TRABAJO DE FIN DE CARRERA

TÍTULO DEL TFC: Cómo conocer el uso actual de las redes WLAN basadas en IEEE 802.11

TITULACIÓN: Ingeniería Técnica de Telecomunicaciones, Especialidad Telemática

AUTOR: Xavier Tena Carbonell

DIRECTOR: Eduard Garcia Villegas

FECHA: Miércoles 4 de Diciembre 2013

Título: Maqueta de TFC/PFC

Autor: Xavier Tena Carbonell

Director: Eduard Garcia Villegas

Fecha: Miércoles 4 de Diciembre 2013

Resumen

Los objetivos de este trabajo son el análisis de las redes inalámbricas bajo los estándares IEEE 802.11a, 802.11b 802.11g y 802.11n. Se estudian distintos parámetros y características para posteriormente hacer un estudio estadístico sobre su uso actual en nuestro entorno. Los parámetros a estudiar son: estándares utilizados, velocidades soportadas por los dispositivos, velocidades requeridas por los AP, seguridad soportada, tipo de encriptación, tipos de autenticación, canales utilizados, tipología de las redes inalámbricas, fabricantes de hardware, convivencia entre estándares y eficiencia de las tramas de gestión

La metodología del trabajo ha consistido en la captura de tramas IEEE 802.11abgn con el software y hardware específico. Las herramientas hardware han sido dispositivos portátiles y antenas capaces de capturar en las dos bandas (2GHz y 5GHz). En cuanto al software, Kismet ha sido la aplicación de captura y se ha creado una herramienta software programada en Java, encargada de realizar el análisis de todas las características mencionadas.

Los resultados obtenidos, han permitido obtener una visión global del estado actual de las redes 802.11abgn y la convivencia entre ellas.

The objectives of this work are the analysis of wireless networks based on IEEE 802.11a, 802.11b 802.11g and 802.11n standards. We study various parameters and characteristics to later carry out a statistical study on its current utilization. The parameters studied are: standards used, bit rates supported by the devices, rates required by APs, security features supported, use of frequency channels, type of wireless networks, hardware manufacturers, coexistence between standards and efficiency of the management frames.

The methodology of the work consisted in sniffing IEEE 802.11abgn frames with a specific software and hardware. Hardware tools were portable devices and dual band antennas (2GHz and 5GHz). As for the software, Kismet was the packet sniffing application the output of which was analyzed by a custom-made Java application, responsible for providing statistics about the aforementioned network configuration parameters and features.

The results allowed us to obtain an overview of the current state of 802.11abgn networks and the coexistence issues that arise.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

INTRODUCCIÓN

Las conexiones inalámbricas se han popularizado fuertemente los últimos años en nuestras vidas. Unos de los "culpables" de este auge han sido los *smartphones, tablet PCs* y los ordenadores portátiles desde los que se accede frecuentemente a Internet mediante diferentes tecnologías de acceso inalámbrico. Esta gran cantidad de dispositivos inalámbricos deben ser dirigidos de la manera más óptima posible.

Para asegurar el correcto funcionamiento de todos estos dispositivos inalámbricos se creó el estándar *IEEE 802.11,* especificando sus normas de funcionamiento en una WLAN. Actualmente conviven distintas revisiones del estándar original. Los estándares que se pueden encontrar en mayor cantidad son 802.11a, 802.11b, 802.11g y 802.11n. Cada uno de ellos presenta mejoras respecto al estándar original en cuanto a velocidad y seguridad.

Sin embargo, la aparición de nuevos estándares WLAN 802.11 no significa la actualización o substitución del parque de dispositivos ya existentes. La convivencia entre estos estándares, antiguos y nuevos, provoca que dispositivos modernos y más eficientes, que podrían ir a una mayor velocidad tengan que reducir esta velocidad para poder intercambiar información en el medio. En redes bajo el estándar 802.11g, la presencia de nodos bajo el estándar 802.11b reduce significativamente la velocidad de transmisión. Lo mismo pasa entre 802.11b y 802.11n y entre 802.11g y 802.11n.

Teniendo en cuenta este conflicto de convivencia entre los estándares, en este trabajo se tiene como uno de los objetivos principales, estudiar el uso actual del estándar 802.11b en distintos escenarios reales para sacar conclusiones sobre las limitaciones que provocan los dispositivos bajo este estándar en convivencia con dispositivos más modernos.

Otra fuente de conflictos entre redes WLAN proviene del escaso espectro disponible y del hecho de que se utilizan bandas sin licencia. Los dispositivos inalámbricos se deben configurar para trabajar en unas determinadas frecuencias. Estas frecuencias se agrupan para formar canales. Para que no existan problemas de interferencias, los dispositivos cercanos deben configurarse en canales suficientemente alejados. Estos datos se tendrán en cuenta en el estudio realizado para comprobar el buen uso de las configuraciones, o descubrir oportunidades de mejora en el uso de los recursos radio.

Otro de los objetivos de este trabajo es el análisis de la seguridad de las redes inalámbricas. La seguridad en las redes inalámbricas es uno de los problemas más graves de este tipo de redes. Existen distintos tipos de mecanismos de seguridad según el estándar utilizado, es decir, según la antigüedad de los dispositivos con los que se trabaja, algunos más vulnerables que otros.

Con el fin de obtener información sobre el estado actual de las redes WLAN IEEE 802.11 con respecto a la problemática que se ha mencionado

anteriormente, se ha realizado una campaña de medidas consistente en una serie de capturas de tráfico reales de redes inalámbricas, con un software específico, de libre distribución, para este tipo de tareas y se ha desarrollado una aplicación Linux, basada en el lenguaje de programación *Java*, para el análisis de las capturas.

Los escenarios reales en los que se ha realizado el estudio han sido:

- **Zonas Residenciales (*Res*):** distritos de ciudades densamente poblados en el área metropolitana de Barcelona.
- **Zonas Comerciales (*Com*):** Calles turísticas con una cantidad considerable de edificios de oficinas y zonas industriales.
- **Zonas *HotSpot* (*HotS*):** Campus universitarios y centros comerciales.

Gracias a la información que se extrae de las capturas realizadas en los distintos escenarios, se hace un análisis de los siguientes datos:

- Estándares utilizados.
- Velocidades soportadas por los dispositivos.
- Velocidades requeridas por los AP.
- Seguridad soportada.
- Tipo de encriptación.
- Tipos de autenticación.
- Canales utilizados.
- Tipología de las redes inalámbricas.
- Fabricantes de hardware.
- Fabricantes de los AP.
- Fabricantes de los Clientes.
- Convivencia entre estándares.
- Eficiencia de las tramas de gestión.

La elección de estos tipos de escenarios se debe a las distintas configuraciones y características que se prevén para una WLAN en estos diferentes entornos.

En el primer escenario, convivirán mayoritariamente AP de características similares en gran cantidad debido a que cada vivienda o local con conexión a internet, dispondrá de un AP optimizado para su uso doméstico aunque con configuraciones heterogéneas debido a su gestión totalmente descentralizada.

En el segundo escenario, muy parecido al anterior, se detectarán AP con configuraciones empresariales. Estas incluyen una mayor seguridad y configuraciones más complejas a las de uso doméstico.

En el último escenario, se encontrarán AP distribuidos de forma más eficiente con configuraciones homogéneas más elaboradas y conviviendo con redes inalámbricas de ambas bandas (2,4GHz y 5GHz).

Lo que se espera obtener de este estudio es una visión global de la situación actual respecto al uso de las tecnologías de redes de área local inalámbricas basadas en el IEEE 802.11. El uso de los distintos estándares, la seguridad en las redes inalámbricas, la convivencia entre ellos y la compatibilidad entre todos los dispositivos.

Este documento está estructurado de la siguiente manera:

A continuación, en el CAPÍTULO 1 se proporcionan las bases sobre la tecnología 802.11, desde su historia hasta las últimas novedades.

En el CAPÍTULO 2, se expone el estudio realizado. Se define el proceso, las herramientas, el funcionamiento y sus características más relevantes.

En el CAPÍTULO 3, se analizan los resultados obtenidos en el estudio.

El CAPÍTULO 4 y definitivo, contiene las conclusiones del estudio realizado.

Al final de este documento, en LOS ANEXOS se ofrece un glosario con la definición de los acrónimos y las abreviaciones que aparecerán a lo largo de todo el documento. También se adjunta la metodología del uso de la aplicación *Kismet* y las imágenes de los distintos escenarios donde se han realizado las capturas.

CAPÍTULO 1. LA FAMILIA TECNOLÓGICA DEL IEE802.11

La especificación IEEE 802.11 es un estándar internacional que define las características de una red de área local inalámbrica (WLAN). Por el uso indebido de los términos (y por razones de marketing) el nombre del estándar se confunde con el nombre de la certificación. Una red Wi-Fi es en realidad una red que cumple con el estándar 802.11. Wi-Fi es el nombre de la certificación otorgada por la WECA (Actualmente Wi-Fi Alliance).

En este Apartado se define la historia y las bases teóricas del estándar 802.11 y sus versiones, para entender el funcionamiento y el procedimiento del estudio realizado.

1.1. Red de Área Local Inalámbrica (WLAN)

Una **red de comunicaciones** es un conjunto de medios técnicos que permiten el intercambio de datos entre dispositivos a través de un medio (aire, vacio, cable de cobre, fibra óptica, etc.).

En concreto, una **WLAN** es una red de comunicaciones inalámbrica flexible, que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas.

Un **punto de acceso (AP)** es un puente entre la red inalámbrica y otra red, que se encarga de realizar las conversiones de trama pertinentes.

El bloque mínimo de una red WLAN es el **BSS** (Basic Service Set) y se identifica mediante un **BSSID** (*BSS IDentifier*) y puede configurarse en dos modos [1]:

- **Independiente o *ad-hoc* (IBSS):** Las estaciones se intercomunican directamente entre ellas. Es la forma más simple de organizar una red 802.11. El conjunto de estaciones de una red *ad-hoc* forman un IBSS (Independent Basic Service Set).
- **Infraestructura o gestionado (BSS):** Se caracteriza por la presencia de un AP como mínimo. En este caso se conoce también como BSS la cobertura del AP (que es quien gestiona la red). El BSSID es la dirección MAC del AP.

  Un **ESS** (Extended Sevice Set) es un conjunto de uno o más BSS que funcionan como un único BSS para la capa lógica de red (N2 LLC). Este conjunto se identifica mediante una cadena de caracteres llamada ESSID (*ESS Identifier*) definida por el administrador. Este ESSID es a veces llamado simplemente SSID o "nombre de la red". Los distintos BSS del ESS pueden trabajar en el mismo canal o en distintos canales para ampliar la capacidad de la red.

1.2. Estándares y su historia

El estándar '***IEEE 802.11'*** define el uso de los dos niveles inferiores de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN. Los protocolos de la rama 802.x definen la tecnología de redes de área local y redes de área metropolitana.

La familia 802.11 consiste en una serie de técnicas de modulación Half-duplex que usan el mismo protocolo a través del aire.

IEEE 802.11 tiene sus orígenes en 1985 cuando la comisión Federal de Comunicaciones de EE.UU. lanzó la banda ISM para su uso sin licencia.

En 1991 NCR Corporation/AT&T (actualmente Alcatel-Lucent y LSI Corporation) inventaron el precursor de 802.11 en Holanda. Los inventores intentaron usar inicialmente la tecnología para sistemas de cajeros. Más tarde, el primer producto sin cables fue vendido bajo el nombre de WaveLAN con tasas de transferencia de 1 y 2Mbps.

A continuación se dan unas bases teóricas e históricas de la evolución del estándar IEEE 802.11 desde sus inicios hasta la actualidad. Los siguientes estándares serán los analizados en este estudio [2].

1.2.1. El inicio de 802.11

La versión original del estándar IEEE 802.11 fue publicado en 1997 y reconocido en 1999 pero hoy en día ha quedado obsoleto. En él se especifican dos tasas de transferencia, 1 y 2 Mbps, y Direct Sequence Spread Spectrum (DSSS) operando a 1 y 2Mbps. Usaban transmisiones de microondas en la banda *Industrial Scientific and Medical (ISM)* de 2,4GHz.

1.2.2. 802.11a

Fue la corrección a las especificaciones de 802.11 que definió los requerimientos para el sistema de comunicación, capa física, con O*rtogonal Frequency Division Multiplexing* (OFDM) de 52 portadoras. Inicialmente fue diseñada para soportar comunicaciones inalámbricas en el rango de frecuencias sin licencia de 5-6GHz regulado en EEUU.

Originalmente descrita como cláusula 17 de la especificación de 1999, ahora se define en la cláusula 18 de 2012 y proporciona protocolos que definen tasas de transmisión de 6 a 54Mbps.

802.11a utiliza el mismo protocolo de enlace de datos y el mismo formato de trama que el 802.11 original, opera en la banda de 5GHz con una tasa de transferencia máxima de 54Mbps que realmente se reduce a un throughput máximo de unos 20Mbps. Originalmente ofrecía 12 canales de frecuencia no solapados, 8 usados en interior y 4 para conexiones punto a punto en exterior.

De las 52 sub-portadoras OFDM, 48 son para datos y 4 portadoras piloto. Las sub-portadoras poseen una separación de 312,5 KHz entre ellas y pueden ser moduladas digitalmente con BPSK, QPSK, 16QAM o 64 QAM.

Las ventajas de 802.11a son:

- La banda de 5GHz no está tan usada o llena como la banda de 2,4GHz por parte de las WLAN Wi-Fi.
- Ausencia de los sistemas de interferencia de la banda de 2,4GHz (hornos microondas, teléfonos inalámbricos, bluetooth, monitores de bebes...)
- Las frecuencias más altas permiten la construcción de antenas más pequeñas con una mayor ganancia del sistema.
- OFDM tiene ventajas de propagación en entornos de trayectos múltiples (rebotes).

La principal desventajas es:

- El radio de cobertura de la banda de 5GHz es significativamente menor que el de 2,4GHz ya que las señales son fácilmente absorbidas por muros u otros objetos sólidos.

Los productos con 802.11a empezaron a venderse tarde ya que eran más difíciles de fabricar y muchos países habían abierto solo parcialmente la banda ISM de 5GHz, imponiendo serias restricciones al convivir con sistemas de radar. La primera generación de productos tuvo problemas. Cuando se empezó a vender la segunda generación de productos, ya se había extendido el uso de productos a menor coste del estándar 802.11b. Sin embargo más adelante fue implantado sobre todo en el área de trabajo de las empresas.

1.2.3. 802.11b

Fue la corrección a las especificaciones de 802.11 que extendió la tasa máxima de transferencia hasta 11Mbps usando la misma banda de 2,4GHz. Esta especificación fue comercializada como Wi-Fi y fue implementada por todo el mundo. La corrección fue incorporada en el estándar IEE 802.11b-1999.

802.11b tiene una tasa de transferencia máxima de 11Mbps y utiliza el mismo mecanismo de acceso al medio CSMA/CA que el 802.11 original. En la práctica el máximo throughtput es de 5,9Mbps en TCP y 7,1Mbps en UDP.

La gran aceptación de 802.11b fue gracias al incremento de la velocidad (respecto al 802.11) y al reducido coste de fabricación.

Los primeros productos con 802.11b aparecieron a mediados de 1999. El primer ordenador que lo incorporó fue el Apple iBook de manera opcional.

Para la capa física se utiliza CCK (Complementary Code Keying).

1.2.4. 802.11g

Fue la corrección a las especificaciones de 802.11 que aumentó la tasa máxima de transferencia hasta 54Mbps usando la misma banda de 2,4GHz como 802.11b. En la práctica el throughput máximo es de 28Mbps.

El estándar 802.11g es totalmente compatible con 802.11b aunque la presencia de nodos bajo el estándar 802.11b reduce significativamente la velocidad de transmisión.

El esquema de modulación en 802.11g es *Orthogonal Frequency-Division Multiplexing* (OFDM) copiado de 802.11a con tasas de transmisión de hasta 54Mbps. Vuelve a CCK (igual que en 802.11b) para tasas de transmisión de 5,5 y 11Mbps y DBPSK/DQPSK+DSSS para 1 y 2Mbps.

Antes de la aceptación del estándar, sobre enero del 2003, ya fue aceptado por los usuarios y sobre verano del mismo año se fabricaron dispositivos dual-banda y tri-banda capaces de soportar 802.11a/b/g en un solo adaptador inalámbrico o Acces Point.

1.2.5. 802.11n

Durante los siguientes años, se publicaron otras correcciones a los estándares anteriores para finalmente crear un documento (802.11-2007) en 2007 donde se recogieron todas estas correcciones.

802.11n fue aprobada y publicada en 2009. Es una corrección del documento 802.11-2007 que mejora los estándares 802.11 anteriores.

802.11n trabaja en las dos bandas de frecuencias de 2,4 y 5GHz aunque este último es opcional. La tasa máxima de transferencia es de 600Mbps. A la práctica se puede llegar a los 300Mbps.

Añade antenas Multiple-Input Multiple-Output (MIMO), mejoras de seguridad, *frame agregation* a la capa MAC y canales de 40MHz en la capa física.

- **MIMO** es una tecnología que aprovecha fenómenos físicos como la propagación multicamino para incrementar la tasa de transmisión y reducir la tasa de error. MIMO aumenta la eficiencia espectral por medio de la utilización del dominio espacial.
- **Canales de 40MHz**. Duplica el tamaño de los canales y proporciona dos veces más la tasa de transmisión. Sólo se puede usar en la banda de 5GHz o en la de 2,4GHz cuando no interfiera con otro 802.11 u otra señal en esta banda (p.ej. Bluetooth).
- **Frame agregation** permite enviar dos o más tramas de datos en un solo acceso al medio. Se definen dos tipos de agregación de tramas:
  - **MAC Service Data Unit MSDU.**
  - **MAC Protocol Data Unit MPDU.**

Se empaquetan múltiples MSDU o MPDU juntos para reducir las cabeceras y parte de ellos a través de múltiples tramas.

En la **Tabla 1.1** se resumen los datos más relevantes mencionados en este Apartado sobre las características de los cuatro estándares estudiados en este trabajo.

Tabla 1.1 Características IEEE 802.11

Características	802.11	802.11a	802.11b	802.11g	802.11n
Año de estandarización	1997	1999	1999	2003	2009
Transferencia en capa física	2 Mbps	54 Mbps	11 Mbps	54 Mbps	600Mbps
Transferencia de datos	1,2 Mbps	20 Mbps	5,9 Mbps	28 Mbps	300Mbps
Banda de frecuencia	2,4 GHz	5 GHz	2,4 GHz	2,4 GHz	2,4 GHz y 5GHz
Capa física	IR FHSS DSSS	OFDM	DSSS	DSSS OFDM	OFDM FHSS DSSS
Control de Acceso al Medio	CSMA/CA	CSMA/CA	CSMA/CA	CSMA/CA	CSMA/CA
Orientado a conexión	NO	NO	NO	NO	NO
Modulación	DBPSK DQPSK	BPSK QPSK 16-QAM 64-QAM	CCK	CCK DBPSK DQPSK	BPSK QPSK 14-QAM 64-QAM

1.3. Evolución de la seguridad en 802.11

Las redes *Wireless LAN* utilizan el aire como medio compartido de transmisión, por lo que cualquiera puede acceder al mismo medio por el que estén viajando las tramas. Esto hace que las WLAN sean especialmente vulnerables a una serie de ataques informáticos.

A continuación se exponen los principales mecanismos de seguridad utilizados por los distintos estándares.

1.3.1. Wired Equivalent Privacity (WEP)

Fue introducido como parte del estándar original 802.11. Pretendía dar a las redes inalámbricas el mismo nivel de seguridad básico que tienen las redes cableadas. Para autenticarse en un AP, el cliente debe demostrar que conoce la clave de 10 o 26 dígitos hexadecimales.

Existen dos métodos de autenticación:

1.3.1.1. Clave compartida:

1. El cliente manda una petición de autenticación al AP.
2. El AP responde con un texto sin cifrar.
3. El cliente encripta el texto usando la clave WEP y lo envía al AP.
4. El AP desencripta la respuesta. Si es correcto responde de nuevo al cliente para realizar asociación.

Después de la autenticación y asociación se utiliza la clave WEP para encriptar las tramas de datos usando RC4.
El inconveniente del proceso de autenticación por clave compartida es que un equipo externo puede capturar este proceso de autenticación y descubrir cuál es la clave WEP [3].

1.3.1.2. Autenticación abierta

En este proceso, más recomendado, no hay ningún tipo de intercambio inicial. Aún así, con este método de autenticación abierta, se demostró que un equipo informático básico podía descifrar la clave WEP, capturando suficientes paquetes cifrados, mediante herramientas que combinan ataques por estadística con ataques de fuerza bruta.

1.3.2. Wi-Fi Protected Access (WPA)

Al comprobarse que se podía descubrir la clave WEP en unos pocos minutos por un ordenador básico, se desarrolló el estándar de seguridad avanzada 802.11i. Su desarrollo fue lento y se presentó en 2003 una versión reducida del estándar 802.11i, el llamado WPA (Wi-Fi Protected Acces) [4] [5].

WPA podía ser implementado, en las tarjetas de red anteriores, con una actualización de los firmwares de los dispositivos. Para los AP, la actualización era más complicada.

WPA añade varios mecanismos nuevos de cifrado. Uno de ellos es *Temporary Key Integrity Protocol* (TKIP). TKIP utiliza una *semilla* inicial de 128 bits compartida por todos los usuarios y los puntos de acceso. Después, esa clave temporal se combina con la dirección MAC del usuario y se le añade un vector de inicialización de 16 bits para producir la clave que cifrará los datos. Mediante este proceso cada usuario utilizará diferentes claves para la encriptación. TKIP

fuerza por defecto un cambio de las claves entre el usuario móvil y el punto de acceso para cada paquete de información transmitida y aplica un algoritmo de "Hash" a los valores del vector de inicialización. Es decir, se cifra dicho vector, por lo que es más complicado averiguar su valor. Además TKIP se encarga de cambiar la clave compartida entre punto de acceso y cliente cada cierto tiempo, para evitar ataques que permitan revelar la clave. El cambio de la clave de cifrado está sincronizado entre el usuario y el punto de acceso. El inconveniente es que este proceso supone un aumento del *Overhead* de la comunicación. El esquema de encriptación sigue siendo RC4.

Existen dos modos de autenticación diferentes WPA-PSK (Pre Shared Key) y WPA EAP (*Extensible Autentication Protocol*) junto a IEEE 802.1X.

- **WPA-PSK:** Para entornos personales, como usuarios residenciales y pequeños comercios. La PSK es conocida por todas las estaciones del medio además del AP. No se utiliza para encriptar los paquetes de datos. Se construye la llamada PMK (*Primary Master Key*) a partir de la PSK y un proceso de modificación. Una vez obtenida la PMK comienza el proceso de autenticación con el AP que se denomina *4-Way Handshake.* De este proceso de autenticación, tanto la estación como el AP generan la PTK (Pairwise Key Expansion) y la GTK (Group Temporal Key) utilizados para cifrar los datos. Siendo ambas diferentes en cada sesión.

- **WPA-EAP:** Para entornos empresariales junto con mecanismos IEEE802.1X. EAP es utilizado para el transporte extremo a extremo para los métodos de autenticación entre el dispositivo de usuario y el punto de acceso. IEEE802.1X es utilizado como marco para encapsular los mensajes EAP en el enlace radio. El conjunto de estos dos mecanismos junto con el esquema de cifrado forman una fuerte estructura de autenticación, que utiliza un servidor de autenticación centralizado, como por ejemplo RADIUS.

