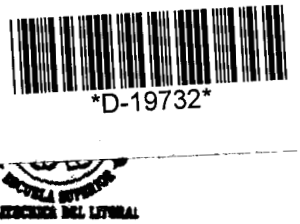


ESCUELA SUPERIOR POLITECNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Trabajo de Graduación

"Monitor de Tráfico IP para Redes Ethernet"

Previo a la obtención del Título de

INGENIERO EN COMPUTACION

PRESENTADO POR:

Jorge Enrique Crespo Cedeño
Eduardo Francisco Damian Malan
Maria Verónica Macias Mendoza
Jorge Arturo Perez Maldonado
Jessica Maria Suarez Garcia
Victor Manuel Viejo Chabla
Lucia Marisol Villacres Falconí

Guayaquil – Ecuador
1999

AGRADECIMIENTO

A Dios por cada dia de nuestras vidas.

A nuestros padres por el amor y los sacrificios que han hecho para hacer de nosotros personas de provecho para la sociedad.

A las personas que de alguna u otra manera colaboraron con la realización de este proyecto y al Ing. Guido Caicedo Rossi por compartir sus conocimientos y experiencias con todos sus alumnos del Topico.

DEDICATORIA

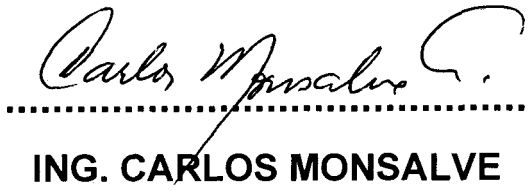
A NUESTROS PADRES

ANUESTROSMAESTROS

A NUESTROS AMIGOS

A NUESTROS COMPANEROS

TRIBUNAL DE GRADO

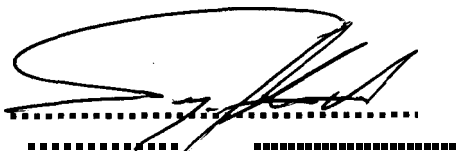


ING. CARLOS MONSALVE

Presidente del Tribunal

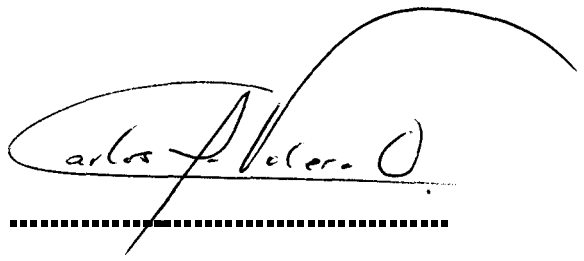
ING. GUIDO CAICEDO

Director de Topico



ING. SERGIO FLORES

Miembro del Tribunal



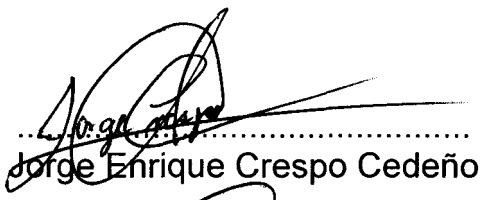
ING. CARLOS VALERO

Miembro del Tribunal

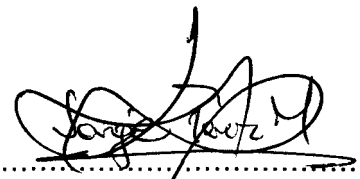
DECLARACION EXPRESA

"La responsabilidad por los hechos, ideas y doctrinas expuestos en este proyecto, nos corresponden exclusivamente; y, el patrimonio intelectual del mismo, a la ESCUELA SUPERIOR POLITECNICA DEL LITORAL"

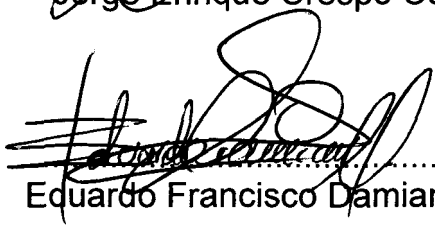
(Reglamento de Examenes y Titulos Profesionales de la ESPOL)



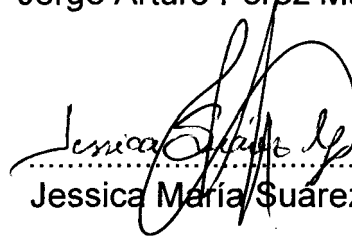
Jorge Enrique Crespo Cedeño



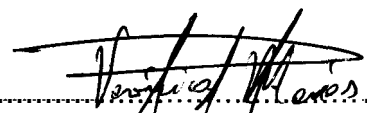
Jorge Arturo Pérez Maldonado



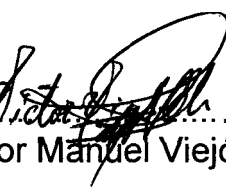
Eduardo Francisco Damian Malan



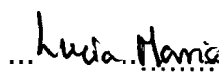
Jessica María Suárez García



María Verónica Macías Mendoza



Víctor Manuel Viejó Chabla



Lucia Marisol Villacrés Falconi

RESUMEN

El sistema Monitor, permite realizar un análisis cuantitativo y cualitativo del trafico IP de una red Ethernet mediante la visualización de curvas lineales, generadas a partir de los tipos de consulta grafica que se pueden realizar. Estas consultas pueden ser en *tiempo real* o *historicas.*

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

El sistema provee al usuario comun la capacidad de consultar el estado del monitoreo de trafico, realizar las consultas graficas basadas y consultar las fechas en las cuales estuvo el monitoreo activo.

El usuario Administrador, además de las opciones disponibles para el usuario comun tiene la capacidad de iniciar o detener el monitoreo de trafico, configurar caracteristicas del sistema de monitoreo, consultar ***o*** eliminar los registros del monitoreo activo, ingresar, editar o eliminar usuarios.

INDICE GENERAL

INTRODUCCIÓN

Para llevar a cabo el intercambio de informacion de manera exitosa se han desarrollado diferentes reglas de comunicacion, a las que se han llamado protocolos, asi como al conjunto de ellos llamados arquitectura, entre las cuales resalta la TCP/IP que es la base de la gran red de redes Internet.

Usar a la Internet como fuente de informacion ha llevado al aumento progresivo de los usuarios y de las redes, por este motivo, mantener una red se ha convertido en una labor complicada para los administradores.

MONITOREADOR DE TRAFICO IP PARA REDES ETHERNET trata de ser una herramienta tanto para el administrador como para el usuario, que permita ver las estadisticas graficas del trafico circulante por una red o por una computadora, informacion que resulta muy valiosa y necesaria para el administrador ya que basado en esto, podría redistribuir su ancho de banda y optimizar los recursos existentes.

1 Especificaciones

1.1 Objetivos

Este proyecto tiene como objetivo primordial el de proveer un sistema capaz de mostrar graficamente el trafico TCP/IP existente en una red Ethernet. Entre las metas a lograr estan:

- Aplicar el paradigma Cliente/Servidor sobre TCP/IP
- Permitir el análisis comparativo entre las diferentes aplicaciones y/o protocolos de comunicacion.
- Administrar el sistema desde un navegador web, facilitando el acceso desde cualquier punto de la red.
- Proveer capacidad multiusuario
- Brindar una interfaz amigable al usuario
- Poder analizar el trafico histórico o en tiempo real (en línea).

1.2 Descripción General

1.2.1 Antecedentes

Este proyecto se apoya en dos aplicaciones anteriores, la primera implementada en Borland C++ 3.0 bajo Windows95 y la segunda desarrollada aplicando el paradigma Cliente/Servidor, utilizando el lenguaje de programacion JAVA. Ambas aplicaciones solo capturaban el trafico correspondiente a ciertas direcciones IP las cuales debian ser guardadas en un archivo al igual que el tipo de trafico a ser capturado; a este archivo se lo conocia con el nombre de archivo de Configuración. Bajo esta perspectiva la segunda aplicacion tenia un mejor ambiente de trabajo y podia ser administrado desde cualquier sitio conectado a la red donde se hallaba el sistema.

1.2.2 Justificación

La comunicacion de datos se ha convertido en parte fundamental del desarrollo tecnologico y de las actividades diarias de la fuerza laboral.

Buscar formas de difundir la informacion a traves de redes por todo el mundo es algo cotidiano, por lo cual la administración de una red se ha convertido en una tarea compleja, y resulta necesario contar con herramientas que permitan conocer el estado de las redes, el trafico que soportan y otro tipo de informacion que permita optimizar el uso de las mismas y mejorar el servicio a los usuarios.

La ausencia en nuestro medio de una herramienta de bajo costo que permita realizar consultas graficas acerca del trafico de una red, sea esta historica o en línea de cualquier dirección IP, y el gran aporte que representa para los administradores de red en cuanto a la toma de decisiones para un mejor manejo del ancho de banda.

1.2.3 Funcionalidad

El sistema es capaz de monitorear todo el trafico que circula a traves de la red Ethernet donde se esta ejecutando y almacenando la información obtenida para permitir realizar las consultas respectivas.

El acceso al interfaz del sistema se lo realiza desde un navegador web autenticando al usuario que desea ingresar, el cual puede ser:

- Usuario comun, que solo podra realizar las consultas de trafico.
- Usuario con privilegios, llamado administrador, que puede configurar todo el sistema y realizar las consultas

El sistema provee al Usuario comun la capacidad de:

- Consultar el estado en el que se encuentra el monitoreo de trafico.
- Realizar las consultas graficas basadas en las direcciones IP y los protocolos de aplicacion disponibles.
- Consultar las fechas en las cuales estuvo el monitoreo activo.

El administrador tiene la capacidad de:

- Iniciar o Detener monitoreo de trafico segun su criterio.
- Realizar consultas graficas del trafico de la red en un rango de fecha dado o en línea
- Configurar caracteristicas del sistema de monitoreo como:
  - ✓ Direcciones de Red o estaciones de trabajo y protocolos de aplicacion que estaran disponibles para que los usuarios hagan sus respectivas consultas.
  - ✓ Direcciones de Red a excluir, es decir, no se tomarán en cuenta el trafico entre estaciones de trabajo que pertenecen a la red para la realización de las graficas a consultar
- Consultar o eliminar los intervalos de tiempo durante los cuales el monitoreo se encuentra activo.
- 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.

1.2.4 Alcance

Si se cumplen con los requerimientos de hardware y el sistema es bien empleado, este puede proporcionar información cien por cien real y confiable sobre la cantidad de trafico que pasa por una red, o por un host, y ademas ofrecer resultados graficos de tipo comparativos, que reflejaran el comportamiento del flujo de trafico.

El sistema desarrollado ademas proporciona herramientas de administración de recursos como es la base de datos y la eliminación de ciertos archivos en tiempos determinados, para de esta manera liberar espacio.

2 Arquitectura General

En esta sección se detalla la arquitectura utilizada en la comunicacion entre los componentes que intervienen en el sistema y se da una breve descripción de los mismos.

2.1 Descripción General

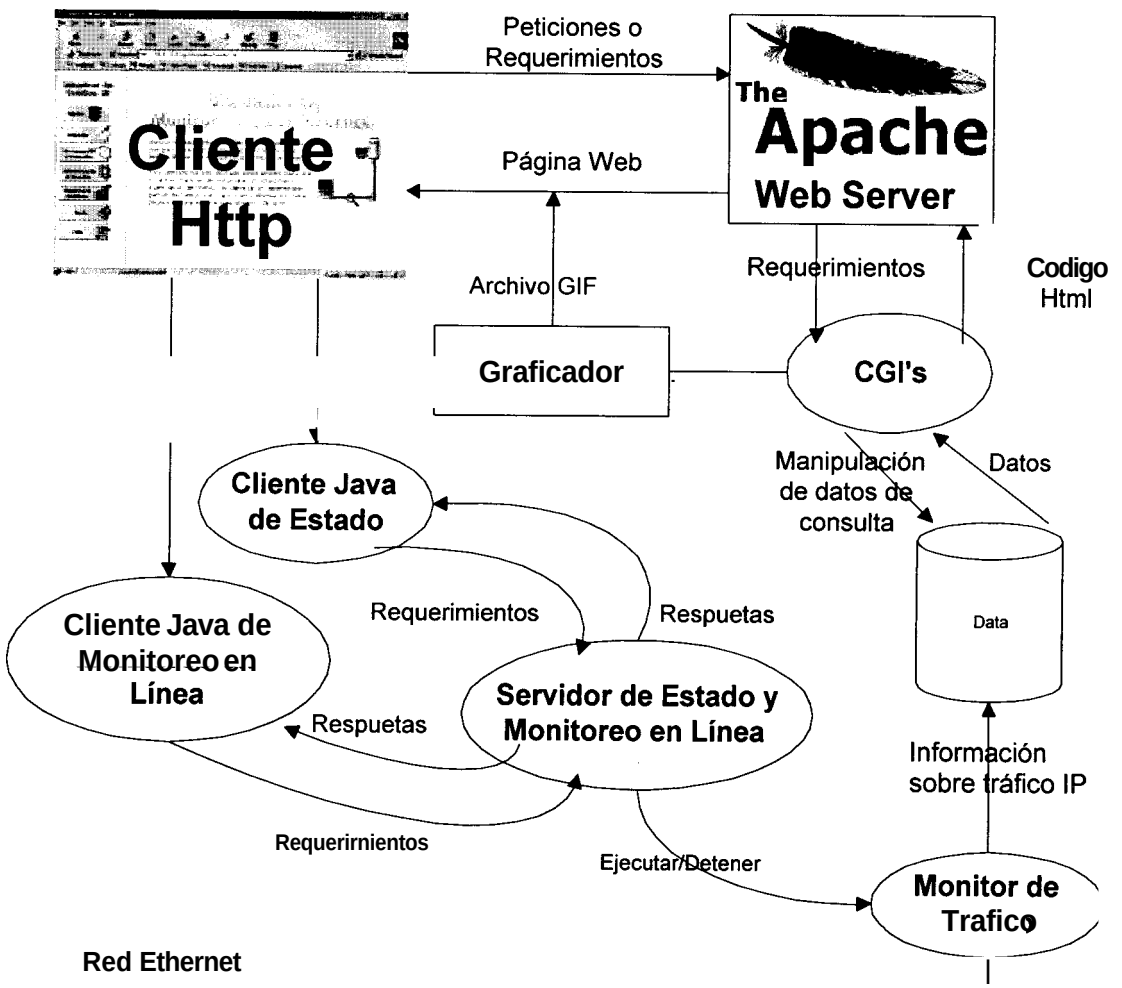


Fig. 2.1 Componentes del sistema

El sistema monitoreador de Trafico IP consta de 5 componentes principales:

Base de datos

Monitor de Trafico

Servidor de Monitoreo General

Servidor de estado y monitoreo en linea

Clientes JAVA.

La figura 2.1.muestra la relación de los componentes. Cuando un usuario se conecta al sitio web del sistema monitor de trafico, hace un requerimiento al Servidor apache, el cual muestra al usuario las páginas Web que los CGI's generen. A su vez los CGI's suministran al Graficador los datos necesarios para que genere un archivo grafico que muestra el trafico IP vs tiempo de las consultas historicas. Además los CGI´s se comunican con la base de datos para mostrar ingresar o eliminar los datos de configuración de monitoreo que el usuario requiera.

Por otra parte, el servidor de estado y monitoreo en linea contesta los requerimientos solicitados por los clientes de estado y monitoreo en linea respectivamente. Cabe recalcar que existen dos tipos de clientes de estado, un cliente administrador y un cliente usuario comun, ambos muestran el estado actual de monitoreo, pero el cliente administrador de estado tiene la capacidad

de iniciar o detener el monitoreo ejecutando el monitor de trafico o enviandole una señal para que se detenga.

Por ultimo, el monitor de trafico es el encargado de capturar la informacion necesaria sobre el trafico IP circulante en una red ethernet y almacenar esta inforrnacion en una base de datos.

2.2 Descripción de los componentes del Sistema

2.2.1 Base de Datos

El Almacenamiento de la informacion capturada y de los datos de configuración se mantiene en una base de datos, pues dada la cantidad de inforrnacion que se va a manejar en cuanto al trafico por estacion de trabajo, resulta mas conveniente por la rapidez de acceso y la facilidad de manejo.

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

2.2.2 Monitor de Trafico

La recopilacion de la informacion de los paquetes es un componente medular en el sistema, pues es mediante la captura de informacion que obtenemos los datos del trafico existente en la red y que posteriormente serviran para construir las curvas de trafico IP **vs** tiempo.

El proceso captura todos los paquetes circulantes en la red **y** toma cierta informacion para identificarlos; almacenandolos temporalmente en memoria principal por un minuto, luego de lo cual guarda en la base de datos la informacion obtenida. (Figura 2.2)

Con el proposito de responder a posteriores requerimientos de una dirección IP cualquiera, el sistema captura informacion de todo el trafico que circula en la red.

Además de la informacion concerniente a cada paquete, tambien se almacena la fecha de inicio **y** pausa del monitoreo, asi como el numero total de paquetes y bytes capturados durante este intervalo.

En cuanto a la capacidad de iniciar o detener la captura de informacion y de presentar siempre el estado en el que se encuentra el monitoreo, se optó hacerlo mediante un applet de **JAVA,** pues de esta manera se podría estar sensando constantemente el estado de monitoreo y mostrar al usuario esta informacion sin necesidad de recargar la pagina.

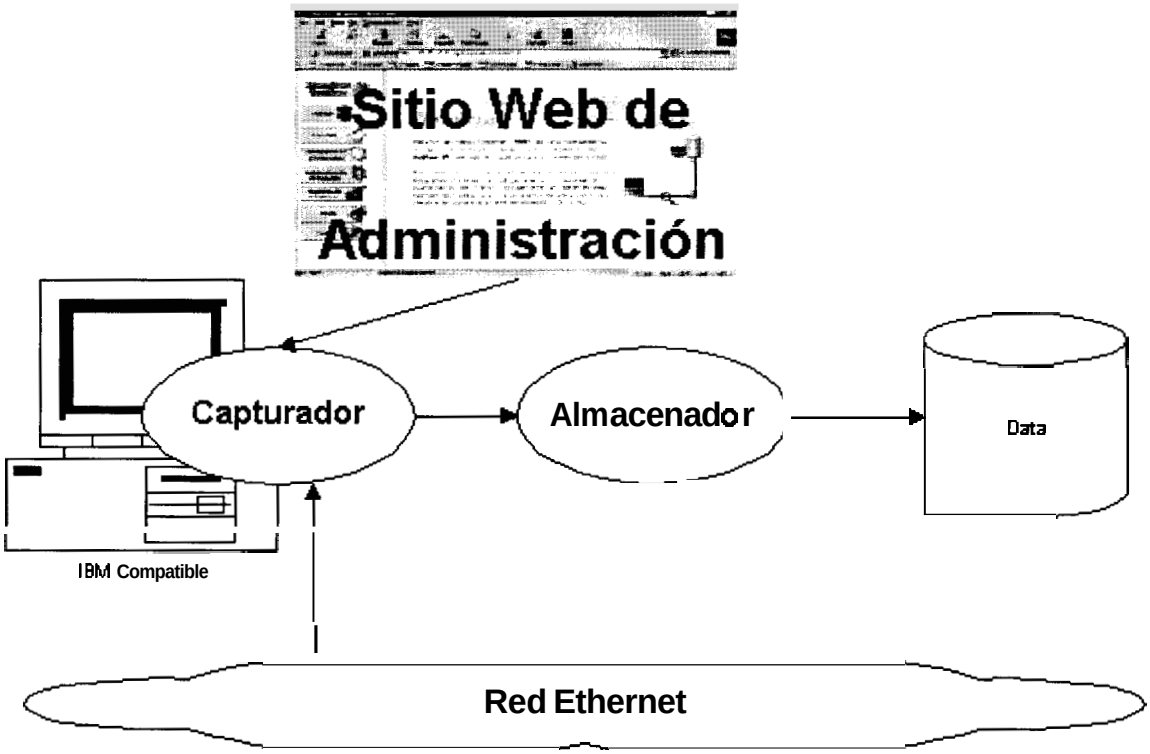


Figura 2.2.- Esquema general del Monitor de Trafico

2.2.3 Servidor de Monitoreo General

Consta de dos modulos bien definidos:

CGI's: encargados de responder a los requerimientos de administración de información concerniente a los Usuarios, direcciones IP, Protocolos de o puertos de comunicacion **y** configuración de consultas. Tambien responden a los requerimientos de consultas Historicas.

Graficador: Se encarga de realizar las graficas de "trafico **vs** tiempo" para las consultas historicas, en base a los datos generados por los CGI's obtenidos de la Base.

2.2.4 Servidor de Monitoreo en Línea

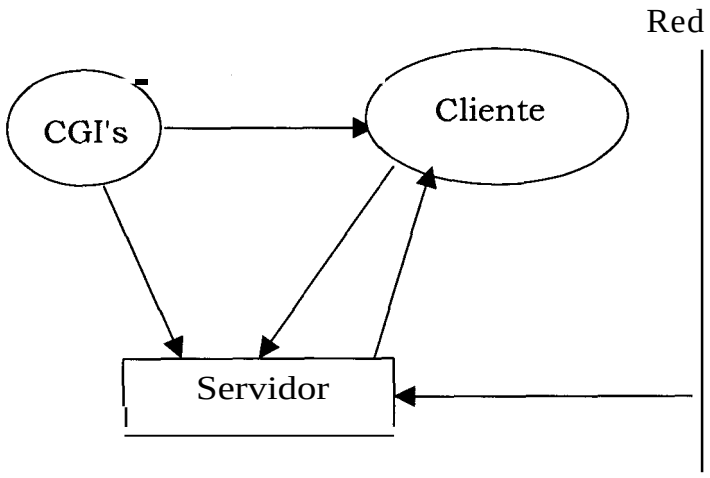


Figura 2.3 Servidor de monitoreo en Línea

El servidor de *Monitoreo en línea* se encarga de responder a los requerimientos de consultas en línea. Este modulo cuenta con sus propios modulo de configuracion -basados en una configuracion inicial obtenida de los CGI´s- y de Monitoreo de Trafico, para responder rapidamente y presentar trafico por segundo.

2.2.5 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 de trafico en línea. Tiene como funcion principal mostrar los datos del trafico 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 este siempre visible al usuario.

3 Plataforma y Herramientas de Desarrollo

Las Plataformas y Herramientas de desarrollo utilizados en la implementacion del sistema han sido seleccionados luego de un análisis completo de las ventajas que presentan cada una de ellas. En este capitulo se detallan las razones por las cuales fueron seleccionadas.

3.1 Sistemas Operativos

Los sistemas Operativos sobre los cuales se ha implementado el Sistema Monitoreador de Trafico IP son Red Hat Linux y Windows NT.

3.1.1 Red Hat Linux

Es un sistema operativo robusto y eficiente. Su popularidad y uso han alcanzado grandes niveles, ya sea por su bajo costo o bien por la cantidad de software pre-instalado que posee. Además, debido a que LINUX es un sistema operativo basado en UNIX, es capaz de correr procesos en ***background,*** lo que permite ejecutar un proceso mientras se esta realizando otra actividad.

3.1.2 Windows NT

Este sistema operativo suministrado por Microsoft es bastante poderoso en administracion de redes. Es considerado importante por el ambiente de ventanas que es muy conocido, lo que facilita la administracion del sistema. Además una gran parte de las empresas que implementan redes cuenta con esta plataforma.

3.2 Lenguajes de Programacion

3.2.1 C para Linux

Usado para desarrollar el capturador de paquetes sobre LINUX. Ofrece ventajas como la facilidad para trabajar con los puertos de comunicacion y la conexión con la base de datos PostgreSQL. Por otro lado esta la alternativa de crear varios procesos (procesos hijos) que se rigen bajo un mismo programa (proceso padre).

3.2.2 Borland C

Utilizado en el desarrollo del capturador para WINDOWS NT. Facilita la implementación de la conectividad con la base de datos ya que cuenta con las librerias MFC (MicroSoft Fundation Classes). Además, permite aumentar progresivamente la memoria principal utilizando punteros.

3.2.3 Java

Es un lenguaje robusto y sobre todo portable, por esta razon se lo utilizo para desarrollar los clientes. La ventaja es que el sistema solo debe ser instalado en el servidor y cada cliente necesita solamente un navegador grafico. Por ultimo, sus nuevas herramientas graficas proveen mayor numero de funcionalidades para el manejo de la interfaz.

3.2.4 Perl

Usado para desarrollo de los CGI tanto para windows NT como para **LINUX.** Por su facilidad de programacion (muy parecido al lenguaje C) y por la compatibilidad de conexión con los motores de base de datos usados.

3.2.5 HTML

Para la creación de la paginas WEB. **Es** un lenguaje basico y primordial porque con el se ha desarrollado la interfaz del sistema. Además resulta sencillo **y** de facil edición.

3.2.6 JavaScript

Es un lenguaje de muy facil interpretación que pueden ser incluidos en las paginas web sin necesidad de compiladores. Ha sido utilizado sobre todo para la interfaz y validaciones.

3.3 Bases De Datos

3.3.1 PostgreSQL

Esta incluida en el paquete de Linux y es una base de datos con bastante beneficios y sobre todo muy consistente.

3.3.2 Access

A pesar de no ser una base de datos gratuita, es muy fácil de obtener. Presta todos los servicios necesarios y además no tiene problemas de acoplamiento con el windows, porque es propia de la Microsoft.

3.4 Otras

3.4.1 Apache Web Server

La necesidad de tener un servidor de WEB que responda a los requerimientos de administración y sobre todo por la disponibilidad de las versiones para las

plataformas de LINUX y Windows, su facil instalacion y mantenimiento hicieron de APACHE la herramienta mas importante en el desarrollo de la interfaz del sistema.

3.4.2 GNUPlot

Es una herramienta que viene incluida en el paquete de Linux, ha sido utilizada para la construcción de graficas historicas en este mismo tipo de consulta. Genera un archivo grafico en formato *GIF* que es referenciado en las páginas web de la consulta.

Del análisis de la informacion que se requiere almacenar, las siguientes son las entidades resultantes:

1. Red
2. Dominio
3. Aplicacion
4. Paquete
5. DatosUsuario
6. Usuario
7. Rango_Tiempo
8. Datos_Gráfico
9. Historial

4.2 Descripción de Entidades

ENTIDAD RED

Esta entidad tendra la caracteristica de registrar informacion acerca de las redes de cornputadoras de las cuales se conozcan sus datos importantes como son dirección y mascara de red. Estos datos seran utilizados para asignar la

direccion de red origen y la direccion de red destino de los paquetes monitoreados.

ENTIDAD DOMINIO

Su funcion es almacenar la información de los dominios que estaran disponibles para realizar las consultas. Cada dominio consta de los datos de la computadora que origina los paquetes y los datos de la computadora a la que se envian los paquetes, y para cada una de ellas, se debe conocer su direccion, la direccion de la red a la que pertenece y el numero de bits que ocupa la mascara de su red.

De esta manera se obtienen pares origen-destino que seran los que se presentaran en las opciones de consultas de monitoreo.

Adicionalmente para cada dominio se puede especificar si forma parte de la configuración predeterminada, esto quiere decir, que los dominios marcados como predeterminados apareceran seleccionados por defecto en las transacciones de consulta.

ENTIDAD APLICACION

El proposito de la entidad aplicacion es mantener registradas aquellas aplicaciones sobre las cuales se podrán realizar requerimientos de consultas. Para estas aplicaciones se necesita especificar su sigla o mnemonico, el numero de puerto que utiliza y su nombre completo.

Al igual que en la entidad descrita anteriormente, las aplicaciones son susceptibles de declararlas predeterminadas, con lo cual seran seleccionadas por defecto al realizar consultas.

ENTIDAD PAQUETE

La funcion de esta entidad es almacenar la información relevante de los encabezados o headers de los paquetes monitoreados, es decir aquellas propiedades que servirán de metodos de busqueda para consultas posteriores.

Un registro en esta entidad representa los paquetes capturados durante un intervalo de tiempo especifico (1 minuto) que tuvieron el mismo origen y destino, y en el que se almacenan sus datos de manera consolidada.

La información relevante incluye fecha y hora en que fueron moniteados los paquetes, direccion IP de la computadora y de la red origen, direccion IP de la computadora y de la red destino, protocolo de la capa de red y protocolo de la capa de transporte que utilizaron los paquetes, puerto de aplicacion origen, puerto de la aplicacion destino y, tamaño total en bytes y numero de paquetes monitoreados en período de tiempo indicado.

ENTIDAD DATOSUSUARIO

La caracteristica de la entidad DatosUsuario es mantener registrados los datos de los usuarios que podrán acceder al sistema, como son nombre, apellido, codigo de usuario y password de acceso al sistema.

ENTIDAD USUARIO

Esta entidad tiene el proposito de registrar informacion sobre cada una de las conexiones que se realicen al sistema. A cada acceso al sistema se le asigna un numero entero aleatorio que servira para poder identificar la conexion y los requerimientos que esta conexion realice.

Como dato informativo se registra la fecha y hora de entrada al sistema.

ENTIDAD RANGO TIEMPO

Esta entidad se utilizara para almacenar los rangos o periodos de tiempo que se generan producto de un requerimiento de consulta de monitoreo histórico y que seran de utilidad para efectos de la consolidación de la informacion solicitada, de acuerdo a los intervalos de tiempo resultantes.

Asi pues, el período de tiempo que el usuario consulta, se divide en intervalos de tiempo de acuerdo a lo solicitado (minutos, horas, dias) y estos intervalos resultantes son los que se almacenan en esta entidad. Un registro completo

consta del usuario que realiza la consulta, el numero asignado a la conexion, fecha y hora inicial y final del intervalo de tiempo.

ENTIDAD DATOS GRAFICO

La funcion de esta entidad es mantener los resultados de una consulta realizada de una manera consolidada, con el fin de poder determinar rapidamente datos estadisticos, como son minimos y maximos, que son presentados siempre en las opciones de consulta.

Para lograr su cometido, se necesita registrar el usu rio, el ódigo de la conexion, el identificador del dominio, el identificador del tipo de consulta (a nivel de dominios, de capa de red, de capa de transporte o a nivel de capa de aplicacion), identificador del intervalo de tiempo, identificador del protocolo del tipo de consulta correspondiente, y datos acumulados de bytes y numero de paquetes.

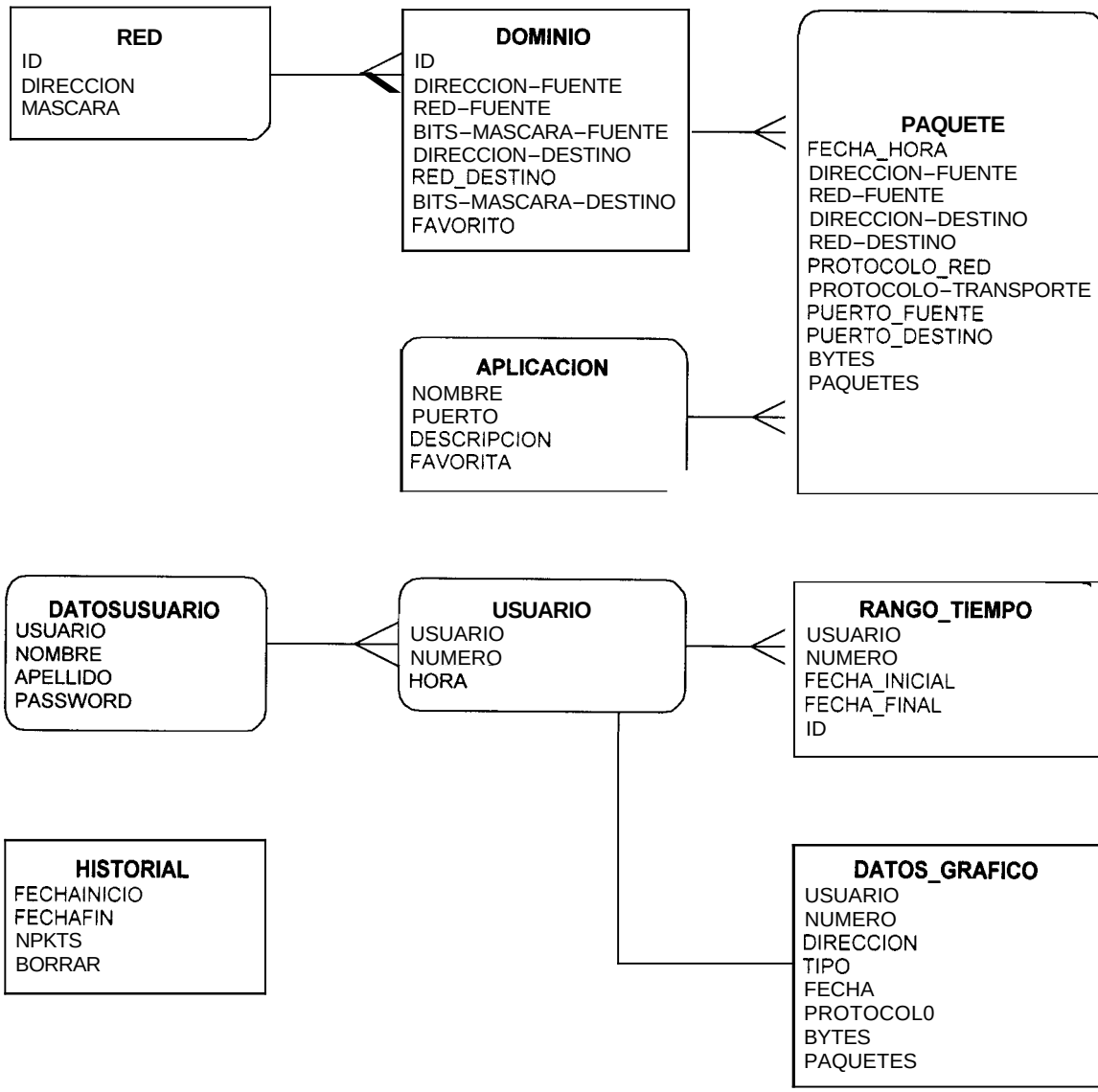
ENTIDAD HISTORIAL

Esta entidad es la encargada de registrar los periodos de tiempo en los cuales se realizo un monitoreo de paquetes en el sistema. Esta informacion es necesaria primero como datos informativos y luego como punto de partida para la administración del volumen de informacion monitoreada.

La informacion de los monitoreos consta de la fecha y hora de inicio y de culminación del monitoreo, y del numero de paquetes capturados.

Adicionalmente esta entidad mantiene un atributo que indica que el monitoreo registrado ha sido marcado para su eliminación.

4.3 Diagrama de Entidad-Relacion.



4.4 Atributos de las Entidades.

En esta sección se detalla de manera tabular los atributos de cada entidad.

