Práctica

10

GESTIÓN Y UTILIZACIÓN DE REDES LOCALES

Curso 2001/2002

Monitorización de una LAN

Introducción

Un monitor de red es un programa que nos permite observar el tráfico de la red, conocer el estado en que se encuentra la red, el contenido de los paquetes que circulan por ella, la evolución temporal del tráfico, etc.

Para monitorizar una red existen en el mercado numerosos productos software y hardware, en versiones para diferentes tecnologías de red de área local. En esta práctica vamos a utilizar una versión de demostración del programa NetXray 3.0. Dado que se trata de una versión de evaluación, existen numerosas restricciones, principalmente el tiempo de uso y la capacidad de examinar paquetes, que está restringida a 5 paquetes.

El objetivo de la práctica es introducir una herramienta de gestión de redes, así como el análisis de algunos parámetros que pueden obtenerse con la herramienta.

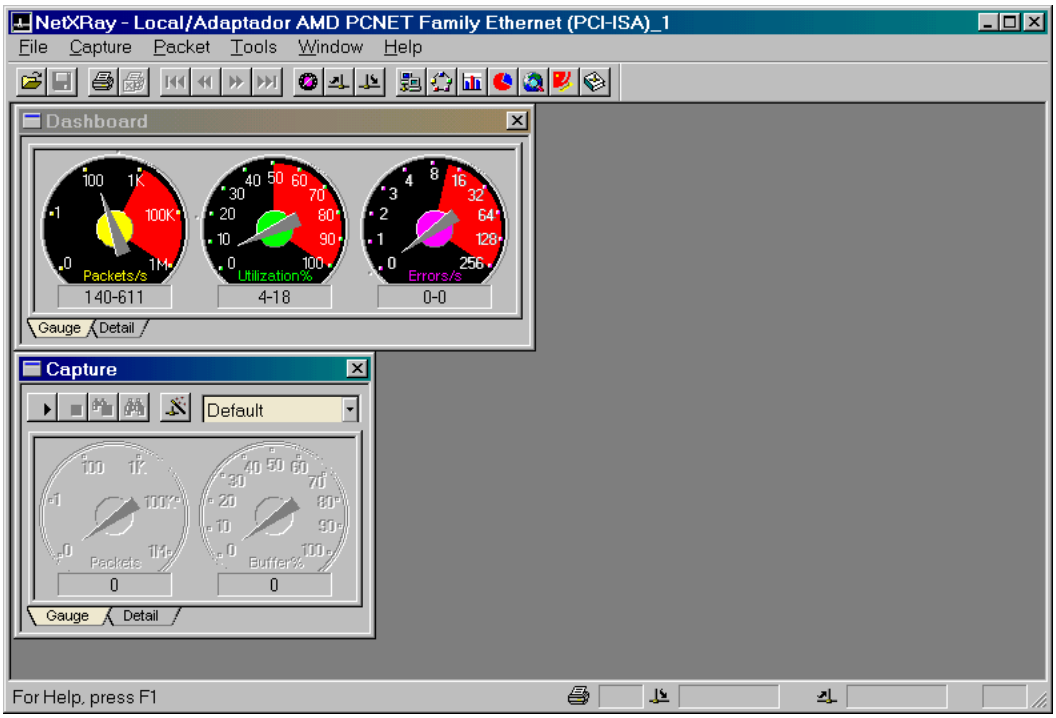
Instalación

Para la instalación del programa se deben seguir los siguientes pasos:

1. Ejecutar el programa **`nx30demo.exe`** que se encuentra disponible en el servidor herodes, en el directorio **`\\herodes\practicas\Gyurl\Practica10`**
2. Conforme avanza la instalación, aceptar las opciones por defecto.
3. Una vez acabada la instalación del programa, ejecutar el programa NetXRay, que se encuentra en el menú de **Inicio**, en **Programas**.
4. **IMPORTANTE**: Al terminar la práctica desinstalar el programa. Para ello hay que ir al botón de Inicio, escoger el **Panel de Control** y allí la opción de "**Agregar o quitar programas**". Finalmente, en la lista que aparece, escoger **NetXRayV0300Demo-D** y pulsar el botón "**Agregar o quitar ...**".

