Prácticas de laboratorio

de

Redes de Ordenadores

Práctica 1:

Configuración nodo IP

Uploaded by

IngTeleco

http://ingteleco.iespana.es
ingtelecoweb@hotmail.com

La dirección URL puede sufrir modificaciones en el futuro. Si no funciona contacta por email

PRACTICA 1: Configuración de un nodo IP

1. Objetivos de la práctica

Esta práctica tiene como objetivo primordial familiarizarse con el funcionamiento del protocolo IP.

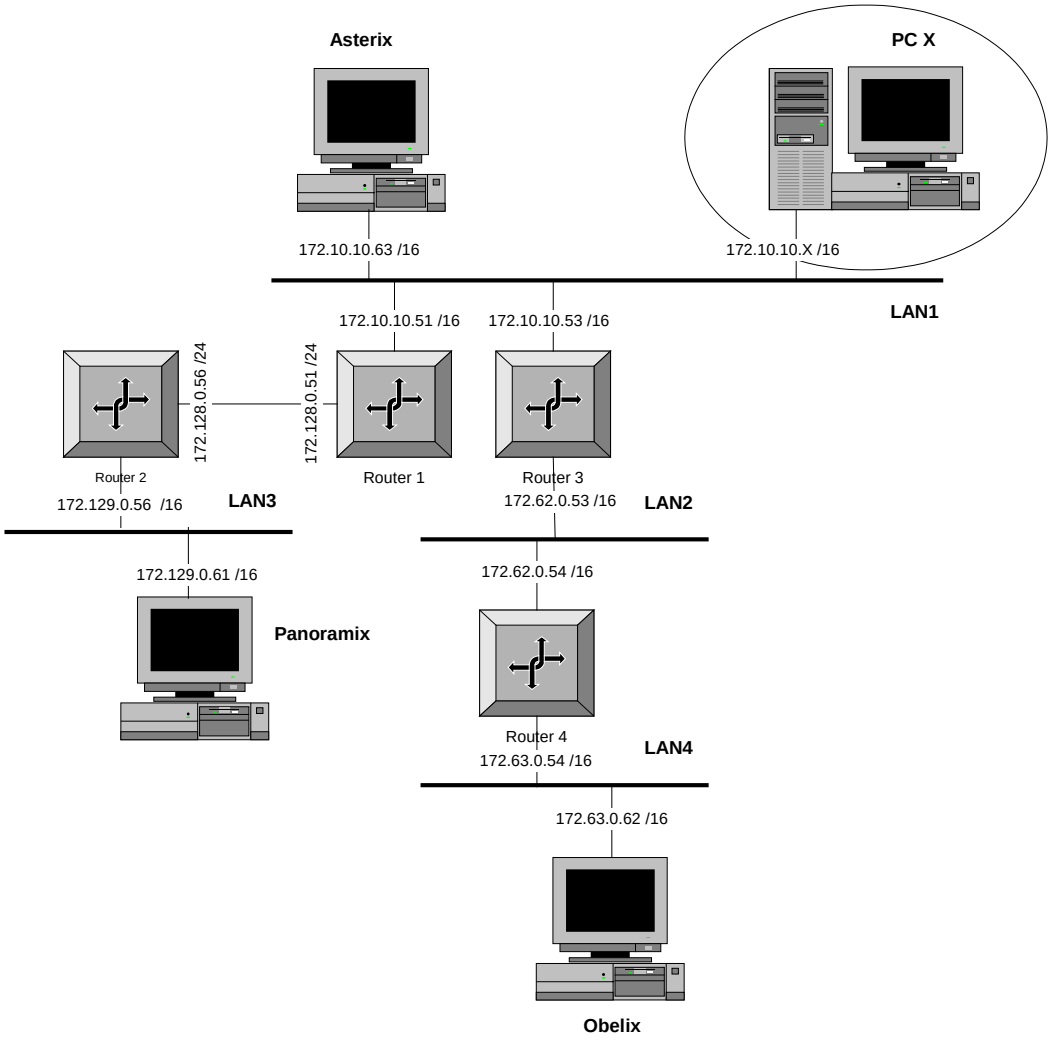
- Configurar el protocolo IP (direcciones, máscara, tabla de encaminamiento) de una estación de trabajo Windows NT.
- Utilizar el monitor de red del System Management Server (SMS) de Microsoft para la captura y análisis del tráfico generado en la red, familiarizándose con sus opciones de captura y análisis.
- ARP.

2. Descripción del entorno

El entorno de red sobre el que se desarrollará la práctica aparece representado en la Figura 1 y está compuesto por:

- Un puesto de trabajo del alumno: PC-X, con Windows NT Server 4.0 y un interfaz de red.
- Cuatro routers, conectados tal y como aparece en la Figura.
- Tres servidores (Asterix, Obelix y Panoramix).

El PC de cada uno de los puestos de trabajo (PC-X) debe conectarse a la LAN indicada en la figura (accesible a través del hub disponible en la parte superior de las mesas) mediante uno de sus interfaces de red con las direcciones IP y máscaras correspondientes pero sin hacer routing entre ellas.



3. GUIÓN DE LA PRACTICA

Se describen a continuación los pasos a seguir para realizar la práctica, en cada uno de ellos e indicado por la figura adjunta se indican las cuestiones que deben incluirse en la memoria de la práctica.

Es muy recomendable leer completamente la práctica antes de comenzar a realizarla, así como consultar los apuntes de la asignatura y la bibliografía relacionada.

3.1 Configuración del interfaz Ethernet

Arrancar el PC en el modo preparado para el Laboratorio de Redes de Ordenadores.

Cada estación de trabajo dispone de dos interfaces Ethernet de los que en esta práctica sólo será preciso utilizar y configurar uno de ellos. Uno de los interfaces se encontrará conectado a una toma de red de la mesa y el segundo con un cable UTP a uno de los puertos del hub disponible en la parte superior de la mesa, comprobando que se encienden los led tanto de la tarjeta de red como el correspondiente al puerto del hub.

Configurar la direcciones IP de este interfaz con la dirección 172.10.10.X /16 (máscara 255.255.0.0). En el apéndice A del guión se explica el proceso de configuración del protocolo TCP/IP de un servidor Windows NT. El segundo interfaz, que no se utiliza en esta práctica, se encuentra configurado con una dirección IP de la red 130.206.139.0 y deberá dejarse con dicha dirección, eliminando el GATEWAY POR DEFECTO si es que estuviera configurado en dicho interfaz.

Para visualizar la configuración de la estación se emplea el comando *ipconfig* desde la ventana DOS, recomendándose analizar y familiarizarse con las opciones del mismo. A su vez, para visualizar la tabla de encaminamiento de la estación se emplea el comando *route print* y al igual que en el caso anterior se recomienda analizar las opciones del mismo.

Una vez terminada la configuración, debe comprobarse que es correcta haciendo ping a la estación ASTERIX. El comando *ping* es accesible desde la ventana DOS y genera un mensaje ICMP de *petición de eco* y los correspondientes mensajes de respuesta. En el apéndice B del documento puede encontrarse una descripción de las opciones de dicho comando. En caso de que con el comando ping no se obtenga respuesta desde ASTERIX revisar la configuración (a modo de sugerencia revisar que la tarjeta Ethernet configurada es la que se encuentra conectada a la red LAN1).

	• Ejecutar el comando *ipconfig /all* e incluir en la memoria el resultado conseguido. (La dirección MAC de la tarjeta Ethernet configurada se necesitará más adelante). • Ejecutar el comando *route print* e incluir en la memoria el resultado conseguido. (el alumno debería ser capaz de explicar el significado de cada una de las entradas de la tabla y el porqué de su valor).

3.2 Manejo del monitor de red

La segunda parte de la práctica consiste en la utilización de un monitor de red para capturar y analizar el tráfico que circula en la red LAN1. En el apéndice D de esta práctica se describe con detalle el manejo del monitor de red que vamos a emplear que es el de SMS de Microsoft y que funciona sobre Windows NT 4.0.

1. Arrancar el monitor de red. Seleccionar la tarjeta conectada a la LAN1 para efectuar capturas (como se explica en el apéndice D sólo se puede capturar a través de un interfaz y la selección de este se hace en base a la dirección MAC del mismo). Hacer ping a ASTERIX tres veces consecutivas, especificando en cada una de ellas el envío de UN SOLO mensaje y un tamaño diferente en cada una de ellas (el valor por defecto, 1500 octetos y 2000 octetos). Después,

detener el monitor de red para analizar el tráfico capturado guardando la captura con el nombre captura1.cap, que deberá entregarse junto con la memoria de la práctica en un disquete. Analizar el formato de una cabecera Ethernet y una cabecera IP comparándolas con el formato presentado en los apuntes y comprobando los valores que tienen.

- Filtrar la captura, seleccionando los datagramas que contienen mensajes ICMP procedentes/dirigidos a la estación de trabajo del alumno. Incluir en la memoria el filtro utilizado y el número de datagramas IP que se han capturado. Dar una explicación a este número.
- Indicar el tamaño de los datagramas IP correspondientes al primer, segundo y tercer ping (solicitudes y respuestas). Dar una explicación al valor del tamaño de los datagramas correspondientes al segundo y tercer ping.
- Filtrar la captura utilizando las propiedades del protocolo IP seleccionando sólo aquellos datagramas que sean fragmentos procedentes/dirigidos a la propia estación de trabajo y no datagramas completos. Indicar el tamaño de estos fragmentos y deducir la MTU de la red.
- Identificar los datagramas que componen las peticiones y respuesta de eco del segundo y tercer ping. Indicar en la memoria para cada uno de ellos los valores de los flags, el valor del desplazamiento de fragmento y la longitud del datagrama (el alumno debería ser capaz de haber obtenido dichos valores sabiendo el valor de la MTU de su red).
- Dar una explicación de por qué los fragmentos posteriores al primero no aparecen en el filtro realizado por protocolo ICMP aunque corresponden a una petición o respuesta de eco.
- Filtrar por propiedades del protocolo IP sólo aquellos fragmentos que son los últimos correspondientes a un datagrama. Indicar en la memoria el filtro aplicado.

2. Arrancar de nuevo el monitor de red y conectarse al servidor web de ASTERIX mediante un navegador (http://172.10.10.63) con lo que se descargará una página de bienvenida. Después de esto detener el monitor de red para analizar el tráfico capturado guardando la captura con el nombre captura2.cap que se incluirá junto a la memoria.