ENTIDAD RED		
ATRIB TO	PO	DE RIP N
ID	ENTERO	Codigo utilizado para identificar una red registrada
DIRECCION	TEXTO	Dirección IP de la red
MASCARA	TEXTO	Mascara de Red de la dirección registrada

ENTIDAD DOMINIO		
ATRIBUTO	***TIPO***	***DESCRIPCION***
ID	ENTERO	Codigo utilizado para identificar un dominio registrado
DIRECCION_FUENTE	TEXTO	Dirección IP del computador origen
RED–FUENTE	TEXTO	Direccidn IP de la red del computador origen
BITS–MASCARA–FUENTE	ENTERO	Numero de bits que utiliza la mascara de red del computador origen
DIRECCION–DESTINO	TEXTO	Direccidn IP de la PC destino
RED–DESTINO	TEXTO	Direccidn IP de la red de la PC destino
BITS–MASCARA–DESTINO	ENTERO	Numero de bits que utiliza la mascara de red de la computadora destino
FAVORITO	TEXTO	Atributo que indica con una letra ***'S'*** que el dominio registrado es favorito, es decir que debe aparecer seleccionado por defecto al realizar una consulta

Tabla 4.2. Atributos de la entidad Dominio

ENTIDAD APLICACIÓN		
ATRIBUTO	***TIPO***	***DESCRIPCION***
NOMBRE	TEXTO	Sigla o Mnemónico de la aplicación registrada
PUERTO	ENTERO	Puerto que utiliza la aplicacion para el envio de los paquetes
DESCRIPCION	TEXTO	Descripción de la aplicación
FAVORITA	TEXTO	Atributo que indica con una letra 'S' que la aplicacion registrada es favorita, **es** decir que debe aparecer seleccionada por defecto al realizar una consulta

Tabla 4.3. Atributos de la entidad Aplicacion

ENTIDAD PAQUETE		
ATRIBUTO	***TIPO***	***DESCRIPCION***
FECHA_HORA	FECHA	Fecha y hora de monitoreo de los paquetes
DIRECCION_FUENTE	TEXTO	Direccion IP de la computadora origen
(RED–FUENTE	TEXTO	Direccion IP de la red a la cual pertenece el cornputador origen
DIRECCION_DESTINO	TEXTO	Dirección IP de la computadora destino
RED–DESTINO	TEXTO	Direccion IP de la red a la que pertenece el cornputador destino
PROTOCOLO–RED	TEXTO	Protocolo de red con el que se enviaron los paquetes (IP, ICMP, ARP)
PROTOCOLO–TRANSPORTE	TEXTO	Protocolo de transporte que utilizaron los paquetes (TCP, UDP)
PUERTO_FUENTE	ENTERO	Numero del puerto en el cornputador origen que se utilizó para el envio de los paquetes
PUERTO_DESTINO	ENTERO	Numero del puerto en la cornputadora destino
BYTES	ENTERO	Tamaño total de los paquetes en bytes
PAQUETES	ENTERO	Cantidad de paquetes rnonitoreados

Tabla 4.4. Atributos de la entidad Paquete

ENTIDAD DATOSUSUARIO		
A RI O	*TIPO*	*DESCRIPCION*
USUARIO	TEXTO	Codigo que utilizará el usuario para la conexion al sistema
NOMBRE	TEXTO	Nombre del usuario
APELLIDO	TEXTO	Apellido del usuario
PASSWORD	TEXTO	Clave de acceso al sistema para el usuario registrado

ENTIDAD USUARIO		
ATRIBUTO	*TIPO*	*DESC PC N*
USUARIO	TEXTO	Codigo de usuario conectado al sistema
NUMERO	ENTERO	Numero aleatorio asignado a la conexion
HORA	FECHA	Fecha y hora de conexion al sistema

Tabla 4.6. Atributos de la entidad Usuario

ENTIDAD RANGO_TIEMPO		
ATRIBUTO	***TIPO***	***DESCRIPCION***
USUARIO	TEXTO	Código del usuario que realiza
NUMERO	ENTERO	Numero aleatorio asignado a al sistema
FECHA_INICIAL	FECHA	Fecha y hora de inicio del intervalo de tiempo
FECHA_FINAL	FECHA	Fecha y hora en que culmina el intervalo de tiempo
ID	ENTERO	Codigo para identificar un rango registrado

Tabla 4.7. Atributos de la entidad Rango_Tiempo

ENTIDAD DATOS_GRAFICO		
ATRIBUTO	***TIPO***	***DESCRIPCION***
USUARIO	TEXTO	Código del usuario que realiza la consulta
NUMERO	ENTERO	Numero aleatorio asignado a la conexión al sistema
DIRECCION	ENTERO	Código identificador del dominio consultado
TIPO	TEXTO	Descripcibn del tipo de consulta (A nivel de dominios, de capa de Aplicacion, de capa de Transporte o de capa de Red)
FECHA	ENTERO	Código que identificada el intervalo de tiempo
PROTOCOLO	ENTERO	Codigo identificador del protocolo utilizado
BYTES	ENTERO	Tamaño total de los paquetes en bytes
PAQUETES	ENTERO	Cantidad de paquetes

Tabla 4.8. Atributos de la entidad Datos_Grafico

ENTIDAD HISTORIAL		
ATRIBUTO	***TIPO***	***DESCRIPCION***
FECHAINICIO	TEXTO	Fecha y hora de inicio del monitoreo
FECHAFIN	TEXTO	Fecha y hora de culminación del monitoreo
NPKTS	ENTERO	Cantidad de paquetes capturados
BORRAR	TEXTO	Atributo que indica si se ha solicitado la eliminación de los paquetes capturados en el período de tiempo registrado

5 Monitor de Trafico

En esta sección se detalla la arquitectura del Monitor de trafico y las consideraciones que se tomaron en cuenta para maximizar la captura de paquetes.

5.1 Diseiio

El principal objetivo del monitoreo de trafico, es lograr un alto rendimiento, es decir, perder la minima cantidad de paquetes posibles durante el proceso de captura de información, esta perdida se da cuando se realiza el almacenamiento fisico en la base de datos ya que requiere tiempo de procesamiento, lapso durante el cual el capturador estaria inactivo. Por este motivo el monitoreo de trafico esta subdividido en tres modulos que se muestran en la figura 5.1.

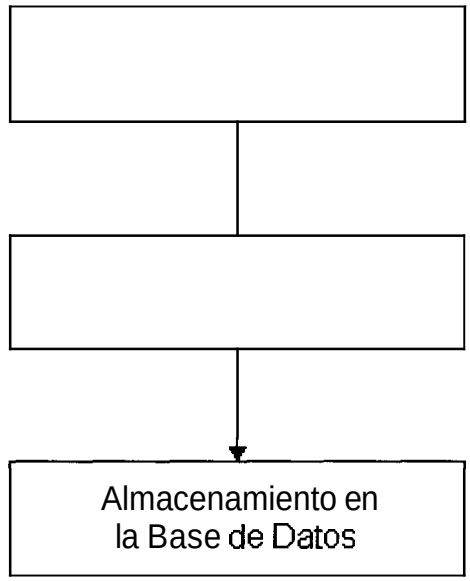


Figura 5.1. Arquitectura del Monitor de Trafico.

La información obtenida en la captura es tomada por el modulo de almacenamiento temporal, el cual verifica si los paquetes pertenecen a una misma sesion, entendiendose de que dos o mas paquetes pertenecen a una misma sesion siempre y cuando tengan iguales sus direcciones IP fuente y destino, sus protocolos a nivel de capas de red y transporte y además sus puertos de comunicacion fuente y destino; si se da este caso se acumula la cantidad de paquetes por la sesion y bytes transmitidos.

El objetivo de este almacenamiento temporal es el de independizar el proceso de captura del de almacenamiento en la base de datos ya que, de esta manera el sistema puede capturar mas informacion mientras se esta almacenando. El modulo de almacenamiento en la base de datos se lo realiza cada minuto.

5.2 Captura de informacion

De cada paquete que circula por la red se captura solamente los 68 primeros bytes, los cuales corresponden a los headers de los paquetes Ethernet y TCP/IP mas **14** bytes de datos. Esta informacion ***es*** procesada mediante el diagrama de flujo que se muestra en la figura 5.2

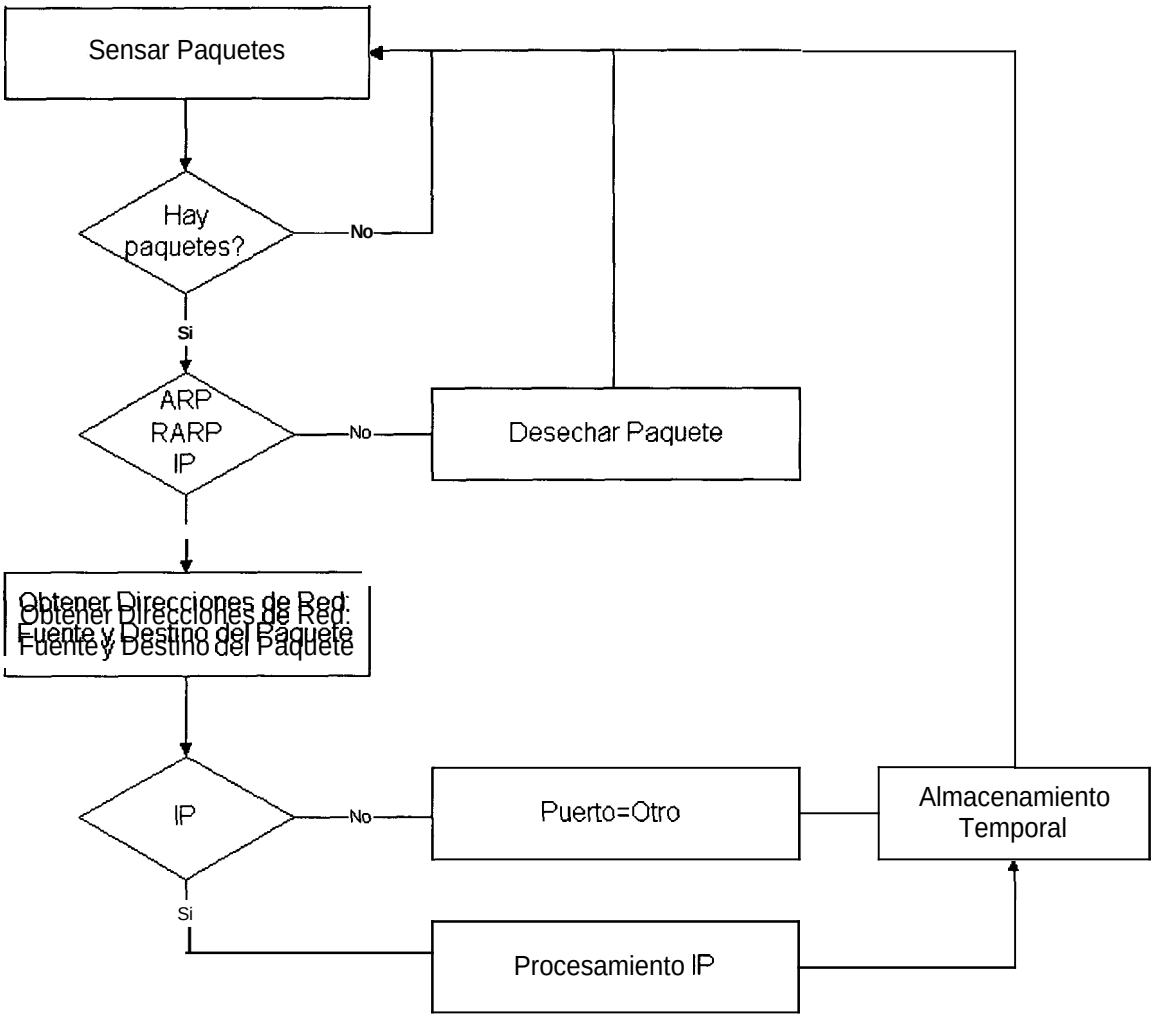


Figura 5.2. Diagrama **de** flujo **de** Captura **de** Información

Para tomar las decisiones tanto como para decidir si el paquete es IP, ARP, RARP, asi como para el procesamiento IP; el sistema se basa en las especificaciones del formato de cada protocolo las cuales son detalladas en el

apendice I. La informacion que se obtiene finalmente es: protocolos de red y transporte usados, Direcciones IP fuente y destino, puertos de comunicacion fuentes y destino, y por ultimo el numero de bytes que transporta el paquete.

5.3 Almacenamiento Temporal

Una vez obtenida la informacion descrita, se procede a almacenarla en una lista enlazada cuyo procesamiento de detalla en la figura 5.3. Si ha transcurrido un minuto desde la ultima vez que se envio a grabar a la base de datos, entonces se almacena este set de datos y se sigue con la captura de informacion.

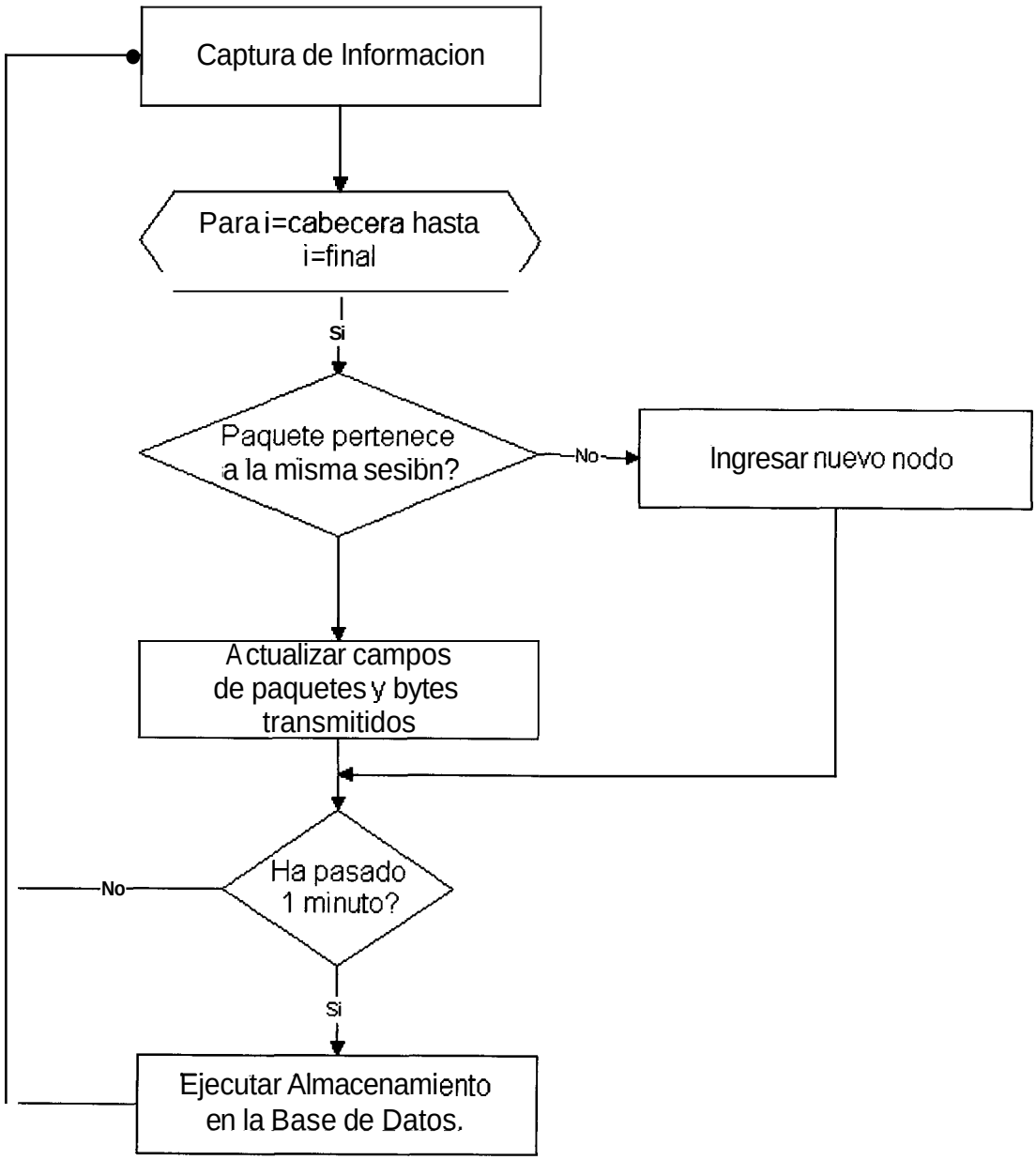


Fig. 5.3 Diagrama de Almacenarniento Temporal

5.4 Almacenamiento en la Base de datos

Como se lo describio anteriormente el almacenamiento en la base de datos se lo realiza cada minuto. Si el almacenamiento temporal envía a grabar en la base de datos y esta se encuentra procesando, el requerimiento pasara a una cola para su posterior procesamiento.

Una vez que se pasa la información de un nodo a la base de datos, este es eliminado de la lista para lograr un manejo optimo de la memoria.

El almacenamiento de datos se lo realiza cada minuto por las siguientes razones:

- Mejorar el rendimiento de captura de datos. Pues de esta manera no perdemos tiempo insertando por cada paquete un registro en la base, sino que esperamos a que pasa este intervalo y asi almacenamos que cantidad de paquetes de una misma sesion han circulado.
- La minima escala de presentación gráfica de datos es en minutos.

5.5 Plataforma Linux

5.5.1 Implementación

El capturador para esta plataforma esta basado en una aplicación llamada TCPDUMP. Se adaptó este programa para que ingrese los datos en una base de datos implementada en PostgreSQL y solo tomara los paquetes pertenecientes al protocolo IP. A esta nueva version se la denomino CPEthLX (Capturador de Paquetes Ethernet para **LINUX).**

5.5.2 Detalle de funciones y procedimientos

beginCapturer(): Es un procedimiento que realiza, valiendose de un set de funciones, el monitoreo de Tráfico.

pcap_lookupdev(ebuf): Se encarga de buscar las interfazs de red del sistema, retorna el nombre de la interfaz en caso de existir alguna o un valor nulo en caso contrario y muestra el error que se produjo el cual se almacena en

ebuf. En caso de existir mas de una interfaz entonces retorna el valor del adaptador de mas bajo orden (eth0)[1]

pcap_open_live(char *device, int snaplen, int promisc, int to–ms, char *ebuf): Se encarga de establecer en modo promiscuo la interfaz de red; recibe como parametro el puntero a la tarjeta dentro de la variable device, si la variable *promisc* es mayor que 0 la interfaz se establece en modo promiscuo[2], caso contrario esta en modo normal de operación, snaplen es la longitud de datos que se van a leer del paquete capturado, si ocurre algun error la descripción del mismo se la almacena en ebuf para luego ser visualizada en pantalla y se termina con la ejecucion del capturador.

lookup_printer(pcap_datalink(pd)): Esta funcion busca dentro de un arreglo (printers), con el que se referencia las diferentes tecnologias de red como ETHERNET, ATM, FDDI, entre otras, para saber que tipo de paquetes va a sensar. Recibe el puntero a la interfaz de red como parametro dentro de pd.

---

1 Linux nombra sus interfazs de red como eth0, eth1,.....ethn, donde n es igual numero de tarjetas de red que tiene la maquina.

2 Acepta todos los paquetes cirulantes por la red

pcap_read(pcap_t *p, int cnt, pcap–handler callback, u_char *user): Es la que se encarga de leer el paquete proveniente de la red **y** guarda los datos leidos dentro de la estructura p; cnt indica el numero de paquetes.

pcap_loop(pcap_t *p, int cnt, pcap–handler callback, u_char *user): Esta funcion hace referencia a pcap_read constantemente para lograr capturar todos los paquetes de la red hasta cuando reciba una señal indicado detener el monitoreo, una vez que se obtienen todos los datos del paquete este es insertado en una lista almacenamiento temporal para luego ser insertado en la base de datos por medio de la funcion joinPacket.

joinPacket(list_t *l, vpket_t *paqte): Esta funcion se encarga de realizar el almacenamiento temporal. Recibe como parametros una lista de nodos global cuya estructura es *vpket_t* la cual contiene toda la información referente a los paquetes, sus campos son los siguientes:

```
vpket_t {
        u_int32_t fuente;
        u_int32_t destino;
        char red[LRED];              /* IP-ARP-RARP */
        char transporte[LTCP];       /* UDP-TCP-ICMP */
        int puerto–fuente;   /* Aplicacion */
        int puerto_destino;
        unsigned long longitud;
        int paquetes;
};
```

El campo fuente y destino contienen la dirección IP fuente y destino del paquete respectivamente, los campos de red y transporte especifican el protocolo que llevan en las capas de su mismo nombre, los campos puerto–fuente y puerto_destino especifican la puertos de comunicacion fuente y destino respectivamente, longitud y paquetes almacenan el acumulado de bytes y de paquetes correspondientes a una sesion.

Para establecer si dos o mas paquetes son de una misma sesion, **joinPacket** realiza una comparacion bit a bit se valiendose de la siguiente directiva:

Criterio de comparacion = tamaño(estructura_vpket_t) -
tamaño(campo_paquetes) -
tamaño(campo_longitud).

tinsert(void *ptr): Se encarga de realizar el almacenamiento en la Base de Datos, recibe como parametro *ptr* que indica el tiempo que ha transcurrido desde que se ejecuto la primera inserción en el almacenamiento temporal, Si ptr es igual a un minuto tinsert es invocada por un hilo', se almacena el id[2] para saber si la base de datos se encuentra procesando, si se da este caso el hilo espera a que el hilo anterior se termine de ejecutar.

---

[1] Proceso que *se* ejecuta paralelamente **al** proceso actual.

[2] Identificador

5.5.3 Consideraciones Especiales

El Monitor de Trafico asume que su tarjeta de red esta completamente configurada, en caso contrario simplemente terminará anormalmente el proceso de captura de información indicandole que tipo de error se produjo.

El proceso de almacenamiento en la base de datos del Monitor no se preocupa por la creación de la base, si esta existe el proceso se realiza exitosamente, caso contrario un mensaje le indicara que tipo de error ocurrio.

Cuando se ejecuta el proceso de almacenamiento en la base de datos, y esta se encuentra procesando, debe esperar que se termine de ejecutar el requerimiento anterior; durante este lapso de espera el capturador se encuentra inactivo, es decir no lograra sensar paquetes circulantes por la red. Cabe recalcar que esta posibilidad es poco probable, pero se puede dar, ya que el almacenamiento a la base de datos se lo realiza cada minuto y el proceso en sí demora un promedio de 10 segundos.

5.6 Plataforma Windows **NT**

5.6.1 Implementación

El Monitor de Trafico en Windows NT se basó en el Packet Driver Packet.sys el cual viene incluido en el *Microsoft Windows NT Device Development Kit (DDK).* este driver añade a la interfaz de red varias operaciones de alto nivel que permiten monitorear el trafico de una red Ethernet. El monitor solo tomara los paquetes pertenecientes al protocolo IP, Los resultados obtenidos son almacenados en una base de datos implementada en Access 97; a esta version se la denomino cpethWNT(**C**apturador de Paquetes Ethernet para Windows **NT).**

5.6.2 Detalle de funciones **y** procedimientos

PacketGetAdapterNames(PTSTR pStr, PULONG pSize): Esta funcion accesa al registro de Windows NT y almacena el nombre de todos los adaptadores ae red disponibles en el computador en que se ejecuta el programa, en un puntero a un buffer referenciado por *pStr* cuya longitud es determinada por *pSize*.

PacketOpenAdapter(LPTSTR AdapterName): Inicializa el adaptador de red especificado por AdapterName, de esta manera se encuentre listo para enviar/recibir paquetes.

PacketSetFilter(LPADAPTER lpAdapter, ULONG Filter): Se encarga de setear la interfaz referenciada por lpAdapter en un modo de operación indicado por Filter, que para nuestro caso va a ser Filter[5] valor que representa al modo promiscuo.

PacketAllocatePacket(): Reserva espacio en memoria y recursos del sistema para la estructura de datos de tipo LPPACKET:

```
*LPPACKET {
   HANDLE     hEvent;
   OVERLAPPED  OverLapped;
   PVOID      Buffer;
   UINT       Length;
   };
```

En esta estructura se almacena temporalmente el paquete leído de la red.

PacketInitPacket(LPPACKET IpPacket, PVOID Buffer, UINT Length): Inicializa con los valores especificados por el puntero *Buffer* y *Length,* los campos del mismo nombre de la estructura referenciada por IpPacket. Buffer es un puntero a un buffer de memoria y Length indica el espacio ocupado por el mismo.

PacketReceivePacket(LPADAPTER IpAdapter,LPPACKET IpPacket, BOOLEAN Sync, PULONG BytesReceived): Es la que se encarga de leer el paquete proveniente de la red y guarda los datos leidos dentro de la estructura IpPacket, Bytes received especifica el tamaño de IpPacket. Una vez que se obtienen todos los datos del paquete este es insertado en una lista almacenamiento temporal para luego ser insertado en la base de datos por medio de la funcion **joinPacket y tinsert** respectivamente, las cuales son similares en su funcionamiento a la implementado para la plataforma Linux,con la unica salvedad de la conexión a la base de datos a la que accesan.

PacketFreePacket(LPPACKET IpPacket): Libera los recursos asignados a IpPacket.

PacketCloseAdapter(LPADAPTER IpAdapter): Cierra el adaptador y libera los recursos asignados a este.

Todas estas funciones se encuentran especificadas en la libreria de enlace dinamico Packet32.dll.

5.6.3 Manejador de Interfaz de Red

El Packet Driver **PACKET.SYS**, permite acceder a los manejadores de Interfaz de REd **NDIS**[1] mediante **NDIS.SYS**, además de brindar librerias de alto nivel a traves de la libreria de enlace dinamico **Packet32.dll.** Una breve descripción de como la aplicacion interactua con Packet.sys para poder accesar a la Tarjeta de Red se muestra en la figura **5.4.**

---

[1] Network Driver **Interfaz** Specification: Describe una interfaz mediante la cual el adaptador se comunica con otros protocolos o con el Sistema Operativo.

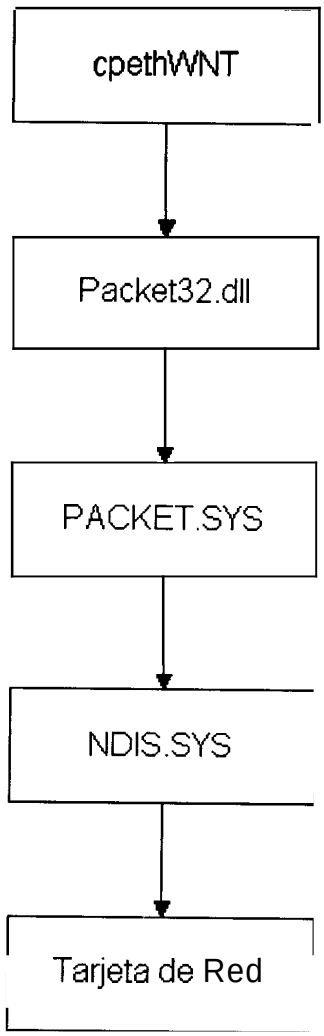


Figura 5.4 Acceso a la interfaz de red a través de Packet.sys

5.6.4 Consideraciones Especiales

El Monitor de Trafico asume que su tarjeta de red esta completamente configurada, en caso contrario simplemente terminara anormalmente el proceso de captura de información indicandole el error producido.

Antes de poder ejecutar el Monitor de Trafico se debe instalar el Packet Driver PACKET.SYS. La instalacion se describe en el Apendice I.

El proceso de almacenamiento en la base de datos del Monitor no se preocupa por la creación de la base, si esta existe el proceso se realiza exitosamente, caso contrario un mensaje le indicara que tipo de error ocurrio.

Cuando se ejecuta el proceso de almacenamiento en la base de datos, y esta se encuentra procesando, debe esperar que se termine de ejecutar el requerimiento anterior; durante este lapso de espera el capturador se encuentra inactivo, es decir no lograra sensar paquetes circulantes por la red. Cabe recalcar que esta posibilidad es poco probable, pero se puede dar, ya que el almacenamiento a la base de datos se lo realiza cada minuto y el proceso en si demora un promedio de 10 segundos.

6 Servidor de Monitoreo General

En esta sección se describira el servidor de monitoreo general, que esta compuesto principalmente por cgi's.

6.1 CGI

Esta parte esta compuesta por cgi's que generan el codigo HTML de las paginas que sirven de interfaz con el usuario. Estas paginas a su vez reciben los requerimientos del usuario y se los envian a los cgi's para que estos los procesen y retornen la respuesta apropiada.

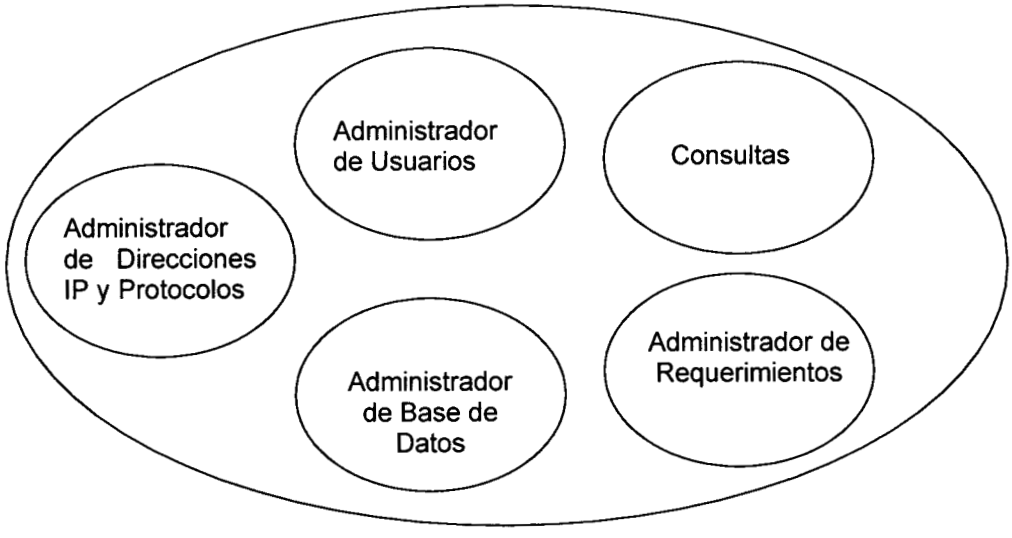


Fig. 6.1 Modulos de cgi

6.2 Administrador de Requerimientos

El modulo Administrador de Requerimientos llama al procedimiento que corresponde al requerimiento generado por el usuario a traves de la pagina WEB. Por ejemplo, si el administrador desea ingresar un nuevo usuario, el modulo Administrador de Requerimientos recibe el pedido y llama al procedimiento encargado de construir el codigo HTML que se envía al servidor WEB para mostrar la pagina correspondiente.

En el siguiente dibujo presentamos la interacción del modulo Administrador de Requerimientos con el resto del sistema.

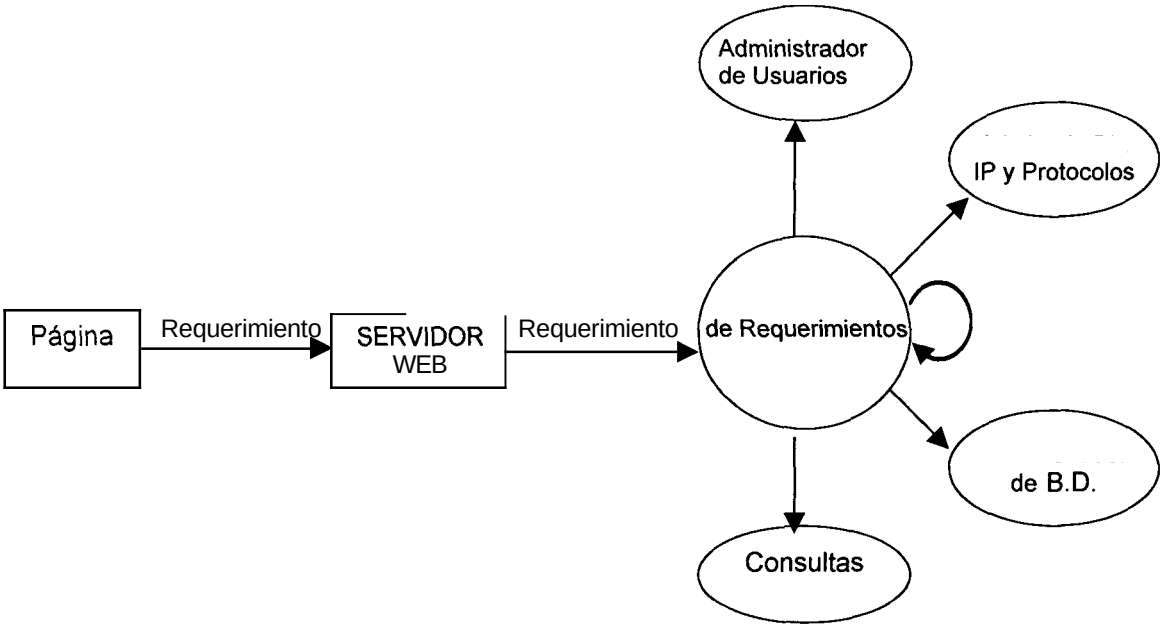


Fig. 6.2 Diagrama de interacción del mddulo Administrador de Requerimientos

Como podemos apreciar en el dibujo anterior, el Administrador de Requerimientos, tambien se llama a sí mismo. Esto sucede cuando se trata del requerimiento de ingreso al sistema; es decir cuando llamamos a la pagina inicial que recibe los datos de user y password para ingresar al mismo. Los datos ingresados por el usuario tambien son procesados por este modulo y si estos son correctos se presenta la pagina correspondiente al tipo de usuario (administrador o usuario comun).

6.3 Consulta

Es llamado por el Administrador de Requerimientos. Genera llamadas a la base de datos para obtener todos los dominios de direcciones IP existentes en la tabla dominio, los protocolos de aplicaciones existentes en la tabla aplicacion y las redes existentes en la tabla red. Con esta información el submodulo arma un codigo HTML que contiene un formulario. Este código se pasa al sitio WEB para que presente la pagina resultante. El formulario presenta todos los datos necesarios para realizar una consulta, y recibe el requerimiento de generación del grafico correspondiente.

Para la generación del grafico historico, se reciben los datos ingresados en el formulario y se lleva a cabo la respectiva validación. En caso de que sean correctos se genera la llamada a la base de datos para obtener la información monitoreada que cumpla los requerimientos especificados. El resultado que recibe de la base de datos es almacenado en tres archivos planos (capas de: red, transporte y aplicacion) con el formato aceptado por el Graficador, una vez hecho esto se llama al submodulo de presentación y actualización de graficos.

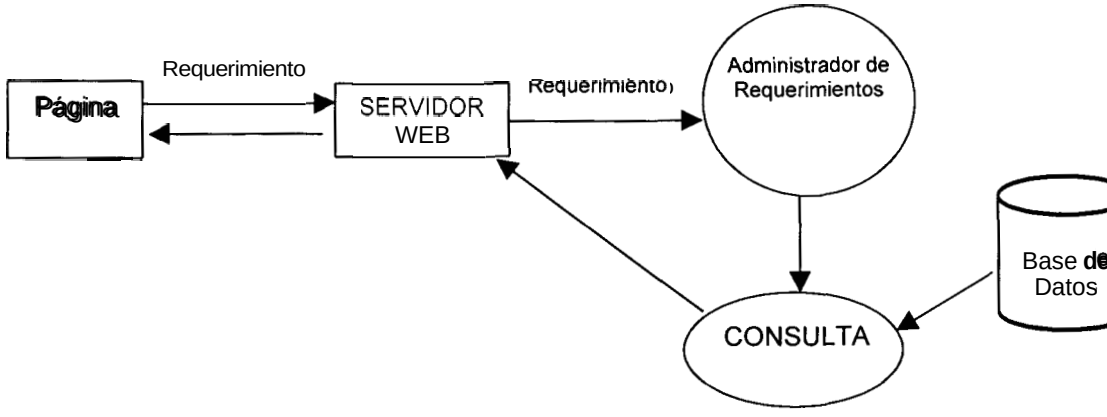


Fig. 6.3 Interacción del modulo de consulta

6.3.1 Actualización y Presentación de Gráficos

Utilizando los archivos planos generados, el Graficador construye un archivo grafico que muestra los datos en un plano cartesiano tiempo (minutos, horas, dias y meses) vs. cantidad (bytes, Kbytes o paquetes). **El** submodulo envía al servidor WEB un codigo HTML para cargar la pagina correspondiente en el navegador WEB. Dicha pagina presenta el grafico y un formulario con los dominios de direcciones IP y protocolos, seleccionados en el modulo de Consulta. Estos datos ayudan al usuario a visualizar mejor las caracteristicas de la consulta.

