

# Redes

- [Redes](#)
- [Estructura de una red](#)
- [Cableado](#)
- [Router](#)
- [Protocolos](#)
- [IPs](#)
- [DNS](#)
- [Wifi](#)
- [A experimentar](#)

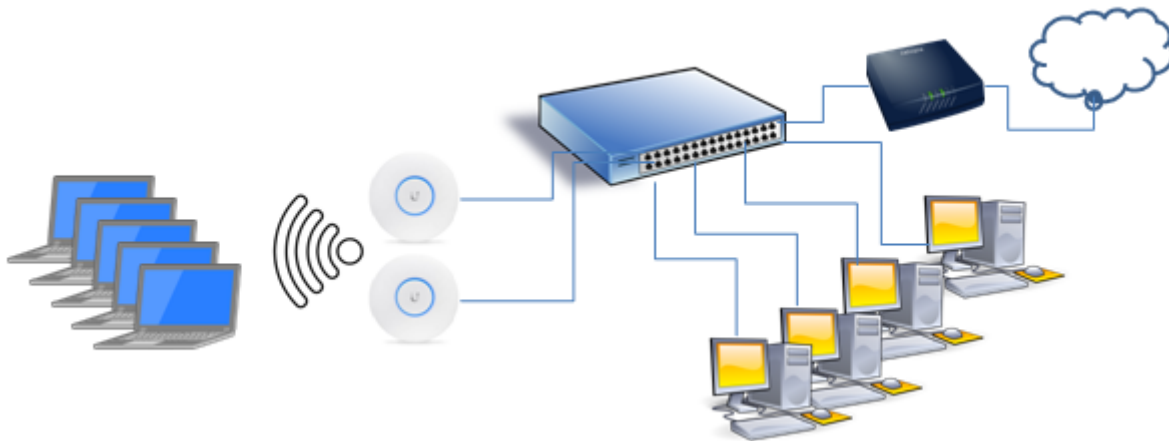
# Redes

La mayoría de problemas en los centros es "**no funciona Internet**" por lo que consideramos que es necesario que el responsable de medios informáticos tenga unos conocimientos mínimos de la red para saber gestionar y entender los problemas.



# Estructura de una red

La red local de tu centro (**LAN** Local Area Network) seguramente tiene esta estructura en estrella o árbol:



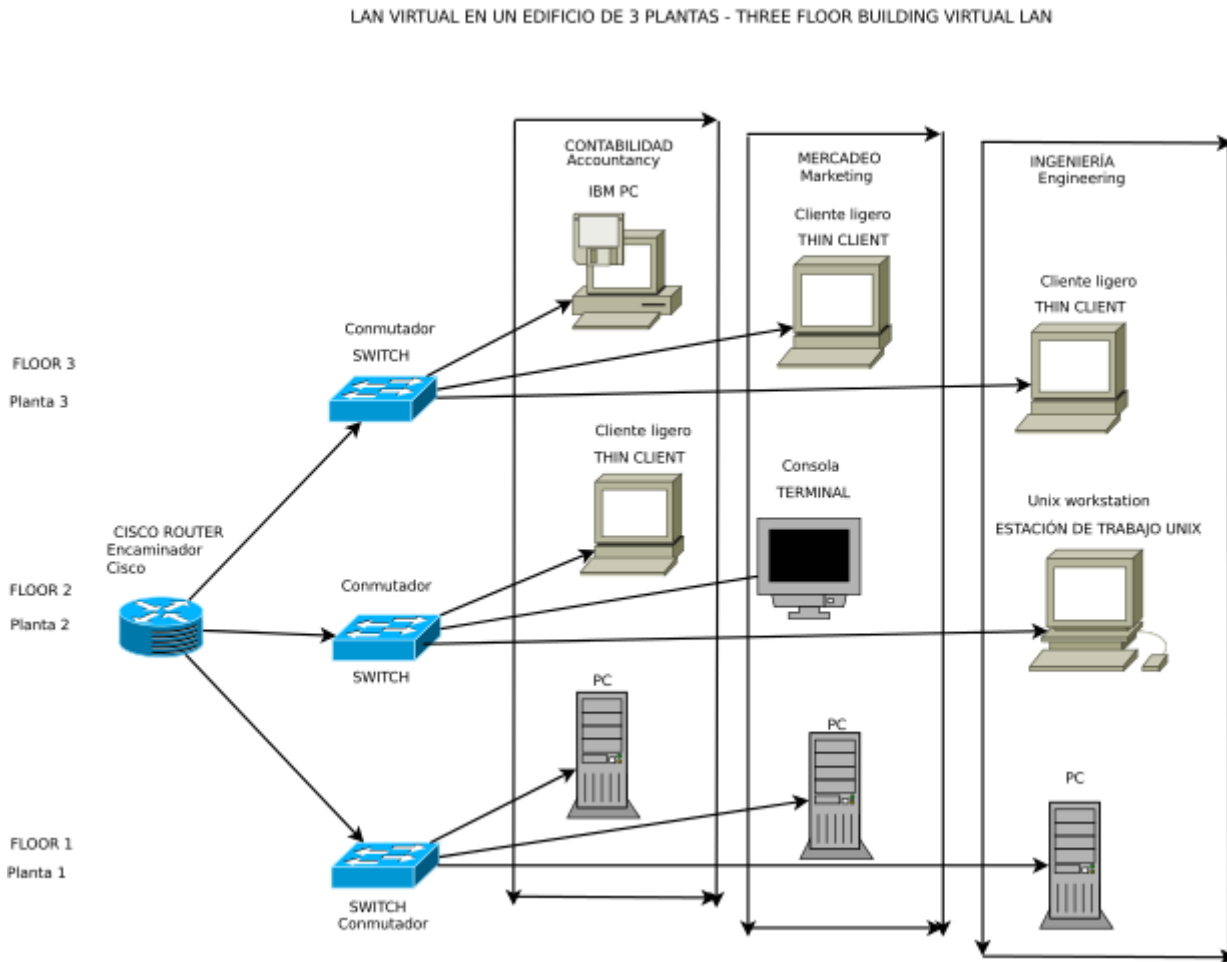
*Fuente elaboración propia con imágenes CC de Wikipedia*

- Los portátiles tienen una conexión inalámbrica con un **Punto de acceso AP Access Point** probablemente de la marca *Ubiquiti*.
- Los PCs y los AP están conectados a un **switch** por medio de cableado:
  - Los **switch** o conmutadores (en azul) son dispositivos hardware que permiten la transmisión de información entre varios equipos. Antiguamente se utilizaban concentradores **Hub** o concentradores que transmitían la información a todos indistintamente, lo que ralentizaba la red por ser *tontos*, los switch son *inteligentes* y almacena la dirección MAC de cada dispositivo conectado de manera que envía el paquete de información al equipo al que va dirigido, es decir no lo envía por todos los cables sino al cable concreto.
  - Es importante tener unos buenos switch que permita velocidades de Gbps y no sean un cuello de botella en la red del centro.
  - Las conexiones se realizan por medio de un cableado que dentro son 4 pares de hilos trenzados y en sus extremos conectores RJ45 que lo veremos [más adelante](#).
- En **router** (en la figura en negro) une nuestra red LAN con Internet, lo veremos [más adelante](#) es importante este elemento pues es el **cuello de botella**
- Seguramente no sólo existe un switch en tu centro sino varios que en forma de pirámide o cascada van conectando todos los equipos de tu LAN. Luego veremos una foto de un **rack**. Cada Switch agrupa a varios equipos de un edificio o de una planta, por lo tanto los switch no separan redes, sino se distribuyen según el espacio físico.

En la figura siguiente puedes ver que hay tres switch para tres plantas pero no tiene nada que ver con las tres redes que se han definido en esta estructura : *contabilidad, mercadeo e ingeniería*.

Técnicamente tres redes virtuales **VLAN** que verás cómo se hacen en [IPs](#).

Ya de paso puedes ver los símbolos comunes del Router (círculo con cuatro flechas que apuntan al centro) y el de Switch (cuadrado con cuatro flechas paralelas).



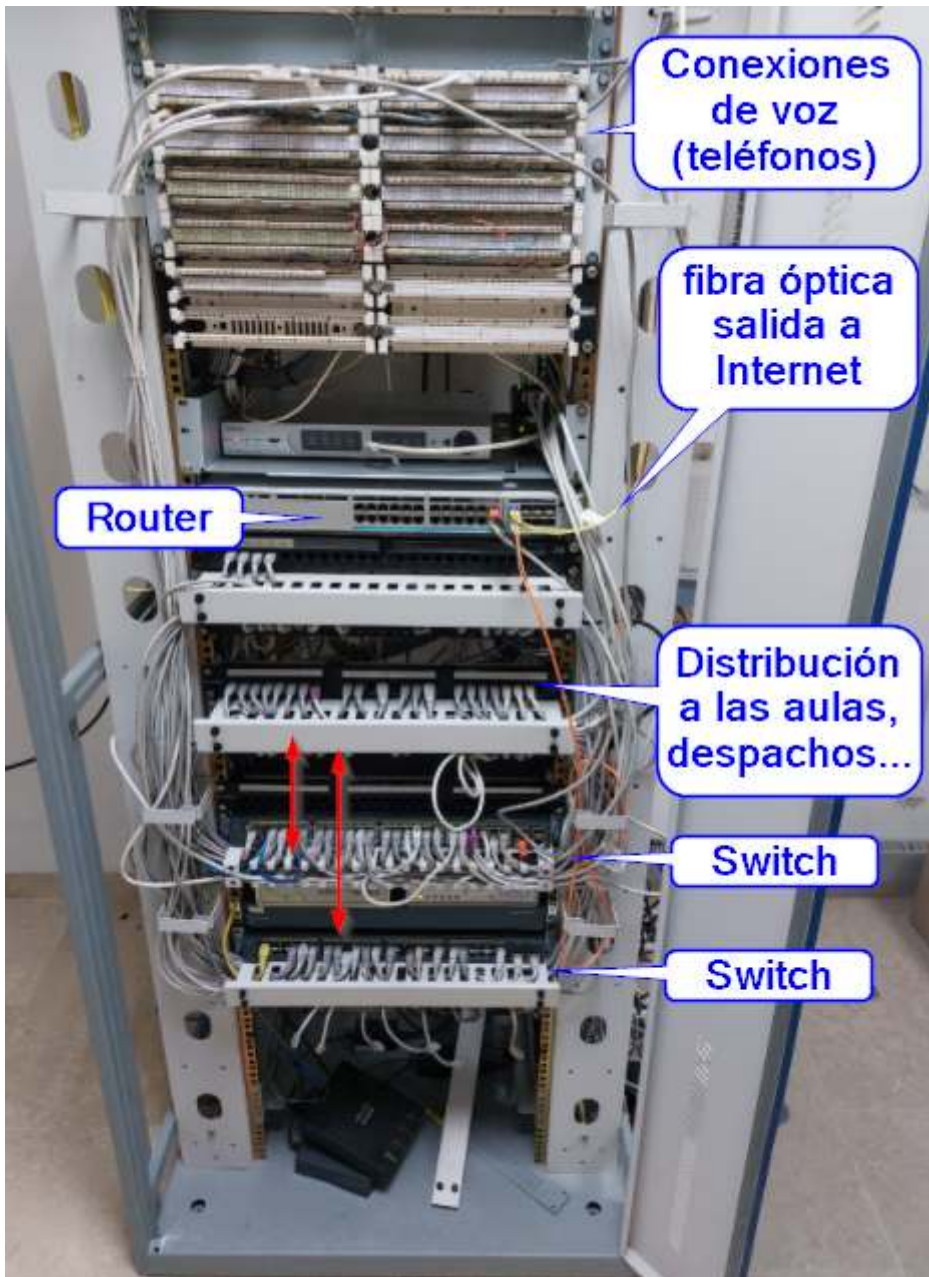
Fuente [Wikipedia](#)

## Rack

En la siguiente foto se muestra el **rack** (armario metálico donde se centraliza el cableado y los switches y router) de un centro educativo, puedes ver :

- es posible que veas unos cables finos sin conexión RJ45 enganchados en unas regletas, son los cables de voz o de teléfonos
- uno o unos cables de salida de Internet, en la foto son amarillos que son los cables de fibra óptica, pero puede ser de otro color y puede ser ADSL
- el aparato que hace de puente entre los switches y el cable de salida de Internet es el **router**.

- unos agujeros con bocas RJ45 que tienen etiquetas, esas bocas están directamente conectados con las aulas, despachos..
- de esas bocas a los switchs hay cables con conexiones RJ45 que parecen una locura de cables, pero simplemente es conectar la distribución del edificio a las aulas, se señala en la figura con flechas rojas
- finalmente los switchs



# Cableado

## Cable de par entrelazado

Este cable está formado por 4 pares de hilos entrelazados, en total 8 cables. Según su calidad (sobre todo por la cantidad de vueltas para evitar interferencias) se divide en diferentes categorías:

- **Cat 5** es muy vieja, hasta 100 Mbps.
- **Cat 5e** es la más común, soporta 1000 Mbps.
- **Cat 6** trabajan bien los 1000 Mbps.
- **Cat 6a** pueden aguantar 10000 Mbps = 10Gbps.
- **Cat 7** son los que se utilizan 10 gigabit ethernet.
- **Cat 7A** igual pero con una frecuencia de 1000MHz
- **Cat 8** compatible con frecuencias 2000 MHz y 40 Gbps.

**PROBLEMA :** En mi centro Internet va lento y tengo un cableado Cat5 ¿tengo que hacer una inversión de cambiar todo el cableado?

La respuesta es que seguramente NO ES NECESARIO pues de nada sirve cambiar a una categoría superior si la conexión de Internet es lenta, los switch no soportan esas velocidades y lo más común: Las tarjetas de red no aguantan velocidades por encima de los 100Mbps. Además van a salir nuevos protocolos que permitirán velocidades de Gbps con cableado Cat5.

Recuerdo un centro, de cuyo nombre no me quiero acordar, que realizó un importante esfuerzo económico de cambiar todo el cableado y la velocidad seguía siendo pésima. Al final era porque tenían una Botnet ver diapositiva 8.

