

TEMA 6 (11 del libro) Interconexión de redes de área local

Objetivos

- Conocer los distintos equipos que se emplean para la interconexión de redes, sus características y ámbito principal de utilización
- Introducir la familia de protocolos TCP/IP, ampliamente utilizada en Internet, la estructura de los datagramas IP y el funcionamiento del protocolo
- Presentar dos de los servicios utilizados para la interconexión de redes de área local, mediante Frame relay, y multimedia, haciendo uso del protocolo ATM

1 Necesidad de la interconexión

Inicialmente las redes son independientes, pero si se quieren intercambiar archivos con otras redes, necesitan conectarse.

La forma más extendida para interconectar redes es el uso de dispositivos.

Las funciones principales de éstos son:

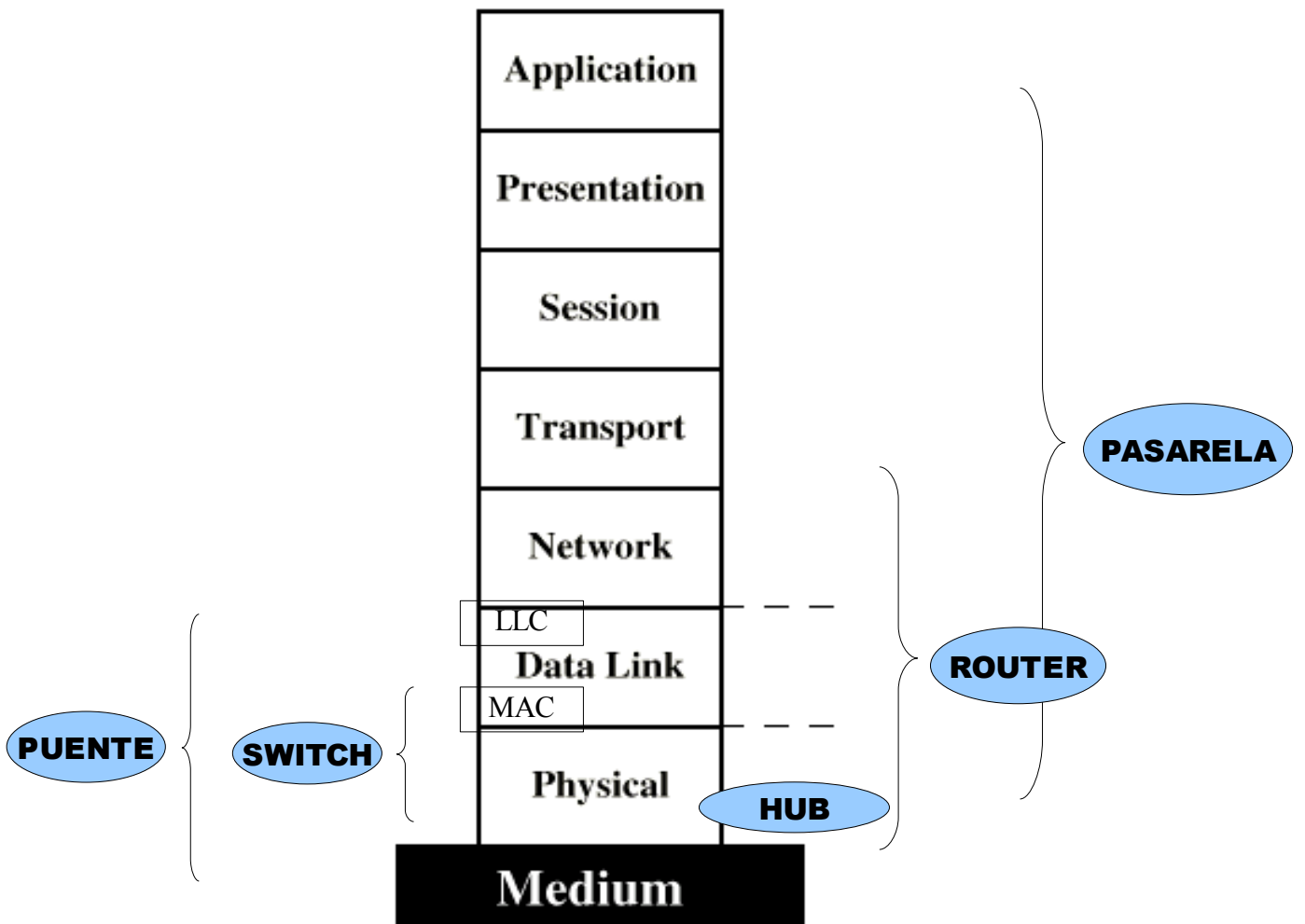
- establecer un camino físico entre redes para el intercambio de mensajes
- adaptación o conversión de protocolos de acceso a las redes
- enrutamiento de mensajes entre redes

