SEGUNDA UNIDAD: EL MODELO OSI

Las primeras redes LAN, MAN y WAN demostraron rápidamente su utilidad, pero eran sistemas cerrados y poco escalables, a principios de la década de los 80 el crecimiento en la cantidad y tamaño de las redes se volvió exponencial, lo que produjo un auge en la tecnología de networking, con la aparición de nuevas tecnologías y productos de red. A mediados de los 80, los problemas de compatibilidad y escalabilidad se volvieron inmanejables, existían diferentes especificaciones en los sistemas de networking propietarios (pertenecientes y controlados por organizaciones privadas). La necesidad de un sistema abierto era innegable, donde el uso libre de la tecnología debe estar disponible para todos. Para enfrentar el problema la Organización Internacional para la Normalización (ISO) estudió esquemas de red como DECNET, SNA y TCP/IP para encontrar un conjunto de reglas y desarrolló un modelo de red que ayudaría a los fabricantes a crear redes que fueran compatibles y que pudieran operar con otras redes, de manera transparente, para ello se trazó la meta de dividir comunicaciones complejas en tareas más pequeñas, especializadas y separadas a manera de una línea de fabricación de un producto en grandes cantidades.

El modelo de *Interconexión de Sistemas Abiertos* (OSI, Open System Interconection) fue presentado en 1984 como un el modelo de red descriptivo, este modelo proporcionó a los fabricantes un conjunto de estándares que aseguraron la compatibilidad e interoperabilidad entre los distintos tipos de tecnologías de red existentes a nivel mundial. En un segunda momento, siguiendo el esquema de este modelo se crearon protocolos al principio muy rígidos, pero que soportaron el desarrollo de las comunicaciones, Alrededor de 1995 comienzan a aparecer protocolos más flexibles, donde las capas no están tan demarcadas y la correspondencia con los niveles no es tan clara, lo que centra la atención en las arquitecturas (realizaciones físicas) específicas, sin embargo sigue siendo el esquema lógico que permite entender el intercambio de información.

El modelo en sí mismo no puede ser considerado una arquitectura, ya que no especifica el protocolo que debe ser usado en cada capa, por esta razón es que cuando se le menciona, suele hablarse de “modelo de referencia”.

2.1 ESTÁNDARES DE REDES

La cantidad y tamaño de los sistemas de comunicación o redes ha crecido exponencialmente, desde su aparición, para garantizar las condiciones de escalabilidad, confiabilidad y calidad de servicio, propias de un sistema abierto, la Organización Internacional para la Normalización (ISO) definió en 1984 un modelo de referencia, con la finalidad de que los diseñadores de red pudieran implementar redes que luego pudieran comunicarse y trabajar en conjunto (interoperabilidad).

La IEEE (The Institute of Electrical and Electronics Engineers), es la mayor asociación internacional sin fines de lucro formada por profesionales de la tecnologías, que tiene como uno de sus principales fines el trabajar hacia la estandarización, en el campo de las redes y la comunicación de datos, ha desarrollado el *Proyecto 802* (febrero de 1980) que definió *estándares de redes para los componentes físicos* de una red (la tarjeta de red y el cableado) que corresponden a los niveles físico y de enlace de datos del modelo OSI. Las especificaciones 802 definen la forma en que las tarjetas de red acceden y transfieren datos sobre el medio físico. Éstas incluyen conexión, mantenimiento y desconexión de dispositivos de red.

Asimismo, la selección del protocolo a ejecutar en el nivel de enlace de datos define la velocidad de la red de área local, el método utilizado para acceder a la red física, los tipos de cables que se pueden utilizar y las tarjetas de red y dispositivos que se instalan.

Los organismos encargados de fijar estándares son:

- ✓ La Organización Internacional para la Estandarización (ISO)
- ✓ El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE)
- ✓ El Instituto Nacional Estadounidense de Estándares (ANSI)
- ✓ La Unión Internacional de Telecomunicaciones (ITU)
- ✓ La Asociación de Industrias Electrónicas/Asociación de la Industria de las Telecomunicaciones (EIA/TIA)

- ✓ Autoridades de las telecomunicaciones nacionales, como la Comisión Federal de Comunicaciones (FCC) en EE.UU.

2.2 MODELO OSI

El modelo de referencia OSI es el modelo principal para las comunicaciones por red, todos los fabricantes de redes relacionan sus productos con el modelo de referencia OSI, sobre todo en la capacitación de sus usuarios. Este modelo permite entender las funciones de red que se producen en cada capa y permite entender cómo se mueve la información a través de una red, dividida en muchos paquetes de datos, generada en los programas de aplicación (por ej., hojas de cálculo, documentos, etc.), a través de un medio de red (por ej., cables, etc.), hasta otro programa de aplicación ubicado en otro computador de la red, aun cuando el transmisor y el receptor tengan distintos tipos de medios de red.

El modelo de referencia OSI, está dividido en siete capas numeradas, cada una soportando una función de red distinta, lo que se denomina división en capas. Esta división aporta las siguientes ventajas:

- Divide la comunicación de red en partes más pequeñas, independientes y especializadas.
- Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes.
- Permite a los distintos tipos de hardware y software de red comunicarse entre sí (interoperatividad).
- Impide que los cambios en una capa puedan afectar las demás capas, para que se puedan desarrollar cada una de ellas con independencia y mayor rapidez.
- Divide la comunicación de red en partes más pequeñas claramente identificable.

El modelo de interconexión de sistemas abiertos (OSI) tiene siete capas, desde la más baja en la jerarquía (la física) y hacia la más alta (la aplicación). Las capas se apilan de esta forma:

Figura 2.1 Modelo OSI

El propósito de cada capa es proveer los servicios para la capa superior, haciendo invisible a esta capa superior los detalles de cómo los servicios son implementados (de manera vertical funciona bajo un modelo de tipo cliente/servidor). Las capas son abstraídas físicamente, de tal manera que cada capa cree (de manera lógica) que se está comunicando con la capa equivalente en la otra computadora, usando las reglas definidas por un protocolo específico, cuando realmente cada capa se comunica sólo con las capas adyacentes de la misma computadora.

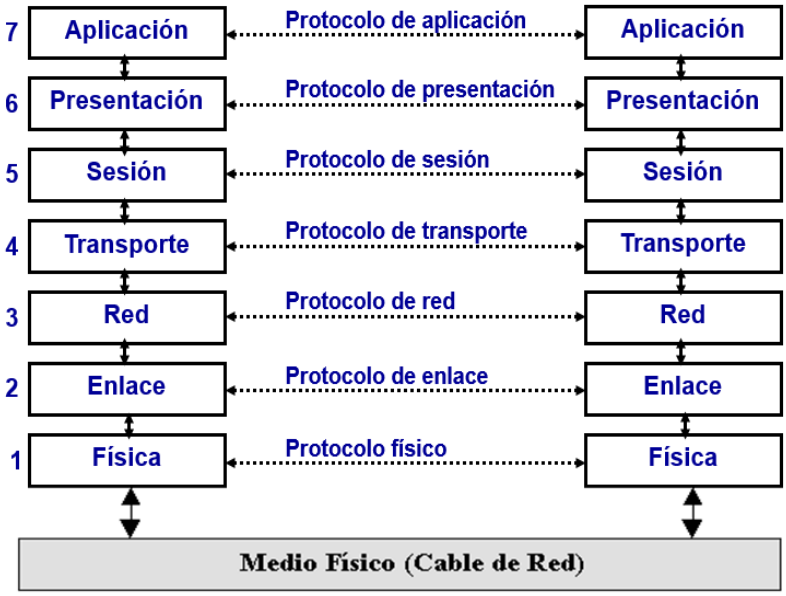

Figura 2.2 Modelo físico/lógico de comunicación entre dos hosts

A excepción de la capa más baja del modelo OSI, ninguna capa puede pasar información directamente a su equivalente en la otra computadora. La información que envía una computadora debe de pasar por todas las capas inferiores, hasta llegar al nivel físico, la información entonces se mueve a través del cable de red hacia la computadora que recibe y hacia arriba a través de las capas de esta hasta que llega al mismo nivel de la capa que envió la información. La interacción entre las capas adyacentes se llama **interface**, esta define qué servicios de la capa inferior son ofertados a la capa superior y como esos servicios son accesados. La serie de las reglas que se usan para la comunicación entre las capas se llama **protocolo**.

2.2.1 Funciones de los niveles del modelo OSI

Aunque se verán a detalle de manera individual, la función general de cada capa se indica a continuación

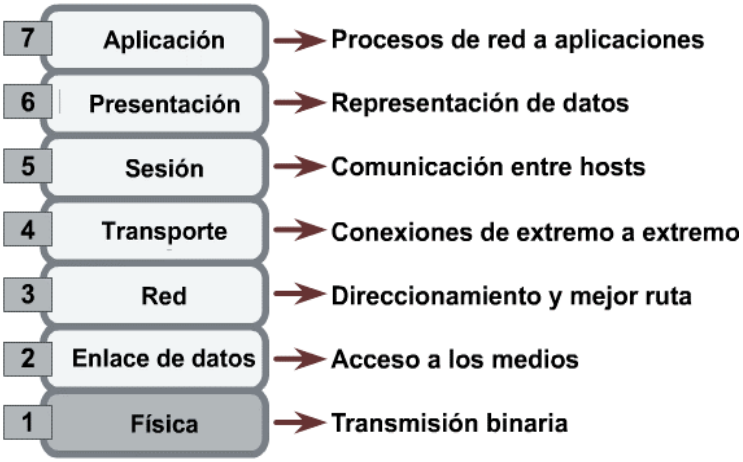

Figura 2.3 La función por cada capa

- *Capa de aplicación*: define como el usuario accede a la red, para una transferencia de archivos, login remoto, correo electrónico, consulta a bases de datos, etc.

- *Capa de presentación*: establece una sintaxis y semántica de la información transmitida, define la estructura de los datos a transmitir (campos de un registro: nombre, dirección, teléfono, etc). Define el código a usar para representar una cadena de caracteres (ASCII, EBCDIC, etc), y las funciones asociadas a la compresión de datos y la seguridad (criptografía).

