PRACTICA 3

Monitorización de redes mediante *Analyzer*

Justificación y objetivos.

La monitorización de redes resulta una herramienta fundamental en dos sentidos. Por un lado, permite apreciar de forma realista muchos de los conceptos fundamentales de las redes en general, y de los protocolos TCP/IP en particular (encapsulación, fragmentación, secuenciación de mensajes, etc). Por otro lado, permite realizar un diagnóstico muy preciso de las redes en funcionamiento, desde la detección de errores, la verificación de los mecanismos de seguridad y la evaluación de prestaciones de la red.

Es por ello que en esta práctica estudiaremos una herramienta gratuita de monitorización de redes, denominada *Analizer*, que trabaja sobre un interfaz de red denominado *WinPCap*. Es posible encontrar más información en la web http://analyzer.polito.it/

La monitorización de red, o captura de tramas, consiste en la obtención de todas las tramas que aparecen a nivel de LAN. Puesto que el medio de transmisión es, generalmente, una línea de difusión, esto permitirá observar la totalidad de las comunicaciones que tienen lugar a través de la misma, y por tanto resulta una herramienta muy potente, tanto desde el punto de vista positivo (diagnóstico de red) como el negativo (compromete la confidencialidad de las comunicaciones).

La cantidad de información obtenida de una monitorización es enorme. Por tanto, es necesario establecer unos **filtros** de aceptación, que permiten que las tramas no consideradas relevantes no se almacenen ni muestren al usuario.

Los objetivos de la presente práctica pueden resumirse en los siguientes:

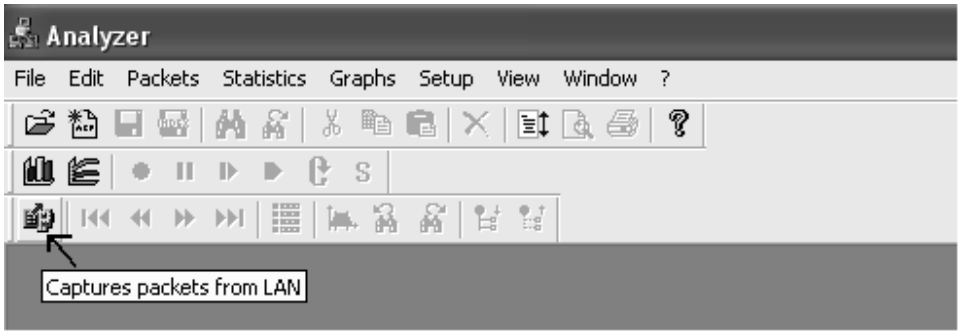
- Que el alumno conozca y comprenda los fundamentos de la monitorización de redes, encapsulado de unidades a diferentes niveles y descomposición de las mismas.
- Que el alumno adquiera la habilidad necesaria para realizar sin dificultades la selección de los filtros adecuada.
- Que el alumno afiance sus conocimientos teóricos acerca del protocolo ARP mediante observación de casos reales.