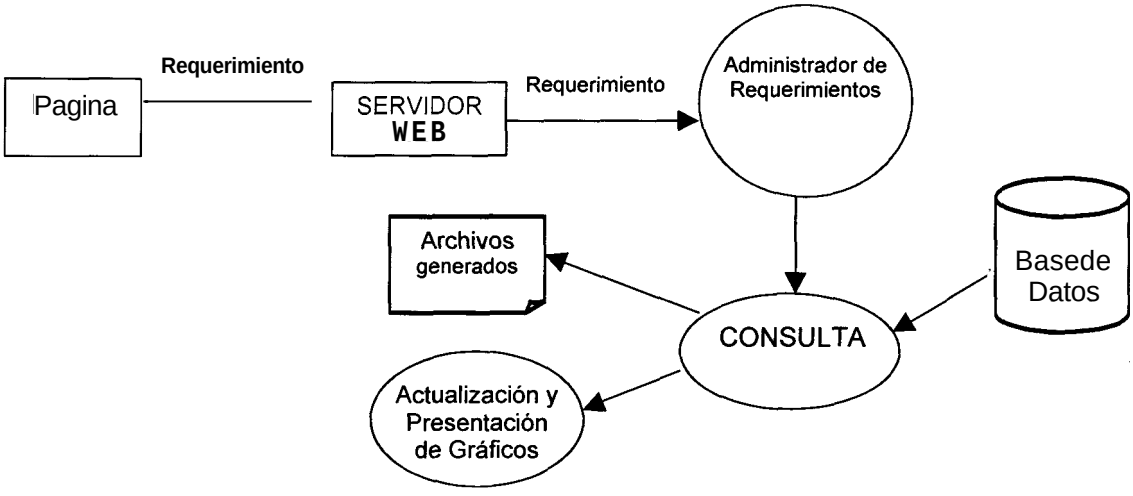


Fig. 6.4 Proceso para presentar los graficos

El submodulo recibe los nuevos requerimientos ingresados en el formulario para generar otra visualización de la consulta, si el usuario asi lo quisiere.

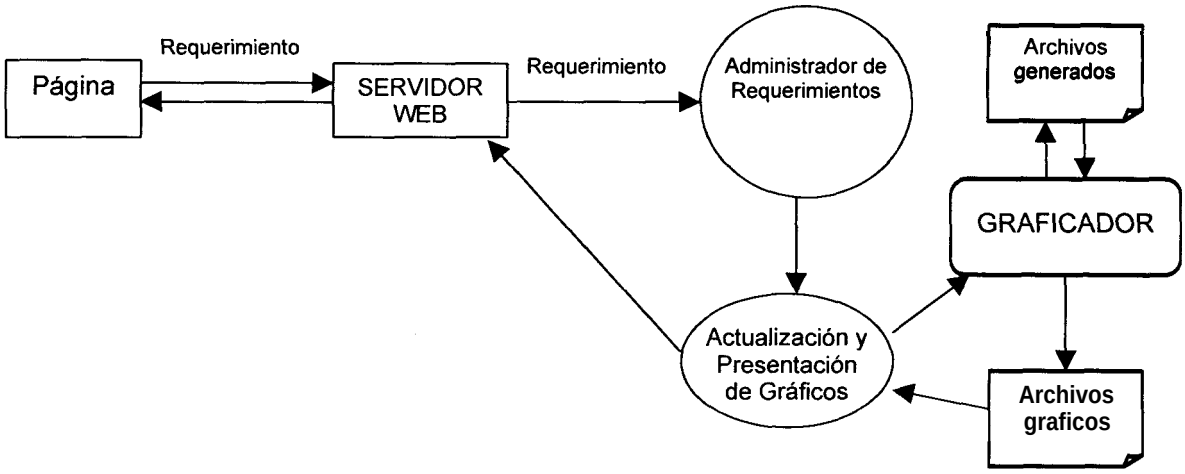


Fig. 6.5 Proceso para actualizar graficos

6.4 Direcciones IP y Protocolos de Aplicacion

El modulo de Administración de Direcciones IP se encarga de procesar los requerimientos de Ingreso y Eliminación de Direcciones IP, Protocolos de aplicacion y Redes a Excluir. Tambien recibe el requerimiento para la Predeterminación de Datos en la Consulta; además genera la pagina **HTML** con un formulario que recibe los requerimientos del usuario.

Este modulo se divide a su vez en 7 submodulos: Ingreso de Direcciones IP, Eliminacion de Direcciones IP, Ingreso de Protocolos de Aplicacion, Eliminacion de Protocolos de Aplicacion, Ingreso de Redes a Excluir, Eliminacion de redes a excluir y Predeterminación de Consulta.

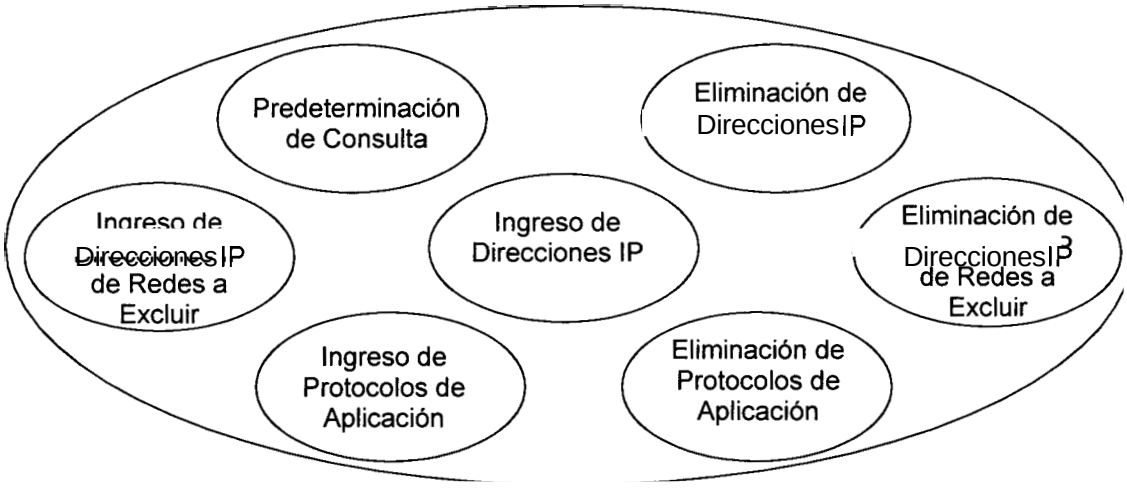


Fig. 6.6 Submodulos de Administración de Direcciones IP y Protocolos de Aplicacion

6.4.1 Ingreso de Direcciones IP

Recibe el requerimiento para el ingreso de una nueva direccion IP y verifica que los datos ingresados por el administrador en el formulario sean correctos. Si los datos son correctos, llama a un proceso que determina el tipo de direccion IP (red o maquina). Si se trata de una red, se genera una llamada a la base de datos para que dicha direccion sea ingresada en tabla red (sí es que ya no existe un registro para la misma); y en cualquiera de los casos se genera una llamada a la base de datos para ingresar los datos en la tabla dominio.

Por otro lado, si los datos ingresados no son correctos se envía un codigo HTML al servidor WEB para que presente una pagina de error

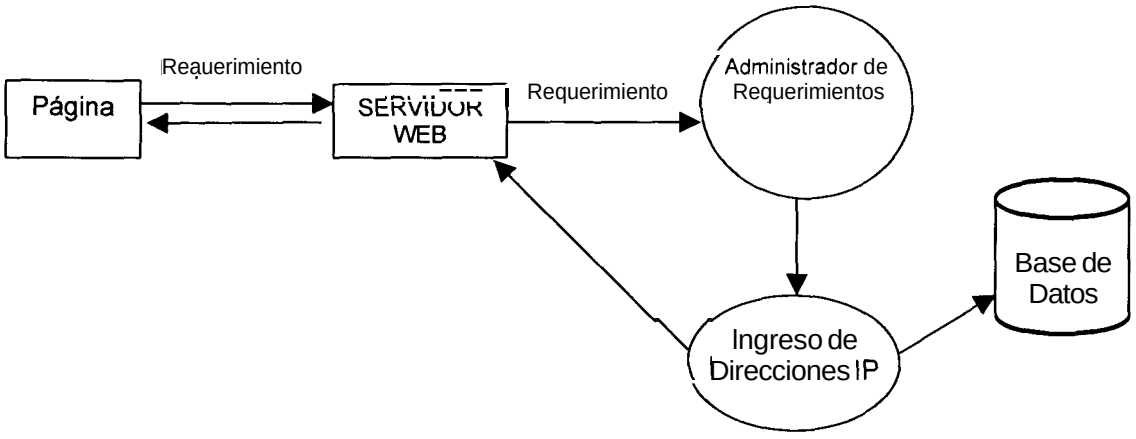


Fig. 6.7 Proceso para el ingreso de una dirección IP

6.4.2 Eliminacion de Direcciones IP

Al ser llamado, este submodulo recibe los id de las direcciones IP a ser borradas, y genera una llamada a la base de datos que las elimina de la tabla dominio. Si estas no existen en ningún otro registro de la tabla dominio y además son direcciones de red son eliminadas de la tabla de red.

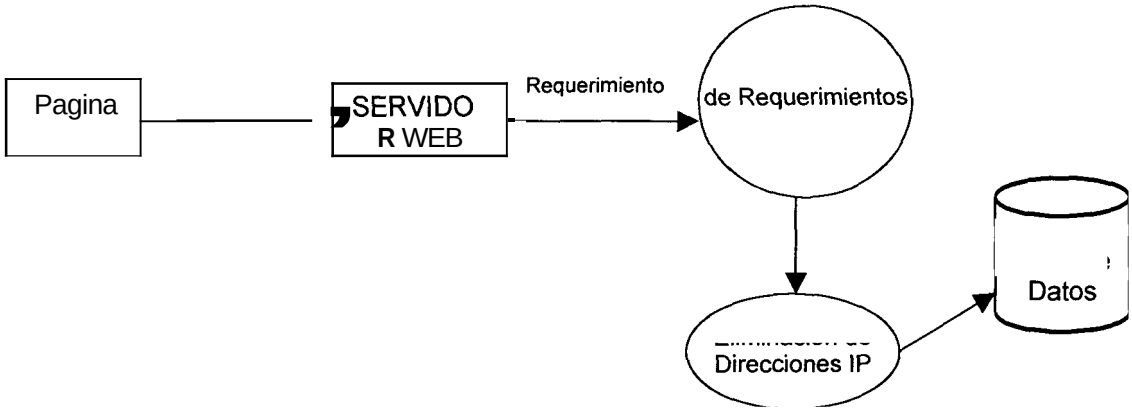


Fig. 6.8 Proceso para la eliminación de una Dirección IP

6.4.3 Ingreso de Protocolos de Aplicacion

Cuando es llamado, verifica que los datos ingresados por el administrador en el formulario sean correctos. Si es asi, genera una llamada a la base de datos que los ingresa en la tabla aplicacion. Si los datos no son correctos, se envía el codigo HTML al servidor WEB para que presente una pagina de error.

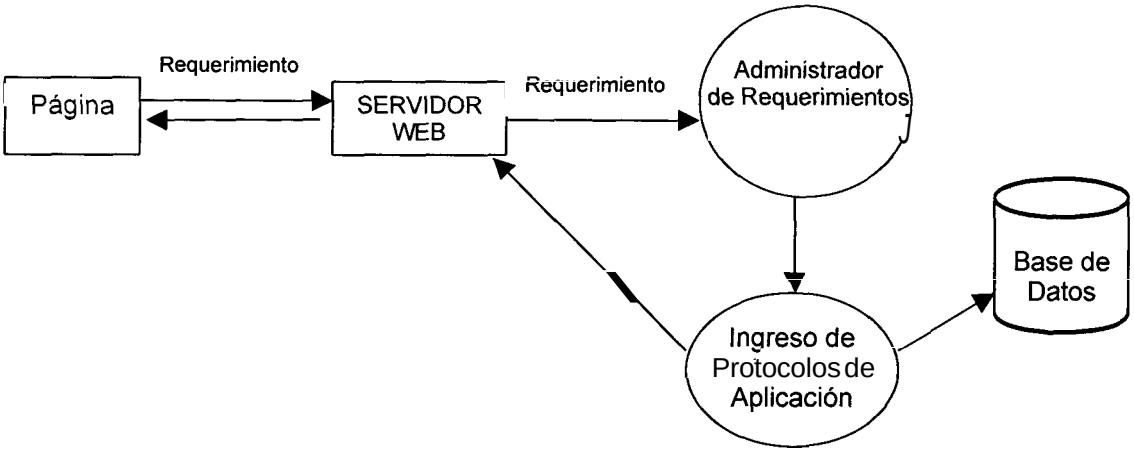


Fig. 6.9 Proceso para el ingreso de Protocolos de Aplicacion

6.4.4 Eliminacion de Protocolos de Aplicacion

Cuando es llamado, recibe el numero de puerto de los protocolos a ser borrados y genera una llamada a la base de datos que los elimina de la tabla aplicacion.

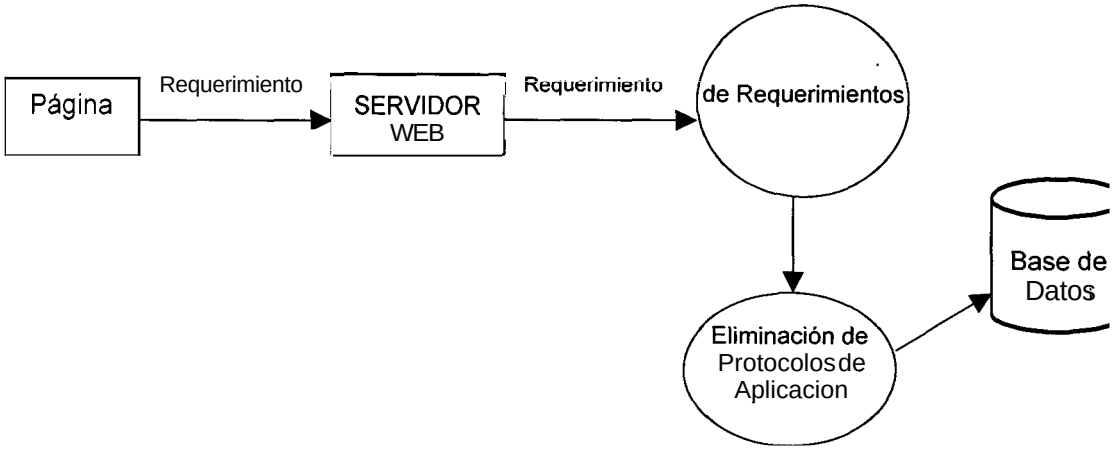


Fig.6.10 Proceso para la eliminación de Protocolos de Aplicacion

6.4.5 Ingreso de Redes a Excluir

Cuando es llamado, verifica que los datos ingresados por el administrador en el formulario sean correctos. Si es asi, genera una llamada a la base de datos que los ingresa en la tabla red con un valor para el campo dominio igual a cero. Si

los datos no son correctos, se envía un codigo HTML al servidor WEB para que presente una pagina de error.

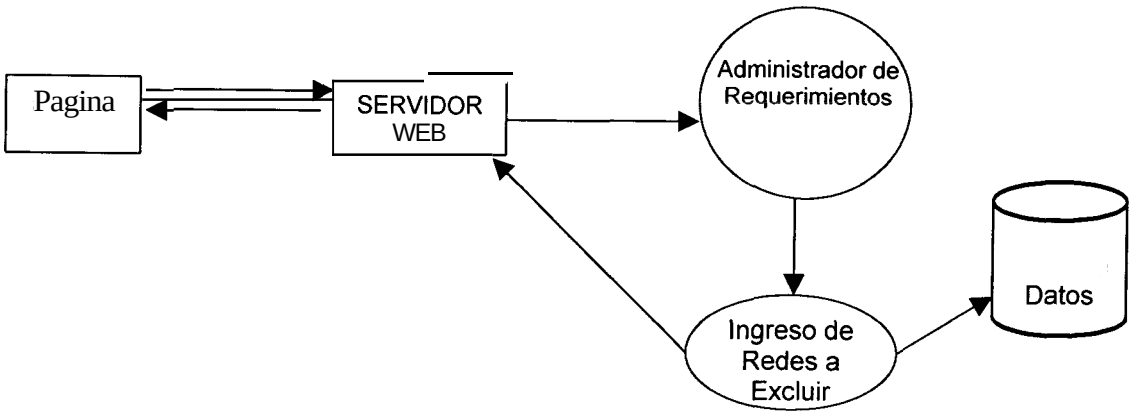


Fig. 6.11 Proceso para el ingreso de una red a excluir

6.4.6 Eliminación de Redes a Excluir

Cuando es llamado, recibe la dirección IP de las redes que se desean eliminar por parte del administrador de requerimientos, y genera una llamada a la base de datos que los elimina de la tabla red.

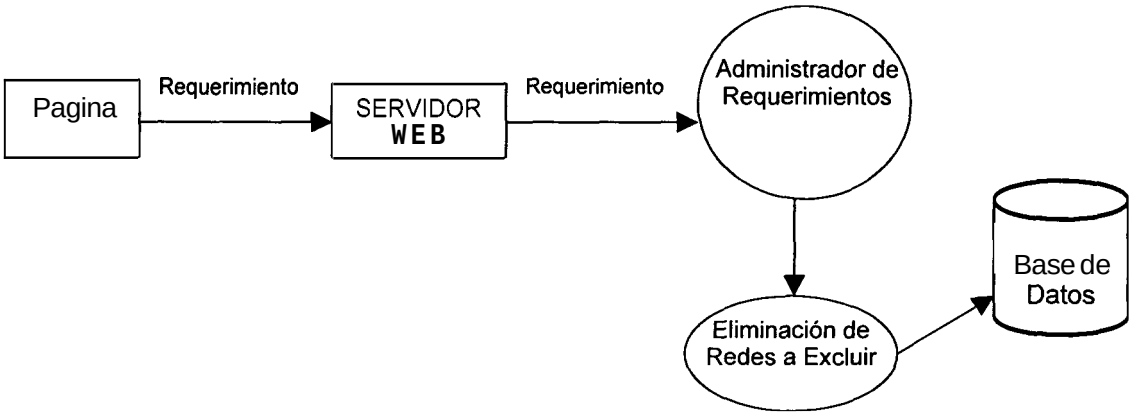


Fig. 6.12 Proceso para la eliminación de redes a excluir

6.5 Predeterminación de Consulta

Genera una llamada a la base de datos para obtener todas las aplicaciones y dominios de direcciones IP existentes, dividiendolas en funcion de predeterminadas y no predeterminadas. Llama al servidor WEB para que presente esta informacion en un formulario HTML. En la pagina HTML el administrador puede manipular los datos visualizados y, una vez que se recibe el requerimiento de actualizar la informacion, se hace una llamada a la base de datos para que las tablas respectivas sean actualizadas.

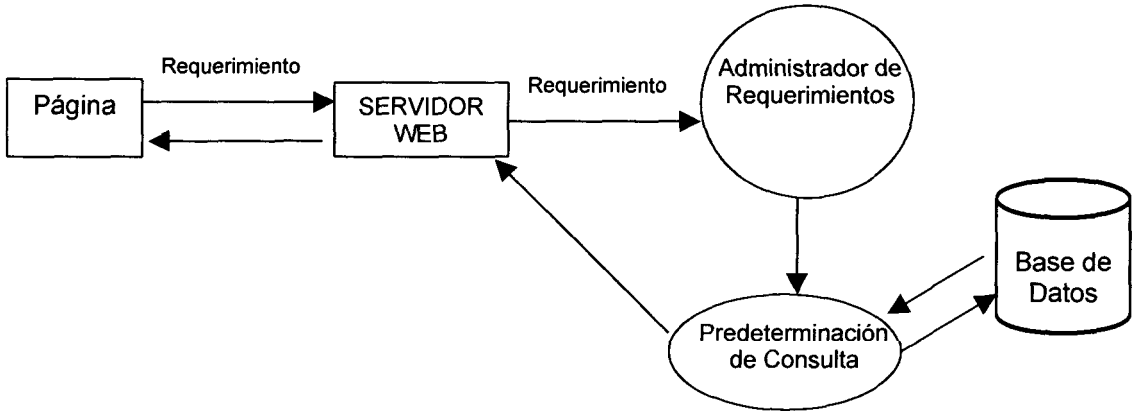


Fig. 6.13 Predeterrninacion de la consulta

6.6 Administración de Usuarios

El modulo administrador de usuarios se encarga de procesar los requerimientos de creacion, edicion y eliminacion de usuarios; para lo cual el modulo ha sido dividido en tres submodulos: creacion de usuarios, edicion de usuarios y eliminación de usuarios. En el momento que es llamado por el Administrador de Requerimientos genera una llamada a la base de datos para obtener la información de todos los usuarios del sistema y presentarla en una pagina HTML.

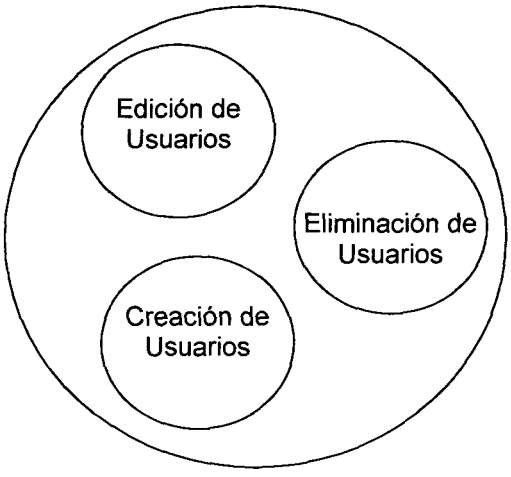


Fig. 6.14 Submbdulos de Administración de usuarios

6.6.1 Creación de Usuarios.

El Administrador de Requerimientos llama a este submódulo. Este genera un formulario en formato HTML con los campos de informacion necesarios para identificar a un usuario. El submodulo recibe estos datos para realizar la validación apropiada de los mismos. En caso de que la informacion sea correcta se genera la llamada a la base de datos, que los guarda en la tabla usuarios.

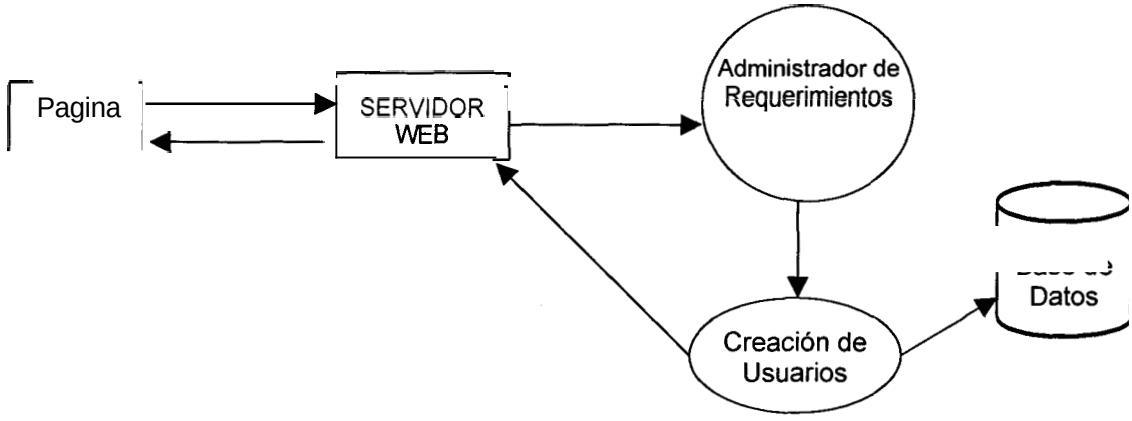


Fig. 6.15 Proceso para la creación de usuarios

6.6.2 Eliminación de Usuarios.

Al ser llamado por el Administrador de Requerimientos, este submodulo recibe el id del usuario (unico para cada usuario) a ser eliminado. Con este dato se genera la llamada a la base para la eliminación efectiva del mismo de la tabla usuario.

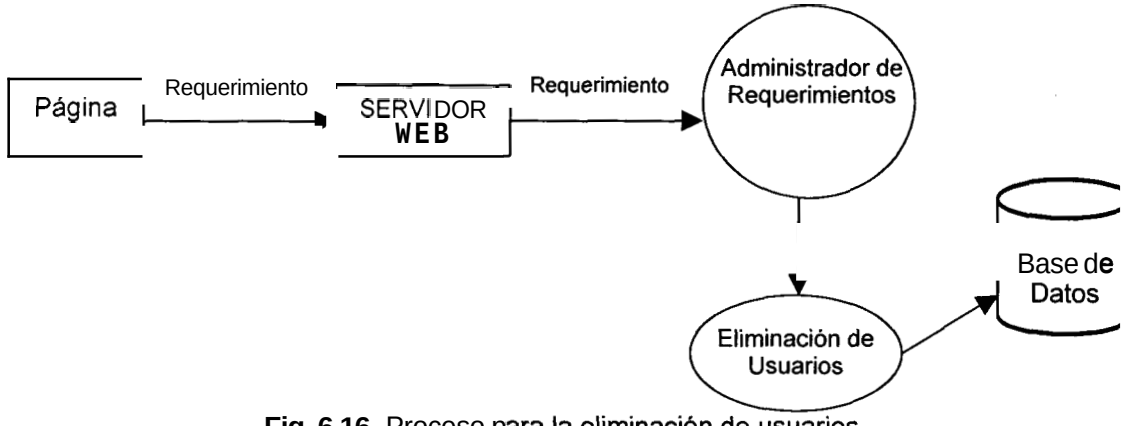


Fig. 6.16 Proceso para la eliminación de usuarios

6.6.3 Edición de Usuarios.

Este submodulo genera una llamada a la base de datos para obtener toda la informacion del usuario cuyo id recibimos del Administrador de Requerimientos. Presenta dicha informacion en una pagina HTML junto con un formulario que recibe los datos que el usuario desee modificar. Si el usuario decide confirmar, el submodulo valida los datos. En caso de que sean correctos, genera una llamada a la base de datos que actualiza la informacion pertinente al usuario en cuestion. Si los datos son incorrectos se envía al servidor WEB una pagina HTML indicando cual fue el error.

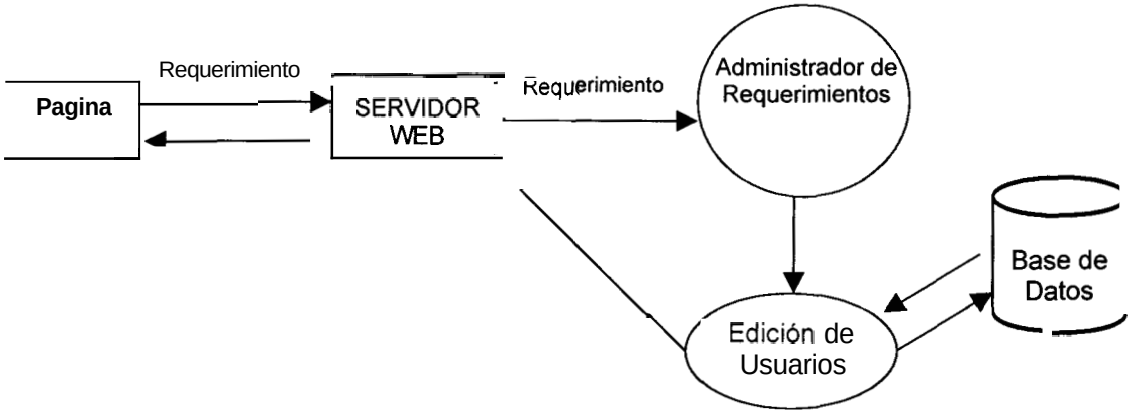


Fig. 6.17 Proceso para editar los usuarios existentes

6.7 Registros de Monitoreo

Al ser llamado por el Administrador de Requerimientos, este modulo genera una llamada a la base de datos para obtener todos los intervalos de tiempo en que el sistema monitoreo el trafico de la red. Construye un codigo HTML para presentar dicha información en un formulario y envía este codigo al servidor WEB.

El modulo tambien es llamado por el Administrador de Requerimientos para la Eliminación de intervalos de Monitoreo. En este caso, el modulo genera una llamada a la base de datos para actualizar la bandera de selección de borrado de los intervalos correspondientes, en la tabla historial. Hecho esto, llama a al proceso managedb, que encuentra en la base de datos todos los intervalos con bandera de borrado activada y borra todos los datos de los paquetes capturados durante cada uno de estos intervalos, borra de la tabla historial dichos intervalos y por ultimo realiza una actualización del espacio fisico de la base. Esta tarea puede ser muy larga dependiendo de la cantidad de datos que existan en la base, por lo cual se crea un archivo vacio que sirve como bandera para que el sistema pueda determinar el inicio y con el borrado del mismo el fin de este proceso.

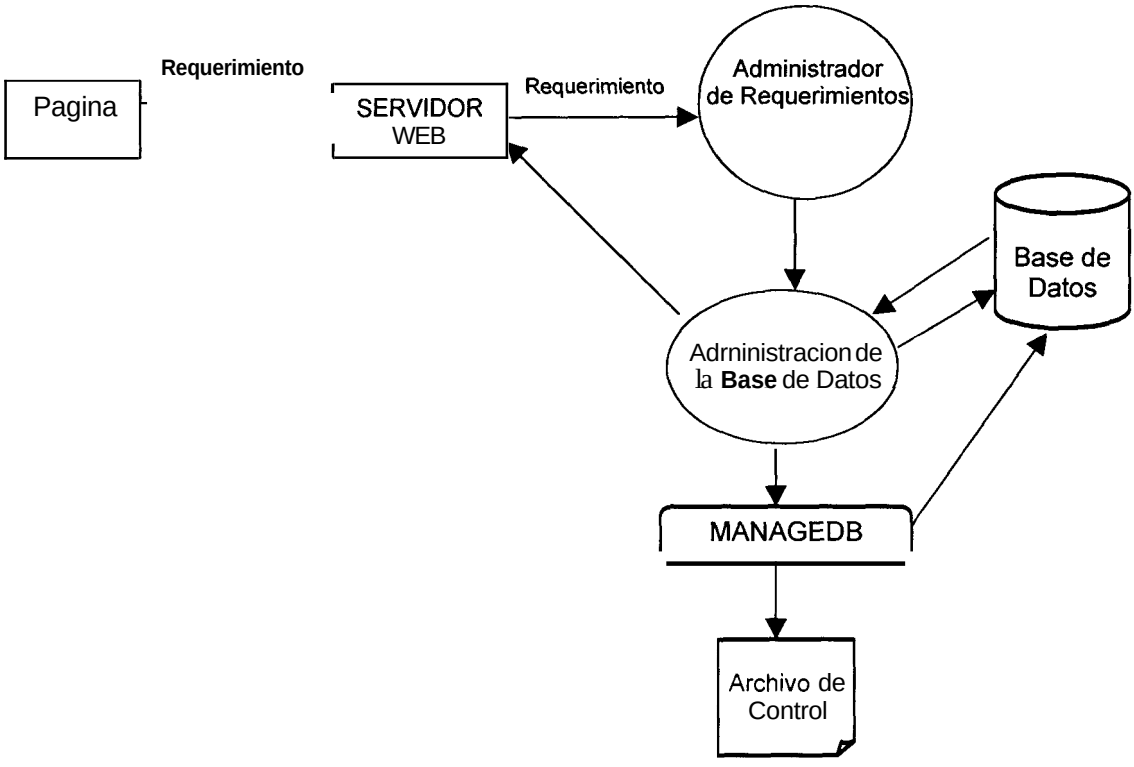


Fig. 6.18 Proceso para la Adrninistracion de la Base de Datos

6.8 Graficador

Para la generación de los graficos el sistema utiliza una utilidad denominada gnuplot (Linux version 3.5(pre 3.6) patchlevel beta **347).** Gnuplot es un programa grafico para plataformas como **UNIX,** MSDOS y VMS cuya funcion es permitir a cientificos y estudiantes visualizar funciones matematicas y datos. Gnuplot soporta diferentes tipos de terminales, plotters e impresoras y da

facilidades para extender soporte a nuevos dispositivos. Esta herramienta maneja dos tipos de curvas (2 dimensiones) y superficies (3 dimensiones). Las superficies pueden ser dibujadas acoplandose a funciones especificas, flotando en un espacio de 3-dimension, o como contorno en un plano x-y. Para diagramas en 2 dimensiones, existen muchos estilos de diagramacion, incluyendo lineas, puntos, lineas con puntos, barras de errores e impulsos(gráficos de barra). El grafico puede ser descrito utilizando leyendas arbitrarias, flechas, titulos, fechas, etc. La interfaz incluye un modo de edición en línea de comando y un historico, para la mayoría de las plataformas. Para la generación de los graficos, el sistema utiliza el estilo de lineas en un plano cartesiano(2 dimensiones) y soporta la posibilidad de mostrar varias graficas en un mismo archivo grafico de salida.

El Graficador utiliza los archivos planos creados por el modulo de Consulta de los CGIs, especificandole a la utilidad gnuplot, que estos seran los datos que serviran de base para la construcción de los graficos. Los datos dentro de cada archivo fueron almacenados con un formato especifico para que la utilidad gnuplot pueda procesar la informacion.

Las caracteristicas principales de este formato son las siguientes:

- Cada linea del archivo debe contener un punto por grafica. Para el grafico, cada punto representa un par de coordenadas. Los datos que representan al eje **x** aparecen una sola vez en cada linea. Los datos que representan al eje **y** aparecen en cada linea una vez por grafica.

- Los datos en cada linea del archivo deben estar separados por un espacio en blanco. Este espacio divide a cada linea en columnas.

- Los datos del eje **x** pueden ser omitidos. Si se da ese caso, asigna como valores de eje **x,** el numero de linea respectivo, comenzando desde 0.

- Una linea en blanco dentro del archivo significa el paso de una curva a otra.

El sistema genera siempre 3 archivos que contienen los datos de protocolos de aplicacion, protocolos de transporte **y** protocolos de red respectivamente. En cada archivo la información se puede describir de la siguiente manera:

- **Los** datos correspondientes a cada dominio de direcciones IP estan divididos por dos líneas en blanco, que representan el paso de una grafica a otra.

  El grupo de dominios de direcciones IP incluye los dominios seleccionados en el modulo de Consulta de los CGI´s mas un grupo que representa la suma de los dominios restantes.

- En cada línea de un bloque de datos perteneciente a un dominio de direcciones IP específico aparece la siguiente información:
  - Fecha/hora de monitoreo
  - Cantidad de datos en Bytes x Protocolo
  - Cantidad de datos en Paquetes x Protocolo

El grupo de protocolos incluye los protocolos(por capa) seleccionados en el modulo de Consulta de los CGIs mas un grupo que representa la suma de los protocolos restantes.

