Contenido

Autor: M. Celeste Weidmann / Bárbara Carina Yunges

¡Copia este texto!

Protocolos de Red

Introducción

De manera general, protocolo es el término que se emplea para denominar al conjunto de normas, reglas y pautas que sirven para guiar una conducta o acción. El concepto de protocolo de red se utiliza en el contexto de la informática para nombrar normativas y criterios que fijan cómo deben comunicarse los diversos componentes de un cierto sistema de interconexión. Esto quiere decir que, a través de este protocolo, los dispositivos que se conectan en red pueden intercambiar datos.

También conocido como protocolo de comunicación, el protocolo de red establece la semántica y la sintaxis del intercambio de información, algo que constituye un estándar. Las computadoras en red, de este modo, tienen que actuar de acuerdo a los parámetros y los criterios establecidos por el protocolo en cuestión para lograr comunicarse entre sí y para recuperar datos que, por algún motivo, no hayan llegado a destino.

En todos los protocolos de red se incluye información que es imprescindible para la conexión. El protocolo indica cómo se concreta la conexión física, establece la manera en que debe comenzar y terminar la comunicación, determina cómo actuar ante datos corrompidos, protege la información ante el ataque de intrusos, señala el eventual cierre de la transmisión, etc.

En la presente unidad estudiaremos los siguientes protocolos: TCP, UDP, FTP, ICMP, SNMP, ARP, DHCP y HTTP. Además veremos algunas herramientas útiles necesarias para el funcionamiento de algunos protocolos: NAT y DNS.

TCP :: Protocolo de Control de la Transmisión

TCP (Protocolo de Control de Transmisión, del inglés Transmission Control Protocol) se diseñó específicamente para proporcionar un flujo de bytes confiable de extremo a extremo a través de una interred no confiable. Una interred difiere de una sola red debido a que sus diversas partes podrían tener diferentes topologías, anchos de banda, retardos, tamaños de paquete y otros parámetros. TCP se diseñó para adaptarse de manera dinámica a las propiedades de la interred y sobreponerse a muchos tipos de fallas.

Es un protocolo confiable orientado a la conexión que permite que un flujo de bytes originado en una máquina se entregue sin errores a cualquier otra máquina en la interred. Este protocolo segmenta el flujo de bytes entrante en mensajes discretos y pasa cada uno a la capa de interred o de red. En el destino, el proceso TCP receptor vuelve a ensamblar los mensajes recibidos para formar el flujo de salida. El TCP también maneja el control de flujo para asegurar que un emisor rápido no pueda inundar a un receptor lento con más mensajes de los que pueda manejar.

Cada máquina que soporta TCP tiene una entidad de transporte TCP, ya sea un procedimiento de biblioteca, un proceso de usuario o (lo más común) sea parte del kernel. En todos los casos, maneja flujos TCP e interactúa con la capa IP. Una entidad TCP acepta flujos de datos de usuario de procesos locales, los divide en fragmentos que no excedan los 64 KB, y envía cada pieza como un datagrama IP independiente. Cuando los datagramas

que contienen datos TCP llegan a una máquina, se pasan a la entidad TCP, la cual reconstruye los flujos de bytes originales.

El protocolo TCP es un protocolo de la capa de la capa de transporte del modelo TCP/IP. El protocolo al ser orientado a conexión, realiza las conexiones y agrega confiabilidad mediante las retransmisiones, junto con el control de flujo y el control de congestión, todo en beneficio de las aplicaciones que lo utilizan. A grandes rasgos debe contemplar el establecimiento de la conexión, el manejo de las conexiones en uso y la desconexión de las mismas.

TCP usa un acuerdo de tres vías para establecer las conexiones. En este acuerdo, el cliente realiza una conexión enviando un paquete SYN al servidor, en el servidor se comprueba si el puerto está abierto (si existe un proceso escuchando por ese puerto), si el puerto no está abierto se le envía al cliente un paquete de respuesta RCT, esto significa un rechazo de intento de conexión. Si el puerto esta abierto, el servidor responde con un paquete SYN/ACK. Entonces el cliente respondería al servidor con un ASK, completando así la conexión.

ACK (acknowledge): Es un mensaje que se envía para confirmar que un mensaje o un conjunto de mensajes han llegado. SYN (synchronize): Se usa para sincronizar los números de secuencia en tres tipos de segmentos: petición de conexión, confirmación de conexión (con ACK activo) y la recepción de la confirmación (con ACK activo). RST (reset): Se utiliza para reiniciar la conexión.

Para el manejo de las conexiones en uso, las cuestiones clave son el control de errores y el control de flujo. El control de errores consiste en asegurar que los datos se entreguen con el nivel deseado de confiabilidad, por lo general que todos los datos se entreguen sin errores. El control de flujo consiste en evitar que un transmisor rápido sature a un receptor lento.

Para la desconexión, en el caso normal en el que uno de los usuarios envía un segmento DR de solicitud de desconexión (DISCONNECTION REQUEST) con el fin de iniciar la liberación de una conexión. Al llegar, el receptor devuelve también un segmento DR e inicia un temporizador, por si acaso se pierde su DR. Cuando este DR llega, el emisor original envía de regreso un segmento ACK y libera la conexión. Finalmente, cuando llega el segmento ACK, el receptor también libera la conexión. Liberar una conexión significa que la entidad de transporte remueve la información sobre la conexión de su tabla de conexiones abiertas y avisa de alguna manera al dueño de la conexión (el usuario de transporte).

La entidad TCP emisora y receptora intercambian datos en forma de segmentos. Un segmento TCP consiste en un encabezado fijo de 20 bytes (más una parte opcional), seguido de cero o más bytes de datos. El encabezado TCP, cuenta entre sus campos con los campos Puerto de origen y Puerto de destino, que identifican los puntos terminales locales de la conexión. Un puerto TCP más la dirección IP de su host forman un punto terminal único de 48 bits. Los puntos terminales de origen y de destino en conjunto identifican la conexión. Además contiene una serie de bits de bandera que le permiten saber si hay congestión, si el datagrama es urgente, si el número de confirmación es válido, indicadores para establecer conexiones o liberarlas

Los números de puerto menores que 1024 están reservados para los servicios estándar que, por lo general, sólo los usuarios privilegiados pueden iniciar, por ejemplo, el usuario root. Éstos se llaman puertos bien conocidos.

Todas las conexiones TCP son full dúplex y de punto a punto. Full dúplex significa que el tráfico puede ir en ambas direcciones al mismo tiempo. Punto a punto significa que cada conexión tiene exactamente dos puntos terminales. TCP no soporta la multidifusión ni la difusión.

UDP :: Protocolo de Datagrama de Usuario

Al igual que TCP, UDP es un protocolo de la capa de transporte. UDP es un protocolo sin conexión, prácticamente no hace nada más que enviar paquetes entre aplicaciones, y deja que las aplicaciones construyan sus propios protocolos en la parte superior según sea necesario.

