Modulo 15: capa de aplicacion

15.0 Introducción

Desplázate para empezar

15.0.1 ¿Por qué debería tomar este módulo?

Bienvenido a la Capa de aplicación

Como ha aprendido, la capa de transporte es donde los datos se mueven realmente de un host a otro. Pero antes de que eso pueda tener lugar, hay muchos detalles que deben determinarse para que este transporte de datos ocurra correctamente. Esta es la razón por la que hay una capa de aplicación tanto en los modelos OSI como en los modelos TCP/IP. Como ejemplo, antes de que hubiera streaming de vídeo a través de Internet, teníamos que ver películas caseras de una variedad de otras maneras. Imagina que grabaste algún partido de fútbol de tu hijo. Tus padres, en otra ciudad, sólo tienen un videograbador. Tienes que copiar el vídeo de tu cámara en el tipo correcto de casete para enviarlos. Tu hermano tiene un reproductor de DVD, por lo que transfieres tu video a un DVD para enviarlo. De esto se trata la capa de aplicación, asegurándose de que los datos estén en un formato que el dispositivo receptor pueda usar. ¡Vamos a bucear!

15.0.2 ¿Qué aprenderé en este módulo?

Título del módulo: Capa de aplicación

Objetivos del módulo: Explique el funcionamiento de los protocolos de la capa de aplicación en cuanto a dar soporte a las aplicaciones de usuario final.

15.1 Aplicación, presentación y sesión

Desplázate para empezar

15.1.1 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.

La figura es una comparación de las capas de modelo OSI y TCP/IP. El modelo OSI se muestra a la izquierda. De arriba a abajo se encuentran los siguientes números de capa y nombres: 7) Aplicación, 6) Presentación, 5) Sesión, 4) Transporte, 3) Red, 2) Enlace de datos y 1) Física. El modelo TCP/IP se muestra a la derecha. De arriba a abajo, los nombres de capa y los números de capa del modelo OSI asociados son: Aplicación (Capas OSI 7, 6 y 5), Transporte (Capa OSI 4), Internet (Capa OSI 3) y Acceso de red (Capas OSI 2 y 1). El texto al pie de la figura dice que Las similitudes clave se encuentran en la capa de transporte y en la capa de red. Sin embargo, los dos modelos se diferencian en el modo en el que se relacionan con las capas que están por encima y por debajo de cada capa. Esta capa se utiliza para describir protocolos que abordan y dirigen mensajes a través de una internetwork. La capa OSI 4, la capa de transporte, asigna directamente a la capa de transporte TCP/IP. Esta capa describe los servicios y las funciones generales que proporcionan la entrega ordenada y confiable de datos entre los hosts de origen y de destino. La capa de aplicación TCP/IP incluye un número de protocolos que proporciona funcionalidad específica a una variedad de aplicaciones de usuario final. Las capas 5, 6 y 7 del modelo OSI se utilizan como referencias para proveedores y desarrolladores de software de aplicación para fabricar productos que funcionan en redes. Tanto el modelo TCP/IP como el modelo OSI se utilizan comúnmente en la referencia a protocolos en varias capas. Dado que el modelo OSI separa la capa de enlace de datos de la capa física, se suele utilizan cuando se refiere a esas capas inferiores. Entre las aplicaciones de ejemplo de la capas de aplicación del modelo OSI se incluyen el sistema de nombres de dominio, el protocolo de transferencia de hipertexto, el protocolo simple de transferencia de correo, el protocolo de oficina de correos, el protocolo de configuración dinámica de host, el protocolo de transferencia de archivo y el protocolo de acceso a mensajes de Internet.

Modelo OSI
7. Aplicación
6. Presentación
5. Sesión
4. Transporte
3. Red
2. Enlace de datos
1. Física
Modelo TCP/IP
Aplicación
Transporte
Internet
Acceso
a la red
Capas de
aplicación
Capas de
flujo de datos

Sistema de nombres de dominio

Protocolo de transferencia de hipertexto

Protocolo simple de transferencia de correo

Protocolo de oficina de correo

Protocolo de configuración dinámica de host

Protocolo de transferencia de archivos

Protocolo de acceso a mensajes de Internet

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).

