

2 Comunicación a través de la red

2.0 Introducción del capítulo

2.0.1 Introducción del capítulo

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 necesitamos. A medida que nuestra red humana continúa ampliándose, también debe crecer la plataforma que la conecta y respalda.

En vez de desarrollar sistemas exclusivos e individuales para la entrega de cada nuevo servicio, la industria de networking en su totalidad ha desarrollado los medios para analizar la plataforma existente y mejorarla progresivamente. Esto asegura que se mantengan las comunicaciones existentes mientras se presentan nuevos servicios económicos y seguros a nivel tecnológico.

En este curso, nos centraremos en estos aspectos de la red de información:

- dispositivos que conforman la red,
- medios que conectan los dispositivos,
- mensajes que se envían a través de la red,
- reglas y procesos que regulan las comunicaciones de red, y
- herramientas y comandos para construir y mantener redes.

El uso de modelos generalmente aceptados que describen funciones de la red es central para el estudio de redes. Estos modelos proporcionan un marco para entender las redes actuales y para facilitar el desarrollo de nuevas tecnologías para admitir futuras necesidades de comunicación.

En este curso, utilizamos estos modelos y las herramientas diseñadas para analizar y simular la funcionalidad de la red.

2.1 Plataforma para las comunicaciones

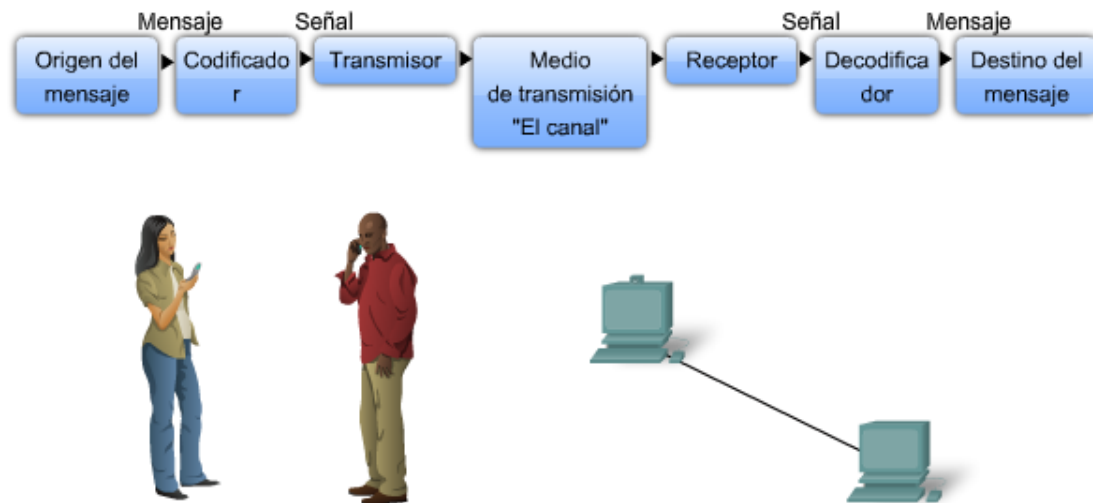
2.1.1 Elementos de la comunicación

La comunicación comienza con un mensaje o información que se debe enviar desde 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 de computadoras, el medio generalmente es un tipo de cable o una transmisión inalámbrica.

El término *red* en este curso se referirá a datos o redes de información capaces de transportar gran cantidad de diferentes tipos de comunicaciones, que incluye datos informáticos, voz interactiva, video y productos de entretenimiento.



2.1.2 Comunicación de mensajes

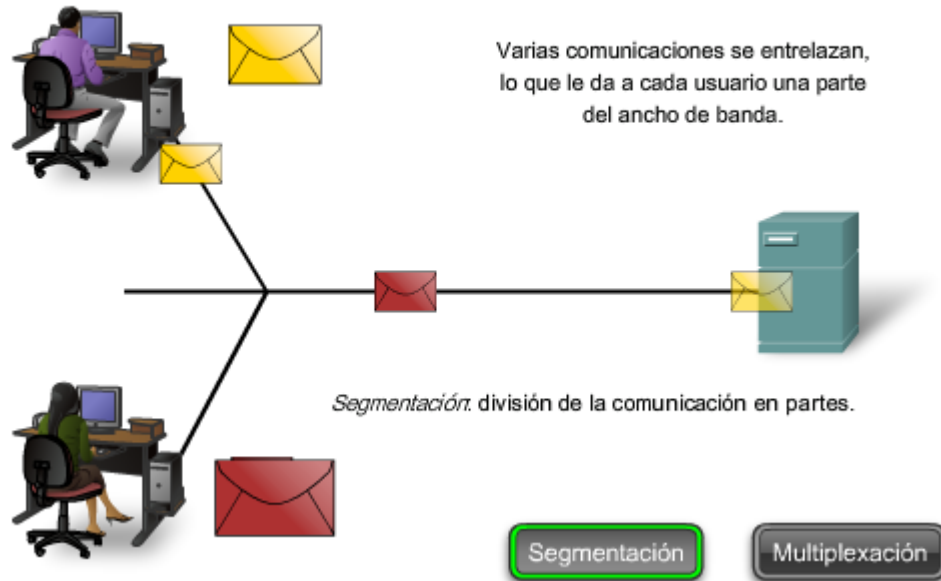
En teoría, una comunicación simple, como un video musical o un e-mail puede enviarse a través de la red desde un origen hacia un destino como un stream de bits masivo y continuo. Si en realidad los mensajes se transmitieron de esta manera, significará que ningún otro dispositivo podrá enviar o recibir mensajes en la misma red mientras esta transferencia de datos está en progreso. Estos grandes streams de datos originarán retrasos importantes. Además, si falló un enlace en la infraestructura de red interconectada durante la transmisión, se perderá todo el mensaje y tendrá que retransmitirse por completo.

Un mejor enfoque para enviar datos a través de la red es dividir los datos en partes más pequeñas y más manejables. 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 entrelazar diversas conversaciones en la red. El proceso que se utiliza para entrelazar 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.

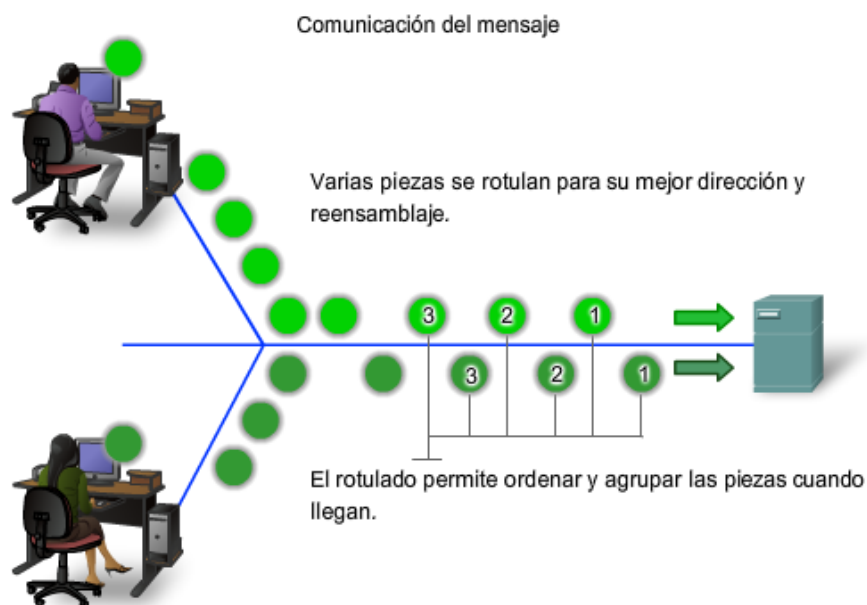
Comunicación del mensaje



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.

