ESTUDIOS DE INGENIERÍA DE TELECOMUNICACIÓN

PROYECTO DE FIN DE CARRERA

CONFIGURACIÓN Y EVALUACIÓN DE REDES 802.11n

CURSO: 2012/2013

LUIS ANTONIO CANO PÉREZ

Universidad de Granada

ESTUDIOS DE INGENIERÍA DE TELECOMUNICACIÓN

CONFIGURACIÓN Y EVALUACIÓN DE REDES 802.11n

REALIZADO POR:
LUIS ANTONIO CANO PÉREZ

DIRIGIDO POR:
D. PABLO ALMEIGEIRAS GUTIÉRREZ
D. JORGE NAVARRO ORTIZ

DEPARTAMENTO
TEORÍA DE LA SEÑAL, TELEMÁTICA Y COMUNICACIONES

Granada, Diciembre 2012

CONFIGURACIÓN Y EVALUACIÓN DE REDES 802.11n

Luis Antonio Cano Pérez

PALABRAS CLAVE: redes wireless, WLAN, 802.11n, MIMO, Hotspot, rendimiento

RESUMEN: Se implementa una red 802.11n formada por un punto de acceso (creado mediante un pc) y una estación. A partir de esta configuración realizaremos pruebas sobre diferentes escenarios para comprobar el rendimiento de la red. También se lleva a cabo la implementación de un servicio Hotspot.

KEYWORDS: wireless networks, WLAN, 802.11n, MIMO, Hotspot, performance

ABSTRACT: It is set up a 802.11n network which consists of an access point (created with a pc) and a station. After that we will test the network performance in different testbeds. It is also set up a Hostspot service.

D. Pablo Ameigeiras Gutiérrez y D. Jorge Navarro Ortiz

Profesores del departamento de Teoría de la Señal, Telemática y Comunicaciones de la Universidad de Granada, como directores del Proyecto Fin de Carrera de D. Luis Antonio Cano Pérez,

Informan:

que el presente trabajo, titulado: “Configuración y evaluación de redes 802.11n”

Ha sido realizado y redactado por el mencionado alumno bajo nuestra dirección, y con esta fecha autorizo a su presentación.

Granada, a _____ de _____ de 20___

Fdo. D. Pablo Ameigeiras Gutiérrez

Fdo. D. Jorge Navarro Ortiz

Los abajo firmantes autorizan a que la presente copia de Proyecto Fin de Carrera se ubique en la Biblioteca del Centro y/o departamento para ser libremente consultada por las personas que lo deseen.

Granada, a ____ de _____ de 20__

Fdo. D. Pablo Ameigeiras Gutiérrez

Fdo. D. Jorge Navarro Ortiz

Fdo. Luis Antonio Cano Pérez

El tribunal constituido para la evaluación del proyecto PFC titulado:

CONFIGURACIÓN Y EVALUACIÓN DE REDES 802.11n

Realizado por el alumno: Luis Antonio Cano Pérez

Y dirigido por los tutores: D. Pablo Almeigeiras Gutiérrez y D. Jorge Navarro Ortiz

Ha resuelto asignarle la calificación de:

- ☐ SOBRESALIENTE (9 - 10 puntos)
- ☐ NOTABLE (7 – 8.9 puntos)
- ☐ APROBADO (5 – 6.9 puntos)
- ☐ SUSPENSO

Con la nota: ☐ puntos.

El Presidente: _____

El Secretario: _____

El Vocal: _____

Granada, a ___ de _____ de 200__

AGRADECIMIENTOS

En primer lugar quisiera agradecer a mis tutores Jorge y Pablo, por la ayuda que me han prestado incluso desde la distancia.

A mi familia, por su apoyo incondicional tanto en los buenos como en los malos momentos.

A mis amigos y compañeros de clase, incluso a los que desertaron en primer curso, porque gracias a todos ellos estos seis años y medio se han hecho más amenos. En especial, José Manuel, por sus consejos y apuntes, porque sin él, todo hubiera sido un poco más difícil.

A mis amigos de toda la vida, que siempre han estado y estarán para lo que haga falta.

A mis amigos que conocí durante mi programa de intercambio Erasmus, el cual fue uno de los mejores momentos de mi vida, aunque a algunos no los volveré a ver, pero siempre me acordaré de todos ellos.

Gracias a todos.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

GLOSARIO

WLAN: Wireless Local Area Network

IEEE: Institute of Electrical and Electronics Engineers

ISM: Industrial, Scientific and Medical

FCC: Federal Communication Comision

IrDA: Infrared Data Association.

WLI Forum: Wireless LAN Interoperability Forum

SIG: Special Interest Group

WiMAX: Worldwide Interoperability for Microwave Access

UMTS: Universal Mobile Telecommunications System

LTE: Long Term Evolution

MIMO: Multiple Input Multiple Output

COITT: Colegio Oficial de Ingenieros Técnicos de Telecomunicación

IP: Internet Protocol

SSID: Service Set Identifier

2/4GFSK: level 2/4 Gaussian Frequency Shift Keying

DPSK: Differencial Phase Shift Keying

DBPSK: Differential Binary Phase Shift Keying

DQPSK: Differencial Quadrature Phase Shift Keying

CSMA/CA: Carrier Sense Multiple Access with Collision Avoidance

NAV: Network Allocation Vector

WECA: Wireless Ethernet Compatibility Alliance

U-NII: Unlicensed National Information Infrastructure

PBCC: Packet Binary Convolutional Coding

VoIP: Voice over IP

QoS: Quality of Service

WEP: Wireless Equivalent Privacy

SNR: Signal-to-Noise Ratio

BPSK: Binary Phase Shift Keying

QPSK: Quadrature Phase Shift Keying

N-QAM: Quadrature Amplitude Modulation (N estados)

HT: High Throughput

TCP: Transmission Control Protocol

HTTP: Hipertext Transfer Protocol

DHCP: Dynamic Host Configuration Protocol

FTP: File Transfer Protocol

PCIe: Peripheral Component Interconnect Express

SSL: Secure Sockets Layer

ETSIIT: Escuela Técnica Superior de Ingeniería Informática y telecomunicaciones

PER: Packet Error Rate

CAPÍTULO 1: INTRODUCCIÓN

1.1 ¿Qué es una red inalámbrica?

Las redes inalámbricas son aquellas en las que la comunicación se lleva a cabo por un medio de transmisión no guiado (sin cables), mediante ondas electromagnéticas que viajan por el aire. La transmisión y la recepción de las ondas se realizan a través de antenas.

No se espera que las redes inalámbricas lleguen a reemplazar a las cableadas, si no que deben verse como un complemento de las mismas.

1.2 ¿Por qué tecnología inalámbrica?

Las redes inalámbricas ofrecen diversas ventajas sobre las redes cableadas [1]:

- **Movilidad**

Los usuarios se mueven, pero los datos normalmente se guardan centralmente. Permitir a los usuarios acceder a los datos cuando se desplazan puede conducir a la obtención de grandes beneficios de productividad. Las redes se construyen porque pueden ofrecer servicios valiosos a los usuarios. En el pasado, los diseñadores se centraban en trabajar con puertos de red porque normalmente eran los que se asignaban al usuario. Con las redes inalámbricas no existen puertos y la red se puede asignar alrededor de la identidad del usuario.

- **Facilidad y velocidad de desarrollo**

Muchas áreas son difíciles de cablear para las LAN con cables tradicionales. Los montajes más antiguos suelen constituir un problema; cablear a través de un edificio de piedra puede convertirse en un reto. Además, en muchos lugares las leyes de preservación histórica dificultan la instalación de nuevas LAN en edificios más antiguos. Incluso en instalaciones modernas, contratar una instalación por cable puede ser caro y tardar mucho tiempo.

- **Flexibilidad**

Estas redes permiten a los usuarios formar rápidamente redes de grupos pequeños para una reunión y facilitan el movimiento entre las diversas estancias de una oficina. La expansión con redes wireless es sencilla ya que el medio de la red se encuentra en cualquier parte. No existen cables que tengamos que conectar. Las redes sin cables utilizan diversas estaciones base para conectar a los usuarios a una red. Sin embargo, la parte de la infraestructura es cualitativamente la misma con la conexión de un usuario o de un millón. Una vez creada la infraestructura, añadir usuario es sólo una cuestión de autorización.

- **Coste**

Algunas veces, el coste se puede reducir mediante la utilización de una tecnología de este tipo. Por ejemplo, se puede utilizar el equipamiento inalámbrico para crear un puente inalámbrico entre dos edificios. La configuración de este requiere de un capital inicial que estará en función del equipamiento externo, los puntos de acceso y las interfaces inalámbricas. Sin embargo, tras el gasto de capital inicial, una red de tecnología wireless solamente tendrá un gasto mensual recurrente poco significativo.

1.3 Tipos de redes inalámbricas

Veremos dos clasificaciones diferentes. En primer lugar según quienes sean los usuarios de la red:

- **Redes privadas**

Aquellas que son propiedad de una entidad concreta (persona, empresa o institución), cuyos miembros son los únicos beneficiarios de uso de dicha red.

- **Redes públicas**

Aquellas que son propiedad de una entidad concreta que cobra a terceras personas por el uso de su infraestructura.

En segundo lugar, por su alcance geográfico [2]:

- **WPAN (Wireless Personal Area Network)**

Redes inalámbricas de área personal. Son las redes de menor alcance. Representan el concepto de redes centradas en las personas, y que les permiten a dichas personas comunicarse con sus dispositivos personales (PDAs, tablets, agendas electrónicas, portátiles) para así hacer posible establecer una conexión inalámbrica con el mundo externo. Estas deben proporcionar una conectividad usuario a usuario. El sistema tendrá que soportar diferentes aplicaciones y distintos escenarios de operación, y así poder abarcar una gran variedad de dispositivos. Son redes privadas. La tecnología más utilizada en estas redes es Bluetooth [3].

- **WLAN (Wireless Local Area Network)**

Redes inalámbricas de área local. En este tipo de redes y más en concreto en el estándar 802.11n [4] es en el que se va a central nuestro proyecto. Según el IEEE [5], una WLAN es un sistema de comunicación de datos que permite que un número de dispositivos independientes se comuniquen directamente entre sí, dentro de un área geográfica de tamaño moderado y utilizando un canal de comunicación físico con una velocidad de datos moderada. Están constituidas por ordenadores, tarjetas de interfaz de red, dispositivos periféricos, medios de red y dispositivos de red. En general son redes privadas. La tecnología más importante para este tipo de redes es WIFI, basada en el estándar 802.11 [6]

- **WMAN (Wireless Metropolitan Area Network)**

Redes inalámbricas de área metropolitana. Son redes que se extienden por un área metropolitana, como una ciudad o un área suburbana. Conectan WLAN que esta separadas por la distancia y que están ubicadas dentro de un área geográfica común. Por ejemplo, un banco con varias sucursales puede utilizar una WMAN. Pueden ser redes públicas o privadas. La tecnología más extendida en estas redes es WiMAX [7].

- **WWAN (Wireless Wide Area Network)**

Red inalámbrica de área extensa. Son las redes de mayor alcance. Están diseñadas para operar sobre grandes áreas geográficas, tales como un país. Permiten que los usuarios mantengan una comunicación en tiempo real con otros usuarios. Algunas de estas son construidas por y para una organización o empresa particular y son de uso privado, otras son construidas por los proveedores de Internet para proveer de conexión a sus clientes. En este caso tenemos varias tecnologías importantes para redes WWAN como UMTS [8] y el reciente LTE [9].

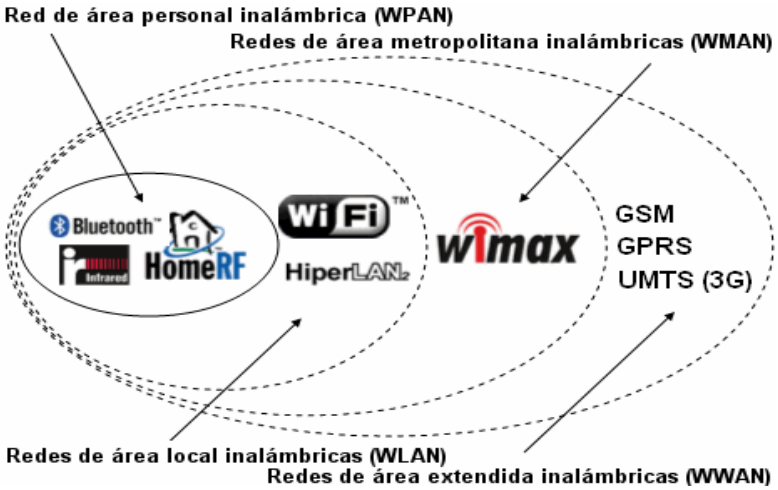

Figura 1.1: Redes inalámbricas según su alcance geográfico

1.4 Evolución histórica de las WLAN

Los expertos empezaban a investigar en las redes inalámbricas hace más de 30 años. Los primeros experimentos fueron llevados a cabo por IBM, cuando en 1979, publicaba los resultados de su experimento con infrarrojos en una fábrica suiza. La idea de los ingenieros era construir una red local en la fábrica. Los resultados se publicaron en el volumen 67 de los Proceeding del IEEE y han sido considerados como el punto de partida en la línea evolutiva de las redes inalámbricas.

Las siguientes investigaciones se harían en laboratorios, siempre utilizando altas frecuencias, hasta que en 1985 la FCC asigna una serie de bandas al uso de IMS. Este hecho propició una mayor actividad en el seno de la industria: ese respaldo hizo que las WLAN empezaran a dejar ya el laboratorio para iniciar el camino hacia el mercado.

En 1989, en el seno de IEEE 802, se formó el comité IEEE 802.11, que empieza a trabajar para tratar de generar una norma para las WLAN.

Después, en Mayo de 1991 se publicaron varios trabajos referentes a WLAN operativas que superaban la velocidad de 1 Mbps, el mínimo establecido por el IEEE para que la red sea considerada LAN.

En 1992 se creó Winforum, consorcio liderado por Apple y formado por empresas del sector de las telecomunicaciones y de la informática para conseguir bandas de frecuencia para los sistemas PCs.

En 1993 también se constituyó la IrDA para promover el desarrollo de las WLAN basadas en enlaces por infrarrojos.

Más tarde, en 1996, un grupo de empresas del sector de informática móvil y de servicios formaron el WLI Forum para potenciar este mercado mediante la creación de un amplio abanico de productos y servicios interoperativos.

En 1997 el IEEE ratificó el estándar para WLAN IEEE 802.11, que alcanzaba una velocidad de 2 Mbps y trabajaba en la banda de 2,4 GHz y se definió el funcionamiento y la interoperabilidad entre redes inalámbricas.

Un poco más tarde, en 1999, se aprobó 802.11b [10], una extensión de 802.11 para WLAN empresariales, con una velocidad máxima de 11 Mbps y un alcance de 100 metros. También trabajaba en 2,4 GHz.

En Junio del mismo año, el IEEE ratificó otra modificación, 802.11a [11], la cual, alcanzaba una velocidad de hasta 54 Mbps en la banda de 5 GHz, pero con un alcance limitado a 50 metros.

Cuatro años después, en 2003, el IEEE aprobó la corrección 802.11g [12], compatible con la 802.11b, capaz de alcanzar una velocidad de 54 Mbps en la banda de 2,4 GHz.

Finalmente, en 2009, fue aprobada la última corrección a 802.11, 802.11n, el cual puede alcanzar una velocidad de hasta 600 Mbps y puede trabajar en ambas bandas, 2,4 y 5 GHz. Se hablará con más en detalle sobre este en capítulos posteriores, ya que será el tema principal de nuestro proyecto.

Actualmente, la modificación 802.11ac se encuentra en fase de desarrollo. Se espera su terminación para finales de año, y su ratificación para 2013. Esta modificación promete mejorar las tasas de transferencia hasta 1 Gbps dentro de la banda de 5 GHz, ampliar el ancho de banda hasta 160 MHz (40 Mhz en las redes 802.11n), hasta 8 flujos MIMO y modulación de alta densidad (256 QAM).

Se han nombrado las modificaciones más importantes de 802.11 pero existen muchas otras, las cuales se verán con más detalle en el capítulo siguiente.

1.5 Evolución del mercado de las comunicaciones inalámbricas

La evolución del mercado de redes inalámbricas fue lenta al principio debido, entre otros motivos, a los desequilibrios entre oferta y demanda, las prestaciones de los productos o servicios, los precios, normalmente elevados, y la ausencia de normas.

A pesar de todo esto, el crecimiento del mercado de redes inalámbricas, tanto mundial como europeo, ha sido realmente espectacular durante los últimos años, en los que ha experimentado crecimientos anuales superiores al cien por cien, principalmente por tres razones: el auge experimentado por el mercado de los equipos portátiles, el desarrollo de las comunicaciones móviles y la conclusión del estándar IEEE 802.11.

Figura 1.2: Crecimiento mercados redes inalámbricas 2001-2004

Según un reciente informe [13] realizado por Cisco, una de las empresas líderes en el ámbito de las telecomunicaciones, el tráfico global de redes móviles se multiplicará por 26 entre 2010 y 2015. De hecho, el crecimiento del tráfico de datos móviles a nivel mundial seguirá un ritmo exponencial. La Figura 1.3 muestra el crecimiento del tráfico de datos móviles mientras que en la imagen de debajo, Figura 1.4, el crecimiento en el tráfico según el tipo de dispositivo. En todos los casos la tendencia es de forma ascendente a un ritmo muy alto.

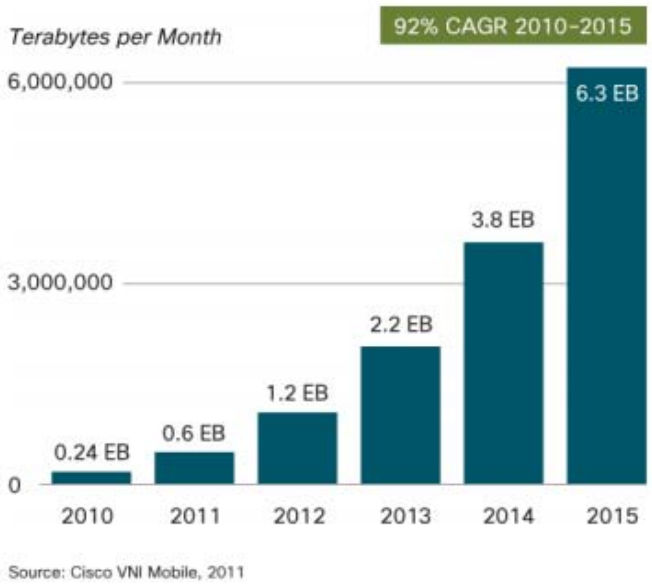

Figura 1.3: Crecimiento comunicaciones móviles 2010-2015

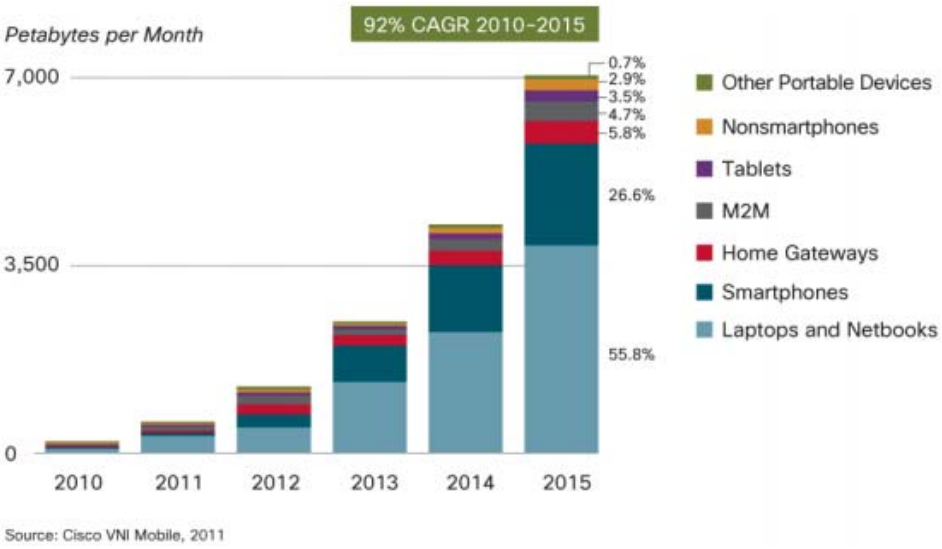

Figura 1.4: Crecimiento por dispositivo 2010-2015

Algunos datos de especial relevancia en este estudio son los siguientes:

- En 2010, el tráfico mundial de datos móviles superó en tres veces el tamaño de todo el tráfico global de Internet (fijo y móvil) generado en el año 2000.
- En 2015 habrá más de 5600 millones de dispositivos personales conectándose a redes móviles y 1500 millones de conexiones entre máquinas. Todos en conjunto, equivalen a una conexión móvil a la red por cada habitante del mundo.
- El tráfico móvil que se realizará desde dispositivos tablets se multiplicará por 205 entre 2010 y 2015.
- Para 2015, los dispositivos tablets generarán por sí solos más tráfico que la suma total de datos que han cruzado la Red móvil durante 2010. Serán responsables de un tráfico de 248 petabytes mensuales en 2015, frente a los 237 petabytes mensuales generados en 2010 por todos los dispositivos de acceso.

Se han realizado y se realizan numerosos estudios sobre el auge de las comunicaciones inalámbricas en los últimos años para mostrar la penetración de esta forma de comunicación en nuestras vidas. Todos ellos reflejan una tendencia ascendente tanto en el número de dispositivos como en el tráfico que se va a producir en el futuro.

1.6 Motivación y objetivos

El auge de las comunicaciones inalámbricas es un hecho incuestionable. Cada vez disponemos de más dispositivos con interfaz wireless, como hemos visto en el apartado anterior. En un futuro muy próximo incluso las cosas [14] dispondrán de su interfaz propio.

Este proyecto está centrado en las WLAN, y más en concreto en 802.11, debido a los siguientes motivos:

- Según [15], actualmente, alrededor del 50% del tráfico wireless se origina en escenarios interiores (indoor).

- Según un artículo de Jose Manuel Huidobro para el COITT [16], WIFI está incrementando su relevancia, ya que a día de hoy supone la mejor alternativa ante el problema de la congestión de las redes 3G. Para ello se lleva a cabo la descarga de tráfico de estas redes a redes fijas (traffic offloading).

- Según un estudio de ABI Research [17], la venta de chipsets WIFI se está incrementando desde 2007 a un ritmo del 27% al año y lo seguirá haciendo hasta 2015, llegando a sobrepasar la venta de chipsets móviles.

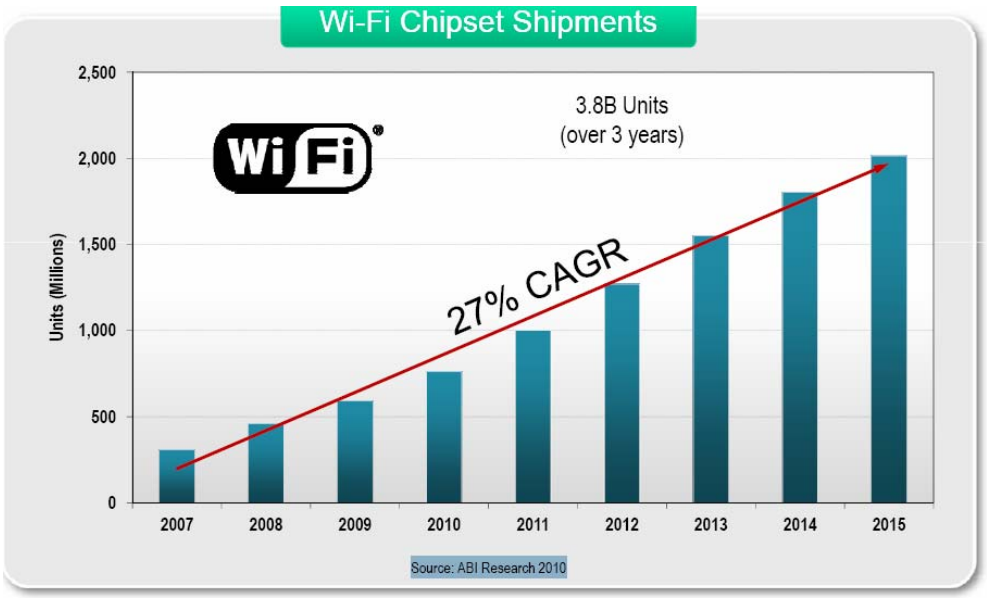

Figura 1.5: Incremento venta chipsets WIFI

- Las nuevas redes 802.11n, prometen una gran mejora de la capacidad y el bit rate debido a la inclusión de MIMO [18]. Se pueden alcanzar hasta un máximo de 600 Mbps [19]

Los objetivos que se persiguen en este proyecto están bien definidos:

- En primer lugar, configurar una red 802.11n. Para ello se configurará un equipo como punto de acceso y otro como estación. Después se implementará un servicio Hotspot para la red.

- En segundo lugar, entender el funcionamiento de 802.11n viendo sus características comunes y diferencias con las demás extensiones.

- Por último, analizar el rendimiento de la red 802.11n previamente creada. Para ello se realizarán una serie de experimentos de los cuales se obtendrán unos resultados que serán comparados con la teoría.

1.7 Organización

La documentación de este PFC está estructurada en 7 capítulos.

El primero de ellos, en el que nos encontramos, constituye una introducción en el que se realiza una primera aproximación al marco en el que se desarrolla el proyecto, las redes inalámbricas y con más detalle las WLAN.

El segundo capítulo es también introductorio, pero algo más específico. En este se hace una revisión detallada del protocolo 802.11.

En el tercer capítulo se describirá la extensión 802.11n de la cual se va a hacer uso en este proyecto.

En el capítulo cuatro se presentará la planificación temporal del proyecto y la estimación de los costes del mismo.

En el capítulo cinco se detallarán los dos escenarios con los que trabajaremos, así como las configuraciones de ambos.

En el capítulo seis muestra los resultados extraídos de los experimentos realizados en el escenario 1.

Por último, el capítulo siete está dedicado a conclusiones y posibles líneas futuras de estudio.

CAPÍTULO 2: PROTOCOLO 802.11

2.1 Elementos de una WLAN 802.11

Las redes 802.11 están compuestas por cuatro componentes físicos principalmente [20]:

- **Estaciones (STA, station)**

Las redes se crean para transferir datos entre estaciones. Las estaciones son dispositivos informáticos con interfaces de red inalámbrica. Normalmente, las estaciones son equipos portátiles que funcionan con baterías, pero podrían ser también equipos no portables. En algunos entornos, el sistema de red inalámbrico se utiliza para evitar tener que incluir un nuevo cableado y los equipos de sobremesa se conectan mediante WLAN inalámbricas.

- **Puntos de acceso (AP, access point)**

Los puntos de acceso son las puertas de enlace de las estaciones a Internet. Realizan la función de puente entre la red inalámbrica y la cableada. También son los encargados de encapsular las tramas 802.11 en las tramas IP, para su entrega al resto del mundo.

- **Medio inalámbrico (WM, wireless medium)**

Para mover las tramas de una estación a otra, el estándar utiliza un medio inalámbrico. Este contempla tres capas físicas: 2 capas físicas de radiofrecuencia y una de infrarrojos, aunque las capas RF han resultado ser mucho más populares.

- **Sistema de distribución (DS, distribution system)**

Cuando existen varios puntos de acceso en una red para formar una gran área de cobertura, es necesaria la comunicación entre ellos para registrar los movimientos de las estaciones móviles. Esta es la función del sistema distribuido. 802.11 no especifica ninguna tecnología particular para este.

Figura 2.1: Componentes de una WLAN 802.11

2.2 Configuraciones de una red 802.11

La base de una red 802.11 [21] es el **Conjunto de Servicio Básico (BSS, Basic Service Set)**, que es simplemente un grupo de estaciones que se comunican entre sí. Las comunicaciones tienen lugar dentro de un área poco definida denominada área de servicio básico definida por las características de propagación del medio inalámbrico. Cuando una estación está en el área de servicio básico, puede comunicarse con el resto de miembros del BSS. Los BSS pueden ser de dos tipos:

- **BSS independiente (IBSS)**

Las estaciones en un IBSS se comunican directamente entre sí, y por tanto, deben encontrarse dentro del alcance directo de la comunicación. La red 802.11 más pequeña posible es un IBSS con dos estaciones. Normalmente, los IBSS se componen de una pequeña cantidad de estaciones configuradas para un propósito específico y durante un corto período de tiempo. Debido a su corta duración, pequeño tamaño y objetivo principal, los IBSS a veces se conocen como BSS provisionales. También son conocidos como redes ad-hoc.

- **BSS infraestructura**

En este caso las estaciones utilizan un punto de acceso para todas las comunicaciones, incluyendo la comunicación entre nodos móviles en la misma área de servicio. Si una estación móvil en una BSS de infraestructura necesita comunicarse con otra estación móvil, la comunicación debe tener dos saltos. Primero, la estación móvil de origen transfiere la trama al punto de acceso. Segundo, el punto de acceso transfiere la trama a la estación de destino. Aunque la transmisión de múltiples saltos requiere

mayor capacidad de transmisión que una trama dirigida desde el remitente al receptor, tiene dos ventajas importantes:

- Aumenta la cobertura del área de servicio, ya que pueden comunicarse dos estaciones que no son accesibles directamente, siempre que cada una de ellas pueda acceder al punto de acceso.

- Las estaciones móviles pueden entrar en modo de ahorro de energía, ya que el punto de acceso guardará sus paquetes y los enviará cuando salga de dicho modo.

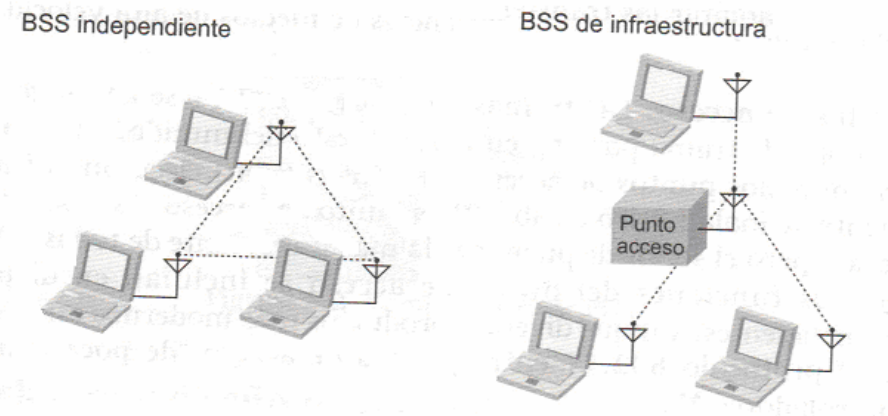

Figura 2.2: BSS Independiente e Infraestructura

Los BSS pueden ofrecer cobertura en oficinas pequeñas y en domicilios particulares, pero no pueden ofrecer cobertura de red para áreas más grandes.

802.11 permite crear redes inalámbricas de un tamaño arbitrariamente grande y enlazar los BSS en un Conjunto de **Servicios Extendido (ESS, Extended Service Set)**. Un ESS se crea encadenando los BSS entre sí con una red troncal. Todos los puntos de acceso en un ESS tienen el mismo SSID, que sirve como nombre de red a los usuarios. La red troncal puede estar implementada con cualquier tecnología, pero habitualmente se utiliza Ethernet [22]

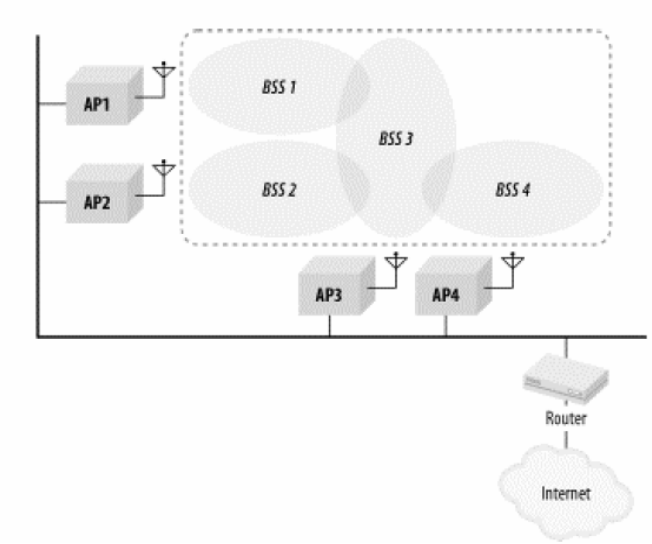

Figura 2.3: Conjunto de servicio extendido

2.3 Arquitectura 802.11

El estándar IEEE 802.11 define el uso de los dos niveles inferiores de la arquitectura OSI [23], la capa física y la de enlace.