Parte I: Captura inicial de tráfico

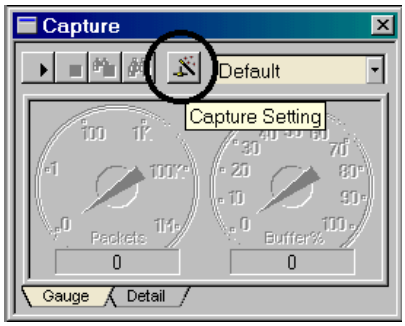
En algunos de los ejercicios que se van a plantear será necesario generar tráfico en la red. Para ello se sugiere que se ejecuten aplicaciones que hagan uso de la red, como el Internet Explorer (para generar paquetes de TCP/IP), o una consulta a un directorio compartido en red (para obtener paquetes de NetBIOS/NetBEUI). Una vez ejecutado el monitor de red, el aspecto de la aplicación será algo similar al mostrado en la siguiente figura:



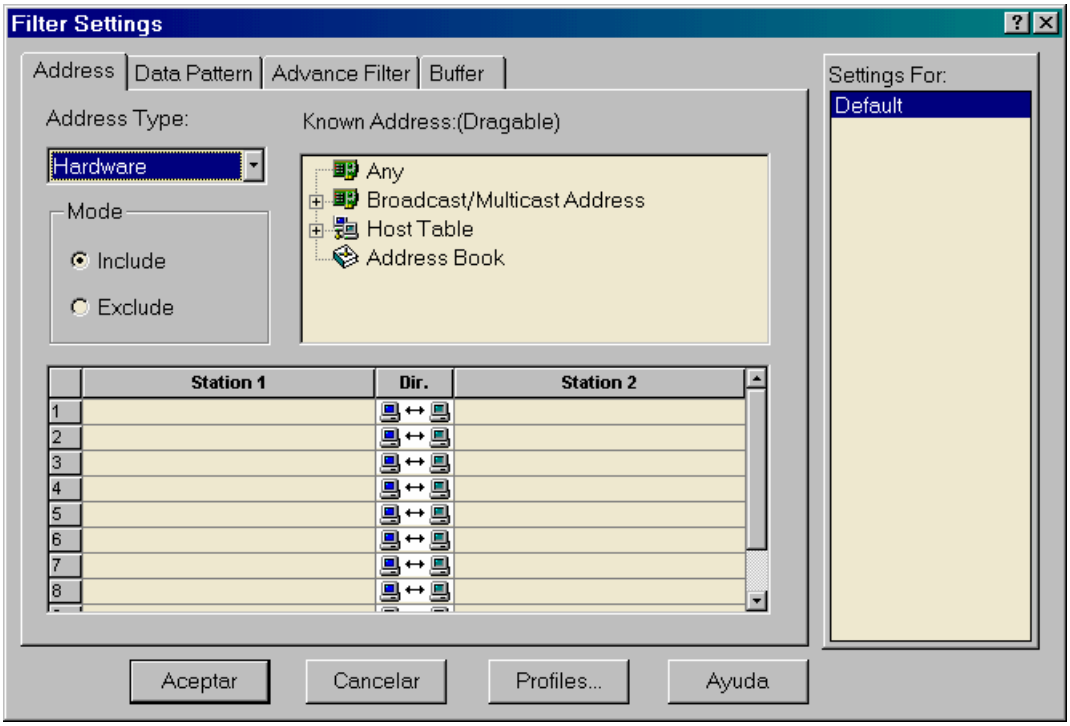
En la figura anterior podemos ver la pantalla principal de nuestro monitor de red, en la que hay dos ventanas. La primera, llamada "Dashboard", proporciona distintos parámetros de funcionamiento de la red, como son el número de paquetes por segundo que circulan por la red, la utilización o la tasa de error. La segunda ventana, llamada "Capture", nos permite realizar la captura de paquetes, que en esta versión está limitada a 256K paquetes y de todos ellos sólo se pueden visualizar 5 paquetes.

