

Despliegue de aplicaciones web

# Repaso Redes



Actualizado Septiembre 2024


## Licencia




**Reconocimiento – NoComercial - CompartirIgual (BY-NC-SA):** No se permite un uso comercial de la obra original ni de las posibles obras derivadas, la distribución de las cuales se debe hacer con una licencia igual a la que regula la obra original.

## Nomenclatura

A lo largo de este tema se utilizarán distintos símbolos para distinguir elementos importantes dentro del contenido. Estos símbolos son:

 Importante

 Atención

 Interesante

## ÍNDICE DE CONTENIDO

1. Introducción	4
2. Arquitectura de redes TCP/IP	4
2.1 ¿Qué es un protocolo?	4
2.2 Modelo de capas	6
2.2.1 Capa de aplicación	6
2.2.2 Capa de transporte	7
2.2.3 Capa de red (o interred, o Internet)	8
2.2.4 Capa de acceso a la red	8
2.2.5 Capa física	9
2.3 Encapsulamiento	9
2.4 Estructura de la red	11
2.4.1 Modelo cliente/servidor	12
2.4.2 Redes igual a igual	14
3. El protocolo IP	14
3.1 Configuración de un nodo	14
3.1.1 Direcciones MAC	15
3.1.2 Direccionamiento IP	16
3.1.3 Máscaras de subred	17
3.1.4 Clases de red IPv4	18
3.1.5 Direcciones de red y difusión	19
3.1.6 Direcciones IP Reservadas	20
3.1.7 Subnetting (este apartado es importante refrescarlo, pero no se va a evaluar)	22
3.1.8 CIDR	22
3.1.9 VLSM (este apartado es importante que lo conozcáis, pero no se va a evaluar)	23
3.1.10 IPv6	23
4. Bibliografía	24
5. Autores (en orden alfabético)	25

## 1. INTRODUCCIÓN

Las redes son un aspecto fundamental dentro de cualquier ámbito dentro de la informática, por lo tanto, como desarrolladores web, es muy importante que tengamos un mínimo de conocimientos sobre el funcionamiento de éstas. En este documento, se realizará una introducción a las redes.

## 2. ARQUITECTURA DE REDES TCP/IP

Internet es una red pública y global de ordenadores que están interconectados mediante el protocolo de Internet (Internet Protocol) y que se comunican mediante la conmutación de paquetes. Internet es la unión de millones de redes domésticas, académicas, comerciales y gubernamentales, es por eso que a veces es llamada red de redes.

A pesar de que hay una gran variedad de arquitecturas de red, la familia de protocolos TCP/IP se utiliza en la mayoría de las redes que conforman Internet, así como las intranets de las empresas, centros educativos, zonas Wifi, oficinas...

La denominación TCP/IP hace referencia precisamente a sus dos protocolos más importantes: el protocolo de Internet (IP) y el protocolo de transferencia de datos (TCP).

Los conceptos básicos de una red son los siguientes:

- **Nodo (hosts):** un nodo es **cualquier estación de trabajo**, servidor, impresora o cualquier otro dispositivo (teléfonos VoIP, cámaras...) que pueda ser conectado a la red, estando a disposición de ésta mientras permanezca conectado a ella.
  - **Estación de Trabajo:** todo nodo (cliente), que usualmente es un Personal Computer (PC) y que puede hacer uso de los servicios proporcionados por algún servidor.
  - **Servidor:** nodo que provee servicios a las Estaciones de Trabajo.
- **Equipos de red:** dispositivos imprescindibles para una red, sin ellos, una red no existiría. Ya que permiten la interconexión de nodos y que, por lo tanto, permiten la creación de una red (switch, routers, hub, access points...).
- **Tarjeta de red:** dispositivo físico que forma parte de los nodos y permite la conexión de estos a la red.
- **Medio de transmisión:** camino físico que conecta a todos los nodos de la red.
- **Topología:** forma física de interconexión entre los nodos de la red.
- **Protocolos y estándares:** conjunto de reglas y convenciones que controlan el intercambio de información en una red.
- **Software de red:** programas que permiten la conexión de un ordenador a la red y que puedan comunicarse a través de ella. Sistema operativo, drivers de la tarjeta de red, etc.

## 2.1 ¿Qué es un protocolo?

Un protocolo es un conjunto de normas perfectamente organizadas y mutuamente acordadas entre los participantes de una comunicación. Su misión es regular algún aspecto de la comunicación. Veamos un ejemplo para entenderlo mejor:

*Para que dos ordenadores se comuniquen, necesitan utilizar los mismos protocolos. En la vida diaria seguimos muchos protocolos sin darnos cuenta. Por ejemplo, cuando realizamos una llamada telefónica seguimos los siguientes pasos:*

1. *Seleccionamos el contacto de nuestra agenda o marcamos el número.*
2. *Pulsamos el botón de llamar.*
3. *Escuchamos el tono de llamada mientras esperamos a que descuelguen el teléfono.*
4. *Dejamos de escuchar el tono cuando la otra persona descuelga el teléfono y esperamos a que la otra persona diga algo (“¿dígame?”).*
5. *En ese momento ya podemos empezar a hablar.*
6. *Cuando hemos terminado de hablar pulsamos el botón de colgar.*

*Todos estos pasos son reglas que hemos tenido que seguir para que dos personas puedan comunicarse a través de un teléfono. Lo mismo ocurre con los ordenadores, para que se puedan comunicar, deberán seguir una serie de reglas (de protocolos).*

Puesto que en este módulo nos centramos principalmente en la web y, aunque en menor medida, en los protocolos (de aplicación) que de alguna manera son de utilidad para trabajar con ella, nos centraremos exclusivamente en ellos:

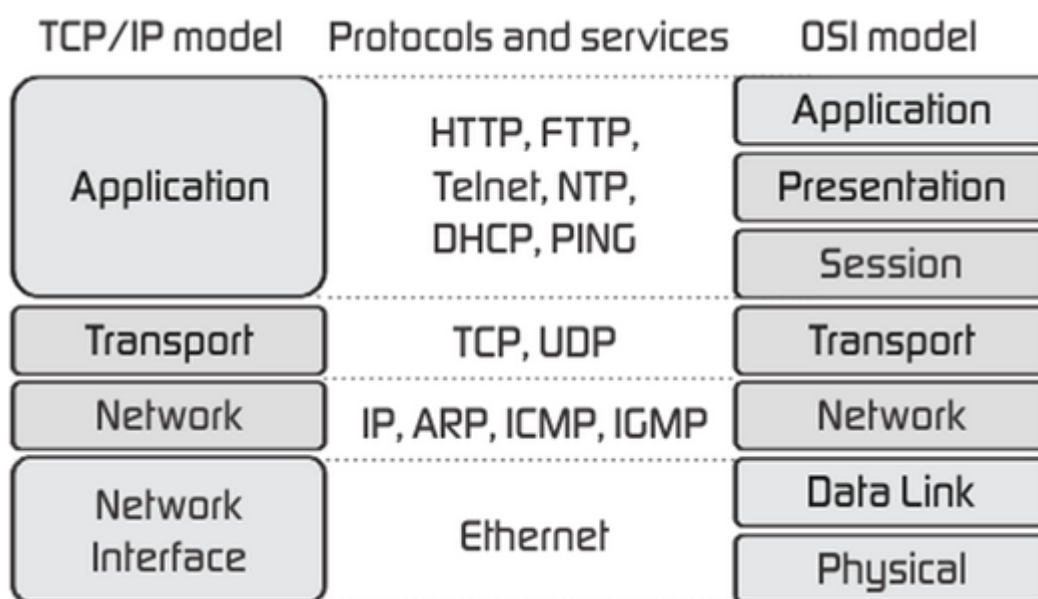
- **HTTP**: HyperText Transfer Protocol. Protocolo de comunicación para la web. Por defecto, su **puerto** es el **80**.
- **HTTPS**: HTTP Secure. Protocolo seguro de comunicación para la web. Surge de aplicar una capa de seguridad, utilizando SSL/TLS, al protocolo HTTP. Por defecto, su **puerto** es el **443**.
- **Telnet**: Es un protocolo que establece una línea de comunicación basada en texto entre un cliente y un servidor. Desde su aparición se utilizó ampliamente como vía de comunicación remota con el sistema operativo ya que permitía la ejecución remota de comandos. Con el tiempo ha ido cayendo en desuso a favor de un protocolo seguro que lo sustituye, SSH. Su **puerto** por defecto es el TCP **23**.
- **SSH**: Secure Shell. Protocolo seguro de comunicación ampliamente utilizado para la gestión remota de sistemas, ya que permite la ejecución remota de comandos. Surge como reemplazo para el protocolo no seguro Telnet. Su **puerto** por defecto es el TCP **22**.
- **SCP**: Secure Copy. Es un protocolo seguro (basado en RCP, Remote Copy) que permite transferir ficheros entre un equipo local y otro remoto o entre dos equipos remotos. Utiliza SSH por lo que garantiza la seguridad de la transferencia así como de la autenticación de los usuarios.
- **FTP**: File Transfer Protocol. Es un protocolo que se utiliza para la transferencia de archivos entre un equipo local y otro remoto. Su principal problema es que tanto la autenticación como la transferencia se realizan como texto plano, por lo que se considera un protocolo

no seguro. Su **puerto** por defecto es el **21** y envía los datos por el **puerto 20**.

