

# INTRODUCCIÓN

---

El desarrollo de la Informática ha estado muy ligado en estos últimos años a la expansión de las redes de comunicaciones. Un ordenador aislado tiene una gran capacidad de cálculo, pero sus posibilidades se van a ver muy mermadas si no dispone de una conexión para el intercambio de información con otros equipos.

Las redes locales son infraestructuras informáticas que facilitan el trabajo de los usuarios en las empresas, sobre todo cuando éste se desempeña en entornos donde es muy importante el intercambio de información entre personas, grupos o departamentos. Para que una red local de estas características funcione en las mejores condiciones, es imprescindible disponer del equipamiento necesario, que fundamentalmente está formado por cableado, equipos electrónicos y programas. Además, también es necesario realizar una serie de tareas de instalación, configuración y mantenimiento de esos equipos y programas. Este libro está dedicado fundamentalmente a explicar los equipos necesarios y las operaciones de instalación y configuración que hay que llevar a cabo. También explica las técnicas utilizadas para detectar y resolver problemas de funcionamiento.

El capítulo 1 de este libro está dedicado a introducir el concepto de red local, sus características más importantes y los estándares más utilizados. El capítulo 2 describe los elementos que forman parte de una red local, tanto el cableado como los equipos electrónicos. El capítulo 3 explica con más detalle el funcionamiento de los programas encargados de controlar las comunicaciones. En el capítulo 4 se explican los procedimientos a seguir para configurar los programas de comunicación que se utilizan en las redes locales. En el capítulo 5 se describen los procedimientos utilizados para la verificación y prueba de los elementos que forman parte de la red local. Por su parte, en el capítulo 6 se enumeran los tipos de incidencias que se pueden producir durante el funcionamiento de una red local. En el capítulo 7 se explican las herramientas de diagnóstico y los procesos de gestión de incidencias. A continuación, en el capítulo 8 se explican los procedimientos y las herramientas empleadas en la comprobación del cableado. Finalmente, en el capítulo 9 se explican las técnicas empleadas para detectar y diagnosticar incidencias relacionadas con el funcionamiento de los protocolos de alto nivel.



## ARQUITECTURA DE REDES DE ÁREA LOCAL

---

Desde el punto de vista de la Informática, una red de comunicación es un sistema que permite la comunicación entre los ordenadores que se encuentran conectados a ella. La red está formada por los siguientes elementos: los terminales (ordenadores), el medio de transmisión, los elementos de interconexión, los adaptadores de comunicación y los protocolos que funcionan en ellos.

Una red de comunicación ofrece una serie de **servicios**, es decir, pone a disposición de los usuarios un conjunto de funciones que pueden utilizar. Así mismo, esos servicios se basan en una serie de **protocolos**, que son las normas que se deben seguir para que las comunicaciones se realicen correctamente.

Todas las redes de comunicación se clasifican atendiendo al territorio que abarcan: redes locales (limitadas a uno o varios edificios), redes de área metropolitana (limitadas a una ciudad) y redes de área extensa (que abarcan territorios extensos como estados, continentes o incluso todo el planeta).

En este capítulo se explican los conceptos fundamentales sobre redes locales, además de las características más importantes que las definen, que son: la topología, el control de acceso al medio y los protocolos de comunicaciones.

---

### 1.1 CLASIFICACIÓN DE LAS REDES EN FUNCIÓN DEL TERRITORIO QUE ABARCAN

---

La localización geográfica de la red es un factor a tener en cuenta a la hora de diseñarla y montarla. No es lo mismo montar una red para un aula de informática que interconectar las oficinas de dos sucursales que la misma empresa tiene instaladas en diferentes países. Sin embargo, esta clasificación muchas veces resulta confusa o arbitraria, ya que se basa en criterios vagamente definidos:

- **Subred o segmento de red:** un segmento de red está formado por un conjunto de estaciones que comparten el mismo medio de transmisión (normalmente están conectadas con el mismo cable). Gracias a esta característica, es posible reducir el

coste de la instalación de la red. El segmento está limitado en espacio al departamento de una empresa, un aula de informática, etc. Se considera al segmento como la red de comunicación más pequeña y todas las redes de mayor tamaño están constituidas por la unión de varios segmentos de red.

- **Red de área local** (*Local Area Network* o **LAN**): una LAN es un término vago que se refiere a uno o varios segmentos de red conectados mediante dispositivos especiales. Normalmente se le da este calificativo a las redes cuya extensión no sobrepasa el mismo edificio donde está instalada (o la misma habitación).
- **Red de campus**: una red de campus se extiende entre varios edificios dentro de un mismo polígono industrial que se conectan generalmente a un tendido de cable principal. Normalmente, la empresa es propietaria del terreno por el que se extiende el cable y tiene libertad para poner cuantos cables sean necesarios sin tener que solicitar permisos especiales.
- **Red de área metropolitana** (*Metropolitan Area Network* o **MAN**): generalmente, una MAN está confinada dentro de una misma ciudad y se halla sujeta a regulaciones locales. Puede constar de varios recursos públicos o privados, como el sistema de telefonía local, sistemas de microondas locales o cables enterrados de fibra óptica. Una empresa local construye y mantiene la red, y la pone a disposición del público. Puede conectar sus redes a la MAN y utilizarla para transferir información entre redes de otras ubicaciones de la empresa dentro del área metropolitana.
- **Red de área extensa** (*Wide Area Network* o **WAN**) y **redes globales**: las WAN y redes globales abarcan varias ciudades, regiones o países. Los enlaces WAN son ofrecidos generalmente por empresas de telecomunicaciones públicas o privadas que utilizan enlaces de microondas, fibra óptica o vía satélite. Actualmente, el método empleado para conectar una WAN utiliza líneas telefónicas estándar o líneas telefónicas modificadas para ofrecer un servicio más rápido.

---

## 1.2 CARACTERÍSTICAS DE UNA RED LOCAL

---

Según la *Unión Internacional de Telecomunicaciones*, se define formalmente **telecomunicación** como toda transmisión, emisión o recepción de signos, señales, imágenes, sonidos o informaciones de cualquier tipo que se transmiten por hilos, medios ópticos, radioeléctricos u otros sistemas electromagnéticos.

Por su parte, una **red de transmisión de datos** es una estructura formada por determinados medios **físicos** (dispositivos reales) y **lógicos** (programas de transmisión y control) desarrollada para satisfacer las necesidades de comunicación de una determinada zona geográfica. Se trata, pues, de un soporte que permite la conexión de diversos equipos

informáticos (o cualquier otro dispositivo electrónico) con el objetivo de suministrarles la posibilidad de que intercambien informaciones.

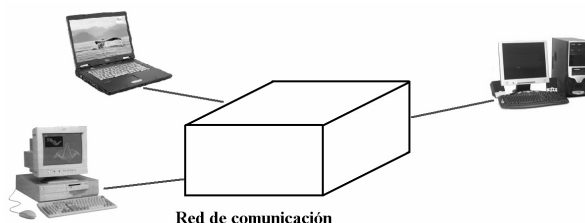


Figura 1.1. Red de comunicación de datos. Diagrama simplificado

La señal recibida por el receptor es la suma de la señal enviada por el emisor más una componente de ruido que se suma durante su circulación a través de la red. Por lo tanto, habrá que introducir mecanismos de detección y corrección de errores. En la mayoría de los casos, todos los errores producidos no pueden ser corregidos, pero sí la mayoría de ellos. El límite se sitúa teniendo en cuenta el máximo aceptable por el usuario y el coste de la instalación de la red.

