Tipos de redes

Clasificación de las redes

Se denomina red de computadores una serie de host autónomos y dispositivos especiales intercomunicados entre sí.

Ahora bien, este concepto genérico de red incluye multitud de tipos diferentes de redes y posibles configuraciones de las mismas, por lo que desde un principio surgió la necesidad de establecer clasificaciones que permitieran identificar estructuras de red concretas.

La posibles clasificaciones de las redes pueden ser muchas, atendiendo cada una de ellas a diferentes propiedades, siendo las más comunes y aceptadas las siguientes:

Clasificación de las redes según su tamaño y extensión:

1. **Redes LAN**. Las redes de área local (Local Area Network) son redes de ordenadores cuya extensión es del orden de entre 10 metros a 1 kilómetro. Son redes pequeñas, habituales en oficinas, colegios y empresas pequeñas, que generalmente usan la tecnología de broadcast, es decir, aquella en que a un sólo cable se conectan todas las máquinas. Como su tamaño es restringido, el peor tiempo de transmisión de datos es conocido, siendo velocidades de transmisión típicas de LAN las que van de 10 a 100 Mbps (Megabits por segundo).
2. **Redes MAN**. Las redes de área metropolitana (Metropolitan Area Network) son redes de ordenadores de tamaño superior a una LAN, soliendo abarcar el tamaño de una ciudad. Son típicas de empresas y organizaciones que poseen distintas oficinas repartidas en un mismo área metropolitana, por lo que, en su tamaño máximo, comprenden un área de unos 10 kilómetros.
3. **Redes WAN**. Las redes de área amplia (Wide Area Network) tienen un tamaño superior a una MAN, y consisten en una colección de host o de redes LAN conectadas por una subred. Esta subred está formada por una serie de líneas de transmisión interconectadas por medio de routers, aparatos de red encargados de rutear o dirigir los paquetes hacia la LAN o host adecuado, enviándose éstos de un router a otro. Su tamaño puede oscilar entre 100 y 1000 kilómetros.
4. **Redes internet**. Una internet es una red de redes, vinculadas mediante ruteadores gateways. Un gateway o pasarela es un computador especial que puede traducir información entre sistemas con formato de datos diferentes. Su tamaño puede ser desde 10000 kilómetros en adelante, y su ejemplo más claro es Internet, la red de redes mundial.
5. **Redes inalámbricas**. Las redes inalámbricas son redes cuyos medios físicos no son cables de cobre de ningún tipo, lo que las diferencia de las redes anteriores. Están basadas en la transmisión de datos mediante ondas de radio, microondas, satélites o infrarrojos.

Clasificación de las redes según la tecnología de transmisión:

1. **Redes de Broadcast**. Aquellas redes en las que la transmisión de datos se realiza por un sólo canal de comunicación, compartido entonces por todas las máquinas de la red. Cualquier paquete de datos enviado por cualquier máquina es recibido por todas las de la red.

2. **Redes Point-To-Point**. Aquellas en las que existen muchas conexiones entre parejas individuales de máquinas. Para poder transmitir los paquetes desde una máquina a otra a veces es necesario que éstos pasen por máquinas intermedias, siendo obligado en tales casos un trazado de rutas mediante dispositivos routers.

Clasificación de las redes según el tipo de transferencia de datos que soportan:

- **Redes de transmisión simple**. Son aquellas redes en las que los datos sólo pueden viajar en un sentido.
- **Redes Half-Duplex**. Aquellas en las que los datos pueden viajar en ambos sentidos, pero sólo en uno de ellos en un momento dado. Es decir, sólo puede haber transferencia en un sentido a la vez.
- **Redes Full-Duplex**. Aquellas en las que los datos pueden viajar en ambos sentidos a la vez.

Tipos de redes

Topologías de red

Hemos visto en el tema sobre el modelo OSI y la arquitectura TCP/IP que las redes de ordenadores surgieron como una necesidad de interconectar los diferentes host de una empresa o institución para poder así compartir recursos y equipos específicos.

Pero los diferentes componentes que van a formar una red se pueden interconectar o unir de diferentes formas, siendo la forma elegida un factor fundamental que va a determinar el rendimiento y la funcionalidad de la red.

La disposición de los diferentes componentes de una red se conoce con el nombre de **topología de la red**. La topología idónea para una red concreta va a depender de diferentes factores, como el número de máquinas a interconectar, el tipo de acceso al medio físico que deseemos, etc.

Podemos distinguir tres aspectos diferentes a la hora de considerar una topología:

1. La topología física, que es la disposición real de las máquinas, dispositivos de red y cableado (los medios) en la red.
2. La topología lógica, que es la forma en que las máquinas se comunican a través del medio físico. Los dos tipos más comunes de topologías lógicas son broadcast (Ethernet) y transmisión de tokens (Token Ring).
3. La topología matemática, mapas de nodos y enlaces, a menudo formando patrones.

La topología de broadcast simplemente significa que cada host envía sus datos hacia todos los demás hosts del medio de red. Las estaciones no siguen ningún orden para utilizar la red, sino que cada máquina accede a la red para transmitir datos en el momento en que lo necesita. Esta es la forma en que funciona Ethernet.

En cambio, la transmisión de tokens controla el acceso a la red al transmitir un token eléctrico de forma secuencial a cada host. Cuando un host recibe el token significa que puede enviar datos a través de la red. Si el host no tiene ningún dato para enviar, transmite el token hacia el siguiente host y el proceso se vuelve a repetir.

