Redes Locales e Internet

Conceptos y Práctica

educàlia

Arturo Mora Rioja
Mª Mercedes Rodríguez Villafáfila

Redes Locales e Internet

Conceptos y práctica

Arturo Mora Rioja

Mª Mercedes Rodríguez Villafáfila

educàlia

Primera edición, 2014

Autores: Arturo Mora Rioja y Mª Mercedes Rodríguez Villafáfila
Maquetación: Mª Mercedes Rodríguez Villafáfila
Diseño de cubierta: Arturo Mora Rioja
Imprime: Escenarigràfic S.L.
ISBN: 978-84-942836-2-6
Depósito Legal: v-2067-2014

Printed in Spain / Impreso en España.

Educàlia Editorial S.L.
Avda. Jacarandas nº 2 - loft 326-327 - 46100 Burjassot - València
Tel: 96 327 35 17
e-mail: educaliaeditorial@e-ducalia.com
http://www.e-ducalia.com/material-escolar-colegios-ies.php

PRÓLOGO

Cuando el laboratorio del Dr. Leonard Kleinrock en UCLA (Universidad de California en Los Ángeles) consiguió enviar el primer mensaje sobre la red ARPANET el 29 de octubre de 1969, ni ellos ni ningún otro ser humano podía imaginar la importancia que las redes de ordenadores y especialmente la sucesora de ARPANET, Internet, iban a cobrar en las décadas siguientes. Hoy en día estamos permanentemente conectados a todo tipo de redes en nuestros hogares, en el trabajo, a través de nuestros teléfonos móviles y hasta cuando encendemos el televisor. A medida avanza el siglo XXI se puede decir que más que usar redes vivimos en ellas.

Este libro ofrece información estructurada orientada a la comprensión de diversos aspectos fundamentales sobre las redes de ordenadores en general y sobre Internet en particular: cómo funcionan, qué criterios de diseño existen, qué pasos seguir de cara a su implantación, de qué manera se gestionan, cuál es el fundamento teórico subyacente. En los capítulos principales del libro, capítulos 6 y 7, en los que se sientan las bases del funcionamiento de *routers* y *switches*, se hace especial incapié en la parte práctica de la administración de estos dispositivos.

Si bien esta obra puede aplicarse a varios niveles, desde la Formación Profesional de Grado Medio hasta el mundo universitario y profesional, el núcleo de contenidos está basado en el Real Decreto 1629/2009, de 18 de noviembre, de enseñanzas mínimas del título de Técnico Superior en Administración de Sistemas Informáticos en Red, y por el desarrollo del currículo definido en el Decreto 12/2010, de 18 de marzo, de la Comunidad de Madrid. No obstante el grueso de los contenidos se ha ampliado sustancialmente, y su organización se ha visto beneficiada por la amplia experiencia docente de los autores en este campo, siendo especialmente notable el esfuerzo por ofrecer información vigente y actualizada en un área de trabajo que evoluciona a velocidades vertiginosas.

Los autores:

Arturo Mora Rioja
Profesor de Enseñanza Secundaria
Departamento de Informática y Comunicaciones, IES Clara del Rey, Madrid
Ingeniero Técnico en Informática de Sistemas, Universidad Politécnica de Madrid

Mª Mercedes Rodríguez Villafáfila
Profesora de Enseñanza Secundaria
Departamento de Informática y Comunicaciones, IES Clara del Rey, Madrid
Licenciada en Ciencias Físicas, Universidad de Salamanca
MSc in Information Systems, University of Portsmouth

ÍNDICE GENERAL

Capítulo 1: Caracterización de redes

1. Telecomunicaciones

El intercambio de información ha permitido establecer la comunicación entre seres humanos desde el comienzo de los tiempos, no sólo gracias al lenguaje sino a una amplia variedad de símbolos y códigos. De acuerdo con la tercera acepción de la Real Academia Española, **comunicación** es la "transmisión de señales mediante un código común al emisor y al receptor". En esa categoría podemos incluir desde las señales de tráfico hasta el intercambio de información en una red de satélites, pasando por las facturas de compra.

Según la Unión Internacional de Telecomunicaciones, **telecomunicación** es "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". La informática, ciencia que estudia el tratamiento automatizado de la información, se ha servido de las telecomunicaciones (en muchos casos ambas áreas se han integrado unitariamente) para conseguir sus cometidos.

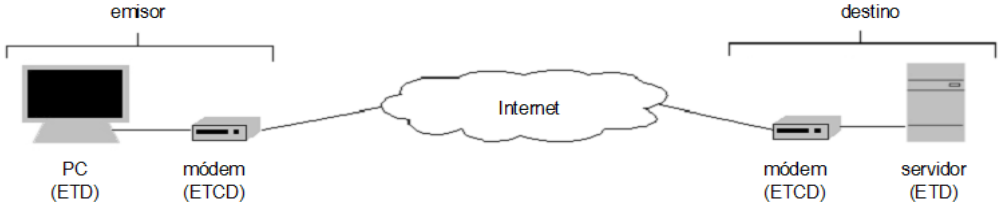
1.0.1. Evolución histórica

Fecha	Evento
Antes de 1900	Mensajeros a pie o a caballo, señales de humo, paloma mensajera o telégrafo
1890s	Invención del teléfono (Alexander Graham Bell). Expansión del servicio telefónico
1901	Primera transmisión inalámbrica transatlántica (Guglielmo Marconi)
1920s	Radio AM
1939	Radio FM
1940s	Desarrollo de la radio y las microondas fomentada por la Segunda Guerra Mundial
1948	Se publica "Teoría de la Comunicación Electrónica" (Claude Shannon)
1960s	Computadores *mainframe*
1962	Redes de conmutación de paquetes (Paul Baran)
1967	Publicado el primer informe sobre ARPANET (Larry Roberts)
1969	Establecimiento de ARPANET en UCLA, UCSB, U-Utah y Stanford
1972	Creación de *software* para envío de correo electrónico (Ray Tomlinson)
1973	Desarrollo de la arquitectura TCP/IP (Bob Kahn y Vint Cerf)
Finales 1970s	Las compañías usan arquitecturas propietarias
1981	Se comienza a utilizar el término Internet
1982	ISO presenta el modelo OSI
1984	Se introduce el Servicio de Nombre de Dominio (DNS)
1991	Desarrollo de código para la *World Wide Web* (Tim Berners-Lee)
1993	Se presenta Mosaic, primer navegador web con interfaz de usuario gráfica
1994	Se presenta Netscape Navigator
Finales 1990s	Crecimiento exponencial de usuarios de Internet

2. Elementos de un sistema de comunicaciones

El objetivo de un sistema de comunicaciones es intercambiar información entre dos entidades, para lo que utiliza medios físicos (dispositivos tangibles) y lógicos (*software* de transmisión y control). Se compone de los siguientes elementos:

1. Fuente o emisor. Genera los datos a transmitir. Es un ETD (Equipo Terminal de Datos) o DTE (en inglés, *Data Terminal Equipment*).
2. Transmisor. Da a los datos un formato que permita su transmisión. Es un ECD (Equipo de Comunicación de Datos, también llamado ETCD – Equipo Terminal del Circuito de Datos) o DCE (en inglés, *Data Communications Equipment*).
3. Sistema o línea de transmisión. Transporta la información.
4. Receptor. Transforma la señal recibida en los datos originales. También es un ECD.
5. Destino. Lee los datos del receptor. También es un ETD.



3. Redes de ordenadores

La conexión de ordenadores en red formando un sistema de comunicaciones es una práctica extendida en la actualidad debido a las ventajas que ofrece:

- Disponibilidad de recursos. Aplicaciones, servicios e información se encuentran a disposición de quien lo necesite.
- Fiabilidad.
  - Al encontrarse duplicada en la red, la información se puede recuperar desde fuentes de suministro alternativas.
  - Al disponerse de varios procesadores, si un equipo falla los trabajos pendientes se pueden ejecutar en otro.
- Bajo coste. De forma general, un diseño de red basado en ordenadores personales y de tamaño medio ofrece una relación coste-rendimiento superior que si se usan *mainframes*.
  - Se sustituyen los sistemas centralizados por los distribuidos.
  - Se sustituye el modelo jerárquico por el cliente-servidor.
- Escalabilidad. El sistema puede crecer incorporando nuevos procesadores al mismo.
- Facilidad de colaboración entre recursos. Se permite trabajar juntos a recursos humanos y materiales físicamente alejados.

  Los elementos habituales de una red de ordenadores son:
  - Servidor. Ofrece servicios a las máquinas cliente. Dichos servicios pueden ser de mensajería, correo electrónico, archivos, bases de datos, impresión, etc.
  - Cliente. También llamado estación de trabajo (*workstation*). Puesto de red que ejecuta aplicaciones de usuario y utiliza los servicios que ofrecen otros equipos (servidores).
  - Sistema operativo de red. Soporta los protocolos de comunicaciones que permiten a los distintos equipos conectarse entre sí y acceder a los recursos compartidos.
  - Conexiones físicas. Tarjetas de red, cableado, *switches*, *routers*, etc.

4. Tipos de redes

4.1. Por extensión geográfica

- PAN (*Personal Area Network*, red de área personal). Distancias muy cortas. Integra pequeños dispositivos como teléfonos móviles o PDAs. Según autores, es un subtipo de LAN.

- LAN (*Local Area Network*, red de área local). No suele exceder el edificio en que está instalada, pudiendo cubrir otros edificios cercanos. Generalmente es de explotación privada.

- MAN (*Metropolitan Area Network*, red de área metropolitana). Se encuentra en una localidad, y está sujeta a regulaciones administrativas.

- WAN (*Wide Area Network*, red de área extensa). Abarca varias ciudades, regiones o países. De explotación pública en muchos casos.

4.2. Por propietario

- Públicas. Están implantadas y disponibles para su uso por parte de todo tipo de usuarios. Son propiedad del estado o de empresas de telecomunicaciones, denominadas coloquialmente *telcos,* que ofrecen servicios a particulares y empresas.
  - » Reducción de costes de gestión y mantenimiento.
  - » Evolución tecnológica garantizada.
  - » Diseño de red no personalizado.
  - » Falta de control y supervisión del tráfico de la red.

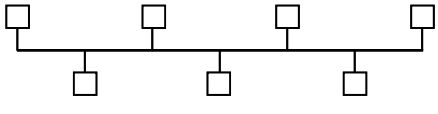
- Privadas. Se fabrican para un propósito específico y son de uso privado.
  - » Diseño a medida.
  - » Control y capacidad de explotación.
  - » Coste elevado.
  - » Envejecimiento de equipos, desfase tecnológico.

