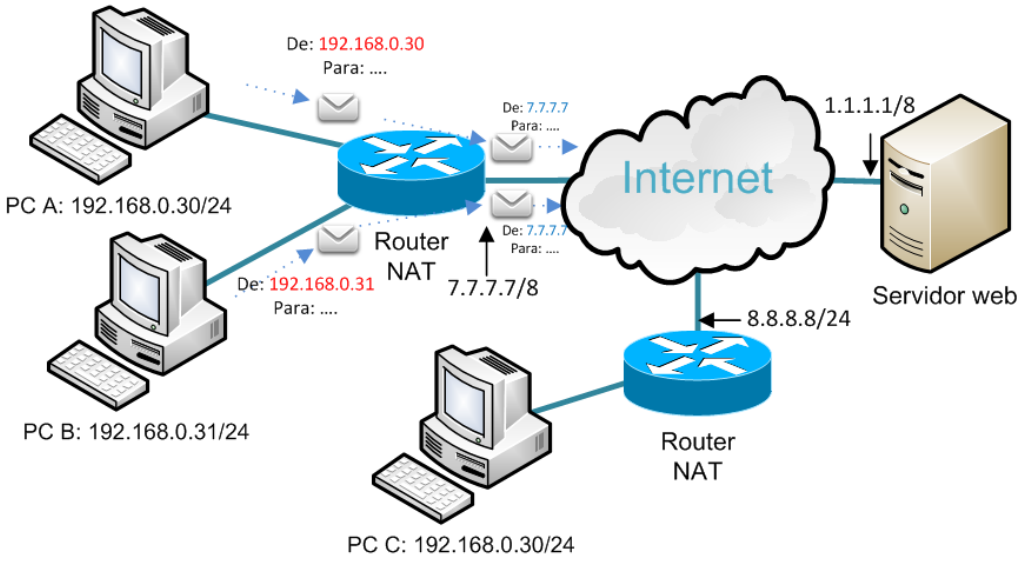
Actividad: Consulto la IP de mi PC de casa, es 192.168.1.30. Consulto la IP de mi PC del trabajo, es 192.168.1.30. ¿Cómo puede haber dos PCs con la misma IP?

Esto es algo "habitual", cuando surgió el problema del agotamiento de IPs hubo que buscar una solución para poder dar conexión a internet a más equipos sin cambiar el direccionamiento IP. Se implantó la técnica NAT, compartir una IP pública entre varios equipos, esto es lo que tenemos todos en casa, un router ADSL que tiene una IP pública compartida por toda la casa.

La técnica NAT sustituye la IP privada (192.168.0.X) por una IP pública única y envía el paquete hacia el exterior. Es decir, en cada casa se repiten las IPs privadas de los PCs conectados pero la IP pública es única en el mundo.

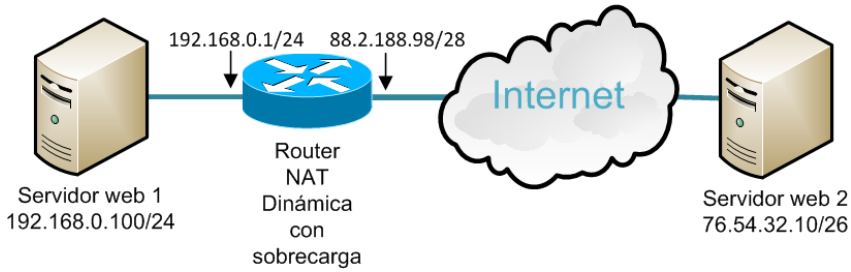
Como se puede apreciar en el esquema todos los PCs de una red doméstica tienen la misma IP pública (7.7.7.7) pero distinta IP privada (192.168.0.30 192.168.0.31).

En internet solo tiene sentido la IP pública, que es única, y por tanto, nos identifica de forma única en el mundo.



Actividad: En el siguiente esquema el router realiza una típica NAT. Responde a las siguientes cuestiones:

a) ¿qué URL teclearás desde el servidor web 1 para visualizar la web 2?
b) ¿qué URL teclearás desde el servidor web 2 para visualizar la web 1?
c) ¿qué sería necesario para visualizar la web 1?



En esta situación el router no realiza ninguna traducción hasta que no llega el primer paquete de la LAN con destino al exterior.

a) ¿qué URL teclearás desde el servidor web 1 para visualizar la web 2?

Sencillamente marcamos la IP del servidor web 2, la URL será http://76.54.32.10, esto no cambia nunca, el router envía al exterior el paquete, traduciendo la IP y el puerto origen por la externa

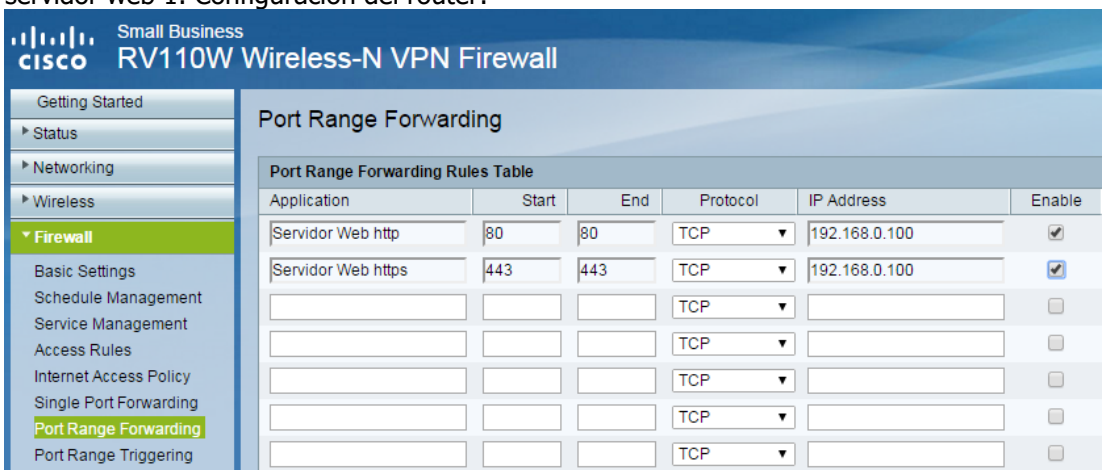
(88.2.188.98), cuando llegue la respuesta del servidor web 2 deshace la traducción y envía la respuesta al servidor interno 1.

b) ¿qué URL teclearás desde el servidor web 2 para visualizar la web 1?

Para poder acceder a la web la única posibilidad es teclear la IP pública del router http://88.2.188.98 pero, si aún no hemos abierto los puertos, las traducciones que encontraremos en la tabla NAT será de aplicaciones clientes de los PCs de la LAN que han accedido al exterior, por lo tanto no encontraremos ninguna entrada en la tabla NAT que nos redirija hacia la web 1.

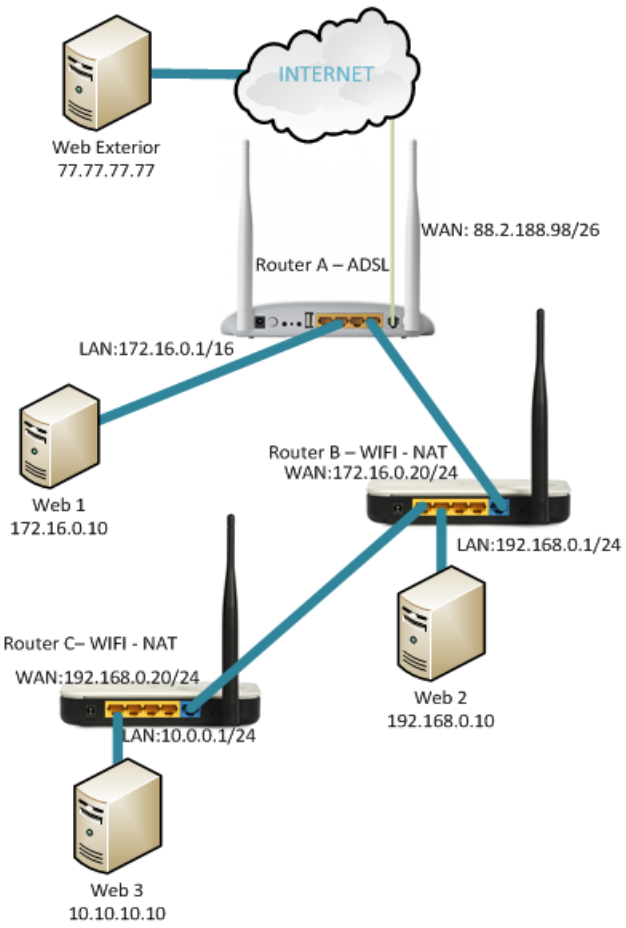
c) ¿que sería necesario para visualizar la web 1?