EJERCICIO: Mediante el panel de captura, configurar 4 capturas distintas, analizando el formato de los paquetes (Ethernet):

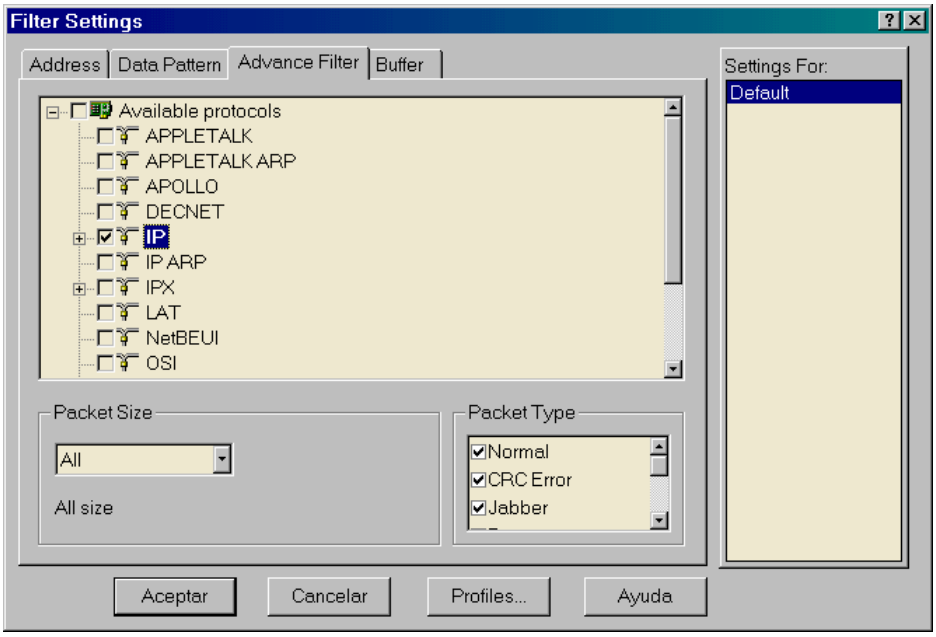
Captura 1) Paquetes con datos del protocolo IP. Para ello, en la ventana "Capture" pinchad en el botón "Capture Setting", como se muestra en la figura de la derecha.



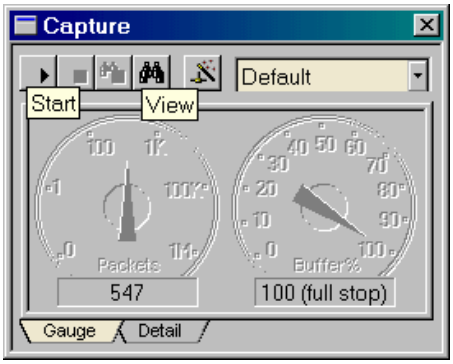
Al pinchar en este botón aparece la ventana que nos permite especificar el filtro que vamos a aplicar en la captura de paquetes.



De momento en la pestaña "Address" no hay que especificar ningún valor. Sin embargo, tenemos que seleccionar el protocolo "IP" en la pestaña "Advance Filter", como se muestra en la figura siguiente.

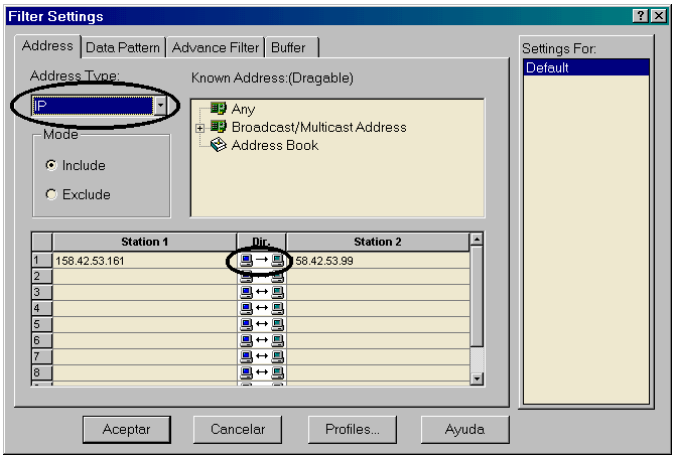


Una vez hayamos especificado el protocolo, podemos comenzar la captura, pinchando en el botón "Start" de la ventana "Capture". Tras unos segundos podemos ver los paquetes con el botón "View". Después de pinchar en "View", aparece una ventana con cinco de los paquetes capturados. Analizad los diferentes paquetes, haciendo especial énfasis en el formato de trama Ethernet.