- Privadas virtuales (VPN – *Virtual Private Network*). Tecnología que permite extender una LAN privada sobre una red pública. Sus funciones pueden incluir el acceso de un cliente a una LAN empresarial o la conexión entre sedes corporativas remotas.
  - » Mismas ventajas que las redes públicas.
  - » La disponibilidad y eficiencia depende de la red pública.
  - » Menor nivel de seguridad que en una red privada.

4.3. Por topología

La topología define la estructura física o lógica de una red.

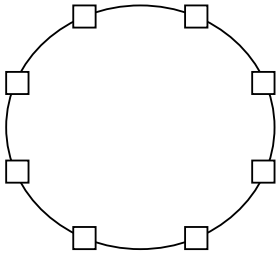
- Bus. Utiliza un enlace de cable (*backbone*) al que todos los equipos se conectan de forma directa. Requiere *n-1* segmentos de cable para conectar *n* nodos.



  - » Bajo coste, requiere poco cableado.

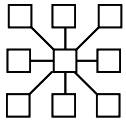
  - » Si falla una estación, el resto no se ve afectado.
  - » Si falla un segmento de cable, el bus falla.

- Anillo. Enlaza los distintos equipos de la red de forma secuencial y cerrada. Requiere *n* segmentos de cable para conectar *n* nodos.



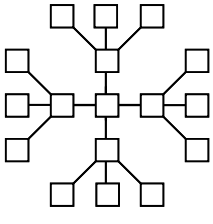
  - » Mejora el modelo en bus.
  - » Si falla un equipo, el enlace se reconfigura con un bypass de manera que exista continuidad en el anillo.
  - » Si falla un segmento de cable, el anillo falla. En ese caso se puede implementar un doble anillo redundante.

- Estrella. Conecta los equipos con un nodo central. Requiere *n-1* segmentos de cable para conectar *n* nodos.



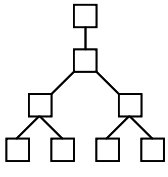
  - » Si falla una estación no afecta al resto.
  - » Flexibilidad para añadir o eliminar equipos
  - » Si falla el nodo central se inutiliza toda la red.

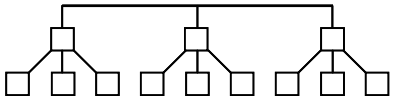
- Estrella extendida. Se conectan varias estrellas entre sí. Requiere *n+m-1* segmentos de cable para conectar *n+m* nodos.



  - » Cableado más corto que en el modelo en estrella.
  - » Cada nodo central conecta menos dispositivos.
  - » El fallo del nodo principal aisla las estrellas secundarias. El de un nodo secundario inutiliza parte de la red.

- Jerárquica o en árbol. Estrella extendida con un nodo dominando la topología completa. Al igual que la estrella extendida, requiere *n+m-1* segmentos de cable para conectar *n+m* nodos.

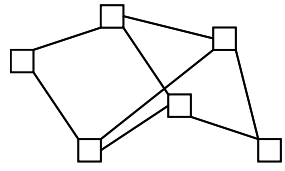




- Árbol binario. Cada nodo se divide en dos enlaces.
- Árbol *backbone*. Se parte de un enlace troncal de nodos o *backbone*.

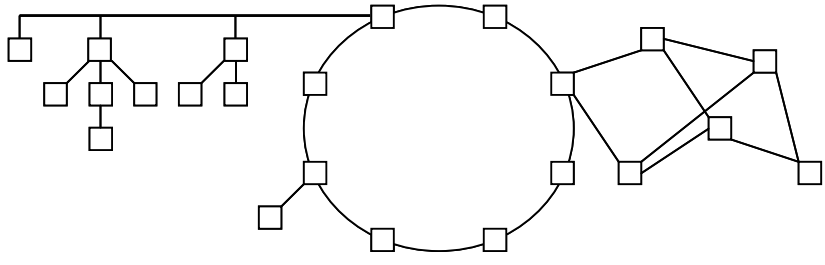
- Malla. Cada equipo tiene sus propias conexiones con los demás. Es irregular y no sigue un patrón fijo. La malla puede ser completa o sólo parcial. Para una malla completa de *n* nodos el número de segmentos de cable se calcula con la siguiente fórmula:

$$\sum_{k=1}^{n-1} k = 1 + 2 + \ldots + (n-1) = \frac{n \cdot (n-1)}{2}$$



  - » Si una ruta falla, hay alternativas.
  - » Alto coste, necesidad de mucho cable.

- Híbrida. Mezcla varias de las topologías anteriores.



4.4. Por el tipo de enlaces entre nodos de red

- De difusión (*broadcast*) o multipunto. Cada equipo envía su información a todos los nodos, siendo el destinatario el encargado de captar e interpretar dicha información. Configuración típica en redes en bus, anillo, estrella con un *hub* como dispositivo central o inalámbricas.

  Tipos de transmisión en redes de difusión:

  - *Broadcast*. Cada equipo envía sus datos hacia todos los demás. Las estaciones de trabajo no siguen ningún orden para utilizar la red (el primer mensaje que llega es el primero que se envía).

  - Transmisión de *tokens*. Los equipos reciben testigos (*tokens*) que les informan sobre cuándo pueden transmitir, retransmitiendo el *token* cuando finaliza la transmisión o bien si no hay nada que transmitir.

- Conmutadas o punto a punto. La conmutación es la técnica que permite interconectar dos nodos cualesquiera de una red, aunque se encuentren alejados. Se establece una vía de conexión entre el emisor y el receptor de la transmisión.

  - Conmutación de circuitos. Se establece a priori y de forma exclusiva el circuito físico (camino único dedicado), aunque tramos del mismo se compartan con otras transmisiones. Eficiente si existe transmisión continua en ambos sentidos. Si no, la línea permanece ocupada aunque no haya transmisión efectiva.Implica una secuencia de tres pasos:
    1. Establecimiento del circuito.
    2. Transferencia de información.
    3. Liberación del circuito.

- Conmutación de mensajes. El mensaje a enviar incorpora información de direccionamiento (origen y destino), y va pasando de nodo a nodo. Cada uno de ellos almacena el mensaje y lo retransmite cuando encuentra un camino libre. Se utiliza con mensajes pequeños.

  Existe la posibilidad de enviar mensajes multipaquete: en cada nodo el mensaje completo se recupera y segmenta de nuevo antes de ser enviado al nodo siguiente, con el consiguiente retardo en el envío.

- Conmutación de paquetes. Si el mensaje es demasiado grande, se divide en paquetes formados por cabecera y datos de usuario. En la cabecera, además del origen y el destino, aparece el número de secuencia del paquete e información adicional como el acuse de recibo, si este se solicita.

  - Datagrama. Transmisión de paquetes desordenada y por circuitos independientes (cada paquete puede tomar una ruta distinta). No orientado a conexión. Es barato, pero poco eficiente.
  - Circuito virtual. Se establece una conexión lógica entre origen y destino.
    - Permanente (C.V.P.). Ruta preestablecida entre cada par de nodos, pero no dedicada (se comparte con otras transmisiones mediante multiplexación en el tiempo).
    - Conmutado (C.V.C.). Ruta establecida en cada transmisión entre nodos (puede no ser la misma en dos transmisiones distintas entre los dos mismos nodos).

4.4.1. Comparación por tipo de enlace

Auque históricamente se ha identificado a las LAN como redes de difusión y a las WAN como redes de conmutación, hoy en día se puede encontrar una gran cantidad de LAN conmutadas. En todo caso sí se puede afirmar que una WAN de difusión sería muy poco eficiente, debido a las grandes distancias que cubre.

Difusión	Conmutación
Software simple No implementa algoritmos de encaminamiento. Control de errores extremo a extremo.	*Software* complejo Algoritmos de encaminamiento complicados. Control de errores extremo a extremo y entre nodos intermedios
Si la estación receptora reconoce su dirección en el campo de destino, recibe el mensaje	Además, si la estación receptora no reconoce la dirección de destino como la suya, ha de reenviar el mensaje
Un único medio de transmisión soporta todos los mensajes de la red.	Varias líneas de comunicación pueden funcionar en paralelo.
Necesidad de líneas de alta velocidad	Se pueden usar líneas de baja velocidad
Retrasos debidos a las esperas para ganar el acceso al medio	Retrasos debidos a la retransmisión del mensaje entre varios nodos intermedios

5. Tipos de transmisión

- Por tipo de destinatario.
  - *Unicast*. La información se dirige a una máquina.
  - *Multicast*. La información se dirige a varias máquinas concretas.
  - *Broadcast*. La información se dirige a todas las máquinas.

- Por uso de la línea.
  - *Simplex*. Comunicación en un solo sentido.
  - *Half-duplex* o semidúplex. En ambos sentidos de forma exclusiva.
  - *Full-duplex* o dúplex. En ambos sentidos de forma simultánea.

6. Dispositivos de red

Se verán con más detalle en sucesivas unidades de trabajo. No obstante los más habituales son:

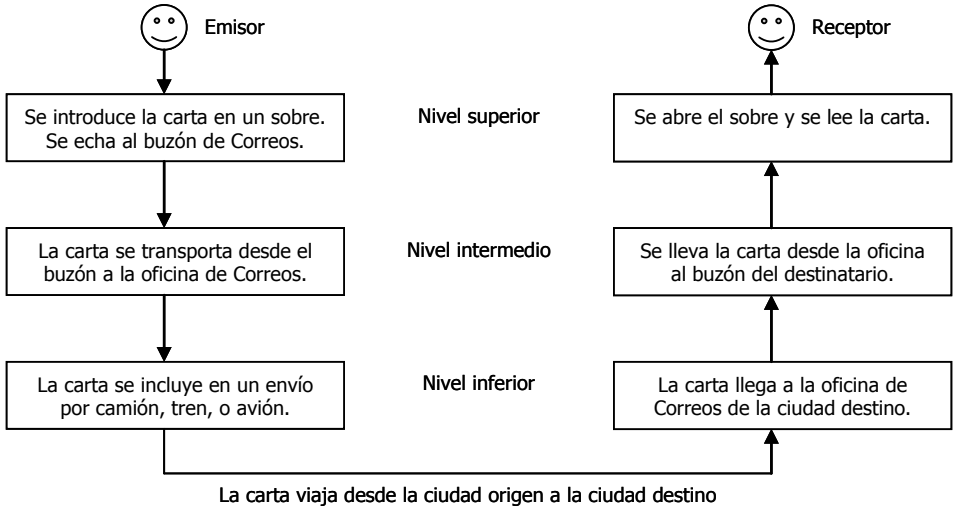
- *Hub* (concentrador). Conecta varios equipos en un punto central, retransmitiendo a todos ellos las señales que recibe por cada uno de sus puertos.
- *Switch* (conmutador). También centraliza la conexión de varios equipos, si bien es capaz de interpretar el contenido de los mensajes que recibe, reenviándolos únicamente al destinatario.
- *Router* (encaminador). Separa redes, aislando el tráfico interno de cada una de ellas y redireccionando (encaminando) mensajes que van dirigidos a equipos de redes distintas.

