

1.2.3 Redes de área Amplia WAN. Abarca un área geográfica amplia. Contiene un conjunto de máquinas diseñadas para aplicaciones de usuarios que llamaremos **Hosts**. Los hosts están conectados por una **Subred de comunicación**, o sólo **subred**. Los clientes son los que poseen a los hosts, mientras que las compañías telefónicas o los proveedores de internet poseen y operan la subred de comunicación. La función de la subred es llevar mensajes de un host a otro.

En la mayoría de la redes WAN la subred consta de 2 componentes distintos: líneas de transmisión y elementos de conmutación. Las **líneas de transmisión** mueven bits entre máquinas. Pueden estar hechas de cable de cobre, fibra óptica o, incluso radioenlaces. **Los Elementos de conmutación** (Routers) son computadoras especializadas que conectan tres o más líneas de transmisión.

Cada host se conecta frecuentemente a una LAN en la que existe un enrutador, aunque en algunos casos un host puede estar conectado de manera directa a un enrutador. El conjunto de líneas de comunicación y enrutadores forma la subred.

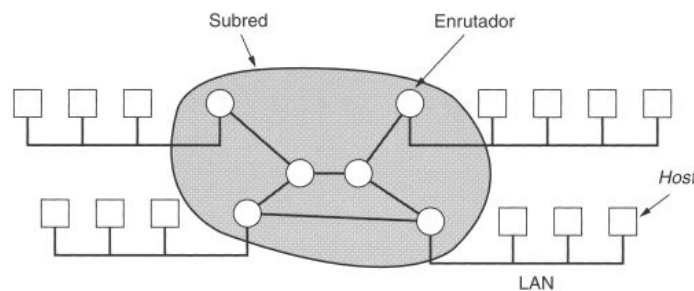


Figura 1-9. Relación entre *hosts* de LANs y la subred.

En la mayoría de las WAN, la red contiene numerosas líneas de transmisión, cada una de las cuales conecta un par de enrutadores. Si dos enrutadores que no comparten una línea de transmisión quieren conectarse, deberán hacerlo de manera indirecta, a través de otros enrutadores. Cuando un paquete es enviado desde un enrutador a otro a través de uno o más enrutadores intermedios, el paquete se recibe en cada enrutador intermedio en su totalidad, se almacena ahí hasta que la línea de salida requerida esté libre y, por último se reenvía. Una subred de este tipo se conoce como subred de almacenamiento y reenvío o de **conmutación de paquetes**. Cuando los paquetes son pequeños y del mismo tamaño se les llama celdas.

Cuando un proceso de cualquier host tiene un mensaje que se va a enviar a un proceso de algún otro host, el host emisor divide primero el mensaje en paquetes, los cuales tienen un número de secuencia. Estos paquetes se envían por la red de uno a uno en una rápida sucesión. Los paquetes se transportan de forma individual a través de la red y se depositan en el host receptor, donde se reensamblan en el mensaje original y se entregan al proceso receptor.

En algunas redes todos los paquetes de un mje determinado **DEBEN** seguir la misma ruta, en otras, cada paquete se enruta por separado. Esto se decide localmente en cada enrutador y la manera en que toma esa decisión se conoce como **algoritmo de enrutamiento**.

No todas las WAN son de conmutación de paquetes. Una segunda posibilidad es un sistema satelital. Cada enrutador tiene una antena a través de la cual puede enviar y recibir.

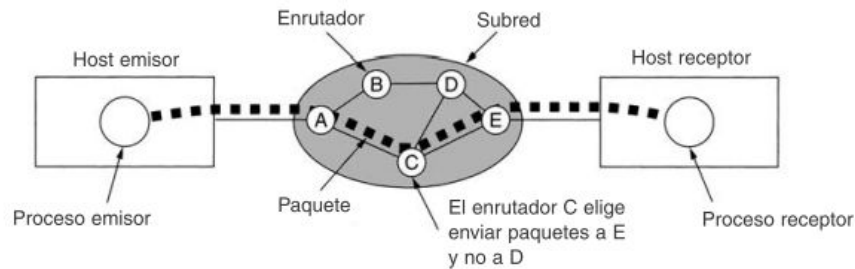


Figura 1-10. Flujo de paquetes desde un emisor a un receptor.