15.1.2 Capa de presentación y sesión

Presentation Layer

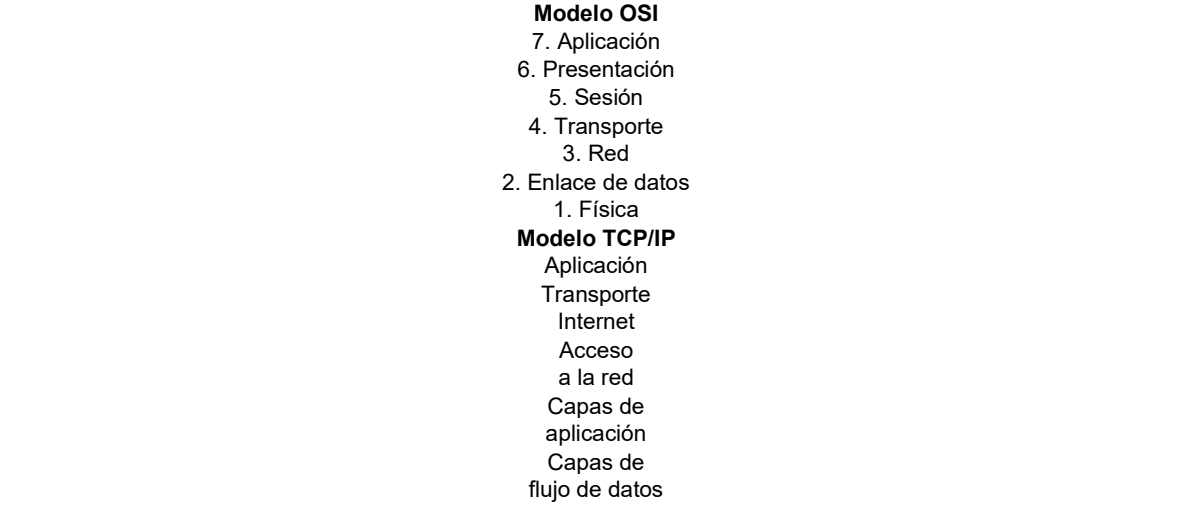
La capa de presentación tiene tres funciones principales:

- 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).

La figura es una comparación de las capas de modelo OSI y TCP/IP. El modelo OSI se muestra a la izquierda. De arriba a abajo se encuentran los siguientes números de capa y nombres: 7) Aplicación, 6) Presentación, 5) Sesión, 4) Transporte, 3) Red, 2) Enlace de datos y 1) Física. El modelo TCP/IP se muestra a la derecha. De arriba a abajo, los nombres

de capa y los números de capa del modelo OSI asociados son: Aplicación (Capas OSI 7, 6 y 5), Transporte (Capa OSI 4), Internet (Capa OSI 3) y Acceso de red (Capas OSI 2 y 1). El texto al pie de la figura dice que Las similitudes clave se encuentran en la capa de transporte y en la capa de red. Sin embargo, los dos modelos se diferencian en el modo en el que se relacionan con las capas que están por encima y por debajo de cada capa. Esta capa se utiliza para describir protocolos que abordan y dirigen mensajes a través de una internetwork. La capa OSI 4, la capa de transporte, asigna directamente a la capa de transporte TCP/IP. Esta capa describe los servicios y las funciones generales que proporcionan la entrega ordenada y confiable de datos entre los hosts de origen y de destino. La capa de aplicación TCP/IP incluye un número de protocolos que proporciona funcionalidad específica a una variedad de aplicaciones de usuario final. Las capas 5, 6 y 7 del modelo OSI se utilizan como referencias para proveedores y desarrolladores de software de aplicación para fabricar productos que funcionan en redes. Tanto el modelo TCP/IP como el modelo OSI se utilizan comúnmente en la referencia a protocolos en varias capas. Dado que el modelo OSI separa la capa de enlace de datos de la capa física, se suele utilizan cuando se refiere a esas capas inferiores. Entre los ejemplos para la capa de presentación del modelo OSI, se incluyen Quick Time, Motion Picture Experts Group (MPEG), formato de intercambio de gráficos (GIF), Joint Photographic Experts Group (JPEG) y gráficos de red portátiles (PNG).



QuickTime

Motion Picture Experts Group (MPEG)

Formato de intercambio de gráficos (GIF)

Joint Photographic Experts Group (JPEG)

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.

15.1.3 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.

Haga clic en cada protocolo de aplicación para aprender más sobre cada protocolo.
Sistema de nombres
Configuración de host
Correo electrónico
Transferencia de archivos
La web

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

15.2 Punto a punto

Desplázate para empezar

15.2.1 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.

La figura representa el modelo de servidor cliente. Un cliente que se representa como un teléfono celular, computadora o teléfono VoIP está conectado a un servidor y descarga archivos desde el servidor.

Descargar
Red
Cliente
Servidor

15.2.2 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.

