Sección 5

REDES LOCALES INALÁMBRICAS

Redes locales inalámbricas

Historia

Las ***redes inalámbricas consisten en los medios e infraestructuras*** que permiten la incorporación de ***sistemas en red mediante medios no guiados*** (***ondas electromagnéticas***). La ***facilidad de implantación***, sus ***grandes ventajas*** para muchos tipos de usuarios y el crecimiento de los ***dispositivos que pueden usarlas*** (portátiles, tablets, teléfonos móviles, etc.) han hecho que esta tecnología esté ***presente en prácticamente todos los hogares, empresas e instituciones.***

Esta tecnología se denomina **Wi-Fi**.

Wi-Fi es una marca de la ***Wi-Fi Alliance***, la organización comercial que adopta, prueba y ***certifica*** que los equipos cumplen los ***estándares 802.11*** relacionados a ***redes inalámbricas de área local.***

Surgió por la necesidad de establecer un ***mecanismo de conexión inalámbrica que fuese compatible entre distintos dispositivos***. Buscando esa compatibilidad, varias empresas se reunieron para crear la ***Wireless Ethernet Compatibility Alliance (WECA),*** actualmente llamada ***Wi-Fi Alliance***. El objetivo de la misma fue designar una marca que permitiese fomentar más fácilmente la tecnología inalámbrica y asegurar la compatibilidad de equipos.
En abril de 2000 WECA certifica la interoperabilidad de equipos según la ***norma IEEE 802.11b, bajo la marca Wi-Fi***. Esto quiere decir que el usuario tiene la garantía de que todos los equipos que tengan el sello ***Wi-Fi pueden trabajar juntos sin probl***emas, independientemente del fabricante de cada uno de ellos.
Se puede obtener ***un listado completo de equipos que tienen la certificación Wi-Fi en Alliance - Certified Products.***
En 2002 la asociación ***WECA*** estaba formada ya por casi 150 miembros en su totalidad. La familia de estándares ***802.11*** ha ido naturalmente ***evolucionando*** desde su creación, mejorando el ***rango y velocidad*** de la transferencia de información, su ***seguridad***, entre otras cosas.
La norma IEEE ***802.11*** fue diseñada para sustituir el equivalente a las ***capas físicas y MAC de la norma 802.3 (Ethernet).*** Esto quiere decir que en lo único que se ***diferencia una red Wi-Fi de una red Ethernet*** es en cómo se ***transmiten las tramas o paquetes*** de datos; el resto es idéntico. Por tanto, una ***red local inalámbrica 802.11*** es completamente ***compatible*** con todos los servicios de las ***redes locales (LAN) de cable 802.3*** (***Ethernet***).

Redes locales inalámbricas

Estándar IEEE 802.11 y certificación Wi-Fi

- **IEEE 802.11** define la tecnología para ***redes locales*** mediante medios no guiados (***radio frecuencia***).
- Su ***diferencia*** está centrada en las ***capas 1(físico) y 2(enlace)*** del modelo OSI.
- Utiliza zonas del espectro radioeléctrico llamadas **ISM (Industrial, Scientific and Medical)**que no precisan de licencia de uso, aunque tienen sus limitaciones, se situan en ***2,4 GHz y 5 GHz***. Esta banda se comparte con otros dispositivos que pueden causar interferencias, por ello la potencia de uso permitida en todos los casos es baja.
- Existen diferentes versiones:
  - **IEEE 802.11a**
  - **IEEE 802.11b**
  - **IEEE 802.11g**
  - **IEEE 802.11n**
  - **IEEE 802.11ac**

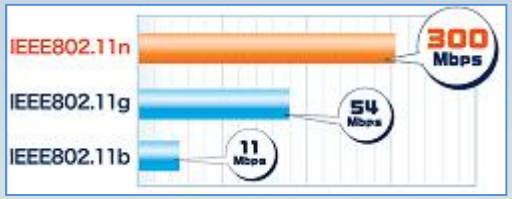
- La ***certificación WiFi*** la otorga la ***WiFi Alliance***, esta certificación ***implica*** que se cumplen los criterios de ***compatibilidad*** que permiten que los equipos certificados ***puedan operar entre si***.

Nota: *Existe un estándar 802.11 para comunicación por infrarrojos y radiofrecuencia a 2 Mbps que nunca se llegó a usar comercialmente.*
Puntos de acceso interesantes: *http://www.ubnt.com/unifi*

Redes locales inalámbricas

Versiones IEEE 802.11

- **IEEE 802.11a**
  - ✓ Se publica en 1999, usa la ***banda de 5 GHz***. , esto hace que su uso esté limitado a pocos países, ya que por ejemplo, en ***Europa no estaba permitido*** legalmente el uso de esa banda.
  - ✓ Su velocidad de comunicación máxima es de ***54 Mbps***.



- **IEEE 802.11b**
  - ✓ Se publica en 1999, usa la banda de ***2,4 GHz***. , es la ***más usada*** ya que esta zona del espectro está liberada.
  - ✓ Su velocidad de comunicación máxima es de ***11 Mbps***.
- **IEEE 802.11g**
  - ✓ Se publica en 2003, usa la banda ***de 2,4 GHz***. , al ***mejorar las prestaciones es el estándar más extendido***, sobre todo en Europa donde no se podía usar la banda de 5 GHz.
  - ✓ Su velocidad de comunicación máxima es de ***54 Mbps***.

- **IEEE 802.11n**
  - ✓ Se publica en 2009, usa las bandas de ***2,4 GHz y la de 5 GHz***. , se implanta cuando se ***permite el uso en Europa*** de esta banda. Usa ***tecnología MIMO***.
  - ✓ Su velocidad de comunicación es de ***150 Mbps y 300 Mbps***. La ***máxima posible*** teórica sería de ***600 Mbps***.

Redes locales inalámbricas

Versiones IEEE 802.11

- **IEEE 802.11n**
  - ✓ La tecnología ***MIMO (Múltiple Inpunt Múltiple Output)*** se basa en el uso de ***varias antenas***, tanto en el emisor como en el receptor, con el uso de ***ambas bandas***.
  - ✓ Utiliza un método llamado ***SDM (Spatial División Multiplexing),*** es decir, multiplexación por división espacial que consigue ***varios flujos de información en las mismas frecuencias***, usando el ***multitrayecto (rebotes),*** con otras tecnologías esto representa un problema, pero ***con SDM se aprovechan para el envío de información***.
  - ✓ El ***aumento de la velocidad*** se consigue con los ***mismos anchos*** de banda que las anteriores.

- **IEEE 802.11ac**
  - ✓ Se publica en 2013, usa la banda de ***5 GHz***., usa ***mayor ancho de banda*** y se plantea como alternativa de alta velocidad para redes WiFi, usa ***tecnologías heredadas de la 802.11n***.
  - ✓ Su velocidad de comunicación ***supera 1 Gbps*** y puede alcanzar ***1.3 y 1.9 Gbps*** dependiendo de las condiciones de la red.

❑ **Nota:** Todos los ***dispositivos*** con estándares más recientes se fabrican con ***retro-compatibilidad***. Por ejemplo, los dispositivos 802.11ac no necesitan incorporar la frecuencia de 2.4 GHz, pero llevan el hardware necesario para realizar comunicaciones con estándares inferiores tales como el 802.11n o el 802.11g que si la usan. Las ***potencias de emisión están limitadas***.

Redes locales inalámbricas

Arquitecturas redes inalámbricas

El estándar ***802.11*** contempla ***dos formas de funcionamiento***, ***la básica y la extendida***. Aparte de estas formas que posibilitan diferentes arquitecturas, algunos fabricantes incorporan ***formas de servicio 'extras'.***

Basic Service Set (BSS)

Esta arquitectura proporciona los ***'bloques' básicos de una LAN inalámbrica sencilla***. Existen ***dos modos de trabajo***, el primero el modo ***infraestructura*** y en segundo lugar el modo ***ad-hoc***.

El ***modo infraestructura*** es el ***más usado en hogar y pequeñas oficinas***, en este modo, ***solo hay un punto de acceso*** (acces point – ***AP***) junto con ***estaciones asociadas*** (dispositivos conectados al punto de acceso - STAs). ***El ancho de banda está compartido*** por todos los dispositivos conectados a la red WiFi, podríamos definirlo como un ***hub inalámbrico.***

El ***punto de acceso actua como 'maestro'*** en la ***regulación del tráfico de datos*** y en la mayoría de los casos está conectado a una red cableada. El ***punto de cceso también determina quien está asociado a esa red y quien no***.

El ***modo ad-hoc*** de red es ***menos usado*** y sirve para conectar ***dos o más dispositivos de forma directa sin la intervención de un punto de acceso***. Las comunicaciones en este modo ***suelen ser temporales*** y se ***degradan*** de forma notable para ***más de dos dispositivos***.

Redes locales inalámbricas

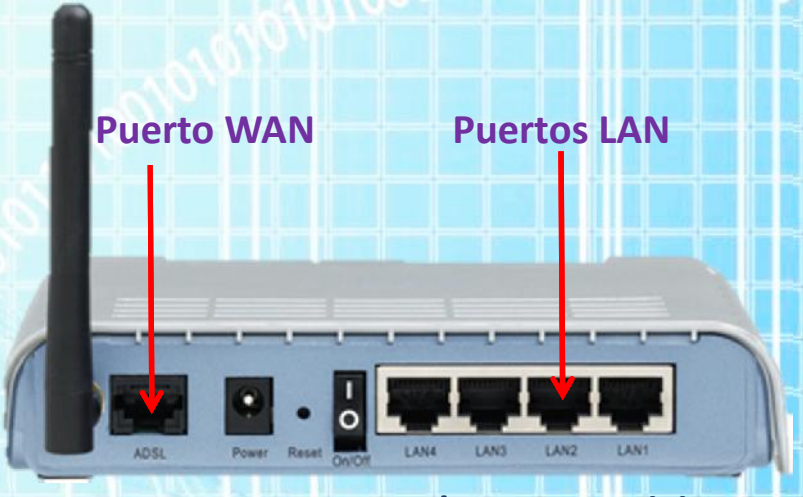
Arquitecturas redes inalámbricas

Es importante distinguir que ***en hogar y oficina*** es muy común usar equipos que cumplen ***dos funciones***: ***router de banda ancha y punto de acceso***.

- Un ***punto de acceso*** solo tiene ***la sección Wi-Fi y la conexión a LAN*** (simple o múltiple).