El paquete Analyzer

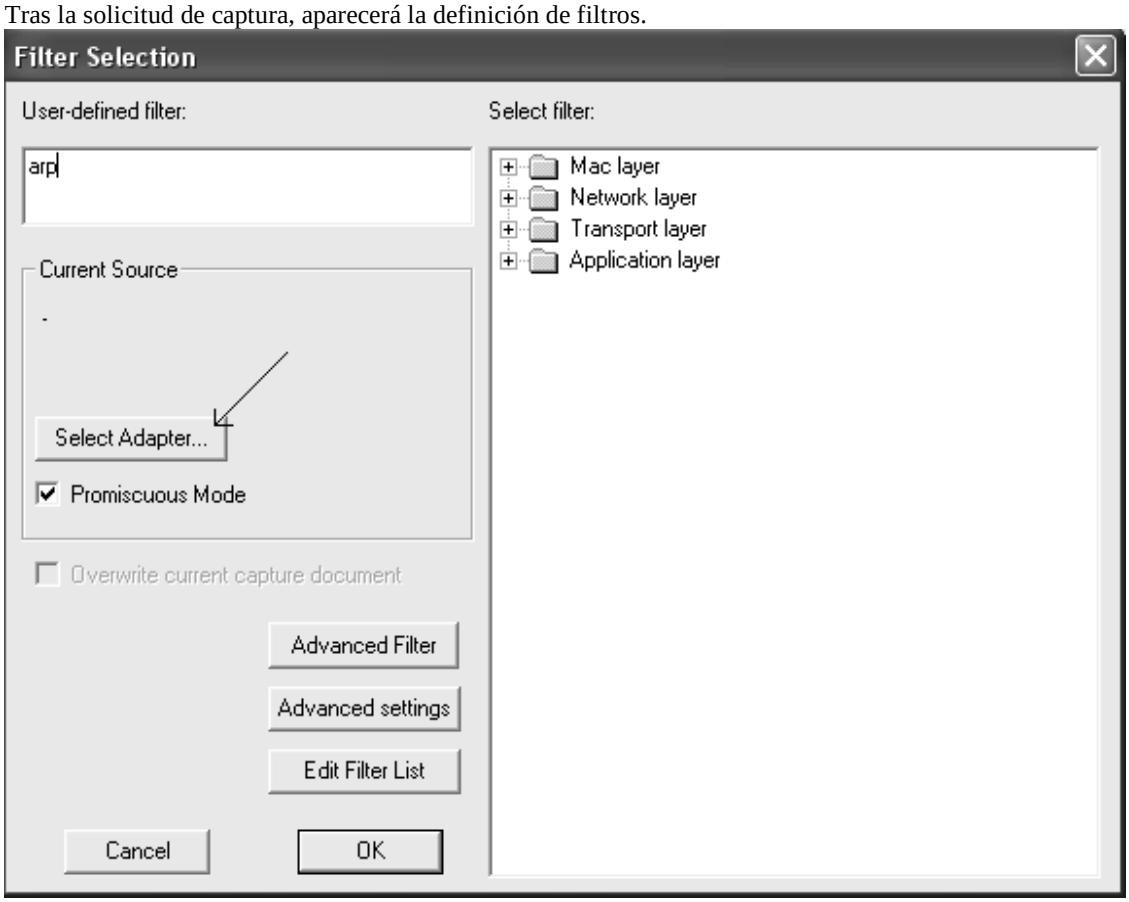
Analyzer es una aplicación completamente configurable para el análisis mediante monitorización de redes locales en entorno Win32 que soporta todas las tecnologías soportadas por el interfaz *WinPcap*. El programa aún se encuentra en desarrollo en el Politecnico di Torino. Su instalación debe ir precedida por la instalación de *WinPcap*.

Ambos programas se encuentran disponibles en versión e instalable en la página anteriormente mencionada. Como puede apreciarse en la figura 1, tras la pantalla de presentación, la pantalla principal de la aplicación está encabezada por un menú, así como varias barras de iconos que resultan equivalentes a la misma.