1.2.4 Redes Inalámbricas.

Como primera aproximación, las redes inalámbricas se pueden dividir en 3 categorías principales:

- Interconexión de Sistemas.
- LANs inalámbricas.
- WANs inalámbricas.

La interconexión de sistemas se refiere a la interconexión de componentes de una computadora que utiliza radio de corto alcance.

En la forma más sencilla, las redes de interconexión de sistemas utilizan el paradigma del maestro y el esclavo. El maestro le dice a los esclavos qué direcciones utilizar, cuándo pueden difundir, durante cuánto tiempo pueden transmitir, qué frecuencias pueden utilizar, etc.

El siguiente paso en la conectividad inalámbrica son las LANs inalámbricas. Son sistemas en los que cada computadora tiene un módem de radio y una antena mediante los que se puede comunicar con otros sistemas. Existe un estándar para éstas, llamado IEEE 802.11.

El tercer tipo de red inalámbrica se utiliza en sistemas de área amplia. La red de radio utilizada para teléfonos celulares es un ejemplo de un sistema inalámbrico de banda ancha baja. Este sistema ha pasado por 3 generaciones. La primera analógica y solo para voz. La segunda digital y solo para voz. La tercera digital tanto para voz como para datos. En cierto sentido, las redes inalámbricas celulares son como las LANs inalámbricas, excepto porque las distancias implicadas son mucho más grandes y las tasas de bits son mucho más bajas. La mayoría de las redes inalámbricas se enlaza a la red alámbrica en algún punto para proporcionar acceso a archivos, datos e internet.

1.2.5 Redes Domésticas.

La conectividad doméstica tiene algunas propiedades diferentes a las de otro tipo de redes. Primero, la red y los dispositivos deben ser fáciles de instalar.

Segundo, la red y los dispositivos deben estar plenamente probados en operación.

Tercero, el precio bajo es esencial para el éxito.

Cuarto, la principal aplicación podría implicar multimedia, por lo que la red necesita capacidad suficiente.

Quinto, se podría empezar con uno o dos dispositivos y expandir de manera gradual el alcance de la red. Esto significa que no habrá problemas con el formato.

Sexto, la seguridad y la confianza serán muy importantes.

Para abreviar, la conectividad doméstica ofrece muchas oportunidades y retos. La mayoría de ellos se relaciona con la necesidad de que sean fáciles de manejar, confiables y seguros, en particular en manos de usuarios no técnicos, y que al mismo tiempo proporcionen alto desempeño a bajo costo.

1.2.6 Interredes.

Existen muchas redes en el mundo, a veces con hardware y software diferentes. Con frecuencia, las personas conectadas a una red desean comunicarse con personas conectadas a otra red diferente. La satisfacción de este deseo requiere que se conecten diferentes redes, con frecuencia incompatibles, a veces mediante máquinas llamadas **puerta de enlace** (gateways) para hacer la conexión y proporcionar la traducción necesaria, tanto en términos de HW como de SW. Un conjunto de redes interconectadas se llama **interred**.

Una forma común de interred es el conjunto de LANs conectadas por una WAN.

Subredes, redes e interredes con frecuencia se confunden. La subred tiene más sentido en el contexto de una red de área amplia, donde se refiere a un conjunto de enrutadores y líneas de comunicación poseídas por el operador de redes. La combinación de una subred y sus hosts forma una red. En el caso de una LAN, el cable y los hosts forman la red. En realidad, ahí no hay una subred. Una interred se forma cuando se interconectan redes diferentes.

1.3 SW de redes.

1.3.1 Jerarquías de protocolos.

Para reducir la complejidad de su diseño, la mayoría de las redes está organizada como una pila de **capas** o **niveles**, cada una construida a partir de la que está debajo de ella. El propósito de cada capa es ofrecer ciertos servicios a las capas superiores, a las cuales no se les muestran detalles reales de implementación de los servicios ofrecidos.

