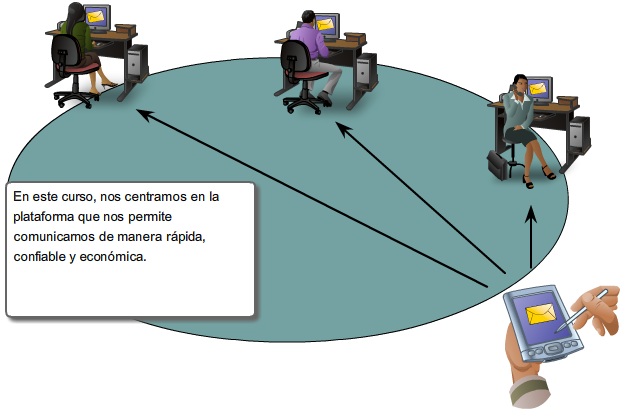
## a capa de Sesión en varias Redes

|  |
| --- |
| Capa de Sesión en ARPANET ARPANET no tiene una capa de sesión o algo que se le parezca; sino mas bien depende de las aplicaciones individuales al manejo de sus sesiones, siempre que sea necesario. Por otro lado, se ha trabajado mucho sobre RPC(caso especial de comunicación asíncrona, el emisor envía una petición de servicio al receptor y espera la respuesta) dentro de la comunidad de conexión de redes ARPA, especialmente en Xerox PARC y en la Universidad de Carnegie-Mellon. Capa de Sesión en MAP y TOP MAP y TOP utilizan una forma restringida de la capa de sesión del modelo OSI. El establecimiento de sesión, la transferencia de datos y la liberación de sesión están totalmente soportados para el modo dúplex; mientras que el modo semidúplex no está soportado. El servicio de sincronización, la administración de actividades, la notificación de excepciones, los datos tipados y el servicio de datos de capacidad no son requeridos. Este subconjunto corresponde a grandes rasgos al desaparecido subconjunto básico sincronizado, con la omisión del modo semidúplex y datos tipados. Los protocolos de sesión MAP y TOP son subconjuntos de los protocolos completos de sesión del modelo OSI. Aquellas SPDU necesarias para realizar el subconjunto MAP y TOP deberán ser realizadas. Las demás son opcionales. Capa de Sesión en USENET Al igual que en ARPANET, USENET no cuenta con una capa de sesión. A diferencia de ARPANET, no es ni siquiera posible, para las capas superiores, realizar por sí mismas los servicios de sesión. Ninguno de los servicios de sesión se necesitan en absoluto |

**INTRODUCCION DEL CAPITULO**

**‍2.0.1 Introducción**

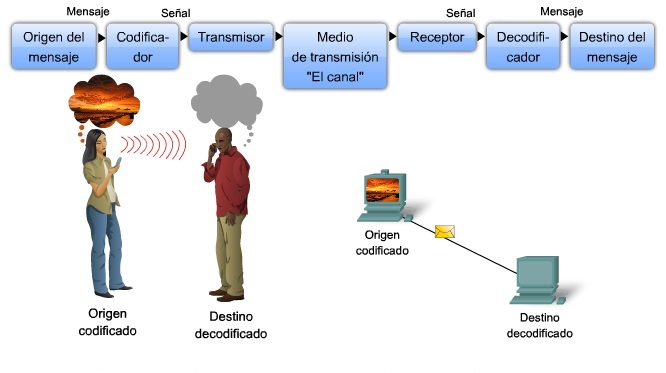
Las redes nos conectan cada vez más. Las personas se comunican en línea desde cualquier lugar. La tecnología confiable y eficiente permite que las redes estén disponibles cuando y donde las necesitemos. A medida que la red humana sigue creciendo, la plataforma que la conecta y le da soporte también debe hacerlo.  
  
La industria de la red, como un todo, ha creado los medios para analizar la plataforma existente y para mejorarla de forma progresiva, en lugar de desarrollar sistemas únicos e independientes para la entrega de cada servicio nuevo. Esto asegura que las comunicaciones existentes se mantengan, mientras se introducen los servicios nuevos, los cuales son económicos y tecnológicamente sólidos.  
  
En este curso, nso enfocamos en estos aspectos de la red de información:  
Dispositivos que forman la red  
Medios que conectan los dispositivos  
Mensajes que se transmiten a través de la red  
Reglas y procesos que rigen las comunicaciones de la red  
Herramientas y comandos para construir y mantener las redes  
  
Algo importante para el estudio de redes es el uso de modelos generalmente aceptados que describan las funciones de la red. Estos modelos proporcionan un esquema para entender las redes actuales y para facilitar el desarrollo de nuevas tecnologías para dar apoyo a las necesidades de comunicación a futuro.  
  
En este curso, utilizamos estos modelos, así como las herramientas diseñadas para analizar y simular la funcionalidad de la red. Dos de las herramientas que le permitirán crear e interactuar con redes simuladas son el software Packet Tracer y el analizador de protocolos de red Wireshark.  
  
Este capítulo lo prepara para:  
Describir la estructura de una red, incluso los dispositivos y los medios necesarios para que las comunicaciones sean exitosas.  
Explicar la función de los protocolos en las comunicaciones de red.  
Explicar las ventajas del uso de un modelo en capas para describir la funcionalidad de la red.  
Describir la función de cada capa en dos modelos de red reconocidos: El modelo TCP/IP y el modelo OSI.  
Describir la importancia de direccionar y nombrar esquemas en las comunicaciones de red.  
=



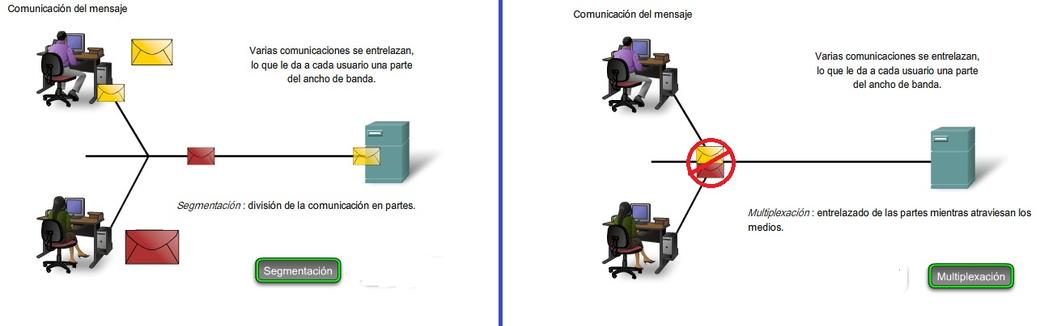
**‍2.1 PLATAFORMA PARA LAS COMUNICACIONES=**

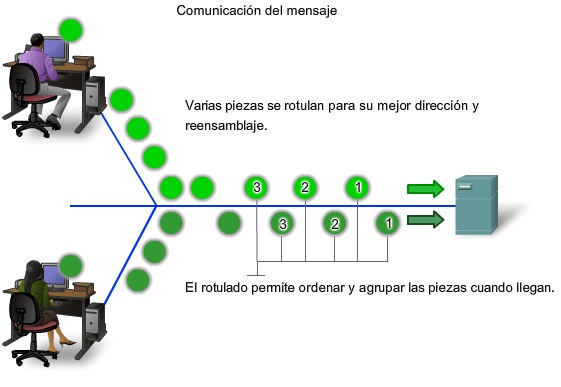
**‍2.1.1 Elementos de la comunicación**

La comunicación comienza con un mensaje o información que se debe enviar de una persona o dispositivo a otro. Las personas intercambian ideas mediante diversos métodos de comunicación. Todos estos métodos tienen tres elementos en común. El primero de estos elementos es el origen del mensaje, o emisor. Los orígenes de los mensajes son las personas o los dispositivos electrónicos que deben enviar un mensaje a otras personas o dispositivos. El segundo elemento de la comunicación es el destino o receptor del mensaje. El destino recibe el mensaje y lo interpreta. Un tercer elemento, llamado canal, está formado por los medios que proporcionan el camino por el que el mensaje viaja desde el origen hasta el destino.  
  
Considere, por ejemplo, que desea comunicar mediante palabras, ilustraciones y sonidos. Cada uno de estos mensajes puede enviarse a través de una red de datos o de información convirtiéndolos primero en dígitos binarios o bits. Luego, estos bits se codifican en una señal que se puede transmitir por el medio apropiado. En las redes computacionales, el medio es generalmente un tipo de cable o transmisión inalámbrica.  
  
El término red en este curso se refiere a las redes de datos o información capaces de transmitir muchos tipos diferentes de comunicaciones, incluyendo datos computacionales tradicionales, voz interactiva, video y productos de entretenimiento.



