4. Modelos de Referencia

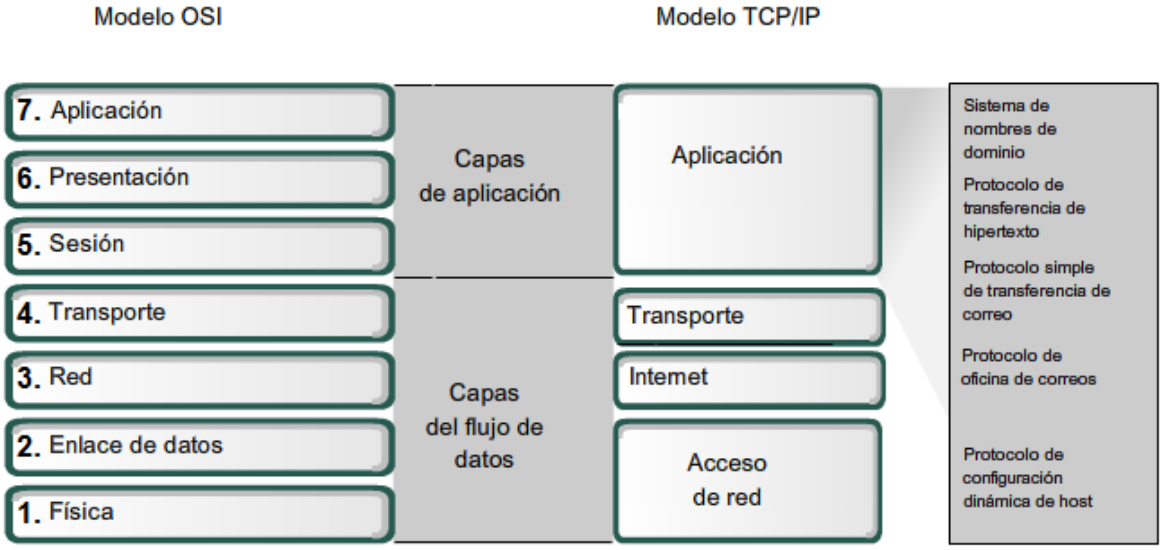
Ya que se analizaron en lo abstracto redes basadas en capas, siendo estos el fundamento para:

- Modelo de referencia OSI.
- Modelo de referencia TCP/IP

4.1. Modelo OSI y TCP/IP

El modelo de interconexión de sistemas abiertos es una representación abstracta en capas, creada como guía para el diseño del protocolo de red. El modelo OSI divide el proceso de networking en diferentes capas lógicas, cada una de las cuales tiene una funcionalidad única y a la cual se le asignan protocolos y servicios específicos.

En este modelo, la información se pasa de una capa a otra, comenzando en la capa de aplicación en el host de transmisión, siguiendo por la jerarquía hacia la capa física y pasando por el canal de comunicaciones al host de destino, donde la información vuelve a la jerarquía y termina en la capa de aplicación. La figura describe los pasos en este proceso.



4.1.1. La capa de aplicación

La séptima capa, es la capa superior de los modelos OSI y TCP/IP. Es la capa que proporciona la interfaz entre las aplicaciones que utilizamos para comunicarnos y la red subyacente en la cual se transmiten los mensajes. Los protocolos de capa de aplicación se utilizan para intercambiar los datos entre los programas que se ejecutan en los hosts de origen y destino. Existen muchos protocolos de capa de aplicación y siempre se desarrollan protocolos nuevos.

Aunque el grupo de protocolos TCP/IP se desarrolló antes de la definición del modelo OSI, la funcionalidad de los protocolos de la capa de aplicación de TCP/IP se adaptan aproximadamente a la estructura de las tres capas superiores del modelo OSI. Capas de aplicación, presentación y sesión.

La mayoría de los protocolos de la capa de aplicación de TCP/IP se desarrollaron antes de la aparición de computadoras personales, interfaces del usuario gráficas y objetos multimedia. Como

resultado, estos protocolos implementan muy poco de la funcionalidad que es especifica en las capas de presentación y sesión del modelo OSI.

Software de la capa de aplicación

Las funciones asociadas con los protocolos de la capa de aplicación permiten a la red humana comunicarse con la red de datos subyacente. Cuando abrimos un explorador Web o una ventana de mensajería instantánea se inicia una aplicación, y el programa se coloca en la memoria del dispositivo donde se ejecuta. Cada programa ejecutable cargado a un dispositivo se denomina proceso.

Dentro de la capa de aplicación, existen dos formas de procesos o programas de software que proporcionan acceso a la red: aplicaciones y servicios.

Aplicaciones reconocidas por la red

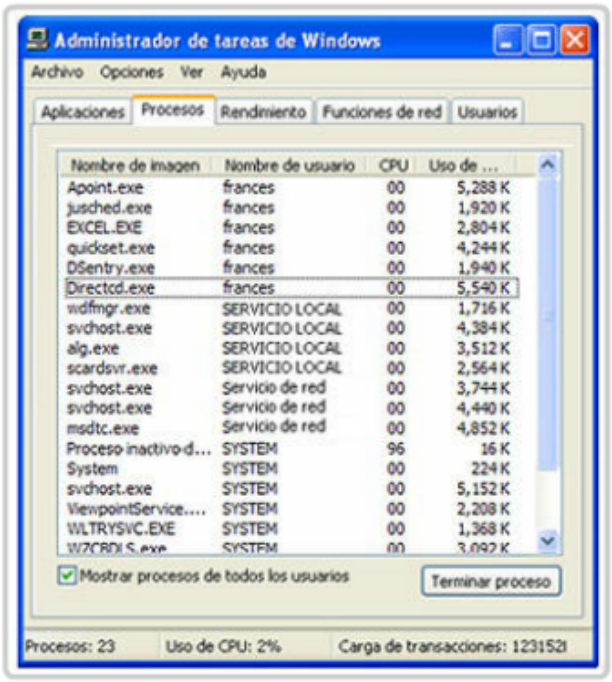
Las aplicaciones son los programas de software que utiliza la gente para comunicarse a través de la red.. Algunas aplicaciones de usuario final son reconocidas por la red, lo cual significa que implementan los protocolos de la capa de aplicación y pueden comunicarse directamente con las capas inferiores del stack de protocolos. Los clientes de correo electrónico y los exploradores Web son ejemplos de este tipo de aplicaciones.

Servicios de la capa de aplicación

Otros programas pueden necesitar la ayuda de los servicios de la capa de aplicación para utilizar los recursos de la red, como transferencia de archivos o cola de impresión en la red. Aunque son transparentes para el usuario, estos servicios son los programas que se comunican con la red y preparan los datos para la transferencia. Diferentes tipos de datos, ya sea texto, gráfico o video, requieren de diversos servicios de red para asegurarse de que estén bien preparados para procesar las funciones de las capas inferiores del modelo OSI.

Cada servicio de red o aplicación utiliza protocolos que definen los estándares y formatos de datos a utilizarse. Sin protocolos, la red de datos no tendría una manera común de formatear y direccionar los datos. Es necesario familiarizarse con los protocolos subyacentes que rigen la operación de los diferentes servicios de red para entender su función.

Procesos de software



Ejemplos de procesos en ejecución en el sistema operativo Windows

Los procesos son programas de software individuales que se ejecutan en forma simultánea.

Los procesos pueden ser

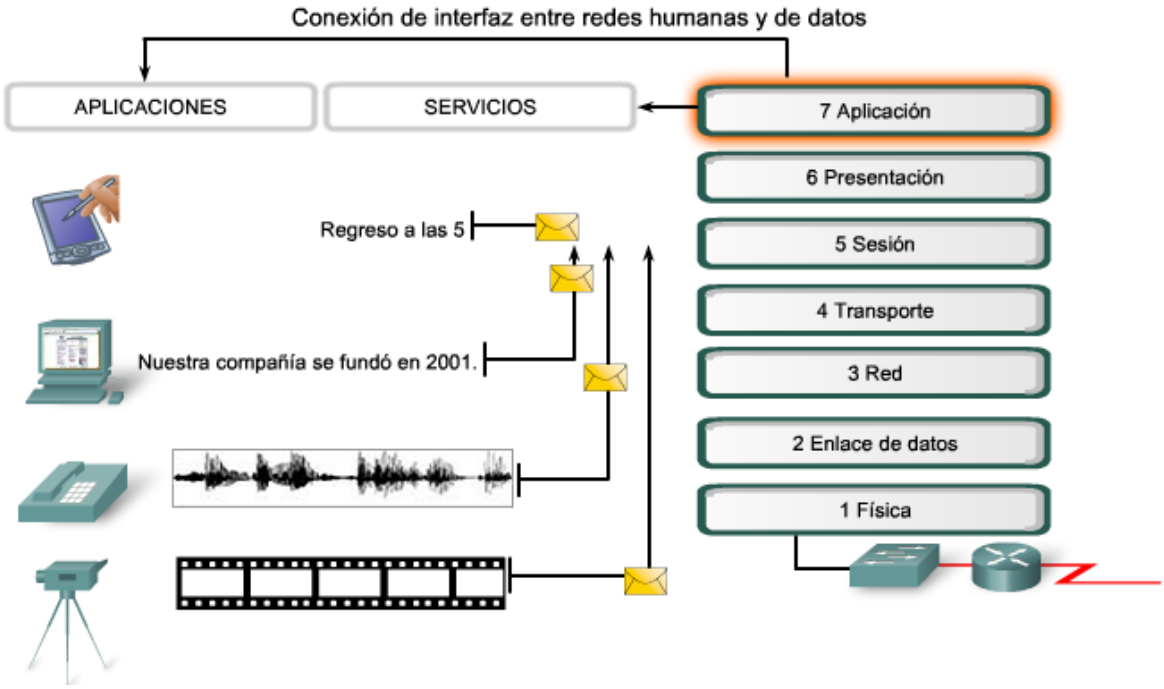
1. Aplicaciones
2. Servicios
3. Operaciones del sistema
4. Un programa puede estar en ejecución varias veces, cada vez dentro de su propio proceso.

Coloque el cursor sobre un elemento.

Aplicación del usuario, servicios y protocolos de capa de aplicación

Como se mencionó anteriormente, la capa de aplicación utiliza los protocolos implementados dentro de las aplicaciones y servicios. Mientras que las aplicaciones proporcionan a las personas una forma de crear mensajes y los servicios de la capa de aplicación establecen una interfaz con la red, los protocolos proporcionan las reglas y los formatos que regulan el trato de los datos. Un solo programa ejecutable debe utilizar los tres componentes e inclusive el mismo nombre. Por ejemplo, al hablar de "Telnet" podemos estar refiriéndonos a la aplicación, al servicio o al protocolo.

En el modelo OSI, las aplicaciones que interactúan directamente con la gente se considera que están en la parte superior del stack, como la misma gente. Al igual que todas las personas dentro del modelo OSI, la capa de aplicación se basa en la funciones de las capas inferiores para completar el proceso de comunicación. Dentro de la capa de aplicación, los protocolos especifican qué mensajes se intercambian entre los host de origen y de destino, la sintaxis de los comandos de control, el tipo y el formato de los datos que se transmiten y los métodos adecuados para notificación y recuperación de errores.



Toma de medidas para las aplicaciones y servicios

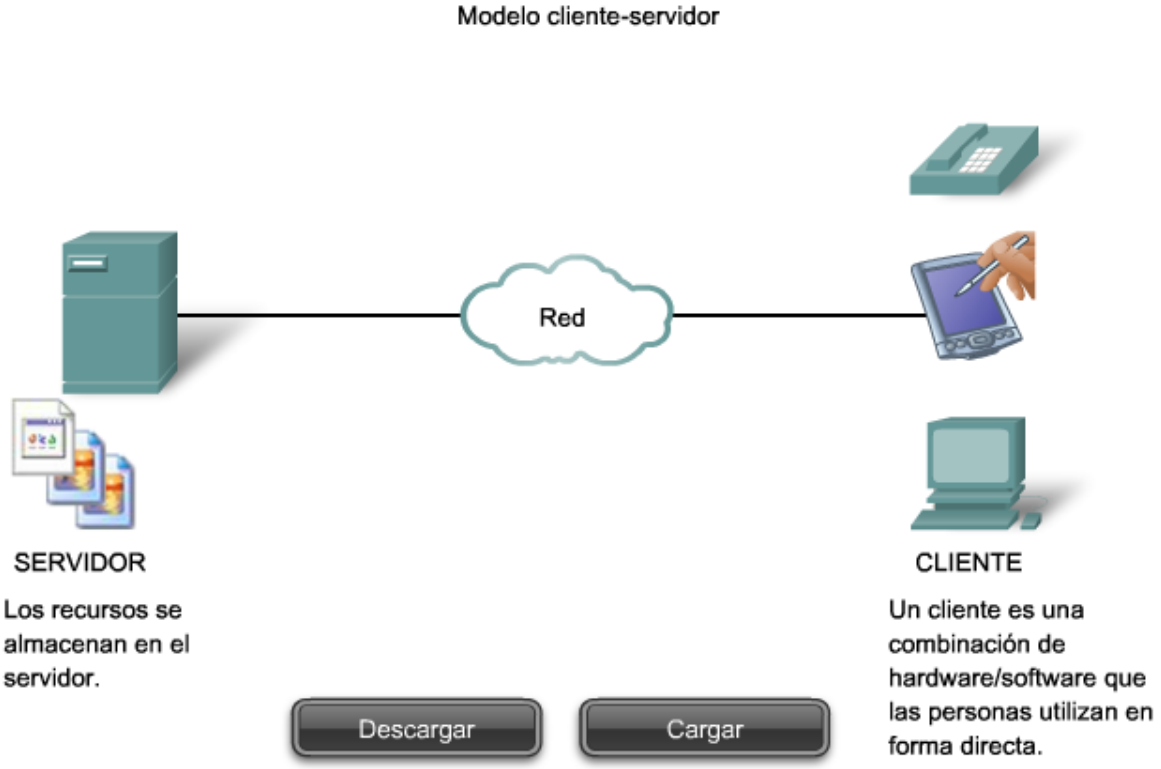
Cuando la gente intenta acceder a información en sus dispositivos, ya sean éstos una computadora personal o portátil, un PDA, un teléfono celular o cualquier otro dispositivo conectado a la red, los datos pueden no estar físicamente almacenados en sus dispositivos. Si así fuera, se debe solicitar permiso al dispositivo que contiene los datos para acceder a esa información.

El modelo cliente-servidor

En el modelo cliente/servidor, el dispositivo que solicita información se denomina cliente y el dispositivo que responde a la solicitud se denomina servidor. Los procesos de cliente y servidor se consideran una parte de la capa de aplicación. El cliente comienza el intercambio solicitando los datos al servidor, quien responde enviando uno o más streams de datos al cliente. Los protocolos de la capa de aplicación describen el formato de las solicitudes y respuestas entre clientes y servidores. Además de la transferencia real de datos, este intercambio puede requerir de información adicional, como la autenticación del usuario y la identificación de un archivo de datos a transferir.

Un ejemplo de una red cliente-servidor es un entorno corporativo donde los empleados utilizan un servidor de correo electrónico de la empresa para enviar, recibir y almacenar correos electrónicos. El cliente de correo electrónico en la computadora de un empleado emite una solicitud al servidor de correo electrónico para un mensaje no leído. El servidor responde enviando al cliente el correo electrónico solicitado.

Aunque los datos se describen generalmente como el flujo del servidor al cliente, algunos datos fluyen siempre del cliente al servidor. El flujo de datos puede ser el mismo en ambas direcciones, o inclusive puede ser mayor en la dirección que va del cliente al servidor. Por ejemplo, un cliente puede transferir un archivo al servidor con fines de almacenamiento. La transferencia de datos de un cliente a un servidor se denomina cargar y de datos de un servidor a un cliente se conoce como descarga.



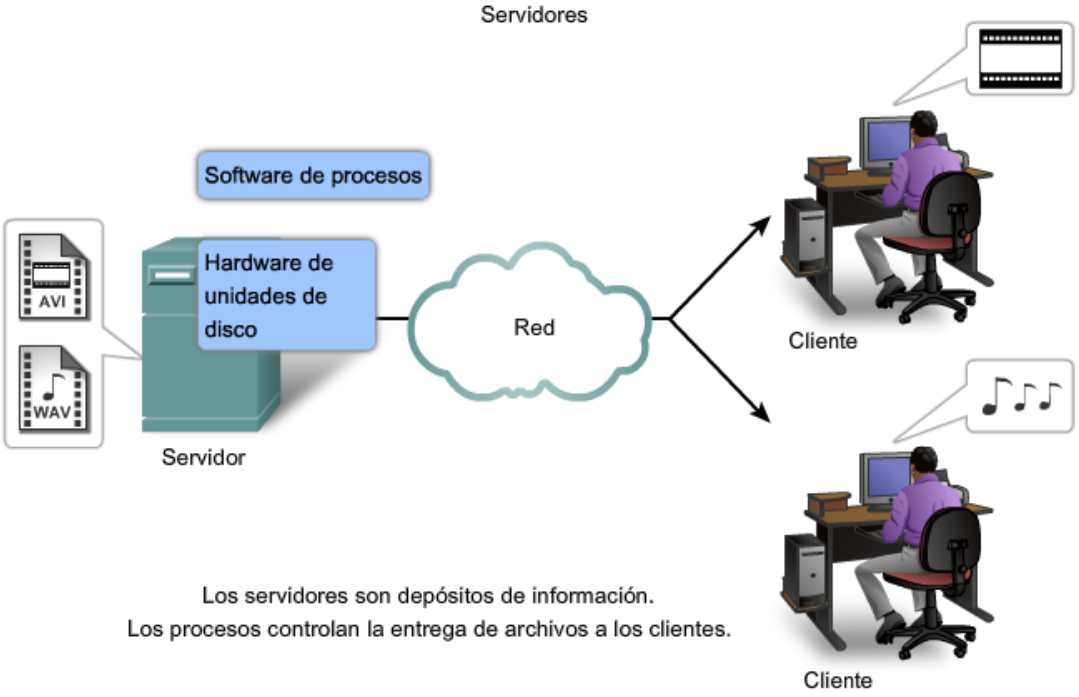
Servidores

En un contexto general de redes, cualquier dispositivo que responde a una solicitud de aplicaciones de cliente funciona como un servidor. Un servidor generalmente es una computadora que contiene información para ser compartida con muchos sistemas de cliente. Por ejemplo, páginas Web, documentos, bases de datos, imágenes, archivos de audio y video pueden almacenarse en un servidor y enviarse a los clientes que lo solicitan. En otros casos, como una impresora de red, el servidor de impresión envía al cliente solicitudes para la impresora que se especifica.

