TEMA REDES INALÁMBRICAS.

1 Introducción.

Los medios inalámbricos son medios no guiados que basan su funcionamiento en la radiación de energía electromagnética. Uno de los principales problemas en el uso de redes inalámbricas es sin duda la seguridad que pueden o no, ofrecer contra intrusiones.

Aunque una red inalámbrica implica falta de cableado, en la práctica es poco frecuente encontrar redes inalámbricas puras, generalmente se encuentran formando parte de otras redes con cableado generando lo que se conoce como **redes híbridas.**

2 Tipos de redes sin hilos.

Como acabamos de ver una red inalámbrica (*Wireless*) utiliza ondas electromagnéticas para enlazar los equipos a la red, en lugar de los cables que se utilizan en las LAN convencionales cableadas (Ethernet, Token Ring, etc.).

Las redes sin hilos o inalámbricas, al igual que las redes cableadas admiten varias clasificaciones, vamos a ver algunas de ellas.

- Las redes sin hilos se pueden dividir en dos categorías, basándose en ***su tecnología***: LAN y Computación móvil.

  La diferencia fundamental entre estas categorías radica en el sistema de transmisión utilizado. Las LAN sin hilos utilizan transmisores y receptores propiedad de la compañía donde funciona la red. La computación móvil utiliza medios de transporte público, por lo tanto se trata de una WAN.

- Al igual que las redes cableadas vamos a clasificar a las redes inalámbricas según ***su alcance*** en los siguientes grupos:
  - **Redes Inalámbricas de Área Personal** o *WPAN* (*Wireless Personal Area Network*): definidas por el estándar IEEE 802.15, es una red sin cables que se extiende a un espacio de funcionamiento personal con un radio máximo de 10 metros. Están pensadas para interconectar los distintos dispositivos de un usuario. Es el caso de la tecnología **Bluetooth**.
  - **Redes Inalámbricas de Área Local** o *WLAN* (*Wireless Local Area Network*): cubren distancias de unos cientos de metros. Están pensadas para crear un entorno de red local entre ordenadores situados en un mismo edificio o grupo de edificios. Es el caso de las tecnologías **Wi-Fi** o **HomeRF,** por ejemplo.
  - **Redes inalámbricas de Área Metropolitana** o *WMAN*: pretenden cubrir el área de una ciudad o entorno metropolitano. Ejemplo más conocido para este tipo de redes es **WiMAX** definido en el protocolo IEEE 802.16 que busca dotar de conectividad a dispositivos fijos que se encuentran a una distancia considerable, por ejemplo, en zonas rurales a las cuales no se tiene acceso a través de medios guiados extendiendo las redes inalámbricas a un ámbito metropolitano.
  - **Redes globales o** redes inalámbricas de Área Extensa (WWAN): que ofrecen la posibilidad de cubrir una región, país o grupo de países. Estas redes se basan en tecnología celular y han aparecido como evolución de las redes telefonía móvil.

En este tema nos centraremos fundamentalmente en las redes inalámbricas de área local (WLAN) y dentro de estas en el estándar más extendido, el IEEE 802.11 que define la tecnología Wi-Fi.

3 Medios de transmisión inalámbricos.

Son medios no guiados que basan su funcionamiento en la radiación de energía electromagnética. Los medios de transmisión inalámbricos se pueden clasificar en cuatro tecnologías:

- Ondas de radio
- Microondas
- Infrarrojos
- Láser

En todas ellas existen dos configuraciones para la emisión y recepción: direccional y omnidireccional:

- En **transmisión direccional** toda la energía se concentra en un haz que es emitido en una cierta dirección, por lo que el emisor y el receptor deben estar alineados.
- En **transmisión omnidireccional** la energía es dispersada en todas direcciones, por lo que varias antenas pueden captarlas.

El uso de una u otra configuración dependerá de la frecuencia a la que se emite ya que para frecuencias altas es mejor la transmisión direccional.

Para enlaces con varios receptores se utilizan ondas de radio que emiten a bajas frecuencias.

A continuación se detallan las características de cada tipo de tecnología inalámbrica:

- **Ondas de radio**:

  Son fáciles de generar, pueden recorrer largas distancias, penetran en los edificios sin problemas y viajan en *todas las direcciones* desde la fuente emisora.

