UNIVERSIDAD DON BOSCO

FACULTAD DE INGENIERIA

TRABAJO DE GRADUACION PARA OPTAR AL GRADO DE INGENIERO EN CIENCIAS DE LA COMPUTACION

DESARROLLO DE UN SISTEMA DE ADMINISTRACION Y MONITOREO DE RED

PRESENTADO POR:

ALFONSO JOSE CORNEJO PLATERO

LUIS ARMANDO CASTRO CHAVEZ

MELVIN RODRIGO AGUILAR RUBIO

ING. RAFAEL COBOS
JURADO

ING. JULIO RIVERA
JURADO

ING. JUAN CABRERA
JURADO

ING. CARLOS BRAN
ASESOR

ING. JAIME ANAYA
TUTOR

SEPTIEMBRE - 2006

SOYAPANGO - EL SALVADOR - CENTRO AMERICA

Damos las gracias a Dios por habernos iluminado para
poder completar esta tarea y a nuestras familias por el apoyo
brindado a lo largo de todos estos años ya que sin ellos este logro
no hubiera sido posible.

INTRODUCCION

Actualmente el uso de redes de computadoras constituye una verdadera necesidad para la realización de la mayoría de actividades de la vida cotidiana, el rápido crecimiento de estas implica constantes tareas de administración y monitoreo para la verificación de su correcto funcionamiento.

Los sistemas de administración y monitoreo de redes de datos, son una herramienta esencial para la relación entre los administradores de red y los dispositivos dentro de esta. Una red correctamente administrada y monitoreada permite realizar cambios de manera fácil, supervisar el rendimiento de los dispositivos así como también detección y el control de fallas en el sistema.

El presente proyecto consiste en un sistema de administración y monitoreo de red, para ello, se utilizan varios protocolos de red, herramientas de administración y programación.

- SNMP (Simple Network Management Protocol)
- ICMP (Protocolo de control de mensajes de Internet)
- ARP (Protocolo de resolución de direcciones)
- NetBios
- WinPcap, Net-SNMP, Nmap/WiNmap, MySQL

Se ofrece una interfaz gráfica que permite la visualización de los dispositivos de red y se muestran datos relevantes del host estudiado durante el desarrollo de la aplicación para el funcionamiento de la red, además se realiza la revisión del estado de los puertos y servicios de red activos de un dispositivo.

Posteriormente contara también la opción de establecimiento de alarmas en los dispositivos esenciales. Con el desarrollo de esta herramienta se pretende beneficiar a cualquier usuario que desee tener una herramienta gratuita para la administración y monitoreo de una red.

CAPITULO I
ANTECENDENTES E IMPORTANCIA

1.1 ANTECEDENTES

La investigación se enfoca en la especialidad de redes, se presenta una herramienta útil para administradores de redes, capaz de monitorear y administrar estas sin importar la topología que esta presente, permitiendo de esta forma visualizar, comprender y administrar el funcionamiento de la misma.

Para elaborar una aplicación que tenga todas las funciones necesarias de un sistema de administración de red, se deben estudiar aquellos protocolos que sean capaces de proporcionar información de los dispositivos presentes en la red.

Entre la información necesaria deben considerarse la dirección IP, el estado del dispositivo (activo o inactivo), el uso del microprocesador, sistema operativo utilizado, y en dispositivos como routers, se obtendrá el número de interfaces utilizadas y la información respecto a la dirección física y lógica.

Uno de los protocolos necesarios para la obtención de esta información es el ICMP pues es uno de los mecanismos que al producirse un error en la entrega de un paquete IP, notifica que el datagrama no pudo ser entregado; este protocolo no corrige los errores solamente notifica de estos a la estación que envió el paquete.

Por otra parte el protocolo SNMP se utiliza para la comunicación de información de gestión de red entre las estaciones y los agentes de red, se enfoca en tres objetivos, minimizar el número y complejidad de las funciones de gestión realizadas por el propio agente de gestión, ser flexible para posibilitar aspectos de gestión y operación de la red, que sean independientes de la arquitectura de dispositivos particulares.

Para una administración de red eficiente, es necesario determinar la ubicación física de los dispositivos en estudio, es por eso que obtener el diseño de la topología de red se vuelve indispensable para resolver problemas de capa física que presentara la red.

Una vez definidos los protocolos y herramientas a utilizar debe explicarse el por qué de un sistema de administración de red. Todo administrador desea que la red a su cargo no presente ningún tipo de inconveniente. Teniendo una perspectiva gráfica de la estructura la red se podrá minimizar los problemas con acciones tales como la identificación de dispositivos no activos la cual puede atenderse rápidamente si una alarma es activada.

1.2 IMPORTANCIA DE LA INVESTIGACIÓN

La administración de Redes es un conjunto de técnicas orientadas a mantener una red operativa, eficiente, segura, constantemente monitoreada y con una planeación adecuada y propiamente documentada.

Sus objetivos son:

- Mejorar la continuidad en la operación de la red con mecanismos adecuados de control y monitoreo, de resolución de problemas y de suministro de recursos.
- Hacer uso eficiente de la red y utilizar mejor los recursos.
- Hacer la red más segura al protegerla contra accesos no autorizado.
- Controlar cambios y actualizaciones en la red de modo que ocasionen el menor número posible de interrupciones en el servicio a los usuarios.
- Proyectar la escalabilidad de las redes.
- Predecir análisis y solución de problemas técnicos (troubleshooting).

El sistema de administración y monitoreo de red opera bajo los siguientes lineamientos:

- Colección de información acerca del estado de la red y componentes del sistema. La información recolectada de los recursos debe incluir: eventos, atributos y acciones operativas.
- Transformación de la información para su presentación en formatos apropiados para el entendimiento del administrador.
- Transporte de información del equipo monitoreado al centro de control.
- Almacenamiento de datos coleccionados en el centro de control.
- Análisis de parámetros para obtención de conclusiones que permitan la deducción rápida de los eventos en la red.
- Generación de acciones rápidas y automáticas en respuesta a una falla mayor.

La característica fundamental de un sistemas de administración de red moderno es la de ser un sistema abierto, capaz de manejar varios protocolos y trabajar con varias arquitecturas de red.

Un administrador de redes en general, se encarga principalmente de asegurar la correcta operación de la red, tomando acciones remotas o localmente. Se encarga de administrar cualquier equipo de telecomunicaciones de voz, datos y video, así como de administración remota de fallas, configuración rendimiento, seguridad e inventarios.

El desarrollo de este proyecto permite la generación de una herramienta que puede utilizarse con fines didácticos ya que mediante su uso podrá explicarse de manera práctica el funcionamiento de los protocolos que se utilizan para el desarrollo del sistema.

1.3 PLANTEAMIENTO DEL PROBLEMA

Las diferentes empresas que hacen uso de redes de computadoras, las cuales siempre tienden a ser muy extensas, comparten un mismo problema, la administración permanente de todos los elementos presentes en su topología y principalmente los constantes cambios a los que esta se encuentra sometida, como la introducción de algún dispositivo sin ningún tipo de notificación, la irregularidad en alguno de ellos, el mal funcionamiento o la repentina desactivación de un equipo indispensable para el funcionamiento de la red, por ejemplo, un router o un servidor.

Dicha gestión se realiza con aplicaciones de costos muy elevados, que tienen como fines primordiales la detección y distribución de los dispositivos así como identificar e informar, cuando sea necesario, el estado de los mismos (activo o inactivo) y el rendimiento de los mismos.

1.4 JUSTIFICACIÓN

La administración y monitoreo de redes implica la adquisición de herramientas útiles para conocer aspectos importantes de la red tales como el diagrama de la misma, el esquema de direccionamiento IP, el estado y cantidad de dispositivos existentes en la red, entre otro. Existen varias aplicaciones capaces de desarrollar este trabajo, sin embargo las que se implementan bajo la plataforma Windows tienen altos costos económicos y este factor influye de gran manera en la decisión de adquirir una o no.

Debe tenerse presente que para realizar administración y monitoreo eficiente es necesario contratar servicios profesionales de personal capacitado, con ello se visualiza la importancia de la investigación previa que se realiza en este documento sobre conocimientos generales de networking y sobre todo de los protocolos que servirán para comprender el proceso de monitoreo y poder así implementar una aplicación eficiente.

La creciente demanda de servicios de transmisión de datos y de acceso a Internet a obligado a las empresas e instituciones a tener funcionando sus redes de manera casi perfecta, el uso de una herramientas de administración y monitoreo de red brinda un gran apoyo para mantener la red funcional y poder responder rápidamente ante cualquier problema.

1.5 OBJETIVOS

1.5.1 OBJETIVO GENERAL

Desarrollar un sistema informático para la administración de red, que permita mediante técnicas de networking monitorear el rendimiento y obtener la distribución de los dispositivos presentes en la misma.

1.5.2 OBJETIVOS ESPECÍFICOS

- Desarrollar una sección del sistema que permita identificar e informar el estado de los elementos de la red.
- Desarrollar una consola gráfica de administración para presentar la configuración de los dispositivos activos, el estado de los dispositivos pasivos y el conjunto de variables de rendimiento de este.
- Desarrollar una sección del sistema para el descubrimiento y mapeo de la topología de la red.
- Proveer al sistema de administración la capacidad de establecimiento de alarmas de notificación del estado de dispositivos esenciales de la red.

- Generar un modulo para la obtención de estadísticas de las variables relevantes en los dispositivos presentes así como también las revisión del estado de los puertos y servicios de red activos en un dispositivo específico.
- Otorgar una aplicación que facilite la compresión de asignaturas relacionadas con redes informáticas que pueda contribuir en el aprendizaje del funcionamiento de los protocolos que se han de utilizar para desarrollo de sistemas.

1.6 ALCANCES

Con el desarrollo del presente proyecto se lograra:

- Presentar un diseño estructurado de la elaboración del sistema.
- Se desarrollara una interfaz gráfica amigable facilite la operación y la visión de la red en estudio.
- Se mostraran todos los dispositivos existentes en la red, con una ilustración que identifique el tipo.
- Se obtendrá el rendimiento básico de los elementos, por medio de la información recabada por los protocolos del sistema.
- Describir los dispositivos presentes, identificar cada uno de ellos si es un router, switch o una computadora personal.
- Permitir programación de alertas en los dispositivos detectados.
- Identificar el sistema operativo que las unidades ejecutan ya sea este Windows o Linux.
- Obtener datos de consumo de microprocesador, memoria, y variables que puedan considerarse relevantes durante el desarrollo de la aplicación para el buen funcionamiento de la red y generar estadísticas a partir de ellas.
- Detectar el estado de los puertos y servicios de red activos de un dispositivo.

1.7 LIMITACIONES

- El sistema será capaz de realizar sus operaciones en una Red Ethernet.
- Si existiera un dispositivo no administrable o no identificado por el sistema, se colocara una figura por defecto y no se mostrarán sus estadísticas pero se permitirá personalizar dicho dispositivo con características como las de símbolo y nombre.
- Las alertas estarán sujetas a las especificaciones del administrador, es decir no se programará ninguna alerta por el sistema mismo.
- Se detectarán redes basadas en protocolos TCP/IP.
- La aplicación solo obtendrá las estadísticas, puertos activos y servicios de red funcionales de los dispositivos especificados por el administrador.
- La aplicación es capaz de detectar dispositivos en diferentes sub-redes aun si estas se encuentran en VLANs o a través de enlaces WAN, siempre que estos posean una dirección IP dentro del rango valido inicial, exista conexión física y enrutamiento que permita conectividad entre el dispositivo que aloja la aplicación y el elemento remoto.
- La cantidad máxima de elementos a descubrir será 255, definida en el ultimo octeto de la mascara de red clase C introducida en el formulario inicial.

1.8 PROYECCIÓN SOCIAL

El desarrollo de la aplicación será de importancia para los administradores de redes pues brindara una herramienta de código libre eficiente.

Será beneficiado cualquier personal técnico que desee tener una aplicación disponible de forma gratuito que le facilite la tarea de administración de redes.

1.9 METODOLOGÍA DE LA INVESTIGACIÓN

La investigación a realizar es directa como también de tipo experimental. En una primera fase se realizo la recopilación de información, física y digital, centrando esta investigación en los diferentes protocolos tales como SNMP, ICMP, entre otros, los cuales fueron utilizados a lo largo de esta investigación y diseño del sistema de administración de red.

Como segunda fase se diseña una aplicación capaz de descubrir la topología de red, para poder ser administrada por medio de distintos aspectos básicos de un dispositivo, sea una computadora personal o cualquier otro elemento de comunicación de datos.

1.9.1 INVESTIGACIÓN BIBLIOGRÁFICA

Se ha realizado una investigación bibliográfica acerca de distintos componentes y herramientas de programación necesarias para la implementación de un monitor de red basado en distintos protocolos como SNMP, ICMP, NetBios y ARP. El material utilizado incluye manuales, trabajos de graduación, libros, currículum Cisco e información existente en Internet.

1.9.2 ASESORIA PROFESIONAL

Se crearon sesiones con profesionales en la materia, como responsables de administrar o monitorear una red, son ellos los que tienen mayor contacto con los distintos problemas que una red presenta, así mismo también pueden brindar mayor información acerca de los aspectos a vigilar en las redes empresariales.

1.9.3 INFORMACIÓN DISPONIBLE EN INTERNET

Una fuente de información conocida mundialmente que tiene una inmensa variedad de contenidos relacionados con este tema es la Internet, se convirtió en una de las principales técnicas de investigación para el presente trabajo, permitiéndonos así tener distintos puntos de vistas de universidades, personas, proyectos y hasta de aplicaciones ya realizadas, algunas implementadas y otras en calidad de prototipo.

1.9.4 ESTUDIO TÉCNICO DE APLICACIONES EXISTENTES

Existen aplicaciones similares a la que se pretende desarrollar, entre las más destacadas tenemos:

1.9.4.1 NETWORKVIEW V3.1

Es un software desarrollado por la empresa NetworkView situada en Suiza. Con este es posible descubrir rápidamente una nueva red, permite imprimir un mapa y finalmente, es posible revisar la disponibilidad de un nodo al instalar nuevos servidores, routers o cualquier otro dispositivo de la red. Sus especificaciones son descritas brevemente:

- **Rastreo de las direcciones.** Tres tipos de descubrimiento: escoja la dirección, rango de direcciones, subred completa. Posibilidad de seleccionar que puertos utilizar, ya sea de DNS, de SNMP, de WMI y/o de TCP.
- **Direcciones MAC.** NetworkView conseguirá la mayoría de las direcciones del MAC en la LAN usando la tabla del ARP, el SNMP, el NetBIOS y el WMI locales.

- **Tipo de Nodos.** Cada nodo de red se clasifica como uno del tipo y del icono incorporado como servidor, estación de trabajo, estación Unix, router, impresora. Actualmente son 23 tipos disponibles.
- **SNMP.** Una base de datos que contiene más de 20,500 dispositivos. Con capacidades para agregar o eliminar. Importación de los archivos de texto (formato delimitado .csv) si se tienen sus propias listas. Una lista de varios dispositivos y empresas populares está agregada en el ejecutable.
- **WMI.** Las consultas de WMI se desarrollan durante el descubrimiento. Esto permite un inventario completo de todos los nodos de Windows. 16 consultas se pueden definir con sus propios valores (procesadores, RAM, discos, etc.). Hasta 8 cuentas de WMI para permitir consultas WMI de multi domain/workgroup.
- **Descubrimiento de la ruta.** Un gráfico se muestra para cada nodo que actúa como router, mostrando las direcciones de las redes conectadas. Se puede agregar cualquier texto al lado de la información del IP (edificio, ciudad, el país.) para describir el destino.
- **Requisitos del Sistema.** Windows Server 2003, Windows XP, Windows NT 4.0 Server/Workstation, Windows 2000 Professional, Server or Advanced Server, (Windows ME, 98 Windows 95 no son soportados).
- **Costos y Licenciamiento.** El precio de una licencia personal es de US $79.00, con ella se puede instalar en varias computadoras de una misma red.

1.9.4.2 NETCRUNCH V3.0

Sistema desarrollado por la empresa AdRem Software, ofrece una herramienta para monitorear todos los dispositivos de red. AdRem NetCrunch ayuda a visualizar, monitorear, analizar y reportar de manera simple todos los dispositivos de una red multiplataforma desde una sola consola. Sus características principales se mencionan a continuación:

- Escaneo y visualización de la red.
- Monitoreo de red y análisis de datos.
- Alertas y solución de problemas.
- Reporte histórico y tendencias.

