PRACTICA SOBRE ANALIZADORES DE PROTOCOLOS

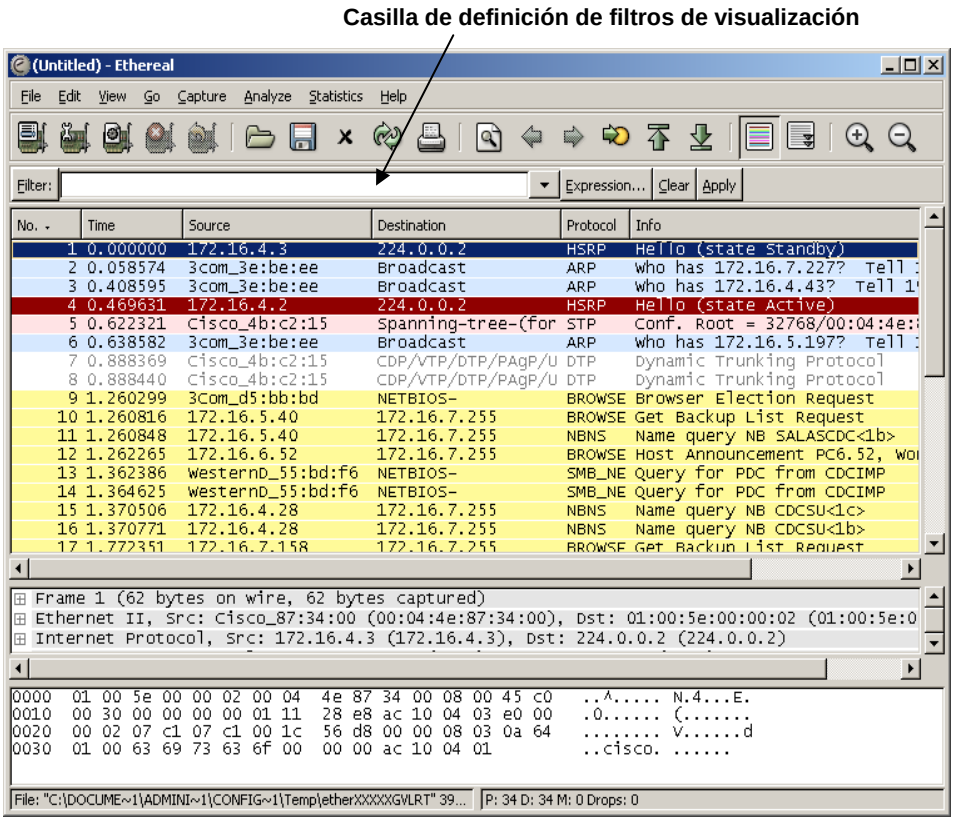
FUNDAMENTOS

Observará una ventana dividida en tres zonas; en cada una de ellas se muestran los paquetes capturados con distinto nivel de detalle:

- En la zona superior se presenta una línea por cada trama capturada con un resumen de sus contenidos: básicamente un número de secuencia, el instante de captura (por defecto, relativo al inicio de la captura), origen y destino, protocolo más alto de los detectados, e información relativa al protocolo concreto (por ejemplo, en caso de ser un paquete ICMP, puede identificar que se trata de una petición de eco). También es posible añadir otras columnas para visualizar más información de cada trama, aunque esto no será necesario en la práctica. Esta zona es el sitio indicado para observar qué secuencia de mensajes ha tenido lugar a grandes rasgos en una comunicación. Seleccionando una trama en esta sección superior se muestra información más detallada sobre la misma en las otras dos zonas.
- En la zona central se puede ver los valores de los campos de las distintas cabeceras detectadas en la trama, comenzando por la cabecera del nivel de enlace (por ejemplo, Ethernet), de una manera fácilmente legible, en forma de árbol de información. Éste es un buen sitio para buscar, por ejemplo, qué valor tiene el campo TTL de la cabecera IP de un datagrama determinado.
- Finalmente, en la zona inferior se ofrece el valor de cada octeto de la trama capturada, escrito en notación hexadecimal, lo que permite analizar los contenidos del paquete que no han sido decodificados en las secciones menos detalladas.