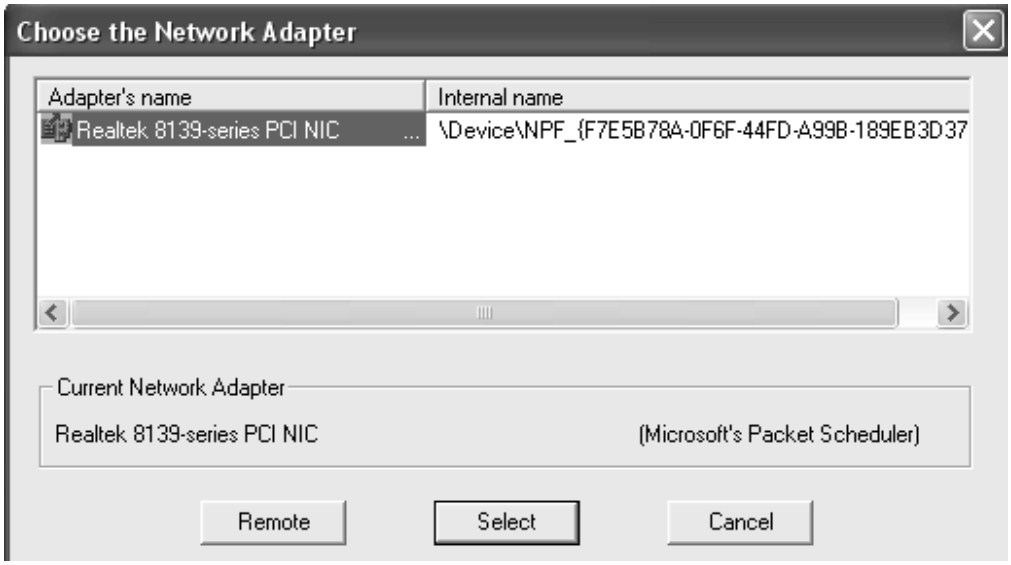
Para comenzar la captura emplearemos el menú correspondiente, indicado en la imagen con una flecha



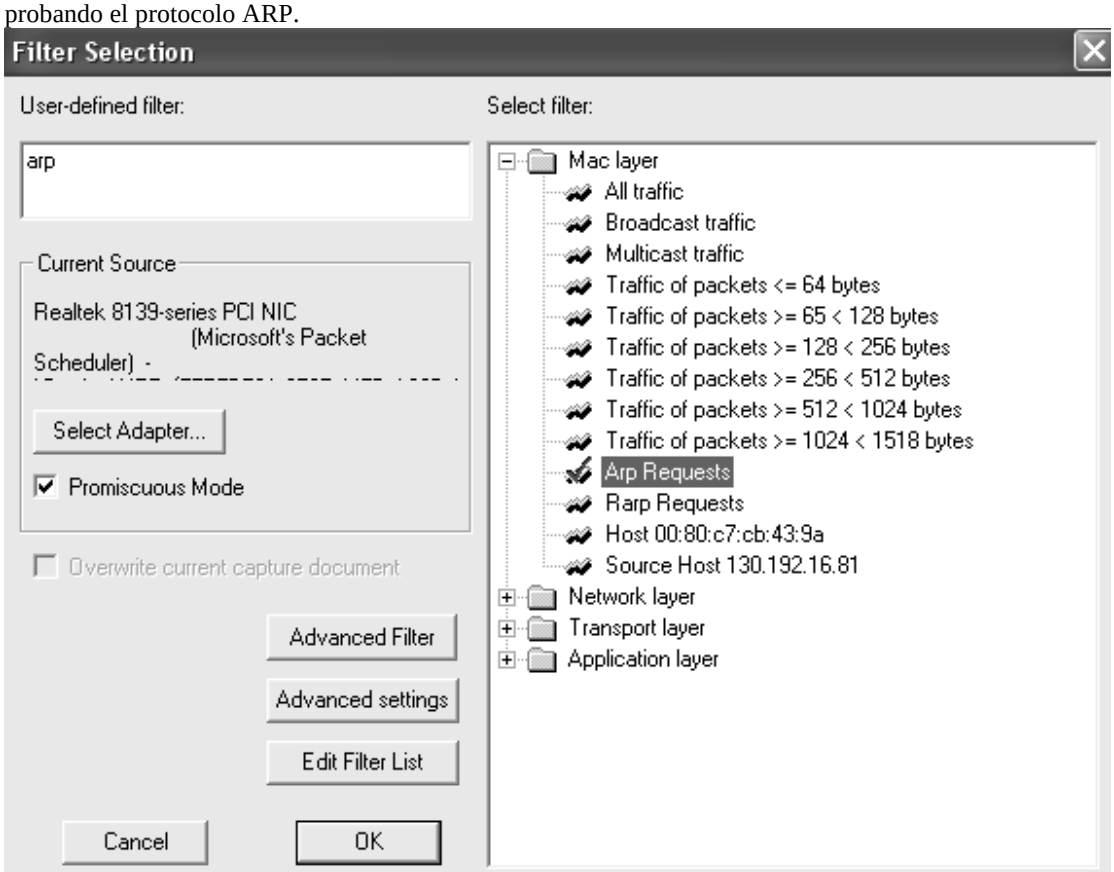
Tras la solicitud de captura, aparecerá la definición de filtros.



