Ingeniería Técnica de Telecomunicación,
Especialidad Telemática

Prácticas de Laboratorio de Redes y
Servicios de Comunicaciones

Práctica 3. La herramienta de monitorización Ethereal

María Victoria Bueno Delgado
Pablo Pavón Mariño

INDICE

3.1 Introducción

Las herramientas de monitorización son indispensables para el trabajo de gestión y mantenimiento de un red. Permiten descubrir y analizar el tráfico que circula por la misma, para p.e. detectar fallos en protocolos o dispositivos que generen tráfico caóticamente.

En esta asignatura los alumnos estudiarán distintos protocolos y tecnologías, y se hace indispensable el dominio de al menos una herramienta de monitorización que les ayude en cada momento a resolver las prácticas. Didácticamente, es muy interesante ya que ofrece a los alumnos la posibilidad de observar realmente los conceptos que estudian en teoría.

Esta práctica pretende iniciar al alumno en la herramienta de libre distribución *Ethereal*, que ha sido seleccionada para este laboratorio.
La práctica consistirá en un conjunto de ejemplos de utilización de la herramienta en la captura y análisis de distintos tipos de tráfico (conexiones *FTP*, *Telnet*, *HTTP*, comandos ping…). La documentación asociada a esta práctica es:

- Los apuntes de la asignatura (protocolos ICMP, UDP y TCP).
- Se ha generado un manual de resumen con las funcionalidades principales de *Ethereal*. en el enlace http://ait.upct.es/asignaturas/lrys/ManualEthereal.doc
- La documentación completa de la herramienta (y el software completo, de libre distribución) se puede encontrar en el *site* http://www.ethereal.com.

3.2 Proceso de captura de tráfico

Arranque el ordenador bajo el sistema operativo Windows. **Debe arrancar como administrador para que no haya problemas**. La contraseña se la proporcionará el profesor. de la asignatura. Abra la herramienta *Ethereal*, que se encuentra instalada en su PC. A través del menú *Capture* acceda al menú de captura. Indique brevemente la funcionalidad de las opciones siguientes especificadas más abajo. Para ello, lea el manual con atención, consulte el manual *on-line* de *Ethereal*, y haga las pruebas oportunas. NO INICIE LA CAPTURA TODAVÍA.

- Interface

- Capture File:file

- Capture packets in promiscuous mode

- Update list of packets in real time

- Enable MAC name resolution

- Enable network name resolution

- Enable transport name resolution

Inicie una captura de tráfico sobre la interfaz *Ethernet* de su PC, sin activar ninguna resolución automática de nombres. A continuación ejecute el comando *ping 192.168.6.254*. Después de unos 10 segundos, pare el comando anterior, y ejecute el comando *ping 212.128.44.34*. Después de unos 20 segundos, pare la captura. Guarde la captura en un fichero, dentro del directorio *Mis Documentos*, con el nombre *captura1.txt*. Para almacenar el fichero debe utilizar la opción *File-->Save*. ¿Qué tipos de fichero de captura están permitidos?.

Guarde el fichero con el formato *"libpcap (tcpdump, Ethereal, etc.)"*. Ahora abra el fichero con un editor de textos. ¿Sería posible manejar el fichero de captura con un procesador de textos?.

Ahora cierre la captura que tiene en pantalla (opción *File-->Close*) recupere el fichero de capturas almacenado. ¿Se ha recuperado toda la información?

3.3 Filtrado de tráfico

El fichero de capturas con el tráfico generado, incluye tramas de distintos tipos. Utilice el campo *Filter* situado en la parte inferior de la pantalla, para introducir condiciones de filtrado sobre el tráfico mostrado en la pantalla. Para introducir los filtros necesarios de las siguientes cuestiones deberá consultar el manual de Ethereal indicado en la introducción de estas prácticas.

- Indique el filtro necesario para quedarse únicamente con las tramas del protocolo *ARP*.

- Ídem para las tramas que NO sean *ARP*.