1.3.3. 802.11i WPA2

El estándar definitivo fue ratificado en Junio de 2004. El cambio más importante que introduce es el esquema de encriptación. Se pasa a utilizar el algoritmo AES-CCMP ("*Advanced Encryption System* **-** *Counter Cipher Mode with block chaining Message authentication code Protocol*"), un cifrado de clave simétrica que utiliza grupos de bits de longitud fija.

1.4. Diferentes capas físicas

La capa física (Nivel 1 del modelo OSI) proporciona los medios mecánicos, eléctricos, funcionales y de procedimiento para activar, mantener y desactivar conexiones físicas en la transmisión de información entre entidades de la Capa Enlace. [6] [7]

A continuación se describen las características de distintas implementaciones de la capa física utilizadas por las distintas versiones 802.11.

1.4.1. Direct Sequence Spread Spectrum (DSSS)

En esta técnica se multiplica cada bit original por una secuencia de 11 chips, llamado código Barker. Es una secuencia rápida diseñada para que aparezca aproximadamente la misma cantidad de 1 que de 0. El receptor debe conocer la secuencia para poder recomponer la señal. De esta manera, si parte de la señal se ve afectada por interferencias, el receptor puede reconstruir la información a partir de la señal recibida.

Esta técnica es utilizada por el estándar 802.11b, 802.11g y 802.11n.

1.4.2. Complementary Code Keying (CCK)

Esta técnica se creó para reemplazar el uso del código Barker en redes digitales a cortas distancias que logran superar los 2Mbps. Se basa en la técnica DSSS.

Esto es debido a la secuencia más corta en CCK (8 chips frente a los 11 del código Barker). Permite codificar directamente varios bits de datos en un solo chip al utilizar ocho secuencias de 64 bits. Por lo tanto, el método CCK puede alcanzar una velocidad máxima de 11Mbps al codificar 8 bits de datos.

Esta técnica es utilizada por el estándar 802.11b y 802.11g cuando trabaja a las velocidades de 802.11b.

1.4.3. Frequency Hopping Spread Spectrum (FHSS)

En esta técnica se divide el canal en sub-canales de 1MHz. Se define una secuencia de saltos rápidos de frecuencia y se transmite la información en una determinada frecuencia durante un intervalo de tiempo llamada *dwell time* e inferior a 400 ms.

En la trama *Beacon* se asigna a cada estación una secuencia de saltos. Esta secuencia es pseudoaleatória. Si se mantiene la sincronización en los saltos de frecuencias se consigue que, aunque en el tiempo se cambie de canal físico, a nivel lógico se mantiene un solo canal por el que se realiza la comunicación.

Esta técnica es utilizada por el estándar 802.11b.

1.4.4. Orthogonal Frequency Division Multiplexing (OFDM)

Esta técnica consiste en enviar un conjunto de ondas portadoras de diferentes frecuencias, donde cada portadora transporta información.

Se aprovechan los ceros de una soportadora para centrar un máximo de otra sub-portadora. De esta forma los sub-canales que se forman se superponen pero no se interfieren.

Esta técnica es utilizada por los estándares 802.11a, 802.11g y 802.11n.

1.5. Nivel de Acceso al Medio

El nivel de acceso al medio debe disponer de medios para solucionar problemas relacionados con los errores en la transmisión. Para ello, se dividen los datos suministrados por el nivel de red en “tramas” de datos, formados por unos cientos o miles de bytes, que son transmitidos de forma secuencial y que llevan asociado un acuse de recibo que también gestiona la capa de acceso al medio.

Puesto que el nivel físico no interpreta las tramas (únicamente los procesa como información que enviar o recibir), es el nivel de acceso al medio el que debe poner inicio y fin a las tramas que envía o recibe, asignando secuencias especiales de bits al inicio y al final de cada trama que sean fácilmente reconocibles. En caso de pérdida o mala transmisión de una trama, la capa de enlace de datos puede solicitar su reenvío aunque el procedimiento debe ser lo suficientemente fiable como para que no lleguen tramas duplicadas al receptor.

Otro problema que debe resolver la capa de acceso al medio es el supuesto en que un emisor veloz pueda llegar a saturar a un receptor más lento. Para ello se incorporan mecanismos de control de tráfico que informan al emisor del espacio de almacenamiento temporal (*buffer*) de que dispone el receptor en un momento dado.

En las transmisiones inalámbricas, el medio de transmisión es el aire. Por lo tanto, se trabaja con un medio compartido ya que todos los dispositivos que intercambian datos de forma inalámbrica utilizan el mismo medio.

1.5.1. Distribuida (DCF)

DCF utiliza el mecanismo de control de acceso al medio CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) con acuse explícito de recibo mediante tramas de reconocimiento (ACK) enviadas por el receptor tras una recepción correcta y un acceso opcional mediante el intercambio RTS/CTS. Usa comunicación asíncrona entre estaciones.

Este protocolo de bajo nivel permite que múltiples estaciones utilicen un mismo medio de transmisión. Su mecanismo se basa en:

- **Carrier Sense:** El dispositivo que desea transmitir, primero escucha el medio para determinar si otro dispositivo está transmitiendo o no.
- **Collision Avoidance:** Si se escucha a otro dispositivo transmitiendo, se espera un número de slots temporales aleatorio escogido en el rango 0-CW *(Contention Window*) antes de volver a escuchar el medio para comprobar si está libre. Cada transmisión incorrecta, provoca que el valor de CW se duplique hasta llegar a un valor máximo. Este proceso se repite hasta encontrar el medio libre y empezar la transmisión.

Para este mecanismo existe un problema llamado **nodo oculto.**

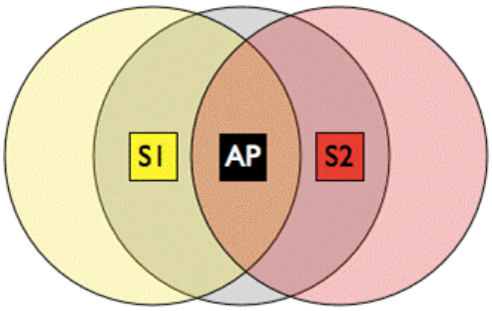

Figura 1.1 Ilustración del nodo oculto

Como se observa en la **Figura 1.1**, si S1 quiere transmitir a AP y escucha el medio cuando S2 está transmitiendo de S2 a AP, verá el medio libre. Empezará a transmitir y AP recibirá las dos transmisiones pero no podrá entender ninguna porque ambas provocan una gran interferencia.

Este problema se puede disminuir utilizando un protocolo, que consiste en cuatro pasos y cuatro mensajes diferentes: petición de envío (RTS), listo para emitir (CTS), datos y confirmación (ACK).

Una estación que está lista para transmitir envía una RTS que contiene un campo que indica cuánto tiempo necesita estar reservado el canal. El destinatario, en este caso el punto de acceso (AP), responde con un mensaje CTS que también contiene la duración de la reserva del canal. Idealmente, este CTS será recibido por todos los transmisores interferentes que están en el rango de transmisión de AP, que pospondrán sus transmisiones para evitar la colisión, así que la estación que había emitido inicialmente la RTS transmite su paquete de datos sin incidentes y el punto de acceso envía una confirmación.

Puesto que los paquetes de RTS, CTS y ACK son paquetes de señalización cortos, la posibilidad de que se produzcan errores y colisiones es baja. Si se produce una colisión entre dos paquetes RTS, será una colisión breve, por lo tanto no se desperdicia demasiado tiempo del canal.

Con esta técnica, se evitan las colisiones entre los paquetes de datos largos. Pero los paquetes extra RTS/CTS añaden sobrecarga adicional, reduciendo el tiempo del canal disponible para la transmisión de datos del usuario. Así que RTS/CTS solo está habilitado para los paquetes largos, y se suele deshabilitar completamente.

Después de cada envío de tramas, se establece un intervalo de tiempo llamado SIFS y DIFS, según el tipo de trama enviada.

Este mecanismo de acceso basado en CSMA tiene sus inconvenientes y éstos se hacen evidentes cuando coexisten estaciones que usan tasas de transmisión diferentes. Si hay nodos que trabajan a velocidades lentas en la misma celda donde existen estaciones rápidas, se crea un problema de rendimiento. El rendimiento de todos los nodos que tienen una tasa de transferencia mayor queda degradado [8]. La principal razón es que CSMA/CA garantiza que todos los nodos que comparten el mismo medio, tienen las mismas probabilidades de acceder al canal (a largo plazo, diferentes estaciones podrán acceder el mismo número de veces al canal). Es injusto, en cuanto al reparto del tiempo de utilización del canal, porque las estaciones más lentas tardarán más en transmitir una trama, ocupando el canal de manera ineficiente y robando tiempo a las estaciones más rápidas.

En la **Figura 1.2** se puede observar un caso en el que 3 estaciones, *A*, *B* y *C* que transmiten a distintas velocidades y que comparten el mismo medio para transmitir tramas iguales de *L* Bytes. Dada la justicia a largo plazo proporcionada por CSMA, asumimos que en un tiempo *T* suficientemente largo, todas las estaciones obtienen las mismas oportunidades de transmisión.

El tiempo t_g corresponde a los tiempos DIFS sumado al tiempo de *backoff* restante de la siguiente estación transmisora [9] [10] [11].

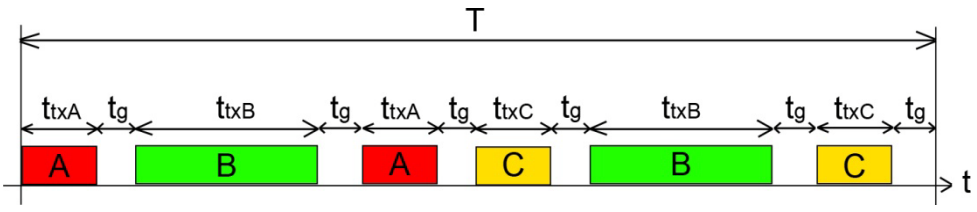

Figura 1.2 Repartición de tiempo en CSMA/CA.

Si suponemos que las tres estaciones transmiten tramas de la misma longitud (*L* Bytes) y que *A* y *C* son dispositivos rápidos, mientras que *B* es un dispositivo lento (por ejemplo, 802.11b), se puede observar como el ancho de banda queda reducido para todas las estaciones.

Mientras *A* y *C* mandan sus tramas de longitud *L* Bytes en un tiempo reducido, *B* mantiene el canal utilizado durante más tiempo para transmitir una trama del mismo tamaño.

Por lo tanto, el ancho de banda de cada estación es igual para todas, independientemente de su tasa física y queda reducido aproximadamente a:

(1.1)

$$BW \approx \frac{2 \cdot L \cdot 8}{T}$$

Donde el tiempo total T de la transmisión está formado por los tiempos de transmisión de cada estación más los tiempos, t_g, entre transmisiones. Para simplificar, asumimos un tiempo de backoff de 0s.

(1.2)

$$T = (t_{txA} + t_{txB} + t_{txC}) \cdot 2 + DIFS \cdot 6$$

Por esta razón, la tasa de bits efectiva del canal para cada estación *x* queda reducido a:

(1.3)

$$BW_x = \frac{2 \cdot L \cdot 8}{(t_{txA} + t_{txB} + t_{txC}) + 3 \cdot DIFS}$$

Simplificando, y asumiendo una longitud de cabeceras de *H* bits, el tiempo de transmisión de cada estación lo podríamos escribir como:

(1.4)

$$t_{tx} \approx \frac{H + L \cdot 8}{bitrate_x} + SIFS + DIFS + t_{txACK} + DIFS + backoff$$

Si observamos un ejemplo concreto, en el que las tres estaciones *A, B y C* trabajan con el estándar IEEE 802.11g a 54Mbps y desean enviar dos tramas de datos de 1500 Bytes de datos, tendremos que el tiempo total de la transmisión, de acuerdo a **(1.2)** es de 1,84ms y el ancho de banda total por cada estación es de 13Mbps.

Este valor, lógicamente es inferior a 54Mbps porque se está compartiendo el canal entre 3 estaciones y se reparten el ancho de banda a partes iguales.

En cambio, en el caso de que *A* y *C* son estaciones 802.11g trabajando a 54Mbps, mientras que *B* es una estación 802.11b trabajando a 1Mbps y las tres estaciones desean enviar dos tramas de datos de 1500 Bytes, tendremos un tiempo de transmisión total de 26ms, más del 90% de los cuales están ocupados por la estación más lenta.

En este caso, el ancho de banda total para cada estación es aproximadamente de 920Kbps.

En este caso, se puede observar como el ancho de banda queda reducido a un 7% de su capacidad potencial por la presencia de una estación lenta.

Esto demuestra que la presencia de un dispositivo 802.11b, reduce la velocidad de transmisión de los demás dispositivos a causa de que CSMA/CA garantiza

que todos los nodos que comparten el mismo medio, tienen las mismas probabilidades de acceder al canal.

El modo de OFDM de 802.11g es el llamado Extended Rate PHY - Orthogonal Frequency Division Multiplexing (ERP-OFDM). Por lo tanto, las redes que no utilizan este modo (802.11b) son llamadas redes No ERP.

Cuando existe un problema de convivencia entre estaciones 802.11b y estaciones con estándares ERP, los AP deben comunicarlo a las demás estaciones. Se informa con el campo ERP de la trama de gestión de 802.11g *Beacon Frame*. Este campo, contiene los flags [12] [13]:

- **NonERP_Present:** Tiene que ser activado a 1 cuando una estación No ERP se asocia al BSS. También tiene que ser activado a 1 en un IBSS si un miembro del IBSS detecta una o más estaciones no ERP que son miembros del mismo IBS. [14]

- **Use Protection:** Tiene que ser activado a 1 si una o más estaciones No ERP se asocian en un BSS donde el AP es 802.11g. También tiene que ser activado a 1 en un IBSS si un miembro del IBSS detecta una o más estaciones no ERP que son miembros del mismo IBSS o de una celda vecina. [14]

- **Barker Preamble Mode:** Si todas las estaciones asociadas son capaces de usar el preámbulo corto, el bit *Barker Preamble Mode* es 0. Cuando se asocie una estación que no sea capaz de usar el preámbulo corto se activa el bit *Barker Preamble Mode* y todas las tramas se utilizan con el preámbulo largo, produciendo mayor overhead. [14]

Estos datos enviados en las tramas *Beacon Frame*, nos serán útiles en el estudio realizado para encontrar la cantidad de dispositivos "802.11b only" que existen trabajando junto a dispositivos con tasas de transferencias superiores.

1.5.2. Centralizada (PCF)

PCF alterna dos periodos de tiempo: periodos con conflictos (CP: *Contention Period*) y periodos libres de conflictos (CFP: *Contention Free Period*). Durante los CP las estaciones simplemente utilizan DCF. Durante los CFP el punto de coordinación (el AP) controla qué estación puede transmitir en cada momento de manera síncrona con un algoritmo Round-Robin. Esta coordinación centralizada permite ciertas gestiones de QoS, por ejemplo para conexiones sensibles al tiempo, como emisiones de vídeo, y se puede utilizar para minimizar el problema de los nodos ocultos (si ningún nodo queda oculto al controlador).

El principal inconveniente es que no define clases de tráfico.

1.5.3. Híbrida (HCF) o Controlled Channel Access (HCCA)

HCF (Hybrid Coordination Function) trabaja igual que PCF pero se diferencia en:

- Permite que los CFP sea iniciados en casi cualquier momento durante un CP.
- Se define *Traffic Class (TC)* y *Traffic Streams (TS)* y se pueden asignar prioridades a las estaciones.

Es considerado el sistema de coordinación más avanzado y complejo. Se puede configurar el QoS con gran precisión.

1.6. Canales

La creciente popularidad de los equipos WLAN es una de las causas de la problemática del despliegue de redes Wi-Fi 802.11b/g/n. Actualmente se busca a toda costa una máxima cobertura y una mayor optimización de la tasa de transferencia y reducir las interferencias debidas al pequeño tamaño de la banda de comunicaciones disponible para los protocolos 802.11, sobretodo en la congestionada banda de los 2,4GHz.

Las primeras causas de los problemas en las redes WLAN en zonas de alta densidad son:

1.6.1. Interferencia co-canal

El primer problema es un problema de capacidad. Hay demasiados AP tratando de utilizar el mismo canal al mismo tiempo en la misma zona. Cuantos más dispositivos utilicen el mismo canal, la comunicación será más lenta a causa del sistema de CSMA/CA, ya que estarán compartiendo el mismo medio y no pueden transmitir todos a la vez. A este tipo de interferencia se le llama **interferencia co-canal.**

802.11b, 802.11g y 802.11n utilizan la banda de 2,4GHz.

802.11a y 802.11n utilizan la banda de 5GHz.

Cada espectro está subdividido en canales con una frecuencia central y un ancho de banda.

Como se muestra en la **Figura 1.3** la banda de 2,4 GHz está subdividida en 14 canales distanciados de 5MHz, empezando por el canal 1 a 2,412GHz y acabando por el canal 14 a 2.484GHz (puede variar según legislación de cada país).

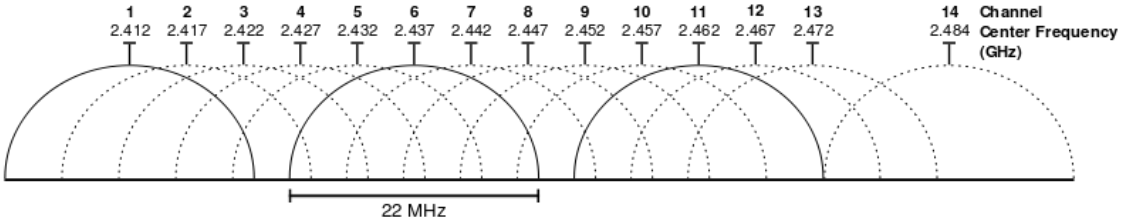

Figura 1.3 Espectro de frecuencias

- Canal 01: 2.412 GHz
- Canal 02: 2.417 GHz
- Canal 03: 2.422 GHz
- Canal 04: 2.427 GHz
- Canal 05: 2.432 GHz
- Canal 06: 2.437 GHz
- Canal 07: 2.442 GHz
- Canal 08: 2.447 GHz
- Canal 09: 2.452 GHz
- Canal 10: 2.457 GHz
- Canal 11: 2.462 GHz
- Canal 12: 2.467 GHz
- Canal 13: 2.472 GHz
- Canal 14: 2.484 GHz

Para cada canal es necesario un ancho de banda de unos 22 MHz para poder transmitir la información, por lo que se produce un inevitable solapamiento de los canales próximos. Si se tiene que configurar algunos AP cercanos inevitablemente, deberíamos separarlos lo suficiente siendo recomendable usar canales que no se solapen (1, 6 y 11 por ejemplo).

Los dispositivos que operan en la banda de 5GHz, deben emplear un mecanismo para evitar la interferencia con radares meteorológicos y aplicaciones militares. Estos mecanismos son la **Selección Dinámica de Frecuencias (DFS)** y el **Control de Potencia de Transmisión (TPC)**. Existen muchas regularizaciones respecto al uso de esta banda de 5GHz y varía según el país. Tal y como se muestra en la **Tabla 1.2**, en Europa no se permite el uso de los canales 38, 42, y 46. Además los canales 36, 40, 44 y del 48 al 64 sólo se permite su uso en interior. De este modo, únicamente se autoriza el uso en exterior, al rango de frecuencias de 5500-5700GHz.

Tabla 1.2 Uso de canales en la banda de 5GHz en Europa [15]

Canal	Frecuencia	Europa 40-20MHz
36	5180	Interior
38	5190	No
40	5200	Interior
42	5210	No
44	5220	Interior
46	5230	No
48	5240	Interior
52	5260	Interior/DFS/TPC
56	5280	Interior/DFS/TPC
60	5300	Interior/DFS/TPC
64	5320	Interior/DFS/TPC
100	5500	DFS/TPC
104	5520	DFS/TPC
108	5540	DFS/TPC
112	5560	DFS/TPC
116	5580	DFS/TPC

Canal	Frecuencia	Europa 40-20MHz
120	5600	DFS/TPC
124	5620	DFS/TPC
128	5640	DFS/TPC
132	5660	DFS/TPC
136	5680	DFS/TPC
140	5700	DFS/TPC
149	5745	En estudio, SRD (25mW)
153	5765	En estudio, SRD (25mW)
157	5785	En estudio, SRD (25mW)
161	5805	En estudio, SRD (25mW)
165	5825	En estudio, SRD (25mW)

1.6.2. Interferencia entre WLAN cercanas.

La segunda causa recae en la interferencia por radiofrecuencia. Toda forma de comunicación se constituye de dos componentes: la señal, que es la parte que contiene la información deseada, y el ruido, que es todo lo demás.

La **Figura 1.4** muestra un diagrama de espectro **idealizado** (potencia vs. frecuencia) de una señal 802.11b. Este gráfico muestra que la potencia transmitida se reduce en 30dB (dBr) a +/-11 MHz del centro del canal y a 50dB a +/-22MHz de distancia. [16]

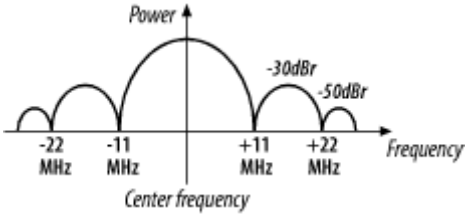

Figura 1.4 Diagrama de espectro idealizado en IEEE 802.11b

En la **Figura 1.5** se representan dos canales adyacentes. La zona amarilla representa la potencia de señal del canal 2 que se solapa con el canal 1. En este caso la comunicación de ambos canales se verá afectada.

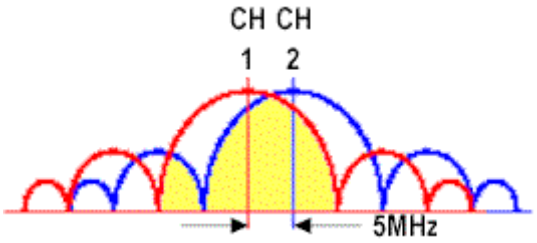

Figura 1.5 Ilustración de dos canales solapados

En la **Figura 1.6** se muestran señales de 3 canales "no-solapados". Como se puede observar, la señal de los demás canales sí que se introduce dentro de las demás frecuencias pero es menor a 30dB y se considera suficientemente baja y no afecta a la comunicación. Otro factor a tener en cuenta es la distancia física entre los dispositivos. Está demostrado [17] que dos AP configurados en canales no solapados entre ellos a corta distancia pueden interferir.

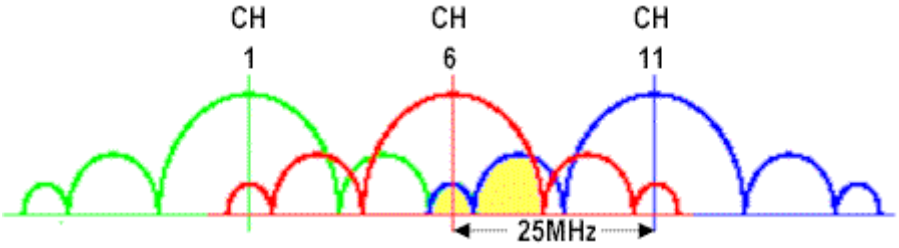

Figura 1.6 Canales 1, 6 y 11 separados 25MHz

Otros estudios realizados, en cambio, demuestran que el uso parcial de canales sí solapados puede ser beneficioso para aprovechar el espectro de las redes 802.11 [18] [19].