REQUISITOS DEL SISTEMA

Procesador Intel Pentium o compatible de 1GHz, 256 MB en memoria RAM, 40 MB para archivos de programa luego de instalación, 100 MB para almacenar datos de tendencia, Súper VGA (800 x 600 píxeles) High Color (16 bit), Internet Explorer 5.5 y sistema operativo Windows 2000 o Windows XP o Windows Server 2003.

COSTOS Y LICENCIAMIENTO

AdRem NetCrunch 3, en sus versiones Standard y Premium, se licencia basándose en la cantidad de estaciones de monitoreo desde las cuales NetCrunch operará. Esto significa que una única licencia permite al usuario instalar NetCrunch en una única estación de trabajo.

El costo de una licencia de NetCrunch Premium es de US $2,390 y en su versión Standard el costo es de US $1,690.

Una sola licencia le permite al usuario monitorear todos los dispositivos que posea en su red basada en IP. No se requerirán licencias adicionales cada vez que se incorporen dispositivos a la red luego de la instalación inicial.

1.9.4.3 FLUKE NETWORKS LAN MAPSHOT

Fluke Networks ha migrado su experiencia en instrumentos para pruebas de red al escritorio de Microsoft Windows y se ha asociado con Microsoft Visio para crear LAN MapShot. Esta solución permite una útil visión de las redes conmutadas al combinar el descubrimiento detallado con una excepcional facilidad de uso.

El personal de tecnologías de información (IT) podrá realizar las siguientes actividades mediante el uso de este software:

- Descubrir las redes conmutadas.
- Asignar conmutadores, servidores, enrutadores, impresoras, hosts e incluso concentradores.
- Observar la conectividad de dispositivos hasta el nivel de detalle de ranura o puerto.
- Obtener detalle desde el dominio de emisión hasta un puerto del conmutador único.

REQUISITOS DEL SISTEMA

Microsoft Visio 2000 English, Service Release 1 (SR1) Microsoft Windows® 2000, Windows NT® versión 4.0 (Service Pack 5 o superior), Windows® 98 o Windows® Millennium Edition, Pila TCP/IP de Microsoft, Microsoft WinSock2, Procesador Pentium a 200 MHz, IBM o compatible, 64 MB de RAM, 150 MB de memoria virtual, 100 MB de espacio libre en disco duro. Esta diseñado para redes conmutadas Ethernet TCP/IP a velocidades de 10 MB, 100 MB o 1 GB; puede detectar hasta 50 conmutadores (máximo por dominio de difusión) y 2000 nodos (máximo por dominio de difusión).

COSTOS Y LICENCIAMIENTO

El costo por licencia es de $499.00. Una sola licencia le permite al usuario monitorear todos los dispositivos que posea en su red basada en IP. No se requerirán licencias adicionales al incorporar dispositivos a la red luego de la instalación inicial.

1.9.4.4 TRABAJOS DE GRADUACIÓN

"HERRAMIENTAS DE MONITOREO DE RED, CASO PRÁCTICO: IMPLEMENTACIÓN Y CONFIGURACIÓN EN EL CENTRO DE COMPUTO DE LA UNIVERSIDAD DON BOSCO Y ACADEMIA CISCO"

Desarrollado en el año 2002 por Hugo Alberto Orellana Guevara, Marvin Alexis Peña Pelitez y Amilcar Alexander Rivas Morales para optar al grado de Ingeniero en Ciencias de la Computación en la Universidad Don Bosco.

El objetivo general del trabajo era implementar un sistema de monitoreo y diagnóstico de fallas de red que sirva como recurso auxiliar en el proceso enseñanza – aprendizaje en la academia cisco y en las asignaturas que impliquen el estudio de redes en la Universidad Don Bosco, además de proveer una herramienta de monitoreo de red al Centro de Cómputo de la Universidad Don Bosco.

El trabajo consistió en una investigación sobre herramientas disponibles bajo la plataforma Linux que fueran útiles para el monitoreo de red, para ello inicialmente se desarrolló una investigación de diversos elementos que eran necesarios para lograr una mejor compresión del tema tales como conceptos

de dispositivos de networking, protocolos, topologías de red, modelo OSI, protocolos TCP/IP, GNU, Administración de redes, monitoreo de red, protocolo SNMP para finalmente concluir con la implementación de herramientas ya existentes en el entorno Linux, estas son: Ntop, NetSaint y MRTG y mediante una interfaz Web asociarlas a todas para que juntas formaran al Monitor de Red UDB.

"SISTEMA DE MONITOREO DE REDES DE DATOS BASADO EN EL PROTOCOLO SNMP"

Desarrollado en el año 2001 por Herbert Edgardo Ascencio Hurtado, Carlos Alfredo Bolaños Guerrero y Rafael Adalberto Cobos Meléndez para optar al grado de Ingeniero Electrónico.

El objetivo del trabajo era desarrollar un sistema que permita establecer procedimientos de monitoreo sobre elementos específicos ubicados en una red de comunicación de datos, por medio del protocolo SNMP.

Se realizó una amplia investigación sobre elementos de networking, protocolos de red, modelo OSI, modelo TCP/IP, gestión de redes, protocolo SNMP y posteriormente se procedió a la implementación del sistema haciendo uso de Linux Redhat 7.0, Perl, Postgrey SQL y apache Web Server.

La herramienta implementada permitió la supervisión de la operación de una red de datos, así como también el monitoreo de los elementos de la red con lo cual era posible detectar fallas y así determinar que pasos se han de seguir para corregirlas.

La herramienta implementada permitió la supervisión de la operación de una red de datos, así como también el monitoreo de los elementos de la red con lo cual era posible detectar fallas y así determinar que pasos se han de seguir para corregirlas.

2.1. MARCO HISTÓRICO

La historia de networking en la informática es compleja. Participaron en ella personas de todo el mundo a lo largo de los últimos 35 años.

En la década de 1940, las computadoras eran enormes dispositivos electromecánicos propensos a fallas, no fue sino hasta 1947 que disminuyeron su tamaño gracias a la invención del transistor semiconductor. En la década de 1950 las computadoras mainframe, que funcionaban con programas en tarjetas perforadas, comenzaron a ser utilizadas por las grandes instituciones corporativas. A fines de esta década, se creó el circuito integrado, que combinaba muchos y, en la actualidad, millones de transistores en un pequeño semiconductor. Para la década de 1960, los mainframes con terminales eran comunes.

Hacia fines de la década de 1960 y durante la década de 1970, se inventaron computadoras más pequeñas, denominadas mini computadoras. En 1977, Apple Computer Company presentó la microcomputadora, también conocida como computadora personal. En 1981 IBM presentó su primera computadora personal.

A mediados de la década de 1980 los usuarios con computadoras autónomas comenzaron a usar módems para conectarse con otras y compartir archivos. Esta práctica se expandió a través del uso de computadoras que funcionaban como punto central de comunicación en una conexión de acceso telefónico, los usuarios se conectaban a ellas depositaban y levantaban mensajes, además de cargar y descargar archivos.

La desventaja de este tipo de sistema era que había poca comunicación directa pues se reducía únicamente a quienes conocían dicha computadora. Por otra parte existía la necesidad de un módem por cada conexión al computador del tablero de boletín. Si por ejemplo cinco personas se conectaban simultáneamente, hacían falta cinco módems conectados a cinco

líneas telefónicas diferentes. A medida que crecía el número de usuarios interesados, el sistema no fue capaz de soportar la demanda.

A partir de la década de 1960 y durante las décadas de 1970, 1980 y 1990, el Departamento de Defensa de Estados Unidos (DoD) desarrolló redes de área amplia (WAN) de gran extensión y alta confiabilidad, para uso militar y científico.

Esta tecnología era diferente de la comunicación punto-a-punto usada por los tableros de boletín. Permitía el internetworking de varias computadoras mediante diferentes rutas. La red en sí determinaba la forma de transferir datos de una estación a otra. En lugar de poder comunicarse con una sola computadora a la vez, podía acceder a varias de estas mediante la misma conexión. La WAN del DoD finalmente se convirtió en la Internet.

Las redes de datos se desarrollaron como consecuencia de aplicaciones comerciales diseñadas para microcomputadoras. Se tornó evidente que el uso de disquetes para compartir datos no era un método eficaz ni económico para desarrollar la actividad empresarial.

La red a pie creaba copias múltiples de los datos. Cada vez que se modificaba un archivo, debía compartirse nuevamente con el resto de usuarios y al compartirlo, se perdía alguno de los dos conjuntos de modificaciones. Las empresas necesitaban una solución que resolviera con éxito los tres problemas siguientes:

- Duplicación de equipos informáticos y de otros recursos
- Comunicación eficiente
- Configuración y administración una red

Las empresas se dieron cuenta de que la tecnología de networking podía aumentar la productividad y disminuir gastos. Las redes se extendieron casi con la misma rapidez con la que se lanzaban nuevas tecnologías y

productos de red. A principios de la década de 1980 networking se expandió enormemente, aun cuando en sus inicios su desarrollo fue desorganizado.

A mediados de la década de 1980, las tecnologías de red que habían emergido se habían creado con implementaciones de hardware y software distintas.

Cada empresa dedicada a crear hardware y software para redes utilizaba sus propios estándares corporativos. Por tanto, muchas de las tecnologías no eran compatibles entre sí.

Se volvió cada vez más difícil la comunicación entre redes que utilizaban distintas especificaciones. Esto a menudo obligaba a deshacerse de equipos de la antigua red al implementar equipos de red nuevos.

Una de las primeras soluciones al problema anterior fue la creación de los estándares de Red de área local (LAN). Como los estándares LAN proporcionaban un conjunto abierto de pautas para la creación de hardware y software de red, se podrían compatibilizar los equipos provenientes de diferentes empresas. Esto permitía la estabilidad en la implementación de las LAN, con el tiempo incluso estas no eran suficientes.

Lo que se necesitaba era una forma en que la información se pudiera transferir rápidamente y con eficiencia, no solamente dentro de una misma empresa sino también de una empresa a otra. La solución fue la creación de redes de área metropolitana (MAN) y redes de área amplia (WAN). Como las WAN podían conectar redes de usuarios dentro de áreas geográficas extensas, permitieron que las empresas se comunicaran entre sí a través de grandes distancias.

Las empresas salvadoreñas han implementado poco a poco redes informáticas que les ha permitido compartir información y recursos distribuidos en distintas sedes.

CAPITULO II
MARCO TEORICO

2.2 FUNDAMENTOS DE REDES

2.2.1 CONCEPTOS GENERALES SOBRE REDES

Los equipos que se conectan de forma directa a un segmento de red se denominan dispositivos. Estos se clasifican en dos grandes grupos.

El primer grupo está compuesto por los dispositivos de usuario final, los cuales incluyen las computadoras, impresoras, escáneres, y demás dispositivos que brindan servicios directamente al usuario.

El segundo grupo está formado por los dispositivos de red estos son todos aquellos que conectan entre sí a los dispositivos de usuario final, posibilitando su intercomunicación.

Los dispositivos de usuario final que conectan a los usuarios con la red se conocen con el nombre de hosts; permiten a los usuarios compartir, crear y obtener información.

Los host pueden existir sin una red, pero sin esta sus capacidades se ven sumamente limitadas. Los host están físicamente conectados con los medios de red mediante una tarjeta de interfaz de red (NIC). Utilizan esta conexión para realizar las tareas de envío de correo electrónico, impresión de documentos, escaneado de imágenes o acceso a bases de datos.

No existen símbolos estandarizados para los dispositivos de usuario final en la industria de networking. Son similares en apariencia a los dispositivos reales para permitir su fácil identificación.

2.2.1.1 TOPOLOGÍA DE LA RED

La topología de red define la estructura de una red. Una parte de la definición topológica es la topología física, que es la disposición real de los cables o medios. Existe también la topología lógica, que define la forma en que los hosts acceden a los medios para enviar datos.

Las topologías físicas que se utilizan con mayor frecuencia se presentan a continuación:

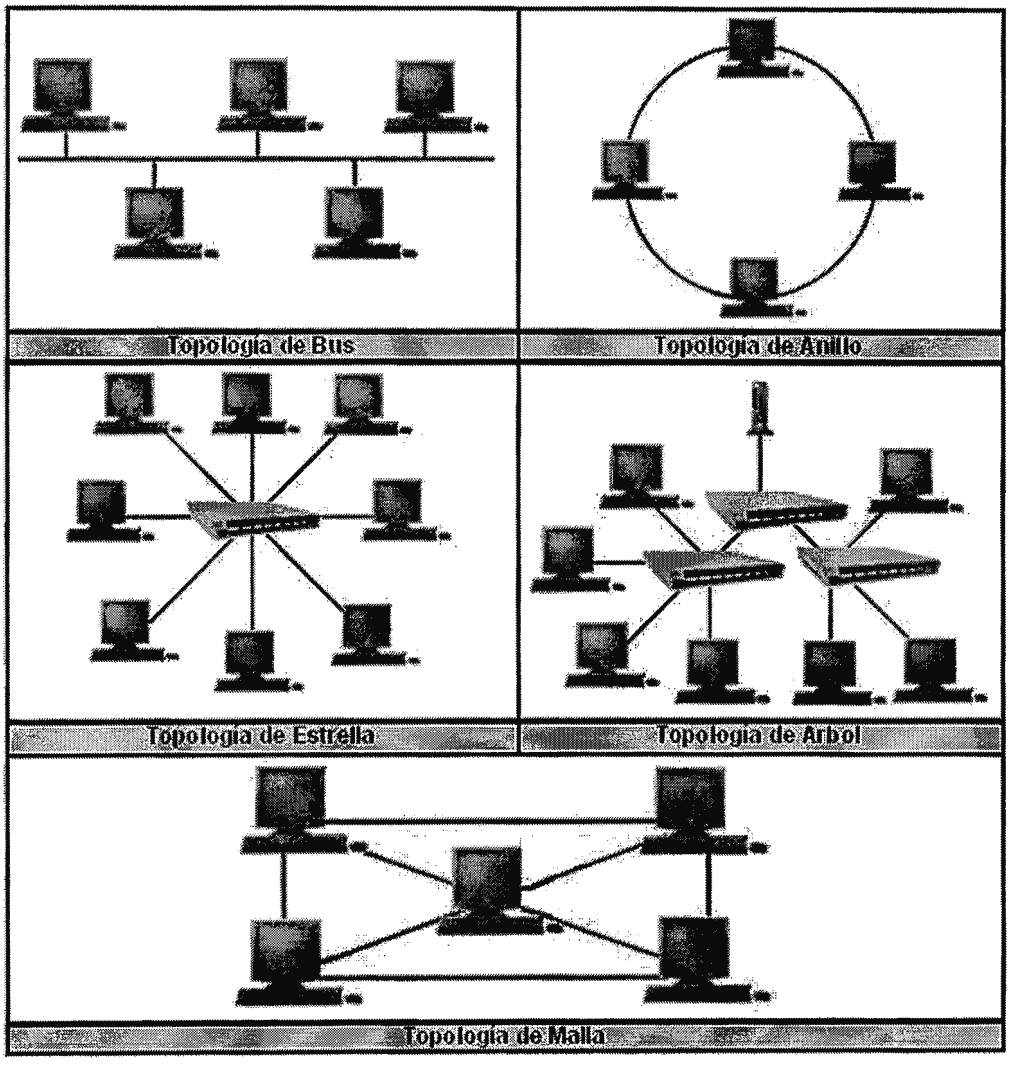


Fig. 1 – Topologías de Red

2.2.2 MODELOS DE REFERENCIA

El desarrollo de redes sucedió con desorden en muchos sentidos. De la misma forma en que las personas que no hablan un mismo idioma tienen dificultades para comunicarse, las redes que utilizaban diferentes especificaciones e implementaciones tenían dificultades para intercambiar información. El mismo problema surgía con las empresas que desarrollaban tecnologías de networking privadas o propietarias (una sola empresa o un pequeño grupo de empresas controlan todo uso de la tecnología).

Para enfrentar el problema de incompatibilidad de redes, la Organización Internacional de Normalización (ISO) investigó modelos de networking como la red de Digital Equipment Corporation (DECnet), la Arquitectura de Sistemas de Red (SNA), el Sistema Abierto de Interconexión (OSI) y TCP/IP a fin de encontrar un conjunto de reglas aplicables de forma general a todas las redes.