Para estas cuestiones es mejor contar con el asesoramiento del servicio de informática del [Departamento](#).

No se tienen que hacer cableados muy largos pues la señal se atenúa, cuanto más largo más probabilidad hay que algunos paquetes de información sean erróneos y por lo tanto ralentiza la conexión. El máximo es 100m.

# RJ45

Es la interfaz que conecta nuestro cableado.



Fuente [Wikipedia](#)

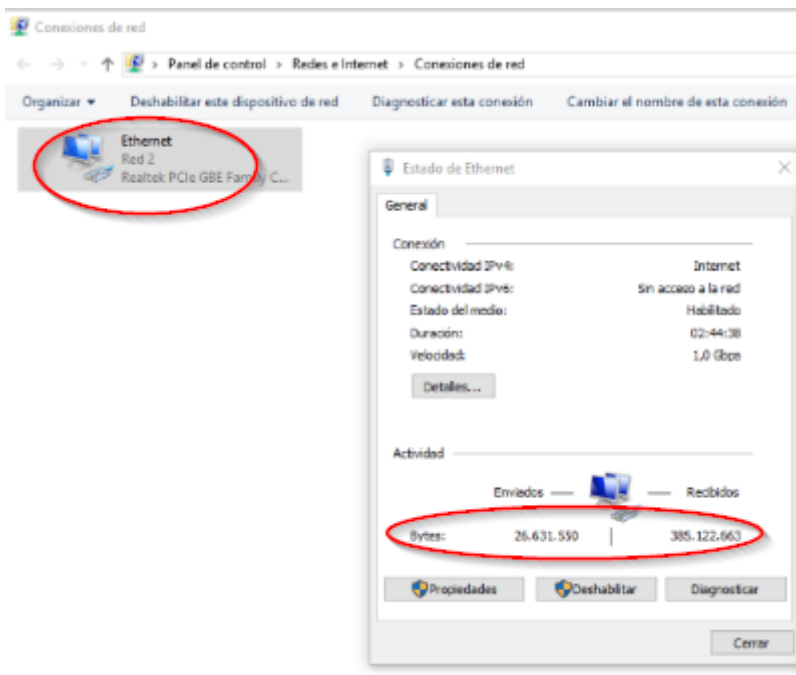
**No podemos conectar** dos ordenadores con un cable normal o directo, si no es a través de un Switch o Hub, la razón es que los cables se tienen que *cruzar* es decir el pin de transmisión tiene que ir al de recepción del otro y viceversa. Esto lo hace el Switch o Hub. Hay cables especiales llamados *cruzados* que ya están conectados el RJ45 de forma cruzada y sólo sirven para este propósito.

Suele ser un elemento muy castigado si el PC donde está conectado no está fijo o está en una mesa con ruedas luego suele ser un punto crítico ante problemas de conexión:

**PROBLEMA: NO VA INTERNET** en un equipo concreto conectado por cable.

Primero valoraremos si hay o no conexión entrando en Panel de control - Redes e Internet - Conexiones de red:





Si encontramos que no hay conexión o no hay tráfico, el problema puede ser que el cable con RJ25 está estropeado. Una comprobación simple de cambiar el cable puede ahorrarnos tiempo.

Si quieres, son útiles los *comprobadores de cable* que por menos de 10€ se pueden comprar en proveedores online Aliexpress o Amazon.



Metes los dos extremos (uno *master* que envía la señal y otro *slave* que recoge la señal y lo visualiza en forma de luces) y tienen que encenderse las luces en su mismo orden tanto en un extremo como en el otro 1-1 2-2 3-3 ... 8-8 si hay algún fallo ya podemos desechar ese cable. En el siguiente vídeo explica cómo se testea.



Si quieres hacer tú mismo el cables hay muchos tutoriales, busca "hacer cable red". Se hace con una **crimpadora** se sigue un criterio de colores.

PREGUNTA: ¿Se puede comprobar un cable con el tester teniendo un extremo en el tester y el otro extremo conectado a una "cosa" (router, switcht, AP, PC...) ?

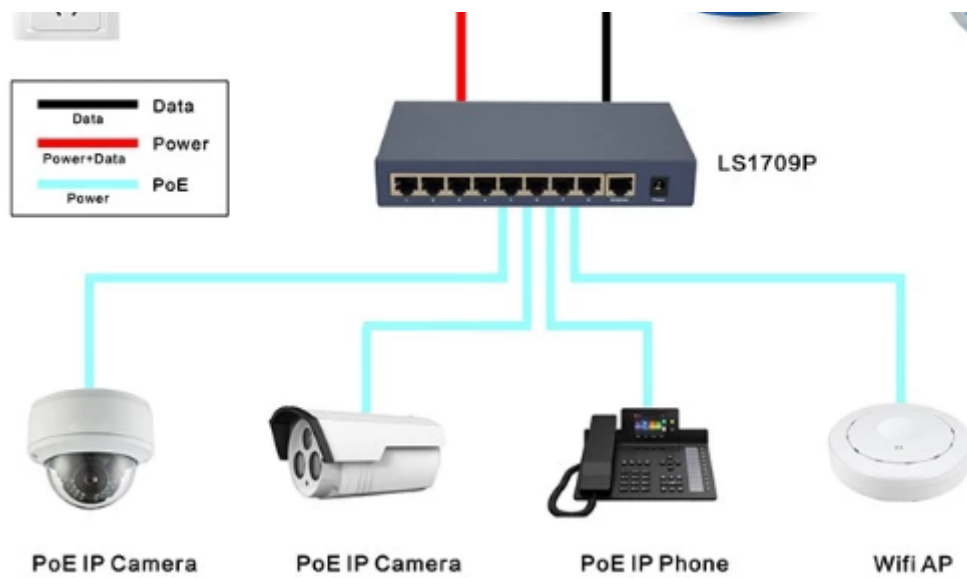
Respuesta: **Pues no**, si introduces el extremo suelto en el *master* del tester que envía la señal (inyecta voltios), te cargas esa "cosa" en el otro extremo. En resumen: si tienes que comprobar un cable, asegúrate que tenga los dos extremos desconectados.

PREGUNTA: ¿Qué conexión es mejor la conexión por cable o la conexión por Wifi?

Respuesta: La conexión cableada **siempre** nos va a dar más velocidad, fiabilidad y conexión segura frente a la wifi. La wifi la tenemos que dejar cuando no hay otro remedio (aula con tablets, carro de portátiles, etc...)

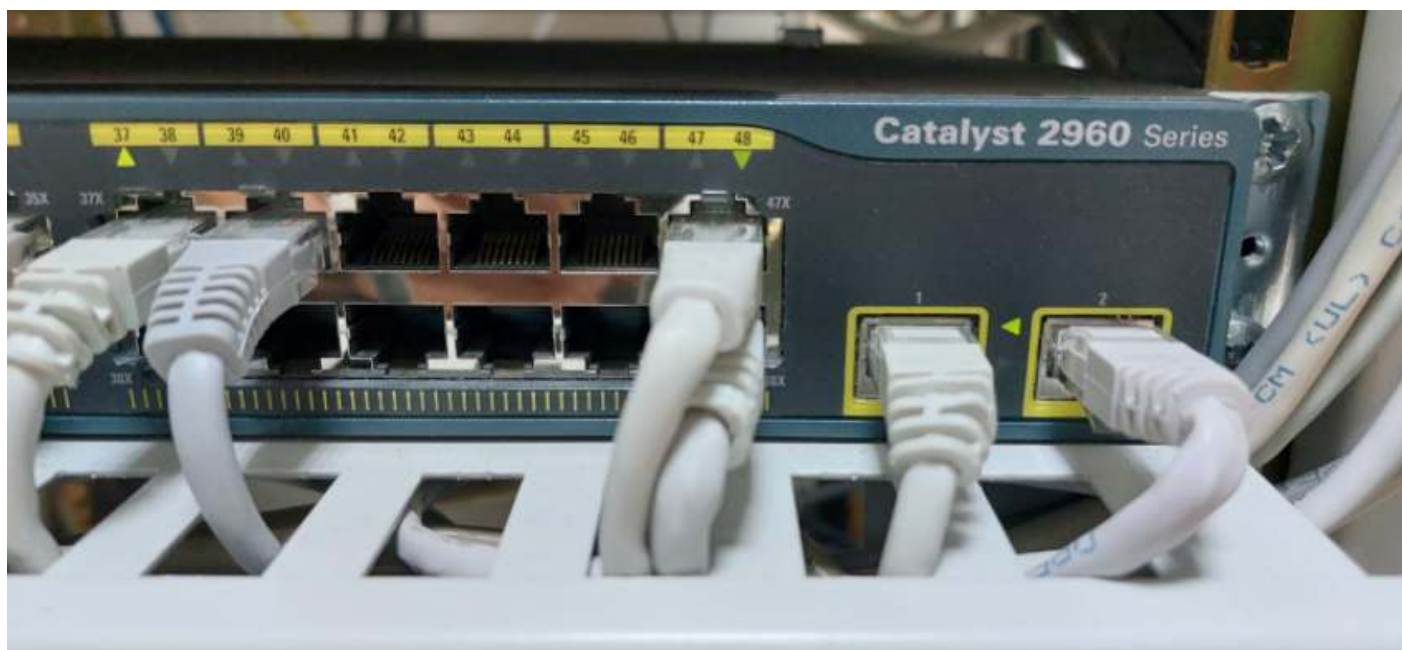
## POE

Los cables **POE** (Power Over Internet) son cables entrelazados pero están conectados a un **Switch PoE** que tiene puertos que además de transmitir los datos, transmiten también la alimentación, de tal manera que el dispositivo destino puede alimentarse con sólo llegar el cable entrelazado (es típico en teléfonos IPs, WebCams y APs)



*Fuente Ali-express*

En la siguiente figura puedes ver un switch que no es POE



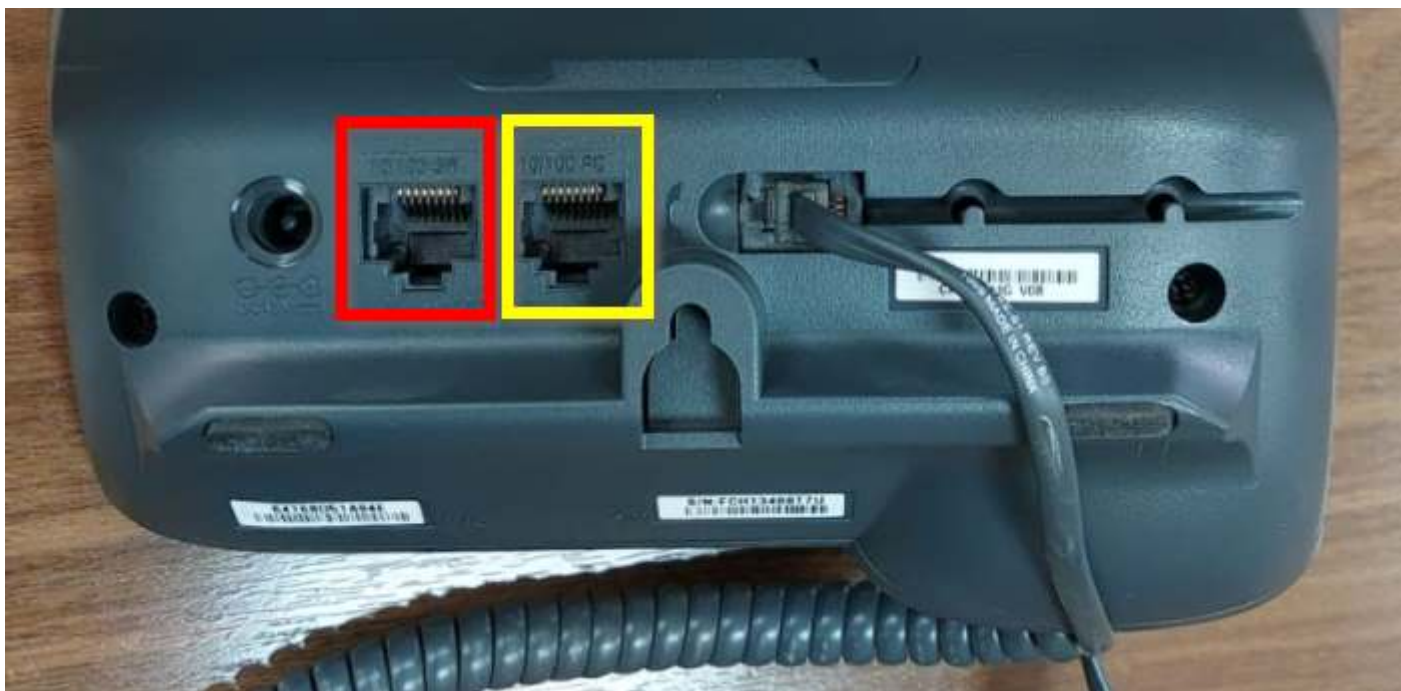
Y un switch que SI QUE ES POE



Esto nos facilita la instalación de dispositivos que necesitan datos y alimentación, pues sólo hay que llevar un cable entrelazado. Un ejemplo de dispositivo que necesita POE son los teléfonos IP (teléfonos que se van por la red de datos de Internet, no por la red voz tradicional)



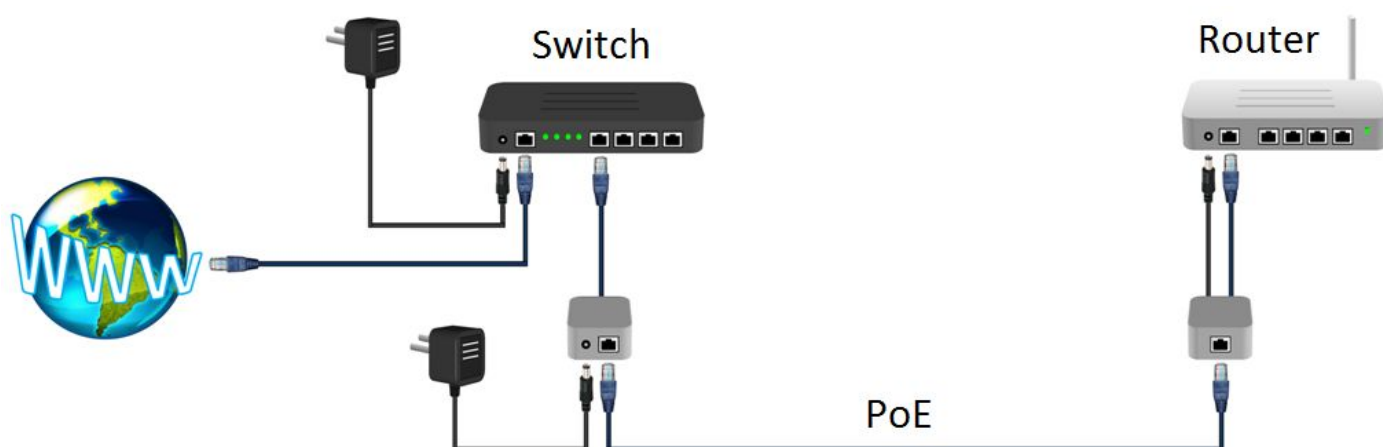
Si vemos su conexión, tiene bocas RJ45 de 8 hilos (los teléfonos tradicionales de voz son RJ11 de 4 pines), uno marcado en rojo que es la entrada, y necesita alimentación del teléfono (PoE) y otro marcado en amarillo que es salida de datos, que pone PC donde no es PoE y se puede conectar un ordenador. Vemos a la izquierda una boca redonda para tener la posibilidad de alimentarlo externamente sin necesidad de PoE.