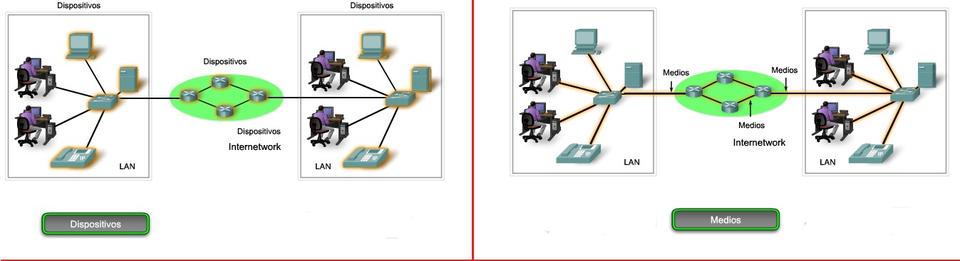
**‍2.1.2 Comunicación de mensajes**

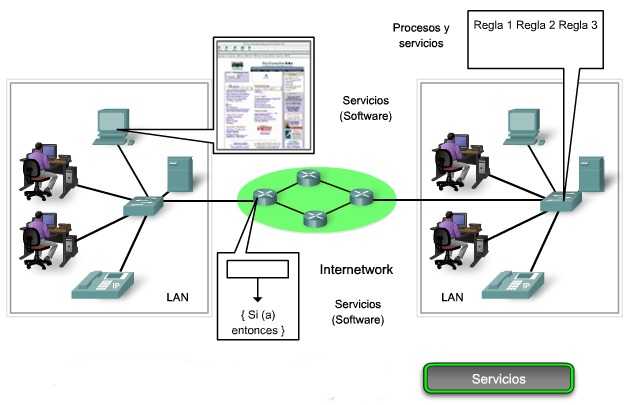
En teoría, una comunicación simple, como un video musical o un correo electrónico puede enviarse a través de la red desde un origen hacia un destino como un stream de bits masivo y continuo. Si en realidad los mensajes se transmitieron de esta manera, significará que ningún otro dispositivo podrá enviar o recibir mensajes en la misma red mientras esta transferencia de datos está en progreso. Estos grandes streams de datos originarán retrasos importantes. Además, si falla un enlace en la infraestructura de la red interconectada durante la transmisión, el mensaje completo se perdería y tendría que retransmitirse completamente.  
  
Un método mejor es dividir los datos en partes más pequeñas y manejables para enviarlas por la red. La división del stream de datos en partes más pequeñas se denomina segmentación. La segmentación de mensajes tiene dos beneficios principales.  
  
Primero, al enviar partes individuales más pequeñas del origen al destino, se pueden intercalar diversas conversaciones en la red. El proceso que se utiliza para intercalar las piezas de conversaciones separadas en la red se denomina multiplexación.  
  
Segundo, la segmentación puede aumentar la confiabilidad de las comunicaciones de red. No es necesario que las partes separadas de cada mensaje sigan el mismo recorrido a través de la red desde el origen hasta el destino. Si una ruta en particular se satura con el tráfico de datos, o falla, las partes individuales del mensaje aún pueden direccionarse hacia el destino mediante los recorridos alternativos. Si parte del mensaje no logra llegar al destino, sólo se deben retransmitir las partes faltantes.  
  
La desventaja de utilizar segmentación y multiplexación para transmitir mensajes a través de la red es el nivel de complejidad que se agrega al proceso. Supongamos que tuviera que enviar una carta de 100 páginas, pero en cada sobre sólo cabe una. El proceso de escribir la dirección, etiquetar, enviar, recibir y abrir los cien sobres requerirá mucho tiempo tanto para el remitente como para el destinatario.  
  
En las comunicaciones de red, cada segmento del mensaje debe seguir un proceso similar para asegurar que llegue al destino correcto y que puede volverse a ensamblar en el contenido del mensaje original.  
  
Varios tipos de dispositivos en toda la red participan para asegurar que las partes del mensaje lleguen a los destinos de manera confiable.



**‍2.1.3 Componentes de la red**

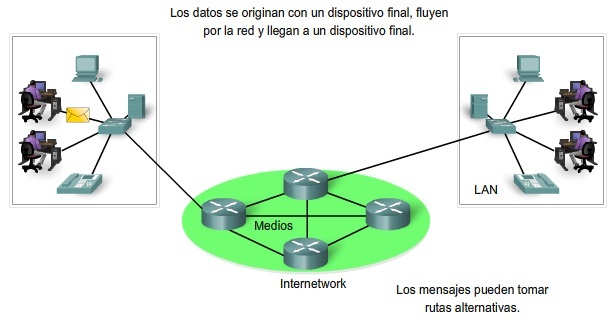
La ruta que toma un mensaje desde el origen hasta el destino puede ser tan sencilla como un solo cable que conecta una computadora con otra o tan compleja como una red que literalmente abarca el mundo. Esta infraestructura de red es la plataforma que respalda la red humana. Proporciona el canal estable y confiable por el cual se producen las comunicaciones.  
  
Los dispositivos y los medios son los elementos físicos o hardware de la red. El hardware es generalmente el componente visible de la plataforma de red, como una computadora portátil o personal, un switch, o el cableado que se usa para conectar estos dispositivos. A veces, puede que algunos componentes no sean visibles. En el caso de los medios inalámbricos, los mensajes se transmiten a través del aire mediante radio frecuencias invisibles u ondas infrarojas.  
  
Los servicios y procesos son los programas de comunicación, llamados software, que se ejecutan en los dispositivos conectados a la red. Un servicio de red proporciona información en respuesta a una solicitud. Los servicios incluyen una gran cantidad de aplicaciones de red comunes que utilizan las personas a diario, como los servicios de correo electrónico hosting y los servicios de Web hosting. Los procesos proporcionan la funcionalidad que direcciona y traslada mensajes a través de la red. Los procesos son menos obvios para nosotros, pero son críticos para el funcionamiento de las redes.





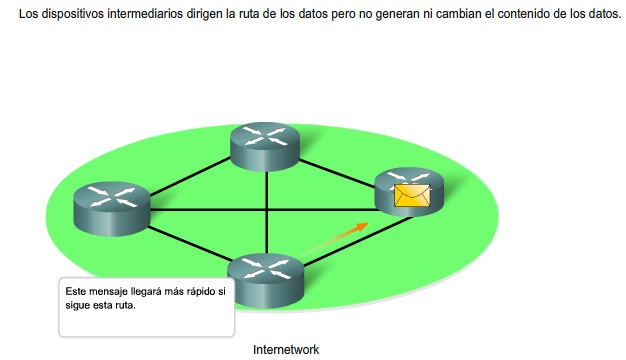
**‍2.1.4 Dispositivos finales y su función en la red**

Los dispositivos de red con los que la gente está más familiarizada se denominan dispositivos finales. Estos dispositivos constituyen la interfaz entre la red humana y la red de comunicación subyacente. Algunos ejemplos de dispositivos finales son:  
Computadoras (estaciones de trabajo, computadoras portátiles, servidores de archivos, servidores web)  
Impresoras de red  
Teléfonos VoIP  
Cámaras de seguridad  
Dispositivos portátiles móviles (tal como los escáner inalámbricos para códigos de barras y los PDA)  
  
En el contexto de una red, se hace referencia a los dispositivos finales como hosts. Un dispositivo host puede ser el origen o el destino de un mensaje transmitido a través de la red. Para distinguir un host de otro, cada host en la red se identifica por una dirección. Cuando un host inicia la comunicación, utiliza la dirección del host de destino para especificar a dónde se debe enviar el mensaje.  
  
En las redes modernas, un hosts pueden actuar como un cliente, un servidor o ambos. El software instalado en el host determina qué función tiene en la red.  
  
Los servidores son hosts con software instalado que les permite proporcionar información y servicios, por ejemplo correo electrónico o páginas Web, a otros hosts de la red.  
  
Los clientes son hosts que tienen instalado un software que les permite solicitar información al servidor y mostrar la información obtenida.



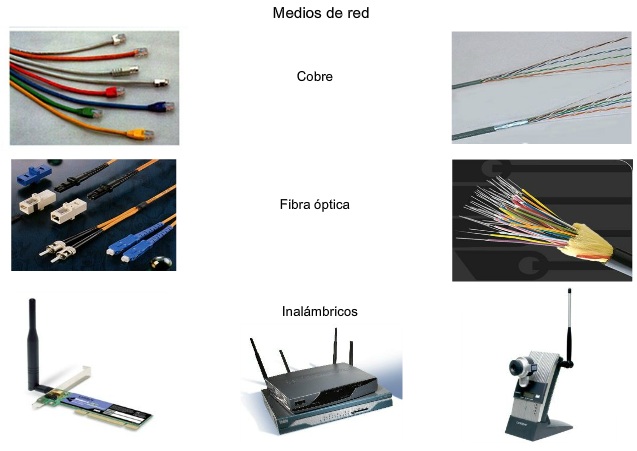
**‍2.1.5 Dispositivos intermediarios y su función en la red**

Además de los dispositivos finales con los cuales la gente está familiarizada, las redes dependen de dispositivos intermediarios para proporcionar conectividad y para trabajar detrás del escenario y garantizar que los datos fluyan a través de la red. Estos dispositivos conectan los hosts individuales a la red y pueden conectar varias redes individuales para formar una internetwork. Los siguientes son ejemplos de dispositivos de red intermediarios:  
Dispositivos de acceso a la red (hubs, switches y puntos de acceso inalámbrico)  
Dispositivos de internetwork (routers)  
Servidores y módems de comunicación  
Dispositivos de seguridad (firewalls)  
  
