MONITOREADOR DE TRÁFICO IP PARA REDES ETHERNET

Jorge Crespo Cedeño[1], Eduardo Damian Malan[2], Verónica Macías Mendoza[3], Jorge Pérez Maldonado[4], Jessica Suárez García[5], Víctor Viejó Chabla[6], Marisol Villacrés Falconí[7], Guido Caicedo Rossi[8]

[1]Ingeniero en Computación 2000
[2]Ingeniero en Computación 2000
[3]Ingeniera en Computación 2000
[4]Ingeniero en Computación 2000
[5]Ingeniera en Computación 2000
[6]Ingeniero en Computación 2000
[7]Ingeniera en Computación 2000
[8]Director de Tópico. Ingeniero Eléctrico, Escuela Superior Politécnica del Litoral, Masterado EEUU, State University of New York 1993, Profesor de ESPOL desde 1990.

RESUMEN

El sistema "Monitoreador de Tráfico IP para redes Ethernet[1]" ha sido diseñado con el propósito de facilitar a los administradores de redes una herramienta capaz de monitorear el tráfico que pasa por una red específica.

Esta herramienta proporciona gráficos de tipo comparativo sobre el tráfico de una red, además permite la administración de recursos y de usuarios, así como también la configuración del mismo.

El software desarrollado ha sido dividido en tres módulos: el monitoreador del tráfico, la Interfase con el usuario y la base de datos.

El monitoreador del tráfico constituye la parte del sistema destinada a recopilar, seleccionar y guardar la información que resulta relevante para las consultas.

La Interfase se encarga de la interacción con el usuario. El administrador del sistema podrá por medio de ella manejar los recursos y realizar las consultas; mientras que, el usuario común podrá realizar solamente las consultas deseadas.

La base de datos resulta ser la conexión entre la interfase y el monitoreador de tráfico. Se utiliza para guardar la información en forma clasificada por medio de tablas.

INTRODUCCIÓN

Este proyecto tiene como precedentes dos aplicaciones anteriores, la primera realizada en Borland C++ 3.0 para Windows95. La otra aplicación fue desarrollada en el mismo lenguaje de programación para la captura, pero el acceso y administración se lo hacía vía web aplicando el paradigma Cliente/Servidor utilizando e lenguaje JAVA. Ambas aplicaciones sólo capturaban el tráfico correspondiente a ciertas direcciones IP y se guardaba en un archivo denominado “Archivo de Configuración”. Bajo esta perspectiva la segunda aplicación tenía un mejor ambiente de trabajo y podía ser administrado desde cualquier sitio conectado a la red donde se hallaba el sistema.

El sistema “Monitoreador de Tráfico IP para redes Ethernet” constituye una herramienta más sofisticada que las versiones anteriores, puesto que es capaz de:

- Mostrar gráficamente el tráfico TCP/IP existente en una red Ethernet
- Permitir el análisis comparativo entre las diferentes aplicaciones y/o protocolos de comunicación.
- Administrarlo y ejecutarlo desde un Navegador, facilitando el acceso desde cualquier punto de la red.
- Atender requerimientos de usuarios concurrentes.
- Brindar una interfaz amigable al usuario.

CONTENIDO

El sistema consta de 5 componentes principales:

1. Base de datos
2. Monitor de Tráfico
3. Servidor Monitoreo General
4. servidor de monitoreo en línea
5. Clientes JAVA.

La comunicación entre los componentes se ilustra en la figura 1.

El Almacenamiento de la información capturada y de los datos de configuración se lo

realiza en una base de datos, pues dada la cantidad de información que se va a manejar en cuanto al tráfico por estación de trabajo, resulta más conveniente por la rapidez de acceso y la facilidad de manejo.

Los datos a almacenar serán los concernientes a tráfico, direcciones IP de red y estaciones de Trabajo disponibles para las consultas, además de los usuarios que pueden acceder al sistema.

