Capítulo 1
Introducción a las redes

1.1 Concepto de red y clasificaciones

Una *red* es un sistema de transmisión de datos que permite el intercambio de información entre ordenadores. Si bien esta definición es demasiado general, nos sirve como punto de partida. La información que pueden intercambiar los ordenadores de una red puede ser de lo más variada: correos electrónicos, vídeos, imágenes, música en formato MP3, registros de una base de datos, páginas web, etc. La transmisión de estos datos se produce a través de un medio de transmisión o combinación de distintos medios: cables de fibra óptica, tecnología inalámbrica, enlaces vía satélite (el intercambio de información entre ordenadores mediante disquetes no se considera una red).

En la definición anterior hemos indicado el término ordenadores en un intento por simplificar. Sin embargo, los ordenadores son sólo una parte de los distintos dispositivos electrónicos que pueden tener acceso a las redes, en particular a Internet. Otros dispositivos de acceso son los asistentes personales (PDA) y las televisiones (Web TV). Incluso, ya existen frigoríficos capaces de intercambiar información (la lista de la compra) con un supermercado virtual.

> ***Nota:*** *En la práctica el término "red" se suele utilizar con una acepción distinta a la que hemos visto. A partir del siguiente capítulo cada vez que lo usemos nos estaremos refiriendo a un conjunto de máquinas con la misma dirección de red. La dirección de red está relacionada con la configuración lógica que hagamos a las máquinas no con la disposición del cableado. Lo habitual es que las empresas tengan solamente una red, aunque también pueden tener varias con objeto de facilitar su administración o mejorar su seguridad. Las redes se conectan mediante encaminadores (routers). Esto es precisamente lo que queremos significar cuando hablamos de que Internet es la Red de redes.*

Clasificación según su tamaño: LAN, MAN y WAN

Las redes LAN (*Local Area Network*, redes de área local) son las redes que todos conocemos, es decir, aquellas que se utilizan en nuestra empresa. Son redes pequeñas, entendiendo como pequeñas las redes de una oficina, de un edificio… Debido a sus limitadas dimensiones, son redes muy rápidas en las cuales cada estación se puede comunicar con el resto.

Las redes WAN (*Wide Area Network*, redes de área extensa) son redes punto a punto que interconectan países y continentes. Por ejemplo, un cable submarino entre Europa y América, o bien una red troncal de fibra óptica para interconectar dos países. Al tener que recorrer una gran distancia sus velocidades son menores que en las LAN aunque son capaces de transportar una mayor cantidad de datos.

Como vemos, las redes LAN son pequeñas y las redes WAN, muy grandes: debe existir algún término para describir unas redes de tamaño intermedio. Esto es, las redes MAN (*Metropolitan Area Network*, redes de área metropolitana). Un ejemplo es la red utilizada en una pequeña población de la Comunidad Valenciana, Villena, para interconectar todos sus comercios, hogares y administraciones públicas (proyecto *InfoVille*).

Clasificación según su distribución lógica

Todos los ordenadores tienen un lado cliente y otro servidor: una máquina puede ser servidora de un determinado servicio pero cliente de otro servicio.

- **Servidor**. Máquina que ofrece información o servicios al resto de los puestos de la red. La clase de información o servicios que ofrezca determina el tipo de servidor que es: servidor de impresión, de archivos, de páginas web, de correo, de usuarios, de *IRC* (charlas en Internet), de base de datos...
- **Cliente**. Máquina que accede a la información de los servidores o utiliza sus servicios. Ejemplos: Cada vez que estamos viendo una página web (almacenada en un servidor remoto) nos estamos comportando como clientes. También seremos clientes si utilizamos el servicio de impresión de un ordenador remoto en la red (el servidor que tiene la impresora conectada).

Dependiendo de si existe una función predominante o no para cada puesto de la red, las redes se clasifican en:

- Redes cliente/servidor. Los papeles de cada puesto están bien definidos: uno o más ordenadores actúan como servidores y el resto como clientes. Los servidores suelen coincidir con las máquinas más potentes de la red. No se utilizan como puestos de trabajo. En ocasiones, ni siquiera tienen monitor puesto que se administran de forma remota: toda su potencia está destinada a ofrecer algún servicio a los ordenadores de la red. Internet es una red basada en la arquitectura cliente/servidor.
- Redes entre iguales. No existe una jerarquía en la red: todos los ordenadores pueden actuar como clientes (accediendo a los recursos de otros puestos) o como servidores (ofreciendo recursos). Son las redes que utilizan las pequeñas oficinas, de no más de 10 ordenadores.

1.2 Conmutación de circuitos, de mensajes y de paquetes

La comunicación entre un origen y un destino habitualmente pasa por nodos intermedios que se encargan de encauzar el tráfico. Por ejemplo, en las llamadas telefónicas los nodos intermedios son las centralitas telefónicas y en las conexiones a Internet, los *routers* o encaminadores. Dependiendo de la utilización de estos nodos intermedios, se distingue entre conmutación de circuitos, de mensajes y de paquetes.

- En la conmutación de circuitos se establece un camino físico entre el origen y el destino durante el tiempo que dure la transmisión de datos. Este camino es exclusivo para los dos extremos de la comunicación: no se comparte con otros usuarios (ancho de banda fijo). Si no se transmiten datos o se transmiten pocos se estará infrautilizando el canal. Las comunicaciones a través de líneas telefónicas analógicas (RTB) o digitales (RDSI) funcionan mediante conmutación de circuitos.

- Un mensaje que se transmite por conmutación de mensajes va pasando desde un nodo al siguiente, liberando el tramo anterior en cada paso para que otros puedan utilizarlo y esperando a que el siguiente tramo esté libre para transmitirlo. Esto implica que el camino origen-destino es utilizado de forma simultánea por distintos mensajes. Sin embargo, éste método no es muy útil en la práctica ya que los nodos intermedios necesitarían una elevada memoria temporal para almacenar los mensajes completos. En la vida real podemos compararlo con el correo postal.

- Finalmente, la conmutación de paquetes es la que realmente se utiliza cuando hablamos de *redes*. Los mensajes se fragmentan en paquetes y cada uno de ellos se envía de forma independiente desde el origen al destino. De esta manera, los nodos (*routers*) no necesitan una gran memoria temporal y el tráfico por la red es más fluido. Nos encontramos aquí con una serie de problemas añadidos: la pérdida de un paquete provocará que se descarte el mensaje completo; además, como los paquetes pueden seguir rutas distintas puede darse el caso de que lleguen desordenados al destino. Esta es la forma de transmisión que se utiliza en Internet: los fragmentos de un mensaje van pasando a través de distintas redes hasta llegar al destino.

1.3 Comunicación *simplex*, *half-duplex* y *full-duplex*

- En una comunicación simplex existe un solo canal unidireccional: el origen puede transmitir al destino pero el destino no puede comunicarse con el origen. Por ejemplo, la radio y la televisión.
- En una comunicación half-duplex existe un solo canal que puede transmitir en los dos sentidos pero no simultáneamente: las estaciones se tienen que turnar. Esto es lo que ocurre con las emisoras de radioaficionados.
- Por último, en una comunicación full-duplex existen dos canales, uno para cada sentido: ambas estaciones pueden transmitir y recibir a la vez. Por ejemplo, el teléfono.

1.4 Mecanismos de detección de errores

¿Cómo puede saber el receptor que ha recibido el mismo mensaje que envió el emisor? ¿Cómo puede saber que no se ha producido ningún error que haya alterado los datos durante la transmisión? Estas cuestiones son las que vamos a plantear en este apartado: se necesitan mecanismos de detección de errores para garantizar transmisiones libres de errores. Si el receptor detecta algún error, puede actuar de diversas maneras según los protocolos que esté utilizando. La solución más sencilla es enviarle un mensaje al emisor pidiéndole que le reenvíe de nuevo la información que llegó defectuosa.

