

Sistemas Informáticos

UD 10. Redes de ordenadores. Arquitecturas. TCP/IP

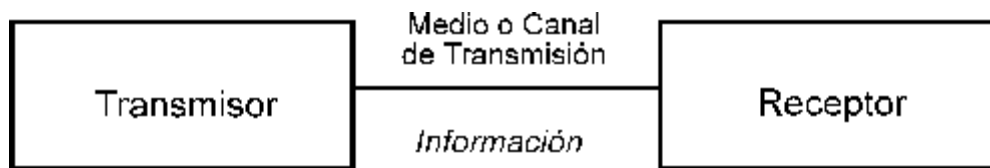
ÍNDICE

1.	SISTEMAS DE COMUNICACIÓN	2
2.	REDES DE ORDENADORES.....	2
3.	COMPONENTES.....	3
4.	CARACTERÍSTICAS	3
5.	TIPOS	4
6.	TOPOLOGÍAS	5
7.	ARQUITECTURA DE RED.....	8
8.	MODELO DE REFERENCIA OSI	9
9.	ARQUITECTURA TCP/IP	10

1. SISTEMAS DE COMUNICACIÓN

La Comunicación es la transferencia de información con sentido desde un lugar (remitente, origen, fuente, transmisor) a otro lugar (destino, receptor).

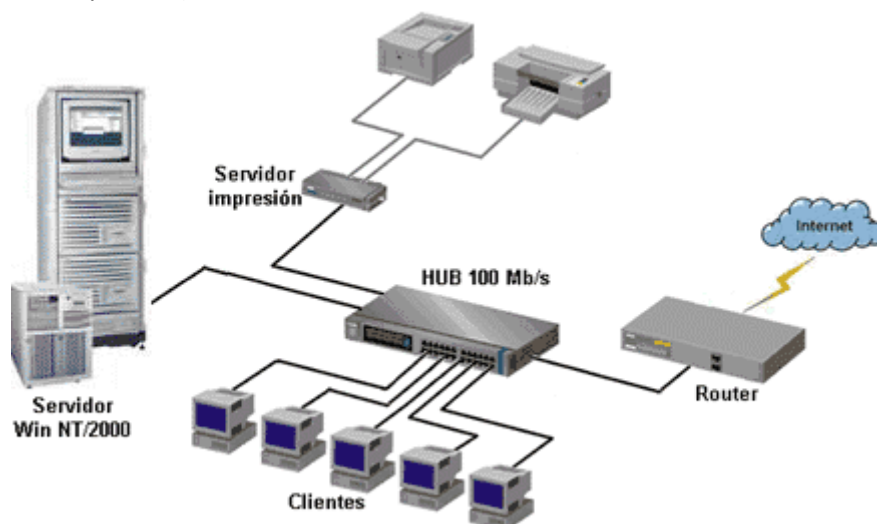
Elementos básicos de un sistema de comunicaciones:



- El **Transmisor** pasa el mensaje al canal en forma de señal. Para lograr una transmisión eficiente y efectiva, se deben desarrollar varias operaciones de procesamiento de la señal. La más común e importante es la modulación, un proceso que se distingue por el acoplamiento de la señal transmitida a las propiedades del canal, por medio de una onda portadora.
- El **Canal** de Transmisión o medio es el enlace eléctrico entre el transmisor y el receptor, siendo el puente de unión entre la fuente y el destino. Este medio puede ser un par de alambres, un cable coaxial, el aire, etc. Pero sin importar el tipo, todos los medios de transmisión se caracterizan por la atenuación, la disminución progresiva de la potencia de la señal conforme aumenta la distancia.
- La función del **Receptor** es extraer del canal la señal deseada y entregarla al transductor de salida. Como las señales son frecuentemente muy débiles, como resultado de la atenuación, el receptor debe tener varias etapas de amplificación. En todo caso, la operación clave que ejecuta el receptor es la demodulación, el caso inverso del proceso de modulación del transmisor, con lo cual vuelve la señal a su forma original.