Es un protocolo sin conexión, no confiable para aplicaciones que no desean la asignación de secuencia o el control de flujo de TCP y prefieren proveerlos por su cuenta. También se utiliza mucho en las consultas de petición-respuesta de una sola ocasión del tipo cliente-servidor, y en las aplicaciones en las que es más importante una entrega oportuna que una entrega precisa, como en la transmisión de voz o video.

UDP proporciona una forma para que las aplicaciones envíen datagramas IP encapsulados sin tener que establecer una conexión. El protocolo UDP se describe en el RFC 768. UDP transmite segmentos que consisten en un encabezado de 8 bytes seguido de la carga útil, el encabezado contiene información de los puertos origen y destino. Los puertos sirven para identificar los puntos terminales dentro de las máquinas de origen y destino. Cuando llega un paquete UDP, su carga útil se entrega al proceso que está conectado al puerto de destino.

El valor principal de contar con UDP en lugar de simplemente utilizar IP puro es la adición de los puertos de origen y destino. Sin los campos de puerto, la capa de transporte no sabría qué hacer con cada paquete entrante. Con ellos, entrega el segmento incrustado a la aplicación correcta.

Una aplicación que utiliza de esta manera a UDP es DNS (el Sistema de Nombres de Dominio), el cual analizaremos en esta misma unidad. En resumen, un programa que necesita buscar la dirección IP de algún host, por ejemplo, www.unlvirtual.edu.ar, puede enviar al servidor DNS un paquete UDP que contenga el nombre de dicho host. El servidor responde con un paquete UDP que contiene la dirección IP del host. No se necesita configuración por adelantado ni tampoco una liberación posterior. Sólo dos mensajes que viajan a través de la red.

El puerto de origen se necesita principalmente cuando hay que enviar una respuesta al origen

A continuación mencionaremos de manera explícita algunas de las cosas que UDP no realiza. No realiza control de flujo, control de congestión o retransmisión cuando se recibe un segmento erróneo. Todo lo anterior le corresponde a los procesos de usuario. Lo que sí realiza es proporcionar una interfaz para el protocolo IP con la característica agregada de demultiplexar varios procesos mediante el uso de los puertos y la detección de errores extremo a extremo opcional. Un área en la que UDP es especialmente útil es en las situaciones cliente-servidor. Con frecuencia, el cliente envía una solicitud corta al servidor y espera una respuesta corta. Si se pierde la solicitud o la respuesta, el cliente simplemente puede esperar a que expire su temporizador e intentar de nuevo. El código no sólo es

simple, sino que se requieren menos mensajes (uno en cada dirección) en comparación con un protocolo que requiere una configuración inicial, como TCP.

HTTP :: Protocolo de Transferencia de Hipertexto

Hypertext Transfer Protocol es el protocolo de comunicación que permite las transferencias de información en la World Wide Web. HTTP fue desarrollado por el World Wide Web Consortium y la Internet Engineering Task Force, colaboración que culminó en 1999 con la publicación de una serie de RFC, el más importante de ellos es el RFC 2616 que especifica la versión 1.1.

HTTP define la sintaxis y la semántica que utilizan los elementos de software de la arquitectura web (clientes, servidores, proxies) para comunicarse. HTTP es un protocolo sin estado, es decir, no guarda ninguna información sobre conexiones anteriores. El desarrollo de aplicaciones web necesita frecuentemente mantener estado. Para esto se usan las cookies, que es información que un servidor puede almacenar en el sistema cliente. Esto le permite a las aplicaciones web instituir la noción de "sesión", y también permite rastrear usuarios ya que las cookies pueden guardarse en el cliente por tiempo indeterminado.

Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor.

El protocolo de transferencia de hipertexto (HTTP) es un protocolo de comunicaciones que permite la transferencia de documentos de lenguaje de marcas de hipertexto (HTML) desde servidores web a navegadores web. HTML es un lenguaje de identificadores para la creación de documentos que contienen enlaces a información relacionada.

Para enviar y recibir documentos HTML e interaccionar con la World Wide Web, tanto el servidor como el cliente deben soportar HTTP. En el proceso, el navegador realiza una solicitud HTTP, entonces el servidor procesa la solicitud y después envía una respuesta HTTP. En realidad, la comunicación se realiza en más etapas si se considera el procesamiento de la solicitud en el servidor, pero de en esencia consiste en una solicitud y una respuesta.

Una solicitud HTTP es un conjunto de líneas que el navegador envía al servidor. Incluye un linea de solicitud, un encabezado y un cuerpo de solicitud.

Una línea de solicitud es una línea que especifica el tipo de documento solicitado, el método que se aplicará y la versión del protocolo utilizada. La línea está formada por tres elementos que deben estar separados por un espacio:

- el método
- la dirección URL
- la versión del protocolo utilizada por el cliente (por lo general, HTTP/1.0)

Los campos del encabezado de solicitud son un conjunto de líneas opcionales que permiten aportar información adicional sobre la solicitud y/o el cliente (navegador, sistema operativo, etc.). Cada una de estas líneas está formada por un nombre que describe el tipo de encabezado, seguido de dos puntos (:) y el valor del encabezado.

El cuerpo de la solicitud es un conjunto de líneas opcionales que deben estar separadas de las líneas precedentes por una línea en blanco y, por ejemplo, permiten que se envíen datos por un comando POST durante la transmisión de datos al servidor utilizando un formulario.

Desde el punto de vista del usuario, internet consiste en una enorme colección de contenido en forma de páginas web, por lo general, conocidas simplemente como páginas. Cada una puede contener vínculos a otras páginas en cualquier lugar del mundo. Para seguir un vínculo, los usuarios pueden hacer clic en él, y a continuación los llevará a la página apuntada. Este proceso se puede repetir de manera indefinida. La idea de hacer que una página apunte a otra, lo que ahora se conoce como hipertexto, fue inventada por un profesor del MIT, Vannevar Bush, en 1945. Esto fue mucho antes de que se inventara Internet.

Por lo general, las páginas se ven mediante un programa llamado navegador. Mozilla Firefox, Chromium y Iceweasel son ejemplos de navegadores. El navegador obtiene la página solicitada, interpreta el contenido y despliega la página en pantalla con el formato adecuado. El contenido en sí puede ser una mezcla de texto, imágenes y comandos de formato, ya sea en forma de un documento tradicional u otras formas de contenido, como un video o programas que produzcan una interfaz gráfica con la que puedan interactuar los usuarios.

A continuación el navegador obtiene la nueva página y la despliega en pantalla. El navegador se encarga del proceso de obtención de las páginas, sin ninguna ayuda del usuario. De esta forma, el proceso de desplazarse entre máquinas al momento de ver contenido es transparente para el usuario. El navegador despliega una página web en la máquina cliente. Para obtener cada página, se envía una solicitud a uno o más servidores, los cuales responden con el contenido de la página. HTTP es el protocolo de solicitud-respuesta para obtener páginas, es un protocolo simple basado en texto que se ejecuta sobre TCP.