El primer paso será la selección del adaptador de red correspondiente.



Una vez seleccionado el interfaz, podremos seleccionar el filtro deseado. En nuestro caso, comenzaremos probando el protocolo ARP.



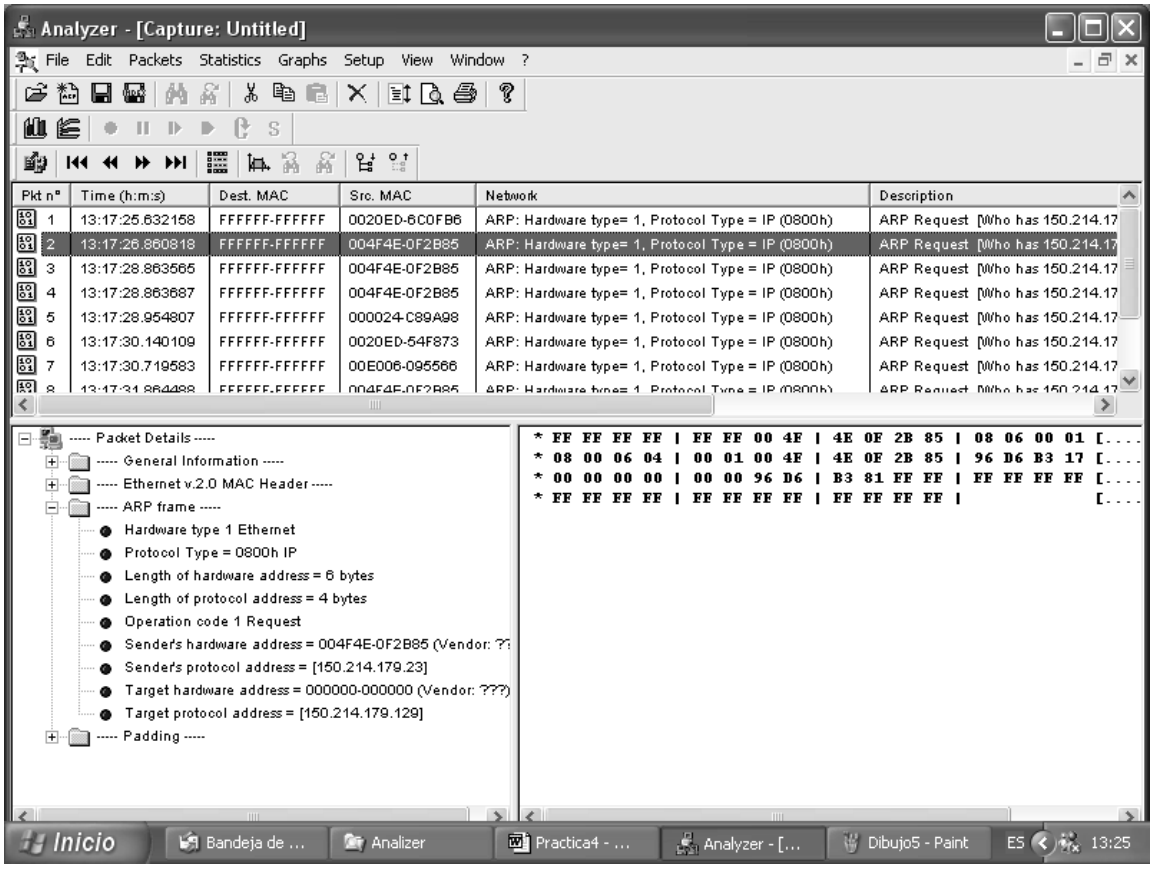
Asimismo, es posible seleccionar el modo promiscuo. Por omisión, el adaptador de red únicamente recogerá las tramas dirigidas directamente a nuestro adaptador de red, las difusiones y las multidifusiones.