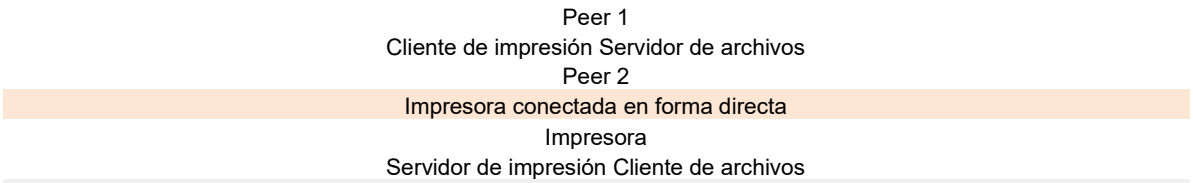
En una red P2P, hay dos o más PC que están conectadas por medio de una red y pueden compartir recursos (como impresoras y archivos) sin tener un servidor dedicado. Todo terminal conectado puede funcionar como servidor y como cliente. Un equipo puede asumir la función de servidor para una transacción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

La figura representa el modelo de par a par. Dos computadoras están conectadas por un conmutador y se comunican directamente entre sí. Además, una impresora es compartida por uno de los equipos y puede ser accedida por cualquiera de los equipos de la figura.

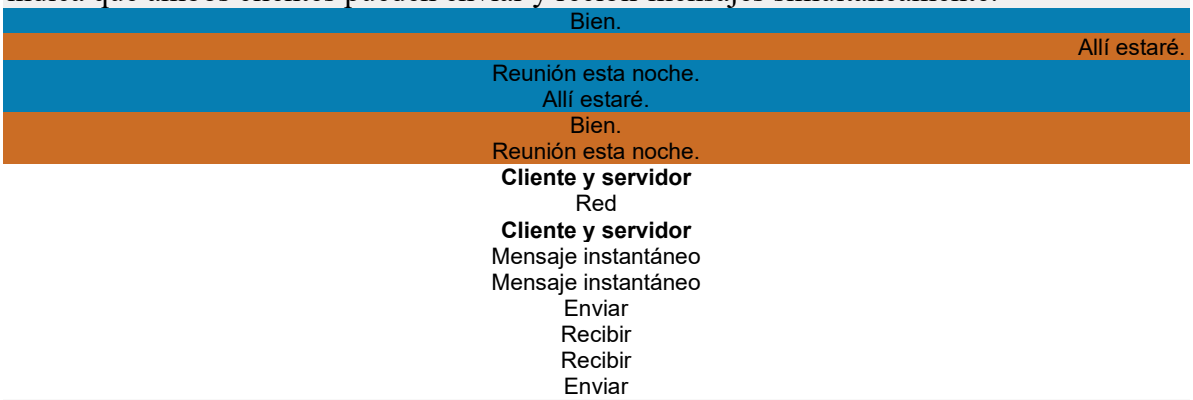


15.2.3 Peer-to-Peer Applications

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.

La figura muestra una conversación de mensajería instantánea con dos máquinas que se comunican entre sí a través de la red. Cada máquina actúa como cliente y servidor. El título indica que ambos clientes pueden enviar y recibir mensajes simultáneamente.



Ambos clientes pueden enviar y recibir mensajes simultáneamente.

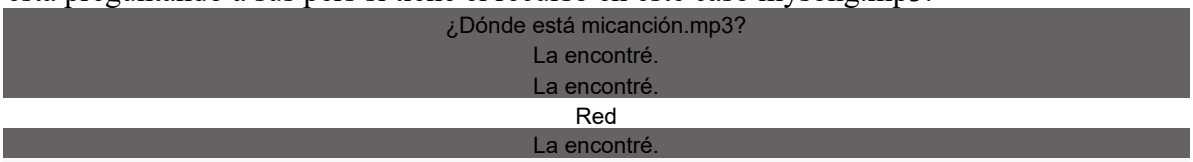
15.2.4 Aplicaciones P2P comunes

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.

La figura muestra una aplicación P2P que busca recursos compartidos. La P2Papplication está preguntando a sus pers si tiene el recurso en este caso mysong.mp3.



Gnutella permite que las aplicaciones P2P busquen recursos compartidos entre puntos.

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.

15.3 Protocolos web y de correo electrónico

Desplázate para empezar

15.3.1 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. Para este ejemplo, utilice el URL http://www.cisco.com/index.html.

Haga clic en cada botón para obtener más información.
Paso 1
Paso 2
Paso 3
Paso 4

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)

muestra un servidor http conectado a través de Internet a un equipo cliente. El equipo cliente está solicitando la URL www.cisco.com que es el servidor HTTP.

Servidor HTTP
Red
Cliente
http://www.cisco.com/index.html

15.3.2 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.

