MONITOR DE TRÁFICO IP PARA REDES ETHERNET

Guido Caicedo[1], Jorge Crespo[2], Eduardo Damian[2], Verónica Macías[2], Jorge Pérez[2], Jessica Suárez[2], Víctor Viejó[2], Marisol Villacrés[2]

RESUMEN

La mayoría de las herramientas de libre distribución existentes que permiten el análisis gráfico del tráfico de una red, son sistemas con funcionalidad limitada y poco amigables con el usuario. El sistema "Monitor de Tráfico IP para redes Ethernet" que se describe en este artículo ha sido diseñado atendiendo a las necesidades de los administradores de red de conocer mejor el comportamiento del Tráfico IP que se da sobre una Red Ethernet.

El Sistema sensa y almacena la información del tráfico en una red Ethernet, para que esta pueda ser consultada mediante un navegador Web. Las consultas pueden ser históricas o en línea y solamente podrán acceder a estas usuarios autorizados. Provee además un conjunto de herramientas de administración que permiten al Administrador de la Red un total dominio sobre la configuración del tipo de tráfico que se desea consultar, así como también del acceso al sistema en sí. Todo esto a través de una interfaz intuitiva y de fácil manejo. Al proveer la funcionalidad anteriormente descrita, se pretende que el Sistema "Monitor de Tráfico IP para redes Ethernet" sea una herramienta útil para la administración de redes.

1. INTRODUCCION

La Internet se ha convertido en la mayor fuente de información alrededor del mundo. Por ello el crecimiento vertiginoso del número de usuarios ha hecho del mantenimiento de las redes de computadoras una ardua y tediosa labor, sobre todo en el aprovechamiento de los recursos de ancho de banda y servidores de aplicaciones.

El sistema **Monitor de Tráfico IP para Redes Ethernet**, (al cual denominaremos de aquí en adelante como ***Monitor***) pretende ser una herramienta tanto para el administrador como para el usuario que permita ver las estadísticas del tráfico circulante por una red mediante la visualización de curvas de tráfico IP vs tiempo. Esta información, resulta muy valiosa y necesaria para el administrador ya que

[1] M. Sc. Ingeniero Eléctrico, Profesor, Facultad de Ingeniería en Electricidad y Computación, ESPOL, Guayaquil - Ecuador
[2]Ing. en Computación, Facultad de Ingeniería en Electricidad y Computación, ESPOL, Guayaquil - Ecuador

basado en esto, podría redistribuir el ancho de banda de algún enlace o en su defecto tomar decisiones relevantes en cuanto a la administración de la red

2. SISTEMA MONITOR

El sistema Monitor permite un análisis cuantitativo y cualitativo del tráfico IP de una red Ethernet mediante la visualización de curvas lineales, generadas a partir de los tipos de consulta gráfica que se pueden realizar. Estos tipos de consulta son:
Consulta en tiempo real, que permite consultar el tráfico que en ese momento esta circulando por la red.
Consulta histórica, mediante el cual se consulta del tráfico de periodos de monitoreo anteriores.

La operación del sistema se realiza desde un navegador de web autenticando al usuario que lo maneja, el cual puede ser un: usuario común o un usuario administrador

El sistema provee al usuario común la capacidad de:

- ✓ Consultar el estado en el que se encuentra el monitoreo de tráfico, (Estado del Monitoreo) pudiendo ser este activo o inactivo.
- ✓ Realizar las consultas gráficas basadas en las direcciones IP y los protocolos de aplicación disponibles. Estas consultas pueden hacerse para un rango de fecha dado o en tiempo real.
- ✓ Consultar las fechas en las cuales estuvo el monitoreo activo.