Los diferentes tipos de aplicaciones de servidor pueden tener diferentes requisitos para el acceso del cliente. Algunos servidores pueden requerir de autenticación de la información de cuenta del usuario para verificar si el usuario tiene permiso para acceder a los datos solicitados o para utilizar una operación en particular. Dichos servidores deben contar con una lista central de cuentas de usuarios y autorizaciones, o permisos (para operaciones y acceso a datos) otorgados a cada usuario. Cuando se utiliza un cliente FTP, por ejemplo, si usted pide cargar datos al servidor FTP, se

le puede dar permiso para escribir en su carpeta personal, pero no para leer otros archivos del sitio.

En una red cliente-servidor, el servidor ejecuta un servicio o proceso, a veces denominado daemon. Al igual que la mayoría de los servicios, los demonios generalmente se ejecutan en segundo plano y no se encuentran bajo control directo del usuario. Los demonios se describen como servidores que "escuchan" una solicitud del cliente porque están programados para responder cada vez que el servidor recibe una solicitud para el servicio proporcionado por el demonio. Cuando un demonio "escucha" la solicitud de un cliente, intercambia los mensajes adecuados con el cliente, según lo requerido por su protocolo, y procede a enviar los datos solicitados en el formato correspondiente.



Redes y aplicaciones punto a punto

El modelo punto a punto

Además del modelo cliente-servidor para networking, existe también un modelo punto a punto. Las redes punto a punto tienen dos formas distintivas: diseño de redes punto a punto y aplicaciones punto a punto (P2P). Ambas formas tienen características similares, pero en la práctica son muy diferentes.

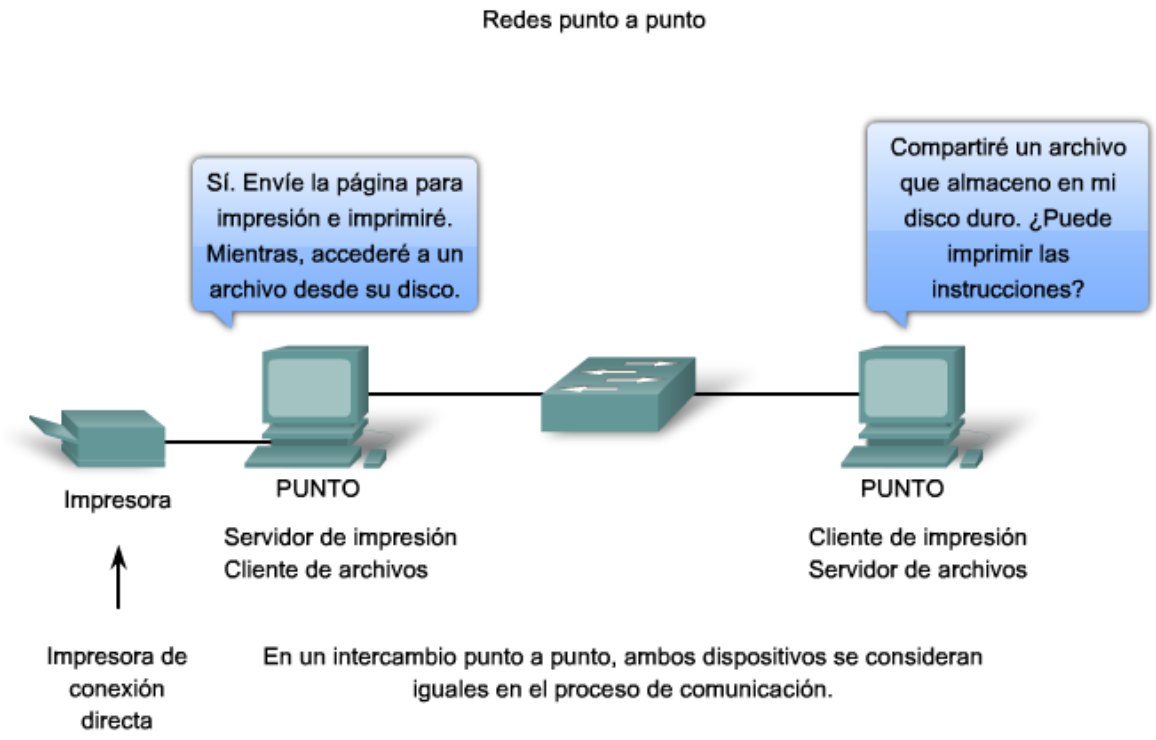
Redes punto a punto

En una red punto a punto, dos o más computadoras están conectadas por medio de una red y pueden compartir recursos (como impresoras y archivos) sin tener un servidor dedicado. Cada

dispositivo final conectado (conocido como punto) puede funcionar como un servidor o como un cliente. Una computadora puede asumir la función de servidor para una transacción mientras funciona en forma simultánea como cliente para otra transacción. Las funciones de cliente y servidor se establecen por solicitud.

Una red doméstica sencilla con dos computadoras conectadas compartiendo una impresora es un ejemplo de una red punto a punto. Cada persona puede configurar su computadora para compartir archivos, habilitar juegos en red o compartir una conexión de Internet. Otro ejemplo sobre la funcionalidad de la red punto a punto son dos computadoras conectadas a una gran red que utilizan aplicaciones de software para compartir recursos entre ellas a través de la red.

A diferencia del modelo cliente-servidor, que utiliza servidores dedicados, las redes punto a punto descentralizan los recursos en una red. En lugar de ubicar información para compartir en los servidores dedicados, la información puede colocarse en cualquier parte de un dispositivo conectado. La mayoría de los sistemas operativos actuales admiten compartir archivos e impresoras sin requerir software del servidor adicional. Debido a que las redes punto a punto generalmente no utilizan cuentas de usuarios centralizadas, permisos ni monitores, es difícil implementar las políticas de acceso y seguridad en las redes que contienen mayor cantidad de computadoras. Se deben establecer cuentas de usuario y derechos de acceso en forma individual para cada dispositivo.



Protocolo y servicios DNS

Ahora que tenemos una mejor comprensión de cómo las aplicaciones proporcionan una interfaz para el usuario y acceso a la red, veremos algunos protocolos específicos utilizados comúnmente.

Como veremos más adelante en este curso, la capa de transporte utiliza un esquema de direccionamiento llamado número de puerto. Los números de puerto identifican las aplicaciones y los servicios de la capa de aplicación que son el origen y el destino de los datos. Los programas del servidor generalmente utilizan números de puerto predefinidos comúnmente conocidos por los clientes. Mientras examinamos los diferentes servicios y protocolos de la capa de aplicación de TCP/IP, nos referiremos a los números de puerto TCP y UDP normalmente asociados con estos servicios. Algunos de estos servicios son:

- Sistema de nombres de dominios (DNS) - TCP/UDP puerto 53
- Protocolo de transferencia de hipertexto (HTTP) - TCP puerto 80
- Protocolo simple de transferencia de correo (SMTP) - TCP puerto 25
- Protocolo de oficina de correos (POP) - TCP puerto 110
- Telnet - TCP puerto 23
- Protocolo de configuración dinámica de host - UDP puertos 67 y 68
- Protocolo de transferencia de archivos (FTP) - TCP puertos 20 y 21

DNS

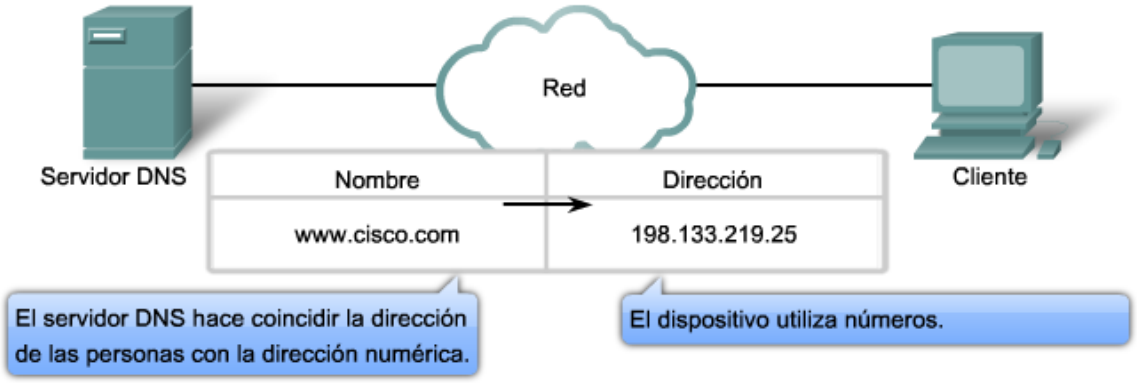
En las redes de datos, los dispositivos se etiquetan con una dirección IP numérica, de manera que pueden participar en el envío y la recepción de mensajes de la red. Sin embargo, la mayoría de las personas pasan mucho tiempo tratando de recordar estas direcciones numéricas. Por lo tanto, los nombres de dominios se crearon para convertir las direcciones numéricas en un nombre sencillo y reconocible.

En Internet, estos nombres de dominio, tales como www.cisco.com, son mucho más fáciles de recordar para la gente que algo como 198.133.219.25, el cual es la dirección numérica actual para ese servidor. Además, si Cisco decide cambiar la dirección numérica, es transparente para el usuario, ya que el nombre de dominio seguirá siendo www.cisco.com. La nueva dirección simplemente estará enlazada con el nombre de dominio existente y la conectividad se mantendrá. Cuando las redes eran pequeñas, resultaba fácil mantener la asignación entre los nombres de dominios y las direcciones que representaban. Sin embargo, a medida que las redes y el número de dispositivos comenzó a crecer, el sistema manual dejó de ser práctico.

El Sistema de nombres de dominios (DNS) se creó para que el nombre del dominio busque soluciones para estas redes. DNS utiliza un conjunto distribuido de servidores para resolver los nombres asociados con estas direcciones numéricas.

El protocolo DNS define un servicio automatizado que coincide con nombres de recursos que tienen la dirección de red numérica solicitada. Incluye las consultas sobre formato, las respuestas y los formatos de datos. Las comunicaciones del protocolo DNS utilizan un formato simple llamado mensaje. Este formato de mensaje se utiliza para todos los tipos de solicitudes de clientes y respuestas del servidor, mensajes de error y para la transferencia de información de registro de recursos entre servidores.

Resolución de direcciones DNS



DNS es un servicio cliente-servidor; sin embargo, difiere de los otros servicios cliente-servidor que estamos examinando. Mientras otros servicios utilizan un cliente que es una aplicación (como un explorador Web o un cliente de correo electrónico), el cliente DNS ejecuta un servicio por sí mismo. El cliente DNS, a veces denominado resolución DNS, admite la resolución de nombres para otras aplicaciones de red y servicios que lo necesiten.

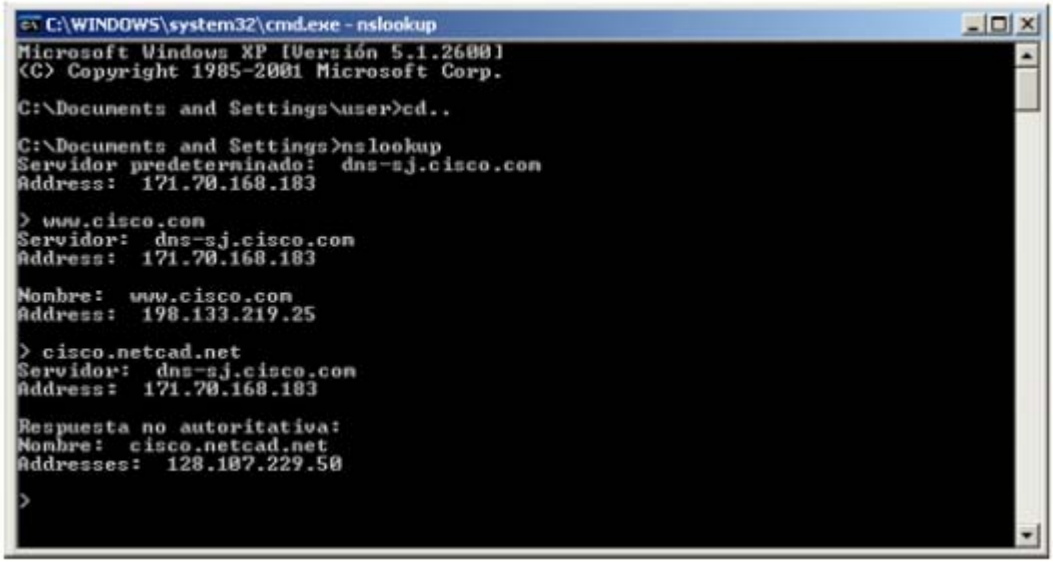
Al configurar un dispositivo de red, generalmente proporcionamos una o más direcciones del servidor DNS que el cliente DNS puede utilizar para la resolución de nombres. En general, el proveedor de servicios de Internet provee las direcciones para utilizar con los servidores DNS. Cuando la aplicación del usuario pide conectarse a un dispositivo remoto por nombre, el cliente DNS solicitante consulta uno de estos servidores de denominación para resolver el nombre para una dirección numérica.

Los sistemas operativos computacionales también cuentan con una herramienta llamada nslookup que permite que el usuario consulte de forma manual los servidores de nombres para resolver un nombre de host dado. Esta utilidad también puede utilizarse para solucionar los problemas de resolución de nombres y verificar el estado actual de los servidores de nombres.

En la figura, cuando se ejecuta nslookup, se muestra el servidor DNS predeterminado configurado para su host. En este ejemplo, el servidor DNS es dns-sjk.cisco.com que tiene una dirección de 171.68.226.120.

Luego podemos escribir el nombre de un host o dominio para el cual deseamos obtener la dirección. En la primer consulta de la figura, se hace una consulta para www.cisco.com. El servidor de nombre que responde proporciona la dirección 198.133.219.25.

Las consultas mostradas en la figura son sólo pruebas simples. La herramienta nslookup tiene muchas opciones disponibles para lograr una extensa verificación y prueba del proceso DNS.



El sistema de nombres de dominios utiliza un sistema jerárquico para crear una base de datos y así proporcionar una resolución de nombres. La jerarquía es similar a un árbol invertido con la raíz en la parte superior y las ramas por debajo.

En la parte superior de la jerarquía, los servidores raíz mantienen registros sobre cómo alcanzar los servidores de dominio de nivel superior, los cuales a su vez tienen registros que apuntan a los servidores de dominio de nivel secundario y así sucesivamente.

Los diferentes dominios de primer nivel representan el tipo de organización o el país de origen. Entre los ejemplos de dominios del nivel superior se encuentran:
.au: Australia
.co: Colombia
.com: una empresa o industria
.jp: Japón
.org: una organización sin fines de lucro

Después de los dominios del nivel superior, se encuentran los nombres de los dominios de segundo nivel y debajo de estos hay otros dominios de nivel inferior.

Cada nombre de dominio es una ruta hacia este árbol invertido que comienza de la raíz.

Por ejemplo, como se muestra en la figura, el servidor DNS raíz puede no saber exactamente dónde se ubica el servidor de correo electrónico mail.cisco.com, pero conserva un registro para el dominio "com" dentro del dominio de nivel superior. Asimismo, los servidores dentro del dominio "com" pueden no tener un registro de mail.cisco.com, pero sí tienen un registro para el dominio "cisco.com". Los servidores dentro del dominio cisco.com tienen un registro (un registro MX para ser precisos) para mail.cisco.com.

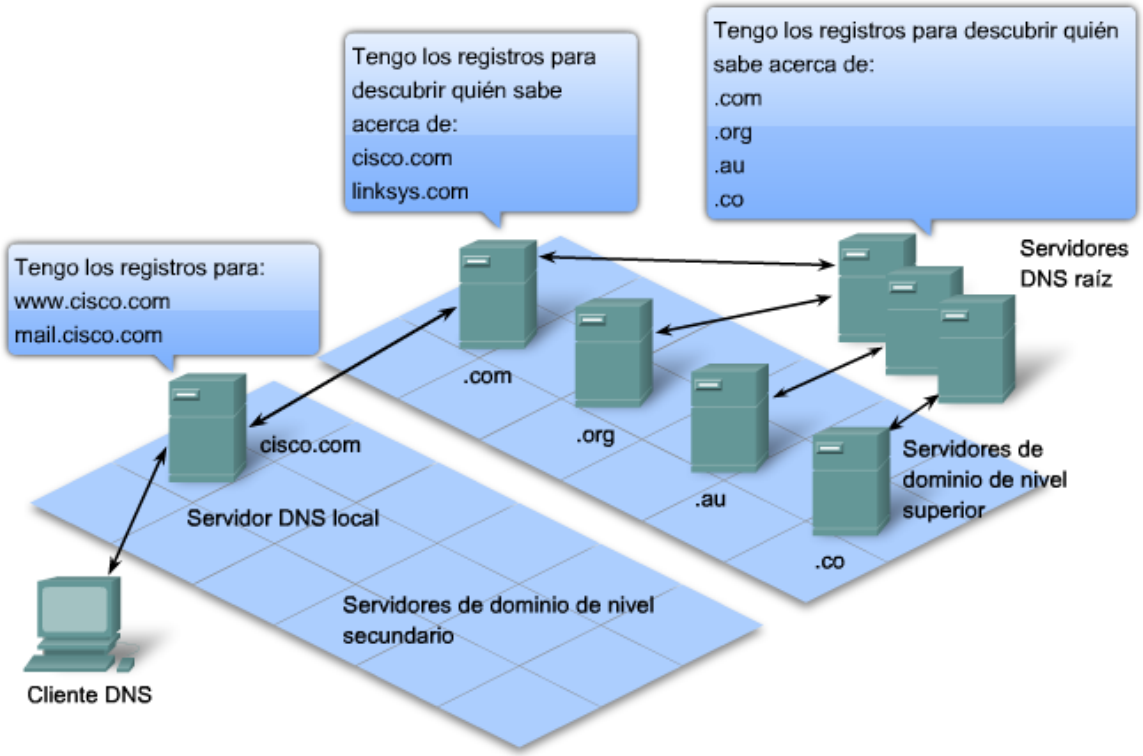
El DNS depende de esta jerarquía de servidores descentralizados para almacenar y mantener estos registros de recursos. Los registros de recursos enumeran nombres de dominios que el servidor puede resolver y servidores alternativos que también pueden procesar solicitudes. Si un servidor dado tiene registros de recursos que corresponden a su nivel en la jerarquía de dominios, se dice que es autoritativo para dichos registros.