Los mecanismos de detección se basan en añadir a las transmisiones una serie de *bits* adicionales, denominados *bits de redundancia*. La redundancia es aquella parte del mensaje que sería innecesaria en ausencia de errores (es decir, no aporta información nueva: sólo permite detectar errores). Algunos métodos incorporan una redundancia capaz de corregir errores. Estos son los *mecanismos de detección y corrección de errores*.

Como ejemplos de mecanismos de detección de errores vamos a estudiar a continuación la paridad y los códigos CRC.

Paridad

Las transmisiones se dividen en palabras de cierto número de bits (por ejemplo, 8 bits) y se envían secuencialmente. A cada una de estas palabras se le añade un único bit de redundancia (*bit de paridad*) de tal forma que la suma de todos los bits de la palabra sea siempre un número par (*paridad par*) o impar (*paridad impar*).

El emisor envía las palabras añadiendo los correspondientes bits de paridad. El receptor comprobará a su llegada que la suma de los bits de la palabra incluyendo la redundancia es un número par (si la codificación convenida entre emisor-receptor es de paridad par) o un número impar (paridad impar). Si el receptor encuentra alguna palabra que no se ajuste a la codificación establecida, le solicitará al emisor que le reenvíe de nuevo la información.

La paridad únicamente permite detectar errores simples, esto es, que varíe un único bit en cada palabra. Si varían 2 bits, este mecanismo no es capaz de detectar el error.

Veamos un ejemplo de paridad par:

Datos *(8 bits)*	**Datos + redundacia** *(9 bits)*	**Suma de bits**
10110110	101101101	6
00101001	001010011	4
11001001	110010010	4
11111010	111110100	6
00010000	000100001	2

El receptor realizará la suma de bits a la llegada del mensaje. Si alguna palabra no suma un número par, significará que se ha producido un error durante la transmisión.

CRC

Los códigos de paridad tienen el inconveniente de que se requiere demasiada redundancia para detectar únicamente errores simples. En el ejemplo que hemos visto, sólo un 8/9 de la información transmitida contenían datos, el resto era redundancia. Los *códigos de redundancia cíclica* (CRC) son muy utilizados en la práctica para la detección de errores en largas secuencias de datos. Se basan en representar las cadenas de datos como polinomios. El emisor realiza ciertas operaciones matemáticas antes de enviar los datos. El receptor realizará, a la llegada de la transmisión, una división entre un polinomio convenido (*polinomio generador*). Si el resto es cero, la transmisión ha sido correcta. Si el resto es distinto significará que se han producido errores y solicitará la retransmisión al emisor.

1.5 Control de flujo

El control de flujo determina cómo enviar la información entre el emisor y el receptor de forma que se vaya recibiendo correctamente sin saturar al receptor. Nótese que puede darse el caso de un emisor rápido y un receptor lento (o un receptor rápido pero que esté realizando otras muchas tareas).

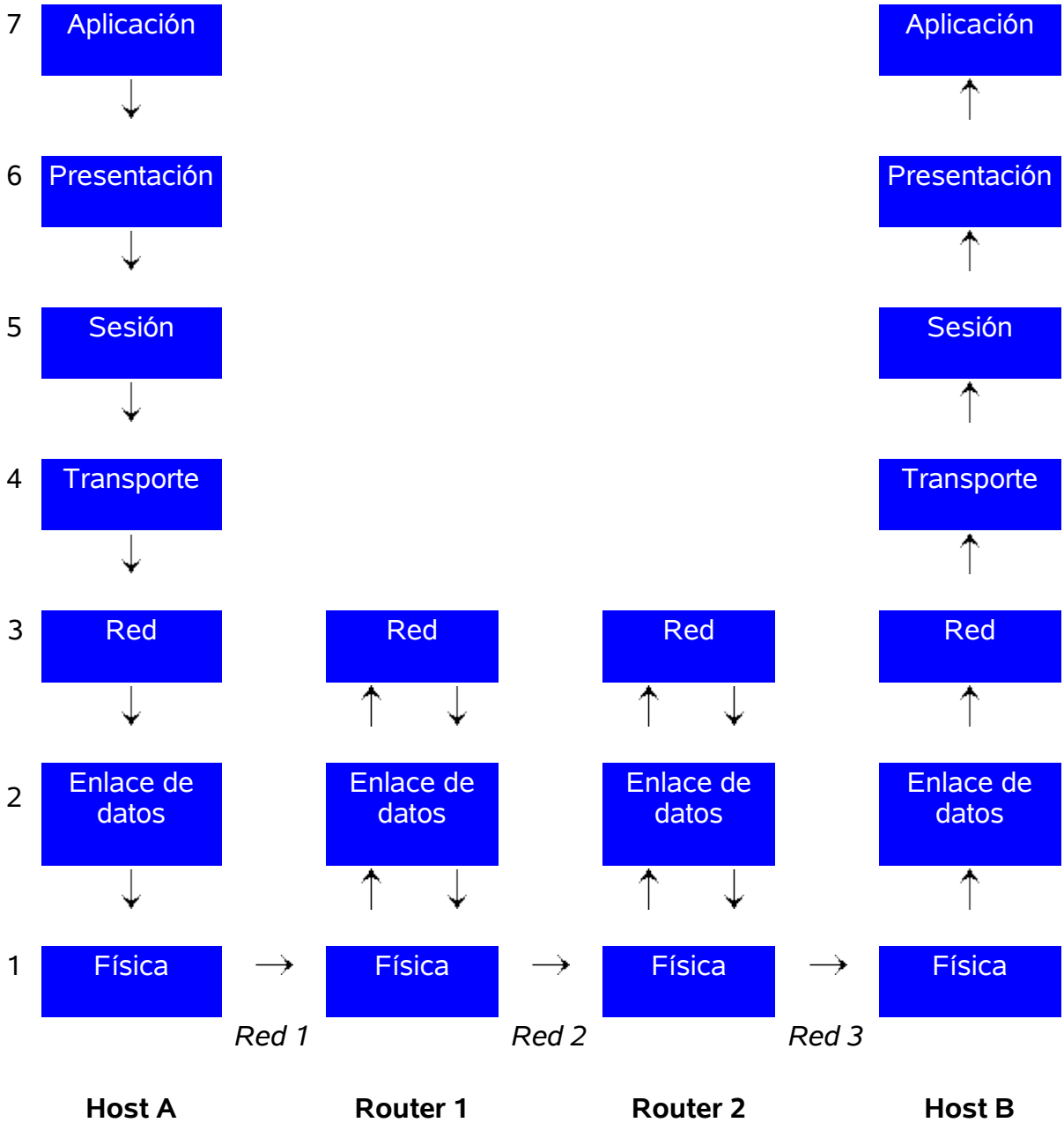
El mecanismo más sencillo de control de flujo se basa en devolver una *confirmación* o *acuse de recibo* (ACK) cada vez que el receptor reciba algún dato correcto o una señal de error (NACK) si el dato ha llegado dañado. Cuando el emisor recibe un ACK pasa a enviar el siguiente dato. Si, en cambio, recibe un NACK reenviará el mismo dato.

El procedimiento anterior tiene el gran inconveniente de que el canal se encuentra infrautilizado: hasta que el emisor no reciba un ACK no enviará ningún dato más, estando el canal desaprovechado todo ese tiempo. Una mejora de este método es el envío de una serie de datos numerados, de tal forma que en un sentido siempre se estén enviando datos (dato1, dato2, dato3...) y en el otro sentido se vayan recibiendo las confirmaciones (ACK1, ACK2, ACK3...). La cantidad de datos pendientes de ACK o NACK se establecerá según la memoria temporal del emisor.