Habría que abrir el puerto 80 en el router, es decir, hay que añadir una entrada estática en la tabla NAT que traduzca 88.2.188.98:80 (IP pública: puerto habitual web) a 192.168.0.100:80, de tal forma que cuando algún dispositivo externo teclee la combinación 88.2.188.98:80 se envía al servidor web 1. Configuración del router:



Actividad: A partir del siguiente esquema de conexión NAT (todos los routers realizan NAT).

a) Indicar que puertos que abrirías y hacia cuales en cada router (A B y C) para poder acceder a todas las web
b) Indicar las URLs para ver desde el servidor Web Exterior las web 1 2 y 3
c) Indicar las URLs para ver desde el servidor Web 1 las web 2 3 y Exterior
d) Indicar las URLs para ver desde el servidor Web 2 las web 1 3 y Exterior
e) Indicar las URLs para ver desde el servidor Web 3 las web 1 2 y Exterior



a) Indicar los puertos a abrir

Vamos a empezar por el router C, cuando llegue una petición al puerto 80 a la IP exterior (192.168.0.20) haremos que responda el PC con IP 10.10.10.10 en el puerto 80 (web 3).

Por tanto la tabla de apertura de puertos del router es la siguiente:

Router C				
Puerto Externo	IP Externa	Protocolo	Puerto Interno	IP Interna
80	192.168.0.20	TCP	80	10.10.10.10

En el router B, cuando llegue una petición al puerto 80 a la IP exterior (172.16.0.20) haremos que responda el PC con IP 192.168.0.10 en el puerto 80 (web 2). El problema es que si el puerto 80 lo hemos abierto hacia la web 2, necesitamos un puerto diferente para la web 3, por ejemplo el puerto 81, abrimos entonces el puerto 81 al 80 del router C.

Router B				
Puerto Externo	IP Externa	Protocolo	Puerto Interno	IP Interna
80	172.16.0.20	TCP	80	192.168.0.10
81	172.16.0.20	TCP	80	192.168.0.20

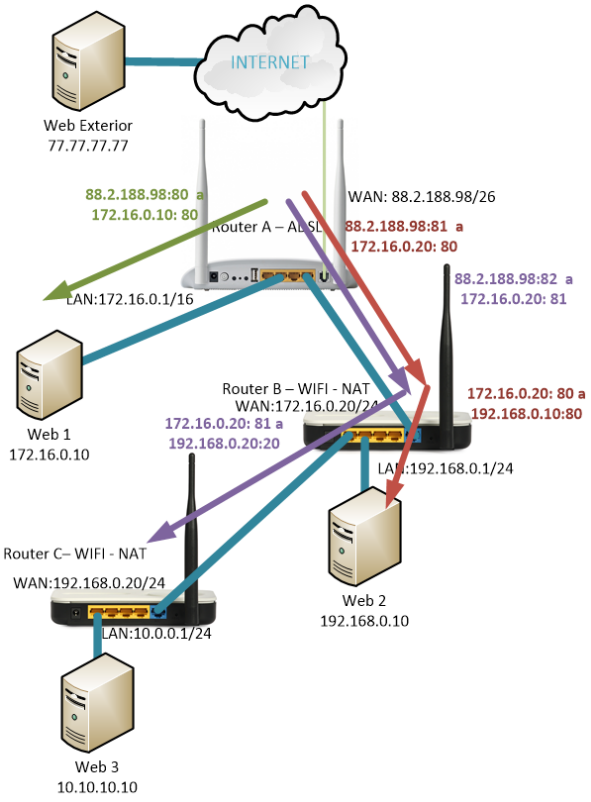
En el router A vamos a recibir 3 peticiones diferentes una por cada web interna, por tanto, necesitamos abrir 3 puertos diferentes (un solo puerto implica un solo servidor).
Podemos usar los puertos 80, 81 y 82

Router A				
Puerto Externo	IP Externa	Protocolo	Puerto Interno	IP Interna
80	88.2.188.98	TCP	80	172.16.0.10
81	88.2.188.98	TCP	80	172.16.0.20
82	88.2.188.98	TCP	81	172.16.0.20

Si enlacemos las tres tablas anteriores (eliminando el protocolo) nos quedará:

Router A				Router B				Router C			
P	IP Externa	P	IP	P	IP Externa	P	IP	P	IP Externa	P	IP
80	88.2.188.98	80	172.16.0.10	Web 1							
81	88.2.188.98	80	172.16.0.20	80	172.16.0.20	80	192.168.0.10	Web 2			
82	88.2.188.98	81	172.16.0.20	81	172.16.0.20	80	192.168.0.20	80	192.168.0.20	80	10.10.10.10

Es decir, el puerto 80 se desvía hasta la web1 (los paquetes llegan a la IP 172.160.10 y ahí responde el servidor web 1), el puerto 81 se desvía hasta la web 2 (los paquetes llegan hasta la IP 192.168.0.10 y ahí responde el servidor web 2) y el puerto 82 se desvía (atravesando los 3 routers) hasta la web 3.



b) Indicar las URLs para ver desde el servidor Web Exterior las web 1 2 y 3

Desde el Servidor Web Exterior únicamente tiene sentido conectar con la IP pública, recordemos que las IPs privadas pueden estar en multitud de redes privadas.
Para ver el servidor Web 1 la URL será http://88.2.188.98:80 o lo que es lo mismo http://88.2.188.98
Para ver el servidor Web 2 la URL será http://88.2.188.98:81
Para ver el servidor Web 3 la URL será http://88.2.188.98:82

c) Indicar las URLs para ver desde el servidor 1 las demás

Para ver la web exterior pública haremos lo normal cuando estamos en un PC dentro de una red local con ADSL, es decir, la instalación que todos tenemos en casa, la URL será la IP pública o su domino asociado: http://77.77.77.77 o http://77.77.77.77:80
Para ver el servidor Web 2 la URL será http://172.16.0.20 o http://172.16.0.20:80 puesto que la IP externa del router B está en la misma red que el servidor 1.
Para ver el servidor Web 3 la URL será http://172.16.0.20:81

d) Indicar las URLs para ver desde el servidor 2 las demás

Para ver el servidor Web exterior la URL será http://77.77.77.77
Para ver el servidor Web 1 la URL será http://172.16.0.10
Para ver la Web 3 la URL será http://192.168.0.20

e) Indicar las URLs para ver desde el servidor 3 las demás

Para ver el servidor Web exterior la URL será http://77.77.77.77
Para ver el servidor Web 1 la URL será http://172.16.0.10
Para ver la Web 2 la URL será http://192.168.0.10

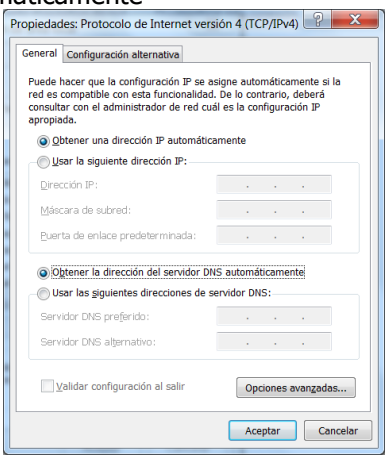
Actividad: Manipulación de routers domésticos.

a) Nos entregan un nuevo router doméstico ¿Cómo accedemos a la configuración?
b) Se nos ha bloqueado el router doméstico ¿Cómo lo desbloqueamos?
c) Accedemos al router pero hemos olvidado la clave ¿Qué hacemos?
d) Cambiar la clave del administrador
e) Cambiar la red privada a 10.0.0.0/8
f) Configurar con la máxima protección la WIFI de nuestro router-ADSL