Por otro lado, el usuario administrador, además de las opciones disponibles para el usuario común tiene la capacidad de:

- ✓ Iniciar o detener el monitoreo de tráfico.
- ✓ Configurar características del sistema de monitoreo tales como:
  - ❑ Direcciones de red o estaciones de trabajo y protocolos de aplicación que estarán disponibles para que los usuarios hagan sus respectivas consultas.
  - ❑ Direcciones de red a excluir, es decir, direcciones de redes o estaciones de trabajo que no se considere convenientes de incluir en las consultas.
- ✓ Consultar o eliminar los datos de los intervalos de tiempo durante los cuales el monitoreo estuvo activo. De esta manera se hace un uso óptimo del espacio destinado para almacenar la información del monitoreo.
- ✓ Ingresar o eliminar a los usuarios que harán uso del Sistema de Monitoreo teniendo además la capacidad de editar la información concerniente a los mismos.

Las principales ventajas del sistema Monitor se podrían resumir en los siguientes puntos:

- ✓ *Acceso remoto:* Se permite el ingreso al sistema desde cualquier punto conectado a la red, ya que el usuario administrador tiene la capacidad de administrarlo desde cualquier estación de trabajo a través de un navegador web.

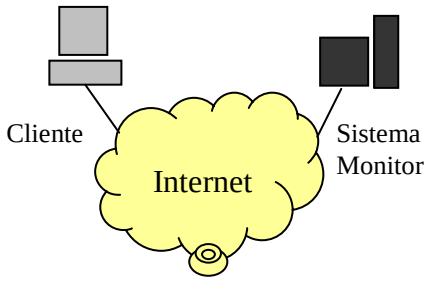

Fig. 1 *El Sistema Monitor permite un acceso remoto para su administración y uso.*

- ✓ *Seguridad y nivel de acceso:* el sistema puede ser accedido sólo por dos tipos de usuarios autorizados, uno de administración (usuario administrador) y otro de consulta (usuario común).

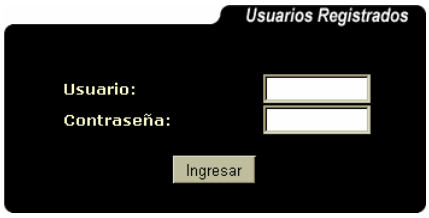

Fig. 2 El sistema autentica el uso del mismo mediante la petición de un usuario y una contraseña.

- ✓ *Herramientas de Administración:* Estas se proporcionan al administrador para que de esta manera tenga total dominio de la configuración del sistema.
- ✓ *Mayor retroalimentación y Ayuda en Línea:* Se da al usuario la información de los intervalos de tiempo en los cuales existen datos para que este pueda realizar consultas; así como también el momento en que cambia el estado de monitoreo, si este evento ocurriera. Se incluye un manual para el administrador así como también para el usuario para una mejor utilización del sistema.
- ✓ *Flexibilidad:* Permite la consulta del tréfico de cualquier protocolo de aplicación que el Administrador considere conveniente.
- ✓ *Multiplataforma:* Se desarrollaron versiones para Windows NT 4.0 y Linux.

3. ARQUITECTURA

El sistema Monitor consta de 5 componentes principales:

Base de Datos.
El almacenamiento de la información capturada y de los datos de configuración del sistema Monitor, se mantienen en una base de datos.
Dada la cantidad de información que se va a manejar, esto resulta más conveniente debido a la rapidez de acceso y la facilidad de manejo. Además de la información concerniente a cada paquete (direcciones IP fuente y destino), también se almacenan las fechas de inicio y pausa del monitoreo, número total de paquetes y bytes capturados durante este intervalo.

Monitor de Tráfico.
La recopilación de la información de los paquetes es un componente medular en el sistema, pues es mediante la captura de información que obtenemos los datos del tráfico existente en la red. El proceso captura todos los paquetes circulantes en la red y toma la información concerniente a cada paquete descrita anteriormente; luego de lo cual la almacena en la base de datos.

Servidor de Monitoreo General.
El servidor de monitoreo general consiste de un servidor WEB el mismo que cuenta con la facilidad de ejecutar *scipts* a través del estándar CGI. Estos *scipts* se encargan de atender los requerimientos de información concerniente a los Usuarios, direcciones IP, Protocolos de comunicación, configuración de consultas, consultas Históricas. Los scripts se encargan también de realizar las gráficas de "tráfico vs tiempo" para las consultas históricas basándose en los datos obtenidos de la Base y enviando luego esta información, mediante un archivo texto, al módulo graficador. Este a su vez construye un archivo de imagen en

formato GIF, el cual será referenciado por la página web que genera el script.