- **SFTP**: SSH FTP. Es una versión del protocolo FTP que utiliza SSH para cifrar tanto la autenticación del usuario como la transferencia de los archivos. Es la opción segura al uso de un protocolo como FTP.

## 2.2 Modelo de capas

Las redes se organizan en **capas o niveles** para reducir la complejidad de su diseño, de modo que cada capa se encarga de realizar unas funciones concretas y se abstrae de los detalles de funcionamiento del resto de capas.



Fiberbit. [Model OSI vs TCP/IP](#) (Todos los derechos reservados)

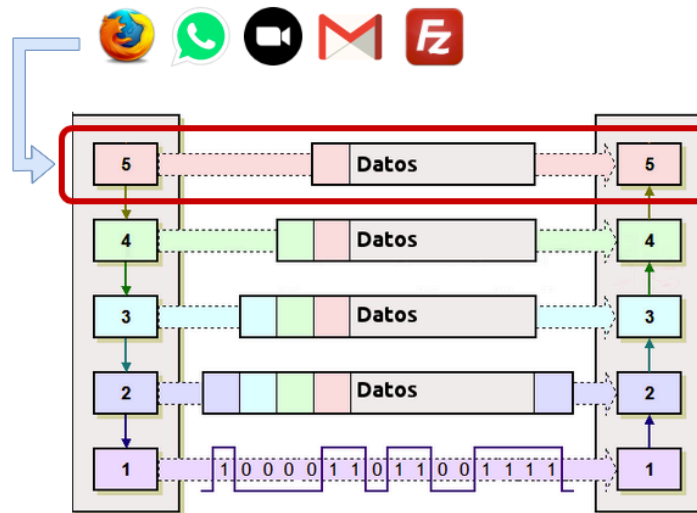
El modelo TCP/IP se ha convertido en un estándar “de facto”, por lo tanto, es el que realmente se implementa en las redes de hoy en día. OSI es un modelo que se utiliza en el ámbito académico, por lo tanto, vamos a centrarnos en conocer las capas de TCP/IP.

*La arquitectura TCP/IP tiene 4 capas (en ocasiones os vais a encontrar que tiene 5 capas, en algunos documentos separan la capa de acceso a internet por un lado y la física por otro, pero esto tampoco es muy relevante. Pero si lo veis, que no os extrañe, en este documento van a aparecer imágenes que indican 5 capas, el orden sería: 5- Aplicación, 4- Transporte, 3- Red, 2- Acceso a la red, 1- Física.*

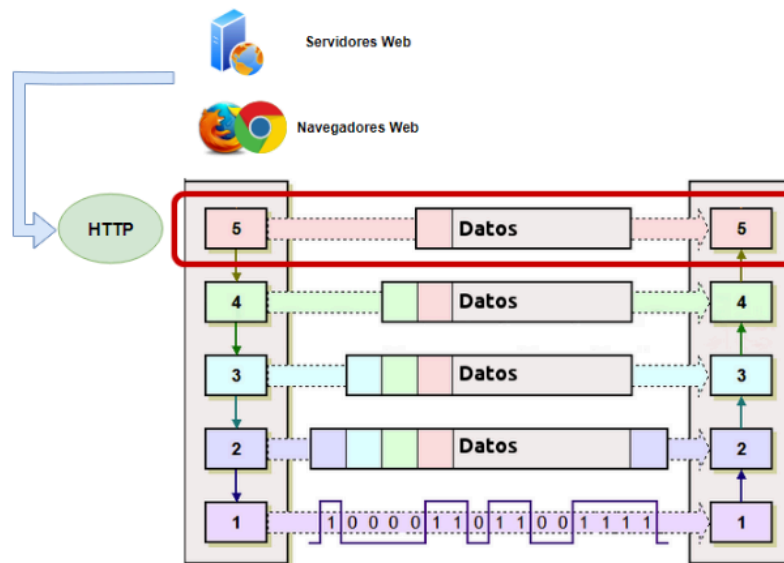
### 2.2.1 Capa de aplicación

La capa de aplicación TCP/IP se corresponde con las capas de aplicación, presentación y sesión del modelo OSI.

La capa de aplicación es la capa que los programas utilizan para comunicarse a través de la red con otros programas.



**IMPORTANTE:** en la capa de aplicación NO se encuentran las aplicaciones, como navegadores web, aplicación Whatsapp, Zoom, etc, si no los protocolos que proporcionan los servicios para que esas aplicaciones puedan comunicarse por la red, por ejemplo, HTTP (hypertext transfer protocol), FTP (file transfer protocol), SMTP (simple mail transfer protocol), SSH (secure Shell) entre otros.



### 2.2.2 Capa de transporte

La capa de transporte TCP/IP se corresponde con la capa de transporte del modelo OSI.

Los protocolos de la capa de transporte solucionan problemas como la fiabilidad y la seguridad de que los datos lleguen al destino correcto y en el orden correcto. Hay dos protocolos básicos de la capa de transporte:

- **TCP:** es un protocolo fiable orientado a la conexión que hace que un flujo de bytes de la aplicación de la máquina origen se libere sin errores hasta la aplicación de la máquina de destino en la red. Este protocolo fragmenta el flujo procedente de la capa de aplicación en mensajes más pequeños y después de encapsularlos los transmite a la capa de Interred (en algunos libros también llamada capa de Internet). En la máquina de destino, el proceso que

los recibe los reensambla para obtener el flujo original que envía hacia la capa de aplicación.

- **UDP:** Es un protocolo no fiable, sin conexión, para aplicaciones que no necesitan ni asignación de secuencia ni control de flujo como TCP, o que quieren usar sus propios medios de control. Este protocolo se usa mucho en consultas de petición y respuesta de un solo paso y en aplicaciones en las que la rapidez es más importante que la exactitud de los datos, como por ejemplo en vídeo o voz.

Uno de los aspectos más importantes de esta capa es la **multiplexación**, permitir varias comunicaciones de manera simultánea permitiendo diferenciar a quién va dirigida cada comunicación.

### 2.2.3 Capa de red (o interred, o Internet)

La capa de Internet del modelo TCP/IP se corresponde con la capa de red del modelo OSI.

Esta capa define 2 de las funciones más importantes:

**Enrutamiento o routing:** hacer que los nodos implicados en el proceso de comunicación envíen los paquetes por cualquier red y los hagan viajar de forma independiente hasta el destino. Los paquetes incluso podrían llegar al destino por caminos diferentes e incluso desordenados. En este caso, la reorganización corresponde a la capa de transporte.

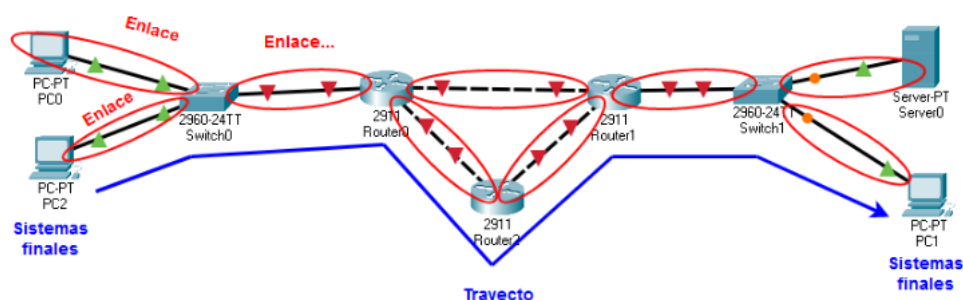
**Direccionamiento:** asignación de direcciones únicas para que los dispositivos implicados en una red se puedan identificar y por lo tanto comunicar. Este direccionamiento se realiza con direcciones IP.