En caso de querer guardar una captura para analizarla más adelante, se puede hacer mediante el menú “File → Save As...”, pudiendo elegir entre guardar todas las tramas capturadas, sólo las que se muestran (por ejemplo, si se ha aplicado un filtro de visualización), o sólo las marcadas (en caso de haber marcado algunas tramas). También se puede seleccionar el formato del archivo (por ejemplo, .pcap). Posteriormente, mediante “File → Open...” es posible abrir cualquier archivo de captura previamente guardado.

La siguiente figura muestra el aspecto de la ventana principal del analizador:



Resumen de cada trama

Árbol de información de protocolos

Volcado hexadecimal de la trama

La documentación del analizador se encuentra accesible en “Help”. En ocasiones le será necesario conocer algunos parámetros de red de su propia máquina. Para ello, debe ejecutar la orden “**`ipconfig /all`**” en una ventana del “Símbolo del sistema”

Escriba los parámetros de red de su propia máquina:

- Dirección Ethernet (física):
- Dirección IP:
- Máscara de subred:
- Router (puerta de enlace) predeterminado:
- Servidor(es) de DNS predeterminado(s):

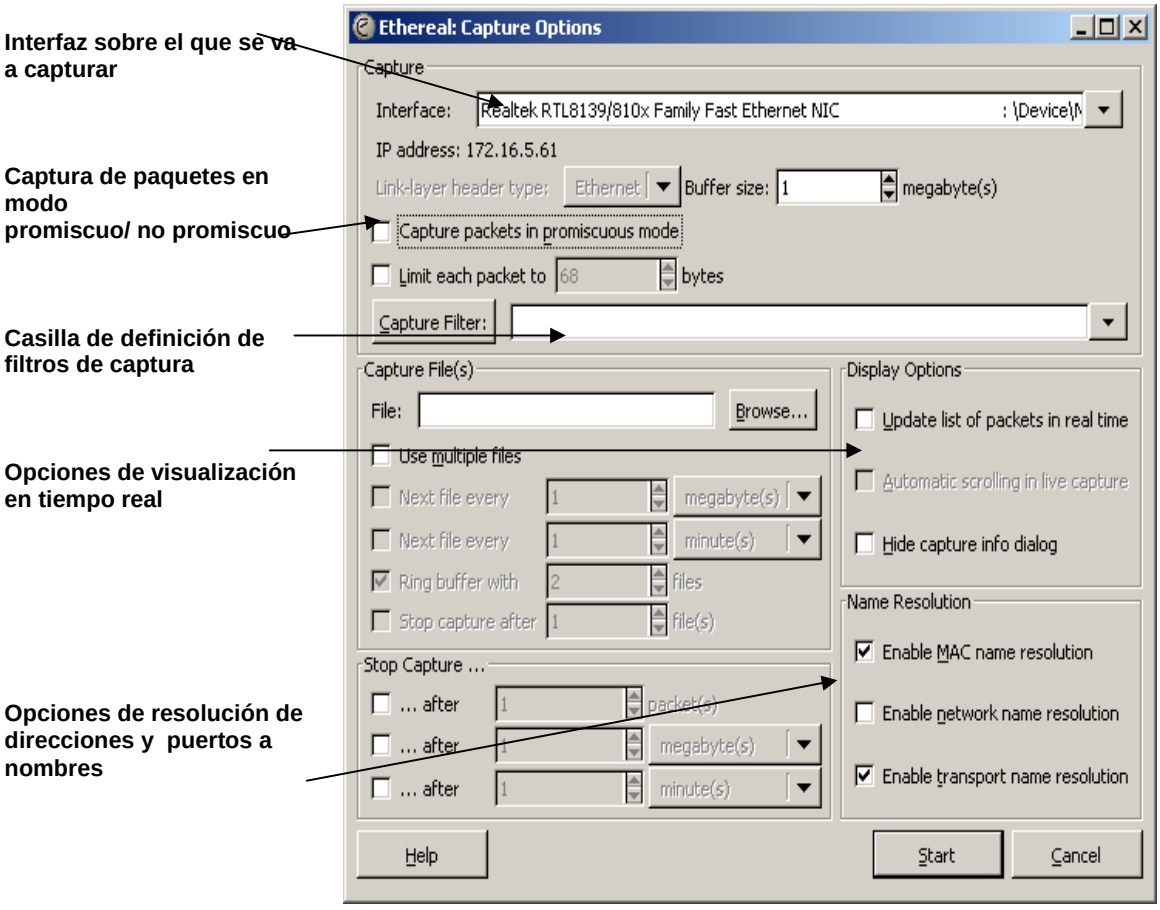
PING A UNA MÁQUINA INTERNA

En este apartado se va a analizar la secuencia de acciones que tiene lugar a consecuencia de la ejecución de la aplicación “ping” en una máquina, siendo el objetivo una máquina de la misma subred. Siga de manera ordenada los pasos que se detallan a continuación:

- Abra una ventana de opciones de captura en el analizador: menú “Capture→ Options...” y aplique las siguientes opciones (sin hacer clic en “OK” aún):

- Seleccione la interfaz sobre la que se desea capturar tráfico en la casilla “Interface”.