7. Arquitecturas de protocolos

7.1. Protocolos

Los protocolos son importantes en la vida diaria. Permiten la comunicación entre personas y fomentan la eficiencia en sistemas de comunicaciones de todo tipo. En el contexto de las redes son los que agrupan las reglas y procedimientos necesarios para que los equipos se comuniquen entre sí.

Al igual que en la vida real, y basándose en el método "divide y vencerás", en las redes de ordenadores la comunicación se divide en distintos niveles o capas, con el objetivo de reducir la complejidad del diseño. A continuación vemos un ejemplo de niveles de comunicación en el envío de una carta por correo de una ciudad a otra:



Se observa que cada una de las capas es responsable de ofrecer servicios a los niveles superiores (la infraestructura de Correos debe soportar una serie de oficinas, cada una de ellas responsable de una serie de buzones repartidos por la ciudad). Cada capa dispone de distintos servicios (el

nivel intermedio podría incluir las gestiones por Internet, y el inferior la posibilidad de enviar burofax). El nivel de abstracción crece desde las capas inferiores (bajo nivel) a las superiores (alto nivel).

Podemos definir **protocolo** como un formato de mensaje más las reglas de intercambio de ese mensaje entre entidades del mismo nivel o capa, y **servicio** como la capacidad de comunicación que ofrece una capa inferior o proveedora a una capa superior o usuaria.

Volviendo al caso genérico de la red de ordenadores, toda jerarquía de protocolos debe cumplir las siguientes reglas:

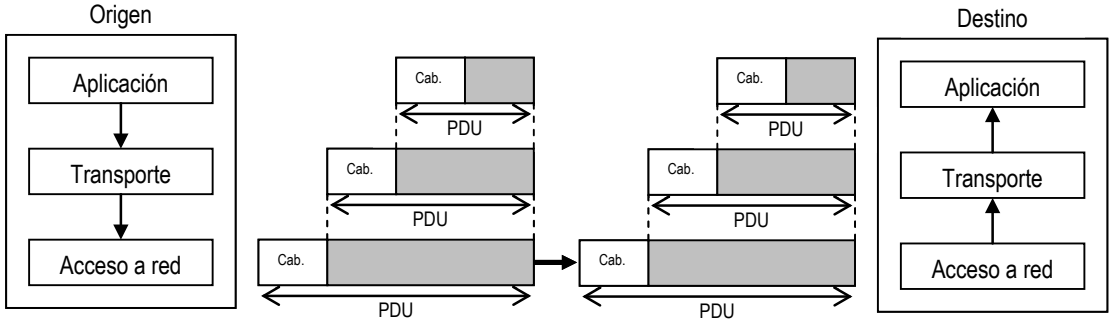
- Cada nivel debe disponer de un conjunto de servicios.
- Cada servicio debe estar definido mediante protocolos estándar.
- Cada nivel es usuario del inmediatamente inferior y proveedor del inmediatamente superior, sin posibilidad de comunicación directa con niveles no adyacentes.

La **arquitectura de una red** viene definida por su topología, su método de acceso a la red y sus protocolos de comunicación.

7.2. Interfaces y servicios

Las siglas PDU corresponden a *Protocol Data Unit* (Unidad de Datos de Protocolo). En cada uno de los niveles de la arquitectura del sistema de comunicaciones, a los datos que se envían en una transmisión se añade cierta información de control (PCI – *Protocol Control Information*) en su cabecera, conformando la PDU. A esto se le llama **encapsulado de datos**. La información a transmitir puede ser fragmentada en alguna de las capas.

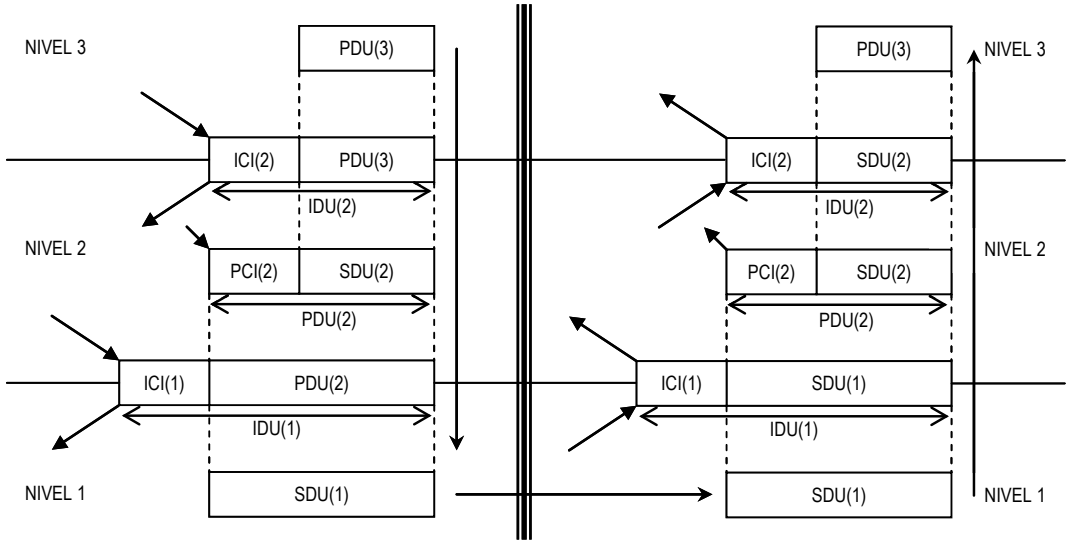
El siguiente ejemplo muestra una sencilla arquitectura en tres capas:



Como se comentaba anteriormente, cada capa debe proveer servicios a la inmediatamente superior. Esta comunicación se hace a través de los llamados SAP (*Service Access Point* – Punto de Acceso al Servicio), situados en la frontera entre dos capas adyacentes. Cada SAP tiene una dirección única. Los procesos de una capa transfieren a los de la capa contigua, a través del SAP, un IDU (*Interface Data Unit* – Unidad de Datos de Interfaz). La IDU está formada por:

- SDU (*Service Data Unit* – Unidad de Datos de Servicio). PDU o conjunto de PDUs.
- ICI (*Interface Control Information* – Información de control de interfaz). Información de control para la capa inferior.

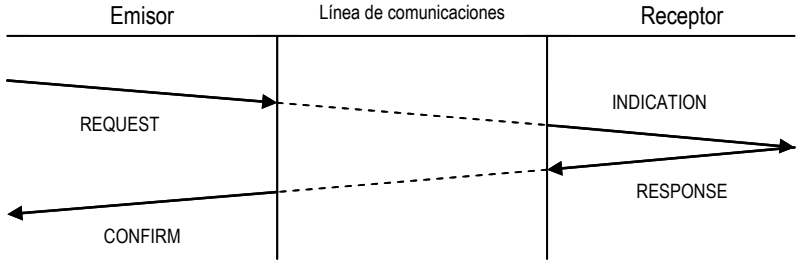
El siguiente esquema muestra cómo se efectúa la comunicación. A la izquierda aparecen los sucesos que ocurrirían en el lado del emisor, a la derecha en el del receptor.



7.3. Primitivas de servicio

La implementación formal de un servicio implica la existencia de operaciones llamadas primitivas de servicio, es decir, llamadas al servicio solicitando funciones, acciones o informes de acciones ya realizadas. Hay cuatro tipos de primitivas de servicio:

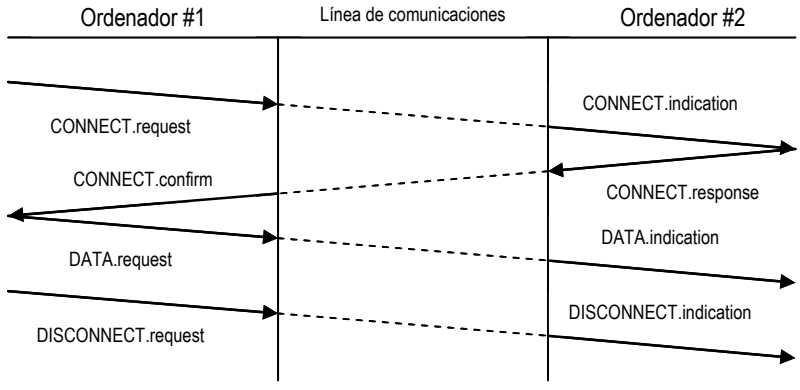
- Petición (*request*). Una entidad solicita al servicio que ejecute un trabajo.
- Indicación (*indication*). Se informa a una entidad de un suceso.
- Respuesta (*response*). Una entidad responde a un suceso.
- Confirmación (*confirmation*). Respuesta a una petición anterior.



Un servicio puede ser confirmado o fiable (utiliza los cuatro tipos de primitiva) o no confirmado o no fiable (sólo utiliza *request* e *indication*).

El siguiente ejemplo de comunicación entre dos equipos muestra el funcionamiento de las primitivas de servicio en tres servicios: CONNECT (etapa de conexión), DATA (transmisión de información) y DISCONNECT (desconexión):

1.	CONNECT.request	Ordenador #1 pide establecer conexión
2.	CONNECT.indication	Ordenador #2 recibe la petición
3.	CONNECT.response	Ordenador #2 devuelve una respuesta afirmativa
4.	CONNECT.confirm	Ordenador #1 recibe dicha confirmación
5.	DATA.request	Envío de los datos
6.	DATA.indication	Recepción de los datos
7.	DISCONNECT.request	Ordenador #1 desea finalizar la conexión
8.	DISCONNECT.indication	Ordenador #2 se entera del fin de la conexión



Un servicio de datos orientado a conexión utiliza los servicios CONNECT y DISCONNECT. Si es no orientado a conexión no los usa.

