Trabajo Final de Carrera

Seguridad en Comunicaciones Sin Hilo: Riesgos y Amenazas Wi-Fi

Autor: Mª Begoña Ortiz Leston
Estudiante de Ingeniería Técnica en Telecomunicaciones
Universitat Oberta de Catalunya (UOC)
bortizl@uoc.edu

Agradecimientos

A Luis y Eduardo por su cariño y comprensión.

Indice de Contenidos

Indice de Figuras

Indice de Tablas

1

1. Introducción

1.1. Preámbulo

Las tecnologías inalámbricas en los últimos años, han ido ganado protagonismo en la vida diaria de las empresas, instituciones y entornos personales. IEEE 802.11 agrupa un conjunto de estándares de comunicación inalámbrica que ofrecen soluciones para compartir información sin hacer uso de medios cableados. Obteniendo la posibilidad de establecer canales de datos entre entornos móviles y estáticos, eliminando las barreras arquitectónicas.

IEEE 802.11 supone uno de los estándares de comunicación por radiofrecuencia más utilizados y populares para redes de área local. No es extraño que dispositivos como ordenadores portátiles, PDA´s, móviles e incluso maquinaria industrial hagan uso de este estándar como solución inalámbrica para interconectar y transferir cualquier tipo de información, datos, voz o video. Como ejemplo basta con realizar una búsqueda mediante su ordenador portátil de las redes inalámbricas disponibles en su entorno, para darse cuenta de la gran acogida que esta tecnología ha tenido en la sociedad.

La Asociación para la Investigación de Medios de Comunicación (AIMC), destacó en su informe de 2012 sobre el perfil del internauta así como sus hábitos en la utilización de Internet, que el 52 % de los usuarios de Internet obtuvo acceso a la red de redes a través de la tecnología inalámbrica. Todo apunta a que el crecimiento y despliegue de este tipo de redes seguirá creciendo en los próximos años. Pero no solo los usuarios domésticos adquieren productos con esta tecnología también lo hacen pequeñas y grandes empresas, instituciones y organismos públicos, cada vez mas hacen uso del estándar como solución de comunicación.

Es por todo esto, que no debe descuidarse la seguridad al hacer uso de dispositivos que implementen la norma 802.11, puesto que puede suponer una ventana abierta al exterior por donde cualquier persona mal intencionada pueda robar información, pudiendo incluso obtener el control de los activos del usuario. Este proyecto esta orientado a identificar las distintas tecnologías sin hilos, analizar los diferentes protocolos y metodologías de protección del canal inalámbrico, realizando un estudio de las vulnerabilidades y métodos de ataques.

1.2. Justificación y punto de partida

En este TFC se realiza una recopilación sobre distintos aspectos de la arquitectura para redes sin hilo, en concreto basada en la tecnología Wireless. Centrándose tanto en el campo de la seguridad en este tipo de redes, como en el análisis de las amenazas, y vulnerabilidades así como en las principales técnicas existentes que permiten para conseguir vulnerarla. Por último se describen las distintas herramientas que se encuentran en el mercado para atacar este tipo de redes.

1.3. Objeto y alcance

El objeto de este trabajo es consolidar los conocimientos adquiridos en el desarrollo de los estudios de Ingeniería Técnica en Telecomunicaciones, especialidad en Telemática en la Universidad Oberta de Cataluña.

De la misma manera se pretende realizar un estudio sobre los riesgos y amenazas existentes en las redes wireless. Analizar las soluciones actuales existente en el mercado y sus características.

1.4. Objetivos específicos

Los objetivos específicos que se marcaron en la propuesta de este TFC fueron los siguientes:

- Describir las distintas infraestructuras de redes wireless más utilizadas en la actualidad.
- Identificar y analizar los Riesgos y Amenazas de las redes wireless.
- Analizar las propuestas de seguridad para sistemas de comunicaciones sin hilos.
- Describir políticas de seguridad, prácticas de seguridad, y las directrices de seguridad para ayudar a abordar mejor el problema de seguridad.
- Identificar y comparar soluciones de seguridad existentes en el mercado.

1.5. Planificación del Proyecto

Para alcanzar los objetivos propuestos, es necesario descomponer y planificar las tareas a llevar a cabo durante todo el proceso de desarrollo de los trabajos, identificando las actividades e hitos según corresponda.

Los documentos entregados en este Trabajo Final de Carrera (TFC) son los siguientes:

- Plan de Trabajo : Planificación y estimación de las tareas necesarias para llevar a cabo los objetivos previstos.

- Memoria : Documento de síntesis final del trabajo realizado y que mostrará que se han alcanzado los objetivos propuestos. Incorporará toda la información relevante sobre el análisis y desarrollo del contenido del Trabajo Final de Carrera.

- Presentación : Resumen claro y conciso del trabajo realizado y de los resultados obtenidos.

El plazo establecido para la entrega de los elementos resultantes del Trabajo Final de Carrera, memoria y presentación es el 22/06/2012.

La planificación elaborada para este proyecto, así como la estimación del esfuerzo, presentan un plan de trabajo adecuado para permitir alcanzar estos objetivos. Se ha adoptado como fecha inicial del proyecto el 7/03/2012, es decir, la fecha de comunicación al tutor de la decisión del proyecto, se realizará tres entregas parciales en las siguientes fechas con el fin de cumplir con las entregas de la evaluación continua.

En la realización del Trabajo Fin de Carrera se ha utilizado el hardware siguiente:

- Ordenador: Mac Mini 2,3 GHz
- Portátil: MacBook Air 1,7 GHz
- Copias de Seguridad: Time Capsule

De la misma manera, en la realización del Trabajo Fin de Carrera se utilizará el siguiente software para la plataforma Mac OSx Lion:

- Microsoft Word 2008.
- Microsoft PowerPoint 2008.
- Adobe Acrobat Pro 10.
- Merlin 2.8 Project Management
- OmniGraffle 5.3.6.

El proyecto está estructurado en función de lo hitos de entrega de documentación para la evaluación continua, en función de estos hitos se planifica una relación de tareas conectadas en cascada de la forma finish-start, es decir cada tarea espera a que finalice su predecesora para comenzar.

La descomposición de Actividades se describen en la siguiente tabla:

TFC – Seguridad en Comunicaciones Sin Hilo: Riesgos y Amenazas
Inicio TFC
Pec1 – Planificación TFC
Elaboración Plan de Trabajo
Revisión Documentación a entregar
Entrega Pec1 – Plan de Trabajo
Pec2
Recopilación Articulos
Recopilación de Bibliografía
Busqueda de Estándares
Elaboración Borrador Memoria
Revisión Documentación a entregar
Entrega Pec2
Pec3
Busqueda Soluciones en el Mercado
Comparación de Caracteristicas Técnicas
Modificación Borrador Memoria
Revisión Documentación a entregar
Entrega Pec3
Entrega Final Documentación
Elaboración Final Memoria
Revisión Documentación a entregar – Memoria Final
Entrega Memoria Final
Elaboracion Presentación
Revisión Documentación a entregar – Presentación
Entrega Presentación
Fin del TFC

Tabla 1.1. Descomposición de actividades del TFC

La planificación del proyecto se define en el siguiente diagrama de Grantt:

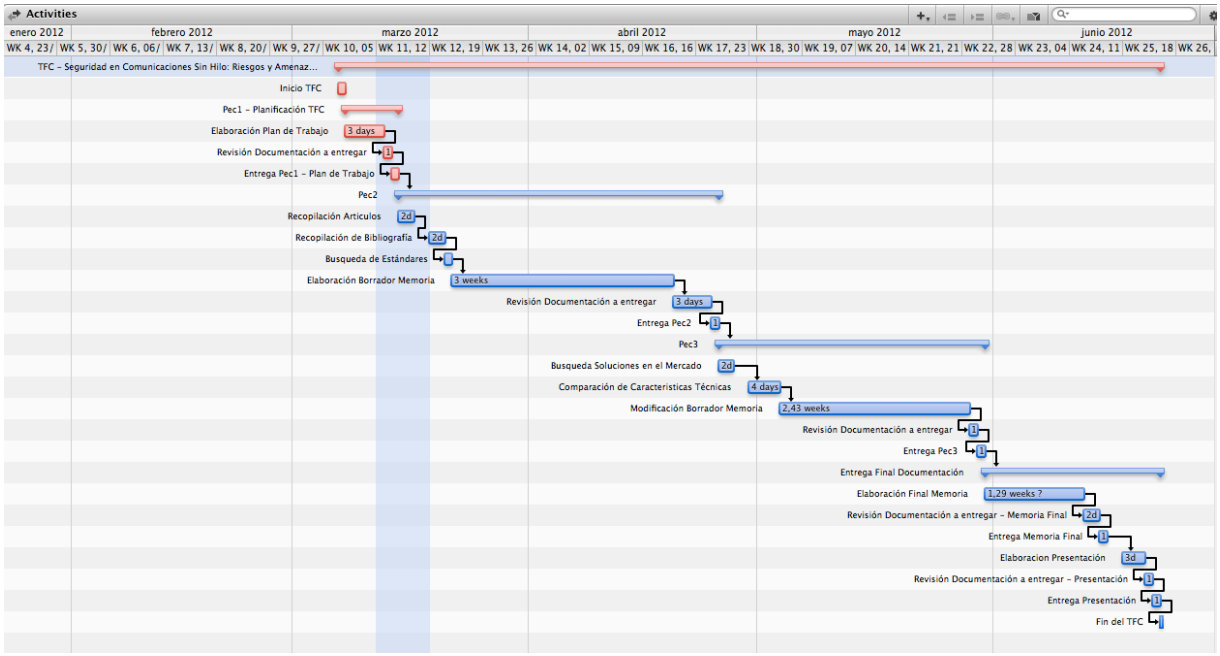

Figura 1.1. Planificación del TFC

2

2. Redes sin Hilo

2.1. Introducción a las Redes sin Hilos

Durante los últimos años han surgido y se han hecho con gran popularidad nuevas tecnologías inalámbricas como WI-FI, WIMAX, GSM, Bluetooth, Infrarrojos, etc, siendo los dispositivos inalámbricos una de las grandes revoluciones tecnológicas de los últimos tiempos.

Además el uso de dispositivos móviles de acceso a Internet ha aumentado de forma casi exponencial en los últimos años. Destaca, por ejemplo, el uso de smartphones, dispositivos que han incrementado enormemente su usabilidad y prestaciones sobre todo a partir de la aparición del iPhone de Apple en Junio del 2007.

La conexión de estos dispositivos móviles a Internet se puede realizar usando diferentes tecnologías. Las más importantes son sin duda las que corresponden a las redes móviles. Aunque las redes GSM proporcionan cierta capacidad de transferencia de datos, pero con prestaciones muy reducidas. La primera tecnología que realmente ha permitido una conexión a la Internet móvil ha sido la tecnología GPRS, en Europa, o EDGE, en los Estados Unidos, conocidas como 2,5G. El ancho de banda proporcionado está en la decena de Kbps, que es suficiente para algunas aplicaciones, pero no suficiente para poder desarrollar aplicaciones móviles en su máxima extensión. Años más tarde apareció la tecnología UMTS, basada en WCDMA, y que comercialmente se conoce como 3G. Durante varios años el éxito comercial de 3G no ha sido substancial, en parte ya que los propios operadores no lo promovieron comercialmente con ofertas interesantes. Esto motivó que las velocidades proporcionadas por 3G, en torno a 300 Kbps, fueran quedando desfasadas respecto a las expectativas de los usuarios, lo que llevó a los operadores al desarrollo de modificaciones en el estándar, conocida como HSDPA/HSUPA, que permiten alcanzar mayores velocidades, con asimetría entre los enlaces de subida y de bajada y que se han comercializado como 3.5 G.

A partir del 2005-2007 el uso de las redes 3G y 3.5G se ha disparado. A ello han contribuido ofertas comerciales más atractivas, la aceptación por parte de los usuarios de este tipo de aplicaciones, y la aparición de terminales de usuarios cada vez más atractivos, como por ejemplo el iPhone de Apple, que además han creado un ecosistema de desarrollo y distribución de aplicaciones que ha provocado una explosión en el desarrollo de aplicaciones móviles.

Ello ha provocado la aparición de un nuevo problema. Los operadores ya no solo se han de preocupar de la velocidad de conexión, sino de la capacidad de la red, lo que ha incrementado el interés en técnicas de descarga de la red 3G y la aceleración en el desarrollo de nuevas tecnologías como la conocida como Long Term Evolution, o 4G.

Por todo lo comentado, son necesarias otras tecnologías, alternativas a las redes móviles, que eviten el colapso de este tipo de redes. Muchos de estos nuevos dispositivos cuentan con conexiones Bluetooth (1 Mbps) y Wi-Fi (11 Mbps utilizando 802.11g), muy potente pero bastante desaprovechada.

2.2. Tipos Redes sin Hilos

Cada una de las tecnologías inalámbricas indicadas en el comienzo del apartado anterior tiene su ámbito de aplicación, sus ventajas y debilidades. A pesar de que nos centraremos en el estudio de las Redes Wi-Fi es conveniente conocer los distintos tipos de redes inalámbricas existentes en el cual se incluye la tecnología Wi-Fi.

Las tecnologías inalámbricas que existen actualmente, tienen sus respectivas limitaciones de velocidad y rango de alcance. En la Fig.2.1 se pueden apreciar los estándares inalámbricos relacionados con estos dos parámetros.

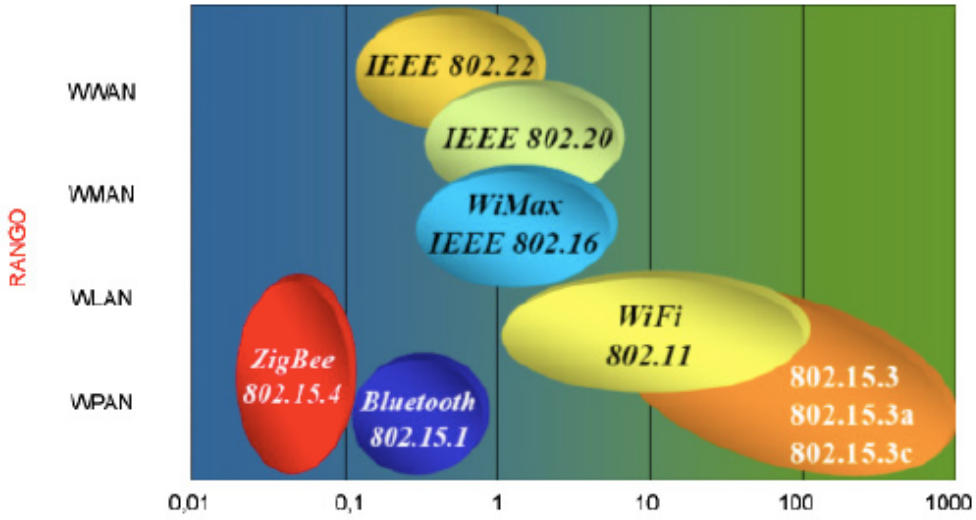

Figura 2.1. Clasificación redes.

A continuación se muestra la clasificación de cada tipo de redes wireless ***en función de la tecnología*** utilizada:

Redes Inalámbricas Personales. Dentro de estas redes podemos integrar a dos principales actores:

- Infrarrojos. Estas redes son muy limitadas dado su corto alcance, su necesidad de visión sin obstáculos entre los dispositivos que se comunican y su baja velocidad (hasta 115 Kbps). Se utilizan principalmente en ordenadores portátiles, PDAs, teléfonos móviles e impresoras.

- Bluetooth. Es el estándar de comunicación entre pequeños dispositivos de uso personal, como PDAs o teléfonos móviles. Funciona en la banda de 2.4 GHz que no requiere licencia y tiene un alcance de entre 10 y 100 metros, según el dispositivo.

Redes Inalámbricas de Consumo. También distinguimos dos tipos:

- Redes CDMA y GSM. Son los estándares de telefonía móvil americano y europeo y asiático respectivamente.

- Wimax. Es una tecnología wireless que ha sido concebida y desarrollada para suministrar servicios de Banda Ancha en tramos de pocos kilómetros, como campus universitarios, urbanizaciones, etc. El rango típico de WIMAX es de 3 a 10 kilómetros, aunque puede alcanzar más de 40.

- Redes Inalámbricas de Área Local. Las WLAN, Redes Inalámbricas de Área Local, o Redes Wi-Fi serán el tipo de redes en el que se basa el presente proyecto, por lo tanto, a continuación se describirán detalladamente sus características, los elementos que las componen y su seguridad.

Si se realiza una clasificación por ***rango de cobertura***, se puede hablar de:

- WPAN (Wireless Personal Area Networks): Redes personales caracterizadas por tener un área de cobertura limitada. Entre las tecnologías que pueden formar este tipo de redes destacan la novedosa ZigBee o la ya consolidada Bluetooth.

- WLAN (Wireless Local Area Network): Redes que aparecen como alternativa a las redes LAN cableadas, creando un sistema de comunicación de datos más flexible. Las tecnologías relacionadas con este tipo de redes, son WI-FI y, si se habla de distancias relativamente cortas, puede incluirse ZigBee.

- WMAN (Wireless Metropolitan Area Networks): Redes de área metropolitana que pueden abarcar hasta 4 Km. de distancia. Entre las tecnologías que pueden encontrarse en este tipo de redes destacan LMDS y WiMax, con ciertas similitudes a WI-FI pero basadas en el estándar IEEE 802.16.

- WWAN (Wireless Wide Area Network): Red a nivel mundial con una gran cobertura, en la que destacan tecnologías como GPRS y UMTS, ambas utilizadas para la telefonía móvil principalmente.

Las redes inalámbricas se pueden diferenciar por el ***rango de frecuencias*** utilizado para transmitir:

- Ondas de radio: en este rango se encuentran las bandas que van desde la ELF hasta la UHF (3Hz – 3GHz). Se propagan por el medio omnidireccionalmente mediante antenas y al operar en frecuencias bajas no sufren atenuación por la lluvia.

- Microondas terrestres: son las señales que van desde 1Ghz a 300GHz. Utilizan antenas parabólicas en enlaces punto a punto donde las distancias no suelen ser muy largas. Al trabajar con frecuencias más elevadas que las ondas de radio sufren interferencias por la lluvia. Tienen el inconveniente de que los puntos que se van a comunicar tienen que estar perfectamente alineados.

- Microondas por satélite: Son muy parecidas a las microondas terrestres pero en este caso desde un punto de la tierra se envía una señal a una satélite que la recibe por una

banda, la amplifica y la envía por otra banda a un receptor de la tierra.

- Infrarrojos: su rango de frecuencias va de 300GHz a 384THz. El transmisor y el receptor deben de estar alineados directamente ya que no es capaz de atravesar paredes.

2.3. Infrarrojos

En general los sistemas de comunicaciones infrarrojos ofrecen ventajas significativas respecto a los sistemas de radio frecuencia. Al utilizar luz, los sistemas Infrarrojos de comunicaciones cuentan con un canal cuyo potencial de ancho de banda es muy grande y no están regulados en ninguna parte del planeta.

Además, los sistemas infrarrojos de comunicaciones son inmunes a interferencias y ruido de tipo radioeléctrico. Como la luz infrarroja no puede atravesar paredes, es posible en comunicaciones interiores operar al menos un enlace (celda) en cada cuarto de un edificio sin interferencia con los demás, permitiendo así una alta densidad de reuso del sistema, obteniéndose una gran capacidad por unidad de área. El confinamiento de las señales infrarrojas hace difícil que escuchas clandestinos las puedan captar. La única manera de que las señales infrarrojas se pudieran captar sin permiso, es a través de las ventanas, peros estas se cubren con persianas o cortinas se evitará tal situación de inseguridad, sin la necesidad de los complicados algoritmos de cifrado utilizados en los sistemas de RF.

En los sistemas infrarrojos de comunicaciones de corto alcance, el esquema de modulación / desmodulación mas práctico, es el de Modulación de Intensidad y Detección Directa (IM/DD). Al utilizar IM/DD los circuitos del transmisor y del receptor son relativa- mente simples comparados con los requeridos en los esquemas coherentes. Además, con la longitud de onda tan corta de la portadora y la gran área activa del detector, se obtiene una eficiente diversidad espacial que previene el desvanecimiento de las señales causado por la propagación en múltiples trayectorias. Las multitrayectorias son una característica del canal infrarrojo difuso, y producen dispersión temporal en los pulsos transmitidos a través de éste, pudiendo causar interferencia entre símbolos (ISI). La ISI es una limitante para la velocidad de transmisión de los sistemas de comunicaciones infrarrojos difusos ya que se hace significativa a tasas de símbolos por arriba de 10 Megabauds.

Aunque los sistemas infrarrojos son inmunes al ruido e interferencias de tipo radioeléctrico, éstos sufren de degradaciones causadas por el ruido infrarrojo existente en ambientes exteriores e interiores, proveniente principalmente del sol y de fuentes de luz fluorescente e incandescente. El ruido infrarrojo, junto con las pérdidas de propagación limita el alcance de los sistemas infrarrojos, debido a que la relación señal a ruido (S/N) en el receptor disminuye a medida que nos alejamos del transmisor, o a medida que aumentamos el ángulo de visión en el detector. Una forma de mejorar la relación S/N es aumentando la potencia de la señal transmitida. En ambientes interiores la potencia pudiera ser aumentada hasta niveles muy grandes sin que esto cause problemas de interferencia en celdas vecinas, pero hay dos aspectos que limitan la potencia del transmisor: uno es el suministro limitado de energía por parte de la batería, en un sistema portátil, y el otro es referente a la seguridad ocular de los

usuarios y demás personas que deambulan en el área de cobertura. La seguridad ocular, es un aspecto muy importante en el diseño de un sistema infrarrojo, y es el único que está regulado.

En la figura 2.2 se ilustran aplicaciones representativas de los sistemas infrarrojos.

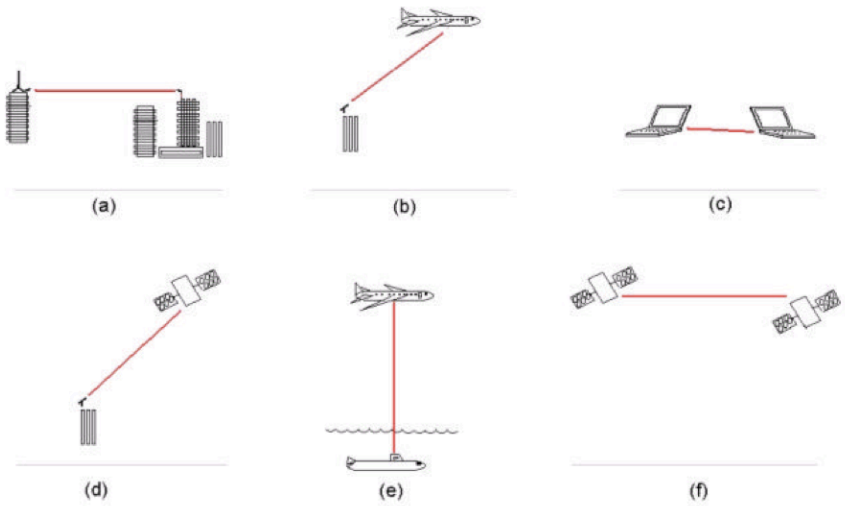

Figura 2.2. Ejemplos de sistemas infrarrojos de comunicaciones inalámbricas. (a) terrestre, (b) tierra-aire, (c) entre dispositivos de computo, (d) tierra-satélite, (e) aire-submarino, (f) Inter-satélites

2.3.1. Clasificación de los sistemas infrarrojos.

En general, los sistemas IR se pueden clasificar de acuerdo a dos criterios. El primero es el grado de direccionalidad del transmisor y del receptor, así podemos encontrar enlaces dirigidos y enlaces no dirigidos. Los enlaces dirigidos emplean transmisores y receptores altamente direccionales, los cuales deben apuntar uno al otro o hacia un área común, generalmente en el techo, para establecer el enlace. Mientras que, en los enlaces no dirigidos se emplean transmisores y receptores de gran ángulo, disminuyendo así la necesidad de tal apuntamiento. En los enlaces directos se maximiza la eficiencia de potencia, ya que ésta se dirige en un rango muy pequeño de direcciones, y por lo mismo se minimizan las pérdidas de propagación y la recepción de ruido causado por la luz ambiental. Al ser mínima la necesidad de apuntamiento, en un enlace no dirigido se facilita su reconfiguración. Es posible establecer enlaces híbridos, en los cuales, se combinan transmisores y receptores con diferente grado de direccionalidad.

El segundo criterio de clasificación está relacionado con la existencia o no de una línea de vista entre el transmisor y el receptor. En los enlaces de línea de vista, la luz emitida por el transmisor llega directamente al receptor, y en los enlaces sin línea de vista, la luz que sale del transmisor llega al receptor generalmente después de haberse reflejado difusamente en una o varias superficies. En un enlace de línea de vista, se utiliza con mayor eficiencia la potencia de las señales y se minimiza la distorsión por multitrayectorias. Y con un enlace sin línea de vista, se obtiene una mayor facilidad de uso, mayor movilidad, y robustez, o sea que el

sistema sigue operando aún cuando existan obstrucciones causadas por personas u objetos que se interpongan entre el transmisor y el receptor. En la figura 2.3 se presenta un esquema de las diferentes clases de sistemas infrarrojos.

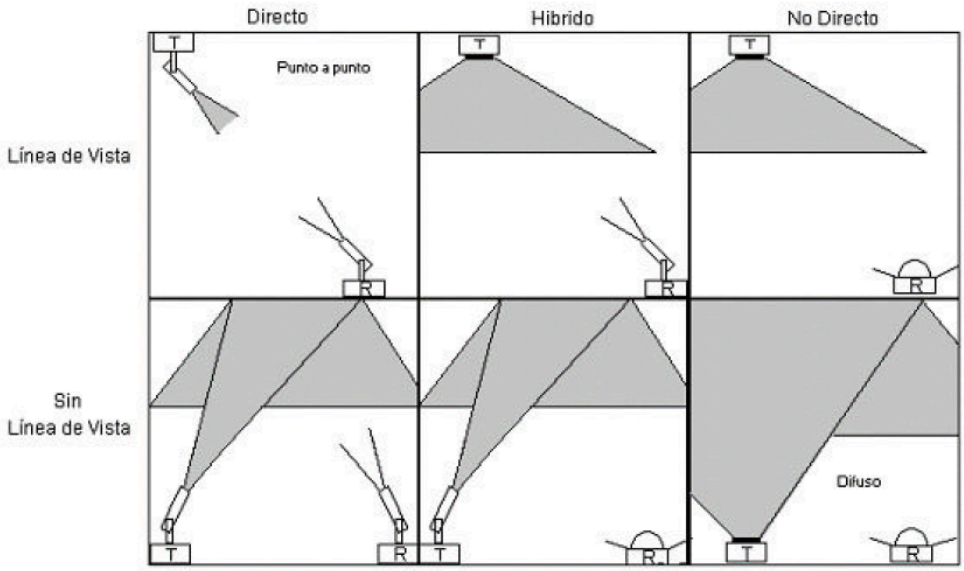

Figura 2.3. Clasificación de los sistemas infrarrojos de acuerdo a la direccionalidad del Tx y del RX, y a la existencia o no de una línea de vista entre ellos.

2.3.2. Sistemas IR punto a punto

En un enlace punto a punto, el transmisor concentra su potencia en una pequeña región del espacio, por lo cual, para una potencia dada, este sistema es el que mayor distancia puede alcanzar. De una manera parecida, el receptor capta luz infrarroja sólo de una pequeña región del espacio, produciéndose así un mínimo de distorsión por multitrayectorias y de ruido causado por las fuentes de luz ambiental. La combinación de estas características da como resultado altas razones de transmisión y grandes alcances. Además de esto, los sistemas punto a punto son relativamente baratos y simples. La principal aplicación de este producto es la interconexión de redes de alta velocidad, tales como, Fast Ethernet a 125 Mbps, FDDI a 125 Mbps y ATM a 155 y 622 Mbps.

Otra aplicación que los sistemas IR punto a punto van a tener en un futuro cercano, está en los enlaces intersatélites, en donde las condiciones ambientales, vacío, permiten que con relativamente pequeña potencia se tengan alcances y razones de transmisión muy grandes, cientos o miles de km y varios Gbps. Aunado a esto, el reducido espacio y poco peso de un sistema IR, cuestiones importantes en los satélites, le dan una gran ventaja respecto a los sistemas de RF en este tipo de aplicaciones.

También, se han diseñado sistemas IR punto a punto para enlazar estaciones terrestres con satélites. Este sistema tiene una razón máxima de 1.0 Gbps y un alcance de 600 a 1800 km.

En ambientes interiores, donde existen restricciones de potencia, encontramos sistemas punto a punto que operan a 10 Mbps en un rango de 457 m, éstos son compatibles con Ethernet y con Token Ring de 16 y 4 Mbps. Estos sistemas son más baratos y presentan mayores facilidades que los sistemas de radio diseñados con propósitos similares. Las desventajas de los sistemas IR punto a punto respecto a los demás, es su poca ó nula capacidad de movimiento y su intolerancia a la interrupción de la línea de vista.