  Las redes Wifi (802.11) utilizan este tipo de transmisión. La tecnología *Bluetooth* también se engloba en este tipo de transmisión.

- **Microondas:**

  Las microondas permiten transmisiones tanto terrestres como con satélites Son *direccionales*. Transmisor y receptor deben estar alineados de forma muy precisa

  A diferencia de las ondas de radio, las microondas **no atraviesan bien los obstáculos,** de forma que es necesario situar antenas repetidoras cuando queremos realizar comunicaciones a largas distancias.

- **Infrarrojos:**

  Se utilizan para comunicaciones de corto alcance y **no pueden atravesar paredes** .

  Utilización *direccional* y en interiores, pues el sol interfiere estas comunicaciones.

- **Láser:**

  Similar a la tecnología de infrarrojos (uso *direccional* con emisor y receptor alineados, **no atraviesan paredes**, etc.) pero puede utilizarse en exteriores por lo

que su uso más común es conectar redes entre dos edificios que tengan visión directa entre ellos.

Cuando distintas tecnologías utilizan una misma banda de frecuencia la compartición del medio supone un problema puesto que dos comunicaciones de distinta tecnología que utilicen la misma banda pueden interferirse, por ejemplo, Bluetooth y Wi-Fi.

Otro problema es la seguridad de la información dado que el medio es accesible por cualquier dispositivo que se encuentre dentro del alcance de la onda.

4 Protocolos de redes inalámbricas.

Como hemos indicado en preguntas anteriores en este tema nos centraremos fundamentalmente en las redes inalámbricas de área local (WLAN) y dentro de estas en el estándar más extendido, el IEEE 802.11 que define la tecnología Wi-Fi.

4.1 Protocolo IEEE 802.11. Wi-Fi

Este protocolo es el estándar más extendido para la creación de LAN sin hilos. Los orígenes de la norma Wi-Fi se remontan a finales del siglo XX. IEEE acogió esta norma en IEEE 802.11.

La norma IEEE 802.11 solo se diferencia de la 802.3 (Ethernet) en la forma en que los equipos acceden a la red, en una red Ethernet el método de acceso al medio es el **CSMA/CD** y en las 802.11 es el **CSMA/CA**. El resto es idéntico en ambas. Por tanto una red local inalámbrica 802.11 es totalmente compatible con todos los servicios de las redes locales cableadas Ethernet.

CSMA/CA Es una variante de CSMA en la que los dispositivos antes de transmitir envían una petición indicando que tienen datos que transmitir.

El estándar IEEE 802.11 tiene variantes (802.11a, 802.11b, 802.11g, 802.11n...). Cuando un dispositivo opera con una tecnología predecesora, toda la red se adapta a esa tecnología, lo que provoca que el rendimiento de la red disminuya considerablemente.

En la actualidad para facilitar el reconocimiento de versiones se ha sustituido la identificación anterior por la siguiente:

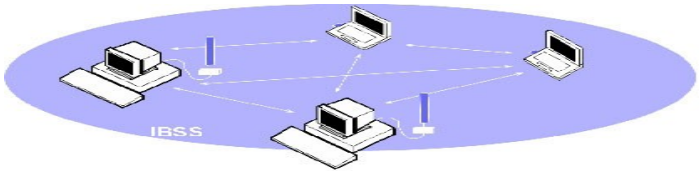
Estándar WiFi	Redes
WiFi 4	802.11n
WiFi 5	802.11ac
Wifi 6	802.11ax

5 Topología para el IEEE 802.11

5.1 Modo Ad-hoc

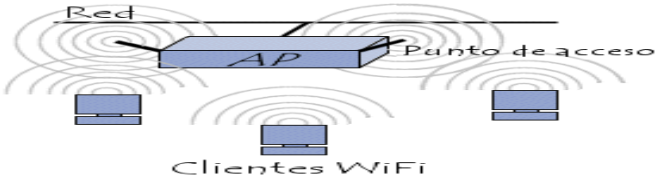
No existe ningún intermediario. No es una forma habitual de montar una red, sería el equivalente de una conexión con cable cruzado entre dos pcs cableados.

Por ejemplo, Bluetooth y la transmisión por infrarrojos utilizan este modo de conexión.



