MONOGRÁFICO: Redes Wifi

Escrito por Tomás Simal

Índice de contenido

Aunque la percepción general es que las redes inalámbricas son algo muy reciente, la realidad es que llevan existiendo y más de 15 años. Inicialmente no eran de uso general, si no que su utilidad se concentraba en mercados muy concretos, como la gestión de almacenes, educación y medicina (estos dos últimos con poca incidencia dentro de España en esa época).

1. Introducción

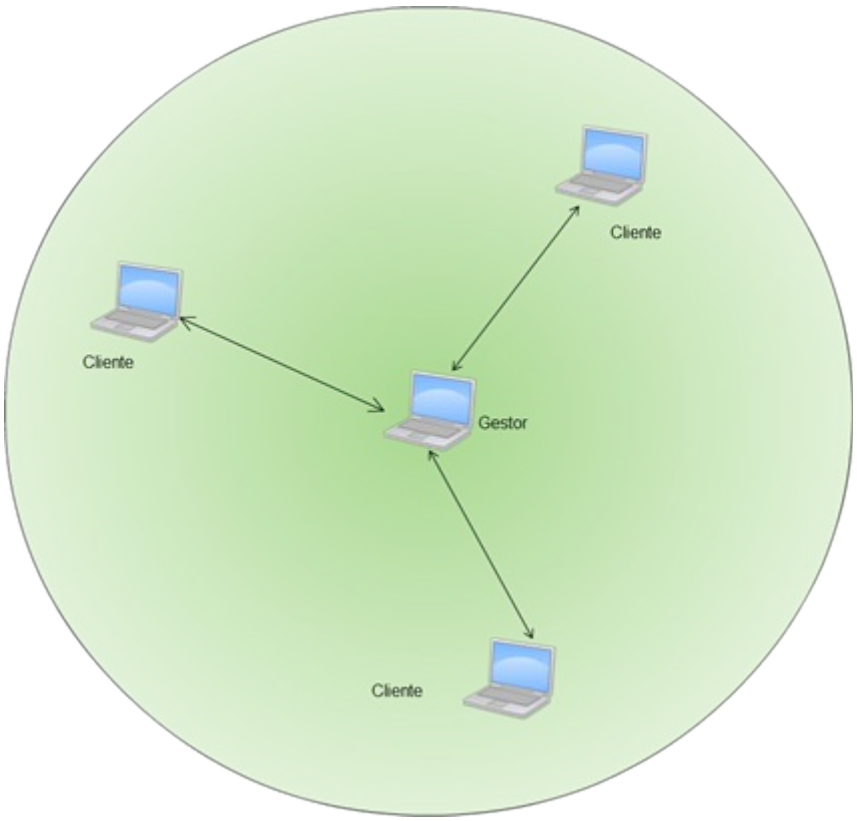
1.1 Uso y utilidad

No fue hasta su estandarización, tras la creación de la “Wi-Fi Alliance” en 1996, organización que nació con la intención de verificar, certificar e impulsar sistemas con el protocolo 802.11, cuando estas redes empezaron a ser utilizadas por el público en general. El principal problema que existía hasta entonces era la falta de compatibilidad entre distintos fabricantes, pues aun cumpliendo todos ellos la norma 802.11, dicha norma dejaba abierta a la interpretación suficientes puntos como para hacer que sistemas de distintos fabricantes no trabajaran entre sí. Así pues la Wi-Fi Alliance permitió homogeneizar productos y hacer posible que se asentaran en el mercado de consumo, hasta el punto que hoy en día las redes inalámbricas se conocen popularmente por redes “Wi-Fi” en referencia a este organismo (termino que utilizaremos también en este documento para referirnos a ellas, aunque se hace notar al lector que existen redes de uso específico que no son “Wi-Fi”, las cuales no trataremos aquí).

Desde su principio la idea de dichas redes fue substituir en la medida de lo posible las redes fijas, terminando así con los problemas inherentes al cableado como sus costes y la falta de movilidad. La situación a día de hoy no es tan perfecta como transmiten los diferentes fabricantes de esta tecnología y en la realidad mantienen su utilidad en aquellos entornos en los que la deslocalización o movilidad de los equipos es necesaria o el cableado es difícil o muy costoso. Sin embargo, a causa de la velocidad de transmisión, su naturaleza de medio compartido y problemas de transmisión, absorción, interferencias, etc. no posibilita que substituyan totalmente a las redes cableadas como algunos analistas llevan vaticinando, sin éxito, desde hace años.
Una segunda utilidad que aún no siendo de uso masivo, si es muy interesante, es la opción de realizar enlaces inalámbricos entre distintas localizaciones. Así pues, es posible substituir con estos equipos enlaces punto a punto o punto multipunto que contratados a proveedores de telecomunicaciones serian costosos y de relativa baja velocidad, por otros de alta velocidad y coste muy bajo, con un retorno de inversión muy rápido. Sin embargo este tipo de enlace tiene limitaciones que no lo hace aplicable a todas las situaciones, pero aún así, no están siendo explotados todo lo que sería posible, normalmente por el desconocimiento de su existencia y características por parte de sus potenciales usuarios.

1.2 Arquitectura general

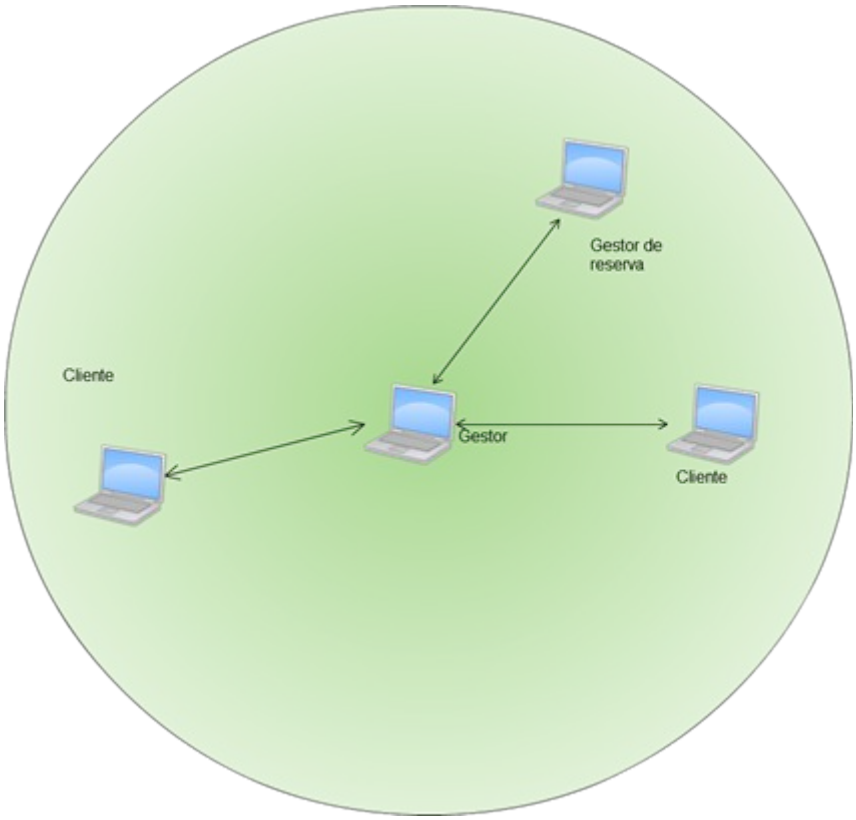
En las redes Wi-Fi siempre existe, como estructura básica, un gestor de la comunicación y una serie de clientes. Los clientes, escucharán siempre para detectar la presencia de uno o más gestores que les indicará, entre otros datos, el nombre de la red que gestionan, el canal a usar, la seguridad y algoritmos de autentificación disponibles, etc.. En base a esta información y la configuración del dispositivo en cuestión, el cliente será capaz de unirse a la red adecuada.
Dependiendo de quién implemente la función de gestión de la red, nos encontraremos ante una red “ad-hoc”, en la que el gestor es un ordenador integrante de la propia red, o una red de tipo “infraestructura” en la que el gestor en un punto de acceso, router o similar.
En la práctica, una red ad-hoc solo la componen ordenadores, conformando una celda aislada (a no ser que uno de los ordenadores desarrolle funciones de bridge/router) y no tiene posibilidad de hacer unidad con otras celdas, mientras que una red del tipo “infraestructura” se integrará en la red cableada existente y permitirá crear varias celdas, que trabajarán conjuntamente, para dar una mayor cobertura espacial.



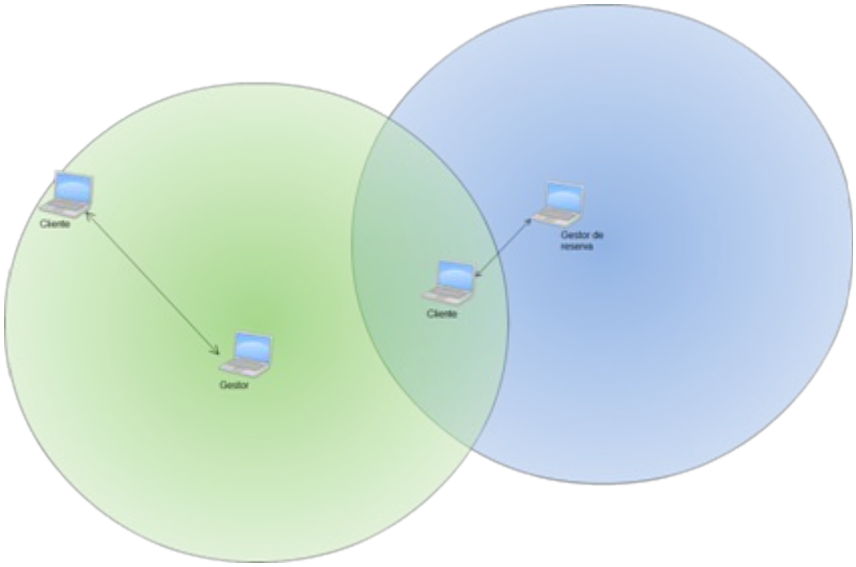
Red ad-hoc

Es importante, como se ha indicado, conocer el funcionamiento de las redes Wi-Fi según el cual los clientes solo se conectan según las indicaciones del gestor de la celda, para prever y solucionar algunos problemas

que pueden surgir estas redes. Por ejemplo, en las redes “ad-hoc” uno de los ordenadores realizará las funciones de gestor. Lo cual indica que dicho ordenador ha de estar siempre funcionando o la red desaparecerá con él. Así mismo su localización ha de ser tal que todos los demás miembros de esa red tengan visibilidad radio con él. Puede suceder incluso, que mas de un ordenador asuma el rol de gestor, bien por un error de configuración, o porque alguno está configurado de forma que cuando el gestor falla tome el control de la red, y en caso de que este gestor de reserva y el gestor activo no se detecten aparecerían dos gestores y por tanto dos redes, con clientes asociados a cada una de ellas dependiendo de la cercanía al gestor que controla la celda, y sin comunicación entre los dos grupos.
En los siguientes esquemas se puede observar dicha situación. En la primera imagen se muestra una red en la que existe un gestor y un equipo que actúa de reserva, para asumir en el rol de gestor en caso de que el gestor principal desaparezca.



Si el gestor de reserva se desplaza de manera que no esté dentro del área de cobertura del gestor (o si el que se desplaza es el gestor, dejando sin cobertura al de reserva), el gestor de reserva asume el rol de gestor principal, al deducir que éste ha desaparecido y es necesario asumir las funciones de control de la celda. Es por esta razón que se producirá la ruptura de la celda en dos redes independientes, como se muestra en la siguiente ilustración.



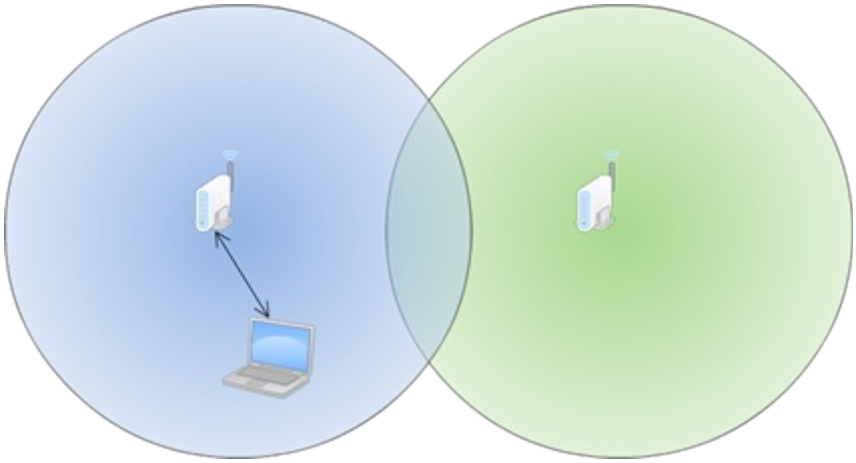
Sin embargo, las redes más habituales son las de tipo “infraestructura” y son las que analizaremos en este documento. En dichas redes, existe un dispositivo, normalmente un punto de acceso o un router (AP, abreviatura de “Access Point”, término ingles que es frecuentemente utilizado, y que lo será así mismo a lo largo del documento junto con otros términos en ingles, bien por ser el de uso habitual o por no existir traducción en nuestro idioma), que se encarga de la gestión de la red inalámbrica, enviando un paquete de información en el que indica el nombre de la red que conforma, métodos de autenticaciones soportados, canal a usar, etc. Con esta información lo clientes podrán solicitar el acceso y tras la autenticación necesaria serán miembros de la red y podrán trasmitir haciendo uso de esta. Para el envío de esta información se utiliza un tipo de trama especial que recibe el nombre de “beacon”.

La trama de beacon es enviada periódicamente, permitiendo así a los equipos reconocer los distintos puntos de acceso existente, las redes disponibles, las potencias de recepción, los parámetros a utilizar en la organización de la transmisión de los diversos clientes, etc. El intervalo de emisión de esta trama es, en muchos equipos, configurable. Si se aumenta el intervalo se conseguirá una menor ocupación del ancho de banda disponible por tráfico de control de la celda y un mayor rendimiento de cara al usuario. Sin embargo la mejoría es muy escasa y en contra partida se producirá el efecto de que los clientes tardarán más en detectar la red, lo cual influirá en la velocidad de conexión a estas o en el tiempo necesario para llevar a cabo el proceso de “roaming” o cambio de celda, como se vera mas adelante.

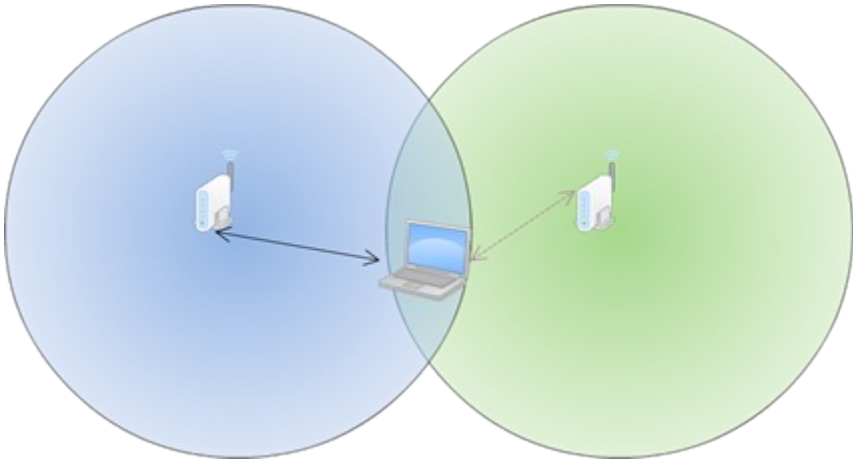
Cada AP conforma una celda, es decir, el área que da cobertura, a donde llega su emisión con la potencia necesaria para ser recibida por los clientes. Sin embargo este área puede no ser suficiente. La normativa implica que no puede emitirse una potencia superior a 100mW lo cual limita el alcance, que suele ser en el mejor de los casos de 300m de diámetro en campo abierto, y 150 en entornos de oficinas, pero con grandes variaciones dependiendo de la norma Wi-Fi del aparato y su calidad, el entorno, materiales, equipos utilizados, etc. lo que conduce a que típicamente los alcances en interior suelen estar más en el orden de 60 metros de diámetro por los distintos materiales y elementos (sobre todo metálicos y electrónicos) que suelen estar presentes en este tipo de entorno. Ante la necesidad de cubrir mayores aéreas se prevé la posibilidad de utilizar más puntos de acceso de manera que la suma de las celdas que cada uno de éstos conforman, cubra toda la superficie que se desea cubrir.

Esta configuración permite que un cliente se conecte a uno u otro punto de acceso dependiendo cuál de ellos proporcione una mejor calidad de recepción, con lo que el cliente podrá moverse libremente por todo el área de cobertura y el enlace físico pasara de una celda a otra según sea necesario (función conocida con el término “roaming”).

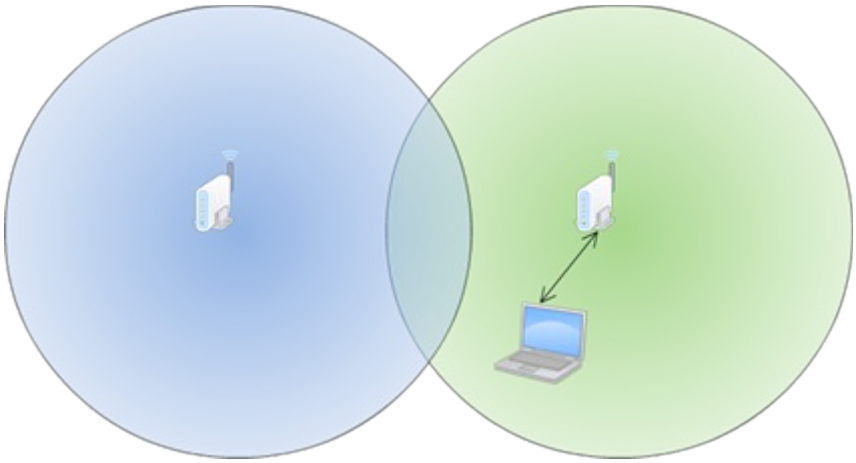
En las siguientes imágenes se muestra el proceso de roaming de un dispositivo que se desplaza de la zona de cobertura de una celda a la contigua. En la primera imagen, el equipo se encuentra en la celda azul, con una buena cobertura y sin detectar ninguna otra celda, con lo que la asociación se realiza con el punto de acceso que genera dicha celda.