- Ídem para las tramas que sean del protocolo *IP*. ¿están incluidas las tramas que llevan mensajes *ICMP*?. ¿Por qué?

- Ídem para las tramas que encapsulen datagramas *IP* con dirección de origen la propia (PC del grupo de prácticas) y dirección destino *212.128.44.34*.

Elija una trama cualquiera generada por su PC. Observe los campos de su cabecera *Ethernet*. ¿Cuáles son esos campos?. ¿Que tipo de tarjeta *Ethernet* dispone en su PC (*Ethernet II* o *IEEE 802.3*)?.

Elija una trama de la captura, del protocolo *ICMP* con un mensaje *echo request*. Dibuje la encapsulación por protocolos de una trama de ese tipo. Indique el tamaño de las cabeceras de los protocolos, y muestre qué protocolos son transportados dentro de otros (debe seguir el mismo formato que el visto en teoría).

3.4 Protocolo ICMP. Herramienta ping y herramienta traceroute

De la captura anterior, elija una trama que transporte un mensaje *ICMP echo request*. ¿Qué campos tiene este mensaje *ICMP*? (escriba también el contenido de todos los campos, salvo el de datos). Indique los nombres de los campos de la cabecera *ICMP* en el mensaje *echo request,* tal y como los utiliza *Ethereal* (serán del tipo *icmp.????*).

Indique de la misma manera el nombre *Ethereal* de los campos de la cabecera de un mensaje *ICMP echo reply*. ¿Cuál es la utilidad del campo *Identifier* y *Sequence Number*?

La herramienta *traceroute ip_destino* (*tracert* en Windows) permite mostrar por pantalla cuál es la ruta que sigue un datagrama hacia su destino. Ejecute el comando Windows *tracert* y observe las opciones que permite. ¿Cuál es la utilidad de la opción -d?

Realice una captura con el resultado del comando *tracert -d 212.128.20.252*. Observando la captura, se da cuenta que el comando *tracert* está basado en mensajes *ICMP echo request*. Para ello, el comando inicialmente envía un mensaje de este tipo con el campo *TTL* de la cabecera *IP* a *1*. Este mensaje será descartado por el primer *router* al que llegue. ¿Por qué?. ¿Qué mensaje enviará al origen (escriba el campo *type* y *code* de este mensaje)?

El PC origen continúa enviando mensajes *echo request*, con el campo *TTL* de la cabecera *IP 2, 3, 4*... con lo que continúa conociendo los *routers* en el 2º salto, 3º salto... ¿Existe la seguridad de que la ruta obtenida sea única?. ¿Por qué?.

¿Cuándo se da por finalizado el envío de mensajes *echo request* incrementando el *TTL*?

La herramienta *netstat* de Windows y de Linux tiene numerosas opciones que permiten conocer aspectos del tráfico recibido y enviado por la máquina, conexiones *TCP* activas, tabla de encaminamiento... Por ello, puede ser de utilidad en operaciones de monitorización y mantenimiento. En un PC Windows como el utilizado en el laboratorio, ¿cuál es la utilidad de la opción *-s*?, ¿cuál es la diferencia con la opción *-es*?

Ejecute el comando *netstat -es* y observe los estadísticos que ahí se muestran. ¿Qué tipos de mensajes ICMP son los más frecuentes en su PC?. ¿A qué comandos que ha utilizado en esta práctica corresponden?. ¿Cuántos datagramas fragmentados ha transmitido?.

3.5 Protocolo ARP. Control de caché ARP. (Comando arp)

En un PC con Windows, es posible controlar la caché ARP (con entradas que asocian IP-MAC de la red Ethernet a la que se está conectado), utilizando el comando arp en una ventana MS-DOS. Observe las opciones incluidas dentro de ese comando. ¿Cuál es la opción que permite el borrado de entradas en la caché ARP?