- *Capa de sesión*: permite a usuarios en diferentes máquinas establecer una sesión. Una sesión puede ser usada para efectuar un login a un sistema de tiempo compartido remoto, para transferir un archivo entre 2 máquinas, etc. Controla el diálogo (quién habla, cuándo, cuánto tiempo, half duplex o full duplex) y se encarga de la función de sincronización en la comunicación.

- *Capa de transporte*: establece conexiones punto a punto sin errores para el envío de mensajes. Permite multiplexar una conexión punto a punto entre diferentes procesos del usuario. Provee la función de difusión de mensajes (broadcast) a múltiples destinos y el control de flujo.

- *Capa de red*: divide los mensajes de la capa de transporte en paquetes y los ensambla. Utiliza el nivel de enlace para el envío o de paquetes, previo enrutamiento de paquetes. Para el envío de paquetes lo hace de nodo a nodo usando ya sea un circuito virtual o como datagramas. Finalmente se ocupa del control de la congestión.

- *Capa de enlace de datos*: estructura el flujo de bits bajo un formato predefinido llamado trama, para lo que agrega una secuencia especial de bits al principio y al final del flujo inicial de bits. Transfiere tramas de una forma confiable libre de errores (utiliza reconocimientos y retransmisión de tramas).

- *Capa física*: se encarga de la transmisión de flujo de bits a través del medio, por lo que se encarga de manejar las señales eléctricas, específica cables, conectores y componentes de interfaz con el medio de transmisión.

2.2.2 Capa física

Es la más baja del modelo OSI, se encarga de la transmisión y recepción de una secuencia no estructurada de bits sin procesar a través de un medio físico. Describe las especificaciones de las interfaces en tres aspectos: eléctrico/óptico, mecánico y funcional para poder accesar al medio físico, y en el caso de funcionar como receptor lleva las señales recibidas enviándolas hacia las capas superiores.

Funciones:

- Codificación de datos: modifica el modelo de señal digital sencillo (1 y 0) que utiliza el equipo para acomodar mejor las características del medio físico y para ayudar a la sincronización entre bits y trama. Determina:
  - ✓ Qué estado de la señal representa un binario 1
  - ✓ Como sabe la estación receptora cuándo empieza un bit, en término de tiempos
  - ✓ Cómo delimita la estación receptora una trama

- Como anexarse al medio físico, define:
  - ✓ Si se usa un transceptor externo (MAU) para conectarse con el medio
  - ✓ Forma física de los conectores y la función de cada patilla

- Técnica de transmisión: si se transmiten los bits codificados por señalización de banda base (digital) o de banda ancha (analógica).

- Transmisión de medio físico: transmite los bits como señales eléctricas u ópticas según medio físico:
  - ✓ Qué medios físicos pueden utilizarse, en función a sus características (cable de pares trenzados (o no, como en RS232/EIA232), coaxial, guías de onda, aire, fibra óptica.)

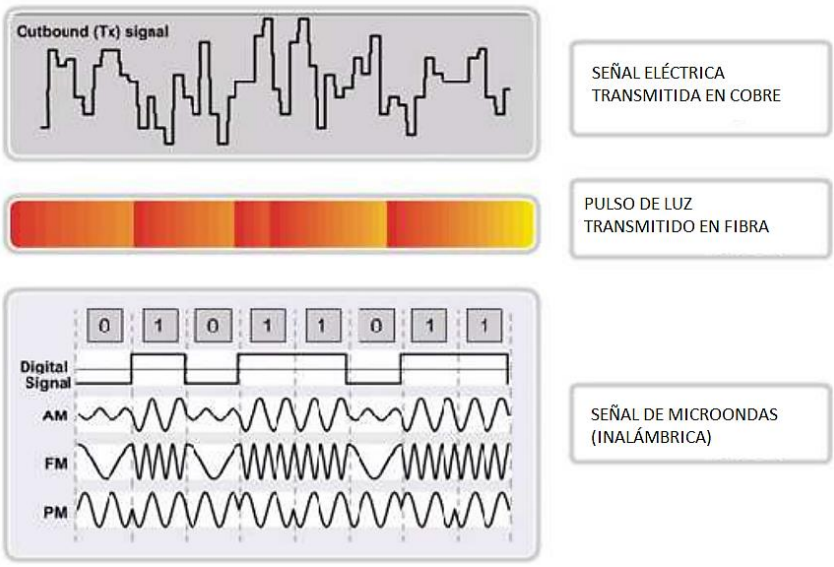

Figura 2.4 Medio físico/señal usada

- ✓ Cuántos voltios/db se deben utilizar para representar un estado

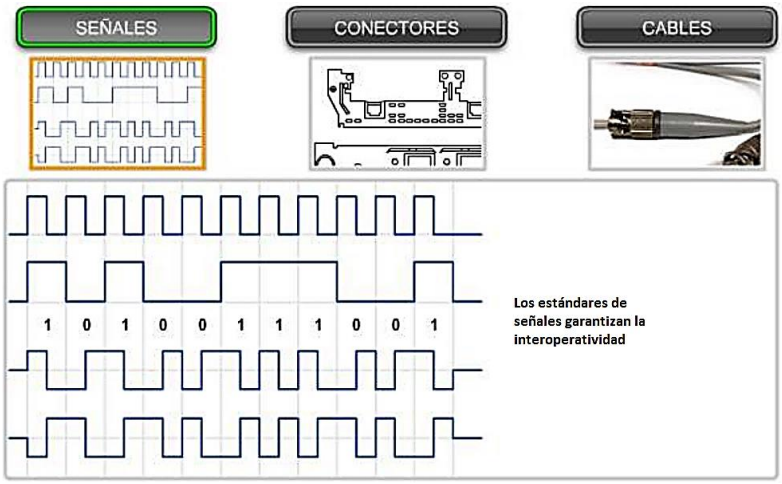

Figura 2.5 Señales

- ✓ Especificar cables, conectores y componentes de interfaz con el medio de transmisión, polos en un enchufe, etc.

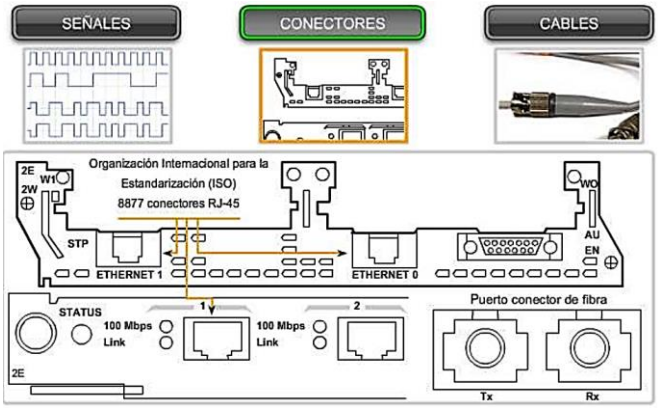

Figura 2.6 Conectores

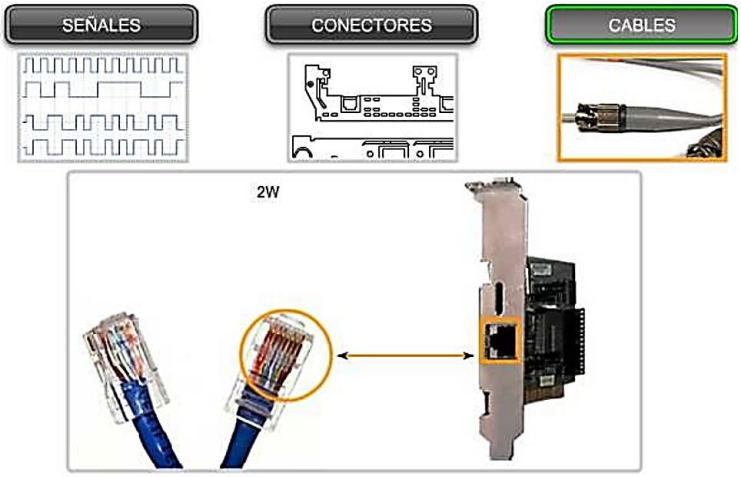

Figura 2.7 Cables

Entonces los **estándares** asociados (ISO-IEEE-ANSI-ITU-EIA/TIA) definen:

- Propiedades físicas y eléctricas de los medios
- Definición de señales para la información de control
- Propiedades mecánicas de los conectores

Problemas a considerar:

- Interferencia de señal externa
- Los datos se transmiten en cables de cobre como impulsos eléctricos, por lo que se requiere un detector en la interfaz de red del dispositivo de destino debe recibir una señal que pueda decodificarse exitosamente para que coincida con la señal enviada.
- Los valores de voltaje y sincronización en estas señales son susceptibles a interferencias o "ruidos" generado fuera del sistema de comunicaciones, las que pueden distorsionar y corromper las señales de datos que se transportan por los medios de cobre (ondas de radio y dispositivos electromagnéticos como fluorescentes, motores eléctricos y otros).

Equipos (dispositivos de red) adicionales en esta capa:

- Repetidores, equipos que amplifican la señal, pudiendo también regenerarla.
- Concentradores o hubs, equipos de interconexión usados en topología física estrella para convertirla en un bus lógico
- Conmutadores (switches) que actúan no sólo a nivel físico sino también de enlace.