5.2 Modo AP, Normal o Raíz

En **modo infraestructura , Puntoa de Acceso, normal o Raíz** está coordinado por una entidad denominada **"punto de acceso"** (Access Point, AP o SAP). Si una estación quiere transmitir datos a otra deberá hacerlo pasando por el punto de acceso. Puede decirse que el punto de acceso actúa como un hub inalámbrico. En este modo dos estaciones que no tengan cobertura entre sí, pueden transmitirse datos gracias al punto de acceso.

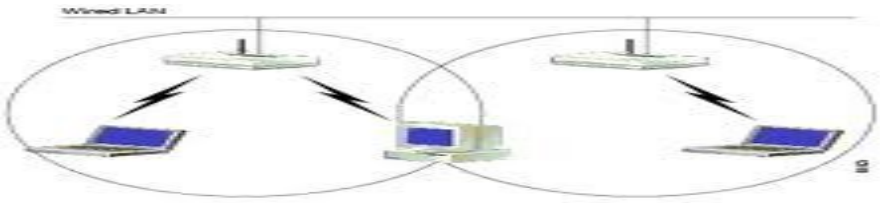


Varios Puntos de Acceso

5.3 Modo Roaming.

En esta configuración existen varios puntos de acceso **pertenecientes a una misma red**, de forma que se pueda cubrir un área mayor. El dispositivo que se conecta a la red es capaz de ir cambiando de un punto de acceso a otro según la potencia de la señal emitida y sin pérdida de la conexión.

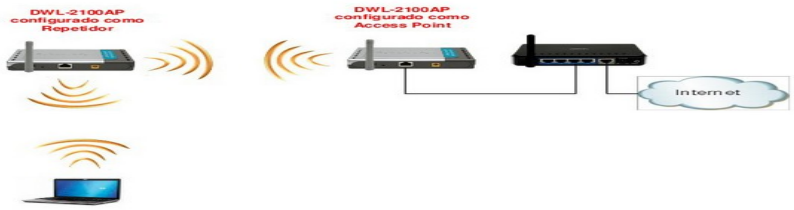
Cuando varios AP operan en modo AP o Raíz en una misma zona, deberán utilizar canales diferentes para no interferirse. Este es el modo que se utiliza en las redes WiFi con roaming.



5.4 Modo Repetidor

En esta configuración existen varios puntos de acceso pertenecientes a una misma red, pero **sólo uno de ellos está conectado a la red cableada.**

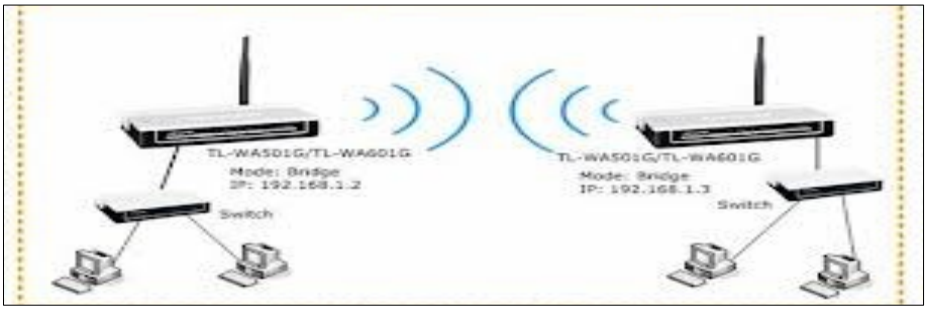
El **resto de los Aps repiten la señal emitida por el primero** para ampliar el alcance de la red inalámbrica, es decir el resto de Aps no publican un BSS, sino que se conectan a uno ya existente en otro AP.



5.5 Modo Puente o Bridge

En esta configuración se crea un puente entre dos redes distintas. **Cada AP sólo se comunicará con el otro.**

El AP no pública un BSS sino que se conecta a uno ya existente de otro AP para hacer de puente**.**



5.6 Modo Cliente

En esta configuración un **AP se conecta por cable a un dispositivo y funciona como si se tratara de una tarjeta de red inalámbrica para dicho dispositivo**.

