

El Modelo de Referencia OSI.

Cuántas veces nos hemos hecho la pregunta *¿QUÉ ES UNA RED?*, y no siempre tuvimos una respuesta del todo acertada. No se preocupe, existen muchas respuestas a esta pregunta. Por ello nosotros tomaremos la siguiente definición:

Se llama red a todo sistema de comunicación que soporta múltiples usuarios.

Como vemos es una definición muy amplia y tomará un significado diferente dependiendo del ambiente en el que se la ubique.

Una red en general consiste de dos componentes:

- La línea de transmisión (circuitos, canales, etc).
- Los elementos de conmutación, que son ordenadores especializados para conectar dos o más líneas de transmisión (Hub, Switch, Router, etc.).

En términos generales tenemos dos tipos de canales:

- Punto a punto. En este caso el mensaje va de un extremo a otro íntegramente. Estas redes son conocidas como Punto a Punto, Almacenamiento y reenvío, conmutación de paquetes, etc.
- De difusión. Estas redes tienen un solo canal compartido por todos los Host. Los mensajes de una máquina se envían al canal y son recibidos por todas las demás. Aquella a la cual va dirigida es la que lo leerá. Las redes locales en general son las que usan los canales de difusión.

Una red debe brindar servicios a varios usuarios, pero no necesariamente al mismo tiempo. Por ejemplo, considerando la red telefónica, cuyos usuarios son todos aquellos que tengan un teléfono, no es utilizada por todos al mismo tiempo.

Tenemos que entender que al definir una red estamos definiendo algo más que una terminal conectada a distancia con un sistema de computación central; por lo tanto, habrá más cuestiones a resolver.

Estas cuestiones pueden ser tales como:

- ¿Se permitirá que un usuario se comunique con varios al mismo tiempo?.
- ¿Qué sucederá si varios usuarios tratan de usar la red al mismo tiempo?.
- ¿Cómo manejará la red la detección de ruidos y errores de transmisión?.
- ¿Cómo se manejará las fallas de vínculos de interconexión?. ¿Solo se dejará fuera de servicio una parte, o toda la red se verá afectada?.
- ¿Cómo se asegurara que los mensajes lleguen a destino sin demora excesiva debido a la operación de la red?.

Afortunadamente existen diferentes elementos de software y hardware para administrar las redes, quedando a nuestro criterio seleccionar la solución que mejor se adapte a nuestras necesidades.

Sin embargo para contestar las preguntas formuladas más arriba, es imprescindible analizar en forma técnica algunos aspectos de la red, como ser:

- **TOPOLOGIA:** determina la interconexión entre los usuarios.
- **PROTOCOLO:** sincrónico o asincrónico, formato de los mensajes, etc.
- **INTERFACES ELECTRICAS:** RS-232, RS-422, V.35, V.24/V.28, etc.
- **VINCULOS SELECCIONADOS:** Este elemento condiciona la velocidad, distancia, confiabilidad, seguridad, facilidad de incorporar nuevos usuarios. Entre otros podemos mencionar: par telefónico, cable coaxil, radioenlaces (VHF, UHF, Microondas), enlaces satelitales, fibras ópticas, etc.
- **PROCEDIMIENTOS DE RECUPERACION:** Procedimientos para el manejo de problemas tales como errores, ruido, etc.

Dado una red debe poder integrar equipos de múltiples proveedores, y con el fin de evitar situaciones confusas, la **International Standard Organization (ISO)** definió un modelo de red por niveles o capas

Este se conoce como el modelo de referencia **OSI (Open System Interconnection)**, o Interconexión de Sistemas Abiertos (ISA).

En una red existe una colección de máquinas destinadas a ejecutar programas de usuario (HOST).

El trabajo de la red consiste en enviar mensajes (comunicación ó diálogo) entre HOST.

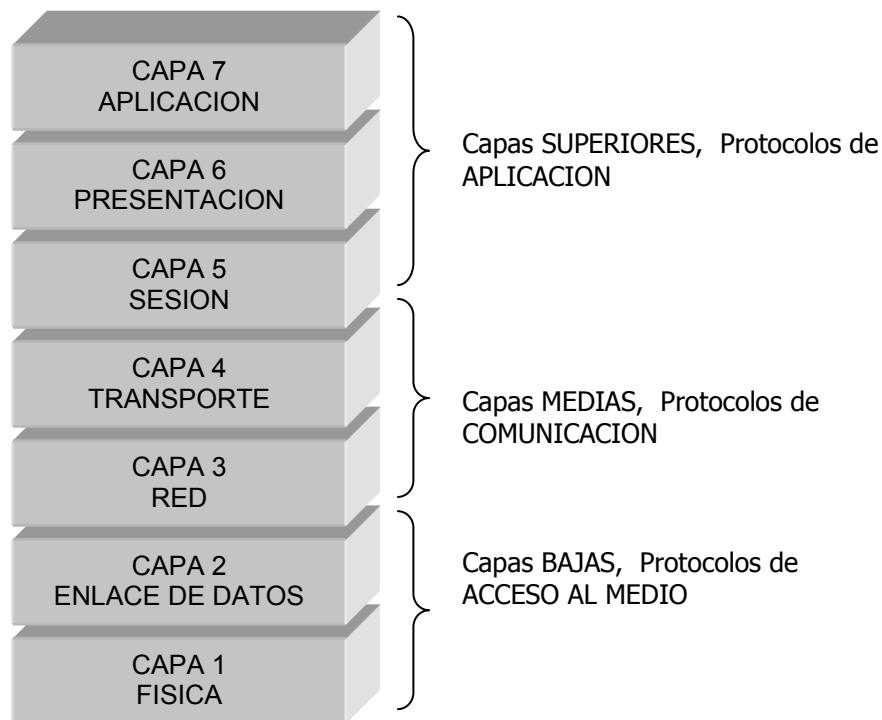


Figura 7

El diseño se simplifica si separamos los aspectos de comunicación de los de aplicación. Una red en general consiste de dos componentes:

- La línea de transmisión (circuitos, canales, etc).
- Los elementos de conmutación, (Hub, Switch, Router, etc).

Es importante destacar que OSI es un Modelo de Referencia, y tiene un alto valor académico, sin embargo no existe como una arquitectura de red.

Usando un lenguaje más llano, el Modelo de Referencia define qué es lo que debe hacer cada capa, pero no siempre especifica los protocolos y servicios exactos que deben llevar a cabo dichas tareas, es decir cómo deben hacerse. La ISO ha elaborado estándares para algunos protocolos, pero los mismos no han tenido gran trascendencia en el mercado.

En el otro extremo se encuentra el Modelo TCP/IP, que a diferencia de OSI es más bien “*escaso*” en cuanto a las definiciones de las capas, pero cuenta con una gran cantidad de protocolos muy desarrollados, plenamente operacionales y de gran uso en la industria actual, a tal punto que es el modelo que se utiliza en Internet.

Resumiendo, podemos decir que la tendencia actual es la de utilizar el Modelo de Referencia OSI como estructura conceptual y usarlo como una “*regla*” para comparar otros modelos o simples pilas de protocolos.

A diferencia del sencillo modelo presentado anteriormente a modo de ejemplo, OSI cuenta con 7 capas:

Para facilitar el análisis es preferente considerar a las 7 capas de OSI agrupadas en “*Capas Superiores*”, “*Capas Medias*” y “*Capas Inferiores*” como se muestra en la figura 7.

Antes de comentar las funciones encomendadas a cada capa por la gente de la ISO, comparemos el Modelo de referencia OSI con el modelo TCP/IP.