2.2. Monitor de Tráfico

La recopilación de la información del tráfico es un componente medular en el sistema, debido a que con esta información obtenemos los datos del tráfico existente en la red y que

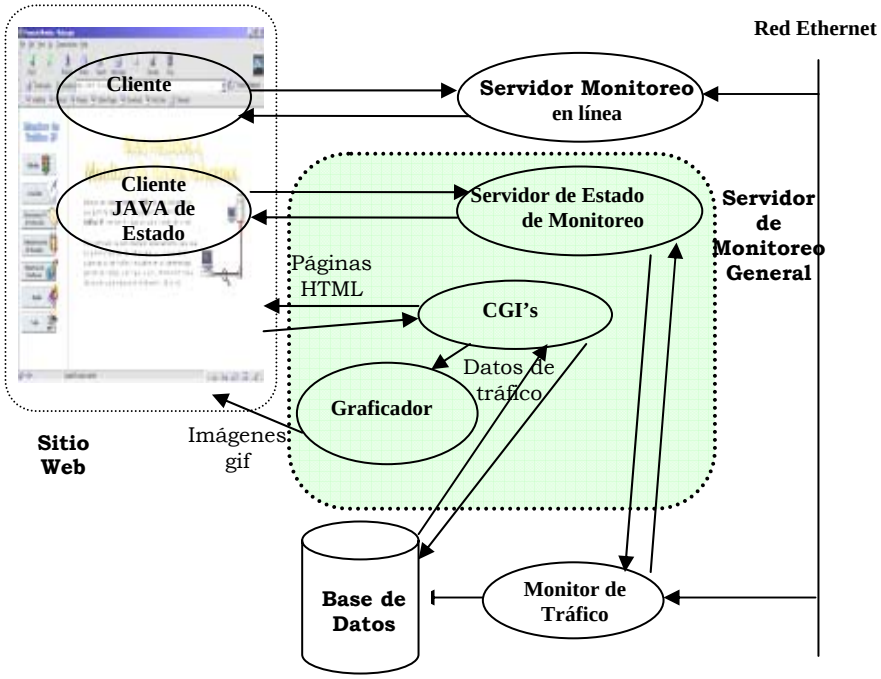

Figura 1 Estructura General

posteriormente servirán para construir las curvas de tráfico IP vs tiempo.

El proceso captura todos los paquetes circulantes en la red y toma cierta información para identificarlos; almacenándolos temporalmente en memoria principal por un minuto, luego de lo cual guarda en la base de datos la información obtenida (fig. 2).

Con el objeto de poder responder a posteriores requerimientos de una dirección IP cualquiera, el sistema captura todo el tráfico que circula en la red.

Además de la información concerniente a cada paquete, también se almacena la fecha de inicio y pausa del monitoreo, así como el número total de paquetes y bytes capturados durante este intervalo.

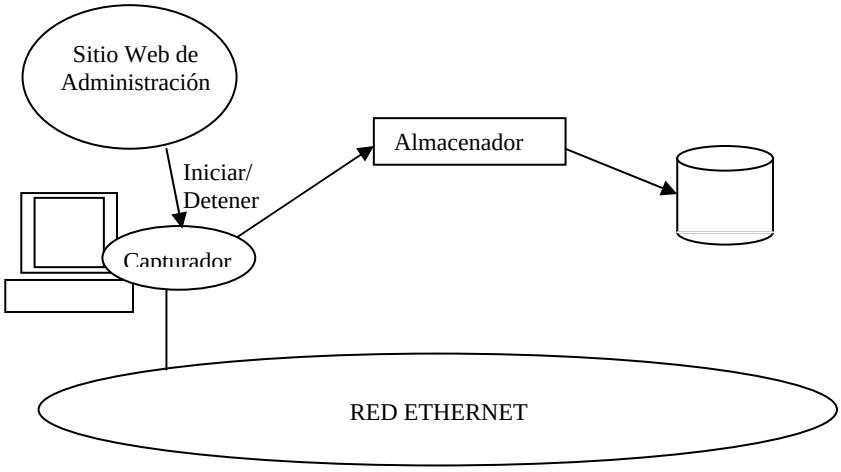

Figura 2 Esquema de Monitoreo de Tráfico

En cuanto a la capacidad de iniciar o detener la captura de información y de presentar siempre el estado del monitoreo, se optó hacerlo mediante un applet de java.