Los dispositivos de red más importantes que trabajan en esta capa son los **Routers**.

### 2.2.4 Capa de acceso a la red

La capa de acceso a la red del modelo TCP/IP es equivalente a las capas de enlace y física del modelo OSI.

Mientras la capa de red se encarga de la comunicación a nivel de los caminos a seguir (del trayecto completo), esta capa se encarga de la comunicación más cercana, los enlaces de ese trayecto. La misión de esta capa es establecer una línea de comunicación libre de errores entre esos enlaces.





Los dispositivos más importantes que trabajan en esta capa son los **Switches** y el direccionamiento en esta capa es realizado a través de las direcciones **MAC**.

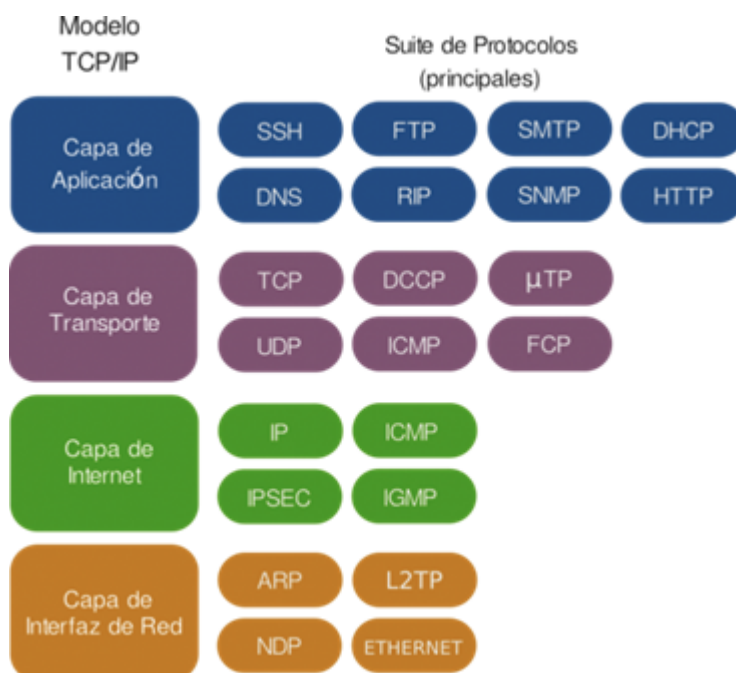
### 2.2.5 Capa física

El propósito de la capa física es transportar la corriente de bits de una máquina a otra.

La capa física es la más baja en la jerarquía de las comunicaciones. Es donde se definen las señales y los medios usados para transmitir estas señales.

Hay diferentes medios físicos para este transporte, cada uno con diferentes características respecto al ancho de banda, retardo, coste, facilidad de instalación y mantenimiento.

Aplicación	Web (HTTP)	Transf. fich. (FTP)	e-mail (SMTP)	Resol. nombres (DNS)	Vídeo streaming	Telefonía
Transporte	TCP (Transmission Control Prot.)			UDP (User Datagram Prot.)		
Red	IP (Internet Protocol)					
Enlace	Ethernet		WiFi		ADSL	
Física	Cable o Fibra (1-1000 Mbps)		Radio 2,4 ó 5 GHz (1-54 Mbps)		Cable telefónico (0,5-25 Mbs)	
					Cable coaxial 50 Ω (30-40 Mbps)	



## 2.3 Encapsulamiento

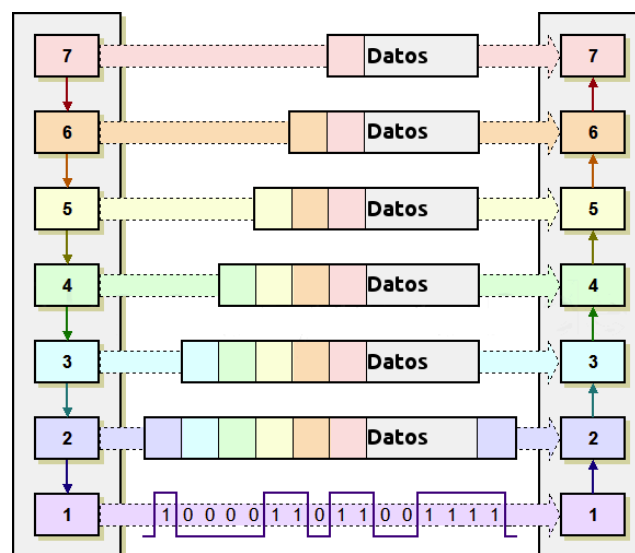
Para entender bien el funcionamiento de las capas veamos una analogía.

*Si queremos enviar una carta por el servicio de correo postal, si escribimos una carta y la metemos directamente en un buzón sin meterla en un sobre, ¿Llegará la carta al destino?*

*No, la carta no llegará porque no tiene ningún tipo de información para que el servicio de correo postal sepa qué hacer con ella. Lo mismo pasa con las comunicaciones en las redes, si quiero enviar un mensaje (correo electrónico, un Whatsapp), a ese mensaje se le tiene que añadir información extra para que pueda llegar al destino (dirección origen, dirección destino, etc, etc etc).*

A grosso modo, la encapsulación consiste en eso, en ir añadiéndole información extra al mensaje para que éste pueda llegar al destino.

El mensaje se genera en la aplicación pertinente (Whatsapp, email...), ese dato o datos pasan primero a la capa de aplicación y va atravesando cada capa donde varios protocolos le agregan información adicional hasta que se transmiten por los medios de la red. Esto comúnmente se conoce como proceso de encapsulación.



*Piensa que los **datos** serían el mensaje que queremos enviar y observa como cada capa le ha añadido más información haciendo un mensaje cada vez más grande.*

La información adicional que se le añade a los datos se denomina **cabecera** (información de cabecera).

La forma que adopta una sección de datos en cualquier capa se denomina Unidad de datos del protocolo (PDU). Durante la encapsulación, cada capa encapsula las PDU que recibe de la capa superior de acuerdo con el protocolo que se utiliza. En cada etapa del proceso, una PDU tiene un nombre distinto para reflejar su nuevo aspecto. Aunque no existe una convención universal de nombres para las PDU, en este curso se denominan de acuerdo con los protocolos de la suite TCP/IP.

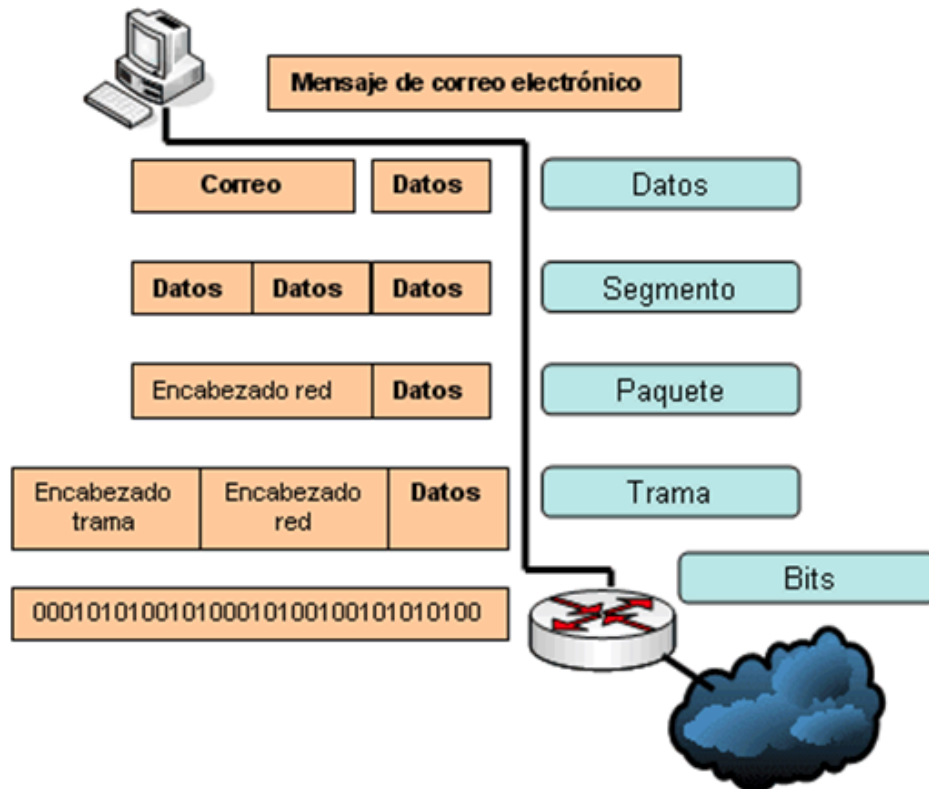
**Datos:** el término general para las PDU que se utilizan en la capa de aplicación.