2.2.2.1 MODELO OSI

En base a esta investigación, la ISO desarrolló un modelo de red que ayuda a los fabricantes a crear redes que sean compatibles con otras.

El modelo OSI es un marco que se puede utilizar para comprender cómo viaja la información de un dispositivo a otro a través de varias capas para recorrer una red, aun cuando el remitente y el destinatario poseen diferentes tipos de medios de red.

Se basa en siete capas: aplicación, presentación, sesión, transporte, red, enlace de datos y física; cada una de estas ilustra una función de red específica. La división de la red en siete capas permite principalmente obtener las siguientes ventajas:

- Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos por diferentes fabricantes.
- Divide la comunicación de red en partes más pequeñas para simplificar el aprendizaje.

Cada una de las capas del modelo OSI se describe brevemente en la tabla 1 que se muestra a continuación:

Nivel	Nombre	Función
7	APLICACIÓN	Se entiende directamente con el usuario final, al proporcionarle el servicio de información distribuida para soportar las aplicaciones y administrar las comunicaciones por parte de la capa de presentación
6	PRESENTACIÓN	Permite a la capa de aplicación interpretar el significado de la información que se intercambia. Esta realiza las conversiones de formato mediante las cuales se logra la comunicación de dispositivos
5	SESIÓN	Administra el diálogo entre las dos aplicaciones en cooperación mediante el suministro de los servicios que se necesitan para establecer la comunicación, flujo de datos y conclusión de la conexión
4	TRANSPORTE	Representa el corazón de la jerarquía de los protocolos que permite realizar el transporte de los datos en forma segura y económica
3	RED	Proporciona los medios para establecer, mantener y concluir las conexiones conmutadas entre los sistemas del usuario final. Por lo tanto, la capa de red es la más baja, que se ocupa de la transmisión de extremo a extremo
2	ENLACE	Asegura confiabilidad del medio de transmisión, ya que realiza la verificación de errores, retransmisión, control fuera del flujo y la secuenciación de la capacidades que se utilizan en la capa de red
1	FISICO	Se encarga de las características eléctricas, mecánicas, funcionales y de procedimiento que se requieren para mover los bits de datos entre cada extremo del enlace de la comunicación

Tabla 1 – Niveles del modelo OSI

2.2.2.2 MODELO TCP/IP

Otro modelo de referencia muy importante es el diseñado por El Departamento de Defensa de EE.UU. (DoD), quien presento el modelo TCP/IP pues necesitaba una red que pudiera sobrevivir ante cualquier circunstancia; se ha convertido en el estándar en el que se basa la Internet.

El modelo TCP/IP tiene cuatro capas: la capa de aplicación, la capa de transporte, la capa de Internet y la capa de acceso de red. Es importante observar que algunas de las capas del modelo TCP/IP poseen el mismo nombre que las capas del modelo OSI, tal como se mostrará en la tabla 2. Sin embargo desempeñan diferentes funciones en cada modelo.

Cada dispositivo conectado a una red TCP/IP debe recibir un identificador exclusivo o una dirección IP (dirección lógica) así como también todos los equipos de red cuentan con una dirección física exclusiva, conocida como dirección MAC.

Capa	Descripción
APLICACIÓN	Se corresponde con los niveles OSI de aplicación, presentación y sesión. Aquí se incluyen protocolos destinados a proporcionar servicios, tales como correo electrónico (SMTP), transferencia de ficheros (FTP), conexión remota (TELNET) y otros más recientes como el protocolo HTTP (Hypertext Transfer Protocol)
TRANSPORTE	Coincide con el nivel de transporte del modelo OSI. Los protocolos de este nivel, tales como TCP y UDP, se encargan de manejar los datos y proporcionar la fiabilidad necesaria en el transporte de los mismos
INTERNET	Es el nivel de red del modelo OSI. Incluye al protocolo IP, que se encarga de enviar los paquetes de información a sus destinos correspondientes. Es utilizado con esta finalidad por los protocolos del nivel de transporte
ACCESO DE RED	Los niveles OSI correspondientes son el de enlace y el nivel físico. Los protocolos que pertenecen a este nivel son los encargados de la transmisión a través del medio físico al que se encuentra conectado cada host, como

Tabla 2 – Capas del modelo TCP/IP

2.3 MARCO CONCEPTUAL

2.3.1 ADMINISTRACIÓN DE RED

La administración de red se encarga de mantener la red operativa, eficiente, segura, constantemente monitoreada y con una planeación adecuada y propiamente documentada. Los objetivos que se buscan en una administración de red eficiente son:

- Mejorar la continuidad en la operación de la red con mecanismos adecuados de control y monitoreo, de resolución de problemas y de suministro de recursos.
- Hacer uso eficiente de los recursos de la red, como por ejemplo, el ancho de banda.
- Proteger la red contra partes no autorizadas, haciendo imposible que personas ajenas puedan acceder a la información que circula en ella.
- Controlar cambios y actualizaciones en la red de modo que ocasionen el menor número de interrupciones posibles en el servicio a los usuarios.

Es importante recordar que para la obtención de los objetivos mencionados las redes deben soportar los diferentes factores, como ejemplo podemos mencionar:

- Mezclas de diversas señales (voz, datos, imagen)
- Interconexión de diferentes tipos de redes (LAN, WAN, MAN)
- Arquitectura de red (Ethernet, Fast Ethernet, Token Ring)
- Protocolos de comunicación, (TCP/IP, SPX/IPX, SNA)
- Diferentes sistemas operativos

Los sistemas de administración de red operan bajo los siguientes pasos una serie de pasos básicos:

1. Colección de información acerca del estado de la red y componentes del sistema. La información recolectada de los recursos incluye eventos, atributos y acciones operativas.
2. Transformación de la información para presentarla en formatos apropiados.
3. Transportación de la información del equipo monitoreado al centro de control
4. Almacenamiento de los datos obtenidos.
5. Análisis de parámetros para obtener determinar el desempeño de la red.
6. Determinar el tipo de respuesta a las diferentes fallas detectadas.

La administración de red utiliza diferentes elementos para la obtención de los datos acerca de ella:

- **Objetos.** son los elementos de más bajo nivel y constituyen los aparatos administrados.

- **Agentes.** un programa o conjunto de programas que colecciona información de administración del sistema en un nodo o elemento de la red. El agente genera la administración apropiada mediante la transmisión de información de la red acerca de:

    - Identificación del nodo
    - Características del nodo
    - Datos de diagnóstico
    - Notificación de fallas

- **Administrador del sistema.** Es un conjunto de programas ubicados en un punto central al cual se dirigen los mensajes que requieren acción o que contienen información solicitada por el administrador al agente.

La utilización de herramientas adecuadas permite realizar de forma centralizada la administración de múltiples redes de gran tamaño compuestas de cientos de servidores, puestos de trabajo y periféricos.

Normalmente las herramientas de administración de red forman un conjunto muy diverso de aplicaciones provenientes de, por ejemplo, sistema de gestión de red, herramientas de fabricantes de los dispositivos, herramientas autónomas e independientes. Además muchas de estas herramientas suelen tener interfaces de programación de aplicaciones, API.

Hoy en día estas herramientas corren sobre diferentes sistemas operativos y suelen tener en común la característica de disponer de interfaces gráficas basadas en la interacción de ventanas

La característica fundamental de los sistemas de administración de red modernos es la de ser sistemas abiertos, capaces de manejar varios protocolos y operar con varias arquitecturas de red.

2.3.2 OPERACIONES DE LA ADMINISTRACION DE RED

Las principales operaciones de un sistema de administración de red son las siguientes:

- **Administración de fallas.** Consiste en el manejo de condiciones de error en todos los componentes de la red, en las siguientes fases

- **Control de fallas.** Monitoreo continuo de todos los elementos de la red.

- **Administración de cambios.** Comprende la planeación y programación de eventos e instalación de nuevos elementos a la red.

- **Administración del comportamiento.** Asegurar el funcionamiento óptimo de la red; estudia por ejemplo el número de paquetes transmitidos en un periodo determinado, tiempos de respuesta a diferentes pericones y disponibilidad de la red

- **Servicios de contabilidad.** Datos concernientes al cargo por uso de la red. Proporcionados datos como el tiempo de conexión, mensajes transmitidos o recibidos y razón por la que terminó la conexión.

- **Control de Inventarios.** Registro de los componentes que de la red y de los movimientos y cambios que se lleven a cabo.

- **Seguridad.** Se debe proveer mecanismos de seguridad apropiados para autentificación de usuarios, autorización de acceso a los recursos, y confidencialidad en el medio de comunicación y en los medios de almacenamiento; se recomiendan medios de criptografía, tanto simétrica como asimétrica.

2.3.3 FUNCIONES DE ADMINISTRACIÓN DEFINIDAS POR OSI

OSI define cinco funciones básicas para lograr el desarrollo de una administración de red efectiva, estas son descritas a continuación:

- **Configuración.** Comprende funciones de monitoreo y mantenimiento del estado de la red.

- **Fallas.** Incluye la detección, aislamiento y corrección de fallas en la red.

- **Contabilidad.** Permite el establecimiento de cargos a usuarios por uso de los recursos de la red.

- **Comportamiento.** Mantiene el comportamiento de la red en niveles aceptables.

- **Seguridad.** Provee mecanismos para autorización, control de acceso, confidencialidad y manejo de claves

El modelo OSI incluye cinco componentes respecto a la administración de redes:

- **CMIS (Common Management Information Services).** Servicio para recolección y transmisión de información de administración de red a las entidades de red que lo soliciten.

- **CMIP (Common Management Information Protocol).** Protocolo de OSI que soporta a CMIS, proporciona un servicio de petición/respuesta que posibilita intercambiar información de administración de red entre aplicaciones.

- **SMIS (Specific Management Information Services).** Define servicios específicos de administración de red respecto a instalación, configuración, fallas, contabilidad, comportamiento y seguridad.

- **MIB (Management Information Base).** Define un modelo conceptual de la información requerida para tomar decisiones de administración de red. La información en el MIB incluye: número de paquetes transmitidos, número de conexiones intentadas, datos de contabilidad, entre otras.

- **Servicios de Directorio.** Define las funciones necesarias para administrar la información nombrada, como asociación de nombres lógicos y direcciones físicas.

2.3.4 PROTOCOLOS DE RED

Las reglas a seguir para posibilitar la comunicación de un host a otro a través de una red se conocen como protocolos de comunicación. Son convenciones que rigen un aspecto particular de cómo los dispositivos de una red se comunican entre sí; determinan el formato, sincronización, secuenciación y control de errores en la comunicación de datos. Sin protocolos, las computadoras no pueden armar o reconstruir el formato original del flujo de bits entrantes desde otra computadora.

Los protocolos controlan todos los aspectos de la comunicación de datos, que incluye lo siguiente:

- Cómo se construye la red física
- Cómo las computadoras se conectan a la red
- Cómo se les da formato a los datos para lograr una transmisión efectiva
- Cómo se envían los datos
- Cómo se manejan los errores

Estas normas de red son creadas y administradas por una serie de organizaciones y comités. Entre ellos se incluyen el Instituto de Ingeniería Eléctrica y Electrónica (IEEE), el Instituto Nacional Americano de Normalización (ANSI), la Asociación de la Industria de las Telecomunicaciones (TIA), la Asociación de Industrias Electrónicas (EIA) y la Unión Internacional de Telecomunicaciones (UIT).

Para el desarrollo del presente proyecto se hace uso esencialmente de cuatro protocolos:

- **SNMP**, Simple Network Managment Protocol
- **ICMP**, Internet Control Message Protocol
- **ARP**, Address Resolution Protocol
- **NetBEUI/NetBIOS**, NetBIOS Extended User Interface /Network Basic Input/Output

Cada uno de los protocolos mencionados anteriormente se describirá de manera detallada en el desarrollo del presente documento

2.3.5 SNMP - SIMPLE NETWORK MANAGMENT PROTOCOL

2.3.5.1 GENERALIDADES DEL PROTOCOLO SNMP

SNMP, *Simple Network Management Protocol*, es un protocolo que facilita el intercambio de información de la gerencia entre los dispositivos de la red. Es parte habitación del protocolo del Transmission Control Protocol/del Internet Protocol, TCP/IP. Añadió las mejoras de muchos años de experiencia con SGMP, Simple Gateway Monitoring Protocol, y le permitió trabajar con los objetos definidos en la MIB, Management Information Base, con la representación del SIM, Structure and Identification of Management Information.

El RFC 1157 define Network Management Station, NMS, como una estación que ejecuta aplicaciones de gestión de red (Network Management application, NMA) que monitorean y controlan elementos de red (Network element, NE) como hosts, pasarelas y servidores de terminales. Estos elementos usan un agente de gestión (Managment Agent, MA), para realizar estas funciones. El uso de SNMP para la comunicación de información entre las NMS y los MA se describe a continuación.

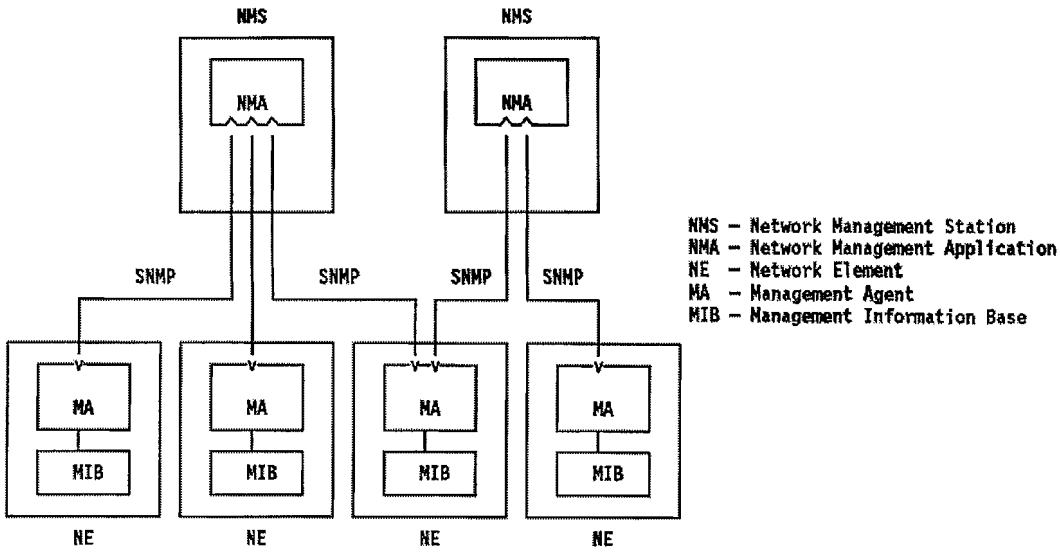


Fig. 2 - Componentes de SNMP

Todas las funciones de los MA son sólo alteraciones (set) o consultas (get) de variables, limitando así el número de funciones esenciales a dos y simplificando el protocolo.

En la comunicación NE-NMS, se utilizan un número limitado de mensajes no solicitados (traps) para informar de eventos asíncronos. Del mismo modo, en un intento de mantener la sencillez, el intercambio de información requiere sólo un servicio de datagramas y cada mensaje se envía en un único datagrama. Esto significa que SNMP es adecuado para una gran variedad de protocolos de transporte. El RFC 1157 especifica el intercambio de mensajes vía UDP, aunque es posible emplear otros.

Las entidades que residen en las NMS y los elementos de red que se comunican con otros a través de SNMP se denominan: *entidades de aplicación de SNMP*. Los procesos que las implementan son llamados: *entidades de protocolo*.

Un agente SNMP con un conjunto arbitrario de entidades es una comunidad SNMP, en la que cada entidad se nombra con un grupo de bytes que debe ser unívoca para esa comunidad.

Un mensaje de SNMP consiste en un identificador de la versión de este protocolo, nombre de la comunidad SNMP y un PDU (Protocol Data Unit).

Toda implementación del protocolo SNMP debe soportar las cinco PDU siguientes:

PDU	Descripción
GetRequest	Recuperar los valores de un objeto de la MIB
GetNextRequest	Realiza una petición del objeto siguiente a uno dado en la MIB del agente
SetRequest	Alterar los valores de un objeto del MIB
GetResponse	Respuesta a los valores solicitados por los tipos de Get y Set
Trap	Informe de sucesos inusuales predefinidos como inicialización, reinicio o fallo en el enlace del agente.

