

TEMA 2: Conceptos básicos de TCP/IP

Módulo

Despliegue de aplicaciones web

para los ciclos

Desarrollo de Aplicaciones Web



Despliegue FP-GS; Tema2:ConceptosBasicosTCPIP

© Gerardo Martín Esquivel, Septiembre de 2023

Algunos derechos reservados.

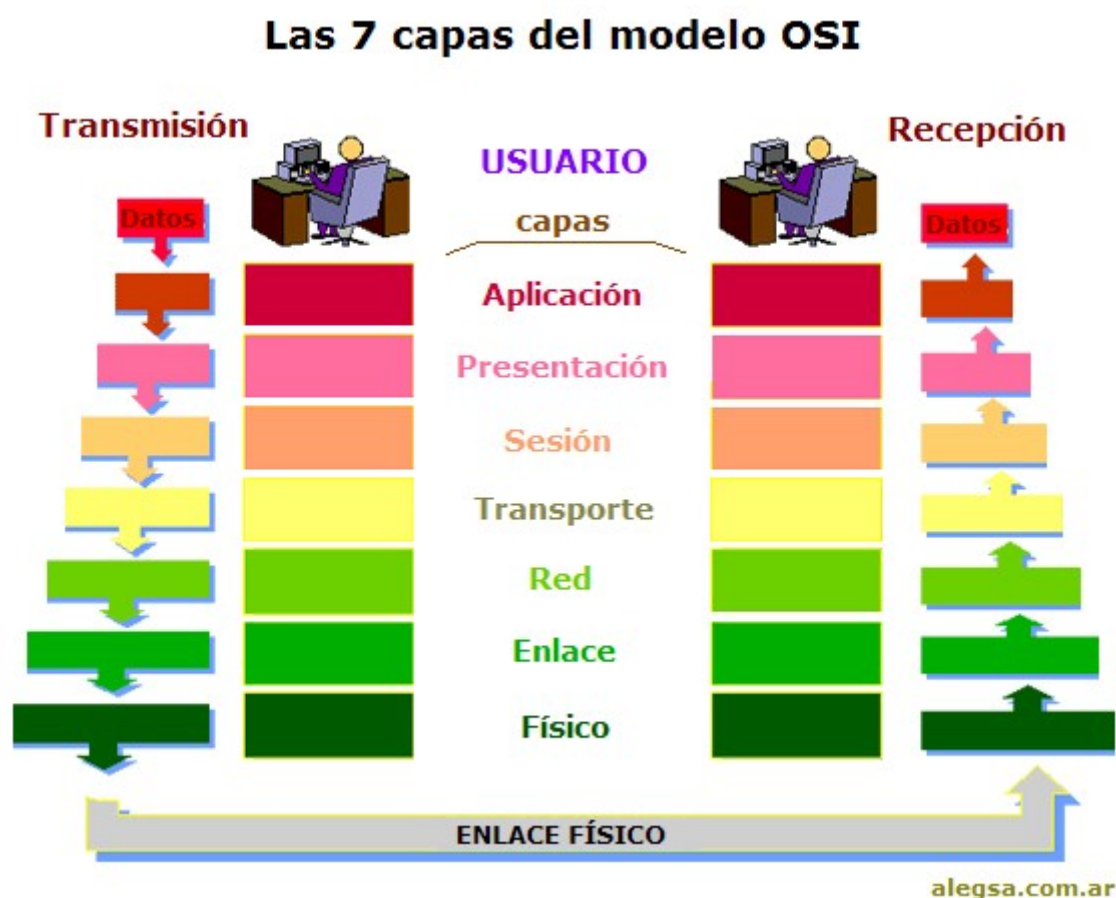
Este trabajo se distribuye bajo la Licencia "Reconocimiento-No comercial-Compartir igual 3.0 Unported" de Creative Commons disponible en <http://creativecommons.org/licenses/by-nc-sa/3.0/>

2.1 El modelo OSI.....	3
2.1.1 Los 7 niveles del modelo teórico OSI.....	4
2.1.2 Transmisión de los datos.....	5
2.2 Familia de protocolos de Internet: TCP/IP.....	6
2.2.1 Los 4 niveles del modelo real TCP/IP.....	6
2.3 Direccionamiento IP.....	7
2.3.1 Direccionamiento con clases.....	7
Números de red reservados.....	9
Redes privadas.....	10
Puerta de enlace.....	10
2.3.2 Dirección IP pública y dirección IP privada.....	11
2.3.3 Direccionamiento con máscara. Subnetting.....	11
2.3.4 Resumiendo.....	13
2.3.5 IPv6.....	13
2.4 El protocolo DHCP.....	14
2.4.1 Funcionamiento.....	15
2.4.2 Clientes DHCP.....	15
2.5 "No tengo Internet"	17

2.1 El modelo OSI

El **modelo de interconexión de sistemas abiertos** (ISO/IEC 7498-1), también llamado **OSI** (en inglés **Open System Interconnection**) es el modelo de red descriptivo, es decir, es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.

Fue desarrollado en 1984 por la Organización Internacional de Estándares (**ISO**), una federación global de organizaciones que representa aproximadamente a 130 países. El núcleo de este estándar es el modelo de referencia **OSI**, una normativa formada por siete capas que define las diferentes fases por las que deben pasar los datos para viajar de un dispositivo a otro sobre una red de comunicaciones.



Este modelo es teórico, no se utiliza en la realidad más que con fines didácticos para los estudiantes, porque otros modelos más flexibles se implantaron con mayor éxito, como el modelo **TCP/IP**.