El contenido puede ser simplemente un documento que se lea de un disco, o el resultado de una consulta en una base de datos y la ejecución de un programa. El contenido de la respuesta de los servidores se integra para que el navegador lo despliegue. La visualización conlleva un rango de procesamiento que depende del tipo de contenido. Además de generar texto y gráficos, puede implicar la reproducción de un video o la ejecución de una secuencia de comandos (script) que presente su propia interfaz de usuario como parte de la página.

El lado del cliente

En esencia, un navegador es un programa que puede mostrar una página web y capturar clics del ratón para los elementos de la página visualizada. Al seleccionar un elemento, el navegador sigue el hipervínculo y obtiene la página seleccionada. Cuando se creó la web por primera vez, resultó obvio a primera vista que para hacer que una página apuntara a otra página web se requerían mecanismos para nombrar y localizar páginas. En particular, había que responder a tres preguntas para desplegar una página:

- ¿Cómo se llama la página?
- ¿En dónde está ubicada?
- ¿Cómo se puede acceder a ella?

La solución que se eligió identifica a las páginas de una manera que resuelve los tres problemas a la vez. A cada página se le asigna un URL (Localizador Uniforme de Recursos, del inglés Uniform Resource Locator) que sirva de manera efectiva como el nombre mundial de la página. Los URL tienen tres partes: el protocolo (también conocido como esquema, el nombre DNS de la máquina en la que se encuentra la página y la ruta que indica de manera única la página específica (un archivo a leer o un programa a ejecutar en la máquina).

En el caso general, la ruta tiene un nombre jerárquico que modela la estructura de un directorio de archivos. Sin embargo, la interpretación de la ruta depende del servidor; puede o no reflejar la estructura del directorio real. Como ejemplo, el URL de la página: http://www.unlvirtual.edu.ar/campus-virtual-unl/ consiste de tres partes: el protocolo (http), el nombre DNS del host (www.unlvirtual.edu.ar) y el nombre de la ruta (campus-virtual-unl).

Cuando un usuario hace clic en un hipervínculo, el navegador lleva a cabo una serie de pasos para obtener la página a la que apunta.

1. El navegador determina el URL (al ver lo que se seleccionó).
2. El navegador pide al DNS la dirección IP del servidor www.unlvirtual.edu.ar.
3. El DNS responde con 190.122.240.127.
4. El navegador realiza una conexión TCP a 190.122.240.127 en el puerto 80, el puerto conocido para el protocolo HTTP.
5. Después envía una solicitud HTTP para pedir la página /campus-virtual-unl/.
6. El servidor www.unlvirtual.edu.ar envía la página como una respuesta HTTP, por ejemplo, enviando el archivo /campus-virtual-unl/.
7. Si la página incluye los localizadores URL necesarios para desplegar en pantalla, el navegador obtiene los otros URL mediante el mismo proceso. En este caso, los URL incluyen una imagen incrustada que también se obtienen de www.unlvirtual.edu.ar, y varias secuencia de comandos (script), por ejemplo de google-analytics.com.
8. El navegador despliega la página /campus-virtual-unl/.
9. Se liberan las conexiones TCP si no hay más solicitudes para los mismos servidores durante un periodo corto.

Muchos navegadores tienen la opción de "inspeccionar documento" para poder visualizar la estructura de la página web, las peticiones del protocolo HTTP y los recursos a los que hacer referencia. En Mozilla Firefox, por ejemplo, esta opción está disponible haciendo clic con el botón derecho del mouse sobre el documento, opción "inspeccionar elemento". En Chromium a través de la opción "Inspeccionar" disponible con el botón derecho del mouse sobre la página; En el navegador Midori, con la opción "inspeccionar elemento".

El lado del servidor

Cuando el usuario escribe un URL o hace clic en una línea de hipertexto, el navegador analiza el URL e interpreta la parte entre http:// y la siguiente barra diagonal como un nombre DNS que debe buscar. Equipado con la dirección IP del servidor, el navegador establece una conexión TCP con el puerto 80 de ese servidor. Después envía un comando que contiene el

resto del URL, que es la ruta a la página en ese servidor. A continuación, el servidor devuelve la página para que el navegador la despliegue en pantalla.

Los pasos que el servidor web realiza en su ciclo principal son:

1. Aceptar una conexión TCP de un cliente (un navegador).
2. Obtener la ruta a la página, que viene siendo el nombre del archivo solicitado.
3. Obtener el archivo (del disco).
4. Enviar el contenido del archivo al cliente.
5. Liberar la conexión TCP.

Los servidores web modernos tienen más características, pero en esencia esto es lo que hace un servidor web para el caso simple del contenido que se encuentra en un archivo. En cuanto al contenido dinámico, el tercer paso se puede reemplazar por la ejecución de un programa (que se determina con base en la ruta) que devuelve el contenido.

Los servidores web se implementan con un diseño diferente para atender muchas solicitudes por segundo. Un problema con el diseño simple es que el proceso para acceder a los archivos es comúnmente el “cuello de botella”. Las lecturas de disco son muy lentas en comparación con la ejecución de un programa; además los mismos archivos se pueden leer repetidas veces del disco mediante el uso de las llamadas del sistema operativo. Otro problema es que sólo se procesa una solicitud a la vez. El archivo puede ser extenso y bloqueará a las otras solicitudes mientras se esté transfiriendo.

Una mejora evidente (que utilizan todos los servidores web) es mantener una caché en memoria de los n archivos leídos más recientes, o un cierto número de gigabytes de contenido. Así, antes de ir al disco para obtener un archivo, el servidor revisa la caché. Si el archivo está ahí, puede servirse directamente de la memoria, con lo cual se elimina el acceso al disco. Aunque un uso efectivo de la caché requiere de una gran cantidad de memoria principal y cierto tiempo de procesamiento adicional para verificar la caché y administrar su contenido, el ahorro en tiempo justifica casi siempre la sobrecarga y los gastos implícitos.

HTTPS :: Protocolo seguro de transferencia de hipertexto

Hypertext Transfer Protocol Secure (en español: Protocolo seguro de transferencia de hipertexto), más conocido por sus siglas HTTPS, es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hipertexto, es decir, es la versión segura de HTTP.

El sistema HTTPS utiliza un cifrado basado en SSL/TLS para crear un canal cifrado (cuyo nivel de cifrado depende del servidor remoto y del navegador utilizado por el cliente) más apropiado para el tráfico de información sensible que el protocolo HTTP. De este modo se consigue que la información sensible (usuario y claves de paso normalmente) no pueda ser usada por un atacante que haya conseguido interceptar la transferencia de datos de la conexión, ya que lo único que obtendrá será un flujo de datos cifrados que le resultará imposible de descifrar.

El puerto estándar para este protocolo es el 443. En el protocolo HTTP las URLs comienzan con "http://" y utilizan por omisión el puerto 80, las URLs de HTTPS comienzan con "https://" y utilizan el puerto 443 por omisión.