Utilice esta opción para borrar la entrada de su caché con la dirección IP del servidor (192.168.6.254). Comience una captura en Ethereal, y ejecute el comando ping 192.168.6.254. Pare la captura. Ésta debe incluir la consulta ARP desde su PC preguntando por la MAC asociada al servidor. ¿Cuál es la razón de que se haya producido esta consulta?

Aplique el filtro de pantalla que permita quedarse únicamente con las consultas ARP generadas por su PC. Responda a las siguientes preguntas:

- ¿Cuál es ese filtro?

- ¿Cuáles son los campos del mensaje consulta ARP?

- ¿Los mensajes de respuesta ARP tiene los mismos campos que los mensajes de consulta?

- ¿Qué contenido hay en el campo dirección MAC destino de la cabecera Ethernet?. ¿Por qué?

Aplique el filtro de pantalla que permita quedarse únicamente con las respuestas ARP generadas por el servidor, con destino su PC.

- ¿Cuál es ese filtro?.

- ¿Qué campos tiene el mensaje respuesta ARP?.

Realice una captura de una situación donde se produzca una consulta ARP que no es contestada (por ejemplo, ping 192.168.6.100). ¿Qué tramas se transmiten y reciben?. ¿Se obtiene alguna respuesta?

3.6 Protocolo Telnet (sobre TCP)

La aplicación Telnet es una aplicación del tipo cliente-servidor. Esto quiere decir, que su funcionamiento está basado en dos aplicaciones distintas el cliente Telnet, y el servidor Telnet, que se comunican entre sí, a través de una red TCP/IP.

Un cliente Telnet que desea conectarse a un servidor Telnet, abre una conexión TCP con el servidor (indicando su dirección IP). El cliente Telnet debe simplemente enviar las pulsaciones de teclas del usuario hacia el servidor. El servidor Telnet debe abrir un intérprete de comandos (shell) en la máquina servidora. Este intérprete de comandos se alimenta con las pulsaciones enviadas por el cliente. Los comandos enviados por el cliente serán por tanto ejecutados en la máquina servidor EXACTAMENTE igual que si hubieran sido introducidos por un usuario sentado delante de esta máquina. El resultado (stdout y stderr) de estos comandos se

redirecciona hacia la conexión TCP con el cliente. Una vez llegan a este, la aplicación cliente Telnet muestra en pantalla este resultado.

Inicie una captura sobre la interfaz Ethernet de su máquina. A continuación, ejecute el comando telnet 192.168.6.254. Entre en la cuenta lrys, e introduzca la clave proporcionada por el profesor. A continuación ejecute el comando ls. Pare la captura y conteste a las siguientes preguntas:

- ¿Cuál es el tamaño de la cabecera TCP?

- ¿Cuál es el puerto TCP en la máquina cliente?

- ¿Cuál es el puerto TCP en al máquina servidor?

- ¿Cuál es el filtro más sencillo que permite quedarse con las tramas correspondientes a los mensajes telnet?

Una utilidad muy interesante proporcionada por Ethereal, es la posibilidad de obtener visualmente los datos intercambiados en una conexión TCP. Para ello, seleccione una trama que transporte una conexión TCP. A continuación, con el botón derecho, seleccione la opción Follow TCP Stream. Se mostrará en una ventana separada, los datos intercambiados en todos los segmentos de la conexión TCP a la que pertenece el segmento seleccionado. Los datos en un sentido y en otro se muestran en colores distintos. Observando los datos de la conexión TCP en la que está basada la aplicación Telnet indique:

- ¿Por qué las pulsaciones del cliente aparecen repetidas, en dos colores?

- ¿Transmite el protocolo *Telnet* la clave de la sesión en texto claro por la red?

- ¿Qué pulsaciones no son enviadas de vuelta hacia el cliente?

Responda a las siguientes cuestiones, fijándose en las tres tramas de establecimiento de conexión *TCP*, y el primer segmento con datos transmitido en cada sentido.

NOTA: Para entender este apartado es necesario que el alumno realice sobre papel un diagrama de flujo de la transmisión/recepción de la conexión *TCP* a realizar, mirando los apuntes de teoría.