2 Dispositivos para la interconexión de redes

- Repetidores (repeaters) y hubs
- Conmutadores (switches)
- Puentes (bridges)
- Encaminadores (routers)
- Pasarelas (gateways)

Niveles (OSI) de operatividad:

OSI Reference Model



3 Repetidores

Los repetidores se limitan a regenerar la señal, sin cambiar su contenido, para ampliar el rango de distancia que se alcanza. Según los estándares de cableado estructurado, en una red Ethernet no se pueden usar más de cuatro repetidores entre dos ordenadores (con una distancia máxima de cable par trenzado de 100 metros)

Trabajan en el nivel físico de OSI.

Los hubs son unos repetidores multipuerto, que se usan para conectar varios ordenadores.

Para asegurarse de que el mensaje llega al destino, reenvían la señal recibida por todos sus puertos, no hacen ningún tipo de filtro o lectura de la información, simplemente reenvían.

<http://reparesupc.com/redes.aspx> (diapositivas 1 y 2)

Colisión

Al reenviar por todos sus puertos, es posible que dos tramas colisionen. Cuando se produce una colisión, los paquetes de datos involucrados se destruyen bit a bit.

Las colisiones son perjudiciales porque disminuyen el rendimiento de la red. Muchos protocolos cuando encuentran un error en la transmisión piden la retransmisión, por lo que la velocidad en una red con muchas colisiones es más lenta de lo que podría ser.

Dominio de colisión: es el área dentro de la red donde los paquetes se originan y colisionan e incluye todos los medios compartidos. Todas las conexiones de nivel 1 forman parte del dominio de colisión.

Por ejemplo, si los ordenadores de una clase estuvieran conectados por un hub, y con los demás ordenadores con un switch, el dominio de colisión sería la propia clase. Si en cambio, dos clases estuvieran conectadas por hubs y con el resto de los ordenadores mediante un switch, el dominio de colisión serían las dos clases.

Por la forma de operar del hub (no hace ningún tipo de filtro), todos los elementos conectados por un hub forman parte del mismo dominio de colisión. El hub extiende el dominio de colisión

<http://reparesupc.com/redes.aspx> (diapositiva 3)

Cuestiones

- Haz un esquema del funcionamiento del hub
- ¿Qué es un dominio de colisión?
- ¿Qué ocurre cuando se produce una colisión?
- ¿Cuál es el dominio de colisión si se usa un hub? Explica por qué

4 Conmutadores ó switches

El switch es un dispositivo que opera en el subnivel MAC del nivel de enlace.

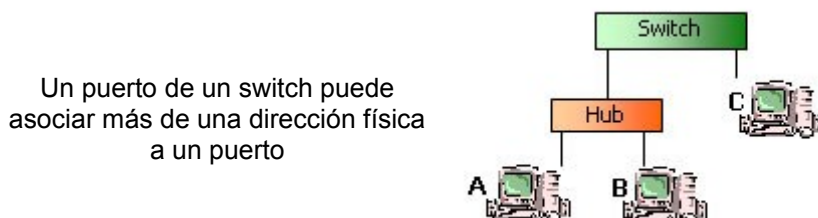
El switch accede a la trama MAC y redirecciona sólo a la estación destinataria