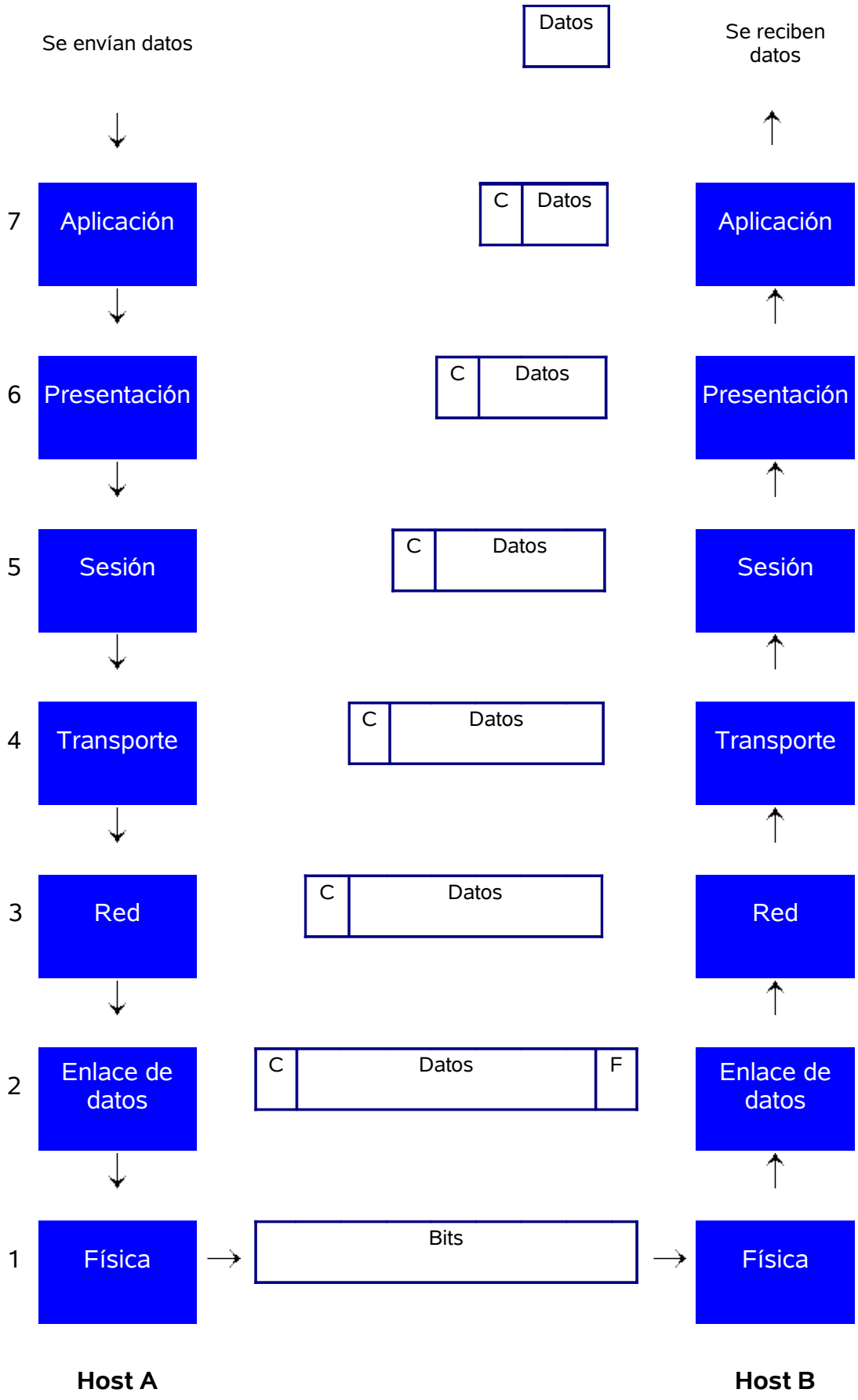
1.6 Modelo de referencia OSI. Comparación con el modelo TCP/IP

El modelo OSI (*Open Systems Interconnection*, interconexión de sistemas abiertos) fue un intento de la Organización Internacional de Normas (ISO) para la creación de un estándar que siguieran los diseñadores de nuevas redes. Se trata de un modelo teórico de referencia: únicamente explica lo que debe hacer cada componente de la red sin entrar en los detalles de implementación.

El modelo divide las redes en capas. Cada una de estas capas debe tener una función bien definida y relacionarse con sus capas inmediatas mediante unos interfaces también bien definidos. Esto debe permitir la sustitución de una de las capas sin afectar al resto, siempre y cuando no se varíen los interfaces que la relacionan con sus capas superior e inferior. Los creadores del modelo OSI consideraron que era 7 el número de capas que mejor se ajustaba a sus requisitos.



El gráfico anterior muestra las 7 capas del modelo OSI. Las tres primeras capas se utilizan para *enrutar*, esto es, mover la información de unas redes a otras. En cambio, las capas superiores son exclusivas de los nodos origen y destino. La capa física está relacionada con el medio de transmisión (cableado concreto que utiliza cada red). En el extremo opuesto se encuentra la capa de aplicación: un programa de mensajería electrónica, por ejemplo. El usuario se situaría por encima de la capa 7. El siguiente gráfico muestra el flujo de información entre capas.



El host A es el nodo origen y el host B, el nodo destino. Nótese que estos papeles se intercambian continuamente en cualquier comunicación. Supongamos que mediante este modelo queremos enviar un mensaje al usuario del host B. El mensaje son los "datos" que se han dibujado por encima de la capa 7. Estos datos van descendiendo de capa en capa hasta llegar a la capa física del host A. Cada capa añade un encabezado (C = cabecera) a los datos que recibe de la capa superior antes de enviárselos a su capa inferior. En la capa de enlace de datos se ha añadido también una serie de códigos al final de la secuencia

(F = final) para delimitar no sólo el comienzo sino también el final de un paquete de datos. La capa física no entiende de datos ni de códigos: únicamente envía una secuencia de bits por el medio de transmisión (un cable).

Estos bits llegarán, probablemente pasando por varios encaminadores intermedios, hasta la capa física del host destino. A medida que se van recibiendo secuencias de bits, se van pasando a las capas superiores. Cada capa elimina su encabezado antes de pasarlo a una capa superior. Obsérvese que el mensaje que envía cada capa del host A a su capa inferior es idéntico al que recibe la capa equivalente del host B desde una capa inferior. Finalmente los datos llegarán a la capa de aplicación, serán interpretados y mostrados al usuario del host B.

Los paquetes de datos de cada capa suelen recibir nombres distintos. En la capa de enlace de datos se habla de *marcos* o *tramas*; en la capa de red, de *paquetes* o *datagramas*. En la capa de transporte, en ocasiones se utiliza el término *segmento*.