El Modelo TCP/IP consta de menos capas que el OSI, sólo tiene 4. Esto no significa que TCP/IP tenga que realizar menos funciones sino que varias de estas funciones no se encuentran discriminadas en capas distintas. La equivalencia entre ambos modelos se muestra en la siguiente figura 8:

Como se puede observar las diferencias fundamentales se producen en las capas superiores, y de acceso a la red o capa de acceso al medio ya que en el modelo TCP/IP las 3 capas superiores de OSI se encuentran englobadas en una única capa, y sobre las 2 capas inferiores, TCP/IP, no revela detalles, dejando a los protocolos ya estandarizados la función de presentar el acceso al medio. Como mencionaba anteriormente esto no significa que en TCP/IP no sean necesarias las funciones que OSI ha asignado a las capas de Presentación y Sesión, sino que en el caso de TCP/IP éstas deben formar parte de los protocolos implementados en la capa de aplicación, es decir deben “formar parte del mismo paquete”.

La otra diferencia fundamental se da en las capas inferiores, ya que TCP/IP no establece características para las capas que se encuentren debajo de la capa de Internet (Red), los diseñadores de TCP/IP confiaron plenamente en las soluciones que la industria había establecido, siempre que sean capaces de comunicarse con la capa Internet, y dado que éstas se apoyan fundamentalmente en OSI, es natural considerar que TCP/IP tiene las mismas capas bajas.

Comparación de los modelos OSI y TCP/IP

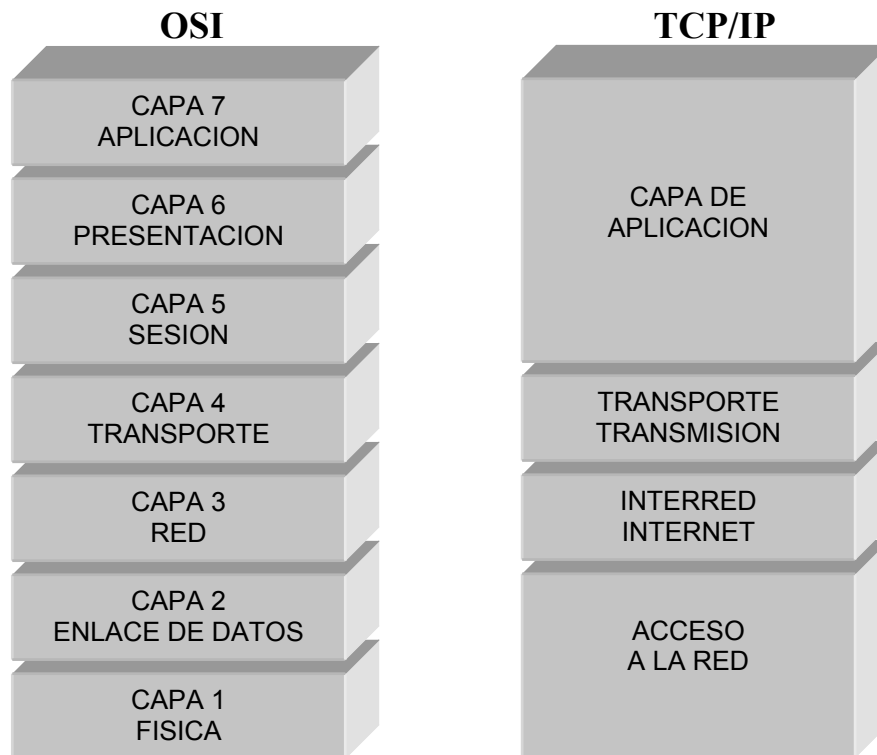


Figura 8

Sin entrar en detalles simplemente comentaremos (por ahora) que las capas bajas de ambos modelos se encargan de las topologías de red, las placas de red, los cableados y la forma eléctrica en que se transmitirán los bits a través del medio.

Las capas medias establecen los Protocolos de Comunicación (por ejemplo TCP, IP, UDP, ARP, RARP, ICMP, RIP, IGRP, BGPI y otros, en el caso del modelo TCP/IP), que permitirán que la información llegue a la computadora destino, sin importar dónde se encuentre físicamente. Son los protocolos que permiten que Ud., por ejemplo, pueda comunicarse desde su casa con una computadora en otro país utilizando Internet.

En las capas altas encontramos los protocolos de aplicación, que en caso de TCP/IP suelen ser: HTTP, FTP, SMTP, Telnet y otros. Los nombres pueden parecer extraños, pero seguramente ya se ha acostumbrado a alguno de ellos: cuando navega por Internet (o por la intranet de su empresa) con el Internet Explorer o el Netscape Navigator está utilizando el protocolo HTTP (Hyper Text Transfer Protocol o Protocolo de transferencia de Hipertexto) que es el que permite que vea las páginas Web. El protocolo HTTP especifica cómo debe hacer su navegador para mostrar en pantalla los Bytes enviados desde el sitio web.

¿Ha usado el correo electrónico (e-mail)? ¿Si?. Entonces, ha estado utilizando el protocolo SMTP (Single Mail Transfer Protocol, o Protocolo Simple de Transferencia de Correo); este protocolo es el que le permite a su programa cliente de correo electrónico (como puede ser el Outlook Express, el de Netscape, el Eudora mail, el Pegasus o Lotus Notes, entre otros) mostrarle los mails que recibió, qué poner en cada uno de los campos que utiliza habitualmente como la dirección de correo electrónico de destino, el subject (o asunto), el campo CC etc.

A continuación investigaremos con algo más de detalle las distintas capas del modelo OSI, empezando por las capas bajas. En este capítulo investigaremos las capas bajas, en las situaciones profesionales posteriores nos abocaremos al estudio de las restantes.

Problemas de Diseño para las Capas

Vamos a mencionar algunos de los más importantes definidos en el Modelo OSI:

- Cada capa deber tener un mecanismo para el establecimiento de la conexión. Se necesita un medio que permita especificar con quien establecer la conexión. Al tener destinatarios múltiples, se necesita alguna forma de direccionamiento.
- Un mecanismo para terminar una conexión dentro de la red, una vez que esta no se necesita. Este punto que parece trivial suele ser bastante más complejo.
- Regla para la transferencia de datos:
 1. Comunicación unilateral o simplex.
 2. Comunicación bilateral o semidúplex.
 3. Comunicación bilateral simultánea o dúplex.
- Número de canales lógicos que corresponden a la conexión.
- Procedimientos para la corrección de errores.
- El receptor debe tener alguna forma de indicar que mensajes ha recibido, y cuales de ellos son correctos.
- Incapacidad de aceptar mensajes extensos. Esto nos conduce a la segmentación, transmisión y ensamblaje.

Las Capas de Acceso al Medio: Física y Enlace de Datos

La Capa Física

“La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico en la red.”

El párrafo anterior parece un tanto difícil de entender. Sin embargo lo escribimos de esa forma porque ésa suele ser la terminología técnica que se usa habitualmente.

Pero no debe preocuparse, porque ya sabe de qué se trata, lo que queremos decir es que:

La capa física define las características que debe tener el medio de transmisión (por ejemplo el cable), cuánto debe medir, con qué velocidad se puede transmitir por él, cada cuántos metros se deben regenerar la señal con un repetidor, cómo se representarán los 0 y 1 lógicos con niveles de tensión eléctrica o voltaje (¿recuerda la codificación Manchester?).

Esperamos que sí porque son detalles que ya hemos visto cuando analizamos los tipos de cableados definidos en la norma IEEE 802.3 y en la norma Ethernet.

La capa física también define *cómo deben ser los conectores que vinculan el cable a la placa de red y los conectores que se utilizan para unir distintos segmentos de cable.*

Podemos decir que el objetivo fundamental de la capa física es conseguir que cuando la computadora emisora envíe un 1 lógico, la computadora receptora reciba un 1 lógico.

¡Así que cuando le pedimos que defina un tipo de cable para una red LAN hipotética, lo que estamos haciendo es que elija las características de la capa física de su red LAN!

Además del cableado de red, también se encuentra involucrada en los servicios de la capa física y de enlace, **la placa de red o NIC (Network Interface Card)**, ya que ella es la que genera los 1 y 0 lógicos como señales eléctricas, las cuales luego vuelca en el medio de transmisión.