2.3.3. Sistemas IR difusos

Los sistemas IR difusos son los más fáciles de utilizar y también los más robustos, no se requiere apuntar tanto al transmisor como al receptor, ni se requiere que haya línea de vista entre éstos. Sin embargo, los sistemas IR difusos tienen más altas pérdidas de propagación que sus contrapartes de línea de vista, requiriendo altas potencias de transmisión y un receptor que tenga una gran área de colección de luz. Transmisores difusos típicos emplean varios LEDs, los cuales son orientados en diferentes direcciones, para proveer una diversidad de trayectorias de propagación. Cuando transmiten, típicamente emiten una potencia óptica promedio en el intervalo de 100 a 500 mW, esto causa un consumo de potencia eléctrica más alto que el de un transmisor típico IrDA. Los receptores difusos típicos emplean como detectores diodos pin de silicio encapsulados en lentes hemisféricos, los cuales concentran la luz y tienen un amplio campo visual. En algunos casos se usan varios detectores, cada uno orientado en diferentes direcciones.

Un sistema IR difuso puede ser realizado de dos maneras, como se ilustra en la figura 2.4. En la primera técnica, un enlace IR difuso es utilizado para accesar los recursos de una red local cableada. Claramente se ve que esta arquitectura también permite la comunicación entre terminales portátiles vía el sistema cableado. Esta arquitectura resulta apropiada para comunicación inalámbrica de datos, en los cuales el costo de instalar una red sobre medios guiados (Backbone) y puntos de acceso inalámbricos puede ser justificado.

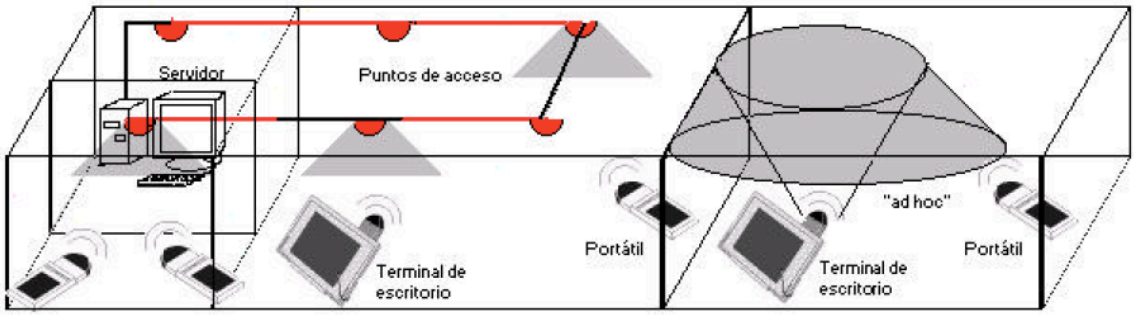

Figura 2.4. Técnicas empleadas en los enlaces infrarrojos difusos

En la segunda técnica, enlaces infrarrojos difusos son empleados para comunicaciones de igual a igual entre un número de terminales de escritorio y/o portátiles. Este tipo de interconexión Ad-Hoc es apropiado para utilizarse en recintos cerrados para establecer redes locales en donde todos los nodos están localizados en un solo cuarto.

2.4. Bluetooth

Bluetooth es un estándar abierto de tecnología inalámbrica diseñado para intercambiar datos en distancias cortas, utilizando ondas cortas, entre dispositivos fijos y móviles, creando redes locales personales, PAN personal area network, con altos niveles de seguridad. Se concibió como una alternativa al RS-232, conocido como puerto com. Puede conectar diversos dispositivos superando problemas de sincronización.

Figura 2.5. Símbolo Bluetooth

2.4.1. Comunicación y conexión

Bluetooth se basa en una estructura maestro-esclavo. Un maestro puede comunicarse con hasta 7 esclavos en un grupo inalámbrico de usuarios, Wireless user group. Este grupo de hasta 8 dispositivos recibe el nombre de piconet. Los dispositivos pueden cambiar de rol, mediante acuerdos, con lo que los esclavos podrán convertirse en maestros en cualquier momento.

En cualquier momento, los datos pueden transferirse entre el maestro y cualquier otro dispositivo.

Los maestros cambian de un dispositivo a otro utilizando el patrón round-robin. La transmisión simultánea del maestro a múltiples dispositivos es posible mediante el modo broadcast, pero no es comúnmente utilizada.

2.4.2. Implementación

Bluetooth utiliza una tecnología de radio llamada, Frecuency-hopping spread spectrum, que divide los datos que están siendo enviado y transmite sus trozos en hasta 79 bandas de 1MHz en el rango 2402-2480MHz. En su modo Basic Rate puede llegar a un ancho de banda de 1Mbit/s y utilizando el Extended Data Rate alcanzaría los 2 y 3 Mbits/s.

Dentro de una piconet, los dispositivos comparten el reloj del maestro. El intercambio de paquetes está basado en un reloj básico, definido por el maestro, que se incrementa en ticks de 312.5 µs. Dos ticks forman un slot de 625 µs; dos slots forman un par slot de 1250 µs. En el caso simple de paquetes single-slot, el maestro transmite en slots pares y recibe en los impares; el esclavo, al contrario. Los paquetes pueden ocupar 1, 3 o 5 slots, pero en todos los

casos el maestro empezará a transmitir en slots pares y el esclavo en impares.

2.4.3 Usos

Bluetooth es un protocolo estándar de comunicaciones diseñado principalmente para un bajo consumo, con un rango bastante corto, dependiendo de la clase como se puede comprobar en la figura siguiente. Basado en microchips transmisores de bajo coste en cada dispositivo. A consecuencia de que los dispositivos utilizan un sistema de comunicaciones broadcast, no necesitan estar en línea de visión entre ellos.

Class	Maximum Permitted Power		Range (approximate)
	mW	dBm	
Class 1	100	20	~100 meters
Class 2	2.5	4	~10 meters
Class 3	1	0	~1 meters

Tabla 2.1. Clases de Bluetooth

2.4.4 Especificaciones y características

La especificación de Bluetooth se desarrolló en 1994 por Jaap Haartsen and Sven Mattisson, los cuales trabajaban para Ericsson en Suecia. Se basaron en la tecnología Frecuency-hoping spread spectrum. El grupo "Bluetooth Special Interest Group (SIG)" formalizó las especificaciones. Se anunció formalmente en 1998. Hoy tiene una cartera de miembros de 13000 compañías de todo el mundo. Fue establecido por Ericsson, IBM, Intel, Toshiba y Nokia.

Bluetooth v1.1

Fue la primera versión estandarizada en el IEEE 802.15.1-2002. Arreglaba muchos de los errores de previas versiones, añadió soporte para canales no encriptados.

Bluetooth v1.2

Esta versión era compatible con la anterior y multitud de mejoras, de entre las cuales mencionaremos a continuación las más importantes:

- Conexión y descubrimiento mucho más rápidos.
- Mayores velocidades de transmisión, hasta 721 kbits/s
- Extended Synchronous Connections (eSCO), tecnología que mejoró la calidad de los enlaces de audio permitiendo la transmisión de paquetes corruptos y opcionalmente podía incrementar la latencia de audio para proporcional soporte a transferencia de datos concurrentes.
- Se introdujeron modos de control de flujo y retransmisión para L2CAP

- Se ratificó en el estándar IEE 802.15.1-2005

Bluetooth v2.0 + EDR

Esta versión de Bluetooth se lanzó en 2005 y es compatible con las anteriores. La principal diferencia es la introducción de un Enhanced Data Rate (EDR) para transmisiones de datos más rápidas. La velocidad nominal es de alrededor de 3Mbits/s aunque en la práctica llega a unos 2.1 Mbits/s. Además el EDR proporciona un consumo de energía menor.

Bluetooth v2.1 + EDR

Compatible con las versiones anteriores, el punto fuerte de esta versión es una mejora en seguridad. Se introdujo el "Secure simple pairing" (SSP) que mejoraba la experiencia de enlace entre dos dispositivos mientras incrementaba el uso y la fuerza de la seguridad.

Bluetooth v3.0 + HS

Esta versión fue adoptada por el grupo SIG en 2009. Soporta una velocidad de transmisión teórica de hasta 24 Mbits/s aunque no utilizando la conexión Bluetooth. En lugar de ello, Bluetooth se utiliza para la negociación y el establecimiento y el tráfico de datos se realiza utilizando tecnología 802.11 (Wi-Fi).

Bluetooth low energy

Esta tecnología es una reciente mejora que permite dos tipos de implementación, modo dual y modo sigle.

En una implementación de modo dual, la funcionalidad Bluetooth low energy se integra en un controlador de Bluetooth clásico. La arquitectura resultante comparte muchos detalles con el bluetooth clásico y resulta en un mínimo incremento de coste en relación al Bluetooth clásico. Adicionalmente los fabricantes pueden usar los chips de Bluetooth actuales con la nueva tecnología energética, mejorando el desarrollo de dispositivos bluetooth pero añadiéndoles nuevas capacidades.

Los chips en modo single, los cuales permitirán dispositivos compactos altamente integrados contarán con una conexión muy ligera proporcionando modos de ultra bajo consumo y conexiones seguras encriptadas al menor coste posible.

Version	Data Rate
Version 1.2	1 Mbit/s
Version 2.0 + EDR	3 Mbit/s
Version 3.0 + HS	24 Mbit/s

Tabla 2.2. Versiones de Bluetooth

2.5. GPRS

El sistema GPRS actualiza los servicios de datos GSM para hacerlos compatibles con LANs ,WANs e Internet. Mientras el actual sistema GSM fue originariamente diseñado con un especial énfasis en las sesiones de voz, el principal objetivo de GPRS es ofrecer un acceso a redes de datos estándar, como TCT/IP. Estas redes consideran GPRS como una subred normal. El actual sistema GSM opera en un modo de transmisión de circuitos conmutados, extremo a extremo, en el cual los circuitos son reservados a lo largo del sistema para el uso de una sola comunicación incluso cuando no se transmiten datos.

Cuando un usuario transmite datos, éstos son encapsulados en paquetes cortos, en cuya cabecera se indica las direcciones origen y destino, cada uno de estos paquetes puede seguir rutas diferentes a través de la red hasta llegar a su destino, así mismo, los paquetes originados por distintos usuarios pueden ser intercalados, de esta forma se comparte la capacidad de transmisión.

Los paquetes, no son enviados a intervalos de tiempo, sino que cuando se necesita, se asigna la capacidad de la red, siendo liberada cuando no es necesaria. GPRS utiliza los recursos radio solamente cuando hay datos que enviar o recibir, adaptándose así perfectamente a la muy intermitente naturaleza de las aplicaciones de datos.
El uso de los enlaces de este modo conserva la capacidad de red y la interfaz. Además permite a los operadores ofrecer un servicio a mejor precio, ya que la facturación se puede basar en la cantidad de datos enviados o recibidos.

2.5.1. Características técnicas

El concepto principal que gobierna el comportamiento de GPRS es su orientación a la comunicación de paquetes. La diferencia principal entre una comunicación orientada a circuitos y una orientada a paquetes es la utilización de los recursos de red; mientras en circuitos se ocupa el recurso durante toda la comunicación, en paquetes sólo se requiere cuando existe algo que transmitir o recibir. Si pensamos, por ejemplo, en un acceso a Internet, una conexión de paquetes únicamente usaría los recursos cuando el usuario estuviera bajando una página, no cuando la estuviera consultando. Esto posibilita una mejora en la eficacia de uso de los recursos y permite tarificar no por tiempo de conexión, sino por volumen de datos intercambiado.

Como se aprecia en la figura 2.6., GPRS está basado en la arquitectura GSM incorporando dos nuevos nodos, el SGSN (Serving GPRS Support Node) y el GGSN (Gateway GPRS Support Node), cuyas misiones son complementarias. A nivel general, el SGSN es el que se encargará de toda la gestión de la movilidad, y mantenimiento del enlace lógico entre móvil y red, mientras que el GGSN es el que proporciona acceso a las redes de datos actuales, sobre todo a las basadas en IP.

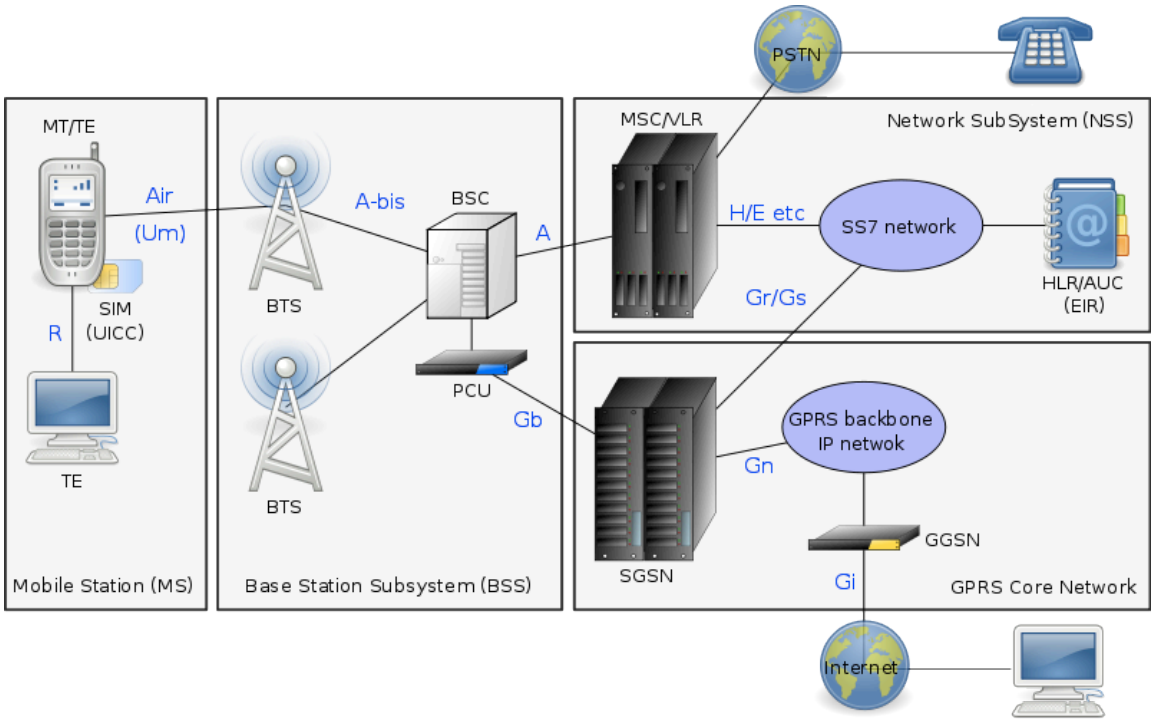

Figura 2.6. Esquema general de una red GPRS

2.5.2. Características del Sistema

En este tipo de técnica no es necesario establecer un canal dedicado para cada usuario sino que la conexión se realiza en el momento de utilización del canal, por lo tanto se pierde el concepto de facturación por tiempo, pasando a ser por utilización del canal de emisión. La vía de conexión es mucho más utilizada, ya que permite a los usuarios compartir el mismo medio.

La entidad transmisora segmenta el mensaje a transmitir en PDUs (paquetes de datos) independientes, de tamaño apropiado. La entidad receptora se encarga de reconstruirlos (reensamblarlos) hasta obtener el mensaje original completo. Cada paquete de datos se transfiere de un nodo a otro como una sola unidad. Contienen información de control (direcciones de origen y destino, identificador, etc.) que permite su manejo en la red.

El PDU se almacena temporalmente en cada uno de los nodos por los que pasa mientras espera ser enviado al siguiente. Esto conlleva un aumento del retardo en función del volumen de tráfico existente y de la capacidad del enlace. Todos los PDUs que componen los datos están relacionados unos con otros, pero la forma en que viajan y son reagrupados varía. La propia red puede fragmentar los PDUs si la longitud de éstos es mayor que la unidad máxima de transferencia (MTU) de la red.

Los canales de comunicación (time-slots) se comparten entre los distintos usuarios dinámicamente en función de sus necesidades y son asignados, únicamente, cuando se está

transmitiendo datos. Así una vez que el paquete de datos ha sido transmitido a través de la interfaz aérea, los recursos radio pueden ser liberados para el uso por parte de otros usuarios.

- Conexiones a redes estándar de datos
- Aplicaciones bajo protocolo TCP/IP (WWW, FTP, Telnet) y en general aplicaciones convencionales basadas en TCP/IP
- Aplicaciones basadas en X.25

Direccionamiento.

El direccionamiento se realiza por medio de direcciones IP. La dirección IP, es un numero de 32 bits. Estos campos son variables en extensión para poder ser flexibles al asignar direcciones de red . Hay diferentes tipos de redes que se pueden implantar en la dirección de red . Unas son grandes (con muchas subredes) , otras medianas y otras pequeñas . Es posible y adecuado mezclar en una dirección los tres tipos de clases de redes.

Según la naturaleza de estas direcciones tendremos:

- Direcciones IP Privadas: accesibles sólo dentro de un entorno determinado dentro de la red.
- Direcciones IP Públicas: accesibles desde cualquier punto de Internet.

Según la asignación de estas direcciones tendremos:

- Direcciones IP Estáticas: estas direcciones irán asociadas de forma estática vía el HLR
- Direcciones IP Dinámicas: estas direcciones se obtienen de unos pools de direcciones gestionados bien por el Operador de la red bien por una Entidad Externa (como un servidor DHCP).

Seguridad.

Con el fin de proteger contra errores los paquetes transmitidos tiene lugar la codificación del canal radio, mediante el método GEA (GPRS Encryption Algorithm, algoritmo de cifrado GPRS) con algoritmos secretos. El cifrado en GPRS abarca desde las funciones de cifrado del terminal móvil hasta las funciones de cifrado en el SGSN, en contraste con GSM donde se usa un canal lógico entre el móvil y la BTS (repetidor de ondas).

2.6. Redes de Datos UMTS (3G)

UMTS, con nombre comercial 3G, es la tecnología utilizada en la actualidad para proveer servicios móviles de datos de alta velocidad en las redes móviles. Antes de entrar en la definición de 3G y sus características, es necesaria una tabla que muestre los estándares a lo largo del tiempo, comienza con los más antiguos hasta llegar a los planeados para el futuro.

0G (radio telephones)		MTS · MTA · MTB · MTC · IMTS · MTD · AMTS · OLT · Autoradiopuhelin
1G	**AMPS family**	AMPS · TACS · ETACS
	Other	NMT · Hicap · Mobitex · DataTAC
2G	**GSM/3GPP family**	GSM · CSD
	3GPP2 family	CdmaOne (IS-95)
	AMPS family	D-AMPS (IS-54 and IS-136)
	Other	CDPD · iDEN · PDC · PHS
2G transitional (2.5G, 2.75G)	**GSM/3GPP family**	HSCSD · GPRS · EDGE/EGPRS
	3GPP2 family	CDMA2000 1xRTT (IS-2000)
	Other	WiDEN
3G (IMT-2000)	**3GPP family**	UMTS (UTRAN) · WCDMA-FDD · WCDMA-TDD · UTRA-TDD LCR (TD-SCDMA)
	3GPP2 family	CDMA2000 1xEV-DO (IS-856)
3G transitional (3.5G, 3.9G)	**3GPP family**	HSDPA · HSUPA · HSPA+ · LTE (E-UTRA)
	3GPP2 family	EV-DO Rev. A · EV-DO Rev. B
	Other	Mobile WiMAX (IEEE 802.16e-2005) · Flash-OFDM · IEEE 802.20
4G (IMT-Advanced)	**3GPP family**	LTE Advanced
	WiMAX family	IEEE 802.16m
Related articles		History · Cellular network theory · List of standards · Comparison of standards · Channel access methods · Spectral efficiency comparison table · Cellular frequencies · GSM frequency bands · UMTS frequency bands · Mobile broadband

Tabla 2.3. Generaciones de tecnologías móviles

La tercera generación (3G) o International Mobile Telecommunications-2000, es una familia de estándares para telecomunicaciones móviles que cumple las especificaciones de la Unión de telecomunicaciones internacional (ITU) que incluye UMTS, CDMA2000, DECT y WiMAX. Los servicios incluyen: telefonía inalámbrica, video llamada y transferencias inalámbricas de gran alcance. Comparado con los servicios 2G y 2.5G, 3G permite el uso simultáneo de voz y datos a altas velocidades (al menos 200 kbits/s). Los servicios actuales (como se puede ver en el capítulo siguiente) llegan a alcanzar 14 Mbits/s y más en el futuro.

2.6.1. Visión general

Hay estándares revolucionarios que son compatibles con las redes 2G preexistentes y también estándares que requieren redes y asignaciones de frecuencias completamente nuevas. El

último grupo es la familia UMTS que consiste en estándares desarrollados para el IMT-2000, al igual que los estándares DECT y WiMAX desarrollados independientemente, los cuales están incluidos porque encajan en la definición del MIT-2000

ITU IMT-2000	common name(s)		bandwidth of data	pre-4G	duplex	channel	description	geographical areas
TDMA Single-Carrier (IMT-SC)	EDGE (UWT-136)		EDGE Evolution	*none*	FDD	TDMA	evolutionary upgrade to GSM/GPRS[nb 1]	worldwide, except Japan and South Korea
CDMA Multi-Carrier (IMT-MC)	CDMA2000		EV-DO	UMB[nb 2]		CDMA	evolutionary upgrade to cdmaOne (IS-95)	Americas, Asia, some others
CDMA Direct Spread (IMT-DS)	UMTS[nb 3]	W-CDMA[nb 4]	HSPA	LTE			family of revolutionary standards.	worldwide
CDMA TDD (IMT-TC)		TD-CDMA[nb 5]			TDD			Europe
		TD-SCDMA[nb 6]						China
FDMA/TDMA (IMT-FT)	DECT		*none*			FDMA/TDMA	short-range; standard for cordless phones	Europe, USA
IP-OFDMA			WiMAX (IEEE 802.16)			OFDMA		worldwide

Tabla 2.4. Tecnologías móviles

2.6.2. Velocidades de Datos

El ITU no proporcionaba una definición clara de las velocidades que los usuarios esperaban de los proveedores 3G. Así que los usuarios que empezaron a utilizar servicios 3G no podían apoyarse en ningún estándar para poder reclamar que las velocidades especificadas no se estaban cumpliendo. Mientras que se afirma en el comentario "Se espera que IMT-2000 proporcione velocidades de transmisión más altas, un mínimo de 2Mbits/s para usuarios quietos o a pie y 384kbits/s en un vehículo móvil", el ITU no especifica realmente unas velocidades medias ni mínimas o que modelos de interfaces se pueden llamar 3G. Así que se vendieron varias velocidades llamándolas 3G destinados a cumplir las expectaciones de ancho de banda de los clientes.

2.6.3. Seguridad

Las redes 3G ofrecen mejor seguridad que las anteriores 2G y 2.5G. Permitiendo al equipo de usuario autentificar la red a la que se está uniendo, el usuario puede estar seguro que la red a la que se une es la que cree y no una red que la sustituye de manera ilegal. Aunque en los últimos tiempos se han identificado varios problemas en la nueva tecnología de encriptación.
Además de la seguridad en la infraestructura de la red, se ha añadido seguridad end-to-end aunque no es estrictamente una propiedad de 3G.

2.6.4. Evolución

El grupo 3GPP (3rd Generation Partnership Project) trabajan en extensiones al estándar 3G que están basados en infraestructura de redes IP. La idea es hacer una gran evolución de estas redes, llamada 4G Long Term Evolution (LTE).

2.7. 4G LTE - Long Term Evolution

En este caso no se trata de una tecnología sino de un conjunto de tecnologías de telefonía móvil ya desarrolladas, en desarrollo y por desarrollar. El grupo 3GPP se trata de un proyecto de colaboración internacional de planificación de la próxima generación de servicios de telecomunicaciones celulares. La mejora de la tecnología celular UMTS se ha denominado LTE (Long term evolution). La idea es que 4G LTE permitirá velocidades mucho mayores utilizando una latencia de paquete mucho menor.

La situación actual es que se cuenta con la tecnología HSPA (High speed Packet Access) una combinación de HSDPA y HSUPA, además la tecnología HSPA+ se está desplegando actualmente.

En este apartado no se entrará en detalle de las tecnologías puesto que no son el objetivo de estudio, pero si se hablará de cómo comenzó la tecnología 4G y cuál será su evolución. La razón de incluir esta información es la alta utilización de las redes 3G actúales debido a la masificación de los dispositivos móviles de nueva generación. Esta alta utilización está llevando a una sobrecarga de las redes 3G, de ahí la importancia de este estudio y la posible utilización de redes Wi-Fi en modo Ad-Hoc como alternativa a muchos de los actuales usos de 3G. Sin embargo es necesario un conocimiento de la futura Cuarta generación para poder analizar la importancia o no de la tecnología Wi-Fi en este camino.

2.7.1. Comienzos de 4G LTE

El grupo 3GPP que supervisó el desarrollo de la tecnología UMTS 3G empezó en la evolución de la tecnología 4G con un estudio de factibilidad que finalizó con unos requisitos de alto nivel para la evolución de 4G:

- Coste por bit reducido
- Más servicios a menor coste, con una mejora de la experiencia de usuario.
- Flexibilidad de uso de las bandas de frecuencia existentes y algunas nuevas.
- Arquitectura simplificada, interfaces abiertas.
- Exigir un consumo razonable de energía.

En términos numéricos, los objetivos de LTE incluyen ratio de descarga de hasta 100 Mbps y de subida de 50 Mbps por cada espectro de 20MHz. Además se requiere que soporte al menos 200 usuarios activos por cada célula de 5 MHz También se incluyeron objetivos que implicaban la latencia de entrega de paquetes IP debido al uso creciente de servicios incluyendo Voz sobre IP, juegos online y muchas otras aplicaciones con requisitos en cuanto a

latencia. Como resultado el objetivo es tener latencias por debajo de 10milisegundos para paquetes pequeños.

2.7.2. Evolución

Aunque hay grandes cambios entre LTE y sus predecesores, se trata de una evolución de los estándares actuales de 3G. Utiliza diferentes interfaces radio, no obstante hay muchas concordancias con la actual tecnología 3G con lo que hay mucho ámbito para la reutilización.

	WCDMA (UMTS)	HSPA HSDPA / HSUPA	HSPA+	LTE
Max downlink speed bps	384 k	14 M	28 M	100M
Max uplink speed bps	128 k	5.7 M	11 M	50 M
Latency round trip time approx	150 ms	100 ms	50ms (max)	~10 ms
3GPP releases	Rel 99/4	Rel 5 / 6	Rel 7	Rel 8
Approx years of initial roll out	2003 / 4	2005 / 6 HSDPA 2007 / 8 HSUPA	2008 / 9	2009 / 10
Access methodology	CDMA	CDMA	CDMA	OFDMA / SC-FDMA

Tabla 2.5. Comparación de tecnologías móviles

Además, LTE está basado en redes IP, con soporte a IPv4 e IPv6. Tampoco hay previsiones para la voz aunque podrían utilizarse servicios VoIP (Voz sobre IP).

2.7.3. Tecnologías

LTE ha introducido un gran número de nuevas tecnologías comparando con los sistemas celulares previos. Éstas permiten operar de forma mucho más eficiente con respeto al uso del espectro y también proporcionan ratios de transferencia muchísimo más altos. De entre ellas comentaremos dos bastante importantes.

- OFDM (Orthogonal Frequency Division Multiplex): La tecnología OFDM, usada por ejemplo en 802.11g y 802.11ª, se ha incorporado a LTE porque permite transmitir de forma eficiente datos a muy altas velocidades mientras que sigue proporcionando un alto nivel de resistencia a reflexiones e interferencias.

- MIMO (Multiple Input Multiple Output): Uno de los principales problemas de los sistemas de telecomunicaciones previos fueron las señales derivadas de las reflexiones que se encontraban. Utilizando MIMO estos caminos adicionales de la señal pueden utilizarse para incrementar el rendimiento.

Al utilizar MIMO, se necesita utilizar varias antenas para permitir distinguir los diferentes caminos. Con esto aparece el problema de instalar las antenas. Mientras que es muy fácil hacerlo en una estación base, instalar las antenas en los teléfonos será bastante difícil debido a las dimensiones y los requisitos de consumo de estos. Dicha tecnología también se usa en 802.11n para poder alcanzar mayores velocidades y rango de alcance.

2.7.4. Visión general de la especificación

A continuación se muestra una tabla con los parámetros clave de la especificación 4G LTE. En vista del hecho de que hay varias diferencias entre las operaciones de subida y las de bajada, estas naturalmente difieren en el rendimiento que pueden ofrecer.

