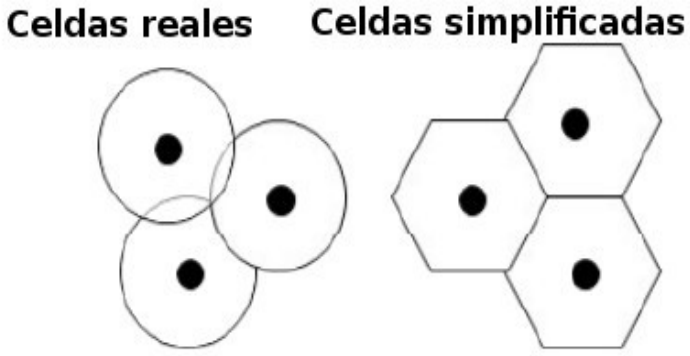
# UD9. WIFI

## Índice

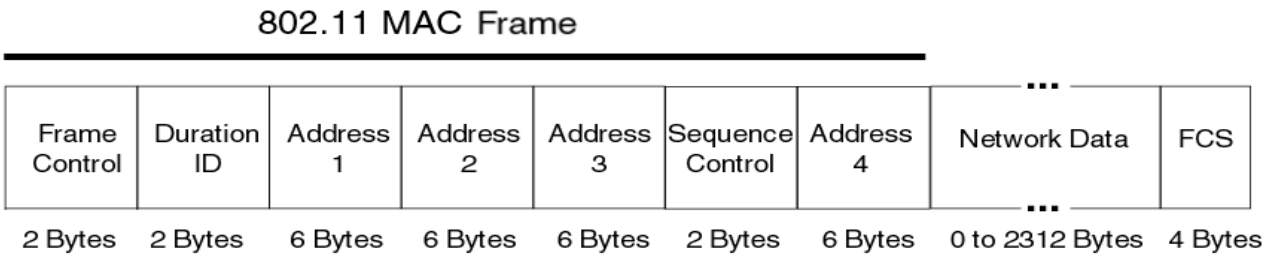
# Conexión y modos del conmutador

Las redes de telefonía móvil y otras redes inalámbricas similares están constituidas por un conjunto de estaciones cada una de las cuales tiene un área de cobertura. De esta forma, el territorio se divide en **celdas**, en teoría, de forma hexagonal, controladas cada una por una estación terrestre, que soportan un número limitado de llamadas. Cuando un usuario se encuentra en determinada célula, será atendido por su estación correspondiente. Pero si al desplazarse pasa a otra célula, entonces será otra estación la que le permita seguir manteniendo la conversación.




En las zonas limítrofes, las células se solapan, de forma que el usuario no pierda la cobertura cuando pasa de una a otra. Cada estación utiliza un rango de frecuencias específico y diferente del de las células que la rodean, que son adyacentes a ella, pues en caso contrario podrían producirse interferencias entre células. Células no adyacentes si pueden usar el mismo rango de frecuencias. El conjunto de todas las celdas de una red forman la zona de **cobertura**.

# Trama 802.11 (Wi-Fi)




**Cabecera 802.11**

- Dirección 1: Receptor de la trama en la red inalámbrica
- Dirección 2: Transmisor de la trama en la red inalámbrica
- Dirección 3: puede ser varias cosas, depende del caso
- Dirección 4: No se suele utilizar

El control de trama (Frame Control) tiene dos bits ‘Hacia’ y ‘Desde’ que significan:

| Hacia DS | Desde DS | Significado |
|---|---|---|
| 0 | 0 | Trama de estación a estación (red ‘ad hoc’) |
| 1 | 0 | Trama de estación hacia AP |
| 0 | 1 | Trama de AP hacia estación |
| 1 | 1 | Trama de AP hacia AP (DS inalámbrico) |

# Dispositivos

## Antenas

Una antena es un dispositivo (**conductor metálico**) diseñado con el objetivo de **emitir o recibir ondas electromagnéticas** hacia el espacio libre. Una antena transmisora transforma voltajes en ondas electromagnéticas, y una receptora realiza la función inversa.

Existe una gran diversidad de tipos de antenas. En unos casos deben expandir en lo posible la potencia radiada, es decir, no deben ser directivas o direccionales (ejemplo: una emisora de radio comercial o una estación base de teléfonos móviles), otras veces deben serlo para canalizar la potencia en una dirección y no interferir a otros servicios (antenas entre estaciones de radioenlaces). También es una antena la que está integrada en la computadora portátil para conectarse a las redes Wi-Fi.

### Diagramas de radiación

Es la representación gráfica de las características de radiación de una antena, en función de la dirección (coordenadas en azimut y elevación). Lo más habitual es **representar la densidad de potencia radiada**, aunque también se pueden encontrar diagramas de polarización o de fase.

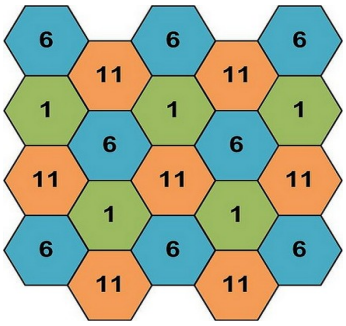

Atendiendo al diagrama de radiación, podemos hacer una clasificación general de los tipos de antena y podemos definir la **directividad de la antena (antena isotrópica, antena directiva, antena bidireccional, antena omnidireccional, ...)**

## Puntos de acceso (AP: Access Point)

Si deseamos crear una red Wi-Fi cuya cobertura esté soportada por varios puntos de acceso, deberemos de establecer los canales de los distintos puntos de acceso de forma que no se solapen. Canales Wi-Fi en 2,4 GHz

Existen 14 canales, aunque en Europa solo se utilizan 13.

Por ello se recomienda utilizar los canales 1, 6 y 11. También pueden usarse 2, 7 y 12. Otra posibilidad son 3, 8 y 13.




| Canal | Frecuecia (MHz) | Norte America | Japón | Mayor parte del mundo |
|---|---|---|---|---|
| 1 | 2412 | Yes | Yes | Yes |
| 2 | 2417 | Yes | Yes | Yes |
| 3 | 2422 | Yes | Yes | Yes |
| 4 | 2427 | Yes | Yes | Yes |
| 5 | 2432 | Yes | Yes | Yes |
| 6 | 2437 | Yes | Yes | Yes |
| 7 | 2442 | Yes | Yes | Yes |
| 8 | 2447 | Yes | Yes | Yes |
| 9 | 2452 | Yes | Yes | Yes |
| 10 | 2457 | Yes | Yes | Yes |
| 11 | 2462 | Yes | Yes | Yes |
| 12 | 2467 | No | Yes | Yes |
| 13 | 2472 | No | Yes | Yes |
| 14 | 2484 | No | 11b only | No |

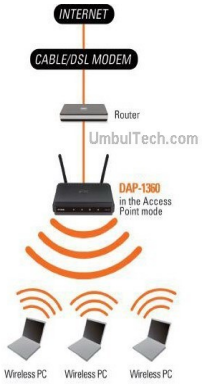
# Modos básicos de un AP

Un punto de acceso (AP) puede configurar de muchas maneras, según la funcionalidad que queramos proporcionarle. Los modos básicos son:

- Modo punto de acceso
- Modo repetidor
- Modo puente (bridge)

## Modo Punto de Acceso

En el modo de punto de acceso, los clientes deben utilizar el mismo SSID (nombre de red inalámbrica) y canal que el AP con el fin de conectarse. Si la seguridad inalámbrica está activada en el AP, será necesario que el cliente introduzca una contraseña para conectarse a la AP. En el modo de punto de acceso, múltiples clientes pueden conectarse al punto de acceso al mismo tiempo.