La capa N de una máquina mantiene una conversación con la capa N de otra máquina. Las reglas y convenciones utilizadas en esta conversación se conocen como protocolo de capa N. Básicamente, un **protocolo** es un acuerdo entre las partes en comunicación sobre cómo se debe llevar a cabo la comunicación.

Se ilustra una red de 5 capas (Fig. 1-13). Las entidades que abarcan las capas correspondientes en diferentes máquinas se llaman **iguales (peers)**. Los iguales son los que se comunican a través del protocolo.

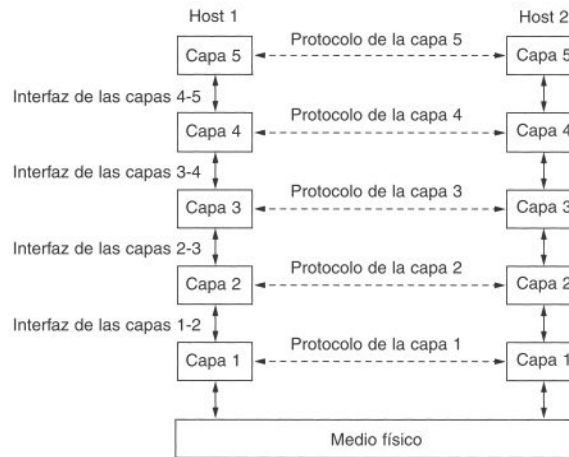


Figura 1-13. Capas, protocolos e interfaces.

En realidad, los datos no se transfieren de manera directa desde la capa N de una a otra máquina, sino que cada capa pasa los datos y la información de control a la capa inmediatamente inferior, hasta que se alcanza la capa más baja. Debajo de la capa 1 se encuentra el **medio físico** a través del cual ocurre la comunicación real.

Entre cada par de capas adyacentes está una **interfaz**. Ésta define qué operaciones y servicios primitivos pone la capa más baja a disposición de la capa superior inmediata. Con este diseño se requiere que la capa desempeñe un conjunto específico de funciones bien entendidas. Además de minimizar la cantidad de información que se debe pasar entre las capas, las interfaces bien definidas simplifican el reemplazo de la implementación de una capa con una implementación totalmente diferente porque todo lo que se pide de la nueva implementación es que ofrezca exactamente el mismo conjunto de servicios a su vecino de arriba. Es común que diferentes hosts utilicen diferentes implementaciones.

Un conjunto de capas y protocolos se conoce como **arquitectura de red**. La lista de protocolos utilizados por un sistema, un protocolo por capa, se conoce como **pila de protocolos**.

Ejemplo: cómo proporcionar comunicación a la capa superior de la red de 5 capas del siguiente ejemplo.

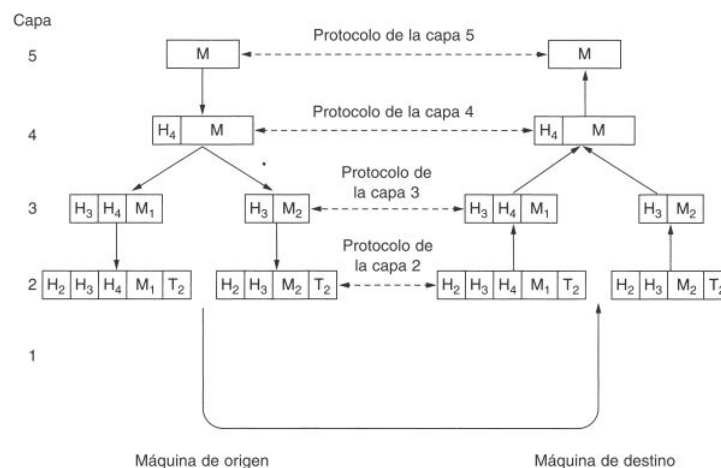


Figura 1-15. Ejemplo de flujo de información que soporta una comunicación virtual en la capa 5.

Un proceso de aplicación que se ejecuta en la capa 5 produce un mensaje, M, y lo pasa a la capa 4 para su transmisión.

