En el caso de TCP/IP, esto se implementa a partir del siguiente esquema

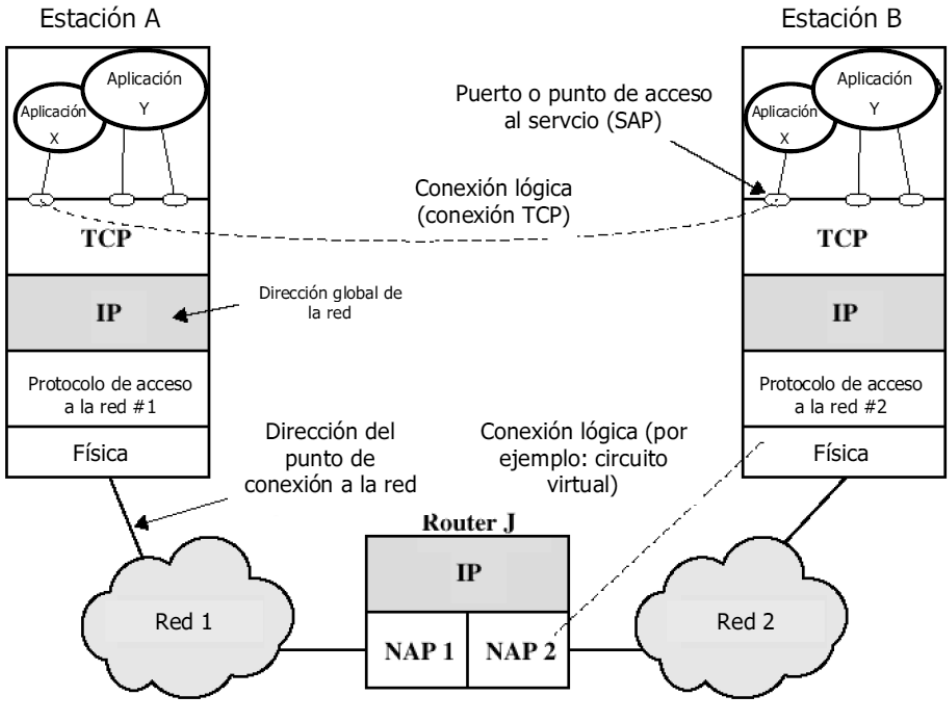


Figura 2.44 Uso del direccionamiento

8) *Multiplexación*: es la capacidad de establecer varias conexiones simultáneas en un único sistema.

2.8 LAS CAPAS SUPERIORES DEL MODELO OSI Y DE TCP/IP

En cuanto al modelo OSI, las capas superiores son la de sesión, presentación y aplicación, resumiendo la función de cada una de ellas tenemos:

- La capa de aplicación: proporciona la interfaz entre las aplicaciones que requieren comunicación y la red física por la cual se transmiten esta información, sus protocolos permiten el intercambio de datos entre los programas ejecutados en los hosts de origen y destino. Existen muchos protocolos de capa de aplicación y siempre se desarrollan protocolos nuevos.

- La capa de presentación: tiene tres funciones principales: la codificación y conversión de datos de la capa de aplicación para que los datos del dispositivo de origen puedan ser entendidos por la aplicación en el dispositivo de destino; la compresión de los datos para hacer más rápida la transmisión, pero garantizando que los pueda descomprimir el dispositivo de destino y la encriptación de los datos para la transmisión y la desencriptación de los mismos cuando lleguen a su destino.

  - ✓ Estándares para videos y gráficos: QuickTime (de Apple) y Moving Picture Experts Group (MPEG)
  - ✓ Estándares de imagen: formato de intercambio gráfico (GIF), Grupo de expertos en fotografía (JPEG) y Formato de archivo de imagen etiquetada (TIFF).

- La capa de sesión: tiene funciones que crean y mantienen diálogos entre las aplicaciones de origen y destino. La capa de sesión maneja el intercambio de información para iniciar los diálogos y mantenerlos activos, y para reiniciar sesiones que se interrumpieron o desactivaron durante un periodo de tiempo prolongado.

Estas tres capas proveen la misma funcionalidad que la capa de aplicación de TCP/IP por lo que trabajan de manera conjunta, los **protocolos de capa de aplicación de TCP/IP** son los que proporcionan intercambio de la información, por lo que manejan información de control y formato necesaria para muchas de las funciones de comunicación de Internet más comunes. Tenemos:

- Protocolo servicio de nombres de dominio (DNS, Domain Name Service) para asignar direcciones IP.
- Protocolo de transferencia de hipertexto (HTTP, Hypertext Transfer Protocol) para transferir archivos que forman las páginas Web de la World Wide Web.
- Protocolo simple de transferencia de correo (SMTP) para transferencia de mensajes de correo.
- Telnet, protocolo de emulación de terminal, para proporcionar acceso remoto a servidores y a dispositivos de red.
- Protocolo de transferencia de archivos (FTP) para transferencia de archivos interactiva entre sistemas.

2.8.1 El modelo cliente-servidor

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

Cualquier dispositivo que responde a una solicitud de aplicaciones de cliente funciona como un servidor. Generalmente es una computadora que contiene información para ser compartida con muchos sistemas de cliente (páginas Web, documentos, bases de datos, imágenes, archivos de audio y video) o recursos, como una impresora de red. Puede haber requisitos para el acceso del cliente, como autenticación de la información de cuenta del usuario (se suele implementar una lista central de cuentas de usuarios y autorizaciones).

