

# Direccionamiento IP v4

Versión 1.4.27 (c) 2007-2020 Eduardo José Moreira. Este documento está bajo [licencia GNU FDL](#).

## Contenido

<a href="#">Direccionamiento IP v4.....</a>	<a href="#">1</a>
<a href="#">    Contenido.....</a>	<a href="#">1</a>
<a href="#">    Introducción.....</a>	<a href="#">2</a>
<a href="#">    Direcciones IP v4.....</a>	<a href="#">3</a>
<a href="#">    Clases de direcciones IP.....</a>	<a href="#">6</a>
<a href="#">    Máscara de subred y dirección IP de red.....</a>	<a href="#">10</a>
<a href="#">    Direcciones IP especiales (o IP reservadas).....</a>	<a href="#">14</a>
<a href="#">    Direcciones IP privadas o IP libres. Rangos.....</a>	<a href="#">16</a>
<a href="#">    Direcciones IP públicas.....</a>	<a href="#">19</a>
<a href="#">    Direcciones IP estáticas y dinámicas.....</a>	<a href="#">20</a>
<a href="#">    Recordatorio: tipos de direcciones en una red.....</a>	<a href="#">22</a>
<a href="#">    IP del router: Consejos prácticos.....</a>	<a href="#">24</a>

## Introducción

Las direcciones IP están definidas dentro de la arquitectura de red TCP/IP, en el nivel 3 de la misma, el nivel de Interred o Internet (en inglés). En concreto forman parte del protocolo IP (Internet Protocol), del que toman su nombre.

Como se ha universalizado el empleo de redes TCP/IP en todo tipo de ordenadores, encontraremos direcciones IP casi en cualquier equipo.

Existen dos tipos de direcciones IP:

- Direcciones IP versión 4 (abreviado IP v4)
- Direcciones IP versión 6 (abreviado IP v6)

Las direcciones IP v4 son números de 32 bit (4 Bytes), y las direcciones IP v6 son números de 128 bit (16 Bytes).

Con IP v4, al ser números de 32 bit, podemos tener hasta

$$2^{32} = 4.294.967.296 \quad (4 \text{ mil } 294 \text{ millones y pico})$$

números o dir. IP distintas posibles (en la práctica son menos), mientras que con IP v6 podemos tener hasta

$$2^{128} = 3,4028236692093846346337460743177e+38. \quad (\text{una montoná :-})$$

números o dir. IP distintas (muchísimas más).

Las IP v6 se desarrollaron cuando parecía que las IP v4 estaban empezando a agotarse en el mundo. Pero enseguida aparecieron formas de reutilizar direcciones IP v4 definiendo rangos de IP privadas y protocolos como NAT para conectar redes que utilicen esas IP privadas mediante dispositivos como los router (encaminadores).

En la actualidad el empleo de IP v4 es universal (además podemos reutilizarlas como se explica antes, lo que evita que se acaben o al menos frena su agotamiento), mientras que IP v6 comienza a utilizarse en ámbitos reducidos. En estos apuntes nos centraremos en las IP v4.

## Direcciones IP v4

Las dirs. IP son números de 32 bit que identifican a cada ordenador en una red TCP/IP.

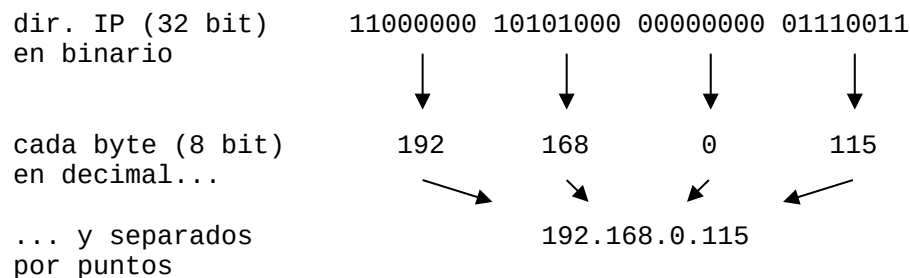
Nota: Recordar que cada ordenador (realmente cada tarjeta de red) tiene dos direcciones:

Dirección IP – 4 bytes (32 bits) las v4. Definidas en el nivel 3 o nivel de Interred de OSI y de TCP/IP. Las ponemos/cambiamos nosotros.

Dirección MAC – 6 bytes (48 bits). Definidas en el nivel 2 de OSI o nivel de Enlace (que no existe en TCP/IP). Son fijas en principio, es decir, no las podemos cambiar.

Nota: También recordar que la red TCP/IP sirve para redes de todos los tamaños, tanto pequeñas (LAN), medianas (MAN) como grandes (WAN). Como en toda red las direcciones de cada equipo tienen que ser distintas, las IP también tienen que ser distintas en una red dada, sea cual sea su tamaño (en n.º de ordenadores, tablets, móviles, etc.)

En la práctica las IP v4 se manejan como 4 números separados por puntos: cada número es un byte (8 bit) y se escribe en decimal. Un ejemplo de dir. IP es:



Luego cada IP se escribe como 4 números de 8 bit cada uno, separados por puntos; si lo pensamos las cosas cuadran: se puede expresar un mismo valor como 32 bits en binario, o como 4 bytes (es decir, escribiendo los bytes como 4 números en decimal).

En una IP cada uno de esos 4 valores es un número de 8 bits, luego puede tomar un valor entre 0 y 255 (tomando esos números sin signo) ya que con 8 bit (con 8 dígitos binarios) podemos tener hasta

$$2^8 \text{ bit} = 256 \text{ valores distintos}$$

donde esos 256 valores pueden ir del 0 al 255. Por ejemplo, esto **no** sería una dir. IP:

192.268.0.1  
└─┬─┘  
  └─┬─┘  
      0 .. 255 (leído “268 **no pertenece** al conjunto que va del 0 al 255”)

ya que uno de los 4 valores, el 268, no está en el intervalo 0..255.