- Un ***router/punto de acceso***, aparte de la sección ***Wi-Fi*** y la parte ***LAN*** tiene otra conexión para la ***WAN***. Esta conexión se identifica de diferentes formas: ***ADSL, WAN, Internet, Cable, etc.***

Punto de acceso WiFi



Router + punto de acceso WiFi

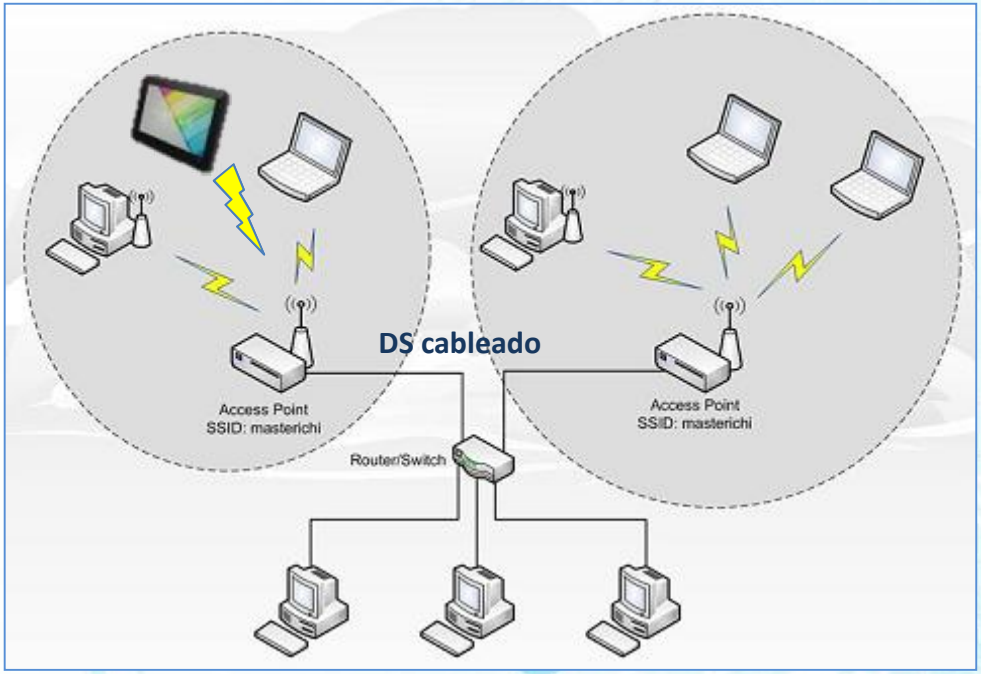
Redes locales inalámbricas

Arquitecturas redes inalámbricas

Extended Service Set (ESS)

Un '***extended service set***' (***ESS***) se podría definir como ***uno o más 'Basic Service Sets' (BSSs) conectados entre sí*** y con sus LAN asociadas. Cada ***BSS consta de un punto de acceso (AP) junto con todos los clientes*** inalámbricos (STAs) formando una WLAN.

Para ***cualquiera de las estaciones conectadas, hay solo un BSS aparente***, ***no se distinguen diferentes redes***.

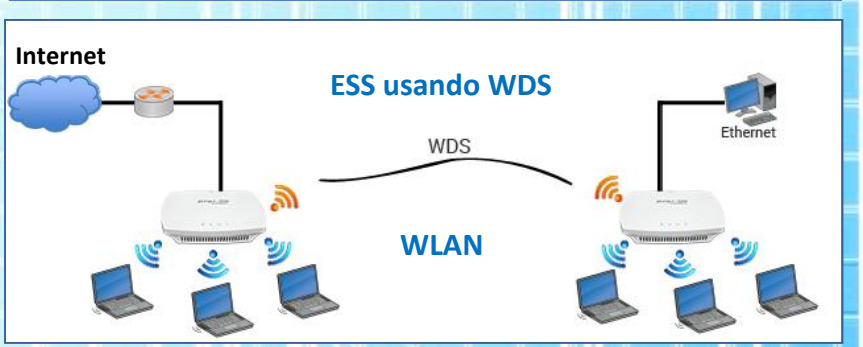


Ejemplo de ESS con dos APs

- La principal función del uso de esta arquitectura ***(ESS)*** es la ***ampliación de la cobertura inalámbrica usando varios puntos de acceso*** para ***diferentes zonas***.

- Los ***puntos de acceso se conectan entre sí*** formando el '***Sistema de Distribución***' o Distribution System (***DS***) que ***gestiona la conectividad y comunicación*** en la red ***como si solo hubiese un punto de acceso.***

- Los ***puntos de acceso*** se pueden ***conectar*** mediante uno o ***varios switches (DS cableado)*** o mediante ***conexión inalámbrica (WDS)***. Como se podrá deducir la interconexión cableada es más eficiente.



Redes locales inalámbricas

Arquitecturas redes inalámbricas

Identificador de red inalámbrica (SSID)

El '***Service Set ID (SSID)'*** permite distinguir a unas redes inalámbricas de otras que pueden estar presentes en la misma zona. Este SSID es el identificador único de la red y es una cadena de texto de hasta 32 caracteres.

- **BSSID**: Cada ***BSS está formado por un AP y sus asociados***, el identificador de este AP en una red ***BSS es su MAC***, es decir un número de 48 bits expresado en hexadecimal.

- **ESSID**: En un ESS, al ***existir diferentes puntos de acceso***, no podemos tomar como identificador la MAC, por lo que aparece el ***concepto de ESSID***, que es un nombre '***alfanumérico'*** de la red y que podrá ser el ***mismo para todos los puntos de acceso***. Este nombre lo configurá el administrador de la red. Los AP pueden trabajar en canales diferentes.

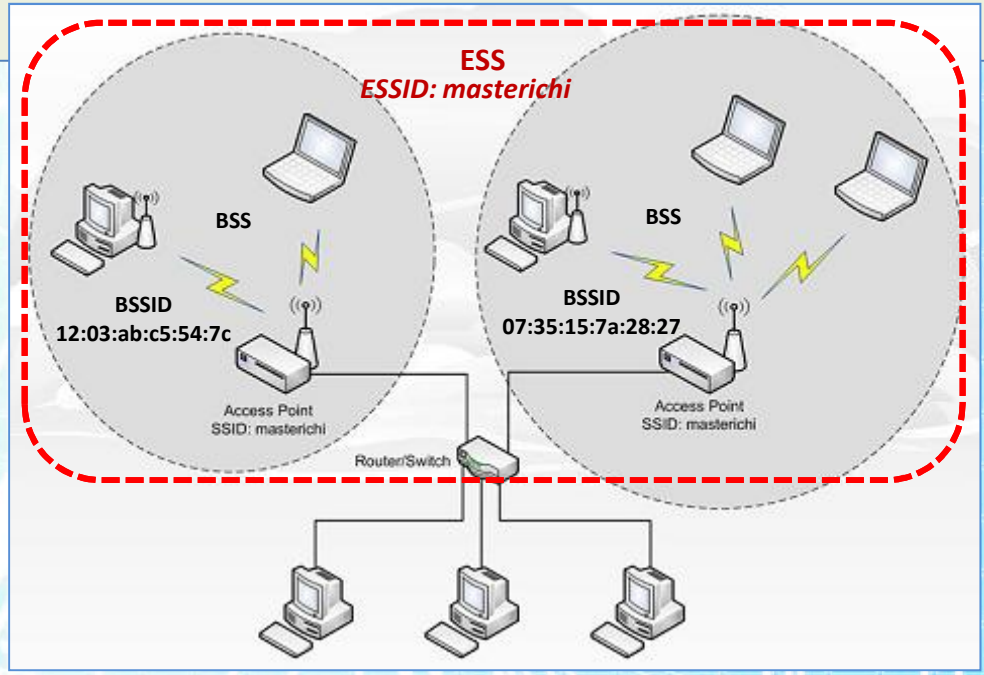
Notas: En ***redes con un solo punto de acceso***, por comodidad, también ***se suele usar el ESSID***, en redes ***ad-hoc, al no existir un AP,*** se asigna como ***BSSID un número aleatorio***.

- En la imagen de la derecha podemos observar ***dos puntos de acceso con diferentes BSSID*** (la MAC del AP) y con un ***SSID o ESSID*** común (***masterichi***).

- Los ***clientes conectados*** a la LAN cableada y a la WLAN ***'ven***' el sistema como ***una única LAN*** y se comunican entre sí a nivel de ***capa 2 (enlace).***

- Si un ***equipo móvil (teléfono, portátil, etc.) se desplaza*** de una zona a la otra, ***seguiría conectado a la misma red a través de otro punto de acceso*** con el mismo ESSID, esta capacidad se llama ***'roamming'.***

- Los ***canales*** para los puntos de acceso de una red WLAN ***suelen ser diferentes para evitar interferencias*** entre ellos.



Redes locales inalámbricas

Arquitecturas redes inalámbricas

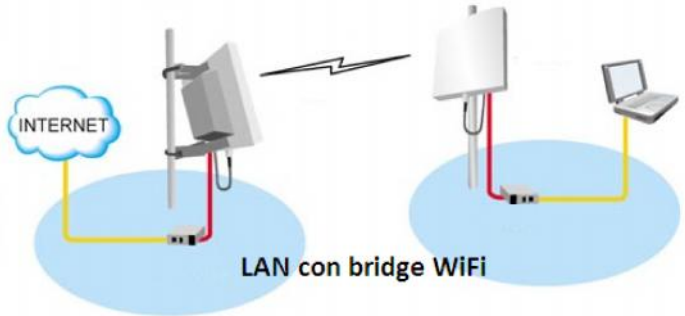
Modo 'Bridge' (puente) – Punto a punto

Este modo de conexión es muy común y ***algunos puntos de acceso lo permiten***. Sirve para ***conectar dos redes entre sí***. La aplicación típica es la conexión de ***dos edificios o espacios que no pueden ser conectados de forma sencilla por cable***. Por ejemplo, unas ***oficinas y una nave industrial, un domicilio y una oficina, etc.***

Para que este modo se pueda establecer ***es necesario que el AP lo permita***. El AP solo se dedicará a ***esa función de enlace*** y se usan las ***MAC de los puntos de acceso*** para conseguir la ***asociación/conexión***.

Es muy común usar ***antenas directivas*** que permiten ***mayor calidad de enlace*** y ***menor posibilidad de ataque externo*** al disminuir el ***'haz'*** de radiofrecuencia usado (lóbulo más estrecho). La ***seguridad en la conexión*** ante 'ataques' externos ***es muy importante***.

Algunos puntos de acceso permiten ***instalarse en el exterior*** si están dedicados a esta función.



Redes locales inalámbricas

Arquitecturas redes inalámbricas

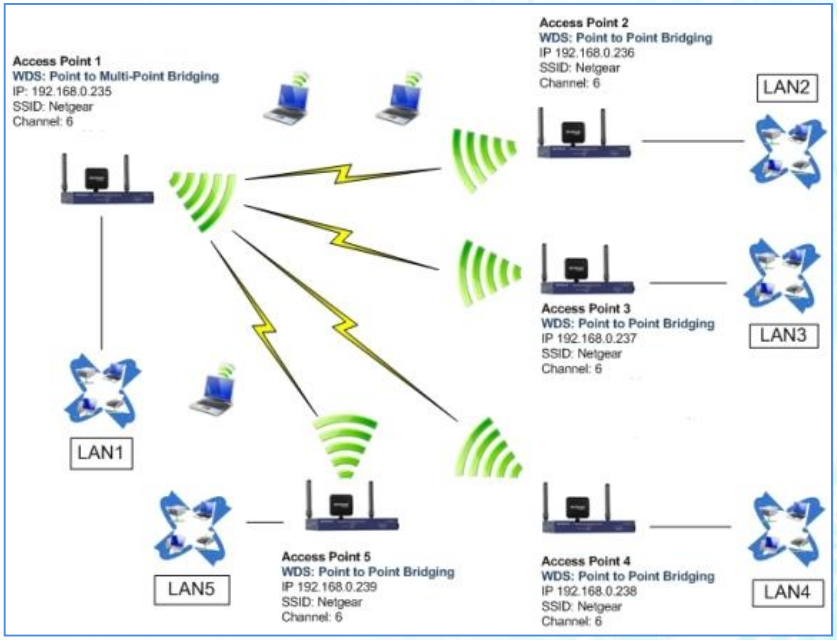
Modo punto a multipunto

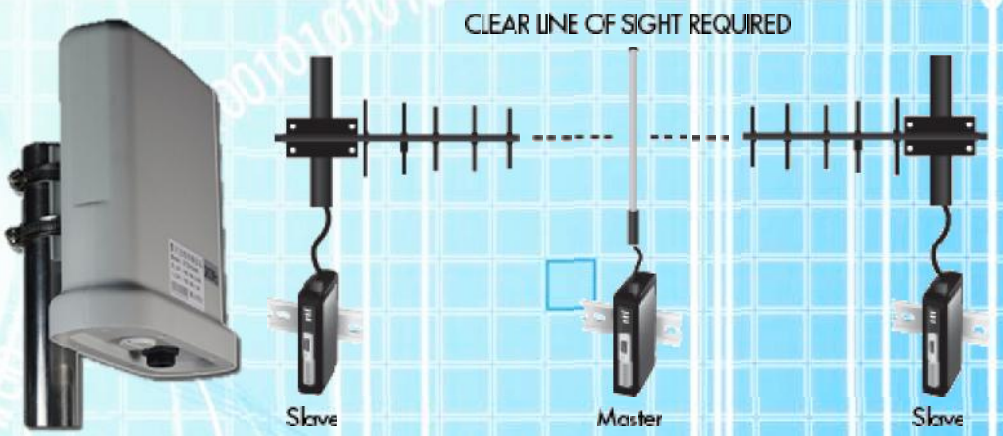
Esta es una alternativa que permiten ***algunos puntos de acceso***. Sirve para ***conectar varias redes entre sí***. La aplicación típica es la conexión de más de ***dos edificios o espacios que no pueden ser conectados de forma sencilla por cable*** a uno '***central***' para integrarlos en la ***misma red***.

