Redes

Manual

Vol. 4 (Capa 5, 6 y 7 Modelo OSI)

ALHUBO

Alejandro Huerta Bolaños

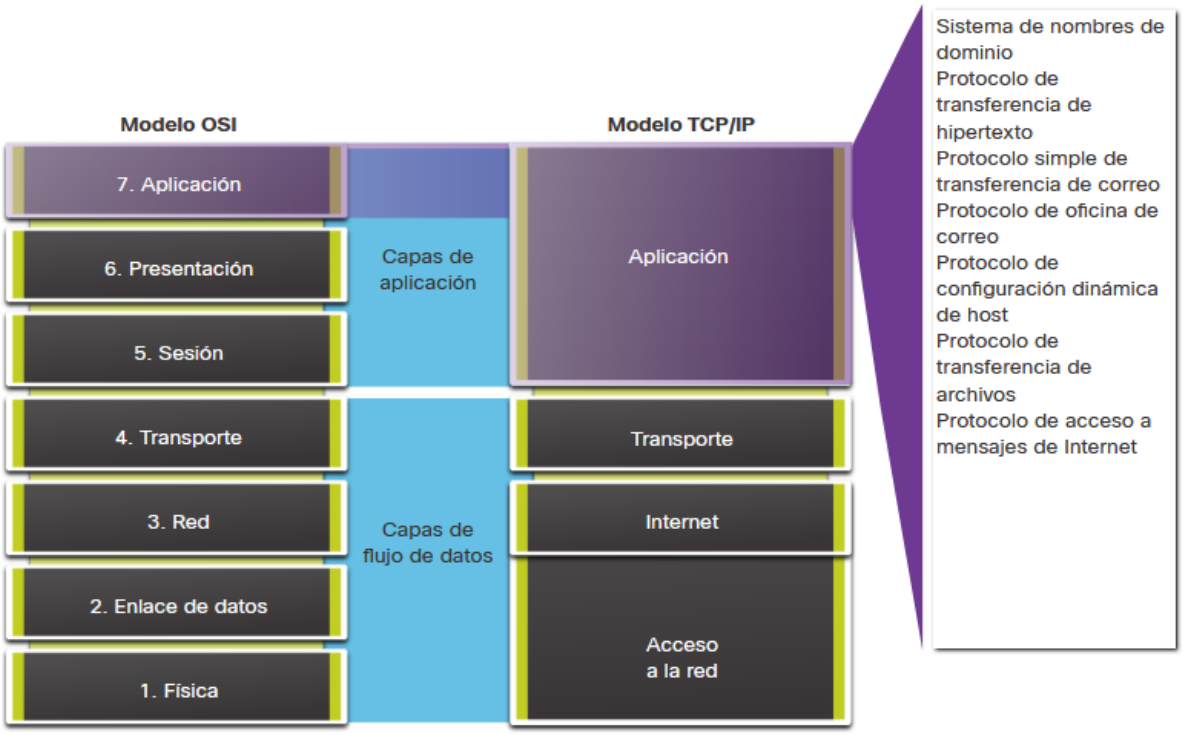
Primera Edición

2023

Índice

Capa de aplicación

En los modelo OSI y TCP/IP La capa de aplicación es la más cercana al usuario final. Como se muestra en la figura, es la capa que proporciona la interfaz entre las aplicaciones utilizada para la comunicación 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.



Basado en el modelo TCP/IP Las tres capas superiores del modelo OSI (aplicación, presentación y sesión) definen funciones de la capa de aplicación TCP/IP única.

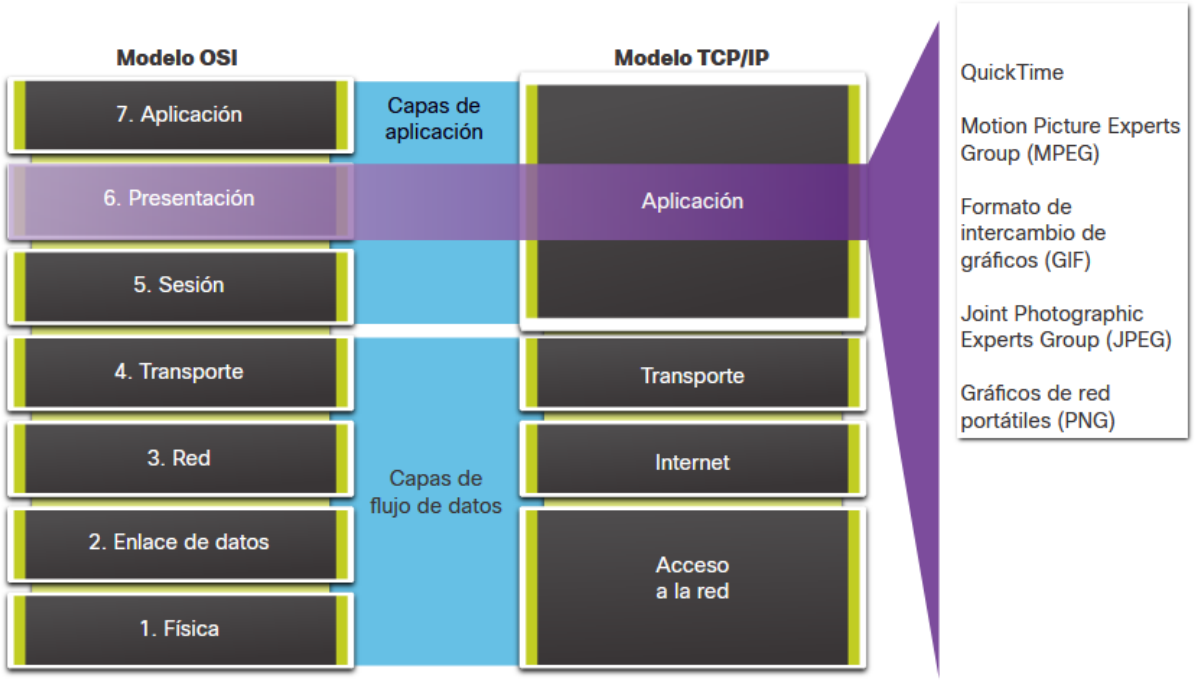
Existen muchos protocolos de capa de aplicación, y están en constante desarrollo. Algunos de los protocolos de capa de aplicación más conocidos incluyen el protocolo de transferencia de hipertexto (HTTP), el protocolo de transferencia de archivos (FTP), el protocolo trivial de transferencia de archivos (TFTP), el protocolo de acceso a mensajes de Internet (IMAP) y el protocolo del sistema de nombres de dominios (DNS).

Capa de presentación

La capa de presentación tiene tres funciones principales:

- Dar formato a los datos del dispositivo de origen, o presentarlos, en una forma compatible para que lo reciba el dispositivo de destino.
- Comprimir los datos de forma tal que los pueda descomprimir el dispositivo de destino.
- Cifrar los datos para transmitirlos y descifrarlos al recibirlos.

Como se muestra en la ilustración, la capa de presentación da formato a los datos para la capa de aplicación y establece estándares para los formatos de archivo. Dentro de los estándares más conocidos para vídeo encontramos QuickTime y el Grupo de expertos en películas (MPEG). Entre los formatos gráficos de imagen conocidos que se utilizan en redes, se incluyen los siguientes: formato de intercambio de gráficos (GIF), formato del Joint Photographic Experts Group (JPEG) y formato de gráficos de red portátiles (PNG).



Capa de Sesión

Como su nombre lo indica, las funciones de la capa de sesión 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 que estuvieron inactivas durante un período prolongado.

Protocolos de capa de aplicación de TCP/IP

Los protocolos de aplicación TCP/IP especifican el formato y la información de control necesarios para muchas funciones de comunicación comunes de Internet. Los protocolos de capa de aplicación son utilizados tanto por los dispositivos de origen como de destino durante una sesión de comunicación. Para que las comunicaciones se lleven a cabo correctamente, los protocolos de capa de aplicación que se implementaron en los hosts de origen y de destino deben ser compatibles.

Sistema de nombres

DNS - Sistema de nombres de dominio (o servicio)

- TCP, UDP cliente 53
- Traduce los nombres de dominio tales como cisco.com a direcciones IP

Configuración de host

BOOTP - Protocolo de arranque

- Cliente UDP 68, servidor 67
- Permite que una estación de trabajo sin disco obtenga su propia dirección IP, la dirección IP de un servidor BOOTP en la red y un archivo que se debe cargar en la memoria para arrancar la máquina.
- El protocolo DHCP reemplaza al protocolo BOOTP.

DHCP - Dynamic Host Configuration Protocol

- Cliente UDP 68, servidor 67
- Permite que las direcciones vuelvan a utilizarse cuando ya no son necesarias

Correo electrónico

SMTP - Protocolo simple de transferencia de correo.