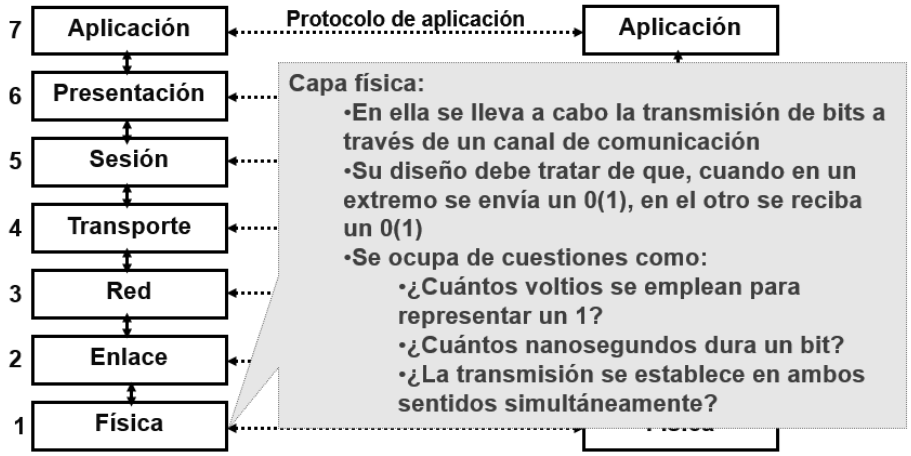

Figura 2.8 Capa física

2.2.3 Capa de enlace de datos

Ofrece una transferencia sin errores de datos desde un nodo a otro a través de la capa física (control de acceso al medio), por lo que las capas superiores asumen la transmisión sin errores (transferencia de datos confiable en el medio), para ello utiliza bloques de información denominadas tramas.

Funciones:

- Establecimiento y finalización de enlaces: establece y finaliza el enlace lógico entre dos nodos.
- Control del tráfico de tramas: mientras existan tramas en el buffer de transmisión
- Secuenciación de tramas: transmite y recibe tramas secuencialmente.
- Confirmación de trama: envía o espera confirmaciones de trama. Detecta errores y se recupera de ellos cuando se producen en la capa física mediante la retransmisión de tramas no confirmadas y el control de la recepción de tramas duplicadas.
- Delimitación de trama: crea y reconoce los límites de la trama.
- Comprobación de errores de trama: comprueba la integridad de las tramas recibidas.
- Administración de acceso al medio: determina si el nodo "tiene derecho" a utilizar el medio físico.
- Direccionamiento físico
- Topología de la red

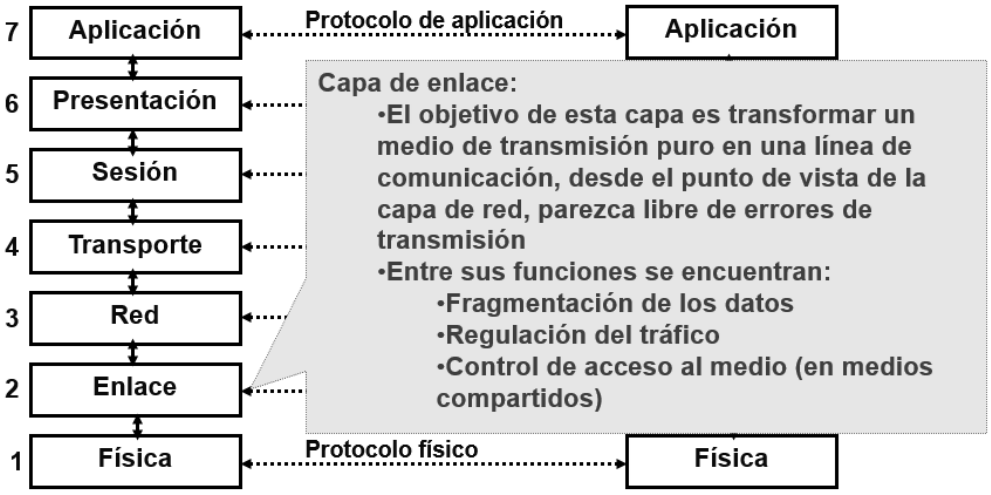

Figura 2.9 Capa de enlace de datos

La tarjeta NIC (Network Interface Card, Tarjeta de Interfaz de Red en español o Tarjeta de Red) se encarga que tengamos conexión a la red y soporta que esta capa de Enlace de Datos esté **subdividida en las subcapas de Control de Acceso a Medios (MAC) y de Control de Enlaces Lógicos (LLC)**. La primera reside en el hardware y la segunda en los drivers de la tarjeta

La subcapa LLC provee las direcciones de Puntos de Acceso a Servicios (SAP's) para las capas superiores, mientras que la subcapa MAC provee la dirección física de red de un dispositivo. Las SAP's son específicamente las direcciones de uno o más procesos de aplicaciones ejecutándose en una computadora o dispositivo de red.

a) Subcapa Logical Link Control (LLC)

Las *funciones* de esta subcapa son:

- Gestión del enlace: orientado a conexión, no orientado a conexión
- Establecer el sincronismo de tramas o caracteres
- Recuperar errores de transmisión

Provee los siguientes *servicios* o modos de operación:

- Servicio orientado a la conexión CONS (Connection Oriented Network Service) (envío en secuencia y con recuperación de errores), en el que una sesión es empezada con un destino, y sólo terminada cuando la transferencia de datos se completa. Cada nodo participa activamente en la transmisión, pero cada sesión requiere un tiempo de configuración y monitoreo en ambas estaciones. Es un servicio que establece una conexión entre las estaciones del enlace, y que garantiza la entrega de las unidades de datos que fluyen a través de dicha conexión (servicio confiable). El servicio de conexión (VC o circuito virtual) le garantiza al receptor la entrega en secuencia de las unidades de datos y la protección contra pérdidas y duplicados. Con ese fin dispone de los mecanismos necesarios para controlar el flujo y corregir los errores, es claro que en este caso se usan identificadores de conexión y no direcciones. Este servicio contiene tres fases

  1) Establecer el canal de comunicación
  2) Transmitir datos
  3) Terminar la conexión

  Los circuitos virtuales pueden ser de dos tipos: conmutados (Switched Virtual Circuits SVC) o permanentes (Permanent Virtual Circuits PVC)

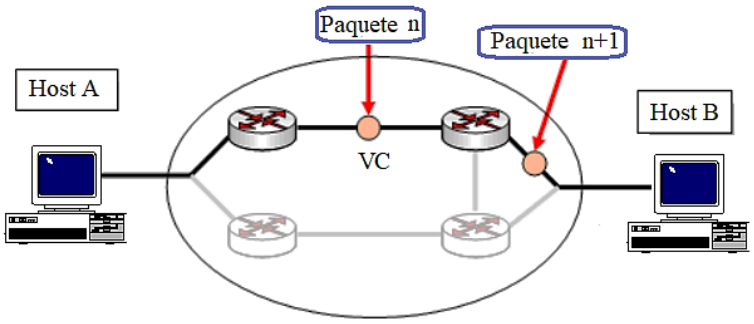

Figura 2.10 LLC-Servicio orientado a la conexión

- No orientado a conexión (Connection Less Network Service CLNS), la conexión es menos formal, la información se envía por paquetes, usando direcciones, no es necesario la existencia de un circuito virtual, por lo que cada paquete puede seguir un camino diferente, ser almacenados por nodos intermedios, duplicados, retransmitidos, etc.

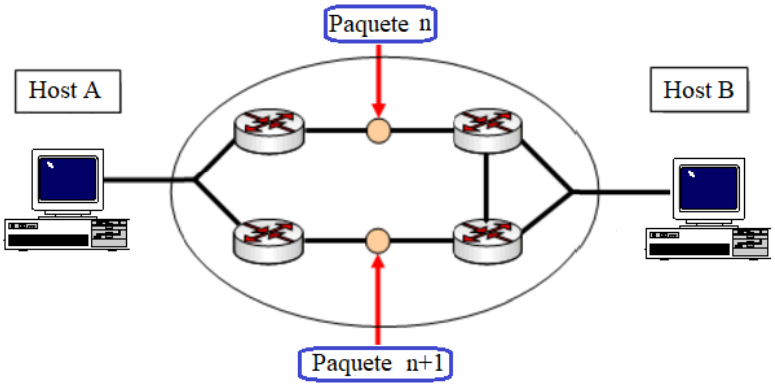

Figura 2.11 LLC-Servicio no orientado a la conexión

Existen dos tipos de servicios sin conexión

- Sin confirmación o por datagrama, cada paquete viaja de forma independiente, sin ningún seguimiento *Send & Pray* (sin control de flujo ni corrección de errores), en el cual no se define una sesión. Los paquetes son puramente enviados a su destino. Los protocolos de alto nivel son responsables de solicitar el reenvío de paquetes que se hayan perdido. Este es el servicio normal en redes de área local (LAN's), por su alta confiabilidad.

- Con confirmación o acuse de recibo (ASK), el receptor debe enviar el reconocimiento de que ha recibido la información (permite la recuperación de errores y ordenar la información), similares al anterior, pero en el que son reconocidos los paquetes de transmisión de cada sesión (cada aplicación corriendo).

Los dispositivos de red que soportan la tarea de recuperación de errores son los switchs, para ello se requiere haber introducido redundancia en la data; se tiene que identificar que el bit recibido está errado (la probabilidad de que la información tenga errores es igual a la probabilidad de no detectar el error). Las principales técnicas de recuperación de errores son: ARQ (Automatic Repeat reQuest) y FEC (Forward Error Correction). La primera evalúa la presencia de errores y, en caso afirmativo, le solicita al origen que retransmita nuevamente el paquete. Bajo las técnicas FEC, el receptor es capaz de recuperar la información original, sin requerir una retransmisión. La conveniencia en utilizar una técnica u otra dependerá de las características del canal.

b) Subcapa Medium Access Control (MAC)

El control de acceso MAC está asociado a la topología de red (forma de interconexión física de los hosts) elegida, y soporta la función de encaminamiento dentro de la subred. Para redes con topología en bus, se utiliza la técnica de transmisión de información bajo la autorización de un token o mediante el tratamiento de colisiones; para topología en anillo, se utiliza la retransmisión entre estaciones, y la activación selectiva del transceptor (retransmisor). A este nivel, operan las tarjetas de red (NIC), y a cada una de ellas le corresponde una única dirección física universal MAC compuesta por 48 bits.