Cada capa se comunica con la capa equivalente de otro host (por ejemplo, la capa de red de un host *se entiende* con la capa de red de otro host) . Sin embargo, como hemos visto, la comunicación realmente se realiza descendiendo capas en el host origen, transmitiendo por el medio físico y aumentando capas en el host destino. Cada capa añade algo nuevo a la comunicación, como vamos a ver ahora:

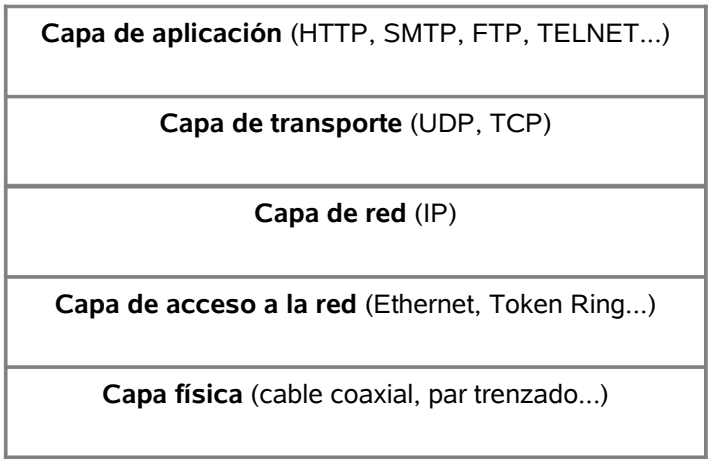
- **Capa física**. Se encarga de la transmisión de bits por un medio de transmisión, ya sea un medio guiado (un cable) o un medio no guiado (inalámbrico). Esta capa define, entre otros aspectos, lo que transmite cada hilo de un cable, los tipos de conectores, el voltaje que representa un 1 y el que representa un 0. La capa física será diferente dependiendo del medio de transmisión (cable de fibra óptica, cable par trenzado, enlace vía satélite, etc.) No interpreta la información que está enviando: sólo transmite ceros y unos.
- **Capa de enlace de datos**. Envía tramas de datos entre hosts (o *routers*) de una misma red. Delimita las secuencias de bits que envía a la capa física, escribiendo ciertos códigos al comienzo y al final de cada trama. Esta capa fue diseñada originalmente para *enlaces punto a punto*, en los cuales hay que aplicar un control de flujo para el envío continuo de grandes cantidades de información. Para las *redes de difusión* (redes en las que muchos ordenadores comparten un mismo medio de transmisión) fue necesario diseñar la llamada subcapa de acceso al medio. Esta subcapa determina quién puede acceder al medio en cada momento y cómo sabe cada host que un mensaje es para él, por citar dos problemas que se resuelven a este nivel.
- **Capa de red**. Se encarga del encaminamiento de paquetes entre el origen y el destino, atravesando tantas redes intermedias como sean necesarias. Los mensajes se fragmentan en paquetes y cada uno de ellos se envía de forma independiente. Su misión es unificar redes heterogéneas: todos los host tendrán un identificador similar a nivel de la capa de red (en Internet son las direcciones IP) independientemente de las redes que tengan en capas inferiores (Token Ring con cable coaxial, Ethernet con cable de fibra óptica, enlace submarino, enlace por ondas, etc.)
- **Capa de transporte**. Únicamente se preocupa de la transmisión origen-destino. Podemos ver esta capa como una canalización fiable que une un proceso de un host con otro proceso de otro host. Un host puede tener varios procesos ejecutándose: uno para mensajería y otro para transferir archivos, por ejemplo. No se preocupa del camino intermedio que siguen los fragmentos de los mensajes. Integra control de flujo y control de errores, de forma que los datos lleguen correctamente de un extremo a otro.
- **Capa de sesión**. Se encarga de iniciar y finalizar las comunicaciones. Además proporciona servicios mejorados a la capa de transporte como, por ejemplo, la creación de puntos de sincronismo para recuperar transferencias largas fallidas.
- **Capa de presentación**. Codifica los datos que recibe de la capa de aplicación a un sistema convenido entre emisor y receptor, con el propósito de que tanto textos como números sean interpretados correctamente. Una posibilidad es codificar los textos según la *tabla ASCII* y los números en *complemento a dos*.
- **Capa de aplicación**. Aquí se encuentran los protocolos y programas que utiliza el usuario para sus comunicaciones en red. Esta capa tendrá que ser adaptada para cada tipo de ordenador de forma que sea posible el envío de un correo electrónico (u otros servicios) entre sistemas heterogéneos como Macintosh, Linux o Windows.

El modelo OSI, patrocinado por la Comunidad Europea y, más tarde, por el gobierno de los Estados Unidos, nunca llegó a tener la implantación esperada. Entre otros motivos, porque el modelo TCP/IP ya había sido aceptado por aquella época entre investigadores los cuales se resistieron a un cambio que, para la mayoría, era un cambio a peor. Las bases que sustentan Internet son realmente sencillas y quizás esto ha sido la clave de su éxito; el modelo OSI, en cambio, fue tan ambicioso y complejo que terminó arrinconado en las estanterías de los laboratorios.

Sin embargo, la idea de la división por capas del modelo OSI es realmente valiosa. Esta misma idea se aplica a todas las redes actuales, incluyendo Internet.

Como hemos comentado al principio, OSI es un modelo teórico general que da preferencia a un buen diseño en papel, antes que a la implementación de los protocolos. El modelo TCP/IP se hizo justamente al revés: primero vinieron los protocolos y, después, se pensó en sus especificaciones. De tal forma, que el modelo TCP/IP únicamente es aplicable para la pila de protocolos TCP/IP pero no es válido para nuevas redes.

El modelo TCP/IP tiene únicamente 3 capas: capa de red, de transporte y de aplicación. No tiene las capas de sesión ni de presentación que, por otro lado, estaban prácticamente vacías en el modelo OSI. Tampoco dice nada de las capas física y de enlace a datos. Sin embargo, nosotros seguiremos un modelo de referencia fruto de combinar los modelos OSI y TCP/IP. Se trata del modelo real que se está utilizando actualmente en las redes TCP/IP. El siguiente gráfico refleja las 5 capas de nuestro modelo.



1.7 Capa física: medios de transmisión

La capa física determina el soporte físico o medio de transmisión por el cual se transmiten los datos. Estos medios de transmisión se clasifican en *guiados* y *no guiados*. Los primeros son aquellos que utilizan un medio sólido (un cable) para la transmisión. Los medios no guiados utilizan el aire para transportar los datos: son los medios inalámbricos.

Los medios guiados se estudian más abajo.

- **Cable coaxial**
- **Par trenzado**
- **Fibra óptica**

Entre los medios no guiados se encuentran:

- **Ondas de radio**. Son capaces de recorrer grandes distancias, atravesando edificios incluso. Son ondas omnidireccionales: se propagan en todas las direcciones. Su mayor problema son las interferencias entre usuarios.
- **Microondas**. Estas ondas viajan en línea recta, por lo que emisor y receptor deben estar alineados

cuidadosamente. Tienen dificultades para atravesar edificios. Debido a la propia curvatura de la tierra, la distancia entre dos repetidores no debe exceder de unos 80 Kms. de distancia. Es una forma económica para comunicar dos zonas geográficas mediante dos torres suficientemente altas para que sus extremos sean visibles.

- **Infrarrojos**. Son ondas direccionales incapaces de atravesar objetos sólidos (paredes, por ejemplo) que están indicadas para transmisiones de corta distancia.
- **Ondas de luz**. Las ondas láser son unidireccionales. Se pueden utilizar para comunicar dos edificios próximos instalando en cada uno de ellos un emisor láser y un fotodetector.

Cable coaxial

El cable coaxial es similar al cable utilizado en las antenas de televisión: un hilo de cobre en la parte central rodeado por una malla y separados ambos elementos conductores por un cilindro de plástico. Las redes que utilizan este cable requieren que los adaptadores tengan un conector apropiado: los ordenadores forman una fila y se coloca un segmento de cable entre cada ordenador y el siguiente. En los extremos hay que colocar un terminador, que no es más que una resistencia de 50 ohmios. La velocidad máxima que se puede alcanzar es de 10Mbps.

