

**REDES**

# ÍNDICE

<b>1. Introducción</b>	<b>3</b>
<b>2. Clasificación de redes</b>	<b>4</b>
<b>3. Arquitectura de Red</b>	<b>6</b>
<b>4. Modelo OSI</b>	<b>7</b>
<b>5. Modelo TCP/IP</b>	<b>10</b>
Capa 1. Acceso a la red/enlace/subred	10
Capa 2. Red/Internet	10
Capa 3. Transporte	10
Capa 4. Aplicación	11
4.1 Acceso	11
4.2 Red	13
4.3 Transporte	15
4.4 Aplicación	17
<b>6. Topologías de red</b>	<b>18</b>
Componentes de un red informática	20
Los switches y routers en el modelo TCP/IP	21
Tipos de Subredes	24
<b>Glosario de Términos</b>	<b>25</b>

# 1. Introducción

De acuerdo con Andrew S. Tanenbaum, una red de computadoras, también llamada red de ordenadores o red informática, es un conjunto de equipos informáticos conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información y recursos. . Estos dispositivos pueden ser computadoras, servidores, impresoras, teléfonos inteligentes, tablets, dispositivos IoT y otros equipos electrónicos.

En términos más simples, una red informática es como una telaraña digital que conecta diferentes dispositivos.

## Funciones de una red informática

- **Compartir información:** Permite a los usuarios acceder a archivos, datos y otros recursos almacenados en otros equipos de la red.
- **Comunicación:** Facilita la comunicación entre usuarios a través de diferentes herramientas como el correo electrónico, la mensajería instantánea o las videollamadas.
- **Compartir recursos:** Permite compartir recursos como impresoras, escáneres o dispositivos de almacenamiento.
- **Acceso a internet:** Brinda acceso a internet a todos los dispositivos conectados a la red.
- **Colaboración:** Facilita el trabajo en equipo y la colaboración entre usuarios.

*Nota: No todas las redes cumplen todas las funciones*

## 2. Clasificación de redes

Las redes se pueden clasificar según alcance, funciones y tipo de conexión

### Según alcance:

**Red de área personal** o PAN (personal area network) es una red de ordenadores usada para la comunicación entre los dispositivos del ordenador cerca de una persona. Un ejemplo típico de red PAN sería una conexión entre dos dispositivos mediante Bluetooth, como por ejemplo dos teléfonos móviles entre sí, o unos auriculares inalámbricos con un ordenador.

**Red de área local** o LAN (local area network) es una red que se limita a un área especial, relativamente pequeña, tal como un cuarto, un aula, un solo edificio, una nave, o un avión. Las redes de área local suelen tener las mayores velocidades, además de considerarse como el componente esencial para la creación de redes más grandes.

**Red de área de campus** o CAN (campus area network) es una red de computadoras que conecta redes de área local a través de un área geográfica limitada, como un campus universitario, o una base militar. Este término se suele utilizar como extensión del de LAN, ya que realmente lo que se tienen son redes locales conectadas entre sí para abarcar una área más extensa.

**Red de área metropolitana** o MAN (metropolitan area network) es una red de alta velocidad (banda ancha) que da cobertura en un área geográfica extensa. Este concepto se utiliza para definir redes que abarcan extensiones relativamente grandes, y que necesitan recursos adicionales a los que necesitaría una red local.

**Red de área amplia** o WAN (wide area network) son redes informáticas que se extienden sobre un área geográfica extensa. Dentro de esta clasificación podemos encontrar las redes de telecomunicaciones que permiten el uso de Internet, y el propio **Internet** que puede considerarse como una gigantesca red WAN.

**Red de área local óptica pasiva (POLAN)**

### Según las **funciones** de sus componentes:

**Redes de igual a igual** o entre iguales, también conocidas como redes **peer-to-peer**, son redes donde ningún ordenador está a cargo del funcionamiento de la red. Cada ordenador controla su propia información y puede funcionar como cliente o servidor según lo necesite. Los sistemas operativos más utilizados incluyen la posibilidad de trabajar de esta manera, y una de sus características más destacadas es que cada usuario controla su propia seguridad.

**Redes cliente-servidor**, se basan en la existencia de uno o varios servidores, que darán servicio al resto de ordenadores que se consideran clientes. Este tipo de redes facilitan la gestión centralizada. Para crear redes de este tipo necesitamos sistemas operativos de tipo servidor, tales como Windows 2008 server o GNU-Linux. Cabe destacar que en principio cualquier distribución Linux pueden actuar como servidor, aunque existen distribuciones especialmente recomendadas para este cometido, tales como Debian, Ubuntu server, Red Hat enterprise, etc.

Según el **tipo de conexión** podemos tener:

**Redes cableadas:** En este tipo de redes se utilizan diferentes tipos de cables para conectar los ordenadores, más adelante estudiaremos lo relacionado con los tipos de cables más utilizados.

**Redes inalámbricas:** Son las redes que no necesitan cables para comunicarse, existen diferentes tecnologías inalámbricas que más adelante estudiaremos.

**Redes mixtas:** Son redes en las que algunos equipos se conectan de manera cableada, mientras que otros lo hacen de manera inalámbrica.

Otra clasificación interesante es teniendo en cuenta el **grado de difusión**, en esta clasificación distinguimos dos tipos de redes:

**Intranet** es una red de computadoras que utiliza alguna tecnología de red para usos comerciales, educativos o de otra índole de forma privada, esto es, que no comparte sus recursos o su información con otras redes, a no ser que autentifiquen, o cumplan unas medidas de seguridad determinadas.

**Internet** es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial. Precisamente esta característica, es la que ha hecho que el uso de Internet se generalice y que todas las redes funcionen utilizando protocolos TCP/IP.

Fuente: 1.3 Clasificación de las redes. Tipos de redes.