- Filtrar los protocolos HTTP y TCP procedentes/dirigidos a la propia estación de trabajo, lo que hará que se visualicen todas las tramas relacionadas con la descarga realizada.
- ¿Cuál es el protocolo de transporte que emplea HTTP? ¿cuál es el código hexadecimal correspondiente a este protocolo en el campo protocolo?

  El protocolo que utiliza HTTP es orientado a la conexión y fiable (con confirmaciones) por lo cual antes de transferir los datos HTTP es preciso crear una conexión de nivel de transporte y se confirman los datos enviados mediante mensajes de reconocimiento. Por este motivo hemos filtrado no sólo los mensajes HTTP sino también los segmentos TCP que crean las conexiones y los que confirman los datos. Podrán verse varios grupos de tres segmentos TCP que se intercambian (para crear una conexión) o segmentos individuales (para confirmar los datos) y entre ellas datagramas con datos correspondientes a HTTP. De hecho se crea una conexión para cada elemento de la página, motivo por el cual aunque se ha descargado una sola página se han creado varias conexiones.

- Indicar en la memoria el valor del balance "aproximado" entre los datos útiles transferidos y los datos totales. Consideraremos datos totales la suma de las longitudes de todas las tramas intercambiadas (creación de conexión TCP, mensajes HTTP y confirmaciones) y datos útiles el campo de datos de los segmentos TCP (longitud de la trama menos cabeceras de enlace de datos, red y transporte).

3.3 Funcionamiento del protocolo ARP

En este apartado se analizará el funcionamiento del protocolo ARP capturando las peticiones/respuestas ARP y analizando el contenido de la caché ARP del PC-X. Para visualizar el contenido de la caché arp se utilizará el comando *arp* accesible desde la ventaja DOS y descrito en el apéndice E con el que el alumno deberá familiarizarse antes de comenzar esta parte de la práctica.

1. Borrar en primer lugar todas las entradas de la caché arp (si es que no estuviera vacía). Arrancar el monitor de red, hacer *ping* al nodo ASTERIX, y a las direcciones IP de los routers 1 y 3; detener el monitor de red. Guardar la captura con el nombre captura3.cap.

	• Consultar la caché arp, e incluir el resultado en la memoria (el alumno debería ser capaz de explicar cada uno de los valores obtenido). Deberán aparecer tres entradas, si no es así es que se ha hecho algo mal o que ha pasado demasiado tiempo desde la realización del ping, repetirlo en este caso porque las entradas de la memoria caché tienen una vida limitada. • Filtrar las tramas ARP originadas/destinadas a PC-X. Indicar en la memoria el filtro utilizado y cuántas tramas aparecen. Identificar para cada ping las dos tramas ARP (6 en total) capturadas e indicar en la memoria las cuatro direcciones que figuran en la cabecera ARP de cada una de ellas. • ¿Cuál es el identificador de protocolo (en hexadecimal) en la cabecera Ethernet del protocolo ARP? ¿Cuál era el correspondiente al protocolo IP? (puede utilizarse esta misma captura visualizando algún datagrama IP)

Comprobar que mientras están las entradas en la memoria caché y realizando un ping a alguno de dichos destinos no se envían tramas ARP (arrancando el monitor y comprobando que no captura ninguna trama).

3.4 Inclusión de rutas en la tabla de encaminamiento

En este apartado se analizará el contenido de la tabla de encaminamiento de PC-X relacionándola con la operación del encaminamiento IP. Para visualizar y modificar el contenido de dicha tabla utilizaremos el comando *route* que se describe en el apéndice C.

1. Visualizar el contenido de la tabla de encaminamiento de PC-X mediante el comando *route print*.

2. Comprobar si se obtiene respuesta al hacer ping a los nodos Obelix y Panoramix.

	• Indicar en la memoria por qué no se obtiene respuesta a los ping anteriores. • Indicar en la memoria las rutas a añadir en la tabla de encaminamiento de PC-X para obtener respuestas a los dos ping anteriores. Incluirlas mediante el comando *route add* y comprobar que efectivamente ahora se recibe la respuesta correspondiente a los ping. • Visualizar el contenido de la tabla de encaminamiento mediante el comando *route print* e incluir en la memoria su contenido.

3. Comprobar si se recibe contestación a un ping realizado a una dirección IP de la LAN2.

	• Indicar la ruta a añadir en la tabla de encaminamiento de PC-X para obtener respuesta al ping anterior. Incluirla mediante el comando *route add* y comprobar que efectivamente ahora se recibe la respuesta correspondiente al ping. • Buscar la forma de reducir el número de rutas incluidas por el alumno en la tabla de encaminamiento de PC-X de modo que sigan consiguiendo respuesta los ping propuestos anteriormente. Indicar los cambios (rutas eliminadas y añadidas). Comprobar que con los cambios propuestos efectivamente se obtiene

	respuesta.

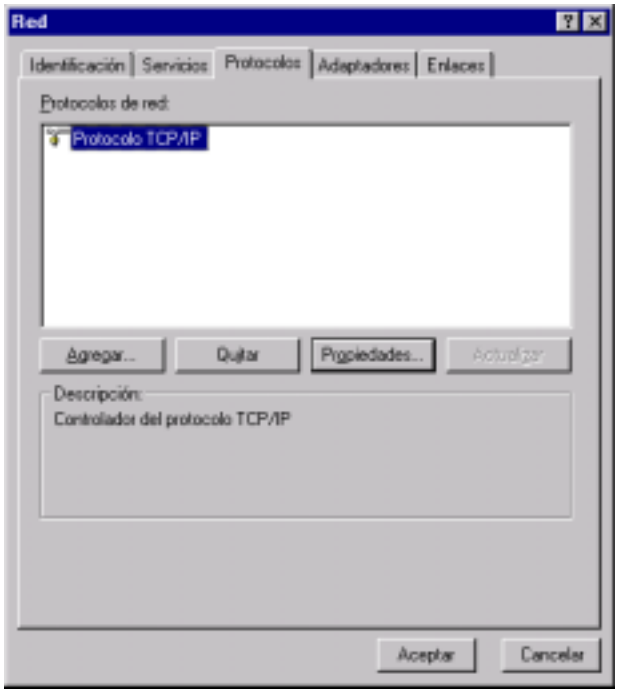
4. Configurar en el interfaz ethernet un gateway por defecto como se indica en el apéndice A, especificando que se utilice el interfaz del router 1. Arrancar el monitor de red y hacer ping a una dirección inexistente, por ejemplo, 172.70.10.10.

	• Filtrar la captura para visualizar los mensajes de eco. Explicar el resultado de la captura.

APENDICE A

Configuración del Protocolo TCP/IP en Windows NT

La configuración del protocolo TCP/IP puede llevarse a cabo durante la instalación de NT o bien puede ser añadido y configurado con posterioridad a la misma; en cualquiera de los dos casos el proceso de instalación y configuración es similar.



Panel de Control

La configuración del protocolo TCP/IP se lleva a cabo en Panel de control/Red/Protocolos, En caso de no encontrarse ya instalado, debe añadirse dicho protocolo mediante el botón Agregar si es que no apareciera en la ventana. Es posible que además del protocolo TCP/IP aparezcan otros si es que han sido configurados en la estación.

Propiedades de TCP/IP

La configuración propiamente dicha del protocolo se lleva a cabo en la ventana de Propiedades de TCP/IP a la que se accede pulsando el botón correspondiente.

En la ventana Propiedades aparecen cuatro pestañas que permiten configurar respectivamente:

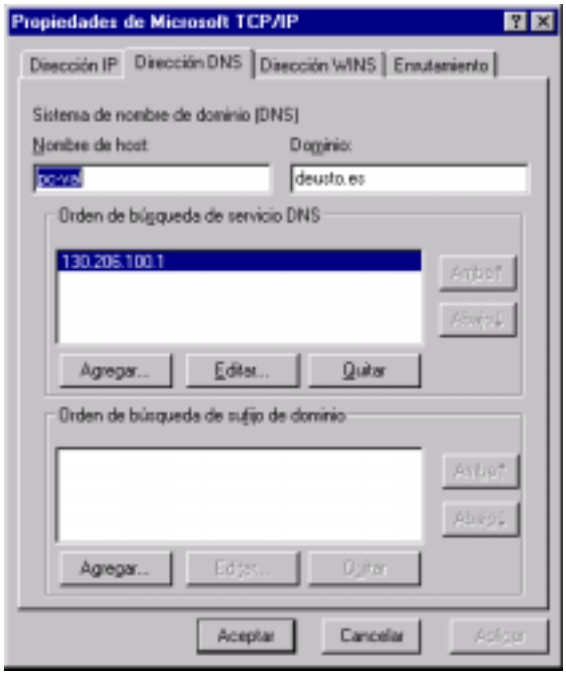
- Direcciones IP.
- Uso de servidor de Nombres de Dominio.
- Uso de servidores Wins.
- Habilitación de la estación para actuar como router.

Dirección IP

Se puede configurar las características IP para cada uno de los interfaces, que podrán seleccionarse en la lista que aparece en la parte superior de la ventana.

En caso de no utilizar direcciones IP fijas sino las proporcionadas por un servidor DHCP se habilitará la opción correspondiente, debiendo dejar en blanco el resto de los campos.

Si se utilizan direcciones fijas se rellenarán los campos de dirección IP del interfaz de red, la máscara de subred y la dirección IP del router por defecto que se utilizará para el encaminamiento de datagramas.