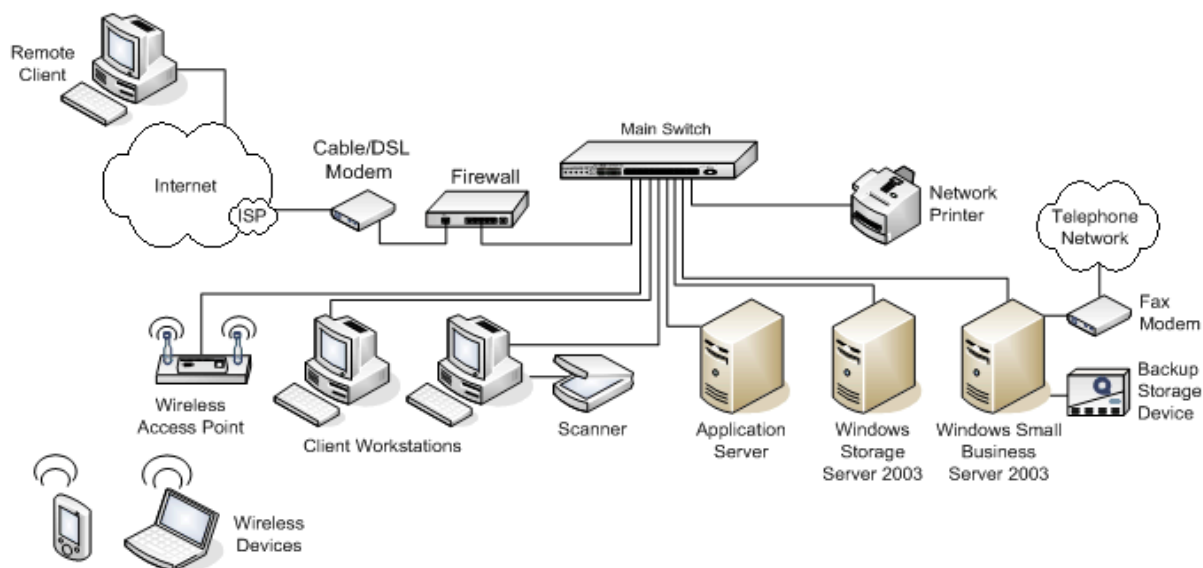
2. REDES DE ORDENADORES

Podríamos definir una **red** como un conjunto de ordenadores conectados entre sí para compartir datos y/o recursos (como, por ejemplo, una impresora).



3. COMPONENTES

Una red de computadoras está conectada tanto por hardware como por software. El hardware incluye tanto las tarjetas de red como los cables que las unen y los dispositivos de interconexión de los equipos (switches, puntos de acceso...), y el software incluye los controladores o drivers (programas que se utilizan para gestionar los dispositivos) y el sistema operativo de red que gestiona la red entre otros.



4. CARACTERÍSTICAS

Tanto si se trata de una instalación de cableado estructurado UTP o bien se dispone de una red inalámbrica, hay una serie de características que nos permiten definir su funcionalidad.