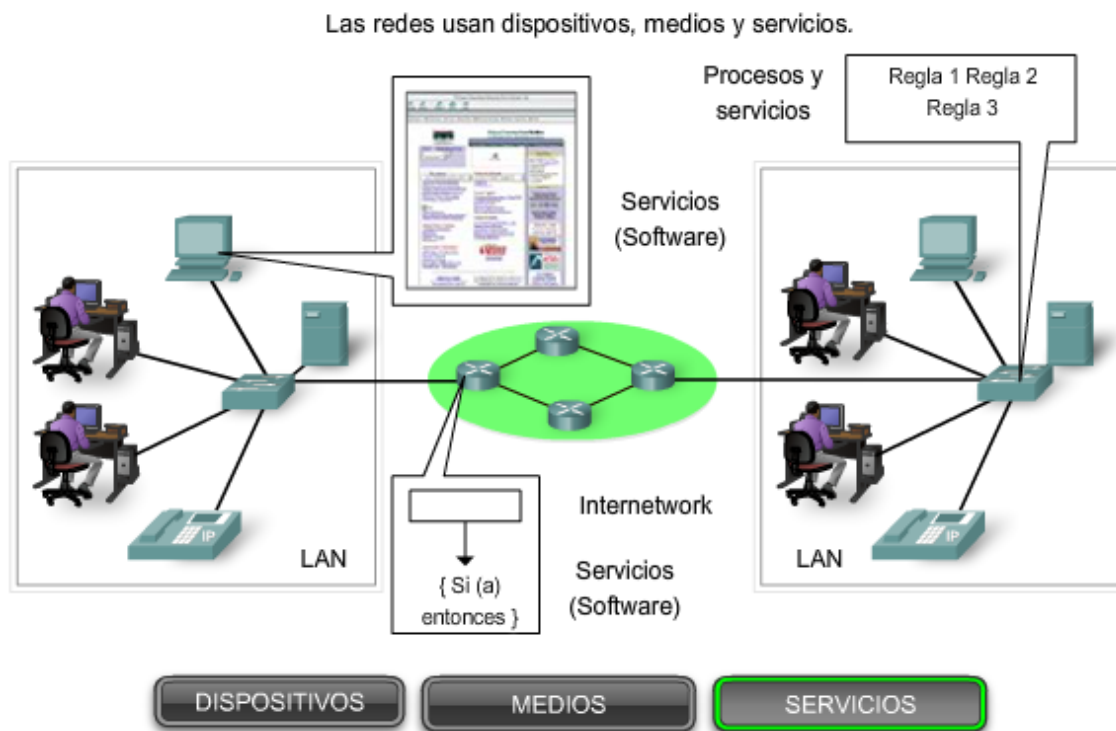


2.1.3 Componentes de la red

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 utilizando radio frecuencia invisible u ondas infrarrojas.

Los servicios y procesos son los programas de comunicación, denominados 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 e-mail 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 rol 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:

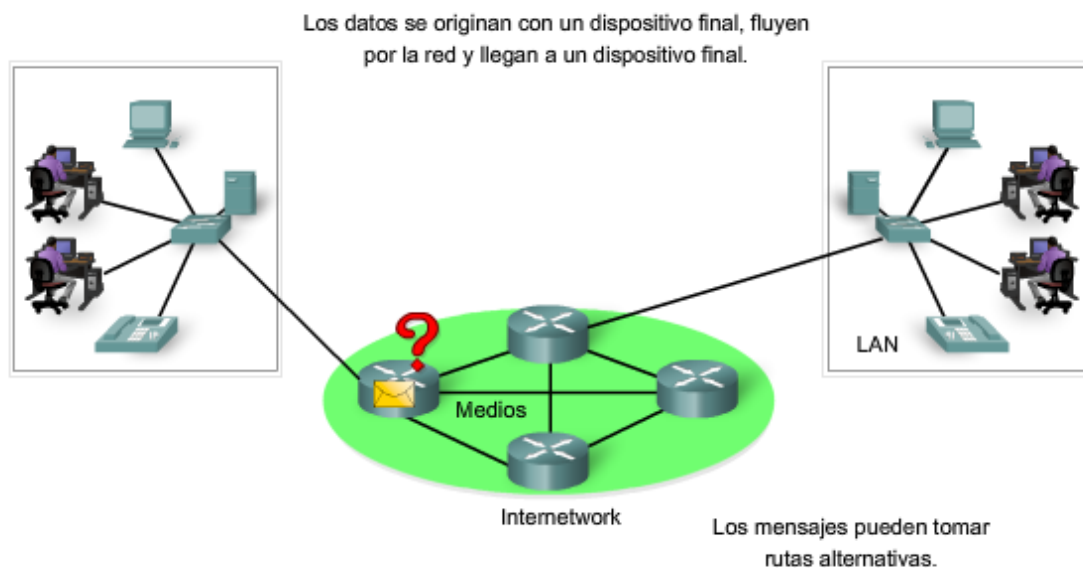
- Computadoras (estaciones de trabajo, computadoras portátiles, servidores de archivos, servidores Web)
- Impresoras de red
- Teléfonos VoIP
- Cámaras de seguridad
- Dispositivos móviles de mano (como escáneres de barras inalámbricos, asistentes digitales personales (PDA))

En el contexto de una red, los dispositivos finales se denominan host. 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 una comunicación, utiliza la dirección del host de destino para especificar dónde debe ser enviado el mensaje.

En las redes modernas, un host puede funcionar como un [cliente](#), como un servidor o como ambos. El software instalado en el host determina qué rol representa en la red.

Los servidores son hosts que tienen software instalado que les permite proporcionar información y servicios, como e-mail o páginas Web, a otros hosts en la red.

Los clientes son hosts que tienen software instalado que les permite solicitar y mostrar la información obtenida del servidor.



2.1.5 Dispositivos intermediarios y su rol en la red

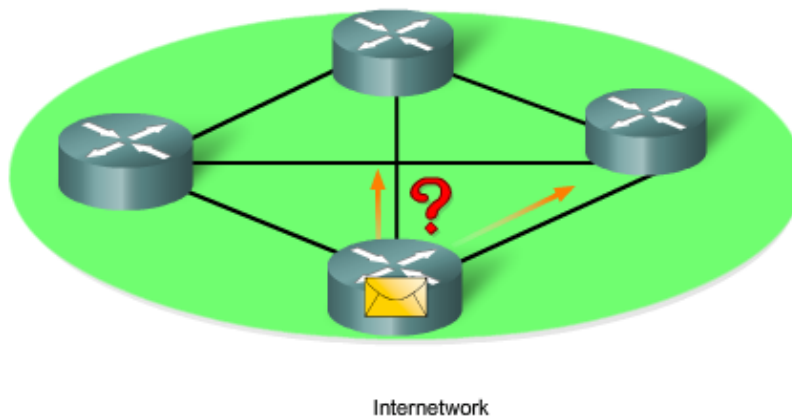
Además de los dispositivos finales con los cuales la gente está familiarizada, las redes dependen de [dispositivos intermediarios](#) para proporcionar conectividad y para trabajar detrás de escena y garantizar que los datos fluyan a través de la red. Estos dispositivos conectan los hosts individuales 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 inalámbricos),
- dispositivos de internetworking (routers),
- servidores de comunicación y módems, y
- dispositivos de seguridad (firewalls).

La administración de datos mientras fluyen a través de la red también es 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:

- regenerar y retransmitir señales de datos,
- mantener información sobre qué rutas existen a través de la red y de la internetwork,
- notificar a otros dispositivos los errores y las fallas de comunicación,
- direccionar datos por rutas alternativas cuando existen fallas en un enlace,
- clasificar y direccionar mensajes según las prioridades de QoS (calidad de servicio), y
- permitir o denegar el flujo de datos en base a configuraciones de seguridad.

Los dispositivos intermediarios dirigen la ruta de los datos pero no generan ni cambian el contenido de los datos.



2.1.6 Medios de red

La comunicación a través de una red es transportada 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 los cables,

- fibras de vidrio o plásticas (cable de fibra óptica), y
- transmisión inalámbrica.

La [codificación](#) de señal que se debe realizar para que el mensaje sea transmitido 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.

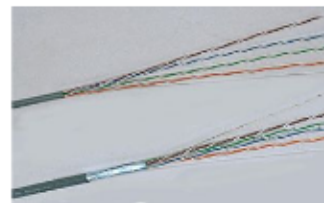
Los diferentes tipos de medios de red tienen diferentes características y beneficios. No todos los medios de red tienen las mismas características ni son adecuados para el mismo fin. Los criterios para elegir un medio de red son:

- 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, y
- el costo del medio y de la instalación.

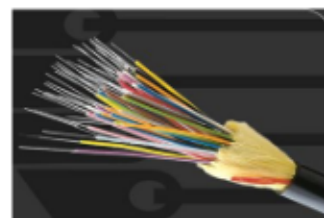
Medios de red



Cobre



Fibra óptica



Inalámbricos



2.2 LAN (Red de área local), WAN (Red de área amplia) e Internetworks

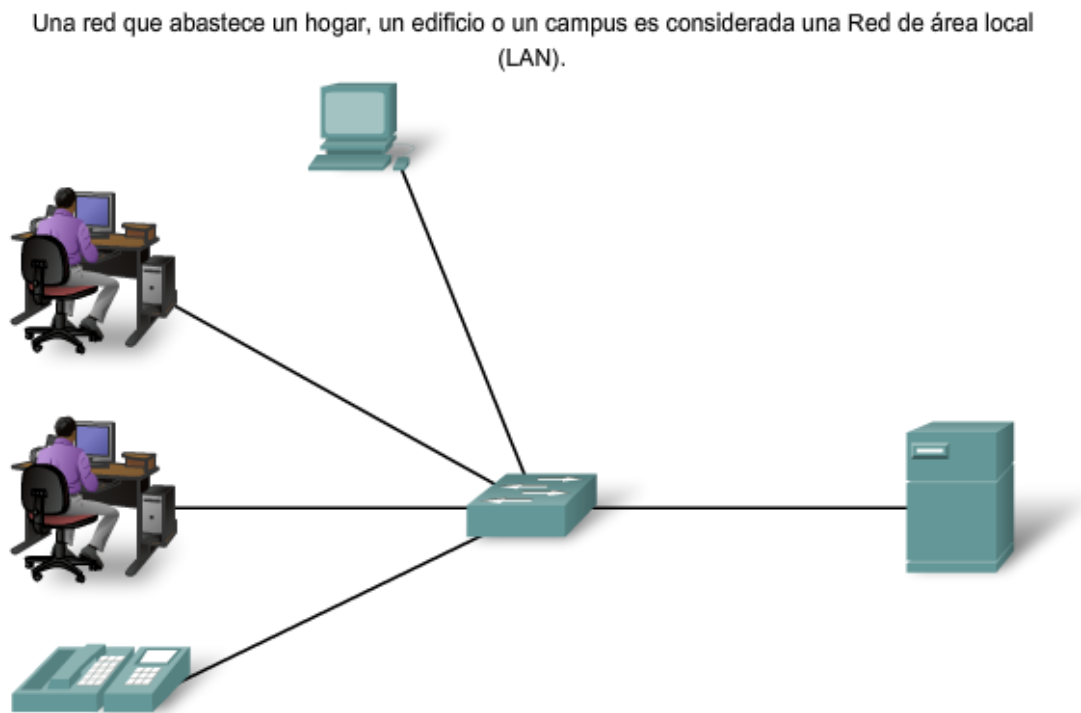
2.2.1 Redes de área local

Las infraestructuras de red pueden variar en gran medida en términos de:

- el tamaño del área cubierta,
- la cantidad de usuarios conectados, y

- la cantidad y 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 subscriptores servicios de red convergente de información.

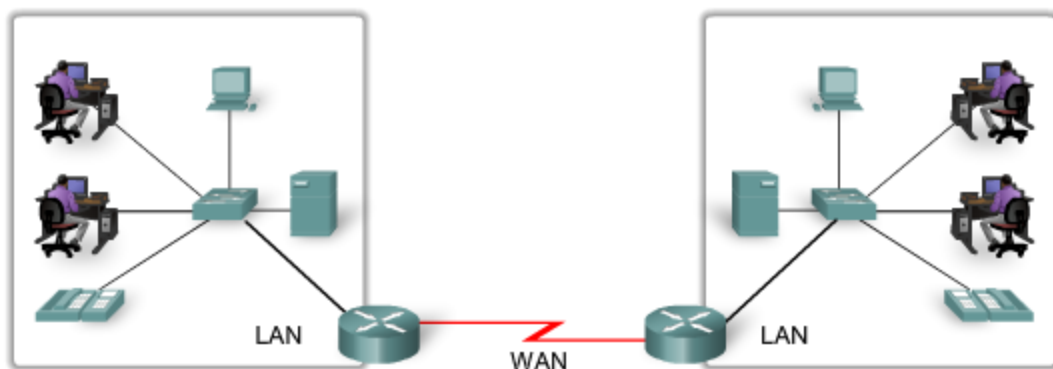
Por lo general, las organizaciones individuales alquilan las conexiones a través de una red de proveedores de servicios de telecomunicaciones. Estas redes que conectan las LAN en ubicaciones separadas geográficamente se conocen como Redes de área amplia (WAN). Aunque la organización mantiene todas las 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 son controladas por 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, instalación y mantenimiento de éstos son aptitudes complementarias de la función de una red de la organización.

Las LAN y WAN son de mucha utilidad para las organizaciones individuales. Conectan a los usuarios dentro de la organización. Permiten gran cantidad de formas de comunicación que incluyen intercambio de e-mails, capacitación corporativa y acceso a recursos.

Las LAN separadas por una distancia geográfica están conectadas por una red que se conoce como Red de área extensa (WAN).



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 u otra red, fuera de la organización local.

Los ejemplos de este tipo de comunicación incluyen:

- enviar un correo electrónico a un amigo en otro país,
- acceder a noticias o productos de un sitio Web,
- obtener un archivo de la computadora de un vecino,
- mensajería instantánea con un pariente de otra ciudad, y
- seguimiento de la actividad de un equipo deportivo favorito a través del teléfono celular.

Internetwork

Una malla global de redes interconectadas (internetworks) cubre estas necesidades de comunicación humanas. 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 más conocida, ampliamente utilizada y a la que accede el público en general 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 la comunicación efectiva a

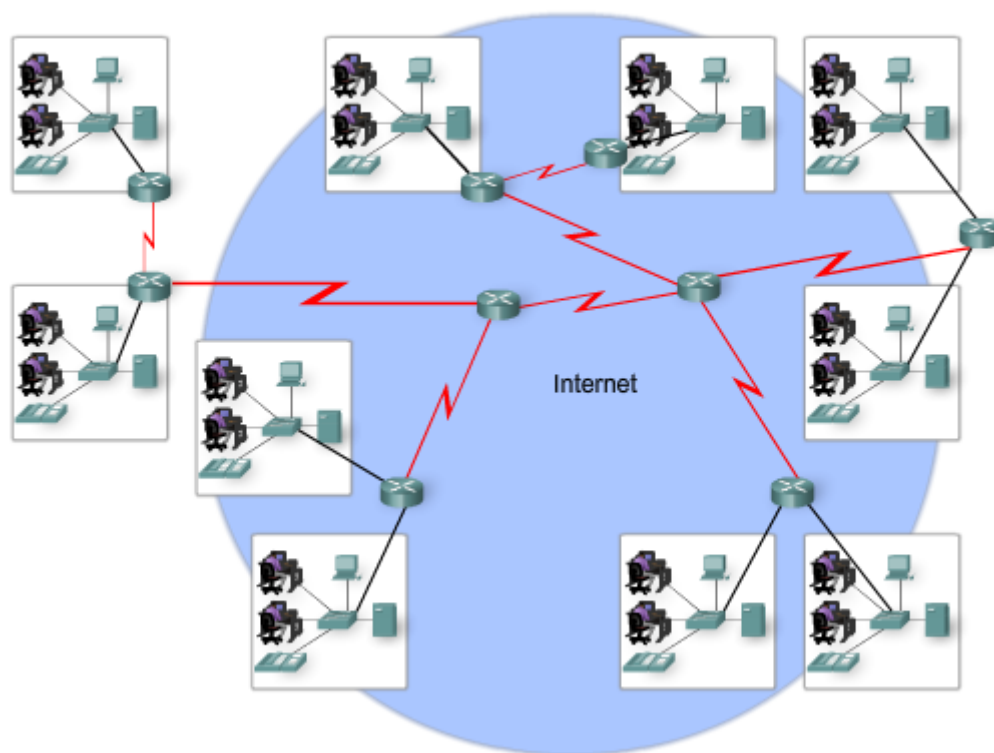
través de esta infraestructura diversa requiere la aplicación de tecnologías y protocolos consistentes y reconocidos comúnmente, como también la cooperación de muchas agencias de administración de redes.

Intranet

El término [intranet](#) se utiliza generalmente para referirse a una conexión privada de algunas LAN y WAN que pertenecen a una organización y que está diseñada para que puedan acceder solamente los miembros y empleados de la organización u otros que tengan autorización.

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 y del momento, a veces los términos pueden ser intercambiados.

Las LAN y WAN pueden estar conectadas a internetworks.



2.2.4 Representaciones de red

Cuando se transporta información compleja como la conectividad de red y el funcionamiento de una gran internetwork, es de mucha utilidad utilizar 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. Durante todo este curso y pruebas de

laboratorio, aprenderá cómo funcionan estos dispositivos y cómo se realizan con ellos tareas básicas de configuración.

Además de estas representaciones, se utiliza terminología especializada cuando se analiza la manera en que se conectan unos con otros. Algunos términos importantes para recordar son:

Tarjeta de interfaz de red (NIC): una NIC o adaptador LAN proporciona la conexión física con la red en la computadora personal u otro dispositivo [host](#). El medio que conecta la computadora personal con el dispositivo de red se inserta directamente en la NIC.

Puerto físico: conector o toma en un dispositivo de red en el cual el medio se conecta con un host o con otro dispositivo de red.

Interfaz: [puertos](#) especializados de un dispositivo de internetworking que se conecta con redes individuales. Puesto que los routers se utilizan para interconectar redes, los puertos de un router se conocen como interfaces de red.

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 denominadas protocolos. Estos protocolos son específicos de las características de la conversación. En nuestras comunicaciones personales cotidianas, las reglas que utilizamos para comunicarnos a través de un medio, como el teléfono, no necesariamente son las mismas que los protocolos que se usan en otro medio, como escribir una carta.

Piense cuántas reglas o protocolos diferentes rigen los distintos métodos de comunicación que existen actualmente en el mundo.