FTP :: Protocolo de Transferencia de Archivos

Una de las primeras aplicaciones básicas desarrolladas en el entorno de lo que después sería la red Internet fue la transferencia de ficheros entre diferentes sistemas. Al principio de los años setenta ya se elaboraron las primeras especificaciones del protocolo más utilizado para esta finalidad, el FTP. Después de algunas modificaciones y mejoras, la especificación oficial del protocolo se publicó en 1985 en el documento RFC 959.

FTP (siglas en inglés de File Transfer Protocol, 'Protocolo de Transferencia de Archivos') este protocolo de red fue desarrollado para la transferencia de archivos entre sistemas conectados a una red TCP, basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

El servicio FTP es ofrecido por la capa de aplicación del modelo de capas de red TCP/IP al usuario, utilizando normalmente el puerto de red 20 y el 21. Un problema básico de FTP es que está pensado para ofrecer la máxima velocidad en la conexión, pero no la máxima seguridad, ya que todo el intercambio de información, desde el login y password del usuario en el servidor hasta la transferencia de cualquier archivo, se realiza en texto plano sin ningún tipo de cifrado, con lo que un posible atacante puede capturar este tráfico, acceder al servidor y/o apropiarse de los archivos transferidos.

Para solucionar este problema son de gran utilidad aplicaciones como SCP y SFTP, incluidas en el paquete SSH, que permiten transferir archivos pero cifrando todo el tráfico.

El protocolo proporciona también operaciones para que el cliente pueda manipular el sistema de ficheros del servidor: borrar ficheros o cambiarles el nombre, crear y borrar directorios, listar sus contenidos, etc. Uno de los objetivos principales de este protocolo consiste en permitir la interoperabilidad entre sistemas muy distintos, escondiendo los detalles de la estructura interna de los sistemas de ficheros locales y de la organización de los contenidos de los ficheros.

En el modelo general descrito en la especificación del FTP, tanto en el servidor como en el cliente hay dos entidades que intervienen en la transferencia de ficheros: el intérprete de protocolo y el proceso de transferencia.

a) El intérprete de protocolo se encarga del intercambio de los comandos del protocolo. En la parte del cliente, las operaciones que el usuario solicita por medio de la interfaz de usuario, el intérprete las convierte en una secuencia adecuada de comandos FTP y se envían al servidor. En la parte del servidor se interpretan los comandos recibidos, se generan las respuestas correspondientes y se envían al cliente. Por tanto, el intérprete cliente debe analizar estas respuestas, por ejemplo, para informar al usuario del resultado de la operación o para proseguir la secuencia de comandos FTP.

b) El proceso de transferencia de datos, que está bajo el control del intérprete de protocolo, se encarga de intercambiar los datos que deben transferirse, es decir, los contenidos de los ficheros o bien los listados de los directorios. Tanto en la parte del cliente, como en la del

servidor este proceso interactúa directamente con el sistema de ficheros locales para leer sus datos o para almacenarlos en los mismos.

Los dos intérpretes de protocolo se comunican mediante una conexión TCP llamada conexión de control. Cuando deben transferirse datos de un sistema al otro, se establece otra conexión TCP entre los dos procesos de transferencia de datos denominada conexión de datos. Generalmente, la parte activa de esta conexión (la que la inicia) constituye el proceso de transferencia del servidor, y la parte pasiva, el del cliente.

El FTP está basado en conexiones TCP. El intérprete de protocolo del servidor debe estar preparado para recibir peticiones de conexión en un puerto TCP que, por defecto, es el asignado oficialmente al servicio FTP: el número 21.

El intérprete de protocolo del cliente establece una conexión de control con el puerto del intérprete servidor. En esta conexión se utilizan las reglas especificadas en el protocolo Telnet. Ello significa que, por defecto, los intérpretes de protocolo se intercambian mensajes codificados con bytes de 8 bits, según el juego de caracteres ASCII, y representan los finales de línea con la secuencia <CRLF>.

Los comandos FTP constituyen los mensajes que envía el intérprete cliente, y los que envía el intérprete servidor son respuestas a dichos comandos. Las respuestas se generan siguiendo el orden en que el cliente envía los comandos, puesto que en general el servidor efectúa las operaciones de manera secuencial (no empieza una nueva operación hasta que no ha acabado la anterior).

Filezilla es una solución FTP libre, en el sitio oficial del proyecto se encuentra disponible para descarga el cliente FTP y el servidro FTP. https://filezilla-project.org/

ICMP Protocolo de Mensajes de Control de Internet

Los enrutadores supervisan muy de cerca el funcionamiento de Internet. Cuando ocurre algo inesperado durante el procesamiento de un paquete en un enrutador, ICMP (Protocolo de Mensajes de Control en Internet, del inglés Internet Control Message Protocol) informa sobre el evento al emisor. ICMP también se utiliza para probar Internet. Hay definidos alrededor de una docena de tipos de mensajes ICMP, cada uno de los cuales se transporta encapsulado en un paquete IP.

Mensajes de ICMP

- El mensaje DESTINATION UNREACHABLE (DESTINO INACCESIBLE) se usa cuando el enrutador no puede localizar el destino o cuando un paquete con el bit DF no puede entregarse porque hay una red de “paquetes pequeños” que se interpone en el camino.
- El mensaje TIME EXCEEDED (TIEMPO EXCEDIDO) se envía al descartar un paquete porque su contador Ttl (Tiempo de vida) ha llegado a cero. Este evento es un síntoma de que los paquetes se están repitiendo o que los valores establecidos en el contador son muy bajos.
- El mensaje PARAMETER PROBLEM (PROBLEMAS DE PARÁMETROS) indica que se ha descubierto un valor ilegal en un campo de encabezado. Este problema indica un

error en el software de IP del host emisor, o tal vez en el software de un enrutador por el que se transita.

- El mensaje SOURCE QUENCH (FUENTE DISMINUIDA) se utilizaba hace tiempo para regular a los hosts que estaban enviando demasiados paquetes. Se esperaba que cuando un host recibiera este mensaje, redujera la velocidad. En la actualidad raras veces se usa pues cuando ocurre una congestión, estos paquetes tienden a agravar más la situación y no está claro cómo responderles. Ahora, el control de congestión en Internet se hace sobre todo en la capa de transporte, en donde se utilizan las pérdidas de paquetes como señales de congestión.
- El mensaje REDIRECT (REDIRECCIONAR) se usa cuando un enrutador se percata de que un paquete parece estar mal enrutado. Lo utiliza el enrutador para avisar al host emisor que se actualice con una mejor ruta.
- Los mensajes ECHO (ECO) y ECHO REPLY (RESPUESTA DE ECO) se utilizan para ver si un destino dado es alcanzable y está vivo. Se espera que el destino envíe de vuelta un mensaje ECHO REPLY luego de recibir el mensaje ECHO. Estos mensajes se utilizan en la herramienta ping que verifica si un host está activo en Internet.
- Los mensajes TIMESTAMP REQUEST (PETICIÓN DE ESTAMPA DE TIEMPO) y TIMESTAMP REPLY (RESPUESTA DE ESTAMPA DE TIEMPO) son similares, excepto que el tiempo de llegada del mensaje y el tiempo de salida de la respuesta se registran en ésta. Esta característica se puede usar para medir el desempeño de la red.
- Los mensajes ROUTER ADVERTISEMENT (ANUNCIO DE ENRUTADOR) y ROUTER SOLICITATION (SOLICITUD DE ENRUTADOR) se usan para permitir que los hosts encuentren los enrutadores cercanos. Un host necesita aprender la dirección IP de por lo menos un enrutador para enviar paquetes por la red local.