Al desplazarse, el cliente Wi-Fi entra en la zona en la cual se solapan ambas celdas. Empezará a detectar las tramas beacon enviadas por el punto de acceso de la segunda celda y tras comprobar que se trata de la misma red y que se posee la acreditación necesaria (por ejemplo la clave correcta), empezará a evaluar la calidad de recepción de esta celda, monitorizando ambas señales.



al continuar el desplazamiento, llegará un punto en que la calidad de recepción de la celda verde sea mejor que la de la celda azul, con lo que se asociará al nuevo punto de acceso que conforma la celda verde y cancelará la asociación del punto de acceso que genera la celda azul.



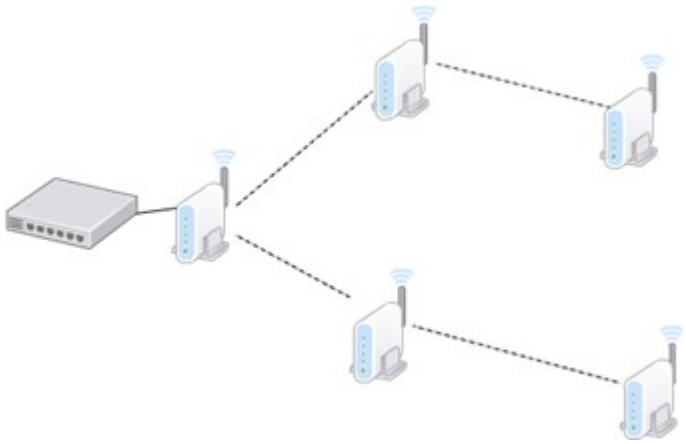
Este cambio suele ser rápido para la mayoría de los propósitos, pero depende de los terminales y los puntos de acceso. Así mismo en algunos casos es posible configurar el modo de funcionamiento del proceso de roaming, primando la permanencia en la celda actual o el cambio rápido a una celda con mejor recepción. Es obvio que la segunda opción permitirá que el cliente este siempre asociado al mejor punto de acceso, por lo que se conseguirán mejores rendimientos, pero tiene el peligro de que si se mueve por el limite de las celdas, puede estar cambiando constantemente de celda, causando una gran carga en los equipos, que estarán un porcentaje del tiempo significativo realizando la función de roaming en vez de transmitir los datos, ralentizando la comunicación y logrando por tanto el efecto contrario al deseado,

Al colocar varios puntos de acceso para dar cobertura a un área mayor que el de la celda individual, hay que tener en cuenta que dichas áreas se solapen ligeramente, para que los clientes tengan un espacio en el que hacer el cambio de una celda a otra sin perder conectividad. Se debe tener en cuanta así mismo que todos los puntos de acceso han de tener una configuración coherente en cuanto a nombre de red y sistemas de autenticación. A cerca de las frecuencias se intentará no repetirlas entre celdas que solapen, distanciando las frecuencias tanto como sea posible para evitar interferencia entre ambas celdas, pues en caso de no hacerlo, la influencia entre estas influiría en un menor ancho de banda disponible para los clientes.

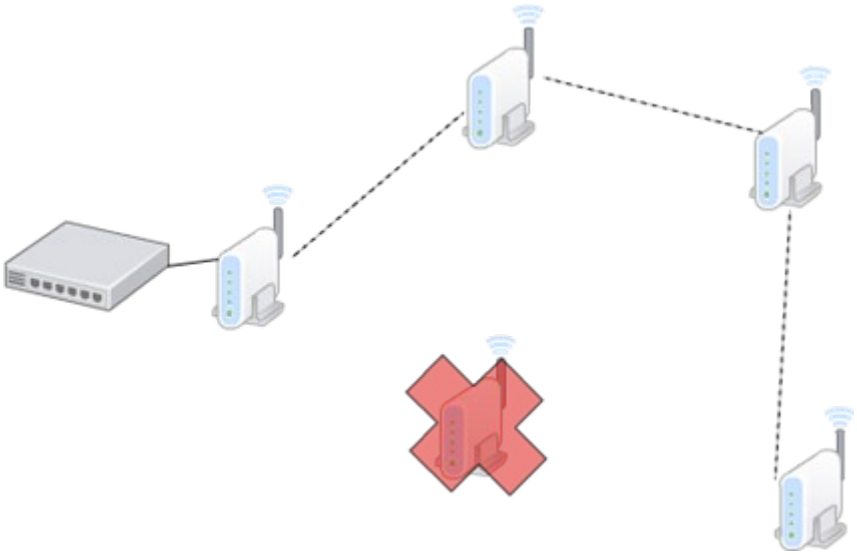
Existe una estructura, variante del tipo “infraestructura” que se conoce habitualmente como red en malla o mas habitualmente por su termino inglés “mesh”. En esta estructura existirán puntos de acceso que no tiene conexión a la red cableada. Éstos crearán un enlace inalámbrico con alguno de aquellos que sí tengan conexión a la red fija, y a su vez creará una celda local que dará cobertura a los clientes de la zona. Esto por si solo no sería más que una extensión inalámbrica, pero en una red mesh se permite la existencia de varios niveles. Para alcanzar puntos lejanos es posible que un punto de acceso se conecte con otro punto de acceso, y así sucesivamente en tantos niveles como sean necesarios o como permitan los equipos utilizados, hasta que a su vez se cree un enlace con aquel que tiene conexión con la red cableada.

Esto ofrece la posibilidad de crear áreas de cobertura Wi-Fi en zonas que no tienen posibilidad de conectarse a una red de datos cableada, aunque sea una zona lejana y sean necesarios varios saltos. Así mismo, en los sistemas avanzados, se posibilita que los enlaces entre los puntos de acceso se reconfiguren en el caso de que un fallo en alguno de los equipos o un elemento externo impida el funcionamiento de alguno de los enlaces preconfigurados.

En el gráfico siguiente se muestra un ejemplo de red tipo mesh.



En ella se observa como solo un punto de acceso tiene conexión a la red cableada, mientras que el resto mantiene enlaces inalámbricos para acceder a la red fija, en algunos casos mediante varios saltos. En el caso de que uno de los puntos de acceso presentara un fallo, la red podría reconfigurarse, en el caso de algunos sistemas de manera automática, para permitir seguir dando servicio a los usuarios, tal como se muestra en el gráfico siguiente, en el que se muestra la red anterior, en la que un punto de acceso dejado de funcionar:



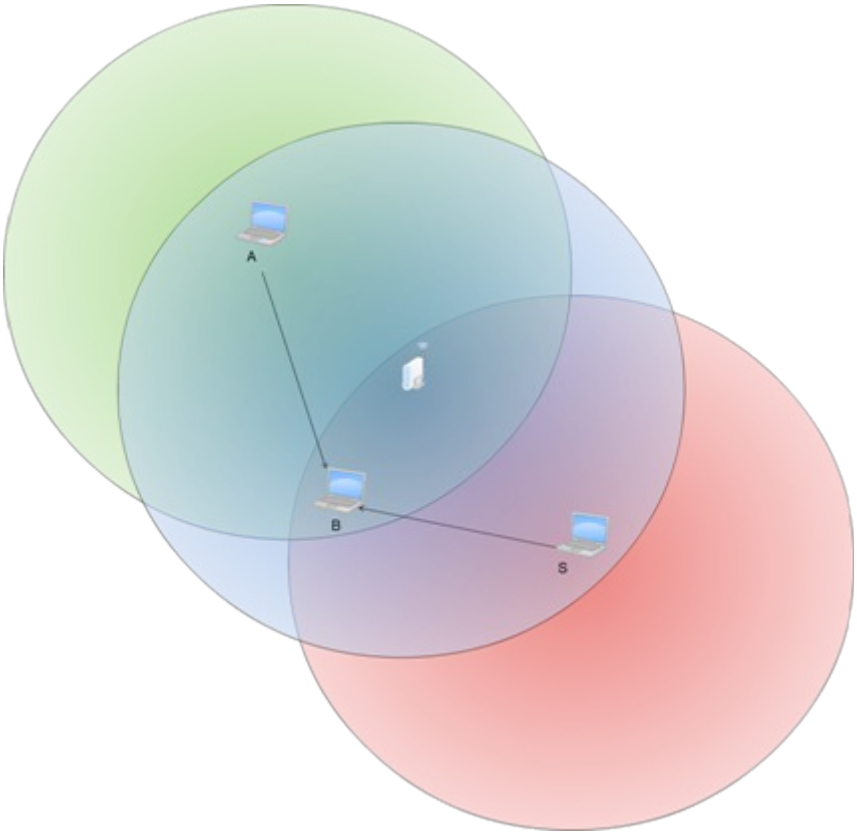
Existen herramientas que posibilitan la configuración automática y coherente de los puntos de acceso, así como funcionalidades avanzadas de las que hablaremos en un punto posterior.

Es importante tener en cuenta que todos los puntos de acceso que conforman una red, han de estar conectados al mismo segmento lógico de red cableada. Hay dos puntos que fuerzan a que así sea; uno es que resulta habitual que los puntos de acceso tengan que comunicarse entre ellos por la red cableada para gestionar el roaming, y otro es que el cliente sale a la red cableada a través del punto de acceso que conforma la celda en la que está en ese momento. Esto hace que el cliente, debido a sus cambios de celda, entre a la red por diferentes puntos, pero manteniendo las mismas direcciones IP y MAC. Si dos puntos de acceso estuvieran en subredes diferentes, la dirección IP del cliente dejaría de ser válida al cambiar de celda/AP (que equivaldría a cambiar de subred), además podría dar problemas en firewalls, configuraciones de listas de acceso en switches, etc. que habrá que tener en cuenta a la hora de diseñar la red. Una solución a este problema seria la utilización de un controlador con funciones de tunelización como se verá en un apartado posterior.
En general, la constitución básica de una red inalámbrica, consta de tres parámetros principales: el nombre de la red, los canales utilizados y la seguridad implementada.
Cada red se definirá mediante un nombre, denominado SSID, que es un identificador alfanumérico que designa la red. Todos aquellos puntos de accesos que conformen una red deberán compartir el mismo SSID. El cliente cuando busca las redes existentes, las reconoce por el nombre que estas publican. Sin embargo es posible que una red no publique el nombre. Este funcionamiento es una medida que se puede adoptar como estrategia de seguridad, en cuyo caso, para conectarse a esa red, habrá que conocer su nombre y será necesario configurarlo manualmente en el cliente.
En cada punto de acceso se indicará cual es el canal que se utilizará. El cliente que desee conectarse a la celda deberá utilizar el canal indicado. Así pues, no es el cliente, si no el punto de acceso (o en el caso de redes ad-hoc, el equipo que toma el rol de gestor de la celda), el que fija el canal a utilizar. Aunque dos o mas equipos coincidan en el mismo canal, será posible diferenciarlos por el nombre de red asignado a cada uno de ellos. En caso de tener el mismo SSID y por tanto pertenecer a la misma red será el cliente el que elegirá a cual conectarse dependiendo de la calidad de recepción (o forzará la conexión el punto de acceso en caso de existir listas de acceso que fuercen al cliente la elección de uno de ellos mediante la denegación del permiso de conexión a los demás).
Tras tener el cliente conocimiento de la red a la cual desea pertenecer, los puntos de acceso que pertenecen a ella y que están a su alcance para conectarse, en base a la calidad de recepción elegirá uno de dichos puntos de acceso y fijará su canal en el que este le indique. Para proceder a la conexión deberá cumplir con los requisitos de seguridad que le imponga la red y que le serán indicados por el punto de acceso. Será imprescindible que todos los puntos de acceso que pertenezcan a la misma red (es decir, que tengan el mismo SSID), implementen los mismos requisitos de identificación y autentificación de los usuarios. Lo más habitual es realizar dicha autentificación mediante una clave compartida, que deberá ser conocida por el cliente y compartida por todos los puntos de acceso que integran la red, aunque no es el único método como veremos en puntos posteriores. Así mismo el método de autentificación deberá ser común y soportado por todas las partes.

Como se ha comentado brevemente con anterioridad, existen varias frecuencias/canales en las que funcionan estos sistemas. Actualmente hay distintas variedades de redes Wi-Fi, descritas cada una por su propia norma. Cada una de estas normas se sitúa en uno banda de frecuencias disponibles para este uso (excepto la 802.11n que puede funcionar en ambas frecuencias): la banda de 2,4 GHz y la de 5 GHz.
La banda más ampliamente utilizada es la de 2,4GHz, por distintos motivos, como el menor coste de los dispositivos, la más temprana utilización de esta banda,… pero principalmente, en Europa, y en particular en España, por regulaciones del espectro radioeléctrico. La banda de 2,4 GHz fue de uso libre no regulado ya cuando las redes inalámbricas surgieron, pero la banda de 5 GHz no se liberó hasta más adelante, cuando las redes Wi-Fi ya estaban en uso, por tener un uso gubernamental en España. Actualmente ambas frecuencias son de libre uso, lo cual permite la utilización de dispositivos Wi-Fi que hagan uso de ellas.
Dentro de cada una de esas banda de frecuencia, existe una división en canales que permite posicionar las distintas redes o celdas que coinciden en un mismo área, en diferentes frecuencias para facilitar un funcionamiento más ordenado y evitar, en la medida de lo posible, las colisiones, interferencias, etc.

2 Consideraciones generales

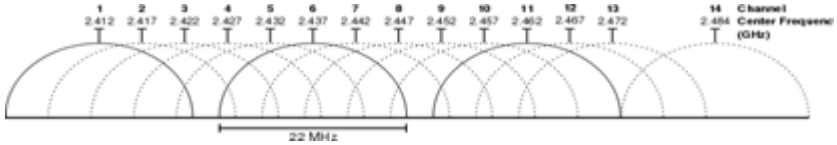
Las redes Wi-Fi son redes inalámbricas, por tanto redes vía radio, con todo lo que ello implica respecto a frecuencias, interferencias, influencia del entorno, etc. Esto nos obliga a recapacitar sobre las implicaciones que ello tiene, tanto en la manera de funcionar como en las limitaciones y problemas que de ello pueden surgir.
La primera consecuencia de esto es que los clientes no están claramente definidos, ni en número, ni en situación, lo cual provoca la necesidad de una gestión de éstos. Será necesario autentificarlos, notificarles parámetros de funcionamiento como el canal a utilizar, etc. Así mismo al ser un medio compartido (aquí cada cliente comparte el aire, no tiene un cable independiente cada uno) es necesario tener un mecanismo que ordene su funcionamiento y acceso al medio, para evitar en lo posible las colisiones, situación en que uno o más equipos transmiten a la vez, interfiriéndose entre ellos e invalidando la comunicación, y en el caso de que éstas sucedan, proveer los mecanismos para solventar la incidencia. Todo ello es realizado de forma transparente para el usuario, pero tiene un coste total: una reducción de la velocidad de transmisión.
Para el control de la transmisión se utilizan dos protocolos complementarios: CSMA/CA y RTS/CTS.
El mecanismo definido en el CSMA/CA es una adaptación del CSMA/CD utilizado en las redes Ethernet, pero modificado para tener en cuenta la limitación de las comunicaciones por radiofrecuencia según la cual una estación transmitiendo no puede detectar una colisión con otra transmisión simultánea. El algoritmo dicta que un equipo que desea transmitir, antes de hacerlo ha de escuchar para comprobar si ya existe otra estación enviando datos. En caso de no ser así podrá transmitir, pero si ya hubiera algún equipo transmitiendo deberá esperar un tiempo aleatorio y transcurrido este, volver a comprobar si el medio esta ocupado por otra transmisión. Este algoritmo presenta varios problemas. Uno es que existe la posibilidad de que dos o mas equipos comprueben a la vez si se esta transmitiendo y al detectar que el canal esta libre, empiecen a emitir de forma simultanea. Este problema deberá ser solucionado por protocolos superiores como TCP que se encargarán de detectar pérdidas de información y pedir la retransmisión de esta. Así mismo, al ser el tiempo de espera, cuando se detecta el canal ocupado, tomado de forma aleatoria se consigue paliar en parte el problema de la concurrencia de equipos al comprobar el uso del canal. Otro es el problema conocido como “terminal oculto”, que se muestra en la siguiente ilustración.



Este problema se produce cuando, estando los terminales “A”, “B” y “S” en la misma celda, cuya cobertura esta mostrada en azul, un terminal “A” tiene visibilidad de otro terminal “B” pero no de un terminal “S”, como se ve por su área de cobertura mostrada en verde. Un caso típico en el que puede pasar esto es que se encuentren en fila por lo que la distancia de “A” a “B” sea relativamente corta, pero la de “A” a “S” suficientemente larga como para que no se detecten, pero sin embargo “B” al estar a mitad de camino si tenga recepción de “S”, cuya área de cobertura se muestra en rojo. Esta situación también puede suceder por elementos arquitectónicos que impidan la visibilidad entre “A” y “S”, pero si permitan la comunicación entre “S” y “B” y entre “A” y “B”.