2.1.1 Los 7 niveles del modelo teórico OSI

- **Capa física:** Es la que se encarga de transmitir, bit a bit, toda la información. Naturalmente la capa física será distinta si la transmisión se hace por cable coaxial, por cable **RJ45**, por par trenzado, por fibra óptica o por **wifi**, pero en cualquier caso la capa física debe saber transmitir las cadenas de bits que le ordene la capa inmediatamente superior.
- **Capa de enlace de datos:** Esta capa se ocupa del direccionamiento físico, de la topología de la red, del acceso al medio, de la detección de errores, de la distribución ordenada de tramas y del control del flujo. Cabe recalcar que el dispositivo que usa la capa de enlace es el **Switch** que se encarga de recibir los datos y enviar cada uno de estos a sus respectivos destinatarios.
- **Capa de red:** El objetivo de la capa de red es hacer que los datos lleguen desde el origen al destino, aún cuando ambos no estén conectados directamente. Los dispositivos que facilitan tal tarea se denominan **routers** (enrutadores o encaminadores).
- **Capa de transporte:** Capa encargada de efectuar el transporte de los datos de la máquina origen a la de destino, independizándolo del tipo de red física que se esté utilizando. A esta capa pertenecen los protocolos **TCP** o **UDP**, el primero orientado a conexión y el otro sin conexión.
- **Capa de sesión:** Esta capa es la que se encarga de mantener y controlar el enlace establecido entre dos computadores que están transmitiendo datos de cualquier índole. Por lo tanto, el servicio proporcionado por esta capa es la capacidad de asegurar que, dada una sesión establecida entre dos máquinas, la misma se pueda efectuar para las operaciones definidas de principio a fin, reanudándolas en caso de interrupción. En muchos casos, los servicios de la capa de sesión son parcial o totalmente prescindibles.
- **Capa de presentación:** El objetivo es encargarse de la representación de la información, de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres los datos lleguen de manera reconocible.

Esta capa es la primera en trabajar más el contenido de la comunicación que el cómo se establece la misma. En ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos, ya que distintas computadoras pueden tener diferentes formas de manejarlas.

Esta capa también permite cifrar los datos y comprimirlos. Por lo tanto, podría decirse que esta capa actúa como un traductor.

- **Capa de aplicación:** Ofrece a las aplicaciones la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico (**SMTP**) y servidor de ficheros (**FTP**), por **UDP** pueden viajar (**DNS** y **Routing Information Protocol**). Hay tantos protocolos como aplicaciones distintas y puesto que continuamente se desarrollan nuevas aplicaciones el número de protocolos crece sin parar.

Cabe aclarar que el usuario normalmente no interactúa directamente con el nivel de aplicación. Suele interactuar con programas que a su vez interactúan con el nivel de aplicación pero ocultando la complejidad subyacente.

2.1.2 Transmisión de los datos

La idea es la siguiente: Un usuario sólo necesita conocer los programas (por ejemplo, debe saber como usar una aplicación de correo electrónico) porque se supone que todos los equipos conectados a la red le van a ofrecer esa aplicación independientemente de otros detalles (sistema operativo, conexión por cable o wifi, etc.). De la misma forma, los protocolos de la capa de Enlace sólo necesitan saber cómo se ordena enviar un paquete desde un ordenador a otro, porque el envío realmente lo hará la capa físico (quizá por cable, quizá por wifi).

El usuario tendrá la idea de que se comunica directamente con el otro usuario, sin embargo la comunicación siempre recorre todos los niveles en el emisor (desde la capa de aplicación a la de enlace) y en el receptor (desde la capa de enlace hasta la capa de aplicación).

Imagina que un profesor de tu instituto necesita comprar un libro: llama por teléfono a un comercial de la editorial y hace el trámite. Ya sólo le queda esperar el libro y puedes tener la sensación de que el comercial es el que proporciona el libro al profesor. Sin embargo probablemente el comercial sólo deje una nota en una bandeja, un operario que recoge la nota empaqueta el libro y al ver la dirección lo coloca en la carretilla que irá al servicio de correos. En correos, según la dirección lo mandarán por carretera, tren, avión, etc. El cartero del destino lo entrega en conserjería del instituto y el conserje se lo lleva al profesor.

De forma similar, el intercambio de información entre dos capas **OSI** consiste en que cada capa en el sistema fuente le agrega información de control a los datos, y cada capa en el sistema de destino analiza y quita la información de control de los datos como sigue:

Si un ordenador (A) desea enviar datos a otro (B), los datos deben empaquetarse a través de un proceso denominado encapsulamiento, es decir, a medida que los datos se desplazan hacia abajo a través de las capas del modelo **OSI** del ordenador A, reciben encabezados, información final y otros tipos de información.

Al llegar al nivel físico se envían los datos que son recibidos por la capa física del receptor.

Cada capa del receptor se ocupa de extraer la cabecera, que anteriormente había añadido su capa homóloga, interpretarla y entregar a la capa superior.

Finalmente llegará a la capa de aplicación la cual entregará el mensaje al usuario.