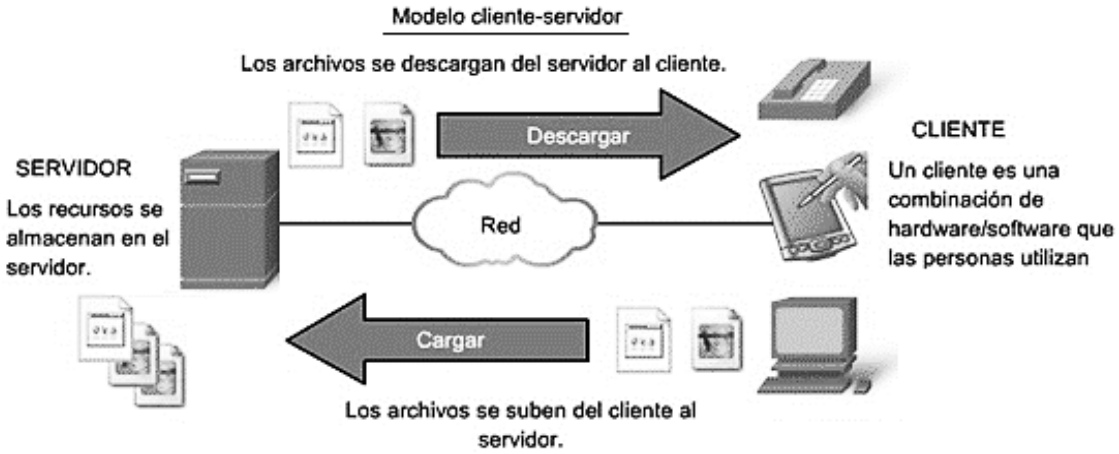


Figura 2.45 Modelo cliente/servidor

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

Una sola aplicación puede emplear diferentes servicios de la capa de aplicación, así lo que aparece para el usuario como una solicitud para una página Web puede, de hecho, equivaler a docenas de solicitudes individuales. Y, para cada solicitud, pueden ejecutarse múltiples procesos. Por ejemplo, un cliente puede necesitar de diversos procesos individuales para formular sólo una solicitud al servidor. Además, los servidores

generalmente tienen múltiples clientes que solicitan información al mismo tiempo. Por ejemplo, un servidor Telnet puede tener varios clientes que requieren conectarse a él. Estas solicitudes individuales del cliente pueden manejarse en forma simultánea y separada para que la red sea exitosa. Los servicios y procesos de la capa de aplicación dependen del soporte de las funciones de la capa inferior para administrar en forma exitosa las múltiples conversaciones.

2.8.2 El modelo punto a punto P2P

En una red punto a punto, dos o más computadoras están conectadas por medio de una red y pueden compartir recursos (como impresoras y archivos) sin tener un servidor dedicado. Cada dispositivo final conectado (9conocido como punto) puede funcionar como un servidor o como un cliente. Una computadora puede asumir la función de servidor para una transacción mientras funciona en forma simultánea como cliente para otra transacción. Las funciones de cliente y servidor se establecen por solicitud. Debido a que las redes punto a punto generalmente no utilizan cuentas de usuarios centralizadas, permisos ni monitores, es difícil implementar las políticas de acceso y seguridad en las redes que contienen mayor cantidad de computadoras. Se deben establecer cuentas de usuario y derechos de acceso en forma individual para cada dispositivo.

Una aplicación punto a punto (P2P), a diferencia de una red punto a punto, permite a un dispositivo actuar como cliente o como servidor dentro de la misma comunicación. En este modelo, cada cliente es un servidor y cada servidor es un cliente. Ambos pueden iniciar una comunicación y se consideran iguales en el proceso de comunicación. Sin embargo, las aplicaciones punto a punto requieren que cada dispositivo final proporcione una interfaz de usuario y ejecute un servicio en segundo plano. Cuando inicia una aplicación punto a punto específico, ésta invoca la interfaz de usuario requerida y los servicios en segundo plano. Después de eso, los dispositivos se pueden comunicar directamente.

Las aplicaciones punto a punto pueden utilizarse en las redes punto a punto, en redes cliente-servidor y en Internet.

2.9 LA CAPA DE APLICACIÓN TCP/IP

La capa de transporte utiliza un esquema de direccionamiento llamado número de puerto, los que identifican las aplicaciones y los servicios de la capa de aplicación que son el origen y el destino de los datos. Los programas del servidor generalmente utilizan números de puerto predefinidos comúnmente conocidos por los clientes. Algunos de estos servicios son:

- Protocolo de transferencia de archivos (FTP) - TCP puertos 20 y 21
- Telnet - TCP puerto 23
- Protocolo simple de transferencia de correo (SMTP) - TCP puerto 25
- Sistema de nombres de dominios (DNS) - TCP/UDP puerto 53
- Protocolo Whois (petición respuesta sobre base de datos – TCP 63
- Protocolo de configuración dinámica de host - UDP puertos 67 y 68
- Protocolo Gopher (predecesor de WWW) – TCP 70
- Protocolo Finger (informa de los usuarios de una máquina) TCP/UDP 79
- Protocolo de transferencia de hipertexto (HTTP) - TCP puerto 80
- Protocolo de oficina de correos (POP) - TCP puerto 110

Tarea: identificar los protocolos asociados a los puertos 22, 66, 107, 118, 119, 137, 138, 150, 194, 443, 522, 6891, 6901 indicando si son TCP o UDP y brevemente la función que soportan

2.9.1 Protocolo y servicios de DNS

En las redes de datos, los dispositivos se etiquetan con una dirección IP numérica, de manera que pueden participar en el envío y la recepción de mensajes de la red. Sin embargo, es difícil recordar estas direcciones numéricas; por lo que los nombres de dominios se crearon para convertir las direcciones numéricas en un nombre sencillo y reconocible. DNS utiliza un conjunto distribuido de servidores para resolver los nombres

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

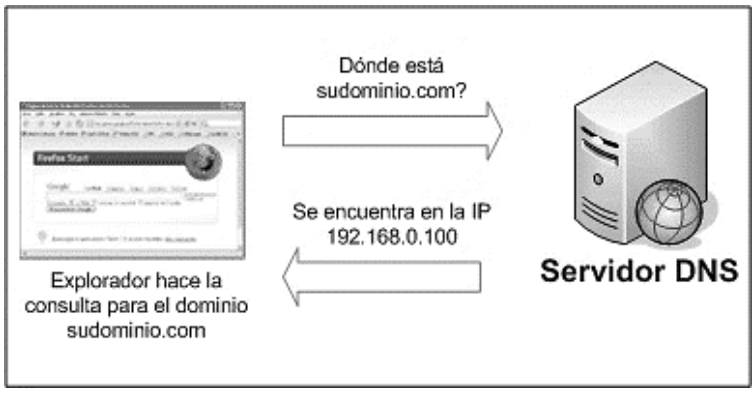


Figura 2.46 Protocolo DNS

Los sistemas operativos cuentan con una herramienta llamada *nslookup* que permite que el usuario consulte de forma manual los servidores de nombres para resolver un nombre de host dado. Esta utilidad también puede utilizarse para solucionar los problemas de resolución de nombres y verificar el estado actual de los servidores de nombres. En la figura, cuando se ejecuta nslookup, se muestra el servidor DNS predeterminado configurado para su host. En este ejemplo, el servidor DNS es dns-sjk.cisco.com que tiene una dirección de 171.68.226.120