Cable par trenzado

El par trenzado es similar al cable telefónico, sin embargo consta de 8 hilos y utiliza unos conectores un poco más anchos. Dependiendo del número de trenzas por unidad de longitud, los cables de par trenzado se clasifican en categorías. A mayor número de trenzas, se obtiene una mayor velocidad de transferencia.

- Categoría 3, hasta 16 Mbps
- Categoría 4, hasta 20 Mbps
- Categoría 5 y Categoría 5e, hasta 1 Gbps
- Categoría 6, hasta 1 Gbps y más

Los cables par trenzado pueden ser a su vez de dos tipos:

- UTP (*Unshielded Twisted Pair*, par trenzado no apantallado)
- STP (*Shielded Twisted Pair*, par trenzado apantallado)

Los cables UTP son los más utilizados debido a su bajo coste y facilidad de instalación. Los cables STP están embutidos en una malla metálica que reduce las interferencias y mejora las características de la transmisión. Sin embargo, tienen un coste elevado y al ser más gruesos son más complicados de instalar.

El cableado que se utiliza en la actualidad es UTP CAT5. El cableado CAT6 es demasiado nuevo y es difícil encontrarlo en el mercado. Los cables STP se utilizan únicamente para instalaciones muy puntuales que requieran una calidad de transmisión muy alta.

Los segmentos de cable van desde cada una de las estaciones hasta un aparato denominado *hub* o concentrador, formando una topología de estrella.

Cable de fibra óptica

En los cables de fibra óptica la información se transmite en forma de pulsos de luz. En un extremo del cable se coloca un diodo luminoso (LED) o bien un láser, que puede emitir luz. Y en el otro extremo se sitúa un detector de luz.

Curiosamente y a pesar de este sencillo funcionamiento, mediante los cables de fibra óptica se llegan a alcanzar velocidades de varios Gbps. Sin embargo, su instalación y mantenimiento tiene un coste elevado y solamente son utilizados para redes troncales con mucho tráfico.

Los cables de fibra óptica son el medio de transmisión elegido para las redes de *cable* que ya están funcionando en algunas zonas de España. Se pretende que este *cable* pueda transmitir televisión, radio, Internet y teléfono.

Capítulo 2
Instalación de cableado

2.1 Cable coaxial

(No disponible)

2.2 Cable par trenzado

Cable par trenzado directo

Los conectores de cada extremo siguen el mismo esquema de colores.

[En revisión. Se completará próximamente]

Estos cables se utilizan para unir:

- Ordenador con hub.
- 2 hubs (utilizando el puerto *uplink* de uno de ellos y un puerto normal del otro).

> ***Nota:*** *Los puertos uplink y la interconexión de hubs se explica en el apartado* *Interconexión de hubs**.*

Cable par trenzado cruzado

En un extremo del cable se utiliza el esquema propuesto en el apartado anterior. En el otro extremo, se utiliza el siguiente:

Lo que estamos haciendo es cruzar los pines de transmisión (Tx+ y Tx-) de un extremo con los pines de recepción (Rx+ y Rx-) del otro. Los hilos marcados como N/U no se utilizan.

Estos cables se utilizan para unir:

- 2 ordenadores sin necesidad de hub (el cable va de una tarjeta de red a la otra).
- 2 hubs (sin utilizar el puerto *uplink* de ninguno de ellos o utilizando el puerto *uplink* en ambos).

2.3 Comparación entre *hub* y *switch*

Un *hub* pertenece a la capa física: se puede considerar como una forma de interconectar unos cables con otros. Un *switch*, en cambio, trabaja en la capa de acceso a la red (son la versión moderna de los puentes o *bridges*) pero también puede tratarse como un sistema de interconexión de cables, eso sí, con cierta *inteligencia*. Los puestos de la red no tienen forma de conocer si las tramas Ethernet que están recibiendo proceden de un hub, switch o han pasado directamente mediante un cable par trenzado cruzado. Estos dispositivos no requieren ninguna configuración software: únicamente con enchufarlos ya comienzan a operar.

> ***Nota:*** *Un router (encaminador) pertenece a la capa de red. Trabaja con direcciones IP. Se utiliza para interconectar redes y requiere una configuración. Podemos averiguar los routers que atraviesan nuestros datagramas IP mediante el comando* ***Tracert****.*

Un *hub* o concentrador es el punto central desde el cual parten los cables de par trenzado hasta las distintos puestos de la red, siguiendo una topología de estrella. Se caracterizan por el número de puertos y las velocidades que soportan. Por ejemplo, son habituales los hubs 10/100 de 8 puertos.

- Los hubs *difunden* la información que reciben desde un puerto por todos los demás (su comportamiento es similar al de un ladrón eléctrico).
- Todas sus ramas funcionan a la *misma velocidad*. Esto es, si mezclamos tarjetas de red de 10/100 Mbps y 10 Mbps en un mismo hub, todas las ramas del hub funcionarán a la velocidad menor (10 Mbps).
- Es habitual que contengan un *diodo luminoso* para indicar si se ha producido una colisión. Además, los concentradores disponen de tantas lucecitas (LED) como puertos para informar de las ramas que tienen señal.

Un *switch* o conmutador es un hub mejorado: tiene las mismas posibilidades de interconexión que un hub (al igual que un hub, no impone ninguna restricción de acceso entre los ordenadores conectados a sus puertos). Sin embargo se comporta de un modo más eficiente reduciendo el tráfico en las redes y el número de colisiones.

- Un switch *no difunde* las tramas Ethernet por todos los puertos, sino que las retransmite sólo por los puertos necesarios. Por ejemplo, si tenemos un ordenador A en el puerto 3, un ordenador B en el puerto 5 y otro ordenador C en el 6, y enviamos un mensaje desde A hasta C, el mensaje lo recibirá el switch por el puerto 3 y sólo lo reenviará por el puerto 6 (un hub lo hubiese reenviado por todos sus puertos).
- Cada puerto tiene un *buffer* o memoria intermedia para almacenar tramas Ethernet.
- Puede trabajar con *velocidades distintas* en sus ramas (*autosensing*): unas ramas pueden ir a 10 Mbps y otras a 100 Mbps.
- Suelen contener 3 *diodos luminosos* para cada puerto: uno indica si hay señal (link), otro la velocidad de la rama (si está encendido es 100 Mbps, apagado es 10 Mbps) y el último se enciende si se ha producido una colisión en esa rama.

¿Cómo sabe un switch los ordenadores que tiene en cada rama?

Lo averigua de forma automática mediante *aprendizaje*. Los conmutadores contienen una tabla dinámica de direcciones físicas y números de puerto. Nada más enchufar el switch esta tabla se encuentra vacía. Un procesador analiza las tramas Ethernet entrantes y busca la dirección física de destino en su tabla. Si la encuentra, únicamente reenviará la trama por el puerto indicado. Si por el contrario no la encuentra, no le quedará más remedio que actuar como un hub y difundirla por todas sus ramas.

Las tramas Ethernet contienen un campo con la dirección física de origen que puede ser utilizado por el switch para agregar una entrada a su tabla basándose en el número de puerto por el que ha recibido la trama. A medida que el tráfico se incrementa en la red, la tabla se va construyendo de forma dinámica. Para evitar que la información quede desactualizada (si se cambia un ordenador de sitio, por ejemplo) las entradas de la tabla desaparecerán cuando agoten su tiempo de vida (TTL), expresado en segundos.

Dominios de colisión

Un *dominio de colisión* es un segmento del cableado de la red que comparte las mismas colisiones. Cada vez que se produzca una colisión dentro de un mismo dominio de colisión, afectará a todos los ordenadores conectados a ese segmento pero no a los ordenadores pertenecientes a otros dominios de colisión.

