ANDREA RECALDE BARAIBAR
MANUEL RODRÍGUEZ ALIJA

REDES INALÁMBRICAS.

El objetivo de este trabajo es la construcción y análisis de WLANs en base a las diversas topologías existentes. Su realización se ha llevado a cabo bajo el sistema operativo Linux, pero los conceptos básicos expuestos sobre este tipo de redes son válidos para cualquier SO.

INTRODUCCIÓN. ESTÁNDAR 802.11.

Wireless Local-Area Network: Red de Área Local Inalámbrica. Es un tipo de red de área local que usa ondas de radio de alta frecuencia en lugar de cable para comunicar cada nodo.

Las principales características de las WLANs son la ***movilidad***, las máquinas pueden moverse con libertad sin perder conexión, incluso es posible saltar de una red a otra, ***facilidad de instalación,*** no es necesario tirar cable ni hacer obra, y ***flexibilidad,*** puede llegar donde el cable no puede, saltar obstáculos o atravesar paredes.

El protocolo IEEE 802.11 o WI-FI es el utilizado para especificar las normas de funcionamiento de las redes inalámbricas. En él se define el uso de los dos niveles más bajos de la arquitectura OSI (capas física y de enlace de datos). Dentro de la familia de estándares 802.11, los más importantes son los 802.11a, b, g y e. Los estándares a, b y g son estándares en los que se especifica la velocidad y la frecuencia a la que se puede transmitir. Mientras que el estándar 802.11e especifica los mecanismos a nivel de capa MAC para soportar los servicios que requieren garantías de Calidad de Servicio.

El 802.11a alcanza velocidades de hasta 54 Mbps y su frecuencia de transmisión está entorno a los 5 GHz. Los estándares b y g transmiten en torno a 2.4 GHz y se diferencian en la velocidad de transmisión, para 802.11b es de 11 Mbps y para 802.11g es de 54 Mbps.

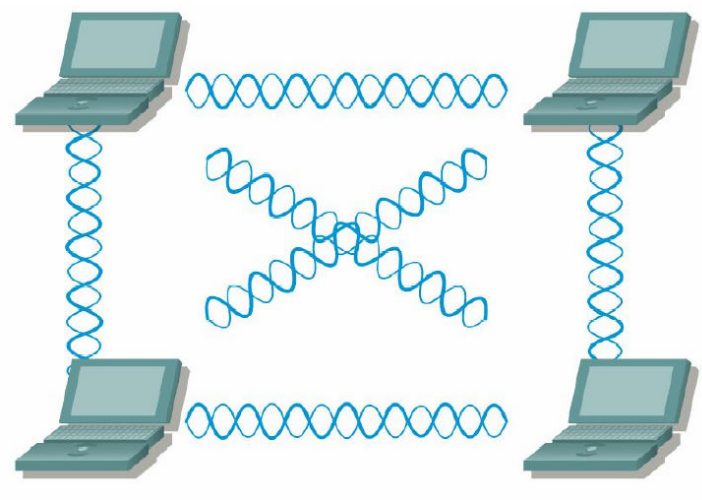
TOPOLOGÍAS.

Para la realización de las diversas topologías hemos utilizado el paquete "Wireless Tools" que sirve para la configuración de tarjetas inalámbricas de los PCs y el conocimiento del estado de la red.

Dentro de este paquetes están los comandos `iwconfig`, `iwlist`, `iwpriv`, `iwspy`, `iwgetid` y `iwevent`. Los más utilizados son `iwconfig` que, con sus respectivas opciones, permite configurar las tarjetas inalámbricas según nos sea necesario; e `iwlist` usado para mostrar información sobre puntos de acceso a nuestro alcance (la opción `scan` escanea las redes inalámbricas disponibles en ese momento) y para ver los canales, la encriptación,...

- Independent Basic Service Set (IBSS).