Por ejemplo, un servidor de nombres en el dominio cisco.netacad.net no sería autoritativo para el registro mail.cisco.com porque dicho registro se mantiene en un servidor de nivel de dominio superior, específicamente el servidor de nombres en el dominio cisco.com.

Enlaces

http://www.ietf.org//rfc/rfc1034.txt

http://www.ietf.org/rfc/rfc1035.txt



Una jerarquía de servidores DNS contiene los registros de recursos que coordinan los nombres con las direcciones.

Servicios WWW y HTTP

Cuando se escribe una dirección Web (o URL) en un explorador de Internet, el explorador establece una conexión con el servicio Web del servidor que utiliza el protocolo HTTP. URL (o

Localizador uniforme de recursos) y URI (Identificador uniforme de recursos) son los nombres que la mayoría de las personas asocian con las direcciones Web.

El URL http://www.cisco.com/index.html es un ejemplo que se refiere a un recurso específico, una página Web llamada index.html en un servidor identificado como cisco.com (haga clic en las pestañas de la figura para ver los pasos que utiliza el HTTP).

Los exploradores Web son las aplicaciones cliente que utilizan nuestras computadoras para conectarse a la World Wide Web y acceder a recursos almacenados en un servidor Web. Al igual que con la mayoría de los procesos de servidores, el servidor Web funciona como un servicio básico y genera diferentes tipos de archivos disponibles.

Para acceder al contenido, los clientes Web realizan conexiones al servidor y solicitan los recursos deseados. El servidor responde con el recurso y, al recibirlo, el explorador interpreta los datos y los presenta al usuario.

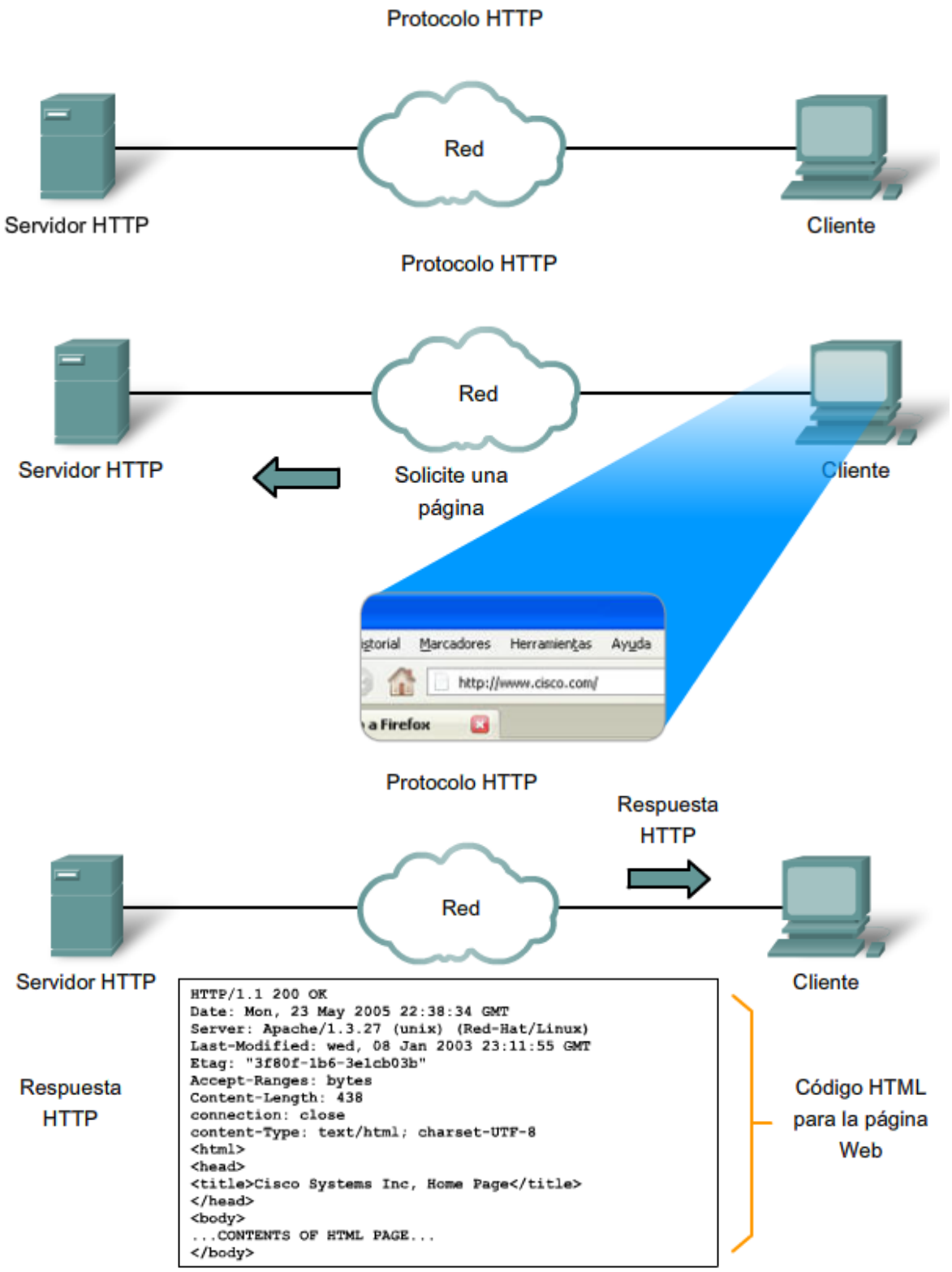
Los buscadores pueden interpretar y presentar muchos tipos de datos, como texto sin cifrar o Lenguaje de marcas de hipertexto (HTML, el lenguaje en el que se crean las páginas Web). Otros tipos de datos, sin embargo, requieren de otro servicio o programa. Generalmente se les conoce como plug-ins o complementos. Para ayudar al explorador a determinar qué tipo de archivo está recibiendo, el servidor especifica qué clase de datos contiene el archivo.

Para comprender mejor cómo interactúan el explorador Web y el cliente Web, podemos analizar cómo se abre una página Web en un explorador. Para este ejemplo, utilizaremos la dirección URL: http://www.cisco.com/web-server.htm.

Primero, el explorador interpreta las tres partes del URL:

1. http (el protocolo o esquema)
2. www.cisco.com (el nombre del servidor)
3. web-server.htm (el nombre de archivo específico solicitado).

Después, el explorador verifica con un servidor de nombres para convertir a www.cisco.com en una dirección numérica que utilizará para conectarse con el servidor. Al utilizar los requerimientos del protocolo HTTP, el explorador envía una solicitud GET al servidor y pide el archivo web-server.htm. El servidor, a su vez, envía al explorador el código HTML de esta página Web. Finalmente, el explorador descifra el código HTML y da formato a la página para la ventana del explorador.



En respuesta a la solicitud, el servidor HTTP envía el código para una página Web.

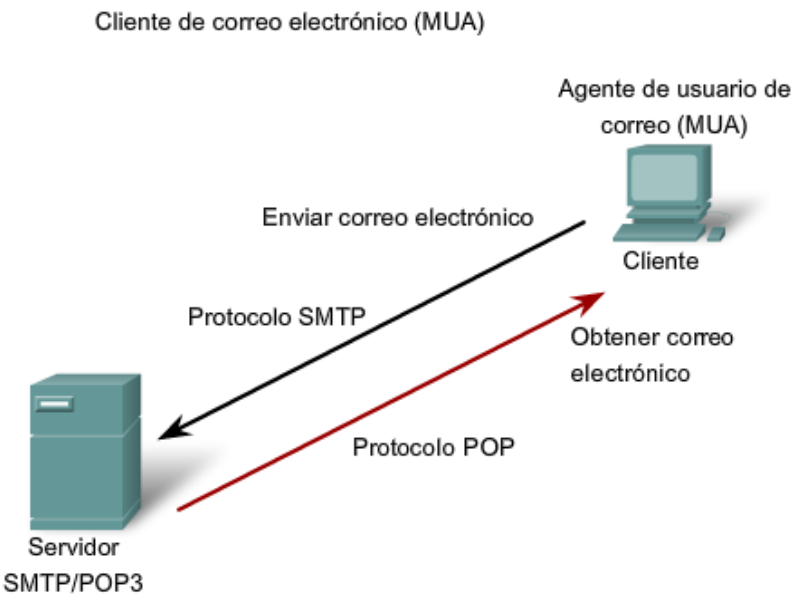
El navegador interpreta el código HTML y muestra una página Web.

Servicios de correo electronico y protocolos SMTP/POP

Correo electrónico, el servidor de red más conocido, ha revolucionado la manera en que nos comunicamos, por su simpleza y velocidad. Inclusive para ejecutarse en una computadora o en otro dispositivo, los correos electrónicos requieren de diversos servicios y aplicaciones. Dos ejemplos de protocolos de capa de aplicación son el Protocolo de oficina de correos (POP) y el Protocolo simple de transferencia de correo (SMTP), que aparecen en la figura. Como con el HTTP, estos protocolos definen los procesos de cliente-servidor.

Cuando la gente redacta mensajes de correo electrónico, generalmente utilizan una aplicación llamada Agente de usuario de correo (MUA), o un cliente de correo electrónico. MUA permite enviar los mensajes y colocar los recibidos en el buzón del cliente; ambos procesos son diferentes.

Para recibir correos electrónicos desde un servidor de correo, el cliente de correo electrónico puede utilizar un POP. Al enviar un correo electrónico desde un cliente o un servidor se utilizan formatos de mensajes y cadenas de comando definidas por el protocolo SMTP. En general, un cliente de correo electrónico proporciona la funcionalidad de ambos protocolos dentro de una aplicación.



Los clientes envían correo electrónico a un servidor mediante SMTP y reciben correo electrónico mediante POP3.

FTP

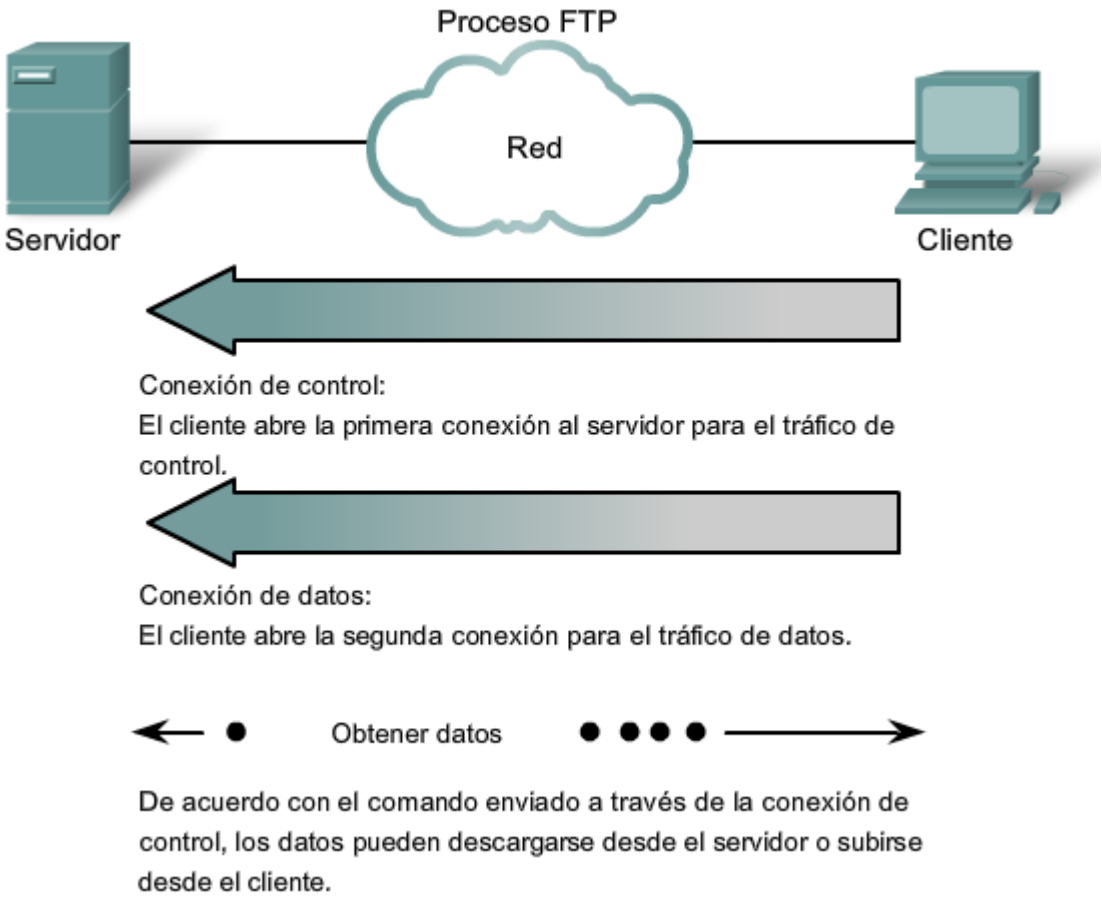
El Protocolo de transferencia de archivos (FTP) es otro protocolo de la capa de aplicación de uso común. El FTP se desarrolló para permitir las transferencias de archivos entre un cliente y un servidor. Un cliente FTP es una aplicación que se ejecuta en una computadora y que carga y descarga archivos de un servidor que ejecuta el demonio FTP (FTPd).

El FTP necesita dos conexiones entre el cliente y el servidor para transferir archivos de forma exitosa: una para comandos y respuestas, otra para la transferencia real de archivos.

El cliente establece la primera conexión con el servidor en TCP puerto 21. Esta conexión se utiliza para controlar el tráfico, que consiste en comandos del cliente y respuestas del servidor.

El cliente establece la segunda conexión con el servidor en TCP puerto 20. Esta conexión es para la transferencia real de archivos y se crea cada vez que se transfiere un archivo.

La transferencia de archivos puede producirse en ambas direcciones. El cliente puede descargar (bajar) un archivo desde el servidor o el cliente puede cargar (subir) un archivo en el servidor.



DHCP

El servicio del Protocolo de configuración dinámica de host (DHCP) permite a los dispositivos de una red obtener direcciones IP y otra información de un servidor DHCP. Este servicio automatiza la asignación de direcciones IP, máscaras de subred, gateway y otros parámetros de networking del IP.

DHCP permite a un host obtener una dirección IP de forma dinámica cuando se conecta a la red. Se realiza el contacto con el servidor de DHCP y se solicita una dirección. El servidor DHCP elige una dirección del rango configurado llamado pool y la asigna ("alquila") para el host por un tiempo establecido.

En redes locales más grandes, o donde los usuarios cambien con frecuencia, se prefiere el DHCP. Los nuevos usuarios llegan con computadoras portátiles y necesitan una conexión. Otros tienen nuevas estaciones de trabajo que necesitan conexión. En lugar de que el administrador de red asigne direcciones IP para cada estación de trabajo, es más eficaz que las direcciones IP se asignen automáticamente mediante el DHCP.

Las direcciones distribuidas por DHCP no se asignan de forma permanente a los hosts, sino que sólo se alquilan por un periodo de tiempo. Si el host se apaga o se desconecta de la red, la dirección regresa al pool para volver a utilizarse. Esto es especialmente útil para los usuarios móviles que entran y salen de la red. Los usuarios pueden moverse libremente desde una

ubicación a otra y volver a establecer las conexiones de red. El host puede obtener una dirección IP cuando se conecte el hardware, ya sea por cables o por LAN inalámbrica.

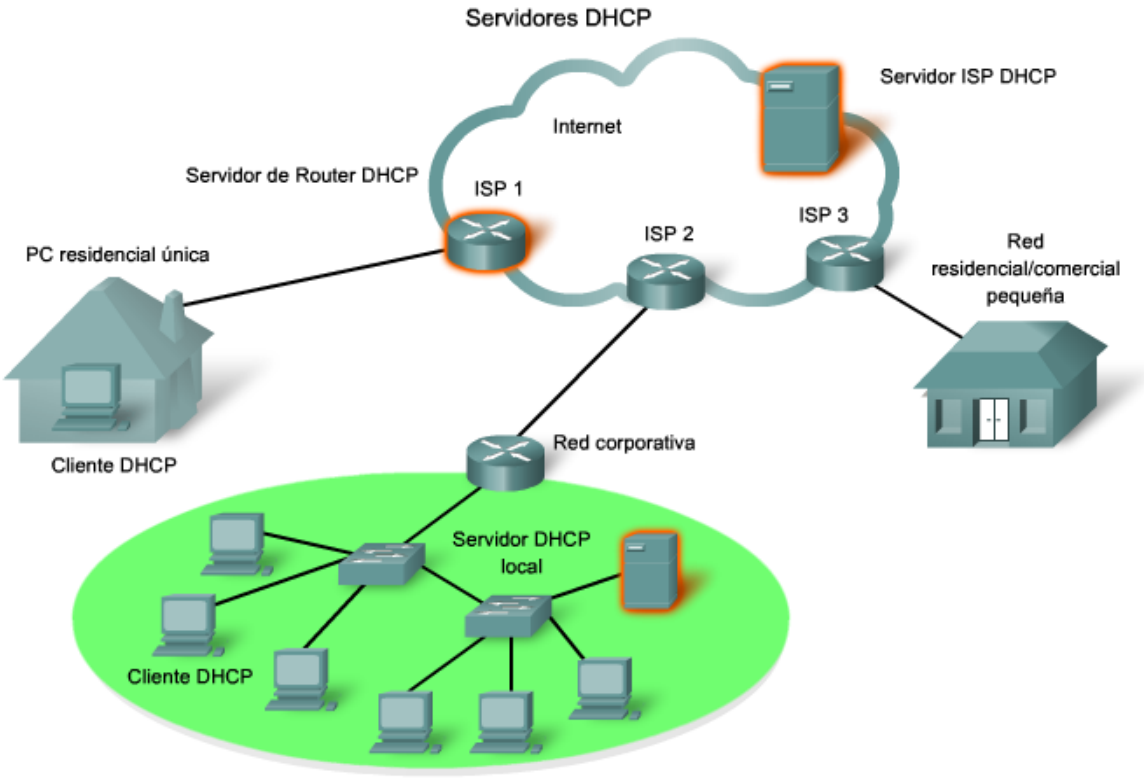
DHCP le permite el acceso a Internet por medio de Internet utilizando zonas de cobertura inalámbrica en aeropuertos o cafeterías. Una vez que ingresa al área, el cliente de DHCP de la computadora portátil contacta al servidor de DHCP mediante una conexión inalámbrica. El servidor de DHCP asigna una dirección IP a la computadora portátil.

