Tarea N° 3

Entregue las preguntas marcadas con *

"Dime y lo olvido, enséñame y lo recuerdo, involúcrame y lo aprendo." Proverbio Chino.

En esta tarea usted analizará y experimentará con el comportamiento de TCP. Lo hará analizando al secuencia de segmentos TCP enviados y recibidos al transferir un archivo de 150KB desde su computador a un servidor remoto. En esta tarea usted estudiará, entre otros, el uso de números de secuencia y de acuse de recibo para proveer confiabilidad en la transferencia de datos en TCP; verá el algoritmo de control de congestión en acción (partida lenta y abolición de congestión); y verá el mecanismo de TCP de control de flujo.

En esta taarea estudiaremos el comportamiento de TCP al subir un archivo desde su computador a un servidor WEB en Internet. Haga los siguientes pasos:

a) Baje a su computador el archivo de texto Alice in Wonderland desde (éste será uploaded luego) :

http://gaia.cs.umass.edu/wireshark-labs/alice.txt.

b) Usando su browser visite la página:

http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html

En esta página seleccione "Choose File" y seleccione el archivo alice.txt previamente bajado. No presione "upload" aún.

c) Ejecute Wireshark y comience la captura de paquetes, enseguida vuelva a su browser y presione "Upload alice.txt file". Así la captura tomará la transferencia de este archivo desde su computador al servidor gaia.cs.umass.edu. Una vez que el archivo es recibido por el servidor, la página web muestra un mensaje de éxito.

d) Ahora detenga la captura de paquetes en Wireshark.

e) Ingrese "tcp" en la ventana de filtro y dé una mirada a su captura. Observe el Handshake de TCP (SYN) y el requerimiento POST de HTTP. Dependiendo de su versión de Wireshark usted podría ver una serie de mensajes "HTTP Continuation" siendo enviados desde su computador. No existe ningún mensaje HTTP Continuation, ésta en la manera de Wireshark de indicar que hay múltiples segmentos TCP usados para transferir un único mensaje HTTP. En versiones más recientes de Wireshark usted verá "[TCP segment of a reassembled PDU]" para indicar que este segmento TCP contiene datos pertenecientes a un mensaje de protocolo de capa superior (HTTP en este caso). También usted debería notar los segmentos TCP ACKs retornados desde el servidor a su computador.

Responda:

A) ¿Cuál es la IP y puerto de su computador usados en la conexión POST?

* B) ¿Cuál es la IP y puerto del servidor usados en la conexión POST?

Si Wireshark está configurado para listar paquetes de protocolo HTTP, Wireshark muestra el mensaje POST después que se han enviado todos los segmentos de datos de este mensaje. Aparece después y se muestra completo en la ventana de contenido del paquete. Para ver el orden en que realmente salieron los paquetes es mejor desactivar la visualización del protocolo HTTTP.

Para focalizarnos en TCP, cambie la opción para el listado de paquetes capturados de Wireshark, para esto seleccione Analyze->Enabled Protocols y luego quite la selección de la caja HTTP y seleccione OK.

C) ¿Cuál es el número de secuencia del mensaje TCP SYN enviado por su computador? ¿Qué valores tienen los bits A, S, y F del encabezado TCP en este mensaje? Muestre imagen wireshark usada para obtener respuestas.

Nota: Fijarse que Wireshark, para facilitar lectura, muestra los números de secuencia y ACK en términos relativos al primer número de secuencia. Para obtener el valor real enviado en el paquete debe ver la ventana contenido del paquete.

* D) ¿Cuál es el número de secuencia del mensaje TCP SYNACK enviado por el servidor hacia su computador? ¿Qué valores tienen los bits A, S, y F del encabezado TCP en ese mensaje? ¿Cuál es el tamaño del buffer de recepción de la conexión TCP en el servidor WEB? Muestre imagen wireshark usada para obtener respuestas.

Nota: Notar que el campo para el tamaño de la ventana de recepción debe multiplicarse por el valor enviado en el campo opción para conseguir el tamaño real del buffer. Recuerde la explicación dada en clases, 2^16 bytes era adecuado para los computadores cuando la Internet comenzó, ahora es un campo pequeño para las memorias de los host actuales, por ello se usa el campo multiplicador enviado en opciones.

* E) Muestre la gráfica hecha por Wireshark para los RTT de la conexión TCP POST. Para ello seleccione un TCP segment en la ventana de listado de paquetes capturados que son enviados desde el cliente al servidor. Luego seleccione: Statistics->TCP Stream Graph- >Round Trip Time Graph.

* F) ¿Puede usted identificar casos donde el receptor envíe acuse de recibo cada dos segmentos? Muestre campos de dos ACKs sucesivos que lo llevan a esa conclusión. ¿Cuántos datos son confirmados en los primeros 5 ACKs enviados desde el servidor WEB?

* G) Haga un gráfico de números de secuencia versus tiempo para los segmentos TCP del POST. Para ello selecciones los segmentos TCP y luego selecciones: Statistics->TCP Stream Graph-> Time-Sequence-Graph(Stevens). Haga dos comentarios sobre la diferencias que usted observe entre los datos medidos y el modelo idealizado de TCP visto en clase (o el texto).