El siguiente ejemplo es una analogía con una llamada telefónica para solicitar un pedido a una empresa. El proveedor del servicio es el sistema telefónico:

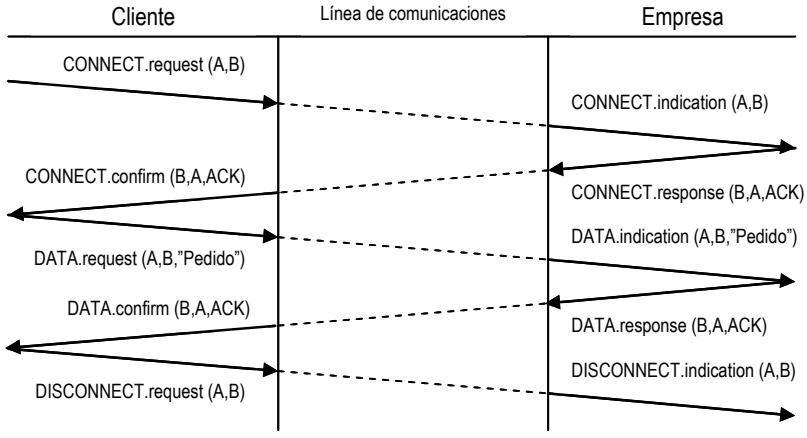
1.	CONNECT.request	El cliente marca el número de teléfono
2.	CONNECT.indication	El teléfono suena en la empresa
3.	CONNECT.response	El dependiente descuelga el teléfono
4.	CONNECT.confirm	El cliente deja de escuchar el tono de llamada
5.	DATA.request	El cliente efectúa el pedido
6.	DATA.indication	El dependiente escucha el pedido
7.	DATA.response	El dependiente valida el pedido
8.	DATA.confirm	El cliente escucha al dependiente validar el pedido
9.	DISCONNECT.request	El cliente cuelga el teléfono
10.	DISCONNECT.indication	El dependiente se da cuenta y también cuelga

Cada una de las primitivas puede pasar parámetros, entre los que se encuentran el remitente, el destinatario, la información a transmitir (en el caso de un servicio DATA) y el éxito o fracaso de la transmisión (en primitivas *response* y *confirm*), siendo "ACK" una confirmación positiva y "NAK" una confirmación negativa. A continuación vemos ejemplos de primitivas del servicio DATA con parámetros (A y B son los identificadores de los equipos origen y destino, respectivamente):

DATA.request (A, B, "Hola")
DATA.response (B, A, ACK)
DATA.response (B, A, NAK)

El ejemplo anterior quedaría del siguiente modo:

1. CONNECT.request (A, B)
2. CONNECT.indication (A, B)
3. CONNECT.response (B, A, ACK)
4. CONNECT.confirm (B, A, ACK)
5. DATA.request (A, B, Información del pedido)
6. DATA.indication (A, B, Información del pedido)
7. DATA.response (B, A, ACK)
8. DATA.confirm (B, A, ACK)
9. DISCONNECT.request (A, B)
10. DISCONNECT.indication (A, B)



7.4. Elementos de una arquitectura de protocolos

- Direccionamiento. Permite acceder a las distintas interfaces mediante su dirección.

- Transferencia de información. Hay que fijar reglas. Generalmente la transmisión es *full-duplex* salvo en capas inferiores y casos puntuales donde el medio físico no soporta este sistema

- Detección y corrección de errores. Forzando la existencia de acuses de recibo, o bien mediante códigos redundantes.

- Numeración de paquetes. Necesario para la reconstrucción consistente del mensaje por parte del receptor.

- Mecanismos de control de flujo y congestión. Adecúan las diferentes velocidades de las interfaces de red y evitan la saturación de los nodos intermedios de la transmisión.

- Mecanismos de segmentación y concatenación. En ocasiones las distintas capas de la arquitectura no soportan tamaños iguales de PDU. Por ello se necesitan herramientas de división de SDU en varias PDU y viceversa, a fin de reconstruir esa segmentación en la entidad par.

- Multiplexación y división. Se dividen los recursos de un canal entre diferentes comunicaciones (multiplexación) o bien se separan las comunicaciones entre distintos canales (división y agregación).

7.5. Sistemas abiertos

Según ISO: "Sistemas informáticos capaces de interconectarse con otros según unas normas establecidas".

Según X/Open: "Entornos de software diseñados e implantados según normas divulgadas e independientes de los fabricantes".

Las características principales de un sistema abierto son las siguientes:

- Interoperabilidad. Capacidad de operar con otros elementos del sistema o de sistemas diferentes.

- Portabilidad. Posibilidad de integrar el sistema o parte del mismo en otro sistema distinto.
- Escalabilidad. Capacidad de crecimiento del sistema.
  - Horizontal. Añadiendo más equipos.
  - Vertical. Creciendo hacia sistemas superiores.

Ventajas para el usuario:

- Libertad de elección.
- Mejor relación precio-rendimiento.
- Garantía de comunicación e interoperabilidad entre sistemas.

Lo contrario a un sistema abierto es un sistema propietario, es decir, aquel cuyas especificaciones de manejo e interoperabilidad pertenecen a una compañía, presentando incompatibilidades con sistemas de otros fabricantes.

8. El modelo OSI

Las primeras arquitecturas de redes se idearon para conectar entre sí equipos del mismo fabricante, sin tener en cuenta la compatibilidad con equipos de fabricantes distintos. La organización de estandarización ISO decidió crear un modelo teórico de red que pudiera ayudar a los diseñadores a implementar redes capaces de comunicarse y trabajar en conjunto de forma estándar. En 1977 creó un subcomité con la tarea de investigar acerca de los esquemas de red vigentes, definiendo en 1984 el estándar ISO 7498, conocido como OSI (*Open System Interconnection* – Interconexión de Sistemas Abiertos). OSI es un modelo en siete capas que no especifica protocolos y servicios exactos (no es una arquitectura de red en sí), sino las especificaciones funcionales de cada nivel.

Los siete niveles OSI son, de arriba a abajo:

» 7. **Aplicación**. Proporciona servicios de red a aplicaciones (*e-mail*, web…).

» 6. **Presentación**. Representación de la información (formato, sintaxis).

» 5. **Sesión**. Comunicación entre *hosts* (sesiones entre aplicaciones).

» 4. **Transporte**. Conexiones de extremo a extremo (flujo, errores, CVs).

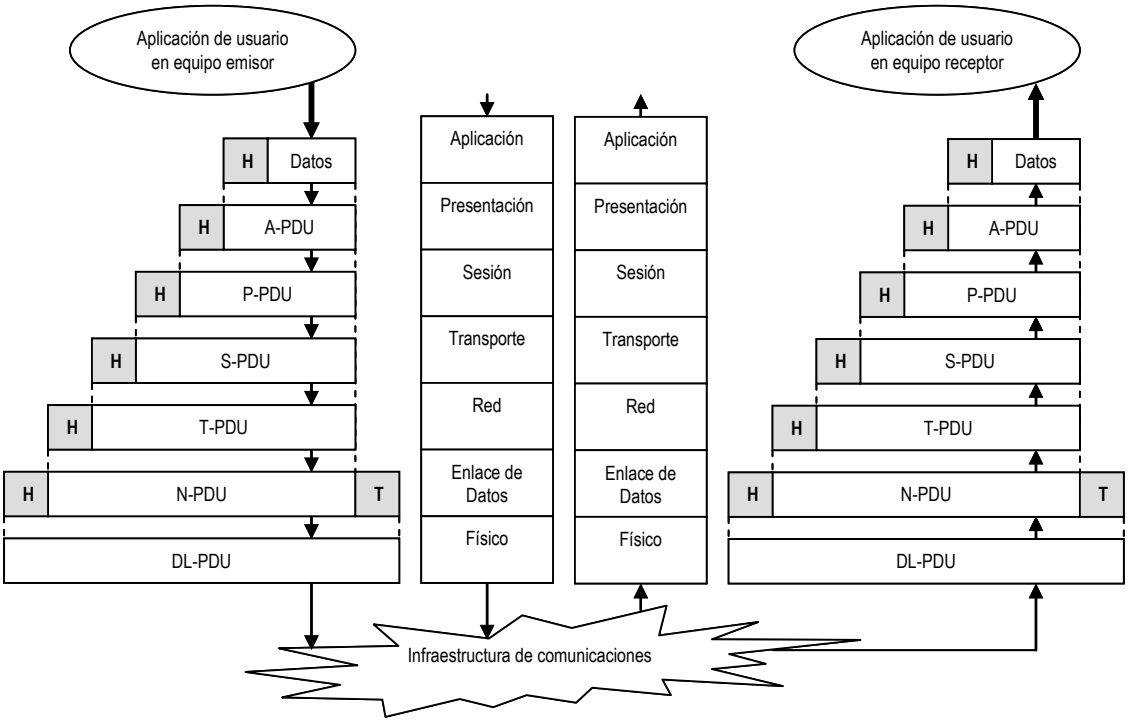
» 3. **Red**. Direccionamiento y búsqueda de la mejor ruta.

» 2. **Enlace de datos**. Acceso al medio (direccionamiento físico, topología).

» 1. **Físico**. Transmisión de bits en el medio físico (cables, conectores, voltajes).

Esquema de comunicación entre dos equipos utilizando el modelo OSI:

Leyendas:		
H	Header	Cabecera
T	Tail	Cola
A-PDU	Application PDU	PDU del nivel de aplicación
P-PDU	Presentation PDU	PDU del nivel de presentación
S-PDU	Session PDU	PDU del nivel de sesión
T-PDU	Transport PDU	PDU del nivel de transporte
N-PDU	Network PDU	PDU del nivel de red
DL-PDU	Data Link PDU	PDU del nivel de enlace de datos



Las tres capas inferiores (física, enlace y red) engloban lo que se conoce como **bloque de transmisión**, encargándose de definir los protocolos asociados a la red de conmutación de paquetes subyacente.

El nivel 4 (transporte) enmascara a los niveles superiores los detalles de trabajo de los niveles inferiores y, junto a ellos, forma lo que se conoce como **bloque de transporte**. Dicho bloque, común para todas las aplicaciones, se encarga del transporte fiable de los datos sin intervenir en el significado de los mismos.

Por otro lado, los tres niveles superiores (aplicación, presentación y sesión) son usuarios del bloque de transporte. Tienen que ver con aspectos de las aplicaciones de usuario y aíslan la comunicación de las características específicas del sistema informático.

8.5.1. Nivel 1 – Físico

La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales. Define características como niveles de voltaje, temporización de cambios de voltaje, velocidad de datos físicos, distancias de transmisión máximas o conectores físicos.

Su unidad de datos es el bit, es decir la PDU de nivel físico corresponde a un bit. No reconoce otro tipo de estructura de datos ni actúa sobre el significado de la información, quedando dichas tareas para los niveles superiores.

La capa física proporciona sus servicios a la capa de enlace de datos. Sus principales funciones son:

- Definición de características mecánicas (componentes y conectores mecánicos) y eléctricas (niveles de tensión, tipo de señal) que se van a utilizar en la transmisión de los datos por el medio físico.

- Definición de las características funcionales de la interfaz en cuanto a establecimiento, mantenimiento y liberación del enlace físico.
- Definición de reglas de procedimiento, es decir, la secuencia de eventos a transmitir.
- Transmisión de flujos de bits a través del medio.
- Manejo de voltajes y pulsos eléctricos para representar unos o ceros.
- Especificación de cables, polos en un enchufe, componentes de interfaz con el medio, etc.
- Especificación del medio físico de transmisión (cable coaxial, fibra óptica, par trenzado, etc.).
- Garantía de conexión física, pero no fiabilidad de la misma (en este nivel no se realiza ningún control de errores).