Las consecuencias de estas interferencias son un aumento de las retransmisiones de la tramas que no se han recibido correctamente, ralentizando la transmisión de datos.

1.7. Descubrimiento de la red

La señalización involucrada en diversos mecanismos de una red WLAN proporciona información muy importante para descubrir las características de dicha WLAN. En estos mecanismos, entre los que destacan la autenticación y la asociación, las diferentes estaciones se intercambian tramas de gestión cuyos detalles se dan al final de esta sección.

Los estados en los que puede estar una estación local respecto a una estación remota son:

Estado 1: Estado inicial, sin autenticar, sin asociar
Estado 2: Autenticada, no asociada
Estado 3: Autenticada y asociada (Pending RSN Authentication)
Estado 4: Autenticada y asociada

La **Figura 1.7** muestra la transición de los estados de una estación.

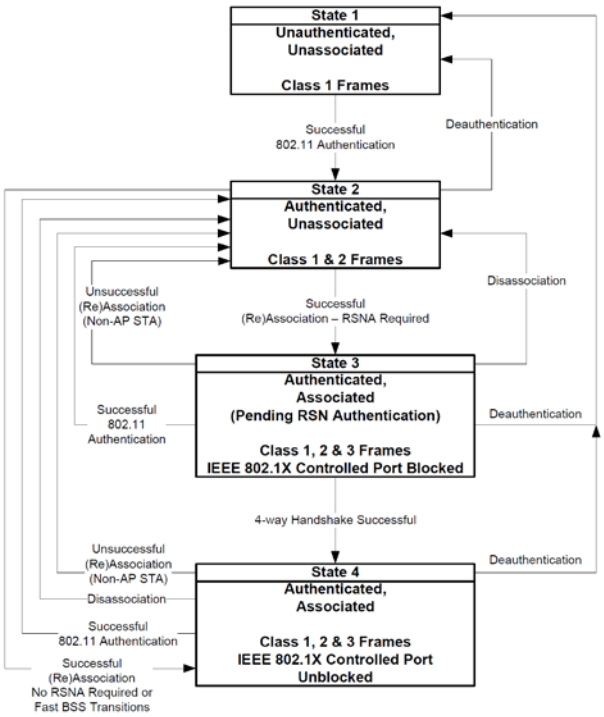

Figura 1.7 Relación entre los estados y los servicios.

1.7.1. Sincronización

En el proceso de sincronización, una vez se enciende una estación, se examina si existen otras estaciones o algún AP al que unirse, antes de llevar a cabo cualquier proceso de autenticación o asociación con alguno de ellos.

La sincronización se consigue mediante una función de sincronización (TSF) que mantendrá los relojes de las estaciones sincronizados.

La sincronización es útil y necesaria para los siguientes mecanismos:

- Determinar cuándo una estación en modo ahorro tiene que despertar.
- Determinar los saltos de canal en el modo físico con FH.
- Sincronizar los mecanismos de reserva del medio.

En el modo **infraestructura**, existen dos modos para que las estaciones realicen el descubrimiento de la red:

- **Barrido Pasivo:** La estación escucha cada canal durante un tiempo máximo definido en el parámetro *MaxChannelTime* y espera la transmisión de tramas *Beacon*. Una vez se detecta la trama *Beacon* se comienza el proceso de autenticación y asociación.
- **Barrido Activo:** La estación envía una trama *Probe Request* indicando el SSID de la red a la que se quiere conectar. Es posible que sea un SSID broadcast para que respondan todas las redes dentro del alcance. Los puntos de acceso alcanzados responden con la trama *Probe Response.*

En el modo **ad-hoc**. Por una parte, la estación que instancie la red, establece un intervalo de *Beacon*, esto es, una tasa de transferencia de portadoras que permitan la sincronización. Sin embargo en este caso el control está distribuido y entre todas las estaciones se mantiene la sincronización. Si una estación, en un tiempo determinado de *Backoff*, no detecta la trama de sincronización, envía ella misma una trama de *Beacon* para intentar mantener la sincronización de la red.

1.7.2. Autenticación

Todo equipo que se desee conectar a una BSS deberá identificarse. El punto de acceso verificará su identidad, comunicándole la resolución. En los estándares basados en 802.11 se definen dos tipos fundamentales de autenticación:

- **Abierto:** Cualquier estación que lo desee puede asociarse con el punto de acceso.
- **Clave compartida:** Esta opción comprende un riguroso intercambio de tramas para finalizar el proceso de autenticación. WEP genera una clave de encriptación que comparte con el receptor, para que sólo ellos sean capaces de recuperar la información contenida en las tramas.
- **Autenticación 802.1x:** Comprende tres partes: Un solicitante, un autenticador y un servidor de autenticación. El solicitante (cliente) proporciona credenciales para el autenticador (AP) quien proporciona los datos al servidor de autenticación que es típicamente un nodo con software RADIUS y protocolos EAP. El autenticador actúa como personal de seguridad para proteger la red.

1.7.3. Asociación

Es uno de los servicios de distribución encargados de gestionar la relación de un equipo con una determinada celda y hacia donde ha de ser enviada la información.

De entre los puntos de acceso a los que está autenticado la estación deberá elegir uno al que conectarse. La dirección MAC del equipo queda registrada en las tablas del punto de acceso. En cualquier instante, cada estación está registrada únicamente en un punto de acceso.

1.8. Tipos de tramas

Las tramas MAC se pueden clasificar según tres tipos:

- **Tramas de gestión.** Como ejemplo podemos citar los diferentes servicios de distribución, como el servicio de Asociación, las tramas de *Beacon* o portadora.
- **Tramas de control.** Los ejemplos de tramas de este tipo son los reconocimientos o ACKs, las tramas para multiacceso RTS y CTS, y las tramas libres de contienda.
- **Tramas de datos.**

Para el estudio realizado los tipos de tramas más relevantes han sido las tramas de gestión. En concreto las siguientes:

1.8.1. Beacon Frame

Es una de las tramas de gestión usadas por el estándar IEEE 802.11. En una red de infraestructura, estas tramas son emitidas por el AP periódicamente, para anunciar la presencia de redes Wi-Fi. En una red Ad-hoc estas tramas son distribuidas a través de las estaciones.

Mantienen el sincronismo entre las estaciones que usan la misma capa física ya que incorporan una marca de tiempo. Permiten a las estaciones obtener una lista de puntos de acceso disponibles buscando tramas *Beacon* continuamente en todos canales 802.11.

Contienen toda la información sobre la red y no están cifradas. Gracias a esto, han sido de gran utilidad para el estudio realizado.

Puede contener información, entre otras muchas, sobre:

- **SSID**: Indica la identidad del emisor. Se debe diferenciar entre BSSID y **ESSID**. El BSSID es la MAC del AP e identifica el BSS. Un conjunto de uno o más BSSs que funcionan como un único BSS se identifica como ESSID (ESS Identifier) definida por el administrador.

- **Supported rates**: Velocidades soportadas. Dependerá de la tecnología soportada. Si trabaja bajo el estándar 802.11b aceptará las velocidades de 1, 2, 5.5, y 11Mbps. Bajo el estándar 802.11g trabajará con 6, 9, 12, 18, 24, 36, 48 y 54Mbps, etc. En este campo también se indica las velocidades Basic, es decir las que debe ser capaz de alcanzar un dispositivo si quiere conectarse al AP que envía la trama *Beacon*.
- **Extended Supported Rates**: Si se indican más de 8 *Supported Rates*. En este campo también se indican las velocidades Basic.
- **ERP**: Indica la necesidad de activar mecanismos de compatibilidad con dispositivos 802.11 más antiguos. Este campo está solo presente en redes 802.11g y posteriores. Incluye tres flags: *Non_ERP_Station present, Use protection y Barker preamble mode*.
- **CF Parameter Set**: Es generado por un AP con función de punto de coordinador (soporta acceso PCF). Ver Apartado 1.5.2.
- **APSD**: Dos modos de ahorro de energía.
- **HT Capabilities**: Advierte de las capacidades HT de la estación. Este campo nos indica que la red soporta el estándar 802.11n.
- **Vendor Specific**: Campos adicionales no estandarizados usados por diferentes fabricantes para el funcionamiento de mecanismos propietarios.

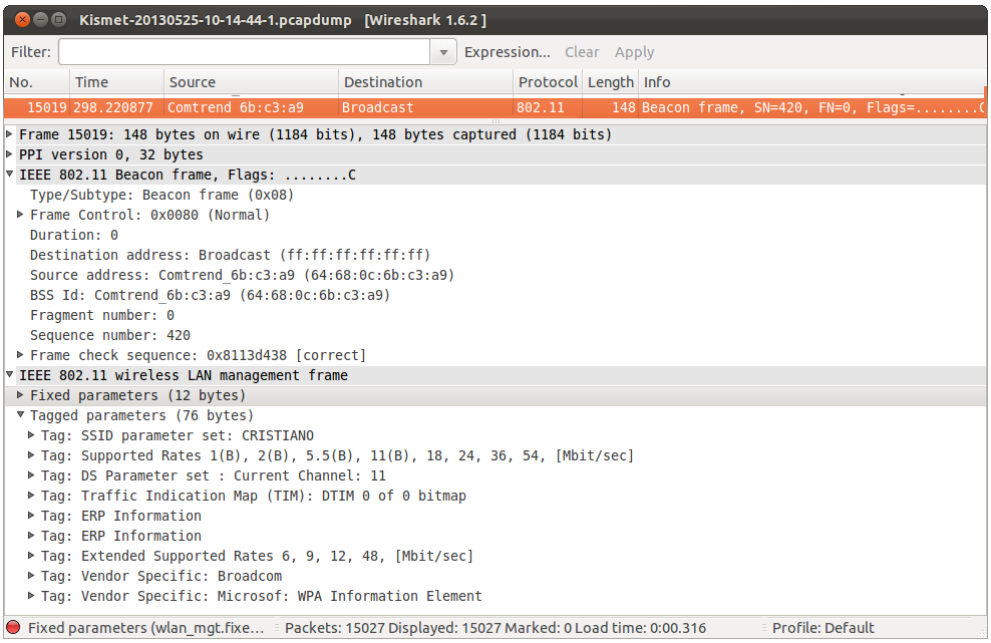

Figura 1.8 Ejemplo de trama *Beacon* en *Wireshark.*

1.8.2. *Probe Request* Frame

La trama *Probe Request*, es una de las tramas de gestión usadas por el estándar IEEE 802.11 en el escaneo activo. Estas tramas son emitidas por los clientes cuando necesitan obtener información de un punto de acceso específico, especificando su SSID, o todos los puntos de acceso dentro del área de cobertura, especificando un SSID broadcast.

Los clientes envían *Probe Request* en un canal y esperan durante un pequeño periodo de tiempo la respuesta (*Probe Response*). Si no reciben respuesta en este periodo de tiempo saltan de canal y vuelven a repetir el proceso.

Puede contener información, igual que la trama *Beacon*, sobre: *SSID, Supported rates, , Extended Supported Rates, HT Capabilities, Extended Capabilities, Vendor Specific.*

Además puede contener información, entre otras, sobre:

- **Request information:** Indica una lista de identificadores sobre los elementos que se desea información.
- **DSSS Parameter Set:** Sólo necesario para transmisiones DSSS donde las transmisiones del canal adyacente pueden ser filtradas.
- **Supported Operating Classes:** Indica un tipo de operación que se desea encontrar.
- **20/40 BSS Coexistence:** Se utiliza para evitar conflictos en situaciones en las que el uso de los 40MHz pueda interferir a otras estaciones que usan únicamente 20MHz [20].
- **SSID List:** Lista de los SSID a los que se manda la trama *Probe Request.*

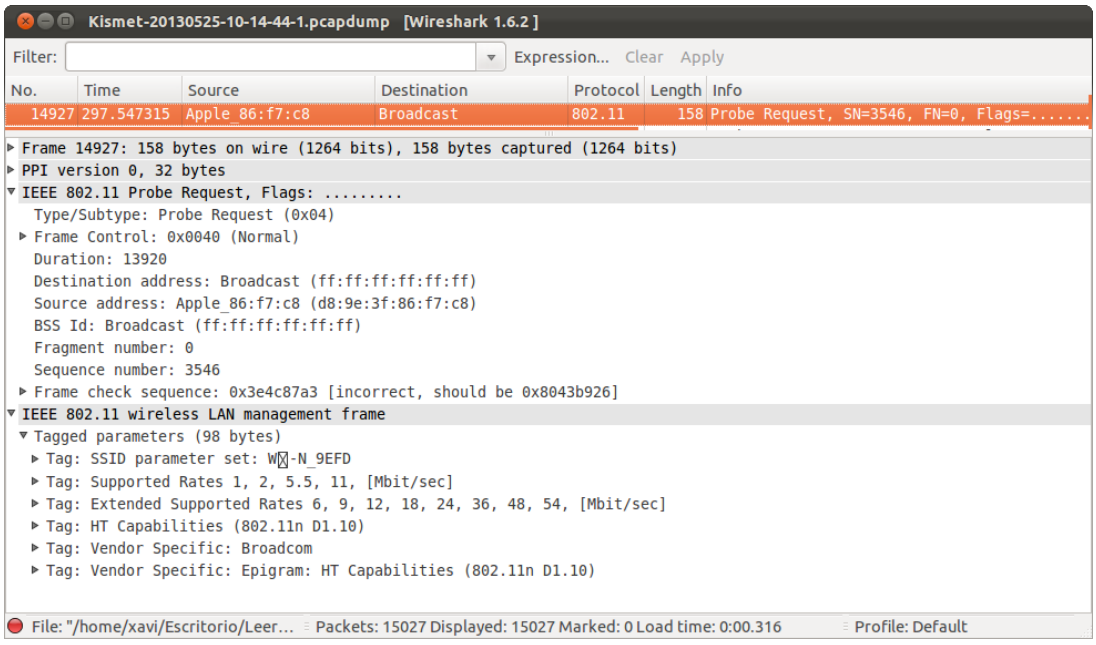

Figura 1.9 Ejemplo de trama *Probe Request* en *Wireshark*

1.8.3. Probe Response Frame

La trama ***Probe Response*****,** es una de las tramas de gestión usadas por el estándar IEEE 802.11.

Cuando una estación recibe una *Probe Request*, responde con una trama *Probe Response*. Esta trama es unicast ya que va dirigida al cliente que ha realizado la petición. Es enviada a la mínima tasa de transferencia.

Puede contener información sobre: *SSID, Supported rates, , DSSS Parameter Set, CF Parameter Set, IBSS Parameter Set, Country, , ERP, Extended Supported Rates, HT Capabilities, HT Operation, 20/40 BSS Coexistence, Extended Capabilities, Vendor Specific,* entre muchos otros.

Además puede contener información, entre otras, sobre:

FH Parameter Set: Indica el tiempo de permanencia en el canal, el patrón de salto y el índice de salto.
FH Pattern Table: Indica Patrón de *Frequency Hopping.*
Channel Switch Announcement: Mecanismo que permite notificar a las estaciones la intención de cambio de canal o cambiar el ancho de banda del canal.

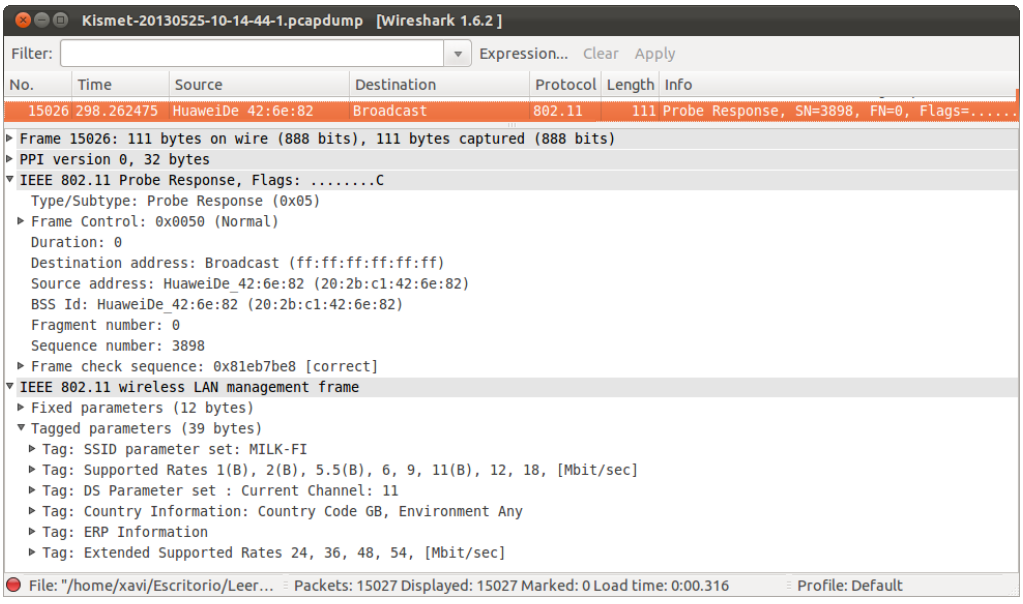

Figura 1.10 Ejemplo de trama *Probe Response* en *Wireshark*

CAPÍTULO 2. PROCESO DE TRABAJO

En este trabajo se ha realizado el estudio de las redes inalámbricas bajo el estándar IEEE 802.11 en la ciudad de Barcelona y alrededores.

El estudio se ha realizado en 4 procesos diferenciados. El primero de ellos fue el proceso de **Decisiones técnicas.** Una vez decididas cuales serían las herramientas técnicas necesarias, se realizaron dos procesos simultáneos, el **Desarrollo de la aplicación** y el **Proceso de captura.** Como último se realizó el **Análisis de los resultados**, cuyo resultado se detalla en el CAPÍTULO 3**.**

2.1. Decisiones técnicas

En el proceso inicial del trabajo se tuvieron que decidir cuáles serían las herramientas, tanto de software como de hardware, que se utilizarían para realizar el estudio.

Se creó un plan de trabajo en el que se definieron los procesos a realizar. Cada proceso requería de unas herramientas y se barajaron distintas posibilidades.

Para el proceso de captura se necesitarían herramientas hardware y software de captura. Las opciones, en cuanto a software, fueron varias (*Netstumbler*, *Kismet*, *Tshark*, *rawshark*) y finalmente *Kismet* fue el software de captura utilizado bajo Linux.

Para el hardware, por motivos de movilidad, se decidió realizar las capturas con un ordenador portátil equipado con una tarjeta capaz de capturar redes bajo los estándares IEEE 802.11abgn. Estas herramientas se definen con más exactitud en el Apartado 2.2.

Para el proceso de desarrollo de la aplicación se tuvo que decidir con qué lenguaje de programación realizar el programa y el IDE que fuera capaz de analizar los resultados de las capturas. El lenguaje elegido fue Java con Eclipse. En el Apartado 2.3 se describen sus características.

El análisis de los resultados, muy ligado al proceso de captura, requirió ciertas herramientas software que fueron introducidas durante el desarrollo de la aplicación, estas fueron herramientas como *Tshark*, *JDOM* o *gnuplot* que son explicadas en el Apartado 2.3.

2.2. Proceso de captura

Una vez se tuvieron las decisiones sobre las herramientas necesarias y se dispuso de ellas, se procedió a la realización de las capturas.

El proceso de captura es la etapa donde se recogen todos los datos necesarios para su posterior análisis. Para la realización de las capturas se dispuso de un ordenador portátil bajo el sistema operativo Linux mediante la distribución Wifiway, una antena capaz de trabajar tanto en la banda de 2,4GHz como en la de 5GHz y el software específico *Kismet*, capaz de recopilar todas las tramas IEEE 802.11 que puede recibir de la antena.

Para iniciar el proceso de captura, se deben realizar configuraciones en el equipo informático para su correcta realización. Se debe configurar el driver de la interfaz radio para que funcione en modo *monitor*, de esta forma es capaz de recopilar, en archivos locales, el tráfico 802.11 sin el requerimiento de que este vaya dirigido al propio equipo, es decir, se guardan todas las tramas 802.11 que existen en el radio de cobertura de la antena y transmitidos en el canal configurado en la interfaz. Para capturar el tráfico de todos los canales, se configura *Kismet* de tal forma que cada cierto periodo de tiempo cambie de canal. El tiempo que permanece en cada canal es del orden de magnitud de milisegundos, de esta forma, permite una velocidad razonable al técnico en el momento de realizar las capturas.

El método de captura, consiste en ejecutar el software *Kismet* a pie de calle, capturando paquetes de datos de redes inalámbricas bajo los estándares IEEE 802.11a/b/g/n. El método, detallado en el CAPÍTULO 2 de los anexos, extrae varios archivos de captura de los cuales los que han sido útiles para este estudio han sido los *.netxml* y *.pcapdump.* El primero de ellos es un archivo de formato XML con información legible de las configuraciones de los AP y de los clientes capturados. El segundo fichero contiene todos los paquetes capturados en un formato compatible con las herramientas de análisis de protocolos *Wireshark.* (ver *Tshark*, Apartado 2.3.1.).

Figura 2.1 Equipo de captura en vehículo privado

Figura 2.2. Equipo de captura en un portaequipajes.

Estas capturas, tal y como se observa en la **Figura 2.1** y en la **Figura 2.2**, fueron realizadas a pie de calle, bien a pie o en transporte privado y público, a

una velocidad moderada, para poder capturar el máximo número de redes posibles. Contienen toda la información sobre las redes detectadas. Según el escenario, el tiempo o el espacio en el que se ha realizado la captura, éstas contendrán más cantidad o menos de redes capturadas.

Se definieron tres escenarios diferenciados por sus características de infraestructura. Los escenarios tal y como se describe en la introducción de este trabajo son:

- **Zonas Residenciales (*Res*):** distritos de ciudades densamente poblados en el área metropolitana de Barcelona.
- **Zonas Comerciales (*Com*):** Calles turísticas con una cantidad considerable de edificios de oficinas y zonas industriales.
- **Zonas *HotSpot* (*HotS*):** Campus universitarios y centros comerciales.

De este modo se definieron distintas zonas de la ciudad de Barcelona y alrededores que se ajustaran a las características indicadas y se desplazaron los técnicos a realizar el proceso de captura. Los escenarios concretos fueron los que se indican en la **Tabla 2.1**.

Tabla 2.1 Escenarios de las medidas.

