Analizador de protocolos TCP/IP para ayuda en la docencia de redes de computadores.

Román García, Miguel Mateo, Manuel Pérez
Dept. Informática de Sistemas y Computadoras
Universidad Politécnica de Valencia
46014 Valencia
e-mail: {roman,mimateo,mperez}@disca.upv.es

Resumen

Este documento describe el programa analizador de protocolos TCP/IP (denominado TCPMON), diseñado e implementado por el departamento DISCA de la Universidad Politécnica de Valencia para su uso, principalmente, en la docencia de las asignaturas de redes de computadores.

TCPMON es un programa para Windows 9x que permite capturar y analizar las tramas que circulan por la red. De esta manera se puede observar el funcionamiento de cualquier protocolo de red, lo cual es muy interesante para el estudiante de estas materias. TCPMON es también una poderosa herramienta para cualquier programador que desarrolle aplicaciones que utilicen la red.

1. Motivación

Un analizador de protocolos es una herramienta tradicional en el desarrollo y depuración de protocolos y aplicaciones de red. Una analizador de protocolos es un programa que permite al ordenador capturar tramas de la red para, posteriormente o en tiempo real, proceder a su análisis. Por analizar se entiende que el programa es capaz de reconocer que la trama capturada transporta información asociada a un protocolo concreto (por ejemplo a TCP, a ICMP,...) y muestra al usuario la información convenientemente decodificada. De esta manera el usuario puede, de forma cómoda, ver qué es lo que está circulando por la red. Esto es básico para un programador que éste desarrollando un protocolo (o cualquier programa que transmita y reciba datos de la red) ya que le permite comprobar qué es lo que realmente hace el programa.

Una analizador de protocolos es también útil a un estudiante que desee experimentar / comprobar cómo funcionan los protocolos tradicionales de red [1][2][5][6]. En nuestra experiencia personal, el estudio de un protocolo puede resultar poco ameno al alumno, sobre todo si el estudio se limita a la estructura y funcionalidad de las unidades de datos que el protocolo intercambia. El uso de un analizador es muy útil para clarificar la dinámica de un protocolo, al tiempo que refuerza la curiosidad del alumno por saber qué es lo que está circulando por la red. Además, permite al alumno comprobar la relación entre los diferentes protocolos, lo que facilita la comprensión de su funcionamiento.

Existen distintos tipos de analizadores disponibles comercialmente, y de distintos precios, pero normalmente son productos caros. El precio depende, en gran medida, de la capacidad de análisis (el número de protocolos que es capaz de reconocer y decodificar), de la tecnología de red soportadas (Ethernet, ATM, FDDI, ...) y de si se trata sólo de software (programas para PC) o si es un equipo hardware especializado.

En cualquier caso, hemos considerado que tiene interés desarrollar un analizador con fines docentes, de uso fácil y de libre distribución.

Por uso fácil queremos decir que el programa realiza exclusivamente las tareas que hemos considerado son las requeridas por nuestros alumnos. De esta manera, las opciones de configuración del programa son las justas y no se requiere que el alumno sea, en este momento, un experto capaz de entender todas las opciones posibles en un analizador comercial.

A continuación se describen la utilización y de la herramienta, junto con las conclusiones obtenidas durante su diseño y utilización.

2. El analizador TCPMON

2.1. Estructura interna de TCPMON

El programa se basa en la utilización de un Packet Driver [3][4] que permite el acceso a la interface NDIS de Windows. NDIS, a su vez, virtualiza el acceso al dispositivo de red, lo que permite desarrollar aplicaciones (como TCPMON) independientes del hardware de red utilizado por el PC (tarjetas Ethernet, Modems…)

La Figura 1 muestra la arquitectura de red en Windows y la ubicación de la interface NDIS y el Packet Driver (VPACKET en la figura). La referencia a "Win32 application" puede ser cualquier programa Windows, y en nuestro caso es TCPMON.

