Universitat d'Alacant
Universidad de Alicante

BIBLIOTECA UNIVERSITARIA

Internet y la web - Conexiones

Material formativo

BUA
Biblioteca de la Universitat d' Alacant
Biblioteca de la Universidad de Alicante

CI2
COMPETENCIAS INFORMÁTICAS E INFORMACIONALES

INTERNET Y LA WEB - CONEXIONES

BREVE INTRODUCCIÓN A LAS REDES (cableadas e inalámbricas)

Las conexiones domésticas a internet han sufrido una drástica mejora desde los lejanos tiempos de los módems de marcación telefónica a 56k, allá al principio de los 2000, hasta la fibra óptica de la actualidad, con velocidades medias del orden de 300 Mbps. La evolución técnica ha sido enorme, pero el problema básico sigue siendo el mismo: cómo conseguir la máxima velocidad en todos los rincones de nuestro hogar (o centro educativo).

Si a finales del siglo pasado nos conectábamos a internet típicamente mediante un cable de red ethernet con un ordenador de sobremesa caro y difícil de mover (torre más monitor de TRC, o Tubo de Rayos Catódicos), en la actualidad nos conectamos con toda una miriada de dispositivos, la mayoría de ellos portables (es decir, de uso personal) y portátiles, con lo que se hace imprescindible contar tanto con una conexión a internet de banda ancha, como con una red inalámbrica correctamente diseñada y configurada para poder aprovechar todo el ancho de banda de nuestro proveedor de internet.

El término red informática hace referencia a un conjunto de equipos y dispositivos informáticos conectados entre sí, cuyo objeto es transmitir datos para compartir recursos e información.

Para ello se requiere la creación de una infraestructura física que permita la comunicación, así como los desarrollos informáticos necesarios para asegurar la conexión y la seguridad de la misma, lo que se conoce con el término de protocolos, que son las normas que regulan la prioridad de acceso de unos equipos sobre otros, la autorización de uso de la red, el lenguaje de comunicación entre los diferentes ordenadores que conforman la red, etc.

El objetivo fundamental de una red informática es compartir recursos (archivos, aplicaciones o hardware, una conexión a Internet, etc.). Otros objetivos son facilitar la comunicación entre personas (correo electrónico, debates en vivo, etc.) y la comunicación entre procesos (por ejemplo, entre equipos industriales), garantizar el acceso único y universal a la información (bases de datos en red) e incluso poder jugar videojuegos de tipo multijugador

Elementos básicos de las redes informáticas

Los componentes fundamentales de una red son:

- **el servidor (host)**
- **los dispositivos cliente**: todos aquellos que hacen uso de la red (ordenadores, impresoras, consolas, smartphones, smartTVs, tablets, videocámaras, etc.)
- **los dispositivos de re**d: el hardware, los dispositivos necesarios para interconectar al host o hots con los dispositivos clientes
- **el medio de comunicación o transporte de la señal**: el cable, en caso de redes cableadas, o las ondas electromagnéticas, en el caso de redes inalámbricas

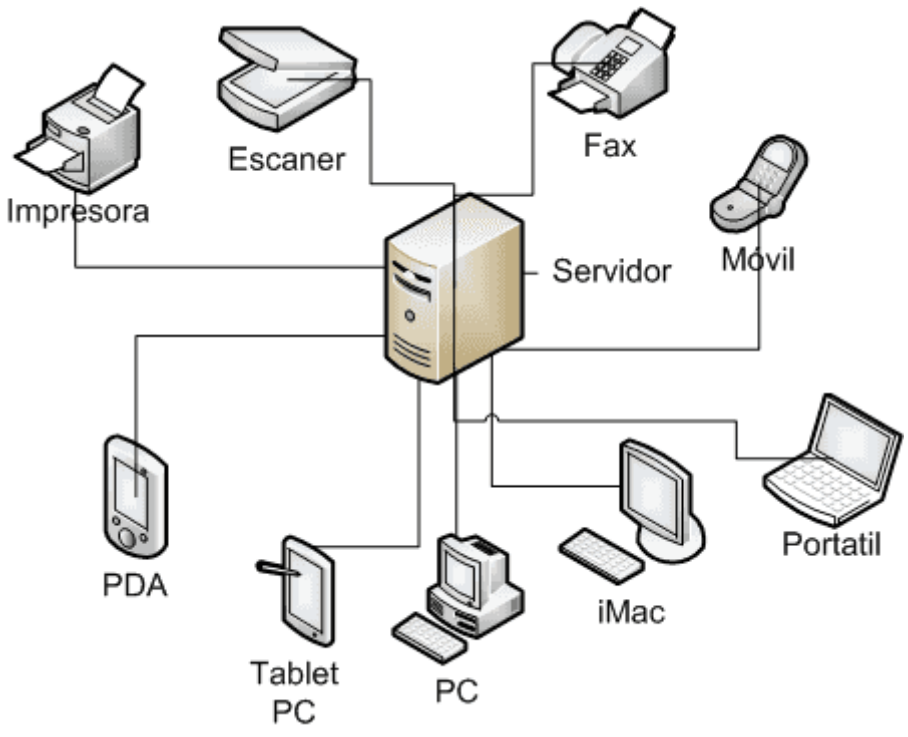
Los principales **dispositivos de red** necesarios para configurar una red serían

- modem
- router
- switch o concentrador

El host o servidor

Un **host o servidor** es una máquina que ejecuta un software capaz de atender las peticiones de varias máquinas (clientes) y devolverles la respuesta correspondiente. Normalmente se trata de consultas o peticiones de datos de todo tipo (archivos de texto, video, audio, imágenes, correo electrónico, aplicaciones de gestión, programas, consultas a base de datos, etc).

El host debe tener una dirección IP y, obviamente, estar interconectado con uno o más equipos.



Hay varios tipos de servidores, que te mencionamos a título informativo (aunque su conocimiento más extenso escapa a los objetivos de esta unidad): servidor de correo, servidor proxy, servidor web, servidor de base de datos, servidores de imágenes, servidor de impresiones...

Modem

El modem es un dispositivo que convierte (modula) la señal analógica procedente de nuestro proveedor de internet (ISP, Internet Service Provider, o Proveedor de Servicios de Internet) para que pueda ser usada por nuestros equipos informáticos, y viceversa (de ahí viene su nombre: modular-demodular).

La señal del ISP puede transmitirse a través del cable telefónico, coaxial o fibra óptica, y aunque puede ser analógica, en la banda ancha moderna (ADSL, fibra óptica) es digital.

Router

El router es un dispositivo que permite la interconexión de otros dispositivos electrónicos (ordenadores, tablets, impresoras, consolas, etc.) en red.

Concentradores y conmutadores

Los hubs (concentradores) y los switchers (conmutadores) son dispositivos que también se encargan de interconectar dispositivos digitales en red, con distinto grado de complejidad: los switchers proporcionan mayor rendimiento que los hubs cuando necesitamos conectar cuatro o más dispositivos. Esto es lo que, a nuestro nivel, necesitamos saber, aunque detrás hay una mayor complejidad técnica

Los switchers se utilizan para conectar varios segmentos de red, mientras que el hub o concentrador conecta varios dispositivos Ethernet juntos, haciéndolos actuar como un único segmento de red.