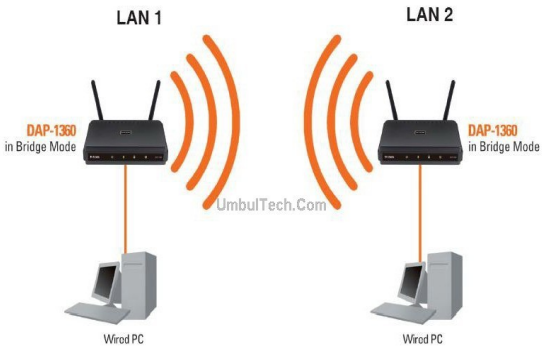

Wireless PCs Using the DAP-1360 as a Central Connection Point

## Modo Repetidor

En el modo de repetidor, el AP aumenta el alcance de la red inalámbrica mediante la ampliación de la cobertura inalámbrica de otro punto de acceso o router inalámbrico. Los puntos de acceso y router inalámbrico (si existiese) debe estar dentro del alcance del otro. Asegúrese de que todos los clientes, puntos de acceso y el router inalámbrico utilizan el mismo SSID (nombre de red inalámbrica) y el mismo canal.


## Modo Puente (Bridge)

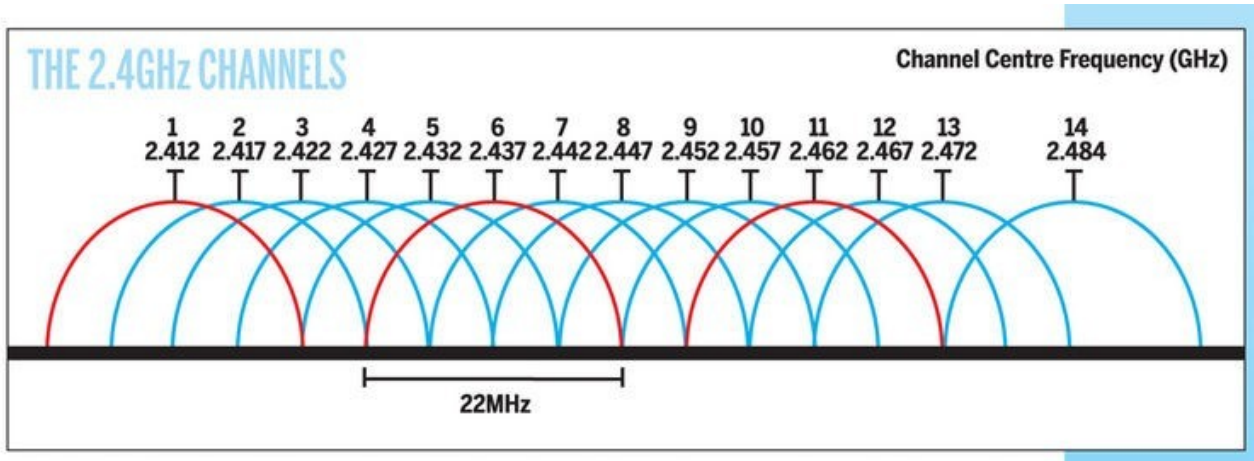
En el modo de puente, el AP se conectan dos LAN separadas que no pueden ser fácilmente conectadas entre sí mediante un cable. Por ejemplo, si hay dos LANs cableadas separadas por un pequeño patio, sería costoso enterrar los cables para la conexión entre las dos partes. Una mejor solución es utilizar dos AP para conectar de forma inalámbrica las dos LAN. En el modo de puente, ambas unidades AP no actuan como puntos de acceso.




Connecting Two Separate LANs Together Through Two DAP-1360 Units
(Wireless PCs Cannot Access the DAP-1360 Units)

# Estándares WIFI

| ESTÁNDAR | ANCHO DE BANDA MÁXIMO | BANDA DE FRECUENCIA | ALCANCE ESTIMADO |
|---|---|---|---|
| 802.11a | Hasta 54 Mbps | 5 GHz (canales de 20 MHz) | 35 m |
| 802.11b | Hasta 11 Mbps | 2,4 GHz (canales de 20 MHz) | 35 m |
| 802.11g | Hasta 54 Mbps | 2,4 GHz (canales de 20 MHz) | 38 m |
| 802.11n | Hasta 600 Mbps (150 Mbps por flujo/antena, 4 antenas máx.) | 2,4 / 5 GHz (canales de 20/40 MHz) | 70 m (*) |
| 802.11ac (Wi-Fi 5) | Hasta 3,5 Gbps (433 Mbps por flujo/antena, 8 antenas máx.) | 5 GHz (canales de hasta 160 MHz) | 36-42 m (*) |
| 802.11ax (Wi-Fi 6) | Hasta 9,6 Gbps (600 Mbps por flujo/antena) | 2,4 / 5 GHz (canales de hasta 160 MHz) | Mejor que Wi-Fi 5 (*) |




The 2.4GHz channels contain a vast amount of overlap, which is why some routers only allow you to choose from channels 1, 6 and 11. The use of channel 14 isn't permitted in the UK.

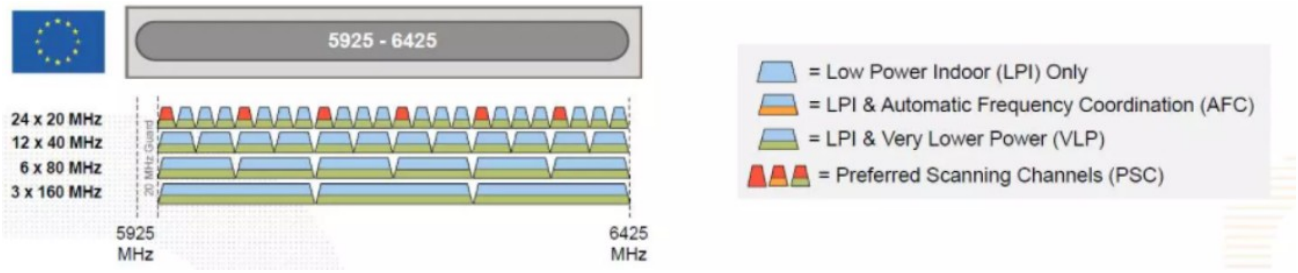
En Wifi 5 y 6 se usan agrupamientos de canales de 5GHz hasta formar canales de 160MHz de ancho de banda.

Al hacer esto se reduce el número de canales disponibles en toda la banda a un total de 8 de 40MHz, 4 de 80MHz o solo 2 de 160MHz


Las posibilidades de usar un canal ocupado son mayores mientras mayor ancho de banda tenga el agrupamiento de canales escogido. Sin embargo, al tener un ancho de banda mayor se permite una velocidad máxima teórica superior

En Wifi 6E (una mejora sobre wifi6 que trabaja también en torno a los 6GHz) se soluciona esto agregando 14 canales más de 80MHz mejorando su cobertura.

Con WIFI 6E tendermos 59 canales de 20MHz, 29 de 40MHz, 15 de 80MHz y 7 de 160MHz (En la UE tendremos 3 canales de 160MHz en dispositivos compatibles.

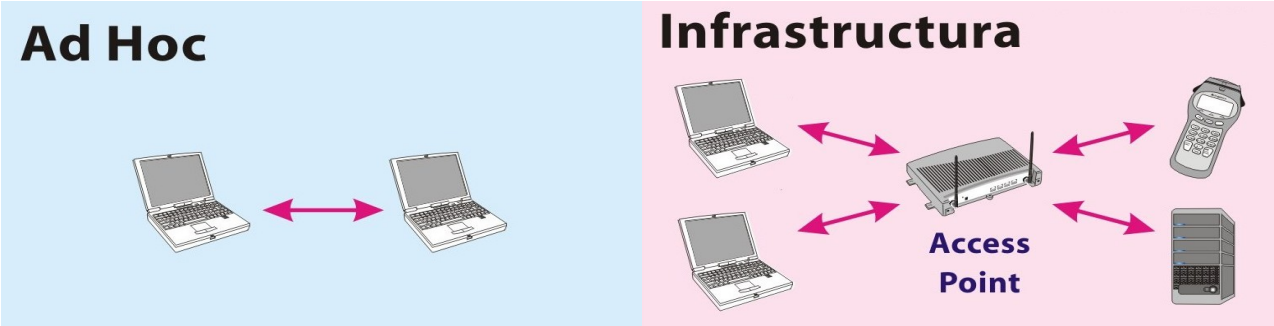



## MIMO

Multiple Input, Multiple Output nace con la 802.11n y desde entonces todos los puntos de acceso WIFI la incluye.

