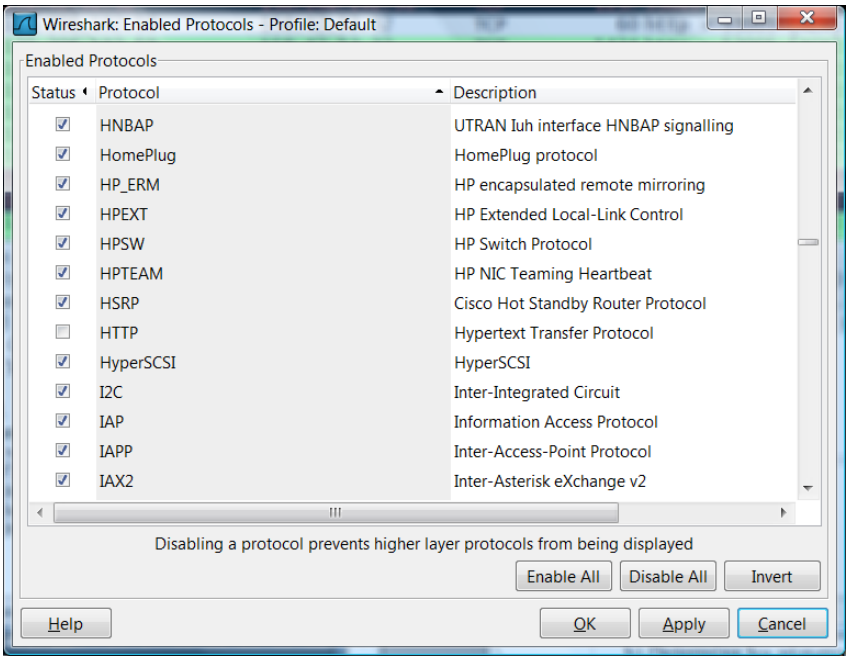
TCP

Sesión 7: Análisis del funcionamiento de TCP

Lectura previa: Tema 4 del curso, repaso del funcionamiento del analizador Wireshark

En esta sesión vamos a realizar un estudio del funcionamiento de TCP mediante la captura y posterior análisis de transferencias con el analizador Wireshark.

En primer lugar, como el objetivo principal de la práctica es analizar el funcionamiento de TCP sin preocuparnos de los datos contenidos en los segmentos transferidos, le diremos al analizador que únicamente deseamos visualizar las estructura de los segmentos TCP. Si recordáis las primeras prácticas del curso, vimos transferencias HTTP (como vamos a realizar ahora) de una forma cómoda ya que el analizador interpretaba los datos de los segmentos TCP y nos indicaba en pantalla si se estaba realizando, por ejemplo, un GET en vez de tener que buscar en la zona de datos del segmento TCP dicho método. Ahora no nos interesa ver los GET, POST,... es decir, no nos interesa interpretar el protocolo que se usa en la zona de datos, sino únicamente los segmentos según el formato que hemos visto en clase que sigue TCP. Para ello, en la opción *Analyze* → *Enabled Protocols*, quitaremos la marca a este protocolo. De esta forma, aunque en un segmento TCP se transporte HTTP, el analizador no interpretará el protocolo HTTP y mostrará únicamente el segmento TCP que lo lleva.



• **Ejercicio 1**: Realizar una captura mediante el analizador Wireshark de una conexión a la página web de la Universidad: http://www.upv.es/index-es.html. Puede ser muy útil establecer un filtro (*port* 80 desde el menú *Capture* → Options o *tcp.port == 80* desde el filtro de la ventana principal) para facilitar la interpretación de los datos.

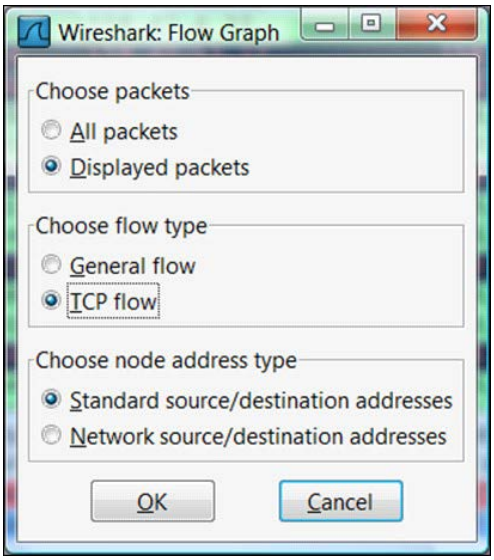
a) Analiza el establecimiento de la conexión e identifica el protocolo a tres fases. ¿Qué MSS se elige para realizar la transferencia? ¿Qué otras opciones establece cada uno de los extremos?

b) Determina los números de secuencia de cada extremo. Diferencia entre el número relativo que pone el analizador para realizar un seguimiento más cómodo, del real que aparece en el segmento (pulsa sobre el número de secuencia relativo y verás el número real que figura en el segmento transferido en la ventana inferior de la ventana principal -contenido en hexadecimal-). De igual forma, seleccionado el segmento TCP en la ventana intermedia, con el botón derecho del ratón

(Protocol preferences) podemos indicarle que no queremos usar números relativos (aunque es más cómodo seguir usando en el resto de la práctica los números relativos).

c) Seleccionando el primer flujo TCP (*Follow TCP Stream),* analiza el cierre de la conexión. ¿Quién toma la iniciativa? ¿Es un cierre en tres o cuatro fases? Comprueba lo mismo para los flujos siguientes (recuerda eliminar el filtro que establece la opción *Follow TCP Stream*)

d) Vuelve a seleccionar el primer flujo TCP. A continuación ejecuta la opción *Statistics → Flow Graph* seleccionando el flujo TCP como se muestra en la figura siguiente:



Interpreta lo que estás viendo.