TOPOLOGÍA DE LAS REDES CABLEADAS

La topología de una red es la forma en la que están conectados entre sí los elementos de la red, es decir, la forma en que está diseñada la red, tanto en el plano físico como en el plano lógico.

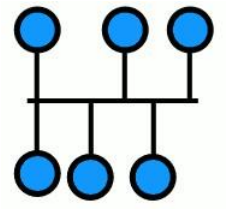
Hablamos de **topología física** cuando nos referimos a la configuración espacial de la red, es decir, a la configuración del cableado entre los distintos dispositivos y elementos de control, conmutación y enrutamiento.

Hablamos de **topología lógica** cuando nos referimos a la forma en que los datos viajan por las líneas de comunicación.

Como podéis imaginar, hay muchos tipos de topologías, pero los cinco más importantes serían:

- Topología en Bus
- Topología en Estrella
- Topología en Anillo
- Topología en Malla
- Topología en Árbol

Topología en bus



Es la forma más sencilla en que podemos organizar una red: todos lo equipos están conectados a una única línea de transmisión denominada bus, backbone o troncal. Todos los dispositivos comparten, pues, el mismo canal para comunicarse entre sí. El bus es pasivo, no se produce generación de señales en cada nodo.

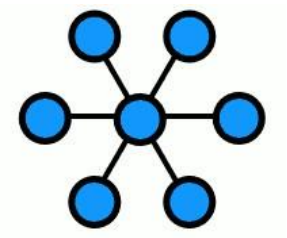
Los extremos del cable han de terminarse con una resistencia de acople denominada terminador, que indica que no existen más ordenadores o dispositivos en el extremo y cierra el bus gracias al acople de impedancias.

La principal ventaja de esta tipología es su facilidad de implementación

Esta topología tiene también importantes desventajas:

- El límite de equipos está determinado por la calidad de la señal.
- Puede producirse degradación de la señal.
- Complejidad de reconfiguración y aislamiento de fallos.
- Es muy vulnerable: una conexión defectuosa afecta a toda la red.
- Un problema en el canal usualmente degrada toda la red.
- El rendimiento disminuye a medida que la red crece.

Topología de estrella



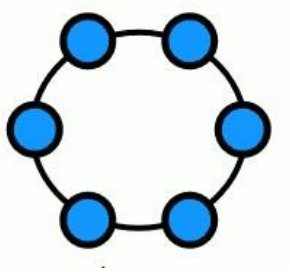
Todos los dispositivos de la red están conectados a un nodo central (router, hub o switcher), de tal forma que todas las comunicaciones han de realizarse a través del nodo.

Se utiliza mucho para las redes locales (LAN, o Local Area Network).

Ventajas:

- Pueden agregarse nuevos equipos o dispositivos fácilmente
- Rápida reconfiguración ante cualquier problema
- Los fallos se detectan y aíslan con facilidad
- Desventajas:
- Si falla el nodo central (router, hub o switcher), toda la red queda sin conexión
- Es costosa, ya que requiere más cableado que las topologías en bus o en anillo

Topología en anillo



En la red en anillo cada nodo o equipo tiene una única conexión de entrada y una única conexión de salida. Cada equipo tiene un receptor y un transmisor que hace la función de traductor, pasando la señal a la siguiente estación.

Con la red en anillo, la comunicación se da por el paso de un token o testigo, para así evitar posibles pérdidas de información debidas a colisiones. En realidad, el token es una señal que se pasa entre los distintos nodos para autorizarlos a comunicarse.

Podemos imaginar de manera muy gráfica cómo funciona la comunicación en una red en anillo si pensamos en un mensajero que pasa por los distintos equipos entregando y recogiendo paquetes de información.

Debido a las limitaciones de esta topología, se suele implementar como un anillo doble (token ring), lo que permite enviar datos simultáneamente en ambas direcciones (token passing)

La configuración en doble anillo o token ring aumenta la tolerancia a fallos

Ventajas:

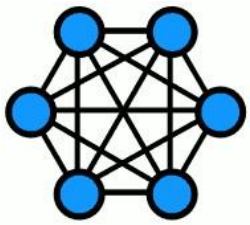
- Es una arquitectura muy sólida
- El rendimiento se mantiene constante independientemente del número de usuarios

Desventajas

- Los datos han de pasar por todos los equipos intermedios entre dos nodos
- El canal se degrada a medida que va creciendo el número de nodos o equipos
- Es complicado diagnosticar y reparar los problemas
- La velocidad de transmisión de datos es menor que en otras topologías porque la información debe pasar por todos los equipos intermedios.

Esta topología la desarrolló IBM en los 70 y ha caído en desuso por la popularización de Ethernet

Topología en malla



En esta topología, todos los nodos están conectados entre sí, de tal forma que la información puede viajar de un nodo o dispositivo a otro por distintos caminos. Si la red de malla está totalmente conectada, es muy difícil que puedan producirse interrupciones en las comunicaciones, ya que cada dispositivo tiene conexiones con todos los demás dispositivos o hosts.

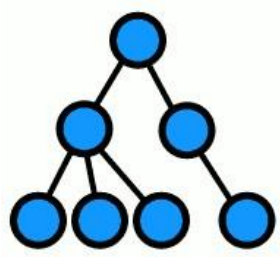
A diferencia de otras topologías, en la de malla no se requiere de un nodo central, lo que reduce mucho el riesgo de fallos, puesto que la caída de un nodo no implica, ni mucho menos, la caída de toda la red.

Además, si implementamos un enrutamiento dinámico, la red podría reconfigurarse automáticamente ante la caída de uno o más nodos.

Es, por tanto, una de las topologías más robustas, ideal para aplicaciones críticas y redundantes a fallos: por ejemplo, es una topología ideal para conectar una red de defensa nacional, en la que no pueden tolerarse fallos.

Como principal desventaja apuntaríamos el elevado coste de su implementación.

Topología en árbol



Podemos ver esta topología como una combinación de varias topologías en estrella, con un nodo de enlace troncal (generalmente ocupado por un switch o hub) desde el que se ramifican los demás nodos.

Junto a la topología de estrella, es una de las más utilizadas, principalmente en edificios con varias alas o varias plantas.

Ventajas:

- Tiene cableado punto a punto para segmentos individuales
- Fácil resolución de problemas
- Está soportada por multitud de vendedores de software y hardware

Desventajas

- Si cae el segmento troncal, cae toda la red en conjunto
- Configuración compleja
- Si cae un nodo, todos los equipos conectados a él se desconectarán a su vez
- Requiere mucho cableado

ESTÁNDARES WI-FI

Los estándares wifi especifican los diversos protocolos de frecuencia, codificación, multiplexado, velocidad de transmisión y otros parámetros necesarios para que la conexión inalámbrica alcance los óptimos adecuados para la especificación de que se trate

El nombre completo del estandar es IEEE 802.11, (IEEE por Institute of Electrical and Electronics Engineers, o Instituto de Ingenieros Eléctricos y Electrónicos).