La figura muestra a un cliente que realiza una solicitud HTTP a un servidor HTTP. El archivo solicitado es un nombre de dominio completo. La solicitud utiliza un Get para recuperar la página web. El campo URL se muestra en el equipo cliente como una solicitud http://www.cisco.com.

Servidor HTTP

Cliente

Localizador uniforme de recursos (URL)

Solicitud de protocolo HTTP

Archivo solicitado

Host: www.cisco.com

GET /index.html HTTP/1.1

Nombre de dominio totalmente calificado

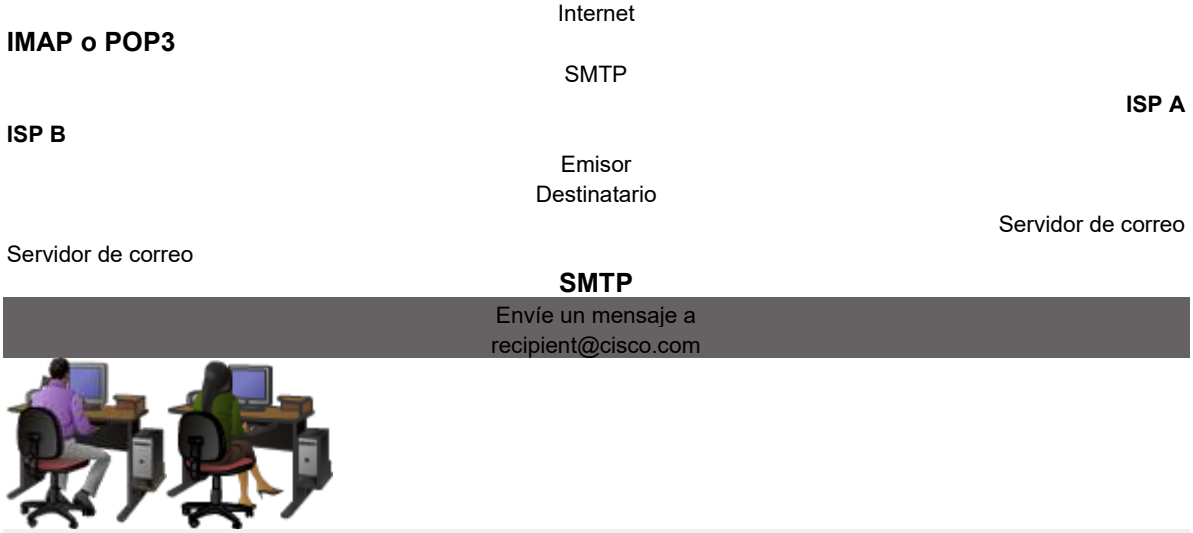
Aunque HTTP es sumamente flexible, no es un protocolo seguro. Los mensajes de solicitud envían información al servidor en texto sin formato que puede ser interceptado y leído. Las respuestas del servidor, generalmente páginas HTML, también están sin cifrar.

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.

15.3.3 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.

La figura muestra una transacción de correo electrónico de un remitente que usa el protocolo SMTP y envía un correo electrónico a destinatario@cisco.com a través de un servidor de correo A de I S P que llega al servidor de correo B de I S P de los destinatarios y el destinatario lee el correo electrónico usando un protocolo I MAP o POP .



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.

15.3.4 SMTP, POP e IMAP

Haga clic en cada botón para obtener más información.
SMTP
POP
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.

Esta es una figura con un equipo remitente y un equipo destinatario. Dos servidores SMTP/POP3 están conectados entre ambos. Se envía un mensaje de correo desde el equipo remitente con la etiqueta recipient@domain.com mediante el protocolo smtp. El primer SMTP/POP3 recibe el mensaje del remitente y pregunta ¿Está el destinatario en mi lista de destinatarios? No. Reenviar correo electrónico a otro servidor. El segundo servidor SMTP/POP3 recibe el mensaje a través del protocolo SMTP y reenvía el mensaje al destinatario.

15.4 Servicios de direccionamiento IP

Desplázate para empezar

15.4.1 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.

Haga clic en cada botón para obtener más información.
Paso 1
Paso 2
Paso 3
Paso 4
Paso 5

Paso 1

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

esta es una figura con un cliente que se pone en contacto con un servidor DNS a través de la red con un FQDN escrito en un campo URL del navegador porque el nombre de un sitio web es más fácil para las personas usar

El nombre es fácil de usar.
Servidor DNS
Red
Cliente

15.4.2 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.