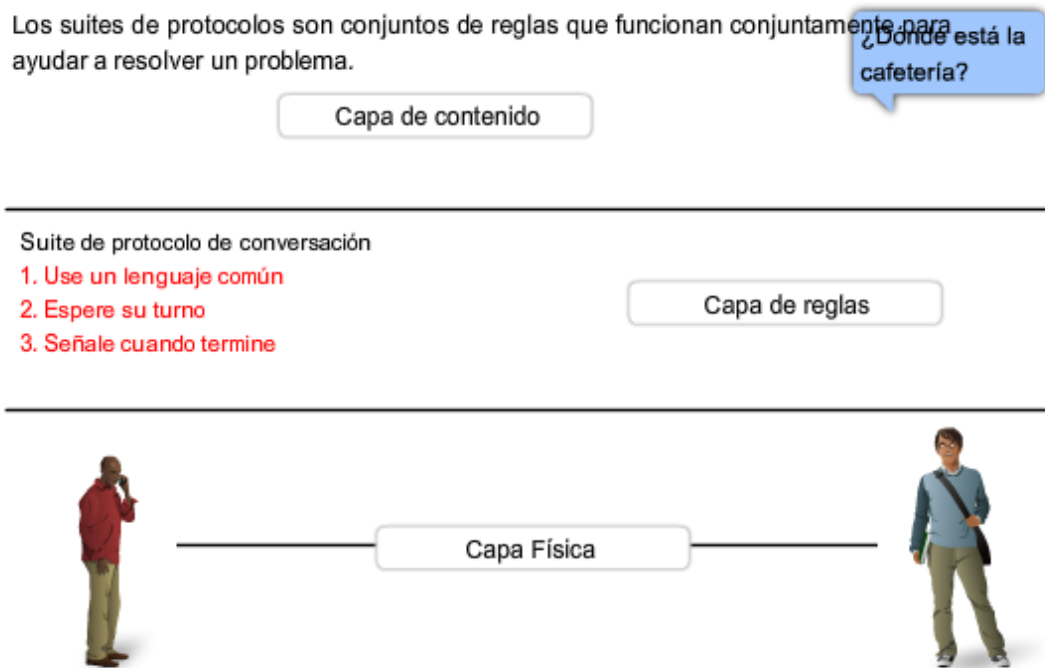
La comunicación exitosa entre los hosts de una red requiere la interacción de gran cantidad de protocolos diferentes. Un grupo de protocolos interrelacionados que son necesarios para realizar una función de comunicación se denomina [suite de protocolos](#). Estos protocolos se implementan en el software y hardware que está cargado en cada host y dispositivo de red.

Una de las mejores maneras de visualizar de qué manera todos los protocolos interactúan en un host en particular es verlo como un stack. Una stack de protocolos muestra cómo los protocolos individuales de una suite se implementan 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 compiten a los movimientos de datos por la red y a la provisión de servicios a las capas superiores, concentrados en el contenido del mensaje que se está enviando y en la interfaz del usuario.

Uso de capas para describir una comunicación cara a cara

Por ejemplo: considere a dos personas comunicándose 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, están las palabras que en realidad se pronuncian, el contenido de la comunicación.

Si somos testigos de esta conversación, en realidad no veremos "capas" flotando en el espacio. 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 sobreentendidas o implícitas, basadas en los usos y costumbres. Para que los dispositivos se puedan comunicar en forma exitosa, una nueva [suite](#) de protocolos debe describir los requerimientos e interacciones precisos.

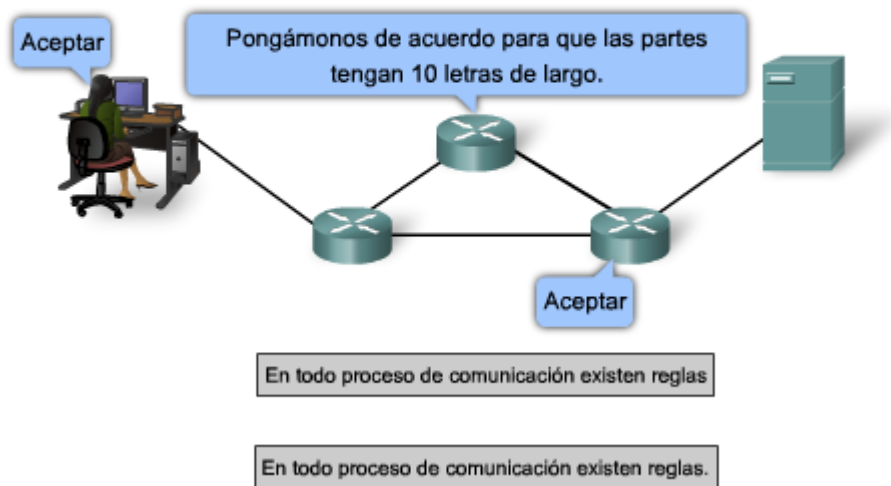
Las suite de protocolos de networking describen procesos como los siguientes:

- el formato o estructura del mensaje,
- el método por el cual los dispositivos de networking comparten información sobre rutas con otras redes,
- cómo y cuando se pasan los mensajes de error y del sistema entre dispositivos, o
- el inicio y terminación de las sesiones de transferencia de datos.

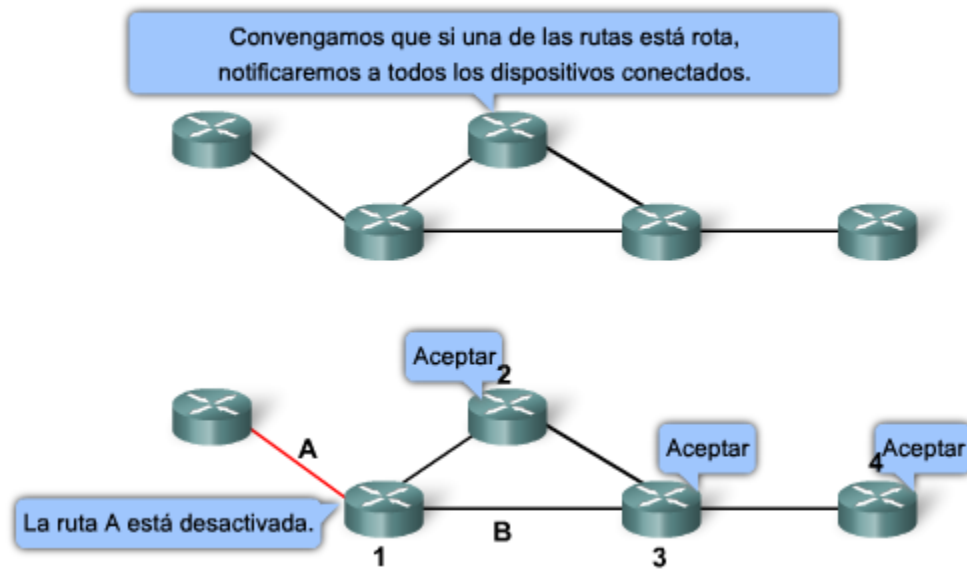
Los protocolos individuales de una suite de protocolos pueden ser específicos de un fabricante o de propiedad exclusiva. Propietario, en este contexto, significa que una

compañía o proveedor controla la definición del protocolo y cómo funciona. Algunos protocolos propietarios pueden ser utilizados por distintas organizaciones con permiso del propietario. Otros, sólo se pueden implementar en equipos fabricados por el proveedor propietario.