Como lo muestra la figura, varios tipos de dispositivos pueden ser servidores de DHCP cuando ejecutan software de servicio de DHCP. En la mayoría de las redes medianas a grandes, el servidor de DHCP generalmente es un servidor local dedicado con base en una PC.

Con las redes domésticas, el servidor de DHCP se ubica en el ISP y un host de la red doméstica recibe la configuración IP directamente desde el ISP.

DHCP puede representar un riesgo a la seguridad porque cualquier dispositivo conectado a la red puede recibir una dirección. Este riesgo hace que la seguridad física sea un factor importante al determinar si se utiliza el direccionamiento dinámico o manual.

Ambos direccionamientos tienen su lugar en los diseños de red. Muchas redes utilizan tanto el direccionamiento estático como el DHCP. DHCP se utiliza para hosts de propósitos generales, como los dispositivos de usuario final, y las direcciones fijas se utilizan para dispositivos de red como gateways, switches, servidores e impresoras.



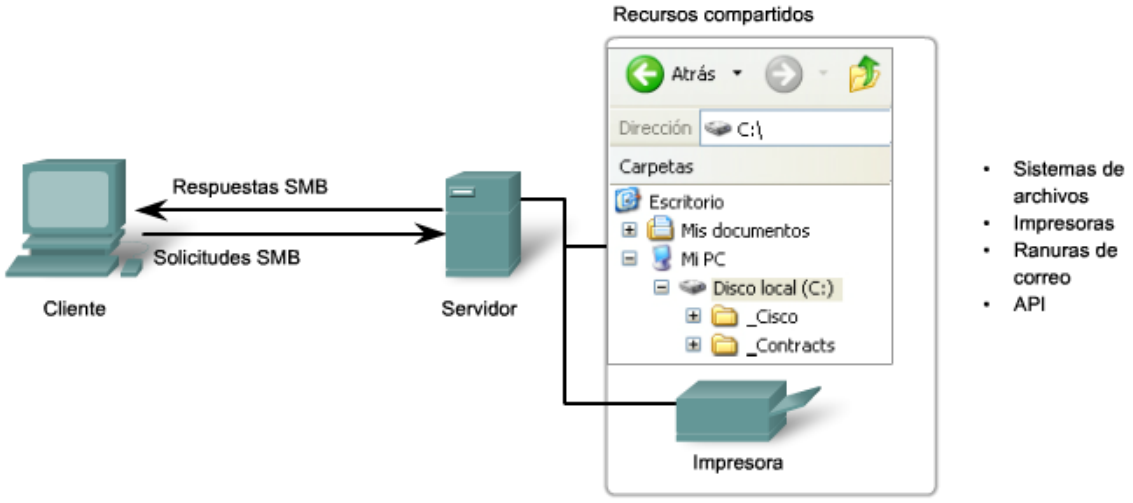
Protocolo SMB y servicios para compartir archivos

El Bloque de mensajes del servidor (SMB) es un protocolo cliente-servidor para compartir archivos. IBM desarrolló el Bloque de mensajes del servidor (SMB) a fines de la década de los 80 para describir la estructura de recursos de red compartidos, como directorios, archivos, impresoras y puertos seriales. Es un protocolo de solicitud-respuesta. A diferencia del protocolo para compartir archivos respaldado por FTP, los clientes establecen una conexión a largo plazo con los servidores. Una vez establecida la conexión, el usuario del cliente puede acceder a los recursos en el servidor como si el recurso fuera local para el host del cliente.

El intercambio de archivos SMB y los servicios de impresión se han transformado en el pilar de networking de Microsoft. Con la presentación de la serie Windows 2000 del software, Microsoft cambió la estructura subyacente para el uso del SMB. En versiones anteriores de los productos de Microsoft, los servicios de SMB utilizaron un protocolo que no es TCP/IP para implementar la resolución de nombres. Comenzando con Windows 2000, todos los productos subsiguientes de Microsoft utilizan denominación DNS. Esto permite que los protocolos TCP/IP den soporte directamente al intercambio de recursos SMB, como se muestra en la figura.

Los sistemas operativos LINUX y UNIX también proporcionan un método de intercambio de recursos con redes de Microsoft mediante una versión del SMB llamado SAMBA. Los sistemas operativos Macintosh de Apple también admiten recursos compartidos por medio del protocolo SMB.

Compartir archivos mediante el protocolo SMB



SMB es un protocolo de solicitud-respuesta y cliente-servidor. Los servidores pueden poner sus recursos a disposición de los clientes en la red.

Protocolos y servicios TELNET

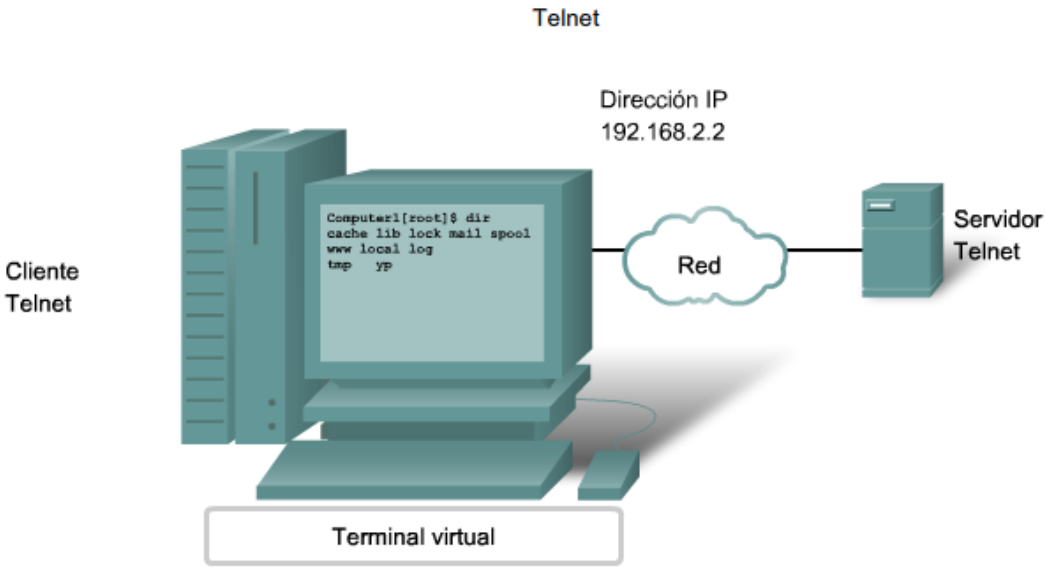
Mucho antes de que existieran las computadoras de escritorio con interfaces gráficas sofisticadas, las personas utilizaban sistemas basados en textos que eran simplemente terminales conectadas físicamente a una computadora central. Una vez que las redes estaban disponibles, las personas necesitaban acceder en forma remota a los sistemas informáticos de la misma manera en que lo hacían con las terminales conectadas directamente.

Telnet se desarrolló para satisfacer esta necesidad.. Telnet se remonta a principios de la década de los 70 y se encuentra entre los servicios y protocolos de capa de aplicación más antiguo dentro del grupo TCP/IP. Telnet proporciona un método estándar de emulación de dispositivos de terminal con base en texto en la red de datos. El protocolo y el software del cliente que implementa son conocidos como Telnet.

De un modo adecuado, una conexión que utiliza Telnet se llama sesión o conexión de terminal virtual (VTY). En lugar de utilizar un dispositivo físico para conectarse al servidor, Telnet utiliza software para crear un dispositivo virtual que proporcione las mismas características de una sesión de terminal con acceso a la interfaz de línea de comandos (CLI) del servidor.

Para admitir conexiones del cliente a Telnet, el servidor ejecuta un servicio llamado demonio de Telnet. Se establece una conexión de terminal virtual desde un dispositivo final utilizando una aplicación del cliente Telnet. La mayoría de los sistemas operativos incluye un cliente de Telnet de la capa de aplicación. Telnet puede ejecutarse desde el indicador del sistema en una PC de Microsoft Windows. Otras aplicaciones de terminal comunes que ejecutan clientes Telnet son HyperTerminal, Minicom y TeraTerm.

Una vez establecida una conexión Telnet, los usuarios pueden realizar cualquier función autorizada en el servidor, como si utilizaran una sesión de línea de comandos en el servidor mismo. Si están autorizados, pueden iniciar y detener procesos, configurar el dispositivo e inclusive apagar el sistema.



Telnet proporciona una forma de utilizar una computadora, conectada a través de la red, para acceder a un dispositivo de red como si el teclado y el monitor estuvieran conectados directamente al dispositivo.

4.1.2. La capa de presentación

La capa de presentación tiene tres funciones principales:

- Codificación y conversión de datos de la capa de aplicación para garantizar que los datos del dispositivo de origen se puedan interpretar por la aplicación adecuada en el dispositivo de destino.
- Compresión de los datos de forma que los pueda descomprimir el dispositivo de destino.
- Encriptación de los datos para la transmisión y la encriptación de los mismos cuando lleguen a su destino.

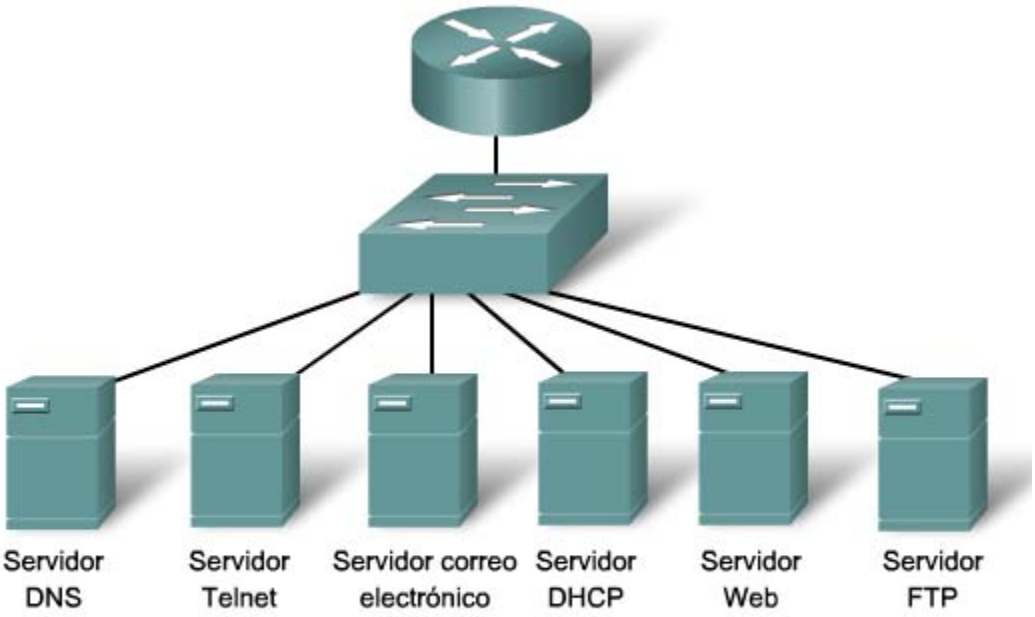
Generalmente, las implementaciones de la capa de presentación no están relacionadas con un stack de protocolos en particular. Los estándares para videos y gráficos son algunos ejemplos. Dentro de los estándares más conocidos para video encontramos QuickTime y el Grupo de expertos en películas (MPEG). QuickTime es una especificación de Apple Computer para audio y video, y MPEG es un estándar para la codificación y compresión de videos.

Dentro de los formatos de imagen gráfica más conocidos encontramos el Formato de intercambio gráfico (GIF), Grupo de expertos en fotografía (JPEG) y Formato de archivo de imagen etiquetada (TIFF). GIF y JPEG son estándares de compresión y codificación para imágenes gráficas, y TIFF es un formato de codificación estándar para imágenes gráficas.

4.1.3. La capa de sesión

Como lo indica el nombre de la capa de sesión, las funciones en esta capa crean y mantienen diálogos entre las aplicaciones de origen y destino. La capa de sesión maneja el intercambio de información para iniciar los diálogos y mantenerlos activos, y para reiniciar sesiones que se interrumpieron o desactivaron durante un periodo de tiempo prolongado.

La mayoría de las aplicaciones, como los exploradores Web o los clientes de correo electrónico, incorporan la funcionalidad de las Capas 5, 6 y 7 del modelo OSI.



Granja de servidores

Los protocolos de capa de aplicación de TCP/IP más conocidos son aquéllos que proporcionan intercambio de la información del usuario. Estos protocolos especifican la información de control y formato necesaria para muchas de las funciones de comunicación de Internet más comunes.
Algunos de los protocolos TCP/IP son:
El Protocolo servicio de nombres de dominio (DNS, Domain Name Service) se utiliza para resolver nombres de Internet para direcciones IP.
El Protocolo de transferencia de hipertexto (HTTP, Hypertext Transfer Protocol) se utiliza para transferir archivos que forman las páginas Web de la World Wide Web.
El Protocolo simple de transferencia de correo (SMTP) se utiliza para la transferencia de mensajes de correo y adjuntos.
Telnet, un protocolo de emulación de terminal, se utiliza para proporcionar acceso remoto a servidores y a dispositivos de red.
El Protocolo de transferencia de archivos (FTP) se utiliza para la transferencia de archivos interactiva entre sistemas.

Los protocolos en la suite de TCP/IP los definen generalmente las Solicitudes de comentarios (RFC). El Grupo de trabajo de ingeniería de Internet mantiene las RFC como los estándares para la suite de TCP/IP.

4.1.4. La capa de transporte

La capa de transporte permite la segmentación de datos y brinda el control necesario para reensamblar las partes dentro de los distintos streams de comunicación. Las responsabilidades principales que debe cumplir son:
Rastreo de comunicación individual entre aplicaciones en los hosts de origen y destino
Segmentación de datos y manejo de cada parte
Reensamble de segmentos en streams de datos de aplicación
Identificación de diferentes aplicaciones

Rastreo de conversaciones individuales

Cualquier host puede tener múltiples aplicaciones que se comunican a través de la red. Cada una de estas aplicaciones se comunicará con una o más aplicaciones en hosts remotos. Es responsabilidad de la capa de transporte mantener los streams de comunicación múltiple entre estas aplicaciones.

Segmentación de datos

Así como cada aplicación crea datos de stream para enviarse a una aplicación remota, estos datos se pueden preparar para enviarse a través de los medios en partes manejables. Los protocolos de la capa de transporte describen los servicios que segmentan estos datos de la capa de aplicación. Esto incluye la encapsulación necesaria en cada sección de datos. Cada sección de datos de aplicación requiere que se agreguen encabezados en la capa de transporte para indicar la comunicación a la cual está asociada.

Reensamble de segmentos

En el host de recepción, cada sección de datos se puede direccionar a la aplicación adecuada. Además, estas secciones de datos individuales también deben reconstruirse para generar un stream completo de datos que sea útil para la capa de aplicación. Los protocolos en la capa de transporte describen cómo se utiliza la información del encabezado de la capa para reensamblar las partes de los datos en streams para pasarlos a la capa de aplicación.

Identificación de aplicaciones

Para pasar streams de datos a las aplicaciones adecuadas, la capa de transporte debe identificar la aplicación meta. Para lograr esto, la capa de transporte asigna un identificador a la aplicación. Los protocolos TCP/IP denominan a este identificador número de puerto. A todos los procesos de software que requieran acceder a la red se les asigna un número de puerto exclusivo en ese host. Este número de puerto se utiliza en el encabezado de la capa de transporte para indicar qué aplicación se asocia a qué parte.

La capa de transporte es el enlace entre la capa de aplicación y la capa inferior que es responsable de la transmisión de la red. Esta capa acepta los datos de diferentes conversaciones y las pasa a las capas inferiores como partes manejables que se pueden multiplexar de forma eventual en la red.

Las aplicaciones no necesitan saber los detalles operativos de la red en uso. Las aplicaciones generan datos que se envían desde una aplicación a otra sin tener en cuenta el tipo de host destino, el tipo de medios sobre los que los datos deben viajar, el paso tomado por los datos, la congestión en un enlace o el tamaño de la red.

Además, las capas inferiores no tienen conocimiento de que existen varias aplicaciones que envían datos en la red. Su responsabilidad es entregar los datos al dispositivo adecuado. La capa de transporte clasifica entonces estas piezas antes de enviarlas a la aplicación adecuada.