En esta situación el terminal “S” puede emitir para enviar información a “B”. Si el terminal “A” así mismo quisiera transmitir, escucharía el canal, y al no tener visibilidad de “S” encontrará el canal vacío y transmitirá. El problema surge del hecho de que “B” sí tiene visibilidad de ambos terminales, así que detectará ambas señales de forma simultánea, que interferirán y harán la comunicación inválida, y lo peor es que ni “A” ni “S” tendrán constancia del problema, así que la situación puede dilatarse en el tiempo indefinidamente.
Para solventar este problema, así como alguno más (por ejemplo la iteración entre clientes 802.11b y 802.11g) se implementó en estas redes Wi-Fi el protocolo RTS/CTS. Es obligatorio para los equipos tener implementado este protocolo, pero no lo es tenerlo activado, aunque por defecto suele estar activo para evitar problemas como el del terminal oculto.
Cuando el protocolo RTS/CTS esta activado, se añade al CSMA/CA, de manera que una vez que el terminal que ha detectado que nadie está transmitiendo, enviará una trama RTS al terminal destino, indicándole que desea transmitir y, entre otros datos, cuanto tiempo (en bytes) durará esa transmisión. Si en terminal destino está en condiciones de recibir la información, responderá con una trama CTS repitiendo así mismo la información que indica cuanto tiempo durará la transmisión. Con este intercambio, se consigue que el canal quede reservado y los demás equipos sepan que han de esperar al menos el tiempo que se indica en las tramas RTS y CTS para poder transmitir ellos, y puesto que tanto emisor como receptor transmiten la información, todos aquellos sistemas que pudieran interferir con esa transmisión recibirán la trama RTS, la CTS o ambas.
Es un error común y fuente de problemas suponer que la velocidad de transmisión que publicita una norma o un producto es la real que alcanzaremos, tal como sucede en el caso de las redes cableadas, si los equipos implicados no presentan alguna limitación de diseño. No es así en el caso de las redes inalámbricas, pues la gestión de la comunicación, mayormente por el control de usuarios y los mecanismos de organización de la transmisión descritos anteriormente, implica que la velocidad de transmisión (ancho de banda) disponible para

el usuario ronda el 50% de la velocidad máxima de la red. Esta situación será la ideal, y el rendimiento puede ser incluso menor por limitaciones de los equipos implicados (tanto APs como clientes).
Añadido a ello, aunque los equipos implicados sean capaces de proporcionar la máxima velocidad, hay otros factores como interferencias, reflexiones, etc. que influirán en el rendimiento. Aún siendo el medio ideal, la distancia también influirá en el rendimiento. Dentro del mecanismo de funcionamiento de las redes Wi-Fi se prevé que cuando la potencia baje o el ruido o interferencias aumenten, el cliente sincronizará a una velocidad menor, de manera que el mecanismo de transmisión para esa menor velocidad proporcione mayor inmunidad ante la degradación de la señal. La distancia es uno de esos factores que disminuyen la potencia de la señal, así que dentro de la celda, la velocidad disponible para los clientes disminuye con la distancia, creándose áreas con velocidades decrecientes según sea mayor la distancia al punto de acceso.
En lo sucesivo, al indicar las diferentes velocidades alcanzables según las diferentes normas, se suministra el valor de la máxima velocidad de transmisión alcanzable por los sistemas que a dicha norma se ajusten, que será mayor a la disponible por el usuario tal como se acaba de explicar.
Es necesario considerara así mismo las frecuencias concretas que utilizan los quipos Wi-Fi. Como se comentó en el punto anterior, las redes actuales pueden utilizar las bandas de 2,4 GHz o 5 GHz.



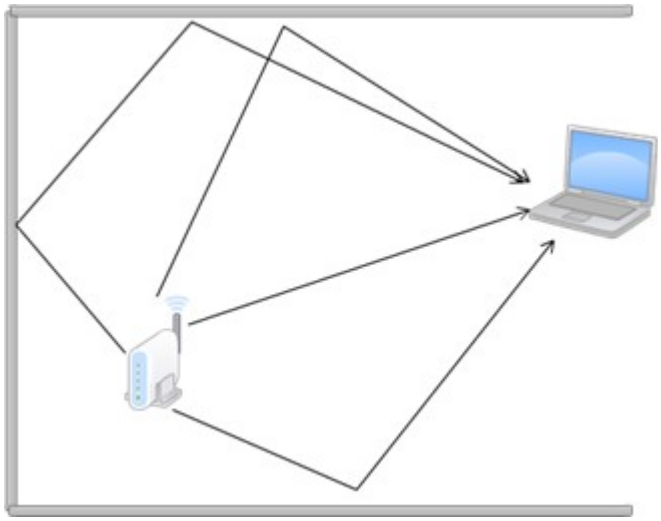
La banda de 2,4GHz abarca desde las frecuencias de 2.400 GHz hasta 2.4835 GHz y contiene 13 canales, con un ancho 22 MHz de ancho cada uno, en Europa (pues por la regulación de los organismos que aplican a cada país o región, varia en alguno de los casos, como Estados unidos con 11 canales o Japón con 14). Sin embargo, en contra de lo que suele creerse, no son canales independientes, pues se solapan parcialmente entre ellos, de manera que solo existen tres canales totalmente independientes, el canal uno, el seis y el once.
*Gráfico creado por Michael Gauthier, publicado en Wikimedia Commons, bajo licencia Creative Commons Attribution-Share Alike 2.0 Unported
Como se puede apreciar en la gráfica anterior existe un fuerte solapamiento entre canales, quedando resumido éste en la siguiente tabla.

Canal	Frecuencia central	Rango de frecuencia	Canales solapados
1	2.412 GHz	2.401 GHz - 2.423 GHz	2,3,4,5
2	2.417 GHz	2.406 GHz - 2.428 GHz	1,3,4,5,6
3	2.422 GHz	2.411 GHz - 2.433 GHz	1,2,4,5,6,7
4	2.427 GHz	2.416 GHz - 2.438 GHz	1,2,3,5,6,7,8
5	2.432 GHz	2.421 GHz - 2.443 GHz	1,2,3,4,6,7,8,9
6	2.437 GHz	2.426 GHz - 2.448 GHz	2,3,4,5,7,8,9,10
7	2.442 GHz	2.431 GHz - 2.453 GHz	3,4,5,6,8,9,10,11
8	2.447 GHz	2.436 GHz - 2.458 GHz	4,5,6,7,9,10,11,12
9	2.452 GHz	2.441 GHz - 2.463 GHz	5,6,7,8,10,11,12,13
10	2.457 GHz	2.446 GHz -2.468 GHz	6,7,8,9,11,12,13,14
11	2.462 GHz	2.451 GHz - 2.473 GHz	7,8,9,10,12,13,14
12	2.467 GHz	2.456 GHz - 2.468 GHz	8,9,10,11,13,14
13	2.472 GHz	2.461 GHz - 2.483 GHz	9,10,11,12,14

14	2.484 GHz	2.473 GHz - 2.495 GHz	10,11,12,13

Recientemente se aprobó una nueva norma, la 802.11n, que permite mayores velocidades de transmisión y puede funcionar en la banda de 2,4 GHz. Es importante conocer que los equipos que funcionan bajo esta norma, consiguen esta mayor velocidad gracias al uso, entre otras estrategias, de canales con un ancho de 40 MHz. El uso de este ancho de banda implica la utilización de dos canales no solapados, como podía ser el 1 y el 6. Por la tabla anterior, vemos que solo quedaría libre sin solapamiento los canales 11 a 13, lo cual podría acomodar sin comparición de frecuencias, algún canal 802.11b o 802.11g pero no otro canal 802.11n.
Esto implica que no hay espacio en la banda de 2,4 GHz para acomodar dos canales de 802.11n que no se solapen. La consecuencia de esta circunstancia será que la existencia de dos o más equipos 802.11n provocará que parte o la totalidad de su canal solape, y por tanto genere y reciba interferencia de los otros equipos, reduciendo el ancho de banda. Así mismo la convivencia de estos equipos con otros Wi-Fi de normas anteriores que funcionen en la misma banda, será compleja, puesto que quedarán pocos canales libres sin solapamiento. Esto no quiere decir que no puedan funcionar conjuntamente, si no que interferirían entre ellos en cuanto exista solapamiento y el rendimiento de la red se reducirá.
En la banda de 2,4 GHz aparece otra circunstancia particular. El lector podrá comprobar que su microondas tiene una frecuencia de trabajo situada en la misma banda de frecuencias (con ligeras variaciones). Esto indica claramente que la frecuencia utilizada por las redes Wi-Fi de esta banda está en la el rango de la resonancia de las moléculas de agua y, tal como ocurre con las generadas por el magnetrón del microondas, será absorbida por todo objeto que contenga este elemento.
Así pues, como norma la señal será fuertemente absorbida por elementos como agua, madera, cartón, plantas, personas o animales, etc. en general, todo aquello que se caliente en un microondas. Esta es una de las razones por las que existe una normativa tan fuerte en la potencia de emisión (100mW), la cual pretende evitar causar daños a los organismos vivos. La otra razón de esta limitación es controlar el alcance de estos sistemas, ya que es una banda de uso libre, con una reducida potencia máxima de emisión se minimizan las interferencias y se permite la convivencia con otros sistemas existentes.
Otro problema de la banda de 2,4 GHz es que existen multitud de sistemas que emiten en esta banda: teléfonos inalámbricos, dispositivos bluetooth, centrales de alarma inalámbricas, microondas, ratones y cascos inalámbricos, etc. los cuales generan interferencias que reducirán el rendimiento de la comunicación. Se trata de una banda muy saturada, que por su temprana liberalización, ha sido profusamente utilizada por multitud de equipos
La banda de 5GHz fue liberalizada con posterioridad a la de 2,4GHz y aparecieron normas que hacen uso de ella; la 802.11a y, recientemente, la 802.11n.
La banda de 5 GHz ofrece 24 canales no solapados entre sí (aunque con diferencias entre países debido a la normativa diferente en cada región), lo cual es una gran ventaja sobre la banda de 2,4 GHz en la que solo existen tres canales sin solapamiento. Esto permite que sea más fácil evitar las interferencias entre equipos, pues es muy probable la existencia de un canal libre que nos permita la configuración del equipo sin entrar en conflicto con sus vecinos.
Añadido al mayor número de canales disponibles, el menor número de equipos electrónicos existentes que usan esta banda, comparativamente con la banda de los 2,4 GHz, hace que las interferencias sean potencialmente menores, y los puntos de acceso Wi-Fi que operen en esta frecuencia tendrán menos señales compitiendo por la misma porción del espectro.
Sin embargo, la banda de 5 GHz tiene problemas que hacen que su implantación sea mucho menor que la de 2,4 GHz. Por un lado la menor oferta de sistemas que hacen uso de esta banda, lo cual reduce la posibilidad de elección. Por otro lado, el peso del parque de equipos instalados, a los que normalmente se desea seguir dando servicio, y que, en la mayoría de los casos, sería extremadamente costoso substituir. Otro factor es el mayor coste los equipos de 5GHz. Aunque los procesos de fabricación se han ido abaratando, los equipos de radiofrecuencia son, como norma general, más costosos cuanto mayor es la frecuencia a la que trabajan. El consumo así mismo es mayor para equipos que trabajen a frecuencias más altas, lo cual influye en los equipos móviles negativamente, en los que la duración de la batería suele ser un dato crucial, y aunque la diferencia no sea objetivamente significativa, si puede ser decisiva desde el punto de vista publicitario y percepción por el usuario. Por último, la propagación radioeléctrica es más costosa cuanto mayor es la frecuencia, pues la absorción de la señal por el medio se incrementa, lo cual tiene como consecuencia un mayor consumo para un igual alcance, y en la práctica un menor alcance de ésta banda, en campo abierto, comparado con la de 2,4 GHz.
Este último punto es matizado en muchas ocasiones, pues la banda de 5 GHz no presenta la absorción por

parte del agua, que sí afecta a la de 2,4 GHz. Así pues en entornos húmedos, lluvia, niebla, arboles, cartón, etc. la absorción será menor y su comportamiento mejor que con la banda de 2,4 GHz.
En un futuro cercano, se prevé que la banda de 5 GHz tome mucha más relevancia debido a las ventajas antes expuestas, y sobre todo a la implantación de 802.11n que hará que el uso de esta banda sea mucho más positivo mostrando claramente sus ventajas.
Una característica general, que afecta a todas las transmisiones inalámbricas, es la reflexión de las ondas. Cualquier elemento metálico actuará como un espejo a las ondas, lo cual tendrá un doble efecto: bloqueará la transmisión y producirá un reflejo.
El bloqueo de la señal deberá ser tenido en cuenta pues podrá crear áreas sin cobertura, y por tanto sin acceso a la red Wi-Fi. Es un efecto fácil de ver y evaluar, aunque en muchas ocasiones no tan fácil de solventar.
La reflexión de señal es un efecto un tanto más complejo de evaluar y solventar. Los puntos de acceso habitualmente emiten omnidireccionalmente, con una cierta polarización en alguno de los sentidos, pero a no ser que estén destinados a algún uso específico (como la unión de edificios, en cuyo caso lo habitual es utilizar antenas direccionales con una mayor ganancia de señal) es deseable que la cobertura sea homogénea en todas direcciones lo cual provoca que el diseño de antenas se realice para que irradien igual en cualquier dirección.
La señal, por tanto, se propagara en dirección al cliente, pero así mismo en el resto de direcciones. Si en esas otras direcciones se encuentra con un material que no sea absorbente, si no que refleje la señal, puede resultar que al cliente le llegue una nueva señal producto de esa reflexión. El problema de dicha señal reflejada es que el camino recorrido no será igual en longitud y por tanto llegara con un cierto retraso con respecto a la señal directa y con un retraso o adelanto con respecto a otras señales reflejadas. El cliente detectara una señal que será la suma de las diversas señales que le llegan, tanto directas como reflejadas. Al estar estas retrasadas unas respecto a las otras, detectará una onda con una forma potencialmente muy diferente a la original. Se ve por tanto que las señales reflejadas se comportan como interferencias influyendo negativamente en el funcionamiento de la red inalámbrica.



El efecto de recibir varias señales, causado por la suma de la señal directa mas las reflejadas se denomina con el termino ingles “multipath” y es un problema común a toda comunicación por radiofrecuencia, pero que el caso de redes Wi-Fi es mas notorio dado que habitualmente son redes que se desarrollan en entornos de interior donde existen gran cantidad de obstáculos tanto arquitectónico como objetos que pueden provocar estas reflexiones.
Con el objeto de evitar este problema la acción más inmediata es buscar una nueva ubicación para el punto de acceso, pues es su situación espacial la que determinara los distintos reflejos y caminos que puede tomar la señal. No hay un método teórico para elegir la ubicación del punto de acceso, puesto que el cálculo de los diferentes caminos es inviable en la práctica y deberá hacerse de forma empírica mediante el proceso de prueba y error, ayudado de alguna herramienta de las que hablaremos en apartados posteriores.
Un sistema que se ha popularizado en los últimos tiempos, y más aun tras la adopción de la norma 802.11n que lo contempla como parte de la norma, es la inclusión de sistemas M.I.M.O. (Multiple Input Multiple Output, o, traducido libremente, sistemas de recepción y emisión múltiple) Estos sistemas disponen de varias antenas (no siempre visibles externamente) que permiten emitir y recibir desde diversos puntos, direcciones,.. lo cual, permite al sistema ser más robusto ante interferencias, rebotes de señal y alcanzar mayores distancias y

velocidades.
Es necesario tener en cuenta a que la identificación de elementos metálicos no es siempre tan simple como suele pensarse. Objetos como los cristales tintados (cuyo tinte se suele realizar con plomo, y no es necesario que el cristal sea totalmente oscuro, si no que una ligera coloración no siempre apreciable sin una observación detenida puede ser suficiente para bloquear una gran parte de la señal), muros prefabricados con aislante interior o placas metálicas ocultas, ladrillos confeccionados con barro con un alto contenido metálico, etc. pueden afectar notablemente la propagación de la señal o incluso bloquearla totalmente.
Al respecto de las interferencias, y con carácter general, no propietario en exclusiva de ninguna de las dos bandas, es una fuente muy importante cualquier elemento que pueda provocar una chispa eléctrica, la cual producirá una interferencia de amplio espectro. Así pues motores eléctricos, como los presentes en frigoríficos, fotocopiadoras, aires acondicionados, etc. son en ocasiones fuentes de interferencia, sobre todo en el arranque de estos, máxime si son de baja calidad o están deteriorados con el uso. Así mismo elementos de iluminación como los tubos fluorescentes en mal estado pueden provocar interferencias apreciables.

3 Tecnologías

3.1 802.11b

La norma 802.11b surgió como una evolución de la 802.11 en el año 1999, con el objetivo de solventar el problema de velocidad que esta presentaba. Con la adopción de esta nueva norma se popularizaron las redes Wi-Fi pues la velocidad que ofrece, aun estando lejos de la red cableada, la hace apta para los usos más comunes. Añadido a esto, los costes de fabricación disminuyeron y los equipos fueron asequibles para un gran número de empresas y particulares.
Trabaja en la banda de 2,4 GHz y permite obtener una velocidad de hasta 11 Mb/s.
La modulación y el sistema de transmisión de la señal, hace que los canales tengan forma de campana, con mayor amplitud de señal en la frecuencia central. Esto provoca que la señal que ”invade” los otros canales tenga menor frecuencia y la interferencia sea menor que en otras normas como la 802.11g, aunque no por ello la hace carecer de importancia.

3.2 802.11a

La norma 802.11a define el funcionamiento de equipos en la banda de 5 GHz, permitiendo velocidades de hasta 54 Mb/s.
Fue aprobada el mismo año que la norma 802.11b pero, a pesar de las ventajas de la tecnología debido a la banda de frecuencia utilizada, su adopción ha sido muy lenta, y en nuestro país casi nula debido a varios problemas. En un principio la calidad de lo sistemas 802.11a presentó problemas en cuanto a fiabilidad, lo cual junto a un precio elevado debido al mayor coste y dificultad de fabricación de los elementos necesarios para construir estos sistemas, retrasó su implantación en un primer momento.
Particularmente en Europa se produjo un retraso en la adopción de esta norma por cuestiones de regulación del espectro electromagnético que en la fecha de la creación de la norma estaba asignado a usos privados. No fue hasta el año 2002 cuando la banda de 5 GHz se liberalizó permitiendo el uso de estos equipos en Europa.
Para esas fechas la base implantada de sistemas 802.11b hacía costosa la migración hacia 802.11a, ya que ambas normas no son compatibles. El mayor coste inicial de estas soluciones, el retraso en su salida al mercado, la menor disponibilidad de sistemas compatibles con esta norma y el coste de reciclado de equipos a la nueva norma fueron elementos disuasorios para la adopción de la nueva norma.
A esto se añadió el echo de que en un año estaría ratificada la nueva norma 802.11g, compatible con la base instalada y que proporciona la misma velocidad que la 802.11a.