**Segmento:** PDU de la capa de transporte.

**Paquete:** PDU de la capa de Internetwork.

**Trama:** PDU de la capa de acceso a la red.

**Bits:** una PDU que se utiliza cuando se transmiten físicamente datos a través de un medio.



Piensa este concepto de encapsulación como las Matrioshkas, donde la muñeca más pequeña sería realmente el dato que queremos enviar, pero lo que realmente se envía por la red es la muñeca grande con toda la información que se le ha añadido capa por capa.



Luego está el proceso inverso, la **desencapsulación**, que se realiza para ir leyendo la información

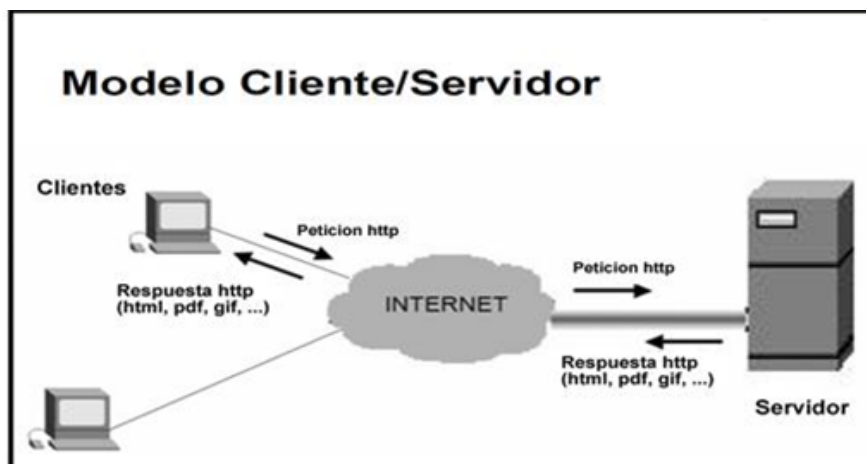
de cada capa hasta llegar a leer el dato real (muñeca pequeña).

## 2.4 Estructura de la red

Cuando la gente intenta acceder a la información en sus dispositivos, ya sea un ordenador personal o portátil, Tablet, teléfono o cualquier dispositivo conectado a la red, los datos pueden estar o no almacenados físicamente en el dispositivo, en caso de no estarlo deberíamos acceder a ellos de forma remota haciendo uso de redes **cliente/servidor** o **redes de igual a igual (P2P)**.

### 2.4.1 Modelo cliente/servidor

Una red cliente/servidor es aquella donde todos los clientes están conectados a un servidor donde se centralizan los diferentes recursos. Estos recursos están a disposición de los clientes cada vez que los solicitan. Esto hace que todas las gestiones que se realizan se concentren en el servidor, que dispone los recursos de los clientes con prioridad, los archivos que son públicos, los restringidos, los archivos de solo lectura, los que pueden ser modificados, etc.



En el modelo cliente/servidor, el dispositivo que solicita información se denomina cliente y el dispositivo que responde la solicitud se denomina servidor. Los procesos de cliente y servidor se consideran una parte de la capa de aplicación. El cliente comienza el intercambio solicitando los datos al servidor, que responde enviando uno o más bloques de datos al cliente. Los protocolos de la capa de aplicación describen el formato de las solicitudes y respuestas entre clientes y servidor. Además de la transferencia real de datos, este intercambio puede requerir información adicional, como la autenticación del usuario y la identificación de un archivo de datos para transferir.

Un ejemplo de red cliente/servidor es un entorno corporativo en el que los empleados usan un servidor de correo electrónico de empresa para enviar, recibir y almacenar correos. El cliente de correo electrónico en el ordenador emite una solicitud al servidor de correo sobre un mensaje que no ha leído. El servidor responde enviando el correo solicitado al cliente.

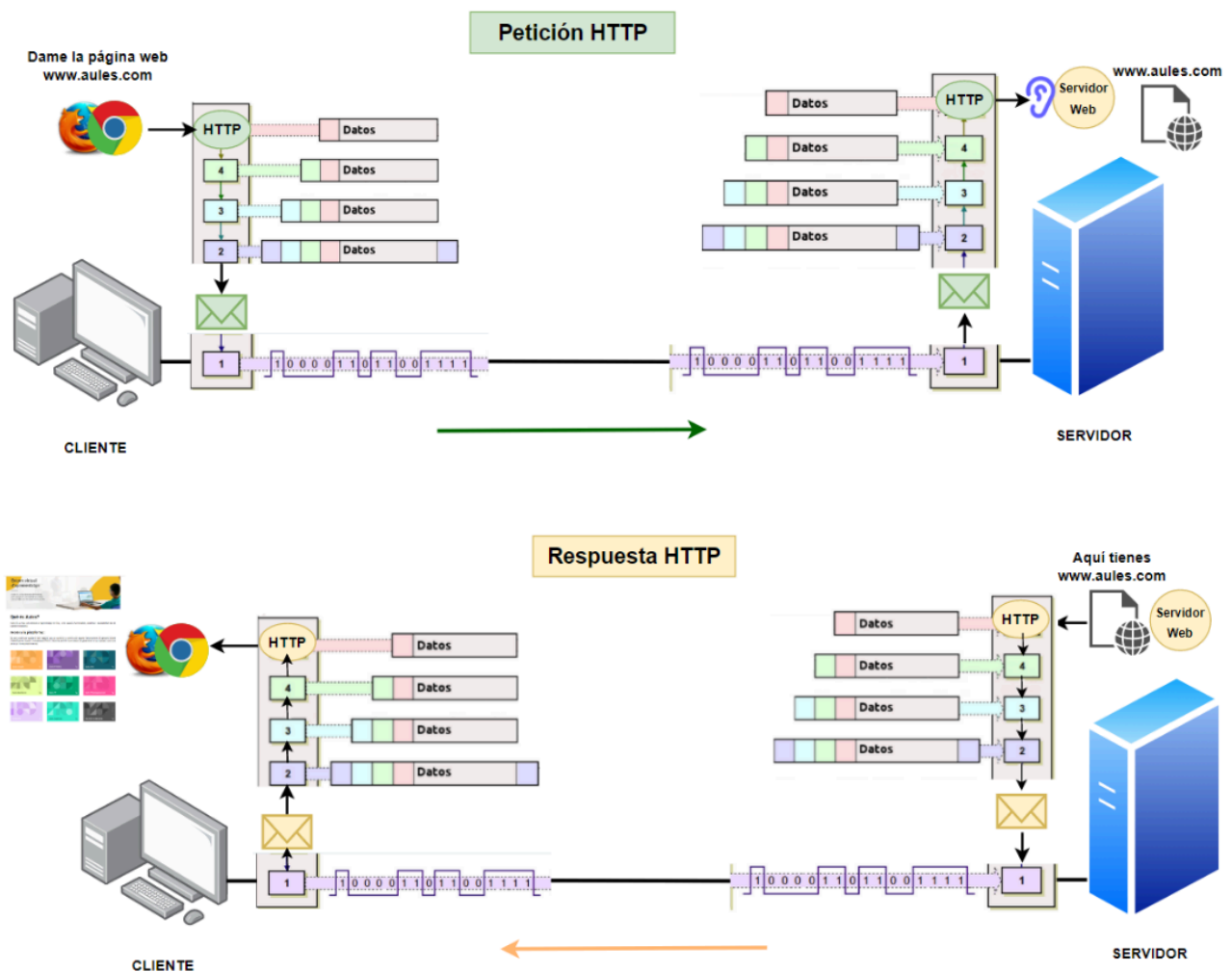
También es un modelo ampliamente utilizado en la web, donde el cliente (navegador) solicita una

página web a un servidor (por ejemplo, google.com).