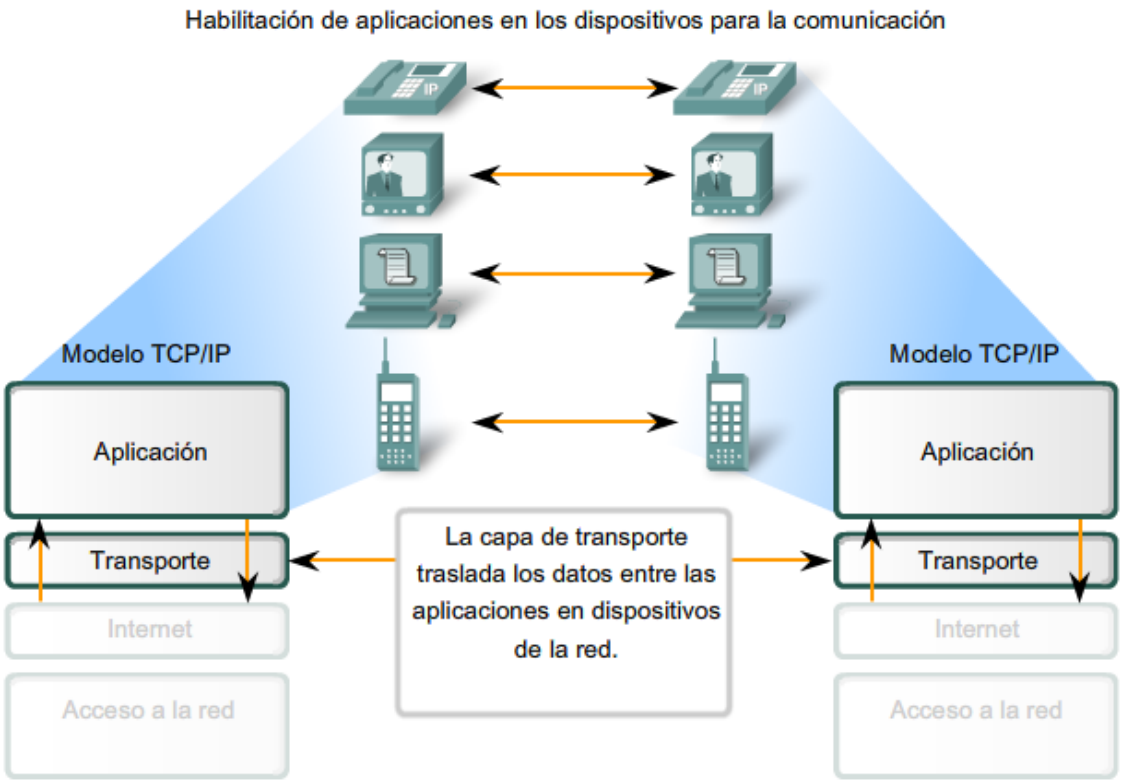
Los requisitos de datos varían

Hay múltiples protocolos de la capa de transporte debido a que las aplicaciones tienen diferentes requisitos. Para algunas aplicaciones, los segmentos deben llegar en una secuencia específica de manera que puedan ser procesados en forma exitosa. En algunos casos, todos los datos deben recibirse para ser utilizados por cualquiera de las mismas. En otros casos, una aplicación puede tolerar cierta pérdida de datos durante la transmisión a través de la red.

En las redes convergentes actuales, las aplicaciones con distintas necesidades de transporte pueden comunicarse en la misma red. Los diferentes protocolos de la capa de transporte poseen distintas reglas para permitir a los dispositivos manejar estos diversos requerimientos de datos.

Algunos protocolos proporcionan sólo las funciones básicas para enviar de forma eficiente partes de datos entre las aplicaicones adecuadas. Estos tipos de protocolos son útiles para aplicaciones cuyos datos son sensibles a retrasos.

Otros protocolos de la capa de transporte describen los procesos que proporcionan características adicionales, como asegurar un envío confiable entre las aplicaciones. Si bien estas funciones adicionales proveen una comunicación más sólida entre aplicaciones de la capa de transporte, representan la necesidad de utilizar recursos adicionales y generan un mayor número de demandas en la red.

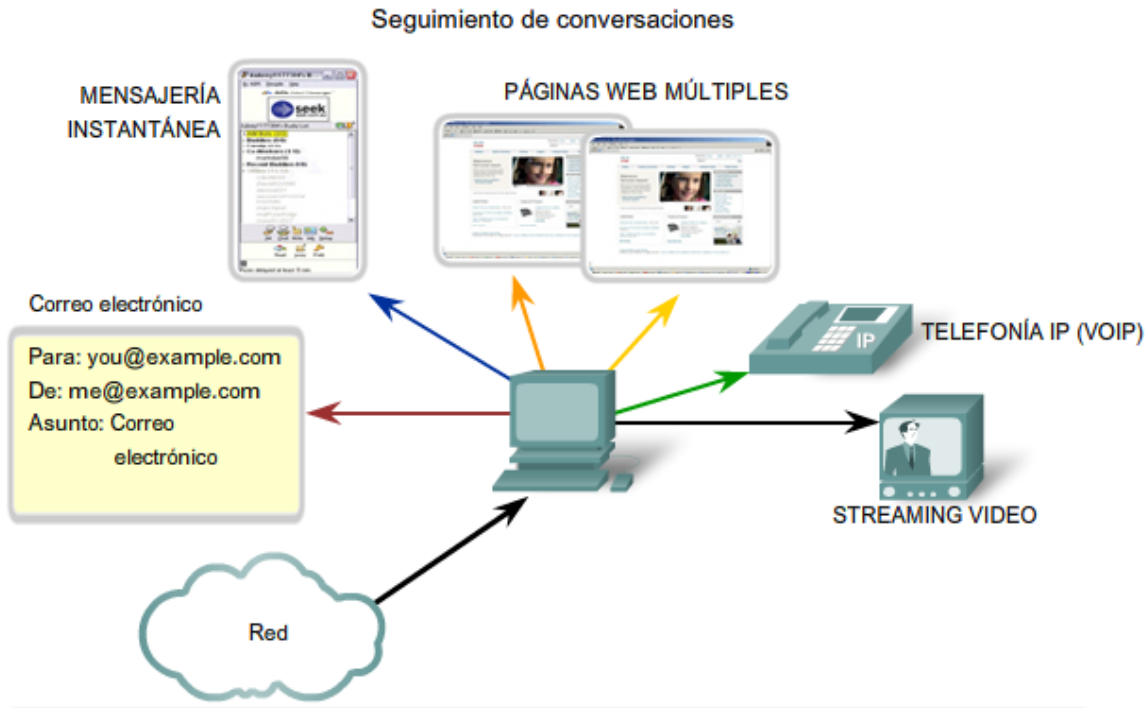


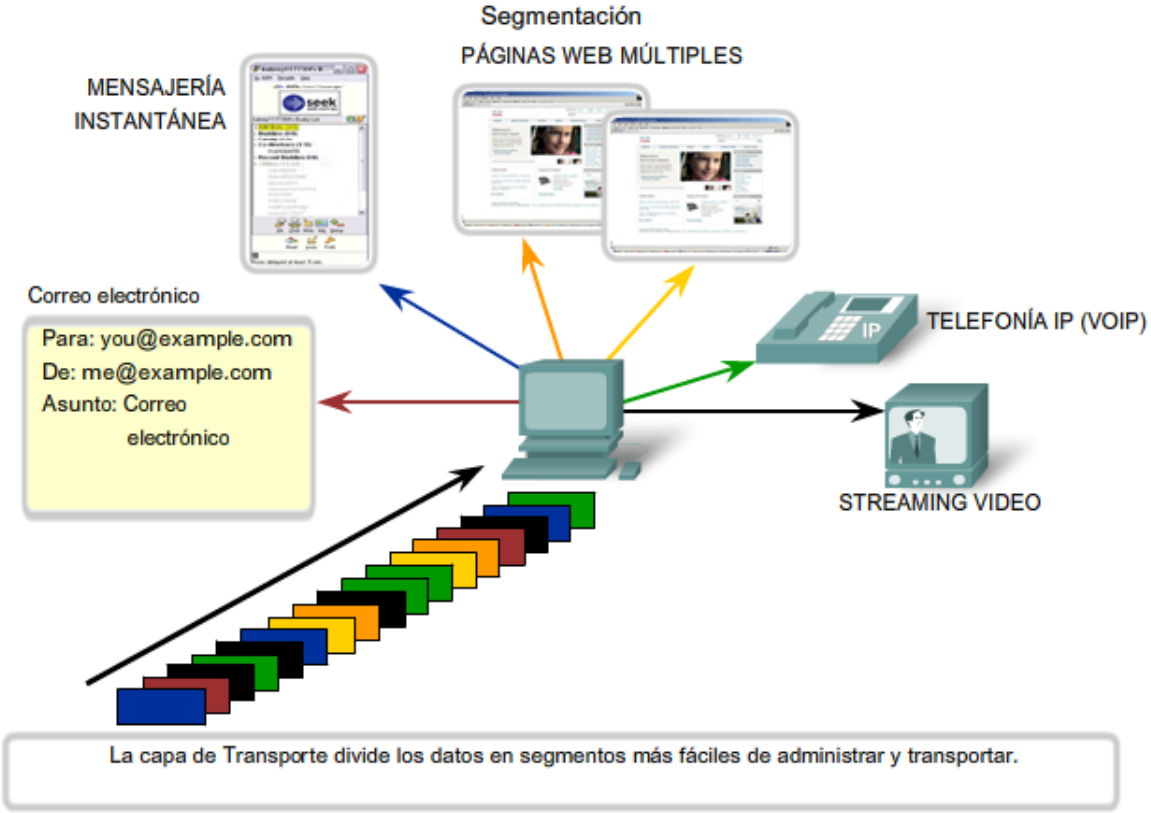
Separación de comunicaciones múltiples

Considere una computadora conectada a una red que recibe y envía correos electrónicos y mensajes instantáneos, explora sitios Web y realiza una llamada telefónica de VoIP de manera simultánea. Cada una de estas aplicaciones envía y recibe datos en la red al mismo tiempo. Sin embargo, los datos de la llamada telefónica no están dirigidos al explorador Web, y el texto de un mensaje instantáneo no aparece en el correo electrónico.

Además, los usuarios necesitan que el correo electrónico o página Web se reciba por completo y se presente para la información que se considere útil. Los retrasos ligeros se consideran aceptables para asegurar que la información se reciba y se presente por compelto.

En cambio, la pérdida ocasional de partes pequeñas de una conversación telefónica se puede considerar aceptable. Se puede inferir la parte de audio perdida del contexto de la conversación o se puede solicitar a la otra persona que repita lo que dijo. Es preferible esto último a las demoras que se producirían si se solicita a la red que gestione y vuelva a enviar los segmentos perdidos. En este ejemplo, el usuario, no la red, gestiona el reenvío o reemplazo de información que falta.


Seguimiento de conversaciones
MENSAJERÍA INSTANTÁNEA
PÁGINAS WEB MÚLTIPLES
Correo electrónico
Para: you@example.com
De: me@example.com
Asunto: Correo electrónico
IP
TELEFONÍA IP (VOIP)
STREAMING VIDEO
Red
La capa de Transporte segmenta los datos y administra la separación de datos para diferentes aplicaciones. Las aplicaciones múltiples que se ejecutan en un dispositivo reciben los datos correctos.


Segmentación
MENSAJERÍA INSTANTÁNEA
PÁGINAS WEB MÚLTIPLES
Correo electrónico
Para: you@example.com
De: me@example.com
Asunto: Correo electrónico
IP
TELEFONÍA IP (VOIP)
STREAMING VIDEO
La capa de Transporte divide los datos en segmentos más fáciles de administrar y transportar.

TCP y UDP

Los dos protocolos más comunes de la capa de transporte del conjunto de protocolos TCP/IP son el Protocolo de control de transmisión (TCP) y el Protocolo de datagramas de usuario (UDP). Ambos protocolos gestionan la comunicación de múltiples aplicaciones. Las diferencias entre ellos son las funciones específicas que cada uno implementa.

Protocolo de datagramas de usuario (UDP)

UDP es un protocolo simple, sin conexión, descrito en la RFC 768. Cuenta con la ventaja de proveer la entrega de datos sin utilizar muchos recursos. Las porciones de comunicación en UDP se llaman datagramas. Este protocolo de la capa de transporte envía estos datagramas como "mejor intento".

- Las aplicaciones que utilizan UDP incluyen:
- Sistema de nombres de dominio (DNS)
- Streaming video
- Voz sobre IP (VOIP)

Protocolo de control de transmisión (TCP)

TCP es un protocolo orientado a la conexión descrito en RFC 793. El TCP utiliza recursos adicionales para ganar funciones. Las funciones adicionales especificadas por TCP están en el mismo orden de entrega, son de entrega confiable y de control de flujo. Cada segmento de TCP posee 20 bytes de carga en el encabezado que encapsulan los datos de la capa de aplicación, mientras que cada segmento UDP sólo posee 8 bytes de carga. Vea la figura para hacer una comparación.

- Las aplicaciones que utiliza el TCP son:
- Exploradores Web
- Correo electrónico
- Transferencias de archivos

Encabezados TCP y UDP

Segmento de TCP

Bit (0)	Bit (15)	Bit (16)	Bit (31)
Puerto de origen (16)		Puerto de destino (16)	
Número de secuencia (32)			
Número de acuse de recibo (32)			
Longitud del encabezado (4) Reservado (6) Bits de código (6)		Ventana (16)	
Checksum (16)		Urgente (16)	
Opciones (0 ó 32 si las hay)			
DATOS DE LA CAPA DE APLICACIÓN (el tamaño varía)			

20 Bytes

Datagrama de UDP

Bit (0)	Bit (15)	Bit (16)	Bit (31)
Puerto de origen (16)		Puerto de destino (16)	
Longitud (16)		Checksum (16)	
DATOS DE LA CAPA DE APLICACIÓN (el tamaño varía)			

8 Bytes

Direccionamiento del puerto

La Autoridad de números asignados de Internet (IANA) asigna números de puerto. IANA es un organismo normativo responsable de asegurar diferentes estándares de direccionamiento.

Hay diversos tipos de números de puerto:

Puertos bien conocidos (números del 0 al 1023): estos números se reservan para servicios y aplicaciones. Por lo general, se utilizan para aplicaciones como HTTP (servidor Web), POP3/SMTP (servidor de correo electrónico) y Telnet. Al definir estos puertos bien conocidos para las aplicaciones de los servidores, las aplicaciones cliente se pueden programar para solicitar una conexión a dicho puerto y su servicio asociado.

Puertos registrados (números del 1024 al 49151): estos números de puerto se asignan a procesos o aplicaciones del usuario. Estos procesos son principalmente aplicaciones individuales que el usuario elige instalar en lugar de aplicaciones comunes que recibiría un puerto bien conocido. Cuando no se utilizan para un recurso del servidor, estos puertos se pueden utilizar también seleccionados de forma dinámica por un cliente como su puerto de origen.

Puertos dinámicos o privados (números 49152 a 65535): también conocidos como puertos efímeros, están usualmente asignados de forma dinámica a las aplicaciones cliente cuando se

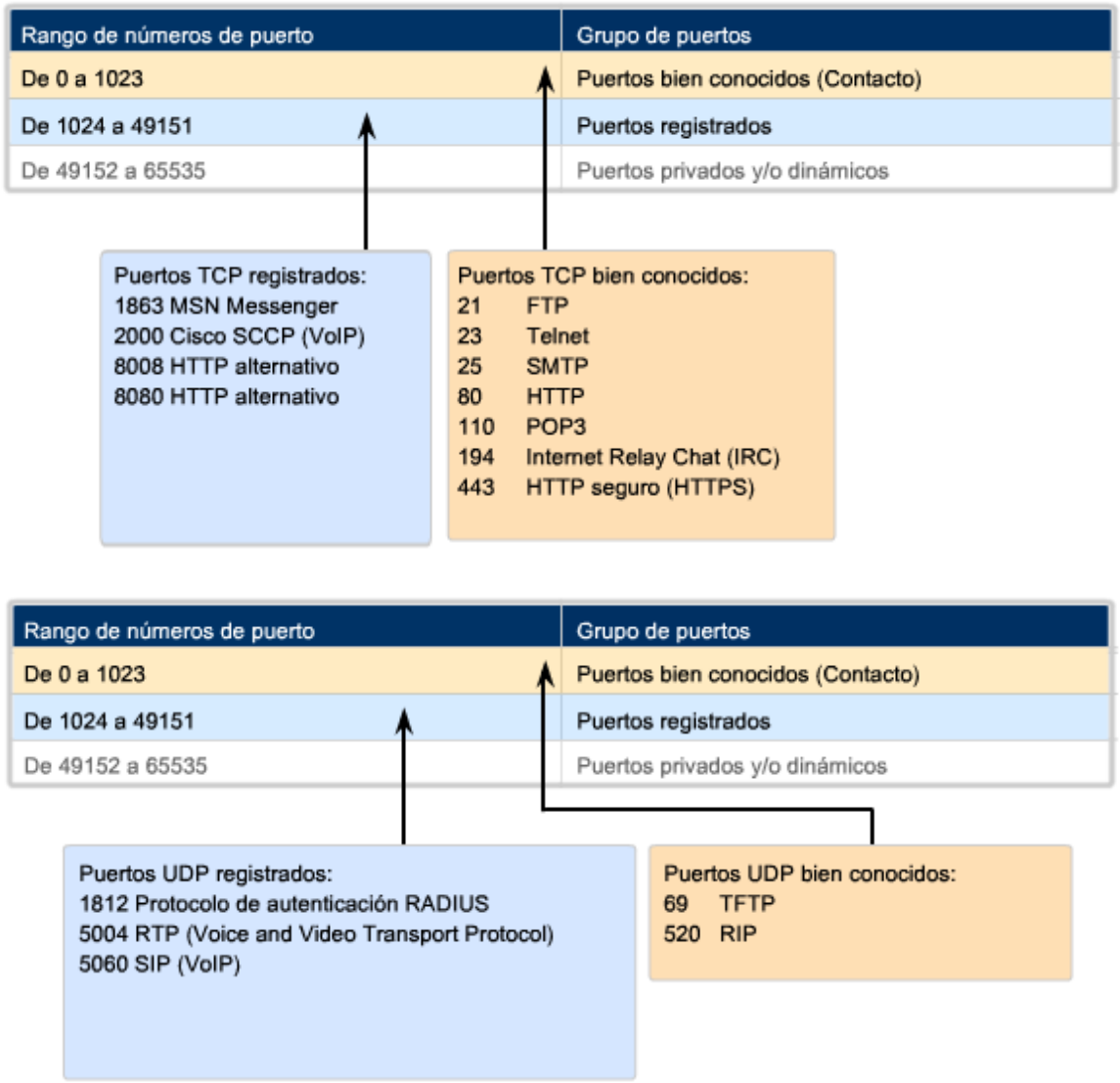
inicia una conexión. No es muy común que un cliente se conecte a un servicio utilizando un puerto dinámico o privado (aunque algunos programas que comparten archivos punto a punto lo hacen).