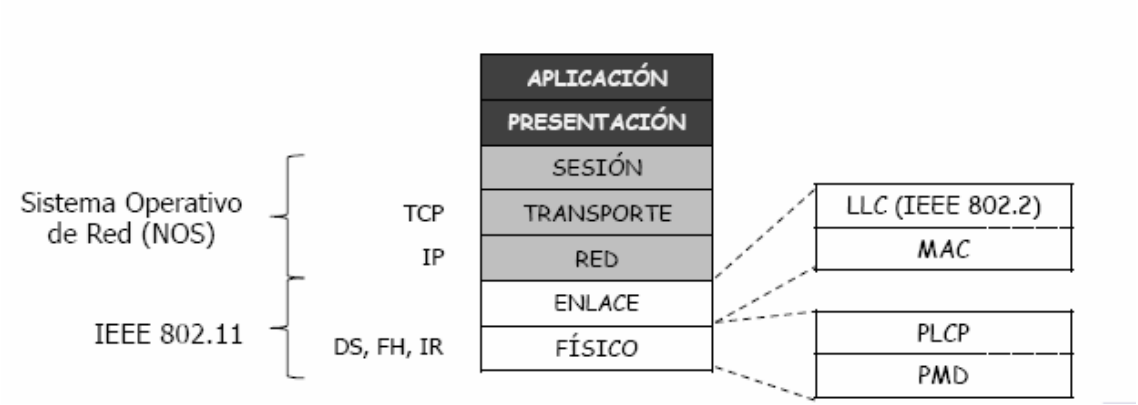

Figura 2.4: Arquitectura 802.11 modelo OSI

2.3.1 Capa física (PHY)

El estándar 802.11 define en la capa física los medios eléctricos, mecánicos, de procedimiento y funcionales para activar y mantener el enlace físico entre sistemas.

La capa física se divide en dos subcapas como se puede ver en la figura 2.4: PLCP (Physical Layer Convergence Procedure) y PMD (Physical Medium Dependent).

La subcapa PCLP básicamente se encarga de formatear los datos para su posterior modulación por la capa PMD.

PMD es la subcapa dependiente del medio. Maneja directamente las comunicaciones radio con el medio inalámbrico.

En la revisión inicial de 802.11 en 1997 se estandarizaron tres capas físicas:

- **Capa física de radio de Espectro Expadido de Salto de Frecuencia (FHSS, Frecuency Hopping Spread Spectrum)**

De todas las capas físicas estandarizadas en el primer borrador esta fue la primera en implantarse ampliamente. Los sistemas electrónicos utilizados para admitir la modulación FH son relativamente baratos y no requieren gran cantidad de potencia. Al principio la ventaja de utilizar redes de salto en frecuencia era que podían coexistir una gran cantidad de redes y el rendimiento global de todas ellas era muy alto. Actualmente, sólo un suministrador sigue fabricando y vendiendo sistemas de salto en de frecuencia y se están quedando desfasados.

El salto de frecuencia depende del cambio rápido de frecuencia de transmisión de una manera predeterminada pseudo-aleatoria, tal y como se ilustra en la figura 2.5. El eje vertical divide la frecuencia disponible en diversas franjas. Asimismo, el tiempo también se divide en franjas. Un patrón de salto controla como se utilizan las franjas. Cronometrar correctamente los saltos en la clave del éxito, tanto el transmisor como el receptor deben sincronizarse para que el receptor este siempre escuchando en la frecuencia del transmisor.

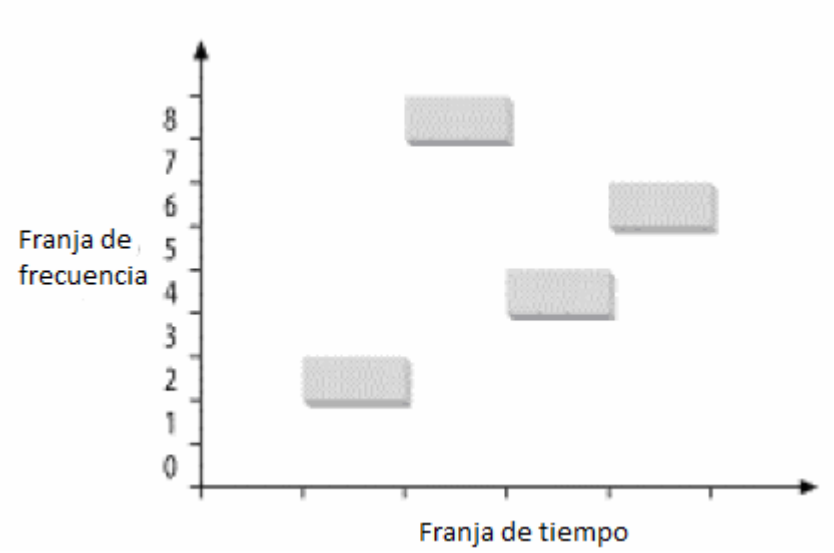

Figura 2.5: Salto de Frecuencia

FHSS divide la banda ISM en 79 canales de 1 MHz. Aproximadamente el 90% de la energía de radio se configura para el canal. El método de modulación utilizado por 802.11 codifica los bits de datos como cambios en la frecuencia de transmisión desde el centro del canal (2GFSK y 4GFSK).

- **Capa física de radio de Espectro Expandido de Secuencia Directa (DSSS, Direct Sequence Spread Spectrum)**

Aunque DS operaba a la misma velocidad que FH, enseguida se hizo evidente que la tecnología de secuencia directa tenía potencialmente velocidades superiores a la tecnología de salto de frecuencia. Como resultado, la secuencia directa se convirtió en la PHY de elección.

La solución básica de las técnicas de secuencia directa es propagar la energía RF sobre una banda ancha y los receptores pueden ejecutar procesos correlativos para buscar cambios. La solución básica de alto nivel se muestra en la figura 2.6.

A la izquierda se encuentra una señal de radio de banda estrecha tradicional. Se procesa a través de un propagador que aplica una transformación matemática para recoger una entrada de banda estrecha y nivelar la amplitud a través de una banda de frecuencia relativamente ancha. Para un receptor de banda estrecha, la señal transmitida parece un ruido de bajo nivel ya que su energía RF se propaga a través de una banda muy ancha. La clave de la transmisión de secuencia directa es que cualquier modulación de la portadora de RF también se propaga a través de la banda de frecuencia. Los receptores pueden supervisar una banda de frecuencia ancha y buscar cambios que se

producen a través de toda la banda. La señal original se puede recuperar con un correlador que invierte el proceso de transmisión.

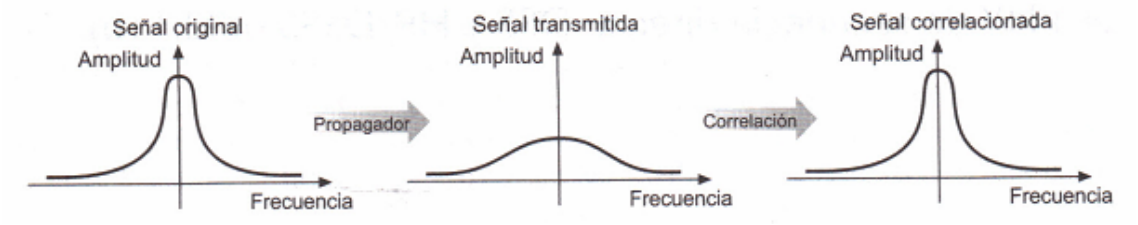

Figura 2.6: Secuencia Directa

La tecnología de secuencia directa funciona aplicando una secuencia de chips pseudoaleatoria para el flujo de datos. Un chip es un dígito binario utilizado por el proceso de propagación. Los bits son datos de nivel superior mientras que los chips son números binarios utilizados en el proceso de codificación.

Para el código pseudoaleatorio se adoptó una palabra de Barker de 11 bits. Cada bit se codifica utilizando una palabra Barrer como una secuencia de chips.

Los canales para secuencia directa son mucho más grandes que para salto de frecuencia. En este caso la banda ISM de 2,4 GHz se divide en 14 canales de 22 MHz de ancho cada uno, con una separación de 5 MHz entre ellos. Por tanto se produce solapamiento entre canales. Pero no todos los canales están disponibles en todo el mundo. En Europa solo se pueden usar del 1 al 13. Además en cada región se definen grupo de canales que pueden trabajar sin interferencia entre ellos. En Europa se han definido los canales 1,7 y 13.

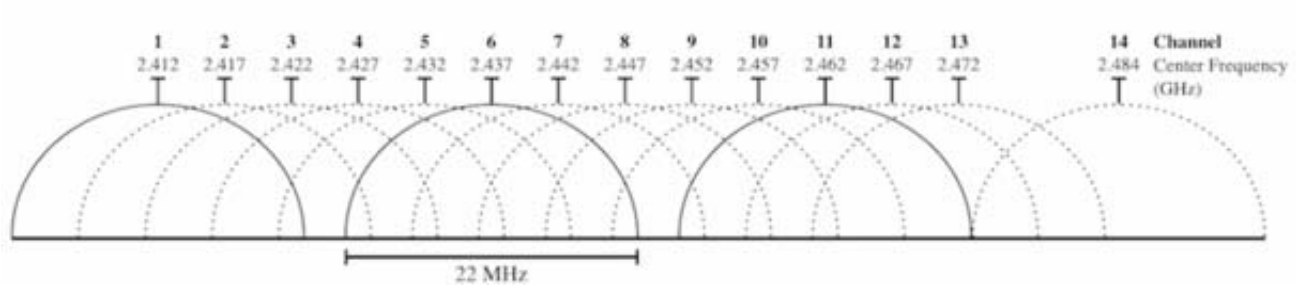

Figura 2.7: Canales secuencia directa

Las modulaciones utilizadas en secuencia directa son: DPSK, DBPSK y DQPSK.

- **Capa física de Luz Infrarroja (IR, Infrarred Light)**

No se va a analizar, ya que hasta el momento no se ha implantado en ningún producto comercial. Tan solo decir que necesita visión directa y que es muy sensible a objetos móviles.

2.3.2 Capa de enlace

La capa de enlace se divide en dos subcapas como se ve en la figura 2.4: MAC (Medium Access Control) y LCC (Logical Control Link).

La subcapa LLC es la responsable del control de enlace lógico. Maneja el control de errores, control del flujo, entramado, control de diálogo y direccionamiento de la subcapa MAC.

La subcapa MAC es la encargada de gestionar los procesos y funciones necesarios para el acceso de los dispositivos a la red. Hace uso de dos funciones para controlar el acceso al medio inalámbrico:

- **Función de coordinación distribuida (DCF, Distributed Coordination Function)**

DCF esta basado en el protocolo de acceso al medio **CSMA/CA**, que proporciona un servicio basado en contención. DCF permite que múltiples estaciones interactúen sin un control central, si no que son las propias estaciones las que gestionan el acceso. Por tanto, se puede utilizar tanto en redes IBSS como en redes infraestructura. Es necesaria su implementación tanto en estaciones como en puntos de acceso. Es la función más extendida entre los productos comerciales.

El funcionamiento de CSMA/CA es el siguiente. Cuando una estación quiere transmitir, primero tiene que escuchar el medio, para detectar el estado de este (libre/ocupado) si se determina como libre después de un tiempo de contención determinado, transmite y envía la trama. Por su parte, el receptor responde con una trama ACK (Acknowledgement) para confirmar la recepción. Si el emisor no recibe esta trama durante un tiempo indicado, asume que los datos se han perdido y empieza a retransmitir. Después de cada trama colisionada se introduce un tiempo de espera (backoff) antes de volver a transmitir.

Sin embargo CSMA/CA presenta algunas deficiencias como la del nodo oculto y la del nodo expuesto. El problema del nodo oculto consiste en que dos o más estaciones no pueden detectar las transmisión ajenas cuando no están en el área de alcance de las otras. Se puede ver muy claramente en la figura 2.8

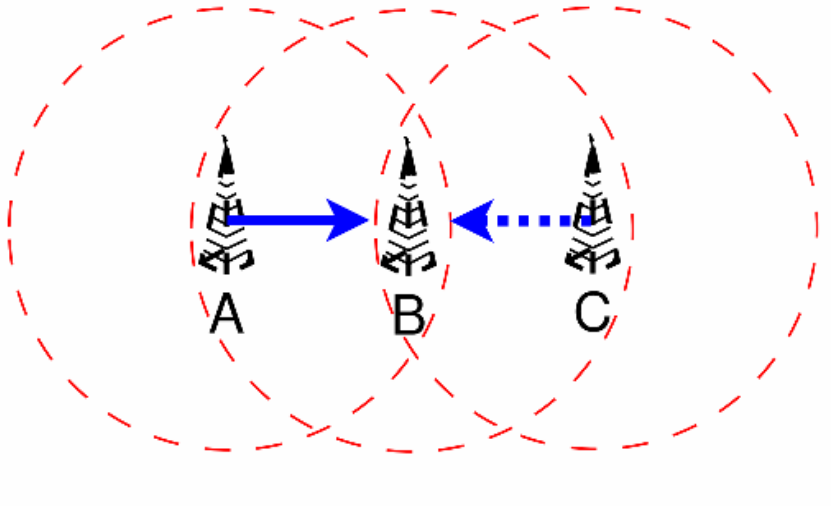

Figura 2.8: Problema del nodo oculto

El problema del nodo expuesto se da cuando una estación que quiere transmitir a un nodo escucha una transmisión de otro nodo a un destino distinto al suyo, con lo que asume que el medio está ocupado y no transmite.

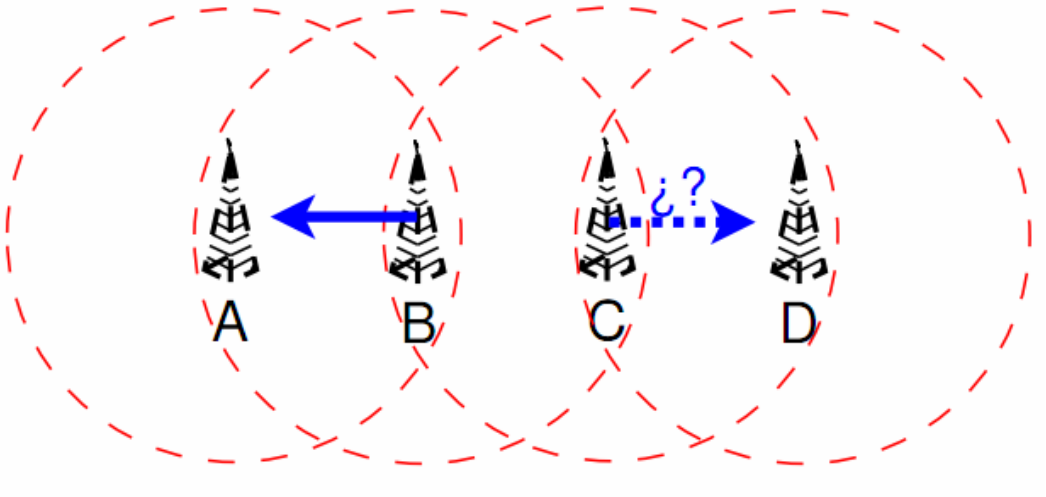

Figura 2. 9: Problema del nodo expuesto

Para resolver estos problemas, se propone **MACA** (MultiAccess Collision Avoidance) como solución a las deficiencias de CSMA/CA.

La entrega de datos se realiza con reserva del medio por parte de las estaciones emisora y receptora. Esto se lleva a cabo con las tramas RTS (Request To Send) y CTS (Clear), las cuales se verán más adelante, en el apartado de tramas.

En la figura 2.10 se puede ser el proceso de entrega de datos con DCF. En primer lugar la estación debe esperar un tiempo DIFS, que es el tiempo mínimo que el medio debe estar vacío para poder transmitir. Pasado este tiempo, el transmisor manda una trama RTS para sondear si el receptor esta disponible para recibir datos. A su vez, reserva el medio, ya que las demás estaciones ven que esta quiere transmitir. A continuación, el receptor, tras un tiempo SIFS (tiempo mínimo de respuesta para transmisiones de alta prioridad, ACK y RTS/CTS), contesta al transmisor con una trama CTS confirmándole que puede transmitir. Después el emisor, tras otro tiempo SIFS, transmite la trama de datos. Por último el receptor, tras haber esperado un tiempo SIFS, confirma la correcta recepción de los datos mediante una trama ACK.

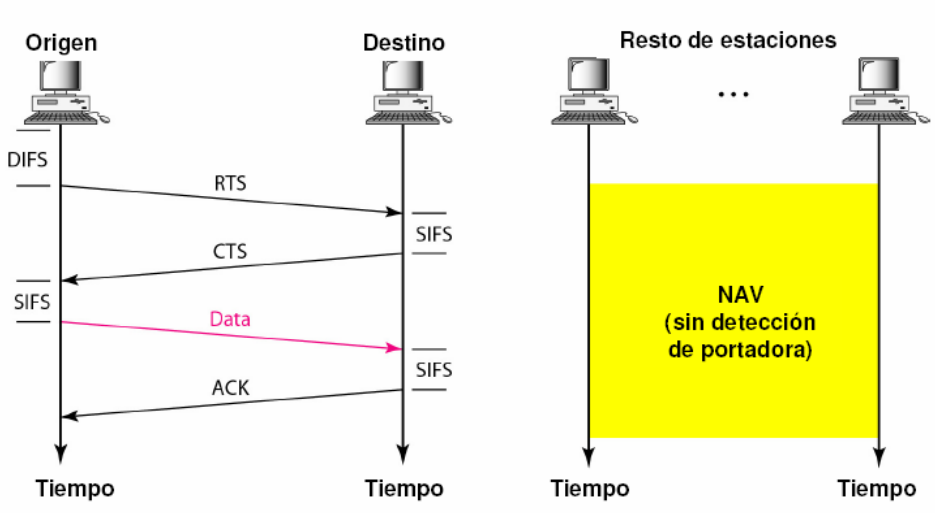

Figura 2.10: Entrega de datos con DCF

- **Función de coordinación puntual (PCF, Point Coordination Function)**

La función de coordinación puntual proporciona servicios sin contención. Los PC (Point Coordinator) coordinan la transmisión de las estaciones. El papel de PC reside en los puntos de acceso, por lo que PCF se restringe a las redes infraestructura. No es una función muy extendida. Solamente esta implementada en algunos AP. Permite soportar servicios con requisitos estrictos de tiempo.

Cuando se usa PCF el tiempo del medio se divide entre el período sin contención y el período de contención. El acceso al medio en el primer caso está controlado por PCF mientras que el acceso al medio en el segundo caso está controlado por DCF. Períodos alternativos de servicios sin contención y servicios con contención se repiten a intervalos regulares, lo que se denomina intervalos de repetición sin contención.

En la figura 2.11 podemos ver el proceso de entrega de datos. En primer lugar se lleva a cabo la reserva del medio durante el período sin contención por parte del PC. Para ello el AP transmite una trama Beacon, en la que se indica la duración del período. Cuando el punto de acceso ha obtenido el control del medio, busca en su lista de polling y asigna turnos a las estaciones, mediante un esquema Round-Robin. Durante el período de contención, las estaciones pueden transmitir sólo si el punto de acceso solicita la transmisión con una trama de sondeo FC-Poll). Cada FC-Poll es una licencia para transmitir una trama. Si una estación no respondiera, perdería su turno. Al final del período de contención el AP avisa de este hecho a las estaciones mediante una trama FC-End.

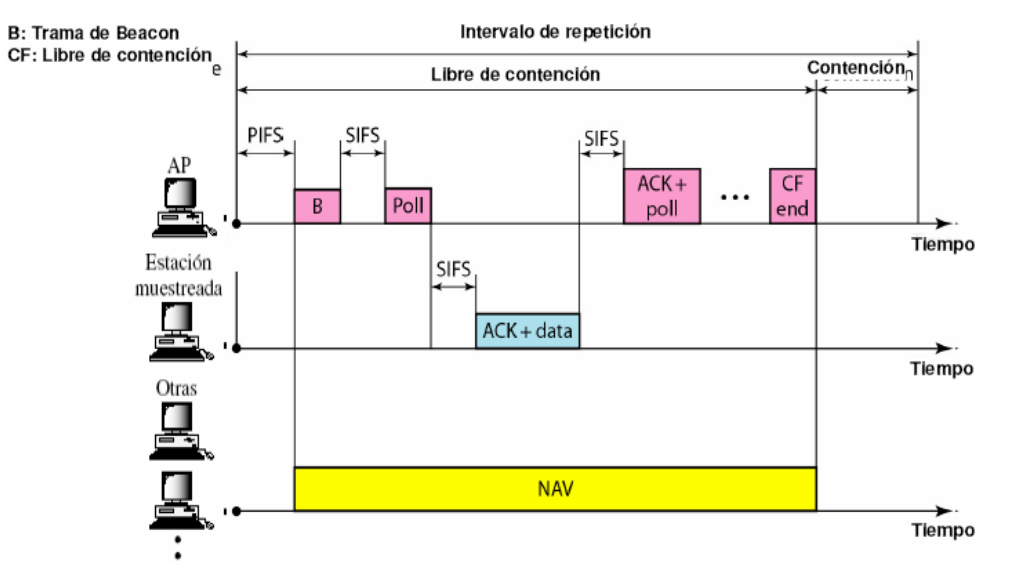

Figura 2.11: Entrega de datos con PCF

2.4 Tramas MAC 802.11

2.4.1 Formato de trama

El formato de trama MAC 802.11 genérico se puede ver en la figura 2.12.

Figura 2.12: Trama MAC 802.11 genérica

- **Control de trama**

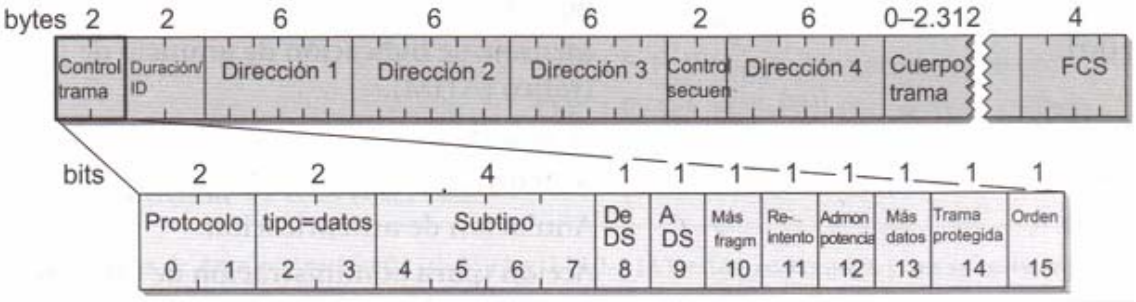

Figura 2.13: Campo de control de trama

Cada trama se inicia con un campo de control de trama de dos bytes. Los componentes de este campo son:

- **Versión del protocolo**: dos bits indican que versión de MAC 802.11 se contiene en el resto de la trama. Actualmente sólo se ha desarrollado una versión a la cual se le ha asignado el número de protocolo 0.

- **Campos tipo y subtipo**: estos campos identifican el tipo de trama utilizado. En el siguiente apartado se verán los tipos de tramas.

- **Bits ToDS y FromDS**: estos bits indican si una trama está destinada para el sistema de distribución. Todas las tramas en redes infraestructura tendrán un conjunto de bits del sistema de distribución. En la tabla 2.1 se muestra la interpretación de estos bits.

	ToDS= 0	ToDS=1
FromDS=0	Todas las tramas de administración y control Tramas de datos dentro de un IBSS (nunca tramas de datos de infraestructura).	Tramas de datos transmitidas desde una estación inalámbrica en una red de infraestructura.
FromDS=1	Tramas de datos recibidos para una estación inalámbrica en una red de infraestructura.	Tramas de datos en un "puente inalámbrico".

Tabla 2.1: Interpretación bits ToDS y FromDS

- **Bit more fragments**: funciona de manera muy similar al bit del mismo nombre que contienen los paquetes IP. Cuando se ha fragmentado un paquete de nivel superior a través de MAC, el siguiente fragmento inicial y cualquier fragmento que no sea el final establece este bit a 1. Algunas tramas de datos y de administración pueden ser lo bastante largas como para necesitar fragmentación.

- **Bit retry**: en alguna ocasión, las tramas pueden ser retransmitidas. Cualquier trama retransmitida establece este bit a 1 para ayudar a la estación receptora a eliminar tramas duplicadas.

- **Bit de administración de potencia**: este bit indica si el remitente esta en modo ahorro de potencia tras la finalización del intercambio de tramas actual. El número 1 indica que la estación estará en modo de ahorro de potencia y el 0 indica que la estación esta activa. Los puntos de acceso ejecutan diversas funciones de administración importantes y no admiten este modo, por lo que este bit siempre es 0 para tramas transmitidas por un AP.

- **Bit more data**: para acomodar las estaciones al modo de ahorro de potencia, los puntos de acceso pueden guardar en un búfer las tramas recibidas desde el sistema de distribución. Un AP establece este bit a 1 para indicar que se encuentra disponible y se dirige a una estación en estado de suspensión.

- **Bit trama protegida**: las transmisiones inalámbricas son más fáciles de interceptar que las transmisiones en una red fija. Si la trama está protegida por protocolos de seguridad en la capa de enlace, este bit se establece a 1. Anteriormente era conocido como bit WEP, tal y como viene nombrado en la figura 2.13.

- **Bit orden**: las tramas y los fragmentos se pueden transmitir en un determinado orden a costa de un procesamiento adicional tanto transmisor como para receptor. Cuando se emplea la entrega en orden estricto este bit se establece a 1.

- **Campo duración/ID**

Este campo tiene diversos usos y adopta una de las tres formas mostradas en la figura 2.14.

Figura 2.14: Formatos del campo Duración/ID

- **Configuración de NAV**: cuando el bit 15 es 0, el campo se utiliza para establecer el NAV. El valor representa el número de microsegundos que se espera que permanezca ocupado el medio para la transmisión actual en progreso. Todas las estaciones tienen que supervisar los encabezados de todas las tramas que reciben y actualizar el NAV en consecuencia.

- **Tramas transmitidas durante el período sin contención**: durante los períodos sin contención, el bit 14 es 0 y el 15 es 1. El resto de bits son 0, por lo que este campo toma un valor de 32.768. Este valor se interpreta como un NAV. Permite a cualquier estación que no haya recibido el anuncio del período de contención actualizar el NAV con un valor superior apropiado para evitar la interferencia con transmisiones si contención.

- **Tramas PS-Poll**: los bits 14 y 15 se establecen a 1 en estas tramas (sondeo de ahorro de potencia). Las estaciones móviles tienen la opción de ahorrar batería desactivando las antenas. Las estaciones dormidas deben despertarse periódicamente. Para asegurarse que no se pierde ninguna trama, las estaciones despiertan de su letargo transmitiendo una trama de este tipo para recuperar cualquier trama guardada en el búfer del punto de acceso. En la trama PS-Poll se incorpora el ID de asociación (AID) que indica el BSS al que pertenece la estación. El AID puede variar de 1 a 2.007. Los valores comprendidos entre 2.008 y 16.383 no se utilizan.

- **Campo de dirección**

Una trama 802.11 puede contener hasta cuatro campos de dirección. Los campos de dirección se enumeran porque se utilizan distintos campos para distintos propósitos, dependiendo del tipo de trama. El direccionamiento en 802.11 sigue los convenios utilizados por las otras redes IEE 802, incluyendo Ethernet. Las direcciones ocupan 48 bits. Si el primer bit es 0 la dirección representa una sola estación (unicast). Cuando el primer bit es 1 la dirección representa un grupo de estaciones físicas (multidifusión). Si todos los bits son 1 la trama es broadcast y se entrega a todas las estaciones conectadas al medio. Las direcciones se utilizan para diversos propósitos:

- **Dirección de destino (DA, Destination Address)**: la dirección de destino es el identificador IEEE MAC que se corresponde con el receptor final.

- **Dirección de origen (SA, Source Address)**: la dirección de origen identifica el origen de la transmisión. Solamente una estación puede ser origen de una trama.

- **Dirección del receptor (RA, Receiver Address)**: esta dirección indica qué estación inalámbrica debe procesar la trama. En el caso de un IBSS, no se utilizan puntos de acceso y no hay un sistema de distribución. Por tanto, en este caso el transmisor es el origen y el receptor es el destino.

- **Dirección del transmisor (TA, Transmitter Address)**: esta dirección identifica la interfaz inalámbrica que ha transmitido la trama hacia el medio. Los transmisores no son necesariamente los remitentes. El remitente es la trama que ha generado el paquete de protocolos de la capa de red. Por otro lado, el transmisor coloca la trama en el enlace de radio

- **ID del conjunto de servicios básicos (BSSID)**: sirve para identificar las distintas WLAN en la misma área. En las redes infraestructura, la BSSID es la dirección MAC utilizada por la interfaz inalámbrica en el punto de acceso. Las redes adhoc generan un BSSID aleatorio.

- **Campo de control de secuencia**

Es un campo de 16 bits que se utiliza tanto para la desfragmentación como para las tramas duplicadas descartadas. Está compuesto por un subcampo de número de fragmento de 4 bits y un subcampo de número de secuencia de 12 bits, tal y como muestra la figura 2.15. Los números de secuencia no se utilizan en la tramas de control, por lo que este campo no se encuentra presente.

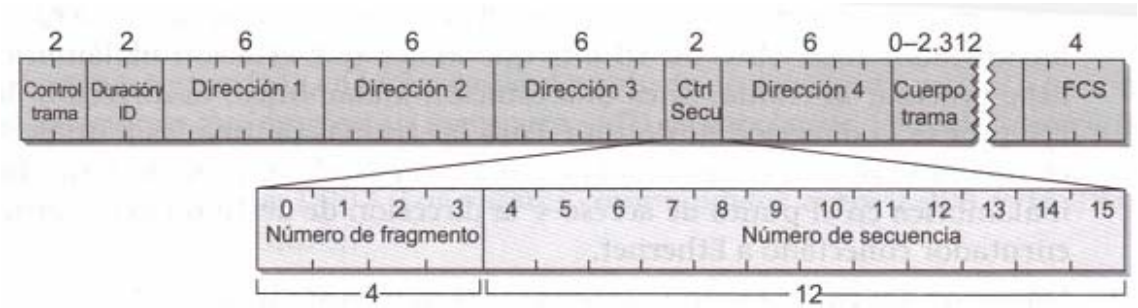

Figura 2.15: Campo de control de secuencia

- **Cuerpo de la trama**

El cuerpo de la trama, también conocido como campo de datos, desplaza la carga útil de la capa superior de una estación a otra. Tal como se especificó originalmente, 802.11 puede transmitir tramas con una carga útil máxima de 2304 bytes de datos de nivel superior. 802.11 difiere de otras tecnologías de capa de enlace en dos puntos significativos. Primero, en la trama 802.11 no existe una etiqueta de protocolo de nivel superior para distinguir entre los distintos tipos de protocolo de capa superior. Los protocolos de nivel superior se etiquetan con un campo de tipo mediante un encabezado adicional que se utiliza como inicio de la carga útil. Segundo, 802.11 generalmente no

rellena las tramas para obtener una longitud mínima. Muchas tramas utilizadas son cortas y los chips y mecanismos electrónicos utilizados en las interfaces de red han progresado hasta el punto que ya no es necesario el relleno.