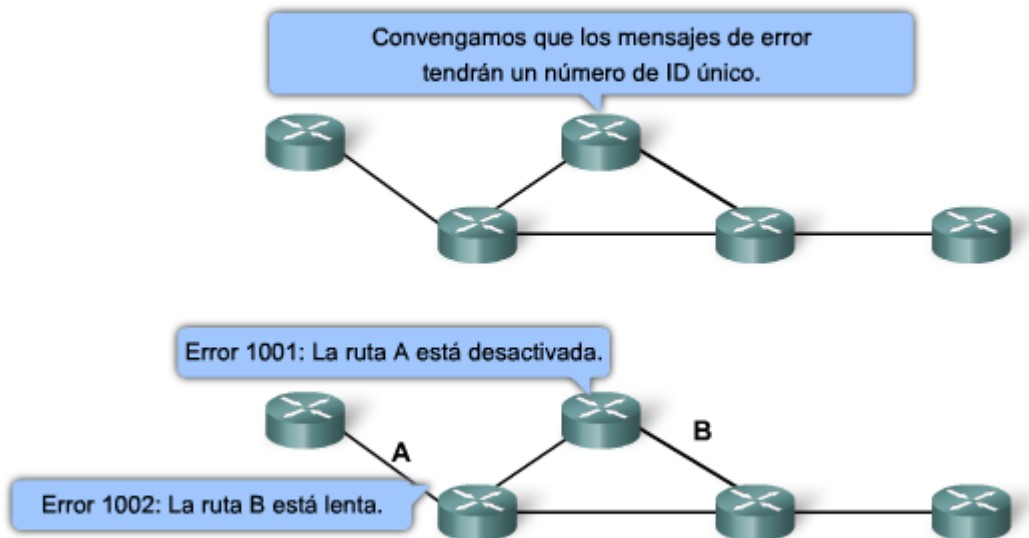
El rol de los protocolos



El rol de los protocolos

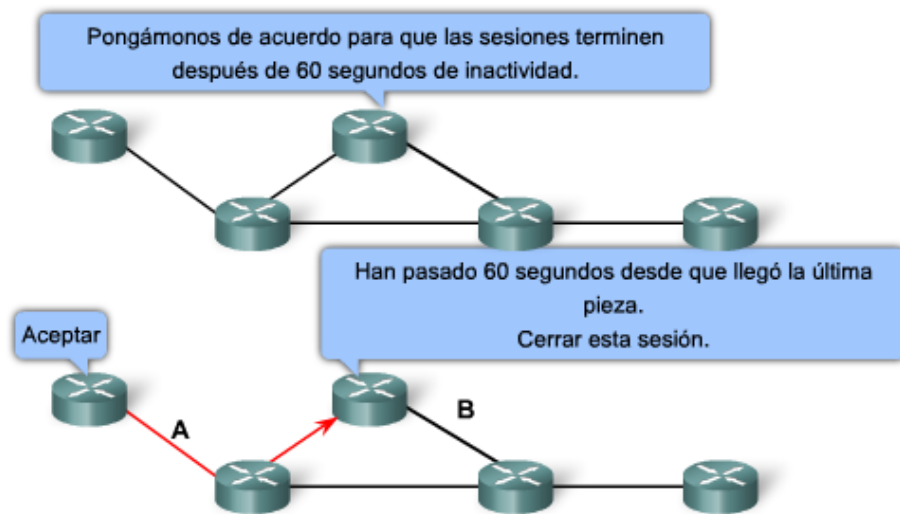


El rol de los protocolos



Cómo y cuándo los mensajes de error y del sistema se pasan entre dispositivos

El rol de los protocolos



La configuración y finalización de las sesiones de transferencia de datos

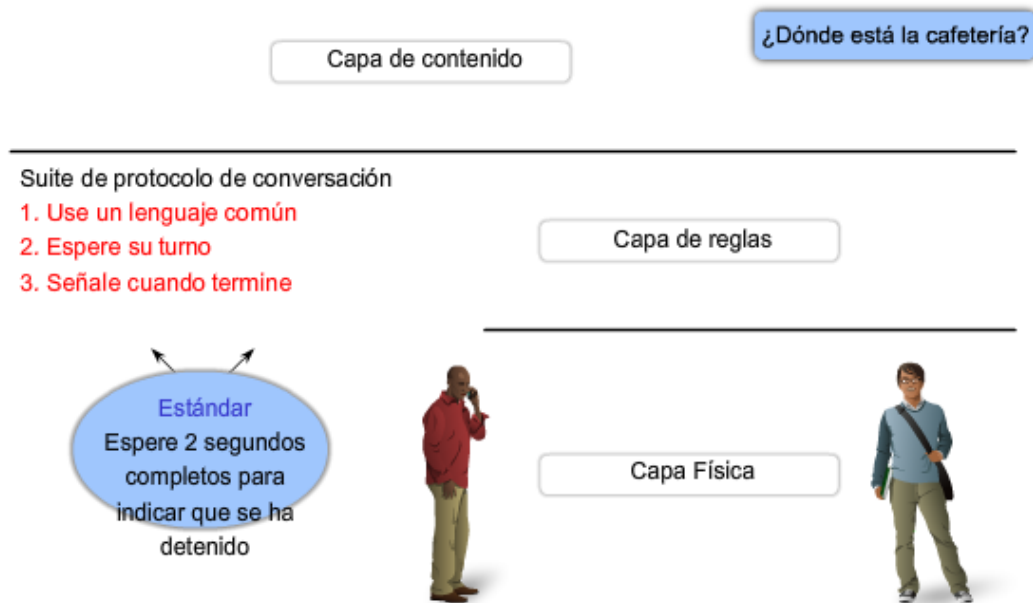
2.3.3 Suites de protocolos y estándares de la industria

Con frecuencia, muchos de los protocolos que comprenden una suite de protocolos aluden 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 protocolo no es observado estrictamente por un fabricante en particular, 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.

Los estándares son protocolos y acuerdos muy usados y aceptados.



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:

[Protocolo de transferencia de hipertexto \(HTTP\)](#) es un protocolo común que regula 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. El protocolo HTTP se basa en otros protocolos para regir de qué manera se transportan los mensajes entre el cliente y el servidor

Protocolo de transporte:

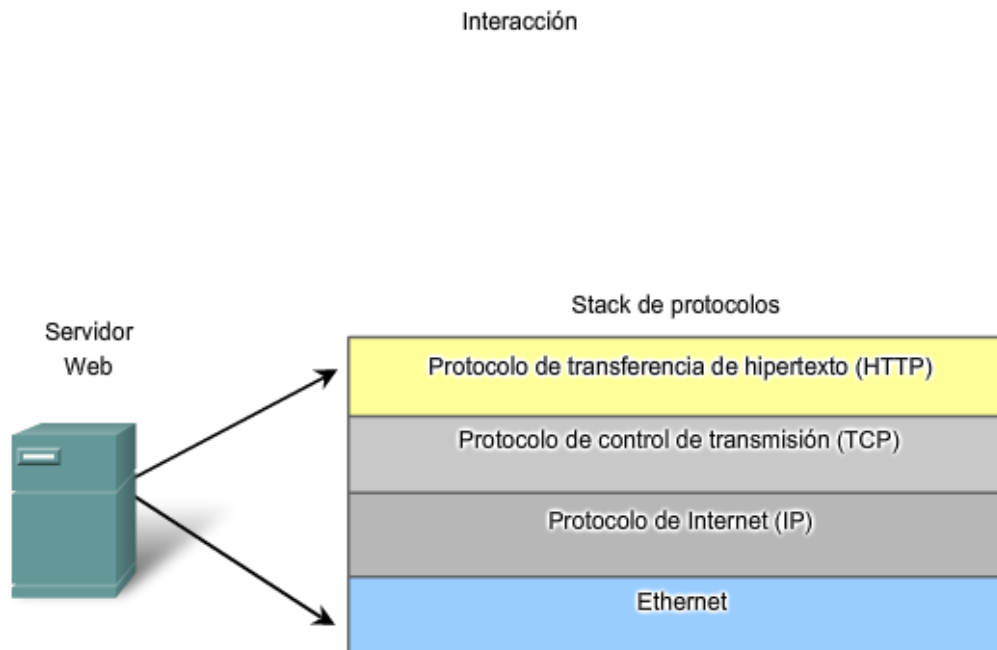
[Protocolo de control de transmisión \(TCP\)](#) es el protocolo de transporte que administra las conversaciones individuales entre servidores Web y clientes Web. TCP divide los mensajes HTTP en pequeñas partes, denominadas segmentos, para enviarlas al cliente de destino. También es responsable de controlar el tamaño y los intervalos a los que se intercambian los mensajes entre el servidor y el cliente.

Protocolo de internetwork:

El protocolo internetwork más común es el [Protocolo de Internet \(IP\)](#). IP es responsable de tomar los segmentos formateados del TCP, encapsularlos en paquetes, asignarles las direcciones correctas y seleccionar la mejor ruta hacia el host de destino.

Protocolos de acceso a la red:

Estos protocolos describen dos funciones principales: administración de enlace de datos y 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

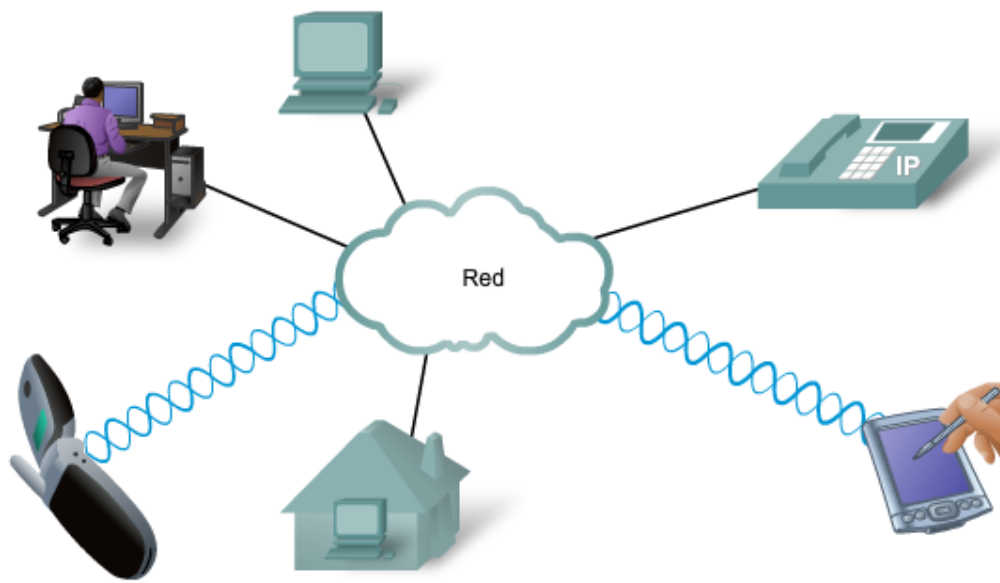
Los protocolos de red describen las funciones que se producen durante las comunicaciones de red. En el ejemplo de la conversación cara a cara, es posible que un protocolo para comunicar establezca que para indicar que la conversación ha finalizado, el emisor debe permanecer en silencio durante dos segundos completos. Sin embargo, este protocolo no especifica *cómo* el emisor debe permanecer en silencio durante los dos segundos.