Nota: Con x bits podemos tener o contar  $2^x$  (dos elevado a x) valores. ¿Por qué?

Para verlo veamos varios ejemplos:

Con 1 bit ¿cuántos valores podemos contar? Pues el 0 y el 1 → 2 valores =  $2^1$

Con 2 bit “ “ “ “ Pues 00, 01, 10, 11 → 4 valores =  $2^2$

Con 3 bit “ “ “ “ Pues 000, 001, 010, 011, 100, ..., 111 → 8 valores =  $2^3$

...  
Con x bit “ “ “ “ Pues desde x ceros hasta x unos →  $2^x$  valores  
Además., siempre nos sale un 2 elevado a algo: es porque estamos en base 2 (en binario), así que el 2 es la base que estamos usando. Si estuviéramos en base 8 usaríamos un 8, si en base 341 usaríamos un 341, etc.

Luego con 8 bit podemos contar  $2^8 = 256$  valores, del 0 al 255 (255 es 256-1). Recordemos que si empezamos a contar desde 0 podemos llegar hasta el 256-1, por la siguiente fórmula:

$$\text{num\_valores} = \text{último} - \text{primero} + 1$$

Luego si contamos usando 8 bits (256 valores) y empezamos en el 0, el último valor será

$$256 = \text{último} - 0 + 1$$

que despejando la incógnita, queda

$$256 - 1 = \text{último}$$

Es decir, último = 255

Por otra parte, la dir. IP de cada ordenador debe ser única, tanto en una red como entre redes conectadas entre sí (y si están conectadas a Internet, llegamos a que la IP de cada ordenador debe ser distinta a nivel mundial, ya que Internet une redes de todo el mundo).

Esto se consigue de 2 maneras:

- Mediante una serie de organismos, como el IANA (Internet Assigned Numbers Authority) para el ámbito internacional y de EEUU, y otros organismos similares para los distintos continentes y para cada país, que se ocupan de asignar IP y grupos de IP a instituciones, ISPs (Internet Service Providers), que son las empresas proveedoras de servicios de Internet, como las telefónicas de los distintos países y particulares.

Nota: Las empresas proveedoras de servicios de Internet se abrevian como ISP (en inglés *Internet Service Providers*). Suelen ser las telefónicas en cada país: en España serían Orange, Vodafone, Movistar (antes Telefónica), ONO (ahora parte de Vodafone), etc.

- Además de la anterior, separando nuestra red LAN de las demás (y de Internet) mediante un router: [ así en Internet no se ven IP repetidas, aunque usemos las mismas IP en varias LAN, ya que el router de cada LAN “oculta” las IP de la LAN (red interna) y de esa LAN sólo se ve en Internet un equipo, el router, con IP la externa del router. Dicho de otra manera, separando nuestra LAN de otras con un router conseguimos usar las mismas IPs en nuestra LAN que en otras LAN, porque nuestro router no deja que se “vean” esas IP en las demás redes y así no hay IP repetidas. Sólo se ve de nuestra LAN una sola IP, la externa del router, que sí debe ser única a nivel mundial, es decir, asignada por un ISP u otro organismo). Detallaremos esta forma más adelante] .

Normalmente usamos las 2 maneras anteriores juntas: ¿Por qué? Porque la IP externa de nuestro router nos la asigna nuestro ISP, y además usamos un router que “oculta” las IPs que usamos en nuestra LAN cara a la red externa (la que va conectada a Internet, o forma parte de Internet). Esta red externa sólo “ve” de nuestra LAN un único aparato, el router, y una única IP, la IP del router en la red externa.

## Clases de direcciones IP

Cualquier dirección IP identifica dos cosas a la vez:

- Red en que está nuestro equipo
- Equipo (ordenador, router, AP, cámara Web, etc.) en esa red.

Es decir, en una dirección IP podemos distinguir dos partes:

- **Parte de red**: Parte de la IP que está fija (tiene el mismo valor) de un ord. a otro. **Identifica a la red** en que está el ordenador, móvil, tablet
- **Parte de host** (o de ordenador): Parte de la IP que varía de un ord. a otro. **Identifica a un ordenador**, móvil/tablet o dispositivo dentro **de esa red**.

Por ejemplo en la IP **192.168.5.14** tenemos que la **parte de red** son los **3 primeros valores empezando por la izquierda, 192.168.5**, y la **parte de host** es el **cuarto valor, 14**. Además, en esta LAN **las IP de 20 ordenadores serían:**

**192.168.5.1**  
**192.168.5.2**  
**192.168.5.3**  
...  
**192.168.5.20**

¿Por qué en este ejemplo la parte de red son 3 números y la de host 1?

El motivo es que existe una clasificación de las direcciones IP en **clases**, de la A a la E, donde cada clase tiene una parte de red y una de host distintas, que permiten usar IPs de una clase o de otra **según sea el tamaño previsto de la red** (el número máximo de ordenadores previsto en ella).

De ahí que existan:

- Clases de IP adecuadas para redes grandes (clase A)
- Clases de IP adecuadas para redes medianas (clase B)
- Clases de IP adecuadas para redes pequeñas (clase C)

además de algunas otras clases de IP de uso reservado (clases D y E, no se utilizan a la hora de montar redes).

Luego la división de las direcciones IP en clases es una manera de clasificar las IP según su uso.

La siguiente tabla resume las clases de direcciones IP: el rango de direcciones que abarca cada una, qué parte es de red y cual de host en ellas y el número de redes y host en cada una de las clases (en gris las clases reservadas –no hace falta saberlas-).