Sin embargo, para permitir la captura de tramas que no son enviadas ni dirigidas a nuestro adaptador (p.e. el tráfico entre otras dos máquinas de nuestra red) es necesario pasar el adaptador a modo promiscuo, en cuyo caso todas las tramas visibles en la red pueden ser capturadas.

Es necesario realizar un inciso acerca de la visibilidad de tramas. En un medio de difusión, como por ejemplo ethernet sobre coaxial o con hubs, todas las tramas son visibles por todas las estaciones. Sin embargo, si existen en la topologías puentes, switches o routers, estos elementos actúan como divisores de dominios de colisión, y por tanto impiden la visibilidad de las tramas que no entran en el dominio de colisión del monitor.

El siguiente paso consiste en lanzar la captura de tramas, aplicando el filtro seleccionado.

Cuando se considere realizada la captura, se detendrá y la aplicación pasará a mostrar los paquetes capturados con el siguiente formato:



Cuando se selecciona en la lista de tramas capturadas en el recuadro inferior aparece un árbol con el detalle de los campos de cada nivel (información general, información de ethernet, etc.), y a la derecha un volcado hexadecimal y otro ASCII del campo de datos de la trama.

Realización de la práctica.

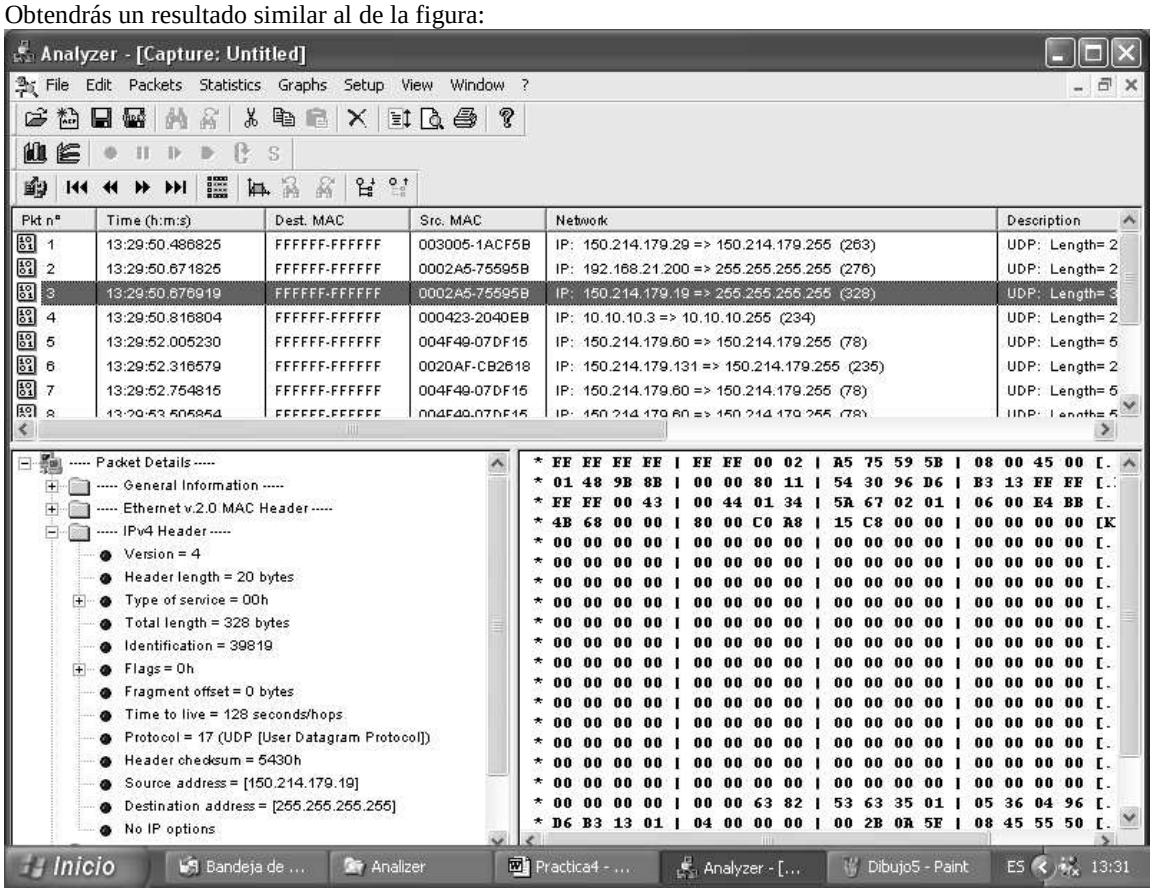
1ª PARTE. Captura de paquetes

Como primera aproximación a la utilización de la aplicación para captura de paquetes y análisis de protocolos *Analyzer*, a continuación realizaremos una captura de paquetes IP y analizaremos los formatos de las tramas generadas que contengan datagramas IP

Paso 1: Iniciamos una captura ("File" → "New Capture..."), o bien mediante el icono correspondiente , y definimos un filtro que capture todas las tramas que contengan datagramas IP que entren o salgan de nuestro computador. Para realizar esta selección podríamos seleccionar el protocolo IP del árbol de la derecha o bien escribir en el campo ***User-defined filter*** el filtro "*ip*". No obstante, si queremos evitar sobrecargar la captura con paquetes de difusión, podemos afinar más el filtro indicando "*ip and not ip broadcast and not ip multicast*".

Una vez definido el filtro, se comienza la captura de paquetes pulsando **OK**.
