

1.4. Componentes y protocolos de una red



Índice

Introducción	4
Componentes de una red informática	4
Topologías de red	9
Topología en bus	9
Topología en anillo	11
Topología en estrella	13
Topología en árbol	13
Topología en malla	14
Topologías mixtas	15
Qué son las pilas de protocolos	15
Las "pilas" de protocolos	15
¿Y cómo funciona esto de los protocolos?	16
Los niveles OSI	16
Nivel 1 – Capa física	17
Nivel 2 – Enlace	17
Nivel 3 – Red	18
Nivel 4 – Transporte	18
Nivel 5 – Sesión	19
Nivel 6 - Presentación	19
Nivel 7 – Aplicación	19
Recuerda	19
Protocolos TCP/IP	20
Estándares IEEE	21
Tipos de cableado	22
Especificaciones de los sistemas de cableado estructurado	22
Categorías de cable UTP	23
Conectores	23
Conectar periféricos y PC	23
Conexiones de vídeo	24
Conexiones de datos y LAN	25
Mapa físico y lógico de una red	25
Despedida	27
Resumen	27

Los equipos presentes en una red de datos pueden tener diferentes funciones y reciben diferentes nombres en función de ello. Saber distinguirlos y conocer los protocolos que manejan es parte del trabajo de un administrador de sistemas.

Los protocolos responden a estándares emitidos por organismos de normalización o bien por tecnologías predominantes en el mercado que acaban convirtiéndose en "estándares de facto" y aceptados generalmente.

La visión global nos permitirá establecer el mapa físico y lógico de la red, que no necesariamente tienen que ser coincidentes.

Introducción

Componentes de una red informática

En una red podemos encontrar diferentes elementos interconectados y con diferentes funcionalidades dentro de la arquitectura de la propia red.

A grandes rasgos, podemos distinguir entre equipos que son origen o destino de los datos a transmitir a través de la red, y otros equipos encargados de hacer progresar esta información a través de la red, y que genéricamente hemos denominado "**nodos de conmutación**", pero que pueden tener funciones y características muy diferentes.

Tipos de elementos que encontraremos en una red por su funcionalidad:

Estaciones de trabajo

Aunque podemos llamar "**estación de trabajo**" a cualquier ordenador conectado a la red sobre el que trabajan los usuarios, las "estaciones de trabajo" (*workstations*) suelen ser máquinas con muy altas prestaciones y una elevada potencia de cálculo, normalmente con sistemas operativos dedicados a un uso profesional que va más allá de las aplicaciones ofimáticas de una oficina.



Servidor

Un servidor puede ser cualquier ordenador que se encuentre conectado a nuestra red y que esté realizando esa función (atender las peticiones de los ordenadores "clientes" para el acceso a ficheros, ejecutar aplicaciones, etc.).

Los servidores suelen ser equipos especialmente construidos y optimizados para esa función. Esto no quiere decir que un ordenador normal no pueda actuar como "**servidor**" (por ejemplo para controlar la cola de impresión de una impresora), pero si queremos un alto rendimiento y necesitamos atender a un gran volumen de datos o peticiones lo mejor es tener servidores dedicados especializados.

En los centros de datos, por ejemplo, podemos llegar a tener enormes infraestructuras para albergar los servidores de las webs de los clientes del centro.

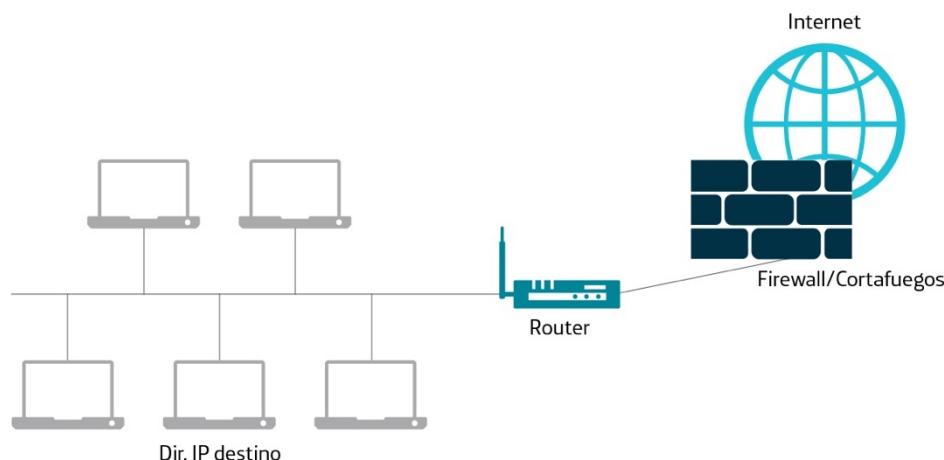


Cortafuegos (firewall)

Realmente el “**cortafuegos**” es una función que puede ser realizada por un solo equipo o un conjunto de dispositivos en la red. El cortafuegos se encarga de establecer una barrera de seguridad entre una parte (normalmente la red interna) y otra (el exterior), por ejemplo para impedir el acceso no autorizado o la realización de determinadas acciones.

Existen cortafuegos que se implementan en un hardware especializado y también cortafuegos implementados por software que se carga en un ordenador de la red.

El cortafuegos puede impedir o permitir el acceso en base a las direcciones de los paquetes de datos, o también por ejemplo en función del tipo de protocolo que se quiere ejecutar (el acceso a ficheros, una traducción de nombres DNS o el acceso a una página web).

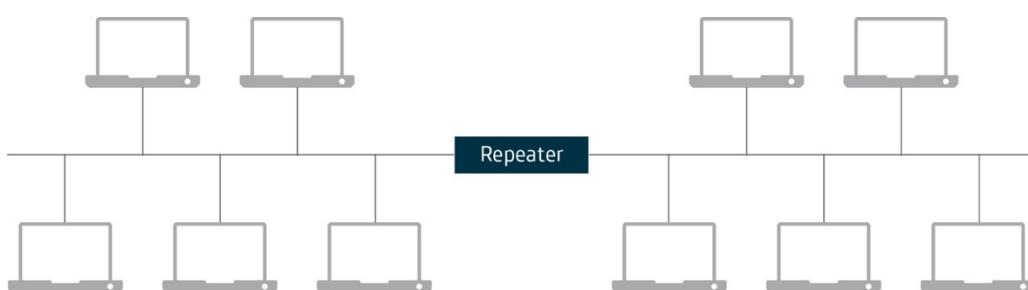


Repetidores (repeaters)

Cuando la longitud del medio de transmisión es elevada y las señales de datos tienen que recorrer una gran distancia se produce un aumento en la atenuación de la señal y puede ser necesario “regenerarla”.

Los **repetidores** simplemente reciben una señal (normalmente débil) y la regeneran amplificada sobre otro tramo del medio de transmisión.

Puede haber repetidores para líneas de cable y también para enlaces radio, y son los que estamos acostumbrados a ver para lograr una mayor cobertura de las redes WIFI en entornos de dificultad de transmisión de la señal.



Concentrador (hub)

Un “*hub*” (concentrador) reproduce la señal que recibe por un puerto por todos los demás (a esto le llamamos hacer “*broadcast*”), es decir, que la señal es “vista” por todos los equipos de la red, lo cual nos permite configurar un “bus lógico” (como veremos más adelante).

Esta forma de funcionar hace que se comparta entre todos el ancho de banda disponible, y que a todos afecten por ejemplo las “*colisiones*” (cuando dos equipos intentan enviar datos al mismo tiempo) en un punto o rama de la red.

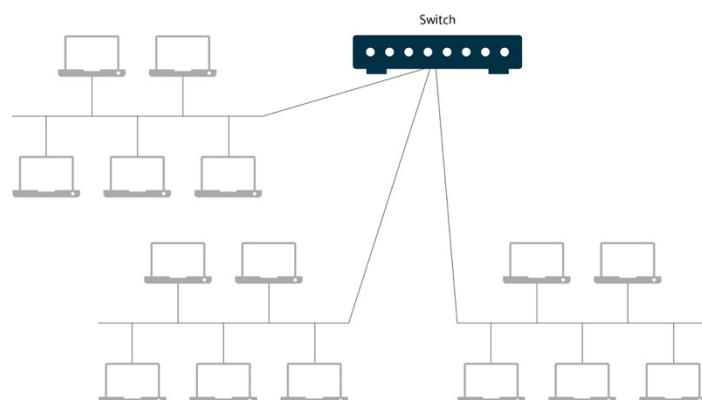
En nuestro uso más cotidiano todos estamos acostumbrados a los “*hub*” de puertos USB, que nos permiten extender el número de interfaces USB de nuestro ordenador, conectándolos a uno de ellos y admitiendo luego varias entradas USB en el concentrador. Los hay con alimentación propia de la red eléctrica o que se alimentan directamente del USB anfitrión del ordenador, con lo cual su capacidad estará más limitada.