<https://apuntes-daw.javiergutierrez.trade/sistemas-informaticos/ut3/redes-de-ordenadores.html>

### 3. Arquitectura de Red

Conjunto de capas o niveles, junto con los protocolos definidos en cada una de estas capas, que hacen posible que un dispositivo se comuniquen con otro independientemente de la red en la que se encuentre.

La arquitectura de red tendrá que tener en cuenta al menos tres factores importantes como son:

- La forma como se conectan los nodos de una red, que suele conocerse como **topología**, además de las características físicas de estas conexiones.
- La manera de como compartir información en la red, que en algunos casos obligará a elegir un **método de acceso a la red** y unas reglas para evitar pérdida de información.
- Unas reglas generales que no sólo favorezcan la comunicación, si no que la establezcan, mantengan y permitan la utilización de la información, estas reglas serán los **protocolos de comunicación**.

Fuente: 1.4 Clasificación de las redes. Tipos de redes.


<https://apuntes-daw.javiergutierrez.trade/sistemas-informaticos/ut3/redes-de-ordenadores.html>


## 4. Modelo OSI

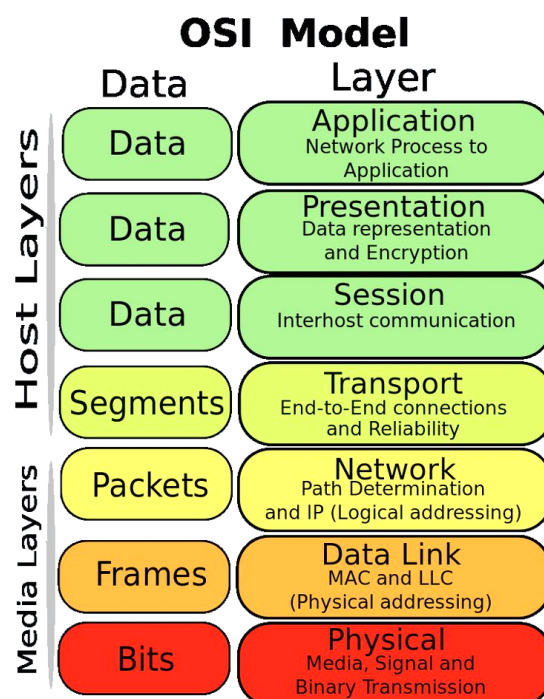
Open Systems Interconnection Reference Model

Define las normas, mecanismos, formatos y protocolos utilizados para guiar el flujo de datos de un dispositivo a otro. OSI en sí mismo **no se aplica realmente exactamente** cómo define la norma, sino que el hardware de red, los protocolos y otros programas informáticos que forman una red siguen las directrices del modelo.

- 1. Capa física:** Se encarga de la transmisión de bits a través del medio físico (cables, fibra óptica, etc.).
- 2. Capa de enlace de datos:** Convierte los bits en tramas y controla el acceso al medio de red.
- 3. Capa de red:** Enruta los paquetes a través de la red utilizando direcciones IP.
- 4. Capa de transporte:** Garantiza la entrega fiable de datos entre dos hosts.
- 5. Capa de sesión:** Controla la comunicación entre dos aplicaciones.
- 6. Capa de presentación:** Formatea los datos para que sean interpretados por la capa de aplicación.
- 7. Capa de aplicación:** Proporciona servicios a las aplicaciones del usuario (correo electrónico, web, etc.).

 Las tres primeras capas están relacionadas con el hardware, la 5,6,7 de software y la 4 es tanto hardware y software.

 Cada capa solo afecta a las colindantes (superior o inferior según sea el flujo de la señal), o su *par* en el equipo destino



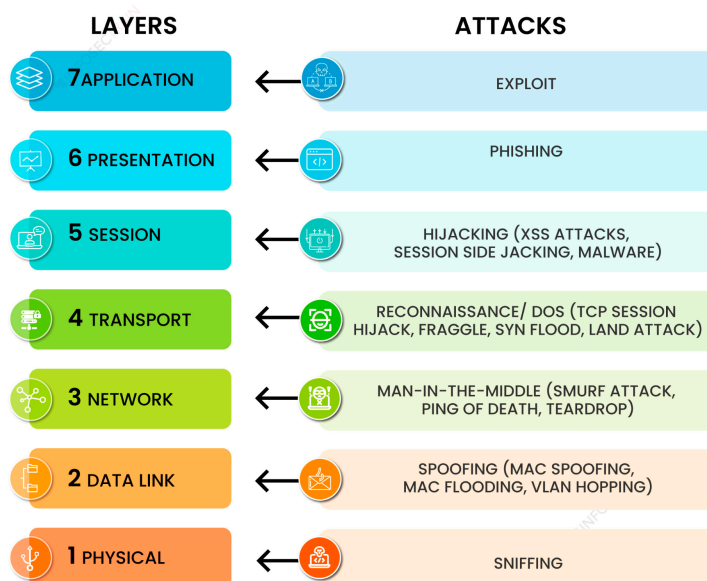
<https://www.lifewire.com/osi-model-reference-guide-816289>

Otra representación de OSI con más detalle.