Zona	Población	Tipo
Balmes-Diagonal	Barcelona	Comercial
Catedral	Barcelona	Comercial
Francesc Macià	Barcelona	Comercial
Mirablau	Barcelona	Comercial
Plaza Catalunya	Barcelona	Comercial
Cercanías Renfe	Castelldefels - Gavà - Prat - Hospitalet de Llobregat	Comercial
Zona Franca Industrial	Barcelona	Comercial
Anec Blau	Castelldefels	*HotSpot*
Campus del Baix Llobregat	Castelldefels	*HotSpot*
Campus Nord	Barcelona	*HotSpot*
Gran Via 2	Hospitalet de Llobregat	*HotSpot*
La Illa	Barcelona	*HotSpot*
Sants Estació	Barcelona	*HotSpot*
Terminal 1	El prat de Llobregat	*HotSpot*
Avenida Madrid	Barcelona	Residencial
Balmes	Barcelona	Residencial
Bonanova	Barcelona	Residencial
Castelldefels	Castelldefels	Residencial
Les Corts	Barcelona	Residencial
Mataró	Mataró	Residencial
Sants	Barcelona	Residencial
Sagrada Familia	Barcelona	Residencial
Sant Cugat	Sant Cugat	Residencial
Zona Franca Residencial	Barcelona	Residencial

Las herramientas **software** utilizadas para el proceso de captura fueron:

2.2.1. Sistema operativo Wifiway

Es una distribución GNU/Linux pensada y diseñada para la auditoría de seguridad de redes *Wi-Fi*, *Bluetooth* y *RFID*. El kernel de Wifiway es Linux v.3.0.4 y la interfaz gráfica por defecto *es* KDE. Se debe destacar que Wifiway no está basada en otras distribuciones sino que se realizó usando *Linux From Scratch*. Además los autores que trabajan actualmente en el desarrollo de esta distribución GNU/Linux son los mismos que desarrollaron *WifiSlax* [21].

Para el desarrollo de este trabajo se necesitaba un entorno Linux con la finalidad de monitorizar redes inalámbricas. De la misma manera que *Wifiway*, existen varios SO destinados a esta función como son *Wifislax, Backtrack* o *Beini.* La decisión final de usar *Wifiway* fue porque dispone de un buen soporte a través de la red y bastante información. Aún así el trabajo realizado se podría haber elaborado con cualquiera de los anteriores Sistemas Operativos mencionados.

2.2.2. Kismet

Para realizar las capturas de las redes inalámbricas se utilizó la aplicación ***Kismet*** incluido en Wifiway. *Kismet* es un detector de redes, un *sniffer* (analizador de paquetes) y un detector de intrusión en 802.11abgn. Los *sniffers* son útiles en redes donde el medio de transmisión es compartido. De esta manera se pueden capturar tramas no dirigidas al dispositivo donde se ejecuta el *sniffer.* Para conseguir esto, el analizador debe configurar la tarjeta de red en un estado llamado *modo promiscuo* o *modo monitor* en el cual en la capa de enlace de datos no son descartadas las tramas no destinadas a la dirección MAC de la tarjeta. De esta manera se captura todo el tráfico capaz de recibir la tarjeta de red.

Kismet funciona con cualquier tarjeta inalámbrica que soporte el modo de monitorización *raw*, en los estándares 802.11a, 802.11b, 802.11g y 802.11n.
Kismet se diferencia de los otros analizadores de paquetes en que trabaja en modo **pasivo.** Es capaz de detectar la presencia de puntos de acceso y clientes sin mandar ningún tipo de paquete. *Kismet* genera un archivo de registro compatible con tcpdump/*Wireshark*. También es capaz de detectar redes sin configurar, *Probe Request* y determinar el nivel de encriptación inalámbrica usado por un AP.

Otro analizador de paquetes que se podría haber usado es *Netstumbler*. La decisión final a la hora de elegir *Kismet* fue por los siguientes motivos:

- A diferencia de *Netstumbler*, *Kismet* muestra información sobre los clientes conectados a la red.

- *Kismet* funciona con la tarjeta en modo monitor y guarda un archivo con los paquetes capturados. Esto es fundamental.

Las herramientas **hardware** utilizadas para el proceso de captura fueron:

2.2.3. Tarjeta de red Alfa Network UBDo-a.

Uno de los requerimientos básicos para la realización de las capturas era poder recibir las tramas de las redes inalámbricas de la banda de 5GHz para los estándares 802.11a y 802.11n y de la banda de 2,4GHz para los estándares 802.11b, 802.11g y 802.11n. Para poder capturar en ambas bandas de frecuencia se adquirió la tarjeta de red de exterior **Alfa Network UBDo-a.** Esta tarjeta está soportada por Linux, incluso en modo monitor, mediante drivers *opensource*.

La **Alfa Network UBDo-a** es una tarjeta de red 802.11abgn de exterior de largo alcance con conexión USB. A continuación tenemos sus especificaciones técnicas:

Tabla 2.2 Características técnicas Alfa UBDo-a [22].

Figura 2.3
Alfa UBDo-a

Estándares	IEEE 802.11a/b/g/n USB v1.0/1.1/2.0	
Longitud del cable	5M	
Data Rate	IEEE 802.11a 54Mbps	
	IEEE 802.11g 54Mbps	
	IEEE 802.11b 11Mbps	
	IEEE 802.11n 300Mbps	
Potencia de salida	27dBm	
Sensibilidad de recepción	IEEE 802.11a	
	-76dBm	54Mbps
	-92dBm	6Mbps
	IEEE 802.11bg	
	-77dBm	54Mbps
	-93dBm	6Mbps
Antena	Conector tipo N externo	
Rango de frecuencias	5150MHz ~ 5350MHz	
	5725MHz ~ 5850MHz (USA)	
	5150MHz ~ 5350MHz	
	5470MHz ~ 5725MHz (Europa)	
	5150MHz ~ 5250MHz (Japón)	
	2412MHz ~ 2482MHz	
Seguridad	64/128-bit WEP Encryption, WPA, WPA2, TKIP, AES	
SO soportados	Windows XP/2000/Vista, Windows 7, Linux, Mac	

2.2.4. Antena omnidireccional Air Live WAE-5AG

La tarjeta inalámbrica **Alfa Network UBDo-a**, tal y como indica en sus especificaciones, dispone de un conector tipo N para acoplar una antena externa. Para la realización de este trabajo se ha adquirido una antena Omnidireccional capaz de capturar en la banda de 2,4GHz y la de 5GHz. La antena adquirida ha sido la **Air Live WAE-5AG.** A continuación tenemos sus especificaciones técnicas [23]:

Figura 2.4 Air Live WAE-5AG.

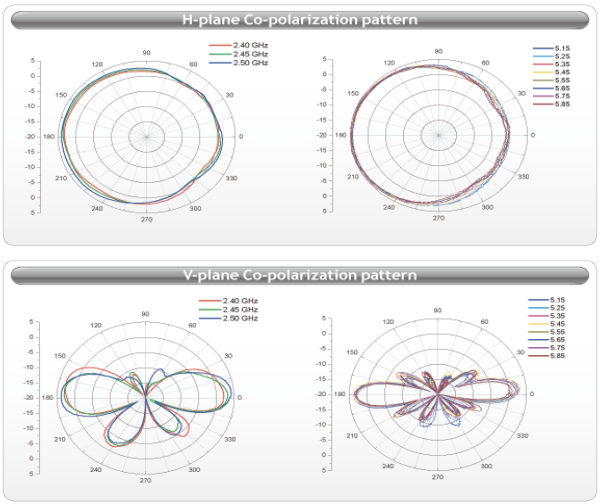

Figura 2.5 Diagrama de radiación de la Air Live WAE-5AG.

Tabla 2.3 Características técnicas Air Live WAE-5AG.

Rango de frecuencias 2.4GHz	2400 MHz - 2483 MHz
Ganancia Máxima 2.4GHz	4.5 dBi
Ganancia Media 2.4GHz	2.5 dBi
Rango de frecuencias 5GHz	5150 MHz - 5875 MHz
Ganancia Máxima 5GHz	7.0 dBi
Ganancia Media 5GHz	5.0 dBi
2.4GHz HPBW / horizontal	360°
2.4GHz HPBW / vertical	30°
5GHz HPBW / horizontal	360°
5GHz HPBW / vertical	15°
VSWR	2.0 : 1 Max.
Polarización	Lineal, vertical
Potencia	2 W
Impedancia	50 Ohmios
Conector	Macho Tipo-N
Resistencia al viento	216 km/h
Temperatura	-40°C to +70°C
Humedad	95% @ 55°C

2.3. Desarrollo de la aplicación

Simultáneamente al proceso de captura se ha desarrollando la aplicación que analiza las capturas.

De forma muy resumida, la función de la aplicación consiste en leer los ficheros de salida de la aplicación *Kismet*, realizar recuentos sobre los parámetros deseados y extraer los resultados en ficheros.

A medida que se fueron extrayendo los resultados se realizaron cambios en la aplicación para optimizar y ampliar los resultados.

Esta aplicación se ha realizado con el lenguaje de programación Java bajo el sistema operativo Linux. No obstante, al ser Java un lenguaje interpretado, esta aplicación podría ser ejecutada desde cualquier sistema operativo que disponga de una máquina virtual de Java, adaptando algunos *scripts* externos. Además de este motivo, se ha elegido el lenguaje de programación Java por ser la programación orientada a objetos más intuitiva. Es un lenguaje cuyo estudio se incluye en el plan de enseñanza de la Ingeniería, por lo tanto más conocido y bien documentado.

Seguidamente se explica, a grandes rasgos, el hilo de proceso de la aplicación realizada:

Para empezar se deben realizar capturas en los escenarios reales que se describen en el Apartado 2.2. Estas capturas se introducen en la aplicación para proceder a su análisis.

El hilo principal de la aplicación se inicia en la clase *Programa* y requiere como argumento de entrada el nombre del directorio en el que se encuentran las capturas a analizar. En el directorio se pueden almacenar diferentes capturas que se analizarán para obtener un resultado conjunto.

Seguidamente se crea una lista vacía de redes inalámbricas donde se irán añadiendo una a una las redes detectadas en las capturas.

La recopilación de información se empieza en la clase ***LeerXml*** que, como su nombre indica, lee el archivo de captura en formato XML. Además en esta clase se ejecutan comandos externos *Tshark* que extraen la información deseada de otro de los archivos de salida del software de captura con extensión *.pcapdump*. (Ver Apartado 2.3.1).

Se empieza leyendo los archivos extraídos de las capturas. Se añade a la lista cada red inalámbrica detectada en la captura con la información de:

1. **Encriptación:** Tipos de encriptación utilizada.
2. **Fabricante:** Nombre del fabricante.
3. **Canal:** Número del canal.
4. **Tipología:** ad-hoc o infraestructura.
5. **BSSID:** Dirección MAC del AP.

6. **ESSID:** Nombre de la red.
7. **Velocidades:** Velocidades soportadas.
8. **Velocidades Basic:** Velocidades obligatorias para poder conectarse.
9. **Estándares:** Estándares soportados.
10. **Estándares Basic:** Estándares obligatorios para poder conectarse.
11. **Parámetros de Configuración:** Se tienen recopila el estado de los bytes **ERP, USE_PROTECTION, BARKER, CFP, APSD** y **SPECTRUM.**

A su vez también se detectan los clientes conectados en el momento de la captura a los puntos de acceso detectados y se almacena dentro de las propiedades de la red correspondiente. Gracias al envío frecuente de tramas *Probe Request* involucradas en el mecanismo de descubrimiento activo cada cliente contiene información de:

- **Fabricante:** Fabricante de la interfaz de red.
- **MAC:** Dirección MAC de la interfaz de red.
- **Velocidades:** Velocidades soportadas por el cliente.

No todas las redes inalámbricas detectadas son de utilidad. Las capturas contienen datos de redes que podrían alterar los resultados. Por este motivo se hace una selección exhaustiva de las redes y clientes detectados, descartando o agrupando los datos necesarios. Algunos de estos casos son descritos a continuación:

Para un AP configurado con múltiples *Virtual AP* (VAP) aparece en las capturas un mismo ESSID con varios BSSID. Si no se tratara este caso de manera especial se estaría contabilizando este AP, múltiples veces cuando en realidad el AP es único con distintas configuraciones. Cuando se encuentra con este caso se agrupan las distintas configuraciones de los VAP como si se tratara de una única red inalámbrica.

Otro de los casos que se ha tratado de forma especial son los clientes de los AP. Durante el proceso de desarrollo de la aplicación se detectó que algunos clientes eran en realidad interfaces virtuales de otros AP ya contabilizados, por lo tanto, no podían ser contabilizados como tal.

Otro aspecto a tener en cuenta es que *Kismet* indica el nombre del fabricante de las redes detectadas según una base de datos local analizando los 3 primeros pares de dígitos hexadecimales de la dirección MAC. Si alguna numeración no coincide con la base de datos de *Kismet*, indica el fabricante como *Unknown.* Para minimizar el número de redes con el fabricante *Unknown* se ha obtenido el fichero actualizado con los nombres de los fabricantes y su respectiva numeración del sitio web de IEEE[1] para resolver los nombres de los fabricantes que *Kismet* no reconozca. Aún así, en el caso de que no se encuentre el nombre del fabricante en este fichero, la aplicación realiza una comunicación *M2M* con un *webservice* a través de una petición GET que obtendrá el resultado en forma de JSON. Para ello se ha usado Jersey, la implementación *opensource* de REST para Java. De esta forma se realiza una

[1] http://standards.ieee.org/develop/regauth/oui/oui.txt.

conexión con un sitio web[2], que devuelve el nombre del fabricante en el caso de que lo contenga en su base de datos.

Otra situación problemática son las redes de las que no se han recibido correctamente las tramas y las que se ha recibido ningún paquete de control. Estas redes son descartadas y únicamente se tienen en cuenta los clientes en el caso de que los tenga.

El último ejemplo de caso especial, son los clientes capturados que en ese momento estaban enviando tramas *Probe Request* en descubrimiento activo sin ningún AP definido. Todos estos clientes son agrupados aparte ya que no corresponden a ningún AP y se obtendrán sus características.

Una vez se tiene toda la información deseada, lo siguiente que realiza la aplicación es un cálculo estadístico de los parámetros que nos interesan. Para este proceso se recorre toda la lista de redes inalámbricas almacenadas y se actualizan los contadores con los parámetros a estudiar.

A continuación se hacen los cálculos estadísticos y se generan diferentes ficheros de texto con los resultados de cada parámetro. También se extrae un fichero de texto con el resumen de la información recopilada de todas las redes encontradas y sus correspondientes clientes conectados.

Finalmente, se genera un fichero de salida con el formato compatible con Gnuplot para obtener resultados gráficos de:

- **Fabricantes AP:** Estadística de fabricantes más utilizados.
- **Fabricantes clientes:** Estadística de fabricantes más utilizados.
- **Canales:** Estadística de los canales utilizados.
- **Tipología:** Estadística del tipo de redes detectadas.
- **Encriptación:** Estadística de los tipos de encriptación utilizados de manera conjunta.
- **Encriptación Individual:** Estadística de los tipos de encriptación individuales.
- **Velocidad:** Estadística de las velocidades soportadas de manera conjunta.
- **Velocidad Individual:** Estadística de las velocidades individuales.
- **Estándares:** Estadística de los estándares soportados.
- **Estándares Basic:** Estadística de los estándares obligatorios.

[2] http://www.macvendorlookup.com/

A continuación se describen las herramientas **software** utilizadas para el desarrollo de la aplicación:

2.3.1. Tshark

Es un analizador de protocolos de red. Permite capturar paquetes de una red activa o leer paquetes de un archivo de capturas guardado con anterioridad. El formato de archivo de captura nativa de *Tshark* es *libpcap* que es el mismo formato utilizado por tcpdump, *Kismet* y otras herramientas. [24]

Tshark se ejecuta desde el terminal de Linux. Si no se modifican las opciones, *Tshark* trabaja de la misma manera que *tcpdump*. Utilizará la librería *pcap* para capturar el tráfico a través de la primera interfaz de red disponible y mostrará un resumen por la salida estándar de cada paquete recibido. *Tshark* es capaz de detectar, leer y escribir los mismos archivos de captura que son soportados por *Wireshark*. El fichero de entrada no necesita una extensión específica.

Por este motivo *Tshark* ha sido el analizador de paquetes utilizados para este trabajo ya que nos permite analizar las capturas realizadas previamente con *Kismet* y guardadas en los archivos *.pcapdump*.

Tshark permite realizar todo tipo de filtros. Los filtros se pueden realizar tanto en capturas en vivo como en la lectura de un archivo. Para nuestra aplicación las opciones y filtros más importantes han sido:

- **-R <read (display) filter>:** Indica el tipo de filtro deseado que se aplicará antes de imprimir los paquetes decodificados. Utiliza la sintaxis de lectura/mostrar filtros en lugar de la de filtros de captura. Los paquetes que no coincidan con el filtro son descartados y no se imprimirán. Si el filtro contiene espacios debe indicarse entre comillas "".
- **-T pdml|psml|ps|text|fields:** Establecer el formato de salida. Las opciones son**:**
  - **pdml:** Packet Details Markup Language, basado en el formato XML con los detalles de los paquetes codificados.
  - **psml:** Packet Summary Markup Language, basado en el formato XML con un resumen de la información de los paquetes codificados.
  - **ps:** PostScript, basado en un formato legible por las personas con un resumen de la información de los paquetes codificados.
  - **text:** Texto, basado en un formato legible por las personas con los detalles de los paquetes codificados.
  - **field:** Los valores de los campos especificados con la opción **-e .**
- **-e <field>:** Añade un campo a la lista de campos para mostrar si la opción **-T fields** está seleccionada. Esta opción puede ser usada en múltiples ocasiones en la línea de comandos.
- **-r<infile>:** Lee los datos de los paquetes del fichero de entrada indicado en el siguiente argumento.

Como ejemplo de integración de *Tshark* en la aplicación creada, el siguiente comando genera un fichero con el nombre 1.txt en el directorio ./temp/ap/ con las direcciones origen de los paquetes que soportan velocidades de 1Mbps:

```
Tshark -R "wlan_mgt.supported_rates == "2"" -T fields -e
wlan.sa -r nombreFichero >> ./temp/ap/1.txt
```

- El filtro "wlan_mgt.supported_rates == "2"" selecciona los paquetes que soporten la velocidad de 1Mbps.
- El campo -T fields -e wlan.sa indica que nos muestre la *source adress* del paquete.
- El campo -r nombreFichero indica el fichero de entrada.
- El campo >> ./temp/ap/1.txt redirecciona la salida estándar al fichero 1.txt.

2.3.2. Eclipse

Eclipse es un programa informático compuesto por un conjunto de herramientas de programación de código abierto multiplataforma para desarrollar lo que el proyecto llama "Aplicaciones de Cliente Enriquecido". Esta plataforma, típicamente ha sido usada para desarrollar entornos de desarrollo integrados (del inglés IDE), como el IDE de Java llamado *Java Development Toolkit* (JDT) y el compilador (ECJ) que se entrega como parte de Eclipse (y que son usados también para desarrollar el mismo Eclipse).

Eclipse, desarrollado originalmente por IBM, es ahora desarrollado por la Fundación Eclipse, una organización independiente sin ánimo de lucro que fomenta una comunidad de código abierto y un conjunto de productos complementarios, capacidades y servicios.

En este trabajo se ha utilizado Eclipse como plataforma de desarrollo del programa informático que analiza las capturas.

2.3.3. Java

Java es un lenguaje de programación, originalmente desarrollado por James Gosling de Sun Microsystems, publicado en 1955. Su sintaxis deriva mucho de C y C++, pero tiene menos facilidades de bajo nivel que cualquiera de ellos.

Las aplicaciones de Java son generalmente compiladas a bytecode (clase Java) que puede ejecutarse en cualquier máquina virtual Java (JVM) sin importar la arquitectura de la computadora subyacente.

Es un lenguaje Orientado a Objetos. La programación orientada a objetos está basada en varias técnicas, incluyendo herencia, cohesión, abstracción, polimorfismo, acoplamiento y encapsulamiento. Un objeto es una abstracción

de algún hecho o ente del mundo real, con atributos que representan sus características o propiedades, y métodos que emulan su comportamiento o actividad. Todas las propiedades y métodos comunes a los objetos se encapsulan o agrupan en clases. Una clase es una plantilla, un prototipo para crear objetos; en general, se dice que cada objeto es una instancia de una clase.

El programa informático realizado en este trabajo se ha creado en lenguaje Java. Una de las tareas requeridas por la aplicación ha sido recoger datos de un archivo XML. Para esta acción se ha utilizado la biblioteca JDOM.

JDOM es una biblioteca de código abierto para manipulaciones de datos XML optimizado para JAVA. JDOM se creó específicamente para usarse con Java y por lo tanto beneficiarse de las características de Java, incluyendo sobrecarga de métodos, colecciones, etc.

Otra tarea requerida ha sido obtener el nombre del fabricante de las tarjetas de red a un servidor remoto indicando la dirección MAC. Para esta acción se ha utilizado Jersey i JSON.

JAX-RS: Java API for RESTful Web Services (Jersey) es una API del lenguaje de programación Java que proporciona soporte en la creación de servicios web de acuerdo con el estilo arquitectónico *Representational State Transfer* (REST) [25]. La comunicación que se ha establecido en esta aplicación, responde con un objeto JSON.

JSON es un lenguaje para representar estructuras de datos simples. JSON i XML son claros competidores entre sí. La ventaja de JSON sobre XML como formato de intercambio de datos en este contexto es que es mucho más sencillo de analizar (parser).

2.3.4. Gnuplot

Gnuplot es un programa de línea de comandos muy flexible para generar gráficos bi y tridemensionales, funciones y datos. Se puede utilizar interactivamente o a través de scripts. [26].

Para el trabajo realizado se ha utilizado para generar automáticamente las gráficas que muestran los datos capturados.

En el Apartado siguiente se proporcionan más detalles sobre la implementación de cada una de las clases desarrolladas para el funcionamiento de esta aplicación de análisis de datos de tráfico Wi-Fi.

2.3.5. Explicación del código fuente

La aplicación realizada se compone de 10 clases que interaccionan entre sí para leer las capturas provenientes de la herramienta *Kismet*, almacenar los datos requeridos, calcular y generar los resultados del análisis y gestionar el flujo principal de la aplicación:

1. La clase **Programa** es la clase principal (contiene el método principal *main()*). En esta clase se inicia el programa eliminando, si existen, todos los archivos que contienen los directorios: Resultados, temp/ap y temp/clientes. A continuación, se modifica el fichero que contiene la relación entre las direcciones MAC y sus fabricantes. Esta modificación se realiza para que este fichero tenga el mismo formato que los datos que obtenemos del fichero XML proporcionado por el software *Kismet*. Si cuando se inicia la aplicación por línea de comandos no se indica en el primer argumento el nombre del directorio que contiene los archivos XML a leer, este lo pide por pantalla. Seguidamente, se obtiene el nombre de cada uno de los archivos de captura de dentro del directorio indicado y se pasa el nombre a una instancia de la clase **LeerXml**.

2. La clase **LeerXml** es la encargada de analizar los ficheros de captura extraídos de la aplicación *Kismet*. Primero obtiene las características de la/las tarjeta/s de red inalámbricas y devuelve una colección con todas las interfaces de red inalámbricas encontradas. Con estos datos, se crea un archivo de texto con la información de las interfaces de red utilizadas para realizar las capturas. En este instante, se crea una copia del fichero XML original sobre el que se analizarán los datos de las redes que contiene. Seguidamente se obtienen las características de las redes inalámbricas capturadas y se devuelve una colección de objetos de la clase **WifiCapturada** con todas las redes inalámbricas encontradas. Si el tipo de red es *data*[3] o *Probe*[4] o se informa que el canal es *0*[5], se descarta la red y sus clientes se añaden a la colección "**listaClientesHuerfanos**" que contendrá todos los clientes que no están asociados a ningún AP. Desde esta misma clase se realizan llamadas al sistema para ejecutar los comandos externos *Tshark* para obtener un archivo de texto con información filtrada de cada captura con los datos que se quieren analizar. El fichero de captura con el que trabaja *Tshark* es un fichero con extensión *.pcapdump* que contiene todos los paquetes capturados. En primer lugar se filtran las capturas para obtener las direcciones MAC de los AP y clientes que soportan las diferentes tasas físicas de los diferentes estándares (e.g. de 1Mbps a 54Mbps). Con este mismo mecanismo también se obtiene un fichero con información sobre ERP, USE_PROTECTION, BARKER, CFP, APSD, SPECTRUM, bytes_beacon, bytes_request, bytes_response y bytes_total de los AP.