Comutador (switch)

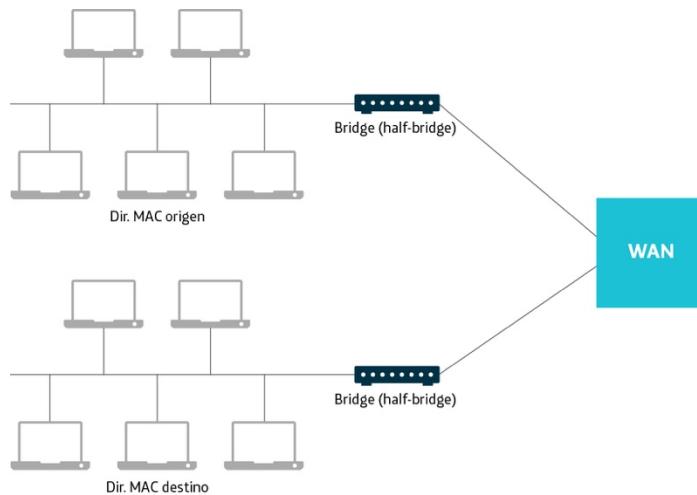
Un “*switch*” también interconecta ramas de la red, pero funciona de forma algo diferente al *hub*. El *switch* recibirá las tramas de información por uno de sus puertos y la reproducirá en otro puerto, por el cual se podrá alcanzar el equipo de destino, es decir, no la copia en todas las ramas de la red, sino que hace un filtrado y la envía solamente por aquella rama que le corresponde para alcanzar el destino de la información.

Como vemos el *switch* es algo más sofisticado, hace una cierta gestión del tráfico entre las ramas de nuestra red y contribuye a su separación (no dejando pasar a una rama la información que no debe ir hacia allí), evitando de este modo que se envíe tráfico innecesario por las ramas de la red, por ello contribuye a aumentar la seguridad y a gestionar el tráfico de la red.



Puente (bridge)

Externamente pueden ser muy parecidos a los *switch*, y realizan prácticamente las mismas funciones, pero el *switch* suele tener un número mayor de puertos (es multipuerto) y se usa para interconectar segmentos a nivel local, mientras que el “**bridge**” se utiliza para interconectar segmentos de la red que están distantes. Se suelen conectar **a través de una red de área amplia (WAN)**, en cuyo caso habrá un *bridge* en cada uno de los extremos o puntos de acceso a la WAN. Cada uno de ellos se suele conocer también como “**half-bridge**” porque juntos realizan la función de “puente”.



Router

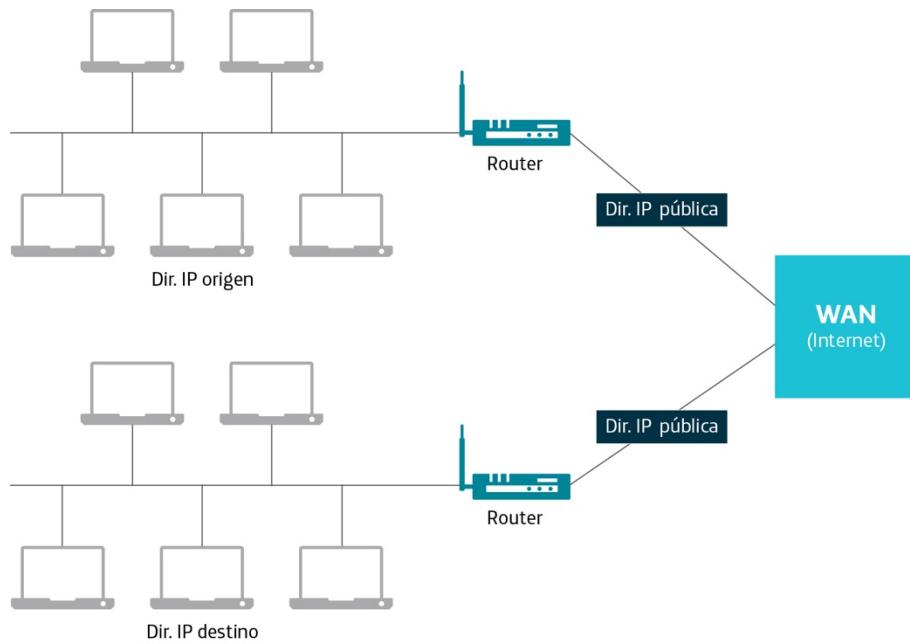
Los “**router**” (**enrutadores**) son dispositivos utilizados para la interconexión de redes. Pueden encaminar el tráfico de los datos siguiendo un **esquema de direccionamiento global a nivel de toda la red**, es decir, en base a “direcciones de red”, un identificativo único que tiene el equipo a nivel de toda la red. Son capaces de ir llevando una determinada información desde un origen a un destino.

Seguramente conocerás lo que son las “**direcciones IP**”; el mecanismo de direccionamiento de Internet (a nivel de toda la red) y de las redes IP en general. También sabrás que las direcciones IP de Internet son direcciones “**públicas**” (que pueden ser conocidas por los demás para enviarnos información) y que las direcciones que puedes tener en la red local de la oficina pueden ser “**direcciones IP privadas**” (solo válidas dentro de nuestra red privada).

Un *router*, a través del cual nuestra red de la oficina se conecta a Internet, deberá entenderse internamente con nuestros equipos manejando las IP privadas de nuestra red, pero de cara al exterior (Internet) deberá manejar una dirección IP pública.

Te pondremos un ejemplo, mi ordenador puede tener una dirección IP privada que sea igual a “192.168.0.192” que es válida en mi red local, y tu ordenador puede tener la misma IP en tu red (es decir, una IP privada con el mismo valor). Pero si nos conectamos a Internet, de cara hacia afuera, no podemos coincidir en nuestras IP, porque son IP públicas y únicas en toda la red mundial. Por ejemplo, ¿sabes cuál es la dirección IP de google.es? Respuesta: 216.58.211.195

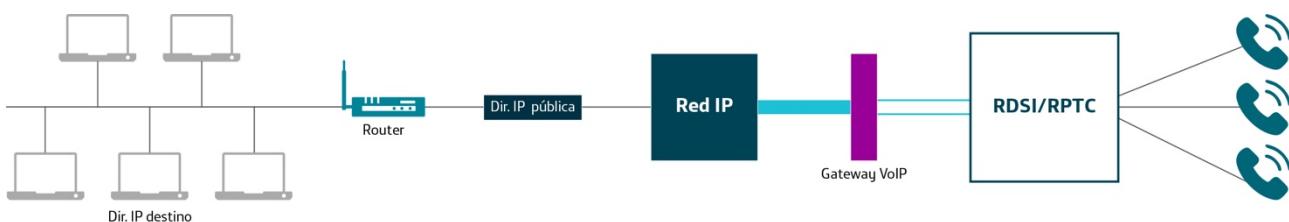
(tranquilo, te enseñaremos como averiguar tanto la tuya como la de Google y muchas más cosas).



Pasarela (gateway)

Un “**gateway**” (pasarela) es un equipo que permite conectar redes que manejan diferentes protocolos, incluso conectar redes que tienen diferentes sistemas de commutación. Por ejemplo, una red de commutación de circuitos, como la red telefónica o la RDSI, y una red de paquetes como Internet.

Los *gateways* trabajan a todos los niveles de protocolo de la red, puesto que tienen que “desempaquetar” la información de un protocolo de una red y volver a “empaquetarla” siguiendo el otro protocolo de la otra red. Decimos que los *gateways* hacen una traducción completa entre protocolos de diferentes redes.



Topologías de red

Ya hemos visto un poco sobre las diferentes topologías de red. Veámoslas ahora un poco más en detalle.

