Herramientas para el análisis de comunicaciones TCP/UDP

Arquitectura de Redes de Ordenadores
Arquitectura de Internet

Departamento de Teoría de la Señal y Comunicaciones y
Sistemas Telemáticos y Computación

Abril 2017

Contenidos

netstat

- La herramienta `netstat` muestra el listado de comunicaciones activas en una máquina, en concreto, muestra detalles de las conexiones TCP y comunicaciones UDP que hay establecidas en una determinada máquina.
- `netstat` mostrará la siguiente información para las comunicaciones activas:

```
pc1:~# netstat -una
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
```

  - La columna `Proto` indica el protocolo utilizado, en nuestro caso visualizaremos comunicaciones TCP y UDP.
  - La columna `Local Address` muestra la dirección IP local de la máquina donde se esperan recibir datos y el número de puerto.
  - En la columna `Foreign Address` muestra la dirección IP y puerto de las máquina remota con la que se ha establecido una comunicación.
  - Las columnas `Recv-Q` (`receiving queue`) y `Send-Q` (`sending queue`) muestran la cantidad de bytes que hay almacenados en los buffers locales reservados para la recepción de datos y emisión de datos de este servidor.
  - La columna `State` indicará el estado de la comunicación.

netstat: comunicaciones UDP (I)

- Para visualizar las comunicaciones UDP activas:

```
pc1:~# netstat -una
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 0.0.0.0:7777            0.0.0.0:*
```

  - El resultado de ejecutar este comando muestra un servidor UDP esperando recibir conexiones de clientes en el puerto 7777.
  - La columna `Local Address` muestra la dirección 0.0.0.0 que indica que se esperan recibir comunicaciones UDP en cualquiera de las direcciones IP configuradas actualmente en la máquina local.
  - En la columna `Foreign Address` se mostrarán las direcciones IP y puertos de las máquinas clientes remotos que se conecten con este servidor. Actualmente no hay ninguna.
  - Las columnas `Recv-Q` y `Send-Q` muestran que no hay datos almacenados en los buffers.

netstat: comunicaciones UDP (II)

- Para visualizar las comunicaciones UDP activas:

```
pc1:~# netstat -una
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 11.0.0.1:7777           11.0.0.2:32768          ESTABLISHED
```

  - El resultado de ejecutar este comando muestra una comunicación UDP entre la dirección IP local 11.0.0.1 y puerto 7777 y la dirección IP remota 11.0.0.2 y puerto 32768.
  - Las columnas `Recv-Q` y `Send-Q` muestran que no hay datos almacenados en los buffers.

netstat: comunicaciones TCP (I)

- Para visualizar las comunicaciones UDP activas:

```
pc1:~# netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:7777            0.0.0.0:*               LISTEN
```

  - El resultado de ejecutar este comando muestra un servidor TCP esperando recibir conexiones de clientes en el puerto 7777.
  - La columna `Local Address` muestra la dirección 0.0.0.0 que indica que se esperan recibir comunicaciones UDP en cualquiera de las direcciones IP configuradas actualmente en la máquina local.
  - En la columna `Foreign Address` se mostrarán las direcciones IP y puertos de las máquinas clientes remotos que se conecten con este servidor. Actualmente no hay ninguna.
  - Las columnas `Recv-Q` y `Send-Q` muestran que no hay datos almacenados en los buffers.

netstat: comunicaciones TCP (II)

- Para visualizar las comunicaciones UDP activas:

```
pc1:~# netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 11.0.0.1:7777           11.0.0.2:33715          ESTABLISHED
```

  - El resultado de ejecutar este comando muestra una comunicación TCP entre la dirección IP local 11.0.0.1 y puerto 7777 y la dirección IP remota 11.0.0.2 y puerto 33715.
  - Las columnas `Recv-Q` y `Send-Q` muestran que no hay datos almacenados en los buffers.

Contenidos

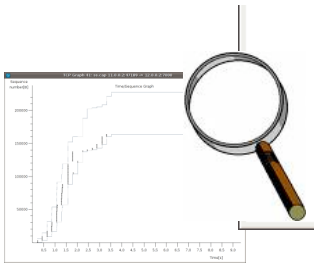
Gráfica de *tcptrace* dentro de Wireshark

