Los protocolos de capa física describen los medios mecánicos, eléctricos, funcionales y de procedimiento para activar, mantener y desactivar conexiones físicas para la transmisión de bits hacia un dispositivo de red y desde él.

Los protocolos de capa de enlace de datos describen los métodos para intercambiar tramas de datos entre dispositivos en un medio común.

La capa de red proporciona servicios para intercambiar los datos individuales en la red entre dispositivos finales identificados.

La capa de transporte define los servicios para segmentar, transferir y rearmar los datos para las comunicaciones individuales entre dispositivos finales.

La capa de sesión proporciona servicios a la capa de presentación para organizar su diálogo y administrar el intercambio de datos.

La capa de presentación proporciona una representación común de los datos transferidos entre los servicios de la capa de aplicación.

La capa de aplicación proporciona los medios para la conectividad de extremo a extremo entre individuos de la red humana mediante redes de datos.

Las redes nos conectan cada vez más. Las personas se comunican en línea desde cualquier lugar. Las conversaciones que tienen lugar en las aulas pasan a las sesiones de chat de mensajes instantáneos, y los debates en línea continúan en el lugar de estudios. Diariamente, se desarrollan nuevos servicios para aprovechar la red.

En lugar de crear sistemas exclusivos e independientes para la prestación de cada servicio nuevo, el sector de redes en su totalidad adoptó un marco de desarrollo que permite que los diseñadores comprendan las plataformas de red actuales y las mantengan. Al mismo tiempo, este marco se utiliza para facilitar el desarrollo de nuevas tecnologías, a fin de satisfacer las necesidades de las comunicaciones y las mejoras tecnológicas futuras.

Un aspecto fundamental de este marco de desarrollo es el uso de modelos generalmente aceptados que describen reglas y funciones de red.

En este capítulo, obtendrá información sobre estos modelos, sobre los estándares que hacen que las redes funcionen y sobre la forma en que se produce la comunicación a través de una red.

Una red puede ser tan compleja como los dispositivos conectados a través de Internet, o tan simple como dos PC conectadas directamente entre sí mediante un único cable, o puede tener cualquier grado de complejidad intermedia. Las redes pueden variar en lo que respecta al tamaño, la forma y la función. Sin embargo, realizar simplemente la conexión física entre los dispositivos finales no es suficiente para habilitar la comunicación. Para que se produzca la comunicación, los dispositivos deben saber “cómo” comunicarse.

Las personas intercambian ideas mediante diversos métodos de comunicación. Sin embargo, independientemente del método elegido, todos los métodos de comunicación 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.

La comunicación comienza con un mensaje, o información, que se debe enviar desde un origen hasta un destino. El envío de este mensaje, ya sea mediante comunicación cara a cara o a través de una red, está regido por reglas llamadas “protocolos”. Estos protocolos son específicos del tipo de método de comunicación en cuestión. 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.

Por ejemplo, piense en dos personas que se comunican cara a cara, como se muestra en la figura 1. Antes de comunicarse, deben acordar cómo hacerlo. Si en la comunicación se utiliza la voz, primero deben acordar el idioma. A continuación, cuando tienen un mensaje que compartir, deben poder dar formato a ese mensaje de una manera que sea comprensible. Por ejemplo, si alguien utiliza el idioma español, pero la estructura de las oraciones es deficiente, el mensaje se puede malinterpretar fácilmente. Cada una de estas tareas describe protocolos implementados para lograr la comunicación. Esto es válido para la comunicación por computadora, como se muestra en la figura 2.

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

**Establecimiento de reglas**

Antes de comunicarse entre sí, las personas deben utilizar reglas o acuerdos establecidos que rijan la conversación. Por ejemplo, tenga en cuenta la figura 1, donde los protocolos son necesarios para la comunicación eficaz. Los protocolos que se utilizan son específicos de las características del método de comunicación, incluidas las características del origen, el destino y el canal. Estas reglas, o protocolos, deben respetarse para que el mensaje se envíe y comprenda correctamente. Se encuentran disponibles muchos protocolos que rigen la comunicación humana correcta. Una vez que se acuerda un método de comunicación (cara a cara, teléfono, carta, fotografía), los protocolos implementados deben contemplar los siguientes requisitos:

* Un emisor y un receptor identificados
* Idioma y gramática común
* Velocidad y temporización de la entrega
* Requisitos de confirmación o acuse de recibo

Los protocolos que se utilizan en las comunicaciones de red comparten muchas de las características fundamentales de los protocolos que se utilizan para regir las conversaciones humanas correctas. Consulte la figura 2. Además de identificar el origen y el destino, los protocolos informáticos y de red definen los detalles sobre la forma en que los mensajes se transmiten a través de una red para cumplir con los requisitos anteriores. Si bien hay muchos protocolos que deben interactuar, entre los protocolos informáticos habituales, se incluyen los siguientes:

* Codificación de los mensajes
* Formato y encapsulación del mensaje
* Tamaño del mensaje
* Temporización del mensaje
* Opciones de entrega del mensaje

A continuación, se analizan más detalladamente cada uno de estos protocolos.

**Codificación de los mensajes**

Uno de los primeros pasos para enviar un mensaje es codificarlo. La codificación es el proceso mediante el cual la información se convierte en otra forma aceptable para la transmisión. La decodificación invierte este proceso para interpretar la información.

Imagine a una persona que planifica un viaje de vacaciones con un amigo y llama a ese amigo para analizar los detalles respecto de dónde desean ir, como se muestra en la figura 1. Para comunicar el mensaje, el emisor primero debe convertir, o codificar, sus ideas y percepciones acerca del lugar en palabras. Las palabras se articulan a través del teléfono utilizando los sonidos y las inflexiones del lenguaje oral que transmiten el mensaje. En el otro extremo de la línea telefónica, la persona que está escuchando la descripción recibe los sonidos y los decodifica para visualizar la imagen del atardecer descrita por el emisor.

La codificación también tiene lugar en la comunicación por computadora, como se muestra en la figura 2. La codificación entre hosts debe tener el formato adecuado para el medio. El host emisor, primero convierte en bits los mensajes enviados a través de la red. Cada bit se codifica en un patrón de sonidos, ondas de luz o impulsos electrónicos, según el medio de red a través del cual se transmitan los bits. El host de destino recibe y decodifica las señales para interpretar el mensaje.

