

---

# Redes de comunicación

---

PID\_00247328

Jesús Alonso-Zárate

---

Tiempo mínimo de dedicación recomendado: 3 horas

---



*Ninguna parte de esta publicación, incluido el diseño general y la cubierta, puede ser copiada, reproducida, almacenada o transmitida de ninguna forma, ni por ningún medio, sea éste eléctrico, químico, mecánico, óptico, grabación, fotocopia, o cualquier otro, sin la previa autorización escrita de los titulares del copyright.*

# Índice

<b>Introducción</b> .....	5
<b>Objetivos</b> .....	6
<b>1. Introducción a las redes de comunicaciones</b> .....	7
1.1. Una posible definición .....	7
1.2. Elementos de una red .....	7
1.3. Topologías de red .....	8
1.4. La conmutación en las redes de comunicaciones .....	9
1.4.1. Conmutación de circuitos .....	10
1.4.2. Conmutación de paquetes .....	10
1.4.3. Conmutación de paquetes con circuito virtual .....	11
1.5. Redes de difusión y punto a punto .....	12
1.6. Clasificación de las redes según el alcance .....	13
1.6.1. Redes de gran alcance .....	13
1.6.2. Redes de área local .....	14
<b>2. Principales tecnologías de red para la industria 4.0</b> .....	15
2.1. Tecnologías de red cableadas .....	15
2.2. Tecnologías de red sin cables .....	16
2.2.1. Tecnologías LAN que operan en bandas libres de licencia ..	17
2.2.2. Tecnologías LPWA que operan en bandas libres de licencia.	18
2.2.3. Tecnologías celulares operando en bandas licenciadas .....	18
<b>3. El software en las redes de comunicaciones</b> .....	20
3.1. Introducción a la pila de protocolos y sus capas .....	20
3.2. Diseño de redes por capas .....	20
3.3. Ejemplo de operativa por capas .....	22
3.4. Funciones que hay que implementar en las capas .....	23
<b>4. El modelo de referencia OSI</b> .....	25
4.1. La capa física: PHY .....	26
4.2. La capa de enlace .....	26
4.3. La capa de red .....	28
4.4. La capa de transporte .....	29
4.5. La capa de sesión .....	30
4.6. La capa de presentación .....	30
4.7. La capa de aplicación .....	31
<b>5. El modelo de referencia TCP/IP</b> .....	32
5.1. La capa interfaz de red .....	33

---

5.2. La capa de red (internet) .....	33
5.3. La capa de transporte .....	34
5.4. La capa de aplicación .....	35
<b>Resumen</b> .....	<b>36</b>

## Introducción

En el material «Fundamentos de comunicaciones» hemos introducido los sistemas de comunicación, y hemos presentado el caso más básico de comunicación, entre un emisor y un receptor, a través de un canal de comunicaciones.

Sin embargo, en muchos casos, esta comunicación no va a ser punto a punto, entre dos elementos únicamente, sino que se va a dar entre un número de dispositivos dispuestos en forma de red de comunicaciones.

En este material, definimos el concepto de red, sus elementos funcionales, las topologías (formas) de red, así como los tipos red en función de la naturaleza del intercambio de información en la red.

Posteriormente, vamos a describir las tecnologías principales de red basadas en medios cableados y en medios sin cables (*wireless*).

Seguidamente, introduciremos el concepto de pila de protocolos: la piedra angular sobre la que se construyen y definen «los idiomas» que usan los diferentes elementos de una red para poder entenderse entre ellos. Se trata de la pila de protocolos basada en la arquitectura OSI de 7 capas, como veremos más adelante.

Finalmente, presentaremos el modelo de referencia de la pila de protocolos de internet, la arquitectura TCP/IP, sobre el que se construyen todas las redes de comunicación que, eventualmente, necesitan conexión con internet. Este es, por tanto, el modelo de referencia para la gran mayoría de las aplicaciones de los sistemas ciberfísicos.

## Objetivos

Los objetivos de este material son:

- 1) Entender el concepto de red de comunicaciones.
- 2) Conocer los elementos que constituyen una red y las diferentes tipologías de red existentes.
- 3) Entender el papel fundamental de los protocolos de comunicaciones para poder establecer comunicación en una red.
- 4) Conocer el modelo de referencia OSI para la pila de protocolos.
- 5) Conocer el modelo de referencia TCP/IP, que es la base de todas las redes «compatibles» con internet.

## 1. Introducción a las redes de comunicaciones

### 1.1. Una posible definición

Una **red de comunicaciones** es un conjunto de dispositivos con capacidad de comunicación que pueden intercambiar información a distancia.

En este material nos vamos a centrar en las comunicaciones entre máquinas, ordenadores o dispositivos electrónicos. Esto no implica que no pueda haber una persona detrás de estos dispositivos para interpretar o generar los datos, pero en principio, nos centraremos en las redes de comunicaciones cuando la comunicación se da entre dispositivos.

### 1.2. Elementos de una red

Los elementos de una red son fundamentalmente de tres tipos:

- 1) Equipos finales.
- 2) Equipos intermedios (encaminadores, conmutadores, enrutadores, etc.).
- 3) Enlaces, que unen los equipos finales y los intermedios.

1) Los **equipos finales** pueden ser de varios tipos, por ejemplo:

- Ordenadores de sobremesa o portátiles (*laptops*).
- Dispositivos móviles (tabletas, teléfonos inteligentes, etc.).
- Dispositivos equipados con sensores o actuadores.
- Máquinas con capacidad de procesamiento de datos o instrucciones, como los PLC (*programmable logic controllers*).

Estos equipos finales tienen al menos uno de los siguientes dos roles:

- a) Origen de información.
- b) Destino de información.

Esta información puede estar preparada (codificada) para que la entienda una persona –un ser humano–, o puede ser comunicación directa entre máquinas, las llamadas comunicaciones máquina a máquina (M2M).

2) A su vez, los **equipos intermedios no son origen ni destino de la información**, pero son necesarios para llevar a cabo funciones esenciales, como por ejemplo:

- **Enrutamiento y direccionamiento**; para ayudar a los orígenes de datos a encontrar el destino.
- **Amplificación**; para amplificar señales entre orígenes de datos y destinos cuando la distancia entre ellos es grande.
- **Adaptación de protocolos**; para permitir que equipos finales «hablando diferentes idiomas» puedan entenderse entre ellos.
- **Seguridad**; para poder implementar mecanismos de autenticación y garantizar la seguridad y privacidad en la comunicación entre dos o más equipos finales.
- **Tarificación**; para medir el uso de los medios de comunicación y poder permitir a los operadores de red cobrar por el uso de los mismos para poder cubrir los costes de mantenimiento y operación de la red, así como, por supuesto, poder generar un beneficio del servicio ofrecido.
- **Gestión de recursos**; para poder asignar recursos de comunicación de manera dinámica, según las necesidades cambiantes de la red de comunicación.
- **Concentración y tratamiento de datos**; para poder fusionar datos, comprimir y tomar decisiones intermedias que permitan mejorar el rendimiento total de la red.
- **Control de congestión**; para regular el tráfico que circula en una red de comunicaciones y gestionar los recursos de manera eficiente para poder ofrecer a cada equipo final la calidad esperada o contratada.

3) Finalmente, los **enlaces** permiten conectar equipos finales entre sí, y equipos intermedios entre sí y con equipos finales. Estos enlaces, como vimos en el apartado de *Introducción a los sistemas de comunicación* del material «Fundamentos de comunicaciones», pueden ser guiados o no guiados; es decir, pueden ser enlaces por cable (coaxial, fibra óptica, par trenzado de cobre, etc.) o mediante enlaces radio (*wireless*).

### 1.3. Topologías de red

Una **topología de red** es el modo en el que están distribuidos los nodos que la forman.

Como hemos introducido antes, las redes actuales están formadas por tres tipos de entidades:

- 1) Equipos finales.
- 2) Equipos intermedios (encaminadores o conmutadores).
- 3) Enlaces, que unen los equipos finales y los intermedios.