Funcionamiento

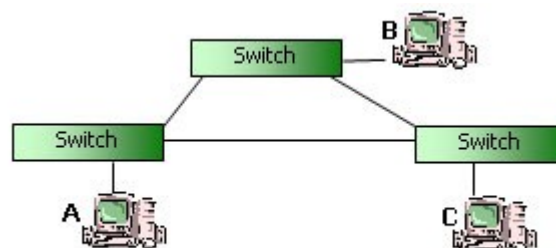
El switch dispone de una tabla que asocia direcciones físicas a puertos de comunicación. Así, cuando le llega una trama, sabe por qué puerto debe enviarla.

Cuando el switch recibe una trama de una estación a través de un puerto, si no tiene la dirección MAC de esa trama en su tabla, introduce en la tabla la dirección MAC de dicha estación, y la asocia al puerto al que está conectada.

Cuando un switch tiene que reexpedir una trama, primero consulta su tabla para conocer el puerto de salida asociado a la MAC destino. Si no tiene asociada esa MAC ningún puerto, envía la trama por todos sus puertos (técnica de inundación o flooding).



Si un nodo puede tener varias rutas alternativas para llegar a otro un switch, tiene problemas para aprender su dirección, ya que aparecerá en dos de sus entradas. A esto se le llama bucle (loop) y suele haber una lucecita destinada a eso delante de los switch. El protocolo de Spanning Tree Protocol IEEE 802.1d se encarga de solucionar este problema, aunque los switch domésticos no suelen tenerlo. Por eso se prefiere tener una estructura estrellada o arbolado



Mecanismo de reexpedición

En función del mecanismo de reexpedición empleado, se distinguen dos tipos de switches:

- **Almacenamiento y reexpedición (store-and-forward)**

Un switch de este tipo realiza una copia completa de cada trama que recibe y comprueba el código de redundancia (CRC), si la trama contiene errores es descartada, si no, se reenvía.

Este proceso de almacenamiento y chequeo de la trama puede introducir retardos

significativos en la red.

- **Truncamiento (cut-through)**

Sólo copia los primeros bytes para conocer la dirección de destino. Una vez conocida, el resto de la trama se envía directamente hacia la salida adecuada.

Estos switches no hacen comprobación de errores, pero los retardos son menores.

Velocidad de trabajo

Los switches se usan mucho en redes Ethernet, que pueden tener velocidades de 10, 100 y 1000 Mb/s. Según puedan mezclar distintas velocidades ó no, se distinguen dos tipos:

- **Switches simétricos**

En este tipo de switches todos los puertos trabajan a la misma velocidad, ya sea 10, 100 ó 1000 Mb/s, y por tanto no es posible mezclar redes Ethernet, Fast Ethernet ó Gigabit Ethernet.

- **Switches asimétricos**

Este tipo de switches pueden mezclar redes de velocidades distintas. Se requiere búfering de memoria en un switch asimétrico para permitir que el tráfico del puerto de mayor velocidad pueda enviarse al puerto de menor velocidad, sin provocar demasiada congestión en éste último.

Segmentación

Una red se puede dividir en unidades pequeñas denominadas **segmentos**. Cada segmento usa el protocolo CSMA/CD y mantiene el tráfico entre los usuarios en el segmento. Al usar segmentos en una red, hay menos usuarios ó dispositivos que comparten el mismo medio físico y por tanto el mismo dominio de colisión.

Usando switches se puede segmentar una red al reducir el tráfico en la red filtrando la información en función de la dirección física de la estación destinataria, reexpidiendo los datos hacia la salida adecuada.

Así se tiene una red que se comporta como si tuviera sólo dos nodos: el emisor y el receptor. El ancho de banda de la red se comparte sólo entre ellos dos, a diferencia de las redes conectadas por hubs en las que el medio está compartido por todos los equipos.