Hay que tener en cuenta que ***este sistema comparte el ancho de banda***, por lo que si los equipos conectados son numerosos la conexión puede ser pobre, aunque es una alternativa en caso de no poder optar por otras soluciones mejores.

En este caso ***puede que sea necesario el uso de antenas no direccionales*** si los diferentes puntos ***'clientes' no están en la misma zona***.

Igual que el sistema punto a punto, la ***seguridad en la conexión es un factor muy importante***.





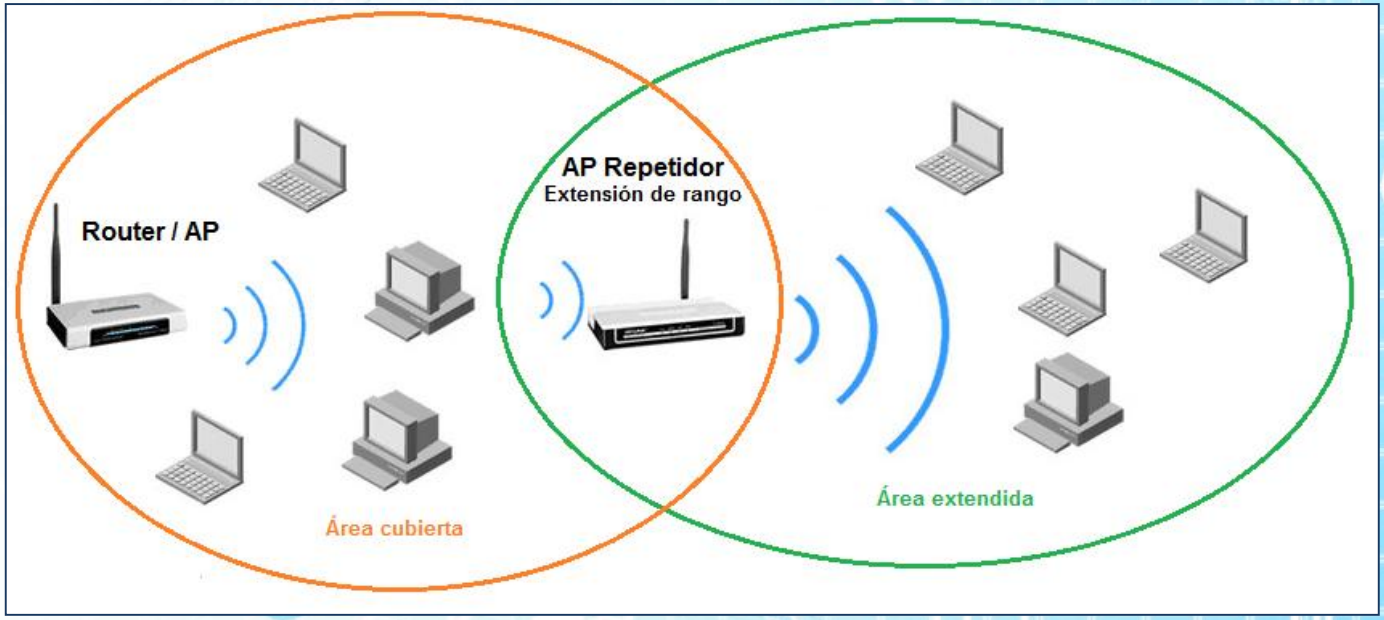
Redes locales inalámbricas

Arquitecturas redes inalámbricas

Modo 'repetidor'

Algunos fabricantes de puntos de acceso incorporan también el modo '***repetidor***'. Este modo sirve para ***'prolongar' la distancia cubierta por un punto de acceso Wi-Fi.*** Como podemos ver en el esquema, es una solución, pero es un eslabón débil en la red, ya que ***todo el tráfico de los nodos conectados al repetidor se comparte en ese punto de acceso que además lo comparte con la red principal***. El concepto se ve claramente en el gráfico de la instalación.

No es muy común la implantación de este modo ***en los puntos de acceso***.



Otros servicios

Algunos fabricantes tienen en ***APs avanzados servicios o modos extras de funcionamiento***, por ejemplo el servicio '***HotSpot***' usado en hoteles y otros lugares para acceso a la red mediante pago, sistemas de ***distribución de carga*** balanceada en caso de diferentes puntos de acceso, funciones de ***correo electrónico para administración***, etc. Al ser modos 'extra' deberemos leer los manuales del fabricante.

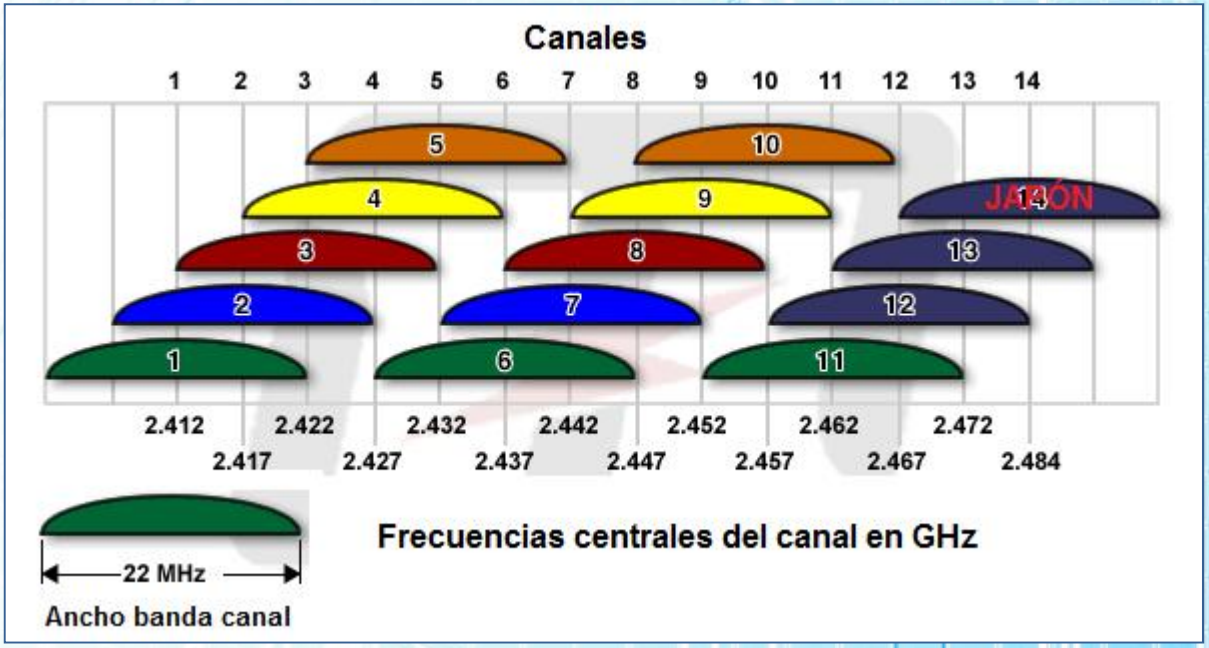
Redes locales inalámbricas

Arquitecturas redes inalámbricas

Canales

El ***espectro asignado a WiFi en Europa*** para la banda de ***2.4 GHz se reparte en 13 canales*** separados entre sí por ***5 MHz***., pero los equipos usados ***emplean un ancho de banda de 22 MHz por canal*** para transmitir sus datos, por lo tanto, ***podemos deducir*** que cuando un canal para emitir estamos ***invadiendo los canales adyacentes***.

Canal	Frecuencia (MHz)
1	2412
2	2417
3	2422
4	2427
5	2432
6	2437
7	2442
8	2447
9	2452
10	2457
11	2462
12	2467
13	2472
14	2484



Como podemos ver en la figura, en caso de ***necesitar establecer un WDS*** (***varios puntos de acceso para la misma red***), la única forma de conseguir que ***no tengan interferencias entre sí*** es optando por los ***canales 1, 6 y 11 o por los canales 1, 7 y 13***.

Además de este caso, nos ***podemos encontrar con gran cantidad de puntos de acceso próximos*** que ***bajen el rendimiento*** de nuestra ***conexión inalámbrica.***

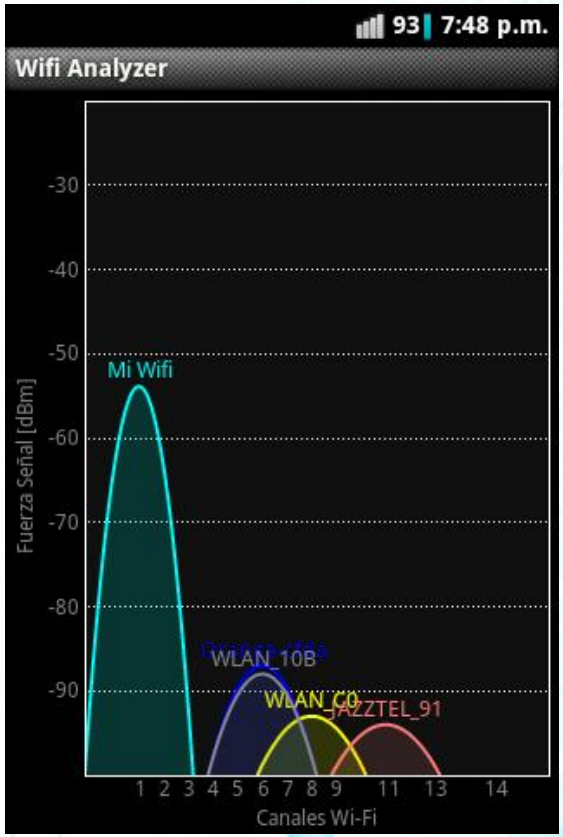
Para intentar ***minimizar estos problemas*** tenemos algunas ***herramientas y métodos*** a nuestro alcance.