Dentro de la familia del 802, tendríamos:

- IEEE 802.1, para conexiones LAN.
- IEEE 802.3, para conexiones Ethernet por LAN.
- IEEE 802.11, para conexiones inalámbricas por Wi-Fi.
- IEEE 802.15, para conexiones Bluetooth.

A continuación, puedes ver los datos técnicos más importantes de cada uno de los estándares, con su año de implementación.

802.11

Velocidad (teórica)- 2 Mbit/s

Velocidad (práctica) - 1 Mbit/s

Frecuencia - 2,4 Ghz

Ancho de banda - 22 MHz

Alcance - 330 metros

Año de implementación – 1997

802.11a

Velocidad (teórica)- 54 Mbit/s

Velocidad (práctica) - 22 Mbit/s

Frecuencia - 5,4 Ghz

Ancho de banda - 20 MHz

Alcance - 390 metros

Año de implementación - 1999

802.11b

Velocidad (teórica)- 11 Mbit/s

Velocidad (práctica) - 6 Mbit/s

Frecuencia - 2,4 Ghz

Ancho de banda - 22 MHz

Alcance - 460 metros

Año de implementación - 1999

802.11g

Velocidad (teórica)- 54 Mbit/s

Velocidad (práctica) - 22 Mbit/s

Frecuencia - 2,4 Ghz

Ancho de banda - 20 MHz

Alcance - 460 metros

Año de implementación - 2003

802.11n

Velocidad (teórica)- 600 Mbit/s

Velocidad (práctica) - 100 Mbit/s

Frecuencia - 2,4 Ghz y 5,4 Ghz

Ancho de banda - 20/40 MHz

Alcance - 820 metros

Año de implementación - 2009

Disponible en la mayoría de los dispositivos modernos.

802.11ac

Velocidad (teórica)- 6.93 Gbps

Velocidad (práctica) - 100 Mbit/s

Frecuencia - 5,4 Ghz

Ancho de banda - 80 o hasta 160 MHz

Año de implementación - 2013

Nuevo estándar sin interferencia pero con menos alcance, aunque hay tecnologías que lo amplían.

802.11ad

Velocidad (teórica)- 7.13 Gbit/s

Velocidad (práctica) - Hasta 6 Gbit/s

Frecuencia - 60 Ghz

Ancho de banda - 2 MHz

Alcance - 300 metros

Año de implementación - 2012

802.11ah

Frecuencia - 0.9 Ghz

Ancho de banda - 2 MHz

Alcance - 1000 metros

Año de implementación - 2016

Conocida como Wi-Fi HaLow

Los protocolos más usados a día de hoy en la mayoría de los dispositivos son el b, g y n.

El 802.11a y el 802.11b se desarrollaron al mismo tiempo: el a utilizaba la frecuencia de 5GHz frente a los 2.4GHz del b.

Pese a la mayor velocidad de transferencia (hasta 54 Mbits/seg) del 802.11a, es más popular el 802.11b porque al utilizar una frecuencia menor tiene mayor alcance (hasta cuatro veces más).

Sin embargo, el 802.11b presentaba el problema de las interferencias con aparatos inalámbricos y electrónicos, como los microondas.

La **especificación 802.11g** (del 2003) combinaba lo mejor de sus dos predecesores: la velocidad de hasta 54 Mbit/s del 802.11a, y el alcance del 802.11b gracias a utilizar los 2.4 Ghz. Además, tenía la ventaja de ser retrocompatible con el 802.11b, lo cual aseguraba que los nuevos dispositivos que utilizaran el 802.11g pudieran conectarse a routers y puntos de acceso que emitieran en 802.11b.

La introducción del 802.11n en 2009 fue el cambio más importante en la historia del estándar. Supuso un punto de inflexional introducir las redes MIMO (Multiple-input Multiple-output, Múltiple entrada múltiple salida).

Estas redes MIMO hacen uso de varias antenas en un mismo router para enviar y recibir datos de manera simultánea, agilizando así la velocidad de la conexión. Además, se consiguió mejorar la cobertura, llegando a 120 metros en interior y 300 metros en exteriores.

El estándar 802.11ac, características y ventajas

El estándar 802.11ac se está implementando desde el comienzo del 2014; los componentes que lo emplean consumen menos energía, por lo que es ideal para dispositivos portables, además ahora es posible transmitir datos idénticos a usuarios diferentes.

Usando la banda de 5 GHz el radio de alcance es menor, pero en la práctica se pueden alcanzar distancias mayores usando la tecnología "Beamforming" que focaliza la señal de radio en determinadas zonas

La velocidad del 802.11a se debe a dos factores:

1- La posibilidad de usar canales de radio más anchos: En lugar de usar 40 MHz de ancho de canal, AC puede funcionar con 80 o hasta 160 MHz.

Otra posibilidad es la de usar la característica "Channel Bonding", es decir poder combinar dos canales independientes.

2- Antenas múltiples: Los routers actuales transfieren al mismo tiempo hasta seis flujos de datos (spatial streams) usando tres antenas. Con AC se pueden utilizar hasta cuatro antenas.

El estándar 802.11ah o Wi-Fi HaLow, caracteristicas y ventajas

IEEE 802.11ah es un nuevo protocolo de redes inalámbricas que comienza a implementarse en el 2016. Surge a causa de los constantes requerimientos de la tecnología, la información y el mercado.

Se diferencia de los anteriores por:

- Usar frecuencias inferiores a 1 GHz
- Permitir aumentar el rango de alcance de estas redes, hasta alrededor de 1000 metros, con todas las posibilidades que ello conlleva.
- Tener un menor consumo de energía.

Wi-Fi alliance anunció que 802.11ah se conocería con el nombre Wi-Fi HaLow, y está desarrollado expresamente para el IoT (Internet of Things, o Internet de las cosas).

Será el gran competidor de Bluetooth en los próximos años, ya que está pensado para pulseras de monitorización, sensores domésticos, cámaras de seguridad, etc.; campos hasta ahora copados por el Bluetooth, respecto al que según la Wi-Fi Alliance ofrece un rendimiento energético similar.

CONFIGURAR LA CONEXIÓN A UNA RED WI-FI

Elementos básicos de una red Wi-Fi

Los dispositivos necesarios para construir una pequeña red Wi-Fi doméstica o educativa serían los siguientes:

- Módem
- Router Wi-Fi
- Extensor de red (wifi o por línea eléctrica) / Punto de acceso
- Switch de red