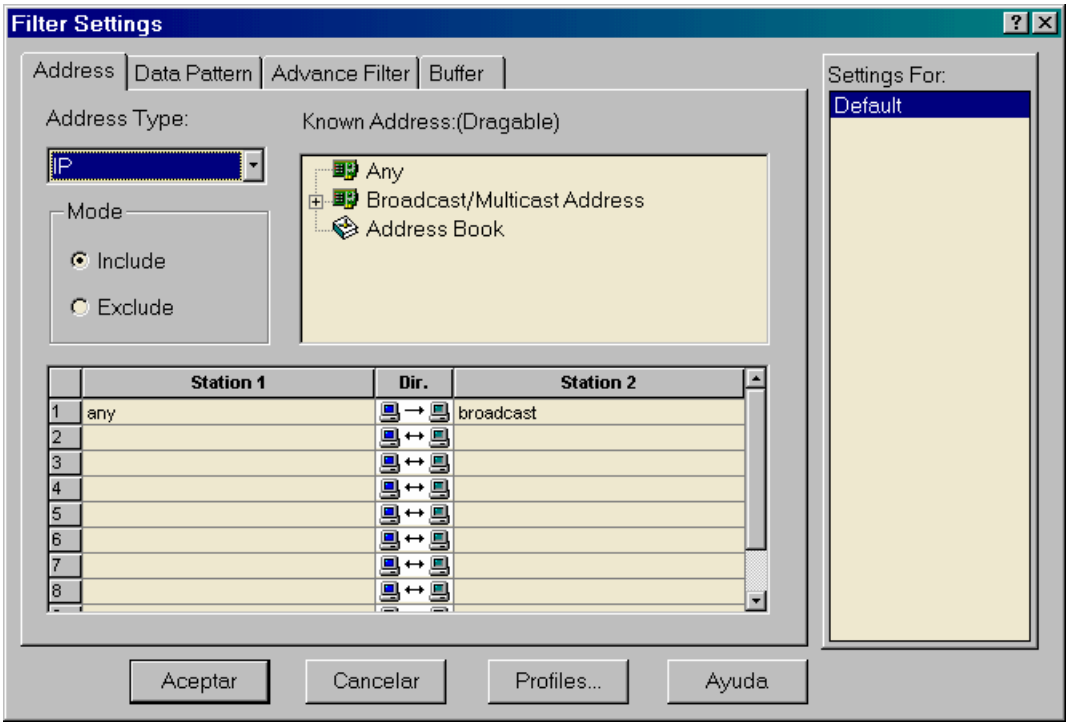
Captura 2) Esta vez capturad paquetes del protocolo NetBEUI.

Captura 3) Configurando un filtro de direcciones, capturad paquetes con origen en la máquina en la que estáis, utilizando su dirección IP. Como destino poned la dirección de "zoltar.redes.upv.es" (158.42.180.62). Recordad indicar que el tipo de las direcciones es IP y que nos interesan sólo los paquetes que parten de nuestra máquina. Asimismo, recordad seleccionar el protocolo "IP" en la pestaña "Advance Filter". Podéis generar tráfico con una sesión telnet en zoltar.



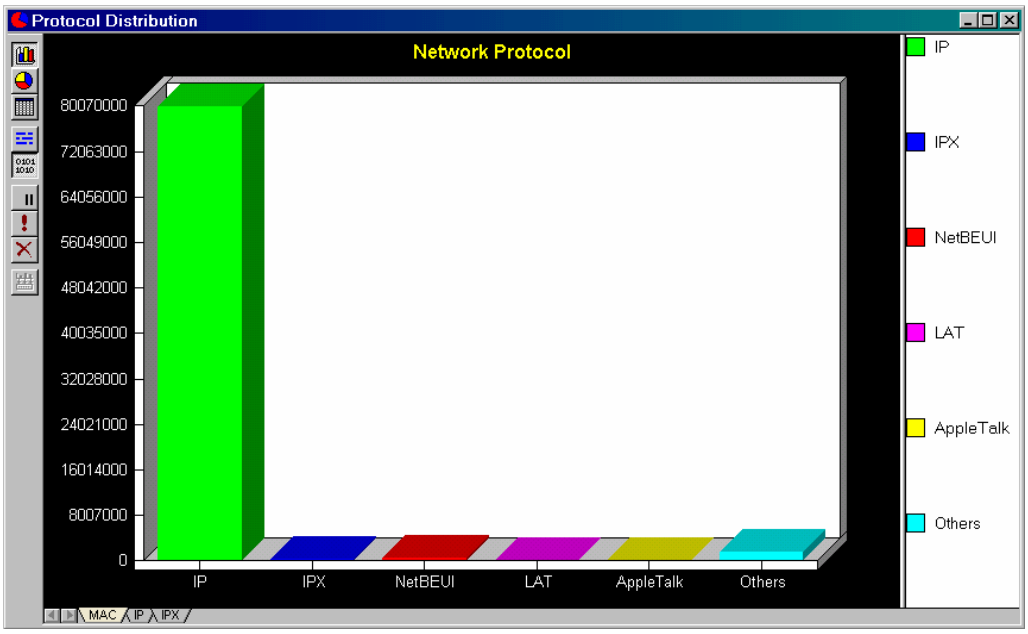
- ¿Cuál es la dirección física de zoltar?
- ¿Qué protocolo de transporte usa Telnet?
- ¿Qué identificativo usa ese protocolo en la cabecera IP?
- ¿Qué puerto está utilizando el cliente de Telnet?
- ¿A qué puerto en zoltar se conecta el cliente de Telnet?