Figura 2.47 nslookup

Un servidor DNS proporciona la resolución de nombres utilizando el demonio de nombres que generalmente se llama named (name-dee). 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 de dispositivo final
- NS: un servidor de nombre autoritativo

- CNAME: el nombre canónico (Nombre de dominio completamente calificado) para un alias que se utiliza cuando varios servicios tienen una dirección de red única, pero cada servicio tiene su propia entrada en el DNS
- MX: registro de intercambio de correos; asigna un nombre de dominio a una lista de servidores de intercambio de correos para ese dominio

Cuando un cliente hace una consulta, el proceso "nombrado" del servidor busca primero en sus propios registros (en "caché") para ver si puede resolver el nombre. Si no puede resolverlo con sus registros almacenados, contacta a otros servidores para hacerlo. La solicitud pasa por varios servidores, lo cual puede tomar más tiempo y consumir banda ancha. Una vez que se encuentra una coincidencia y se devuelve al servidor solicitante original, el servidor almacena temporalmente en la caché la dirección numerada que coincide con el nombre. Si vuelve a solicitarse ese mismo nombre, el primer servidor devuelve la dirección almacenada en el caché de nombres. El almacenamiento en caché reduce el tráfico de la red de datos de consultas DNS y las cargas de trabajo de los servidores más altos de la jerarquía.

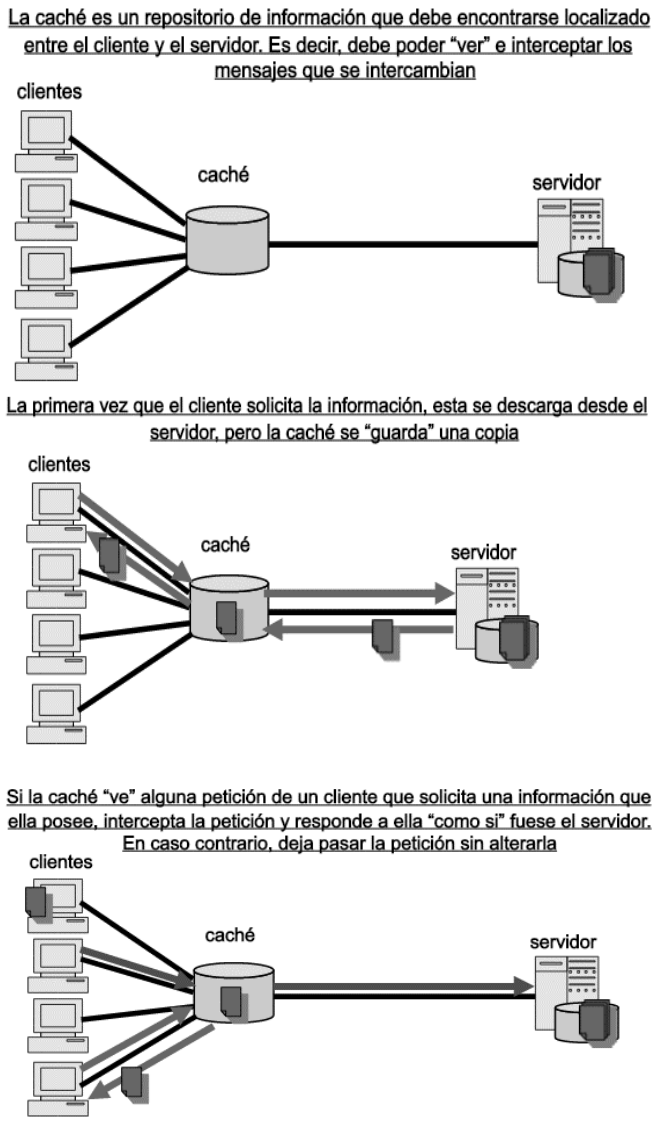


Figura 2.48 Consulta DNS

El sistema de nombres de dominios utiliza un sistema jerárquico para crear una base de datos y proporcionar una resolución de nombres. La jerarquía es piramidal, los servidores raíz mantienen registros sobre cómo alcanzar los servidores de dominio de nivel superior, los cuales a su vez tienen registros que apuntan a los servidores de dominio de nivel secundario y así sucesivamente. Los dominios de primer nivel representan el tipo de organización o el país de origen:

- .pe: Perú
- .co: Colombia
- .com: una empresa o industria
- .jp: Japón
- .org: una organización sin fines de lucro

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

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

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

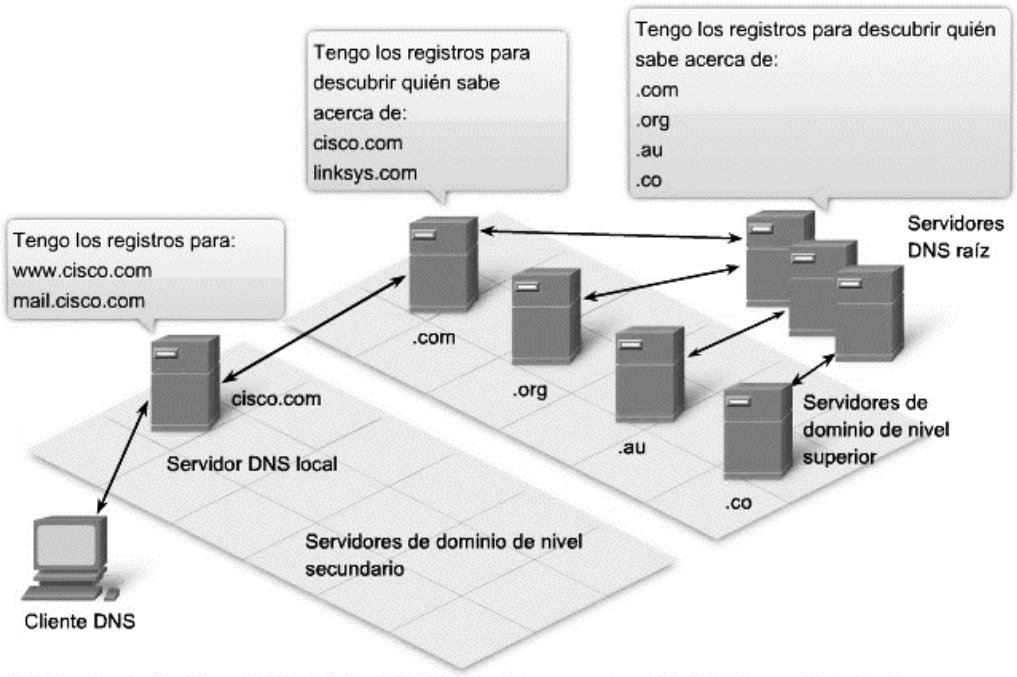


Figura 2.49 Organización DNS

2.9.2 Protocolo WWW y HTTP

El protocolo de transferencia de hipertexto (HTTP), uno de los protocolos del grupo TCP/IP, se desarrolló en sus comienzos para publicar y recuperar las páginas HTML, y en la actualidad se utiliza para sistemas de información distribuidos y de colaboración. HTTP se utiliza a través de la World Wide Web para transferencia de datos y es uno de los protocolos de aplicación más utilizados.