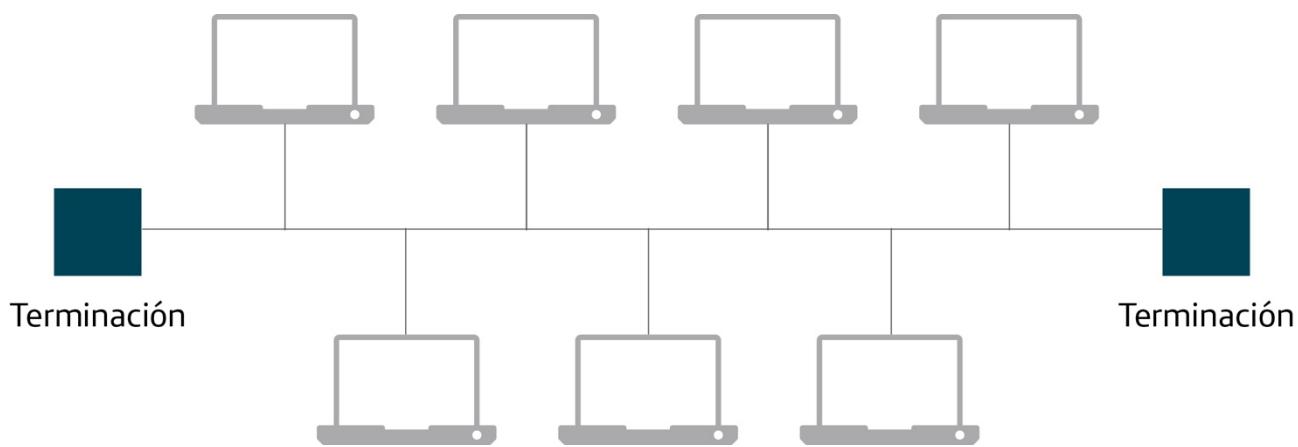
Topología en bus

En esta configuración de la red los equipos se conectan a un único medio de transmisión, en cuyos extremos se colocan unas terminaciones (resistencias).

- **Ventajas:** es bastante fácil de instalar y mantener, y si falla una estación el resto de la red sigue funcionando.
- **Inconvenientes:** si se produce una rotura en el bus los segmentos a ambos lados del fallo quedan aislados.

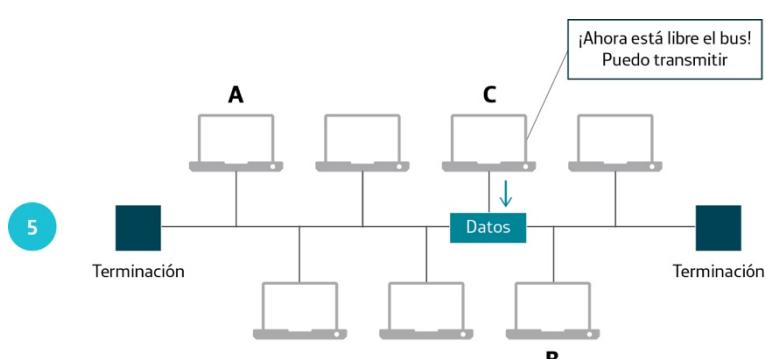
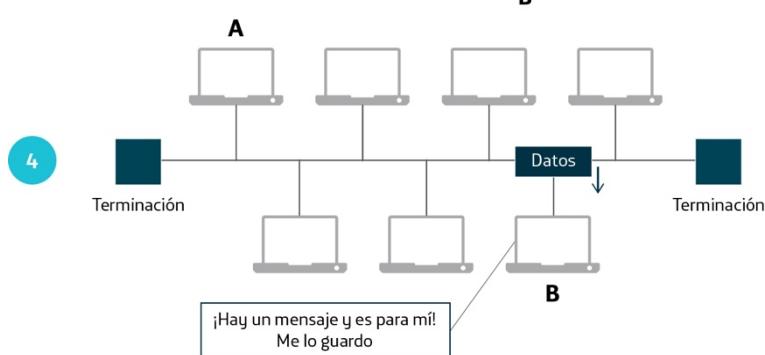
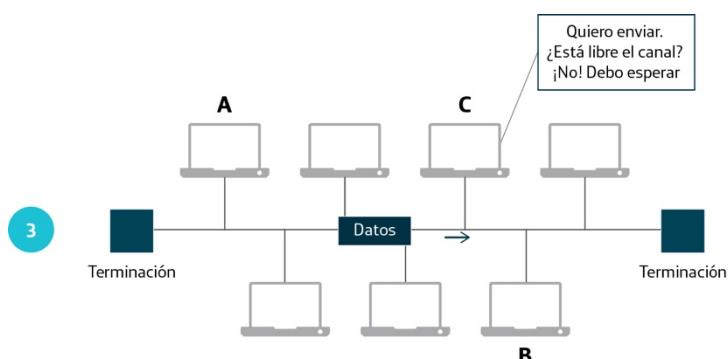
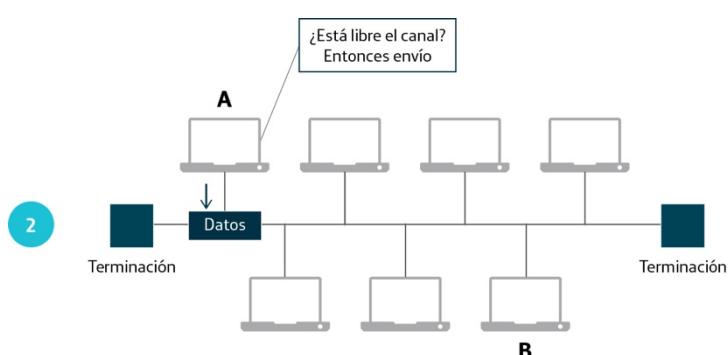
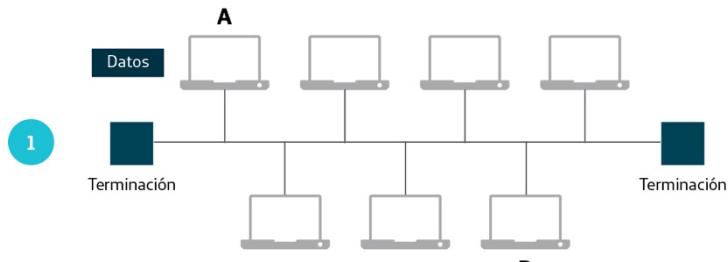
El tipo de red más conocido que utiliza esta tecnología son las redes “**Ethernet**”. El acceso al medio por parte de las estaciones sigue un protocolo de escucha con detección de contienda y colisión (la técnica se llama “acceso múltiple con detección de portadora” y con detección de colisión, y sus siglas son **CSMA/CD**).

Básicamente los equipos escuchan si algún otro está transmitiendo y cuando termina esperan un tiempo antes de empezar a transmitir. Si se produce una colisión porque dos de ellos transmitan al mismo tiempo ambos la detectan, intentan confirmar la transmisión y esperan un tiempo antes de intentarlo de nuevo.



Ethernet trabaja a velocidades de 10 Mbps, 100 Mbps (“**Fast Ethernet**”), 1 Gbps (“**Gigabit Ethernet**”) y 10 Gbps.

¿Cómo funciona? Veamos un ejemplo. Imagina que el equipo **A** quiere enviar un paquete de datos al equipo **B**. Mira la secuencia de gráficos:



Tenemos un equipo A que tiene un paquete de datos que debe enviar hacia otro equipo B, situado en la misma red.

El equipo A, que quiere enviar datos, mira si el bus está libre y si es así envía el paquete de datos por el bus.

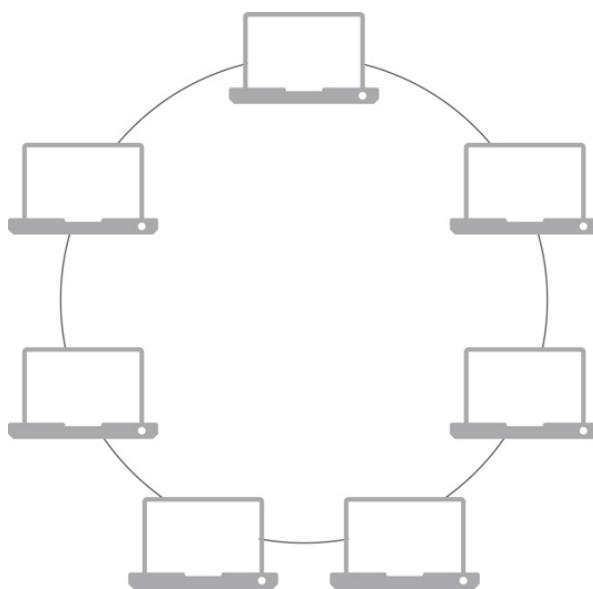
Los datos viajan por el bus, de forma que son “vistos” por todos los equipos conectados a él. Si otro equipo quisiera transmitir también se daría cuenta de que el bus está ocupado y se esperaría a que estuviese libre.