Popularmente se conoce como **redes Ad-Hoc** y se basan en la comunicación directa entre las estaciones inalámbricas (clientes inalámbricos) y en la no utilización de punto de acceso. Las estaciones se conectarán entre ellas arbitrariamente y de forma dinámica, de manera que todos los nodos funcionan como encaminadotes. La cobertura estará limitada por el alcance de cada estación



Para su realización bajo Linux se utiliza básicamente el comando `iwconfig` con las opciones `mode`, `channel` (o `freq`) y `essid`, para poner las tarjetas inalámbricas de todos los clientes en modo ad-hoc, transmitiendo en el mismo canal y con el mismo identificador de red:

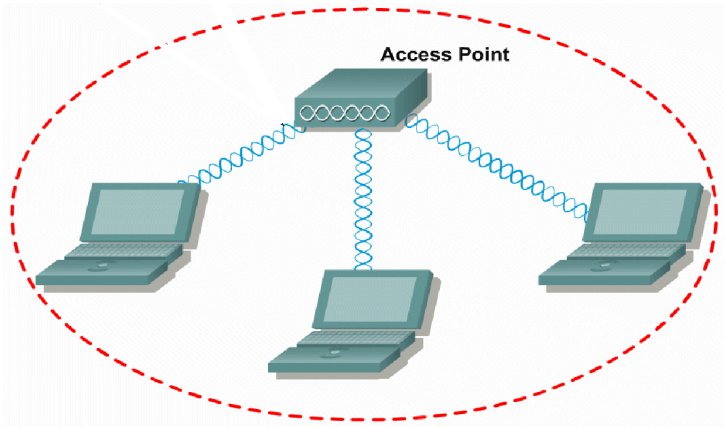
```
iwconfig <interfaz inalámbrico> mode ad-hoc
iwconfig <interfaz inalámbrico> channel <igual para todos>
iwconfig <interfaz inalámbrico> essid  <igual para todos>
```

Si todas las tarjetas utilizan DHCP no hará falta configurar las direcciones IP, pero, en caso contrario, se utilizará el comando `ifconfig`, asignando a cada tarjeta una dirección de una misma red.

- Basic Service Set o Infraestructura BSS.

Existe un nodo central llamado punto de acceso (AP) que sirve de enlace para todas las demás estaciones inalámbricas que se encuentran dentro de la zona de cobertura del AP.

A diferencia de IBSS, en BSS las estaciones no se pueden comunicar directamente entre ellas, todas las comunicaciones deberán pasar obligatoriamente por el AP que será el encargado de gestionar esa información y encaminarla.



Para la realización de esta topología en Linux hay que configurar tanto el punto de acceso, en nuestro caso un router wifi, como las tarjetas inalámbricas de los clientes.

- Configuración router.

  Esta configuración se lleva a cabo desde la página web del dispositivo y en ella configuraremos parámetros como el identificador del punto de acceso (essid), el canal de transmisión, la clave de encriptación, las direcciones de los interfaces del router, etc.

- Configuración tarjetas inalámbricas.

  Utilizamos básicamente `iwconfig` con las opciones `mode`, `channel` y `essid`. Pero a diferencia de IBSS, en BSS pondremos modo managed, canal en el que transmite el punto de acceso que es al que queremos conectarnos y el essid del punto de acceso para todas las tarjetas inalámbricas.

  Si el AP al que queremos conectarnos está encriptado tendremos que poner la clave a todas las tarjetas, con la opción `key`, para que se puedan autentificar.

```
iwconfig <interfaz> mode ad-hoc
iwconfig <interfaz> channel <número canal>
iwconfig <interfaz> essid  <el del AP>
iwconfig <interfaz> key <el del AP>
```

  Se puede utilizar el comando `iwlist scan` para escanear los puntos de acceso disponibles:

```
iwlist <interfaz> scan
```

  También habrá que configurar las direcciones IP de los PC´s para que estén en la misma red del punto de acceso al que se quiere conectar.