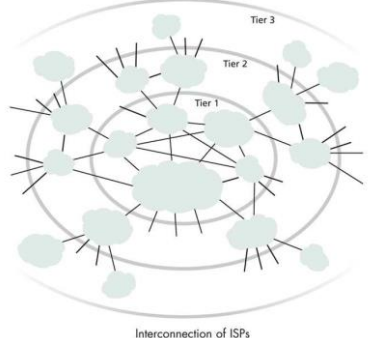
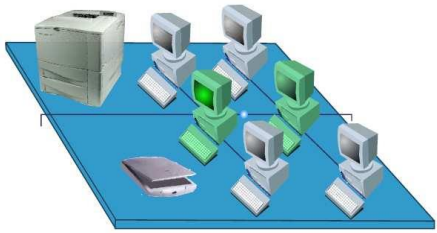
- **Velocidad:** Es la velocidad a la que se transmiten los datos por segundo a través de la red. Suelen medirse con un test de velocidad. La rapidez de subida y descarga de datos será diferente según los estándares que utilicemos y también según el tipo de red o medio a través del que se transmiten los datos (inalámbrica, fibra óptica, cables de teléfono o coaxial).
- **Seguridad de la red:** Es uno de los aspectos más peligrosos que rodean a las redes inalámbricas, como ya hablamos en otra ocasión. La aparición de intrusos que nos quitan ancho de banda es una de las razones que convierte estas redes en bastante más vulnerables. Por otro lado, las redes cableadas pueden sufrir interferencias como consecuencia del uso de otros aparatos como el microondas. A diferencia de estas, la fibra óptica es la que ofrece una mayor seguridad.
- **Confiabilidad:** Mide el grado de probabilidades que existe de que uno de los nodos de la red se averíe y por tanto se produzcan fallos. En parte dependerá de la topología de la red que hallamos instalado y del lugar que ocupa el componente averiado. Cuando uno de los componentes no funciona, puede afectar al funcionamiento de toda la red o por el contrario constituir un problema local. Por esta razón resulta determinante contar con un hardware redundante para que, en caso de fallo en uno de los componentes, haya una gran tolerancia a los errores y los demás equipos puedan seguir trabajando.
- **Escalabilidad:** Una red no puede añadir nuevos componentes de forma continua y esperar que funcione a la misma velocidad. A medida que añadimos nuevos nodos y estos se hallan funcionando a la vez, la conexión a Internet se reduce, la velocidad de transmisión de datos en general es menor y hay más probabilidad de errores.
- **Disponibilidad:** Es la capacidad que posee una red para hallarse disponible y completamente activa cuando la necesitamos. Hablamos de la cantidad de tiempo posible en que podemos someter los nodos a unas condiciones de rendimiento necesarias en nuestra empresa. El objetivo es conseguir que la red se halle disponible según las necesidades de uso para las que se ha instalado.

5. TIPOS

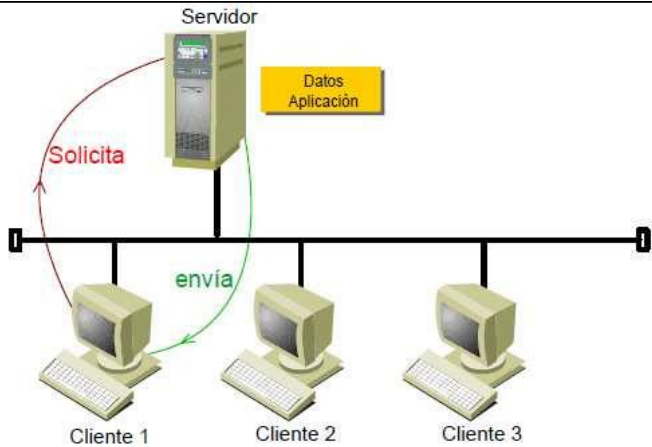
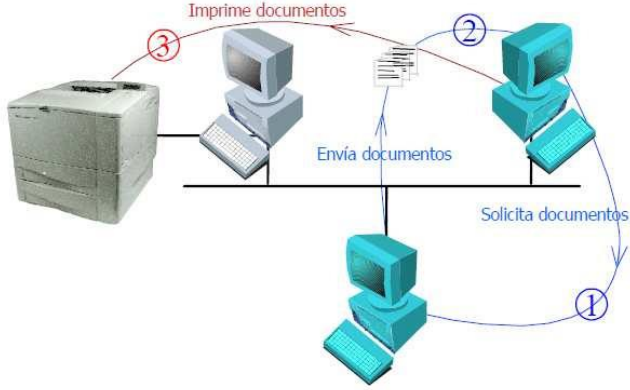
Podemos clasificar las redes en función de varios factores.

De este modo, podemos distinguir:

- En función de su **titularidad**:

<ul style="list-style-type: none">○ Redes públicas: están disponibles para todo el mundo, no son propiedad exclusiva. Ejemplo: internet	 <p>Interconnection of ISPs</p>
<ul style="list-style-type: none">○ Redes privadas: son propiedad de una organización. Ejemplo: el aula de clase	

- Por su **funcionalidad**:

<ul style="list-style-type: none">○ Ciente-servidor: un equipo actúa como servidor de una serie de servicios al resto de equipos que son los clientes. En este modelo la administración de los servicios está centralizada en el servidor.	
<ul style="list-style-type: none">○ Peer-to-peer (de igual a igual): todos los equipos ofrecen y toman servicios (no existe una gestión centralizada de la red).	