Las topologías de red más habituales son:

- **Estrella.** Esta topología está formada por un nodo central, que actúa como nodo intermedio de la red (conmutador o encaminador) y gestiona el envío y la recepción de los datos. El resto de las estaciones se conectan a este nodo principal.
- **Bus.** Todos los equipos están conectados a un único medio de transmisión compartido entre todas las estaciones de la red. Por lo tanto, es necesario establecer un sistema de acceso al medio para evitar que más de una estación transmita al mismo tiempo y se produzcan colisiones.
- **Anillo.** Una topología en anillo está formada por un enlace que forma un bucle, de manera que cada estación está conectada al anillo mediante dos enlaces, el de entrada y el de salida. Generalmente, cuando la estación emisora recibe su propio paquete, lo elimina de la red.
- **Árbol.** Una topología en árbol es una topología mixta de las topologías en bus y en estrella. A veces, también se conoce como topología jerárquica. Un ejemplo es el de la figura 1d, en la que varios nodos intermedios se conectan entre sí y, a su vez, tienen conectados equipos finales. Esta topología es la más utilizada en la actualidad.
- **Mallada.** La topología mallada es aquella en la que todos los equipos están conectados con todos los del resto. Existen casos de redes malladas parciales, es decir, en los que las estaciones no forman una malla completa. Generalmente, esta topología se emplea en el núcleo de grandes redes, como internet, en la que solo se conectan equipos intermedios, no finales.

#### 1.4. La conmutación en las redes de comunicaciones

En el ámbito de las redes, la conmutación hace referencia al establecimiento de un circuito (real o lógico) entre dos puntos de la red que permite la interconexión y, por lo tanto, el intercambio de información entre esos puntos.

En esencia, esta conmutación se puede dividir, al menos, en tres clases diferentes:

- 1) Conmutación de **circuitos**.
- 2) Conmutación de **paquetes**.
- 3) Conmutación de **paquetes con circuito virtual**.

Describimos estos tipos de conmutación en las siguientes secciones.

### 1.4.1. Conmutación de circuitos

La conmutación de circuitos se basa en la creación de un **circuito físico** entre los dos interlocutores de la red.

Este circuito físico se establece antes de transmitir cualquier tipo de información y está formado por diferentes enlaces entre los nodos. El ejemplo clásico de conmutación de circuitos es la telefonía tradicional; en el momento en el que se establece una llamada entre origen y destino, existe un canal de comunicación dedicado al intercambio de información entre dos equipos finales de red.

En conmutación de circuitos, se distinguen tres fases para el envío de información:

- 1) **Establecimiento del circuito:** esta fase se encarga de buscar un camino entre los nodos intermedios que lleven al destino. La estación origen pide la creación del circuito al nodo al que está conectada, que a su vez envía la petición al siguiente nodo. Este otro nodo hará lo mismo respecto al siguiente, y así hasta llegar al destino final. A medida que se va formando el circuito, cada nodo intermedio verifica la existencia de suficientes recursos para establecerlo, y en el caso de que no sea así, se aborta la petición de circuito. En el caso de que el establecimiento no sea viable, cuando llegue al destino este enviará una señal al origen para comunicar que ya puede enviar información.
- 2) **Transferencia de datos.** En este caso, las estaciones pueden intercambiar la información deseada.
- 3) **Desconexión.** Una vez que se ha acabado la comunicación, se deben liberar los recursos, para estar más adelante a disposición de otras conexiones.

### 1.4.2. Conmutación de paquetes

Uno de los principales problemas que encontramos en la conmutación de circuitos es la **exclusividad de los recursos**; cuando se establece un circuito, aunque no haya intercambio de datos, los recursos están reservados y no pueden ser utilizados por ninguna otra estación. El problema se ve agravado porque en conexiones de datos como las actuales, el tráfico, en lugar de ser constante, suele llegar a ráfagas. Por ejemplo, cuando un usuario carga una página web, la carga solo implica unos pocos centenares de milisegundos, mientras que su lectura puede suponer minutos.

Otro problema impuesto por la conmutación de circuitos es el de la necesidad de que todos los nodos de la comunicación trabajen a la misma velocidad, cosa que no se puede garantizar en los sistemas de comunicación actuales, dada la gran variedad de equipos finales que se pueden conectar a las redes de comunicación y la cantidad dispersa de aplicaciones que se prevén dentro del contexto de la industria 4.0.

**La conmutación de paquetes es la alternativa a la conmutación de circuitos.** La conmutación de paquetes se basa en la creación de un **circuito lógico** entre los dos interlocutores de la red. Este circuito lógico se establece antes de transmitir cualquier tipo de información, y está formado por diferentes enlaces entre los nodos que, en este caso, se comparten entre varios enlaces lógicos.

La información se «paquetiza» y se transmite en bloques de información delimitados. En lugar de reservar recursos con un circuito, la conmutación de paquetes dota a los nodos intermedios de la red de capacidad de procesado y de un sistema de colas (*buffers*) que permite almacenar temporalmente un paquete, procesarlo, localizar a su destinatario (o siguiente salto en el camino a su destino) y enviarlo al nodo que corresponda.

La conmutación de paquetes permite:

- 1) Optimizar el empleo de los canales de comunicación.
- 2) Interconectar terminales con diferentes velocidades de transmisión y procesado de datos.
- 3) Crear conexiones simultáneas sin reserva de recursos.
- 4) La coexistencia de diferentes velocidades de transmisión en un mismo enlace.

Las colas de los nodos de conmutación tienen un tamaño determinado; esto implica que si una cola se llena antes de ser procesada, se perderán paquetes.

Otra consideración importante en la conmutación de paquetes es el tamaño del paquete que se quiere transmitir. Históricamente, en un principio, se pensó que los paquetes tuvieran el mismo tamaño que el mensaje que iba a ser enviado y se hablaba de conmutación de mensajes. Sin embargo, enseguida se vio que para mensajes grandes los nodos intermedios necesitaban demasiada memoria (ya que almacenan el paquete en su totalidad antes de enviarlo y, por ello, requieren demasiado tiempo para procesarlo). En consecuencia, en la gran mayoría de los sistemas de comunicación actual, los mensajes se **fragmentan** en paquetes pequeños, con un tamaño máximo fijado, y se envían de manera independiente, asegurando que todos lleguen a su destino. En el destino, es importante comprobar que se han recibido todos los fragmentos de un mismo mensaje para poder recuperar el mensaje original. Existen técnicas específicas para ello.

### 1.4.3. Conmutación de paquetes con circuito virtual

Aunque la conmutación de paquetes es mejor que la conmutación de mensajes, y claramente que la conmutación de circuitos, las dos soluciones tienen el problema de que, según el tamaño y el estado de las colas de los nodos intermedios, el retraso

en la llegada de la información varía (lo que se llama *jitter*), lo cual implica que en comunicaciones críticas en tiempo (como una conversación de voz), esto pueda llegar a ser un problema. Por ejemplo, si un paquete de voz llega demasiado tarde, no podrá ser descodificado y el interlocutor notará un pequeño corte en la conversación. Puesto que no tiene sentido recibir un paquete de voz fuera de tiempo, es mejor descartarlo que entregarlo tarde.

Para minimizar este problema, se diseñó el concepto de **conmutación de paquetes con circuito virtual**. El objetivo es conseguir las ventajas de la flexibilidad de la conmutación de paquetes y de mensajes, así como la esencia de la conmutación de circuitos. De este modo, en lugar de enviar independientemente todos los fragmentos o paquetes de una conexión entre una fuente y un destino, se establecen unos circuitos virtuales que deciden, antes de iniciar el intercambio de información, el camino entre fuente y destino (como sucede en la conmutación de circuitos). Una vez establecido, se transmiten los paquetes individuales. De este modo, todos los paquetes seguirán el mismo camino, en el mismo orden, y se podrá contar con una reserva de recursos que asegure que los paquetes llegan ordenados y con el mismo retardo, lo que permitirá el intercambio de información para aplicaciones de *streaming* o tiempo real.

### 1.5. Redes de difusión y punto a punto

1) **Redes de difusión:** una red de difusión es aquella en la que el medio es compartido por las estaciones que forman la red. Todos los equipos reciben todos los paquetes, aunque solo procesan los dirigidos a ellos. Entre otras cosas, esto implica serios problemas de privacidad, y por ello, en este tipo de redes es recomendable utilizar mecanismos de cifrado en las conexiones y en las redes inalámbricas. **Las redes inalámbricas son, por definición, redes de difusión.**

2) **Redes punto a punto:** en contraposición a las redes de difusión, las redes punto a punto son aquellas en las que las conexiones se encuentran entre dos puntos determinados de la red. A pesar de que un enlace punto a punto puede parecer poco flexible, en realidad es el tipo de conexión más utilizado actualmente, ya que puede ser extendido para formar topologías de estrella, árbol o malladas de un modo muy sencillo. También hay que destacar que en una red por naturaleza de difusión, como las redes por vía radio, se pueden establecer conexiones punto a punto, con un origen y destino definidos.

