2.3 Componentes de una red

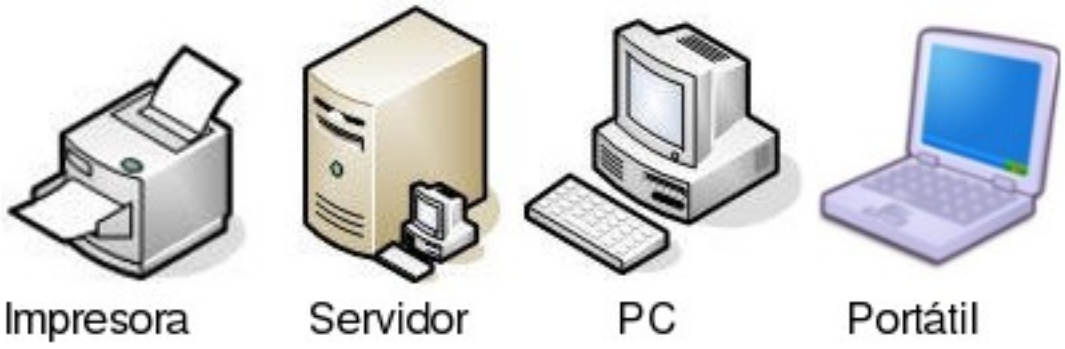
Ahora que tenemos una noción básica sobre el modelo OSI y sobre lo que sucede con los paquetes de datos a medida que recorren las capas del modelo, es hora de que comencemos a echar un vistazo a los dispositivos básicos de redes. A medida que vayamos repasando las capas del modelo de referencia OSI, veremos cuáles son los dispositivos que operan en cada capa según los paquetes de datos vayan viajando a través de ellas desde el origen hacia el destino. Las LAN son redes de datos de alta velocidad y bajo nivel de errores que abarcan un área geográfica relativamente pequeña. Las LAN conectan estaciones de trabajo, dispositivos, terminales y otros dispositivos que se encuentran en un mismo edificio u otras áreas geográficas limitadas.

2.3.1 Nubes

El símbolo de nube indica que existe otra red, por ejemplo Internet. Nos recuerda que existe una manera de conectarse a esa otra red (Internet), pero no suministra todos los detalles de la conexión, ni de la red. Simplemente es útil para realizar los esquemas, si vemos que se conecta a una nube sabemos que esa conexión va a otra red que no es nuestra y que desconocemos, por ejemplo Internet

El propósito de la nube es representar un gran grupo de detalles que no son pertinentes para una situación, o descripción, en un momento determinado. Es importante recordar que solo nos interesa la forma en que las LAN se conectan a las WAN de mayor tamaño, y a Internet (la mayor WAN del mundo), para que cualquier ordenador pueda comunicarse con cualquier otro ordenador, en cualquier lugar y en cualquier momento. Como la nube en realidad no es un dispositivo único, sino un conjunto de dispositivos que operan en todos los niveles del modelo OSI, se clasifica como un dispositivo de las Capas 1-7.

2.3.2 Dispositivos terminales (Capas 1 a 7)



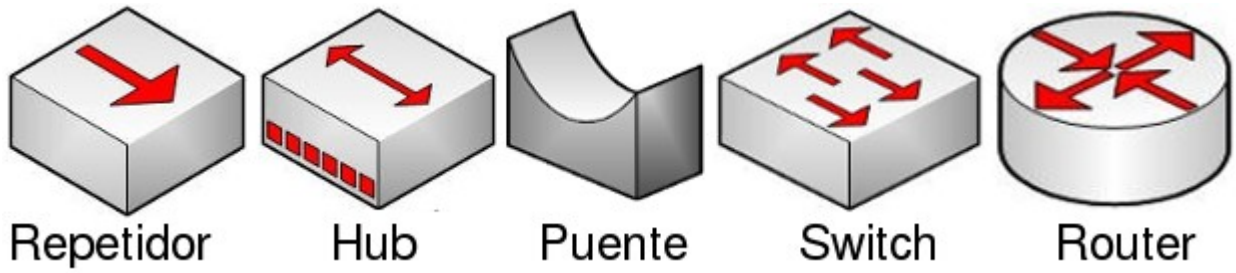
Los dispositivos que se conectan de forma directa a un segmento de red se denominan hosts. Estos hosts incluyen ordenadores, tanto clientes y servidores, impresoras, escáneres y otros dispositivos de usuario. Estos dispositivos suministran a los usuarios conexión a la red, por medio de la cual los usuarios comparten, crean y obtienen información.

Los dispositivos host no forman parte de ninguna capa. Tienen una conexión física con los medios de red ya que tienen una tarjeta de red (NIC) y las demás capas OSI se ejecutan en el software ubicado dentro del host. Esto significa que operan en todas las 7 capas del modelo OSI. Ejecutan todo el proceso de encapsulamiento y desencapsulamiento para

realizar la tarea de enviar mensajes de correo electrónico, imprimir informes, escanear figuras o acceder a las bases de datos.

No existen símbolos estandarizados para los hosts, pero por lo general es bastante fácil detectarlos. Nosotros dibujaremos éstos como si fueran ordenadores:

2.3.3 Dispositivos intermedios (Capas 1, 2 y 3)



Medios (cableado o inalámbrico). Nivel 1

Los símbolos correspondientes a los medios o cableado son distintos según el que realice los esquemas o documentación. Por ejemplo: el símbolo de Ethernet es normalmente una línea recta con líneas perpendiculares que se proyectan desde ella, el símbolo de la red token ring es un círculo con los equipos conectados a él y el símbolo correspondiente a una FDDI (fibra óptica) son dos círculos concéntricos con dispositivos conectados).

Las funciones básicas del cableado, ya sabes, llamado «medios» por ser el medio de conexión, consisten en transportar un flujo de información, en forma de bits y bytes, a través de una LAN. Salvo en el caso de las LAN inalámbricas los medios de red limitan las señales de red a un cable o fibra. Los medios de red se consideran componentes de Capa 1 de las LAN.