La administración de datos, así como fluye en la red, es también una función de los dispositivos intermediarios. Estos dispositivos utilizan la dirección host de destino, conjuntamente con información sobre las interconexiones de la red, para determinar la ruta que deben tomar los mensajes a través de la red. Los procesos que se ejecutan en los dispositivos de red intermediarios realizan las siguientes funciones:  
Volver a generar y transmitir las señales de datos  
Conservar información acerca de las rutas que existen a través de la red y de internetwork  
Notificar a otros dispositivos los errores y las fallas de comunicación  
Dirigir los datos a lo largo de rutas alternativas cuando hay una falla en el enlace  
Clasificar y dirigir mensajes de acuerdo a las prioridades de QoS  
Permitir o denegar el flujo de datos de acuerdo a los parámetros de seguridad



**‍2.1.6 Medios de red**

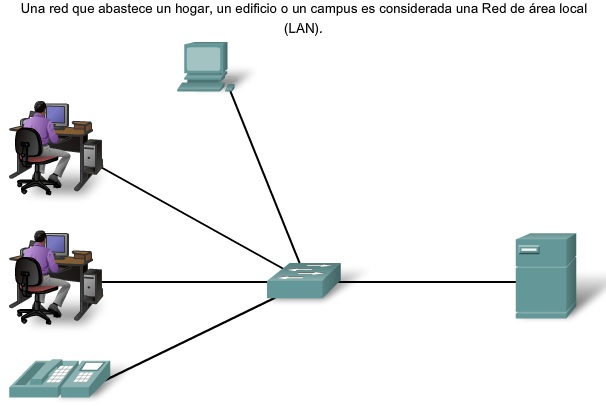
La comunicación a través de una red se transporta por un medio. El medio proporciona el canal por el cual viaja el mensaje desde el origen hasta el destino.  
  
Las redes modernas utilizan principalmente tres tipos de medios para interconectar los dispositivos y proporcionar la ruta por la cual pueden transmitirse los datos. Estos medios son:  
Hilos metálicos dentro de cables  
Fibras de vidrio o plástico (cable de fibra óptica)  
Transmisión inalámbrica  
  
La codificación de la señal que se debe realizar para que se transmita el mensaje es diferente para cada tipo de medio. En los hilos metálicos, los datos se codifican dentro de impulsos eléctricos que coinciden con patrones específicos. Las transmisiones por fibra óptica dependen de pulsos de luz, dentro de intervalos de luz visible o infrarroja. En las transmisiones inalámbricas, los patrones de ondas electromagnéticas muestran los distintos valores de bits.  
  
Los diferentes tipos de medios de red tienen diferentes características y beneficios. No todos los medios de red tienen las mismas características ni son adecuados para el mismo fin. Los criterios para elegir un medio de red son:  
La distancia en la cual el medio puede transportar exitosamente una señal.  
El ambiente en el cual se instalará el medio.  
La cantidad de datos y la velocidad a la que se deben transmitir.  
El costo del medio y de la instalación.



**‍2.2 LAN, WAN E INTERNETWORKS**

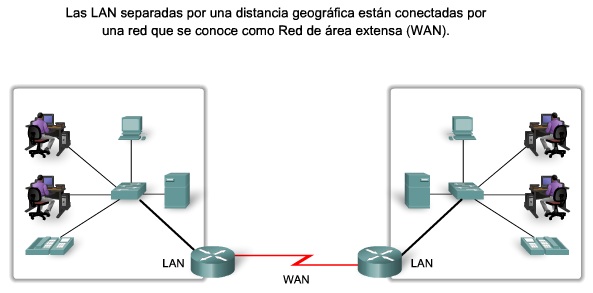
**‍2.2.1 Redes de Area Local**

Las infraestructuras de red pueden variar en gran medida en términos de:  
El tamaño del área cubierta  
El número de usuarios conectados  
El número y los tipos de servicios disponibles  
  
Una red individual generalmente cubre una única área geográfica y proporciona servicios y aplicaciones a personas dentro de una estructura organizacional común, como una empresa, un campus o una región. Este tipo de red se denomina Red de área local (LAN). Una LAN por lo general está administrada por una organización única. El control administrativo que rige las políticas de seguridad y control de acceso está implementado en el nivel de red.



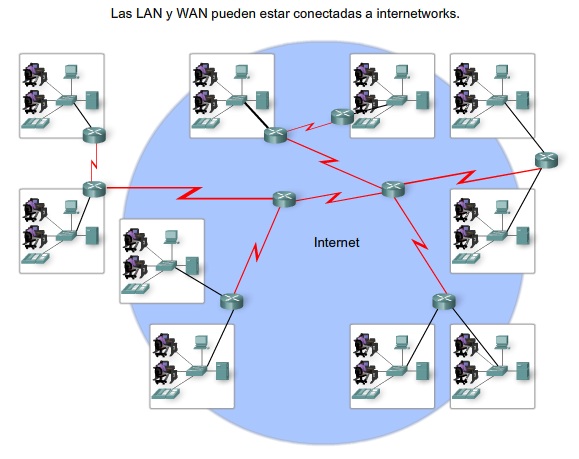
**‍2.2.2 Redes de área amplia**

Cuando una compañía o una organización tiene ubicaciones separadas por grandes distancias geográficas, es posible que deba utilizar un proveedor de servicio de telecomunicaciones (TSP) para interconectar las LAN en las distintas ubicaciones. Los proveedores de servicios de telecomunicaciones operan grandes redes regionales que pueden abarcar largas distancias. Tradicionalmente, los TSP transportaban las comunicaciones de voz y de datos en redes separadas. Cada vez más, estos proveedores ofrecen a sus suscriptores servicios de red convergentes de información.  
  
Por lo general, las organizaciones individuales alquilan las conexiones a través de una red de proveedores de servicios de telecomunicaciones. Estas redes que conectan las LAN en ubicaciones separadas geográficamente se conocen como Redes de área amplia (WAN). Aunque la organización mantiene todas las políticas y la administración de las LAN en ambos extremos de la conexión, las políticas dentro de la red del proveedor del servicio de comunicaciones las controlada el TSP.  
  
Las WAN utilizan dispositivos de red diseñados específicamente para realizar las interconexiones entre las LAN. Dada la importancia de estos dispositivos para la red, la configuración, la instalación y el mantenimiento de los mismos son aptitudes complementarias de la función de la red de una organización.  
  
Las LAN y las WAN son muy útiles para las organizaciones individuales. Conectan a los usuarios dentro de la organización. Permiten gran cantidad de formas de comunicación que incluyen intercambio de correos electrónicos, capacitación corporativa y acceso a recursos.



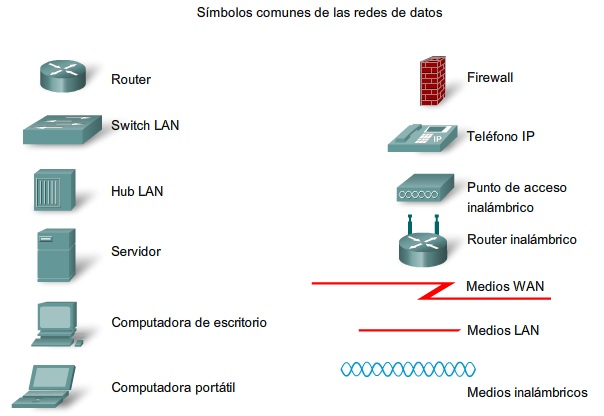
**‍2.2.3 Internet: Una red de redes**

Aunque existen beneficios por el uso de una LAN o WAN, la mayoría de los usuarios necesitan comunicarse con un recurso en otra red, fuera de la organización local.  
  
Los ejemplos de este tipo de comunicación incluyen:  
Envío de un correo electrónico a un amigo que se encuentra en otro país  
Acceso a noticias o productos en un sitio Web  
Recepción de un archivo desde la computadora de un vecino  
Mensajería instantánea con un familiar en otra ciudad  
Ver el juego de su equipo favorito en un celular  
  
Internetwork  
  
Una malla mundial de redes interconectadas (internetworks) que cumple estas necesidades de comunicación humana. Algunas de estas redes interconectadas pertenecen a grandes organizaciones públicas o privadas, como agencias gubernamentales o empresas industriales, y están reservadas para su uso exclusivo. La internetwork accesible al público en general más conocida y ampliamente utilizada es Internet.  
  
Internet se crea por la interconexión de redes que pertenecen a los Proveedores de servicios de Internet (ISP). Estas redes ISP se conectan entre sí para proporcionar acceso a millones de usuarios en todo el mundo. Garantizar una comunicación efectiva en esta infraestructura heterogénea requiere la aplicación de protocolos y tecnologías uniformes, y comúnmente reconocidas, así como también la cooperación de muchas agencias de administración de red.  
  
Intranet  
  
El término intranet con frecuencia se utiliza para hacer referencia a una conexión privada de LAN y WAN que pertenece a una organización y está diseñada para que accedan a ella sólo los miembros y los empleados de la organización u otras personas autorizadas.  
  