OSI (Open Source Interconnection) 7 Layer Model				
Layer	Application/Example	Central Device/Protocols		DOD4 Model
<b>Application (7)</b> Serves as the window for users and application processes to access the network services.	<b>End User layer</b> Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management	<b>User Applications</b> SMTP	<b>G A T E W A Y</b> Can be used on all layers	<b>Process</b>
<b>Presentation (6)</b> Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	<b>Syntax layer</b> encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • Character Set Translation	JPEG/ASCII EBDIC/TIFF/GIF PICT		
<b>Session (5)</b> Allows session establishment between processes running on different stations.	<b>Synch &amp; send to ports</b> (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.	<b>Logical Ports</b> RPC/SQL/NFS NetBIOS names		
<b>Transport (4)</b> Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	<b>TCP</b> Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	<b>TCP/SPX/UDP</b> <b>Routers</b> IP/IPX/ICMP	<b>Host to Host</b>	<b>Internet</b>
<b>Network (3)</b> Controls the operations of the subnet, deciding which physical path the data takes.	<b>Packets</b> ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting			
<b>Data Link (2)</b> Provides error-free transfer of data frames from one node to another over the Physical layer.	<b>Frames</b> ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgement • Frame delimiting • Frame error checking • Media access control	<b>Switch Bridge WAP</b> PPP/SLIP	<b>Land Based Layers</b>	<b>Network</b>
<b>Physical (1)</b> Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	<b>Physical structure</b> Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts	<b>Hub</b>		

<https://blogs.cisco.com/cloud/an-osi-model-for-cloud>

### COMMON SECURITY ATTACKS IN THE OSI LAYER MODEL



<https://www.infosectrain.com/blog/common-security-attacks-in-the-osi-layer-model/>



## 4.1 Capa física

### Características cableado

- Atenuación: En casi todos los cables existe un límite de distancia a partir del cual la señal se debilita y deja de ser reconocible.
- Interferencias electromagnéticas (EMI): Prácticamente todos los dispositivos eléctricos emiten ondas electromagnéticas que pueden causar interferencias y afectar a las señales de otros dispositivos
- RFI Los dispositivos que emiten señales inalámbricas o de radio pueden producir interferencias a través de las transmisiones de ondas de radio captadas por otros dispositivos eléctricos, lo que constituye la causa de las IEM.-
- Cancelación: Los campos electromagnéticos de dos cables situados muy cerca pueden anularse mutuamente. Por lo general, esto es bueno y ayuda a controlar las señales que se envían a través de los cables individuales, pero demasiada cancelación puede destruir la integridad de la señal transportada en cualquiera de los cables.

## 4.2 Capa de Enlace (Data Link)

### 4.3 Red

### 4.4 Transporte

### 4.5 Sesión

### 4.6 Aplicación

## 4.7 Presentación

🤔 Por valorar si se explican en detalle

## 5. Modelo TCP/IP

La arquitectura TCP/IP se estructura en capas jerarquizadas y es el utilizado en Internet, es un conjunto de protocolos de comunicación que permite la transmisión de datos entre dispositivos conectados a una red.

Su nombre proviene de dos de sus protocolos más importantes:

- Transmission Control Protocol (TCP): es el protocolo que se ocupa principalmente de la entrega confiable de paquetes que requiere un acuse de recibo de la llegada de un paquete a su destino.
- Internet Protocol (IP).

### Capa 1. Acceso a la red/enlace/subred

Se encarga del acceso al medio de transmisión, es asimilable a los niveles 1 y 2 del modelo OSI, y sólo especifica que deben usarse protocolos que permitan las conexiones entre ordenadores de la red. Hay que tener en cuenta que esta arquitectura está pensada para conectar ordenadores diferentes en redes diferentes, por lo que las cuestiones de nivel físico no se tratan, y se dejan lo suficientemente abiertas para que se pueda utilizar cualquier estándar de conexión. Permite y define el uso de direcciones físicas utilizando las direcciones MAC.

La principal función de este nivel es convertir la información suministrada por el nivel de red, en señales que puedan ser transmitidas por el medio físico. La función inversa es convertir las señales que llegan por el medio físico en paquetes de información manejables por el nivel de red. Las cuestiones relacionadas con las conexiones físicas, que en las redes locales vienen definidas por el estándar Ethernet. Este estándar define las características de cableado y señalización de nivel físico, y los formatos de las tramas de datos del nivel de enlace de datos. Ethernet es la base para el estándar IEEE 802.3, que es un estándar internacional que tiene posibilidades de uso tanto en redes locales como en redes de área amplia.

### Capa 2. Red/Internet

Al igual que la capa de red del modelo OSI, esta capa se encarga de estructurar la información en paquetes, determina la ruta que tomarán los paquetes y define el direccionamiento. En esta arquitectura los paquetes pueden viajar hasta el destino de forma independiente, pudiendo atravesar redes diferentes y llegar desordenados, sin que la ordenación de los paquetes sea responsabilidad de esta capa, por tanto tampoco se encarga de los errores. El protocolo más significativo de esta capa es el protocolo IP, y entre sus funciones está la de dar una dirección lógica a todos los nodos de la red.

### Capa 3. Transporte

Es igual al nivel de transporte del modelo OSI. Se encarga de que los paquetes de datos tengan una secuencia adecuada y de controlar los errores. Los protocolos más

importantes de esta capa son: TCP y UDP. El protocolo TCP es un protocolo orientado a conexión y fiable, y el protocolo UDP es un protocolo no orientado a conexión y no fiable.

## Capa 4. Aplicación

Esta capa englobaría conceptos de las capas de sesión, presentación y aplicación del modelo OSI. Incluye todos los protocolos de alto nivel relacionados con las aplicaciones que se utilizan en Internet (navegadores, correo electrónico, etc.).

Capas según el modelo OSI		Capas según el modelo TCP/IP	
7	Aplicación <i>Application</i>	4	Aplicación <i>Process</i>
6	Presentación <i>Presentation</i>		
5	Sesión <i>Session</i>		
4	Transporte <i>Transport</i>	3	Transporte <i>Host-to-Host</i>
3	Red <i>Network</i>	2	Internet <i>Network</i>
2	Enlace de datos <i>Data Link</i>	1	Acceso al medio <i>Media</i>
1	Física <i>Physical</i>		

El modelo TCP/IP funciona dividiendo el archivo en pequeños paquetes de datos. Cada paquete:

- Lleva una dirección IP de destino (como la dirección de tu amigo en la red).
- Utiliza un protocolo de transporte (como TCP para archivos importantes o UDP para streaming) para garantizar la entrega o simplemente enviar paquetes rápidamente.
- Puede pasar por varios dispositivos de red (routers, switches) que lo reenvían hacia la dirección correcta.