Aunque los datos generalmente se describen como un flujo del servidor al cliente, algunos datos siempre fluyen del cliente al servidor. El flujo de datos puede ser el mismo en las dos direcciones e incluso ser mayor desde el cliente hacia el servidor. Por ejemplo, un cliente puede transferir un archivo al servidor para ser almacenado. La transferencia de datos de un cliente al servidor se conoce como la subida y la del servidor hacia el cliente como descarga. Piensa en una web donde te registras, toda la información que añades en el formulario tiene que ser enviada al servidor desde el cliente (navegador).

Algunos protocolos de aplicación ampliamente utilizados que emplean este modelo son HTTP/HTTPS o FTP, etc.

Aquí tienes un ejemplo completo de cliente/servidor



### 2.4.2 Redes igual a igual

En una red entre iguales, dos o más ordenadores están conectados por medio de una red y pueden compartir recursos, como impresoras o archivos, sin tener un servidor dedicado. Cada dispositivo final conectado (conocido como punto) puede funcionar como servidor y como cliente. Un ordenador puede asumir el papel de servidor para una transacción mientras está funcionando de manera simultánea como cliente para otra transacción. Los papeles de cliente y de servidor se configurarán según las solicitudes.

Un ejemplo de red entre iguales es una simple red doméstica con dos ordenadores conectados que comparten una impresora. Cada persona puede configurar su ordenador para compartir archivos, habilitar sitios de red, o compartir la conexión a Internet. Otro ejemplo son dos ordenadores conectados a una gran red que utilizan aplicaciones de software para compartir recursos a través de la red local.



## 3. EL PROTOCOLO IP

La versión más usada actualmente del protocolo IP es el protocolo IPv4, definida en el RFC 791 de 1981. Actualmente también se emplea la versión 6, IPv6 de la que hablaremos más adelante.

Todas las versiones del protocolo IP permiten el envío de paquetes entre equipos sin establecer conexión. Esto quiere decir que el ordenador de origen envía los datos al destino sin esperar ninguna notificación de que los datos se han recibido correctamente, de hecho, pueden incluso no llegar al destino. El control de errores solamente se realiza sobre la cabecera. Para realizar el envío de datos seguros, [esta capa se sirve del protocolo de la capa de transporte TCP](#).

### 3.1 Configuración de un nodo

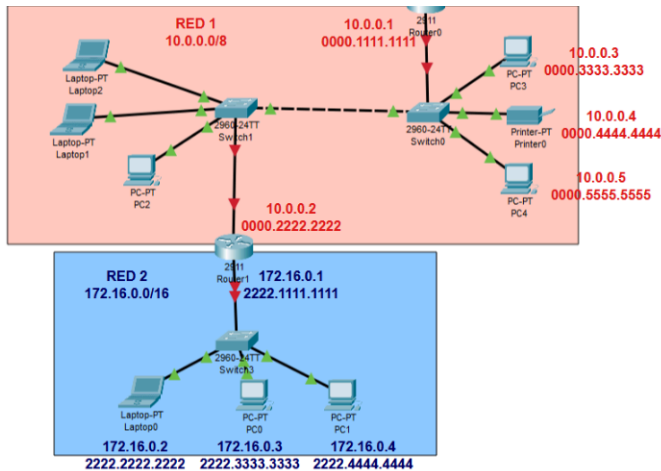
A la hora de configurar un equipo, se deberá rellenar la siguiente información:

- La **dirección IP**, ya sea de la versión 4 o de la nueva versión 6.
- La **máscara de subred**, que sirve para identificar la red o subred.

Si la comunicación se establece con equipos que se encuentran en otras subredes o con Internet, se necesita, además:

- La dirección de la **puerta de enlace** (Gateway) o pasarela que se corresponde con el router y con el cual se dirige el tráfico a Internet o a otras subredes.

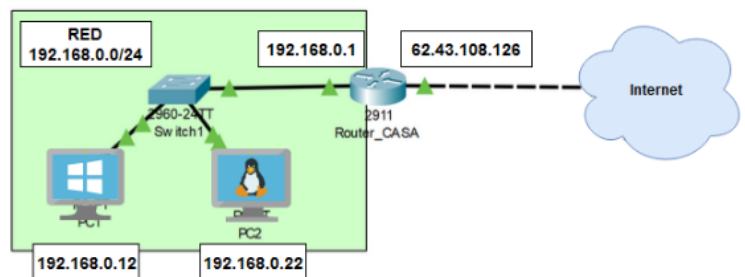
- Las direcciones IP del **servidor DNS**.



Piensa en la puerta de enlace como una **puerta de salida** de los mensajes a otras redes.

En este ejemplo, si la red azul quisiera comunicarse con la red roja, necesita una puerta de salida para llegar a otro lugar, esa puerta es el router, éste se encargará de reenviar el mensaje a la otra red. Por lo tanto, la dirección de puerta de enlace que se debería añadir a cada equipo de esa red, sería la 172.16.0.1

Aquí otro ejemplo más familiar. Para que nos podamos comunicar con internet, necesitamos indicarles a los equipos cual es la puerta de salida a internet, en este caso la puerta es el Router\_CASA, por lo tanto, la puerta de enlace será la 192.168.0.1



El protocolo IP tiene las siguientes funciones:

- **Enrutamiento o routing:** elegir el camino más adecuado para enviar los paquetes.
  - Las características de envío de este protocolo son las siguientes:
    - No orientado a la conexión: cada paquete puede seguir un camino distinto. Por lo cual pueden llegar desordenados.
    - No fiable. Los paquetes pueden perderse, dañarse o llegar con retraso.
- **Direccionamiento:** proporciona un mecanismo de direccionamiento lógico (direcciones IP).

### 3.1.1 Direcciones MAC

El objetivo de toda comunicación es hacer llegar un mensaje de origen a destino, para ello, al igual que en una carta de código postal, necesitamos direcciones.

Para identificar un ordenador en una red, necesitamos concretamente dos:

- Dirección IP (dirección lógica)
- Dirección MAC (dirección física)

Las direcciones MAC no forman parte del protocolo IP, si no que estás direcciones se emplean en la capa de acceso a internet o capa de enlace.

Por lo tanto, para el tratamiento de las comunicaciones a nivel de **enlace**, los NIC (tarjetas de red) llevan asociada una **dirección física**, o dirección hardware, llamada MAC, que viene programada de



serie por el fabricante del NIC, y que identifica al adaptador de red a nivel mundial.

Veamos la estructura de la MAC con un ejemplo:

01:1F:D0:C8:D6:6E

Vendor ID (identificador del fabricante) : Device ID (identificador del dispositivo)

En este caso, el código 01:1F:D0 corresponde al fabricante GIGA-BYTE TECHNOLOGY CO. (se pueden consultar en la siguiente página web: [http://www.coffer.com/mac\\_find/](http://www.coffer.com/mac_find/)).