Las principales técnicas MAC se agrupan en tres grandes categorías:

- Reserva: la asignación estática de la capacidad del canal entre las N estaciones que conforman la red (como una multiplexación en tiempo, cada canal tiene asignado un intervalo de la trama). Ejemplos: Reservation Aloha y PRMA (Packet Reservation Multiple Access)

- Sondeo y Selección: se utilizan en sistemas centralizados y jerárquicos.

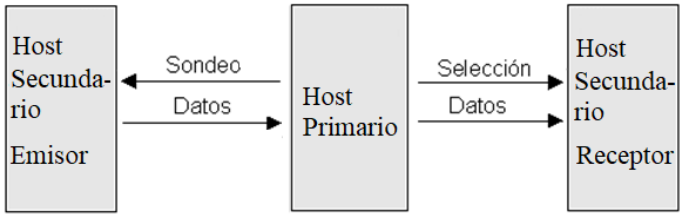

Figura 2.12 MAC: Sondeo y Selección

Para la Selección, se establece un host *Primario* que controla el flujo de información en la red, el que interroga a los demás hosts sobre la necesidad de efectuar una transmisión, el host *Secundario* que tiene datos, responde enviando su información al *Primario*, quien se encarga de retransmitirla al host destino correspondiente (Maestro/Esclavo).

Para el Sondeo la estación primaria puede usar una de tres técnicas:
  - Por lista (polling), se establece una lista con todas las estaciones secundarias de la red, y se van interrogando una a una en forma circular (centralizado).
  - Por prueba, las estaciones secundarias se agrupan en varios conjuntos, y se interroga primero a los conjuntos, ahorrando tiempo en el proceso de sondeo (centralizado).
  - Por Token, organizando lógicamente a los hosts en un anillo (distribuido)

- Contienda: En ellas las estaciones compiten entre sí por el uso del canal, presentan retardos de acceso bajos cuando hay poco tráfico y su principal inconveniente está cuando hay excesiva demanda del canal (alta carga). Los protocolos de contienda no garantizan ni la equidad ni el tiempo máximo para el acceso al canal.

- Contienda simple (Aloha): El host transmite cuando tiene datos pendientes, si el Primario recibe dos o más transmisiones simultaneas, se produce colisión y no indica la recepción, los hosts emisores al no recibir asentimiento asumen la colisión esperando un tiempo aleatorio para repetir la transmisión. El periodo de tiempo que una trama o paquete puede sufrir colisión (periodo vulnerable) es de *2T*, siendo *T* el tiempo que se tarda en transmitir una trama. Este método permite como máximo aprovechar el 18% de la capacidad del canal, un mayor uso genera el bloqueo del canal.

Figura 2.13 Contienda simple

- Contienda ranurada (slotted Aloha): mejora del anterior, todos los hosts usan la misma señal de reloj (sincronizados). Se divide el tiempo en intervalos o ranuras de longitud fija *T* (igual al tiempo de trama) y se impone la condición de que una estación tan sólo puede transmitir al comienzo de una ranura. Reduce el periodo vulnerable y el tiempo perdido a *T* y el rendimiento del canal sube al doble (32% de la capacidad canal para los usuarios).

Figura 2.14 Contienda ranurada

- Contienda con escucha (CSMA: Carrier Sense Medium Access) mejora el rendimiento de la contienda simple y ranurada en los casos dónde el tiempo de transmisión del paquete (*T*) sea muy superior al tiempo máximo de propagación de la señal en el medio (*tp*). Cuando una estación tiene un paquete que transmitir escucha el medio físico para verificar si está libre u ocupado. En caso de que esté ocupado retrasa la transmisión, evitando así una colisión. Este método no evita del todo las colisiones, ya que, si dos estaciones quieren transmitir a la vez, ambas encontrarán el medio libre y se producirá colisión. En el caso más desfavorable, una estación no se dará cuenta de que otra está transmitiendo hasta pasados *tp* segundos, que será ahora el periodo vulnerable. La eficacia de este método se incrementa (y por tanto el caudal eficaz) conforme el ratio $a = tp/T$ se reduce (esto es, para tramas grandes y tiempos de propagación pequeños). En caso de producirse una colisión, el tiempo perdido será ahora de (en el peor de los casos) $T+2tp$.

  - ✓ CSMA-0 Persistente: si el canal está libre transmite y si está ocupado espera un tiempo aleatorio (el mismo que ante una colisión) y vuelve a comprobar el canal

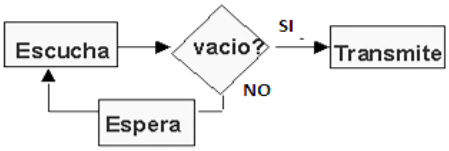

Figura 2.15 CSMA-0 Persistente

  - ✓ CSMA-1 Persistente: si el canal está libre transmite y si está ocupado chequea continuamente el canal, transmitiendo en cuanto queda libre

  - ✓ CSMA-p Persistente: si el medio está libre transmite y si está ocupado chequea continuamente hasta que quede libre, en cuyo caso usa un esquema de transmisión rasurado:
    - En canal al inicio de un nuevo slot (*tp*) el host transmite con probabilidad *p* y espera al siguiente slot con probabilidad *1-p*
    - Si el canal está libre en el nuevo instante, repite lo anterior.

- Si el canal estuviera ocupado, espera un tiempo aleatorio (igual que el caso de colisión) y comienza desde el principio

Figura 2.16 CSMA-p Persistente

- Contienda con escucha y detección de colisión (CSMA-CD): uno de los problemas de CSMA es el tiempo perdido tras la colisión (*T+2tp*), con la detección de colisión (CD), el terminal se encuentra escuchando el medio mientras transmite. Si el terminal detecta diferencia entre lo que transmite y lo que escucha, entiende que hubo colisión y deja de transmitir inmediatamente, enviando a continuación una señal especial (*jamming*) para que todos los terminales descarten el paquete recibido. En tal caso, el terminal esperará un tiempo aleatorio (en función del tipo de CSMA que emplee) antes de volver a intentarlo. En CSMA/CD no se requiere una respuesta por parte del receptor, pero si se requiere que una estación tenga capacidad de transmitir y recibir simultáneamente (full duplex). Para que una estación tenga la certeza de que su paquete no sufrió colisión, debe permanecer a la escucha del canal al menos *2tp*, por lo que una de las condiciones para emplear CSMA/CD es que *T> 2tp*. Al disminuir el tiempo perdido tras la colisión aumenta el tráfico eficaz, que puede llegar cerca al 90% en función de tipo de CSMA y del parámetro *a*.

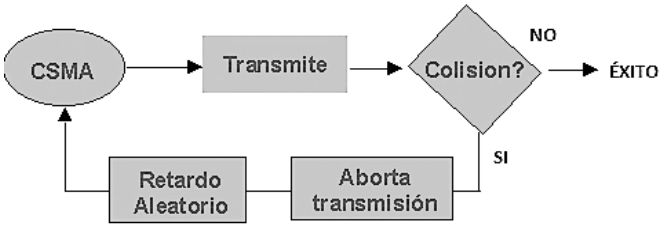

Figura 2.17 CSMA/CD

2.2.4 Capa de red

El nivel de red o capa de red, proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas. Debe asegurar que los datos lleguen desde el origen al destino, aunque no tengan conexión directa. Para la consecución de su tarea, puede asignar direcciones de red únicas, interconectar subredes distintas, encaminar paquetes, utilizar un control de congestión y control de errores. La capa de red controla funcionamiento de la subred, decidiendo qué ruta de acceso física deberían tomar los datos en función de las condiciones de la red, la prioridad de servicio y otros factores.

Funciones:

- Enrutamiento.
- Control de tráfico de subred: los enrutadores (sistemas intermedios de capa de red) pueden indicar a una estación emisora que disminuya la frecuencia de transmisión de tramas cuando el búfer del enrutador se llene.
- Fragmentación de trama: si determina que el tamaño de la unidad de transmisión máxima (MTU) que sigue en el enrutador es inferior al tamaño de la trama, un enrutador puede fragmentar una trama para la transmisión y volver a ensamblarla en la estación de destino.
- Asignación de direcciones lógico-físicas: traduce direcciones lógicas, o nombres, en direcciones físicas.
- Cuentas de uso de subred: dispone de funciones de contabilidad para realizar un seguimiento de las tramas reenviadas por sistemas intermedios de subred con el fin de producir información de facturación.

Esta capa libera a las capas superiores de conocer sobre la transmisión de datos y las tecnologías de conmutación intermedias. Establece, mantiene y finaliza las conexiones entre las instalaciones de comunicación que intervienen. En la capa de red y las capas inferiores, existen protocolos entre pares (entre un nodo y su vecino inmediato), pero es posible que el vecino sea un nodo a través del cual se enrutan datos, no la estación de destino. Las estaciones de origen y de destino pueden estar separadas por muchos sistemas intermedios.