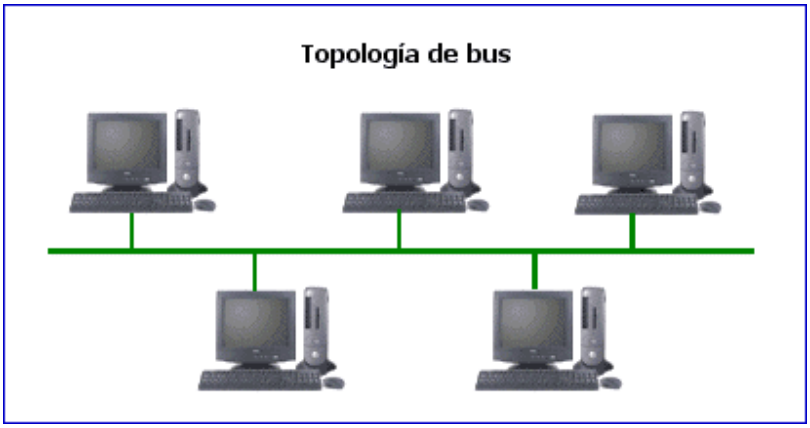
Vamos a ver a continuación los principales modelos de topología.

Modelos de topología

Las principales modelos de topología son:

Topología de bus

La topología de bus tiene todos sus nodos conectados directamente a un enlace y no tiene ninguna otra conexión entre nodos. Físicamente cada host está conectado a un cable común, por lo que se pueden comunicar directamente, aunque la ruptura del cable hace que los hosts queden desconectados.



La topología de bus permite que todos los dispositivos de la red puedan ver todas las señales de todos los demás dispositivos, lo que puede ser ventajoso si desea que todos los dispositivos obtengan esta información. Sin embargo, puede representar una desventaja, ya que es común que se produzcan problemas de tráfico y colisiones, que se pueden paliar segmentando la red en varias partes.

Es la topología más común en pequeñas LAN, con hub o switch final en uno de los extremos.

Topología de anillo

Una topología de anillo se compone de un solo anillo cerrado formado por nodos y enlaces, en el que cada nodo está conectado solamente con los dos nodos adyacentes.

Los dispositivos se conectan directamente entre sí por medio de cables en lo que se denomina una cadena margarita. Para que la información pueda circular, cada estación debe transferir la información a la estación adyacente.

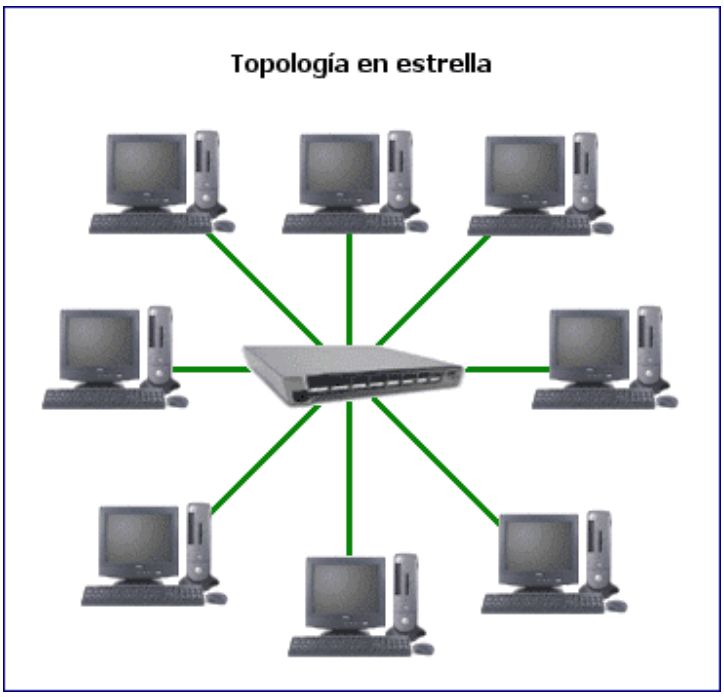
Topología de anillo doble

Una topología en anillo doble consta de dos anillos concéntricos, donde cada host de la red está conectado a ambos anillos, aunque los dos anillos no están conectados directamente entre sí. Es análoga a la topología de anillo, con la diferencia de que, para incrementar la confiabilidad y flexibilidad de la red, hay un segundo anillo redundante que conecta los mismos dispositivos.

La topología de anillo doble actúa como si fueran dos anillos independientes, de los cuales se usa solamente uno por vez.

Topología en estrella

La topología en estrella tiene un nodo central desde el que se irradian todos los enlaces hacia los demás nodos. Por el nodo central, generalmente ocupado por un hub, pasa toda la información que circula por la red.



La ventaja principal es que permite que todos los nodos se comuniquen entre sí de manera conveniente. La desventaja principal es que si el nodo central falla, toda la red se desconecta.