Como puede observar las normas Ethernet, IEEE 802.3, IEEE 802.4, IEEE 802.5 brindan los servicios exigidos por los modelos OSI y TCP/IP para la capa física de redes LAN.

La siguiente figura le muestra la relación que existe entre la capa física del modelo OSI (y también del TCP/IP) y algunas normas que lo implementan para redes LAN.

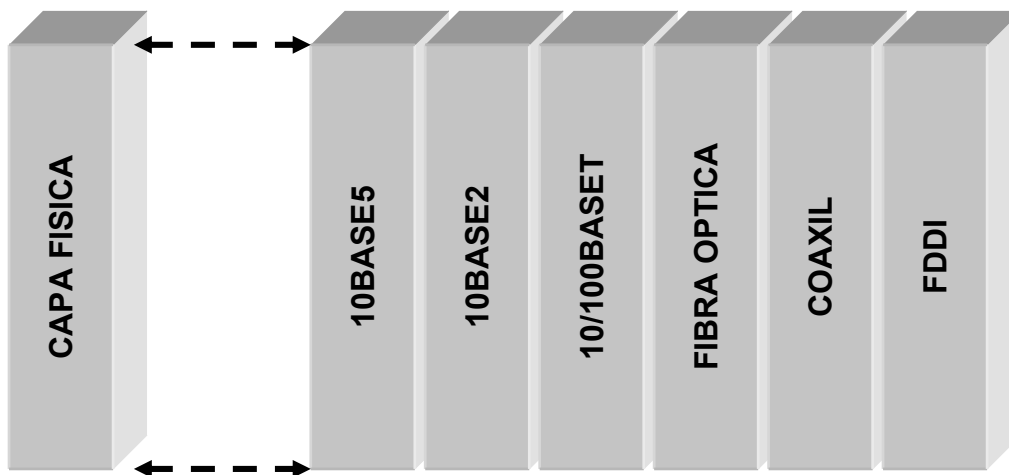


Figura 9

Hacemos especial hincapié en que las mostradas en la figura son las especificaciones para implementar redes LAN (de área local), ya que las mismas no son utilizables para redes WAN.

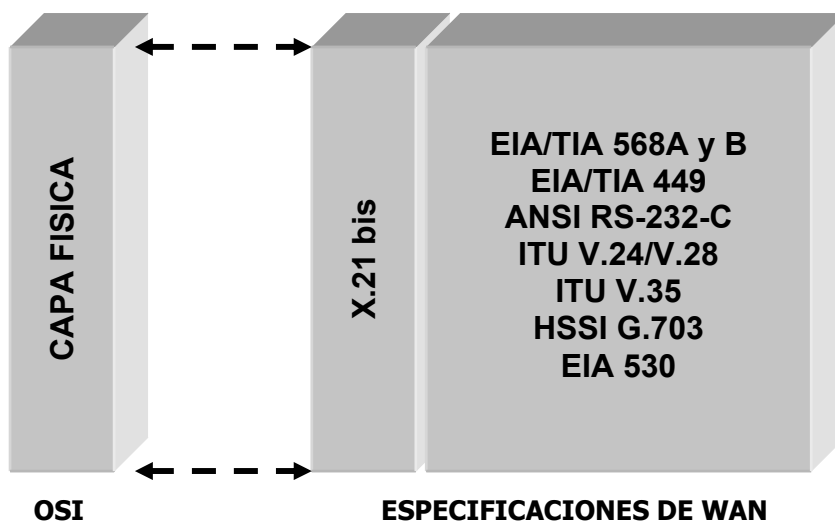


Figura 10

La figura anterior muestra algunas especificaciones normalizadas para la capa física en redes WAN.

En términos generales tenemos dos tipos de canales:

- **Punto a punto**
- **De difusión.**

En el primero cada cable conecta un Host o dispositivo de conmutación (a veces se lo llama IMP (Interchange Message Procesor))

El mensaje va de uno a otro Host íntegramente. Estas redes se pueden ser **Punto a Punto, Almacenamiento y Envío, Conmutación por Paquetes**, etc.

Los de difusión tienen un solo canal compartido por todos los Host. Los mensajes de una máquina se envían al canal y son recibidos por todas las demás. Aquella a la cual va dirigida es la que la leerá. Las redes locales en general son las que usan los canales de difusión.

La Capa de Enlace

La definición de topología de red forma parte de la normativa de correspondiente a la Capa de Enlace de Datos.

En esta capa también se define cómo se establecerán las *direcciones físicas* de cada computadora (direccionamiento físico), y cómo deberán ser las tramas de bits. También se define cómo se establece la *secuencia de tramas enviadas (secuenciamiento)* y asimismo controla cuándo una computadora puede enviar bits a otra sin saturarla (*control de flujo*).

Lo más importante de esta capa es que especifica el *Método de Acceso al Medio* (no nos olvidemos que todas las computadoras de la red usan el mismo medio o cable para comunicarse), como por ejemplo CSMA/CD o Token Ring. Esto lo veremos más en detalle cuando estudiemos Redes LAN.

Por último también se encarga de *detectar posibles errores en la transmisión* (control de errores), aplicando por ejemplo algoritmos de suma de verificación (al estilo checksum, CRC, etc.).

La mayoría de las funciones mencionadas se implementan directamente sobre la placa de red, es decir en lo que suele denominarse firmware (software grabado en circuitos integrados).

En cuanto a las normas que cumplen estos requisitos para redes LAN, podemos decir que la norma Ethernet cubre por completo las capas física y de enlace, en tanto que las normas de la IEEE 802 han subdividido la capa de enlace en dos subcapas:

- **LLC (Logic Link Control o Control de enlace Lógico)** y
- **MAC (Media Access Control o Control de Acceso al Medio)**, como se muestra en la figura 11:

Como puede observarse, según la normativa de la IEEE, las Normas IEEE 802.3 y 802.5 cumplimentan la capa física y la subcapa MAC quedando a cargo de la Norma IEEE 802.2 la subcapa LLC.

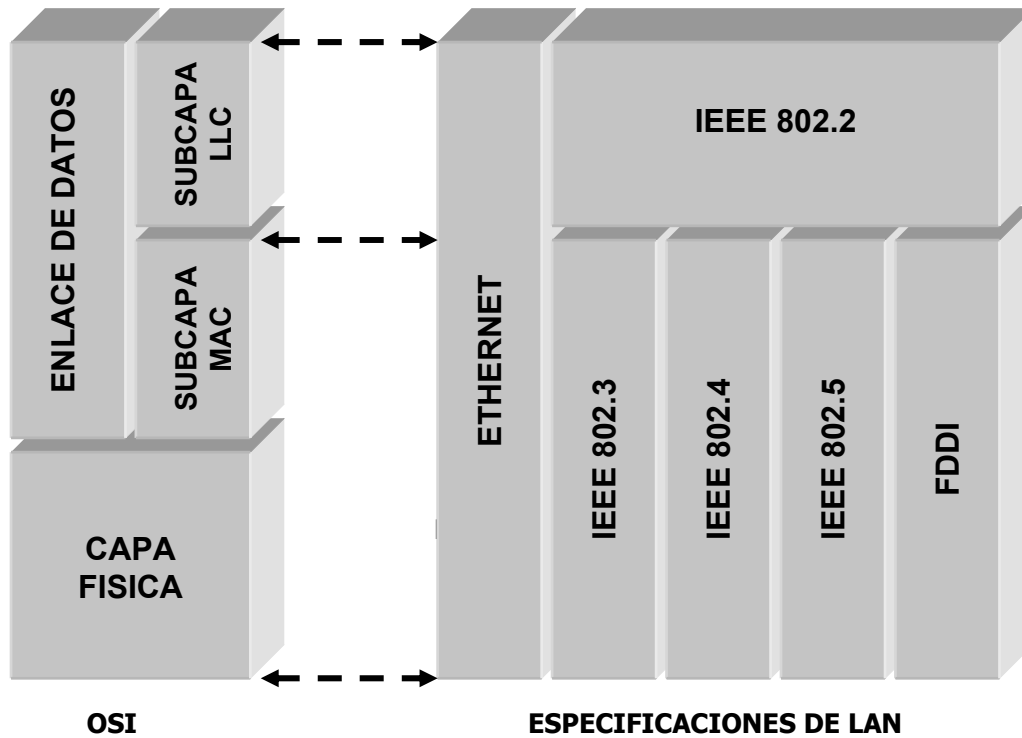


Figura 11

Veremos más en detalle estas subcapas cuando veamos Redes LAN.