A continuación un ejemplo, tomado del archivo de protocolos de transporte:

Rango de Tiempo	TCP		UDP	
Bloque de Datos del dominio 200.9.176.0 -.....				
	Bytes	Paquetes	Bytes	Paquetes
1999/11/21/01/03/00	7744	176	15000	250
1999/11/21/01/04/00	7260	165	14160	236
1999/11/21/01/05/00	7350	167	14400	240
1999/11/21/01/06/00	4054	92	7440	124
1999/11/21/01/07/00	0	0	0	0
Bloque de Datos del dominio 200.9.176.5 -.....				
1999/11/21/01/03/00	0	0	0	0
1999/11/21/01/04/00	0	0	0	0
1999/11/21/01/05/00	0	0	0	0
1999/11/21/01/06/00	0	0	0	0
1999/11/21/01/07/00	0	0	0	0

El sistema no utiliza la línea de comandos de la utilidad gnuplot para generar el grafico; en su lugar construye un archivo con las instrucciones necesarias para que la utilidad gnuplot las ejecute. Este archivo debe tener extension gp, y las instrucciones allí almacenadas determinan las leyendas de los ejes, y de las curvas de la grafica, asi como los bloques y columnas del archivo plano que se tomaran en cuenta para la generación del grafico.

Una vez construido el archivo, el Graficador finalmente llama a la utilidad generadora de graficos (gnuplot), que recibe el archivo y produce un archivo grafico como salida.

7 Servidor de Estado y Monitoreo en Linea

El servidor de monitoreo en línea y estado es un programa que se ejecuta en una maquina esperando atender requerimientos. El cliente es el programa que se conecta al programa servidor para pedirle algun servicio.

Para simplificar el texto, se utilizará el nombre de "maquina servidora" para la maquina donde se esta ejecutando el programa servidor, "maquina cliente" para indicar la maquina donde se esta ejecutando el programa cliente, el programa servidor se denominara simplemente "servidor" y el programa cliente simplemente "cliente".

7.1 Caracteristicas del Servidor

El servidor es orientado a conexion, multiproceso y multihilo. Es orientado a conexion porque utiliza el protocolo TCP (Transfer Conexion Protocol). Las razones por las cuales se ha seleccionado este tipo de conexion son las siguientes:

1. Dado que el servidor debe responder a diferentes requerimientos de consulta, envía diferentes respuestas y necesita cerciorarse de que estas lleguen en orden. El software TCP garantiza la entrega de la informacion en el orden correcto.
2. Debido al acceso remoto que provee el sistema, las maquinas clientes pueden encontrarse fisicamente distantes de la maquina servidora e incluso en una red lógica distinta. El software TCP da confiabilidad de que la informacion llegara correctamente y sin errores.

7.2 Estructura básica del servidor

El servidor consta de:

- Un proceso padre el cual espera por un puerto las conexiones de los clientes para atender los requerimientos, este puerto recibe el nombre de "puerto de control". Los requerimientos que se pueden atender son los siguientes:

a) Iniciar el capturador historico.

b) Pedir el estado del capturador historico.

c) Detener el capturador historico

d) Iniciar el monitoreo en línea.

Cada uno de estos servicios implica una conexión nueva al puerto de control del servidor.

- Un proceso denominado hijo, que espera requerimientos del proceso padre indicandole que puede habilitar un puerto, al cual denominaremos "puerto de transferencia". Para que el proceso hijo no acepte conexiones de cualquier cliente el proceso padre envía al proceso hijo como parametros la dirección IP y el puerto mediante el cual se conecta el cliente. Una vez habilitado este puerto, el cliente especificado puede solicitar la transferencia de datos del monitoreo en línea.

7.3 Protocolo de Comunicacion entre procesos

La comunicacion entre procesos se realiza por medio de pipes (fig.) Un pipe es como una especie de entubamiento, donde un proceso escribe y el otro lee. Si un proceso escribe mas rapido de lo que el otro proceso lee, lo que se va escribiendo queda almacenado en una cola. Para esta comunicacion se utilizan dos pipes asociados a cada proceso, uno para escribir y otro para leer. El pipe que usa un proceso para escribir lo usa el otro proceso para leer, y viceversa.

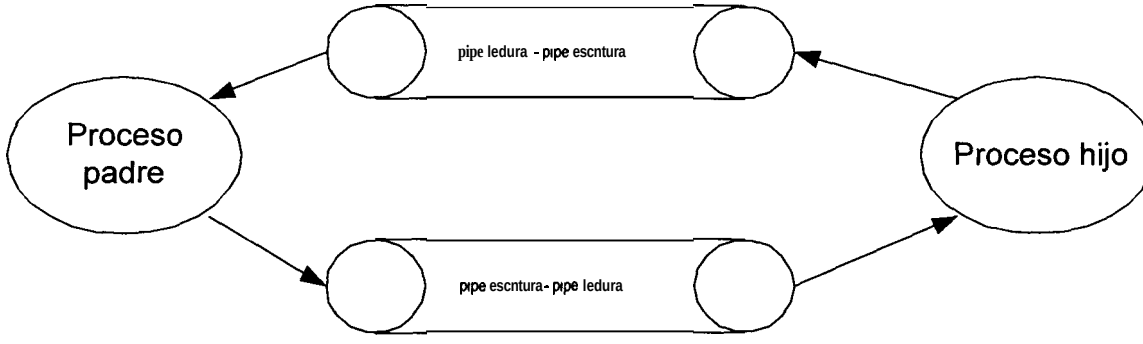


Figura 7.1 Descripción de comunicación mediante PIPE's

Como se observa en la figura 7.1, lo que un proceso escribe por un lado de un tubo (pipe) es lo que le llega al otro proceso por el otro extremo del mismo tubo.

El proceso que espera por el puerto de control es padre del proceso que espera por el puerto de transferencia. De ahora en adelante al proceso que espera por el puerto de control se lo llamara proceso padre y al que habilita el puerto de transferencia, proceso hijo.

Cada proceso esta en capacidad de crear nuevos procesos y nuevos hilos. De esta forma el servidor puede atender a varios clientes al mismo tiempo.

7.3.1 Comportamiento Iterativo y Concurrente

El servidor esta diseñado para atender ciertos requerimientos como servidor de tipo iterativo y otros como servidor de tipo concurrente. Se comporta como un servidor iterativo cuando atiende los servicios denominados requerimientos de monitoreo historico que son: iniciar o detener el monitoreo de trafico y consultar el estado del capturador historico. Es de tipo concurrente para atender los requerimientos del monitoreo en línea.

7.3.2 Proceso de Atencion de requerimientos

El proceso de atencion de requerimientos se detalla a continuación:

1. El cliente Se conecta al servidor por el puerto de control.
2. Envía un valor que implica una acción, esto es:
   a) Iniciar el capturador de paquetes
   b) Detener el capturador de paquetes
   c) Pedir un estado del capturador de paquetes
   d) Iniciar el monitoreo en línea
3. El servidor atiende los requerimientos a), b) y c) iterativamente, es decir, no crea un hilo o proceso con la nueva conexion dedicada. El servidor levanta al monitoreador de trafico cuando el cliente haga un requerimiento **a).** Para llevar a cabo esta operacion el proceso padre crea un nuevo proceso, el cual envía a ejecutar al monitor de trafico. El proceso padre verifica si se ha levantado el monitor de trafico enviando al cliente un valor indicando el exito o fracaso de la operacion, cerrando finalmente la conexion; cabe recalcar que el cliente no es atendido concurrentemente, pues el proceso que se crea es **solo** para delegar el levantamiento del monitoreo y no para atender

a un cliente y que no pueden haber dos instancias de monitor de tráfico. Para el caso **b),** el proceso padre devuelve un valor, que indica si el monitor de trafico está o no levantado. Para atender el caso **c),** el proceso padre envía una setial al monitor de trafico y devuelve un valor de exito o fracaso, segun se haya o no detenido el monitoreo.

4. Para atender el requerimiento **d),** el proceso padre crea un nuevo hilo, entregandole a este ultimo la conexion como parametro; de esta manera el nuevo hilo maneja y atiende los requerimientos del cliente. Si otro cliente pide iniciar el monitoreo en línea, el servidor sera capaz de atenderlo, creando otro hilo y pasandole como parametro la nueva conexion al nuevo hilo. El servidor esta disetiado para atender simultaneamente muchos clientes que deseen ver el trafico IP en línea.

7.4 Protocolo de Comunicacion Cliente-Servidor

A medida que se vaya explicando el monitoreo historico, se ira detallando el protocolo que se utiliza para la comunicacion cliente-servidor.

Como ya se explico, en el servidor existe un proceso padre que es el que espera requerirnientos de los clientes por un puerto de control. Por defecto el puerto es el 2000.

El cliente es un programa hecho en Java que corre desde un browser (applet).

7.4.1 Protocolos cliente/servidor de estado de monitoreo

Para iniciar el monitoreo historico, el cliente sigue los siguientes pasos:

1. Establece una conexion al puerto de control del servidor.
2. Envía un valor (100) que indica que se desea iniciar el monitoreo historico.
3. El servidor crea un nuevo proceso, y este reemplaza su imagen con la del capturador que guarda los paquetes en la base.
4. Si el proceso se crea correctamente y carga el ejecutable (el capturador) correctamente, el proceso padre envía 110 al cliente si esta bien, 0 si esta mal.
5. El servidor cierra la conexion
6. El cliente dependiendo del valor recibido, informa al usuario del exito o fracaso de la operación.

Para ver el estado del monitoreo de trafico:

1. Se establece una conexion al puerto de control del servidor
2. El cliente envia el valor 102, indicando que desea que le retornen el estado del monitoreo historico.
3. El servidor responde cualquier valor mayor a cero si el monitoreo de trafico logro ejecutarse satisfactoriamente caso contrario envia el valor de cero. El proceso padre del servidor determina si se esta ejecutando el monitoreo de trafico, si es que existe un proceso asignado a la ejecucion del mismo (de hecho, lo que devuelve en ese caso es el process–id del nuevo proceso creado que corre el capturador de paquetes, he aqui la razon por la cual se devuelve un valor mayor a cero.
4. El servidor cierra la conexion.
5. El cliente, dependiendo del valor recibido, modifica su estado o lo mantiene.

Para detener el monitoreo historico, el cliente:

1. Establece una conexion al puerto de control del servidor.
2. Envía el valor 101, que indica al proceso padre del servidor que el cliente desea detener el monitoreo de trafico.

3. El proceso padre verifica si el monitoreo se esta ejecutando. De ser asi, manda la señal SIGINT (Ctrl-C) al proceso asignado a la ejecucion del monitoreo, y espera a que el proceso termine. El monitoreo, al recibir dicha señal, deja de capturar paquetes, guarda los ultimos paquetes en la base, y modifica los registros de monitoreo.
4. El servidor responde con el valor 111 indicando que el monitoreo ya no esta activo.
5. En caso de que no haya un proceso corriendo el monitoreo y el servidor recibe un requerimiento de detener el monitoreo historico, el proceso padre devuelve igualmente el valor 111, ya que pudo haber sido que otro cliente detuvo el monitoreo y el primer cliente aun no habia actualizado su estado Cabe mencionar que el cliente actualiza su estado cada 4 segundos.
6. El servidor cierra la conexion.
7. El cliente actualiza su estado.

7.4.2 Protocolos cliente/servidor del monitoreo en línea e interacción entre protocolos

A medida que se vaya explicando el funcionamiento del monitoreo en línea, se ira detallando el protocolo cliente-servidor, así como tambien el protocolo entre procesos.

El cliente es un programa hecho en Java, que corre desde un browser (applet). A este cliente se le llamara simplemente el applet. Este programa cada vez que es iniciado recibe un conjunto de parametros. El applet usa estos parametros para saber que redes debe monitorear, que red debe excluir, que protocolos debe monitorear, y cuales son todas las posibles redes que debe excluir.

El applet tiene la particularidad cambiar las redes y protocolos que monitorea junto con las redes que excluye aun cuando este funcionando. A esta operación se le llamara regenerar el grafico.

El applet inicialmente recibe solo cero o una red a excluir, pero le es entregado todo un conjunto de posibles redes a excluir. Cuando el cliente decide regenerar el grafico, puede escoger mas redes a excluir.

Antes de profundizar en la explicación del funcionamiento del servidor, se describira unos conceptos utiles.

Dominio: Un dominio es un par de direcciones que se van a sensar. Por **ejemplo,** de la red 200.9.176.0 a la maquina 192.188.59.2. Las maquinas son tambien conocidas como hosts.

Tipos de dominio: Los dominios son de 8 tipos, a saber:

1 Hosta Host
2 Host a Red
3 Red a Host
4 Red a Red
5 Host a Mundo
6 Reda Mundo
7 Mundoa Host
8 Mundo a Red

Los dominios del 5 al **8,** constan solo de una dirección IP, ya que el mundo es cualquier maquina del mundo. Los dominios del 1 al **4,** como se indico en la definición de dominio, constan de un par de direcciones IP.

Protocolo: Es una interfaz completa que sirve de plataforma para toda una capa de modelo de comunicacion de datos. Sobre un protocolo pueden funcionar muchas aplicaciones. Ejemplos de protocolos son: TCP, UDP, ICMP.

Aplicacion: El concepto de aplicacion es muy amplio, pero el usado es el de aplicacion como programa hecho para funcionar sobre algun protocolo y que esta en capacidad de brindar algun servicio. En pocas palabras, es un servidor, pero tiene el nombre de aplicacion ya que, como su nombre lo indica, aplica la funcionalidad de algun protocolo para brindar algun servicio. Para que las aplicaciones esten en capacidad de brindar servicios, esperan por un puerto o puertos, por ejemplo: TELNET espera en el puerto 23, etc.

Asociacion: Una asociacion es un par dominio-aplicacion o dominio-protocolo que el servidor sensara.

Redes a excluir: Puede el cliente especificar una o varias redes a excluir. Por ejemplo, si se va a sensar una asociacion cuyo dominio es de tipo red a mundo, y es de la dirección 200.9.176.0 al mundo, excluyendo la red 200.9.176.0, el servidor sabe que lo que va a excluir son los paquetes cuya red destino sea la red 200.9.176.0. No tendría sentido excluir los paquetes cuya red fuente sea la 200.9.176.0, porque entonces no sensaria nada.

La tabla 7.1 muestra cómo el servidor excluye, para cada tipo de dominio, basandose en las dos redes (RedO y Redl) que le son enviadas por el cliente como redes a excluir.

Cada vez que el servidor captura un paquete, por cada asociacion obtiene el dominio, y segun el tipo del dominio observa si debe excluir el paquete tomando en cuenta la red fuente o la red destino del paquete.

Host a Host	Nunca excluye
Host a Red	Excluye los paquetes cuya red destino es igual a RedO o a Redl
Red a Red	Excluye los paquetes cuya red fuente es igual a RedO o a Red1, o los paquetes cuya red destino es igual a RedO o a Redl
Red a Host	Excluye los paquetes cuya red fuente es igual a RedO o a Redl
Host a Mundo	Excluye los paquetes cuya red destino sea igual a RedO o a Redl
Red a Mundo	Excluye los paquetes cuya red destino sea igual a RedO o a Redl
Mundo a Host	Excluye los paquetes cuya red fuente sea igual a RedO o a Redl
Mundo a Red	Excluye los paquetes cuya red fuente sea igual a RedO o a Redl

El servidor, no siempre excluye un paquete basandose solo en su red fuente, sino para ciertos tipos de dominio excluira un paquete basandose en su red fuente, y otros los excluira basandose en la red destino del paquete.

El servidor excluye basandose en la red fuente del paquete para los siguientes tipos de dominios: Red a Host, Red a Red, Mundo a Host y Mundo a Red

El servidor excluye basandose en la red destino del paquete para los siguientes tipos de dominios: Host a Red, Red a Red, Host a Mundo y Red a Mundo.

Una vez aclarados estos conceptos, se dara en detalle la forma como funciona el cliente junto con el servidor. Mas adelante se muestra un diagrama de estados y una tabla de interacción de protocolos, que ayudaran a aclarar el funcionamiento cliente/servidor.

7.5 Monitoreo en línea

El cliente se conecta al proceso padre del servidor al puerto de control y envía 34 por la conexion, indicando que desea iniciar el monitoreo en línea. A esta conexion se le llamara conexion de control.

El servidor, como ya se explico, tiene dos procesos: un proceso padre que espera por un puerto de control, y un proceso hijo que espera por una setial del proceso padre para habilitar la espera por puerto de transferencia. El proceso padre, al recibir el valor 34, detecta que se trata de un monitoreo en linea, procede entonces a crear un hilo y le pasandole como parametro la conexion. A este nuevo hilo creado por el proceso padre, lo llamaremos hilo de control.

7.5.1 Protocolo de monitoreo en linea.

Los pasos que sigue el hilo de control para iniciar el monitoreo en linea son:

1. El cliente envia un cero, indicando que desea iniciar el monitoreo.
2. El hilo de control envia el valor de cero al proceso hijo por medio del pipe, indicandole que un cliente desea iniciar el monitoreo en linea. El proceso hijo entonces, espera por una conexion.
3. El cliente se conecta ahora al puerto de transferencia que fue habilitado a raiz de que el proceso hijo recibio el cero que le envio el proceso padre por el pipe. A esta conexion se la llamara conexion de transferencia.

4. El cliente envia por la conexion de control los datos de la conexion de transferencia, es decir, la direccion de IP del cliente y el puerto de transferencia del cliente.
5. El hilo de control espera por la conexion de control estos datos (direccion y puerto). Si dentro de ocho segundos el cliente no envia estos datos, las conexiones de control y transferencia son cerradas, y termina el hilo de control.
6. Una vez que el cliente envia su direccion ip y numero del puerto usado para la conexion al hilo de control, este envia estos datos por medio del pipe de escritura del proceso padre, al proceso hijo. El proceso hijo lee del pipe los datos, obtiene la direccion ip y el puerto de la conexion que acaba de recibir, si son iguales deduce que el cliente es correcto. Si el cliente no es correcto, el proceso hijo envia un cero por medio del pipe al proceso padre.
7. El proceso hijo crea un nuevo hilo y le envia como parametro la conexion de transferencia. A este hilo lo llamaremos hilo de transferencia. Luego, el proceso hijo envia un 1 al proceso padre por el pipe, indicandole que el cliente es correcto. Adicionalmente el proceso hijo envia despues del 1 el identificador del hilo de transferencia por medio del pipe al hilo de control. Esto se hace para que cuando el cliente desee terminar la transferencia,

el hilo de control sepa indicarle al proceso hijo que hilo debe detenerse pasandole como parametro al proceso hijo este identificador.

8. Dependiendo de que recibe el padre, 0 ó 1, de parte del proceso hijo para indicarle que el cliente es correcto, el padre realiza ciertas acciones. Si recibe 1, coloca 1 en una bandera indicando que esta corriendo el hilo de transferencia, y luego espera por algun requerimiento del cliente (parar la transferencia o terminar). Si recibe cero, espera a que el hilo de transferencia termine y espera por otro cliente.
9. El hilo de control ahora se encarga de manejar los requerimientos del cliente. El hilo de transferencia recibe:
    1. El tipo de senso a efectuar: cero paquetes, uno bytes.
    2. La frecuencia a sensar, llamada hz: cada hz-1 segundos, el hilo de transferencia se dormira, y sensara durante 1 segundo los bytes o paquetes, segun el tipo de senso, para cada asociacion dominio-protocolo especificada, y enviara estos valores en orden al cliente.
    3. El numero de total de redes ingresadas por el cliente al momento de configurar la consulta (Capitulo 6.).
    4. Las redes ingresadas por el cliente, junto con la mascara de red de cada una.
    5. El numero de dominios a sensar.

6. Las asociaciones dominio-protocolo a sensar junto con el tipo de asociacion.
7. El numero de redes a excluir.
8. Las redes a excluir, junto con la mascara de red de cada una.

10. El servidor respondera cada **hz** segundos al cliente por cada par dominio-protocolo que halla notificado para sensar.
11. El hilo de transferencia inicia la captura de paquetes e inicia un ciclo por medio del cual se le envian al proceso padre los valores de la captura. Este ciclo sensa por una bandera, de tal forma que cuando esta bandera es configurada a cero sale del ciclo.

La figura 7.2 muestra un resumen del funcionamiento cliente/servidor del presente sistema:

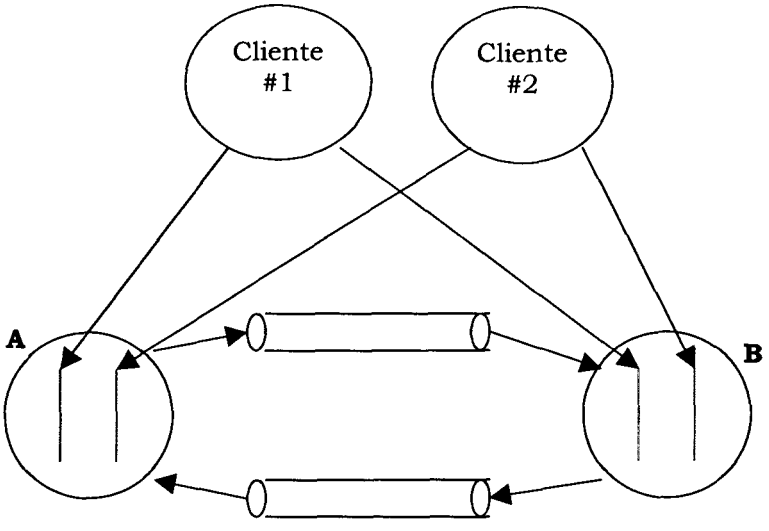


Figura 7.2 Esquema funcional cliente/servidor del Sistema monitor de tráfico

Donde el circulo **A** representa al proceso padre, el circulo B al proceso hijo. El proceso padre **(A)** posee dos hilos de control. El segmento izquierdo representa el hilo de control del cliente **#**1, **y** la flecha que une el cliente **#1** con este segmento es la conexion de control. El segmento derecho representa el hilo de control del cliente #2, **y** la flecha que une al cliente **#2** con este segmento es la conexion de control del cliente #2. El proceso hijo (B) posee dos hilos de transferencia. El segmento izquierdo representa el hilo de transferencia asignado al cliente **#**1, **y** la flecha que une este cliente con este segmento es la conexion de transferencia del cliente **#1**. El segmento derecho representa el hilo de transferencia asignado al cliente #2, **y** la flecha que une este cliente con este segmento representa la conexion de transferencia del cliente #2.

7.5.2 Cambio de configuración de monitoreo en línea.

Cuando se cambia la configuracion de las asociaciones que se estan sensando, primero se detiene la transferencia de datos para luego regenerar el grafico en linea.

Detención de transferencia de datos: Para lograr este objetivo el cliente debe:

1. Enviar un 1 por la conexion de control al hilo de control, indicando que desea detener el monitoreo.
2. El hilo de control envia este mensaje mediante el pipe al proceso hijo, junto con el identificador del hilo de transferencia cuya sesion se va a cerrar.
3. El proceso hijo setea la bandera que mantiene al hilo de transferencia en cero, para que el ciclo termine. Luego el proceso hijo espera al hilo de transferencia a que termine por medio de una llamada al sistema que devuelve un valor, indicando si finalizó correctamente.
4. El hilo de transferencia a su vez, a la salida del ciclo, cierra la conexion de transferencia y termina.
5. Cuando el proceso hijo a terminado de esperar al hilo de transferencia, envia el valor 17 al hilo de control por medio del pipe, indicandole que ha terminado la transferencia correctamente.
6. El hilo de control envia el 17 al cliente, indicandole que fue finalizada correctamente la transferencia. En caso de que este **17** no sea recibido, simplemente se cierran la conexion de transferencia.

Regeneración de grafico en línea: Cuando el cliente ha finalizado la transferencia, puede iniciarla nuevamente pero con distintos parámetros, por

ejemplo, distintas asociaciones dominio-protocolo y distintas redes a excluir. Para esto se siguen exactamente los mismos pasos del inicio inicia el monitoreo en linea.

7.5.3 Finalización del monitoreo en línea.

Cuando el cliente desea terminar, envía un 2 al hilo de control por la conexión de control. El hilo de control, al recibir este 2, termina decrementando un contador que indica el numero de hilos de control actualmente activos en el proceso padre.

7.5.4 Diagrama de estados del servidor.

Un diagrama de estados clarifica mejor la situación:

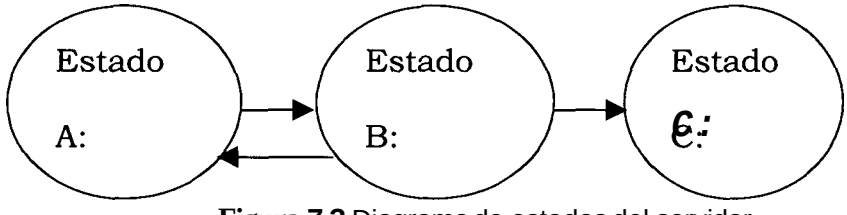


Figura 7.3 Diagrama de estados del servidor

Cada hilo de control tiene una bandera que le indica el estado en que se encuentra. Recordemos de que el una vez creado el hilo de control, este se encarga de manejar los requerimientos del cliente, ya no el proceso padre. Diremos ahora que el cliente envia los requerimientos al hilo de control.

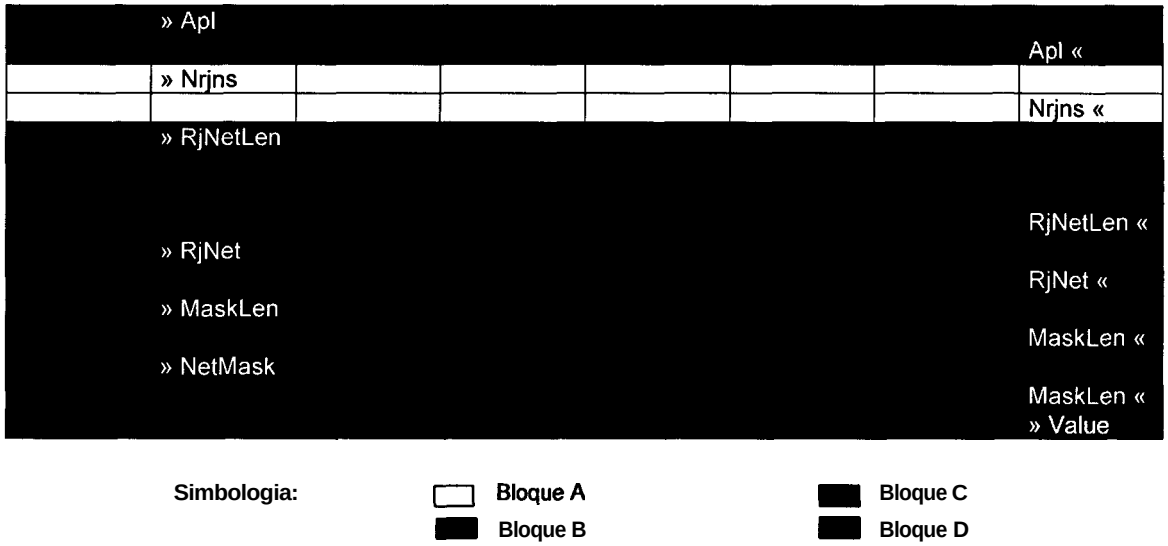
1. El hilo de control cae en el estado **A** cada vez que el cliente envia un requerimiento de iniciar la transferencia. El proceso padre para atender al cliente, crea un nuevo hilo de control, este ultimo envia un requerimiento al proceso hijo de que se desea inicia una transferencia, el proceso hijo habilita el puerto de transferencia, el cliente se conecta al puerto de transferencia, se valida que el cliente sea correcto, se crea un nuevo hilo de transferencia y el proceso hijo envia el identificador del hilo de transferencia al hilo de control. Entonces este hilo de control setea esta bandera a *corriendo*, indicando que se halla en el estado **A.** En este estado, solo se puede pasar a un unico estado posible: el estado **B**. Cabe recordar que luego de esto, quien se encarga de recibir todos los dominios que se van a monitorear, las redes a excluir y los protocolos a sensar, es el hilo de transferencia a traves de su conexion (la conexion de transferencia).
2. Cuando el hilo de control recibe un requerimiento del cliente de finalizar la transferencia, este lo envia al proceso hijo junto con el identificador del hilo

que se debe terminar, de tal manera que si hay muchos hilos de transferencia de varios clientes, se sabe cual es el que debe finalizar. El proceso hijo envia una señal al hilo de transferencia indicado y lo espera, y luego envia al hilo de control un valor indicando que fue correctamente finalizada la transferencia. El hilo de control seta la bandera a *detenido*, indicando que se encuentra en el estado **B.** De aqui se puede pasar a dos estados posibles: Volver al estado de transferencia iniciada o terminar definitivamente el hilo de control, lo cual se registra a nivel del proceso padre que pasa a un estado ***C.***

3. Si el cliente desea volver a iniciar la transferencia, envia de nuevo el requerimiento al hilo de control de regenerar el grafico y se repiten todos los pasos descritos en el punto 1 hasta llegar al estado **A.** Si el cliente desea terminar su sesion, envia un valor al hilo de control indicando que desea salir y terminar el monitoreo en linea definitivamente, para lo cual el hilo de control cierra la conexión de control y termina, no sin antes decrementar un contador global a nivel del proceso padre, que es el que lleva un registro del numero de hilos de control creados (el numero de clientes que se esta atendiendo simultaneamente).

7.5.5 Cuadro esquematico de interacción de protocolos.

Cliente		**Proceso padre**		**Proceso hijo**		**Hilo control**	**Hilo trans.**
Conexión control	Conexión trans.	Conexión control	Pipe	Conexión trans.	Pipe	Conexión control	Conexión trans.
» 0							
						0 «	
» Dir ip							
						Dir ip «	
» Puerto							
						Puerto «	
			» Dir ip				
					Dir ip «		
			» Puerto				
					Puerto «		
			1 «				
						» 1	
1 «							
					» Thread id		
			Thread id «				
	» tsenso						
							tsenso «
	» Hz						
							Hz «
	» Nnets						
							Nnets «
	» NetIpLen						
							NetIpLen «
	» NetIp						
							NetIp «
	» MaskLen						
							MaskLen «
	» Mask						
							Mask «
	» Ndoms						
							Ndoms «
	» DomType						
							DomType «
	» SrcIpLen						
							SrcIpLen «
	» SrcIp						
							SrcIp «
	» DstIpLen						
							DstIpLen «
	» DstIp						
							DstIp «



Este es un cuadro descriptivo de todo el proceso que ocurre tanto en la comunicacion cliente-servidor, como en la comunicacion entre procesos.

El signo » antepuesto a algo, indica que se envia. Por ejemplo, » 0, indica que se envia 0. Lo que tiene a continuacion el signo «, es que se recibe. Por ejemplo, 1 «, indica que se recibe el 1. A continuacion redactaremos cierta nomenclatura:

Dirip: Direccion ip del cliente

Puerto: Puerto del cliente utilizado en la conexión de transferencia

Thread *id:* Identificador del hilo de transferencia

Tsenso: Tipo de senso a efectuar: 0 si es paquetes, 1 si es bytes

Hz: Numero de segundos + 1 que el hilo de transferencia dormira antes de capturar y sensar los paquetes en el siguiente segundo

Nnets: Numero de redes conocidas ingresadas por el usuario en administración de direcciones ip

NetIpLen: Longitud de la direccion ip la red. Por ejemplo: 192.188.59.2 tiene longitud 12

NetIp: Direccion ip de la red cuya longitud se envio previamente (NetIpLen)

MaskLen: Longitud de mascara de red de la direccion que se envio previamente (Netlp). Por ejemplo: 255.255.0.0 tiene longitud 11

Mask: Mascara de red correspondiente a la longitud enviada previamente

Ndoms: Numero de asociaciones dominio-protocolo que se sensarán

DomType: Tipo de dominio que se va a enviar

SrcIpLen: Longitud de la direccion ip fuente del dominio que se esta enviando

SrcIp: Direccion ip fuente del dominio que se esta enviando

DstIpLen: Longitud de la direccion ip destino del dominio que se esta enviando

DstIp: Direccion ip destino del dominio que se esta enviando

Apl: Protocolo o aplicacion que se sensara para ese dominio

Nrjns: Numero de redes que se excluiran

RjNetLen: Longitud de la direccion ip de la red a excluir

RjNet: Red a excluir

MaskLen: Longitud de la mascara de la red a excluir

Mask: Mascara de la red a excluir

Value: Valor que se envía al cliente cada Hz segundos y que indica la cantidad de paquetes o bytes en ese ultimo segundo.

Las secciones marcadas son bloques que se ejecutan dentro de lazos. A continuación se detalla:

a) El *bloque A* indica un lazo regulado por Nnets. Es decir, esta seccion sera repetida Nnets veces.

b) El *bloque B* indica un lazo regulado por Ndoms. Esta seccion se repetira Ndoms veces. Hay que notar que dependiendo del tipo de dominio, varia el bloque. Por ejemplo, en los dominios cuyo tipo es de una direccion ip a otra (host a host, host a red, red a host, red a red), se envian y reciben SrcIpLen, Srclp, DstIpLen, Dstlp. Pero si los dominios que se van a recibir del cliente son de tipo de una direccion IP al mundo o del mundo a una direccion IP (host a mundo, red a mundo, mundo a host, mundo a red), solo se recibe un par: IpLen e Ip. Apl siempre se recibe.

c) El *bloque* C se ejecuta Nrjns veces.

d) El *D* es un bloque que se ejecuta Ndoms veces enviando los valores que son de interes para el cliente.

*¿ Como el cliente sabe **que** valor corresponde a **que** asociacion dominio-protocolo?* Pues, en el mismo orden en que el cliente envio sus asociaciones, el servidor respondera. Estas asociaciones son recibidas en el bloque B. Por ejemplo: si el cliente envio como asociaciones a monitorearse:

Asociacion 1: Red1 a red2, TELNET

Asociacion 2: Host3 a mundo, HTTP

Asociacion **3:** Red5 a host6, FTP

El servidor respondera 3 valores: valor para asociacion 1, valor para asociacion 2 **y** por ultimo, valor para asociacion 3, en ese orden. De esta forma el cliente sabe que valor corresponde a que asociacion.

8 Clientes Monitoreo

A continuación se detallara los clientes que interactuan con el servidor de monitoreo, son: Cliente de monitoreo en linea y Cliente de estado de monitoreo.

Tanto el cliente del monitoreo en linea como el cliente de estado de monitoreo, es un programa en Java que corre desde un browser. Estos programas en Java comunmente se los denomina applets.

8.1 Cliente de monitoreo en linea

Una vez que este cliente es invocado, inmediatamente trata de conectarse al servidor por el puerto de control (por defecto el 2000). Si falla, el cliente envía al usuario un mensaje de servidor inactivo.

8.1.1 Estructura y funcionamiento

El cliente monitorea asociaciones que, como se explico en capitulo 7, son un par dominio-aplicacion o dominio-protocolo que se desea monitorear. En cada uno

de los dominios de las asociaciones, se puede especificar una direccion IP inicial y una final. Por ejemplo, si el usuario lo desea, puede monitorear los paquetes o bytes que van desde la red 200.9.176.0 al host 192.188.59.2.

Tambien se puede especificar en los dominios de las asociaciones, que no necesariamente debe haber una direccion IP inicial y una final, sino solo una de ambas, y la otra puede ser cualquier direccion IP. Por ejemplo, se puede monitorear desde la red 200.9.176.0 al mundo, o del mundo al host 192.188.59.2.

El cliente puede especificar una o varias redes a excluir. Tambien esta en capacidad de elegir si desea monitorear paquetes o bytes, igualmente puede especificar una frecuencia de muestreo, esto es, que indica al servidor cada cuanto desea el cliente que se tome una muestra de los paquetes que hay en la red.

El cliente esta diseñado para contener una pantalla con un plano de coordenadas **X** e Y en donde se van mostrando las curvas del trafico que se este sensando. En el eje **X** se muestra el tiempo y en el eje Y el numero de paquetes o bytes (segun el cliente halla seleccionado).

Las curvas corresponden a las asociaciones seleccionadas para ser sensadas. Cada curva tiene un color diferente y por ende, corresponde a una asociacion distinta.