### 4.1 Acceso

La arquitectura TCP/IP en su estandarización original no se preocupaba demasiado del nivel físico en sí, de hecho, en un principio sólo se preocupó de estandarizar los protocolos relacionados con el enlace de datos, de ahí el nombre de este nivel.

Posteriormente con el auge de las redes de todo tipo, se vio que los estándares que ya existían desde un punto de vista físico, cada vez se tenían que tener más en cuenta, y por

esto algunos autores, desarrolladores y diseñadores consideran que la arquitectura TCP/IP realmente consta de cinco capas, siendo la primera la capa física o de hardware y la segunda la de enlace de datos, tal y como recomienda el modelo OSI.

Para nosotros nos basta con considerarla como una sola, tal y como viene referido en el RFC 1122, documento que define el modelo TCP/IP.

La principal función de este nivel es convertir la información suministrada por el nivel de red, en señales que puedan ser transmitidas por el medio físico. La función inversa es convertir las señales que llegan por el medio físico en paquetes de información manejables por el nivel de red.

En este nivel se deben tener en cuenta las cuestiones relacionadas con las conexiones físicas, que en las redes locales vienen definidas por el estándar Ethernet. Este estándar define las características de cableado y señalización de nivel físico, y los formatos de las tramas de datos del nivel de enlace de datos. Ethernet es la base para el estándar IEEE 802.3, que es un estándar internacional que tiene posibilidades de uso tanto en redes locales como en redes de área amplia.

Otro aspecto importante de este nivel es lo relacionado con el **direccionamiento físico (Data link)**. Este concepto viene de lo que se considera una subcapa del nivel de enlace de datos, y que se llama control de acceso al medio, cuyas siglas en inglés, MAC, se utilizan para definir lo que se conoce como direcciones MAC.

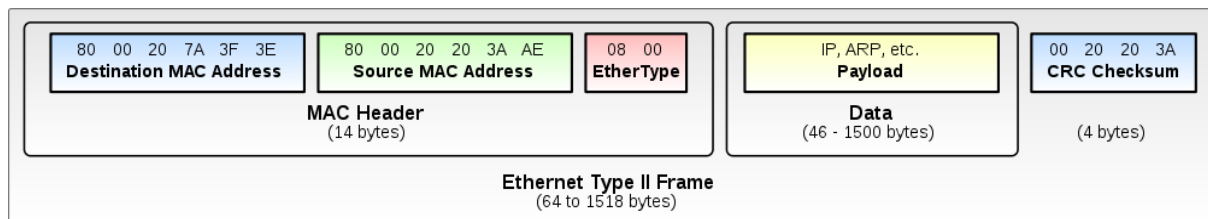
Las dirección MAC es un identificador de 48 bits, que suele representarse en forma de números hexadecimales, en un formato de 6 bloques de dos números hexadecimales, divididos por dos puntos. El formato es el siguiente:

FF:FF:FF:FF:FF:FF

Los 24 bits más significativos (los de la izquierda) determinan el fabricante y se les conoce como **Identificador Único de Organización** y los 24 bits menos significativos (los de la derecha), identifican una interfaz concreta. De esta forma ninguna tarjeta de red tiene la misma dirección física.

En este nivel hay un protocolo relacionado con el direccionamiento físico. Este protocolo es el **ARP**. ARP son las siglas en inglés del **protocolo de resolución de direcciones**, este protocolo trabaja a **nivel de enlace de datos** y se encarga de encontrar la dirección física o MAC que tiene relación con la correspondiente dirección lógica, que, como veremos en el siguiente apartado, se corresponde con la dirección IP. Lo que hace ARP es traducir direcciones lógicas (IP) a direcciones físicas (MAC). Existe su inverso el RARP que son las siglas en inglés del protocolo de resolución de direcciones inverso, hace la función inversa del protocolo ARP pero no es tan utilizado.

Para terminar mostramos el formato de la unidad de información de este nivel. Cada nivel tendrá una unidad de información, en este nivel se llama **TRAMA**, y tiene un formato determinado.



[Bruceadler.](#)

Sólo destacaremos que en la trama tenemos los datos que recibimos de las capas superiores, y que la capa de enlace le agrega una cabecera, con las direcciones MAC origen y destino, junto con el tipo de trama Ethernet que se utiliza, y una cola donde se agrega información para el control de errores.

## 4.2 Red

El nivel de red del modelo TCP/IP se considera el nivel de la arquitectura más importante, ya que permite que las estaciones envíen información a la red en forma de paquetes. Estos paquetes viajan por la red de forma independiente, pudiendo atravesar diferentes redes y sin un orden establecido. Está es una de las principales ventajas de esta arquitectura y por eso es la base de Internet.

El objetivo principal del nivel de red será encaminar los paquetes desde el nodo origen hasta el nodo destino.

En la arquitectura TCP/IP la capa de red es casi totalmente asimilable a la capa de red del modelo OSI, pero en el caso de la arquitectura TCP/IP la capa de red no se preocupa de las tareas de ordenación de los paquetes cuando llegan a su destino. Esto es lo que se conoce como servicio no orientado a conexión. Cuando los paquetes se tratan de forma independiente, conteniendo cada uno la dirección de destino, se dice que se usa la técnica de **datagrama**, por tanto, **Internet es un red de conmutación de paquetes basada en datagramas**.

Entre las funciones de la capa de red se encuentran:

**El direccionamiento:** Permite identificar de forma única cada nodo de la red.

Cuando se habla de direccionamiento en este nivel, se está hablando de direccionamiento lógico, para distinguirlo del direccionamiento físico que ya hemos visto anteriormente.