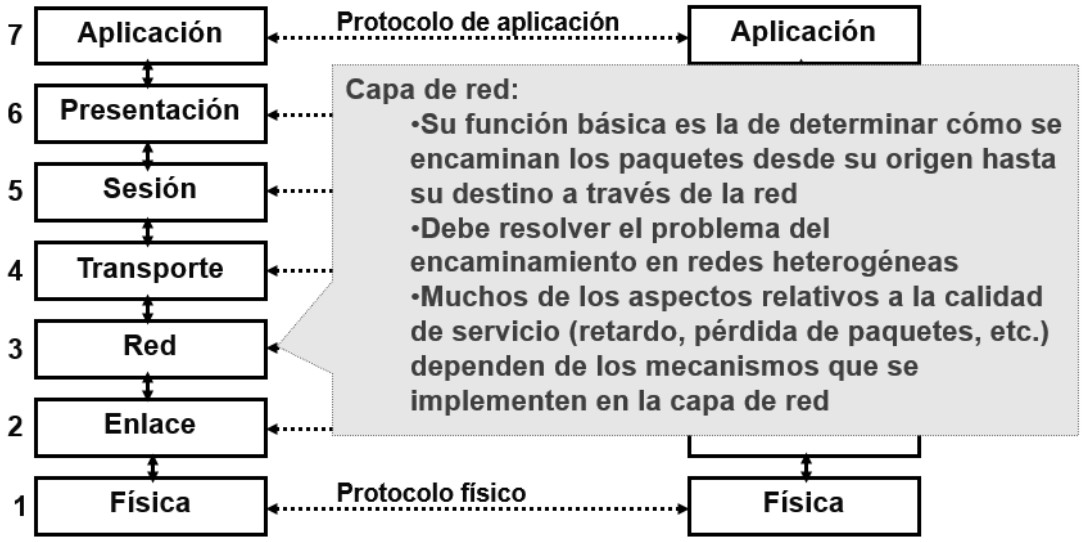

Figura 2.18 Capa de red

Hay dos formas en las que el nivel de red puede funcionar internamente, pero independientemente de que la red funcione internamente con datagramas o con circuitos virtuales puede dar hacia el nivel de transporte un servicio orientado a conexión:

- Datagramas: Cada paquete se encamina independientemente, sin que el origen y el destino tengan que pasar por un establecimiento de comunicación previo.
- Circuitos virtuales: En una red de circuitos virtuales dos equipos que quieran comunicarse tienen que empezar por establecer una conexión. Durante este establecimiento de conexión, todos los routers que haya por el camino elegido reservarán recursos para ese circuito virtual específico.

Por esta razón se dice que esta capa ofrece dos tipos de servicios:

- Servicios orientados a la conexión: Sólo el primer paquete de cada mensaje tiene que llevar la dirección destino. Con este paquete se establece la ruta que deberán seguir todos los paquetes pertenecientes a esta conexión. Cuando llega un paquete que no es el primero se identifica a que conexión pertenece y se envía por el enlace de salida adecuado, según la información que se generó con el primer paquete y que permanece almacenada en cada conmutador o nodo.

- Servicios No orientados a la conexión: Cada paquete debe llevar la dirección destino, y con cada uno, los nodos de la red deciden el camino que se debe seguir. Existen muchas técnicas para realizar esta decisión, como por ejemplo comparar el retardo que sufriría en ese momento el paquete que se pretende transmitir según el enlace que se escoja.

Las técnicas de encaminamiento suelen basarse en el estado de la red, que es dinámico, por lo que las decisiones tomadas respecto a los paquetes de la misma conexión varían a cada instante, de manera que pueden seguir distintas rutas. El problema es encontrar un camino óptimo entre un origen y un destino, en base a diferentes criterios: velocidad, retardo, seguridad, regularidad, distancia, longitud media de las colas, costos de comunicación, etc. Los equipos encargados de esta labor se denominan encaminadores (router), aunque

también realizan labores de encaminamiento los switchs multicapa o de nivel 3 (que también funcionan en el nivel de enlace).

Algunos protocolos que trabajan en la capa de red son: IP (IPv4, IPv6, IPsec), OSPF, IS-IS, ARP, RARP, RIP, ICMP, ICMPv6, IGMP, DHCP, X.25.

2.2.5 Capa de transporte

Se encarga de que los mensajes se entregan sin errores, en secuencia y sin pérdidas o duplicaciones. Libera a los protocolos de capas superiores de saber cómo es la transferencia de datos entre ellos y sus pares. El tamaño y la complejidad de un protocolo de transporte depende del tipo de servicio que pueda obtener de la capa de transporte. Si la capa de red no es confiable o solo admite datagramas, el protocolo de transporte debería incluir detección y recuperación de errores extensivos.

Funciones:

- Segmentación de mensajes: acepta un mensaje de la capa (de sesión) que tiene por encima, lo divide en unidades más pequeñas (si no es aún lo suficientemente pequeño) y transmite las unidades más pequeñas a la capa de red. La capa de transporte en la estación de destino vuelve a ensamblar el mensaje.
- Confirmación de mensaje: proporciona una entrega de mensajes confiable de extremo a extremo con confirmaciones.
- Control del tráfico de mensajes: indica a la estación de transmisión que "dé marcha atrás" cuando no haya ningún búfer de mensaje disponible.
- Multiplexación de sesión: multiplexa varias secuencias de mensajes, o sesiones, en un vínculo lógico y realiza un seguimiento de qué mensajes pertenecen a qué sesiones.

Aunque la capa de transporte puede aceptar mensajes relativamente grandes de la capa de sesión, atiende las estrictas limitaciones de tamaño de mensajes impuestas por la capa de red (inferior), por lo que debe dividir los mensajes recibidos en unidades más pequeñas (tramas) añadiendo un encabezado a cada una de ellas. Este encabezado debe incluir información de control, como marcadores de inicio y fin de mensajes, para permitir a la capa de transporte del otro extremo reconocer los límites del mensaje; si las capas inferiores no mantienen la secuencia de tramas, el encabezado de transporte debe contener información de secuencias para permitir a la capa de transporte en el extremo receptor reordenar las tramas en el orden correcto antes de enviar el mensaje recibido a la capa superior. Las Unidades de Datos de Protocolo PDU de esta capa se llaman segmentos.

A diferencia de las capas inferiores, donde los protocolos comunican nodos inmediatamente adyacentes, la capa de transporte y las capas superiores son capas "end to end" o de un extremo a otro, y no les importa los detalles de la instalación de las comunicaciones subyacente, conversan con sus similares usando encabezados en los mensajes y mensajes especiales de control.

Esta capa es el corazón en la jerarquía de protocolos, proporcionando un transporte confiable, eficiente y económico de la máquina de origen a la máquina de destino, independientemente de la red o redes físicas en uso. Para lograr este objetivo, la Capa de Transporte, hace uso de los servicios proporcionados por la capa de red. El hardware o software que se encarga del trabajo se llama entidad de transporte que puede estar:

- En la Tarjeta de interfaz de red
- En el núcleo del sistema operativo
- En un proceso de usuario independiente
- En un paquete de biblioteca que forma parte de las aplicaciones de la red

Hay dos tipos de servicio de transporte: orientado a conexiones y sin conexiones, (al igual que en el servicio de red), en ambos casos las conexiones tienen tres fases:

- Establecimiento
- Transferencia de Datos
- Liberación

Esta capa encima de la de red, ofrece la redundancia necesaria para solucionar los problemas en las conexiones "desde fuera" de la subred. Por ello una capa es necesaria encima de la de red para mejorar la calidad del servicio. Si a la mitad de una transmisión larga, se informa a la entidad de transporte que su conexión de red ha terminado, sin indicación de lo sucedido, la entidad de transporte, puede comunicarse con la entidad de transporte remota, y por medio de esta nueva conexión pedir que se le informe sobre qué datos llegaron y cuales no para reiniciar desde la interrupción.

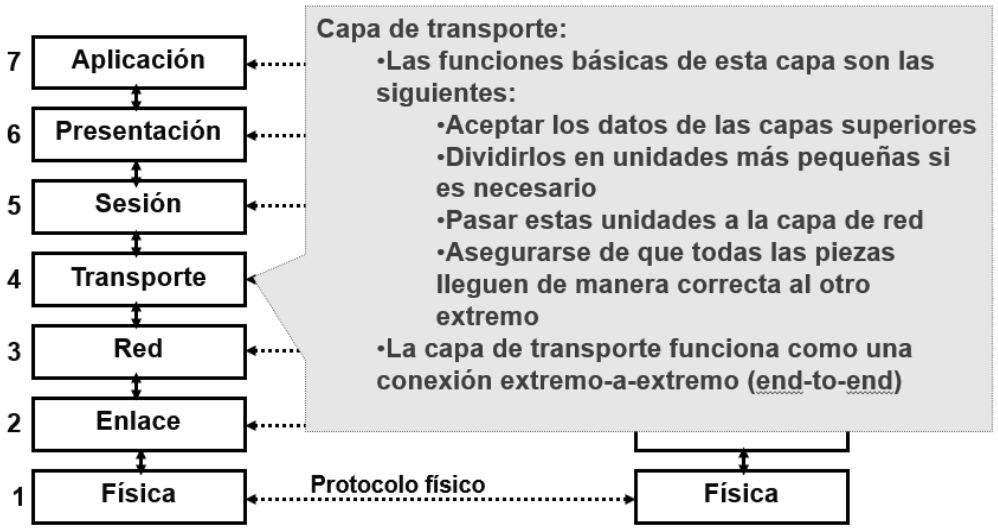

Figura 2.19 Capa de transporte

Los protocolos más importantes de la capa de transporte son TCP y UDP

2.2.6 Capa de sesión

Permite establecer sesiones entre procesos que se ejecutan en diferentes estaciones.

Funciones:

- Establecer un camino de comunicación lógico (conexión de sesión) con otra entidad de aplicación, utilizarlo para intercambiar datos (unidades de diálogo) y liberar la conexión de una forma ordenada.
- Soporte de sesión: realiza las funciones que permiten a estos procesos comunicarse a través de una red, ejecutando la seguridad, el reconocimiento de nombres, el registro, etc.
- Establecer puntos de sincronización durante un diálogo y, en caso de ocurrir errores, reanudar el diálogo a partir de un punto de sincronización convenido
- Interrumpir (suspender) un diálogo y reanudarlo después en un punto convenido de antemano.
- Mantener informada de ciertas excepciones que pueden surgir de la red subyacente durante una sesión.