**Formato y encapsulación del mensaje**

Cuando se envía un mensaje desde el origen hacia el destino, se debe utilizar un formato o estructura específicos. Los formatos de los mensajes dependen del tipo de mensaje y el canal que se utilice para entregar el mensaje.

La escritura de cartas es una de las formas más comunes de comunicación humana por escrito. Durante siglos, el formato aceptado para las cartas personales no ha cambiado. En muchas culturas, una carta personal contiene los siguientes elementos:

* Un identificador del destinatario
* Un saludo
* El contenido del mensaje
* Una frase de cierre
* Un identificador del emisor

Además de tener el formato correcto, la mayoría de las cartas personales también deben colocarse, o encapsularse, en un sobre para la entrega, como se muestra en la figura 1. El sobre tiene la dirección del emisor y la del receptor, cada una escrita en el lugar adecuado del sobre. Si la dirección de destino y el formato no son correctos, la carta no se entrega. El proceso que consiste en colocar un formato de mensaje (la carta) dentro de otro formato de mensaje (el sobre) se denomina encapsulación. Cuando el destinatario revierte este proceso y quita la carta del sobre se produce la desencapsulación del mensaje.

La persona que escribe la carta utiliza un formato aceptado para asegurarse de que la carta se entregue y de que el destinatario la comprenda. De la misma manera, un mensaje que se envía a través de una red de computadoras sigue reglas de formato específicas para que pueda ser entregado y procesado. De la misma manera en la que una carta se encapsula en un sobre para la entrega, los mensajes de las PC también se encapsulan. Cada mensaje de computadora se encapsula en un formato específico, llamado trama, antes de enviarse a través de la red. Una trama actúa como un sobre: proporciona la dirección del destino propuesto y la dirección del host de origen, como se muestra en la figura 2.

El formato y el contenido de una trama están determinados por el tipo de mensaje que se envía y el canal que se utiliza para enviarlo. Los mensajes que no tienen el formato correcto no se pueden enviar al host de destino o no pueden ser procesados por éste.

**Tamaño del mensaje**

Otra regla de comunicación es el tamaño. Cuando las personas se comunican, los mensajes que envían, normalmente, están divididos en fragmentos más pequeños u oraciones. El tamaño de estas oraciones se limita a lo que la persona que recibe el mensaje puede procesar por vez, como se muestra en la figura 1. Una conversación individual puede estar compuesta por muchas oraciones más pequeñas para asegurarse de que cada parte del mensaje sea recibida y comprendida. Imagine cómo sería leer este curso si todo el contenido apareciera como una sola oración larga; no sería fácil de comprender.

De manera similar, cuando se envía un mensaje largo de un host a otro a través de una red, es necesario dividirlo en partes más pequeñas, como se muestra en la figura 2. Las reglas que controlan el tamaño de las partes, o tramas que se comunican a través de la red, son muy estrictas. También pueden ser diferentes, de acuerdo con el canal utilizado. Las tramas que son demasiado largas o demasiado cortas no se entregan.

Las restricciones de tamaño de las tramas requieren que el host de origen divida un mensaje largo en fragmentos individuales que cumplan los requisitos de tamaño mínimo y máximo. Esto se conoce como segmentación. Cada segmento se encapsula en una trama separada con la información de la dirección y se envía a través de la red. En el host receptor, los mensajes se desencapsulan y se vuelven a unir para su procesamiento e interpretación.

**Temporización del mensaje**

Otro factor que afecta la correcta recepción y comprensión del mensaje es la temporización. Las personas utilizan la temporización para determinar cuándo hablar, la velocidad con la que lo harán y cuánto tiempo deben esperar una respuesta. Éstas son las reglas de la participación.

**Método de acceso**

El método de acceso determina en qué momento alguien puede enviar un mensaje. Estas reglas de temporización se basan en el contexto. Por ejemplo: tal vez usted pueda hablar cada vez que quiera decir algo. En este contexto, una persona debe esperar hasta que nadie más esté hablando antes de comenzar a hablar. Si dos personas hablan a la vez, se produce una colisión de información, y es necesario que ambas se detengan y vuelvan a comenzar, como se muestra en la figura 1. De manera similar, las computadoras deben definir un método de acceso. Los hosts de una red necesitan un método de acceso para saber cuándo comenzar a enviar mensajes y cómo responder cuando se produce algún error.

**Control de flujo**

La temporización también afecta la cantidad de información que se puede enviar y la velocidad con la que puede entregarse. Si una persona habla demasiado rápido, la otra persona tendrá dificultades para escuchar y comprender el mensaje, como se muestra en la figura 2. La persona que recibe el mensaje debe solicitar al emisor que disminuya la velocidad. En las comunicaciones de redes, un host emisor puede transmitir mensajes a una velocidad mayor que la que puede recibir y procesar el host de destino. Los hosts de origen y destino utilizan el control del flujo para negociar la temporización correcta, a fin de que la comunicación sea exitosa.

**Tiempo de espera de respuesta**

Si una persona hace una pregunta y no escucha una respuesta antes de un tiempo aceptable, supone que no habrá ninguna respuesta y reacciona en consecuencia, como se muestra en la figura 3. La persona puede repetir la pregunta o puede continuar la conversación. Los hosts de las redes también tienen reglas que especifican cuánto tiempo deben esperar una respuesta y qué deben hacer si se agota el tiempo de espera para la respuesta.

**Opciones de entrega del mensaje**

Puede ser necesario entregar un mensaje mejor, de distintas maneras, como se muestra en la figura 1. En algunos casos, una persona desea comunicar información a un solo individuo. Otras veces, esa persona puede necesitar enviar información a un grupo de personas simultáneamente o, incluso, a todas las personas de un área. Una conversación entre dos personas constituye un ejemplo de una entrega de uno a uno. Cuando es necesario que un grupo de destinatarios reciba un mismo mensaje de manera simultánea, se necesita una entrega de mensaje de uno a varios o de uno a todos.

También puede ocurrir que el emisor de un mensaje necesite asegurarse de que el mensaje se haya entregado correctamente al destino. En estos casos, es necesario que el receptor envíe una confirmación al emisor. Si no se necesita ningún acuse de recibo, se dice que el envío del mensaje es sin acuse de recibo.

Los hosts en una red utilizan opciones de entrega similares para comunicarse, como se muestra en la figura 2.