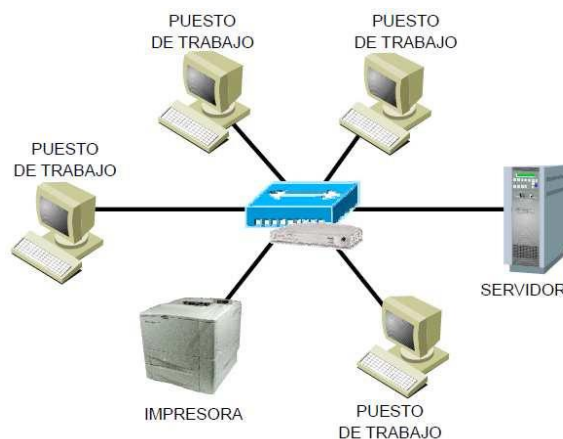
- En función de la **extensión** alcanzada:
 - **LAN** (redes locales):
 - Tienen una extensión muy limitada. Ej: una oficina, una clase...
 - Es una red privada (pertenecen a una determinada organización)
 - Tienen una velocidad de transmisión elevada.
 - Ejemplo:
 - Ethernet: 10 Mbps
 - Fast Ethernet: 100 Mbps
 - Gigabit Ethernet: 1Gbps
 - Las transmisiones son muy fiables (tienen una tasa de error muy baja)
 - Se suelen organizar según cableado estructurado.
 - En este tipo también podríamos incluir las **WLAN** (Wireless LAN, es decir, LAN inalámbricas).
 - **WAN** (redes de área extensa):
 - Intercomunica equipos en un área muy amplia
 - Las transmisiones son a través de líneas públicas (compartidas por muchos usuarios a la vez)
 - Tienen una velocidad de transmisión menor que las LAN
 - **MAN** (redes de área metropolitana):
 - Red de datos para un área geográfica de una ciudad. Ej: distribución de TV por cable o las redes WiMAX
 - **PAN** (redes de área personal): conexión de dispositivos informáticos personales (teléfonos móviles, palms...) mediante infrarrojos o bluetooth.
- También podríamos establecer otras clasificaciones, por ejemplo, en función de la **tecnología de transmisión** tendríamos **redes de difusión** (multipunto) y **redes conmutadas** (punto a punto).

6. TOPOLOGÍAS

La **topología** es la forma en la que están conectados físicamente los distintos elementos (nodos) de una red.

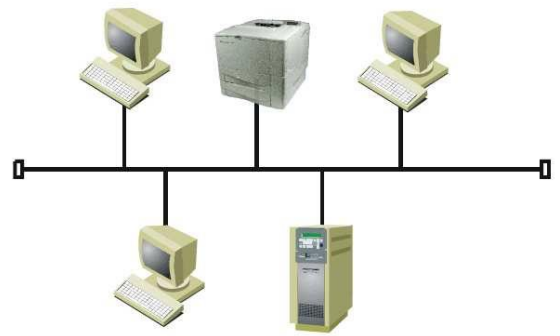
Tipos:

- **Estrella:**
 - todos los nodos se conectan a un nodo central que asume las tareas de conmutación de la red.
 - Es la más usada en la actualidad.
 - Ventajas:
 - Fácil administración
 - Sencillo añadir o desconectar nodos
 - Inconvenientes:
 - Si falla el nodo central, deja de funcionar la red
 - Requiere una línea (cable) para cada equipo
 - Ej: LAN



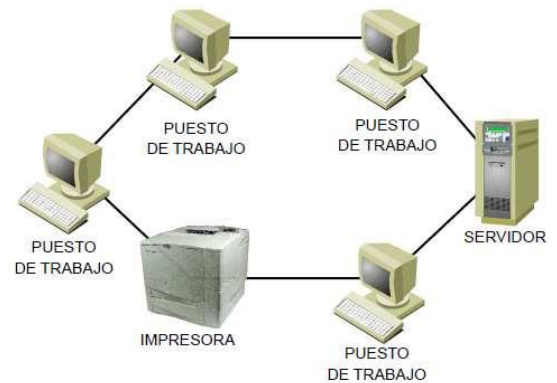
- **Bus:**

- Todas las estaciones se conectan a un único medio de transmisión (cable coaxial) mediante conectores en T
- Ventajas:
 - Sencillez
 - Bajo coste
- Inconvenientes:
 - La rotura del cable principal dejaría sin servicio a todos los equipos de la red
- Ejemplo: antiguas redes Ethernet sobre cable coaxial