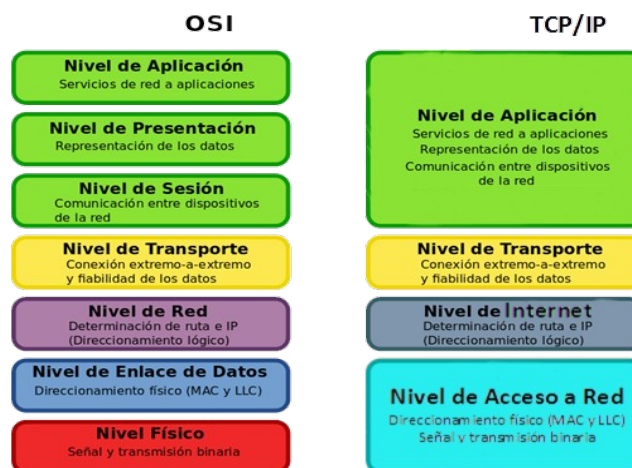
Resumiendo, en una pila de protocolos, cada nivel resuelve una serie de tareas relacionadas con la transmisión de datos, y proporciona un servicio bien definido a los niveles más altos. Los niveles superiores son los más cercanos al usuario y tratan con datos más abstractos, dejando a los niveles más bajos la labor de traducir los datos de forma que sean físicamente manipulables.

2.2 Familia de protocolos de Internet: TCP/IP

TCP/IP es la parte común que conocen todos los ordenadores conectados a Internet. Es un modelo similar al modelo **OSI**, pero más simple, por eso se acabó imponiendo. El modelo **OSI** es una aproximación teórica y fue una primera fase en la evolución de las redes de ordenadores. Por lo tanto, el modelo **OSI** es más fácil de entender, pero el modelo **TCP/IP** es el que realmente se usa.

TCP/IP no es un único protocolo, sino que es en realidad lo que se conoce con este nombre es un conjunto de protocolos que cubren los distintos niveles del modelo. Los dos protocolos más importantes son el **TCP** (**T**ransmission **C**ontrol **P**rotocol) y el **IP** (**I**nternet **P**rotocol), que son los que dan nombre al conjunto.

En el modelo **TCP/IP** sólo hay cuatro capas, no obstante, se cumplen todas las funciones necesarias. En la siguiente imagen vemos como se corresponden las capas del modelo **OSI** con **TCP/IP**:



2.2.1 Los 4 niveles del modelo real TCP/IP

- **Aplicación:** Se corresponde con los niveles **OSI** de aplicación, presentación y sesión. Aquí se incluyen protocolos destinados a proporcionar servicios, tales como correo electrónico (**POP** o **SMTP**), transferencia de ficheros (**FTP**), conexión remota (**TELNET**) y otros como el protocolo **HTTP**.
- **Transporte:** Coincide con el nivel de transporte del modelo **OSI**. Los protocolos de este nivel, (como **TCP** y **UDP**) se encargan de manejar los datos y proporcionar la fiabilidad necesaria en su transporte.
- **Red o Internet:** Es el nivel de red **OSI**. Incluye al protocolo **IP**, que envía los paquetes de información a sus destinos correspondientes. Es utilizado con esta finalidad por los protocolos del nivel de transporte.
- **Enlace o Acceso a red:** Los niveles **OSI** correspondientes son el de enlace y el nivel físico. Los protocolos (**ARP** (**A**ddress **R**esolution **P**rotocol), para la resolución de direcciones) que pertenecen a este nivel son los encargados de la transmisión a través del medio físico al que se encuentra conectado cada **host**, como puede ser una línea punto a punto o una red Ethernet.

El **TCP/IP** necesita funcionar sobre algún tipo de red o de medio físico que proporcione sus propios protocolos para el nivel de enlace de Internet. Por eso hay que tener en cuenta que los protocolos utilizados en este nivel pueden ser muy diversos y no forman parte del conjunto **TCP/IP**. Sin embargo, esto no debe ser problemático puesto que una de las funciones y ventajas principales del **TCP/IP** es proporcionar una abstracción del medio de forma que sea posible el intercambio de información entre medios diferentes y tecnologías que inicialmente son incompatibles.

2.3 Direccionamiento IP

Nota: Antes de comenzar este apartado puede ser conveniente repasar la conversión binario-decimal y decimal-binario.

El **protocolo IP** forma parte del conjunto de protocolos **TCP/IP** (en los que se basa Internet)

Este protocolo se encarga de hacer llegar paquetes de datos a su dirección de destino, sin establecer una conexión, es decir, que cada paquete será enviado de forma independiente y, posiblemente, por distintos caminos. En su camino, el paquete irá pasando por los **routers** y en cada uno de ellos se tomará la decisión de hacia donde se encamina el próximo salto según su destino y las condiciones de la red en ese momento.

Para que esto sea posible, cada equipo de la red debe tener una **dirección IP** única. El **direccionamiento IP** es la asignación de direcciones a cada uno de los nodos o **hubs** de la red.

Nota: En una red se conectan naturalmente ordenadores, pero no en exclusiva. En la red nos encontramos otros equipos como los **routers** o incluso impresoras. Cada uno de esos elementos de la red se denomina **host** o entidad.

Aclaración a la nota: Una impresora conectada directamente a la red es un nodo más de la red. Sin embargo, si la impresora está conectada a un ordenador, no es un nodo, aunque podría ser utilizada desde otros equipos de la red si el ordenador al que se conecta se ofrece como servidor de impresión.

Cada uno de los nodos de la red debe ser identificado con una dirección distinta conocida como **dirección IP**. Las **direcciones IP** ocupan 4 bytes, o lo que es lo mismo, 32 bits. He aquí un ejemplo de **dirección IP**:

```
11000000101010000000101000000101
```

Aunque para hacerlas más legibles, se suelen separar los bytes con puntos:

```
11000000.10101000.00001010.00000101
```

y escribirse en decimal:

```
192.168.10.5
```




Habitualmente usaremos las direcciones **IP** en este último formato, es decir, 4 números decimales entre 0 y 255, separados por puntos.