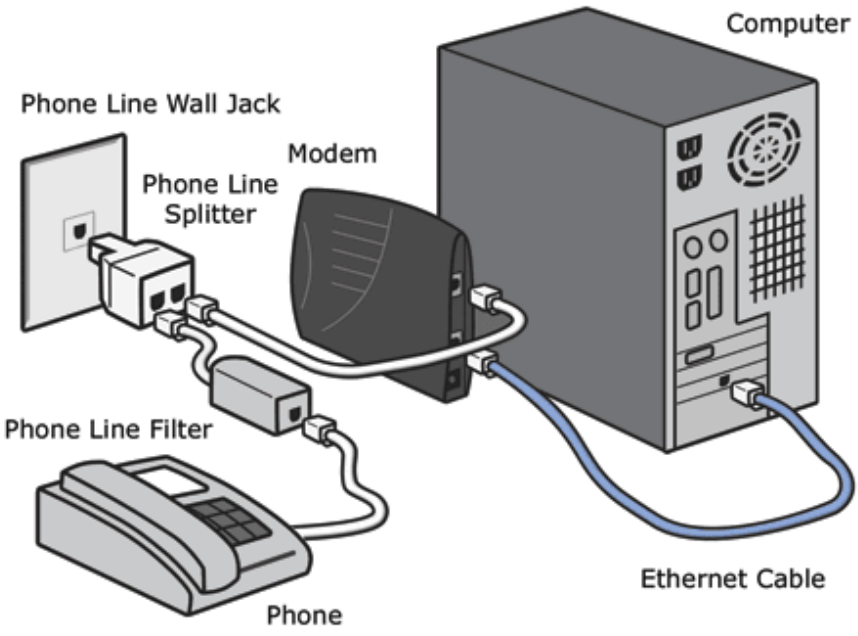
El elemento central y a priori más importante de toda nuestra red doméstica es el Router WiFi o enrutador, que es el que nos va a proporcionar conexión a todos nuestros dispositivos. El enrutador, junto con el módem, son los dos elementos indispensables para poder montar nuestra red wifi doméstica. Los otros dispositivos serán o no necesarios en función de las características y particularidades de nuestra vivienda u oficina

Vamos a ver a continuación una explicación más detallada de estos elementos.

Módem

El módem se encarga, como su propio nombre deja entrever, de modular y demodular la señal de internet, es decir, que interpreta y transforma la señal que le llega a través del cable telefónico RJ11 (ADSL), cable coaxial (el cableado coaxial que también lleva la señal de televisión, como por ejemplo el que realizó originalmente la compañía ONO) o fibra óptica, y proporciona una salida mediante un cable estándar RJ45, que es el comúnmente utilizado para realizar el cableado de red. Este cable ya podría conectarse directamente a un PC y tendríamos conexión a internet.

Si nos retrotraemos a los albores de Internet, las conexiones se efectuaban mediante módems de marcación telefónica: el modem emitía una serie de pitidos que permitían traducir la señal digital a analógica para poder conectarnos a internet a través del teléfono, con muchas limitaciones: si alguien llamaba, se cortaba la conexión porque se compartía línea con el teléfono doméstico. La velocidad de la conexión era desesperadamente lenta para los estándares actuales: 14.4k, 28.8 k o unos celéricos 56k para los más afortunados. Había que poner, además, un filtro en la roseta de conexión telefónica de la pared para discriminar la señal del teléfono y la del modem (esto también se sigue usando para la conexión ADSL)



No era necesario, en la mayor parte de los casos, un router porque sólo se conectaba a internet un ordenador de sobremesa.

El aspecto de los módems no ha cambiado mucho desde entonces:

Después llegó la RDSI (Red Digital de Servicios Integrados); la línea dejó de ser analógica y pasamos a las líneas digitales conmutadas con capacidad multimedia. Fue el preludio de la llegada del ADSL (Asymmetric Digital Subscriber Line, o Línea de abonado digital asimétrica) y de la deseada banda ancha: con las tecnologías ADSL2 y ADSL2+ hablamos de velocidades de 12 y 24 Mbit/seg. Usa la infraestructura existente de la red telefónica básica, por lo cual los costes son menores y es una buena solución para una conexión a internet barata, o para lugares en los que no se haya implantado el cable o la fibra óptica, como zonas rurales o núcleos de población aislados. Como ya comentamos antes, sigue siendo necesario el uso de un filtro discriminador para la señal telefónica y la digital conmutada.

El filtro tiene este aspecto:

En cuanto a los módems ADSL, se distinguen muy poco de los anteriores. Seguimos viendo las conexiones RJ11 (línea telefónica) y RJ45 (cable de datos)

Paralelamente al ADSL, la otra puerta de acceso a la banda ancha de internet es el internet por cable, que usa el ancho de banda que no utiliza la televisión por cable en una infraestructura CATV (Community Antenna Television). En España, algunas de las principales empresas de cable son ONO, R, Telecable o Euskaltel.

Los cables modem son módems muy similares a los que hemos visto, pero con entrada coaxial (típicamente cable RG-6 con conector F) y salida RJ45 (cable Ethernet).

Por último, tras el despliegue de fibra óptica realizado por las operadoras, podemos acceder a todo un mundo de servicios multimedia y con velocidades máximas que van de 300 a 500 Mb/seg. En este caso, el módem cambia su denominación aunque sus funciones siguen siendo las mismas: transformar la señal de fibra óptica para que podamos usarla en nuestra red particular.

El dispositivo en cuestión se denomina ONT (Optical Network Terminal, o Terminal de Red Óptica); se utiliza para terminar la línea de fibra óptica, y como ésta no proporciona corriente para los terminales locales, debe proporcionar corriente a los teléfonos del cliente y, además, demultiplexar la señal óptica en sus componentes utilizables, a saber:

- Conexión a internet
- Televisión HD/4K por IP
- Teléfono sobre IP con simulación de la línea clásica POTS (Plain Old Telephone Service, o servicio telefónico ordinario). Es decir, la telefonía básica.

Éste es el aspecto que ofrece uno de los ONT que viene montando Movistar:

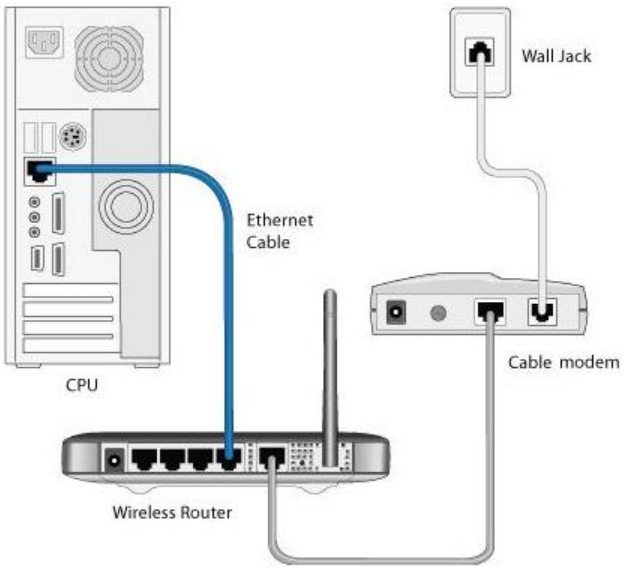
En la parte inferior podemos observar la terminación de la fibra óptica:

Hemos hablado anteriormente que los módems suelen proporcionar sólo una salida de señal de internet hacia el router. Vemos que, en el caso del ONT hay 4 salidas ETH (Ethernet) y 2 salidas TELF (teléfono): la operadora sólo deja activa 1 salida Ethernet y una salida de teléfono, así que a todos los efectos estamos en la misma situación que en los módems tradicionales.