Para generar algo de tráfico en tu máquina, abre un cliente web (Netscape, Explorer) y realiza una conexión una URL cualquiera. Cuando haya finalizado la descarga de la página seleccionada, detén la captura.

Obtendrás un resultado similar al de la figura:



Selecciona en la parte superior de la ventana la primera trama que ha generado tu computador (normalmente se tratará de una consulta al servidor de nombres pidiéndole que le traduzca el nombre del servidor web accedido).

Analiza los diferentes campos de la cabecera de la trama Ethernet y de la cabecera IP. A partir de esta información rellena las siguientes tablas:

Cabecera de la trama Ethernet capturada:

Dirección física destino	Dirección física origen	tipo

Cabecera del paquete IP capturado:

Versión	longc	tipo servicio	long total	
Identificación			flags	desplaz. fragmento
tiempo vida	protocolo		checksum de la cabecera	
dirección IP fuente				
dirección IP destino				
opciones (variable)				

*La orden **arp***

El computador que estamos utilizando en esta práctica está conectado a una red de área local Ethernet que, a su vez, se conecta a Internet a través de un *router*. Cuando las aplicaciones en red (Netscape, por ejemplo) generan peticiones para otros computadores de Internet, crean paquetes (también llamados datagramas) que contienen la dirección IP de la máquina destino. El uso de direcciones IP (y de los protocolos TCP/IP) crea la ilusión de que todas la máquinas que se comunican pertenecen a una única (es inmensa) red común: Internet.

Si la dirección IP destino corresponde a una máquina de nuestra propia (sub)red (192.168.13.xxx), el paquete puede ser entregado directamente a su destino sin más intermediarios. Sin embargo, cuando la dirección IP corresponde a una red o subred externa, la entrega de la información debe realizarse a través del *router*. En primer lugar, habrá que entregar la información al *router* de nuestra red y éste será el encargado de encaminar el paquete para hacerlo llegar e la red destino donde se encuentra el computador referenciado. Como vemos, en cualquiera de los dos casos, en una primera instancia se realiza una transmisión de información a través de la red de área local.