El cliente provee la capacidad al usuario de cambiar las escalas del eje X y del eje Y.

En el eje X se especifica 20 divisiones del area de grafico, con 20 intervalos iniciales por defecto. Un intervalo es lo que avanza la grafica en un segundo, o el tiempo de muestreo que el usuario halla seleccionado.

En el caso de 20 divisiones y 20 intervalos, la grafica cada segundo avanza una division. Si el cliente aumenta los intervalos a 40, cada segundo la grafica avanzara ½ division.

En el eje Y se especifican 10 divisiones. El cliente selecciona la amplitud del eje Y basado en el valor maximo de todas las curvas que se estan graficando. El usuario puede escoger, si desea que el cliente automaticamente regule la escala al valor maximo, o si desea definir un valor maximo unico.

8.1.2 Diagrama de clases

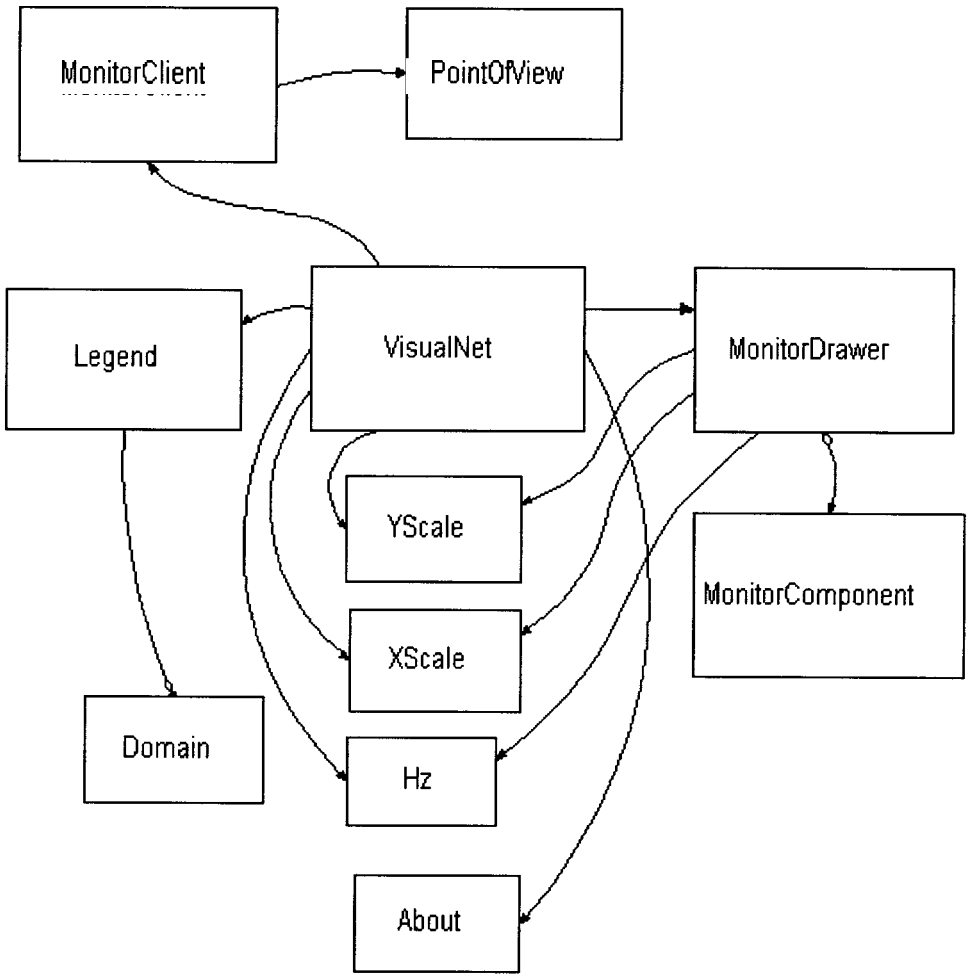


Figura 8.1 Diagrama de clases

A continuación se procede a detalla cada clase participante en el diagrama que se muestra en la figura 8.1

VisualNet: Objeto que coordina las actividades entre todos los otros objetos. Es el que recibe tambien todos los parametros enviados desde la pagina HTML. VisualNet indica cuando cada objeto debe operar y cuando otros deben esperar.

Monitorclient: Es el objeto encargado de manejar la conexión con el servidor. Monitorclient contiene un objeto PointOfView que envía a MonitorDrawer con los datos que se deben graficar.

MonitorDrawer: Es el objeto que controla el grafico. Se comunica con YScale, XScale, Hz y Legend para determinar respuestas a los eventos generados por el usuario.

MonitorComponent: Es el objeto que realmente realiza las curvas. Es parte de MonitorDrawer, es decir que este objeto no puede ser accesado si no es a traves de MonitorDrawer.

Legend: Es un objeto que contiene las asociaciones que se grafican por medio de curvas. Legend lanza el evento NewGraphicEvent, que es capturado por su VisualNet, para indicarle a este ultimo que debe regenerar el grafico.

XScale: Objeto que controla el eje X.

YScale: Objeto que controla el eje **Y.**

Hz: Objeto que controla la frecuencia de muestreo.

Domain: Objeto que representa una asociacion. Este tiene una propiedad que indica de que tipo es su dominio.

About: Objeto que muestra los nombres de los desarrolladores del sistema.

Existen mas objetos que intervienen en el sistema, como NewGraphicEvent y TestCellRenderer, pero estos no se los presentan en el diagrama debido a que corresponden a la categoria de *business objects,* osea objetos que se obtienen de un diseiio orientado a objetos.

Los objetos que no son business objects, son los que complementan y ayudan al funcionamiento de los business objects. La mayoría de las veces, vienen ya en las bibliotecas propias de cada lenguaje de programacion, otras veces son diseiiados y creados por el mismo desarrollador de la aplicacion, pero extendiendo la funcionalidad de alguna clase creada para aumentarle o redefinirle comportamiento

8.2 Cliente de estado de monitoreo

El cliente de estado de monitoreo en realidad se divide en dos applets sencillos, uno para el administrador y otro para los usuarios normales.

La diferencia esta en que el applet del administrador es un boton que le permite iniciar el monitoreo y detenerlo. En cambio el applet del usuario es un label, que solo le permite ver al usuario si el monitoreo historico esta activo o detenido.

8.2.1 Applet del administrador

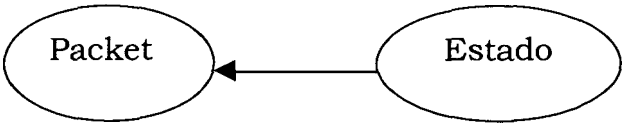


Fig. 8.2 Objetos del applet administrador

Son sólo dos objetos. PacketClient es el objeto encargado de conectarse con el servidor. Estado es el encargado de mostrarle al administrador el boton junto con el estado actual del monitoreo.

8.2.2 Applet del usuario

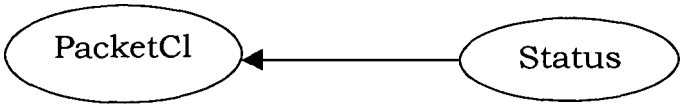


Fig. 8.3 Objetos del applet del usuario

Tambien son solo dos objetos. PacketClient es la misma clase utilizada en el applet del administrador. Su funcion es la de conectarse con el servidor. La funcion de Status es la de mostrar al usuario el estado por medio de una etiqueta y un icono representativo.

CONCLUSIONES

El manejo de interfaz de red en la plataforma Linux resulto ser mas eficiente que la implementada en la plataforma Windows NT debido a que en Linux, los controladores de interfaz 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 interfaz web permite que los usuarios del mismo accedan a este en forma remota.

El procesamiento multihilo facilito 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 interfaz interactiva y sobre todo ligera que hace que el sistema tenga un eficiente desempeño.

RECOMENDACIONES

Migrar los datos desde PostgresSQL hacia una base de datos mas robusta debido a que esta tiene limitaciones en tiempo de respuesta cuando el tamaño de las tablas crece excesivamente.

Mejorar la implementación de la cola de espera para el almacenamiento en la base de datos tanto para Windows NT como para Linux.

APENDICE I

Formato del Paquete

Ethernet

Formato del Paquete Ethernet.

La manera general en que trabaja **TCP/IP** es que la aplicacion le entrega una cadena de datos al protocolo de transporte (**TCP** o **UDP**) el cual se encarga de contactar a la capa de red **(IP)** y entregarle paquetes que pueden ser hasta de 65 Kb de longitud (aunque la mayoría de las tarjetas de red manejas una longitud maxima de 1500 bytes denominada Maximum Transmission Unit). La capa de red **IP** transmite los paquetes, tal vez divididos en unidades mas pequeñas (fragmentos) hasta el destino, haciendo su mejor esfuerzo para que los paquetes lleguen a su destino. En el destino la capa **IP** ensambla los fragmentos y entrega los paquetes a la capa de transporte quien a su vez se los entrega a la aplicacion. El formato del paquete que circula a traves de una red Ethernet se explica en la figura 1.

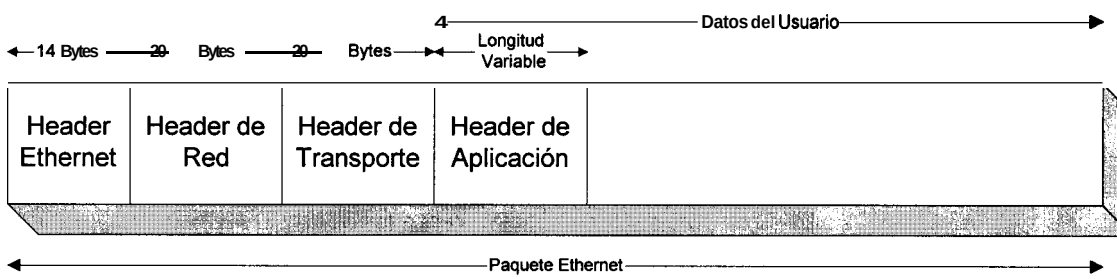


Figura 1. Formato del Paquete Ethernet

El header Ethernet consta de **14** bytes y su estructura se muestra en la Figura2.

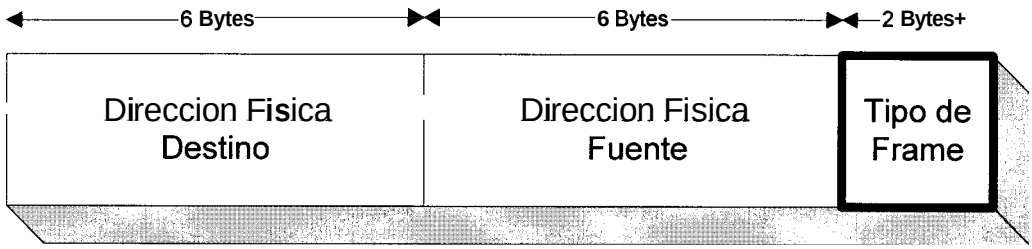


Figura 2. Estructura del Header Ethernet

La direccion Fisica Destino y Fuente, indican la direccion Ethernet destino y fuente respectivamente, el campo Tipo de Frame (Bytes 13 y **14**) indican el protocolo que tiene en capas superiores el paquete, los valores que pueden tomar estos dos bytes se muestra en la tabla 1.

Protocolo	Valor Hexadecimal
IP	0800
ARP	0806
RARP	8035

Tabla 1. Valores hexadecimales **de** los Protocolos

El header de Red, que para nuestro caso sera IP, consta de 20 bytes **fijos** que son mostrados en la figura 3 y de una parte de opciones cuyo tamaño es variable (de cero o mas bytes).

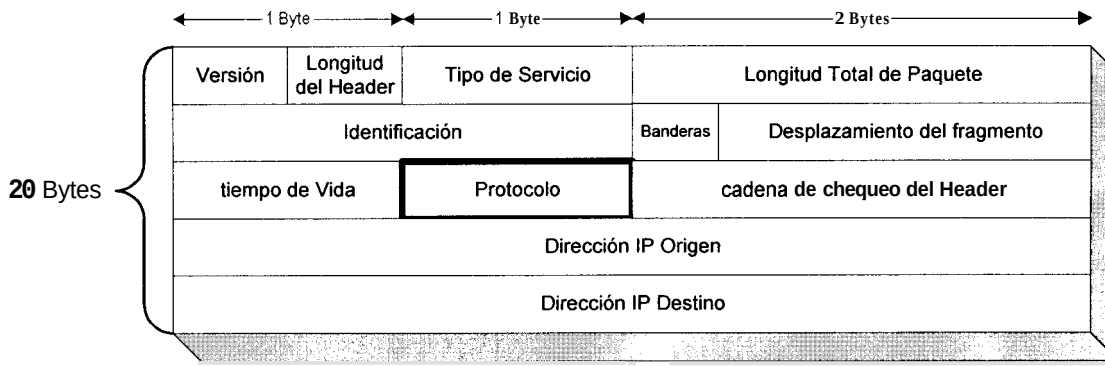


Figura 3. Estructura del Header de Red

Campo Version: Permite saber si un paquete es de una misma version de IP o si necesita alguna conversion cuando se estan usando versiones diferentes.

Campo longitud de encabezado: Permite saber el tamaño total del header que consta de 20 bytes fijos y hasta **40** bytes de opciones.

Campo tipo de servicio: Permite especificar a que servicio pertenece este paquete o cual se requiere (confiable, rapido, con prioridad, etc.).

Campo de longitud total: Indica la longitud del paquete incluyendo header y datos.

Campo de identificación: Indica el numero de paquete, lo cual permite ensamblar fragmentos de un mismo paquete en la capa IP.

Campo de Banderas: Indica a los ruteadores si el paquete debe o no fragmentarse.

Campo de desplazamiento: Indica el numero de fragmento que es de determinado paquete.

Campo de tiempo de vida: Se inicializa a un numero entre **1** y 255 que se supone son segundos aunque en la practica se usa para indicar saltos entre ruteadores. cada vez que un fragmento cruza por un ruteador este campo se decrementa en una unidad, o en varias unidades si permanecio suficiente tiempo en una cola. Esto permite que los paquetes cuyo tiempo de vida llega a cero sean descartados y no vaguen por la red indefinidamente.

Campo de protocolo: Indica si el protocolo de transporte es TCP o UDP u otro los valores que puede tomar este campo son mostrados en la tabla 2.

Protocolo	Valor (decimal)
TCP	06
UDP	17
ICMP	01
IGMP	02

Tabla 2. Valores decimales de los protocolos

Campo de chequeo: Permite calcular si el encabezado llegó íntegro o no.

Campos IP Origen e IP Destino: Indican la dirección IP única a nivel mundial del nodo origen y nodo destino.

Campo de opciones: Estos bytes se dejaron sin especificar con el objeto de darles significado cuando el protocolo tuviera más necesidades. Se han especificado algunas opciones como son paquetes con seguridad, rutas de entrega estrictas o sugeridas, registro de rutas y registro de tiempos de travesía.

El header de Transporte consta de 20 bytes, puede ser: TCP ó UDP, los dos protocolos tienen dos campos en comun los cuales son mostrados en la figura 4.

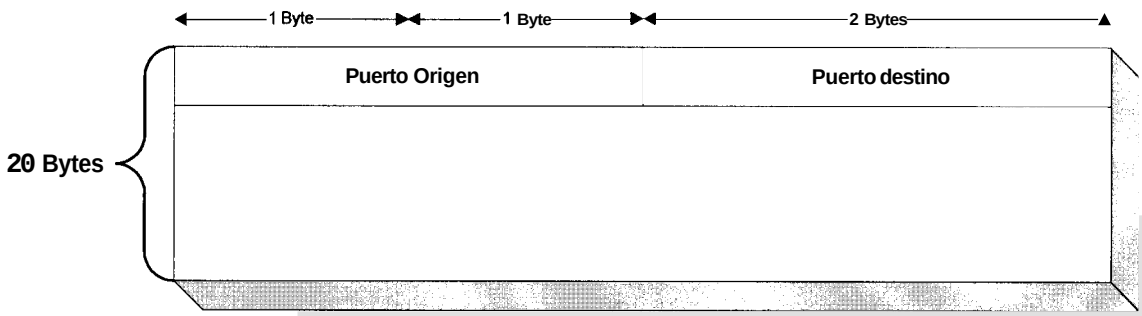


Figura 4. Estructura del Header de Transporte

El puerto Origen y Puerto Destino indican la aplicacion a la que pertenece el paquete, en la tabla 3 se muestra posibles valores de estos campos

Aplicación (Puerto)	Valor (decimal)
TELNET	23
MAIL	25
FTP	21

Tabla 3. Valores para los puertos

APENDICE II

Manual de Instalacion del Sistema

1. Requerimientos del Sistema

Requerimientos de Hardware:

- Procesador Pentium de 133Mhz o superior.
- **64** Mb de RAM mínimo
- Tarjeta de Red Ethernet

Requerimientos de Software:

- Sistema Operativo Red Hat Linux version 5.2 o superior
- Lenguaje de Programacion Perl
- Gnuplot
- Base de Datos

NOTA: Red Hat Linux proporciona los elementos restantes, los cuales deben ser instalados.

2. Instalacion para Linux

Para llevar a cabo la instalacion del sistema, se recomiendan los siguientes pasos:

1. Ingrese al sistema operativo como root
2. Inserte el CD proporcionado en la distribución.
3. Monte el CD-ROM , escribiendo en la línea del prompt :

   [root@tuco root]# ***mount /dev/cdrom /mnt/cdrom***

4. Ejecute el shell-script instalador dentro de la carpeta **Instaladores/Linux**, para crear los directorios y copiar los archivos fuentes

   [root@tuco Linux]# ***./instalador***

5. Ingrese el password del postgres para la creación de las tablas en la base de datos:

   password : postgres

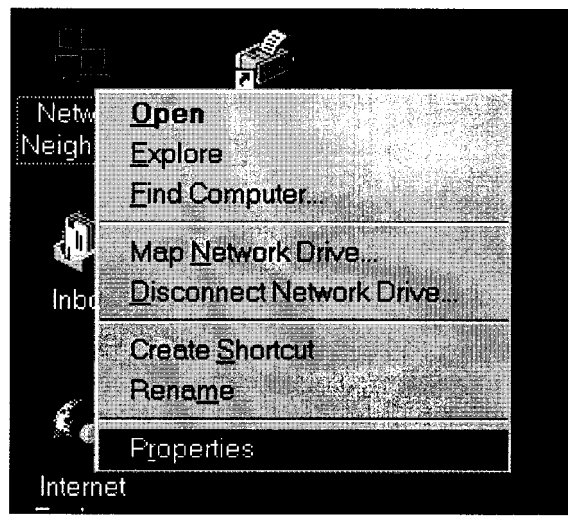
   NOTA: al digitalizar el password, este no aparecera en pantalla

6. El sistema ha sido instalado.

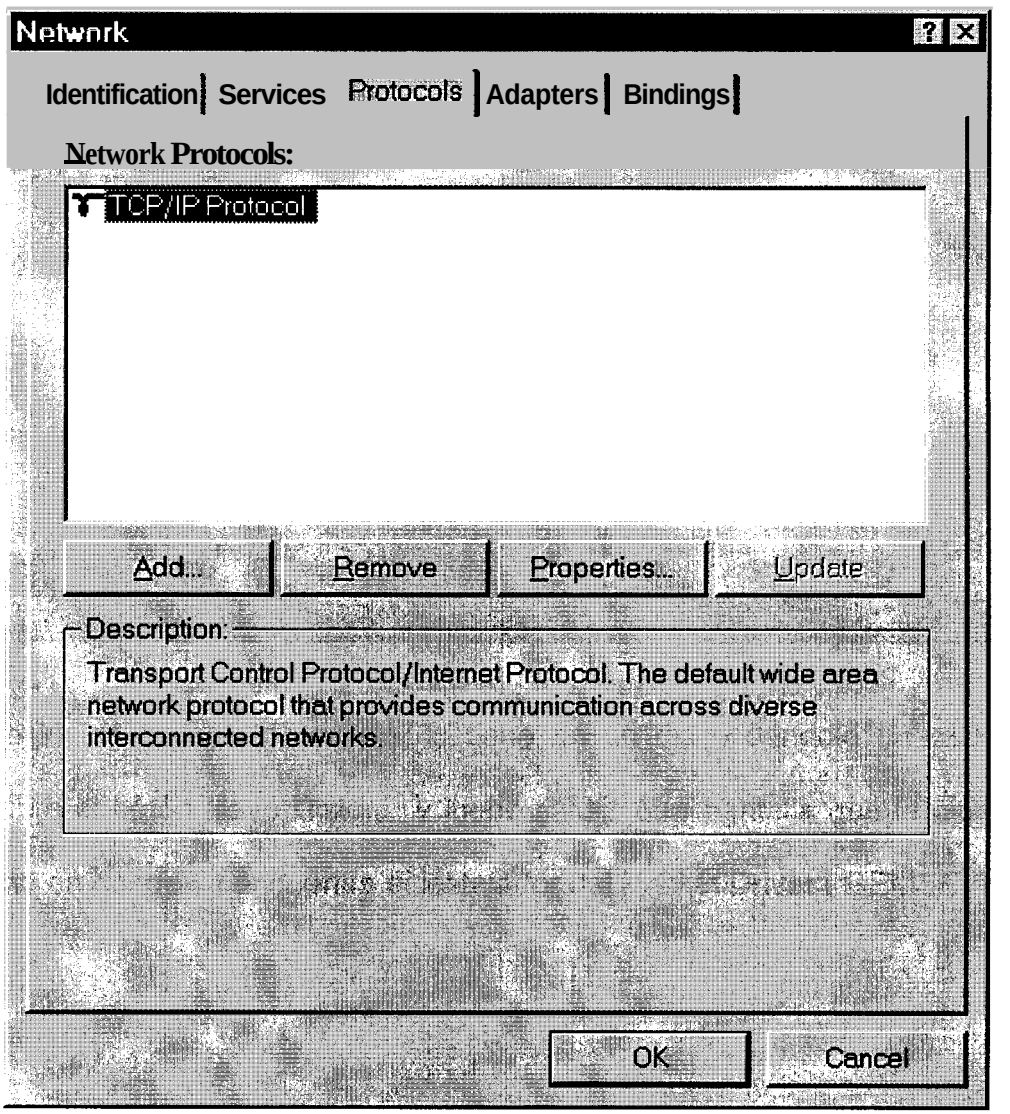
3. Instalacion del Packet Driver para Windows NT 4.0.

Para poder accesar a la interfaz de red se debe instalar primero como protocolo el Packet Driver Packet32.sys, los pasos para realizar esta operación se detallan a continuación:

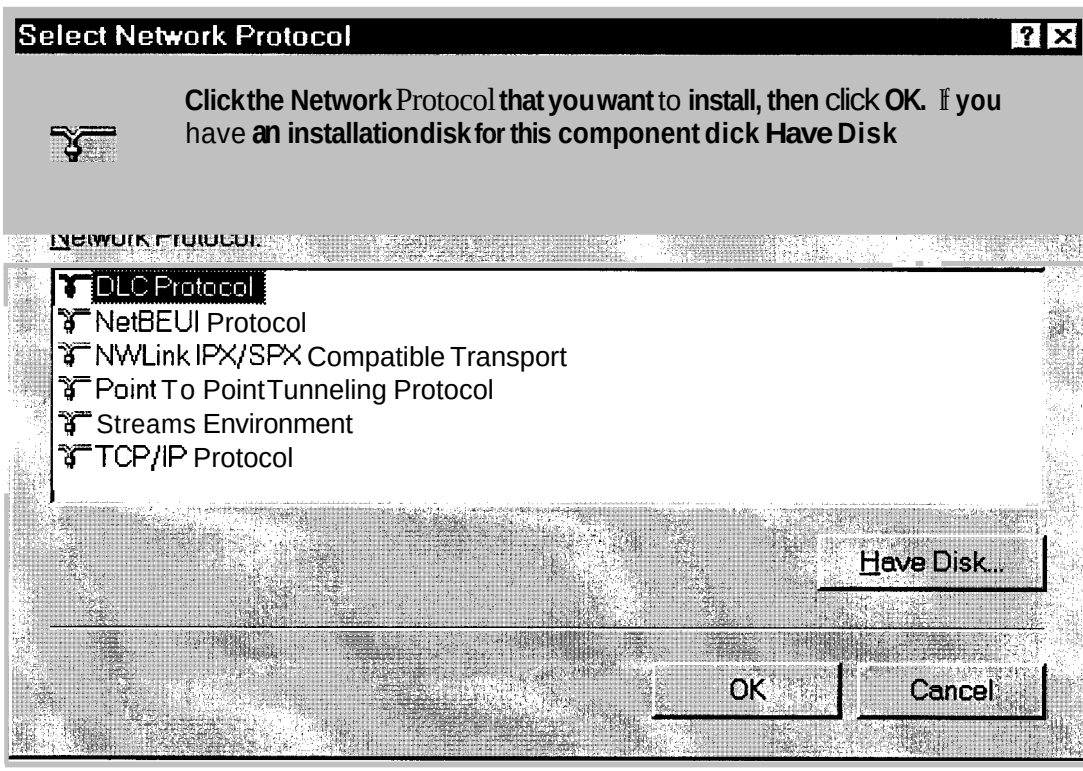
Iniciar la sesion en Windows NT, ubicar en el escritorio el Icono de Entorno de Red (Network Neighborhood)



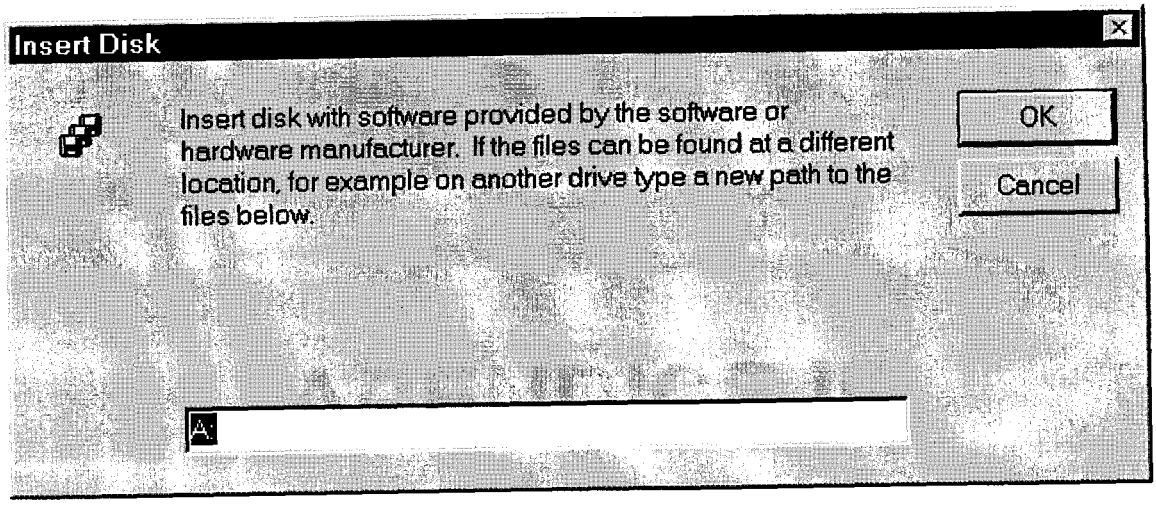
Dar un click derecho sobre el icono anteriormente mencionado e ingresar dentro de la opción Propiedades (Properties), Una vez realizado esto seleccionar Protocolos (Protocols)



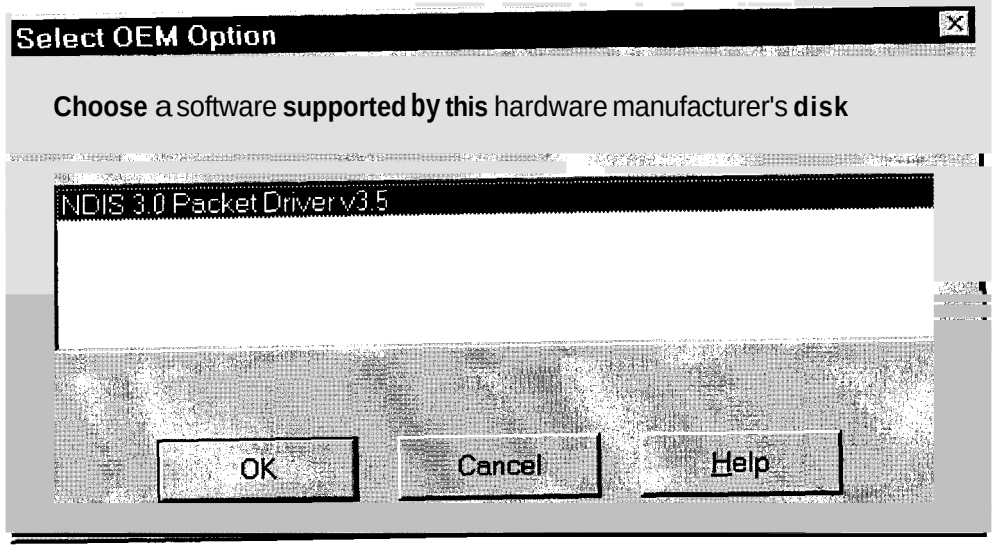
Escoger Añadir (Add..) un protocolo y le saldra la siguiente pantalla, la cual le pide indicar que protocolo de red desea añadir a su interfaz.



Se indica que el controlador lo tiene en un disco dandole un click izquierdo sobre el boton Have Disk.... y luego saldra otra pantalla que le pide indicar la ruta en donde se encuentra el instalador del Packet Driver (OEMSETUP.INF).



Una vez ubicada la ruta de acceso al instalador le saldra el nombre del protocolo a atiadir.



Se acepta y luego de esto le pedira reiniciar la maquina y el Packet Driver estara totalmente instalado.

APENDICE III

Manual del Administrador del Sistema

I.- Entrada al sistema

El Administrador del sistema "Monitor de Trafico IP para Redes Ethernet" tiene la capacidad de configurarlo segun los requerimientos de la red en la que se esta ejecutando.

Para poder hacer uso de los privilegios de administrador se debe ingresar como usuario *root* y digitar el password correspondiente (Fig. **1).**

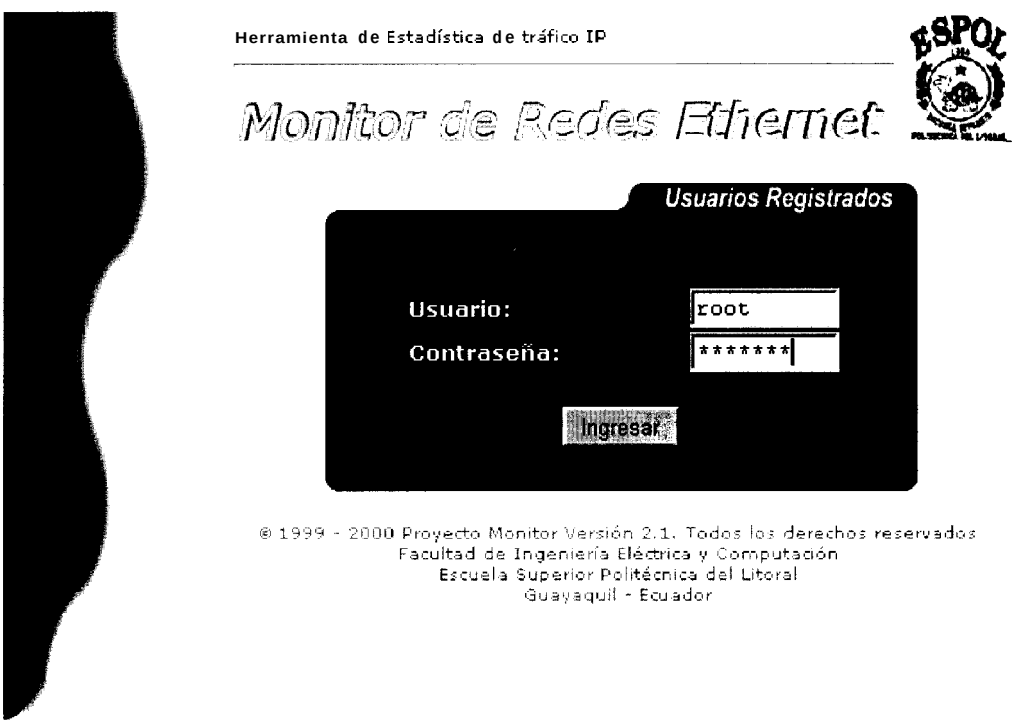


Fig. 1 Ingreso a monitor de Tráfico IP

El sistema realizara la validación de los datos, y si es correcta ingresara al mismo (fig.2), caso contrario mostrara error.

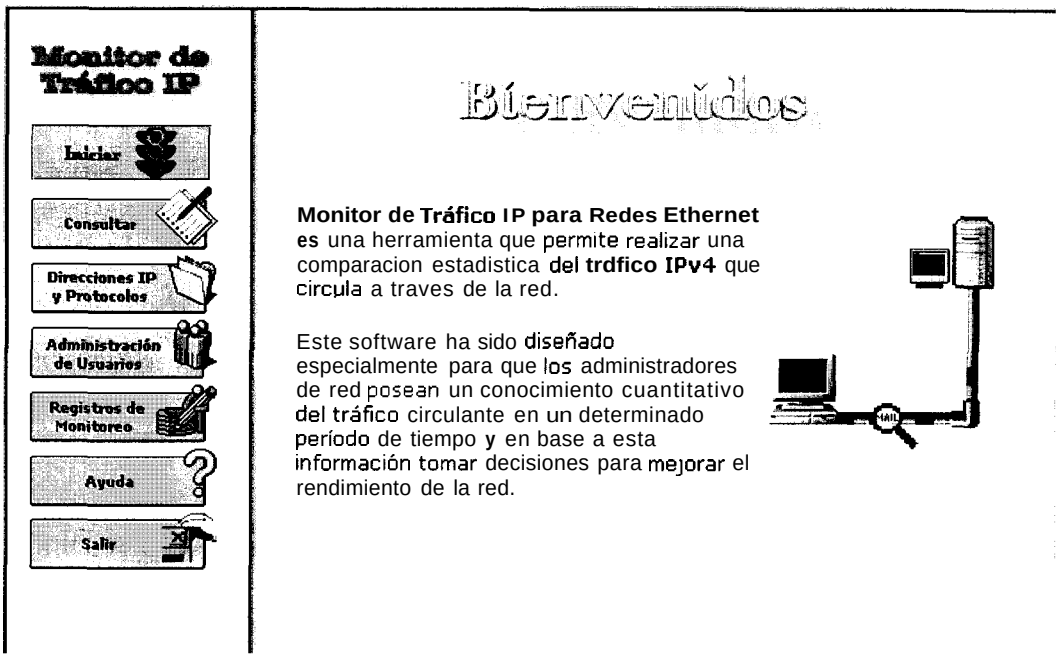


Fig. 2 Bienvenida y Menu del Administrador

La pantalla que se presenta consta de dos partes claramente diferenciadas. El lado izquierdo muestra el menu con las opciones que el administrador puede manejar; y en el lado derecho el mensaje de bienvenida.

2. Iniciar / Detener Monitoreo

El estado del monitoreo puede ser consultado directamente desde el menu de opciones. Estara activo cuando las luces del semaforo estan cambiando de color constantemente; e inactivo cuando el semaforo se encuentra detenido en luz roja **(fig.** 3).

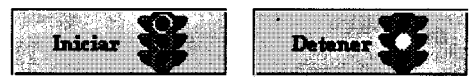


Fig. 3 Iniciar/detener monitoreo

Para iniciar o detener el monitoreo es necesario pulsar el boton *Iniciar/Detener* que *se* muestra en el menu de opciones. La acción que se realiza se indica en la etiqueta del boton.