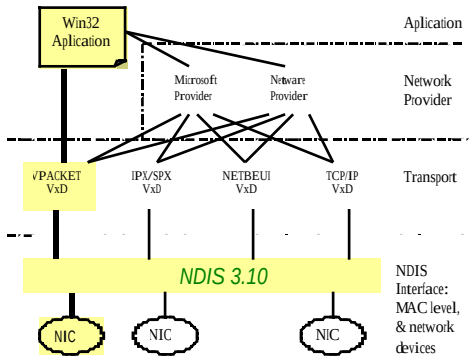


Figura 1:Arquitectura de red de Windows9x

2.2. Instalación: requerimientos del PC

TCPMON es un programa para plataformas Windows 9x. Para su correcto funcionamientoes necesario que el ordenador en el que se instale cumpla los siguientes requisitos:

1. PC compatible 486 o superior con, al menos, 32 Mbytes de RAM y 2 Mbytes libres de HD.
2. Sistema operativo Windows 9x y ME.
3. Adaptador de red con interface NDIS.
   El programa ha sido probado satisfactoriamente con tarjetas de red Ethernet, Fast Ethernet y con el Acceso Telefónico a Redes.

La instalación es totalmente automática, al estilo de la mayoría de los programas comerciales.

Nota: la utilización de una a CPU o una tarjeta de red poco potentes incrementada la posibilidad de pérdida de tramas. Es decir, existe la posibilidad de que el equipo no sea capaz de capturar todas las tramas que circulan por la red. Esta circunstancia, aunque poco frecuente, puede darse incluso en equipos muy potentes si el tráfico de la red es muy alto.

2.3. Características del programa analizador TCP/IP

1. Captura de tramas.
   El proceso de captura pregunta al usuario qué tipo de tramas desea capturar. Como puede observarse en la Figura 2, el programa puede capturar todas, pero sólo almacena las tramas que es capaz de analizar, y éstas son las que contienen los protocolos:
   a) ARP y RARP
   b) IP e ICMP
   c) UDP y TCP
   d) IGMP

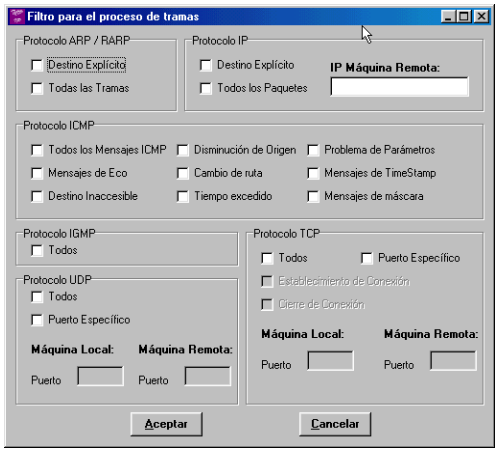


Figura 2: Configuración de la captura

2. Análisis de tramas.
   Este función es activada automáticamente tras la captura. También se puede activar sobre una captura previa almacenada en disco.
   El programa muestra la estructura de la trama y los protocolos en ella contenidos (ver

Figura 2). Por ejemplo, si se trata de una trama que contiene datos de una aplicación sobre TCP, se muestra:

a) Los campos de la trama.
b) Los campos del datagrama IP
c) Los campos del segmento TCP, y finalmente...
d) Los datos de la aplicación (estos últimos sin decodificar puesto que el analizador no conoce protocolos de aplicación)

3. Estadísticas de red.
   El programa también suministrará estadísticas, en formato numérico (%) y en formato gráfico (diagramas de tartas, gráficos de barras,...) del tráfico capturado. Existe la posibilidad de pedirle al programa que muestre estadísticas del tráfico actual sin que almacene las tramas que escucha. La figura 4 muestra distintas imágenes de la función "estadística".

4. Otras características
   Junto a las características principales ya comentadas, el programa dispone de un conjunto de facilidades básicas para hacerlo totalmente funcional, como son:
   a) Recuperación y almacenamiento en disco duro de sesiones capturadas.
   b) Opciones de búsqueda de una trama (por dirección física) en una sesión de captura.(Utilizada cuando la tarjeta es Ethernet)
   c) Opciones para personalizar la presentación de la aplicación (activar-desactivar la barra de menús, mostrar ventana de estadísticas…)
   d) Opciones de configuración
      Selección de la tarjeta de red con la que operará el analizado (en caso de que existan varias).
   e) Información sobre los parámetros operativos de la red.