En los centros que no tienen Switch con POE tienen estos dispositivos para crear un cable POE: (un mezclador data+power y un separador data+power marca D-Link)



Y el esquema era el siguiente, donde el Router blanco de la derecha es un ejemplo de dispositivo que por cuestiones físicas no se puede instalar hasta allí un cable de alimentación por que está en un lugar difícil, en el techo etc.. para tener un enchufe :



Fuente <https://www.instructables.com/>

Luego si en tu centro ves un AP con esta conexión es porque el cable que sale de la caja es POE:



Fuente Wikipedia

OJO fíjate que **NO SE CONECTA DIRECTAMENTE** sino a través del separador D-Link.

Hay dispositivos que en la conexión hembra RJ45 pone Data o NonPOE y otros que pone Data+Power o POE en la foto anterior el AP Punto de acceso es NonPOE por lo tanto necesita el separador, es fácil saber que es NonPOE pues tiene un conector de alimentación (cable negro de la foto) si fuese POE no lo tendría.

**¿Por qué tengo que saber esto?** Porque si conectas un cable POE a un dispositivo no POE **lo puedes estropear** pues estás conectando unos voltios a la tarjeta red que no está preparado.

Puedes hacer un desastre si conectas un portátil a un cable POE, o peor todavía: simplemente hacer de manitas en el Switch de conserjería e intercambias cables en los puertos del Switch, y no te das cuenta que unos son POE y otros NonPOE.

Luego ojo con este símbolo:



**POE**



Actualmente los switchs POE inteligentemente detectan si el dispositivo que has conectado necesita alimentación o no, luego en teoría no pasaría nada si conectas un dispositivo no PoE a un switch PoE, pero mejor no hagas esos experimentos.

# Fibra óptica

Es un cableado formado por filamentos transparentes donde viaja la luz por medio de rebotes entre las paredes. Al ser luz, se puede trabajar con frecuencias mucho mayores sin casi pérdidas por lo que aumenta la velocidad de transmisión. El problema es que las conexiones no son tan fáciles como en el RJ45.

De momento sólo se utiliza a nivel de WAN es decir de entrada en el router en las localidades donde llega la fibra óptica. En la LAN se trabaja con cable trenzado.

# Router

Conecta dos redes diferentes, nuestra LAN con la WAN (Wide Area Network) o sea, con Internet.

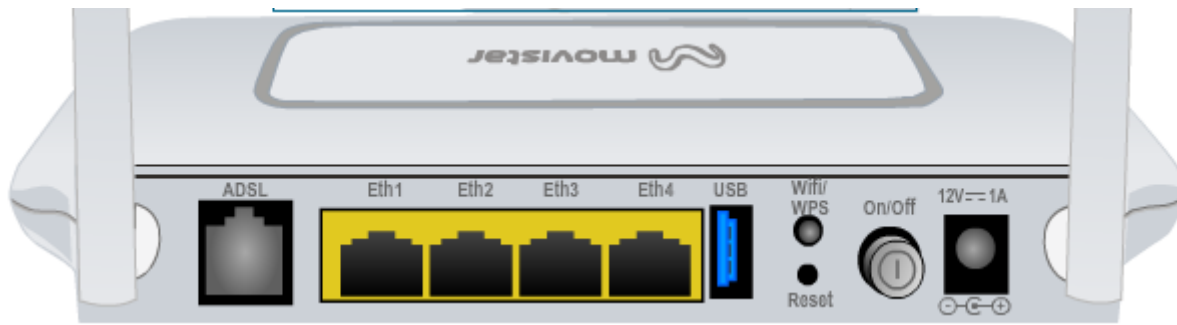
Puede ser con una línea telefónica ADSL o con fibra óptica y puede tener también ser punto de acceso Wifi como el router doméstico de la figura, es un router ADSL antiguo pero nos sirve para entender los conceptos.



Detrás del router tenemos que saber que tenemos:

- La conexión de la línea ADSL o de fibra óptica
- Un botón de **Reset** a veces sólo accesible con la ayuda de por ejemplo un clip, para resetearlo mantenemos pulsado con el clip el botón reset durante unos segundos hasta que veamos que el router se apaga sólo y se vuelve a encender.
- Las diferentes conexiones **Ethernet** para el cableado a los diferentes switches. (en amarillo)
- Un puerto USB para configuraciones técnicas
- Botón de encendido y apagado y la conexión a la alimentación, también válido para hacer un reset.





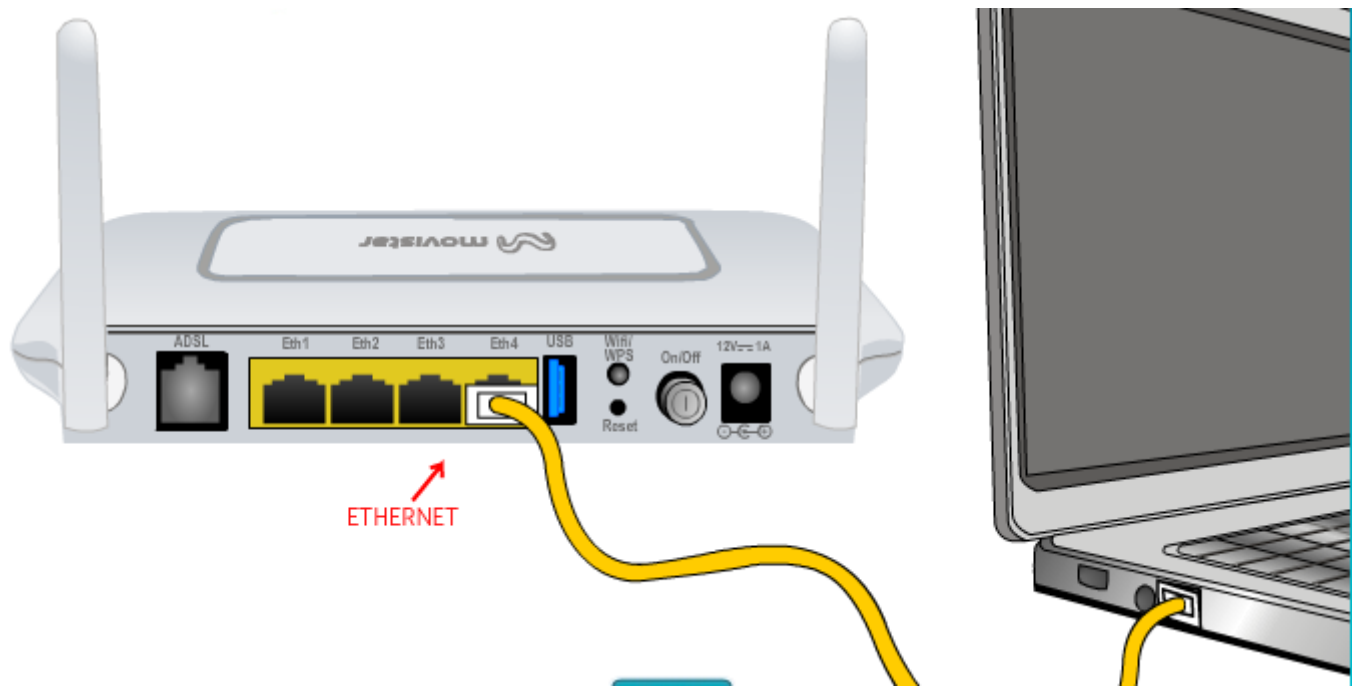
Es importante saber estos elementos y localizarlos para cualquier problema.

## PROBLEMA : Internet no va en mi centro.

El principal sospechoso sería el router, hay que comprobar si están encendidos todos los leds del router.



- si alguno está en **rojo** ya nos informa donde está el problema, por ejemplo si el led ADSL/Internet está en rojo, el problema está en nuestro proveedor (Movistar, Vodafone, Embou... ). **EN ESTE CASO, PRIMER PASO QUE SE PUEDE HACER ES RESETEAR EL ROUTER A VER SI VUELVE LA CONEXIÓN**
- Si están encendidos todos en **verde**, podemos conectar por ejemplo un portátil en uno de las conexiones Eth y comprobar si hay Internet.



- Si hay Internet: el problema no es el router sino el siguiente elemento de arriba de la cascada de nuestra red: El switch o el cableado entre el switch y el router.
- NO hay Internet: el fallo es el router. Podemos resetear el router a ver si vuelve la conexión.

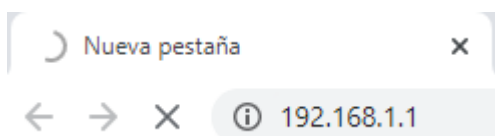
En el caso de que haciendo estas simples comprobaciones sigue sin funcionar, [llamamos al servicio CAU](#).

## El router es un mini-ordenador

Con un sistema operativo llamado **firmware** (software almacenado en los chips de un dispositivo) funcionando y accesible mediante una aplicación web.

**OJO : El acceso a la aplicación del router de tu centro educativo SOLO ES ACCESIBLE POR EL SERVICIO CAU.** No obstante, consideramos importante que, como COFOTAP, conozcas la existencia de la configuración del router por la importancia que tiene en la LAN de tu centro y por los conceptos implícitos en la configuración de tu red.

Para acceder a la aplicación hay que teclear [la IP puerta de enlace](#) en un navegador:



y **CADA MODELO DE ROUTER TIENE UNA APLICACION WEB DISTINTA** aquí por ejemplo vamos a enseñar capturas del modelo del router Movistar:



Para acceder se pide un usuario y contraseña

**Iniciar sesión** ? ✕

**Para configurar tu Home Station debes iniciar sesión.**



Contraseña de configuración

....|

✕ Cancelar    ▶ Aceptar

**info** Es curioso saber que el router es siempre ignorado como elemento crítico de seguridad, esto ha provocado muchos problemas. Una vez en una PYME de un amigo mio, se le infectaba cualquier PC que se conectaba en la red LAN de su pequeña oficina. Al final descubrí que el virus estaba en su router pues tenía de contraseña : 1234 ¿la conocerán los hackers rusos? fue cambiarla y actualizar el firmware y problema resuelto. ¿Y tú? ¿has cambiado la contraseña de tu router de tu casa y tienes actualizado su firmware o llevas la misma de fábrica? [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]

Entrar en la aplicación Web nos permite por ejemplo [cambiar la puerta de enlace](#), [las DNS](#) de tu red

Configurar Home Station

**Red inalámbrica (WiFi)**

Estado: **ACTIVADA**

Nombre: MOVISTAR\_8014 Visible

**Seguridad**

Nivel: Medio (WPA)

Clave: 00000000 Fortaleza de la clave: Buena

Buscar canal: Automáticamente

Ir a filtrado MAC

**LAN (Dirección de mi Home Station)**

IP: 192.168.1.1

Máscara: 255.255.255.0

**Configuración DHCP (Asignación automática de direcciones IP)**

Estado: **ACTIVADO**

Inicio: 192.168.1.33

Fin: 192.168.1.254

**Servidores DNS (Te recomendamos no modificar)**

Servidor DNS 1: 80.58.61.250

Servidor DNS 2: 80.58.61.254

O cambiar el nombre de la red wifi y su contraseña si es un router con wifi.

**Red inalámbrica (WiFi)**

Estado: **ACTIVADA**

Nombre: MOVISTAR\_8014 Visible

**Seguridad**

Nivel: Medio (WPA)

Clave: 00000000 Fortaleza de la clave: Buena

Buscar canal: Automáticamente

Ir a filtrado MAC

Es importante cambiar la **SSID** o nombre de red y su **contraseña**, y la encriptación que sea **WPA2-PSK (TKIP)** ver [Wifi](#)

**info** Existen muchas aplicaciones para piratear Wifis que simplemente tienen los valores por defecto de los routers inalámbricos. El servicio CAU de tu centro ya ha tenido esta precaución ¿y tú? ¿en tu casa? ¿tienes el mismo nombre de red y contraseña Wifi en tu router que cuando lo compraste? [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]

Antiguamente para actualizar el Firmware hay que descargarlo de la web del fabricante y luego en la aplicación web del router entrar en opciones avanzadas:

## Otras opciones avanzadas

Configuración sin NAT (monopuesto)

Crear perfil o recuperar uno guardado

Copia de seguridad o Restaurar Configuración por PC

Actualización de firmware



Configuración Red IPv6

 Cancelar

 Aceptar

Y seleccionar el fichero, teniendo en cuenta que mientras estamos actualizando el Firmware no se podía desconectar el router pues si se apaga, se inutiliza de forma permanente el router.