**La conectividad:** Conseguir que los nodos de una red se conecten, independientemente de la red a la que pertenezcan.

**El enrutamiento:** También llamado encaminamiento, los protocolos de esta capa deben ser capaces de encontrar el mejor camino entre dos nodos.

**El control de la congestión:** Es conveniente realizar un control del tráfico, ya que si un nodo recibe más información de la que puede procesar, se produce una saturación y este problema puede extenderse a toda la red.

Para realizar todas estas funciones el nivel de red utiliza diferentes protocolos, entre los protocolos más destacados de este nivel tenemos:

**IP:** Internet Protocol, o Protocolo de Internet proporciona un enrutamiento de paquetes no orientado a conexión y es usado tanto por el origen como por el destino para la comunicación de datos.

**ARP y RARP:** También se utilizan en la capa de enlace de datos y sirven para relacionar direcciones IP con direcciones MAC y viceversa.

**ICMP:** Protocolo de mensajes de control en Internet, suministra capacidades de control y envío de mensajes. También se considera protocolo del nivel de transporte, y herramientas tales como [ping](#) y [tracert](#) lo utilizan para poder funcionar.

**OSPF:** Es un protocolo de enrutamiento que busca el camino más corto entre dos nodos de la red.

**RIP:** Protocolo de enrutamiento de información, al igual que OSPF, también busca el camino más corto, pero utilizando otras técnicas de enrutamiento.

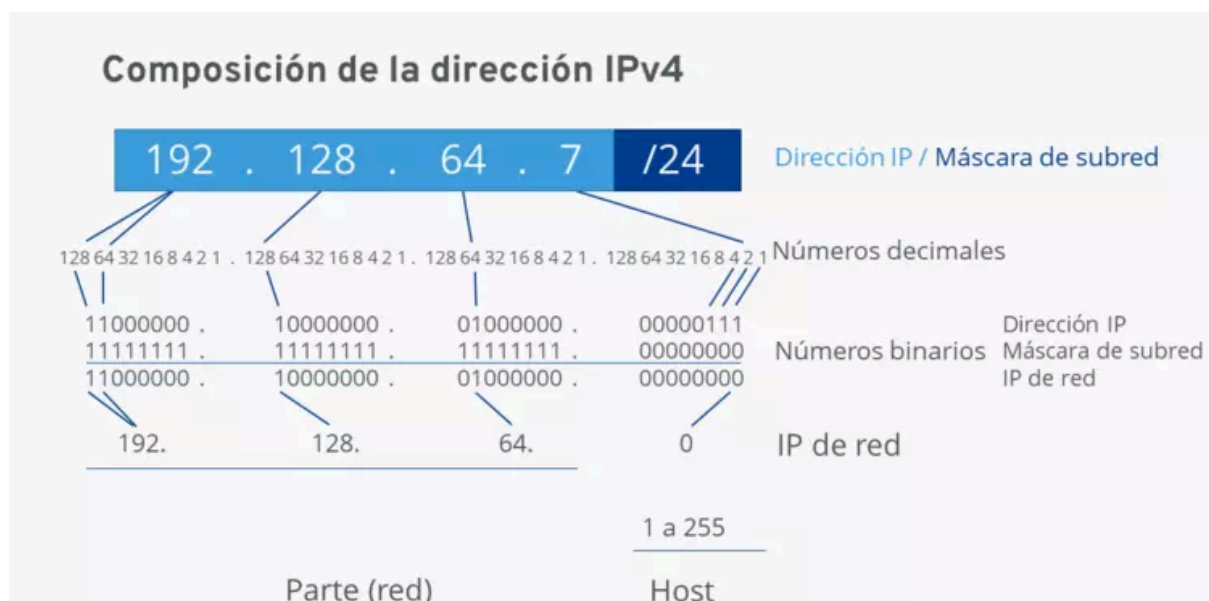
Como se puede comprobar este nivel tiene varias funciones, y varios protocolos, pero podemos decir que el más importante de todos, de hecho da nombre a la arquitectura, es el protocolo IP.

El **protocolo IP**, además de lo mencionado anteriormente, también proporciona las direcciones IP. Una dirección IP es un número que identifica de manera lógica y jerárquicamente a una interfaz dentro de una red que utilice el protocolo de Internet. Más adelante conocerás más sobre el direccionamiento IP, pero ahora es conveniente que conozcas que existen dos versiones IPv4 (IP versión 4) e IPv6 (IP versión 6). Se diferencian en el número de bits que utilizan, versión 4 utiliza direcciones de 32 bits y la versión 6 utiliza direcciones de 128 bits. Ejemplo de direcciones IP son:

**IP versión 4:** 192.168.1.11 (Utilizando valores en decimal).

**IP versión 6:** 2001:0DB8:0000:0000:0000:0000:1428:57AB (Utilizando valores en hexadecimal y puede simplificarse como: 2001:0DB8::1428:57AB)

⚠ No son compatibles, según el caso deberemos activar uno u otro, o dejar ambos activos ⚠



## 4.3 Transporte

Cumple la función de establecer las reglas necesarias para establecer una conexión entre dos dispositivos remotos. Al igual que las capas anteriores, la información que maneja esta capa tiene su propio nombre y se llama **segmento**.

Por tanto la capa de transporte se debe de encargar de unir múltiples segmentos del mismo flujo de datos. Como la capa de red en la arquitectura TCP/IP no se preocupa del orden de los paquetes ni de los errores, es en esta capa donde se deben cuidar estos detalles.

El nivel de transporte de la arquitectura de TCP/IP es totalmente asimilable al nivel de transporte del modelo OSI, por tanto podemos decir que este nivel es el encargado de la transferencia libre de errores de los datos entre el emisor y el receptor, aunque no estén directamente conectados, así como de mantener el flujo de la red. La tarea de este nivel es proporcionar un transporte de datos confiable de la máquina de origen a la máquina destino, independientemente de la red física.