En general, una red local está formada por los siguientes elementos (véase la figura 1.1):

- **Terminales:** son los equipos que se comunican, como ordenadores, teléfonos, etc. Estos determinan la naturaleza de la información que va a tener que manejar la red (voz, datos, etc.).
- **Dispositivos de red:** se corresponde con el conjunto de elementos físicos que hacen posible la comunicación entre el terminal emisor y el receptor. Estos dispositivos son:
  - **Canal de comunicación:** es el medio por el que circula la información. Habitualmente, suele tener la forma de un cable o el aire (en las comunicaciones inalámbricas).
  - **Elementos de interconexión:** son los encargados de interconectar todos los terminales de la red y también trabajan para seleccionar el mejor camino por el que circulará la información (en caso de que exista más de un camino). En las redes locales, los dispositivos que más comúnmente se utilizan para interconectar todos los equipos son los concentradores de cableado y los conmutadores (véase la figura 1.2).
  - **Adaptadores de red:** son los encargados de convertir el formato de información de los terminales (normalmente en forma de señales eléctricas) en el formato utilizado por la red de comunicación (señales eléctricas, ondas de radio, etc.).

- **Programas de red:** son todos los programas que permiten controlar el funcionamiento de la red, para hacerla más fiable. Las primeras redes de ordenadores se diseñaron pensando en los dispositivos y dejando en un segundo plano los programas; hoy en día el *software* de redes es un elemento muy importante y está altamente estructurado.

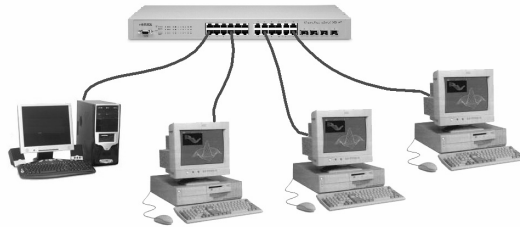


Figura 1.2. Ejemplo simplificado de conexión de equipos en redes locales. Aquí se utiliza un equipo especial que recibe todas las conexiones, denominado concentrador de cableado o conmutador (su aspecto externo es casi idéntico)

---

## 1.3 ARQUITECTURAS DE REDES DE ÁREA LOCAL

---

Como se explica en el apartado anterior, el *software* de red es el conjunto de programas encargado de gestionar la red, controlar su uso, realizar detección y corrección de errores, etc. Al igual que un sistema operativo realiza una gestión eficiente de los recursos de una máquina de cara a su utilización por los usuarios y las aplicaciones, el *software* de red realiza esta misma tarea de cara a los recursos físicos (*hardware*) de la red.

La **arquitectura de una red** viene definida por tres características fundamentales, que dependen de la tecnología que se utilice en su construcción:

- **Topología:** la topología de una red es la organización de su cableado, ya que define la configuración básica de la interconexión de estaciones y, en algunos casos, el camino de una transmisión de datos sobre el cable.
- **Método de acceso a la red:** todas las redes que poseen un medio compartido para transmitir la información necesitan ponerse de acuerdo a la hora de enviar información, ya que no pueden hacerlo a la vez. Si dos estaciones transmiten a la vez en la misma frecuencia, la señal recogida en los receptores será una mezcla de las dos. Para las redes que no posean un medio compartido, el método de acceso al cable es trivial y no es necesario llevar a cabo ningún control para transmitir.
- **Protocolos de comunicaciones:** son las reglas y procedimientos utilizados en una red para realizar la comunicación. Esas reglas tienen en cuenta el método utilizado para corregir errores, establecer una comunicación, etc.

Existen diferentes niveles de protocolos. Los **protocolos de alto nivel** definen cómo se comunican las aplicaciones (programas de ordenador) y los **protocolos de bajo nivel** definen cómo se transmiten las señales por el cable. Entre los protocolos de alto y bajo nivel, hay protocolos intermedios que realizan otras funciones, como establecer y mantener sesiones de comunicaciones y controlar las transmisiones para detectar errores. Observe que los protocolos de bajo nivel son específicos del tipo de cableado utilizado para la red.

### 1.3.1 Topologías básicas

---

La topología de una red es la forma en la que se interconectan los diferentes equipos entre sí. Según esta clasificación, podemos tener los siguientes tipos de redes:

- **Malla:** es una interconexión total de todos los nodos, con la ventaja de que, si una ruta falla, se puede seleccionar otra alternativa. Este tipo de red es más costoso, ya que hace falta más cable.

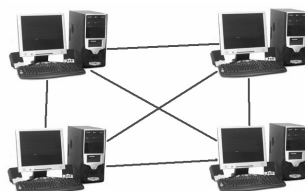


Figura 1.3. Red con topología en malla

- **Estrella:** los equipos se conectarán a un nodo central con funciones de distribución, conmutación y control. Si el nodo central falla, quedará inutilizada toda la red; si es un nodo de los extremos, sólo éste quedará aislado. Normalmente, el nodo central no funciona como estación, sino que más bien suele tratarse de dispositivos específicos.

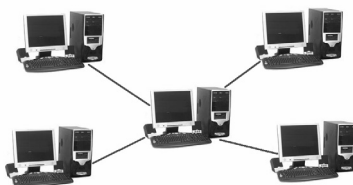


Figura 1.4. Red con topología en estrella

- **Árbol:** es una forma de conectar nodos como una estructura jerarquizada. Esta topología es la menos utilizada, y se prefiere la topología irregular, ya que el fallo de un nodo o un enlace deja a conjuntos de nodos incomunicados entre sí. Sin embargo, se utiliza ampliamente en redes de telefonía, donde los enlaces intermedios son centralitas locales y regionales.

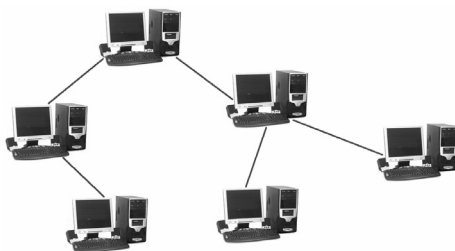


Figura 1.5. Red con topología en árbol

- **Anillo:** todos los nodos están conectados a una única vía con sus dos extremos unidos. Al igual que ocurre con la topología en *bus*, si falla algún enlace, la red deja de funcionar completamente.



Figura 1.6. Red con topología en anillo

- **Intersección de anillo:** varios anillos conectados por nodos comunes. El inconveniente de esta topología es que, si fallan los nodos comunes de los anillos, toda la red dejará de funcionar.



Figura 1.7. Red con topología en intersección de anillo

- **Bus:** utiliza un único cable para conectar los equipos. Esta configuración es la que requiere menos cableado, pero tiene el inconveniente de que, si falla algún enlace, todos los nodos quedan aislados (debido a que este cable se rompe y queda abierto).



Figura 1.8. Red con topología en bus



- **Irregular:** cada nodo debe estar conectado, como mínimo, por un enlace, pero no existen más restricciones. Esta topología es la más utilizada en redes que ocupan zonas geográficas amplias. Esta topología permite la búsqueda de rutas alternativas cuando falla alguno de los enlaces.

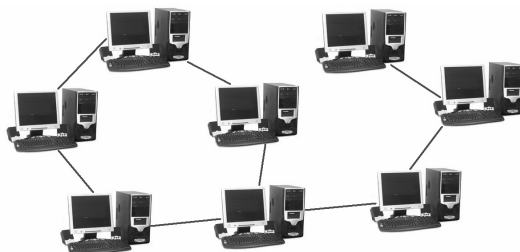


Figura 1.9. Red con topología irregular

La topología de una red de comunicación tiene que ver con la manera en la que están conectados los equipos, lo que también determina la forma en la que la información es enviada por ella. Por ejemplo, en una topología en bus o anillo, la información se envía a todos los equipos, mientras que en otras topologías la información se puede enviar solamente al destinatario, quizá atravesando equipos intermedios. En una topología en estrella, por ejemplo, el equipo que funciona en el centro de la estrella debe saber dónde están conectados el resto de ordenadores, porque debe decidir por dónde enviar la información para que llegue al destinatario correcto. Sin embargo, para simplificar los mecanismos de comunicación, ese equipo simplemente puede enviar los mensajes que le llegan a todos los equipos, por lo que la topología de la red sigue siendo en estrella, aunque el envío de los mensajes se realiza como si fuera un bus. En el capítulo 2 se explica cómo determinados tipos de dispositivos de interconexión de redes pueden hacer que la comunicación se realice de una forma distinta a como está definida la topología de la red.