Nota: Es posible que los siguientes términos sean sinónimos: internetwork, red de datos y red. Una conexión de dos o más redes de datos forma una internetwork: una red de redes. También es habitual referirse a una internetwork como una red de datos, o simplemente como una red, cuando se consideran las comunicaciones a alto nivel. El uso de los términos depende del contexto en el momento, a veces los términos se pueden intercambiar.



**‍2.2.4 Representaciones de red**

Cuando se transporta información compleja como la conectividad de red y el funcionamiento de una gran internetwork, es muy útil el uso de representaciones visuales y gráficos. Como cualquier otro idioma, el lenguaje de interconexión de redes utiliza un grupo común de símbolos para representar los distintos dispositivos finales, los dispositivos de red y los medios. La capacidad de reconocer las representaciones lógicas de los componentes físicos de networking es fundamental para poder visualizar la organización y el funcionamiento de una red. A lo largo de este curso y de estos laboratorios, aprenderá cómo operan estos dispositivos y cómo realizar tareas de configuración básica en los mismos.  
  
Además de estas representaciones, se utiliza terminología especializada al hablar sobre cómo se conectan estos dispositivos y los medios unos a otros. Algunos términos importantes para recordar son:  
  
Tarjeta de interfaz de red (NIC): una NIC, o adaptador de LAN, proporciona la conexión física a la red en la computadora personal u otro dispositivo host. Los medios que realizan la conexión de la PC al dispositivo de networking se conectan en la NIC.  
  
Puerto físico: un conector o conexión en un dispositivo de networking donde se conectan los medios a un host u otro dispositivo de networking.  
  
Interfaz: puertos especializados en un dispositivo de internetworking que se conecta a redes individuales. Puesto que los routers se utilizan para interconectar redes, los puertos de un router se conocen como interfaces de red.

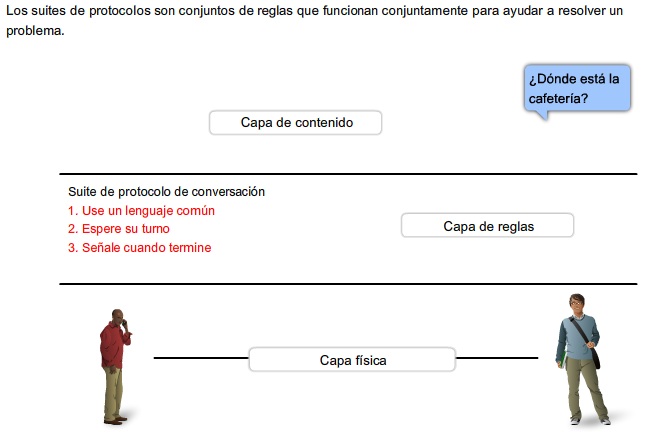


Actividad 2.2.4

**‍2.3 PROTOCOLOS**

**‍2.3.1 Reglas que rigen las comunicaciones**

Toda comunicación, ya sea cara a cara o por una red, está regida por reglas predeterminadas que se denominan protocolos. Estos protocolos son específicos de las características de la conversación. En nuestra comunicación personal diaria, las reglas que utilizamos para comunicarnos por un medio, como una llamada telefónica, no son necesariamente las mismas que los protocolos para utilizar otro medio, como enviar una carta.  
  
Piense cuántas reglas o protocolos diferentes rigen todos los métodos de comunicación que existen actualmente en el mundo.  
  
La comunicación exitosa entre los hosts de una red requiere la interacción de gran cantidad de protocolos diferentes. Un grupo de protocolos interrelacionados que son necesarios para realizar una función de comunicación se denomina suite de protocolos. Estos protocolos se implementan en el software y el hardware que está cargado en cada host y dispositivo de red.  
  
Una de las mejores formas de ver cómo interactúan los protocolos en un host particular es verlo como un stack. Un stack de protocolos muestra cómo se implementan los protocolos individuales de una suite en el host. Los protocolos se muestran como una jerarquía en capas, donde cada servicio de nivel superior depende de la funcionalidad definida por los protocolos que se muestran en los niveles inferiores. Las capas inferiores del stack se encargan del movimiento de datos por la red y proporcionan servicios a las capas superiores, las cuales se enfocan en el contenido del mensaje que se va a enviar y en la interfaz del usuario.  
  
Uso de capas para describir la comunicación cara a cara  
  
Por ejemplo, considere a dos personas que se comunican cara a cara. Como muestra la figura, se pueden utilizar tres capas para describir esta actividad. En la capa inferior, la capa física, puede haber dos personas, cada una con una voz que puede pronunciar palabras en voz alta. En la segunda capa, la capa de las reglas, existe un acuerdo para hablar en un lenguaje común. En la capa superior, la capa de contenido, tenemos las palabras que se hablan: el contenido de la comunicación.  
  
Si fueramos testigos de esta conversación, realmente no veríamos las "capas" flotando en el lugar. Es importante entender que el uso de capas es un modelo y, como tal, proporciona una vía para fraccionar convenientemente en partes una tarea compleja y describir cómo funciona.



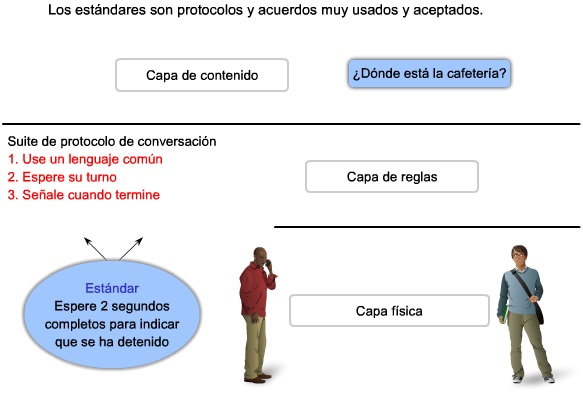
**‍2.3.2 Protocolos de red**

A nivel humano, algunas reglas de comunicación son formales y otras simplemente se entienden, o están implícitas, de acuerdo a los usos y costumbres. Para que los dispositivos se puedan comunicar en forma exitosa, un nuevo conjunto de aplicaciones de protocolos debe describir los requerimientos e interacciones precisos.  
  
Las suites de protocolos de networking describen procesos como los siguientes:  
El formato o la estructura del mensaje  
El método por el cual los dispositivos de networking comparten información sobre las rutas con otras redes  
Cómo y cuándo se transmiten mensajes de error y del sistema entre los dispositivos  
La configuración y la terminación de sesiones de transferencia de datos  
  
Los protocolos individuales en una suite de protocolos puede ser específica para el vendedor y exclusiva. Exclusiva, en este contexto, significa que una compañía o proveedor controla la definición del protocolo y cómo funciona. Algunos protocolos exclusivos los pueden utilizar distintas organizaciones con permiso del propietario. Otros, sólo se pueden implementar en equipos fabricados por el proveedor exclusivo.

|  |  |
| --- | --- |
| 15._El_rol_de_los_protocolos.jpg | 16._El_rol_de_los_protocolos.jpg |
|  |  |
| 17._El_rol_de_los_protocolos.jpg | 18._El_rol_de_los_protocolos.jpg |

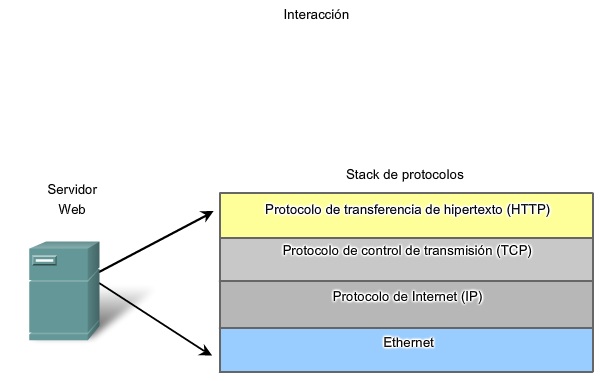
**‍2.3.3 Suites de protocolos y estándares de la industria**

Con frecuencia, muchos de los protocolos que comprenden una suite hacen referencia a otros protocolos ampliamente utilizados o a estándares de la industria. Un estándar es un proceso o protocolo que ha sido avalado por la industria de networking y ratificado por una organización de estándares, como el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE, Institute of Electrical and Electronics Engineers) o el Grupo de trabajo de ingeniería de Internet (IETF).  
  
El uso de estándares en el desarrollo e implementación de protocolos asegura que los productos de diferentes fabricantes puedan funcionar conjuntamente para lograr comunicaciones eficientes. Si un fabricante en particular no observa un protocolo estrictamente, es posible que sus equipos o software no puedan comunicarse satisfactoriamente con productos hechos por otros fabricantes.  
  
En las comunicaciones de datos, por ejemplo, si un extremo de una conversación utiliza un protocolo para regir una comunicación unidireccional y el otro extremo adopta un protocolo que describe una comunicación bidireccional, es muy probable que no pueda intercambiarse ninguna información.