Los protocolos generalmente no describen *cómo* cumplir 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 detecta errores el servidor, aunque sí describe qué hace el servidor si se produce un 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 tipo de sistema operativo desde cualquier lugar de Internet.

Muchos tipos de dispositivos pueden comunicarse con los mismos conjuntos de protocolos. Esto se debe a que los protocolos especifican la funcionalidad de red, no la tecnología subyacente para admitir esta funcionalidad.



2.4 Uso de modelos en capas

2.4.1 Beneficios del uso de un modelo en capas

Para visualizar la interacción entre varios protocolos, es común utilizar un modelo en capas. Un modelo en capas muestra el funcionamiento de los protocolos que se produce dentro de cada capa, como así también la interacción de las capas sobre y debajo de él.

Existen beneficios al utilizar un modelo en capas para describir los protocolos de red y el funcionamiento. Uso de un modelo en capas:

- Asiste en el diseño del protocolo, porque los protocolos que operan en una capa específica poseen información definida que van a poner en práctica y una interfaz definida según las capas por encima y por debajo.
- 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 red.

2.4.2 Modelos de protocolo y referencia

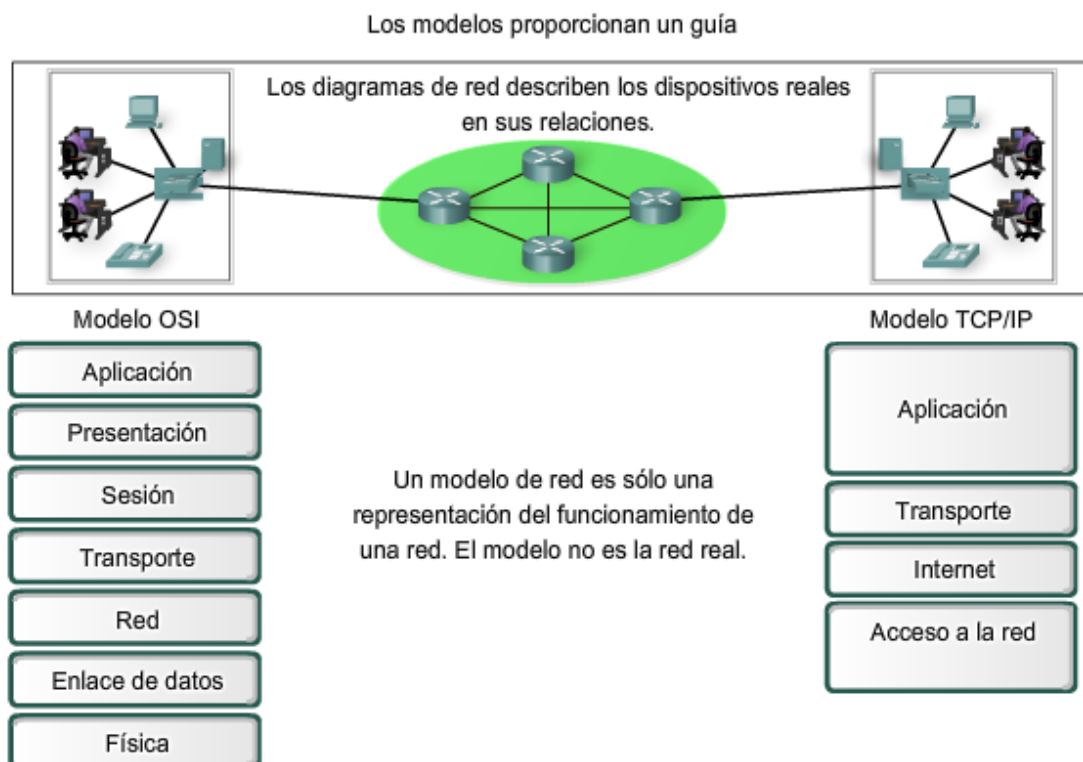
Existen dos tipos básicos de modelos de networking: modelos de protocolo y modelos de referencia.

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 modelo de protocolo porque describe las funciones que se producen en cada capa de los protocolos dentro del conjunto TCP/IP.

Un modelo de referencia proporciona una referencia común para mantener consistencia en 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 propósito principal de un modelo de referencia es asistir en la comprensión más clara de las funciones y los procesos involucrados.

El modelo de interconexión de sistema abierto (OSI) es el modelo de referencia de internetwork más ampliamente conocido. Se utiliza para el diseño de redes de datos, especificaciones de funcionamiento y resolución de problemas.

Aunque los modelos TCP/IP y OSI son los modelos principales que se utilizan cuando se analiza la funcionalidad de red, los diseñadores de protocolos de red, servicios o dispositivos pueden crear sus propios modelos para representar sus productos. Por último, se solicita a los diseñadores que se comuniquen con la industria asociando sus productos o servicios con el modelo OSI, el modelo TCP/IP o ambos.

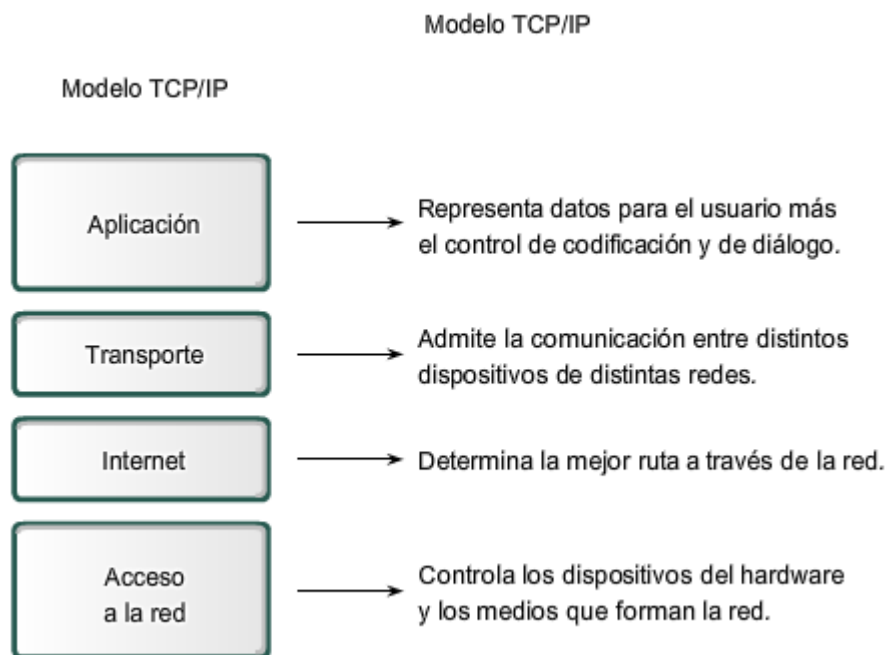


2.4.3 Modelo TCP/IP

El primer modelo de protocolo en capas para comunicaciones de internet 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 tener lugar 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 lo 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 (RFCs). 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. Esos protocolos, que se implementan tanto en el host emisor como en el receptor, interactúan para proporcionar la entrega de aplicaciones de extremo a extremo a través de una red.

Un proceso completo de comunicación incluye estos pasos:

1. Creación de datos a nivel de la capa de aplicación del dispositivo final origen.
2. Segmentación y [encapsulación](#) de datos cuando pasan por la stack de protocolos en el dispositivo final de origen.
3. Generación de los datos sobre el medio en la capa de acceso a la red de la stack.
4. Transporte de los datos a través de la internetwork, que consiste de los medios y de cualquier dispositivo intermediario.
5. Recepción de los datos en la capa de acceso a la red del dispositivo final de destino.
6. Desencapsulación y rearmado de los datos cuando pasan por la stack en el dispositivo final.
7. Traspaso de estos datos a la aplicación de destino en la capa de aplicación del dispositivo final de destino.