- TCP 25
- Permite a los clientes enviar correo electrónico a un servidor de correo.
- Permite a los servidores enviar correo electrónico a otros servidores.

POP3 - Post Office Protocol

- TCP 110
- Permite a los clientes recibir correo electrónico de un servidor de correo.
- Descarga el correo electrónico a la aplicación de correo local del cliente

IMAP - Internet Message Access Protocol

- TCP 143

- Permite que los clientes accedan a correos electrónicos almacenados en un servidor de correo.
- Mantiene el correo electrónico en el servidor.

Transferencia de Archivos

Protocolo de transferencia de archivos (FTP, File Transfer Protocol)

- TCP 20 a 21
- Establece las reglas que permiten a un usuario en un host acceder y transferir archivos hacia y desde otro host a través de una red.
- FTP Es un protocolo confiable de entrega de archivos, orientado a la conexión y con acuse de recibo.

TFTP - Trivial File Transfer Protocol

- Cliente UDP 69
- Un protocolo de transferencia de archivos simple y sin conexión con entrega de archivos sin reconocimiento y sin el máximo esfuerzo
- Utiliza menos sobrecarga que FTP.

Web

HTTP- Protocolo de transferencia de hipertexto

- TCP 80, 8080
- Un Conjunto de reglas para intercambiar texto, imágenes gráficas, sonido, video y otros archivos multimedia en la World Wide Web.

HTTPS - HTTP Secure

- TCP, UDP 443
- El navegador usa cifrado para proteger las comunicaciones HTTP.
- Autentica el sitio web al que se conecta el navegador.

Peer-to-Peer (Punto a punto)

Modelo cliente-servidor

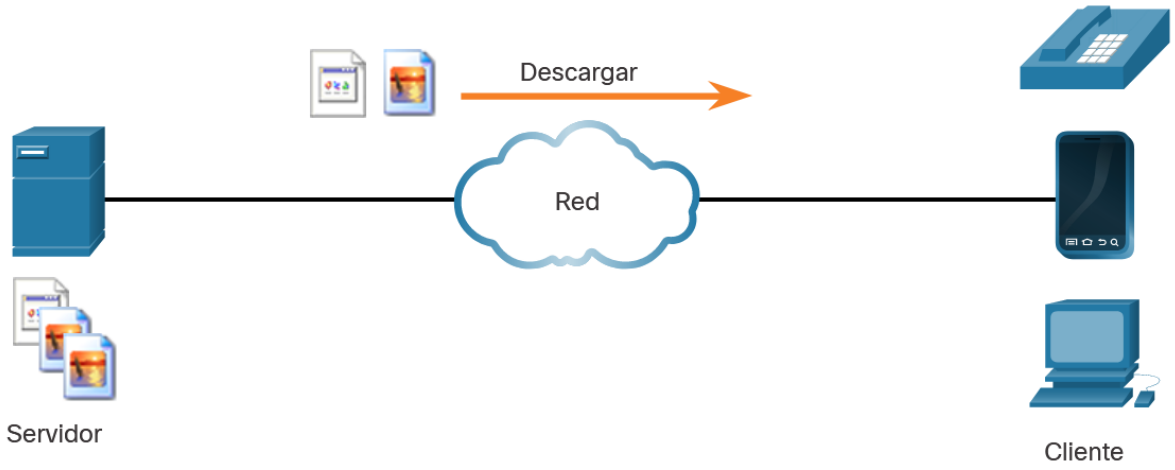
En el tema anterior, aprendió que los protocolos de capa de aplicación TCP/IP implementados tanto en el host de origen como en el de destino deben ser compatibles. En este tema aprenderá sobre el modelo cliente/servidor y los procesos utilizados, que se encuentran en la capa de aplicación. Lo mismo ocurre con una red Cliente a 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”. El cliente es una combinación de hardware/software que las personas utilizan para acceder directamente a los recursos que se almacenan en el servidor.

Los procesos de cliente y servidor se consideran parte de la capa de aplicación. El cliente comienza el intercambio solicitando los datos al servidor, quien responde enviando uno o más flujos 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 también puede requerir la autenticación del usuario y la identificación de un archivo de datos que se vaya a transferir.

Un ejemplo de una red cliente-servidor es el uso del servicio de correo electrónico de un ISP para enviar, recibir y almacenar correo electrónico. El cliente de correo electrónico en una PC doméstica emite una solicitud al servidor de correo electrónico del ISP para que se le envíe todo correo no leído. El servidor responde enviando al cliente el correo electrónico solicitado. La transferencia de datos de un cliente a un servidor se conoce como “carga” y la transferencia de datos de un servidor a un cliente se conoce como “descarga”.

Como se muestra en la figura los archivos se descargan del servidor al cliente.



Peer-to-Peer Networks (Redes entre pares)

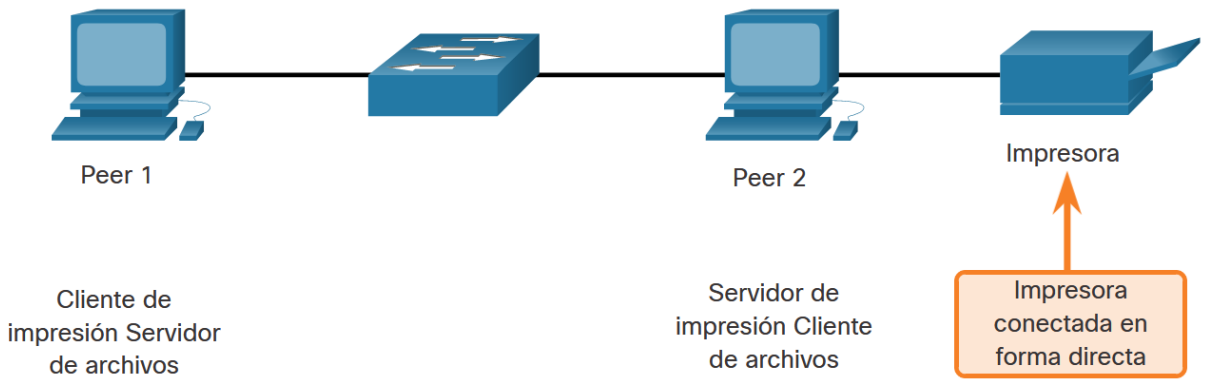
En el modelo de red entre pares (P2P), se accede a los datos de un dispositivo par sin utilizar un servidor dedicado.

El modelo de red P2P consta de dos partes: las redes P2P y las aplicaciones P2P. Ambas partes tienen características similares, pero en la práctica son muy diferentes.

En una red P2P, hay dos o más PC que están conectadas por medio de una red y pueden compartir recursos (como impresoras y archivos) sin tener un servidor dedicado. Todo terminal conectado puede funcionar como servidor y como cliente. Un equipo 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.

Además de compartir archivos, una red como esta permitiría que los usuarios habiliten juegos en red o compartan una conexión a Internet.

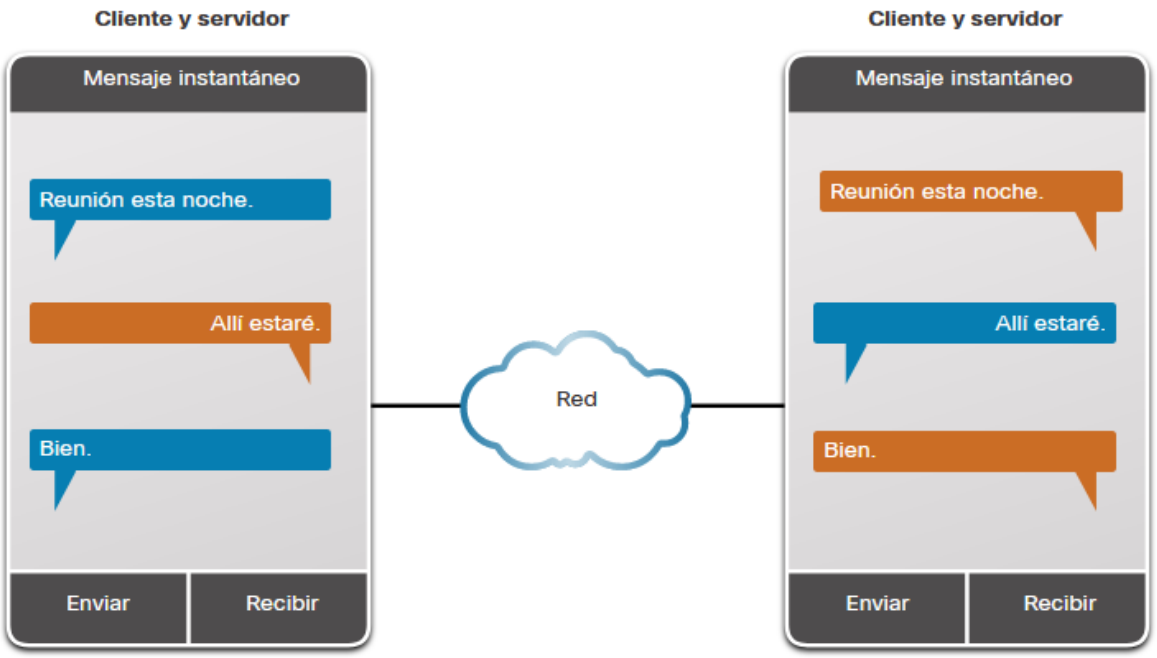
En un intercambio entre pares, ambos dispositivos se consideran iguales en el proceso de comunicación. El par 1 tiene archivos que se comparten con el par 2 y puede acceder a la impresora compartida que está conectada directamente al par 2 para imprimir archivos. El par 2 comparte la impresora conectada directamente con el par 1 mientras accede a los archivos compartidos en el par 1, como se muestra en la figura.



