Capa de aplicación.

Las aplicaciones como los navegadores web, los juegos en línea, el chat y el correo electrónico con amigos nos permiten enviar y recibir información con relativa facilidad. En general, podemos acceder a estas aplicaciones y utilizarlas sin saber cómo funcionan. Sin embargo, para los profesionales de las redes, es importante saber cómo una aplicación puede formatear, transmitir e interpretar mensajes que se envían y se reciben a través de la red.

La visualización de los mecanismos que permiten la comunicación a través de la red se hace más fácil si utilizamos el esquema en capas del modelo OSI.

En este capítulo, analizaremos la función de la capa de aplicación y la manera en que las aplicaciones, los servicios y los protocolos que están dentro de la capa de aplicación hacen posible una comunicación sólida a través de las redes de datos.

Aplicación, presentación y sesión.

Capa de aplicación.

Capa de aplicación

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.

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).

Capas de presentación y sesión.

La 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 la transmisión 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 Motion Picture Experts Group (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 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. Haga clic en cada protocolo de aplicación de la figura para obtener más información sobre ellos.

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: Sitema de Nombres de dominio (o servidor): protocolo TCP, UDP 53

- Traduce los nombres de dominio tales como cisco.com a direcciones IP

Configuración de host

BOOTP: Protocolo de arranque: protocolo UDP 68 para cliente, 67 para servisor

- 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: Protocolo de configuración dinámica de host: UDP 68 para cliente, 67 Para servidor

- Asigna de manera dinámica direcciones IP a estaciones cliente en la puesta en marcha.

- Permite reutilizar las direcciones cuando ya no se necesitan.

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.

POP: Protocolo de oficina de correo: TCP 110

- Permite a los clientes recibir correo electrónico de un servidor de correo.
- Descarga correo electrónico desde el servidor de correo al escritorio.

IMAP: Protocolo de acceso a mensajes de internet: 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

FTP: Protocolo de transferencia de archivos: 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
- Un protocolo de entrega de archivos confiable, orientado a la conexión y que requiere acuse de recibo.

TFTP: Protocolo de transferencia de archivos trivial: UDP 69

- Es un protocolo de transferencia de archivos simple y sin conexión.
- Es un protocolo de entrega de archivos de mejor esfuerzo y no reconocido.
- Utiliza menos sobrecarga que FTP.

WEB

HTTP: Protocolo de transferencia de hipertexto: TCP 80, 8080

- Conjunto de reglas para intercambiar texto, imágenes gráficas, sonido, vídeo y otros archivos multimedia en la World Wide Web

HTTP: Protocolo seguro de transferencia de hipertexto: TCP, UDP 443

- El navegador usa cifrado para proteger las comunicaciones HTTP.

Autentica el sitCómo interactúan los protocolos de aplicación con las aplicaciones de usuario final.

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 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. Como se muestra en la figura, 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".

- io web al que se conecta el navegador.

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.

En la figura se muestra un ejemplo simple de red P2P. Además de compartir archivos, una red como esta permitiría que los usuarios habiliten juegos en red o compartan una conexión a Internet.

Aplicaciones entre pares.

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:

- eDonkey
- G2
- BitTorrent
- Bitcoin

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. Hay muchas aplicaciones del cliente Gnutella disponibles, como gtk-gnutella, WireShare, Shareaza y Bearshare.

Muchas aplicaciones P2P permiten a los usuarios compartir partes de muchos archivos entre sí al mismo tiempo. 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, lo que se conoce como un enjambre. Esta tecnología se llama BitTorrent. Hay muchos clientes de BitTorrent, incluidos BitTorrent, uTorrent, Frostwire 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. Complete la práctica de laboratorio en la página siguiente para obtener más información sobre estos temas legales.

Protocolos web y de correo electrónico.

Protocolo de transferencia de hipertexto y lenguaje de marcado de hipertexto.

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 que se ejecuta en el servidor mediante el protocolo HTTP. Los nombres que la mayoría de las personas asocia con las direcciones web son URL e identificadores uniformes de recursos (URI).