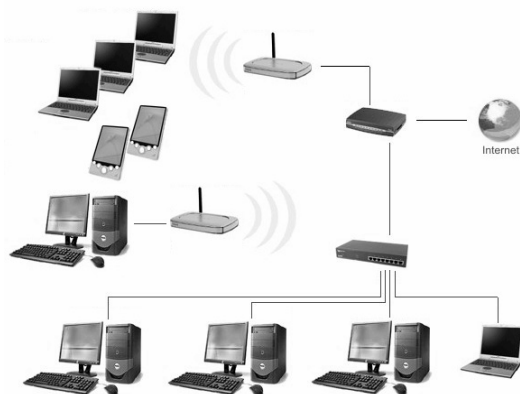


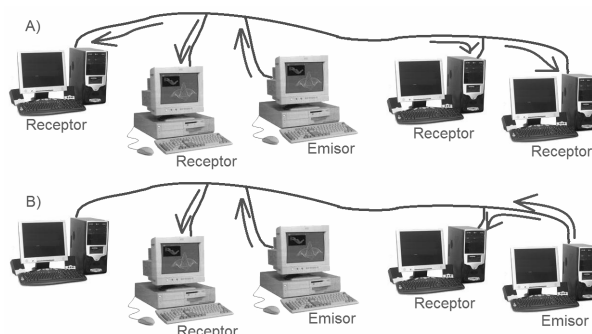
Figura 1.10. Ejemplo de topología de red real. Las redes reales pueden llegar a tener topologías bastante complejas ya que mezclan estructuras de diferentes tipos, añadiendo además la complejidad que suponen las redes inalámbricas que no usan cables

### 1.3.2 Topología física y lógica

Como se explica en el apartado 1.3.1, la topología de la red es la forma en la que se conectan los diferentes equipos que la componen. A esta topología también se le conoce como **topología física**, por que es la forma en la que está físicamente organizado el cableado de la red. Esta topología física es la que determina los protocolos que son necesarios para su correcto funcionamiento (existencia de posibles rutas alternativas, control de la congestión, etc.).

Como contrapartida a la topología física, en una red también existe una **topología lógica**, que determina cómo se transmite la información. Habitualmente, la topología lógica coincide con la topología física porque depende de ella, pero en algunos casos una red con un determinado tipo de topología física no tiene por qué tener el mismo tipo de topología lógica. Esto dependerá del comportamiento de los diferentes dispositivos de interconexión a la hora de transmitir la información desde el origen al destino.

Por ejemplo, una red con una topología física en bus como la de la figura 1.11 tendrá también una topología lógica en bus si la información se transmite también como un bus. Es decir, si un equipo envía un mensaje y éste es recibido por todos los equipos que están conectados a ella, entonces podemos afirmar que la topología lógica de esa red es en bus. Por el contrario, si la información que transmite un equipo es enviada al que tiene más cerca y éste, a su vez, la envía al siguiente y así sucesivamente hasta el destino, entonces debemos afirmar que la topología lógica de la red es en anillo, aunque los equipos estén conectados formando un bus.



*Figura 1.11. Ejemplos de dos redes con la misma topología física pero distinta topología lógica. Ambas tienen una topología física en bus, pero mientras que A) tiene una topología lógica en bus (porque todos los equipos comparten el mismo medio de transmisión y, por lo tanto, reciben los mismos mensajes), la red B) tiene una topología lógica en anillo, porque el mensaje que transmite un equipo lo envía sólo al siguiente*

Actualmente, la mayoría de las redes locales cableadas utilizan una topología física en estrella (véase la figura 1.2). Esto significa que todos los equipos se conectan a otro equipo que hace las veces de centro de la estrella. Este equipo especial no suele ser un ordenador porque necesitaría disponer de muchas conexiones y necesitaría estar encendido todo el

tiempo, lo que supone un coste muy elevado. En su lugar, se utilizan equipos especiales cuya única misión consiste en conectar todos los ordenadores y redirigir los mensajes desde el origen al destino, como si se tratase de una centralita telefónica en miniatura. Estos equipos habitualmente son concentradores de cableado o conmutadores y se explican con más detalle en el capítulo 2.

La forma en la que un concentrador de cableado o un conmutador distribuyen los mensajes a través de la red determina su topología lógica. Esta topología lógica puede ser (véase la figura 1.12):

- **En bus:** cuando el dispositivo recibe un mensaje, lo envía por todos los puertos que tiene menos por el que llegó.
- **En anillo:** cuando el dispositivo recibe un mensaje por un puerto, lo envía por el siguiente.
- **En estrella:** el dispositivo envía el mensaje solamente por el puerto donde se encuentra conectado el equipo destinatario.

Actualmente, las redes locales se montan utilizando conmutadores que tienen una topología lógica en estrella, ya que envían los mensajes solamente por los puertos donde están conectados los equipos destinatarios. Este funcionamiento es más eficiente, pero tiene el inconveniente de que los conmutadores tienen que saber en todo momento los equipos que están conectados en cada puerto. Actualmente, esto ya no es un problema gracias a la evolución de la tecnología, pero hasta no hace muchos años estos dispositivos eran demasiado caros y resultaba más rentable utilizar concentradores con topología lógica en bus o anillo.

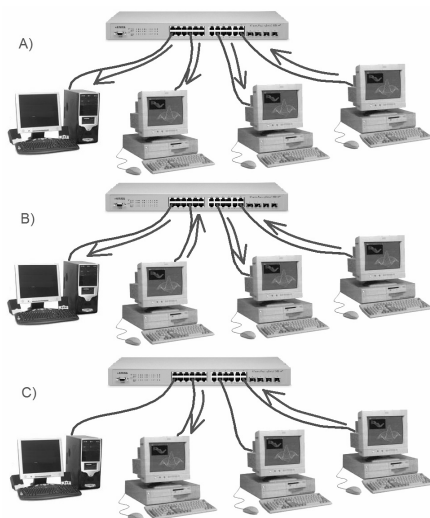


Figura 1.12. Ejemplos de redes con la misma topología física en estrella pero distinta topología lógica. En A) la topología lógica es un bus, mientras que en B) es un anillo y en C) es una estrella. Obsérvese que en los casos B) y C) las redes son más eficientes porque permiten varias comunicaciones simultáneas, ya que el medio no es compartido como en A)

### 1.3.3 Método de acceso al cable

---

En los apartados anteriores se ha puesto de manifiesto que muchas redes locales trabajan con un medio compartido, es decir, un único canal por el que circulan los mensajes de todos los equipos conectados. Estas redes tienen una topología lógica en bus, enviando los mensajes a todos los equipos o utilizan un medio de difusión como es el aire (en las redes locales inalámbricas). En este tipo de redes, al existir un único canal por el que se transmite la información y es enviada en una frecuencia determinada, no es posible o por lo menos deseable que dos equipos transmitan a la vez. Si esta situación se produce, la información que envían se mezcla e interfiere entre sí, con el resultado de que los mensajes son completamente ilegibles y deben ser reenviados de nuevo para que no se pierdan. Situaciones como ésta, conocida comúnmente como **colisión**, se produce en las comunicaciones inalámbricas que utilizan la misma frecuencia de transmisión, por ejemplo cuando se utilizan dispositivos *walkie-talkie*.

Por lo tanto, en las redes de difusión, debe existir algún mecanismo que controle el orden de transmisión de los interlocutores. Mediante este mecanismo de control, se pueden evitar o reducir en la medida de lo posible las situaciones de colisión. Una colisión no solamente hace que los mensajes se pierdan, sino que también puede reducir considerablemente la capacidad de transmisión de una red en la que los equipos tienen que reenviar de nuevo la información perdida.

Existen muchos métodos de control de acceso al medio que se utilizan en las redes locales actuales. Algunos de ellos evitan que se produzcan colisiones, mientras que otros no las evitan completamente pero consiguen que se puedan reducir drásticamente. En el apartado 3.4 del capítulo 3 se explican con detalle algunos mecanismos de control de acceso al medio muy utilizados en redes locales.