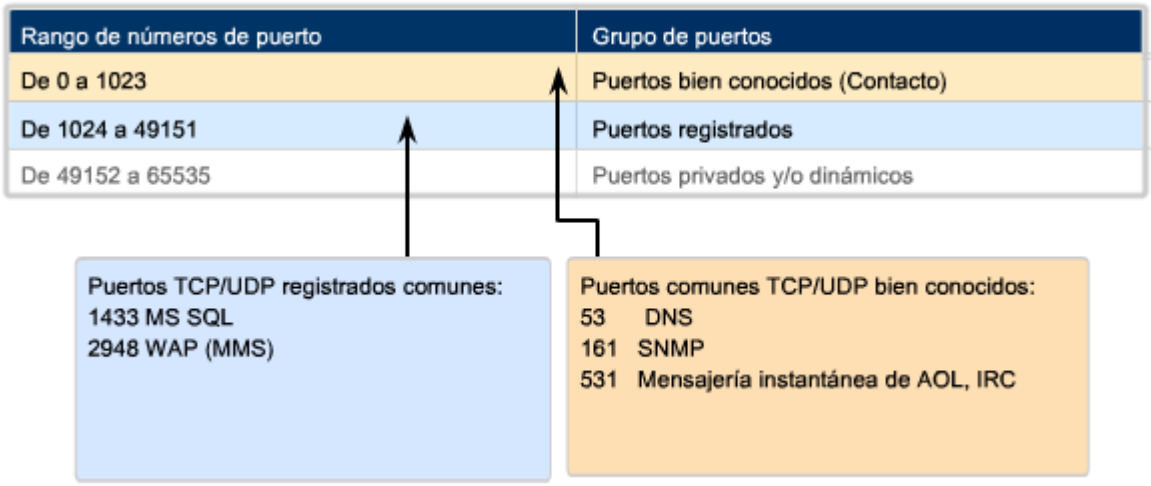
Uso de TCP y UDP

Algunas aplicaciones pueden utilizar ambos. Por ejemplo, el bajo gasto de UDP permite que DNS atienda rápidamente varias solicitudes de clientes. Sin embargo, a veces el envío de la información solicitada puede requerir la confiabilidad de TCP. En este caso, el número de puerto bien conocido de 53 lo utilizan ambos protocolos con este servicio.

Enlaces

Una lista actual de números de puerto se puede encontrar en http://www.iana.org/assignments/port-numbers.





A veces es necesario conocer las conexiones TCP activas que están abiertas y en ejecución en el host de red. Netstat es una utilidad de red importante que puede usarse para verificar esas conexiones. Netstat indica el protocolo en uso, la dirección y el número de puerto locales, la dirección y el número de puerto ajenos y el estado de la conexión.

Las conexiones TCP no descritas pueden representar una importante amenaza a la seguridad. Esto se debe a que pueden indicar que algo o alguien está conectado al host local. Además, las conexiones TCP innecesarias pueden consumir recursos valiosos del sistema y por lo tanto disminuir el rendimiento del host. Netstat debe utilizarse para determinar las conexiones abiertas de un host cuando el rendimiento parece estar comprometido.

Existen muchas opciones útiles para el comando netstat.

```
C:\>netstat

Active Connections

Proto    Local Address          Foreign Address        State
TCP      kenpc:3126             192.168.0.2:netbios-ssn    ESTABLISHED
TCP      kenpc:3158             207.138.126.152:http       ESTABLISHED
TCP      kenpc:3159             207.138.126.169:http       ESTABLISHED
TCP      kenpc:3160             207.138.126.169:http       ESTABLISHED
TCP      kenpc:3161             sc.msn.com:http            ESTABLISHED
TCP      kenpc:3166             www.cisco.com:http         ESTABLISHED

C:\>
```

4.1.5. La capa de Red

La capa de red, o Capa 3 de OSI, provee servicios para intercambiar secciones de datos individuales a través de la red entre dispositivos finales identificados. Para realizar este transporte de extremo a extremo la Capa 3 utiliza cuatro procesos básicos:
Direccionamiento
Encapsulación
Enrutamiento
Desencapsulación

Direccionamiento

Primero, la capa de red debe proporcionar un mecanismo para direccionar estos dispositivos finales. Si las secciones individuales de datos deben dirigirse a un dispositivo final, este dispositivo debe tener una dirección única. En una red IPv4, cuando se agrega esta dirección a un dispositivo, al dispositivo se lo denomina host.

Encapsulación

Segundo, la capa de red debe proporcionar encapsulación. Los dispositivos no deben ser identificados sólo con una dirección; las secciones individuales, las PDU de la capa de red, deben, además, contener estas direcciones. Durante el proceso de encapsulación, la Capa 3 recibe la PDU de la Capa 4 y agrega un encabezado o etiqueta de Capa 3 para crear la PDU de la Capa 3. Cuando nos referimos a la capa de red, denominamos paquete a esta PDU. Cuando se crea un paquete, el encabezado debe contener, entre otra información, la dirección del host hacia el cual se lo está enviando. A esta dirección se la conoce como dirección de destino. El encabezado de la Capa 3 también contiene la dirección del host de origen. A esta dirección se la denomina dirección de origen.

Después de que la capa de red completa el proceso de encapsulación, el paquete se envía a la capa de enlace de datos a fin de prepararse para el transporte a través de los medios.

Enrutamiento

Luego, la capa de red debe proporcionar los servicios para dirigir estos paquetes a su host de destino. Los host de origen y destino no siempre están conectados a la misma red. En realidad, el paquete podría recorrer muchas redes diferentes. A lo largo de la ruta, cada paquete debe ser

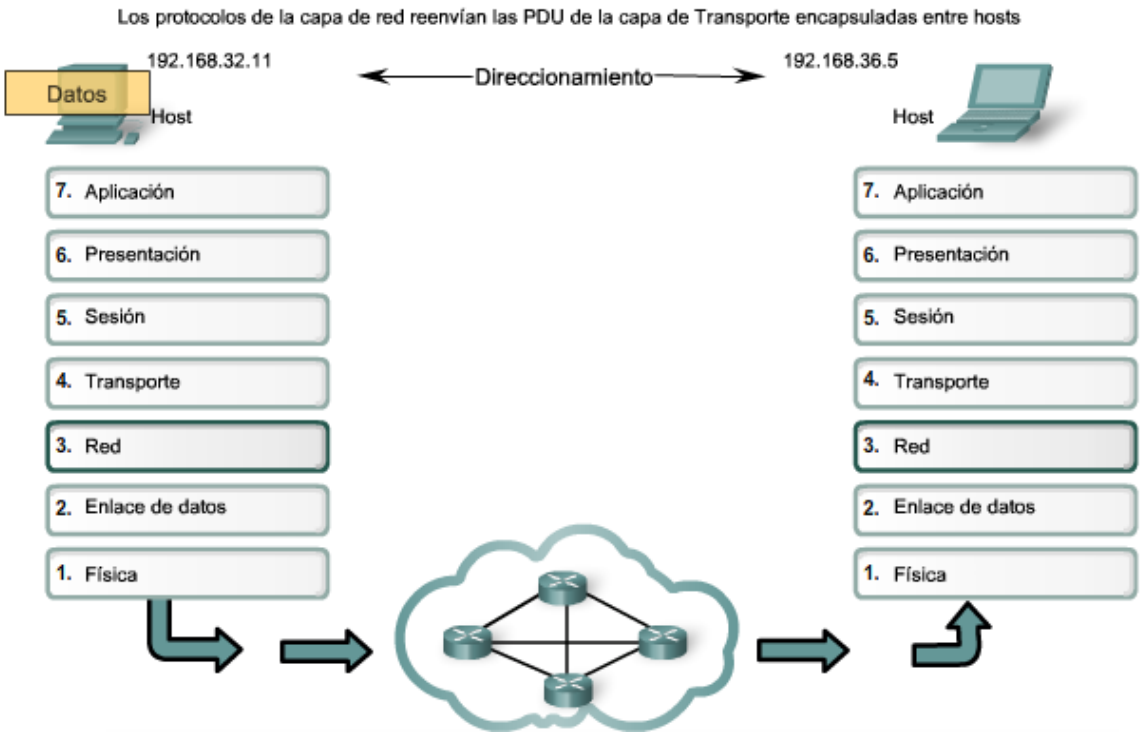
guiado a través de la red para que llegue a su destino final. Los dispositivos intermediarios que conectan las redes son los routers. La función del router es seleccionar las rutas y dirigir paquetes hacia su destino. Este proceso se conoce como enrutamiento.

Durante el enrutamiento a través de una internetwork, el paquete puede recorrer muchos dispositivos intermediarios. A cada ruta que toma un paquete para llegar al próximo dispositivo se la llama salto. A medida que se reenvía el paquete, su contenido (la unidad de datos del protocolo [PDU] de la capa de transporte) permanece intacto hasta que llega al host de destino.

Desencapsulación

Finalmente, el paquete llega al host de destino y es procesado en la Capa 3. El host examina la dirección de destino para verificar que el paquete fue direccionado a este dispositivo. Si la dirección es correcta, el paquete es desencapsulado por la capa de red y la PDU de la Capa 4 contenida en el paquete pasa hasta el servicio adecuado en la capa de Transporte.

A diferencia de la capa de transporte (Capa 4 de OSI), que administra el transporte de datos entre los procesos que se ejecutan en cada host final, los protocolos de la capa de transporte especifican la estructura y el procesamiento del paquete utilizados para llevar los datos desde un host hasta otro host. Operar ignorando los datos de aplicación que se llevan en cada paquete permite a la capa de red llevar paquetes para múltiples tipos de comunicaciones entre diversos hosts.



Protocolos de la capa de red

Los protocolos implementados en la capa de red que llevan datos del usuario son:

- Protocolo de Internet versión 4 (IPv4)
- Protocolo de Internet versión 6 (IPv6)
- Intercambio Novell de paquetes de internetwork (IPX)
- AppleTalk
- Servicio de red sin conexión (CLNS/DECNet)

El Protocolo de Internet (IPv4 e IPv6) es el protocolo de transporte de datos de la Capa 3 más ampliamente utilizado y será el tema de este curso. Los demás protocolos no se analizarán en profundidad.

4.1.6. Capa de enlace de datos

La capa de enlace de datos proporciona un medio para intercambiar datos a través de medios locales comunes.

La capa de enlace de datos realiza dos servicios básicos:
Permite a las capas superiores acceder a los medios usando técnicas como tramas.
Controla cómo se ubican los datos en los medios y cómo se reciben desde los medios usando técnicas como el control de acceso a los medios y la detección de errores.

Al igual que con cada una de las capas OSI, existen términos específicos para esta capa:

Trama: la PDU de la capa de enlace de datos

Nodo: la notación de la Capa 2 para dispositivos de red conectados a un medio común

Medios/medio (físico)*: los medios físicos para la transferencia de información entre dos nodos

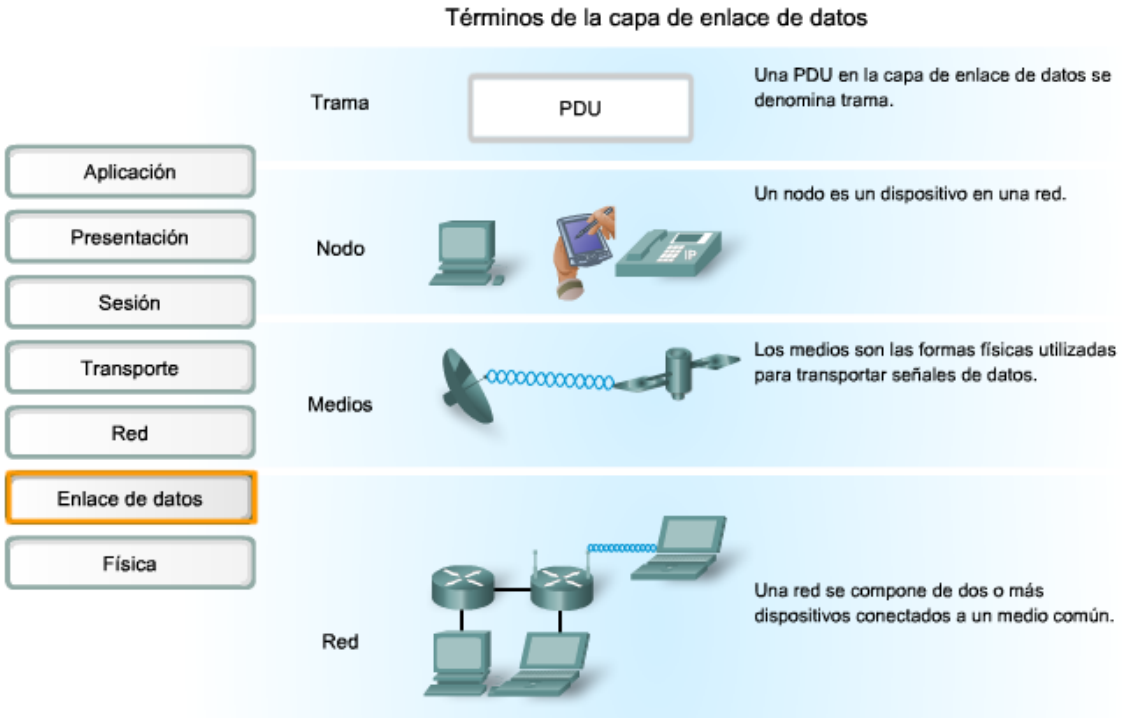
Red (física)**: dos o más nodos conectados a un medio común

La capa de enlace de datos es responsable del intercambio de tramas entre nodos a través de los medios de una red física.

* Es importante comprender el significado de las palabras medio y medios dentro del contexto de este capítulo. Aquí, estas palabras se refieren al material que realmente transporta las señales que representan los datos transmitidos. Los medios son el cable de cobre, la fibra óptica físicos o el entorno a través de los cuales la señal viaja. En este capítulo, medios no se refiere a programación

de contenido tal como audio, animación, televisión y video, como se utiliza al referirse a contenidos digitales y multimedia.

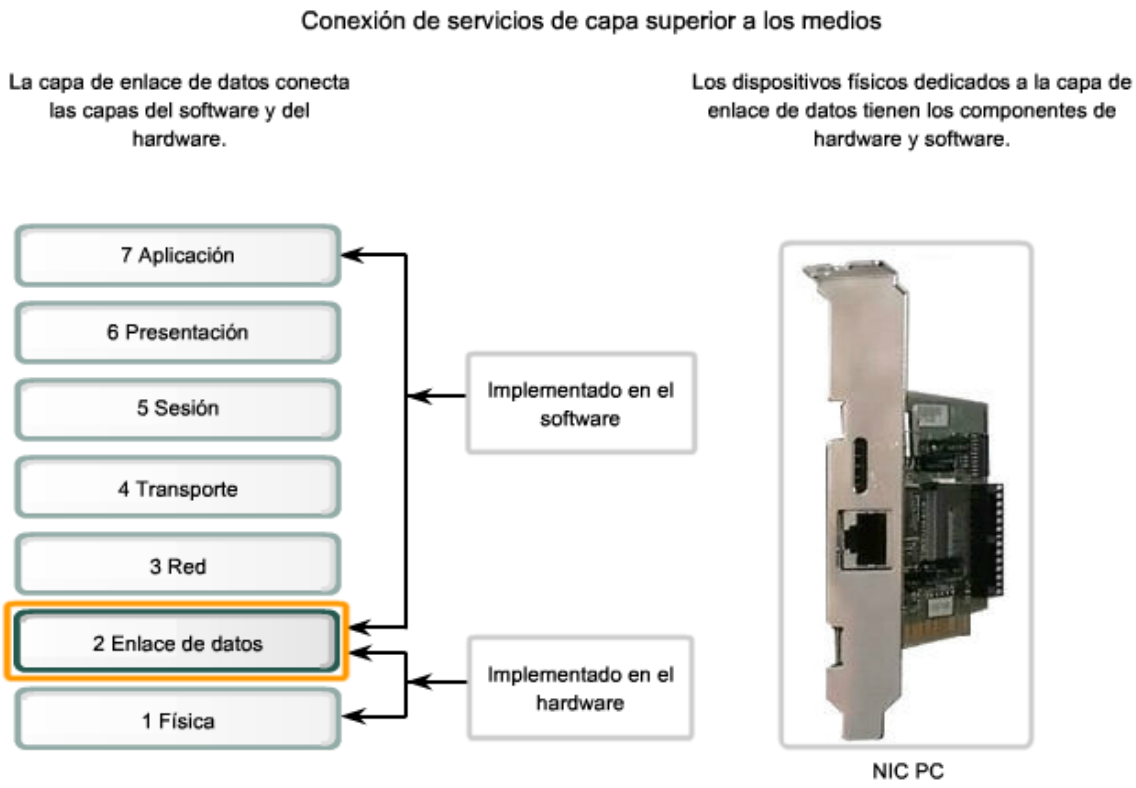
** Una red física es diferente de una red lógica. Las redes lógicas se definen en la capa de red mediante la configuración del esquema de direccionamiento jerárquico. Las redes físicas representan la interconexión de dispositivos de medios comunes. Algunas veces, una red física también se denomina segmento de red.



Conexión de servicios de capa superior a los medios

La capa de enlace de datos existe como una capa de conexión entre los procesos de software de las capas por encima de ella y de la capa física debajo de ella. Como tal, prepara los paquetes de capa de red para la transmisión a través de alguna forma de medio, ya sea cobre, fibra o entornos o medios inalámbricos.

En muchos casos, la capa de enlace de datos está incorporada como una entidad física, tal como una tarjeta de interfaz de red (NIC) de Ethernet, que se inserta dentro del bus del sistema de una computadora y realiza la conexión entre los procesos de software que se ejecutan en la computadora y en los medios físicos. Sin embargo, la NIC no es solamente una entidad física. El software asociado con la NIC permite que ésta realice sus funciones de intermediara preparando los datos para la transmisión y codificándolos como señales que se envían en los medios asociados.