Ejemplos de Capa de Enlace en Redes Públicas

Casi todos se derivan del protocolo de enlace usado en SNA, conocido como SDLC (Synchronous Data Link Control) de IBM.

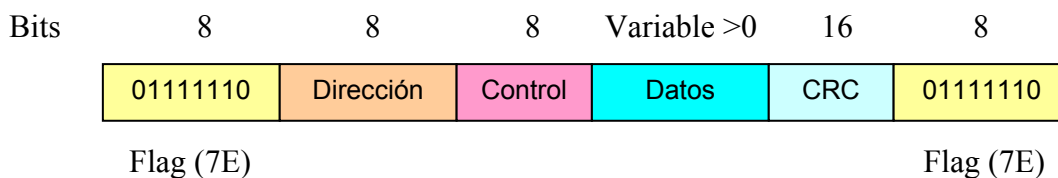
ANSI lo modificó para generar el ADCCP (Advanced Data Control Communication Protocol), y la ISO generó el HDLC (High-Level Data Link Control).

Posteriormente el CCITT modificó el HDLC para dar lugar al LAP (Link Access Procedure), como parte de la norma X.25, pero más tarde lo modificó creando el LAPB (Link Access Procedure Balanced), de manera de hacerlo más compatible con el HDLC.

Todos estos protocolos tienen algo en común, están orientados al bit, y utilizan inserción de bits (inserción de ceros) para la transparencia de datos.

Todos los protocolos orientados al bit utilizan la estructura de trama como la de la figura:

Trama HDLC de OSI



El campo Dirección es fundamental en líneas multipunto.

El campo Control se utiliza para los números de secuencia, asentimientos etc.

El campo Datos es la información del usuario, puede ser arbitrariamente largo, pero la eficiencia del CRC decrecerá a medida que el campo de datos aumente, debido a la posibilidad de tener errores de grupo.

El campo CRC (Código de Redundancia Cíclica).

Hay tres tipos de tramas, variando fundamentalmente el campo control:

1. Información.
2. Supervisoras.
3. Sin numerar.

Las Capas Medias: Red y Transporte

La Capa de Red (Network Layer)

Esta capa se ocupa del control de la operación de la red. Un punto muy importante en su diseño es la determinación de como encaminar los mensajes (o paquetes).

Las rutas podrían basarse en tablas estáticas previamente cableadas en la red, siendo cualquier cambio difícil de realizar. También pueden ser tablas estáticas que se establecen al inicio de cada diálogo.

Por último, pueden ser de tipos dinámicos, determinándose la ruta para cada paquete en el momento en que este es emitido.

El control de congestión por lo tanto también depende de la capa de red.

A veces se coloca una función de contabilidad para realizar tareas de facturación.

La responsabilidad para resolver problemas de interconexión de redes heterogéneas recae en la capa de red.

En las redes de difusión, el encaminamiento es simple, por lo tanto la capa de red es muy pequeña, o a veces no existe.

La capa de red proporciona servicios a la de transporte.

La capa de red opera esencialmente en los Routers, mientras que la de transporte opera en los HOST, los límites entre estas capas, es también el límite entre la red y el Host (usuario). Esto implica que los servicios de la capa de red definen los servicios ofrecidos por la propia red.

Cuando la red es operada por un proveedor de servicios portadores, y los Host son operados por los usuarios, el servicio de capa de red se convierte en la interfase entre el proveedor y los usuarios. Como tal define las obligaciones y responsabilidades del proveedor y del usuario.

Los servicios de la capa de red se han diseñado con los siguientes objetivos:

1. Deben ser independientes de la tecnología de la red.
2. La capa de transporte debe tener oculto el número, tipo y topología de las redes que se encuentren presentes.
3. Las direcciones de red a disposición de la capa de transporte deben utilizar un plan de numeración uniforme, aún a través de redes LAN y WAN.

Uno de los grupos argumenta que la capa de red solo debe mover los bits, y nada más. Desde este punto de vista, los Host deben aceptar que la red es poco fiable y llevar a cabo ellos mismos el control de errores y de flujo. Esto nos conduce a que el servicio de red debería ser no orientado a conexión.

El otro grupo (representado por las empresas telefónicas), argumenta que la capa de red debe proporcionar un servicio fiable, orientado a conexión con las siguientes propiedades:

1. Antes de transmitir datos, deberá establecerse la conexión entre las entidades de transporte origen y destino. Esta conexión se utilizará hasta que finalice la sesión.
2. Cuando se establezca una conexión, las entidades de transporte y de red negociarán los parámetros de calidad y costo del servicio.
3. La comunicación se establecerá en ambas direcciones, y los paquetes se entregarán sin errores y en forma secuencial. El modelo conceptual se basa en la cola de espera normal, en donde el primero que entra es el primero en salir.
4. El control de flujo se proporciona automáticamente para impedir que un emisor rápido inunde de paquetes a la cola de espera.

Encaminamiento

La función real de la capa de red es la de proveer encaminamiento o enrutamiento de paquetes desde el origen hasta el destino. En muchas redes los paquetes necesitan realizar muchos saltos para completar un viaje. La excepción la dan las redes de difusión (broadcast), pero aun aquí el encaminamiento es interesante cuando el origen y el destino no se encuentran en la misma red.

El algoritmo de encaminamiento es la parte del software correspondiente a la capa de red, que es responsable de decidir sobre por cual línea de salida deberá transmitir un paquete que llega.

Cuando se utilizan datagramas, la decisión deber tomarse con cada paquete que llegue, mientras que en el caso de circuitos virtuales, las decisiones de encaminamiento solo se tomarán cuando se establezca un nuevo circuito virtual, después los paquetes seguirán la ruta establecida.

A esto último se le conoce como encaminamiento de sesión, ya que la ruta permanece durante toda la sesión.

Algoritmos de Encaminamiento

Se pueden agrupar en dos clases principales: no adaptativos y adaptativos.

Los algoritmos no adaptativos no basan sus decisiones en mediciones o estimaciones del tráfico o topología actual, sino que la elección de la ruta para ir del nodo "i" al nodo "j" se determina anticipadamente, fuera de línea cuando la red se arranca. También se le denomina encaminamiento estático.

Los algoritmos adaptativos, intentan cambiar sus decisiones de encaminamiento para reflejar los cambios de topología y de tráfico actual.

Existen tres familias de algoritmos adaptativos, que se diferencian de acuerdo con la información que utilizan.

1. Los algoritmos globales, utilizan información recogida en toda la red. A esto se le conoce como encaminamiento centralizado.
2. Los algoritmos locales operan en forma separada sobre cada nodo, y solo utilizan la información que se encuentra disponible allí, como por ejemplo la longitud de las colas de espera. A estos se los conoce como algoritmos aislados.
3. Por último, la tercera clase de algoritmos utiliza una combinación del tipo global y local, y se le conoce como algoritmos distribuidos.

Encaminamiento por el Camino más Corto

La idea consiste en construir una gráfica de la red. Para escoger cada ruta el algoritmo solo debe determinar el camino más corto existente entre ellos.