3.3 802.11g

La norma 802.11g fue aprobada en el año 2003. Se trata de una tecnología que opera en la banda de los 2,4 GHz y proporciona una velocidad máxima de 54 Mb/s. La principal ventaja de esta tecnología reside en la mayor velocidad aportada y la compatibilidad con la base de equipos Wi-Fi conformes a la norma 802.11b ya instalados.
Los equipos 802.11g comparten los mismos canales que la norma 802.11b (cosa por otro lado necesaria si queremos aportar compatibilidad entre ambas tecnologías). Sin embargo, de forma nativa, la modulación utilizada es diferente, lo que le proporciona la mayor velocidad de transmisión. A causa de esta nueva modulación también se observa que la ocupación del espectro dentro del canal, en vez de tener forma de campana como en la norma 802.11b, tiene forma rectangular, lo cual implica que los bordes del canal, aquellos que solapan con los canales adyacentes, ya no tiene una menor potencia que el centro de éste, lo que tiene como consecuencia que interfieran con mayor intensidad con los otros canales puesto que las potencias son

comparables y es mas difícil discernir ambas señales.
Los puntos de acceso 802.11g permiten la operación un modo compatible 802.11b o en modo que solo acepten clientes 802.11g. En caso de que funcionen en modo compatible, aceptaran los dos tipos de modulaciones, tanto la correspondiente a 802.11b como la correspondiente a 802.11g. Así mismo se activará obligatoriamente el protocolo RTS/CTS.
Cuando en una celda existan clientes 802.11b, antes de emitir los clientes deberán utilizar el protocolo RTS/CTS utilizando la modulación correspondiente a 802.11b para asegurar que todos los clientes de ambas normas pueden recibir la información. Así pues, al querer emitir un cliente 802.11g se enviarán las tramas RTS/CTS en las que se marcará el tiempo que durará dicha transmisión. Los clientes 802.11b deberán esperar hasta transcurrido ese intervalo para poder emitir. Una vez que el cliente 802.11g ha reservado el canal, transmitirá la información utilizando su modulación nativa a la velocidad que le permite 802.11g y su situación actual. Los clientes 802.11b, durante la transmisión, no serán capaces de interpretar la información, interpretándola como ruido de fondo. Pero puesto que por las tramas RTS/CTS saben que han de esperar, y no tiene influencia que no puedan interpretar la transmisión pues no es información dirigida a ellos (pues en otro caso se habría utilizado su modulación para enviarles la información) se garantiza la convivencia de ambas normas.
Debido a la negociación que debe utilizarse, con tiempos mas lentos y compatible con 802.11b, la velocidad ofrecida por la celda decrece notablemente al trabajar en modo dual b/g y puesto que habrá intervalos de tiempo en los que se emitirá a 11 Mb/s para ofrecer compatibilidad para los clientes 802.11b la velocidad global para los clientes 802.11g se reducirá muy significativamente en cuanto haya trafico 802.11b en la celda.
Es de mencionar, que si la red Wi-Fi se compone de varias celdas, auque tan solo una de ellas tenga clientes 802.11b, todos los puntos de acceso funcionarán en modo compatible b/g pues los clientes pueden tener movilidad y pasar de la zona de cobertura de un punto de acceso al adyacente, lo cual provocara un menor rendimiento en toda la red, no solo en la celda con clientes 802.11b.
Es por estas razones por lo que resulta recomendable evitar en la medida de lo posible el modo de compatibilidad b/g y fijar el modo puro 802.11g si en la red no se ha de dar servicio a clientes 802.11b.

3.4 802.11n

La norma 802.11n fue publicada en el año 2007, con el objeto de dar mayor velocidad que las existentes hasta el momento, pasando de 54 Mb/s a unos teóricos 600 Mb/s.
Sin embargo a día de hoy lo normal son 300 Mb/s, existiendo algún sistema que llega hasta los 450 Mb/s, no siendo lo habitual. Pero la norma contempla la posibilidad y los medios para alcanzar velocidades mayores, con lo que es de esperar que en los equipos disponibles vaya acercándose a los 600 Mb/s en un futuro cercano.
Se obliga a tener dispersión espacia, utilizando tecnología MIMO, lo cual, junto con el resto de características de esta norma, permite un mayor alcance que el las normas anteriores. No resulta posible calcular dicho alcance de forma general, pues depende fuertemente de la configuración de las radios y antenas de los equipos, y existen diseños muy diversos.
La norma 802.11n ofrece la posibilidad de funcionar en ambas bandas, tanto en 2,4 GHz como en 5 GHz. Una de las grandes ventajas de la nueva norma es la compatibilidad con las normas anteriores lo cual posibilita la integración de sistemas nuevos en redes ya existentes y una migración sencilla y económica.
Actualmente hay una gran oferta de sistemas con posibilidades de conexión Wi-Fi 802.11n en 2,4 GHz, pero pocos que soporten la banda de 5 GHz o proporcione conexión dual. El menor coste y la compatibilidad con los sistemas Wi-Fi anteriores que funcionan en la banda de 2,4 GHz causo esta tendencia del mercado.
Para conseguir esta mayor velocidad, los equipos 802.11n siguen dos estrategias: un mayor ancho de banda del canal y uso de la tecnología MIMO con división por multiplexación espacial (SDM).
El ancho de banda que ocupa un canal en 802.11n pasa de los 20 MHz que ocupaban los sistemas anteriores, a 40 MHz. Esto no es un problema en 5GHz, donde los canales no se solapaban, pero en 2,4 GHz, un canal de 40 MHz ocupa el 82% de la banda disponible. Esto implica que no podrán coexistir dos canales 802.11n sin solapamiento en 2,4 GHz y que este solapamiento abarcará ademas la mayoría del canal. Incluso con sistemas Wi-Fi de otras normas o equipos no Wi-Fi que emitan en esta frecuencia (como Bluetooth, teléfonos inalámbricos,…) el espectro libre será mínimo, quedando casi asegurada la interferencia con el resto de sistemas.
La compatibilidad con sistemas 802.11a/b/g puede ser realizada en dos modos: encapsulando la transmisión en los canales de 20 MHz o utilizando un canal de 40 MHz.
Encapsulando la transmisión en los canales de 20 Hz, la transmisión será siempre encapsulada en 802.11a u 802.11g. Esta encapsulación propiciará que los propios medios de protección de las normas a/g sean

suficientes para la protección de los dos canales que utilizará el terminal 802.11n, pero en presencia de un terminal 802.11b será necesaria la utilización del protocolo RTS/CTS, al igual que debían hacerlo los equipos 802.11g, para asegurar una transmisión ordenada.
Si se opta por la emisión en un canal de 40 MHz en entornos mixtos, será imprescindible que los clientes 802.11n utilicen el protocolo RTS/CTS en cada uno de los dos canales de 20 MHz, correspondientes a las normas 802.11b/g, que conforman en canal de 40 MHz, para asegurarse no entrara en conflicto la transmisión en ninguno de los dos subcanales con otros sistemas que pudieran estar transmitiendo.
Al igual que ocurría con el modo de compatibilidad que presentaba la norma 802.11g para la norma 802.11b, aquí también se experimentará una reducción significativa de velocidad al mezclar distintas normas en una red.
La otra estrategia que sigue la norma 802.11n para conseguir mayor velocidad es el uso de tecnología MIMO con dispersión por separación espacial (SDM). Los equipos 802.11n disponen siempre de varias antenas para transmitir y otras tantas para recibir. Lo sistemas son capaces de emitir un flujo de datos diferente por cada antena, permitiendo así una mayor velocidad de global transmisión. Esta tecnología precisa de circuitería específica por cada antena, en concreto un emisor de radio y un conversión analógico/digital independiente, lo que redunda en un mayor coste y complejidad técnica. Esta es la razón de que existan varias configuraciones de antenas, dependiendo del equipo seleccionado.
El número de flujos de datos simultáneos que se pueden emitir está limitado por el número de antenas disponibles en ambos lados, así pues si el equipo transmisor dispone de tres antenas emisoras pero el destino solo de dos receptoras, la comunicación solo podrá efectuarse con dos flujos de datos independientes.
Las radios limitan el número de antenas y flujos de datos que pueden utilizarse, debido a un diseño seleccionado en base a la dificultad técnica y el coste. El tipo de radio que incorpora un equipo se designa con la siguiente nomenclatura “a x b : c”. “a” indica el número máximo de antenas o canales de radiofrecuencia de emisión que la radio puede utilizar, “b” expresa el número máximo de antenas o canales de radiofrecuencia de recepción del que puede hacer uso el sistema y “c” indica el número máximo de flujos de datos que pueden ser usados. Así pues un sistema 3x2:2 podrá utilizar hasta tres antenas de transmisión, dos de recepción y dos flujos de datos independientes. Es importante interpretar éste dato puesto que las antenas no suelen ser visibles, y desde luego, los flujos de datos no lo son, y es importante para evaluar el rendimiento del sistema, sobre todo para no invertir en puntos de acceso muy capaces si los clientes no lo serán, o viceversa.
Actualmente las configuraciones mas habituales son 2x2:2, 2x3:2, 3x3:2 siendo el máximo previsto por la norma 4x4:4. Lo cual justifica la discrepancia entre la velocidad de los sistemas actuales (300 Mb/s) y la máxima prevista por la norma (600 Mb/s). Así mismo se ve que los sistemas que empiezan a salir con configuraciones 3x3:3, que deberían ser capaces de alcanzar 450 Mb/s, pero solo serán útiles si los clientes poseen la misma configuración, cosa que no es habitual de momento.
Se llama la atención al lector sobre el hecho de que es habitual sistemas con más antenas que flujos de datos. Esta configuración les permite tener una mayor diversidad espacial, no para alcanzar una mayor velocidad de comunicación, si no para obtener una mejor resistencia ante interferencias y proporcionar mayor alcance.
Con el objeto de incrementar la velocidad de transmisión, los sistemas 802.11n incluyen un concepto nuevo, no existente en las anteriores normas: la supertrama. Los equipos 802.11n no transmiten la información tal cual se les requiere, si no que la encapsulan en una trama mayor con el fin de optimizar la utilización de la radio. Esta característica, aun siendo teóricamente deseable, presenta diversos problemas en los equipos, pues han de almacenar la información que les llega para ser transmitida hasta que conforman la supertrama. Así mismo han de encajar los paquetes de información de manera eficiente en la supertrama y en la recepción, deben desempaquetarla. Esto supone una mayor demanda de los equipos 802.11n y una mayor potencia de proceso de la necesaria en generaciones anteriores, y es, así mismo, fuente de problemas en algunas implementaciones, no siendo extraño observar grandes diferencias en la velocidad de transmisión dependiendo del tipo de información transmitida, sobre todo para ciertos tamaños de paquetes o mezcla de tamaños, debido al proceso de empaquetado y desempaquetado y los algoritmos de optimización de este proceso.

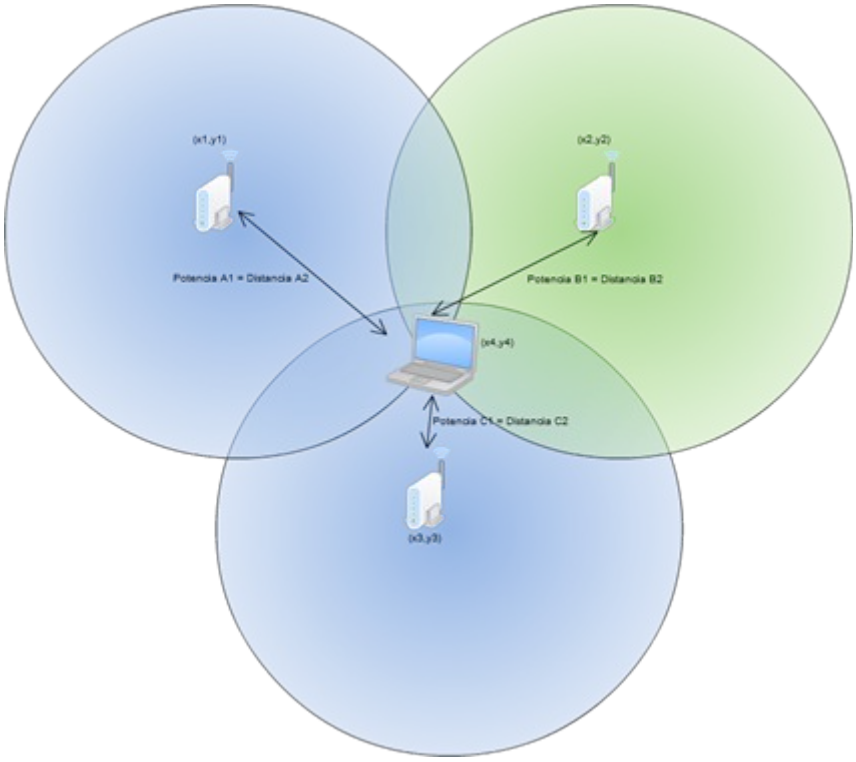
4 Sistemas de gestión Wi-Fi centralizados

Originalmente los sistemas Wi-Fi eran autónomos. Cada punto de acceso tenía toda la capacidad para crear la celda y gestionar los clientes a ella asociados y las comunicaciones entre estos, y entre ellos y la red cableada. Cuando las redes Wi-Fi pasaron de ser una solución puntual para solventar problemas concretos, y siempre de tamaño reducido, a grandes instalaciones complejas que soportan gran parte de las comunicaciones de una empresa, o incluso en algunos casos son en si mismo la fuente de ingresos (como puede ser el caso de los

hot-spots en aeropuertos), se vio la necesidad de disponer de sistemas de gestión centralizados.
La primera aparición de estos sistemas vino dado por el alto precio de los puntos de acceso en sus primeros tiempos. Para abaratar las grandes instalaciones, se tomó la decisión de hacer puntos de accesos menos inteligentes, y se transfirió esa inteligencia a un sistema centralizado. Es cierto que este sistema de control suele tener un coste elevado, pero si la instalación es grande, la reducción en el precio de cada punto de acceso lo compensa y el precio global es mas reducido que en el caso de una instalación realizada con puntos de acceso autónomos.
Con el tiempo, las redes Wi-Fi fueron soportando más servicios y se demando cada vez mas de ella, teniendo que aportar más opciones de configuración y funcionalidades que las hicieran aptas para las aplicaciones y servicios que de ellas hicieran uso. En instalaciones con un elevado número de puntos de acceso, la configuración manual de cada uno de ellos y su mantenimiento, así como la detección y corrección de errores se tornó compleja y el coste en tiempo y personal demasiado elevado.
Los sistemas de gestión centralizados tienen como objetivo paliar estos problemas y ofrecer funcionalidades añadidas.
Es cierto que no se pueden enumerar las funcionalidades de estos sistemas, puesto que no existe un modelo y cada fabricante toma la aproximación que le parece más conveniente, pero suele tener algunas características y funcionalidades básicas comunes.
Habitualmente el controlador se vende como un sistema independiente cerrado, pero internamente es siempre un ordenador con un software asociado y preinstalado, al cual el usuario no tiene acceso más que por la consola de configuración. En cualquier caso, los controladores se conectarán en la red Ethernet del cliente, desde la que detectarán a los puntos de acceso con los que sea compatible. Una vez detectados, realizará una configuración previa de estos y permitirá su gestión centralizada desde un solo punto, el controlador.
Dependiendo el fabricante, se implementarán distintas medidas para elegir que puntos de acceso han de ser gestionado, ya sea mediante una precofiguración de la dirección IP en el punto de acceso, o mediante algún tipo de filtrado y/o clave en el controlador. Una vez añadido el punto de acceso se le cargara automáticamente una configuración base, lo cual reduce los tiempos de instalación y minimiza los errores de configuración.
El objetivo general de esta fase es que la instalación de nuevos sistemas se simplifique.
Una vez realizado el despliegue inicial el controlador permitirá desde una sola consola configurar los distintos puntos de acceso, individualmente, por grupos o globalmente así como recibir alarmas asociadas al funcionamiento de ellos.
Como se ha comentado, la funcionalidad depende de cada fabricante, pero estas son algunas de las ofrecidas:

- Gestión centralizada: Una sola consola para gestionar los distintos puntos de acceso.
- Centralización de eventos: En instalaciones amplias, con un elevado numero de puntos de acceso, resulta inviable accede a cada uno de ellos para tener conocimiento de los eventos acontecidos y posteriormente relacionar los datos obtenidos de cada uno de ellos. El controlador permite automatizar este proceso con un ahorro en costes y un aumento en la fiabilidad de la red.
- Seguridad avanzada y centralizada: Permite gestionar la admisión de clientes Wi-Fi, definir perfiles, permitir acceso de éstos a distintas partes de la red o servicios dependiendo de su identidad, filtrado y detección de accesos, etc. Servicios que serán analizados más profundamente en capítulo posterior dedicado a la seguridad.
- Servicios de localización de clientes Wi-Fi: Puesto que el sistema de gestión centralizada controla todos los puntos de acceso, es capaz de obtener los datos de potencia de recepción que cada uno de ellos obtiene de cada uno de los clientes. Gracias a estos datos, relacionando los que distintos puntos de acceso obtienen de un mismo cliente, por triangulación, y conociendo previamente la localización de los puntos de acceso (datos que deberán ser introducidos manualmente previamente) el gestor será capaz de obtener la localización de los terminales.

  En la siguiente imagen se muestra como con tres puntos de acceso se puede deducir la distancia a ellos de un terminal, basándose en la potencia recibida, y con estas tres distancias, obtener la localización del cliente Wi-Fi.



- Autorización por localización: relacionado con el punto anterior, al tener conocimiento de la localización de los clientes, este servicio puede limitar el acceso a la red, solo a aquellos que es encuentren en las áreas permitidas.
- Respuesta automatizada ante fallos. Es posible, por ejemplo, que ante el fallo de un punto de acceso, el controlador, de forma automática active alguno que estuviera de reemplazo, o aumente la potencia de los circundantes para aumente su cobertura y cubrir el área que se quedo sin servicio.
- Gestión de la calidad de servicio: Puede priorizar, penar o controlar el tráfico de ciertas aplicaciones, servicios o usuarios.
- Tunelización: Es posible ofrecer el servicio de que los datos de la red Wi-Fi no sean inyectados a la red cableada directamente por el punto de acceso, si no que se genere un túnel entre este y el gestor centralizado. De esta manera se permite que el gestor pueda controlar los datos del cliente realizando sobre ellos funciones como priorización, filtrado y monitorización.
- Gestión de estructuras de red “mesh”: La incorporación de un gestor permitirá la elección de forma automática de los enlaces atendiendo a la calidad de estos, de manera que se optimicen los caminos y por tanto el rendimiento y fiabilidad. Además es posible que el gestor, ante el fallo de un punto de acceso o un enlace, recomponga de forma automática la arquitectura de la malla de forma que la comunicación se mantenga

5 Enlaces inalámbricos (WDS)

Una funcionalidad ofrecida por muchos puntos de acceso es la posibilidad de realizar enlaces inalámbricos entre dos de ellos, con el objetivo principal de unir dos redes, y en algunos casos, para proporcionar cobertura inalámbrica en puntos donde no hay acceso a la red cableada, sin renunciar a la comunicación con esta.