- Deshabilite “Capture packet in promiscuous mode” (de manera que sólo se capturará el tráfico Ethernet con origen o destino esta máquina, además del tráfico difusivo).
- Deshabilite igualmente “Enable MAC name resolution”, “Enable network name resolution” y “Enable transport name resolution”, de manera que el analizador no intente resolver direcciones a nombres (para evitar que se genere y capture más tráfico debido a esto).

En la figura que sigue se puede observar las posibilidades que ofrece la ventana de opciones de captura:



- Averigüe la dirección IP de una máquina de su misma subred que no sea el router (por ejemplo, desde una ventana de “Símbolo del sistema”, realice un ”ping [máquina]“ al nombre de la máquina elegida y anote la dirección IP que le corresponde).

Escriba la dirección IP de la máquina a la que hace el *ping*:

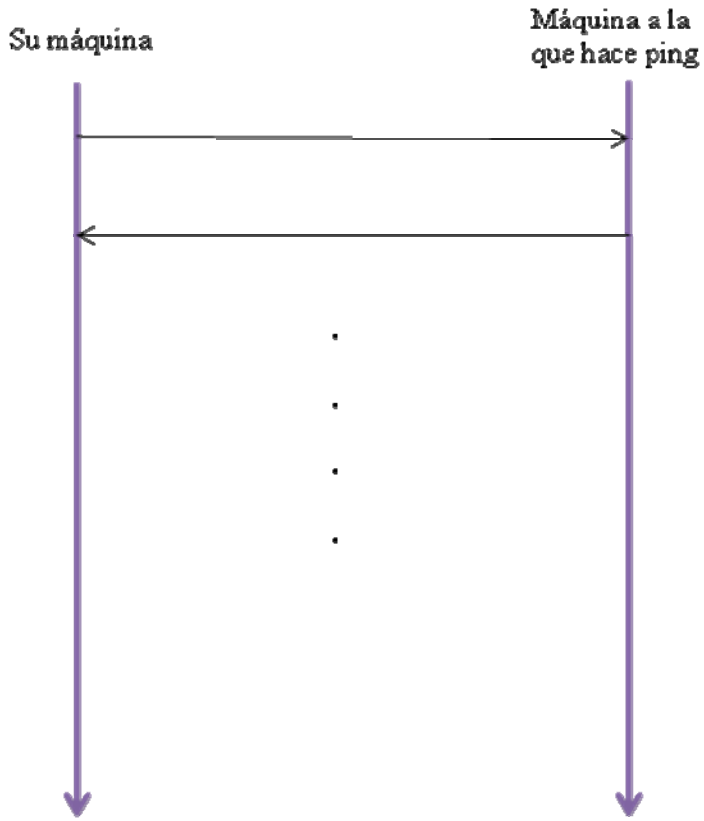
- Desde una ventana de “Símbolo del sistema” observe el estado de la tabla ARP de su PC. Para ello ejecute la orden “**`arp -a`**”. En caso de no estar vacía, borre todas las entradas presentes ejecutando la orden “**`arp -d`**”. Tras hacerlo, compruebe que efectivamente ahora la tabla está vacía (mediante “**`arp -a`**”).
- Arranque una captura en el analizador (botón “OK” de la ventana de opciones de captura). Se abrirá una nueva ventana de captura que muestra algunas estadísticas.
- Ejecute la orden “**`ping`**” a la dirección IP (no al nombre) de la máquina elegida y espere las cuatro respuestas.
- Pare la captura (botón “Stop” de la ventana de captura).
- Observe qué entradas han aparecido en su tabla de ARP. ¿Cuánto tiempo tardan en borrarse aproximadamente? (para averiguarlo, teclee cada pocos segundos la orden “**`arp -a`**” hasta que la(s) entrada(s) relacionada(s) con el ping hayan desaparecido).