15.4.3 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

En la figura, se muestra la jerarquía DNS. En la parte superior está el dominio de nivel raíz con los dominios de nivel superior (TLD) conectados debajo del dominio de nivel raíz. Los TLD son .net, .edu, .com, .au, .co y otros doamins de nivel superior. Bajo el TLD .com está el dominio de segundo nivel www.cisco.com y bajo cisco.com son www.cisco.com, ftp.cisco.com y mail.cisco.com.

Dominio de nivel raíz
Dominios de nivel superior (TLD)
Dominio de segundo nivel
cisco.com
www.cisco.com
ftp.cisco.com
mail.cisco.com
.net
.edu

.com
.au
.co
Otros
Dominios de nivel
superior

15.4.4 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
>
```

15.4.5 Comprobador de## sintaxis - El comando nslookup

Practique la introducción del comando nslookup tanto en Windows como en Linux.

En el símbolo del sistema de Windows, introduzca el**nslookup** comando para iniciar una consulta manual de los servidores de nombres.

```
C:\>
```

MostrarMostrar todoRestablecer

15.4.6 Protocolo de configuración dinámica de host

El protocolo DHCP del servicio IPv4 automatiza la asignación de direcciones IPv4, máscaras de subred, gateways y otros parámetros de redes IPv4. Esto se denomina “direccionamiento dinámico”. La alternativa al direccionamiento dinámico es el direccionamiento estático. Al utilizar el direccionamiento estático, el administrador de redes introduce manualmente la información de la dirección IP en los hosts.

Cuando un host se conecta a la red, se realiza el contacto con el servidor de DHCP y se solicita una dirección. El servidor de DHCP elige una dirección de un rango de direcciones configurado llamado grupo y la asigna (concede) al host.

En redes más grandes, o donde los usuarios cambian con frecuencia, se prefiere asignar direcciones con DHCP. Es posible que los nuevos usuarios necesiten conexiones; otros pueden tener PC nuevas que deben estar conectadas. En lugar de usar asignación de direcciones estáticas para cada conexión, es más eficaz que las direcciones IPv4 se asignen automáticamente mediante DHCP.

DHCP puede asignar direcciones IP durante un período de tiempo configurable, denominado período de concesión. El período de concesión es una configuración DHCP importante. Cuando caduca el período de concesión o el servidor DHCP recibe un mensaje DHCPRELASE, la dirección se devuelve al grupo DHCP para su reutilización. Los usuarios pueden moverse libremente desde una ubicación a otra y volver a establecer con facilidad las conexiones de red por medio de DHCP.

Como lo muestra la figura, varios tipos de dispositivos pueden ser servidores DHCP. En la mayoría de las redes medianas a grandes, el servidor DHCP suele ser un servidor local y dedicado con base en una PC. En las redes domésticas, el servidor de DHCP suele estar ubicado en el router local que conecta la red doméstica al ISP.

En la figura se muestra un servidor DHCP ISP conectado a Internet con tres routers ISP con la etiqueta ISP1, ISP2, ISP #. Cada router ISP está conectado a una red diferente. ISP1 se conecta a una antena inalámbrica a un trabajador móvil que es el cliente DCHP. ISP2 está conectado a un router de red coporate que se conecta a una LAN coporate con su propio servidor DHCP local conectado a un switch conectado a seis clientes DHCP. ISP3 está conectado a un servidor DHCP inalámbrico para una red doméstica y pequeña empresa a los tres clientes DHCP conectados.

Internet
ISP 2
ISP 1
ISP 3
Servidor de DHCP del ISP
Servidor de DHCP del router
Trabajador móvil
Red doméstica y red empresarial pequeña
Cliente DHCP
Red corporativa
Clientes DHCP
Clientes DHCP
Servidor de DHCP local
Servidor DHCP

Muchas redes utilizan tanto el direccionamiento estático como DHCP. DHCP se utiliza para hosts de propósito general, tales como los dispositivos de usuario final. El direccionamiento estático se utiliza para los dispositivos de red, tales como gateways, switches, servidores e impresoras.