El sistema para realizar este tipo de enlace no esta estandarizado, existiendo multitud de soluciones propietarias, cada una con sus virtudes y defectos, aunque los principios básicos de funcionamiento son similares. Sin embargo hay un método de comunicación que aun no teniendo certificación de la Wi-Fi Alliance ni de ningún otro organismo es ampliamente utilizado. Hay que tener en cuenta sin embargo, que al no tener ninguna certificación, los sistemas que utilicen este protocolo no serán en la mayoría de los casos compatibles entre si, y en muchos ni tan siquiera entre distintos modelos de pertenecientes al mismo fabricante.

El método referido es el Wireless Distribution System (WDS). La meta de este protocolo es permitir la interconexión de los puntos de acceso de una red 802.11 sin necesidad de estar conectados a una red cableada, preservando la dirección MAC (equivalente a la dirección Ethernet cuando la trama llegue a la red cableada) de cada uno de los clientes. La conservación de la dirección MAC de los clientes provoca que el enlace WDS sea percibido por el resto de los equipos como un cable que no influye en la comunicación.

En una red WDS un punto de acceso puede ser configurado de manera que asuma uno de los siguientes tres

roles:

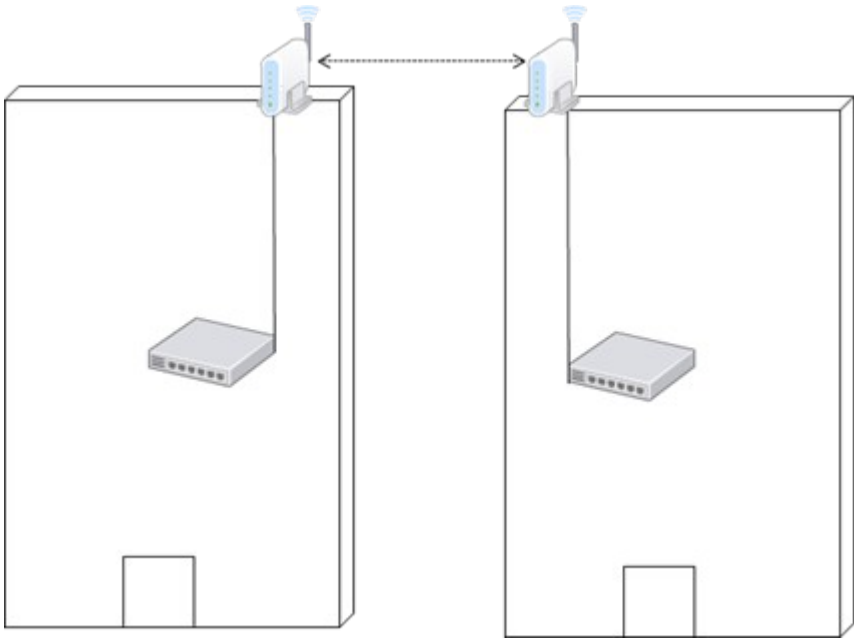
- Estación base principal: Es el punto de acceso que esta conectado a la red cableada. Podrá dar cobertura clientes locales y aceptará conexiones de estaciones base repetidoras o remotas.
- Estación base repetidora: Es aquella que recibe y tramita datos ente una estación base remota u otra estación base repetidora y una estación base principal u otra estación base repetidora. Por tanto realizará saltos intermedios y como su propio nombre indica repetirá la señal para alcanzar puntos más lejanos. Así mismo puede dar servicio a clientes inalámbricos locales.
- Estación base remota: Es aquella que da servicio a clientes locales y que tiene enlaces a estaciones base remotas o estaciones base principales, pero no es un salto intermedio para otras estaciones base.

Cuando un punto de acceso, funcionando en modo WDS con enlace a otros, da cobertura a clientes locales, hay que tener en cuenta que el ancho de banda disponible para los clientes locales pertenecientes a su celda se reduce a la mitad, pues toda transmisión proveniente del cliente ha de ser repetida por el enlace WDS, y viceversa, toda comunicación que provenga del resto de la red por el enlace WDS ha de ser repetida en la celda local, con lo que cada trama será transmitida por duplicado. Así pues, si la estación base puede ofrecer a sus clientes 54 Mb/s, la estación base repetidora que se conecte a ella podrá ofrecer tan solo 27 Mb/s, y a cada salto la velocidad ofrecida se seguirá reduciendo a la mitad.

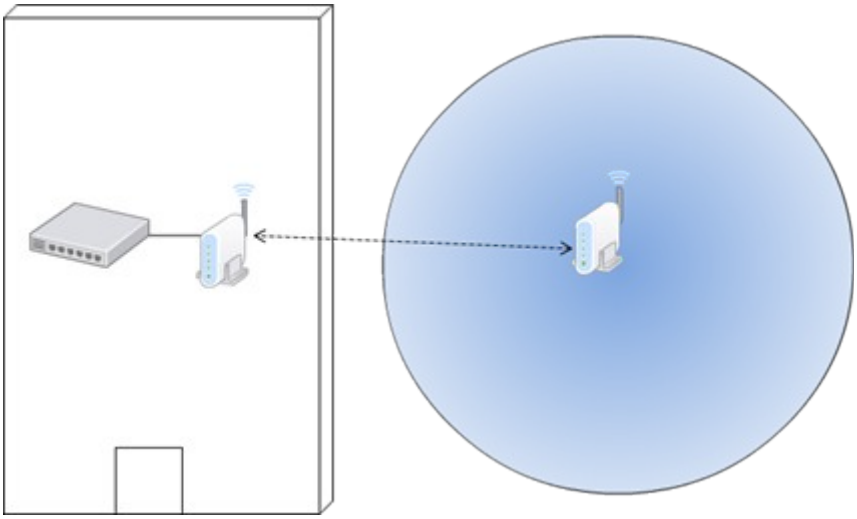
Dependiendo del fabricante, los puntos de acceso pueden tener la posibilidad de crear más de un enlace WDS, lo que les permitirá crear redes en malla (“mesh”). Así mismo hay productos, que para evitar la perdida de velocidad con cada salto, dotan a sus productos con dos módulos de radio, pudiendo así utilizar uno para crear el enlace con otras estaciones base y el segundo para dar cobertura local.

Como se puede ver por lo expuesto hasta ahora, las redes WDS pueden ser utilizadas en dos modos:

- Puente inalámbrico: En este modo el equipo no permite la conexión de clientes locales, no forma una celda de cobertura Wi-Fi. Se utiliza para crear enlaces punto a punto, por ejemplo entre edificios.



- Repetido inalámbrico: Con esta configuración el equipo, ademas de crear el enlace WDS con otras estaciones base, permite la conexión de clientes, creando una celda que será una extensión de la red Wi-Fi.



Los enlaces WDS usualmente presentan limitaciones en el campo de la seguridad. No están disponibles todas las opciones de encriptación y en los equipos mas económicos (aunque sorprendentemente no solamente en ellos) solo los métodos mas básicos de encriptación y autentificación están disponibles. Esto es peligroso, puesto que lo normal es que estos enlaces se efectúen a través de lugares públicos y espacios abiertos, porque son justamente estos espacios los que impiden el acceso a la red cableada y hace necesario un enlace inalámbrico. Así pues, si el equipo no implementa mecanismos fiables de encriptación, expondrá un punto de infusión y ataque a la red.

Es habitual que los equipos que soporten esta funcionalidad tengan la opción de conectar una antena exterior. En el caso de enlaces punto a punto no es deseable que la señal se irradie en todas las direcciones, si no que es preferible que se concentre en una dirección concreta, con lo que se gana seguridad y sobre todo alcance. Es por tanto posible, en muchos equipos, conectar antenas externas direccionales, tipo yagi o parabólicas, que proporcionan alcances mayores de los obtenidos con antenas convencionales, siendo en algunos casos de varios kilómetros.

6 Video, Voz y Datos

La mayor capacidad de las redes de datos y de los equipos, tanto ordenadores como sistemas especializados, así como su menor coste, ha hecho que se popularice el uso de tráfico multimedia. Actualmente es normal que las diferentes operadoras de telefonía ofrezcan lo que se suele llamar “triple play”, que designa el servicio de datos, voz y audio sobre redes IP.

Este servicio se ha popularizado en las redes privadas, siendo habitual que conviva la voz sobre IP (VoIP) con los datos en la misma red, debido a las ventajas en funcionalidad y reducción de costes que ofrece sobre la telefonía convencional.

Recientemente el servicio de video se ha desarrollado notablemente, tanto a nivel particular, como empresarial, y muy notablemente en centros de enseñanza donde aporta nuevas posibilidades docentes.

La transmisión de video y voz a través de una red IP convencional presenta una serie de retos, debido a las necesidades específicas de este tipo de tráfico, que fuerzan a que los elementos de red deban poseer ciertas características necesarias para el buen funcionamiento del servicio. Si esto es cierto en redes cableadas, lo es mucho mas en redes Wi-Fi puesto que en este ultimo caso, el medio es compartido, no solo con interferencias y elementos externos, si no con el resto de los clientes.

A continuación se expondrán las distintas necesidades de cada uno de los tres tipos de tráfico, con el objeto de que el lector comprenda la problemática asociada y sea capaz de evaluar las estrategias que existen para intentar solventar o minimizar los problemas derivados de las peculiaridades de este tráfico.

6.1 Necesidades del tráfico de datos

La transmisión de datos, como pueden ser ficheros de un servidor, correo electrónico o páginas WEB, es un tráfico poco exigente. El servicio demanda la mayor velocidad de transmisión y la menor pérdida de paquetes posible.

Es cierto que en las redes Wi-Fi estos dos parámetros no son tan fáciles de optimizar como en las redes cableadas, pues las velocidades de transmisión son menores y siempre existe alguna interferencia externa, o simple colisión entre clientes (que como se vio, es posible que ocurra a pesar de las protecciones implementadas), lo que provocará alguna perdida.

El usuario lo que apreciará es la velocidad de acceso a los datos, pero a no ser que ésta se reduzca por debajo de un cierto umbral que la haga inaceptable, y ese umbral dependerá de la aplicación, no habrá una mayor exigencia.

6.2 Necesidades del tráfico de video

El tráfico de video es más exigente. Con respecto a la transmisión de datos, este tipo de tráfico añade requerimientos extra, los cuales están motivados porque el video ha de ser mostrado en el instante que corresponde. El hecho de que los datos lleguen mas despacio, en una pagina web influye en que tarde menos o mas en bajar, pero los fotogramas del video se han de mostrar cuando corresponden, o el video no será visionado de forma correcta, apreciándose artefactos, sonido deficiente, aceleraciones del vídeo, pausas, etc.

En general, a parte de una velocidad de transmisión mínima para poder transmitir en video con fiabilidad, y una falta de perdida de paquetes, hará falta un cumplimiento de otros parámetros como el jitter, latencia, duplicación y reordenación de paquetes y emisión en ráfagas.

Aunque no son conceptos propios de las redes Wi-Fi si no de cualquier comunicación en general, son ampliados por este tipo de redes y es necesario explicarlos para entender apartados posteriores.

El video, dependiendo de la codificación y la calidad de la imagen, demandará un ancho de banda mínimo, que deberá ser soportado por la red Wi-Fi para proporcionar un buen servicio. En caso de que la red no sea capaz de proporcionar esta velocidad, se perderá información al no poder ser enviada por la red, provocando perdida de paquetes.

La pérdida de paquetes, ya sea por causa de un tráfico excesivo para la red, por interferencias o cualquier otra causa, provocará video de calidad deficiente, mostrándose los típicos cuadros, cortes de sonido o chasquidos. Si no existen mecanismos de corrección de errores, y estos solo suelen implementarse en proveedores de televisión dada su complejidad y coste, cada paquete perdido se traducirá en un error apreciable por el usuario.

El jitter es la variación en el retardo o latencia de los paquetes. Si los paquetes no llegan con la misma cadencia, el sistema receptor ha de ser capaz de ofrecer un buffer (termino para designar capacidad de almacenaje de paquetes) para no perderlos cuando lleguen mas juntos de lo debido o de tener almacenados los suficientes paquetes para soportar una espera mayor en la recepción del siguiente paquete, cuando este demore su llegada más de lo esperado. De no ser así se producirán errores análogos a los ocurridos por las perdidas de paquetes en el caso de que se reciban mas paquetes de los que se pueden almacenar hasta que llegue el momento de mostrarlos, o congelaciones de imagen en el caso de que el retraso en la llegada de información no permita al sistema actualizar la imagen.

La latencia mide el tiempo que tarda un paquete en viajar desde el origen del video hasta el destino. No es muy importante en video a no ser que se emita un evento en directo y la simultaneidad sea importante, como es el caso de eventos deportivos. Pero en la mayoría de los casos no es un parámetro crítico para el video.

La duplicación y reordenación de paquetes es un fenómeno que sucede en las redes más habitualmente de lo que se cree, y en video es importante, pues si se produce y no se detecta, gracias a la inclusión de algún protocolo junto con los algoritmos pertinentes en los clientes, dará como resultado que se muestre información que no corresponde con el instante y fotograma en curso, con la consecuente degradación en la calidad de la imagen y sonido.

Las ráfagas son algo habitual en sistemas de comunicación que adolecen de congestión. Sucede cuando el equipo de red, en nuestro caso un punto de acceso o un cliente Wi-Fi, no puede enviar información la almacena temporalmente y la enviará de golpe cuando le sea posible, si no media ningún mecanismo de control. Esto provoca que el cliente reciba en una ráfaga mas información de la que debería, por lo que si los buffers no son del tamaño adecuado, tendremos el mismo efecto que en el jitter (De echo las ráfagas son una forma de jitter extremo, pues los paquetes no llegan con una cadencia constante, si no agrupados tras un periodo de parada o precediéndolo)

En la emisión de vídeo, cuando la difusión de este se realiza a varios clientes simultáneamente, es habitual un tipo de transmisión que recibe el nombre de multicast. En este tipo de emisión se transmite un paquete con una dirección especial que capturarán los clientes interesados en recibirlo, para lo cual se subscribirán a la recepción de dicho flujo de datos. Este método permite que solo se envíe un paquete, independientemente del número de clientes que deseen recibirlo, con el consiguiente ahorro de ancho de banda. Sin embargo, como contrapartida exige más a los elementos de red, que han de ser capaces de gestionar dicho tráfico de forma correcta, lo cual les demanda mayor capacidad de proceso y memoria así como implementar los algoritmos y protocolos adecuados.

Es interesante aquí llamar la atención sobre el hecho de que el video Flash (el utilizado por portales como youtube) tiene unas necesidades diferentes. Su método de transmisión y tratamiento difiere, pues es

transmitido como datos sobre una conexión TCP con todo lo que ello implica, y no como video y es precisamente esa diferente filosofía de transmisión lo que lo ha popularizado en Internet al hacerlo inmune a los parámetros antes mencionado, pero no apto para transmisiones simultaneas a diversos clientes, ni emisiones en tiempo real.

6.3 Necesidades del tráfico de voz

Las necesidades del tráfico de voz, en este caso voz sobre IP (VoIP), son análogas a la del video, puesto que se trata de un servicio que no permite perdida de información y que precisa de una temporización muy estricta.
Sin embargo, existen dos diferencias con respecto al servicio de video. La primera es que aunque es necesario que se garantice un acho de banda y que este dependerá del sistema de codificación de la voz que utilice el sistema, esta velocidad de transmisión será mucho menor que en caso del video.
La segunda diferencia a tener en cuenta es que la latencia es un parámetro importante para la voz. Si esta es alta, la red no será apta para conversaciones de voz, pues un retraso mínimo es percibido muy negativamente por los usuarios. Para ilustrar al lector, el efecto es el apreciado en las comunicaciones telefónicas por satélite, y la causa, la misma.