Router

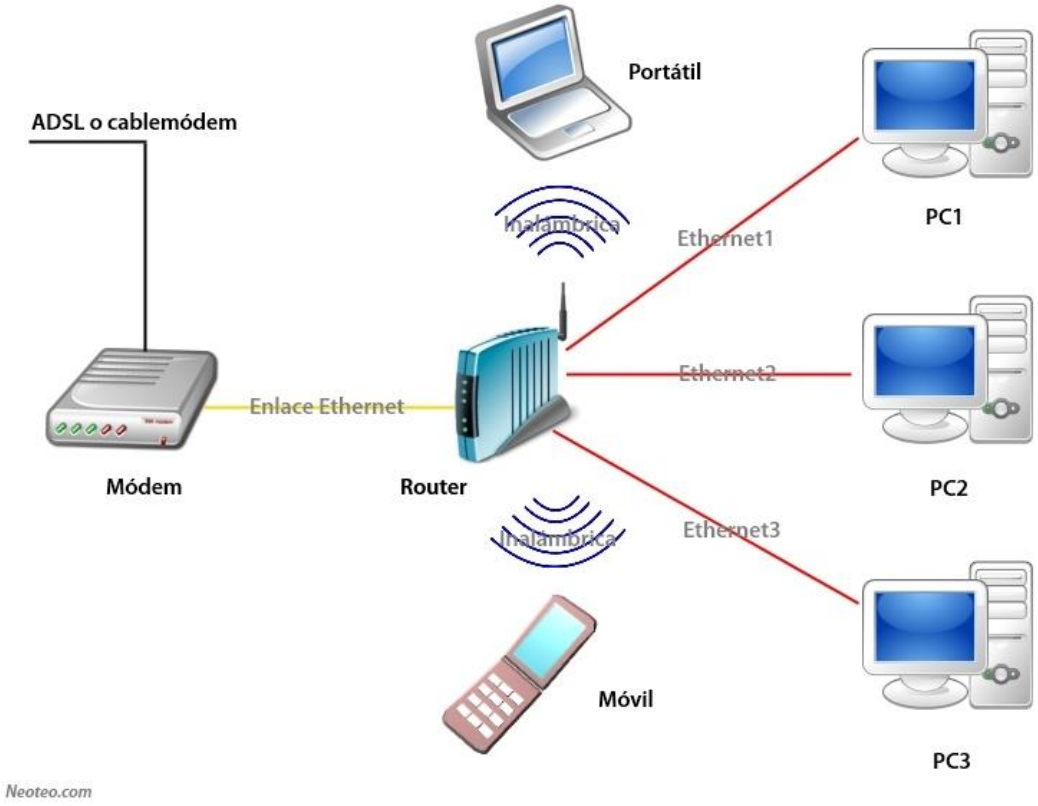
El otro dispositivo imprescindible para montar una LAN (Local Area Network, Red de Área Local) doméstica es el router o enrutador que, como ya hemos mencionado con anterioridad, se encarga de la conexión de los múltiples dispositivos que podemos tener conectados: portátiles, ordenadores de sobremesa, tablets, smartTVs, impresoras, servidores, NAS (Newtork Attached Storage, o Almacenamiento Conectado en Red), smartphones, radios IP, cámaras IP, consolas de videojuegos, etc.

Aunque el conjunto módem-router es más flexible porque nos permite cambiar el router que nos ofrece la operadora por uno con mejores características (y con muchas más posibilidades de configuración), las operadoras suelen ofrecer un dispositivo conjunto para las conexiones ADSL. Los equipos de las operadoras, además, no son de una calidad sobresaliente: suelen ofrecer conectividad sólo en una banda (la de 2'4 GHz), y las conexiones Ethernet suelen ser del tipo 10/100 en lugar de Gigabit Ethernet.



El tema de la banda de comunicación (no confundir con los canales) tiene su importancia, porque con un router dual (con doble banda: 2.4 GHz y 5 GHz) podemos configurar dos WiFi's independientes, dado que la banda de 5GHz permite velocidades de conexión más elevadas (hasta 450Mbs, frente a los 300 Mbs de la banda de 2.4 GHz). Así pues con un router con doble banda podemos dedicar la de 5GHz para los dispositivos que manejen contenidos multimedia, mientras que la banda de 2.4 GHz la dejaremos para los dispositivos que se conecten a la web o utilicen servicios más ligeros.

La topología típica simplificada de una LAN doméstica quedaría así:



El número de equipos domésticos que se conectan a internet es cada vez mayor, e irá incrementándose de forma dramática con el progresivo desarrollo del IoT (Internet of Things, o Internet de las cosas) que, en un sentido laxo, haría referencia a la conexión a internet de cualquier cosa y, más concretamente, de cualquier objeto cotidiano (siempre, claro, que dispongamos de los sensores adecuados y del software necesario para gestionarlo).

Extensor de red / Punto de acceso

Hasta ahora hemos repasado las funciones de los dos elementos indispensables en una LAN doméstica: el módem y el enrutador. Sin embargo, hay situaciones en las cuales la señal generada por el router no es suficientemente potente para alcanzar todos los rincones de la casa, centro educativo u oficina. Hemos de recurrir entonces a un dispositivo que amplifique la señal y, caso de que hubiese que gestionar más equipos remotos, sea capaz de hacerlo. Pero vayamos por partes.

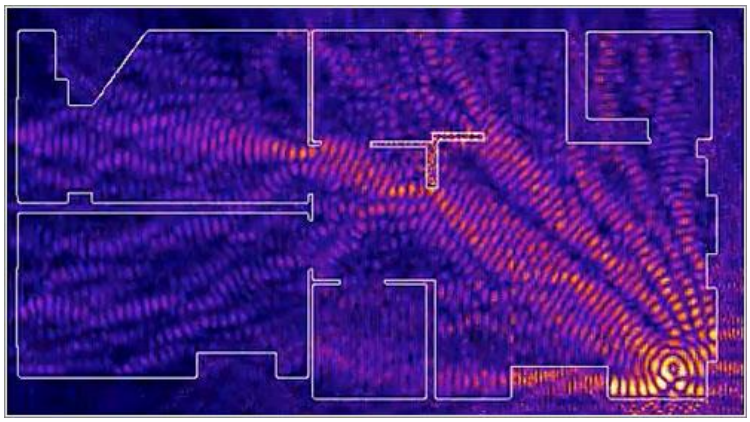
La idea central tanto del extensor como del punto de acceso es muy sencilla: amplificar la señal del router cuando ésta aún es relativamente fuerte para extender el alcance de la WiFi. ¿Cuándo hemos de recurrir a un extensor de red? Cuando, por cualquier circunstancia, la señal del router llega demasiado debilitada al punto en que deseemos hacer uso de la wifi.

Cómo se propaga la WiFi en el interior de un edificio

La WiFi es una radiación electromagnética que se propaga en forma de ondas y a la que afectan tanto la distancia como los obstáculos, así como las interferencias en sus frecuencias (es un clásico que la wifi no funcione si hay un microondas en funcionamiento en sus cercanías). Además, ciertos materiales permiten su paso mucho peor que otros: por ejemplo los metales y superficies metálicas, los azulejos (cocinas, cuartos de baño) y las baldosas.