Entradas que han aparecido en la tabla ARP, y por qué ha aparecido cada una:

Tiempo aproximado que tardan en borrarse la(s) entrada(s):

- Vaya a la ventana principal del analizador. De las tramas capturadas debe distinguir aquéllas que se han visto implicadas en todo el proceso (desde la ejecución de la orden “**`ping`**” en el PC hasta la recepción de las respuestas de la otra máquina; no serán únicamente paquetes ICMP). Dibuje en un diagrama las tramas que han intervenido, por su orden, junto con información sobre el protocolo al que pertenecen y su propósito. ¿Puede identificar qué información ha decidido introducir su máquina en el campo de datos de las peticiones de eco?

Tramas que han intervenido. Complete el diagrama con flechas que indiquen qué mensajes se han intercambiado las máquinas (incluyendo los protocolos y tipos de mensajes):



Información que su máquina pone en el campo de datos de las peticiones de eco:

PING A UNA MÁQUINA EXTERNA

En este caso se va a ejecutar un "**`ping`**" de manera muy similar al apartado anterior, pero a una máquina no perteneciente a la subred. Los pasos a seguir son, por este orden:

- Abra una ventana de opciones de captura en el analizador.
- Elija el nombre (no la dirección IP) de una máquina externa a su subred y realice un "**`ping`**" para asegurarse de que contesta al mismo (por ejemplo, puede intentarlo con www.us.es, o con cualquier otra).

- Asegúrese de vaciar a continuación la caché de DNS de la máquina, mediante la orden "**`ipconfig /flushdns`**".
- Asegúrese también de que la tabla ARP de su PC está vacía, de la manera descrita anteriormente.
- Arranque la captura.
- Ejecute la orden "**`ping`**" en su máquina utilizando el nombre (no la dirección IP) de la máquina elegida, y espere las cuatro respuestas.
- Pare la captura.
- ¿Qué entradas han aparecido en este caso en la tabla ARP?

Entradas que han aparecido en la tabla ARP, y por qué ha aparecido cada una:

- Vaya a la ventana principal del analizador y localice las diferencias entre los procedimientos seguidos en el caso anterior y éste. ¿A qué se deben?