### 1.3.4 Protocolos de comunicaciones

---

Las redes de comunicaciones se diseñan para ofrecer una serie de servicios a los usuarios. En las redes locales, el servicio más importante es el intercambio de información, ya sea en forma de archivos de texto o imagen, mensajes instantáneos, correo electrónico, vídeo en tiempo real, etc.

En una red local, para que la información se transmita correctamente hasta el destino, es necesario que exista un medio por el que ésta debe circular, además de una serie de dispositivos que se encargan de encauzarla y realizar las conversiones o traducciones que sean necesarias. Sin embargo, también es necesario que todos los equipos sigan una serie de normas para que la comunicación se pueda llevar a cabo correctamente y con fluidez.

Estas normas, aunque al principio puedan parecer algo extrañas o con poco sentido, las seguimos todos en una conversación normal entre personas, aunque nuestra costumbre nos haga olvidarnos de ellas mientras hablamos. Algunos ejemplos de estas normas son:

- Utilizar el mismo idioma en la conversación, para que todos los interlocutores interpreten correctamente la información.
- Cuando una persona está hablando, es recomendable dejar que termine antes de que otra empiece a hablar.
- Para evitar que una persona acapare la conversación, es recomendable seguir un turno de palabra.
- Si no se ha entendido algo, los interlocutores pueden solicitar que se repita esa parte de la conversación.

A las normas que deben respetarse en una comunicación se les denomina **protocolos**. Un protocolo de una red local establece las normas que se deben seguir para que un determinado servicio relacionado con ella se realice correctamente y sin fallos. Las normas que determina el protocolo pueden ser muy variadas, como la velocidad de transmisión, el tipo de información a enviar, el formato de los mensajes, etc.

Por ejemplo, podemos hacer la analogía con el sistema telefónico para establecer una conversación entre dos abonados. Para que la comunicación se realice convenientemente, el protocolo determina que hay que seguir los siguientes pasos:

1. Descolgar el teléfono.
2. Comprobar si hay línea. Si no hay, colgar y volver al paso 1.
3. Marcar el número del otro usuario.
4. Esperar tono.
5. Si el tono es "comunicando", colgar y volver al paso 1.
6. Si da más de 6 tonos y no contesta, ir al paso 8.
7. Hablar cuando el otro usuario conteste.
8. Colgar.

Si no se siguen las reglas del protocolo estrictamente, la comunicación no se realizará en condiciones. Resulta absurdo que el usuario comience a hablar antes de tiempo porque la otra persona no oíría la conversación; así mismo, si cuelga de forma precipitada, también se perderá una parte de la conversación.

Este ejemplo de protocolo resulta a primera vista muy simple y todos nosotros estamos acostumbrados a seguirlo. En comunicaciones de datos, los protocolos empleados son más complejos porque deben ser capaces de corregir errores; en el caso de una comunicación normal, si el usuario no entiende, sólo tiene que decir: *¿Cómo dices?*, o,

*¿puedes repetir?* Sin embargo, para ambos casos, la idea de base es la misma. En muchas ocasiones no está clara la división entre protocolo y red, ya que existen redes de transmisión que utilizan sus propios protocolos.

Aunque a primera vista parezca que el diseño de un sistema de comunicación parece simple, cuando se aborda resulta mucho más complejo, ya que es necesario resolver una serie de problemas. Estos problemas se resuelven en el diseño de la arquitectura de la red a través de los protocolos, teniendo en cuenta la topología y el control de acceso al medio, que son los que determinarán las características de la red local. Algunos de los problemas más importantes a los que se enfrentan los diseñadores de redes locales son:

- **Encaminamiento:** cuando existen diferentes rutas posibles entre el origen y el destino (si la red tiene una topología de malla o irregular), se debe elegir una de ellas (normalmente, la más corta o la que tenga un tráfico menor). Sin embargo, en una red local que utiliza un medio compartido, esta cuestión es trivial, porque sólo existe un camino posible entre un origen y un destino cualesquiera.
- **Direccionamiento:** puesto que una red normalmente tiene muchos ordenadores conectados, algunos de los cuales tienen múltiples procesos (programas), se requiere un mecanismo para que un proceso en una máquina especifique con quién quiere comunicarse. Como consecuencia de tener varios destinos, se necesita alguna forma de direccionamiento que permita determinar un destino específico.
- **Acceso al medio:** en las redes donde existe un medio de comunicación de difusión (un único medio compartido, debe existir algún mecanismo que controle el orden de transmisión de los interlocutores. De no ser así, todas las transmisiones se interfieren y no es posible llevar a cabo una comunicación en óptimas condiciones.
- **Saturación del receptor:** esta cuestión suele plantearse en todos los niveles de la arquitectura y consiste en que un emisor rápido pueda saturar a un receptor lento. En determinadas condiciones, el proceso en el otro extremo necesita un tiempo para procesar la información que le llega. Si ese tiempo es demasiado grande en comparación con la velocidad con la que le llega la información, será posible que se pierdan datos. Una posible solución a este problema consiste en que el receptor envíe un mensaje al emisor indicándole que está listo para recibir más datos.
- **Mantenimiento del orden:** algunas redes de transmisión de datos desordenan los mensajes que envían, de forma que, si los mensajes se envían en una secuencia determinada, no se asegura que lleguen en esa misma secuencia. Para solucionar esto, el protocolo debe incorporar un mecanismo que le permita volver a ordenar los mensajes en el destino. Este mecanismo puede ser la numeración de los fragmentos, por ejemplo.
- **Control de errores:** todas las redes de comunicación de datos transmiten la información con una pequeña tasa de error, que en ningún caso es nula. Esto se

debe a que los medios de transmisión son imperfectos. Tanto emisor como receptor deben ponerse de acuerdo a la hora de establecer qué mecanismos se van a utilizar para detectar y corregir errores, y si se va a notificar al emisor que los mensajes llegan correctamente.

- **Multiplexación:** en determinadas condiciones, la red puede tener tramos en los que existe un único medio de transmisión que, por cuestiones económicas, debe ser compartido por diferentes comunicaciones que no tienen relación entre sí. Así, el protocolo deberá asegurar que todas las comunicaciones que comparten el mismo medio no se interfieran entre sí.

Puesto que el diseño de un sistema de comunicación requiere de la resolución de muchos y complejos problemas, los protocolos de las redes locales se organizan en capas o niveles para reducir la complejidad de su diseño. Esta técnica se ha heredado de la metodología de programación consistente en dividir el problema en subproblemas más sencillos de tratar y en la programación modular ("Divide y vencerás"). Cada una de estas capas o subniveles (equivalente a un módulo) se construye sobre su predecesor (es decir, utiliza los servicios o funciones diseñados en él) y cada nivel es responsable de ofrecer servicios a niveles superiores.

Dentro de cada nivel de la arquitectura coexisten diferentes servicios. Así, los servicios de los niveles superiores pueden elegir cualquiera de los ofrecidos por las capas inferiores, dependiendo de la función que se quiera realizar. A la arquitectura por niveles también se le llama **jerarquía de protocolos**. Si los fabricantes quieren desarrollar productos compatibles, deberán ajustarse a los protocolos definidos para esa red. Por lo tanto, en una jerarquía de protocolos se siguen las siguientes reglas:

- Cada nivel dispone de un conjunto de servicios.
- Los servicios están definidos mediante protocolos estándares.
- Cada nivel se comunica solamente con el nivel inmediato superior y con el inmediato inferior.
- Cada uno de los niveles inferiores proporciona servicios a su nivel superior.

Cuando se comunican dos ordenadores que utilizan la misma arquitectura de red, los protocolos que se encuentran al mismo nivel de la jerarquía deben coordinar el proceso de comunicación. Por ejemplo, el nivel 2 de un equipo (transmitiendo, por ejemplo) coordina sus actividades con el nivel 2 del otro extremo (que se encargaría de recibir). Esto quiere decir que ambos deben ponerse de acuerdo y utilizar las mismas reglas de transmisión (es decir, el mismo protocolo).