Los datos son también vistos por el equipo B y como van identificados y lo tiene a él como destino, el equipo B los lee y almacena para procesarlos.

Cuando el bus ha quedado libre el otro equipo que quería transmitir puede hacerlo, y continúa el proceso de igual forma.

Topología en anillo

La red más conocida con topología en anillo es la de tecnología “**token ring**”. Los equipos se conectan al anillo a través de unas unidades llamadas “repetidores”, que sirven para insertar y extraer (o eliminar) datos del anillo. Los datos circulan por el anillo en un determinado sentido, pasando de nodo en nodo, y aquel cuya dirección de destino sea la de la información se quedará con ella.

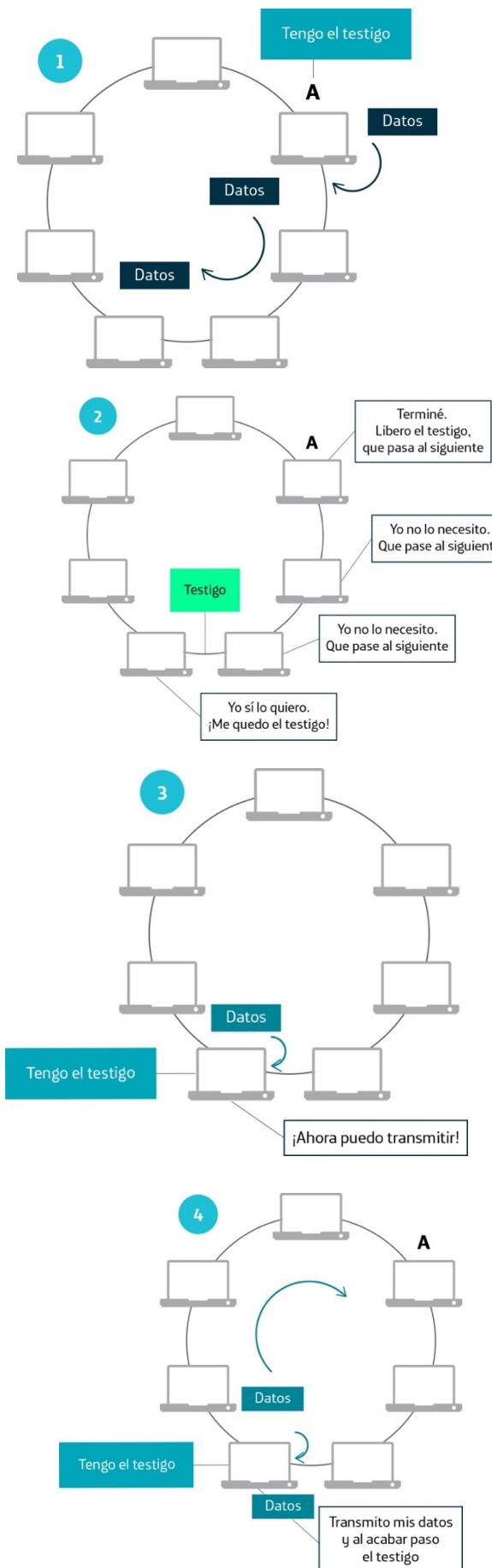


El acceso al medio para el envío de paquetes se controla mediante un “testigo” (“**token**”), que no es más que una trama especial que circula pasando por las estaciones cuando el medio está libre. Si una estación quiere transmitir esperará a que le llegue el token, y entonces lo cambiará para indicar que “tiene el testigo” y comenzará a enviar sus datos.

Las velocidades típicas de trabajo son de 4 Mbps y 16 Mbps, también a 100 Mbps y 1 Gbps (estas dos últimas con un método de acceso al medio ligeramente diferente, el DTR – “*Dedicated Token Ring*”).

Otra red con topología en doble anillo y con paso de testigo son las redes **FDDI**, creadas en principio para la interconexión de redes LAN a través de redes MAN, a velocidades de 100 Mbps.

¿Cómo funciona? Bueno, en este tipo de redes los equipos pueden transmitir solamente si tienen el “testigo”, y cuando terminan lo ceden al siguiente, que lo tomará si lo necesita y si no lo pasará a otro, y así hasta que le llegue a alguno que quiera transmitir y lo “utilice” hasta que termine. Mira la secuencia en los gráficos.



Si un equipo tiene el testigo puede enviar datos al bus. Los datos viajan por el bus llegando a todos los otros equipos, pero solo el destino se quedará con ellos.

Cuando el equipo que estaba transmitiendo termina, libera el “token” (testigo) que pasa al siguiente y si no lo necesita a otro, y así hasta que haya un equipo que tenga datos para transmitir.

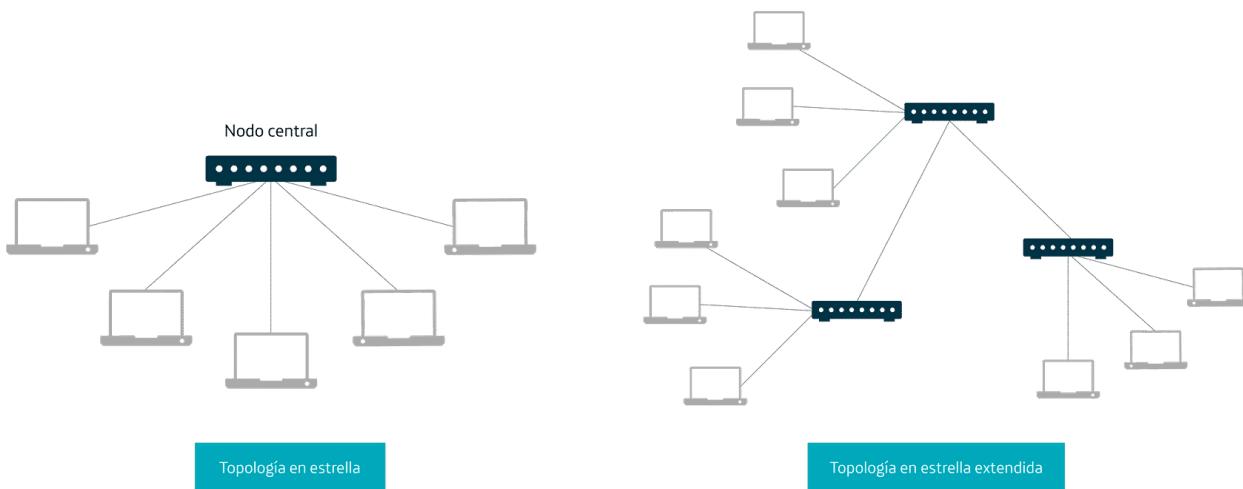
El que quiere enviar datos se queda con el testigo y entonces puede transmitir.

Una vez que tiene el token transmite sus datos hasta que termine, y entonces liberará de nuevo el testigo.

Topología en estrella

En las redes en estrella todos los equipos se conectan a un nodo central y todas las comunicaciones pasan por ese punto, por lo cual será el elemento clave y de su potencia dependerá la calidad de las comunicaciones.

Esta topología se utiliza a menudo en redes locales utilizando como nodo central un conmutador (“**switch**”) o un concentrador (“**hub**”) al que se conectan el resto de los equipos, aunque también puede utilizarse un *router*, que es en realidad lo que hacemos cuando conectamos varios de nuestros ordenadores personales a nuestro *router* de acceso a Internet.