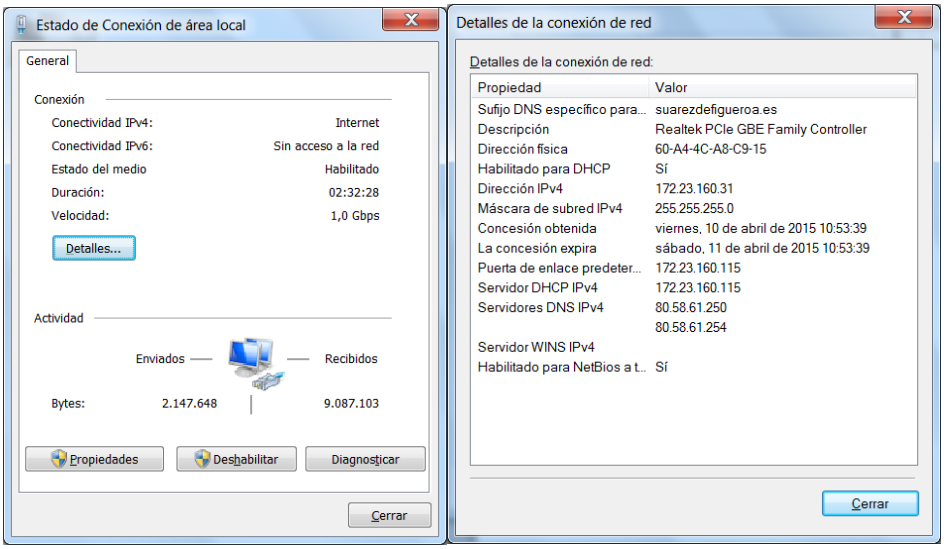
Aunque cada modelo suele funcionar de diferente forma y cada fabricante suele tener menús de configuración diferentes vamos a indicar las formas más habituales para realizar las diferentes tareas

a) Nos entregan un nuevo router doméstico ¿Cómo accedemos a la configuración?

Lo habitual es que se configure a través del navegador, para conectar al router hay que conocer su IP por defecto y teclearla en el navegador.
Si no la conocemos: estos routers de fábrica suelen venir con el servidor DHCP activado, así que, lo más rápido es conectar nuestro PC por cable al router (porque algunos traen de fábrica la WIFI desactivada) y esperar a que nos asigne una IP, nuestro equipo debe estar configurado para "Obtener una dirección IP automáticamente"



Para comprobar la IP recibida accedemos al estado de la conexión de área local, y vemos los detalles:



La puerta de enlace (172.23.160.115 en este caso) es la IP del router.

b) Se nos ha bloqueado el router doméstico ¿Cómo lo desbloqueamos?

Hay que buscar un botón de reset en el router, lo mantenemos pulsado y esperamos, depende de cada modelo, normalmente basta 15 segundos pero si tiene el firmware dd-wrt hay que hacer un reset 30-30-30 (pulsamos el botón reset durante 30 segundos, apagamos sin soltar el botón del reset otros 30 segundos, volvemos a encender sin soltar el botón de reset durante otros 30 segundos).

Después del reset el router volverá a los parámetros de fábrica y procederemos como en el ejercicio anterior.

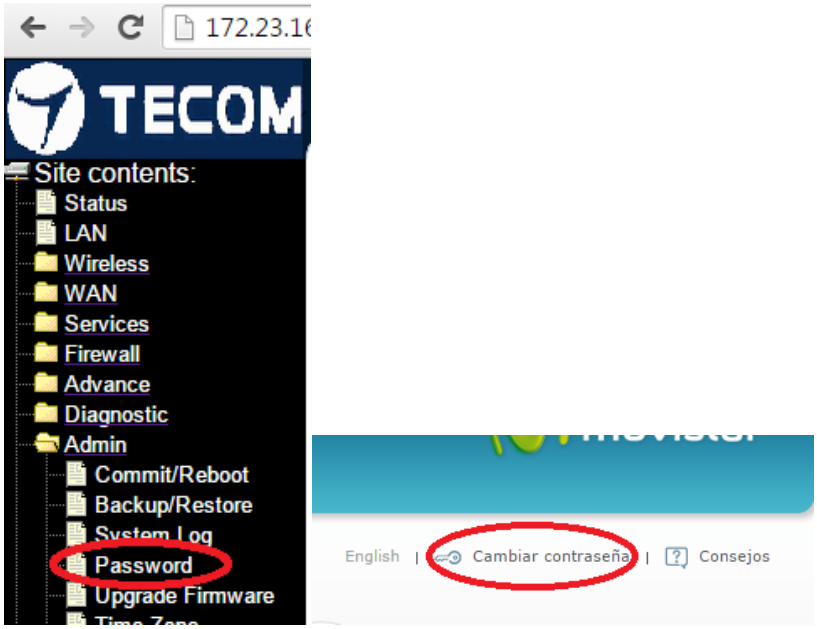
Los usuarios y claves de acceso suelen variar pero es muy común: admin, 1234, root. Podemos probar con estos.

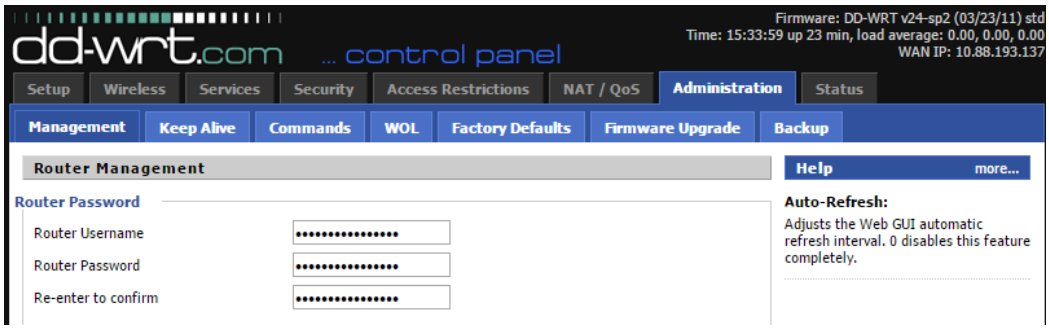
c) Accedemos al router pero hemos olvidado la clave ¿Qué hacemos?

Resetear el router igual que en punto anterior y volver a configurar todos los menús igual que los teníamos. Muchos modelos permiten hacer copia de seguridad de su configuración, evidentemente, es recomendable tener una copia para restaurar los valores y evitar tener que configurar todo de nuevo.

d) Cambiar la clave del administrador

Esta es una de las primeras medidas que tenemos que tomar, si no cambiamos los valores de fábrica, cualquier persona a través de la señal inalámbrica podría manipular nuestro router. Aquí mostramos varias pantallas de cambio de claves:





e) Cambiar la red privada a 10.0.0.0/8

Las redes privadas más habituales que se utilizan en los routers domésticos son 192.168.0.0/24 o 192.168.1.0/24, si por algún motivo queremos cambiar esta red privada debemos acceder a la configuración del router, buscar la configuración LAN, lo habitual es que se configure a través del navegador, para conectar al router hay que acceder a la web, apartado LAN y cambiarla. OJO, cuando la cambiamos lo habitual es que nos desconecte porque ya no estaremos en la misma red que el router (acabamos de cambiar la red del router).