Desafortunadamente, las direcciones IP no son, por sí mismas, válidas para transmitir una trama a través de la red de área local. Las tarjetas adaptadoras de red que conectan las estaciones con el medio no entienden las direcciones IP, sólo entienden direcciones físicas. Por tanto, para que un datagrama IP viaje por la red de área local, este debe encapsularse dentro de un trama (Ethernet en nuestro caso).

Esa trama Ethernet contiene la dirección física del siguiente destino que, como hemos visto, puede tratarse del computador final al que van dirigidos los paquetes (origen y destino en la misma red local) o del *router* que encaminará el paquete hacia el exterior (origen y destino distintas redes o subredes).

En redes TCP/IP se utiliza un protocolo para la obtención de direcciones físicas a partir de direcciones IP dentro de una red de área local. Este protocolo se conoce con el nombre ARP (*Address Resolution Protocol*). Los detalles del funcionamiento de este protocolo se han visto en las clases de teoría del curso. En esta práctica nos limitaremos a comprobar la existencia de este protocolo a través de la orden **arp** de DOS.

Esta orden nos permite ver (y modificar) la caché ARP de nuestro computador. La caché ARP es una tabla que almacena temporalmente las relaciones entre direcciones IP y direcciones físicas, que ha conseguido averiguar nuestro computador utilizando el protocolo ARP. Es importante destacar, que la mayoría de estas entradas se generaran automáticamente (y de forma transparente al usuario) cuando se ejecuta una aplicación Internet (ping, cliente web, cliente ftp, etc.). Por tanto, muy rara vez (fuera de esta práctica) requiere el usuario modificar manualmente esta tabla.

Más concretamente, la orden **arp** de DOS permite:

- Ver la caché local de ARP (**arp –a**)
- Eliminar entradas manualmente de la caché (**arp –d dirección_IP o arp –d ***)
- Añadir entradas manualmente a la caché (**arp –s dirección_IP dirección_Física**)

2ª PARTE:

Paso 1: Desde una ventana DOS ejecuta la orden **arp –a** para comprobar que la caché ARP está vacía. Si no lo está, cierra todas las aplicaciones que hagan uso de la red y elimina la entradas de la caché ARP usando la orden **arp –d ***, o simplemente esperando un par de minutos (sin ejecutar nuevas aplicaciones en red) y las entradas desaparecerán de la caché.

A continuación ejecuta un navegador WEB para acceder a la máquina **150.214.170.105** (es la dirección de la máquina **www.ujaen..es**) mediante el URL http://150.214.170.105 y examina de nuevo la caché ARP. Anota la información obtenida en la tabla siguiente:

Dirección IP	**Dirección Física**

Repite de nuevo la operación http://150.214.170.105 y coge trafico con el analizer, ¿Se tiene algun tipo de mensaje con el formato del ARP?, justifica tu respuesta.

Paso 2: Elimina manualmente las entradas de la caché ARP (o espera un par de minutos) y utiliza el mismo navegador para acceder al servidor **www.uma.es**. Anota la información obtenida en la tabla siguiente:

Dirección IP	**Dirección Física**

Cuestión 1: ¿A qué máquina corresponde la dirección almacenada en la caché?. Consulta la información ofrecida por la orden **ipconfig** para resolver este apartado. ¿Crees que esta dirección corresponde a la máquina www.uma.es? ¿Por qué?

Cuestión 2: Busca en el *Analizer* el par de tramas que provoca la búsqueda de las direcciones físicas y la respuesta. Busca los 4 campos que nos da esa información.

Cuestión 3: ¿Cuándo se mandan paquetes ARP?, ¿para qué se mandan?

Paso 3: Monitoriza la cantidad de paquetes ARP que recibe tu PC. Para ello inicia el *Analyzer* y selecciona la opción ***statistics*** → ***New Real Time monitor***. El filtro adecuado es **arp.**
En el ajuste de las características de monitorización selecciona la opción de visualizar el tráfico en número de paquetes (**show** → **traffic** → **packets**) , dejando el resto de los parámetros con los valores por omisión.
A continuación se nos presentan cuatro tipos de visualización: Texto en columna de valores, líneas, barras verticales o diagramas de tartas. Selecciona **líneas** y procede a la captura. Observa el monitor en marcha durante algunos minutos, y anota de forma aproximada los valores máximos que aparecen y el momento en que se producen.