Servidor de estado y Monitoreo en Línea.

Ambos servicios se dan a través de un mismo servidor el cual está diseñado para atender ciertos requerimientos como servidor iterativo (cuando atiende los requerimientos denominados de monitoreo histórico, los cuales son: iniciar, detener o consultar el estado del monitoreo de tráfico) y otros como servidor concurrente (cuando necesita atender los requerimientos de las consultas en línea). Además este servidor tiene las siguientes características:

- *orientado a conexión,* para mantener una comunicación confiable.
- *Multiproceso* pues el sistema cuenta con dos procesos (*sockets*) para atender los requerimientos de los clientes: uno encargado de controlar la comunicación y otro de transferir de datos (muy parecido al FTP)

El funcionamiento del sistema es sencillo, del lado del servidor existe un *socket* (llamado socket de control)que se encuentra esperando por requerimientos. Cuando alguno llega, se abren un par de *sockets* adicionales, uno del lado del servidor (al que llamaremos socket de tranferencia) y otro del lado del cliente (denominado socket de recepción). Mediante el socket de control, el socket de recepción se encarga de comunicar al servidor los cambios que realice en la consulta, en tanto que mediante el socket de transferencia se envían los datos de tráfico IP según esté configurada la consulta.

Navegador de Web y Clientes.

El *Navegador Web* es el encargado de presentar la interfaz del sistema, realizar los requerimientos al servidor Web y cargar los *clientes* cuando los scripts de CGI's lo indiquen. Los *Clientes* que presenta el sistema son:

- ✓ **Cliente de Monitoreo en Línea:** es un Applet que se carga cuando el usuario realiza una consulta de tráfico en línea. Tiene como función principal graficar los datos del tráfico IP que haya sido seleccionado por el usuario.
- ✓ **Cliente de Estado:** Es un Applet que se carga cuando el usuario ingresa al sistema. Tiene como finalidad hacer que el estado del monitoreo esté siempre visible. Existen dos clientes de estado: uno para el usuario administrador, con el que puede cambiar el estado del monitoreo o simplemente consultarlo, y otro para el usuario común, con el que sólo muestra el estado actual del monitoreo.

En la **figura 3** podemos observar la relación de los diferentes componentes del sistema. Cuando un usuario se conecta al sitio web del sistema Monitor mediante un navegador, hace un requerimiento al Servidor Web, el cual muestra las páginas que los scripts de CGI's generen. A su vez los scripts invocan al programa graficador suministrándole los datos necesarios para que genere un archivo gráfico que muestre el tráfico IP vs tiempo de las consultas históricas. Además los scripts se comunican con la base de datos para mostrar, ingresar o eliminar los datos de configuración de monitoreo que el usuario requiera.

Si el usuario consulta el monitoreo en línea entonces se cargará el cliente

respectivo (applet), el que iniciará la conexión con el servidor de estado y monitoreo en línea.

Por último, el monitor de tráfico es el encargado de capturar la información necesaria sobre el tráfico IP circulante en una red Ethernet y almacenar esta información en una base de datos. Este proceso captura información cuando se activa el monitoreo desde el cliente de