Peer-to-Peer Applications

Una aplicación P2P permite que un dispositivo funcione como cliente y como servidor dentro de la misma comunicación, como se muestra en la figura. En este modelo, cada cliente es un servidor y cada servidor es un cliente. Las aplicaciones P2P requieren que cada terminal proporcione una interfaz de usuario y ejecute un servicio en segundo plano.

Algunas aplicaciones P2P utilizan un sistema híbrido donde se descentraliza el intercambio de recursos, pero los índices que apuntan a las ubicaciones de los recursos están almacenados en un directorio centralizado. En un sistema híbrido, cada punto accede a un servidor de índice para obtener la ubicación de un recurso almacenado en otro punto.

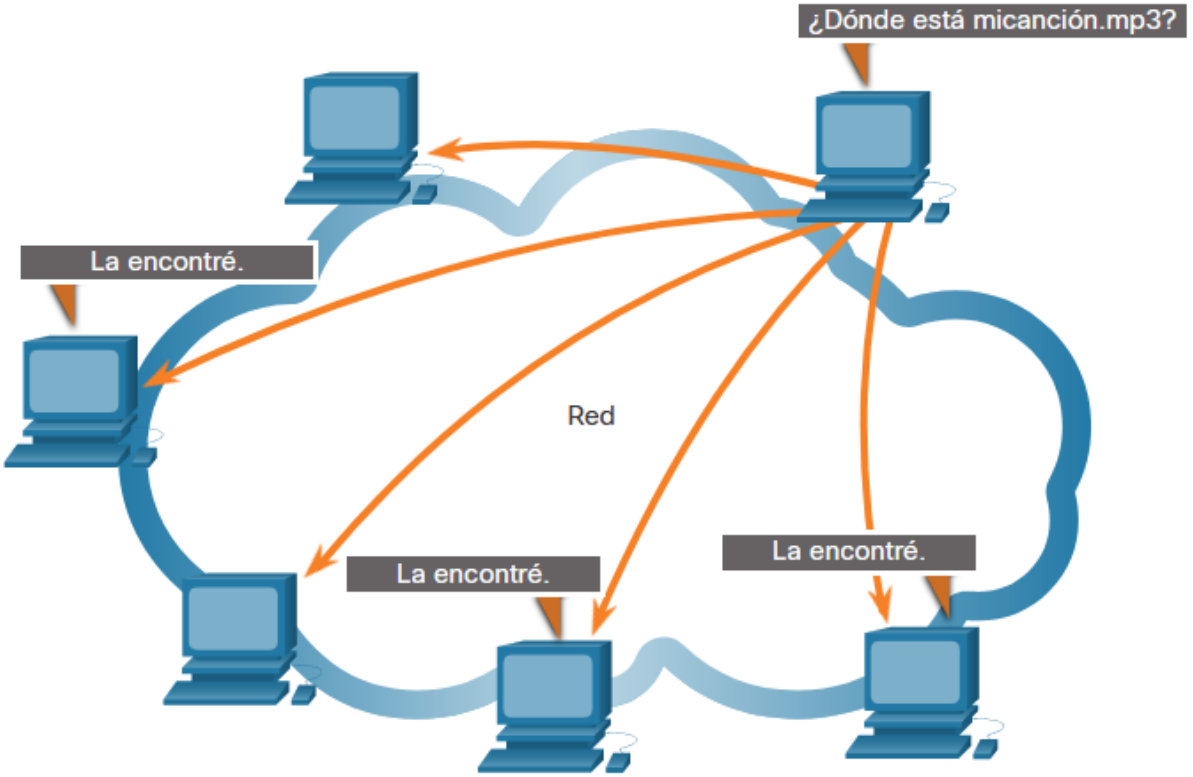


Aplicaciones P2P comunes

Con las aplicaciones P2P, cada PC de la red que ejecuta la aplicación puede funcionar como cliente o como servidor para las otras PC en la red que ejecutan la aplicación. Las redes P2P comunes incluyen las siguientes:

- BitTorrent
- Conexión directa
- eDonkey
- Freenet

Algunas aplicaciones P2P se basan en el protocolo Gnutella, con el que cada usuario comparte archivos enteros con otros usuarios. Como se muestra en la ilustración, el software de cliente compatible con Gnutella permite a los usuarios conectarse a los servicios Gnutella a través de Internet, además de ubicar los recursos compartidos por otros puntos Gnutella y acceder a dichos recursos. Muchas aplicaciones cliente de Gnutella están disponibles, incluyendo µTorrent, BitComet, DC++, Deluge y emule.



Muchas aplicaciones P2P permiten que los usuarios compartan partes de varios archivos con otro usuario a la vez. Los clientes utilizan un pequeño archivo llamado archivo torrent para localizar a otros usuarios que tienen las piezas que necesitan y conectarse directamente a ellos. Este archivo también contiene información sobre los equipos de seguimiento que realizan el seguimiento de qué usuarios tienen qué archivos. Los clientes piden partes de varios usuarios al mismo tiempo. Esta tecnología se denomina BitTorrent. BitTorrent tiene su propio cliente. pero existen muchos clientes BitTorrent, incluidos uTorrent, Deluge,y qBittorrent.

Nota: Cualquier tipo de archivo se puede compartir entre los usuarios. Muchos de estos archivos están protegidos por derechos de autor, lo que significa que sólo el creador tiene el derecho de utilizarlos y distribuirlos. Es contrario a la ley descargar o distribuir archivos protegidos por derechos de autor sin el permiso del titular de los derechos de autor. La violación de los derechos de autor puede ocasionar cargos penales y demandas civiles.

Protocolos web y de correo electrónico

Protocolo de transferencia de hipertexto y lenguaje de marcado de hipertexto

Existen protocolos específicos de la capa de aplicación diseñados para usos comunes, como la navegación web y el correo electrónico. El primer tema le dio una visión general de estos protocolos. Este tema entra en más detalle.

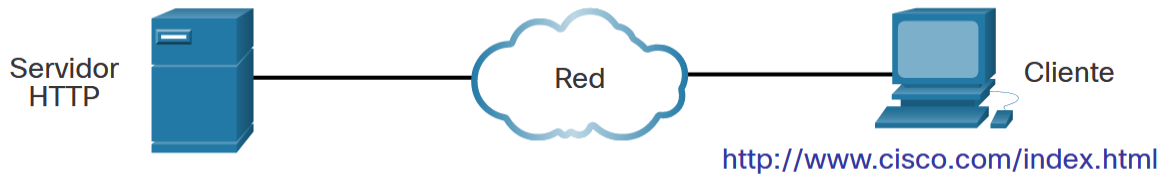
Cuando se escribe una dirección web o un localizador uniforme de recursos (URL) en un navegador web, el navegador establece una conexión con el servicio web. El servicio web se está ejecutando en el servidor que está utilizando el protocolo HTTP. Los nombres que la mayoría de las personas asocia con las direcciones web son URL e identificador uniforme de recursos (URI).

Para comprender mejor cómo interactúa el navegador web con el servidor web, podemos analizar cómo se abre una página web en un navegador.