Podemos imaginarnos cómo se propaga la wifi en nuestra casa o centro educativo imaginándolo a oscuras y con un punto de luz en el salón, y qué ocurriría si vamos abriendo

puertas. Incluso sería más adecuado imaginarlo como un sonido proveniente del salón: se propaga por las zonas abiertas, pero presentaría problemas con las paredes, los ángulos o las puertas cerradas. El grosor de las paredes también es un hándicap.



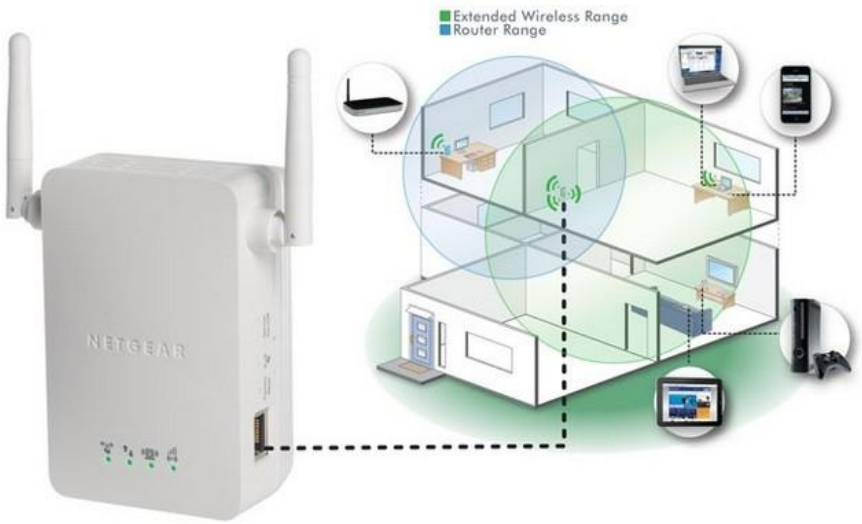
La imagen anterior es una reconstrucción matemática de cómo se propagaría el wifi en un apartamento de dos habitaciones.

Podemos seguir algunos consejos para mejorar la cobertura de nuestra wifi:

- Instalar el router a varias alturas. En principio, cuanto más alto esté, mejor.
- El router debería estar lo más cerca posible del centro de la vivienda, para evitar la distribución irregular de la señal.
- No escondas el router detrás o debajo de la TV, ni lo pongas cerca de superficies metálicas y/o reflectantes.
- La cobertura mejora si el router está alejado de paredes y rincones, y si no lo metemos en estanterías o cajones, rodeado por todos sus lados.
- Obviamente, el router se instalará lo más cerca posible a la zona de mayor uso, y a ser posible sin obstáculos intermedios.
- Evitar su instalación cerca de ventanas y balcones.
- Probar varias orientaciones de las antenas, aunque se recomienda la vertical como la más idónea.
- Los muros de carga, más gruesos, son auténticas barreras para la señal.
- Evitar la cercanía con fuentes de interferencias, en especial las que más le afectan: microondas, teléfonos inalámbricos y televisiones. Las luces fluorescentes y los problemas en la instalación eléctrica también influyen.

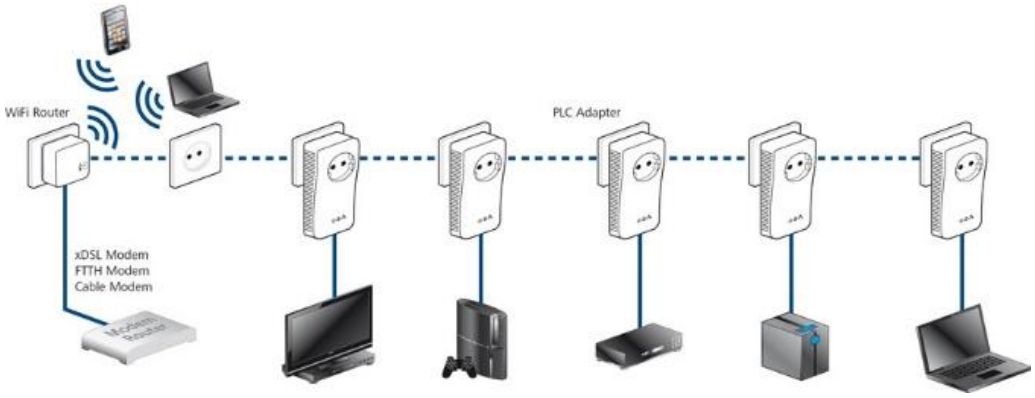
- Si hay demasiadas wifis cercanas, probar a cambiar de canal, para evitar la saturación.

Los extensores de red o antenas repetidoras ayudan a propagar la señal del router y a aumentar su potencia para que alcancen lugares más lejanos de la casa, como por ejemplo la planta superior o el sótano. Siempre han de instalarse en puntos donde llegue la señal del router con la suficiente potencia, pues actúan como puentes entre el router y las zonas más alejadas del mismo: si colocamos el repetidor o extensor en una zona con baja señal, la velocidad disponible bajará drásticamente, pues básicamente estarán ampliando una señal WiFi degradada.



Si necesitamos tener una cierta velocidad de conexión en los puntos alejados, no siempre es óptima la solución de usar un extensor, o incluso tampoco es cuestión de cablear toda la casa con cables Gigabit Ethernet.

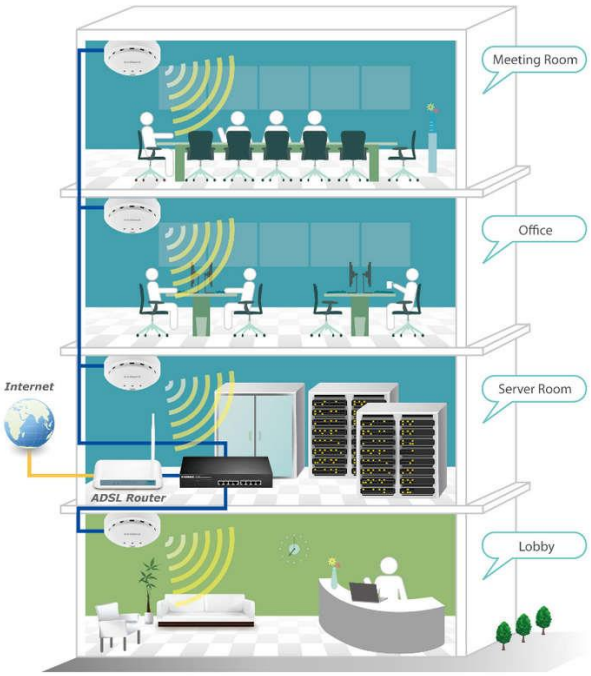
Una buena alternativa para obtener altas velocidades de conexión (necesarias, por ejemplo, para videoconsolas o smart TVs) en puntos alejados del router es usar un Adaptador PLC (Power Line Communications, o Comunicaciones por la línea eléctrica). Se trata de un adaptador que "inyecta" la señal de internet en la instalación eléctrica de nuestro hogar para llegar a ubicaciones en que no llegaría la WiFi de modo óptimo, y de un conjunto de dispositivos que posteriormente "extraen" esa señal del cableado eléctrico. Es totalmente compatible con la existencia de una WiFi, y su uso es muy sencillo: se enchufan los dispositivos, el 'emisor' en una toma de corriente cercana al router, y los demás (receptores) en los lugares que necesitemos. Se emparejan los dispositivos, y listo.