3. Consultar

Para realizar las consultas el administrador deberá llenar la forma (fig. **4)** con los datos necesarios que permitiran obtener las graficas deseadas.

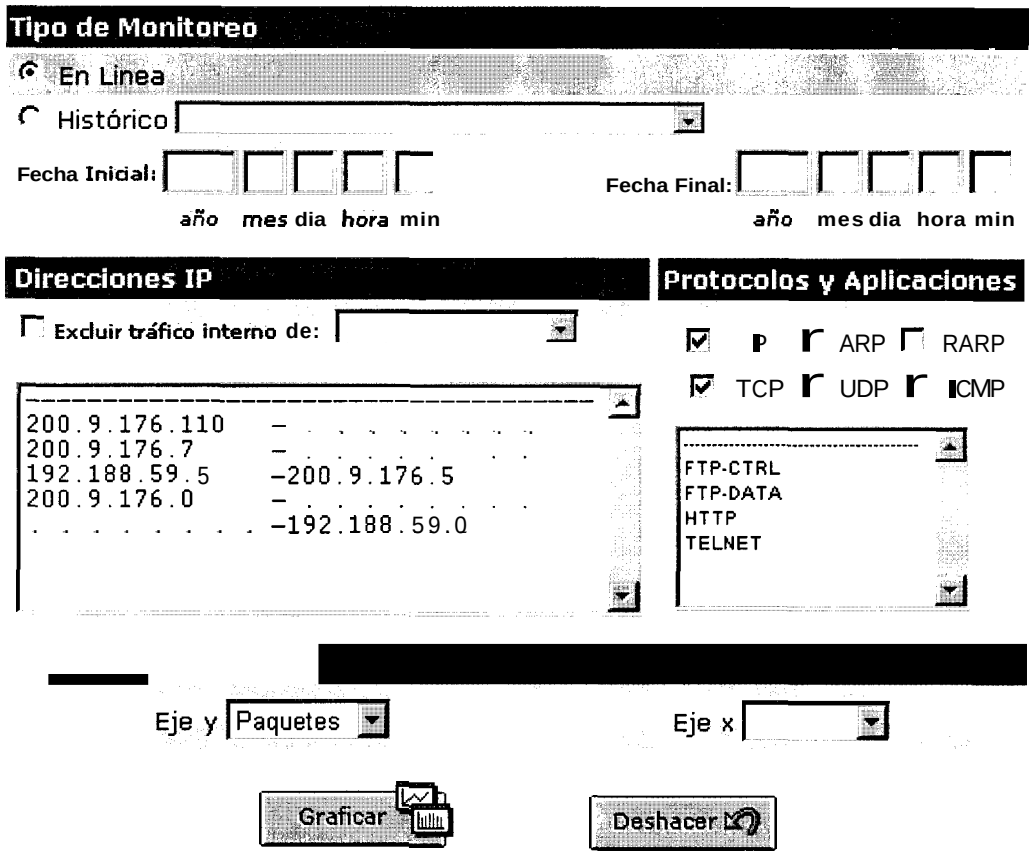


Fig 4. Formulario para las consultas

3.1. Tipo de Consulta

La consulta puede ser historica o en línea (fig. 5). Ambas opciones son mutuamente excluyentes, esto es, el administrador solo podra seleccionar un tipo a la vez.

Por defecto, el sistema mostrara como seleccionado el tipo *en línea,* en este caso los campos del histórico permaneceran en blanco.

Fig. 5 Tipo de Consulta

Al seleccionar la consulta *histórica*, los campos se activaran automaticamente y el administrador podra escoger algun intervalo particular de los que se encuentran en la lista desplegable (fig. 6). Los campos para las fechas inicial y final se llenaran automaticamente con las fechas del primer intervalo de muestreo que tenga registrado.

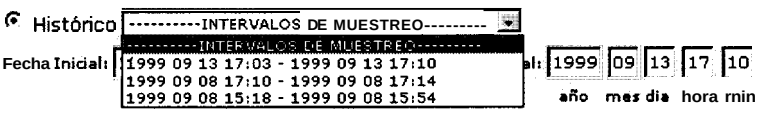


Fig. 6 Intervalos de Consulta Histbrica

Si los limites de los intervalos deseados no constan en la lista, el administrador podra ingresar en los campos las fechas deseadas (fig. 7) .

Fig. 7 Ingreso de fechas de la consulta historica

Se recomienda que el intervalo ingresado se encuentre entre la primera fecha mostrada en el primer intervalo y la segunda fecha del ultimo intervalo (fig. 8). Si las fechas ingresadas estan fuera de este intervalo, es posible que el sistema no tenga datos que graficar, por lo tanto solamente presentara la información de cero.

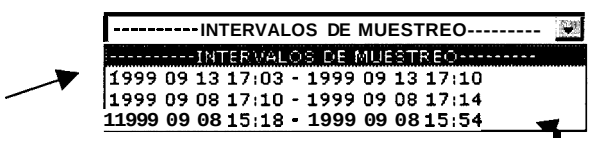


Fig. 8 Fechas inicial y final para la edición.

3.2. Direcciones IP

Excluir el tráfico inferno implica realizar la consulta de todo el trafico que pasa por las direcciones IP seleccionadas, excepto el trafico de la red seleccionada en este campo (fig. 9). Para hacer uso de esta opción es necesario seleccionarla.

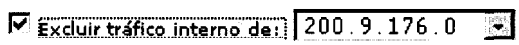


Fig. 9 Excluir el trafico interno de una red

La red a excluir debe seleccionarse de la lista desplegable que contiene las opciones existentes (fig. 10). En caso de no encontrar la red deseada, el administrador deberá ingresarla previo a la consulta (ver Direcciones IP y Protocolos).

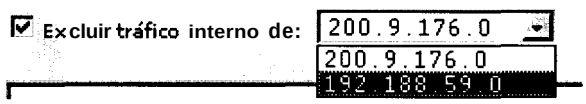


Fig.'10 Lista de redes existentes

En este campo se muestra una lista de las *direcciones IP* que han sido ingresadas en el sistema por parte del administrador (fig. 11). Si desea consultar alguna direccion IP que no consta en la lista, el administrador deberá ingresarla previamente (ver direcciones IP y Protocolos).

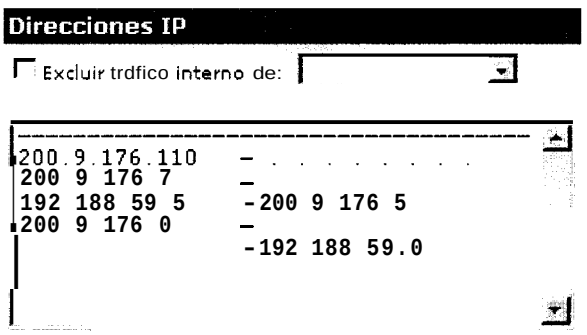


Fig. 11 DireccionesIP

Para seleccionar una direccion IP sobre la cual se va a consultar, es necesario posicionarse con el mouse sobre ella y presionar. En el caso de dos o mas se debe mantener presionado la tecla CONTROL y seleccionar con el mouse cada una de las opciones (fig. 12).

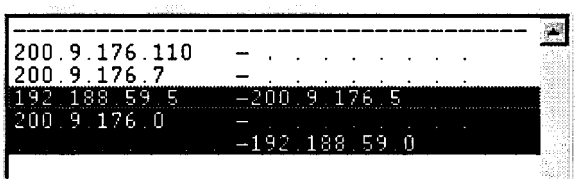


Fig. 12 Selección de DireccionesIP

3.3. Protocolos y Aplicaciones

Los *Protocolos* que se pueden consultar se muestran en esta sección del formulario. La lista muestra las aplicaciones existentes (fig. 13).

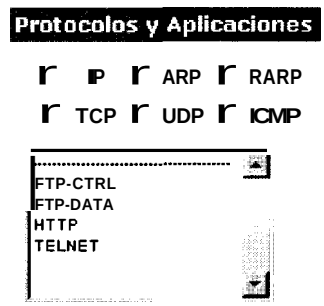


Fig. 13 Protocolos y Aplicaciones

Los protocolos existentes pertenecen a la capa de red (IP, ARP, RARP), y a la capa de transporte (TCP, UDP, ICMP) del modelo OSI. El sistema permite seleccionar ninguno, uno o **mas** de dichos protocolos (fig. 14).

Fig. 14 Protocolos disponibles

Las aplicaciones existentes sobre las cuales se puede realizar las consultas se muestran en una lista de selección multiple (fig. 15). En el caso de que la

aplicacion a consultar no conste en la lista, el administrador deberá ingresarla previo a la consulta (ver Direcciones IP y Protocolos).

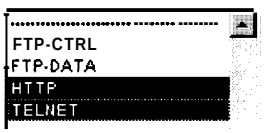


Fig. 15 Aplicaciones seleccionadas

Para seleccionar una opción es necesario pulsar sobre ella con el mouse. En el caso de dos o mas, se debe mantener presionada la tecla CONTROL y realizar la selección.

3.4. Unidades

Para generar las curvas es necesario seleccionar las unidades de los ejes de las graficas (fig. **16).** Para la consulta en línea, el eje **x** (escala del tiempo) permanece deshabilitado.

Fig. 16 Unidades de los ejes

El ***eje y*** representa la unidad de trafico (fig. 17). El administrador podra seleccionar entre las opciones existentes el tipo de unidad para la curva a generar. La unidad de trafico puede ser paquetes, bytes o kbits.

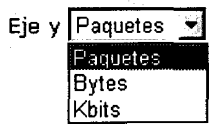


Fig. 17 Unidades de Tráfico

El ***eje X*** representa la unidad de tiempo (fig. 18). El grafico puede generarse en escalas de minutos, hora, dia o mes.

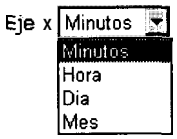


Fig. 18 Unidades de tiempo

3.5. Graficar

Para generar las curvas con las especificaciones escogidas tanto en línea como historico, se debe presionar el boton *Graficar* (fig. 19). Durante esta acción deberá esperar unos minutos mientras se recolectan los datos de la Base.

Fig. 19 Botón para graficar

3.5.1. Graficar en linea

La consulta en linea permite al usuario obtener curvas en tiempo real del tráfico actual de la red en la cual esta monitoreando. Para realizar este tipo de consulta es necesario seleccionar de la forma : *el tipo de monitoreo en linea, mínimo una dirección IP y una aplicación., el eje y* (fig.20).

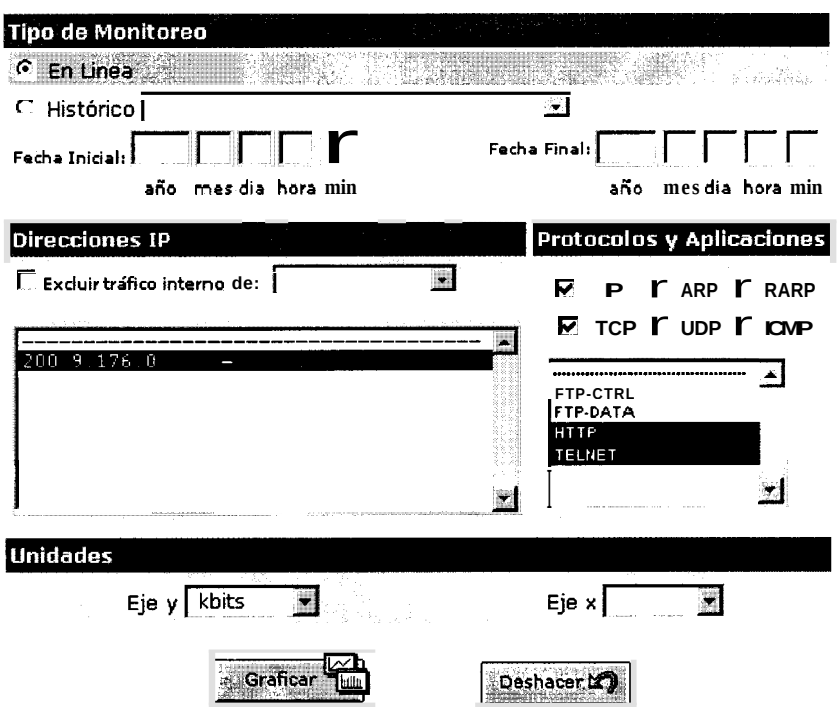


Fig. 20 Forma para realizar una consulta en linea

El grafico se va generando en ejes coordenados con respecto al tiempo (fig. 21).

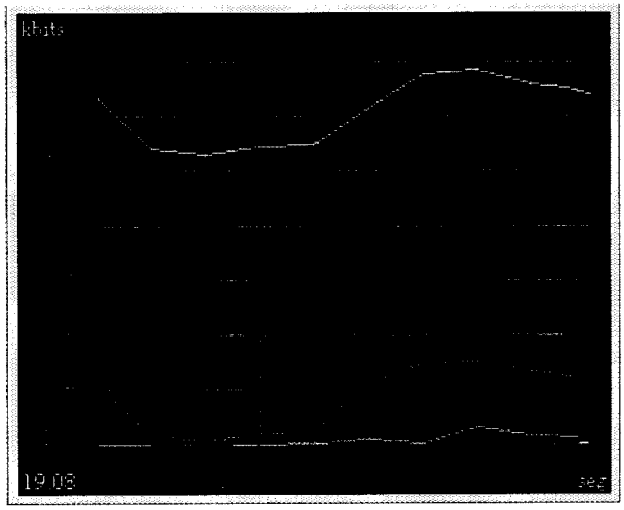


Fig. 21 Grafico de consulta en línea

3.5.1.1. Opciones

Ocultar/mostrar grid:

Oculta o visualiza las cuadriculas en la grafica

Eje Y

Muestra por defecto el valor maximo, pero el usuario puede determinar un valor deshabilitando la autoescala

Eje x

Muestra el intervalo que va a presentar en pantalla. El valor por defecto es 20.

Dominios

Presenta las direcciones IP escogidas y el tipo de trafico con distincion de colores, necesarios para la interpretación del grafico.

Frecuencia

Representa el intervalo en el que el servidor va a realizar el muestreo de los datos a graficar.

Color grid

Muestra una paleta de colores y permite cambiar el color de las cuadriculas.

3.5.1.2. Ventana de Dominios

Para visualizar los detalles de los dominios basta con pulsar el boton de dominios y el sistema le mostrara una ventana con los dominios y protocolos a consultar **(fig.** 22)

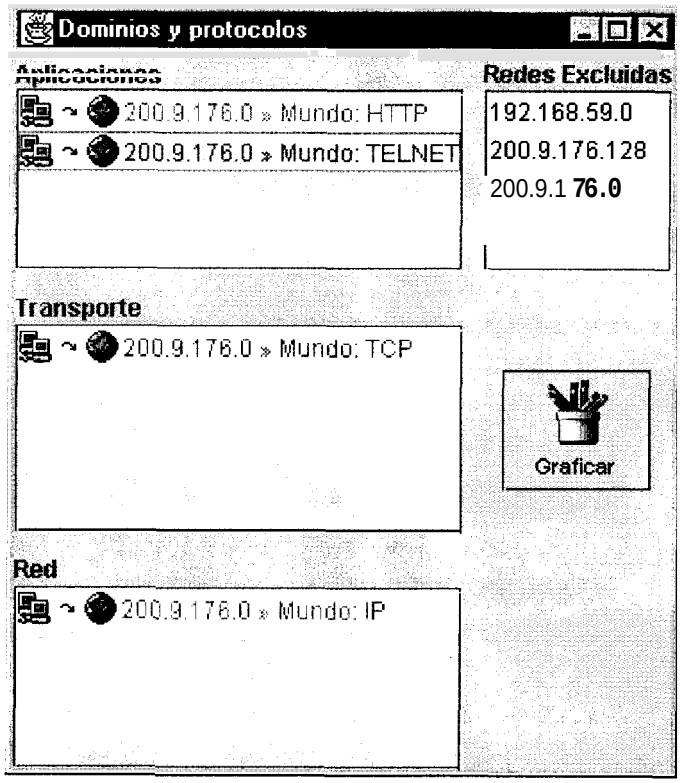


Fig. 22 Ventana de Dominios y protocolos

Con esta opción, el usuario esta en la capacidad de :

- Distinguir por medio de colores las curvas con su respectiva leyenda (direcciones IP y tipo de trafico).
- Graficar otra curva entre las opciones presentes.
- Excluir alguna red del trafico que desea visualizar

3.5.2. Graficar Histórico

La consulta Historica permite obtener graficos de intervalos de tiempos anteriores en los cuales existan datos. Para realizar este tipo de consulta, es necesario llenar la forma (fig. 23)

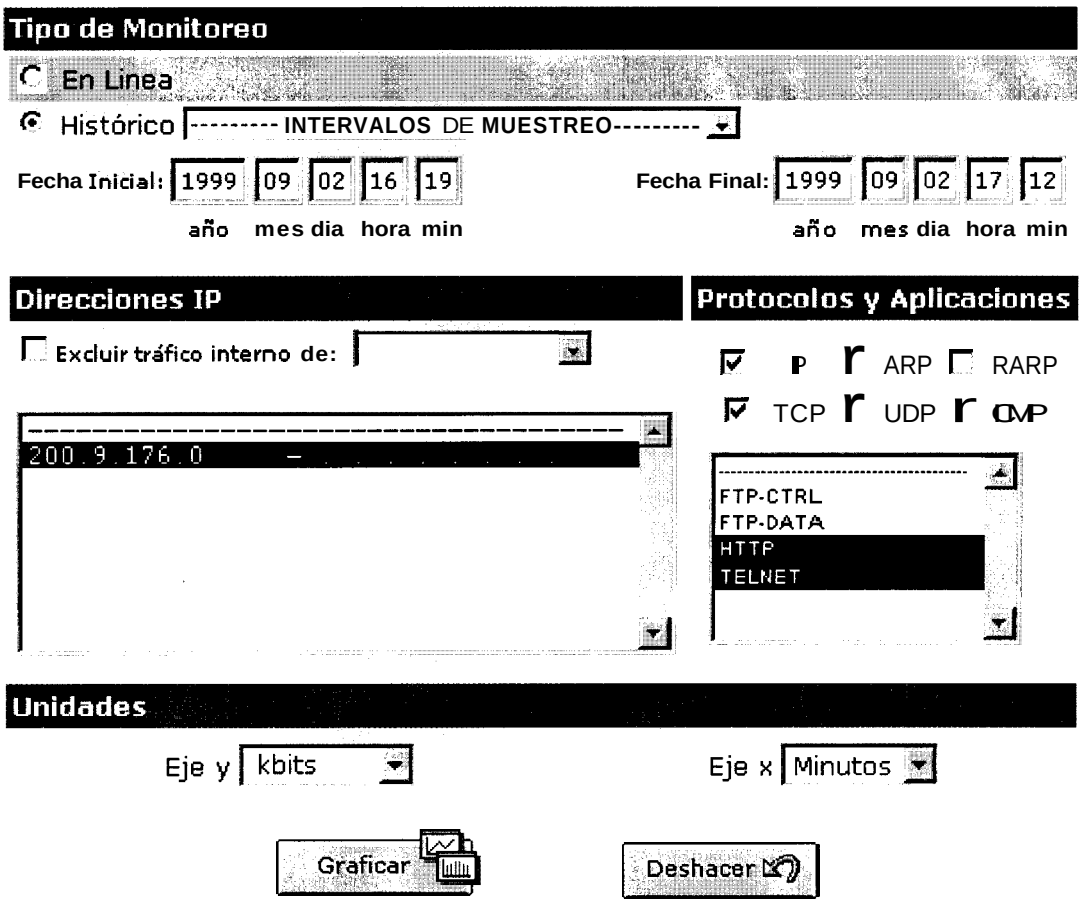


Fig. 23 Forma para realizar una consulta histórica

Para realizar este tipo de consulta es necesario:

- Seleccionar el tipo de monitoreo histórico
- Fecha maxima y minima de muestreo.
- Minimo una dirección IP y una aplicacion.
- Las unidades de los ejes.

El gráfico obtenido se muestra en ejes coordenados. La leyenda indica el trafico total y la dirección a la cual pertenece.(fig. **24)**

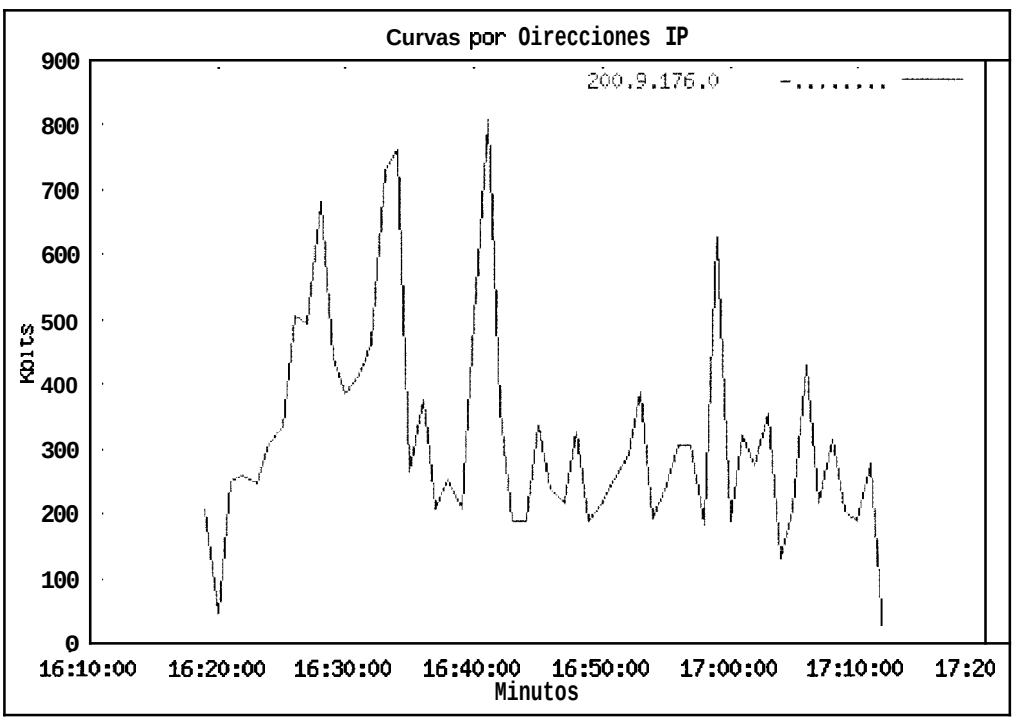


Fig. 24 Curva del tráfico consultado en histórico

3.5.2.1. Curvas Específicas

El sistema permite al administrador generar las curvas especificas de cada una de las opciones que selecciono al iniciar la consulta. Para ello, se debe seleccionar de la forma que se presenta con el grafico general (fig. 25).

Fig 25. Forma para obtener gráficas especificas

El administrador tiene capacidad para:

- Cambiar la unidad de trafico (eje Y).
- Obtener graficos de cada una de las direcciones IP. (OTROS representa todas las demas direcciones IP, excepto la seleccionada.)
- Realizar curvas especificas de una o todas las direcciones IP, de todo el trafico o de alguno en particular. Cada curva tendra un color distintivo.

Las opciones de las curvas especificas se limitan a las establecidas en el formulario.

3.5.2.2. Puntos maximos y minimos

El sistema permite consultar los puntos maximos y minimos de las curvas presentes en el grafico. Cada una de las direcciones IP se presentaran con el color distintivo de la curva a la cual se refieren (fig. 26).

Direcciones IP	Puntos Mínimos		Puntos Máximos	
	Fecha	Kbits	Fecha	Kbits
200.9.176.0 -	1999/09/02 16:20:00	0.000	1999/09/02 16:41:00	806.239

Fig 26 Puntos máximos y minimos de los gráficos

3.5.2.3. Ajustar Graficos

El usuario tiene la opción de ajustar los gráficos en otros intervalos internos, es decir, los puntos maximos y minimos del nuevo grafico deben estar incluidos en el intervalo inicial (fig. 27).

Fig 27 Límites para ajustar gráfico

En caso de no establecer maximos y minimos, o ingresar datos fuera del rango, el sistema toma los maximos y minimos originales.

IMPORTANTE : El grafico solo puede ajustarse dentro del rango original.

4. Direcciones IP y Protocolos

Para configurar las Direcciones IP y los Protocolos que se muestran como opciones, el sistema proporciona una forma que le permite al Administrador ingresar o eliminar los datos (fig. 28).

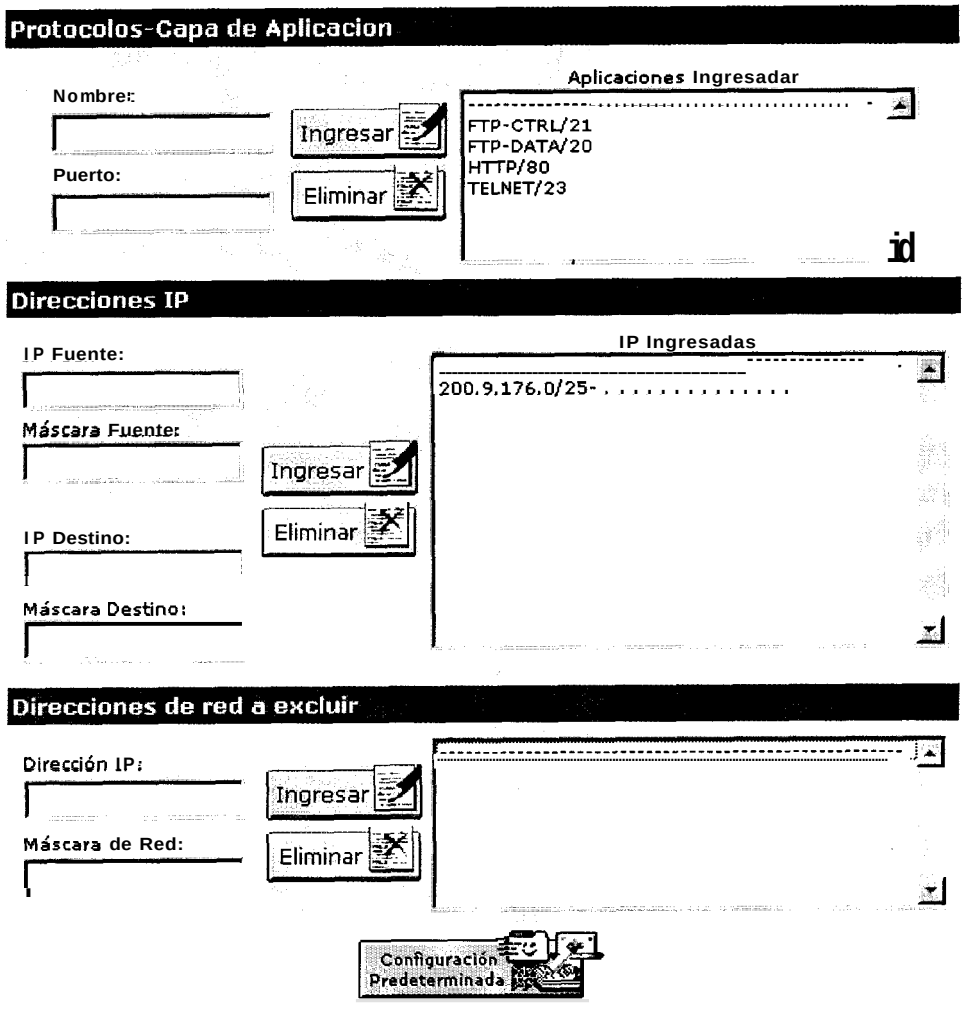


Fig. 28 Forma para administrar direcciones IP y Protocolos

4.1. Protocolos

Los protocolos de la capa de aplicacion pueden ser ingresados o eliminados por el administrador del sistema. Para ello cuenta con una forma (fig. 29)

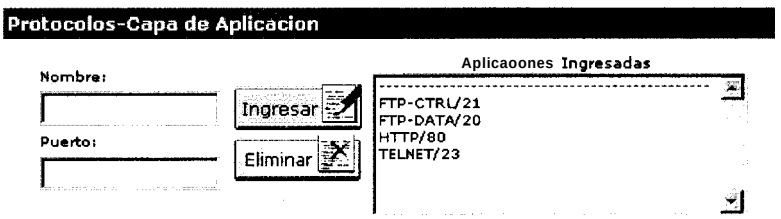


Fig. 29 Forma para ingresar Protocolos

4.1.1. Ingreso de Protocolos de aplicacion

Para ingresar los protocolos al sistema, es necesario ingresar los datos en los campos nombre y puerto y luego pulsar Ingresar (fig. 30).

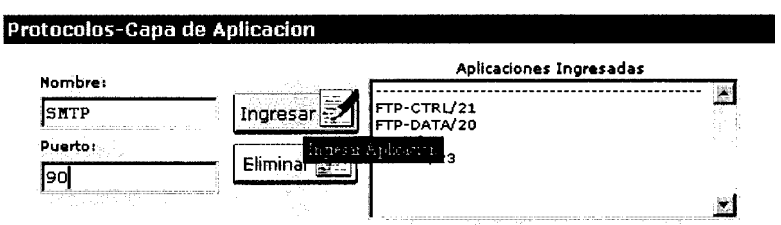


Fig. *30* Ingreso de un nuevo Protocolo de Aplicación

El sistema verificara que los datos sean correctos y luego los insertara en la lista de "Aplicaciones Ingresadas" (fig. 31)

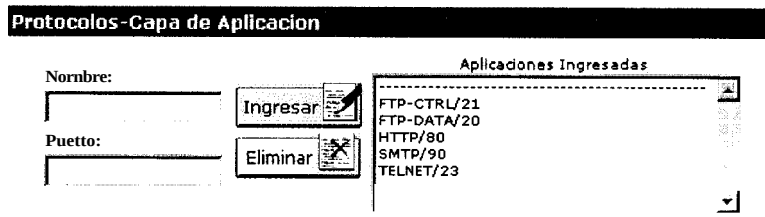


Fig. 31 Protocolo ingresado exitosamente

4.1.2. Eliminación de Protocolos de Aplicacion

Para eliminar deberá seleccionar una o varias apiicaciones y luego pulsar el boton eliminar (fig. 32).

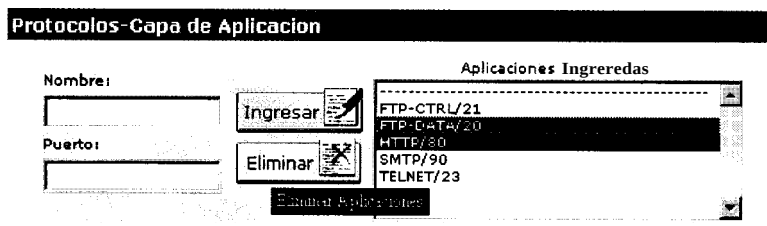


Fig. 32 Selección de los protocolos a eliminar

Una vez que la eliminación ha sido realizada, las aplicaciones eliminadas no se mostraran en la lista (fig. 33)

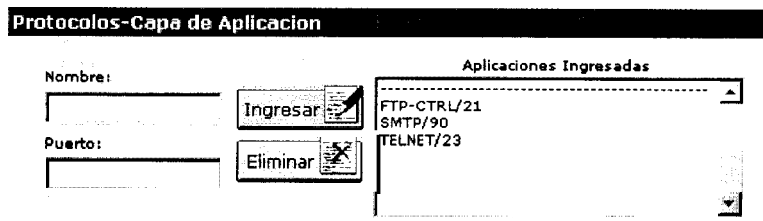


Fig. 33 Lista actualizada de los protocolos de aplicación

4.2. Ingreso de Direcciones IP

El ingreso de las direcciones IP se realiza por medio de la forma (fig. 34). El administrador puede ingresar nuevas direcciones IP o eliminar las existentes.

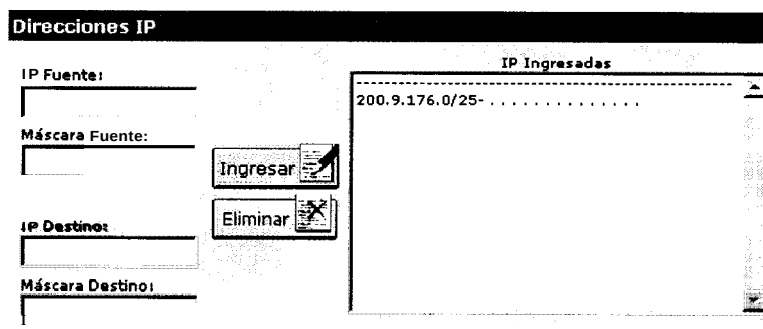


Fig. 34 forma para ingresar direcciones IP

Las direcciones IP que se ingresan al sistema pueden ser de red o de host. Los campos de mascara fuente y destino no son necesarios, si el administrador no ingresa datos, el sistema les asigna una mascara segun el tipo de red ingresada (fig. 35).

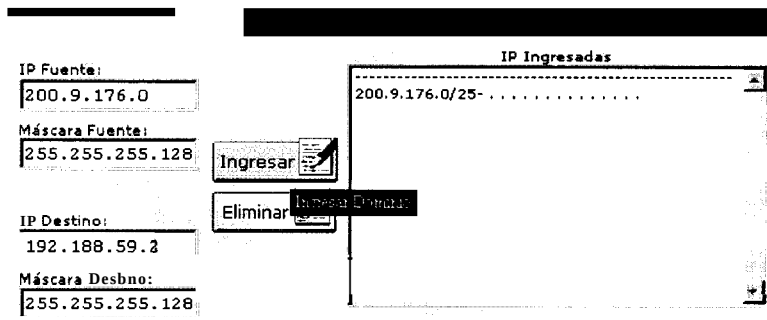


Fig. 35 Ingreso de Direcciones IP fuente y destino

Si las direcciones IP son correctas, el sistema las mostrara en la lista de IP ingresadas (fig. 36).

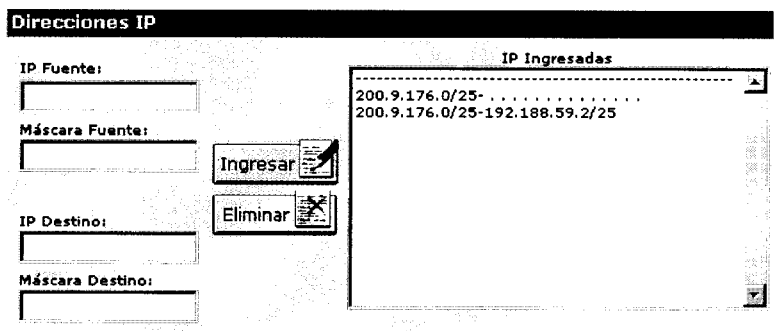


Fig. 36 Dirección IP ingresada

Cuando la direccion IP destino no ha sido ingresada, el sistema interpreta que se analizara todo el trafico que sale de la direccion fuente (fig. 37). Por el contrario, cuando la direccion fuente no ha sido ingresada, el sistema interpreta que se va a analizar todo el trafico que llega a la direccion destino.

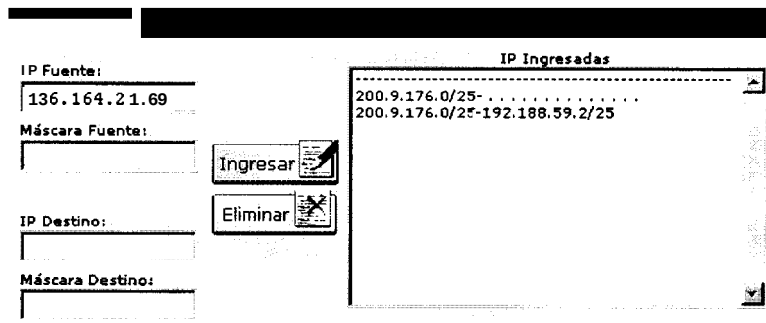


Fig. 37 Ingreso de Dirección IP fuente solamente

En el campo que no ha sido ingresado el sistema muestra una línea de puntos (fig.38).