- **Secuencia de comprobación de tramas**

Igual que Ethernet, la trama 802.11, se cierra con una secuencia de comprobación de trama (FCS, Frama Check Sequence). Normalmente, FCS se conoce como comprobación de redundancia cíclica (CRC, Cyclic Redundancy Check), debido a las operaciones matemáticas subyacentes. FCS permite a las estaciones comprobar la integridad de las tramas recibidas. Todos los campos en el encabezado MAC y en el cuerpo de la trama se incluyen en la FCS. Cuando se envían tramas a la interfaz inalámbrica, se calcula la FCS antes de que dichas tramas se envíen sobre el enlace inalámbrico. Los receptores pueden calcular posteriormente la FCS a partir de la trama recibida y compararla con la FCS recibida. Si las dos secuencias coinciden, existe una probabilidad muy alta de que la trama no se haya dañado durante el tránsito.

2.4.2 Tipos de tramas

- **Trama de datos**

Las tramas de datos transportan datos de protocolo de nivel superior en el cuerpo de la trama. La estructura genérica de una trama de datos es la que se muestra en la figura 2.12. Los distintos tipos de tramas de datos pueden catalogarse según su función. Una categoría sería la de las tramas de datos utilizadas para el servicio basado en contención y otra las utilizadas para el servicio sin contención. Cualquier trama que aparezca en el período sin contención no se podrá utilizar nunca en una red IBSS. Otra posible división entre las tramas de datos, es las que transportan datos y las que ejecutan funciones de administración. La tabla 2.2 recoge la división en las tramas.

Tipo de trama	Servicio basado en contención	Servicio sin contención	Transporta datos	No transporta datos
Datos	✓	✓		
Datos+CF-Ack		✓	✓	
Datos+CF-Poll		Sólo AP	✓	
Datos+CF-Ack+CF-Poll		Sólo AP	✓	
Null	✓	✓		✓
CF-Ack		✓		✓
CF-Poll		Sólo AP		✓
CF-Ack+CF-Poll		Sólo AP		✓

Tabla 2.2: División de tramas de datos

Estos son los distintos subtipos de tramas de datos que se utilizan normalmente:

- **Datos**: este subtipo de tramas se transmite sólo durante los períodos de acceso basados en contención. Se trata de simples tramas con el único propósito de mover el cuerpo de la trama de una estación a otra.

- **Null**: este subtipo consiste en un encabezado MAC seguido por el FCS. En una red Ethernet tradicional, las tramas vacías serían una sobrecarga extraña. En las redes 802.11 las utilizan las estaciones móviles para informar al punto de acceso de los cambios producidos durante el estado de ahorro de potencia. Cuando las estaciones no están activas, el punto de acceso tiene que iniciar la introducción de tramas en el búfer para la estación que esta suspendida. Si la estación no tiene datos para enviar a través del sistema de distribución, puede utilizar una trama null con el bit de administración de potencia a 1.

Existen otros tipos de tramas de datos para su uso dentro del período de contención, tal y como se ha visto anteriormente en este mismo apartado. Sin embargo, el servicio sin contención no está ampliamente implantado. Algunas de estas tramas son: Datos+CF-ACK, Datos+CF-Poll, Datos+CF-ACK+CF-Poll, CF-Poll, CF-ACK. Algunas de ellas se han mencionado en apartados anteriores.

- **Tramas de control**

Las tramas de control ayudan a la entrega de datos. Administran el acceso al medio inalámbrico y proporcionan funcionen de fiabilidad de la capa MAC. Todas las tramas de control están formadas sólo por un encabezado y un campo FCS. Los subtipos de tramas de control más importantes que veremos a continuación son RTS, CTS, ACK y PS-Poll.

- **Petición de emisión (RTS, Request To Send)**: las tramas RTS se utilizan para obtener el control del medio para la transmisión de tramas de una determinada longitud denominada umbral RTS y que puede ajustarse en los parámetros de la tarjeta de red. El acceso al medio sólo se puede reservar para tramas unidifusión. Las tramas de difusión y multidifusión simplemente se transmiten. Como ya se comentó en el apartado anterior, en el campo duración de la cabecera se indica el tiempo que el remitente necesita reservar el medio para su transmisión. Esta trama sólo contiene 2 campos de direcciones: la dirección del transmisor y la del receptor.

- **Autorización de emisión (CTS, Clear To Send)**: el propósito de estas es responder a las tramas RTS. El remitente de una trama CTS utiliza la duración de la trama RTS como base para los cálculos de su propia duración. Esta trama sólo contiene un campo de dirección que es la dirección del receptor, que se copia directamente de la dirección del transmisor de la trama RTS.

- **Acuse de recibo (ACK, Acknowledgment)**: las tramas de acuse de recibo se utilizan para enviar los acuses de recibo positivos requeridos por la MAC y se utilizan en todas las transmisiones, incluyendo tramas precedidas por una conexión RTS/CTS y tramas fragmentadas. Esta trama, al igual que la CTS, solamente contiene un campo de dirección que es la del receptor.

- **Sondeo de ahorro de potencia (PS-Poll, Power Save Poll)**: este subtipo de trama ya se explicó en el apartado anterior de formato de trama. Cuando una estación móvil despierta del modo de ahorro de potencia, transmite una trama PS-Poll al AP para recuperar cualquier trama guardada en el búfer mientras se encontraba en modo de ahorro de potencia. En lugar de campo de duración, estas tramas incluye un ID de asociación el cual se explicó anteriormente. Este

tipo de tramas contienen 2 campos de direcciones: la dirección del transmisor y el BSSID.

- **Tramas de administración**

La administración es un componente importante en la especificación 802.11. En una red Ethernet la administración es muy sencilla. 802.11 desglosa el procedimiento en tres componentes. Las estaciones móviles en busca de conectividad primero tienen que localizar una red inalámbrica disponible para el acceso. En las redes de cable este paso sólo implica buscar la toma adecuada en la pared. A continuación, la red tiene que autenticar las estaciones móviles para establecer que la identidad autenticada permita conectarse a la red. En la red con cable esto es automático, la red con cable equivalente se proporciona a través de la propia red. Por último, las estaciones móviles tienen que asociarse a un AP para obtener acceso a la red troncal, un proceso equivalente a conectar el cable a la red con cable. Todos los subtipos de tramas de administración tienen el mismo encabezado. Las tramas de administración utilizan elementos de información, pequeños fragmentos de datos con una etiqueta numérica, para comunicar la información al resto de sistemas.

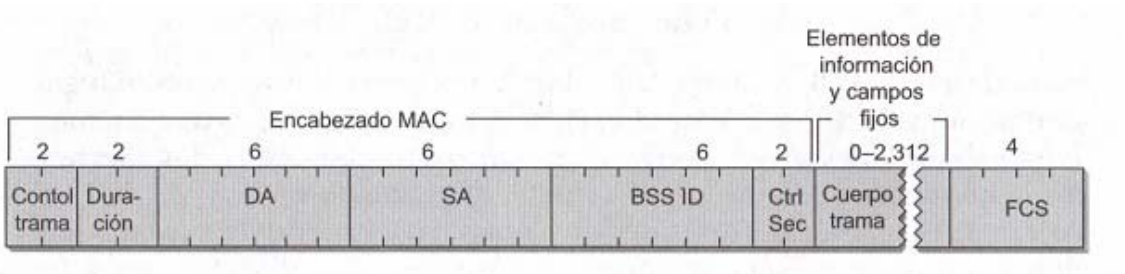

Figura 2.16 Trama de administración genérica

Este tipo de trama es bastante flexible. La mayoría de los datos contenidos en el cuerpo utilizan campos de longitud fija denominados campos fijos y campos de longitud variable conocidos como elementos de información. Cada elemento de información está etiquetado con un número de tipo y un tamaño y se entiende que un elemento de información de un tipo determinado tiene su propio campo de datos interpretado de una manera determinada.

Los campos fijos y los elementos de información se utilizan en el cuerpo de las tramas de administración para la comunicación. Existen diversos tipos de tramas de administración que se utilizan en distintas funciones de mantenimiento de la capa de enlace:

- **Beacon**: las tramas Beacon anuncian la existencia de una red y constituyen un elemento importante para muchas tareas de mantenimiento de la red. Se transmiten a intervalos regulares (intervalo beacon) para permitir a las estaciones móviles buscar e identificar una red así como parámetros de comparación para unirse a la misma. En una red infraestructura, el AP es el responsable de transmitir las tramas Beacon. El área en la que aparecen estas tramas define el área de servicio básico.

- **Petición de Prueba (Probe Request)**: las estaciones móviles utilizan las tramas de petición de prueba para examinar un área en busca de redes 802.11 existentes.

- **Respuesta de Prueba (Probe Response)**: si una petición de prueba encuentra una red con parámetros compatibles, la red envía una trama de respuesta de prueba. El AP que envió la última Beacon es el responsable de responder a las pruebas entrantes (red infraestructura).

- **Autenticación (Authentication)**: las estaciones se autentican utilizando una clave compartida e intercambiando tramas de autenticación. Pueden coexistir distintos algoritmos de autenticación. El campo número de algoritmo de autenticación se utiliza para la selección de algoritmo. El proceso de autenticación puede implicar seguir diversos pasos (dependiendo del algoritmo), por lo que existe un número de secuencia para cada trama en el intercambio de autenticación.

- **Petición de Asociación (Association Request)**: cuando las estaciones móviles identifican una red compatible y la autentican pueden intentar unirse a la red enviando una trama de petición de asociación. El campo información de capacidad se utiliza para indicar el tipo de red al que desea unirse la estación móvil. Antes de que el conjunto de acceso acepte una Petición de Asociación, comprueba que la información de capacidad, el SSID y las velocidades admitidas coinciden con los parámetros de la red.

- **Respuesta de Asociación (Association Response)**: cuando las estaciones móviles intentan asociarse a un punto de acceso, este responde con una trama de Respuesta de Asociación. Todos los campos de la trama son obligatorios. Como parte de la respuesta, el AP asigna un ID de asociación.

- **Disociación y Desautenticación (Disassociation and Deauthentication)**: las tramas de Disociación se utilizan para finalizar una relación de asociación y las tramas de Desautenticación, para finalizar una relación de autenticación. Ambas tramas incluyen un solamente campo fijo, el código de razón. Los campos de control son diferentes, porque se trata de dos tipos diferentes de tramas.

2.4.3 Transmisión de tramas y estados

Los tipos de tramas admitidos varían según el estado de las estaciones. Las estaciones pueden autenticarse/desautenticarse y asociarse/desasociarse. Estas dos variables se pueden combinar en tres estados admitidos en la jerarquía 802.11:

- Estado inicial: no autenticado y no asociado

- Autenticado pero todavía, no asociado

- Autenticado y asociado

Cada estado es un punto progresivamente superior en el desarrollo de una conexión 802.11. La figura 2.42 muestra un diagrama general de los estados para la transmisión de tramas 802.11.

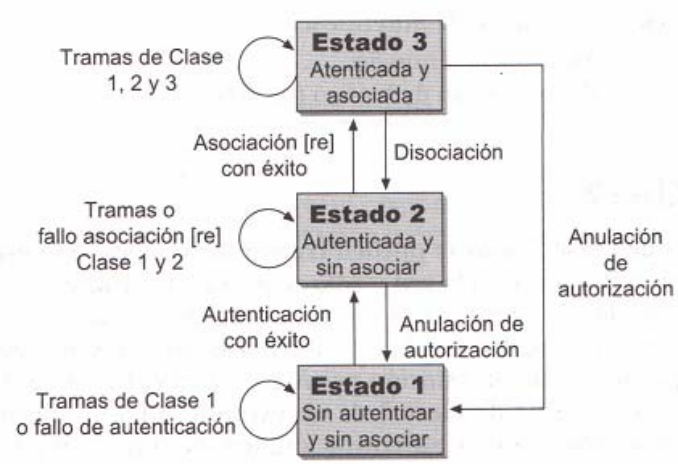

Figura 2.17: Diagrama general de estados en 802.11

Las tramas se dividen en distintas clases. Las tramas de clase 1 se pueden transmitir en el estado 1, las tramas de clase 1 y 2 en el estado 2 y las tramas de clase 1,2 y 3 en el estado 3.

- **Tramas de clase 1**

Las tramas de clase 1 se pueden transmitir en cualquier estado y se utilizan para proporcionar las operaciones básicas utilizadas por las estaciones. En la tabla 2.4 se puede ver las tramas de clase 1.

Control	Administración	Datos
Petición de envío (RTS)	Petición de prueba	Cualquier trama con ToDS y FromDS falsos (0).
Autorización de emisión (CTS)	Respuesta de prueba	
Acuse de recibo (ACK)	Beacon	
CF-End	Autenticación	
CF-End+CF-Ack	Anulación de autenticación	
	Mensaje de anuncio de indicación de tráfico (ATIM)	

Tabla 2.3: Tramas de clase 1

- **Tramas de clase 2**

Las tramas de clase 2 sólo se pueden transmitir cuando una estación se ha autenticado correctamente en la red y sólo se pueden utilizar en los estados 2 y 3. Las tramas de clase 2 administran asociaciones.

Control	Administración	Datos
Ninguno	Petición/Respuesta de asociación Petición/Respuesta de reasociación Disociación	Ninguno

Tabla 2.4: Tramas de clase 2

- **Tramas de clase 3**

Las tramas de clase 3 se utilizan cuando una estación se ha autenticado y asociado correctamente con un punto de acceso. Cuando una estación llega al estado 3, se le permite utilizar los servicios del sistema de distribución y llegar a destinos que se encuentran más allá de su punto de acceso.

Control	Administración	Datos
PS-Poll	Anulación de autenticación	Cualquier trama, incluyendo las que tienen establecidos los bits ToDS o FromDS.

Tabla 2.5: Tramas de clase 3

2.5 Extensiones de 802.11

2.5.1 Extensiones de capa física

- **802.11b**

Fue creada en 1999. En la actualidad esta fuera de uso. Alcanzaba una velocidad máxima de 11 Mbps. Trabajaba en la banda de 2,4 GHz. Se popularizó en el 2000, haciéndose la preferida para comunicaciones inalámbricas, debido a la bajada de precios de las tarjetas. Además la WECA aseguraba interoperatividad entre equipos 802.11b que tuvieran su certificado Wi-fi.

En este se desarrolla una nueva capa física basada en Secuencia directa de alto porcentaje (HR/DS, High-Rate Direct Sequence), gracias a la cual se consigue llegar a los 11 Mbps.

- **802.11a**

Fue creado también en 1999, aunque hasta 2001 no irrumpió en el mercado. Actualmente se sigue utilizando. Alcanza una velocidad de 54 Mbps. Trabaja en la banda de 5 GHz, la cual ser verá en el capítulo siguiente. Como trabaja en frecuencias más altas, permite mayores velocidades de transmisión que 802.11b. No obstante, trabajar a frecuencias más altas supone una reducción en el área de cobertura. No es compatible con 802.11b.

Este introduce la capa física de multiplexado de división de frecuencia ortogonal **(OFDM**, Orthogonal Frequency Division Multiplexing). OFDM no es una técnica nueva. Gran parte del trabajo fundamental se llevo a cabo a finales 1960.OFDM difiere de otras técnicas como CDMA en su solución. CDMA utiliza transformaciones matemáticas complejas en una sola portadora. OFDM codifica una sola transmisión en múltiples portadoras.

OFMD esta estrechamente relacionado con el sencillo multiplexado de división de frecuencia (FDM, Frequency Division Multiplexing). Ambos dividen el ancho de banda disponible en sectores denominados portadoras o subportadoras. OFDM incrementa el rendimiento utilizando diversas subportadoras en paralelo y realizando multiplexado de datos sobre el conjunto de las subportadoras.

FMD se utilizó ampliamente en los teléfonos móviles de primera generación como método de asignación del canal de radio. A cada usuario se le proporcionaba un canal exclusivo y se utilizaban bandas de protección para asegurarse de que la pérdida espectral de un usuario no causara problemas a los usuarios de los canales adyacentes. La figura 2.43 ilustra la solución FDM tradicional.

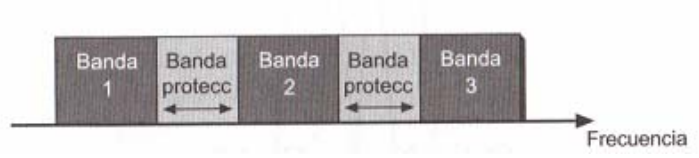

Figura 2.18: FDM tradicional

El problema de FMD tradicional es que las bandas de protección desperdician ancho de banda y por tanto, reducen la capacidad. Para evitar este desperdicio de la capacidad de transmisión, OFDM selecciona canales superpuestos pero que no interfieren entre sí. La figura 2.44 ilustra el contraste entre FDM y OFDM.

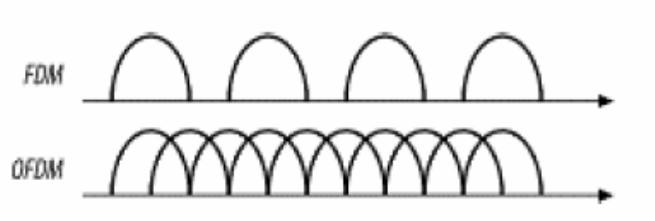

Figura 2.19: FDM vs OFDM

Se permiten las portadoras superpuestas porque las subportadoras se definen de forma que pueden distinguirse fácilmente. La capacidad para separar las subportadoras crea una relación matemática compleja denominada ortogonalidad.

En matemáticas, la palabra ortogonal se utiliza para describir elementos independientes. La ortogonalidad se puede ver mejor en el dominio de la frecuencia que busca una descomposición espectral una señal. OFDM funciona porque las frecuencias de las subportadoras se seleccionan de forma que en cada frecuencia de subportadora, el resto de subportadoras no contribuye a la forma de onda global. Una forma común de considerar la ortogonalidad se muestra en la figura 2.45. La señal se ha dividido en tres subportadoras. El pico de cada subportadora, mostrado por el punto de la parte superior, codifica los datos. El conjunto de subportadoras está perfectamente diseñado para ser

ortogonal. Se puede observar que en el pico de cada una de las subportadoras el resto de las subportadoras tiene amplitud cero.

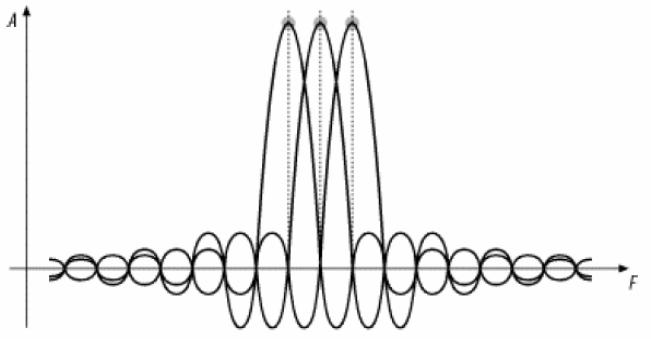

Figura 2.20: Ortogonalidad en el dominio de la frecuencia

OFDM recoge la señal codificada para cada subcanal y utiliza la transformada de Fourier rápida inversa (IFFT, Inverse Fast Fourier Transform) para crear una forma de onda compuesta a partir de la fuerza de cada subcanal. Los receptores OFDM pueden aplicar entonces FFT (Fast Fourier Transform) a una forma de onda recibida para extraer la amplitud de cada subportadora.

Igual que la capa física DS, la OFDM organiza el espectro en canales operativos. Cada canal de 20 MHz esta compuesto por 52 subportadoras, 4 de las cuales se utilizan como portadoras piloto mientras que las otras 48 se utilizan para transmitir datos. Las subportadoras se separan por 0,3125 MHz. Tal como se ilustra en la figura 2.46, los canales se numeran de -26 a 26. La subportadora 0 no se utiliza por motivo de procesamiento de señal.

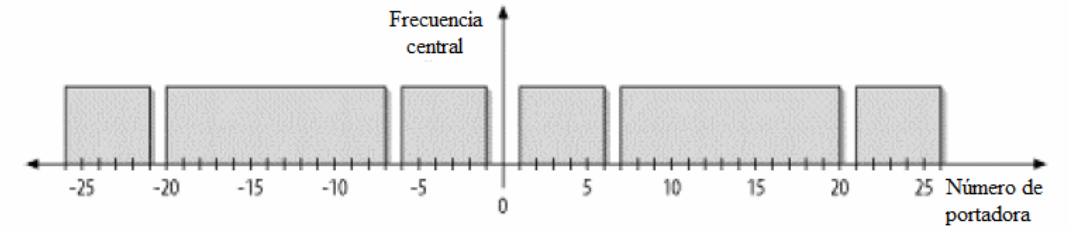

Figura 2.21: Estructura de un canal OFDM

Las subportadoras piloto se asignan a las subportadoras -21,-7, 7 y 21.

- **802.11g**

Es la extensión más popular actualmente. Fue creado en 2003. Permite una velocidad de 54 Mbps, igual que 802.11a, pero a diferencia de este trabaja en la banda de 2,4 GHz y es compatible con 802.11b. Combina las ventajas de los dos estándares anteriores, la velocidad de 802.11a y el alcance de 802.11b.

802.11g esta compuesto por diversas especificaciones de capa física en una sola. Añade una cláusula que comprende la capa física de velocidad extendida (ERP, Extended Rate PHY). Existen diversos tipos de ERP:

- **ERP-DSSS y ERP-CCK**: estos modos son compatibles hacia atrás con la especificación de secuencia directa original (1 y 2 Mbps) así como con las mejoras de 802.11b (5,5 y 11 Mbps).

- **ERP-OFDM**: este es el modo principal de 802.11g. Básicamente ejecuta 802.11a en la banda ISM (2,4 GHz) con algunos cambios menores para proporcionar compatibilidad hacia atrás. Admite las mismas velocidades que 802.11a.

- **ERP-PBCC**: esta es una extensión opcional para el estándar PBC proporcionado por 802.11b y proporciona velocidades de datos de 22 y 33 Mbps. Aunque forma parte del estándar, no está implantado en la mayoría de los conjuntos de chips más importantes del mercado y no se utiliza ampliamente.

- **DSSS-OFDM**: este es un esquema híbrido que codifica los paquetes utilizando encabezados DSSS y la codificación OFDM de la carga útil. Parte del motivo de desarrollar esta implantación era la compatibilidad hacia atrás. Es opcional y no esta ampliamente implantado.

802.11g adopta el plan de frecuencias de 802.11b (banda ISM de 2,4 GHz) por lo que sólo existen 3 canales no superpuestos para su uso.

- **802.11n**

Es el punto clave de este proyecto. Se dedicará el siguiente tema completo a hablar sobre este.

ESTÁNDARD	AÑO DE CREACIÓN	MODULACIONES	FRECUENCIAS	VELOCIDAD
802.11	1997	2GFSK, 4GFSK	2,4Ghz e IR.	1-2Mbps
802.11a	1999	BPSK, QPSK, 16QAM, 64QAM	5Ghz	Hasta 54Mbps
802.11b	1999	DBPSK, DQPSK, CKK	2,4Ghz.	Hasta 11Mbps
802.11g	2003	DBPSK, DQPSK, CCK, BPSK, QPSK, 16QAM, 64QAM.	2,4Ghz	Hasta 54Mbps
802.11n	2004	DBPSK, DQPSK, CCK y OFDM (BPSK/QPSK/16-QAM/64-QAM)	2,4 Ghz, 5Ghz	Hasta 600Mbps

Tabla 2.6: Estándares 802.11 de capa física

2.5.2 Extensiones de capa MAC

- **802.11e**

Fue creado debido al aumento de las aplicaciones en tiempo real (VoIP, streaming). Incluye nuevos mecanismos a nivel MAC para soportar servicios que requieren garantias de QoS. Este estándar define un nuevo mecanismo, conocido como **HCF (Hybrid Coordination Function)**, compatible con DCF y PCF. Este permite a las estaciones mantener múltiples colas de servicio y equilibrar el acceso al medio inalámbrico en favor de las aplicaciones que requieran una mejor calidad de servicio. HCF hace uso de dos métodos de acceso:

- **EDCA (Enhanced Distributed Channel Access)**: permite dar prioridad a distintos tipos de tráfico a la hora de conseguir el acceso al medio durante el período de contención. Supone una mejora a DCF. Dispone de 4 colas de servicio para soportar las distintas prioridades de usuario (8 prioridades de usuario se mapean a 4 colas). Cada cola funciona como una estación DCF independientemente y tiene sus propios parámetros de contención y backoff. Las prioridades relativas se consiguen configurando el tiempo que hay que esperar para acceder al canal y cambiando el tamaño de la ventana de congestión.

- **HCCA (HCF Controlled Channel Access)**: es un esquema de acceso al canal basado en consulta (polling). Se considera una mejora de PCF. El mecanismo HCCA se diseñó para permitir la provisión de Qos parametrizada, utilizando un coordinador híbrido (HC, Hybrid Coordinator) que gestiona la asignación del ancho de banda para transmitir en el medio inalámbrico. El HC tiene una prioridad de acceso mayor que las estaciones, algo necesario para que pueda asignar las oportunidades de transmisión a las estaciones en los períodos con o sin contención.

- **802.11f**

Este posibilita la interoperabilidad entre puntos de acceso dentro de una red WLAN. Esta extensión define el registro de AP dentro de una red y el intercambio de información entre APs cuando un usuario se traslada de un AP a otro, es decir, cuando realiza una itinerancia (handover). Utiliza el protocolo IAPP (Inter Access Point Protocol). Se puede utilizar en todos los estándares físicos 802.11a/b/g/n.

- **802.11i**

Este mejora la seguridad en la capa de enlace. Se creo para sustituir la ineficiencia del sistema de cifrado WEP. Hace uso de los protocolos WPA2 (Wi-fi Protected Access) y TKIP (Temporal Key Integrity Protocol). Se aplica a los estándares 802.11a/b/g.

- **802.11r**

Es parecido a la 802.11f. Garantiza la interoperatividad entre APs realizando la transición en menos de 50 ms, lo que mejora las comunicaciones VoIP, ya que podemos mantener una comunicación sin cortes perceptibles. Su principal característica es permitir a la red que establezca los protocolos de seguridad que identifican a un

dispositivo en el nuevo AP antes de que abandone el actual y se pase a el. Esta característica es conocida como Fast Basic Service Set Transition.

- **802.11k**

Actualmente los dispositivos se conectan al AP con señal más potente, pero esto no conduce necesariamente a una mejor conexión, ya que podemos colapsarlo si es una ubicación con muchos dispositivos. Este estándar mide los recursos de radio frecuencia (carga del canal, canal bloqueado, historia del ruido), y comparte esa información entre los APs y los demás dispositivos para que puedan elegir al AP que les dará mejor conexión.

- **802.11d**

Esta permite la conexión a redes inalámbricas sin importar el país o la región en la que se encuentre el dispositivo. Es capaz de adaptar la capa física según los requerimientos normativos de la ubicación (canales, frecuencias).

ESTÁNDARD	MEJORA / ACTUALIZACIÓN / CORRECIÓN	UTILIDAD
802.11e	Soporte para servicios que requieren QoS.	Aplicaciones en tiempo real, VoIP.
802.11f	Permite realizar Handover (interoperabilidad entre AP's).	Movilidad entre red con vatios AP's
802.11i	Mejora la seguridad en las conexiones inalámbricas.	Seguridad WPA2, TKIP.
802.11r	Permite interoperabilidad entre AP's a velocidades elevadas.	Mantener aplicaciones en tiempo real (VoIP) sin cortes cuando cambiamos de AP.
802.11k	Mide recursos RF y comparte información con los demás dispositivos.	Mejor rendimiento de nuestra red.
802.11d	Adapta la capa física según requerimientos de la ubicación.	Conexión a redes inalámbricas de diferentes países o región.

Tabla 2.7: Estándares 802.11 de capa MAC

CAPÍTULO 3: 802.11n

3.1 Introducción

802.11n surgió a finales de 2002 y tardó exactamente siete años desde su comienzo hasta su ratificación. Al igual que todas las extensiones IEEE 802, empezó como un grupo de estudio. El grupo de estudio de High Throughput se fundó para investigar sobre la implementación de una capa física 802.11 que pudiera proporcionar velocidad de 100 Mbps en la capa MAC.

Una de las reglas antiguas que había para WLAN es que el Throughput en la capa MAC sería la mitad de la velocidad de transmisión. En 802.11b, con unos 11 Mbps de velocidad de transmisión, el Throughput no superaba los 5-6 Mbps. En 802.11a/g, donde la velocidad de transmisión era de 54 Mbps, el Througtput resultante era de unos 25-30 Mbps. Por eso unos de los objetivos de 802.11n era incrementar la eficiencia del protocolo para que los incrementos en la velocidad de transmisión no estuvieran limitados por la sobrecarga del protocolo.

El primer gran logro en el desarrollo de 802.11n fue el segundo borrador (draft). Después de resolver unos 12000 comentarios sobre el borrador 1.0, a principios de 2007 salió el borrador 2.0, mucho más completo que el primero. Por esa misma época Wi-fi Alliance lanzó un programa de certificación para llevar a cabo la certificación del entonces emergente estándar 802.11n. Este programa fue un éxito rotundo.

Finalmente, en Septiembre de 2009 802.11n fue ratificado.

3.2 Capa física 802.11n

Para incrementar la velocidad de una red se pueden utilizar dos técnicas. La primera de ellas consiste en aumentar la tasa de datos. Esta técnica es la que se ha llevado a cabo en todos los estándares 802.11 para mejorar la velocidad de la red. La segunda de ellas consiste en aumentar la eficiencia del protocolo para transmitir más bits en un período de tiempo dado. Aunque 802.11n usa ambas técnicas, la mayoría de la ganancia viene dada por el aumento en la tasa de datos. El motor de esta técnica es MIMO.

3.2.1 MIMO

Antes de MIMO, 802.11 utilizaba un único flujo (stream) de datos. El transmisor usaba una antena y el receptora otra. El enlace de transmisión en dispositivos pre-802.11n puede ser descrito en términos de sus dos componentes. Se llamaba Single-Input porque el receptor usaba una sola antena, y Single-Output porque el transmisor usaba una sola antena también. Entonces, el sistema de comunicación completo se llamaba Single-Input/Single-Output (SISO). Entre dos estaciones en un sistema SISO fluye un conjunto de datos llamado **stream**.

En MIMO, en lugar de tener sólo un transmisor y un receptor en el sistema, ambos lados tienen varios transmisores y receptores. Esto quiere decir que el receptor tiene varias entradas y el transmisor tiene varias salidas. Además, cada antena se controla independientemente de las demás. Una antena puede transmitir o recibir un conjunto de bits completamente diferentes a los que manda/recibe otra, al mismo tiempo y en el mismo canal.

En la figura 3.1 se puede ver una comparación simplificada entre un sistema MIMO y un SISO. En un sistema SISO una única antena activa trasmite a otra antena activa. Aunque un sistema SISO podría tener varias antenas, solamente una puede estar activa para una transmisión dada. En un sistema MIMO todas las antenas están activas simultáneamente. Cada antena transmisora manda su propio stream de datos a través del canal radio y cada antena receptora recoge su propio stream de datos.

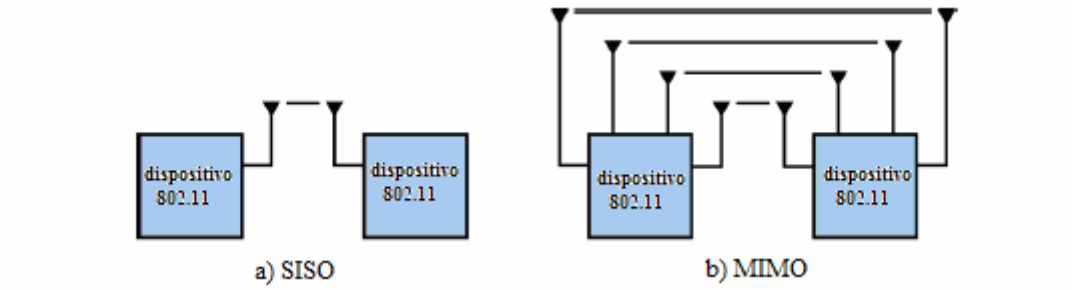

Figura 3.1: Transmisión SISO vs transmisión MIMO

En la figura 3.1 se muestra el caso más simple, en el que un stream de datos viaja entre pares de antenas, sin embargo no siempre es así. De hecho, hay dos técnicas básicas de transmisión con múltiples antenas en MIMO:

- **Multiplexación espacial (Spatial Multiplexing, SM)**

En ambientes 802.11, el fenómeno de **multipath** [24] ha causado grandes problemas. Multipath es un fenómeno de propagación que produce que 2 o más réplicas de la misma señal lleguen a la antena receptora al mismo tiempo o con unos nanosegundos de diferencia unas de otras. Entre los efectos negativos del multipath pueden incluirse pérdida de amplitud de la señal y corrupción de datos. Sin embargo, los sistemas 802.11n MIMO se aprovechan de este efecto. En la figura 3.2 se puede ver un ejemplo de multipath.