Resuma y justifique las diferencias entre los acontecimientos que tienen lugar en este caso y en el caso del apartado anterior:

TRACEROUTE

Ahora se va a observar qué tipo de tramas ICMP entran en juego al ejecutar una aplicación típica de "tracert". Para ello, en este orden:

- Abra una ventana de opciones de captura en el analizador.
- Arranque una captura de tráfico.
- En una ventana de "Símbolo del sistema" ejecute la aplicación *traceroute* (la orden es "**`tracert`** ***`[dirección-o-nombre]`***" utilizando el nombre 'www.us.es'. Espere hasta su conclusión.
- Pare la captura.
- Vaya a la ventana principal del analizador y observe qué paquetes ICMP (no tenga en cuenta el resto de protocolos) se han generado como consecuencia de la ejecución del *traceroute*: entre qué máquinas, y de qué tipo. **Nota**: para esto puede resultar muy útil la utilización de un filtro de visualización, que selecciona, de entre todas las tramas capturadas,

aquéllas que coinciden con el criterio especificado (y no muestra el resto). En este caso, es útil seleccionar las tramas en las que se ha detectado el protocolo ICMP. Para ello, escriba en la casilla inferior izquierda (señalada por “Filter:”) la palabra “**`icmp`**” (sin las comillas) y aplique el filtro (“Apply”). Recuerde que para volver a visualizar todas las tramas debe pulsar el botón “Reset”.

Resumen de los paquetes ICMP observados (entre qué máquinas, de qué tipo):

- A la vista de los resultados, describa de manera resumida qué procedimiento utiliza la aplicación *traceroute* para ir averiguando el camino que siguen los datagramas desde la máquina en que se ejecuta la orden hasta el destino especificado.

Describa brevemente el procedimiento que utiliza la aplicación *traceroute*:

- Indique si con el comando *ping* se puede obtener la misma información de la ruta a un destino (al ejecutar "**`ping`**" en la ventana de "Símbolo del sistema" se proporcionan todos los parámetros que se pueden usar). En caso afirmativo, describa la forma en que se haría.

¿Existen otras posibilidades de obtener la ruta a una máquina, usando el comando *ping*? En caso afirmativo, descríbalas brevemente:

DESCARGA DE UN ARCHIVO

En este apartado se llevará a cabo la descarga de un archivo relativamente voluminoso con un navegador web para observar la velocidad de descarga en función del tiempo.

- Borre el filtro de visualización que definió en el apartado anterior.
- Abra una ventana de opciones de captura en el analizador.
- En este caso se va a definir un filtro de captura (casilla señalada por "Filter:" en la ventana de opciones de captura). Un filtro de captura, a diferencia de uno de visualización, impide que se capture el tráfico que no coincida con el criterio seleccionado. De esta manera, posteriormente sólo se podrá analizar el tráfico que este filtro haya permitido capturar. En este caso estamos interesados en capturar todo el tráfico TCP que tenga origen o destino (a nivel IP) en nuestra máquina. Para ello, en la casilla destinada al filtro de captura, teclee lo siguiente (sustituyendo la dirección de ejemplo "10.0.0.1" por la de su máquina):

```
ip proto \tcp and ip host 10.0.0.1
```

- Arranque una captura.
- Descargue con el navegador un archivo de algunos cientos de kilobytes para provocar el establecimiento de una conexión TCP de varios segundos de duración. Como sugerencias, puede probar con:
  - `http://www.ietf.org/iesg/1rfc_index.txt`

    - http://sunsite.utk.edu/ftp/usr-218-2/iesg/1rfc_index.txt
    - http://public.www.planetmirror.com/pub/ietf/iesg/1rfc_index.txt
- Cuando se haya terminado de descargar el archivo, pare la captura ("Stop").
- Localice entre los paquetes mostrados por pantalla uno que pertenezca a la conexión TCP por la que se ha transferido el archivo y que haya viajado desde el servidor a su ordenador. Si ha descargado un archivo de texto, uno de estos paquetes es fácilmente identificable observando cómo en los datos HTTP del paquete se puede leer parte del contenido del archivo (sección inferior de la ventana del analizador, parte derecha). Seleccione este paquete y posteriormente elija "Tools → TCP Stream Analysis → Throughput Graph" para representar la velocidad a la que ha sido transferido el archivo en cada intervalo. Observe la gráfica que se genera y conteste a las siguientes preguntas. ¿Es constante la velocidad a la que se ha transferido el archivo? De su conocimiento del funcionamiento del protocolo TCP, ¿puede explicar por qué lo es / no lo es?