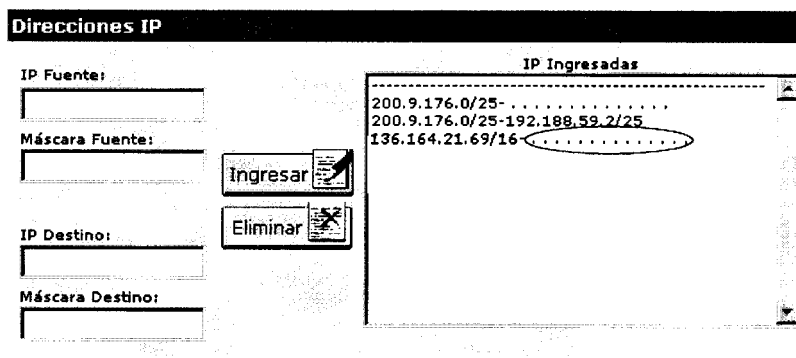


Fig.38 Dirección IP fuente con destino todo el mundo

4.2.1. Eliminacion de direcciones IP

Para eliminar una o varias direcciones IP, basta con seleccionarlas y pulsar el boton eliminar (fig.39).

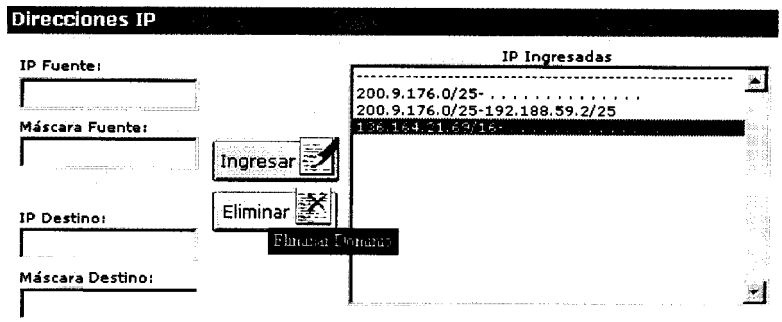


Fig. 39 Eliminacion de una dirección IP existente

Una vez que la direccion IP ha sido eliminada de la base de datos, tampoco aparecera en la lista de IP ingresadas (fig.40).

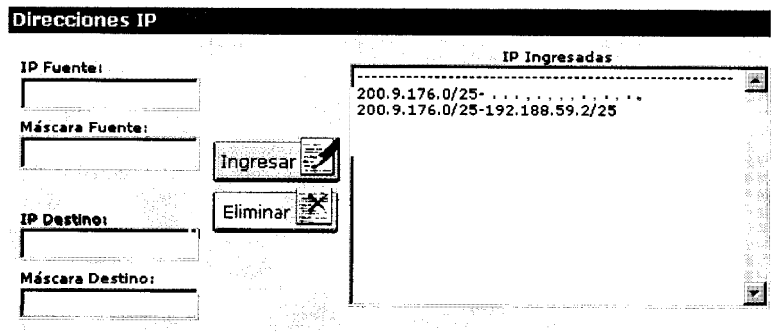


Fig. 40 Lista de direcciones IP actualizada

4.3. Direcciones de red a excluir

El sistema permite al administrador ingresar las direcciones IP cuyo trafico se desea excluir en las consultas. Para ello muestra una sección del formulario con ese mismo título (fig.41)

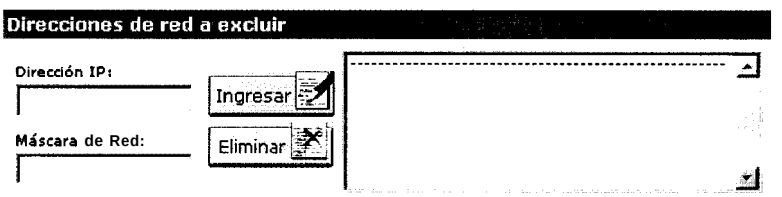


Fig. 41 Forma para las Direcciones de Red a excluir

4.3.1. Ingreso de Direcciones de red a excluir

El campo Dirección IP es necesario, mientras que el campo mascara de red es opcional. En caso de no ingresar, el sistema le asigna una por defecto. (fig. 42)

Fig.42 Ingreso de direcciones IP a excluir

Si la dirección IP ha sido ingresada correctamente, esta se mostrara en la lista de direcciones IP. (fig. 43)

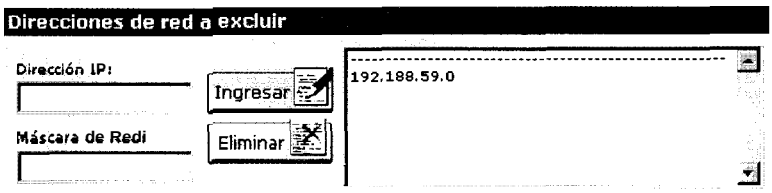


Fig. 43 Direccion de red a excluir ingresada

4.3.2. Eliminación de direcciones de red a excluir

Para eliminar direcciones de red a excluir es necesario seleccionar una o varias de ellas desde la lista y luego presionar el boton eliminar (fig.44)

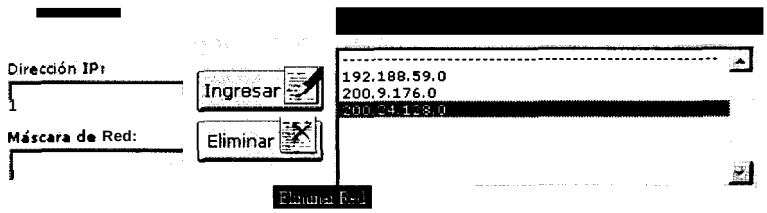


Fig.44 Eliminación de Dirección de red a excluir

Si la dirección IP ha sido eliminada, no aparecera en la lista de direcciones de red a excluir. **(fig.45)**

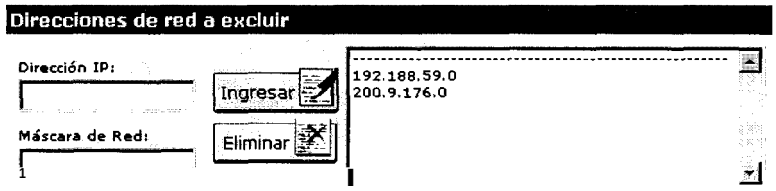


Fig. 45 Lista actualizada de direcciones de red a excluir

5. Configuracion Predeterminada.-

Esta opción permite al administrador establecer una configuracion predeterminada al momento de las consultas, esto es el sistema mostrara seleccionadas por defecto aquellas opciones que han sido escogidas en la configuracion predeterminada.

El formulario que permite realizar esta configuracion se muestra en la fig.46

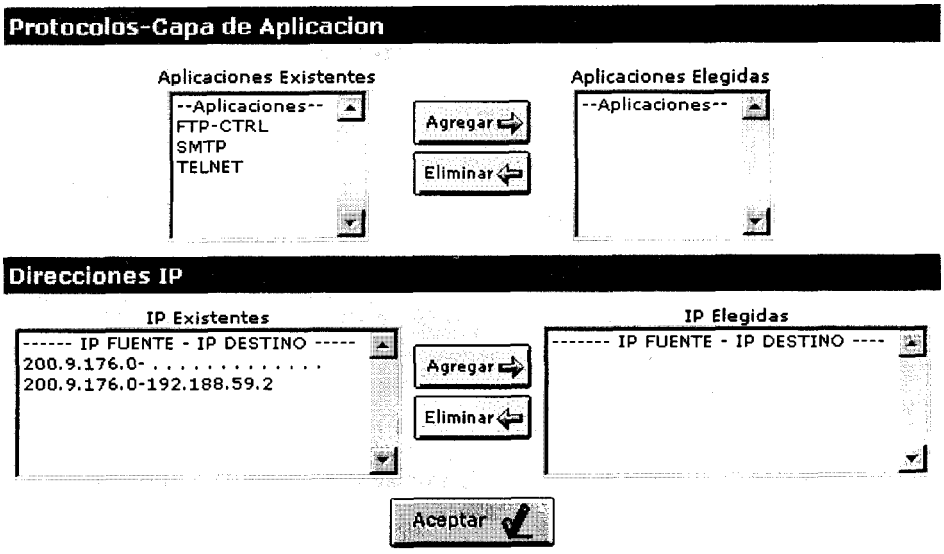


Fig.46 Formulario para la Configuracion Predeterminada

5.1. Protocolos de Aplicacion

5.1.1. Selección de Protocolos

La sección *Protocolos- **Capa** de Aplicación* consta de dos listas: Aplicaciones existentes que contiene las aplicaciones ingresadas al sistema. Aplicaciones elegidas que contiene las aplicaciones escogidas como predeterminadas. (fig. 47)

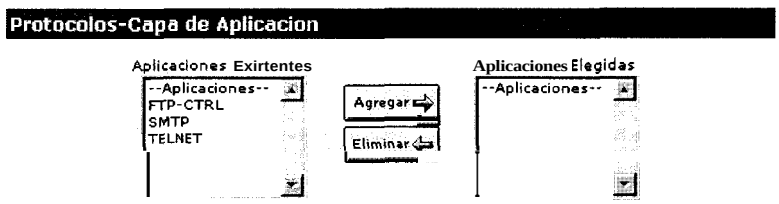


Fig.47 Protocolos de la Capa de Aplicacion

Para realizar la configuración predeterminada, se debe escoger de la lista una o varias aplicaciones existentes y presionar el boton agregar (fig.48)

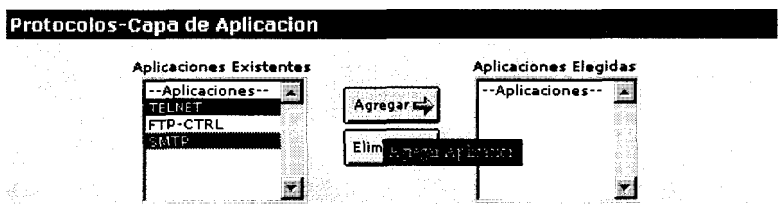


Fig.48 Selección e Ingreso de aplicaciones existentes

Si la elección se realizo correctamente, las aplicaciones se mostraran en la lista de elegidas. (fig.49)

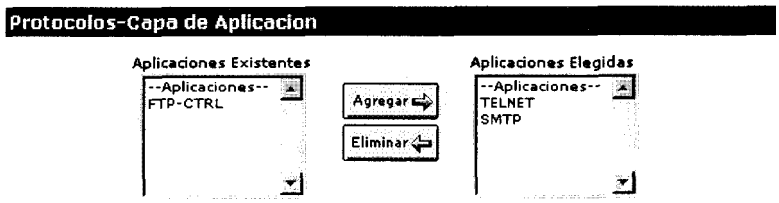


Fig.49 Aplicaciones elegidas ingresadas correctamente

5.1.2. Elirninacion de Protocolos

Para eliminar alguna de las aplicaciones elegidas, el procedimiento es el mismo; se escoge la aplicacion a eliminar **y** se presiona el boton eliminar (fig.50)

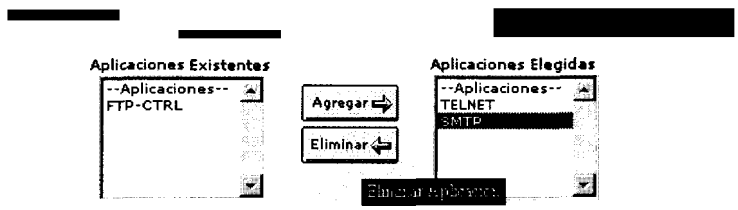


Fig.50. Eliminacion de aplicación elegida

Una vez que la eliminación se ha realizado, la aplicacion eliminada regresa a la lista de aplicaciones existentes (fig.51)

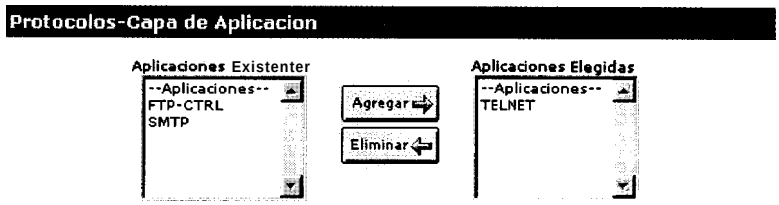


Fig.51. Aplicación eliminada en aplicaciones elegidas

5.2. Direcciones IP

5.2.1. Selección de Direcciones

Del mismo modo, para configurar direcciones IP como predeterminadas, se escoge una o varias de la lista de IP existentes y se presiona boton agregar (fig. 52)

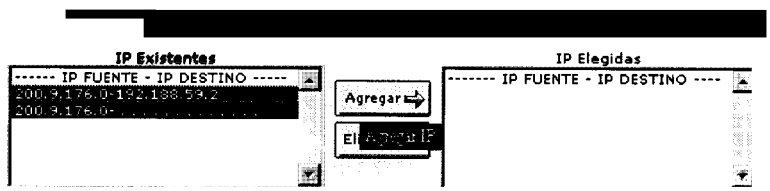


Fig.52. Configurar direcciones IP como predeterminadas

Si la acción fue realizada exitosamente, las direcciones se mostraran en la lista de elegidas (fig.53)

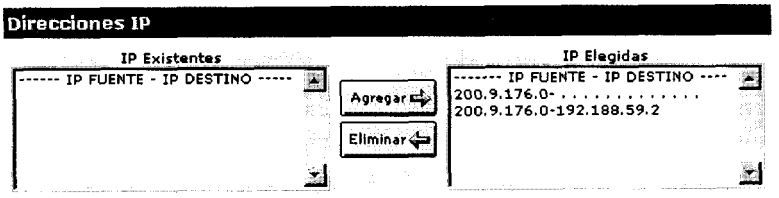


Fig.53 Ingreso exitoso de direcciones IP elegidas.

5.2.2. Eliminación de Direcciones IP

Para eliminar una o varias direcciones IP elegidas, es necesario seleccionarlas y presionar el boton Eliminar (fig. **54)**

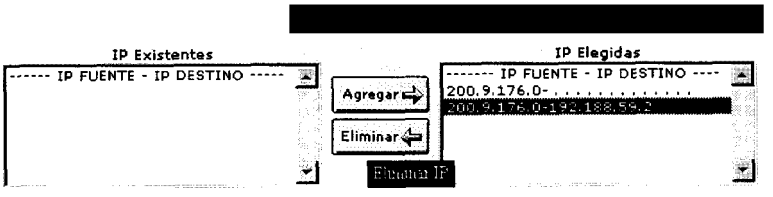


Fig. 54 Eliminación de Direcciones IP elegidas.

Una vez que la dirección IP elegida ha sido eliminada,. se listara en *IP existentes* (fig. 55).

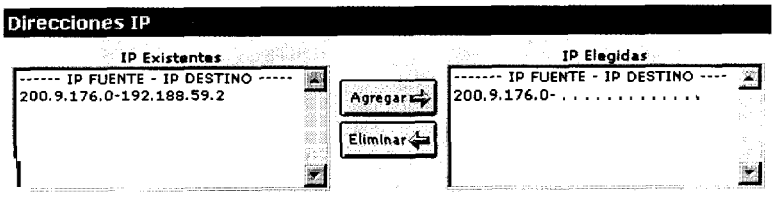


Fig.55. Dirección IP eliminada de IP elegidas

5.3. Mantener Configuración Predeterminada

Luego de realizar la elección para la configuracion predeterminada, es necesario presionar el boton Aceptar (fig. 56)

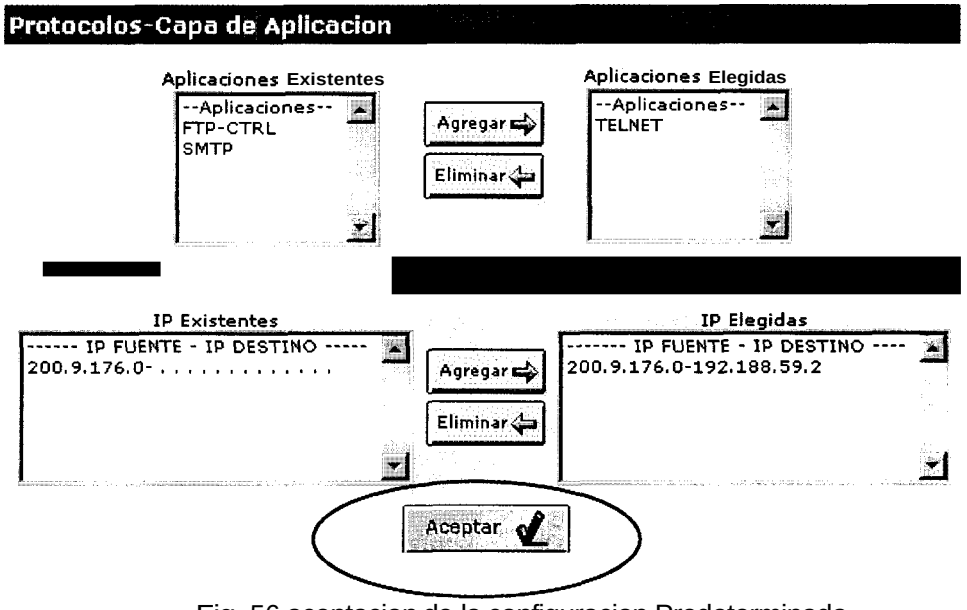


Fig. 56 aceptacion de la configuracion Predeterminada

Si los datos han sido ingresados exitosamente, el sistema mostrara el mensaje respectivo (fig. 57)

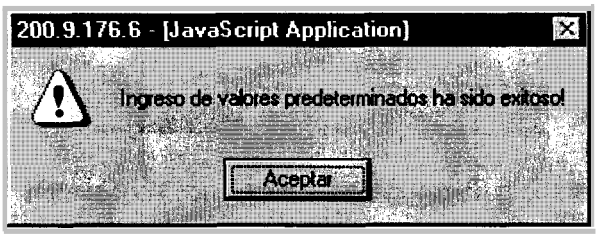


Fig. 57 Mensaje de ingreso exitoso

5.4. Configuración Predeterminada en la forma de la consulta.

Los valores escogidos como predeterminados apareceran seleccionados en la consulta (fig. 58). Para desactivarlos se debe dar un click en el area vacia de la lista.

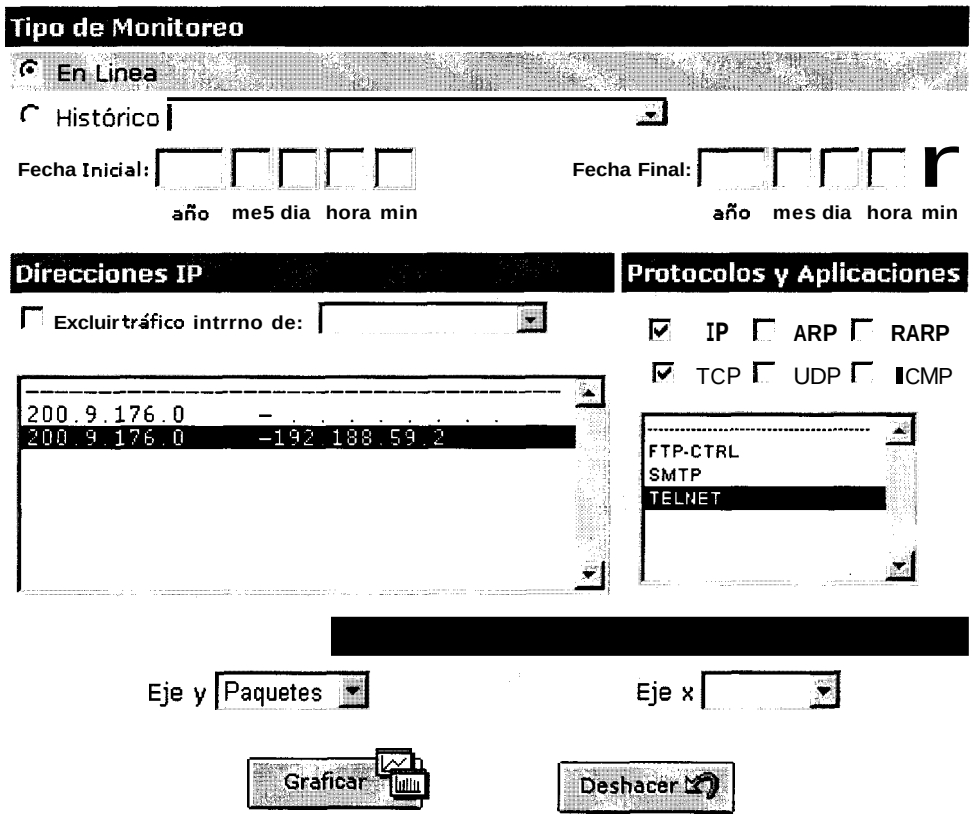


Fig. 58 Forma de la consulta con configuración predeterminada

6. Administracion de Usuarios.-

El sistema Monitor de Trafico IP le ofrece al administrador la capacidad de crear nuevos usuarios, editar y eliminar los usuarios existentes del sistema (fig. 59).

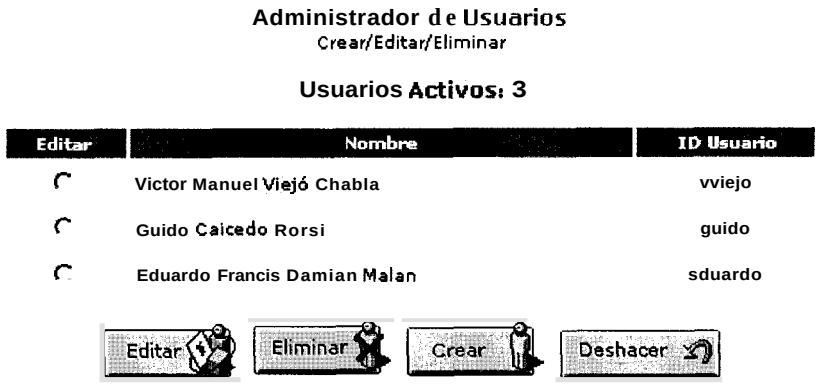


Fig.59 Adrninistracion de usuarios

El sistema presenta una lista de los usuarios activos junto con sus respectivos ID. Para seleccionar un usuario es necesario marcarlo con el mouse en el boton de radio.

6.1. Editar usuario

Para editar un usuario existente, es necesario seleccionarlo por medio del boton de radio y luego se presiona el boton Editar (fig. 60)

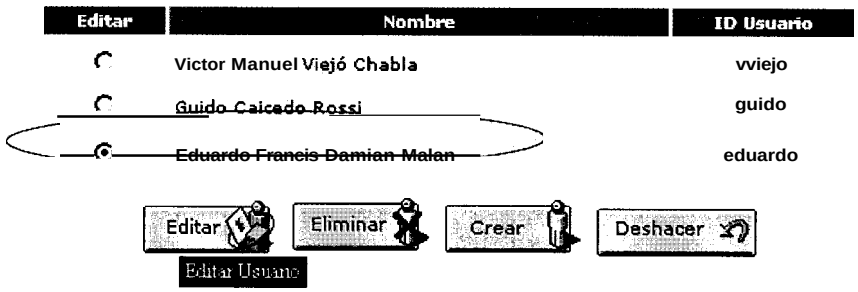


Fig. 60 Usuario seleccionado para la edicion

En la edicion de los datos , uno o varios campos pueden ser cambiados (fig. 61). Si el administrador no inserta dato alguno en cualquiera de los campos, el sistema mantendra los datos anteriores.

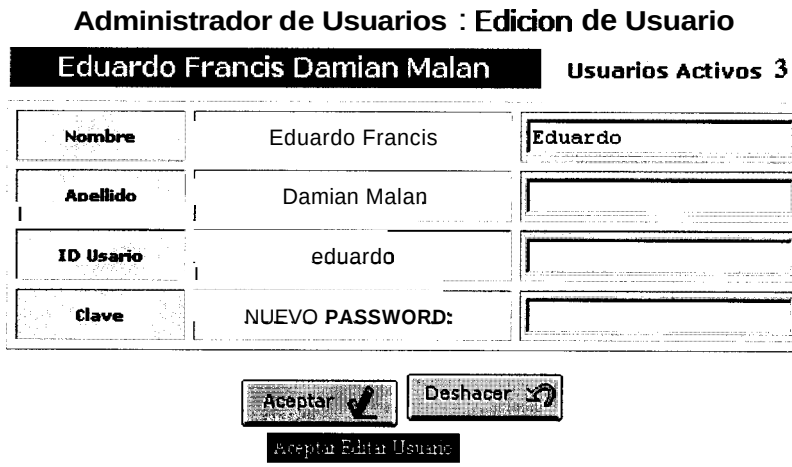


Fig. 61 Edición de un usuario especifico

Cuando uno o todos los datos editados estan incorrectos, el sistema retorna los valores iniciales al presionar el boton Deshacer.

Una vez que los datos han sido cambiados, el sistema mostrara los nuevos datos en la lista de usuarios. (fig. 62)

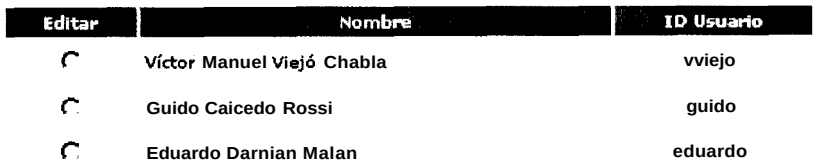


Fig. 62 Edición de usuario exitosa

6.2. Eliminar usuario

De la misma manera; para eliminar un usuario ***es*** necesario seleccionarlo por medio del boton de radio **y** luego presionar Eliminar (fig. 63)

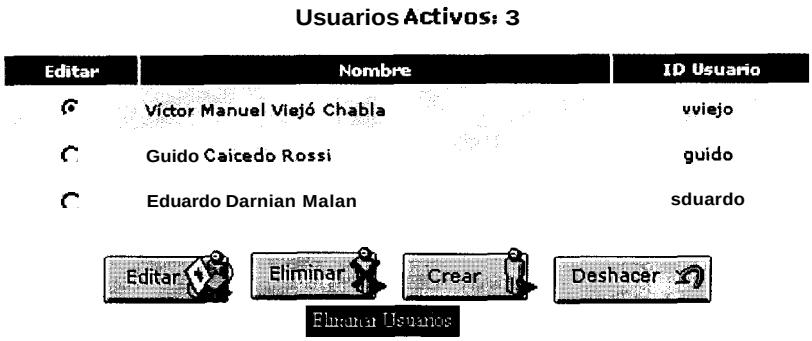


Fig. 63 Eliminación de Usuarios

Cuando un usuario ha sido eliminado no aparecera en la lista de usuarios activos (fig. **64)**

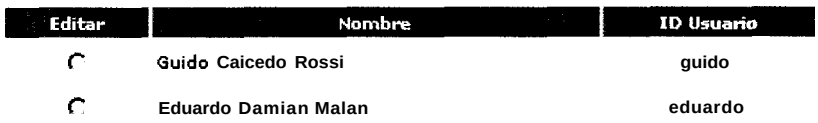


Fig. 64 Eliminación exitosa de un usuario

6.3. Crear Usuario

Si el administrador desea crear un usuario nuevo debera presionar el boton Crear **(fig.** 65)

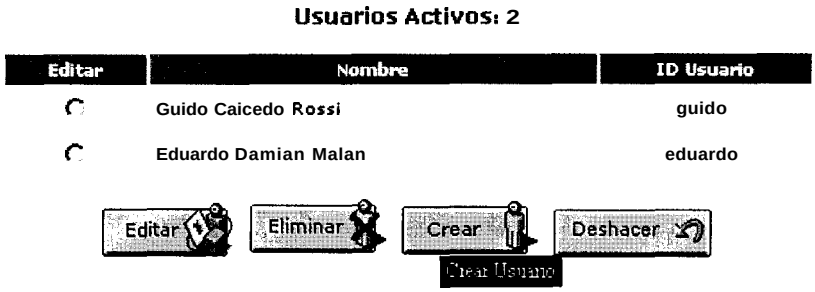


Fig. 65 Creación de un nuevo usuario

Para crear un nuevo usuario el administrador debera llenar la forma con los datos respectivos y luego presionar Aceptar (fig. *66)*

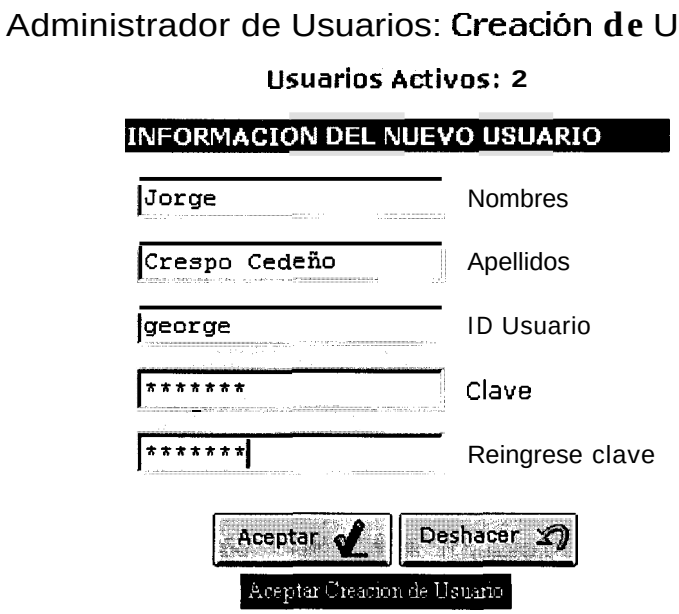


Fig. 66 Creación de un nuevo usuario

Cuando el usuario ha sido ingresado correctamente, el sistema aumentara en 1 el numero de usuarios activos (fig. 67)

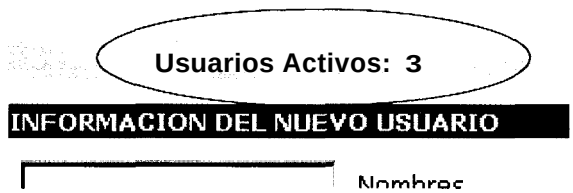


Fig.67 Numero de usuarios activos

Si la inserción del nuevo usuario se ha realizado correctamente, este aparecera en la lista de usuarios activos (fig. 68)

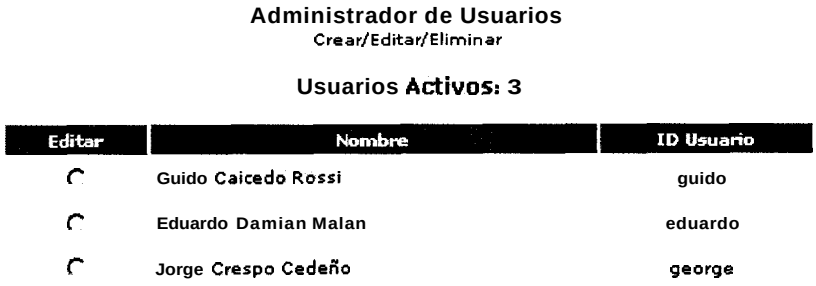


Fig. 68 Inserción de un nuevo usuario

6.4. Ingreso incorrecto de usuario

Cuando uno o todos los datos de un nuevo usuario son incorrectos, el sistema borra todos los campos al presionar Deshacer (fig. 69)

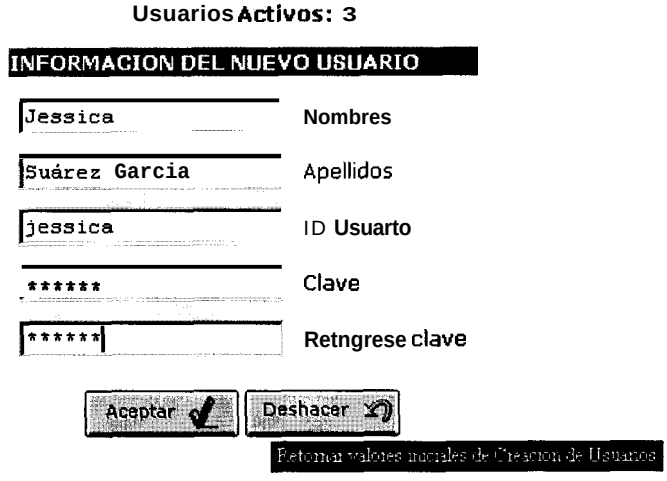


Fig.69 Ingreso incorrecto de usuario

El formulario para crear nuevos usuarios se mostrara sin dato alguno en todos los campos (fig. 70)

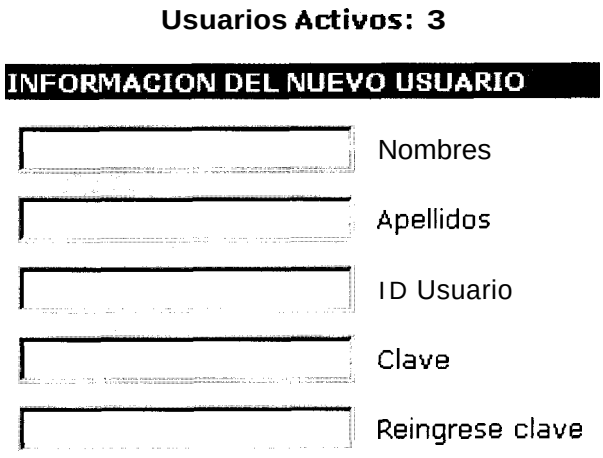


Fig.70 Campos vacios por la acción de deshacer

7. Registros de Monitoreo

El sistema diseiiado guarda registros de las fechas de inicio y pausa de los monitoreos realizados, así como el tamaiio en paquetes y kbytes (fig. 71)

Fecha de Inicio	Fecha de Pausa	Paquetes	KBytes
1999 09 08 15:18:34	1999 09 08 15:54:19	104978	69056.77
1999 09 08 17:10:46	1999 09 08 17:14:16	8541	5862.14
1999 09 08 17:14:40	1999 09 08 17:14:43	1772	1677.94
1999 09 13 17:03:19	1999 09 13 17:10:37	7671	2575.03

Fig. 71 Registros de Intervalos de monitoreo activo

7.1. Eliminación de Registros

El Administrador tiene la capacidad de eliminar cualquiera de los registros existentes.

Para eliminar debe seleccionar el/los registros de la lista que se presenta **(fig.** 72), y luego presionar el boton Eliminar Registros.

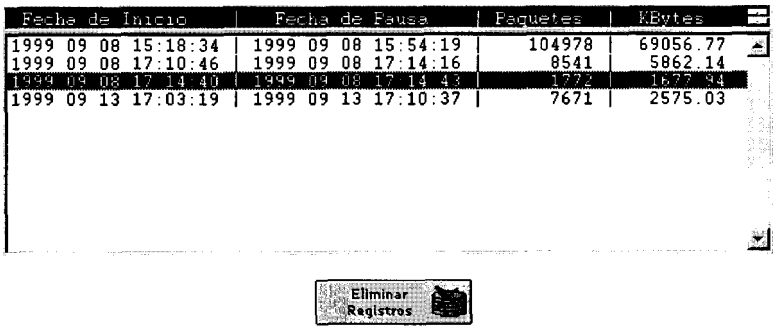


Fig. 72 Selección de registro a eliminar

En esa instancia, los registros no son eliminados, los intervalos seleccionados se muestran nuevamente en una lista (fig. 73). Se requiere que el Administrador acepte para proceder a la eliminacion de los registros.