Una **dirección IP** es un número que identifica lógicamente y jerárquicamente a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el **protocolo IP**, que corresponde al nivel de red o nivel 3 del modelo de referencia **OSI**. Dicho número no se debe confundir con la dirección **MAC** que es un número físico que es asignado a la tarjeta o dispositivo de red (viene impuesta por el fabricante), mientras que la dirección **IP** se puede cambiar.

2.3.1 Direccionamiento con clases

Inicialmente se distinguieron tres grupos de direcciones **IP** que establecían las direcciones que había que usar en función del número de equipos de la red. Actualmente las direcciones se pueden asignar con una mayor libertad, no obstante, de esa división inicial quedan algunas consecuencias vigentes hoy día.

En la siguiente tabla podemos ver las clases de redes (**A**, **B** y **C**). Para cada una se muestra (verde) cuántos bytes se usan para designar la red y cuántos bytes se usan para designar al equipo dentro de la red (amarillo). Para distinguir si una **dirección IP** pertenece a una u otra clase miramos el valor de los primeros bits. En la tabla podemos ver esos valores en binario y en decimal.

Tipo de red	Red/host	Formato (binario)	Formato (decimal)	Nº hosts
Clase A		0xxxxxxxxx	de 0.x.x.x a 127.x.x.x	16.777.214
Clase B		10xxxxxxxx	de 128.x.x.x a 191.x.x.x	65.534
Clase C		110xxxxxxxx	de 192.x.x.x a 223.x.x.x	254

Dentro de cada red asignamos direcciones a cada equipo usando todos los números posibles en la parte de host, salvo dos:

- el que tiene todos los bits de host a cero (**dirección de red**). La dirección de red se usa para nombrar a la red en su conjunto. No hace referencia a un equipo de la red, sino a la red completa
- el que tiene todos los bits a uno (**broadcast**). El **broadcast** es necesario cuando se pretende hacer que un mensaje sea visible para todos los equipos conectados a la misma red. Si necesitamos enviar un mismo paquete a todos los equipos, lo que hacemos es enviarlo a la dirección de **broadcast** y todos lo recibirán. De este modo nos ahorramos hacer muchos envíos del mismo paquete, cada uno a un equipo.

Nota: En la clasificación de direcciones anterior se puede observar que ciertos números no se usan: las direcciones cuyo primer byte sea superior a **223** (clases **D** y **E**, que aún no están definidas, o dicho de otro modo, se reservaron para necesidades futuras).

Ejemplo 1: En una red de **clase C** podemos tener las siguientes direcciones:

- **192.168.20.0** como **dirección de red**.
- **192.168.20.1** a **192.168.20.254** como direcciones disponibles para **hosts** de la red.
- **192.168.20.255** como dirección de **broadcast**.

Vamos a analizarlo:

- Sabemos que se trata de una red de **clase C** porque el primer byte es **192** (o dicho de otra manera, los primeros bits son **110**).
- Si es una red de **clase C**, ya sabemos que todas las direcciones de la red coinciden en los tres primeros bytes, que son la parte de la dirección que identifica a la red. Nos queda por tanto, el último byte para asignar un número distinto a cada equipo.
- La dirección que resulta de poner a **0** todos los bits de host (**192.168.20.0**) no se puede asignar a un equipo, porque está reservada para la **dirección de red**.
- La dirección que resulta de poner a **1** todos los bits de host (**192.168.20.255**) no se puede asignar a un equipo, porque está reservada para el **broadcast**.
- El resto de combinaciones de los bits de host (desde 1 hasta 254) son las direcciones disponibles para los equipos de la red.

Ejemplo 2: En una red de **clase B** podemos tener las siguientes direcciones:

- **141.87.0.0** como **dirección de red**.
- **141.87.0.1** a **141.87.255.254** como direcciones disponibles para **hosts** de la red.
- **141.87.255.255** como dirección de **broadcast**.

Vamos a analizarlo:

- Sabemos que se trata de una red de **clase B** porque el primer byte es **141** (o dicho de otra manera, los primeros bits son **110**).
- Si es una red de **clase B**, ya sabemos que todas las direcciones de la red coinciden en los dos primeros bytes, que son los que identifican a la red. Nos quedan por tanto, los dos últimos bytes para asignar un número distinto a cada equipo.
- La dirección que resulta de poner a **0** todos los bits de host (**141.87.0.0**) no se puede asignar a un equipo, porque está reservada para la **dirección de red**.
- La dirección que resulta de poner a **1** todos los bits de host (**141.87.255.255**) no se puede asignar a un equipo, porque está reservada para el **broadcast**.
- El resto de combinaciones de los bits de host (desde **0.1** hasta **255.254**) son las direcciones disponibles para los equipos de la red.

Nota: Cuando se expresa una dirección **IP** se suele indicar el número de bytes que forman parte de la red. Por ejemplo, la dirección **192.168.20.17/24** se expresa con el **/24** para indicar que los primeros **24 bits** son la parte de red y, por tanto, los **8 bits** restantes son la parte del host.

De la misma manera, hacemos **referencia a la red completa** poniendo la dirección de red (con ceros en la parte del host) y el número de bits que forman parte de red: **192.168.20.0/24** es la red a la que pertenece la **IP** del ejemplo.