[3] Redes detectadas en las que no se han detectado paquetes de control
[4] Clientes que no están asociados a ningún AP. Están en el proceso de búsqueda activa
[5] Redes mal detectadas, con tramas cortadas o mal recibidas.

Cuando ya se tienen todos los datos almacenados, se imprime un fichero (*Wi-Fis.txt*) con las características de todas las redes y sus clientes.

Llegados a este punto, se recorren todos los objetos **WifiCapturada** y se procede al recuento de:

- **Los fabricantes** de AP y de los clientes. Si *Kismet* no ha reconocido el fabricante y se ha indicado como *Unknown* en el fichero XML de entrada, se comprueba si la dirección MAC existe en el fichero de la IEEE, de manera local[1]. Si la aplicación no reconoce el fabricante, se hace una consulta mediante el *webservice* REST proporcionado por *www.macvendorlookup.com* para obtener el fabricante según su MAC y se actualiza el fichero local de fabricantes.
- **Los canales** utilizados (para 2,4GHz y 5GHz).
- **La tipología** de red (Ad-hoc o Infraestructura).
- Los **tipos de autenticación** utilizados por los AP.
- Los tipos de encriptación combinados e individuales utilizados.
- La información sobre ERP, USE_PROTECTION, BARKER, CFP, APSD, SPECTRUM, bytes_beacon, bytes_request, bytes_response y bytes_total.
- Las **velocidades individuales**, las **velocidades Basic** y las **combinaciones** de velocidad anunciadas por los AP y los clientes
- Los **estándares 802.11** utilizados por los AP.
- Los **bits** y **tramas** capturados que corresponden a tramas *Beacon*, *Probe Request* y *probe response***.**

Como punto final, se realizan llamadas al sistema para ejecutar los comandos externos *Ggnuplot* que contiene el fichero ubicado en */Gnuplot/Comandosgnuplot.gnu* para crear los gráficos de los archivos de recuento.

3. La clase **LeerTxt**, es utilizada desde la clase **LeerXml** y es la encargada de leer los ficheros de texto obtenidos con los comandos *Tshark.* Estos ficheros contienen información relevante que se extraer y se añade a cada objeto **WifiCapturada** de la lista. Los archivos se encuentran en el directorio */temp/ap/* y */temp/clientes/*. El nombre de cada archivo, con las direcciones MAC de cada AP, corresponde a la velocidad. Para las velocidades incluidas en el *Basic Rate Set*, el nombre del archivo va precedido del carácter B. Los archivos que indican información ERP, USE_PROTECTION, BARKER, CFP, APSD y SPECTRUM que contienen las direcciones MAC y los archivos bytes_beacon, bytes_request, bytes_response y bytes_total que contienen el tamaño de cada paquete de su tipo, también tienen su nombre según la información que contiene. La clase **LeerTxt** contiene métodos que optimizan y adaptan los archivos de texto para un mayor rendimiento del proceso. La clase **LeerXml** también utiliza estos métodos. Como proceso final de esta clase, se recorre cada fichero en búsqueda de la dirección MAC de cada AP o cliente almacenados en la colección creada desde **LeerXml** para añadir cada información a su respectivo objeto **WifiCapturada**.

4. La clase **InterfazCaptura** consiste en un *POJO* (Plain Old Java Object) [27] que envuelve la información de las propiedades de las diferentes interfaces de red inalámbrica usada en la captura:

- **cardNumber:** Indica el número de la interfaz de red.
- **uuid:** Identificador de la interfaz de red.
- **cardSource:**nombre_de_la_interfaz:name=nombre_asignado,hop=true /false.
- **cardName:** nombre asignado en el archivo *Kismet.conf.*
- **cardInterface:** nombre_de_la_interfaz.
- **cardType:** tipo de interfaz (driver).
- **cardHope:** Indica si la interfaz de red está configurada para hacer los saltos de canal.
- **cardChannels:** Indica los canales en los que trabaja la interfaz de red y por los que *Kismet* hace los "saltos".

5. La clase **WifiCapturada** contiene información sobre cada una de las redes inalámbricas capturadas en sus atributos. Se almacena en una colección de objetos **WifiCapturada** en la clase **LeerXml** para poder acceder a cada uno de los atributos de cada una de las redes capturadas. Se define el objeto con los atributos:

- **number:** Indica el número de la interfaz de red.
- **encriptacion:** Colección con todos los tipos de encriptación.
- **fabricante:** *String* con el nombre del fabricante.
- **canal:** *String* con el número del canal.
- **tipologia:** ad-hoc o infraestructura.
- **bssid:** Dirección MAC de la red capturada.
- **essid:** Nombre de la red capturada.
- **velocidades:** Colección de *String*s con todas las velocidades.
- **info:** Vector de *String*s con información sobre ERP, USE_PROTECTION, BARKER, CFP, APSD, SPECTRUM**.**
- **listaClientes:** Colección con objetos **ClienteCapturado**. Contiene todos los objetos cliente de la **WifiCapturada** actual.
- **huerfano:** Boolean que indica si el objeto **WifiCapturada** es el AP con clientes sin AP asociado.

6. La clase **ClienteCapturado** contiene información sobre los clientes capturados asociados a los AP. Se almacenan todos los clientes de un AP en una colección en la clase **WifiCapturada.** Define el objeto con los atributos:

- **manufCliente:** Fabricante de la interfaz de red del objeto cliente.
- **macCliente:** Dirección MAC de la interfaz de red del objeto cliente.
- **numberCliente:** Numeración por orden indicada en el XML.
- **numberWi-Fi:** Numeración del AP asociado.

7. La clase **Velocidad** es utilizada desde la clase **LeerXml** para realizar los recuentos de combinaciones de velocidad. Define el objeto con los atributos:

- **velocidad:** Colección de *String* con las velocidades soportadas y Basic del objeto AP o cliente.
- ***String*Veocidad:** *String* con la velocidad individual.
- **cantidad:** cantidad de AP que tienen la misma combinación de velocidades.

8. La clase **Encriptacion** es utilizada desde la clase **LeerXml** para realizar los recuentos de combinaciones de encriptación. Define el objeto con los atributos:

- **encriptacion:** Colección con todas las combinaciones de encriptaciones con las que trabaja el AP.
- **encriptacionIndividual:** *String* con la encriptación individual.
- **cantidad:** cantidad de AP que tienen el mismo tipo de encriptación.

9. La clase **Fabricante** es utilizada desde la clase **LeerXml** para realizar los recuentos de fabricantes. Define el objeto con los atributos:

- **fabricante:** *String* con el nombre del fabricante.
- **cantidad:** Cantidad de dispositivos del mismo fabricante.

10. La clase **Canales** es utilizada desde la clase **LeerXml** para realizar los recuentos de canales. Define el objeto con los atributos:

- **canal:** *String* que indica el canal.
- **cantidad:** *String* que indica la cantidad de dispositivos que usan el mismo canal.

CAPÍTULO 3. ANÁLISIS DE LOS RESULTADOS

El estudio realizado se ha llevado a cabo en las ciudades de Barcelona, Castelldefels, Mataró y Sant Cugat del Vallès. Los tres escenarios estudiados han sido Zonas Residenciales, Zonas Comerciales y Zonas *HotSpot*. El total de Puntos de Acceso detectados ha superado los 13000 y el total de clientes conectados a estos Puntos de Acceso se acerca a los 26000.

Se realizaron las capturas de tráfico de redes inalámbricas, trabajando en los estándares 802.11a,b,g,n en las bandas ISM de 2,4 y 5GHz. Las capturas fueron realizadas con ordenadores portátiles con sistemas operativos Linux a pie de calle a un ritmo normal a pié, a 20Km/h en transporte privado y a la velocidad habitual en transporte público.

A continuación se presentan los resultados obtenidos del análisis realizado.

3.1. Estándares

El primer campo a analizar son los estándares utilizados por los AP. El resultado, como resultado global de los tres escenarios ha sido el **Gráfico 3.1**.

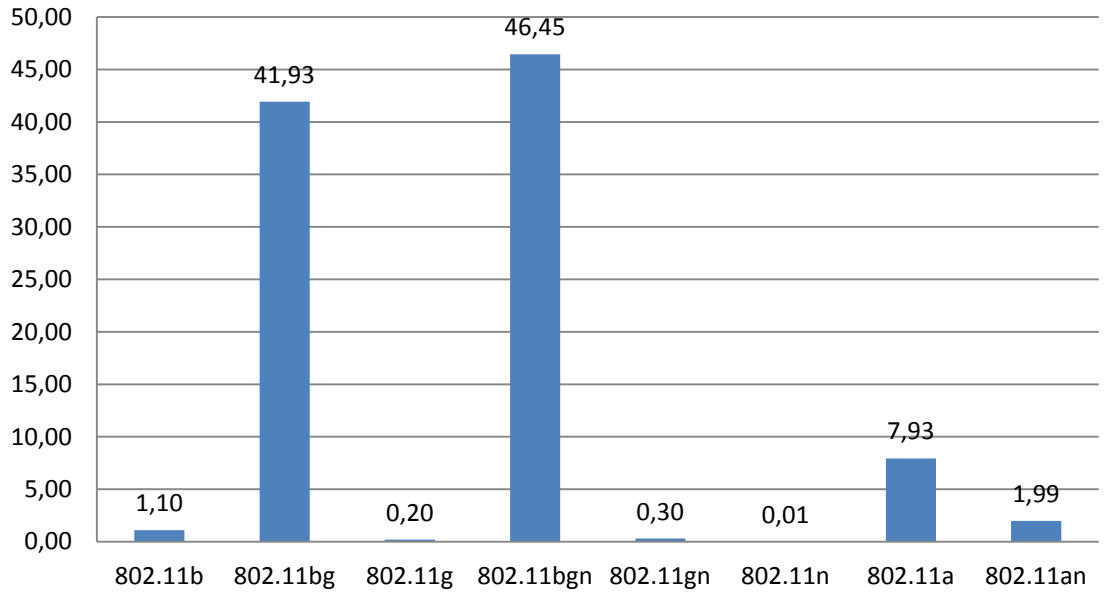

Gráfico 3.1 Estándares

Únicamente un 1,10% de los AP detectados trabajan con 802.11b exclusicamente, valor que supera el 0,20% de AP que trabajan exclusivamente con el estándar 802.11g.

No obstante, hay que tener en cuenta que, aproximadamente un 88% de los AP, son compatibles con estos dos estándares prácticamente a partes iguales.

Para verlo de forma más concreta se puede corroborar con el **Gráfico 3.2** que muestra las velocidades soportadas por los AP en tanto porciento. Está claro, por lo tanto, que el uso de los tres estándares 802.11bgn. está fuertemente implantado a nivel general y que la tendencia es la del uso de dispositivos compatibles con diversos estándares a la vez.

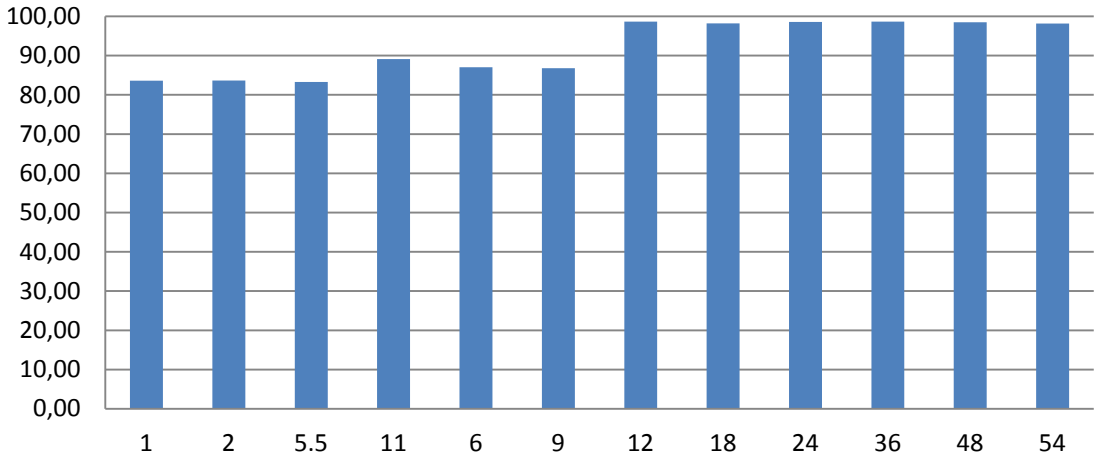

Gráfico 3.2 Velocidad Individual

Si nos fijamos en el **Gráfico 3.3** que muestra las Tasas de Transferencia Básicas que anuncian los AP, un 87,14% de los AP detectados obliga a trabajar en el estándar 802.11b. Es decir un 87,14% de AP deniegan el servicio a estaciones que no soporten el estándar 802.11b. Esto demuestra que 802.11b, aunque sea el estándar con menores tasas de transferencia, es necesario para poder conectarse a la gran mayoría de las redes detectadas. Es posible que el motivo sea, porque algunas tramas de gestión, imprescindibles para la conexión, se transmiten a tasas de transferencia típicamente de 802.11b. Obviamente, los dispositivos de 802.11a requieren su estándar.

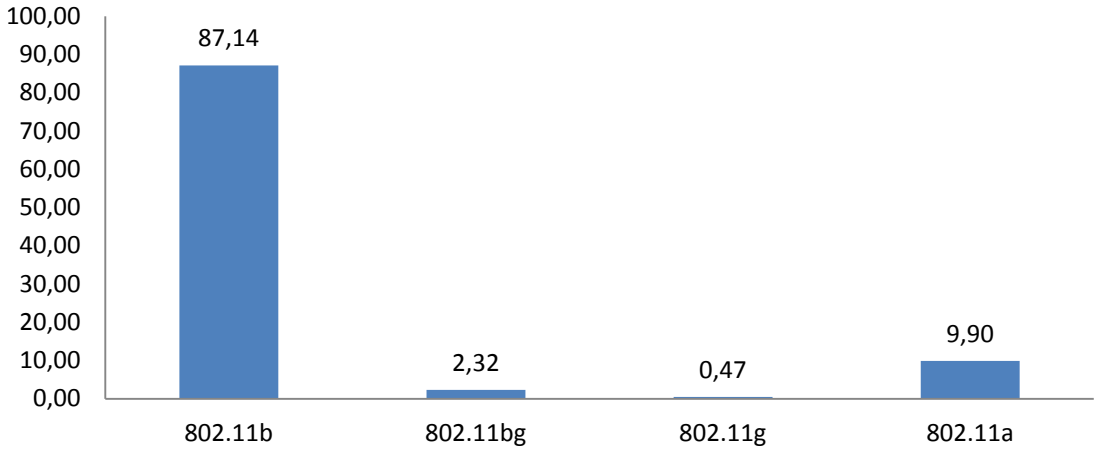

Gráfico 3.3 Estándares Basic

Para verlo de una forma más concreta, en el **Gráfico 3.4** se pueden observar las velocidades obligatorias que exigen los AP.

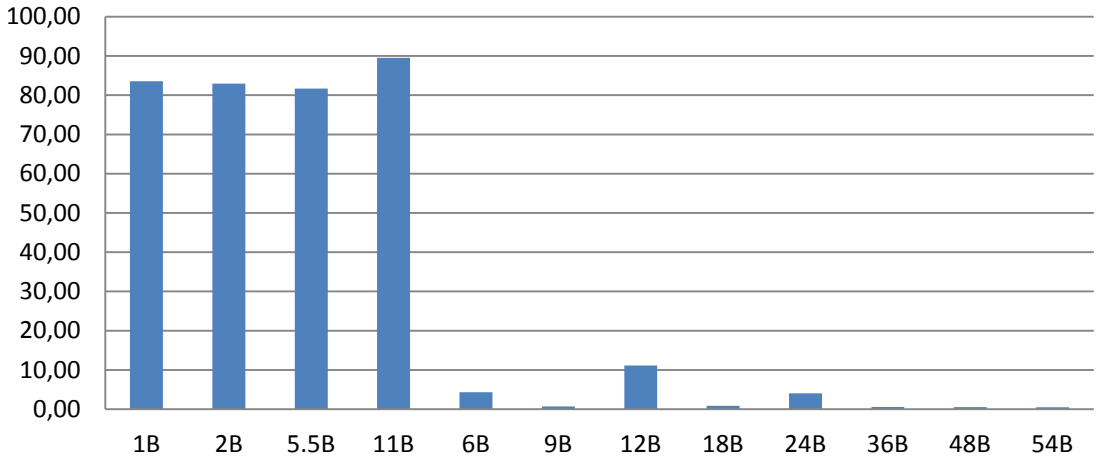

Gráfico 3.4 Velocidad Individual Basic

Es evidente que las tasas de transferencia de 802.11b son obligatorias en la mayoría de AP.

Para diferenciar los distintos escenarios tratados, en el Gráfico 3.5 se muestra la comparativa entre las zonas residenciales, las zonas comerciales y las zonas *HotSpot*.

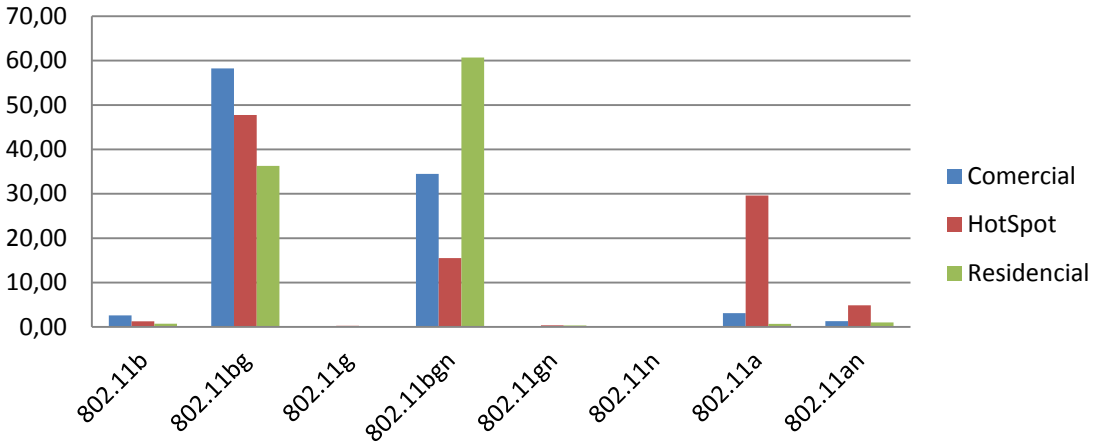

Gráfico 3.5 Estándares

Como se puede observar, el escenario que contiene más cantidad de AP con el último estándar (802.11n) es el de las zonas Residenciales. Este dato demuestra que este tipo de escenario es más propenso a la renovación de sus

equipos. Además se demuestra que el estándar 802.11a está fuertemente implantado y casi de manera exclusiva en las conexiones *HotSpot*.

El **Gráfico 3.6** muestra los estándares obligados por cada tipo de escenario.

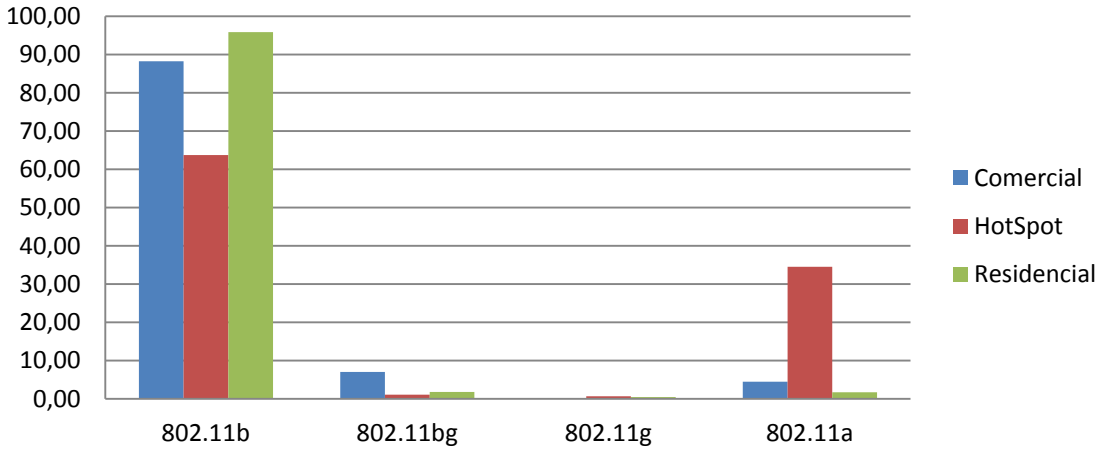

Gráfico 3.6 Estándares Basic

El **Gráfico 3.7** muestra la problemática de la convivencia entre estándares 802.11b y los de velocidad superior. Durante las capturas, únicamente se ha encontrado un 0,79% de casos en los que estén convivendo dispositivos que únicamente trabajan a 802.11b junto con otros dispositivos a 802.11g o 802.11n. Un 27,90% de los AP capturados han detectado tramas de gestión de otra celda vecina con el bit *Non_ERP_present* activado o han detectado que soporta únicamente velocidades de dispositivos non_ERP (802.11b). De manera que, aunque menos del 1% de los AP dan servicio a estaciones 802.11b, los mecanismos de compatibilidad afectan a casi un tercio de las redes.

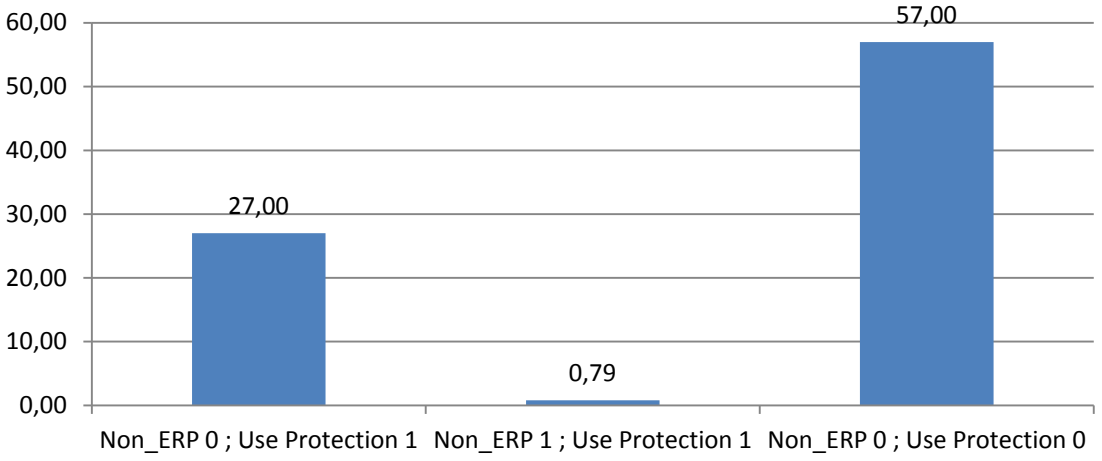

Gráfico 3.7 ERP y USE PROTECTION

Tal y como se ha explicado en el Apartado 1.5.1, existen distintas situaciones problemáticas que necesitan mecanísmos específicos. Estos son plasmados en el **Gráfico 3.8**.