Se pueden desarrollar redes informáticas con varios tipos de medios distintos. Cada medio tiene sus ventajas y desventajas. Lo que constituye una ventaja para uno de los medios (costo de la categoría 5) puede ser una desventaja para otro de los medios (costo de la fibra óptica). Algunas de las ventajas y las desventajas son las siguientes:

- Longitud del cable
- Costo
- Facilidad de instalación

El cable coaxial, la fibra óptica o incluso el espacio abierto pueden transportar señales de red, sin embargo, el medio principal que se estudia en esta clase se denomina cable de par trenzado no blindado de categoría 5 (UTP CAT 5) o el categoría 6 (UTP CAT 6).

Repetidores. Nivel 1

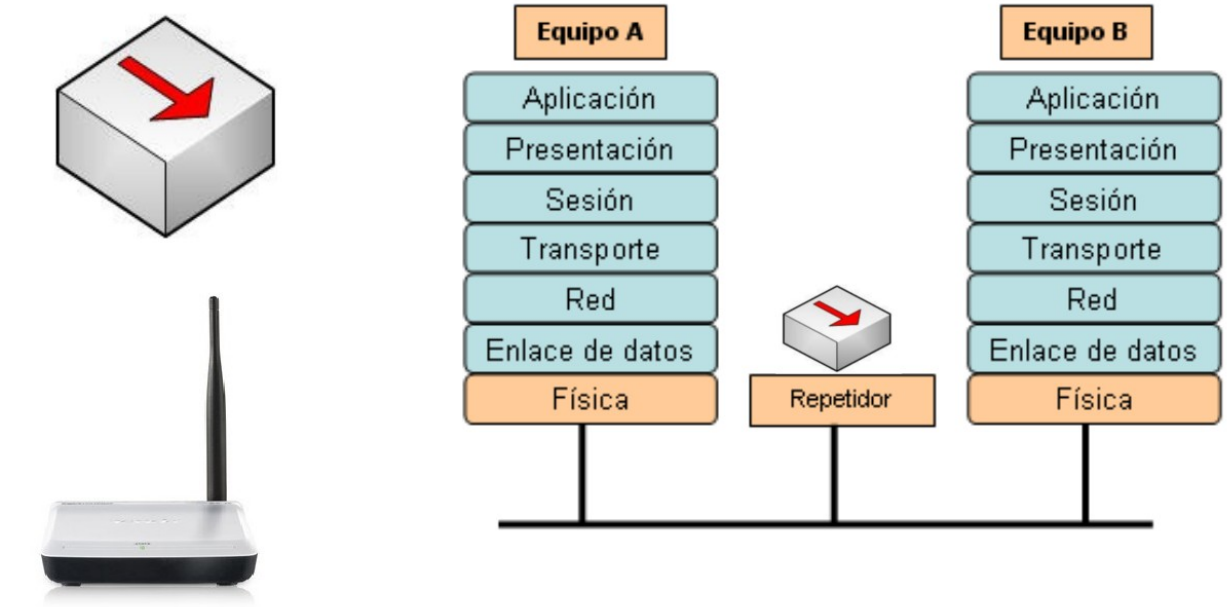
Sabemos pues que según el cableado que utilicemos existen ventajas y desventajas. Por ejemplo una de las desventajas del tipo de cable que utilizamos principalmente (UTP CAT 5) es la longitud del cable. La longitud máxima para el cableado UTP de una red es de 100 metros. Si necesitamos ampliar la red más allá de este límite, debemos añadir un dispositivo a la red llamado repetidor.

El término repetidor se ha utilizado desde la primera época de la comunicación visual, cuando una persona situada en una colina repetía la señal que acababa de recibir de la persona ubicada en la colina de la izquierda, para poder comunicar la señal a la persona que estaba ubicada en la colina de la derecha. También proviene de las comunicaciones telegráficas, telefónicas, por microondas y ópticas, cada una de las cuales usan repetidores para reforzar las señales a

través de grandes distancias, ya que de otro modo en su debido tiempo las señales se desvanecerían gradualmente o se extinguirían.

El propósito de un repetidor es regenerar y retemporizar las señales de red a nivel de los bits para permitir que los bits viajen a mayor distancia a través de los medios. Ten en cuenta la Norma de cuatro repetidores para Ethernet de 10Mbps, también denominada Norma 5-4-3, al extender los segmentos LAN. Esta norma establece que se pueden conectar cinco segmentos de red de extremo a extremo utilizando cuatro repetidores pero sólo tres segmentos pueden tener ordenadores en ellos, curioso ¿no?.

El término repetidor se refiere tradicionalmente a un dispositivo con un solo puerto de «entrada» y un solo puerto de «salida». Sin embargo, en la terminología que se utiliza en la actualidad, el término repetidor multipuerto se utiliza también con frecuencia. En el modelo OSI, los repetidores se clasifican como dispositivos de Capa 1, dado que actúan sólo a nivel de los bits y no tienen en cuenta ningún otro tipo de información. El símbolo para los repetidores no está estandarizado, así que nosotros utilizaremos este:



Repetidor (nivel 1)