Actualización de Firmware



Esta opción te permite actualizar el firmware de tu Home Station ADSL. Es una operación delicada por lo que se te recomienda seguir cuidadosamente las instrucciones.

La versión actual del firmware de tu Home Station ADSL es: BHS\_RTA\_ES\_034

Asegúrate de que tienes una versión de firmware homologado por Movistar. Puedes comprobar las versiones más recientes disponibles en la web de Movistar. Si ya te has descargado una versión más reciente, por favor localiza el archivo en tu PC y pulsa Actualizar Firmware para instalar.

Seleccionar archivo

No...o

☐ Volver a configuración por defecto

RECUERDA no apagar tu Home Station ADSL ni desconectar el cable de conexión telefónica mientras el proceso de actualización está en curso. Es MUY IMPORTANTE no interrumpir esta proceso ya que podría inutilizar tu Home Station ADSL.

Actualizar Firmware

Esto lo decimos como curiosidad pero lo comentamos aquí pues aún es común esta forma de actualizar firmwares en algunos dispositivos electrónicos

Hoy en día los routers modernos se actualizan en remoto, pero no dejan de ser unos ordenadores, luego es bueno **reiniciarlos** de vez en cuando.

En esta aplicación web también se pueden **abrir puertos** PERO ESTO ES UNA PUERTA ABIERTA AL EXTERIOR con el consecuente peligro de seguridad. En la figura se puede ver que se ha abierto al equipo con la IP 192.168.1.33 diferentes puertos seguramente para descargas punto a punto P2P tipo Torrent, eMule y similares.

Configurar aplicaciones y puertos

Lista de aplicaciones

PRUEBA

PRUEBA\_1

Reglas que se aplican

+ Añadir regla

Abrir	el puerto	número	1976	protocolo	UDP	−		
Abrir	el puerto	número	13	protocolo	TCP	−		
Abrir	los puertos	desde	3000	hasta	3500	protocolo	TCP y UDP	−
Abrir	el puerto	número	112	protocolo	TCP y UDP	−		
Abrir	los puertos	desde	4321	hasta	4333	protocolo	TCP y UDP	−

Para el dispositivo 192.168.1.33

+ −

Cancelar Guardar cambios

# PARA SABER MÁS

Te recomendamos el artículo ++[Tu router, tu castillo. Medidas básicas para su protección de OSI](#)

# Protocolos

Digamos que son las reglas del lenguaje de los paquetes de información, hay muchos protocolos, los comunes son:

- **HTTP** es el protocolo de las páginas Web, [se inventó en el CERN](#) para publicar información entre científicos.
- **HTTPS** es el mismo que en anterior pero añadiendo una seguridad de su origen. **Nunca tenemos que navegar en una página web importante por ejemplo un banco o tienda virtual que no sea en su inicio HTTPS** (o el símbolo del candado en el navegador) de lo contrario es una página web falsa o fishing que nos quiere robar las contraseñas.
- **FTP** es el protocolo para la transferencia de ficheros.
- **SMTP POP3** el de los correos electrónicos.

## TCP/IP

Todos estos protocolos utilizan paquetes de información, pero estos a su vez utilizan el protocolo **TCP/IP** digamos que es *el protocolo de Internet*.

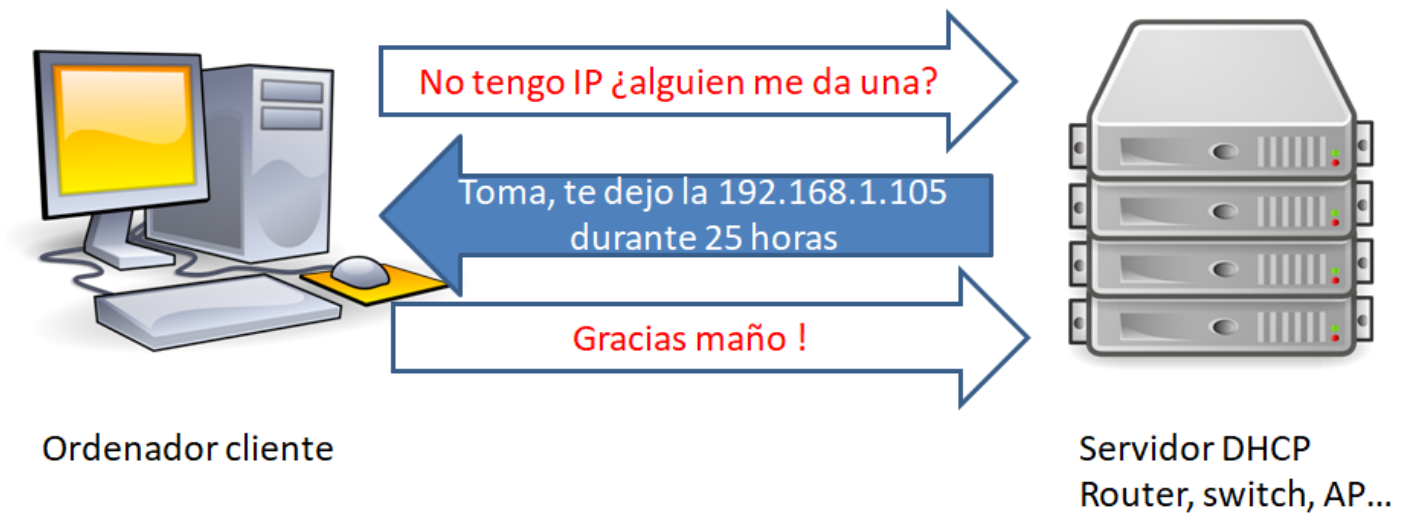
- **TCP** (transmission control protocol) se encarga de asegurar que el paquete tenga su contenido correcto.
- **IP** (Internet protocol) es la dirección del equipo destino. **Todos** los equipos conectados a Internet tienen un número.

Cuando se inventó este protocolo fue cuando realmente se inventó Internet pues posibilitaba la interconexión entre ordenadores de forma masiva y con libertad ¿sabías que tiene su origen [en la guerra fría](#)?

## DHCP

DHCP, Dynamic Host Configuration Protocol se inventó para simplificar las asignaciones de IPs a los equipos para hacerlo automático, básicamente es una conversación entre el ordenador que quiere conectarse a Internet y el servidor, esta figura sería el esquema dentro de tu LAN:





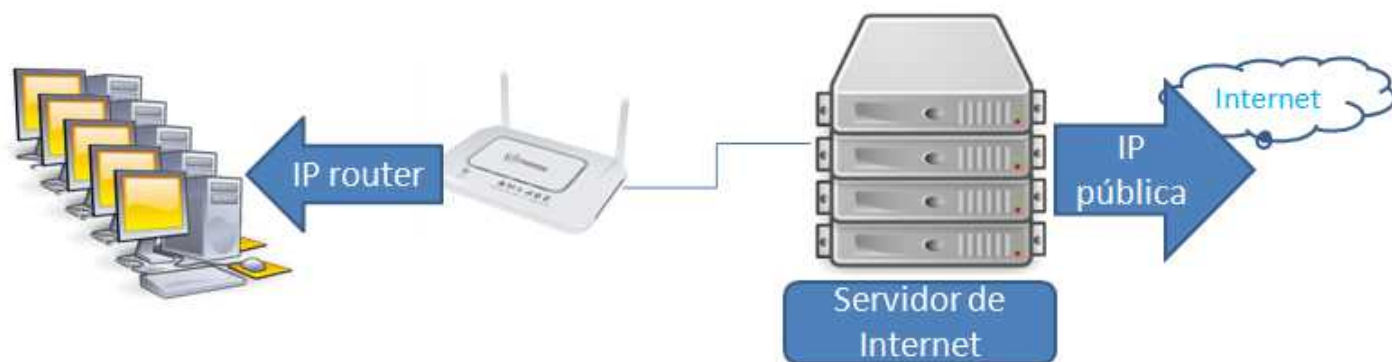
La pregunta del ordenador cliente "No tengo IP ¿alguien me da una?" la lanza a una IP especial llamada **Broadcast** que son todo unos al final y que lo leen todos los de su LAN.

# La IP pública

También ocurre esto entre tu router y el servidor de tu proveedor de telefonía de Internet, luego tenemos:

- La IP que muestra nuestro router a nuestra LAN que la podemos definir nosotros, es fija, llamada **puerta de enlace**
- Una IP del router al servidor de Internet que la define el servidor de Internet por su propio protocolo DHCP, al ser una IP temporal, entonces se llama **IP dinámica**..
- La que navega el servidor de Internet y la que ve el mundo. Es la **IP Pública** y esta geolocalizada. ¿Cual es? Pues por ejemplo lo puedes averiguar en <https://ipleak.net>
- Esta información **es pública** aunque navegues de incógnito esta información se utiliza por ejemplo cuando visitas una página web, los anuncios te personalizan su contenido.
- Como puedes ver **todo lo que hacemos en Internet deja un rastro** .

Investiga: Entra en <https://ipleak.net> cuando estés por el ámbito rural (aunque sea con tu móvil) verás que no coincide con tu situación real. Yo por ejemplo estoy ahora en Calamocha y me dice que navego con 188.244.80.254 de Zaragoza. Esto es debido a que mi servidor de Internet está en los servidores de AST de Pignatelli y tienen esa IP.



INVESTIGA UN POCO: Entra en dos equipos diferentes de tu centro (o de tu casa, por ejemplo un ordenador y el móvil pero ojo, el móvil conectado a la misma LAN que el ordenador (o sea por Wifi no con datos móviles)) y a la vez a la página [ipleak.net](http://ipleak.net) en los dos equipos ¿cómo es posible que están navegando con la misma IP? Respuesta: Esto es debido a que las IPs de tu LAN son reservadas y navegan con la misma IP pública que es el mismo servidor de Internet

## La IP del router, puerta de enlace, acceso o Gateway

Esta IP privada del router hacia nuestra LAN es la IP que todos los equipos de nuestro centro tienen que saber para poder navegar, pues necesitan saber quién es el que les va a proveer el servicio de Internet. Esta IP especial se llama **IP DE LA PUERTA DE ENLACE** o también **GATEWAY**, suele ser en tu centro la 172.168.1.1.

## ¿Cómo se configura el DHCP ?

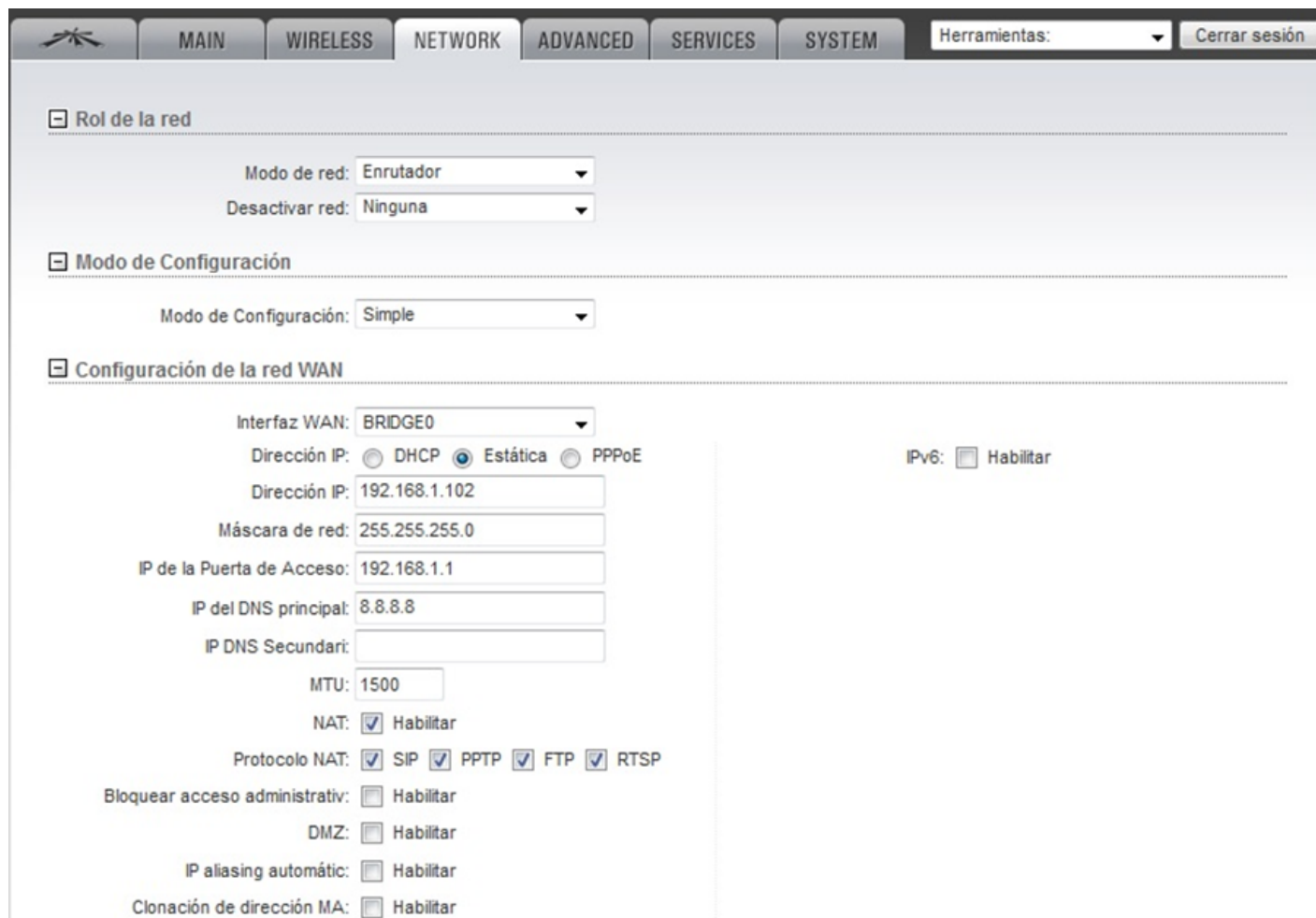
Vamos a poner el ejemplo de configurar el DHCP de un AP Ubiquiti.