Topología en estrella extendida:

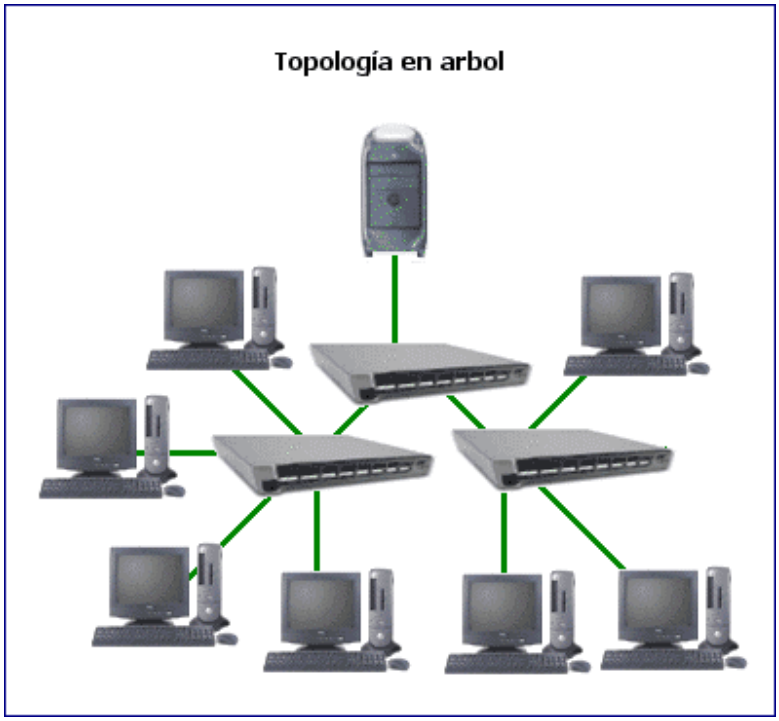
La topología en estrella extendida es igual a la topología en estrella, con la diferencia de que cada nodo que se conecta con el nodo central también es el centro de otra estrella. Generalmente el nodo central está ocupado por un hub o un switch, y los nodos secundarios por hubs.

La ventaja de esto es que el cableado es más corto y limita la cantidad de dispositivos que se deben interconectar con cualquier nodo central.

La topología en estrella extendida es sumamente jerárquica, y busca que la información se mantenga local. Esta es la forma de conexión utilizada actualmente por el sistema telefónico.

Topología en árbol

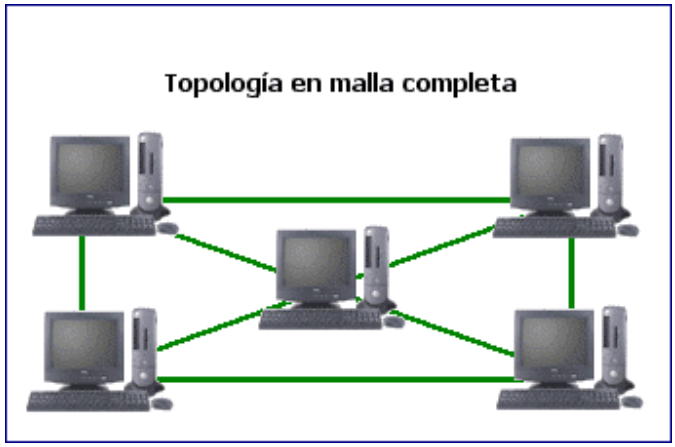
La topología en árbol es similar a la topología en estrella extendida, salvo en que no tiene un nodo central. En cambio, un nodo de enlace troncal, generalmente ocupado por un hub o switch, desde el que se ramifican los demás nodos.



El enlace troncal es un cable con varias capas de ramificaciones, y el flujo de información es jerárquico. Conectado en el otro extremo al enlace troncal generalmente se encuentra un host servidor.

Topología en malla completa

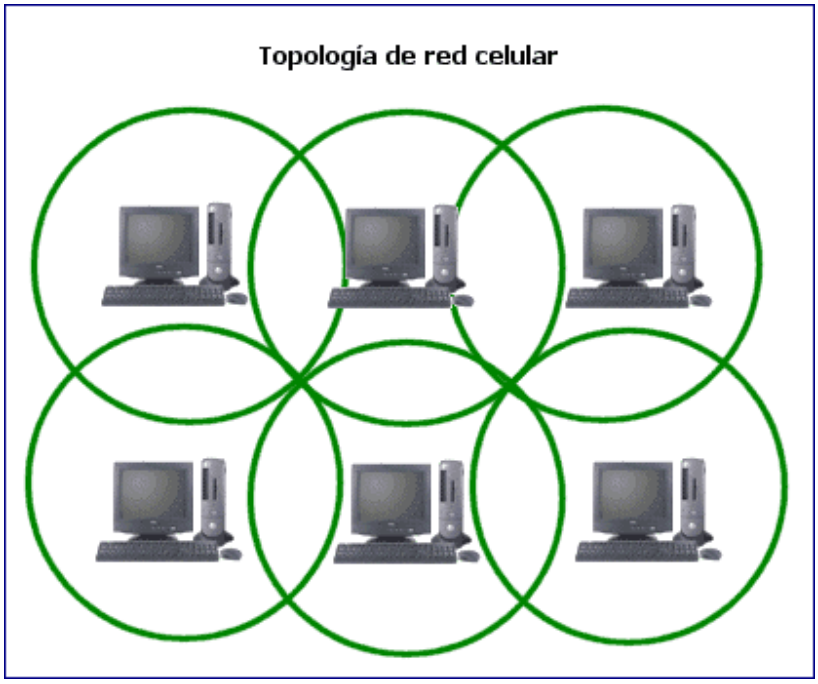
En una topología de malla completa, cada nodo se enlaza directamente con los demás nodos. Las ventajas son que, como cada todo se conecta físicamente a los demás, creando una conexión redundante, si algún enlace deja de funcionar la información puede circular a través de cualquier cantidad de enlaces hasta llegar a destino. Además, esta topología permite que la información circule por varias rutas a través de la red.