Paso 1

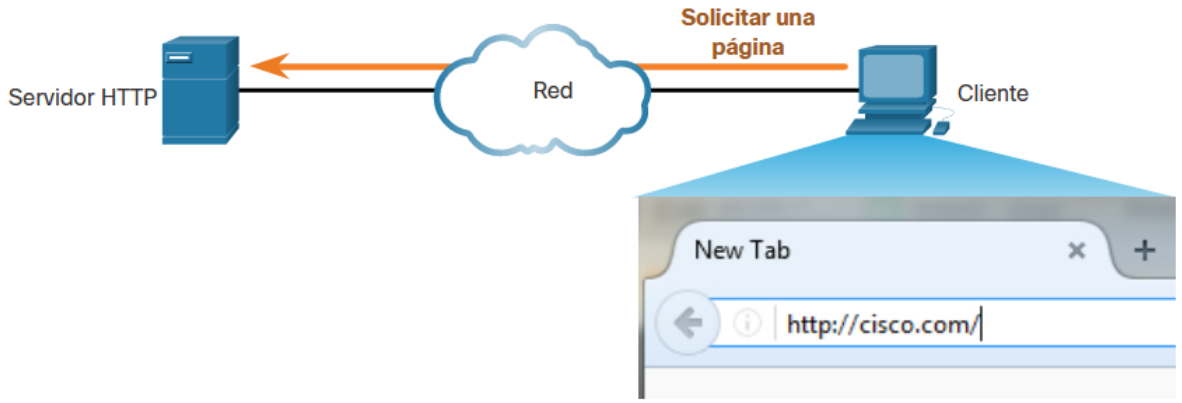
El explorador interpreta las tres partes del URL:

- http (el protocolo o esquema)
- www.cisco.com (el nombre del servidor)
- index.html (el nombre de archivo específico solicitado)



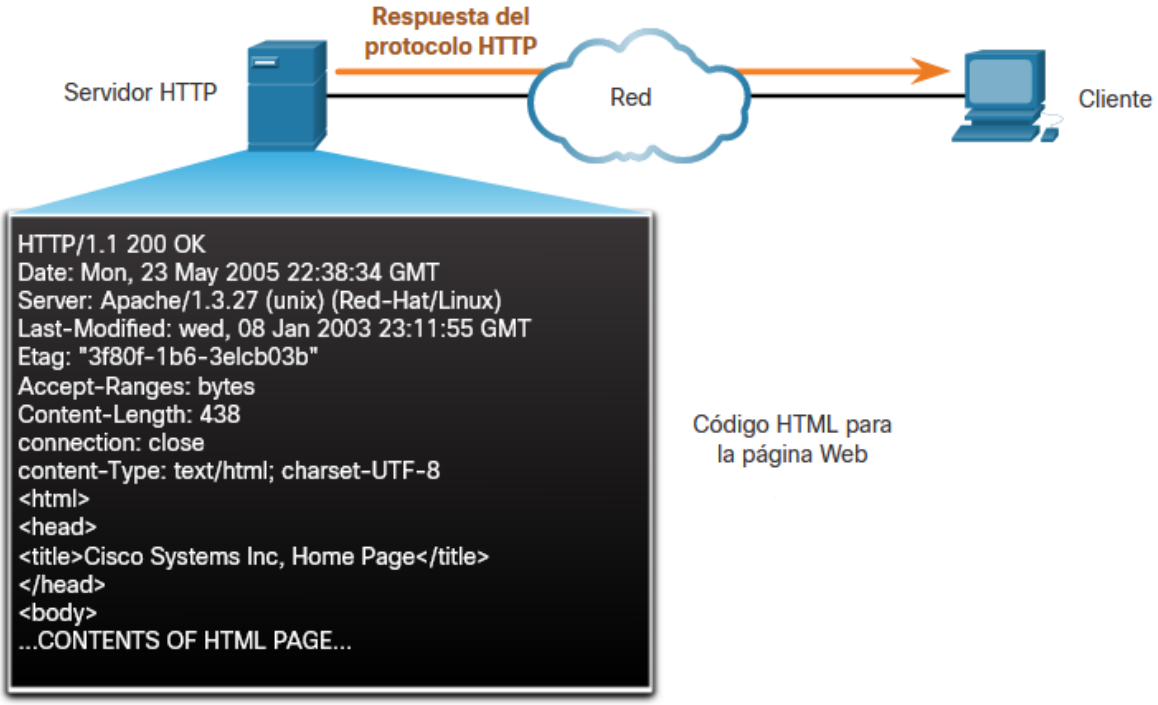
Paso 2

El navegador luego verifica con un Servidor de nombres de dominio (DNS) para convertir a www.cisco.com en una dirección numérica que utiliza para conectarse con el servidor. El cliente inicia una solicitud HTTP a un servidor enviando una solicitud GET al servidor y solicita el archivo index.html.



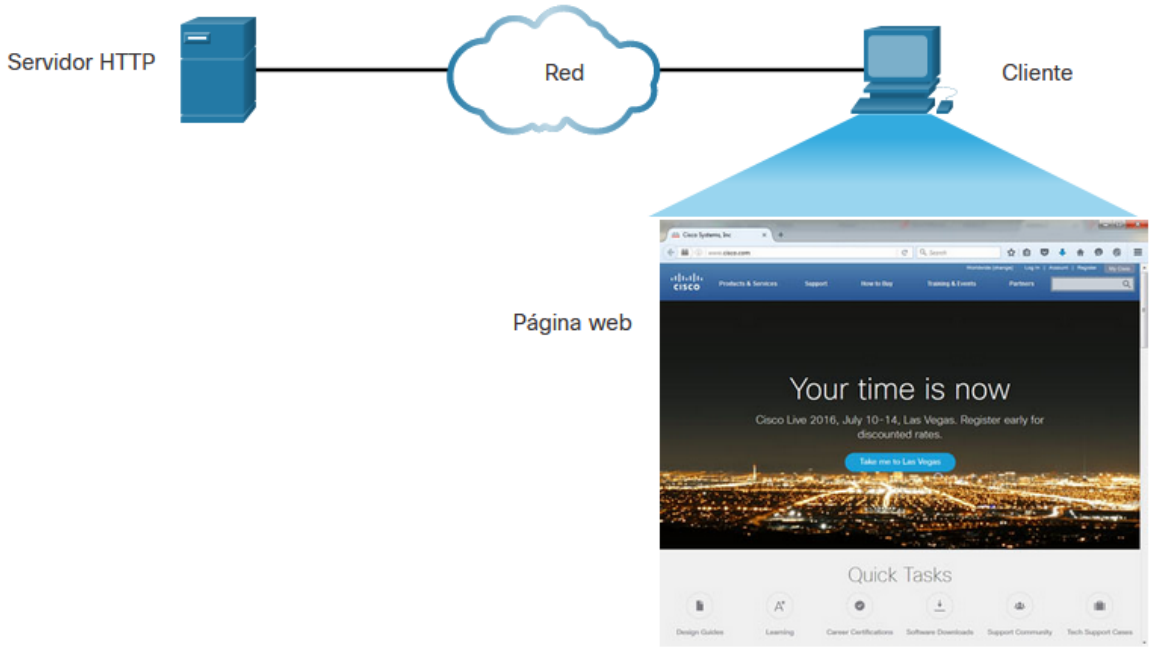
Paso 3

En respuesta a la solicitud, el servidor envía el código HTML de esta página web al navegador.



Paso 4

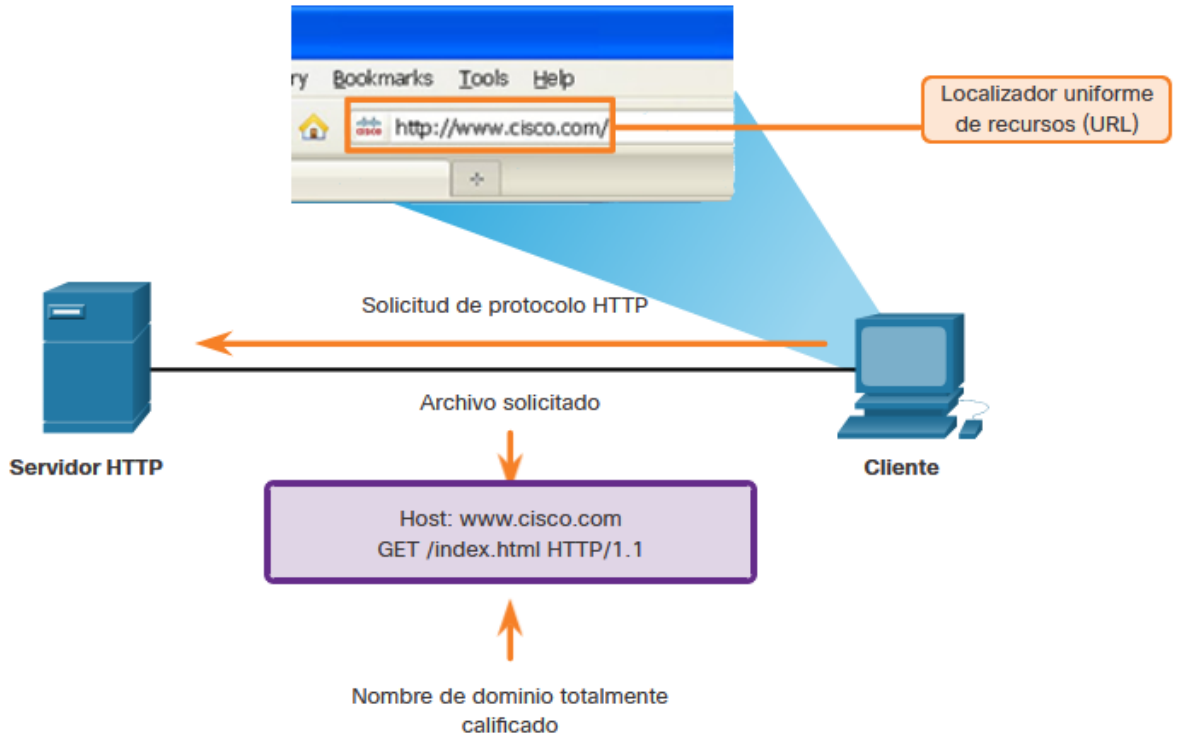
El navegador descifra el código HTML y da formato a la página para que se pueda visualizar en la ventana del navegador.