La tecnología permite el uso de más de una antena, interna o externa, para establecer más de un flujo de comunicación, mejorar la velocidad de acceso de las estaciones y el acceso simultáneo, así como permitir gestionar un mayor ancho de banda total.

# Interconexión



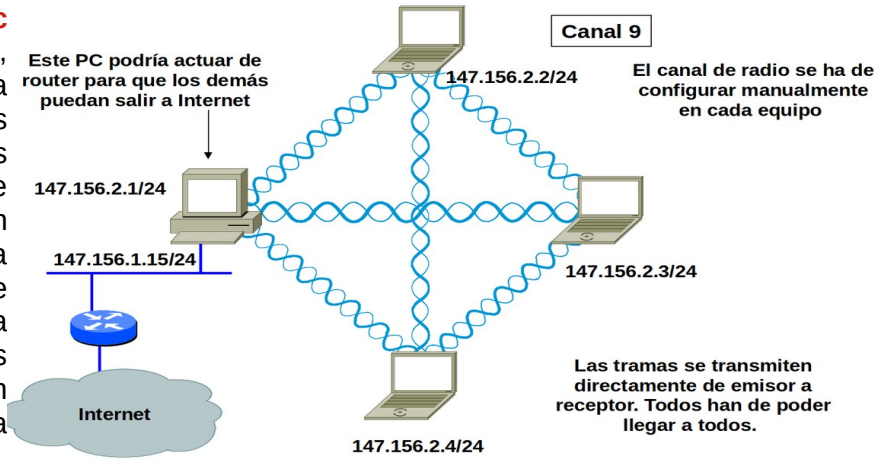

En las redes Wi-Fi siempre existe, como estructura básica, un gestor de la comunicación y una serie de clientes. Los clientes, escucharán siempre para detectar la presencia de uno o más gestores que les indicará, entre otros datos, el nombre de la red que gestionan, el canal a usar, la seguridad y algoritmos 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. Distinguimos:

- BSS (Basic Service Set): está formado por un AP y su área de cobertura.
- ESS (Extended Service Set): es un conjunto de dos o más BSS, es decir dos o más APs, interconectados de alguna manera a nivel 2. La red que los interconecta se denomina DS (Distribution System)

Los APs actúan como puentes transparentes traductores entre 802.11 y otras redes 802.x (normalmente x=3)

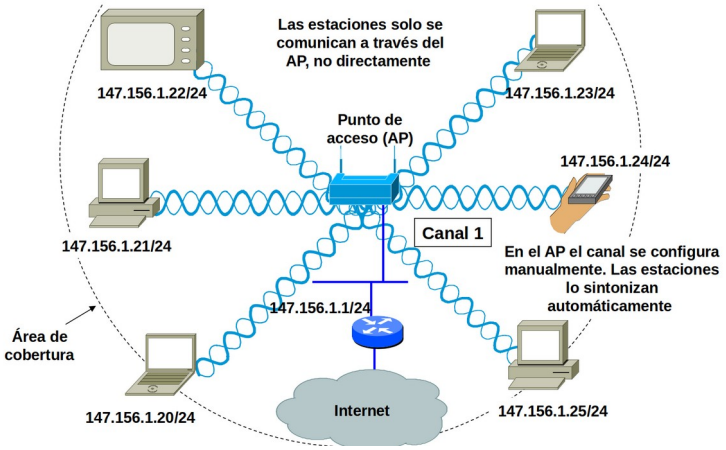
En la práctica, una **red ad-hoc** solo la componen ordenadores, conformando una celda aislada (a no ser que uno de los ordenadores desarrolle funciones de bridge/router) y no tiene posibilidad de hacer unidad con otras celdas, mientras que una red del tipo “infraestructura” se integrará en la red cableada existente y permitirá crear varias celdas, que trabajarán conjuntamente, para dar una mayor cobertura espacial.




Sin embargo, las redes más habituales son las de tipo “infraestructura”. 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), 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” (baliza).

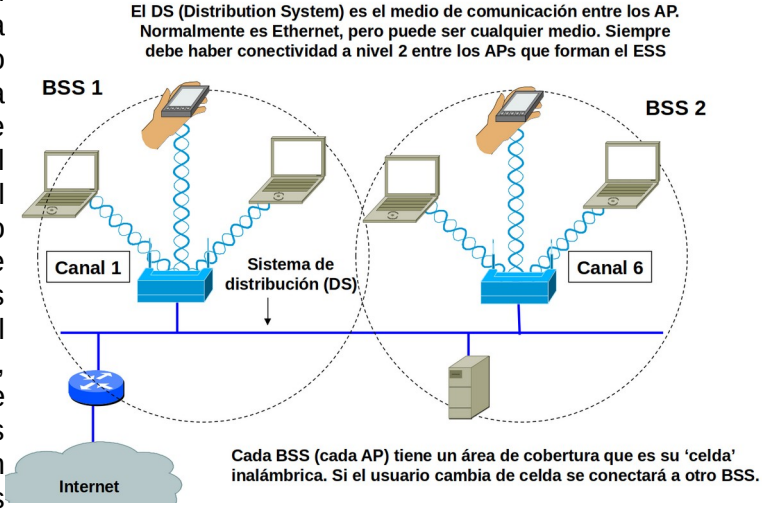
La trama de beacon es enviada periódicamente, permitiendo así a los equipos reconocer los distintos puntos de acceso existentes, las redes disponibles, las potencias de recepción, los parámetros a utilizar en la organización de la transmisión de los diversos clientes, etc. El intervalo de emisión de 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.

BSS (Basic Service Set) ó IBSS (Independent Basic Service Set)

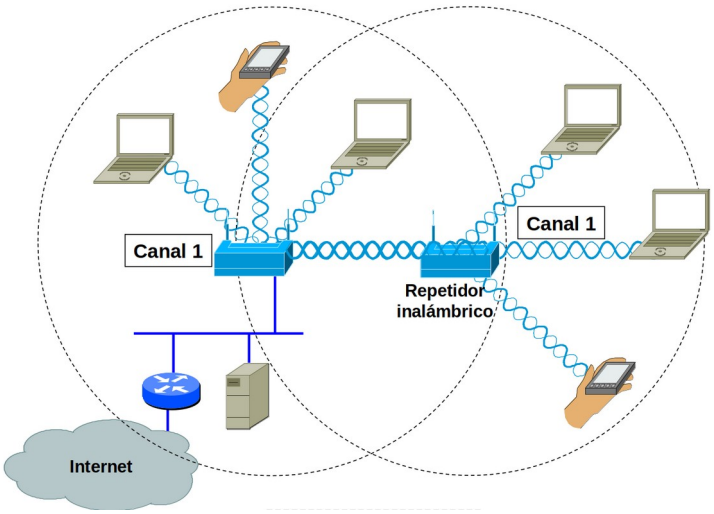



Cada AP conforma una celda, es decir, el área que da cobertura, a donde llega su emisión con la potencia necesaria para ser recibida por los clientes. Sin embargo este área puede no ser suficiente. La normativa implica que no puede emitirse una potencia superior a 100mW lo cual limita el alcance, que 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.