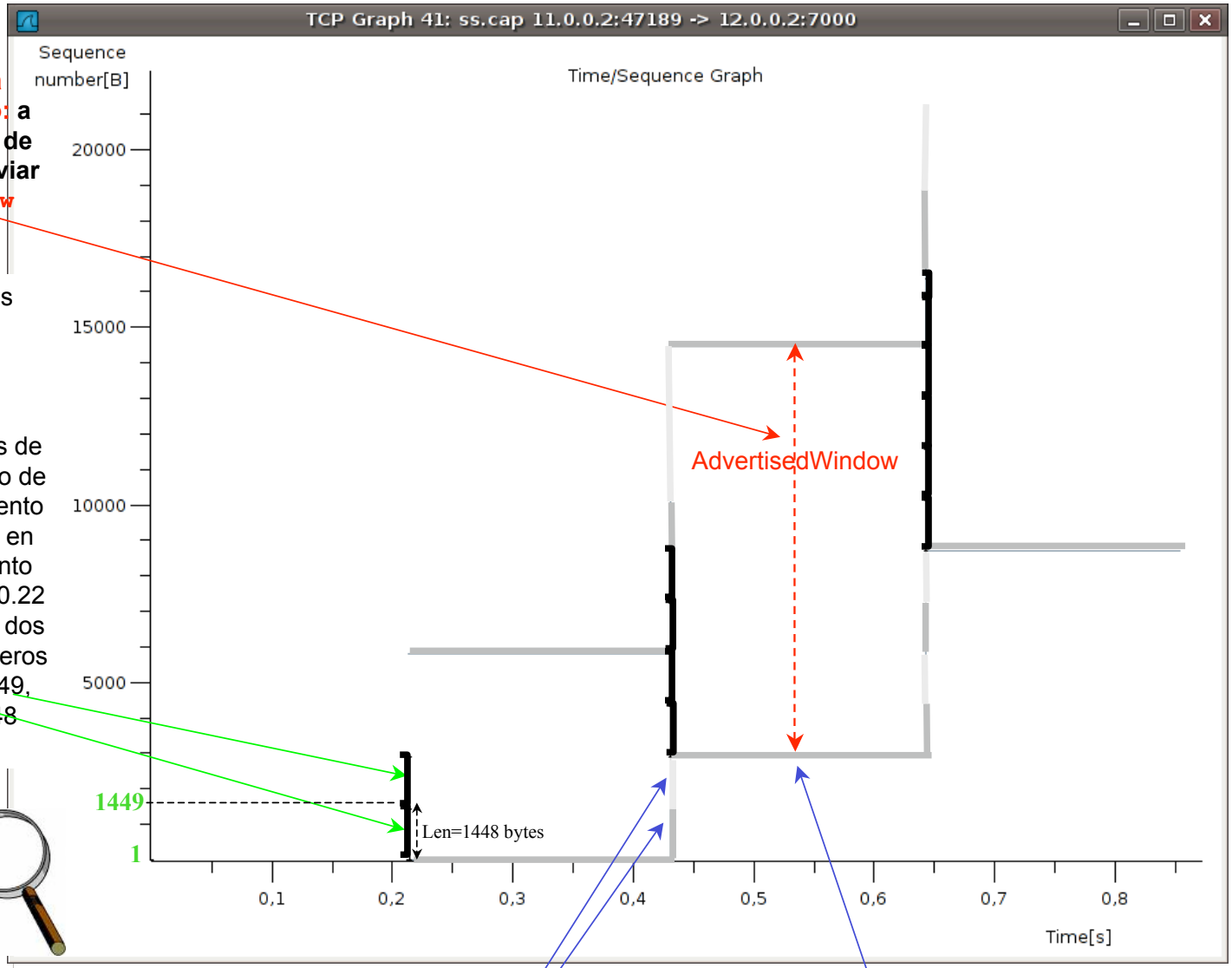
- En Wireshark, además de mirar el contenido de los paquetes de una conexión TCP, puede verse en una gráfica la **evolución del envío de datos y recepción de acks respecto al tiempo**.
- Wireshark permite mostrar varios tipos de gráficas de una conexión TCP: Nosotros utilizaremos la gráfica de *tcptrace*.
- Como una conexión TCP permite el envío de datos en ambos sentidos, se pueden visualizar 2 gráficas de *tcptrace* diferentes: las correspondientes a cada sentido de la comunicación.
- Para ver en Wireshark la gráfica de *tcptrace* de uno de los sentidos de una conexión TCP es necesario:
  - Cargar el fichero de una captura que contenga los paquetes de una conexión TCP.
  - Seleccionar un segmento de la conexión del sentido de la comunicación que queremos analizar (si el segmento seleccionado va del proceso A al proceso B, la gráfica que se mostrará será la correspondiente al envío de datos de A a B).
  - Seleccionar en el menú de Wireshark:
    Statistics→TCP Stream Graph→Time-Sequence Graph (tcptrace)

Ejemplo

Ventana anunciada por el otro extremo: a partir del último nº de ACK se pueden enviar `AdvertisedWindow` bytes

Segmentos verticales negros: **segmentos TCP de datos enviados**. Cada segmento ocupa un conjunto de números de secuencia: el número de secuencia del segmento TCP más la longitud en bytes de ese segmento TCP. En el instante 0.22 segundos se envían dos segmentos con números de secuencia 1 y 1449, cuya longitud es 1448 bytes.





Segmentos verticales grises: **segmentos TCP de ACK** recibidos

Línea inferior gris claro: **último nº de ACK recibido**

Acciones sobre la gráfica *tcptrace*

- **Click central**: zoom in
- **MAYS + Click central**: zoom out
- **Arrastrar con el botón derecho**: desplazar el gráfico (útil si se ha hecho "zoom in")
- **ESPACIO**: activa/desactiva una cruz para ayudar a ver sobre los ejes la posición del ratón.
- **Click izquierdo sobre un segmento**: seleccionar el paquete concreto en la lista de paquetes de Wireshark.
- **CTRL + arrastrar con el botón derecho**: lupa
- **s**: Alterna entre números de secuencia relativos y absolutos, sólo si está desactivada la opción Edit→Preferences→Protocols→TCP→Relative sequence numbers and window scaling.