La desventaja física principal es que sólo funciona con una pequeña cantidad de nodos, ya que de lo contrario la cantidad de medios necesarios para los enlaces, y la cantidad de conexiones con los enlaces se torna abrumadora.

Topología de red celular

La topología celular está compuesta por áreas circulares o hexagonales, cada una de las cuales tiene un nodo individual en el centro.



La topología celular es un área geográfica dividida en regiones (celdas) para los fines de la tecnología inalámbrica. En esta tecnología no existen enlaces físicos; sólo hay ondas electromagnéticas.

La ventaja obvia de una topología celular (inalámbrica) es que no existe ningún medio tangible aparte de la atmósfera terrestre o el del vacío del espacio exterior (y los satélites). Las desventajas son que las señales se encuentran presentes en cualquier lugar de la celda y, de ese modo, pueden sufrir disturbios y violaciones de seguridad.

Como norma, las topologías basadas en celdas se integran con otras topologías, ya sea que usen la atmósfera o los satélites.

Topología irregular

En este tipo de topología no existe un patrón obvio de enlaces y nodos. El cableado no sigue un modelo determinado; de los nodos salen cantidades variables de cables. Las redes que se encuentran en las primeras etapas de construcción, o se encuentran mal planificadas, a menudo se conectan de esta manera.

Las topologías LAN más comunes son:

- **Ethernet**: topología de bus lógica y en estrella física o en estrella extendida.
- **Token Ring**: topología de anillo lógica y una topología física en estrella.
- **FDDI**: topología de anillo lógica y topología física de anillo doble.

Routers

Routers y comunicación entre redes

Un ordenador solitario, sin conexión con ningún otro, es una isla de información y de recursos que no resulta rentable, especialmente cuando para el trabajo diario se precisa recurrir a diferentes fuentes de datos.

De esto se dieron cuenta muy pronto las empresas, que solicitaron a las compañías de desarrollo de hardware y software un medio compartido de trabajo, en el que diferentes estaciones de trabajo, servidores e impresoras pudieran comunicarse entre ellos y compartir recursos. De este modo surgieron las primeras redes de ordenadores.

Una red está formada por una serie de estaciones de trabajo unidas entre sí por medios de transmisión físicos (cables) o basados en ondas (redes inalámbricas), coordinados por unas máquinas especiales, denominadas servidores, y por una conjunto variable de dispositivos de trabajo, como impresoras, escaners, etc. Además, existen diferentes dispositivos que añaden funcionalidades a las redes, como los routers, switches y hubs.

Pila de protocolos TCP/IP

Las diferentes máquinas que forman una red se comunican entre sí usando un medio compartido, pudiendo tener además cada una de ellas características propias, como componentes de hardware, sistemas operativos y aplicaciones de usuario.

Por solventar estas diferencias se hizo necesaria la introducción de una serie de reglas que controlaran el acceso al medio compartido y la forma correcta en que las máquinas se debían comunicar y transmitir los datos, surgiendo con ello diferentes protocolos de comunicación y control.

En un principio, cada empresa desarrolladora implementó un sistema propio de comunicación de red, con una arquitectura y unos protocolos diferentes, por lo que no fue posible, cuando se necesitó, unir redes de diferentes fabricantes. Simplemente, no se entendían entre ellas, pues hablaban “idiomas” diferentes.

Intentando solucionar este problema, la ISO (Organización Internacional de Estándares) creó un modelo de comunicación para redes dividido en una serie de niveles de trabajo, denominados capas, cada uno de los cuales se encargaría de uno o más aspectos concretos de la comunicación mediante una serie de protocolos específicos.

Este modelo se llamó OSI (Intercomunicación de Sistemas Abiertos) y, lamentablemente, no llegó a utilizarse en la práctica, debido a que cuando se publicó ya se habían desarrollado otros arquitecturas de comunicación en redes que funcionaban más o menos bien, y que fueron las que al final se usaron y extendieron.

De ellas, la más conocida y usada en la actualidad es la arquitectura TCP/IP, formada por un extenso conjunto de protocolos, cada uno de los cuales se encarga de un aspecto concreto de la comunicación entre máquinas en red. TCP/IP se basa en un modelo de capas, al igual que OSI, pero más reducido, actuando cada protocolo en una de las capas del mismo.

El número de capas en que se divide TCP/IP y el nombre de las mismas varía según el autor (recordemos que no es un estándar, si no una implementación “de facto”), pero podemos considerar la siguiente división:

- Capa de Aplicación: encargada de dar soporte de red a las aplicaciones de usuario, convirtiendo los datos de estas a un formato estándar apropiado para su transmisión por red. En ella actúan protocolos como HTTP (web), FTP (transferencia de ficheros) y SMTP (correo electrónico).
- Capa de Transporte: encargada de dividir los datos en unidades de información de tamaño apropiado y de controlar la correcta transmisión lógica de las mismas. Sus principales protocolos son TCP y UDP.

- Capa de Internet: su misión principal es enrutar o dirigir los datos de una máquina a otra, usando para ello el protocolo IP, siendo el responsable principal del tráfico de datos entre diferentes redes interconectadas.A
- Capa de Enlace de datos: se ocupa de identificar los datos transmitidos entre máquinas de una misma red y de controlar la validez de los mismos tras su emisión y recepción a través del medio físico.
- Capa Física: responsable de la conversión de los datos a transmitir en impulsos eléctricos o en ondas y de su transmisión física.
- Cada capa trabaja independientemente de las otras, comunicándose entre ellas por medio de interfaces apropiadas.