Clase	Rango de direcciones	Parte de red	Parte de host	Número de redes	Número de host / red
A	1.0.0.0 - 127.255.255.255	1 Bytes(8 bits)	3 Bytes(24 bits)	$\sim 2^8$	$\sim 2^{24}$
B	128.0.0.0 - 191.255.255.255	2 Bytes(16 bits)	2 Bytes(16 bits)	$\sim 2^{16}$	$\sim 2^{16}$
C	192.0.0.0 - 223.255.255.255	3 Bytes(24 bits)	1 Bytes(8 bits)	$\sim 2^{24}$	$\sim 2^8$
D	224.0.0.0 - 239.255.255.255	--	--	--	--
E	240.0.0.0 - 247.255.255.255	--	--	--	--

La tabla, simplificada, con sólo lo principal es: **(ESTUDIAR ESTA TABLA)**

Clase	Rango de direcciones	Parte de red	Parte de host (los bytes restantes)	Tamaño de red (nº de host / red (Lo da la parte de host))
A	1.x.x.x - 127.x.x.x	1 B	3 B	Grande, $\sim 2^{24}$
B	128.x.x.x - 191.x.x.x	2 B	2 B	Mediano, $\sim 2^{16}$
C	192.x.x.x - 223.x.x.x	3 B	1 B	Pequeño, $\sim 2^8$

Truco: para recordar de qué número a qué número van las clases A, B y C:

- A: son **unos 128** valores (del 1 al 127)
- B: son la mitad, **unos 64** valores (del 128 al 191)
- C: son la mitad, **unos 32** valores (del 192 al 223)

**PERO** no podemos usar cualquier IP libremente. Las IP que debemos usar para montar nuestras redes son las **IP de uso libre** o **IP privadas**. Las puede usar cualquiera para sus redes, sin pedir permisos ni pagar, pero la red ha de estar separada de las demás por un **ROUTER**. Podemos utilizarlas tanto particulares como organismos, empresas, etc. Las IP de uso libre (o IP privadas) **son**:

IPs de uso libre (o IPs privadas)		
Clase A (1 red posible)	Clase B (16 redes posibles)	Clase C (256 redes posibles)
<b>10.x.x.x</b>	<b>172.16.x.x</b> <b>172.17.x.x</b> <b>172.18.x.x</b> ... <b>172.31.x.x</b>	<b>192.168.0.x</b> <b>192.168.1.x</b> <b>192.168.2.x</b> ... <b>192.168.250.x</b> <b>192.168.251.x</b> <b>192.168.252.x</b> <b>192.168.253.x</b> <b>192.168.254.x</b> <b>192.168.255.x</b>

Veremos esto con más detalle en el apartado “Direcciones IP privadas. Rangos”.

- - - - - Hasta aquí el examen - - - - -

Volviendo a las partes de red y de host en una dir. IP, la tabla de arriba muestra lo siguiente:

- Las dirs. IP de clase A tienen como parte de red el 1er byte (por la izquierda) y como parte de host los 3 bytes restantes.
- Las dirs. IP de clase B tienen como parte de red los 2 primeros bytes (por la izquierda) y como parte de host los 2 bytes restantes
- Las dirs. IP de clase C tienen como parte de red los 3 primeros bytes (por la izquierda) y como parte de host el byte restante.

Luego con direcciones de **clase A** podemos tener **pocas redes** (lo da la **parte de red, 1 byte**), **pero muy grandes**, con muchos ordenadores por red (lo da la **parte de host, 3 bytes**).

En redes de **clase B** podemos tener un **número medio de redes** (lo da **la parte de red, 2 bytes** de la parte de red), **cada una de tamaño medio**, con un número medio de ordenadores (lo indica la **parte de host, 2 bytes**).

Y en redes de **clase C** podemos tener un **número muy grande de redes** de esta clase (lo indica la **parte de red, 3 bytes**), **pero pequeñas**, cada una con un número pequeño de host (dado por la **parte de host, 1 byte**).

Lo anterior se podría resumir así (es una **manera de memorizar esto** de la parte de red y de host en cada clase, no son valores exactos):

- Redes de clase A: aprox.  $2^8$  redes, cada una con aprox.  $2^{24}$  host
- Redes de clase B: aprox.  $2^{16}$  redes, cada una con aprox.  $2^{16}$  host
- Redes de clase C: aprox.  $2^{24}$  redes, cada una con aprox.  $2^8$  host.

Una **regla práctica para averiguar a qué clase pertenece una dir. IP** es **mirar el valor de su primer byte por la izquierda**; con ese valor podemos hallar la clase a que pertenece la IP. La **regla** es:

- Si el 1er byte por la izquierda está en **1..127** → IP es de clase A
- Si el 1er byte por la izquierda está en **128..191** → IP es de clase B
- Si el 1er byte por la izquierda está en **192..223** → IP es de clase C

Veamos esto con algunos **ejemplos**.

La IP 85.231.11.37 pertenece a la clase A, porque el primer valor por la izquierda, 85, está entre 1 y 127 (ambos incluidos).

La IP 175.0.0.115 pertenece a la clase B porque 175 está entre 128 y 191 (ambos incluidos).

La IP 223.1.170.3 pertenece a la clase C porque 223 está entre 192 y 223 (ambos incluidos).

**Otra regla práctica** para acordarnos de los valores de cada rango sería:

- El rango de la clase A (1..127) abarca la mitad de 1 byte, 128 valores

- El rango de la clase B (128..191) abarca la mitad de la clase A, 64 valores
- El rango de la clase C (192..223) abarca la mitad de la clase B, 32 valores

Por tanto podemos saber cual es la parte de red y de host de una IP cualquiera sin más que consultar el valor del primer byte a la izqda. de la IP: ese valor nos da la clase (A, B o C) y de ahí ya sabemos qué bytes son la parte de red y cuáles la de host.

