Protocolo de datagramas de usuario (UDP)

Protocolo de datagramas de usuario (UDP)

El grupo de protocolos de Internet también maneja un protocolo de transporte sin conexiones, el UDP (User Data Protocol, protocolo de datos de usuario). El UDP ofrece a las aplicaciones un mecanismo para enviar datagramas IP en bruto encapsulados sin tener que establecer una conexión.

Muchas aplicaciones cliente-servidor que tienen una solicitud y una respuesta usan el UDP en lugar de tomarse la molestia de establecer y luego liberar una conexión. El UDP se describe en el RFC 768. Un segmento UDP consiste en una cabecera de 8 bytes seguida de los datos. La cabecera se muestra a continuación. Los dos puertos sirven para lo mismo que en el TCP: para identificar los puntos terminales de las máquinas origen y destino. El campo de longitud UDP incluye la cabecera de 8 bytes y los datos. La suma de comprobación UDP incluye la misma pseudocabecera de formato, la cabecera UDP, y los datos, rellenados con una cantidad par de bytes de ser necesario.

Esta suma es opcional, y se almacena como 0 si no se calcula. Inutilizarla seria absurdo, a menos que la cantidad de los datos no importe, por ejemplo, voz digitalizada.

UDP no admite numeración de los datagramas, factor que, sumado a que tampoco utiliza señales de confirmación de entrega, hace que la garantía de que un paquete llegue a su destino sea mucho menor que si se usa TCP. Esto también origina que los datagramas pueden llegar duplicados y/o desordenados a su destino. Por estos motivos el control de envío de datagramas, si existe, debe ser implementado por las aplicaciones que usan UDP como medio de transporte de datos, al igual que el reeensamble de los mensajes entrantes.

Es por ello un protocolo del tipo best-effort (máximo esfuerzo), porque hace lo que puede para transmitir los datagramas hacia la aplicación, pero no puede garantizar que la aplicación los reciba.

Tampoco utiliza mecanismos de detección de errores. Cuando se detecta un error en un datagrama, en lugar de entregarlo a la aplicación destino, se descarta.

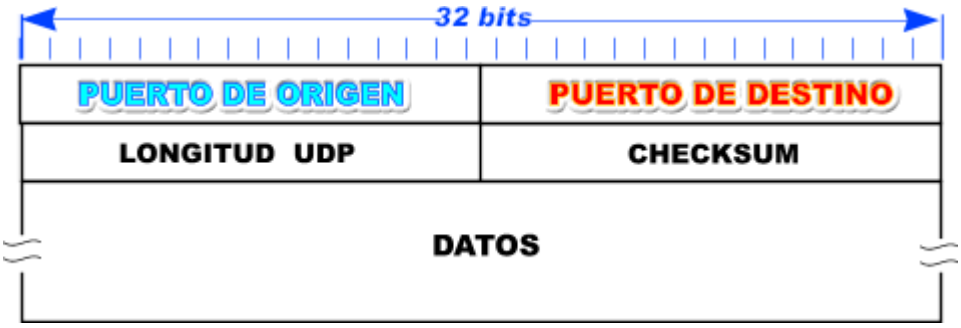
Cuando una aplicación envía datos a través de UDP, éstos llegan al otro extremo como una unidad. Por ejemplo, si una aplicación escribe 5 veces en el puerto UDP, la aplicación al otro extremo hará 5 lecturas del puerto UDP. Además, el tamaño de cada escritura será igual que el tamaño de las lecturas.

El Protocolo de datagramas de usuario (UDP) es un estándar TCP/IP que está definido en RFC 768, "User Datagram Protocol (UDP)". Algunos programas utilizan UDP en lugar de TCP para el transporte de datos rápido, compacto y no confiable entre hosts TCP/IP.

UDP proporciona un servicio de datagramas sin conexión que ofrece entrega de mejor esfuerzo, lo que significa que UDP no garantiza la entrega ni comprueba la secuencia de los datagramas.

Un host de origen que necesita comunicación confiable debe utilizar TCP o un programa que proporcione sus propios servicios de secuencia y confirmación.

Los mensajes UDP están encapsulados y se envían en datagramas IP, como se muestra en la siguiente ilustración.



Puertos UDP

Los puertos UDP proporcionan una ubicación para enviar y recibir mensajes UDP. Un puerto UDP funciona como una única cola de mensajes que recibe todos los datagramas destinados al programa especificado mediante cada número de puerto del protocolo. Es decir, los programas basados en UDP pueden recibir varios mensajes a la vez.