Uso de un servidor DNS

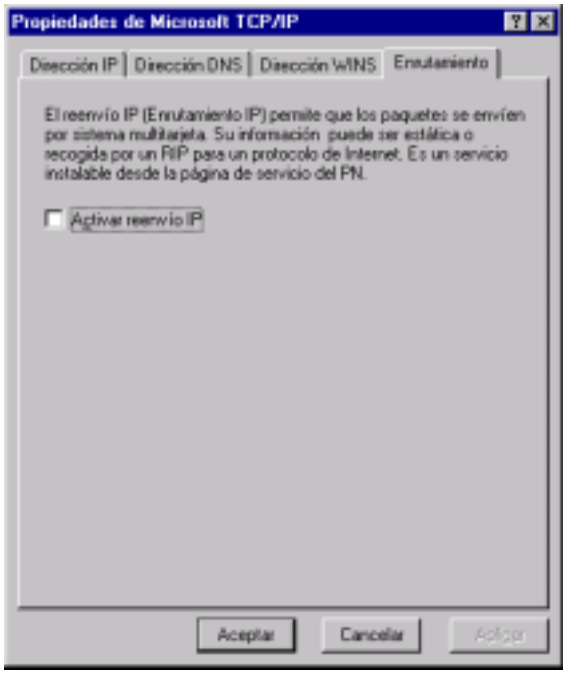
Si se dispone de servidores de un Sistema de Nombres de Dominios (DNS) en la red puede configurarse el servidor NT para sacar provecho de los mismos.

Los pasos a seguir para configurar los elementos de la solapa DNS de la ventana Propiedades de TCP/IP de Microsoft son los siguientes:

1. Introducir el *nombre de host* DNS TCP/IP y el *nombre del dominio* DNS en los campos apropiados. Por defecto el nombre de la computadora se introduce automáticamente en el campo Nombre del host, con el mismo nombre con el que fue registrado en el dominio NT.

2. Pulsar Agregar para añadir la dirección del servidor DNS. Se pueden añadir hasta tres servidores DNS y usar las flechas para modificar el orden en el que están ordenados; de este modo si se falla al resolver correctamente el nombre, se intentará con un segundo y finalmente con un tercero.

3. Pulsar Aceptar y finalizar la configuración.



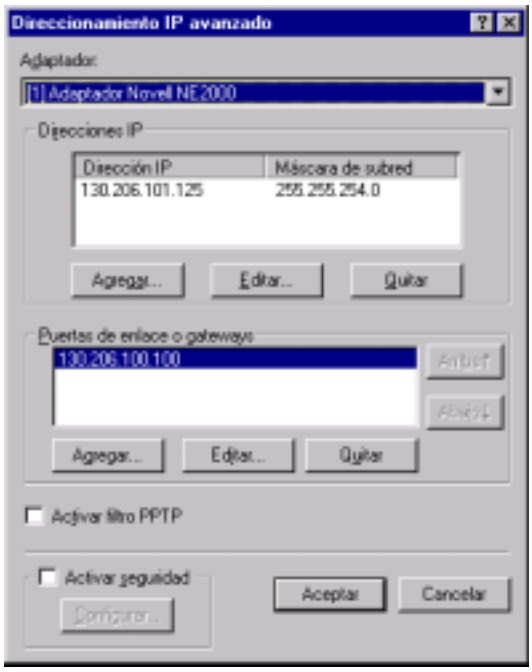
Configuración de WINS

La solapa Direcciones WINS en la ventana Propiedades TCP/IP de Microsoft permite configurar el sistema para sacar provecho a los servidores WINS disponibles en la red. Se trata de especificar el adaptador de red que se quiere configurar, e indicar las direcciones del servidor primario y secundario de WINS.

Enrutamiento

En caso de que la estación disponga de varios interfaces de comunicaciones y deseemos que actúe encaminando datagramas entre ellos, debe seleccionarse la opción correspondiente en la ventana Enrutamiento.

OPCIONES AVANZADAS DE TCP/IP



Adaptadores Multihome lógicos

Es posible configurar más de una dirección IP para una única tarjeta de red, lo que habitualmente se denomina configurar un *adaptador de red multihome lógico*. Windows NT permite asignar hasta cinco direcciones IP a un único adaptador de red.

Una de las ventajas de un sistema multihome lógico viene al utilizar el servidor de Información de Internet (IIS). Por ejemplo si queremos ejecutar tres páginas web desde el servidor, el multihome lógico lo hace más fácil. Supongamos que se quisiese ser el host de micompañía.com, universidad.edu y musica.es desde el servidor, simplemente se designará una dirección diferente para cada site y a continuación se asociarán las tres direcciones IP al adaptador de red.

Para ello se debe utilizar el botón Agregar y añadir direcciones IP adicionales y pares de máscaras de subred para el adaptador de red seleccionado hasta un máximo de cinco.

Gateways con direcciones IP múltiples

Si se necesita usar TCP/IP para comunicarse con nodos fuera de la subred, la comunicación deberá hacerse a través de una pasarela. Muchas redes para tener mayor tolerancia a fallos se diseñan con varios gateways IP entre sus subredes principales.

Windows NT permite sacarle provecho a los gateways múltiples, de tal forma que el sistema será tolerante al fallo en caso de que el gateway por defecto no esté disponible. Para cada tarjeta de red en la que se vaya a usar TCP/IP se pueden especificar tantos gateways de seguridad como gateways se tengan disponibles. Si el gateway por defecto falla, NT intentará usar automáticamente en el orden listado cada uno de los gateways IP que se tengan disponibles, hasta que encuentre uno que funciona correctamente.

Se utilizará el botón Agregar en el grupo de gateways para añadir cualquier gateway adicional disponible al interfaz seleccionado.

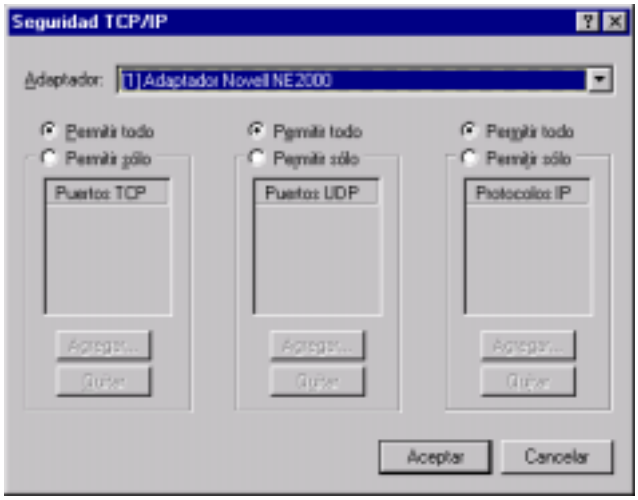
Filtrado PPTP

Windows NT incluye una nueva tecnología denominada Protocolo de Transferencia Punto a Punto (PPTP) que permite construir redes privadas seguras dentro de redes de transmisión públicas, siendo capaz de encapsular los diferentes protocolos de red empleados en NT, como son NETBEUI, TCP/IP y IPX/SPX. Este protocolo utiliza cifrado de los paquetes, y algoritmos de clave pública que hacen muy difícil examinar los paquetes enviados a través de una red como puede ser Internet.

Si se está usando PPTP y se desea restringir el acceso de red a PPTP, se debe habilitar la opción Filtrado PPTP.

Seguridad TCP/IP

Otra de las prestaciones de Windows NT 4 es la posibilidad de filtrar el tráfico de red mediante TCP o por el número de puerto UDP, así como el valor del protocolo IP. Esto permitirá controlar el tipo de tráfico TCP (IP al que el servidor responderá), facilitando un mayor nivel de seguridad.



Si se desea hacer filtrado IP o a nivel de puerto, deberá seleccionarse la opción Activar Seguridad, y a continuación pulsar el botón Configurar. Esto mostrará la ventana Seguridad TCP/IP.

Si se quieren activar ciertos puertos TCP o UDP, deberá seleccionarse la opción Permitir sólo sobre el campo apropiado, a continuación pulsar el botón Agregar para añadir las direcciones de los puertos TCP o UDP que se quieran permitir. Las direcciones válidas se encuentran entre 1 y 65.335.

Si se quiere habilitar cierto protocolo IP, se seleccionará la opción Permitir sólo sobre el campo de Protocolos IP. A continuación pulsar el botón Añadir para añadir los valores del protocolo IP que se quieran permitir. Los valores válidos para el protocolo IP se encuentran entre 1 y 255.

APENDICE B

Comando ping

Este comando se emplea desde la línea de comando de la ventana DOS y permite comprobar la accesibilidad de un nodo remoto generano un mensaje ICMP “echo request”.

C:\WINDOWS>ping

La sintaxis de este comando y sus opciones está descrita en la tabla siguiente:

Uso: ping [-t] [-a] [-n cantidad] [-l tamaño] [-f] [-i TTL] [-v TOS] [-r cantidad] [-s cantidad] [[-j lista de host] | [-k lista de host]] [-w Tiempo de espera agotado] lista de destino

Opción	**Explicación**
-t	Solicita eco al host hasta ser interrumpido. Para ver estadísticas y continuar: presione Ctrl-Inter. Para interrumpir: presione Ctrl-C.
-a	Resuelve direcciones a nombres de host.
-n cantidad	Cantidad de solicitudes de eco a enviar.
-l tamaño	Tamaño del búfer de envíos.
-f	No fragmentar el paquete.
-i TTL	Tiempo de vida.
-v TOS	Tipo de servicio.
-r cantidad	Registrar la ruta para esta cantidad de saltos.
-s cantidad	Registrar horarios para esta cantidad de saltos.
- j lista de hosts	Ruta origen variable en la lista de host.
-k lista de hosts	Ruta origen estricta en la lista de host.

APENDICE C

Comando route

Este comando permite controlar las tablas de enrutamiento. Su sintaxis y sus opciones está descrita en la tabla siguiente:

ROUTE [-f] [comando [destino] [MASK máscara] [puerta][METRIC métrica]]

Opción	Explicación
-f	Borra de las tablas de enrutamiento todas las entradas de las puertas de enlace. Cuando se utiliza junto con otro comando, las entradas se eliminan antes de ejecutar el comando.
Comando	PRINT Imprime una ruta ADD Agrega una ruta DELETE Elimina una ruta CHANGE Modifica una ruta existente
Destino	Especifica el host de destino.
MASK	Si la clave MASK está presente, el siguiente parámetro es interpretado como el parámetro de la máscara de red.
Máscara	Especifica un valor de máscara de subred asociado con esta ruta. Si no se especifica, se predermina a 255.255.255.255.
Puerta	Especifica la puerta de enlace.
METRIC	Especifica que el siguiente parámetro 'métrica' es el costo para este destino

Ejemplos:

> route PRINT
> route ADD 157.0.0.0 MASK 255.0.0.0 157.55.80.1 METRIC 3
> route DELETE 157.0.0.0

APENDICE D

¿Qué es el Monitor de Red?