Todas las ramas de un *hub* forman un mismo dominio de colisión (las colisiones se retransmiten por todos los puertos del hub). Cada rama de un *switch* constituye un dominio de colisiones distinto (las colisiones no se retransmiten por los puertos del switch). Este es el motivo por el cual la utilización de conmutadores reduce el número de colisiones y mejora la eficiencia de las redes. El ancho de banda disponible se reparte entre todos los ordenadores conectados a un mismo dominio de colisión.

> ***Nota:*** *Podemos indicar un número aproximado de 25-30 como medida máxima de ordenadores que se pueden conectar dentro de un mismo dominio de colisión. Sin embargo, este número dependerá en gran medida del tráfico de la red. En redes con mucho tráfico se debe tratar de reducir el número de ordenadores por dominio de colisión lo más posible mediante la creación de distintos dominios de colisión conectados por switches o mediante la creación de distintas subredes conectadas por routers.*

¿Qué instalar hubs o switches?

- Siempre que el presupuesto lo permita *elegiremos un switch antes que un hub*.
- Si nuestra red tiene un elevado número de ordenadores (hay que utilizar varios concentradores enlazados) pero sólo nos podemos permitir un switch, éste lo colocaremos en *el lugar de la red con más tráfico* (habitualmente será el concentrador situado en el centro de la estrella de estrellas o bien, aquél que contenga a los servidores). En el resto de las posiciones colocaremos hubs. El esquema descrito se utiliza a menudo: un hub en cada departamento y un switch para interconectar los departamentos con los servidores. Desde luego, lo ideal sería colocar switches en todas las posiciones.
- Además de la mejora en eficiencia que supone utilizar un switch frente a un hub, debemos considerar también el *aumento de seguridad*: si en un ordenador conectado a un switch se instala, con fines nada éticos, un programa para escuchar el tráfico de la red (*sniffer*), el atacante sólo recibirá las tramas Ethernet que corresponden a ese ordenador pero no las tramas de otros ordenadores que podrían contener contraseñas ajenas.

2.4 Interconexión de hubs

Los concentradores incluyen un puerto diferenciado, etiquetado con el nombre "uplink" o "cascade", para facilitar su interconexión con otros hubs. El puerto "uplink" de un hub se conecta mediante un cable par trenzado directo hasta un puerto cualquiera (que no sea el "uplink") del otro hub. Si ninguno de los dos hubs tuviese el puerto "uplink" libre todavía se podrían interconectar utilizando un cable par trenzado cruzado.

> ***Nota:*** *Todo lo que se comenta en este apartado referente a hubs (concentradores) es equivalente para los switches (conmutadores).*

¿Dónde se encuentra el puerto "uplink"? Dependiendo de los fabricantes se suele dar una de estas dos situaciones:

- El hub es de *n* puertos pero tiene *n+1* conectores, uno de ellos tiene una marca especial. Por ejemplo, son habituales los hubs que tienen 9 conectores: 7 puertos normales y un puerto mixto con dos conectores contiguos los cuales no se pueden utilizar simultáneamente. El número máximo de cables que podemos conectar es de 8, quedando un conector vacío (el marcado como "uplink" o el que tiene justo a su lado).
- El hub es de *n* puertos y tiene *n* conectores, uno de ellos tiene una marca especial. Mediante un botón conmutamos la función del conector diferenciado entre "uplink" y puerto normal. Las prestaciones son las mismas que en el caso anterior. Este diseño es habitual de los hubs del fabricante 3COM.

¿Cómo enlazar unos hubs con otros? Los diseños más habituales son los dos siguientes, aunque se suelen combinar:

- *Hubs encadenados*. Un hub se va conectando con el siguiente formando una cadena. No es conveniente conectar de esta forma más de 3 hubs puesto que el rendimiento de la red disminuirá considerablemente (las señales tardan en pasar desde el primer hub de la cadena hasta el último).
- *Hubs en estrella*. Se coloca un hub en el centro y de éste se tiran cables hasta el resto de los hubs. Con esta solución se consiguen velocidades más altas en la red aunque el cableado es más costoso.

Capítulo 3
Protocolos

En cada una de las capas de los modelos que estudiamos en el apartado 1-6 (excepto en la capa física) se utiliza un protocolo distinto. Estos protocolos se van apilando de forma que los de capas superiores aprovechan los servicios de los protocolos de capas inferiores. Durante una transmisión cada protocolo se comunica con su homónimo del otro extremo sin preocuparse de los protocolos de otras capas.

Una de las decisiones más importantes que debemos tomar a la hora de diseñar una red es elegir un protocolo de la capa de acceso al medio y otro de las capas de red y transporte. A continuación estudiamos los distintos protocolos. Adelantamos, no obstante, que la combinación más interesante para redes locales nuevas es Ethernet + TCP/IP.

3.1 Protocolos de la capa de acceso al medio

En la capa de acceso al medio se determina la forma en que los puestos de la red envían y reciben datos sobre el medio físico. Se responden preguntas del tipo: ¿puede un puesto dejar información en el cable siempre que tenga algo que transmitir?, ¿debe esperar algún turno?, ¿cómo sabe un puesto que un mensaje es para él?

Un organismo de normalización conocido como IEEE (Instituto de ingenieros eléctricos y electrónicos) ha definido los principales protocolos de la capa de acceso al medio conocidos en conjunto como estándares 802. Los más importantes son los IEEE 802.3 y IEEE 802.5 que se estudian a continuación.

> ***Otros estándares 802.--*** *El estándar 802.1 es una introducción al conjunto de estándares y define algunos aspectos comunes. El estándar 802.2 describe la parte superior de la capa de enlace de datos del modelo OSI (entre la capa de acceso al medio y la capa de red) que puede proporcionar control de errores y control de flujo al resto de estándares 802 utilizando el protocolo LLC (Logical Link Control, control lógico de enlace). Las normas 802.3 a 802.5 definen protocolos para redes LAN. El estándar 802.4 que no vamos a estudiar por su escasa implantación se conoce como Token Bus (bus con paso de testigo). Finalmente, 802.6 es un estándar adecuado para utilizarse en redes MAN. Se trata de DQDB (Distributed Queue Dual Bus, bus doble de colas distribuidas).*

El protocolo utilizado en esta capa viene determinado por las tarjetas de red que instalemos en los puestos. Esto quiere decir que si adquirimos tarjetas Ethernet sólo podremos instalar redes Ethernet. Y que para instalar redes Token ring necesitaremos tarjetas de red especiales para Token ring. Actualmente en el mercado únicamente se comercializan tarjetas de red Ethernet (de distintas velocidades y para distintos cableados).

Token ring (802.5)

Las redes Token ring (paso de testigo en anillo) fueron utilizadas ampliamente en entornos IBM desde su lanzamiento en el año 1985. En la actualidad es difícil encontrarlas salvo en instalaciones antiguas de grandes empresas.

El cableado se establece según una topología de anillo. En lugar de utilizar difusiones, se utilizan enlaces punto a punto entre cada puesto y el siguiente del anillo. Por el anillo Token ring circula un mensaje conocido como *token* o ficha. Cuando una estación desea transmitir espera a recibir el token. En ese momento, lo retira de circulación y envía su mensaje. Este mensaje circula por el anillo hasta que lo recibe íntegramente el destinatario. Entonces se genera un token nuevo.

Las redes Token ring utilizan una estación monitor para supervisar el funcionamiento del anillo. Se trata de un protocolo complejo que debe monitorizar en todo momento el buen funcionamiento del token (que exista exactamente uno cuando no se transmiten datos) y sacar del anillo las tramas defectuosas que no tengan destinatario, entre otras funciones.