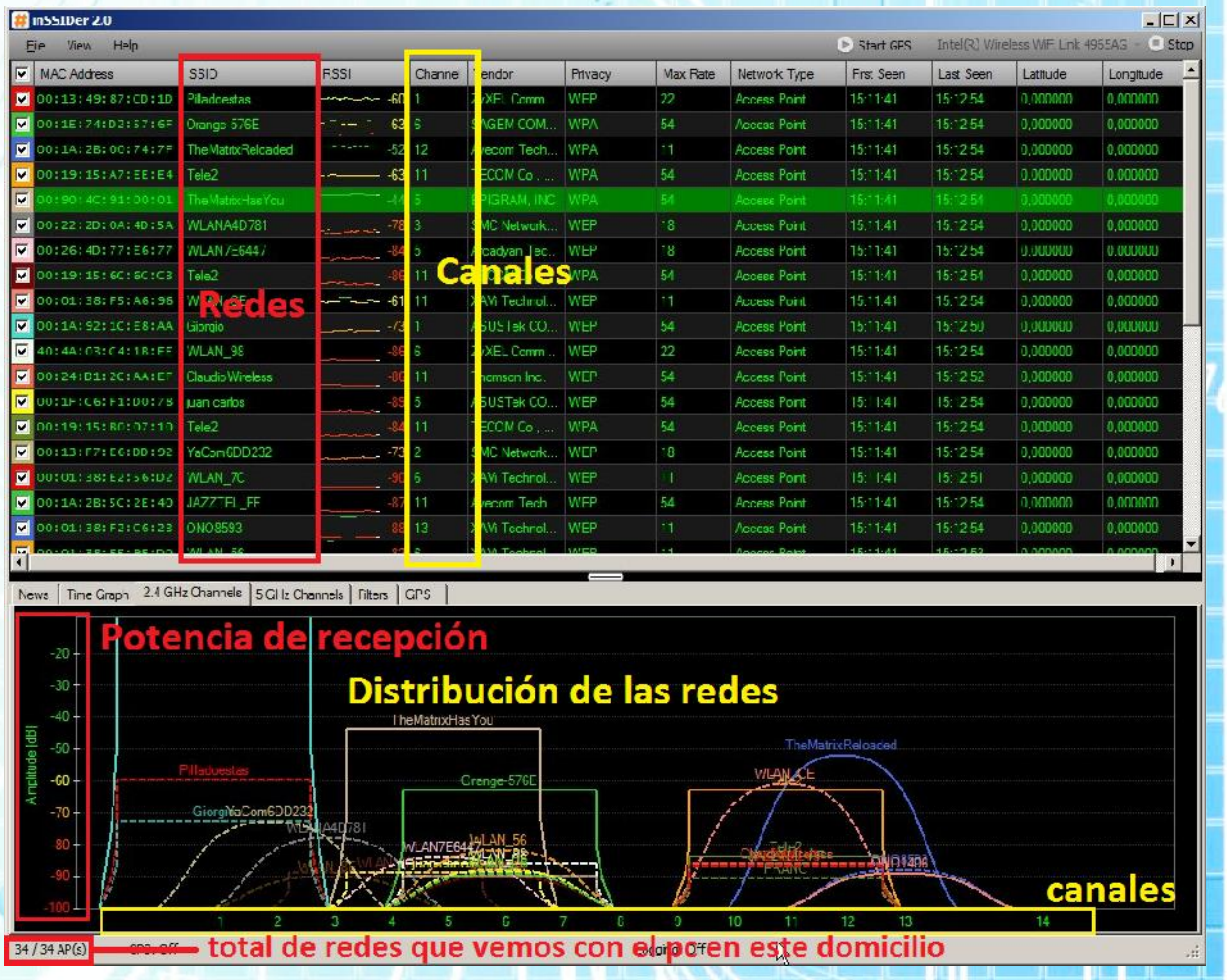
Redes locales inalámbricas

Arquitecturas redes inalámbricas

Canales

En el caso de necesitar ***poner en marcha un AP*** en una zona en la que ***puede haber gran cantidad de ellos***, usaremos una ***herramienta software*** para ***analizar el espectro***. Existen multitud de ***aplicaciones para teléfonos móviles y para PC*** que realizan esta función.





Redes locales inalámbricas

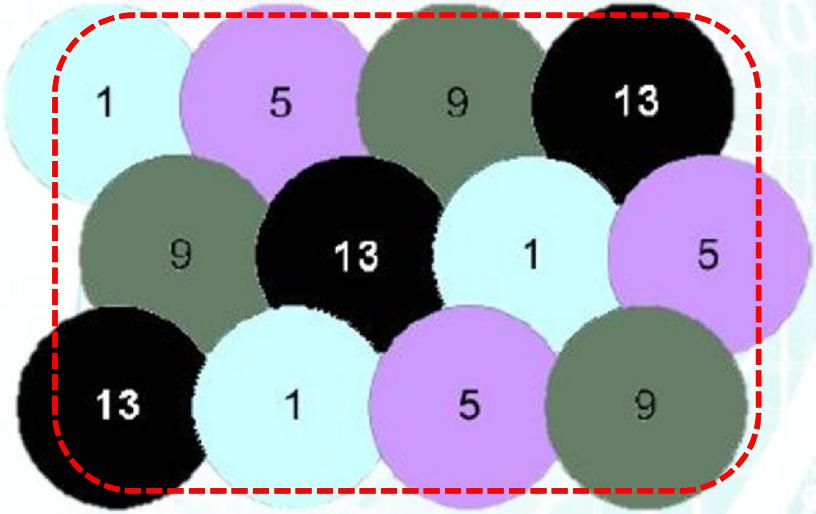
Arquitecturas redes inalámbricas

Canales

A la vista de los ***canales ajenos a nuestra instalación***, seleccionaremos uno en el que las ***interferencias externas sean las menores*** posibles. Algunas aplicaciones llegan a recomendar el canal a escoger. También se da el caso de que algunos ***AP pueden seleccionar el canal de funcionamiento más adecuado de forma automática***.

En el caso de que precisemos ***establecer una distribución Wi-Fi (WDS) por una empresa, un centro educativo, etc***. De forma que todos los ***AP pertenezcan a la misma red*** y ***se interfieran lo menos posible entre sí***, crearemos ***áreas de solapamiento de cobertura*** usando ***canales diferentes***. La figura siguiente puede aclarar el concepto, de esta forma, ***un usuario Wi-Fi tendrá cobertura en toda la instalación*** y los ***APs se interferirán de forma mínima***. Esta organización ***se complic***a si aparte de tener en cuenta el 'plano' debemos tener en cuenta ***diferentes plantas (niveles).***

Área aproximada cubierta por la red



WDS con diferentes canales

Redes locales inalámbricas

Arquitecturas redes inalámbricas

Canales

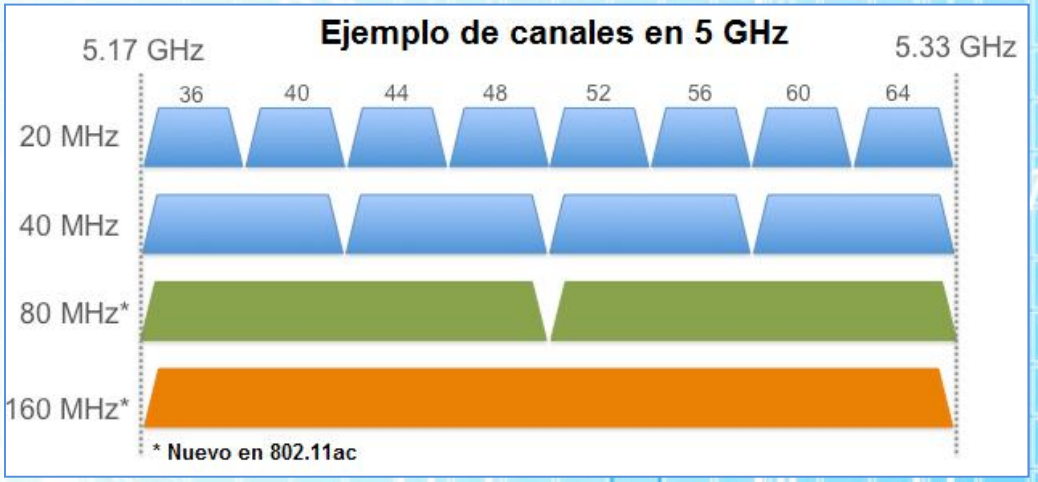
En el estándar ***IEEE 802.11n, además, se usan dos canales no solapados, cubriendo 40 MHz***, por ello, lo que hemos visto en las imágenes anteriores ***solo sirve para 802.11bg***.

Se recomienda ***usar canales de 40 MHz (modo 'n')*** solo si ***todos los dispositivos van a usar el estándar IEEE 802.11n.***

El ***estándar IEEE 802.11n*** es que también ***puede utilizar la banda de 5 GHz***, con ***menos problemas de interferencias*** y canales sin solapamiento.

El nuevo modo 802.11ac usa varios canales para poder lograr las prestaciones que vimos anteriormente.

bg WiFi n CERTIFIED	Antennas (Tx*Rx)	Spatial Streams	Maximum Link Speed	Band Support
Single Stream	1 x 1	1	72 Mbps	2.4
Dual Stream	1 x 2	2	150 Mbps	2.4
Dual Stream	2 x 2	2	150 Mbps	2.4
Dual Stream	2 x 3	2	150 Mbps	2.4
Dual Stream	2 x 2	2	300 Mbps	2.4 & 5
Dual Stream	2 x 3	2	300 Mbps	2.4 & 5
Multi Stream	3 x 3	3	450 Mbps	2.4 & 5



Otros parámetros a considerar

- La ***potencia máxima autorizada*** en España para ***emisión es de 100 mW o 20 dBm***.
- La ***sensibilidad de los equipos*** mínima para decodificar la señal recibida ***se expresa también en dBm***, ***por ejemplo -50 dBm.***
- El ***alcance varía con los obstáculos*** y depende en gran medida de los ***materiales de los mismos*** (hormigón, madera, cristal, etc.)
- Con ***antenas específicas***, de plano, directivas, etc ***podemos mejorar las condiciones*** de funcionamiento.

Redes locales inalámbricas

Dispositivos en redes inalámbricas

Dispositivos Wi-Fi

Cualquier dispositivo con la ***circuitería necesaria para establecer una conexión 802.11*** se puede considerar un dispositivo Wi-Fi que se ***puede incorporar a una red inalámbrica***.

Algunos ***equipos llevan incorporada la circuitería*** y en otros casos, ***se incorpora mediante interfaces y periféricos***. Podemos destacar los siguientes elementos como los más representativos:

- ***Puntos de acceso inalámbricos*** de todo tipo y variantes (interior, exterior, bridges, etc.)
- ***Tarjetas de red Wi-Fi*** para incorporar a equipos informáticos.
- ***Interfaces Wi-Fi*** a través de conexiones USB.
- Equipos con capacidad Wi-Fi incorporada:
  - ✓ Impresoras
  - ✓ Ordenadores portátiles
  - ✓ Routers ADSL, fibra óptica, etc.
  - ✓ Cámaras fotográficas
  - ✓ Teléfonos móviles
  - ✓ Tablets
  - ✓ Televisores
  - ✓ Receptores de satélite
  - ✓ Equipos multimedia (video, música, etc.)
  - ✓ Juquetes interactivos (robots, vehículos, muñecos, etc.)
  - ✓ Receptores de radio
  - ✓ Cámaras de vigilancia
- Módulos para incorporar en circuitos de desarrollo.