7 Wi-Fi y QoS

Las redes Wi-Fi, al ser redes inalámbricas de canal compartido entre todos los clientes de una celda, implementan controles de acceso al medio, necesarios para evitar colisiones e interferencias en caso de que más de un usuario emita al mismo tiempo, como ya se pudo ver en apartados anteriores. Estos mecanismos son el CSMA/CA y el RTS/CTS que se engloban dentro de lo que se denomina DCF (Distributed Coordination Function).
Sin embargo este sistema de control de acceso al medio no previene que un cliente pueda monopolizar el medio en mucha mayor medida que el resto, afectando al servicio en la celda e imposibilitando su utilización con algunas aplicaciones sensibles al retardo y el jitter.
Una primera solución a este problema viene de la mano de un sistema de control que recibe el nombre de PCF (Point Coordination Function). Dicho mecanismo solo es funcional en redes de tipo infraestructura, nunca en redes ad-hoc, pues será el punto de acceso el encargado de realizar dicho control. Cuando se activa el PCF, el tiempo que existe entre dos paquetes “beacon” (aquellos que usa el punto de acceso para anunciar su presencia y las características de la red) enviados por el punto de acceso, se divide en dos periodos CFP (Content Free Period) y CP (Content Period). Durante el periodo CFP el funcionamiento de la red es como se ha explicado hasta el momento a lo largo del documento, mientras que durante el CP, los clientes no emitirán por iniciativa propia, si no que el punto de acceso le enviará un paquete a cada usuario por turnos, dándoles la oportunidad de emitir. El cliente aprovechara la oportunidad para emitir o, si no tiene datos para enviar, responderá con un paquete indicándolo. Con este método se permite evitar el monopolio de un cliente, permitiendo a todos la emisión de datos con una frecuencia aceptable.
Sin embargo, este sistema no es capaz de diferenciar los tipos de tráfico, solo diferencia a los clientes, y tratará igual tanto a un cliente que deba transmitir video, como al que espere emitir datos o voz. Añadido a esta limitación, existen muy pocos sistemas en el mercado que implementen este método de control.
Las necesidades de los distintos tráficos, expuestas en el apartado anterior, hacen necesario que este sea gestionado de manera eficiente para que los servicios puedan ser ofrecidos con la calidad debida.
Puesto que cada servicio, cada tipo de tráfico, tiene unas necesidades diferentes, es preciso diferenciarlo y aplicarle un tratamiento individual acorde a sus requerimientos. Este proceso recibe el nombre de calidad de servicio y se referencia por las siglas QoS (Quality of Service).
La aplicación de políticas de QoS no solo proporciona la posibilidad de ofrecer datos, voz y videos con calidad, si no que aporta herramientas para priorizar tráficos, ya sea por la naturaleza de éste (priorizar web, sobre el correo, y todas sobre las transferencias de ficheros P2P), o por el origen (el tráfico de la dirección de un centro escolar podrá ser priorizado sobre el de los alumnos).
No es suficiente con disponer de ancho de banda suficiente. Un sistema que deba transmitir datos sensibles, como voz o video, debe de implementar necesariamente QoS. La razón es simple, si durante una transferencia de voz o video, se produce una descarga de datos, esta podría ocupar todo el ancho de banda disponible. De hecho, la misma naturaleza de la transferencia de datos suele hacer deseable que así sea, pues la descarga llevará menos tiempo. La red debería sacrificar paquetes de datos en favor de los de voz o video, pues los primeros tienen mecanismos de recuperación y la única consecuencia será una ralentización del servicio y no interrupción de éste, como pasaría si el sacrificio lo realizara el tráfico de voz o video.
Sin embargo el problema no surge solo en ese caso, pues aunque la descarga de datos no demande la velocidad máxima de transferencia, emitirá tráfico, y el dispositivo de red, en nuestro caso el punto de acceso o

el controlador de la red Wi-Fi, deberá tener mecanismos para decir que paquetes ha de emitir antes y/o con una cadencia fija, minimizando las perdidas, la latencia, el jitter, las ráfagas, etc.
Para conseguir este objetivo y minimizar los problemas en la transmisión de contenido multimedia, existieron protocolos propietarios, pero en un entorno como el de las redes Wi-Fi, donde es posible tener control sobre los puntos de acceso pero no sobre los clientes, donde suelen convivir distintos dispositivos y de distintos fabricantes, no resultaba funcional ni se obtenían los resultados deseados. Fue con la llegada del protocolo 802.11e y su respaldo por parte de la Wi-Fi Alliance con su certificación Wireless Multimedia Extension (WME), más conocida como Wi-Fi MultiMedia (WMM), cuando la QoS llego al mundo Wi-Fi.

7.1 802.11e (WMM)

Por lo expuesto en el punto anterior, surgió la necesidad de tener algún mecanismo, no solo para que todos los clientes pudieran transmitir sus datos eficientemente, si no también para priorizar la transmisión de los datos sensibles, razón por la cual se desarrolló la norma 802.11e.
La norma 802.11e clasifica el tráfico en cinco categorías, dependiendo las necesidades y características del tráfico. Estas categorías ordenadas de la más prioritaria a menos prioritaria son:

- Voz (AC_VO): A esta categoría pertenecerá el tráfico de Voz.
- Video (AC_VI): Categoría en la que se encuadrará el trafico de video que necesite prioridad, lo cual, en principio, debería excluir al video Flash.
- “Best Effort” (AC_BE): Tráfico que deberá transmitirse tan pronto como sea posible, tras atender a aquel que le sea mas prioritario. Tráfico de este tipo podría ser una sesión Telnet o de control remoto de un equipo, tráfico que aunque no sea tan crítico como los anteriores si será sensible a lentitud y perdidas, dando sensación al usuario de falta de respuesta.
- “Background” (AC_BK): Es el tráfico que no entra en ninguna de las otras categorías. Es el tráfico de fondo o de relleno, de aquellas aplicaciones que no necesitan un tratamiento especial, como puede ser correo electrónico, la trasferencia de ficheros o el acceso a páginas WEB.
- “Legacy DCF”: Esta no es realmente una categoría contemplada en la norma 802.11e, pero aun así es un grupo de tráfico que recibe un tratamiento diferente. Engloba a todo el tráfico que no tenga tratamiento prioritario, normalmente gestionado por equipos que no cumplen con la norma 802.11e y por tanto no se engloba en ninguna de las categorías que la norma prevé. Por esta razón, no tener indicación de la prioridad con que ha de ser tratado, será el menos prioritario de todos.

Esta norma amplia los sistemas de control existentes hasta el momento, DCF y PCF, con un nuevo esquema denominado HCF (Hybrid Coordination Function) que define dos métodos de acceso al canal para la emisión de datos, priorizando aquellos que mas sensibles sean: Enhanced Distributed Channel Access (EDCA) y HCF Controlled Channel Access (HCCA).
Ambos métodos tienen una base común, siendo el EDCA el más extendido y obligatorio para los sistemas certificados Wi-Fi y que soporten WMM. El método HCCA incorpora un mayor control del tráfico, pero su cumplimiento es opcional y a día de hoy esta menos extendido y es soportado por un número muy reducido de sistemas.

7.1.1 Enhanced Distributed Channel Access (EDCA)

Este método, de obligado cumplimiento para los equipos que posean la certificación WMM de la Wi-Fi Aliance, se basa en la variación de los temporizadores presentes en los controles estándar de las redes Wi-Fi.
Para comprender el funcionamiento, previamente será necesario conocer los mecanismos que regulan el momento de transmisión de los clientes y su acceso al medio.
Añadido a la regulación impuesta por los controles DCF (que a su vez se compone de los controles CSMA/CA y RTS/CTS), existe una regularización en el momento de acceso a la red, principalmente orientado a evitar la monopolización del canal por un terminal y minimizar el acceso simultáneo al canal de dos o más terminales.
Para ello, un cliente que ha transmitido datos, no podrá volver a transmitir hasta pasado un tiempo fijo, que recibe el nombre de Arbitration Inter-Frame Space (AIFS). Esta espera posibilita a otros sistemas tener la oportunidad ocupar el canal y transmitir, pues de otra forma una sola estación podría estar emitiendo continuamente no dando opción a otra a hacerlo pues siempre verían el canal ocupado y según el protocolo CSMA/CA no podrían transmitir para evitar colisiones.
Para minimizar la situación en que los terminales que deseen emitir comprueben la ocupación del canal simultáneamente y emitan colisionando, y lo que es mas importante, que entren en un bucle en el cual siempre comprueben la ocupación del canal y emitan a la vez, tras esperar el tiempo AIFS, realizarán una segunda espera, durante un tiempo aleatorio que recibe el nombre de Contention Window (CW). Este valor será obtenido como un tiempo aleatorio entre un valor máximo y uno mínimo fijado en la red. De manera que, dado

su carácter de aleatoriedad evitara en gran medida que dos terminales accedan al medio en el mismo instante.
La variante de la norma 802.11e basada en el algoritmo EDCA actúa sobre estos tiempos, AIFS, CW máximo y CW mínimo. En base a las cuatro categorías que contempla la norma, fija unos valores de tiempo AIFS menores para las más prioritarias con respecto a las menos prioritarias. Así mismo los valores de CW máximo y CW mínimo serán menores cuanto más prioritaria es la clase de tráfico. Todos estos valores, claramente serán menores que los valores adjudicados para el tráfico que no cumple con la 802.11e.
Puesto que los tiempos que ha de esperar el tráfico más prioritario para volver a transmitir, será menor que el tráfico menos prioritario, estadísticamente se favorecerá la transmisión del tráfico más sensible y perteneciente a una clase de mayor prioridad que el menos sensible.

7.1.2 HCF Controlled Channel Access (HCCA)

Este sistema de QoS sobre redes Wi-Fi es más avanzado que el EDCA y permite un mejor control del tráfico emitido en la red. Sin embargo se considera opcional dentro de la certificación Wi-Fi WMM. Su carácter no obligatorio, junto con la mayor complejidad de implementación hace que pocos puntos de acceso y clientes Wi-Fi lo implementen.
Se puede entender el HCCA como una variación mas elaborada del PCF. Un punto de acceso que cumpla con HCCA, enviará una trama a cada uno de los clientes de forma secuencial, interrogándolos con el objeto de saber si disponen de tráfico para enviar, al igual que en el protocolo PCF.
La diferencia consiste en que ante esta trama los clientes no responderán con un mensaje indicando que no disponen de tráfico para transmitir, o transmitiéndolo en caso contrarío, si no que informarán al punto de acceso de si disponen de tráfico, y que tipo de tráfico, es decir, cuanto tráfico en cada una de las categorías previstas por la norma 802.11e tienen esperando para ser enviado.
El punto de acceso, con el conocimiento del tipo de tráfico que tiene cada uno de los clientes, decidirá cual de ellos ha de transmitir. Así pues será el punto de acceso quien indicara a los clientes elegidos que pueden transmitir y el intervalo de tiempo que tienen para hacerlo. Con ello, al tener un director del tráfico con conocimiento y datos objetivos de decisión, se consigue una transmisión ordenada y que proporciona la calidad de servicio deseada.
Por su parte, los clientes deberán tener varias colas de espera, donde almacenarán los paquetes de cada una de las categorías por separado, para ser enviadas cuando el punto de acceso se lo indique. Así mismo deberán implementar un algoritmo de calidad que permita priorizar el tráfico de las diversas categorías y enviarlo de la forma adecuada cuando tenga posesión del canal.
Como puede verse este método de control de la calidad de servicio implica una mayor “inteligencia” en los dispositivos, lo que se traduce en procesadores mas potentes, mas memoria, mejor y mas elaborado software y todo en ello implica un mayor coste, lo cual motiva que no suela ser implementado en los dispositivos Wi-Fi de uso general.

7.2 Sistemas propietarios

Desde la aparición de la norma 802.11e y sobre todo desde la existencia de la certificación Wi-Fi WMM no existen sistemas propietarios Wi-Fi que implementen redes ad-hoc o del tipo infraestructura. Es lógico si tenemos en cuenta que tanto el punto de acceso como los clientes han de hablar el mismo protocolo, y es fácil controlar el punto de acceso que se instala, pero, en la mayoría de los casos, tener control sobre los clientes resultará imposible y estos serán de diversos fabricantes y por tanto incompatibles con sistemas propietarios.
El escenario cambia en los enlaces punto a punto, como la unión de edificios. En ese caso ambos extremos suelen implementarse con equipos del mismo fabricante, pues de otra forma lo más probable será que aparezcan problemas de incompatibilidades, pues como se comentó en el apartado de dedicado WDS, no hay un estándar con la certificación correspondiente.
Así mismo, este escenario permite muchas optimizaciones, pues no es necesario llevar un control de asociaciones de clientes, roaming, etc. De hecho, si la organización de la transmisión se realiza con un control duro, que podría ser similar al HCCA, podrían relajarse los protocolos de acceso al medio, con lo que se pueden obtener rendimientos mas elevados e implementar algoritmos de calidad de servicios propietarios más elaborados.
Cada fabricante tiene su estrategia y esta varia con las nuevas versiones de producto, pero parece razonable que se tienda a un modelo HCCA por su funcionalidad y existencia de normativa al respecto, teniendo en cuenta que en estos sistemas punto a punto el precio es un factor menos crítico.

8 Seguridad en redes Wi-Fi

La seguridad en las redes en general es una asignatura pendiente, de que tan solo recientemente se ha tomado conciencia. En las redes inalámbricas esta necesidad es mas patente, por sus propias características,

y forma parte del diseño de las redes Wi-Fi.
El mayor problema de seguridad de las redes Wi-Fi viene dado por su dispersión espacial. No está limitada a un área, a un cable o una fibra óptica, ni tienen puntos concretos de acceso o conexión, si no que se expande y es accesible desde cualquier punto dentro de su radio de cobertura. Esto hace muy vulnerables a las redes inalámbricas pues la seguridad física de dichas redes es difícil de asegurar.
La posibilidad del acceso o monitorización de los datos es una amenaza muy real. Es por esta razón que todos los equipos permiten la encriptación de las comunicaciones mediante diversos algoritmos, que permiten tanto autenticar a los usuarios para evitar accesos no autorizados, como evitar la captura del tráfico de la red por sistemas ajenos a esta.
Otra de las consecuencias de ser una red vía radio es la influencia de otras fuentes radioeléctricas, ya sean otras redes Wi-Fi, equipos radio que trabajen en la misma banda o aparatos de distinta índole que generen interferencias. Es por tanto posible la generación de una interferencia premeditada que bloquee la red Wi-Fi y evite el funcionamiento de esta.
Añadido a esto, existe al posibilidad de la realización de ataques de denegación de servicio (DoS), tanto los clásicos, comunes a todas las redes, como específicos de las redes Wi-Fi. Tanto ataques reales a los distintos protocolos de autentificación, como terminales que no cumplan con los tiempos y reglas de acceso impuestas por las normas Wi-Fi, pueden degradar o incluso parar totalmente el funcionamiento de una red Wi-Fi. Como ejemplo, existen en el mercado terminales, que relajan el cumplimiento de las temporizaciones tanto de AIFS como CW, acortándolas, con lo que se optimiza su funcionamiento al aumentar sus posibilidades de transmitir datos, pero entorpeciendo el del resto de los terminales que sí cumplen con la norma. No son equipos pensados para atacar redes, si no que se basa en una decisión comercial que tiene por objetivo conseguir, ante la percepción del usuario, un mejor funcionamiento del terminal propio frente a la competencia, a consta de ésta.
Cando se piensa en vulnerabilidad de una red Wi-Fi se considera, como lo hemos hecho hasta ahora, la posibilidad de que un cliente no autorizado acceda a datos de la red. Sin embargo existe otro peligro: la inclusión de un punto de acceso no autorizado en la red. Un atacante puede añadir un punto de acceso que anuncie el mismo nombre de red, confundiendo así a algunos clientes que se podrán llegar a conectar a el en vez de a la red legal. Dependiendo de la elaboración de la suplantación, el cliente puede llegar a revelar datos y claves importantes.
Para minimizar el peligro que supone la implementación de una red inalámbrica, existen una serie de normas básicas a tener en cuenta a la hora de configurar la red, tales como:

- Cambiar las configuraciones por defecto: En contra de lo que suele pensarse, son muchos los administradores de la red que no cambian la configuración fijada en fábrica. Parámetros como las calves y usuarios o el nombre de red se mantienen inalterados. Es cierto que la en la mayoría de las instalaciones se cambia el nombre de la red, pero algo tan importante como la clave de acceso del administrador, en muchos casos, se mantiene inalterada, provocando un punto de acceso simple para cualquier intruso.
- Activar encriptación: Es una de las prácticas claves y necesarias. Es el método básico y más inmediato de impedir accesos no autorizados a la red, así como capturas de tráfico y datos privados. Existen varios sistemas de encriptación que analizaremos en un punto posterior.
- Uso de claves “fuertes”: Puesto que es la llave a la red, las claves utilizadas han de ser suficientemente seguras y complejas de averiguar para asegurar la seguridad de la red. Es frecuente usar claves de solo letras, con palabras comunes y muy habitualmente referenciado a datos personales del administrador, como nombres de hijos, edades, etc. que hacen dicha clave fácil de averiguar.
- Desactivar el anuncio del nombre de red (SSID): Aunque no es viable en todos los casos, la desactivación del anuncio del nombre de la red es un elemento de seguridad añadido. Por un lado, impedirá al atacante identificar la naturaleza y propietario de la red, y por otro hará necesario introducir el nombre de la red manualmente para permitir la asociación a la red Wi-Fi, por lo que previamente deberá ser conocida por el atacante.
- Filtrados de direcciones MAC: En la mayoría de los puntos de acceso es posible especifica una lista de direcciones MAC que serán admitidas, siendo todas las demás rechazadas. La dirección MAC es una dirección de nivel 2 que lleva la tarjeta de red Wi-Fi grabada de fábrica (análoga a la dirección MAC-Ethernet). Por tanto, si se permite solo el acceso a las direcciones MAC pertenecientes a los equipos propios se impedirá que algún sistema externo pueda conectarse de forma accidental o premeditada. Sin embargo, hay que hacer notar que existen tarjetas de red que permiten el cambio de la dirección MAC, y en ese caso sería posible para un atacante de nuestra red, asignarle una

dirección válida de alguno de nuestros equipos y evitar esta medida de seguridad. No obstante para ello, el atacante, debería conocer la dirección MAC de alguno de nuestros equipos, lo cual si las medidas de seguridad física e informática están correctamente implementadas no resultará fácil.

- Uso de direcciones IP estáticas: No un problema real para un hacker con conocimientos, peor si dificulta el acceso a intrusos ocasionales. Es habitual tener en las redes Wi-Fi la asignación automática de direcciones IP, Gateway y DNS. La práctica de asignar las direcciones manualmente a los terminales inalámbricos tiene la ventaja de que el atacante ha de averiguar en primer lugar los datos de la red, y más importante, nos permite habilitar filtros de manera que solo las direcciones IP asignadas sean permitidas. En caso de que el atacante utilice alguna de las IP asignadas, eventualmente podrá ser detectado pues entrará en conflicto con los terminales legales.
- VLAN propia para la red Wi-Fi. Es interesante la implementación, en aquellos equipos que lo permitan, de una VLAN específica para la red Wi-Fi. Al ser una red insegura por su propia naturaleza, es recomendable mantenerla separada en todo momento de la red cableada. Así pues, si el punto de acceso, o el controlador asociado, es capaz de gestionar VLANs, mantener el tráfico proveniente de la red Wi-Fi en una VLAN distinta permitirá implementar mecanismos de seguridad y acceso suplementarios que controlen el acceso de los usuarios Wi-Fi a los datos de la red corporativa.
- Instalación de un Firewall: Relacionado con el punto anterior, el acceso de los clientes Wi-Fi a la red cableada debería ser gestionado por un Firewall, ya sea actuando de puente entre las correspondientes VLANs o como elemento físico de control, interponiéndose en flujo de tráfico Wi-Fi. En cualquier arquitectura, la inclusión de un firewall nos permitirá implementar políticas de acceso seguras y complejas que aseguren que, aunque algún intruso hubiera conseguido conectarse a la red inalámbrica, no progrese hasta tener acceso a datos sensibles.