Las opciones de entrega de uno a uno se denominan “unicast”, lo que significa que el mensaje tiene un único destino.

Si un host necesita enviar mensajes utilizando una opción de envío de uno a varios, se denomina “multicast”. Multicasting es el envío de un mismo mensaje a un grupo de hosts de destino de manera simultánea.

Si es necesario que todos los hosts de la red reciban el mensaje a la vez, se utiliza el método de broadcast. El broadcasting representa una opción de entrega de mensaje de uno a todos. Además, los hosts tienen requisitos para los mensajes con confirmación que son diferentes de los requisitos para los mensajes sin confirmación.

Al igual que en la comunicación humana, los diversos protocolos informáticos y de red deben poder interactuar y trabajar en conjunto para que la comunicación de red se lleve a cabo correctamente. Un grupo de protocolos interrelacionados que son necesarios para realizar una función de comunicación se denomina “suite de protocolos”. Los hosts y los dispositivos de red implementan las suites de protocolos en software, hardware o ambos.

Una de las mejores formas para visualizar la forma en que los protocolos interactúan dentro de una suite es ver la interacción como un stack. Un stack de protocolos muestra la forma en que los protocolos individuales se implementan dentro de una suite. Los protocolos se muestran 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 envía. Como se muestra en la ilustración, podemos utilizar capas para describir la actividad que tiene lugar en el ejemplo de comunicación cara a cara. En la capa inferior, la capa física, hay 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 se pronuncian realmente. Este es el contenido de la comunicación.

Si fuéramos testigos de esta conversación, realmente no veríamos las capas flotando en el lugar. El uso de capas es un modelo que proporciona una forma de dividir convenientemente una tarea compleja en partes y describir cómo funcionan.

A nivel humano, algunas reglas de comunicación son formales y otras simplemente se sobreentienden, según 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. Los protocolos de red definen un formato y un conjunto de reglas comunes para intercambiar mensajes entre dispositivos. Algunos protocolos de red comunes son IP, HTTP y DHCP.

En las ilustraciones, se muestran los protocolos de red que describen los siguientes procesos:

* La manera en que se da formato o se estructura el mensaje, como se muestra en la figura 1.
* El proceso por el cual los dispositivos de red comparten información sobre rutas con otras redes, como se muestra en la figura 2.
* La manera y el momento en que se transmiten mensajes de error y del sistema entre los dispositivos, como se muestra en la figura 3.
* La configuración y la terminación de sesiones de transferencia de datos, como se muestra en la figura 4

Por ejemplo, IP define la forma en que un paquete de datos se entrega dentro de una red o a una red remota. La información del protocolo IPv4 se transmite en un formato específico de modo que el receptor pueda interpretarlo correctamente. Esto no difiere mucho del protocolo utilizado para escribir la dirección en un sobre al enviar una carta. La información debe respetar un determinado formato, ya que, de lo contrario, la oficina de correos no puede entregar la carta en el destino.

Un ejemplo del uso de una suite de protocolos en comunicaciones de red es la interacción entre un servidor Web y un cliente 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 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 depende de otros protocolos para regular la forma en que los mensajes se transportan 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 partes más pequeñas, llamadas “segmentos”. Estos segmentos se envían entre los procesos del servidor y el cliente Web que se ejecutan en el host de destino. TCP también es responsable de controlar el tamaño y la velocidad a los que se intercambian los mensajes entre el servidor y el cliente.
* **Protocolo de Internet:** IP es responsable de tomar los segmentos con formato de TCP, encapsularlos en paquetes, asignarles las direcciones adecuadas y enviarlos a través del mejor camino hacia el host de destino.
* **Protocolos de acceso a la red:** los protocolos de acceso a la red describen dos funciones principales, la comunicación a través de un enlace de datos y la transmisión física de datos en los medios de red. 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 la forma en que se envían las señales y la forma en que las interpretan los clientes que las reciben. Ethernet constituye un ejemplo de un protocolo de acceso a la red.

Como se indicó anteriormente, una suite de protocolos es un grupo de protocolos que trabajan en forma conjunta para proporcionar servicios integrales de comunicación de red. Las suites de protocolos pueden estar especificadas por un organismo de estandarización o pueden ser desarrolladas por un proveedor.

Los protocolos IP, HTTP y DHCP son todos parte de la suite de protocolos de Internet conocida como protocolo de control de transmisión/IP (TCP/IP). La suite de protocolos TCP/IP es un estándar abierto, lo que significa que estos protocolos están disponibles para el público sin cargo, y cualquier proveedor puede implementar estos protocolos en su hardware o software.

Un protocolo basado en estándares es un proceso o un protocolo que recibió el aval del sector de redes y fue ratificado, o aprobado, por un organismo de estandarización. El uso de estándares en el desarrollo y la implementación de protocolos aseguran que productos de distintos fabricantes puedan interoperar correctamente. 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 ningún dato.

Algunos protocolos son exclusivos. Exclusivo, en este contexto, significa que una compañía o un proveedor controlan la definición del protocolo y cómo funciona. Algunos protocolos exclusivos los pueden utilizar distintas organizaciones con permiso del propietario. Otros, solo se pueden implementar en equipos fabricados por el proveedor exclusivo. AppleTalk y Novell Netware constituyen ejemplos de protocolos exclusivos.

Incluso es posible que varias compañías trabajen conjuntamente para crear un protocolo exclusivo. Es común que un proveedor (o grupo de proveedores) desarrolle un protocolo exclusivo para satisfacer las necesidades de sus clientes y posteriormente ayude a hacer de ese protocolo exclusivo un estándar abierto. Por ejemplo, Ethernet fue un protocolo desarrollado inicialmente por Bob Metcalfe en el XEROX Palo Alto Research Center (PARC) en la década de los setenta. En 1979, Bob Metcalfe creó su propia compañía, 3COM, y trabajó junto con Digital Equipment Corporation (DEC), Intel y Xerox para promover el estándar “DIX” para Ethernet. En 1985, el Instituto de Ingenieros en Electricidad y Electrónica (IEEE) publicó el estándar IEEE 802.3, que era casi idéntico a Ethernet. Actualmente, 802.3 es el estándar común que se utiliza en redes de área local (LAN). Otro ejemplo: más recientemente, Cisco abrió el protocolo de enrutamiento EIGRP como RFC informativa para satisfacer las necesidades de los clientes que desean utilizar el protocolo en una red de varios proveedores.