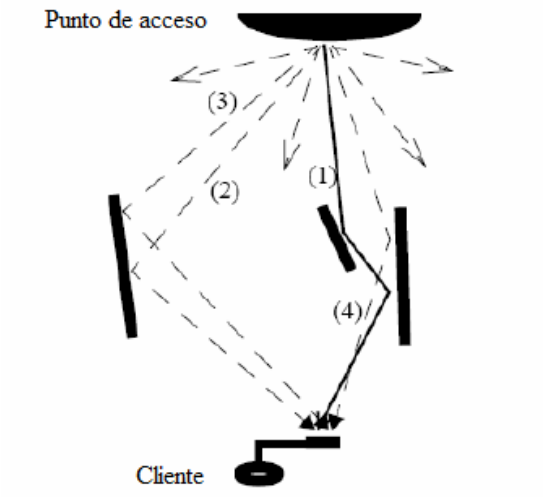

Figura 3.2: Efecto multipath

MIMO transmite varias señales de radio al mismo tiempo y se aprovecha del efecto multipath. En esta técnica, cada señal de radio se transmite por su propia antena. Cada una de estas señales de radio independientes se conoce como **stream espacial (spatial stream)**, y cada uno de los streams contiene datos diferentes a los contenidos en los demás. Además, cada stream viaja por un camino diferente, debido a que las antenas transmisoras se sitúan con una separación de al menos un medio de la longitud de onda de la señal que transmiten. El hecho de que varios streams sigan caminos diferentes debido a la separación entre las antenas transmisoras se conoce como **multiplexación espacial**. Cuando se usa SM, tanto el emisor como el receptor deben participar, en otras palabras, ambos deben implementar MIMO. El beneficio de enviar streams de datos independientes es que el Throughput aumenta notablemente.

La figura 3.3 muestra una situación que supuso un gran problema para los administradores de redes 802.11a/b/g. En la figura, el transmisor y el receptor tienen 2 caminos. Uno es el camino de línea de visión entre ellos. En el otro, la señal rebota en la pared y se desfasa con respecto a la señal del primero. Si los caminos se usan para transmitir el mismo conjunto de bits, interferirán destructivamente y no habrá señal en el receptor. Sin embargo, los sistemas MIMO explotan la existencia de varios caminos consiguiendo el doble de Throughput. Ya que los caminos no interfieren entre sí, se pueden mandar transmisiones independientes por cada uno de ellos y de esta forma multiplicar el Throughput.

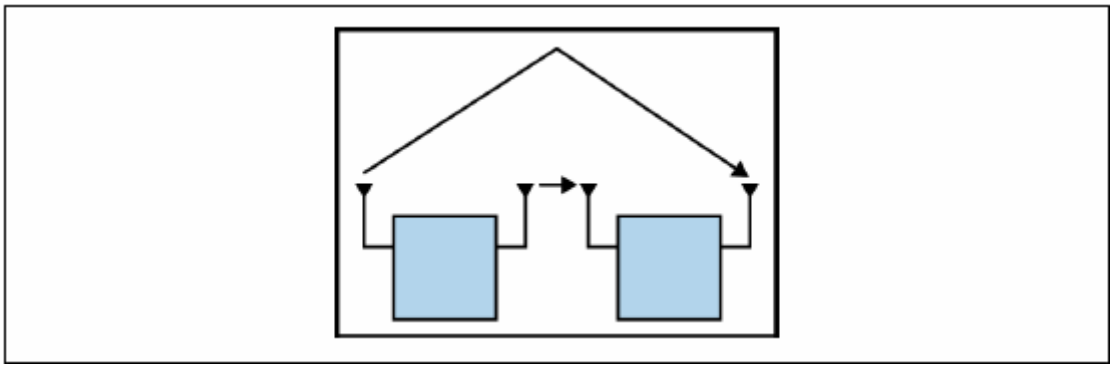

Figura 3.3: Streams espaciales con multipath

El grado de semejanza entre los caminos se llama **correlación**. Los caminos de la figura 3.3 se dice que no están correlados, porque son totalmente diferentes. En el proceso de diseño de dispositivos, los diseñadores de radio frecuencia pasan bastante tiempo pensando sobre la colocación de las antenas para minimizar la correlación entre ellas.

Cada camino en un sistema 802.11n es aproximadamente equivalente a una transmisión individual de un sistema 802.11a/g. 802.11n soporta hasta un máximo de 4 streams espaciales. En la figura 3.4 se puede ver un ejemplo en el que un AP 3 x 3 MIMO transmite 3 streams independientes a un cliente 3 x 3 MIMO. Cada señal saliente se divide en tantos streams como antenas haya, antes de ser mandada. Después cada stream se transmite por una antena diferente. En el receptor, cada antena recibe uno de los streams transmitidos, y estos se recomponen para formar la señal original.

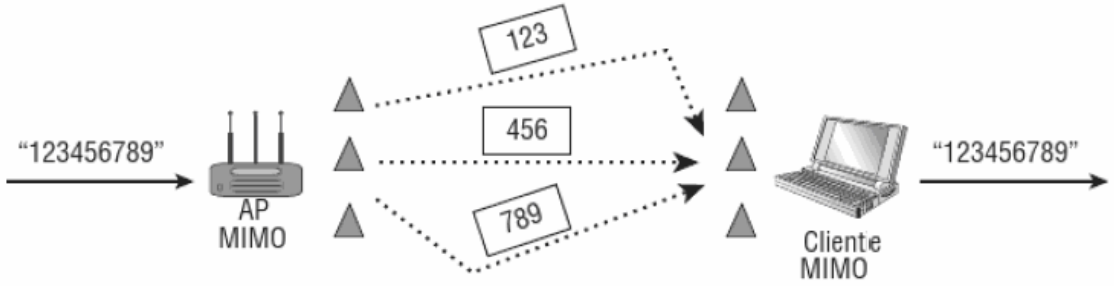

Figura 3.4: Transmisión con multiplexación espacial

En el ejemplo de la figura 3.4, todos los streams podrían tener la misma modulación **(equal modulation)**, o por el contrario, podrían usar diferentes modulaciones **(unequal modulation)**. Un sistema en el que todos los streams tengan la misma modulación conseguiría mayor Throughput que otro que use diferentes modulaciones para sus streams.

Otra forma de ver como benefician los streams espaciales, es comparar la eficiencia espectral. Es muy fácil incrementar la velocidad de una tecnología de red mediante el aumento de los recursos de utilización. En 802.11 el recurso clave que necesita ser optimizado es el espectro de radio. En la tabla 3.1 se compara las distintas capas físicas 802.11 en términos de eficiencia espectral, la cual se define como el número de bits que se pueden transmitir por unidad de espectro.

802.11 PHY	Eficiencia Espectral (Mbps/MHz)
802.11 secuencia directa/salto de frecuencia	0,09
802.11b	0,5
802.11a/g	2,7
802.11n (Canal de 20 MHz y MCS 15)	6,5
802.11n (Canal de 40 MHz y MCS 15)	6,75

Tabla 3.1: Comparación de eficiencia espectral

Entre el sistema operativo y la antena, hay un interfaz radio que tiene que llevar a cabo varias tareas. Cuando se está transmitiendo, las tareas principales son, por un lado, realizar la transformada inversa de Fourier para pasar la señal del dominio de la frecuencia al dominio del tiempo y después, amplificar la señal. En el lado del receptor el proceso está invertido. En cuanto la señal llega a la antena, un amplificador incrementa la potencia de esta para que se pueda trabajar con ella. A continuación se realiza la transformada de Fourier para extraer las subportadoras. En un interfaz 802.11 estos componentes esta unidos y forma lo que se conoce como **circuito de procesado de capa física (radio chain)**. En un dispositivo SISO (802.11a/g), solamente es necesario un transformador de Fourier y un amplificador en la cadena del transmisor. Sin embargo, un sistema 802.11n necesita varios circuitos de procesado de capa física para transmitir bits independientes a través de cada camino. En la figura 3.5 se muestra un diagrama de bloque simplificado de un interfaz radio 802.11n con 4 circuitos de procesado de capa física. Construir un interfaz radio que cuente con varios de estos es una tarea mucho más compleja que hacerlo sólo con uno.

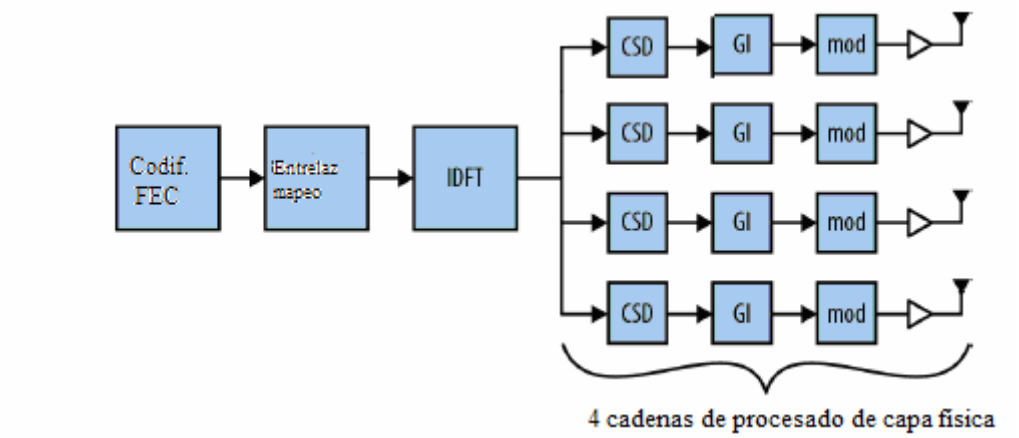

Figura 3.5: Diagrama de bloque de interfaz radio

Tener múltiples circuitos de procesado de capa física puede incrementar la velocidad, pero también tiene un efecto negativo. Los bloques que realizan la transformada de Fourier usan matemática compleja y tienen unos elevados requerimientos de potencia. Los amplificadores también tienen un consumo alto. El consumo de potencia depende directamente de la anchura del canal y de los streams espaciales que se utilicen en la comunicación.

- **Diversidad espacial (Spatial Diversity)**

La **diversidad de antenas** a veces se confunde con la multiplexación espacial de MIMO. En diversidad de antenas, hay realmente un único transceptor. Varias antenas pueden alimentar al transceptor, pero a la hora de transmitir o recibir se debe

seleccionar una de ellas. Además, la diversidad de antenas es una técnica de compensación del efecto multipath, al contrario que la diversidad espacial que se aprovecha de este efecto. En recepción, normalmente se elige la antena que recibe la señal más fuerte. Respecto a la transmisión, a menudo se utiliza siempre la misma antena (antena primaria).

802.11n además de realizar SM, lleva a cabo técnicas de diversidad de antenas más avanzadas que las anteriores, tanto en transmisión como en recepción. Respecto a la **diversidad en transmisión**, algunos dispositivos 802.11n MIMO incorporan una funcionalidad llamada **STBC (Space-Time Block Coding)**, que requiere varias cadenas de radio para transmitir un solo stream espacial. Difundiendo el stream espacial a través de varios caminos, es posible incrementar la redundancia en transmisión para compensar las pérdidas de transmisión. Sin embargo esta redundancia se consigue a costa de reducir el número de streams espaciales y por tanto la velocidad de transmisión.

Muchos dispositivos 802.11n implementan **MRC (Maximal Ratio Combining)**. MRC es una técnica de **diversidad en recepción** que trabaja combinando la información recibida por cada antena. Para ello, toma las componentes más altas de la señal recibida en cada antena. MRC esta ampliamente implantado en puntos de acceso de entornos empresariales y ofrece beneficios a todos los dispositivos, incluyendo la recepción de transmisiones realizadas desde dispositivos 802.11a/g. En la figura 3.6 podemos ver un ejemplo gráfico de cómo trabaja MRC con una estación que no implementa MIMO. Según [25] se consigue un aumento teórico del rango de recepción cuando se usa MRC.

Figura 3.6: Recepción AP utilizando MRC

La nomenclatura [26] para referirse a un dispositivo MIMO es **T x R: S**. La **R** se refiere al número de antenas que pueden funcionar en recepción. La **T** identifica el número de antenas que pueden utilizarse para transmisión. La **S** se refiere al máximo número de streams con los que puede operar el dispositivo. Normalmente, T y R tienen el mismo valor, ya que cada antena requiere su propia cadena de procesado de capa física, independientemente de su función (transmitir, recibir o ambas). Sin embargo, existen excepciones como la de la figura 3.7. En esta se puede ver dos dispositivos 802.11n, uno 2 x 3 y el otro 3 x 3. Notar que ambos dispositivos tienen 3 circuitos de procesado de capa física. Sin embargo, la diferencia entre ambos es que el dispositivo 3 x 3 tiene 3 transmisores, mientras que el 2 x 3 tiene solamente 2. De la figura 3.6 se puede deducir que cada circuito de procesado de capa física puede contar con un transmisor y un receptor o sólo con uno de ellos.

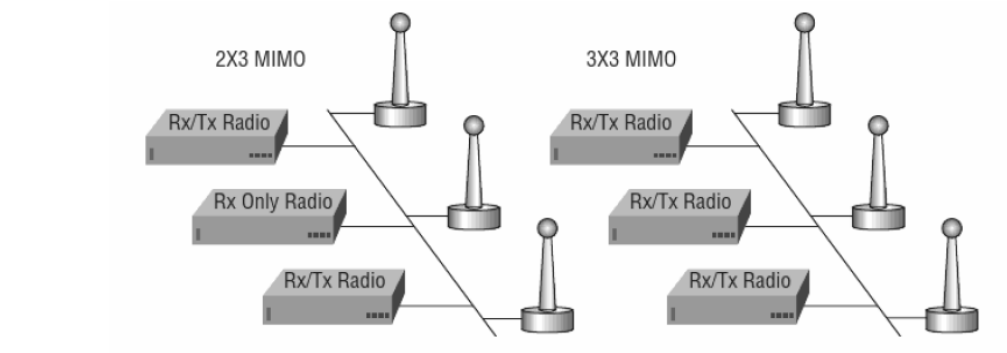

Figura 3.7: Sistemas MIMO 2x3 y 3x3

Para que un dispositivo opere correctamente, T y R deben ser al menos igual que S. En SM cada antena va a transmitir un stream independiente, entonces normalmente T es igual a R y a S. Con diversidad espacial puede que 2 o más antenas transmitan o reciban un mismo stream espacial. En este caso, T y R pueden ser mayores que S. Lo que no es posible, es que haya más streams que antenas.

3.2.2 Canales

Aunque las especificaciones de 802.11 definen una gran cantidad de canales, especialmente en la banda de 5 GHz, sólo algunos de ellos están disponibles para uso, según la regulación del país donde se despliega la red. 802.11n opera en las bandas de 2,4 usada por 802.11b/g así como en la banda de 5 GHz utilizada por 802.11a. En ambos casos, 802.11n reutiliza la numeración establecida anteriormente. La figura 3.8 ilustra la última información disponible sobre regulación en la banda de 5 GHz. Los canales son identificados por los números de canal de IEEE. Los bloques indican si un canal de 20 o 40 MHz está disponible en cada canal o pareja de canales.

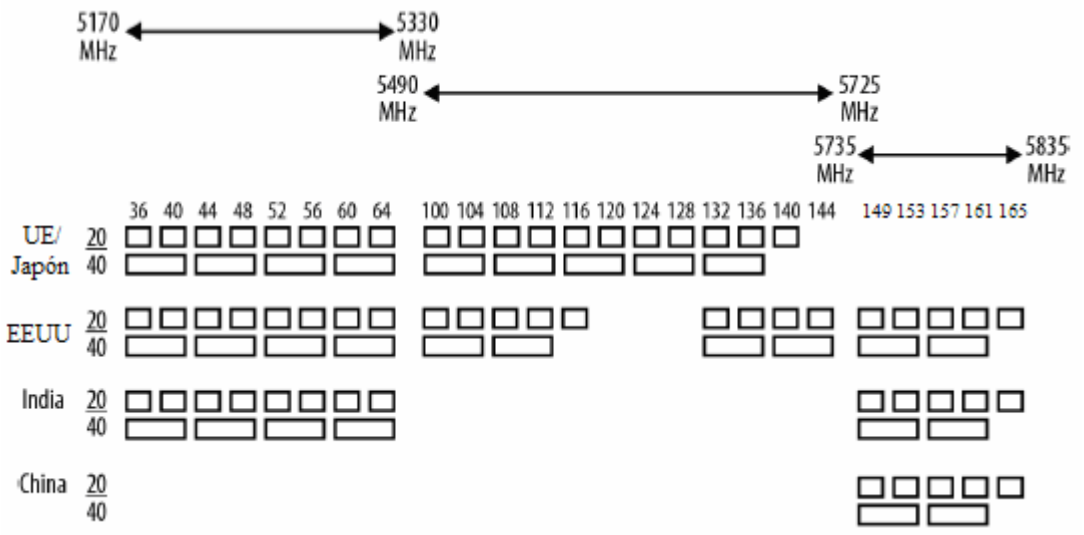

Figura 3.8: Canales permitidos en la banda de 5 GHz

En la figura 3.9 se puede ver un esquema de la estructura de la banda de 5 GHz, también conocida como banda UNII. Esta se divide en distintas subbandas: UNII-1, UNII-2, UNII-2 Extendida y UNII-3. A diferencia de la banda ISM de 2,4 GHz, en este caso no hay superposición entre canales.

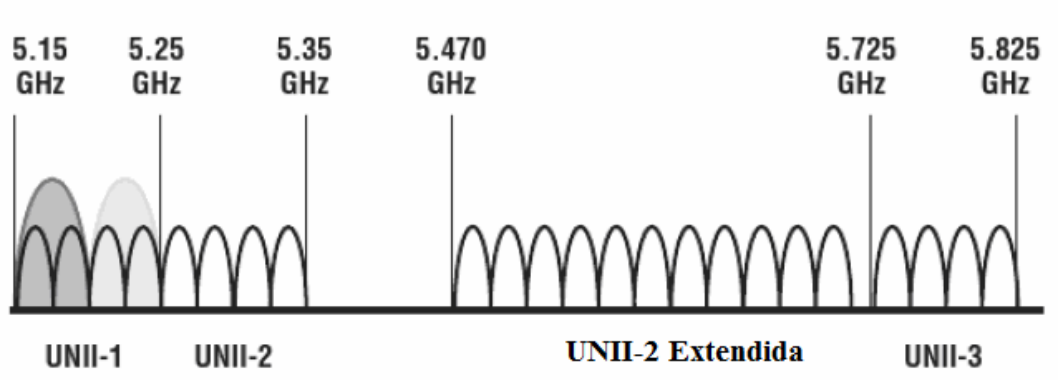

Figura 3.9: Canalización 5 GHz

La estructura de un canal en 802.11n es prácticamente igual que en 802.11a/g. Ambos están basados en OFDM, el cual se explicó en el capítulo anterior.

802.11n ofrece 2 funcionalidades para incrementar la utilización del espectro de radio. Una de ellas fue conservar el canal de 20 MHz usado anteriormente por 802.11 pero añadirle subportadoras que no se usaban en 802.11a/g para mejorar la eficiencia espectral, como se muestra en la figura 3.10. A pesar de que 802.11n añade 4 subportadoras, incrementado el Throughput alrededor de un 8%, no es necesario añadir ninguna portadora piloto. Las portadoras piloto se utilizan para calibración dinámica entre emisor y receptor y son una forma de sobrecarga. El incremento que consigue MIMO en la eficiencia de transmisión hace que aumente también la eficiencia de operación de las portadoras piloto.

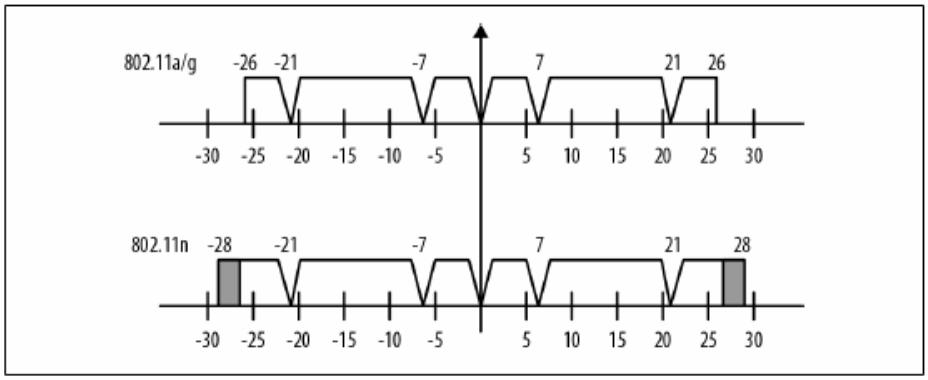

Figura 3.10: Comparación estructura canal 802.11a/g vs 802.11n

El segundo cambio hecho por 802.11n, es el soporte para canales más anchos, de 40MHz. Aunque el estándar describe muchas formas de operación de los canales de 40 MHz, hasta ahora la técnica más común es **Channel Bonding**, que consiste en usar dos canales adyacentes de 20 MHz que son tratados como uno solo. Los canales se identifican como primario y secundario. En la figura 3.11 se puede ver un esquema de esta técnica en la banda de 5 GHz.

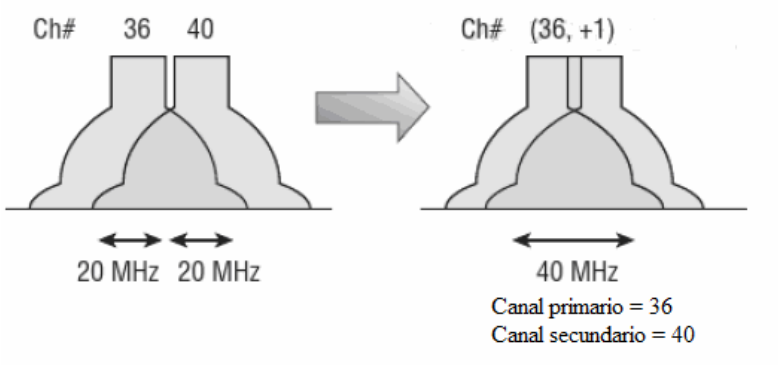

Figura 3.11: Channel bonding

Los canales de 40 MHz consiguen más del doble de Throughput si se comparan con los estrechos canales tradicionales, porque el formato de los canales de 40 MHz hace que se reduzca la sobrecarga del canal. Las portadoras piloto no transmiten datos de protocolos de capas más altas, sin embargo, son una sobrecarga necesaria en OFDM. 802.11n dobla la anchura del canal de 20 a 40 MHz, pero sólo incrementa el número de portadoras piloto en un medio como describe la tabla 3.2 (de 4 a 6 subportadoras piloto).

Estándar PHY	Rango de subportadoras	Subportadoras piloto	Subportadoras (total/datos)
802.11a/g	-26 a +26	-21, -7, +7, +21	Total: 52, Usables: 48
802.11n, 20 MHz	-28 a +28	-21, -7, +7, +21	Total: 56, Usables: 52
802.11n, 40 MHz	-57 a +57	-53, -25, -11, +11, +25, +53	Total: 114, Usables: 108

Tabla 3.2: Parámetros de canal 802.11a/g vs 802.11n

Aprovechando el incremento en la eficiencia de las portadoras piloto en un sistema MIMO, la eficiencia espectral aumenta un 4%.

En la figura 3.12 se pueden ver las diferencias entre un canal de 20 MHz en 802.11n y otro de 40 MHz.

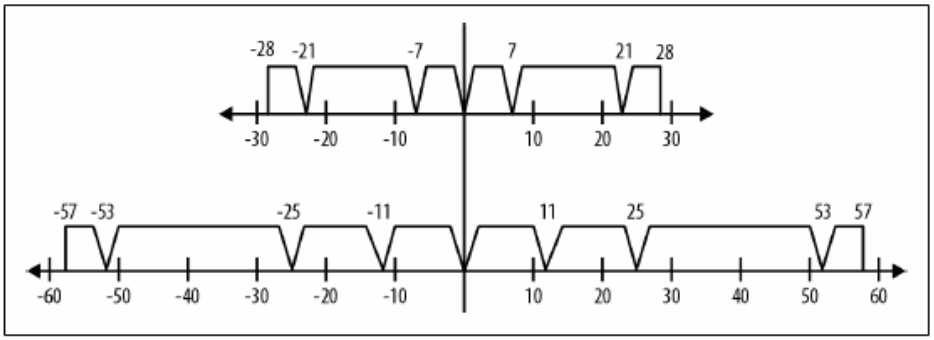

Figura 3.12: Comparación de canales 802.11n 20 MHz vs 40 MHz

Algunos dispositivos 802.11n están diseñados para trabajar en la banda de 2,4 GHz (conocidos como 802.11ng). Otros por el contrario trabajan en la de 5 GHz (802.11na). Por último también los hay que trabajan en ambas bandas (dual-band o 802.11agn).

Por último, decir que, los canales de 40 MHz se ajustan perfectamente a la banda de 5 GHz porque hay un total de 24 canales que pueden ser juntados en pares, como se puede ver en la figura 3.8. Sin embargo los canales de 40 MHz en la banda ISM de 2,4

GHz no se ajustan bien. Aunque hay 14 canales disponibles, sólo hay 3 canales disponibles sin solapamiento. Cuando se juntan canales de 20 MHz para formar uno de 40 MHz en la banda ISM, cualesquiera 2 canales de 40 MHz se solaparán, tal y como se puede ver en la figura 3.13.

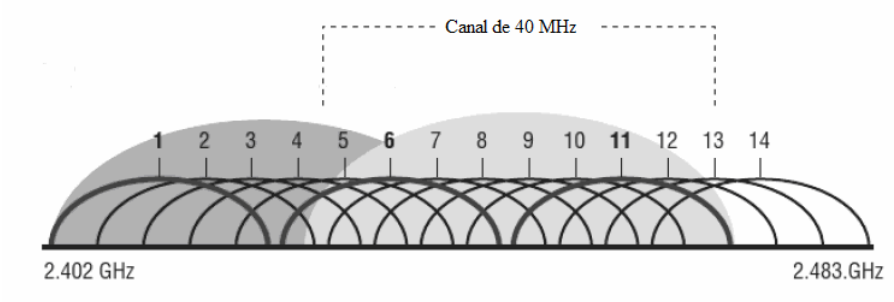

Figura 3.13: Channel Bonding en la banda ISM

3.2.3 Intervalo de guarda (Guard Interval, GI)

El intervalo de guarda es un período de tiempo entre símbolos OFDM que se utiliza para preparar al sistema ante la llegada tardía de símbolos a través de caminos largos. En escenarios multipath, los símbolos viajan por diferentes caminos y por eso algunos símbolos pueden llegar más tarde. Un nuevo símbolo podría llegar al receptor antes de que un símbolo, el cual ha llegado tarde, haya sido recibido completamente. Este efecto se conoce como Interferencia Intersimbólica (ISI).

Aunque no es una regla en el sentido legal, una buena regla usada por los diseñadores OFDM es que el intervalo de guarda debe ser igual a 4 veces el máximo retraso de expansión multipath (multipath delay spread), siendo este la diferencia de tiempo entre varios caminos de una misma señal. Cuando 802.11a fue diseñado, los diseñadores usaron un valor conservador de 200 ns para el retraso de expansión, y siguiendo la regla anterior fijaron el GI a 800 ns. Después la experiencia ha demostrado que en la mayoría de entornos interiores casi nunca se llega a los 100 ns de retraso de expansión y a menudo suele estar comprendido entre los 50 y 75 ns. Por eso para conseguir un rendimiento mayor del enlace radio, 802.11n incluye una opción para intervalo de guarda corto, el cual se reduce a 400 ns. El éxito del GI corto depende de la expansión multipath. En general, la interferencia multipath es peor cuando hay importantes reflexiones debido a metales.

El resto de parámetros OFDM se quedan igual. La velocidad global se incrementa porque la parte del tiempo de símbolo dedicada a la transmisión de datos es todavía de 3,2 µs, pero cada símbolo es más corto. La longitud total de cada símbolo se reduce de 4 µs con el GI largo a 3,6 (3,2 µs + 0,4 µs) con el GI corto, reduciendo de esta forma la sobrecarga de OFDM en un 10% como se ilustra en la figura 3.14.

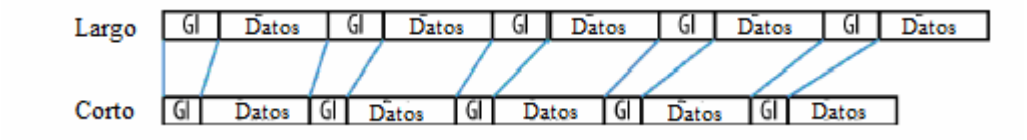

Figura 3.14: Comparación GI largo vs GI corto

3.2.4 Códigos FEC (Forward Error Correction)

802.11n define el uso de dos códigos FEC para proporcionar protección a las tramas cuando son mandadas. Los códigos FEC toman los datos que deben ser transmitidos y los codifica con bits redundantes para permitir la corrección de errores en el receptor. Estos códigos disminuyen la eficiencia del canal al requerir la transmisión de bits adicionales, pero permite que se puedan recuperar muchos errores en el receptor. Si la pérdida de eficiencia debido a los bits redundantes es menor que la pérdida de eficiencia producida por las retrasmisiones, entonces el código FEC mejora la eficiencia del canal.

Un parámetro clave en los códigos FEC es la **tasa de codificación (code rate)**, que describe el número de bits de sobrecarga sobre el número total de bits. Por ejemplo, un código con una tasa R=1/2 transmite un bit de sobrecarga por cada 2 bits.

802.11n continúa con el uso de un código convolucional tal como se hace en OFDM y además añade soporte opcional para **Low-Density Parity Check (LDCP)** [27] y [28]. En casi todos los aspectos, el código convolucional usado en 802.11n es idéntico al usado en 802.11a/g. La única diferencia, es que al aumentar la velocidad efectiva de la capa física, 802.11n añade una tasa de codificación adicional R=5/6.

3.2.5 Modulation and Coding Scheme (MCS)

En 802.11n las velocidades de datos están ahora definidas por un esquema de codificado y modulación (Modulation and Coding Scheme, MCS). En 802.11a/g, las velocidades se definían en base a la modulación y estaban comprendidas entre los 6 y 54 Mbps. Sin embargo, en 802.11n las velocidades de datos dependen de varios factores: la modulación, el número de streams espaciales, la anchura del canal, el intervalo de guarda y el coding rate. Cada MCS puede suponer una variación del número de streams espaciales, la modulación y el coding rate. Dentro de cada MCS hay distintas velocidades en función del ancho de banda del canal y el intervalo de guarda. 802.11n define 77 MCS diferentes. Los 32 primeros con equal modulation y el resto con unequal modulation. Actualmente, la mayoría de los productos solamente soportan equal modulation. Unequal modultation es útil cuando un stream espacial está más dañado que los demás. Cuando se transmite con **beamforming** [29] las operaciones matemáticas que se utilizan para separar los streams espaciales podrían producir que algunos de ellos tuvieran una SNR significativamente diferente a la de otros, lo que requeriría que algunos streams se transmitieran usando una modulación más conservadora. Las modulaciones usadas son BPSK, QPSK, 16-QAM y 64-QAM. En las tablas 3.3 se muestran los 32 MCS posibles con sus diferentes parámetros y las velocidades de datos permitidas para cada MCS, para equal modulation.