Cuestiones

- Identifica en la primera figura los distintos dominios de colisión. Explica con tus palabras qué es un dominio de colisión, usa esta dirección <http://inet.webcindario.com/capasOSI.htm>
- Visita la dirección <http://reparesupc.com/redes.aspx> y observa las diapositivas de la cuatro a la ocho.
- Usando estos apuntes y el libro de texto, explica por qué es importante segmentar una red.

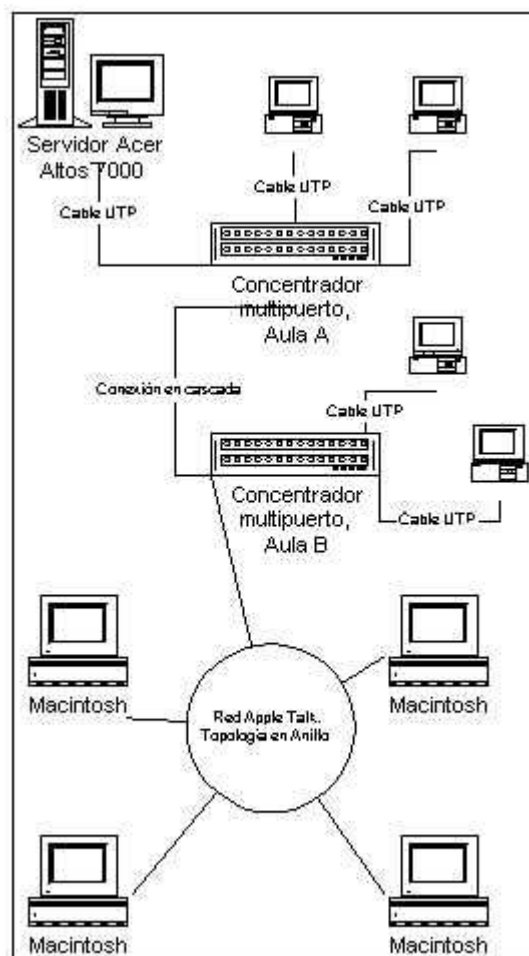
- Rellena una tabla de este tipo, en las celdas centrales escribe las comparaciones del switch con el hub.

	Mejor	Peor
Switch		
Hub		

- ¿Qué es una VLAN? Visita esta página <http://es.wikipedia.org/wiki/VLAN>
- Visita la página <http://www.monografias.com/trabajos35/subnetting-vlsm/subnetting-vlsm.shtml#ejercicios> y establece una relación entre VLAN y la creación de subredes
- Usa esta dirección <http://fis.unab.edu.co/docentes/rcarvaja/cursos/conmuta.pdf> para:
 - explica qué es la latencia
 - explica la segmentación con switches

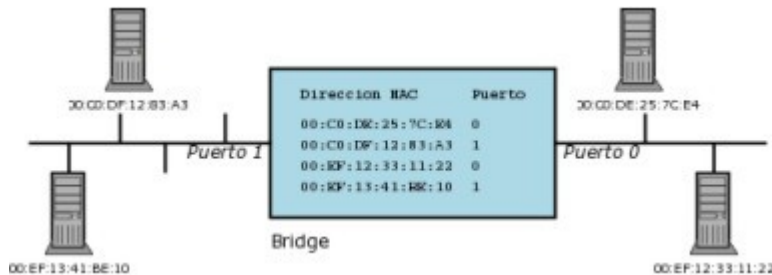
5 Puentes

El puente es un dispositivo que actúa en la subcapa LLC del nivel de enlace. Por tanto, las redes que conecta un puente pueden tener distinto protocolo de subnivel MAC (IEEE 802.3, 802.4 802.5 u otras), pero idéntica capa LLC (IEEE 802.2)



Los puentes copian las tramas MAC completas, observan su dirección de destino y las redirige hacia las salidas o puertos adecuados. En cierto sentido es bastante parecido a un switch de almacenamiento y reexpedición, aunque tiene dos diferencias fundamentales:

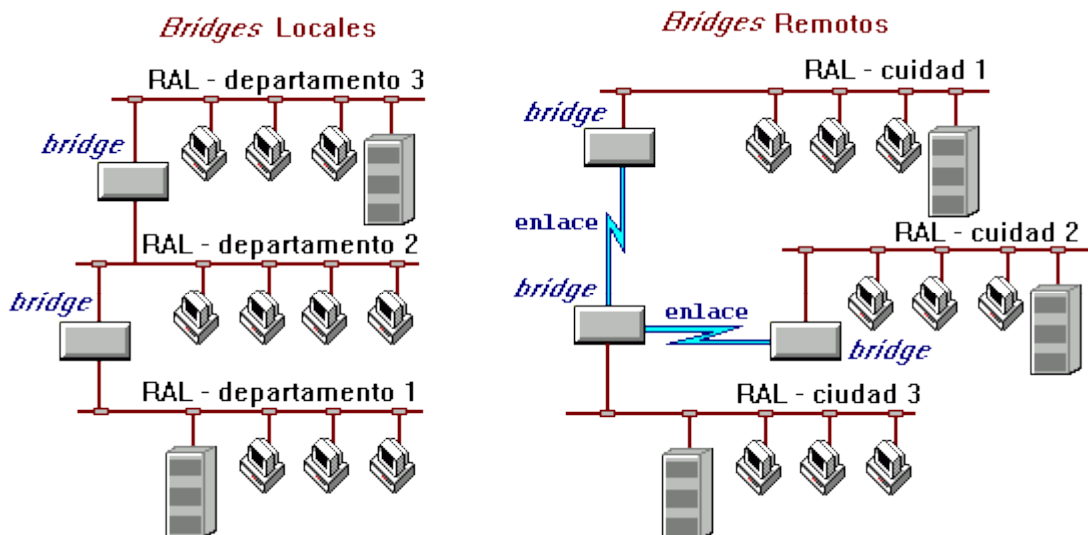
- al operar en la capa LLC puede conectar redes con distinta capa MAC y por tanto, debe ser capa de convertir los formatos de las tramas MAC.
- Pueden tomar decisiones de encaminamiento más complejas que los switches, en caso de que exista más de una ruta posible entre la red origen y la red destino.



Tipos de puentes en función del alcance

Hay dos tipos de puentes:

- **Locales:** conectan segmentos de red situados en la misma área
- **Remotos:** se conectan en parejas, enlazando dos o más redes locales, formando una red de área extensa, a través de líneas telefónicas



<http://www.csi.map.es/csi/silice/Redcon10.html>

Tipos de puentes en función de la técnica de filtrado

Se puede realizar otra división de los puentes en función de la técnica de filtrado y envío (bridging) que utilicen:

- **Spanning Tree Protocol Bridge o Transparent Protocol Bridge** (Protocolo de Arbol en Expansión o Transparente, STP).

Estos puentes deciden qué paquetes se filtran en función de un conjunto de

tablas de direcciones almacenadas internamente. Su objetivo es evitar la formación de bucles entre las redes que interconecta. Se emplea normalmente en entornos Ethernet.

- **Source Routing Protocol Bridge** (Puente de Protocolo de Encaminamiento por Emisor, SRP).

El emisor ha de indicar al puente cuál es el camino a recorrer por el paquete que quiere enviar. Se utiliza normalmente en entornos TokenRing.

- **Source Routing Transparent Protocol Bridge** (Puente de Protocolo de Encaminamiento por Emisor Transparente, SRTP).

Este tipo de puentes pueden funcionar en cualquiera de las técnicas anteriores.

Ventajas y desventajas de los puentes

Ventajas de la utilización de puentes:

- **Fiabilidad.** Utilizando *bridges* se segmentan las redes de forma que un fallo sólo imposibilita las comunicaciones en un segmento.
- **Eficiencia.** Segmentando una red se limita el tráfico por segmento, no influyendo el tráfico de un segmento en el de otro.
- **Seguridad.** Creando diferentes segmentos de red se pueden definir distintos niveles de seguridad para acceder a cada uno de ellos, siendo no visible por un segmento la información que circula por otro.
- **Dispersión.** Cuando la conexión mediante repetidores no es posible debido a la excesiva distancia de separación, los *bridges* permiten romper esa barrera de distancias.