PARAMETER	DETAILS
Peak downlink speed 64QAM (Mbps)	100 (SISO), 172 (2x2 MIMO), 326 (4x4 MIMO)
Peak uplink speeds (Mbps)	50 (QPSK), 57 (16QAM), 86 (64QAM)
Data type	All packet switched data (voice and data). No circuit switched.
Channel bandwidths (MHz)	1.4, 3, 5, 10, 15, 20
Duplex schemes	FDD and TDD
Mobility	0 - 15 km/h (optimised), 15 - 120 km/h (high performance)
Latency	Idle to active less than 100ms Small packets ~10 ms
Spectral efficiency	Downlink: 3 - 4 times Rel 6 HSDPA Uplink: 2 -3 x Rel 6 HSUPA
Access schemes	OFDMA (Downlink) SC-FDMA (Uplink)
Modulation types supported	QPSK, 16QAM, 64QAM (Uplink and downlink)

Tabla 2.6. Requisitos marcados por LTE

Con estas especificaciones a grandes rasgos se puede ver un conjunto del rendimiento que LTE ofrecerá. Cumple los requisitos de la industria para grandes velocidades de descarga además de una latencia reducida. Además proporciona grandes mejoras en el uso del espectro.

2.8. WIMAX

La tecnología WiMAX, estándar IEEE 802.16e proporciona servicio inalámbrico para usuarios fijos y móviles en cualquier escenario, desde áreas metropolitanas a interiores de edificios. WiMAX es una tecnología de acceso inalámbrico que se basa en los estándares proporcionados por el grupo de trabajo IEEE 802.16 que desarrolla el estándar de acceso inalámbrico de elevado régimen binario en redes de área metropolitana o Wireless MAN.

El primer despliegue comercial WiMAX se produce en 2006 en Corea del Sur con el despliegue de servicio WiMAX en 2.3 GHz, conocido bajo el nombre WiBRO, en el área metropolitana de Seúl para ofertar servicios de audio y vídeo de alta calidad. En un reciente estudio se estiman en unos 140 millones los potenciales usuarios de WiMAX a nivel mundial para 2012. El Wim, WiMAX Forum, es un grupo industrial sin ánimo de lucro cuyo objetivo es asegurar la interoperabilidad entre los distintos productos WiMAX basados en la familia de estándares IEEE 802.16, a través de un proceso de certificación. En este grupo se encuentran agrupados operadores, industrias electrónicas, proveedores de servicios, fabricantes de chips e industria de contenidos. La actividad de este grupo es el eje fundamental del desarrollo actual de WiMAX, puesto que su actividad permite asegurar la compatibilidad de todos los productos comerciales.

La irrupción del estándar WiMAX con características de movilidad o Mobile WiMAX es una respuesta al cambio en el modelo tradicional de redes móviles celulares, buscando aumentar la capacidad y escalabilidad de los sistemas, y crear arquitecturas compatibles con el trafico IP, además de asegurar la transparencia al usuario y el acceso a nuevos servicios basados en Internet. Todo ello permite el desarrollo de una solución completa End-to-End que responda a estas demandas y a las nuevas oportunidades que de ellas se desprenden, como por ejemplo en las futuras recomendaciones en torno comunicaciones móviles 4G, recogidas en IMT-Advance prevista para principios de 2010.

Mobile WiMAX surgió ligado en 2005 al nuevo estándar IEEE 802.16-2005 revisión 1.0, también conocido como IEEE 802.16e, que soporta WiMAX con especificaciones concretas de parámetros de calidad de servicio y movilidad. Paralelamente, WiMAX Forum planteó un perfil de requisitos para Mobile WiMAX basado en este estándar que permitió incluirlo en su proceso de certificación. Todo estos trabajos dieron como resultado la adopción de Mobile WiMAX como el 6º interfaz radio de la familia IMT-2000 de ITU en 2007, definido como una tecnología de acceso dúplex OFDM por división en el tiempo para redes de tipo WMAN. Con ello, WiMAX IEEE 802.16e se convierte en el estándar que permite la convergencia para el acceso de servicios de elevado régimen binario en redes fijas y móviles.

A la tecnología WiMAX IEEE 802.16e también se le conoce como acceso de banda ancha por microondas, BWA Broadband Wireless Access.

2.8.1. Mobile WiMAX

La principal característica de Mobile WiMAX es el uso de OFDMA como tecnología de acceso. OFDMA proporciona diversidad en frecuencia frente a desvanecimientos multicamino y por lo tanto es adecuado para situaciones sin visión directa, NLOS Non-Light of Sight. Esto

permite la utilización de WiMAX IEEE 802.16e en frecuencias por debajo de 10.66 GHz. OFDMA incluye una subcanalización que permite reubicar dinámicamente los recursos temporales y de frecuencia disponibles para cada usuario a través de las subtramas de subida Uplink (UL) y bajada Downlink (DL). De esta forma, varios usuarios asignados a diferentes grupos de frecuencias de subportadoras pueden transmitir simultáneamente en el tiempo. Los usuarios son recolocados dinámicamente en la duración de la subtramas tanto en tiempo como en frecuencia. Esta asignación dinámica aumenta la eficiencia de los recursos radio disponible, pero a su vez aumenta la complejidad del control de la capa física.

Otra característica de la revisión 1.0 de WiMAX 802.16e es el uso de TDD como forma de operación en el sistema. Como se especificaba, TDD permite el tráfico asimétrico entre DL y UL. El tráfico asimétrico aumenta la reutilización espectral y la eficiencia del sistema en comparación con la operación de división por duplexión en frecuencia, FDD Frequency-Division Duplexing, que requiere de anchos de banda iguales para DL y UL. El uso de un canal común para las transmisiones UL y DL en TDD simplifica el diseño de los transceptores WiMAX. TDD permite la reubicación de recursos radio para soportar tráfico variable, además asegura la reciprocidad en el canal de transmisión, lo cual permite disponer de conocimiento del canal en transmisión y aplicar determinadas técnicas MIMO, especialmente beamforming.

2.8.2. Componentes de WIMAX

Se definen los siguientes componentes de en una arquitectura de red WIMAX.

• Estación del abonado WIMAX.

En el extremo izquierda de la figura 2.7, los abonados móviles (MS) usan las estaciones móviles de abonados (MSS), terminales móviles, que proporciona conectividad entre los equipos de abonado y la estación base equipo.

• Acceso al servicio de red WiMAX .

El ASN, Acceso Servicio de red, se define como un conjunto completo de funciones de red que proporcionan el acceso vía radio a un abonado WiMAX, que incluyen un Servidor Proxy, servicio AAA, Authentication, Authorization y Accounting, la función de direccionamiento DHCP, y otros servicios basados en IP, incluyendo los recursos gestión de la red.

• Servicio de Conectividad de la red WiMAX.

El CSN, Servicio de conectividad de red se define como un conjunto de funciones de red que proporcionan IP servicios de conectividad a los suscriptores de WiMAX a través de la ADN.

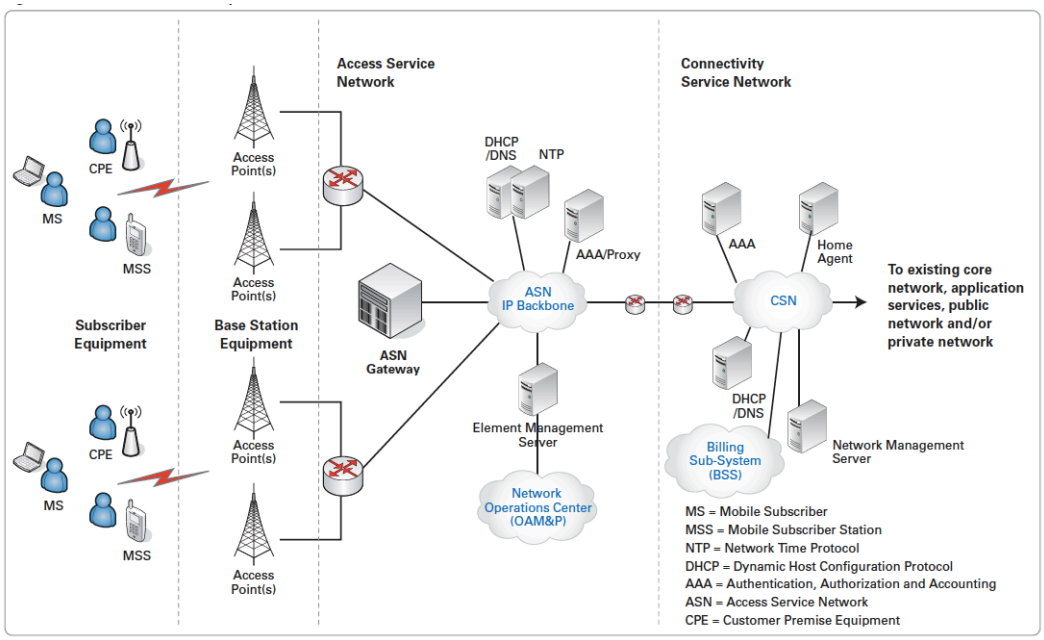

Figura 2.7. Componentes principales de una red WiMAX.

2.8.3. Seguridad

El estándar WiMAX dispone de las mejores características de seguridad entre otras tecnologías de su clase, lograda gracias a la adopción de las mejores tecnologías disponibles actualmente. Las características de seguridad son independientes al tipo de operador, ILEC Incumbent Local Exchange Carrier o CLEC Competitive Local Exchange Carrier, y a la topología de la red de acceso. En este sentido, el estándar aborda las cuatro áreas principales a tener en cuenta: cómo prevenir el uso clandestino de la conexión wireless; denegación de servicios para unidades robadas o utilizadas de forma fraudulenta; suministrar servicios sólo a los usuarios finales específicos; y cumplir con la Gestión de Acceso Seguro. Respecto a cómo prevenir la utilización clandestina de la conexión wireless, la clave está en la encriptación

La seguridad WiMAX soporta dos estándares de encriptación de calidad, DES3 y AES, que es considerado tecnología de vanguardia. Básicamente, todo el tráfico en redes WiMAX debe ser encriptado empleando el Counter Mode con Cipher Block Chaining Message Authentication Code Protocol (CCMP) que utilizan AES para transmisiones seguras y autenticación de la integración de datos.

La autenticación end-to-end de la metodología PKM-EAP, Protocolo de Autenticación Extensible) es utilizada de acuerdo con el estándar TLS de encriptación de clave pública. El estándar define un proceso de seguridad dedicada en la estación base para los principiantes. Del mismo modo, también hay unos requerimientos de encriptación mínimos para el tráfico, así como para la autenticación end-to-end -lo último que es adaptado desde la especificación del interface del servicio de datos sobre cable (DOCSIS) BPI y el protocolo de seguridad. En relación al suministro de servicios sólo a los usuarios finales específicos, la autenticación -

basada en certificados digitales X.509, es incluida en la capa de control de acceso a los medios y da a cada usuario 802.16 receptor su propio certificado incorporado, más otro para el fabricante, permitiendo a la estación base autorizar al usuario final. La privacidad de la conexión es implementada como parte de otro subnivel MAC, la capa de privacidad. Ésta se basa en el protocolo Privacy Key Management que es parte de la especificación DOCSIS BPI.

2.8.4. Debilidades del WiMAX

Los mecanismos de seguridad que poseen los actuales estándares son diferentes. La descripción de cada uno de ellos es la siguiente:

IEEE 802.16-2005.
Provee manejo de privacidad de llaves para autenticación e intercambio de llaves (PKM) y un protocolo de encapsulación de datos para el manejo de confidencialidad e integridad. Entre las principales debilidades detectadas se pueden mencionar:

- No existe autenticación de red, por lo que es posible realizar ataques usando estaciones base falsas.
- El método de generación de números pseudo-aleatorios es potencialmente débil comparado con otros métodos estándares.
- No se especifica la forma de manejar certificados.
- Utiliza DES para la encriptación, lo cual es considerado inseguro.
- Existen potenciales ataques de denegación de servicio debido a la no existencia de protección de integridad en los paquetes.

IEEE 802.16e.
Este estándar es un gran paso en términos de seguridad con respecto al estándar anterior, ya que la mayor parte de las debilidades fueron corregidas. El estándar provee mejoras en los mecanismos de autenticación, EAP, PKMv2, la mayoría de los paquetes de control son firmados para protección de integridad, se usan mecanismos basados en AES para encriptación de datos y se efectúa una pre-autenticación para proveer un inicio de sesión más eficiente para movilidad. Los análisis han detectado algunas probables debilidades:

- Es posible un ataque de DoS en la autenticación debido a que no todos los paquetes EAP están protegidos.
- El manejo de certificados es aún poco claro, ya que no se han resuelto asuntos como el almacenamiento de los mismos y sus llaves privadas.

3

3. Redes Wi-Fi

3.1. Introducción a las Redes Wi-Fi

Durante los últimos años han surgido y se han hecho con gran popularidad nuevas tecnologías inalámbricas como WI-FI, WIMAX, GSM, Bluetooth, Infrarrojos, etc, siendo los dispositivos inalámbricos una de las grandes revoluciones tecnológicas de los últimos tiempos.

Las tecnologías inalámbricas, o wireless, han conseguido esa popularidad gracias a la movilidad que permiten, llegando a cambiar la estructura y topología de las redes empresariales. Los dispositivos de almacenamiento de información que antes eran fijos ahora pueden ser portados y cambiar su conexión a distintas redes de una manera sencilla. Es probable que en un futuro cercano todos los dispositivos que hoy utilizamos se unifiquen, pudiendo pasar a llamarse "Terminales Internet", en los que se reunirían funciones de teléfono, agenda, reproductor multimedia, ordenador personal, etc.

Aunque hace bastante tiempo que existen las comunicaciones de red inalámbricas, existía un grave problema de incompatibilidades, ya que prácticamente cada fabricante usaba un estándar diferente. Por este motivo, en 1999 varias empresas (las principales del sector de las comunicaciones y redes, como 3com, Airones Intersil, Lucent Technologies, Nokia y Symbol Technologies) crean la WECA (Wireless Ethernet Compability Aliance), actualmente Wi-Fi Alliance. Esta asociación se encarga de certificar los diferentes estándares, así como su compatibilidad.

En el año 2000 certifica la interoperatividad (es decir, que puedan operar entre ellos) de equipos bajo la especificación IEEE 802.11b, a la que denomina Wi-Fi. Esto quiere decir que el usuario tiene la garantía de que todos los equipos que tengan el sello Wi-Fi pueden trabajar juntos sin problemas, independientemente del fabricante de cada uno de ellos.

La norma IEEE 802.11 fue diseñada para sustituir el equivalente a las capas físicas y MAC de la norma 802.3 (Ethernet). Esto quiere decir que en lo único que se diferencia una red Wi-Fi de una red Ethernet es en cómo se transmiten las tramas o paquetes de datos; el resto es idéntico. Por tanto, una red local inalámbrica 802.11 es completamente compatible con todos los servicios de las redes locales (LAN) de cable 802.3 (Ethernet).

Esta denominación por extensión se utiliza para todas las especificaciones posteriores basadas en el estándar 802.11x de comunicaciones inalámbricas.

3.2. Tecnología Wi-Fi

Wi-Fi, es un conjunto de estándares para redes inalámbricas de área local (WLAN) basado en las especificaciones IEEE 802.11. Fue creada por la Wi-Fi Alliance (anteriormente WECA, Wireless Ethernet Compability Alliance), la organización comercial que prueba y certifica que los equipos cumplen los estándares 802.11.

Figura 3.1. Símbolo Wi-fi

Se identifica con un símbolo con el estilo del ying-yang y su nombre no es un acrónimo de Wireless Fidelity, a pesar de que en sus comienzos se añadió junto con el nombre Wi-Fi la frase "The Standard for Wireless Fidelity" con el fin de dar significado al mismo, sino que fue creado como un juego de palabras relacionado con Hi-Fi (High Fidelity). Resaltando sus principales características, se podría decir que las Redes Inalámbricas Wi-Fi son muy fáciles de adquirir, no tanto de configurar y muy difíciles de proteger.

Es necesario aclarar que la tecnología Wi-Fi no es compatible con otros tipos de conexiones wireless como Bluetooth, GPRS, UMTS, etc.

La norma IEEE 802.11 fue diseñada para sustituir a las capas físicas y de enlace de las redes Ethernet (802.3) especificando su funcionamiento en redes WLAN (redes wireless de área local), por lo que las redes Wi-Fi y las Ethernet son idénticas salvo en el modo en el que los terminales acceden a la red, lo que supone compatibilidad entre ambas.

Las principales diferencias entre las redes cableadas Ethernet y las redes inalámbricas Wi-Fi son:
· Medio de transmisión. Mientras las redes cableadas utilizan un medio exclusivo como es el cable, las redes Wi-Fi utilizan el aire, un medio compartido.
· Señalización. Ethernet utiliza señales eléctricas y Wi-Fi ondas de Radio Frecuencia.
· Seguridad. Al utilizar cableado Ethernet "no permite", al menos tan fácilmente, que la información sea vista por extraños. Sin embargo con las redes inalámbricas la información puede ser capturada por cualquiera.

La comodidad conseguida gracias a la movilidad que ofrece la tecnología Wi-Fi, junto con la supresión del cableado son sin duda alguna los puntos fuertes de este tipo de redes. Sin embargo a su vez aparecen desventajas como la pérdida de velocidad en comparación con redes cableadas, debida a las interferencias y pérdidas de señal que el medio puede provocar.

Como se verá más adelante el principal problema que surge en las redes WLAN es la debilidad de su seguridad, ya que con las herramientas apropiadas en pocos minutos la contraseña de red se puede ver comprometida si no es correctamente protegida. Con el fin de solucionar este problemas la Wi-Fi Alliance hizo pública la clave WPA y posteriormente la WPA2, un nuevo tipo de clave mucho más robusta que las WEP, pero todo esto será explicado con más detenimiento en el apartado de seguridad.

En 1999 los principales vendedores de soluciones inalámbricas (3com, Aironet, Intersil,

Lucent Technologies, Nokia y Symbol Technologies) crearon una asociación conocida como WECA, con el fin de resolver el problema que suponía la existencia de diferentes estándares, lo que provocaba problemas de incompatibilidad. Por lo tanto esta asociación se propuso crear una marca que permitiese fomentar la tecnología inalámbrica y asegurar la compatibilidad de los dispositivos. Es en el año 2000 cuando WECA con la norma IEEE 802.11b certifica la interoperabilidad de equipos bajo la marca Wi-Fi, con lo que se garantiza que todos los elementos con el sello Wi-Fi pueden trabajar juntos sin problemas independientemente del fabricante de cada uno de ellos. En 2002 la asociación, formada ya por casi 150 miembros, anuncia la marca Wi-Fi5 utilizada para certificar equipos IEEE 802.11a de la banda de 5 Ghz, debido a que las velocidades máximas ofrecidas por la norma 802.11b (11 Mbps) había sido superada.

3.3. Familia de Tecnologías 802

La familia de estándares IEEE 802 define las capas DLC y física dentro del marco OSI de ISO, dentro de la cuál 802.11 es un miembro. La figura siguiente muestra la relación entre varios de los componentes de 802 y su relación con el modelo OSI.

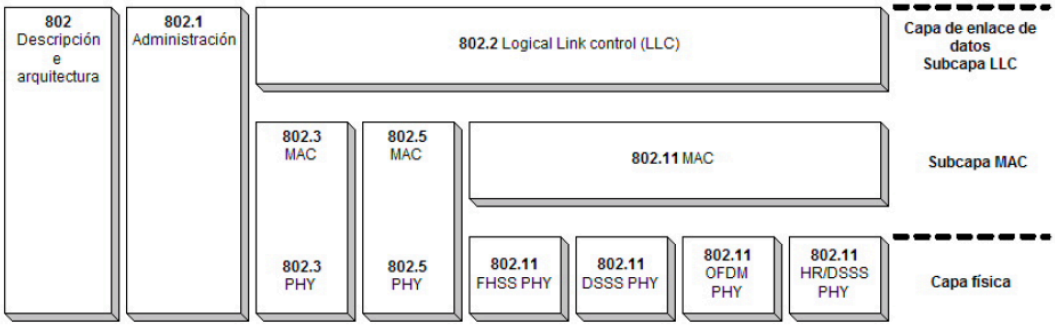

Figura 3.2. Familia IEEE 802 y la relación con OSI

Las especificaciones de IEEE 802 se centran en dos capas inferiores del modelo OSI porqu incorporan tanto componentes físicos como de control de enlace. Todas las redes 802 tienen un componente MAC y otro físico (PHY). El MAC es un conjunto de reglas que establecen como acceder al medio y como enviar los datos, pero los detalles de la transmisión y de la recepción se delegan en la capa PHY.

Las especificaciones individuales en la serie 802 se identifican con unsegundo número. Por ejemplo, 802.3 es la especificación para una red CSMA/CD (Carrier Sense Multiple Access/Collision Detection), que está relacionado con Ethernet, llamado erronamente ethernet en muchas ocasiones, y 802.5 es la especificación de Token Ring. Otras especificaciones describen otras partes de la pila de protocolos de 802, 802.2 especifica una capa de enlace común.

Las caracteristicas de administración para las redes 802 se edfinen en el 802.1. Entre las especificaciones de 802.1 están el bridging (802.1d) y las LANs virtuales o VLANs (802.1q).

Dentro de 802.11 aparecen distintas especificaciones para cada una de las posibles opciones de enlace físico, como pueden ser las basadas en FHSS, DSSS, OFDM o el enlace mediante infrarrojos.

Se puede decir también que 802.11 es otra capa de enlace a parte de 802.2 por que 802.11 se ocupa de las redes móviles, a las que añade cierta complejidad, y un conjunto de nuevas funcionalidades que no estaban recogidas anteriormente. Como resultado de esto, tenemos que la subcapa MAC de 802.11 es bastante más compleja que la equivalente de otas especificaciones MAC de 802.

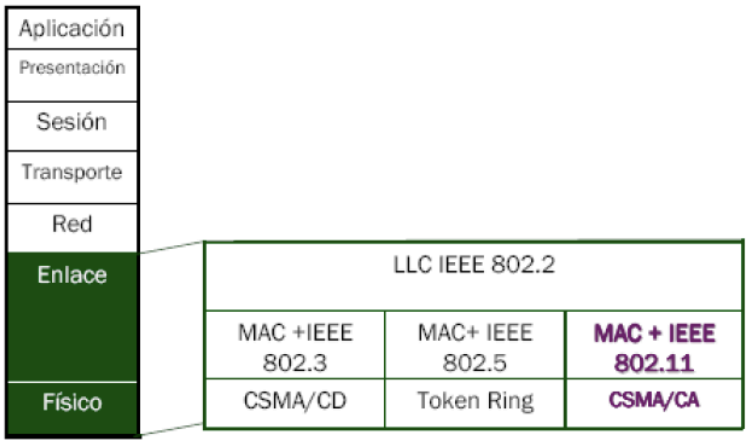

Figura 3.3 Situación IEEE 802.11 en las capas Física y Enlace

3.3.1. Protocolos 802.11

Desde 1997, cuando se certificó el primer estándar 802.11 con una velocidad de transferencia máxima de 2 Mbps, han ido surgiendo nuevos estándares que permiten velocidades cada vez mayores y con distintas bandas de frecuencias, alcanzando hoy en día hasta 300 Mbps.

A continuación se describen los diferentes protocolos para redes Wi-Fi que han sido certificados como estándares desde la aparición del IEEE 802.11

802.11 legacy

Publicado en 1997, es la versión original del estándar IEEE 802.11. Permitía dos velocidades teóricas de transmisión, 1 y 2 Mbps, mediante señales infrarrojas en la banda ISM (Industrial, Scientific and Medical, de uso no comercial) a 2,4 GHz.

Este estándar definía el protocolo CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) como método de acceso. Una parte importante de la velocidad de transmisión se utiliza en las necesidades de esta codificación para mejorar la calidad de la transmisión bajo condiciones ambientales diversas, lo que produjo dificultades de interoperabilidad entre

equipos de diferentes marcas y rechazo entre los consumidores.

En la actualidad no se fabrican productos sobre este estándar.

802.11b

Certificado en 1999, corrige las principales debilidades del estándar original y es el primer protocolo de la familia en ser aceptado por los consumidores.

Permite una velocidad máxima de transmisión de 11 Mbps trabajando en la misma banda de frecuencia de 2.4 GHz. También utiliza el método de acceso CSMA/CA lo que reduce en la práctica la velocidad máxima de transmisión a 5.9 Mbps sobre TCP y a 7.1 Mbps sobre UDP.

802.11ª

Creado en 1997, no fue aprobado hasta 1999, cuando lo hizo junto con el 802.11b, y apareció en el mercado en productos en el 2001.

Este estándar utiliza el mismo protocolo de base que el estándar original, pero opera en la banda de 5 GHz y utiliza 52 subportadoras OFDM (Orthogonal Frequency Division Multiplexing) con una velocidad máxima de 54 Mbps, lo que hace que sea un estándar práctico para redes inalámbricas con velocidades reales de unos 20 Mbps.

No puede interoperar con equipos del estándar 802.11b, a menos que dicho equipo implemente ambos estándares.

Un punto a favor para este protocolo es que al utilizar la banda de frecuencias de 5 GHz se presentan muchas menos interferencias, debido a que la banda de 2.4 GHz es utilizada por una gran cantidad de aparatos domésticos. Como contrapartida esta banda restringe el uso de los equipos a puntos en línea de vista, lo que requiere una instalación de un mayor número de puntos de acceso y a una cobertura menor. Algo que priori es negativo puede suponer una ventaja en instalaciones donde se desea que el rango de cobertura sea pequeño. Este protocolo conserva su velocidad máxima de 54 Mbps en un rango de 30 metros en el exterior y de 12 metros en el interior.

802.11h

Aparece en 2003 como una modificación del 802.11a con el fin de resolver los problemas derivados de la coexistencia de las redes Wi-Fi con sistemas de radares y satélites, debido a que la banda de 5 GHz era utilizada generalmente por sistemas militares.

Este nuevo protocolo proporciona a las redes 802.11a la capacidad de gestionar dinámicamente tanto la frecuencia, como la potencia de transmisión mediante las siguientes funcionalidades:

- DFS (Dynamic Frequency Selection): Permite evitar interferencias con sistemas de radar y asegurar una utilización uniforme de los canales disponibles.

- TPC (Transmitter Power Control): Asegura que se respetan las limitaciones de potencia transmitida que puede haber para diferentes canales en una determinada región, de manera que se minimiza la interferencia con sistemas de satélite.

802.11g

Aprobado en 2003, al igual que el 802.11b utiliza la banda de 2.4 GHz y es compatible con el mismo, pero opera con una velocidad teórica máxima de 54 Mbps (unos 24.7 Mbps de velocidad real), semejante a la del 802.11a.

El diseño del estándar se realizó pretendiendo hacerlo compatible con el 802.11b, pero en redes bajo el estándar g, la presencia de nodos bajo el estándar b reduce significativamente la velocidad de transmisión.

En la actualidad se comercializan equipos con esta especificación que, con potencias de hasta medio vatio, permiten establecer comunicaciones de hasta 50 km de distancia mediante antenas parabólicas apropiadas.

802.11n

Se espera que este protocolo se implante en 2008, aunque existen dispositivos que ofrecen de forma no oficial este estándar. La velocidad real de transmisión podría llegar a 600 Mbps, lo que significa una velocidad teórica todavía mayor, y lo que supondría redes 10 veces más rápidas que las de estándar a y g, y casi 40 veces más rápidas que las de estándar b.

El alcance que se espera sea alcanzado también se incrementará gracias a la tecnología MIMO (Multiple Input – Multiple Output), que permite utilizar varios canales a la vez para enviar y recibir datos gracias a la incorporación de varias antenas.

802.11e

Este estándar permite soportar tráfico en tiempo real en todo tipo de entornos y situaciones. El objetivo de este estándar es introducir nuevos mecanismos a nivel de enlace para soportar los servicios que requieren garantías de Calidad de Servicio (QoS).

Para conseguir dicho objetivo el protocolo introduce un nuevo elemento, el HCF (Hybrid Coordination Function), con dos tipos de acceso:

- EDCA: Enhanced Distributed Channel Access.
- HCCA: Controlled Channel Access.

802.11i

Este protocolo está dirigido a batir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación, abarcando los protocolos 802.1x, TKIP (Protocolo de Claves Integra – Seguras – Temporales), y AES (Estándar de Cifrado Avanzado).

802.11 Super G

Trabaja en la banda de 2.4 GHz y gracias al chipset Atheros alcanza velocidades de transferencia de 108 Mbps.

3.4. Topologías

El estándar 802.11 define dos modos operativos:

- El modo de infraestructura en el que los clientes de tecnología inalámbrica se conectan a un punto de acceso. Éste es por lo general el modo predeterminado para las tarjetas 802.11b.

- El modo Ad-Hoc en el que los clientes se conectan entre sí sin ningún punto de acceso.

3.4.1 Modo de Infraestructura

En el modo de infraestructura, cada estación informática (abreviado EST) se conecta a un punto de acceso a través de un enlace inalámbrico. La configuración formada por el punto de acceso y las estaciones ubicadas dentro del área de cobertura se llama conjunto de servicio básico o BSS. Estos forman una célula. Cada BSS se identifica a través de un BSSID (identificador de BSS) que es un identificador de 6 bytes (48 bits). En el modo infraestructura el BSSID corresponde al punto de acceso de la dirección MAC.

Es posible vincular varios puntos de acceso juntos (o con más exactitud, varios BSS) con una conexión llamada sistema de distribución (o SD) para formar un conjunto de servicio extendido o ESS. El sistema de distribución también puede ser una red conectada, un cable entre dos puntos de acceso o incluso una red inalámbrica.

