**1.1.- Conceptos básicos.**

Antes de conocer cuáles son los riesgos y cómo hacer frente a los problemas de las redes wifi, es necesario conocer algunos conceptos:

**Cobertura, canales y SSID**

Es importante saber que, en este tipo de redes, existe una limitación con el radio de cobertura. En interiores suele ser de unos 20 metros y esta distancia es mayor al aire libre que puede llegar a ser de cientos de metro si las condiciones lo permiten.

Otro elemento importante, es la potencia de la señal que en el caso de las redes wifi se va a medir en mili vatios. A mayor potencia, también mayor alcance. El tipo de receptor o antena que tengamos también influirá en la cobertura, incluso podemos usar antenas alimentadas eléctricamente para ganar varios kilómetros de cobertura.

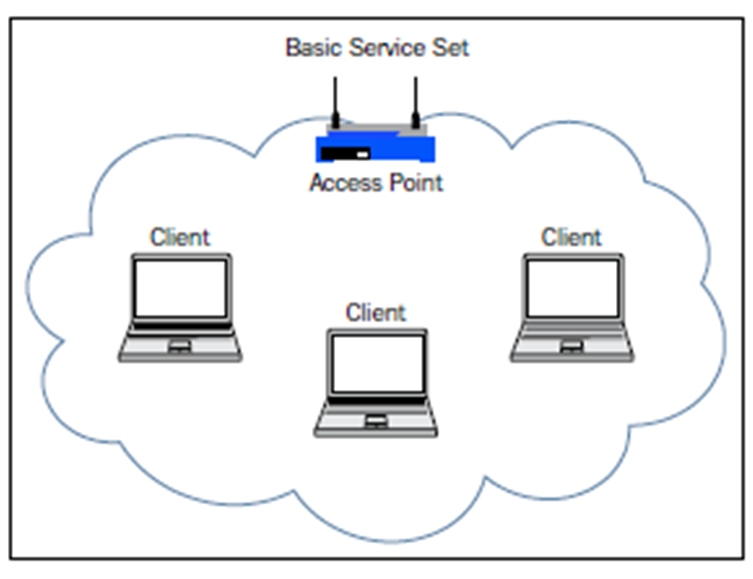
En interiores, si se usa la banda de 2,4 Ghz la señal wifi se extenderá más pero será menos veloz, y si usamos la de 5 Ghz, tendrá menos alcance pero la conexión será más rápida. En relación con esto, los puntos de acceso pueden ser configurados para que la señal wifi que se transmite se lleve a cabo a través de diferentes canales que pueden ir del 1 al 17 en función de las características del dispositivo. En realidad esta función es para mejorar la transmisión evitando contaminación por otros dispositivos o señales en las bandas que se estén usando.

El SSID (Service Set Identifier) es el nombre de la red wifi. Los puntos de acceso (routers inalámbricos) “anuncian” su red continuamente, permitiendo a los clientes listar las redes disponibles. Es posible encontrar redes “ocultas” que no anuncian de forma activa su SSID, pero hay que destacar que no es una medida de protección aunque antes así se pensara.

**BSS**

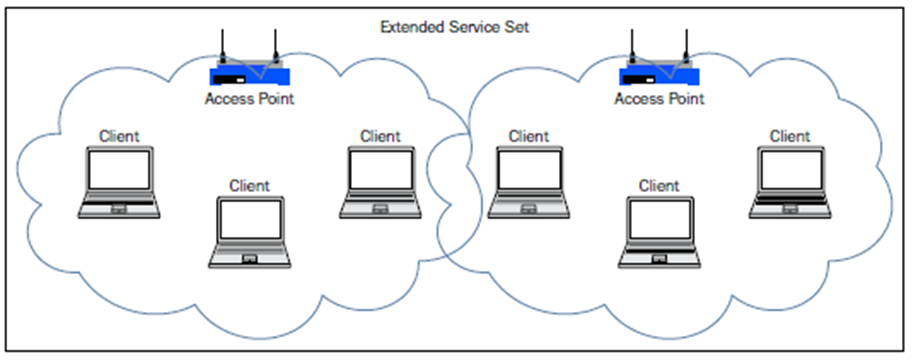
O Basic Service Set, se trata de la configuración normal/habitual. Un punto de acceso al que se conectan varios clientes. De cara a los que veremos posteriormente, en este tipo de configuraciones hay que tener en cuenta que están formadas por:

* El SSID: visto en el punto previo.
* El BSSID: O Basic SSID que es la [MAC](https://es.wikipedia.org/wiki/Direcci%C3%B3n_MAC), o dirección física del punto de acceso (AP).



**ESS**

O Extended Service Set:  se trata de la configuración que contempla más de un punto de acceso para crear la conexión. En este tipo de configuraciones hay que tener en cuenta que existirá el ESSID (Extended SSID), similar al SSID pero con la diferencia de que puede haber varios puntos de acceso con diferentes SSID que forman parte del de este tipo de infraestructura. Este tipo de redes wifi son las que se despliegan en ciudades, universidades, aeropuertos, y en menor medida en empresas con gran extensión.



**Modos**

* **Infraestructura**: se trata del modo más común de implementación. Este tipo de red es generada por los propios router wifi o puntos de acceso. Es la que podemos encontrar en los hogares, empresas y ciudades.
* **Ad-hoc**: también se conoce como modo "peer-to-peer". Las redes ad-hoc no requieren un punto de acceso centralizado. En su lugar, los dispositivos de la red inalámbrica se conectan directamente entre sí. Hay dispositivos que nos son compatibles con este modo pero casi el 100% son compatibles con el modo infraestructura.

**Frames**

1. **Management [frames](http://www.wi-fiplanet.com/tutorials/article.php/1447501/Understanding-80211-Frame-Types.htm" \o "Acceder a la web wi-fiplanet.com para recabar información sobre management frames. Se abre en una nueva ventana" \t "_blank)**: conocidos como paquetes de gestión estos son responsables de mantener la comunicación que está presente entre el punto de acceso y el cliente asociado a él. Alguno de sus subtipos:
   * Beacon frame
   * ATIM frame
   * Probe response
   * Probe request
   * Disassociation frame
   * Association Request frame
   * Association Response frame
2. **Control frames**: paquetes de control, estos son responsables de un intercambio adecuado de  información (Data) entre el punto de acceso y los clientes asociados. Tiene varios subtipos:
   * CTS: Clear to Send
   * RTS: Request to Send
   * ACK: Acknowledgement frame
3. **Data frames**: son paquetes con información. Son los más importantes cuando uno está tratando de descifrar la  contraseña encriptada por algún tipo de cifrado en particular  WEP, ya que dichos paquetes contienen toda la información que se envía a través de nuestra red wifi.

A la hora de llevar a cabo tanto una auditoría como un ataque a un red de estas características, hay que centrarse en los beacon frames, los probe request y los probe response. A través del análisis de estos paquetes se podrá obtener información como:

* SSID
* Tipo de cifrado
* Canal
* MAC
* Información del fabricante