Un ESS formado por dos BSS



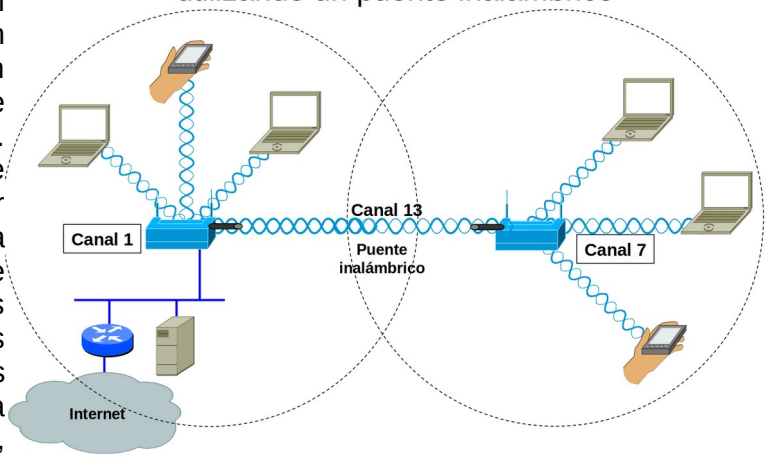

Un ESS formado por dos BSS en un DS sin cables (WDS, Wireless Distribution System)



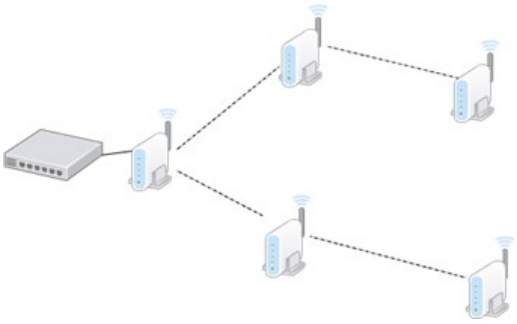

Esta configuración permite que un cliente se conecte a uno u otro punto de acceso dependiendo cuál de ellos proporcione una mejor calidad de recepción, con lo que el cliente podrá moverse libremente por todo el área de cobertura y el enlace físico pasara de una celda a otra según sea necesario (función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

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.

Otro ESS con dos BSS y un DS sin cables utilizando un puente inalámbrico

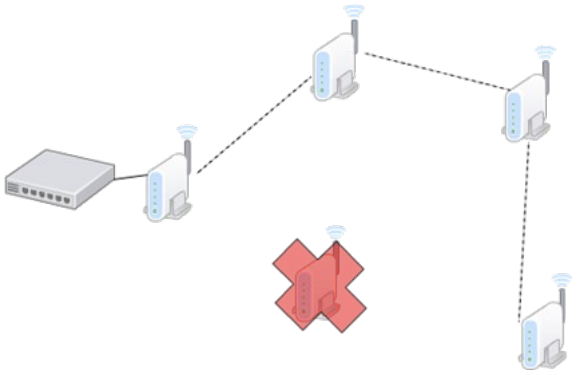



Existe una estructura, variante del tipo “infraestructura” que se conoce habitualmente como **red en malla o mas habitualmente por su termino inglés “mesh”**. En esta estructura existirán puntos de acceso que no tiene conexión a la red cableada. Éstos crearán un enlace inalámbrico con alguno de aquellos 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.

Una red Mesh cuenta con una estación base (puede ser un punto de acceso o router wifi) que tiene conexión a la red cableada, mientras que el resto (satélites) 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 de la derecha, en el que se muestra la red anterior, en la que un punto de acceso dejado de funcionar.



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 las colisiones, interferencias, etc.

## El BSSID y el SSID

Cada AP tiene un BSSID, de fábrica (la MAC de su interfaz inalámbrica). El BSSID no se puede cambiar.

Cada red inalámbrica tiene un SSID (Service Set identifier) también llamado a veces ESSID (Extended SSID). El SSID es una cadena de 2 a 32 caracteres cualesquiera, configurable por el usuario.

Si tenemos un AP aislado (Basic Service Set, BSS) tendrá un BSSID y un SSID.

Si tenemos varios APs formando un Extended Service Set (ESS), es decir todos conectados a nivel 2 por un DS (Distribution System) cada AP tiene un BSSID y todos comparten el mismo SSID.

En una red ad hoc la estación que inicia la red ad hoc elige el BSSID al azar. El usuario configura el ESSID.

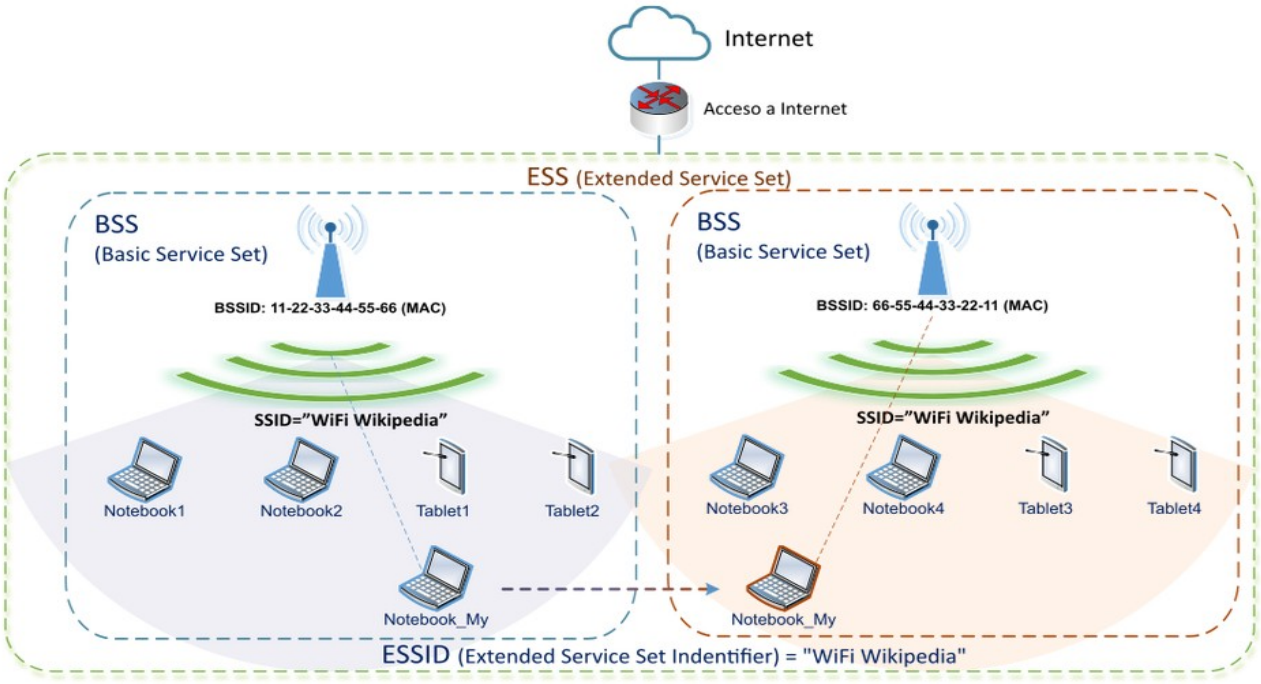
Los APs modernos pueden participar simultáneamnete en varias redes inalámbricas. En ese caso cada red inalámbrica tiene un SSID diferente y el AP crea un BSSID diferente para cada SSID.