Nota: Las IP de clase C se usan en redes pequeñas (con pocos ordenadores), como redes domésticas, la red de un aula, de una oficina, de una biblioteca, etc. Las IP de clase B se usan en redes donde sobrepasamos los 256 ordenadores (o pensamos que habrá más de 256 en el futuro), como una red de campus, una red de un polígono industrial que abarca varios edificios, etc. Y las IP de clase A se usan en redes todavía más grandes, como las de los ISP.

Dicho esto, podemos usar para nuestra red pequeña unas IP que sean de clase B o A (en vez de las de clase C que serían lógicas)? Sí, claro que podemos usar en nuestra red IPs de clase A o B, pero la práctica recomienda usar las IP que más se ajusten al tamaño de la red que tengamos (o que pueda tener en el futuro).

Por otro lado, si tenemos una red de casi 256 ordenadores (clase c), o casi 65.536 ordenadores (clase B), puede que se añadan más en el futuro, así que conviene poner a todos los equipos IPs de la siguiente clase (clases B y A respectivamente), para evitar que si nos pasamos del tamaño máximo en que estamos, no tengamos que ir luego uno por uno cambiando las IP porque se hayan añadido unos pocos equipos a la red.



## Máscara de subred y dirección IP de red

En el apartado anterior vimos que al estar las direcciones IP divididas en clases, una forma de saber cual es la parte de red y de host de la IP es averiguar la clase de esa IP

(basta mirar el primer byte por la izqda. en la IP para saber a qué clase pertenece).

Sin embargo existe otra forma de indicar cual es la parte de red y de host de una IP, que consiste en utilizar las llamadas máscaras de subred.

### MIRAR CUADRO

Nota: En realidad las máscaras de subred sirven para 2 cosas:

- Saber cual es la **parte de red y de host** de una IP
- Hallar la **IP de red** (es una IP que identifica a toda la red)

El primer uso lo vemos ahora, el segundo más abajo en este mismo apartado.

La máscara de subred es un número de 32 bit, escrito como 4 bytes separados por puntos (como en una dir. IP) cuyos valores pueden ser 0 (los 8 bit a 0) o bien 255 (los 8 bit a 1). Por ejemplo lo siguiente es una máscara de subred:

Máscara de subred en binario      11111111 11111111 11111111 00000000

Máscara de subred en decimal      255.255.255.0

Como vemos, las máscaras tienen el mismo aspecto que las dir. IP; sólo cambia los valores que puede tomar cada byte, 0 ó 255.

Cada clase de direcciones IP tiene asignada una máscara de subred por defecto. La siguiente tabla indica las máscaras de subred usadas por defecto en cada clase (los bytes a 255 indican parte de red, los bytes a 0 parte de host).

Clase	Máscara de subred por defecto	Parte de red	Parte de host
A	255.0.0.0	1er byte	3 bytes restantes
B	255.255.0.0	2 primeros bytes	2 bytes restantes
C	255.255.255.0	3 primeros bytes	1 byte restante

Luego la forma de saber qué parte de la IP es de red y qué parte es de host es consultar la máscara de subred asociada: los bytes con todos los bits a 1 (los valores 255) indican la parte de red de la IP, y los bytes con todos los bits a 0 (los valores a 0) indican la parte de host de la IP.

Normalmente cuando se escribe una IP también se indica la máscara de subred que la acompaña: siempre se da el par *IP, máscara*, no únicamente la IP. Por ejemplo

IP      172.16.0.4 → IP de clase B porque 172 está en 128..191

Máscara    255.255.0.0 → máscara de clase B por defecto

Una forma más moderna (y más corta) de escribir la máscara de subred es con una barra inclinada, /, seguida del número de bits a 1 en la máscara (es decir, el número de bits que indican parte de red).

La equivalencia entre las máscaras escritas de forma tradicional y como /xx es la siguiente:

Clase	Máscara (forma tradicional)	Máscara (forma corta = n° bits a 1 en máscara = n° bits usados como parte de red en la IP)
A	255.0.0.0	/8
B	255.255.0.0	/16
C	255.255.255.0	/24

Por ejemplo 172.16.0.4 con máscara 255.255.0.0 se escribiría  
172.16.0.4 / 16

y 192.168.5.21 con máscara 255.255.255.0 es  
192.168.5.21 / 24

Además, esta forma corta de escribir las máscaras nos lleva a otra cosa: hoy en día, podemos usar una **1 máscara de otra clase en una IP**, por ejemplo usar una máscara de clase B con una IP de clase C. También podemos usar **2 máscaras distintas a las por defecto** (que en vez de un cero tengan otro valor), por ejemplo para definir subredes dentro de una red. Estos usos nos dicen que la máscara dicta cómo usar la IP, si como clase A, B o C. A esta manera de usar las IP (mirar la máscara para saber de qué clase considerar la IP, en vez de mirar la propia IP para saber su clase) es lo que se denomina **“classless IPs”** o **IPs sin clase** (sí que la tienen, pero la define la máscara, no la propia IP).

Ejemplos de *classless IPs* (IPs con máscara distinta a la por defecto):

172.16.0.4 / 8 → Máscara 255.0.0.0, de clase A, dice que usemos la IP como de clase A

192.168.1.137 / 16 → Máscara 255.255.0.0, clase B, dice que usemos la IP como de clase B

192.168.1.137 / 26 → Máscara 255.255.255.192 (para definir subredes, el 192 dice que hay 2 bit a uno y 6 a cero, luego parte de red es 26 bit y host 6 bit)

Otro uso interesante de la máscara de subred es determinar cual es la dirección IP de la red en que se encuentra un ordenador cualquiera.