Estándares

A diferencia de los protocolos de las capas superiores del conjunto de aplicaciones TCP/IP, los protocolos de capa de enlace de datos generalmente no están definidos por la solicitud de comentarios (RFC). A pesar de que el Grupo de trabajo de ingeniería de Internet (IETF) mantiene los protocolos y servicios funcionales para la suite de protocolos TCP/IP en las capas superiores, la IETF no define las funciones ni la operación de esa capa de acceso a la red del modelo. La capa de acceso de red TCP/IP es el equivalente de las capas de enlace de datos OSI y la física. Estas dos capas se verán en capítulos separados para un análisis más detallado.

Los protocolos y servicios funcionales en la capa de enlace de datos son descritos por organizaciones de ingeniería (como IEEE, ANSI e ITU) y compañías de comunicaciones. Las organizaciones de ingeniería establecen estándares y protocolos públicos y abiertos. Las compañías de comunicaciones pueden establecer y utilizar protocolos propios para aprovechar los nuevos avances en tecnología o las oportunidades del mercado.

Los servicios y las especificaciones de la capa de enlace de datos se definen mediante varios estándares basados en una variedad de tecnologías y medios a los cuales se aplican los protocolos. Algunos de estos estándares integran los servicios de la Capa 2 y la Capa 1.

Las organizaciones de ingeniería que definen estándares y protocolos abiertos que se aplican a la capa de enlace de datos incluyen:

Organización Internacional para la Estandarización (ISO)
Instituto de Ingenieros Eléctricos y Electrónicos (IEEE)
Instituto Nacional Estadounidense de Estándares (ANSI)
Unión Internacional de Telecomunicaciones (ITU)

A diferencia de los protocolos de la capa superior que están implementados principalmente en el software, como el sistema operativo de host o en aplicaciones específicas, los procesos de la capa de enlace de datos se producen tanto en el software como en el hardware. Los protocolos en esta capa se implementan dentro de la electrónica de los adaptadores de red con los que el dispositivo se conecta a la red física.

Por ejemplo, un dispositivo que implementa la capa de enlace de datos en una computadora sería la tarjeta de interfaz de red (NIC). En una computadora portátil, se utiliza comúnmente un adaptador PCMCIA inalámbrico. Cada uno de estos adaptadores es el hardware que cumple con los estándares y protocolos de la Capa 2.

http://www.iso.org

http://www.ieee.org

http://www.ansi.org

http://www.itu.int

Estándares para la capa de enlace de datos

ISO:	HDLC (Control de enlace de datos de alto nivel)
IEEE:	802.2 (LLC) 802.3 (Ethernet) 802.5 (Token Ring) 802.11(Wireless LAN [LAN inalámbrica])
ITU:	Q.922 (Estándar de Frame Relay) Q.921 (Estándar de enlace de datos ISDN) HDLC (Control de enlace de datos de alto nivel)
ANSI:	3T9.5 ADCCP (Protocolo de control de comunicación avanzada de datos)

Colocar tramas en los medios

La regulación de la colocación de tramas de datos en los medios es conocida como control de acceso al medio. Entre las diferentes implementaciones de los protocolos de la capa de enlace de datos, hay diferentes métodos de control de acceso a los medios. Estas técnicas de control de acceso a los medios definen si los nodos comparten los medios y de qué manera lo hacen.

El control de acceso a los medios es el equivalente a las reglas de tráfico que regulan la entrada de vehículos a una autopista. La ausencia de un control de acceso a los medios sería el equivalente a vehículos que ignoran el resto del tráfico e ingresan al camino sin tener en cuenta a los otros vehículos.

Sin embargo, no todos los caminos y entradas son iguales. El tráfico puede ingresar a un camino confluyendo, esperando su turno en una señal de parada o respetando el semáforo. Un conductor sigue un conjunto de reglas diferente para cada tipo de entrada.

De la misma manera, hay diferentes formas de regular la colocación de tramas en los medios. Los protocolos en la capa de enlace de datos definen las reglas de acceso a los diferentes medios.

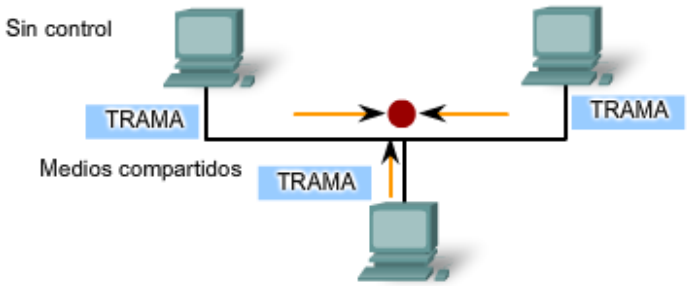
Algunos métodos de control de acceso al medio utilizan procesos altamente controlados para asegurar que las tramas se coloquen con seguridad en los medios. Estos métodos se definen mediante protocolos sofisticados que requieren mecanismos que introducen sobrecargas a la red.

El método de control de acceso a los medios que se utiliza depende de:

- Compartir medios: definir si los nodos comparten los medios y cómo lo hacen
- Topología: cómo se muestra la conexión entre los nodos a la capa de enlace de datos

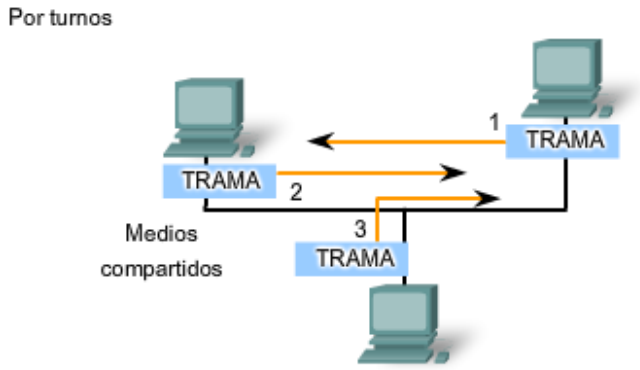
Métodos de control de acceso al medio

Si no se realiza ningún control, se producirían muchas colisiones.Las colisiones producen tramas corruptas que deben volver a enviarse.



Los métodos que cumplen con un alto grado de control impiden las colisiones, pero el proceso tiene muchas sobrecargas.

Los métodos que cumplen con un bajo nivel de control tienen pocas sobrecargas, pero hay colisiones con mayor frecuencia.



Control del acceso del medio para medios compartidos

Algunas topologías de la red comparten un medio común con varios nodos. En cualquier momento puede haber una cantidad de dispositivos que intentan enviar y recibir datos utilizando los medios de red. Hay reglas que rigen cómo esos dispositivos comparten los medios.

Hay dos métodos básicos de control de acceso para medios compartidos:
Controlado: cada nodo tiene su propio tiempo para utilizar el medio
Con base en la contención: todos los nodos compiten por el uso del medio

Haga clic en las pestañas de la figura para ver las diferencias entre los dos métodos.

Acceso controlado para medios compartidos

Al utilizar el método de acceso controlado, los dispositivos de red toman turnos en secuencia para acceder al medio. A este método también se le conoce como acceso programado o determinista. Si un dispositivo no necesita acceder al medio, la oportunidad de utilizar el medio pasa al siguiente dispositivo en línea. Cuando un dispositivo coloca una trama en los medios, ningún otro dispositivo puede hacerlo hasta que la trama haya llegado al destino y haya sido procesada por el destino.

Aunque el acceso controlado está bien ordenado y proporciona rendimiento predecible, los métodos deterministas pueden ser ineficientes porque un dispositivo tiene que esperar su turno antes de poder utilizar el medio.

Acceso por contención para medios compartidos

Estos métodos por contención, también llamados no deterministas, permiten que cualquier dispositivo intente acceder al medio siempre que haya datos para enviar. Para evitar caos completo en los medios, estos métodos usan un proceso de Acceso múltiple por detección de portadora (CSMA) para detectar primero si los medios están transportando una señal. Si se detecta una señal portadora en el medio desde otro nodo, quiere decir que otro dispositivo está transmitiendo. Cuando un dispositivo está intentando transmitir y nota que el medio está ocupado, esperará e intentará después de un período de tiempo corto. Si no se detecta una señal portadora, el dispositivo transmite sus datos. Las redes Ethernet e inalámbricas utilizan control de acceso al medio por contención.

Es posible que el proceso CSMA falle y que dos dispositivos transmitan al mismo tiempo. A esto se le denomina colisión de datos. Si esto ocurre, los datos enviados por ambos dispositivos se dañarán y deberán enviarse nuevamente.

Los métodos de control de acceso a los medios por contención no tienen la sobrecarga de los métodos de acceso controlado. No se requiere un mecanismo para analizar quién posee el turno para acceder al medio. Sin embargo, los sistemas por contención no escalan bien bajo un uso intensivo de los medios. A medida que el uso y el número de nodos aumenta, la probabilidad de acceder a los medios con éxito sin una colisión disminuye. Además, los mecanismos de recuperación que se requieren para corregir errores por esas colisiones disminuyen aún más el rendimiento.

Generalmente se implementa CSMA junto con un método para resolver la contención del medio. Los dos métodos comúnmente utilizados son:

CSMA/Detección de colisión

Con el método CSMA/Detección de colisión (CSMA/CD), el dispositivo controla los medios para detectar la presencia de una señal de datos. Si no hay una señal de datos, que indica que el medio está libre, el dispositivo transmite los datos. Si luego se detectan señales que muestran que otro dispositivo estaba transmitiendo al mismo tiempo, todos los dispositivos dejan de enviar e intentan después. Las formas tradicionales de Ethernet utilizan este método.

CSMA/Prevención de colisiones

Con el método CSMA/Prevención de colisiones (CSMA/CA), el dispositivo analiza los medios para detectar la presencia de una señal de datos. Si el medio está libre, el dispositivo envía una notificación a través del medio, sobre su intención de utilizarlo. El dispositivo luego envía los datos. Este método es utilizado por las tecnologías de redes inalámbricas 802.11.

Control de acceso al medio para medios no compartidos

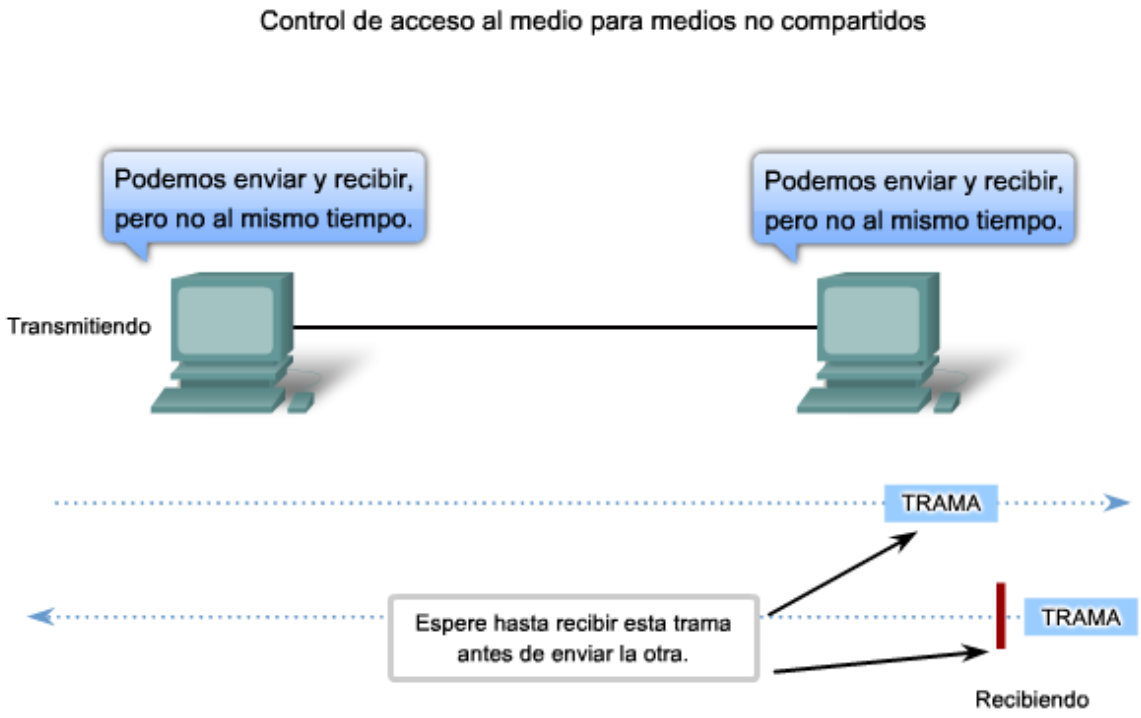
Los protocolos de control de acceso para medios no compartidos requieren poco o ningún control antes de colocar tramas en los medios. Estos protocolos tienen reglas y procedimientos más simples para el control de acceso al medio. Tal es el caso de las topologías punto a punto.

En las topologías punto a punto, los medios interconectan sólo dos nodos. En esta configuración, los nodos no necesitan compartir los medios con otros hosts ni determinar si una trama está destinada para ese nodo. Por lo tanto, los protocolos de capa de enlace de datos hacen poco para controlar el acceso a medios no compartidos.

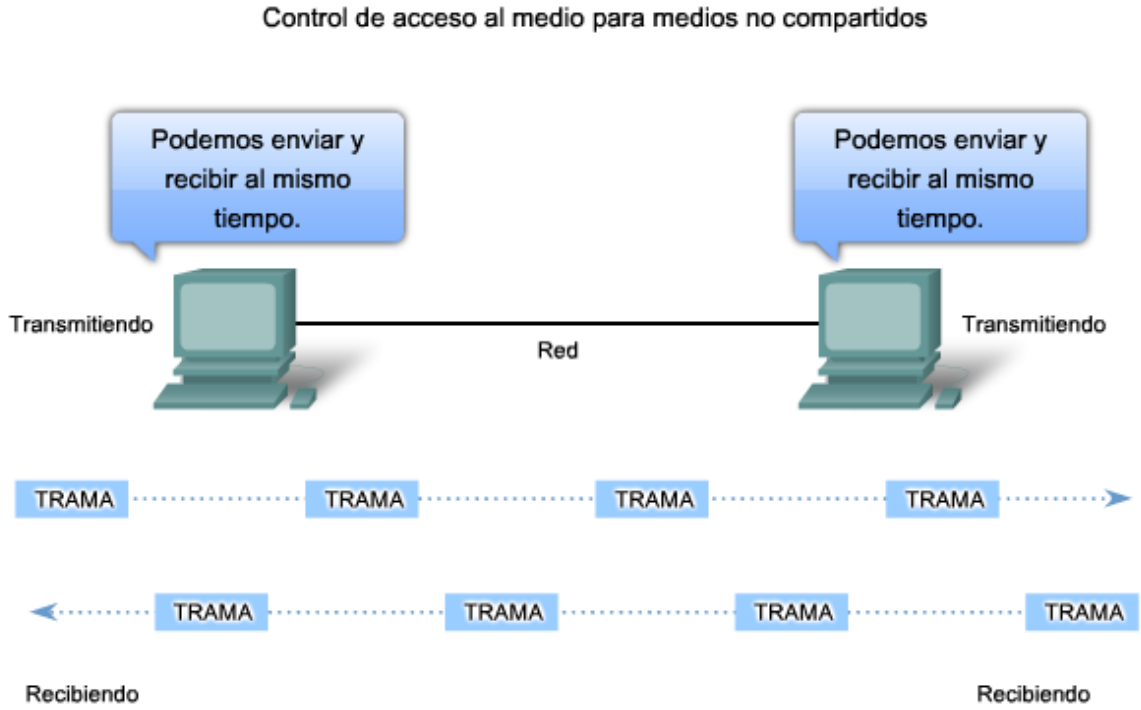
Full Duplex y Half Duplex

En conexiones punto a punto, la capa de enlace de datos tiene que considerar si la comunicación es half-duplex o full-duplex.

Comunicación half-duplex quiere decir que los dispositivos pueden transmitir y recibir en los medios, pero no pueden hacerlo simultáneamente. Ethernet ha establecido reglas de arbitraje para resolver conflictos que surgen de instancias donde más de una estación intenta transmitir al mismo tiempo.



En la comunicación full-duplex, los dos dispositivos pueden transmitir y recibir en los medios al mismo tiempo. La capa de enlace de datos supone que los medios están disponibles para transmitir para ambos nodos en cualquier momento. Por lo tanto, no hay necesidad de arbitraje de medios en la capa de enlace de datos.



Los detalles de una técnica de control de acceso a los medios específica que sólo pueden examinarse estudiando un protocolo específico. Dentro de este curso, estudiaremos Ethernet tradicional, que utiliza CSMA/CD. Otras técnicas se abarcarán en cursos posteriores.

4.1.7. Capa Fisica

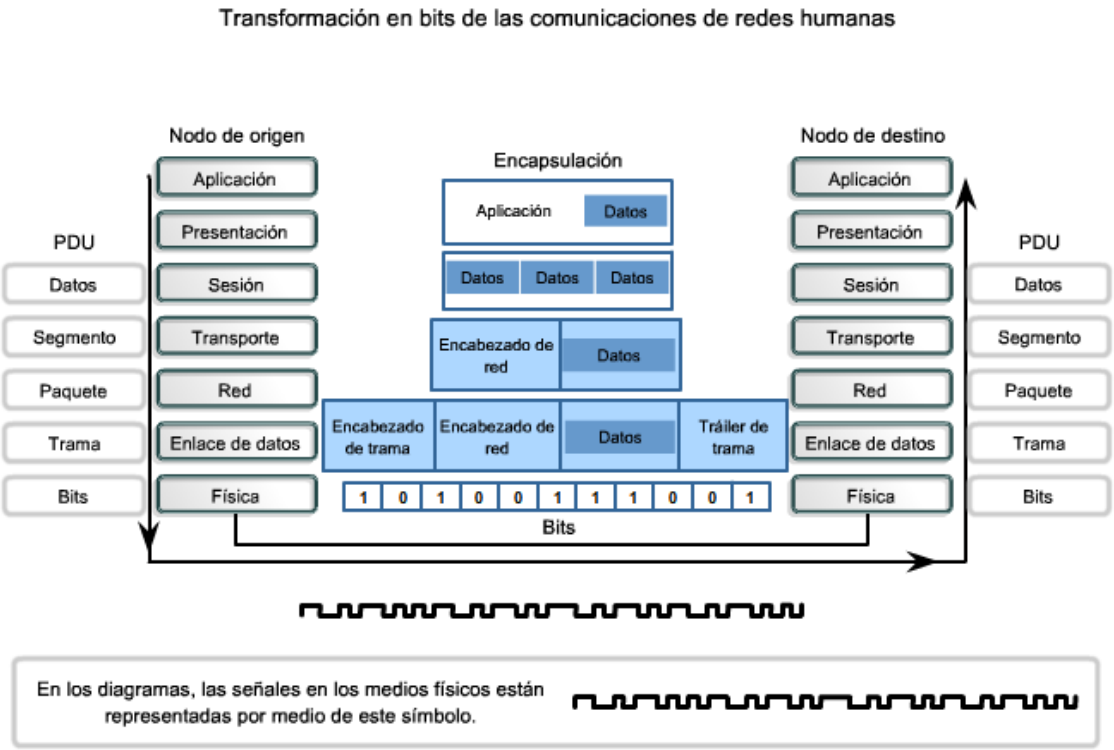
La capa Física de OSI proporciona los medios de transporte para los bits que conforman la trama de la capa de Enlace de datos a través de los medios de red. Esta capa acepta una trama completa desde la capa de Enlace de datos y la codifica como una secuencia de señales que se transmiten en los medios locales. Un dispositivo final o un dispositivo intermediario recibe los bits codificados que componen una trama.