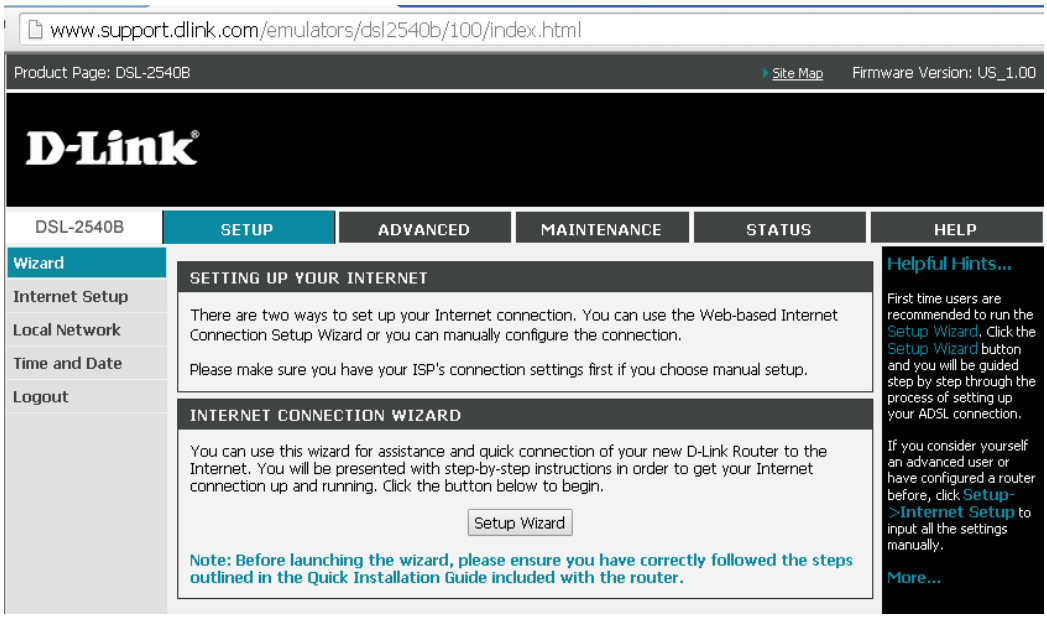
f) Configurar con la máxima protección la WIFI de nuestro router-ADSL

Siempre es posible que nos roben una señal WIFI, la cuestión es ponerlo lo más difícil que se pueda. Hay, como hemos visto en el tema 4 medidas a tomar, cada fabricante diseña menús y pantallas diferentes pero todos suelen permitir las medidas:

- Camuflaje SSID - Deshabilite los broadcasts SSID de los puntos de acceso, esto significa que el router no va a informar de la existencia de la conexión, por tanto, no aparecerá en las redes disponible, debemos conocer el nombre para configurar el acceso.
- Filtrado de direcciones MAC – Cada tarjeta de red tiene asociada un identificador único, la MAC, con esta opción limitamos el acceso a los dispositivos de los cuales indiquemos su MAC.
- Implementación de la seguridad WPA3 (si no es posible usaremos WPA2-PSK AES). Hay varios tipos de seguridad pero esta es la que más garantías da, además no olvidemos elegir una clave compleja (Mayúsculas, minúsculas, números, símbolos y longitud de la clave)
- Evitar el uso de parámetros predeterminados. Lo mismo que nosotros para configurar un router lo primero que probamos es 1234, admin, etc. cualquier intruso también lo hará, así que no olvidemos cambiar estas credenciales de fábrica.

Actividad: Manipulación de routers domésticos. Analiza el modelo DLINK DSL-2540B

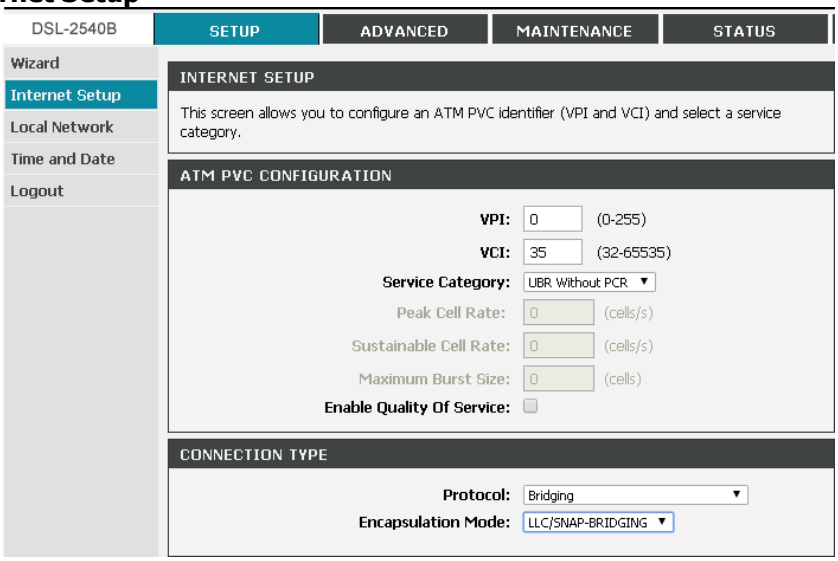
Las opciones de los routers ADSL son similares de unos fabricantes a otros.
La pantalla inicial de este modelo es la siguiente:



En la zona superior tenemos el menú principal formado por Setup – Advanced – Maintenance – Status y Help. Cambiando en este menú en la zona de la derecha aparece cada uno de los submenús correspondientes a las opciones del menú principal superior.

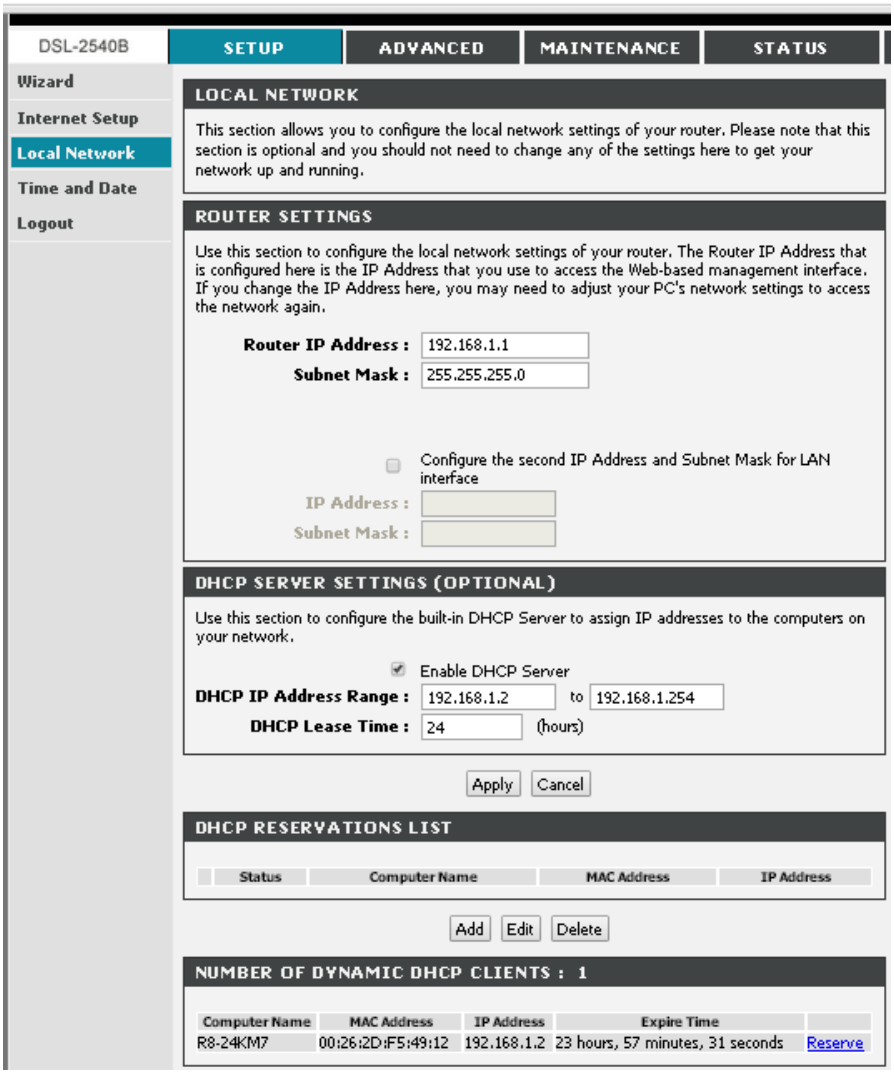
La primera pantalla nos sugiere "Setup Wizard", es un asistente para realizar la configuración inicial del router. Nos pedirá clave, configuración horaria y parámetros de conexión.
Pero podemos optar por configurarlo poco a poco a través de los menús.

Setup-Internet Setup



En esta pantalla introducimos los parámetros de conexión a internet, cada proveedor de internet tiene parámetros diferentes, lo normal es que el router ADSL que nos facilita el proveedor tenga configurados estos parámetros de fábrica. Pero estos parámetros pueden manipularse y, podemos usar un router de Telefónica en una conexión de Orange por ejemplo.