Cada AP de la red inalámbrica mantiene en todo momento una lista de las estaciones que tiene asociadas (identificadas por sus direcciones MAC)

**Asociarse a un AP en una red inalámbrica equivale a conectarse por cable a un switch en una red ethernet**

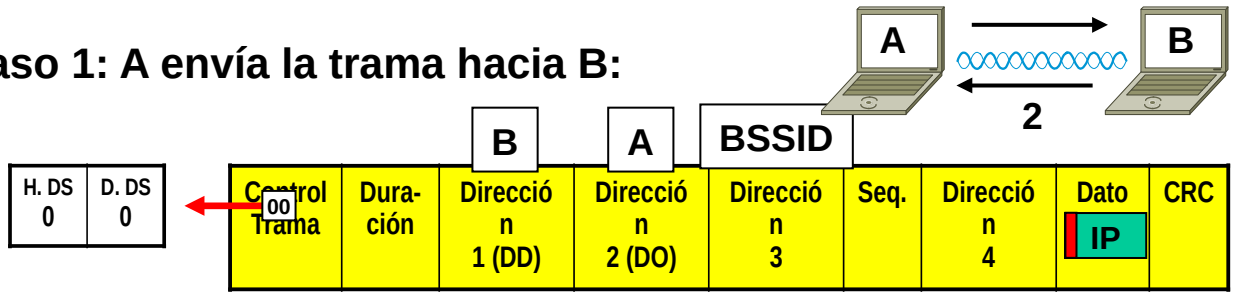
Cuando un AP recibe una trama del DS mira si la MAC de destino está en su lista de estaciones asociadas. Si es así envía la trama por radio, si no la descarta.

En lo relativo al intercambio de tráfico entre su interfaz inalámbrica y su interfaz de cable el funcionamiento de un AP es similar al de un puente transparente o un switch LAN, salvo que el AP no inunda por la red inalámbrica las tramas que le llegan por el DS con destino desconocido. En cambio en el funcionamiento con las estaciones asociadas al AP en su interfaz inalámbrica el funcionamiento se asemeja al de un hub half-duplex



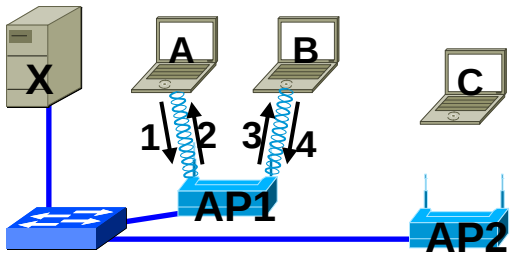
# Red Ad HOC

## Caso 1: A envía la trama hacia B:

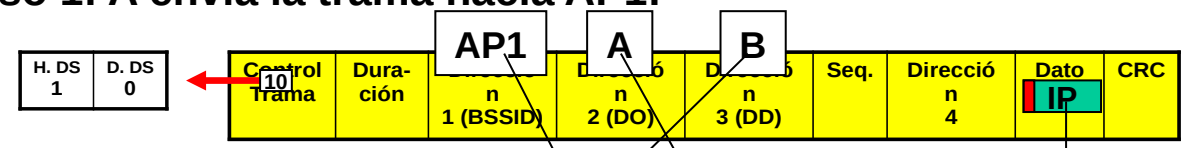



Cuando se crea una red ad hoc la primera estación que aparece genera un BSSID aleatorio que identifica la red (la celda)

## Caso 2: A-AP1-B

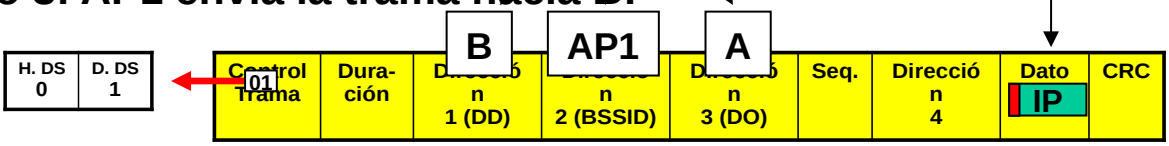



### Paso 1: A envía la trama hacia AP1:




### Paso 2: AP1 envía el ACK hacia A

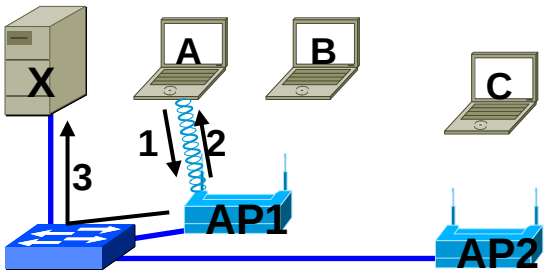
### Paso 3: AP1 envía la trama hacia B:



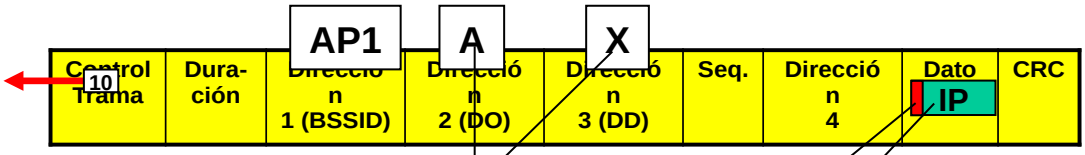

### Paso 4: B envía el ACK hacia AP1

En 802.11 es preciso indicar quien transmite la trama pues es a quien hay que enviar el ACK. Las direcciones del transmisor y receptor pueden se diferentes de las de origen y destino de la trama

# Caso 2: A-AP1-X

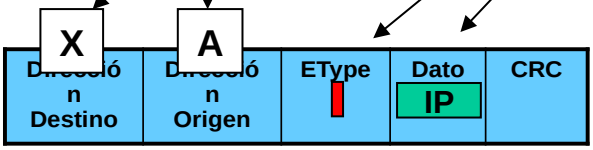



**Paso 1: A envía la trama hacia AP1:**



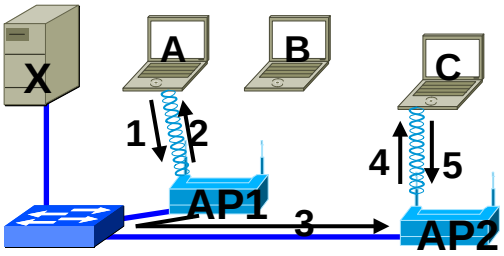

**Paso 2: AP1 envía el ACK hacia A**

**Paso 3: AP1 envía la trama hacia X:**

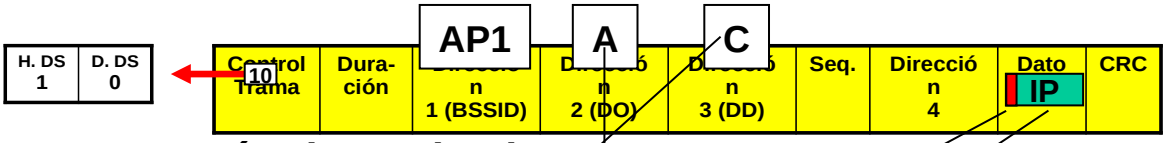



En 802.11 se utiliza encapsulado LLC/SNAP (802.2), en Ethernet se usa Ethertype.
El AP se encarga de convertir uno en otro (es un puente transparente)
La trama Ethernet no contiene el BSSID la dirección del AP