El Monitor de Red es un componente de Microsoft System Management Server (SMS) que se puede utilizar para detectar y resolver problemas en redes LAN o redes WAN conectadas al Servicio de Acceso Remoto (RAS) de Microsoft.

Con el Monitor de Red podemos analizar y monitorizar el tráfico de la red, así como detectar los posibles problemas que puedan surgir. Por ejemplo, podemos detectar un equipo que hace un número desproporcionado de peticiones o identificar usuarios no autorizados en nuestra red.

¿Qué puede hacer el Monitor de Red?

- Capturar paquetes directamente de la red.
- Visualizar y filtrar los paquetes capturados.
- Capturar paquetes de una computadora remota y visualizar estadísticas locales en intervalos predefinidos.
- Editar los paquetes capturados.

¿Cómo trabaja el Monitor de Red?

El Monitor de Red rastrea el flujo de la red, que consiste en toda la información transferida a través de la red en cualquier momento. Antes de la transmisión, el software de funcionamiento de la red divide dicha información en segmentos de menor tamaño denominados frames o paquetes. Cada paquete contiene la siguiente información:

- Dirección fuente de la máquina que envía el mensaje.
- Dirección destino de la máquina que recibe el mensaje.
- Información de cabecera de cada protocolo utilizado para enviar el mensaje.
- Los datos que son enviados al destino.

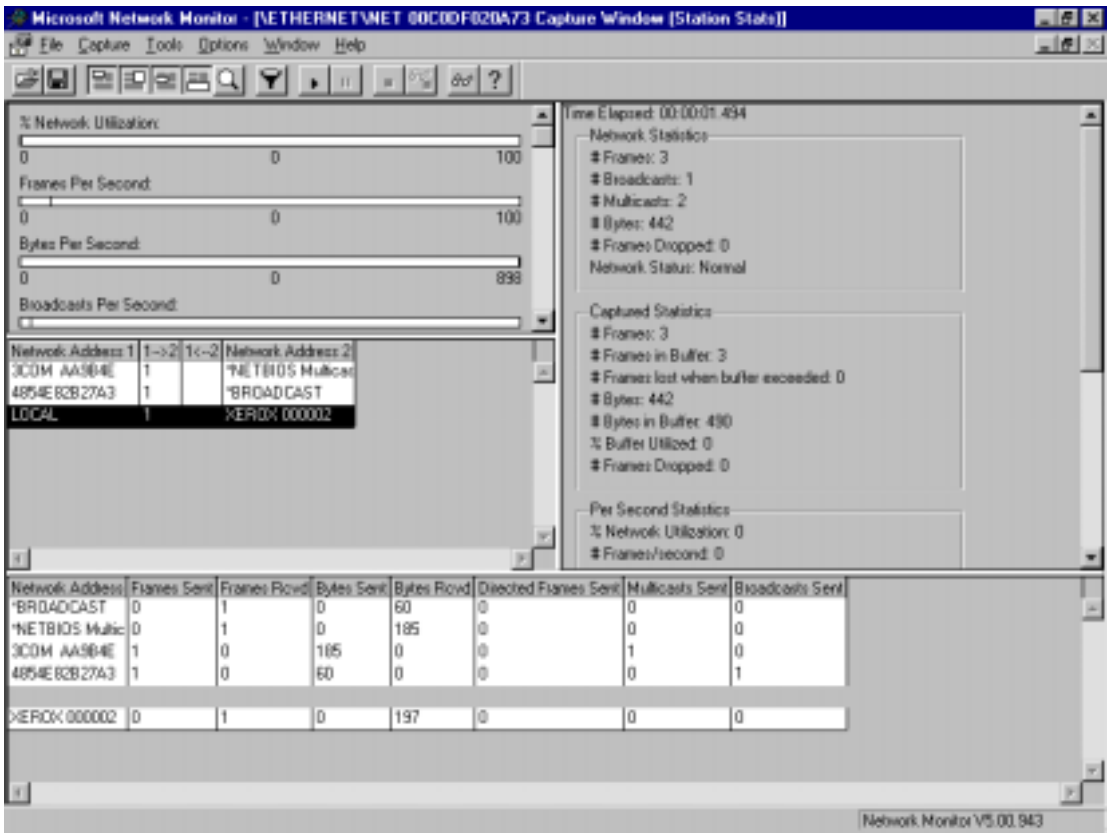
Todos los paquetes de un segmento de red pasa por todas las máquinas conectadas al segmento. Sin embargo, la tarjeta de red normalmente pasa al software de red solamente los paquetes dirigidos a la máquina destino. Un adaptador que pasa al software de red todos los paquetes que son transmitidos por la red funciona en modo promiscuo. El Monitor de Red copia todos los paquetes detectados a un archivo de captura temporal.

¿Cómo iniciar el programa?

Pulsamos Inicio, Programas, System Management Server y Network Monitor. En ese momento se abrirá el programa.

Ventana de captura

La ventana de captura tiene el siguiente formato:



Mientras el Monitor de Red captura paquetes de la red, aparecen las estadísticas sobre dichos paquetes en la ventana de captura, que se divide en cuatro paneles:

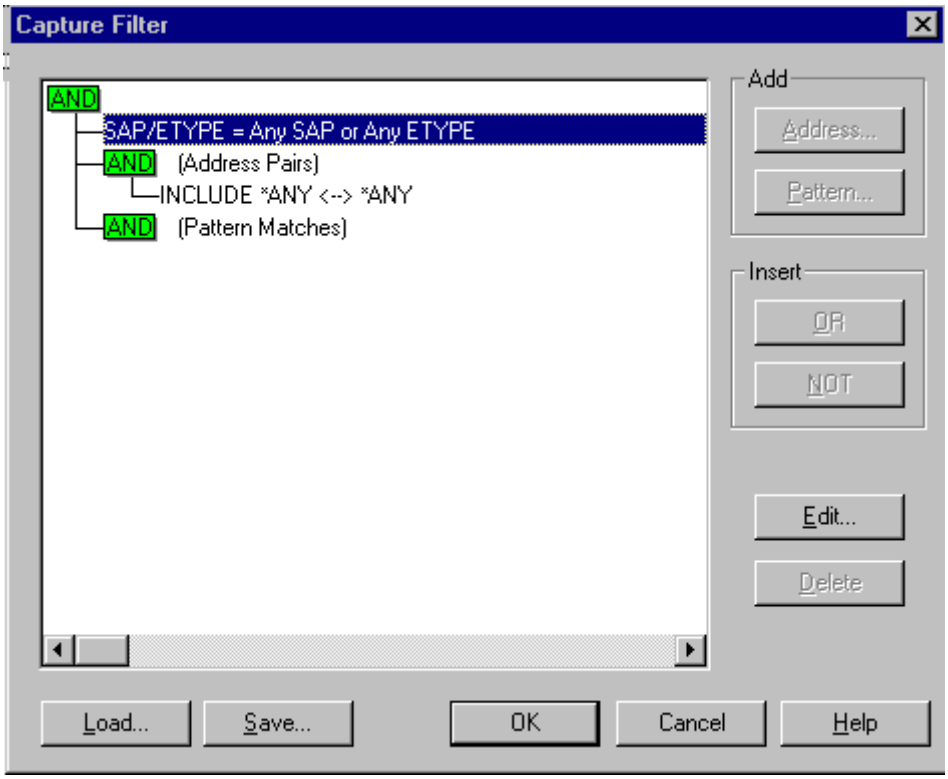
Panel	Visualiza
Gráfico	Incluye unas barras horizontales que muestran el porcentaje de utilización de la red. Las barras horizontales que se muestran son Tramas por segundo, Bytes por segundo, Broadcasts por segundo y multicasts por segundo.
Estadísticas de sesión	Es un resumen de las transacciones entre dos nodos y muestra cuál de los dos nodos inició el broadcast o el multicast.
Estadísticas totales	Son estadísticas del tráfico de la red, generalmente las tramas capturadas, estadísticas por segundo.
Estadísticas de la estación	Es un resumen del número de tramas y bytes enviados y recibidos, del número de tramas iniciadas por un nodo y el número de broadcasts y multicasts.

¿Cómo realizar un filtro para capturar?

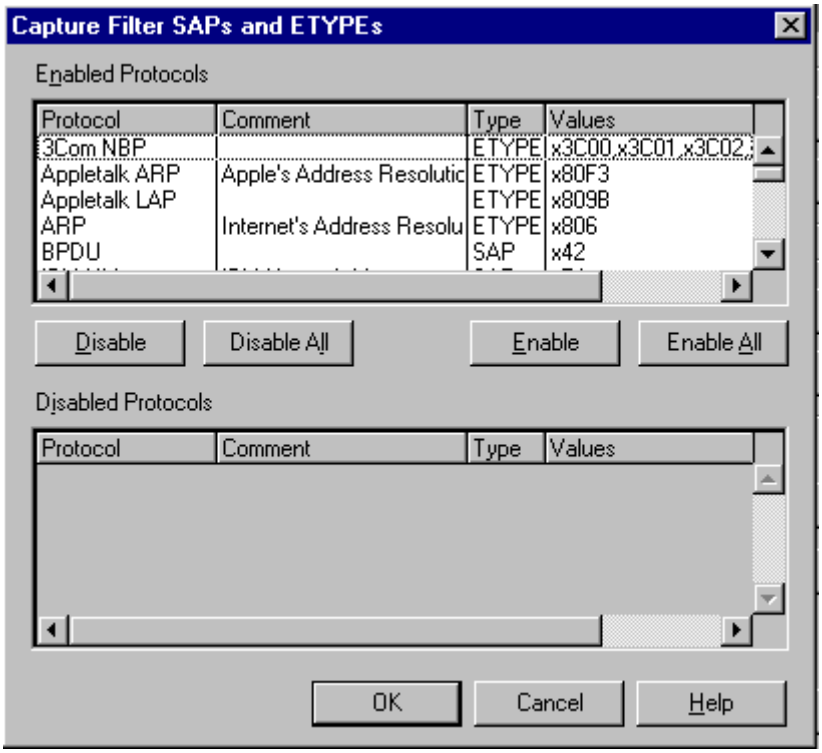
En redes grandes se capturará tráfico proveniente de muchas estaciones. Es por tanto interesante ser capaz de realizar un filtro para capturar sólo el tráfico deseado, de manera que es más fácil interpretar los resultados.