Qué es un punto de acceso y en qué se diferencia de un extensor de red

Un punto de acceso es un dispositivo que crea una red de área local inalámbrica (WLAN, o Wireless Local Area Network). Se emplean para gestionar el acceso WiFi de un gran número de equipos de forma óptima, pues pueden gestionar unas 60 conexiones simultáneas por dispositivo (un extensor de red típico no es capaz de manejar más de unas 20 conexiones simultáneas, pues aunque incrementan la cobertura del router no incrementan su ancho de banda).

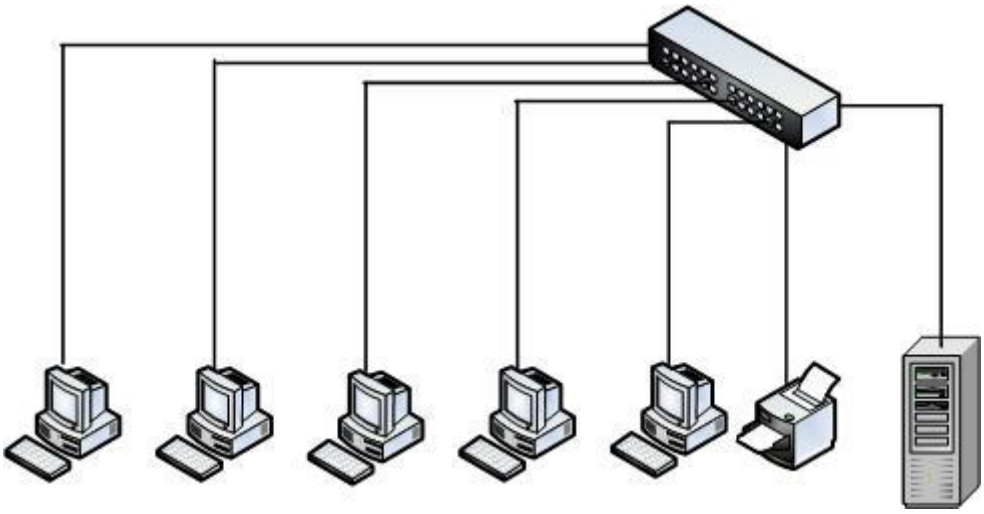
Los puntos de acceso se emplean en oficinas o edificios de varias plantas: cada punto de acceso puede colocarse para gestionar una planta, conectándose a un router o más típicamente un switch. A diferencia de los extensores de red, los puntos de acceso son una muy buena opción para instituciones educativas o empresas.



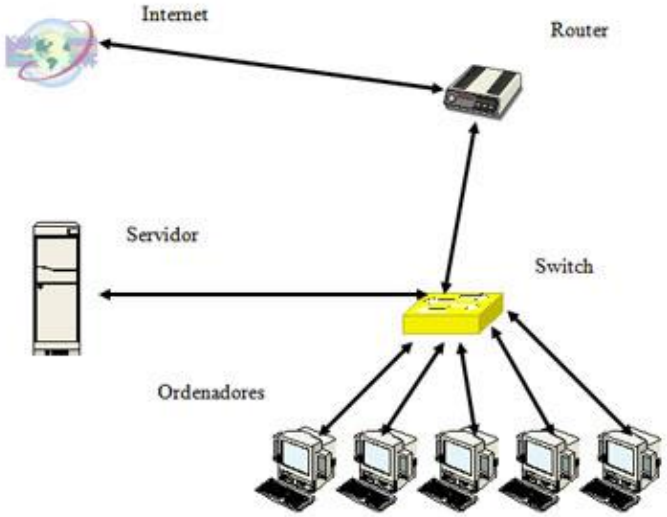
Switch de red

Los switches o conmutadores son los dispositivos digitales lógicos encargados de la interconexión de equipos dentro de una misma red, formando la red de área local (LAN) de la que venimos hablando, y cuyas especificaciones técnicas siguen el estándar Ethernet (o IEEE 802.3).

Las redes locales cableadas actuales siguen el estándar Ethernet, con una topología en estrella en la que el switch constituye el elemento central.



La función básica de un switch es la de conectar dispositivos en red. El switch no proporciona por sí solo conectividad con otras redes ni con internet, para ello es necesario un router.



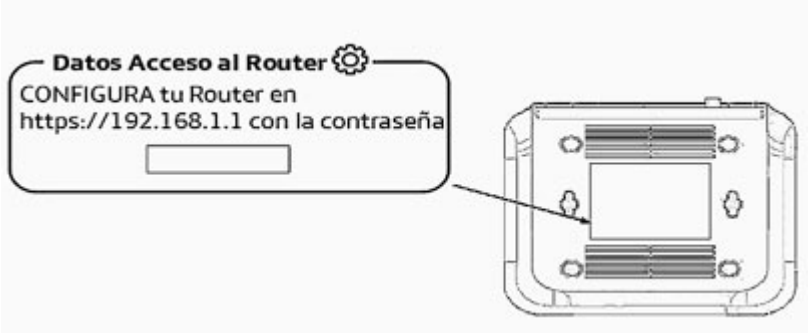
En grandes empresas o instituciones educativas con gran número de conexiones, los switches se montan en rack para disponer de un gran número de puertos Ethernet en un espacio reducido.

La configuración del router

Vamos a dar unas pautas generales que nos puedan guiar en la configuración inicial de un router WiFi más o menos estándar, pues las interfaces de configuración pueden variar mucho de un modelo a otro, incluso dentro de la misma marca:

El primer paso para configurar un router es acceder a su interfaz de configuración a través de un navegador web, desde cualquier dispositivo conectado en red local (se suele recomendar que sea conectándose por cable al router).

La IP del router es, típicamente, https://192.168.1.1



Algunos routers pueden tener una IP similar, siempre dentro del mismo rango, por ejemplo: 192.168.0.1, 192.168.1.2, 192.168.1.254