Concentradores o hubs. Nivel 1

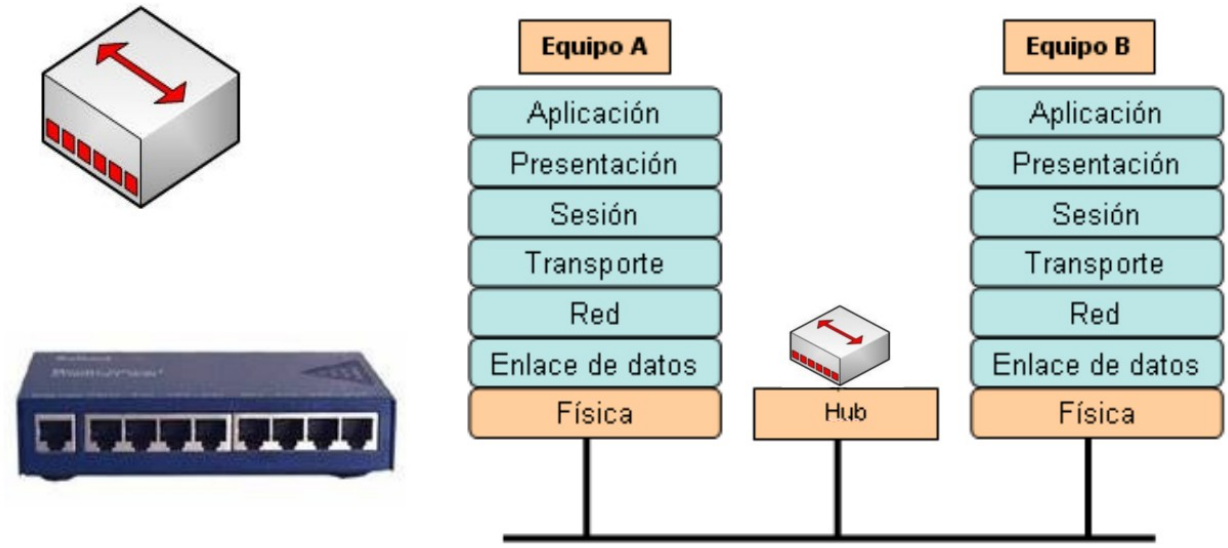
El propósito de un hub es regenerar y retemporizar las señales de red. Esto se realiza a nivel de los bits para un gran número de equipos (por ej., 4, 8 o incluso 24) utilizando un proceso denominado concentración. Como ves es prácticamente la misma definición que la del repetidor, pues si, a los hub también se les llama **repetidor multipuerto**. La diferencia es la cantidad de cables que se conectan al dispositivo, que en este caso admiten varios ordenadores conectados en este hub.

Los hubs se utilizan por dos razones: para crear un punto de conexión central para los ordenadores y para aumentar la fiabilidad de la red. La fiabilidad de la red se ve aumentada al permitir que cualquier cable falle sin provocar una interrupción en toda la red. Esta es la diferencia con la topología de bus, en la que, si un cable fallaba, se interrumpía el funcionamiento de toda la red. Los hubs se consideran dispositivos de Capa 1 dado que sólo regeneran la señal y la envían por medio de un broadcast (ya lo veremos pero consiste en que mandan la información a todos los demás equipos) a todos los puertos.

Hay una pequeña clasificación de los hubs que son los inteligentes y no inteligentes. Los hubs inteligentes tienen puertos de consola, lo que significa que se pueden programar para administrar el tráfico de red. Los hubs no inteligentes

simplemente toman una señal de red de entrada entrante y la repiten hacia cada uno de los puertos sin la capacidad de realizar ninguna administración.

El símbolo correspondiente al hub no está estandarizado pero utilizaremos este.



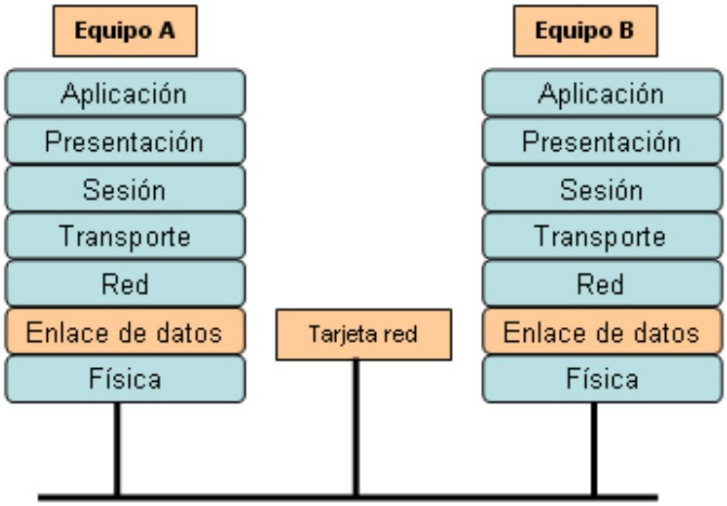
Hub o concentrador (nivel 1)

Tarjeta de red o NIC. Nivel 2

Hasta este momento, en este capítulo nos hemos referido a dispositivos y conceptos de la capa uno. A partir de la tarjeta de interfaz de red, nos trasladamos a la capa dos: la capa de enlace de datos del modelo OSI. En términos de aspecto, una tarjeta de interfaz de red (tarjeta NIC o NIC) es un pequeño circuito impreso que se coloca en un slot de expansión de un bus de la (placa madre) del ordenador, aunque ahora ya casi todos los ordenadores la incorporan de fábrica y no hay que añadirla. También se denomina adaptador de red.

Las NIC se consideran dispositivos de Capa 2, cada tarjeta de red (NIC) lleva un nombre codificado único, denominado dirección de Control de acceso al medio (MAC o MAC Address) y es único en el mundo. Si, como lo lees, cada fabricante tiene asignada una numeración y a cada tarjeta de red le pone esa dirección física única, es como su DNI y nunca pueden existir dos tarjetas de red con ese mismo número interno. Esta dirección es muy importante ya que identifica perfectamente y de forma única al ordenador origen y al destino.

Las tarjetas de red no tienen ningún símbolo estandarizado. Se da a entender que siempre que haya dispositivos de red conectado a la de red, existe alguna clase de NIC o un dispositivo similar aunque por lo general no aparezcan. Siempre que haya un punto en una topología, significa que hay una NIC o una interfaz (puerto), que actúa por lo menos como parte de una NIC.