Cuando un explorador de Internet recibe una dirección Web (URL) establece una conexión con el servicio Web del servidor que utiliza el protocolo HTTP. Hay que recordar que URL (Localizador uniforme de recursos) y URI (Identificador uniforme de recursos) son los nombres asociados a las direcciones Web. Los

exploradores Web son las aplicaciones cliente que las computadoras utilizan para conectarse a la World Wide Web y acceder a recursos almacenados en un servidor Web, que funciona como un servicio básico y genera diferentes tipos de archivos disponibles. Para acceder a un contenido, los clientes Web realizan conexiones al servidor y solicitan los recursos deseados. El servidor responde con el recurso solicitado, al recibirlo, el explorador interpreta los datos y los presenta al usuario.

Los exploradores pueden interpretar y presentar muchos tipos de datos, como texto sin cifrar o Lenguaje de marcas de hipertexto (HTML, el lenguaje en el que se crean las páginas Web). Otros tipos de datos, requieren de otros servicios o programas, los que reciben el nombre de plug-ins o complementos. Para ayudar al explorador a determinar qué tipo de archivo está recibiendo, el servidor especifica qué clase de datos contiene el archivo.

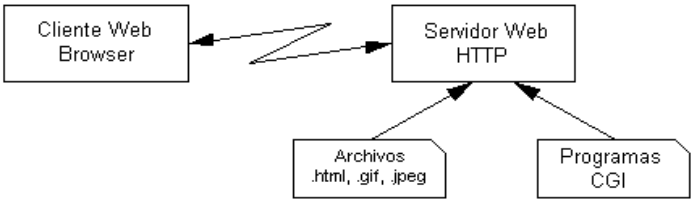
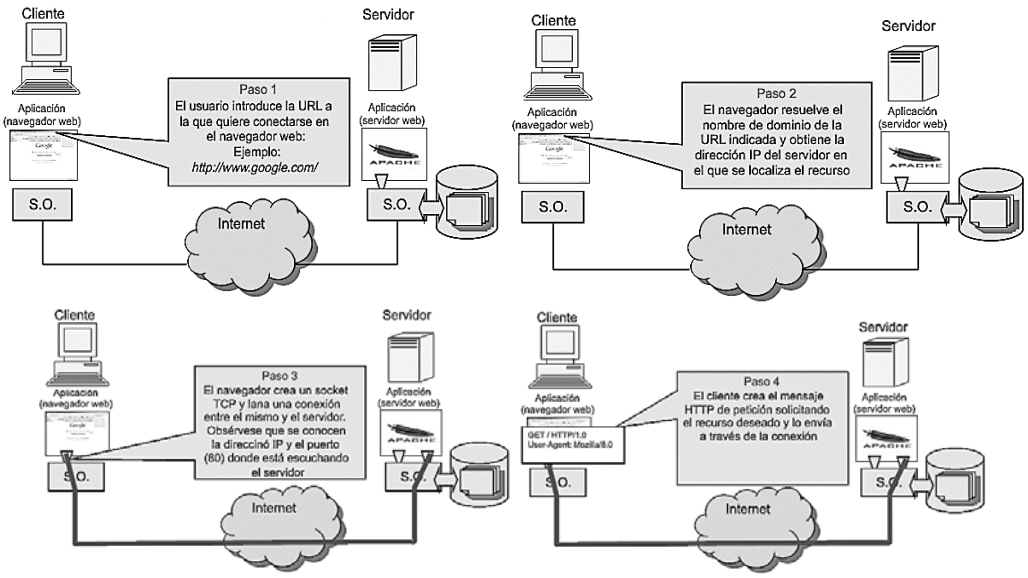


Figura 2.50 HTTP

Si en el explorador Web se escribe la dirección URL: http://www.google.com/web-server.htm. El explorador interpreta las tres partes del URL:

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

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



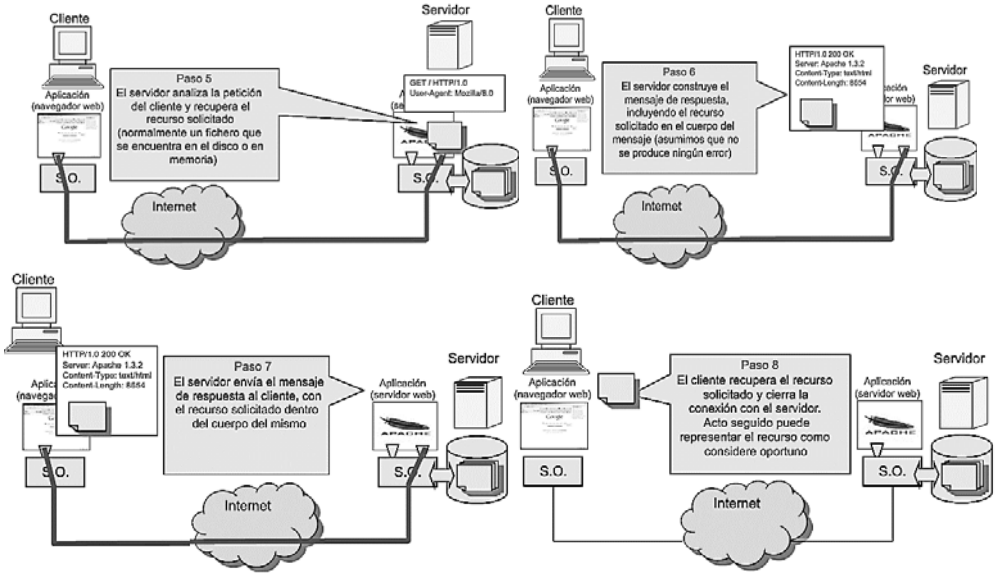


Figura 2.51 Consulta HTTP

El protocolo de transferencia de hipertexto (HTTP), uno de los protocolos del grupo TCP/IP, se desarrolló en sus comienzos para publicar y recuperar las páginas HTML, y en la actualidad se utiliza para sistemas de información distribuidos y de colaboración. HTML exige el uso de formularios