En general, el nivel  $n$  de una máquina se comunica de forma indirecta con el nivel  $n$  homónimo de la otra máquina. Como se ha mencionado anteriormente, las reglas y convenciones usadas en esa comunicación se conocen como **protocolo de nivel  $n$** . A los elementos activos de cada capa se les llama **entidades** o **procesos** y son estos los que se

comunican mediante el uso del protocolo. Al grupo formado por las entidades o procesos en máquinas diferentes que están al mismo nivel se le llama **entidades pares** o **procesos pares**.

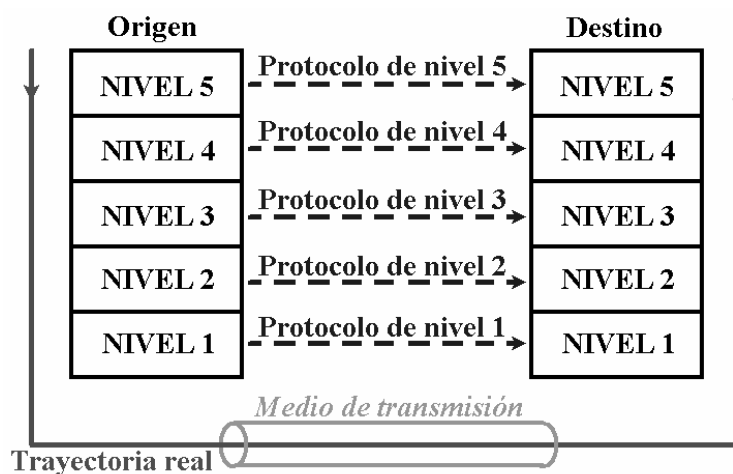


Figura 1.13. Diagrama simplificado de comunicación por niveles. Las líneas discontinuas representan la comunicación "virtual" entre los procesos pares, mientras que las líneas continuas indican la trayectoria real de la comunicación

El modelo de arquitectura por niveles necesita **información adicional** para que los procesos pares puedan comunicarse a un determinado nivel. Estos datos adicionales dependen del protocolo utilizado y sólo se conoce su verdadero significado a ese nivel; normalmente, los niveles inferiores los tratan como si fuera información propiamente dicha. A ese añadido se le llama generalmente **cabecera** o **información de control** y suele ir al principio y/o al final del mensaje.

### 1.3.5 Arquitecturas de redes de área local más usadas

En este apartado se explican algunas de las arquitecturas de redes locales que más se utilizan en la actualidad. Son muchas las arquitecturas de redes locales que se han utilizado a lo largo de la historia, pero solamente unas pocas se han convertido en normas reconocidas internacionalmente.

#### 1.3.5.1 TCP/IP

**TCP/IP** se suele confundir muchas veces con un protocolo de comunicaciones concreto, cuando, en realidad, es una compleja arquitectura de red que incluye varios de ellos, apilados por capas. Es, sin lugar a dudas, la más utilizada del mundo, ya que es la base de comunicación de Internet y también se utiliza ampliamente en muchas redes locales donde existen equipos con sistemas operativos Unix y GNU/Linux (aunque debido a su gran



utilización ha sido también implantado en otros sistemas como Microsoft Windows, como se explica en el apartado siguiente).

En el año 1973, el DoD (*Departamento de Defensa de Estados Unidos*) inició un programa de investigación para el desarrollo de tecnologías de comunicación de redes de transmisión de datos. El objetivo fundamental era desarrollar una red de comunicación que cumpliera las siguientes características:

- Que permita interconectar redes diferentes. Esto quiere decir que la red en general puede estar formada por tramos que usan tecnología de transmisión diferente.
- Que sea tolerante a fallos. El DoD deseaba una red que fuera capaz de soportar ataques terroristas o incluso alguna guerra nuclear sin perderse datos y manteniendo las comunicaciones establecidas.
- Que permita el uso de aplicaciones diferentes: transferencia de archivos, comunicación en tiempo real, etc.

Todos estos objetivos implicaron el diseño de una red con topología irregular donde la información se fragmentaba para seguir rutas diferentes hacia el destinatario. Si alguna de esas rutas fallaba repentinamente, la información podría seguir rutas alternativas. Así, surgieron dos redes distintas: una dedicada a la investigación, ARPANET, y otra de uso exclusivamente militar, MILNET.

El DoD permitió a varias universidades que colaboraran en el proyecto, y ARPANET se expandió gracias a la interconexión de esas universidades e instalaciones del Gobierno. Este modelo se nombró después como **arquitectura TCP/IP**, por las iniciales de sus dos protocolos más importantes. En 1980, TCP/IP se incluyó en Unix 4.2 de Berkeley y fue el protocolo militar estándar en 1983. En ese mismo año nació la red global Internet, que utiliza también esta arquitectura de comunicación. ARPANET dejó de funcionar en 1990.

Algunos de los motivos de la popularidad alcanzada por esta arquitectura son:

- Es independiente de los fabricantes y las marcas comerciales.
- Soporta múltiples tecnologías de redes.
- Es capaz de interconectar redes de diferentes tecnologías y fabricantes.
- Puede funcionar en equipos con cualquier sistema operativo instalado.
- Se ha convertido en estándar de comunicación en EEUU desde 1983.

La arquitectura de TCP/IP se construyó diseñando inicialmente los protocolos y después se creó la arquitectura completa. Por esta razón, a TCP/IP muchas veces se la califica como **pila de protocolos**.

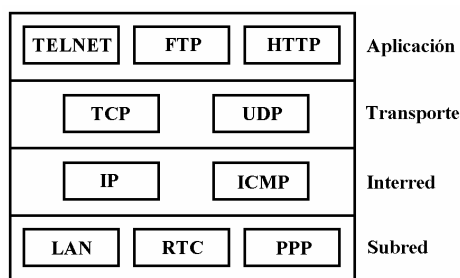


Figura 1.14. Protocolos de la arquitectura TCP/IP. Aquí aparecen algunos de los más importantes del modelo. Obsérvese que en el nivel de subred están definidos los protocolos de comunicación de algunas redes comerciales, como RTC (estándar de la red telefónica conmutada), el estándar de redes de área local IEEE 802 (se explica en el apartado 3.5 del capítulo 5), etc.

Obsérvese que TCP/IP tiene definidas cuatro capas y sus funciones son las siguientes:

- **Capa de subred:** el modelo no da mucha información de esta capa y solamente se especifica que debe existir algún protocolo que conecte la estación con la red. La razón fundamental es que, como TCP/IP se diseñó para su funcionamiento sobre redes diferentes, esta capa depende de la tecnología utilizada y no se especifica de antemano (véase el apartado 3.4 del capítulo 3).
- **Capa de interred:** esta capa es la más importante de la arquitectura y su misión consiste en permitir que las estaciones envíen información (**paquetes**) a la red y los hagan viajar de forma independiente hacia su destino. Durante ese viaje, los paquetes pueden atravesar redes diferentes y llegar desordenados. Esta capa no se responsabiliza de la tarea de ordenar de nuevo los mensajes en el destino. El protocolo más importante de esta capa se llama **IP** (*Internet Protocol* o *Protocolo de Interred*), aunque también existen otros protocolos.
- **Capa de transporte:** ésta cumple la función de establecer una conversación entre el origen y el destino, de igual forma que hace la capa de transporte en el modelo OSI. Puesto que las capas inferiores no se responsabilizan del control de errores ni de la ordenación de los mensajes, ésta debe realizar todo ese trabajo. Aquí también se han definido varios protocolos, entre los que destacan **TCP** (*Transmission Control Protocol* o *Protocolo de Control de Transmisión*), orientado a la conexión y fiable, y **UDP** (*User Datagram Protocol* o *Protocolo de Datagrama de Usuario*), no orientado a la conexión y no fiable.
- **Capa de aplicación:** esta capa contiene, al igual que la capa de aplicación de OSI, todos los protocolos de alto nivel que utilizan los programas para comunicarse. Aquí se encuentra el protocolo de terminal virtual (TELNET), el de transferencia de archivos (FTP), el protocolo HTTP que usan los navegadores para recuperar páginas en la *World Wide Web*, los protocolos de gestión del correo electrónico, etc.