Las redes Token ring de IBM pueden funcionar a 4 Mbps o a 16 Mbps utilizando cable par trenzado o cable coaxial.

Ethernet (802.3)

Las redes Ethernet son actualmente las únicas que tienen interés para entornos LAN. El estándar 802.3 fue diseñado originalmente para funcionar a 10 Mbps, aunque posteriormente ha sido perfeccionado para trabajar a 100 Mbps (802.3u) o 1 Gbps.

Una red Ethernet tiene las siguientes características:

- *Canal único*. Todas las estaciones comparten el mismo canal de comunicación por lo que sólo una puede utilizarlo en cada momento.
- Es de *difusión* debido a que todas las transmisiones llegan a todas las estaciones (aunque sólo su destinatario aceptará el mensaje, el resto lo descartarán).
- Tiene un *control de acceso distribuido* porque no existe una autoridad central que garantice los accesos. Es decir, no hay ninguna estación que supervise y asigne los turnos al resto de estaciones. Todas las estaciones tienen la misma prioridad para transmitir.

  Comparación de Ethernet y Token ring.-- *En Ethernet cualquier estación puede transmitir siempre que el cable se encuentre libre; en Token ring cada estación tiene que esperar su turno. Ethernet utiliza un canal único de difusión; Token ring utiliza enlaces punto a punto entre cada estación y la siguiente. Token ring tiene siempre una estación monitor que supervisa el buen funcionamiento de la red; en Ethernet ninguna estación tiene mayor autoridad que otra. Según esta comparación, la conclusión más evidente es que, a iguales velocidades de transmisión, Token ring se comportará mejor en entornos de alta carga y Ethernet, en redes con poco tráfico.*

En las redes Ethernet, cuando una estación envía un mensaje a otra, no recibe ninguna confirmación de que la estación destino haya recibido su mensaje. Una estación puede estar enviando paquetes Ethernet a

otra que está desconectada y no advertirá que los paquetes se están perdiendo. Las capas superiores (y más concretamente, TCP) son las encargadas de asegurarse que la transmisión se ha realizado de forma correcta.

El protocolo de comunicación que utilizan estas redes es el CSMA/CD (*Carrier Sense Multiple Access / Collision Detect*, acceso múltiple con detección de portadora y detección de colisiones). Esta técnica de control de acceso a la red ha sido normalizada constituyendo el estándar IEEE 802.3. Veamos brevemente el funcionamiento de CSMA/CD:

> Cuando una estación quiere transmitir, primero escucha el canal (detección de portadora). Si está libre, transmite; pero si está ocupado, espera un tiempo y vuelve a intentarlo.
>
> Sin embargo, una vez que una estación ha decidido comenzar la transmisión puede darse el caso de que otra estación haya tomado la misma decisión, basándose en que el canal estaba libre cuando ambas lo comprobaron. Debido a los retardos de propagación en el cable, ambas señales colisionarán y no se podrá completar la transmisión de ninguna de las dos estaciones. Las estaciones que están transmitiendo lo advertirán (detección de colisiones) e interrumpirán inmediatamente la transmisión. Después esperarán un tiempo aleatorio y volverán a intentarlo. Si se produce una nueva colisión, esperarán el doble del tiempo anterior y lo intentarán de nuevo. De esta manera, se va reduciendo la probabilidad de nuevas colisiones.

Debemos recordar que el canal es único y por lo tanto todas las estaciones tienen que compartirlo. Sólo puede estar una estación transmitiendo en cada momento, sin embargo pueden estar recibiendo el mensaje más de una.

> ***Nota:*** *La existencia de colisiones en una red no indica que exista un mal funcionamiento. Las colisiones están definidas dentro del protocolo Ethernet y no deben ser consideradas como una situación anómala. Sin embargo, cuando se produce una colisión el canal se desaprovecha porque ninguna estación logra transmitir en ese momento. Debemos tratar de reducir el número de colisiones que se producen en una red. Esto se consigue separando grupos de ordenadores mediante un switch o un router. Podemos averiguar las colisiones que se producen en una red observando el correspondiente LED de nuestro hub.*

Direcciones físicas

¿Cómo sabe una estación que un mensaje es para ella? Está claro, que hay que distinguir unas estaciones de otras utilizando algún identificador. Esto es lo que se conoce como *direcciones físicas*.

Los adaptadores Ethernet tienen asignada una dirección de 48 bits de fábrica que no se puede variar. Los fabricantes nos garantizan que no puede haber dos tarjetas de red con la misma dirección física. Si esto llegase a ocurrir dentro de una misma red la comunicación se volvería imposible. Los tres primeros bytes corresponden al fabricante (no puede haber dos fabricantes con el mismo identificador) y los tres últimos al número de serie (no puede haber dos tarjetas del mismo fabricante con el mismo número de serie). Por ejemplo,

5D:1E:23:10:9F:A3

Los bytes 5D:1E:23 identifican al fabricante y los bytes 10:9F:A3 al número de serie del fabricante 5D:1E:23

> ***Nota:*** *Los comandos* **ipconfig / all |more** *y* **winipcfg** *muestran la dirección física de nuestra tarjeta de red Ethernet. Observe que estos comandos pueden recoger también información relativa al adaptador virtual "PPP Adapter" (se corresponde con el módem o adaptador RDSI) además de la referente a la tarjeta de red real.*

No todas las direcciones representan a máquinas aisladas, algunas de ellas se utilizan para enviar

mensajes de multidifusión. Esto es, enviar un mensaje a varias máquinas a la vez o a todas las máquinas de la red. Ethernet permite que el mismo mensaje pueda ser escuchado por más de una máquina a la vez.

Formato de la trama

La comunicación entre una estación y otra a través de una red Ethernet se realiza enviando tramas Ethernet. El mensaje que se quiere transmitir se descompone en una o más tramas con el siguiente formato:

8 bytes	6 bytes	6 bytes	2 bytes	64-1500 bytes	4 bytes
Preámbulo	Dirección física destino	Dirección física origen	Tipo de trama	Datos de la trama	CRC

Las *direcciones origen* y *destino* son las direcciones físicas de los adaptadores de red de cada ordenador. El campo *Tipo de trama* indica el formato de los datos que se transfieren en el campo *Datos de la trama*. Por ejemplo, para un datagrama IP se utiliza el valor hexadecimal de 0800 y para un mensaje ARP el valor 0806. Todos los mensajes (*datagramas*) que se envíen en la capa siguiente irán encapsulados en una o más tramas Ethernet utilizando el campo *Datos de la trama*. Y esto mismo es aplicable para cualquier otro tipo de red distinta a Ethernet. Como norma general, cada mensaje que transmite una capa se coloca en el campo datos de la capa anterior. Aunque es muy frecuente que el mensaje no quepa en una sola trama y se utilicen varias.

Velocidades

Ethernet puede funcionar a tres velocidades: 10 Mbps, 100 Mbps (*FastEthernet*) y 1 Gbps (1000 Mbps). 10 Mbps es la velocidad para la que se diseñó originalmente el estándar Ethernet. Sin embargo, esta velocidad se ha mejorado para adaptarse a las crecientes exigencias de las redes locales. La velocidad de 100 Mbps es actualmente la más utilizada en la empresa. Las redes a 1 Gbps están comenzado a ver la luz en estos momentos por lo que tardarán un tiempo en implantarse en el mercado (los precios son todavía muy altos).

Para crear una red que trabaje a 10 Mbps es suficiente con utilizar cable coaxial o bien, cable par trenzado de categoría 3 o superior. Sin embargo, es recomendable utilizar cables par trenzado de categoría 5 y concentradores con velocidades mixtas 10/100 Mbps. De esta forma, en un futuro se podrán ir cambiando gradualmente los adaptadores de 10 Mbps por unos de 100 Mbps sin necesidad de instalar nuevo cableado.