El envío de tramas a través de medios locales requiere los siguientes elementos de la capa física:

- Medios físicos y conectores asociados
- Una representación de los bits en los medios
- Codificación de los datos y de la información de control
- Sistema de circuitos del receptor y transmisor en los dispositivos de red

En este momento del proceso de comunicación, la capa de transporte ha segmentado los datos del usuario, la capa de red los ha colocado en paquetes y luego la capa de enlace de datos los ha encapsulado como tramas. El objetivo de la capa Física es crear la señal óptica, eléctrica o de microondas que representa a los bits en cada trama. Luego, estas señales se envían por los medios una a la vez.

Otra función de la capa física es la de recuperar estas señales individuales desde los medios, restaurarlas para sus representaciones de bit y enviar los bits hacia la capa de enlace de datos como una trama completa.



Funcionamiento

Los medios no transportan la trama como una única entidad. Los medios transportan señales, una por vez, para representar los bits que conforman la trama.

Existen tres tipos básicos de medios de red en los cuales se representan los datos:

- Cable de cobre
- Fibra
- Inalámbrico

La presentación de los bits (es decir, el tipo de señal) depende del tipo de medio. Para los medios de cable de cobre, las señales son patrones de pulsos eléctricos. Para los medios de fibra, las señales son patrones de luz. Para los medios inalámbricos, las señales son patrones de transmisiones de radio.

Identificación de una trama

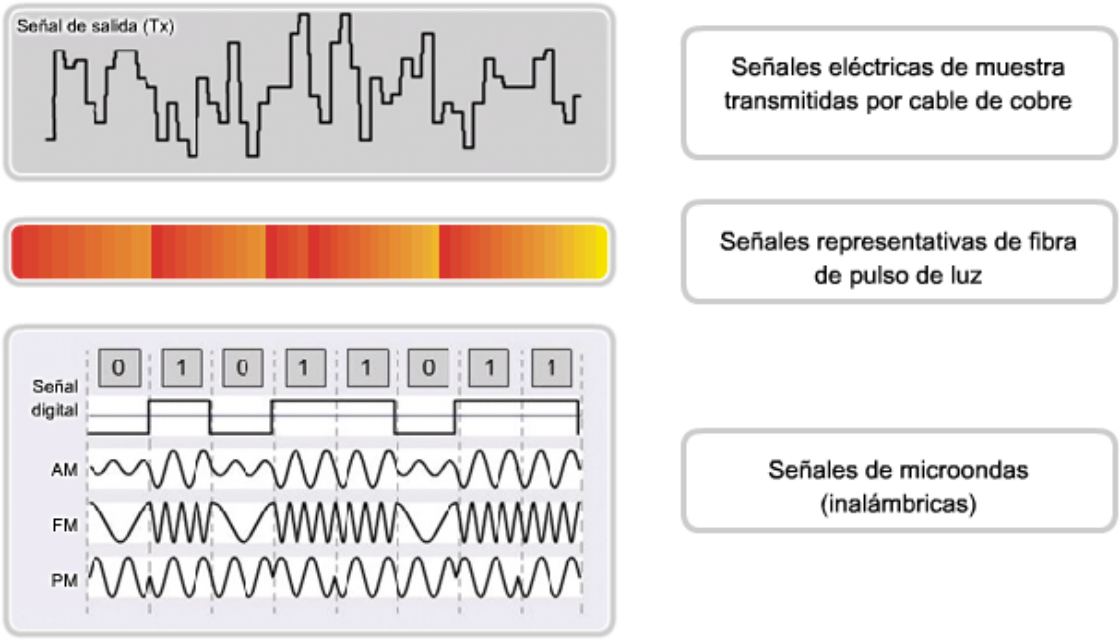
Cuando la capa física codifica los bits en señales para un medio específico, también debe distinguir dónde termina una trama y dónde se inicia la siguiente. De lo contrario, los dispositivos de los medios no reconocerían cuándo se ha recibido exitosamente una trama. En tal caso, el dispositivo de destino sólo recibiría una secuencia de señales y no sería capaz de reconstruir la trama correctamente. Como se describió en el capítulo anterior, indicar el comienzo de la trama es a

menudo una función de la capa de Enlace de datos. Sin embargo, en muchas tecnologías, la capa Física puede agregar sus propias señales para indicar el comienzo y el final de la trama.

Para habilitar un dispositivo receptor a fin de reconocer de manera clara el límite de una trama, el dispositivo transmisor agrega señales para designar el comienzo y el final de una trama. Estas señales representan patrones específicos de bits que sólo se utilizan para indicar el comienzo y el final de una trama.

En las siguientes secciones de este capítulo se analizarán detalladamente el proceso de codificación de una trama de datos de bits lógicos a señales físicas en los medios y las características de los medios físicos específicos.

Representaciones de señales en los medios físicos



Estandares

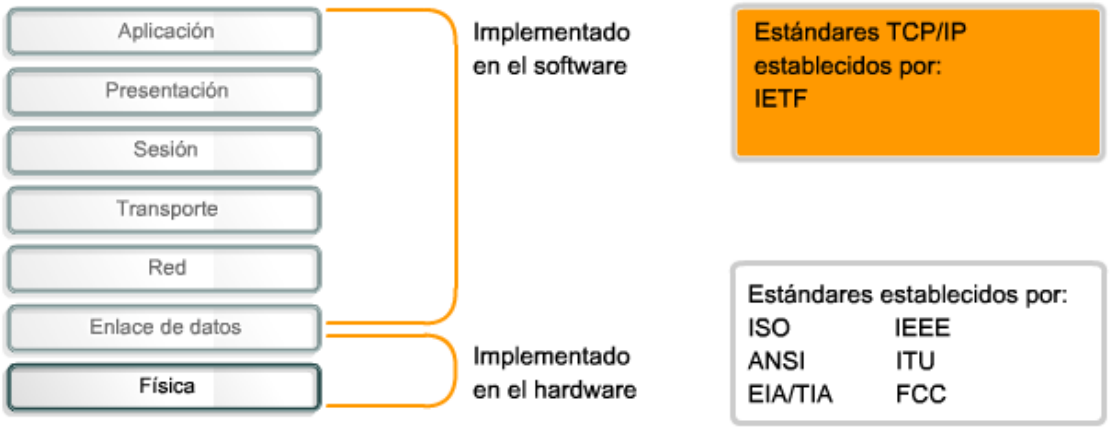
La capa física consiste en un hardware creado por ingenieros en forma de conectores, medios y circuitos electrónicos. Por lo tanto, es necesario que las principales organizaciones especializadas en ingeniería eléctrica y en comunicaciones definan los estándares que rigen este hardware.

Por el contrario, las operaciones y los protocolos de las capas superiores de OSI se llevan a cabo mediante un software y están diseñados por especialistas informáticos e ingenieros de software. Como vimos en el capítulo anterior, el grupo de trabajo de ingeniería de Internet (IETF) define los servicios y protocolos del conjunto TCP/IP en las RFC.

Al igual que otras tecnologías asociadas con la capa de Enlace de datos, las tecnologías de la capa Física se definen por diferentes organizaciones, tales como:

- Organización Internacional para la Estandarización (ISO)
- Instituto de Ingenieros Eléctricos y Electrónicos (IEEE)
- Instituto Nacional Estadounidense de Estándares (ANSI)
- Unión Internacional de Telecomunicaciones (ITU)
- La Asociación de Industrias Electrónicas y la Asociación de las Industrias de las Telecomunicaciones (EIA/TIA)
- Autoridades de las telecomunicaciones nacionales, como la Comisión Federal de Comunicaciones (FCC) en EE. UU.

Comparación entre los estándares de capa física y los estándares de capa superior



Hardware y tecnologías de la capa física

Las tecnologías definidas por estas organizaciones incluyen cuatro áreas de estándares de la capa física:
Propiedades físicas y eléctricas de los medios
Propiedades mecánicas (materiales, dimensiones, diagrama de pines) de los conectores
Representación de los bits mediante señales (codificación)
Definición de las señales de la información de control

Todos los componentes de hardware, como adaptadores de red (NIC, tarjeta de interfaz de red), interfaces y conectores, materiales y diseño de los cables, se especifican en los estándares asociados con la capa física.

Capacidad para transportar datos

Los diferentes medios físicos admiten la transferencia de bits a distintas velocidades. La transferencia de datos puede medirse de tres formas:

- Ancho de banda
- Rendimiento
- Capacidad de transferencia útil

Ancho de banda

La capacidad que posee un medio de transportar datos se describe como el ancho de banda de los datos sin procesar de los medios. El ancho de banda digital mide la cantidad de información que puede fluir desde un lugar hacia otro en un período de tiempo determinado. El ancho de banda generalmente se mide en kilobits por segundo (kbps) o megabits por segundo (Mbps).

El ancho de banda práctico de una red se determina mediante una combinación de factores: las propiedades de las tecnologías y los medios físicos elegidos para señalizar y detectar señales de red.

Las propiedades de los medios físicos, las tecnologías actuales y las leyes de la física desempeñan una función al momento de determinar el ancho de banda disponible.

Unidades de ancho de banda, velocidad de transmisión (throughput) y capacidad de transferencia útil

Unidad de ancho de banda	Abreviatura	Equivalencia
Bits por segundo	bps	1 bps = unidad fundamental de ancho de banda
Kilobits por segundo	kbps	1kbps = 1000bps = 10^3bps
Megabits por segundo	Mbps	1Mbps = 1000000bps = 10^6bps
Gigabits por segundo	Gbps	1Gbps = 1000000000bps = 10^9bps
Terabits por segundo	Tbps	1Tbps = 1000000000000bps = 10^12bps

Rendimiento

El rendimiento es la medida de transferencia de bits a través de los medios durante un período de tiempo determinado. Debido a diferentes factores, el rendimiento generalmente no coincide con el ancho de banda especificado en las implementaciones de la capa física, como Ethernet.

Muchos factores influyen en el rendimiento. Entre estos factores se incluye la cantidad y el tipo de tráfico además de la cantidad de dispositivos de red que se encuentran en la red que se está

midiendo. En una topología multiacceso como Ethernet, los nodos compiten por el acceso y la utilización de medios. Por lo tanto, el rendimiento de cada nodo se degrada a medida que aumenta el uso de los medios.

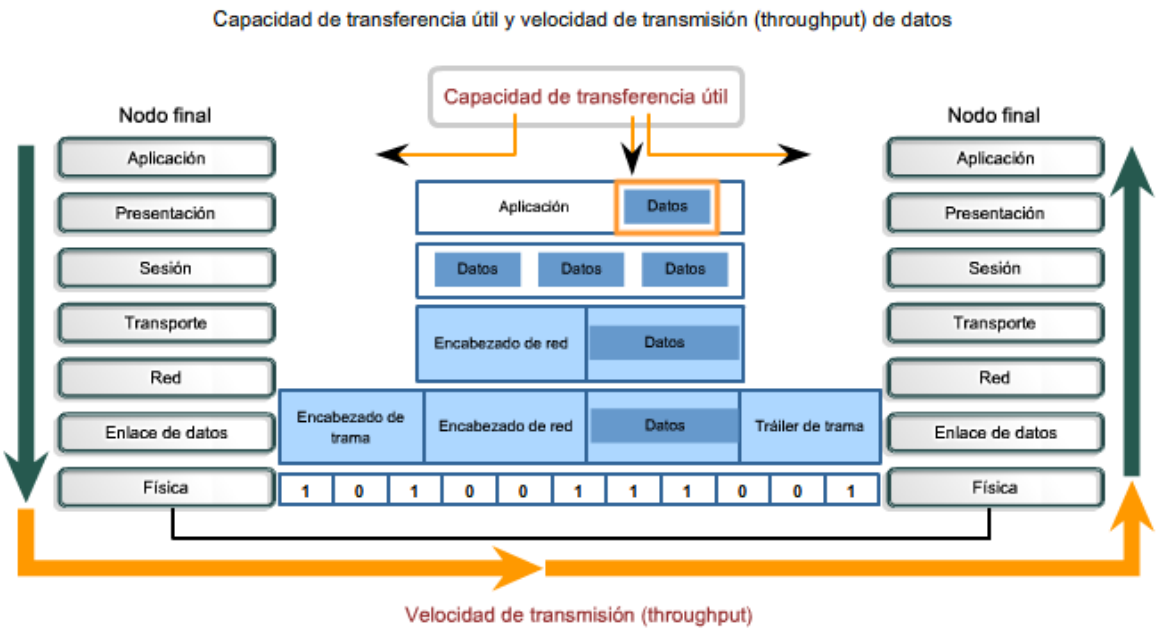
En una internetwork o una red con múltiples segmentos, el rendimiento no puede ser más rápido que el enlace más lento de la ruta de origen a destino. Incluso si todos los segmentos o gran parte de ellos tienen un ancho de banda elevado, sólo se necesita un segmento en la ruta con un rendimiento inferior para crear un cuello de botella en el rendimiento de toda la red.

Capacidad de transferencia útil

Se ha creado una tercera medida para evaluar la transferencia de datos utilizables. Dicha medición se denomina capacidad de transferencia útil. La capacidad de transferencia útil es la medida de datos utilizables transferidos durante un período de tiempo determinado. Por lo tanto, es la medida de mayor interés para los usuarios de la red.
Como se muestra en la figura, la capacidad de transferencia útil mide la transferencia efectiva de los datos del usuario entre las entidades de la capa de aplicación, por ejemplo entre el proceso de un servidor web de origen y un dispositivo con explorador web de destino.

A diferencia del rendimiento, que mide la transferencia de bits y no la transferencia de datos utilizables, la capacidad de transferencia útil considera los bits que generan la sobrecarga del protocolo. Esta capacidad representa el rendimiento sin la sobrecarga de tráfico para establecer sesiones, acuses de recibo y encapsulaciones.

Por ejemplo, considere dos hosts en una LAN que transfiere un archivo. El ancho de banda de la LAN es de 100 Mbps. Debido al uso compartido y al encabezado de los medios, el rendimiento entre los equipos es solamente de 60 mbps. Con una sobrecarga del proceso de encapsulación de stack TCP/IP, la velocidad real de los datos recibidos por la computadora de destino, es decir la capacidad de transferencia útil, es sólo de 40 Mbps.



La velocidad de transmisión (throughput) de datos es el rendimiento real de la red. La capacidad de transferencia útil es una medida de la transferencia de datos utilizables una vez que se ha eliminado el tráfico de encabezado de protocolo.

Tipos de medios fisicos

La capa física se ocupa de la señalización y los medios de red. Esta capa produce la representación y agrupación de bits en voltajes, radiofrecuencia e impulsos de luz. Muchas organizaciones que establecen estándares han contribuido con la definición de las propiedades mecánicas, eléctricas y físicas de los medios disponibles para diferentes comunicaciones de datos. Estas especificaciones garantizan que los cables y los conectores funcionen según lo previsto mediante diferentes implementaciones de la capa de enlace de datos.

Por ejemplo, los estándares para los medios de cobre se definen según lo siguiente:
Tipo de cableado de cobre utilizado
Ancho de banda de la comunicación
Tipo de conectores utilizados
Diagrama de pines y códigos de colores de las conexiones a los medios
Distancia máxima de los medios

La figura muestra algunas de las características de los medios de networking.

Esta sección también describirá algunas de las características importantes de los medios inalámbricos, ópticos y de cobre comúnmente utilizados.

Medios físicos: Características

Medios Ethernet

	10BASE-T	100BASE-TX	100BASE-FX	1000BASE-CX	1000BASE-T	1000BASE-SX	1000BASE-LX	1000BASE-ZX	10GBASE-ZR
Medios	UTP Categoría 3, 4, 5 EIA/TIA, cuatro pares	UTP Categoría 5 EIA/TIA, dos pares	50/62,5m fibra multimodo	STP	UTP Categoría 5 (o superior) EIA/TIA, cuatro pares	fibra multimodo de 50/62,5 micrones	fibra multimodo de 50/62,5 micrones o fibra monomodo de 9 micrones	fibra monomodo de 9m	fibra monomodo de 9m
Longitud máxima del segmento	100m (328 pies)	100m (328 pies)	2km (6562 pies)	25m (82 pies)	100m (328 pies)	Hasta 550m (1804 pies) según la fibra utilizada	550m (MMF)10km (SMF)	Aprox. 70km	Hasta 80km
Topología	Estrella	Estrella	Estrella	Estrella	Estrella	Estrella	Estrella	Estrella	Estrella
Conector	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)		ISO 8877 (RJ-45)					

Medios físicos: Características

Medios inalámbricos

Estándares	Bluetooth 802.15	802.11 (a, b, g, n), HiperLAN 2	802, 11, MMDS, LMDS	GSM, GPRS, CDMA, de 2,5 a 3G
Velocidad	<1Mbps	de 1 a 54+ Mbps	22Mbps+	de 10 a 384Kbps
Rango	Corto	Medio	De medio a largo	Largo
Aplicaciones	Punto a punto dispositivo a dispositivo	Redes empresariales	Fijo, acceso de última milla	PDA, teléfonos móviles, acceso celular