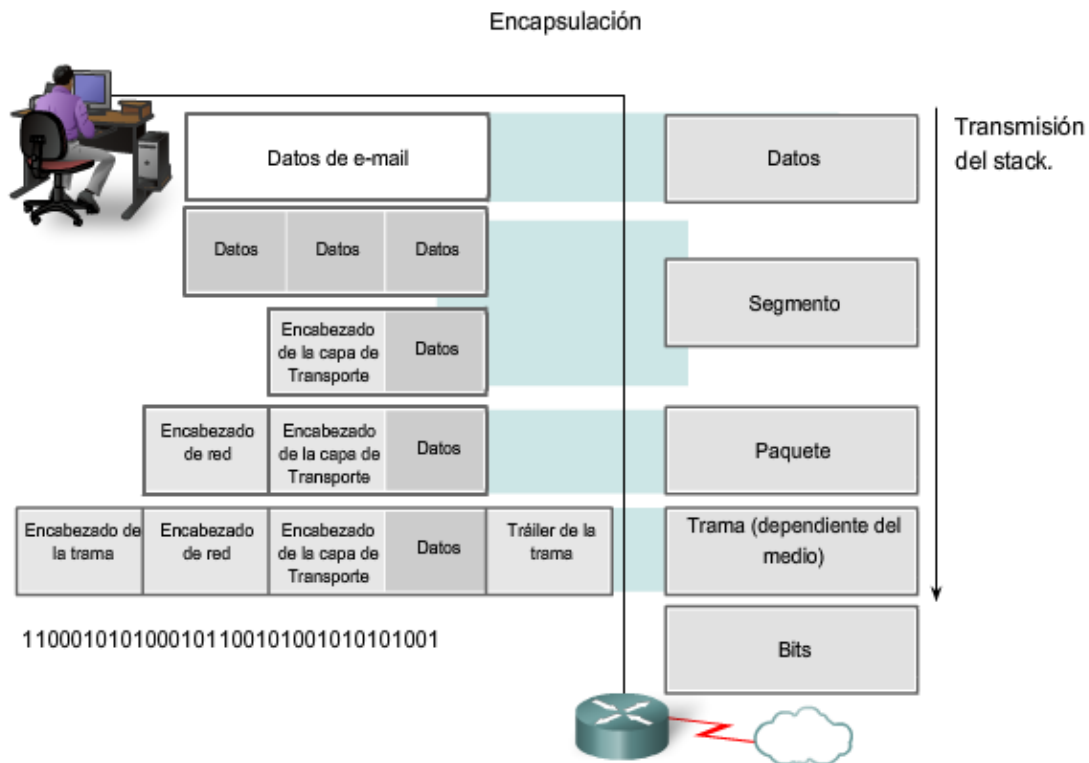


2.4.5 Unidad de datos del protocolo y encapsulación

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 superior 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 TCP/IP.

- Datos: el término general para las PDU que se utilizan en la capa de aplicación.
- Segmento: PDU de la capa de transporte.
- Paquete: PDU de la capa de Internetwork.
- Trama: PDU de la capa de acceso a la red.
- Bits: una PDU que se utiliza cuando se transmiten físicamente datos a través de un medio.



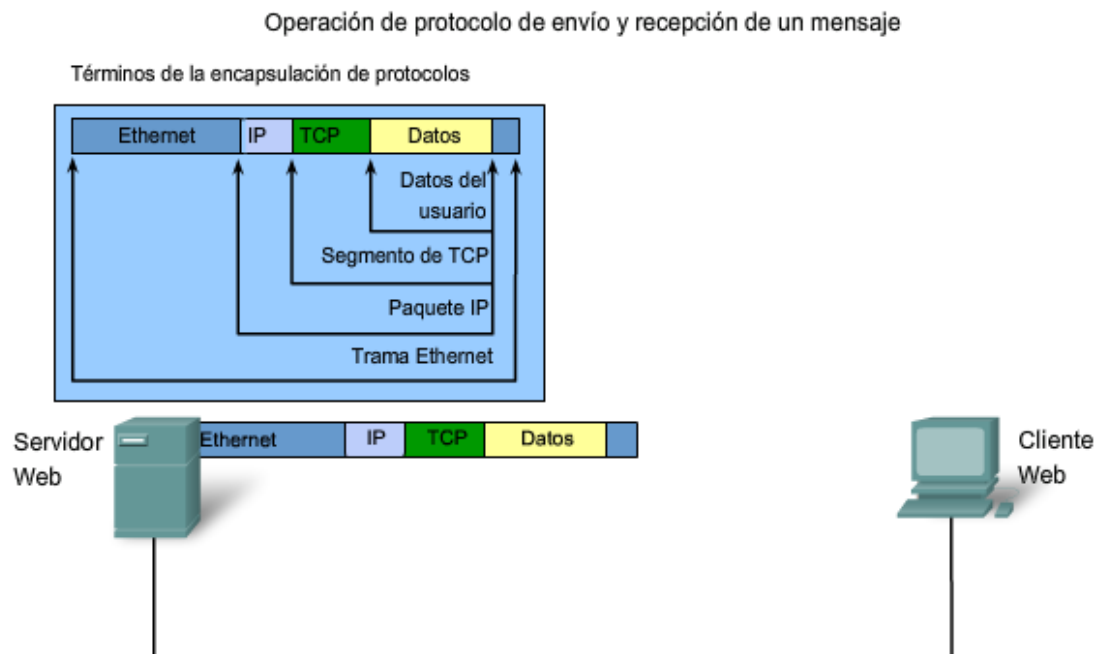
2.4.6 Proceso de envío y recepción

Cuando se envían mensajes en una red, el stack del protocolo de un host funciona desde arriba hacia abajo. 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 Transporte. Allí, los datos de aplicación se dividen en segmentos TCP. A cada segmento 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 nuevamente los datos a su formato original.

La capa Transporte encapsula los datos HTML de la página Web dentro del segmento y los envía a la capa Internet, donde se implementa el protocolo IP. Aquí, el segmento TCP en su totalidad es encapsulado 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 correspondiente proceso de destino.

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 el servidor NIC.



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 marco 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 basada en TCP/IP y la proporción en la que se expandió ocasionaron que el desarrollo y la aceptación de la suite de protocolos OSI quedaran atrás. Aunque pocos de los protocolos desarrollados mediante las especificaciones OSI son de uso masivo en la actualidad, el modelo OSI de siete capas ha realizado aportes importantes para el desarrollo de otros protocolos y productos para todos los tipos de nuevas redes.

Como modelo de referencia, el modelo OSI proporciona una amplia lista de funciones y servicios que pueden producirse 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 estructurará en torno al modelo OSI, el eje del análisis serán 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 Aplicación del modelo TCP/IP están subdivididas para describir funciones discretas que deben producirse en estas capas.

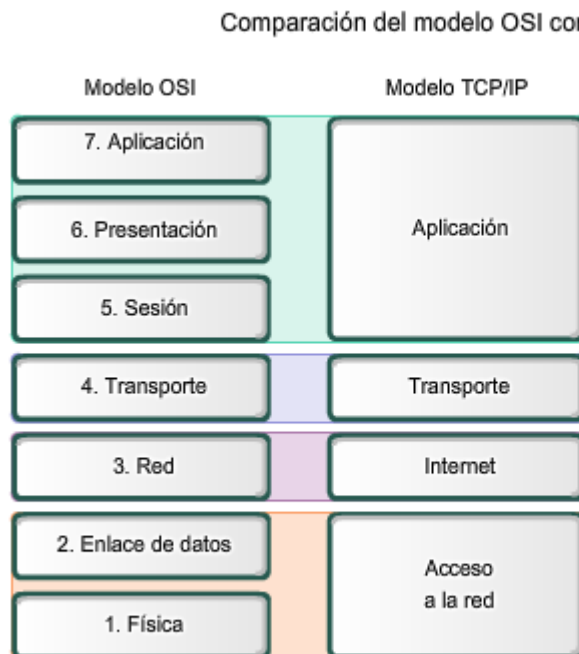
En la capa Acceso a la red, la suite de protocolos TCP/IP no especifica cuáles protocolos utilizar cuando se transmite por un medio físico; sólo describe la transferencia desde la capa de Internet a los protocolos de red física. Las Capas OSI 1 y 2 analizan los procedimientos necesarios para tener acceso a los medios y los medios físicos para enviar datos por una red.

Los paralelos clave entre dos modelos de red se producen en las Capas 3 y 4 del modelo OSI. La Capa 3 del modelo OSI, la capa Red, se utiliza casi universalmente para analizar y documentar el rango de 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 Transporte del modelo OSI, con frecuencia se utiliza para describir servicios o funciones generales que administran conversaciones individuales entre los hosts de origen y de destino. Estas funciones incluyen acuse de recibo, [recuperación de errores](#) y secuenciamiento. En esta capa, los protocolos TCP/IP, Protocolo de control de

transmisión (TCP) y [Protocolo de datagramas de usuario \(UDP\)](#) proporcionan la funcionalidad necesaria.

La capa de aplicación TCP/IP incluye una cantidad de protocolos que propocionan funcionalidad específica para 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.



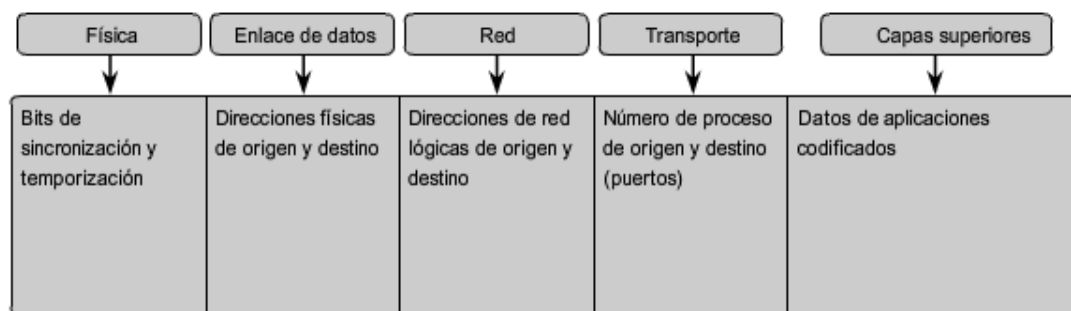
Las semejanzas claves están en la capa de Red y de Transporte.