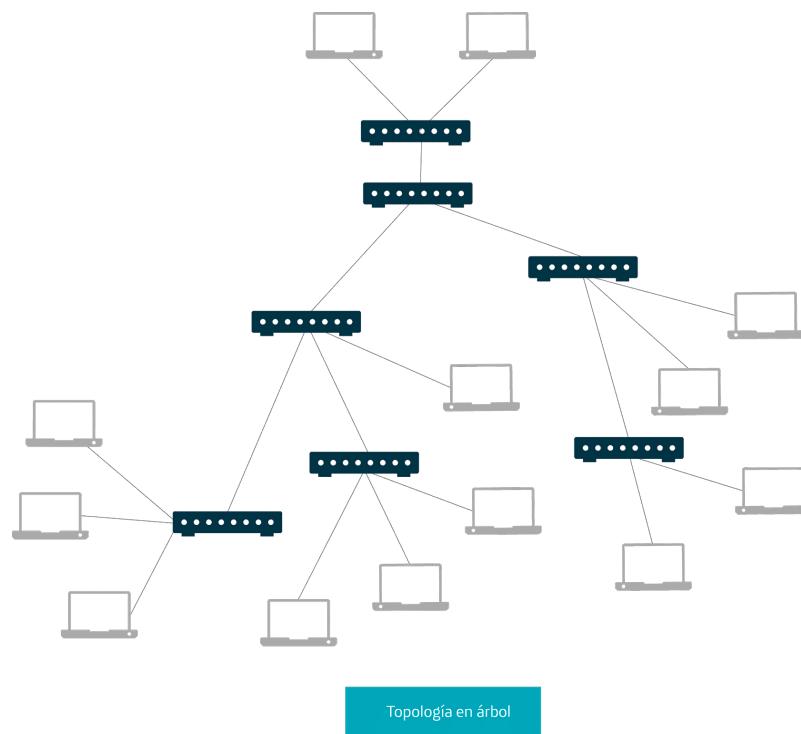
Tiene como ventaja su facilidad de configuración, ya que se realiza de forma centralizada en el nodo central.

Una variante de esta es la “**topología en estrella extendida**”, en la cual los nodos pueden convertirse a su vez en “nodo central” para otro conjunto de equipos.

Topología en árbol

La **topología en árbol** puede verse como la combinación de varias topologías en estrella, aunque sin nodo haciendo la función de “nodo central”, y con un nodo que hace de enlace troncal desde el cual se ramifican los demás nodos.

Al igual que en la red en bus, el fallo de una estación no afecta a las demás, aunque el fallo de un nodo puede afectar a todos los equipos de esa “rama”.

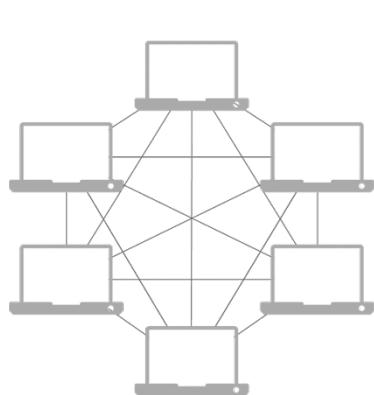


Topología en malla

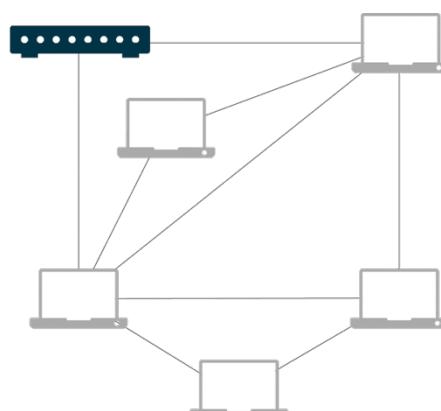
La “**malla**” implica que cada nodo está conectado a uno o varios nodos de la misma red de forma directa, de manera que la información puede seguir diferentes caminos.

Si la red es “**completamente mallada**” quiere decir que todos los equipos tienen conexión con todos los demás, lo cual aporta mucha fiabilidad al disponer de caminos redundantes de comunicación, pero esto es algo difícil de conseguir en cuanto el número de nodos es algo elevado.

Cuando la red está “**parcialmente mallada**” no todos los nodos están conectados, pero alguno/s de ellos sí tienen conexiones con varios de los otros, proporcionando rutas alternativas para el envío de información si fuese necesario.



Red completamente mallada



Topología en malla parcial

Topologías mixtas

Como indica su nombre, son topologías formadas a base de la combinación de otras diferentes. Normalmente la adopción de este tipo de topología viene determinado por la necesidad de hacer convivir redes históricamente diferentes, o bien porque las necesidades de las ubicaciones son tan dispares que requieren el uso de tecnologías diferentes.

La ventaja es precisamente esa, que los elementos de los que disponemos nos permiten conectar redes muy diferentes, pero el hacerlo tiene inconvenientes; como una gestión y configuración mucho más difícil del conjunto; la necesidad de un diseño muy cuidadoso para no producir errores, cuellos de botella o puntos críticos en cuanto a la fiabilidad; y sobre todo que seguramente el mantenimiento será más complejo al disponer de elementos distintos y de diversos fabricantes.

Qué son las pilas de protocolos

Entendemos por "**protocolo**" el conjunto de normas que nos indican cómo han de intercambiarse los datos a través de la red. El **protocolo** determina cómo deben funcionar los equipos, qué información de gestión han de añadir a la información de usuario antes de enviarla por la red y cómo debe interpretarse. Por ejemplo, nos dirán cómo deben ser las direcciones de origen y destino empleadas para poner en el encabezamiento de los paquetes de datos, etc.

Históricamente los protocolos se han ido normalizando a nivel internacional, lo cual ha permitido que fabricantes diferentes puedan hacer componentes que se entiendan entre sí. Estos protocolos son generados por organismos de normalización nacionales e internacionales, a los cuales tenemos que hacer caso si queremos que nuestros equipos puedan trabajar con los de otros proveedores.

MODELO OSI
Nivel 7-Aplicación
Nivel 6-Presentación
Nivel 5-Sesión
Nivel 4-Transporte
Nivel 3-Red
Nivel 2-Enlace
Nivel 1-Capa física

```

graph LR
    Data[Data] --- N6[Nivel 6]
    Segments[Segments] --- N5[Nivel 5]
    Packets[Packets] --- N4[Nivel 4]
    Frames[Frames] --- N2[Nivel 2]
    Bits[Bits] --- N1[Nivel 1]
  
```

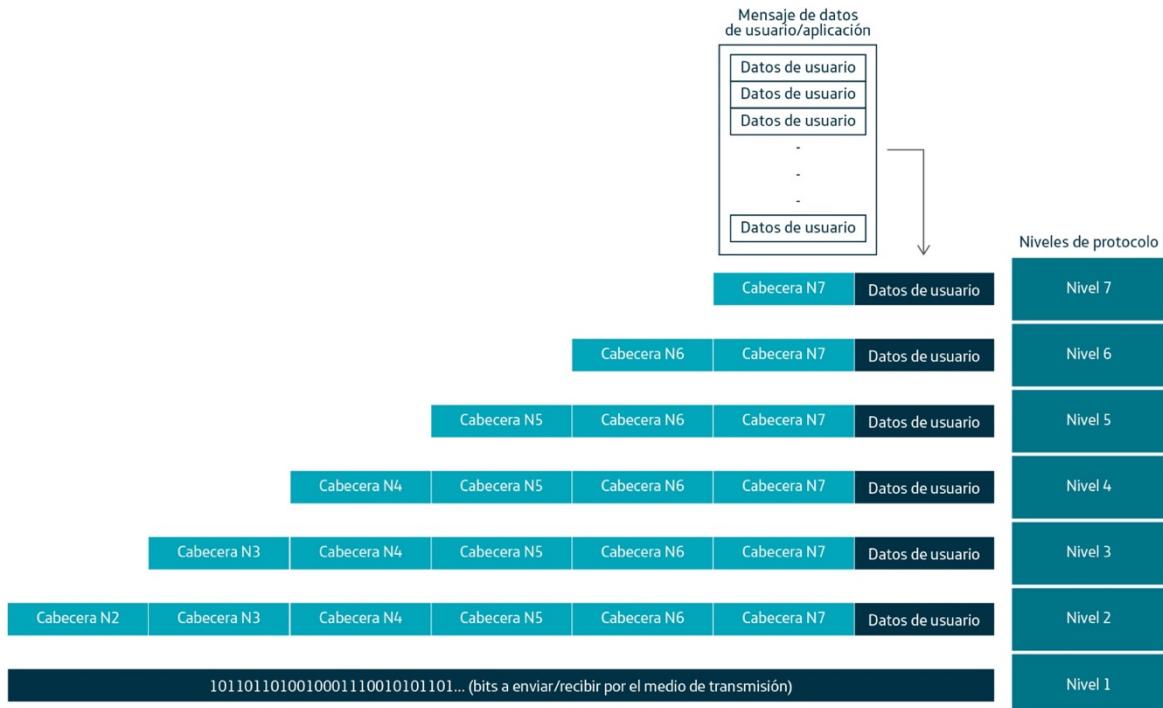
Las "pilas" de protocolos

Existen multitud de protocolos para la transmisión de datos. Normalmente **se definen con una organización en niveles (capas)**, donde cada nivel se ocupa de definir una serie de funciones y cómo deben llevarse a cabo. Es por ello que hablamos de "**pilas de protocolos**", donde la "pila" está formada por el conjunto de niveles "apilado".