Tabla 3 – PDU de SNMP en V1, V2, V3

Los formatos de los mensajes del protocolo SNMP son descritos en la siguiente figura:

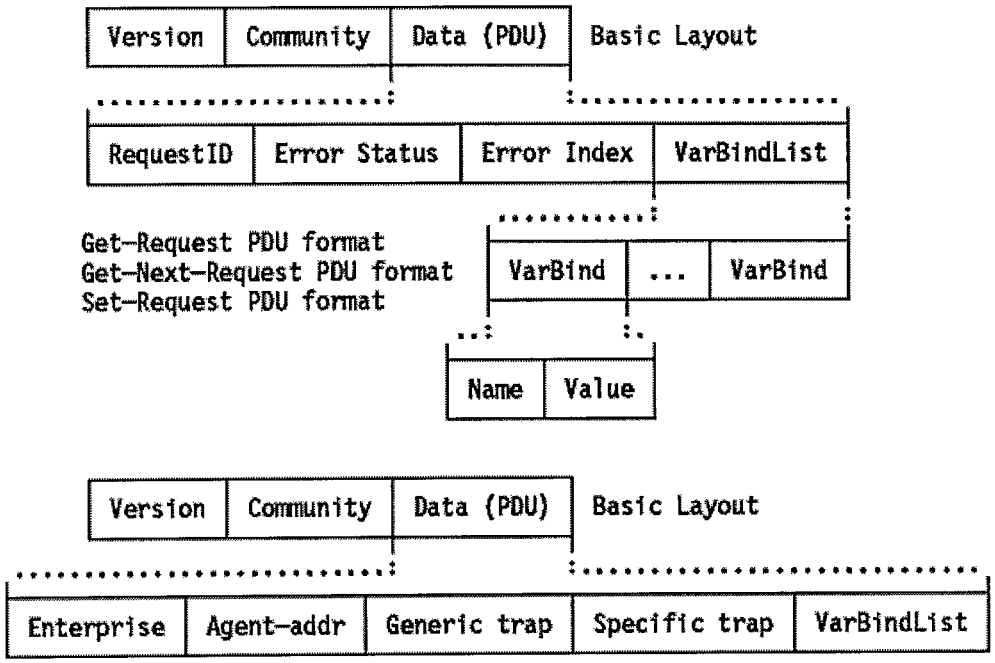


Fig. 3 - Formato de mensaje SNMP - Formato de las PDU Request, Set y Trap.

2.3.5.2 ELEMENTOS DEL PROTOCOLO SNMP

2.3.5.2.1 ESTACIÓN DE GESTIÓN (NMS)

Una estación de administración de red es una máquina que ejecuta el protocolo y aplicaciones de administración de red. Si el protocolo es el encargado de proporcionar los mecanismos de administración, entonces las aplicaciones determinan la política a utilizar para la administración.

El añadir administración a una red debería tener un impacto mínimo en los nodos; en consecuencia la carga se desplaza a las estaciones. Sin embargo podríamos pensar que la estación de administración es más potente que un nodo, así que ¿cuánta potencia es necesaria entonces? La experiencia muestra que la mayoría de las estaciones de trabajo pueden proporcionar los recursos necesarios para soportar una buena estación de administración.

Debe considerarse que a medida aumenta el número de nodos administrables en una red, se favorece desplazar la carga hacia la estación de administración.

La estación de gestión cumple el papel de una interfaz entre el gestor humano y la aplicación de gestión de red, debe incluir:

- Interfaz para monitorear y controlar la red.
- Aplicaciones de gestión para análisis de datos, recuperación de fallos, entre otros.
- Capacidad de traducir los requerimientos del gestor en órdenes concretas de monitoreo y control de los elementos remotos de la red.
- Base de datos de información extraída de las MIB de todas las entidades gestionadas en la red SNMP.

Al mismo tiempo las estaciones de gestión tienen, principalmente, las funciones descritas a continuación:

- Recuperar valores de objetos en estaciones de red mediante agentes (Get).
- Cambiar valores de objetos en estaciones de red mediante agentes (Set).
- Enviar requerimientos a los agentes.
- Recibir respuestas y notificaciones (Trap) de los agentes.

2.3.5.2.2 NODO ADMINISTRABLE

Un nodo administrable es un dispositivo tal que puede clasificarse en una de las tres siguientes categorías:

- Un Host, como una estación de trabajo, mainframe, o impresora.
- Un sistema de enrutamiento.
- Un dispositivo de acceso al medio; como un repetidor o un puente.

Estas tres categorías coinciden en que clasifican a algún tipo de dispositivo con alguna capacidad de trabajo en red. Las dos primeras son independientes del medio, mientras que la principal característica de los dispositivos de la tercera clase es la dependencia del medio.

2.3.5.2.2.1 AXIOMA FUNDAMENTAL

"El impacto de añadir una administración de red a un nodo administrable debe ser mínima, reflejando un común denominador más bajo."

Lo anterior indica que los sistemas de administración de red eficientes deben conocer la diversidad de dispositivos existentes y proporcionar un entorno apropiado.

Este axioma se debe a las grandes diferencias entre los distintos nodos administrables que existen.

2.3.5.2.2.2 CARACTERÍSTICAS DE LOS NODOS ADMINISTRABLES

Podemos considerar que cada nodo administrable está formado por tres componentes:

- Funciones de usuario.
- Protocolo de administración, que permite monitorear y controlar el nodo administrable.
- Instrucciones de administración, que interactúan con la implementación del nodo administrable para permitir el monitoreo y control.

La interacción entre estos componentes es sencilla: Las instrucciones actúan como una clase de pegamento entre las funciones de usuario y el protocolo de administración. Esto se debe a un mecanismo de comunicación interno en el que las estructuras de datos de las funciones de usuario deben ser accesibles y modificables a petición del protocolo de administración.

2.3.5.3 MODELO ADMINISTRATIVO

Actualmente los intercambios de información son insuficientes para la administración de los nodos. El protocolo de administración trabaja en el entorno del modelo administrativo, que mantiene políticas de autorización y autentificación.

Las políticas mencionadas con anterioridad permiten determinar al nodo como se está administrando, de modo que sólo los procesos de aplicaciones autorizadas realicen las funciones de administración.

2.3.5.3.1 AGENTE

Son implementaciones de software que proporcionan acceso a los datos de gestión de un dispositivo en particular tales como hosts, puentes, routers, switches o hubs.

El protocolo de gestión SNMP soporta dos tipos de transacciones POLL y TRAPS, las cuales se describen a continuación:

- **Petición (POLL) por parte del gestor, y respuesta por parte de agente**

  Este término se refiere a la técnica general de hacer que quien desea la información la pida por si mismo. Un ejemplo común de la "vida real" puede ser la revisión diaria de nuestro correo electrónico; cada día usted comprueba si ha recibido algún nuevo mensaje.

- **Notificaciones no solicitadas (TRAPS) desde el agente al gestor**

  Este término indica que se cuenta con un dispositivo que posee la información que otros necesitan para poder enviarla. En SNMP, esto se representa en un agente que envía información a las NMS que estas no han solicitado. Éste es el modelo usado por el más famoso de los dispositivos interruptores, el teléfono.

2.3.5.3.2 BASE DE INFORMACIÓN DE GESTIÓN (MIB)

La MIB define los objetos que pueden ser gestionados para cada capa en el protocolo TCP/IP. Hay dos versiones, MIB-I y MIB-II. La primera fue definida en el RFC 1156, y está clasificado ahora como protocolo histórico con status no recomendado.

Group	Objects for	#
system	basic system information	7
interfaces	network attachments	23
at	address translation	3
ip	internet protocol	38
icmp	internal control message protocol statistics	26
tcp	transmission control protocol	19
udp	user datagram protocol	7
egp	exterior gateway protocol	18
transmiss.	transmission. Media-specific	0
snmp	snmp applications entities	30

#: Numero de objetos en un grupo

Fig. 4 – Objetos de MIB para ciertos grupos de gestión

2.3.5.3.2.1 DEFINICIÓN DE GRUPO PARA MIB – II

Cada nodo gestionado soporta sólo los grupos apropiados. Por ejemplo, si no existe una pasarela, el grupo EGP no tiene por qué estar incluido. Pero si un grupo es apropiado, todos los objetos en ese grupo deben estar soportados.

La lista de objetos gestionados definidos deriva de aquellos elementos considerados esenciales. Este enfoque que consistente en tomar sólo los objetos esenciales no es restrictivo, ya que el SMI proporciona mecanismos de extensibilidad tales como la definición de una nueva versión de MIB o de objetos privados o no estandarizados.

A continuación se muestran algunos ejemplos de objetos de cada grupo de los cuales se hará uso en la presente aplicación [1].

- **Grupo de sistema**

Objetos generales de importancia para la mayoría de los dispositivos. Por ejemplo, una descripción general del dispositivo es un objeto en este grupo, al igual que el identificador del objeto.

Objeto	Descripción
sysDescr	Descripción completa del sistema (versión, HW, OS).
sysObjectID	Identificación que da el distribuidor al objeto.
sysUpTime	Tiempo desde la última reinicialización.
sysContact	Nombre de la persona que hace de contacto.
sysServices	Servicios que ofrece el dispositivo.

Tabla 4 – Miembros del grupo de sistema

- **Grupo de interfaces**

Objetos relacionados a las interfaces IP entre un dispositivo y la red interna; generalmente un host tiene una sola interfaz mientras que dispositivos administrables (routers o switches) tiene dos o más.

Objeto	Descripción
ifIndex	Número de interfaz.
ifDescr	Descripción de la interfaz.
ifType	Tipo de la interfaz.
ifMtu	Tamaño máximo del datagrama IP.
ifAdminisStatus	Status de la interfaz.
ifLastChange	Tiempo que lleva la interfaz en el estado actual.
ifINErrors	Número de paquetes recibidos que contenían errores.
ifOutDiscards	Número de paquetes enviados y desechados.

Tabla 5 – Miembros del grupo de Interfaces

[1] Para una mayor referencia, la lista completa se define en el RFC 1213.

- **Grupo IP**

Son los objetos relacionados a la capa del IP del dispositivo en su totalidad, algunos de los primordiales son:

Objeto	Descripción
ipForwarding	Indicación de si la entidad es una pasarela IP
ipInHdrErrors	Número de datagramas de entrada desechados debido a errores en sus cabeceras IP
ipInAddrErrors	Número de datagramas de entrada desechados debido a errores en sus direcciones IP
ipInUnknownProtos	Número de datagramas de entrada desechados debido a protocolos desconocidos o no soportados
ipReasmOKs	Número de datagramas IP reensamblados con éxito
ipRouteMask	Máscara de subred para el encaminamiento

Tabla 6 – Miembros del grupo de IP

- **Grupo ICMP**

Los objetos relacionados con la operación del protocolo ICMP son descritos en la siguiente tabla:

Objeto	Descripción
icmpInMsgs	Número de mensajes ICMP recibidos
icmpInDestUnreachs	Número de mensajes ICMP "destino inalcanzable" (destination unreachable) recibidos
icmpInTimeExcds	Número de mensajes ICMP "time exceeded" (tiempo excedido) recibidos
icmpInSrcQuenchs	Número de mensajes ICMP "source quench (desbordamiento del emisor) recibidos
icmpOutErrors	Número de mensajes ICMP no enviados debido a problemas en ICMP

Tabla 7 – Miembros del grupo del protocolo ICMP

- **Grupo TCP**

A continuación se describen algunos de los objetos relacionados con las operaciones del protocolo TCP:

Objeto	Descripción
tcpRtoAlgorithm	Algoritmo que determina el timeout para retransmitir octetos para los que no se ha recibido reconocimiento
tcpMaxConn	Límite en el número de conexiones TCP que puede soportar la entidad
tcpActiveOpens	Número de veces que las conexiones TCP han efectuado una transición directa del estado SYN-SENT al estado CLOSED
tcpInSegs	Número de segmentos recibidos, incluyendo aquellos con error
tcpConnRemAddress	La dirección IP remota para esta conexión TCP
tcpInErrs	Número de segmentos desechados debido a errores de formato
tcpOutRsts	Número de reset generados

Tabla 8 – Miembros del grupo del protocolo TCP

- **Grupo UDP**

Algunos de los objetos relacionados con las operaciones del protocolo UDP se muestran en la tabla 9:

Objeto	Descripción
udpInDatagrams	Número de datagramas UDP entregados a usuarios UDP
udpNoPorts	Número de datagramas UDP recibidos para los que no existía aplicación en el puerto de destino
udpInErrors	Número de datagramas UDP recibidos que no se pudieron entregar por razones otras que la ausencia de la aplicación en el puerto de destino
udpOutDatagrams	Número de datagramas UDP enviados por la entidad

Tabla 9 – Miembros del grupo del protocolo UDP

2.3.5.3.3 SMI - STRUCTURE AND IDENTIFICATION OF MANAGEMENT INFORMATION

El SMI define las reglas para describir los objetos gestionados mencionados anteriormente y cómo los protocolos sometidos a la gestión pueden acceder a ellos. La descripción de los objetos gestionados se hace utilizando un subconjunto de ASN.1 (Abstract Syntax Notation 1, estándar ISO 8824), un lenguaje de descripción de datos. La definición del tipo de objeto consta de cinco campos:

- **Objeto.** Nombre textual, llamado *descriptor del objeto*, para el tipo del objeto, junto con su correspondiente *identificador de objeto.*

- **Sintaxis.** La sintaxis abstracta para el tipo el objeto. Las opciones son SimpleSyntax (entero, octeto de caracteres, identificador de objeto, Null), ApplicationSyntax (dirección de red, contador, escala, ticks, opaco) u otro tipo de sintaxis de aplicación[2].

- **Definición.** Descripción textual de la semántica del tipo de objeto de la SMI.

- **Acceso.** El objeto podrá tener acceso de sólo lectura, sólo escritura, lectura - escritura o inaccesible.

- **Estatus.** Este campo puede contener uno de los valores obligatorio, opcional u obsoleto.

Basados en los campos de la definición del tipo de objeto obtenemos una estructura de SMI de la siguiente forma:

[2] Ver el RFC 1155 para más detalles

```
OBJECT
        sysDescr { system 1 }
Syntax  OCTET STRING
Definition This value should include the full name and version
           identification of the system's hardware type, software
           operating-system, and networking software. It is
           mandatory that this contain only printable ASCII
           characters.
Access  read-only.
Status  mandatory.
```

Fig. 5 – Definición de un objeto contenido en la MIB

Los objetos gestionados deben ser descritos pero también identificados. Esto se hace utilizando el identificador de objeto (Object Identifier) ASN.1 al igual que un número de teléfono, reservando grupos de números para distintas localizaciones. En el caso de la gestión de red para TCP/IP, el número reservado fue *1.3.6.1.2* y SMI lo usa como base para la definición de nuevos objetos.

Este valor se obtiene al reunir los grupos de números que identifican diferentes tipos de estudios:

- El primer grupo define el nodo administrador
  (1) *Para ISO.*
  (2) Para CCITT.
  (3) Para la unión ISO-CCITT

- El segundo grupo para el nodo administrador, ISO define (3) para su uso por parte de otras organizaciones.

- El tercer grupo define (6) para su uso por parte del DoD (U.S. Department of Defense).

- En el cuarto grupo, el DoD no ha indicado cómo ha de gestionarse se grupo correspondiente por lo que la comunidad de Internet ha asumido (1).

- El quinto grupo fue aprobado por el IAB, Internet Architecture Board, para ser:

  (1) Para el uso del directorio OSI en Internet.

  (2) *Para la identificación de objetos con propósitos de gestión.*

  (3) Para la identificación de objetos con fines experimentales.

  (4) Para la identificación de objetos para uso privado.