El concepto de camino más corto, es una forma de medir la longitud del camino a través del número de saltos, para ello podemos utilizar varias formas de definirlo, según la métrica que se utilice. Por ejemplo, se puede tomar el camino geográfico, pero también podría etiquetar cada enlace con el retardo promedio de las colas de espera. Con esto, el camino más corto resulta ser el de menor retardo.

En general las etiquetas podrían calcularse como una función de la distancia, ancho de banda, promedio de tráfico, costo de comunicación, retardo medio, etc. De esta manera los algoritmos calcularan el camino más corto como una combinación de estos parámetros.

Encaminamiento de Camino Múltiple

Es una variante del anterior, en donde no sólo se calcula el camino más corto, como única alternativa, sino, entre varios nodos pueden utilizarse varios caminos igualmente buenos y con frecuencia es conveniente dividir el tráfico entre varios caminos. Esto se conoce como encaminamiento múltiple.

Encaminamiento Centralizado

Los algoritmos vistos anteriormente, necesitan tener información acerca de la topología y el tráfico de la red para poder tomar las mejores decisiones. Si la topología es estática y el tráfico se mantiene más o menos constante, la construcción de las tablas de encaminamiento es sencilla, y se realiza una sola vez fuera de línea.

Sin embargo si los nodos se desactivan y se restablecen, o, bien si el tráfico sufre variaciones muy grandes durante el día, se necesita de un mecanismo para actualizar las tablas.

Cuando se utiliza un algoritmo centralizado, en algún punto de la red hay un Centro de Control de Encaminamiento o de Red. Periódicamente, cada nodo transmite a este centro información sobre su estado, que al conocer el estado de toda la red puede tomar decisiones.

Esto parece atractivo a primera vista, pero también tiene sus serios problemas. Si la red tiene que adaptarse a tráfico muy variable, el cálculo del encaminamiento deberá efectuarse con demasiada frecuencia. Para una red grande este cálculo tomará bastante tiempo. Otro problema insalvable se da si el centro de red se ve aislado o se desactiva por fallas propias o de las líneas de enlace.

Encaminamiento Aislado

En este algoritmo, los nodos toman decisiones basados en la información que ellos mismos tienen. Estos algoritmos lo que hacen es, cuando llega el paquete, ponerlo inmediatamente en la cola de espera de salida más corta, sin tener en cuenta el lugar de dirección de esa línea.

Una variante de este es el de combinarlo con el algoritmo centralizado, entonces cada paquete que llegue se colocará en la salida cuyo peso estático y colas de espera sean menores.

Otra variante es la de utilizar el mejor peso estático, a menos que se supere un cierto umbral.

Otra variante es la del aprendizaje hacia atrás. Este consiste en preguntarle a cada paquete que llega cual es la situación de donde proviene. Para ello deberá incluirse la identidad del nodo origen en cada paquete, junto a un contador que se incrementa con cada salto. Si un nodo ve llegar un paquete del nodo "B" por la línea "h" y su contador está en 5, sabrá que el nodo "B" no está más lejos de él que 5 saltos sobre esa línea.

De esta manera puede estimar cual es el mejor enlace entre él y el nodo "B".

Encaminamiento Distribuido

En este algoritmo, cada nodo intercambia información con sus vecinos. Cada nodo mantiene una tabla de encaminamiento con una entrada por cada uno de los demás nodos vecinos. Esta entrada consta de dos partes: la línea preferida de salida que utilice para dicho destino, y alguna estimación del tiempo o distancia hacia él. La métrica utilizada podría ser el número de saltos, el retardo, los paquetes encolados, ancho de banda, etc.

Se supone que el nodo conoce la "distancia" a cada uno de sus vecinos, la que puede estar constituida por algunos o combinaciones de varios de los parámetros anteriores.

Congestión

Cuando existen muchos paquetes dentro de la red, el rendimiento se degrada. Esta situación se conoce como congestión.

Algoritmos de Control de la congestión

Existen varias estrategias para el control de la congestión:

1. Que asignen recursos anticipados
2. Que desechen paquetes cuando no se pueden procesar.
3. Que se restrinja el número de paquetes en la red.
4. Utilizar el control de flujo para evitar la congestión.
5. Obstruir la entrada de datos cuando la red está sobrecargada

Bloqueo

La máxima congestión es el bloqueo, también llamado estancamiento. En este caso los nodos no pueden proseguir hasta tanto su vecino no realice una acción, el que a su vez espera de otro nodo, y este del primero, creándose un círculo vicioso del cual no podrán salir produciéndose un bloqueo.

Si bien existen varios algoritmos que previenen el bloqueo, todos se basan en la asignación y el control de los recursos de cada nodo, evitando la transmisión si no se asegura la continuidad del camino del paquete.

Ejemplo de Capa de Red

Existen varios protocolos de Capa de Red el modelo más adecuado como ejemplo es el de IP (Internet Protocol), utilizado como protocolo de red del modelo TCP/IP y que veremos con más detalles en próximas situaciones profesionales. Otro protocolo bastante común es X.25 utilizado en las redes de conmutación de paquetes (cajeros automáticos y algunos enlaces satelitales).

Capa de Transporte (Transport Layer)

La función principal de la capa de transporte consiste en aceptar los datos de la capa de sesión, dividirlos (si es necesario) en unidades más pequeñas, pasarlos a la capa de red y asegurar que todos los pedazos (segmentos) lleguen correctamente al otro extremo. Además debe aislar a la capa de sesión de los cambios de tecnología del Hardware.

La capa de transporte es el corazón de la jerarquía de protocolos. Su tarea consiste en asegurar el transporte de datos desde la máquina FUENTE a la máquina DESTINO, independientemente de la red física en uso.

Hay muchas aplicaciones que solo necesitan un método fiable para transmitir un flujo de bits entre dos máquinas. Por ejemplo en Linux, los buses entre máquinas solo necesitan un proceso de transporte de bits. Para realizar esta función dichos buses no necesitan ningún servicio de sesión o presentación.

Hay muchas aplicaciones que no tienen capa de sesión y presentación.

Existe solo un protocolo de transporte, anterior a OSI que está bien establecido, es el TCP.

El objetivo principal de la capa de transporte consiste en proporcionar un servicio a las entidades de la capa de sesión. Para alcanzar este objetivo utilizará los servicios de la capa de red. Al Hardware y Software que hacen este trabajo se los conoce como "**entidades de transporte**".

Así como hay dos tipos de servicios de red, también existen dos tipos de servicios de transporte, es decir orientado a conexión y sin conexión (por ejemplo TCP), o no orientado a conexión (UDP).

El servicio de transporte orientado a conexión es similar al servicio de red orientado a conexión. En ambos casos, las conexiones tienen tres fases:

- la de establecimiento,
- la de transferencia de datos,
- la de liberación.

Los procedimientos de direccionamiento y control de flujo son similares en ambas capas.

El servicio de transporte sin conexión es similar al de red sin conexión.

Por supuesto surgen las preguntas obvias:

¿Si el servicio de transporte es tan similar al de red, cuál es la razón de tener dos capas diferentes?, ¿por que razón una sola capa es inadecuada?

La respuesta es delicada, pero crucial y nos lleva a la siguiente figura del modelo de comunicaciones.