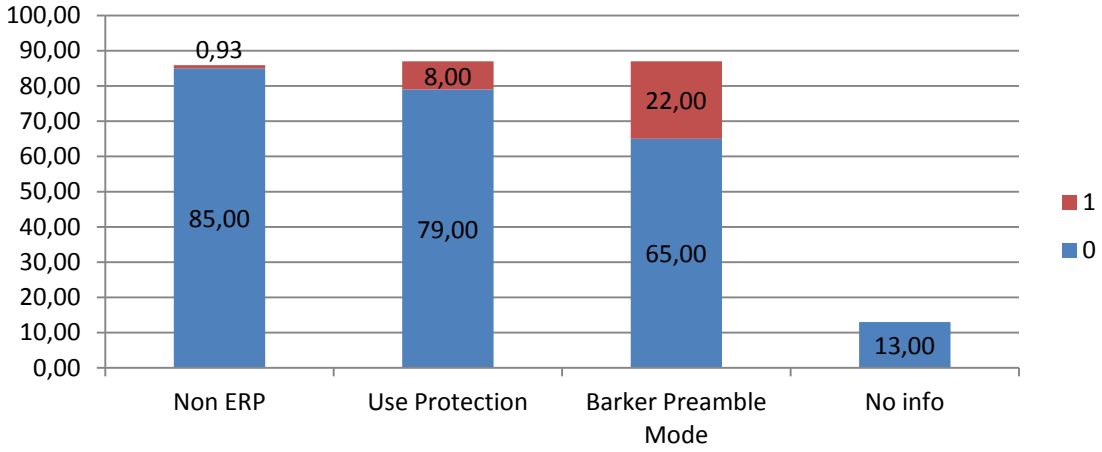

Gráfico 3.8 Mecanismos de Protección

Non ERP indica que existe algun dispositivo No ERP asociado en el BSS. Se ha detectado únicamente un 0,93%.

Use Protection es activado por el bit Non_ERP_Present. Puede indicar que existen dispositivos 802.11b en celdas vecinas. Este valor aumenta ya que la cantidad de dispositivos en celdas vecinas es mayor.

Se ha detectado un 22,39% de estaciones con el bit Barker Preamble Mode activado: Esto sucede cuando una estación no es capaz de usar el preámbulo corto.

Por lo tanto, se observa un 30% de los casos en los que se necesitan mecanismos de protección por la presencia de dispositivos con estándares anteriores. Esto provoca ineficiencia en la red.

3.2. Canales

El siguiente dato a estudiar ha sido la configuración de los canales por parte de los AP.

Como se comenta en el Apartado 1.6, óptimamente en la banda de 2,4GHz, los AP deberían estar configurados para trabajar en los canales 1, 6 y 11 para que no existan solapamientos de frecuencias que provoquen interferencias.

Si nos fijamos en **Gráfico 3.9** se puede observar cómo un 60% de los AP detectados cumple esta configuración. El resto de dispositivos están

configurados de manera aleatoria sobre el resto de canales, de manera que si estuviesen a distancias relativamente cerca podrían crear interferencias entre canales.

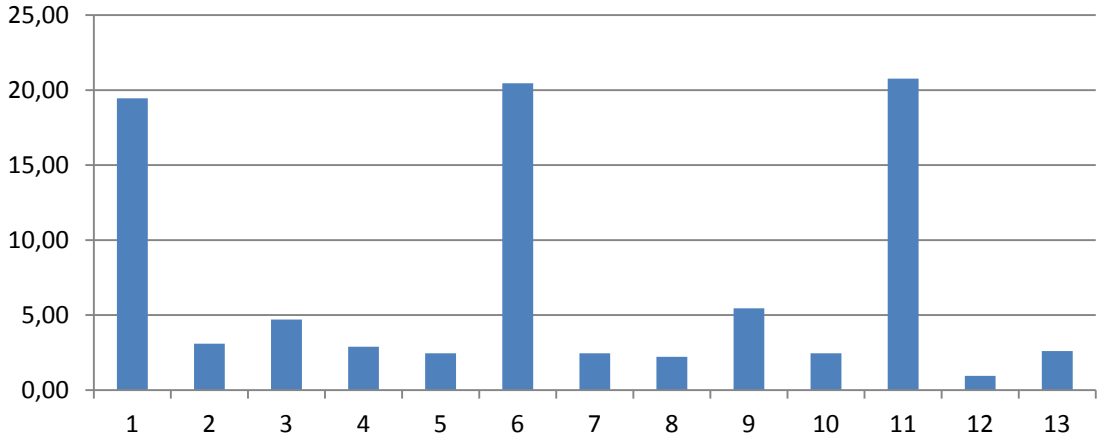

Gráfico 3.9 Canales 2,4GHz

En la banda de 5GHz se observa como la mayoría de AP se configuran en los canales 36, 40, 44 y 48 que son los permitidos en interior y no requieren el uso de mecanismos de **Selección Dinámica de Frecuencias** o **Control de Potencia de Transmisión**. Los siguientes canales hasta el 64 sí que requieren el uso de estos mecanismos y se observa cómo se intenta evitar este uso por su complejidad de configuración. Dado que los siguientes canales pueden usarse en exterior, es muy probable que los pocos AP que observamos a partir del canal 100 sean AP de exterior.

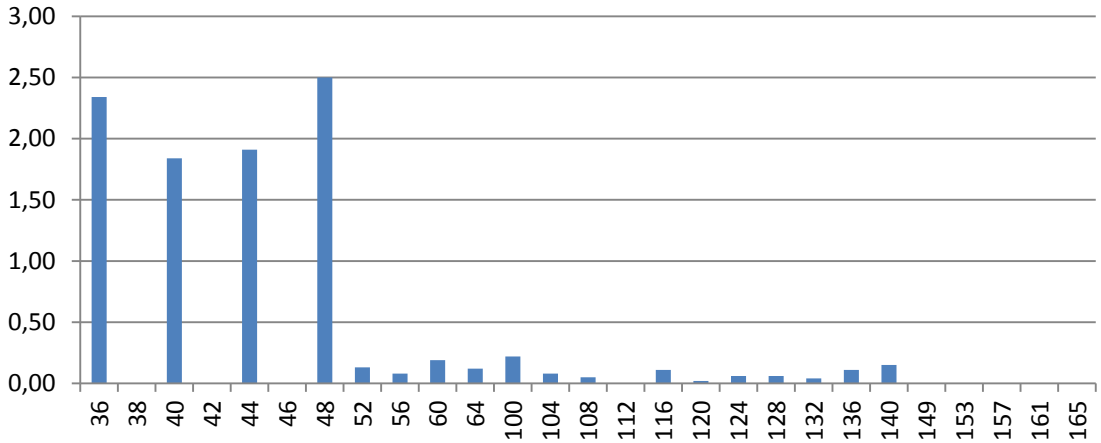

Gráfico 3.10 Canales 5GHz

3.3. Seguridad

Si observamos los tipos de autenticación implementados nos encontramos con tres opciones: Autenticación abierta, Pre-Shared Key y 802.1x.

Tal y como se observa en el **Gráfico 3.11**, únicamente un 4% de los AP requieren IEE802.1x. Este tipo de autenticación ha sido implantado sobre todo en entornos empresariales y *HotSpot*.

Un 17% de las WLAN no requieren autenticación y son en mayor parte AP *HotSpot* sin encriptación. Es posible que algunos de estos tengan mecanismos de inicio de sesión web para poder acceder a los servicios que ofrecen los AP. Finalmente cabe destacar que la gran mayoría de WLAN, un 79%, requieren autenticación a través de PSK, configuración típica de entorno doméstico.

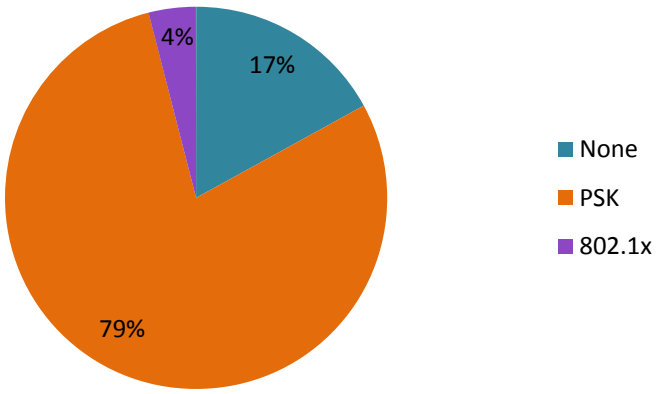

Gráfico 3.11 Autenticación

A continuación, se muestran los distintos mecanismos de encriptación detectados. Como se esperaba, la mayoría de WLAN soportan los mecanismos de encriptación más robustos. WEP, aunque se ha demostrado que no es un mecanismo de seguridad fiable, aún sigue estando presente aunque en menor medida. Pocas WLAN residenciales mantienen sus comunicaciones sin encriptación. A diferencia de las *HotSpot* que son las que contienen más comunicaciones sin cifrar, es decir más inseguras o pensadas para ofrecer solamente un servicio de acceso web, dejando las tareas de cifrado para capas superiores (e.g. navegación HTTPS). Cabe decir que con los estudios realizados no se puede cuantificar las WLAN sin encriptación que requieren este inicio de sesión web para poder acceder a los servicios ofrecidos.

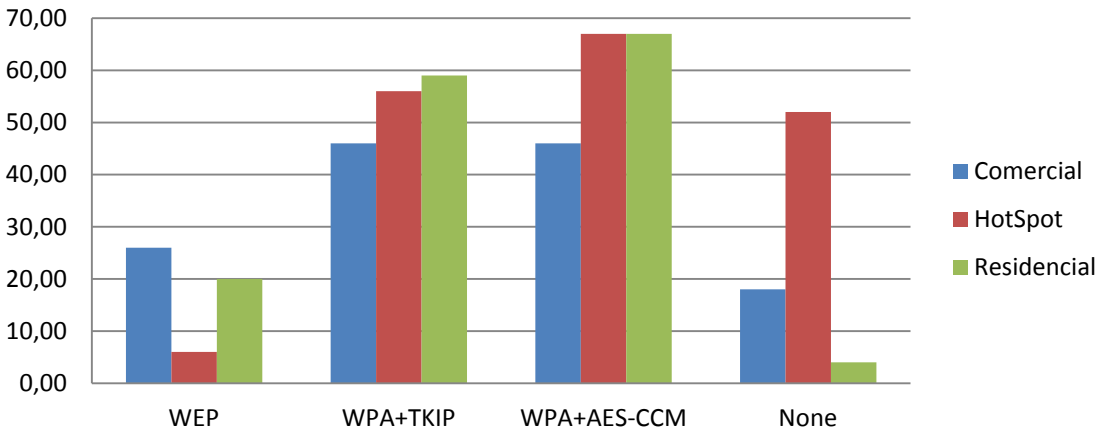

Gráfico 3.12 Encriptación Individual

3.4. CFP, APSD Y SPECTRUM:

Las tramas *Beacon* capturadas también dan información sobre otros parámetros interesantes de las redes 802.11. Algunos de estos se muestran en el **Gráfico 3.13**.

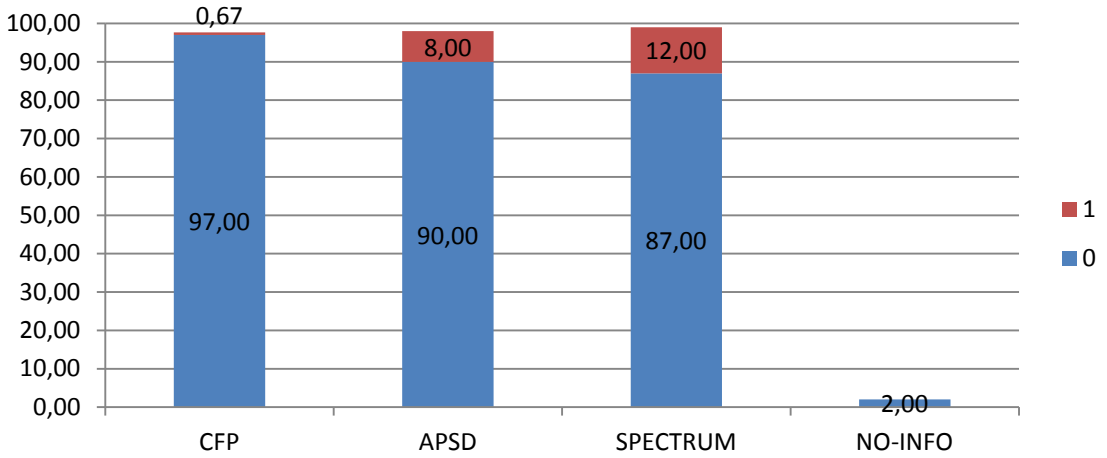

Gráfico 3.13 CFP, APSD Y SPECTRUM

El primero de ellos es *Contention Free Period* (CFP). Utilizado en redes PCF, indica que el dispositivo es capaz de utilizar PCF además de DCF. Como era de prever, casi la totalidad de las redes detectadas trabajan en DCF. Sorprendentemente se ha encontrado un 0,34% de redes anunciando CFP.

El siguiente parámetro es *Automatic Power Save Delivery* (APSD). Este es un mecanismo de ahorro de energía con el cual un dispositivo puede enviar múltiples tramas durante un periodo de servicio y pasar a un estado de inactividad hasta el próximo periodo de servicio. En el **Gráfico 3.13** se puede comprobar cómo únicamente un 8,71% de las redes detectadas soportan este sistema.

Finalmente el último parámetro es *Spectrum Power Management*. Este parámetro, asociado a las banda de 5GHz y IEEE 802.11h, es utilizado para asegurar que los canales utilizados por sistemas de radar son detectados. Se corresponde con los canales de la banda de 5GHz que utilizan estos mecanismos. Ver Apartado 1.6.1.

3.5. Tipología

Tal y como se expone en el Apartado 1.1, existen dos modos de redes WLAN: *ad-hoc* e *infraestructura.* La configuración típica en la gran mayoría de entornos en los que la finalidad es una conexión compartida a internet a través de un AP, es el modo *infraestructura.* En cambio, el modo *ad-hoc* es utilizado para la conexión entre dispositivos de forma directa y no es muy común. En el

siguiente gráfico se observa como la tipología de más del 99% de los AP detectados es *infraestructura*.

3.6. Fabricantes

La batalla comercial en el sector de las redes inalámbricas ha sido otro de los datos estudiados en este trabajo. Se ha comprovado que según el tipo de escenario, los fabricantes tanto de AP como de clientes varían.

En el ámbito **Comercial** *Cisco Systems, Inc,* es el fabricante ganador con diferencia en cuanto a AP. En cuanto a clientes, compiten en igualdad las empresas estadounidenses *Cisco Systems, Inc* y *Apple, Inc*.

Si nos fijamos en los escenarios ***HotSpot***, vuelve a ganar con una gran diferencia *Cisco Systems, Inc*. en cuanto a AP. Para los clientes presentes en este tipo de redes el fabricante ganador con diferencia es *Apple, Inc*.

En los escenarios **Residenciales**, la empresa ganadora de fabricación de AP es la Taiwanesa *Ayecom Technology*, seguida de cerca por *Comtrend Corporation*. El fabricante de clientes conectados en las zonas residenciales ganador vuelve a ser Apple aunque muy seguida por *Comtrend Corporation*.

Esta distribución de fabricantes de AP según el escenario puede explicarse debido a que los productos de *Cisco Systems, Inc*, son de gama más elevada, soportan elevado tráfico, más cantidad de usuarios, gestión centralizada, etc. Por este motivo estos dispositivos se ubican en configuraciones con mayor afluencia de usuarios y mayor requerimientos de configuración, como son las zonas **Comerciales** y los **HotSpot**. En cambio, para uso doméstico suelen usarse equipos de gama baja, más económicos, con menores prestaciones y más fáciles de configurar como los de *Ayecom Technology* o *Comtrend Corporation*.

En cuanto a los clientes, como la gran mayoría son dispositivos como ordenadores portátiles, *smartphones, tablets PC*, sorprende la gran cantidad de dispositivos *Apple, Inc* detectados y su gran dominio respecto a los demás fabricantes. La siguiente, *Samsung* junto a *Apple, Inc,* son las empresas actuales que dominan el sector de los *smartphones*, por este motivo es posible que ambas aparezcan como las dos primeras como fabricantes de clientes.

Finalmente, en la siguiente gráfica se muestra el ranking de fabricantes de AP y de clientes global.

Cisco es el ganador en cuanto a la fabricación de AP seguido de *Ayecom Technology* y *Comtrend*.

Apple es el ganador con diferencia de clientes conectados. Le prosigue la Koreana *Samsung Electronics*.

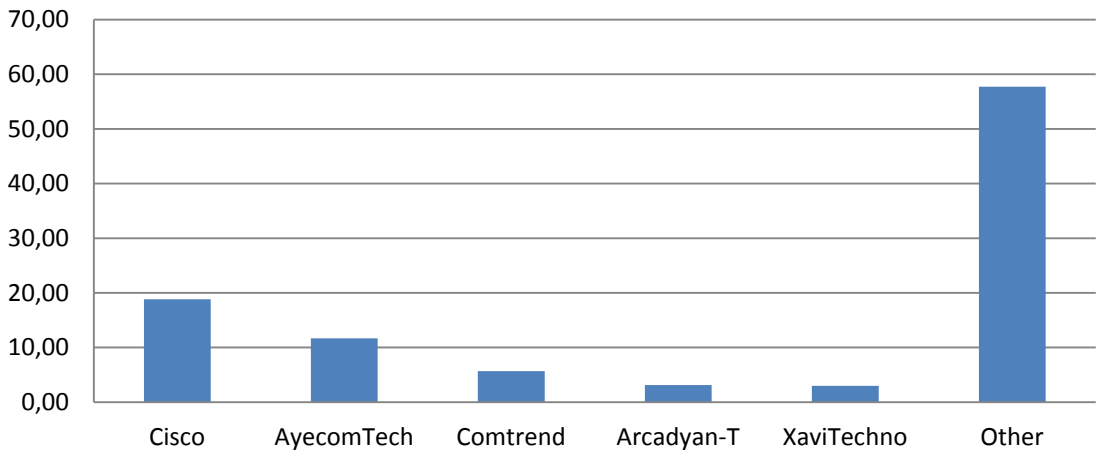

Gráfico 3.14 Fabricantes AP

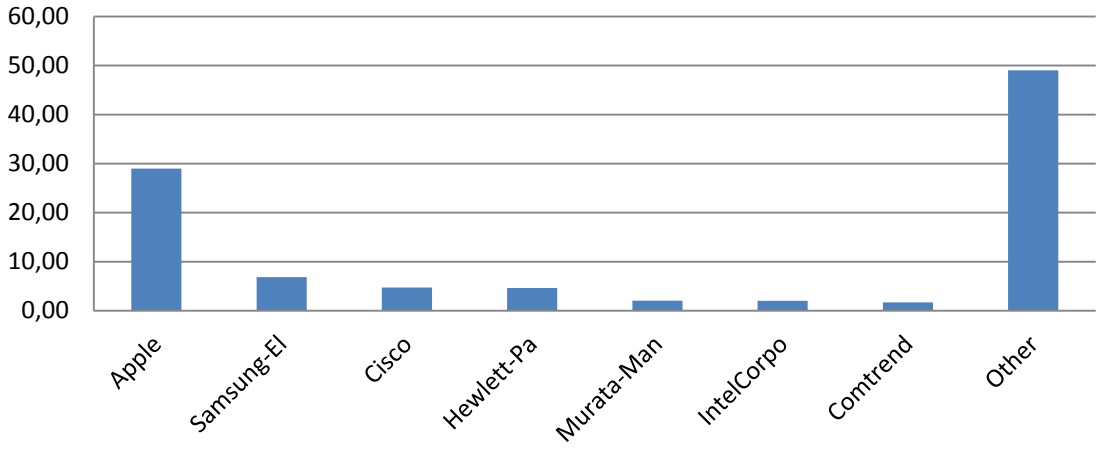

Gráfico 3.15 Fabricantes Clientes

3.7. Porcentaje de tramas de gestión:

Las tramas *Beacon*, *Probe Request* y *Probe Response*, explicadas en el Apartado 1.8, son enviadas a tasas de transferencia bajas ya que las tienen que poder recibir todos los dispositivos. Una gran cantidad de transmisiones de estas tramas ocupando el canal puede afectar al rendimiento de este.

El **Gráfico 3.16** muestra la cantidad de tramas *Beacon*, *Probe Request* y *Probe Response* capturadas. El total ha sido de 1.013.472 tramas capturadas de las cuales se observa que 345.355 tramas, un 34%, son *Beacon* y tanto las tramas *Probe Request* como las *Probe Response* se acercan al 8%, 80.000 aproximadamente respectivamente. Esto repercute seriamente en el rendimiento del canal ya que, tal y como se expone en el Apartado 1.5.1, el

medio sólo puede usarse por un equipo a la vez y se reparte a partes iguales entre todos los dispositivos del canal.

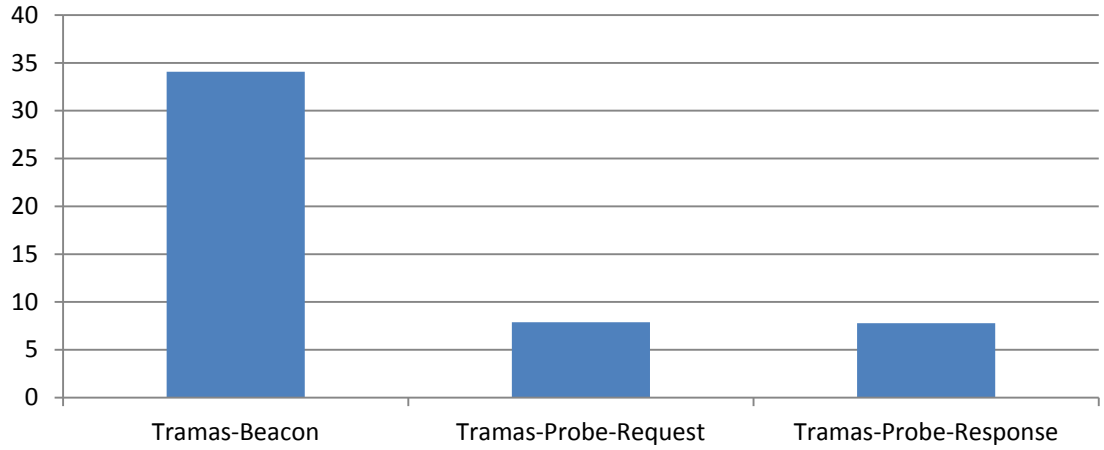

Gráfico 3.16 Porcentaje de cantidad de tramas.

Estas tramas ocupan el medio tiempo importante, aunque sean de reducido tamaño. En el **Gráfico 3.17** se observa que las tramas *Beacon* siguen correspondiendo a un 32% del total de los bytes, mientras se observa como las tramas *Probe Request* disminuyen y las *Probe Response* aumentan debido a su mayor tamaño.