La nomenclatura anterior podremos definirla mediante el análisis del siguiente esquema:

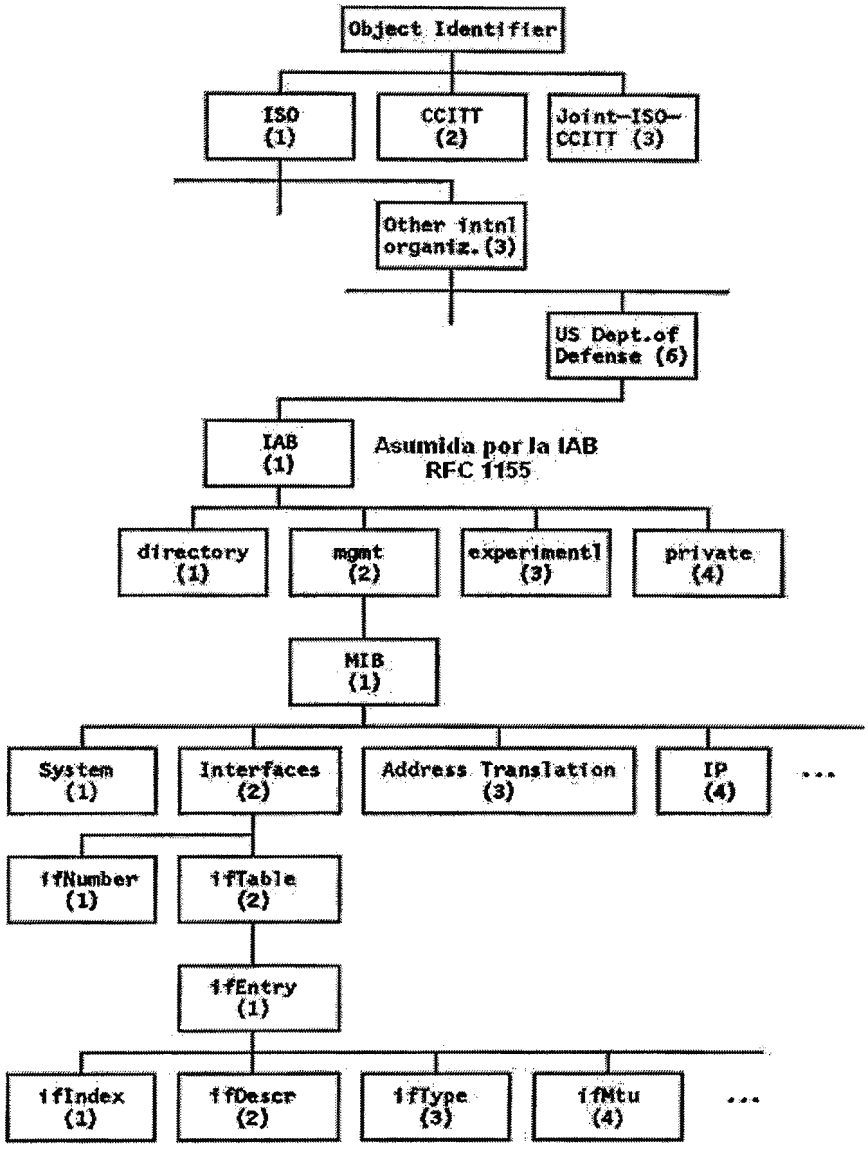


Fig. 6 - Identificador de objeto - Asignación para redes TCP/IP

2.3.5.4 COMUNIDAD SNMP

Es la relación entre un agente SNMP y un conjunto de estaciones de gestión SNMP, define características de autentificación y control de acceso. Los agentes pueden establecer una comunidad para cada combinación deseada de autentificación y control de acceso, al mismo tiempo pueden poseer el número de comunidades que deseen; con lo anterior dan a cada comunidad un nombre único dentro del agente (Community name).

Además cada estación de gestión puede pertenecer a varias comunidades, y deben almacenar los nombres de comunidad asociados a cada agente.

Mediante el uso de comunidades, un agente puede limitar el acceso a su MIB en dos formas, limitando la vista de su MIB (view MIB), que no es más que un subconjunto de los objetos de la MIB, o modificando su modo de acceso: READ-ONLY o READ-WRITE.

La combinación de ambas se denomina perfil de la comunidad SNMP (SNMP community profile), y a cada comunidad se le asigna uno formándose una política de acceso SNMP (SNMP access policy).

Como se ha visto, en cada paquete SNMP irá el nombre de la comunidad, y el agente sólo atenderá el mensaje si el nombre de la comunidad es correcto para el tipo de acceso solicitado. Por eso puede vérsele como una contraseña para el acceso al agente.

2.3.5.5 ESPECIFICACIONES DEL PROTOCOLO SNMP

Cuando una entidad de protocolo envía un mensaje, se realizan las siguientes acciones:

1. Construye una PDU apropiada como un objeto definido con el lenguaje ASN.1.

2. Pasa esta PDU, junto con un nombre de comunidad y las direcciones de transporte de fuente y destino, a un servicio de autentificación. Este servicio generará en respuesta otro objeto en ASN.1

3. La entidad construye ahora un mensaje en ASN.1 usando el objeto que le ha devuelto el servicio de autentificación y el nombre de comunidad

4. Este nuevo objeto se envía a la entidad destino usando un servicio de transporte.

Cuando una entidad de protocolo recibe un mensaje, realiza las siguientes acciones:

1. Hace un análisis del datagrama recibido para garantizar que corresponde con un mensaje en ASN.1. Caso contrario, el datagrama es descartado y la entidad no realiza más acciones.

2. Observa el número de versión. Si no concuerda descarta el datagrama y no realiza más acciones.

3. Pasa los datos de usuario, el nombre de comunidad y las direcciones de transporte de fuente y destino al servicio de autentificación. Si es correcto, este devuelve un objeto ASN.1. Si no lo es, envía una indicación de fallo. Entonces la entidad de protocolo puede generar una trampa (Trap), descarta el datagrama y no realiza más acciones.

4. La entidad intenta reconocer la PDU. Si la reconoce, según el nombre de comunidad adopta un perfil y procesa la PDU, si esta exige respuesta, la entidad iniciará la respuesta ahora. Si la PDU no es reconocida el datagrama se descarta.

Los agentes y gestores interactúan para llevar a cabo la detección de fallos en los dispositivos de la red mediante un sondeo por Traps (tramas específicas del protocolo).

2.3.5.5.1 FORMATO DEL PAQUETE SNMP

El paquete SNMP se puede dividir en dos campos más el resto de este que es la PDU de SNMP.

Nombre	Sintaxis	Tamaño (bytes)	Descripción
Version	Integer	4	**Version Number:** Describe el número de versión de SNMP del mensaje, es utilizado para asegurar la compatibilidad entre versions.
Community	Octet String	Variable	**Community String:** Identifica la comunidad SNMP en la que el transmisor y el receptor están localizados
PDU	—	Variable	**Protocol Data Unit:** La PDU que será comunicada como el cuerpo del mensaje

Tabla 10 – Formato de paquete SNMP

La sintaxis general de la estructura genérica de una PDU se muestra a continuación:

<table>
<tr><th>Nombre</th><th>Sintaxis</th><th>Tamaño (bytes)</th><th colspan="2">Descripción</th></tr>
<tr><td rowspan="10">PDU Type</td><td rowspan="10">Integer (Enumerated)</td><td rowspan="10">4</td><td>Valor PDU</td><td>Tipo de PDU</td></tr>
<tr><td>0</td><td>GetRequest-PDU</td></tr>
<tr><td>1</td><td>GetNextRequest-PDU</td></tr>
<tr><td>2</td><td>Response-PDU</td></tr>
<tr><td>3</td><td>SetRequest-PDU</td></tr>
<tr><td>4</td><td>Obsoleta (Trap-PDU en SNMPv1)</td></tr>
<tr><td>5</td><td>GetBulkRequest-PDU</td></tr>
<tr><td>6</td><td>InformationRequest-PDU</td></tr>
<tr><td>7</td><td>Trapv2-PDU</td></tr>
<tr><td>8</td><td>Report-PDU</td></tr>
<tr><td>Request ID</td><td>Integer</td><td>4</td><td colspan="2">Request Identifier: Entero que indica el orden de emisión de los datagramas. Este parámetro sirve también para identificar datagramas duplicados en los servicios de datagramas poco fiables.</td></tr>
<tr><td>Error Status</td><td>Integer (Enumerated)</td><td>4</td><td colspan="2">Error Status: Valor entero que utilizado en una Response-PDU, indica a la entidad que realice la petición SNMP el resultado de su petición; cero indica que no a ocurrido ningún error, otros valores indican que a ocurrido un error.
Los primeros seis valores (0-5) se mantienen por compatibilidad con SNMPv1 pero SNMPv2 agrega varios códigos de error que proveen una indicación más específica de la naturaleza de un error en una petición. El código genErr es utilizado cuando ninguno de los tipos específicos de errores aplica.</td></tr>
<tr><td>Error Index</td><td>Integer</td><td>4</td><td colspan="2">Error Index: cuando el Error Status no es cero, este campo indica qué variable de una lista ha generado ese error.</td></tr>
<tr><td>Variable Bindings</td><td>Variable</td><td>Variable</td><td colspan="2">Variable Bindings: Número de parejas de valores que identifican los objetos de la MIB en la PDU, en caso de mensajes en lugar de peticiones contienen sus valores.</td></tr>
</table>

Tabla 11 – Sintaxis de PDU

SNMP Versión 2 (SNMPv2) PDU VALORES DEL CAMPO ERROR STATUS

Error Status	Código del Error	Descripción
0	noError	No ha ocurrido ningún error, código utilizado en toda petición PDU, pues no existe ningún error que reportar.
1	tooBig	El tamaño de la Response-PDU es demasiado grande para ser transportada
2	noSuchName	El nombre de un objeto solicitado no fue encontrado
3	badValue	El valor en la petición no encaja la estructura que el receptor de la petición tiene del objeto.
4	readOnly	Un intento fue hecho para colocar una variable que tiene un valor de acceso indicando que es solo lectura
5	genErr	Ocurrió un error que no está especificado en esta tabla de errores.
6	noAccess	El acceso fue denegado al objeto por razones de seguridad
7	wrongType	El tipo de objeto en una variable es incorrecto para el objeto
8	wrongLength	Una variable especifica una longitud incorrecta para el objeto
9	wrongEncoding	Una variable especifica una codificación incorrecta para el objeto
10	wrongValue	El valor dado en una variable no es posible para el objeto
11	noCreation	Una variable especificada no existe y no puede ser creada
12	inconsistentValue	Una variable especifica un valor que puede ser manejado por la variable pero no puede ser asignado a ella al mismo tiempo
13	resourceUnavailable	Un intento de definir a una variable con un recurso que no está disponible
14	commitFailed	Un intento para definir una variable en particular falló
15	undoFailed	Un intento para definir una variable en particular con parte de un grupo de variables falló, y el intento de deshacer los cambios no fue exitoso
16	authorizationError	Un problema ocurrió en la autorización
17	notWritable	La variable no puede ser escrita o creada
18	inconsistentName	El nombre en una variable utilizada no existe

Tabla 12 – Valores del campo Error Status en la PDU

TIPOS DE DATOS PERMITIDOS POR SMI PARA SNMPV2

Tipo de dato	Descripción
Integer	Enteros en el rango -2^{31} a $2^{31}-1$
Uinteger 32	Enteros en el rango de 0 a $2^{32}-1$
Counter 32	Un entero no negativo que se puede incrementar módulo 2^{32}
Counter 64	Un entero no negativo que se puede incrementar módulo 2^{64}
Gauge 32	Un entero no negativo que se puede incrementar o decrementar, pero no excederá un valor máximo. El valor no puede ser mayor que $2^{32}-1$.
TimeTicks	Un entero no negativo que representa el tiempo, módulo 2^{32}, en centésimas de segundo.
Octet String	Cadena de Octetos para datos arbitrarios binarios o textuales, puede estar limitada a 255.
IP Address	Una dirección de Internet (IP) de 32 bits.
Opaque	Un campo de bits arbitrario.
Bit String	Una enumeración de bits con nombre.
Object Identifier	Nombre asignado administrativamente a objetos u otros elementos normalizados. El valor es una secuencia de hasta 128 enteros no negativos.

Tabla 13 – Tipos de datos SNMPv2

2.3.5.5.2 ASIGNACIÓN DE VARIABLES - VarBindList

Lista de nombres de variables con su valor asociado. Algunas PDU quedan definidas sólo con los nombres, pero aún así deben llevar valores asociados. Se recomienda para estos casos la definición de un valor NULL.

Los nombres son especificados como identificadores de objeto (OID). En getRequest, como se estudiara más adelante los valores son NULL.

2.3.5.5.3 TIPOS DE PDU Y FUNCIONALIDAD

Cuando los programas de administración del Protocolo simple de administración de redes, SNMP, envían solicitudes a un dispositivo de red, el software del agente en ese dispositivo recibe las solicitudes y recupera la información de las MIB.

Posteriormente, el agente vuelve a enviar la información solicitada al programa de administración SNMP que lo inició. Para realizar estas tareas, el agente utiliza los tipos de mensaje presentados en la tabla número 14.

Cuatro de estos tipos de mensajes son protocolos de solicitud y respuesta simples en los que SNMP utiliza el Protocolo de datagramas de usuario, UDP.

Esto significa que existe la posibilidad de que una solicitud del sistema de administración no llegue al agente y de que la respuesta del agente no llegue al sistema de administración. SNMP es un protocolo de red sin conexión, por lo que no existen garantías de que los mensajes de este protocolo lleguen a su destino.

Mensaje de SNMP	Descripción
Get	Mensaje básico de solicitud de SNMP. Enviado por un sistema de administración SNMP, solicita información acerca de una única entrada de la base de datos MIB de un agente SNMP. Por ejemplo, la cantidad de espacio libre en el disco.
Get-next	Tipo ampliado de mensaje de solicitud que puede utilizarse para examinar todo el árbol de objetos de administración. Cuando se procesa una solicitud Get-next para un objeto determinado, el agente devuelve la identidad y el valor del objeto que sigue lógicamente al objeto de la solicitud. La solicitud Get-next resulta útil en el caso de tablas dinámicas, como una tabla interna de rutas IP.
Set	Si está permitido el acceso de escritura, este mensaje puede utilizarse para enviar y asignar un valor de MIB actualizado al agente.
Getbulk	Solicita que el tamaño de los datos transferidos por el agente del host sea lo más grande posible, dentro de las limitaciones dadas para el tamaño de los mensajes. Esto reduce al mínimo el número de intercambios de protocolo necesarios para recuperar una gran cantidad de información de administración. El tamaño máximo del mensaje no debe ser superior a la unidad de transmisión máxima (MTU) de la ruta de acceso, el tamaño de trama máximo permitido para una única trama de la red, o de lo contrario se puede producir fragmentación.
Trap	Un mensaje no solicitado enviado por un agente SNMP a un sistema de administración de SNMP cuando el agente detecta que se ha producido un tipo determinado de suceso localmente en el host administrado. La consola de administración de SNMP que recibe un mensaje de captura se conoce como destino de captura. Por ejemplo, puede enviarse un mensaje de captura sobre un suceso de reinicio del sistema.

Tabla 14 – Mensajes SNMP

2.3.6 ICMP - INTERNET CONTROL MESSAGE PROTOCOL

2.3.6.1 GENERALIDADES DEL PROTOCOLO ICMP

El protocolo ICMP permite el intercambio de mensajes de control y de supervisión entre dos dispositivos de red. Toda anomalía detectada por el protocolo IP provoca el intercambio de mensajes ICMP entre los nodos de la red. ICMP forma parte de la capa Internet y usa la facilidad de enviar paquetes IP para enviar mensajes.

ICMP es un protocolo de control que utilizan los dispositivos de encaminamiento para notificar las diferentes incidencias que puede haber en una red IP; se utiliza cuando:

- Un datagrama no es capaz de alcanzar su destino.

- El dispositivo de encaminamiento no tiene la capacidad de almacenar temporalmente el datagrama para reenviarlo.

- El dispositivo de encaminamiento indica a un host que envíe el tráfico por una ruta mas corta. Cada mensaje ICMP se encapsula en un paquete IP y luego es enviado de la forma habitual. Como los mensajes ICMP se transmiten en mensajes IP, no puede garantizarse que lleguen a su destino.

Cuando un router o un host de destino debe informar al host fuente acerca del procesamiento de datagramas hace uso de ICMP y el comportamiento de este puede caracterizarse del modo siguiente:

- ICMP puede informar de errores en cualquier datagrama IP con la excepción de mensajes IP, para evitar repeticiones infinitas.

- Para datagramas IP fragmentados, los mensajes ICMP sólo se envían para errores ocurridos en el fragmento cero. Es decir, los mensajes ICMP nunca se refieren a un datagrama IP con un campo de desplazamiento de fragmento.