MCS	Nº de streams espac	MODULACIÓN	Coding rate	$N_{BPSCS(iss)}$	N_{ES}		N_{SD}		N_{CBPS}		N_{DBPS}		Tasa de datos (GI = 800ns)		Tasa de datos (GI = 400ns)	
					20MHz	40MHz	20MHz	40MHz	20MHz	40MHz	20MHz	40MHz	20MHz	40MHz	20MHz	40MHz
0	1	BPSK	1/2	1	1	1	52	108	52	108	26	54	6.5	13.5	7.2	15.0
1	1	QPSK	1/2	2	1	1	52	108	104	216	52	108	13.0	27.0	14.4	30.0
2	1	QPSK	3/4	2	1	1	52	108	104	216	78	162	19.5	40.5	21.7	45.0
3	1	16-QAM	1/2	4	1	1	52	108	208	432	104	216	26.0	54.0	28.9	60.0
4	1	16-QAM	3/4	4	1	1	52	108	208	432	156	324	39.0	81.0	43.3	90.0
5	1	64-QAM	2/3	6	1	1	52	108	312	648	208	432	52.0	108.0	57.8	120.0
6	1	64-QAM	3/4	6	1	1	52	108	312	648	234	486	58.5	121.5	65.0	135.0
7	1	64-QAM	5/6	6	1	1	52	108	312	648	260	540	65.0	135.0	72.2	150.0
8	2	BPSK	1/2	1	1	1	52	108	104	216	52	108	13.0	27.0	14.4	30.0
9	2	QPSK	1/2	2	1	1	52	108	208	432	104	216	26.0	54.0	28.9	60.0
10	2	QPSK	3/4	2	1	1	52	108	208	432	156	324	39.0	81.0	43.3	90.0
11	2	16-QAM	1/2	4	1	1	52	108	416	864	208	432	52.0	108.0	57.8	120.0
12	2	16-QAM	3/4	4	1	1	52	108	416	864	312	648	78.0	162.0	86.7	180.0
13	2	64-QAM	2/3	6	1	1	52	108	624	1296	416	864	104.0	216.0	115.6	240.0
14	2	64-QAM	3/4	6	1	1	52	108	624	1296	468	972	117.0	243.0	130.3	270.0
15	2	64-QAM	5/6	6	1	1	52	108	624	1296	520	1080	130.0	270.0	144.4	300.0
16	3	BPSK	1/2	1	1	1	52	108	156	324	78	162	19.5	40.5	21.7	45.0
17	3	QPSK	1/2	2	1	1	52	108	312	648	156	324	39.0	81.0	43.3	90.0
18	3	QPSK	3/4	2	1	1	52	108	312	648	234	486	58.5	121.5	65.0	135.0
19	3	16-QAM	1/2	4	1	1	52	108	624	1296	312	648	78.0	162.0	86.7	180.0
20	3	16-QAM	3/4	4	1	1	52	108	624	1296	468	972	117.0	243.0	130.0	270.0
21	3	64-QAM	2/3	6	1	2	52	108	936	1944	624	1296	156.0	324.0	173.3	360.0
22	3	64-QAM	3/4	6	1	2	52	108	936	1944	702	1458	175.5	364.5	195.0	405.0
23	3	64-QAM	5/6	6	1	2	52	108	936	1944	780	1620	195.0	405.0	216.7	450.0
24	4	BPSK	1/2	1	1	1	52	108	208	432	104	216	26.0	54.0	28.9	60.0
25	4	QPSK	1/2	2	1	1	52	108	416	864	208	432	52.0	108.0	57.8	120.0
26	4	QPSK	3/4	2	1	1	52	108	416	864	312	648	78.0	162.0	86.7	180.0
27	4	16-QAM	1/2	4	1	1	52	108	832	1728	416	864	104.0	216.0	115.6	240.0
28	4	16-QAM	3/4	4	1	2	52	108	832	1728	624	1296	156.0	324.0	173.3	360.0
29	4	64-QAM	2/3	6	1	2	52	108	1248	2592	832	1728	208.0	432.0	231.1	480.0
30	4	64-QAM	3/4	6	1	2	52	108	1248	2592	936	1944	234.0	486.0	260.0	540.0
31	4	64-QAM	5/6	6	1	2	52	108	1248	2592	1040	2160	260.0	540.0	288.9	600.0
32	1	BPSK	1/2	1	1	1	—	48	—	48	—	24	—	6.0	—	6.7

Tabla 3.3: MCS equal modulation

La operación con un stream (MCS 0-7) es obligatoria para todas las estaciones. La operación con 2 streams (MCS 8-15) es obligatoria para puntos de acceso. La operación con 3 y 4 streams (MCS 16-31) es opcional para todos los dispositivos. Los AP con 3 streams dominan sobre los de 4. Al MCS 32 se le conoce como High Throughput Duplicate Mode. Este usa un canal de 40 MHz y un único stream espacial a una tasa de 6 Mbps. Es un modo muy conservador para conseguir una alta fiabilidad. Normalmente se utiliza en redes de gran escala. Los MCS del 33 al 76 se usan para unequal modulation.

Los parámetros de la tablas 3.3 que no se han explicado son:

- **N_{BPSCS}**: número de bits codificados por subportadora OFDM (6 para 64-QAM, 4 para 16-QAM. 2 para QPSK y 1 para BPSK).
- **N_{ES}**: número de codificadores FEC utilizados (1 para R<300 Mbps y 2 para R>300 Mbps).
- **N_{SD}**: número de subportadoras OFDM de datos (52 para 20 MHz y 108 para 40 MHz como se explicó anteriormente).
- **N_{CBPS}**: número de bits codificados por símbolo OFDM (total de todos los stream espaciales). Se obtiene sumando para cada stream, el producto de N_{SD} x N_{BPSCS}.
- **N_{DBPS}**: número de bits de datos por símbolo OFDM. Se obtiene multiplicando N_{BPSCS} por el coding rate.

3.2.6 Adaptación de enlace (Link Adaptation, LA)

Un problema importante en las redes WLAN 802.11 es, que los canales sufren pérdidas variables en el tiempo, debido a la movilidad y a las interferencias, conduciendo a un rendimiento pobre en determinadas situaciones. Por tanto, LA es un recurso fundamental para dispositivos 802.11.

LA se refiere al conjunto de técnicas en donde la modulación, el coding rate y otros parámetros de transmisión de una señal, se cambian sobre la marcha para adaptarse a las condiciones cambiantes del canal.

En este caso, en 802.11n, los parámetros que cambian son la modulación, el coding rate y el número de streams espaciales utilizados. En general, los algoritmos de LA en 802.11n eligen un MCS adecuado (cambiando los parámetros anteriores), para incrementar el Throughput del sistema en diferentes medios.

El tipo de algoritmo de LA utilizado, depende del driver que controla el interfaz inalámbrico del dispositivo. En este caso se utiliza el driver **Ath9k** [30], que es un driver de licencia libre (open source) para sistemas operativos Linux y dispositivos con chipsets Atheros [31]. El algoritmo de LA implementado en Ath9k es conocido como **ONOE** [32].

En ONOE se definen 4 tasas de datos (r_0, r_1, r_2, r_3) y 4 números máximos de intentos de transmisión (c_0, c_1, c_2, c_3), asociados a cada una de las tasas de datos, para cada trama. La tasa de datos r_0 se usa para el primer intento de transmisión de una trama y para los siguientes $c_0 - 1$ retransmisiones. Si la transmisión sigue fallando, el transmisor intenta transmitir a una tasa de datos r_1 durante c_1 veces, después a una tasa r_2 durante c_2 veces y por último a una tasa r_3 durante c_3 veces, antes de descartar la trama. Concretamente, los valores del número máximo de intentos de transmisión son c_0=4 y c_1= c_2= c_3= 2. Con respecto a las tasas de datos, r_3 es la más baja y r_0 la más alta. Por tanto, a medida que aumenta el subíndice, disminuye la tasa de datos. r_3 siempre se fija a la mínima tasa de datos. Por otro lado r_1 y r_2 se eligen a partir de r_0, eligiendo las siguientes tasas disponibles por debajo de esta. Para seleccionar la tasa r_0 en cada instante, el algoritmo asocia un número de créditos a la tasa r_0 actual. Para ser más precisos, si menos del 10% de las tramas transmitidas fallan durante el último período, cuya duración por defecto es de un segundo, entonces el número de créditos se incrementa en una unidad. Esto es lo mismo, que decir que el contador de créditos se incrementa en una unidad si el PER (Packet Error Rate), es menor del 10% en el último período. En cualquier otro caso, el número de créditos se reduce en una unidad. La tasa de datos r_0 sólo se incrementa si el número de créditos esta por encima del umbral (10 por defecto). Si el PER es mayor del 50% durante el último período de observación, entonces la tasa de transmisión disminuye inmediatamente. En cuanto se cambia de tasa, el contador de créditos y las estadísticas sobre las tasas de datos se resetean.

3.2.7 Modos PLCP

Como en las anteriores capas físicas de 802.11 (aunque no se explicara en el capítulo 2), la especificación 802.11n define una trama de capa física usando PLCP. En 802.11n PLCP soporta 3 modos diferentes:

- **Non-HT mode**

Todos los dispositivos tienen que soportar este modo, el cual permite la compatibilidad con dispositivos 802.11a/b/g. Ninguna funcionalidad de 802.11n está disponible en este modo. El formato de trama para este modo es exactamente igual que el de 802.11a o 802.11g. Alguna documentación se refiere a el como modo legado (legacy mode), porque opera acorde con las mismas reglas que las especificaciones anteriores.

- **HT mixed mode (HT-MM)**

Este modo también debe ser soportado por todos los dispositivos 802.11n. Este sólo tiene compatibilidad con 802.11a/g, pero la parte de High Throuhput no puede ser decodificada por un dispositivo 802.11a/g.

- **HT greenfield mode (HT-GF)**

Este ultimo modo no es compatible con ninguna otra corrección de 802.11, por ello es conveniente utilizarlo solamente en áreas donde todos los dispositivos son compatibles con 802.11n. El modo HT greenfield consigue un pequeño aumento en le rendimiento con respecto al modo mixto, ya que la cabecera PLPC es 8 µs más corta. No es obligatorio y no es muy frecuente su implementación en dispositivos 802.11n.

En la figura 3.15 se puede ver el formato de trama PLCP de los distintos modos.

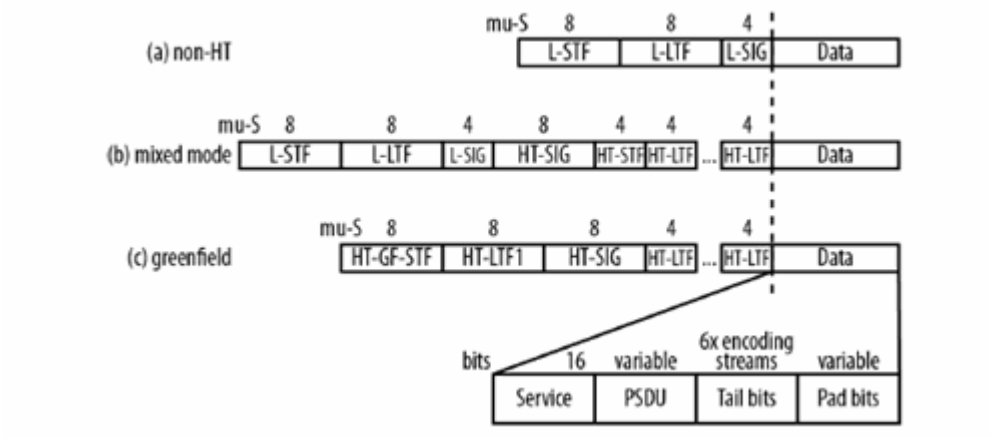

Figura 3.15: Formatos de trama PLCP 802.11n

3.3 Capa MAC

Antes de 802.11n, la capa MAC se veía desde el punto de vista del 50% de eficiencia. Cuando las tasas de datos eran relativamente bajas el coste de la ineficiencia en la MAC era manejable. Por ejemplo, perder la mitad de una red de 1 Mbps es sólo 500 Kbps. A medida que las velocidades de transmisión aumentaron, las pérdidas se hicieron más y más significativas. 802.11n desarrolla varias funcionalidades para recuperar una parte de esta ineficiencia. Centrarse en la eficiencia ha merecido la pena: bajo ciertas condiciones, 802.11n puede tener una eficiencia de hasta el 70%.

Aunque no está relacionado directamente con la eficiencia de transmisión, la capa MAC de 802.11n amplia las capacidades de ahorro de potencia de 802.11 [33]. Las tarjetas 802.11n tienen un alto consumo de potencia. Esto no es una gran desventaja para dispositivos con grandes reservar de batería, como un portátil, sin embargo, en pequeños dispositivos tales como teléfonos y tablets, reducir el consumo de potencia es esencial.

3.3.1 Cambios en las tramas

La trama de datos sólo se cambia ligeramente en 802.11n. En la figura 3.16 se ilustra el formato de una trama de datos modificada por 802.11n. Los cambios más importantes realizados en las tramas de datos son el incremento de tamaño, la adición del subcampo opcional de control HT, y el hecho de que el campo de control de QoS se utiliza ampliamente en los bloques de confirmación. La carga de la capa MAC se incrementa alrededor del cuádruple y puede ser usada para agregar tramas de capas superiores para mejorar la eficiencia.

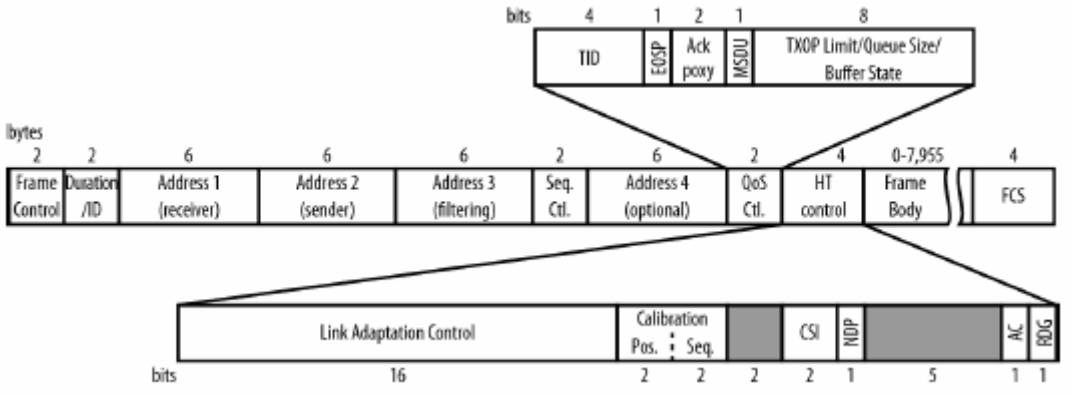

Figura 3.16: Formato trama de datos 802.11n

Las tramas de administración que forman parte de una red 802.11n incluyen un nuevo elemento de información denominado Capacidades HT (HT Capabilities), el cual se muestra en la figura 3.17. Cuando una estación incluye **el elemento de información de Capacidades HT (HT Capabilities IE)** en sus transmisiones, está declarando que es un dispositivo 802.11n. HT Capabilities IE está incluido en las tramas Beacon para que las estaciones puedan saber si una red soporta 802.11n. Las estaciones a su vez, insertan HT Capabilities IE en sus tramas de petición de prueba (Probe Request) para tratar de localizar redes 802.11n y anunciar a los AP que es compatible con 802.11n. Este elemento de información también se incluye en las tramas de asociación y reasociación.

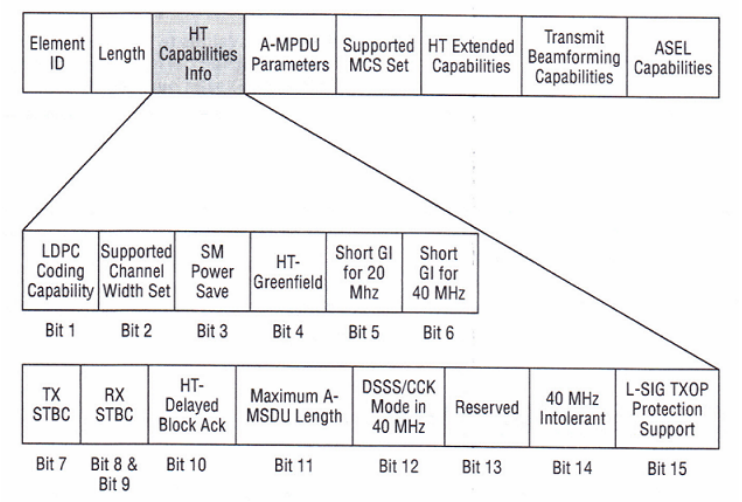

Figura 3.17: Elemento de información de capacidades HT

El **elemento de información de Operación HT (HT Operation IE)**, mostrado en la figura 3.18, también es importante. Este se incluye en las transmisiones desde un punto de acceso para informar a los dispositivos clientes del estado actual de la red. Se incluye en las tramas Beacon, en las de respuesta de prueba y en las de respuesta de asociación.

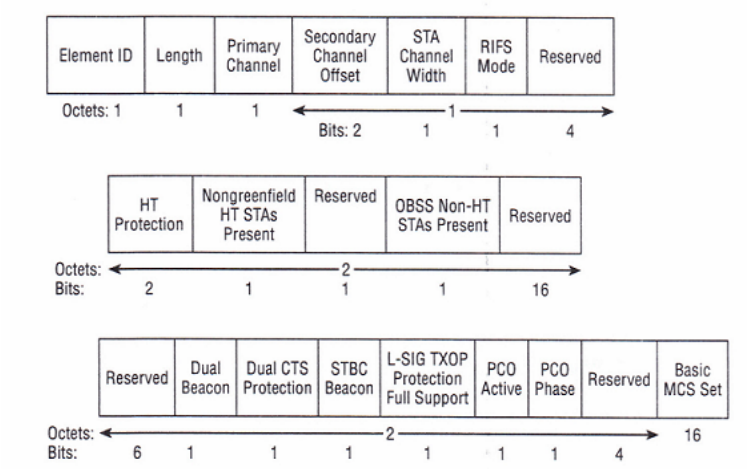

Figura 3.18: Elemento de información de operación HT

3.3.2 Mejoras en la eficiencia del tiempo de emisión

La idea clave detrás de la agregación es que el proceso de acceso al medio inalámbrico en 802.11 es tiempo perdido. Formando una trama agregada, un dispositivo 802.11 puede pasar más tiempo transmitiendo. De hecho, de esta forma reparte el tiempo de acceso al medio entre tramas que llevan varios paquetes de capas superiores. 802.11n define dos tipos de tramas: la **trama agregada de protocolo MAC de unidad de datos (Aggregate MAC Protocol Data Unit, A-MPDU)** y la **trama agregada de servicio MAC de unidad de datos (Agrégate MAC Service Data Unit, A-MSDU)**. Las 2 tramas se diferencian según de la pila de protocolos en la que se realiza la agregación.

- **A-MPDU**

La forma más común de agregación de trama es A-MPDU, la cual se muestra en la figura 3.18. Esta es una forma relativamente simple de agregación, en la que el paquete de capa superior (IP) que podría ser transmitido normalmente, se le pone una cabecera MAC y se manda "back to back". En la figura 3.19(a), se puede ver como al paquete IP se le añade una cabecera MAC y una cola, y la trama (desagregada) se pone en una trama de capa física para su transmisión. Por otro lado, en la figura 3.19(b) se muestra el proceso de agregación. A cada paquete IP se le da su propia cabecera. Ya que todos estos paquetes individuales se pondrán juntos en el proceso de agregación, se les conoce como subtramas A-MPDU en este punto. En el proceso de agregación, el delimitador MAC se inserta para ayudar al receptor a extraer las subtramas individuales. Cada subtrama A-MPDU tiene su cabecera 802.11 y su FEC y además cada A-MPDU se rellena para que este alineada y no haya problemas en la transmisión física. Ya que cada subtrama tiene su propia cabecera MAC, la encriptación se aplica individualmente a cada subtrama. Entonces cada trama tiene su propia secuencia de comprobación de trama. Gracias a esto, un error en una subtrama solo afectará a esa subtrama, mientras que las otras podrán ser recuperadas. Todas las subtramas dentro de una A-MPDU deben ser destinadas a la misma dirección de receptor en el enlace inalámbrico, pero podrían tener múltiples direcciones de destino.

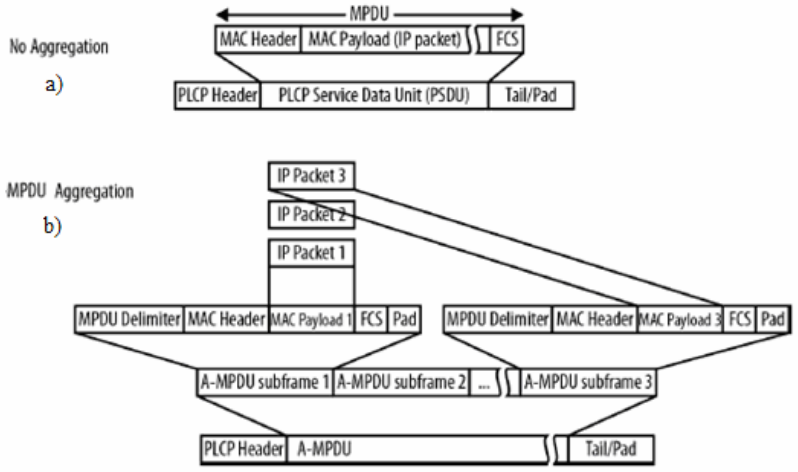

Figura 3.19: Agregación A-MPDU

A-MPDU está ampliamente implantado entre los dispositivos del mercado. El programa de certificación de 802.11 de Wi-fi Alliance requiere soporte para la recepción de tramas A-MPDU. El soporte para la transmisión de estas es opcional. A pesar de su amplia implantación en dispositivos, no es sencillo ver en un analizador de redes si una trama MPDU ha sido transmitida. Muchos analizadores se introducen en un nivel de la capa de protocolos en el cual la trama agregada ya ha sido separada en subtramas y cada una de estas subtramas está disponible para ser analizada por separado. Una trama A-MPDU está limitada en tamaño solamente por la trama PLCP 802.11n, de esta forma pueda llegar hasta 65535 bytes.

- **A-MSDU**

Además de la agregación justo antes de entregar los bits a la capa física para su transmisión, es posible empaquetar múltiples paquetes de capa superior en una única trama MAC. Construir una trama A-MSDU requiere más soporte software, ya que los driver de red deben tomar varios paquetes de capa superior y agregarlos en un carga de una sola trama MAC. El formato de la trama A-MSDU se puede ver en la figura 3.19. La figura 3.20 ilustra como un paquete de capa superior se pone dentro de una subtrama A-MSDU y esas subtramas a su vez se ponen todas juntas en una única trama MAC. A diferencia de A-MPDU, este tipo de agregación contiene solamente una trama MAC.

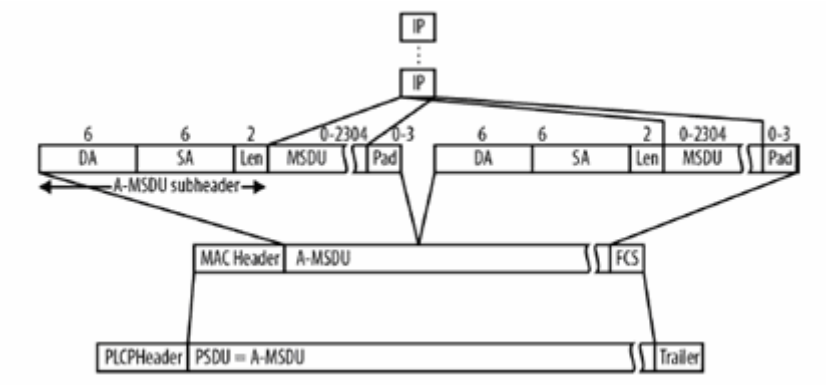

Figura 3.20: Agregación A-MSDU

Una trama A-MSDU tiene un tamaño máximo de 7995 bytes, ya que todas las tramas agregadas deben encajar en la carga de una trama 802.11n

Los dos tipos de agregación se pueden combinar. Cada una de las subtramas A-MPDU puede estar formada por una trama A-MSDU, como se muestra en la figura 3.21. En la figura, la última subtrama en la trama A-MPDU está formada por 2 tramas A-MSDU.

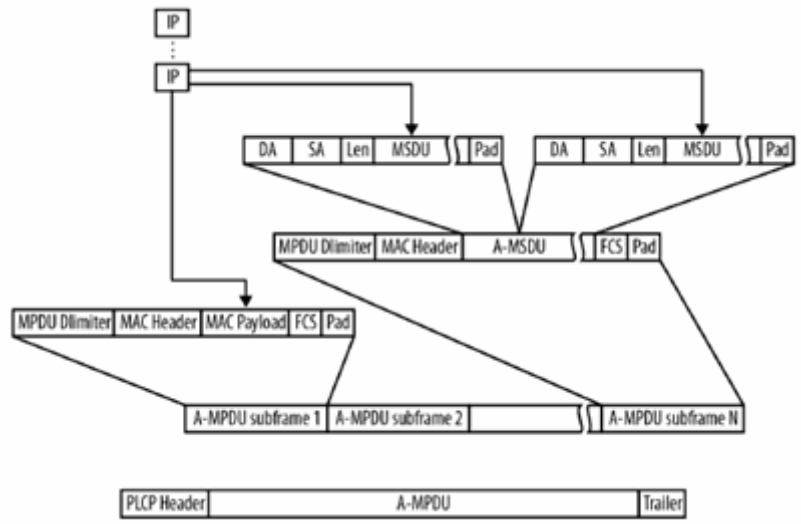

Figura 3.21: A-MPDU formada por A-MSDU

- **Bloque de confirmación (Block Acknowledgment)**

En la versión original de 802.11, tal y como se vio en el capitulo anterior, cada trama requería una confirmación positiva. Cada transmisión no se completaba hasta que su correspondiente confirmación no hubiera llegado. El tráfico en la red se transmite normalmente en forma de ráfagas. Por ejemplo, un usuario leyendo páginas webs mandará una petición, recibirá un conjunto de paquetes que transportan la página web solicitada y después la red estará ociosa mientras el usuario lee la página. El concepto original de la MAC 802.11 requería que cada trama enviada al receptor fuera confirmada por separado, como se muestra en la figura 3.22(a). Las funcionalidades de calidad de servicio en 802.11e introdujeron el bloque de confirmación (abreviado en inglés como Block ACK), el cual permite al emisor enviar un conjunto de tramas y confirmarlas todas juntas de una sola vez. Conceptualmente, Block ACK trabaja de forma similar a la opción de ACK selectivo en TCP. Se definieron dos formas de Block ACK en 802.11e y se mantuvieron en 802.11n, y ambas se ilustran en la figura 3.22(b). Con la forma de Block ACK inmediato, el emisor transmite una serie de tramas y espera una confirmación inmediatamente, mientras que con la forma de Block ACK retrasado, el receptor puede mandar su confirmación más tarde.

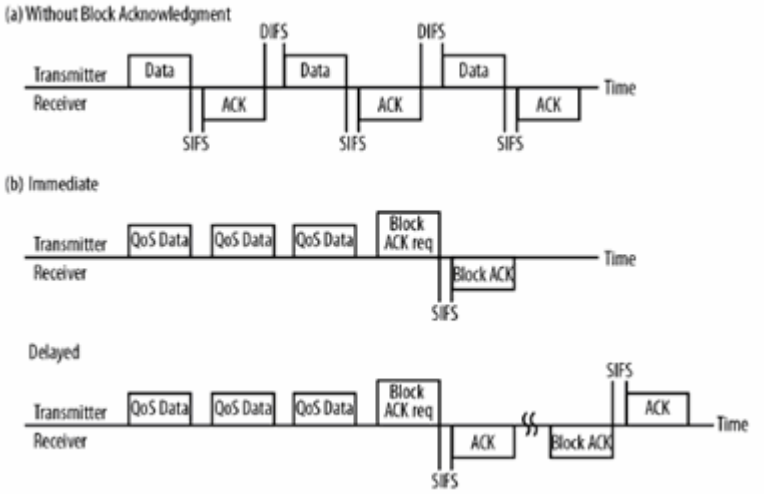

Figura 3.22 Transmisiones con Block ACK

En la figura 3.22(b), las tramas de datos con calidad de servicio se mandan sin haber recibido ninguna confirmación positiva. En lugar de requerir que cada trama sea confirmada individualmente, el intercambio de una única trama Block ACK gestiona todas las confirmaciones. La eficiencia del medio se mejora, ya que el intercambio con la trama Block ACK es más rápido que las con confirmaciones individuales.

La agregación de tramas funciona bien con Block ACK, ya que una trama agregada está formada por varias tramas individuales. Block ACK inicialmente era opcional, pero la ganancia de eficiencia que se consigue cuando se une con agregación de tramas era tan buena que el soporte para Block ACK se hizo obligatorio para todos los dispositivos 802.11n.

Para solicitar un Block ACK, una estación manda una trama de **petición Block ACK (Block ACK Request)**, la cual se muestra en la figura 3.23. El campo más importante de esta es el campo comprimido.

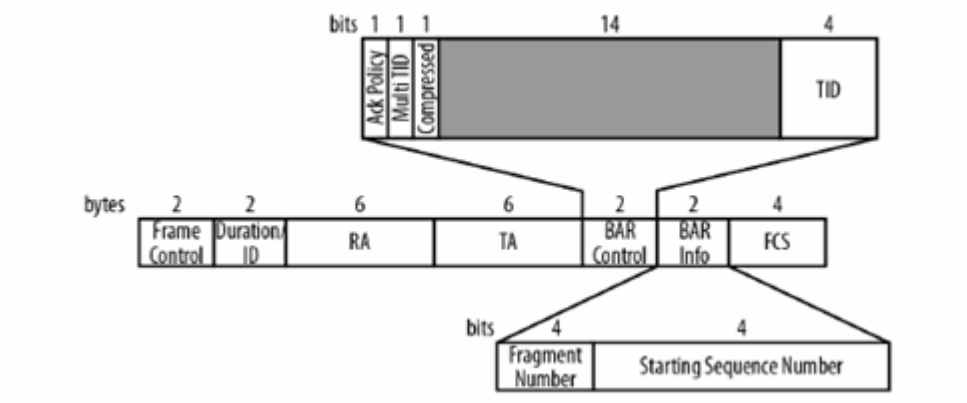

Figura 3.23: Trama de petición Block ACK

Para enviar un bloque de confirmación, el receptor usa la trama comprimida Block ACK, que se muestra en la figura 3.24. Una única trama Block ACK se puede usar para confirmar hasta 64 MSDU.