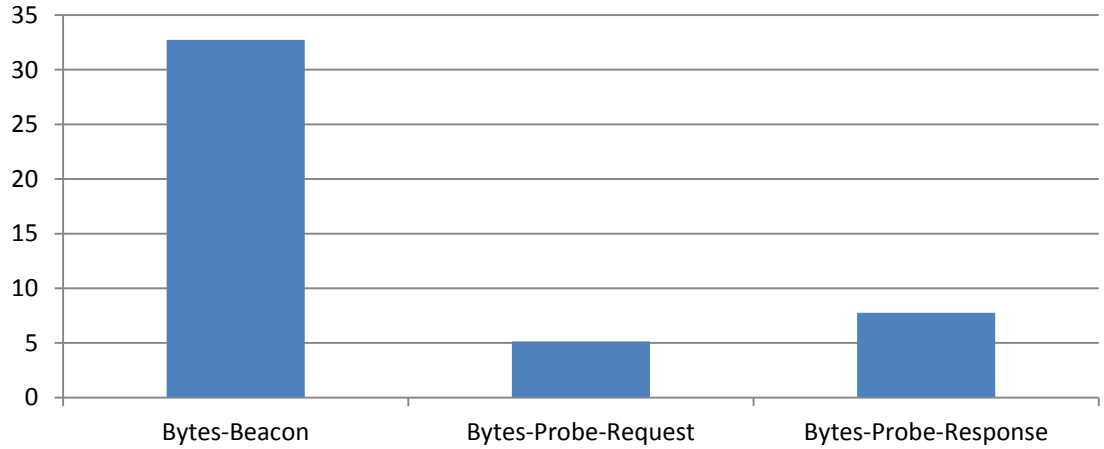

Gráfico 3.17 Porcentaje de bytes de las tramas

3.8. Proveedores de ADSL

La mayoría de los proveedores de ADSL proporcionan *routers* con Wi-Fi activado a sus clientes. Estos *routers* contienen un ESSID predefinido con el cual se puede distinguir el proveedor. En la **Tabla 3.1** se indica la relación entre los ESSID y el proveedor.

Tabla 3.1 Interpretación de los ESSID.

Proveedor	Patrón de ESSID
Movistar	WLAN_??; WLAN_????
Vodafone	Vodafone*
Jazztel	JAZZTEL_*
Ono	ONO????;ONO??????
Orange	Orange-????

Un 49% de los AP no siguen ninguno de estos patrones. Estos AP pertenecen a otros operadores como Tele2, Ya.com, etc. y a clientes que han cambiado manualmente su ESSID.

Del resto de AP que siguen los patrones detallados en la **Tabla 3.1**, en el **Gráfico 3.18** se observa como destaca, con un 27%, Movistar frente a los demás proveedores repartidos a partes iguales en un 6% cada uno.

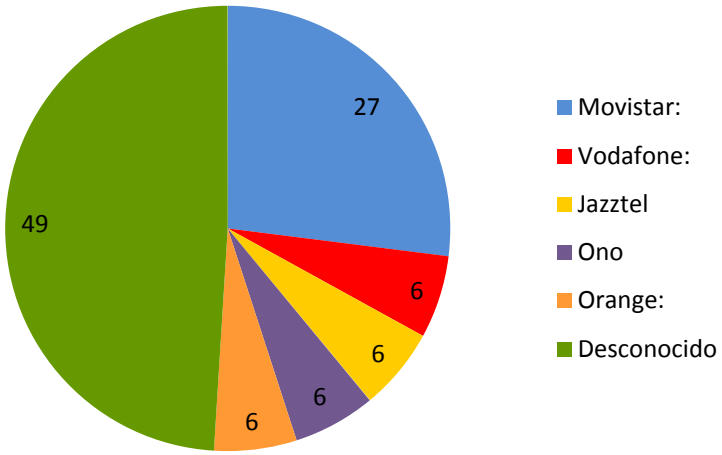

Gráfico 3.18 Proveedores de ADSL

CAPÍTULO 4. CONCLUSIONES

Las redes Wi-Fi, son unas de las más elaboradas y utilizadas en la actualidad por los usuarios. Por este motivo el análisis de este tipo de redes es de gran interés debido a la gran cantidad de mecanismos que garantizan su correcto funcionamiento. Por eso nuestros objetivos iniciales, se basaban en el análisis del uso actual de las redes inalámbricas bajo los estándares IEEE 802.11abgn y la convivencia entre ellos. El objetivo principal es el estudio del uso de 802.11b en convivencia con los nuevos estándares 802.11g y 802.11n. Llegados al final del trabajo podemos afirmar que los objetivos marcados al inicio se han cumplido prácticamente en su totalidad.

Los parámetros y las características analizadas de estas redes han sido las más relevantes dentro de las posibilidades que ofrecían las herramientas utilizadas. Al inicio del trabajo se tuvo que analizar las posibilidades que ofrecían estas herramientas para optar por unas u otras. A medida que se iba avanzando con la familiarización de las herramientas y la introducción de otras nuevas herramientas que aportaban más información, los parámetros a analizar fueron aumentando. Estos análisis incluían herramientas, tecnologías y configuraciones de las redes detectadas.

Los métodos utilizados para los distintos procesos del trabajo, descritos en este documento, han sido elegidos rigurosamente en función de los objetivos deseados. Las herramientas utilizadas han permitido obtener todos aquellos datos deseados y, junto a la aplicación realizada, se ha podido analizar al completo los parámetros marcados.

Como conclusiones sobre los resultados obtenidos, en primer lugar destaca el estudio sobre los estándares utilizados, como era de prever, actualmente los dispositivos inalámbricos son compatibles mayoritariamente con los estándares 802.11bgn, repartidos a partes iguales entre dispositivos 802.11bg y 802.11bgn. La presencia de nodos que únicamente trabajan con el estándar 802.11b prácticamente es nula. Aún así casi la totalidad de dispositivos 802.11 siguen requiriendo la compatibilidad con el estándar 802.11b. Los estándares utilizados también van en función del tipo de escenario. Los más avanzados, como es el caso de 802.11n, están implantados en gran parte en las zonas residenciales debido a que estos dispositivos son ofrecidos por las compañías telefónicas de forma gratuita y tienen, por tanto, un recambio frecuente. En cambio el estándar 802.11a prácticamente ha sido implantado en los ámbitos como centros comerciales, campus universitarios o aeropuertos.

El reparto de canales, como análisis estadístico, ha dado como resultado que aproximadamente un 60% de las redes detectadas cumplen con la recomendación de utilizar los canales 1, 6 y 11. El resto, un 30%, están configurados prácticamente a partes iguales sobre el resto de canales provocando, en el caso de que se solapen los canales, interferencias entre los AP cercanos. En la banda de 5GHz, la mayoría de los AP están configurados en los primeros canales útiles debido a la mayor facilidad de configuración de los dispositivos que trabajan en estos canales y por motivos de restricciones en el uso de estos canales.

Otra de las características de las redes 802.11 que podemos destacar en el estudio, es la seguridad utilizada por los AP. Se ha comprobado cómo, en cuanto a autenticación, una gran cantidad de estos utiliza sistemas de clave compartida, mientras que los AP sin autenticación se concentran en los escenarios *HotSpot* para conexiones esporádicas en sitios públicos. Si se tiene en cuenta la encriptación, se llega a la conclusión de que la gran mayoría utiliza los sistemas más avanzados como son WPA+TKIP y WPA+AES-CCM a partes iguales. La presencia de WEP, aunque sorprendentemente sigue en uso, su presencia hoy en día es meramente testimonial. En los escenarios Comerciales y HotSpot, son los escenarios donde se ha detectado una mayor cantidad de dispositivos con sistemas de autenticación 802.1x.

Se ha podido comprobar que la banda de 2,4GHz contiene el 90% de dispositivos. Esta banda está saturada y según el escenario, conviven una gran cantidad de dispositivos utilizando el mismo medio compartido. Sería lógico que en un futuro, muchos sistemas utilicen ambas bandas de frecuencia y que la tendencia sea el uso del estándar 802.11n aunque la banda de 5GHz tenga más limitaciones de alcance.

Las tramas de gestión *Beacon,* enviadas a tasas de transferencia bajas, suponen un 34% del total de tramas enviadas en las capturas realizadas. Teniendo en cuenta que son enviadas a tasas de transferencia bajas, repercute en el uso del canal. Además de estas, las tramas *Probe Request* y *Probe Response* suponen un 13% del total. Reducir la cantidad de estas tramas supondría un aumento del rendimiento del canal.

Los resultados obtenidos reflejan que las tecnologías Wi-Fi tienden a actualizarse a los estándares más avanzados manteniendo siempre la compatibilidad con los más antiguos siempre que sea posible.

Pese a que el resultado de este trabajo cumple con los objetivos iniciales, se han detectado posibles líneas futuras que permitirían mejorar o extender el estudio aquí presentado. En primer lugar, este estudio refleja un análisis estadístico global sobre la implantación de los parámetros estudiados, pero no contempla algunos casos concretos. Por ejemplo en cuanto a la repartición de canales, no se puede asegurar que exista solapamiento en los AP configurados fuera de los canales 1, 6 y 11. Se debería realizar un análisis por zonas de cobertura de cada uno de estos AP. *Kismet* es capaz de generar archivos con datos de geolocalización. En las líneas futuras de este trabajo se podría trabajar y tener en cuenta esta información.

Otro de los aspectos a trabajar en un futuro es en la aplicación creada por el alumno. Esta aplicación ha permitido automatizar el análisis de las múltiples capturas de la herramienta *Kismet*. Sin embargo, los resultados que se obtienen de esta aplicación, han sido diseñados explícitamente para este estudio. Las líneas futuras de este trabajo, podrían llevar a cabo una base de datos informática en la que se almacenen todas las características de las redes inalámbricas que proporciona *Kismet*, para poder extraer, posteriormente, la información deseada sin tener que cambiar código ni realizar todo el análisis de

nuevo. También sería interesante optimizar el código fuente de manera que el análisis resulte más eficiente.

Sería interesante que este estudio, realizado a fecha del año 2013, se repitiera periódicamente a lo largo de los años para poder contemplar la evolución del uso de las redes a lo largo del tiempo, añadiendo (si los hay) nuevos estándares y características al estudio.

También sería interesante extender este estudio a otros tipos de escenarios como por ejemplo entornos rurales.

BIBLIOGRAFÍA

[1] Güimi, «Redes de comunicaciones,» Abril 2009. [En línea]. Available: http://guimi.net/monograficos/G-Redes_de_comunicaciones/G-Redes_de_comunicaciones.pdf. [Último acceso: Setiembre 2013].

[2] «Wikipedia,» IEEE 802.11, 17 Octubre 2013. [En línea]. Available: http://es.wikipedia.org/wiki/IEEE_802.11.

[3] R. Amado Gimenez, «Archive.org. Análisis de la seguridad en redes 802.11,» Marzo 2008. [En línea]. Available: http://www.securityartwork.es/wp-content/uploads/2008/10/seguridad-en-redes-80211.pdf. [Último acceso: Setiembre 2013].

[4] «Escuela Técnica Superior de Ingeniería de Bilbao, SEGURIDAD EN WI-FI,» 2006. [En línea]. Available: http://det.bi.ehu.es/redesLAN/attach?page=Grupos06_07%2FResumen+seguridad+WIFI.pdf. [Último acceso: 2013].

[5] J. J. Yunquera Torres, «Biblioteca de Ingeniería. Universidad de Sevilla,» [En línea]. Available: http://bibing.us.es/proyectos/abreproy/11138/fichero/memor%C3%ADa%252FCap%C3%ADtulo+7.pdf. [Último acceso: Setiembre 2013].

[6] «Wikipedia,» Capa física, 8 Noviembre 2013. [En línea]. Available: http://es.wikipedia.org/wiki/Capa_f%C3%ADsica. [Último acceso: Noviembre 2013].

[7] J. J. Yunquera Torres, «Biblioteca de Ingeniería. Universidad de Sevilla,» [En línea]. Available: http://bibing.us.es/proyectos/abreproy/11138/fichero/memor%C3%ADa%252FCap%C3%ADtulo+4.pdf. [Último acceso: Octubre 2013].

[8] J.-H. C. J.-H. H. a. C. Y. See-hwan Yoo, «Springer Link. Eliminating the Performance Anomaly of 802.11b,» 17 Abril 2005. [En línea]. Available: http://link.springer.com/chapter/10.1007/978-3-540-31957-3_120.

[9] L. Casals, E. Zola y P. Chaparro, «Xarxes LAN sense fils,» Barcelona, 2008.

[10] A. Masalias Falcon y D. Pérez Díaz de Cerio, «UPCommons. Adaptación y test del protocolo 802.11e al simulador ns-2.28,» 23 Febrero 2006. [En línea]. Available: http://upcommons.upc.edu/pfc/bitstream/2099.1/3555/1/53833-1.pdf.

[11] J. J. Yunquera Torres, «Biblioteca de Ingeniería. Universidad de Sevilla,» [En línea]. Available: http://bibing.us.es/proyectos/abreproy/11138/fichero/memor%C3%ADa%252FCap%C3%ADtulo+5.pdf. [Último acceso: Octubre 2013].

[12] «Dot Eleven,» Chapter 4 - 802.11 Management frames, 14 Diciembre 2011. [En línea]. Available: http://dot11.info/index.php?title=Chapter_4_-_802.11_Management_frames. [Último acceso: Octubre 2013].

[13] D. Akin, «Certified Wireless Network Professional. Protection Ripple in ERP 802.11 WLANs,» Junio 2004. [En línea]. Available: http://www.cwnp.com/cmsAdmin/uploads/protection_ripple_in_erp_802-11_wlans.pdf. [Último acceso: Setiembre 2013].

[14] IEEE, «IEEE Std 802.11™-2012 (Revision of IEEE Std 802.11-2007),» New York, 2012.

[15] «List of WLAN channels,» [En línea]. Available: http://en.wikipedia.org/wiki/List_of_WLAN_channels.

[16] «Small Net Builder,» 30 Noviembre 2003. [En línea]. Available: http://www.smallnetbuilder.com/wireless/wireless-features/24424-atherossupergpt1?start=2. [Último acceso: Octubre 2013].

[17] P. Fuxjager, D. Valerio y F. Ricciato, «Userver,» 1 Julio 2007. [En línea]. Available: http://userver.ftw.at/~valerio/files/wons.pdf. [Último acceso: Noviembre 2013].

[18] A. Mishra, E. Rozner, S. Banerjee y W. Arbaugh, «acm SIGCOMM,» 10 Agosto 2005. [En línea]. Available: http://conferences.sigcomm.org/imc/2005/papers/imc05efiles/mishra/mishra.pdf. [Último acceso: Octubre 2013].

[19] E. García Villegas, R. Vidal Ferré y J. Paradells, «Wiley Online Library, Frequency assignments in IEEE 802.11 WLANs with efficient spectrum sharing,» 1 Setiembre 2008. [En línea]. Available: http://onlinelibrary.wiley.com/doi/10.1002/wcm.670/abstract. [Último acceso: Noviembre 2013].

[20] A. B. a. A. Z. Ariton E. Xhafa, «http://www.academypublisher.com/. On the 20/40 MHz Coexistence of Overlapping BSSs in WLANs,» Julio 2008. [En línea]. Available: http://www.academypublisher.com/jnw/vol03/no07/jnw03075663.pdf. [Último acceso: Octubre 2013].

[21] «WifiWay,» [En línea]. Available: http://www.wifiway.org/. [Último acceso: 2013].

[22] [En línea]. Available: http://www.ciudadwireless.com/alfa_network_ubdo-a-ubdo-a5-_802-11a-b-g-n_long-range_outdoor_radio_with_type_external_antenna_connector_cable-p-4658.html. [Último acceso: 2013].

[23] [En línea]. Available: http://fs.airlive.com/manual/AirLive_WAE-5AG_SpecSheet.pdf.

[24] «www.Wireshark.org,» [En línea]. Available: http://www.wireshark.org/docs/man-pages/tshark.html.

[25] «JAX-RS,» [En línea]. Available: http://es.wikipedia.org/wiki/JAX-RS.

[26] «Gnuplot,» Setiembre 2010. [En línea]. Available: http://www.gnuplot.info/docs_4.6/gnuplot.pdf. [Último acceso: Junio 2013].

[27] «Capítulo 4. Clases persistentes,» [En línea]. Available: http://docs.jboss.org/hibernate/core/3.5/reference/es-ES/html/persistent-classes.html.

[28] M. Canet, V. Almenar, J. Marin-Roig y J. Valls, «URSI España. SINCRONIZACIÓN DE TIEMPO PARA EL ESTÁNDAR IEEE 802.11a/g,» 2007. [En línea]. Available: http://ursi.usc.es/articulos_modernos/la_laguna_2007/PDF/P123.PDF. [Último acceso: 2013].

[29] P. D. Chávez Muñoz y E. Montes Moscol, «Repositorio Digital de Tesis PUCP. ESTUDIO DE LA MIGRACIÓN DEL ESTÁNDAR 802.11 AL

ESTÁNDAR 802.16 EN ZONAS RURALES,» Noviembre 2008. [En línea]. Available: http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/209/MONTES_EDUARDO_ESTUDIO_MIGRACION_DEL%20_ESTANDAR_ZONAS_RURALES.pdf?sequence=2. [Último acceso: Noviembre 2013].

[30] S. Ekhator, «http://www.bth.se/. Evaluating Kismet and NetStumbler as Network Security Tools & Solutions,» 29 Junio 2010. [En línea]. Available: http://www.bth.se/fou/cuppsats.nsf/all/198f78117200478fc1257751004cb78f/$file/Kismet%20Thesis.pdf. [Último acceso: Junio 2013].

[31] E. P. y M. Burton, «Tech online. Channel Overlap Calculations for 802.11b Networks,» 25 Febrero 2002. [En línea]. Available: http://www.microalcarria.com/descargas/documentos/Wireless/Four%20channel%20in%20802.11b.pdf. [Último acceso: Octubre 2013].

[32] J. J. Yunquera Torres, «Biblioteca de Ingenieria. Universidad de Sevilla. EL ESTÁNDAR IEEE 802.11,» [En línea]. Available: http://bibing.us.es/proyectos/abreproy/11138/fichero/memor%C3%ADa%252FCap%C3%ADtulo+3.pdf. [Último acceso: 2013].

Escola d'Enginyeria de Telecomunicació i Aeroespacial de Castelldefels
UNIVERSITAT POLITÈCNICA DE CATALUNYA

ANEXOS

TÍTULO DEL TFC: Cómo conocer el uso actual de las redes WLAN basadas en IEEE 802.11

TITULACIÓN: Ingeniería Técnica de Telecomunicaciones, Especialidad Telemática

AUTOR: Xavier Tena Carbonell

DIRECTOR: Eduard García Villegas

FECHA: Miércoles 4 de Diciembre 2013

CAPÍTULO 1. DEFINICIONES, ACRÓNIMOS Y ABREVIACIONES

Durante todo el documento se tratarán términos de forma abreviada. En este Apartado se indican dichos términos y una pequeña definición.

- **QAM:** Quadrature Amplitude Modulation.
- **20/40 BSS Coexistence:** Se utiliza para evitar conflictos en situaciones en las que el uso de los 40MHz pueda interferir a otras estaciones que usan únicamente 20MHz
- **802.11:** Estándar que define el uso de los dos niveles inferiores de la arquitectura OSI, especificando sus normas de funcionamiento en una WLAN.
- **ACK:** Acknowledgement. Acuse de recibo.
- **Ad-hoc:** Red inalámbrica en la que no hay un nodo central, sino que todos los dispositivos están en igualdad de condiciones.
- **AES-CCMP:** Advanced Encryption Standard. Esquema de cifrado
- **AP:** Access Point. Un Punto de Acceso es un puente entre la red inalámbrica y otra red, que se encarga de realizar las conversiones de trama pertinentes.
- **APSD:** Automatic Power Save Delivery. Mecanismo de ahorro energético definido en 802.11. Permite al cliente solicitar tráfico en cola a la vez que espera una trama *Beacon*.
- **BARKER:** Secuencia finita de N valores de +1 y -1.
- **BPSK:** Binary PSK
- **BSS:** Basic Service Set. Define el bloque básico en una WLAN 802.11. En modo infraestructura un AP con todas las estaciones asociadas forman un BSS.
- **Buffer:** Memoria física usada temporalmente para guardar datos mientras son movidos de un sitio a otro.
- ***CF Parameter Set*:** Contention Free Parameter Set.
- **CFP:** Contention Free Period. Periodo libre de contención.
- ***Channel Switch*:** Mensaje enviado por el AP avisando de un cambio de canal.
- ***Channel Usage*:** Mensaje que indica el estado del canal
- **CSMA/CA:** Carrier Sense Multiple Access with Collision Avoidance. Protocolo de control de acceso a redes de bajo nivel que permite que múltiples estaciones utilicen el mismo medio de transmisión.
- **CTS:** Clear to Send. Trama que indica que está preparado para transmitir.
- **DBPSK:** BPSK diferencial.
- **DCF:** Distributed Coordination Function. Ver Apartado 1.5.1
- ***DSSS** Parameter Set*: Parámetros de DSSS.
- **DSSS:** Direct Sequence Spread Spectrum. Ver Apartado 1.4.1
- **EAP:** Extensible Authenticacion Protocol. Autenticación Framework. Es una estructura de soporte para crear mecanismos de autenticación.
- **ECJ:** Eclipse Compiler for Java.
- ***ERP*:** Extended Rate PHY. Indica la presencia de estaciones 802.11b

- ***Extended Supported Rates*:** Campo de la trama *Beacon* utilizado cuando existen más de 8 supported rates
- ***FH Parameter*:** Frequency Hop Parameter. Contiene todos los parámetros necesarios para empezar el salto de frecuencias.
- ***FH Pattern Table*:** Contiene el patrón de saltos de canal.
- **FHSS:** Frequency Hopping Spread Spectrum. Es una técnica de modulación en espectro ensanchado.
- **GTK:** Group Temporal Key.
- **HCCA:** HCF Controlled Acces. Es equivalente a HCF
- **HCF:** Hybrid Coordination Function. Es un mecanismo de acceso al medio. Ver apartado 1.5.3
- ***HT Capabilities*:** High Throughput Capabilities. Indica las opciones de 802.11n
- ***HT Operation*:** Indica los modos de operacion de 802.11n
- **IDE:** Integrated Development Enviroment. Programa informático compuesto por un conjunto de herramientas d programación
- **IEEE:** Instituto de Ingenieros Eléctricos y Electrónicos. Es una asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas
- **ISM:** Industrial Scientific and Medical. Son bandas de frecuencias reservadas internacionalmente para uso no comercial de radiofrecuencia electromagnética en áreas industrial, científica y médica.
- **JDOM:** Biblioteca de código abierto para manipulaciones de datos XML optimizados para java
- **JDT o JDK:** Java Development ToolKit. Software que provee herramientas de desarrollo para la creación de programas en Java.
- **JSON:** JavaScript Object Notation. Es un formato ligero para el intercambio de datos que no requiere el uso de XML.
- **JVM:** Java Virtual Machine. Es una máquina virtual ejecutable en una plataforma específica, capaz de interpretar y ejecutar instrucciones expresadas en el bytecode Java.
- **KDE:** Es una comunidad internacional que desarrolla software libre.
- **MAC:** Media Acces Control. Conjunto de mecanismos y protocolos a través de los cuales varios "interlocutores" se ponen de acuerdo para compartir un medio de transmisión común.
- ***Mesh ID*:** Identificador de una red mallada.
- **MIMO:** Multiple-Input Multiple-Output. Uso de múltiples antenas a la vez para transmitir y recibir tramas.
- **MPDU:** MAC Protocol Data Unit. Múltiples unidades de datos tras la fragmentación.
- **MSDU:** MAC Service Data Unit. Representa los datos antes de la fragmentación.
- ***Multiple BSSID*:** Varios AP con distintos SSID y distinta seguridad (pero en el mismo canal).
- **OFDM:** Ortogonal Frequency Division Multiplexing. Ver Apartado 1.4.4
- **OSI:** Open System Interconnection. Es un marco de referencia para la definición de arquitecturas en la interconexión de los sistemas de comunicaciones.
- **PCF:** Point Coordination Function. Es un mecanismo de acceso al medio.