- Los mensajes ICMP nunca se envían en respuesta a datagramas con una dirección IP de destino que sea de broadcast o de multicast.

- Los mensajes ICMP nunca se envían en respuesta a un datagrama que no tenga una dirección IP de origen que represente a un único host. Es decir, la dirección de origen no puede ser cero, una dirección de looopback, de broadcast o de multicast.

- Los mensajes ICMP nunca se envían en respuesta a mensajes ICMP de error. Pueden enviarse en respuesta a mensajes ICMP de consulta (los tipos de mensaje ICMP 0, 8, 9, 10 y 13 al 18).

El RFC 792 establece que los mensajes ICMP pueden ser generados para informar de errores producidos en el procesamiento de datagramas IP, no que deban.

En la práctica, los routers generarán casi siempre mensajes ICMP para los errores, pero en el caso de los host de destino, el número de mensajes ICMP generados es una cuestión de implementación.

2.3.6.2 MENSAJES ICMP

Los mensajes ICMP se describen en los RFC 792 y 950, correspondientes al STD 5 y su estatus es requerido.

Los mensajes ICMP se envían en datagramas IP. La cabecera IP siempre tendrá un número de protocolo de 1, indicando que se trata de ICMP y un servicio de tipo 0, rutina. El campo de datos de IP contendrá el auténtico mensaje ICMP en el formato mostrado a continuación.

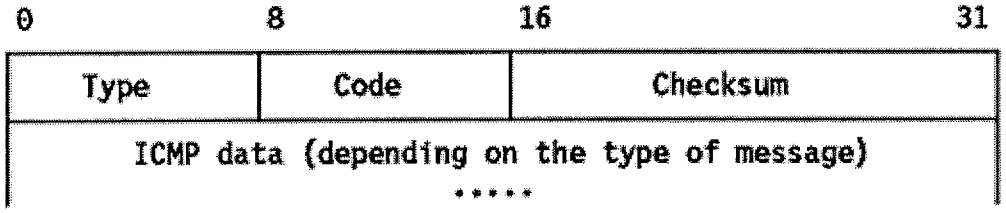


Fig. 7 - Formato de mensajes ICMP

Type. Especifica el tipo del mensaje enviado por el protocolo ICMP, este campo puede tener cualquiera de los siguientes valores:

Cod	Descripción	Cod	Descripción
0	Echo reply	12	Parameter Problem
3	Destination unreachable	13	Timestamp request
4	Source quench	14	Timestamp reply
5	Redirect	15	Information request (obsolete)
8	Echo	16	Information reply (obsolete)
9	Router Advertisement	17	Address mask request
10	Router Solicitation	18	Address mask reply
11	Time exceeded		

Tabla 15 - Tipo de mensajes ICMP

Code. Contiene el código de error para el datagrama del que da parte el mensaje ICMP. La interpretación dependerá del tipo de mensaje.

Checksum. Contiene el complemento a 1 de 16 bits de la suma del mensaje ICMP comenzando por el campo *Type*. Para interpretar este *checksum* se asume en principio que su valor es cero. Este algoritmo es el mismo que el usado por IP para el cálculo de su cabecera.

Data. Contiene información para el mensaje ICMP. Típicamente se tratará de parte del mensaje IP original para el que se generó el mensaje ICMP. La longitud de los datos puede calcularse como la diferencia entre la longitud del datagrama IP que contiene el mensaje y la cabecera IP.

Los tipos de mensajes del protocolo ICMP utilizados para la presente aplicación se explican a continuación.

2.3.6.2.1 ECHO REPLY (0) Y ECHO (8)

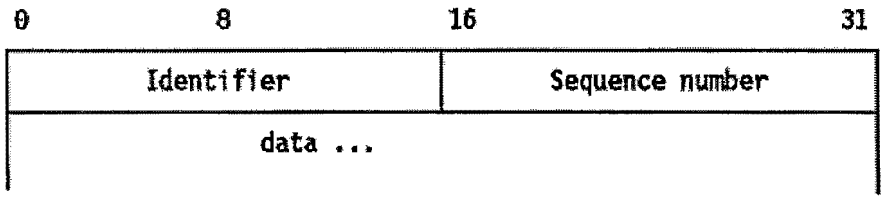


Fig. 8 - ICMP Echo y Echo Reply

Echo se usa para detectar la existencia de otro host activo en la red. La fuente inicializa el identificador y el número de secuencia (utilizado cuando se envían múltiples mensajes del tipo *echo request*), añade algunos datos al campo de datos y envía el "echo" ICMP al host de destino. El código de la cabecera ICMP es cero. El receptor cambia el tipo del mensaje a *echo reply* y devuelve el datagrama al host fuente. El comando Ping emplea este mecanismo paca determinar si es posible alcanzar a un host de destino.

2.3.6.2.2 TIME EXCEEDED (11)

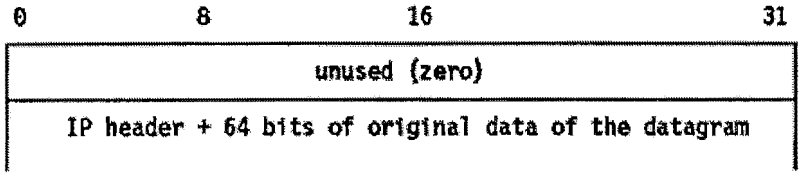


Fig. 9 - Time Exceeded de ICMP

Si se recibe este mensaje de un router intermedio, significa que el TTL de un datagrama IP ha expirado.

Si se recibe del host destino, significa que el TTL para ensamblar el datagrama ha expirado mientras el host esperaba uno de sus fragmentos. La cabecera ICMP puede tener uno de los siguientes valores:

Cod	Descripción
0	transit TTL exceeded
1	reassembly TTL exceeded

Tabla 16 - Códigos de cabecera ICMP si excede tiempo

2.3.6.3 APLICACIONES DE ICMP

Hay dos aplicaciones esenciales realizadas mediante el protocolo de mensajes de error ICMP de las cuales se hace uso en la presente aplicación:

- **Ping**

  Utiliza los mensajes ICMP Echo y Echo Reply, 8 y 0 respectivamente, para determinar si un host es alcanzable.

- **Traceroute**

  Envía datagramas IP con bajos TTL para que expiren durante la ruta que les dirige al destino. Utiliza los valores de los mensajes ICMP Time Exceded para determinar en que parte de la red expiraron los datagramas y reconstruye así un esquema de la ruta hasta el host de destino.

2.3.7 NetBEUI / NetBIOS

2.3.7.1 NetBEUI - NetBIOS Extended User Interface

NetBEUI, NetBIOS Extended User Interface (Interfaz extendida de usuario de NetBIOS), es un protocolo de capa de red sencillo utilizado en las primeras redes de Microsoft como *Lan Manager* o *Windows 95*. La comunicación entre equipos se consigue gracias al intercambio de sus nombres en una red de área local, pero no dispone de mecanismos para conectar equipos que estén en redes separadas; es un protocolo sin encaminamiento.

2.3.7.2 NetBIOS - NETWORK BASIC INPUT/OUTPUT

NetBIOS, Network Basic Input/Output, es un protocolo de red originalmente creado para redes locales de computadoras IBM. Utiliza los servios de red que le proporciona NetBEUI; en los sistemas actuales NetBIOS puede funcionar sobre protocolos más completos y extendidos como IPX o el propio IP empleado en la arquitectura TCP/IP de Internet e intranets. NetBIOS provee tres tipos de servicios:

- **Servicio de nombres.** Permite el registro de nombres de una computadora, aplicaciones y otros identificadores en general en la red. Un programa puede, a través de este servicio, determinar qué computadora en la red corresponde un determinado nombre.

- **Servicio de paquetes.** Posibilita el envío y recibimiento de paquetes en la red, punto a punto o por difusión.

- **Servicio de sesión.** Establece conexiones entre dos puntos en la red y es análogo al protocolo TCP.

Este protocolo corresponde con la era pre-Internet, año 1985, y se utilizaba en equipos con Windows 98/95 y "Microsoft Windows para Trabajo en Grupo".

En esa época, una red de las dimensiones de Internet era inimaginable; el modelo sobre el que se trabajaba era el de redes segmentadas en racimos de unos pocos equipos (grupos de trabajo) bajo el principio de confianza; se presumía que todos las computadoras de cada segmento eran seguros.

Debido a este diseño para grupos pequeños (óptimamente, una decena, máximo unos 200 equipos), NetBIOS es un protocolo no enrutable: cada equipo se identifica con un nombre (equipo_de_silvia, equipo_de_juan) y no

con una dirección lógica, viéndose entre si únicamente los equipos situados en el mismo segmento, y siendo necesario utilizar puertas de enlace (gateway) para conectar los segmentos entre si, o con un ordenador principal.

En realidad, y pese a su antigüedad y limitaciones, para redes pequeñas, posiblemente siga siendo el protocolo más rápido.

NetBIOS originariamente trabajaba sobre el protocolo NetBEUI que era el responsable del transporte de datos.

Con la difusión de Internet, sin embargo, y la propagación del protocolo TCP/IP, los sistemas operativos de Microsoft mas recientes permiten ejecutar NetBIOS sobre el protocolo TCP/IP, prescindiendo de NetBEUI, de hecho este protocolo no aparece por defecto disponible en Windows XP.

En principio no hace falta NetBIOS si solo se quiere conectar a Internet. Pero en el caso de que se deba tener NetBios (por ejemplo para compartir una impresora en una red doméstica), se puede ejecutar sobre TCP/IP, lo que permite prescindir del protocolo NetBEUI, lo que es bueno, porque limita el número de protocolos instalados. Pero como NetBEUI no es accesible desde Internet, por no ser enrutable, quizás sea una mayor ventaja ejecutar NetBIOS sobre NetBEUI, desactivando NetBIOS sobre TCP/IP.

NetBIOS utiliza los puertos 137, 138 y 139. Es un protocolo exclusivo de máquinas Windows. Para saber si una computadora tiene NetBIOS activado utilizando el la siguiente instrucción en la ventana de comandos: *netstat -an*. Este comando informará si se tienen los tres puertos anteriores en modo LISTENING.

Por ejemplo:

C:\WINDOWS>netstat -an

Conexiones activas

Protocolo	Dirección local	Dirección remota	Estado
TCP	192.168.0.2:137	0.0.0.0:0	LISTENING
TCP	192.168.0.2:138	0.0.0.0:0	LISTENING
TCP	192.168.0.2:139	0.0.0.0:0	LISTENING
UDP	192.168.0.2:137	*:*	
UDP	192.168.0.2:138	*:*	

Existen numerosas críticas respecto a la seguridad hacia los entornos Windows que se centran en el protocolo NetBIOS. Es recomendable que si este protocolo no es imprescindible debe ser deshabilitado.

A continuación se plantean 4 ejemplos en los que se muestra quien necesita tener activo el protocolo NetBIOS y quien debería deshabilitarlo.

1. Un servidor Web

2. Una computadora de escritorio conectada a Internet mediante un módem

3. Una computadora de escritorio que participa en la red de una empresa

4. Un servidor de usuarios y archivos

En el primer caso, NetBIOS debería estar deshabilitado ya que un servidor Web no comparte recursos mediante Entorno de red ni accede a recursos compartidos de otros ordenadores, el servicio de páginas Web, HTTP, funciona exclusivamente con TCP/IP.

En el segundo caso, NetBIOS es también innecesario por las mismas razones antes expuestas.

En el caso número tres es accesible la activación del protocolo puesto que esta computadora de escritorio probablemente necesite acceder a recursos compartidos de otras computadoras así como utilizar servicios de impresoras remotas.

El servidor del ejemplo cuatro requiere NetBIOS, pues de esta forma los usuarios podrán acceder a sus archivos de una forma cómoda.

2.3.7.2.1 ESTRUCTURA DEL PROTOCOLO NETBIOS

Los paquetes tienen diferentes formatos de acuerdo a los servicios, tipos de mensajes así como también los protocolos de transporte usados para trasladar los paquetes.

Como se menciono con anterioridad los servicios básicos de NetBIOS son: *nombre, sesión y datagrama*. A continuación se presenta el formato de un paquete del servicio *Nombre* en ambiente TCP/IP:

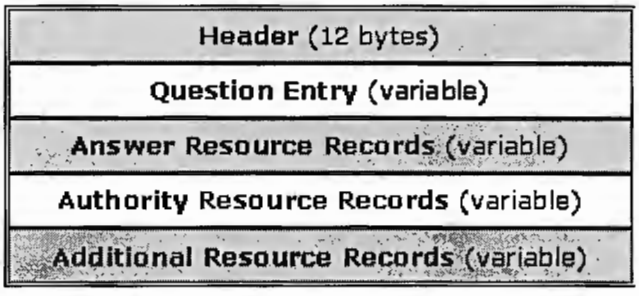


Fig. 10 – Formato del servio Nombre de NetBIOS visto por TCP/IP

El formato del Header de NetBIOS se muestra en la siguiente figura:

2	2	1	1	2	2	2 bytes
Length	Delimintor	Command	Data1	Data2	XMIT Cor	RSP Cor
Destination name (16 bytes)						
Source name (16 bytes)						

Fig. 11 – Formato Header de NetBIOS

Campo	Descripción
Length	Longitud de la cabecera de NETBIOS
Deliminator	Un símbolo delimitador que indica que los datos subsiguientes se destinan para la función de NetBIOS
Command	Una orden específica del protocolo que indica el tipo de la función del marco
Data 1	Un byte de datos opcionales por cada comando específico
Data 2	Dos byte de datos opcionales por cada comando específico
Xmit/response correlator	Utilizado para asociar las respuestas recibidas con pedidos transmitidos
Destination name/num	En una no-sesión este campo contiene un nombre de 16 caracteres
Source name/num	En una no-sesión este campo contiene el nombre de la fuente de 16 caracteres. En la sesión encuadra este campo contiene un 1 byte del número de la sesión de la fuente

Tabla 17 – Descripción de los campos en Header

2.3.8 ARP - ADDRESS RESOLUTION PROTOCOL

2.3.8.1 GENERALIDADES DE ARP

En una sola red física, los hosts individuales se conocen en la red a través de su dirección física. Los protocolos de alto nivel se encargan de dirigir los mensajes de hosts de destino con una dirección simbólica (en este caso la dirección IP). Cuando tal protocolo quiere enviar un datagrama a la dirección IP de destino w.x.y.z, el manejador de dispositivo no la entiende.

En estos casos, se suministra un módulo (ARP) que traducirá la dirección IP a la dirección física del host destino. ARP utiliza una tabla, *caché ARP*, para realizar dicha traducción.

Cuando la dirección física no se encuentra en la caché ARP, se envía un broadcast en la red, con un formato especial llamado *petición ARP*. Si una de las máquinas en la red reconoce su propia dirección IP en la petición, devolverá una *respuesta ARP* al host que la solicitó. La respuesta contendrá la dirección física del hardware así como información de encaminamiento (si el paquete atravesó otros dispositivos durante su trayecto) tanto esta dirección como la

ruta se almacenan en la caché del host solicitante. Todos los posteriores datagramas enviados a esta dirección IP se podrán asociar a la dirección física correspondiente, que será la que utilice el manejador de dispositivo para mandar los datagramas a la red.

ARP se diseño para ser usado en redes que soportasen mensajes de multidifusión por hardware. Esto significa, por ejemplo, que ARP no funcionará en redes tipo X.25.

ARP se emplea en redes IEEE 802 además de en las viejas redes DIX Ethernet (El estándar lanzado en 1978 por Xerox Corporation, Intel Corporation y Digital Equipment Corporation) para el mapeo direcciones IP a direcciones físicas. La funcionalidad de ARP depende en gran medida del manejador de dispositivo para el tipo de red correspondiente, que suele estar codificado en el *micro código del adaptador*.

2.3.8.2 PAQUETES ARP

2.3.8.2.1 FORMATO Y GENERACIÓN DEL PAQUETE ARP

Si una aplicación desea enviar datos a una determinado dirección IP de destino, el mecanismo de encaminamiento IP determina primero la dirección IP del siguiente salto del paquete (que puede ser el propio host de destino o un router) y el dispositivo físico al que se debería enviar. Si se trata de una red 802.3/4/5, deberá consultarse el módulo ARP para establecer el mapeo para el par *<tipo de protocolo, dirección de destino>* a una dirección física de 48 bits.