La mejor opción actualmente para redes nuevas es *FastEthernet*. Para conseguir velocidades de 100 Mbps es necesario utilizar cable par trenzado con una categoría mínima de 5, un concentrador que soporte esta velocidad y tarjetas de red de 100 Mbps. Generalmente, los cables UTP cumplen bien con su función pero en situaciones concretas que requieran el máximo rendimiento de la red o existan muchas interferencias, puede ser necesario un cableado STP.

Tipos de adaptadores

La siguiente tabla resume los principales tipos de adaptadores Ethernet en función del cableado y la velocidad de la red. (T se utiliza para par trenzado, F para fibra óptica y X para *FastEthernet*).

	10Base5	10Base2	10BaseT	10BaseFP	100BaseTX	100BaseFX
Cableado	Coaxial		Par trenzado	Par de fibra óptica	Par trenzado	2 fibras ópticas
Velocidad	10 Mbps				100 Mbps	
Topología	Bus		Estrella			
Longitud máxima segmento	500 m	185 m	100 m	500 m	100 m	100 m
Nodos por segmento	100	30	2 (un extremo es el hub y el otro el ordenador)			

Los adaptadores pueden ser compatibles con varios de los estándares anteriores dando lugar a numerosas combinaciones. Sin embargo, lo habitual es encontrar en el mercado tarjetas de red de tan sólo estos dos tipos:

- *Tarjetas de red combo*. Tienen 2 conectores, uno para cable coaxial y otro para RJ45. Su velocidad máxima es de 10 Mbps por lo que soportan 10Base2 y 10BaseT. La tarjeta de red RTL8029 del fabricante Realtek pertenece a este tipo. Este grupo de tarjetas de red tienden a desaparecer (al igual que el cable coaxial).

- *Tarjetas de red 10/100*. Tienen sólo conector para RJ45. Se adaptan a la velocidad de la red (10 Mbps o 100 Mbps). Son compatibles con 10BaseT y 100BaseT. Como ejemplos de este tipo se encuentran las tarjetas Realtek RTL8139 y 3COM 3C905.

3.2 Protocolos de las capas de red y transporte

Los protocolos que vamos a describir a continuación no se preocupan por el medio de transmisión: dan por hecho que existe un protocolo de la capa de acceso al medio que se encarga del envío y recepción de los paquetes a través del medio de transmisión. Para su funcionamiento requieren alguno de los protocolos que hemos estudiado en el apartado anterior.

IPX/SPX

La familia de protocolos IPX/SPX (*Internetwork Packet Exchange / Sequential Packet Exchange*, intercambio de paquetes entre redes / intercambio de paquetes secuenciales) fue desarrollada por Novell a principios de los años 80. Gozó de gran popularidad durante unos 15 años si bien actualmente ha caído en desuso. Estos protocolos fueron creados como parte del sistema operativo de red Novell NetWare. En un principio fueron protocolos propietarios aunque más adelante se comenzaron a incorporar a otros sistemas operativos: Windows los incluye con los nombres de *Protocolo compatible con IPX/SPX* o *Transporte compatible NWLink IPX/SPX* según las versiones.

IPX/SPX es *enrutable*: hace posible la comunicación entre ordenadores pertenecientes a redes distintas interconectadas por encaminadores (*routers*). Los principales protocolos de IPX/SPX son, como su nombre indica, IPX y SPX. El primero pertenece a la capa de red y se encarga del envío de los paquetes (fragmentos de mensajes) a través de las redes necesarias para llegar a su destino. SPX pertenece a la capa de transporte: gestiona el envío de mensajes completos entre los dos extremos de la comunicación.

La estructura de protocolos IPX/SPX se corresponde en gran medida con TCP/IP. Su configuración es más sencilla que en TCP/IP aunque admite menos control sobre el direccionamiento de la red. El identificador de cada puesto en la red es un número de 6 bytes, que coincide con la dirección física de su adaptador, seguido de un número de 6 bytes, que representa la dirección de la red. Por ejemplo: 44.45.EA.54.00.00:4C.34.A8.59 (nodo:red).

AppleTalk

Es el protocolo propietario de Apple utilizado para interconectar ordenadores Macintosh. Es un protocolo enrutable. El identificador de cada puesto es un número de 1 byte y el de cada red, un número de 2 bytes. Por ejemplo, "50.8" representa el ordenador 8 de la red 50. Si el número de puestos en una red es superior a 253 hosts, se utilizan varios números de redes contiguos en lugar de sólo uno. Por ejemplo, la red "100-101" dará cabida a 506 hosts. Un host conectado a la red "100-101" tendrá una dirección de la forma "100.*x*". En la terminología de Apple, una red se conoce como una *zona*.

NetBEUI

NetBEUI (*NetBIOS Extended User Interface*, interfaz de usuario extendida para NetBIOS) es un protocolo muy sencillo que se utiliza en redes pequeñas de menos de 10 ordenadores que no requieran salida a Internet. Su funcionamiento se basa en el envío de difusiones a todos los ordenadores de su red. Sus difusiones no atraviesan los encaminadores a no ser que estén configurados para dejar pasar este tráfico: es un protocolo no enrutable.

La ventaja de este protocolo es su sencillez de configuración: basta con instalar el protocolo y asignar un nombre a cada ordenador para que comience a funcionar. Su mayor desventaja es su ineficiencia en redes grandes (se envían excesivas difusiones).

Actualmente es un protocolo exclusivo de las redes Microsoft. Fue diseñado para ofrecer una interfaz sencilla para NetBIOS (este protocolo trabaja en la capa de aplicación, lo estudiaremos cuando veamos las redes en Windows 98).

TCP/IP

TCP/IP (*Transport Control Protocol / Internet Protocol*, protocolo de control de transporte / protocolo de Internet) es el estándar en las redes. Fue diseñado por el Departamento de Defensa de los Estados Unidos a finales de los años 70 para utilizarse en una red resistente a bombas: aunque se destruyese alguna línea de comunicación o encaminador, la comunicación podría seguir funcionando por rutas alternativas. Lo sorprendente de TCP/IP es que no fue pensado para resistir el espionaje: los protocolos originales transmiten las contraseñas y datos sin codificación alguna.

TCP/IP es el protocolo de Internet (en realidad, es una familia de protocolos). En la actualidad es la elección recomendada para casi todas las redes, especialmente si la red tiene salida a Internet. En el resto del curso nos centraremos exclusivamente en las redes TCP/IP.

Los dos protocolos principales de TCP/IP son IP, perteneciente a la capa de red, y TCP, perteneciente a la

capa de transporte. Estos protocolos se estudian detalladamente en el *Curso de protocolos TCP/IP*. El identificador de cada puesto es la *dirección IP*. Una dirección IP es un número de 4 bytes. Por ejemplo: 194.142.78.95. Este número lleva codificado la dirección de red y la dirección de host (*ver máscara de subred*). Las direcciones IP se clasifican en:

- *Direcciones públicas*. Son visibles desde todo Internet. Se contratan tantas como necesitemos. Son las que se asignan a los servidores de Internet que sirven información 24 horas al día (por ejemplo, un servidor web).
- *Direcciones privadas*. Son visibles sólo desde una red interna pero no desde Internet. Se utilizan para identificar los puestos de trabajo de las empresas. Se pueden utilizar tantas como se necesiten; no es necesario contratarlas.

3.3 Familia de protocolos TCP/IP

(Ver Curso de protocolos TCP/IP)