La capa 4 pone un **encabezado** al frente del mensaje para identificarlo y pasa el resultado a la capa 3. El encabezado incluye información de control, como números de secuencia, para que la capa 4 de la máquina de destino entregue los mensajes en el orden correcto si las capas inferiores no mantienen la secuencia. En algunas capas los encabezados también pueden contener tamaños, medidas y otros campos de control.

En muchas redes no hay límites para el tamaño de mensajes transmitidos en el protocolo de la capa 4, pero casi siempre hay un límite impuesto por la capa 3. En consecuencia, la capa 3 debe desintegrar los mensajes en unidades más pequeñas llamadas **paquetes**, y a cada paquete se le coloca un encabezado. En el ej. M se divide en 2, M1 y M2.

La capa 3 decide cuál de las líneas utilizar de las que salen y pasa los paquetes a la capa 2. Ésta agrega también un encabezado a cada pieza y también un terminador, y pasa la unidad resultante a la capa 1 para su transmisión física. En la máquina receptora el mje pasa hacia arriba de capa en capa, perdiendo los encabezados conforme avanza. Ninguno de los encabezados de las capas inferiores a N llega a la otra capa N.

Lo que se debe entender en este ejemplo es la relación entre las comunicaciones virtual y real, y la diferencia entre protocolos e interfaces.

1.3.2 Aspectos de diseño de capas.

Cada capa necesita un mecanismo para identificar a los emisores y a los receptores. Puesto que una red por lo general tiene muchas computadoras, se necesita un método para que un proceso en una máquina especifique con cuál de ellas quiere hablar. Como consecuencia de tener múltiples destinos, se necesita alguna forma de **direccionamiento** a fin de precisar un destino específico.

Reglas de transferencia de datos. En algunos sistemas los datos viajan sólo en una dirección; en otros, pueden viajar en ambas direcciones. El protocolo también debe determinar a cuántos canales lógicos corresponde la conexión y cuáles son sus prioridades (datos normales y urgentes).

El **control de errores** es importante porque los circuitos no son perfectos. Muchos códigos de detección y corrección de errores son conocidos, pero los dos extremos de la conexión deben estar de acuerdo en cuál es el que se va a utilizar y el receptor debe tener algún medio de decirle al emisor qué mensajes fueron recibidos correctamente y con errores.

Los mjes pueden llegar en cualquier orden, el protocolo debe incluir un mecanismo que permita al receptor volver a unir los pedazos en forma adecuada.

Un aspecto que ocurre en cada nivel es cómo evitar que un emisor rápido sature de datos a un receptor lento. Una forma es limitar al emisor a una velocidad de transmisión acordada. Se conoce como **control de flujo**.

Otro problema que se debe resolver en algunos niveles es la incapacidad de todos los procesos de aceptar de manera arbitraria mjes largos. Esta propiedad conduce a mecanismos para desembalar, transmitir y reensamblar mjes. (**Entramar**). Un aspecto relacionado es el problema de qué hacer cuando los procesos insisten en transmitir datos en unidades tan pequeñas que enviarlos por separado es ineficaz. La solución a esto es

reunir en un solo mje grande varios mjes pequeños que tengan un destino común y separar los mjes cuando llegue a su destino.

Cuando es inconveniente o costoso establecer una conexión separada para cada par de procesos de comunicación, la capa subyacente podría decidir utilizar la misma conexión para múltiples conversaciones sin relación entre sí. (**Multiplexión y desmultiplexión**). Cuando hay múltiples rutas entre el origen y el destino, se debe elegir la mejor entre todas ellas. A veces esta decisión se debe dividir en 2 o más capas, dependiendo de la carga de tráfico actual. (**Enrutamiento**).

1.3.3 Servicios orientados a la conexión y no orientados a la conexión.

Las capas pueden ofrecer estos dos tipos de servicios a las capas que están sobre ellas.

El servicio **orientado a la conexión** (basado en el sistema telefónico). En algunos casos, al establecer una conexión, el emisor, el receptor y la subred realizan una negociación sobre los parámetros a utilizar. El usuario del servicio primero establece una conexión, la utiliza y luego la abandona. El aspecto esencial de una conexión es que funciona como un tubo: el emisor empuja objetos en un extremo y el receptor los toma del otro lado. En la mayoría de los casos se mantiene el orden en que se enviaron.