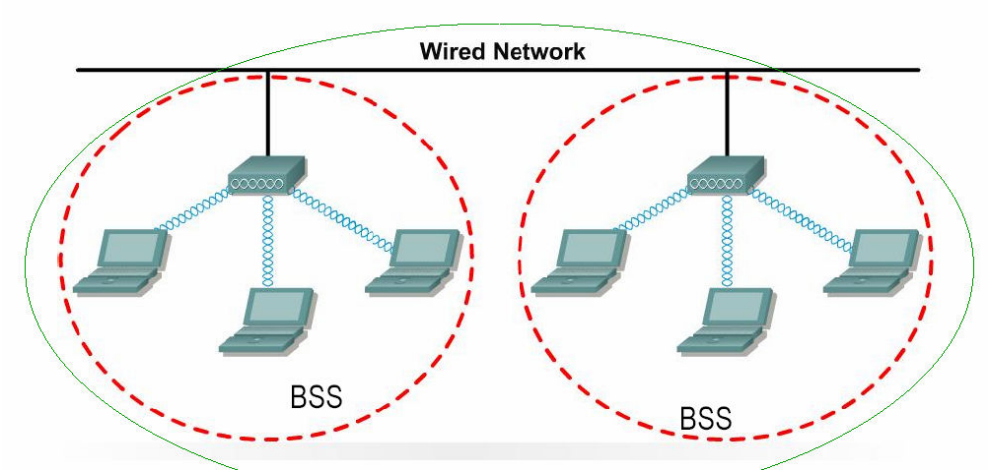
Existe la posibilidad de que un PC realice la función de punto de acceso para ello deberemos ponerlo en modo master. Sin embargo, no todas las tarjetas inalámbricas aceptan este modo de operación.

```
iwconfig <interfaz> mode master
```

- Extended Service Set o Infraestructura (ESS).

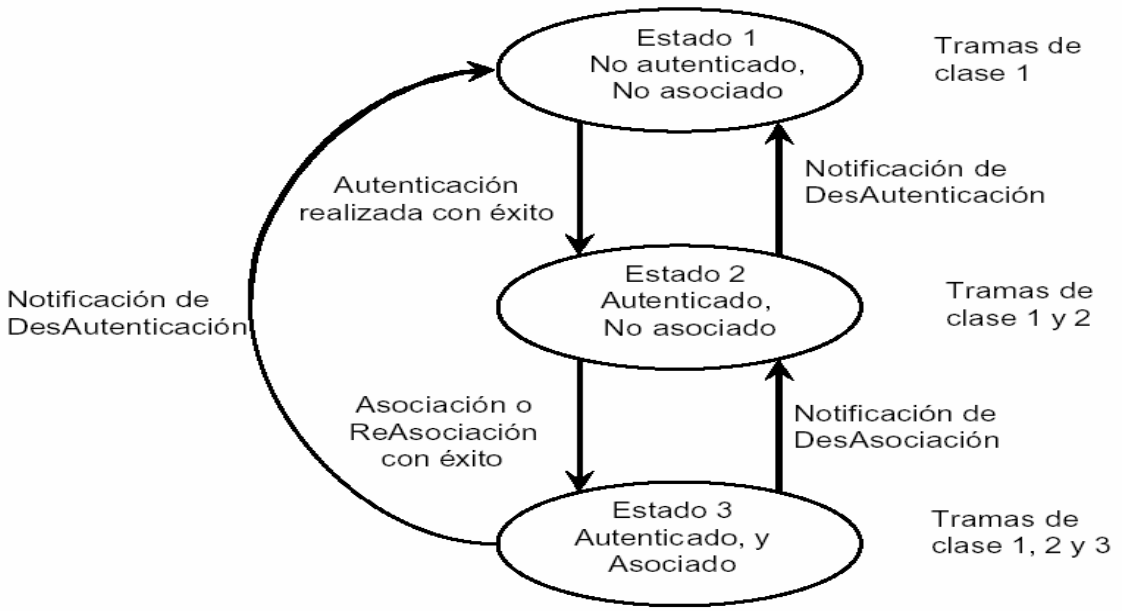
Se trata de un conjunto de BSS conectados mediante un sistema de distribución. Los puntos de acceso se comunican entre sí para permitir que las estaciones puedan pasar de un BSS a otro sin perder la comunicación, servicio denominado ***roaming***.

El sistema de distribución puede ser cableado o inalámbrico. Para el caso del DS inalámbrico (WDS) será necesario que el punto de acceso o dispositivo que realice la función de AP soporte este tipo de funcionamiento. En caso contrario, existe la posibilidad de instalar en el dispositivo inalámbrico un software que soporte WDS.



ASOCIACIÓN Y AUTENTIFICACIÓN. ETHEREAL Y AIRCRACK.