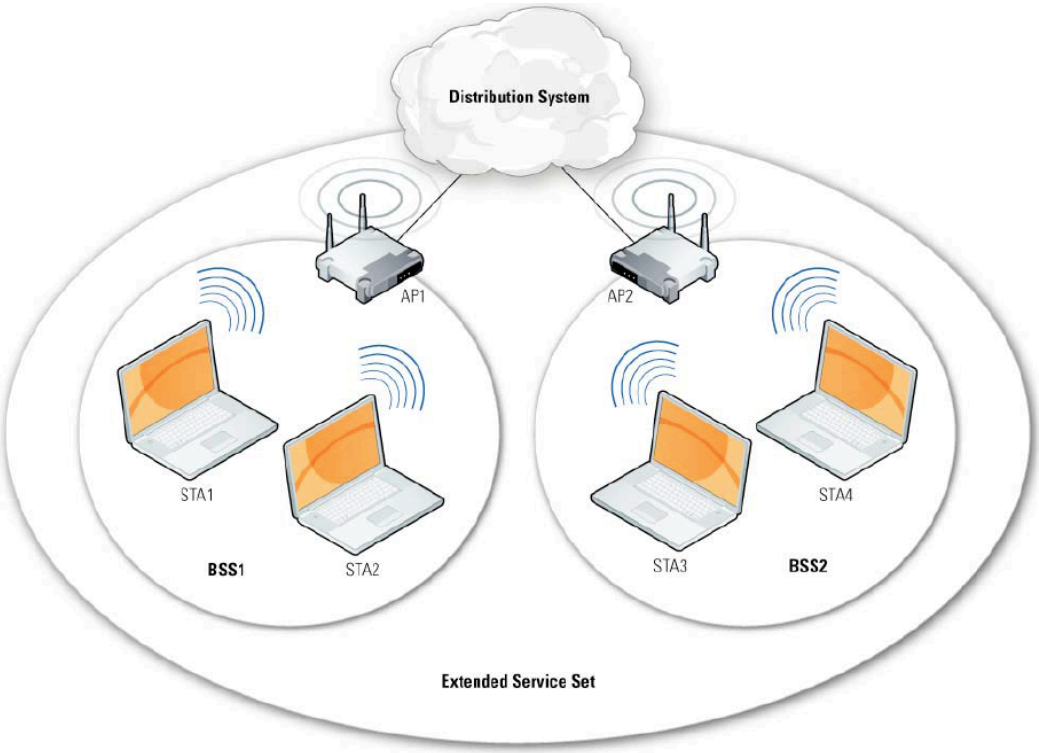

Figura 3.4. Modo infraestructura

Un ESS se identifica a través de un ESSID (identificador del conjunto de servicio extendido), que es un identificador de 32 caracteres en formato ASCII que actúa como su nombre en la red. El ESSID, a menudo abreviado SSID, muestra el nombre de la red y de alguna manera representa una medida de seguridad de primer nivel ya que una estación debe saber el SSIDara conectarse a la red extendida.

Cuando un usuario itinerante va desde un BSS a otro mientras se mueve dentro del ESS, el adaptador de la red inalámbrica de su equipo puede cambiarse de punto de acceso, según la calidad de la señal que reciba desde distintos puntos de acceso. Los puntos de acceso se comunican entre sí a través de un sistema de distribución con el fin de intercambiar información sobre las estaciones y, si es necesario, para transmitir datos desde estaciones móviles. Esta característica que permite a las estaciones moverse "de forma transparente" de un punto de acceso al otro se denomina itinerancia.

Comunicación con un punto de acceso

Cuando una estación se une a una célula, envía una solicitud de sondeo a cada canal.
Esta solicitud contiene el ESSID que la célula está configurada para usar y también el volumen de tráfico que su adaptador inalámbrico puede admitir. Si no se establece ningún ESSID, la estación escucha a la red para encontrar un SSID.

Cada punto de acceso transmite una señal en intervalos regulares (diez veces por segundo aproximadamente). Esta señal, que se llama señalización, provee información de su BSSID, sus características y su ESSID, si corresponde. El ESSID se transmite automáticamente en

forma predeterminada, pero se recomienda que si es posible se deshabilite esta opción.

Cuando se recibe una solicitud de sondeo, el punto de acceso verifica el ESSID y la solicitud del volumen de tráfico encontrado en la señalización. Si el ESSID dado concuerda con el del punto de acceso, éste envía una respuesta con datos de sincronización e información sobre su carga de tráfico. Así, la estación que recibe la respuesta puede verificar la calidad de la señal que envía el punto de acceso para determinar cuán lejos está. En términos generales, mientras más cerca un punto de acceso esté, más grande será su capacidad de transferencia de datos.

Por lo tanto, una estación dentro del rango de muchos puntos de acceso (que tengan el mismo SSID) puede elegir el punto que ofrezca la mejor proporción entre capacidad de carga de tráfico y carga de tráfico actual.

3.4.2 Modo Ad-Hoc

En el modo Ad-hoc los equipos cliente inalámbricos se conectan entre sí para formar una red punto a punto, es decir, una red en la que cada equipo actúa como cliente y como punto de acceso simultáneamente.

Figura 3.5. Modo Ad-Hoc

La configuración que forman las estaciones se llama conjunto de servicio básico independiente o IBSS. Un IBSS es una red inalámbrica que tiene al menos dos estaciones y no usa ningún punto de acceso. Por eso, el IBSS crea una red temporal que le permite a la gente que esté en la misma sala intercambiar datos. Se identifica a través de un SSID de la misma manera en que lo hace un ESS en el modo infraestructura.

En una red Ad-hoc, el rango del BSS independiente está determinado por el rango decada estación. Esto significa que si dos estaciones de la red están fuera del rango de la otra, no podrán comunicarse, ni siquiera cuando puedan "ver" otras estaciones. A diferencia del modo infraestructura, el modo Ad-hoc no tiene un sistema de distribución que pueda enviar tramas de datos desde una estación a la otra. Entonces, por definición, un IBSS es una red inalámbrica restringida.

3.5. Componentes de IEEE 802.11

El protocolo IEEE 802.11 tiene cuatro componentes principales:

1. Estaciones. Las estaciones (STAs) son dispositivos que actúan como origen y destino de los datos transmitidos. El objetivo de las redes inalámbricas es permitir la transmisión de datos entre estaciones. Como se verá posteriormente, para el caso de IEEE 802.11e las denominaremos QSTAs ya que soportan calidad de servicio.

2. Medio inalámbrico. El medio inalámbrico es el soporte que permite la transferencia de datos entre estaciones. El estándar permite dos tecnologías diferentes para la propagación de la señal, radiofrecuencia e infrarrojos, siendo ésta última la más utilizada

3. Punto de acceso. Un Punto de Acceso (AP) es una estación que permite conectar otras estaciones al sistema de distribución. Los puntos de acceso se sitúan de forma que puedan proporcionar la cobertura necesaria para dar servicio a los terminales que no tienen comunicación directa, aumentando su radio de cobertura. Además, el AP centraliza todas las comunicaciones entre STA, ya que, si dos estaciones quieren comunicarse entre ellos, deben hacerlo a través del AP. Por tanto, el radio de cobertura de un AP limita la distancia a la cuál puede comunicarse una determinada estación. Sin embargo, es posible aumentar la cobertura de la red mediante un sistema de distribución.

4. Sistema de distribución. Un sistema de distribución está formado por varios puntos de acceso conectados entre ellos mediante alguna tecnología, de forma que se pueda obtener un área de cobertura mayor. Los puntos de acceso deben comunicarse para gestionar la movilidad de las estaciones. La tecnología mas habitual en los sistemas de distribución es Ethernet, aunque se pueden utilizar otras tecnologías, incluso el estándar IEEE 802.11 creando un Sistema de Distribución Inalámbrico (WDS). Cuando una estación móvil se mueve de una zona de cobertura de un AP a la de otro (roaming), se hace evitando los cortes en la comunicación y la pérdida de cobertura.

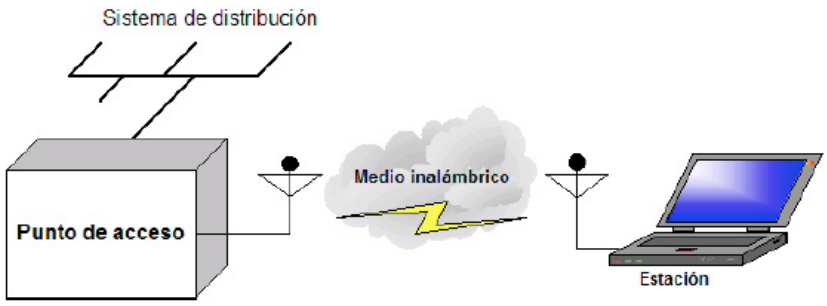

Figura 3.6. Componentes IEEE 802.11

3.6. Canales y frecuencias

Los estándares 802.11b y 802.11g utilizan la banda de 2.4 a 2.5 Ghz. En esta banda, se definen 11 canales utilizables por equipos Wi-Fi, que se pueden configurar de acuerdo a necesidades. Sin embargo, los 11 canales no son completamente independientes, los canales contiguos se superponen y se producen interferencias y en la práctica sólo se pueden utilizar 3 canales en forma simultánea, el canal 1, 6 y el canal 11. Esto es correcto para Estados Unidos y muchos países de América Latina, pero en Europa el ETSI ha definido 13 canales. En este caso, por ejemplo en España, se pueden utilizar 4 canales no-adyacentes, el canal 1, 4, 9 y el canal 13. Esta asignación de canales usualmente se hace sólo en el Access Point, pues los clientes Wi-Fi automáticamente detectan el canal, salvo en los casos en que se forma una red Ad-Hoc cuando no existe Access Point.

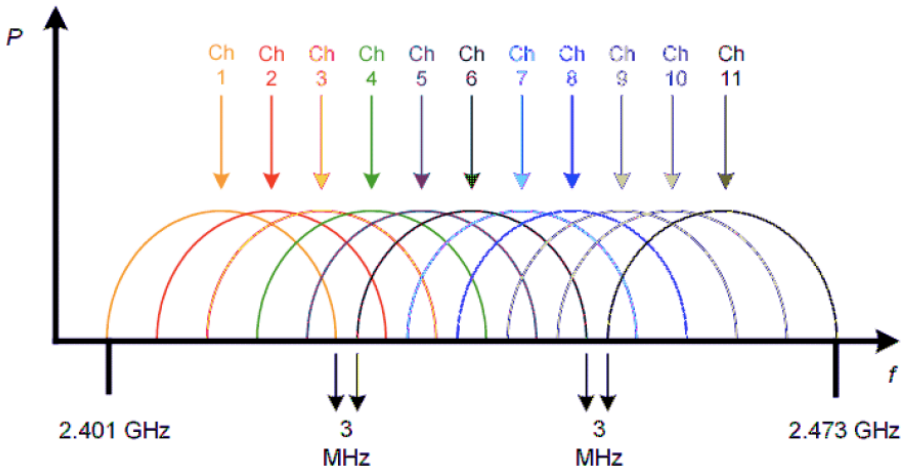

Figura 3.7. Canales y frecuencias Wi-Fi

3.7. Redes de Área Local Inalámbrica Uso y Alcance

El rango de cobertura fiable para redes WLAN IEEE 802.11 depende de varios factores, incluyendo los requisitos de velocidad de datos y la capacidad, las fuentes de interferencia de RF, las características físicas de la zona, de energía, conectividad y uso de la antena. El rango típico para la conectividad de los equipos de red IEEE 802.11 es de 50 a 100 metros (unos 328 pies) bajo techo, con un alcance significativamente mayores al aire libre. El uso de antenas de alta ganancia puede aumentar el número de dispositivos de red IEEE 802.11 alcanzables a varios kilómetros.

Los puntos de acceso AP también puede proporcionar la función de puente que conecte dos o más redes entre sí y les permite comunicarse a través de la radio inalámbrica. Permitiendo comunicaciones punto-a-punto o una configuración multipunto. En una arquitectura de punto a punto, dos LANs cableadas están conectados entre sí a través de LAN inalámbrica. En múltiples puntos de transición, una subred LAN por cable está conectada a una o varias subredes LAN de cable a través de dispositivo inalámbricos AP, eliminando así la necesidad de establecer vínculos con cable.

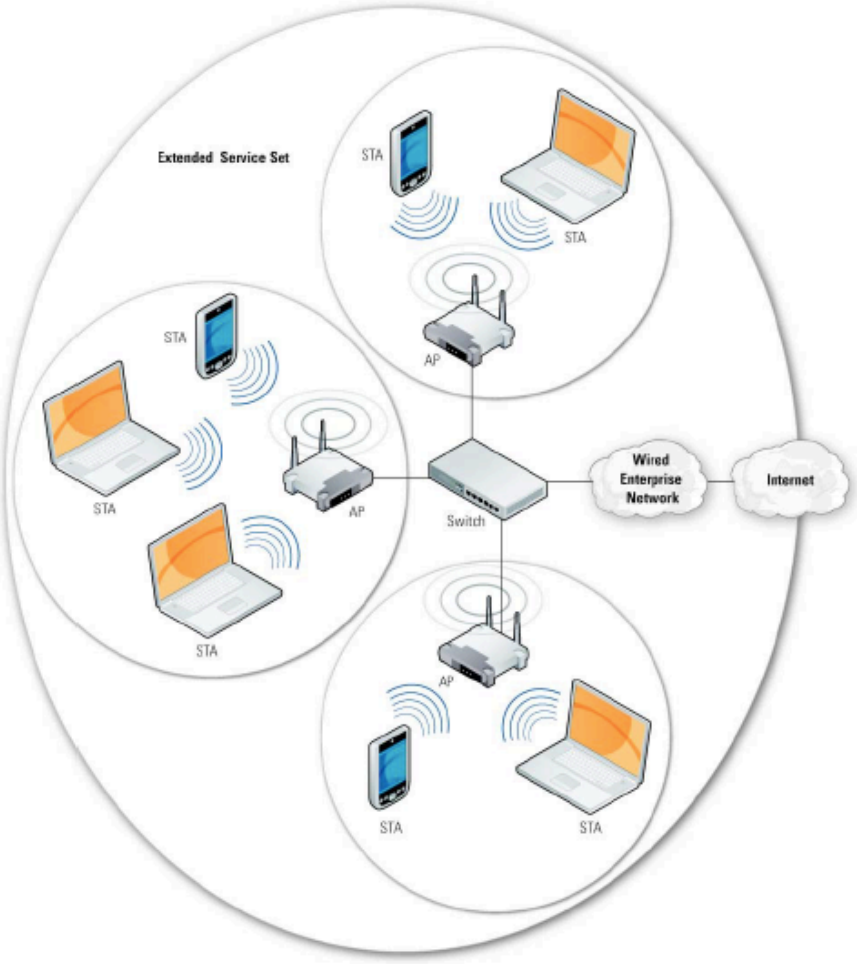

Figura 3.8. Conjunto de servicios extendidos en una empresa

Las empresas pueden conectar la distintas LAN por cable entre los diferentes edificios campus corporativos usando redes inalámbricas. Los dispositivos de bridging se colocan normalmente en la parte superior de los edificios para lograr una mayor recepción de la antena. Puentes típicos pueden extenderse por varios kilómetros, pero pueden variar dependiendo de varios factores, incluyendo el receptor específico o transceptor que se utiliza, la potencia de salida, el tipo de antena, y las condiciones ambientales. La figura siguiente ilustra una red inalámbrica punto a punto de puente entre dos redes LAN inalámbricas ubicado en dos edificios separados. En el ejemplo, los datos inalámbricos se está transmitiendo de un dispositivo cliente en el Edificio A un dispositivo cliente en el edificio B, el uso de puentes en cada edificio convenientemente situados permiten transmitir y recibir datos entre los dos edificios. Un dispositivo cliente en el edificio A se conecta a la red de la empresa por cable ubicada en el Edificio A, que luego transmite los datos destinados a un dispositivo cliente en el edificio B a través del enlace de puente inalámbrico.

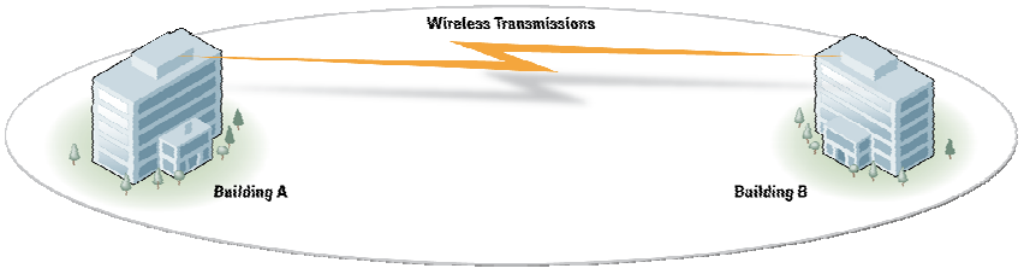

Figura 3.9. Access Point Bridging

4

4. Seguridad Wi-Fi. Riesgos y Amenazas.

Las redes Wi-Fi, a diferencia de las redes cableadas, poseen un punto débil en seguridad en el medio utilizado para la transmisión. Mientras las redes Ethernet utilizan un medio privado como el cable, las redes inalámbricas utilizan el aire, un medio compartido y altamente inseguro.

Como se verá a lo largo de este trabajo, el hecho de no disponer de redes Wi-Fi en una organización, o tenerlas bien aseguradas, no tiene por que suponer que el sistema sea seguro, ya que con que exista algún dispositivo Wi-Fi, como portátiles con tarjetas de red inalámbricas, el sistema se torna vulnerable y frágil. Es decir, el peligro no reside realmente en las propias redes, sino en la propia tecnología Wi-Fi.

4.1. Proceso de Asociación de 802.11

Una parte clave del proceso de 802.11 es descubrir una WLAN y, a continuación conectarse a ella. Los componentes principales de este proceso son los siguientes:

- Beacons - Tramas que utiliza la red WLAN para comunicar su presencia.
- Sondas - Tramas que utilizan los clientes de la WLAN para encontrar sus redes.
- Autenticación - Proceso que funciona como instrumento del estándar original 802.11, que el estándar todavía exige.
- Asociación - Proceso para establecer la conexión de datos entre un punto de acceso y un cliente WLAN.

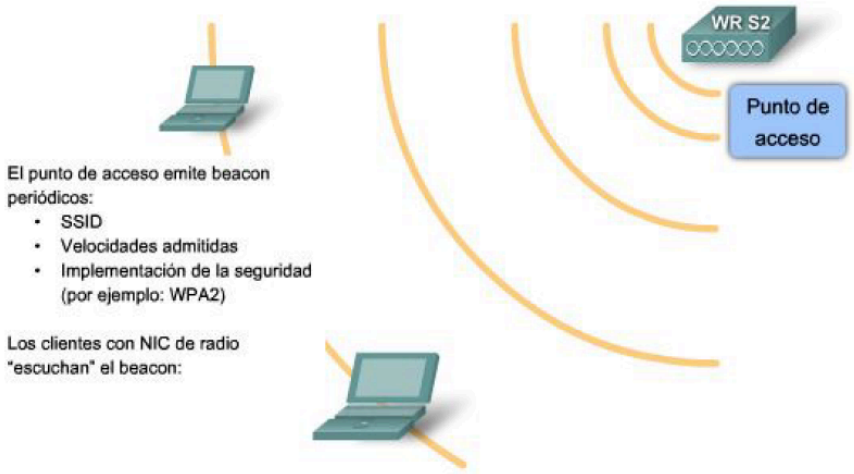

Figura 4.1. Asociación del Cliente y el Punto de Acceso

El propósito principal de la beacon es permitir a los clientes de la WLAN conocer qué redes y puntos de acceso están disponibles en un área dada, permitiéndoles, por lo tanto, elegir qué red y punto de acceso utilizar. Los puntos de acceso pueden transmitir beacons periódicamente. Aunque las beacons pueden transmitirse regularmente por un punto de

acceso, las tramas para sondeo, autenticación y asociación se utilizan sólo durante el proceso de asociación (o reasociación).

Antes de que un cliente 802.11 pueda enviar información a través de una red WLAN, debe atravesar el siguiente proceso de tres etapas:

Primera etapa.
Los clientes buscan una red específica mediante un pedido de sondeo a múltiples canales. El pedido de sondeo especifica el nombre de la red (SSID) y las tasas de bit. Un cliente típico de WLAN se configura con el SSID deseado, de modo que los pedidos de sondeo del cliente WLAN contienen el SSID de la red WLAN deseada. Si el cliente WLAN sólo quiere conocer las redes WLAN disponibles, puede enviar un pedido de sondeo sin SSID, y todos los puntos de acceso que estén configurados para responder este tipo de consulta, responderán. Las WLAN con la característica de broadcast SSID deshabilitada no responderán.

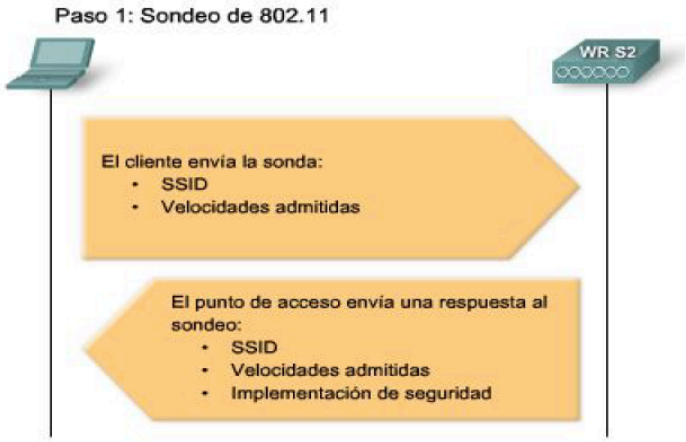

Figura 4.2. Sondeo de 802.11

Segunda etapa.

802.11 se desarrolló originalmente con dos mecanismos de autenticación. El primero, llamado autenticación abierta, es fundamentalmente una autenticación NULL donde el cliente dice "autentícame", y el punto de acceso responde con "sí". Éste es el mecanismo utilizado en casi todas las implementaciones de 802.11. Un segundo mecanismo de autenticación se basa en una clave que es compartida por la estación del cliente y el punto de acceso llamado Protección de equivalencia por clave. La idea de la clave WEP compartida es que le permita a una conexión inalámbrica la privacidad equivalente a una conexión por cable, pero cuando originalmente se implementó este método de autenticación resultó deficiente. A pesar de que la clave de autenticación compartida necesita estar incluida en las implementaciones de cliente y de punto de acceso para el cumplimiento general de los estándares, no se utiliza ni se recomienda.

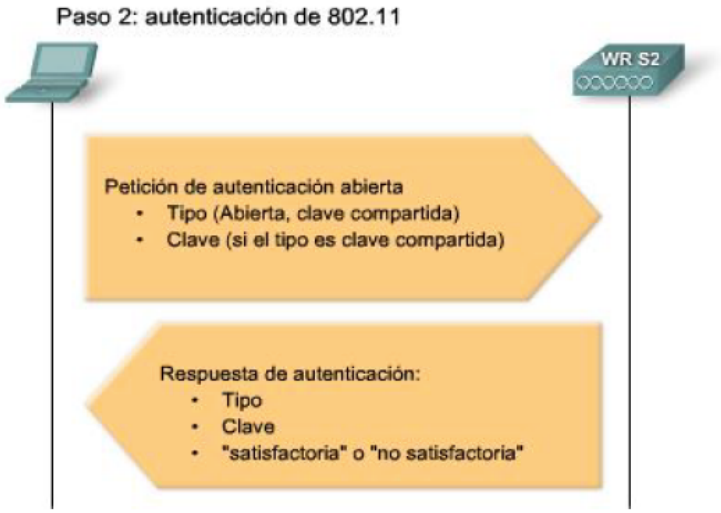

Figura 4.3. Autenticación de 802.11

Tercera etapa.

Esta etapa finaliza la seguridad y las opciones de tasa de bit, y establece el enlace de datos entre el cliente WLAN y el punto de acceso. Como parte de esta etapa, el cliente aprende el BSSID, que es la dirección MAC del punto de acceso, y el punto de acceso traza un camino a un puerto lógico conocido como el identificador de asociación (AID) al cliente WLAN. El AID es equivalente a un puerto en un switch. El proceso de asociación permite al switch de infraestructura seguir la pista de las tramas destinadas para el cliente WLAN, de modo que puedan ser reenviadas.

Una vez que un cliente WLAN se asoció con un punto de acceso, el tráfico puede viajar de un dispositivo a otro.

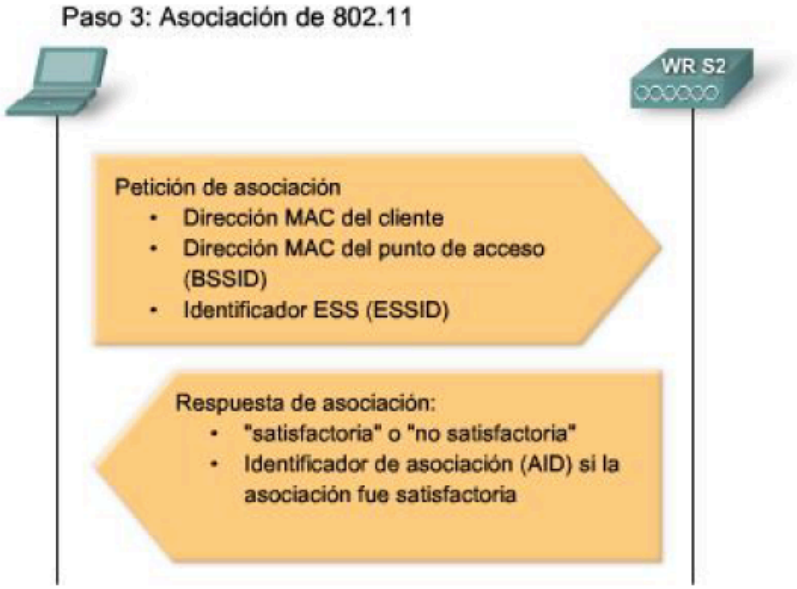

Figura 4.4. Asociación de 802.11

4.2. Protocolos de Seguridad. WEP / WPA / WPA2

IEEE publicó un mecanismo opcional de seguridad, denominado WEP, en la norma de redes inalámbricas 802.11. Pero WEP que es utilizado ampliamente en redes WLAN, ha sido roto de múltiples formas, lo que lo ha convertido en una protección inservible. Para solucionar sus deficiencias, el IEEE comenzó el desarrollo de una nueva norma de seguridad, conocida como 802.11i, que permitiera dotar de suficiente seguridad a las redes WLAN. La idea de proteger los datos de usuarios remotos conectados desde Internet a la red corporativa se extendió, por lo que la asociación de empresas Wi-Fi decidió lanzar un mecanismo de seguridad intermedio, el resultado, en 2003 lanzó WPA. Analizaremos las características de los mecanismos de seguridad WEP, WPA y WPA2.

4.2.1 WEP

WEP (Wired Equivalent Privacy, privacidad equivalente al cable) es el algoritmo opcional de seguridad incluido en la norma IEEE 802.11. Los objetivos de WEP, según el estándar, son proporcionar confidencialidad, autentificación y control de acceso en redes WLAN.

WEP utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso. El estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red. Esto genera varios inconvenientes. Por un lado, la clave está almacenada en todas las estaciones, aumentando las posibilidades de que sea comprometida. Y por otro, la distribución manual de claves provoca un aumento de mantenimiento por parte del administrador de la red, lo que conlleva, en la mayoría de ocasiones, que la clave se cambie poco o nunca.

El algoritmo de encriptación utilizado es RC4 con claves (seed), según el estándar, de 64 bits. Estos 64 bits están formados por 24 bits correspondientes al vector de inicialización más 40 bits de la clave secreta. Los 40 bits son los que se deben distribuir manualmente. El vector de inicialización (IV), en cambio, es generado dinámicamente y debería ser diferente para cada trama. El objetivo perseguido con el IV es cifrar con claves diferentes para impedir que un posible atacante pueda capturar suficiente tráfico cifrado con la misma clave y terminar finalmente deduciendo la clave. Como es lógico, ambos extremos deben conocer tanto la clave secreta como el IV. La clave secreta es conocida puesto que está almacenado en la configuración de cada elemento de red. El IV, en cambio, se genera en un extremo y se envía en la propia trama al otro extremo, por lo que también será conocido. Al viajar el IV en cada trama es sencillo de interceptar por un posible atacante.

El algoritmo de encriptación de WEP funciona de la siguiente manera, se calcula un CRC de 32 bits de los datos. Este CRC-32 es el método que propone WEP para garantizar la integridad de los mensajes (ICV, Integrity Check Value). El PRNG (Pseudo-Random Number Generator) de RC4 genera una secuencia de caracteres pseudoaleatorios (keystream), a partir del seed, de la misma longitud que los bits obtenidos en el punto 1. Se calcula la O exclusiva (XOR) de los caracteres del punto 1 con los del punto 3. El resultado es el mensaje cifrado. Se envía el IV (sin cifrar) y el mensaje cifrado dentro del campo de datos (frame body) de la trama IEEE 802.11.
El algoritmo para descifrar es similar al anterior. Debido a que el otro extremo conocerá el IV

y la clave secreta, tendrá entonces el seed y con ello podrá generar el keystream. Realizando el XOR entre los datos recibidos y el keystream se obtendrá el mensaje sin cifrar (datos y CRC-32). A continuación se comprobara que el CRC-32 es correcto.