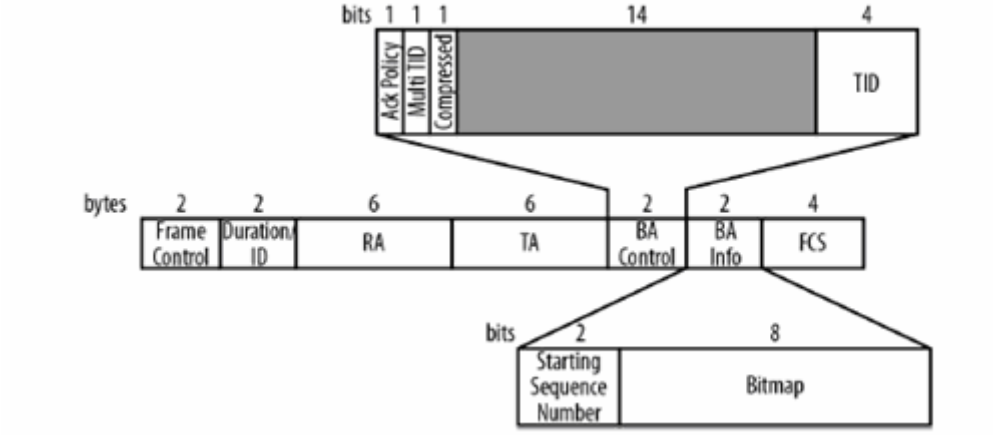

Figura 3.24: Trama comprimida de Block ACK

- **Espacio reducido entre tramas (Reduced Interframe Space, RIFS)**

Las funciones de acceso al canal básicas de 802.11 introducen espacios entre transmisiones como un método para establecer el acceso al medio. La idea principal del método de mediación de espacio entre tramas, es que las transmisiones de alta prioridad, como confirmaciones, tengan un período de espera menor. Antes de 802.11n, el espacio más corto entre tramas era el espacio corto entre tramas (short interframe space, SIFS), y se usaba para completar el intercambio de tramas, permitiendo responder tramas para ser transmitidas inmediatamente siguiendo sus disparadores (triggers). Por ejemplo, una confirmación puede ser transmitida después de esperar sólo un SIFS. De la misma manera, una trama CTS transmitida inmediatamente siguiendo a una trama RTS necesita esperar solo un SIFS antes de acceder al medio.

802.11n define un nuevo espacio entre tramas, llamado tiempo reducido entre tramas (Reduced Interframe Space, RIFS). Tiene una función equivalente a la del SIFS y se usa en donde SIFS se podría usar. Sin embargo, es más corto, como se muestra en la tabla 3.4. No define un nuevo nivel de prioridad. Su único propósito es ser usado en lugar de SIFS para aumenta la eficiencia. Obviamente no esta disponible en dispositivos 802.11a/b/g y de hecho, no se debe usar cuando hay dispositivos 802.11a/b/g

representes en la red porque podría evitar que estos leyeran el campo de duración en la cabecera de trama y actualizaran la información de acceso al medio.

La mayoría de los dispositivos no transmiten usando RIFS porque la eficiencia que se consigue es relativamente pequeña. Sin embargo, todos los dispositivos con la certificación Wi-fi n deben tener la habilidad de recibir tramas transmitidas después de un RIFS.

Banda	Valor SIFS (µs)	Valor de RIFS (µs)
2,4 GHz	10	2
5 GHz	16	2

Tabla 3.4: Longitud de espacio entre tramas

3.3.3 Seguridad

La seguridad en 802.11n está basada en la arquitectura que se estandarizó en 802.11i pero con pequeñas variaciones. Sólo hay 2 pequeños cambios con respecto a esa arquitectura de seguridad. Primero, se utiliza CCMP [34] (Counter Cipher Mode Protocol) para proteger las nuevas tramas más largas de 802.11n. Segundo y más importante, 802.11n especifica que TKIP no está permitido para su uso con 802.11n.

La decisión de eliminar TKIP para su uso con 802.11n fue objeto de debate dentro del grupo de trabajo 802.11. TKIP fue originalmente diseñado como una medida provisional, y trajo cierta cantidad de robustez en términos de seguridad, para que pudiera modernizar los dispositivos 802.11b entonces existentes. Sin embargo, el diseño de TKIP no era fácil de extenderse a nuevas funcionalidades. Por ejemplo, cuando surgieron las capacidades de QoS, TKIP no protegía el contenido del campo de control de QoS, lo que condujo a un pequeño ataque debido a este error de seguridad.

CAPÍTULO 4: PLANIFICACIÓN Y ESTIMACIÓN DE COSTES

4.1 Recursos

4.1.1 Humanos

- D. Jorge Navarro Ortiz y D. Pablo Almeigeiras Gutiérrez, profesores del Departamento de Teoría de la Señal, Telemática y Comunicaciones, de la Universidad de Granada, en calidad de tutores del proyecto.
- Luis Antonio Cano Pérez, alumno de la Escuela Técnica Superior de Ingeniería Informática y Telecomunicación de la Universidad de Granada, autor del proyecto.

4.1.2 Hardware

- Dos ordenadores del departamento para la configuración y las pruebas.
- Dos tarjetas de red inalámbricas PCIe 802.11a/g/n 3 x 3 iguales.
- Una tarjeta de red inalámbrica USB 802.11 b/g.

4.1.3 Software

- Sistema operativo GNU/Linux Ubuntu 11.10 (32 bits).
- Sistema operativo Windows 7 (64 bits).

- Hostapd, herramienta para creación de puntos de acceso y servidores de autenticación (Linux) [35].
- ISC DHCP server, servidor DHCP (Linux) [36].
- ProFTPD, servidor FTP (Linux) [37].
- FileZilla, cliente FTP (Windows) [38].
- inSSIDer, herramienta para análisis de redes WLAN (Windows) [39].
- Tshark, versión por comandos de Wireshark, herramienta sniffer (Windows) [40].
- ChilliSpot, portal captivo (Linux) [41].
- Apache 2, servidor web (Linux) [42].
- FreeRADIUS, servidor radius (Linux) [43].
- MySQL, base de datos (Linux) [44].
- Iw (Linux) [45]

4.1.4 Otros recursos

- Mesa con ruedas, proporcionada por la escuela, para mover la estación.
- Metro de 20 metros, para realizar el mapa de la zona donde se realizan las pruebas, y para localizar los puntos de prueba de la estación.
- Alargadera, parar realizar las medidas de forma cómoda, sin tener que apagar el ordenador cada vez que la estación cambia de punto.

4.2 Fases de desarrollo

La distribución temporal de los cinco paquetes de trabajo puede verse en diagrama de Gantt de la figura 4.1.

4.2.1 Especificación de requisitos

Se analizan detalladamente los problemas que tenemos que resolver en pos de una correcta especificación de nuestros 2 escenarios.

4.2.2 Implementación

Se implementan los 2 escenarios con los que se va a trabajar, los cuales serán descritos en el capítulo siguiente.

4.2.3 Proceso de medida

Se realizan una serie de medidas sobre el escenario 1, para distintas configuraciones de red.

4.2.4 Evaluación de los resultados

Se hace un análisis de los resultados obtenidos en la fase anterior y se extraen conclusiones a partir de ese análisis.

4.2.5 Documentación

La redacción de la documentación es una tarea que se realiza de forma paralela al resto, salvo en el último tramo.

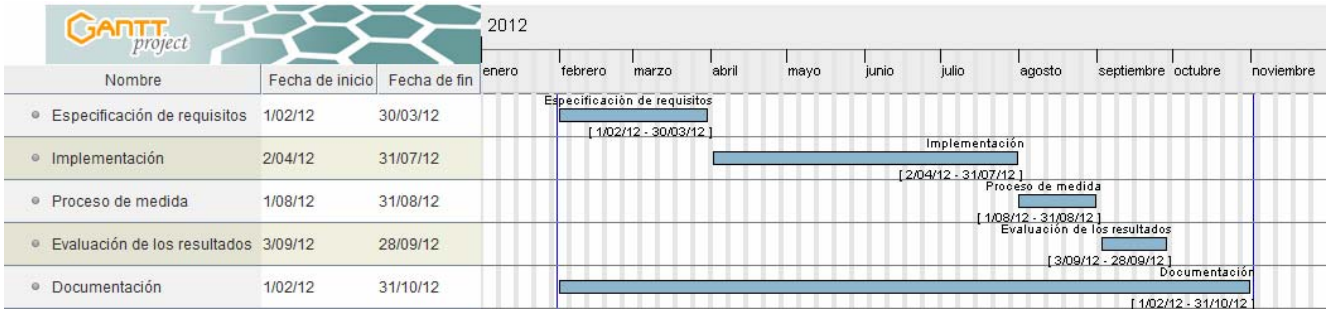

Figura 4.1: Planificación temporal del proyecto

4.3 Estimación de costes

4.3.1 Recursos humanos

En la tabla 4.1 puede verse el coste temporal de los diferentes paquetes de trabajo. El total se computa en días (jornadas de 6 horas a 20 €/hora), sin contar sábados, domingos y festivos. La documentación no aparece por ser una tarea que se realiza en paralelo con las demás. La figura 4.2 refleja el coste monetario asociado a cada una de las fases del proyecto.

Fase	Duración (días)
Especificación de requisitos	42
Implementación	81
Proceso de medida	22
Evaluación	20
Documentación	23
Total	188

Tabla 4.1: Coste temporal del proyecto

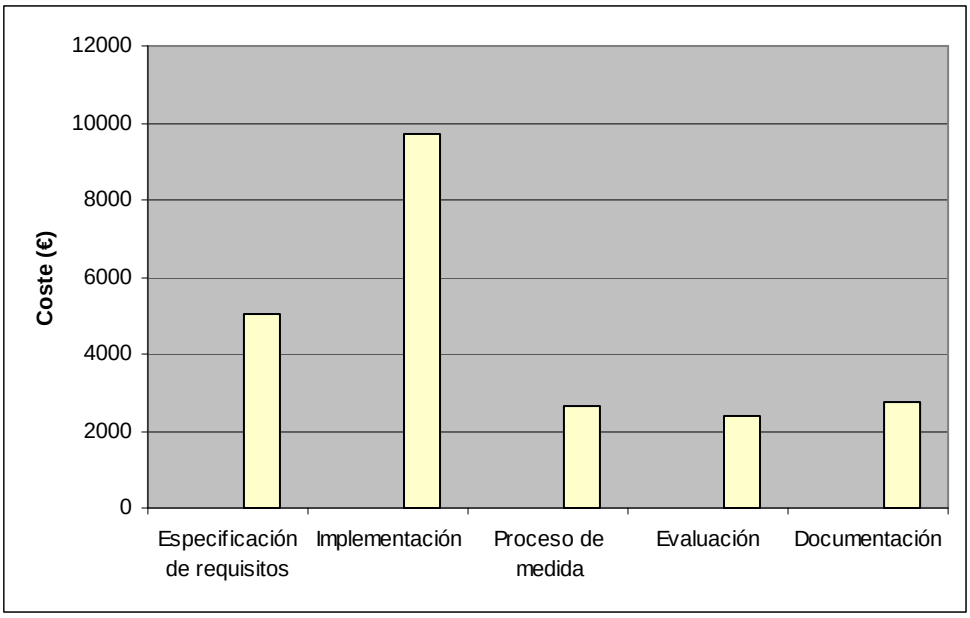

Figura 4.2: Coste monetario asociado a cada fase del proyecto

4.3.2 Recursos hardware

En la tabla 4.2 se recoge el coste monetario de los recursos hardware.

Recurso	Unidades	Coste unitario (€)	Vida media
Ordenador personal	2	800	36 meses
Tarjeta de red inalámbrica PCIe 802.11n 3x3	2	40	-
Tarjeta de red inalámbrica USB 802.11g	1	20	-

Tabla 4.2: Coste monetario asociado al hardware

4.3.3 Recursos software

Se han usado herramientas gratuitas, para minimizar el coste del proyecto, por tanto el coste asociado al software es nulo.

4.4 Presupuesto

Por último la tabla 4.3 registra el presupuesto del proyecto.

Concepto	Cantidad (€)
Recursos humanos: 188 días x 6 horas/día x 20 €/hora	22560
Recursos hardware:	
2 ordenadores personales x 800 €/unidad x 6,27 meses / 36 meses	268,67
2 tarjetas PCIe 802.11n 3x3 x 40 €/unidad	80
1 tarjeta USB 802.11g x 20 €/unidad	20
Total	22928,67

Tabla 4.3: Presupuesto del proyecto

CAPÍTULO 5: ESCENARIOS Y CONFIGURACIÓN AVANZADA

En este capítulo se definen los 2 escenarios con los que vamos a trabajar y la configuración de cada uno de ellos. Ambos están formados por dos equipos: uno de ellos funcionando como AP y el otro como estación. La diferencia, es que en el primer escenario el AP no tiene acceso a Internet, ya que lo que nos interesa, es el enlace AP-STA, mientras que en el segundo escenario, el AP tiene 2 interfaces, uno de ellos conectado a Internet, ya que la finalidad de un servicio HotSpot no es otra que permitir la conexión a Internet de los usuarios. Además, en el primer escenario se van a medir parámetros de la conexión (Throughput, RSSI y MCS). La decisión de utilizar un AP creado mediante un equipo en lugar de un AP real, de la universidad, se basa principalmente en dos razones: la primera es que actualmente los AP de la UGR no son compatibles con 802.11n, y segundo, aunque lo fueran, no sería muy seguro realizar experimentos con estos, ante la posibilidad de que se produzca cualquier conflicto o error en la red de la universidad.

5.1 Escenarios

En ambos escenarios vamos a trabajar únicamente con el modo MIMO de multiplexación espacial, transmitiendo un stream espacial independiente por cada antena, ya que los modos de diversidad espacial no son compatibles con el driver (Ath9k) que utilizamos. El modo PLCP utilizado será el modo mixto, ya que, aunque tanto el AP como la STA son compatibles con 802.11n y teóricamente podría usarse el modo greenfield, este no está implementado en las tarjetas de red de las que se dispone.

5.1.1 Escenario 1: Punto de acceso y estación

Los objetivos de este primer escenario son 2: por un lado, configurar una red 802.11n y entender su funcionamiento, y por otro lado, evaluar el comportamiento de la misma.

En este escenario, el equipo que actúa como estación se conectará a la red creada por el equipo que funciona como punto de acceso, pero que no estará conectado a Internet. A continuación, la estación descargará un archivo desde el AP mediante FTP. Este experimento se repetirá para varias localizaciones de la estación y distintas configuraciones de red. Mediante este experimento se medirán ciertos parámetros de la conexión. En el capítulo siguiente, se explica en detalle el proceso de medición. En la figura 5.1 podemos ver una representación del escenario 1.

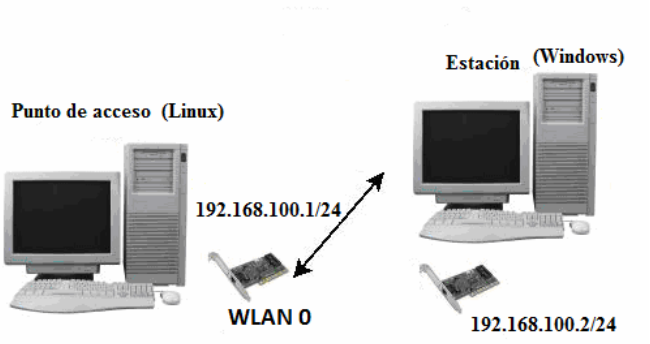

Figura 5.1: Escenario 1

Punto de acceso

De aquí en adelante, AP. Es un ordenador que pertenece al departamento con las siguientes características:

- Procesador Pentium Dual-Core ES400 2 núcleos a 2,70 GHz.
- 4 GB de memoria RAM.
- Sistema Operativo GNU/Linux Ubuntu 11.10 (32 bits).
- Tarjeta de red inalámbrica PCIe TP-LINK, modelo TL-WDN4800 [46] con chipset Atheros AR9380 [47], compatible con 802.11a/g/n (3 x 3).

Estación

De aquí en adelante, STA. Es un ordenador que pertenece al departamento, con las siguientes características:

- Procesador Intel Core 2 Dúo 6400 con 2 núcleos a 2,13 GHz.
- 2 GB de memoria RAM.
- Sistema Operativo Windows 7 (64 bits).

- Tarjeta de red inalámbrica PCIe TP-LINK, modelo TL-WDN4800 con chipset Atheros AR9380, compatible con 802.11a/g/n (3 x 3).

5.1.2 Escenario 2: Servicio Hotspot

En este escenario, el único objetivo es implementar el servicio Hotspot y entender su funcionamiento. Por tanto, no se realizan medidas de ningún tipo. Para entender mejor este escenario se va a hacer una breve descripción de los Hotspots y los portales cautivos.

Hotspot

En el contexto de las comunicaciones inalámbricas, un HotSpot (punto caliente) es una zona de alta demanda de tráfico, y por tanto el dimensionamiento de su cobertura está condicionado a cubrir esta demanda por parte de un punto de acceso o varios, y de este modo proporcionar servicios de red a través de un proveedor de servicio de Internet inalámbrico (WISP, Wireless Internet Service Provider).

Los HotSpots se encuentran en lugares públicos, como aeropuertos, bibliotecas, centros de convenciones, hoteles, etcétera. Este servicio se puede cubrir mediante Wi-Fi y permite mantenerse conectado a Internet en lugares públicos. Puede brindarse de manera gratuita o pagando una suma que depende del proveedor. Todo tipo de dispositivos con interfaz inalámbrica pueden conectarse a un HotSpot: portátil, móvil, PDA, tablet...

Portal cautivo

Un portal cautivo (o captivo) es un programa o máquina que, en una red informática, controla el tráfico HTTP y fuerza a los usuarios a pasar por una página paralela para habilitar la navegación por Internet de forma normal. Este intercepta todo el tráfico HTTP hasta que el usuario se autentifique. El portal se encargará de hacer que esta sesión caduque al cabo de un tiempo.

Los portales cautivos se usan en Hotspots, donde interesa mostrar un mensaje de bienvenida a los usuarios para informar de las condiciones de acceso (puertos permitidos, responsabilidad legal). Los administradores suelen hacerlo para que sean los propios usuarios quienes se responsabilicen de sus acciones, y así evitar problemas de cualquier tipo. También nos permite configurar el acceso por un tiempo limitado, o por un tamaño de bytes descargados.

Tras este breve paréntesis, se continúa con la descripción del escenario 2. Al igual que en el primero, un equipo se configura como AP y otro como estación. A continuación, la estación se conecta al AP. La diferencia, es que ahora el AP implementa un servicio de Hotspot para gestionar la conexión de la estación a Internet. Para ello la estación debe autenticarse mediante un portal web, al que será redireccionado automáticamente, introduciendo sus datos de usuario. Por tanto, el equipo que hace de AP va a tener 2 interfaces de red inalámbrica: uno de ellos para conectar a Internet y el otro para la conexión con la estación. Es necesario aclarar que, el enlace entre el AP e Internet, podría ser cableado. La única razón por la que se ha elegido este tipo de enlace, es la sencillez y disponibilidad de conexión a la red

inalámbrica de la UGR para cualquier estudiante con cuenta de correo institucional. Por el contrario, la conexión cableada sólo esta disponible para profesores e investigadores que trabajen para la UGR. Sin embargo, el enlace entre el AP y la STA debe ser inalámbrico, por la propia definición de Hotspot. El esquema se puede ver en la figura 5.2.

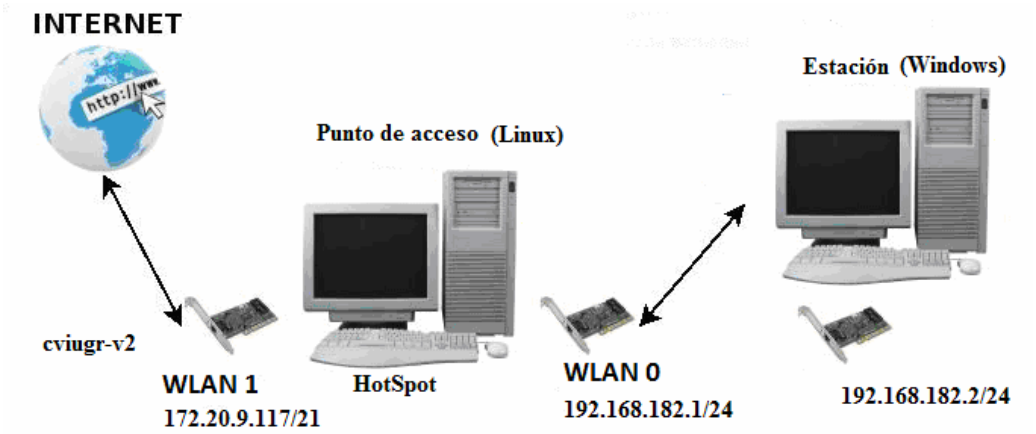

Figura 5.2: Escenario 2

Punto de acceso

De aquí en adelante, AP. Es un ordenador que pertenece al departamento con las siguientes características:

- Procesador Pentium Dual-Core ES400 2 núcleos a 2,70 GHz.
- 4 GB de memoria RAM.
- Sistema Operativo GNU/Linux Ubuntu 11.10 (32 bits).
- Tarjeta de red inalámbrica PCIe TP-LINK, modelo TL-WDN4800 con chipset Atheros AR9380, compatible con 802.11a/g/n (3 x 3).
- Tarjeta de red inalámbrica USB D-Link AirPlus G DWL-G122, compatible con 802.11b/g [48].

Estación

Las características de la estación en el escenario 2 son las mismas que en el primero.

5.2 Configuración avanzada

En este apartado se describen las configuraciones llevadas a cabo en cada uno de los escenarios.

5.2.1 Escenario 1

Punto de acceso

o Hostapd

Se trata de un programa open source, solamente disponible para S.O. Linux, el cual permite que una estación funcione como AP. Para ello, básicamente, lo que hace es cambiar el modo en el que funciona la tarjeta de red inalámbrica, de managed, que es el modo de estación, a modo master, siempre y cuando la propia tarjeta de red sea compatible con este modo. Además incorpora mecanismos de autenticación. Hostapd permite controlar gran cantidad de parámetros, como si de un AP real se tratara: nombre de la red, tipo de autenticación, banda de trabajo, canal, intervalo beacon, parámetros de 802.11n (anchura del canal, intervalo de guarda), etc. A continuación se detallan los pasos seguidos para su configuración:

- Descargamos e instalamos hostapd: # *sudo apt-get install hostapd.*
- Editamos el archivo de configuración etc/hostapd/hostapd.conf:

```
# Interfaz que actúa como AP
interface=wlan0

# Se debe elegir nl80211 si trabajamos con Ath9k
driver=nl80211

# Nombre de la red
ssid=Prueba

# Estandar 802.11 capa fisica (802.11a,802.11g o
#802.11b)
hw_mode=a

# Canal (Depende de la banda en la que trabajemos)
channel=36

#Filtrado de MAC. Desactivado
macaddr_acl=0

# Sistema de autenticación compartido
auth_algs=3

# Enviar beacon con SSID vacío e ignorar probe
#request. Desactivado
ignore_broadcast_ssid=0

# Habilitamos 802.11n
wme_enabled=1
ieee80211n=1

# Capacidades de HT
# Usamos HT40+ o HT40- según esta tabla
#freq      HT40-         HT40+
#2.4 GHz   5-13          1-7 (1-9 in Europe/Japan)
#5 GHz     40,48,56,64   36,44,52
ht_capab=[HT40+]
```

```
# Parámetros de encriptación WEP
wep_default_key=0
wep_key0=123456789a

# Opción necesaria para clientes Windows
eapol_key_index_workaround=0
```

- Modificamos el script de inicio /etc/init.d/hostapd para que la variable DAEMON_CONF apunte al archivo de configuración que acabamos de crear: *DAEMON_CONF=/etc/hostapd/hostapd.conf.*

- Iniciamos hostapd: # *sudo /etc/init.d/hostapd start.*

- Para comprobar errores podemos ejecutarlo en modo debug: *# sudo hostapd -d /etc/hostapd/hostapd.conf.*

- Ejecutando el menú de configuración de interfaces inalámbricas de Linux, podemos ver como el interfaz wlan0 está funcionando como un punto de acceso (modo master): # iwconfig.

```
luis@luis-System-Product-Name:/etc/hostapd$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      no wireless extensions.

wlan0     IEEE 802.11abgn  Mode:Master  Frequency:2.412 GHz  Tx-Power=20 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

wlan1     IEEE 802.11bg  ESSID:"cviugr-v2"
          Mode:Managed  Frequency:2.462 GHz  Access Point: 00:11:92:15:AD:50
          Bit Rate=54 Mb/s   Tx-Power=20 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
          Link Quality=62/70  Signal level=-48 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

Figura 5. 3: Menú iwconfig

o ISC DHCP

Se trata de un simple servidor DHCP open source para Linux, para que el AP pueda asignar direcciones IP a las estaciones que se conectan a su red. Es necesario, ya que hostapd no incorpora servidor DHCP. El proceso de configuración es el siguiente:

- Descargamos el servidor DHCP: *# sudo apt-get install isc-dhcp-server*.

- Modificamos el archivo /etc/default/isc-dhcp-server para indicarle al servidor que utiliza el interfaz wlan0 crear: *INTERFACES=”wlan0”*

- Editamos el archivo de configuración /etc/dhcp/dhcpd.conf:

```
# Parámetros del servidor DHCP
default-lease-time 600;
max-lease-time 7200;
```

```
# Usamos una subred privada de clase C
subnet 192.168.100.0 netmask 255.255.255.0 {

# Rango de direcciones IP para asignar (solo 1
estación)
range 192.168.100.2 192.168.100.2;

}
```

- Asignamos una ip fija al interfaz wlan0: *# sudo ifconfig wlan0 192.168.100.1 netmask 255.255.255.0.*

- Iniciamos el servidor DHCP: *# sudo /etc/init.d/isc-dhcp-server start.*

- **ProFTPD**

Se trata simplemente de un servidor FTP open source para Linux, donde se alojará un archivo para que la estación lo descargue y de esta forma llevar a cabo los experimentos. El proceso de configuración se detalla a continuación:

- Descargamos e instalamos el servidor FTP: *#sudo apt-get install proftpd.*

- Durante la instalación se nos pide que indiquemos si el servidor se ejecutará desde initd o de forma independiente. Elegimos la segunda opción.

- Editamos el archivo de configuración /etc/proftpd/proftpd.conf. Los únicos parámetros que vamos a modificar son los siguientes:

```
# Utilizaremos el puerto 1980
Port                1980

# Creamos un usuario anónimo sin contraseña
 <Anonymous ~ftp>
   User                 ftp
   Group             nogroup

   # Asignamos el alias ftp al usuario anónimo
   UserAlias            anonymous ftp
```

- Por defecto, el servidor crea un directorio, para compartir los archivos en /srv/ftp. Copiamos a este directorio nuestro archivo de prueba.

- Iniciamos el servidor FTP: *# sudo /etc/init.d/proftpd start.*

- **Iw**

Se trata de una herramienta de Linux para la configuración y control de parámetros de redes inalámbricas. Mediante este obtendremos el valor del MCS entre la estación y el AP.

- Descargamos e instalamos el programa: *# sudo apt-get install iw.*

- Obtenemos las estadísticas para la estación conectada al AP: *# sudo iw dev wlan0 station dump*. Al ejecutar este comando, obtendremos algo similar a lo de la figura 5.4