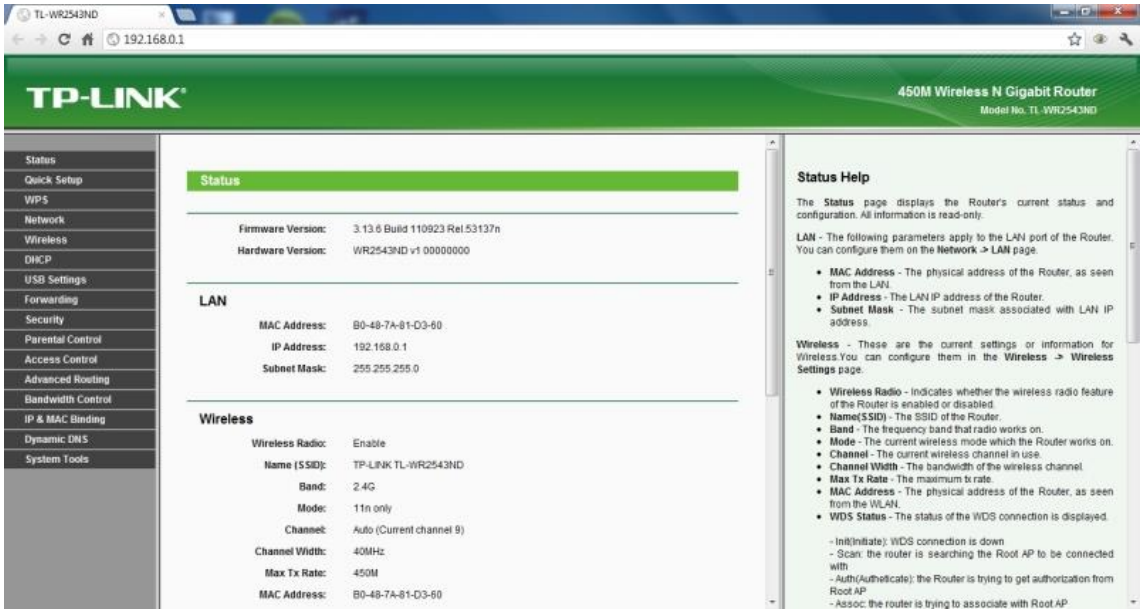
- A continuación, nos pedirá un usuario y contraseña para poder entrar a la interfaz de configuración. Los más usuales son:

  Usuario: admin

Una buena alternativa para obtener altas velocidades de conexión (necesarias, por ejemplo, para videoconsolas o smart TVs) en puntos alejados del router es usar un Adaptador PLC (Power Line Communications, o Comunicaciones por la línea eléctrica). Se trata de un adaptador que "inyecta" la señal de internet en la instalación eléctrica de nuestro hogar para llegar a ubicaciones en que no llegaría la WiFi de modo óptimo, y de un conjunto de dispositivos que posteriormente "extraen" esa señal del cableado eléctrico. Es totalmente compatible con la existencia de una WiFi, y su uso es muy sencillo: se enchufan los dispositivos, el 'emisor' en una toma de corriente cercana al router, y los demás

  Contraseña: admin

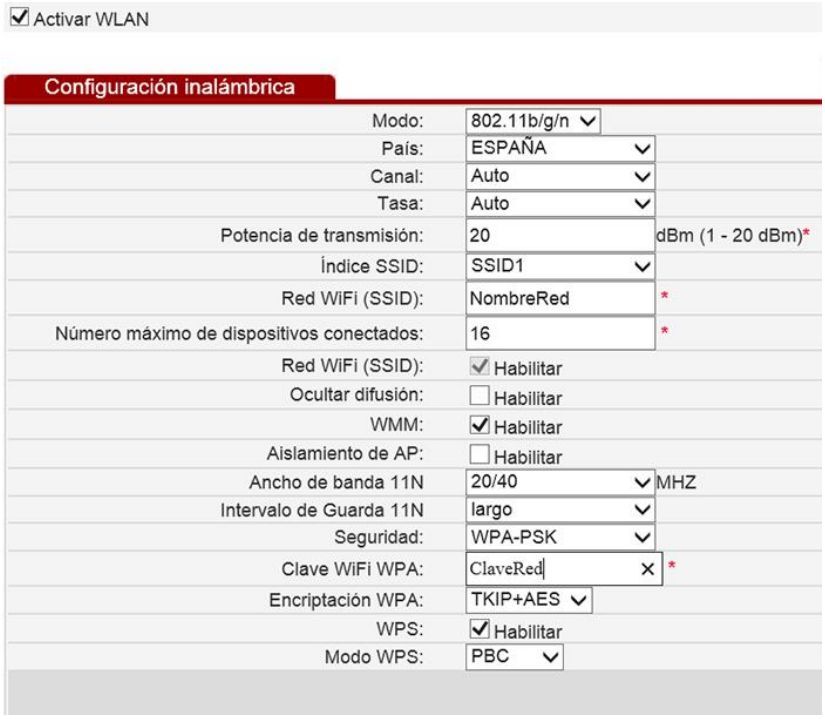
- Una vez entremos en la interfaz web, nos encontraremos con multitud de opciones de configuración.



Como ya hemos dicho, la disposición y opciones variará según marcas y modelos, pero en lo fundamental hemos de tener claro que tenemos dos grandes apartados a configurar:

- La configuración de red, que puede aparecer como TCP/IP settings, Network Settings, Network… Configuraremos cosas como las opciones de conexión a internet, direcciones IP o servidor DHCP.
- La configuración inalámbrica (o WiFi propiamente dicha): puede aparecer como Wireless, Wireless Settings, Link Setup… Aquí configuraremos cosas como el nombre y clave de la red, las opciones de cifrado, o el canal.

Centrándonos en las opciones más básicas de la configuración inalámbrica, nos encontraríamos con:



- Activar/Desactivar WLAN: Con esta opción podremos, simplemente, activar o desactivar el punto de acceso Wi-Fi de nuestro router, manteniendo la conexión por cable funcionando.
- Modo: Hace referencia al estándar wifi a usar. deberíamos dejarlo con la opción 802.11b/g/n. La versión n es la más rápida, pero también ofreceremos compatibilidad con las versiones más antiguas, por si algún dispositivo aún las usa.
- Canal: Cada canal tiene una determinada frecuencia; disponemos de 13 canales a elegir. Si notamos que la conexión va lenta, podemos probar a cambiar de canal por si nuestra red se solapa con otra.
- SSID (identificador de nuestra WiFi): Es el nombre que aparece cuando busquemos redes WiFi desde nuestros dispositivos.
- Ocultar difusión (ocultar SSID): oculta el identificador de nuestra WiFi para que no aparezca en una búsqueda. Nos proporciona más seguridad, ya que necesitaríamos saber para conectarnos, aparte de la clave, el nombre de la red.
- Seguridad (o autenticación): Es el sistema de encriptación que el router usará para identificar a los usuarios. WPA2-PSK es la opción más robusta, seguida de WPA-PSK. WEP no se recomienda por no ser tan seguro como los anteriores, ya que es un cifrado relativamente fácil de romper.
- Clave Wi-Fi: obviamente, la clave que queramos poner.

- WPS (Wi-Fi Protect Setup): es un sistema pensado para evitar tener que introducir claves para conectar un dispositivo a nuestro router; simplemente pulsamos un botón que está en el router y el botón que está en el dispositivo y ambos se enlazarán de manera automática. ¿Cuál es el problema? Que funciona mediante el intercambio de un PIN de 8 dígitos, es decir, simplemente tenemos que enviar esos 8 dígitos para que el router nos permita acceder a la red inalámbrica… Obviamente, es mucho más fácil averiguar ese PIN que romper una contraseña WPA2. La recomendación que te hacemos es que renuncies a la comodidad en aras de la seguridad y desconectes esta funcionalidad.

PARA TERMINAR

En esta unidad del curso CI2 básico hemos aprendido:

- Cuáles son los elementos básicos de una red informática
- Las principales topologías de las redes cableadas
- Las características de los distintos estándares WiFi
- Los principales elementos de una red WiFi
- Cómo configurar una red WiFi doméstica