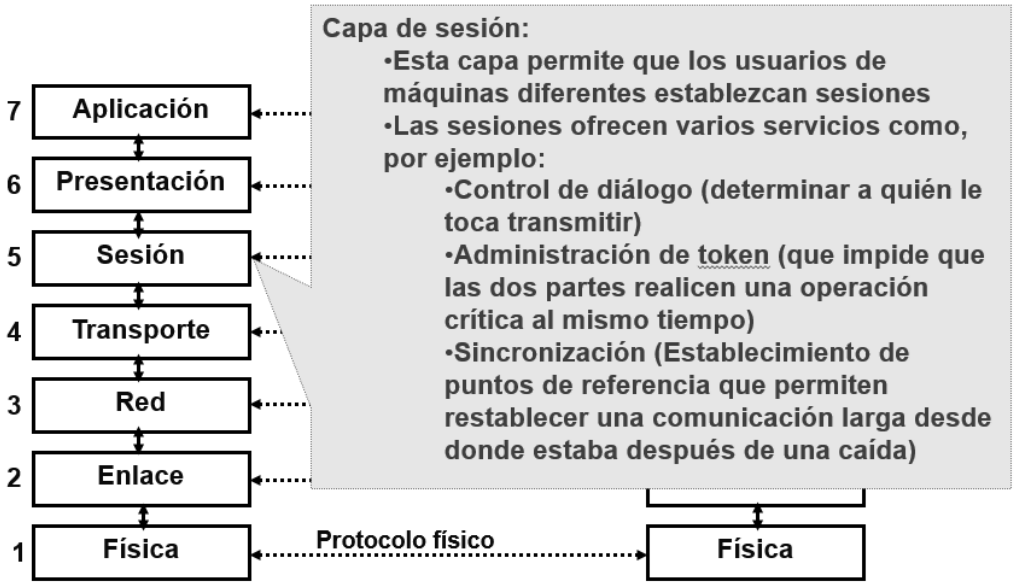

Figura 2.20 Capa de sesión

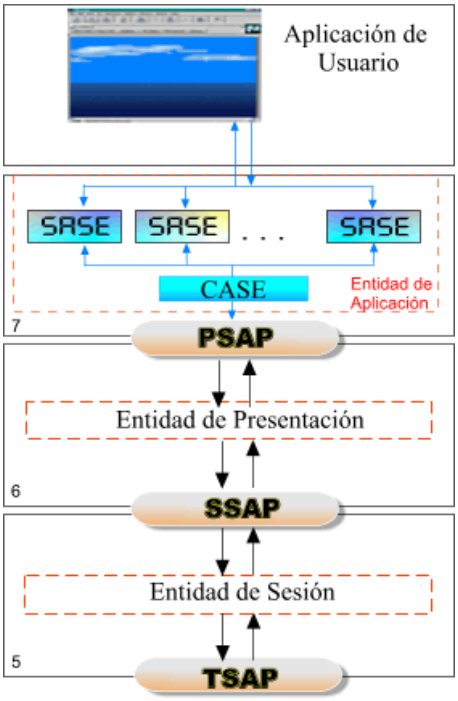

Figura 2.21 Provisión de servicios a las capas superiores

Esta capa maneja 3 protocolos:

- SQL: SQL Server Azure Services es esencialmente una instancia de SQL Server que se expone en la internet, funcionando desde los servidores de Microsoft. Al momento de escribir estas líneas, el servicio se expone de forma estándar, utilizando TDS (Tabular Data Stream),
- RPC: es un protocolo que permite a un programa de ordenador ejecutar código en otra máquina remota sin tener que preocuparse por las comunicaciones entre ambos. El protocolo es un gran avance sobre los sockets usados hasta el momento.
- NETBIOS: es, en sentido estricto, una especificación de interfaz para acceso a servicios de red, es decir, una capa de software desarrollado para enlazar un sistema operativo de red con hardware específico.

2.2.7 Capa de presentación

La capa de presentación da formato a los datos que deberán presentarse en la capa de aplicación. Se puede decir que es el traductor de la red. Esta capa puede traducir datos de un formato utilizado por la capa de la aplicación a un formato común en la estación emisora y a continuación, traducir el formato común a un formato conocido por la capa de la aplicación en la estación receptora.

Funciones:

- Conversión de código de caracteres: por ejemplo, de ASCII a EBCDIC.
- Conversión de datos: orden de bits, CR-CR/LF, punto flotante entre enteros, etc.
- Compresión de datos: reduce el número de bits que es necesario transmitir en la red.
- Cifrado de datos: cifra los datos por motivos de seguridad. Por ejemplo, cifrado de contraseñas.
- Aplicar a los datos procesos criptográficos.
- Definir la estructura de datos a transmitir.

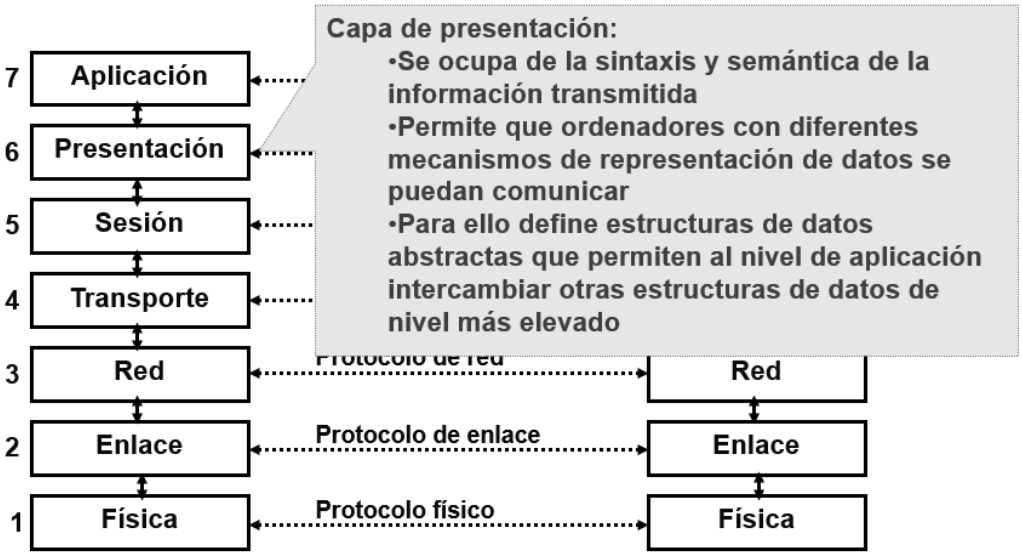

Figura 2.22 Capa de presentación

Algunos protocolos de la capa de presentación son:

- ASN.1: forma normalizada de representar datos.
- MIME: se usa para transportar los archivos adjuntos en protocolos como HTTP o SMTP.

Los estándares de esta capa para imágenes son:

- GIF: Un formato de imagen utilizado en los primeros tiempos de las comunicaciones, en las famosas BBS o boletines electrónicos
- TIFF (Formato de archivo de imagen etiquetado): Un formato para imágenes con asignación de bits de alta resolución
- JPEG (Grupo conjunto de expertos fotográficos): Formato gráfico utilizado para fotografía e imágenes complejas con buena calidad/compresión

Los estándares de esta capa para sonido y películas son:

- MIDI: (Interfaz digital para instrumentos musicales) para música digitalizada
- MPEG (Grupo de expertos en películas): Estándar para la compresión y codificación de vídeo
- QuickTime: Estándar para el manejo de audio y vídeo para los sistemas operativos de los MAC

2.2.8 Capa de Aplicación

El nivel de aplicación actúa como interfaz entre los usuarios y las aplicaciones para tener acceso a servicios de red. Los protocolos de capa de aplicación se utilizan para intercambiar los datos entre los programas que se ejecutan en los hosts de origen y destino. Existen muchos protocolos de capa de aplicación y siempre se desarrollan protocolos nuevos.

Funciones:

- Uso compartido de recursos y redirección de dispositivos
- Acceso a archivos remotos
- Acceso a la impresora remota
- Comunicación entre procesos
- Administración de la red
- Servicios de directorio
- Mensajería electrónica (como correo)
- Terminales virtuales de red

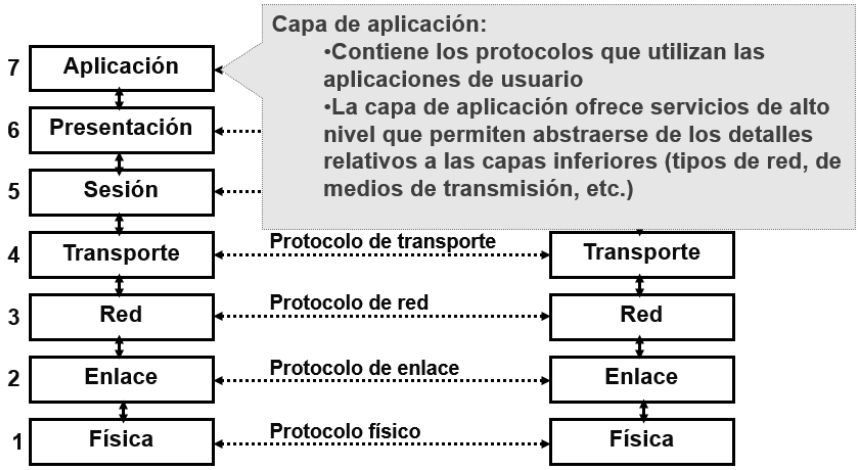

Figura 2.23 Capa de aplicación

Dentro de los protocolos más usados en la capa de aplicación tenemos:

- Protocolo de servicio de nombres de dominios (DNS): se utiliza para resolver nombres de Internet en direcciones IP.
- Telnet: protocolo de emulación de terminal que se utiliza para proporcionar acceso remoto a servidores y dispositivos de red.
- Protocolo bootstrap (BOOTP): un precursor al protocolo DHCP.
- Protocolo de red que se utiliza para obtener información de dirección IP durante el arranque.
- Protocolo de configuración dinámica de host (DHCP): se utiliza para asignar una dirección IP, una máscara de subred, un gateway predeterminado y un servidor DNS a un host.
- Protocolo de transferencia de hipertexto (HTTP): se utiliza para transferir archivos que conforman las páginas Web de la World Wide Web.
- Protocolo de transferencia de archivos (FTP): se utiliza para la transferencia interactiva de archivos entre sistemas.
- Protocolo trivial de transferencia de archivos (TFTP): se utiliza para la transferencia activa de archivos sin conexión.
- Protocolo simple de transferencia de correo (SMTP): se utiliza para la transferencia de mensajes y archivos adjuntos de correo electrónico.
- Protocolo de oficina de correos (POP): lo utilizan los clientes de correo electrónico para recuperar el correo electrónico de un servidor remoto.
- Protocolo de acceso a mensajes de Internet (IMAP): otro protocolo para la recuperación de correo electrónico.