En este nivel trabajan varios protocolos pero los dos más importantes son el TCP y el UDP.

TCP es un protocolo orientado a conexión y fiable, se diseñó específicamente para proporcionar un flujo de bytes confiable de extremo a extremo a través de redes no fiables. Por eso es tan útil en Internet, ya que a diferencia del tráfico en una sola red donde conoceremos sus características, las redes que configuran Internet podrían tener diferentes topologías, anchos de banda, retardos, tamaños de paquete, etc. Pero TCP tiene un diseño que se adapta de manera dinámica a las propiedades de estas redes y permite la conexión en muchos tipos de situaciones.

UDP es un protocolo no orientado a conexión y no fiable, este protocolo proporciona todo lo necesario para que las aplicaciones envíen datagramas IP encapsulados sin tener una conexión establecida. Uno de sus usos es en la transmisión de audio y vídeo en tiempo real, donde no es posible realizar retransmisiones por los estrictos requisitos de retardo que se tiene en estos casos.

Cuando un proceso de aplicación quiere establecer comunicación con otro proceso de aplicación remoto, debe especificar a cuál se conectará. El método que normalmente se emplea es el de definir direcciones de transporte en las que los procesos pueden estar a la escucha de solicitudes de conexión. Estos puntos terminales se llaman puertos.

Por tanto un **puerto** serán las direcciones de transporte en las que los procesos pueden estar a la escucha de solicitudes de conexión. El término puerto se utiliza en Internet, el término genérico es el de Punto de Acceso al Servicio de Transporte, cuyas siglas en inglés son TSAP. Los números de puertos son utilizados por TCP y UDP para identificar las sesiones que establecen las distintas aplicaciones. Algunos **puertos** son:

20: datos de FTP (Protocolo de transferencia de ficheros).

21: control de FTP.

53: DNS (Servicio de nombres de dominio).

80: http (Protocolo utilizado para servir y descargar páginas web).



## 4.4 Aplicación

El nivel de aplicación contiene los programas de usuario (aplicaciones) que hace que nuestro ordenador pueda crear textos, chatear, leer correo, visitar páginas web, etc.

En este nivel se incluyen todos los protocolos de alto nivel que utilizan los programas para comunicarse.

En la arquitectura TCP/IP este nivel incluye a los niveles de sesión, presentación y aplicación del modelo OSI.

Algunos de los protocolos de la capa de aplicación son:

**FTP:** Protocolo utilizado en la transferencia de ficheros entre un ordenador y otro.

**DNS:** Servicio de nombres de dominio, es el sistema utilizado en Internet para convertir los nombres de los nodos de red en direcciones de red.

**SMTP:** Protocolo simple de transferencia de correo, basado en texto y utilizado para el intercambio de mensajes de correo. Está basado en el concepto cliente-servidor, donde un cliente envía un mensaje a uno o varios servidores.

**POP:** Protocolo de oficina de correo, se utiliza en los clientes de correo para obtener los mensajes de correo almacenados en un servidor.

**SNMP:** Protocolo de administración de redes, permite monitorizar y controlar los dispositivos de red y de administrar configuraciones y seguridad.

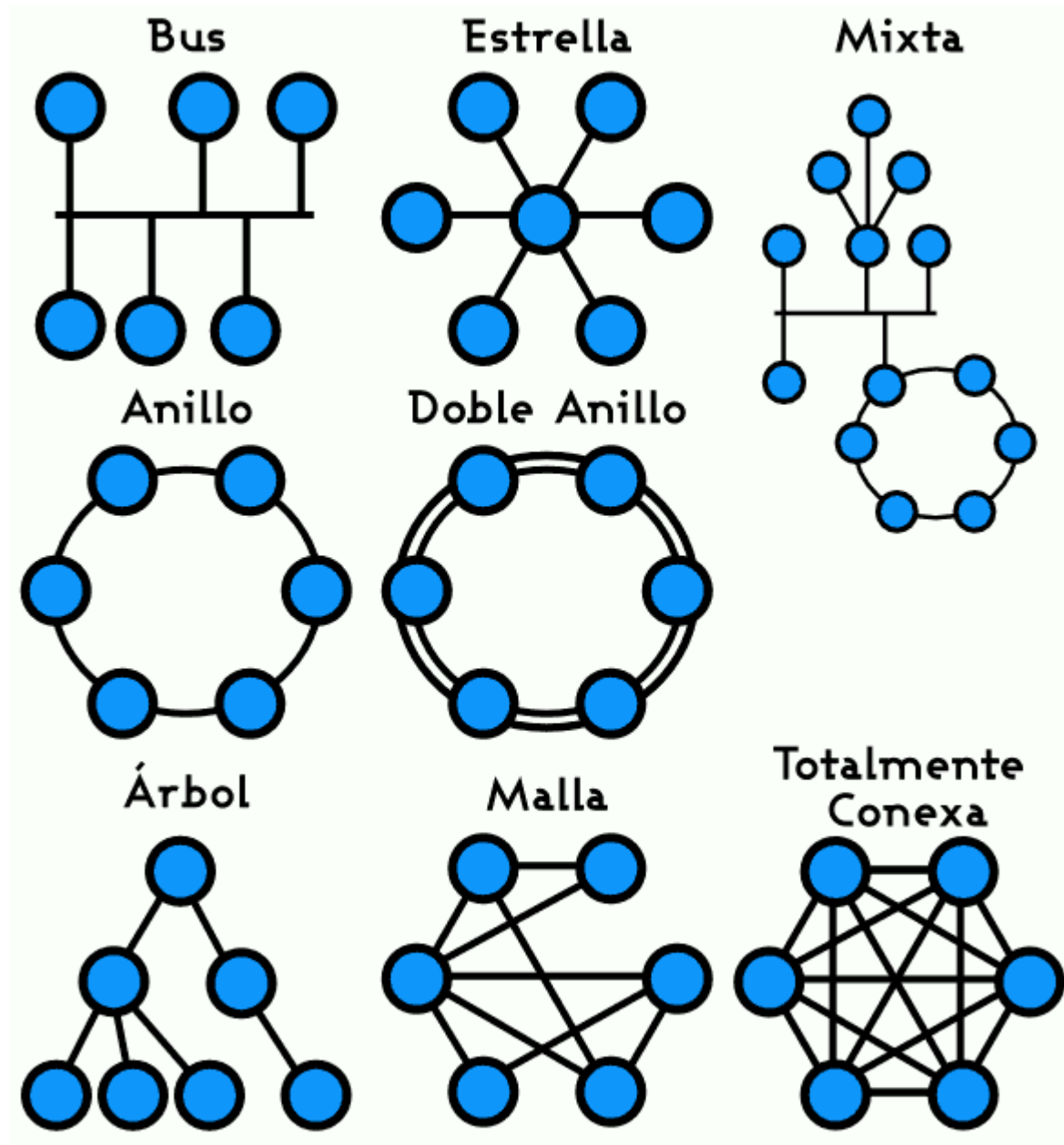
**HTTP:** Protocolo de transferencia de hipertexto, es el protocolo utilizado en las transacciones de páginas web. Define la sintaxis y la semántica que utilizan los elementos de software de la arquitectura web (clientes, servidores, proxies) para comunicarse. Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor.