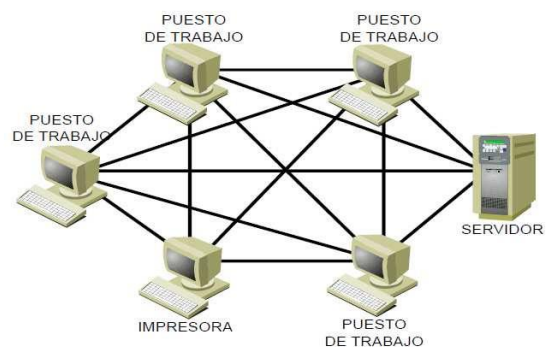
- **Anillo:**

- La red consta de una serie de repetidores que reciben y retransmiten la información conectados unos a otros como en un anillo.
- Ventajas:
 - Localización de errores fácil
 - El software es sencillo
- Inconvenientes:
 - El fallo de un enlace implica el fallo del anillo
 - Difícil adición de nuevos nodos
 - El repetidor de cada nodo ralentiza la velocidad de transmisión
 - Instalación de cableado compleja



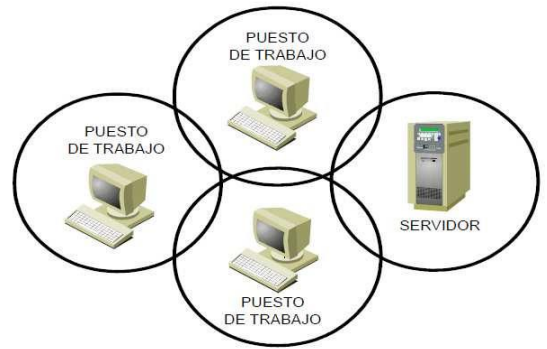
- **Malla:**

- Conexiones punto a punto entre todos o la mayoría de nodos de la red.
- La información puede circular por varias rutas a través de la red.
- Se usa en redes WAN.
- Ventajas:
 - Si algún enlace deja de funcionar la información puede llegar a su destino por otros enlaces
- Inconveniente:
 - Cara y compleja



- **Celular:**

- La red está compuesta por áreas hexagonales o circulares llamadas celdas, cada una de las cuales tiene un nodo en el centro. Todos los elementos que están en el mismo radio de acción pueden conectarse entre sí.
- Se usa en redes inalámbricas.
- Ventajas:
 - Eliminación de los cables
- Inconvenientes:
 - Problemas típicos de las señales electromagnéticas
 - Problemas de seguridad (requiere encriptación de los datos que viajan por el aire)



7. ARQUITECTURA DE RED

A continuación, se analizan las bases de toda arquitectura de sistema de un sistema de comunicación, así como los modelos de más destacados: el modelo OSI y el modelo TCP/IP.

7.1. NIVELES (MODELO DE CAPAS)

Actualmente, el software de redes está altamente estructurado, toda esa estructura de comunicación está organizada jerárquicamente como una pila de **capas o niveles**, cada una construida a partir de la que está debajo de ella. El propósito de cada capa es ofrecer ciertos **servicios**, es decir, operaciones, a las capas superiores, a las cuales se le ocultan los detalles reales de implementación de los servicios ofrecidos. El modo en que cada capa negocia los servicios y se comunica con las capas adyacentes, se denomina interfaz.

La capa n de una máquina lleva a cabo una conversación con la capa n de otra. Las reglas que se siguen en esta conversación se conocen como **protocolo** de la capa n .

En realidad, los datos no se transfieren de la capa n de una máquina al capa n de otra, sino que cada capa pasa datos e **información de control (encabezado)** a la capa que esta inmediatamente debajo de ella, hasta llegar a la capa más baja. Bajo la última capa está el medio físico a través del cual se produce la comunicación real, tal y como se puede ver en la figura (líneas continuas).