Nota: La IP de red y su función se explican en el libro en:

- p. 112 (libro antiguo);
- p. 231 (libro nuevo, recuadro azul titulado “Ejemplo 7.2”)

Para hallar la IP de red basta poner en binario la IP del ordenador y la máscara de subred asociada a esa IP, hacer un AND de los bits de IP y máscara, y el resultado es la dir. IP de la red en que se encuentra el ordenador.

Veamos un ejemplo. Queremos hallar la dirección de la red donde se encuentra un equipo que tiene la IP 192.168.0.45.

Viendo la IP sabemos que es de clase C (el valor 192 pertenece al rango 192..223, luego la IP es de clase C). Tomamos la máscara de subred usada para las IP de clase C, 255.255.255.0, y hacemos el AND (\*) de IP y máscara puestas en binario:

192 . 168 . 0 . 45	→	11000000 10101000 00000000 00101101	
255 . 255 . 255 . 0	→	11111111 11111111 11111111 00000000 (AND	
		11000000 10101000 00000000 00000000	←

El resultado es la IP de la red, 192.168.0.0, que sólo difiere de la IP del equipo 192.168.0.45 en el byte más a la derecha (la parte de host), que es 0.

Luego la dirección de red es como la del equipo (tiene la misma parte de red), pero con la parte de host puesta a 0.

(\*: Ver cómo es la operación lógica AND abajo, en el recuadro)

Nota: Las operaciones lógicas entre bits AND (Y), OR (O) operan con dos bit y devuelven un bit de resultado; la operación NOT (NO) opera con un bit y devuelve un bit. Se definen por sus tablas lógicas (es poner todas las combinaciones de dos bits y al lado el bit que devuelve la operación):

x	y	x AND y	x	y	x OR y	x	NOT x
0	0	0	0	0	0	0	1
0	1	0	0	1	1	1	0
1	0	0	1	0	1		
1	1	1	1	1	1		

Para recordar cómo funcionan las operaciones AND y OR:

- AND sólo da 1 cuando los dos bits son 1
- OR sólo da 0 cuando los dos bits son 0

La forma práctica de hallar la IP de red no necesita que hagamos todas las operaciones binarias anteriores, muy engorrosas (pasar a binario IP y máscara, hacer el AND, pasar el resultado a decimal). La IP de red será igual a la IP que nos dan, poniendo a 0 los bytes de la parte de host.

Esto se puede generalizar para las distintas clases de IP; en general, dada una dir. IP cualquiera, podemos saber la dir. IP de la red en que está sin más que poner a 0 los bytes de host de esa IP; esos bytes de host vienen indicados por la máscara de subred.

Ejemplos. Nos dan las IP de varios ordenadores, y tenemos que hallar las IP de red en que están esos ordenadores. Las IP de ordenador son:

1. 10.0.0.45 → La IP es de clase A (pq. 10 está en 1..127), luego parte de red/host es 1 byte/3 bytes → IP de red: 10.0.0.0
- |          |                |
|----------|----------------|
| -- ----- | -- -----       |
| red host | parte host a 0 |

2. 172.16.0.15 → La IP es de clase B (pq. 172 está en 128..191), luego parte de red/host es 2 bytes/2 bytes → IP de red: 172.16.0.0

----- -----  
 red host

----- -----  
 parte host a 0

3. 192.168.4.25 → La IP es de clase C (pq. 192 está en 192..223), luego parte de red/host es 3 bytes/1 byte → IP de red: 192.168.4.0

----- --  
 red host

----- --  
 parte host a 0

Recapitulando, existe una relación estrecha entre dir. IP y máscara de subred:

- Por un lado, la máscara define:
  - Qué parte de la IP del ordenador es **parte de red** (define la IP de la red)
  - Qué parte de la IP del ordenador es **parte de host** (define la IP del ordenador)
- Por otro la máscara nos da la **IP de la red** en que estamos a partir de la IP del ordenador
- Además, cada dir. IP tiene una máscara de subred adecuada a ella, llamada **máscara por defecto**
- Sin embargo, podemos usar con la IP una máscara distinta a la por defecto: sirve para **hacer subredes**. Hay 2 maneras:
  - Para IPs de clase C, usar máscaras de clase B o A, y con IPs de clase B usar máscaras de clase A.
  - También podemos usar la misma máscara por defecto, y dedicar unos bits de la parte de host para ampliar la parte de red, dando máscaras ligeramente modificadas.

Y por tanto la máscara de subred tiene 3 usos:

1. Saber cual es la parte de red y la parte de host de la IP asociada a la máscara
2. Averiguar la *IP de la red* a partir de la IP del equipo y la máscara
3. Hacer subredes dentro de la red que tenemos (por software, cambiando IPs y máscaras)

## Direcciones IP especiales (o IP reservadas)

Existen una serie de dirs. IP especiales, llamadas reservadas, que no podemos poner a nuestros equipos al configurar la red manualmente.

Nota: Las IP especiales o reservadas están:

- libro antiguo, pág. 112.
- libro nuevo, pág. 248 (sólo las de autoconfiguración, 169.254.x.x)

Entre ellas figuran las siguientes:

0.0.0.0 – Utilizada por los ordenadores cuando arrancan, hasta que se carga del todo el sistema operativo. Es una IP que no se utiliza después, sólo la emplea el software de red que implementa la pila TCP/IP del sistema operativo al iniciar el ordenador. Es decir, la IP 0.0.0.0 se utiliza como IP temporal del equipo entre que se carga el software de red del SO y este mismo software pone la IP, máscara, etc. que usará el equipo normalmente.

Nota: Además, esta IP es especial en el sentido de que no pertenece a ninguna clase (la clase A empieza en 1.0.0.0, y esta queda fuera).