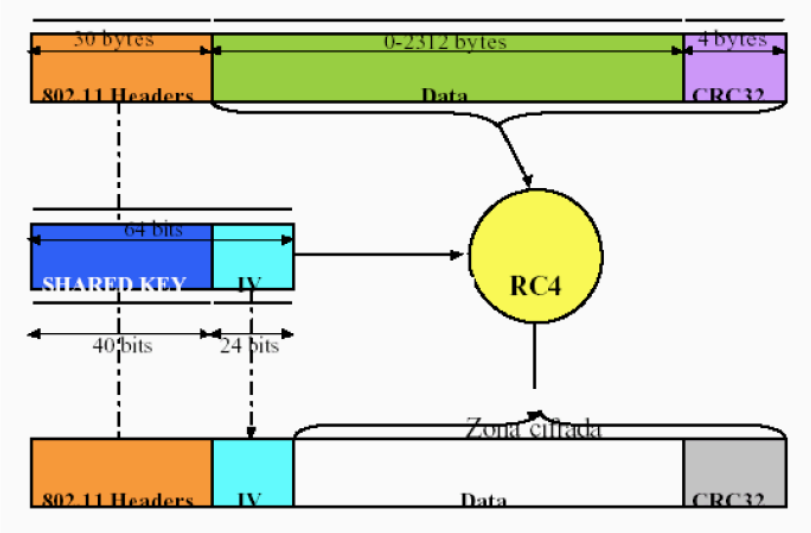

Figura 4.5. Esquema de funcionamiento de WEP

Debilidad del Vector de Inicialización.

La implementación del vector de inicialización (IV) en el algoritmo WEP tiene varios problemas de seguridad. Recordemos que el IV es la parte que varía de la clave (seed) para impedir que un posible atacante recopile suficiente información cifrada con una misma clave.

Sin embargo, el estándar 802.11 no especifica como manejar el IV. Según se indica que debería cambiarse en cada trama para mejorar la privacidad, pero no obliga a ello. Queda abierta a los fabricantes la cuestión de como variar el IV en sus productos. La consecuencia de esto es que buena parte de las implementaciones optan por una solución sencilla: cada vez que arranca la tarjeta de red, se fija el IV a 0 y se incrementa en 1 para cada trama. Y esto ocasiona que las primeras combinaciones de IVs y clave secreta se repitan muy frecuentemente. Mas aun si tenemos en cuenta que cada estación utiliza la misma clave secreta, por lo que las tramas con igual clave se multiplican en el medio.

Por otro lado, el número de vectores de inicialización diferentes no es demasiado elevado (16 millones aprox.), por lo que terminaran repitiéndose en cuestión de minutos u horas. El tiempo seria menor cuanto mayor sea la carga de la red. Lo ideal sería que el IV no se repitiese nunca, pero como vemos, esto es imposible en WEP. La cantidad de veces que se repite un mismo IV dependerá de la implementación elegida para variar el IV por el fabricante (secuencial, aleatoria, etc.) y de la carga de la red. Observemos que es trivial saber si dos tramas han sido cifradas con la misma clave, puesto que el IV se envía sin cifrar y la clave secreta es estática. La longitud de 24 bits para el IV forma parte del estándar y no puede cambiarse. Bien es cierto que existen implementaciones con claves de 128 bits (lo que se conoce como WEP2), sin embargo, en realidad lo único que se aumenta es la clave secreta (104 bits) pero el IV se conserva con 24 bits. El aumento de la longitud de la clave secreta no soluciona la debilidad del IV.

Una vez hemos capturado varias tramas con igual IV, es decir, con igual keystream, necesitamos conocer el mensaje sin cifrar de una de ellas. Haciendo el XOR entre un mensaje sin cifrar y el mismo cifrado, nos dará el keystream para ese IV. Conociendo el keystream asociado a un IV, podremos descifrar todas las tramas que usen el mismo IV. El problema es entonces conocer un mensaje sin cifrar, aunque esto no es tan complicado, porque existen tráficos predecibles o bien, podemos provocarlos nosotros (mensajes ICMP de solicitud y respuesta de eco, confirmaciones de TCP, etc.) .

Con lo que hemos descrito no podemos deducir la clave secreta, aunque sí es posible generar una tabla con los vectores de inicialización de los que sabemos su keystream, la cual permitirá descifrar cualquier mensaje que tenga un IV contenido en la tabla.

Sin embargo, podemos llegar a más y deducir la clave secreta. Una nueva vulnerabilidad del protocolo WEP permite deducir la clave total conociendo parte de la clave (justamente, el IV que es conocido). Para ello necesitamos recopilar suficientes IVs y sus keystreams asociados obtenidos por el procedimiento anterior.

Otras debilidades de WEP.

WEP también adolece de otros problemas además de los relacionados con el vector de inicialización y la forma de utilizar el algoritmo RC4. Entre los objetivos de WEP, como comentamos anteriormente, se encuentra proporcionar un mecanismo que garantice la integridad de los mensajes. Con este fin, WEP incluye un CRC-32 que viaja cifrado. Sin embargo, se ha demostrado que este mecanismo no es válido y es posible modificar una parte del mensaje y a su vez el CRC, sin necesidad de conocer el resto. Esto permitiría, por ejemplo, modificar algún número de la trama sin que el destino se percatara de ello. En lugar del algoritmo de CRC se recomienda como ICV (Integrity Check Value) un algoritmo diseñado para tal fin como SHA1-HMAC.

El estándar IEEE 802.11 incluye un mecanismo de autentificación de las estaciones basado en un secreto compartido. Para ello se utiliza la misma contraseña de WEP en la forma que describimos a continuación. Una estación que quiere unirse a una red, solicita al punto de acceso autentificación. El punto de acceso envía un texto en claro a la estación y ésta lo cifra y se lo devuelve. El punto de acceso finalmente descifra el mensaje recibido, comprueba que su ICV es correcto y lo compara con el texto que envió.

El mecanismo anterior de autentificación de secreto compartido tiene el problema de enviar por la red el mismo texto sin cifrar y cifrado con la clave WEP (esta clave coincide con la utilizada para asegurar la confidencialidad). El estándar es consciente de esta debilidad y aconseja no utilizar el mismo IV para el resto de transmisiones. Sin embargo, tanto si las implementaciones repiten ese IV como sino, el mecanismo ofrece información que podría ser aprovechada para romper la clave WEP utilizando las debilidades del vector de inicialización explicadas anteriormente.

WEP no incluye autentificación de usuarios. Lo más que incluye es la autentificación de estaciones. El sistema de autentificación descrito es tan débil que el mejor consejo sería no utilizarlo para no ofrecer información extra a un posible atacante. En este caso tendríamos una

autentificación de sistema abierto, es decir, sin autentificación.

Entre la larga lista de problemas de seguridad de WEP se encuentra también la ausencia de mecanismos de protección contra mensajes repetidos (replay). Esto permite que se capture un mensaje y se introduzca en la red en un momento posterior. El paquete podría ser, por ejemplo, el que contiene la contraseña de un usuario para utilizar un determinado servicio.

Todos los problemas comentados unidos a las características propias de WEP como es la distribución manual de claves y la utilización de claves simétricas, hacen que este sistema no sea apropiado para asegurar una red inalámbrica.

4.2.2 WAP

WPA (Wi-Fi Protected Access, acceso protegido Wi-Fi) es la respuesta de la asociación de empresas Wi-Fi a la seguridad que demandan los usuarios y que WEP no puede proporcionar. WPA soluciona todas las debilidades conocidas de WEP y se considera suficientemente seguro. Puede ocurrir incluso que usuarios que utilizan WPA no vean necesidad de cambiar a IEEE 802.11i cuando esté disponible.

Las principales características de WPA son la distribución dinámica de claves, utilización mas robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autentificación. WPA incluye las siguientes tecnologías:
IEEE 802.1X. Estándar del IEEE de 2001 para proporcionar un control de acceso en redes basadas en puertos. El concepto de puerto, en un principio pensado para las ramas de un switch, también se puede aplicar a las distintas conexiones de un punto de acceso con las estaciones. Las estaciones tratarán entonces de conectarse a un puerto del punto de acceso. El punto de acceso mantendrá el puerto bloqueado hasta que el usuario se autentifique. Con este fin se utiliza el protocolo EAP y un servidor AAA (Authentication Authorization Accounting) como puede ser RADIUS (Remote Authentication Dial-In User Service). Si la autorización es positiva, entonces el punto de acceso abre el puerto.

El servidor RADIUS puede contener políticas para ese usuario concreto que podría aplicar el punto de acceso (como priorizar ciertos tráficos o descartar otros). EAP. Definido en la RFC 2284, es el protocolo de autentificación extensible para llevar a cabo las tareas de autentificación, autorización y contabilidad.

EAP fue diseñado originalmente para el protocolo PPP (Point-to-Point Protocol), aunque WPA lo utiliza entre la estación y el servidor RADIUS. Esta forma de encapsulación de EAP está definida en el estándar 802.1X bajo el nombre de EAPOL (EAP over LAN). TKIP (Temporal Key Integrity Protocol). Según indica Wi-Fi, es el protocolo encargado de la generación de la clave para cada trama. MIC (Message Integrity Code) o Michael. Código que verifica la integridad de los datos de las tramas.

Mejoras de WPA respecto a WEP.
WPA soluciona la debilidad del vector de inicialización (IV) de WEP mediante la inclusión de vectores del doble de longitud (48 bits) y especificando reglas de secuencia que los fabricantes deben implementar. Los 48 bits permiten generar 2 elevado a 48 combinaciones de claves

diferentes, lo cual parece un número suficientemente elevado como para tener duplicados.

El algoritmo utilizado por WPA sigue siendo RC4. La secuencia de los IV, conocida por ambos extremos de la comunicación, se puede utilizar para evitar ataques de repetición de tramas (replay). Para la integridad de los mensajes (ICV), se ha eliminado el CRC-32 que se demostró inservible en WEP y se ha incluido un nuevo código denominado MIC. Las claves ahora son generadas dinámicamente y distribuidas de forma automática por lo que se evita tener que modificarlas manualmente en cada uno de los elementos de red cada cierto tiempo, como ocurría en WEP.

Para la autentificación, se sustituye el mecanismo de autentificación de secreto compartido de WEP así como la posibilidad de verificar las direcciones MAC de las estaciones por la terna 802.1X / EAP / RADIUS. Su inconveniente es que requiere de una mayor infraestructura: un servidor RADIUS funcionando en la red, aunque también podría utilizarse un punto de acceso con esta funcionalidad.

WPA puede funcionar en dos modos:

- Con servidor AAA, RADIUS normalmente.
  Este es el modo indicado para las empresas. Requiere un servidor configurado para desempeñar las tareas de autentificación, autorización y contabilidad.

- Con clave inicial compartida (PSK).
  Este modo está orientado para usuarios domésticos o pequeñas redes. No requiere un servidor AAA, sino que se utiliza una clave compartida en las estaciones y punto de acceso. Al contrario que en WEP, esta clave sólo se utiliza como punto de inicio para la autentificación, pero no para el cifrado de los datos.

4.2.3 WPA2

WPA2 (Wi-Fi Protected Access 2 - Acceso Protegido Wi-Fi 2) es un sistema para proteger las redes inalámbricas (WI-FI); creado para corregir las vulnerabilidades detectadas en WPA.

WPA2 está basada en el nuevo estándar 802.11i. WPA, por ser una versión previa, que se podría considerar de migración, no incluye todas las características del IEEE 802.11i, mientras que WPA2 se puede inferir que es la versión certificada del estándar 802.11i. El estándar 802.11i fue ratificado en junio de 2004. La alianza WI-FI llama a la versión de clave precompartida WPA-Personal y WPA2-Personal y a la versión con autenticación 802.1x/EAP como WPA-Enterprise y WPA2-Enterprise.

Los fabricantes comenzaron a producir la nueva generación de puntos de accesos apoyados en el protocolo WPA2 que utiliza el algoritmo de cifrado AES (Advanced Encryption Standard). Con este algoritmo será posible cumplir con los requerimientos de seguridad del gobierno de USA - FIPS140-2. WPA2 está idealmente pensado para empresas tanto del sector privado como del público.

Los productos que son certificados para WPA2 le dan a los gerentes de TI la seguridad que la

tecnología cumple con estándares de interoperatividad. Si bien parte de las organizaciones estaban aguardando esta nueva generación de productos basados en AES es importante resaltar que los productos certificados para WPA siguen siendo seguros de acuerdo a lo establecido en el estándar 802.11i.

4.3. Amenazas y Vulnerabilidades

Como el número de organizaciones que implementan redes inalámbricas continúa creciendo cada día, se vuelve aún más importante entender los tipos de vulnerabilidades y amenazas que afectan a las redes WLAN IEEE 802.11 para implementar las medidas de seguridad apropiadas. Algunas de las vulnerabilidades que se describen en esta sección son inherentes a la norma WLAN IEEE 802.11, mientras que otros son comunes para las redes WLAN o redes inalámbricas en general.

4.3.1 La Pérdida de la Confidencialidad

Debido a la naturaleza de la tecnología inalámbrica que utiliza difusión de radio, es más difícil garantizar la confidencialidad en una red inalámbrica a una red cableada. Las redes cableadas tradicionales garantizar la seguridad inherente a través del uso de un medio físico, a la que un atacante debe tener acceso. Las redes inalámbricas se propagan las señales en el espacio, por lo que las contramedidas de seguridad físicos tradicionales menos eficaz y el acceso a la red mucho más fácil, el aumento de la importancia de la confidencialidad adecuada en las redes inalámbricas.

La escucha pasiva sobre las comunicaciones WLAN IEEE 802.11 puede causar un riesgo significativo para una organización. Un intruso puede escanear las señales de RF capturar los datos que atraviesan el medio inalámbrico. La información confidencial, los identificadores de red y las contraseñas y los datos de configuración, son algunos ejemplos de datos que pueden ser capturadas. Además, los atacantes con antenas de alta ganancia puede capturar los datos de las redes inalámbricas más allá del alcance de una red normal, por lo tanto la confidencialidad es una medida de seguridad crítica.

El espionaje realizado con una herramienta de analizador de red inalámbrica o sniffer es particularmente fácil para IEEE 802.11 WLAN. Los rastreadores de red tienen la ventaja de las debilidades del algoritmo de clave para el RC4 utilizado por WEP. Para explotar estas debilidades, el sniffer monitoriza de forma pasiva la WLAN y calcula las claves de cifrado después de escuchar un número variable de paquetes. En una red altamente saturada, recoger la cantidad de datos necesarios para calcular las claves WEP sólo requiere un par de horas, pero si el volumen de tráfico es bajo, puede tardar hasta un día. Por ejemplo, un punto de acceso que está transmitiendo 3.000 bytes a 11 Mbps después de aproximadamente 10 horas la clave puede ser descifrada. Una vez que el atacante recupera los textos cifrados, tanto en la integridad y confidencialidad de datos puede ser fácilmente comprometida.

Existen múltiples herramientas avanzadas que utilizar métodos para explotar la debilidad de la IEEE 802.11 de seguridad en menos tiempo. Después de que los paquetes de red se han capturados, las claves se pueden adivinar en menos de unos segundos. Una vez que el usuario

conoce la clave WEP, puede leer cualquier paquete que viaja por la red WLAN. Otro de los riesgos de las redes WLAN es la pérdida de confidencialidad a través de las escuchas simple en el tráfico broadcast. Los concentradores Ethernet transmite generalmente el tráfico de red a todas las interfaces físicas y los dispositivos conectados, lo que deja el tráfico transmitido vulnerables a la vigilancia no autorizada. Por ejemplo, un punto de acceso conectado a un puerto en un concentrador Ethernet que está transmitiendo el tráfico de datos recibido en su interfaz de la red inalámbrica. El uso de un concentrador en la infraestructura Ethernet aumenta el riesgo de que el AP puede transmitir datos privados o confidenciales que se transmiten a través del Hub, concentrador. Los switches permiten reducir este riesgo al proporcionar canales dedicados entre los dispositivos de comunicación.

Un usuario malintencionado o irresponsable puede físicamente situar un Rogue AP en un armario, debajo de una mesa de conferencia, o en cualquier otra área escondida dentro de un edificio. El punto de acceso ilícito podría ser utilizado para permitir que personas no autorizadas puede tener acceso a una red de una empresa.

La ubicación de un Rogue AP aparece como accesible a los usuarios de la WLAN, y está configurado para que aparezca como un punto de acceso legítimo a los clientes inalámbricos, el punto de acceso ilícito puede convencer a los clientes inalámbricos de su legitimidad y hacer que los clientes inalámbricos pueden conectarse y transmitir el tráfico al punto de acceso ilícito. En este escenario, un atacante puede capturar todos los datos que se transmiten a través del punto de acceso ilícito, por encima de todo el protocolo de confidencialidad inalámbrico. También es importante tener en cuenta que no todos los puntos de acceso son utilizadas por usuarios malintencionados. En muchos casos, los puntos de acceso se han desplegado por usuarios, sin la aprobación del departamento de TI. Estos puntos de acceso que frecuentemente se utilizan sin las configuraciones de seguridad adecuadas y representan un riesgo significativo de seguridad.

4.3.2 La Pérdida de Integridad

Los problemas de integridad de datos en las redes inalámbricas son similares a los de las redes cableadas. Dado que las organizaciones con frecuencia ponen en práctica las comunicaciones inalámbricas y por cable sin la protección adecuada de cifrado de datos, en estos casos la integridad puede ser difícil de lograr. Por ejemplo, un atacante puede comprometer la integridad de los datos mediante la supresión o la modificación de los datos en un correo electrónico a través del sistema inalámbrico. Esto puede ser perjudicial para una organización si el correo electrónico es importante y es ampliamente distribuido entre los destinatarios del correo electrónico. Debido a las características de seguridad del estándar IEEE 802.11 no proporcionan integridad de los mensajes, otros tipos de ataques activos que comprometen la integridad del sistema se basan en las deficiencias específicas de parte del mecanismo CRC-32 de integridad de WEP.

4.3.3 La Pérdida de Disponibilidad

Una negación de la disponibilidad de WLAN a menudo implica alguna forma de ataque de DoS, tales como atascos o inundaciones. Jamming se produce cuando una señal de radiofrecuencia emitida por un dispositivo inalámbrico abruma otros dispositivos

inalámbricos y las señales, causando una pérdida de las comunicaciones. Jamming pueden ser causado deliberadamente por un usuario malicioso o causado accidentalmente por las emisiones de otros dispositivos legítimos que operan dentro de un espectro sin licencia, tales como un teléfono inalámbrico o un horno microondas. Inundaciones ataques se inician utilizando un software diseñado para transmitir un gran número de paquetes a un punto de acceso u otro dispositivo inalámbrico, haciendo que el dispositivo que se va abrumado por los paquetes y dejar de funcionamiento normal. Las inundaciones pueden provocar que una WLAN degrade el nivel de rendimiento aceptable o incluso fallar completamente la WLAN. Las amenazas y las inundaciones son difíciles de combatir en cualquier comunicación de ondas de radio, y el estándar IEEE 802.11 no proporciona ninguna defensa contra ellos.

Las tramas de gestión de IEEE 802.11 son otro punto para ataques de denegación de servicio contra las redes WLAN. Las tramas de gestión para el proceso de asociación y de disociar los AP y STA de una WLAN. Por diseño, el estándar IEEE 802.11 no proporciona una protección contra estos ataques. Si un adversario fuerza una trama de disociación y la envía a un AP o STA, el dispositivo de destino concede la solicitud y cierra su asociación de comunicación. Otro tipo de ataque, conocido como ataque a la asociación, se dirige a la tabla de un punto de acceso, que monitoriza el estado de las entradas asociadas al AP. Un ataque de este tipo, en general inunda esta tabla con peticiones falsas, hasta que el punto de acceso ya no permite que las asociaciones legítimas. Los ataques de asociación más avanzados pueden obligar incluso al STA a conectarse a puntos de acceso falsos.

Otra amenaza para la IEEE 802.11 de disponibilidad de WLAN, es el uso de las redes WLAN IEEE 802.11n. IEEE 802.11n ofrece el modo de Greenfield que deshabilita la compatibilidad con IEEE 802.11n hacia atrás y exige que todos los dispositivos WLAN nativos se ejecute en modo IEEE 802.11n. El modo de Greenfield puede causar interferencia significativa para todos los dispositivos IEEE 802.11n si no se encuentren en su área de transmisión. Por ejemplo, un vecino IEEE 802.11n WLAN en funcionamiento en el modo de Greenfield sin querer puede crear una denegación de servicio potenciales para la WLAN.

Los usuarios también pueden causar una pérdida de disponibilidad al querer monopolizar la capacidad de una WLAN, al querer descargar archivos de gran tamaño, negando a otros usuarios el acceso a la red.

4.4. Ataques sobre Redes Wi-Fi

4.4.1. Clasificación de los ataques

Podemos realizar una clasificación de los ataques que se pueden ser realizados sobre una Red Inalámbrica en dos grandes categorías:

- Ataques Pasivos

  Este tipo de ataques se produce cuando una persona no autorizada accede a la información, pero no realiza ninguna modificación de la misma. Dentro de esta categoría podemos mencionar dos tipos de actividades:

- Vigilar/Espiar. El atacante monitoriza el contenido de las transmisiones para descubrir el contenido de la información.

- Analizar el Tráfico. El atacante captura la información transmitida y trata de descubrir datos sobre los parámetros de la comunicación, como el ESSID, contraseñas, Direcciones MAC o IP, etc.

- Ataques Activos

  Este tipo de ataques se produce cuando una persona no autorizado modifica o altera el contenido de la información, o impide su utilización. En esta categoría existe un mayor número de actividades, pudiendo citar como las más comunes:

  - Denegación de Servicio. El atacante impide la utilización normal de las transmisiones Wi-Fi. Con esta tecnología estos ataques son muy difíciles de evitar y muy fáciles de realizar.

  - Enmascaramiento. Es un robo de identidad, en el que el intruso se hace pasar por un usuario autorizado para acceder a la información.

  - Retransmisión. El atacante se coloca entre el emisor y el receptor, recibe la información y la retransmite, para evitar ser descubierto.

  - Alteración. Basado en modificar mensajes legítimos añadiendo o borrando parte del contenido.

4.5. DoS – Ataques de Denegación de Servicio

Existen multitud de herramientas para lanzar ataques sobre Redes Wi-Fi, en especial de Denegación de Servicio, DoS, que como ya comentamos son fáciles de llevar a cabo y extremadamente difíciles de poder detectar y evitar.

Habitualmente son ataques que duran poco tiempo, lo que hace aumentar su dificultad de detección. A continuación, se describen algunos de los ataques de Denegación de Servicio sobre Redes Wi-Fi más populares.

4.5.1. Saturación del Ambiente con Ruido de RF

Las ondas de RF transmitidas por las redes Wi-Fi son atenuadas e interferidas por diversos obstáculos y ruidos. Lo que se transmite es energía, y esta es absorbida y reducida. A medida que nos alejemos del Punto de Acceso la calidad de la señal se verá atenuada debido a la presencia de paredes o a las transmisiones de otros dispositivos.

Las influencias negativas de las interferencias en las Redes Wireless comentadas anteriormente, hacen que con facilidad un atacante puede producir ruido o interferencias deliberadamente que afecten a nuestra red, pues el medio de transmisión es público,

provocando que la relación entre Señal y Ruido sea muy pequeña y nuestros usuarios pierdan la conectividad a la red.

Es un ataque sencillo, y puede ser realizado con micro-ondas, o más profesionalmente con Generadores de Ruido. Si el administrador no cuenta con las herramientas apropiadas le resultará muy complicado detectar el ataque.

4.5.2. Torrente de Autenticaciones

Este ataque se da en escenarios donde está implantado el estándar 802.1x y un Servidor RADIUS, donde es preciso que cada usuario se autentique. Este procedimiento es criptográficamente complejo y requiere un consumo considerable del procesador, pues se deberán implementar túneles y realizar búsquedas en bases de datos.

Si un atacante se dedicara a enviar falsas peticiones de autenticación repetitivas y en gran cantidad y, además, de manera simultánea, mantendría a la red ocupada con el complejo proceso de autenticación, con lo que lograría impedir que los usuarios legítimos pudieran autenticarse, pues el Servidor RADIUS estaría ocupado con el falso usuario.

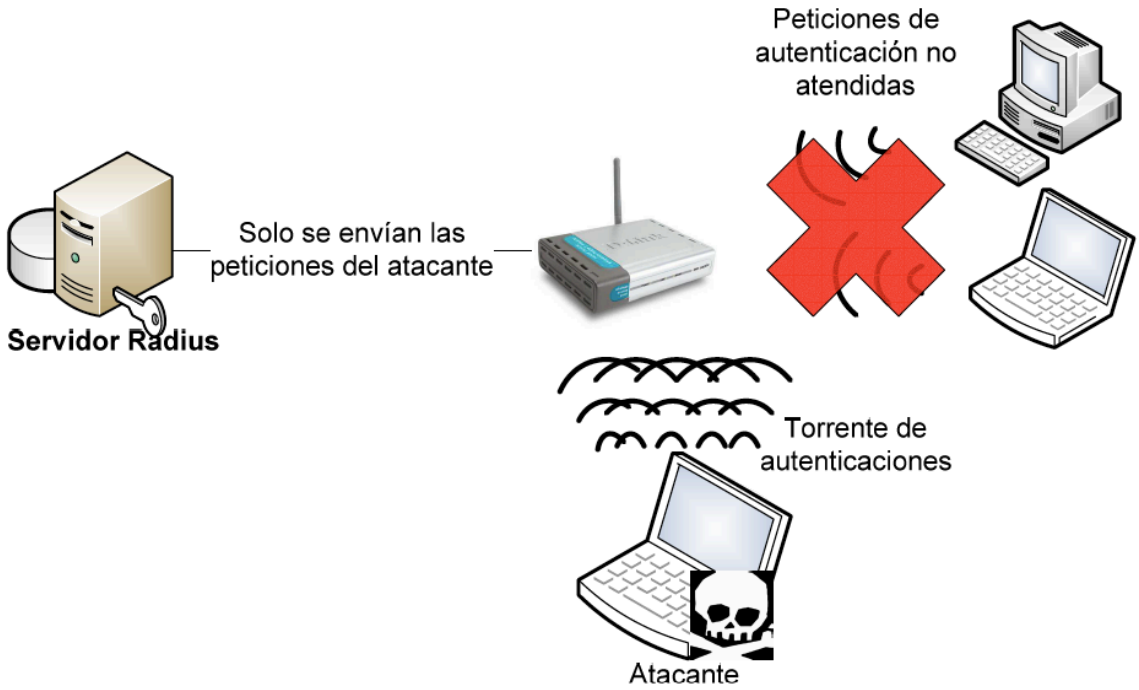

Figura 4.6. Ataque torrente de Autenticaciones

4.5.3. WPA – Modificación de Paquetes

Uno de los fallos importantes del protocolo WEP consiste en la falta de un método de chequeo de integridad. Los paquetes pueden ser alterados o sustraídos, sin que nadie se de cuenta. Una de las mejoras introducidas por WPA fue la inclusión de un sistema de chequeo de integridad

(MIC), sin embargo, este sistema posee una vulnerabilidad que permite realizar ataques de Denegación de Servicio.

El citado mecanismo verifica si los paquetes han sido modificados o manipulados. Cuando detecta que en menos de un minuto se han modificado al menos 2 paquetes el sistema asume que está siendo atacado y, como medida de prevención, desconecta a todos los usuarios de la red inalámbrica. Dicho esto resulta evidente cual será la metodología del ataque, el atacante alterará el contenido de varios paquetes, consiguiendo así la desconexión de todos los usuarios. Esta operación puede ser repetida constantemente provocando la pérdida de rendimiento en la red.