**HTTPS:** versión segura de HTTP, utiliza TLS (SSL) para encriptar las peticiones y respuestas HTTP normales, y para firmar digitalmente esas peticiones y respuestas

Una vez que conocemos los diferentes niveles de la arquitectura podemos definir el concepto de **socket**. Un **socket**, es una conexión que está formada por la unión de la dirección IP más el puerto que se utiliza para la conexión. Como cada puerto está asociado a una aplicación, podemos decir que no habrá dos conexiones iguales en un mismo instante de tiempo. Ejemplo: 192.168.1.11:80, esto significa que el ordenador cuya dirección es 192.168.1.11 está utilizando el puerto 80, que está asociado al protocolo http del nivel de aplicación, por tanto esto puede significar que el ordenador está visitando una página web o sirviendo una página web. Este concepto seguro que te será de utilidad más adelante cuando programes servicios web o aplicaciones que utilicen Internet.

## 6. Topologías de red

- Bus
- Anillo/Ring
- Estrella/Star
- Malla
- Árbol



### Mixtas

- Estrella-bus
- Estrella-anillo

## 7. Ethernet

### Componentes de un red informática

- El **cableado de red** y sus **conectores**, que permite la transmisión de la señal.

#### Tipos de cableado de red

- Cable de par trenzado sin apantallar (UTP)
- Cable de par trenzado apantallado (FTP)
- Cable de par trenzado apantallado (STP)
- Cable coaxial.
- Cable de fibra óptica.

#### Tipos de cables de red Ethernet trenzado con conector RJ45

- CAT5, CAT5e
- CAT6, CAT6e
- CAT7: 4 cables trenzados. 10Gbit

<https://community.fs.com/es/article/quick-view-of-ethernet-cables-cat-5-cat-5e-and-cat-6.html>

*no incluye CAT7*

- El **rack** o armario de conexiones, es un bastidor destinado a alojar equipamiento electrónico, informático y de comunicaciones.
- Los **patch panel**, paneles de conexión que sirven de terminadores del cableado y ayudan a organizarlo.
- Las **tarjetas de red**, que permitirán la conexión del ordenador, bien por cable o de forma inalámbrica.
- Los **conmutadores** o **switch**, que permiten la conexión de diferentes ordenadores entre sí y de segmentos de red entre sí.
- Los **enrutadores** o router, también conocidos como encaminadores, permiten conectar redes diferentes, como por ejemplo una red de área local con Internet.
- Los **puntos de acceso**, que permiten la interconexión de dispositivos inalámbricos entre sí, y/o la conexión de dispositivos cableados con los inalámbricos.
- Los **cortafuegos (firewall)**, que pueden ser dispositivos hardware con un software específico para bloquear acceso no autorizados a la red, o software específico que se instale en los ordenadores y/o servidores para evitar los accesos no autorizados.
- Los **servidores**, que no son más que ordenadores con un sistema operativo específico para actuar como servidor, o con sistemas operativos no servidores pero con software de servidor.

Además de estos componentes, también consideramos como parte de la red a los ordenadores que trabajarán en red, que en muchos casos se les llama **estaciones de trabajo**. Cualquier dispositivo que se pueda conectar a la red para prestar algún

servicio, tales como impresoras, discos duros de red, o cualquier periférico que esté conectado a algún ordenador de la red, es también un componente de la red y se les suele denominar **nodos de red**.

## Switches y routers

Los switches y routers son dos dispositivos de red esenciales que operan en diferentes capas del modelo TCP/IP:

### Switches

- Capa 2: Enlace de datos
- Función: Conectan dispositivos dentro de una misma red local (LAN) utilizando direcciones MAC.
- Ejemplo: Un switch conecta tu ordenador, impresora y smartphone en una red doméstica.

### Routers

- Capa 3: Red
- Función: Interconectan diferentes redes, como LANs e Internet, utilizando direcciones IP.
- Ejemplo: Un router te permite acceder a Internet desde tu red doméstica.

En resumen

- Los switches trabajan a nivel de hardware (MAC) para conectar dispositivos dentro de una misma red.
- Los routers trabajan a nivel de software (IP) para interconectar diferentes redes y enviar paquetes a su destino final.

Diferencias adicionales:

- Los switches son más rápidos que los routers porque no necesitan analizar la información de cada paquete.
- Los routers pueden realizar funciones más complejas, como el filtrado de paquetes y la configuración de redes virtuales.

Analogía:

Imagina una oficina con diferentes departamentos.