6 Redes mixtas.

Las IEEE 802.11 son totalmente compatibles con Ethernet. Para ello necesitamos que el punto de acceso, que debe llevar puertos de red no inalámbricos, haga de intermediario entre la parte cableada de la red y la parte inalámbrica. Este es el modo de conexión habitual utilizado en las instalaciones de red comerciales, formando una red mixta.

7 Elementos de las redes inalámbricas.

Para establecer una conexión de tipo inalámbrico es necesario, realizar dos acciones: *instalar tarjetas de red inalámbricas* en cada equipo y configurar *un punto de acceso*.

Como vimos anteriormente, el punto de acceso es un dispositivo que permite ampliar el alcance de la señal entre dos o más equipos conectados a la red repitiéndola.

7.1 Adaptadores inalámbricos.

Los equipos acceden a la red inalámbrica a través de tarjetas de red.

En las redes inalámbricas, no se usan cables para conectar los equipos. Por ese motivo no tendremos que buscar un conector donde enchufar nada, sino que lo que veremos es una pequeña antena e incluso, a veces ni eso porque va integrada en el adaptador

Al igual que para las redes cableadas, en las redes inalámbricas es necesario:

- Que el adaptador esté conectado físicamente al equipo (interna o externamente) y tenga instalada ala antena (incorporada o independiente).
- Que el controlador software (o *driver*) del adaptador esté instalado en el equipo.
- Que el adaptador esté en la zona local de cobertura de otros equipos también con adaptadores inalámbricos.

Los adaptadores inalámbricos tienen las mismas funciones que vimos para los adaptadores cableados: construcción de tramas, detección de errores y acceso al medio.

7.2 Conexión física del adaptador inalámbrico.

Al igual que para los adaptadores cableados los tipos de adaptadores inalámbricos más comunes son:

1. **Integrada en la placa** Este tipo de adaptadores son los más fiables.

2. **USB.** Tiene la gran ventaja de que no necesita instalación de hardware (solo conectar).

7.3 Puntos de acceso.

El punto de acceso es un dispositivo que hace la función de concentrador (hub) inalámbrico. También permite conectar una red inalámbrica a una red cableada.

En los inicios los Puntos de Acceso eran dispositivos tipo Hub-Switch, porque disponían de:

- un puerto inalámbrico al que se conectaban las máquinas inalámbricas y que funcionaba como un hub,
- varios puertos cableados en los que funcionaba como un Switch.

Lo que solemos encontrar actualmente en el mercado son routers que tienen:

- varios puertos de switch,
- un puerto de router
- un puerto inalámbrico.

Estos routers inalámbricos reciben diferentes nombres según la compañía que los proporciona, entre ellos: router-wifi, modem-router, modem-wifi, punto acceso-wifi….

Es importante tener en cuenta que cuantos más clientes se conecten a la red cableada a través de un punto de acceso, más lento será el acceso.

Si los clientes están muy distantes del punto de acceso es posible utilizar **repetidores**.

8 Conexión a un punto de acceso

Para la asociación a un Punto de Acceso se necesitan los siguientes parámetros:

- ***SSID*:** Identificador del conjunto de servicios básicos. Se trata de un nombre que se asocia a la red Wi-Fi.
- ***Canal de transmisión***: es un parámetro que especifica la frecuencia a la que se transmitirán las señales entre emisor y receptor, y en la que previamente ambos se han puesto de acuerdo.

IEEE 802.11 establece dos métodos de autenticación: sistema abierto y clave compartida. En el primer caso, cualquier estación puede asociarse al punto de acceso sin más que emitir una solicitud que siempre será aceptada. En el segundo caso, al autenticación será correcta si el cliente sabe la clave secreta.

9 Seguridad en redes inalámbricas.

La seguridad en redes inalámbricas es más vulnerable que la de las redes cableadas ya que mientras en redes cableadas la información viaja por un cable, que es un medio **privado y exclusivo**, en las redes inalámbricas, la información viaja por el aire que es un medio **público y compartido**. La información que viaja por el cable no puede ser vista fácilmente por intrusos mientras que la información que viaja por el aire puede ser interceptada por cualquiera, lo que hace que la intrusión en la red sea más sencilla de perpetrar si no la protegemos adecuadamente.