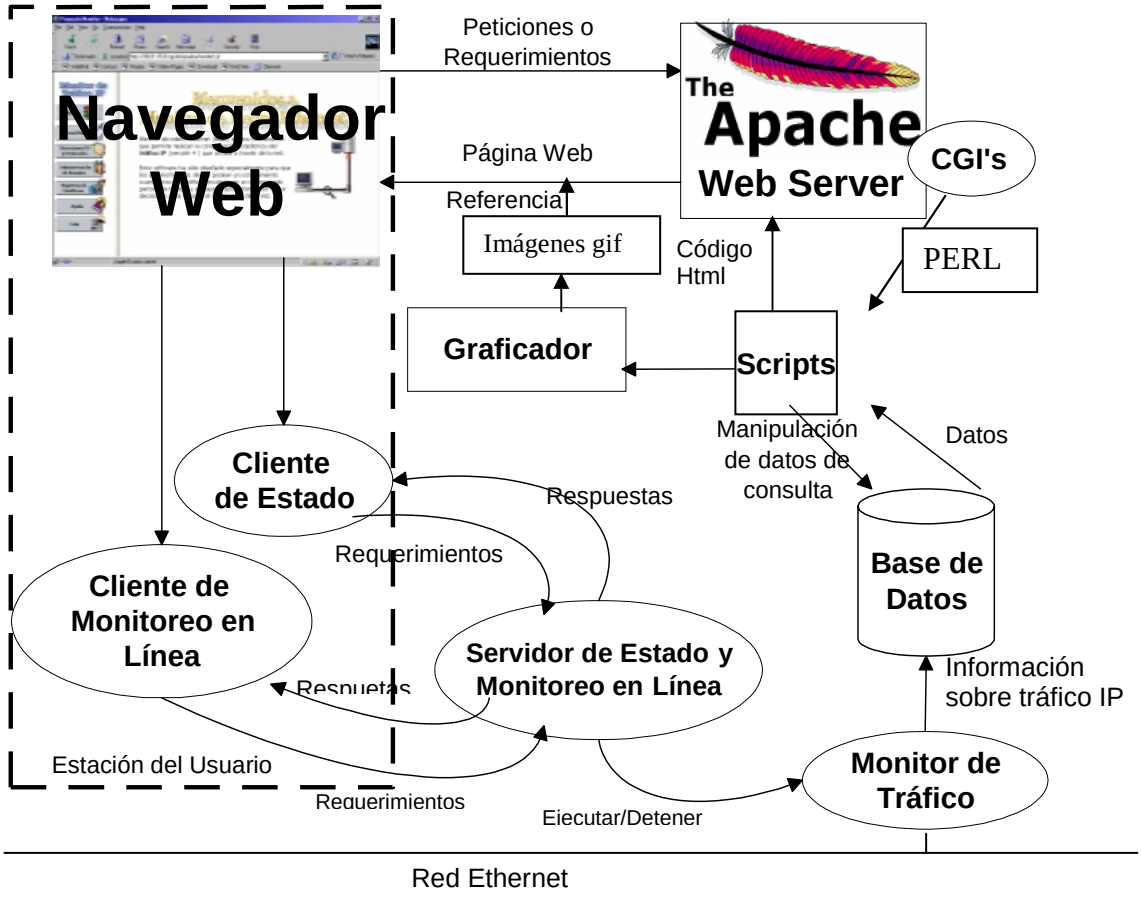

Fig. 3 Arquitectura del Sistema Monitor

estado.

4. CONCLUSIONES

Una vez realizada las pruebas respectivas, se puede concluir:

- ✓ Las Herramientas proporcionadas por el sistema Monitor satisfacen la mayoría de las necesidades de conocer mejor el comportamiento del tráfico de la red tanto de los usuarios como del Administrador.
- ✓ La información mostrada mediante las gráficas tales como: horas pico de tráfico, aplicaciones de mayor utilización, redes o estaciones que generan o reciben mayor tráfico, entre otras, resultan ser de vital importancia en la administración de la red, ya que de esta manera el Administrador puede redistribuir el ancho de banda disponible, para sacarle mayor provecho a los recursos de los que dispone.

5. BIBLIOGRAFIA

1. Douglas E. Comer, Internetworking with TCP/IP Vol. I: Principles, Protocols and Architecture, Publicado 1995

2. Douglas E. Comer / David L. Stevens, Internetworking with TCP/IP Vol. III, Client-Server Programming Aplications – winsock version, Publicado 1996

3. David Pitts / Bill Ball, Red Hat Linux 6, Publicado en 1999

4. J. Crespo, E. Damian, V. Macías, J. Pérez, J. Suárez, V. Viejó, M. Villacrés, "Análisis, Monitoreador de Tráfico IP para redes Ethernet" (Tópico de Graduación, Facultad de Ingeniería Eléctrica y Computación, Escuela Superior Politécnica del Litoral, 2000)