Estas medidas, por sí mismas, correctamente implementadas proporcionan seguridad suficiente para entornos no sensibles. Sin embargo existe la posibilidad de aumentar la seguridad mediante técnicas avanzadas, parte de las cuales precisan de la participación de un controlador de puntos de acceso.

8.1 Métodos de encriptación

Las redes Wi-Fi incorporan la posibilidad de encriptar la comunicación. Es una práctica recomendable ya que al ser un medio inalámbrico, de no hacerlo seria muy simple capturar el tráfico que por ella circula y por tanto la captura, por personas no deseadas, de datos sensibles.

A lo largo del desarrollo de las redes Wi-Fi han ido surgiendo diferentes métodos de encriptación de las comunicaciones, evolución necesaria pues los distintos métodos han resultado ser vulnerables y ha sido necesario implementar algoritmos mas seguros que solventaran los problemas de los anteriores. Estos, a su vez, van demandando más recursos de los equipos que los implementan por lo que la solución adoptada será siempre un compromiso entre rendimiento y seguridad. Los métodos estándar disponibles se detallan a continuación.

- WAP: Al inicio de las redes Wi-Fi ya se vio que las redes inalámbricas tenían problemas de seguridad intrínsecos a su naturaleza. Por esta razón, dichas redes nacieron con la posibilidad de activar encriptación y accesos mediante claves, siendo WAP el primer método que se implementó. Las siglas WAP provienen del inglés Wired Equivalent Privacy (Privacidad equivalente al cable). Ya en el mismo nombre se observa cual era el objetivo de esta encriptación, dar a las redes inalámbricas la misma seguridad que existía en las redes cableadas. Sin embargo la implementación de este protocolo adolece de problemas de diseño, que hace que si un equipo se encuentra dentro del alcance de la red, pueda capturar los paquetes de esta, y con la suficiente cantidad de paquetes capturados se pueda averiguar la clave de la red, y por tanto tener acceso a ella. El proceso de captación de la clave de la red se puede hacer con herramientas públicas gratuitas y tan solo tarda unos pocos minutos.

  WAP permite claves de diversas longitudes de bits, lo cual teóricamente aumenta su seguridad, pero en la práctica, y debidos a los problemas existentes en la implementación de este protocolo, la única repercusión de utilizar una clave mas larga es que aumenta el tiempo necesario para averiguar la clave de la red, pero esta sigue siendo vulnerable.

  Dentro de WEP se reconocen dos métodos de autentificación de usuarios: Open System y Shared Key.

  El método denominado Open System no implementa realmente autentificación. El punto de acceso permitirá que se una cualquier cliente, aunque posteriormente se obligará a que toda comunicación de datos sea codificada según el algoritmo dictado por WEP.

Por el contrario Shared Key dicta que los clientes tendrán que utilizar su clave WEP para autentificarse con el punto de acceso y solo aquellos que tengan las credenciales correctas serán admitidos por el punto de acceso como clientes.
En la práctica es recomendable utilizar autentificación Shared Key, pues Open System no proporciona realmente una autentificación de los clientes, solo encriptación de las comunicaciones, y aunque sería suficiente para preservar los datos, expone al punto de acceso a ataques de denegación de servicio (DoS).
Este protocolo no implementa ninguna gestión de claves. La clave utilizada es compartida por el punto de acceso y todos los clientes y debe ser distribuida a estos manualmente. Una consecuencia de ello es que con tener acceso a un solo equipo, se tiene la clave que compromete a todos los de la red.
Actualmente, por los problemas descritos se aconseja utilizar algún otro método de los disponibles, recurriendo solo a este sistema si no existiera ninguna alternativa viable y procurando acompañarlo de algún otro protocolo de encriptación general como puede ser IPsec o SSL.

- WPAv1: El protocolo de seguridad WPA (Wi-Fi Protected Access) fue desarrollado por la Wi-Fi Alliance como respuesta a los fallos de seguridad detectados en WAP. Sin embargo, la seguridad proporcionada por este nuevo protocolo, se demostró que podía ser rota si se capturaban los paquetes que intercambian el punto de acceso y el cliente durante el proceso de autentificación. Con esa información, si la clave es corta y sencilla, lo cual, aunque no debiera, suele ser lo mas normal, se puede averiguar la clave y por tanto acceder a los datos de la red. También se detectaron puntos de inseguridad en el protocolo que, aunque a día de hoy no han sido explotados por herramientas públicas, no se descarta que aparezca el software necesario para aprovechar dicha vulnerabilidad.
  WPA incorpora varios sistemas de autentificación y encriptación que aportan seguridad extra, entre los que cabe destacar:
  - TKIP: Siglas de Temporal Key Integrity Protocol, se basa en un sistema de verificación de integridad del paquete, es decir, que este no ha sido alterado durante la transmisión, y el uso de una clave que varía durante la comunicación, con lo que se solucionan problemas de WAP, pues la clave variará en menor tiempo y número de paquetes de los que se necesitan para averiguarla, por lo que no se dispondrá de información suficiente para hacerlo, y aunque se llegara a obtener esta, ya no sería válida para la comunicación en curso, pues la clave habría cambiado.
  - AES: Algoritmo de encriptación mas seguro que TKIP, cuya implementación no es obligatoria en sistemas WPAv1. Como contrapartida a esta mayor seguridad, demanda una mayor capacidad de proceso por parte de los puntos de acceso y los clientes. No obstante debería ser elegido, si es posible, ante TKIP.
  - EAP: Es un protocolo de autentificación y encriptación que va asociado al protocolo 802.1x y que, por tanto, trabaja en conjunción con servidores de autentificación tipo RADIUS. Hace años se encontraron problemas de seguridad en el protocolo EAP, lo que desencadeno en nuevas variantes que, mediante el uso de protocolos de seguridad asociados, pretendían solventar los problemas descubiertos. De este proceso surgió lo que se llamo Extended EAP, con diferentes variantes. Es de destacar que alguna de estas variantes como EAP-LEAP tienen fallos conocidos y su seguridad puede ser evitada con herramientas públicas y gratuitas.
- WPAv2: Ante la detección de la existencia de una brecha en la seguridad del protocolo utilizado por WPAv1, la Wi-Fi Alliance desarrollo una segunda versión que corrige dicho problema. Esta segunda versión obliga a la implementación del protocolo de encriptación AES, siendo este de uso por defecto en la norma WPAv2.

Los protocolos WPA permiten la autentificación mediante una clave compartida entre cliente y punto de acceso, o haciendo uso de mecanismos mas elaborados mediante el uso de un servidor de credenciales. Originalmente ambos tipos de arquitectura no tenían un nombre normalizado, y solían recibir el nombre de WPA el que hacia uso de servidor centralizado y WPA-PSK el que hacia uso de clave compartida (que es el significado de PSK, Pre-shared Shared Key). Actualmente se ha normalizado el uso de los términos “personal” para el uso de clave compartida, y “Enterprise” a aquella que provee autentificación contra un servidor RADIUS mediante protocolo 802.1x.

8.2 Autentificación 802.1x

La norma 802.1x surgió como una respuesta a la necesidad de proporcionar seguridad a nivel de usuario. No es de uso exclusivo en redes Wi-Fi, pues de hecho fue creada para dar seguridad a redes Ethernet, pero se vio que podía ser un elemento importante para las redes Wi-Fi y se integro en estas.

El protocolo 802.1x utiliza para autentificación y encriptación el protocolo EAP, normalmente en alguna de las variantes Extended EAP y cuya preferencia dependerá del fabricante de los equipos.

En una arquitectura 802.1x existen siempre tres elementos (Se dan los términos ingleses pues son los que se utilizan mayoritariamente):

- Suplicant (Peticionario): Se designa por este término al cliente que desea acceder a una red e intenta autentificarse. En una red Wi-Fi es el cliente que desea conectar con el punto de acceso para entrar en la red.
- Authenticator (Autentificador): Es el equipo que recibe la petición de conexión del cliente y que por tanto ha de tramitar la autentificación de este. En el caso de las redes Wi-Fi este rol lo lleva a cabo el punto de acceso.
- Athenticator Server (Servidor de Autentificación): Es el equipo que mantiene y gestiona de forma centralizada las credenciales de los usuarios. Dicho servicio se implementa mediante un servidor RADIUS.

En la siguiente ilustración se puede observar la comunicación y relación existente entre los diferentes elementos

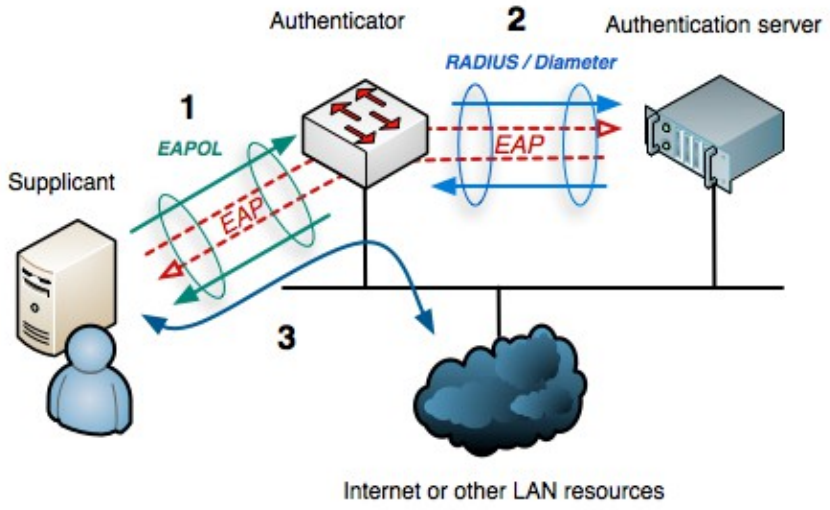


Imagen obtenida de Wikimedia Commons. Autor Arran Cudbard-Bell. Disponible bajo licencia GNU Free Documentation License.

En una red con autentificación 802.1x el funcionamiento ante la conexión de un cliente es como sigue:

- Cuando un cliente intenta conectarse a un punto de acceso, éste le responderá al cliente solicitando una autentificación del tipo 802.1x
- El cliente deberá enviar al punto de acceso las credenciales (claves, certificados…) que sirvan para autenticarse ante la red.
- El punto de acceso no posee los datos necesarios para gestionar dichas credenciales, por lo que hará uso del servidor de autentificación RADIUS. Al que le enviará las credenciales del cliente.
- El servidor RADIUS responderá al punto de acceso, indicándole el tipo de acceso que tiene el usuario en base a las credenciales enviadas.
- El punto de acceso, a partir de la respuesta del servidor RADIUS, denegará o concederá el acceso a la red del cliente, en las condiciones que el servidor RADIUS le haya notificado.

Este tipo de autentificación proporciona grandes ventajas deseables en redes con un número elevado de usuarios o que requieran un control sobre el uso de estos de la red.

La principal característica es que existe un solo punto donde almacenar todas las credenciales y usuarios y que este sistema será el responsable último de asignar el tipo de acceso de cada uno. Así pues, el servidor RADIUS podrá llevar a cabo labores AAA (Athentication, Authorization and Accounting, o lo que es lo mismo, Autentificación, Autorización y Registro) de forma centralizada lo que facilita y abarata el mantenimiento y control de la red y los usuarios.

Al disponer de un servidor RADIUS ya no se dispone de una sola clave para garantizar el acceso a cualquier

usuario de la red, si no que las credenciales dependerán de cada usuario, lo cual permitirá entre otras cosas levar un registro de los accesos a la red y la asignación de diferentes privilegios y niveles acceso dependiendo del usuario.
Así mismo se incrementa la seguridad del sistema, pues las claves ya no residen el punto de acceso, que es el extremo de la red, si no en un servidor dedicado cuyo nivel de seguridad es mayor. También se solventa el problema de robos de claves o credenciales, puesto que, al ser únicas por cada usuario, la sustracción de una solo será significativa para el usuario afectado, y no para el resto e usuarios de la red. Bastará con cambiar las credenciales de ese usuario o bloquearlo para restablecer la seguridad en la red, sin afectar en el proceso al resto de clientes como ocurre en las arquitecturas de clave única.

8.3 Seguridad mediante controlador de puntos de acceso

El uso de un controlador de puntos de acceso, no solo facilita la gestión y mantenimiento de una red Wi-Fi, si no que puede servir así mismo para aumentar su seguridad. Las posibilidades que proporciona un controlador dependerán del fabricante y modelo, pues no hay un estándar, siendo algunas de las más interesantes:

- Firewall (cortafuegos): Es habitual que los controladores implementen funcionalidades de firewall, que permitan controlar el tráfico que pasa de la red cableada a la red Wi-Fi, en base a direcciones de origen o destino, aplicaciones, servicios, etc. El firewall es también un elemento importante en la defensa ante ataques de denegación de servicio (DoS)
- Comunicación por túnel: Si se dispone de esta capacidad, el controlador creara un túnel con cada uno de los puntos de acceso. Dentro de ese túnel (normalmente un encapsulamiento IP o SSL) se transmitirá el tráfico de los clientes desde el punto de acceso al controlador. Esto permite que los clientes Wi-Fi, potencialmente inseguros, no tengan acceso a la red directamente, si no que todo el tráfico deberá pasar por el controlador, el cual, según las políticas asignadas a cada tráfico por la funcionalidad de firewall en éste incluida, denegará o permitirá el acceso a partes o toda la red.
- La tunelización del tráfico también proporciona la posibilidad de que los puntos de acceso estén conectados a segmentos de red diferentes, ya que de este modo el tráfico de los clientes siempre accederá a la red por el mismo punto de ésta, aquel al que este conectado el controlador. Además, si el túnel se realiza con un protocolo seguro como SSL, la comunicación entre los puntos de acceso y el consolador podrá hacerse a través de redes de terceros o incluso Internet, lo que permite la extensión de la red inalámbrica a zonas remotas atravesando redes inseguras sin exponer el trafico propio.
- Gestión por usuario: En conjunción con un servidor de autentificación, ya sea este interno al controlador o un servidor RADIUS externo, será posible asignar diferentes acceso a los usuarios en función de sus credenciales, de una manera más detallada y compleja que si el proceso lo llevara a cabo el punto de acceso. Así pues podrán asignarse a diversas redes, concederles accesos a diferentes servicios, etc.
- Gestión del ancho de banda: El controlador podrá ofrecer una funcionalidad por la cual regulará el ancho de banda disponible en función de la aplicación o usuario que desee hacer uso de ella. Así pues, podrá favorecerse el tráfico de voz sobre el de datos, evitando la saturación y bloqueo de la red Wi-Fi por aplicaciones abusivas como descargas de ficheros, o priorizar el tráfico de la dirección con respecto a los empleados o alumnos.
- Localización espacial: Un controlador puede ofrecer un servicio de localización. Puesto que tiene control de los diferentes puntos de acceso, puede monitorizar los clientes y la potencia de recepción de estos por cada uno de los puntos de acceso. Si el Controlador tiene conocimiento de la situación espacial de los puntos de acceso, triangulando la posición con respecto a los distintos puntos de acceso en base a la potencia recibida por estos, podrá obtener la posición del cliente. Aunque esta posición no sea completamente exacta, sí será importante a la hora de localizar equipos, no solo para la gestión física de estos, si no para encontrar a los atacantes o intrusos de una red.
- Limitación física del alcance de la red: Aunque la propagación de la señal de radiofrecuencia no se puede acotar de forma efectiva en el espacio, un controlador que disponga del servicio de localización, podrá denegar el acceso a la red a aquellos equipos cuya red se encuentre fuera de los limites de aquello que se le indique como zona de cobertura. Es de indicar que con este método los clientes fuera de la zona de cobertura de la red seguirán recibiendo la señal, con lo que podrían intentar otros medios de ataque a esta si la encriptación no es adecuada, pero no podrán conectarse a la red. Esta funcionalidad es útil cuando se quiere dar cobertura Wi-Fi a un edificio pero se desea prevenir que clientes presentes fuera del edificio pedan conectarse a esta como intrusos, por otra

parte difíciles de localizar al estar ubicados en zonas sobre las que no se tiene control físico.

8.4 WIPS (Wireless Intrusion Prevention System)

Un WIPS es un conjunto de equipos de red, que como su mismo nombre indica tienen como objetivo prevenir y detectar intrusiones en la red Wi-Fi (las siglas traducidas significan sistema de prevención de intrusión inalámbrica).

Un sistema WIPS siempre se compone de tres parte lógicas: los sensores que recogerán los datos de la red, el servidor que recolectará los datos de los distintos sensores, los analizara y relacionará, y la consola que utilizará el personal encargado de la seguridad de la red para acceder a los datos y visualizar las alarmas. Estos tres bloques lógicos no siempre están separados físicamente, pues es habitual que el servidor implemente un servidor WEB que sea el utilizado para acceder a sus datos y configuraciones a través de un navegador.

No siempre un WIPS es un sistema independiente, en algunos sistemas esta funcionalidad esta incluida en el controlador de puntos de acceso, que hará la función de servidor, que en conjunción con los puntos de acceso, que harán las funciones de sensores, pueden llevar a cabo parte de las funciones que realizaría un WIPS dedicado.