Junto con la seguridad, la asociación y la autentificación son temas fundamentales para el entendimiento de las redes inalámbricas. Cuando un cliente quiere conectarse a una WLAN se requieren unos ciertos pasos que el cliente debe realizar:



En la transición por los diferentes estados, ambas partes (cliente y AP) intercambian mensajes llamados "management frames". El proceso que realiza un cliente wireless para encontrar y asociarse con un AP es el siguiente:

Los AP transmiten *'beacon frames'* cada cierto intervalo de tiempo fijo. Para asociarse con un AP y unirse a una red en modo infraestructura, un cliente escucha en busca de *'beacon frames'* para identificar los puntos de acceso. El cliente también puede enviar una trama *'prove request'* que contenga un ESSID determinado para ver si le responde un AP que tenga el mismo ESSID.

Después de identificar al AP, el cliente y el AP realizan autenticación mutua intercambiando varios *management frames* como parte del proceso. Hay varios mecanismos de autenticación posibles, pero este tema forma parte del concepto de seguridad en redes inalámbricas que no entran dentro del contenido de esta asignatura, se podrán ver en la asignatura GSRO.

Después de una autenticación realizada con éxito, el cliente pasa a estar en el segundo estado (autenticado y no asociado). Para llegar al tercer estado (autenticado y asociado) el cliente debe mandar una trama *'association request'* y el AP debe contestar con una trama *'association response'*, entonces el cliente se convierte en un host más de la red wireless y ya está listo para enviar y recibir datos de la red.

En este punto sería útil estudiar los paquetes del estándar 802.11 para ver esos procesos de asociación y autentificación, así como el análisis de la cabecera 802.11. Para ello se pueden utilizar diversas herramientas como son Ethereal y Aircrack.

- **Ethereal** es un analizador de protocolos de redes, para máquinas Unix y Windows.
  - Su licencia es libre.
  - Soporta más de 300 protocolos.
  - Permite añadir filtros para ver lo que nos interese en cada momento.

- **Aircrack** es una colección de herramientas para la auditoría de redes inalámbricas.
  - Orientada más hacia el campo de la seguridad (asignatura Gestión y Seguridad en Redes de Ordenadores GSRO).
  - Contiene el comando airodump, parecido a tcpdump, que permite capturar tráfico 802.11.
  - Necesidad de parchear los drivers del dispositivo (tener en cuenta que este trabajo se ha realizado sobre Linux) para trabajar en modo monitor.

CURIOSIDADES: WARCHALKING.

Os preguntareis que quieren decir estas imágenes, fijaos en los símbolos…

Seguro que alguna que otra vez, caminando por la ciudad, has tenido la necesidad de conectarte a Internet. Pues si tienes un dispositivo con interfaz inalámbrico y encuentras algún símbolo como los de la imagen estás de suerte.

Londres **Bilbao**

Warchalking es un lenguaje de símbolos, normalmente escritos con tiza en las paredes, que informa a los posibles interesados de la existencia de una red inalámbrica en ese punto.

SÍMBOLO	ssid bandwidth	ssid	ssid access contact W bandwidth
SIGNIFICADO	Nodo abierto	Nodo cerrado	Nodo con WEP

El origen de esta simbología data de los años 70. Durante la gran depresión que tuvo lugar en EEUU, se crearon una serie de símbolos que escritos cerca de determinados lugares, daban información de la proximidad de sitios donde se podía conseguir algo de comida. Los tiempos han cambiado, y ahora en Londres han retomado el escribir esos símbolos por la calle para avisar de la existencia de una conexión inalámbrica a Internet que sea decente.

La sencillez del lenguaje ha sido uno de los factores que han hecho posible su proliferación por las grandes ciudades. Además otras características como la no perdurabilidad de las marcas durante grandes periodos de tiempo hacen que sea muy dinámico y se vaya adaptando constantemente a las características cambiantes de las redes sobre cuya existencia informa.

A la par de este lenguaje surgen movimientos como Warwalking, Wardriving, WarSkating y WarCycling. Todos son métodos para la búsqueda de redes inalámbricas, diferenciándose en el medio de transporte que utilicemos para desplazarnos (andando, conduciendo, en patines o en bici). Para ello se utilizan programas snnifadores de tráfico como pueden ser NetStumbler (Windows), KisMac (Macintosh) o Kismet (Linux).