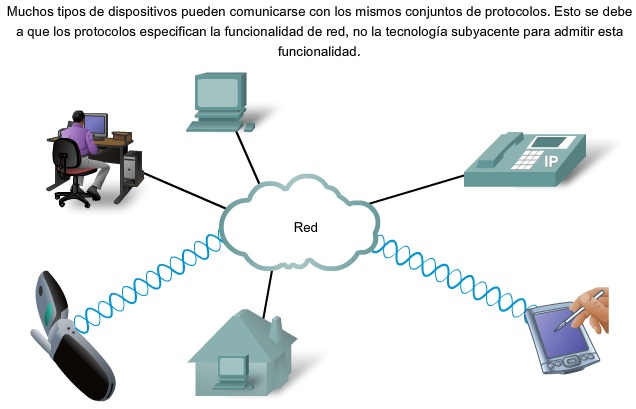
**‍2.3.4 Interacción de los protocolos**

Un ejemplo del uso de una suite de protocolos en comunicaciones de red es la interacción entre un servidor Web y un explorador Web. Esta interacción utiliza una cantidad de protocolos y estándares en el proceso de intercambio de información entre ellos. Los distintos protocolos trabajan en conjunto para asegurar que ambas partes reciben y entienden los mensajes. Algunos ejemplos de estos protocolos son:  
  
Protocolo de aplicación:  
  
El Protocolo de transferencia de hipertexto (HTTP) es un protocolo común que rige la forma en que interactúan un servidor Web y un cliente Web. HTTP define el contenido y el formato de las solicitudes y respuestas intercambiadas entre el cliente y el servidor. Tanto el cliente como el software del servidor Web implementan el HTTP como parte de la aplicación. HTTP se basa en otros protocolos para regular la forma en que se transportan los mensajes entre el cliente y el servidor.  
  
Protocolo de transporte:  
  
El Protocolo de control de transmisión (TCP) es el protocolo de transporte que administra las conversaciones individuales entre servidores Web y clientes Web. TCP divide los mensajes HTTP en pequeñas partes, denominadas segmentos, para enviarlas al cliente de destino. También es responsable de controlar el tamaño y los intervalos a los que se intercambian los mensajes entre el servidor y el cliente.  
  
Protocolo de internetwork:  
  
El protocolo de internetwork más común es el Protocolo de Internet (IP). El IP es responsable de tomar los segmentos formateados del TCP, encapsularlos en paquetes, asignar las direcciones apropiadas y seleccionar la mejor ruta al host de destino.  
  
Protocolos de acceso a la red:  
  
Los protocolos de acceso a la red describen dos funciones principales, la administración de enlace de datos y la transmisión física de datos en los medios. Los protocolos de administración de enlace de datos toman los paquetes IP y los formatean para transmitirlos por los medios. Los estándares y protocolos de los medios físicos rigen de qué manera se envían las señales por los medios y cómo las interpretan los clientes que las reciben. Los transceptores de las tarjetas de interfaz de red implementan los estándares apropiados para los medios que se utilizan.



**‍2.3.5 Protocolos independientes de la tecnología**

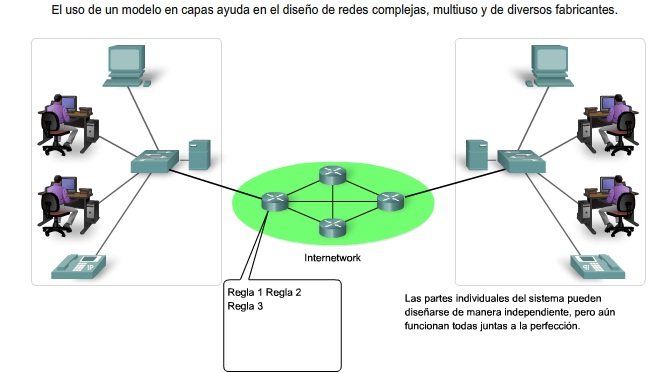
Los protocolos de red describen las funciones que se producen durante las comunicaciones de red. En el ejemplo de la conversación cara a cara, es posible que un protocolo para comunicar establezca que para indicar que la conversación ha finalizado, el emisor debe permanecer en silencio durante dos segundos completos. Sin embargo, este protocolo no especifica cómo debe permanecer en silencio el emisor durante los dos segundos.  
  
Los protocolos generalmente no describen cómo lograr una función en particular. Al describir solamente qué funciones se requieren de una regla de comunicación en particular pero no cómo realizarlas, es posible que la implementación de un protocolo en particular sea independiente de la tecnología.  
  
En el ejemplo del servidor Web, HTTP no especifica qué lenguaje de programación se utiliza para crear el explorador, qué software de servidor Web se debe utilizar para servir las páginas Web, sobre qué sistema operativo se ejecuta el software o los requisitos necesarios para mostrar el explorador. Tampoco describe cómo debe detectar errores el servidor, aunque sí describe lo que debe hacer si ocurre algún error.  
  
Esto significa que una computadora y otros dispositivos como teléfonos móviles o PDA pueden acceder a una página Web almacenada en cualquier tipo de servidor Web que utilice cualquier forma de sistema operativo de cualquier lugar de Internet.



**‍2.4 USO DE MODELOS EN CAPAS**

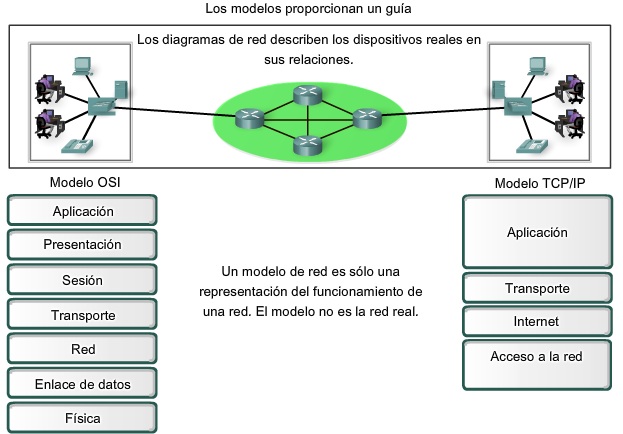
**‍2.4.1 Beneficios del uso de modelos en capas.**

Para visualizar la interacción entre varios protocolos, es común utilizar un modelo en capas. Este modelo describe el funcionamiento de los protocolos que se produce en cada capa y la interacción con las capas que se encuentran por encima y por debajo de ellas.  
  
Hay beneficios por el uso de un modelo en capas para describir protocolos de red y operaciones. Uso de un modelo en capas:  
Ayuda en el diseño de protocolos, ya que los protocolos que operan en una capa específica tienen información definida según la cual actúan, y una interfaz definida para las capas superiores e inferiores.  
Fomenta la competencia, ya que los productos de distintos proveedores pueden trabajar en conjunto.  
Evita que los cambios en la tecnología o en las capacidades de una capa afecten otras capas superiores e inferiores.  
Proporciona un lenguaje común para describir las funciones y capacidades de networking.



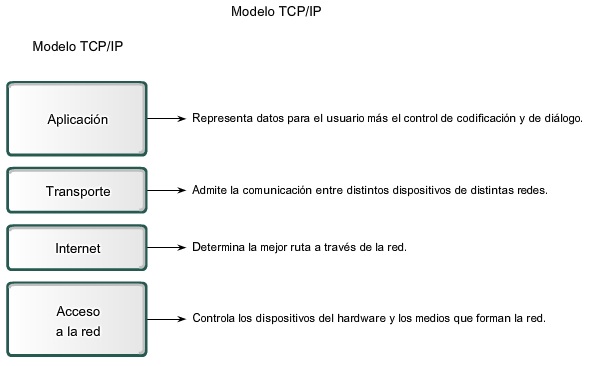
**‍2.4.2 Modelos de Protocolo y Referencia**

Existen dos tipos básicos de modelos de networking: modelos de protocolo y modelos de referencia.  
  
Un modelo de protocolo proporciona un modelo que coincide fielmente con la estructura de una suite de protocolo en particular. El conjunto jerárquico de protocolos relacionados en una suite representa típicamente toda la funcionalidad requerida para interconectar la red humana con la red de datos. El modelo TCP/IP es un protocolo modelo porque describe las funciones que ocurren en cada capa de protocolos dentro de una suite de TCP/IP.  
  
Un modelo de referencia proporciona una referencia común para mantener la consistencia dentro de todos los tipos de protocolos y servicios de red. Un modelo de referencia no está pensado para ser una especificación de implementación ni para proporcionar un nivel de detalle suficiente para definir de forma precisa los servicios de la arquitectura de red. El objetivo principal de un modelo de referencia es ayudar a lograr un mayor conocimiento de las funciones y procesos involucrados.  
  
El modelo de Interconexión de sistema abierto (OSI) es el modelo de referencia de internetwork más conocido. Se usa para diseño de redes de datos, especificaciones de funcionamiento y resolución de problemas.  
  
Si bien los modelos TCP/IP y OSI son los modelos principales que se usan cuando se discute la funcionalidad de la red, los diseñadores de servicios, dispositivos o protocolos de red pueden crear sus propios modelos para representar sus productos. Por último, se solicita a los diseñadores que se comuniquen con la industria al relacionar sus productos o servicios con el modelo OSI, el modelo TCP/IP o ambos.