Tarjeta de red (nivel 2)

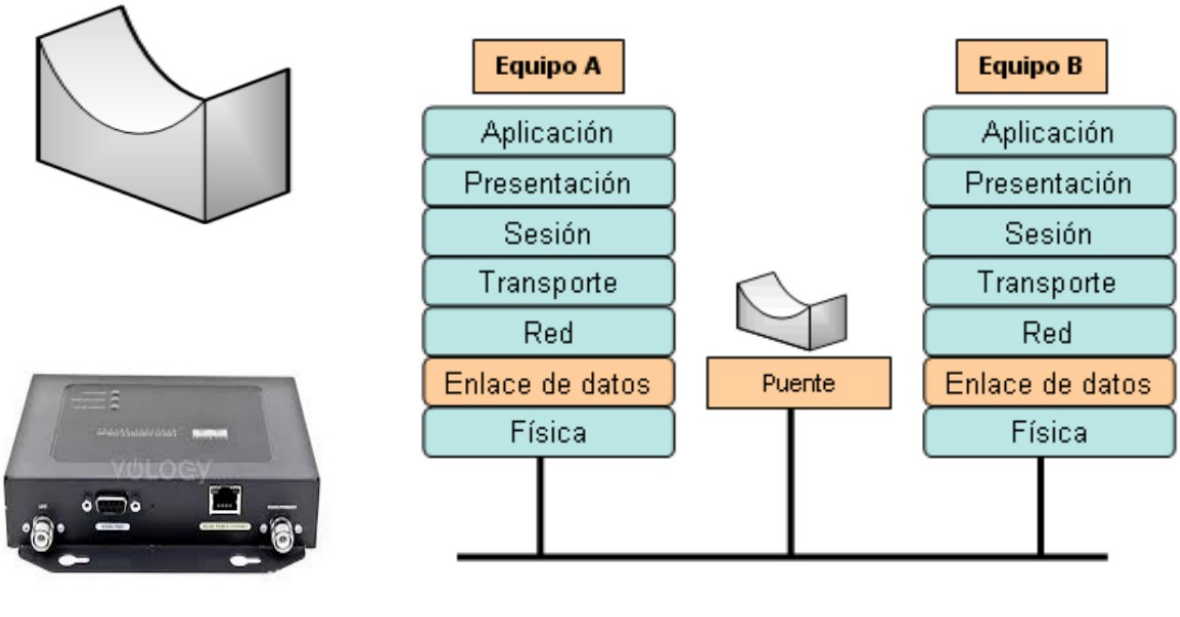
Puentes. Nivel 2

Un puente es un dispositivo de capa 2 diseñado para conectar dos segmentos LAN. El propósito de un puente es filtrar el tráfico de una LAN, para que el tráfico local siga siendo local, pero permitiendo la conectividad a otras partes (segmentos) de la LAN para enviar el tráfico dirigido a esas otras partes.

¿Pero que es un segmento? Es una definición muy variable, nosotros vamos a considerarlo como dos partes distintas de la red. Por ejemplo la red del piso 1 y la red del piso 2 que están conectadas. También podemos ampliarlo, por ejemplo una pequeña empresa que tiene dos oficinas en dos edificios y están conectadas entre si, podemos llamar también a cada una de esas partes segmento.

Vale pero ¿cómo puede detectar el puente cuál es el tráfico de un segmento y cuál no lo es? La respuesta es la misma que podría dar el servicio de correos cuando se le pregunta cómo sabe cuál es el correo local: verifica la dirección local. Cada dispositivo de networking tiene una dirección MAC exclusiva en la tarjeta de red, el puente rastrea cuáles son las direcciones MAC que están ubicadas a cada lado del puente y toma sus decisiones basándose en esta lista de direcciones MAC.

Si el tráfico está entre dos ordenadores del piso 1 el puente decide que no debe mandar ese tráfico al piso 2 porque sabe por las direcciones MAC que el destino está en el mismo piso. Lo mismo para el caso de los dos edificios: el puente conecta los dos segmentos, cuando un ordenador pide información a otro el puente sabe que equipo están conectados en cada lado y sabe si debe mandar el tráfico al otro lado. Tradicionalmente, el término puente se refiere a un dispositivo con dos puertos.



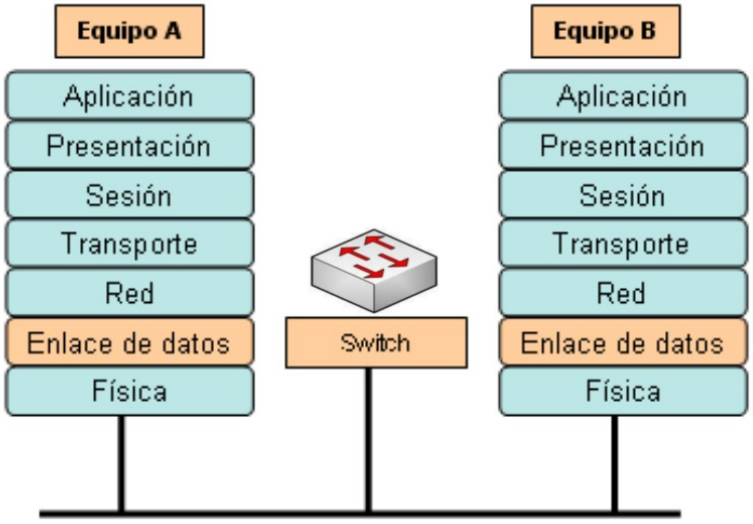
Puente (nivel 2)

Conmutadores o switches. Nivel 2

Un switch, al igual que un puente, es un dispositivo de capa 2. De hecho, el switch se denomina **puente multipuerto**, igual que antes cuando llamábamos al hub «repetidor multipuerto». La diferencia entre el hub y el switch es que los switches toman decisiones basándose en las direcciones MAC y los hubs no toman ninguna decisión. Como los switches son capaces de tomar decisiones, hacen que la LAN sea mucho más eficiente. Los switches hacen esto enviando los datos sólo hacia el puerto al que está conectado el host destino apropiado. Por el contrario, el hub envía datos desde todos los puertos, de modo que todos los hosts deban ver y procesar (aceptar o rechazar) todos los datos.