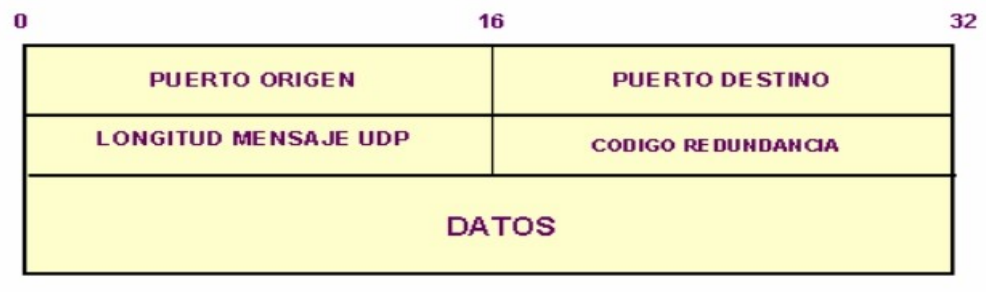
El lado de servidor de cada programa que utiliza UDP atiende los mensajes que llegan a su número de puerto conocido. Todos los números de puerto de servidor UDP inferiores a 1.024 (y algunos números superiores) están reservados y registrados por la Autoridad de números asignados de Internet (*IANA, Internet Assigned Numbers Authority*).

Cada puerto de servidor UDP se identifica mediante un número de puerto conocido o reservado. En la siguiente tabla se muestra una lista parcial de los números de puerto de servidor UDP conocidos que utilizan programas basados en UDP estándar.

Número de puerto UDP	Descripción
53	Consultas de nombres DNS
69	Protocolo trivial de transferencia de archivos (TFTP)

137	Servicio de nombres NetBIOS
138	Servicio de datagramas NetBIOS
161	Protocolo simple de administración de redes (SNMP)
520	Protocolo de información de enrutamiento (RIP -Routing Information Protocol)

Formato Mensaje UDP



- Puerto UDP de origen (16 bits, opcional). Número de puerto de la máquina origen.
- Puerto UDP de destino (16 bits). Número de puerto de la máquina destino.
- Longitud del mensaje UDP (16 bits). Especifica la longitud medida en bytes del mensaje UDP incluyendo la cabecera. La longitud mínima es de 8 bytes.
- Suma de verificación UDP (16 bits, opcional). Suma de comprobación de errores del mensaje. Para su cálculo se utiliza una pseudo-cabecera que también incluye las direcciones IP origen y destino. Para conocer estos datos, el protocolo UDP debe interactuar con el protocolo IP.
- Datos. Aquí viajan los datos que se envían las aplicaciones. Los mismos datos que envía la aplicación origen son recibidos por la aplicación destino después de atravesar toda la Red de redes.

LAS CAPAS DE UDP/IP

Recordemos que el protocolo DNS es el que nos permite utilizar las famosas URLs en lugar de direcciones IP. Es decir, nos permite escribir en nuestro navegador http://www.google.com en lugar de tener que escribir http://216.239.39.99, que es la dirección IP de Google.

Para conseguir esto, existen repartidos por el mundo una serie de servidores encargados de traducir URLs a IPs, e IPs a URLs. Nuestros PCs se comunicarán con alguno de estos servidores cada vez que quieran utilizar una URL, para obtener así su IP correspondiente. Esta comunicación se lleva a cabo a través del protocolo DNS.

Cuando escribimos en nuestro navegador una URL, por ejemplo http://redtauros.com, nuestro sistema enviará una consulta DNS a un servidor, indicando en la consulta el nombre que desea traducir (en este

caso redtauros.com , ya que el prefijo http:// es sólo una indicación al navegador sobre el protocolo a utilizar, pero no forma parte del nombre que deseamos traducir).

El servidor DNS nos enviará una respuesta que contendrá la IP correspondiente a ese nombre.

Gracias a esto, a continuación nuestro navegador podrá acceder a la máquina que contiene la página Web que deseamos visitar, ya que sólo puede existir una comunicación directa entre dos máquinas si cada una conoce la dirección IP de la otra.

Ahora vamos a pensar un poco en cómo se podría conseguir todo este mecanismo del DNS, en el cual un cliente solicita un nombre a un servidor, y el servidor le responde con la IP correspondiente. ¿Qué problemas se nos presentan a la hora de llevar a cabo este proceso aparentemente tan sencillo?