NÚMEROS DE RED RESERVADOS

Como ya sabemos, en la enorme red que es Internet, se utiliza el **protocolo IP**, de modo que cada equipo que esté conectado a Internet tendrá asignada una **dirección IP**. Pero en Internet no se pueden usar todas las direcciones porque algunas de ellas están reservadas. Las direcciones que están reservadas son las siguientes:

- Las direcciones **127.0.0.0/8** se usan para designar a la propia máquina (**bucle local** o **loopback**). Si enviamos un paquete a esas direcciones, llega a la propia máquina.
- Las direcciones **10.0.0.0/8** se usan para una **red privada de clase A**, normalmente para empresas muy grandes, de hasta 16 millones de hosts. Una red que conecte los móviles de una compañía telefónica usará una red privada de clase A.
- Las direcciones **169.254.0.0/16** son direcciones de **enlace local**. Se las autoasigna un equipo cuando no puede averiguar que **dirección IP** le correspondería (por ejemplo, porque no le contesta ningún servidor **DHCP**). Estas direcciones sólo valen para comunicaciones dentro de una red local porque los routers no enrutan sus paquetes. Si un equipo tiene una de estas direcciones indica que la red tiene problemas.
- Las direcciones **172.16.0.0/16** a **172.31.0.0/16** (16 bits red, 16 bits hosts) se usan para **redes privadas de clase B**. Para universidades y grandes compañías.
- Las direcciones **192.168.x.0/24** (24 bits red, 8 bits hosts) se usan para **redes privadas de clase C**. Son 256 redes clase **C** continuas, uso de compañías medias y pequeñas.

REDES PRIVADAS

Pero ¿qué significa esto de las redes privadas? Imagínate que en nuestro aula tenemos 20 ordenadores que queremos conectar a Internet. Si contratamos una conexión a Internet para cada ordenador, cada uno de esos equipos tendría una dirección válida para Internet que sería asignada por el **ISP** (Internet Service Provider, la empresa que nos da el servicio). Esa solución sería muy cara, de modo que lo vamos a resolver de otra manera:

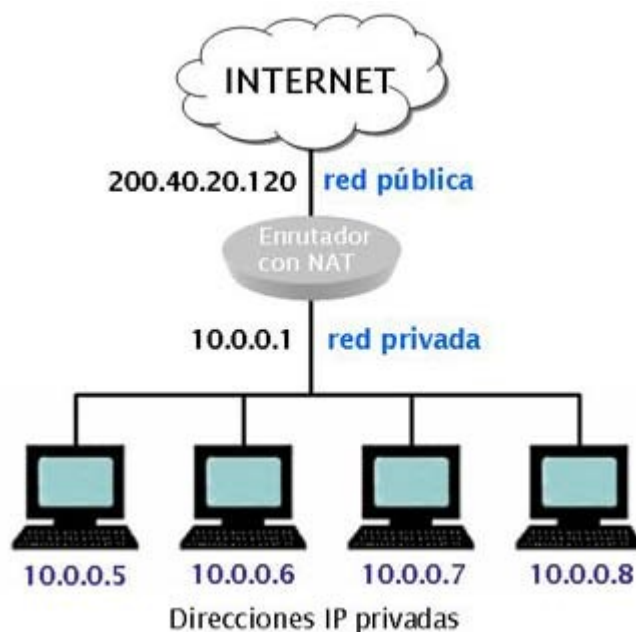
Contratamos una sola conexión a Internet. Esa conexión tendrá una **dirección IP pública** asignada por el **ISP**. Por otro lado, creamos una red privada con nuestros 20 ordenadores. Puesto que son pocos ordenadores nos bastará con una red de **clase C** que admite hasta un máximo de 254 equipos. En nuestra red privada estamos obligados a usar las direcciones reservadas para redes privadas, eso significa que los dos primeros bytes tendrán que ser obligatoriamente **192.168**. El tercer byte lo elegimos como nos dé la gana, desde **0** hasta **255**, porque podemos usar cualquiera de las 256 redes privadas de **clase C**. Y con el último byte, asignamos números distintos a cada equipo, recordando que no podemos usar ni el **0** ni el **255**.



En una misma red no pueden existir dos direcciones iguales, pero sí se pueden repetir en redes privadas distintas. En las redes privadas usaremos direcciones reservadas porque sabemos que esas direcciones nunca existirán como direcciones de Internet y, por tanto, nunca habrá conflicto.

PUERTA DE ENLACE

La **puerta de enlace** en una red es el nodo de la red que permite acceder a una red exterior. Cada vez que se envía un paquete a una dirección que no pertenece a nuestra red, se encaminará hacia la **puerta de enlace** para que salga fuera. Por ejemplo, todos las peticiones y consultas a Internet que se hagan desde los equipos de nuestro instituto tendrán que dirigirse hacia la **puerta de enlace**. Cuando configuramos una red privada, la **puerta de enlace** apuntará siempre al **router** que es el que nos conecta con el exterior (Internet).



En la imagen vemos una red privada de **clase A** (usa las direcciones reservadas para ello). Todos los equipos de la red privada (incluido el **router**) tienen una dirección privada. La **puerta de enlace** será la dirección privada del router (**10.0.0.1**). El router tiene, además, una **dirección IP pública** porque también es miembro de esa otra red (Internet).

2.3.2 Dirección IP pública y dirección IP privada

Como vemos en el ejemplo anterior, cada equipo de nuestro aula tendrá una **dirección IP privada** que sirve para distinguir cada uno de los equipos de nuestra red privada. Esa dirección será del tipo **192.168.x.x** (si hemos montado una red de clase C) o del tipo **172.16.x.x** a **172.31.x.x** (si hemos montado una red de clase B) o del tipo **10.x.x.x** (si hemos montado una red de clase A).

Al mismo tiempo todos los equipos de nuestra red tienen una **dirección IP pública**, que es la misma para todos y que habrá sido asignada por el **ISP**.