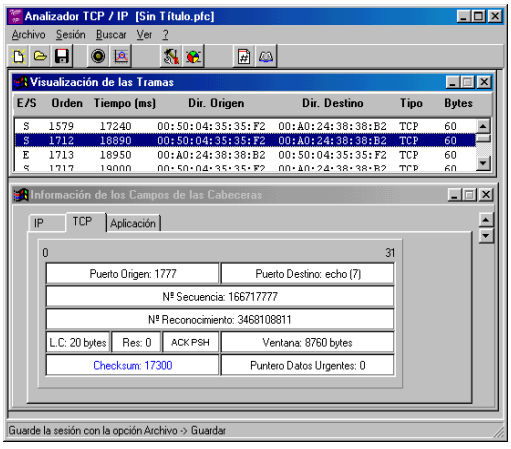
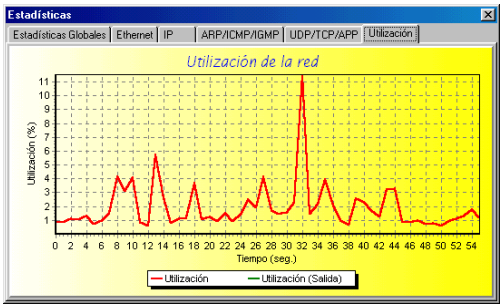
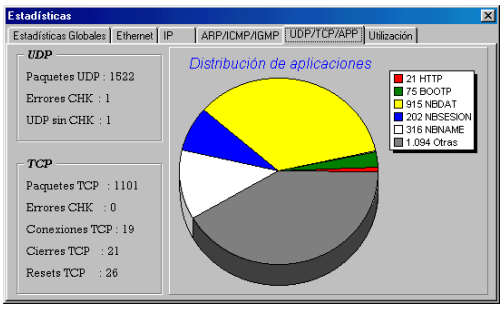


Figura 3: Ejemplo de captura (servicio *echo*).

(a)



(b)



(c)

Figura 4: Ejemplos de ventanas de estadísticas. De arriba abajo: (a) datos globales de captura , (b) utilización calculada y (c) distribución de las tramas en protocolos TCP/UDP .

3. Conclusiones

Esta “demo” presenta la aplicación TCPMON. Un analizador de protocolos con fines docentes y de libre distribución.

Es una herramienta básica para cualquier alumno de asignaturas de redes de computadores. El alumno puede utilizar TCPMON para observar la dinámica de los protocolos de red que estudia y también para depurar cualquier desarrollo de programas que utilicen la red para transmitir y recibir datos.

TCPMON funciona sobre el interface de red NDIS. Puede ser utilizado con el Acceso Telefónico a Redes de Windows (Modem) y con cualquier tarjeta de red. También es útil como analizador *off-line* para el estudio de una captura previa.

Referencias

[1] Comer, D.E., *Internetworking with TCP/IP Vol. I: Principles, Protocols, and Architecture*. Prentice-Hall 1995, ISBN 0130183806

[2] Comer, D.E., *Internetworking with TCP/IP Vol. III Client-Server Programming and Applications-Windows Sockets Version*. Prentice-Hall 1997. ISBN: 0138487146

[3] García, R., M. Pérez, J. Pons, *Redes1: Practicas Documentadas*, Servicio de publicaciones de la UPV nº 97.913

[4] Pérez M., R García. *La arquitectura TCP/IP: ejemplos practicos sobre Windows95*. Universidad Politécnica de Valencia. ISBN 84-7721-595-2

[5] Stallings W., *Data and Computer Communications*. Prentice-Hall 1996; ISBN: 0024154253

[6] Tanenbaum A., *Computer networks*, 3 Edition, Prentice Hall 1995.