En Windows, el comando **ipconfig /all** nos muestra información de todos los adaptadores instalados en el equipo. Entre esa información está la dirección física, que es la MAC del adaptador. En Linux, el comando que se emplea es **ifconfig**, con resultados similares.

```

Microsoft Windows [Versión 10.0.18363.1016]
(c) 2019 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Silvia>ipconfig /all

Configuración IP de Windows

Nombre de host. . . . . : SILVIA
Sufixo DNS principal . . . . :
Tipo de nodo. . . . . : híbrido
Enrutamiento IP habilitado. . . : no
Proxy WINS habilitado . . . . : no

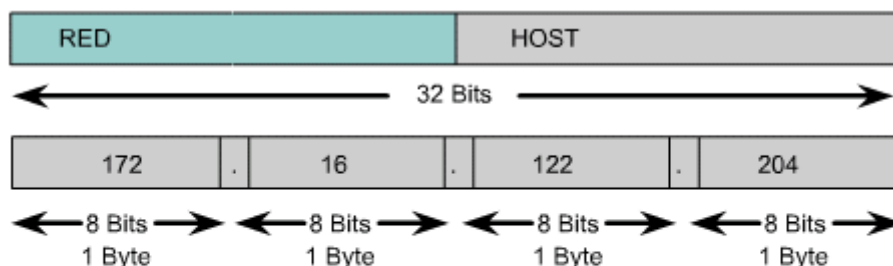
Adaptador de Ethernet Ethernet:

Sufixo DNS específico para la conexión. . :
Descripción. . . . . : Realtek PCIe GbE Family Controller
Dirección física. . . . . : D4-5D-64-00-0D-1B
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::dc90:ca07:4028:2507%12(Preferido)
Dirección IPv4. . . . . : 192.168.0.3(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : sábado, 15 de agosto de 2020 12:02:21
La concesión expira . . . . . : sábado, 15 de agosto de 2020 13:02:21
Puerta de enlace predeterminada . . . : 192.168.0.1
Servidor DHCP . . . . . : 192.168.0.1
IAID DHCPv6 . . . . . : 114580836
DUID de cliente DHCPv6. . . . . : 00-01-00-01-26-50-FC-D0-D4-5D-64-00-0D-1B
Servidores DNS. . . . . : 192.168.0.1
NetBIOS sobre TCP/IP. . . . . : habilitado

```

### 3.1.2 Direccionamiento IP

La dirección IP es un número de 32 bits que identifica a cada una de las máquinas que están conectadas a Internet o a cualquier red, y también la red a la que pertenecen. Una parte de la dirección IP, según sea su máscara de red, sirve para identificar a la red y la otra para identificar al equipo.



Una dirección IP siempre se divide en una parte de red y una parte de host. En un esquema de direccionamiento con clases, estas divisiones tienen lugar en los límites de los octetos.



192.168.0.75

Octeto\_1.Octeto\_2.Octeto\_3.Octeto\_4

Cada número es un octeto (8 bits) que se suele representar con un número en decimal. Por lo tanto, cada octeto de la dirección IP será un número que podrá tomar un valor entre 0 y 255 (o sea, 256 valores posibles).

También se puede representar en binario, en bloques de 8 bits separados por puntos:

11000000.10101000.00000000.01001011

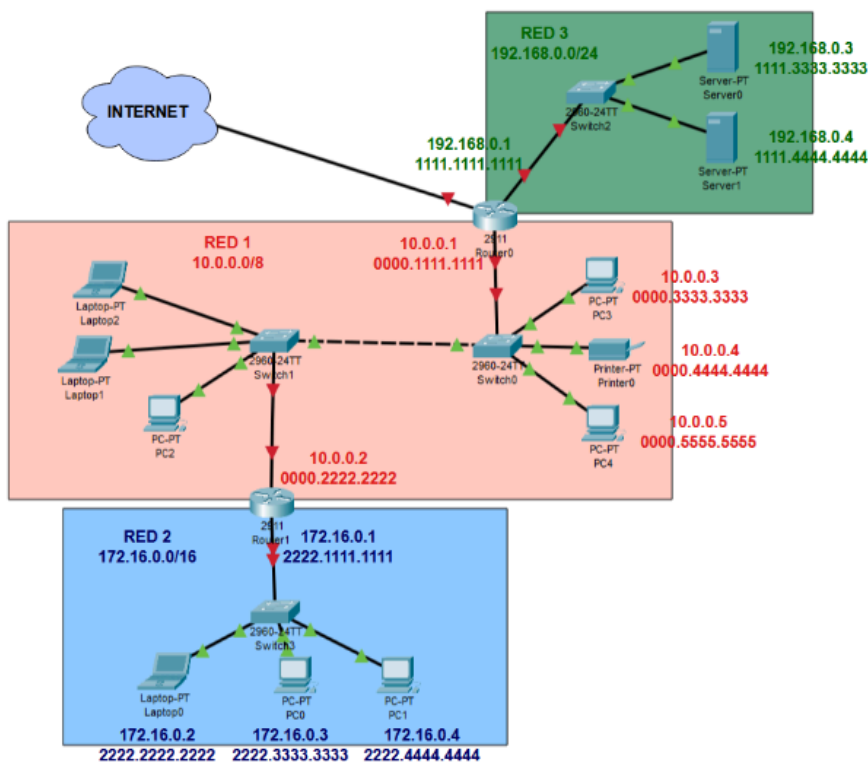
### 3.1.3 Máscaras de subred

En las direcciones IP, la parte más a la izquierda de la dirección IP es lo que se llama el **identificador de red**, y la parte más a la derecha es el **identificador de equipo** dentro de esa red.

Ejemplo: 192.168.0.3

(equipo número 3 de la red cuyo identificador es 192.168.0)

**Todos los equipos que formen parte de la misma red deben tener el mismo identificador de red, pero distintos identificadores de equipo.**



Aquí tienes un ejemplo de 3 redes distintas:

- Red verde: el identificador de la red es 192.168.0 y dentro de esa red está el equipo 3 y 4.
- Red roja: el identificador es 10 y los equipos serían el 0.0.3, 0.0.4, 0.0.5
- Red azul: el identificador es 172.16 y los equipos serían el 0.2, 0.3, 0.4

La cantidad de octetos destinados al identificador de red y, por tanto, al de equipo, es una cantidad variable que depende de la **máscara de subred**: un número-patrón similar a la IP en estructura y que nos indica qué parte de la IP es identificador de red y qué parte es identificador de equipo.

En este apartado trabajaremos sólo con redes con clase (se ven las redes sin clase más adelante), es decir, los octetos de la máscara sólo van a ser 0 o 255. En este caso, los octetos de la IP que se

correspondan con aquellos octetos de la máscara que lleven el valor 255 formarán el identificador de red, y los que lleven el valor 0 formarán el identificador de equipo.

Ejemplos de uso de máscaras de subred:

IP: 80.9.108.62 Máscara: 255.0.0.0

IP: 172.16.35.107 Máscara: 255.255.0.0

IP: 216.157.2.1 Máscara: 255.255.255.0

Las direcciones con sus máscaras de subred se pueden expresar de varias formas:

a) Notación **decimal**, cuatro octetos decimales acompañando a la dirección IP:

172.16.3.45 / 255.255.255.0

b) Notación **binaria**, octetos binarios separados por puntos (no suele usarse para representar, pero sí para hacer cálculos con ella):

10101100.00010000.00000011.00101101

11111111.11111111.11111111.00000000

c) Notación prefija o **CIDR**, un número decimal que indica el número de "unos" que tendría la máscara de subred si la expresamos en binario:

172.16.3.45 / 24

(si te fijas en la imagen anterior donde hemos visto ejemplos de redes, se ha utilizado esta notación)

### 3.1.4 Clases de red IPv4

Hay tres clases principales de direcciones IP

- [Clase A](#): el primer octeto identifica la red.
- [Clase B](#): los dos primeros octetos identifican la red.
- [Clase C](#): los tres primeros octetos identifican la red.

Además, de dos clases adicionales que se tratan por separado:

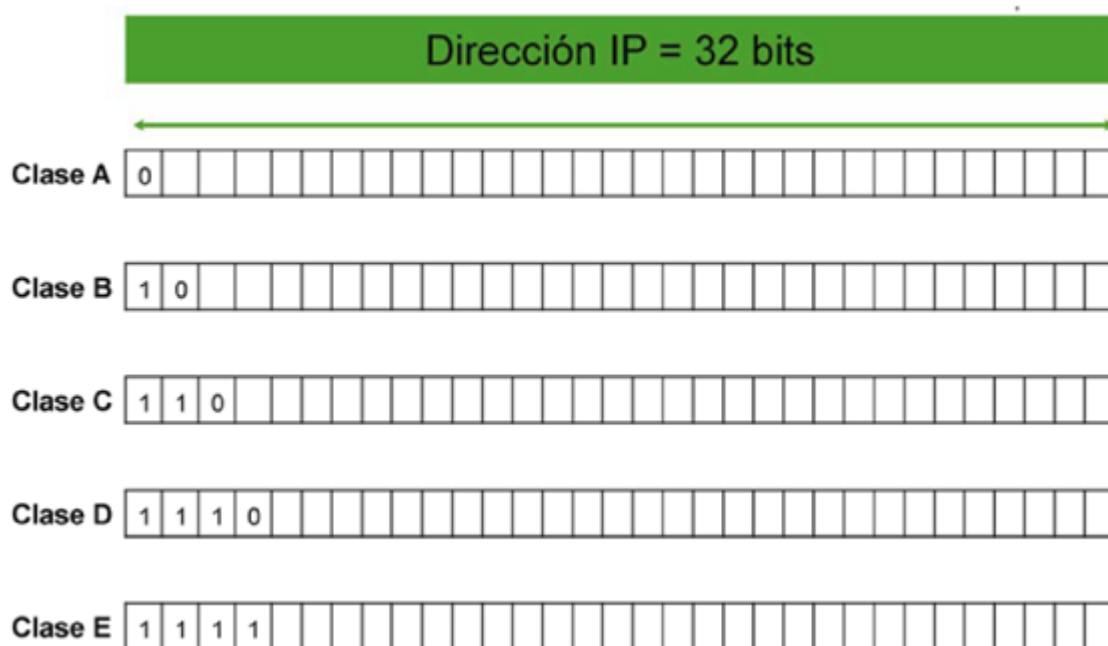
- Clase D: Se trata de un conjunto de direcciones reservadas para multidifusión.
- Clase E: se trata de una clase reservada.