HTTP y HTTPS

HTTP es un protocolo de solicitud/respuesta. Cuando un cliente, por lo general un navegador web, envía una solicitud a un servidor web, HTTP especifica los tipos de mensaje que se utilizan para esa comunicación. Los tres tipos de mensajes comunes son GET, POST y PUT (consulte la figura):

- **GET** - solicitud de datos por parte del cliente. Un cliente (navegador web) envía el mensaje GET al servidor web para solicitar las páginas HTML.
- **POST** - carga archivos de datos, como los datos de formulario, al servidor web.
- **PUT** - carga los recursos o el contenido, como por ejemplo una imagen, en el servidor web.

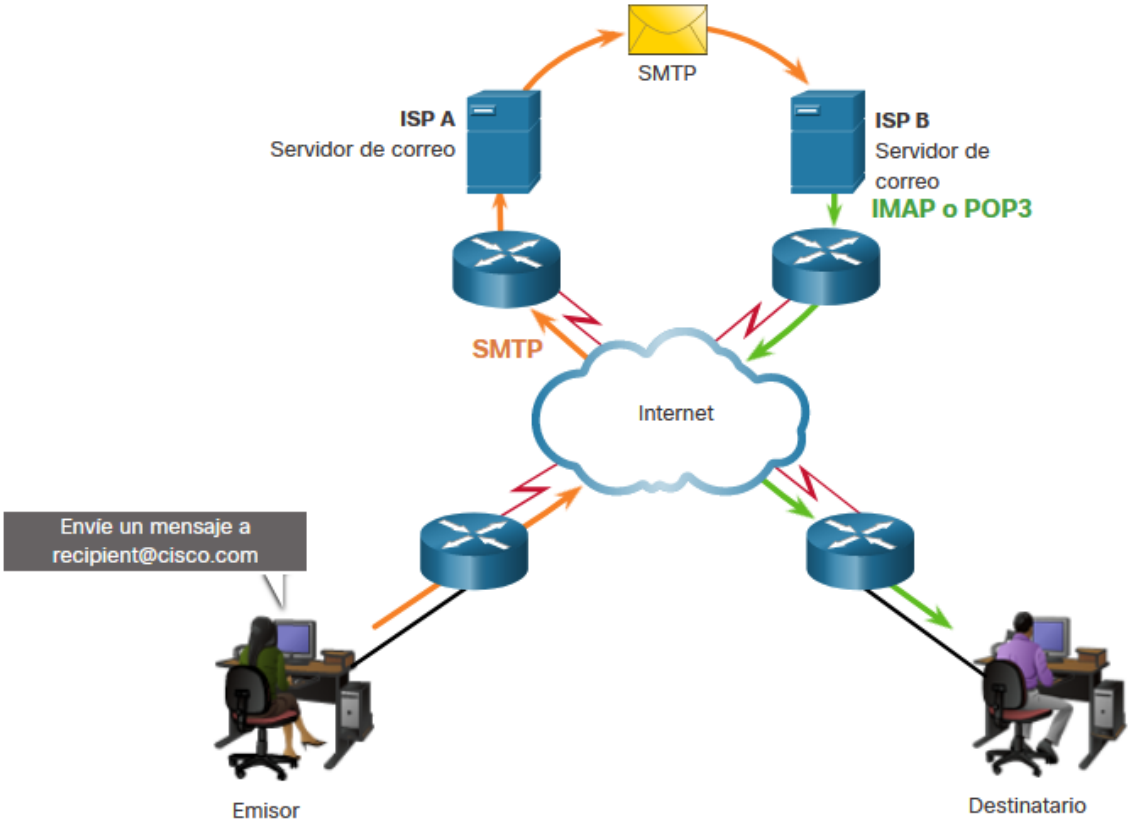


Aunque HTTP es sumamente flexible, no es un protocolo seguro. Los mensajes de solicitud envían información al servidor en texto sin formato que puede ser interceptado y leído. Las respuestas del servidor, generalmente páginas HTML, también están sin cifrar.

Para una comunicación segura a través de Internet, se utiliza el protocolo HTTP seguro (HTTPS). HTTPS utiliza autenticación y cifrado para proteger los datos mientras viajan entre el cliente y el servidor. HTTPS utiliza el mismo proceso de solicitud del cliente-respuesta del servidor que HTTP, pero el flujo de datos se cifra con capa de sockets seguros (SSL) antes de transportarse a través de la red.

Protocolos de correo electrónico

Uno de los principales servicios que un ISP ofrece es hosting de correo electrónico. Para ejecutar el correo electrónico en una PC o en otro terminal, se requieren varios servicios y aplicaciones, como se muestra en la figura. El correo electrónico es un método de guardado y desvío que se utiliza para enviar, guardar y recuperar mensajes electrónicos a través de una red. Los mensajes de correo electrónico se guardan en bases de datos en servidores de correo.



Los clientes de correo electrónico se comunican con servidores de correo para enviar y recibir correo electrónico. Los servidores de correo se comunican con otros servidores de correo para transportar mensajes desde un dominio a otro. Un cliente de correo electrónico no se comunica directamente con otro cliente de correo electrónico cuando envía un correo electrónico. En cambio, ambos clientes dependen del servidor de correo para transportar los mensajes.

El correo electrónico admite tres protocolos diferentes para su funcionamiento: el protocolo simple de transferencia de correo (SMTP), el protocolo de oficina de correos (POP) e IMAP. El proceso de capa de aplicaciones que envía correo utiliza el SMTP. Un cliente recupera el correo electrónico mediante uno de los dos protocolos de capa de aplicaciones: el POP o el IMAP.

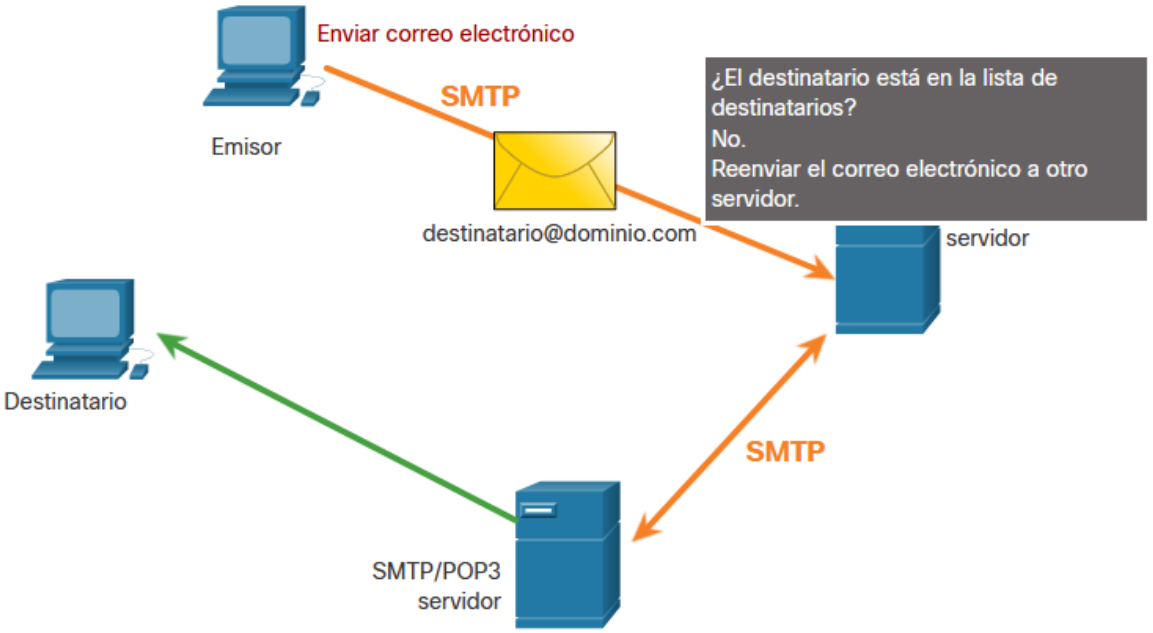
SMTP

Los formatos de mensajes SMTP necesitan un encabezado y un cuerpo de mensaje. Mientras que el cuerpo del mensaje puede contener la cantidad de texto que se desee, el encabezado debe contar con una dirección de correo electrónico de destinatario correctamente formateada y una dirección de emisor.