El **servicio no orientado a la conexión** (basado en el sistema postal). cada mensaje lleva completa la dirección de destino y cada una se enruta a través del sistema, independientemente de los demás. Es posible que el primer mensaje enviado no sea el primero en llegar.

Cada servicio se puede clasificar por la calidad del servicio. Los servicios son **confiables** en el sentido que nunca pierden datos. el receptor envía un mje al emisor para confirmar de que llegó. Este sistema de confirmación de recepción introduce sobrecargas y retardos (valiosos pero indeseables).

Para algunas aplicaciones, los retardos debidos a las confirmaciones, son inaceptables como en el tráfico de voz digitalizada.

A veces, todo lo que se necesita es una forma de enviar un mje único que tenga una alta, aunque no garantizada, probabilidad de llegar. Al servicio no orientado a la conexión **no confiable** , sin confirmación de recepción, se le conoce como “*servicio de datagramas*”. En otras situaciones se desea la conveniencia de no tener que establecer una conexión para enviar un mje corto, pero la **confiabilidad** es esencial. Para estas aplicaciones se puede proporcionar el “*servicio de datagramas confirmados*”.

Otro servicio es de “solicitud-respuesta”. El emisor transmite un solo datagrama que contiene una solicitud; a continuación el servidor envía una respuesta.

	Servicio	Ejemplo
Orientado a la conexión	Flujo confiable de mensajes	Secuencia de páginas
	Flujo confiable de bytes	Inicio de sesión remoto
	Conexión no confiable	Voz digitalizada
No orientado a la conexión	Datagrama no confiable	Correo electrónico basura
	Datagrama confirmado	Correo certificado
	Solicitud-respuesta	Consulta de base de datos

Figura 1-16. Seis tipos de servicio diferentes.

Razones por lo que Ethernet no proporciona comunicación confiable, 1. Los paquetes se pueden dañar en el tránsito. 2. Los retardos del servicio confiable podrían ser inaceptables.

1.3.4 Primitivas de servicio.

Un servicio se especifica formalmente como un conjunto de “**primitivas**” (operaciones) disponibles a un proceso de usuario para que acceda al servicio. Estas primitivas le indican al servicio que desempeñe alguna acción o reporte sobre una acción que ha tomado una entidad igual.

El conjunto de primitivas disponible depende de la naturaleza del servicio que se va a proporcionar. Las primitivas de servicio orientado a la conexión son diferentes de las del servicio no orientado a la conexión.

1.3.5 Relación de servicios a protocolos.

Servicios y protocolos son conceptos distintos.

Un **servicio** es un conjunto de primitivas (operaciones) que una capa proporciona a la capa que está sobre ella. El servicio define qué operaciones puede realizar la capa en beneficio de sus usuarios, pero no da información de cómo se implementan tales operaciones. Un servicio está relacionado con la **interfaz** entre 2 capas, donde la capa inferior es la que provee el servicio y la superior la recibe.

El protocolo, es un conjunto de reglas que rigen el formato y el significado de los paquetes, o mjes., que se intercambiaron las entidades iguales en una capa. Las entidades utilizan protocolos para implementar sus definiciones del servicio. Son libres de cambiar sus protocolos cuando lo deseen, siempre y cuando no cambie el servicio visible a sus usuarios. De esta manera, el servicio y el protocolo no dependen uno del otro.

Los servicios se relacionan con las interacciones entre capas, los protocolos se relacionan con los paquetes enviados entre entidades iguales de máquinas diferentes.

1.4 Modelos de referencia.

1.4.1 Modelo de referencia OSI.

El modelo se llama OSI (Interconexión de Sistemas Abiertos) de ISO porque tiene que ver con la conexión de sistemas abiertos, es decir, que están abiertos a la comunicación con otros sistemas.