### 1.3.5.2 RED MICROSOFT

La arquitectura de red patentada por Microsoft está diseñada con el objetivo de permitir la coexistencia e integración con otras arquitecturas de red como TCP/IP o Novell. Por esta razón, en el modelo de redes Microsoft se pueden añadir los distintos protocolos existentes para que realicen el transporte de la información. La figura 2.6 muestra el esquema simplificado del modelo de redes Microsoft.

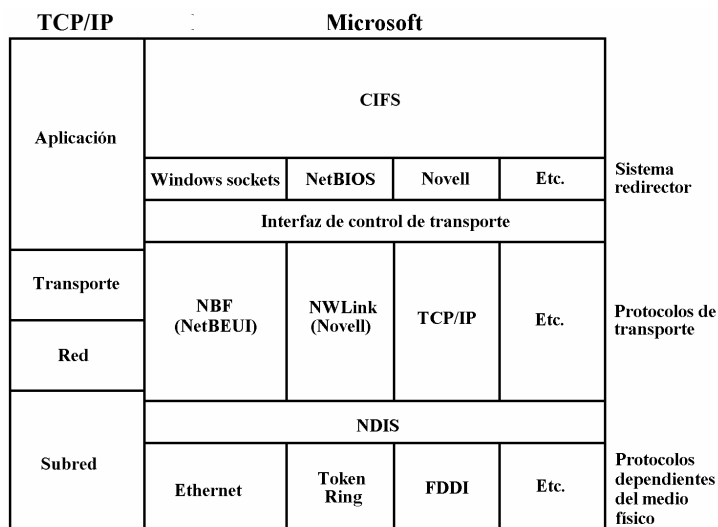


Figura 1.15. Modelo en capas de la red Microsoft. Aquí se puede observar cómo esta arquitectura ha ido incluyendo nuevos protocolos sobre el diseño original. También se puede observar la comparación con los niveles de la arquitectura TCP/IP

El protocolo **NetBIOS** (*Network Basic Input/Output System* o Sistema Básico de Entrada/Salida de Red) fue diseñado por IBM ante la falta de un estándar de alto nivel en redes de área local. Posteriormente ha sido adoptado en las redes Microsoft para el trabajo con estaciones Windows. Su identificación se hace a través de un **nombre de PC**, y el envío de la información de administración y recursos compartidos se realiza por difusión (es decir, los mensajes se envían a todos los equipos a la vez).

**CIFS** (*Common Internet File System* o Sistema de Archivos Común de Interred) es una variante del protocolo **SMB** (*Server Message Block* o *Bloque de Mensajes del Servidor*) diseñada por IBM. Se trata de protocolos de nivel de aplicación usados en redes Microsoft, que permiten convertir las peticiones del estilo "crear archivo", "copiar archivo", etc., en llamadas a servicios del protocolo NetBIOS.

El protocolo **NetBEUI** (*NetBIOS Extended User Interface*) es una extensión del protocolo NetBIOS que trabaja a nivel de red y nivel de transporte en estaciones de trabajo con sistema operativo Windows. Este protocolo es bastante sencillo y está optimizado para su

funcionamiento en LAN, ya que no puede utilizarse para la comunicación con una red de área extensa.

El protocolo NetBIOS puede funcionar sobre NetBEUI, TCP/IP o SPX (en una red Novell), dependiendo de los que se encuentren instalados y de la configuración seleccionada por el usuario. Lo normal es que NetBIOS funcione sobre TCP/IP (a esta pila se le llama **NetBT**), ya que el protocolo NetBEUI ha dejado de utilizarse en las versiones más recientes de Windows. En caso de que la estación tenga acceso a Internet, será necesario usar forzosamente TCP/IP bajo NetBIOS o utilizar algún dispositivo adaptador de protocolos (**pasarela**). También puede resultar útil en determinadas circunstancias el funcionamiento de NetBIOS sobre IPX/SPX, mecanismo denominado **NWLink**.

### 1.3.5.3 APPLE TALK

AppleTalk es una pila de protocolos desarrollados por Apple Inc. para la conexión de redes, cuya función es la misma que la de los protocolos de la red Microsoft. Esta arquitectura se diseñó en 1984 para ser incluida en los ordenadores Macintosh, pero actualmente está en desuso a favor de la arquitectura TCP/IP.

Los usuarios de una red AppleTalk identifican los recursos compartidos de la red a través de nombres largos. Estos nombres largos eran traducidos de forma automática a direcciones AppleTalk que eran números de 4 bytes divididos en tres partes: número de red, número de equipo y número de puerto.

Los protocolos de la arquitectura AppleTalk se comparan con TCP/IP en la figura 1.16. En sus inicios, AppleTalk funcionaba a través de comunicaciones por el puerto RS-422 disponible en todos los Macintosh (LocalTalk), aunque después se integraron los protocolos de la red Ethernet (véase el apartado 1.4.2), lo que se conoció como EtherTalk.

TCP/IP	AppleTalk			
	AFP		PAP	
Aplicación	ZIP	ASP		ADSP
Transporte	Protocolo de Transacciones AppleTalk			
Red	Protocolo de Entrega de Datagramas			
Subred	LLAP	ELAP	TLAP	FDDI
	LocalTalk	Ethernet	Token Ring	FDDI

Figura 1.16. Comparación de la arquitectura AppleTalk con TCP/IP. Al igual que la arquitectura de red de Microsoft, AppleTalk también ha ido integrando con el tiempo nuevos protocolos para coexistir con las redes locales más utilizadas en el momento

---

## 1.4 NORMATIVA

---

Las primeras redes de ordenadores que se construyeron, tanto comerciales como militares, utilizaban sus propios protocolos. Existen compañías que utilizaban normas de comunicación diferentes para sus propios productos. Esta situación llevó a que las empresas mantuvieran redes de diferentes fabricantes. Cuando necesitaron comunicar esas redes, surgieron los problemas: los sistemas de transmisión no eran compatibles y, o bien había que deshacerse de todo lo instalado y montar redes nuevas, o bien había que desarrollar equipos adaptadores de redes, una alternativa de coste muy elevado.

A partir de entonces, se comprobó que era necesario definir un conjunto común de normas, que permitiera coordinar a todos los fabricantes. Estas normas posibilitan la comunicación entre diferentes equipos y permiten que estos tengan un menor coste y una mayor aceptación. Las normas se dividen en dos categorías:

- **Estándares *de facto*:** viene de la palabra que en latín significa *de hecho* y a este grupo pertenecen los estándares que simplemente aparecieron y se impusieron en el mercado por su extensa utilización. El ordenador personal (PC) de IBM y sus sucesores son normas *de facto* porque la mayoría de los fabricantes copiaron los equipos de IBM con mucha exactitud. El sistema operativo UNIX también se ha convertido en un estándar al ser copiado por otros fabricantes: SCO, Minix, Linux, etc.
- **Estándares *de jure*:** viene del latín que significa *por ley* y se trata de estándares formales y legales acordados por algún organismo de estandarización autorizado. Estos organismos son de dos tipos: los creados por tratados entre varios países y las organizaciones voluntarias.

### 1.4.1 Comités de estandarización

---

Existen varias organizaciones internacionales dedicadas a tareas de normalización y estandarización. Entre ellas, destacaremos:

- **ITU** (*Internacional Telecom Union* o Unión Internacional de Telecomunicaciones). Organización de las Naciones Unidas con sede en Ginebra y constituida por las autoridades de Correos, Telégrafos y Teléfonos (PTT) de los países miembros. Se encarga de realizar recomendaciones técnicas sobre teléfono, telégrafo e interfaces de comunicación de datos que, a menudo, se reconocen como estándares. Trabaja en colaboración con ISO, que en la actualidad es miembro del ITU. Tiene tres sectores principales: sector de radiocomunicaciones (ITU-R), sector de desarrollo (ITU-D) y sector de telecomunicaciones (ITU-T).