DHCPv6 (DHCP para IPv6) proporciona servicios similares para los clientes IPv6. Una diferencia importante es que DHCPv6 no brinda una dirección de gateway predeterminado. Esto sólo se puede obtener de forma dinámica a partir del anuncio de router del propio router.

15.4.7 Funcionamiento de DHCP

Como se muestra en la ilustración, cuando un dispositivo configurado con DHCP e IPv4 se inicia o se conecta a la red, el cliente transmite un mensaje de detección de DHCP (DHCPDISCOVER) para identificar cualquier servidor de DHCP disponible en la red. Un servidor de DHCP responde con un mensaje de oferta de DHCP (DHCPOFFER), que ofrece una concesión al cliente. El mensaje de oferta contiene la dirección IPv4 y la máscara de subred que se deben asignar, la dirección IPv4 del servidor DNS y la dirección IPv4 del gateway predeterminado. La oferta de concesión también incluye la duración de esta.

La figura muestra una escala de protocolo con un cliente DHCP en un lado y un cliente DHCP en el otro. El cliente DHCP envía un mensaje DHCPDISCOVER al servidor DHCP. El servidor de DHCPv4 envía el mensaje DHCPOFFER asignado al cliente DHCP. El cliente DHCP envía un mensaje DHCPREQUEST en repoonse al DHCPOFFER desde el servidor DHCP. El servidor DHCP envía un mensaje DHCPACK de vuelta al cliente DHCP. El proceso se llama DORA.

Cliente DHCP
Servidor DHCP

DHCPDISCOVER
DHCPOFFER
DHCPREQUEST
DHCPACK

El cliente puede recibir varios mensajes DHCPOFFER si hay más de un servidor de DHCP en la red local. Por lo tanto, debe elegir entre ellos y enviar un mensaje de solicitud de DHCP (DHCPREQUEST) que identifique el servidor explícito y la oferta de concesión que el cliente acepta. Un cliente también puede optar por solicitar una dirección previamente asignada por el servidor.

Suponiendo que la dirección IPv4 solicitada por el cliente, u ofrecida por el servidor, aún está disponible, el servidor devuelve un mensaje de reconocimiento de DHCP (DHCPACK) que le informa al cliente que finalizó la concesión. Si la oferta ya no es válida, el servidor seleccionado responde con un mensaje de reconocimiento negativo de DHCP (DHCPNAK). Si se devuelve un mensaje DHCPNAK, entonces el proceso de selección debe volver a comenzar con la transmisión de un nuevo mensaje DHCPDISCOVER. Una vez que el cliente tiene la concesión, se debe renovar mediante otro mensaje DHCPREQUEST antes de que expire.

El servidor DHCP asegura que todas las direcciones IP sean únicas (no se puede asignar la misma dirección IP a dos dispositivos de red diferentes de forma simultánea). La mayoría de los proveedores de Internet utilizan DHCP para asignar direcciones a los clientes.

DHCPv6 tiene un conjunto similar de mensajes a los de DHCP para IPv4. Los mensajes de DHCPv6 son SOLICIT, ADVERTISE, INFORMATION REQUEST y REPLY.

15.5 Servicios de intercambio de archivos

Desplázate para empezar

15.5.1 Protocolo de transferencia de archivos

Como aprendió en temas anteriores, en el modelo cliente/servidor, el cliente puede cargar datos a un servidor y descargar datos desde un servidor, si ambos dispositivos utilizan un protocolo de transferencia de archivos (FTP). Al igual que los protocolos HTTP, correo electrónico y direccionamiento, FTP es comúnmente utilizado protocolo de capa de aplicación. En este tema se analiza el FTP con más detalle.

El protocolo FTP se desarrolló para permitir las transferencias de datos entre un cliente y un servidor. Un cliente FTP es una aplicación que se ejecuta en una computadora cliente y se utiliza para insertar y extraer datos en un servidor FTP.

La figura representa una transacción FTP entre un cliente y un servidor. Un cliente se pone en contacto con un servidor a través de una red. Conexión de control: El cliente abre la primera conexión al servidor para el tráfico de control. The second message from the client is a data connection: the client opens a second connection for data traffic. Los datos se pueden descargar desde el servidor o cargar desde el cliente.

TP

Cliente

Red

1. Conexión de control:
El cliente abre la primera conexión al servidor para el tráfico de control.
2. Conexión de datos:
El cliente abre la segunda conexión para el tráfico de datos.

Obtener datos

3. Data Transfer:
El servidor transfiere datos al cliente.

De acuerdo con el comando enviado a través de la conexión de control, los datos pueden descargarse desde el servidor o subirse desde el cliente.

El cliente establece la primera conexión al servidor para controlar el tráfico en el puerto TCP 21. El tráfico consiste en comandos de cliente y respuestas de servidor.

El cliente establece la segunda conexión al servidor para la transferencia de datos propiamente dicha por medio del puerto 20 de TCP. Esta conexión se crea cada vez que hay datos para transferir.

La transferencia de datos se puede producir en ambas direcciones. El cliente puede descargar (extraer) datos del servidor o subir datos a él (insertarlos).

15.5.2 Bloque de mensajes del servidor

El bloque de mensajes del servidor (SMB) es un protocolo de intercambio de archivos cliente/servidor que describe la estructura de los recursos de red compartidos, como archivos, directorios, impresoras y puertos serie. Es un protocolo de solicitud-respuesta. Todos los mensajes SMB comparten un mismo formato. Este formato utiliza un encabezado de tamaño fijo seguido de un parámetro de tamaño variable y un componente de datos.

Aquí hay tres funciones de mensajes SMB:

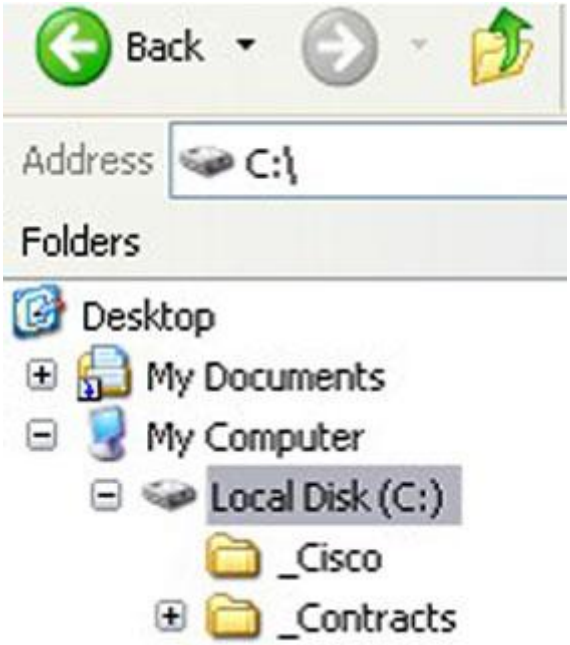
- Iniciar, autenticar y terminar sesiones
- Controlar el acceso a los archivos y a las impresoras
- Autorizar una aplicación para enviar o recibir mensajes para o de otro dispositivo

Los servicios de impresión y transferencia de archivos SMB se han transformado en el pilar de las redes de Microsoft. Con la presentación de la serie de software Windows 2000, Microsoft cambió la estructura subyacente para el uso de SMB. En versiones anteriores de los productos de Microsoft, los servicios de SMB utilizaban un protocolo que no es TCP/IP para implementar la resolución de nombres. A partir de Windows 2000, todos los productos subsiguientes de Microsoft utilizan la convención de nomenclatura DNS, que permite que los protocolos TCP/IP admitan directamente el uso compartido de recursos de SMB, como se muestra en la figura.

La primera figura muestra un recurso compartido de Microsoft Windows de Mis documentos con solicitudes de cliente de un servidor Mis documentos. El cliente envía una solicitud SMB y recibe una respuesta SMB del recurso compartido Mis documentos. Los recursos compartidos incluyen sistemas de archivos, Pronters mostrados como un icono, ranuras de correo y API.

Cliente
Solicitudes SMB
Respuestas SMB
Servidor
Impresora
Recursos compartidos

- Sistemas de archivos
- Impresoras
- Ranuras para correo
- API (Interfaz de Aplicación de Proramación)



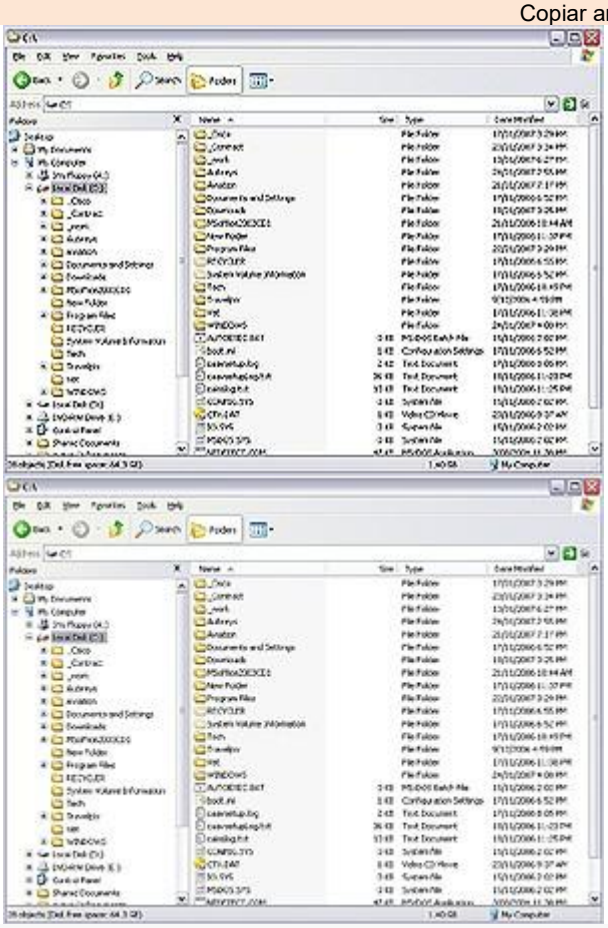
SMB es un protocolo del tipo cliente-servidor, solicitud-respuesta. Los servidores pueden hacer que sus recursos estén disponibles en la red para que los usen los clientes.

El proceso de intercambio de archivos de SMB entre equipos Windows se muestra en la siguiente figura

La segunda figura representa un archivo de copia que tiene lugar entre dos equipos Windows que forman un sistema de archivos al otro a través de la red.

Red

Copiar archivo



Se puede copiar un archivo de una PC a otra con Windows Explorer y usando el protocolo SMB.

A diferencia del protocolo para compartir archivos admitido por FTP, los clientes establecen una conexión a largo plazo con los servidores. Después de establecer 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.

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 utilizando el protocolo SMB.

15.6.1 ¿Qué aprenderé en este módulo?

Aplicación, Presentación y Sesión