Para establecer un filtro se siguen los siguientes pasos:

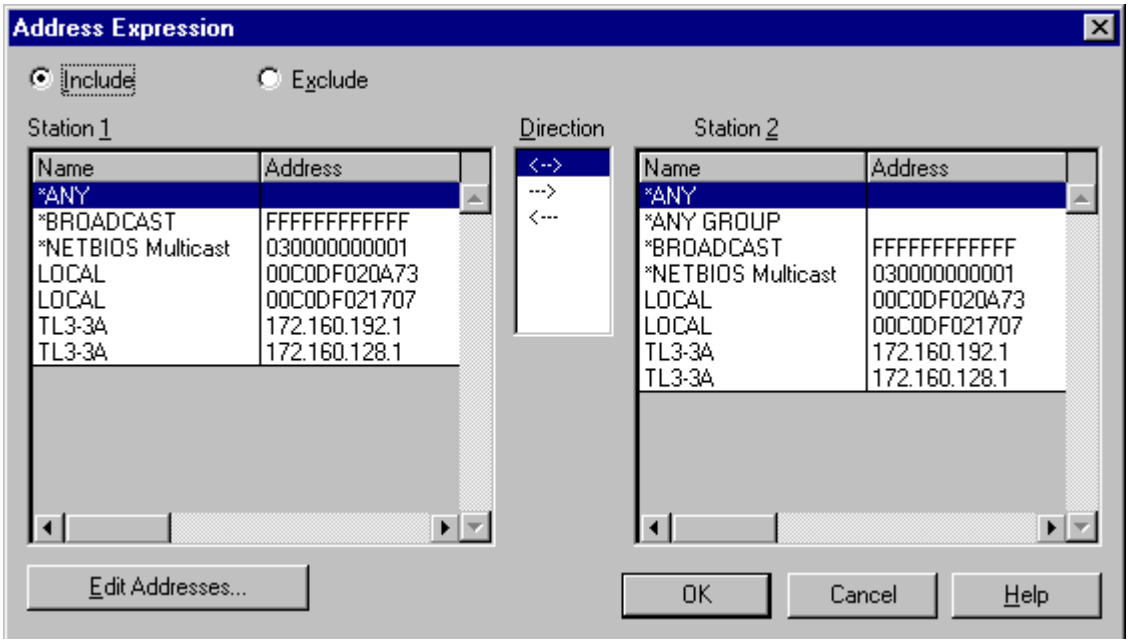
1. Iniciar el monitor de red.
2. Seleccionar Capture, Filter. También pulsando F8.
3. En la ventana que se muestra a continuación, hacer doble clic en SAP/ETYPE = Any SAP or Any ETYPE.



4. Aparecerá entonces la pantalla que se muestra en la primera figura de la siguiente página, en la que seleccionaremos el protocolo que deseamos capturar.
5. Por defecto todos los protocolos están seleccionados.
6. Se pueden seleccionar uno, seleccionar todos, deshabilitar uno o deshabilitar todos los protocolos.
7. Por ejemplo, seleccionamos sólo los protocolos ARP, IP con valor SAP 6 y IP con valor ETYPE 800 (hex).
8. Seleccionamos OK.



9. Tras seleccionar el protocolo, volvemos a la ventana Capture Filter. Pulsamos en INCLUDE ANY <->ANY y se mostrará la siguiente pantalla. Ahora podremos seleccionar el origen y el destino del paquete a filtrar.



10. Seleccionamos OK en la ventana Capture Filter y habremos terminado de definir el filtro.
11. Tenemos la posibilidad de grabar el filtro definido para utilizarlo en un futuro. Se grabará con la opción Save del menú File.
12. Damos un nombre al filtro, por ejemplo SOLOIP.CAP.
13. Podemos cargar el filtro cuando queramos para comenzar con la captura de paquetes.

Con el fin de poder comenzar a capturar paquetes, se puede pulsar F10, seleccionar la opción Start del menú Capture, o pulsar el icono Play de la barra de herramientas. Si el equipo se encuentra conectado a la red, comenzamos a ver estadísticas del tráfico capturado como son tramas por segundo, bytes por segundo...

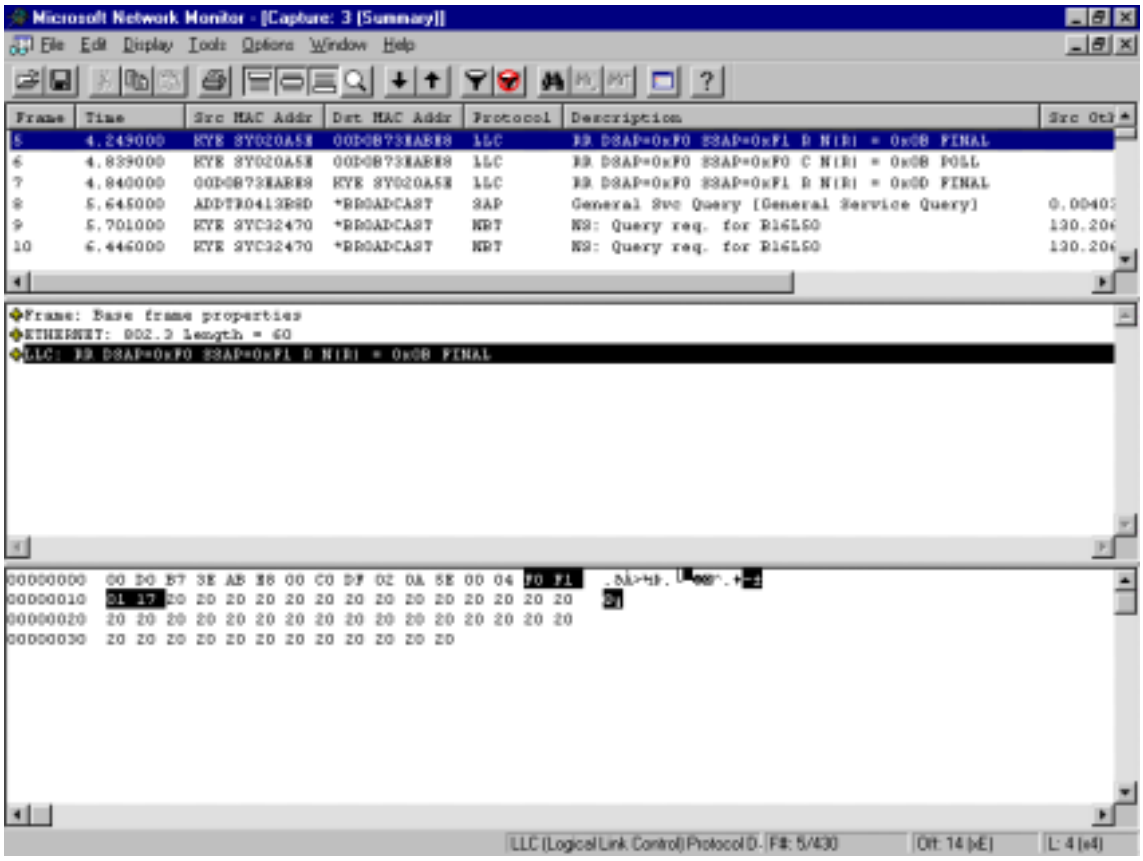
Ventana de Visor de paquetes

Después de que el Monitor de Red captura los paquetes, podemos utilizar la ventana Visor de Paquetes para visualizar sus contenidos. Esta ventana se muestra:

- Seleccionando Stop and view del menú Capture durante la captura.
- Abriendo un fichero de captura (.cap).

Esta ventana tiene tres paneles:

Panel	Visualiza
Panel de detalle	Muestra la información de protocolo para la trama seleccionada en el panel de Resumen. Cuando un protocolo está seleccionado en este panel, la información equivalente hexadecimal está en negrita en el siguiente panel.
Panel hexadecimal	Muestra el contenido de la trama en hexadecimal.
Resumen	Este panel muestra información acerca de las tramas capturadas. Los datos que se muestran son el número de trama, hora de captura, dirección hardware de la máquina que envió la trama, dirección hardware de la máquina que recibió la trama, protocolo usado para el envío de la trama, descripción de la trama enviada, otra dirección del emisor aparte de la dirección MAC (como puede ser la dirección IP o IPX), otra dirección del receptor de la trama y una última columna que indica el otro tipo de dirección que se ha mostrado en las dos columnas anteriores.



Estando situados en la ventana del Visor de Paquetes, si pulsamos sobre la descripción de un paquete en el panel de resumen, en el panel de detalle se muestra el paquete en cuestión.

Vemos que hay unos símbolos de + a la izquierda, lo que significa que hay más información por debajo de ese nivel de detalle. Al pulsar en ese símbolo +, aparecerá el resto de la información. Si por el contrario pulsamos en el símbolo – desaparecerá la información de ese nivel y pasaremos al nivel superior.

En la figura anterior podemos ver el formato de la ventana de Visor de paquetes

En esta ventana deberemos interpretar los datos que se nos muestran para poder analizar el tráfico, los problemas... de la red.