127.0.0.1 – Dirección “loopback” (bucle hacia atrás, de vuelta o sobre sí mismo). Utilizada para referirnos al propio ordenador (es como un alias de la IP ghhque tenga nuestro equipo), y también para comprobar que el software de red TCP/IP funciona bien en un ordenador desconectado de la red (podemos ejecutar comandos de red en el equipo usando esta IP para ver si TCP/IP funciona). Siempre podemos usar esta IP para hacer operaciones de red donde haga falta poner la IP del propio equipo. No interfiere con la IP asignada al equipo bien por nosotros (manualmente) o bien de forma automática mediante DHCP. Por tanto es una IP que podemos usar localmente, sin salir a la red, para probar comandos de red.

Rango de 127.0.0.0 a 127.255.255.255 – Rango de direcciones “loopback”. Reservado para los mismos usos que la IP 127.0.0.1; normalmente se utiliza sólo ésta IP para referirse al propio equipo, pero algún software de red podría usar en su lugar otra dirección de este rango con la misma finalidad que la IP 127.0.0.1.

Dirs. IP con parte de host a 0 – Son direcciones de red, y no las podemos asignar a ningún equipo concreto: no hay por ejemplo un equipo con IP 192.168.0.0 (ésta es la dir. de red) sino con las IP 192.168.0.1, 192.168.0.2, ..., 192.168.0.254. La IP que acaba en 255 tampoco podemos usarla en equipos (ver abajo)

Dirs. IP con parte de host a 255 – Son direcciones de *broadcast* (difusión), y no las podemos asignar a ningún equipo concreto. Se utilizan para enviar datos a todos los equipos de la red simultáneamente

Rango de 169.254.0.0 a 169.254.255.255 – Son direcciones de “autoconfiguración” de los ordenadores. Son utilizadas por algunos PC y Mac cuando están configurados para usar TCP/IP pero no tienen asignada una IP estática (introducida a mano) y la

asignación de una IP dinámica (por DHCP) ha fallado (tal vez por no haber un servidor DHCP en la red, o por no estar activo).

Estas IP son “privadas” o de uso libre (ver apartado sobre IP privadas o libres), es decir, no deben verse desde el exterior de la red ni en Internet (son adecuadas para redes aisladas o que estén conectadas a otra red o a Internet por un dispositivo que haga NAT, como un router).

El rango de 169.254.0.0 a 169.254.255.255 corresponde a una sola red de clase B, la red con dir. IP 169.254.0.0.

## Direcciones IP privadas o IP libres. Rangos

Son ciertos rangos de direcciones IP utilizadas para “usos privados” (realmente para que las use cualquiera, para uso libre: son las IP que usaremos para montar nuestras redes). Estos usos “privados” o libres son los 2 siguientes:

1. Redes aisladas, sin conexión con otras redes (\*)
2. Redes conectadas con otra red o con Internet (también es un caso de conexión con otra red) mediante un dispositivo como el **router** que realice **NAT** (*Network Address Translation*, Traducción de Direcciones de Red, un protocolo de TCP/IP). **NAT** lo que hace es convertir (traducir) las IP libres de nuestra red en los paquetes que salen de ella, cambiando esas IP dentro de los paquetes por la IP externa del propio router.

De esta manera las IP privadas no son “vistas” por la otra red de fuera (la externa), que verá sólo la IP externa del router, detrás del cual se encuentra la red que usa IP privadas.

(\*) De este primer uso viene que llamemos “privadas” a estas IP: como la mayoría de redes aisladas (y también las del 2º caso) son redes montadas por particulares, empresas, centros de estudio, etc. Los cables de red, equipos y ordenadores son propiedad del particular, empresa, centro, etc. Y de ahí el llamar “privadas” a estas IP. Pero realmente son IP para usar por cualquiera, de uso libre, así que en este sentido serían más “públicas” que privadas.

Existen IP privadas o libres de clase A, B y C. Los rangos de estas direcciones IP privadas o libres son:

Clase	Rango de direcciones IP libres o privadas	Núm. de redes posibles	Núm. de host / red	Comentario
A	10.x.x.x	1	$2^{24}-2$ (*)	1 red de clase A grande
B	172.16.x.x - 172.31.x.x	16	$2^{16}-2$ (*)	16 redes de clase B medianas
C	192.168.0.x - 192.168.255.x	256	$2^8-2$ (*)	256 redes de clase C pequeñas

(\*) El restar 2 al número de host por red es porque no podemos usar en equipos ni la 1ª ni la última dirección IP dentro de cada red: la 1ª IP es la acabada en 0, que es la IP de la red, así que no podemos ponerla a un ordenador, mientras que la última IP es la acabada en 255, que es la dirección de broadcast o difusión para la red y tampoco podemos ponerla a un equipo.

En la tabla hay disponibles: 1 red de clase A, 16 redes posibles de clase B y 256 redes posibles de clase C. Esto se muestra mejor a continuación:

**VER MEJOR ESTA TABLA**

Clase	IP libres o privadas posibles, expresadas como IP de red (en amarillo: parte de red)	Núm. de redes posibles	Núm. de host /red	Comentario
A	10.0.0.0 → red 1	1	$2^{24}-2$ (*)	1 red de clase A grande
B	172.16.0.0 → red 1 172.17.0.0 → red 2 172.18.0.0 → red 3 ... 172.30.0.0 → red 15 172.31.0.0 → red 16	16	$2^{16}-2$ (*)	16 redes de clase B medianas
C	192.168.0.0 → red 1 192.168.1.0 → red 2 192.168.2.0 → red 3 192.168.3.0 → red 4 ... 192.168.253.0 → red 254 192.168.254.0 → red 255 192.168.255.0 → red 256	256	$2^8-2$ (*)	256 redes de clase C pequeñas

En la tabla anterior observamos que:

- Hay 1 red libre o privada de clase A disponible, la 10.0.0.0. Utilizable para montar 1 sola red muy grande (nº grande de ordenadores).
- Hay 16 redes libres o privadas de clase B disponibles, de la 172.16.0.0 a la 172.31.0.0. Utilizables para montar hasta 16 redes distintas de tamaño medio (nº medio de ordenadores).
- Hay 256 redes libres o privadas de clase C disponibles, de la 192.168.0.0 a la 192.168.255.0 Utilizables para montar hasta 256 redes distintas de tamaño pequeño (nº pequeño de ordenadores).