Según la naturaleza sobre la capacidad de los dispositivos de una red de transmitir y recibir al mismo tiempo, los enlaces punto a punto pueden ser:

1) **Simplex:** la comunicación es unidireccional. De los dos dispositivos conectados, uno siempre es el origen y el otro, el destino.

2) **Semiduplex:** la comunicación puede ser bidireccional, pero siempre y cuando los dos dispositivos de la comunicación alternen en la generación de tráfico; todo punto puede transmitir y recibir, pero no al mismo tiempo.

3) **Full-duplex**: la comunicación se puede llevar a cabo simultáneamente en los dos sentidos de la comunicación entre dos dispositivos.

En las comunicaciones bidireccionales, la velocidad puede ser igual (**conexión simétrica**) o diferente, en función del sentido de la comunicación (**conexión asimétrica**).

Cabe comentar que, aunque las comunicaciones *full-duplex* en sistemas radio son foco de profunda investigación, y es posible que en un futuro no muy lejano se puedan desplegar masivamente redes inalámbricas basadas en comunicaciones *full-duplex*, hoy día, la gran mayoría de las redes comerciales inalámbricas son *half-duplex*, haciendo duplexación (entre los dos sentidos de las comunicaciones) o bien en tiempo (**TDD**, *time division duplex*) o frecuencia (**FDD**, *frequency division duplex*). En este segundo caso, es necesario que los dispositivos tengan dos receptores radio, lo que encarece considerablemente su implementación.

## 1.6. Clasificación de las redes según el alcance

Una clasificación bastante conocida de las redes es aquella que valora su alcance, aunque según el entorno esta clasificación puede cambiar.

Aunque se puede subclasificar mucho más, generalmente se consideran dos grandes categorías de redes:

- 1) Las redes de gran alcance (**WAN**, *wide area networks*).
- 2) Las redes de alcance local (**LAN**, *local area networks*).

### 1.6.1. Redes de gran alcance

Las redes de gran alcance son aquellas que se utilizan en espacios geográficos extensos. Generalmente, las WAN se encargan de la interconexión de LAN, lo que facilita la conexión de los usuarios de diferentes localizaciones.

La transmisión de los datos suele hacerse mediante grandes operadoras de comunicaciones con líneas de comunicación contratadas, utilizando infraestructuras que se consideran públicas (para evitar monopolios).

Las conexiones WAN son prácticamente siempre punto a punto, exceptuando los enlaces vía satélite, que por el hecho de utilizar el aire como medio de transmisión son inherentemente medios de difusión.

Por su gran extensión, las redes WAN, en general, están compuestas por una topología de árbol, que a su vez está conectada a topologías malladas, formadas por miles de nodos.

Dado que estas redes suelen agregar mucho tráfico y requieren mucha capacidad, acostumbran a estar basadas en enlaces por fibra óptica con gran capacidad de transmisión de datos.

### 1.6.2. Redes de área local

Por el contrario, las LAN están diseñadas para tener un alcance más reducido que las WAN. Esta distancia puede oscilar entre unos pocos kilómetros y algunos metros (e incluso centímetros).

Es habitual crear subclasificaciones de la tecnologías LAN, distinguiendo entre redes de área local (LAN), redes de área personal (PAN), o incluso redes de área «corporal» para hacer referencia a las redes establecidas entre dispositivos conectados alrededor de una persona (ejemplo: *weareables*); estas últimas son las llamadas *body area networks* (BAN).

Las tecnologías LAN están pensadas para conectar a usuarios con relativamente pocos equipos, edificios empresariales e incluso campus enteros. Normalmente, estas LAN se acaban conectando a WAN y, por ende, a internet.

De hecho, en la actualidad, **la interconexión masiva de LAN y WAN es lo que llamamos internet.**

Las LAN se han caracterizado por emplear un medio de difusión para enviar información, pero desde la aparición de conmutadores y otros equipamientos más actuales, han pasado, mediante topologías de árbol y estrella, a ser un conjunto de conexiones punto a punto.

La excepción a esta regla vuelven a ser las redes que utilizan el aire como medio de transmisión, es decir, las redes inalámbricas, que emplean difusión para enviar la información.

Cabe señalar que existen muchos tipos de redes inalámbricas, y que no todas pueden ser clasificadas como LAN. Por ejemplo, las redes de telefonía móvil son redes WAN, que ofrecen cobertura en un ámbito mundial.

## 2. Principales tecnologías de red para la industria 4.0

La lista de tecnologías de red existentes en la actualidad es demasiado extensa para poder incluirla aquí de manera exhaustiva.

No hay duda de que la industria 4.0 se va a caracterizar por una gran flexibilidad, movilidad, y adaptabilidad a necesidades cambiantes, y por este motivo, se prevé que las tecnologías *wireless* dominarán sobre las tecnologías cableadas.

Sin embargo, las tecnologías por cable también van a jugar un papel fundamental en algunos casos particulares en los que, claramente, los cables ofrecen ventajas sobre el medio aéreo para el intercambio de información.

### 2.1. Tecnologías de red cableadas

Aunque seguramente se trata de una selección bastante debatible, a continuación listamos las tecnologías por cable que se pueden considerar más relevantes dentro del contexto de la industria 4.0:

- 1) **Ethernet**, de gran aplicación para la industria 4.0; es la base de la mayoría de las conexiones que se usan hoy día, por ejemplo, para distribuir la conexión a internet en edificios de oficinas, hoteles y entornos industriales.
- 2) **Fibra óptica**, de gran uso para redes de transporte a muy alta velocidad. Esta es la solución adoptada por los proveedores de internet para proveer a sus clientes de conectividad, así como la solución para interconectar centros de datos cuando la cantidad de información que hay que intercambiar es realmente muy grande.
- 3) **Power line communications (PLC)**, de uso para transmisiones a corta distancia en entornos *indoor*, fundamentalmente, haciendo uso de los cables y la infraestructura ya desplegada para la distribución de electricidad.

Dentro de las redes cableadas, la familia de tecnologías por excelencia que tiene y tendrá un papel fundamental en el desarrollo de aplicaciones para la industria 4.0 es **Ethernet** (definida en el estándar IEEE 802.3).

Esta empezó como una tecnología con capacidad de transmisión de 10 Mbps con una topología de bus y medio compartido. En los últimos años, ha ido evolucionando a una topología de estrella de 1 Gbps (Gigabit Ethernet) pasando por Fast Ethernet, a 100 Mbps, y llegando a modelos de 10 Gigabit Ethernet.

Pese a empezar siendo una tecnología limitada a LAN, el bajo coste y su gran adopción permitieron que Ethernet evolucionara hasta el punto de existir hoy enlaces WAN construidos con esta tecnología.

Respecto a las topologías basadas en anillo, como Token Ring (IEEE 802.5) y FDDI (definido en el estándar ANSI X3T12), estas han ido cayendo en desuso, comparadas con Ethernet. La razón principal es su elevado coste y su peor rendimiento.

Actualmente, una topología de anillo muy utilizada es *resilient packet ring* (IEEE 802.17); una tecnología para transportar otras tecnologías mediante anillos de fibra óptica, y que en general transporta directamente tráfico Ethernet y servicios IP (*internet protocol*).

## 2.2. Tecnologías de red sin cables

Las tecnologías *wireless* han ganado mucho terreno a las tecnologías cableadas, dada su flexibilidad, movilidad y bajo coste de despliegue y mantenimiento.

En la industria 4.0, no cabe duda de que las tecnologías sin cables van a jugar un papel fundamental.

Respecto al cable, los sistemas *wireless* ofrecen al menos las siguientes ventajas:

- **Movilidad:** permiten movilidad de los dispositivos de comunicación.
- **Flexibilidad:** ofrecen mucha flexibilidad a la hora de cambiar la topología de la red, añadir o eliminar dispositivos a la arquitectura de la red.
- **Bajo coste:** tanto la instalación como el mantenimiento de este tipo de redes es muy inferior al caso de las redes con cables.
- **Alto rendimiento:** aunque no se pueden lograr las velocidades de transmisión del cable ni, por supuesto, los niveles de fiabilidad y seguridad, las tecnologías *wireless* han madurado mucho en los últimos años y, en las condiciones adecuadas y con un buen diseño, pueden ofrecer un rendimiento similar al que se puede lograr con redes por cable.

Cabe destacar los siguientes tres grandes grupos de tecnologías *wireless* con aplicabilidad para la industria 4.0:

- 1) **Tecnologías LAN** que operan en bandas libres de licencia.
- 2) **Tecnologías LPWA** que operan en bandas libres de licencia.
- 3) **Tecnologías celulares** que operan en bandas licenciadas.