```
luis@luis-GT110-F1:/etc/hostapd$ iw dev wlan0 station dump
Station f8:d1:11:c2:19:39 (on wlan0)
        inactive time:  8 ms
        rx bytes:       457746
        rx packets:     6403
        tx bytes:       231565273
        tx packets:     151323
        signal:         -53 dBm
        tx bitrate:     364.5 MBit/s MCS 22 40Mhz
```

Figura 5. 4: Estadísticas iw

Estación

o InSSIDer

Se trata de un programa open source para analizar redes WLAN. Está disponible para Windows, MAC y Linux. Permite escanear todas las redes que están al alcance de una estación. De cada una de las redes muestra ciertos parámetros como la potencia con la que se recibe, dirección MAC del AP, canal y banda en la que emite, seguridad, tasa máxima de datos, tipo de red, etc. Se utilizará para ver las redes de nuestro entorno, comprobar el correcto funcionamiento de hostapd y medir la potencia que se recibe en la estación. Antes de utilizarlo, debemos seguir una serie de pasos:

- Descargamos el archivo de instalación, en su versión para Windows, directamente desde su página web: http://www.metageek.net/products/inssider/download/.

- Ejecutamos el fichero para instalar el programa.

- A continuación empezamos a trabajar con él. En la pantalla inicial vemos la lista de redes al alcance de la estación. En la primera posición se encuentra la red que hemos creado. Como vemos todos los parámetros están acorde con lo que hemos configurado en el AP.

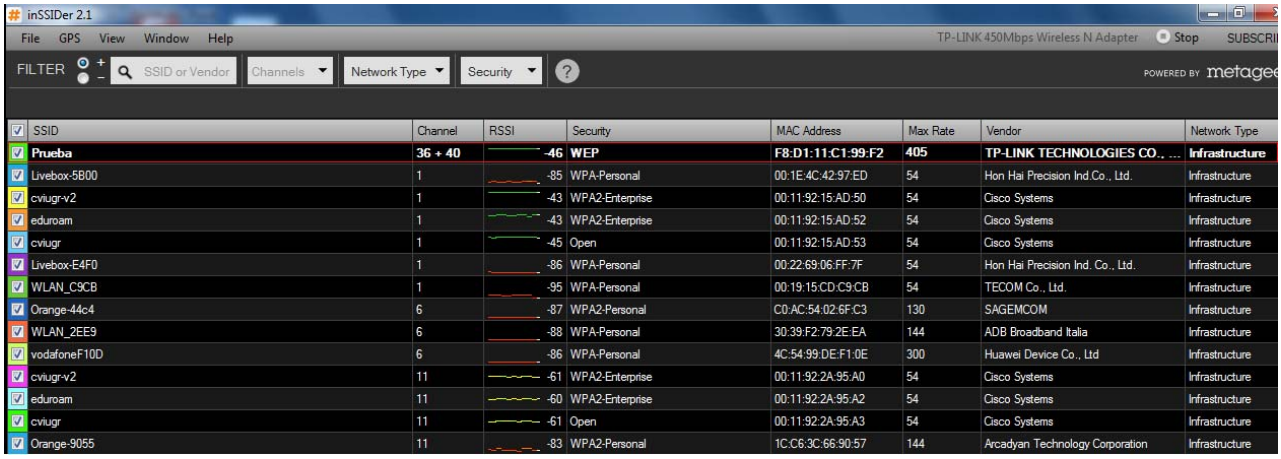

Figura 5.5: Menú principal inSSIDer

- Ahora sin pinchamos en la pestaña de espectro de 5 GHz veremos la banda de 5 GHz y nuestra red situada sobre ella.

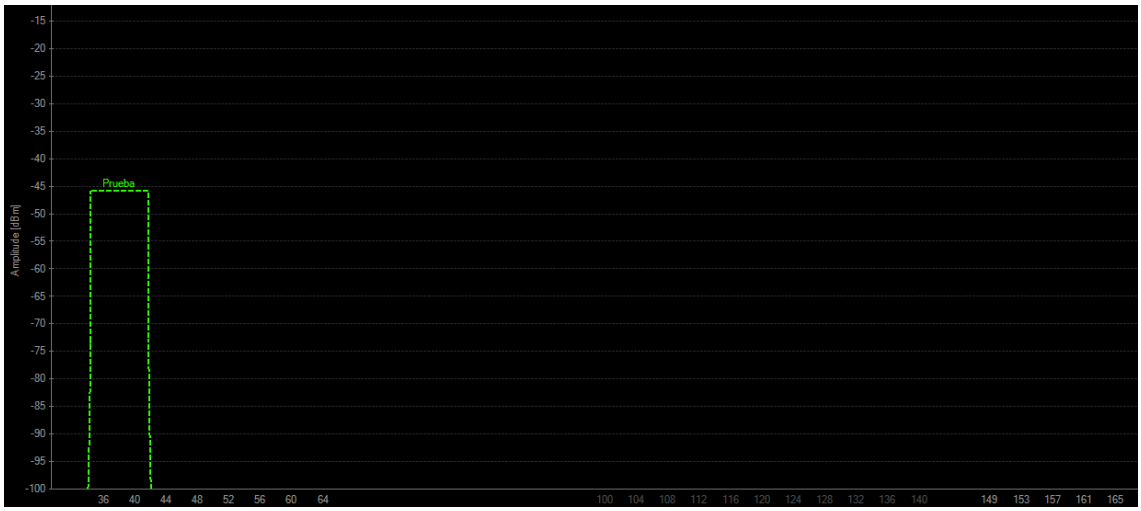

Figura 5.6: Espectro de 5 GHz

- **FileZilla**

Se trata de un software open source de cliente FTP multiplataforma. Hay muchos programas similares, pero se ha elegido este por su simplicidad en la configuración. Será utilizado para descargar un archivo de prueba desde el AP. Para su instalación y configuración tenemos que atender a una serie de pasos:

- Descargamos el archivo de instalación para Windows, directamente desde su página web: http://filezilla-project.org/download.php?type=client.
- Ejecutamos el fichero para instalar el cliente FTP.
- Empezamos a trabajar con él. La configuración es sencilla. Tan solo hay que indicar la dirección IP del servidor FTP, el usuario y el puerto.

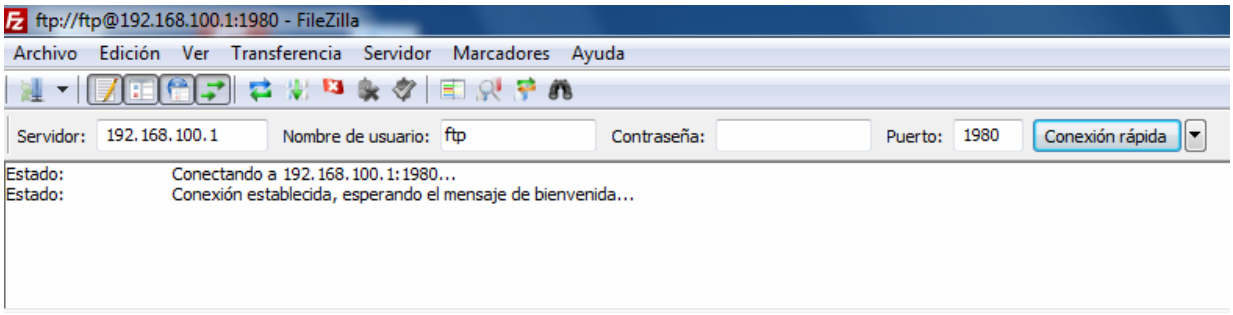

Figura 5.7: Interfaz de FileZilla

- Pinchamos en Conexión rápida y accedemos a la carpeta compartida, desde la cual, podemos descargar el archivo de prueba.

- **Tshark**

Se trata de la versión por línea de comandos de Wireshark, un sniffer o analizador de protocolos de libre distribución. Permite analizar y capturar paquetes de red. Actualmente soporta más de 1000 protocolos. Mediante este se pueden desglosar todas las capas de un paquete de una forma sencilla. Se utilizará para medir el Througput de la conexión entre el AP y la STA. Hemos utilizado esta versión, en lugar de la versión gráfica, debido a que al ejecutar Wireshark se producía una ralentización de la conexión. Además este se bloqueaba debido a la gran cantidad de tramas que recibía en un período tan corto de tiempo. Antes de poder usarlo, debemos seguir ciertos pasos:

- Descargamos el archivo de instalación de Wireshark para Windows (64 bits), ya que tshark viene incluido con este: http://www.wireshark.org/download.html.

- Tenemos que añadir una variable al path de Windows, indicando el camino donde esta tshark. Para ello pinchamos con el botón derecho sobre Equipo (Mi PC en antiguas versiones). A continuación pinchamos en el menú de Propiedades. Hecho esto, en la parte izquierda de la pantalla pinchamos en Configuración avanzada del sistema. Ahora nos aparecen varias pestañas. Pinchamos en la pestaña de Opciones avanzadas y seguidamente, la última opción Variables de entorno. Por último buscamos la variable Path y le damos a editar y añadimos el siguiente camino: C:\Archivos de programa\Wireshark.

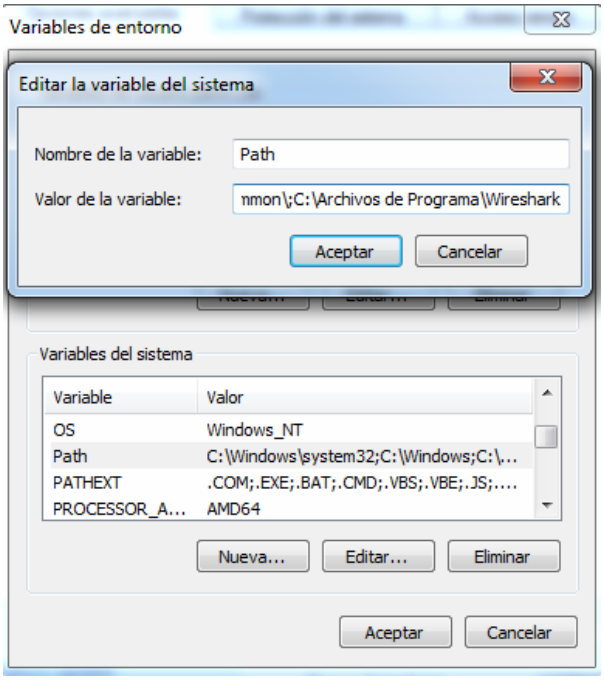

Figura 5.8: Menú de variables de entorno Windows 7

- Ya podemos usar tshark. Para iniciar la captura el comando es el siguiente: *# tshark -a duration:x -w captura.pcap*, siendo x la duración en segundos de la captura.

- Para ver los resultados de la captura ejecutamos otro programa integrado con Wireshark, llamado capinfos. El comando es: *# capinfos*

captura.pcap. Como resultado se obtendrá una lista de estadísticas como las de la figura 5.9. El parámetro que nos interesa es el Throuhput, el cual aparece con el nombre de Average bit rate.

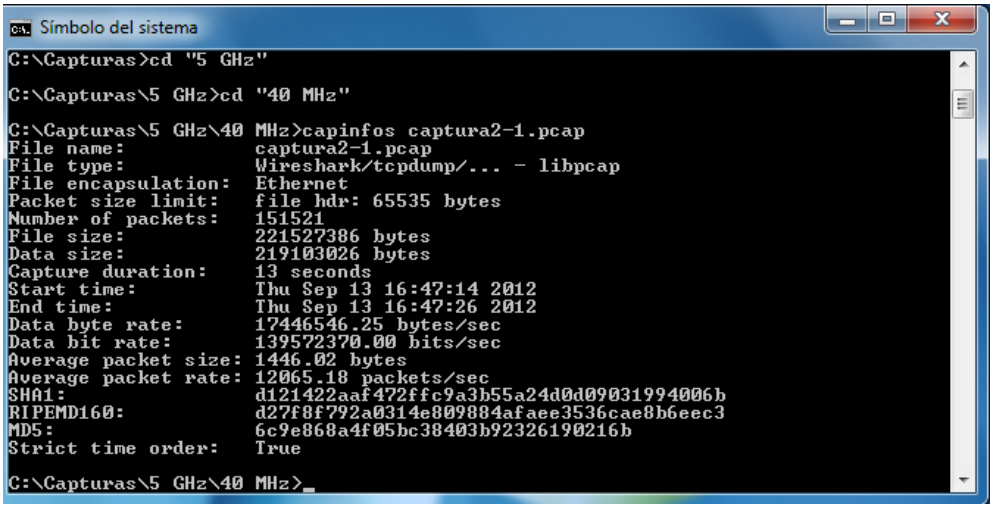

Figura 5.9: Estadísticas tshark

5.2.2 Escenario 2

Punto de acceso

- **Hostapd**

  La misma configuración que para el escenario 1.

- **Sistema operativo**

  - Es necesario que habilitemos el soporte para interfaces virtuales TUN/TAP de Linux, ya que ChilliSpot hará uso de un interfaz virtual. Para ello modificamos el archivo etc/modules e incluimos la sentencia *tun*.

  - A continuación cargamos el modulo tun: *# sudo modprobe tun*.

- **ChilliSpot**

Se trata de un programa open source que hace la función de portal cautivo/captivo y sólo existe en su versión para Linux. Este incorpora un servidor DHCP por tanto no será necesario utilizar un servidor externo, tal y como se hizo en el escenario 1. Como ya se ha comentado, trabaja a través un interfaz virtual. Para su puesta en marcha debemos seguir una serie de pasos:

- Lo descargamos e instalamos: *# sudo apt-get install chillispot*.

- Dentro de la documentación de ChilliSpot (/usr/share/doc/chillispot/) tenemos el archivo hotspotlogin.cgi. Generalmente viene comprimido y lo encontramos como hotspotlogin.cgi.gz. En primer lugar tenemos que descomprimirlo: *#sudo gzip /usr/share/doc/chillispot/hotspotlogin.cgi.gz*.

- A continuación copiamos ese archivo cgi en la carpeta /usr/lib/cgi-bin:
  # sudo cp /usr/share/doc/chillispot/hotspotlogin.cgi /usr/lib/cgi-bin.

- Hecho esto, editamos el archivo de configuración /etc/chilli.conf.

```
# Dirección IP del servidor radius 1. Usamos una
#dirección de bucle local, ya que el servidor radius
# se ejecutará también en el equipo que hace de AP.
radiusserver1 127.0.0.1

# Como sólo tenemos un servidor radius, fijamos el
#valor de radiusserver2 al mismo que radiusserver1
radiusserver2 127.0.0.1

# Secreto del servidor radius
radiussecret radius

# Dirección del servidor DNS
dns1 8.8.8.8

# Indicamos el interfaz por el que se va a asignar
#direcciones IP mediante DHCP
dhcpif wlan0

# URL del servidor web que se encarga de la
#autenticación
uamserver https://192.168.182.1/cgi-
bin/hotspotlogin.cgi

# URL de inicio del portal captivo
uamhomepage http://192.168.182.1/welcome.html

uamallowed 192.168.100.0/24,192.168.182.0/24

#Secreto compartido entre ChilliSpot y el servidor
#web de autenticación
uamsecret apache
```

- Ahora vamos a habilitar el uso de ChilliSpot. Para ello tenemos que modificar el archivo /etc/default/chillispot e incluir la sentencia: *ENABLEB=1*.

- Por último, ejecutamos ChilliSpot: *# sudo /etc/init.d/chillispot start*.

- Ejecutando el menú iwconfig podemos ver como ChilliSpot nos ha creado un interfaz virtual llamado tun0.

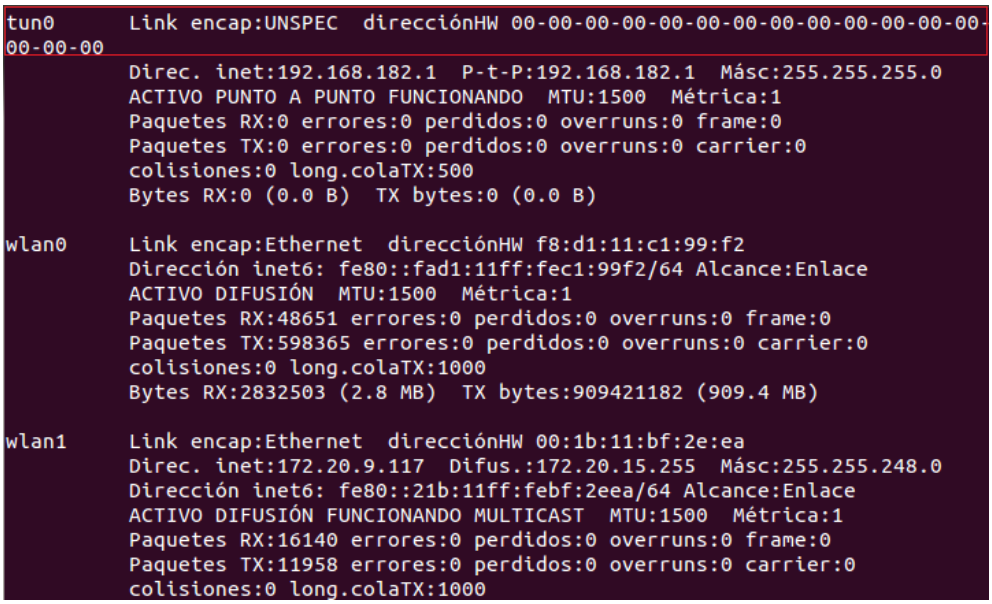

Figura 5.10: Interfaz virtual creado por ChilliSpot

- **Firewall de Linux**

  - En la documentación de ChilliSpot se incluye un archivo de iptables para control las conexiones de las estaciones a la red. Copiamos este archivo usr/share/doc/chillispot/firewall.iptables en el directorio /etc/init.d: *#sudo cp usr/share/doc/chillispot/firewall.iptables /etc/init.d/.*

  - A continuación, modificamos 2 parámetros del archivo de iptables:

```
# Interfaz que permite el acceso a internet
EXTIF="wlan1"

# Interfaz que conecta con la LAN
INTIF="wlan0"
```

  - Ahora damos permiso de ejecución al archivo y agregamos las reglas al inicio del sistema: *# sudo chmod a+x /etc/init.d/firewall.iptables* y *# sudo ln -s etc/init.d/firewall.iptables /etc/rcS.d/S41firewall.iptables.*

  - Por último, ejecutamos la configuración de firewall: *#sudo /etc/init.d/firewall.iptables.*

- **Apache 2 (con soporte para SSL)**

Se trata de un servidor web open source para Linux. Será necesario para alojar el sitio web de nuestro portal cautivo. Se incluye soporte para SSL, de forma que el usuario y la contraseña no se manden como texto plano y puedan ser interceptados por terceras personas. Para su instalación y configuración debemos seguir una serie de pasos:

  - Descargamos e instalamos los paquetes apache2, apache2.2-common, apache2-mpm-worker y apache2-utils: *# sudo apt-get install apache2 apache2.2-common apache2-mpm-worker apache2-utils.*

- Creamos un archivo llamado welcome.html en el directorio /var/www, conteniendo lo siguiente:

```
<a href="http://192.168.182.1:3990/prelogin">Click
here to login</a>
```

- Damos permiso de ejecución al archivo /usr/lib/cgi-bin/hotspotlogin.cgi : *# sudo chmod a+x /usr/lib/cgi-bin/hotspotlogin.cgi*.

- Hecho esto, modificamos el archivo cgi anterior incluyendo lo siguiente:

```
#Secreto entre ChilliSpot y el servidor web
$uamsecret = "apache";
$userpassword=1;
```

- Ya tenemos configurado el servidor web, por tanto vamos a pasar a añadirle el soporte para SSL. En primer lugar creamos una carpeta llamada ssl en el directorio /etc/apache2, que será la ubicación de los archivos SSL que creemos: *#sudo mkdir /etc/apache2/ssl*.

- Nos situamos en el directorio /etc/apache2/ssl y generamos una llave de 1024 bits: *# sudo openssl genrsa -des3 -out portal.key 1024*. Se los pedirá una contraseña. Podemos usar la que queramos.

- Retiramos la contraseña de la llave mediante los siguientes comandos: *#sudo cp portal.key portal.key.org* y *#sudo openssl rsa -in portal.key.org -out portal.key*.

- Creamos la solicitud para firmar el certificado (CSR): *#sudo openssl req -new -key portal.key -out portal.csr*. Se nos pedirá una serie de datos que debemos completar.

- Firmamos el CSR: *#sudo openssl x509 -req -days 365 portal.csr -signkey Server.key -out portal.crt*.

- Habilitamos el módulo SSL: *#sudo a2enmod ssl*.

- Creamos el sitio SSL. Por defecto, Apache 2 trae un fichero de sitio SSL en /etc/apache2/sites-available. Hacemos una copia de este archivo para modificarlo: *#sudo cp /etc/apache2/sites-available/default /etc/apache2/sites-available/ssl*. La configuración del archivo ssl se puede ver en la figura 5.11.

```
NameVirtualHost *:443
<VirtualHost *:443>
        ServerAdmin webmaster@localhost
        SSLEngine On
        SSLOptions +FakeBasicAuth +ExportCertData +StrictRequire
        SSLCertificateFile      /etc/apache2/ssl/portal.crt
        SSLCertificateKeyFile   /etc/apache2/ssl/portal.key
        DocumentRoot /var/www
        <Directory />
                Options FollowSymLinks
                AllowOverride None
        </Directory>
        <Directory /var/www/>
                Options Indexes FollowSymLinks MultiViews
                AllowOverride None
                Order allow,deny
                allow from all
        </Directory>
        ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
        <Directory "/usr/lib/cgi-bin">
                AllowOverride None
                Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch
                Order allow,deny
                Allow from all
        </Directory>
        LogLevel warn
        ErrorLog /var/log/apache2/error.log

        # Possible values include: debug, info, notice, warn, error, crit,
        # alert, emerg.
        LogLevel warn
        CustomLog /var/log/apache2/access.log combined
        ServerSignature On
    Alias /doc/ "/usr/share/doc/"
    <Directory "/usr/share/doc/">
        Options Indexes MultiViews FollowSymLinks
        AllowOverride None
        Order deny,allow
        Deny from all
        Allow from 127.0.0.0/255.0.0.0 ::1/128
    </Directory>
</VirtualHost>
```

Figura 5.11: Configuración sitio SSL

- Habilitamos el sitio ssl: *#sudo a2ensite ssl*
- Por último, iniciamos el servidor: *#sudo /etc/init.d/apache2 start*
- Podemos comprobar que funciona correctamente, escribiendo en el navegador la dirección: https://localhost/. En caso de funcionar correctamente debemos obtener una página similar a la de la figura 5.12

Figura 5.12: Comprobación funcionamiento de Apache 2

- A veces, puede ocurrir, que al ejecutar Apache 2 se indique un error, debido a que el puerto 80 está siendo utilizado. En este caso, en primer

lugar, vemos el proceso xxxx que esta utilizando este puerto: *# sudo netstat -lnp | grep :80*. A continuación, acabamos con este proceso: *#sudo killall -9 xxxx* e iniciamos de nuevo el servidor.

- **Freeradius**

Se trata de un servidor Radius de libre distribución para Linux. ChilliSpot reenvía los datos de autenticación de los usuarios (usuario y contraseña) al servidor Radius. Este compara los datos recibidos con los almacenados en la base de datos MyQSL. En caso de coincidir, permitirá el acceso de los usuarios a Internet, en caso contrario, negará el acceso. El proceso seguido para su puesta en marcha se divide en una serie de pasos:

- Lo descargamos e instalamos: *#sudo apt-get install freeradius*.
- Editamos el archivo de configuración /etc/freeradius/clients.conf. Para ello tenemos que incluir lo siguiente:

```
client localhost {

ipaddr = 127.0.0.1

secret = radius

nastype= other

}
```

- Por último, comprobamos si el servidor Radius funciona correctamente. Para ello editamos el archivo /etc/freeradius/users. Debe quedar tal que así:

```
#Definimos un usuario steve con contraseña testing

steve Cleartext-Password := "testing"

Service-Type = Framed-User,

Framed-Protocol = PPP,

Framed-Compression = Van-Jacobsen-TCP-IP
```

Ahora, iniciamos el servidor en modo depuración: *#sudo freeradius -X*. A continuación, desde otro terminar, ejecutamos el siguiente comando: *#sudo radtest steve testing 127.0.0.1 1812 radius*. Si el servidor está configurado correctamente se debe recibir un mensaje indicando de Access-Acept, como el de la figura 6.13.

```
luis@luis-GT110-F1:/etc/freeradius/sites-available$ sudo radtest steve testing 1
27.0.0.1 1812 radius
Sending Access-Request of id 103 to 127.0.0.1 port 1812
        User-Name = "steve"
        User-Password = "testing"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 1812
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=103, length=38
        Service-Type = Framed-User
        Framed-Protocol = PPP
        Framed-Compression = Van-Jacobson-TCP-IP
```

Figura 5.13: Mensaje Access-Acept de freeRADIUS

- **MySQL**

Se trata de un sistema de gestión de bases de datos de licencia libre para Linux. Es necesario para almacenar los datos de los usuarios. Los pasos necesarios para que empiece a trabajar son los siguientes:

- Descargamos e instalamos los siguientes paquetes mysql-server y freeradius-mysql: *#sudo apt-get install mysql-server freeradius-mysql*.

- Creamos la base de datos donde se almacenarán los datos de los usuarios. Para ello, debemos acceder a MySQL como root: *#sudo mysql –u root –p* Tras introducir este comando, el prompt cambia a mysql>, indicando que podemos ingresar instrucciones de MySQL. Mediante el siguiente comando se crea una base de datos llamada base: *CREATE DATABASE base;*

- Siguiendo dentro del prompt de MySQL, el siguiente paso, es crear un usuario de MySQL “usuario” con contraseña “usuario”:

  *GRANT ALL PRIVILEGES ON base.*TO 'usuario'@'localhost'*

  IDENTIFIED BY 'usuario';

  FLUSH PRIVILEGES;

- Nos situamos en el directorio /etc/freeradius/sql/mysql e introducimos los siguientes comandos en el terminal:

  mysql -u root -p base < admin.sql

  mysql -u root -p base < ippool.sql

  mysql -u root -p base < nas.sql

  mysql -u root -p base < schema.sql

- En el paso anterior, en caso de producirse algún error, modificamos los permisos de los archivos para que se puedan leer:

  sudo chmod a+r /etc/freeradius/sql/mysql/admin.sql

  sudo chmod a+r /etc/freeradius/sql/mysql/ippool.sql

sudo chmod a+r /etc/freeradius/sql/mysql/nas.sql

sudo chmod a+r /etc/freeradius/sql/mysql/schema.sql

- Modificamos el archivo de configuración /etc/freeradius/radiusd.conf para que trabaje con MySQL. Para ello, descomentamos la línea

```
$INCLUDE sql.conf
```

- Editamos el archivo /etc/freeradius/sql.conf, para indicarle al servidor Radius el usuario y la contraseña para que pueda a la base de datos de MySQL:

```
login = "usuario"

password = "usuario"