La suite IP es una suite de protocolos necesaria para transmitir y recibir información mediante Internet. Se conoce comúnmente como TCP/IP, ya que TCP e IP fueron los primeros dos protocolos de red definidos para este estándar. La suite TCP/IP basada en estándares abiertos reemplazó otras suites de protocolos exclusivas de proveedores, como AppleTalk de Apple e Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) de Novell.

La primera red de conmutación de paquetes, antecesora de Internet actual, fue la red Advanced Research Projects Agency Network (ARPANET), que tuvo su origen en 1969 al conectar PC centrales en cuatro ubicaciones. La ARPANET fue fundada por el Departamento de Defensa de los Estados Unidos para que se utilice en universidades y en laboratorios de investigación. Bolt, Beranek and Newman (BBN) fue el contratista que llevó a cabo gran parte del desarrollo inicial de la ARPANET, incluida la creación del primer router conocido como un procesador de mensajes de interfaz (IMP).

En 1973, Robert Kahn y Vinton Cerf comenzaron a trabajar en la suite TCP para desarrollar la siguiente generación de la ARPANET. TCP se diseñó para reemplazar el programa de control de red (NCP) actual de la ARPANET. En 1978, TCP se dividió en dos protocolos: TCP e IP. Posteriormente, se agregaron otros protocolos a la suite de protocolos TCP/IP, entre los que se incluyen Telnet, FTP, DNS y muchos otros.

Haga clic en la línea de tiempo de la ilustración para ver los detalles sobre el desarrollo de otros protocolos y aplicaciones de red.

Actualmente, la suite incluye decenas de protocolos, como se muestra en la figura 1. Haga clic en cada protocolo para ver su descripción. Están organizados en capas y utilizan el modelo de protocolo TCP/IP. Los protocolos TCP/IP están incluidos en la capa de Internet hasta la capa de aplicación cuando se hace referencia al modelo TCP/IP. Los protocolos de capa inferior de la capa de enlace de datos o de la capa de acceso a la red son responsables de enviar el paquete IP a través del medio físico. Estos protocolos de capa inferior son desarrollados por organismos de estandarización, como el IEEE.

La suite de protocolos TCP/IP se implementa como un stack de TCP/IP tanto en los hosts emisores como en los hosts receptores para proporcionar una entrega de extremo a extremo de las aplicaciones a través de la red. Los protocolos 802.3 o Ethernet se utilizan para transmitir el paquete IP a través de un medio físico que utiliza la LAN.

En las figuras 2 y 3, se muestra el proceso de comunicación completo mediante un ejemplo de servidor Web que transmite datos a un cliente.

Haga clic en el botón Reproducir para ver la demostración animada:

**1.** La página de lenguaje de marcado de hipertexto (HTML) del servidor Web es el dato que se va a enviar.

**2.** El encabezado HTTP del protocolo de aplicación se agrega al frente de los datos HTML. El encabezado contiene diversos tipos de información, incluida la versión de HTTP que utiliza el servidor y un código de estado que indica que tiene información para el cliente Web.

**3.** El protocolo de capa de aplicación HTTP entrega los datos de la página Web con formato HTML a la capa de transporte. El protocolo de la capa de transporte TCP se utiliza para administrar la conversación individual entre el servidor Web y el cliente Web.

**4.** Luego, la información IP se agrega al frente de la información TCP. IP asigna las direcciones IP de origen y de destino que corresponden. Esta información se conoce como paquete IP.

**5.** El protocolo Ethernet agrega información en ambos extremos del paquete IP, conocidos como la “trama de enlace de datos”. Esta trama se envía al router más cercano a lo largo de la ruta hacia el cliente Web. Este router elimina la información de Ethernet, analiza el paquete IP, determina el mejor camino para el paquete, coloca el paquete en una trama nueva y lo envía al siguiente router vecino hacia el destino. Cada router elimina y agrega información de enlace de datos nueva antes de reenviar el paquete.

**6.** Estos datos ahora se transportan a través de la internetwork, que consta de medios y dispositivos intermediarios.

**7.** El cliente recibe las tramas de enlace de datos que contienen los datos, y cada encabezado de protocolo se procesa y, a continuación, se elimina en el orden opuesto al que se agregó. La información de Ethernet se procesa y se elimina, seguida por la información del protocolo IP, luego la información de TCP y, finalmente, la información de HTTP.

**8.** A continuación, la información de la página Web se transfiere al software de explorador Web del cliente.

Los estándares abiertos fomentan la competencia y la innovación. También garantizan que ningún producto de una sola compañía pueda monopolizar el mercado o tener una ventaja desleal sobre la competencia. La compra de un router inalámbrico para el hogar constituye un buen ejemplo de esto. Existen muchas opciones distintas disponibles de diversos proveedores, y todas ellas incorporan protocolos estándares, como IPv4, DHCP, 802.3 (Ethernet) y 802.11 (LAN inalámbrica). Estos estándares abiertos también permiten que un cliente con el sistema operativo OS X de Apple descargue una página Web de un servidor Web con el sistema operativo Linux. Esto se debe a que ambos sistemas operativos implementan los protocolos de estándar abierto, como los de la suite TCP/IP.

Los organismos de estandarización son importantes para mantener una Internet abierta con especificaciones y protocolos de libre acceso que pueda implementar cualquier proveedor. Los organismos de estandarización pueden elaborar un conjunto de reglas en forma totalmente independiente o, en otros casos, pueden seleccionar un protocolo exclusivo como base para el estándar. Si se utiliza un protocolo exclusivo, suele participar el proveedor que creó el protocolo.

Los organismos de estandarización generalmente son organismos sin fines de lucro y neutrales en lo que respecta a proveedores, que se establecen para desarrollar y promover el concepto de estándares abiertos.

Entre los organismos de estandarización, se incluyen los siguientes:

* Internet Society (ISOC)
* Internet Architecture Board (IAB)
* Internet Engineering Task Force (IETF)
* Instituto de Ingenieros en Electricidad y Electrónica (IEEE)
* International Organization for Standardization (ISO)

Cada uno de estos organismos se analizará en mayor detalle en las próximas páginas.

En la ilustración, haga clic en cada logotipo para ver la información sobre los estándares.