Como son mucho mejores y eficiente ten en cuenta siempre poner switches en tu red y no hubs, primera recomendación importante. Segunda recomendación: seguramente te parecerá una tontería y obviedad que te diga que si un coche es de buena marca es mejor que uno de marca mala: evidente. Pues aquí pasa lo mismo: hay marcas buenas y marcas malas y la diferencia va a estar evidentemente en las prestaciones y en las posibilidades de configuración. Así que segunda recomendación: invierte un poco de dinero en comprarlo de marca buena: son equipos para toda la vida y considéralo una inversión y no un gasto.

En el gráfico se indica el símbolo que corresponde al switch. Las flechas de la parte superior representan las rutas individuales que pueden tomar los datos en un switch, a diferencia del hub, donde los datos fluyen por todas las rutas



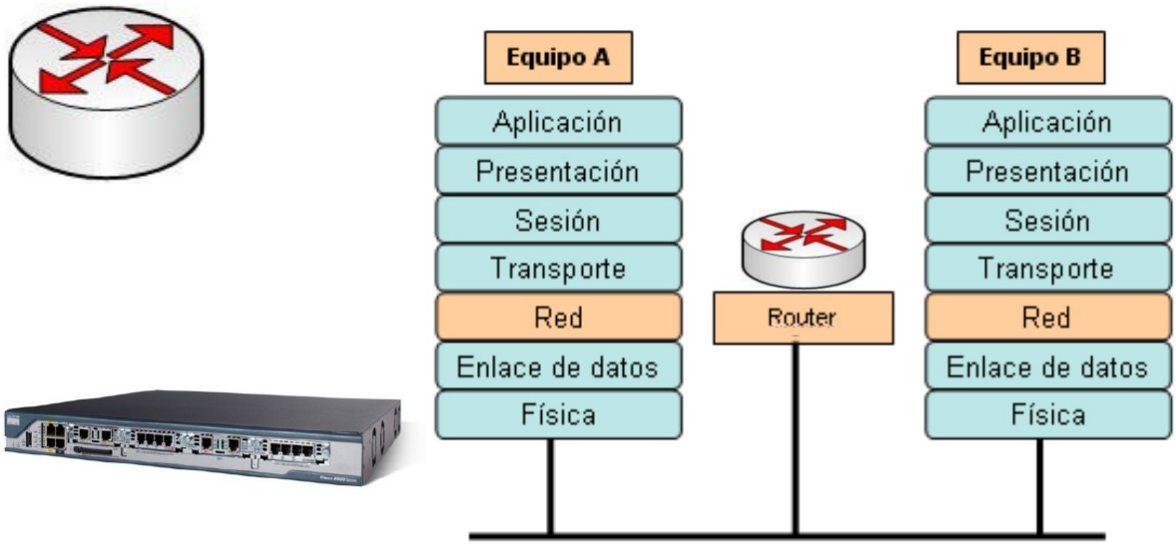
Conmutador o switch (nivel 2)

Encaminadores o routers. Nivel 3

El router es el primer dispositivo con que trabajaremos que pertenece a la capa de red del modelo OSI, o sea la Capa 3. Al trabajar en la Capa 3 el router puede tomar decisiones basadas en grupos de direcciones de red (la famosas direcciones IP) en contraposición con las direcciones MAC de Capa 2 individuales. Los routers también pueden conectar distintas tecnologías de Capa 2, como por ejemplo Ethernet, Token-ring y FDDI (fibra óptica). Sin embargo, dada su aptitud para enrutar paquetes basándose en la información de Capa 3, los routers se han transformado en el núcleo de Internet, ejecutando el protocolo IP.

El propósito de un router es examinar los paquetes entrantes (datos de capa 3), elegir cuál es la mejor ruta para ellos a través de la red y luego enviarlos hacia el puerto de salida adecuado. Los routers son los dispositivos de regulación de tráfico más importantes en las redes grandes. Permiten que prácticamente cualquier tipo de ordenador se pueda comunicar con otro en cualquier parte del mundo.

El símbolo correspondiente al router (observa las flechas que apuntan hacia adentro y hacia fuera) sugiere cuáles son sus dos propósitos principales: la selección de ruta y la transmisión de paquetes hacia la mejor ruta.



Encaminador o router (nivel 3)

2.4 Uso del medio en redes

La interconexión de los distintos nodos que forman una red puede realizarse de dos formas: **por conmutación o por difusión**.

2.4.1 Conmutación

Consisten en un conjunto de nodos interconectados entre sí, a través de medios de transmisión (cables), formando la mayoría de las veces una topología mallada o estrella, donde la información se transfiere encaminándola del nodo de origen al nodo destino mediante conmutación entre nodos intermedios.

Es típica de las WAN. Existe una línea dedicada para cada dos nodos. La conmutación a su vez puede ser de circuitos o de paquetes.