Redes locales inalámbricas

Dispositivos en redes inalámbricas

Dispositivos Wi-Fi

En general, independientemente de los dispositivos ***domésticos, industriales, domóticos, etc. que están en crecimiento***, la mayoría de los dispositivos Wi-Fi que nos vamos a encontrar actualmente en el ***entorno profesional y de hogar serán***:

- ***Equipos informáticos*** (ordenadores, portátiles, tablets, smartphones, etc.).
- ***Periféricos*** (impresoras, escáners, cámaras de vigilancia, etc.) .
- ***Interfaces*** de red (internos, tarjetas, dispositivos USB, etc.)
- ***Puntos de acceso*** de diferentes prestaciones.
- ***Routers de banda ancha*** con capacidad Wi-Fi.

Cabe ***recordar*** las siguientes ***características generales*** de los dispositivos ***Wi-Fi:***

- ✓ Cada dispositivo Wi-Fi tiene una ***MAC que lo identifica*** con carácter único, como veíamos en Ethernet.
- ✓ El ***medio de comunicación es compartido***, no solo por nuestra red, sino por ***todas las existentes en el entorno***.
- ✓ Los modos más ***avanzados son compatibles con los anteriores***, aunque ***a veces no conviene mezclarlos***.
- ✓ La ***cobertura y alcances son variables*** dependiendo del ***medio, obstáculos y de la situación de la instalación***.
- ✓ Es más ***vulnerable a ataques de terceros*** y a ***problemas de seguridad*** por el medio empleado.

Existen gamas especiales para establecimiento de enlaces entre edificios y funcionamiento a la intemperie:

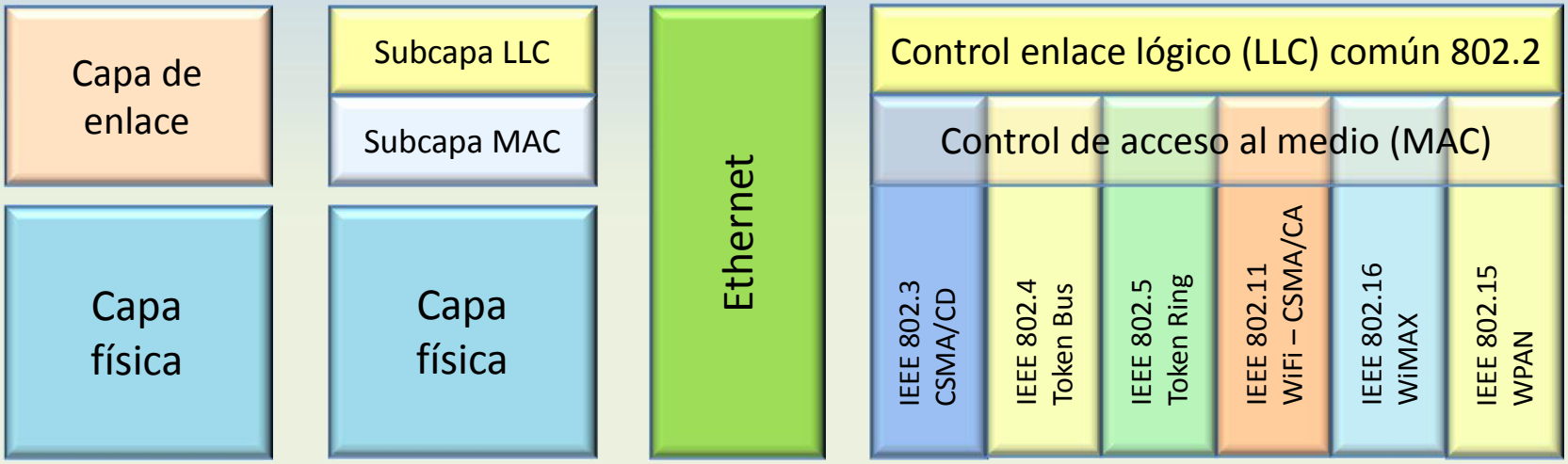
- ❖ ***Antenas directivas, paneles, omnidireccionales, etc.***
- ❖ ***Módulos Wi-Fi para exteriores*** para colocar junta a antena radiante.
- ❖ ***Equipos que soportan PoE*** y accesorios para los mismos.

Redes locales inalámbricas

Comunicaciones

Dispositivos Wi-Fi – IEEE 802.11

Ya en otro capítulo vimos que ***había diferencias entre las comunicaciones 802.3 y las 802.11***, estas diferencias se dan en las capas más bajas, es decir, la ***física y la de enlace***:



Como es lógico, la principal diferencia ***está en la capa física*** por los medios usados para transmitir y recibir los datos al tener que ir la ***información sobre señales de radiofrecuencia en vez de sobre un medio dirigido*** (cable o fibra).

Como se puede deducir, las comunicaciones en este medio son ***'half-duplex'.***

Nos vamos a referir a continuación al sistema de ***gestión de comunicación CSMA/CA*** y a las ***diferencias en las tramas ethernet y Wi-Fi***.

Comunicaciones

CSMA/CA: (Carrier Sense Multiple Access/Collision Avoidance)

Acceso múltiple con detección de portadora / Prevención de colisiones

Como podemos observar, ***el equipo detecta si está el canal ocupado*** antes de transmitir, ***si lo está, espera un tiempo aleatorio*** (contador backoff) y ***procede a volver a comprobar el canal***.

Si el canal está libre se transmite el dato y finaliza la comunicación a la espera del acuse de recibo (ACK) de la otra estación por el mismo método.

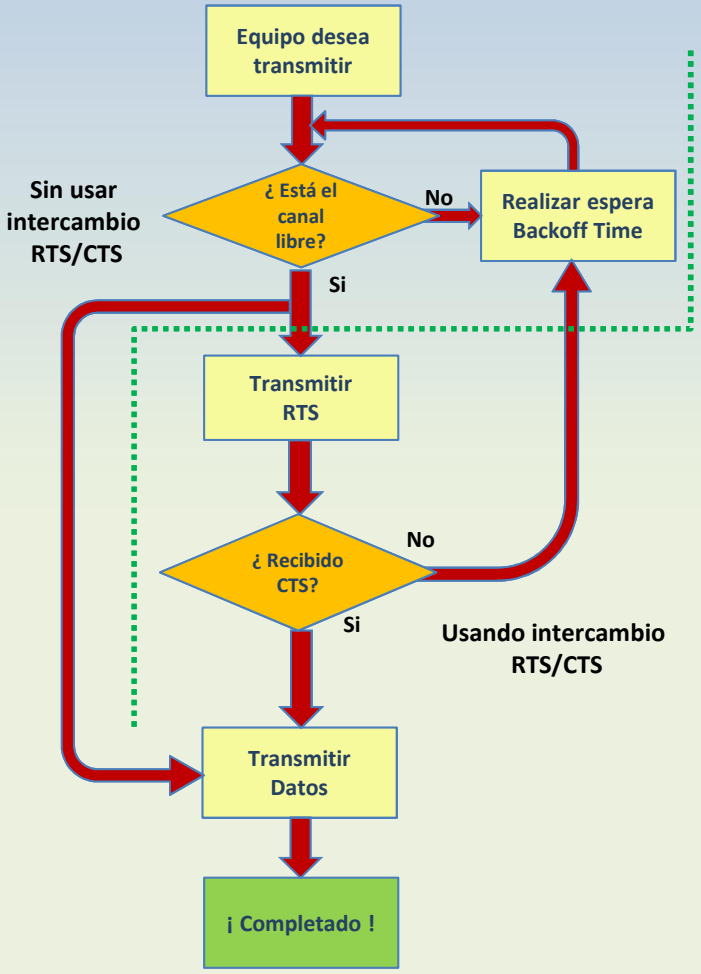
Como podemos ver, ***existe la opción de uso de RTS/CTS*** (*Ready To Send y Clear To Send*), manejada por el ***'master', punto de acceso*** que otorga el ***permiso a trasmitir que se pide con 'RTS'***, si se recibe '***CTS***' ***se procede a la transmisión***.

Los paquetes ***RTS y CTS son de corta duración para facilitar el diálogo***. Esta técnica ***mejora notablemente el efecto de 'estación oculta'*** que en el ***caso de no usar RTS/CTS da problemas***.

Estación oculta

No se trata de que un equipo se esconda, sino que ***en una red Wi-Fi***, todos los equipos ***no se tienen que 'ver' entre si***, de forma que ***no perciben el canal ocupado cuando el otro 'habla'.***

ACK: *Acuse de recibo, reconocimiento de entrega.*



Comunicaciones

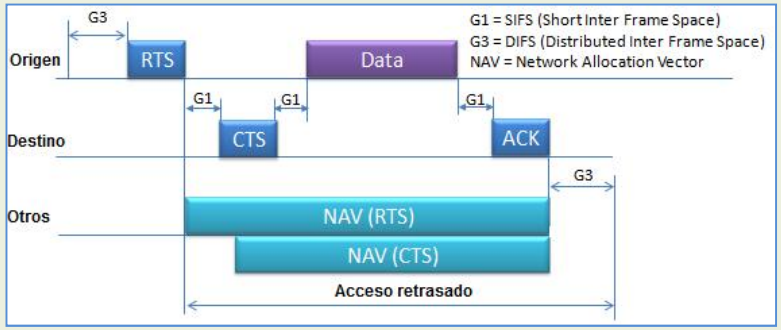
CSMA/CA: Estación oculta RTS / CTS

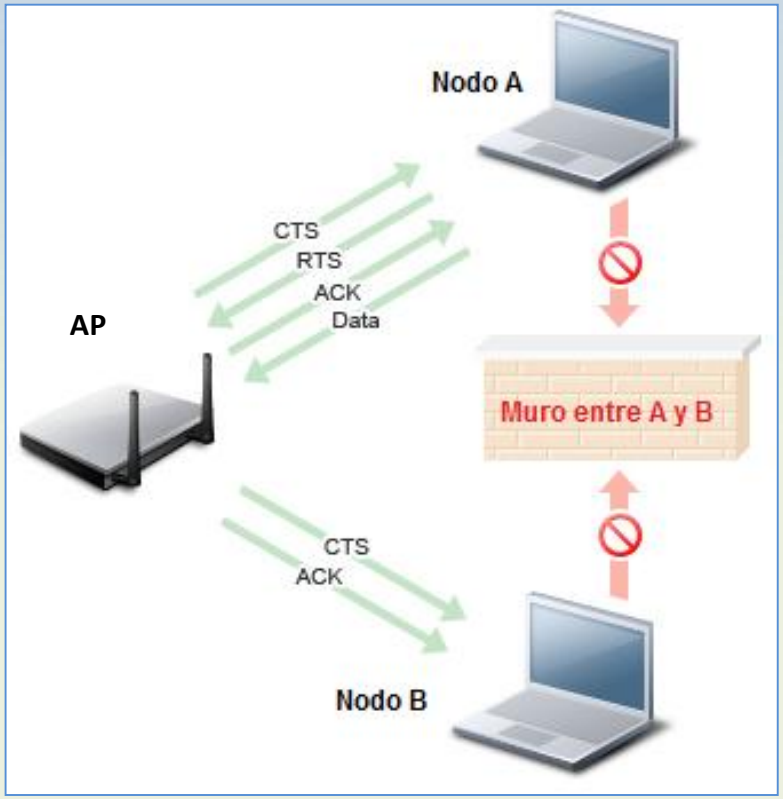
Como se ve en la figura, ***por problemas de cobertura***, el ***Nodo A no sabe cuando el Nodo B transmite y viceversa***, en este caso se podrían dar ***muchas colisiones*** ya que cuando ***A o B desea transmitir***, ***al no 'escucharse' entre sí,*** procedería a ***transmitir, creando problemas de colisión y haciendo que se repitieran muchos paquetes***.

