

Redes de computadoras en L^AT_EX

Nelson Castro

June 24, 2018

0.1 Capa de transporte

La capa de transporte es responsable de la transferencia de extremo a extremo. La capa de transporte incluye también las siguientes funciones:

- Permite aplicaciones múltiples para comunicarse en la red al mismo tiempo que en un dispositivo sencillo.
- Asegura que, si es necesario, la aplicación correcta reciba todos los datos de forma confiable y en orden.
- Emplea mecanismos de manejo de errores.

La capa de transporte permite la segmentación de datos y brinda el control necesario para reensamblar las partes dentro de los distintos streams de comunicación. Las responsabilidades principales que debe cumplir son:

0.1.1 Rastreo de conversaciones individuales

Cualquier host puede tener múltiples aplicaciones que se comunican a través de la red. Cada una de estas aplicaciones se comunicará con una o más aplicaciones en hosts remotos. Es responsabilidad de la capa de transporte mantener los streams de comunicación múltiple entre estas aplicaciones.

0.1.2 Segmentación de datos

Los protocolos de la capa de transporte describen los servicios que segmentan estos datos de la capa de aplicación. Esto incluye la encapsulación necesaria en cada sección de datos.

0.1.3 Re-ensamble de segmentos

Los protocolos en la capa de transporte describen cómo se utiliza la información del encabezado de la capa para reensamblar las partes de los datos en streams para pasarlos a la capa de aplicación.

Segmentación y reensamblaje: Divide y vencerás

Resultaría poco práctico enviar todos estos datos en una sola gran sección. No puede transmitirse ningún otro tráfico de la red mientras se envían estos datos. Una gran sección de datos puede tardar minutos y hasta horas en enviarse.

Además, si hubiera algún error, el archivo de datos completo se perdería o tendría que ser reenviado. Los dispositivos de red no cuentan con que ser reenviado. Los dispositivos de red no cuentan con buffers de memoria lo suficientemente grandes como para almacenar esa cantidad de datos durante la transmisión o recepción.

Dividir los datos de la aplicación en partes asegura que éstos se transmitan dentro de los límites de los medios y que se puedan multiplexar en el medio.

Segmentación diferente para el manejo de TCP y UDP

Aunque los servicios de UDP restrean también las conversaciones entre las aplicaciones, no están preocupados por el orden en que se transmite la información o por mantener una conexión. No existe número de secuencia en el encabezado UDP.

0.1.4 Identificación de aplicaciones

Para pasar streams de datos a las aplicaciones adecuadas, la capa de transporte debe identificar la aplicación meta. Para lograr esto, la capa de transporte asigna un identificador a la aplicación. Los protocolos TCP/IP denominan a este identificador número de puerto. Este número de puerto se utiliza en el encabezado de la capa de transporte para indicar que aplicación se asocia a que parte.

0.1.5 Multiplexación de conversación

Puede haber aplicaciones o servicios que se ejecutan en cada host de la red. A cada una de estas aplicaciones o servicios se les asigna una dirección conocida como puerto, de manera que la capa de transporte determina que aplicación o servicio se identifican los datos.

0.1.6 Establecimiento de una sesión

Estas conexiones preparan las aplicaciones para que se comuniquen entre sí antes de que se transmitan los datos. Dentro de estas sesiones, se pueden gestionar de cerca los datos para la comunicación entre dos aplicaciones.

0.1.7 Entrega confiable

La capa de transporte puede asegurar que todas las partes alcancen su destino haciendo que el dispositivo origen retransmita todos los datos perdidos.

0.1.8 Entrega en el mismo orden

La capa de transporte puede asegurar que los mismos se reensamblen en el orden adecuado.

0.1.9 Control de flujo

Los host de la red cuentan con recursos limitados, como memoria o ancho de banda. Cuando la capa de transporte advierte que estos recursos están sobrecargados, algunos protocolos pueden solicitar que la aplicación reduzca la velocidad de flujo de datos.

El control de flujo puede evitar la pérdida de segmentos en la red y evitar la necesidad de la retransmisión. Las aplicaciones generan datos que se envían desde una aplicación a otra sin tener en cuenta el tipo de host destino, el tipo de medios sobre los que los datos deben viajar, el paso tomado por los datos, la congestión en un enlace o el tamaño de la red. Su responsabilidad es entregar los datos al dispositivo adecuado. La capa de transporte clasifica entonces estas piezas antes de enviarlas a la aplicación adecuada. Hay múltiples protocolos de la capa de transporte debido a que las aplicaciones tienen diferentes requisitos.

Algunos protocolos proporcionan sólo las funciones básicas para enviar de forma eficiente partes de datos entre las aplicaciones adecuadas. Estos tipos de protocolos son útiles par aplicaciones cuyos datos son sensibles a retrasos. Otros protocolos de la capa de transporte describen los procesos que proporcionan características adicionales, como asegurar un envío confiable entre las aplicaciones. Si bien estas funciones adicionales proveen una comunicación

más sólida entre aplicaciones de la capa de transporte, representan la necesidad de utilizar recursos adicionales y generan un mayor número de demandas en la red.

0.1.10 Separación de comunicaciones múltiples

En la cpaa de transporte, cada conjunto de piezas particulares que flute entre la aplicación de origen y la de destino se conoce como conversación.

Para identificar cada segmento de datos, la capa de transporte añade a la pieza un encabezado que contiene datos binarios. Este encabezado contiene campos de bits. Son los valores de estos campos los que permiten que los destinos protocolos de la capa de transporte lleven a cabo las diversas funciones.