Conmutación de circuitos

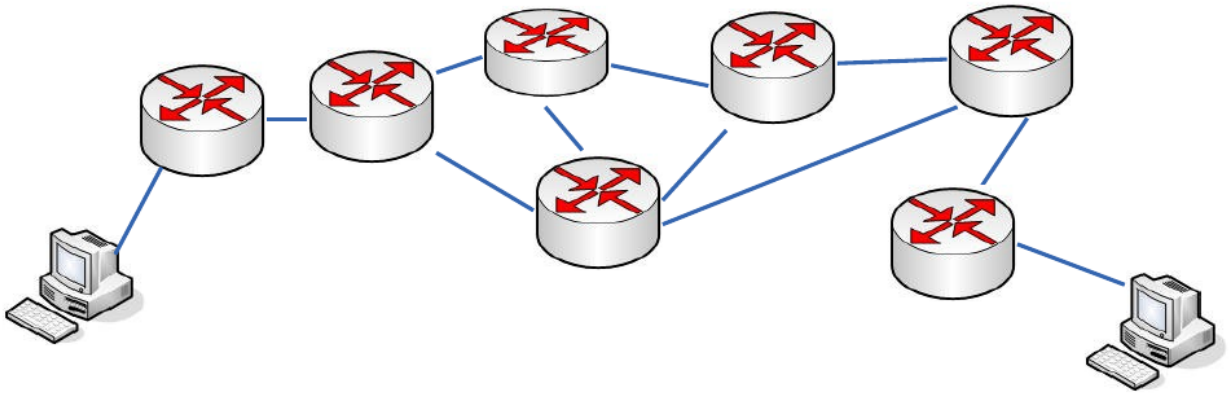
Se establece un único camino entre el origen y el destino para toda la comunicación.

Cuando un emisor quiere enviar un mensaje a un receptor a través de una red de conmutación de circuitos, lo primero que debe hacerse es el **establecimiento** del canal, es decir la conexión entre emisor y receptor, que se hace eligiendo un camino concreto de entre todos los posibles que existen. La ruta que sigue la información se establece al inicio de la comunicación y **se mantiene durante todo el proceso que dure la comunicación**, aunque existan algunos tramos de esa ruta que se comparten con otras rutas diferentes. Al finalizar la transmisión se produce la **liberación** del canal. La **red telefónica clásica** es un ejemplo de conmutación de circuitos.

Conmutación de paquetes

Se trata del procedimiento mediante el cual, cuando un nodo quiere enviar un mensaje a otro, lo divide en paquetes. Cada paquete es enviado por el medio con información de cabecera. En cada nodo intermedio por el que pasa el paquete se detiene el tiempo necesario para procesarlo y decidir el siguiente nodo al cual enviarlo. Así sucesivamente hasta el destino. Los paquetes pueden perderse o llegar en distinto orden.

Los distintos paquetes de un mismo mensaje pueden seguir caminos distintos hasta su destino. **Internet** es un ejemplo de conmutación de paquetes.

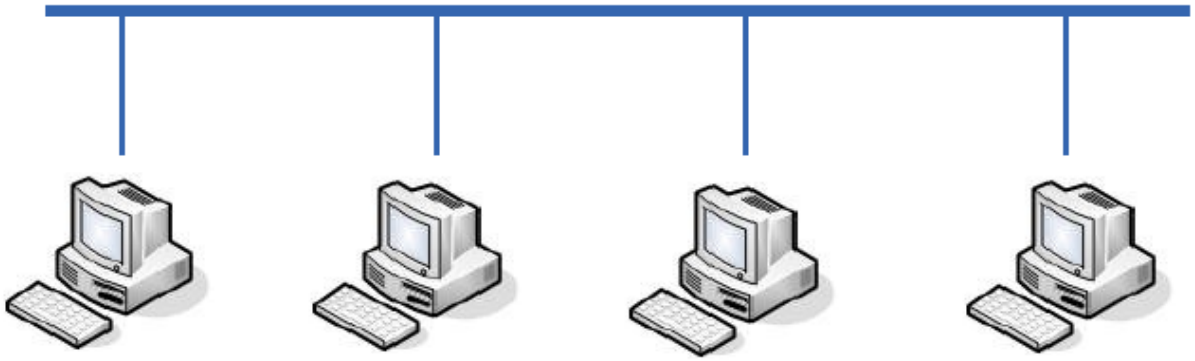


Ejemplo de red conmutada, cuyos equipos finales son ordenadores personales y los equipos intermedios son routers.

2.4.2 Difusión

En medio compartido el emisor envía a todos los nodos la información. El nodo receptor sabe que es para él y la recoge. Los otros nodos la dejan pasar. Las topologías que utilizan este tipo de redes son: bus, anillo y las basadas en ondas de radio.

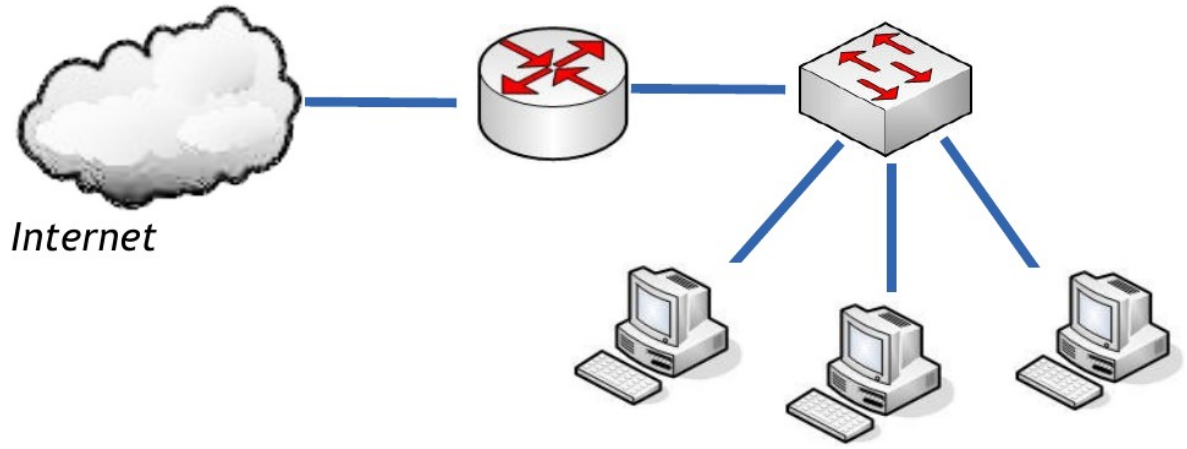
En este tipo de redes no existen nodos intermedios de conmutación. Todos los nodos comparten un medio de transmisión común, por el que la información transmitida por un nodo es conocida por todos los demás. En definitiva, es el destinatario el encargado de seleccionar y captar la información. Este uso del medio es propio de algunas **intranets** y de comunicaciones inalámbricas omnidireccionales.