Con el ***uso de RTS / CTS***, el punto de acceso que ***escucha a todos los nodos,*** es el que ***va dando 'paso'*** para la comunicación ***usando los envíos de CTS al nodo que los solicita***.

Estos paquetes ***(RTS/CTS) son muy cortos*** para que el índice de ***colisiones baje de forma notable***, un equipo que ***no tiene el permiso CTS, esperará a pedir de nuevo permiso para la transmisión***.

Esta gestión cobra mayor importancia ***cuantas más estaciones se encuentran en la red*** dependiendo de un mismo punto de acceso.



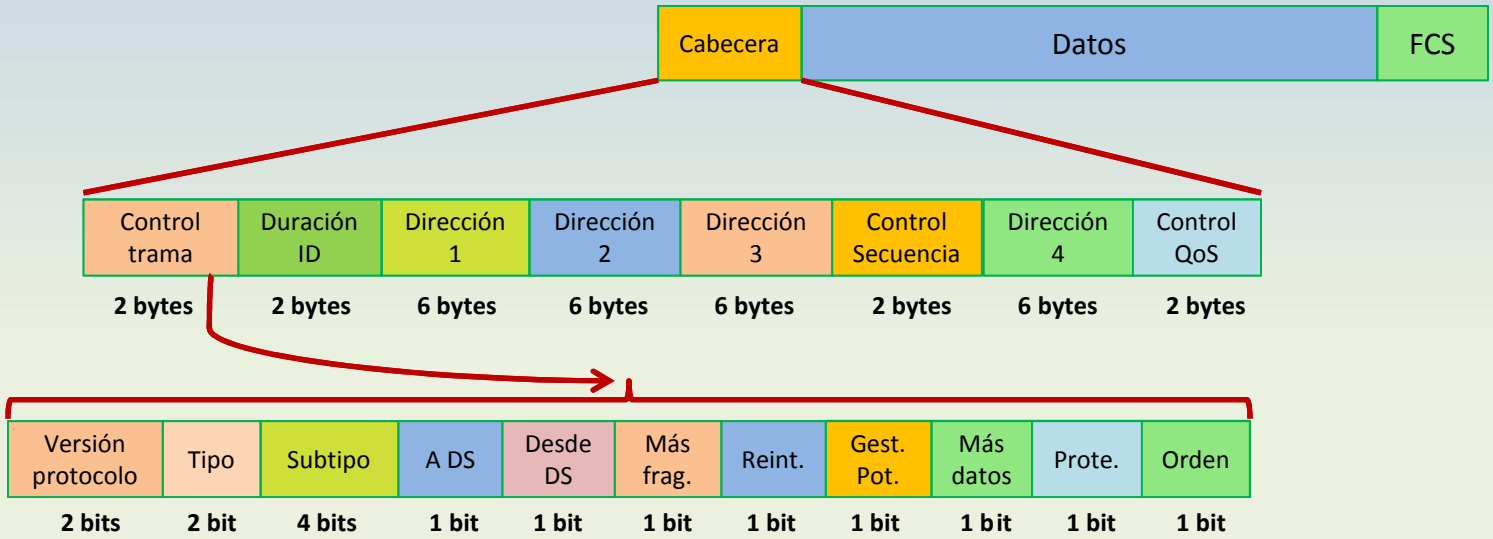


Redes locales inalámbricas

Comunicaciones

Trama IEEE 802.11

- Como comentamos anteriormente, se usa un ***direccionamiento igual al de Ethernet***, basado en ***direcciones MAC de 48 bits***.
- El ***sistema de tramas es diferente***, además de las de ***datos*** existen de ***control y administración*** (***beacon , probe y request frames).***



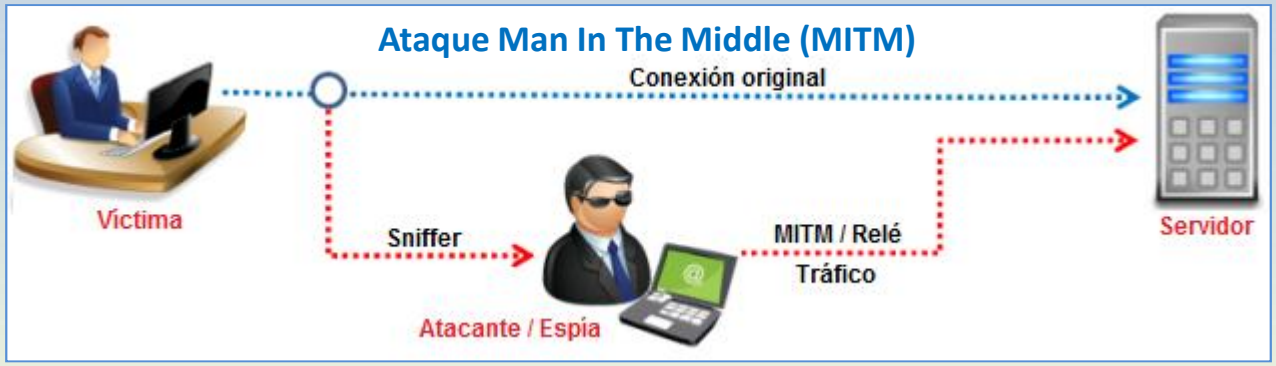
- La trama ***802.11 es similar en parte a las tramas Ethernet y 802.3*** vistas anteriormente pero con una ***cabecera más compleja***.
- Aparecen ***diferentes direcciones*** y la ***longitud de la cabecera puede ser variable*** (24, 26, 30 o 32 bytes).
- Esto se debe a las características variables que deben presentar las comunicaciones a través de puntos de acceso.
- La cabecera varía en función de que exista QoS o no y de que la comunicación sean entre puntos de acceso o punto-estación.
  - **24 bytes** -> Cliente y punto de acceso, sin QoS.
  - **26 Bytes** -> Cliente y punto de acceso, con QoS.
  - **30 bytes** -> Entre puntos de acceso, sin QoS.
  - **32 bytes** -> Entre puntos de acceso, con QoS.

Nota: Para saber más, consultar bibliografía.

Redes locales inalámbricas

Seguridad

El ***gran problema*** de las ***comunicaciones inalámbricas*** es la **seguridad**, ya que al usar un ***medio 'no guiado' y compartido*** se pueden dar multitud de ***situaciones en que las comunicaciones no son seguras***, incluso se pueden realizar ***ataques o escuchas desde el exterior*** y a ***cierta distancia***.



Los ***peligros son diversos***, pero dependiendo del tipo de red pueden ser muy elevados, ***los más comunes son***:

- ***Denegación de Servicios*** (DoS).
- ***Daño en equipos*** (borrados, desconfiguración, etc.)
- ***Accesos no autorizados*** a datos, sistemas, etc.
- ***Robo de Información***.
- ***Inserción de códigos dañinos*** (virús, keylogger, troyanos, etc.).
- ***Robo de credenciales*** (certificados digitales, autenticación, etc.).
- ***Uso fraudulento de Internet***.

✓ ***No existe un sistema seguro al 100%*** en el uso de conexiones inalámbricas, aunque hay ***diversas herramientas y técnicas*** que permiten hacer ***más difícil el acceso*** no deseado a las redes inalámbricas.

✓ En ***algunos casos***, por estos problemas, ***queda prohibido el uso de sistemas inalámbricos en una red corporativa.***

Redes locales inalámbricas

Seguridad

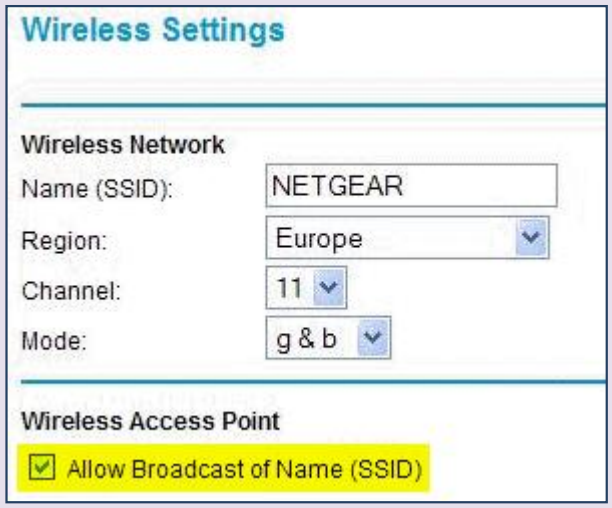
Para intentar ***minimizar este problema*** existen diferentes ***herramientas*** que permiten ***diferentes grados de 'protección',*** vamos a ir viendo las más importantes junto con sus cualidades y defectos. Algunas medidas ***se pueden usar de forma conjunta***.

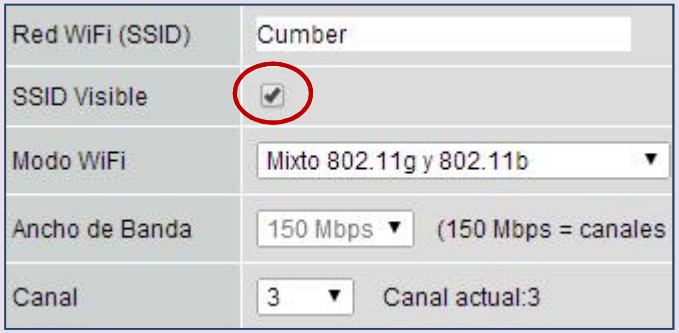
Ocultación del SSID

Si ***ocultamos los paquetes 'baliza'*** que ***identifican el punto de acceso*** ('**beacon frames**') con ***el SSID***, este ***no será visto por equipos clientes al no estar anunciado***, lo cual ***permite evitar que algunos usuarios intenten la conexión***.

Al ***no estar anunciado***, habrá que ***conocer el SSID*** e indicarlo de forma manual ***al configurar el cliente de red WiFi***.

Para ***configurar esta característica en el punto de acceso***, buscaremos algo parecido a '***Beacon frames***' enable / disable, ***Send SSID***, etc., ***no hay una regla fija*** para todos los puntos de acceso, aunque ***será bastante explícita***.





Este ***sistema de protección es bastante limitado***, ya que ***cualquier monitor de tráfico WiFI*** podrá ***ver los otros paquetes del punto de acceso***, haciendo inutil esta **'ocultación'**.