Setup-Local Network

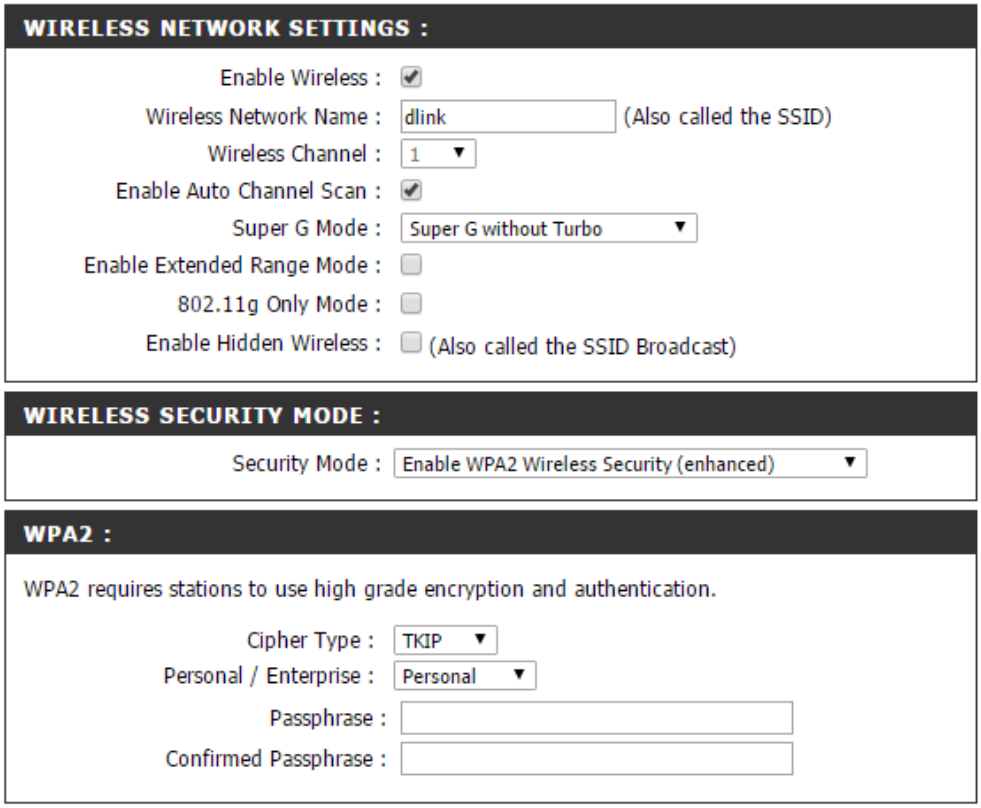


Esta pantalla es una de las que más vamos a manipular, aquí configuramos nuestra red local, lo primero que podemos cambiar es la IP del router (Router IP address), al cambiar esta IP también cambiamos el rango de IPs usadas en nuestra red, es decir, si ponemos 10.0.0.1 255.0.0.0 como IP del router acabamos de cambiar nuestra red local a 10.0.0.0/8.
También tenemos la configuración del servicio DHCP, indicamos las IPs que va a asignar el router a los PCs de nuestra red local (DHCP IP Address Range).
Podemos reservar una IP en concreto para un PC (DHCP Reservations List) para ello debemos indicar la MAC del PC en cuestión y la IP que deseamos asignarle.
Por último en la parte inferior vemos las IPs que asigna el router, nos puede servir para saber cuántos PCs están conectados a nuestra ADSL (si hubiese alguien robando nuestra señal es muy posible que apareciera en las IPs asignadas)

Setup-Time and date
Para configurar fecha y hora, podemos sincronizar la hora con un servidor de tiempo de internet (protocolo NTP)

Setup-Logout
Para desconectarnos del router, es decir, finalizar la configuración.

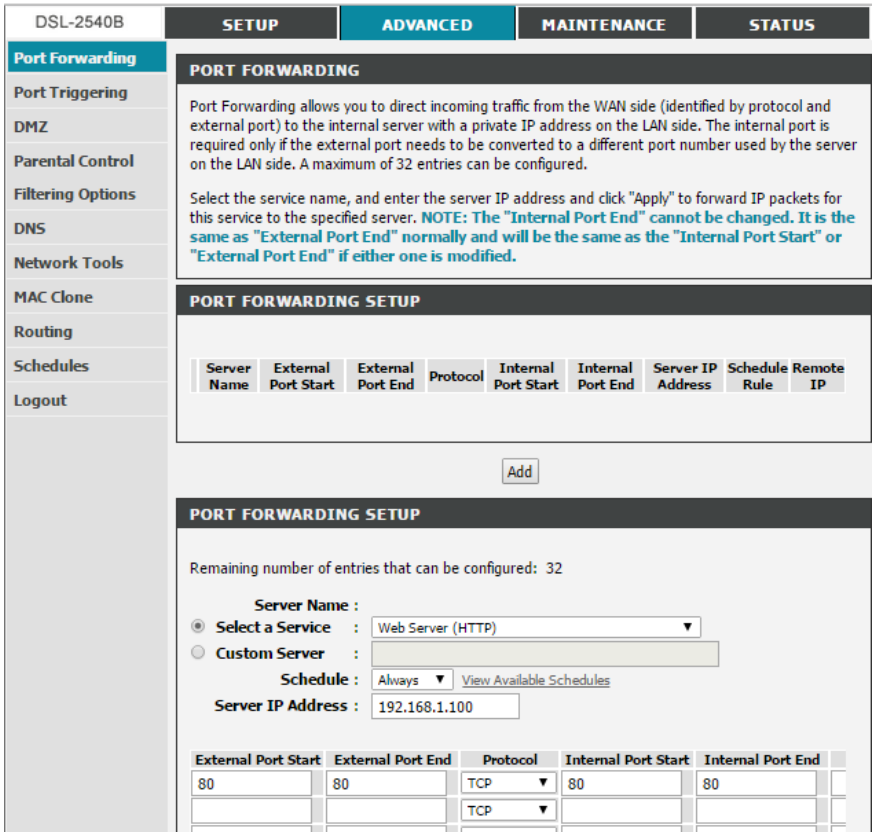
Setup-Wireless
Este modelo no es inalámbrico por lo que esta pantalla corresponde a un modelo diferente pero es una pantalla habitual en cualquier router ADSL



Para empezar en todos los routers es posible activar o no activar la señal WIFI, en algunos modelos lo normal es que venga desactivada por seguridad, en tal caso, basta con marcar la casilla enable.
Una vez activada la WIFI hay varios parámetros que configurar:

- SSID: es el identificador de una señal WIFI, cuando el usuario quiera conectar verá los diferentes identificadores de las señales WIFI a su alcance
- Canal: recordemos que hay, legalmente, 11 canales, que están solapados en frecuencia los canales consecutivos. Es muy habitual que el número de canal lo configure automáticamente el router.
- B/G/N: el protocolo 802.11 (señal WIFI) ha ido evolucionando a lo largo de los años, los routers suelen admitir todas las variantes pero, también, suelen admitir en la configuración limitar la señal a una determinada variante.
- Broadcast: La señal WIFI es propagada para informar a los usuarios de que se encuentra activa, pero, por seguridad, es posible evitar publicitar una señal, en tal caso, el usuario debe conocer el nombre de la señal WIFI a la que se quiere conectar.
- Seguridad: Para evitar accesos indeseados a través de la WIFI se aconseja activar una clave de acceso, el método más seguro es WPA3.

Advanced-Port Forwarding
Esta es la opción avanzada que más se usa, permitirá conectar desde el exterior a nuestra LAN, "abrir puertos".
Algunos fabricantes llaman a esta opción "Virtual Server" o "NAT"
También vamos a encontrar modelos que solo piden un puerto (no hay distinción entre externo e interno) la razón es que lo normal es abrir el puerto 80 externo al puerto 80 interno, pero, evidentemente, es una limitación.



Esta es la opción para abrir puertos en nuestro router, podemos buscar el servicio si no sabemos que puerto en concreto usa o configurarlo manualmente, para ello debemos indicar:

- Server IP Address: IP del PC de la red que tiene instalado el servicio, o sea, PC hacia el que vamos a abrir el puerto.
- External Port Start – External Port End: Si solo queremos abrir un puerto coinciden el primero y el último (es lo habitual). Cuando el router reciba del exterior una petición a este puerto la reenviará al PC que hemos indicado en Server IP Address.
- Protocol: Puede ser TCP, UDP o ambos, lo normal es que sea TCP, casi todos los servicios funcionan con este protocolo
- Internal Port Start – Internal Port End: Puerto donde el PC responde, normalmente coincide con el puerto externo, es decir, si llega una petición al puerto 80 (puerto por defecto de los servidores web) el router la envía al puerto 80 del PC.