# Caso 3: A-AP1-AP2-C

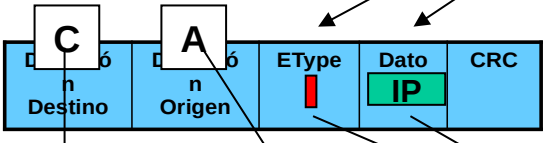



**Paso 1: A envía la trama hacia AP1:**

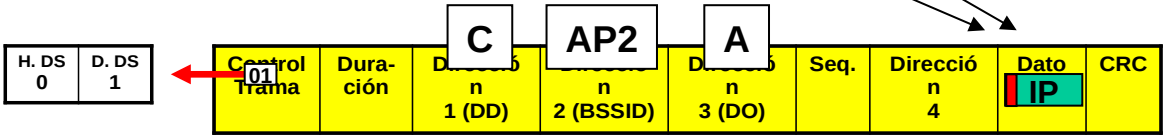



**Paso 2: AP1 envía el ACK hacia A**

**Paso 3: AP1 envía trama hacia AP2:**

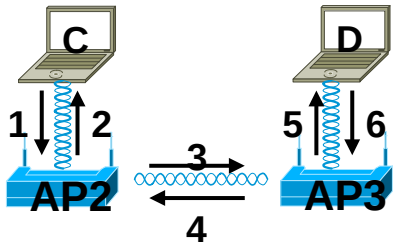



**Paso 4: AP2 envía trama hacia C:**

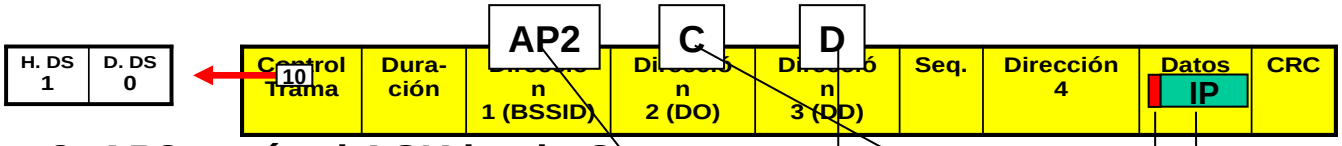



**Paso 5: C envía el ACK hacia AP2**

# Caso 4: C-AP2-AP3-D

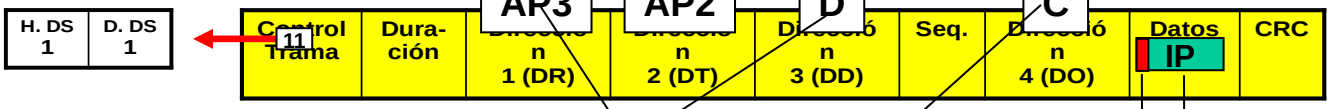



**Paso 1: C envía la trama hacia AP2:**



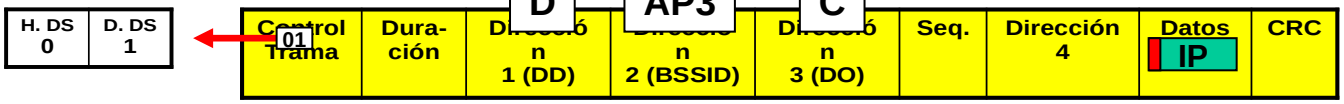

**Paso 2: AP2 envía el ACK hacia C**

**Paso 3: AP2 envía la trama hacia AP3:**




**Paso 4: AP3 envía el ACK hacia AP2:**

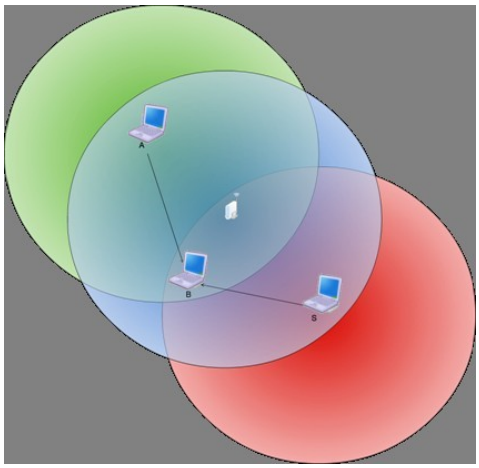
**Paso 5: AP3 envía trama hacia D:**




**Paso 6: D envía el ACK hacia AP3**

# CSMA/CA

Para el control de la transmisión se utilizan dos protocolos complementarios: **CSMA/CA** y **RTS/CTS**. El mecanismo definido en el CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance, **acceso múltiple con escucha de portadora y evasión de colisiones**) 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 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 (Request To Send) 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 (Clear To Send)** 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.

# Operativa

Los dispositivos inalámbricos deben detectar un AP o un router inalámbrico y se deben conectar a este. Los clientes inalámbricos se conectan al AP mediante un proceso de análisis (sondeo). Este proceso puede realizarse de los siguientes modos:

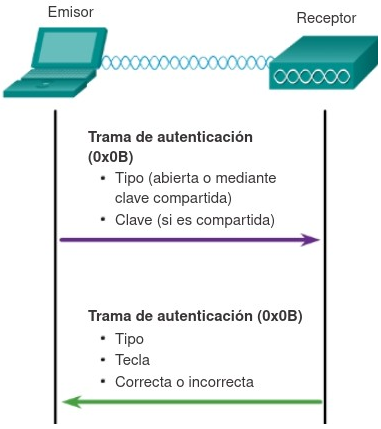
**Modo pasivo**: el AP anuncia abiertamente su servicio al enviar periódicamente tramas de señal de difusión que contienen el SSID, los estándares admitidos y la configuración de seguridad. El propósito principal de la señal es permitir que los clientes inalámbricos descubran qué redes y qué AP existen en un área determinada, de modo que puedan elegir qué red y qué AP usar.

**Modo activo**: los clientes inalámbricos deben conocer el nombre del SSID. El cliente inalámbrico inicia el proceso al transmitir por difusión una trama de solicitud de sondeo en varios canales. La solicitud de sondeo incluye el nombre del SSID y los estándares admitidos. Si un AP o un router inalámbrico se configuran para que no transmitan por difusión las tramas de señal, es posible que se requiera el modo activo.

# Autenticación

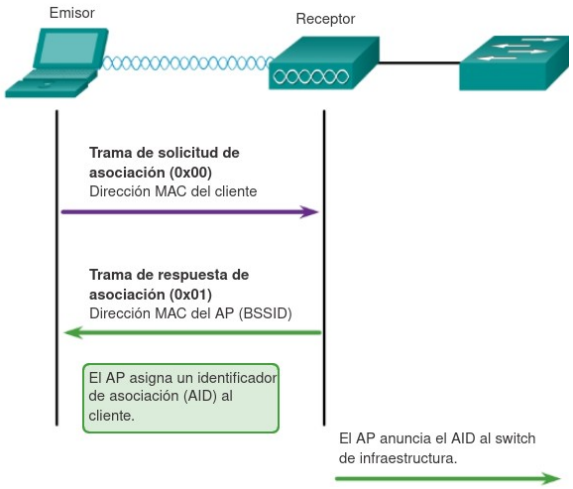
El estándar 802.11 se desarrolló originariamente con dos mecanismos de autenticación:

Autenticación **abierta**: fundamentalmente, una autenticación NULA donde el cliente inalámbrico dice “autentíqueme” y el AP responde “sí”. La autenticación abierta proporciona conectividad inalámbrica a cualquier dispositivo inalámbrico y se debe usar solo en situaciones donde la seguridad no es un motivo de preocupación.




Autenticación de **clave compartida**: es una técnica que se basa en una clave previamente compartida entre el cliente y el AP.

1. El cliente inalámbrico envía una trama de autenticación al AP.
2. El AP responde con un texto de desafío al cliente.
3. El cliente cifra el mensaje mediante la clave compartida y devuelve el texto cifrado al AP.
4. A continuación, el AP descifra el texto cifrado mediante la clave compartida.
5. Si el texto descifrado coincide con el texto de desafío, el AP autentica el cliente. Si los mensajes no coinciden con el texto de desafío, no se autentica el cliente inalámbrico y se deniega el acceso inalámbrico.




Una vez que se autenticó un cliente inalámbrico, el AP continúa con la etapa de asociación.

El cliente inalámbrico reenvía una trama de solicitud de asociación que incluye su MAC.

El AP responde con una respuesta de asociación que incluye el BSSID del AP, que es la dirección MAC del AP.

El AP asigna un puerto lógico conocido como “identificador de asociación” (AID) al cliente inalámbrico. El AID equivale a un puerto en un switch y permite que el switch de infraestructura mantenga un registro de las tramas destinadas a que el cliente inalámbrico las reenvíe.