También podría ser el del router, los conceptos son los mismos pero las pantallas y lugar del menú cambian y depende de las marcas, esto **NO es un tutorial** sino un curso para que entiendas los conceptos.

Esta configuración, igual que lo explicado en el router está reservada al servicio técnico, se muestra aquí para comprender los conceptos.

Entramos en su aplicación web, supongamos que en el AP Ubiquiti es la <http://192.168.1.102> y después de logearnos, en Network la dirección IP del AP, su máscara de red, la dirección Gateway.

Si quisieramos que el router le asigne dinámicamente una IP marcaríamos DHCP, pero es mejor que sea estática para poder localizar este AP Ubiquiti.



The screenshot shows the Ubiquiti EdgeRouter configuration interface. The top navigation bar includes tabs for MAIN, WIRELESS, NETWORK, ADVANCED, SERVICES, and SYSTEM. The 'NETWORK' tab is selected. The interface is divided into sections: 'Rol de la red' (Network Role) with 'Modo de red' set to 'Enrutador' and 'Desactivar red' set to 'Ninguna'; 'Modo de Configuración' (Configuration Mode) with 'Modo de Configuración' set to 'Simple'; and 'Configuración de la red WAN' (WAN Network Configuration). Under 'Configuración de la red WAN', the 'Interfaz WAN' is set to 'BRIDGE0'. The 'Dirección IP' is set to 'Estática' (Static) with a value of '192.168.1.102'. The 'Máscara de red' is '255.255.255.0', the 'IP de la Puerta de Acceso' is '192.168.1.1', the 'IP del DNS principal' is '8.8.8.8', and the 'IP DNS Secundari' is empty. The 'MTU' is set to '1500'. The 'NAT' section has 'Habilitar' checked. The 'Protocolo NAT' section has 'SIP', 'PPTP', 'FTP', and 'RTSP' all checked. The 'Bloquear acceso administrativ', 'DMZ', 'IP aliasing automátic', and 'Clonación de dirección MA' sections all have 'Habilitar' unchecked.

¿Pero no íbamos a configurar la DHCP y ahora dices que es mejor dejarla estática? Ojo no te confundas esa es la IP del AP Ubiquiti, lo que queremos es que ese AP Ubiquiti asigne automáticamente IP a nuestros equipos de la LAN:



En configuración de la LAN es donde activaremos el DHCP

## Configuración de la red LAN

Interfaz LAN: WLAN0

Dirección IP: 169.254.190.1

Máscara de red: 255.255.255.0

MTU: 1500

Servidor DHCP: ☐ Desactivado ☒ Habilitar ☐ Relé

Rango inicial: 169.254.190.2

Rango final: 169.254.190.254

Máscara de red: 255.255.255.0

Tiempo de concesión: 172800

Proxy DNS: ☒ Habilitar

UPnP: ☐ Habilitar

IPv6: ☐ Habilitar

## DHCP Address Reservation

Habilitar	Interfaz	Dirección MAC	Dirección IP	Comentario	Acción
<input checked="" type="checkbox"/>	WLAN0	F0:F0:F0:F0:F0:F0	169.254.190.150	IMPRESORA	<input type="button" value="Editar"/> <input type="button" value="Eliminar"/>
	WLAN0				<input type="button" value="Agregar"/>

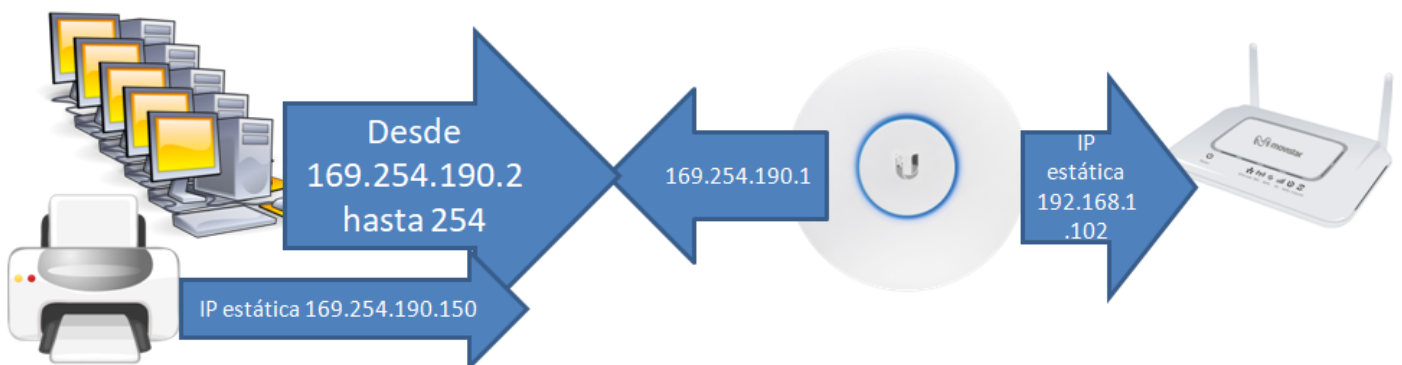
## Redirigir de puerto

## Configuración de Enrutamiento Multicast

Como vemos en la figura se ha activado el DHCP y proporcionará a los equipos IPs desde la 169.254.190.2 hasta la 169.254.190.254 durante 172.800 segundos. También vemos que hay una excepción para la impresora que le dará una IP fija y así la tenemos localizada para poderla instalar en los equipos.

OJO para que el DHCP funcione, en cada equipo tiene que estar configurado la opción DHCP, esto lo veremos en el [siguiente capítulo](#).

Gráficamente la configuración quedaría así:



# IPs

Está formado por 4 números cada uno de ellos puede ser desde 0 hasta 255 y el ordenador lo traduce en una secuencia de 8bits

Por ejemplo la IP `192.168.1.55` es realmente `1100000 10101000 00000001 00110111`

**NO PUEDE HABER EN EL MUNDO DOS EQUIPOS QUE NAVEGUEN CON LA MISMA IP.** Esto provoca que ya quedan pocos IP4 disponibles, por eso se creó el [IPv6](#).

La afirmación anterior no entra en contradicción con lo explicado de las IP Públicas en [Protocolos](#), pues dos equipos de tu LAN pueden navegar con la misma IP Pública pues quien navega realmente es el servidor que te proporciona Internet, luego él distribuye esos paquetes de información a quienes se lo han solicitado gracias a las IP reservadas.

## IPv4 reservadas

Dentro de la LAN de tu centro se asignan a cada equipo, son IP reservadas, cada una es única **dentro de tu LAN** pero esta información llega al router y al servidor de Internet y cambia esa IP por la suya **la IP pública** que es única en la WAN de Internet, o sea que la IP del ordenador del centro que es IP reservada *no viaja como cabecera por Internet*.

Luego el router ya se encarga de distribuir los paquetes a cada equipo de la LAN pues realmente la IP del equipo se sigue conservando dentro del paquete de información.

En resumen que un ordenador del centro puede tener la 192.168.1.55 y en *otro centro educativo* puede tener la 192.168.1.55 en otro equipo. Pero no puede haber dos ordenadores de tu centro con la IP 192.168.1.55.

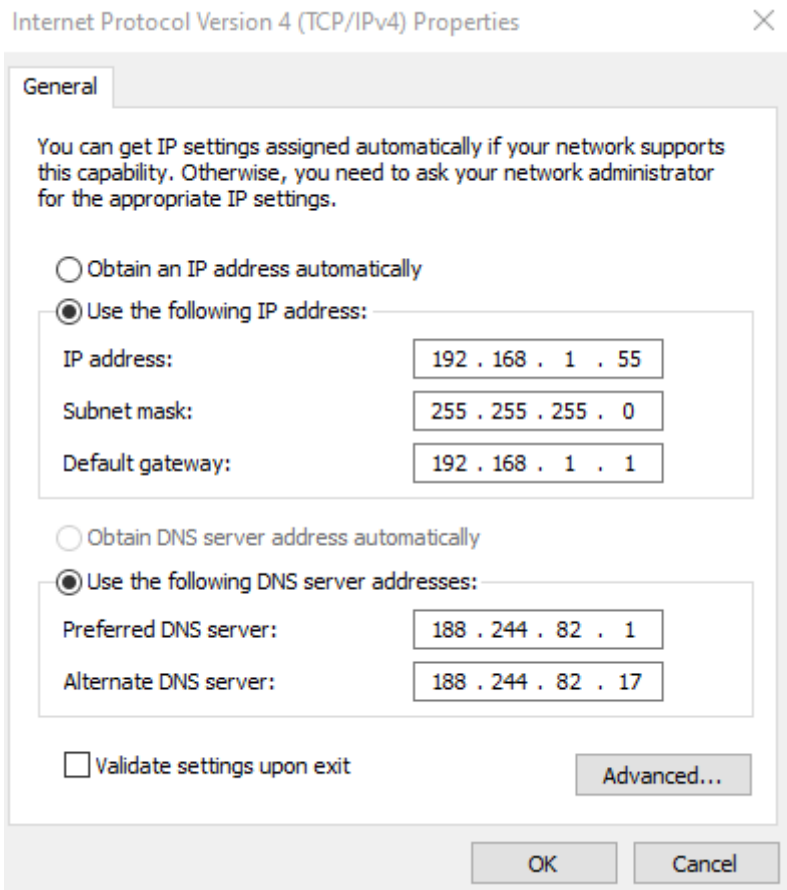
**Conclusión:** Las 192.168.x.x donde x son números entre 0 y 255 están reservadas para uso privado interno dentro de las LAN. También las 172.16.x.x hasta la 172.31.x.x, y otras más...

La 127.0.0.1 es una dirección especial que se usa para referirse a uno mismo y las que tienen todos unos: 255 también es especial que es para referirse a todos (Broadcast).



# CONFIGURAR LA IPv4

Nos vamos a **Inicio - Panel de control - Conexiones de red e Internet - Conexiones de red** y aparecen nuestras conexiones, fija, inalámbrica. Nos vamos a la que queremos configurar con el **botón derecho - Propiedades - Protocolo TCP/IPv4**



Aquí tenemos varias opciones que tienes que ver detenidamente:

## IP AUTOMÁTICA

Podemos hacer que el router, switchs , o los AP asignen automáticamente una IP al equipo. Esto es posible si en la configuración del AP, switch o router se ha activado la **DHCP** ya lo hemos visto en el [anterior capítulo](#)

## IP ESTÁTICA - DIRECCIÓN IP

En muchos centros interesa que los equipos estén localizados, esto suele pasar en equipos fijos e impresoras.

- Hay que tener cuidado con no poner una IP de otro equipo.
- Las tienen que ser de las reservadas pues estamos hablando de tu LAN local no de la WAN (o sea la externa, Internet).

Si por error hemos configurado manualmente una IP estática al rango DHCP de un router, AP... puede ocurrir que dicha dirección sea asignada dinámicamente a otro PC, provocándose un **conflicto de IP**.



# IP ESTÁTICA - MÁSCARA DE RED

La máscara de red es un número de unos y ceros y en la frontera es lo que corta en la dirección IP que parte es lo común en toda la LAN de tu centro y qué parte es exclusiva a cada equipo.

## IP estática - Máscara de red - Tipo C (la más común)

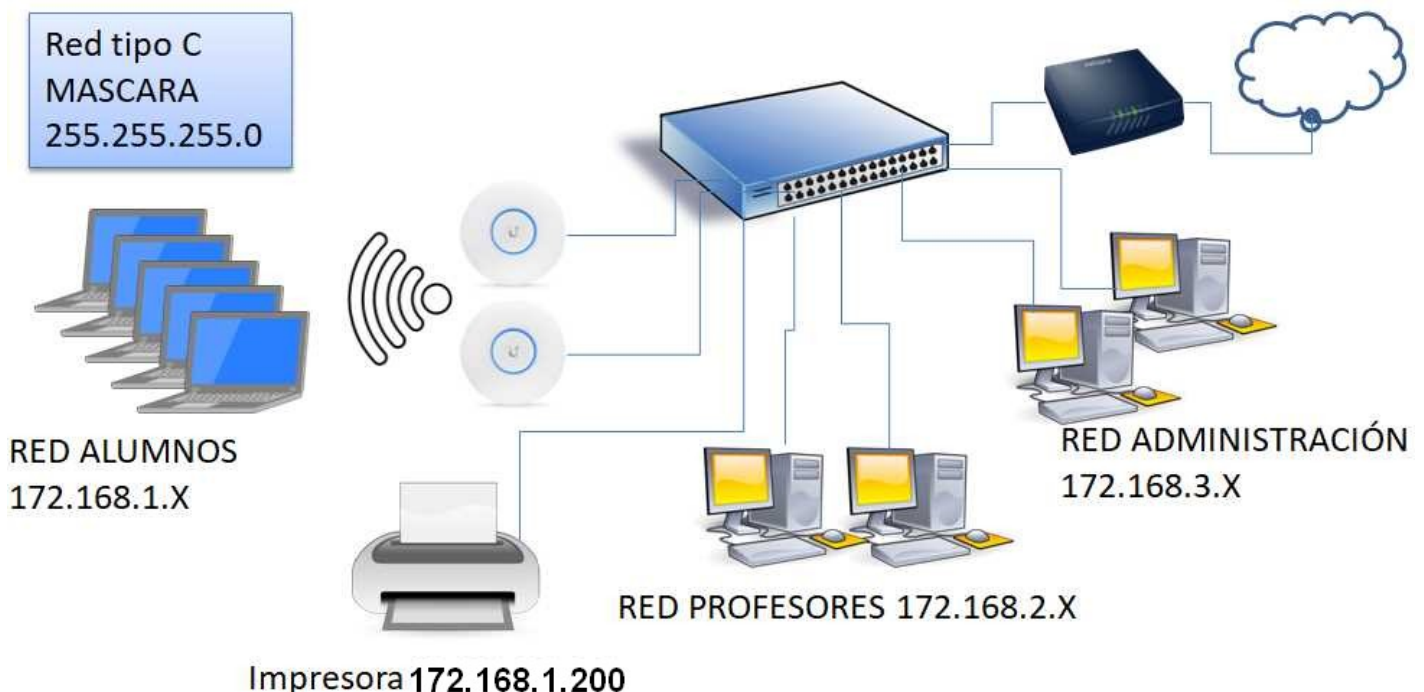
Esto se ve mejor en un ejemplo, supongamos que tenemos una IP en el **ordenador ALUMNO 172.168.1.23** y una MÁSCARA DE RED: **255.255.255.0** o sea en binario 11111111 . 11111111 . 11111111 . 00000000 eso quiere decir que la parte común de toda la LAN de tu centro es 172.168.1 y el número 23 es propio de ese equipo.