El modelo OSI tiene 7 capas. Los principios que se aplicaron para ello fueron:

1. Una capa se debe crear donde se necesite una abstracción diferente.
2. Cada capa debe realizar una función bien definida.
3. La función de cada capa se debe elegir con la intención de definir protocolos estandarizados internacionalmente.
4. Los límites de las capas se deben elegir a fin de minimizar el flujo de información a través de las interfaces.
5. La cantidad de capas debe ser suficientemente grande para no tener que agrupar funciones distintas en la misma capa y lo bastante pequeña para que la arquitectura no se vuelva inmanejable.

La capa física. En esta capa se lleva a cabo la transmisión de bits puros a través de un canal de comunicación. Los aspectos de diseño implican asegurarse de que cuando un lado envía un bit 1, éste se reciba en el otro lado como tal.

La capa de enlace de datos. Funciones: -Enlazar-Controlar errores-Controlar Flujos.

La tarea principal de esta capa es transformar un medio de transmisión puro en una línea de comunicación que, al llegar a la capa de red, aparezca libre de errores de transmisión. Logra esa tarea haciendo que el emisor fragmente los datos de entradas en tramas de datos y transmitiéndolas de manera secuencial. (si el servicio es confiable, el receptor confirma la recepción correcta de cada trama.).

Otra cuestión es cómo hacer que un transmisor rápido no sature de datos a un emisor lento. El manejo de errores y el control de flujo están integrados.

Las redes de difusión tienen un aspecto adicional en la capa de enlace de datos: cómo controlar el acceso al canal compartido. una subcapa especial de la capa de enlace se encarga de eso: la subcapa de control de acceso al medio.

La capa de red. Funciones: -Enrutar (paquetes)-(estático, dinámico).

Esta capa controla las operaciones de la subred. Un aspecto clave del diseño es determinar cómo se enrutan los paquetes desde su origen a su destino. Las rutas pueden estar basadas en tablas estáticas (enrutamiento estático) codificadas en la red y que rara vez cambian.

Evitar los cuellos de botella en la subred también es una función de la capa de red aunque puede ser compartida con la capa de transporte. La calidad del servicio (retardo, tiempo de tránsito, inestabilidad, etc.) también corresponde a la capa de red.

Cuando un paquete tiene que viajar de una red a otra puede tener problemas, el enrutamiento de la otra red podría ser diferente, podría no aceptar el paquete porque es demasiado largo, los protocolos podrían ser diferentes, etc. La capa de red tiene que resolver estos problemas.

La capa de transporte. (Segmentos). Funciones: Entramar-Ordena (control de flujo)-Controla errores.

La función de esta capa es aceptar los datos provenientes de las capas superiores, dividirlos en unidades más pequeñas si es necesario, pasar éstas a la capa de red y asegurarse de que todas las piezas lleguen correctamente del otro lado.

Determina qué tipo de servicio proporcionar a la capa de sesión y a los usuarios.

La capa de transporte es una verdadera conexión de extremo a extremo. En otras palabras, un programa en la máquina de origen lleva a cabo una conversación con un programa similar en la máquina destino, usando los encabezados de mje y los mjs de control.

Controla que los paquetes lleguen si la subcapa falla por time out.

La capa de sesión. (no existe)

Sincroniza capas superiores con inferiores (negocia).

Permite que los usuarios de máquinas diferentes establezcan sesiones entre ellos. Las sesiones ofrecen varios servicios, como el control de diálogo (dar seguimiento de a quién le toca transmitir), administración de token (que impide que las dos partes traten de realizar la misma operación crítica al mismo tiempo) y sincronización (la adición de puntos de referencia a transmisiones largas para permitirles continuar desde donde se encontraban después de la caída).

La capa de presentación. Le corresponde la sintaxis y semántica de la información transmitida. A fin de que las computadoras con diferentes representaciones de datos se puedan comunicar.

La capa de aplicación. Contiene protocolos que requieren los usuarios con frecuencia. por ejemplo: HTTP.

1.4.2 El modelo de referencia TCP/IP

Esta arquitectura tuvo como meta, desde sus inicios, la capacidad de conectar múltiples redes, otro objetivo fue que la red pudiera sobrevivir a la pérdida de HW de la subred, sin que las conversaciones existentes se interrumpieran. Se quería que las conexiones se mantuvieran intactas en tanto las máquinas de origen y destino estuvieran funcionando, aunque algunas de las máquinas o líneas de transmisión intermedias quedarán fuera de operación repentinamente.