Desventajas de los puentes:

- Son ineficientes en grandes interconexiones de redes, debido a la gran cantidad de tráfico administrativo que se genera.
- Pueden surgir problemas de temporización cuando se encadenan varios *bridges*.
- Pueden aparecer problemas de saturación de las redes por tráfico de difusión.

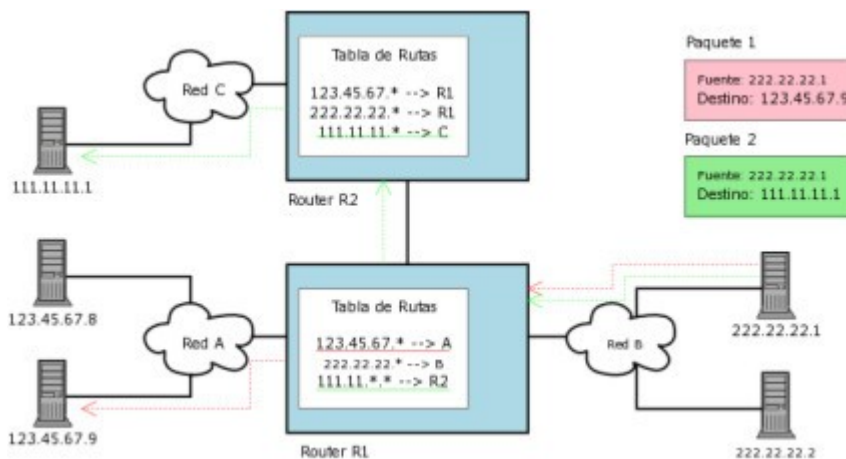
Cuestiones

- Explica brevemente y con tus propias palabras en qué consiste el algoritmo de spanning-tree. Puedes usar estas direcciones
 - <http://www.inf.utfsm.cl/~rpezoa/apuntes/Capitulo10.pdf>
 - <http://www.decom-uv.cl/~mferrand/cursos/redes/spanningtree.pdf>
 - http://es.wikipedia.org/wiki/Spanning_tree
- Se tienen 4 habitaciones con 5 equipos en cada una, y en las que se usa Ethernet, en otra habitación se tienen 25 equipos y también se usa Ethernet. En otra habitación se tienen 30 equipos conectados con Token Ring. Explica qué usarías para conectar los equipos de cada habitación en la que se use Ethernet y para conectar las distintas habitaciones. Explica tus decisiones.
- Haz una tabla comparativa con hubs, switches y puentes.

6 Router

El router (enrutador o encaminador) es un dispositivo hardware o software de interconexión de redes de computadoras que opera en la capa tres (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red.

El router toma decisiones lógicas con respecto a la mejor ruta para el envío de datos a través de una red interconectada y luego dirige los paquetes hacia el segmento y el puerto de salida adecuados. Sus decisiones se basan en diversos parámetros. Una de las más importantes es decidir la dirección de la red hacia la que va destinado el paquete (En el caso del protocolo IP esta sería la dirección IP). Otras decisiones son la carga de tráfico de red en los distintos interfaces de red del router y establecer la velocidad de cada uno de ellos, dependiendo del protocolo que se utilice.



En el ejemplo del diagrama, se muestran 3 redes IP interconectadas por 2 routers. La computadora con el IP 222.22.22.1 envía 2 paquetes, uno para la computadora 123.45.67.9 y otro para 111.11.11.1. A través de sus tablas de enrutamiento configurados previamente, los routers pasan los paquetes para la red o router con el rango de direcciones que corresponde al destino del paquete. Nota: el contenido de las tablas de rutas está simplificado por motivos didácticos. En realidad se utilizan máscaras de red para definir las subredes interconectadas.