8.5.2. Nivel 2 – Enlace de datos

Una vez el nivel físico permite el envío de información, la capa de enlace de datos toma el medio de transmisión en bruto y lo convierte en una línea de comunicaciones, garantizando la fiabilidad en el tránsito de los datos a través de un enlace físico entre dos estaciones, y ocupándose del direccionamiento físico, la topología de red, el acceso a la misma, la notificación de errores, la entrega ordenada de la información y el control de flujo.

Su PDU es la trama y sus funciones principales son:

- Establecimiento de los medios necesarios para la comunicación fiable y eficiente entre dos máquinas en red (activación, mantenimiento y desactivación del canal físico).
- Estructuración de los datos en tramas (secuencia de unos cientos de *bytes* a la que se añade una secuencia especial de bits al principio y otra al final).
- Sincronización en el envío de tramas.
- Detección y control de errores provenientes del medio físico mediante el uso de bits de paridad, CRC (Códigos Cíclicos Redundantes) y envío de acuses de recibo por parte del receptor.
- Utilización de un número de secuencia en las tramas para evitar pérdidas y duplicidades.
- Resolución de los problemas provocados por las tramas dañadas, perdidas o duplicadas.
- Control de la congestión de la red.
- Mecanismos de regulación de tráfico o control de flujo, para evitar que un transmisor veloz sature de datos a un receptor lento.
- Control de acceso al canal compartido (MAC – *Media Access Control*, sólo en redes de difusión).

8.5.3. Nivel 3 – Red

Responsable de la conmutación y encaminamiento de la información, sólo es necesario en redes de conmutación, ya que en redes de difusión hay un canal directo entre equipos, responsabilizándose el nivel 2 de la existencia de una conexión fiable entre ellos. Es una capa compleja, capaz de ofrecer conectividad a *hosts* muy alejados geográficamente. La PDU del nivel de red normalmente se denomina paquete.

Sus funciones principales son:

- Conocimiento de la topología de la red, con objeto de determinar la mejor ruta para la comunicación entre máquinas.
- División de los mensajes de la capa de transporte en unidades más pequeñas y manejables (paquetes) y asignación de direcciones lógicas a los mismos.
- Ensamblado de paquetes en el *host* destino.
- Establecimiento, mantenimiento y liberación de las conexiones de red entre sistemas.
- Determinación del encaminamiento de los paquetes de la fuente al destino a través de dispositivos intermedios (*routers*).
  - Las rutas se pueden basar en tablas estáticas.
  - Las rutas se pueden determinar al inicio de cada conversación.
  - Las rutas pueden ser dinámicas, determinándose con cada paquete en función de la carga de la red.
- Envío de paquetes de nodo a nodo usando un circuito virtual o datagramas.
- Control de la congestión.
- Control de flujo.
- Control de errores.
- Reencaminamiento de paquetes en caso de rotura de un enlace.
- Funciones de contabilidad, para determinar cuántos paquetes, caracteres o bits envía cada cliente (información de facturación).

8.5.4. Nivel 4 – Transporte

Es una capa extremo a extremo, ya que es en ella donde comienza el trabajo de envío de la información entre aplicaciones que se ejecutan en equipos remotos. Posee la interfaz con menos primitivas del modelo OSI, ya que carece de primitivas de confirmación, al ser considerado un nivel fiable. Es la frontera entre los protocolos de aplicación (niveles superiores) y los de flujo de datos (inferiores).

En el origen el nivel 4 recibe datos del 5 (sesión), los divide, si es preciso, en unidades más pequeñas (segmentos), y los envía a la capa de red. En el destino reensambla dichos segmentos.

Otras funcionalidades de esta capa son:

- Establecimiento, mantenimiento y terminación adecuados de los circuitos virtuales. Al iniciarse la conexión, determina la ruta que se utilizará para todo el tráfico de datos posterior de la fuente al destino.
- Determinación, en el momento del establecimiento de la sesión, del tipo de clase de servicio de transporte que se proporcionará a la capa de sesión:
  - Canal punto a punto libre de errores, que entrega los mensajes en el orden en que se envían.
  - Mensajes aislados sin garantía respecto al orden de entrega.
  - Difusión de mensajes a múltiples destinos.

- Control de flujo (distinto al control de flujo entre encaminadores, que tiene lugar en la capa de red). Los datos pueden ser normales o urgentes, en cuyo caso se saltan los mecanismos de control de flujo.
- Detección y recuperación de errores de transporte.
- Control de la congestión.
- Numeración de los segmentos para garantizar la recepción de todos los datos y en el orden adecuado, sin pérdidas ni duplicados.
- Asignación de una dirección única de transporte a cada usuario.
- Aislamiento a las capas superiores de los cambios inevitables de la tecnología del *hardware*.
- Funciones de contabilidad para facturar por el uso de la red.

8.5.5. Nivel 5 – Sesión

Establece, administra y finaliza las conexiones lógicas (sesiones) entre procesos de *hosts* distintos, sincronizando el diálogo y administrando el intercambio de datos.

Si la comunicación es *half-duplex*, el nivel de sesión establece los turnos de comunicación mediante el manejo de *tokens* (sólo puede transmitir el *host* que posea el *token*).

La gestión de sincronización de diálogo la realiza mediante la inserción de puntos de verificación en la corriente de datos (APDU – *Application Protocol Data Unit*), de modo que si se produce una interrupción sólo es necesario repetir la transferencia de los datos tras el último APDU. No obstante, es el nivel 7 (Aplicación) el que decide dónde colocar los APDU.

8.5.6. Nivel 6 – Presentación

Esta capa se ocupa de la sintaxis y semántica de la información a transmitir, permitiendo que los datos transmitidos por el equipo origen sean legibles en el destino. La información es codificada según el modelo estándar de representación de la información en la red, para luego ser formateada en el destino de acuerdo a los criterios de representación del *host*, características locales, etc.

Otros servicios que ofrece a la capa de Aplicación son:

- Garantía de que la información que envía la capa de aplicación de un sistema pueda ser entendida y utilizada por la capa de aplicación de otro sistema.
- Acuerdo y negociación de la sintaxis de transferencia en la fase de establecimiento de la conexión (la sintaxis elegida puede ser cambiada durante el tiempo que dure la conexión).
- Definición del código a utilizar para representar una cadena de caracteres (ASCII, EBCDIC, etc.).
- Interpretación de formatos de números, fechas, etc.
- Compresión de los datos, si es necesario.
- Aplicación de procesos criptográficos, si así se requiere. Es el nivel donde se ubica el sistema de seguridad del modelo OSI.
- Formateo de la información para su visualización o impresión.

8.5.7. Nivel 7 – Aplicación

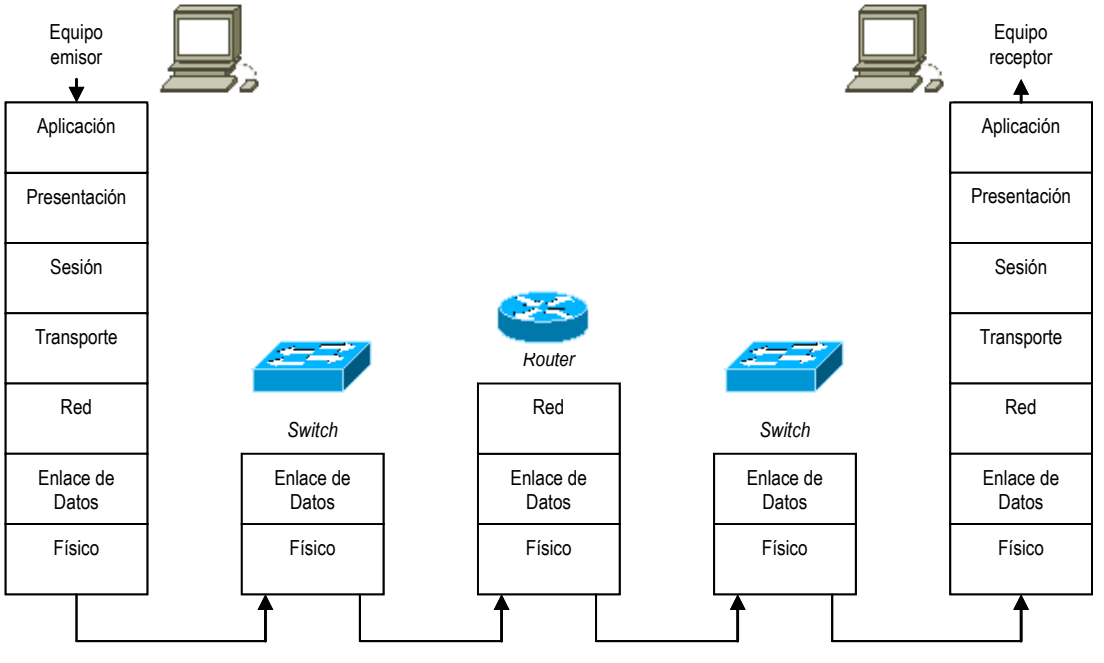
Es la capa del modelo OSI más cercana al usuario. Difiere de las demás capas en que no proporciona servicios a ninguna otra capa OSI, sino a aplicaciones que se encuentran fuera del modelo. Las capas inferiores sirven de mera infraestructura de telecomunicaciones, es decir, mantienen en buen estado el camino para que fluyan los datos. Es la capa de aplicación la que hace posible que una red se pueda usar, a pesar de que el resto de las funciones necesarias para el establecimiento de la comunicación le sean transparentes.

Las aplicaciones más importantes que hacen uso de esta capa, para que los procesos de las aplicaciones accedan al entorno OSI son, entre otras:

- Correo electrónico. Primera aplicación que se normalizó en OSI.
- Terminal virtual de red abstracta, que diferentes editores y programas pueden manejar.
- Transferencia de archivos.
- Carga remota de trabajos.
- Servicios de directorio.
- *Login* remoto.
- Acceso a bases de datos.
- Sistemas operativos de red.
- Aplicaciones Cliente/Servidor.

Las PDUs de la capa de aplicación, APDUs, son de formato muy flexible y variable. Entre dos APDUs de distintas aplicaciones puede haber diferencias sustanciales en cuanto a su tamaño, número de campos presentes, etc. que dependen de las necesidades de cada momento.

8.1. Uso de dispositivos en el modelo OSI



8.2. Críticas al modelo OSI

La verdadera razón de que el modelo OSI tenga siete capas es que, en el momento en que se diseñó, IBM tenía un protocolo patentado de siete capas (SNA) y, en esa época, IBM dominaba la industria de la computación.

Por otro lado, el proceso de estandarización fue demasiado largo. Cuando todavía se trabajaba en la definición de OSI, ya existían implementaciones completas y gratuitas de TCP/IP y aplicaciones como *e-mail*, *telnet*, FTP, etc.