El módulo ARP intenta encontrar la dirección en su caché. Si obtiene el par buscado, devuelve la correspondiente dirección física de 48 bits al llamador (el manejador de dispositivo). Si no lo encuentra, *descarta el paquete* (se asume que al ser un protocolo de alto nivel volverá a transmitirlo) y genera un broadcast de red para una solicitud ARP.

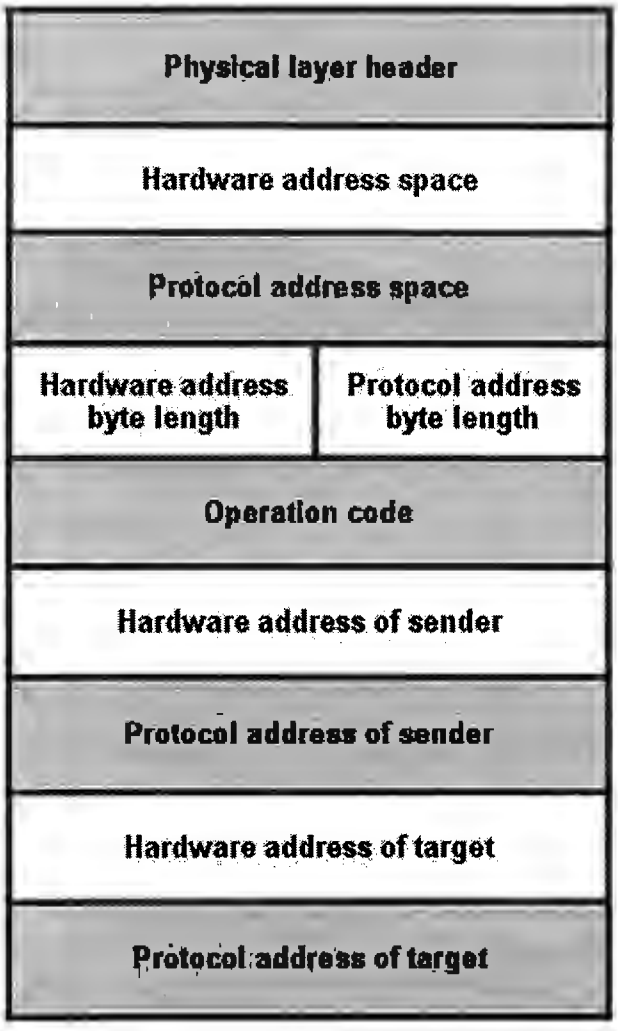


Fig. 12 - Paquete de petición/respuesta ARP

Campo	Descripción
Hardware address space	Especifica el tipo de hardware; ejemplos son Ethernet o Packet Radio Net.
Protocol address space	Especifica el tipo de protocolo, el mismo que en el campo de tipo EtherType en la cabecera de IEEE 802.
Hardware address length	Especifica la longitud (bytes) de la dirección hardware del paquete. Para IEEE 802.3 e IEEE 802.5 será de 6.
Protocol address length	Especifica la longitud (bytes) de las direcciones del protocolo en el paquete. Para IP será de 4.
Operation code	Especifica si se trata de una petición (1) o una respuesta (2) ARP.
Source/target hardware address	Contiene la dirección física de hardware. En IEEE 802.3 son direcciones de 48 bits.
Source/target protocol address	Contiene las direcciones del protocolo. En TCP/IP son direcciones IP de 32 bits.

Tabla 18 – Descripción del Paquete de petición/respuesta ARP

Para el paquete de solicitud, la dirección hardware de destino es el único campo indefinido del paquete.

2.3.8.2.2 RECEPCIÓN DEL PAQUETE ARP

Cuando un host recibe un paquete ARP, sea este por un broadcast o una respuesta punto a punto, el dispositivo receptor pasa el paquete al módulo ARP, el cual lo manipula tal como se muestra en la figura 13.

El host solicitante recibirá esta respuesta ARP, y seguirá el algoritmo ya comentado para tratarla. Como resultado, se añadirá a la caché ARP la tripleta *<tipo de protocolo, dirección de protocolo, dirección hardware>* para el host en cuestión. La próxima vez que un protocolo de nivel superior necesite enviar un paquete al host anterior, el módulo de ARP encontrará la dirección física a la que se enviará el paquete.

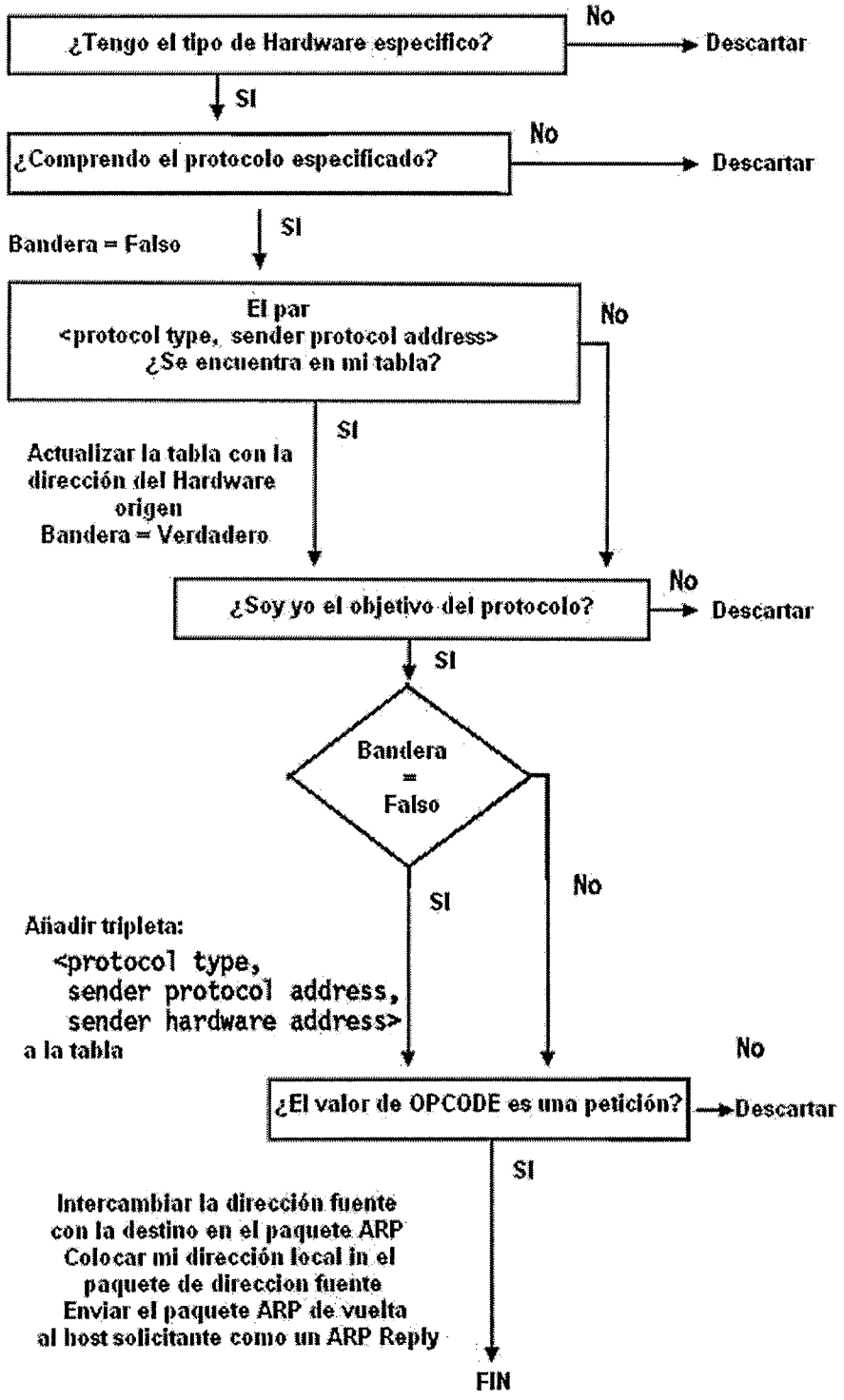


Fig. 13 – Manipulación del paquete ARP por parte del receptor

Es importante recalcar que debido a que la petición ARP original fue un broadcast en la red, todos los host en ella habrán actualizado la dirección del emisor en su propia caché (sólo si previamente ya existía esa entrada) en la tabla.

CAPITULO III
HERRAMIENTAS A UTILIZAR

3.1 WINPCAP

3.1.1 GENERALIDADES

WinPcap es una biblioteca abierta para la captura de paquete y análisis de red para las plataformas Win32. La versión para el sistema operativo Linux es *libpcap*.

La mayoría de aplicaciones acceden a la redes a través de primitivas de los sistemas operativos, tales como la utilización de sockets. Es fácil acceder a los datos en la red con este enfoque pues el sistema operativo se enfrenta con los detalles de más bajo nivel (protocolo de manejo, ensamble de paquete, entre otros) y proporciona una interfaz familiar que es semejante a la utilizada para la lectura y escritura de archivos.

A veces, sin embargo, la "manera fácil" no es la tarea, desde que algunas aplicaciones requieren el acceso directo a paquetes en la red. Esto significa que se necesita acceso a los datos *crudos* en la red sin la interposición de procesamiento de un protocolo por el sistema operativo.

El propósito de WinPcap es brindar esta clase del acceso a aplicaciones Win32; proporciona facilidades de:

- Captura paquetes *crudos*, los destinados a la máquina donde se ejecuta y los intercambiados por otros host (en un entorno de medios compartidos)

- Filtración de paquetes según reglas especificadas por el usuario antes de enviarlos a la aplicación

- Transmisión de paquetes crudos a la red

- Recopilación de información estadística acerca del el tráfico de red

Este conjunto de capacidades se obtiene por medio de un driver de dispositivo, el cual se encuentra instalado en la porción del Kernel de Win32, adicionalmente se hace uso de unos cuantos archivos de extensión DLL.

Todas estas características se exportan utilizando una interfaz de programación poderosa, fácilmente explotable por aplicaciones y se encuentran disponibles en diversos sistemas operativos.

3.1.2 LO QUÉ NO PUEDE HACER WINPCAP

WinPcap recibe y envía paquetes independientemente de los protocolos del host, como por ejemplo TCP-IP. Esto significa que no es capaz de bloquear, filtrar o manipular el tráfico generado por otros programas en la misma máquina: específicamente husmea los paquetes que fueron transmitidos en la red. Por lo tanto, no proporciona el soporte apropiado para aplicaciones como de tráfico y cortafuegos personales.

3.1.3 QUÉ CLASE DE PROGRAMAS UTILIZAN WinPcap

La interfaz de programación de WinPcap puede ser utilizada por muchas tipos herramientas de red para el análisis, localización de fallas, seguridad y control. Pueden mencionarse cierto tipo de aplicaciones que dependen de WinPcap:

- Analizadores de red y protocolo
- Monitores de la red
- Archivos de tráfico (Logs)
- Generadores de tráfico
- Puentes de usuario-nivel y routers
- Sistema de detección de intrusos de red (NIDS)
- Escaneo de red
- Herramientas de seguridad

La presente aplicación utiliza la versión estable mas reciente, WinPcap 3.1 la cual es compatible con los sistemas Windows:

- 95, 98, ME
- NT4, 2000
- XP, 2003
- Vista Beta1[3]

A junio de 2006, la versión mas actualizada pero aun no estable plenamente es WinPcap 4.0 alpha1.

3.2 Net-SNMP 5.3.0.1

3.2.1 GENERALIDADES

Net-SNMP es una serie de aplicaciones utilizadas para la implementación del protocolo SNMP en sus diferentes versiones SNMP v1, SNMP v2c y SNMP v3 que utilizan IPV4 al igual que IPV6.

[3] WinPcap no ha sido puesta a prueba por complete en este sistema operativo pues fue lanzado dos semanas antes de la aparición de esta versión de WinPcap

Este paquete se baso originalmente en la implementación de la Universidad de Carnegie Mellon SNMP (la versión 2.1.2.1), pero ha desarrollado apreciablemente desde entonces. La serie incluye:

- Aplicaciones de línea de comandos para:

    - Recuperación información de un dispositivo que pueda operar SNMP, ya sea mediante el uso de peticiones individuales o peticiones múltiples.
    - Manipulación de información acerca de la configuración en un dispositivo capaz de interactuar con SNMP.
    - Recuperación de colecciones de información fija en dispositivos operables con SNMP.
    - Conversión entre formas numéricas y textuales de OID de MIB, y despliegue del contenido y estructura de MIB.

- Un examinador gráfico de MIB, utilizando Tk/perl.

- Una aplicación de demonio para recepción de notificaciones SNMP. Las notificaciones escogidas pueden ser registradas, reenviadas a otro sistema administración de SNMP, o pasadas a una aplicación externa.

- Un agente extensible para responder a peticiones SNMP para administración de información. Esto incluye apoyo incorporado para una gran variedad de módulos de información MIB, y puede extenderse aun mas utilizando módulos cargados dinámicamente, scripts (escrituras) y comandos externas, y los protocolos SMUX (SNMP Multiplexing) y AgentX (Agente de Extensibilidad).

- Una biblioteca para desarrollar aplicaciones SNMP, tanto con C como API de Perl.

Este agente sostiene actualmente el original SNMPv1, Comunidades basadas en SNMPv2 (RFC 1901-1908) y SNMPv3 (RFC 3411-3418). El agente responderá a las peticiones que utilizan cualquiera de estos protocolos, y todas las herramientas esperan una instrucción en las líneas de comando para determinar cuál versión a utilizar. Trabaja sobre los protocolos de transporte TCP y UDP, así como un SMUX (RFC 1227) agente maestro, AgentX (RFC 2257) en roles de paquetes maestros y de sub-agente, y Proxy SNMP.

3.2.2 SISTEMAS OPERATIVOS

Net-SNMP está disponible para sistemas operativos Unix y similares, también puede ser utilizado por sistemas Microsoft Windows. La funcionalidad puede variar dependiendo del sistema operativo en el que se utilice. Se ha verificado el desempeño de aplicaciones y el agente, por lo menos en parte, en los sistemas operativos siguientes:

- Linux (kernels 2.6 to 1.3)
- Solaris/SPARC (11 to 2.3), Solaris/Intel (10, 9)
- HP-UX (10.20 to 9.01 and 11.11 to 11.0)
- Mac OS X (10.4 to 10.1)
- NetBSD (2.0 to 1.0)
- OpenBSD (3.7, 2.8, 2.6)
- BSDi (4.0.1 to 2.1)
- AIX (5.2, 5.1, 4.1.5, 3.2.5)
- IRIX (6.5 to 5.1)
- OSF (4.0, 3.2 and Tru64 Unix 5.1B)
- SunOS 4 (4.1.4 to 4.1.2)
- Ultrix (4.5 to 4.2)
- Dynix/PTX 4.4
- QNX 6.2.1A
- Plataformas Win32

3.2.3 NET-SNMP EN WINDOWS

La serie debe compilar y debe correr en plataformas Win32, inclusive la biblioteca, la línea de comandos ordena-línea y la estructura básica del agente. Este agente incluye actualmente apoyo para el módulo MIB-II, pero esto requiere la previa instalación de la Plataforma Central SDK de Microsoft.

Algunos otros módulos de MIB, inclusive las extensiones de ventanilla de servicios de UCD, no trabajan en entornos Windows.

3.2.4 ¿CUÁN GRANDE PUEDE SER UNA PETICIÓN O RESPUESTA DE SNMP?

La definición de protocolo especifica un tamaño de paquete "mínimo máximo", 484 bytes para UDP, protocolo que todos sistemas deben sostener, pero no pretende definir un valor superior como tamaño máximo. Esto dependerá de cada implementación individual.

3.2.5 MIB SOPORTADAS

Las MIB soportadas por Net-SNMP, al menos en parte y en algunos sistemas, son descritas:

- MIB-2 Estadística red generales (RFC 1213)
- Recursos del host (RFC 1514 y 2790)
- MIB SNMPv3 (RFCs 2571-5, 3411-3418; incluyendo USM, VACM, MIB objetivo y notificación)

- MIB de acontecimiento DisMan
- MIB de horario de DisMan
- MTA-MIB (sendmail, envío de correo)
- Extensiones privadas del agente (procesos específicos del monitor y discos, memoria, unidad de procesamiento central (CPU), carga promedio, extensión del agente utilizando órdenes del Shell).