Por otro lado, entre cada par de capas adyacentes, hay una **interfaz**, la cual define las operaciones y servicios primitivos que ofrece la capa inferior a la superior.

Definimos la **Arquitectura de una red** o **Arquitectura de un Sistema de Comunicaciones** como el conjunto organizado de niveles y protocolos utilizados para implementar las tareas de comunicación de la misma. La lista de protocolos empleados por cierto sistema, se llama **pila de protocolos**.

ARQUITECTURA DE RED = (qué y cuántas) CAPAS + (con qué) PROTOCOLOS

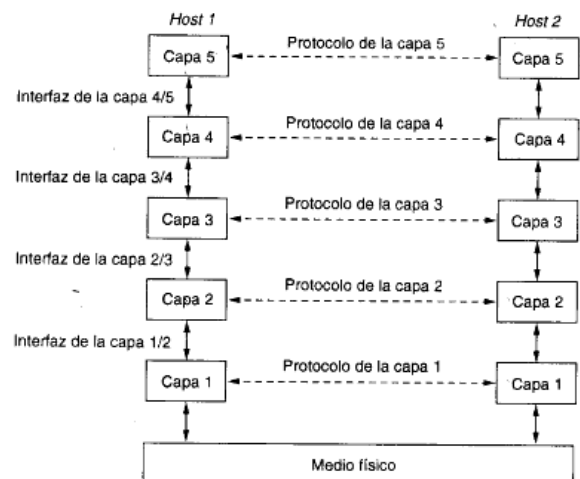
Una capa se diferencia de otras por las funciones que desempeña en el proceso de la comunicación. La capa N puede solicitar servicios a la capa $N-1$. Del mismo modo, la capa $N+1$ solo puede solicitar servicios de la N . Si se cambia algo en la capa N , ninguna otras se verá afectada si se mantienen las estructuras de las interfaces entre las capas $(N+1)/N$ y $N/(N-1)$.

Esto hace que las redes configuradas según el modelo de capas sean muy flexibles.

7.2. SERVICIOS

Las entidades en un nivel N ofrecen servicios que son utilizados por las entidades del nivel $N + 1$. El nivel N es, entonces, el **proveedor del servicio** y el nivel $N + 1$ el **usuario del servicio**. A su vez, el nivel N para proporcionar sus servicios puede utilizar los servicios que le ofrece el nivel $N - 1$.

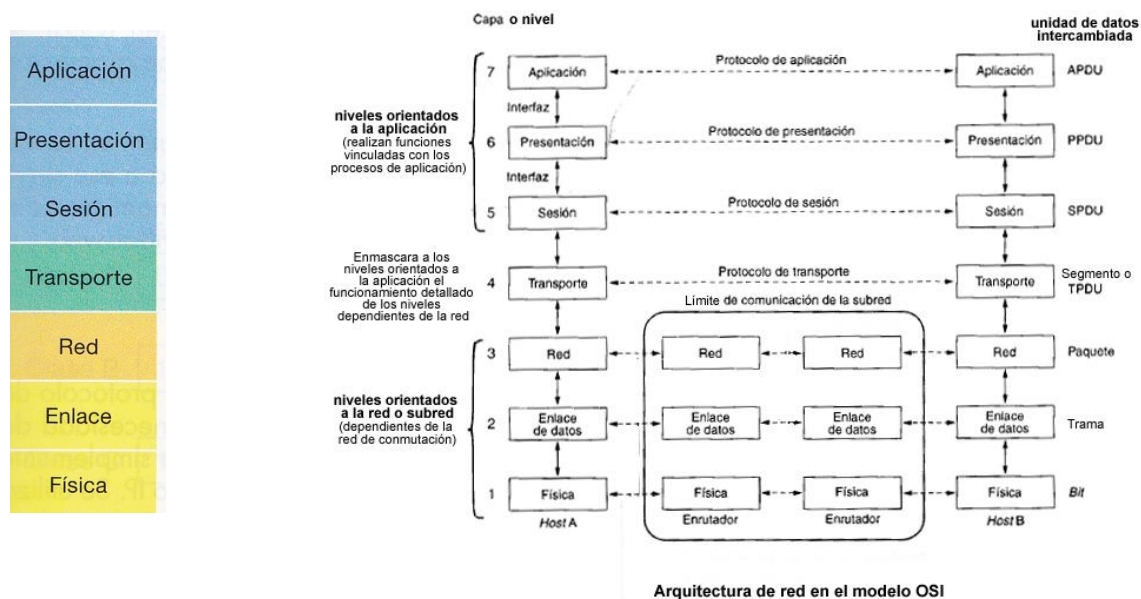
Los servicios se hacen disponibles en los **SAP** (Puntos de acceso al servicio). Los SAPs del Nivel N son los puntos donde el nivel $N + 1$ puede acceder a los servicios ofrecidos.