- **PMK:** Primary Master Key
- **POJO:** Plain Old Java Object
- **PSK:** Phase Shift Keying
- **PTK:** Pairwise Key Expansion
- **QoS:** Quality of Service. Conjunto de estándares y mecanismos que realizan el control de reservas de recursos en red.
- **QPSK:** Offset Quadrature PSK
- **RC4:** Sistema de cifrado de flujo con un algoritmo simple.
- **RFID:** Radio Frequency Identiication. Tarjetas de identificación por radiofrecuencia.
- **RTS:** Request To Send. Trama enviada por el emisor indicando que desea transmitir.
- **SSID:** Service Set Identifier. Código de un máximo de 32 caracteres incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de esa red.
- ***Supported rates*:** Tasas de transmisión soportadas.
- **TC:** Traffic Class. Definición del tipo de tráfico utilizado en HCF.
- **TCP:** Transmission Control Protocol. Protocolo orientado a conexión dentro del nivel de transporte del modelo OSI que permite la entrega de paquetes de manera fiable.
- **TKIP:** Temporal Key Protocol. Protocolo de seguridad que combina una clave secreta con un vector de inicialización cifrado con RC4
- **TS:** Traffic Stream. Tipo de tráfico utilizado en HCF.
- **TSF:** Timing Syncrhonization Function. Clock local sincronizado con el TSF de las demás estaciones dentro del mismo BSS
- **UDP:** User Datagram Protocol. Protocolo de nivel de transporte basado en el intercambio de datagramas sin la necesidad de que haya establecido previamente una conexión.
- **Use Protection:** Mensaje enviado para advertir de la presencia de estaciones lentas en la red.
- **WEP:** Wired Equivalent Privacy. Sistema de cifrado incluido en el estándar 802.11.
- **Wi-Fi:** Wireless Fidelity. Es una red que cumple con el estándar 802.11. Wi-Fi es el nombre de la certificación otorgada por la WECA (Actualmente Wi-Fi Alliance).
- **WLAN:** Wireless Local Area Network. Red de Área Local inalámbrica.
- **WPA:** Wi-Fi Protected Access. Sistema para proteger las redes inalámbricas.
- **WPA2:** Versión avanzada de WPA. También llamada 802.11i.
- **XML:** eXtensible Markup Language. Lenguaje de marcas utilizado para almacenar datos en forma legible

CAPÍTULO 2. METODOLOGÍA

A continuación se presenta el funcionamiento de todo el proceso para realizar las estadísticas de este trabajo.

2.1. Capturas con *Kismet*

2.1.1. Activar tarjeta/s Wi-Fi en modo monitor

Lo primero que se debe hacer antes de iniciar y configurar *Kismet* es activar el modo monitor para las tarjetas Wi-Fi con el siguiente comando:

```
airmon-ng start nombreinterfaz
```

Una vez realizado este paso se visualizará la configuración de las interfaces inalámbricas con el comando:

```
iwconfig
```

Deben aparecer dos unidades (mon0 y wlan0mon) como en la siguiente captura:

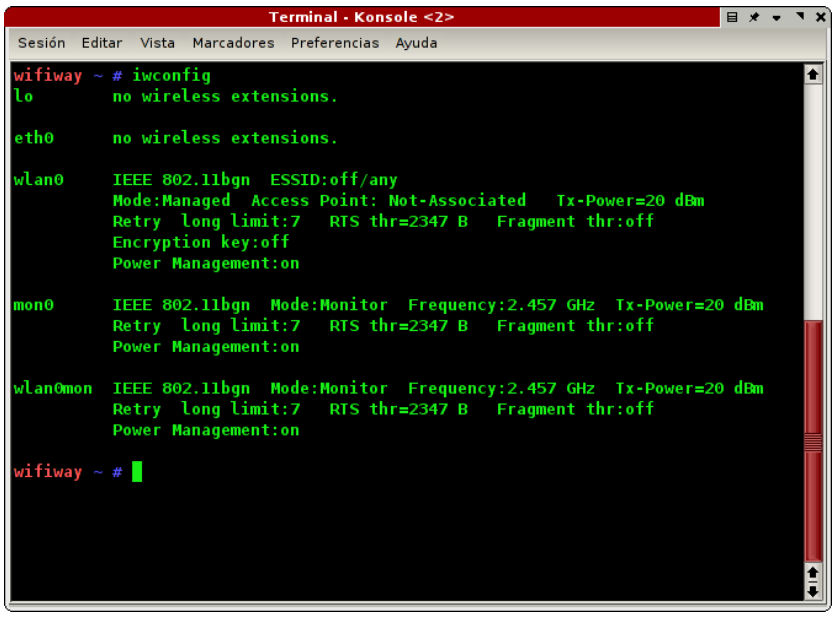

Figura 2.1

2.1.2. Configurar *Kismet*

Editar y configurar el fichero *Kismet.conf*:

El fichero *Kismet*.conf se encuentra en el directorio /usr/local/etc/.

En caso de no encontrarlo en este directorio se puede hacer la búsqueda con el siguiente comando como root:

```
find / -name 'Kismet.conf'
```

Para editar el fichero *Kismet.conf* usaremos *kwrite* o cualquier editor de texto siempre como usuario root.

Las modificaciones que se deben hacer en el fichero *Kismet.conf* son:

- `ncsource=mon0:name=nombredelatarjeta,hop=true`
- `suiduser=nombredeltécnico`
- `channelvelocity=3`
- `gps=false`
- `logtypes=pcapdump,netxml`
- `pcapdumpformat=80211`
- `logdefault=lugarDeCaptura`
- `logtemplate=%p%n-%d-%t-%i.%l`

2.1.3. Ejecutar *Kismet*:

Abrir un nuevo terminal y dirigirse al directorio donde se quiere guardar los ficheros que se crearán al finalizar la captura.
Escribir el comando:

```
Kismet
```

Se iniciará el programa y aparecerá el siguiente mensaje de advertencia:

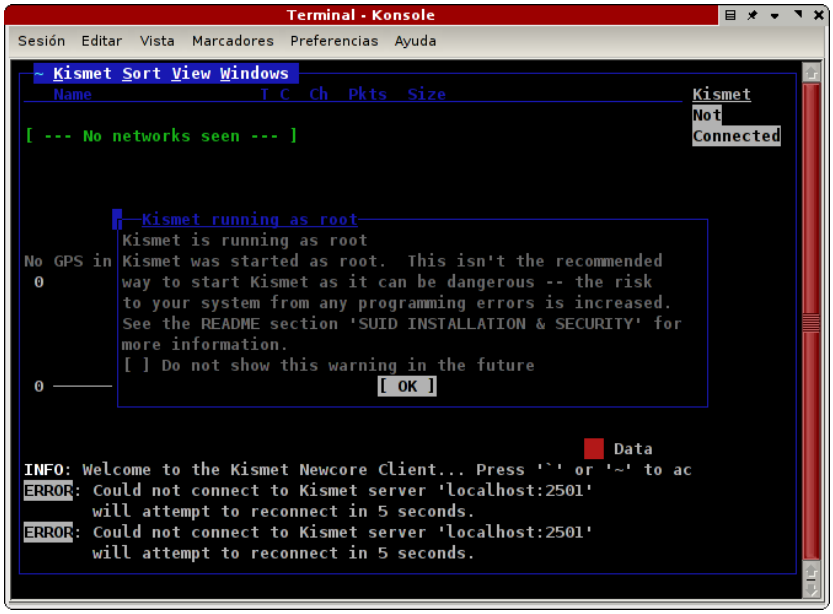

Figura 2.2

Pulsar *Enter* para aceptar. Aparecerá el siguiente mensaje:

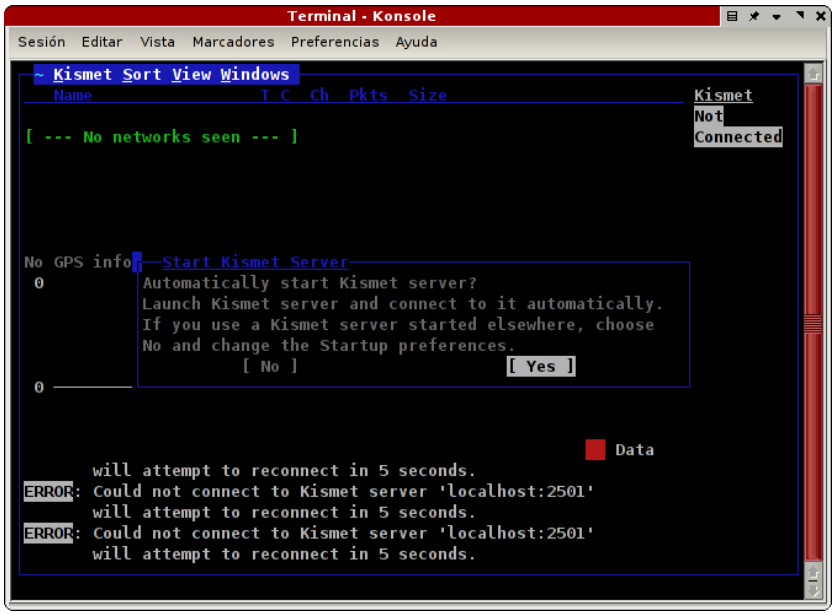

Figura 2.3

Pulsar *Enter* para aceptar. Aparecerá el siguiente mensaje.

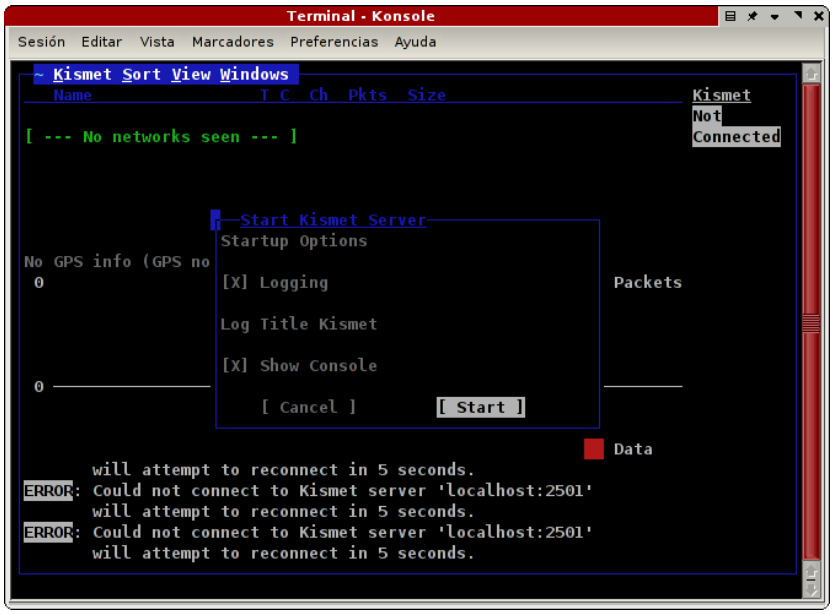

Figura 2.4

Pulsar Enter para aceptar. *Kismet* empezará a capturar paquetes en este mismo instante. Se verá cierta información de las redes capturadas en pantalla.

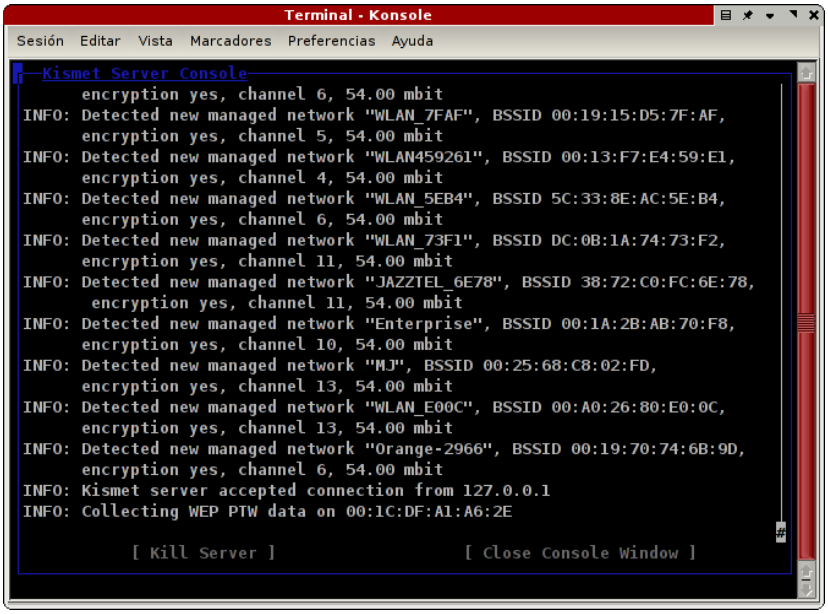

Figura 2.5

Con la tecla "tabulador" se seleccionará "Close Console Window", Pulsar Enter y aparecerá la siguiente ventana:

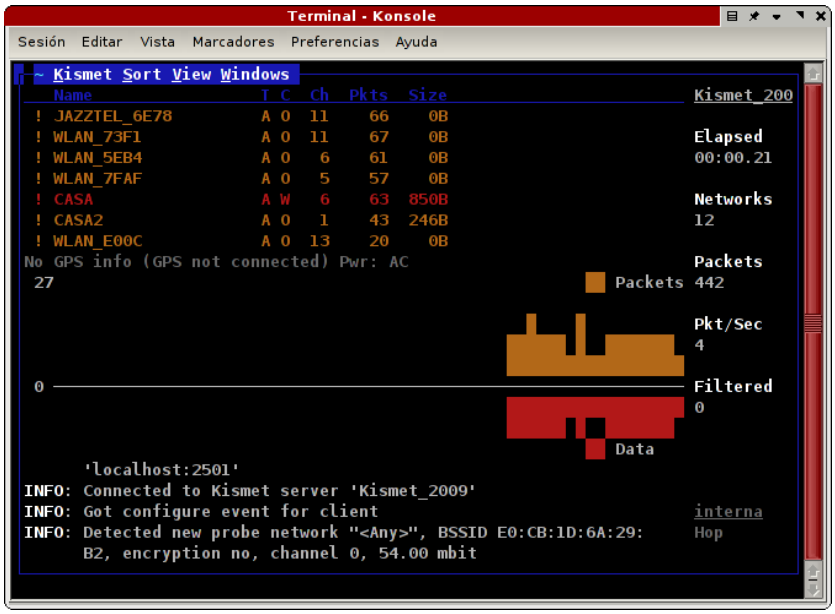

Figura 2.6

Se dejará la aplicación realizando la captura durante el tiempo deseado. Para detener la captura se clicará (con el mouse) en Quit dentro del menú *Kismet*.

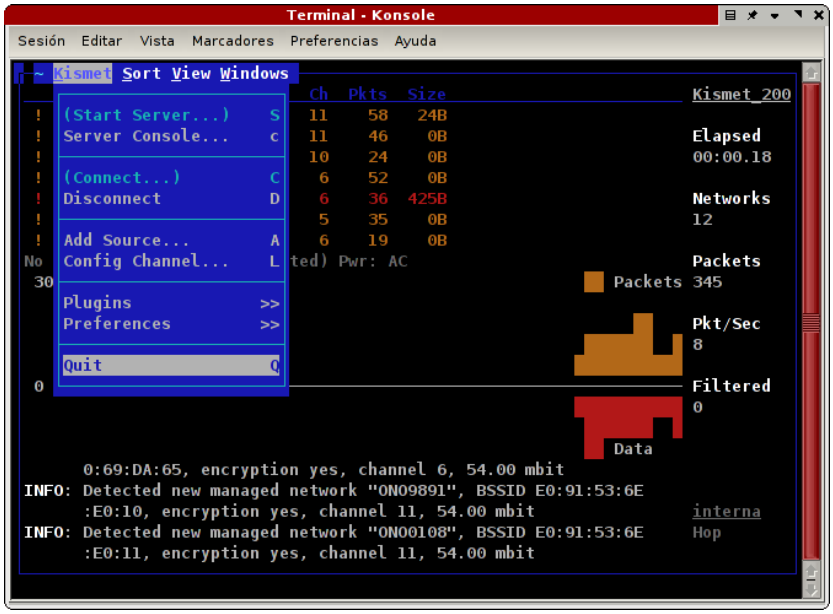

Figura 2.7

Aparecerá el siguiente mensaje y se seleccionará la opción *Kill*.

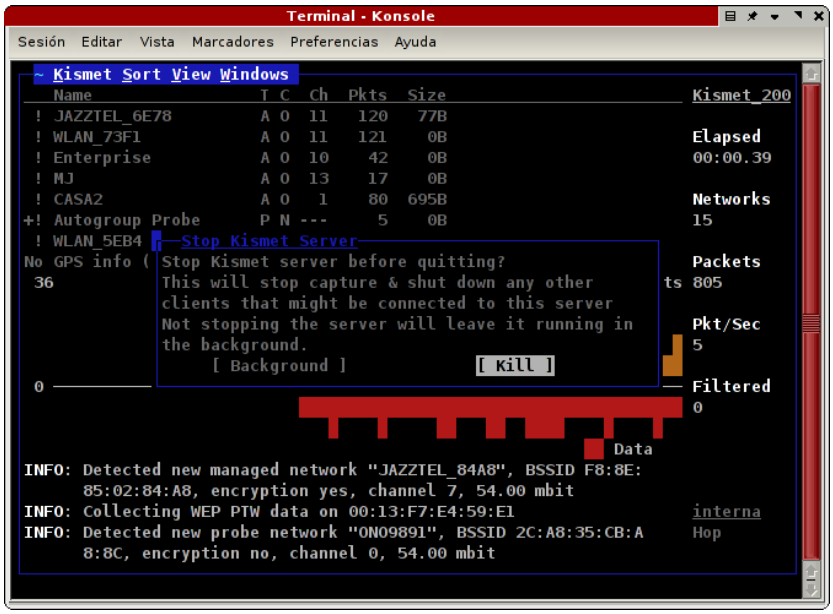

Figura 2.8

Una vez finalizada la captura se comprobará que la aplicación *Kismet* haya generado dos archivos en el directorio desde donde se estaba ejecutando la aplicación.

Las extensiones de los archivos serán *.netxml* y *.pcapdump*. Se comprobará que los archivos contengan información sobre las redes WLAN capturadas abriendo el archivo *.netxml* con un editor de textos y el *.pcapdump* con *Wireshark*

Si no se desean realizar más capturas quitaremos el modo monitor de la tarjeta Wi-Fi. Para ello ejecutaremos el siguiente comando:

```
airmon-ng stop nombreinterfaz
```

2.2. Ejecutar la aplicación

Una vez se tienen las capturas realizadas se procede al análisis de las mismas.

Las capturas que se quieren analizar deben estar todas dentro del mismo directorio. En concreto deben estar en la ruta "./*Kismet*/nombreDelDirectorio/". Se analizan todas las capturas con extensión *.netxml* y *.pcapdump*. Los dos ficheros asociados deben tener el mismo nombre.

Una vez se tiene el directorio creado con los ficheros de captura dentro se abre un terminal y se escribe la ruta de la aplicación.

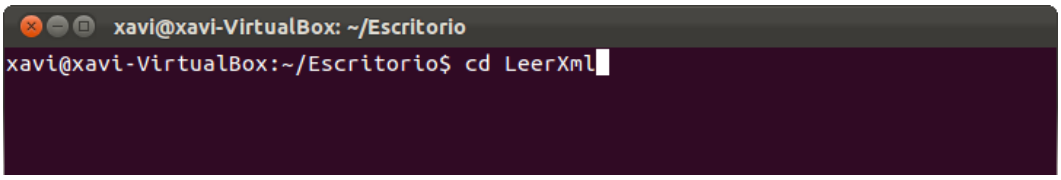

Figura 2.9

A continuación se ejecuta el script ./executar.sh seguido del nombre del directorio en el que están todos los ficheros de captura (*.netxml* y *.pcapdump*).

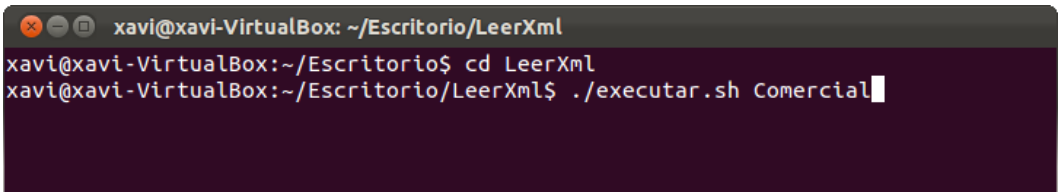

Figura 2.10

La aplicación se encarga de leer y analizar los ficheros y como resultado se obtendrán varios ficheros de texto y gráficas con los resultados.

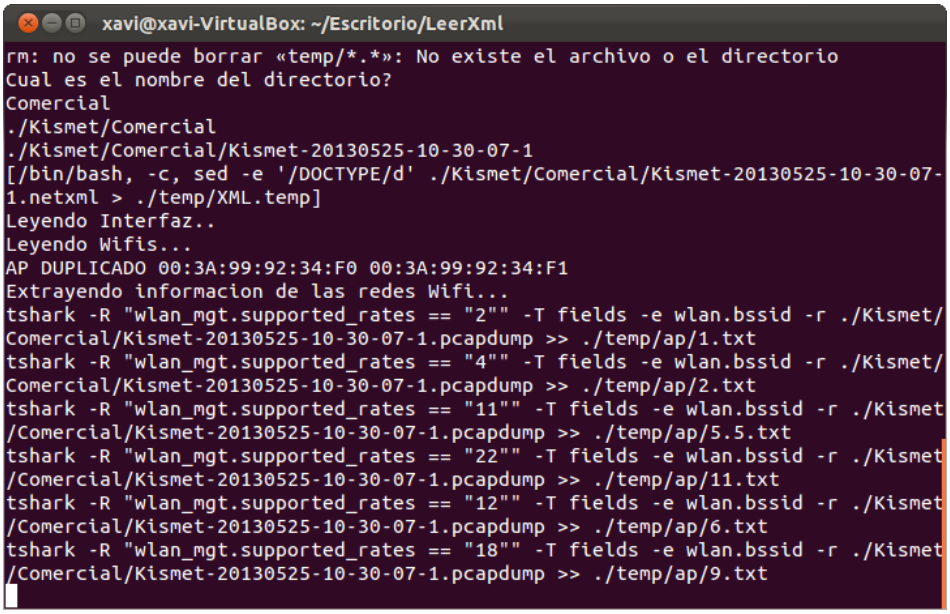

Figura 2.11

CAPÍTULO 3. MAPA DE LOS ESCENARIOS

Sant Cugat

Mataró