Castillo Martínez Leonel Jafet

TCP (Transmission Control Protocol)

Responde de manera breve cada una de las siguientes preguntas:

1. ¿Por qué se dice que TCP es un protocolo orientado a flujo?

Porque permite al proceso emisor entregar datos como un flujo de bytes y permite al proceso receptor obtener datos como un flujo de bytes.

2. ¿Qué nombre recibe la PDU de TCP?

Segmento.

3. ¿Por qué TCP se considera un protocolo orientado a conexión?

Porque cuando un proceso en el sitio A quiere enviar y recibir datos de otro proceso en el sitio B;

- Los dos TCP establecen una conexión virtual entre ellos.
- Los datos son intercambiados en ambas direcciones.
- La conexión se termina.

4. ¿Por qué TCP se considera un protocolo confiable?

Porque verifica la seguridad y la llegada correcta de los datos, además de implementar un mecanismo de control de errores.

5. ¿En qué consiste el acuerdo de las tres vías (three-ways hadshaking)?

En TCP, una transmisión orientada a conexión requiere tres fases, la primera de estas fases es el *establecimiento de la conexión*, llamado **acuerdo de las tres vías.**

Consiste en los siguientes tres pasos:

- El cliente envía el primer segmento, en el cual solamente la bandera SYN está establecida.
- El servidor envía el segundo segmento, un segmento con las banderas SYN y ACK.
- El cliente envía el tercer segmento, solamente con un segmento ACK. El cual confirma la recepción del segundo segmento con la bandera ACK y el campo de número de confirmación.

6. ¿Qué significa que TCP use confirmaciones acumulativas?

Que se reporta la recepción del último byte consecutivo; no se reportan los bytes que han llegado fuera de orden, ni se informa sobre los segmentos duplicados.

7. ¿Qué estrategias se pueden utilizar para mitigar el ataque de inundaciones SYN?

Tener impuesto un límite de solicitudes de conexión durante un periodo de tiempo especificado. Otros tratan de filtrar datagramas que vienen de una dirección fuente no deseada. O bien, posponer la asignación de recursos hasta que el servidor pueda verificar que la solicitud de la conexión viene de una dirección IP válida, usando lo que se conoce como *cookie.*

8. ¿Cuáles son las diferencias entre la ventana emisora utilizada por TCP y la del protocolo de repetición selectiva?

- La naturaleza de las entidades relacionadas con la ventana.
  - La ventana en RS enumera los paquetes.
  - La ventana en TCP enumera los bytes.
- En algunas implementaciones TCP puede almacenar los datos recibidos de un proceso y enviarlos después, pero se asume que el TCP emisor es capaz de enviar los segmentos de datos tan pronto como los recibe de su proceso.
- El protocolo teórico RS puede usar varios temporizadores para cada paquete, mientras que TCP usa solamente un temporizador.

9. ¿Cuáles son las diferencias entre la ventana receptora utilizada por TCP y la del protocolo de repetición selectiva?

- TCP permite al proceso receptor extraer datos a su propio paso. Por lo que, el tamaño de la ventana receptora es siempre más pequeña o igual a la del tamaño del buffer.
- En RS, las confirmaciones son utilizadas de manera selectiva, mientras quez en TCP, el principal mecanismo de confirmación es una confirmación acumulativa que anuncia el próximo byte esperado a recibir, y las nuevas versiones de TCP usan confirmaciones acumulativas y selectivas.

10. ¿Por qué la ventana en el emisor TCP puede contraerse?

Ya que la ventana del receptor no puede contraerse, si éste define un valor para *rwnd* que resulta en la contracción de la ventana del emisor.

11. ¿En qué consiste el síndrome de la ventana tonta en el emisor cómo se soluciona?

En el envío de datos en segmentos muy pequeños, lo cual reduce la eficiencia de la operación de la ventana deslizante cuando el programa de aplicación emisor crea datos lentamente o el programa de aplicación receptor consume datos lentamente, o ambos.

12. ¿En qué consiste el síndrome de la ventana tonta en el receptor cómo se soluciona?

Cuando se está sirviendo a un programa de aplicación que consume los datos lentamente, por ejemplo, 1 byte a la vez.

13. ¿Qué incluye el control de errores en TCP?