Figura 2.52 HTML

HTTP se utiliza a través de la World Wide Web para transferencia de datos y es uno de los protocolos de aplicación más utilizados, especifica un protocolo de solicitud/respuesta. Cuando un cliente, generalmente un explorador Web, envía un mensaje de solicitud a un servidor, el protocolo HTTP define los tipos de mensajes que el cliente utiliza para solicitar la página Web y envía los tipos de mensajes que el servidor utiliza para responder. Los tres tipos de mensajes comunes son GET, POST y PUT.

- GET es una solicitud de datos por parte del cliente, el explorador Web envía el mensaje GET para solicitar las páginas desde un servidor Web, una vez que el servidor recibe la solicitud GET, responde con una línea de estado, como HTTP/1.1 200 OK, y un mensaje propio, el cuerpo del cual puede ser el archivo solicitado, un mensaje de error u otra información.

- POST y PUT se utilizan para enviar mensajes que cargan datos en el servidor Web. Por ejemplo, cuando el usuario ingresa información en un formato incluido en una página Web, POST incluye la información en el mensaje enviado al servidor.

- PUT carga los recursos o el contenido en el servidor Web.

Aunque es muy flexible, HTTP no es un protocolo seguro. Los mensajes POST cargan información al servidor en un texto sin formato que se puede interceptar y leer. De forma similar, las respuestas del servidor, generalmente páginas HTML, también se descifran. Para una comunicación segura a través de Internet, se utiliza el protocolo HTTP seguro (HTTPS) para acceder o subir información al servidor Web. HTTPS puede utilizar autenticación y encriptación para asegurar los datos cuando viajan entre el cliente y el servidor. HTTPS especifica reglas adicionales para pasar los datos entre la capa de aplicación y la capa de transporte.

TAREA: Realizar una investigación sobre

- *API de Servlets de Java*
- *Servlets HTTP*
- *Set-Cookie*
- *Cookie*
- *Carrito de compra*

2.9.3 Correo electrónico y protocolos SMTP/POP

El correo electrónico requiere de diversos servicios y aplicaciones, los más importantes son el Protocolo de oficina de correos (POP) y el Protocolo simple de transferencia de correo (SMTP), que definen los procesos de cliente-servidor. Al redactar mensajes de correo electrónico se utiliza un Agente de usuario de correo (MUA), o un cliente de correo electrónico, este envía los mensajes y coloca los recibidos en el buzón del cliente; ambos procesos son diferentes, ya que para recibir el cliente de correo electrónico puede utilizar un POP, mientras que al enviar un correo electrónico desde un cliente se utilizan formatos de mensajes y cadenas de comando definidas por el protocolo SMTP. Normalmente el cliente de correo electrónico proporciona la funcionalidad de ambos protocolos dentro de una misma aplicación.

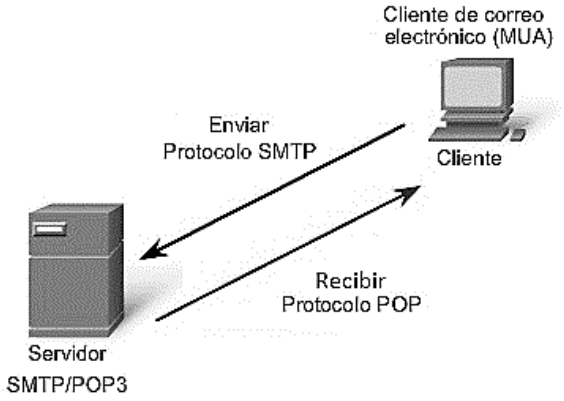


Figura 2.53 Protocolos de correo electrónico

Entonces el servidor de correo electrónico utiliza dos procesos independientes:

- El *Agente de transferencia de correo (MTA)* se utiliza para enviar correo electrónico, este recibe mensajes desde el MUA (emisor o receptor) u algún MTA en otro servidor de correo. Según el encabezado del mensaje recibido determinará cómo reenviar el mensaje para que llegue a su destino. Si el correo está dirigido a un usuario cuyo buzón está en el servidor local, el correo se pasa al MDA. Si el correo es para un usuario que no está en el servidor local, el MTA enruta el correo electrónico al MTA en el servidor correspondiente.

- El *Agente de entrega de correo (MDA)* recibe todo el correo entrante desde el MTA y lo coloca en los buzones de los usuarios correspondientes. El MDA también implementar análisis de virus, correo no deseado filtrado y manejo de acuses de recibo. La mayoría de las comunicaciones de correo electrónico utilizan las aplicaciones MUA, MTA y MDA.

Cuando se utiliza un sistema de correo electrónico corporativo, como Lotus Notes de IBM, Groupwise de Novell o Exchange de Microsoft, estos tienen su propio formato interno de correo electrónico y se utiliza un protocolo propietario, si la comunicación es vía Internet, un gateway de correo del producto realizará los reformateos necesarios. También es posible conectarse a un servicio de correo en un explorador Web para así recuperar y enviar mensajes.