Cuando un cliente envía correo electrónico, el proceso SMTP del cliente se conecta a un proceso SMTP del servidor en el puerto bien conocido 25. Después de que se establece la conexión, el cliente intenta enviar el correo electrónico al servidor a

través de esta. Una vez que el servidor recibe el mensaje, lo ubica en una cuenta local (si el destinatario es local) o lo reenvía a otro servidor de correo para su entrega.

El servidor de correo electrónico de destino puede no estar en línea, o estar muy ocupado, cuando se envían los mensajes. Por lo tanto, el SMTP pone los mensajes en cola para enviarlos posteriormente. El servidor verifica periódicamente la cola en busca de mensajes e intenta enviarlos nuevamente. Si el mensaje aún no se ha entregado después de un tiempo predeterminado de expiración, se devolverá al emisor como imposible de entregar.



POP

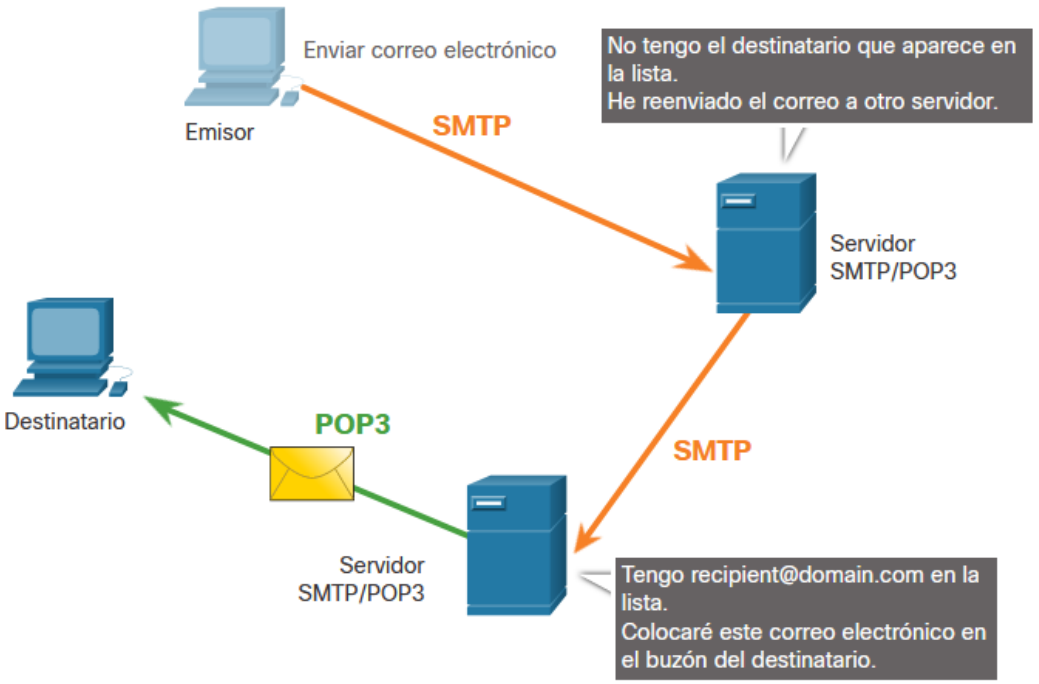
POP es utilizado por una aplicación para recuperar correo electrónico de un servidor de correo. Con POP, el correo se descarga desde el servidor al cliente y después se elimina en el servidor. Esta es la operación predeterminada de POP.

El servidor comienza el servicio POP escuchando de manera pasiva en el puerto TCP 110 las solicitudes de conexión del cliente. Cuando un cliente desea utilizar el servicio, envía una solicitud para establecer una conexión TCP con el servidor, como se muestra en la figura. Una vez establecida la conexión, el servidor POP envía un saludo. A continuación, el cliente y el servidor POP intercambian comandos y respuestas hasta que la conexión se cierra o cancela.

Con POP, los mensajes de correo electrónico se descargan en el cliente y se eliminan del servidor, esto significa que no existe una ubicación centralizada donde

se conserven los mensajes de correo electrónico. Como POP no almacena mensajes, no es una opción adecuada para una pequeña empresa que necesita una solución de respaldo centralizada.

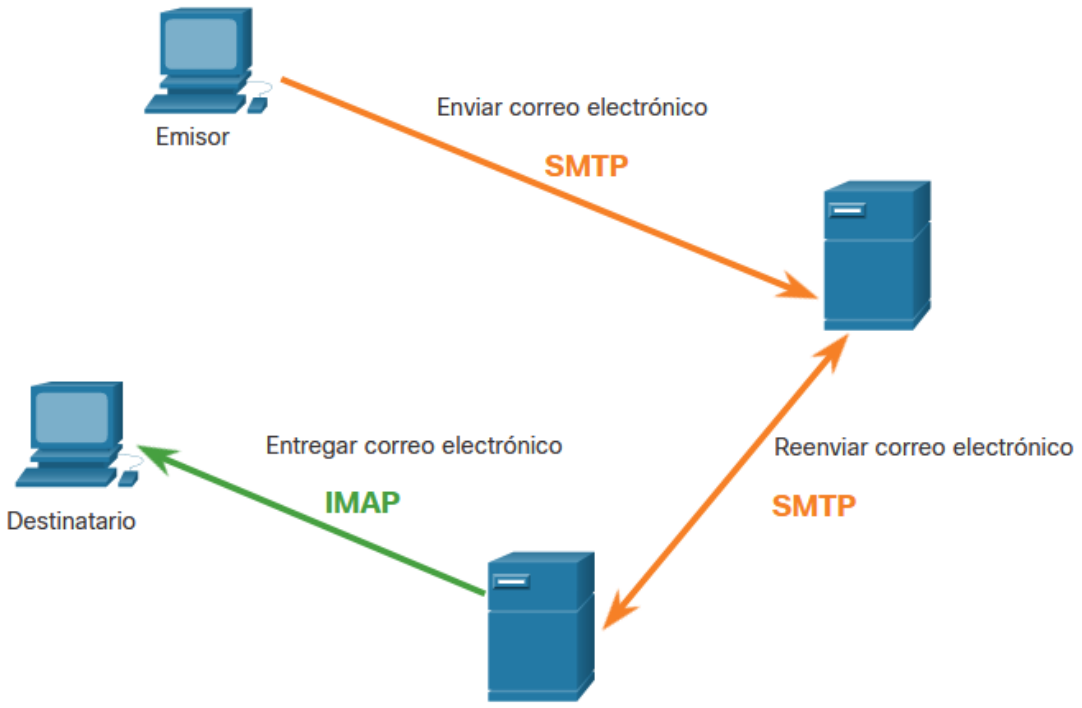
POP3 es la versión más utilizada.



IMAP

IMAP es otro protocolo que describe un método para recuperar mensajes de correo electrónico. A diferencia de POP, cuando el usuario se conecta a un servidor con capacidad IMAP, se descargan copias de los mensajes a la aplicación cliente, como se muestra en la figura. Los mensajes originales se mantienen en el servidor hasta que se eliminen manualmente. Los usuarios ven copias de los mensajes en su software de cliente de correo electrónico.

Los usuarios pueden crear una jerarquía de archivos en el servidor para organizar y guardar el correo. Dicha estructura de archivos se duplica también en el cliente de correo electrónico. Cuando un usuario decide eliminar un mensaje, el servidor sincroniza esa acción y elimina el mensaje del servidor.



Servicios de direccionamiento IP

Servicio de nombres de dominios

Existen otros protocolos específicos de capa de aplicación diseñados para facilitar la obtención de direcciones para dispositivos de red. Estos servicios son esenciales porque llevaría mucho tiempo recordar direcciones IP en lugar de direcciones URL o configurar manualmente todos los dispositivos de una red mediana a grande. El primer tema de este módulo le dio una visión general de estos protocolos. En este tema se detallan los servicios de direccionamiento IP, DNS y DHCP.

En las redes de datos, los dispositivos se etiquetan con direcciones IP numéricas para enviar y recibir datos a través de las redes. Los nombres de dominio se crearon para convertir las direcciones numéricas en un nombre sencillo y reconocible.