- Para averiguar la dirección **IP privada** de un equipo con **Windows**, abre la terminal de comandos y escribe el comando:

```
ipconfig /all
```

- Para averiguar la dirección **IP privada** de un equipo con **Linux**, abre la terminal de comandos y escribe el comando:

```
ifconfig
```

Nota: Desde la versión **18.04** de **Ubuntu** el comando **ifconfig** no estará disponible hasta que instales el paquete **net-tools** (**sudo apt-get install net-tools**).

- Para averiguar la dirección **IP privada** de un móvil con **Android**, entra en:

AJUSTES/ACERCA DEL DISPOSITIVO/ESTADO/DIRECCIÓN IP

- Para averiguar la **IP pública** a través de la que te conectas a Internet puedes usar alguna página web de las muchas que existen para ver esa información, por ejemplo:

<http://www.whatsmyip.org>

2.3.3 Direccionamiento con máscara. Subnetting

El direccionamiento por clases tiene inconvenientes: es poco flexible y hay una enorme diferencia de tamaño entre redes de distintas clases. Si tenemos que crear una red con 300 ordenadores no nos vale una red de **clase C** porque sólo admite 254, por tanto tenemos que recurrir a una de **clase B** que está dimensionada para 65.534 que, como puedes ver, es exagerado.

Por este motivo se recurre al **subnetting** (subredes). Consiste en coger algunos bits de la parte de host y "prestarlos" a la parte de red, para dimensionar una red más adecuada a nuestro tamaño. Para definir una subred tenemos que dar dos datos: la dirección de red y la máscara.

- La **dirección de red**: como ya sabemos la dirección de red es aquella que tiene todos los bits de la parte del host a ceros.
- La **máscara**: la máscara es una forma de indicar el tamaño de cada una de las partes. Se puede indicar como una dirección **IP** que tiene todos los bits de la parte de red a unos y todos los bits de la parte de host a ceros. Y también se puede indicar simplemente con un número que indica el número de bits dedicados a la red.

Por ejemplo, la máscara de red en una red de **clase A** debe indicar que la parte de red ocupa los 8 primeros bits, o sea:

```
11111111.00000000.00000000.00000000
```

Eso se puede expresar de dos formas:

```
255.0.0.0
```

o bien

```
/8
```

Igualmente la máscara de una red de **clase B**:

11111111.11111111.00000000.00000000

se puede indicar con **255.255.0.0** ó **/16** y la de una red de **clase C**:

11111111.11111111.11111111.00000000

Se puede indicar como **255.255.255.0** ó **/24**.

Cuando usamos el **subnetting** indicamos de forma explícita (con la **máscara**) el tamaño de cada una de las partes de la **dirección IP**. Eso nos permite olvidarnos de las clases **A**, **B** y **C** y dimensionar nuestra red con mayor libertad.

Nota: Aunque el **subnetting** deja anticuado el uso de clases, perduran las direcciones reservadas que se establecieron con esas clases.

Ejemplo:

Supongamos que en el instituto tenemos una red de **clase C** con la dirección **192.168.20.0** y queremos separarla en 3 subredes para destinarlas a profesorado, alumnado y dirección. Para ello cogeremos "prestados" dos bits de los inicialmente destinados al host. Esos dos bits indicarán la subred, por ejemplo **00** para profesorado, **01** para alumnado y **10** para administración. Y cada una de las subredes podrá tener hasta 62 equipos (porque quedan 6 bits para el host y $2^6-2=62$).



La subred del profesorado la definimos con la dirección de red **192.168.20.0** y la máscara **255.255.255.192**. La otra forma de definirla es **192.168.20.0/26**.

La subred del alumnado la definimos con la dirección de red **192.168.20.64** y la máscara **255.255.255.192**. La otra forma de definirla es **192.168.20.64/26**.

La subred de administración la definimos con la dirección de red **192.168.20.128** y la máscara **255.255.255.192**. La otra forma de definirla es **192.168.20.128/26**.

Observa que la máscara de red corresponde a **11111111.11111111.11111111.11000000**. En una máscara nunca se mezclan los unos y los ceros. Los unos, que son la parte de red, están al principio. Los ceros, que son la parte de host, están al final. Esta máscara escrita como dirección **IP** es **255.255.255.192** y escrita como número es **/26**.

Ejemplo:

La dirección **172.16.1.1** con máscara **255.255.255.0** nos indica que los tres primeros octetos identifican la red y el cuarto identifica el host. Hay dos direcciones de cada subred que quedan reservadas: aquella que identifica la subred y que tiene todos los bits de la parte del host a **0** (en este caso **172.16.1.0**) y la dirección para realizar broadcast en la subred y que tiene todos los bits de la parte del host a **1** (en este caso **172.16.1.255**).

2.3.4 Resumiendo

La configuración completa de un equipo para que forme parte de una red que usa **TCP/IP** requiere únicamente tres datos:

- **Dirección IP** única para ese equipo.
- **Máscara de red.**
- **Puerta de enlace.**

Además es habitual que durante esta configuración se soliciten las direcciones de **DNS**. Esto no forma parte de esa configuración mínima que ya tiene conectados completamente todos los equipos con esos tres datos. En los temas siguientes hablaremos extensamente del **DNS**.

2.3.5 IPv6

Las direcciones **IP**, tal y como las acabamos de contar, pertenecen a la versión 4 del protocolo (**IPv4**). Existe una versión más reciente del protocolo (**IPv6**) que utiliza direcciones **IP** distintas.

El número de direcciones **IP** distintas con **IPv4** es $2^{32} = 4.294.967.296$ que se queda corto para un mundo con 7.000 millones de habitantes, cada uno de los cuales dispone de varios equipos (PC, móvil, coche...) conectados a Internet. La versión 6 utiliza 128 bits para cada dirección, con lo que podemos tener hasta 2^{128} equipos, que son unos 340 sextillones (3.4×10^{38} hosts direccionables).