2.3 FUNCIONAMIENTO DEL MODELO

Llamamos entidades a los elementos activos (hardware o software) que se hallan en cada una de las capas. Si las entidades residen en la misma capa de dos computadores, se les llama entidades pares. Si un computador (host A) debe enviar datos a otro computador (host B), los datos deben empaquetarse y ser preparados antes de transmitirse, por lo que se realiza un proceso denominado **encapsulamiento**, los datos se desplazan a través de las capas del modelo OSI, recibiendo encabezados, información de inicio y fin e información de control, en este proceso cada capa tiene una unidad de datos entrante y genera una unidad de datos saliente

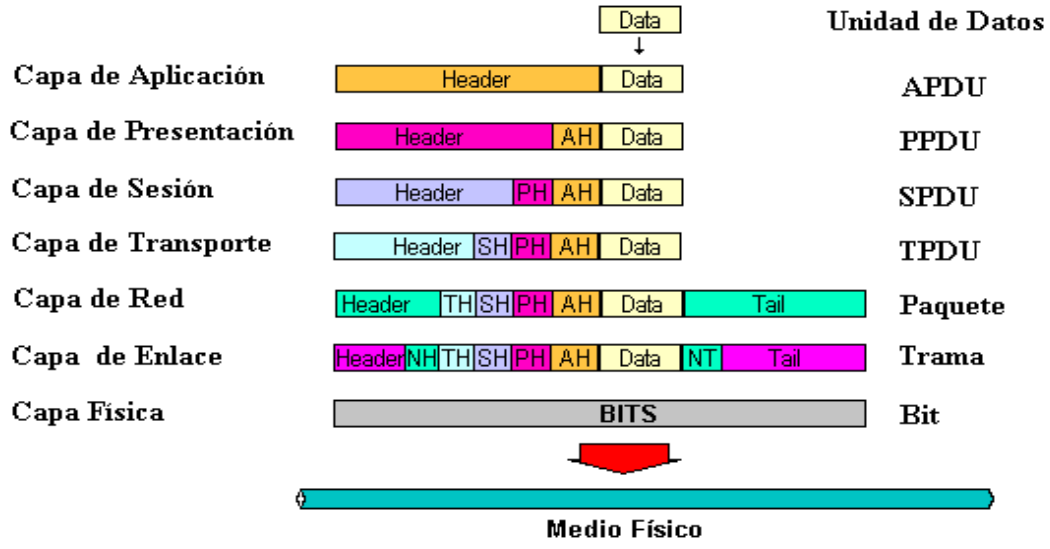

Figura 2.22 Trayectoria de los datos al atravesar las capas en el host emisor

En este proceso llamamos:

- N-PDU (*Unidad de datos de protocolo*): es la información intercambiada entre las capas N pares (entidades pares) de dos hosts comunicados. Está compuesta por:
    - N-SDU (*Unidad de datos del servicio*) son los datos intercambiados por las unidades pares a través de la red.
    - N-PCI (*Información de control del protocolo*) Información intercambiada entre entidades pares conectadas para coordinar su operación conjunta.
- N-IDU (Unidad de datos de la interface): es el bloque de información transferido entre dos capas adyacentes del mismo host, a través de la interface entre ellas. Está compuesta por:
    - N-ICI (Información de control de la interface): es la información intercambiada entre una entidad y otra para coordinar la operación, controla la interface
    - Datos de Interface-(N) Información transferida entre entidades pares a través de la red, coincide con la (N+1) PDU

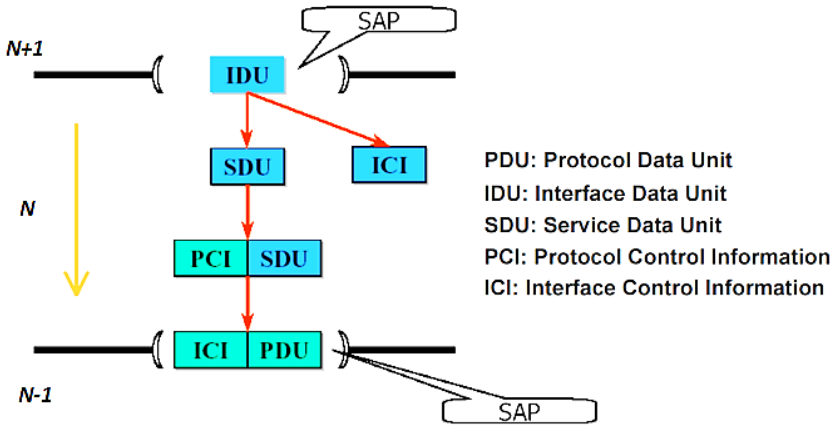

Figura 2.23 Trayectoria de los datos al atravesar las capas adyacentes en el host emisor

En el proceso de atravesar todas las capas se van formando las PDU (Protocol Data Unit) o unidad de datos de protocolos, este proceso recibe el nombre de *encapsulamiento* en el host emisor, mientras que en el host receptor al subir por la pila de capas se revierte el proceso, implementado el *desencapsulamiento.*

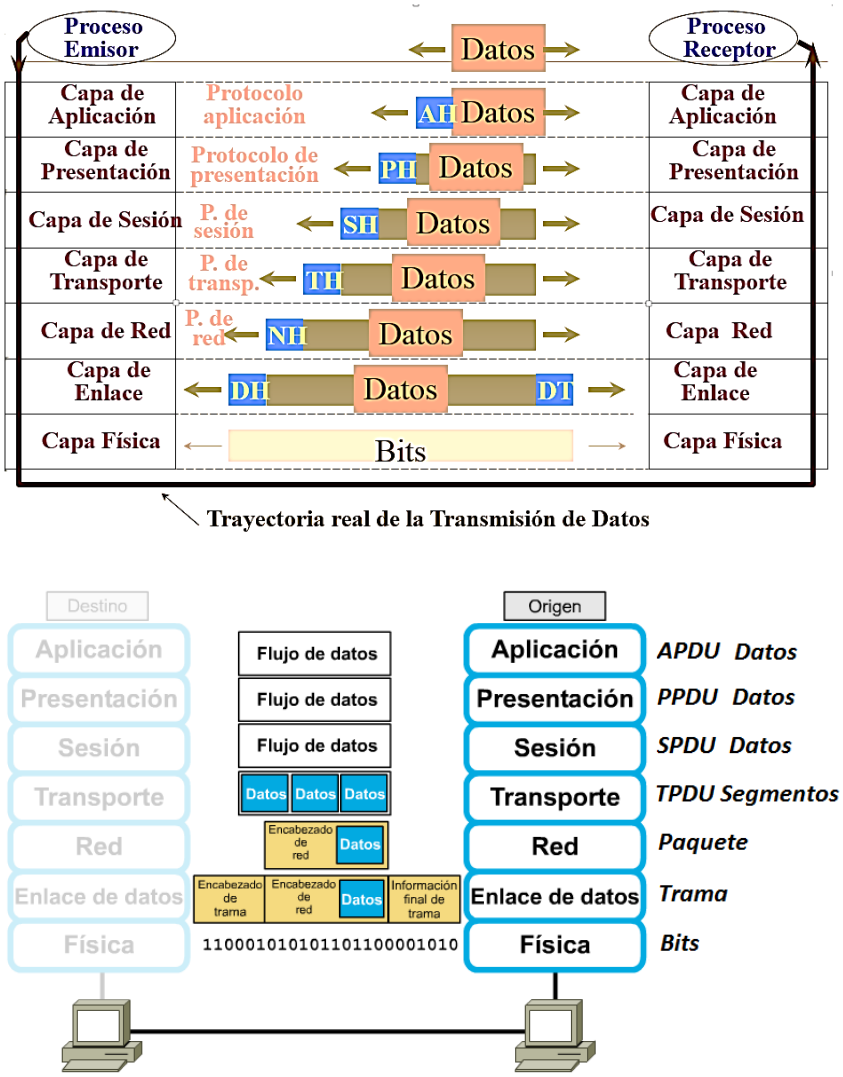

Figura 2.24 Encapsulamiento en el Modelo OSI

2.3.1 Servicios

Si hablamos de los servicios ofertados en el modelo OSI, las entidades en un nivel *N* ofrecen servicios que son utilizados por las entidades del nivel *N+1*. El nivel *N* es el proveedor del servicio y el nivel *N+1* el usuario del servicio. Los servicios están disponibles en los *SAPs* (Puntos de Acceso al Servicio). Los SAPs del nivel *N* son los puntos donde el nivel *N+1* puede acceder a los servicios ofrecidos por este. Un servicio es requerido por el usuario o es ofertado por el proveedor del servicio mediante el intercambio de un conjunto de primitivas de servicio a través de la interfaz entre los niveles *N* y *N+1*, estas primitivas son cuatro: *Request, Indication, Response, Confirm*.

En general, los servicios pueden ser confirmados o no, se denomina servicio confirmado a aquel que utiliza las cuatro primitivas (se produce un diálogo de control), mientras que un servicio sin confirmar solo hace uso de las primitivas *Request* e *Indication*. El establecimiento de una conexión siempre es un servicio confirmado, mientras que la transferencia de datos puede ser sin confirmar o no.