También debe tener en cuenta que en el enunciado que se expone A" simboliza el extremo iniciador de la conexión TCP. "B" simboliza el extremo no iniciador de la conexión TCP.

- Campo *Sequence* de primer segmento de establecimiento de conexión:

- Campo *ACK* de segundo segmento de establecimiento de conexión:

- Campo *Sequence* de tercer segmento de establecimiento de conexión:

- Campo *Sequence* 1º segmento de datos sentido *A->B*:

- Campo *ACK* de primer segmento de establecimiento de conexión:

- Campo *Sequence* de segundo segmento de establecimiento de conexión:

- Campo *ACK* de tercer segmento de establecimiento de conexión:

- Campo *Sequence* 1º segmento de datos sentido *B->A*:

¿Tiene alguna relación el campo *Sequence* de los segmentos que viajan en un sentido con el campo *Sequence* de los segmentos que viajan en sentido contrario?

Para las mismas tramas del apartado anterior, observe la evolución del campo *Window Size* y conteste a las siguientes preguntas:

- ¿Cuál es el significado/utilidad de este campo?

- ¿Debe ser el mismo para ambos sentidos?

- ¿Puede un extremo variar el tamaño de la ventana de transmisión del otro extremo de una conexión TCP?

Para las mismas tramas del apartado anterior, observe la negociación del campo *Maximum Segment Size* (campo opciones de la cabecera TCP) y conteste a las siguientes preguntas:

- ¿En qué segmentos se produce esta negociación?

- ¿Qué valor aparece en cada sentido?

- ¿Cuál es el significado/utilidad de este campo?.

Elija una trama de la captura que incluya un mensaje *Telnet* con un solo *byte*, correspondiente a una pulsación de tecla. Escriba la encapsulación por protocolos de una trama de ese tipo. Indique el tamaño de las cabeceras de los protocolos, y muestre qué protocolos son transportados dentro de otros (el profesor de laboratorio le indicará la forma en que desea que especifique esta encapsulación). ¿Cuántos bytes son necesarios entre cabecera *TCP* e *IP* para transmitir este byte de datos?.

3.7 Protocolo DNS (sobre UDP)

El protocolo *DNS* (*Domain Name System*) permite traducir nombres de dominio (del tipo *www.upct.es*) a direcciones *IP*. Este servicio es proporcionado por un conjunto de servidores interconectados. Un cliente que desea realizar la traducción, tiene almacenada una lista de servidores *DNS* a los que plantear la consulta. Esta consulta se realiza bajo la forma de mensajes *UDP* dirigidos a un puerto *UDP* concreto del servidor. Cada una de ellas incluye un puerto *UDP* del cliente, donde el servidor debe enviar la respuesta.

Inicie una captura sobre la interfaz *Ethernet* de su máquina. A continuación, ejecute el comando *ping www.upct.es*. Este comando debe provocar una consulta *DNS* al servidor configurado en su PC.

- ¿Cuál es la dirección *IP* de su servidor?

- ¿Cuál es el puerto donde el servidor *DNS* recibe las consultas?.

Elija una trama de la captura que incluya un mensaje *DNS*. Escriba la encapsulación por protocolos de una trama de ese tipo. Indique el tamaño de las cabeceras de los protocolos, y muestre qué protocolos son transportados dentro de otros (el profesor de laboratorio le indicará la forma en que desea que especifique esta encapsulación).