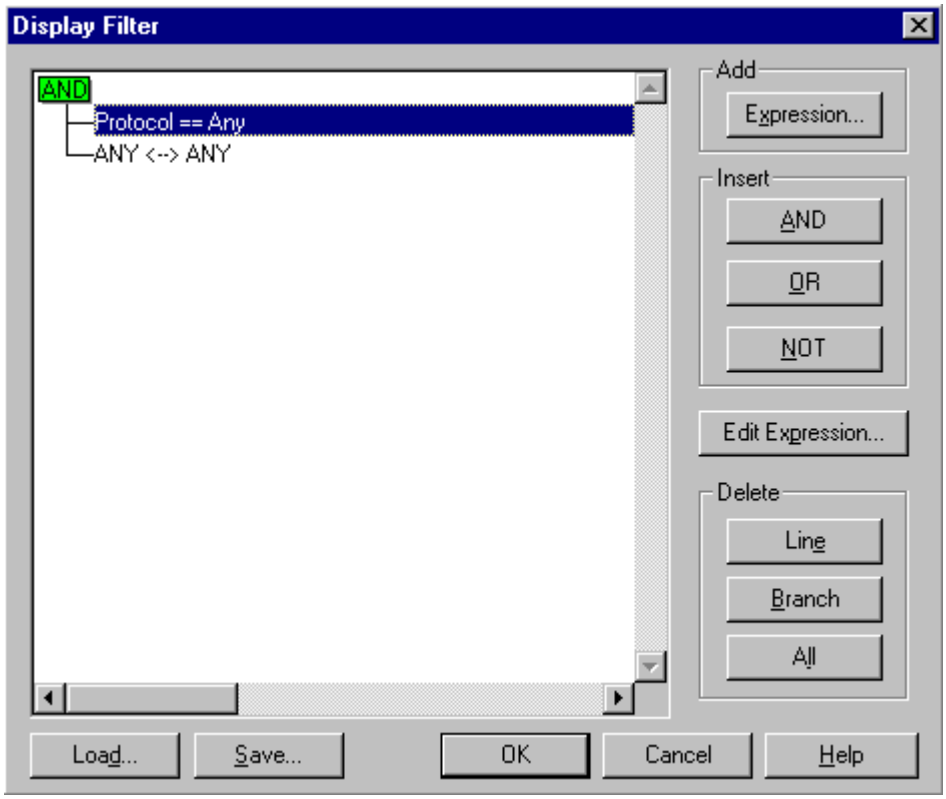
¿Cómo definir filtros sobre una captura terminada?

Cuando hemos llevado a cabo una captura y deseamos obtener los resultados de forma más clara, podemos realizar un filtro sobre la captura. Por ejemplo si de toda la captura deseamos ver sólo los paquetes relacionados con RIP.

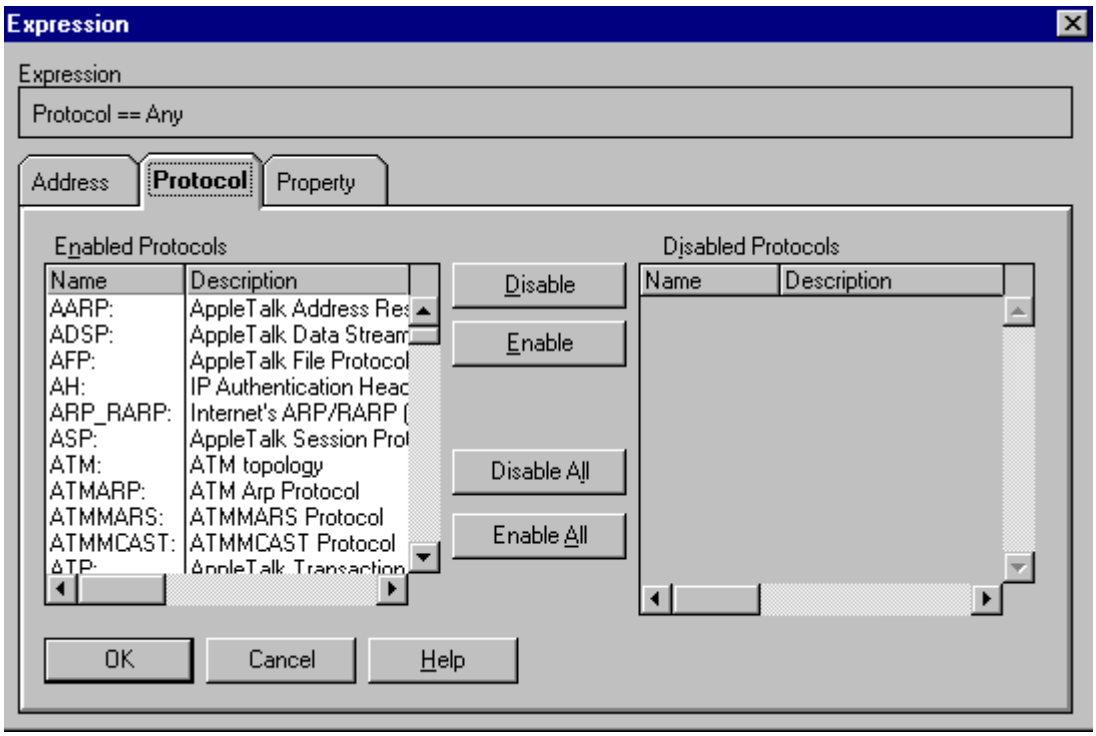
Pasos para definir el filtro:

1. Estando en la ventana del Visor de paquetes.
2. En el menú Display seleccionamos Filter o podemos pulsar el icono de la barra de herramientas siguiente:

3. A continuación se mostrará la siguiente ventana, la ventana de Visualizar Filtro:



4. En esta ventana podemos seleccionar el protocolo a filtrar, así como el destino y origen de los paquetes. Si pulsamos sobre PROTOCOL==ANY o sobre ANY<->ANY, se mostrará la siguiente pantalla:



5. Para finalizar el filtro pulsamos OK y a continuación aparecerán en la ventana del Visor de Paquetes solamente los paquetes del protocolo filtrado y en las direcciones seleccionadas.

¿Cómo copiar el contenido de Panel de Detalle?

Para poder copiar el contenido del panel de detalle de un paquete determinado, seleccionamos el paquete en la ventana de resumen y pulsamos la opción Copy del menú Edit. Con cualquier editor de texto podremos pegarlo y veremos lo siguiente:

```
2 0.098000 LOCAL XEROX 000002 Bone Security Check (0x03)
Frame: Base frame properties
   Frame: Time of capture = 29/09/00 11:49:12.429
   Frame: Time delta from previous physical frame: 15000 microseconds
   Frame: Frame number: 2
   Frame: Total frame length: 197 bytes
   Frame: Capture frame length: 197 bytes
   Frame: Frame data: Number of data bytes remaining = 197 (0x00C5)
ETHERNET: 802.3 Length = 197
   ETHERNET: Destination address : 030000000002
      ETHERNET: .......1 = Group address
      ETHERNET: ......1. = Locally administered address
   ETHERNET: Source address : 00C0DF020A73
      ETHERNET: .......0 = No routing information present
      ETHERNET: ......0. = Universally administered address
   ETHERNET: Frame Length : 197 (0x00C5)
   ETHERNET: Data Length : 0x00B4 (180)
   ETHERNET: Ethernet Data: Number of data bytes remaining = 183 (0x00B7)
LLC: UI DSAP=0x03 SSAP=0x02 C
   LLC: DSAP = 0x03 : GROUP
   LLC: SSAP = 0x02: COMMAND
   LLC: Frame Category: Unnumbered Frame
   LLC: Command = UI
   LLC: LLC Data: Number of data bytes remaining = 180 (0x00B4)
Bone: Security Check (0x03)
   Bone: Signature = RTSS
   Bone: Command = Security Check (0x03)
   Bone: Flags = 0x00
00000:  03 00 00 00 00 02 00 C0 DF 02 0A 73 00 B4 03 02   .......ÀßŠ..s.´..
00010:  03 52 54 53 53 03 00 00 00 00 00 A8 00 01 00 00   .RTSS.....¨....
00020:  00 4D D7 8A E0 54 4C 33 2D 33 41 00 00 00 00 00   .M×ŠàTL3-3A.....
                                  .....
```

¿Cómo utilizar los Expertos del Monitor de Red?

Aunque con el Monitor de Red es posible capturar tramas y analizar la red, es complicado hacer un análisis completo si no se tiene un conocimiento detallado del tráfico de nuestra red. Este conocimiento detallado implica el examinar trama por trama los datos sabiendo qué servicio de la red genera cada trama. El Monitor de Red incluye un conjunto de expertos, que son unas herramientas automatizadas diseñadas para ayudar en la interpretación de la información capturada.

Se incluyen varios expertos con funciones diferentes:

Experto	**Función**
Experto de tiempo medio de respuesta del servidor	Calcula el tiempo medio de respuesta de un servidor de la red
Experto de propiedad de distribución	Calcula estadísticas para una propiedad específica encontrada en la secuencia de tramas de una captura
Experto de distribución de protocolo	Calcula estadísticas sobre la distribución de protocolos en las tramas de una captura
Experto en retransmisión TCP	Localiza todas las tramas TCP que han sido retransmitidas a la misma máquina en una captura
Experto de usuarios	Determina los remitentes y destinatarios en una captura basándose en las direcciones origen y destino de cada trama
Experto en composición de protocolo	Recompone los datos para una transacción que ha sido enviada en múltiples tramas por la red

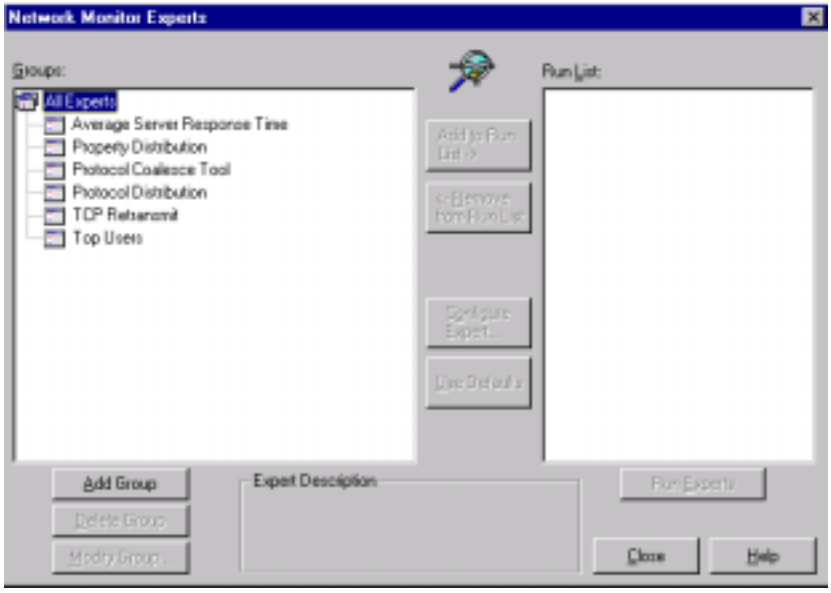
Primeramente deberemos realizar la captura tal y como se ha explicado anteriormente. Una vez finalizada (seleccionar la opción stop & view), en el menú tools escogemos Experts.