Para comprender mejor cómo interactúan 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.

Primero, el navegador interpreta las tres partes del URL, como se muestra en la Figura 1:

1. **http** (el protocolo o esquema)

2. **www.cisco.com** (el nombre del servidor)

3. **index.html** (el nombre de archivo específico solicitado)

A continuación, el navegador se comunica con un servidor de nombres para convertir www.cisco.com en una dirección IP numérica que utiliza para conectarse al servidor, como se muestra en la figura 2. Mediante los requisitos de HTTP, el navegador envía una solicitud GET al servidor y solicita el archivo index.html . El servidor envía el código HTML para esta página web al navegador, como se muestra en la figura 3. Finalmente, el navegador descifra el código HTML y da formato a la página para que se pueda visualizar en la ventana del navegador, como se muestra en la figura 4.

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 un 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 para almacenar y enviar que se utiliza para enviar, almacenar 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 mensajes de 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 mensaje. Más bien, ambos clientes dependen del servidor de correo para el transporte de 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 aplicación que envía correo utiliza SMTP. Sin embargo, un cliente recupera el correo electrónico mediante uno de dos protocolos de capa de aplicación: POP o IMAP.

Funcionamiento de 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, como se muestra en la figura.

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.

Funcionamiento de 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. POP funciona de esta forma, de manera predeterminada.

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. 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.

Funcionamiento de 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. 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.

Haga clic aquí para obtener más información acerca de los protocolos de correo electrónico.

Servicios de direccionamiento IP.

Servicio de nombres de dominios.

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, estos nombres de dominio, como http://www.cisco.com, son mucho más fáciles de recordar que algo como 198.133.219.25, que es la dirección numérica real de ese servidor. Si Cisco decide cambiar la dirección numérica de www.cisco.com, 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.

En las figuras 1 a 5, se muestran los pasos relacionados con la resolución DNS.

Formato del 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:

- **A:** una dirección IPv4 de terminal
- **NS:** un servidor de nombre autoritativo
- **AAAA:** una dirección IPv6 de terminal
- **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 DNS en caché.

Jerarquía DNS.

El protocolo DNS utiliza un sistema jerárquico para crear una base de datos que proporcione la resolución de nombres. La jerarquía es similar a un árbol invertido con la raíz en la parte superior y las ramas por debajo (consulte 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.

Nota: 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. Entre los ejemplos de dominios del nivel superior se encuentran:

- **.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 la figura 1, cuando se ejecuta el comando nslookup, se muestra el servidor DNS predeterminado configurado para su host. El nombre de un host o de un dominio se puede introducir en el símbolo del sistema de nslookup. La utilidad nslookup tiene muchas opciones disponibles para realizar una prueba y una verificación exhaustivas del proceso DNS.

En la figura 2, utilice la actividad Verificador de sintaxis para practicar la introducción del comando nslookup tanto en Windows como en Linux.

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.

Las direcciones distribuidas mediante DHCP se conceden durante un tiempo establecido. Una vez que la concesión expira, la dirección se devuelve al grupo para volverse a utilizarla si el host se ha apagado o retirado de la red. 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.

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.

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.

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 que se muestran en la figura de DHCP para IPv4. Los mensajes de DHCPv6 son SOLICIT, ADVERTISE, INFORMATION REQUEST y REPLY

Servicios de intercambio de archivos.

Protocolo de transferencia de archivos.

FTP es otro protocolo de capa de aplicación que se utiliza comúnmente. 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.

Como se muestra en la figura, para transferir datos correctamente, FTP requiere dos conexiones entre el cliente y el servidor, una para los comandos y las respuestas y la otra para la transferencia de archivos propiamente dicha:

- El cliente establece la primera conexión al servidor para el tráfico de control por medio del puerto 21 de TCP, que está constituido por comandos del cliente y respuestas del 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).

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.

Los mensajes SMB pueden:

- 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 1. El proceso de intercambio de archivos de SMB entre equipos Windows se muestra en la figura 2.

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.