La Internet Society (ISOC) es responsable de promover el desarrollo, la evolución y el uso abiertos de Internet en todo el mundo. ISOC facilita el desarrollo abierto de estándares y protocolos para la infraestructura técnica de Internet, incluida la supervisión del Internet Architecture Board (IAB).

El Internet Architecture Board (IAB) es responsable de la administración y el desarrollo general de los estándares de Internet. El IAB supervisa la arquitectura para los protocolos y los procedimientos que utiliza Internet. El IAB consta de 13 miembros, entre los que se incluye el presidente del Internet Engineering Task Force (IETF). Los miembros del IAB actúan como personas, y no como representantes de compañías, agencias u otros organismos.

La misión del IETF es desarrollar, actualizar y mantener Internet y las tecnologías TCP/IP. Una de las responsabilidades clave del IETF es producir documentos de solicitud de comentarios (RFC), que son un memorándum que describe protocolos, procesos y tecnologías para Internet. El IETF consta de grupos de trabajo (WG), el mecanismo principal para desarrollar las pautas y especificaciones del IETF. Los WG son a corto plazo, y después de que se cumplen los objetivos del grupo, se pone fin al WG. El Internet Engineering Steering Group (IESG) es responsable de la administración técnica del IETF y el proceso de los estándares de Internet.

The Internet Research Task Force (IRTF) se centra en la investigación a largo plazo relacionada con los protocolos, las aplicaciones, la arquitectura y las tecnologías de TCP/IP y de Internet. Mientras que el IETF se centra en problemas más a corto plazo de la creación de estándares, el IRTF consta de grupos de investigación para esfuerzos de desarrollo a largo plazo. Algunos de los grupos de investigación actuales incluyen Anti-Spam Research Group (ASRG), Crypto Forum Research Group (CFRG), Peer-to-Peer Research Group (P2PRG) y Router Research Group (RRG).

El Instituto de Ingenieros en Electricidad y Electrónica (IEEE, que se pronuncia “I, triple E”) es un organismo profesional para aquellos que trabajan en los campos de la electrónica y de la ingeniería eléctrica y se dedican a promover la innovación tecnológica y crear estándares. A partir de 2012, el IEEE consta de 38 sociedades, publica 130 diarios y patrocina más de 1300 conferencias cada año en todo el mundo. El IEEE tiene más de 1300 estándares y proyectos actualmente en desarrollo.

El IEEE tiene más de 400 000 miembros en más de 160 países. Más de 107 000 de esos miembros son miembros estudiantes. El IEEE proporciona oportunidades de mejora en el ámbito educativo y laboral para promover las habilidades y el conocimiento con el sector de la electrónica.

El IEEE es una de los organismos de estandarización líderes en el mundo. Crea y mantiene estándares que influyen en una amplia variedad de sectores, como energía, salud, telecomunicaciones y redes. La familia de estándares IEEE 802 se ocupa de redes de área local y redes de área metropolitana, incluidas tanto las redes conectadas por cable como las inalámbricas. Como se muestra en la ilustración, cada estándar del IEEE consta de un WG que se encarga de crear y mejorar los estándares.

Los estándares IEEE 802.3 e IEEE 802.11 son estándares IEEE importantes en redes de computadoras. El estándar IEEE 802.3 define el control de acceso al medio (MAC) para Ethernet por cable. Esta tecnología generalmente es para las LAN, pero también tiene aplicaciones para redes de área extensa (WAN). El estándar 802.11 define un conjunto de estándares para implementar redes de área local inalámbricas (WLAN). Este estándar define el MAC físico y de enlace de datos del modelo de interconexión de sistema abierto (OSI) para las comunicaciones inalámbricas.

La ISO, la International Organization for Standardization, es el mayor desarrollador del mundo de estándares internacionales para una amplia variedad de productos y servicios. ISO no es un acrónimo del nombre del organismo; por el contrario, el término proviene de la palabra griega “isos”, que significa “igual”. La International Organization for Standardization eligió el término ISO para afirmar su posición como igualitaria para todos los países.

En redes, la ISO se conoce principalmente por su modelo de referencia de interconexión de sistema abierto (OSI). La ISO publicó el modelo de referencia OSI en 1984 para desarrollar un esquema en capas para los protocolos de red. El objetivo original de este proyecto era no solo crear un modelo de referencia sino también servir como base para una suite de protocolos que se fuera a usar para Internet. Esto se conoció como la “suite de protocolos OSI”. Sin embargo, debido a la creciente popularidad de la suite TCP/IP, desarrollada por Robert Kahn, Vinton Cerf y otros, no se eligió la suite de protocolos OSI como la suite de protocolos para Internet. En cambio, se seleccionó la suite de protocolos TCP/IP. La suite de protocolos OSI se implementó en equipos de telecomunicaciones y aún puede encontrarse en redes de telecomunicaciones antiguas.

Es posible que conozca algunos de los productos que utilizan estándares ISO. La extensión de archivo ISO se utiliza en muchas imágenes de CD para indicar que utiliza el estándar ISO 9660 para el sistema de archivos. La ISO también es responsable de crear estándares para protocolos de enrutamiento.

Los estándares de redes incluyen otros varios organismos de estandarización. Algunos de los más comunes son los siguientes:

* **EIA:** la Electronic Industries Alliance (EIA), conocida anteriormente como Electronics Industries Association, es un organismo internacional comercial y de estandarización para organizaciones de la industria electrónica. La EIA es conocida principalmente por sus estándares relacionados con el cableado eléctrico, los conectores y los bastidores de 19 in que se utilizan para montar equipos de red.
* **TIA:** la Telecommunications Industry Association (TIA) es responsable de desarrollar estándares de comunicación en diversas áreas, entre las que se incluyen equipos de radio, torres de telefonía móvil, dispositivos de voz sobre IP (VoIP) y comunicaciones satelitales. Muchos de los estándares se crean en colaboración con la EIA.
* **UIT-T:** el Sector de Normalización de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones (UIT-T) es uno de los organismos de estandarización de comunicación más grandes y más antiguos. El UIT-T define estándares para la compresión de videos, televisión de protocolo de Internet (IPTV) y comunicaciones de banda ancha, como la línea de suscriptor digital (DSL). Por ejemplo, al marcar a otro país, se utilizan los códigos de país de la UIT para realizar la conexión.
* **ICANN:** la Internet Corporation for Assigned Names and Numbers (ICANN) es un organismo sin fines de lucro con base en los Estados Unidos que coordina la asignación de direcciones IP, la administración de nombres de dominio utilizados por DNS y los identificadores de protocolo o los números de puerto utilizados por los protocolos TCP y UDP. ICANN crea políticas y tiene una responsabilidad general sobre estas asignaciones.
* **IANA:** la Internet Assigned Numbers Authority (IANA) es un departamento de ICANN responsable de controlar y administrar la asignación de direcciones IP, la administración de nombres de dominio y los identificadores de protocolo para ICANN.