(\*) No todas las IP se pueden usar para hosts/equipos, el restar 2 es pq. Las IP acabadas en 0 y en 255 no se pueden poner a equipos (son de red -o de subred- y de broadcast o difusión).

Esto \*es importante\* Esto está subrayado Esto está ~~tachado~~

La idea de estas IP privadas o libres es que las puedan usar simultáneamente muchas empresas, organismos, particulares, etc. en sus diferentes redes, con la condición de que sean redes aisladas de otras o bien se conecten a otras mediante un router o una pasarela que realice NAT (es decir, que se cumpla alguno de los 2 usos privados de arriba).



Estas IP privadas son para uso libre por cualquiera, es decir, no hay que pagar a ningún ISP (proveedor de Internet) ni pedir permiso a la IANA o sus equivalentes regionales para utilizar estas IP en una red en el trabajo, en casa, en una instalación que hagamos por cuenta ajena, etc.

Estos bloques de direcciones nunca deben aparecer en Internet. Por eso sólo se utilizan en redes LAN aisladas o en redes LAN unidas a otras por un router, el cual “oculta” las IP .

## *Direcciones IP públicas*

En general, las IP que no son privadas se denominan IP públicas (\*\*): son utilizables en Internet previo registro de la IP y pago de una cantidad.

(\*\*): Esto no es del todo cierto: están las IP reservadas o especiales (nadie las puede usar, ni en Internet ni para nada), las IP de las clases D y E y otras, que aunque no son privadas tampoco son públicas.

Realmente las IP públicas deberían llamarse “privadas” ya que tenemos que registrarnos para usarlas y pagar por su uso.

Las IP públicas no se pueden usar sin más ni más, primero hay que solicitarlas al organismo regional encargado de registrar las IP en uso en Internet (el IANA central o uno regional -IANA = Internet Assigned Numbers Authority-). Estos organismos suelen delegar en empresas como los ISP (proveedores de Internet, -ISP = Internet Service Provider-), que las registran y venden a otras empresas y a particulares. Los ISP suelen ser las compañías de telefonía, como Movistar, Vodafone, Orange, etc.

## Direcciones IP estáticas y dinámicas

Existe una distinción en las IP por la forma en que se asignan al ordenador (no por su valor, son IP normales, ya sean privadas o públicas).

Las IP pueden ser de dos tipos:

- **IP estáticas** - Son las IP asignadas manualmente (tecleadas por nosotros). No cambian con el tiempo (por ejemplo al reiniciar el equipo, o al desconectarnos de la red y conectarnos más tarde), por eso se denominan IP “estáticas”.
- **IP dinámicas** - Son las IP que nos asigna automáticamente otro equipo de la red –normalmente el router-. Son IP asignadas al ordenador mediante DHCP por algún equipo en la red (como el router) que actúa como servidor de DHCP. Pueden cambiar con el tiempo (al reiniciar el ordenador, y también al desconectarnos de la red y conectarnos luego), por eso se denominan IP “dinámicas”.

Nota: DHCP significa “Dynamic Host Configuration Protocol”, es decir, protocolo de configuración dinámica de host. Es un protocolo de TCP/IP.

El funcionamiento de DHCP es como sigue.

Un ordenador pide una IP dinámica en el arranque, cuando se está cargando el sistema operativo (SO) y éste tiene puesta la opción “Usar IP dinámica” (también se la llama “usar DHCP para conseguir una IP” y de otras maneras); el ordenador pide la IP por broadcast (difusión) a todos los equipos que estén en la red, y si hay uno que actúa como servidor de DHCP (suele ser el router), contesta al ordenador y le envía por la red la IP que va a usar, que es la primera libre de una lista de IP que mantiene para asignar a equipos. Además de la IP también asigna otros datos relacionados (la máscara de subred, las IP de los servidores de DNS que utilizar y la IP de la puerta de enlace –es la IP interna del router-).

Si se desconecta el ordenador de la red y se vuelve a conectar pasado cierto tiempo, es posible que el equipo vuelva a solicitar una IP por DHCP. El motivo es que las IP dinámicas se asignan por un tiempo concreto: puede ser 1 hora, todo el día, etc. o bien mientras esté en red el ordenador al que se asigna la IP (todo esto es configurable en el servidor de DHCP, o sea, en el router). El asignar las IP dinámicas durante un tiempo es para poder “reutilizarlas”: si pasado el tiempo de uso de la IP dinámica un ordenador no la “renueva” mediante una nueva petición, esa IP pasa a estar disponible de nuevo para que el router la asigne a otro equipo. Por eso cuando el ordenador ha estado desconectado de la red más de ese tiempo puede que el servidor haya “reclamado” la anterior IP al no tener noticias del equipo desconectado y ahora la IP esté asignada a otro equipo.

Como se ve las IP dinámicas no son fijas, porque tras un reinicio o una desconexión de la red el ordenador vuelve a solicitar una IP y demás valores, y la IP que le asignan por DHCP puede ser distinta a la que usaba antes.

El protocolo DHCP (*Dynamic Host Configuration Protocol*) es parte de TCP/IP y funciona en modo cliente / servidor, donde el ordenador que pide una IP es el cliente, y hay otro equipo en la red que actúa como servidor para atender esas peticiones (puede ser otro ordenador, o bien un router o una pasarela, que suelen actuar de servidores de varios servicios, entre ellos DHCP). Muchos protocolos de TCP/IP funcionan de este modo cliente / servidor, sobre todo los del nivel de aplicación: DHCP, HTTP, FTP, los de correo electrónico, etc.