En la pantalla está abierto el puerto 80 al PC 192.168.1.100

Advanced-Port Triggering

Esta opción permite abrir un puerto como consecuencia de que haya sido usado otro puerto, es decir, si usamos el puerto "Trigger" se abre el puerto "Open"

Advanced-DMZ

Cuando llegue una petición al router a un puerto que no esté indicado en Port Forwading (un puerto no abierto) se enviará al PC indicado en la IP.
Esta es una forma fácil de abrir todos los puertos a un PC. DMZ significa Zona desmilitarizada, el PC está más expuesto al exterior y, por tanto, hay más riesgo de ataques en este PC.

Advanced-Parental control

Aquí tenemos una especie de cortafuegos, cada fabricante diseña diferentes medidas en esta opción, en este caso es un bloqueo por MAC y horas.

Advanced-Filtering Options

Esta opción es para diseñar las ACLs que queremos aplicar en nuestra red.

Advanced-DNS
Para indicar las IPs de los servidores DNS a los que se enviarán las consultas DNS

Advanced-Network tools
En esta opción se incluyen una serie de herramientas: QoS (Calidad de servicio, dar preferencia a servicios o usuarios sobre otros), UPnP (Plug and Play para redes, no aconsejable activarlo), SNMP (Protocolo para administración de dispositivos de red), …

Advanced-MAC Clone
Cada dispositivo tiene una MAC asociada a la tarjeta de red, esta MAC está grabada en la ROM (solo lectura, imposible modificar), pero realmente lo que hace la tarjeta de red es usar una copia en RAM (escritura-lectura) de la MAC, cuando cambiamos esta copia, es decir, en la memoria RAM grabamos una MAC diferente a la del equipo estamos clonando la MAC.
Esta opción es útil cuando tenemos un filtro por MAC que saltarnos.

Advanced-Routing
Es para configurar el enrutamiento pero, como ya hemos visto en los temas anteriores, los router ADSL traen un enrutamiento básico de fábrica que es suficiente. Esta opción es para configuración más avanzadas del enrutamiento.

Advanced-Schedules
Para controlar los accesos por tiempo.

Maintenance-System
Podemos desde esta opción: reiniciar el router, hacer una copia de seguridad de la configuración, restaurar una copia de seguridad y restaurar los valores de fábrica (igual que resetear el router físicamente con el botón reset)

Maintenance-Firmware Update
Los fabricantes suelen sacar actualización del sistema operativo del router (firmware), desde esta opción podemos actualizar el firmware o también instalar un firmware libre como dd-wrt.

Maintenance-Access control
Esta opción permite controlar el acceso a la configuración del router: clave, IP de dispositivo desde el cual nos conectamos y método de conexión (telnet, http,…)

Maintenance-Diagnostics
Para comprobar el estado de la conexión

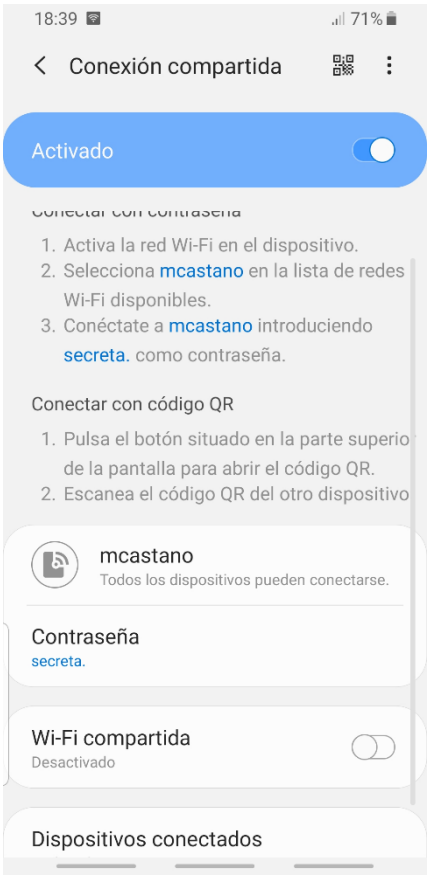
Maintenance-System log
Registro de los eventos del router (accesos, copias, desconexiones, …)
Status
Diferentes estadísticas e informaciones del sistema.

Actividad: Formas de conectar nuestro PC a internet a través de un móvil Android.

En Android hay 3 formas de compartir una conexión a internet:

1. Conexión compartida, el móvil actuará como router NAT, la interface WAN será la antena 4G y la interface LAN será la antena WIFI de nuestro móvil.
Lo primero es activar la zona Wi-Fi, el móvil nos solicitará que indiquemos SSID y configuración de la seguridad inalámbrica.

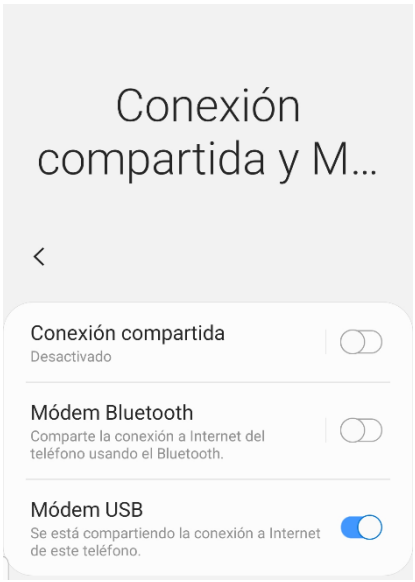
El SSID es el nombre que debemos buscar entre las redes WIFI disponibles.
Como se ve en la imagen podemos desactivar el broadcast, es decir, que no se publique el nombre del SSID, en tal caso debemos escribirlo en el PC.



La seguridad recomendada es WPA3.

Desde el PC o los PCs que queramos conectar bastará buscar la red y escribir la clave. La IP recibida corresponderá a la red privada que haya construido el móvil.

2. Modem USB, conectamos por cable USB el móvil al PC (LAN), el móvil permitirá marcar la casilla Modem USB, recibirá internet por la señal WIFI o por la antena HDSPA (WAN), primero intenta compartir la señal WIFI, si no es posible comparte la señal HDSPA.



Aunque "Modem USB" en teoría sería una conexión directa a internet, Android realiza una traducción de dirección, es decir, funciona como un router-NAT y asigna una IP privada a nuestro PC.

3. Modem Bluetooth, al igual que en caso anterior se realiza una traducción de direcciones, es decir el móvil funciona como router-NAT, la antena bluetooth es la interface LAN y la antena WIFI o HDSPA es la interface WAN.
Primero debemos vincular los dispositivos por bluetooth, después en nuestro móvil marcamos "Modem Bluetooth" y en el dispositivo cliente indicamos que queremos conectar a internet a través del móvil.

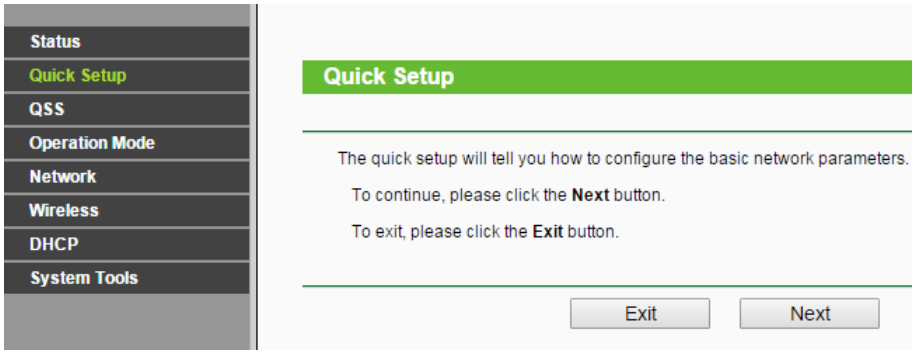
Actividad: Adquirimos una antena sectorial para una vivienda aislada donde no hay internet con el fin de conseguir captar una señal WIFI (SSID: ADSL_123 WPA2: 321_LSDA) situada a 3 kilómetros.