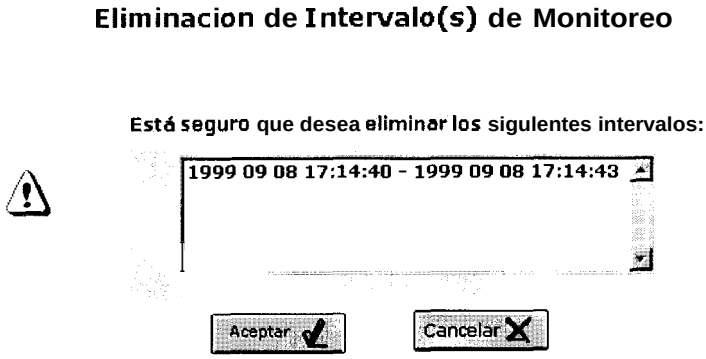


Fig. 73 Confirmación de la eliminación de intervalos

Eliminar los registros desde la base toma ciertos minutos, mientras esta acción se realiza el sistema mostrara un mensaje (fig. **74).**

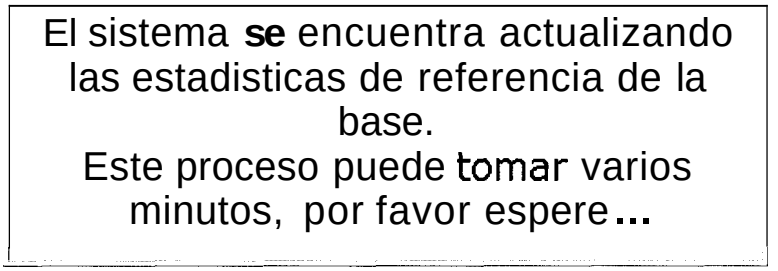


Fig. 74 Mensaje de actualización de la base de datos

8. Salir.-

Si el administrador desea abandonar el sistema, es necesario que haga uso del boton Salir que se encuentra en el menu.

Fig.75 Boton **para** salir del sistema

Al presionar este boton el sistema se cierra correctamente, lo que implica que todos los archivos temporales seran borrados automaticamente para evitar así el congestionamiento del servidor por el exceso de archivos.

Finalmente se mostrara el mensaje de salida.

Monitor de Trafico IP se encuentra procesando su salida.
Espere por favor...

Fig. *76* Mensaje de salida del sistema

APENDICE IV

Manual del Usuario del Sistema

El Usuario del sistema Monitor de Trafico IP para Redes Ethernet tiene la capacidad de obtener información del trafico de la red por medio de las consultas.

Podrán hacer uso del sistema todos los usuarios que posean un user–id y un password, necesarios para ingresar. Caso contrario, contacte con el administrador.

1 Iniciando la sesion

Para iniciar la sesion, el usuario necesita abrir un browser y colocar la dirección http donde se encuentra el sistema. Luego de que este ha sido cargado deberá ingresar el user y el password (Fig. 1).

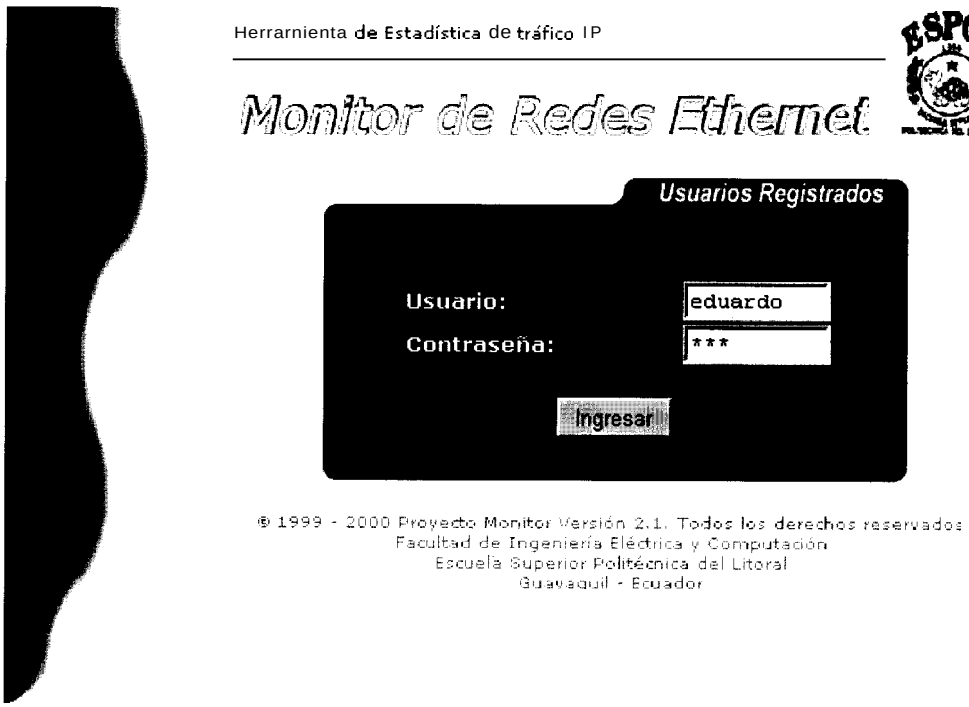


Fig. 1 Pantalla **de** Ingreso

Si los datos del usuario son correctos, el sistema iniciara la sesion (Fig. **2),** caso contrario mostrara el mensaje de error respectivo **y** permitira al usuario realizar un nuevo intento de ingreso.

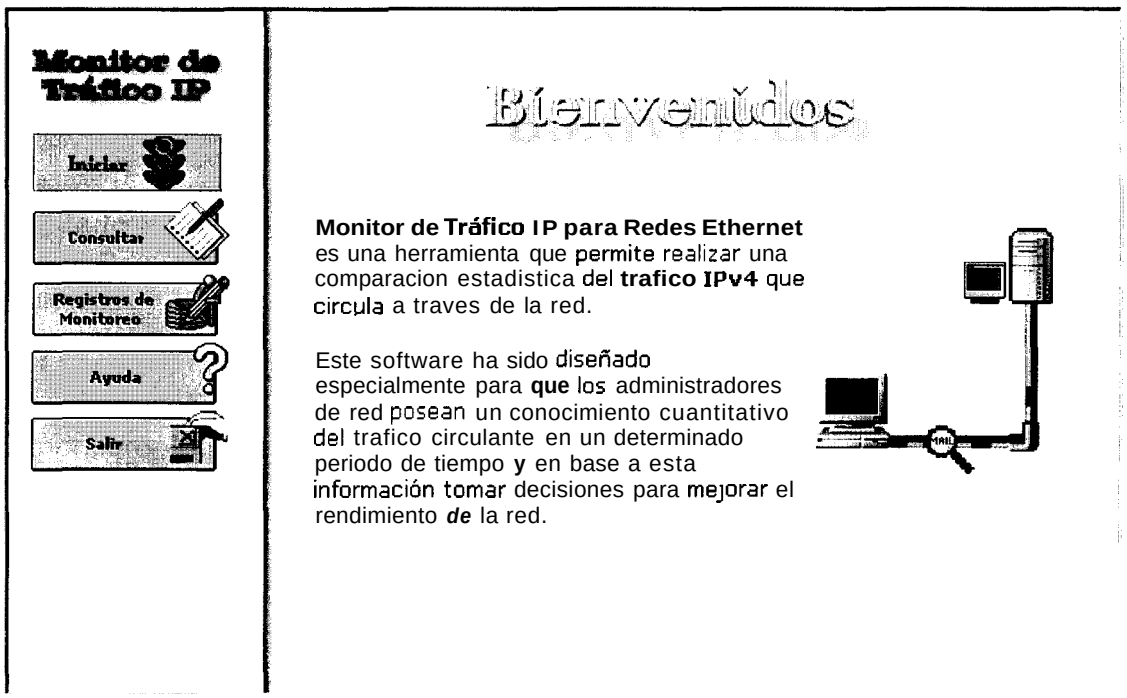


Fig. 2 Bienvenida y **Menu** del Usuario

Al iniciar, el sistema muestra una pantalla que consta de dos partes claramente diferenciadas. El lado izquierdo que contiene el menu con las opciones disponibles para el usuario; y en el lado derecho el mensaje de bienvenida al sistema.

2 Estado del Monitoreo

El estado del monitoreo puede ser consultado directamente desde el menu de opciones.

El monitoreo puede tener dos estados:

Activo .- Cuando las luces del semaforo estan cambiando de color constantemente (Fig. 3)

Fig. 3 Monitoreo Activo

Inactivo .- Cuando el semaforo se encuentra detenido en luz roja (Fig. **4)**

Fig. 4 Monitoreo Inactivo

NOTA: *El usuario no tiene la capacidad de iniciar o detener el monitoreo.*

3 Consultar

Para realizar las consultas el usuario deberá llenar la forma (Fig. 5) con los datos necesarios que permitiran obtener las graficas deseadas.

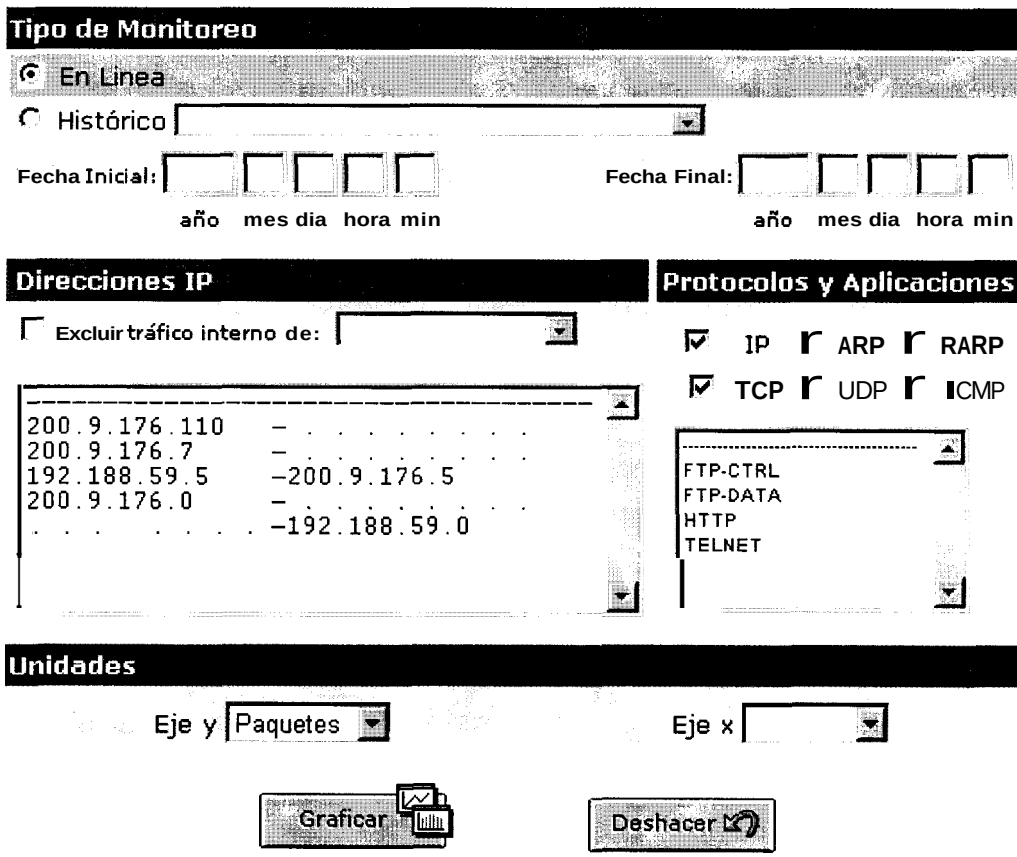


Fig. 5. Formulario para las consultas

3.1 Tipo de Consulta

La consulta puede ser historica o en línea (Fig. 6). Ambas opciones son mutuamente excluyentes, esto es, el usuario solo podra seleccionar un tipo a la vez.

Por defecto, el sistema mostrara como seleccionado el tipo en línea, en este caso los campos del histórico permaneceran en blanco.

Fig. 6 Tipo de Consulta

Al seleccionar la consulta historica, los campos se activaran automaticamente y el usuario podra escoger algun intervalo particular de los que se encuentran en la lista desplegable (Fig. 7). Los campos para las fechas inicial y final se llenaran automaticamente con las fechas del primer intervalo de muestreo que tenga registrado.

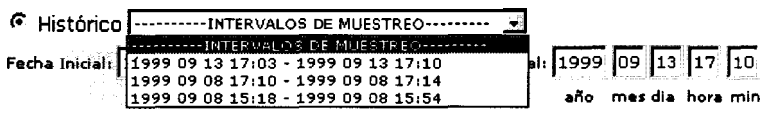


Fig. 7 Intervalos de Consulta Histórica

Si los limites de los intervalos deseados no constan en la lista, el usuario podra ingresar en los campos las fechas deseadas (Fig. 8) .

Fig. 8 Ingreso de fechas de la consulta histórica

Se recomienda que el intervalo ingresado se encuentre entre la primera fecha mostrada en el primer intervalo **y** la segunda fecha del ultimo intervalo (Fig. 9). Si las fechas ingresadas estan fuera de este intervalo, es posible que el sistema no tenga datos que graficar, por lo tanto solamente presentara la información de cero.

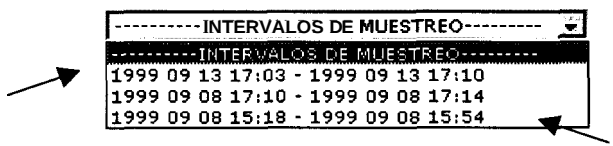


Fig. 9 Fechas inicial y final para la edicibn.

3.2 Direcciones IP

Excluir el *tráfico interno* implica realizar la consulta de todo el trafico que pasa por las direcciones IP seleccionadas, excepto el trafico de la red seleccionada en este campo (Fig.10). Para hacer uso de esta opción es necesario seleccionarla.

Fig. **10** Excluir el tráfico interno de una red

La red a excluir debe seleccionarse de la lista desplegable que contiene las opciones existentes (Fig. 11).

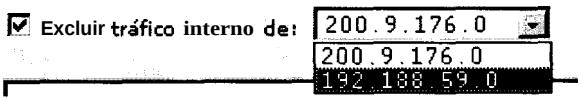


Fig. 11 Lista de redes existentes

En este campo se muestra una lista de las Direcciones IP que han sido ingresadas en el sistema por parte del administrador (Fig. 12). Si desea consultar alguna direccion IP que no consta en la lista, consulte con el administrador del sistema.

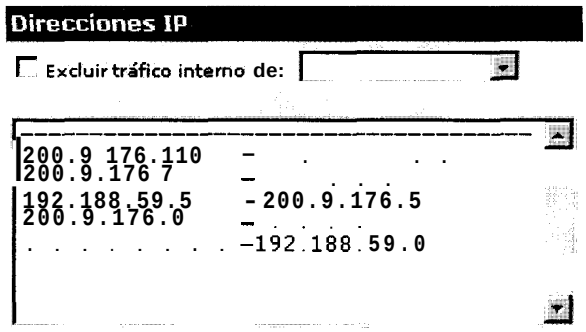


Fig. 12 Direcciones IP

Para seleccionar una direccion IP sobre la cual se va a consultar, es necesario posicionarse con el mouse sobre ella y presionar. En el caso de dos o mas se debe mantener presionado la tecla CONTROL y seleccionar con el mouse cada una de las opciones (Fig. 13).

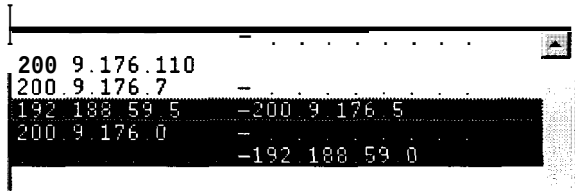


Fig. 13 Selección de Direcciones IP

3.3 Protocolos y Aplicaciones

Los Protocolos que se pueden consultar se muestran en esta sección del formulario. La lista muestra las aplicaciones existentes (Fig. **14).**

Fig. 14 Protocolos y Aplicaciones

Los protocolos existentes pertenecen a la capa de red (IP, **ARP,** RARP), **y** a la capa de transporte (TCP, UDP, ICMP) del modelo OSI. El sistema permite seleccionar ninguno, uno o **mas** de dichos protocolos (Fig. 15).

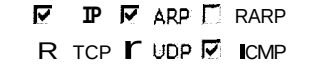


Fig. 15 Protocolos disponibles

Las aplicaciones existentes sobre las cuales se puede realizar las consultas se muestran en una lista de seleccion multiple (Fig. 16). En el caso de que la aplicacion a consultar no conste en la lista contactese con el administrador.

Fig. 16 Aplicaciones seleccionadas

Para seleccionar una opción es necesario pulsar sobre ella con el mouse. En el caso de dos o mas, se debe mantener presionada la tecla CONTROL y realizar la seleccion.

3.4 Unidades

Para generar las curvas es necesario seleccionar las unidades de los ejes de las gráficas (Fig. 17). En el caso de consulta en línea, el eje x (escala del tiempo) permanece deshabilitado.

Fig. 17 Unidades de los ejes

El **eje y** representa la unidad de trafico (fig. 18). El usuario podra seleccionar entre las opciones existentes, el tipo de unidad para la curva a generar. La unidad de trafico puede ser paquetes, bytes o kbits.

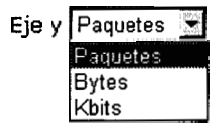


Fig. 18 Unidades de Tráfico

El **eje X** representa la unidad de tiempo (fig. 19). El grafico puede generarse en escalas de minutos, hora, dia o mes.

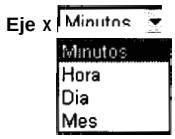


Fig. **19** Unidades de tiempo

3.5 Graficar

Para generar las curvas con las especificaciones escogidas tanto en línea como historico, se debe presionar el boton Graficar (Fig. 20). Durante esta acción deberá esperar unos minutos mientras se recolectan los datos de la Base.

Fig. 20 Botón para graficar

3.5.1 Graficar en linea

La consulta en linea permite obtener curvas en tiempo real del trafico actual de la red en la cual esta monitoreando. Para realizar este tipo de consulta es necesario seleccionar de la forma : el tipo de monitoreo en linea, minimo una dirección IP y una aplicacion., el eje y (Fig.21).

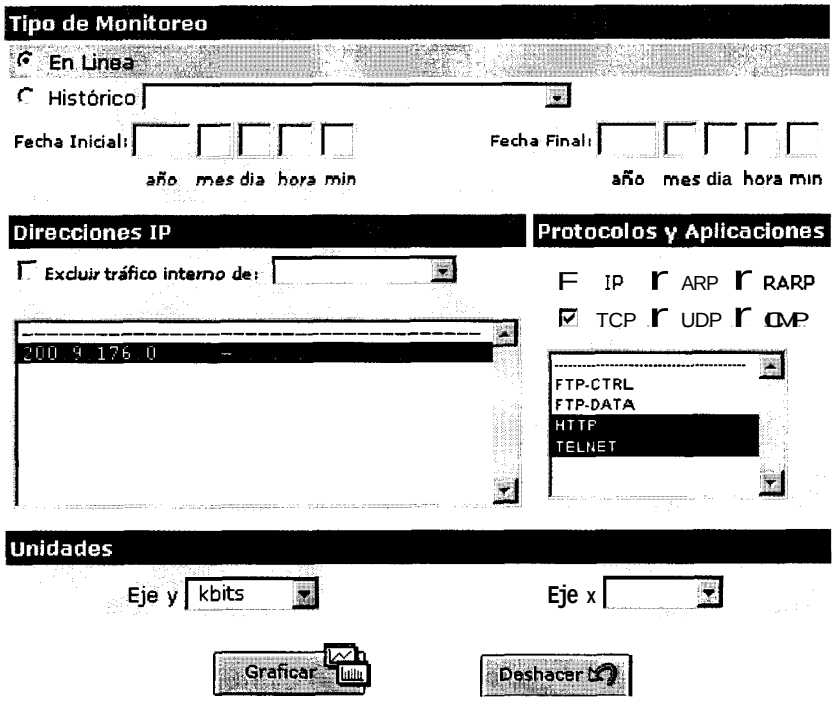


Fig. 21 Forma para realizar una consulta en linea

El grafico resultante se muestra en ejes coordenados **y** se va generando con respecto al tiempo (Fig. **22).**

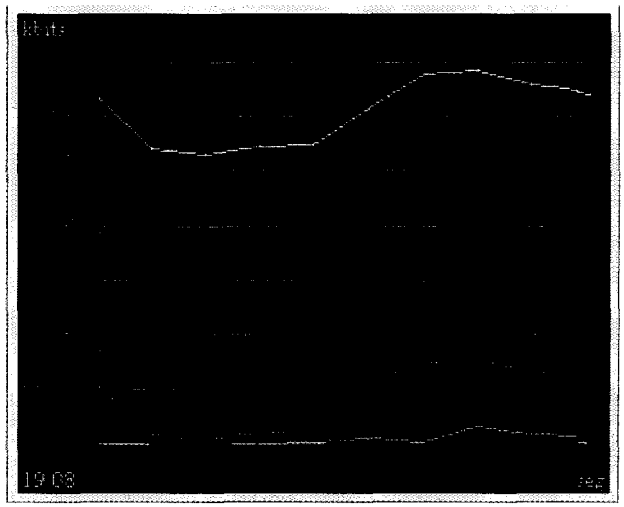


Fig. 22 Gráfico de consulta en línea

3.5.1.1 Opciones

Ocultar/mostrar grid:

Oculta o visualiza las cuadriculas en la grafica

Eje Y

Muestra por defecto el valor maximo, pero el usuario puede determinar un valor deshabilitando la autoescala

Eje x

Muestra el intervalo que va a presentar en pantalla. El valor por defecto es 20.

Dominios

Presenta las direcciones IP escogidas y el tipo de trafico con distincion de colores, necesarios para la interpretación del grafico.

Frecuencia

Representa el intervalo en el que el servidor va a realizar el muestreo de los datos a graficar.

Color grid

Muestra una paleta de colores y permite cambiar el color de las cuadriculas.

3.5.1.2 Ventana de Dominios

Para visualizar los detalles de los dominios basta con pulsar el boton de dominios y el sistema le mostrara una ventana con los dominios y protocolos a consultar (Fig. 23)

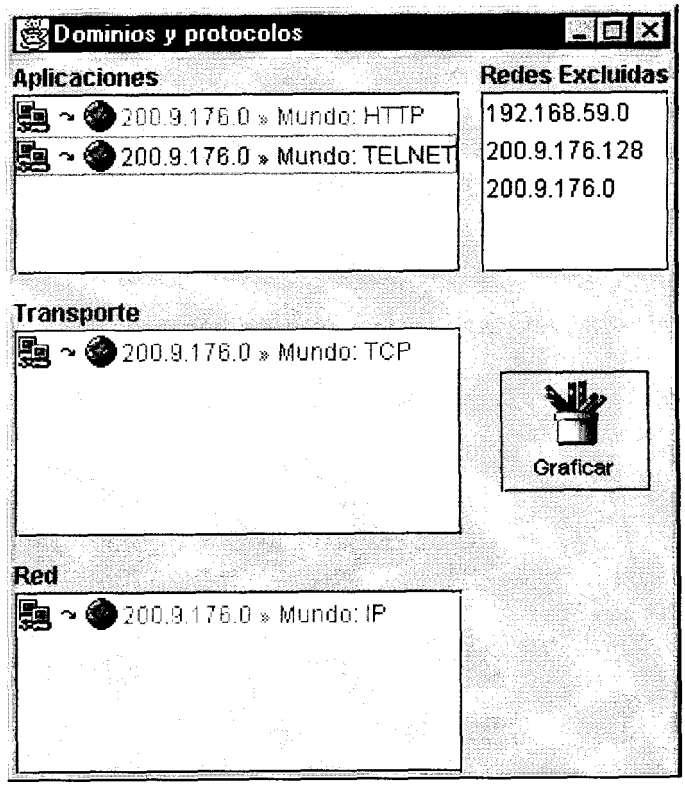


Fig. 23 Ventana de Dominios y protocolos

Con esta opción, el usuario esta en capacidad de :

- Distinguir por medio de colores las curvas con su respectiva leyenda (direcciones IP y tipo de trafico).
- Graficar otra curva entre las opciones presentes.
- Excluir alguna red del trafico que desea visualizar

3.5.2 Graficar Histórico

La consulta Histórica permite obtener graficos de intervalos de tiempos anteriores en los cuales existan datos. Para realizar este tipo de consulta, es necesario llenar la forma (fig. **24)**

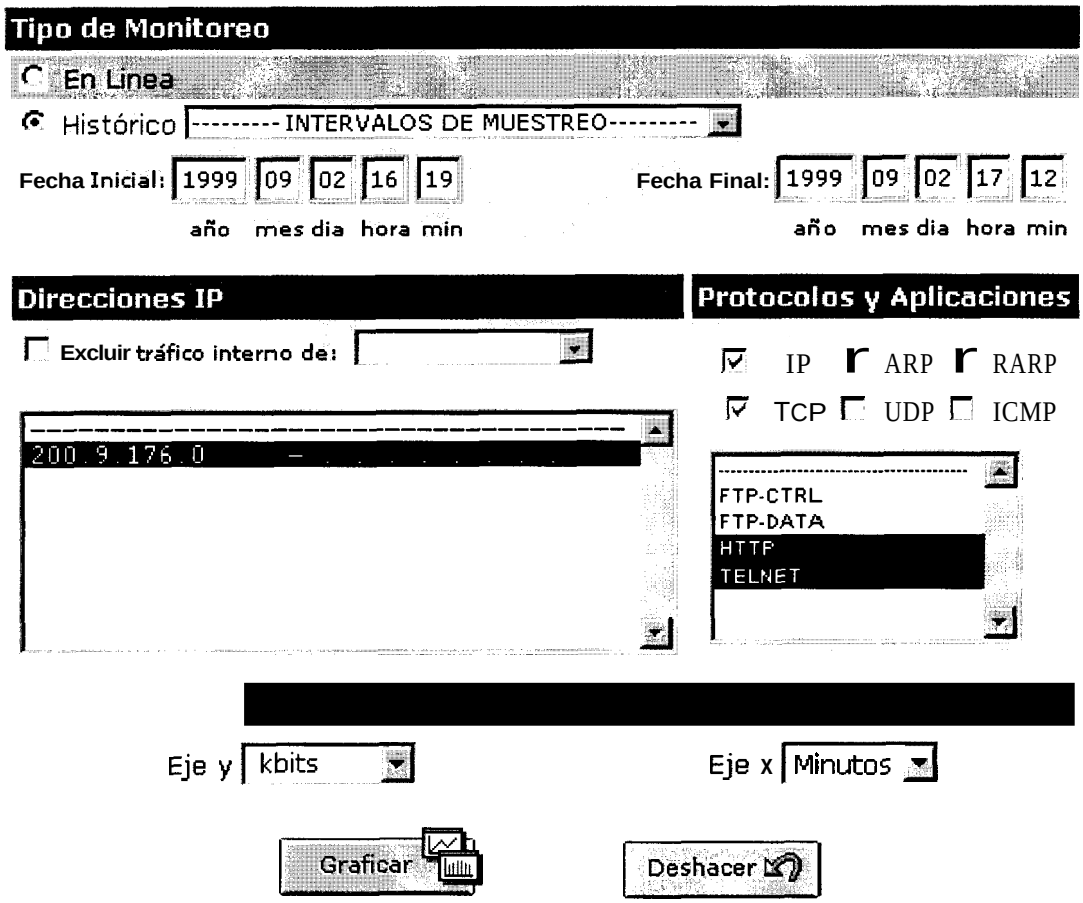


Fig. 24 Forma para realizar una consulta historica

Para realizar este tipo de consulta el usuario debe:

- Seleccionar el tipo de monitoreo histórico
- Fecha maxima y minima de muestreo.
- Minimo una dirección IP y una aplicacion.
- Las unidades de los ejes.

El grafico obtenido representa todo el trafico de cada una de las direcciones IP consultadas y se muestra en ejes coordenados: La leyenda indica la dirección a la cual pertenece. (fig. 25)

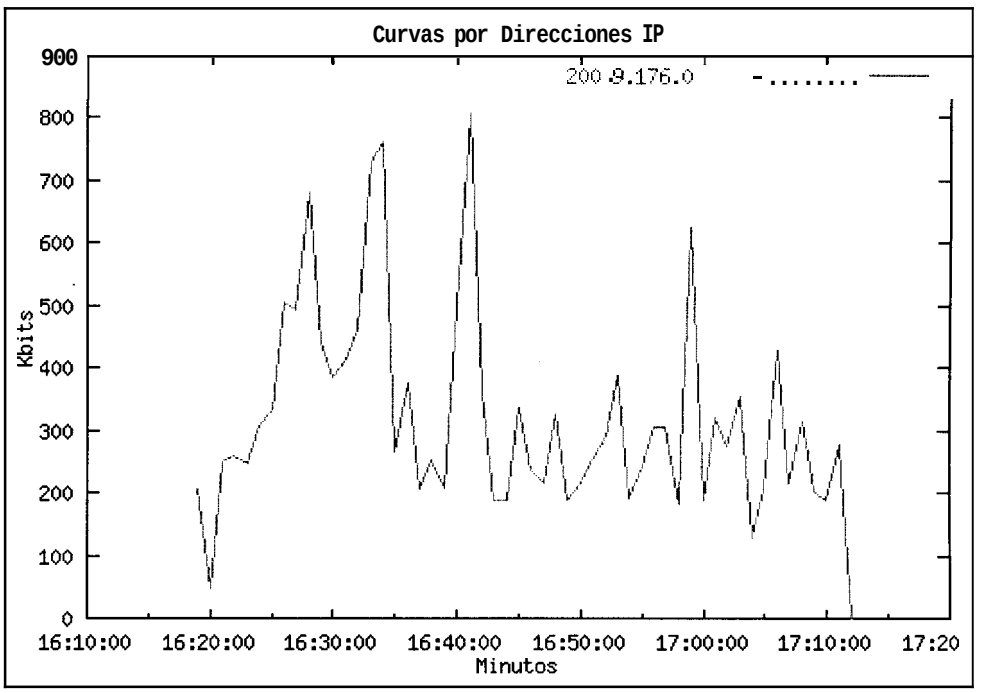


Fig. 25 Curva **del** tráfico consultado en histórico

3.5.2.1 Curvas Específicas

El sistema permite al usuario obtener las curvas específicas de cada una de las opciones que selecciono al iniciar la consulta. Para ello, se debe escoger de la forma que se presenta con el grafico general (fig. 26.).

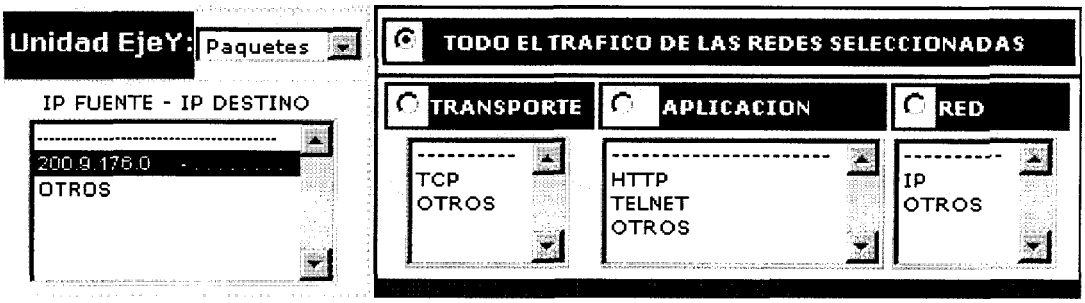


Fig. 26 Forma para obtener graficas especificas

El usuario tiene capacidad para:

- Cambiar la unidad de trafico (eje **Y).**
- Obtener graficos de cada una de las direcciones IP. (OTROS representa todas las demas direcciones IP, excepto la seleccionada.)
- Realizar curvas especificas de una o todas las direcciones IP, de todo el trafico o de alguno en particular. Cada curva tendra un color distintivo.

Las opciones de las curvas especificas se limitan a las establecidas en el formulario.

3.5.2.2 Puntos maximos y minimos

El sistema permite consultar los puntos maximos y minimos de las curvas presentes en el grafico. Cada una de las direcciones IP se presentaran con el color distintivo de la curva a la cual se refieren (fig. 27).

Direcciones IP	Puntos Mínimos		Puntos Máximos	
	Fecha	Kbits	Fecha	Kbits
200.9.176.0 -	1999/09/02 16:20:00	0.000	1999/09/02 16:41:00	806.239

Fig. 27 Puntos maximos y minimos de los gráficos

3.5.2.3 Ajustar Graficos

El usuario tiene la opción de ajustar los graficos en otros intervalos internos, es decir, los puntos maximos y minimos del nuevo grafico deben estar incluidos en el intervalo inicial (fig. 28).

Fig. 28 Limites para ajustar gráfico

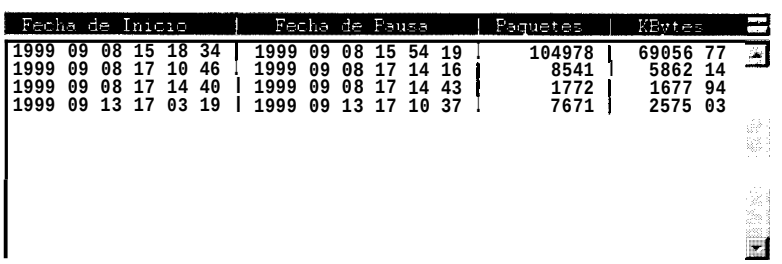
En caso de no establecer maximos y minimos, o ingresar datos fuera del rango, el sistema tomara los maximos y minimos originales.

IMPORTANTE : El grafico solo puede ajustarse dentro del rango original.

4 Registros de Monitoreo

El sistema diseñado guarda registros de las fechas de inicio y pausa de los monitoreos realizados, asi como el tamaiio en paquetes y kbytes

El usuario esta en la capacidads de consultar dichos registros con el objeto de informarse en que intervalos existen datos.(fig.29)



Fecha de Inicio	Fecha de Pausa	Paquetes	KBytes
1999 09 08 15 18 34	1999 09 08 15 54 19	104978	69056 77
1999 09 08 17 10 46	1999 09 08 17 14 16	8541	5862 14
1999 09 08 17 14 40	1999 09 08 17 14 43	1772	1677 94
1999 09 13 17 03 19	1999 09 13 17 10 37	7671	2575 03

Fig. 29 Registros de Intervalos de monitoreo activo

5 Salir.-

Si el usuario desea abandonar el sistema, es necesario que haga uso del boton *Salir* que se encuentra en el menu. (fig 30)

Fig. 30 Botón para salir del sistema

Al presionar este boton el sistema se cierra correctamente, lo que implica que todos los archivos temporales seran borrados automaticamente para evitar así el congestionamiento del servidor por el exceso de archivos.

Finalmente se mostrara el mensaje de salida.

Monitor de Tráfico IP se encuentra procesando su salida.
Espere por favor...

Fig.31 Mensaje de salida del sistema

BIBLIOGRAFIA

1. Douglas E. Comer, Redes Globales de Información con Internet y TCP/IP, principios basicos, protocolos y Arquitectura (3ra. Edición; Mexico; Prentice Hall Hispanoamerica S.A., 1996).

2. Douglas E. Comer and David L. Stevens, Cliente-Server Programming and Applications, Volumen III (Prentice Hall, Inc. Upper Saddle River, New Jersey 07458).