Algunos de los problemas o fallos que se han detectado en el modelo de referencia OSI son:

- El modelo está concebido desde un punto de vista de telecomunicaciones, no siendo inmediata su adaptación al contexto de las redes de ordenadores.
- Al ser un modelo teórico sus estándares son difíciles de implementar.
- Las funcionalidades asignadas a cada capa han sido posteriormente discutidas por diseñadores de arquitecturas.
- Las capas de sesión y presentación apenas se usan en la mayor parte de las aplicaciones.
- Las capas de red y enlace de datos están saturadas, llegando a dividirse en subcapas.
- Algunas funciones como el direccionamiento, el control de flujo y el control de errores se repiten en más de una capa.
- Inicialmente la función de cifrado y seguridad de los datos se dejó fuera del modelo por falta de acuerdo sobre en qué capa colocarlo.

9. TCP/IP

En los años 60 en plena Guerra Fría, el DoD (Departamento de Defensa de EE.UU.) necesitaba una red que pudiera sobrevivir ante cualquier circunstancia, incluso una guerra nuclear. Para ello la Agencia de Proyectos de Investigación Avanzada para la Defensa (DARPA – *Defense Advance Research Projects Agency*) desarrolló el modelo TCP/IP (*Transfer Control Protocol/ Internet Protocol* – Protocolo de Control de Transferencia/Protocolo de Internet), cuyo objetivo fundamental consistía en que la información a transmitir (organizada en forma de paquetes) llegara siempre a su destino con independencia del estado de los nodos de la red (que podrían estar físicamente destruidos), utilizando cualquier tipo de conexión posible (cables, microondas, fibra óptica, enlaces de satélite).

Desarrollado a principios de los años 70, en 1983 ya estaba considerado como único protocolo oficial independiente de cualquier fabricante, y se convirtió en el estándar sobre el que se implantó Internet. Tiene mayor aplicación que el modelo OSI, ya que se desarrolló antes y las especificaciones asociadas a sus protocolos son de dominio público. Varios sistemas, como Unix (Berkeley), Linux, Windows o MacIntosh, lo soportan de forma nativa.

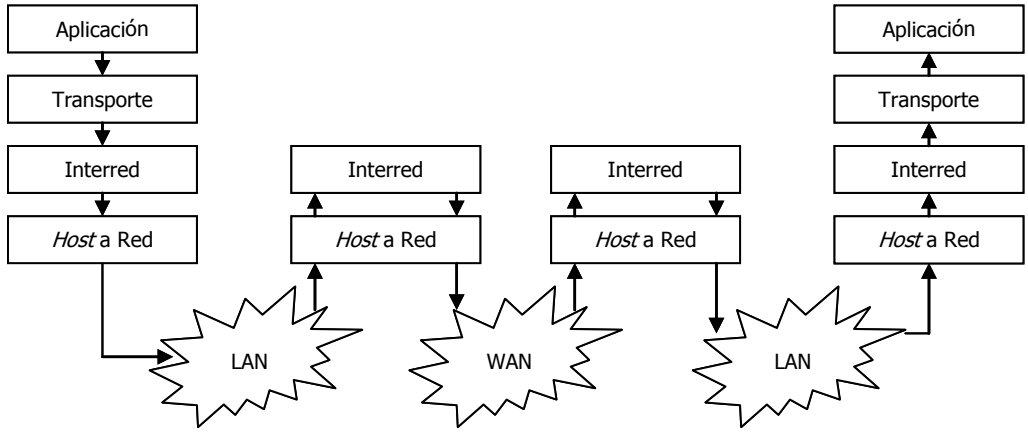
Sus características principales son las siguientes:

- Agrupa redes, creando una red mayor llamada Internet.
- Es independiente del *hardware* y sistema operativo subyacentes, así como de la tecnología del medio de transmisión y del enlace de datos.
- Ofrece capacidad de encaminamiento adaptativo de forma transparente al usuario.

- Es una red de conmutación de paquetes.

Su arquitectura consta de cuatro capas o niveles:

- Nivel de **aplicación**. Se ocupa de facilitar el acceso del *software* de servicios o de aplicaciones de usuario a las comunicaciones.
- Nivel de **transporte** (TCP). Su objetivo es la fiabilidad en la entrega de los datos.
- Nivel de **interred** o **internet** (IP). Su función principal es el encaminamiento de los datos.
- Nivel de ***host* a red**. Representa el enlace físico. Depende de la tecnología subyacente.



9.2.1. Nivel de *host* a red (acceso a red, nodo a red o subred)

Esta capa se concibe como mera interfaz con el protocolo de enlace y el medio físico que trabajan por debajo de TCP/IP. Queda patente de ese modo la capacidad de la arquitectura para funcionar sobre cualquier tipo de red.

Protocolos del nivel de acceso a la red:

- ARP (*Address Resolution Protocol* – protocolo de resolución de direcciones). Traduce las direcciones IP a direcciones físicas, comprensibles para el *hardware* subyacente.
- RARP (*Reverse Address Resolution Protocol* – protocolo inverso de resolución de direcciones). Obtiene la dirección IP a partir de la física (por ejemplo, al iniciar un *host* sin disco en una red).
- OSPF (*Open Shortest Path First* – protocolo de encaminamiento de pasarela interior). Originalmente situado en la capa de Internet, pasó a la de acceso a red en 1999 al ser modificado para soportar IPv6. Es un protocolo de encaminamiento que busca la eficiencia en la transmisión de paquetes. Desde 1990 es una alternativa al protocolo RIP (*Routing Information Protocol* – protocolo de información de encaminamiento), que sólo funciona en redes pequeñas.

9.2.2. Nivel de interred o *internet*

Permite el envío de paquetes entre dos equipos con independencia de la ruta a seguir y de las redes transitadas. El protocolo específico que rige esta capa se denomina Protocolo Internet (IP – *Internet Protocol*). En esta capa se produce la determinación de la mejor ruta y la conmutación de paquetes.

Es un servicio no fiable. No hay garantía de que los paquetes lleguen al destino ni de que lo hagan en el orden deseado, tareas reservadas a las capas superiores.

Además de IP, en esta capa se usan varios protocolos de control:

- ICMP (*Internet Control Message Protocol* – protocolo de control de mensajes de Internet). Informa sobre sucesos en la transmisión. Sus mensajes se encapsulan en los paquetes IP. Hay mensajes ICMP informativos y de error.

- IGMP (*Internet Group Management Protocol* – protocolo de gestión de grupos de Internet). Se utiliza para transmitir a una cantidad grande de receptores de forma simultánea (actualizaciones de *software*, bases de datos distribuidas, etc.).

- IPSec (*Internet Protocol Security* – seguridad IP). Provee autenticación y cifrado de paquetes IP con independencia de los procesos de nivel superior.

Al margen de los protocolos comentados, merece especial mención el protocolo IPv6 (también llamado IPng – *Internet Protocol Next Generation*), cuyo cometido fundamental es ampliar el rango de direcciones IP, agotado desde el 1 de febrero de 2011. Por ese motivo las direcciones IPv6 tienen 16 *bytes* de longitud, frente a los 4 *bytes* de IPv4. Las ventajas de IPv6 son:

- Incrementar el rango de direcciones disponibles.
- Reducir el tamaño de las tablas de encaminamiento y permitir a los *routers* un procesamiento de paquetes más rápido.
- Aportar más seguridad.
- Diferenciar los paquetes según el tipo de servicio a prestar.
- Mejorar el envío *multicast*.
- Facilitar la movilidad de *hosts* sin cambiar sus direcciones.
- Fomentar la flexibilidad del protocolo, de modo que sea escalable y compatible con versiones anteriores.

9.2.3. Nivel de transporte

Análoga a la capa de transporte de OSI, permite establecer una comunicación entre las entidades pares de los nodos origen y destino, proporcionando transferencia de datos extremo a extremo. Permite garantizar la recepción ordenada de los datos y puede incluir mecanismos de seguridad.

Presenta cuatro protocolos básicos:

- TCP (*Transmission Control Protocol* – protocolo de control de transmisión). Orientado a conexión. Garantiza el envío de un paquete desde una máquina a otra. Es fiable y realiza detección y corrección de errores (mediante las técnicas de ventana deslizante y ARQ).

- UDP (*User Datagram Protocol* – protocolo de datagrama de usuario). Servicio de transporte tipo datagrama. Más rápido que TCP, al no comprobar errores ni establecer conexión.

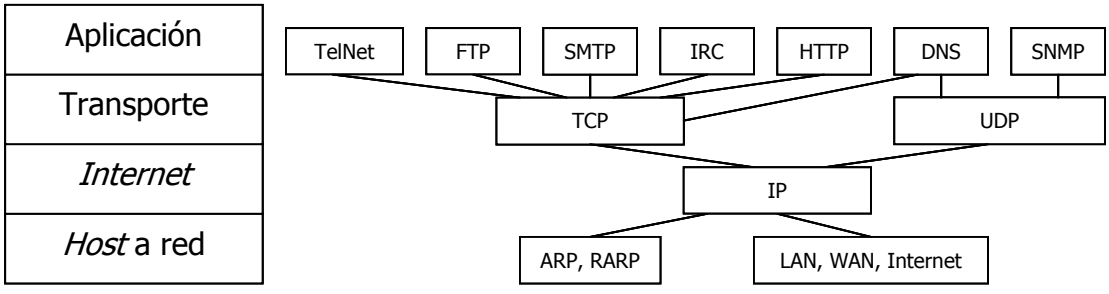
- SCTP (*Stream Control Transmission Protocol* – protocolo de transmisión de control de flujo). Diseñado en 2000 para servir a aplicaciones de telefonía IP y videoconferencia.

- DCCP (*Datagram Congestion Control Protocol* – protocolo de control de congestión de datagramas). Creado en 2006 y pensado para en el transporte de datos de aplicaciones multimedia en tiempo real, como servicios de *streaming* o juegos *on-line*.

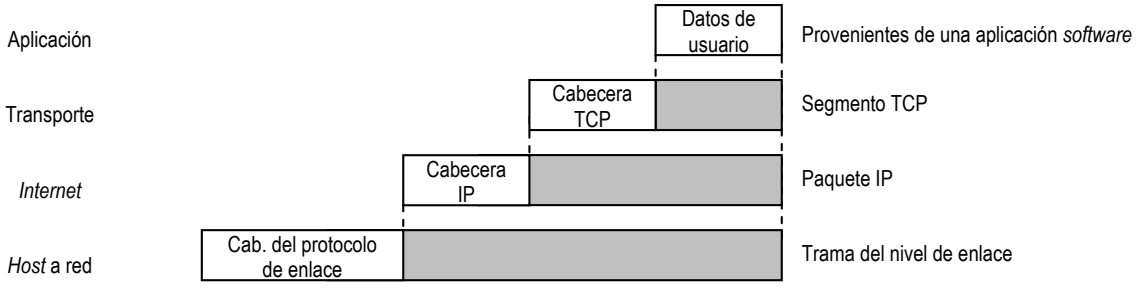
9.2.4. Nivel de aplicación

Gestiona la comunicación entre procesos o aplicaciones del *host* emisor y receptor. Incluye todos los protocolos de alto nivel (aspectos de representación, codificación y control de diálogo), agrupando las funciones de los tres niveles superiores del modelo OSI.