Los protocolos POP y POP3 (Protocolo de oficina de correos v.3) envían correos electrónicos desde el servidor al cliente (MUA). El MDA escucha cuando un cliente se conecta a un servidor y una vez establecida la conexión, el servidor envía el correo electrónico al cliente. El SMTP rige la transferencia de correos salientes desde el cliente emisor al servidor de correos (MDA), así como el transporte de correos entre MTA. Este protocolo utiliza un conjunto rígido de comandos y respuestas, dentro de los que tenemos HELO (identifica el proceso del cliente SMTP para el proceso del servidor SMTP), EHLO (nueva versión del HELO), MAIL FROM (emisor), RCPT TO (receptor) y DATA (cuerpo del mensaje)

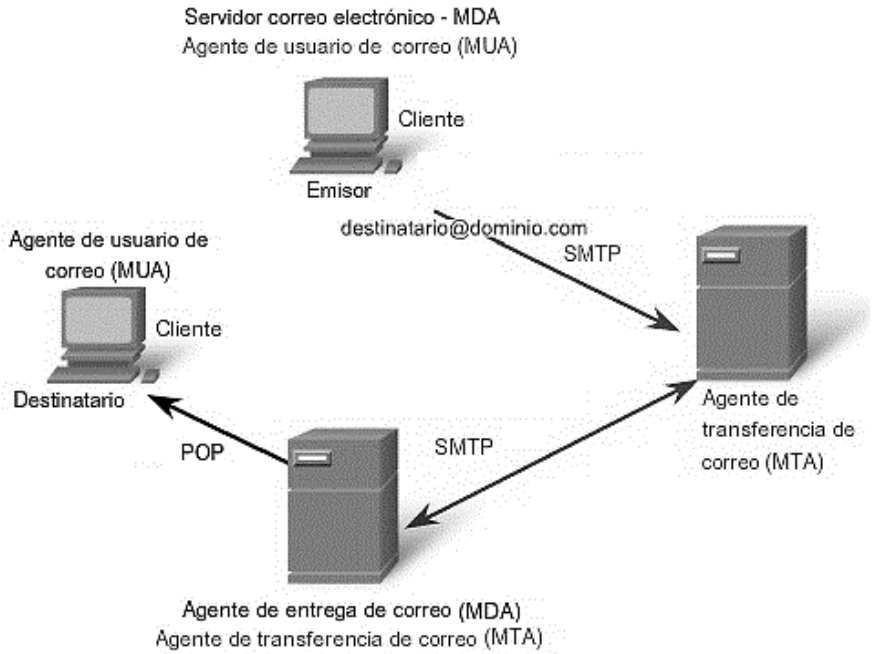


Figura 2.54 Agentes de correo electrónico

2.9.4 FTP

El Protocolo de transferencia de archivos (FTP), permite las transferencias de archivos entre un cliente y un servidor. Un cliente FTP es una aplicación que se ejecuta en una computadora y que carga y descarga archivos de un servidor que ejecuta el demonio FTP (FTPd), para ello requiere dos conexiones entre el cliente y el servidor, una para comandos y respuestas y la otra para la transferencia real de archivos.

Para la primera, el cliente establece la conexión con el servidor en TCP puerto 21, con ella se manejan comandos del cliente y respuestas del servidor, para manejar el tráfico. Para la segunda, el cliente establece la conexión con el servidor en TCP puerto 20 que dura mientras se transfiere el archivo y la transferencia puede ser en ambos sentidos, este modo se conoce como modo activo, también existe el modo pasivo donde el firewall del servidor debe configurarse para aceptar las conexiones en cualquier puerto.

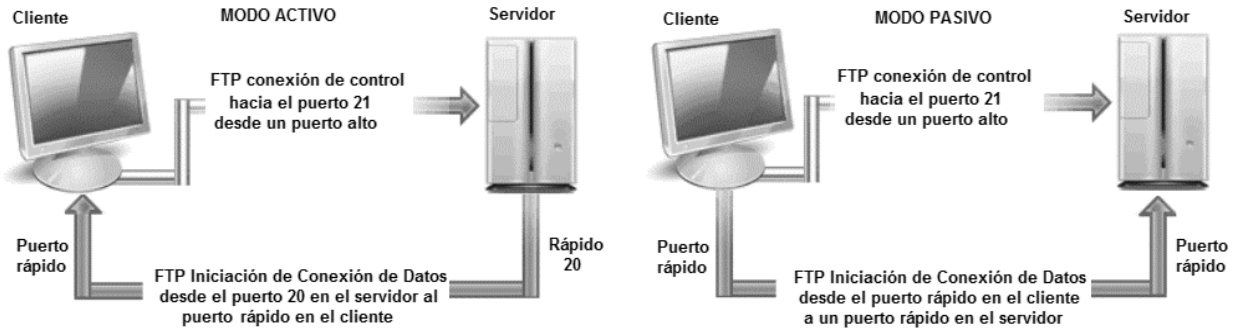


Figura 2.55 FTP

2.9.5 DHCP

El servicio del Protocolo de configuración dinámica de host (DHCP) permite a los dispositivos y hots de una red obtener direcciones dinámicas IP y otra información de un servidor DHCP. Este servicio automatiza la asignación de direcciones IP, máscaras de subred, gateway y otros parámetros de networking del IP. Cuando un host se conecta, se solicita una dirección IP y el servidor DHCP elige una dirección del rango configurado llamado pool y la asigna al host por un tiempo establecido, si el host se desconecta o el tiempo terminó la dirección regresa al pool. Este servicio es imprescindible cuando la dimensión de la red es impredecible. La función de servidor DHCP la puede cumplir un servidor local instalado en una PC o ubicarse en el ISP.

Este esquema genera problemas de seguridad, por lo que suele emplearse una solución mixta DHCP se utiliza para hosts de propósitos generales, como dispositivos de usuario final, y las direcciones fijas se utilizan para dispositivos de red como gateways, switches, servidores e impresoras. Sin DHCP los usuarios tienen que ingresar manualmente la dirección IP, la máscara de subred y otras configuraciones para poder unirse a la red.

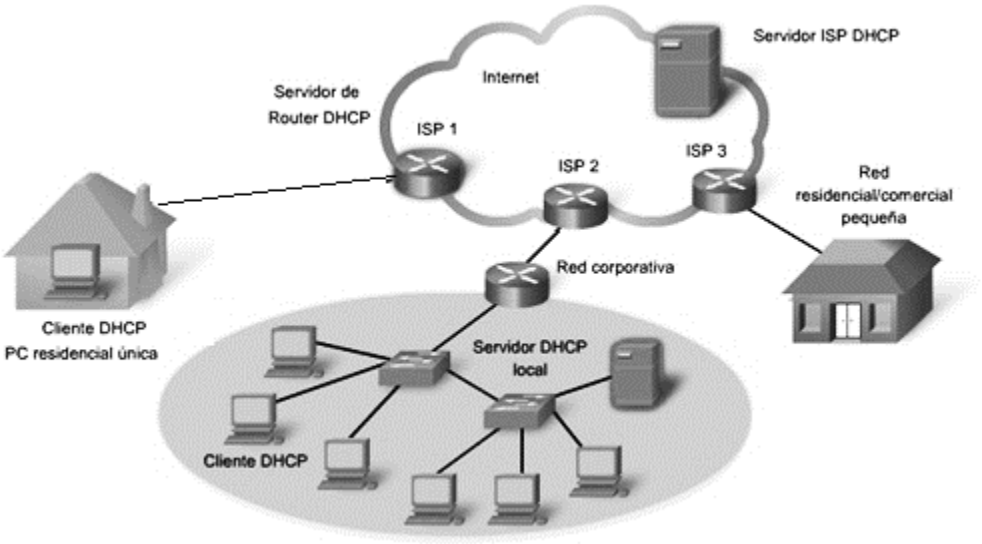


Figura 2.56 DHCP

Proceso:

- Dispositivo configurado por DHCP se conecta a la red

- Cliente envía paquete DESCUBRIMIENTO de DHCP para identificar servidor de DHCP disponible
- Cada servidor de DHCP responde con OFERTA DE DHCP (mensaje de oferta de alquiler = dirección IP, máscara de subred, servidor DNS, Gateway y duración del alquiler)
- Cliente elige entre ofertas y envía paquete de SOLICITUD DE DHCP que identifique el servidor explícito y la oferta de alquiler que el cliente acepta.
- Servidor devolverá mensaje ACK DHCP que informa al cliente que finalizó el alquiler.
- Cliente debe renovar con otro mensaje de SOLICITUD DE DHCP, antes de que termine el alquiler.

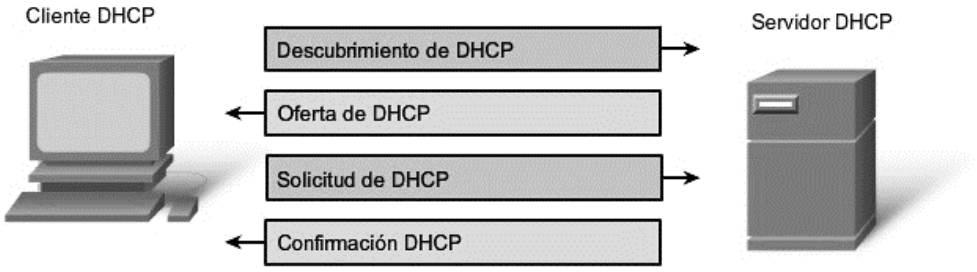


Figura 2.56 Servicio DHCP

2.9.6 Protocolo SMB

El Bloque de mensajes del servidor (SMB) es un protocolo cliente-servidor para compartir archivos, es un protocolo de solicitud-respuesta, los clientes establecen una conexión a largo plazo con los servidores, una vez establecida la conexión, el usuario del cliente puede acceder a los recursos en el servidor como si el recurso fuera local. El intercambio de archivos SMB y los servicios de impresión se han transformado en el pilar de networking de Microsoft, LINUX y UNIX proporcionan SAMBA, Macintosh de Apple usa SMB.

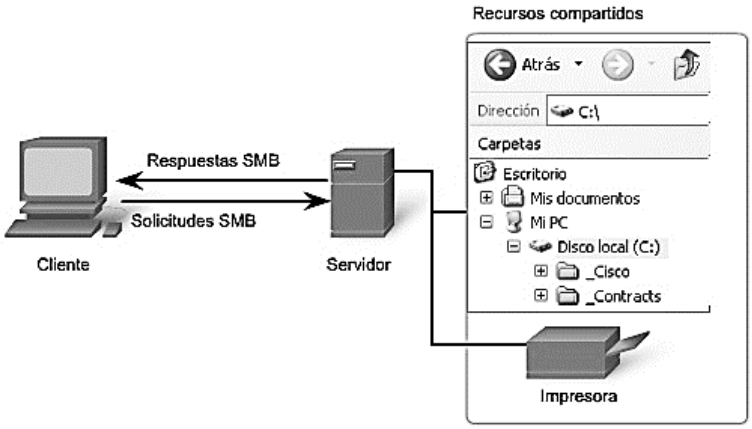


Figura 2.57 Comunicaciones SMB

El formato de mensaje SMB, utiliza un encabezado de tamaño fijo seguido por un parámetro de tamaño variable y un componente de datos, tienen como función:

- Iniciar, autenticar y finalizar sesiones
- Controlar acceso a archivos e impresoras
- Autorizar a una aplicación el enviar o recibir mensajes de otro dispositivo

2.9.7 Telnet

Telnet surge en los 70, es un protocolo antiguo dentro de TCP/IP, proporciona un método de emulación de dispositivos para enviar texto en la red. Una conexión que utiliza Telnet se llama conexión de terminal virtual (VTY), en lugar de usar un dispositivo físico para conectarse al servidor, utiliza software para crear un dispositivo virtual con acceso a la interfaz de línea de comandos (CLI) del servidor.

Para admitir conexiones del cliente a Telnet, el servidor ejecuta un servicio demonio de Telnet, para conectarse se crea un terminal virtual en el host final utilizando una aplicación del cliente Telnet como HyperTerminal, Minicom y TeraTerm, una vez establecida la conexión Telnet, los usuarios pueden realizar cualquier función autorizada en el servidor (iniciar y detener procesos, configurar o apagar el sistema).

Cada comando Telnet consiste en por lo menos dos bytes, el primero es un caracter especial llamado Interpretar como comando (IAC), el que define el byte siguiente como un comando y no texto, se tiene por ejemplo: Are You There (AYT) y Erase Line (EL), Interrupt Process (IP).

Telnet admite autenticación de usuario, pero no datos encriptados, se transporta como texto sin formato, por lo que la seguridad en el mayor problema, por ello existe el Protocolo shell seguro (SSH), que proporciona la estructura para un inicio de sesión remoto seguro y otros servicios de red seguros.