Aunque en materiales posteriores se describirán estas tecnologías con mucho mayor detalle, vale la pena describirlas brevemente a continuación, para tener una imagen global de las diferentes alternativas.

### 2.2.1. Tecnologías LAN que operan en bandas libres de licencia

De entre todas las posibilidades, podemos destacar:

- **Radio frequency identification (RFID):** tecnología diseñada para evolucionar los códigos de barras y poder identificar objetos. Esta tecnología tiene una gran aplicación en almacenamiento, logística y en gran consumo, ya que permite la trazabilidad y seguimiento de los objetos y de inventario.
- **Bluetooth y bluetooth low energy (BLE):** diseñadas para redes de muy corto alcance (menos de 10 metros), con un número reducido de dispositivos y aprovechando el muy bajo coste y consumo de energía de esta tecnología. La modalidad BLE es la que se utiliza para los *beacons*, que tienen gran utilidad industrial para el posicionamiento en interiores, así como el envío de información de contexto; un ejemplo claro de aplicación de los *beacons* se materializa en la posibilidad de enviar a un teléfono móvil publicidad personalizada al acercarse a un establecimiento en particular, por ejemplo. De este modo, un *beacon* instalado en un restaurante permitiría enviar publicidad sobre ofertas y menús a los transeúntes al pasar cerca de su establecimiento. Las posibilidades de los *beacons* son realmente amplias y de gran utilidad para la visión de la industria 4.0.
- **Tecnologías basadas en el 802.15.4 (Zigbee y variantes):** diseñadas para redes de baja potencia de transmisión (atención, que decimos baja potencia, no bajo consumo de energía). Esta tecnología se diseñó para redes de sensores; el estándar original, que es la base de Zigbee, ha demostrado ser poco eficiente en entornos industriales en la práctica, dada la complejidad de configurar y operar redes de multisalto con una infraestructura relativamente compleja, así como la poca fiabilidad de la tecnología. En los últimos años, se han desarrollado nuevas versiones del estándar, como la 802.15.4e, que mejoran considerablemente el rendimiento de esta tecnología y que pueden tener mucha más aplicación en entornos industriales y aplicaciones en las que el determinismo es un criterio importante que hay que valorar.
- **Tecnologías basadas en el 802.11 (Wi-Fi y variantes):** diseñadas para redes de área local con rangos de cobertura no superiores a 100 metros. Existen muchas variantes de la tecnología que sirve de base para lo que popularmente se llama Wi-Fi. Aunque hay una versión específica para redes de sensores y actuadores, el estándar 802.11ah, las versiones para transmisión de datos de alta velocidad también tienen gran relevancia en multitud de aplicaciones de la industria 4.0. Cabe destacar los estándares 802.11n, 802.11ac, 802.11ad y el 802.11ax, que describiremos

#### Aclaración

La Wi-Fi Alliance es una alianza de fabricantes de equipos y dispositivos que promueve el uso y la interoperabilidad entre equipos de tecnología Wi-Fi; el estándar de comunicación se basa en la norma IEEE 802.11, que define las capas físicas y de acceso de las redes.

en el material «Sistemas de comunicación en la banda ISM» dedicado a este tipo de tecnologías.

### 2.2.2. Tecnologías LPWA que operan en bandas libres de licencia

En los últimos años, han emergido las denominadas redes *low power wide area* (LPWA). Estas redes han surgido como respuesta a la necesidad de poder transmitir pocos datos, consumiendo poca energía, y alcanzando grandes distancias.

Hasta su aparición, no había en el mercado ninguna tecnología capaz de ofrecer una solución eficiente desde el punto de vista técnico y económico.

Existen varias alternativas, entre las cuales cabe destacar:

- **SigFox:** tecnología propietaria diseñada por la empresa francesa SigFox. En los últimos años, ha desplegado su red por muchos países en todo el mundo, y hoy día ofrece una gran cobertura. Se basa en una tecnología de banda muy estrecha, y se aplica un modelo de negocio basado en el modelo de los operadores de telefonía móvil. El usuario no debe preocuparse por el despliegue y mantenimiento de la red; tan solo se compra una suscripción mensual o anual, y ya se puede acceder al sistema.
- **LoRaWAN:** la tecnología LoRa (*long range*) está siendo promovida por la LoRa Alliance. Un gran número de empresas de comunicaciones y fabricantes de dispositivos promueven una tecnología de largo alcance, propiedad de la empresa SEMTECH, y basada en el uso de espectro ensanchado para operar en bandas libres de frecuencia. En este caso, a diferencia del modelo de negocio de SigFox, el uso de LoRaWAN sí implica el despliegue de una red propia y su mantenimiento y operación.
- **Otras tecnologías LPWA:** además de LoRa y Sigfox, como actores principales de este nuevo escenario de las redes LPWA, existen otras alternativas que también están intentando tener su sitio; es el caso de **Weightless** o **Ingenu**, que pese a ser técnicamente interesantes, no están teniendo la tracción que sí están teniendo LoRaWAN y SigFox.

### 2.2.3. Tecnologías celulares operando en bandas licenciadas

En este grupo se engloban, fundamentalmente, las tecnologías definidas y promovidas por el 3GPP. Estas son las siglas del *3rd Global Partnership Project*; una alianza entre operadores y fabricantes de equipos de red para promover la definición de estándares para sistemas de comunicación celulares.

El 3GPP es el responsable de la definición de las diferentes generaciones de sistemas de telefonía móvil, desde GSM hasta la siguiente generación, el 5G.

**El 3GPP no es un organismo de estandarización.** El 3GPP define las especificaciones técnicas, que posteriormente los organismos de estandarización trasponen como estándares internacionales (ITU) o regionales (por ejemplo, la ETSI en Europa).

Entre las tecnologías promovidas por el 3GPP, cabe destacar cuatro grandes grupos de especificaciones técnicas:

- **GSM, GPRS/EDGE, y UMTS (2G, 2.5G, Y 3G):** diseñadas fundamentalmente para la transmisión de voz, aunque en los dos casos se pueden transmitir datos.
- **LTE, LTE-Advanced, y LTE-Advanced Pro (4G):** primer sistema realmente orientado a internet, que ofrece tasas de transmisión verdaderamente elevadas.
- **EC-GSM y LTE-M:** evoluciones de las generaciones anteriores para dar cobertura tanto a las necesidades de las personas como las necesidades de la comunicación entre máquinas, el denominado internet de las cosas (IoT), que es lo que habilita la posibilidad de pensar en la revolución de la industria 4.0.
- **NB-IOT y 5G:** nuevas tecnologías de radio para satisfacer las crecientes necesidades del tráfico de banda ancha y del tráfico generado por la máquinas.

Todas estas especificaciones se definen y cierran en documentos técnicos que reciben el nombre de *release*; cada nueva *release* añade nuevas funcionalidades a la *release* anterior o, en algunos casos, define nuevas tecnologías. Por ejemplo, la *release* 99 definió la tecnología de tercera generación (3G); la *release* 8, publicada en diciembre del 2008, fue la base del primer sistema LTE; o la *release* 15 será la formalización técnica del 5G.

#### Información adicional

La cronología detallada y descripción de las *releases* del 3GPP se pueden consultar en el siguiente enlace:  
<http://www.3gpp.org/specifications/67-releases>

### 3. El software en las redes de comunicaciones

#### 3.1. Introducción a la pila de protocolos y sus capas

Cuando originalmente aparecieron las redes de ordenadores, los fabricantes hacían los diseños pensando en que todo el proceso de gestión y operación de red se efectuaría mediante hardware dedicado.

De algún modo, se asumía que los protocolos y los mecanismos empleados serían propietarios, sin necesidad de definir un sistema estándar ni un consentimiento conjunto entre los fabricantes para interactuar los unos con los otros.

Sin embargo, a medida que fueron evolucionando las redes, se observó que si no se planteaba algún tipo de estandarización, una vía común que permitiera interconectar tecnologías y utilizar mecanismos regulados, los esfuerzos de cada fabricante serían demasiado grandes y la competencia no beneficiaría a nadie.

Fue entonces cuando fabricantes como IBM comprendieron que era más viable pasar una buena parte de la carga de la red al software, mucho más flexible y barato de producir y actualizar que el hardware.

De este modo, apareció lo que se conocen como arquitecturas de red organizadas por capas, siguiendo el modelo de referencia OSI (*open systems interconnect*) definido por la International Standards Organization (ISO).