La capa interred.

Todos los requerimientos condujeron a la elección de una red de conmutación de paquetes basada en una capa de interred no orientada a la conexión. Esta capa es la pieza clave que mantiene unida la arquitectura. Su trabajo es permitir que los hosts inyecten paquetes dentro de cualquier red y que éstos viajen a su destino de manera independiente (podría ser en una red diferente). Tal vez lleguen en un orden diferente al que fueron enviados, en cuyo caso las capas más altas deberán ordenarlos. (analogía: correo)

La capa de interred define un paquete de formato y protocolo oficial llamado IP (protocolo de internet). El trabajo de esta capa es entregar paquetes IP al destinatario. Aquí, el enrutamiento de paquetes es claramente el aspecto principal, con el propósito de evitar la congestión.

La capa de transporte.

Está diseñada para permitir que las entidades iguales en los hosts de origen y destino pueden llevar a cabo una conversación.(transporte-OSI). Aquí se han definido 2 protocolos de transporte de extremo a extremo. El primero, TCP (protocolo de control de transmisión), es un protocolo confiable, orientada a la conexión, que permite que un flujo de bytes que se origina en una máquina se entregue sin errores en cualquier otra máquina en la interred. TCP también maneja el control de flujo para asegurarse de que un emisor rápido no sature a un receptor lento.

El segundo protocolo de esta capa, UDP (Protocolo de Datagrama de Usuario), es un protocolo no confiable y no orientado a la conexión para aplicaciones que no desean la secuenciación o el control de flujo de TCP y que desean proporcionar el suyo. La relación IP, TCP y UDP se muestra en la Fig. 1-22.

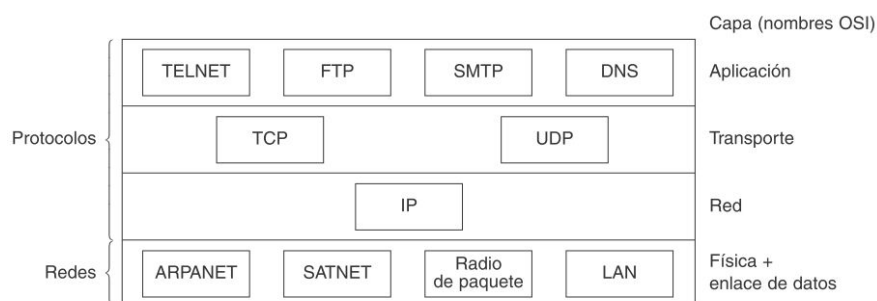


Figura 1-22. Protocolos y redes en el modelo TCP/IP inicialmente.

La capa de aplicación. El modelo TCP/IP no tiene capas de sesión ni de presentación.

Arriba de la capa de transporte está la capa de aplicación. Contiene todos los protocolos de nivel más alto.

La capa host a red. Debajo de la capa de interred hay un gran vacío. El modelo TCP/IP en realidad no dice mucho acerca de lo que pasa aquí, excepto que puntualiza que el host se tiene que conectar a la red mediante el mismo protocolo para que le puedan enviar paquetes IP. Este protocolo no está definido y varía de un host a otro y de una red a otra.

1.4.3 Comparación entre los modelos de referencia OSI y TCP/IP

Los 2 se basan en el concepto de una pila de protocolos independientes. Asimismo, la funcionalidad de las capas es muy parecida.