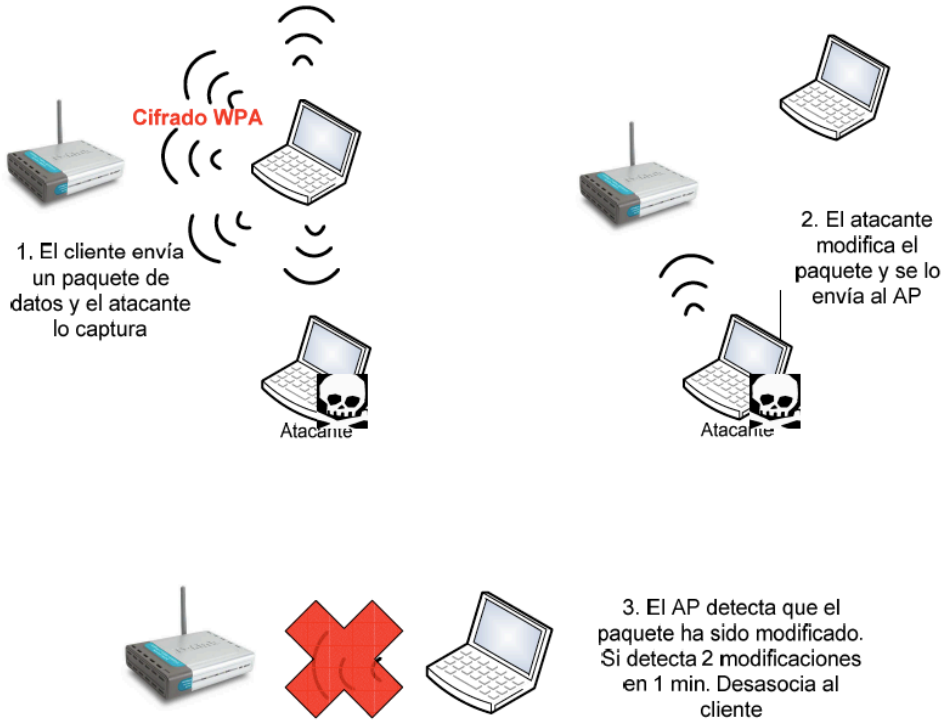

Figura 4.7. Ataque WPA – Modificación de paquetes

4.5.4. Desautenticación de Clientes

El ataque descrito anteriormente provocaba la desautenticación de todos los usuarios de la red por mensajes enviados por el AP. Por lo tanto, disponiendo de las direcciones MAC necesarias, la del AP y la de los clientes asociados, podremos falsificar y crear paquetes de Desauthentication como los que enviaba el AP para desautenticar a estaciones en concreto o, de la misma manera que el método anterior, a todos los clientes de la red, haciéndonos pasar por el AP.

Figura 4.8. Ataque Desautenticación de Clientes

4.6. Falsificación de Identidades

Los ataques que van a ser descritos a continuación se basan en el engaño y suplantación de identidades o dispositivos que pertenecen a la Red Wi-Fi objetivo. Las posibilidades serán hacer creer al AP que el atacante es un usuario legítimo o hacer creer a los clientes que el atacante es el AP al que se deben asociar.

4.6.1. Rogue Access Points – Honeypots

La existencia de Rogue Access Points, Puntos de Acceso Hostiles, son un tema difícil de solucionar en Seguridad Wi-Fi. Son conexiones que se establecen voluntaria o involuntariamente y, por su naturaleza son temporales.

El problema consiste en que hay que detectarlas en el momento, mientras está sucediendo.

Así como nosotros tenemos nuestros Puntos de Acceso, es muy probable, que vecinos o empresas próximas tengan los suyos. Esto supone una amenaza constante a nuestra red y a nuestros dispositivos Wi-Fi, que además es inevitable, pues no se puede prohibir a un vecino que instale su propia Red Wireless, por lo tanto, es un peligro con el que se debe convivir.

La definición de un Punto de Acceso Hostil es, por tanto, todo Punto de Acceso que no ha sido instalado y autorizado por el administrador de nuestra de red, existiendo, básicamente, 3 fuentes: vecinos, insiders (miembros de nuestra red, visitantes, etc.) y hackers.

Básicamente el objetivo del atacante que utiliza un Punto de Acceso Hostil es conseguir información sobre nuestra red, para posteriormente conseguir la información que circula en nuestro sistema. La forma de protegerse frente a este peligro es detectar y localizar los Puntos de Acceso que no pertenecen a nuestra red para, en primer lugar, prevenir. Si se detecta el Punto de Acceso es hostil deberemos tratar de eliminarlo si es posible, o si no es posible, bloquear el acceso a dicho AP por parte de los clientes de nuestra red.

Un problema más difícil de detectar es cuando se trata con un Punto de Acceso Honeypot. Este ataque consiste en utilizar un AP pirata con el mismo ESSID al que se conecta un cliente y una señal fuerte para conseguir que algún usuario se asocie enviando su login y/o contraseña, con la que posteriormente el atacante tendrá acceso a la red.

Una forma de utilizar los Honeypots es en redes donde se realiza roaming. De esta forma será más sencillo que un cliente que detecte una mejor calidad de señal se desasocie del Punto de Acceso legítimo y se asocie al falso.

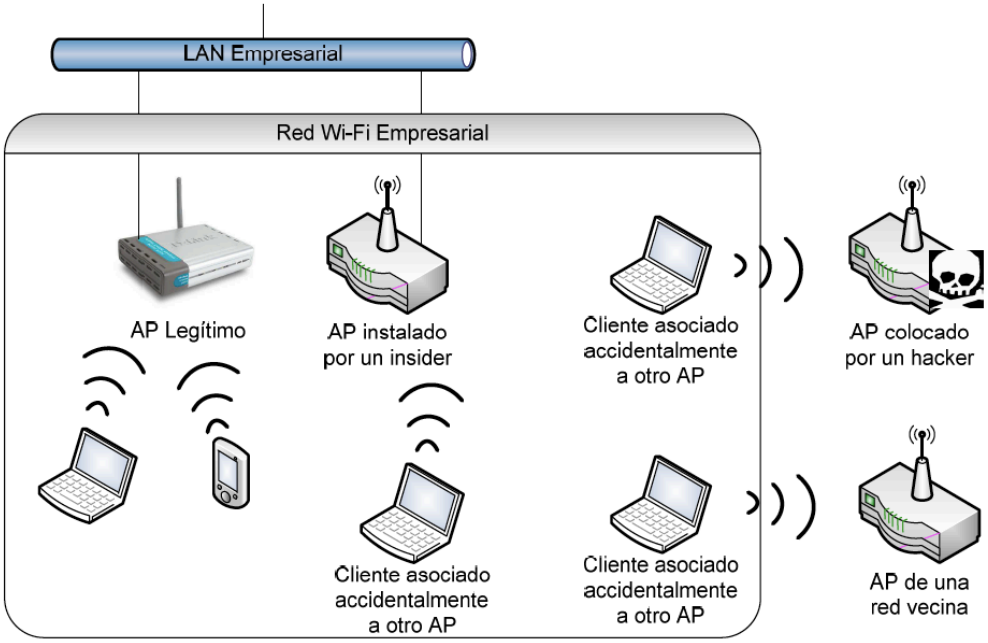

Figura 4.9. Ataque Rogue Access Points – Honeypots

4.6.2. Wi-Phishing

Los Hotspots, antes mencionados, son Puntos de Acceso Wi-Fi públicos, el principal problema de este tipo de APs es que suelen utilizar mecanismos de seguridad muy débiles, ya que los proveedores del servicio no tienen especial interés en proteger la información que circula en sus redes, habitualmente sólo se encuentra implementada seguridad a nivel de acceso. Por esto, es el usuario el que deberá velar por la seguridad de su información, algo que un usuario medio no sabrá como hacer.

Uno de los ataques más populares sobre este tipo de redes es el Wi-Phishing. Un usuario cuando desea conectarse a Internet desde un sitio público debe, en primer lugar, comprobar los Puntos de Acceso que le ofrecen conexión, algo fácil. Un atacante, utilizando ingeniería social, puede colocar un AP con un ESSID que transmita confianza a los posibles clientes víctima.

Una vez un usuario decide conectarse al AP, colocado por el atacante, toda la información que se transmita por la red podrá ser fácilmente comprometida. Muchos Puntos de Acceso

públicos poseen un menú de bienvenida, habitualmente este tipo de redes son utilizadas eventualmente por los usuarios, por lo que se suele desconocer cual debe ser el aspecto auténtico de este menú.

Antes de permitir la conexión puede que el atacante, mediante el menú, intente obtener algún tipo de información confidencial que sea facilitada por los usuarios más confiados, como contraseñas, números de identidad, cuentas bancarias, números de tarjetas de crédito, etc.

Todo lo dicho se refiere a la información que el atacante puede robar mientras permanece activa la conexión al Punto de Acceso, pero un atacante con más paciencia y que no desee bombardear al usuario con solicitudes de información confidencial, algo que podría hacerle desconfiar, puede introducir en la máquina del usuario malware de tipo virus, spyware, troyanos o keyloggers, con los que podría acabar obteniendo la misma información en momentos donde el usuario se sintiese más confiado.

Un tipo de ataque similar al Wi-Phishing, pero más ambicioso en cuanto a su alcance, es el Evil Twin. La metodología de acceso o engaño a la víctima es similar, pero se busca conseguir más datos. El Evil Twin, es en realidad, un ataque Man In The Middle que redirige al usuario a páginas web peligrosas, donde es atacado por malware. Existen páginas donde con tan sólo mover el ratón se descarga spyware.

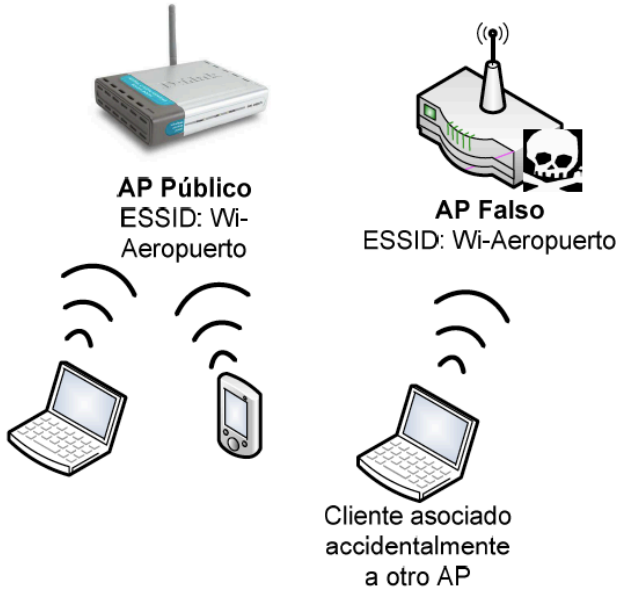

Figura 4.10. Ataque Wi-Phishing

4.6.3. MAC Address Spoofing

Este ataque se realizará cuando la red objetivo está protegida mediante un mecanismo de Filtrado de Direcciones MAC. Ya se comentó que éste era un método de seguridad poco efectivo, que autenticaba a dispositivos y no a usuarios.

Para realizar el ataque simplemente detectando alguna dirección MAC que se encuentra asociada al AP, ésta podrá ser utilizada suplantando a la MAC original de la Tarjeta de Red Wi-Fi del atacante. Dado que las direcciones MAC se envían en claro, el proceso de detección resultará muy sencillo, una vez se falsifique la dirección MAC, el AP permitirá el acceso a la red al atacante.

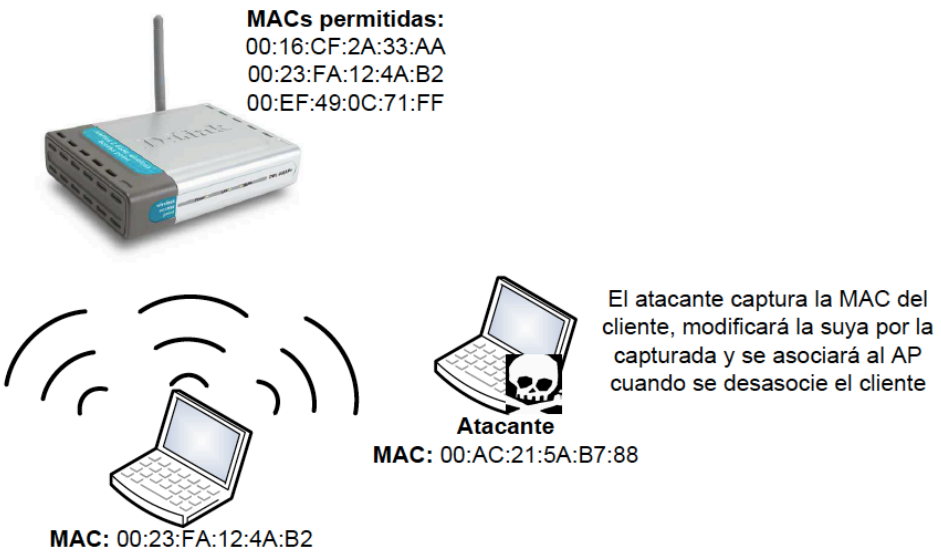

Figura 4.11. Ataque MAC Spoofing

4.6.4. MITM – Man In The Middle

El atacante con este método consigue ubicarse entre el AP y el dispositivo Wi-Fi cliente, de esta manera consigue controlar la comunicación entre el cliente y el AP. Realizando este tipo de ataque el hacker podrá modificar o alterar la información que se está transmitiendo a través suyo, con el fin de engañar al receptor, transmitir la información sin ningún cambio, de manera que nadie se de cuenta de su presencia y pueda conocer el contenido de la conversación, o bloquear la transmisión de manera que la información nunca llegue al receptor.

Para llevar a cabo este ataque, en primer lugar, se deberá localizar la red objetivo y conseguir información sobre la misma, tanto del Punto de Acceso como de los clientes. Además se necesitará un Punto de Acceso Wi-Fi que suplantará al AP original y una estación con una Tarjeta de Red Wi-Fi que suplantará al cliente objetivo. Existe software que emula Puntos de Acceso en un PC, lo que resultaría suficiente para realizar el ataque si se dispone de un tarjeta de red.

Una vez está todo dispuesto, el atacante deberá conseguir que el cliente objetivo se asocie a su Punto de Acceso pensando que es el auténtico y, además, asociarse al AP original con el cliente falso. Una vez conseguido esto, el atacante podrá participar en las actividades de la Red Wi-Fi pues ante el Punto de Acceso será un cliente legítimo.

Figura 4.12. Ataque Man in the middle

4.6.5. Session Hijacking

El ataque de Session Hijacking, "Secuestro de Sesión", esta basado en desautenticar a un usuario que está asociado a la red y reemplazarlo.

El modo de operación, como en todos los ataques, comienza detectando y seleccionado la red objetivo y monitorizándola para obtener información como ESSID, direcciones MAC, etc. A continuación se realiza un ataque de Denegación de Servicio contra el cliente seleccionado para ser suplantado, consiguiendo así que sea desautenticado.
Con la información que había obtenido, el atacante procede a conectarse a la red en reemplazo del usuario expulsado, suplantándolo. El usuario legítimo intentará conectarse, pero el AP no se lo permitirá, pues ya existirá un cliente con sus características conectado. Evidentemente este ataque se realizará cuando el Punto de Acceso utiliza mecanismos o listas de autenticación.

Una vez conectado, el atacante debe actuar rápidamente para evitar sospechas, pues el cliente al notar que no se puede conectar a la red notará que algo no va bien, pudiendo dejar un backdoor en el sistema de seguridad de la red para poder volver a acceder posteriormente. Una vez hecho esto el atacante se deberá retirar permitiendo al cliente volver a conectarse.

Si el tiempo que el atacante quiere dejar desconectado al usuario auténtico de la red no es suficiente para completar posteriores ataques, que requieren que esté asociado a la red, podrá repetir el proceso de suplantación sobre otros clientes evitando así sospechas.

Al ser un ataque que habitualmente dura muy poco tiempo, resulta muy complicado para el administrador de la red detectar el ataque, sobretodo si no se cuenta con herramientas específicas como los Switches WLAN.

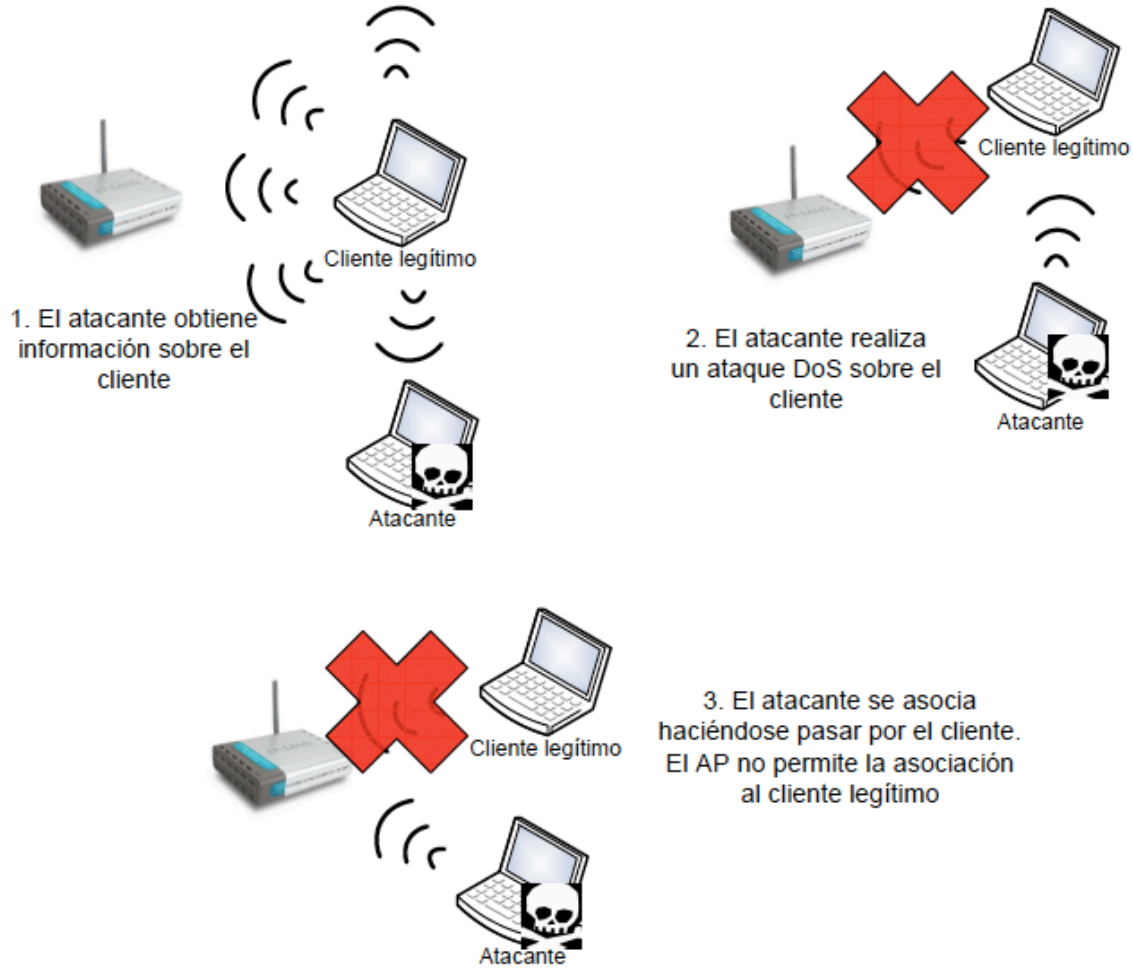

Figura 4.13 Ataque Session Hijacking

4.7. Ataques de Intrusión

Ataques que ya hemos visto como los de Falsificación de Identidades podrían también ser clasificados como Ataques de Intrusión, pero en esta categoría se describirán ataques, que como se verá, explotan otro tipo de vulnerabilidades.

4.7.1. Romper claves WEP

Ya se ha explicado, en las medidas de seguridad, el protocolo de cifrado WEP con sus principales características: su popularidad y su debilidad. Partiendo de que la seguridad de este protocolo puede romperse mediante un ataque de fuerza bruta, es decir, probando todas las combinaciones posibles hasta descubrir la clave, en este apartado se describirá un ataque mucho más rápido y efectivo.

Como ya se comentó WEP se basa en el cifrado RC4 para codificar la información con la clave de red. Esta clave suele estar formada por un total de 64 o 128 bits, siendo la parte fundamental el Vector de Inicialización, 24 bits semialeatorios, que son transmitidos en texto plano.

Una vez se ha seleccionado la red y el Punto de Acceso sobre el que se va a realizar el ataque, se debe capturar el tráfico que se transmite sobre dicha red. Debido a que el tráfico habitualmente es muy bajo, el atacante puede hacer que éste aumenté realizando otros ataques de manera conjunta, provocando desautenticaciones de los clientes y/o inyectando tráfico en la red que provoque la generación de nuevos IVs, como la inyección de peticiones ARP.

Una vez se ha capturado tráfico suficiente comienza el proceso de **"cracking"** de la contraseña utilizando la captura realizada, con lo que se obtendrá la clave WEP.

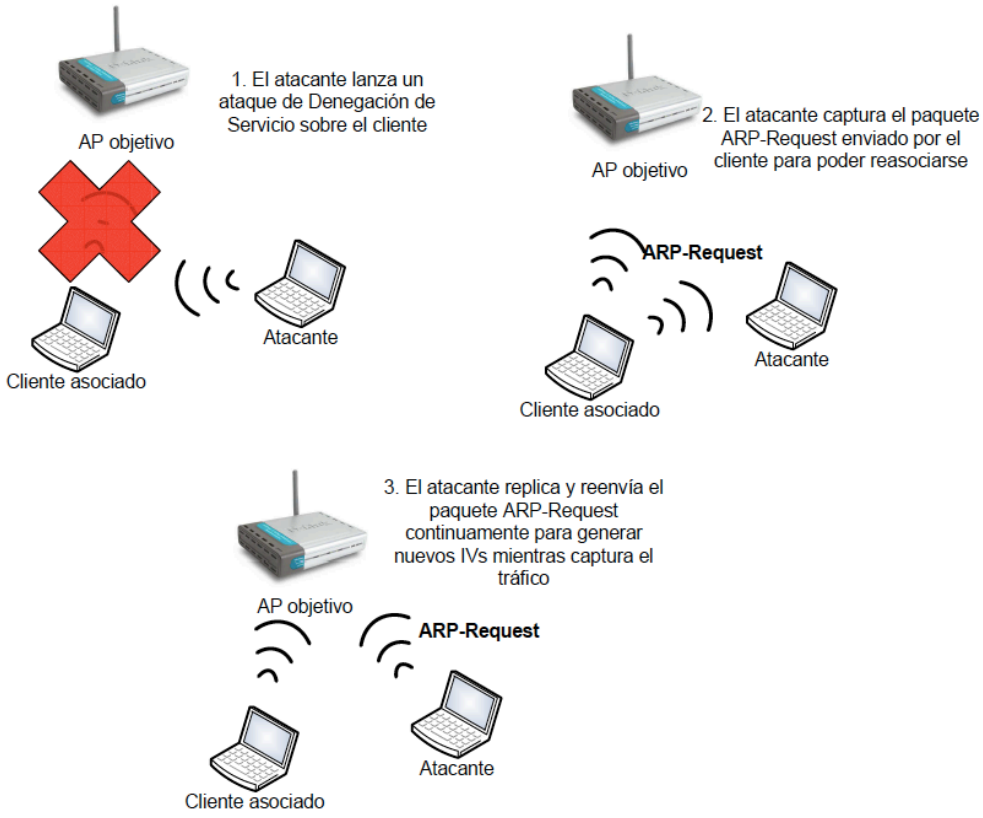

Figura 4.14 Ataque WEP utilizando reenvío de peticiones ARP

4.7.2. Romper claves WPA

Este tipo de ataques es muy semejante a los ataques para romper claves WEP, sin embargo las diferencias entre estos protocolos hace que la metodología de ataque sea un poco distinta.

Una de las principales diferencias a la hora de realizar este ataque es que no importa tanto la cantidad de tráfico capturado como ocurría en los ataques sobre claves WEP, lo realmente

importante es capturar un tipo de tráfico concreto generado en el momento de autenticación del cliente conocido como “handshake”.

Por lo tanto el comienzo del ataque será igual que en el caso anterior, seleccionando la red, capturando tráfico y realizando simplemente un ataque de Denegación de Servicio sobre un cliente, ya que con solamente un handshake será posible descifrar la clave. Adicionalmente será necesario disponer de un diccionario que compare sus valores con dicho paquete.

Debido a que la clave será descubierta sólo en función de que exista la misma en una entrada del diccionario, la elección y la calidad del mismo es fundamental para el éxito del ataque.

Figura 4.15 Ataque WPA

4.7.3. Ataque a Cisco EAP - LEAP

La vulnerabilidad sobre el método de autenticación EAP - LEAP desarrollado por Cisco y la metodología para lanzar un ataque off-line fueron presentadas en 2003.

Todo algoritmo basado en claves o contraseñas puede ser atacado con la finalidad de descubrir la contraseña de acceso. En este caso se realiza un ataque de diccionario, es decir, utilizando un listado de palabras clave.

Existen herramientas que automatizan y facilitan la realización de ataques de diccionario sobre Redes Wi-Fi protegidas con el método de autenticación EAP-LEAP. Como este ataque puede ser realizado off-line, es posible capturar una cantidad de tráfico determinada y luego atacarla hasta descubrir la contraseña.

Explotando APs mal configurados

El encontrarse con un Punto de Acceso mal configurado es algo habitual, esto facilita enormemente la tarea de intrusión en una Red Wi-Fi.

Todos los APs poseen características predeterminadas con las que salen configurados de fábrica. En algunos casos se protegen con contraseña y otros directamente no poseen ninguna, lo mismo ocurre con el ESSID. Estos datos son conocidos por muchísimas personas, pueden ser consultados en Internet, y deben ser cambiados en el momento de la instalación.

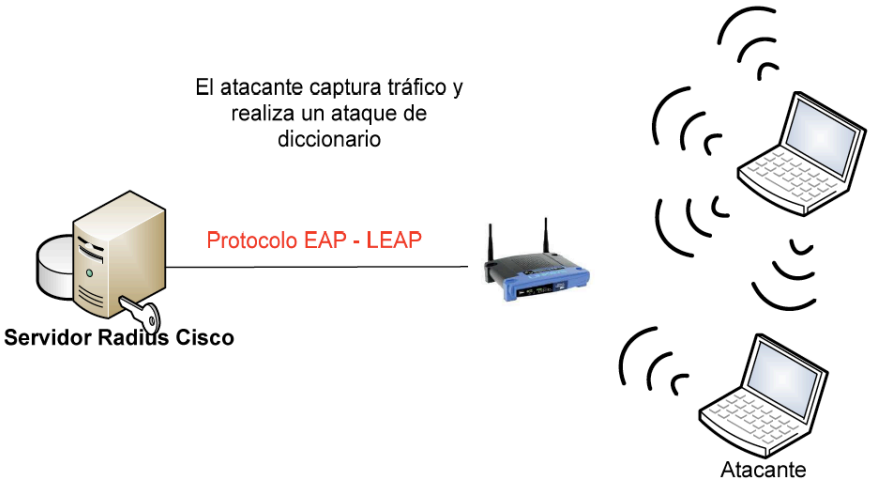

Figura 4.16 Ataque EAP - LEAP

5

5. Software Intrusión, Politicas de Seguridad.

5.1. Software Intrusión

Existen múltiples herramientas en el mercado para detectar y analizar redes Wi-Fi, tanto de uso comercial o gratuito, y que se pueden utilizar en una gran variedad de plataformas, Windows, Mac, Linux, iOS, Android, etc…, lo que pone de manifiesto el interés creciente en la seguridad de este tipo de redes. A continuación se mostrará un amplio listado de ellas, sin menoscabo que puedas encontrarse otras que realicen las mismas funciones.

Se han clasificado por distintas categorías, hay que tener en cuenta que muchas de las siguientes herramientas utilizadas en la intrusión de redes Wireless 802.11 (Wi-Fi) podrían ser incluidas en varias categorías. Sin embargo, cada herramienta aparece en la lista una sola vez, en virtud de su categoría principal. Por ejemplo, si lo que se quiere hacer es encontrar puntos de acceso, se debe elegir una herramienta de descubrimiento. Si se quiere encontrar puntos de acceso y analizar los paquetes capturados Wi-Fi, se elije un analizador de tráfico Wi-Fi. Si lo que se quiere es encontrar puntos de acceso y monitorizar el tráfico Wi-Fi observado por una red de AP, se elija un WIPS.