0.1.11 Soporte de comunicación confiable

Un protocolo de la capa de transporte puede implementar un método para asegurar el envío confiable de datos. En términos de redes, confiabilidad significa asegurar que cada sección de datos que se envía al origen llegue al destino.

Esto requiere que los proceso de la capa de transporte en el origen de seguimiento a todas las partes de datos de cada conversación y retransmitan cualquier dato del cual el destino no acuso recibo. La capa de transporte del host de recepción también debe rastrear los datos a medida que se reciben y reconocer la recepción de los mismos. Estos procesos de confiabilidad generan un uso adicional de los recursos de la red debido al reconocimiento, rastreo y retransmisión.

En la capa de transporte, existen protocolos que especifican métodos para la entrega confiable, garantizada o de máximo esfuerzo. En el contexto de networking, el envío del mejor esfuerzo se conoce como poco confiable, porque no hay acuse de recibo de que los datos se recibieron en el destino.

0.1.12 Determinación de la necesidad de la confiabilidad

Las aplicaciones, tales como bases de datos, páginas web y correo electrónico, necesitan que todos los datos enviados lleguen al destino en su condición original para que los datos sean útiles. Se diseñan para utilizar un protocolo de

capa de transporte que implemente la confiabilidad. Los gastos de red adicionales se consideran necesarios para estas aplicaciones.

Si uno o dos segmentos de un stream de vídeo no llegan al destino, sólo generará una interrupción momentánea en el stream. Esto puede representar distorsión en la imagen pero quizás ni sea advertido por el usuario.

La imagen en un streaming video se degradaría en gran medida si el dispositivo de destino tuvo que dar cuenta de los datos perdidos y demorar el stream mientras espera que lleguen. Es conveniente proporcionar la mejor imagen posible al momento en que llegan los segmentos y renunciar a la confiabilidad, estas aplicaciones pueden proveer verificación de errores y solicitudes de retransmisión.

0.1.13 TCP y UDP

Protocolo de datagramas de usuario(UDP)

UDP es un protocolo simple, No orientado a conexión. Cuenta con la ventaja de proveer la entrega de datos sin utilizar muchos recursos. Este protocolo de la capa de transporte envía datagramas como "mejor intento".

Las aplicaciones que utilizan UDP incluyen:

- Sistema de nombres de dominio (DNS)
- Streaming video
- Voz sobre IP (VoIP)

0.1.14 Protocolo de control de transmisión (TCP)

TCP es un protocolo orientado a la conexión, utiliza recursos adicionales para garantizar funciones. Las funciones adicionales especificadas por TCP están en el mismo orden de entrega, son de entrega confiable y de control de flujo. Cada segmento de TCP posee 20 bytes de carga en el encabezado que encapsulan los datos de la capa de aplicación, mientras que cada segmento UDP solo posee 8 bytes de carga.

Aplicaciones que utilizan TCP son:

- Exploradores Web
- Correo electrónico

- Transferencias de archivos

TCP: Cómo generar conversaciones confiables

La diferencia clave entre TCP y UDP es la confiabilidad. La confiabilidad de la comunicación TCP se lleva a cabo utilizando sesiones orientadas a la conexión. Antes de que un host que utiliza TCP envíe datos a otro host, la capa de transporte inicia un proceso para crear una conexión con el destino. Esta conexión permite el rastreo de una sesión, o stream de comunicación entre los hosts. Este proceso asegura que cada host tenga conocimiento de la comunicación y se prepare. Una conversación completa de TCP necesita establecer una sesión entre los host de ambas direcciones.

Después de establecer una sesión, el destino envía un acuse de recibo al origen por los segmentos que recibe. Estos acuses de recibo forman la base de la confiabilidad dentro de la sesión TCP. Cuando el origen recibe un acuse de recibo, reconoce que los datos se han entregado con éxito y puede dejar de rastrearlos. Si el origen no recibe el acuse de recibo dentro de un tiempo predeterminado, retransmite esos datos al destino.

Parte de la carga adicional que genera el uso de TCP es el tráfico de la red generado por los acuses de recibo y las retransmisiones. El establecimiento de las sesiones genera cargas en forma de segmentos adicionales intercambiados. Hay también sobrecarga en los hosts individuales creada por la necesidad de mantener un registro de los segmentos que esperan un acuse de recibo y por el proceso de retransmisión. Esta confiabilidad se logra al tener archivos en el segmento TCP, cada uno con su función específica.

0.1.15 Direccionamiento del puerto

En el encabezado de cada segmento o datagrama, hay un puerto de origen y uno de destino. El número de puerto de origen es el número para esta comunicación asociado con la aplicación que origina la comunicación en el host local. El número de puerto de destino es el número para esta comunicación asociado con la aplicación de destino que origina la comunicación en el host local. Los números de puerto se asignan de distintas maneras, en virtud de si el mensaje es una solicitud o una respuesta. Mientras que los procesos del servidor tienen números estáticos asignados, los clientes eligen de forma dinámica un número de puerto 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 se ejecuta en el host remoto. El software de cliente debe conocer el número de puerto asociado con el proceso del servidor en el host remoto.

El término socket hace referencia sólo a la combinación exclusiva de dirección IP y número de puerto. Un par de sockets, que consiste en las direcciones IP de origen y destino y los números de puertos, también es exclusivo e identifica la conversación entre los dos hosts.

Hay diversos tipos de números de puerto:

- Puertos bien conocidos (0 al 1023)
- Puertos registrados (1024 al 49151)
- Puertos dinámicos o privados (números 49152 a 65535)