De la misma forma que en la versión 4 las direcciones **IP** se suelen expresar en números decimales separados por puntos, en la versión 6 se expresan en 8 grupos de 4 cifras hexadecimales separados por el símbolo dos puntos (:).

Ejemplo: Dirección IP de la versión 6 del protocolo.

2001:0db8:85a3:08d3:1319:8a2e:0370:7334

Como sabemos, cada dígito hexadecimal se corresponde con cuatro bits según la tabla siguiente:

Cuarteto de bits	Dígito Hex.	Cuarteto de bits	Dígito Hex.
0000	0	1000	8
0001	1	1001	9
0010	2	1010	A
0011	3	1011	B
0100	4	1100	C
0101	5	1101	D
0110	6	1110	E
0111	7	1111	F

Para facilitar la escritura de direcciones se pueden usar las siguientes reglas:

- Los ceros a la izquierda de cada grupo se pueden suprimir. Así, la dirección del ejemplo anterior también la podemos escribir como:

```
2001:db8:85a3:8d3:1319:8a2e:370:7334
```

- Cuando un grupo (o varios consecutivos) es todo ceros se pueden quitar sustituyéndolos por dos veces el símbolo dos puntos (::).

Ejemplo: Varias formas de escribir la misma dirección IPv6

```
2001:0DB8:0000:01A0:0000:0000:1428:57ab  
2001:0DB8::01A0:0000:0000:1428:57ab  
2001:0DB8:0000:01A0::1428:57ab
```

- La regla anterior sólo se puede aplicar una vez en cada dirección.

Ejemplo: Dirección INCORRECTA porque no se sabe cuantos ceros hay en cada lado

```
2001:0DB8:::01A0:::1428:57ab
```

2.4 El protocolo DHCP

Hemos visto que todos los equipos que se conectan a la red han de tener una **dirección IP**. Algunos equipos de Internet siempre tienen la misma dirección IP (**dirección IP fija**) porque alojan servidores (**FTP**, **web**, **DNS**, etc) y deben de tener direcciones conocidas para que todo el mundo pueda acceder.

Las **direcciones fijas** se pueden configurar desde cada uno de los equipos. Junto con la dirección que vamos a usar debemos indicar la **máscara**, la **puerta de enlace** y las direcciones de los servidores **DNS**.

Otros equipos cambian de dirección cada vez que se conectan a Internet (**dirección IP dinámica**), por ejemplo los de los usuarios como nosotros. Esto se hace así para aprovechar mejor las direcciones disponibles. Cuando yo apago mi ordenador mi dirección podrá ser usada por otro equipo que se conecte.

Las **direcciones dinámicas** son asignadas mediante un protocolo llamado **DHCP** (*Dynamic Host Configuration Protocol*). Si se quiere asignar direcciones dinámicas será necesario que exista en la red un equipo que actúe de servidor **DHCP**, es decir, que reciba peticiones y responda asignando la dirección **IP** (y los demás datos: máscara de red y puerta de enlace).

Nota: asignar las direcciones desde cada uno de los equipos supone un trabajo muy complicado para administrar la red (habrá que recordar las direcciones y usadas y las direcciones libres), por eso lo más habitual es asignar direcciones dinámicas mediante **DHCP**. También existe la posibilidad de asignar direcciones fijas desde el servidor **DHCP** emparejando la **dirección IP** deseada con la **MAC** del equipo. Esto se suele llamar **reserva**. Las direcciones reservadas solo se asignan al equipo que le corresponde.

2.4.1 Funcionamiento

1. Cuando un equipo se enciende y está configurado para recibir la **IP** automáticamente de un servidor **DHCP** envía un mensaje (**DHCP DISCOVER**) a todos los equipos (**broadcast**) de la red preguntando si hay un servidor **DHCP**.
2. Ese mensaje llega a todos los equipos de la red y por tanto llega al servidor **DHCP** que es uno de ellos. El servidor responderá (**DHCP OFFER**) ofreciendo una dirección **IP** disponible a ese equipo.
3. El cliente solicita (**DHCP REQUEST**) el uso de unos datos (dirección **IP**, máscara, puerta de enlace,...). Generalmente solicitará el uso de los mismos datos que le han ofrecido.
4. El servidor acepta (**DHCP ACK**) o deniega (**DHCP NAK**) la solicitud del cliente. Naturalmente, si el cliente ha solicitado los mismos que se le ofrecieron, lo normal será que se acepte. Si por algún motivo no se acepta, se le ofrecerá otra dirección.

Debes tener en cuenta que aunque haya un servidor **DHCP** cada equipo puede estar configurado para usarlo o no. Es decir puede solicitar una dirección o tener una dirección fija. Lo normal es que el servidor reparta sólo un rango de direcciones. Los equipos que estén configurados con una dirección fija tienen que evitar ese rango.

Nota: Si en la misma red hubiese dos servidores **DHCP** contestando peticiones se formará un buen lío. Esto es algo habitual cuando los estudiantes de redes hacen prácticas de servicio **DHCP**.