- Los switches son como los mensajeros internos que llevan documentos entre los empleados del mismo departamento.
- Los routers son como la recepción que recibe los documentos de los mensajeros y los envía al departamento correcto en otro edificio.




### Capa 4: Aplicación

Es importante mencionar que algunos switches y routers también pueden tener funcionalidades en la capa 4 del modelo TCP/IP, como la inspección de paquetes a nivel de aplicación (DPI) para controlar el tráfico de red según el tipo de aplicación (por ejemplo juegos, streaming).

# Subnetting

La división en subredes (o **subnetting**) es el proceso de dividir una red y sus direcciones IP en segmentos, cada uno de los cuales se denomina **subred** (subnetwork o subnet).

La **máscara de red** es el número de 32 bits que el router utiliza para cubrir la dirección de red para mostrar qué bits se utilizan para identificar la subred.

 En resumen Subnetting, subred (subnet) y una máscara de red son cosas distintas. De hecho, la primera crea la segunda y es identificada por la tercera.

## Clases de direcciones IP y sus rangos

Todas las direcciones IP contienen cuatro números separados por un punto y conocidos como octetos (cuatro octetos). Estas se dividen en clases dependiendo del valor del primer octeto:

- Clase A (0.0.0.0 - 127.255.255.255): El primer octeto identifica la red y los tres restantes al dispositivo dentro de la red (host). Se utilizan para redes con un gran número de hosts, como por ejemplo las de las universidades. Contiene hasta 16.777.216 hosts ( $2^{24} - 2$ )
- Clase B (128.0.0.0 - 191.255.255.255): Los primeros dos octetos identifican la red y los siguientes al dispositivo dentro de la red (host). Se suelen utilizar en medianas y grandes empresas. Contiene 65.534 host ( $2^{16} - 2$ )
- Clase C (192.0.0.0 - 223.255.255.255): Los primeros tres octetos identificarán a la red y el último octeto al dispositivo dentro de la red (host). Se utiliza en redes que tienen una pequeña cantidad de dispositivos como son las pequeñas empresas. Contiene 254 hosts ( $2^8 - 2$ )
- Clase D (224.0.0.0 - 239.255.255.255): Se usan para optimizar la velocidad y el ancho de banda de una red (multicast).
- Clase E (240.0.0.0 - 255.255.255.255): Son utilizadas para la investigación.

Dentro de la clasificación anterior existe un rango de direcciones que se encuentran reservadas para su uso en **redes privadas**, y, por lo tanto, no van a tener salida a Internet:

- Clase A (10.0.0.0 - 10.255.255.255)
- Clase B (172.16.0.0 - 172.31.255.255)

- Clase C (192.168.0.0 - 192.168.255.255)

Además, existen otras **direcciones especiales** que no pueden ser asignadas en ningún dispositivo de una red:

- Ruta por defecto en tabla de enrutamiento: 0.0.0.0 (todas las redes)
- Loopback testing: 127.0.0.1
- Broadcast a la red local: 255.255.255.255

TIPO Subred	valor primer octeto	Bits red/host	Bits usado para máscara	Máscara red por defecto	Subred en binario
A	0-127	7/24	/8	255.0.0.0	11111111.00000000.00000000.00000000
B	128-191	14/16	/16	255.255.0.0	11111111.11111111.00000000.00000000
C	192-223	21/8	/24	255.255.255.0	11111111.11111111.11111111.00000000

<https://ramprasadtech.com/networking-basics-bits-subnets-network-masks/>

<https://openwebinars.net/blog/direccion-ip-que-es-para-que-sirve-y-como-funciona/#:~:text=Estas%20se%20dividen%20en%20clases.ejemplo%20las%20de%20las%20universidades.>

## Máscara de red

La máscara de subred es un número binario de 32 bits que se utiliza en las redes IP para dividir una dirección IP en dos partes: la parte de la red y la parte del host. La máscara de subred funciona como una plantilla que se aplica a la dirección IP para determinar qué bits de la dirección se utilizan para identificar la red y qué bits se utilizan para identificar el host específico dentro de esa red.

### Funciones de la máscara de red:

- Dividir la red en subredes: La máscara de subred se puede utilizar para dividir una red grande en subredes más pequeñas. Esto puede ser útil para mejorar el rendimiento y la seguridad de la red.
- Determinar si dos dispositivos están en la misma red: La máscara de subred se puede utilizar para determinar si dos dispositivos están en la misma red local (LAN) o en redes diferentes.
- Enrutar el tráfico de red: La máscara de subred se utiliza para enrutar el tráfico de red al dispositivo correcto.

Representación de la máscara de subred:

La máscara de subred se representa como un número decimal de 32 bits, similar a una dirección IP. Sin embargo, en lugar de usar valores del 0 al 255, la máscara de subred usa solo dos valores: 1 y 0.

- Los bits 1 en la máscara de subred indican la parte de la dirección IP que se utiliza para identificar la red.
- Los bits 0 en la máscara de subred indican la parte de la dirección IP que se utiliza para identificar el host.

Ejemplo:

Consideremos la siguiente dirección IP y máscara de subred:

Dirección IP: 192.168.1.100

Máscara de subred: 255.255.255.0

En este caso, los primeros 24 bits de la dirección IP (192.168.1) se utilizan para identificar la red, mientras que los últimos 8 bits (100) se utilizan para identificar el host específico dentro de esa red.

# Glosario de Términos

[Broadcast IP](#)

CRC

Ethernet

Gateway/Puerta de enlace

Hub

ICMP (Internet Control Message Protocol)

IP

MAC

Máscara de Red

OSI

PDU

Ping (Packet Internet Groper)

Protocolo

Proxy

RJ45

[Router](#)/ruter/encaminador/enrutador

[Switch](#)/Conmutador

Subred

Traceroute

TCP/IP

UDP

VLAN

WAN