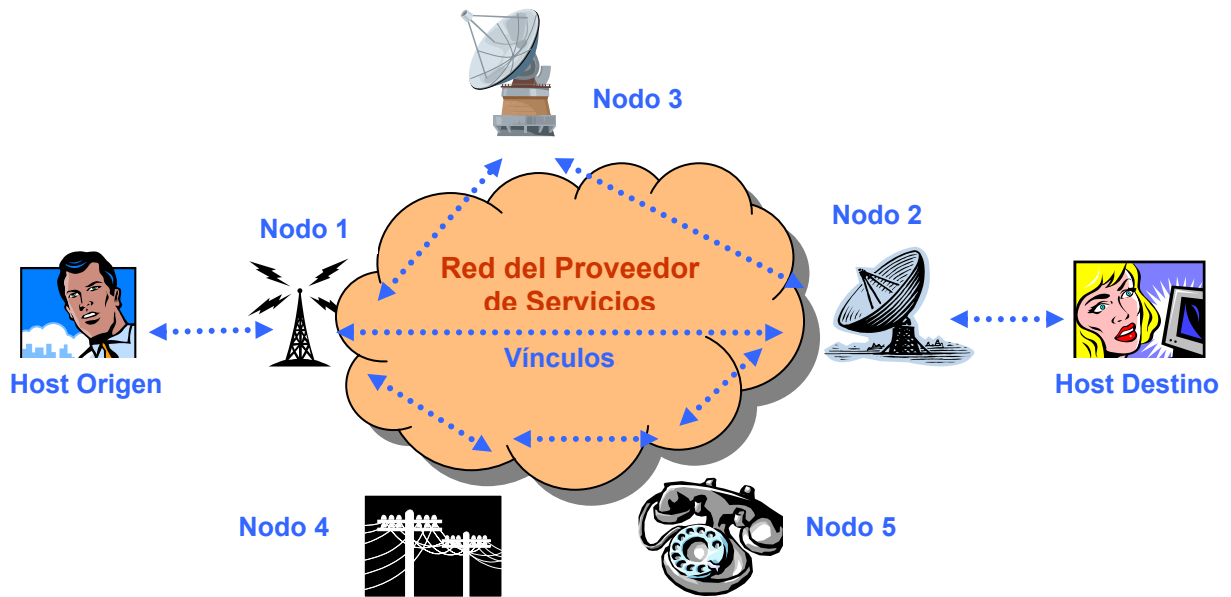


Figura 12

Si trasladamos esto al modelo OSI, podemos ver que las tres capas inferiores se comunican entre adyacentes, o sea del host emisor (origen) al nodo de comunicaciones más cercano, donde están conectadas, desde este nodo al siguiente (puede haber varios en el camino de los mensajes) y de este último al host receptor (destino), mientras que desde la capa de Transporte hacia arriba, todas las demás tienen comunicación extremo a extremo

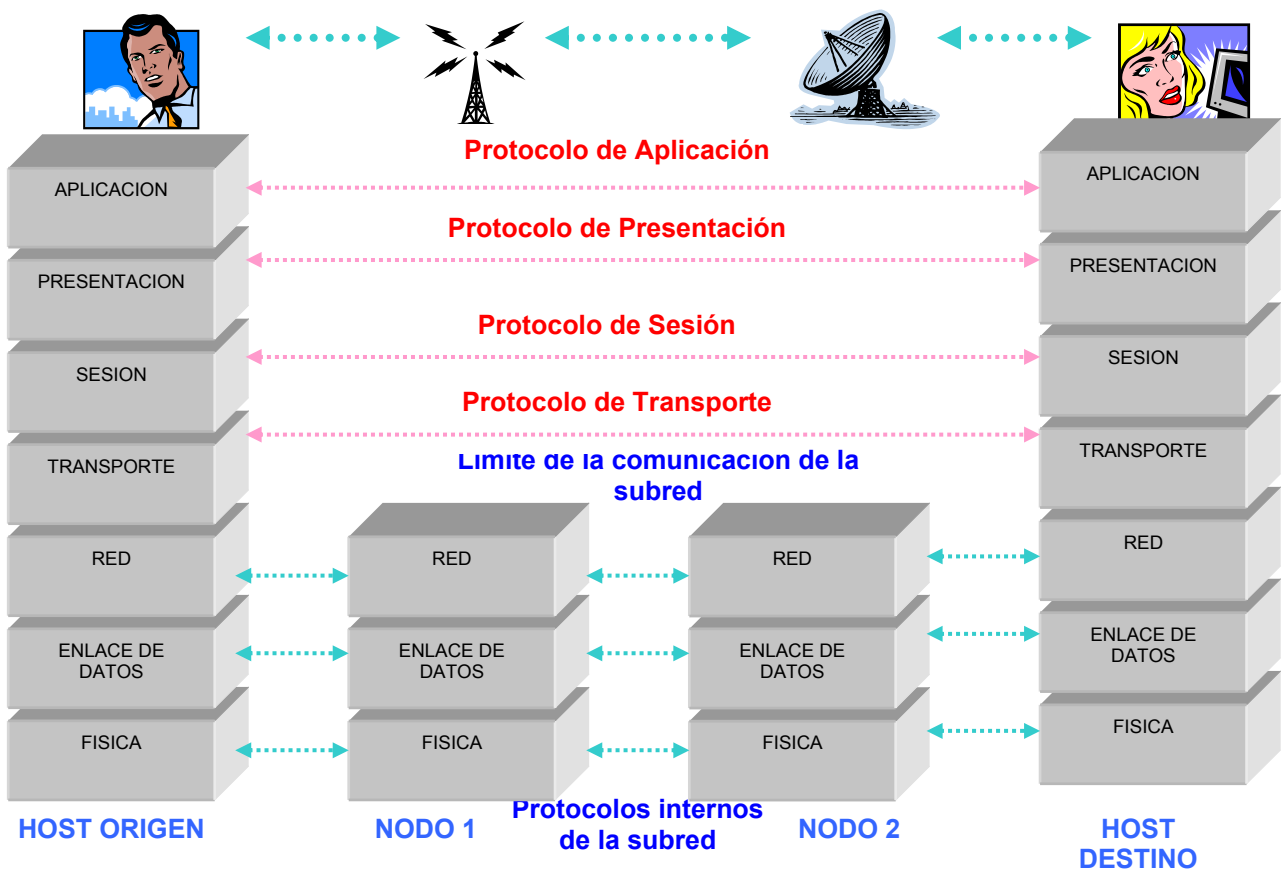


Figura 13

En esta figura podemos ver que la capa de red es parte de la subred de comunicaciones y es operada por el operador del servicio (al menos para las redes WAN).

¿Qué pasaría si la capa de red ofreciera un servicio orientado a conexión, pero inseguro?.

Supongamos que se perdiesen paquetes frecuentemente.

Como los usuarios no ejercen control sobre la subred, no pueden resolver el problema relacionado con un servicio deficiente, ya que no pueden cambiar los equipos en los nodos (routers o switches) o incrementando el tratamiento de errores en la capa de enlace.

La única posibilidad entonces es la de colocar una capa por encima de la de red que mejore la calidad del servicio.

Si a una entidad de transporte se le avisa, a la mitad de una larga transmisión, que se ha interrumpido su conexión de red sin indicación respecto a los datos en tráfico, ella puede establecer una nueva conexión.

Utilizando esta nueva conexión, la entidad de transporte puede preguntar a su corresponsal que datos llegaron y cuales no, y reiniciar la transmisión a partir de allí.

Básicamente podemos decir que la existencia de la capa de transporte hace más confiable el servicio que el proporcionado por la capa de red, dado que la capa de Transporte realiza un **control de extremo a extremo** (end-to-end)

Gracias a la capa de transporte, es posible que los programas de aplicación puedan escribirse usando un conjunto de primitivas y hacer que funcionen en una gran variedad de redes, sin preocuparse de tratar con diferentes interfases de cada red.

Podemos dividir el modelo OSI en dos partes:

- De la capa 1 a la 4 serán proveedoras de servicio de transporte.
- De la capa 5 a la 7 serán usuarios del servicio de transporte.

Esta diferencia entre proveedor y usuario tiene un impacto considerable sobre el diseño de las capas y coloca a la capa de transporte en una posición clave, ya que constituye la frontera entre proveedor y usuario de un servicio de transmisión de datos seguro.

Otra forma de ver la capa de transporte es la de considerar que su función es la de enriquecer la QOS (Quality Of Service) o Calidad de Servicio suministrada por la capa de red.

Si el servicio de red es muy bueno, la capa de transporte puede tener un trabajo muy sencillo.