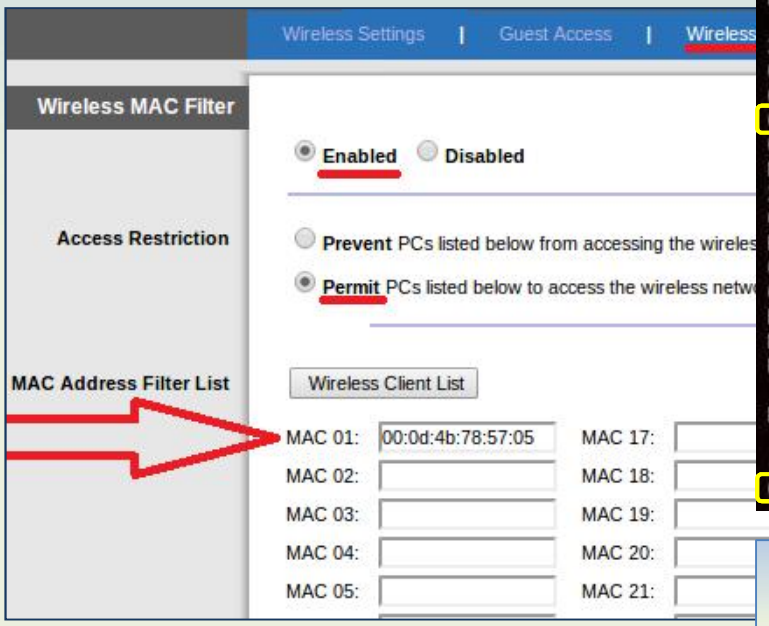
Redes locales inalámbricas

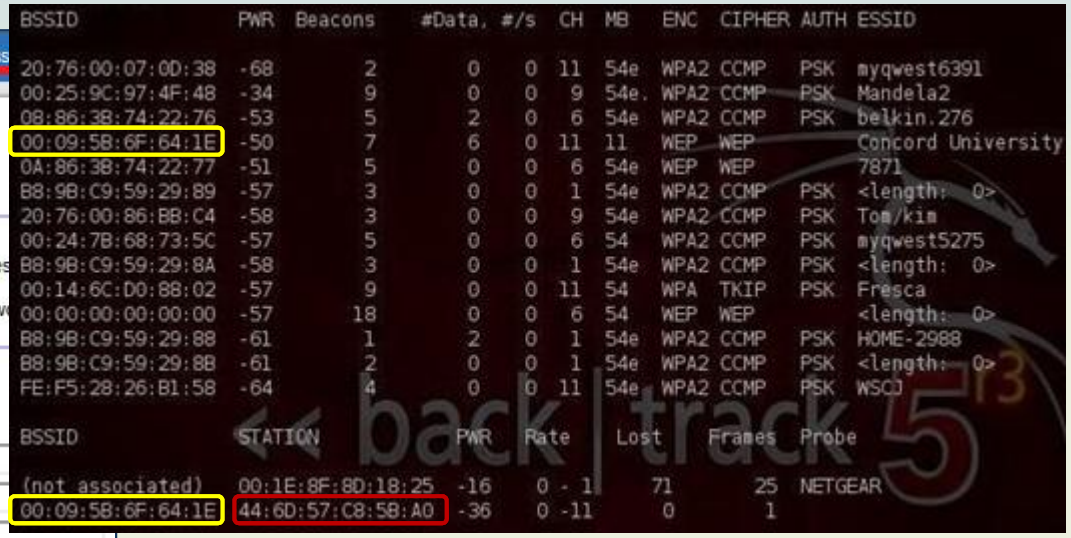
Seguridad

Filtrado por MAC

Otra forma de ***limitar el acceso no deseado*** es ajustar el punto de acceso para que ***solo permita la conexión (asociación) a determinados clientes cuyo NIC WiFi tengan una MAC determinada***. También ***es posible denegar el acceso a MAC de clientes concretas***.

Para ajustar esta característica, buscaremos una ***sección parecida a 'MAC filter', filtrado MAC, etc*** y ajustaremos los parámetros según nuestras necesidades, también es posible, en la mayoría de los casos, elegir si las ***´MAC' indicadas tendrán acceso o se les negará*** el acceso, así como ***habilitar o inhabilitar (enable/disable) esta función***. (Hay que ***mantener la tabla***, es un ***trabajo 'engorroso' ?***):





Este ***sistema de protección es más avanzado que la ocultación del SSID***, aunque ***tampoco es definitivo***, ya que como sabemos, la ***MAC de los clientes autorizados se pueden capturar*** y el ***'intruso' puede 'modificar' su MAC*** para ***sustituir al cliente legítimo***.

Redes locales inalámbricas

Seguridad

Cifrados

La forma más usada de protección a redes WiFi es el uso de mecanismo de cifrado, existiendo en la actualidad diversos sistemas. Vamos a destacar los más importantes.

WEP

Es el ***más antiguo de los sistemas 'populares'***. ***WEP (Wired Equivalent Privacy)*** - Privacidad Equivalente a Cableado - proporciona ***cifrado básico compartido en la capa dos***. WEP trabaja con casi todos los dispositivos WiFi. Usa ***algoritmo de encriptación RC4.***

Su ***única ventaja en la actualidad***, es que está ***soportado por prácticamente el 100% de los dispositivos existentes***, al ser el primero en generalizarse.

Su ***principal inconveniente***, es que tiene ***múltiples fallos de seguridad*** que lo hacen vulnerable, siendo posible ***'romper' el cifrado y 'encontrar' la clave*** mediante herramientas comunes y en ***cuestión de minutos***.

Si usamos ***WEP***, tendremos que ***configurar el punto de acceso y los clientes con una 'clave'*** común para todos ellos.

Hay ***dos formatos posibles*** para la clave, el ***más simple usa 5 caracteres alfanuméricos (diez en hexadecimal / 40 bits)*** y el más ***robusto, o formato 'largo' usa 13 caracteres alfanuméricos (26 en hexadecimal / 104 bits)***.

A estos bits se les añade un ***'vector de inicialización' (24 bits)*** que hace que sumen ***hasta 64 o 128 bits en total***.

Existen ***variantes más modernas con claves más largas***, pero el ***vector de inicialización sigue siendo de 24 bits*** y la debilidad del sistema (***paquetes IV***). Capturando ***paquetes de este tipo se puede desencriptar la clave WEP*** de forma sencilla.

Open y Shared Key son métodos de ***autenticación y asociación*** usando encriptación WEP, ***no implican más seguridad*** uno que otro, solo cambia el ***procedimiento de 'presentación' y 'asociación'.***

Este sistema de seguridad ***se puede combinar con el filtrado por MAC, dando algo más de seguridad a la red WiFi.***

Redes locales inalámbricas

Seguridad

WPA

- Es la siguiente generación de protección para sistemas WiFi para eliminar las debilidades de WEP. WPA significa 'Acceso Protegido WiFi' (*Wi-Fi Protected Access*). Es un ***paso intermedio entre WEP y WPA2***.
- Usa un protocolo de seguridad llamado **TKIP** *(Temporal Key Integrity Protocol), está basado en* ***encriptación RC4 con claves dinámicas de 128 bits.***
- Permite el uso del ***mismo hardware de los sistemas WEP***, con lo que solo es necesario ***actualizar el firmware del equipo***.
- Este estándar tiene ***dos modos de funcionamiento según los requerimientos de seguridad:***

  ✓ **WPA-PSK** o **WPA Personal** (*WPA Pre-Shared Key*): para ***entornos SOHO*** (***pequeñas empresas y hogar***), con una ***clave compartida de hasta 63 caracteres alfanuméricos***.

Este sistema de encriptación es más difícil de descifrar y hoy por hoy ***la forma de ataque más común es por 'diccionario' o fuerza bruta***, es decir, con herramientas software que tienen capacidad para ir ***probando claves de un diccionario*** o incluso generándolas de forma ordenada. Con una ***clave adecuada (?)*** se hace ***casi imposible la desencriptación.***

Nota: Algunos proveedores ISP asignan ***claves 'estandar'*** fáciles de 'calcular' según MAC o algoritmo.

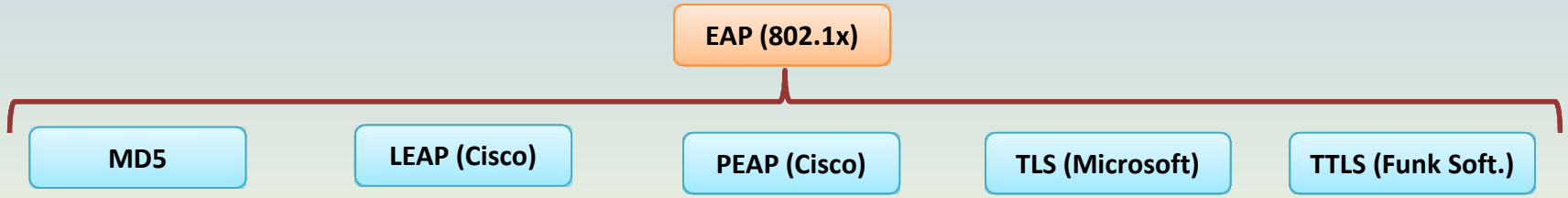
✓ **WPA Enterprise**. Concebido para ***entornos profesionales***, precisa un ***servidor RADIUS para autenticación por credenciales***. Está basado en un ***componente llamado EAP (Extensible Authentication Protocol),*** que surgió como mejora del método de autenticación utilizado en PPP (point to point protocol).

Redes locales inalámbricas

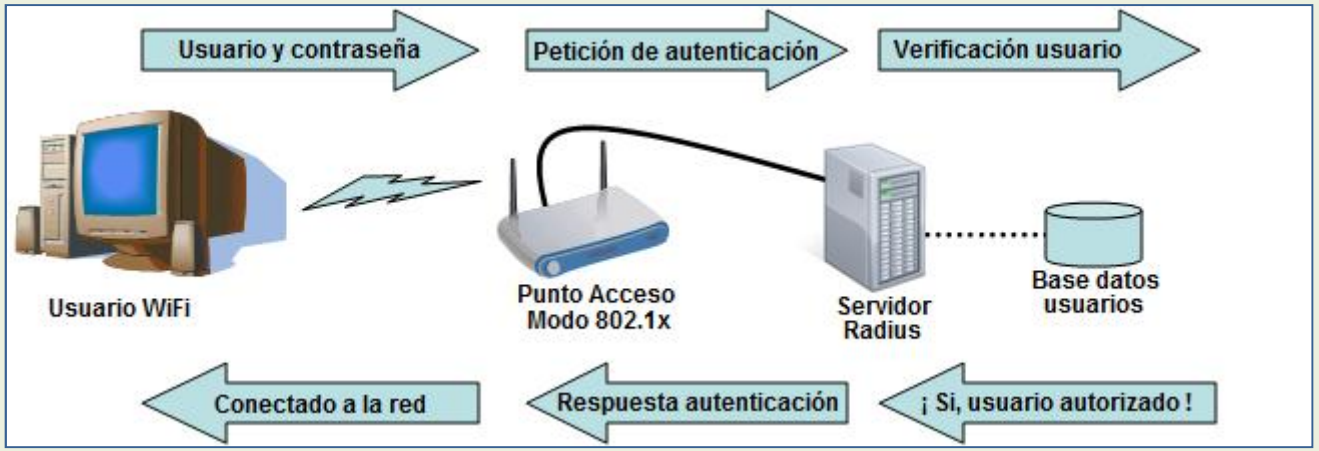
Seguridad

WPA Enterprise (IEEE 802.1x)

- Se usa exclusivamente en entornos profesionales debido a que trabaja con un servidor RADIUS y una base de datos de clientes autorizados.
- Esta basado en EAP ***(Extensible Authentication Protocol), por el que se identifica al usuario del equipo contra una base de datos, no hay una 'contraseña para todos'. Existen diferentes modos de uso de EAP según los fabricantes.***



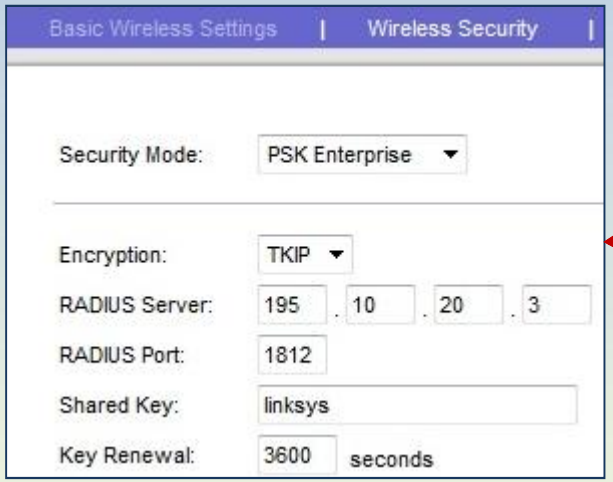
- Tanto el ***punto de acceso como los clientes*** requieren la configuración del ***modo de trabajo como del sistema EAP usado***.