2.4.2 Clientes DHCP

Como hemos visto, cada equipo puede configurarse para usar siempre la misma dirección **IP**. En **Windows** lo podemos hacer en:

Inicio/Panel de Control/Centro de redes/Cambiar configuración del adaptador

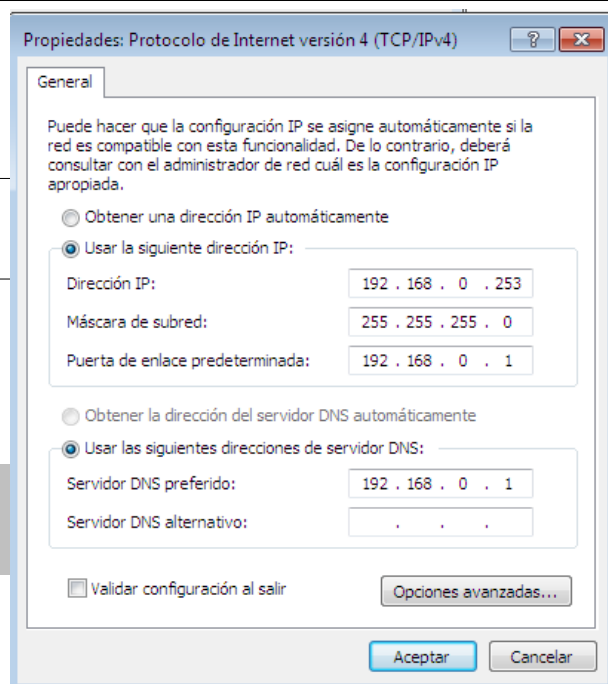
Veremos un icono para cada una de las conexiones que tengamos en nuestro equipo. Seleccionamos la conexión deseada con doble clic y nos vamos a:

Propiedades/Protocolo de Internet version 4/Propiedades

En la imagen vemos que el equipo está configurado para usar siempre la dirección **IP** **192.168.0.253**, con máscara **255.255.255.0** y puerta de enlace **192.168.0.1**.

Nota: Si configuramos así nuestro equipo en la red tendremos un tipo de dirección **IP** conocido como **IP fija**.

Si deseamos que nuestro equipo haga uso del servicio **DHCP** y solicite una dirección de



modo automático, sólo habría que marcar la opción "**Obtener una dirección IP automáticamente**" y no habría que detallar ningún dato más, pues el servidor **DHCP** nos los asigna todos.

Nota: Si configuramos así nuestro equipo en la red tendremos un tipo de dirección **IP** conocido como **IP dinámica**.

En **Ubuntu 16** buscamos el icono de red que se encuentra en la parte derecha de la barra superior. Se trata de un dibujo de doble flecha, o bien, el típico de ondas wifi. Tras ese icono se esconde un menú donde debemos seleccionar:

**Editar las conexiones/
seleccionamos la conexión
adecuada/Editar/Ajustes de
IPv4**

En el desplegable "**Método**" tenemos la posibilidad de elegir **Manual** para configurar todos los datos para una **IP** fija, o bien, **DHCP** para hacer uso del servidor **DHCP**.

En **Ubuntu 18** y posteriores, desde la esquina superior derecha accedemos a la configuración, seleccionamos el apartado **Red** y podemos configurar las redes cableadas o añadir una nueva.

Podemos elegir entre el servicio **DHCP automático**, o la configuración **manual**.

Nota: Recuerda que las direcciones de la red **169.254.0.0/16** están reservadas para el caso de que un equipo no consiga una dirección **IP**. Esto puede ocurrir si está configurado como cliente **DHCP** pero no existe ningún servidor **DHCP**. Así que si en algún momento tu equipo tiene problemas para conectarse y observas que su dirección **IP** comienza por **169.254** tendrás que analizar por qué no encuentra al servidor **DHCP**.

2.5 "No tengo Internet"

Seguramente más de una vez te has visto como **Enjuto Mojamuto** en "**El peor día de su vida**" (en <https://www.youtube.com/watch?v=BBqQLOor0Rk> puedes ver esta historia de 2 minutos). La forma más habitual de descubrir que falla nuestra configuración de red es cuando intentamos acceder a una página web desde el navegador y decimos eso de "no tengo internet".



A estas alturas ya sabemos que hay un montón de parámetros y circunstancias por los que puede fallar la conexión, así que vamos a resumir los pasos que tenemos que dar para solucionar el problema.

1. ¿Tenemos asignada una dirección **IP**?
2. Si no tenemos una dirección **IP** probablemente esté desactivada la conexión o incluso el cable esté desconectado.
3. Si tenemos una dirección **IP** que comienza por **169** significa que no ha sido posible contactar con el servidor **DHCP**.
4. Si tenemos una dirección **IP** correcta haremos un **ping** a la dirección **IP** del router.

```
ping 192.168.0.1
```

Nota: Tendrás que sustituir **192.168.0.1** por la dirección de tu router.

5. Si el router no contesta el problema está en nuestra red interna. Tendremos que comprobar que el router está encendido y los cables conectados.
6. Si funcionó el **ping** al router haremos otro **ping** a la dirección **8.8.8.8**, que es un servidor de Google.

```
ping 8.8.8.8
```

Nota: No tienes por qué usar la dirección **8.8.8.8**, te vale cualquier dirección pública de Internet que sepas que está activa.

7. Si no contesta el **8.8.8.8** significa que nuestra red no está conectada a Internet. Tendremos que comprobar la configuración del router y el cable de entrada de Internet al router.
8. Si funcionó el ping al **8.8.8.8** haremos otro ping a **www.google.com**, que es el dominio de Google.

```
ping www.google.com
```

9. Si no contesta **www.google.com** el problema está en el servidor **DNS**, puesto que tenemos acceso a Internet pero no es capaz de traducir los dominios. Revisa la configuración de la conexión añadiendo o corrigiendo los **DNS**.
10. Si funcionó el ping a **www.google.com** la configuración es correcta. Si el problema sigue existiendo seguramente se trata de un error en la dirección que escribes o un problema del navegador que estás usando.