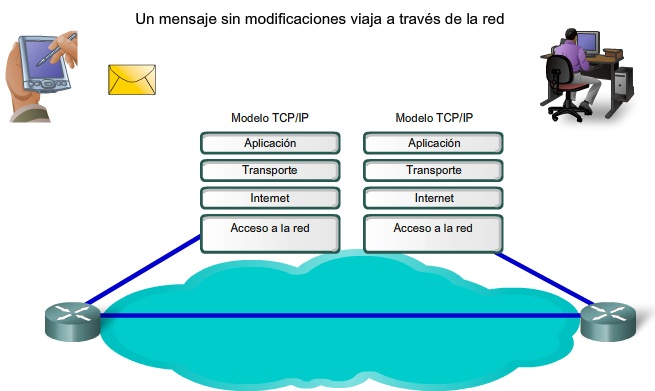
**‍2.4.3 Modelo TCP/IP**

El primer modelo de protocolo en capas para comunicaciones de internetwork se creó a principios de la década de los setenta y se conoce con el nombre de modelo de Internet. Define cuatro categorías de funciones que deben existir para que las comunicaciones sean exitosas. La arquitectura de la suite de protocolos TCP/IP sigue la estructura de este modelo. Por esto, es común que al modelo de Internet se le conozca como modelo TCP/IP.  
  
La mayoría de los modelos de protocolos describen un stack de protocolos específicos del proveedor. Sin embargo, puesto que el modelo TCP/IP es un estándar abierto, una compañía no controla la definición del modelo. Las definiciones del estándar y los protocolos TCP/IP se explican en un foro público y se definen en un conjunto de documentos disponibles al público. Estos documentos se denominan Solicitudes de comentarios (RFC). Contienen las especificaciones formales de los protocolos de comunicación de datos y los recursos que describen el uso de los protocolos.  
  
Las RFC (Solicitudes de comentarios) también contienen documentos técnicos y organizacionales sobre Internet, incluyendo las especificaciones técnicas y los documentos de las políticas producidos por el Grupo de trabajo de ingeniería de Internet (IETF).



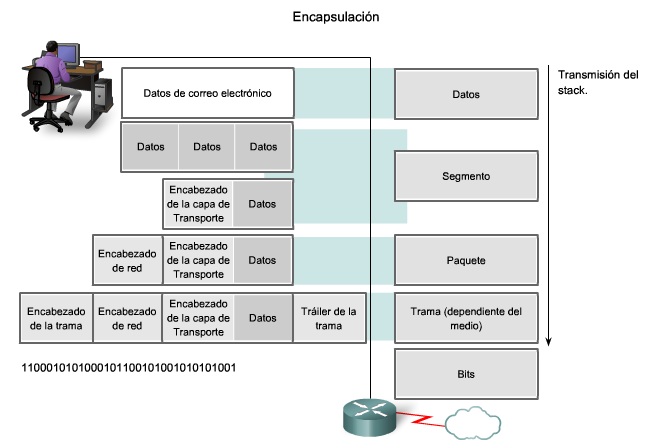
**‍2.4.4 Proceso de comunicación**

El modelo TCP/IP describe la funcionalidad de los protocolos que forman la suite de protocolos TCP/IP. Estos protocolos, que se implementan en los hosts emisores y receptores, interactúan para brindar una entrega extremo a extremo de las aplicaciones a través de la red.  
  
Un proceso de comunicación completo incluye estos pasos:  
  
1. Creación de datos en la capa de aplicación del dispositivo final de origen  
  
2. Segmentación y encapsulación de datos a medida que pasan por el stack de protocolos en el dispositivo final de origen  
  
3. Generación de datos en los medios en la capa de acceso a la red del stack  
  
4. Transportación de los datos a través de internetwork, la cual está compuesta por medios y por cualquier dispositivo intermediario  
  
5. Recepción de los datos en la capa de acceso a la red del dispositivo final de destino  
  
6. Desencapsulación y reensamblaje de los datos a medida que pasan por el stack en el dispositivo de destino  
  
7. Transmisión de estos datos a la aplicación de destino en la capa de aplicación del dispositivo final de destino



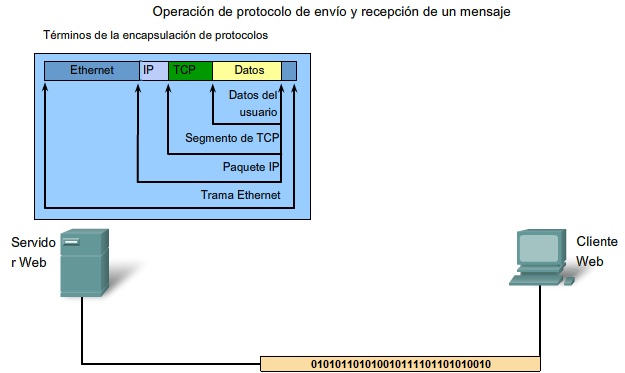
**‍2.4.5 Unidad de datos del Protocolo y encapsulación**

Mientras los datos de la aplicación bajan al stack del protocolo y se transmiten por los medios de la red, varios protocolos le agregan información en cada nivel. Esto comúnmente se conoce como proceso de encapsulación.  
  
La forma que adopta una sección de datos en cualquier capa se denomina Unidad de datos del protocolo (PDU). Durante la encapsulación, cada capa encapsula las PDU que recibe de la capa inferior de acuerdo con el protocolo que se utiliza. En cada etapa del proceso, una PDU tiene un nombre distinto para reflejar su nuevo aspecto. Aunque no existe una convención universal de nombres para las PDU, en este curso se denominan de acuerdo con los protocolos de la suite de TCP/IP.  
Datos: término general que se utiliza en la capa de aplicación para la PDU  
Segmento: PDU de la capa de transporte  
Paquete: PDU de la capa de internetwork  
Trama: PDU de la capa de acceso de red  
Bits: PDU que se utiliza cuando se transmiten datos físicamente por el medio

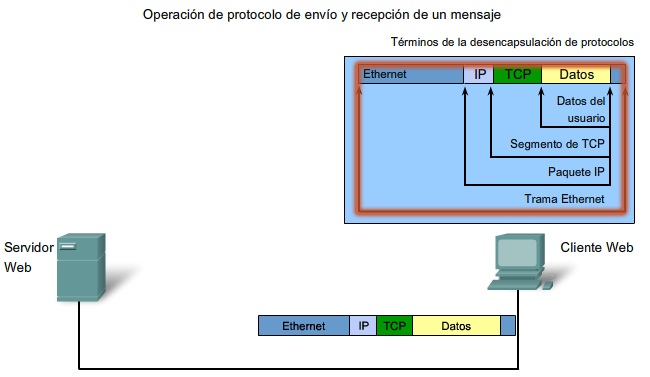


**‍2.4.6 Proceso de envio y de recepción**

Cuando se envían mensajes en una red, el stack de protocolos de un host opera desde las capas superiores hacia las capas inferiores. En el ejemplo del servidor Web podemos utilizar el modelo TCP/IP para ilustrar el proceso de envío de una página Web HTML a un cliente.  
  
El protocolo de la capa aplicación, HTTP, comienza el proceso entregando los datos de la página Web con formato HTML a la capa de transporte. Allí, los datos de aplicación se dividen en segmentos de TCP. A cada segmento de TCP se le otorga una etiqueta, denominada encabezado, que contiene información sobre qué procesos que se ejecutan en la computadora de destino deben recibir el mensaje. También contiene la información para habilitar el proceso de destino para reensamblar los datos de nuevo en su formato original.  
  
La capa de transporte encapsula los datos HTML de la página Web dentro del segmento y los envía a la capa de Internet, donde se implementa el protocolo IP. Aquí, el segmento de TCP se encapsula en su totalidad dentro de un paquete IP que agrega otro rótulo denominado encabezado IP. El encabezado IP contiene las direcciones IP de host de origen y de destino, como también la información necesaria para entregar el paquete a su proceso de destino correspondiente.  
  
Luego el paquete IP se envía al protocolo Ethernet de la capa de acceso a la red, donde se encapsula en un encabezado de trama y en un tráiler. Cada encabezado de trama contiene una dirección física de origen y de destino. La dirección física identifica de forma exclusiva los dispositivos en la red local. El tráiler contiene información de verificación de errores. Finalmente, los bits se codifican en el medio Ethernet mediante la NIC del servidor.



Este proceso se invierte en el host receptor. Los datos se desencapsulan mientras suben al stack hacia la aplicación del usuario final.