9.1. Modelo básico de protocolos TCP/IP



9.2. PDUs en TCP/IP

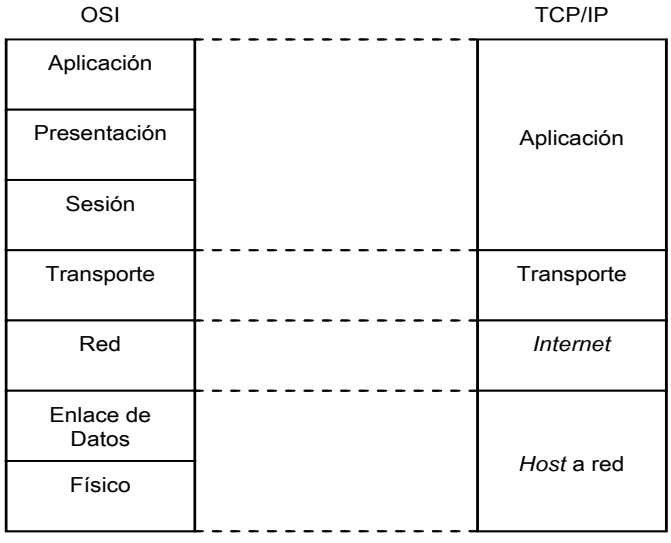


9.3. Críticas a TCP/IP

A pesar de su amplia aceptación, también presenta problemas:

- No distingue con claridad los conceptos de servicio, interfaz y protocolo (dificultad para reemplazar protocolos).
- No es una buena guía para diseñar redes nuevas, ya que tampoco distingue de forma clara entre especificaciones e implementación.
- No es un modelo general, por lo que no resulta adecuado para describir cualquier pila de protocolos distinta de TCP/IP.
- La capa de nodo a red, más que una capa es una interfaz entre la red y las capas física y de enlace de datos.
- Como la distribución de las implementaciones es gratuita, TCP/IP se ha utilizado ampliamente, dificultando mucho su reemplazo.

9.4. Comparación con el modelo OSI



Similitudes

- Ambos tienen capas de aplicación, aunque incluyen servicios muy distintos.
- Ambos tienen capas de transporte y de red similares.
- Se supone que la tecnología es de conmutación de paquetes (no de conmutación de circuitos).
- Los profesionales de *networking* deben conocer ambos.

Diferencias

- TCP/IP combina las funciones de la capa de presentación y de sesión en la capa de aplicación.
- TCP/IP combina las capas de enlace de datos y la capa física del modelo OSI en una sola capa.
- TCP/IP aparenta ser más simple al tener menos capas.
- Los protocolos TCP/IP son los estándares en torno a los cuales se desarrolló Internet, de modo que la credibilidad del modelo TCP/IP se debe en gran parte a que sus protocolos han sido ampliamente probados. En comparación, las redes típicas no se desarrollan normalmente a partir del protocolo OSI, aunque el modelo OSI se usa como guía.

10. Otras arquitecturas de red

10.1. SNA

IBM lanzó en 1974 su primera versión de SNA (*Systems Network Architecture* – Arquitectura de Red de Sistemas), permitiendo sólo redes en forma de árbol con un solo *host*. Dos años después se permitía la interconexión entre varios árboles. En 1981 IBM anunció algunos productos que permitían enlazar componentes SNA con las redes de conmutación de paquetes X.25. En 1985 se incluyó la aparición de topologías arbitrarias de *hosts* y LAN.

En la actualidad SNA es una arquitectura de red que permite a los clientes de IBM construir sus propias redes privadas. Un banco, por ejemplo, puede tener una o más CPUs en un departamento y terminales en cada una de sus sucursales. Con SNA estos componentes aislados pueden transformarse en un sistema coherente.

10.1.1. Comparación con OSI

Al igual que OSI, también consta de siete niveles (OSI se inspiró en SNA):

N	OSI	Función	SNA	Función
7	**Aplicación**	Comunicación con usuarios Gestión de ficheros Gestión de elementos de servicio	**Gestor de servicios UDR**	Intercambio de datos Gestión de dispositivos y formatos de compactación
6	**Presentación**	Gestión de formato Alfabeto Sintaxis	**Servicios NAU**	Sintaxis comunes Gestión de ficheros Conversión de direcciones
5	**Sesión**	Sincronización de diálogos de usuario Gestión de intercambio de datos Servicio de garantía	**Control de flujo de datos**	Sincronización de intercambio de infomación Encadenamiento y agrupamiento Gestión de respuestas
4	**Transporte**	Control de errores Conversión de direcciones Segmentación Agrupamiento de prioridades Calidad de servicio	**Control de transmisión**	Tráfico de datos Cifrado de datos Gestión del estado de la sesión
3	**Red**	Interfaz de paquetes	**Control de camino**	Control de flujo y encaminamiento Conversión de direcciones Segmentación y agrupamiento de mensajes
2	**Enlace**	Gestión del flujo de datos a través de un enlace	**Control de Enlace de Datos**	Gestión del flujo de datos a través de un enlace
1	**Físico**	Interfaz físico y eléctrico	**Físico**	Interfaz físico y eléctrico

10.2. Microsoft Windows

En sus sistemas operativos de la familia Windows, Microsoft propone dos modelos de red:

- Modelo *peer-to-peer* o "entre iguales": todas las máquinas son clientes, compartiendo recursos entre ellas. Tanto las plataformas *Workstation* como las *Server* soportan dicho modelo.
  - » Bajo coste.
  - » Organización autónoma de la red por parte de los usuarios (grupos de trabajo).
  - » Difícil localización de los recursos y ficheros distribuidos.
  - » Compleja administración de red.
  - » Fallos de seguridad.
- Modelo cliente/servidor: máquinas cliente y servidor dedicadas.
  - » Mejor capacidad de administración.
  - » Permite administración centralizada.
  - » Mayor nivel de seguridad.
  - » Más facilidad de protección y recuperación de datos.

La pila de protocolos Windows incluye los siguientes:

- IPX/SPX (*Internetwork Packet Exchange/Sequenced Packet Exchange* – intercambio de paquetes de red de trabajo interconectada/intercambio de paquetes secuenciados). Intercambio con redes Novell.

- TCP/IP. Nativo desde Windows 2000 Server. Integra redes Windows con otro tipo de redes, conexión a redes WAN y acceso a Internet.

- Acceso telefónico a redes. Protocolos de redes de marcación en enlaces punto a punto.

  - SLIP (*Serial Line Internet Protocol* – protocolo de Internet de línea en serie). Acceso a máquinas UNIX e Internet. Servicio de conexión no fiable.

  - PPP (*Point-to-Point Protocol* – protocolo punto a punto). SLIP mejorado con acceso fiable.

  - PPTP (*Point-to-Point Tunneling Protocol* – protocolo de *tunneling* punto a punto). PPP con cifrado de comunicaciones. Usado en conexiones seguras tipo VPN a través de Internet.

- SMB (*Server Message Block* – bloque de mensajes de servidor). Usado para compartir archivos e impresoras. Renombrado como CIFS (*Common Internet File System* – sistema común de ficheros de Internet).

- NetBIOS (*Network Basic Input Output System* – sistema básico de entrada/salida de red). Proporciona un interfaz entre las aplicaciones y la pila de protocolos, asignando nombres simbólicos (nombres NetBIOS) a los recursos de la red.

- NetBEUI (*NetBIOS Extended User Interface* – interfaz de usuario extendido de *NetBIOS*). Antiguo protocolo nativo Windows de red y transporte, no encaminable y recomendable sólo para redes pequeñas de un solo segmento (menos de 50 máquinas Windows).

- WINS (*Windows Internet Naming Service* – servicio de nombres de Internet de Windows). Proporciona el servicio de nombres de *NetBIOS*.

- LDAP (*Lightweight Directory Access Protocol* – protocolo ligero de acceso a directorio). Permite acceder a los servicios de directorio de una red.

- DLC (*Data Link Control* – control de enlace de datos). Conexión con impresoras de red y con *mainframes*.

10.3. Otras arquitecturas de protocolos

- Xerox XNS (*Xerox Network Services* – servicios de red de Xerox). Fue el estándar de facto del mercado hasta la aparición de TCP/IP. Implementaba transmisión fiable y llamadas a procedimientos remotos.

- DEC DNA (*Digital Network Architecture* – arquitectura de red digital). Una de las primeras redes *peer-to-peer* (igual a igual), inicialmente presentaba 4 niveles, para posteriormente adaptarse a los 7 niveles OSI.

- Novell Netware. Previa a OSI, similar a TCP/IP en su esquema de capas. Basada en XNS de Xerox. Es un modelo cliente/servidor con clientes y servidores dedicados.

- Honeywell DSA (*Distributed Systems Architecture* – arquitectura de sistemas distribuidos). Respetaba por completo el modelo OSI.

- Otras: HP Advancenet, Burroughs BNA, ICL IPA, Data General Xodiac y Wang WSN.

11. Características de las redes de área local

El diccionario Merriam-Webster definió en 1977 "red de área local" (de ahora en adelante LAN – *Local Area Network*) como "una red de ordenadores personales en un área pequeña (como una oficina) para compartir recursos (como una impresora) o intercambiar datos".

Algunas de sus características principales son las siguientes:

- Red privada.
- Velocidad media/alta, de 1 Mbps a 10 Gbps.
- Tasa de errores baja, debido a las cortas distancias cubiertas.

11.1. Componentes de una LAN

- Tarjeta de Interfaz de Red (NIC – *Network Interface Card*). Es la interfaz necesaria para que una estación de trabajo se pueda conectar a la red. Puede estar unida al equipo de múltiples formas: mediante una ranura de expansión, un puerto de conexión serie (USB, por ejemplo) o, incluso, integrada en la placa madre del ordenador.

- Medio de transmisión. Infraestructura por la que se transmite la información entre los nodos de la red. Puede ser un sistema de cableado, un medio inalámbrico o ambos.

- Dispositivos de interconexión. Conectan partes de una red, la amplían o conectan redes distintas. Son típicamente el repetidor (*repeater*), concentrador (*hub*), conmutador (*switch*), puente (*bridge*), punto de acceso inalámbrico (*access point*), encaminador (*router*) y pasarela (*gateway*).

- Periféricos y recursos compartidos. Dispositivos conectados a nodos de la red como impresoras, *plotters*, discos ópticos, CD-ROM, etc.