3.8 Ejercicios propuestos

3.8.1 Protocolo HTTP

El protocolo *HTTP* (*Hypertext Transfer Protocol*, http://www.w3.org/Protocols) implica alrededor del 80% del tráfico en Internet. Se trata de nuevo de un protocolo cliente-servidor. La funcionalidad principal de los servidores *HTTP* es de almacén de ficheros HTML (Hypertext Markup Language, http://www.w3.org/MarkUp/), ficheros de sonido, imágenes, etc. Los clientes *HTTP* más habituales se encuentran integrados en programas navegadores (*Internet Explorer*, *Netscape Navigator*...). La consulta más habitual de un cliente *HTTP* es el comando *HTTP GET*, que solicita un fichero al servidor Web. Para ello, el cliente, abre una conexión *TCP* con un puerto *TCP* concreto de la máquina servidor, donde el proceso servidor web espera recibir las consultas. En el caso de encontrarse el fichero pedido, el servidor *HTTP* devuelve sobre la misma conexión *TCP* ese fichero. Posteriormente, en función de la versión del protocolo *HTTP* empleada por el cliente y el servidor, esta conexión *TCP* se cierra, o se mantiene abierta para futuras consultas desde el cliente al mismo servidor web.

Inicie una captura sobre la interfaz *Ethernet* de su máquina. A continuación, abra un navegador, y acceda a una página que no esté en la caché del navegador (www.yahoo.es, www.google.com, ...).

- ¿Cuál es el fichero pedido al servidor en el comando *HTTP GET*?
- ¿Cuál es la versión *HTTP* del mensaje consulta?
- ¿Cuál es la versión *HTTP* del mensaje respuesta?
- ¿Cuántos comandos *HTTP GET* provoca la inicial petición del fichero?
- ¿Se realizan todas sobre la misma consulta conexión *TCP*?.

Elija una trama de la captura que incluya un mensaje *HTTP*. Escriba la encapsulación por protocolos de una trama de ese tipo. Indique el tamaño de las cabeceras de los protocolos, y muestre qué protocolos son transportados dentro de otros (el profesor de laboratorio le indicará la forma en que desea que especifique esta encapsulación).

3.8.2 Protocolo FTP

El servicio FTP (File Transfer Protocol) permite la transferencia de archivos entre dos máquinas conectadas a una red TCP/IP. De nuevo, está basado en una arquitectura cliente-servidor, existiendo la aplicación cliente FTP, y la aplicación servidor FTP.
Un cliente FTP inicia una conexión con un servidor FTP, para iniciar una sesión de intercambio de archivos. Esta sesión está basada en una conexión TCP subyacente, iniciada por el cliente, a un puerto concreto de la máquina servidor. El proceso servidor FTP en esta máquina, espera recibir conexiones escuchando en ese puerto concreto. Sobre cada sesión, se inicia un proceso de autenticación, por la cual el cliente debe introducir un login y una password que le autentifique como usuario de la máquina servidor.

Después de este proceso, la funcionalidad principal de transferencia de archivos la dan las órdenes PUT (el cliente solicita enviar un fichero al servidor) y órdenes GET (el cliente solicita recibir un fichero del servidor). La transmisión de un fichero concreto se realiza sobre un conexión TCP creada al efecto, manteniéndose la conexión TCP inicial para el intercambio de comandos.

Inicie una captura sobre la interfaz Ethernet de su máquina. A continuación, abra el cilente FTP que trae instalado el Sistema Operativo Windows, llamado ftp, iniciando una sesión con el servidor FTP situado en la máquina 192.168.6.254 (o labit601.upct.es si está accediendo desde fuera de la universidad). Autentifíquese en la cuenta correspondiente a su grupo de prácticas (lrys). A continuación ejecute varios comandos como ls (muestra el contenido del directorio actual para esta sesión en el servidor FTP), pwd (muestra el directorio actual para esta sesión en el servidor FTP). Ejecute algunos comandos que supongan transferencia de ficheros, valiéndose del comando de ayuda help que proporciona el cliente FTP. Finalmente cierre la captura.

- ¿Cuál es el puerto TCP donde escucha el servidor FTP?

- ¿Es seguro el proceso de autenticación?. ¿Por qué?

Elija una trama de la captura que incluya un mensaje FTP. Escriba la encapsulación por protocolos de una trama de ese tipo. Indique el tamaño de las cabeceras de los protocolos, y muestre qué protocolos son transportados dentro de otros (el profesor de laboratorio le indicará la forma en que desea que especifique esta encapsulación).