Conocer los organismos que crean estándares que se utilizan en redes lo ayudará a obtener una mayor comprensión de la forma en que estos estándares crean una Internet abierta y neutral en lo que respecta a proveedores, y le permitirá obtener información sobre nuevos estándares a medida que se desarrollan.

Los modelos en capas, como el modelo TCP/IP, con frecuencia se utilizan para ayudar a visualizar la interacción entre diversos protocolos. Un modelo en capas describe el funcionamiento de los protocolos que se produce en cada capa y la interacción de los protocolos 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 redes.

Existen dos tipos básicos de modelos de redes:

* **Modelo de protocolo:** este modelo coincide con precisión con la estructura de una suite de protocolos determinada. 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 tienen lugar en cada capa de protocolos dentro de una suite TCP/IP.
* **Modelo de referencia:** este modelo es coherente con todos los tipos de servicios y protocolos de red al describir qué es lo que se debe hacer en una capa determinada, pero sin regir la forma en que se debe lograr. 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 mejor entendimiento de las funciones y procesos involucrados.

El modelo 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.

Como se muestra en la ilustración, los modelos TCP/IP y OSI son los modelos principales que se utilizan al hablar de funcionalidad de red. Los diseñadores de protocolos, servicios o dispositivos de red 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.

Inicialmente, el modelo OSI fue diseñado por la ISO 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 exclusivos.

En última instancia, la velocidad a la que fue adoptada 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 que se crearon mediante las especificaciones OSI se utilizan ampliamente en la actualidad, el modelo OSI de siete capas hizo más contribuciones al desarrollo de otros protocolos y productos para todo tipo de redes nuevas.

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. Si bien el contenido de este curso está estructurado en torno al modelo de referencia OSI, el análisis se centra en los protocolos identificados en el modelo de protocolo TCP/IP. Haga clic en cada nombre de la capa para ver los detalles.

**Nota:** mientras que a las capas del modelo TCP/IP se hace referencia solo por el nombre, las siete capas del modelo OSI se mencionan con frecuencia por número y no por nombre. Por ejemplo, la capa física se conoce como capa 1 del modelo OSI.

El modelo de protocolo TCP/IP para comunicaciones de internetwork se creó a principios de la década de los setenta y se conoce con el nombre de modelo de Internet. Como se muestra en la ilustración, define cuatro categorías de funciones que deben ocurrir para que las comunicaciones se lleven a cabo correctamente. La arquitectura de la suite de protocolos TCP/IP sigue la estructura de este modelo. Por lo tanto, el modelo de Internet es conocido normalmente 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 RFC disponibles al público. Las RFC contienen la especificación formal de los protocolos de comunicación de datos y los recursos que describen el uso de los protocolos.

Las RFC también contienen documentos técnicos y organizacionales sobre Internet, entre los que se incluyen las especificaciones técnicas y los documentos de las políticas elaborados por el IETF.

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 de 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 qué protocolos se deben utilizar cuando se transmite por un medio físico, sino que solo describe la transferencia desde la capa de Internet hacia los protocolos de red física. Las capas 1 y 2 de OSI tratan los procedimientos necesarios para acceder a los medios y las maneras físicas de enviar datos a través de una red.

Como se muestra en la ilustración, los paralelismos fundamentales entre los dos modelos de red se producen en las capas 3 y 4 de OSI. La capa 3 de OSI, la capa de red, se utiliza casi universalmente para describir el alcance de los procesos que ocurren en todas las redes de datos para dirigir y enrutar mensajes a través de una internetwork. IP es el protocolo de la suite TCP/IP que incluye la funcionalidad descrita en la capa 3 de OSI.

La capa 4, la capa de transporte del modelo OSI, describe los servicios y las funciones generales que proporcionan la entrega ordenada y confiable de datos 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, el protocolo TCP y el protocolo de datagramas del usuario (UDP) proporcionan la funcionalidad necesaria.

La capa de aplicación de 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 desarrolladores de software de aplicación para fabricar productos que funcionan en redes.

En teoría, una única comunicación, como un video musical o un mensaje de correo electrónico, podría enviarse a través de una red desde un origen hasta 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:

* Al enviar partes individuales más pequeñas del origen al destino, se pueden intercalar muchas conversaciones diversas en la red. El proceso que se utiliza para intercalar las piezas de conversaciones separadas en la red se denomina multiplexación. Haga clic en cada botón de la figura 1 y, a continuación, haga clic en el botón Reproducir para ver las animaciones de segmentación y de multiplexación.
* 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, solo 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 solo cabe una. El proceso de escribir la dirección, etiquetar, enviar, recibir y abrir los 100 sobres requeriría mucho tiempo tanto para el emisor 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 pueda volverse a armar en el contenido del mensaje original, como se muestra en la figura 2.

Varios tipos de dispositivos en toda la red participan para asegurar que las partes del mensaje lleguen a los destinos de manera confiable.

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 porción 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 sus nuevas funciones. Aunque no existe una convención universal de nomenclatura para las PDU, en este curso se denominan de acuerdo con los protocolos de la suite TCP/IP, como se muestra en la ilustración:

* **Datos:** término general para la PDU que se utiliza en la capa de aplicación.
* **Segmento:** PDU de la capa de transporte.
* **Paquete:** PDU de la capa de red
* **Trama:** PDU de la capa de enlace de datos
* **Bits:** PDU de la capa física que se utiliza cuando se transmiten datos físicamente por el medio

La encapsulación de datos es el proceso que agrega la información adicional del encabezado del protocolo a los datos antes de la transmisión. En la mayoría de las formas de comunicaciones de datos, los datos originales se encapsulan o envuelven en varios protocolos antes de transmitirse.

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 capa de 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 que permite que el proceso de destino rearme los datos 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.