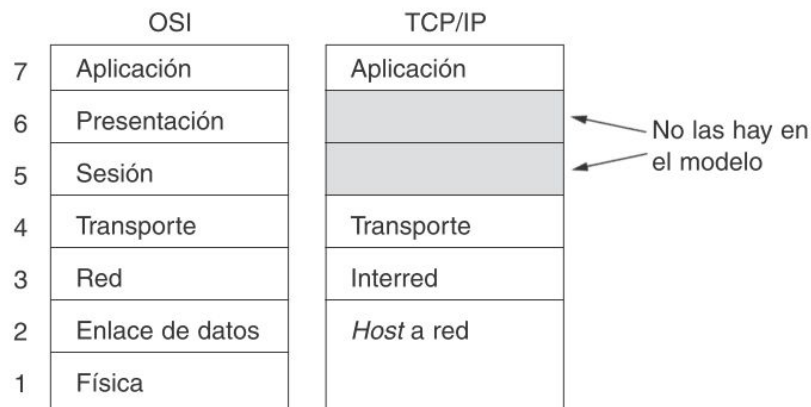


Figura 1-21. El modelo de referencia TCP/IP.

Pero a pesar de estas similitudes fundamentales, los 2 modelos también tienen muchas diferencias. Es importante tener en cuenta que estamos comparando los modelos de referencia, no las pilas de protocolos correspondientes.

Tres conceptos son básicos para el modelo OSI:

1-Servicios.

2-Interfaces.

3-Protocolos.

Probablemente la contribución más grande del modelo OSI es que hace explícita la distinción entre estos 3 conceptos. Cada capa desempeña algunos servicios para la capa que está arriba de ella. La definición de servicio indica qué hace la capa, no la forma en que la entidad superior tiene acceso a ella, o cómo funciona dicha capa. Define el aspecto semántico de la capa.

La interfaz de una capa indica a los procesos que están sobre ella cómo accederla. Especifica cuáles son los parámetros y qué resultados se esperan.

Por último, una capa es quien debe decidir qué protocolos de iguales utilizar. Puede utilizar cualquier protocolo que desee, en tanto consiga que se haga el trabajo.

Originalmente, el modelo TCP/IP no distinguía entre servicios, interfaz y protocolo, aunque las personas han tratado de readaptarlo con el propósito de hacerlo más parecido al OSI.

Como consecuencia, los protocolos del modelo OSI están mejor ocultos que los del modelo TCP/IP y se pueden reemplazar fácilmente conforme cambia la tecnología. La facilidad de realizar tales cambios es uno de los objetivos principales de tener protocolos en capas.

Una **diferencia** patente entre los 2 modelos es el nro de capas: el modelo OSI tiene 7 y el TCP/IP sólo 4. Los 2 tienen capas de (inter)red, transporte y aplicación, pero las otras capas son diferentes.

Otra diferencia está en el área de la comunicación orientada a la conexión comparada con la no orientada a la conexión. El modelo OSI soporta ambas comunicaciones en la capa de red, pero sólo la comunicación orientada a la conexión en la capa de transporte, donde es importante. El modelo TCP/IP sólo tiene un modo en la capa de red (no orientado a la conexión) pero soporta ambos modos en la capa de transporte, lo que da a los usuarios la oportunidad de elegir.

1.4.4 Crítica al modelo OSI y los protocolos.

- 1-Aparición inoportuna.
- 2-Mala tecnología.
- 3-Malas implementaciones.
- 4-Malas políticas.

1.4.5 Crítica del modelo TCP/IP

- 1-No distingue claramente los conceptos de servicio, interfaz y protocolo.
- 2-El modelo no es general del todo y no está bien ajustado para describir ninguna pila de protocolos más que el TCP/IP.
- 3-La capa host a red no es en realidad una capa del todo en el sentido normal del término, como se utiliza en el contexto de los protocolos de capas. Es una interfaz (entre la capa de red y la capa de enlace de datos).
- 4-El modelo no distingue (ni menciona) las capas físicas y de enlace de datos. Son completamente diferentes. La capa física tiene que ver con las características de transmisión de comunicación por cable de cobre, por fibra óptica o inalámbrica. El trabajo de la capa de enlace de datos es delimitar el inicio y fin de las tramas y captarlas de uno a otro lado con el grado deseado de confiabilidad. Un modelo adecuado debería incluir ambas como capas separadas, el modelo TCP/IP no hace esto.
- 5-Aunque los protocolos IP y TCP se idearon e implementaron con sumo cuidado, muchos de los demás protocolos fueron hechos con fines específicos.