- **ISO** (*International Standards Organization* u Organización Internacional de Normalización). Organización de carácter voluntario que agrupa a 89 países. Sus miembros han desarrollado estándares para las naciones participantes. Uno de sus comités se ocupa de los sistemas de información, que ha desarrollado el modelo de referencia OSI y protocolos para varios niveles de ese modelo. ISO también ha desarrollado otros estándares en otros campos, como el ISO 216 (para medidas de papel, como A4), ISO 9000 (sistemas de gestión de calidad), ISO 3166 (códigos de países), etc.
- **ANSI** (*American National Standards Institute* o Instituto Americano de Normas Nacionales). Asociación con fines no lucrativos, formada por fabricantes, usuarios, compañías que ofrecen servicios públicos de comunicaciones y otras organizaciones interesadas en temas de comunicación. Es el representante estadounidense de ISO, que adopta con frecuencia los estándares ANSI como normas internacionales.
- **IEEE** (*Institute of Electrical and Electronics Engineers* o Instituto de Ingenieros Eléctricos y Electrónicos). Es la mayor organización internacional sin ánimo de lucro formada por profesionales de las nuevas tecnologías. Además de publicar revistas y preparar conferencias, esta organización se encarga de elaborar estándares en las áreas de ingeniería eléctrica y computación (como es el estándar IEEE 802 para redes de área local o el estándar POSIX para sistemas operativos).
- **IETF** (*Internet Engineering Task Force* o Grupo de Trabajo en Ingeniería de Internet). Es una organización creada en Estados Unidos en 1986 cuyo objetivo principal consiste en desarrollar los estándares que funcionan en Internet. Está formada por técnicos y especialistas que publican las recomendaciones de los protocolos de Internet, haciendo que los fabricantes tengan que adaptarse a ellas para evitar problemas de compatibilidad y funcionamiento entre sistemas. Los documentos que publica el IETF se denominan **RFC** (*Request For Comments* o *Petición de Comentarios*) y son la base para el desarrollo de todas las tecnologías que funcionan en Internet. Estos documentos, publicados desde 1969, llegan a ser más de 5000 en la actualidad. Ejemplos de estos documentos son el RFC 2616 (protocolo de transferencia de hipertexto o HTTP), RFC 959 (protocolo de transferencia de archivos o FTP) o RFC 2821 (protocolo simple de transferencia de correo o SMTP).
- **ISC** (*Internet Systems Consortium* o Consorcio de Sistemas de Internet). Es una organización sin ánimo de lucro fundada en 1994 que desarrolla y da soporte a determinados programas que funcionan en Internet. Entre estos programas se encuentran algunos tan importantes como BIND (traducción de direcciones de dominio en direcciones numéricas a través del protocolo DNS), DHCP (configuración automática), NTP (sincronización horaria), etc. Todo el software que se desarrolla por el ISC se distribuye bajo licencia ISC, una licencia parecida a la utilizada por el MIT para distribuir OpenBSD.

- **ICANN** (*Internet Corporation for Assigned Names and Numbers* o Corporación de Internet para la Asignación de Nombres y Números). Organización sin ánimo de lucro creada en 1998 para asumir las tareas de la anterior **IANA** (*Internet Assigned Numbers Authority* o *Agencia de Asignación de Números de Internet*). Su función principal consiste en mantener un registro central de números asociados con los protocolos de Internet, además de los nombres de dominios y direcciones.
- **W3C** (*World Wide Web Consortium* o Consorcio de la World Wide Web). Es un organismo que apareció en 1994 y que está presidido por Tim Berners-Lee. Su objetivo es producir estándares para todas las tecnologías que engloba la *World Wide Web* (WWW o *tela de araña mundial*). Actualmente, el W3C está integrado por más de 400 miembros y unos 60 investigadores, y dispone de oficinas regionales en multitud de países. El W3C publica una serie de documentos oficiales, denominados **Recomendaciones del Consorcio**, que contienen los nuevos estándares y son publicados y distribuidos de forma libre para que los fabricantes y desarrolladores se puedan adaptar a ellos. Algunas de las recomendaciones más importantes son HTML, CSS, DOM, XML, etc., que se utilizan para el diseño de páginas *web* y navegadores en Internet.
- **Open Group**. Tiene como objetivo ofrecer estándares abiertos y neutrales para la industria informática. Sus miembros incluyen empresas, organismos e instituciones gubernamentales, como HP, IBM, el Departamento de Defensa de Estados Unidos, etc. Uno de los estándares más conocidos es la **Single Unix Specification**, que certifica los productos de tipo Unix.

## 1.4.2 Estándares de redes de área local

---

Las redes de transmisión de datos ofrecen servicios muy variados a los usuarios. Esta variedad ha hecho que hasta la fecha existan diferentes tipos de redes funcionando a lo largo del planeta, cada una enfocada a ofrecer un conjunto de servicios especializado. Las redes locales no han sido una excepción y se han diseñado multitud de tecnologías para ofrecer determinados servicios con una determinada velocidad de transmisión. En este apartado veremos algunos de los estándares de redes de área local más utilizados en la actualidad.

### 1.4.2.1 ETHERNET

El primer estándar de **Ethernet** fue diseñado en 1976 por Xerox y, posteriormente, revisado en varias ocasiones para permitir velocidades de transmisión de 10, 100, 1.000 o hasta 10.000 Mbps. El estándar Ethernet ha sido adaptado para ser compatible con el estándar **IEEE 802.3**, que fue elaborado en 1990 por la organización IEEE (*Institute of Electrical and Electronics Engineers* o Instituto de Ingenieros Eléctricos y Electrónicos) para la comunicación en redes locales. Por esta razón, al estándar se le conoce comúnmente como Ethernet o IEEE 802.3.

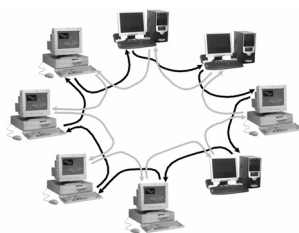
Dentro de este estándar se han definido varios tipos de redes locales en lo que se refiere al tipo de cableado utilizado, velocidad de transmisión, formato de los bloques de información enviados, control de acceso al medio compartido, etc. Estos aspectos están definidos a nivel físico y a nivel de enlace, por lo que IEEE 802 sólo cubre los protocolos de estas dos capas. En el capítulo 3 se explica con detalle los protocolos definidos en Ethernet IEEE 802 y las tecnologías de transmisión que utiliza, por ser este estándar uno de los más utilizados en la actualidad en redes locales.

### 1.4.2.2 FDDI

La red **FDDI** (*Fiber Distributed Data Interface* o Interfaz de Datos Distribuido por Fibra) fue diseñada con el propósito de obtener una red de alta velocidad, alta capacidad y gran fiabilidad. Así, es capaz de transferir información entre 50 y 100 Mbps y permite la conexión de hasta 1.000 estaciones.

FDDI utiliza fibras multimodo para los enlaces, además de concentradores de cableado, lo que le confiere una topología física en estrella. La fiabilidad de la tecnología de fibra le da a esta red una tasa de fallos inferior a un dígito binario por cada 10.000 millones. Otra característica que hace a FDDI muy fiable es su topología lógica en forma de doble anillo, donde la información gira en direcciones opuestas. Si alguna de las estaciones falla o se rompe el cable en algún punto (rompiendo los dos anillos), será posible unirlos formando un solo anillo de doble longitud y la red continuará funcionando. Cada estación dispone de un mecanismo para unir los dos anillos o saltar esa estación si no funciona.

A los anillos de la red se les llama **anillo primario** y **anillo secundario**. También existen dos clases de estaciones: las de **clase A** (también llamadas **DAS**, *Dual Attach Station* o Estación de Doble Enlace), conectadas al anillo primario y al secundario, y las de **clase B** (**SAS**, *Single Attach Station* o Estación de Enlace Simple), solamente conectadas al anillo primario. Si se produce un fallo, serán las estaciones de clase A (DAS) las que reconfiguren el anillo, y alguna de las estaciones de clase B puede quedar aislada. Esta desventaja se compensa con el hecho de que las estaciones de clase B sólo tienen una conexión a la red y, por lo tanto, los costes se reducen. Será responsabilidad del administrador de la red establecer qué estaciones son más importantes y deben conectarse a los dos anillos.