Un WIPS monitoriza el espectro radioeléctrico de la red Wi-Fi con el objeto de detectar ataques de diversa índole, como pueden ser:

- Puntos de acceso infiltrados: Uno de los ataques mas efectivos suele ser la infiltración de un punto de acceso, el cual puede asociar clientes de la red, obteniendo por tanto datos de estos, que transmitirán creyendo estar conectados a la red legal. También, en caso de conectarlo a la red cableada, puede ser un punto de entada a la red de cualquier intruso, que podrá acceder a distancia y por tanto será difícil de localizar.
- El WIPS puede detectar estos puntos de acceso infiltrados, usando técnicas simples como un conteo de los puntos de acceso que detecta, hasta algunas mas complejas que implican relacionar la dirección MAC de cada punto con la potencia que de ellos recibe. En caso de que se reciba información de la misma MAC con una potencia diferente, significaría que o bien se ha cambiado de localización el punto de acceso, lo cual no suele ser habitual, o que un nuevo punto de acceso, en una localización diferente, ha intentado suplantar al equipo legal.
- Una vez detectado el equipo infiltrado el WIPS lo notificará al administrador de la red, y en algunos sistemas permitirá habilitar contramedidas que bloqueen al punto de acceso infiltrado, por ejemplo, suplantando su dirección (MAC spoofing) o interfiriéndole.
- Ataques de denegación de servicio (DoS): Puesto que monitoriza la actividad es capaz de detectar un comportamiento inusual de los clientes, identificándolo, si es el caso, con ataques de denegación de servicio.
- Puntos de acceso mal configurados: Puede detectar conversaciones entre puntos de acceso y los clientes, sobre todo en el momento de la asociación y negociación de la encriptación a usar, detectando parámetros y configuraciones erróneas. Pero incluso de forma más temprana, mediante la información emitida en los paquetes de beacon puede avisar de fallos en la configuración de puntos de acceso.
- Clientes mal configurados: Un cliente cuyos intentos de conexión a la red sean denegados de forma repetitiva, será detectado como un fallo de configuración de dicho cliente, o dependiendo el caso, como el intento de conexión de un atacante, que, especialmente en los casos en que intente averiguar las claves de la red mediante métodos de fuerza bruta, provocara muchos intentos de conexión denegados por la red.
- Conexiones no autorizadas: Si en WIPS tiene una lista de los clientes autorizados, podrá detectar la conexión de los clientes no autorizados, ya sean meros intentos de conexión o clientes que han entrado con éxito en la red.
- Redes ad-hoc: Es muchos escenarios, una red ad-hoc es un punto de vulnerabilidad importante. La red gestionada del tiempo infraestructura puede disponer de diferentes mecanismos de protección, pero una red ad-hoc, puede ser creada involuntariamente, por un error de configuración, un troyano, etc. lo que crea un agujero de seguridad que puede tener consecuencias importantes. El WIPS, mediante la monitorización de los canales Wi-Fi, podrá detectar este tipo de redes y asociaciones, pudiendo indicar así mismo el equipo que crea dicha red y que esta creando la vulnerabilidad.
- Mac spoofing: recibe este nombre el ataque que consiste en suplantar la dirección MAC de otro equipo. Esto, en el caso de una red Wi-Fi, permite ganar el acceso a la red en aquellas que tengan implementada una autorización de clientes basada en sus direcciones de red. Un WIPS podrá

detectar dos señales diferentes con la misma dirección MAC, evidenciando este tipo de ataque.

- Ataques “evil twin”/”honeypot”: Este tipo de ataques consiste en realizar un phishing de un hotspot, es decir, insertar un punto de acceso que muestra al usuario el mismo interfaz que mostraría un hotspot (puntos de acceso a Internet publico que mediante un portal permiten acceso a servicios diversos, como por ejemplo los existentes en los aeropuertos para acceso a Internet mediante pago). Como consecuencia de esto, el cliente no notará diferencia entre el punto de acceso legal y el insertado, y procederá a hacer uso de este. El negocio para el atacante proviene de que los hotspot solicitan al cliente un usuario y clave para acceder al servicio o un pago en el momento mediante tarjeta de crédito, datos que el atacante podrá capturara para su posterior uso fraudulento.
- Ataques “man-in-the-midle”: Este es un tipo de ataque en el cual, el atacante se posiciona entre el cliente y el servicio que ha de utilizar. Así en una red Wi-Fi, este ataque consistiría en que el cliente se conecta al sistema del atacante, gracias a algún engaño por parte de este, y el sistema del atacante a su vez reenvía los datos al punto de acceso legal. De esta forma el cliente no ser percatará de que no esta conectado a la red directamente, pues todo parece funcionar perfectamente, pero el atacante tiene acceso a todos los datos del cliente, puesto que pasan por su sistema. El mayor peligro de este tipo de ataque es que el intruso puede variar la información que envía el cliente, substituyéndola por aquellos datos que para es sean más interesantes, no percatándose de ello ni el cliente ni la red o los servidores en caso de no existir sistemas de seguridad como un WIPS, IDS, IPS..

9 Herramientas

La implantación y mantenimiento de una red Wi-Fi precisa de diversas herramientas que nos permitan llevar a cabo dos tareas importantes: Estudios de cobertura y estudios de frecuencia.

Esta claro que es necesario conocer el alcance de las redes inalámbricas, la cobertura de los puntos de acceso y poder así decidir la ubicación idónea de ellos. Por otro lado, un estudio de frecuencias se perfila como una información útil, pues diversas interferencias, no provenientes del mundo Wi-Fi, peden afectar notoriamente al rendimiento de la red y puede condicionar la elección de canales, ubicaciones o equipamiento.

9.1 Estudios de cobertura

Previo a la implantación de una red Wi-Fi es necesario realizar un estudio de cobertura. Puesto que a priori no se puede saber la absorción y reflexiones de señal que producirán los distintos materiales de que están compuestas las paredes y mobiliario, es necesario un trabajo de campo previo de cara a tener datos objetivos que indiquen la mejor ubicación de los puntos de acceso que conformarán la red Wi-Fi.

Este estudio puede ser realizado de una manera rudimentaria con las propias herramientas que muchos fabricantes de tarjetas de red Wi-Fi incluyen con sus tarjetas, pero su funcionalidad resulta muy básica y hay herramientas gratuitas que proporcionan más datos

A la hora de hacer un estudio de cobertura completo, existe una herramienta gratuita que resulta muy interesante: Ekahau HeatMapper. Este software, permite mostrar la cobertura Wi-Fi en un plano, localizar todos los puntos de acceso y detectar las configuraciones de seguridad de las redes disponibles y cada uno de los puntos de acceso. La localización de la cobertura en un mapa es una funcionalidad muy interesante a la hora de comprobar o planificar la cobertura de una red.

Aunque los estudios de cobertura se suelen centrar solamente en la potencia recibida y, en algunos casos, la relación señal/ruido, es necesario en algunas ocasiones ir mas allá. En esos casos es interesante saber el rendimiento real que la red da en un punto. Esto puede ser realizado de forma gratuita con herramientas software como iPerf (de la que se hablara en un punto posterior), con la que podrá analizarse la mayor velocidad de transmisión real en un punto, pero existen así mismo algunas herramientas comerciales, creadas por compañías como por ejemplo VeriWave con su producto WaveDeploy, que permiten una evaluación del rendimiento según la aplicación, pudiendo realizarse estudios de cobertura no en base a potencia recibida si no a la calidad de video o voz que puede obtenerse en un punto, la velocidad de transferencia, etc.

9.2 Estudios de canales y frecuencias

Como se ha visto, distintos puntos de acceso Wi-Fi pueden emitir en un mismo canal, y en la banda de 2,4 GHz, aunque esto no suceda, los canales están fuertemente solapados, por lo que es importante tener una visión clara de que canales están ocupados y con que potencia se observa la señal en los puntos en los que deseamos crear nuestra celda Wi-Fi, datos que serán cruciales a la hora de elegir el canal que se configurará en el punto de acceso que genere dicha celda.

Existen varias posibilidades gratuitas para tener conocimiento de los canales ocupados en un punto, las redes detectadas, potencias recibidas por canal y porcentaje de utilización de estos. Algunos productos interesantes

son:

- NetStumbler: software que puede descargarse desdewww.netstumbler.comofrece información que suele ser suficiente para la mayoría de los usuarios. Se le conocen problemas de funcionamiento con Windows Vista, existiendo un derivado de este que los soluciona, llamado Vistumbler. Así mismo existe una versión reducida del software llamado MiniStumbler que puede correr sobre Windows CE.
- InSSIDer: Es una alternativa al NetStumbler, gratuito y desarrollado como un proyecto OpenSource, que añade la posibilidad de acoplarle un GPS. Los datos provenientes del interfaz Wi-Fi, junto con los del GPS, permiten generar ficheros KLM que podrán ser visualizados en Google Earth.
- Metageek ofrece gratuitamente una versión reducida de su software de análisis denominada Chanalyzer Lite, que muestra una lista completa de todos los datos de las redes observables junto con una gráfica de la situación de los canales y potencias emitidas. Es así mismo compatible con el analizador de espectro Wi-Spy fabricado por la misma empresa.

Uno de los problemas de la transmisión radio es la interacción con sistemas ajenos a la red que pueden influir negativamente con interferencias o ruido de fondo que degradarán la transmisión. El conocimiento de estos elementos permitirá elegir las frecuencias, canales y ubicación idónea de los sistemas.

Para el estudio de frecuencias no hay medios gratuitos, pues es necesario hardware que implemente un analizador de espectro, junto con el software que aporte los datos e informes necesarios. Aunque cada fabricante pueda elegir alguna característica particular y una diferente forma de presentar los datos, en general aportarán gráficas donde se muestre la potencia recibida en cada frecuencia de la banda estudiada. La forma de la gráfica dará información del tipo de equipo que la genera y la mayoría del software incluye alguna utilidad para ayudar a la interpretación de estas señales, permitiendo más fácilmente identificar equipos Wi-Fi, bluetooth, teléfonos inalámbricos, etc.

Aunque hay varios dispositivos disponibles en el mercado, cabe destacar como fabricantes de estos sistemas a compañías como Metageek, con su producto Chanalyzer Pro basado en un software y un analizador de espectro conectable al puerto USB denominado Wi-Spy, del tamaño de un pendrive y con capacidad de análisis de las bandas de 2,4 GHz y 5 GHzHzH. Otra opción es Airmagnet, la cual pertenece a Fluke Networks, que ofrece un sistema similar al anterior, basado en una tarjeta tipo CardBus en vez de un USB y también soportando las bandas de 2,4 GHz y 5 GHz, llamado AirMagnet Spectrum Analyzer.

9.3 Herramientas complementarias

Aunque no se trate de herramientas específicas del mundo Wi-Fi, si no que se puede utilizar para evaluar cualquier tipo de red, es interesante conocer las posibilidades de dos aplicaciones gratuitas: Wireshark e Iperf

Wireshark es un analizador de protocolos gratuito, que es un estándar de facto en el mundo de las redes y ampliamente utilizado por aficionados y profesionales de toda índole. Permite capturar el tráfico y analizarlo. No esta orientado al tráfico Wi-Fi como tal, es decir a la negociación autentificación, etc. si no que está orientado al tráfico de usuario. Puede resultar muy útil en muchos casos pues permite estudiar problemas como la asignación de direcciones a los clientes, direcciones MAC o IP inválidas o duplicadas, uso de la red global, por estación, por aplicación, etc. Con el fin de poder capturara así mismo el trafico propio de los protocolos Wi-Fi, se puede adquirir un hardware adicional llamado AirPcap, fabricado por CACE Technology, recientemente adquirida por Riverbed Technology, que se integra con Wireshark, aunque tanto nivel de detalle no suele ser necesario para el usuario normal.

Iperf es una aplicación gratuita de generación de tráfico. Permite evaluar el rendimiento de una red, obteniendo el tráfico máximo que es capaz de cursar. En el caso de las redes Wi-Fi es interesante conocer este dato pues dependiendo de las interferencias, solapamiento de canales y calidad de los equipos esta puede variar sustancialmente y no es directamente deducible de la potencia de recepción y la velocidad de conexión, pues estos valores solo nos proporcionan la velocidad máxima que podríamos alcanzar, no la que se alcanza en realidad.

10 Perspectivas de futuro

Actualmente la norma 802.11n se esta erigiendo como es estándar imperante, por un lado por su compatibilidad con las tecnologías anteriores, y por otro por el incremento en su rendimiento.

En un futuro cercano, es de esperar que se desarrolle esta tecnología hasta su completo potencial en las dos áreas que aun no están desarrolladas completamente.

Una de estas áreas son las bandas de conexión. Es inusual en los equipos actuales contar con tarjetas Wi-Fi que puedan operar en ambas bandas de frecuencia, estando la mayoría de ellas limitadas a la banda de 2,4 GHz. Dada la saturación de esta banda y las limitaciones impuesta al uso de canales no solapados, es lógico que en un futuro cercano muchos sistemas implementen ambas bandas y la banda de 5GHz sea cada vez

mas utilizada.
Por otro lado, los equipos actuales soportan hasta 300 Mb/s, lo que supone la mitad de la velocidad máxima prevista por la norma 802.11n. La limitación viene impuesta por los chips de radio disponibles, que solo soportan dos canales de radio independientes de los cuatro máximos que prevé la norma. Las mejoras tecnológicas y la rebaja en los costes de fabricación deberían popularizar equipos con tres y cuatro canales en un futuro cercano. De hecho, actualmente están apareciendo algunos puntos de acceso con rendimientos anunciados de 450 Mb/s, lo cual implica que ya hacen uso de sistemas capaces de gestionar tres canales de radio independientes. Es un avance significativo, que sin embargo ha de ser seguido por los fabricantes de tarjetas de red, pues en otro caso no será útil, pues la comunicación entre ambas partes viene limitada por el menor de los dos. No obstante la fuerza del mercado, que en la mayoría de los casos se mueve por la presión publicitaria, hará que estos sistemas se popularicen antes de que realmente sean útiles y forzarán a los fabricantes a dar el salto a los 450 Mb/s y posteriormente a los 600 Mb/s
Así mismo, el número de antenas deberá ir incrementándose hasta el máximo de cuatro. Actualmente ya hay muchos equipos que cuentan con tres antenas, lo cual les proporciona una dispersión espacial tal que les permite mayores alcances e inmunidad ante interferencias que la mayoría de los equipos que solo implementan dos antenas. Aumentar el número de antenas hasta cuatro permitirá una mayor fiabilidad en la comunicación y unos mejores rendimientos en circunstancias adversas.
No esta claro cual será la norma siguiente a la 802.11n. Hay que tener en cuenta que se tardaron siete años en completarla y hacerla publica, y aun hoy no esta totalmente desarrollada por los fabricantes. Es de esperar que subsista el tiempo suficiente como para llegar a su límite de rendimiento y rentabilizar la inversión en ella realizada.
Lo que se observa, independientemente de la norma utilizada, es que la tendencia del mercado se dirige hacia dispositivos cada vez mas pequeños y portátiles, con las implicaciones de batería y tiempo de autonomía que de ello se deriva. Es por eso que una de las grandes áreas en que se investiga es la optimización del consumo de estos sistemas, consiguiendo dispositivos que demandan menos potencia.
No obstante la investigación continúa. La necesidad de mayores velocidades de transmisión, sobre todo para la distribución de video en alta definición sin comprimir, ha propiciado la aparición de diversos grupo trabajando para al creación de normas que así lo permitan.
Parte de estas normas trabajarán en la banda de los 60 GHz, necesario para conseguir velocidades substancialmente mayores a 1 Gb/s. Sin embargo esta frecuencias permitirá cortas distancias de transmisión, normalmente limitadas a una misma habitación, por la alta absorción de las señales de esta frecuencias por los objetos y por el oxigeno.
La organización IEEE (creadora, entre otras muchas, de las normas 802), creó hace ya dos años dos grupos de investigación diferenciados, para desarrollar sistemas sobre bandas inferiores a los 6 GHz (que presumiblemente continuará las líneas de trabajo efectuadas hasta el momento) y un nuevo grupo para la investigación de bandas de alta frecuencia, en concreto la banda de los 60 GHz. El objetivo principal es conseguir la transmisión multi-gigabit en redes inalámbricas. Se perfilan dos normas principales, la 802.11ac, que será la sucesora del 802.11n, trabajará en 5 GHz y permitirá velocidades mayores a 1 Gb/s y cuya norma podría estar lista para finales del 2012 (lo cual no implica que salgan sistemas que hagan uso de ella para esas fechas, si no que la implementación real podría alargarse más en el tiempo) y la 802.11ad que trabajará en la banda de los 60GHz y permitirá transferencias mayores y posibilitará la transmisión de video en alta definición sin compresión a distancias muy cortas, habitualmente dentro de la misma habitación.
Paralelamente en el año 2009 se creo, bajo el nombre de Wireless Gibabit Alliance (WiGig Alliance), una asociación de empresas, con la participación de los principales fabricantes de hardware y software, como Micrososft, Nokia, Broadcom, Intel, etc. Dicha asociación promociona la creación de redes inalámbricas, funcionando en la banda de 60GHz, con compatibilidad con las redes actuales (mediante la incorporación de radios en 2,4GHz y 5 GHz). Proporcionará velocidades de entre 6 a 7Gb/s, funcionando en distancias cortas. Se espera la aparición de sistemas en breve siendo las estimaciones más optimistas para finales del 2011. Este grupo trabaja activamente para que la especificación sea parte de las norma IEEE y se integre en las normas Wi-Fi.
Existen dos últimas normas que no son aplicables para redes Wi-Fi, pero trabajan en la misma frecuencia que trabajarán las nuevas normas de las que acabamos de hablar, y es interesante conocer su existencia para preveer interferencias entre ellas así como los límites que está alcanzando la tecnología, lo cual nos da visión de a donde podrán llegar las redes inalámbricas, entre otras cosas porque la tecnología por ellas desarrollada podría derivar en usos paralelo en redes inalámbricas convencionales en un futuro.
Una de estas normas, orientada solo a video por radio, es la norma WirelssHD, que ya va por su especificación 2.0 y que permite en su primera versión la transmisión a 10 Gb/s y en la versión 2.0 hasta 28 Gb/s. Se utiliza

para conectar de forma inalámbrica dispositivos (ordenadores, reproductores de video,…) con monitores y televisiones que se encuentren en la misma habitación, existiendo ya dispositivos que incorporan esta tecnología.

La norma WHDI es análoga a la anterior, pero trabajando en la frecuencia de 5 GHz, permitiendo velocidades de hasta 3Gb/s a una distancia de 30 metros. Hay un número cada vez más elevado de dispositivos que lo incorporan y que ya están disponibles en el mercado, sobre todo del entorno informático, como proyectores, monitores, tarjetas de video, portátiles, etc.

Como se ve las perspectivas de futuro del las redes Wi-Fi prometen mayores velocidades, sobre todo para distancias cortas, pero como ocurre siempre al inicio de una nueva tecnología, aparecen nuevas normas que aun han de recorrer un camino hasta que una de ellas, o la combinación de ellas, se perfilen como el siguiente paso en la evolución de las redes inalámbricas. Lo que parece claro es que se bifurcará en redes Wi-Fi tal como las entendemos hoy en día, y una nueva variante de corto alcance y alta velocidad y, de forma más inmediata, en un futuro breve, se podrá disfrutar de la evolución de la norma 802.11n hasta alcanzar su pleno potencial, doblando las prestaciones que ofrece en estos momentos.