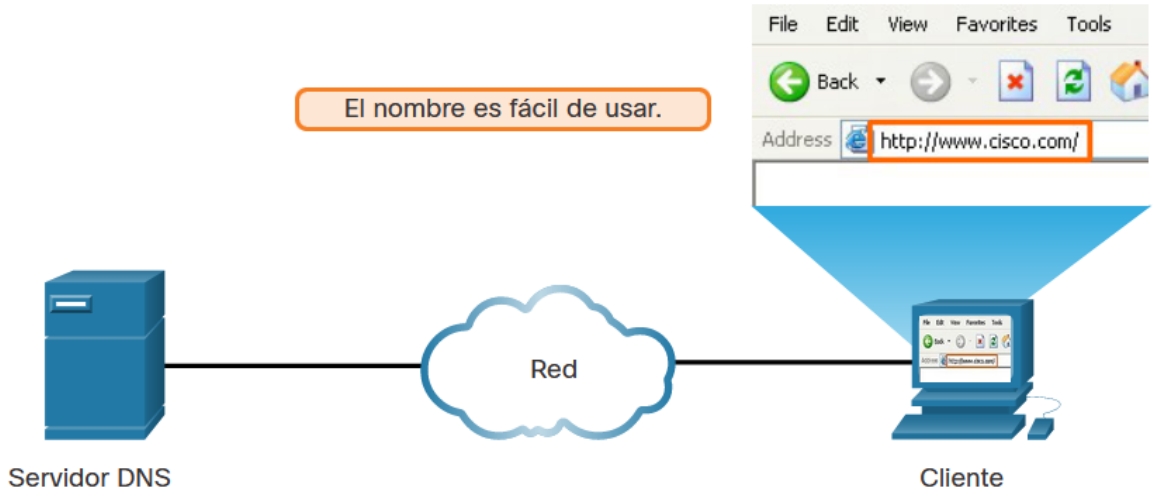
En Internet, los nombres de dominio, como http://www.cisco.com, son mucho más fáciles de recordar para las personas que 198.133.219.25, que es la dirección IP numérica real para este servidor. Si Cisco decide cambiar la dirección numérica de www.cisco.com, esto no afecta al usuario, porque el nombre de dominio se mantiene. Simplemente se une la nueva dirección al nombre de dominio existente y se mantiene la conectividad.

El protocolo DNS define un servicio automatizado que coincide con nombres de recursos que tienen la dirección de red numérica solicitada. Incluye el formato de

consultas, respuestas y datos. Las comunicaciones del protocolo DNS utilizan un único formato 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.

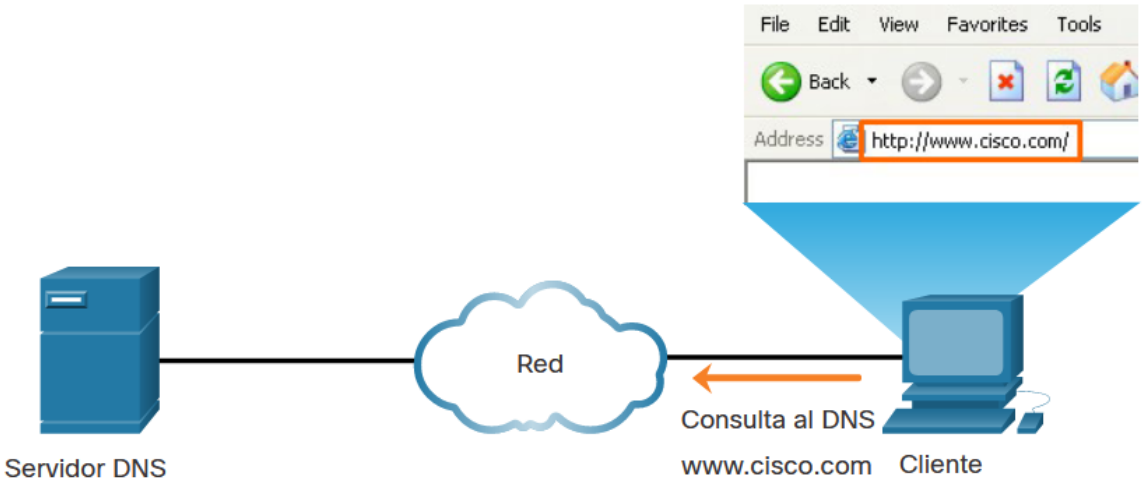
Paso 1

El usuario escribe un FQDN en un campo Dirección de aplicación del explorador.



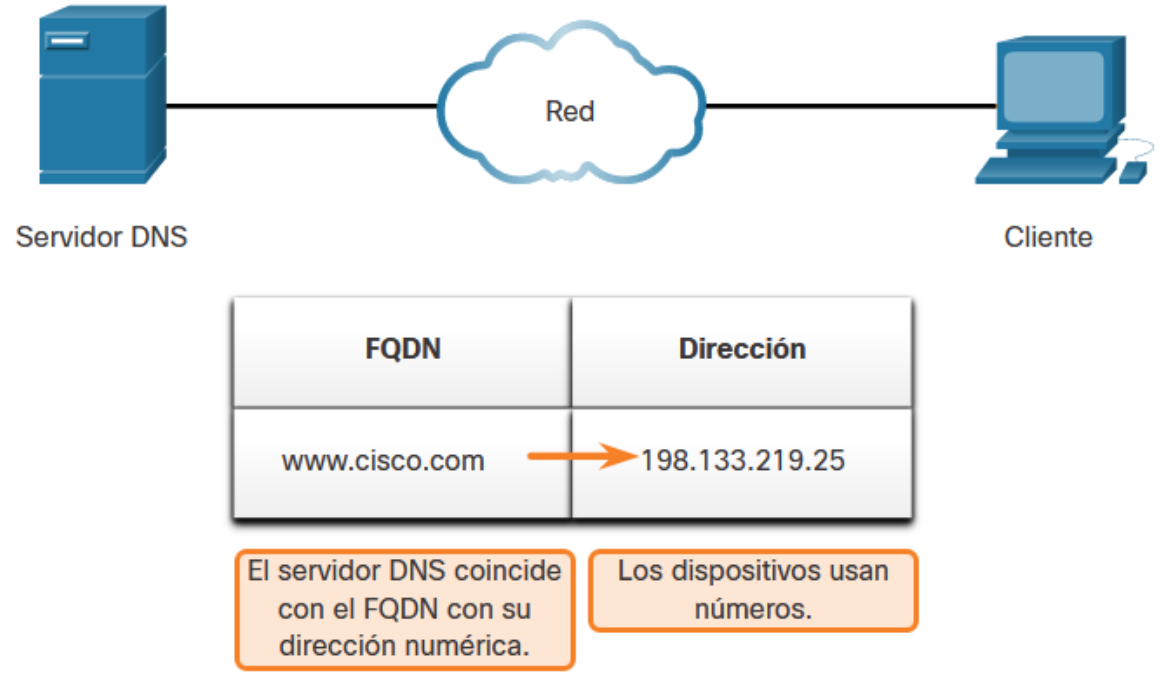
Paso 2

Se envía una consulta DNS al servidor DNS designado para el equipo cliente.



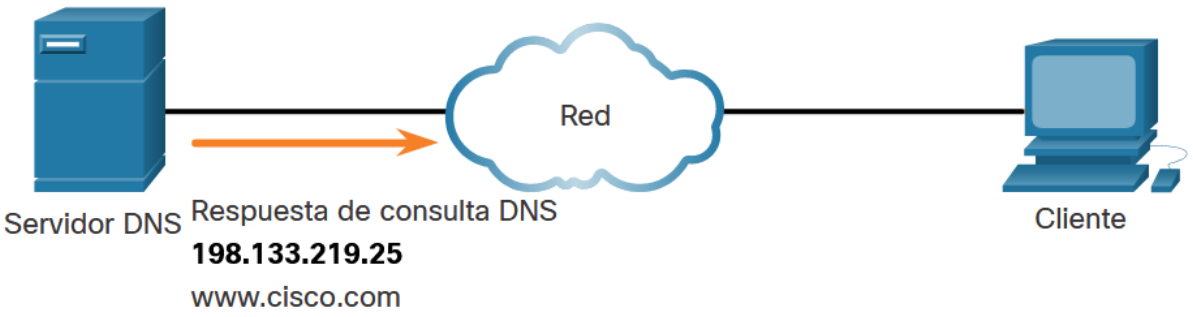
Paso 3

El servidor DNS coincide con el FQDN con su dirección IP.