En principio, las **funciones de cada nivel (o capa)** se definen para realizar una serie de acciones necesarias para **proporcionar servicio al nivel inmediatamente superior**, de esta forma por ejemplo, los protocolos de "nivel 1" (o "capa 1") dan servicio a los de "nivel 2" (o "capa 2"), y estos a su vez dan servicio a los de "nivel 3", etc.

¿Y cómo funciona esto de los protocolos?

Te lo mostramos con un ejemplo en la figura de abajo. El **mensaje de usuario** a enviar se va a partir en trozos y cada uno se enviará por separado. Luego en el destino se reensambla de nuevo para que el usuario/aplicación (del destino) lo entienda.



Cada **nivel de protocolo** añade una serie de datos (**cabeceras**) que va a interpretar el nivel homólogo del lado receptor. De esta forma el paquete de datos a transmitir va “engordando” al transmitirlo. Al recibirlo, cada nivel interpreta y retira su información, y le pasa al nivel superior la que tiene que leer, es decir, en destino los paquetes van “adelgazando” hasta obtener los trozos de “datos de usuario”, que juntos reconstruyen el mensaje inicial.

Veamos algunos de los principales protocolos empleados en las redes de datos.

Los niveles OSI

Hace ya bastantes años la **ISO (“International Organization for Standardization”)** creó el **“Modelo de referencia OSI”** para la interconexión de sistemas (OSI viene de “Open Systems Interconnection”), que proporcionaba a los fabricantes una referencia para lograr la compatibilidad entre sus equipos.

El modelo de referencia OSI define 7 capas o niveles de protocolos (funciones).

Nivel 1 – Capa física

El **nivel físico** es el que determina las **características físicas del medio** a utilizar para enviar la información en cada tramo, es decir, define las características eléctricas, mecánicas, los parámetros del medio y de la señal a enviar (frecuencias, ancho de banda, atenuación máxima, etc.).

Equipos que trabajan a este nivel son, por ejemplo, los repetidores, los *hubs*, los módems, un fax, y cualquier equipo que inserte físicamente la señal de transmisión en el medio físico.

Especificaciones (protocolos) que pertenecen a este nivel son por ejemplo las tecnologías xDSL, norma V.92 para módem, *firewire*, la capa física de ISDN (RDSI), las especificaciones de transmisión SDH, la especificación de la interfaz de radio GSM, y en general la parte de cualquier especificación que nos indica las características del envío de la señal, las del medio a utilizar, etc.

MODELO OSI

Nivel 7-Aplicación
Nivel 6-Presentación
Nivel 5-Sesión
Nivel 4-Transporte
Nivel 3-Red
Nivel 2-Enlace
Nivel 1-Capa física

Nivel 2 – Enlace

El nivel de enlace, también llamado “**capa de enlace de datos**”, es el encargado de **asegurar la entrega fiable de la información en cada tramo del camino**, a través de un determinado enlace físico.

MODELO OSI

Nivel 7-Aplicación
Nivel 6-Presentación
Nivel 5-Sesión
Nivel 4-Transporte
Nivel 3-Red
Nivel 2-Enlace
Nivel 1-Capa física

En cada tramo se establece un protocolo de nivel 2 entre sus extremos, y en base a su información se establece un control de errores, el control de flujo y la ordenación de la información.

Las direcciones que se manejan identifican físicamente a la interfaz. Por ejemplo, si estamos en una red local, en este nivel se utilizan las **direcciones “MAC”** de las tarjetas de red.

En este nivel hablamos de “**tramas**” para referirnos a las unidades paquetizadas de información que se envían a través del enlace.

Protocolos típicos de este nivel son por ejemplo la estructuración en tramas HDLC, el nivel de enlace de RDSI (ISDN), el protocolo de acceso al medio de las redes Ethernet, etc.

Nivel 3 – Red

El **nivel de red** es el encargado del **direccionamiento de la información a través de la red**. Es en este nivel donde se gestionan las “**direcciones de red**” (identificadores únicos a nivel de la red para el encaminamiento de los datos).

Esta capa es la que proporciona los **mecanismos para hacer que un paquete pueda llegar desde un punto de origen a un punto de destino a nivel de toda la red**. En este nivel se suele hablar de “**paquetes**” para referirnos a las unidades de información que se envían hacia el otro punto de la conexión.

MODELO OSI

Nivel 7-Aplicación
Nivel 6-Presentación
Nivel 5-Sesión
Nivel 4-Transporte
Nivel 3-Red
Nivel 2-Enlace
Nivel 1-Capa física

Básicamente se definen dos tipos de servicios en este nivel:

- **Orientados a conexión:** se envía un primer paquete para establecer un “camino virtual” entre origen y destino, y luego todos los demás paquetes siguen esa misma ruta.
- **No orientados a conexión:** cada paquete se redirecciona de forma independiente a través de la red. Es así por ejemplo como funciona IP.

Algunos protocolos de este nivel: el nivel 3 de RSDI (ISDN), el nivel 3 de X.25, el protocolo IP (aunque este no siga la filosofía OSI).

Nivel 4 – Transporte

Este nivel es el encargado de **asegurar una buena transferencia de datos extremo a extremo**. En esta capa se hace una segmentación de los datos (en el origen) que van a ser enviados en paquetes a través de la red, y se produce un re-ensamblado al llegar al destino. Se emplean mecanismos de detección y recuperación de errores y control de flujo.

Esta capa (junto con las capas inferiores) proporciona el servicio de transporte de datos a los niveles superiores y los independiza de esta problemática.

Es este nivel el **encargado de establecer**, mantener mientras dure la comunicación y liberar los “**circuitos virtuales**” para el intercambio de datos cuando la comunicación es “**orientada a conexión**”.

En este nivel es común referirnos a la información a enviar como “**segmentos**” de mensaje, que luego serán particionados y enviados en paquetes de nivel inferior.

MODELO OSI

Nivel 7-Aplicación
Nivel 6-Presentación
Nivel 5-Sesión
Nivel 4-Transporte
Nivel 3-Red
Nivel 2-Enlace
Nivel 1-Capa física

Nivel 5 – Sesión

Este nivel es el encargado de **establecer, administrar y finalizar las sesiones de intercambio de información entre origen y destino** (entre el “*host*” de origen y el “*host*” de destino).

Al administrar la sesión se encarga de informar de posibles problemas de las capas superiores y establecer clases de servicio.

MODELO OSI

Nivel 7-Aplicación
Nivel 6-Presentación
Nivel 5-Sesión
Nivel 4-Transporte
Nivel 3-Red
Nivel 2-Enlace
Nivel 1-Capa física

Nivel 6 - Presentación

Esta capa es la encargada de que la información que se va a enviar a la capa de aplicación va a poder ser leída e interpretada. Se encarga por ejemplo de la **traducción de formatos** cuando es necesario y del **cifrado y descifrado** de la comunicación cuando procede. Trabaja con **estándares para gráficos** como el JPEG, el TIFF y el PICT.

MODELO OSI

Nivel 7-Aplicación
Nivel 6-Presentación
Nivel 5-Sesión
Nivel 4-Transporte
Nivel 3-Red
Nivel 2-Enlace
Nivel 1-Capa física

Nivel 7 – Aplicación

Es la capa superior del modelo, por lo que no proporciona servicio a otras capas, sino que **sirve de interfaz para las aplicaciones de usuario**, atendiendo sus peticiones de comunicación, proporcionando los recursos necesarios y estableciendo procedimientos de comprobación y recuperación de errores con dichas aplicaciones.