La cuestión de si el ICMP es un protocolo, o si más bien es una herramienta que utiliza el protocolo IP para notificar errores genera mucha polémica. Lo cierto es que el ICMP constituye el mecanismo básico para la gestión de las diferentes incidencias que pueden ocurrir en una red IP

Además de estos mensajes, se han definido otros. La lista se conserva en www.iana.org/assignments/icmp-parameters.

ARP: Protocolo de Resolución de Direcciones

Aunque en Internet cada máquina tiene una o más direcciones IP, en realidad éstas no son suficientes para enviar paquetes. Las NIC (Tarjetas de Interfaz de Red) de la capa de enlace de datos no entienden las direcciones de Internet. En el caso de Ethernet, cada NIC de las que se hayan fabricado viene equipada con una dirección Ethernet única de 48 bits. Los fabricantes de NIC Ethernet solicitan un bloque de direcciones Ethernet al IEEE para asegurar que no haya dos NIC con la misma dirección (y evitar conflictos en caso de que las dos NIC aparezcan alguna vez en la misma LAN). Las NIC envían y reciben tramas basadas en direcciones Ethernet de 48 bits. No saben nada sobre direcciones IP de 32 bits.

La pregunta ahora es: ¿cómo se convierten las direcciones IP en direcciones de la capa de enlace de datos, como Ethernet? Para explicar cómo funciona esto, veamos un ejemplo: Supongamos una red ethernet conmutada llamada CC, en dicha red hay dos host, HOST_1

con dirección IP_1 Y dirección MAC MAC_1, y un host llamada HOST_2, cuya dirección ip es IP_2 y dirección mac es MAC_2.

ARP funciona de la siguiente manera, para que el HOST_1 pueda mandar un paquete al HOST_2 (ambos en la red Ethernet CC) el HOST_1 envía un paquete de difusión hacia Ethernet y pregunte quién posee la dirección IP del HOST_2, IP_2 (Esta dirección la obtuvo por DNS). La difusión llegará a cada máquina en la Ethernet CC y cada una verificará su dirección IP. Al HOST_2 le bastará responder con su dirección de Ethernet, la dirección MAC_2. De esta manera, el HOST_1 aprende que la dirección IP_2 está en el host con la dirección Ethernet MAC_2.

El software IP en el HOST_1 crea una trama Ethernet dirigida a MAC_2, pone el paquete IP (dirigido a IP_2) en el campo de carga útil y lo descarga hacia la Ethernet. La NIC Ethernet del HOST_2, MAC_2, detecta esta trama, la reconoce como una trama para sí mismo, la recoge y provoca una interrupción. El controlador de Ethernet extrae el paquete IP de la carga útil y lo pasa al software IP, el cual ve que esté direccionado de forma correcta y lo procesa.

Casi todas las máquinas en Internet ejecutan ARP, la definición de ARP está en el RFC 826. La ventaja de usar ARP en lugar de archivos de configuración es su simpleza. El administrador del sistema sólo tiene que asignar a cada máquina una dirección IP y decidir respecto a las máscaras de subred. ARP se hace cargo del resto.

La descripción anterior es útil para comprender el procesamiento de ARP, pero el protocolo es un poco más complejo, y cuenta con varias optimizaciones para trabajar con más eficiencia. Por ejemplo, una vez que una máquina ha ejecutado ARP, guarda el resultado en caché, en caso de que tenga que ponerse en contacto con la misma máquina en poco tiempo. La siguiente vez encontrará la asociación en su propio caché, con lo cual se elimina la necesidad de una segunda difusión. En muchos casos, el HOST_2 necesitará devolver una respuesta y se verá forzado también a ejecutar el ARP para determinar la dirección Ethernet del emisor (HOST_1). Podemos evitar esta difusión de ARP haciendo que el HOST_1 incluya su asociación IP a Ethernet en el paquete ARP. Cuando la difusión de ARP llega al HOST_2, se introduce el par (IP_1, MAC_1) en la caché ARP del HOST_2. De hecho, todas las máquinas en Ethernet pueden introducir esta asociación en su caché ARP.

Para permitir que las asociaciones cambien, por ejemplo, al configurar un host para que use una nueva dirección IP (pero que mantenga su vieja dirección Ethernet), las entradas en la caché ARP deben expirar después de unos cuantos minutos. Para ayudar a mantener actualizada la información en la caché y optimizar el desempeño, cada máquina difunde su asociación (IP, MAC) cuando se configura. Por lo general, esta difusión se realiza en forma de un ARP que busca su propia dirección IP.

SNMP :: Protocolo Simple de Administración de Red

Simple Network Management Protocol, desde su publicación en 1988, SNMP se ha usado en un número de redes cada vez mayor y en entornos cada vez más complejos; rápidamente se ha convertido en el estándar predominante de gestión de red.

El SNMP es un protocolo de la capa de aplicación que facilita el intercambio de información de gestión entre dispositivos de una red. SNMP es parte de TCP/IP, permite a los

administradores de red supervisar el rendimiento de la red, buscar y resolver sus problemas y planear el crecimiento de la red.

SNMP es una herramienta sencilla para la gestión de red. Define una base de información de gestión (MIB) limitada y de fácil implementación, de variables escalares y tablas de dos dimensiones, y define un protocolo eficiente para permitir que un administrador obtenga y establezca variables de la MIB y que un agente emita notificaciones no solicitadas, llamadas interceptaciones (traps). La robustez de SNMP se basa en esta simplicidad. SNMP se implementa fácilmente y consume una cantidad moderada de recursos de procesador y de red.

Una red administrada a través de SNMP consta de tres componentes clave:

- Sistemas administradores de red (Network Management Systems, NMS)
- Dispositivos administrados (Managed Devices, MD)
- Agentes (Agent).

Un sistema administrador de red (NMS) ejecuta aplicaciones que supervisan y controlan a los dispositivos administrados. Los NMS's proporcionan el volumen de recursos de procesamiento y memoria requeridos para la administración de la red. Uno o más NMS's deben existir en cualquier red administrada. Un dispositivo administrado es un dispositivo que contiene un agente SNMP y reside en una red administrada. Estos recogen y almacenan información de administración, la cual es puesta a disposición de los NMS's usando SNMP. Los dispositivos administrados, a veces llamados elementos de red, pueden ser routers, servidores de acceso, switches, bridges, hubs, computadores o impresoras. Un agente es un módulo de software de administración de red que reside en un dispositivo administrado. Un agente posee un conocimiento local de información de administración (memoria libre, número de paquetes IP recibidos, rutas, etcétera), la cual es traducida a un formato compatible con SNMP y organizada en jerarquías.