Instante de tiempo	**Paquetes/segundo**

Paquetes ICMP

El objetivo de este apartado es estudiar los paquetes ICMP. Para enviar paquetes ICMP se hará uso de la aplicación *ping* y del *analyzer.*

Paso 1: efectuar el comando **ping himilce.ujaen.es**

Cuestión 1: La entrega de mensajes ICMP ¿ha sido directa o indirecta?, ¿porqué sistemas ha pasado los posibles mensajes?

Cuestión 2: Analiza la dirección MAC destino para los mensajes ICMP request

Cuestión 3: Analiza la dirección MAC origen para los mensajes ICMP reply

Cuestión 4: Analiza la cabecera de los paquetes ICMP, ¿qué campos tiene?. Especifícalos y di si puedes qué número de octetos/bytes ocupa cada campo.

Cuestión 5: ¿Qué campo nos dice el tipo de paquete ICMP que es?

Apéndice: Definición de filtros

Analyzer y *Ethereal* utilizan la misma sintaxis para la definición de filtros que la orden de Unix **tcpdump**. La descripción que se ofrece a continuación no es más que una adaptación de la información que aparece en la página man de **tcpdump**.

Un filtro de captura consiste en un conjunto de expresiones primitivas conectadas mediante conjunciones (**and/or**) y opcionalmente precedidas por **not:**
[not] primitiva [and|or [not] primitiva ...]

Ejemplo 1. Captura tráfico telnet (puerto 23) desde y hacia el host 10.0.0.5.
tcp port 23 and host 10.0.0.5

Ejemplo 2. Captura tráfico telnet no dirigido ni generado por el host 10.0.0.5.
tcp port 23 and not host 10.0.0.5

Una primitiva es una de las expresiones siguientes:
[src|dst] host <host>

Permite filtrar el tráfico generado (**src**) o recibido (**dst**) por un **<host>**, indicando su dirección IP o su nombre. Si no se especifica ni **src** ni **dst**, se seleccionan todos los paquetes cuya dirección origen o destino coincide con la del computador especificado.
ether [src|dst] host <ehost>

Permite filtrar basándose en la dirección Ethernet. Como antes, se puede indicar **src** o **dst** para capturar sólo el tráfico saliente o entrante.
gateway host <host>

Permite filtrar paquetes que usan al <**host>** como un **gateway** (router). Es decir, paquetes cuya dirección física (origen o destino) es la del host, pero las direcciones IP (origen o destino) no corresponden al host.
[src|dst] net <net> [{mask <mask>}|{len <len>}]

Permite seleccionar paquetes basándose en las direcciones de red. Adicionalmente, se puede especificar un máscara de red o el prefijo CIDR cuando sea diferente al de la propia máquina desde donde se realiza la captura.
[tcp|udp] [src|dst] port <port>

Permite un filtrado basado en los puertos TCP y/o UDP. Las opciones **[tcp|udp] [src|dst]** permiten restringir el filtrado sólo a los paquetes de un protocolo (TCP o UDP), o sólo a los que utilizan el puerto como origen o como destino.
less|greater <length>

Selecciona paquetes cuya longitud sea menor o igual (**less**) o mayor o igual (**greater)** que un valor dado **<length>.**
ip|ether proto <protocol>

Selecciona paquetes del protocolo especificado, bien al nivel Ethernet o al nivel IP.
ether|ip broadcast|multicast

Permite filtrar difusiones (**broadcast**) o multidifusiones (**multicast**) Ethernet o IP.
<expr> relop <expr>

Esta primitiva permite crear filtros complejos que seleccionan bytes o rangos de bytes en los paquetes.
Véase el manual de **tcpdump** para más detalles.