2.3. Servidor de Monitoreo General

Consta de tres módulos:

CGI's: encargados de responder a los requerimientos de administración de información de los Usuarios, direcciones IP, Protocolos de comunicación y configuración y consultas.

Graficador: Se encarga de realizar las gráficas de "tráfico vs tiempo" para las consultas históricas, en base a los datos generados por los CGI's obtenidos de la Base.

Servidor de Estado: Es el encargado de mostrar el estado en el que se encuentra el Monitoreo de tráfico, sea este Activo o Inactivo. Tiene dos variantes, una para el administrador y otra para el usuario. La diferencia estriba en que dado que el administrador tiene la capacidad de iniciar o detener el monitreo, el servidor de estado es el que se encarga de levantar o detener dicho servicio, en tanto que al usuario sólo le muestra el estado actual del monitoreo.

2.4. Servidor de Monitoreo en Línea

El servidor de *Monitoreo en línea* se encarga de responder a los requerimientos de consultas en línea. Este módulo cuenta con sus propios módulo de configuración

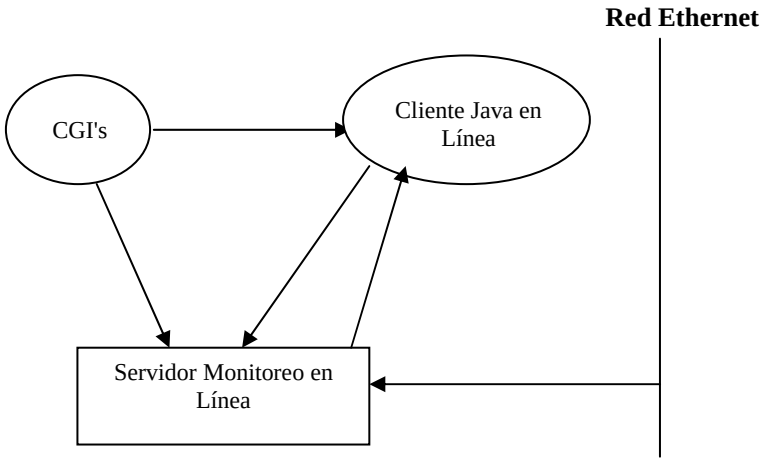

Figura 3. Servidor de monitoreo en Línea

-basados en una configuración inicial obtenida de los CGI´s- y de Monitoreo de Tráfico, para responder rápidamente y presentar tráfico por segundo (fig. 3).

2.5. Clientes JAVA

Cliente JAVA Monitoreo en Línea: El cliente Java del Monitoreo en línea es un Applet que se ejecuta cuando el usuario realiza una consulta en línea. Tiene como función principal mostrar los datos del tráfico IP que haya sido seleccionado por el usuario.

Cliente Java de Estado: Es un Applet que se ejecuta cuando el usuario ingresa al sistema. Tiene como finalidad hacer que el estado del monitoreo esté siempre visible al usuario.

CONCLUSIONES

El manejo de interface de red en la plataforma Linux resultó ser más eficiente que la implementada en la plataforma Windows NT debido a que en Linux, los controladores de interfase son residentes en el sistema operativo, mientras que en Windows NT se cargan cada vez que se realiza un requerimiento.

La implementación del sistema con una interface web permite que los usuarios del mismo accedan a este en forma remota.

El procesamiento multihilo facilitó el manejo de los requerimientos cuando el acceso al sistema de parte de los usuarios se torna concurrente.

El uso de lenguajes como perl, javascripts, html permitieron la realización de una interface interactiva y sobre todo ligera que hace que el sistema tenga un eficiente desempeño.

REFERENCIAS

1. J. Crespo, E. Damian, V. Macías, J. Pérez, J. Suárez, V. Viejó, M. Villacrés, "Análisis, Diseño, Implementación de un Monitoreador de Tráfico IP para redes Ethernet usando TCP/IP y el Paradigma Cliente-Servidor" (Tópico de Graduación, Facultad de Ingeniería Eléctrica y Computación, Escuela Superior Politécnica del Litoral, 2000)