*Figura 1.17. Topología lógica de la red FDDI. Está formada por dos anillos de fibra que transportan la información en direcciones opuestas. En este ejemplo, todas las estaciones tienen conexión con los dos anillos lógicos, aunque en realidad cada estación puede estar conectada solamente a un anillo*



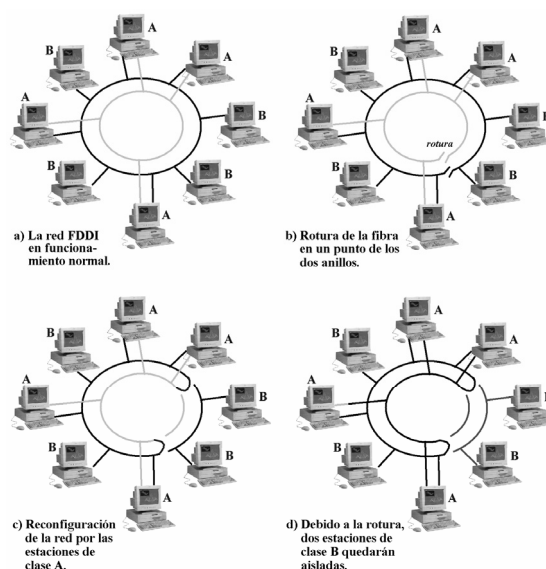


Figura 1.18. Fallo en FDDI. Cuando se rompe un enlace, las estaciones de clase A unen los dos anillos para formar uno solo. Esta reconfiguración puede hacer que una estación de clase B quede aislada de la red, normalmente las situadas entre dos estaciones de clase A

Existe un estándar prácticamente idéntico a FDDI llamado **CDDI** (*Copper Distributed Data Interface* o Interfaz de Datos Distribuido por Cobre) o **TPDDI** (*Twisted Pair Distributed Data Interface* o Interfaz de Datos Distribuido por Par Trenzado) que se diferencia del anterior en que utiliza cable de cobre en vez de fibra óptica, aunque la topología, configuración y formatos de bloques de información que transmite son iguales.

### 1.4.2.3 REDES INALÁMBRICAS

Las **redes locales inalámbricas** que siguen el estándar IEEE 802.11 transmiten datos a través de ondas electromagnéticas a una velocidad que depende de la versión utilizada (1,5 Mbps es la primera versión, de 5,5 a 11 Mbps en el estándar IEEE 802.11b o 54 Mbps en el estándar IEEE 802.11g). Algunos adaptadores que siguen el estándar IEEE 802.11b pueden llegar a transmitir hasta 100 Mbps. Puesto que la capacidad de transmisión de una red inalámbrica se ve directamente afectada por la potencia de la señal, ésta puede adaptar su velocidad de transmisión a la "cobertura" disponible, por lo que la velocidad de transmisión disponible en cada momento se puede reducir considerablemente con respecto a los valores ideales citados anteriormente.

Este tipo de redes se clasifica como LAN, ya que habitualmente se instala dentro del ámbito de un edificio. Su topología está distribuida en emisores y receptores de ondas de radio que están conectados entre sí y dispersados por toda la organización. De esta forma, cualquier equipo que disponga también de un emisor y receptor estará permanentemente conectado en cualquier lugar, sin necesidad de utilizar cables.

Las redes locales pueden utilizar diferentes protocolos de comunicación, dependiendo de las necesidades y de los equipos conectados a ellas. Por ejemplo, si la red local utiliza equipos con sistema operativo Microsoft Windows, entonces se usa la arquitectura de red de Microsoft para comunicarlos. Si existen equipos Linux, entonces utilizarán los protocolos de TCP/IP.

### 1.4.3 Infraestructuras comunes de telecomunicación

---

Una **Infraestructura Común de Telecomunicación (ICT)** es una instalación para captar, adaptar y distribuir señales de radio, televisión (por cable o satélite), teléfono y comunicaciones de banda ancha (cableadas o inalámbricas) en viviendas y locales. En España, el reglamento que regula la instalación de una ICT viene definido en la siguiente legislación:

Real Decreto Ley 1/1998, de 27 de febrero, modificado por la Ley 38/1999, de 5 de noviembre y por la Ley 10/2005, de 14 de junio.

- Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.
- Ley 8/1999 de 6 de abril, de Reforma de la LPH.
- Ley 38/1999, de 5 de noviembre, de Ordenación de la Edificación.
- Ley 10/2005, de 14 de junio, de Medidas Urgentes para el impulso de la TDT.
- R. D. 401/2003 de 4 de abril por el que se aprueba el Reglamento de ICT.
- Orden CTE/1296/2003 de 14 de mayo por el que se desarrolla el Reglamento regulador de infraestructuras comunes de telecomunicación.
- Para la correcta aplicación de esta legislación se debe acudir a los profesionales cualificados.
- Orden ITC/1077/2006, de 6 de abril.

Actualmente, cuando se realiza una construcción o rehabilitación integral de edificios, es obligatorio que estos cuenten con un proyecto de instalación de una ICT. Solamente las empresas autorizadas pueden realizar este tipo de instalaciones, en base al proyecto previamente definido. Una vez realizada la instalación, la empresa autorizada deberá certificarla mediante las pruebas correspondientes y expedir el documento acreditativo, denominado **Boletín de Instalación**.

La instalación de una ICT requiere de un mínimo de dos tomas por vivienda y servicio, de forma que se asegure la disponibilidad de líneas sin necesidad de modificar la instalación. Una instalación ICT incluye las canalizaciones y conductos por donde va el cableado, el propio

cableado, las tomas de pared, los dispositivos de recepción y emisión de las señales y los dispositivos de interconexión y amplificación.



Figura 1.19. Amplificadores monocanal. Estos dispositivos se utilizan comúnmente en las instalaciones de televisión por cable o satélite de ICT en edificios residenciales



## TEST DE CONOCIMIENTOS



- › **1. Un elemento de interconexión de red sirve para:**
  - a) Convertir el formato de los mensajes que van a ser transmitidos.
  - b) Conectar los ordenadores con la red.
  - c) Controlar el funcionamiento de la red.
  - d) Ninguna es cierta.
  
- › **2. La topología física de una red es:**
  - a) La forma en la que se conectan los equipos.
  - b) La forma en la que se transmite la información.
  - c) La forma en la que se comparte el medio.
  - d) La forma en la que se corrigen los errores de la comunicación.
  
- › **3. La topología lógica de una red es:**
  - a) La forma en la que se conectan los equipos.
  - b) La forma en la que se transmite la información.

- c) La forma en la que se comparte el medio.
- d) La forma en la que se detectan los errores de la comunicación.

› **4. Un protocolo de comunicación sirve para:**

- a) Establecer las normas a seguir para que la comunicación se realice correctamente.
- b) Controlar el acceso al medio.
- c) Controlar los errores.
- d) Todas son ciertas.

› **5. La capa de transporte de TCP/IP se usa para:**

- a) Controlar los errores.
- b) Controlar el acceso al medio.
- c) Establecer la ruta hasta el destino.
- d) Ninguna es cierta.

› **6. Un estándar de facto es aquel que:**

- a) Ha sido definido por una organización de estandarización.
- b) Ha sido creado por un país.
- c) No se usa en redes locales.
- d) Ninguna es cierta.

› **7. El estándar Ethernet define:**

- a) Los protocolos en redes de área local.
- b) El tipo de cable a utilizar.
- c) El protocolo de control de acceso al medio.
- d) Todas son ciertas.

› **8. El estándar IEEE 802.11 define:**

- a) Las redes locales inalámbricas.
- b) Las redes locales de par trenzado.

- c) Las redes locales FDDI de fibra óptica.
- d) Las redes locales FDDI de cobre.

› **9. Una red FDDI tiene una topología física en:**

- a) Estrella.
- b) Anillo.
- c) Doble anillo.
- d) Intersección de anillo.

› **10. Una infraestructura común de telecomunicación permite distribuir señales de:**

- a) Radio.
- b) Televisión.
- c) Comunicaciones de banda ancha.
- d) Todas son ciertas.