Una vez que un cliente inalámbrico se asocia a un AP, el tráfico entre el cliente y el AP puede fluir.

# Seguridad

Para que los dispositivos inalámbricos se comuniquen a través de una red, primero se deben asociar a un AP o un router inalámbrico. Una parte importante del proceso 802.11 es descubrir una WLAN y conectarse a esta.

Los dispositivos inalámbricos usan las tramas de administración para completar el siguiente proceso de tres etapas:

- Descubrir nuevos AP inalámbricos.
- Autenticar con el AP.
- Asociarse al AP.

Para asociarse, un cliente inalámbrico y un AP deben acordar parámetros específicos. Para permitir la negociación de estos procesos, se deben configurar los parámetros en el AP y posteriormente en el cliente.

## Parámetros

Los parámetros inalámbricos configurables comunes incluyen lo siguiente:

**SSID**: un SSID es un identificador único que usan los clientes inalámbricos para distinguir entre varias redes inalámbricas en la misma área. El nombre del SSID aparece en la lista de redes inalámbricas disponibles en un cliente. Según la configuración de la red, varios AP en una red pueden compartir un SSID. En general, los nombres tienen una longitud de 2 a 32 caracteres.

Password (Contraseña): el cliente inalámbrico la necesita para autenticarse con el AP. Las contraseñas a veces se denominan “clave de seguridad”. Evita que los intrusos y otros usuarios no deseados accedan a la red inalámbrica.

**Network mode** (Modo de red): se refiere a los estándares de WLAN 802.11a/b/g/n/ac/ad. Los AP y los routers inalámbricos pueden funcionar en modo Mixed (Mixto), lo que implica que pueden usar varios estándares a la vez.

**Security mode** (Modo de seguridad): se refiere a la configuración de los parámetros de seguridad, como WEP, WPA o WPA2. Habilite siempre el nivel más alto de seguridad que se admita.

**Channel settings** (Configuración de canales): se refiere a las bandas de frecuencia que se usan para transmitir datos inalámbricos. Los routers y los AP inalámbricos pueden elegir la configuración de canales, o esta se puede establecer manualmente si existe interferencia con otro AP o dispositivo inalámbrico.

## Amenazas

Un ataque de desconexión suplantada: esto ocurre cuando un atacante envía una serie de comandos de “desasociación” a los clientes inalámbricos dentro de un BSS. Estos comandos hacen que todos los clientes se desconecten. Al desconectarse, los clientes inalámbricos inmediatamente intentan volver a asociarse, lo que crea un estallido de tráfico. El atacante continúa enviando tramas de desasociación, y el ciclo se repite.

Una saturación con CTS: esto ocurre cuando un atacante aprovecha el método de contienda CSMA/CA para monopolizar el ancho de banda y denegar el acceso de todos los demás clientes inalámbricos al AP. Para lograr esto, el atacante satura repetidamente el BSS con tramas de Listo para enviar (CTS) a una STA falsa. Todos los demás clientes inalámbricos que comparten el medio reciben las CTS y retienen sus transmisiones hasta que el atacante deja de transmitirlas

Puntos de acceso no autorizados Un AP no autorizado es un AP o un router inalámbrico que:

Se conectó a una red empresarial sin autorización explícita o en contra de la política de la empresa. Cualquier persona con acceso a las instalaciones puede instalar (malintencionadamente o no) un router inalámbrico económico que puede permitir el acceso a los recursos de red protegidos.

Un atacante lo conectó o habilitó para capturar datos de clientes, como las direcciones MAC de los clientes (inalámbricos y cableados), o para capturar y camuflar paquetes de datos, obtener acceso a los recursos de la red o iniciar un ataque man-in-the-middle (intermediario).

# Protección WLAN

| | WEP | WPA | 802.11i/WPA2 |
|---|---|---|---|
| **Método de autenticación** | Clave pre-compartida | PSK o 802.1x | PSK o 802.1x |
| **Cifrado** | RC4 | TKIP | AES |
| **Integridad del mensaje** | CRC-32 | MIC | CCMP |
| **Seguridad** | Débil | Fuerte | Más seguro |

Las opciones de **Security** son opciones de protocolos de seguridad disponibles. Los usuarios domésticos deben elegir WPA2/WPA Mixed Personal (WPA2/WPA personal combinado), mientras que los usuarios empresariales normalmente eligen WPA2/WPA Mixed Enterprise (WPA2/WPA empresarial combinado). El alcance de 5 GHz ofrece las mismas opciones. La terminal inalámbrica también debe admitir la opción de seguridad seleccionada para asociarse.

Uno de los problemas a los cuales se enfrenta actualmente la tecnología Wi-Fi es la progresiva saturación del espectro radioeléctrico, debido a la masificación de usuarios, esto afecta especialmente en las conexiones de larga distancia (mayor de 100 metros). En realidad Wi-Fi está diseñado para conectar ordenadores a la red a distancias reducidas, cualquier uso de mayor alcance está expuesto a un excesivo riesgo de interferencias.

Un muy elevado porcentaje de redes son instaladas sin tener en consideración la seguridad convirtiendo así sus redes en redes abiertas (o completamente vulnerables ante el intento de acceder a ellas por terceras personas), sin proteger la información que por ellas circulan. De hecho, la configuración por defecto de muchos dispositivos Wi-Fi es muy insegura (routers, por ejemplo) dado que a partir del identificador del dispositivo se puede conocer la clave de éste; y por tanto acceder y controlar el dispositivo se puede conseguir en sólo unos segundos.

El acceso no autorizado a un dispositivo Wi-Fi es muy peligroso para el propietario por varios motivos. El más obvio es que pueden utilizar la conexión. Pero además, accediendo al Wi-Fi se puede monitorizar y registrar toda la información que se transmite a través de él (incluyendo información personal, contraseñas….).

Privacidad equiparable a la de redes cableadas (WEP): especificación 802.11 original, diseñada para proporcionar una privacidad similar a la de conectarse a una red mediante una conexión por cable. Los datos se protegen mediante el método de cifrado RC4 con una clave estática. Sin embargo, la clave nunca cambia al intercambiar paquetes, por lo que es fácil de descifrar.

Acceso protegido Wi-Fi (WPA): un estándar de Wi-Fi Alliance que usa WEP, pero protege los datos con un algoritmo de cifrado del protocolo de integridad de clave temporal (TKIP), que es mucho más seguro. TKIP cambia la clave para cada paquete, lo que hace que sea mucho más difícil de descifrar.

IEEE 802.11i/WPA2: IEEE 802.11i es un estándar del sector para proteger las redes inalámbricas. La versión de Wi-Fi Alliance se denomina WPA2. Tanto 802.11i como WPA2 usan el estándar de cifrado avanzado (AES). En la actualidad, se considera que AES es el protocolo de cifrado más seguro.

- WEP, cifra los datos en su red de forma que sólo el destinatario deseado pueda acceder a ellos. Los cifrados de 64 y 128 bits son dos niveles de seguridad WEP. WEP codifica los datos mediante una “clave” de cifrado antes de enviarlo al aire. Este tipo de cifrado no está muy recomendado debido a las grandes vulnerabilidades que presenta ya que cualquier cracker puede conseguir sacar la clave, incluso aunque esté bien configurado y la clave utilizada sea compleja.
- WPA: presenta mejoras como generación dinámica de la clave de acceso. Las claves se insertan como dígitos alfanuméricos.
- Filtrado de MAC, de manera que sólo se permite acceso a la red a aquellos dispositivos autorizados.
- Ocultación del punto de acceso: se puede ocultar el punto de acceso (Router) de manera que sea invisible a otros usuarios.
- El protocolo de seguridad llamado WPA2 (estándar 802.11i), que es una mejora relativa a WPA. En principio es el protocolo de seguridad más seguro para Wi-Fi en este momento. Sin embargo requieren hardware y software compatibles, ya que los antiguos no lo son.