8. MODELO DE REFERENCIA OSI

Este modelo describe los conceptos fundamentales para la interconexión de **sistemas abiertos**, es decir, sistemas capaces de conectarse con otros sistemas de otros fabricantes de acuerdo con unas normas establecidas.

El modelo OSI propone una **arquitectura de siete capas**:

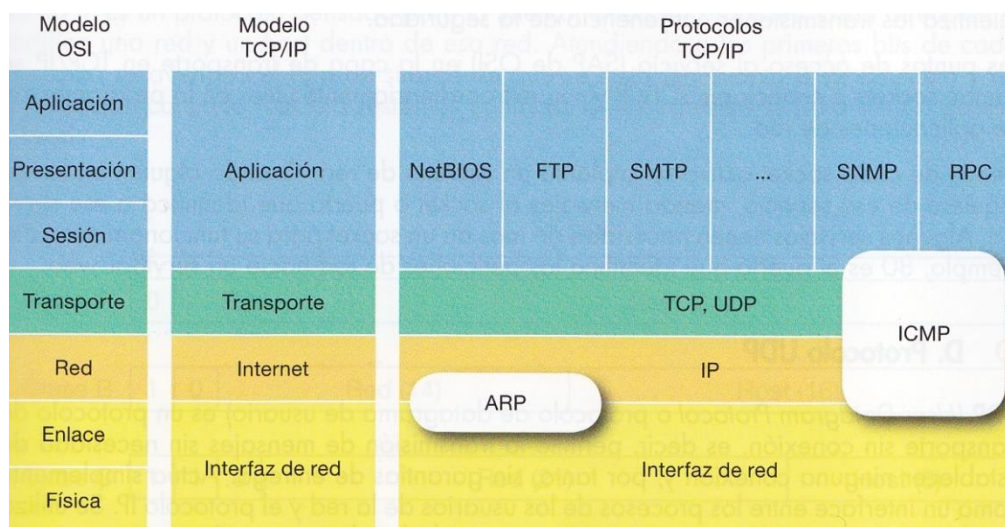


Niveles orientados a la red o subred	Físico	Este nivel define la forma de los cables, su tamaño, voltajes en los que operan, etc...
	Enlace de datos	Aquí encontramos el estándar Ethernet, define el formato de las tramas, sus cabeceras, etc. A este nivel hablamos de direcciones MAC (Media Access Control) que son las que identifican a las tarjetas de red de forma única.
	Red	En esta capa encontramos el protocolo IP . Esta capa es la encargada del enrutamiento y de dirigir los paquetes IP de una red a otra. Normalmente los "routers" se encuentran en esta capa. El protocolo ARP (Address Resolution Protocol) es el que utiliza para mapear direcciones IP a direcciones MAC.
Enmascara a los niveles orientados a la aplicación el funcionamiento detallado de los niveles dependientes de la red	Transporte	En esta capa encontramos 2 protocolos, el TCP (Transmission Control Protocol) y el UDP (User Datagram Protocol). Se encargan de dividir la información que envía el usuario en paquetes de tamaño aceptable por la capa inferior. La diferencia entre ambos es sencilla, el TCP está orientado a conexión, es decir la conexión se establece y se libera, mientras dura una conexión hay un control de lo que se envía y por lo tanto se puede garantizar que los paquetes llegan y están ordenados. El UDP no hace nada de lo anterior, los paquetes se envían y punto, el protocolo se despreocupa si llegan en buen estado etc. El UDP se usa para enviar datos pequeños, rápidamente, mientras que el TCP añade una sobrecarga al tener que controlar los aspectos de la conexión pero "garantiza" la transmisión libre de errores.
Niveles orientados a la aplicación	Sesión	El protocolo de sesión define el formato de los datos que se envían mediante los protocolos de nivel inferior.
	Presentación	External Data Representation (XDR), se trata de ordenar los datos de una forma estándar ya que por ejemplo los Macintosh no usan el mismo formato de datos que los PCs. Este estándar define pues una forma común para todos de tal forma que dos ordenadores de distinto tipo se entiendan.
	Aplicación	Da servicio a los usuarios finales, Mail, FTP, Telnet, DNS, NIS, NFS son distintas aplicaciones que encontramos en esta capa.