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.

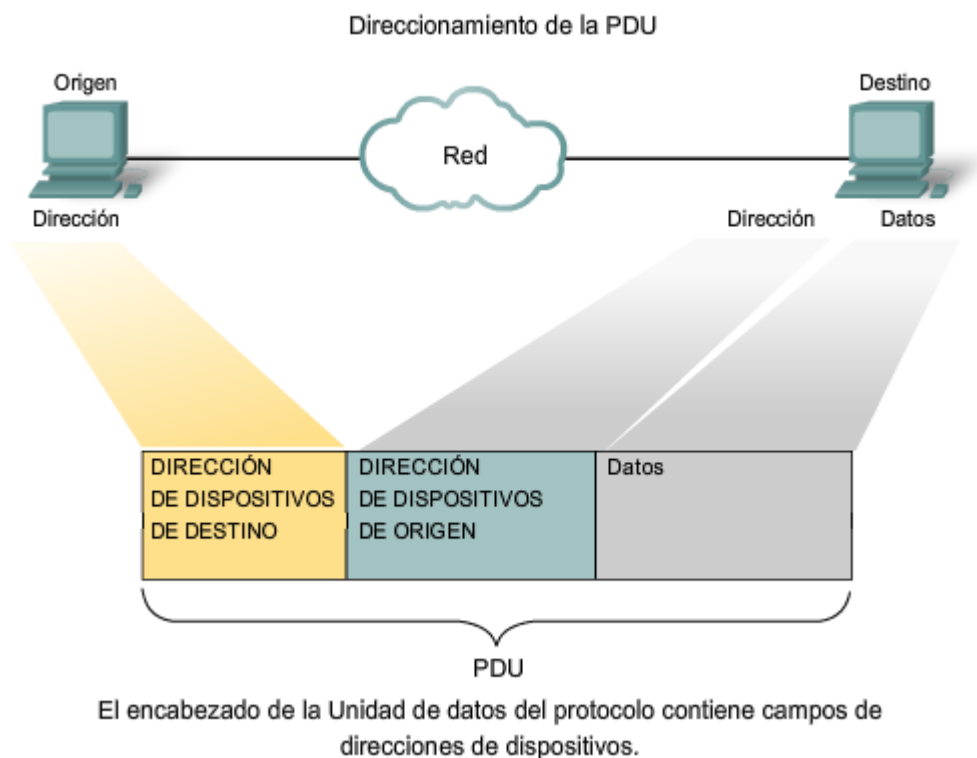
Existen varios tipos de direcciones que deben incluirse para entregar satisfactoriamente los datos desde una aplicación de origen que se ejecuta en un host hasta la aplicación de destino correcta que se ejecuta en otro. Al utilizar el modelo OSI como guía, se pueden observar las distintas direcciones e identificadores necesarios en cada capa.



2.5.2 Envío 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 existen múltiples capas de protocolos que preparan los datos para transmitirlos a sus destinos, existen múltiples capas de direccionamiento para asegurar la entrega.

El primer identificador, la dirección física del host, aparece en el encabezado de la PDU de Capa 2, llamado 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 al medio (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 Transporte de datos a través de internetwork

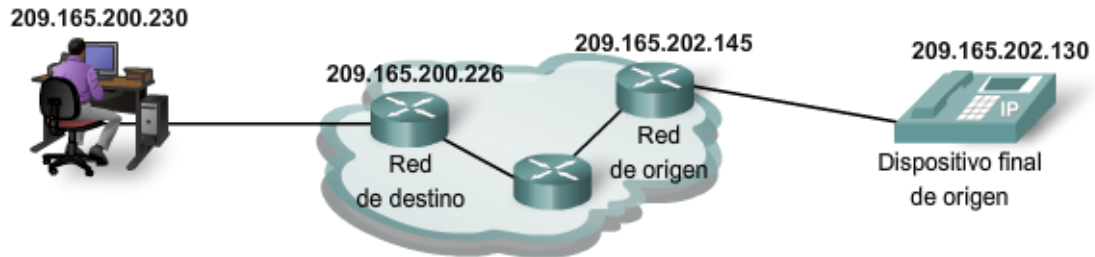
Los protocolos de Capa 3 están diseñados principalmente para mover datos desde una red local a otra red local dentro de una internetwork. Mientras las direcciones de Capa 2 sólo se utilizan para comunicar entre dispositivos de una red local única, las direcciones de Capa 3 deben incluir identificadores 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.

Ubicación de las partes en la red correcta

Unidad de datos del protocolo (PDU)				
Destino		Origen		Datos
Dirección de red	Dirección del dispositivo	Dirección de red	Dirección del dispositivo	

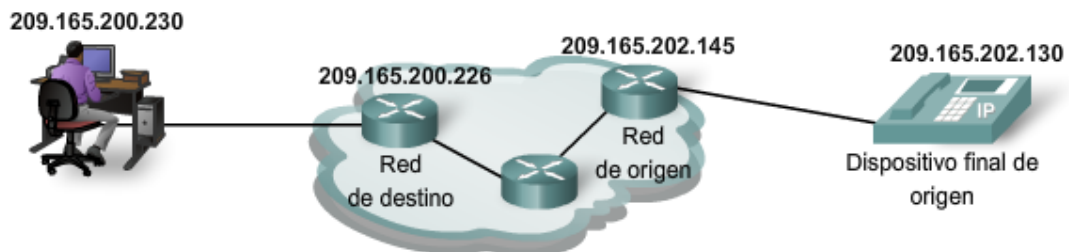
El encabezado de la Unidad de datos del protocolo también contiene la dirección de red.



Ubicación de las partes en la red correcta

Unidad de datos del protocolo (PDU)				
Destino		Origen		Datos
Red 209.165	Dispositivo 200.230	Red 209.165.202	Dispositivo 130	

El encabezado de la Unidad de datos del protocolo también contiene la dirección de red.



2.5.4 Envío de datos a la aplicación correcta

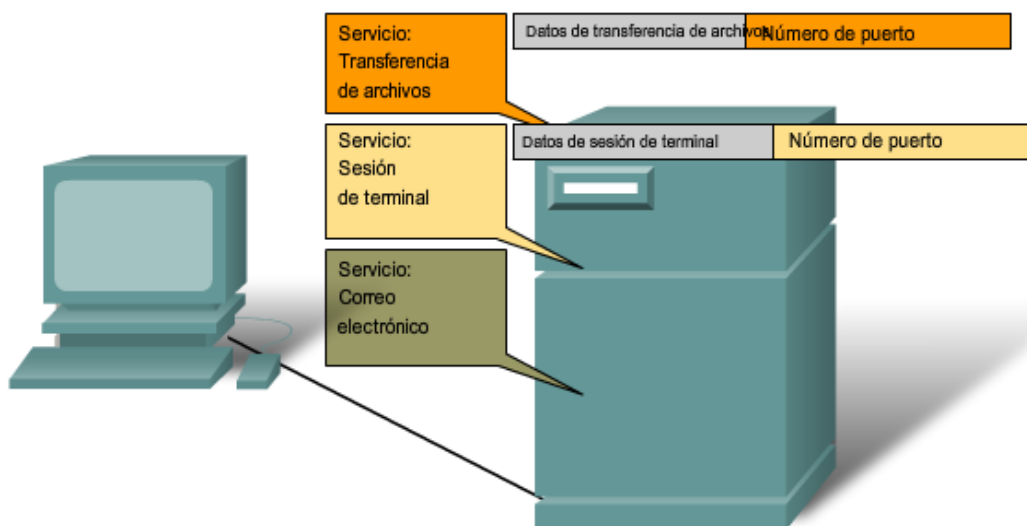
En la Capa 4, la información contenida en el encabezado de la PDU no identifica un host de destino o una red de destino. Lo que sí identifica es el proceso o servicio específico que se ejecuta en el dispositivo host de destino que actuará en los datos que se entregan. Los hosts, sean clientes o servidores 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](#) y, tal vez, incluso 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 cliente de correo electrónico esté enviando o recibiendo un e-mail 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 sola interfaz, sin embargo los mensajes instantáneos no emergen en el medio del documento del procesador de textos o del e-mail que se ve en un juego.

Esto es así porque los procesos individuales que se ejecutan en los hosts de origen y de destino se comunican entre sí. Cada aplicación o servicio es representado 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.

En el dispositivo final, el número de puerto de servicio dirige los datos a la conversación correcta.



Terminología

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 dominante de red de área local.

Dirección MAC: Capa 2 de Ethernet, dirección física.

Dirección IP: [dirección lógica](#)

Máscara de subred de Capa 3: necesario para interpretar la [dirección IP](#).

Gateway por defecto: 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 permite a un dispositivo final participar en una red.

Puerto (hardware): interfaz que le permite a un dispositivo red participar en la red 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 (típicas direcciones MAC Ethernet).

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.

Paquete: PDU de Capa 3.