O sea que las de esa subred de ese centro van desde la 172.168.1.0 hasta la 172.168.1.254 en total puedes tener 255 equipos.

Nota: no se puede utilizar la 172.168.1.255 pues es la dirección especial *Broadcast*.

Si a otro equipo, por ejemplo **ordenador PROFESOR IP 172.168.2.15** entonces pertenece a otra LAN es decir **no se pueden ver entre ellos PROFESOR-ALUMNO**. Y a otro equipo **JEFATURA IP 172.168.3.6** tampoco se verán entre ellos ALUMNO-PROFESOR-JEFATURA. Es lo que se llama crear subredes **VLAN**.

Un ejemplo de arquitectura de red sería la siguiente



Podrías pensar que algún alumno *listo* simplemente cambiando la IP a por ejemplo 172.168.3.24 podría acceder a jefatura 172.168.3.6, pero si el switch que le tiene que dar acceso (los Ubiquitis en el caso de la figura anterior) pertenecen a la red 172.168.1.x no

puede, ese ordenador hacker se queda aislado, ni siquiera podría navegar.

Pero si es *muy listo* [ ] [ ] [ ] puede coger un cable de red RJ45 y conectarse a la red cableada, luego **SI QUE PUEDE**. Luego: los ordenadores de profesores y administración que no compartan nada sin contraseña (eso lo permite Windows, si tuvieran Linux [ ] no habría ese problema).

## IP estática - Máscara de red - Tipo B

Pero si en tu centro quieres una VLAN más amplia puedes utilizar la máscara 255.255.0.0 por lo tanto el rango de esa red para los ordenadores sería desde la 172.168.1.1 hasta 172.168.255.254 (la 172.168.255.255 sería la de *Broadcast*) o sea que pueden haber hasta 2 elevado a 16 o sea 65.536 dispositivos en esa VLAN.

## IP estática - Máscara de red - Otros tipos

Como te puedes imaginar existe la Tipo A con máscara 255.0.0.0 para un número de dispositivos de 2 elevado a 24.

Las máscaras de red no tienen por que ser de las descritas por ejemplo una máscara 255.255.248.0 sería en binario 11111111 . 11111111 . 1111000 . 00000000 lo que permite 2 elevado a 11 equipos en la VLAN (tantos como 0) o sea 2.048 equipos.

# IP ESTÁTICA - PUERTA DE ENLACE o GATEWAY

Es la IP del router, es decir, el equipo tiene que saber qué equipo de su LAN es el que le da acceso a la WAN exterior, o sea Internet. Normalmente suele ser 172.168.1.1 ver [Router](#)

# Registra tus IPs

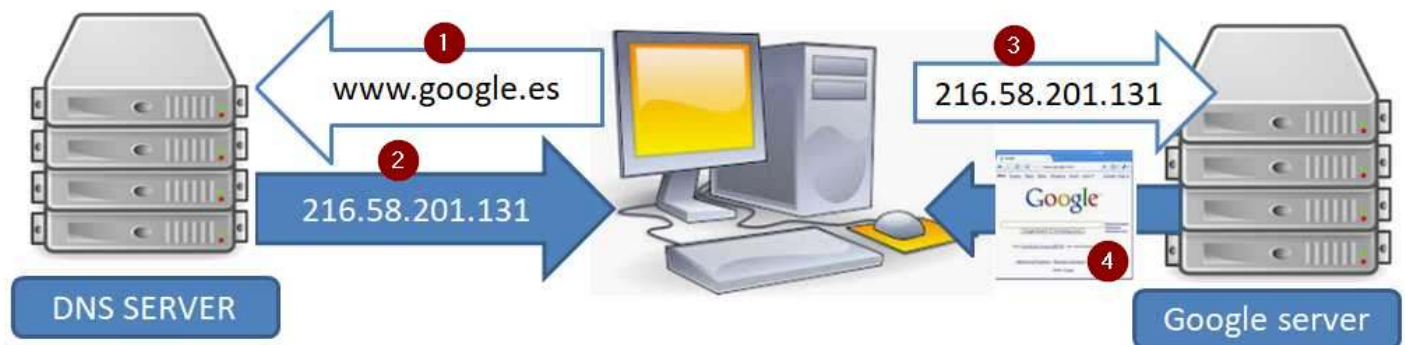
Como responsable de los medios informáticos es **importante** que registres qué IP tiene cada equipo de tu centro (o rangos, por ejemplo de las 172.30.7.1 a 50 es la aula de informática) no lo hagas en papel pues suele ser información muy "viva".

*Pfff eso es mucho curro...* bueno pues asegúrate que **TODOS** los chismes de tu centro están encendidos y ejecuta [Ábreles Network Watcher](#) y en View-HTML Report el resultado de la

tabla la seleccionas y la copias y pegas en una hoja de cálculo. Faena hecha !!

# DNS

Es la IP del servidor que nos proporciona los nombres de dominio, es decir, yo cuando pongo `www.google.es` en el navegador, mi ordenador va a pedir la página web al servidor de Google ¿pero dónde está? ¿Cuál es su dirección IP? Para ello está el servidor , se lo pregunta antes a él:



## ¿Vale pues cualquier dirección de un servidor DNS ?

Sí, puedes poner **cualquier dirección de servidor DNS válida** para que puedas navegar en Internet, por ejemplo los de Google ¿Por qué a Google le interesa proporcionar un servidor donde sabría todas las páginas web que navegamos???

Algunos servidores de DNS tienen filtrado de páginas *no deseadas*. [Ver lista de servidores DNS públicos](#)

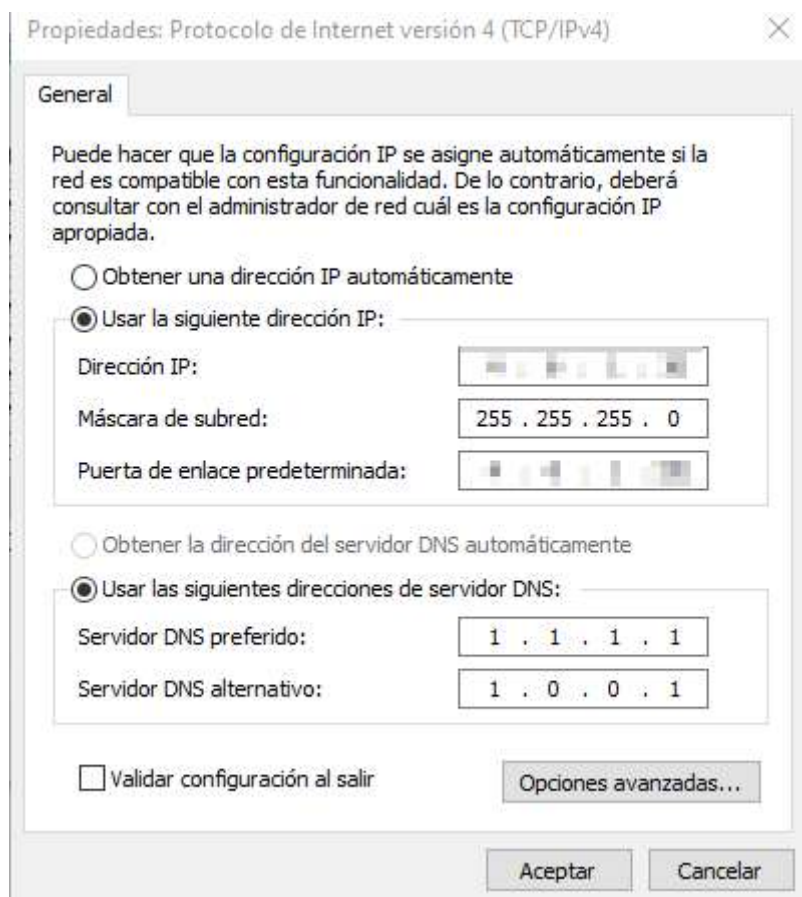
Nombre del servidor	DNS Primario	DNS Secundario	Filtrado
Cloudflare	1.1.1.1	1.0.0.1	
Cloudflare	1.1.1.2	1.0.0.2	Malware
Cloudflare	1.1.1.3	1.0.0.3	Adultos
Google	8.8.8.8	8.8.4.4	
Movistar	80.58.61.250	80.58.61.254	
OpenNIC	58.6.115.42	58.6.115.43	

Te aconsejamos los de Cloudflare pincha [aquí](#) por qué.

**Curiosidad:** En los centros como Servicios Provinciales, Departamento .. que están conectados a la **RACI** (Red Aragonesa de Comunicaciones Institucionales) tienen que tener de DNS los de los servidores de **AST** (Aragonesa de Servicios Telemáticos: 188.244.82.1 y 188.244.82.17 que están físicamente en **WALQA** (en las afueras de Huesca).

Anda, Google facilita de forma gratuita un servidor DNS ¡¡ Qué majos !! ¡¡ Qué altruistas !!! no creo que intenten conseguir información de todas las páginas web que se navegan [ ] [ ] [ ] [ ] [ ] [ ]

luego tiene que quedar así



### **NO LO TENGO ASÍ EN MI CENTRO EDUCATIVO !!! [ ] ESTA PUESTO DNS AUTOMÁTICO**

No pasa nada, el protocolo DHCP hace que tu router le asigne un DNS. Si las direcciones DNS del router están bien configurados, funcionará perfectamente.

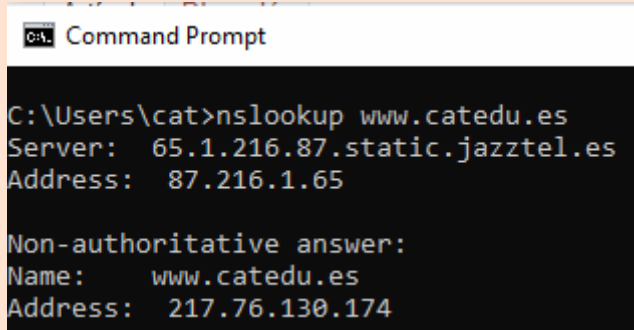
Si el router lo gestiona desde el Servicio Provincial lo habrán hecho correctamente

Si es un router casero (de telefónica o lo que sea) no se configura automáticamente, habría que comprobarlo.

Si tecleas en la [ventana de comandos nslookup](#) puedes ver el nombre de su servidor, como lo he hecho desde un centro RACI me sale el servidor del Gobierno de Aragón :

```
C:\Users\CATEDU>nslookup
Default Server:  codos.aragon.es
Address:  188.244.82.1
```

EXPERIMENTA ¿Qué dirección me proporciona mi servidor para una página concreta? por ejemplo [www.catedu.es](http://www.catedu.es) Respuesta: Teclea **nslookup www.catedu.es** y te saldrá una cosa así:



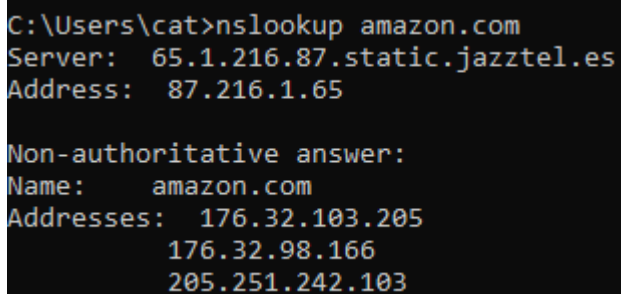
```
CA. Command Prompt

C:\Users\cat>nslookup www.catedu.es
Server:  65.1.216.87.static.jazztel.es
Address:  87.216.1.65

Non-authoritative answer:
Name:     www.catedu.es
Address:  217.76.130.174
```

Donde las primeras dos direcciones son las de tu servidor (en el caso de la figura es un servidor de Embou con IP 87.216.1.65 pues lo he hecho en casa) y las otras dos son las de CATEDU, o sea que su IP es 217.76.130.174.

Según la página que busques, pueden salir varias IPs pues puede tener esa web varios servidores replicados con diferentes IPs:



```
C:\Users\cat>nslookup amazon.com
Server:  65.1.216.87.static.jazztel.es
Address:  87.216.1.65

Non-authoritative answer:
Name:     amazon.com
Addresses: 176.32.103.205
           176.32.98.166
           205.251.242.103
```

# Wifi

Es un elemento importante en la red de tu centro, luego es bueno que veamos algunas cosas

## ¿Los APs no hay que reiniciarlos?

FALSO **Es bueno reiniciar los APs de vez en cuando** pues para que el WiFi vuelva a asignar otro canal de emisión a los dispositivos conectados, pues puede ocurrir que haya saturación en los canales de emisión. Con el reinicio, el router buscará un canal "menos ocupado", y aumentará el ancho de banda disponible para nuestros dispositivos conectados de forma inalámbrica.

## ¿Los APs antiguos no son un problema?

FALSO **Ojo con las AP antiguas** si tienes un AP antiguo (norma 802.11b) **te baja la velocidad de toda la red** que está con norma "n" o "ac". Los AP antiguos con contraseña de protocolo de seguridad antiguos WEP eran muy fáciles de piratear. Actualmente con **WPA2-PSK** no es nada fácil.