- Servidores. Ofrecen una serie de servicios tanto a los usuarios como a los administradores de la red. Algunos ejemplos son:
  - Controlador de Dominio: administra privilegios sobre recursos (Active Directory de Windows, Open LDAP, Novell).
  - Servidor DNS (*Domain Name Service* – Servicio de Nombre de Dominio): guarda los registros DNS, que establecen la correspondencia entre nombres de máquinas y direcciones IP.
  - Servidor DHCP: asigna automáticamente direcciones IP, coordinándose con el servidor DNS.
  - Proxy: funciones de *cache* para optimizar el rendimiento, así como funciones de control de seguridad a nivel de aplicación, actuando de intermediario entre las estaciones de trabajo y el servidor final que proporciona los servicios de aplicación.
  - Servidor de impresión: administra las colas de impresión y el acceso a las impresoras compartidas en la red.
  - Servidor de ficheros: proporciona a los diferentes usuarios de la red un espacio para el almacenamiento y compartición de información.
  - Servidor de base de datos: aloja datos de forma estructurada.
  - Servidor de aplicaciones: permite el acceso a aplicaciones desde cualquier parte de la red.

- Servidor de fax: permite mandar faxes desde cualquier punto de la red.

- Estaciones de trabajo (*workstations*). Son aquellos equipos que utilizan los usuarios de la red para acceder a los recursos. Se conectan a la red convirtiéndose en un nodo de la misma. Pueden ser equipos con o sin disco duro (arranque remoto) y con distintos sistemas operativos.

- *Software*. Sistemas operativos de red, protocolos de red, clientes y servicios de red.

11.2. Aplicaciones de LAN

- LAN de PCs. Crear una LAN a base de ordenadores personales es una tendencia en alza, debido al bajo coste de estos. En algunos casos los PCs se combinan con servicios de procesamiento central, ya que determinados programas requieren demasiada capacidad de proceso o fiabilidad de almacenamiento como para ejecutarse en un PC.

  En contra de la antigua visión centralizada de las redes de ordenadores, la tendencia actual es descargar de trabajo a los ordenadores centrales, transfiriendo la carga de procesamiento a los PCs. Una implementación usual de esta configuración son las aplicaciones cliente/servidor.

- Redes de respaldo y almacenamiento. Las redes de respaldo (*backend*) se utilizan para interconectar grandes sistemas, tales como ordenadores centrales, supercomputadores y dispositivos de almacenamiento masivo. Sus características típicas son:
  - Alta velocidad. Debido al gran volumen de tráfico se necesitan grandes velocidades y anchos de banda e interfaces de alta velocidad entre equipos.
  - Distancia limitada. Este tipo de redes suelen ocupar una sala de computadores o un número reducido de habitaciones contiguas.
  - Número limitado de dispositivos. Dado el coste y las características especiales de los dispositivos, el número de éstos es bastante inferior al de equipos en una LAN típica.

  Un concepto relacionado con el de *backend* es el de red de almacenamiento (SAN – *Storage Area Network*). Se trata de una red independiente que proporciona una infraestructura de almacenamiento en la red, así como el acceso a la información almacenada. De ese modo se desliga a los servidores de dichos procedimientos de acceso y de soportar la capacidad de almacenamiento necesaria. Entre sus dispositivos hay discos duros, unidades de cinta y grabadores de CD y DVD.

- Redes ofimáticas de alta velocidad. Típicamente las oficinas no necesitaban altas velocidades de transferencia. Sin embargo cada día surgen más redes donde aplicaciones de envío de fax, procesadores de imágenes de documentos, programas gráficos y transmisión de audio y vídeo requieren velocidades más elevadas. Dada la evolución del *hardware* en calidad y precio, una red con velocidades superiores a 10 Gbps es más que posible.

- LAN troncales. El crecimiento en el tamaño de las LAN ofimáticas ha propiciado la necesidad de una estrategia LAN flexible. Una LAN que cubra un edificio entero estará sujeta a problemas de seguridad, eficiencia y capacidad. La alternativa es emplear varias LAN de bajo coste en las plantas del edificio, o incluso en departamentos concretos, y unirlas a través de LAN troncales o *backbone*. Dichas troncales poseen mayor capacidad y fiabilidad.

11.3. Arquitectura de LAN

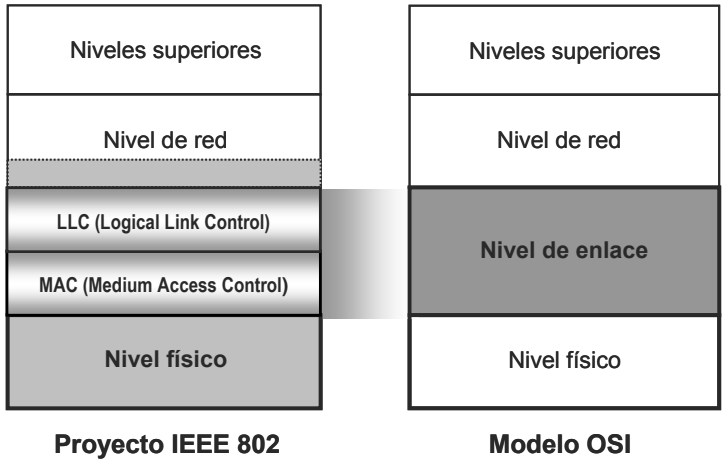
El organismo de estandarización IEEE (*Institute of Electrical and Electronics Engineers* – Instituto de ingenieros eléctricos y electrónicos) inició el proyecto 802 en 1985. El objetivo de dicho proyecto era definir estándares de comunicación entre equipos de distintos fabricantes, especialmente en lo referente a los niveles inferiores del modelo OSI.

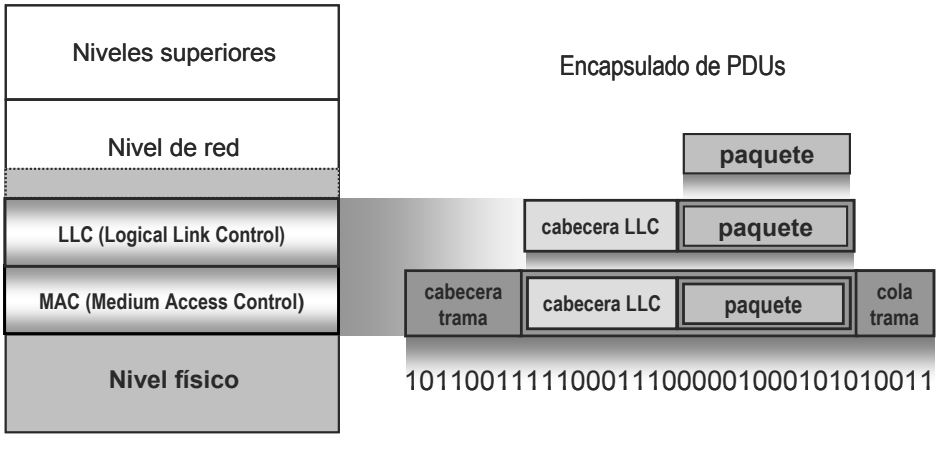
Los estándares IEEE más utilizados en la actualidad (especialmente en conjunción con TCP/IP) son los desarrollados por sus grupos de trabajo 802.3 (Ethernet) y 802.11 (redes WLAN, inalámbricas). Otros estándares IEEE 802 son 802.15 (redes WPAN o *Wireless PAN*, estándar conocido como *Bluetooth*) y 802.16 (redes WMAN o *Broadband Wireless MAN*, estándar más conocido por el nombre de la asociación WiMAX, que agrupa empresas relacionadas con su desarrollo e implantación).

Según IEEE 802 el nivel de enlace se divide, a su vez, en dos subniveles:

- Subcapa LLC. Control del enlace lógico. Se encarga del control del diálogo y la sincronización entre emisor y receptor, control de flujo y control de errores. Es común en la mayoría de LAN actuales.

- Subcapa MAC. Control de acceso al medio compartido, necesario en redes de difusión.





12. Normalización

De cara a la homogeneidad de los sistemas de comunicaciones, los distintos fabricantes, países y organismos internacionales definen una serie de normas comunes que establecen de qué modo se llevará a cabo la comunicación, tanto en el nivel lógico como en el físico.

Siempre y cuando se respete la legislación estatal, los fabricantes pueden proponer sus propias normas o bien acogerse a los estándares definidos por asociaciones de estandarización. Hay dos tipos de estándares:

- De facto o de hecho. No está oficialmente definido, pero se acepta por su uso generalizado.
- De *iure* o de derecho. Legislado por un organismo oficialmente reconocido.

A continuación se listan algunas de las asociaciones de estandarización más importantes:

Organismo	Significado	Enfoque
AENOR	Asociación Española de Normalización y Certificación	Miembro de ISO
ANSI	*American National Standards Institute*	Estandarización. LAN y WAN
Broadband Forum	*Broadband Forum*. Incluye los antiguos *ADSL Forum*, *ATM Forum* y *Frame Relay Forum*	Tecnologías de banda ancha (ADSL, Frame Relay, ATM)
EIA	*Electronic Industries Association*. Dejó de operar en 2010, pasando sus estándares a la ECA (*Electronic Components Association*) que se fusionó en 2011 con la NEDA (*National Electronics Distributors Association*) para formar la ECIA (*Electronic Components Industry Association*)	Interfaces físicas y eléctricas
ETSI	*European Telecommunications Standards Institute*	Telecomunicaciones en general
IEEE	*Institute of Electrical and Electronics Engineers*	LAN y WAN
IETF	*Internet Engineering Task Force*	Internet
IMTC	*International Multimedia Teleconferencing Consortium*	Videoconferencia
ISO	*International Organization for Standardisation*	Tecnologías de la Información
ITU	*International Telecommunications Union*	Telecomunicaciones
ITU-T	*Telecommunication Standardization Sector*. Antiguo CCITT (*International Telegraph and Telephone Consultative Committee*)	Telecomunicaciones
SANS	*Systems Administration Network Security*	Seguridad en redes
TIA	*Telecommunications Industry Association*	Telecomunicaciones
W3C	*World Wide Web Consortium*	Tecnologías web
Wi-Fi Alliance	Asociación de empresas que garantiza la interoperabilidad entre dispositivos inalámbricos fabricados de acuerdo a la norma IEEE 802.11	Certificación de redes WLAN y dispositivos inalámbricos

Existen agencias reguladoras, como el FCC (*Federal Communications Commission*) estadounidense o la CMT (Comisión del Mercado de las Telecomunicaciones) española, que regulan las tecnologías de comunicaciones con el objetivo de proteger el interés público.

En Internet se desarrollan y se publican estándares y recomendaciones en documentos denominados RFC (*Request For Comments* – petición de comentarios), listados en http://www.ietf.org/download/rfc-index.txt.