Con SNMP se puede monitorizar el estado de un enlace punto a punto para detectar cuándo está congestionado y tomar así las medidas oportunas; se puede hacer que una impresora alerte al administrador cuando se ha quedado sin papel, o que un servidor envíe una alerta cuando la carga de su sistema se incrementa significativamente. SNMP también permite la modificación remota de la configuración de dispositivos, de forma que se podría modificar las direcciones IP de un ordenador a través de su agente SNMP, u obligar a la ejecución de comandos (si el agente ofrece las funcionalidades necesarias).

SNMP sirve para configurar dispositivos remotos. La información de configuración puede enviarse a cada host conectado a la red desde el sistema de administración. También sirve para supervisar el rendimiento de la red, puede hacer un seguimiento de la velocidad de procesamiento y el rendimiento de la red, y recopilar información acerca de las transmisiones de datos. Detectar errores en la red o accesos inadecuados, con SNMP se puede configurar las alarmas que se desencadenarán en los dispositivos de red cuando se produzcan ciertos sucesos. Cuando se dispara una alarma, el dispositivo envía un mensaje de suceso al sistema de administración. Además, se puede utilizar para auditar el uso de la red, supervisando el uso general de la red para identificar el acceso de un grupo o usuario (por ejemplo cuando entra "root"), y los tipos de uso de servicios y dispositivos de la red.

DHCP :: Protocolo de Configuración Dinámica de Host

DHCP (de sus siglas en inglés: Dynamic Host Configuration Protocol) es un protocolo de red de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van quedando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después. Así los clientes de una red IP pueden conseguir sus parámetros de configuración automáticamente. Este protocolo se publicó en octubre de 1993, y su implementación actual está en la RFC 2131. Para DHCPv6 se publica el RFC 3315.

El DHCP se describe en los RFC 2131 y 2132. Se utiliza ampliamente en Internet para configurar todo tipo de parámetros, además de proporcionar a los hosts direcciones IP. Al igual que en las redes de negocios y domésticas, los ISP usan DHCP para establecer los parámetros de los dispositivos a través del enlace de acceso a Internet, de modo que los clientes no tengan que comunicarse por teléfono con sus ISP para obtener esta información. Algunos ejemplos comunes de la información que se configura incluyen la máscara de red, la dirección IP de la puerta de enlace predeterminada y las direcciones IP de los servidores DNS y de tiempo. DHCP ha reemplazado en gran parte los protocolos anteriores (conocidos como RARP y BOOTP), con una funcionalidad más limitada.

Con DHCP, cada red debe tener un servidor DHCP responsable de la configuración. Al iniciar una computadora, ésta tiene integrada una dirección Ethernet u otro tipo de dirección de capa de enlace de datos en la NIC, pero no cuenta con una dirección IP. En forma muy parecida al ARP, la computadora difunde una solicitud de una dirección IP en su red. Para ello usa un paquete llamado DHCP DISCOVER. Este paquete debe llegar al servidor DHCP. Si el servidor no está conectado directamente a la red, el enrutador se configurará para recibir difusiones DHCP y transmitirlas al servidor DHCP en donde quiera que se encuentre. Cuando el servidor recibe la solicitud, asigna una dirección IP libre y la envía al host en un paquete DHCP OFFER (que también se puede transmitir por medio del enrutador). Para que esto pueda funcionar incluso cuando los hosts no tienen direcciones IP, el servidor identifica a un host mediante su dirección Ethernet (la cual se transporta en el paquete DHCP DISCOVER).

Un problema que surge con la asignación automática de direcciones IP de una reserva es determinar qué tanto tiempo se debe asignar una dirección IP. Si un host sale de la red y no devuelve su dirección IP al servidor DHCP, esa dirección se perderá en forma permanente. Después de un tiempo, tal vez se pierdan muchas direcciones. Para evitar que eso ocurra, la asignación de direcciones IP puede ser por un periodo fijo de tiempo, una técnica conocida como arrendamiento. Justo antes de que expire el arrendamiento, el host debe pedir una renovación al DHCP. Si no puede hacer una solicitud o si ésta se rechaza, tal vez el host ya no pueda usar la dirección IP que recibió antes.

El protocolo DHCP incluye tres métodos de asignación de direcciones IP:

- Asignación manual o estática: Asigna una dirección IP a una máquina determinada. Se suele utilizar cuando se quiere controlar la asignación de dirección IP a cada cliente, y evitar, también, que se conecten clientes no identificados.

- Asignación automática: Asigna una dirección IP a una máquina cliente la primera vez que hace la solicitud al servidor DHCP y hasta que el cliente la libera. Se suele utilizar cuando el número de clientes no varía demasiado.
- Asignación dinámica: El único método que permite la reutilización dinámica de las direcciones IP. El administrador de la red determina un rango de direcciones IP y cada dispositivo conectado a la red está configurado para solicitar su dirección IP al servidor cuando la tarjeta de interfaz de red se inicializa. El procedimiento usa un concepto muy simple en un intervalo de tiempo controlable. Esto facilita la instalación de nuevas máquinas clientes.

Un servidor DHCP puede proporcionar parámetros de configuración opcionales para el cliente. El RFC 2132 describe las opciones de DHCP disponibles definidas por Internet Assigned Numbers Authority (IANA) - Parámetros DHCP y BOOTP.5 Un cliente DHCP puede seleccionar, manipular y sobrescribir los parámetros proporcionados por un servidor DHCP.

La instalación de un servidor DHCP en GNU/Linux es bastante sencilla, por ejemplo, para la distribuciones Debian, un servidor DHCP se puede instalar a través de alguna de las 3 formas que se detallan a continuación:

```
# apt-get install dhcp
```

```
# apt-get install dhcp3-server
```

```
# apt-get install isc-dhcp-server
```

El principal archivo de configuración es: dhcpd.conf, en dicho archivo, se deberá configurar el rango de dirección ip a ser asignadas, como así también el tipo de asignación: estática o dinámica; como así también otros parámetros adicionales.

Para reiniciar el servico, luego de introducir cambios en el archivo de configuración, cualquiera de las dos opciones:

```
# service dhcpd restart
```

```
# /etc/init.d/dhcpd restart
```

SMTP :: Protocolo para Transferencia Simple de Correo

El Simple Mail Transfer Protocol (SMTP) o “protocolo para transferencia simple de correo”, es un protocolo de red a nivel de capa de aplicación, utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos. Fue definido en el RFC 2821 y es un estándar oficial de Internet.