## No me tengo que preocupar de los canales



FALSO si por ejemplo la casa de enfrente tiene un canal de emisión próximo al tuyo genera interferencias, y si encima el vecino tiene una antigua, ralentiza la tuya

## ¿Qué es eso de los canales?

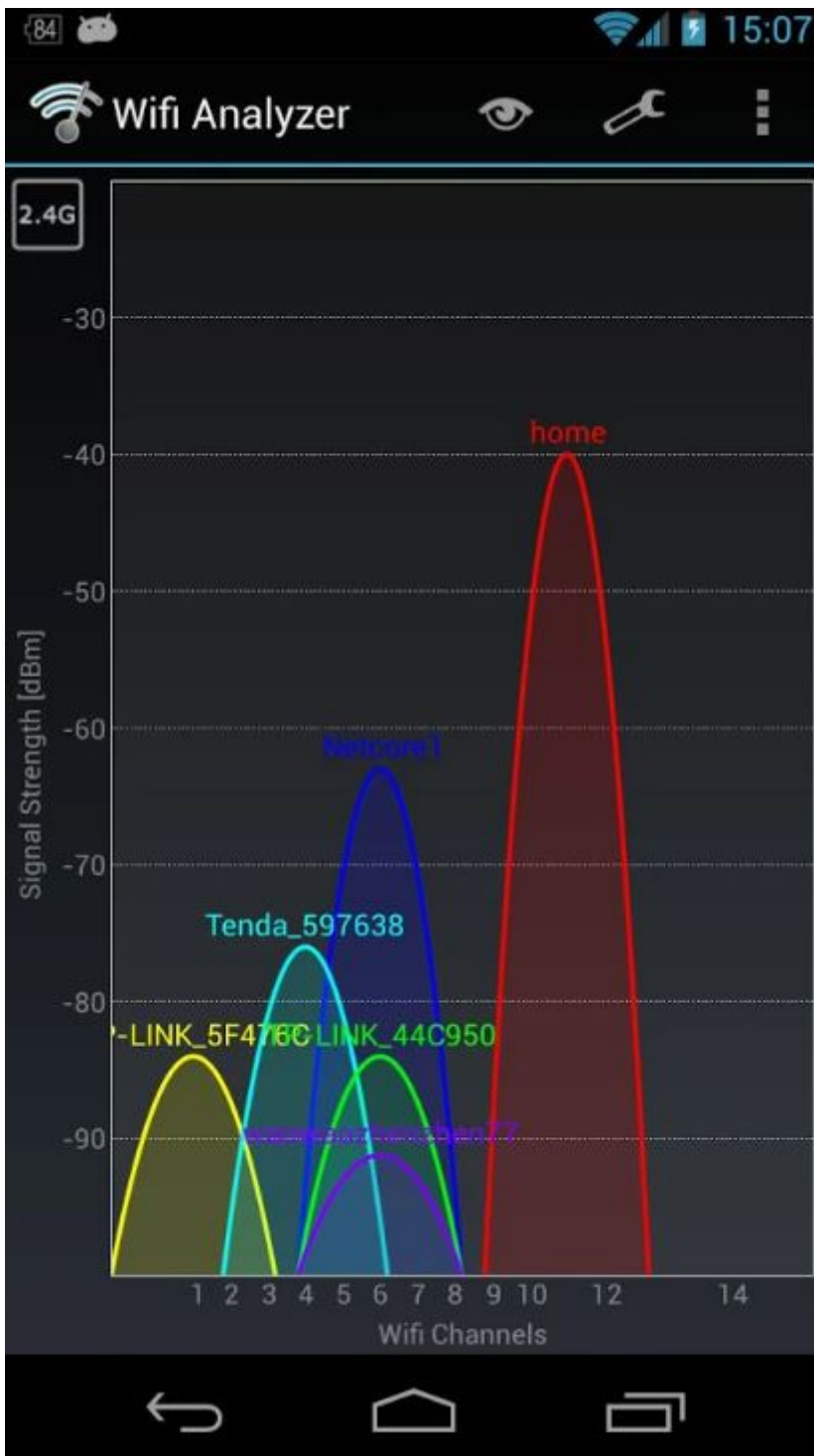
Hay dos bandas: 2.4Ghz y 5Ghz más moderna. Estas bandas se dividen en varios canales:

- La banda 2.4Ghz se divide en 13 canales pero te recomendamos la 1,6 y 11 pues no se solapan.
- La banda 5Ghz se divide en más canales y no están tan saturadas. Tiene muy buena velocidad de conexión pero no llega a largas distancias como la 2.4GHz

Tu AP utiliza un canal para conectarte con los dispositivos. En teoría el modo Auto selecciona el canal menos ocupado pero puede ser que un canal adyacente esté muy ocupado y haga ruido

## ¿Cómo puedo saber los canales?

Utiliza la APP en el móvil [Analizer](#) por la mañana cuando veas que tu centro tiene muchos equipos conectados, te puede dar una idea de los canales próximos y ocupados



## No hay buena cobertura

- Aleja el AP de microondas, teléfonos inalámbricos, peceras, espejos, plantas, estanterías metálicas cerradas, armarios metálicos y paredes gruesas.
- Utiliza la banda 2.4Ghz
- Una solución son repetidores . Consulta con tu Servicio Provincial para comprar e instalar estos equipos.

# A experimentar

## Ver tu IP pública

En un buscador puedes poner ¿Cuál es mi IP? y salen muchas páginas, entra en esta por ejemplo <https://www.whatismyip.com/> te dice tu IP, tu localización y tu ISP (Internet Service Protocol), es decir quien te provee Internet (Embou, Movistar, .. en mi caso AST)



WhatIsMyIP.com

What Is My IP?

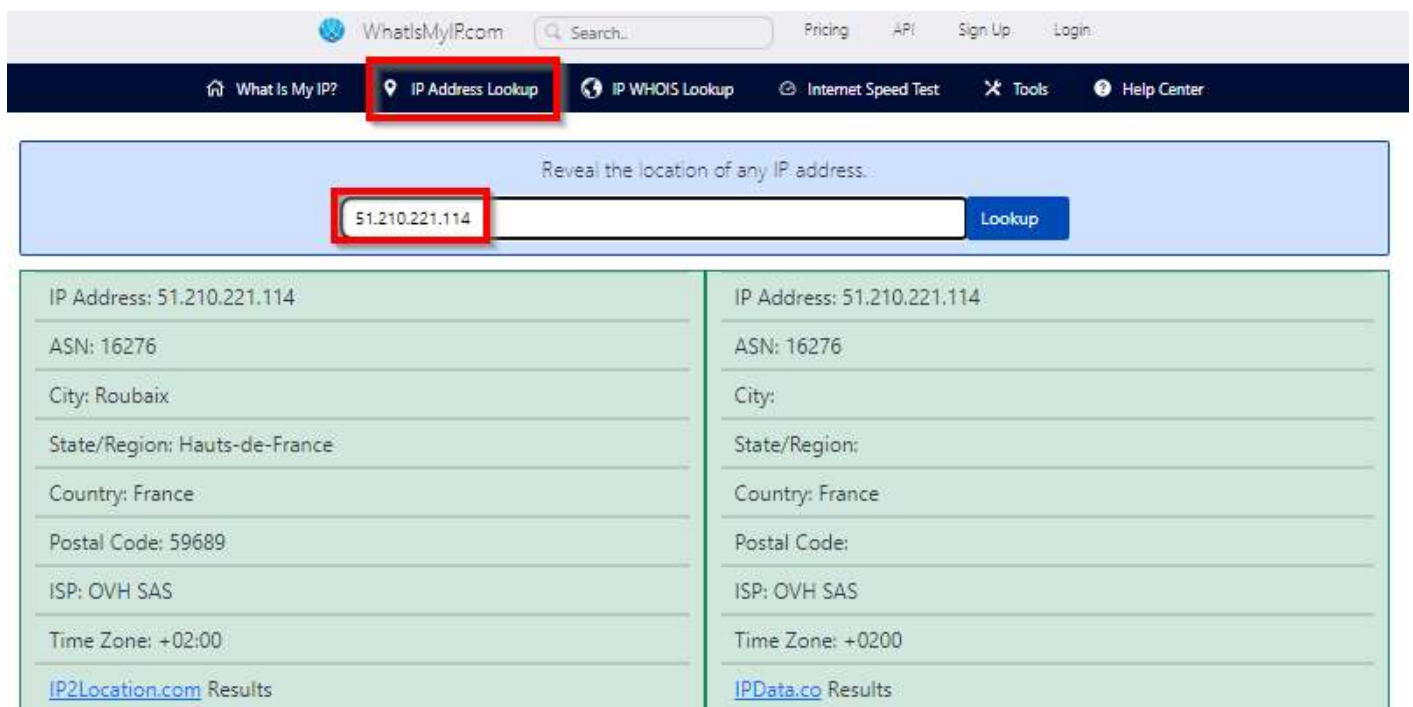
My Public IPv4 is: **188.244.80.254**

My Public IPv6 is: **Not Detected**

My IP Location is: **Zaragoza, AR ES**

My ISP is: **Aragonesa de Servicios Telematicos**

Tiene herramientas útiles como saber dónde está tal IP, por ejemplo la web de aeducar.es está en OVH en Robeaix France



WhatIsMyIP.com

IP Address Lookup

Reveal the location of any IP address.

51.210.221.114

Lookup

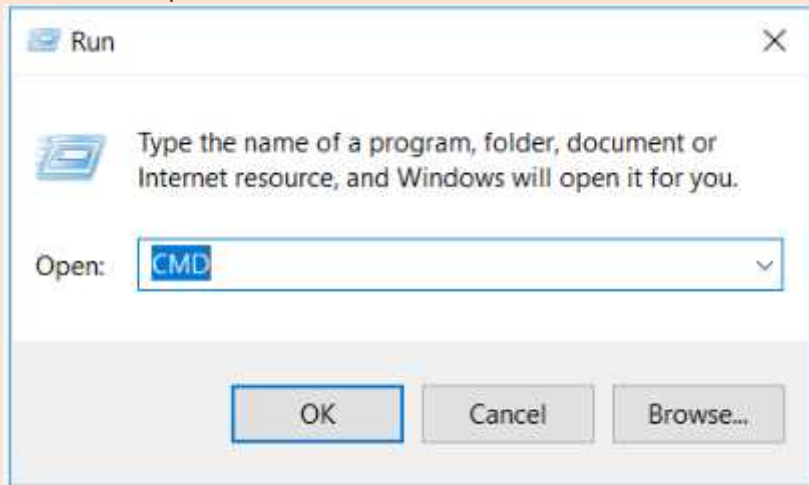
IP Address: 51.210.221.114	IP Address: 51.210.221.114
ASN: 16276	ASN: 16276
City: Roubaix	City:
State/Region: Hauts-de-France	State/Region:
Country: France	Country: France
Postal Code: 59689	Postal Code:
ISP: OVH SAS	ISP: OVH SAS
Time Zone: +02:00	Time Zone: +0200
<a href="#">IP2Location.com</a> Results	<a href="#">IPData.co</a> Results

Practica: Averigua la IP de [www.google.es](http://www.google.es), (para saber la IP de una web mira más adelante cómo se hace) ¿Dónde está registrado esa IP? sorpresa....

## Experimentos con comandos

Entra en la ventana de comandos buscando **cmd** en Windows. En Linux tiene su propia ventana de comandos (busca **terminal** o pulsa Ctrl+Alt+t)

Nota: si tu versión de Windows es XP entra en Inicio-Ejecutar (o las teclas Windows+R) y teclea cmd para entrar en la ventana de comandos:



## ¿Qué dirección IP privada tengo rápidamente?

En Windows teclea en comandos **ipconfig** o si quieres saber también las dns **ipconfig/all**. En Linux teclea **ifconfig**.

Por ejemplo se puede ver que mi IP es 4.6.1.30, que la puerta de enlace es 4.6.1.251 que la máscara de red es de tipo C y que mis DNS son las del Gobierno de Aragón:

```
C:\Users\CATEDU>ipconfig/all
```

#### Windows IP Configuration

```
Host Name . . . . . : DESKTOP-BFKVCNM
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
```

#### Ethernet adapter Ethernet:

```
Connection-specific DNS Suffix . :
Description . . . . . : Realtek PCIe GbE Family Controller
Physical Address. . . . . : [REDACTED]
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::... (Preferred)
IPv4 Address. . . . . : 4.6.1.30(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
4.6.1.251
DHCPv6 IAID . . . . . : 114871178
DHCPv6 Client DUID. . . . . : [REDACTED]
DNS Servers . . . . . : 188.244.82.1
188.244.82.17
NetBIOS over Tcpip. . . . . : Enabled
```

Verás unos números largos que en la figura los he ocultado por seguridad, son **las direcciones físicas MAC** de la tarjeta de red y del router. Son direcciones físicas que vienen de fábrica y son únicas y no se pueden cambiar. Ahora puedes entender ciertos chistes informáticos [1].