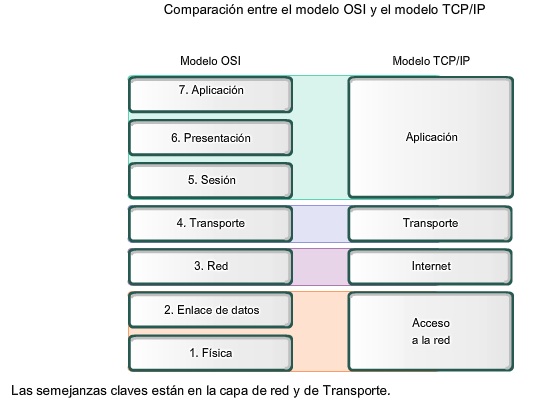
**‍2.4.7 Modelo OSI**

Inicialmente, el modelo OSI fue diseñado por la Organización Internacional para la Estandarización (ISO, International Organization for Standardization) para proporcionar un esquema sobre el cual crear una suite de protocolos de sistemas abiertos. La visión era que este conjunto de protocolos se utilizara para desarrollar una red internacional que no dependiera de sistemas propietarios.  
  
Lamentablemente, la velocidad a la que fue adoptada la Internet con base en TCP/IP y la velocidad a la que se expandió ocasionaron que el desarrollo y la aceptación de la suite de protocolos OSI quedaran atrás. Aunque pocos de los protocolos que se crearon mediante las especificaciones OSI se utilizan ampliamente en la actualidad, el modelo OSI de siete capas ha hecho más contribuciones al desarrollo de otros protocolos y productos para todo tipo de redes nuevas.  
  
Como modelo de referencia, el modelo OSI proporciona una amplia lista de funciones y servicios que se pueden presentar en cada capa. También describe la interacción de cada capa con las capas directamente por encima y por debajo de él. Aunque el contenido de este curso se estructura en torno al modelo OSI, el eje del análisis son los protocolos identificados en el stack de protocolos TCP/IP.  
  
Tenga en cuenta que, mientras las capas del modelo TCP/IP se mencionan sólo por el nombre, las siete capas del modelo OSI se mencionan con frecuencia por número y no por nombre.



**‍2.4.8 Comparación entre el modelo OSI y el modelo TCP/IP**

Los protocolos que forman la suite de protocolos TCP/IP pueden describirse en términos del modelo de referencia OSI. En el modelo OSI, la capa acceso a la red y la capa de aplicación del modelo TCP/IP están subdivididas para describir funciones discretas que deben producirse en estas capas.  
  
En la capa de acceso a la red, la suite de protocolos TCP/IP no especifica cuáles protocolos utilizar cuando se transmite por un medio físico; sólo describe la entrega desde la capa de Internet a los protocolos de red física. Las capas OSI 1 y 2 tratan los procedimientos necesarios para acceder a los medios y las maneras físicas de enviar datos por la red.  
  
Las semejanzas clave entre los dos modelos de red se producen en la Capa 3 y 4 del modelo OSI. La Capa 3 del modelo OSI, la capa de red, se usa casi universalmente para discutir y documentar todos los procesos que se producen en todas las redes de datos para direccionar y enrutar mensajes a través de una internetwork. El Protocolo de Internet (IP) es el protocolo de la suite TCP/IP que incluye la funcionalidad descrita en la Capa 3.  
  
La Capa 4, la capa de transporte del modelo OSI, se utiliza con frecuencia para describir los servicios o funciones generales que administran las conversaciones individuales entre los hosts de origen y destino. Estas funciones incluyen acuse de recibo, recuperación de errores y secuenciamiento. En esta capa, los protocolos TCP/IP, el Protocolo de control de transmisión (TCP) y el Protocolo de datagramas de usuario (UDP) proporcionan la funcionalidad necesaria.  
  
La capa de aplicación TCP/IP incluye un número de protocolos que proporciona funcionalidad específica a una variedad de aplicaciones de usuario final. Las Capas 5, 6 y 7 del modelo OSI se utilizan como referencias para proveedores y programadores de software de aplicación para fabricar productos que necesitan acceder a las redes para establecer comunicaciones.

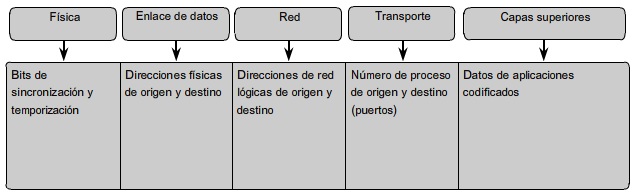


Actividad 2.4.8  
En esta actividad, verá de qué manera el Packet Tracer utiliza el modelo OSI como una referencia para mostrar los detalles de encapsulación de una variedad de los protocolos TCP/IP.

**‍2.5. DIRECCIONAMIENTO DE RED**

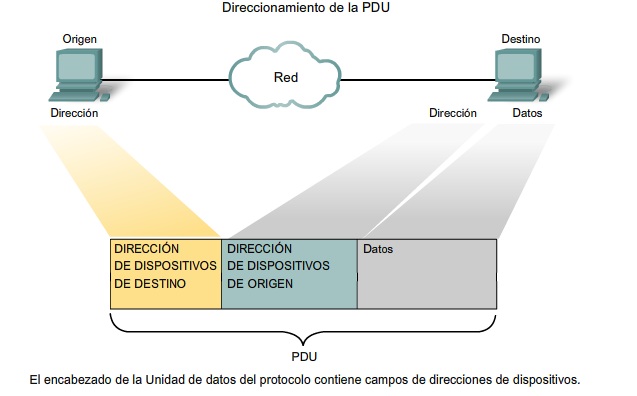
**‍2.5.1 Direccionamiento en la red**

El modelo OSI describe los procesos de codificación, formateo, segmentación y encapsulación de datos para transmitir por la red. Un flujo de datos que se envía desde un origen hasta un destino se puede dividir en partes y entrelazar con los mensajes que viajan desde otros hosts hacia otros destinos. Miles de millones de estas partes de información viajan por una red en cualquier momento. Es muy importante que cada parte de los datos contenga suficiente información de identificación para llegar al destino correcto.  
  
Existen varios tipos de direcciones que deben incluirse para entregar satisfactoriamente los datos desde una aplicación de origen que se ejecuta en un host hasta la aplicación de destino correcta que se ejecuta en otro. Al utilizar el modelo OSI como guía, se pueden observar las distintas direcciones e identificadores necesarios en cada capa.

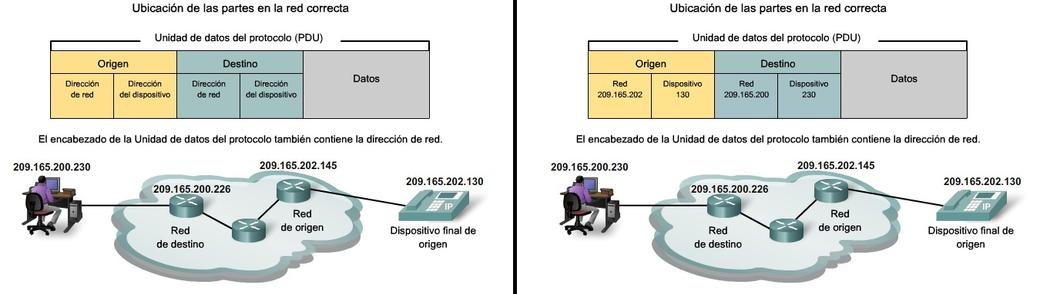


**‍2.5.2 Envio de datos al dispositivo final**

Durante el proceso de encapsulación, se agregan identificadores de dirección a los datos mientras bajan al stack del protocolo en el host de origen. Así como hay capas múltiples de protocolos que preparan los datos para la transmisión a su destino, hay capas múltiples de direccionamiento para asegurar su entrega.  
  
El primer identificador, la dirección física del host, se incluye en el encabezado de la PDU de Capa 2 llamada trama. La Capa 2 está relacionada con la entrega de los mensajes en una red local única. La dirección de la Capa 2 es exclusiva en la red local y representa la dirección del dispositivo final en el medio físico. En una LAN que utiliza Ethernet, esta dirección se denomina dirección de Control de acceso a los medios (MAC). Cuando dos dispositivos se comunican en la red Ethernet local, las tramas que se intercambian entre ellos contienen las direcciones MAC de origen y de destino. Una vez que una trama se recibe satisfactoriamente por el host de destino, la información de la dirección de la Capa 2 se elimina mientras los datos se desencapsulan y suben el stack de protocolos a la Capa 3.

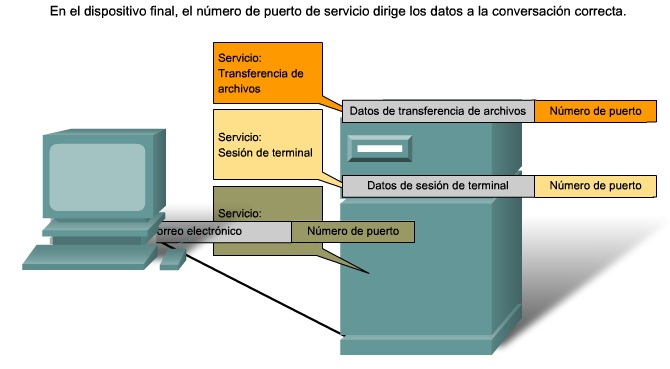


**‍2.5.3. Trasnporte de datos a través de internetwork**

Los protocolos de Capa 3 están diseñados principalmente pata mover datos desde una red local a otra red local dentro de una internetwork. Mientras las direcciones de Capa 2 sólo se utilizan para comunicar entre dispositivos de una red local única, las direcciones de Capa 3 deben incluir identificadores que permitan a dispositivos de red intermediarios ubicar hosts en diferentes redes. En la suite de protocolos TCP/IP, cada dirección IP host contiene información sobre la red en la que está ubicado el host.  
  