- En primer lugar, por supuesto, hay que conseguir que ambas máquinas (cliente y servidor) tengan una conexión física, ya sea por cables, por radio, o por cualquier otro medio físico que les permita establecer una comunicación bidireccional.
- En segundo lugar, sabiendo que en Internet todas las máquinas están conectadas entre sí mediante una compleja red de cables y conexiones inalámbricas, es lógico pensar que será necesario conocer el camino a recorrer en toda esa maraña de cables para enlazar ambas máquinas entre sí.
- En tercer lugar, el cliente necesitará conocer la dirección IP del servidor DNS, ya que sólo conociendo la dirección IP de una máquina puedes acceder a ella a través de Internet.
- En cuarto lugar, tiene que existir algún mecanismo que le indique al servidor que la consulta que le estamos haciendo es una consulta DNS, y no de cualquier otro tipo. Por ejemplo, el servidor DNS podría ser al mismo tiempo un servidor Web, y un servidor de correo electrónico. Por tanto, tiene que existir un mecanismo que le permita distinguir qué clientes solicitan servicios DNS, cuáles solicitan servicios Web, y cuáles solicitan servicios de correo electrónico.

A grandes rasgos, son cuatro los problemas que hemos encontrado para conseguir llevar a cabo esta comunicación. Y, por supuesto, no es coincidencia que sean cuatro las capas de protocolos utilizadas en una comunicación UDP: *capa física, capa de enlace, capa de red, y capa de transporte*.

Si no fuese gracias a la existencia de estas 4 capas diferenciadas, el protocolo DNS debería encargarse por sí sólo de solucionar todos estos problemas. Es decir, el protocolo DNS debería tener sus propias conexiones físicas entre máquinas, sus mecanismos para encontrar un camino entre todas las máquinas que están conectadas simultáneamente, sus propias direcciones IP, y sus propios mecanismos para diferenciarse de otros servicios (como la Web o el correo electrónico).

Esto convertiría al aparentemente sencillo protocolo DNS en un sistema de una complejidad inabarcable, y lo mismo ocurriría con cualquier otro protocolo que tuviese que lidiar él solito con todos los problemas existentes en una comunicación.

Vamos a ver entonces cómo se reparte el trabajo de la comunicación para permitir que el protocolo DNS se abstraiga de todo lo que no sea su misión directa.

Empezamos escribiendo una url en nuestro navegador: http://redtauros.com/site En primer lugar, nuestro navegador quitará la parte de la URL que no corresponda al nombre, que es: redtauros.com/site

Teniendo ya el nombre, nuestro sistema construye un paquete que contiene la consulta DNS.

UDP y TCP

En general, las diferencias en cómo entregan los datos UDP y TCP son similares a las diferencias entre una llamada telefónica y una tarjeta postal. TCP funciona como una llamada telefónica, ya que comprueba que el destino está disponible y preparado para la comunicación. UDP funciona como una tarjeta postal: los mensajes son pequeños y la entrega es probable, pero no siempre está garantizada.

Normalmente, utilizan UDP los programas que transmiten pequeñas cantidades de datos a la vez o que tienen requisitos de tiempo real. En estas situaciones, las capacidades de carga pequeña y multidifusión de UDP (por ejemplo, un datagrama, muchos destinatarios) resultan más apropiadas que TCP.

UDP es notablemente diferente de los servicios y características que proporciona TCP. En la siguiente tabla se comparan las diferencias en el modo de administrar la comunicación TCP/IP según se utilice UDP o TCP para el transporte de datos.

UDP	**TCP**

Servicio sin conexión; no se establece una sesión entre los hosts.	Servicio orientado a la conexión; se establece una sesión entre los hosts.
UDP no garantiza ni confirma la entrega, y no secuencia los datos.	TCP garantiza la entrega mediante el uso de confirmaciones y la entrega secuenciada de datos.
Los programas que utilizan UDP son responsables de proporcionar la confiabilidad necesaria para el transporte de datos.	Los programas que utilizan TCP proporcionan la seguridad del transporte de datos confiable.
UDP es rápido, tiene requisitos de carga pequeños y puede admitir la comunicación punto a punto y de un punto a varios puntos.	TCP es más lento, tiene requisitos de carga mayores y sólo admite la comunicación punto a punto.

UDP y TCP utilizan puertos para identificar las comunicaciones para cada programa TCP/IP.