Captura 4) Capturad las difusiones (de cualquier origen), configurando el filtro de direcciones como se muestra a continuación:



EJERCICIO: Iniciar una transferencia por web (cargar una página de la www.upv.es) y observar cual es el incremento en la utilización de la red. A continuación traete el archivo de instalación del NetXRay del servidor a tu disco local y comprueba el incremento producido.

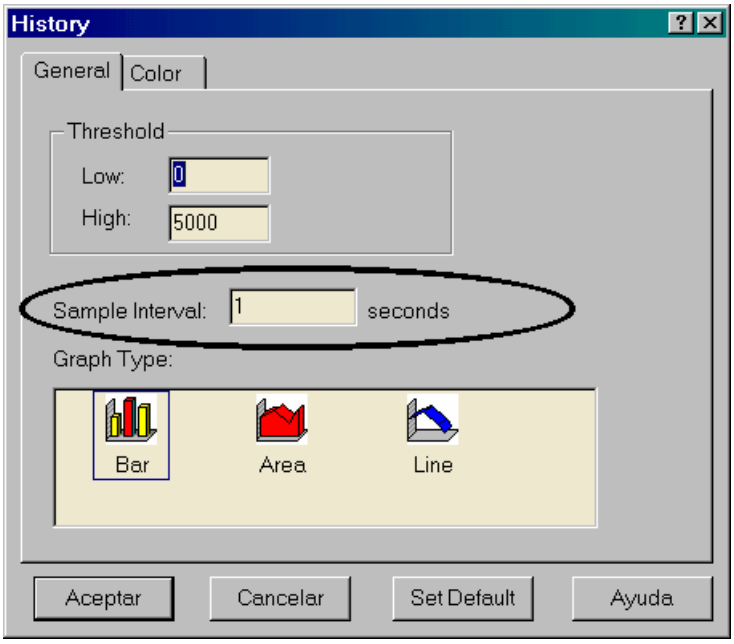
EJERCICIO: En el menú de "Tools → Protocol Distribution" ver cual es la distribución de protocolos a nivel de paquetes de MAC y de tramas IP.



EJERCICIO: En el mismo menú, mediante la opción “Matrix”, ver cual es la conexión más cargada, tanto a nivel de MAC como a nivel IP.

EJERCICIO: En la opción “Global Statistics” de ese mismo menú, se muestra la distribución por tamaño de los paquetes que circulan. ¿Qué conclusión se puede extraer de esta gráfica?

EJERCICIO: Mediante la opcion “History”, ver la evolución de la utilización y el broadcast. Forzar picos mediante la ejecución de aplicaciones que utilicen la red. No olvidéis especificar, en las propiedades de cada una de las medidas a tomar, que el intervalo de muestreo sea un segundo.