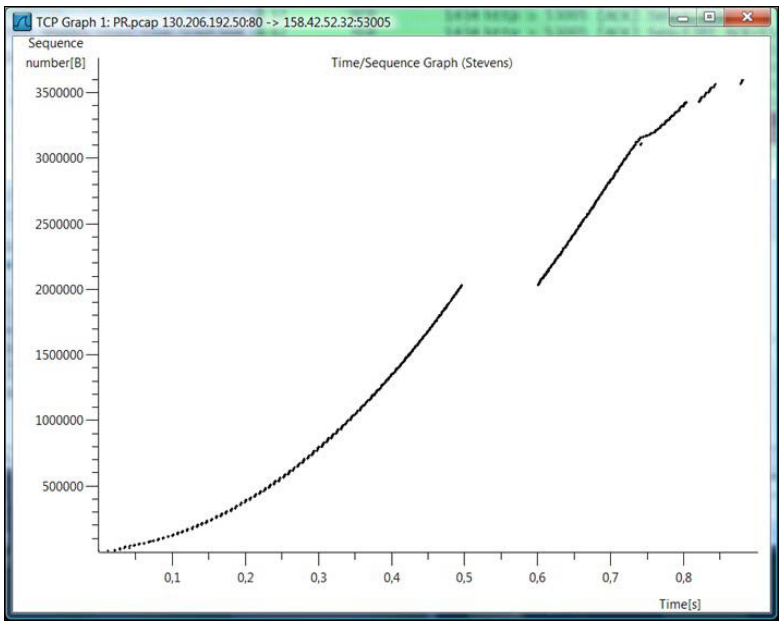
- ¿Cuál es la evolución de los ACKs en relación con el envío de los segmentos? ¿Hay un ACK tras dos envíos desde el servidor? En caso de no haberlo ¿por qué?
- ¿Se usan ACKs acumulativos? ¿Cómo lo aprecias en la captura?

e) Selecciona cualquier de las tramas con origen en el servidor y destino tu máquina y ejecuta la opción *Statistics->TCP Stream Graph → Round Trip*. ¿Qué información estamos viendo? ¿Cuál es el RTT aproximado de esta conexión?

f) Repite el apartado c) para una conexión con http://www.redes.upv.es. ¿Ves el cierre de la conexión? En caso negativo repite esta experiencia cerrando el navegador antes de finalizar la captura con el analizador.

- **Ejercicio 2:** Realiza una captura mediante el analizador Wireshark de una conexión al puerto 81 del servidor web de la Universidad: http://www.upv.es:81. Ten cuidado si tienes algún filtro activo y establécelo al puerto 81. Analiza la captura realizada. ¿Cómo se indica que no hay un servicio en ese puerto? ¿Cómo se cierra la conexión? ¿Qué le contesta tu navegador? ¿Vuelve a intentar tu navegador la conexión? En caso afirmativo ¿cuántas veces?
- **Ejercicio 3:** Descarga el fichero pr.pcap que está en Poliformat. Este fichero es una captura de una transferencia de un documento pdf de 3.5 MB aproximadamente, desde un servidor con IP: 130.206.192.50 a un cliente 158.42.52.32. Cárgalo en el analizador Wireshark.

a) Selecciona un mensaje enviado por el servidor (130.206.192.50) hacia el cliente (158.42.52.32) y ejecuta la opción *Statistics → TCP Stream Graph → Time-Sequence Graph (Stevens).* Debes obtener una gráfica como la que se muestra a continuación:



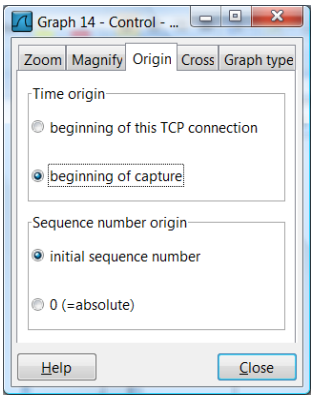
¿Cómo interpretas a grandes líneas esta gráfica? ¿Qué cosas se aprecian ? ¿Hay algo curioso o inquietante? *(Nota: se puede realizar un* zoom *con el botón central del ratón y desplazarte con el botón derecho)*

b) Centrémonos ahora en la parte central de la gráfica, en ese *hueco "misterioso"*. Encuentra una justificación para el mismo. ¿Cómo has llegado a esa conclusión? Puedes ayudarte también con la opción *Statistics → Flow Graph* que has usado antes.

c) Vamos ahora a los instantes de tiempo [0.74..0.755]. Realiza un *zoom* de la gráfica para ver qué está pasando en esa zona. ¿Qué está ocurriendo? Relaciona los conceptos con lo que hemos visto en clase sobre: segmentos perdidos, retransmisiones (rápidas o no), ACKs retardados.....

- Desplázate en la ventana principal, por las tramas, a esos instantes de tiempo. ¿Por qué hay 36 ACKs duplicados antes de que el analizador nos muestre o interprete una retransmisión rápida? ¿Se producirán *timeouts?* Para reflexionar sobre esto te puede ayudar una gráfica del tipo *Statistics → TCP Stream Graph → Round Trip.*¿Cómo evoluciona el RTT en ese período de tiempo? ¿qué puede haber pasado?

(Nota: para que la información se relacione correctamente entre todas las gráficas pon en la ventana de control del gráfico la opción T*ime origin: beginning of capture* en todos los casos. Se muestra en la figura siguiente)



d) Teniendo que el fichero pdf llegó en su totalidad, ¿por qué no se ve en la captura el cierre de la conexión?