Los principales **peligros** a los que debemos hacer frente en redes inalámbricas son:

- Cualquier otro usuario en un radio aproximado de 100 metros puede ser un "intruso potencial", bien con intención o sin ella.
- ¿Quién nos asegura que nos estamos conectando al servidor que deseamos?
- Como administradores de una red, ¿quién nos asegura que cada uno que intente conectarse a la misma es "de los nuestros"?

- Debemos asegurarnos que, una vez establecida la conexión, esta sea segura, o lo que es lo mismo, encriptada.

Existen distintas *técnicas* que nos permitirán hacer *más segura* nuestra red inalámbrica, en concreto, el uso de protocolos de seguridad inalámbrica.

- **WEP,** fue el primer protocolo en aparecer, cifraba los datos que se intercambiaban entre los usuarios y el punto de acceso. WEP dejó de ser seguro ya que pronto aparecieron multitud de aplicaciones capaces de obtener las claves WEP utilizadas y permitían el acceso de intrusos a nuestra red.
- **WPA**. Mientras IEEE trabajaba en la elaboración de un nuevo estándar de seguridad para redes inalámbricas, los distintos fabricantes acordaron un estándar intermedio de seguridad, el WPA.
- **WPA2** Publicado por IEEE en 2004 está basado en el algoritmo de encriptación AES
- **WPA3** es un nuevo protocolo de seguridad, oficial desde Junio de 2018. En abril de 2019 se descubrió un fallo en su diseño y se aconseja actualizar el firmware para solucionarlo.

Además de utilizar estos protocolos para cifrar los datos que circulan por nuestra red inalámbrica, otras medidas a considerar son las siguientes:

- Es recomendable cambiar la contraseña que trae de fábrica el punto de acceso así como el SSID.
- También resulta útil la ocultación del SSID para no divulgar el nombre de nuestra red.
- Otra medida de seguridad es el filtrado de direcciones MAC de forma que sólo se permite el acceso a la red a aquellos dispositivos cuya dirección física haya sido autorizada.
- También puede ser aconsejable desactivar el servidor DHCP que asigna direcciones de red (IP) a los equipos conectados a la red. Si limitamos el número de direcciones IP al número de ordenadores que queramos tener en la red los intrusos no podrán acceder a la misma. .
- Otra posibilidad en lugar de desactivar el servidor DHCP es restringir el rango de direcciones que asigna o modificar el tiempo que dura la asignación.

10 Configuración del Punto de Acceso Inalámbrico

La configuración de un punto de acceso inalámbrico resulta bastante sencilla debido a que no se realiza a través de comandos sino utilizando ventanas y menús con las opciones necesarias, pero dependerá del dispositivo en sí, ya que el software de configuración es distinto para cada fabricante.

Para poder configurar el punto de acceso inalámbrico es necesario:

- Conectar el dispositivo con un ordenador a través de un cable de red y configurar el Pc en la misma red IP que el punto de acceso

- Configurar el dispositivo desde un ordenador a través del navegador Web. Para ello hay que abrir el navegador y donde ponemos la pagina que deseamos visitar poner la IP del punto de acceso.

Una vez conectados debemos poner el SSID, la contraseña de acceso, el protocolo de seguridad y el resto de configuraciones deseadas.

11 .Configuración de Pcs inalámbricos

Los Pcs se configuran igual que en las redes cableadas, poniéndole una IP a la tarjeta de red, en este caso a la tarjeta inalámbrica.

Si el Punto de Acceso tiene un SSID, protocolo de seguridad o cualquier otra configuración, debemos aportar esa información a la tarjeta del Pc. Para proporcionar esa información varia de un Sistema Operativo a otro, pero generalmente en Panel de Control o en el icono de redes del menú inferior podemos configurarlo.

Si el Pc va a utilizar como router el Punto de acceso hay que indicarle como Gateway la IP que tiene el Punto de acceso. **Recuerda** que la IP del router que se utiliza es la que está en la misma red que la máquina.

12 Configuración de Pcs cableados

Los Pcs cableados que se conectan al Punto de acceso se configuran igual que en las redes cableadas.

Si el Pc va a utilizar como router el Punto de acceso hay que indicarle como Gateway la IP que tiene el Punto de acceso. **Recuerda** que la IP del router que se utiliza es la que está en la misma red que la máquina.