2.10 LA CAPA DE TRANSPORTE TCP/IP

Es el enlace entre la capa de aplicación y la capa responsable de la transmisión de la red, acepta los datos de diferentes sesiones y las pasa a las capas inferiores como partes manejables y multiplexables. Cumple las funciones:

- Rastreo de conversaciones individuales: mantiene los streams de comunicación múltiple entre todas las aplicaciones en el host que tienen abiertas sesiones con otros hosts remotos.
- Segmentación de datos en el host de emisión: los datos se deben enviar a través de los medios en partes manejables, por lo que los protocolos de la capa de transporte describen los servicios para segmentar los datos de la capa de aplicación, esto incluye la encapsulación, donde se agregan encabezados en la capa de transporte para indicar la comunicación a la cual está asociada.
- Reensamblaje de segmentos en el host de recepción, para que cada sección de datos se pueda direccionar a la aplicación adecuada y deben reconstruirse para generar un stream completo de datos para la capa de aplicación, en base a la información del encabezado.
- Identificación de aplicaciones: se debe identificar la aplicación meta, usando un identificador para cada aplicación (número de puerto), incluido en el encabezado de la capa de transporte.
- Conversaciones orientadas a la conexión (algunos protocolos), creando una sesión entre las aplicaciones
- Entrega confiable: si una sección de datos se corrompe o pierde al transmitirse por la red, la capa de transporte debe gestionar que el dispositivo origen retransmita todos los datos perdidos. Las tres operaciones básicas de confiabilidad, soportados en un mayor intercambio de datos de control en el encabezado, son:
    - rastreo de datos transmitidos
    - acuse de recibo de datos recibidos
    - retransmisión de cualquier dato sin acuse de recibo
- Reconstrucción de datos ordenada: los datos llegan en orden equivocado, por las múltiples rutas y tiempos de retardo que pueden tener, por ello numeran y secuencian los segmentos para reensamblarse en el orden adecuado.
- Control del flujo: como los hosts de la red cuentan con recursos limitados (memoria o ancho de banda), si la capa de transporte advierte la sobrecarga, los protocolos deben solicitar que la aplicación origen reduzca la velocidad del flujo de datos, con ello se evita la pérdida de segmentos y la necesitad de retransmisión.

2.10.1 Protocolos TCP y UDP

El Protocolo de control de transmisión (TCP) y el Protocolo de datagramas de usuario (UDP), son los dos protocolos más comunes de la capa de transporte, gestionan la comunicación entre aplicaciones. La diferencia son las funciones específicas de cada uno.

a) Protocolo de datagramas de usuario (UDP)

Protocolo simple, sin conexión, descrito en la RFC 768, provee la entrega de datos sin muchos recursos, usando datagramas. Cuando una maquina A envía paquetes a una maquina B, el flujo es unidireccional, la transferencia de datos es realizada sin haber realizado previamente una conexión con la máquina de destino (maquina B), y el destinatario recibirá los datos sin enviar una confirmación al emisor (la máquina A). Esto es debido a que la encapsulación de datos enviada por el protocolo UDP no permite transmitir la información relacionada al emisor. Por ello el destinatario no conocerá al emisor de los datos excepto su IP. Las aplicaciones que utilizan UDP son: Sistema de nombres de dominio (DNS), Streaming video, Voz sobre IP (VOIP)

b) Protocolo de control de transmisión (TCP)

Protocolo orientado a la conexión, descrito en RFC 793, utiliza funciones adicionales en la misma orden de entrega, son entrega confiable y control de flujo. Cuando una máquina A envía datos a una máquina B, la máquina B es informada de la llegada de datos, y confirma su buena recepción. Aquí interviene el control CRC de datos para verificar la integridad de los datos transmitidos. De este modo, si los datos recibidos son corruptos, el protocolo TCP permite que los destinatarios soliciten al emisor que vuelvan a enviar los datos corruptos. Cada segmento de TCP posee 20 bytes en el encabezado que encapsulan los datos de la capa de aplicación, mientras que cada segmento UDP sólo posee 8 bytes. Las aplicaciones que utilizan TCP son: Exploradores Web, Correo electrónico y Transferencias de archivos

Figura 2.58 TCP/UDP

2.10.2 Direccionamiento de puertos

En el encabezado de cada segmento o datagrama, hay un puerto origen y uno de destino. El número de puerto de origen es el número para la comunicación asociada a la aplicación que la origina en el host local. El número de puerto de destino es el número para la comunicación asociada con la aplicación de destino que origina la comunicación en el host local.

Los números de puerto despende de si el mensaje es una solicitud o una respuesta, los procesos del servidor tienen números de puerto estáticos, en los clientes el puerto es dinámico para cada conversación. Cuando una aplicación de cliente envía una solicitud a una aplicación de servidor, el puerto de destino contenido en el

encabezado es el número de puerto asignado al demonio de servicio, este número de puerto de destino se puede configurar o estar predeterminada

El puerto de origen en el encabezado de un segmento o datagrama de la solicitud de un cliente se crea aleatoriamente con números de puerto mayores de 1023, este número de puerto actúa como dirección de retorno para la aplicación que realiza la solicitud, La combinación número de puerto (capa de transporte)-dirección IP (capa de red) genera un identificador único de un proceso en un host específico, la combinación se denomina socket. Ejemplo, una solicitud de página Web HTTP enviado a un servidor Web (puerto 80) ejecutado en un host con dirección IPv4 192.168.1.20, genera el socket 192.168.1.20:80.

La Autoridad de números asignados de Internet (IANA) asigna números de puerto:

- Del 0 al 1023: se reservan para servicios y aplicaciones como HTTP (servidor Web), POP3/SMTP (servidor de correo electrónico) y Telnet.
- Del 1024 al 49151: a procesos o aplicaciones del usuario.
- Del 49152 a 65535: conocidos como puertos efímeros, asignados de forma dinámica a las aplicaciones cliente cuando se inicia una conexión.

RANGOS	GRUPO DE PUERTOS		TCP		UDP
0 - 1023	**Puertos bien conocidos**	Puerto	Protocolo	Puerto	Protocolo
		21 23 25 80 110 443	FTP Telnet SMTP HTTP POP3 HTTPS	69 520	TFTP RIP
1024 - 49151	**Puertos registrados**	1863 8080	MSN HTTP alternativo	1812 5060	RADIUS SIP
49152 - 65535	**Puertos privados o dinámicos**				

Figura 2.59 Rangos de puertos TCP

Puerto preasignado	Protocolo	Aplicación
80	TCP	HTTP
21	TCP/UDP	FTP
23	TCP/UDP	Telnet
25	TCP/UDP	SMTP
110	TCP/UDP	POP3
119	TCP/UDP	NNTP
137	TCP/UDP	serv. de nombres NetBIOS
161	TCP/UDP	SNMP
194	TCP/UDP	IRC
389	TCP/UDP	LDAP
396	TCP/UDP	NetWare sobre IP
458	TCP/UDP	Apple QuickTime
500	TCP/UDP	ISAKMP

Figura 2.60 Puertos TCP más usados