En otras palabras, la capa de transporte está para contribuir y llenar huecos entre lo que los usuarios desean y lo que el servicio de red ofrece.

Bajo condiciones normales la capa de transporte crea una conexión de red distinta para cada conexión de transporte solicitada por la capa de sesión.

Si el transporte necesita un gran caudal, esta capa podría crear múltiples conexiones de red, dividiendo los datos entre las conexiones de red.

La capa de transporte determina que tipos de servicio le brindará a la capa de sesión, y en definitiva a los usuarios.

La capa de transporte es una capa del tipo "**origen-destino**" o "**extremo a extremo**". Es decir un programa en la máquina origen establece un diálogo con uno similar en la máquina destino, usando las cabeceras de los paquetes y mensajes de control.

Los protocolos de la capa de red son entre máquinas inmediatas o vecinas y no entre origen y destino, las cuales podrían estar separadas por varios nodos.

En la figura del modelo OSI (figura 13) puede observarse la diferencia entre las capas 1 a 3 que están encadenadas, y las capas 4 a 7 que son extremo a extremo.

Es normal que se tengan múltiples conexiones, por lo que se necesitará alguna forma de decir que mensajes pertenecen a que conexión. La cabecera de transporte es un lugar donde se puede colocar esta información.

Las Capas Superiores: Sesión, Presentación y Aplicación

Capa de Sesión (Session Layer)

Esta capa permite que los usuarios establezcan sesiones de trabajo entre ellos.

Por ejemplo, una sesión podrá permitir al usuario acceder a un sistema de tiempo compartido a distancia, o transferir un archivo entre dos máquinas. Otra sesión permitirá acceder a una página web de Internet (protocolo http), mientras otra podrá mantener un diálogo de chat entre varios correspondientes.

Uno de los servicios de la capa de sesión consiste en gestionar el control de diálogo.

Las sesiones controlan el tráfico de los mensajes en ambas direcciones.

La administración del testigo es un servicio de la capa de sesión en las redes TOKEN RING.

Otro servicio de la capa de sesión es la SINCRONIZACION.

La capa de sesión proporciona puntos de verificación en el flujo de datos, con objeto de que, después de una caída del enlace, solo se repitan los mensajes desde el último punto de verificación.

El propósito de la existencia de una sesión en OSI) consiste en proveer a las capas superiores un canal libre de errores, independiente de la tecnología de las capas inferiores.

Capa de Presentación (Presentation Layer)

A diferencia de las capas anteriores, preocupadas en el movimiento fiable de los bits de un extremo al otro, la capa de presentación se ocupa de los aspectos de sintaxis y semántica de la información que transmite.

Un ejemplo típico de servicio de esta capa es el relacionado con la codificación de datos conforme a lo acordado previamente.

La mayor parte de los programas de aplicación no intercambian trenes de bits aleatorios, sino estructuras de datos constituidos por varios elementos sencillos. Se pueden tener diferentes códigos (ASCII, EBCDIC), enteros, complementos a uno, a dos, etc.

Para posibilitar la comunicación de ordenadores con diferentes representaciones, la estructura de los datos a intercambiar puede definirse en forma abstracta.

El trabajo de manejar estas estructuras abstractas, y la conversión de la representación utilizada en el ordenador a la representación normal de la red, se lleva a cabo a través de la capa de presentación.

Esta capa está ligada también a otros aspectos de representación de la información. Por ejemplo la **COMPRESION DE DATOS**, que se utiliza para disminuir el tamaño de los mensajes a transmitir.

Otro aspecto es el de criptografía, o encriptación de datos, usada para cambiar la representación de los datos por razones de seguridad.

Capa de Aplicación (Application Layer)

Esta capa contiene una variedad de protocolos necesarios para hacer compatibles los distintos dispositivos de aplicación.

Por ejemplo, considérese un editor orientado a pantalla que deba trabajar en una red con diferentes tipos de terminales, con distintas secuencias de escape, para insertar, borrar, movimientos de cursor, etc.

Una forma de resolver este problema consiste en definir una **Terminal Virtual de Red** abstracta, con la cual los programas pueden ser escritos de forma de tratar con ella.

Para transferir funciones de una terminal virtual de una red a una terminal real se debe escribir un software que permita el manejo de cada tipo de terminal.

Por ejemplo, cuando el editor mueva el cursor del terminal virtual al extremo superior izquierdo, dicho software deber emitir la secuencia de comandos para que el terminal real ubique al cursor en el sitio indicado.

El software completo del terminal virtual se encuentra en la capa de aplicación.

Otra función de la capa de aplicación es la transferencia de archivos.

La transferencia de archivos entre dos sistemas diferentes, requiere de la resolución de las incompatibilidades.

Otros servicios que también corresponden a esta capa son los Navegadores de Internet (Netscape, Explorer, etc) los cuales se tratan de software cliente que permite que un usuario pueda recorrer (navegar) distintos sitios de Internet.

Otros servicios son, el de Correo Electrónico, Servicios de Directorio, etc.

Transmisión de Datos en el Modelo OSI

La figura 14 muestra como pueden transmitirse los datos mediante el modelo OSI.

El proceso emisor tiene datos que desea enviar al proceso receptor.

Los datos son generados en la aplicación, que los pasa a la **Capa de Aplicación**, que le agrega la cabecera **AH** (Application Header), que puede no existir.

Esta la pasa a la **Capa de Presentación** que los transforma en diferentes formas, con la posibilidad de incluir una cabecera en la parte frontal, pasando el resultado a la capa de Sesión.

Es importante observar que la Capa de Presentación no sabe distinguir cuales son datos y cual es el **AH** en lo que le pasó la Capa de Aplicación. Ni le corresponde saberlo.

Este proceso se repite hasta que se llega a la capa Física, lugar donde se transmiten definitivamente, en forma de trenes de bits, al receptor.

En la otra máquina se produce el camino inverso.

La idea fundamental es que si bien la transmisión efectiva de datos es vertical, cada una de las capas está programada como si fuera transmisión horizontal.

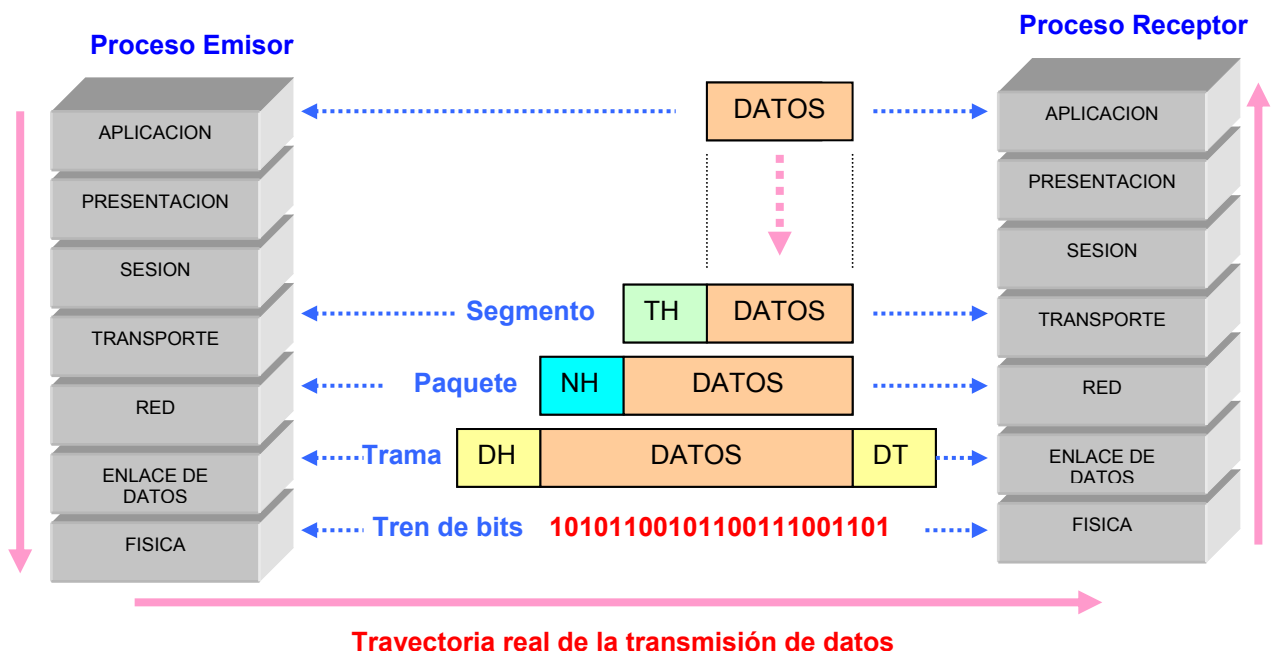


Figura 14

Servicios

La verdadera función de cada una de las capas OSI consiste en proporcionar servicios a las capas superiores.