## Recordatorio: tipos de direcciones en una red

Hoy en día todos los ordenadores utilizan una red local (LAN) como Ethernet, y se conectan a otras redes (y a través de ellas a Internet) utilizando TCP/IP.

La red TCP/IP (sus protocolos) funciona siempre sobre una red LAN, que suele ser una red Ethernet. La LAN define los 2 niveles más bajos de la red, Físico y Enlace, mientras que la red TCP/IP define los 3 niveles por encima de la LAN, Interred, Transporte y Aplicación.

En cada nivel de Ethernet y de TCP/IP se definen y utilizan distintos tipos de dirección. Son las siguientes:

### SABER qué direcciones se usan en cada red (y en los niveles de TCP/IP)

Red TCP/IP (para LAN, MAN, WAN)	Direcciones en los niveles TCP/IP
	Aplicación (niveles 5, 6, 7 OSI) Direcciones: · tripla “IP : num_puerto : num_programa” ·URL “protocolo://nombre_sitio/”
	Transporte (nivel 4 OSI) Direcciones: dupla o par “IP : num_puerto”
	Interred o Internet (nivel 3 OSI) Direcciones: IP
Red Ethernet (para LAN)	Direcciones en los niveles Ethernet
	Enlace (nivel 2 OSI) Direcciones: MAC
	Físico (nivel 1 OSI) Direcciones: (no se definen, se usan las MAC)

Recordemos algo más sobre las MAC y las IP.

Las direcciones MAC son 6 bytes escritos como 6 números en hexadecimal separados por dos puntos (‘.’) o por guiones (‘-’). Por ejemplo

00-16-17-DF-02-3B

Las MAC vienen puestas en la ROM de la tarjeta de red Ethernet (ya sea cableada o inalámbrica) y no se pueden cambiar (sí se pueden cambiar de forma temporal usando algunos programas que “ocultan” la MAC real y dan en su lugar otra que ponemos nosotros).

Las direcciones IP v4 son 4 bytes escritos como 4 números en decimal separados por puntos (‘.’); las IP v6 son 16 bytes escritos como números en decimal y separados por dos puntos (‘.’). Las IP también se asocian a tarjetas de red, pero las ponemos nosotros (bien a mano o bien se asignan por DHCP automáticamente) y las podemos cambiar.

Como vemos en la tabla, casi todos los niveles de red (los de TCP/IP) manejan direcciones IP (con algún añadido, como números de puerto o números de programa) mientras que sólo los niveles LAN (Enlace y Físico) utilizan las MAC.

Luego nos puede surgir la pregunta: en la unión entre el software de red Ethernet y el software de red TCP/IP ¿Cómo hallar la MAC asociada a una IP, o la IP asociada a una MAC?

La respuesta es que TCP/IP tiene dos protocolos para esto, ARP y RARP. Su función es la siguiente:

- **ARP** (*Address Resolution Protocol*, Protocolo de Resolución de Direcciones) toma una IP y devuelve la MAC asociada.
- **RARP** (*Reverse ARP*, ARP inverso) toma una MAC y devuelve la IP asociada

Por cierto, para completar:

- **Num\_puerto**. Los números de puerto son números de 16 bits que sirven para referirnos a un programa o a una familia de programas relacionados (y también al servicio o función que realiza ese programa, o al protocolo de red que utiliza). Cada programa o servicio usa un número de puerto distinto, que lo identifica a la hora de que envíe o reciba datos por la red. Por ejemplo los navegadores se identifican por el puerto 80 y también por el 8080; los programas de FTP por el puerto 21; etc.
- **Num\_programa**. Cuando hay varias instancias (copias) de un programa ejecutándose a la vez, se le asigna a cada una un número (la 1, la 2, etc.) Por ejemplo si tenemos abiertas varias ventanas de navegador Web, la primera es la 1, la segunda la 2, la tercera es la 3, etc.

## IP del router: Consejos prácticos

EL router es un aparato que conecta dos redes.

Por tanto tiene dos enchufes de red:

- Uno para la red nuestra, la **red interna**
- Otro para la otra red (que suele estar conectada a Internet), la **red externa**.

Al tener dos tomas de red, el router tiene 2 IP: una en la red interna y otra en la externa.

En la red interna podemos poner al router cualquier IP de host, como si fuera un ordenador más. Pero se suele poner una de las IP siguientes:

- Primera IP de host en la red interna (la acabada en .1 en el byte más a la dcha.)
- Última IP de host en la red interna (la acabada en .254 en el byte más a la dcha.)

Nota: Se suele poner al router la **última IP** de host porque así podemos numerar nuestros ordenadores –ponerles etiquetas por ejemplo– empezando por el 1 (si usáramos para el router la primera IP de host, nuestros ordenadores empezarían por la IP .2, y su numeración también).

Concretando, la primera IP de host o la última IP de host de nuestra red interna será:

Clase de las IP en nuestra red interna	Ejemplo de IP* usadas en la red interna (estas son las dir. IP de red)	Primera IP de host	Última IP de host
A	10.0.0.0	10.0.0.1	10.255.255.254
B	172.16.0.0	172.16.0.1	172.16.255.254
C	192.168.0.0	192.168.0.1	192.168.0.254

\*: Usamos IP **privadas** (es decir, libres) de cada clase

En la red externa ponemos al router una IP de host de esa red externa, pero normalmente no la ponemos nosotros (al menos en routers ADSL o de cable –fibra óptica-) sino que la asigna automáticamente nuestra empresa proveedora de Internet.