El ejemplo más paradigmático de aplicación de las capas OSI se encuentra en la arquitectura TCP/IP (*transmission control protocol / internet protocol*), pilar fundamental de lo que hoy conocemos como internet y que, posteriormente, describiremos en este material.

#### 3.2. Diseño de redes por capas

La cantidad de funciones que se llevan a cabo en una red de comunicaciones es relativamente compleja. Con el objetivo de reducir la complejidad del diseño de la variedad de funciones necesarias y, como se ha dicho antes, para facilitar la interconexión entre equipos de diferentes redes y distintos fabricantes, **las redes se pueden organizar en una serie de capas o niveles**, cada una situada sobre otra.

El número, el nombre, el contenido de cada capa y las funciones de cada capa difieren de un tipo de red a otra. En todas las redes, el objetivo de cada capa es el de ofrecer determinados servicios en las capas superiores, escondiendo en las capas inferiores los detalles sobre el modo en el que se implementan los servicios ofrecidos.

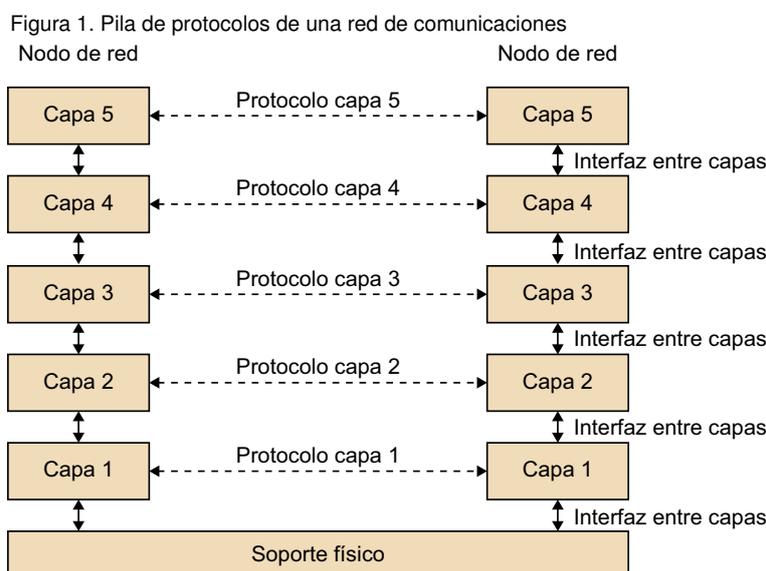
De este modo, la capa de nivel  $N$  de un dispositivo con capacidad de comunicación mantiene comunicación con la capa de nivel  $N$  de otro dispositivo. Estas reglas y convenciones usadas en la capa de nivel  $N$  se denominan **protocolos**.

En esencia, un protocolo es un acuerdo, un conjunto de normas, entre las partes de la comunicación sobre cómo se hace esta. **Es muy importante aclarar que existen protocolos diferentes para cada una de las capas.**

Esta aclaración semántica es fundamental ya que, en el día a día, se tiende a abusar del lenguaje y a comparar protocolos de capas diferentes que hacen funciones distintas, lo que da lugar a conversaciones o discusiones sin sentido. Cuando hablamos de un protocolo de red, es fundamental y absolutamente necesario aclarar en qué nivel o capa de la red se sitúa ese protocolo.

Por poner un ejemplo, no se puede comparar el protocolo HTTP (protocolo de la capa aplicación, la más alta de todas) con IEEE 802.11, que es el estándar que define los protocolos de capa física y de acceso al medio (las 2 capas más bajas de la pila de protocolos, como veremos más adelante) de la tecnología que luego se puede certificar como Wi-Fi. A pesar de esto, todavía es posible escuchar a expertos en tecnología comparando estas tecnologías; es importante evitar esta confusión para la correcta comprensión de las tecnologías de comunicación y de la industria 4.0 en particular.

En la figura 1, se muestra una pila de protocolos: las entidades que utilizan las correspondientes capas en los diferentes ordenadores se denominan **pares** (en inglés, *peers*). **Es decir, los pares se comunican usando un protocolo común.**



En realidad, la información no se transfiere directamente de una capa  $N$  de una máquina a la capa  $N$  de otra máquina:

- 1) En **transmisión**, cada capa pasa la información y el control de esta a la capa inmediatamente inferior, y así sucesivamente hasta llegar a la última capa. Esta última capa se denomina **capa física**, y es en la que se produce la comunicación real.
- 2) En **recepción**, la recepción física de la información se hace en la capa más baja, la capa física. Esta capa procesa la información y la pasa a su capa inmediatamente superior. Así, sucesivamente, hasta llegar a la capa más alta del modelo.

En la figura 1, la comunicación virtual (capa  $N$  con capa  $N$ ) se muestra en líneas punteadas, y la comunicación física o real, en la capa física, el soporte físico.

Entre cada par de capas adyacentes, una encima de otra, se define una **interfaz**. Esta interfaz define las operaciones primitivas y los servicios que la capa inferior ofrece en la capa superior, o viceversa. Cada capa ofrece una colección de funciones perfectamente definidas. De ahí que sea muy fácil reemplazar la implementación de una capa por otra capa con diferente implementación (si queremos cambiar el medio de transmisión de la información, basta con sustituir la capa de nivel 1; por ejemplo, cambiar las líneas telefónicas por canales de satélite, manteniendo el resto del sistema intacto).

El conjunto de capas y protocolos se denomina **arquitectura de la red**. La lista de protocolos, un protocolo por cada capa, se conoce como **pila de protocolos**.

### 3.3. Ejemplo de operativa por capas

Para acabar de asentar el concepto de capas, vamos a describir un ejemplo en el que tengamos una pila de protocolos de 5 niveles y se establezca comunicación entre dos máquinas:

- 1) Consideremos que se produce la comunicación de la capa más alta, la capa 5, que es la que trata con la información útil que puede entender una aplicación concreta. Llamamos  $M$  al mensaje producido por un programa (o proceso) que funciona en la capa de nivel 5.
- 2) La capa 5 envía el mensaje  $M$  a la capa 4. La capa 4 añade una cabecera  $H_4$  antes del mensaje, para identificarlo, y pasa el resultado a la capa 3. La cabecera incluye el control de la información como contador de control de secuencia, para permitir que la capa 4 de la máquina de destino reciba los mensajes en el orden correcto, ya que las capas inferiores no tienen ninguna obligación de mantener la secuencia. En las otras capas, las cabeceras mantienen tamaños, tiempo y otros campos de control.

- 3) En muchas redes no existe límite en el tamaño de los mensajes transmitidos en la capa de nivel 4, pero muchas veces el protocolo de nivel 3 sí que impone restricciones. En consecuencia, la capa 3 debe separar el mensaje que le envía la capa superior en varias unidades menores, denominadas paquetes o fragmentos; la capa de nivel 3 introduce una cabecera de nivel 3 en cada paquete, a la que llamaremos  $H_3$ . En este ejemplo, supongamos que el mensaje  $M$  se divide en dos partes,  $M_1$  y  $M_2$ .
- 4) La capa de nivel 3 decide por qué línea de salida transmitirá los paquetes en la capa de nivel 2.
- 5) La capa de nivel 2 añade una cabecera  $H_2$  en cada fragmento, y ofrece el resultado en la capa de nivel 1 (física) para su transmisión física y real en un ámbito de hardware.
- 6) La capa 1 añade su cabecera  $H_1$ , y transmite el mensaje por el canal o medio físico. En este caso, el mensaje consta de dos fragmentos,  $H_1 + H_2 + H_3 + H_4 + M_1$  y  $H_1 + H_2 + H_3 + H_4 + M_2$ .
- 7) En la máquina que recibe la información, los dos mensajes recorren las diferentes capas en orden ascendente. En cada capa, se procesa la información de la cabecera asociada a dicha capa, se elimina la cabecera y se pasa a la capa superior. Finalmente, el mensaje  $M$  llega a la capa superior, donde puede utilizarse. En este ejemplo, en la capa de nivel 3 se lleva a cabo la unificación de los dos fragmentos, y se asegura que el orden es el adecuado para que el mensaje  $M$  se pueda interpretar en la capa 5.