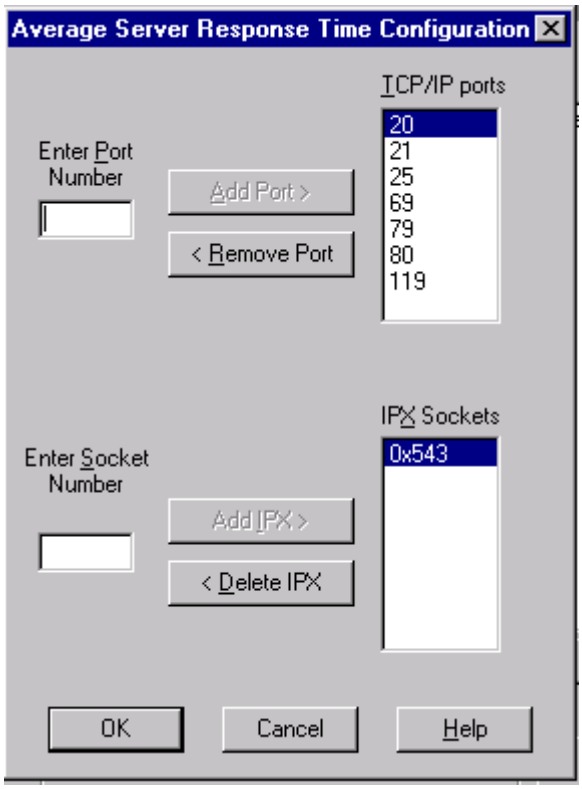
En este momento aparece una pantalla como la que se muestra en la siguiente figura, en la que se debería seleccionar el experto a ejecutar. Los expertos que aparecen en la parte izquierda de la ventana son los que no están seleccionados actualmente, y los de la parte derecha sin embargo, son los seleccionados. Para seleccionar un experto, haremos doble click sobre el experto en cuestión o podemos seleccionarlo y pulsar Add to Run List.

Para dejar de ejecutar un experto, hacemos doble click en el experto de la parte derecha de la ventana o pulsamos Remove from Run List.

Una vez seleccionados los expertos deberemos configurarlos. Para ello pulsamos el botón Configure Expert y rellenaremos los campos requeridos para cada experto.

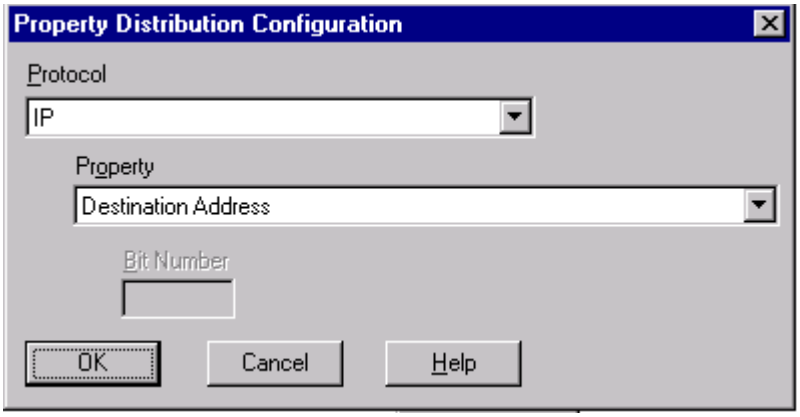
En este momento el experto estará en condiciones de ejecutarse, para lo que deberemos pulsar el botón Run expert.





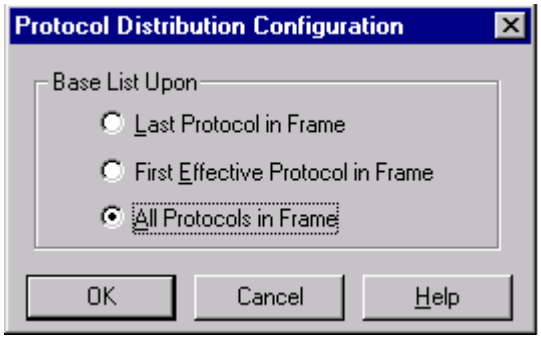
Tiempo medio de respuesta del servidor

En esta ventana de configuración indicaremos al experto los puertos TCP y sockets IPX que deberá monitorizar. Una vez configurado pulsamos Run expert y se mostrará un informe con los resultados de ejecutar dicho experto con la configuración indicada. Algunos de los datos que se mostrarán son el servidor, el tiempo medio de respuesta en segundos y el número de respuestas.



Propiedad de distribución:

Seleccionamos el protocolo y la propiedad a investigar en la captura realizada. Una vez ejecutado, el experto mostrará un informe con el protocolo, la propiedad seleccionada, el número de frames que cumplen dicha propiedad y el porcentaje que supone esa cantidad de tramas en la captura.

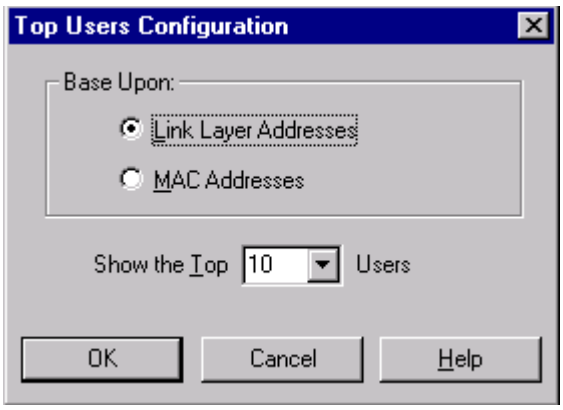


Experto de distribucion de protocolo:

Seleccionamos el protocolo a investigar y el experto realizará un estudio de la presencia de dicho protocolo en la captura. Al finalizar nos mostrará una distribución de protocolos, con el número de tramas y bytes que corresponde a cada uno de ellos, visualizando los datos en números reales y en porcentajes.

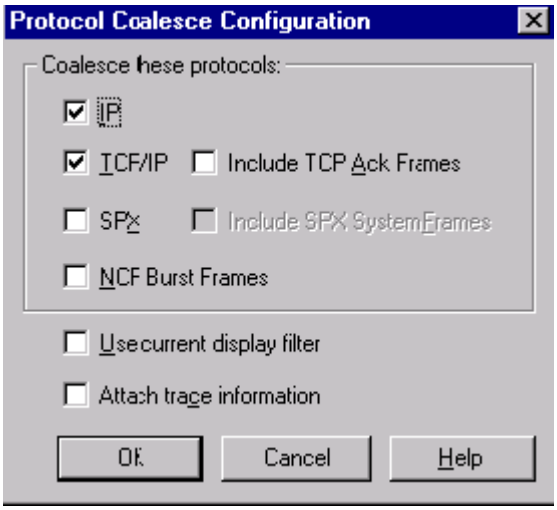
Experto TCP:

Este experto no hace falta configurarlo, por lo que deberemos seleccionarlo y ejecutarlo sin más. Nos mostrará una lista con todas las retransmisiones TCP realizadas en la captura, con sus direcciones origen y destino, hora...



Experto de usuarios:

Seleccionamos el tipo de direcciones en las que se basará el experto a la hora de ejecutarse, direcciones MAC o de capa de enlace. El experto mostrará un listado de paquetes en función de usuarios, direcciones origen, numero y porcentaje tanto de tramas como de bytes en la captura.



Experto en composicion de protocolo:

Seleccionamos el protocolo o protocolos a componer y el experto llevará a cabo la composición. Recompone los datos enviados en múltiples tramas con los protocolos seleccionados y mostrará el nombre y ruta al archivo que contiene la captura compuesta.

Gestionar monitores mediante la Herramienta del Monitor de Control:

Los monitores son herramientas que una vez configuradas y habilitadas, examinan continuamente el tráfico de la red en tiempo real para tratar de localizar unas condiciones específicas en la secuencia de tramas. Cada monitor es programado para detectar una condición o evento, que por ejemplo podría indicar la existencia de un problema en la red.

Cuando el monitor es habilitado y detecta una propiedad específica (pe una dirección IP inválida) o un evento (un router deja de anunciarse a sí mismo), genera un evento. En ese momento el monitor pasa la información en modo de evento al servicio del Monitor de Control, que tratará dicho evento.

La Herramienta del Monitor de Control se utilizará para configurar, iniciar y detener los monitores, así como para visualizar los eventos generados por los monitores activos. Deberemos configurar qué monitores estarán en funcionamiento y el tratamiento que se dará a sus eventos.

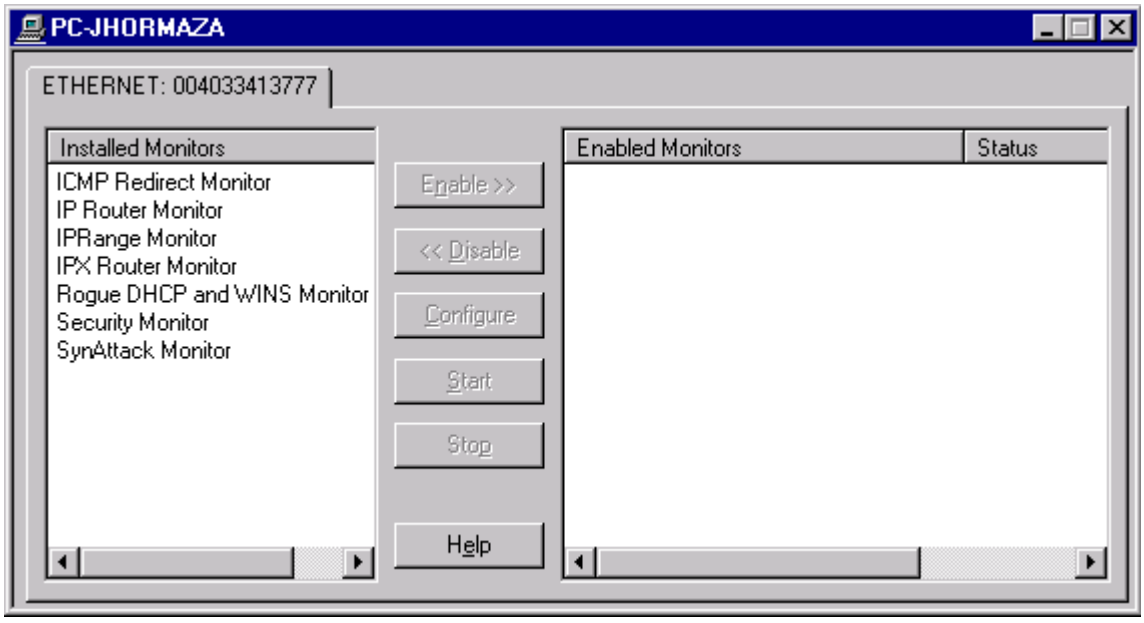
A continuación se listan los monitores disponibles:

Monitor	**Evento**
Monitor de redirección ICMP	Un router no autorizado de la red redirecciona tramas
Monitor de rango IP	Una trama tiene una dirección IP origen fuera de un rango sdefinido por el gestor
Monitor de routers IP	Un router IP de la red falla
Monitor Rogue	Servidor DHCP o WINS inválido o no autorizado localizado en la red
Monitor de seguridad	Instancias del Monitor de Red no autorizadas funcionando y capturando tramas en la red
Monitor SYN attack	Conexiones abiertas pero inactivas con servidores de la red

Para iniciar la herramienta de control del monitor de red: Inicio – Programas – SMS -Net monitor control tool. En ese momento se visualizará la pantalla que se muestra en la siguiente imagen.