- ¿Es el psicólogo que consulta a domicilio? Creo que soy adicto a internet.
- Deme su dirección.
- 87.182.6.27
- Ésa no, la otra.
- [enganchaditoalared@gmail.com](mailto:enganchaditoalared@gmail.com)
- No, la local.
- 127.0.0.1
- Joder, me refiero a la física.
- 0A-5F-64-C0-1F-B1
- Joder, ¡tu casa!
- /home/jose

17:44 ✓✓

Si por ejemplo el ordenador está conectado a Internet desde dos sitios, sale toda la información:

```
Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::...
    IPv4 Address. . . . . : 4.6.1.33
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 4.6.1.251

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . : homestation
    Link-local IPv6 Address . . . . . : fe80::...
    IPv4 Address. . . . . : 192.168.1.33
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

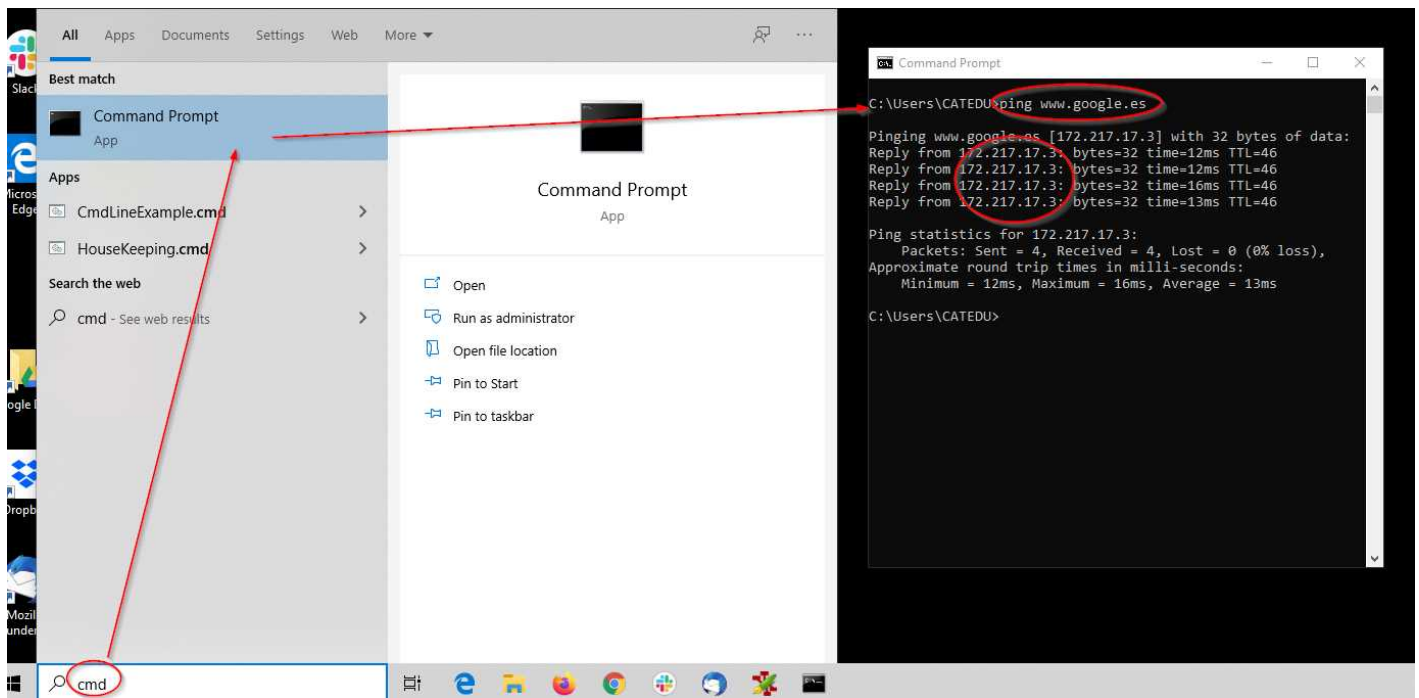
Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
```

En este caso puedes ver que la tarjeta de red está conectado con la IP 4.6.1.33 al router 4.6.1.251 y la tarjeta inalámbrica Wifi está con la ip 192.168.1.33 al router 192.168.1.1

## ¿Cómo puedo saber la IP pública de una página WEB?

Muy fácil, con el comando **ping** a esa página. Por ejemplo para la página [www.google.es](http://www.google.es) teclea **ping google.es** y vemos este resultado:



Sale **172.217.17.3** (a ti te puede salir otra IP pues tiene varios IPs contratados y varios servidores replicados) si lo pones en el navegador ¡¡te sale la página de Google!! No siempre funciona para todas las páginas web, en Google si, pero en otras páginas, los servidores y navegadores no aceptan que entres de forma directa.

Otra manera rápida de averiguarlo es con el comando nslookup que ya vimos en [DNS](#).

## ¿Cuántos switches y servidores hay entre mi ordenador y una página Web?

Pues ya que sabes entrar a la ventana de comandos, teclea **tracert** y la **página que quieras** por ejemplo **tracert google.es** y te sorprenderás. La primera IP que verás es la de tu router (ver [IP puerta de enlace](#))

Éste es el resultado desde el ordenador del centro donde estoy escribiendo (para que veas que no siempre las IPs reservadas de un centro son 192.168.x.x, en este caso es 4.6.1.x)



```

C:\Users\CATEDU>tracert google.es

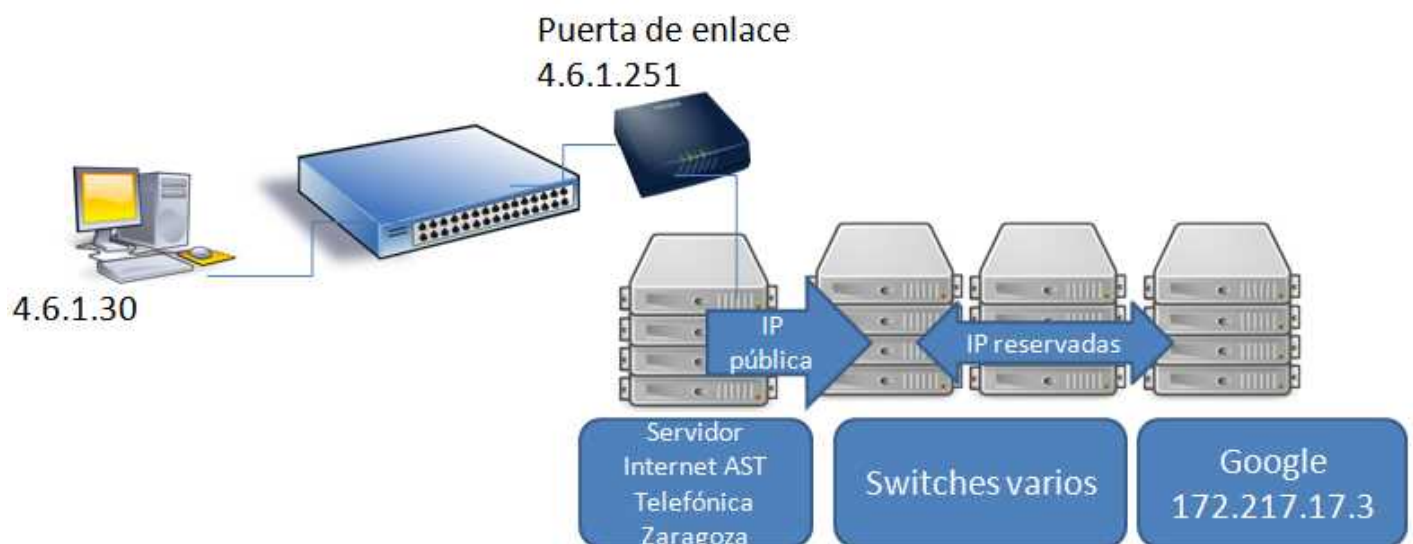
Tracing route to google.es [172.217.17.3]
over a maximum of 30 hops:

  1  <1 ms    1 ms     1 ms    4.6.1.251
  2  2 ms     3 ms     2 ms    7.red-81-46-16.customer.static.ccgg.telefonica.net [81.46.16.7]
  3  3 ms     3 ms     6 ms    192.168.10.1
  4  5 ms     7 ms     4 ms    192.168.2.15
  5  4 ms     4 ms     4 ms    192.168.2.1
  6  4 ms     4 ms     4 ms    192.168.252.3
  7  4 ms     4 ms     4 ms    192.168.252.84
  8  *         *         *      Request timed out.
  9  5 ms     5 ms     5 ms    192.168.12.130
 10  6 ms     5 ms     6 ms    192.168.12.161
 11 11 ms    10 ms    11 ms    172.26.129.149
 12 11 ms    11 ms    16 ms    172.29.33.138
 13 *         *         11 ms    172.29.33.137
 14 *         *         *      Request timed out.
 15 11 ms    11 ms    11 ms    212.166.147.222
 16 *         *         *      Request timed out.
 17 11 ms    11 ms    11 ms    mad07s09-in-f3.1e100.net [172.217.17.3]

Trace complete.

```

o sea



Nos da una idea de la calidad de nuestra conexión a esa web.

## ¿Cómo puedo saber si un ordenador está bien conectado a la LAN?

Haz ping desde ese ordenador al router, por ejemplo si la puerta de enlace es 192.168.1.1 el comando es **ping 192.168.1.1**.

```
C:\Users\cat>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=5ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 5ms, Average = 2ms
```

## ¿Cómo puedo saber si mi ordenador está bien conectado a Internet?

Haz ping a Google por ejemplo **ping 8.8.8.8**.

```
C:\Users\CATEDU>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=11ms TTL=46
Reply from 8.8.8.8: bytes=32 time=11ms TTL=46
Reply from 8.8.8.8: bytes=32 time=14ms TTL=46
Reply from 8.8.8.8: bytes=32 time=11ms TTL=46

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 14ms, Average = 11ms
```

## Estoy bien conectado a Internet (tengo ping 8.8.8.8) pero no me resuelve los nombres (o sea hago ping google.es y no contesta), ¿Cómo es posible?

Muy fácil, si con IPs navegas pero con URLs no, es que **tienes mal las DNS** haz ipconfig/all y comprueba que tienes las DNS del Gobierno de Aragón 188.244.82.1 y 188.244.82.17, teclea nslookup a ver si te salen bien las DNS.

Luego comprueba que las DNS del Gobierno de Aragón funcionan (puede ser que hayan caído), luego haz ping a esas direcciones, en la imagen puedes ver que funcionan :

```
C:\Users\CAT-DESKTOP>ping 188.244.82.1

Haciendo ping a 188.244.82.1 con 32 bytes de datos:
Respuesta desde 188.244.82.1: bytes=32 tiempo=14ms TTL=251
Respuesta desde 188.244.82.1: bytes=32 tiempo=12ms TTL=251
Respuesta desde 188.244.82.1: bytes=32 tiempo=11ms TTL=251
Respuesta desde 188.244.82.1: bytes=32 tiempo=9ms TTL=251

Estadísticas de ping para 188.244.82.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 9ms, Máximo = 14ms, Media = 11ms

C:\Users\CAT-DESKTOP>ping 188.244.82.17

Haciendo ping a 188.244.82.17 con 32 bytes de datos:
Respuesta desde 188.244.82.17: bytes=32 tiempo=15ms TTL=251
Respuesta desde 188.244.82.17: bytes=32 tiempo=10ms TTL=251
Respuesta desde 188.244.82.17: bytes=32 tiempo=10ms TTL=251
Respuesta desde 188.244.82.17: bytes=32 tiempo=15ms TTL=251

Estadísticas de ping para 188.244.82.17:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 10ms, Máximo = 15ms, Media = 12ms
```

## Tengo ping google.es pero no navego

En ese caso tu ordenador está bien conectado y bien configurado pero algo en el software impide la navegación ¿virus? ¿lo formateo? ¡¡¡ espera !!! consulta [el protocolo](#).

## ¿Cómo puedo saber si dos dispositivos están conectados?

Esto es muy útil por ejemplo hacer una IP a la impresora para comprobar que la conexión es correcta y las configuraciones de IPs son correctas. Es simplemente hacer un ping a ese dispositivo, por ejemplo si la impresora la tengo en la 4.6.1.148 hago :

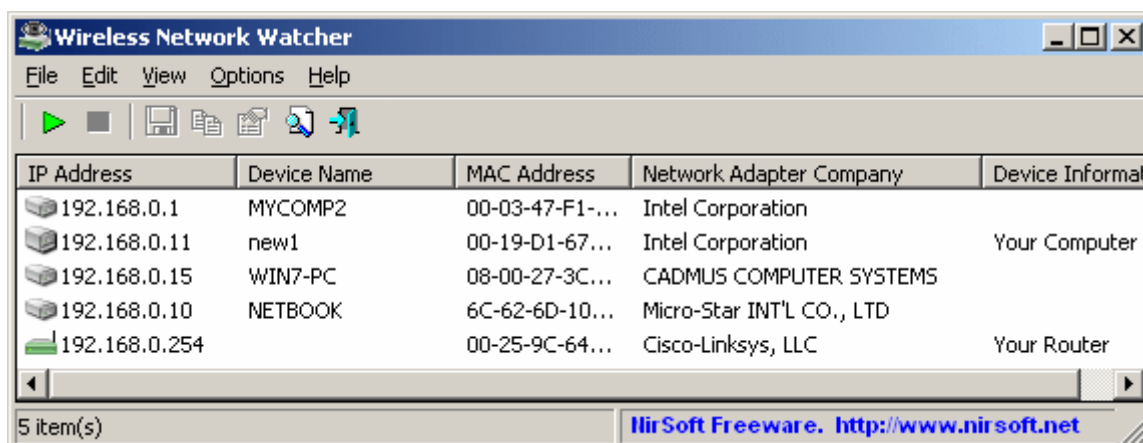
```
C:\Users\CATEDU>ping 4.6.1.148

Pinging 4.6.1.148 with 32 bytes of data:
Reply from 4.6.1.148: bytes=32 time<1ms TTL=64
Reply from 4.6.1.148: bytes=32 time=1ms TTL=64
Reply from 4.6.1.148: bytes=32 time=1ms TTL=64
Reply from 4.6.1.148: bytes=32 time<1ms TTL=64

Ping statistics for 4.6.1.148:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

## ¿Cómo sé si alguien está "pirateando" la wifi?

Hay programas como [Wireless Network Watcher](#) (es portable) que te enseña qué equipos tienes en tu red, y como seguramente nos has hecho caso en [Registra tus IPs](#) entonces puedes detectar al intruso, y es totalmente denunciabile.



IP Address	Device Name	MAC Address	Network Adapter Company	Device Information
192.168.0.1	MYCOMP2	00-03-47-F1-...	Intel Corporation	
192.168.0.11	new1	00-19-D1-67-...	Intel Corporation	Your Computer
192.168.0.15	WIN7-PC	08-00-27-3C-...	CADMUS COMPUTER SYSTEMS	
192.168.0.10	NETBOOK	6C-62-6D-10-...	Micro-Star INT'L CO., LTD	
192.168.0.254		00-25-9C-64-...	Cisco-Linksys, LLC	Your Router



¿A qué esperas a experimentar  
los equipos que hay  
conectados ahora mismos?

*fuentes: elaboración propia*