### 3.4. Funciones que hay que implementar en las capas

La arquitectura de una red por capas ofrece un modo estructurado de diseñar y abstraer las tareas necesarias. Algunas de las tareas que estas capas deben llevar a cabo son:

- 1) **Identificación:** cada nodo de la red debe poder ser identificado de forma única, con el fin de identificar a sus interlocutores. La identificación de los dispositivos debe llevarse a cabo en alguna de las capas.
- 2) **Encaminamiento:** los nodos de la red deben tener mecanismos que permitan enviar la información a cualquier interlocutor de la misma red, y poder encontrar caminos adecuados para encontrar a su interlocutor destinatario de un mensaje cualquiera.
- 3) **Control de errores:** una de las partes más importantes de cualquier comunicación es garantizar que cuando la información llega al destino, esta lo haga sin errores. Hay que notar que los medios de transmisión no siempre son fiables. Por lo tanto, se debe decidir en qué capas se verifican errores y de qué manera lo harán, y si tendrán capacidad para corregir errores.
- 4) **Modo de transferencia:** qué soporte tendrá el protocolo para el envío de información, si se puede enviar información en modo *duplex*, *semiduplex* o *simplex*.
- 5) **Priorización de tráfico:** es posible que sea conveniente priorizar algún tipo de tráfico respecto a otro para satisfacer sus necesidades de calidad de comunicación. Esta priorización debe hacerse en alguno de los niveles de la pila de protocolos.

6) **Control de congestión:** dado que muchas veces las velocidades de transmisión de una red no siempre son homogéneas, y puede haber unos enlaces con más carga que otros, cualquier red debe considerar la posibilidad de disminuir la velocidad a la que se envían los datos y, en el caso de que algún paquete no llegue al destino, se tendrá que llevar a cabo un reenvío de la información. Esta función de control de congestión también debe hacerse en alguno de los niveles de la pila de protocolos.

7) **Tamaño de los paquetes:** como ya hemos comentado anteriormente, enviar mensajes muy grandes no siempre es posible; por lo tanto, se debe decidir qué tamaño máximo podrán tener los paquetes que se envían por la red, fragmentar los mensajes grandes y reagrupar los fragmentos en orden en recepción. Esta tarea también debe llevarse a cabo en algunas de las capas de la pila de protocolos.

**Esta lista de funciones no es completa (ni lo pretende).** Tan solo se quiere transmitir la necesidad de llevar a cabo diferentes funciones en una red de comunicaciones. La estructura en capas, la pila de protocolos, permite el diseño de las diferentes funciones de manera independiente, así como, posteriormente, unir diferentes protocolos de distintas capas usando las interfaces definidas entre capas.

## 4. El modelo de referencia OSI

Actualmente, las dos arquitecturas de red más conocidas son:

- 1) La **arquitectura OSI**, utilizada como modelo teórico, y basada en 7 capas.
- 2) La **arquitectura TCP/IP**, cuyo éxito en el mundo de las redes ha sido enorme y es la base de lo que hoy llamamos internet. Esta arquitectura se basa en 4 capas, y es una simplificación del modelo completo OSI de 7 capas.

Entre los diferentes modelos propuestos por las distintas organizaciones internacionales de normalización en la década de los ochenta, destacó una arquitectura de redes de ordenadores basada en niveles, el modelo OSI (*open systems interconnect*) definido por la ISO (International Standardization Organization).

A finales de los años setenta, la ISO fue definiendo la arquitectura de redes OSI con el fin de promover la creación de una serie de estándares que especificaran un conjunto de protocolos independientes de cualquier fabricante. Pretendía establecer las normas y los estándares para que el software y los dispositivos de diferentes fabricantes pudieran funcionar juntos.

**El modelo OSI está compuesto por 7 niveles o capas**, y en cada nivel se agrupan una serie de funciones o protocolos necesarios para comunicar sistemas. Las capas son:

- 1) **Aplicación**: procesos de la red en la aplicación.
- 2) **Presentación**: representación de los datos.
- 3) **Sesión**: comunicación entre anfitriones.
- 4) **Transporte**: conexión extremo a extremo.
- 5) **Red**: direcciones y mejor ruta.
- 6) **Enlace de datos**: acceso al medio y gestión de enlace.
- 7) **Física (PHY)**: transmisión binaria.

Las capas 1 a 3 son las denominadas **capas inferiores** y son proveedoras de servicios de transporte de las capas superiores. Tratan retos como la codificación; modulación; gestión de acceso al medio; detección y tratamiento de los errores del sistema de transmisión; búsqueda de rutas óptimas; direccionamiento; gestión de congestión; gestión de flujo de transmisión, etc.

Las capas 4 a 7 son las **capas superiores** y su misión es dar servicios al usuario del sistema de comunicaciones. Confían en las prestaciones de los niveles inferiores.

Cuando un usuario o máquina necesitan transmitir datos a un destino, el sistema de red va añadiendo información de control (cabeceras) para cada uno de los servicios que utilizará la red para ejecutar la orden de transmisión.

En las próximas secciones, repasamos las funciones principales de cada capa según el modelo OSI.

#### **4.1. La capa física: PHY**

Es la capa de menor nivel de la pila de protocolos OSI; la más próxima al hardware, la que se encarga de definir las características físicas del medio de transmisión, así como de ejecutar funciones de sincronización en un ámbito físico.

La función de la capa física es proporcionar al nivel de enlace un acceso al sistema de comunicaciones que sea independiente de los detalles técnicos y funcionales de este.

En este nivel, se definen las modulaciones que hay que usar; frecuencias portadoras; formas de onda; anchos de banda y tasas de transmisión de bits; técnicas de multiplexado en tiempo, código, o frecuencia; codificación de fuente y de canal; ecualización, etc.

Son ejemplos de la capa física la norma EIA RS-232-C, utilizada por los puertos serie de los ordenadores personales, EIA-RS-449, ITU-T V.24/V.28/V.35, etc.

En cuanto a las redes locales de difusión, en el nivel físico se suele incluir el subnivel MAC del nivel de enlace (capa 2). Corresponden a este subnivel las especificaciones IEEE 802.3, 802.4, 802.5, etc.

Los equipos que podemos encontrar en este nivel son los siguientes: Hubs Ethernet (LAN), MAU Token Ring (LAN), multiplexores, módems y conmutadores de circuitos (WAN).

#### **4.2. La capa de enlace**

Su principal objetivo consiste en ofrecer a la capa inmediatamente superior (nivel de red) una comunicación fiable de bits a través de un medio físico de transmisión.

Sus funciones principales son:

1) **Sincronización en un ámbito de trama:** agrupa los bits en tramas, la mínima unidad de información con la que trabaja el nivel de enlace, y establece delimitadores de origen y destino para que sea detectada correctamente en la recepción.

2) **Control de flujo:** el dispositivo transmisor y el receptor deben ponerse de acuerdo en el ritmo de transmisión de datos, con el fin de no saturar las memorias del nodo receptor y, así, no perder información.

3) **Dirección:** si existe más de un posible destino para un mensaje, es necesario identificarlo perfectamente. Es importante no confundir este direccionamiento con el direccionamiento de enrutado. El protocolo de enrutado se preocupa de definir rutas extremo a extremo, mientras que el direccionamiento en la capa 2 se refiere al siguiente salto entre un transmisor y un receptor; puede tratarse de un dispositivo intermedio haciendo de encaminador, por ejemplo. La dirección MAC que tenemos en nuestros ordenadores o teléfonos móviles y que nos permite, por ejemplo, filtrar los terminales aceptados en un punto de acceso Wi-Fi, es la dirección utilizada en un ámbito de capa 2.

4) **Gestión del enlace:** todo el proceso de inicio, mantenimiento y finalización de la transmisión requiere un considerable esfuerzo de gestión y coordinación. También se proporcionan los medios para activar, mantener y desactivar el enlace.

5) **Control de acceso al medio (MAC):** funcionalidad necesaria en redes de difusión (radio) o con bus compartido, en la que todos los terminales comparten un medio único físico (en banda base, sin multiplexar). Cuando varios equipos acceden simultáneamente, se pueden generar conflictos, también denominados colisiones. Es necesario un control de acceso al medio en redes *broadcast*.

El IEEE divide la capa de enlace en dos subcapas:

1) **Subcapa MAC**, que se ocupa de resolver el acceso al medio y es la subcapa inmediatamente superior a la capa física.

2) **Subcapa LLC** (control lógico de enlace), inmediatamente superior a la subcapa MAC, y cumple una función equivalente a la de capa de enlace en las líneas punto a punto: es responsable de la identificación de la forma lógica de los diferentes tipos de protocolos y su encapsulación.

Ejemplos de protocolos de la capa de enlace son: SDLC de IBM, HDLC del ISO y el conjunto de protocolos LAP (capa de enlace en ITU-T X.25).