MODELO OSI

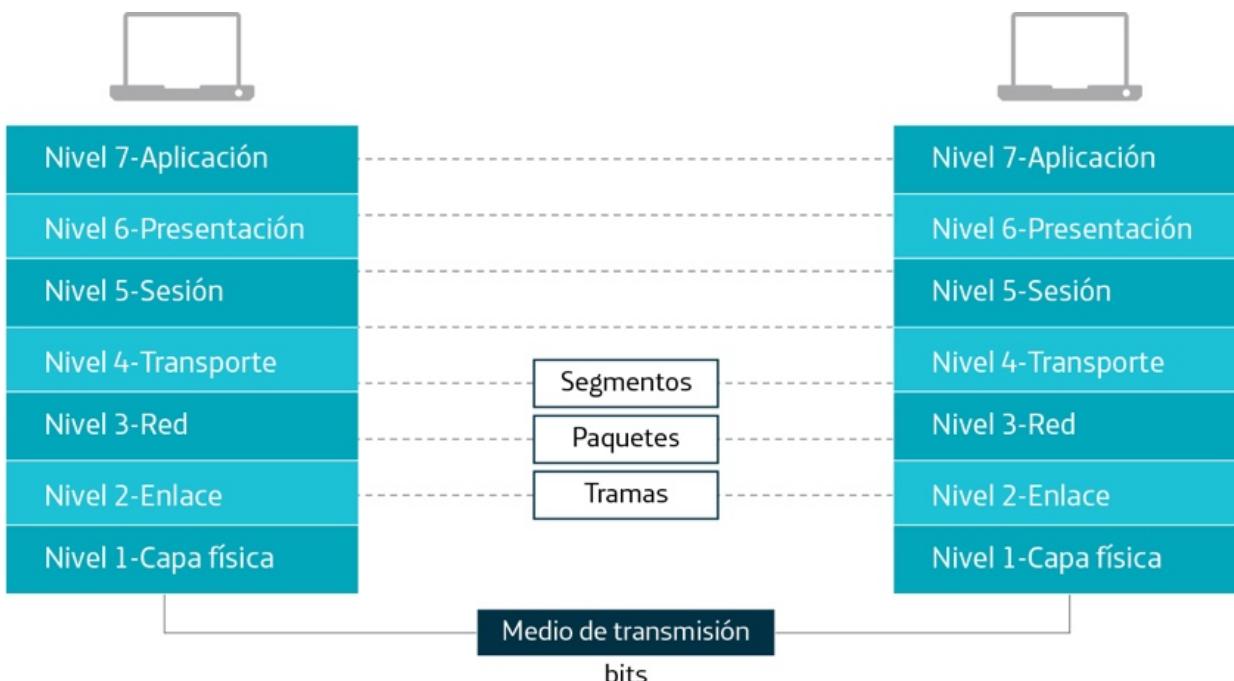
Nivel 7-Aplicación
Nivel 6-Presentación
Nivel 5-Sesión
Nivel 4-Transporte
Nivel 3-Red
Nivel 2-Enlace
Nivel 1-Capa física

Recuerda

Es importante darse cuenta de que **la comunicación entre el origen y destino se realiza entre niveles homólogos**, es decir, la información de un determinado nivel es interpretada por su nivel homólogo en el otro lado (es una comunicación *peer-to-peer*), y es transparente para el resto de los niveles.

En origen, cada capa irá añadiendo información de gestión a la información de la aplicación del usuario (la necesaria para gestionar su transferencia por la red y proporcionar el servicio completo), y al llegar al destino los niveles homólogos irán interpretando y retirando esa

información, de forma que al usuario (aplicación) de destino se le entregue solamente una copia fiel de lo que le ha enviado el origen.



Protocolos TCP/IP

Los niveles OSI se definieron antes de que hubiese Internet y se aplicaron al diseño de las redes de comunicaciones de datos durante mucho tiempo.

Sin embargo, los protocolos que se definieron para Internet, es decir, la **familia de protocolos TCP/IP**, no siguieron esta división de funciones, sino que tienen otra, que se puede asemejar a como ves en la figura.

MODELO OSI	Ej. protocolos	MODELO TCP/IP
Nivel 7-Aplicación	HTTP, HTTPS, FTP, Telnet, SSH, POP3, IMAP, NTP, DHCP, PING, DNS, WINS	Nivel de Aplicación
Nivel 6-Presentación		
Nivel 5-Sesión		
Nivel 4-Transporte	TCP, UDP	Nivel de Transporte
Nivel 3-Red	IP, ARP, ICMP, IGMP	Nivel de Red
Nivel 2-Enlace	Ethernet, Token Ring, SDH, GSM, ATM	Interfaz de Red
Nivel 1-Capa física		

Aunque profundizaremos más adelante, te avanzamos que el protocolo **HTTP** es el que utilizas cada vez que quieras ver una página web, que los protocolos **POP3** e **IMAP** los utilizas para ver tu correo, que el protocolo **Telnet** se utiliza para la conexión remota a otros equipos, o que si queremos intercambiar ficheros entre dos máquinas podemos emplear el **FTP**.

Pero como te decimos, volveremos sobre ello y con mayor detalle.

Estándares IEEE

El **IEEE** es el “*Institute of Electrical and Electronics Engineers*” (Instituto de Ingenieros Eléctricos y Electrónicos), una organización profesional sin ánimo de lucro dedicada a la estandarización y generación de normativa técnica.



El IEEE es quizás el principal generador de estándares para redes de área local a través de la familia de normas “802”, definiendo especificaciones para los niveles físico y de enlace del modelo OSI.

Además de la familia “802”, el IEEE define muchas otras especificaciones, como por ejemplo:

- IEEE 1394 – Entrada/salida serie de datos a alta velocidad (p. ej. cámaras y PC).
- IEEE 488 – Bus de datos digital (instrumentos de medida).
- IEEE 802 – Estándares para redes LAN y MAN.
- IEEE 802.11 – Redes inalámbricas WLAN.
- IEEE 754 – Estándar para aritmética en coma flotante.
- IEEE 830 – Especificación de requisitos software.

Familia de normas “802” de IEEE

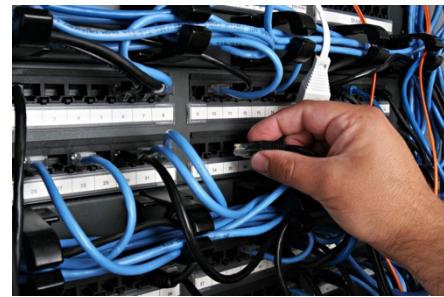
Familia	Área	Objetivo de las especificaciones
802.1	Definición internacional de redes	Relación entre normas 802 de IEEE y OSI.
802.2	Control de enlaces lógicos	Protocolo de control de enlace (LLC).
802.3	Redes CSMA/CD - Redes Ethernet	Define el estándar sobre diferentes medios: par trenzado, coaxial, fibra óptica.
802.4	Redes Token Bus	Estándar para redes de ancho de banda grandes usados en industria.
802.5	Redes Token Ring	Protocolo ANSI 802.1-1985. Define el acceso, cableado e interface para la LAN Token Ring.
802.6	Redes de área metropolitana (MAN)	Protocolo para redes MAN de alta velocidad sobre F.O. usando un método de colas DQDB.
802.7	Grupo asesor técnico de anchos de banda	Comité de apoyo sobre anchos de banda en redes.
802.8	Grupo asesor técnico de fibra óptica	Comité de apoyo sobre fibra óptica.
802.9	Redes integradas de voz y datos	Trabaja en la integración de comunicaciones de voz y datos.
802.10	Grupo asesor técnico de seguridad de redes	Definición de modelo de seguridad y estándar, mecanismos de autenticación y encriptamiento.
802.11	Redes inalámbricas	Estándares para redes inalámbricas.
802.12	Prioridad de demanda (100VG-ANYLAN)	Estándar para Ethernet a 100 Mbps con el método de acceso por prioridad de demanda.

Tipos de cableado

Hasta ahora hemos visto las diferentes topologías de red (anillo, estrella, bus, etc.) y los distintos medios de transmisión a emplear, pero a la hora de realizar la instalación real, en la práctica una de las mayores dificultades es efectuar el **cableado de la red**.

Salvo para las redes inalámbricas, donde el medio de transmisión es el espacio abierto (y que tienen otras dificultades como la cobertura de la señal de radio, el ruido, etc.), para las redes basadas en conexiones por cable resulta crucial hacer un "tendido" lo más eficiente posible y de forma que su mantenimiento posterior sea lo menos complicado posible. Pensemos en lo difícil que puede ser cambiar un cable roto en una maraña de cables todos iguales y sin identificar.