A continuación, el paquete IP se envía a la capa de acceso a la red, donde se encapsula dentro de un encabezado de trama y 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. Por último, los bits se codifican en el medio mediante la tarjeta de interfaz de red (NIC) del servidor. Haga clic en el botón Reproducir de la ilustración para ver el proceso de encapsulación.

Este proceso se invierte en el host receptor, y se conoce como “desencapsulación”. La desencapsulación es el proceso que utilizan los dispositivos receptores para eliminar uno o más de los encabezados de protocolo. Los datos se desencapsulan mientras suben por el stack hacia la aplicación del usuario final. Haga clic en el botón Reproducir de la ilustración para ver el proceso de desencapsulación.

El modelo OSI describe los procesos de codificación, asignación de formato, segmentación y encapsulación de datos para la transmisión a través de la red. La capa de red y la capa de enlace de datos son responsables de enviar los datos desde el dispositivo de origen o emisor hasta el dispositivo de destino o receptor. Los protocolos de las dos capas contienen las direcciones de origen y de destino, pero sus direcciones tienen objetivos distintos.

**Dirección de red**

La dirección lógica de la capa de red, o capa 3, contiene la información necesaria para enviar el paquete IP desde el dispositivo de origen hasta el dispositivo de destino. Una dirección IP de capa 3 tiene dos partes: el prefijo de red y la parte de host. Los routers utilizan el prefijo de red para reenviar el paquete a la red adecuada. El último router de la ruta utiliza la parte de host para enviar el paquete al dispositivo de destino.

Los paquetes IP contienen dos direcciones IP:

* **Dirección IP de origen:** la dirección IP del dispositivo emisor.
* **Dirección IP de destino:** la dirección IP del dispositivo receptor. Los routers utilizan la dirección IP de destino para reenviar un paquete a su destino.

**Dirección de enlace de datos**

La dirección física de la capa de enlace de datos, o capa 2, tiene una función distinta. Su propósito es enviar la trama de enlace de datos desde una interfaz de red hasta otra interfaz de red en la misma red. Antes de que un paquete IP pueda enviarse a través de una red conectada por cable o inalámbrica, se debe encapsular en una trama de enlace de datos de modo que pueda transmitirse a través del medio físico, la red real. Las LAN Ethernet y las LAN inalámbricas constituyen dos ejemplos de redes que tienen distintos medios físicos, cada uno con su propio tipo de protocolo de enlace de datos.

El paquete IP se encapsula en una trama de enlace de datos para enviarse a la red de destino. Se agregan las direcciones de enlace de datos de origen y de destino, como se muestra en la ilustración:

* **Dirección de enlace de datos de origen:** la dirección física del dispositivo que envía el paquete. Inicialmente, es la NIC que es el origen del paquete IP.
* **Dirección de enlace de datos de destino:** la dirección física de la interfaz de red del router del siguiente salto o de la interfaz de red del dispositivo de destino.

Para comprender la forma en que la comunicación se lleva a cabo correctamente en la red, es importante entender las funciones de las direcciones de la capa de red y de las direcciones del enlace de datos cuando un dispositivo se comunica con otro dispositivo en la misma red. En este ejemplo, tenemos un equipo cliente, PC1, que se comunica con un servidor de archivos, servidor FTP, en la misma red IP.

**Direcciones de red**

Las direcciones de la capa de red, o direcciones IP, indican la dirección de red y de host del origen y del destino. La porción de red de la dirección será la misma; solamente cambiará la porción de host o de dispositivo de la dirección.

* **Dirección IP de origen:** la dirección IP del dispositivo emisor, es decir, el equipo cliente PC1: 192.168.1.110.
* **Dirección IP de destino:** la dirección IP del dispositivo receptor, el servidor FTP: 192.168.1.9.

**Direcciones de enlaces de datos**

Cuando el emisor y el receptor del paquete IP están en la misma red, la trama de enlace de datos se envía directamente al dispositivo receptor. En una red Ethernet, las direcciones de enlace de datos se conocen como direcciones MAC de Ethernet. Las direcciones MAC son direcciones de 48 bits que están integradas físicamente en la NIC Ethernet. Las direcciones MAC también se conocen como direcciones físicas (BIA).

* **Dirección MAC de origen:** la dirección de enlace de datos, o la dirección MAC de Ethernet, del dispositivo que envía el paquete IP, es decir, PC1. La dirección MAC de la NIC Ethernet de PC1 es AA-AA-AA-AA-AA-AA.
* **Dirección MAC de destino:** cuando el dispositivo receptor está en la misma red que el dispositivo emisor, la dirección MAC de destino es la dirección de enlace de datos del dispositivo receptor. En este ejemplo, la dirección MAC de destino es la dirección MAC del servidor FTP: CC-CC-CC-CC-CC-CC.

Las direcciones de origen y de destino se agregan a la trama de Ethernet. La trama con el paquete IP encapsulado ahora se puede transmitir desde PC1 directamente hasta el servidor FTP.

Ahora debe estar claro que para enviar datos a otro host en la misma LAN, el host de origen debe conocer tanto la dirección física como la dirección lógica del host de destino. Una vez que se conocen estas direcciones, puede crear una trama y enviarla a través de los medios de red. El host de origen puede obtener la dirección IP de destino de diversas maneras. Por ejemplo, puede descubrir la dirección IP mediante el uso del sistema de nombres de dominios (DNS), o puede conocer la dirección IP de destino porque la dirección se introduce en la aplicación en forma manual, como cuando un usuario especifica la dirección IP de un servidor FTP de destino. Sin embargo, ¿cómo determina un host la dirección MAC de Ethernet de otro dispositivo?

La mayoría de las aplicaciones de red dependen de la dirección IP lógica del destino para identificar la ubicación de los hosts entre los que se produce la comunicación. Se requiere la dirección MAC de enlace de datos para enviar el paquete IP encapsulado dentro de la trama de Ethernet a través de la red hasta el destino.

El host emisor utiliza un protocolo denominado “protocolo de resolución de direcciones” (ARP) para descubrir la dirección MAC de cualquiera de los hosts de la misma red local. El host emisor envía un mensaje de solicitud de ARP a toda la LAN. La solicitud de ARP es un mensaje de broadcast. La solicitud de ARP contiene la dirección IP del dispositivo de destino. Cada dispositivo en la LAN examina la solicitud de ARP para ver si contiene su propia dirección IP. Solamente el dispositivo con la dirección IP contenida en la solicitud de ARP responde con una respuesta de ARP. La respuesta de ARP incluye la dirección MAC asociada con la dirección IP en la solicitud de ARP.