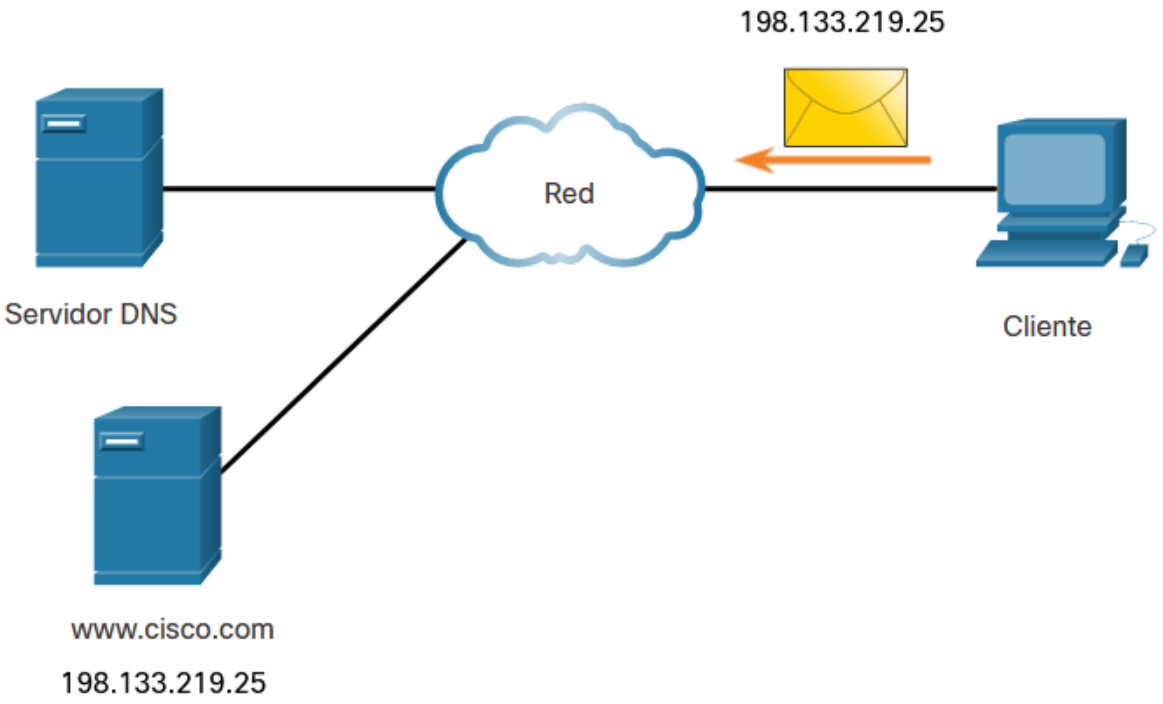
Paso 4

La respuesta de consulta DNS se envía de nuevo al cliente con la dirección IP del FQDN.



Paso 5

El equipo cliente utiliza la dirección IP para realizar solicitudes del servidor.



Formato de mensaje DNS

El servidor DNS almacena diferentes tipos de registros de recursos utilizados para resolver nombres. Estos registros contienen el nombre, la dirección y el tipo de registro. Algunos de estos tipos de registros son los siguientes:

- **A** - una dirección IPv4 de terminal
- **NS** - un servidor de nombre autoritativo
- **AAAA** - una dirección IPv6 de terminal (pronunciada quad-A)
- **MX** - un registro de intercambio de correo

Cuando un cliente realiza una consulta, el proceso DNS del servidor observa primero sus propios registros para resolver el nombre. Si no puede resolverlo con los registros almacenados, contacta a otros servidores para hacerlo. Una vez que se encuentra una coincidencia y se la devuelve al servidor solicitante original, este almacena temporalmente la dirección numerada por si se vuelve a solicitar el mismo nombre.

El servicio del cliente DNS en los equipos Windows también almacena los nombres resueltos previamente en la memoria. El comando **ipconfig /displaydns** muestra todas las entradas de DNS en caché.

Este formato de mensaje que se ve en la figura se utiliza para todos los tipos de solicitudes de clientes y respuestas del servidor, para los mensajes de error y para la transferencia de información de registro de recursos entre servidores.

Sección de mensajes DNS	Descripción
Pregunta	La pregunta para el servidor de nombres
Respuesta	Registros de recursos que responden la pregunta
Autoridad	Registros de recursos que apuntan a una autoridad
Adicional	Registros de recursos que poseen información adicional

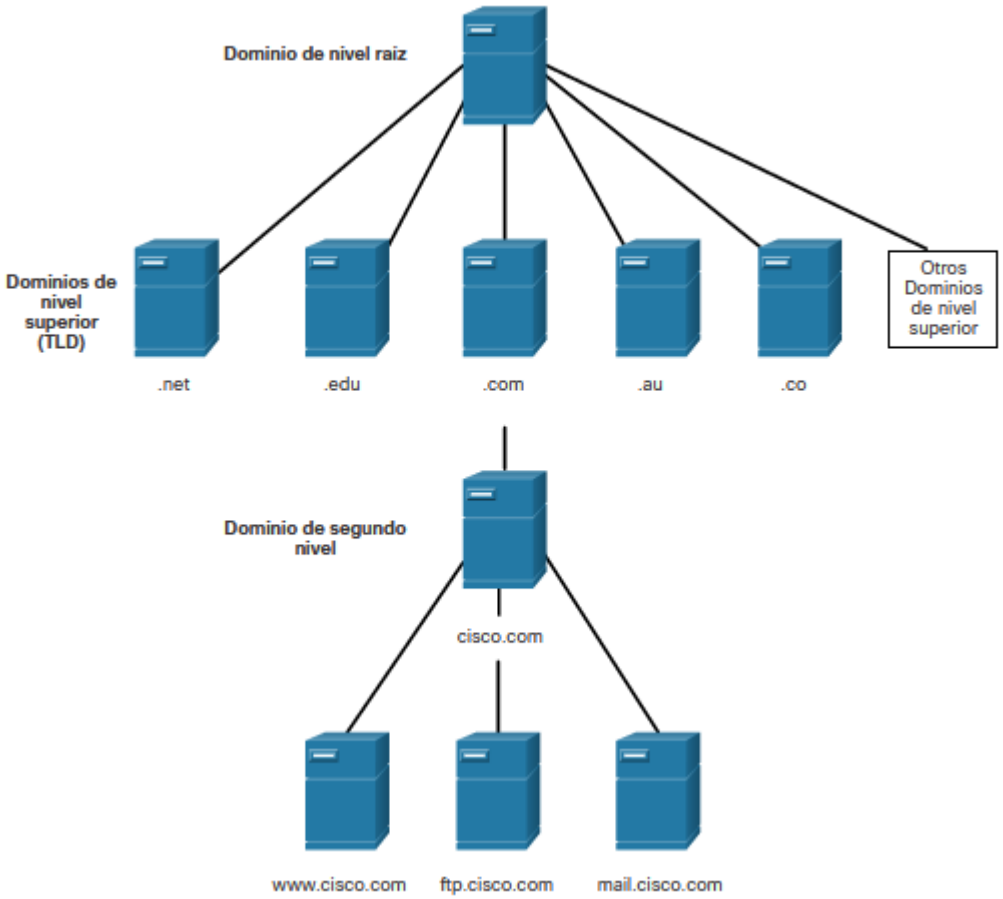
Jerarquía DNS

El protocolo DNS utiliza un sistema jerárquico para crear una base de datos que proporcione la resolución de nombres, como se muestra en la figura. DNS utiliza nombres de domino para formar la jerarquía.

La estructura de nomenclatura se divide en zonas pequeñas y manejables. Cada servidor DNS mantiene un archivo de base de datos específico y sólo es responsable de administrar las asignaciones de nombre a IP para esa pequeña porción de toda la estructura DNS. Cuando un servidor DNS recibe una solicitud para una traducción de nombre que no se encuentra dentro de esa zona DNS, el servidor DNS reenvía la solicitud a otro servidor DNS dentro de la zona adecuada para su traducción. DNS es escalable, porque la resolución de los nombres de hosts se distribuye entre varios servidores.

Los diferentes dominios de primer nivel representan el tipo de organización o el país de origen. Algunos ejemplos de dominios de nivel superior son los siguientes:

- **.com** - una empresa o industria
- **.org** - una organización sin fines de lucro
- **.au** - Australia
- **.co** - Colombia



El comando nslookup

Al configurar un dispositivo de red, se proporcionan una o más direcciones de servidor DNS que el cliente DNS puede utilizar para la resolución de nombres. En general, el proveedor de servicios de Internet (ISP) suministra 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 al servidor de nombres para resolver el nombre para una dirección numérica.

Los sistemas operativos informáticos 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 esta figura **nslookup** cuando se ejecuta el comando, se muestra el servidor DNS predeterminado configurado para su host. El nombre de un host o de un dominio se puede introducir en el **nslookup** prompt. La utilidad nslookup tiene muchas

opciones disponibles para realizar una prueba y una verificación exhaustivas del proceso DNS.

```
C:\Users> nslookup
Default Server:  dns-sj.cisco.com
Address:  171.70.168.183
> www.cisco.com
Server:  dns-sj.cisco.com
Address:  171.70.168.183
Name:    origin-www.cisco.com
Addresses:  2001:420:1101:1::a
          173.37.145.84
Aliases:  www.cisco.com
> cisco.netacad.net
Server:  dns-sj.cisco.com
Address:  171.70.168.183
Name:    cisco.netacad.net
Address:  72.163.6.223
>
```