El funcionamiento de este protocolo se da en línea, de manera que opera en los servicios de correo electrónico. Sin embargo, este protocolo posee algunas limitaciones en cuanto a la recepción de mensajes en el servidor de destino (cola de mensajes recibidos). Como alternativa a esta limitación se asocia normalmente a este protocolo con otros, como el POP o IMAP, otorgando a SMTP la tarea específica de enviar correo, y recibirlos empleando los otros protocolos antes mencionados (POP O IMAP).

El SMTP es el protocolo más utilizado en Internet para transferir mensajes de correo electrónico. Proporciona la funcionalidad necesaria para conseguir una transferencia fiable y eficiente de mensajes de correo entre ordenadores que actúan como oficina de correos.

Siguiendo las ideas del correo postal, el SMTP se basa en el almacenamiento y el reenvío. Es decir, cuando un mensaje llega a una oficina, queda almacenado en la misma cierto tiempo antes de ser entregado a otra oficina o al destinatario final. Conviene señalar, asimismo, que cada usuario debe disponer de un buzón para recibir mensajes, el cual siempre debe estar asociado a una oficina determinada.

El SMTP está basado en conexiones TCP y el puerto que tiene asignado es el 25.

El emisor SMTP hace llegar mensajes de correo al receptor. Para conseguirlo, se establece un diálogo entre los dos con comandos que envía al emisor y respuestas con las que contesta el receptor. Tanto los comandos como las respuestas SMTP siguen las reglas específicas del protocolo Telnet. Es decir, constituyen cadenas de caracteres codificados con bytes según el código ASCII y se utiliza la secuencia <CRLF> para representar el final de línea.

La arquitectura del sistema, consiste en dos tipos de subsistemas: los agentes de usuario, que permiten a la gente leer y enviar correo electrónico, y los agentes de transferencia de mensajes, que mueven los mensajes del origen al destino. También nos referiremos a los agentes de transferencia de mensajes de una manera informal como servidores de correo.

El agente de usuario es un programa que proporciona una interfaz gráfica, que permite interactuar con el sistema de correo electrónico. Incluye un medio para redactar mensajes y respuestas a éstos, desplegar los mensajes entrantes y organizarlos al archivarlos, realizar búsquedas y eliminarlos. Un agente de usuario se ejecuta en la misma computadora en la que un usuario lee su correo. Es sólo otro programa más y se puede ejecutar sólo parte del tiempo. Los agentes de transferencia de mensajes son en general procesos del sistema. Se ejecutan en segundo plano en equipos servidores de correo con la intención de estar siempre disponibles. Su tarea es mover de manera automática el correo electrónico a través del sistema, desde el que lo originó hasta el receptor mediante el SMTP. Éste es el paso de transferencia del mensaje.

Vincular los agentes de usuario y los agentes de transferencia de mensajes son los conceptos de los buzones de correo y un formato estándar de mensajes de correo electrónico. Los buzones de correo almacenan el correo electrónico que recibe un usuario. Los servidores de correo se encargan de su mantenimiento. Para ello, los agentes de usuario envían comandos a los servidores de correo para manipular los buzones de correo, inspeccionar su contenido, eliminar mensajes, etc. La recuperación del correo es la entrega final. Con esta arquitectura, un usuario puede usar distintos agentes de usuario en varias computadoras para acceder a un buzón de correo.

El correo se envía entre un agente de transferencia de mensajes y otro en un formato estándar. El formato RFC 5322, que se extendió con soporte para contenido multimedia y texto internacional. A este esquema se le conoce como MIME. Una idea clave en el formato de los mensajes es la distinción entre la envoltura y su contenido. La primera encapsula el mensaje y contiene toda la información necesaria para transportarlo, como la dirección de destino, la prioridad y el nivel de seguridad, todo lo cual es distinto del mensaje en sí. Los agentes de transporte de mensajes usan la envoltura para el enrutamiento. El mensaje dentro de la envoltura consiste en dos partes separadas: el encabezado y el cuerpo. El primero contiene la información de control para los agentes de usuario. El cuerpo es exclusivo para el destinatario humano; a ninguno de los agentes le importa mucho.

NAT :: Traducción de Dirección de Red

NAT del inglés Network Address Translation, se describe en el RFC 3022.

La función NAT se ha diseñado para simplificar y conservar direcciones IP. La conversión de direcciones de red o NAT se desarrolló para resolver la falta de direcciones IP con el protocolo IPv4. En las direcciones IPv4, la cantidad de direcciones IP enrutables (que son únicas en el mundo) no es suficiente para permitir que todos los equipos que lo requieran estén conectados a Internet; Por lo tanto, el principio de NAT consiste en utilizar una conexión de pasarela a Internet, que tenga al menos una interfaz de red conectada a la red interna y al menos una interfaz de red conectada a Internet (con una dirección IP enrutable) para poder conectar todos los equipos a la red.

NAT permite que las interredes IP privadas que usan direcciones IP no registradas puedan conectarse a Internet. NAT se ejecuta en un router, generalmente, conectando dos redes, y traduce las direcciones privadas (no universalmente únicas) de la red interna en direcciones legales antes de reenviar paquetes a otra red. Como parte de esta funcionalidad, NAT se puede configurar para anunciar una o muy pocas direcciones para toda la red al mundo exterior. De esta forma, se ofrece más seguridad y se oculta de forma efectiva toda la red interna del mundo que está detrás de dicha dirección. NAT ofrece una doble función de seguridad y conservación de red, y generalmente, se implementa en entornos de acceso remoto.

Es cuestión de crear, al nivel de la pasarela, una conversión de paquetes desde la red interna hacia la red externa.

Por lo tanto, se configura cada equipo en la red que necesite acceso a Internet para que utilice una pasarela de NAT (al especificar la dirección IP de la pasarela en el campo "Gateway" con sus parámetros TCP/IP). Cuando un equipo de red envía una solicitud a Internet, la pasarela hace la solicitud en su lugar, recibe la respuesta y la envía al equipo que hizo la solicitud. Debido a que la pasarela oculta completamente las direcciones internas en la red, el mecanismo de conversión de direcciones de red brinda una función segura. De hecho, para un observador externo de la red, todas las solicitudes parecen provenir de la dirección IP de pasarela.

NAT dinámica permite que diversos equipos con direcciones privadas compartan una dirección IP enrutable (o un número reducido de direcciones IP enrutables). Desde afuera, todos los equipos de la red interna poseen la misma dirección IP. Ésta es la razón por la cual a veces se utiliza el término "enmascaramiento IP" para indicar la conversión de direcciones de red dinámica.

Para poder compartir las diferentes direcciones IP en una o varias direcciones IP enrutables, NAT dinámica utiliza la Conversión de direcciones por puerto (PAT, Port Address Translation), la asignación de un puerto de origen diferente para cada solicitud, de manera que se pueda mantener una correspondencia entre las solicitudes que provienen de la red interna y las respuestas de los equipos en Internet, todas enviadas a la dirección IP del router.