Sin embargo, no existe ninguna alternativa totalmente fiable, ya que todas ellas son susceptibles de ser vulneradas.

La **Wi-Fi Alliance** distingue:

- **WPA-Personal y WPA2-Personal** (con PSK, clave pre-compartida)
- **WPA-Enterprise y WPA2-Enterprise** (autenticación 802.1x/EAP)

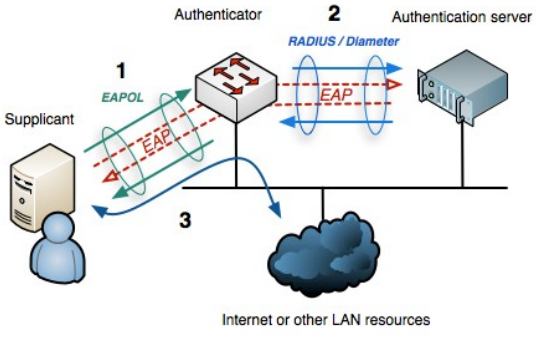
Los fabricantes comenzaron a producir la nueva generación de puntos de accesos apoyados en el protocolo WPA2 que utiliza el algoritmo de **cifrado AES (Advanced Encryption Standard)** superior al TKIP utilizado en WPA.

El WPA-Enterprise requiere de una infraestructura de autenticación 802.1x con un **servidor de autenticación**, generalmente un **servidor RADIUS** (puerto 1645 en CISCO y 1812 en el resto). Este presta un servicio AAA (*Authentication, Authorization and Accounting*, ‘autenticación, autorización y contabilización’)

El **estándar IEEE 802.1x** ofrece una solución a este problema, tanto a redes 802.3 como a 802.11. Consiste en que **cada usuario tiene sus propias credenciales de acceso a la red y se autentica con ellas**, independientemente de que ademas se utilice o no una clave compartida para acceder a la red.

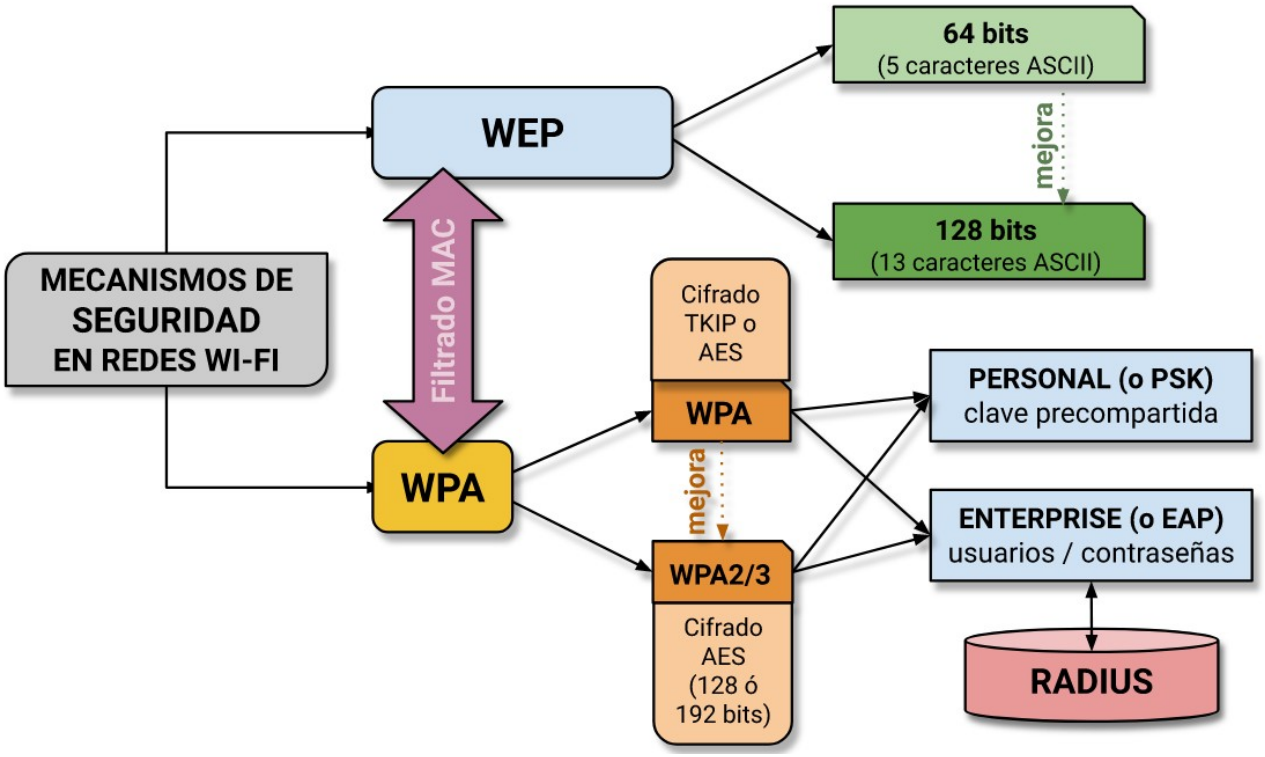
El protocolo 802.1x utiliza para autentificación y encriptación el protocolo EAP, normalmente en alguna de las variantes Extended EAP y cuya preferencia dependerá del fabricante de los equipos. Existen siempre tres elementos:

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.



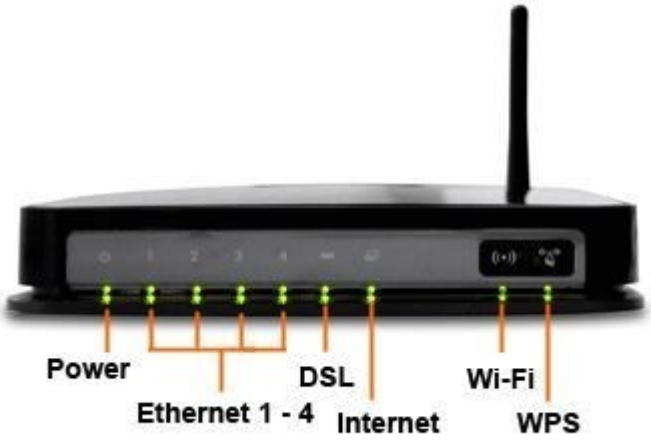

Authenticator (Autentificador): Es el equipo que recibe la petición de conexión del cliente y que por tanto ha de tramitar la autentificación de este. En el caso de las redes Wi-Fi este rol lo lleva a cabo el punto de acceso.

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.




## WPS (Wi-Fi Protected Setup)

WPS (Wi-Fi Protected Setup) es un estándar de 2007, promovido por la Wi-Fi Alliance para facilitar la creación de redes WLAN. En otras palabras, WPS no es un mecanismo de seguridad por sí, se trata de la definición de diversos mecanismos para facilitar la configuración de una red WLAN segura con WPA2, pensados para minimizar la intervención del usuario en entornos domésticos o pequeñas oficinas (**SOHO: Small Office Home Office**). Concretamente, WPS define los mecanismos a través de los cuales los diferentes dispositivos de la red obtienen las credenciales (SSID y PSK) necesarias para iniciar el proceso de autenticación.




## Filtrado MAC

En la mayoría de Aps se puede configurar un sistema que permite establecer mecanismos de control de acceso al mismo basados en la dirección MAC de los adaptadores inalámbricos. Existen dos tipos de filtrado.

Lista de acceso o lista blanca: Filtrado MAC basado en una lista de direcciones físicas cuyo acceso al AP está permitido.

Lista negra: Filtrado MAC basado en lista de direccións físicas cuyo acceso está prohibido.

Teniendo en cuenta que existen formas sencillas de suplantar una MAC es más útil el empleo de lisas blancas.

# Configuración 802.1x en packet tracer