Paquetes de datos

Cuando un host desea enviar una serie de datos a otro, estos son convertidos a un formato de red apropiado (capa de Aplicación) y divididos en una serie de unidades, denominadas segmentos (capa de Transporte), que son numerados para su correcto reensamble en la máquina destino.

Posteriormente, son pasados a la capa de Internet, que les coloca las direcciones IP de la máquina origen y de la máquina destino. Las unidades así obtenidas se conocen con el nombre de paquetes. Entonces son pasados a la capa de Enlace de Datos, que les añade las direcciones MAC de ambas máquinas y un número calculado para la verificación posterior de errores en el envío, pasando entonces a denominarse tramas.

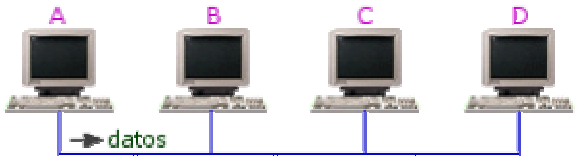
Por último, las tramas son pasadas a la capa Física que las une en trenes de bits apropiados para su transformación en impulsos eléctricos o en ondas, que posteriormente son enviados al medio.

Cuando los impulsos llegan a la máquina destino el proceso se invierte, obteniendo la aplicación receptora los datos en su formato original.

A pesar de que lo que se transmite por el medio físico son impulsos eléctricos, se suele hablar de paquetes transmitidos, ya que son las unidades de información con entidad propia.

Comunicación entre ordenadores en una red

Imaginemos una red formada por varios host, como la representada en la siguiente imagen:



Si el host A (IP=210.23.5.14) se desea comunicar con el host C (IP=210.23.5.27), construye sus paquetes de datos y la capa de Internet les coloca su dirección IP (emisor) y la de C (destinatario), pasándolos a la capa de Enlace de Datos, que no sabe la dirección MAC de C. Para averiguarla, envía un mensaje a todos las máquinas de la red, conocido como petición ARP, preguntando cuál es la dirección MAC correspondiente a la IP 210.23.5.27. Las peticiones ARP son de tipo broadcast, es decir, peticiones que son enviadas a todos y cada uno de los equipos en la red.

La pregunta llega a todas las máquinas, pero sólo C contesta, enviando una respuesta con su dirección MAC. Entonces, A añade ambas direcciones MAC a los paquetes y los pasa a la capa Física, que lo transmite al medio.

Comunicación entre ordenadores en dos redes. Routers.

Imaginemos ahora que el host C (IP=190.200.23.5) no se encuentra en la misma red que A (IP=210.23.5.14). Cuando éste envíe el broadcast preguntando la dirección MAC de C nadie le responderá, por lo que, si no se hace nada al respecto, la comunicación entre ambas máquinas resultará imposible.

Los encargados de solucionar este problema son unos dispositivos de red especiales, llamados routers, que conectan dos o más redes, sirviendo de enlace entre ellas. Los routers trabajan en la capa de Internet, encargándose de encaminar o enrutar paquetes de datos entre máquinas de redes diferentes.

Router Cisco 1601-R

Para poder funcionar de esta forma deben pertenecer a cada una de las redes que conectan, como si fueran un host más de las mismas. De esta forma, un router que conecte dos redes debe tener una tarjeta de red diferente para cada una de las redes y, consecuentemente, dos direcciones MAC diferentes. También debe tener asignada una dirección IP en cada una de las dos redes, ya que si no sería imposible la comunicación con las máquinas de las mismas.

El esquema de dos redes conectadas por un router podría ser el representado en la siguiente imagen:

Ahora, cuando un host envía una petición ARP para averiguar la dirección MAC correspondiente a una IP dada y no es respondido por ningún equipo de su red, envía los paquetes correspondientes a un router que tiene configurado para este tipo de envíos, denominado gateway por defecto.

Una vez que el router recibe los paquetes de datos utiliza un parámetro especial, denominado máscara de red, que sumado lógicamente a la dirección IP destino le da la red a la que pertenece el host buscado. Pasa entonces los paquetes a la red a la que pertenece C, haciendo una nueva petición de broadcast preguntando la MAC de C. Este le responde, y entonces el router le envía los paquetes directamente. Si C desea responder a A, el proceso se invierte.

Este proceso es necesario realizarlo sólo una vez, ya que en esta tanto los host A y C como el router anotan las parejas de direcciones MAC-IP en unas tablas especiales, denominadas tablas de enrutamiento, que usarán en envíos de datos posteriores para enrutar los paquetes directamente.

Resumiendo, los routers son los principales responsables de la correcta comunicación entre máquinas de diferentes redes, encargándose en este proceso de enrutar correctamente los paquetes de datos.

Cómo funciona un router

Los routers son dispositivos de red que raramente se encuentran aislados entre sí. Al contrario, suelen estar interconectados, formando una especie de “telaraña” que hace posible el tráfico de datos entre redes separadas físicamente.