Se llaman entidades a los elementos activos que se encuentran en cada capa, pueden ser software o hardware.

Las entidades de la misma capa pero de distintas máquinas se llaman capas homólogas o pares o iguales.

Las entidades de la capa "N" desarrollan un servicio para la capa "N+1". En este caso, la capa "N" se la denomina PROVEEDOR DE SERVICIO, y a la capa "N+1" USUARIO DEL SERVICIO.

Los servicios están disponibles en el SAP (SERVICES ACCESS POINT) o punto de acceso al servicio.

Los SAP de la capa "N" son los lugares donde la capa "N+1" puede acceder a los servicios que se ofrecen.

Cada SAP tiene una dirección que lo identifica.

En el servicio telefónico, un SAP son los enchufes en donde se conectan los teléfonos y las direcciones de los SAP son los números de abonado correspondientes a esos enchufes.

Para que haya intercambio de información entre dos capas, debe existir un conjunto de reglas acerca de la interfase.

En una interfase típica, la entidad de la capa "N+1" pasa un IDU (Interface Data Unit), o unidad de datos de la interfase a la capa "N", a través del SAP, como se ve en la figura 15.

El IDU está formado por una SDU (Service Data Unit) o unidad de datos del servicio y de información de control ICI (Information Control Interface).

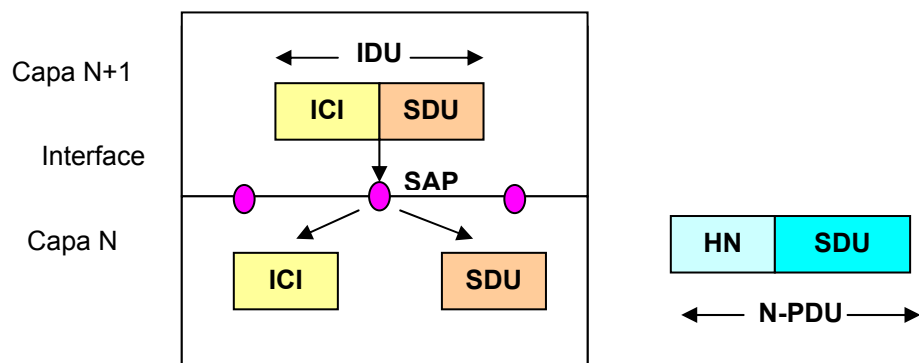


Figura 15

Para hacer la transferencia de una SDU puede ser necesario la fragmentación por parte de la capa "N", de forma que a cada una se le asigne una cabecera y se envíe como PDUs distintas (PDU = Protocol Data Unit) o unidad de datos del protocolo.

Las entidades pares o iguales usan las cabeceras de la PDU para llevar a cabo su protocolo de igual a igual.

Las PDU de transporte se les conoce como TPDU (Transport Protocol Data Unit), o unidad de datos del protocolo de transporte. En TCP/IP, estas Unidades de Datos del Protocolo se las conoce como "Segmentos".

Las de sesión SPDU (Sesion Protocol Data Unit), y las de aplicación APDU (Aplication Protocol Data Unit).

Autoevaluación

Pregunta 1. Una red está formada por dos tipos de componentes. Indique cuales son:

Pregunta 2. Indique que tipos de canales de comunicación conoce

Pregunta 3. Una red punto a punto implica que el canal es compartido por todos los host y los mensajes son recibidos por todas las estaciones.
(A) Verdadero (B) Falso

Pregunta 4. Una red de difusión es una red en la cual el mensaje va de un extremo a otro y no es compartido por todas las estaciones
(A) Verdadero (B) Falso

Pregunta 5. Indicar cuales son algunos de los aspectos tener en cuenta al analizar la red.

Pregunta 6. Indique que define la capa física del Modelo OSI.

Pregunta 7. Indicar en que capas del modelo OSI interviene la placa de red (NIC)

Pregunta 8. ¿En que capa del modelo OSI se definen las direcciones Físicas o de Hardware?
(A) Red
(B) Transporte
(C) Enlace de Datos
(D) Aplicación
(E) No existen las direcciones físicas o de hardware

Pregunta 9. ¿En que capa del modelo OSI se define la topología de la red?.

Pregunta 10. En cuantas subcapas se divide la Capa de Enlace de Datos según IEEE 802.

Pregunta 11. Indique cuantos campos componen una trama HDLC.

Pregunta 12. Indicar cual es la función de la Capa de Red según el modelo OSI.

Respuestas a la Autoevaluación

- Pregunta 1. Respuesta:** Una red, en general consiste de dos componentes: La línea de transmisión y los elementos de conmutación.
- Pregunta 2. Respuesta:** Punto a punto y de difusión.
- Pregunta 3. Respuesta:** Falso estas son redes de difusión.
- Pregunta 4. Respuesta:** Falso estas son redes punto a punto.
- Pregunta 5. Respuesta:** Los aspectos son:
- **TOPOLOGIA:** determina la interconexión entre los usuarios.
 - **PROTOCOLO:** sincrónico o asincrónico, formato de los mensajes, etc.
 - **INTERFACES ELECTRICAS:** RS-232, RS-422, V.35, V.24/V.28, etc.
 - **VINCULOS SELECCIONADOS:** Este elemento condiciona la velocidad, distancia, confiabilidad, seguridad, facilidad de incorporar nuevos usuarios. Entre otros podemos mencionar: par telefónico, cable coaxil, radioenlaces (VHF, UHF, Microondas), enlaces satelitales, fibras ópticas, etc.
 - **PROCEDIMIENTOS DE RECUPERACION:** Procedimientos para el manejo de problemas tales como errores, ruido, etc.
- Pregunta 6. Respuesta:** La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico
- Pregunta 7. Respuesta:** La *placa de red o NIC (Network Interface Card)*, interviene en la Capa Física y Capa de Enlace de Datos.
- Pregunta 8. Respuesta:** En la Capa de Enlace de Datos. La dirección de Hardware o Física la provee la placa de red (NIC).
- Pregunta 9. Respuesta:** En la Capa de Enlace de Datos. La topología de la red lo define el Método de Acceso al Medio.
- Pregunta 10. Respuesta:** Se subdivide en dos subcapas Control (LLC) y Control De Acceso al Medio (MAC).
- Pregunta 11. Respuesta:** Una trama HDLC se compone de los siguientes campos:
- **Dirección** es fundamental en líneas multipunto.
 - **Control** se utiliza para los números de secuencia, asentimientos etc.
 - **Datos** es la información del usuario, puede ser arbitrariamente largo, pero la eficiencia del CRC decrecerá a medida que el campo de datos aumente, debido a la posibilidad de tener errores de grupo.
 - **CRC (Código de Redundancia Cíclica).**
 - Además se identifica el comienzo y fin de la trama con un campo Flag compuesto de la secuencia **01111110 (7E)**.
- Pregunta 12. Respuesta:** Esta capa se ocupa del control de la operación de la red y la determinación de como encaminar los mensajes (o paquetes).