Wi-Fi AP Discovery Tools		
Nombre	Sistema Operativo	Web
AiroCrack-ng	Linux, Windows	www.aircrack-ng.org
AirGrab WiFi Radar	Windows	www.airgrab.com
AirMobile Agent	Windows, WinCE	www.airmobile.se
AirRadar	MacOS	www.koingosw.com
AP Radar	Linux	sourceforge.net/projects/apradar/
Farproc Wifi Analyzer	Android	es.androidzoom.com/android_applications/tools/wifi-analyzer_bgn.html
Fluke AirCheck Wi-Fi Tester	Hardware	www.flukenetworks.com
iStumbler	MacOS	www.istumbler.net
Kismac-ng	MacOS	trac.kismac-ng.org
Meraki Cloud Stumbler	Navegador Web, Android	www.meraki.com/products/wireless/wifi-stumbler
MetaGeek InSSIDer	Windows	www.metageek.net
MiniStumbler	WinCE	www.stumbler.net
NetStumbler	Windows	www.stumbler.net
PassMark WirelessMon	Windows	www.passmark.com/products/wirelessmonitor.htm
ViStumbler	Windows	www.vistumbler.net
Sandy Roads WiFiHopper	Windows	www.wifihopper.com
WaveStumbler	Linux	www.cqure.net/wp/wavestumbler/
WeFi	Windows, WinCE, Android, Symbian	www.wefi.com
WiFiFoFum	WinCE, iOS, Android	www.aspecto-software.com/rw/applications/wififofum/
WiFinder	Android	www.pgmsoft.com/apps/wifinder_for_android/
WiFi Scanner	MacOS	wlanbook.com/mac-os-x-wifi-scanner-snow-leopard/
Xirrus Wi-Fi Inspector	Windows	www.xirrus.com/Products/Wi-Fi-Inspector

Tabla 5.1. Herramientas de Descubrimiento de AP WiFi

Wi-Fi Raw Packet Capture Tools	
Nombre	Web
Aircrack-ng Suite	www.aircrack-ng.org
CACE AirPcap	support.riverbed.com/software/wireshark.htm
ettercap	ettercap.sourceforge.net
libpcap	www.winpcap.org
Pirni Sniffer	code.google.com/p/n1mda-dev/wiki/PirniUsageGuide
Prism2Dump	www.seattlewireless.net/index.cgi/Prism2Dump
tcpdump	www.tcpdump.org/

Tabla 5.2. Herramientas de Capturas de Paquetes Wi-Fi

Wi-Fi Traffic Analyzers	
Nombre	Web
AirMagnet WiFi Analyzer	www.flukenetworks.com
BVS YellowJacket-BAG	www.bvsystems.com/Products/WLAN/YJ-BAG/YJ-BAG.htm
CACE WiFi Pilot	www.riverbed.com/us/products/cascade/cascade_pilot.php
Cambridge vxSniffer	www.cambridgevx.com/vxsniffer.html
Fluke Networks OptiView and EtherScope	www.flukenetworks.com
Javvin Network Packet Analyzer	www.javvin.com/packet.html
Kismet	www.kismetwireless.net
MetaGeek Eye P.A.	www.metageek.net/products/eye-pa/
Motorola AirDefense Mobile	www.airdefense.net/products/admobile/index.php
NetScout Sniffer Portable	www.netscout.com
Network Instruments Network Observer	www.networkinstruments.com
TamoSoft CommView for Wi-Fi	www.tamos.com/products/commwifi/
Ufasoft Snif	ufasoft.com/sniffer/
WildPackets OmniPeek	www.wildpackets.com/products/omnipeek_network_analyzer
WireShark (formerly Ethereal)	www.wireshark.org

Tabla 5.3. Analizadores de Tráfico Wi-Fi

VoWiFi Traffic and QoS Analyzers	
Nombre	Web
AirMagnet VoFi Analyzer	www.flukenetworks.com
VeriWave VoIP QoS Service Assurance Test	www.ixiacom.com/ixveriwave/index.php
WildPackets OmniPeek Enhanced Voice Option	www.wildpackets.com/products/omnipeek_network_analyzer/voip_monitoring

Tabla 5.4. Analizadores de Voz y Calidad de Servicio sobre Wi-Fi

Wi-Fi Intrusion Detection and Prevention Systems	
Nombre	Web
AirMagnet Enterprise	www.flukenetworks.com
AirMobile Server	www.airmobile.se
AirPatrol WLS	www.airpatrolcorp.com/products/wls_manager.php
AirTight Networks SpectraGuard Enterprise and Online	www.airtightnetworks.com/home/products/spectraguard-enterprise.html
Aruba Networks RFProtect	www.arubanetworks.com/products/arubaos/rfprotect-wireless-intrusion-protection
Enterasys HiPath Wireless Management Suite	www.enterasys.com/products/wireless.aspx
HP ProCurve RF Manager	www.hp.com
Cisco Adaptive WIPS	www.cisco.com/en/US/products/ps9817/index.html
Motorola AirDefense Enterprise	www.airdefense.net/products/servicesplatform/index.php

Tabla 5.5. Sistemas de Prevención y Detención de Intrusos Wi-Fi

Wi-Fi Predictive Planning Tools	
Nombre	Web
Aerohive Online Wi-Fi Planner	www.aerohive.com/planner
AirMagnet Planner	www.flukenetworks.com
AirTight Networks SpectraGuard Planner	www.airtightnetworks.com
Cisco Wireless Control System Planning Tool	www.cisco.com/en/US/products/ps6305/index.html
Connect802 Suite Spot Predictive Site Survey	www.connect802.com/suite_spot.htm
Ekahau Wireless Site Survey Professional	www.ekahau.com/products/ekahau-site-survey/overview.html
Motorla LAN Planner	www.motorola.com
Psiber RF3D WifiPlanner	www.psiber.com/rf3d/rf3d.html
Ruckus Wireless ZonePlanner	www.ruckuswireless.com/products/zoneplanner

Tabla 5.6. Herramientas de Planificación Predictiva Wi-Fi

Wi-Fi Site Survey Heatmapping Tools	
Nombre	Web
AirMagnet Survey	www.flukenetworks.com
BVS Hive	www.bvsystems.com/Products/Software/Hive/hive.htm
Ekahau Heatmapper	www.ekahau.com
Ekahau Wireless Site Survey Standard	www.ekahau.com
Helium Networks Wireless Recon	www.heliumnetworks.com
Meraki Cloud WiFi Mapper	www.meraki.com/products/wireless/wifi-mapper
Motorola SiteScanner	www.motorola.com
NetSpot for Mac OS X	www.netspotapp.com
TamoGraph Site Survey	www.tamos.com/products/wifi-site-survey/
VeriWave WaveDeploy	www.ixiacom.com/wavedeploy/index.php
VisiWave Site Survey	www.visiwave.com
WolfWiFiPro	www.wolfwifi.com

Tabla 5.7. Herramientas de Mapeo de Cobertura

Mobile Wi-Fi Spectrum Analyzers	
Nombre	Web
AirMagnet Spectrum Analyzer and AirMedic	www.flukenetworks.com
Aruba Networks RFProtect Spectrum Analyzer	www.arubanetworks.com
AirSleuth and WifiSleuth Spectrum Analyzers	nutsaboutnets.com/airsleuth-spectrum-analyzer/
BVS BumbleBee	www.bvsystems.com/Products/Spectrum/spectrum.htm
Cisco (Cognio) Spectrum Expert and CleanAir Technology	/www.cisco.com/en/US/products/ps9393/index.html
Meru Networks Spectrum Manager	www.merunetworks.com/products/index.html
Oscium WiPry-Spectrum	www.oscium.com/products/wipry-spectrum-spectrum-analyzer
MetaGeek Wi-Spy and Chanalyzer	www.metageek.net/products/wi-spy/

Tabla 5.8. Analizadores de Espectro Wi-Fi

Wi-Fi Endpoint Security Clients	
Nombre	Web
AirPatrol Wireless Policy Manager	www.airpatrolcorp.com/products/policy-manager.php
AirTight SpectraGuard SAFE	www.airtightnetworks.com/home/products/spectraguard-safe.html
Motorola AirDefense Personal	www.motorola.com
ZENworks Endpoint Security	www.novell.com/products/zenworks/endpointsecuritymanagement/

Tabla 5.9. Herramientas de Seguridad en Clientes Wi-Fi

Wi-Fi Vulnerability Scanners and Assessment Toolkits	
Nombre	Web
Airpwn	airpwn.sourceforge.net/Airpwn.html
AP Hopper	linux.softpedia.com/progDownload/AP-Hopper-Download-32710.html
Autoscan	Autoscan-network.com
BackTrack – Penetration Testing Distribution	www.backtrack-linux.org
FastTrack	www.thepentest.com
Immunity SILICA	www.immunityinc.com/products-silica.shtml
Karma	theta44.org/karma/
Motorola AirDefense Wireless VA Module	www.airdefense.net/products/servicesplatform/securitycompliance/wva.php
MDK3	homepages.tu-darmstadt.de/~p_larbig/wlan/
Network Security Toolkit	networksecuritytoolkit.org/nst/index.html
Nmap, Zenmap	nmap.org
Nessus	www.nessus.org/products/nessus
Organizational Systems Wireless Auditor (OSWA) Assistant	securitystartshere.org/page-training-oswa-assistant.htm
Security Auditor's Research Assistant	www-arc.com/sara/
WiCrawl	midnightresearch.com/projects/wicrawl/
WiFiDEnum	community.arubanetworks.co
WiFi-Owl AP Security Audit Tool	www.wifi-owl.com
WiFi Scanner	www.jeffpang.net/research.shtml
WiFiZoo	ommunity.corest.com/~hochoa/wifizoo/index.html

Tabla 5.10. Escáneres de Vulnerabilidad y Herramientas de Evaluación Wi-Fi

5.1.1. Distribuciones Live CD

En la actualidad se pueden encontrar además un conjunto de distribuciones denominadas Live CD de descarga gratuita. Una distribución live o Live CD o Live DVD, es un sistema operativo almacenado en un medio extraíble, tradicionalmente un CD o un DVD, de ahí sus nombres, que puede ejecutarse desde éste sin necesidad de instalarlo en el disco duro de un ordenador para lo cual usa la memoria RAM como disco duro virtual y el propio medio como sistema de archivos.

La mayoría usa un sistema operativo basado en el núcleo Linux. Para usar un Live CD es necesario obtener uno (muchos de ellos distribuyen libremente una imagen ISO que puede bajarse de Internet. Normalmente, un Live CD viene acompañado de un conjunto de aplicaciones, en nuestro caso herramientas útiles para la detección y análisis de redes Wireless

Hay que destacar tres distribuciones Live CD especialmente diseñada para la auditoria de redes Wireless, WiFiSlax, Backtrack y Wifiway.

WiFiSlax es una distribución GNU/Linux con funcionalidades de Live CD o Live USB pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general.

WiFiSlax incluye una larga lista de herramientas de seguridad y auditoría listas para ser utilizadas, entre las que destacan numerosos scanners de puertos y vulnerabilidades, herramientas para creación y diseño de exploits, sniffers, herramientas de análisis forense y herramientas para la auditoría Wireless, además de añadir una serie de útiles lanzadores.

Se puede descargar desde la web: www.wifislax.com

Figura 5.1. Distribución WiFiSlax

Backtrack es la distribución Live CD más antigua de las tres, especialmente diseñada para la auditoría de seguridad de redes, pero que en las últimas versiones incorpora múltiples herramientas para la auditroría de redes Wireless. Actualmente tiene una gran popularidad y aceptación en la comunidad que se mueve en torno a la seguridad informática

Backtrack se deriva de la unión de dos grandes distribuciones orientadas a la seguridad, el Auditor + WHAX. Incluye una larga lista de herramientas de seguridad listas para usar, entre las que destacan numerosos scanners de puertos y vulnerabilidades, sniffers, herramientas de análisis forense y herramientas para la auditoría Wireless.

Backtrack le ofrece al usuario una extensa colección de herramientas completamente usables desde un Live CD por lo que no requiere una instalación para poder usarse. O bien, se ofrece la opción de instalar en un disco duro. Entre las herramientas ofrecidas se encuentran:

- Aircrack-ng, Herramientas para auditoría inalámbrica
- Kismet, Sniffer inalámbrico
- Wireshark, Analizador de protocolos
- Medusa, herramienta para Ataque de fuerza bruta
- Nmap, rastreador de puertos
- Análisis de redes de radio (Wifi, Bluetooth, RFID)

Se puede descargar desde la web: www.backtrack-linux.org

Figura 5.2. Distribución BackTrack

Wifiway es una distribución GNU/Linux pensada y diseñada para la auditoría de seguridad de las redes WiFi, Bluetooth y RFID. Se publican imágenes iso con funcionalidades de LiveCD y LiveUSB

Incluye una larga lista de herramientas de seguridad y auditoría inalámbrica listas para ser utilizadas, especializadas en la auditoría Wireless, además de añadir una serie de útiles lanzadores.

Aunque está influida por inicio de varios desarrollos, algunos muy populares como es el caso de WiFiSlax, 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.

Se puede descargar desde la web: www.wifiway.org

Figura 5.3. Distribución WiFiWay

5.1.2. Aircrack

Aircrack es una suite de herramientas para descifrar claves WEP y WPA de redes Wireless 802.11a/b/g. Aircrack pone en práctica los mejores algoritmos conocidos de craqueo para recuperar las claves inalámbricas, una vez que un número de paquetes encriptados han sido capturados. La suite cuenta con más de una docena de herramientas, incluyendo airodump (un programa de captura de paquetes de 802,11), aireplay (un programa para inyectar paquetes 802.11), aircrack (cracking estática WEP y WPA-PSK), y airdecap (descifra claves WEP / WPA).

Se puede descargar desde la web: www.aircrack.es
Sistemas Operativos Soportados: Windows, Linux

5.1.3. Kismet

Kismet es una consola, detector de redes inalámbrica basado en la capa 2 de 802.11, sniffer, y sistema de detección de intrusiones. Identifica las redes por inhalación pasiva (a diferencia de las herramientas más activas, tales como NetStumbler). Se puede detectar automáticamente los bloques de la red IP por la inhalación de TCP, UDP, ARP, y paquetes DHCP, el tráfico de registro en formato compatible con Wireshark / tcpdump, e incluso dibujar las redes detectadas y rangos estimados en los mapas descargados. Como era de esperar, esta herramienta se utiliza comúnmente para wardriving.

Se puede descargar desde la web: www.kismetwireless.net
Sistemas Operativos Soportados: Linux

5.1.4. NetStumbler

Netstumbler es la herramienta más conocida de Windows para encontrar puntos de acceso inalámbricos abiertos, Wardriving. También distribuyen una versión para WinCE para PDAs y llamada Ministumbler. La herramienta es actualmente gratis pero sólo para Windows y no se proporciona el código fuente. Utiliza un enfoque más activo para la búsqueda de claves de WAP que sniffers pasivos como Kismet o KisMAC.

Se puede descargar desde la web: www.netstumbler.com
Sistemas Operativos Soportados: Windows, WindowsCE

5.1.5. inSSIDer

inSSIDer es un escáner de redes inalámbricas sólo para Windows . Fue diseñado para superar las limitaciones de NetStumbler, es decir, no funciona bien en Windows de 64 bits y Windows Vista. inSSIDer puede encontrar puntos de acceso inalámbricos abiertos, realizar un seguimiento de intensidad de la señal a través del tiempo, y guardar los registros con los registros del GPS.

Se puede descargar desde la web: www.metageek.net
Sistemas Operativos Soportados: Windows

5.1.6. KisMAC

Esta herramienta inalámbrica es una de la más populares para Mac OS X, ofrece muchas de las características de Kismet. A diferencia de la consola basada en Kismet, KisMAC ofrece una interfaz gráfica bastante práctica. También ofrece la importación de cartografía, en formato pcap, e incluso algunos de métodos de descifrado y ataques de autenticación.

Se puede descargar desde la web: kismac-ng.org
Sistemas Operativos Soportados: MacOS

5.2. Casos Prácticos de Ataques Wi-Fi

5.2.1. Ataque WEP en BackTrack 5

BackTrack es una distribución GNU/Linux en formato Live CD pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general. Actualmente tiene una gran popularidad y aceptación en la comunidad que se mueve en torno a la seguridad informática.

Incluye una larga lista de herramientas de seguridad listas para usar, entre las que destacan numerosos scanners de puertos y vulnerabilidades, archivos de exploits, sniffers, herramientas de análisis forense y herramientas para la auditoría Wireless.

Backtrack le ofrece al usuario una extensa colección de herramientas completamente usables desde un Live CD o un Live USB por lo que no requiere una instalación para poder usarse. O bien, se ofrece la opción de instalar en un disco duro. Entre las herramientas ofrecidas se encuentran:

- Aircrack-ng, Herramientas para auditoría inalámbrica
- Kismet, Sniffer inalámbrico
- Ettercap, Interceptor/Sniffer/Registrador para LAN
- Wireshark, Analizador de protocolos
- Medusa, herramienta para Ataque de fuerza bruta
- Nmap, rastreador de puertos

Backtrack se puede descargar desde la web: www.backtrack-linux.org

Para descifrar la clave WEP, primero que todo debemos tener una tarjeta de red inalámbrica cuyo chip soporte el modo de monitoreo. Teniendo dicho dispositivo funcional, procedemos a continuar con el proceso. Para empezar abrimos una consola y verificamos que el sistema detecte nuestra interfaz de red inalámbrica, esto lo hacemos con el siguiente comando:

 # iwconfig

El sistema reconoce la interfaz de red, y ahora hay que ponerla en modo monitor, para ello ejecutamos en la misma consola el siguiente comando:

 # airmon-ng start wlan0

Como podemos ver en la figura , se inicia la interfaz en modo monitor y la denomina como “mon0”. En ocasiones la interfaz de monitoreo puede variar dependiendo de cuantas veces se inicialize (mon0, mon1, mon2, etc.)

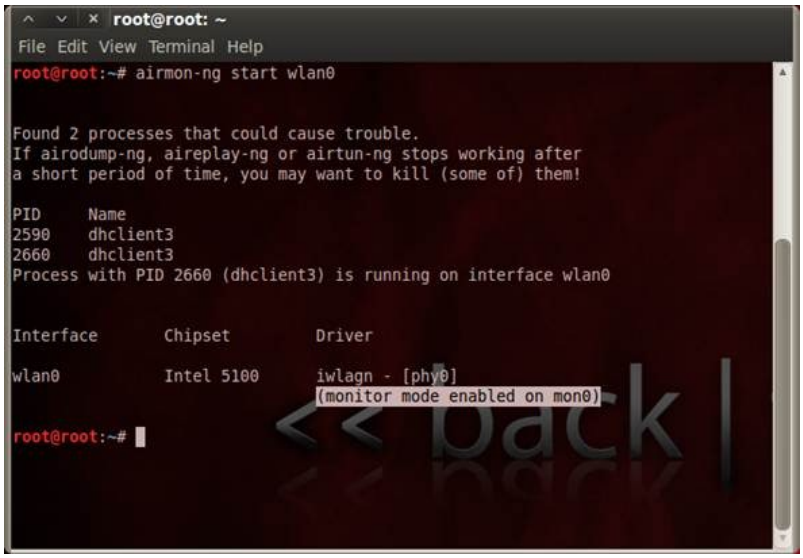

Figura 5.4. Interfaz en Modo Monitor

Seguidamente se realiza el escaneo de las redes activas a nuestro alrededor, para ello se usa la herramienta airodump-ng incluida en el BackTrack con el siguiente comando:

 # airodump-ng mon0

Identificamos la red que va a ser atacada, con el fin de encontrar su clave con cifrado WEP para poder acceder al Access Point. Para el ataque hay que tener en cuenta la siguiente información:

- **BSSID:** Es la dirección MAC del AP.
- **POWER (PWR):** Es la potencia o que tan cerca está el AP, para poder realizar este procedimiento la distancia del AP debe ser razonable, ya que de ello depende que este sea efectivo o no. Se recomienda estar a una potencia no menor a -70.
- **CANAL (CH):** Es la frecuencia que está utilizando el AP para emitir su espectro.
- **ENC y CIPHER:** El tipo de encriptado.
- **ESSID:** Identifica el nombre de la red.

En la siguiente figura se puede observar la información mencionada.

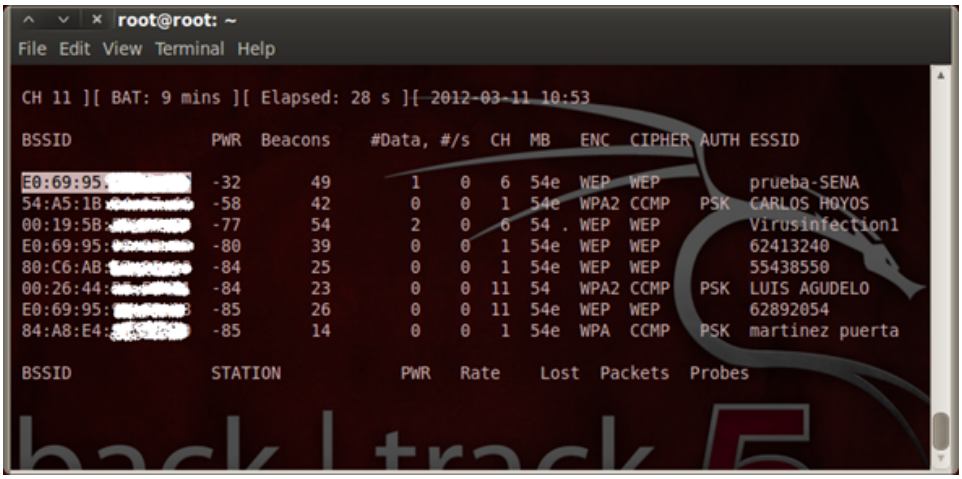

Figura 5.5. Identificación de la red a atacar

Se captura todo el tráfico del AP y se guarda en un archivo para que posteriormente sea analizado con la Suite aircrack.

Con el siguiente comando se captura y se almacena todo el tráfico del AP.

 # airodump-ng –c (canal) –w (Nombre de archivo a guardar) –bssid (MAC del AP) mon0

De haber un cliente conectado al AP, esta captura muestra su dirección MAC la cual se puede utilizar para realizar otra prueba de vulnerabilidades relacionado con el filtrado por MAC en redes inalámbricas. Capturado todo el tráfico, se inyecta paquetes para acelerar el proceso. Los paquetes que necesitamos son los que son conocidos como “IVs”.

Ahora para lograr acelerar este procedimiento, ejecutamos un comando con la finalidad de realizar una falsa autenticación con el AP. El comando que ejecutamos es:

 # aireplay-ng -1 0 –a (MAC del AP) mon0

A continuación se inyecta paquetes con el siguiente comando:

 # aireplay-ng -2 –p 0841 –c (Broadcast) –b (MAC del AP) mon0

Obteniendo la cantidad mínima para descifrar la clave (5000 IVs), podemos utilizar aircrack para desencriptar la clave WEP. En otra consola ejecutamos el siguiente comando:

 # aircrack-ng –n (bits de encriptación 64,128) –b (MAC del AP) archivoguardado-01.cap

Figura 5.6. Análisis archivo capturado

Con esto comando aircrack se comienza a analizar el archivo en el que con anterioridad se ha comenzado a almacenar todo el tráfico capturado. En apenas unos minutos e incluso en segundos se descifra la clave WEP, tal y como se muestra la figura siguiente podemos ver que nos da la clave: KEY FOUND! [98:48:DE:DA:9B].

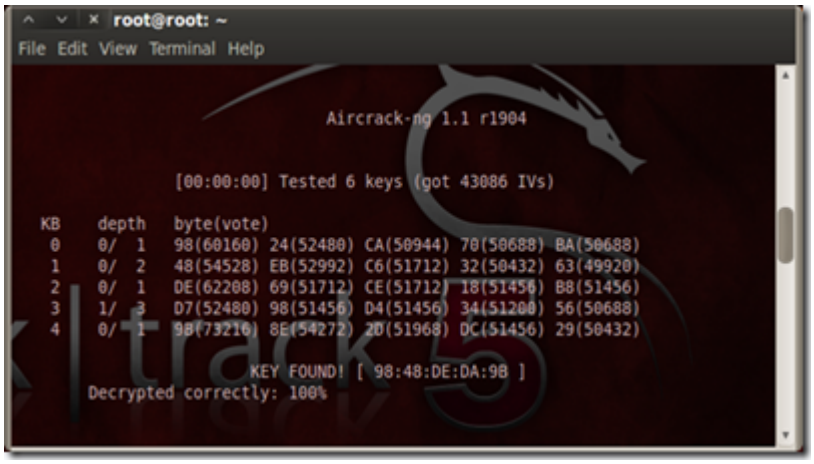

Figura 5.7. Resultado Ataque WEP

Debemos tener en cuenta que para esta prueba utilizamos un cifrado de 64 Bits, si el cifrado fuera de 128 Bits seguro tomaría más tiempo en obtener la clave.

5.2.2. Ataque WPA con Aircrack-Ng

En esta sención vamos a mostrar la inseguridad de las redes WPA, y para ello utilizare la suite Aircrack-ng. Para empezar mostramos el entorno en el que trabajaremos:

- MAC del router (BSSID): aa:bb:cc:dd:ee:ff
- MAC de un cliente asociado al AP: 11:22:33:44:55:66
- Nombre de la red (ESSID): vodafoneF7EF
- Canal del AP: 12
- Sistema operativo utilizado: GNU/Linux(Wifislax 3.1)
- Chipset de la tarjeta(atacante): rt2571f
- Nombre de la interfaz de red: rausb0

Asumiendo que la tarjeta está en modo monitor y que se ha tomado las precauciones de cambiar la MAC, se ha de realizar los siguientes pasos:

1. En primer lugar hay que buscar un AP objetivo con airodump-ng, para ello abrimos una shell y escribimos:

#airodump-ng -w morsa --bssid aa:bb:cc:dd:ee:ff -c12 rausb0

donde:

- airodump-ng: programa para escanear redes wi-fi.
- -w morsa: con -w elegimos el nombre del archivo de captura, en este caso, morsa.
- --bssid aa:bb:cc:dd:ee:ff: en --bssid ponemos la MAC del AP, en este caso, aa:bb:cc:dd:ee:ff.
- -c12: con -c seleccionamos el canal por el que opera el AP, en este caso 12.
- rausb0: nombre con el que wifislax reconoce a la tarjeta de red, en este caso, rausb0.

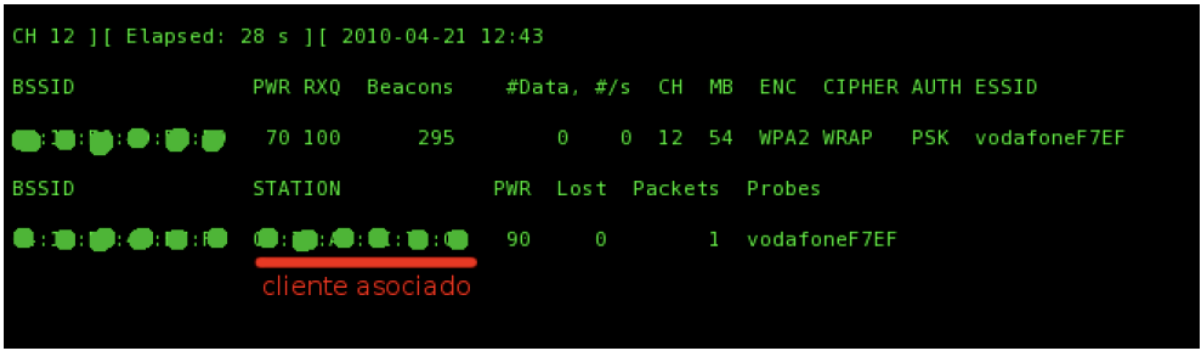

Figura 5.8. Escaneo de AP

2. El siguiente paso es obtener el handshake, para ello o bien esperamos a que un cliente se conecte, o bien desasociamos a un cliente ya conectado al AP, con lo que le forzaremos a volver a conectarse y obtendremos el buscado handshake. Como no queremos esperar, vamos a desasociar a alguien conectado a la red, para hacerlo abrimos una terminal y tecleamos el siguiente comando:

 # aireplay-ng -0 20 -a aa:bb:cc:dd:ee:ff -c 11:22:33:44:55:66 rausb0

donde:

- aireplay-ng: Esta aplicación la utilizaremos para realizar el ataque 0 con el que desasociamos a un cliente asociado al AP víctima.
- -0: Esto implica que utilizamos el ataque 0 con el fin de desconectar a un usuario de el AP objetivo.
- 20: El número de paquetes que mandaremos a la tarjeta asociada con el fin de conseguir que se caiga de la red, en este caso 20, si ponemos 0 no pararán de lanzarse paquetes hasta que nosotros interrumpamos la ejecución del programa (CTRL + C en la shell o cerrando el terminal).
- -a aa:bb:cc:dd:ee:ff: Con -a seleccionamos la MAC del AP objetivo.

• -c 11:22:33:44:55:66: Con -c seleccionamos la MAC de un cliente asociado al AP al que enviaremos los paquetes con el fin de conseguir que se reconecte al AP y obtener el handshake.
• rausb0: nombre con el que wifislax reconoce a la tarjeta de red, en este caso, rausb0.

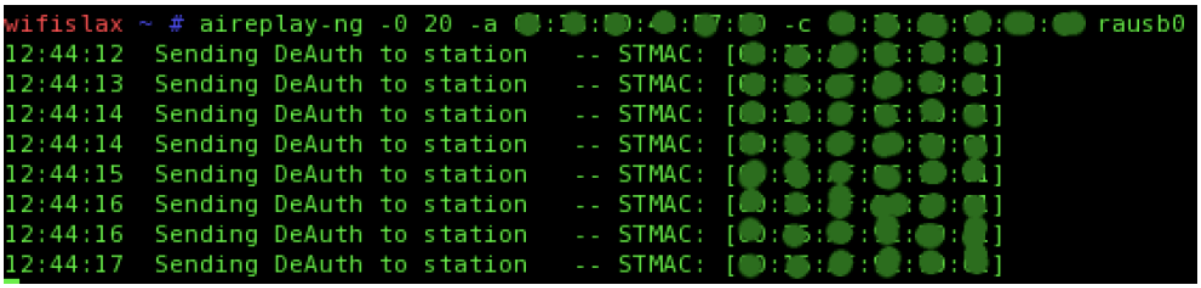

Figura 5.9. Ataque WPA

3 – Una vez el cliente se caiga y se vuelva a conectar, si hemos obtenido el handshake aparecerá en la parte superior derecha de la ventana del airodump-ng:

Figura 5.10. Obtenemos Handshake

Como vemos en la figura anterior pone WPA handshake junto con la MAC del AP, WPA handshake: aa:bb:cc:dd:ee:ff

Para comprobar si hemos obtenido o no el handshake, podemos poner en una shell:

 # aircrack-ng morsa-01.cap
donde:
• aircrack-ng: Programa que utilizaremos para obtener la contrase.a.
• morsa-01.cap: El archivo donde hemos guardado la captura de datos.