DNS :: Sistema de Nombres de Dominio

DNS se define en los RFC 1034, 1035, 2181. El sistema de nombres de dominio, más comúnmente conocido por sus siglas en inglés como Domain Name System o DNS, básicamente es el encargado de traducir las series de números que conforman una dirección IP en palabras que el usuario pueda recordar fácilmente.

Cada página web es accedida mediante una dirección IP. El problema es que al haber tanta cantidad, es imposible recordar el IP de cada una.

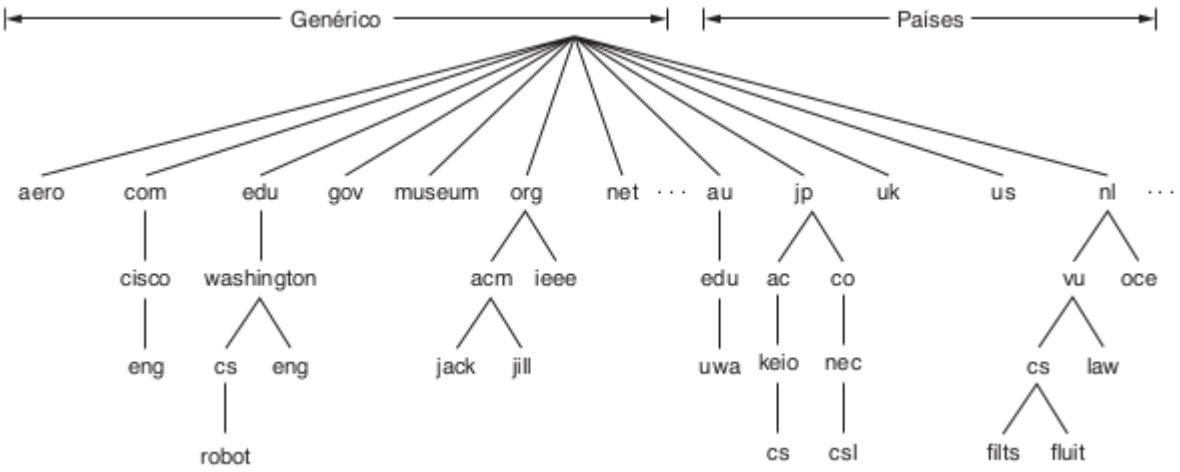
Aunque en teoría los programas pueden hacer referencia a páginas web, buzones de correo y otros recursos mediante las direcciones de red (por ejemplo, IP) de las computadoras en las que se almacenan, a las personas se les dificulta recordar estas direcciones. Además, navegar en las páginas web de una universidad desde un servidor con la dirección ip 190.122.240.127 significa que si la universidad mueve el servidor web a una máquina diferente con una dirección IP distinta, hay que avisar a todos sobre la nueva dirección IP. Por este motivo se introdujeron nombres legibles de alto nivel con el fin de separar los nombres de máquina de las direcciones de máquina. De esta manera, el servidor web de la universidad podría conocerse como www.unlvirtual.edu.ar sin importar cuál sea su dirección IP. Sin embargo, como la red sólo comprende direcciones numéricas, se requiere algún mecanismo para convertir los nombres en direcciones de red.

La esencia del DNS es la invención de un esquema jerárquico de nombres basado en dominios y un sistema de base de datos distribuido para implementar este esquema de nombres. El DNS se usa principalmente para asociar los nombres de host con las direcciones IP, pero también se puede usar para otros fines.

En Internet, el nivel superior de la jerarquía de nombres se administra mediante una organización llamada ICANN (Corporación de Internet para la Asignación de Nombres y Números, del inglés Internet Corporation for Assigned Names and Numbers), la cual se creó para este fin en 1998 como parte del proceso de maduración de Internet, que se convirtió en un asunto económico a nivel mundial.

Internet se divide en más de 250 dominios de nivel superior, cada uno de los cuales abarca muchos hosts. Cada dominio se divide en subdominios, los que a su vez también se dividen, y así en lo sucesivo. Todos estos dominios se pueden representar mediante un árbol. Las hojas del árbol representan los dominios que no tienen subdominios (pero que contienen máquinas). Un dominio de hoja puede contener un solo host, o puede representar a una compañía y contener miles de hosts.

Los dominios de nivel superior se dividen en dos categorías: genéricos y países. Los dominios genéricos incluyen los dominios originales de la década de 1980 y los dominios introducidos mediante solicitudes a la ICANN. Los dominios de país incluyen una entrada para cada país, como se define en la ISO 3166.



El DNS está compuesto por tres partes con funciones bien diferenciadas:

- Cliente DNS: está instalado en el cliente y realiza peticiones de resolución de nombres a los servidores DNS.
- Servidor DNS: son los que contestan las peticiones y resuelven los nombres mediante un sistema estructurado en árbol. Las direcciones DNS que ponemos en la configuración de la conexión, son las direcciones de los Servidores DNS.
- Zonas de autoridad: son servidores o grupos de ellos que tienen asignados resolver un conjunto de dominios determinado (como los .ar o los .org).

La resolución de nombres utiliza una estructura en árbol, mediante la cual los diferentes servidores DNS de las zonas de autoridad se encargan de resolver las direcciones de su zona, y sino se lo solicitan a otro servidor que creen que conoce la dirección.

Bibliografia

- Redes de Computadoras. Andrew S. Tanenbaum, David J. Wetherall. Capitulo 6.5 "LOS PROTOCOLOS DE TRANSPORTE DE INTERNET: TCP"
- Redes de Computadoras. Andrew S. Tanenbaum, David J. Wetherall. Capítulo 6.4 "LOS PROTOCOLOS DE TRANSPORTE DE INTERNET: UDP"
- Redes de Computadoras. Andrew S. Tanenbaum, David J. Wetherall. Capítulo 7.3.4 "HTTP: el Protocolo de Transferencia de HiperTexto"
- Redes de Computadoras. Andrew S. Tanenbaum, David J. Wetherall. Capitulo 7.2 "CORREO ELECTRÓNICO"
- Redes de Computadoras. Andrew S. Tanenbaum, David J. Wetherall. Capítulo 7.1 "DNS: EL SISTEMA DE NOMBRES DE DOMINIO"
- Redes de Computadoras. Andrew S. Tanenbaum, David J. Wetherall. Capítulo 5.6.4 "Protocolos de control en Internet"
- https://es.wikipedia.org/wiki/File_Transfer_Protocol
- https://es.wikipedia.org/wiki/Hypertext_Transfer_Protocol

- https://es.wikipedia.org/wiki/Hypertext_Transfer_Protocol_Secure
- https://es.wikipedia.org/wiki/Categor%C3%ADa:Navegadores_web_libres
- https://es.wikipedia.org/wiki/Internet_Control_Message_Protocol
- https://filezilla-project.org/
- https://es.wikipedia.org/wiki/Simple_Network_Management_Protocol
- https://es.wikipedia.org/wiki/Traducci%C3%B3n_de_direcciones_de_red