En los límites de cada red local, un dispositivo de red intermediario, por lo general un router, desencapsula la trama para leer la dirección host de destino contenida en el encabezado del paquete, la PDU de Capa 3. Los routers utilizan la porción del identificador de red de esta dirección para determinar qué ruta utilizar para llegar al host de destino. Una vez que se determina la ruta, el router encapsula el paquete en una nueva trama y lo envía por su trayecto hacia el dispositivo final de destino. Cuando la trama llega a su destino final, la trama y los encabezados del paquete se eliminan y los datos se suben a la Capa 4.  
  


**‍2.5.4 Envio de datos a la aplicación correcta**

En la Capa 4, la información contenida en el encabezado de la PDU no identifica un host de destino o una red de destino. Lo que sí identifica es el proceso o servicio específico que se ejecuta en el dispositivo host de destino que actuará en los datos que se entregan. Los hosts, sean clientes o servidores en Internet, pueden ejecutar múltiples aplicaciones de red simultáneamente. La gente que utiliza computadoras personales generalmente tiene un cliente de correo electrónico que se ejecuta al mismo tiempo que el explorador Web, un programa de mensajería instantánea, algún streaming media e incluso, tal vez, algún juego. Todos estos programas ejecutándose en forma separada son ejemplos de procesos individuales.  
  
Ver una página Web invoca al menos un proceso de red. Hacer clic en un hipervínculo hace que un explorador Web se comunique con un servidor Web. Al mismo tiempo, en segundo plano, es posible que un cliente de correo electrónico esté enviando o recibiendo un email y un colega o amigo enviando un mensaje instantáneo.  
  
Piense en una computadora que tiene sólo una interfaz de red. Todos los streams de datos creados por las aplicaciones que se están ejecutando en la PC ingresan y salen a través de esa única interfaz, sin embargo los mensajes instantáneos no emergen en medio del documento del procesador de textos o del correo electrónico que se ve en un juego.  
  
Esto es porque los procesos induviduales que se ejecutan en los hosts de origen y destino se comunican unos con otros. Cada aplicación o servicio se representa por un número de puerto en la Capa 4. Un diálogo único entre dispositivos se identifica con un par de números de puerto de origen y de destino de Capa 4 que son representativos de las dos aplicaciones de comunicación. Cuando los datos se reciben en el host, se examina el número de puerto para determinar qué aplicación o proceso es el destino correcto de los datos.



**‍2.5.5 Guerreros de la red**

Un recurso de entretenimiento para ayudar a visualizar los conceptos de networking es la película animada "Warriors of the Net" (Guerreros de la red), por TNG Media Lab. Antes de ver el video, se debe tener en cuenta lo siguiente: Primero, en cuanto a los conceptos que ha aprendido en este capítulo, piense en qué momento del video está en la LAN, en la WAN, en intranet o en Internet, y cuáles son los dispositivos finales vs. los dispositivos intermedios, cómo se aplican los modelos OSI y TCP/IP y qué protocolos están involucrados.  
  
Segundo, es posible que algunos términos que se mencionan en el video no le sean familiares. Los tipos de paquetes mencionados se refieren al tipo de datos de nivel superior (TCP, UDP, ICMP Ping, PING de la muerte) que se encapsulan en los paquetes IP (en definitiva, todo se convierte en paquetes IP). Los dispositivos que los paquetes encuentran en su viaje son el router, el servidor proxy, el switch del router, la intranet corporativa, el proxy, la URL, el firewall, la ancho de banda, los hosts y el servidor Web.  
  
Tercero, mientras se hace referencia los números de puerto 21, 23,25, 53 y 80 de forma explícita en el video, las direcciones IP son referidas sólo de forma implícita, ¿puede ver dónde? ¿Dónde se pudieron involucrar las direcciones MAC en el video?  
  
Finalmente, aunque todas las animaciones con frecuencia tienen simplificaciones en ellas, hay un error categórico en el video. Aproximadamente a los 5 minutos, se formula la siguiente afirmación "Qué sucede cuando el señor IP no recibe un acuse de recibo; simplemente envía un paquete de reemplazo." Como verá en los siguientes capítulos, ésta no es una función del Protocolo de Internet de la Capa 3, el cual es un protocolo "no confiable" de máximo esfuerzo, sino una función del Protocolo TCP de la capa de transporte.  
  
Al final de este curso tendrá un mejor entendimiento de la cobertura de los conceptos descritos en el video. Esperamos que lo disfrute.  
  
Descargue la película de <http://www.warriorsofthe.net>

**‍2.6 LABORATORIOS DEL CAPITULO**

**‍2.6.1 Laboratorio: Orientación de topología y creación de una red pequeña**

Esta práctica de laboratorio comienza con la creación de dos redes pequeñas. Después se mostrará cómo están conectadas a la red de práctica más grande que se utilizó a lo largo de este curso. Esta red es un modelo simplificado de una sección de Internet y se utilizará para desarrollar sus aptitudes prácticas en networking.  
  
La siguiente secuencia de prácticas de laboratorio introduce los términos de interconexión de redes que figuran más abajo. En los capítulos posteriores, se estudiará a detalle esta terminología de networking.  
  
Cable de conexión directa: cable de cobre trenzado no blindado (UTP) para conectar dispositivos de red diferentes  
  
Cable de conexión cruzada: cable de cobre UTP para conectar dispositivos de red similares  
  
Cable serial: cable de cobre típico de las conexiones de área ancha  
  
Ethernet: Tecnología de red de área local dominante  
  
Dirección MAC: Ethernet Capa 2, dirección física  
  
Dirección IP: Capa 3 dirección lógica  
  
Máscara de subred: Requerida para interpretar la dirección IP  
  
Gateway predeterminado: La dirección IP en la interfaz del router a la que una red envía el tráfico que sale de la red local  
  
NIC: tarjeta de interfaz de red; el puerto o interfaz que le permite a un dispositivo final participar en una red  
  
Puerto (hardware): interfaz que le permite a un dispositivo red participar en la misma y estar conectado a través del medio de networking  
  
Puerto (software): dirección de protocolo de Capa 4 en la suite TCP/IP  
  
Interfaz (hardware): un puerto  
  
Interfaz (software): punto de interacción lógica dentro del software  
  
PC: dispositivo final  
  
Computadora: dispositivo final  
  
Estación de trabajo: dispositivo final  
  
Switch: dispositivo intermedio que toma decisiones sobre las tramas basándose en direcciones de Capa 2 (direcciones MAC Ethernet típicas)  
  
Router: dispositivo de Capa 3, 2 y 1 que toma decisiones sobre paquetes basados en direcciones de Capa 3 (generalmente direcciones IPv4)  
  
Bit: dígito binario, lógico 1 o cero, tiene varias representaciones físicas, como pulsos eléctricos, ópticos o microondas; PDU de Capa 1  
  
Trama: PDU de Capa 2  
  
Paquetes: PDU de Capa 3  
  
Haga clic en el icono Laboratorio para obtener más detalles.  
  
Actividad 2.6.1

**‍2.6.2 Uso de wireshark para ver las unidades de datos del protocolo**

En esta práctica de laboratorio, aprenderá a utilizar la poderosa herramienta Wireshark al capturar ("sniffing") tráfico por fuera de la red modelo.

**‍2.6.2 Uso de Packet Tracer para ver las unidades de datos del protocolo**

En esta actividad, utilizará el modo de simulación de Packet Tracer para carpturar y analizar los paquetes del ping de un indicador del sistema de una PC y una solicitud Web mediante una URL.

**‍2.7 RESUMEN DEL CAPITULO**

**‍2.7.1 Resúmen y revisión**

Las redes de datos son sistemas de dispositivos finales, dispositivos intermediarios y los medios que conectan los dispositivos, los cuales proporcionan la plataforma para la red humana.  
  
Estos dispositivos, y los servicios que operan en ellos, pueden interconectarse de forma mundial y transparente para el usuario porque cumplen con las reglas y protocolos.  
  
El uso de modelos en capas como abstracciones significa que las operaciones de los sistemas de red se pueden analizar y desarrollar para abastecer las necesidades de los servicios de comunicación futuros.  
  
Los modelos de networking más ampliamente utilizados son OSI y TCP/IP. Asociar los protocolos que establecen las reglas de las comunicaciones de datos con las distintas capas es de gran utilidad para determinar qué dispositivos y servicios se aplican en puntos específicos mientras los datos pasan a través de las LAN y WAN.  
  
A medida que bajan en el stack, los datos se segmentan en partes y se encapsulan con las direcciones y demás etiquetas. El proceso se revierte a medida que las partes se desencapsulan y pasan hacia el stack del protocolo de destino.  
  
La aplicación de los modelos permite a las distintas personas, empresas y asociaciones comerciales analizar las redes actuales y planificar las redes del futuro