Los protocolos más representativos de la subcapa MAC, citados anteriormente, son IEEE 802.3 (también conocido como Ethernet), 802.4 (Token Bus), 802.5 (Token Ring) y ANSI X3T9.5/ISO 9314 (FDDI). El protocolo de la subcapa LLC para todas las redes locales de difusión es IEEE 802.2.

Los equipos que podemos encontrar en este nivel son: tarjetas de red Ethernet, interruptores Ethernet y Token Ring (LAN), interruptores de conmutación de paquetes *frame relay* o ATM (WAN).

#### Información adicional

La dirección MAC se compone de 12 símbolos hexadecimales, con un formato de este tipo: 00:00:00:00:00:00. Esta dirección es única en el mundo para cualquier dispositivo con capacidad de conectarse a internet.

#### Información adicional

El IEEE es el Institute of Electrical and Electronic Engineers, la mayor organización en un ámbito mundial de ingenieros electrónicos y de telecomunicación, que vela por promover las tecnologías de la información y la ingeniería.

### 4.3. La capa de red

El objetivo funcional fundamental de la capa de red es encaminar los paquetes (unidad de información del nivel de red) desde un origen a un destino, extremo a extremo, mediante los nodos de la red.

Para conseguirlo, la capa de red debe conocer la topología de la red, intentando evitar las conexiones congestionadas y gestionando cuestiones como la ubicación de los ordenadores origen y destino en subredes diferentes.

No obstante, y como en las otras capas, la misión principal de la capa de red es proporcionar servicios en la capa superior, el nivel de transporte.

Los servicios que ofrece la capa 3, en una visión resumida, son los siguientes:

- 1) **Encaminamiento:** la capa de red debe determinar cómo encaminar los paquetes del origen al destino a través de una ruta extremo a extremo. Para ello, utilizará una tabla con información sobre los destinos conocidos.
- 2) **Determinación de la ruta:** funcionalidad muy vinculada a la anterior. Consiste en elegir la mejor ruta entre las disponibles. La capa de red debe conocer la topología de la subred en términos de ciertos parámetros técnicos (número de saltos, ancho de banda, etc.) para poder elegir el mejor recorrido hasta el destino.
- 3) **Control de congestión:** si en un momento dado hay demasiados paquetes presentes en la subred, ellos mismos se obstruyen, lo que da lugar a un cuello de botella y a una degradación del rendimiento. Para evitar la congestión, el nivel de red implementa una serie de mecanismos. El control de congestión y el encaminamiento están estrechamente relacionados.
- 4) **Fragmentación de paquetes:** adapta la longitud de los paquetes a las limitaciones de las capas inferiores.
- 5) **Interconexión de redes:** cuando la fuente y el destino se encuentran en redes diferentes, surgirán una serie de problemas (encaminamiento o redes con diferentes protocolos) que deberá resolver la capa de red.

Algunos ejemplos de protocolos utilizados en la capa de red son ITU-T X.25 y X.75 (pasarelas entre redes X.25), el IPv4 y su sucesor IPv6, el protocolo de encaminamiento OSPF o la capa de red en ATM.

Los equipos que trabajan en este nivel son los encaminadores (*routers*).

#### 4.4. La capa de transporte

La función principal del nivel de transporte es aceptar los datos de las capas superiores (muchas veces, las propias aplicaciones de usuario); fragmentarlos, si es necesario, en unidades más pequeñas; pasarlos al nivel de red; y garantizar que lleguen al destino de manera segura y económica, independientemente de la red o de las redes físicas que se encuentren en uso.

El diálogo entre entidades de transporte es de extremo a extremo y no por saltos, como en los de niveles inferiores.

Dado que el objetivo de la red de comunicación es posibilitar un diálogo directo entre sistemas finales, **el nivel o la capa de transporte podría considerarse el corazón de toda la jerarquía.**

Desde el punto de vista del usuario que necesita conectar varios equipos remotos, el servicio de transporte es el que resuelve su problema.

Las funciones principales de la capa de transporte son:

- 1) Establecer, mantener y acabar las conexiones entre dos ordenadores principales o entre un servidor y un ordenador principal.
- 2) Controlar el flujo extremo a extremo entre dos estaciones finales.
- 3) Controlar la congestión producida en los encaminadores intermedios que forman parte del recorrido entre el origen y el destino.
- 4) Fragmentar la información de la capa de sesión en segmentos más pequeños.
- 5) Recomponer la información en el destino.
- 6) Mejorar la calidad de servicio suministrada por la capa de red. Garantiza una transmisión fiable, sin errores, extremo a extremo, independiente del tipo de red.
- 7) Asegurar que los datos llegan ordenados, sin pérdidas, sin errores y sin duplicaciones al destinatario.
- 8) Multiplexar diferentes conexiones de transporte sobre una misma conexión de red, utilizando uno o más puertos de salida para la misma comunicación.

Entre los protocolos del nivel de transporte, podemos destacar TCP y UDP (TCP/IP), SPX (Netware), etc.

No suele haber dispositivos en la red que trabajen en el nivel 4, exceptuando los terminales y servidores finales de una red. No obstante, los encaminadores con funciones cortafuegos (*firewalls*) también trabajan en este nivel.

#### 4.5. La capa de sesión

Sus funciones son:

- 1) Administra el intercambio de datos, asegurando la entrega correcta de la información.
- 2) Se encarga de establecer, mantener y cerrar el diálogo entre los ordenadores principales que se están comunicando. Esto incluye el establecimiento, la detección y la sincronización de los dos ordenadores principales (servicio de conexión, sincronismo, etc.).
- 3) Controla el orden de intervención de los interlocutores en ciertos diálogos, indicando quién debe emitir en cada instante.
- 4) Mejora el servicio de la capa de transporte: se encarga de la resincronización de la transferencia, lo que permite a los usuarios la vuelta a un estado anterior después de un problema (por ejemplo, para recuperar una sesión después de un *reset*, volver a un estado conocido, etc.).

Como ejemplos de protocolos de este nivel, tenemos: FTP, TELNET, SMTP, TFTP, RPC38 (que es un mecanismo para efectuar llamadas en procedimientos remotos), SNMP, etc.

#### 4.6. La capa de presentación

El principal objetivo de la capa de presentación es eliminar los problemas que puedan surgir al comunicar datos entre diferentes arquitecturas.

Cada arquitectura de ordenadores puede tener su propia estructura de representación interna de los datos, que no tienen por qué ser compatibles. El trabajo de la capa de presentación se concreta en una tarea de traducción, de modo que se asegura el entendimiento entre sistemas diferentes mediante acuerdos y conversiones de datos.

Básicamente, la capa de presentación recibe datos de la capa de aplicación y los codifica antes de su transmisión, para adaptarlos a la manera de codificación propia del sistema de transmisión. Ya en el destino, los descodifica según el sistema de representación que se utilice en el mencionado extremo. Entre sus funcionalidades, podemos destacar las siguientes:

- 1) Define la sintaxis y la semántica de la información que se intercambia.
- 2) Compatibiliza arquitecturas con estructura de datos diferentes.
- 3) Describe el formato de los datos que se intercambiarán entre las aplicaciones:

- Comprime los datos (reducción tamaño): elimina aquellos componentes superfluos de los mensajes que van a transmitirse. Después, pueden ser añadidos directamente en el extremo receptor.
- Encripta la información (privacidad): codifica la información transmitida, de manera que una hipotética escucha del sistema no pueda recuperar el mensaje original si no conoce el código de descodificación.

En protocolos de este nivel, podemos destacar: RFS, SMB, NCP, NFS, etc.

#### 4.7. La capa de aplicación

Es la capa superior del modelo de referencia OSI, que define la interfaz y los protocolos que utilizarán los procesos de los usuarios o aplicaciones.

El objetivo de esta capa es proporcionar:

- 1) Procedimientos precisos que permitan a los usuarios ejecutar los pedidos relativos a sus propias aplicaciones.
- 2) Un medio para que los procesos de las aplicaciones accedan al entorno OSI, utilizando los servicios que ofrece la capa de presentación para las necesidades de comunicación.
- 3) Interacción entre aplicaciones e intercambio de datos.

Ejemplos de protocolos de la capa de aplicación son: FTAM (transferencia de ficheros), X.400 (correo electrónico) y X.500 (directorio) del CCITT; también destacan las normas ISO 8649, 8650 y 8571.

Los equipos que encontramos en este nivel son los terminales (clientes y servidores) y las pasarelas de aplicación o *proxy*.