Redes locales inalámbricas

Seguridad

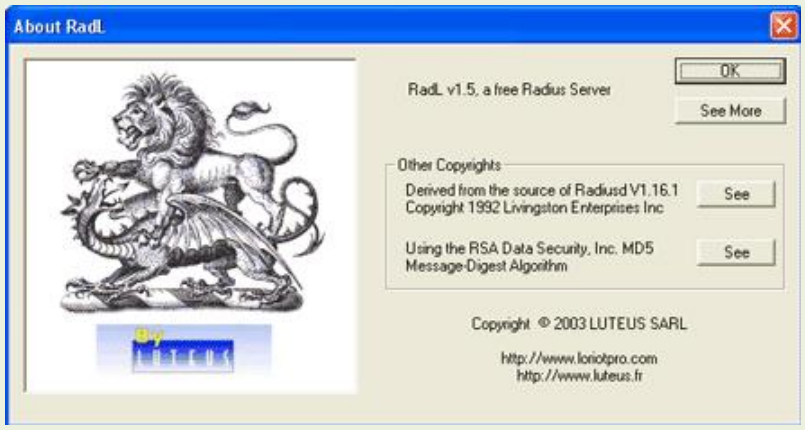
WPA Enterprise (IEEE 802.1x)

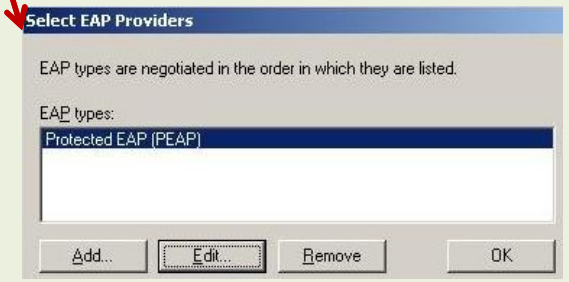


Cliente

Punto Acceso

Servidor





Redes locales inalámbricas

Seguridad

WPA2

- Nuevo estándar que incluye ***todas las características de WPA*** y los ***modos de WPA*** (Personal y Enterprise).
- Cambia la ***encriptación RC4 por encriptación AES***, más robusta.
- Los equipos con ***WPA2 pueden necesitar hardware diferente*** para implementar ***AES***.
- El método de ***ataque más común*** es por ***diccionario***.

Estándar	Seguridad	Autenticación	Encriptación
IEEE 802.11	WEP	No hay	RC4
WPA	TKIP	IEE802.1x (EAP)	RC4
WPA2 (IEEE)	TKIP	IEE802.1x (EAP)	AES

Notas generales seguridad

- En ***sistemas modernos***, existe la posibilidad de ***configurar la red WiFi*** de forma rápida mediante el ***uso de WPS***, este sistema se ***debe desactivar inmediatamente después de la configuración de la red***, pero en muchos casos de deja activo y constituye una ***nueva vulnerabilidad que puede permitir romper la clave en unas horas***.

- Se pueden producir ***ataques del tipo DoS*** (denegación de servicio) que aunque ***no rompen la clave, provocan problemas en la red*** (al ser medio compartido), ***el más común es el de desautenticación***, que ***desconecta a los clientes legales*** atacados de la red WiFi. ***Este tipo de ataque no se puede evitar, algunos fabricantes tienen sistemas que bloquean las órdenes de desautenticación***, pero el problema ***va relacionado con el medio de comunicación (abierto – no guiado).***

Redes locales inalámbricas

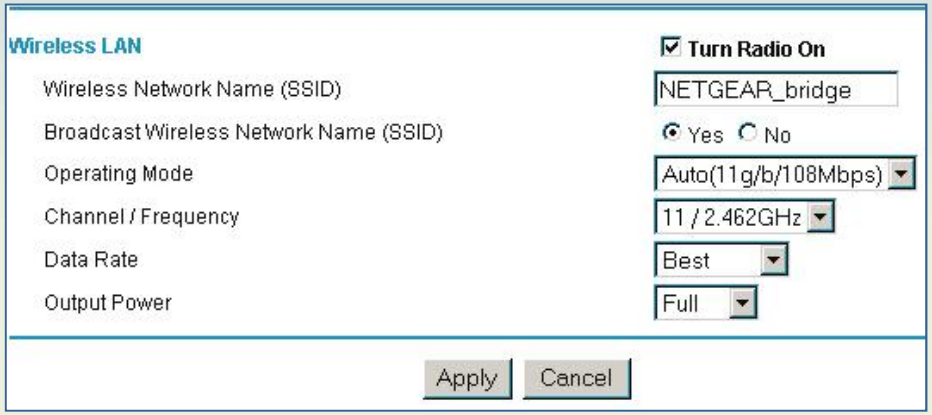
Configuración de un punto de acceso

No existe una forma específica para configurar los puntos de acceso inalámbricos, aunque si se pueden distinguir ***unas tareas que suelen ser comunes*** a todos los sistemas.

- ***Configuración LAN*** (parte correspondiente a red cableada):
  - Dirección IP, máscara de subred, servidores DNS y gateway.
  - Servidor DHCP activado o desactivado (En caso de activarlo se pueden definir rangos de servidor DHCP).

- ***Configuración WiFi:***
  - Modo de trabajo: Punto de acceso, repetidor, bridge (normalmente Punto de Acceso)
  - SSID (Identificador de red WiFi).
  - Canal de trabajo.
  - Emitir SSID (Enabled / disabled) y tiempo de reemisión.
  - Seguridad WiFi: WEP, WAP, WAP2, variantes TKPI / AES, clave de red.
  - Configuraciones avanzadas en caso de usar RADIUS.
  - Modo de trabajo: b, g, n, ac, automático, etc.
  - Potencia de emisión (hay un máximo legal de 100 mW / 20 dBm).

- ***Otros parámetros***:
  - Filtrado de direcciones MAC de clientes.
  - Control parental (limitaciones de horario de acceso).
  - Control de acceso al P.A. (contraseña configuración).
  - Registro de incidencias.



En la mayoría de los casos, los ***puntos de acceso inalámbricos se configuran mediante un navegador***, para ello es necesario ***conocer la IP*** del mismo, en caso de no conocerla, ***se podrá resetear a unos valores por 'defecto',*** en cualquier caso, el ***manual del punto de acceso*** puede ser necesario para llevar a cabo una correcta configuración.

Enlaces a emuladores

http://ui.linksys.com/files/ , http://www.trendnet.com/products/emulators.asp

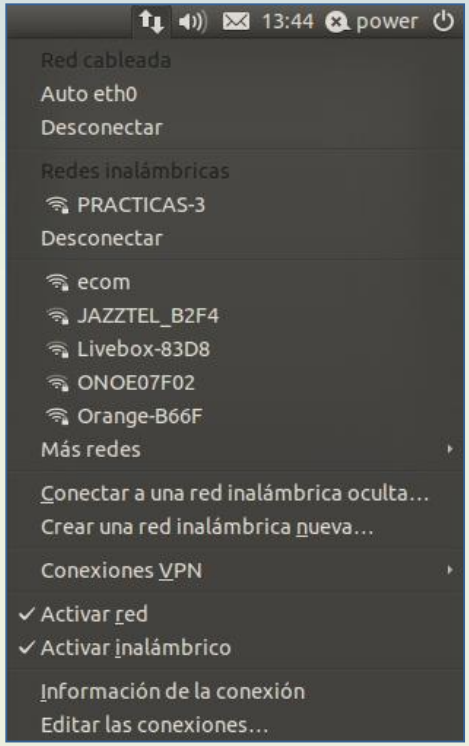
Redes locales inalámbricas

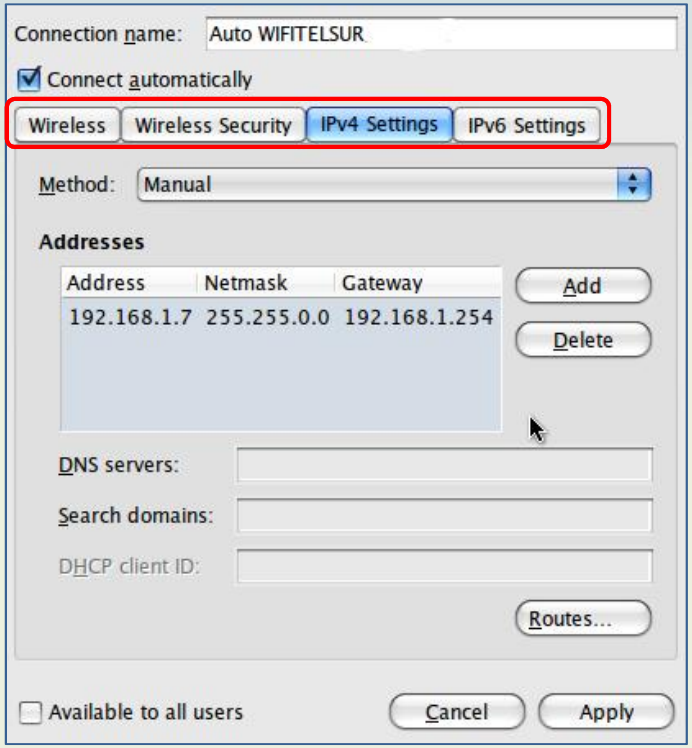
Configuración de clientes WiFi

Existen ***multitud de clientes posibles para redes WiFi***, con diferentes ***tipos de dispositivos y diferentes sistemas operativos***. Teléfonos, tablets, ordenadores portátiles, impresoras, televisores, ordenadores de sobremesa, etc.

En general, los dispositivos ***clientes disponen de sistemas gráficos y/o interactivos que facilitan la configuración***, mostrándonos las ***redes disponibles y en muchos casos basta con introducir la contraseña*** de la red.

En ***otros casos*** es necesario ir más allá y ***establecer el SSID, el modo de seguridad elegido, la IP que tendrá el equipo (si no se oferta por DHCP), etc.***





Bibliografía

- LAN inalámbrica y conmutada - Autor: Lewis - Editorial: Pearson Educación
- Sistemas Informáticos y redes locales - Autor: Manuel Santos y Juan Carlos Moreno - Editorial: Ra-Ma
- Redes de computadoras - Autor: Tanenbaum - Editorial: Pearson
- Redes inalámbricas - Luis Miguel Cabezas y Francisco J. González - Ed. Anaya Multimedia

DIRECCIONES DE INTERÉS

- ✓ www.wikipedia.org - La enciclopedia libre
- ✓ www.cisco.com - Fabricante de dispositivos de red
- ✓ http://www.eslared.org.ve/walc2012/material/track1/05-Introduccion_a_las_redes_WiFi-es-v2.3-notes.pdf
- ✓ media.pearsoncmg.com/aw/aw_kurose_network_2/applets/csma-ca/withouthidden.html
- ✓ Búsquedas con www.google.com