Tomando como ejemplo la Red de redes, Internet, cuando un ordenador envía una serie de paquetes de datos a otro situado en otra ciudad o país, estos son encaminados de router a router a lo largo del camino entre ambas máquinas. Cada paso de un paquete de un router a otro se denomina “salto”, y el principal objetivo de todos y cada uno de los routers que intervienen en la transferencia del paquete es que éste llegue a su destino en el menor número posible de saltos, por la mejor ruta posible.

Para poder realizar esta tarea, los routers se comunican constantemente entre sí, informándose de las rutas bloqueadas, de las máquinas intermedias que se encuentran caídas o saturadas de tráfico, aprendiendo con ello cuál es el router idóneo para enviarle los paquetes recibidos.

Si consideramos ahora el caso de un router segmentando una red local (LAN), aunque ahora no debe enviar los paquetes a otro router, sí que tiene que saber por qué puerto debe enviar los datos para que lleguen a la máquina local destino.

Esta habilidad de “saber” a dónde tienen que enviar los paquetes de datos que reciben la consiguen almacenando en su interior una tabla especial, conocida como tabla de ruteo, en la que van anotando las direcciones IP de las máquinas que se comunican con él y el puerto por el que está accesible esa máquina.

Así, cuando a un router llega un paquete, mira en su tabla de ruteo. Si está en ella referenciada la dirección IP de la máquina destino, también lo estará el puerto por el que ésta es accesible, con lo que envía por él el paquete. En caso de no estar la IP en la tabla, manda una petición de respuesta por todos los puertos, preguntando en cuál de ellos se encuentra la máquina destino, y una vez obtenido el puerto de acceso, ingresa la nueva pareja IP/PUERTO en su tabla de ruteo, con lo que los próximos paquetes para esa máquina los enviará directamente.

Podemos buscar una análogía del funcionamiento de los routers con el de las oficinas de correos. Cuando enviamos una carta desde Mérida (Badajoz) a Linares (Jaén), ésta llega en primer lugar a la oficina local de Mérida, que la reenvía a la de Badajoz, que a su vez la manda a la de Jaén, que la remite a la oficina de Linares, que hace la entrega. Si la oficina de correos de Jaén está cerrada por obras, la de Badajoz la enviará a la de Madrid, que la remitirá a la de Andujar, que a su vez se encargará de mandarla a la de Linares, haciendo ésta de nuevo la entraga. Cierre la oficina que cierre, siempre se encontrará un camino para entregar la carta.

Para evitar mantener en su tabla direcciones IP que hayan quedado obsoletas, cada cierto tiempo borra aquellas que no tienen actividad y las que, tras enviarles paquetes, no han respondido. Esto lo consiguen manteniendo “conversaciones” entre ellos, en unos lenguajes especiales denominados “protocolos de enrutamiento”.

Destino	Métrica	Interface
210.100.12.0	0	eth0
210.100.12.5	0	eth0
192.80.26.13	8	s0
135.0.25.124	5	s1

Tabla de enrutamiento simple

Componentes básicos de un router

Básicamente, podemos considerar un router como un ordenador especial que funciona solo en las tres primeras capas de la arquitectura TCP/IP, al que se la han eliminado una serie de componentes físicos y funcionalidades lógicas que no necesita para su trabajo, mientras que se le han añadido otros componentes de hardware y de software que le ayudan en su trabajo de enrutamiento.

Como todo ordenador, un router necesita un sistema de arranque (bootstrap), encargado de realizar un chequeo del resto de los componentes antes de pasar el control a un sistema operativo (Cisco IOS, en el caso de los routers Cisco).

El sistema de arranque se almacena en una memoria ROM (Read Only Memory=Memoria de Solo Lectura), junto con una parte básica del sistema operativo, la que toma el control inicialmente, mientras que el cuerpo principal de éste se almacena en una memoria especial, de tipo FLASH, que se puede borrar y reprogramar, permitiendo con ello las actualizaciones necesarias. El contenido de la memoria Flash se conserva en caso de cortes de energía o durante los reinicios del router.

Por otra parte, las funcionalidades operativas de los routers son configurables mediante una serie de instrucciones escritas en un fichero de texto, denominado archivo de configuración, que se almacena en un módulo de memoria de tipo NVRAM (No Volatil RAM), cuyo contenido se conserva durante un corte de energía o si se reinicia el equipo.

Una vez inicializado un router, el fichero de configuración es cargado en una memoria RAM (Random Access Memory=Memoria de Acceso Aleatorio), desde la que se va ejecutando el conjunto de órdenes en él contenido. También se almacenan en esta memoria las tablas de enrutamiento, encargadas de almacenar los puertos del router por los que son accesibles las diferentes máquinas.

Por último, el router posee una serie de puertos o interfaces físicas, puntos de conexión del mismo con las diferentes redes a las que está unido, y a través de los cuales se produce la entrada y salida de datos al equipo. El número de interfaces depende del tipo y funcionalidades del router (y de su precio, claro).

Router multipuerto Cisco 2611

Tipos de routers

Los tipos de router a usar en una red varían dependiendo del tipo de ésta, del número de usuarios y de la función o funciones que deba desempeñar, pudiendo variar mucho la complejidad y el precio de ellos en función del tipo elegido.

Si queremos segmentar nuestra red en diferentes subredes, nos hará falta un router de segmentación, con tantos puertos Ethernet como subredes queremos crear (más los de enlace con otros routers), siendo siempre conveniente que nos sobren puertos, con vista a futuras ampliaciones en la red. Cada subred utilizará luego un hub concentrador o un switch para dar acceso a sus clientes individuales.