Clase	Rango de IPs	Nº Redes	Nº Equipos por red	Máscara
A	0.0.0.0 - 127.255.255.255	$2^7 = 128$	16777214	255.0.0.0 - /8
B	128.0.0.0 – 191.255.255.255	16384	65534	255.255.0.0 - /16
C	192.0.0.0 – 223.255.255.255	2097152	254	255.255.255.0 - /24
D	224.0.0.0 – 239.255.255.255	Clase no usada, reservada para mensajes de difusión		

E	240.0.0.0 – 255.255.255.255	Clase no usada, pensada inicialmente para ampliar el espacio de direcciones IPv4
---	-----------------------------	--

Para saber a qué clase pertenece una IP basta solo con ver sus primeros bits:

- Si el primer bit es 0, entonces la IP es de clase A.
- Si el primer bit es 1 y el siguiente es 0 entonces es de clase B.
- Si los dos primeros son 1 y el tercero 0 entonces es de clase C.



### 3.1.5 Direcciones de red y difusión

A. **Dirección de subred:** es la **primera dirección IP** de una red, representa a esa red entera y **no puede ser asignada a un equipo** de la misma. Todos los equipos de una red física cuya dirección de subred sea la misma, estarán en la misma red. Se calcula de la siguiente forma (ejemplo):

**Dirección IP y máscara:** 192.168.3.45 / 24

**Dirección IP (en binario):** 11000000.10101000.00000011.00101101

**Máscara (en binario):** 11111111.11111111.11111111.00000000

**Operación AND (bit a bit):** 11000000.10101000.00000011.00000000

**Dirección de subred:** 192.168.3.0 (es la anterior en decimal)

Truco: realmente no es necesario hacer la operación AND, con poner a ceros los octetos de hosts y dejando los octetos del identificador de red igual, conseguimos obtener la dirección IP de subred.

(identificador de red).ceros

(Este truco sirve únicamente para redes con clase).

- B. **Dirección de difusión:** es la **última dirección IP** de una subred, y **no puede ser asignada a un equipo**. Sirve para cuando un equipo quiere enviar un paquete de difusión a todos los equipos de su subred. Todos los equipos de una misma subred tienen la misma dirección de difusión. Se calcula de la siguiente forma (ejemplo):

**Dirección IP y máscara:** 192.168.3.45 / 24  
**Dirección de subred:** 192.168.3.0 (calculada antes)  
**Dirección de difusión:** 192.168.3.255

En redes con clase se calcula **sustituyendo los octetos del identificador de equipo por 255 o mejor dicho, todo a unos**.

### 3.1.6 Direcciones IP Reservadas

Para evitar conflicto de IP con los equipos que ofrecen servicios en la red internet, existen unos rangos de direcciones reservados para los equipos de **redes privadas** (redes LAN sobre IP en las que sus equipos no forman parte de internet, aunque tengan acceso a la misma a través de routers):

**Definidos en RFC 1918 (rangos utilizados para redes privadas):**

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

**Definido en RFC 3927 (direcciones de enlace local)**

**169.254.0.0 - 169.254.255.255** (se asignan aleatoriamente junto a la máscara /16 a equipos en una LAN en la que no existe un servidor DHCP para auto configuración de IP. En Windows se emplea el protocolo APIPA).

**Definido en RFC 3330 (referencia al propio equipo)**

Define que debe existir un rango de direcciones reservado para hacer referencia al propio equipo en la red o **localhost**. El rango, llamado rango de direcciones *loopback*, es el siguiente:

**127.0.0.0 - 127.255.255.255**

Aunque en la práctica sólo se emplee la dirección **127.0.0.1 / 32** para *localhost*, el documento **RFC 3330** deja clarísimo en su página 1 que *"ninguna dirección de este rango debería aparecer en cualquier red, sea donde sea"*.

Se emplea principalmente para la comprobación de la existencia de software TCP/IP en un equipo, usado con el comando **ping** (para cualquier SO):

## ping 127.0.0.1

La red cero también se considera una dirección especial, que va desde la 0.0.0.0 hasta la 0.255.255.255

Existen **dos formas** de asignar IPs a equipos en una LAN:

- a) **Asignación estática:** asignamos de forma manual la configuración a nivel de red de un equipo; básicamente: dirección IP, máscara de subred, configuración de la/s puerta/s de enlace y de los servidores DNS.
- b) **Asignación automática o dinámica:** hay dos formas de que se asigne la IP automáticamente a un equipo de una red:
  - a. **por DHCP (*Dynamic Host Configuration Protocol*):** DHCP es un protocolo de la capa de aplicación que permite asignar configuración de red a los equipos que se conectan a una red. Para ello, debe existir un equipo en la red que tenga instalado un software servidor DHCP, puede ser un servidor o podría ser un router que permita tener configurado este servidor DHCP, como los routers que nos proporcionan los ISP. Este servidor DHCP asigna una configuración completa de IP a los equipos clientes que así lo soliciten y que estén configurados para trabajar con DHCP (utiliza el modelo cliente/servidor). Aquí tienes un vídeo que lo explica más en detalle: <https://www.youtube.com/watch?v=K07wzpcKrsk>
  - b. **con dirección de enlace local:** si no hay servidor DHCP en la red, aquellos equipos configurados como clientes DHCP obtienen, tras un tiempo, direcciones aleatorias del tipo **169.254.x.x/16**. En sistemas Windows la asignación se hace mediante el protocolo **APIPA** (*Automatic Private IP Addressing*, direccionamiento automático de IP privada).

Las direcciones IP se clasifican en:

- **Direcciones IP públicas:** utilizadas para conectarse a internet:

IANA (Internet Assigned Number Authority) es la autoridad encargada de asignar éstas direcciones IPs en Internet. *IANA fue sustituida en 1998 por ICANN (Internet Corporation for Assigned Names and Numbers).*

Normalmente en una empresa solo un host tiene conexión a Internet (solo un host tiene una IP pública) y el resto de hosts de la red local acceden a Internet a través de este.

Así solo el host conectado a Internet necesita reservar una dirección de IP (pública) con ICANN.

- **Direcciones IP privadas:**

Sin embargo, los otros hosts de la empresa necesitarán una dirección IP para comunicarse entre ellos. ICANN ha reservado una serie de direcciones IP para los host de dentro de la red local. Son las denominadas **IPs privadas (hemos visto este rango de IPs anteriormente, las que hemos denominado “rangos utilizado para redes privadas”)**.

### 3.1.7 Subnetting (este apartado es importante refrescarlo, pero no se va a evaluar)

Es un procedimiento por el cual podemos dividir, a nivel de IP, un rango de red en varias redes más pequeñas de tamaño variable (o subredes).

De esta forma, en una misma infraestructura física de red podemos tener diferentes subredes IP en un mismo rango de IP.