## 5. El modelo de referencia TCP/IP

El **modelo de referencia TCP/IP** es una particularización y simplificación práctica del modelo genérico y teórico OSI descrito en el apartado anterior. Es el modelo utilizado por todos los dispositivos conectados a internet hoy día.

En el **modelo TCP/IP**, se pueden distinguir **cuatro capas**:

- 1) **Capa interfaz de red**, que incluye las capas 1 y 2 del modelo de referencia de la OSI.
- 2) **Capa de red o internet (protocolo IP)**, que coincide con la capa 3 del modelo de referencia OSI.
- 3) **Capa de transporte (protocolos TCP/UDP)**, que coincide con la capa 4 del modelo de referencia OSI.
- 4) **Capa de aplicación**, que incluye los niveles 5, 6 y 7 de la torre OSI.

Según este modelo, el procedimiento es el siguiente:

- 1) Los datos de información del nivel aplicación son encapsulados en la capa de transporte, a la que se añade la cabecera del protocolo TCP. De este modo, se constituye la unidad de información denominada **segmento**.
- 2) Cuando el segmento es enviado al nivel de red, es encapsulado dentro de la cabecera del protocolo IP, en el que se indican las direcciones IP de la unidad de información denominada **paquete** en este nivel.
- 3) Este paquete es enviado a la tarjeta de red, y aquí es encapsulado según las normas del protocolo del nivel de enlace. Normalmente, añade una cabecera de protocolo de enlace al principio del paquete.
- 4) En muchos protocolos, también se añade una cola al final del paquete de datos que sirve para la detección de errores al final del paquete. La unidad de información recibe aquí el nombre de **trama**.
- 5) Por último, los datos son enviados por el medio de transmisión como **impulsos electromagnéticos** o **bits**, según la capa física definida.

A continuación, describimos cada una de las capas.

## 5.1. La capa interfaz de red

Esta capa es una especie de «caja negra» que engloba las funciones de las capas física y enlace del modelo OSI. El modelo TCP/IP solo especifica que esta capa debe ser capaz de conectar el dispositivo principal a la red, por medio de algún protocolo que permita enviar paquetes IP.

## 5.2. La capa de red (internet)

Esta capa es el eje de la maquinaria que mantiene unida la red. Sus funciones encajan completamente en la especificación OSI, es decir, **encaminamiento y control de congestión**, principalmente.

El principal protocolo de la capa de red en internet es IP. Las especificaciones de IP establecen que es posible que paquetes de una misma conversación lleguen a su destino en diferente orden del que fueron depositados en la red. Este funcionamiento se denomina transmisión en modo datagrama.

En este caso, la reordenación es responsabilidad de las capas superiores (este papel lo asume el eficaz protocolo de nivel de transporte de internet, TCP, como veremos más adelante).

Con respecto al encaminamiento, IP establece un esquema de direcciones jerárquico para el reconocimiento de redes y subredes. La versión original de IP fue IPv4, con capacidad de direccionar dispositivos usando direcciones de 32 bits. Sus carencias respecto al explosivo crecimiento de la red han motivado la definición de un sucesor IPv6, que se está implantando gradualmente. IPv6 se basa en un direccionamiento de 128 bits, lo que permite direccionar un número realmente elevado de dispositivos.

### Información adicional

Con los 128 bits de IPv6, se pueden direccionar más de 340 sextillones de dispositivos; exactamente: 340.282.366.920.938.463.463.374.607.431.768.211.456.

El hecho de que IPv6 ofrezca funcionalidades avanzadas y direcciones largas tiene implicaciones en un ámbito de dispositivos. Si queremos que los dispositivos sean sencillos y baratos, es necesario que tengan que gestionar poca información. Por este motivo, el 6LoWPAN (**IPv6 over low power wireless area networks**) constituye una versión simplificada de baja complejidad para poder usar IPv6 en dispositivos de bajo coste. Por este motivo, muchos de los dispositivos de bajo coste equipados con sensores y actuadores están siendo equipados con tecnologías de comunicación compatibles con 6LowPAN.

Los protocolos de nivel 3 se dividen en protocolos encaminados y de encaminamiento:

- 1) **Protocolos encaminados:** son los protocolos que llevan información de usuario desde un origen a un destino.
- 2) **Protocolos de encaminamiento:** son los protocolos de control que utilizan los nodos de la red para conocer las rutas hacia los destinos y elegir las mejores.

El nivel de red de TCP/IP también define dos protocolos auxiliares que ayudan a IP a llevar a cabo sus funciones: **ARP** (*address resolution protocol*), que mantiene la correspondencia entre direcciones lógicas y físicas; e **ICMP** (protocolo de control de mensajes y errores).

### 5.3. La capa de transporte

Esta capa también encaja perfectamente en la definición del nivel de transporte del modelo de referencia OSI.

Su función es ofrecer a las aplicaciones del nivel superior un canal de comunicaciones extremo a extremo (denominado *socket* en UNIX) en nivel de transporte.

El nivel de transporte define un sistema de multiplexación y demultiplexación de aplicaciones, de manera que cada aplicación de red tiene un número asociado denominado puerto, que permite al protocolo de transporte identificarla.

Existen dos protocolos diferentes:

- 1) **TCP** (*transmission control protocol*), que ofrece un servicio fiable orientado a conexión, con el que los paquetes (denominados segmentos en este nivel TCP/IP) llegan ordenados y sin errores. Efectúa retransmisiones, control de flujo y de congestión extremo a extremo (para aplicaciones de datos).
- 2) **UDP** (*user datagram protocol*), que ofrece un servicio de datagramas no orientado a conexión y no fiable. UDP no hace retransmisión de paquetes, ni control de flujo ni de congestión, tareas que quedan encomendadas a los servicios de nivel superior que usen este protocolo. Solo detecta errores extremo a extremo. Las aplicaciones típicas que utilizan UDP son aquellas en las que la velocidad de transmisión interesa más que la precisión en la entrega, como el envío de voz o vídeo (para aplicaciones en tiempo real).

## 5.4. La capa de aplicación

El nivel de aplicación es el que entra en contacto con los usuarios finales. Tiene la particularidad de que incluye cualquier función o servicio que se utilice en la red y que no se suministre en los niveles anteriores.

En el modelo TCP/IP, esta capa aglutina las funciones de las capas de sesión, presentación y aplicación del modelo OSI. Se ha constatado empíricamente que las capas de sesión y presentación son de poca utilidad, debido a que su contenido es escaso y redundante, por lo que la aproximación adoptada por el modelo TCP/IP parece más acertada.

Así, se puede resumir la funcionalidad de la capa de aplicación en:

- 1) Un conjunto de servicios de soporte necesarios para el funcionamiento de las aplicaciones, tales como compresión de información (ZIP o RAR); seguridad y confidencialidad (SSL); gestión de red (SNMP); gestión de conversión; y servicio de resolución de nombres de dominios (DNS).
- 2) Las aplicaciones propias que ofrecen servicios a los usuarios, tales como correo electrónico (POP3, SMTP, IMAP), transferencia de ficheros (FTP y SFTP), World Wide Web (HTTP y HTTPS), terminal remoto (Telnet), etc.

## Resumen

En este material, hemos presentado los conceptos básicos de las redes de comunicaciones. Hemos empezado describiendo los elementos de una red y los tipos de redes existentes.

Posteriormente, hemos introducido el papel del software en la gestión de una red; la definición de **protocolos** permite a los elementos de una red comunicarse entre ellos, de manera independiente de la naturaleza diferente de su hardware.

Hemos presentado también el modelo de referencia OSI para definir la pila de protocolos. Aunque en la práctica el modelo no tiene gran aplicación, sus fundamentos teóricos ayudan a comprender las funciones necesarias que deben implementarse en toda red de comunicaciones.

Finalmente, hemos revisado el modelo TCP/IP, sobre el que se fundamentan las comunicaciones de internet. Este modelo es la base de todas las comunicaciones que se llevan a cabo hoy día. Como veremos más adelante en los próximos materiales, la mayoría de los estándares de comunicaciones definen las capas físicas y capa MAC (control de acceso al medio), y suelen ser compatibles con los protocolos TCP/UP para el transporte de datos y las funciones de red. En los casos en que no lo son, suelen existir protocolos que permiten la adaptación a TCP/IP.

Aunque brevemente, también hemos introducido el concepto de 6LowPAN como una adaptación *lightweight* de IPv6 para su uso en dispositivos de bajo coste y ultrabajo consumo de energía.