Podemos desear un ancho de banda dedicado para un número elevado de equipos individuales, prescindiendo así de los hubs. Necesitaremos entonces un routers de concentración, que precisa aún más puertos Ethernet, aunque no suele ser necesario que sean de alta velocidad de transmisión.

Para conectar una red corporativa a Internet necesitaremos un router de frontera, que actuará como gateway de la red interna, recogiendo todos aquellos paquetes de datos destinados a máquinas externas.

En caso de tener que conectar dos redes WAN o dos segmentos de red en sucursales o campus diferentes, necesitaremos un routers de backbone, que proporciona transporte óptimo entre nodos de la red, con interfaces de alta velocidad que proporcionan un elevado ancho de banda. Generalmente estarán basados en tecnología de fibra óptica.

Por último, también es posible al acceso a redes inalámbrico a redes mediante routers con tecnología wireless, un medio práctico de liberar los equipos de las limitaciones de los cables físicos.

Router wireless Barricade 7004AWBR

Protocolos de enrutamiento

Hemos visto antes que los routers mantienen unas tablas de enrutamiento, en las que van anotando las direcciones IP de las máquinas destino y los puertos adecuados para darles salida de forma óptima.

Los routers suelen encontrarse interconectados entre ellos, pasándose los paquetes de datos de uno a otro, hasta llegar a la máquina destino. Como cada router tan solo es responsable de las máquinas directamente conectadas a él (incluyendo los routers vecinos), se hace necesario un mecanismo que permita a los routers comunicarse entre sí, para evitar que cada uno tenga en sus tablas registros inválidos.

Esto se consigue por medio de una serie de protocolos de enrutamiento, responsables de que los diferentes routers mantengan sus tablas de enrutamiento acordes, obteniéndose una red convergente. Con ello se consigue, por ejemplo, que si un ordenador o un servidor se apaga en una red, los routers sepan que ya no está accesible, evitando el envío de datos que no llegarán a su destino, y disminuyendo con ello el tráfico de red.

Para mantener las tablas de enrutamiento actualizadas, un router pueden mandar a los routers vecinos una copia de su tabla cada determinado periodo de tiempo (enrutamientos por vector de distancia) y también cuando alguna máquina en su red sufre algún cambio (enrutamiento por estado de enlace). Depende del protocolo de enrutamiento con que funcione.

Existen diferentes protocolos de comunicación entre routers, cada uno de los cuales utiliza mecanismos propios para conseguir la convergencia en la red y para determinar el mejor camino que puede seguir un paquete de datos en su viaje hasta la máquina destino, y cada uno utiliza un sistema de determinación de mejor ruta (métrica) diferente.

Según su misión en una red podemos diferenciar dos tipos principales de protocolos de enrutamiento: los protocolos de gateway interior (IGP), encargados de la comunicación entre routers de una misma red, entre los que destacan RIP e IGRP, y los protocolos de gateway exterior (EGP) o de frontera, encargados de la comunicación entre routers de redes diferentes.

Entre los más importantes protocolos de enrutamiento podemos destacar los siguientes:

- **RIP** (Protocolo de Información de Enrutamiento), es un protocolo de enrutamiento por vector de distancia que calcula las distancias hacia la máquina destino en función de cuántos routers debe atravesar un paquete para llegar a su destino (saltos), enviando cada paquete de datos por el camino que en cada momento muestre una menor distancia. RIP actualiza las tablas de enrutamiento a intervalos programables, generalmente cada 30 segundos. Es un buen protocolo de enrutamiento, pero necesita que constantemente se conecten los routers vecinos, generándose con ello una gran cantidad de tráfico de red.
- **IGRP** (Protocolo de Enrutamiento de Gateway Interior), desarrollado por Cisco System, es un protocolo de enrutamiento por vector de distancia que usa una métrica compuesta basada en diferentes variables de red, como ancho de banda, unidades máximas de transmisión (MTU), confiabilidad, etc. Envía actualizaciones de las tablas de enrutamiento cada 90 segundos.
- **EIGRP** (Protocolo de Enrutamiento de Gateway Interior Mejorado), protocolo mixto basado en IGRP, basado en una métrica de vector distancia, pero que manda actualizaciones de las entradas de las tablas que han cambiado por haber sido alterado el estado de alguna máquina de su red.
- **OSPF**, protocolo puro de entado de enlace, que calcula las rutas más cortas y accesibles mediante la construcción de un mapa de la red y el mantenimiento unas bases de datos con información sobre su sistema local y sobre los vecinos. Cuando una máquina de su sistema cambia, se envía esa entrada de la tabla a los routers vecinos.

El protocolo de enrutamiento a elegir en cada caso depende del tipo de red (LAN, WAN, etc.), de su topología y del uso de la misma, siendo posible en la mayoría de los casos configurar varios protocolos en un mismo router.

Topología Lógica

Redes LAN Ethernet

Ethernet es la tecnología de red LAN más usada, resultando idóneas para aquellos casos en los que se necesita una red local que deba transportar tráfico esporádico y ocasionalmente pesado a velocidades muy elevadas. Las redes Ethernet se implementan con una topología física

de estrella y lógica de bus, y se caracterizan por su alto rendimiento a velocidades de 10-100 Mbps.