Entonces si hemos obtenido un handshake valido aparecerá:

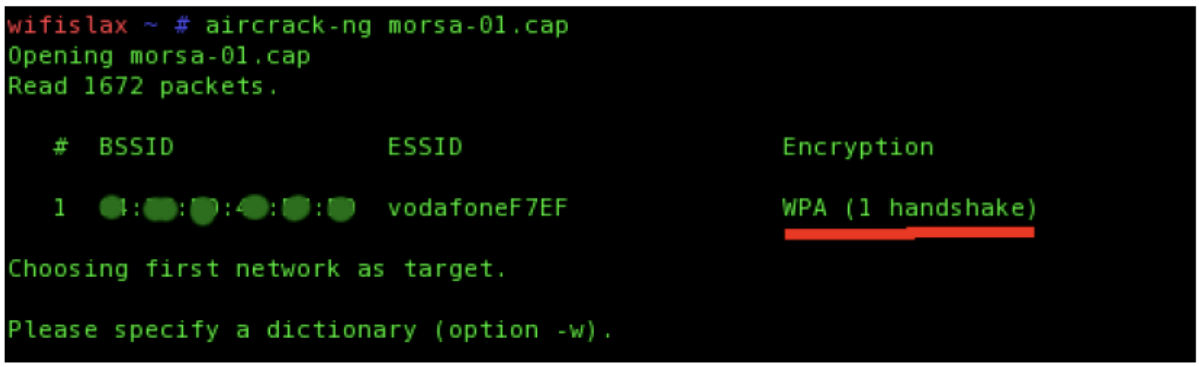

Figura 5.11. Handshake Válido

4. Utilizamos un diccionario amplio, para que la clave del AP este en nuestro diccionario. Usamos el diccionario que Ubuntu trae por defecto, en otras distribuciones también se encuentra, para encontrarlo en Ubuntu hay que ir a ***/etc/dictionaries-common*** y dentro de esta carpeta encontraremos un archivo llamado words.

Una vez escogido el diccionario solo queda lanzar el ataque. Este ataque durará mas o menos en función del tamaño del diccionario.

 # aircrack-ng -w /root/Desktop/words morsa-01.cap

donde:

- aircrack-ng: Programa que utilizaremos para obtener la contraseña.
- -w /root/Desktop/words: Con -w seleccionamos el diccionario que utilizaremos, en el directorio /root/Desktop y se llama words.
- morsa-01.cap: El archivo donde hemos guardado la captura de datos.

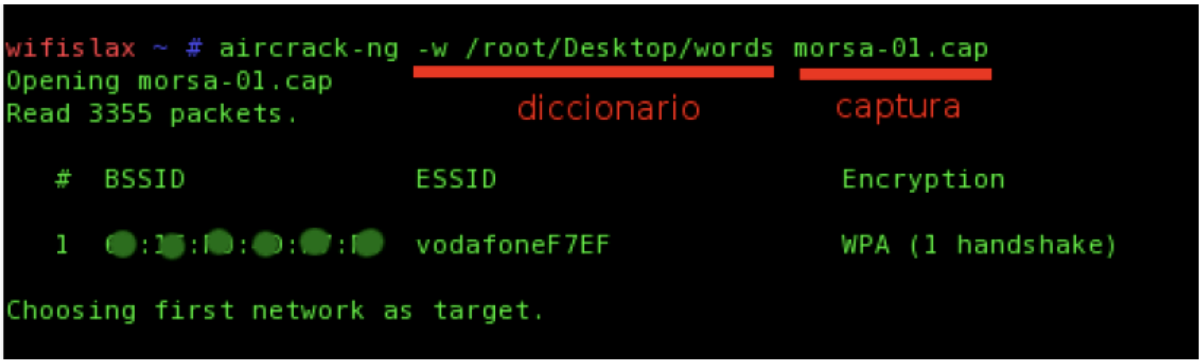

Figura 5.12. Lanzamiento del ataque con diccionario

Una vez iniciado el proceso de crackeo de la contraseña solo nos queda esperar que la contraseña del AP se encuentre en nuestro diccionario como se ha mencionado anteriormente.

Figura 5.13. Resultado Ataque WPA

Finaliza el proceso encontrando la clave WPA, en este caso la clave era JEUKCJRKHCBNQY y tardó un par de minutos en encontrarla.

5.3. Políticas de Seguridad

A continuación se listan una serie de medidas de seguridad que se consideran básicas para poder mantener los dispositivos inalámbricos seguros bajo cualquier circunstancia:

- Cambiar los valores del ESSID, usuarios y contraseñas que trae el AP por defecto. Sustituir el ESSID y las contraseñas por otras más complejas y difíciles de adivinar.
- Deshabilitar o bloquear los Beacon Frames y cualquier mensaje de tipo broadcast que no sea necesario.
- Cifrar las comunicaciones mediante el nivel de cifrado más alto del que se disponga, dando siempre preferencia a WPA frente a WEP, y éste frente a dejar la red abierta.
- Filtrar las conexiones mediante una lista de direcciones MAC o IP blancas, también denominadas Blacklist y Whitelist.
- Deshabilitar la asignación automática de direcciones IP mediante DHCP.
- Cambiar el rango de direcciones IP que trae por defecto el AP.

- Hacer uso de VPNs. Las Redes Privadas Virtuales dan un extra de seguridad que va a permitir la comunicación entre dispositivos con una gran seguridad. Si es posible añadir el protocolo IPSec.

Mientras que las medidas propuestas pueden prevenir el uso indeseado de una red por parte de terceros no autorizados, no conviene olvidar la seguridad de los terminales, para ello es imprescindible:

- Instalar software Antivirus en el ordenador y, lo más importante de todo, mantenerlo actualizado en todo momento frente a las últimas amenazas.

- Emplear un cortafuegos personal en el terminal, el empleo de un cortafuegos personal es recomendable independientemente de otros elementos de seguridad perimetral que puedan estar instalados.

- Disponer de software de detección de intrusos en el ordenador.

- Si el terminal va ha ser empleado por menores es muy aconsejable implantar un software de control parental para evitar el acceso a contenidos no recomendables.

En el ámbito empresarial:

- Establecer políticas y procedimientos de seguridad para la utilización de la tecnología Wi-Fi

- Verificar que los usuarios de esta tecnología están entrenados y conocen los riesgos asociados con su utilización

- Mantener un inventario actualizado de Access Points y dispositivos wireless que pertenecen a la organización

- Establecer normas escritas de configuración de Access Points y estaciones de trabajo

- Prohibir o limitar el uso de dispositivos inalámbricos particulares

- Desactivar la tecnología Wi-Fi, en los dispositivos wireless que no la estén utilizando

- Emitir normas estrictas sobre el comportamiento de los usuarios en Hotspots de Aeropuertos, Hoteles, Universidades, etc.

- Restringir, si es posible, la información que pueden portar los usuarios en los dispositivos wireless

- Testear el alcance exacto de la cobertura de RF de cada Access Point, sobre todo hacia el exterior de la organización
- Cambiar el SSID por defecto y verificar que este no incluya datos sobre la organización, la división, la calle. Desactivar el broadcast del SSID, si es posible

- Desactivar los archivos compartidos y el modo Ad-Hoc, siempre que sea posible
- Instalar todos los parches necesarios en S.O., Access Points, Suplicantes, RADIUS, VPN, Firewalls, etc.
- Implementar control de acceso fuerte a la consola de gestión de los Access Points
- Utilizar 802.1x/EAP y RADIUS
- Implementar herramientas de monitorización del espacio de RF.
- Establecer una rutina de verificación de Access Point Hostiles
- Mantener un inventario actualizado de los Access Point que existen en el perímetro y que pueden interferir con sus usuarios

Para mejorar la calidad de señal:

- Para obtener el mejor rendimiento ubique si es posible el PA en línea visual de todos los usuarios, para que las ondas de radio se puedan propagar sin barreras.
- Colocar el PA en una ubicación central con respecto a los usuarios. Esto también minimizara minimizará la cantidad de señal radiada fuera del edificio evitando que intrusos puedan recibir la señal desde la acera o la calle.
- Ubicar el PA en la posición más alta des del recinto con respecto a todos sus usuarios. Por ejemplo montado en del el cielo raso o techo falso o sobre el armario mas más alto.
- Rotar o girar el PA para obtener el máximo de la intensidad de la señal llegue a los usuarios.
- Materiales metálicos de construcción, pintura metálica, paredes y pisos de cemento y estuco reducen dramáticamente la intensidad de la señal. Evite colocar los PA cerca o montados sobre grandes objetos sólidos como así también muebles de metal.
- Ubicar los Puntos de Acceso lejos de otros dispositivos electrónicos que puedan causar interferencia en particular teléfonos sin hilos (en particular los que operan en la banda de 2.4Ghz) y hornos microondas.
- Si usa antenas externas, ajústelas para que el máximo de la intensidad de la señal llegue al área donde están los usuarios.

6

6. Glosario de Términos y Abreviaturas

- **Ad-Hoc:** dispuesto especialmente para un fin.
- **Canal:** medio por el que se transmite información entre emisor y receptor.
- **Delay:** (véase Retardo).
- **Direccional:** (antena) o también denominada directiva. Es un tipo de antena capaz de concentrar gran parte de la radiación hacia una dirección concreta.
- **DMZ (Demilitaritzed Zone):** Zona desmilitarizada.
- **EMI:** interferencias electromagnéticas.
- **Ethernet:** (compatible IEEE 802.3) estándar de transmisión de datos para redes de área local. Define las características de cableado, señalización a nivel físico y los formatos de las tramas a nivel de enlace de datos, correspondientes al modelo OSI.
- **Ficheros automatizados:** se define como todo conjunto organizado de datos de carácter personal, que permite acceder a la información relativa a una persona física determinada utilizando procedimientos de búsqueda automatizados. De forma menos abstracta, podemos definir estos ficheros como aquéllos que almacenan información en soportes informáticos, y que se encuentran organizados de manera que se puede acceder a los datos utilizando cualquier tipo de aplicación o procedimiento informatizado.
- **Firewall:** dispositivo de red también denominando como cortafuegos.
- **IDS (Intrusión Detection System):** mecanismo para la detección de ataques e intrusiones a equipos informáticos, que permite localizar y reportar todo tipo de actividad maliciosa en una red de datos e incluso reaccionar de forma activa y apropiada frente a dicha actividad. El software Snort, con sensor basado en red, es un ejemplo de este tipo de mecanismo.
- **Intranet:** red de ordenadores privada basada en los estándares de Internet que permite compartir los recursos disponibles. Puede estar conectada a Internet, o incluso extenderse a través de ella (por ejemplo, mediante el uso de VPN).
- **IPsec:** (RFC 2401) arquitectura que añade servicios de seguridad al protocolo IP y puede ser usado por protocolos de niveles superiores como TCP o UDP (en la capa de transporte)
- **Jitter:** distorsión debida a la variación del retardo en un mismo flujo de datos. Concretamente, se corresponde con una desviación del tiempo de llegada entre paquetes que pertenecen a un mismo flujo de datos.
- **Kbits/s**: (o también Kbps) kilobits por segundo.
- **LAN (Local Area Network):** red de área local. Interconexión directa de sistemas informáticos, cuya extensión corresponde a un área reducida y controlada, por ejemplo el interior de un edificio.
- **Mbps:** megabits por segundo.
- **Medio de transmisión:** constituye el canal que permite la transmisión de información, empleando habitualmente ondas electromagnéticas entre emisor y receptor.
- **Mesh:** red de tipo ad hoc, donde los dispositivos de usuario que son capaces de comunicarse entre ellos de manera independiente al punto de acceso.
- **Omnidireccional:** (antena) dícese de las antenas que, en teoría, irradian o reciben señales de radiofrecuencia desde prácticamente cualquier dirección del espacio, sin ninguna preferencia concreta.
- **OSI (Open System Interconnection):** modelo de interconexión de sistemas abiertos.

- **PAN (Personal Area Network):** red de área personal. Su alcance y velocidad de transmisión son muy limitados. A modo de ejemplo generalizado, se puede considerar a Bluetooth como uno de los estándares de referencia PAN.
- **PDA (Personal Digital Assistant):** asistente digital personal. Dispositivo portátil de usuario con ciertas capacidades computacionales.
- **AP (Punto de acceso):** (inalámbrico) dispositivo, de ubicación normalmente fija, que permite la conexión de equipos de comunicación inalámbricos para formar una red de datos no cableada, posibilitando a su vez el acceso a otras redes de datos cableadas.
- **QoS (Quality of Service):** calidad de servicio. Conjunto de requisitos que debe cumplir un determinado flujo de datos respecto a fiabilidad (pérdida de paquetes o tasa de error de bit), retardo en la transmisión, variación del retardo en un mismo flujo (jitter) y ancho de banda o velocidad de transmisión.
- **Radiofrecuencia:** ondas electromagnéticas con una frecuencia determinada, que son empleadas en la radiocomunicación.
- **Retardo (Delay):** tiempo que tarda un paquete de datos en llegar a su destino.
- **Router:** dispositivo hardware para la interconexión de redes que trabaja en la capa de red del modelo OSI.
- **STA:** Station. Estación, cliente wireless.
- **TFC:** Trabajo Fin de Carrera.
- **VPN (Virtual Private Network):** red privada virtual. Red de datos lógica o virtual creada sobre una infraestructura compartida, y que proporciona unos servicios unos servicios de protección necesarios para establecer una comunicación segura.
- **WEP:** WEP es la abreviatura de Wired Equivalent Privacy, un protocolo de seguridad para redes de área local inalámbricas definido en e el estándar 802.11 b. WEP se diseña para proveer el mismo nivel de seguridad que se obtiene en redes locales cableadas.
- **Wi-Fi:** Organización que certifica la interoperabilidad de dispositivos 802.11 como un estándar compatible y global de redes WLAN.
- **WLAN:** LAN inalámbrica.
- **WPA:** Wi-Fi Protected Access es un nuevo estándar diseñado que aparece en escena para optimizar la seguridad de redes inalámbricas. El nuevo estándar, está dirigido a clientes corporativos que quieren optimizar la seguridad. WPA reemplazará el estándar actual (WEP) Wired Equivalent Privacy. WEP utiliza claves fijas de encriptación. WPA utiliza usa el protocolo TKIP (Temporal Key Integrity Protocol), que genera nuevas claves cada 10 K de datos transmitidos en la red, haciendo la red bastante mas segura.

7

7. Referencias bibliográficas

7.1. Libros

- **Rusell Dean Vines** (2002) *Wireless Security Essentials: Defending Mobile Systems from Data Piracy*. Ed Wiley
- **Alan Holt, Chi-Yu Huang** (2010) *802.11 Wireless Networks - Security and Analysis*. Ed Springer
- **Praphul Chandra** (2005) *Bulletproof Wireless Security - GSM, UMTS, 802.11, and Ad Hoc Security*. Ed Newnes
- **Amitabh Mishra** (2008) *Security and Quality of Service in Ad Hoc Wireless.* Ed. Cambridge University Press
- **Edward G. Amoroso** (2010) *Cyber Attacks: Protecting National Infrastructure.* Ed. BH
- **Jim Geier** (2008) *Implementing 802.1X Security Solutions for Wired and Wireless Networks.* Ed Wiley
- **Vipin Kumar, Jaideep Srivastava, Aleksandar Lazarevic** (2005) *Managing Cyber Threats.* Ed. Springer
- **Randall K. Nichols, Panos C. Lekkas** (2002) *Wireless Security Models Threats and Solutions.* Ed. McGraw-Hill
- **Gilbert Held** (2002) Securing Wireless Lans. Ed Wiley
- **Thomas Hardjono, Lakshminath R. Dondeti** (2006) Security In Wireless LANS and MANS. Ed Artech House
- **Klaus David** (2008) Technologies For The Wireless Future - Wireless World Research Forum (WWRF). Ed Wiley
- **Stewart S. Miller** (2004) *Wi-Fi Security*. Ed. McGraw-Hill
- **Erdal Çayırcı, Chunming Rong** (2009) *Security in Wireless Ad Hoc and Sensor Networks.* Ed. Wiley
- ***Hakima Chaouchi, Maryline Laurent-Maknavicius*** *(2009) Wireless and Mobile Network Security.* Ed. Wiley
- **James Kempf** (2009) Wireless Internet Security Architecture and Protocols. Ed Cambridge University Press

- **Yang Xiao, Xuemin (Sherman) Shen, Ding-Zhu Du** (2007) *Wireless Network Security*. Ed. Springer
- **John Rittinghouse James F. Ransome** (2004) *Wireless Operational Security*
- **Aaron E. Earle** (2006) *Wireless Security Handbook*. Ed. Auerbach Publications

7.2. Artículos

- *Federal Agencies Have Taken Steps to Secure Wireless Networks, but Further Actions Can Mitigate Risk*, November 2010.
- *Wireless_Communications_Security_Awareness_Guide*. Ed. Homeland Security
- *Symantec Internet Security Threat* Report Trends for January 06–June 06
- *Infraestructura física de redes críticas para redes LAN inalámbricas empresariales*, Viswas Puran

7.3. Estudios e Informes

- **IEEE Standard 802.11**, 2007 Edition.
- **Murugiah Souppaya, Karen Scarfone.** *Guidelines for Securing Wireless Local Area Networks (WLANs).* NIST Special Publication 800-153.
- **Gary Stoneburner, Alice Goguen, and Alexis Feringa.** *Risk Management Guide for Information Technology Systems.* NIST Special Publication 800-30.
- **Karen Scarfone, Derrick Dicoi, Matthew Sexton, Cyrus Tibbs.** *Guide to Securing Legacy IEEE 802.11 Wireless Networks.* NIST Special Publication 800-48.
- **Sheila Frankel, Bernard Eydt, Les Owens, Karen Scarfone.** *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i.* NIST Special Publication 800-97

7.4. Enlaces Web

- **IEEE** Institute of Electrical and Electronics Engineers
  www.ieee.org

- **IEEE España** Institute of Electrical and Electronics Engineers España
  www.ieeespain.org

- **NIST National Institute of Standards and Technology**
  www.nist.gov

- **ISACA** Information Systems Audit and Control Association.
  www.isaca.org

- **ONTSI** Observatorio de las Telecomunicaciones y la Sociedad de la Información.
  www.ontsi.red.es

- **INTECO** Instituto Nacional de Tecnologías de la Información
  www.inteco.es

- **CCN- CERT**
  www.ccn-cert.cni.e


UOC
Universitat Oberta
de Catalunya
www.uoc.edu


A1

Anexos 1: Summary of IEEE 802.11 Standars

Tabla A-1 summarizes the various IEEE 802.11 standards. The table contains a description, purpose keywords and remarks, and estimated product availability for each standard.

Table A-1. Summary of IEEE 802.11 Standards

IEEE Standard	Description	Purpose Keywords and Other Remarks	Availability
802.11a	A physical layer standard that operates in the 5 GHz UNII radio band. It specifies eight available radio channels. (In some countries, 12 channels are permitted.) The maximum link rate is 54 Mbps per channel; maximum actual user data throughput is approximately half of that, and the throughput is shared by all users of the same radio channel. The data rate decreases as the distance between the user and the AP increases.	**Higher performance** In most office environments, the data throughput will be greater than for IEEE 802.11b. In addition, the greater number of non-overlapping radio channels (eight as opposed to three) provides better protection against possible interference from neighboring APs.	This standard was completed in 1999. Products are available now.
802.11b	This is a physical layer standard in the 2.4 GHz ISM radio band. Maximum link rate is 11 Mbps per channel, but maximum user throughput will be approximately half of this because the throughput is shared by all users of the same radio channel. The data rate decreases as the distance between the user and the AP increases.	**Performance** Installations may suffer from speed restrictions in the future, as the number of active users increase, and the limit of three non-overlapping channels may cause interference from neighboring APs.	This standard was completed in 1999. A wide variety of products has been available since 2001.
802.11d	This standard is supplementary to the MAC layer in IEEE 802.11 to promote worldwide use of IEEE 802.11 WLAN. It will allow APs to communicate information on the permissible radio channels with acceptable power levels for user devices. The IEEE 802.11 standards cannot legally operate in some countries; the purpose of 802.11d is to add features and restrictions to allow WLANs to operate within the rules of these countries.	**Promote worldwide use** In countries where the physical layer radio requirements are different from those in North America, the use of WLANs is lagging behind. Equipment manufacturers do not want to produce a wide variety of country-specific products, and users that travel do not want a bag full of country-specific WLAN PC cards. The outcome will be country-specific firmware solutions.	This standard was completed in 2001. Products are available now.
802.11e	This standard is supplementary to the MAC layer to provide QoS support for WLAN applications. It will apply to IEEE 802.11 physical standards a, b, and g. The purpose is to provide classes of service with managed levels of QoS for data, voice, and video applications.	**Quality of service** This standard provides some useful features for differentiating data traffic streams. It is essential for future audio and video distribution.	This standard was completed in 2005. Products are available now.

IEEE Standard	Description	Purpose Keywords and Other Remarks	Availability
802.11f	This is a "recommended practice" document that aims to achieve AP interoperability within a multi-vendor WLAN. The standard defines the registration of APs within a network and the interchange of information between APs when a user is handed over from one AP to another.	**Interoperability** This standard will work to increase vendor interoperability, reduce vendor lock-in, and allow multi-vendor infrastructures.	This recommended practice was completed in 2003. Products are available now.
802.11g	This is a physical layer standard for WLANs in the 2.4 GHz ISM radio band. The maximum link rate is 54 Mbps per channel whereas IEEE 802.11b offers 11 Mbps. The IEEE 802.11g standard uses orthogonal frequency-division multiplexing (OFDM) modulation but, for backward compatibility with IEEE 802.11b, it also supports complementary code-keying (CCK) modulation and, as an option for faster link rates, allows packet binary convolutional coding (PBCC) modulation.	**Higher performance with IEEE 802.11b backward compatibility** This standard provides speeds similar to IEEE 802.11a and backward compatibility with IEEE 802.11b.	This standard was completed in 2003. Products are available now.
802.11h	This standard is supplementary to the MAC layer to comply with European regulations for 5 GHz WLANs. European radio regulations for the 5 GHz band require products to have transmission power control (TPC) and dynamic frequency selection (DFS). TPC limits the transmitted power to the minimum needed to reach the farthest user. DFS selects the radio channel at the access point to minimize interference with other systems, particularly radar.	**European regulation compliance** This is necessary for products to operate in Europe. Completion of IEEE 802.11h provides better acceptability within Europe for IEEE-compliant 5 GHz WLAN products. A group that is rapidly dwindling will continue to support the alternative HyperLAN standard defined by the European Telecommunications Standard Institute (ETSI).	This standard was completed in 2003. Products are available now.
802.11i	This standard is supplementary to the MAC layer to improve security. It applies to IEEE 802.11 physical standards a, b, and g. It provides improved security over Wired Equivalent Privacy (WEP) with new encryption methods and authentication procedures. IEEE 802.1X forms a key part of IEEE 802.11i.	**Improved security** The IEEE 802.11i amendment defines two data confidentiality and integrity protocols for Robust Security Network Associations (RSNA): TKIP and Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), using AES. Federal agencies are required to use FIPS-validated cryptographic modules.[32] NIST SP 800-97 contains specific recommendations and guidance for IEEE 802.11i.	This standard was completed in 2004. Products are available now.

IEEE Standard	Description	Purpose Keywords and Other Remarks	Availability
802.11k	This standard defines Radio Resource Measurement enhancements to provide management and maintenance interfaces to higher layers for mobile WLANs.	**Resource radio management** This standard will enable seamless Basic Service Set (BSS) transitions between WLANs through the discovery of the best available AP and improve network traffic by distributing users to under-used APs.	Draft 11 was approved in January 2008. Final ratification has not yet occurred.
802.11m	This is a supplementary maintenance standard to the IEEE 802.11-1999 (reaff. 2003) standard.	**Editorial maintenance** This initiative is to perform editorial maintenance, corrections, improvements, clarifications, and interpretations to the IEEE 802.11-1999 (reaff. 2003) Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications standard.	This standard was completed and is part of 802.11-2007.
802.11n	This standard investigated the possibility of improving the IEEE 802.11 standard to provide high throughput at a theoretical 300 Mbps.	**Increased data throughput** The purpose of this standard is to improve the IEEE 802.11 WLAN user experience by providing significantly higher throughput using MIMO antennas and receivers and different coding schemes.	This standard is expected to be completed in 2009.
802.11p	This standard is an amendment of IEEE 802.11 to support communication between vehicles and the roadside and between vehicles while operating at speeds up to a minimum of 200 kilometers/hour for communication ranges up to 1,000 meters. The amendment will support communications in the 5 GHz bands—specifically 5.850–5.925 GHz band within North America—with the aim to enhance the mobility and safety of all forms of surface transportation, including rail and marine. Amendments to the Physical (PHY) and MAC layers will be limited to those required to support communications under these operating environments within the 5 GHz bands. This standard is also referred to as the Wireless Access for Vehicular Environment (WAVE).	**Wireless access for vehicles** This standard amends the existing IEEE 802.11 standard to make it suitable for interoperable communications to and between vehicles. The primary reasons for this amendment include the unique transport environments and the very short latencies required (some applications must complete multiple data exchanges within 4 to 50 milliseconds).	This standard is scheduled to be completed in April 2009.
802.11r	This standard is supplementary to the IEEE 802.11 Medium Access Control (MAC) layer standards and creates improvements to minimize or eliminate the amount of time data connectivity between the Station (STA) and the Distribution System (DS) during a BSS transition.	**Fast BSS transitions** This standard improves BSS handoffs within IEEE 802.11 networks. This is a critical component to support real-time constraints imposed by applications such as Voice over Internet Protocol (VoIP).	This standard is scheduled to be published in mid-2008.

IEEE Standard	Description	Purpose Keywords and Other Remarks	Availability
802.11s	This standard defined the IEEE 802.11 ESS Mesh with an IEEE 802.11 Wireless Distribution System (WDS) using the IEEE 802.11 MAC/PHY layers that supports both broadcast/multicast and unicast delivery over self-configuring multi-hop topologies.	**ESS mesh networking** This standard provides a protocol for auto-configuring paths between APs over self-configuring multi-hop topologies in a WDS to support both broadcast/multicast and unicast traffic in an ESS Mesh using the four-address frame format or an extension.	This standard is scheduled to be completed in 2008.
802.11t	This is a "recommended practice" and will provide a set of performance metrics, measurement methodologies, and test conditions to enable measuring and predicting the performance of IEEE 802.11 WLAN devices and networks at the component and application level as a recommended practice.	**Wireless performance protection** This standard enables testing, comparison, and deployment planning of IEEE 802.11 WLAN products so that performance and products specifications can be captured through common and accepted set of performance metrics, measurement methodologies and test conditions.	This recommended practice is scheduled to be completed in 2008.
802.11u	This standard is an amendment to the IEEE 802.11 MAC and PHY layers to support InterWorking with External Networks.	**Internetworking with external networks** This will provide amendments to the IEEE 802.11 PHY/MAC layers, which will enable InterWorking with other networks and granting of limited access, based on a relationship with an external network. This includes both enhanced protocol exchanges across the air interface and provision of primitives to support required interactions with higher layers for InterWorking.	This standard is in the proposal evaluation stages and a scheduled completion date has not been set.
802.11v	This standard will create amendments to provide Wireless Network Management enhancements to the IEEE 802.11 MAC, and PHY layers to allow configuration of client devices connected to the network.	**Wireless network management** This will provide amendments to the IEEE 802.11 PHY/MAC layers that enable management of attached stations in a centralized or in a distributed fashion (e.g., monitoring, configuring, and updating) through a layer 2 mechanism. Although the IEEE 802.11k Task Group is defining messages to retrieve information from the station, the ability to configure the station is not within its scope. The proposed Task Group will also create an Access Port Management Information Base (AP MIB).	This standard is in the early proposal stages and a scheduled completion date has not been set.

IEEE Standard	Description	Purpose Keywords and Other Remarks	Availability
802.11w	This standard will enhance IEEE 802.11 MAC layer security for selected management frames by providing data integrity, data origin authenticity, replay protection, data confidentiality, and other security features.	**Management frame protection** This will extend the use of IEEE 802.11i to selected management frames to increase the overall security of IEEE 802.11-based networks. The increased level of security is intended to mitigate malicious network-based attacks, such as DoS attacks. In addition, this amendment will provide security for sensitive network information that will be included in transmissions outlined in several new amendments, including IEEE 802.11r, IEEE 802.11k, and IEEE 802.11y.	The standard is under development and is expected to be completed and ratified in 2008.