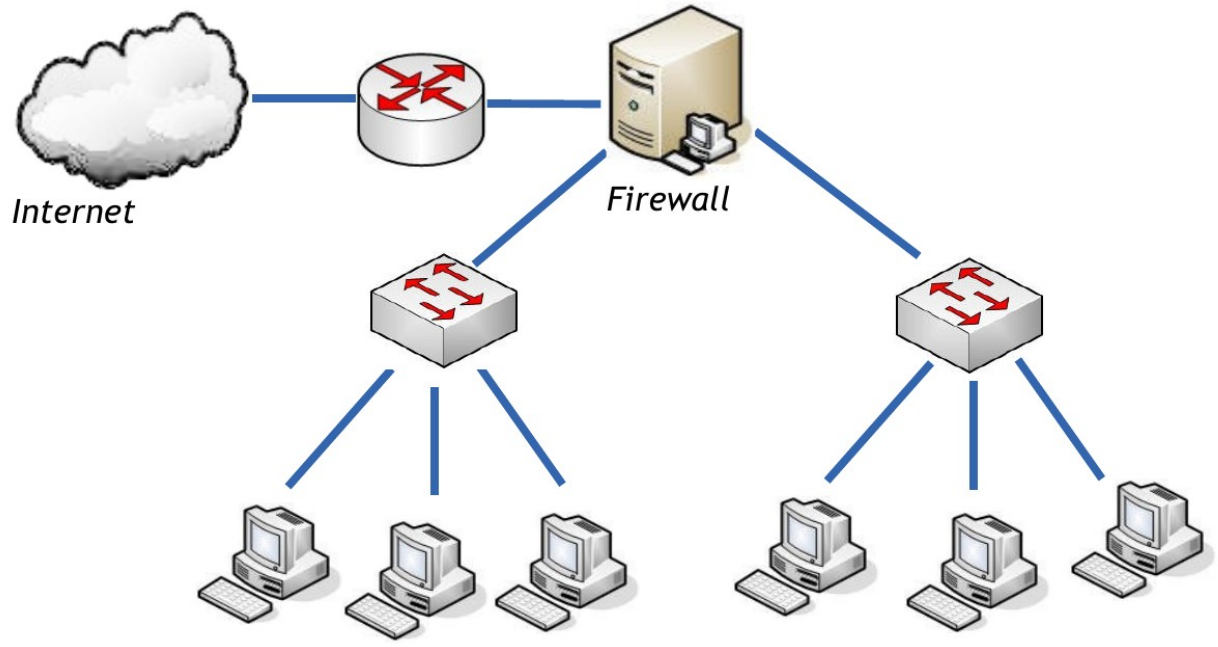
Ejemplo de red de difusión, cuyos equipos finales son ordenadores personales, el medio es un bus compartido y no existen nodos de conmutación.

2.5 Esquemas LAN

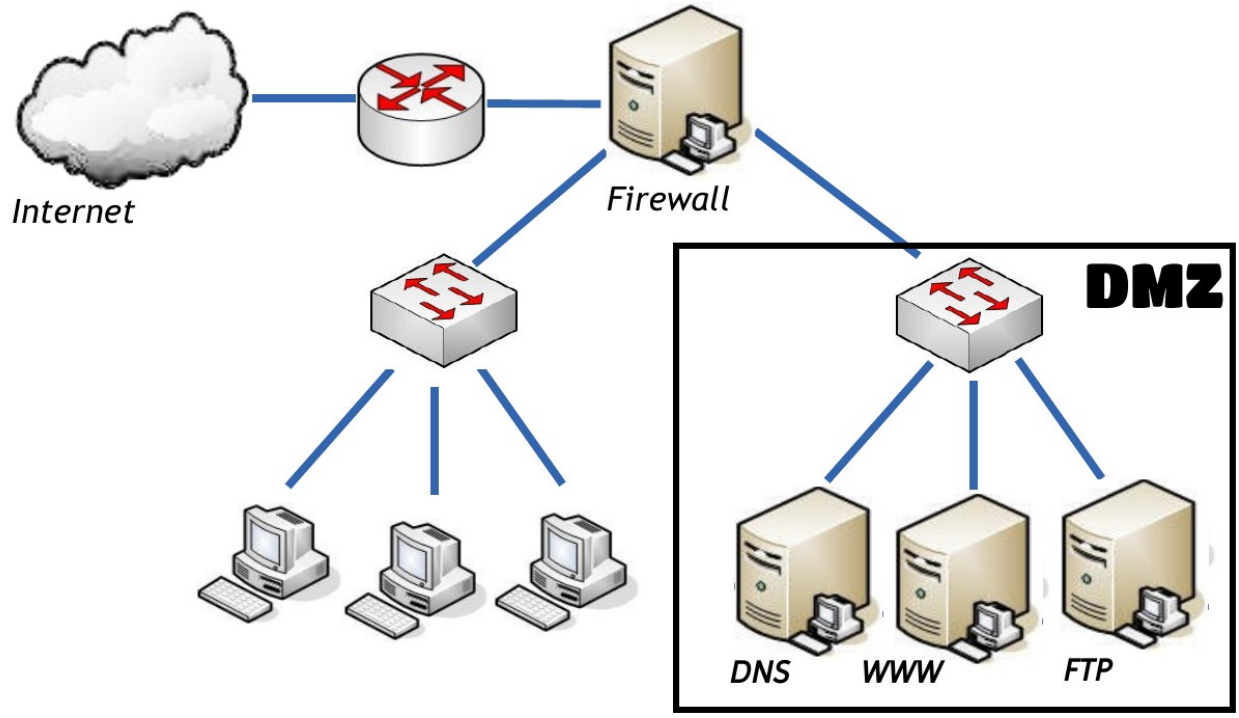
2.5.1 Red local simple



2.5.2 Red local organizada en 2 zonas



2.5.3 Red local con zona de usuarios y Zona DesMilitarizada



Una **DMZ** (del inglés Demilitarized zone) o **Zona DesMilitarizada**. En seguridad informática, una zona desmilitarizada (DMZ) o **red perimetral** es una red local (una subred) que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa – los equipos (hosts) en la DMZ no pueden conectar con la red interna. Esto permite que los equipos (hosts) de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.