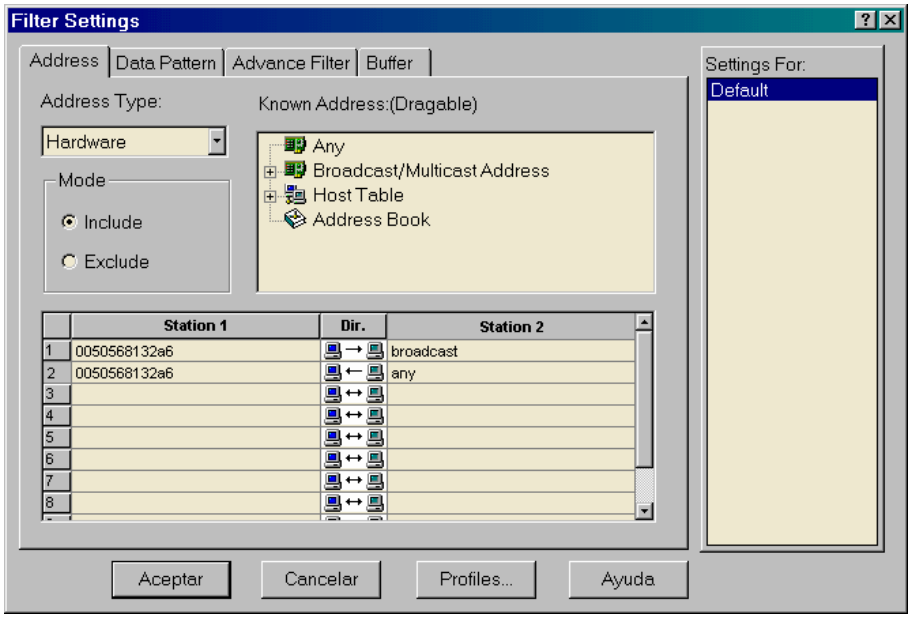
Cuestiones

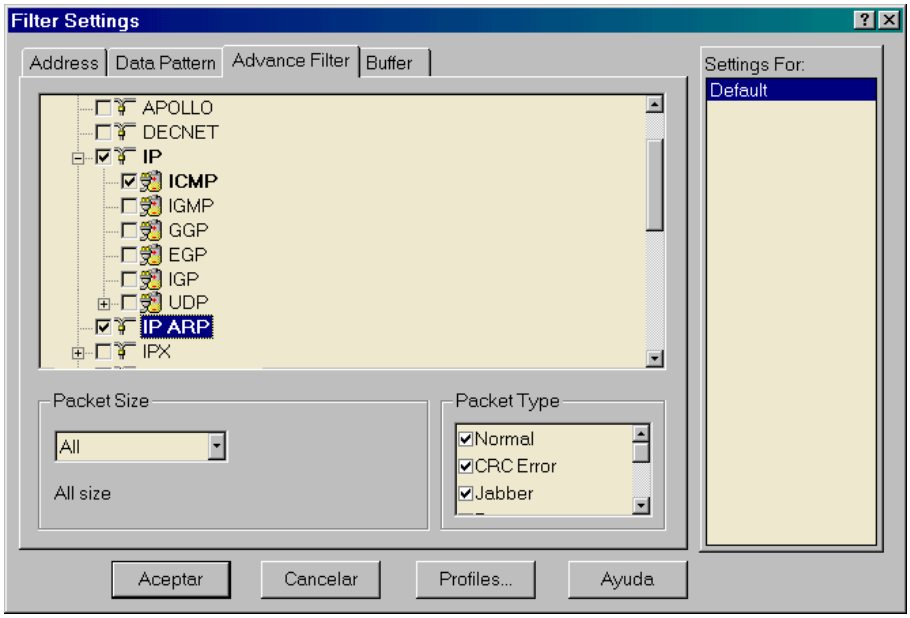
1. Por tus observaciones ¿crees que la red tiene un comportamiento fácilmente predecible?
2. ¿Cómo afecta a la utilización de la red el realizar una transferencia de un fichero?
3. Siendo en una red Ethernet el tamaño máximo de paquete 1500 bytes, ¿cuáles son los tamaños más utilizados?
4. ¿Cuál es el protocolo de la familia TCP/IP más utilizado durante tus medidas?
5. Gran parte del tráfico que llega al laboratorio ha sido filtrado, sin embargo las difusiones no. ¿Por qué crees que las difusiones no se han filtrado?

Parte II: Captura de paquetes ARP

Configuración del filtro

En prácticas anteriores hemos utilizamos la orden “ping”. Esta orden envía un paquete de eco que será contestado por el equipo que especifiquemos a continuación de la orden. Es interesante que capturéis parte del tráfico que se genera como resultado de esta orden. Para ello, en el programa NetXRay en vuestro equipo hay que configurar la captura de paquetes para filtrar sólo aquellos paquetes que se originan o se reciben en vuestro equipo (excluyendo la recepción de las difusiones). De este modo podemos ver parte de los paquetes intercambiados a pesar de la limitación de 5 paquetes del programa NetXRay. En las siguientes imágenes se muestran los cuadros de la aplicación que nos permiten determinar el tipo de filtro.