El método que utilizan los hosts para enviar mensajes a un destino en una red remota difiere de la manera en la que envían mensajes a un destino en la misma red local. Cuando un host necesita enviar un mensaje a otro host ubicado en la misma red, reenvía el mensaje de manera directa. El host utiliza el ARP para determinar la dirección MAC del host de destino. Incluye la dirección IP de destino dentro del encabezado del paquete y encapsula el paquete en una trama que contiene la dirección MAC del destino y lo reenvía.

Cuando un host necesita enviar un mensaje a una red remota, debe utilizar el router, también conocido como “gateway predeterminado”. El gateway predeterminado es la dirección IP de una interfaz de un router en la misma red que el host emisor.

Es importante que en cada host de la red local se configure la dirección de gateway predeterminado. Si no se define ninguna dirección de gateway predeterminado en la configuración de TCP/IP del host, o si se especifica un gateway predeterminado incorrecto, no se podrán entregar los mensajes dirigidos a hosts de redes remotas.

En la ilustración, los hosts en la LAN utilizan R1 como el gateway predeterminado con la dirección 192.168.1.1 establecida en la configuración de TCP/IP. Si el destino de una PDU se encuentra en una red IP distinta, los hosts envían las PDU al gateway predeterminado en el router para su posterior transmisión.

Sin embargo, ¿cuáles son las funciones de la dirección de la capa de red y de la dirección de la capa de enlace de datos cuando un dispositivo se comunica con un dispositivo en una red remota? En este ejemplo, tenemos un equipo cliente, PC1, que se comunica con un servidor, en este caso un servidor Web, en una red IP diferente.

**Direcciones de red**

Las direcciones IP indican las direcciones de red y de los dispositivos de origen y de destino. Cuando el emisor del paquete se encuentra en una red distinta de la del receptor, las direcciones IP de origen y de destino representan los hosts en redes diferentes. Esto lo indica la porción de red de la dirección IP del host de destino.

* **Dirección IP de origen:** la dirección IP del dispositivo emisor, es decir, el equipo cliente PC1: 192.168.1.110.
* **Dirección IP de destino:** la dirección IP del dispositivo receptor, es decir, el servidor Web: 172.16.1.99.

**Direcciones de enlaces de datos**

Cuando el emisor y el receptor del paquete IP se encuentran en redes diferentes, la trama de enlace de datos de Ethernet no se puede enviar directamente al host de destino, debido a que en la red del emisor no se puede tener acceso directamente al host. La trama de Ethernet se debe enviar a otro dispositivo conocido como “router” o “gateway predeterminado”. En nuestro ejemplo, el gateway predeterminado es R1. R1 tiene una interfaz y una dirección IP que se encuentra en la misma red que PC1. Esto permite que PC1 alcance el router directamente.

* **Dirección MAC de origen:** la dirección MAC de Ethernet del dispositivo emisor, PC1. La dirección MAC de la interfaz Ethernet de PC1 es AA-AA-AA-AA-AA-AA.

**Dirección MAC de destino:** cuando el dispositivo receptor está en una red distinta de la del dispositivo emisor, la dirección MAC de destino es la dirección MAC de Ethernet del gateway predeterminado o el router. En este ejemplo, la dirección MAC de destino es la dirección MAC de la interfaz Ethernet de R1 que está conectada a la red de PC1, que es 11-11-11-11-11-11.

La trama de Ethernet con el paquete IP encapsulado ahora se puede transmitir a R1. R1 reenvía el paquete al destino, el servidor Web. Esto puede significar que R1 reenvía el paquete a otro router o directamente al servidor Web si el destino se encuentra en una red conectada a R1.

¿Cómo hace el dispositivo emisor para determinar la dirección MAC del router?

Cada dispositivo conoce la dirección IP del router a través de la dirección de gateway predeterminado definida en la configuración de TCP/IP. La dirección de gateway predeterminado es la dirección de la interfaz del router conectado a la misma red local que el dispositivo de origen. Todos los dispositivos de la red local utilizan la dirección de gateway predeterminado para enviar mensajes al router. Una vez que el host conoce la dirección IP del gateway predeterminado, puede utilizar ARP para determinar la dirección MAC de ese gateway predeterminado. La dirección MAC del gateway predeterminado entonces se coloca en la trama.

Las redes de datos son sistemas de dispositivos finales, dispositivos intermediarios y medios que conectan los dispositivos. Para que se produzca la comunicación, estos dispositivos deben saber cómo comunicarse.

Estos dispositivos deben cumplir con reglas y protocolos de comunicación. TCP/IP es un ejemplo de una suite de protocolos. La mayoría de los protocolos son creados por organismos de estandarización, como el IETF o el IEEE. El Instituto de Ingenieros en Electricidad y Electrónica es un organismo profesional para las personas que trabajan en los campos de la electrónica y de la ingeniería eléctrica. La ISO, la International Organization for Standardization, es el mayor desarrollador del mundo de estándares internacionales para una amplia variedad de productos y servicios.

Los modelos de redes que más se utilizan son OSI y TCP/IP. Asociar los protocolos que establecen las reglas de las comunicaciones de datos con las distintas capas de estos modelos 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.

Los datos que pasan por el stack del modelo OSI se segmentan en trozos y se encapsulan con direcciones y otras etiquetas. El proceso se revierte a medida que esos trozos se desencapsulan y pasan por el stack de protocolos de destino. El modelo OSI describe los procesos de codificación, formateo, segmentación y encapsulación de datos para transmitir por la red.

La suite de protocolos TCP/IP es un protocolo de estándar abierto que recibió el aval de la industria de redes y fue ratificado, o aprobado, por un organismo de estandarización. La suite de protocolos de Internet es una suite de protocolos necesaria para transmitir y recibir información mediante Internet.

Las unidades de datos del protocolo (PDU) se denominan según los protocolos de la suite TCP/IP: datos, segmento, paquete, trama y bits.

La aplicación de los modelos permite a diversas personas, compañías y asociaciones comerciales analizar las redes actuales y planificar las redes del futuro.