Esta pantalla es similar a la de los expertos y en ella deberemos seleccionar los monitores a ejecutar. Para habilitarlos y deshabilitarlos pulsaremos los botones Enable y disable respectivamente.

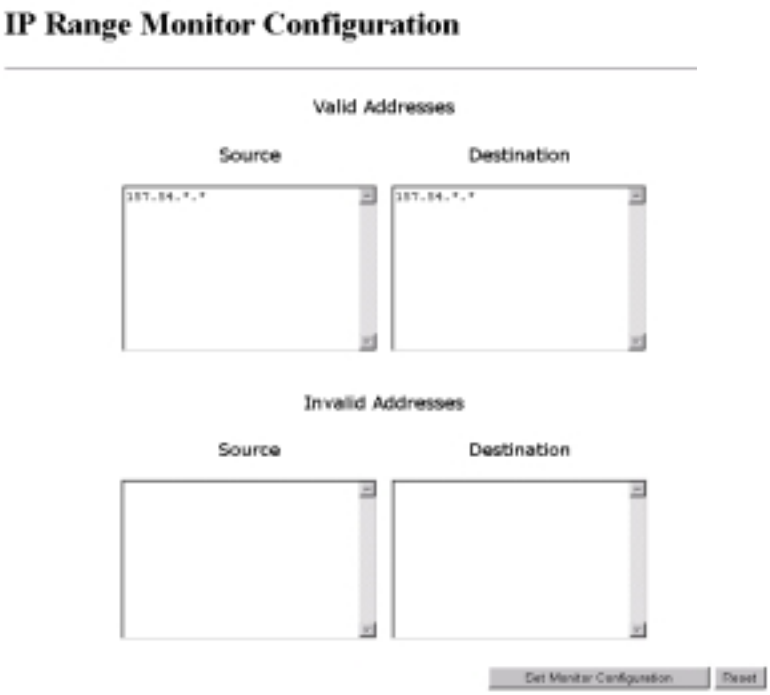
La herramienta nos preguntará si queremos configurar el monitor seleccionado. Cada monitor mostrará una interfaz de configuración diferente que veremos a continuación.



Monitor de redirección ICMP:

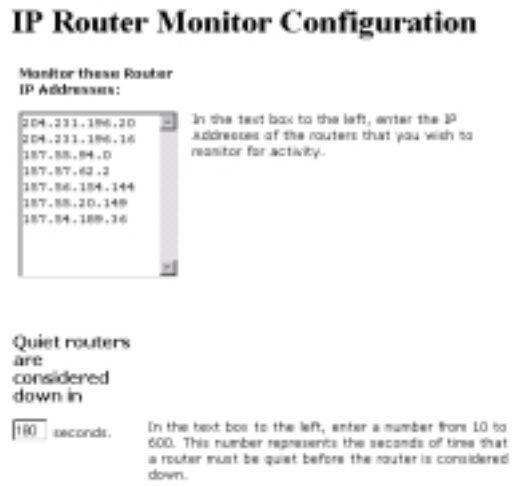
Especificar las direcciones IP de los routers autorizados para redireccionar tramas.

Pulsamos Set monitor configuration y Start. El monitor comienza a funcionar y en caso de que algún router no autorizado en la lista redireccione tramas, nos mostrará información acerca de dicho evento.



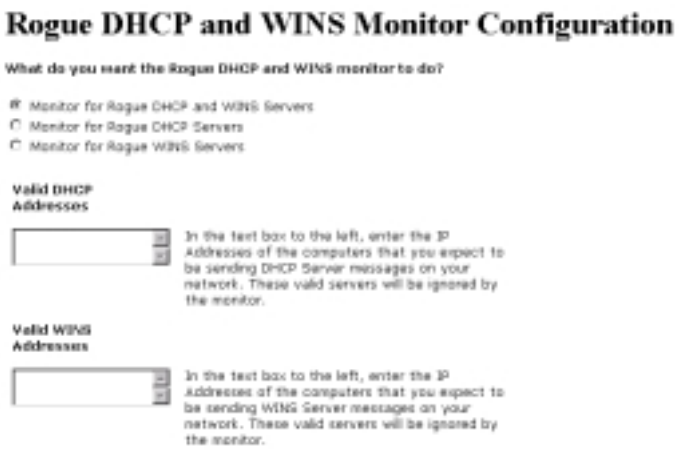
Monitor de rango IP:

Especificar rangos validos e invalidos de direcciones IP de origen y destino. En caso de localizar una trama que no cumpla esas condiciones, nos mostrará información del evento.



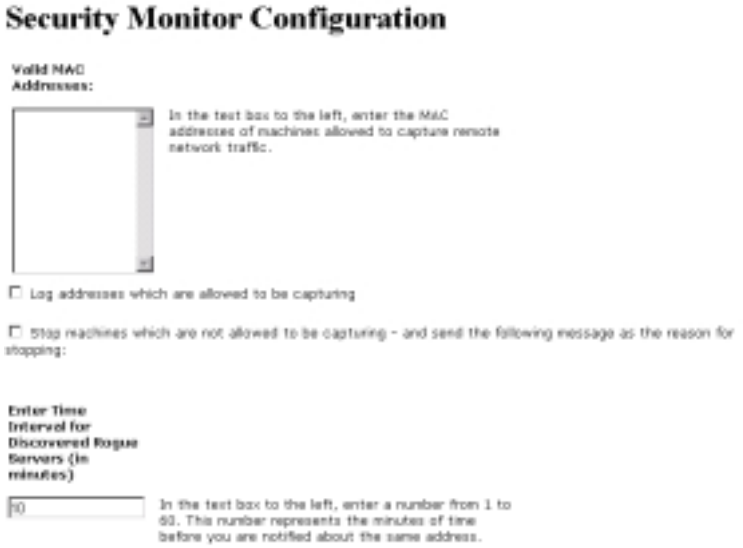
Monitor IP router:

Introducir las direcciones IP de los routers a monitorizar y el tiempo para considerarlos como fallidos.



Monitor rogue:

Primeramente indicamos qué tipo de servidores deseamos monitorizar, DHCP, WINS o ambos. A continuación introducimos las direcciones IP de los servidores DHCP y WINS válidos en la red y el tiempo en minutos antes de ser avisados de algún suceso.



Monitor de seguridad:

Aquí especificaremos las direcciones MAC de las instancias autorizadas a utilizar un monitor de red, si queremos llevar un registro de las instancias autorizadas cuando capturan, si apagaremos las máquinas no autorizadas que capturan y el mensaje que recibirán...

Monitor SYN attack:

Desde esta ventana configuramos las direcciones de los servidores a monitorizar y los diferentes parámetros, de forma que se localizarán las conexiones abiertas pero inactivas contra servidores de nuestra red.

Capturar tráfico en máquinas remotas:

El Monitor de Red captura solamente tráfico que circula por la tarjeta de red de la máquina en la que se ejecuta. Esto significa que sólo podemos capturar tráfico de nuestro segmento de red. Es posible capturar tráfico y generar estadísticas de tramas de otro segmento de red, ejecutando el Agente de Monitor de Red en la máquina situada en el otro segmento de red, conectando entonces la máquina local a la máquina remota.

A partir de ese momento la máquina remota lleva a cabo todas las capturas, transfiere las estadísticas a la máquina local y salva los ficheros de captura en el dispositivo de almacenamiento local.

Iniciar el agente en la máquina remota nos permite utilizar la tarjeta de red de nuestra máquina como si estuviera instalada en una máquina del otro segmento de red. Como cabe esperar, el modo de operar con las capturas es el mismo que funcionando en modo local.

Pasos a seguir:

1. Instalar el Agente de monitor de red en la máquina remota.
2. Iniciar el monitor de red en la máquina local.
3. Menu capture, seleccionar networks. En esa ventana expandir el elemento Remote y hacer doble click en remote NPPs.
4. En esa ventana indicar la dirección IP o el nombre de la máquina remota y OK.
5. Si la máquina remota tuviera más de un interfaz de red, seleccionar la deseada y OK.
6. Para iniciar la captura, en el menú capture seleccionar start.

APENDICE E

Comando arp

La sintaxis de este comando y sus opciones está descrita en la tabla siguiente:

C:\WINDOWS>ARP -a [dir_inet] [-N dir_if]

Opción	**Explicación**
-a	Muestra las entradas actuales de ARP preguntando por los datos del protocolo. Si se especifica dir_inet, se muestran las direcciones IP y Física sólo para el equipo especificado. Cuando ARP se utiliza en más de una interfaz de red, entonces se muestran entradas para cada tabla ARP.
dir_inet	Especifica una dirección internet.
-N dir_if	Muestra las entradas de ARP para las interfaces de red especificadas por dir_if.
-d	Elimina el host especificado por dir_inet.
-s	Agrega el host y asocia la dirección internet dir_inet con la dirección física dir_eth. La dirección física se especifica con 6 bytes en hexadecimal separados por guiones. La entrada es permanente.
dir_eth	Especifica una dirección física.
dir_if	Si está presente, especifica la dirección Internet de la interfaz con la tabla de traducción de direcciones a modificar. Si no se especifica, se utiliza la primera interfaz aplicable.