¿Es constante la velocidad a la que se ha transferido el archivo? ¿Por qué?

DESCARGA DE UN ARCHIVO

En esta ocasión, mediante la captura de tráfico de navegación web, se introducirán algunas posibilidades del analizador a la hora de extraer estadísticas.

- Abra una ventana de opciones de captura en el analizador y mantenga el filtro de captura definido en el apartado anterior. Arranque una captura.
- Visite con un navegador web varias páginas de un portal de Internet.
- Pare la captura.
- Abra la herramienta que permite ver estadísticas de entrada/salida: "Tools → Statistics→ IO → IO-Stat". Observará una ventana con un gráfico que por defecto muestra, para todo el tráfico capturado, el número de tramas

por intervalo. Es posible mostrar varios gráficos con distintos colores, cada uno asociado a un filtro (de manera que se representen los valores del tráfico que coincide con el filtro), así como mostrar otros tipos de estadísticas (como número de octetos por intervalo, por ejemplo). Elija el modo avanzado de estadísticas mediante la selección de “advanced...” en el botón marcado como “Unit:”. (En caso de aparecer una ventana de aviso “Ethereal: Warning”, ignórela pulsando “OK”).

- Se quiere representar por separado el tráfico de entrada y el de salida de nuestra máquina. Para ello escriba, en las casillas de definición de los dos primeros filtros, lo siguiente (sustituya “10.0.0.1” por la dirección IP de su máquina):

  `ip.dst==10.0.0.1 and frame.pkt_len` (tráfico de entrada)
  `ip.src==10.0.0.1 and frame.pkt_len` (tráfico de salida)

- En el botón marcado como “Unit:” seleccione “bytes/tick”, de manera que se muestre en los gráficos la cantidad de octetos total transferida en cada sentido durante cada intervalo. **Nota**: como cabía esperar, al cambiar del modo “advanced” al de “bytes/tick”, desaparecen de la ventana las columnas dedicadas a la especificación de los cálculos avanzados.
- Active la visualización de los dos primeros gráficos y describa las diferencias encontradas entre ambos (¿hay un sentido en el que se observe una mayor transferencia de información en general? Si es así, ¿cuál? ¿por qué?). **Nota**: si lo precisa, puede ajustar los valores del tiempo de intervalo (“Tick Interval”) y el número de pixels que ocupa cada intervalo en el gráfico (“Pixels Per Tick”) de manera que observe los gráficos con una escala adecuada.

Respecto de la cantidad de octetos total intercambiada en cada sentido por intervalo: ¿hay un sentido en el que se observe una mayor transferencia de información en general?

Justifique la respuesta

- Cambie de nuevo el valor del botón “Unit:” a “frames/tick” de manera que se muestre el número de tramas transferidas en cada sentido durante cada intervalo, y visualice los dos primeros gráficos de nuevo. Comente lo que observa, comparándolo con el caso anterior.

Respecto del número de tramas transferidas en cada sentido por intervalo: ¿hay un sentido en el que en general se observe un mayor número de tramas?

Justifique la respuesta

- Vuelva al modo “advanced...” con el botón “Unit:” para realizar cálculos más avanzados. Los cálculos se harán sobre la longitud de las tramas capturadas en octetos. En consecuencia, en las dos primeras casillas dónde se escribe la variable sobre la que hacer los cálculos, teclee lo siguiente:

  `frame.pkt_len`

- En cuanto al tipo de cálculo, seleccione MAX (tamaño máximo de las tramas por intervalo” en ambos y visualice los dos gráficos. Repita esta operación seleccionando el cálculo AVG (tamaño medio de las tramas por intervalo). Comente las diferencias encontradas para ambos sentidos de transmisión y la explicación de las mismas.

Respecto de los tamaños máximo y medio de las tramas transferidas en cada sentido por intervalo: ¿hay un sentido en el que en general se observen tamaños mayores?

Justifique la respuesta