En la primera de las figuras anteriores hemos seleccionado la dirección física de nuestro equipo para que capture todos los paquetes de difusión que envíe, así como todos los paquetes que reciba desde cualquier origen.

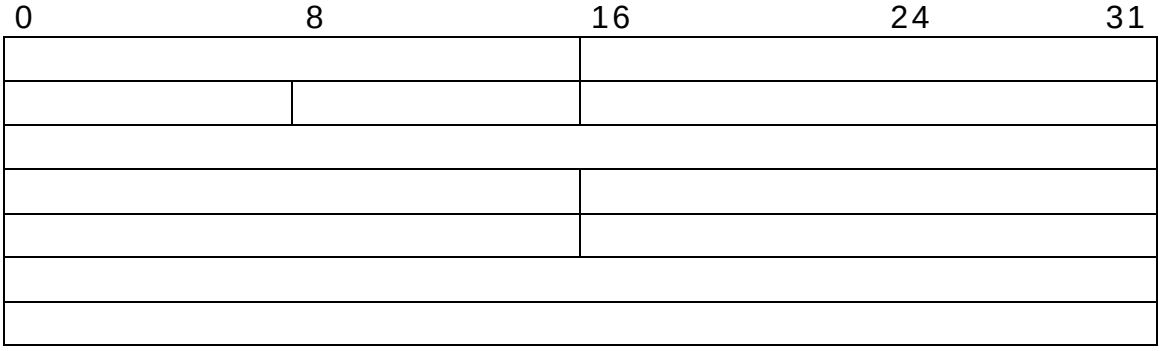
En la segunda figura escogemos el protocolo ICMP, que es el utilizado para el eco que realiza el ping. También hemos seleccionado el protocolo ARP, que resuelve la dirección física a partir de la dirección IP suministrada a la orden ping.

Captura de paquetes

Una vez configurado el filtro, activar la captura y lanzar la orden "**`ping 158.42.180.62 -n 1`**" (desde una ventana de MS-DOS o desde la opción "Ejecutar" del menú de "Inicio").

EJERCICIO: Después de realizar la captura, pasar a examinar los paquetes capturados:

1. Paquetes ARP: ¿Cuántos hay? ¿Qué valor en el tipo de trama identifica a este protocolo?
2. Rellena el siguiente esquema que representa los campos de la cabecera de los paquetes "ARP Request" capturados[1].



¿En qué unidades están expresadas las longitudes de las direcciones hardware y de protocolo?

Una vez analizados los paquetes capturados, vuelve a realizar una captura volviendo a ejecutar la orden ping. ¿Obtienes la misma captura? ¿Qué tipos de paquetes capturas?. Ejecuta la orden ping una última vez. ¿Cuántos paquetes capturas? ¿Qué tipos de paquetes capturas?

[1] Hay un error en el programa al visualizar la dirección física destino en los campos del paquete ARP.

Parte III: Seguridad en la red

Un monitor de red puede utilizarse para otros fines además de para solucionar problemas en la red. A menudo, programas de este tipo se emplean con el fin de *fisgonear* en el tráfico de la red. Por este motivo se habla de *sniffers*, programas que escuchan el tráfico en la red con el fin de capturar información que pertenece a otros. Esta información puede ser cualquier cosa, como el contenido de las páginas web que se están visitando, los correos electrónicos que nos bajamos del servidor de correo, o los *passwords* que se utilizan para acceder a otros ordenadores o servidores.

En redes como Ethernet, donde el tráfico de la red llega a todos los ordenadores del segmento de red en cuestión, es muy fácil capturar la información que viaja por la red. Por este motivo, y como protección ante la posibilidad de que otros "vean" la información que estamos transmitiendo, es habitual utilizar métodos de encriptación, como las páginas web seguras, el protocolo ssh (visto en prácticas anteriores), etc.

Como ejemplo de lo fácil que es capturar información ajena, en esta última parte de la práctica se propone que utilicéis el monitor de red para capturar el password que utilizáis para entrar en **zoltar.redes.upv.es** con el usuario **rdcXX**. Para ello conectaros a zoltar usando telnet y configurad el monitor de red de manera que capture las tramas que salen de vuestro ordenador. ¿Es posible averiguar el password utilizado?