**EJEMPLO:** una corporación recibe del administrador de internet el rango de direcciones IP públicas **221.37.1.x/24** (máscara **255.255.255.0**). El administrador de la red local puede subdividir la red en dos subredes:

- una subred con capacidad para 126 equipos para soporte técnico
- una subred con capacidad para 64 equipos para atención comercial

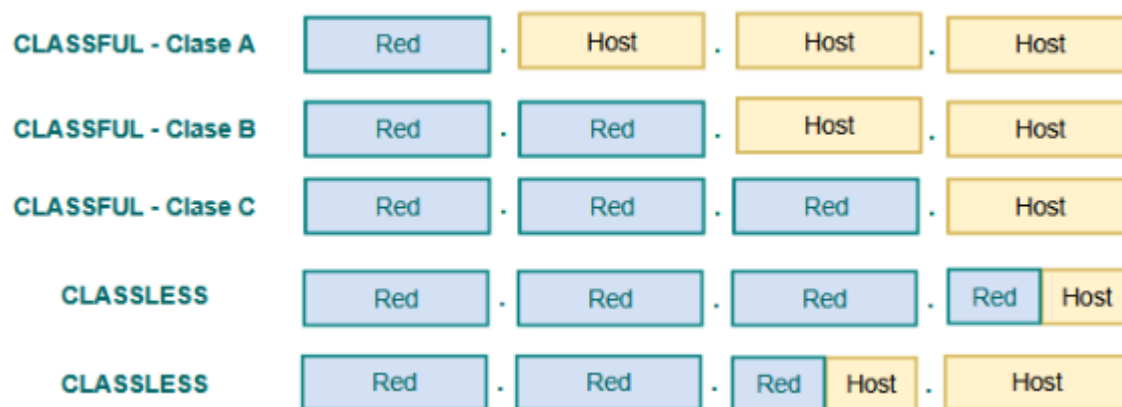
Cuanto más grande es una red, más lento es el tráfico y más lenta es su gestión.

El procedimiento de *subnetting* se realiza para organizar una red grande en **dominios de difusión más pequeños y eficientes**.

Generalmente, la unión de dichas subredes se realizará a través de **routers**.

### 3.1.8 CIDR

Hemos hablado anteriormente de IPs con clase, pero trabajar con ese tipo de IPs es ineficiente porque se desperdician muchas direcciones IP, por ello, existe otra forma de trabajar empleado en la actualidad y es el modelo CLASSLESS o sistema **CIDR** (*Classless Inter-Domain Routing*), que, aunque respeta la organización inicial por clases, permite también trabajar sin ellas:



Como vemos, con el nuevo sistema, podemos tener un octeto que comparta los bits para red y para hosts.

Ejemplo de cálculo de la dirección de red y difusión, calcular la dirección de subred y de difusión de la siguiente dirección IP: 192.168.7.12 / 22

- 1) Convierte la máscara de subred a formato binario y decimal:

11111111.11111111.11111100.00000000  
255.255.252.0

- 2) Localiza el octeto crítico en la IP y la máscara:

192.168. 7 .12  
255.255. 252 .0

- 3) Los bits correspondientes a la parte de red déjalos como están y el resto ponlos a 0:

$7_{(10)} = 00000111$   
 $252_{(10)} = 11111100$   
 $00000100 = 4_{(10)}$

- 4) La **dirección de subred** será:

- la misma que la IP hasta el octeto crítico: 192.168
- el nuevo número obtenido en el paso anterior: 4
- '0' en el resto (si los hubiera)

(en nuestro ejemplo) **192.168.4.0**

- 5) La **dirección de difusión o broadcast** será:

- la misma que la IP hasta el octeto crítico: 192.168
- Hacemos el paso 3, pero en lugar de poner a 0 los bits que no corresponden con la parte de red, los ponemos a 1 y obtenemos el nuevo número:

$7_{(10)} = 00000111$   
 $255_{(10)} = 11111111$   
 $00000111 = 7_{(10)}$

- '1' en el resto (si los hubiera)

(en nuestro ejemplo) **192.168.7.255**

### 3.1.9 VLSM (este apartado es importante que lo conozcáis, pero no se va a evaluar)

VLSM significa: **máscaras de subred de tamaño variable**, representan otra de las tantas soluciones que se implementaron para evitar el agotamiento de direcciones IP en IPv4. Consiste en adaptar la máscara de subred haciendo que sea variable y que se pueda utilizar varias máscaras en la misma red, de esta forma, se desperdician menos direcciones IP.

### 3.1.10 IPv6

IPv6 (Internet Protocol version 6) es una versión del protocolo IP, definida en el [RFC 2460](#) y diseñada para reemplazar a IPv4 ([Internet Protocol version 4](#)), que es la versión actualmente extendida.

### ¿Por qué IPv6?

En IPv4, las direcciones son de 32 bits, lo que conlleva un límite de  $2^{32}=4.295.967.296$  direcciones distintas, número que se consideró suficiente cuando se diseñó el protocolo (año 1973).

Debido al auge de Internet, y a la variedad de equipos conectados (lo que se conoce como [Internet de las Cosas](#) - Internet of Everything), las direcciones IPv4 se están agotando, especialmente en

países altamente poblados de Asia (China, India), continente al cual la IANA ya ha entregado (principios de 2011) el último bloque de direcciones IP disponible para él.

Este problema ya se veía venir desde principios de la década de los 90, en la cual se introdujo el diseño de redes sin clase (CIDR) para realizar subnetting y aprovechar mejor las direcciones IPv4. Pero no ha sido suficiente. Para saber más:

- [IPv6](#) (Wikipedia).
- [IPv6.es](#), del Ministerio de Industria.
- [\*"Hoy se anuncia el fin de las direcciones de Internet"\*](#), noticia aparecida en ABC el 3 de febrero de 2011.

#### 4. BIBLIOGRAFÍA

- [1] [https://despliegue.codeandcoke.com/doku.php?id=apuntes:servidores\\_web](https://despliegue.codeandcoke.com/doku.php?id=apuntes:servidores_web)
- [2] <http://logongas.es/doku.php?id=clase:daw:daw:start>
- [3] <https://pedroprieto.github.io/categories/>
- [4] <https://git-scm.com/book/es/v2/Fundamentos-de-Git-Trabajar-con-Remotos>
- [5] <https://github.com/pedroprieto/curso-github/>
- [6] [https://corriol.github.io/sxe/UD01/1\\_arquitectura\\_de\\_xarxa\\_tcpip.html](https://corriol.github.io/sxe/UD01/1_arquitectura_de_xarxa_tcpip.html)
- [7] <https://www.blai.blog/2018/12/tipos-de-red-en-virtualbox.html>
- [8] <https://sites.google.com/site/wikiredespro/sistemas-operativos-ii/crear-red-entre-maquina-virtual-y-maquina-host-en-virtualbox>
- [9] Desplegament d'aplicacions web. Institut Obert de Catalunya
- [10] Instalación y mantenimiento de servicios de redes locales. Francisco J. Molina. Rama
- [11] <https://www.solvetic.com/tutoriales/article/5771-como-cambiar-nombre-de-grupo-de-trabajo-en-windows-10/>
- [12] <https://support.microsoft.com/es-es/help/17145/windows-homegroup-from-start-to-finish>
- [13] <https://support.microsoft.com/es-es/help/4027674/windows-10-share-files-in-file-explorer>
- [14] <https://docs.microsoft.com/es-es/windows-server/> — documentación muy interesante acerca de la configuración de un servidor en Windows de principio a fin.
- [15] <https://docs.microsoft.com/es-es/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>
- [16] <https://www.solvetic.com/tutoriales/article/7486-como-crear-usuarios-y-grupos-dominio-active-directory-en-windows-server-2019/>
- [17] <https://support.microsoft.com/es-es/help/196464>
- [18] <https://www.solvetic.com/tutoriales/article/3033-como-abrir-y-editar-archivo-hosts-en-windows-10-8-7/>
- [19] <https://www.zeppelinlinux.es/configuracion-del-archivo-etc-resolv-conf/>
- [20] <https://www.muylinux.com/2016/09/23/carpeta-ubuntu-16-04-samba/>
- [21] <https://usuariodebian.blogspot.com/2019/02/samba-compartir-carpetas-en-red.html>
- [22] <https://geekytheory.com/copiar-archivos-a-traves-de-ssh-con-scp>



## 5. AUTORES (EN ORDEN ALFABÉTICO)

A continuación ofrecemos en orden alfabético el listado de autores que han hecho aportaciones a este documento.

- Silvia Amorós Hernández
- David Folgado De la Rosa
- Miguel Mira Flor
- Miguel Ángel Tomás Amat