La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de e-mail, Web y DNS.

Las conexiones que se realizan desde la red externa hacia la DMZ se controlan generalmente utilizando port address translation (PAT).

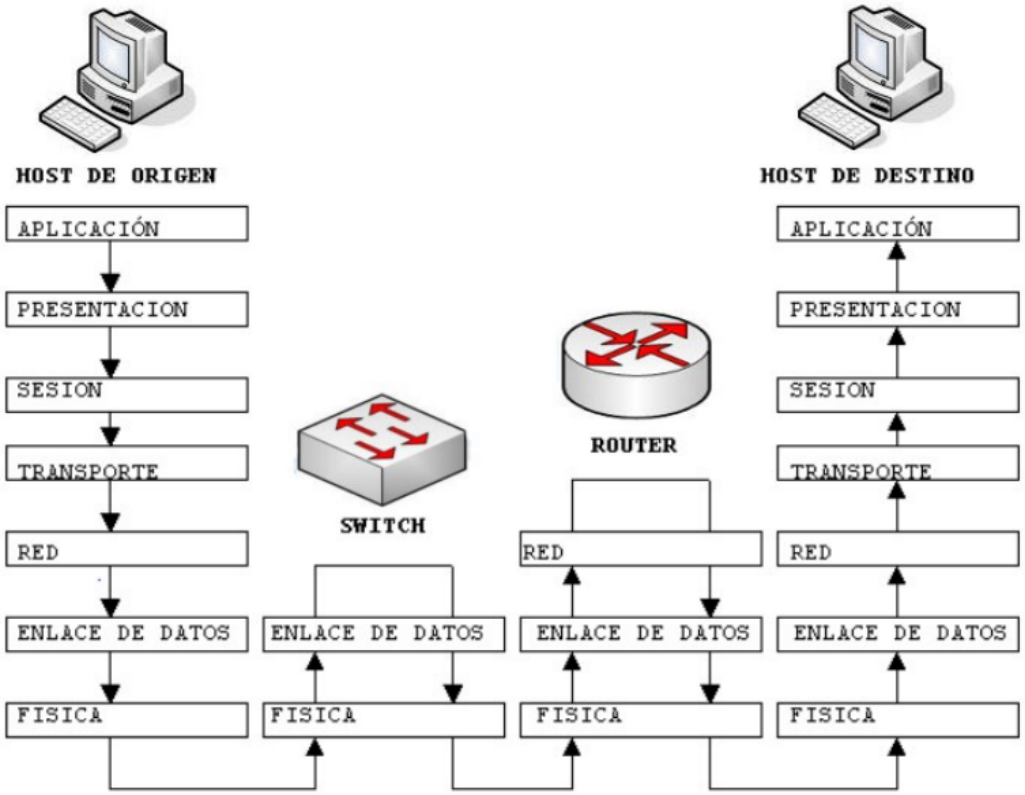
2.6 Referencias

- Planificación y Administración de Redes. Editorial Ra-ma.
- Redes Locales. Editorial Macmillan.

2.7 Actividades

1. Busca información acerca de las normas IEEE 802.3 y 802.11. Haz un breve resumen.
2. Busca información acerca de las normas TIA 568A y TIA 568B. Haz un breve resumen.

3. ¿En qué RFCs se hallan especificados los protocolos TCP e IP?. ¿Qué organismo los pública? ¿Se pueden obtener de forma gratuita?
4. Define protocolo. Nombra 3 protocolos de la capa de aplicación de TCP/IP.
5. Explica los siguientes términos:
   - Direccionamiento
   - Encaminamiento
   - Control de errores
   - Acceso al medio
   - Multiplexación
6. Realiza un esquema comparativo de las capas OSI y TCP/IP.
7. ¿Qué es una PDU? ¿Cómo se denominan en la arquitectura TCP/IP?
8. ¿Qué se entiende por encapsulación de los datos? ¿Y desencapsulación? ¿Cuál se produce cuando bajamos por la pila de protocolos y cuál cuando subimos?
9. Arquitecturas obsoletas. Haz un esquema de la arquitectura SNA. ¿Qué empresa la desarrolló?
10. Arquitecturas obsoletas. Haz un esquema de la arquitectura DECnet. ¿Qué empresa la desarrolló?
11. Arquitecturas obsoletas. Haz un esquema de la arquitectura SPX/IPX. ¿Qué empresa la desarrolló?
12. Arquitecturas obsoletas. Haz un esquema de la arquitectura X.25. ¿Qué organismo la desarrolló?
13. ¿Cómo se interpreta la siguiente imagen?



14. ¿Qué dispositivos trabajan en la capa 1 o física?
15. ¿Qué dispositivos trabajan en la capa 2 o de enlace?
16. ¿Qué dispositivos trabajan en la capa 3 o de red?
17. ¿En qué capa trabajo un host final?
18. ¿Qué diferencia existe entre la conmutación de circuitos y la conmutación de paquetes? Pon un ejemplo de cada una.
19. Nombra los dispositivos por los que pasa la información que un usuario envía desde una red local hacia Internet.
20. ¿Qué es una DMZ? ¿Cuál es su utilidad?