoción y masificación de la Banda Ancha en Colombia.
- www.jalercom.com. Principales estándares Inalámbricos
- www.icesi.edu.co. Seguridad en redes inalámbricas 802.11.
- www.mailxmail.com. Redes inalámbricas. Wi-fi, el futuro de la comunicación.
- http://standards.ieee.org/getieee802/. The IEEE standards Catalog and Store.

GLOSARIO

- **Wi Fi:** Wireless Fidelity.
- **IEEE:** Institute of Electrical and Electronics Engineers.
- **WLAN:** Wireless Local Area Networks.
- **WMAN:** Wireless Metropolitan Area Networks.
- **LAN:** Local Area Networks.
- **IBM:** International Business Machines Corporation.
- **FCC:** Federal Communications Comisión.
- **ISM:** Industrial, Scientific and Medical.
- **MAC:** Medium Access Mechanism.
- **CSMA/CA:** Carrier Sense Multiple Access with Collision Avoidance.
- **PDAs:** Agendas electrónicas personales.
- **CDMA:** Code Division Multiple Access, estándar de telefonía móvil Estadounidense.
- **GSM:** Group Special Mobile, Sistema Global para Comunicaciones Móviles, estándar de telefonía móvil Europeo.
- **802.16:** Estándar conocido en el mundo de las comunicaciones como Wi – Max.
- **QoS:** Posibilidades de aseguro de Calidad de Servicio.
- **WN:** Wireless Networks.
- **TPC:** Transmit Power Control.

- **TKIP:** Temporal Key Integrity Protocol.
- **AES:** Advanced Encryption Standard.
- **PCMCIA:** Personal Computer Memory Card International Association.
- **USB:** Universal Serial Bus.
- **PCI:** Interconexión de Componente Periférico.
- **TX/RX:** Transmisión y Recepción.
- **PLCP:** Physical Layer Convergence Procedure.
- **Checksum (SUMMATION CHECK).** Suma de chequeo: Esquema simple de detección de errores, donde cada mensaje transmitido es acompañado con un valor numérico basado en el número de grupo de bits del mensaje.
- **DBPSK:** Differential Binary Phase Keying.
- **DQPSK:** Differential Quad Phase Shift Keying.
- **PLCP:** Physical Layer Convergence Procedure.
- **PPDU:** PLCP protocol data unit.
- **HR/DSSS**: High Rate Direct Sequence Spread Spectrum.
- **OFDM:** Orthogonal Frequency Division Multiplexing.
- **CFP:** Contention Free Period.
- **PS – Poll:** Power - Save Poll.
- **SSID:** Service Set Identifier. Es un código incluido en todos los paquetes de una red inalámbrica Wi-Fi para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres alfanuméricos. Todos los

dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID.

- **ICV:** Integrity Check Value
- **VPN:** Virtual Private Network.
- **VLAN:** Virtual LAN.
- **TKIP:** Temporary Key Integrity Protocol.
- **EAP:** Extensible Authentication Protocol.
- **PSK:** Pre-Shared Key.
- **OSA:** Open System Authentication.
- **DHCP:** Dynamic Host Configuration Protocol.
- **PSDU:** Physical Layer Service Data Unit .
- **Ruido Blanco:** Whitened en inglés. Se define como ruido aleatorio que contiene energía constante a cada frecuencia o más preciso una distribución uniforme de la energía sobre el espectro de frecuencias.
- **Firmware:** Programa que se imprimió dentro de los circuitos electrónicos del o en su memoria ROM y que no puede ser modificada por el usuario.
- **Firewall:** Sistema diseñado para prevenir el acceso no autorizado a o desde una red privada, en general para intrusos desde el Internet.
- **Troyano:** Virus informático o programa malicioso capaz de alojarse en computadoras y permitir el acceso a usuarios externos, con el fin de socavar la información.