En los modelo OSI y TCP/IP La capa de aplicación es la más cercana al usuario final. 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. La capa de presentación tiene tres funciones principales: formatear o presentar datos en el dispositivo de origen en un formulario compatible para recibirlos por el dispositivo de destino, comprimir los datos de forma que el dispositivo de destino pueda descomprimir y cifrar los datos para su transmisión y descifrar los datos al recibirlos - Sí. La capa de sesión crea y mantiene diálogos entre las aplicaciones de origen y de 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. 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 son utilizados tanto por los dispositivos de origen como de destino durante una sesión. Los protocolos implementados tanto en el host de origen como en el de destino deben ser compatibles.

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 comienza el intercambio solicitando los datos al servidor, quien responde enviando uno o más flujos de datos al cliente. En una red P2P, hay dos o más PC que están conectadas por medio de una red y pueden compartir recursos 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 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. 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.

Protocolos de Correo y WEB

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. 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 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. El correo electrónico soporta tres protocolos separados para funcionar: SMTP, POP e IMAP. El proceso de capa de aplicaciones que envía correo utiliza el SMTP. Un cliente recupera el correo electrónico mediante POP o IMAP. 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. 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. Con IMAP 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. Los mensajes originales se mantienen en el servidor hasta que se eliminen manualmente.

Servicios de Direccionamiento IP

El protocolo del DNS define un servicio automatizado que coincide con los nombres de recursos que tienen la dirección de red numérica solicitada. El protocolo de comunicaciones DNS utiliza un formato de mensaje 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. DNS utiliza nombres de domino para formar la jerarquía. 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. La utilidad nslookup permite que el usuario consulte manualmente los servidores de nombres para resolver un nombre de host determinado. DHCP para IPv4 este servicio automatiza la asignación de direcciones IPv4, máscaras de subred, gateway y otros parámetros de redes IPv4. DHCPv6 proporciona servicios similares para clientes IPv6, excepto que no proporciona una dirección de puerta de enlace predeterminada. Cuando un dispositivo configurado con DHCP e IPv4 se inicia o se conecta a la red, el cliente transmite un mensaje de detección de DHCP (DHCPDISCOVER) para identificar cualquier servidor de DHCP disponible en la red. Un servidor de DHCP responde con un mensaje de oferta de DHCP (DHCPOFFER), que ofrece una concesión al cliente. DHCPv6 tiene un conjunto similar de mensajes a los de DHCP para IPv4. Los mensajes de DHCPv6 son SOLICIT, ADVERTISE, INFORMATION REQUEST y REPLY.

Servicios de Compartir Archivos

Un cliente FTP es una aplicación que se ejecuta en una computadora cliente y se utiliza para insertar y extraer datos en un servidor FTP. El cliente establece la primera conexión al

servidor para controlar el tráfico en el puerto TCP 21. El cliente establece la segunda conexión al servidor para la transferencia de datos propiamente dicha por medio del puerto 20 de TCP. El cliente puede descargar (extraer) datos del servidor o subir datos a él (insertarlos). Aqui hay tres funciones de los mensajes SMB pueden iniciar, autenticar y terminar sesiones, controlar el acceso a archivos e impresoras, y permitir que una aplicación envíe mensajes a otro dispositivo o los reciba de él. A diferencia del protocolo para compartir archivos admitido por FTP, los clientes establecen una conexión a largo plazo con los servidores. Después de establecer 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.