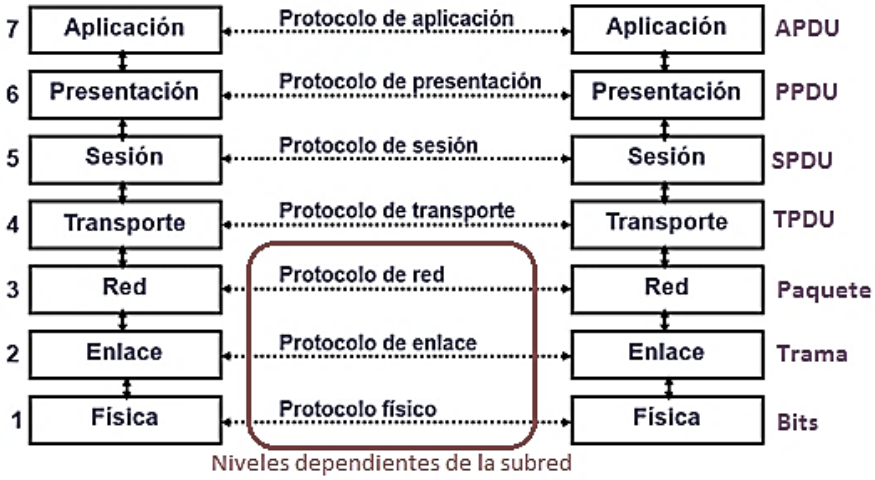

Figura 2.25 Funcionamiento del Modelo

Los tipos de servicios comerciales (en la red) que encontramos son:

- **Servicios orientados a la conexión**: requieren el establecimiento inicial de una conexión y la ruptura o liberación al final de la misma. En esta conexión se produce el intercambio de datos del usuario. Los bloques de datos se reciben en el mismo orden en que fueron emitidos y todos los paquetes siguen la ruta conseguida en la conexión, por ejemplo, el servicio telefónico.

    - Secuencia de mensajes: aquí se establecen fronteras que delimitan cada mensaje, hay un flujo de mensaje confiable (secuencia de páginas).
    - Secuencias de bytes: no hay fronteras entre los mensajes, por lo que existe un flujo de bytes confiable cuya interpretación es responsabilidad del receptor (ingreso remoto).
    - Conexión no confiable (voz digitalizada)

- **Servicios sin conexión**: comunicación sin realizar una conexión con el destinatario. Se envían paquetes de datos con la dirección de destino, es la red la encargada de conducir los datos por una ruta apropiada. En algunos casos, el receptor debe enviar acuse de recibo al emisor, por ejemplo, el sistema postal.

    - Servicio de datagrama sin confirmación, no necesita confirmación del receptor, el datagrama no es confiable, por ejemplo, el protocolo IP, correo electrónico spam.
    - Servicio de datagrama con confirmación, requiere confirmación del emisor, es un datagrama con acuse de recibo (correo electrónico con acuse de recibo, correo registrado).
    - Servicio de petición y respuesta: a cada petición le sigue un mensaje de respuesta que contiene los datos solicitados (consulta de base de datos).

2.3.2 Primitivas utilizadas por OSI

Una primitiva especifica la función que se va a llevar a cabo y los parámetros que se utilizan para pasar datos e información de control entre capas adyacentes. Las primitivas usadas por OSI son cuatro

- *Request*: emitida por la entidad usuario del servicio con el objeto de solicitar un servicio y pasar los parámetros necesarios para realizar el servicio solicitado.
- *Indication*: una entidad es informada que ha ocurrido un evento, es iniciada por el proveedor.
- *Response*: emitida por el usuario del servicio para reconocer o completar algún procedimiento previamente invocado por un *Indication* a dicho usuario.
- *Confirm*: una entidad es informada acerca de una solicitud efectuada anteriormente, también se utiliza para reconocer o completar algún procedimiento solicitado previamente por un usuario del servicio mediante un *Request*.

El **proceso** que se desencadena para realizar una transferencia de información entre dos entidades pares de nivel *N* es:

1) La entidad origen (*N*) invoca a su entidad (*N - 1*) con una primitiva de solicitud *Request*. Asociado a esta primitiva están los parámetros necesarios, como, por ejemplo, los datos que se van a transmitir y la dirección destino
2) La entidad origen (*N - 1*) prepara una PDU (*N - 1*) para enviársela a su entidad par (N - 1).
3) La entidad destino (*N - 1*) entrega los datos al destino apropiado (*N*) a través de la primitiva de indicación *Indication*, que incluye como parámetros los datos y la dirección origen
4) Si se requiere una confirmación, la entidad destino (*N*) emite una primitiva de respuesta *Response* a su entidad (*N-1*).
5) La entidad (*N - 1*) convierte la confirmación en una PDU (*N- 1*).
6) La confirmación se entrega a la entidad origen (*N*) como una primitiva *Confirm*

2.3.3 Categorías de Servicios

1) Confirmados

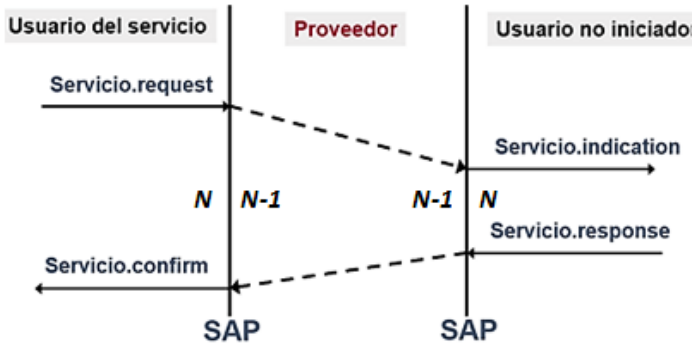

Figura 2.26 Servicio confirmado

2) No confirmado

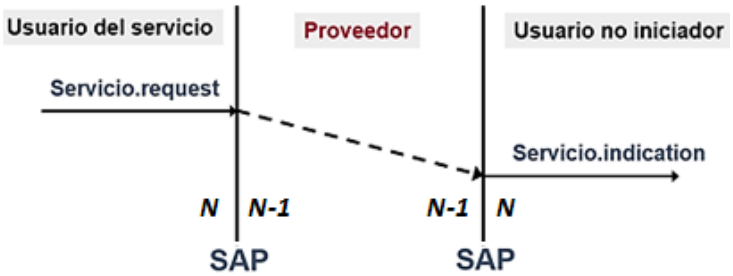

Figura 2.27 Servicio no confirmado

3) Servicio confirmado por el proveedor

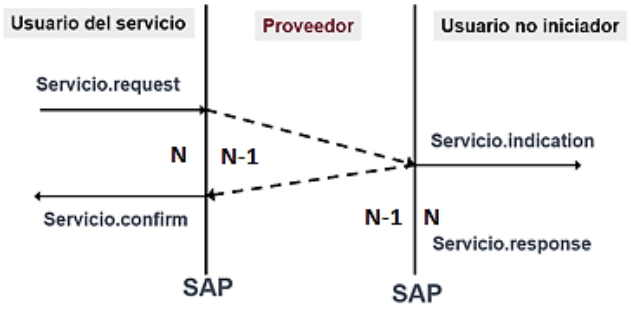

Figura 2.28 Servicio confirmado por el proveedor

2.4 OTROS MODELOS

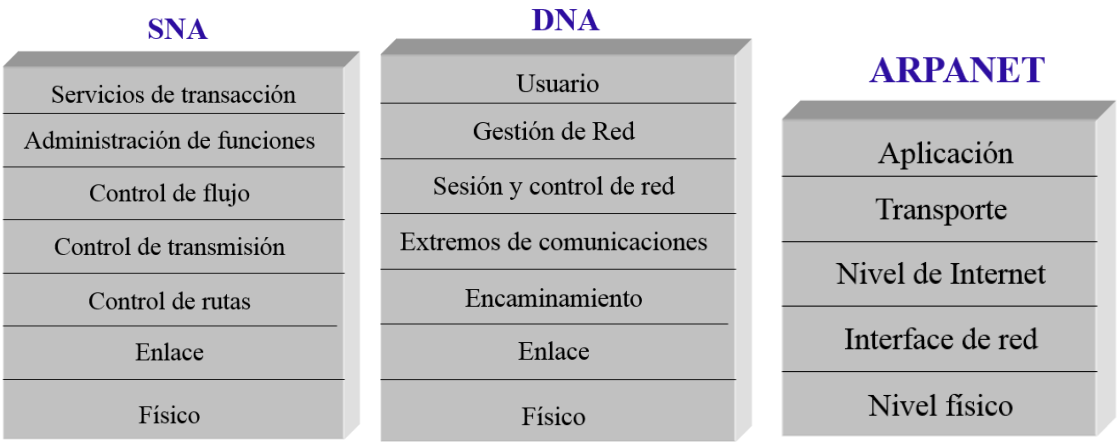

Figura 2.29 Otras arquitecturas y modelos

2.5 ESTÁNDARES

En febrero de 1980 se formó en el IEEE un comité de redes locales (802) específicamente para normar el hardware de redes. El proyecto 802 define aspectos relacionados al cableado físico y transmisión de data. El Estándar IEEE 802 inició el proyecto basado en conseguir un modelo para permitir la intercomunicación de ordenadores para la mayoría de los fabricantes. Para ello se enunciaron una serie de normalizaciones que con el tiempo han sido adaptadas como normas internacionales por la ISO. El protocolo 802 está dividido según las funciones necesarias para el funcionamiento de las LAN. Cada división se identifica por un número: 802.x. Los productos fabricados en base a las normas 802 incluyen tarjetas de la interfaz de red, bridges, routers y otros componentes utilizados para crear LANs de par trenzado y cable coaxial y otros tipos de redes.

Cuando comenzaron a aparecer las primeras redes de área local (LAN, Local Área Networks) como herramientas potenciales de empresa a finales de los setenta, el IEEE observó que era necesario definir ciertos estándares para redes de área local. Para conseguir esta tarea, el IEEE emprendió lo que se conoce como proyecto 802, debido al año y al mes de comienzo (febrero de 1980) y definió estándares de redes para las componentes físicas de una red:

- Tarjetas de red (NIC).
- Componentes de redes de área global (WAN, Wide Área Networks).
- Componentes utilizadas para crear redes de cable coaxial y de par trenzado.

Las especificaciones 802 definen la forma en que las tarjetas de red acceden y transfieren datos sobre el medio físico. Éstas incluyen conexión, mantenimiento y desconexión de dispositivos de red. La selección del