Mecanismos para detectar y reenviar segmentos dañados, reenviar segmentos perdidos, ordenar segmentos fuera de orden hasta que los segmentos perdidos lleguen, y detectar y descartas segmentos duplicados.

14. ¿Qué herramientas utiliza TCP para implementar el control de errores?

Suma de verificación, confirmaciones y expiraciones de temporizador.

15. ¿Cuáles son las reglas que utiliza un receptor TCP para generar una confirmación?

a) Cuando el extremo A envía un segmento de datos al segmento B, debe incluir (piggyback) una confirmación que indique el próximo número de secuencia esperado por el receptor.

b) Cuando el receptor no tiene datos que enviar y recibe un segmento en orden (con el número de secuencia esperado) y el segmento previo ya ha sido confirmado, el receptor retrasa el envío de un segmento ACK hasta que otro segmento llegue o hasta que un periodo de tiempo haya pasado.
c) Cuando un segmento llega con un número de secuencia que es esperado por el receptor, y los segmentos previos en orden no han sido confirmados, el receptor inmediatamente enviará un segmento ACK.
d) Cuando un segmento llega con un número de secuencia fuera de orden que es más alto que el esperado, el receptor inmediatamente envía un segmento de ACK anunciando el número de secuencia del próximo segmento esperado.
e) Cuando un segmento perdido llega, el receptor envía un segmento ACK para anunciar el próximo número de secuencia esperado.
f) Si llega un segmento duplicado, el receptor descarta el segmento, pero inmediatamente envía una confirmación indicando el próximo segmento en orden esperado.

16. ¿En qué consiste cada una de las estrategias utilizada por TCP para implementar el control de congestión?

Para manejar la congestión, y con ayuda de la ventana de congestión, se utiliza una política general que está basada en tres fases:

- Inicio lento: El tamaño de la ventana de congestión se incrementa exponencialmente hasta que se alcanza un umbral. Cuando el tamaño de la ventana de congestión alcanza el umbral de inicio lento, el inicio lento para y la fase
- Evitar congestión: Incrementa la ventana aditivamente en lugar de exponencialmente, cada vez que la “ventana” completa de segmentos se confirma, el tamaño de la ventana de congestión se incrementa en 1. Si ocurre congestión, el tamaño de la ventana debe ser decrementado.
- Detección de congestión: El tamaño del umbral es disminuido a la mitad (decremento multiplicativo).

17. ¿Cuántos temporizadores utiliza TCP y para qué se utiliza cada uno de ellos?

- Retransmisión: Se utiliza para retransmitir los segmentos perdidos.
- Persistencia: Para hacer frente a anuncios de tamaño de ventana cero.
- Keepalive: Se usa en algunas implementaciones para prevenir una conexión inactiva larga.
- TIME-WAIT: Se establece con un tiempo de descanso de dos veces el MSL, el cual es el tiempo de vida máximo que un segmento puede existir en Internet antes de eliminarlo, hay dos razones del estado y temporizador:
    - Para evitar que no se pueda cerrar una conexión entre un cliente y un servidor TCP derivado del hecho de que el cliente nunca reciba el segmento FIN reenviado por el servidor, y que éste no reciba el ACK final.
    - Para prevenir una reencarnación.

18. ¿En qué consiste y para que se utiliza el algoritmo de Karn?

No considera el tiempo de viaje redondo de un segmento retransmitido en el cálculo de RTTs. Tampoco actualiza el valor de RTTs hasta que envía un segmento y recibe una confirmación sin necesidad de retransmisión.

Se utiliza para resolver la ambigüedad ocasionada cuando un emisor TCP recibe una confirmación para un segmento retransmitido y no sabe si la confirmación es para el segmento original o para el retransmitido.

19. ¿Para qué se utiliza la opción de factor de escala de ventana?

Para incrementar la ventana cuando este no sea suficiente, por ejemplo, cuando los datos están viajando a través de un canal largo con un gran ancho de banda.

20. ¿Para qué se utilizan las opciones SACK y SACK permitido?

Se utilizan para tener una mejor idea de qué segmentos están realmente perdidos y cuales han llegado fuera de orden y así mejorar el desempeño de la confirmación acumulativa.

La opción de SACK permitido es usada solamente durante el establecimiento de la conexión. La opción SACK de longitud variable es usada solamente durante la transferencia de datos si ambos extremos están de acuerdo.