Para contribuir a lograr una instalación eficiente de los cables se diseñaron **sistemas de "cableado estructurado"**, que consisten en realizar una preinstalación ordenada del cableado, integrando normalmente los cables para las redes de datos y los de las redes telefónicas, y proporcionando puntos de acceso normalizados en los puestos de trabajo, con puertos de conexión para los ordenadores y equipos de usuario.



Los cables se van agrupando ordenadamente en mazos que se direccionan hasta un cuadro o bastidor central, desde donde se conectan a los equipos de conmutación de la red.

Especificaciones de los sistemas de cableado estructurado

Los sistemas de cableado estructurado tienen sus propias especificaciones, y así para el cableado en edificios comerciales existe la norma "**EIA/TIA 568**", que concibe el cableado como un servicio más a instalar (como la instalación de luz o de gas), y especifica desde las señales que se pueden usar hasta las características mecánicas de los cables, conectores, armarios, etc.

Estos sistemas de cableado normalmente especifican la necesidad de hacer dos tipos de instalación:

- **Instalación horizontal de cableado:** normalmente ocupa cada una de las plantas del edificio, y suele haber un "armario de planta".
- **Instalación vertical de cableado:** desde cada armario de planta se hace una instalación hasta una sala especialmente acondicionada para albergar los dispositivos de red y los equipos de conexión hacia el exterior, coexistiendo a menudo con la centralita telefónica de la empresa, sistemas de alimentación ininterrumpida (SAI), etc.

Todas las conexiones se llevan a un punto central, donde se produce el conexionado y en caso de avería es muy fácil reemplazar la conexión defectuosa. Todas las conexiones de un sistema de cableado estructurado están identificadas y la arquitectura de las líneas tendidas perfectamente documentada.

Categorías de cable UTP

El **cable UTP** (par trenzado no apantallado) es el más utilizado actualmente en el tendido de las redes, pero no todos los cables UTP son iguales. Están normalizados según categorías:

1. **UTP categoría 1**: definido en la norma EIA/TIA 568B, se usa para instalación de telefonía y no es adecuado para redes de datos.
2. **UTP categoría 2**: puede transmitir datos hasta 4 Mbps.
3. **UTP categoría 3**: se usa en redes Ethernet 10 BaseT y puede transportar datos hasta 10 Mbps.
4. **UTP categoría 4**: se usa en redes Token-Ring hasta los 16 Mbps.
5. **UTP categoría 5 y 5e**: puede transmitir datos hasta 100 Mbps (Ethernet 100 BaseT).
6. **UTP categoría 6**: velocidades de hasta 1 Gbps.

Conectores

Los conectores a emplear en nuestras conexiones dependerán del tipo de interfaz al que queramos enchufarlos y del medio de transmisión que conectan.

Algunos de los más utilizados son:

Coneectar periféricos y PC



Conector puerto serie – solo datos. 9 pines.



USB – Conexión “plug and play” de periféricos al ordenador.

Conexiones de vídeo



VGA (RGB) – Conexión de una pantalla o un video-proyector con el PC. 15 pines.



DVI – para conexión de video.



Euroconector – audio y video compuesto.



Firewire (i-link) – audio y video a alta velocidad en cámaras y dispositivos "plug and play".

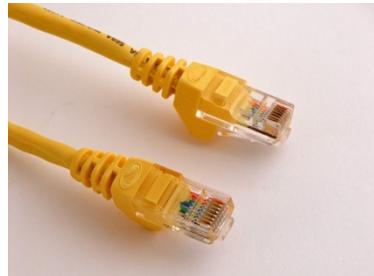


HDMI – audio y vídeo de alta definición.

Conexiones de datos y LAN



RJ11 – Conexión a líneas telefónicas.



RJ45 – Conexión de datos a red local.



BNC – Conexión de cable coaxial.



Conectores de Fibra óptica (SC).



Conectores de Fibra óptica (FC).

Mapa físico y lógico de una red

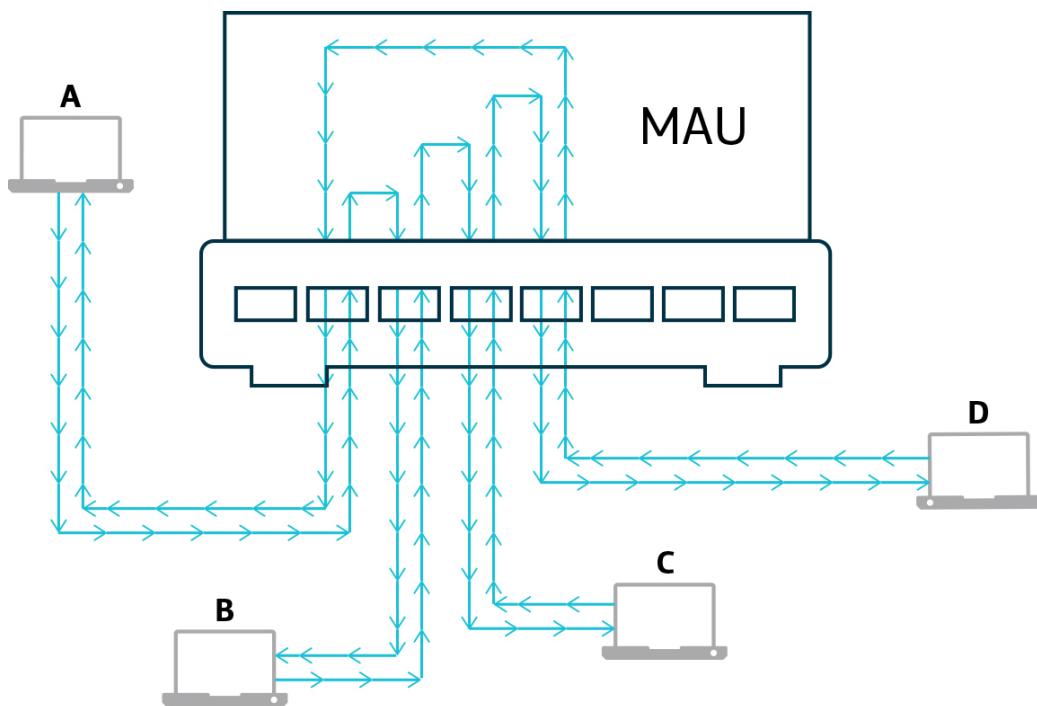
Hemos visto ya las topologías físicas que pueden tener las redes de datos.

Sin embargo, en función de cómo se configuren los dispositivos de conexión y commutación y las reglas que se programen, el camino seguido por los datos puede variar.

Hablamos entonces de “**topología lógica**” o “**mapa lógico**” de la red para referirnos a la configuración lógica de funcionamiento de la red.

Los dos mecanismos de configuración más utilizados a la hora de configurar una topología lógica son el “**broadcast**” (los nodos envían su información a todos los demás) y el “**token**” (cada nodo solo transmite cuando tiene el testigo).

Ejemplos de topologías lógicas:



Anillo lógico / estrella física

- Una red en estrella (arquitectura física) funcionando como un anillo (topología lógica en anillo).
- Una topología lógica de bus sobre una conexión en estrella física.

También pueden utilizarse dispositivos físicos; por ejemplo en una red *Token-Ring* funcionando en anillo se puede instalar lo que se llama una “**Unidad de Acceso Multiestación**” (MAU) como nodo central, a la que se conectan todas las estaciones, con lo cual tendríamos una disposición física en estrella.

Despedida

Resumen

Llegados a este punto ya sabes algo más sobre las redes y su funcionamiento. Debes recordar (es muy importante) la diferencia entre los distintos tipos de elementos que hemos visto, es decir: *repeater, hub, switch, router, bridge, gateway...* Fíjate que los ponemos con el término en inglés porque queremos que te acostumbres a ellos. Los verás muy a menudo y en muchos sitios.

Por favor, recuerda también los distintos tipos de topologías de red (bus, anillo, malla, árbol) y que en la práctica podemos encontrar redes mixtas que combinen varias tipologías.

Otro concepto importante, y que no debes olvidar, es lo que significa un "**protocolo**" de datos. Recuerda también que hay muchos tipos, pero la mayoría estructuran sus funciones en forma de niveles o capas, de forma que cada una de ellas se encarga de realizar parte del trabajo y da servicio a la inmediatamente superior hasta llegar a la que da servicio a la propia aplicación de usuario.

Los protocolos más conocidos en la actualidad, además de la pila OSI, son la familia TCP/IP, pero no te preocupes porque volveremos sobre ello más adelante en este curso.