readclients = yes

radius_db = "base"
```

- Editamos el archivo /etc/freeradius/sites-available/default. Tenemos que agregar la variable *sql* en las secciones authorize{}, accounting{}, session{} y post-auth{}. También es necesario comentar la variable *files* en la sección de authorize{}.

- Creamos algunos usuarios dentro de la base de datos. El primer usuario es “usuario1” con contraseña “usuario1”. El segundo es “usuario2” con contraseña “usuario2”:

mysql -u root -p

use base;

INSERT INTO radcheck (UserName, Attribute, Value) VALUES

('usuario1','Password','usuario1');

INSERT INTO radcheck (UserName, Attribute, Value) VALUES

('usuario2','Password','usuario2');

- Por último, tenemos que reiniciar el servidor Radius, para que se actualicen los cambios realizados en sus archivos de configuración: *#sudo freeradius*.

Estación

En la estación no es necesaria ninguna configuración. Lo único que debe hacer la estación es conectarse a la red e introducir correctamente los datos de usuario. En el anexo A podemos se comprueba el correcto funcionamiento del escenario.

CAPÍTULO 6: EVALUACIÓN

En este capítulo se procede a la evaluación del escenario 1. Para ello, en primer lugar se realizarán medidas del Throughput, potencia recibida y MCS en el enlace AP-STA y después se interpretará los resultados obtenidos.

6.1 Descripción del experimento principal

El experimento principal consiste en que la estación descargue un archivo de 219,5 MB desde al AP, mediante FTP. Este se repetirá para las 23 localizaciones señaladas con un punto amarillo, en el mapa de la figura 6.1. Este mapa representa el ala derecha del Edificio Orquídea, lugar donde se van a realizar las pruebas, que pertenece a la ETSSIT. Los únicos parámetros que se van a modificar son, el ancho de banda del canal, y la banda de frecuencia. El intervalo de guarda se mantiene fijo a su valor por defecto de 800 ns. Con este intervalo de guarda, la velocidad máxima que se puede conseguir con 3 streams espaciales es de 405 Mbps (ver tabla 3.3), tal y como indica inSSIDer en la figura 5.5. Las pruebas se realizarán para ambas bandas, de 2,4 y 5 GHz, con anchos de bandas de 20 y 40 MHz. Por tanto, cada experimento se realizará en cada localización, para cada banda de frecuencia y cada ancho de banda. Se repetirá 3 veces cada experimento para conseguir mayor exactitud. Las medidas se tomarán por la tarde/noche después de que los becarios e investigadores terminen su jornada laboral. De esta forma pretendemos reducir las interferencias.

En cada experimento individual, se tomarán medidas del Throughput (mediante Wireshark), el MCS (mediante suite iw) y la potencia recibida en la estación (mediante inSSIDer).

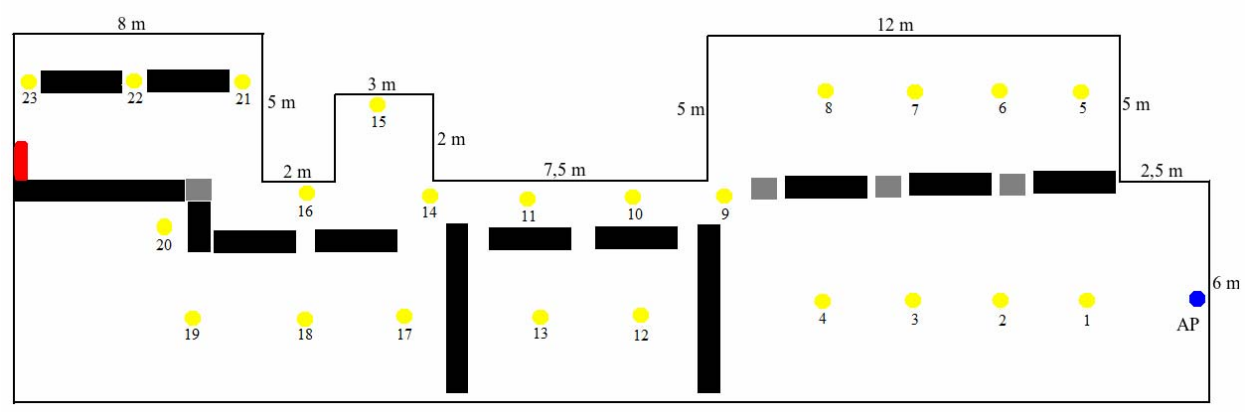

Figura 6.1: Ala derecha Edificio Orquídea

En la banda de los 5 GHz, la elección del canal ha sido prácticamente aleatoria, ya que donde nos encontramos no se recibe señal de ninguna red que emita en esta banda, tal y como se puede apreciar en la figura 5.6 del capítulo anterior. En nuestro caso, para ancho de canal de 20 MHz se eligió el 36, mientras que para ancho de banda de 40 MHz se utilizan el canal 36 más el 40, para formar con ambos un canal de 40 MHz.

Por el contrario, en la banda de 2,4 GHz emiten gran cantidad de redes, por lo que la elección en este caso no es aleatoria. Para ancho de banda de 20 MHz se eligió el canal 13, por ser el menos ocupado de los 14 canales con los que cuenta esta banda, ya que ni en el canal 12 ni en el 13 (el 14 esta prohibido en Europa), emite ninguna red. Podemos apreciar este hecho en la figura 6.2. Mientras que para ancho de banda de 40 MHz se utilizan los canales 9 y 13. En la figura 6.3 podemos ver el canal de 40 MHz en la banda de 2,4 GHz.

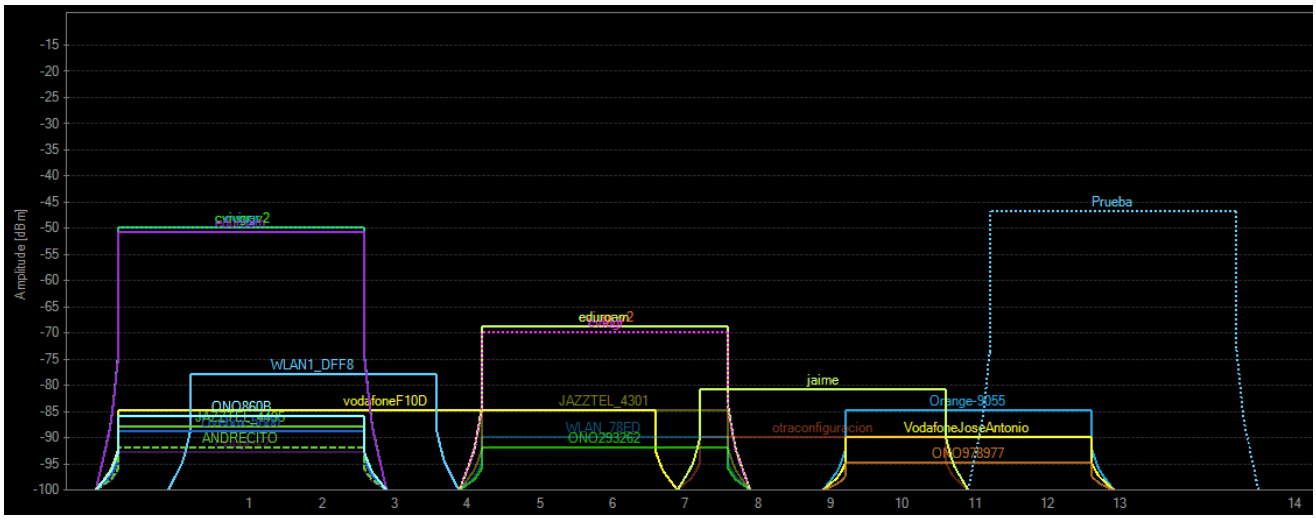

Figura 6.2: Espectro 2,4 GHz (BW=20 MHz). Edificio Orquídea

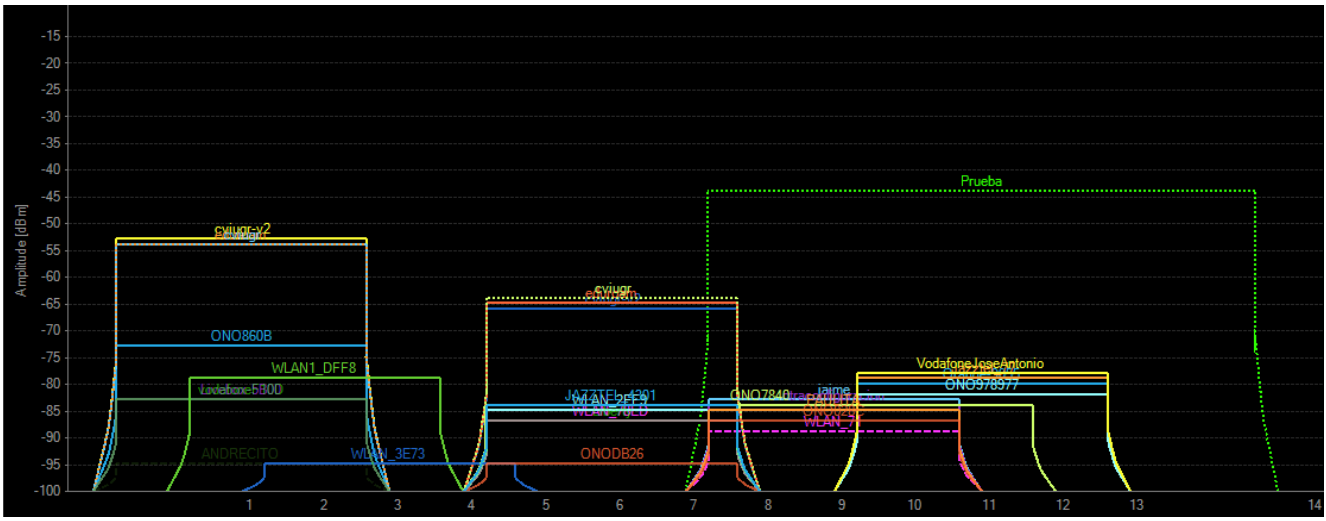

Figura 6.3: Espectro 2,4 GHz (BW=40 MHz). Edificio Orquídea

6.2 Proceso de medida

El procedimiento seguido para cada medida es el siguiente. En primer lugar, se configuran los parámetros de AP (ancho de banda y banda de frecuencia). A continuación desplazamos la estación hasta el punto de medida correspondiente. Ahora es cuando comenzamos a tomar las medidas. Para empezar, tomamos el valor del MCS desde el punto de acceso, una vez que se haya estabilizado, mediante iw tal y como se vio en el capítulo anterior. A continuación, medimos el Throughput de la conexión. Para ello, iniciamos la descarga del archivo desde la estación y al mismo tiempo arrancamos la captura de tshark. Por último, ejecutamos inSSIDer desde la estación para medir la potencia que se recibe en la misma. La razón por la que se mide la potencia en último lugar, es que al ejecutar inSSIDer se produce una ralentización de la conexión, disminuyendo el Throughput y el MCS.

En la figura 6.4 podemos ver una imagen del punto de acceso y en la 6.5, una de la estación durante el proceso de medida.

Figura 6.4: Punto de acceso

Figura 6.5: Estación

6.3 Resultados

En este apartado se va a representar los resultados obtenidos mediante 2 curvas. La primera de ellas es la de Throughput en función de la potencia recibida y la segunda, MCS frente a potencia recibida, todo esto para las dos bandas de frecuencia en las que puede trabajar 802.11n y para los 2 anchos de banda de canal.

6.3.1 MCS vs potencia recibida

Las curvas MCS vs potencia recibida se muestran en las figuras 6.6, 6.7, 6.8 y 6.9.

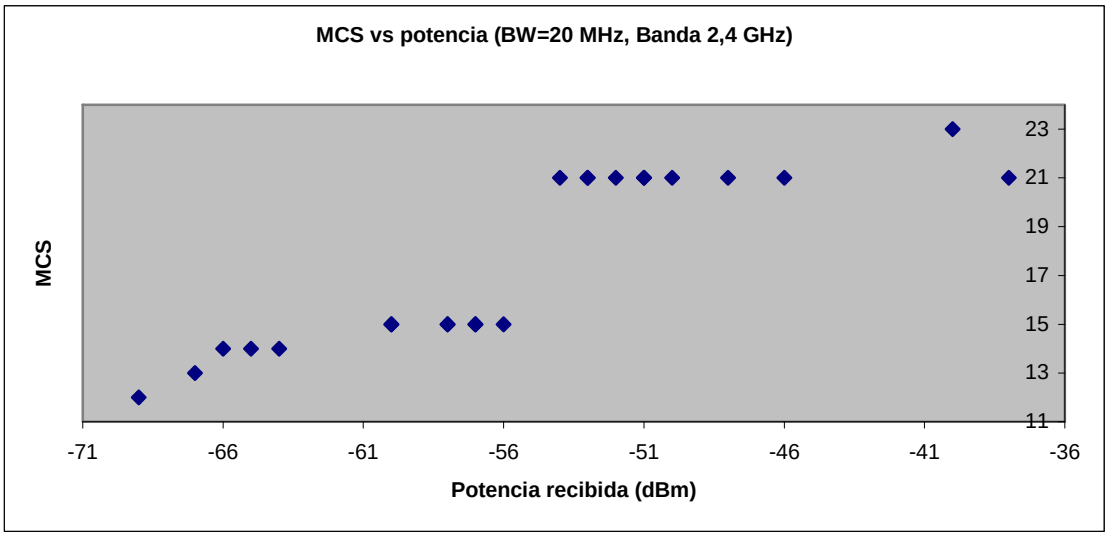

Figura 6.6: MCS vs potencia recibida (BW=20 MHz, Banda 2,4 GHz)

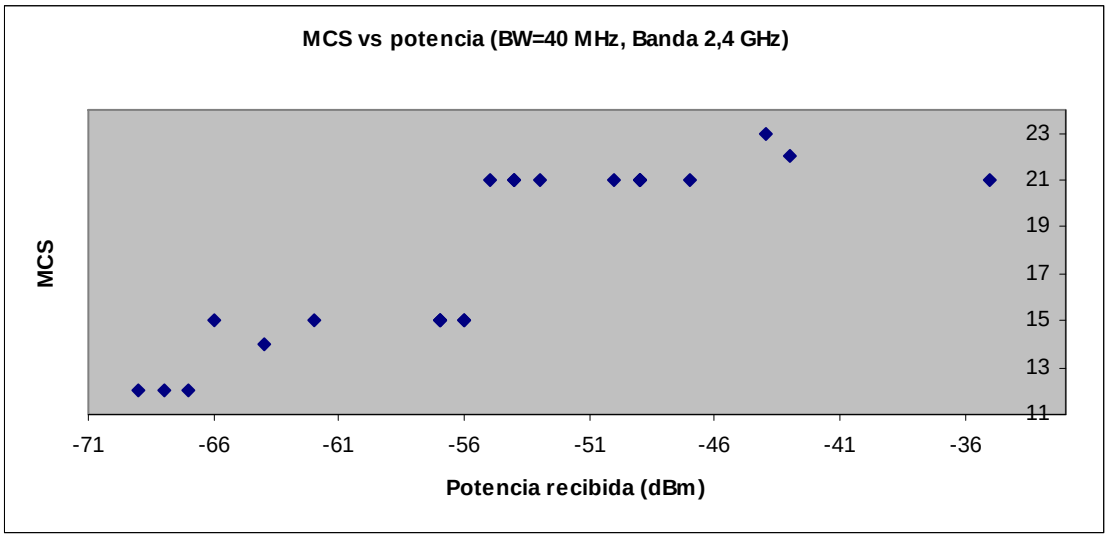

Figura 6.7: MCS vs potencia recibida (BW=40 MHz, Banda 2,4 GHz)

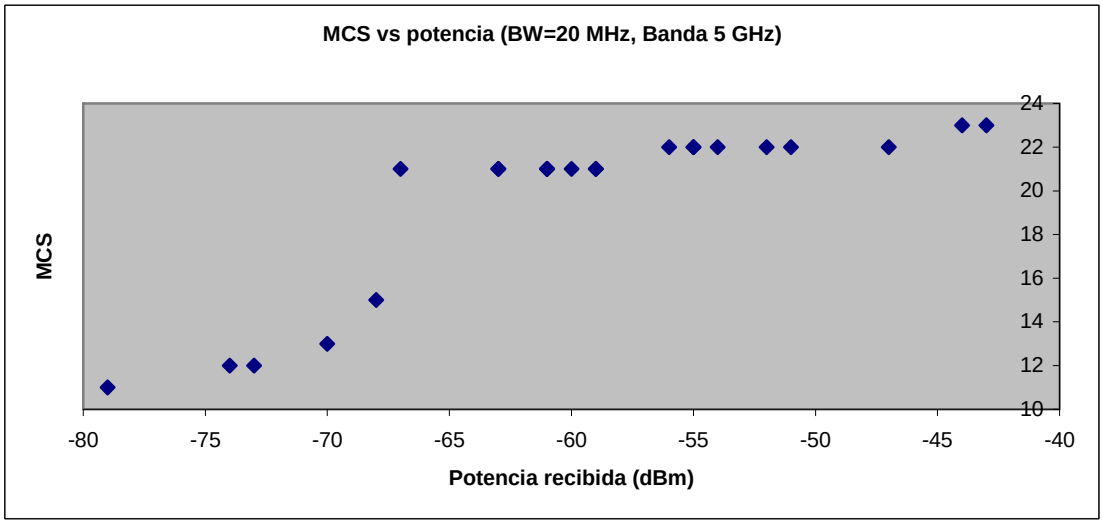

Figura 6.8: MCS vs potencia recibida (BW=20 MHz, Banda 5 GHz)

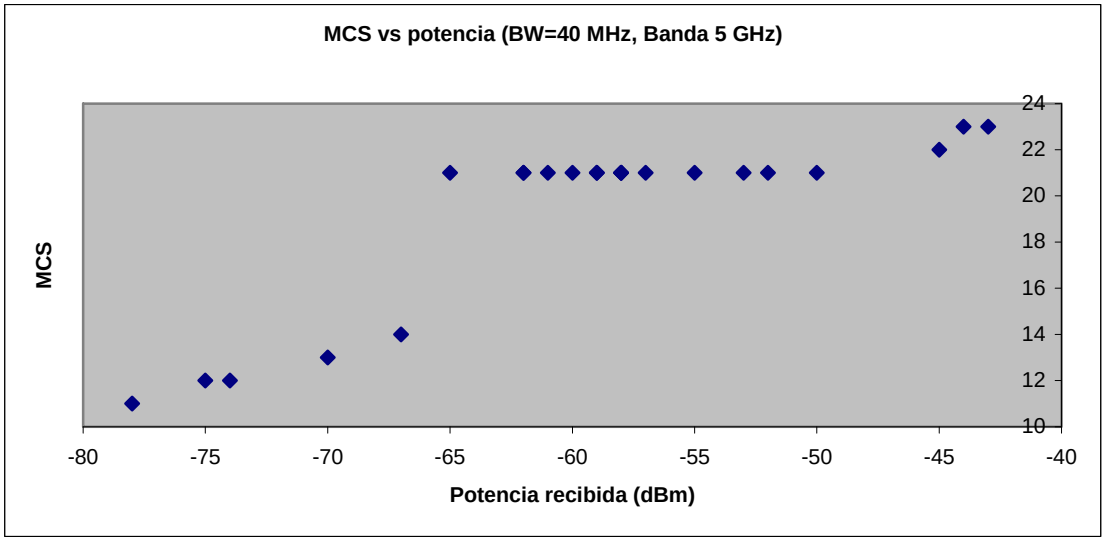

Figura 6.9: MCS vs potencia recibida (BW=40 MHz, Banda 5 GHz)

En términos generales, se puede ver como al aumentar la potencia, se trabaja con un MCS mayor, salvo en casos puntuales en la banda de 2,4 GHz en la cual se producen interferencias con otras redes, lo que puede condicionar la elección del MCS.

Otro aspecto general, es que el máximo valor de MCS que se alcanza en todos los casos es de 23, y es que es no puede transmitirse más de 3 streams espaciales con sólo 3 antenas.

Además, podemos ver como hay valores de MCS en el intervalo [15, 21] que nunca se alcanzan. En todos los casos, siempre se salta del 15 al 21. Este efecto se debe a que para un nivel de potencia recibida determinado, el MCS 21 funciona mejor que los anteriores (20, 19, 18, 17, 16). Esto quiere decir que, aunque el PER sea superior para el MCS 21, el Througput real que se obtiene (Throughtput real= Throughput nominal x (1-PER)) será mayor para el MCS 21 que para los anteriores.

Por último, también relacionado con los MCS, se puede observar en todas estas curvas, como no todos los MCS tienen asociado un rango de potencia del mismo tamaño. Se puede ver claramente, como el MCS 21 abarca un rango bastante amplio de potencias, en comparación con los demás. Este efecto es el mismo que hemos comentado en el párrafo anterior. Para ese rango de potencias, el MCS 21 se comporta mejor que los anteriores, de ahí que se use en todo ese rango.

6.3.2 Throughput vs potencia recibida

Las curvas Throughput vs potencia se pueden observar en las figuras 6.10 y 6.11, 6.12 y 6.13.

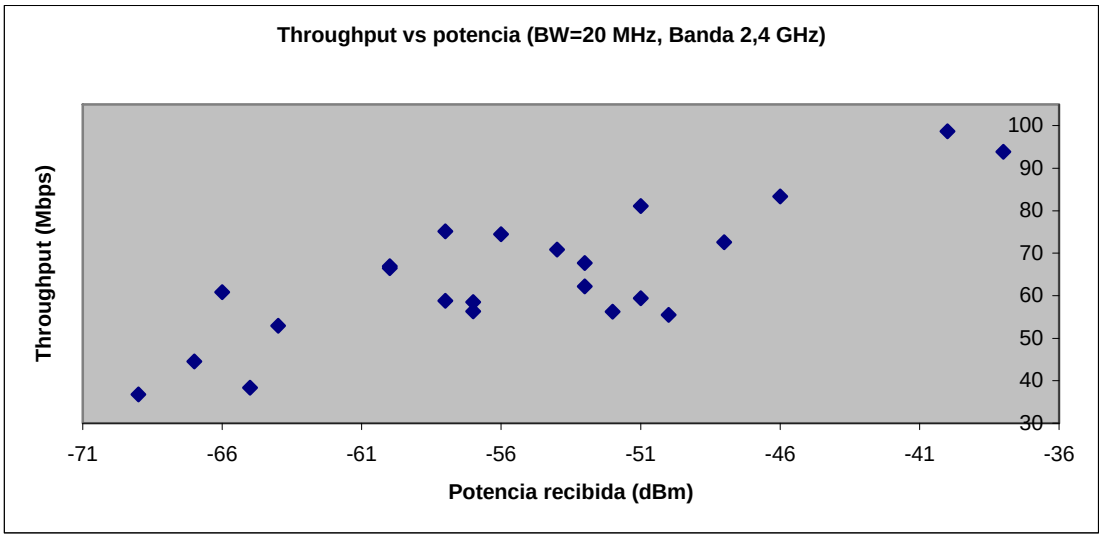

Figura 6.10: Throughput vs potencia recibida (BW=20 MHz, Banda 2,4 GHz)

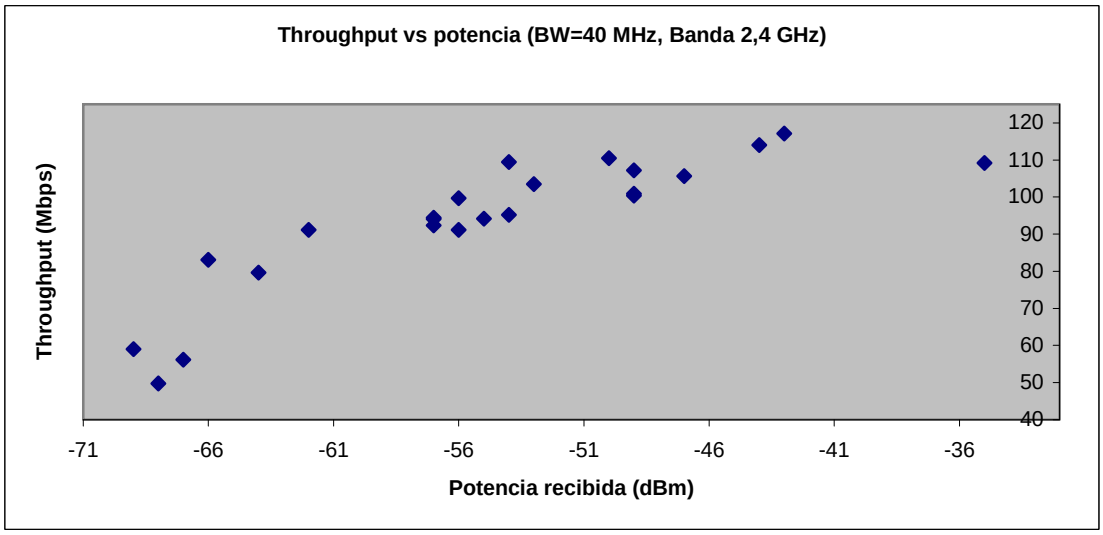

Figura 6.11: Throughput vs potencia recibida (BW=40 MHz, Banda 2,4 GHz)

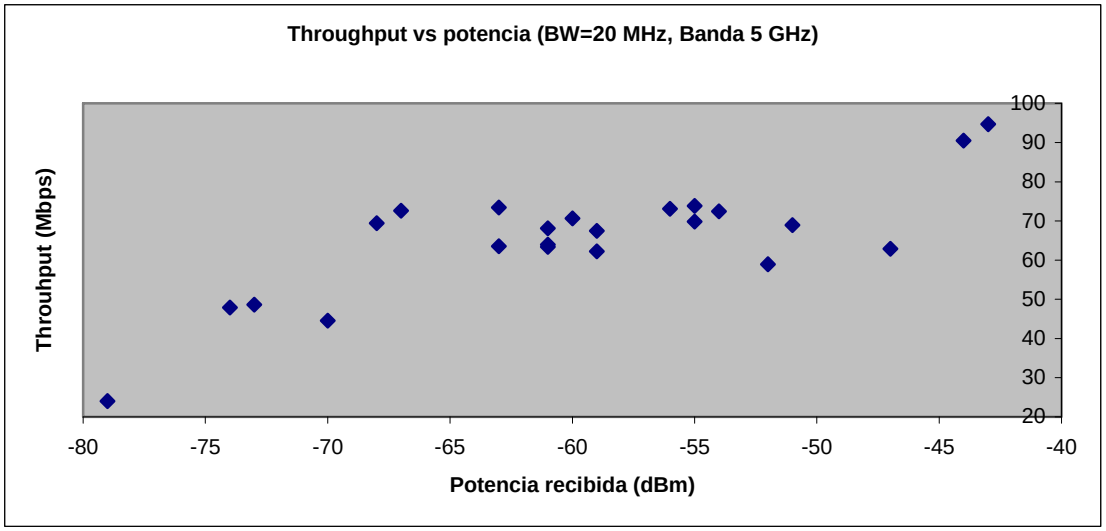

Figura 6.12: Throughput vs potencia recibida (BW=20 MHz, Banda 5 GHz)

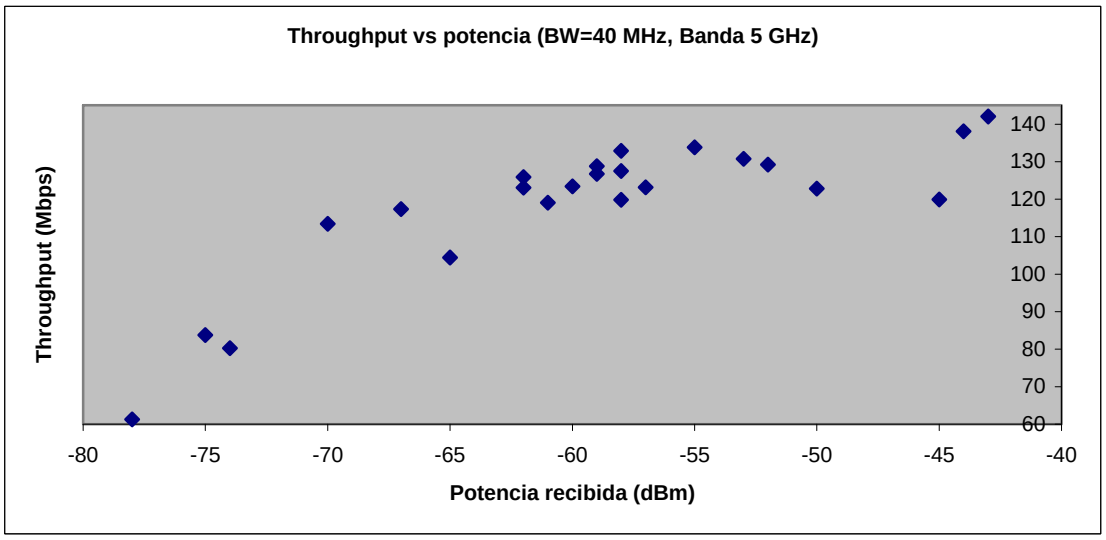

Figura 6.13: Throughput vs potencia recibida (BW=40 MHz, Banda 5 GHz)

Como se vio en el apartado anterior, al aumentar la potencia recibida, aumentaba el MCS y por tanto también lo hará el Throughput. Además podemos ver que no siempre se obtiene el mismo valor de Throughput para un valor determinado de potencia recibida, pero esto es normal, ya que un mismo valor de MCS puede dar lugar a diferentes valores de Throughput, debido a la probabilidad de pérdida de tramas (PER). No hay que olvidar tampoco, que las medidas pueden tener imprecisiones debidas al método y las herramientas utilizadas. Lo importante es que se obtienen valores parecidos de Throughput para un MCS o nivel de potencia dado.

Como era de esperar, los mayores valores de Throughput se obtienen con ancho de banda de canal de 40 MHz, y en la banda de 5 GHz mayor que en la de 2,4 GHz.

También destacar que, la diferencia de Throughput en cada banda, entre canales de 20 y 40 MHz no llega al doble, tal y como indica la teoría. Además como se puede apreciar, se consigue un mayor incremento de Throughput al doblar el ancho de banda del canal en la banda de 5 GHz que en la de 2,4 GHz, algo que es lógico, ya al doblar el

ancho de banda en la banda de 2,4 GHz también estamos aumentando las interferencias con otros canales, cosa que no ocurre en la banda de 5 GHz al no tener ninguna red en nuestro entorno que emita en esta banda.

Por último, es importante decir que los valores de Throughput obtenidos para cada MCS están muy lejos del régimen binario que le corresponde para ese MCS por configuración y que podemos ver en la tabla 3.3. Esto en parte se debe a la sobrecarga del protocolo, a pesar de que se haya conseguido mejor la eficiencia con 802.11n.

En esta sobrecarga debemos incluir el tiempo que se pierde en las retransmisiones de tramas, el tiempo empleado en los procesos de contienda para acceder al medio, el tiempo entre tramas, la cabecera MAC, los intervalos de guarda entre símbolos.

CAPÍTULO 7: CONCLUSIONES Y LÍNEAS DE TRABAJO FUTURAS

7.1 Conclusiones

En este proyecto se ha configurado un pc como punto de acceso a través de software de libre distribución. Después sobre este AP se ha configurado un servicio Hotspot también con software libre. Las contribuciones más destacables son:

- Se ha descrito la mayoría de las funcionalidades de la extensión 802.11n: multiplexación espacial, diversidad espacial, canalización, bandas de frecuencia, intervalo de guarda, modos PLCP, códigos FEC y agregación de tramas, viendo las fortalezas y debilidades de cada una de ellas.

- Se ha evaluado el rendimiento real de algunas de las funcionalidades anteriores mediante una serie de pruebas.

- Se ha aprendido a utilizar una gran cantidad de herramientas open source relacionadas con el tema de redes: servidores DHCP, FTP, web y radius, bases de datos, sniffer, portal captivo y analizador de redes.

7.2 Líneas de trabajo futuras

Aunque la finalización de un Proyecto Fin de Carrera da por cerrado el plan de trabajo diseñado, esto no implica que el trabajo realizado no sea susceptible de ser ampliado.

Algunas de las líneas futuras de este PFC se presentan a continuación:

- Se podría evaluar el rendimiento de un punto de acceso real desde el punto de vista de las funcionalidades que hemos evaluado en nuestro proyecto, para contrastar los resultados con los obtenidos en nuestro caso. De esta forma se podría ver realmente cuan bien funciona nuestro AP comparado con uno real.

- Otra posible ampliación del proyecto, sería utilizar tarjetas 802.11n un poco más avanzadas que las que hemos utilizado, para evaluar algunas otras funcionalidades que ofrece 802.11n que no hemos podido evaluar con las nuestras: beamforming, STBC, unequal modulation, modo PLCP mixto…

- Las 2 ampliaciones anteriores se podrían realizar mientras se ratifica la última modificación de 802.11, 802.11ac. Cuando esta este disponible quizás merecería más la pena evaluar el rendimiento de una red de este tipo, para comprobar si es cierto todo lo que promete: canales de 160 MHz, tasas de frecuencia de hasta 1Gbps y hasta 8 streams espaciales.

ANEXO A: FUNCIONAMIENTO DEL SERVICIO HOTSPOT

En este apartado describiremos el funcionamiento del servicio de Hotspot, certificando su correcta operación.

- Al abrir el explorador e intentar acceder a cualquier página web, Chillispot nos redirecciona a la página de bienvenida del Hotspot. En esta página inicial, podrían ponerse las condiciones de uso del servicio. En nuestro caso, la página de inicio es muy simple como se puede apreciar en la figura A.1.

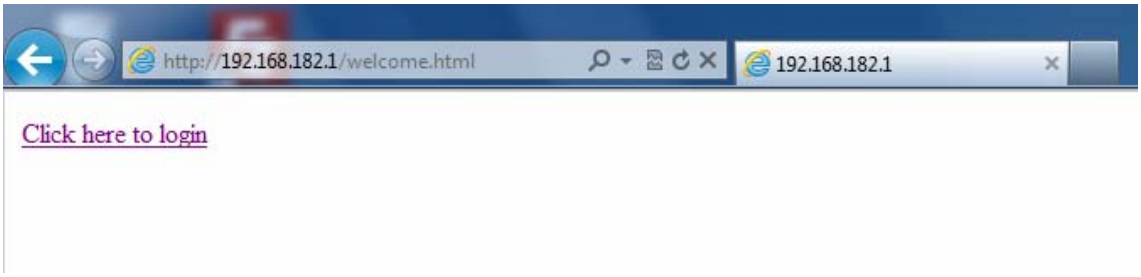

Figura A.1: Página de bienvenida del servicio Hotspot

- El enlace nos conducirá a la página principal de login, pero antes nos aparece un aviso sobre el certificado de seguridad, ya que no ha sido verificado por ninguna entidad de verificación (figura A.2).

Figura A.2: Aviso generado por el explorador

- Pinchamos en *"Vaya a este sitio (no recomendado)"*, y ahora sí, accedemos a la página principal de login.

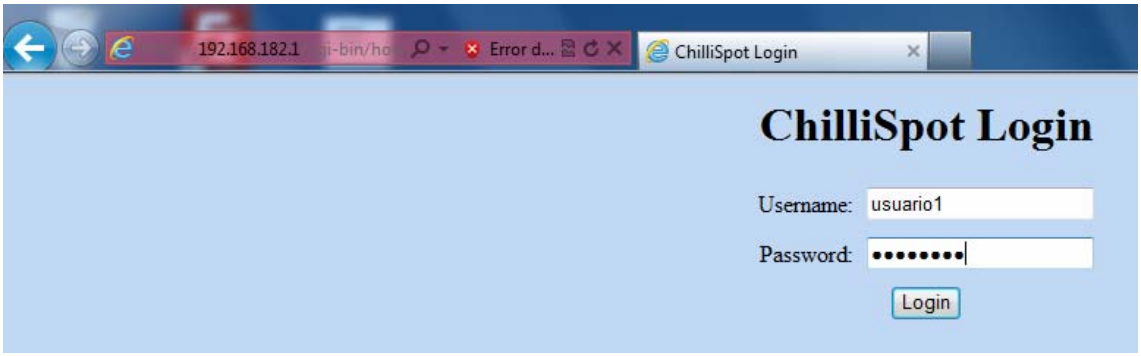

Figura A.3: Página principal de login

- Introducimos uno de los usuarios creados y su contraseña correspondiente y pinchamos en *Login*. El resultado es el que se puede observar en la figura A.4. Ya estamos autenticados y podemos navegar en Internet con total libertad.

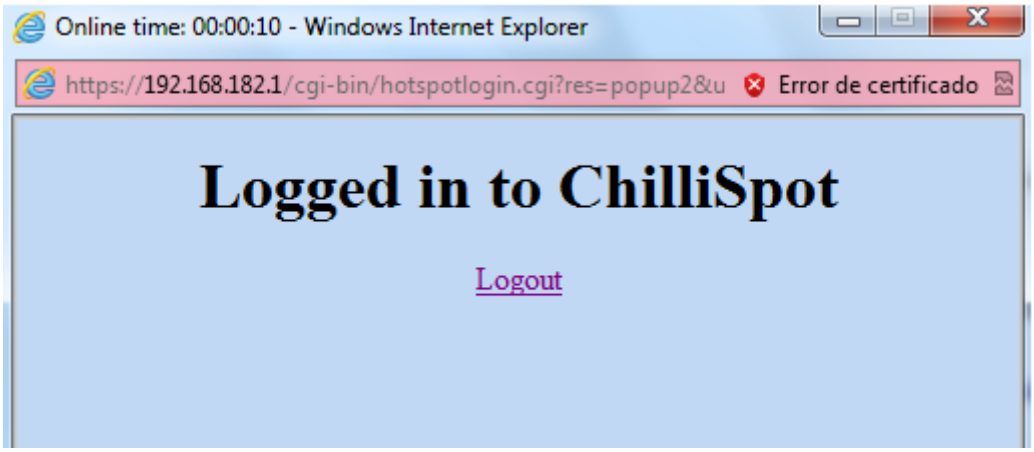

Figura A.4: Indicación de autenticación correcta

- Si queremos terminar la sesión, pinchamos en *Logout*.

Figura A.5: Indicación de cierre de sesión

- En caso de introducir el nombre de usuario y/o la contraseña de forma incorrecta el resultado será el de la figura A.6.

Figura A.6: Indicación de autenticación incorrecta

REFERENCIAS

[1] Matthew S. Gast. Introducción. Redes Wireless 802.11. Madrid: O'Reilly, Pág. 35-37

[2] Cisco Systems. Capítulo 2: Fudamentos de Redes. Academia de Netwoking de Cisco Sytems. Guía de primer año CCNA 1 y 2. Tercera edición. Madrid: Cisco Press, 2004 Pág 45-49

[3] http://standards.ieee.org/getieee802/download/802.15.1-2005.pdf

[4] http://standards.ieee.org/getieee802/download/802.11n-2009.pdf

[5] http://www.ieee.org/index.html

[6] http://standards.ieee.org/getieee802/download/802.11-2007.pdf

[7] http://standards.ieee.org/getieee802/download/802.16-2009.pdf

[8] http://www.tml.tkk.fi/Opinnot/T-109.551/2003/kalvot/UMTS_Tech-Paper.pdf

[9] http://www.nsma.org/conf2008/Presentation/2-1045-Miyahara-LTE_Overview_NMSA%2021March08_final.pdf

[10] http://standards.ieee.org/getieee802/download/802.11b-1999.pdf

[11] http://standards.ieee.org/getieee802/download/802.11a-1999.pdf

[12] http://standards.ieee.org/getieee802/download/802.11g-2003.pdf

[13] Cisco Systems [online]. http://www.cisco.com/web/ES/about/press/2011/11-02-01-vni-trafico-global-datos-moviles-se-multiplicara-por-26.html

[14] http://www.theinternetofthings.eu/internet-of-things-what-is-it%3F

[15] http://www.lmn.net.uk/assets/files/Events/2009Nov26th%20Mobile%20Technologies/FutureMobileTechnology.pdf

[16] http://coitt.es/res/revistas/10%20Wifi.pdf

[17] http://www.abiresearch.com/research/service/wi-fi/

[18] Allain Sibille, Claude Oestges, Alberto Zanella. MIMO From Theory to Implementation. Oxford: Elsevier, 2010

[19] http://mcsindex.com/

[20] Matthew S. Gast. Capítulo 1. Redes Wireless 802.11. Madrid: Anaya, 2004 Pág 60-61

[21] Matthew S. Gast. Capítulo 1. Redes Wireless 802.11. Madrid: Anaya, 2004 Pág 61-64

[22] http://standards.ieee.org/about/get/802/802.3.html

[23] http://blyx.com/public/docs/pila_OSI.pdf

[24] http://electronicstechnician.tpub.com/14092/css/14092_19.htm

[25] Matthew S. Gast. MIMO and the 802.11n PHY. 802.11n. A Survival Guide. Sebastopol: O'Reilly, 2012. Pág 16

[26] David A. Wescott, David D. Coleman, Peter Mackenzie, Ben Miller. High Througput and 802.11n. CWAP. Certified Wireless Analysis Professional. Office Study Guide. Exam PW0-270. Indianapolis: Cybex, 2011. Pág 592.

[27] Matthew S. Gast. Channel, Framing and Coding. 802.11n. A Survival Guide. Sebastopol: O'Reilly, 2012 Forward Error Codes in 802.11n

[28] Matthew S. Gast. Advanced PHY Features for Perfomance. 802.11n. A Survival Guide. Sebastopol: O'Reilly, 2012 Pág 38

[29] Matthew S. Gast. Advanced PHY Features for Perfomance. 802.11n. A Survival Guide. Sebastopol: O'Reilly, 2012 Pág 33-37

[30] http://linuxwireless.org/en/users/Drivers/ath9k

[31] http://www.atheros.com/

[32] http://dl.acm.org/citation.cfm?id=1640557

[33] Matthew S. Gast. Advanced MAC Features for Interoperability. 802.11n. A Survival Guide. Sebastopol: O'Reilly, 2012 Pág 64-66

[34] http://searchmobilecomputing.techtarget.com/definition/CCMP

[35] http://linuxwireless.org/en/users/Documentation/hostapd

[36] http://www.isc.org/software/dhcp/

[37] http://www.proftpd.org/

[38] http://filezilla-project.org/

[39] http://www.metageek.net/products/inssider/

[40] http://www.wireshark.org/

[41] http://www.chillispot.info/

[42] http://httpd.apache.org/

[43] http://freeradius.org/

[44] http://www.mysql.com/

[45] http://wireless.kernel.org/en/users/Documentation/iw

[46] http://www.tp-link.es/products/details/?categoryid=1683&model=TL-WDN4800#over

[47] http://www.qca.qualcomm.com/technology/technology.php?nav1=47&product=88

[48] http://www.dlink.es/