El origen de las redes Ethernet hay que buscarlo en la Universidad de Hawai, donde se desarrollo, en los años setenta, el **Método de Acceso Múltiple con Detección de Portadora y Detección de Colisiones, CSMA/CD** (Carrier Sense and Multiple Access with Collition Detection), utilizado actualmente por Ethernet. Este método surgió ante la necesidad de implementar en las islas Hawai un sistema de comunicaciones basado en la transmisión de datos por radio, que se llamó Aloha, y permite que todos los dispositivos puedan acceder al mismo medio, aunque sólo puede existir un único emisor encada instante. Con ello todos los sistemas pueden actuar como receptores de forma simultánea, pero la información debe ser transmitida por turnos.

Las redes Ethernet son de carácter no determinista, en la que los hosts pueden transmitir datos en cualquier momento. Antes de enviarlos, escuchan el medio de transmisión para determinar si se encuentra en uso. Si lo está, entonces esperan. En caso contrario, los host comienzan a transmitir. En caso de que dos o más host empiecen a transmitir tramas a la vez se producirán encontronazos o choques entre tramas diferentes que quieren pasar por el mismo sitio a la vez. Este fenómeno se denomina **colisión**, y la porción de los medios de red donde se producen colisiones se denomina **dominio de colisiones**.

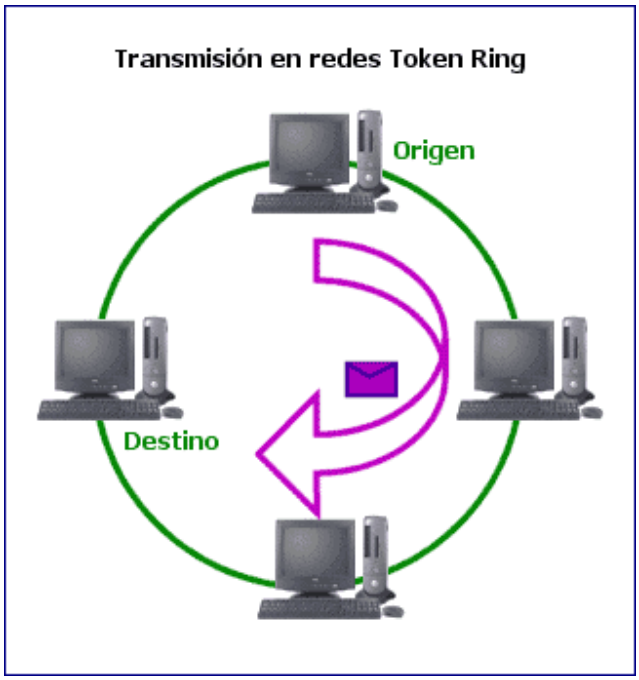
Una colisión se produce pues cuando dos máquinas escuchan para saber si hay tráfico de red, no lo detectan y, acto seguido transmiten de forma simultánea. En este caso, ambas transmisiones se dañan y las estaciones deben volver a transmitir más tarde.

Para intentar solventar esta pérdida de paquetes, las máquinas poseen mecanismos de detección de las colisiones y algoritmos de postergación que determinan el momento en que aquellas que han enviado tramas que han sido destruidas por colisiones pueden volver a transmitirlas.

Redes LAN Token Ring

Las redes Token Ring son redes de tipo determinista, al contrario de las redes Ethernet. En ellas, el acceso al medio está controlado, por lo que solamente puede transmitir datos una máquina por vez, implementándose este control por medio de un token de datos, que define qué máquina puede transmitir en cada instante. Token Ring e IEEE 802.5 son los principales ejemplos de redes de transmisión de tokens.

Las redes de transmisión de tokens se implementan con una topología física de estrella y lógica de anillo, y se basan en el transporte de una pequeña trama, denominada token, cuya posesión otorga el derecho a transmitir datos. Si un nodo que recibe un token no tiene información para enviar, transfiere el token al siguiente nodo. Cada estación puede mantener al token durante un período de tiempo máximo determinado, según la tecnología específica que se haya implementado.



Cuando una máquina recibe un token y tiene información para transmitir, toma el token y le modifica un bit, transformándolo en una secuencia de inicio de trama. A continuación, agrega la información a transmitir a esta trama y la envía al anillo, por el que gira hasta que llega a la estación destino.

Mientras la trama de información gira alrededor del anillo no hay ningún otro token en la red, por lo que ninguna otra máquina puede realizar transmisiones.

Cuando la trama llega a la máquina destino, ésta copia la información contenida en ella para su procesamiento y elimina la trama, con lo que la estación emisora puede verificar si la trama se recibió y se copió en el destino.

Como consecuencia de este método determinista de transmisión, en las redes Token Ring no se producen colisiones, a diferencia de las redes CSMA/CD como Ethernet. Además, en las redes Token Ring se puede calcular el tiempo máximo que transcurrirá antes de que cualquier máquina pueda realizar una transmisión, lo que hace que sean ideales para las aplicaciones en las que cualquier demora deba ser predecible y en las que el funcionamiento sólido de la red sea importante.

La primera red Token Ring fue desarrollada por la empresa IBM en los años setenta, todavía sigue usándose y fue la base para la especificación IEEE 802.5 (método de acceso Token Ring), prácticamente idéntica y absolutamente compatible con ella. Actualmente, el término Token Ring se refiere tanto a la red Token Ring de IBM como a la especificación 802.5 del IEEE.

Las redes Token Ring soportan entre 72 y 260 estaciones a velocidades de 4 a 16 Mbps, se implementan mediante cableado de par trenzado