Para poder captar una señal lejana WIFI es prácticamente imprescindible tener visión directa y usar algún dispositivo con alcance suficiente como una antena sectorial.

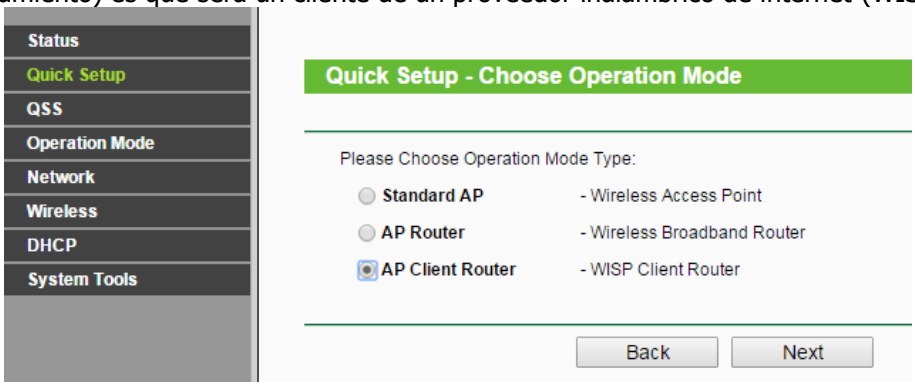
Supongamos que adquirimos una antena TL-WA7510N que colocaríamos en el exterior de la vivienda aislada y podríamos configurar a través de su web (podemos ver en http://www.tp-link.es/resources/simulator/TL-WA7510N/index.htm una simulación de la misma).

Para configurar la antena conectamos un cable desde el PC que usaremos para configurarla a la antena, esperamos a que nos asigne IP, buscamos la puerta de enlace y la marcamos en el navegador, o bien, buscamos en el manual cual es la IP por defecto de la antena para conectarnos a ella.

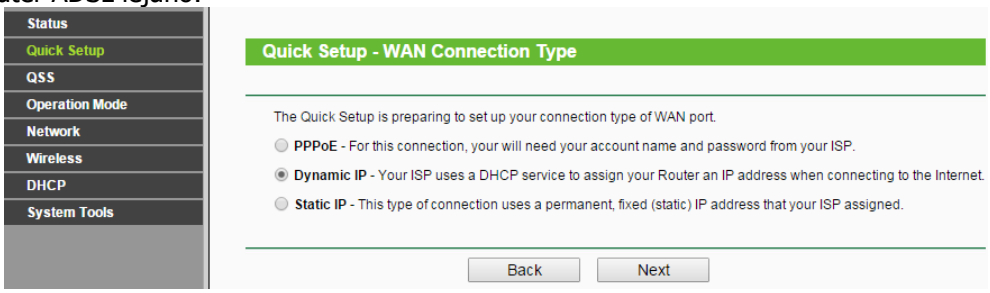
Lo más sencillo para "sintonizar" nuestra WIFI lejana es utilizar la configuración rápida:



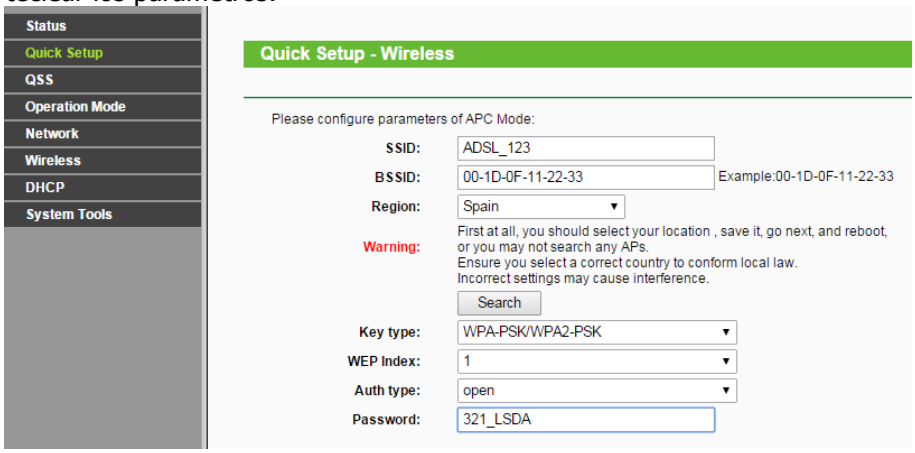
En la primera pantalla activamos el cliente WISP, es decir, el modo de operación (comportamiento) es que será un cliente de un proveedor inalámbrico de internet (WISP):



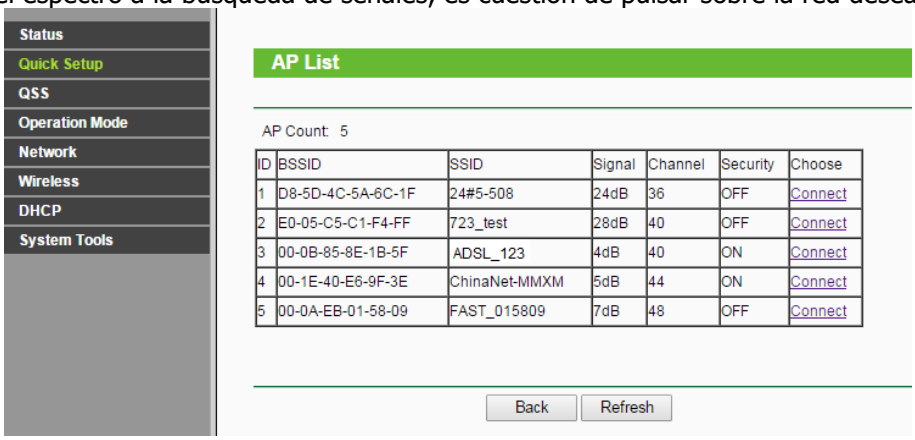
En la siguiente pantalla estableceremos que nuestra antena recibirá una IP de forma dinámica del router ADSL lejano:



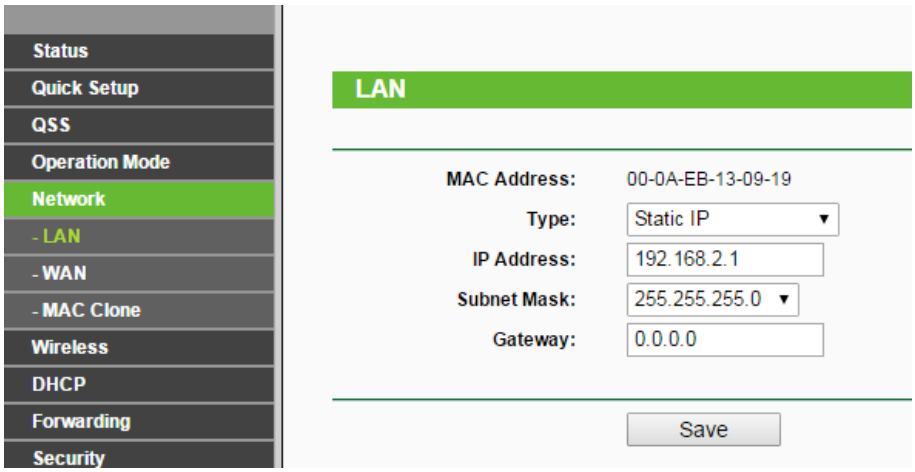
El siguiente punto de la instalación es buscar la WIFI a la que nos queremos conectar, para ello podemos teclear los parámetros:



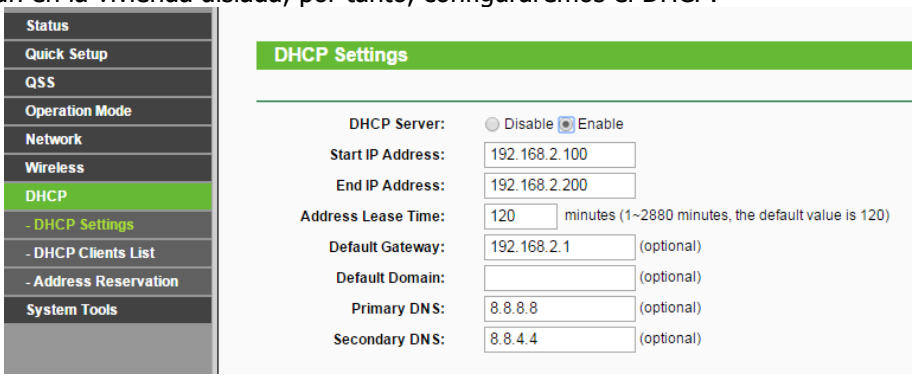
O buscarla, normalmente todos estos dispositivos tienen una utilidad (survey o search) que escanea el espectro a la búsqueda de señales, es cuestión de pulsar sobre la red deseada:



Esta antena, además, hará las funciones de router-NAT, la única precaución que debemos tomar es que la red LAN no sea igual que la red WAN, es decir, que si recibimos una IP del rango, por ejemplo, 192.168.1.0/24, cambiemos nuestra red LAN, por ejemplo, a 192.168.2.0/24, cuidado en este punto nos desconectaremos de la configuración al cambiar de red y deberemos reconectarnos para seguir configurando la antena:



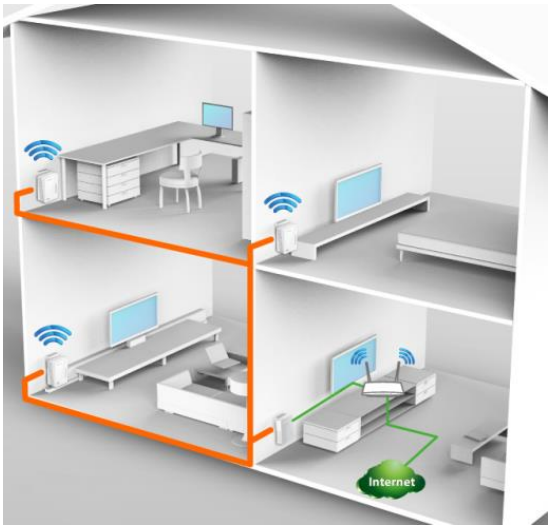
Por último, desde nuestra antena-router, debemos asignar IPs a los dispositivos que se encuentran en la vivienda aislada, por tanto, configuraremos el DHCP:



Observad, que en la primera imagen que hemos mostrado de la antena, solo hay una conexión RJ-45, por tanto, en el otro extremo de esta conexión solo se puede conectar un dispositivo, si queremos conectar varios dispositivos en la vivienda, en el otro extremo debemos conectar un punto de acceso que de internet a todos.

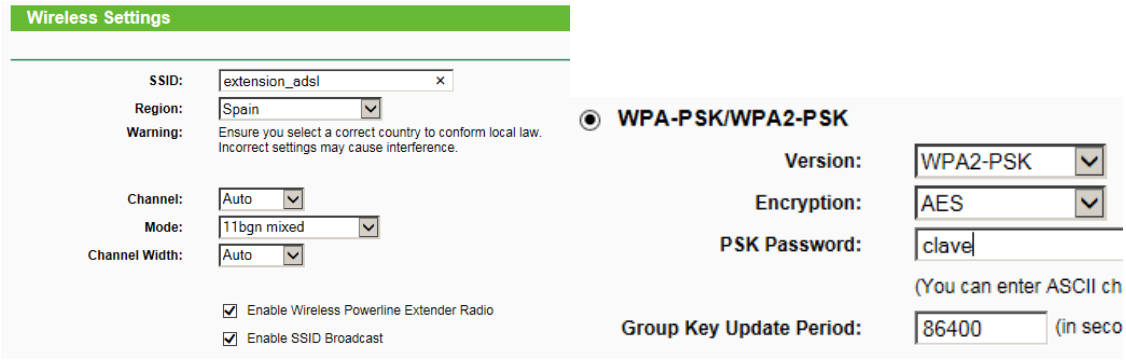
Actividad: En una vivienda con planta irregular se quiere instalar un adaptador PLC con WIFI para extender la señal

El pack básico de estos adaptadores es una pareja de dispositivos, se pueden comprar más adicionales.



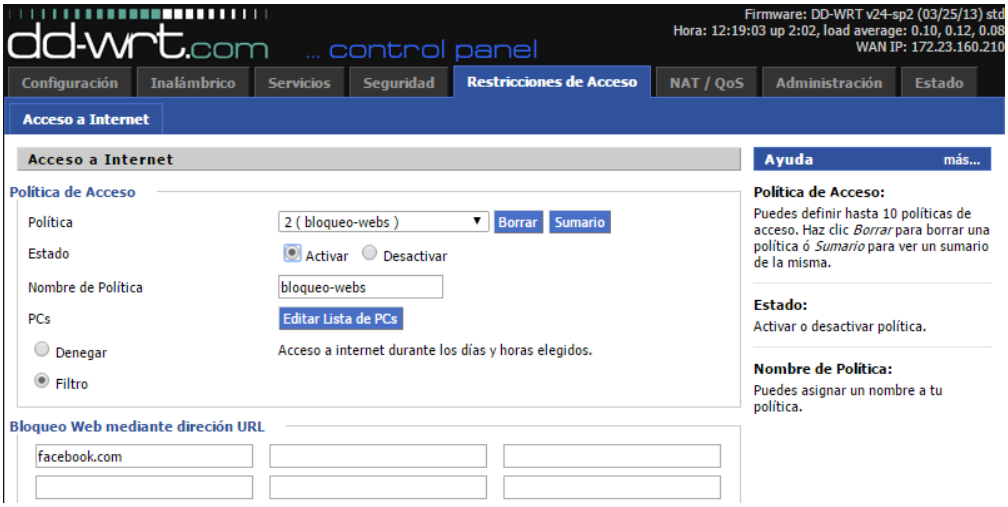
El primer dispositivo lo conectamos con un cable de red al router ADSL y a lo enchufamos a la corriente eléctrica (lo normal es que este primer dispositivo no tenga señal WIFI).

El segundo dispositivo será el que tendremos que configurar, para ello lo normal es que el fabricante nos facilite una IP de acceso o un software para una primera conexión.
La configuración no tiene nada especial, si la IP de acceso nos interfiere con alguno de nuestros dispositivos actuales le asignamos una nueva IP.
Una vez accedamos basta con poner el SSID y clave que deseemos:



Actividad: Bloquea el acceso a Facebook en tu router ADSL

Depende del modelo, muchos incluyen el bloqueo por URL como vemos en la siguiente imagen del firmware dd-wrt:



Si no fuera posible por URL podemos intentar el bloqueo por IP, para ello hacemos ping a Facebook.com, vemos cuál es su IP asociada: 173.252.120.6, el siguiente paso es bloquear todos los paquetes con destino a esta IP.

Actividad: Nos han facilitado un acceso a una red WIFI, para ello nos han solicitado la MAC de nuestro PC. ¿Cómo podríamos conectar más equipos?

Aunque hay un filtrado por MAC y la MAC está grabada en la ROM de la tarjeta de red realmente no se trabaja con este dato directamente sino que esta MAC es grabada a la RAM de nuestro dispositivo y se trabaja con esta copia. Hay una operación que permiten muchos routers que consiste en modificar la copia en la RAM de la MAC, es lo que se denomina CLONAR la MAC.

Por tanto necesitamos un dispositivo que reciba una IP del acceso WIFI y la comparta con varios PCs; además este dispositivo debe permitir clonar la MAC de nuestro PC en su memoria RAM, el dispositivo ideal para esto es un router WISP, es decir, un router cuya WAN es una tarjeta inalámbrica. También podemos adquirir un router-NAT inalámbrico normal que admita dd-wrt, con este firmware podemos configurar el dispositivo como router WISP, desde la opción Estado – Inalámbrica podemos buscar las señales WIFI cercanas y unirnos a ella, el firmware realizará la configuración necesaria:

Además tendremos que clonar la MAC desde la opción Configuración – Clonar Dirección MAC:

Con esto nuestro router utilizará la antena para unirse a la red WIFI y las 4 conexiones LAN para conectar los PCs.

El inconveniente es que no repartimos la señal en inalámbrico, para ello tendríamos que crear una subinterface inalámbrica (hacer que la antena de nuestro router sirva para WAN y para LAN). En la imagen vemos cómo quedaría la configuración inalámbrica de nuestro dispositivo