9. ARQUITECTURA TCP/IP

El modelo de referencia TCP/IP nació a partir de una implementación concreta: la red ARPANET del Departamento de Defensa de los Estados Unidos. La red ARPANET interconectaba redes heterogéneas de instalaciones gubernamentales y universidades, la cual, (ante el temor de ataques a nodos de la red), tenía que funcionar aunque algunos nodos o enrutadores hubieran caído. Se eligió la tecnología de conmutación de paquetes en modo datagrama y a finales de los años 70 nacieron los protocolos TCP e IP, que se utilizan todavía en la actualidad en Internet.

El modelo TCP/IP cuenta con 4 capas, algunas de las cuales coinciden con el modelo OSI. Aunque TCP/IP no sigue la arquitectura OSI, se pueden establecer paralelismos como los que aparecen en la siguiente figura:



En cada capa del modelo TCP/IP encontramos una serie de **protocolos** (conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red). A continuación se describe los más importantes:

- **Protocolo ARP:** permite averiguar la dirección física (MAC) a partir de la dirección lógica (IP) indicada.
- **Protocolo ICMP:** es el protocolo de mensajes de control entre redes. Expresa eventos que se producen en la red, es decir, se usa para informarnos del estado de la red y saber cómo va todo. Es un protocolo de supervisión.
- **Protocolo IP:** sirve para hacer el encaminamiento. Nos da un servicio sin conexión, es decir, no tenemos garantía de que llegue (de esto ya se encargará TCP).
Este protocolo proporciona un sistema de direcciones para que cada nodo de la red quede identificado por una dirección de 4 números enteros (del 0 al 255) separados por puntos (32 bits binarios en 4 grupos de 8 bits) denominada **dirección IP**.
- **Protocolo TCP:** protocolo encargado de la gestión de errores durante el envío de un paquete de información. Proporciona seguridad en la entrega, ya que es el responsable de ensamblar datagramas IP, de modo que si hay algún problema con alguno de ellos, solicita su retransmisión.
- **Protocolo UDP:** protocolo de transporte sin conexión, es decir, permite la transmisión de mensajes sin necesidad de establecer ninguna conexión y, por tanto, sin garantías de entrega. Se usa para transmisiones rápidas que no necesitan seguridad en la transmisión. Por tanto, tiene un mayor rendimiento que TCP, pero también es más inseguro.

- **Protocolos de nivel superior:**

- **FTP:** protocolo usado para la descarga (bajada) o carga (subida) de ficheros en Internet.
- **HTTP:** protocolo usado por la web, concretamente, es usado por los navegadores de internet para el acceso a las páginas web.
- **SNMP:** protocolo usado para la gestión de la red
- **SMTP:** protocolo para el intercambio de mensajes de correo electrónico entre servidores de correo o el que usa la aplicación cliente de correo para enviar mensajes al servidor al que se conecta.
- **POP:** protocolo encargado de descargar mensajes de correo desde el servidor de correo en donde se encuentra el buzón o la bandeja de entrada del cliente de correo. La versión actual del protocolo es la 3 (POP3)
- **IMAP:** protocolo semejante a POP, pero con funcionalidades añadidas que lo hacen recomendable en situaciones de congestión.