3.3 Nmap

3.3.1 GENERALIDADES

Herramienta de código abierto para exploración de redes y auditoria de seguridad.

Fue diseñada para el análisis rápido de redes de gran tamaño, aunque funciona muy bien contra equipos individuales. Utiliza paquetes IP crudos (raw) en formas originales para determinar qué equipos se encuentran disponibles en una red, servicios ofrecidos, sistemas operativos ejecutados, filtros de paquetes o cortafuegos utilizados así como muchas características mas.

Aunque generalmente Nmap se utiliza en auditorias de seguridad, muchos administradores de redes y sistemas lo encuentran útil para realizar tareas rutinarias, como puede ser el inventariado de la red, planificación de actualización de servicios y monitoreo del tiempo que los equipos o servicios que se mantiene activos.

3.3.2 TIPOS DE PUERTOS

Nmap comenzó como un analizador de puertos eficiente, aunque ha aumentado su funcionalidad a través de los años, aquella sigue siendo su función primaria. La sencilla orden **nmap *objetivo*** analiza más de 1660 puertos TCP del equipo *objetivo*. Aunque muchos analizadores de puertos han agrupado tradicionalmente los puertos en dos estados: abierto o cerrado, Nmap es mucho más descriptivo. Se dividen a los puertos en seis estados distintos.

Estos estados no son propiedades intrínsecas del puerto en sí, pero describen como los ve Nmap. Por ejemplo, un análisis con Nmap desde la misma red en la que se encuentra el objetivo puede mostrar el puerto 135/TCP como abierto, mientras que un análisis realizado al mismo tiempo y con las mismas opciones, pero desde Internet, puede presentarlo como filtrado.

- **Abierto**

  Una aplicación acepta conexiones TCP o paquetes UDP en este puerto. El encontrar esta clase de puertos es generalmente el objetivo primario de realizar un sondeo de puertos.

  Los encargados de la seguridad saben que cada puerto abierto es un vector de ataque. Los atacantes y las personas que realizan pruebas de intrusión intentan aprovechar puertos abiertos, por lo que los administradores intentan cerrarlos, o protegerlos con cortafuegos, pero sin que los usuarios legítimos pierdan acceso al servicio.

  Los puertos abiertos también son importantes en sondeos no relacionados con la seguridad porque indican qué servicios están disponibles para ser utilizados en una red.

- **Cerrado**

Un puerto cerrado es accesible; recibe y responde a las sondas de Nmap, pero no tiene una aplicación escuchando en él. Pueden ser útiles para determinar si un equipo está activo en cierta dirección IP (mediante descubrimiento de sistemas, o sondeo ping), y es parte del proceso de detección de sistema operativo.

Como los puertos cerrados son alcanzables, pues no se encuentran filtrados, es necesario puede analizarlos pasado un tiempo determinado, en caso de que alguno se abra. Los administradores pueden considerar el bloqueo de estos puertos con un cortafuegos. Si se bloquean aparecerían filtrados, como se discute a continuación.

- **Filtrado**

Nmap no puede determinar si el puerto se encuentra abierto porque un filtrado de paquetes previene que sus sondas alcancen el puerto. El filtrado puede provenir de un dispositivo de cortafuegos dedicado, de las reglas de un router, o por una aplicación de cortafuegos instalada en el propio equipo.

Estos puertos suelen frustrar a los atacantes, porque proporcionan muy poca información. Algunas veces responden con mensajes de error ICMP del tipo 3, código 13 (destino inalcanzable: comunicación prohibida por administradores), pero los filtros que sencillamente descartan las sondas sin responder son mucho más comunes.

Lo anterior fuerza a Nmap a reintentar varias veces, considerando que la sonda pueda haberse descartado por congestión en la red en vez de haberse filtrado.

- **No Filtrado**

  Indica que el puerto es accesible, pero que Nmap no puede determinar si se encuentra abierto o cerrado. Solamente el sondeo ACK, utilizado para determinar las reglas de un cortafuegos, clasifica a los puertos según este estado. El analizar puertos no filtrados con otros tipos de análisis, como el sondeo Windows, SYN o FIN, pueden ayudar a determinar si el puerto se encuentra abierto.

- **Abierto | Filtrado**

  Nmap marca a los puertos de esta forma cuando no puede determinar si el puerto se encuentra abierto o filtrado. Esto ocurre para tipos de análisis donde no responden los puertos abiertos.

  La ausencia de respuesta puede también significar que un filtro de paquetes ha descartado la sonda, o que se elimina cualquier respuesta asociada. De esta forma, Nmap no puede saber con certeza si el puerto se encuentra abierto o filtrado. Los sondeos UDP, protocolo IP, FIN, Null y Xmas clasifican a los puertos de esta manera.

- **Cerrado | Filtrado**

  Estado utilizado cuando Nmap no puede determinar si un puerto se encuentra cerrado o filtrado, y puede aparecer sólo durante un sondeo IPID pasivo.

Además de la tabla de puertos, Nmap puede dar información adicional sobre los objetivos, incluyendo el nombre de DNS según la resolución inversa de la IP, un listado de sistemas operativos posibles, los tipos de dispositivo, y direcciones MAC.

3.3.3 CONTROL DE TIEMPO Y RENDIMIENTO

Una de las prioridades durante el desarrollo de Nmap ha sido siempre el rendimiento. Un sondeo por omisión de cualquier sistema en una red local tarda un quinto de segundo. Esto tiempo es aun menor que el de un parpadeo, pero se va sumando al tiempo que tarda realizar un sondeo sobre decenas, centenares o miles de equipos. Además, ciertas opciones de sondeo como puedan ser el sondeo UDP y la detección de versiones pueden incrementar los tiempos de sondeos de forma sustancial.

También puede afectar a este tiempo configuraciones de sistemas cortafuegos, especialmente cuando implementan limitaciones a la tasa de respuestas. Aunque Nmap trabaja en paralelo y tiene muchos algoritmos avanzados para acelerar estos sondeos, el usuario tiene el control en última instancia de cómo funciona éste.

Los usuarios con experiencia pueden definir las órdenes a Nmap cuidadosamente para obtener sólo la información que necesitan mientras que, al mismo tiempo, cumplen las limitaciones de tiempo que tengan.

Algunas técnicas que pueden ayudar a mejorar los tiempos de sondeo son el limitar el número de pruebas que no sean críticas y actualizar a la última versión de Nmap (se hacen mejoras de rendimiento con cierta frecuencia). La optimización de los parámetros de control de tiempo puede introducir también diferencias significativas.

WiNmap es una herramienta del GUI de Windows para el nmap. Se basa en el Nmap v3.95. Para que fuese una herramienta fácil de utilizar WinNmap se diseñó con un esquema similar al del front-end para GTK, pero con más opciones. Como herramienta GUI el usuario podrá utilizarla con simplemente la selección de opciones. Esta versión de Nmap vuelve fácil el uso de este en ambiente Win32.

3.4 MySQL

MySQL es uno de los Sistemas Gestores de bases de Datos (SQL) más populares desarrolladas bajo la filosofía de código abierto. La desarrolla y mantiene MySQL AB, pero puede utilizarse gratuitamente y su código fuente está disponible.

3.4.1 CARACTERÍSTICAS (VERSIÓN 4.0 EN ADELANTE)

Inicialmente, MySQL carecía de elementos considerados esenciales en las bases de datos relacionales, tales como integridad referencial y transacciones. A pesar de ello, atrajo a los desarrolladores de páginas Web con contenido dinámico, justamente por su simplicidad; aquellos elementos faltantes fueron completados mediante aplicaciones que la utilizan.

Poco a poco los elementos faltantes en MySQL están siendo incorporados tanto por desarrollos internos, como por desarrolladores de software libre. Entre las características disponibles en las últimas versiones se puede destacar:

- Amplio subconjunto del lenguaje SQL.
- Disponibilidad en gran cantidad de plataformas y sistemas.
- Diferentes opciones de almacenamiento según requerimientos de velocidad en las operaciones o el mayor número de operaciones disponibles.
- Transacciones y claves foráneas.
- Conectividad segura.
- Replicación.
- Búsqueda e indexación de campos de texto.

Una base de datos es una colección estructurada de datos. Esta puede ser desde una simple lista de compras al inventario de una galería. Para agregar, acceder y procesar datos guardados en un computador, se requieren un software administrador de base de datos como MySQL.

MySQL es un sistema de administración relacional de bases de datos. Una base de datos relacional archiva datos en tablas separadas en vez de colocar todos los datos en un gran archivo. Esto permite velocidad y flexibilidad. Las tablas están conectadas por relaciones definidas que hacen posible combinar datos de diferentes tablas sobre pedido.

Las instrucciones utilizadas para interactuar con la base de datos y la aplicación son descritas a continuación:

3.4.1.1 CLÁUSULA SELECT

La recuperación de los datos en el lenguaje SQL se realiza mediante la sentencia SELECT, seleccionar. Esta sentencia permite indicar al SGBD la información que se quiere recuperar. Esta es la sentencia SQL, con diferencia, más habitual. La sentencia SELECT consta de cuatro partes básicas:

- La cláusula SELECT seguida de la descripción de lo que se desea ver, los nombres de las columnas a seleccionar. Esta parte es obligatoria.
- La cláusula FROM seguida de la especificación de las tablas de las que se han de obtener los datos. Esta parte es obligatoria.
- La cláusula WHERE seguida por un criterio de selección, una condición. Esta parte es opcional.
- La cláusula ORDER BY seguida por el criterio de ordenación. Esta parte es opcional.

Un ejemplo básico de esta sentencia se presenta a continuación:

```
SELECT {* | {columna,}+}
FROM {tabla,}+
[WHERE condición]
[ORDER BY {expresiónColumna [ASC | DESC],}+];
```

Como una primera utilización de la sentencia SELECT podemos utilizarla para ver todas las tablas que tenemos en la base de datos.

3.4.1.2 CLÁUSULA FROM

La cláusula FROM define las tablas de las que se seleccionaran las columnas.

Es posible añadir al nombre de las tablas el usuario propietario de las mismas de la forma *usuario.tabla*, de esta manera podemos distinguir entre las tablas de un usuario y otro. Oracle siempre considera como prefijo el nombre del propietario de las tablas, aunque no se lo indiquemos. De esta forma dos o más usuarios pueden tener tablas con igual nombre pero se evita el surgimiento de conflictos. Si se desea acceder a las filas de la tabla X del usuario Y, (además de los privilegios de lectura sobre esa tabla) debe escribirse una sentencia SQL similar a:

```
SQL> select * from Y.X;
```

Además pueden asociarse alias a las tablas para abreviar los nombres de estas.

3.4.1.3 CLÁUSULA WHERE

Hasta este momento se ha considerado el uso de la sentencia SELECT para recuperar todas las columnas o un subconjunto de ellas de una tabla. Pero este afecta a todas las filas de la tabla, a menos que especifiquemos algo más en la cláusula WHERE. Es aquí donde debe proponerse la condición que han de cumplir todas las filas para salir en el resultado de la consulta. La complejidad del criterio de búsqueda es prácticamente ilimitada, y en él se pueden conjugar operadores de diversos tipos con funciones de columnas, componiendo expresiones hasta cierto punto menos complejas, los operadores a utilizar son:

- ***Operadores de Comparación***
  - ***=, <, > Igualdad, mayor, menor entre otros.***
- ***Operadores aritméticos***
  - ***+, -, *, / suma, resta multiplicación, division***
- ***Operadores de cadenas de caracteres***
  - ***|| concatenación***

3.4.1.4 BORRADO

Con insertar y modificar, la otra operación que completa el trío es la de borrado de filas. La sintaxis es la que sigue:

DELETE FROM tabla [WHERE condición];

Borrará todas las filas que cumplan la condición especificada en la cláusula WHERE. Si esta cláusula no se fija, se borrarán todas las filas de la tabla. Aquí cabe decir que aunque con DELETE borremos todas las filas de una tabla, no borramos la definición de la tabla del diccionario y podemos insertar datos posteriormente en la tabla.

CAPITULO IV
APLICACION

4.1 ANÁLISIS DE LOS REQUERIMIENTOS DEL SISTEMA

4.1.1 PROCESO DE SUBNETEO

Para el proceso de descubrimiento es esencial conocer el rango de direcciones que se exploraran, por tal razón el formulario inicial cuenta con campos en los que el administrador deberá introducir una dirección IP y posteriormente la máscara de sub red; con lo anterior se realizan los cálculos necesarios para determinar la cantidad de direcciones que han de analizarse.

4.1.2 DETECCIÓN DE DISPOSITIVOS EN REDES ETHERNET

El sistema presentado es capaz de descubrir dispositivos en redes tipo Ethernet tales como computadoras personales, switches administrables y routers; es necesario que dichos equipos posean una dirección IP asignada y que esta se encuentre en los valores del rango ingresado en el formulario inicial. Para realizar el proceso de descubrimiento de los dispositivos de red se utilizan esencialmente los protocolos *ARP* e *ICMP*. El proceso realizado en conjuntamente por dichos protocolos se explicara detalladamente mas adelante.

4.1.3 DIAGRAMACIÓN DE LOS DISPOSITIVOS DE RED DETECTADOS

Cuando se han descubierto todas las direcciones IP que se encuentran asignadas al rango calculado, el sistema muestra un icono genérico para cada una de las direcciones en las que se detecta un dispositivo; para colocar un icono que represente lo que en realidad es este como por ejemplo un host, switch o un router en el dispositivo monitoreado deberá estar activo un agente de SNMP.

4.1.4 DESPLIEGUE DE DATOS DE DISPOSITIVOS DESCUBIERTOS

El sistema se encarga de mostrar la información básica de los dispositivos descubiertos, los datos a desplegar respecto a los diferentes dispositivos se muestran a continuación:

- Nombre
- Descripción
- Número de procesos en ejecución
- Número de interfaces
- Estado de interfaces
- Dirección física
- Dirección lógica
- Valores de uso de memoria
- Valores de uso de cpu

Para la obtención de los valores mencionados anteriormente se utiliza el protocolo de gestión *SNMP* el cual solicita estos valores mediante peticiones *GET, GETNEXT Y GETBULK*, debe tenerse en cuenta que para realizar el proceso que permite mostrar estos valores deberá activarse un agente de SNMP en el dispositivo objetivo, caso contrario se desplegara una notificación acerca de la no existencia de dicho agente.

4.1.5 REVISIÓN DE ESTADOS DE PUERTOS

Se proveerá al sistema la capacidad de realizar un escaneo de puertos para cada host descubierto con el fin de conocer cuales de ellos están siendo utilizados por la estación y de esta forma saber cuales son los servicios de red disponibles en ella.

4.1.6 CÁLCULO DE ESTADÍSTICAS

El sistema será capaz obtener estadísticas de los dispositivos descubiertos. Los valores que se calcularan periódicamente son:

- Memoria
- Uso de cpu
- Paquetes recibidos

4.1.7 ESTABLECIMIENTO DE ALARMAS

El administrador será capaz de configurar las alarmas del sistema especificando parámetros como:

- No respuesta a una petición de eco
- Uso excesivo de procesador (Valor de CPU mayor al establecido por el administrador de red, 50% como valor preestablecido)

4.1.8 MAPEO DE DISPOSITIVOS

El sistema realiza el mapeo de los dispositivos presentes en la red bajo estudio, a nivel de capa 3 del modelo OSI. El proceso consiste en la presentación de la ruta de interconexión que permite el intercambio de información desde los routers descubiertos a los diferentes elementos presentes en la red.

4.2 REQUERIMIENTOS PARA LA EJECUCIÓN DEL SISTEMA.

La aplicación necesita ejecutarse sobre una estación que posee las siguientes aplicaciones:

SOFTWARE

- **Sistema Operativo Microsoft Windows XP Profesional**

  Windows XP proporciona un nivel de estabilidad que permite la administración de manera eficiente los recursos del sistema, por lo que mantiene el sistema funcionando tan rápido como sea posible aún si se ejecutan múltiples aplicaciones simultáneamente.

  Para responder a fallos inesperados se cuenta con herramientas que permiten regresar el sistema a fechas previas en las que este se ejecutaba eficientemente.

- **WinPcap 3.1**

  Como se explico en el capitulo anterior WinPcap es una biblioteca abierta para la captura de paquete y análisis de red para las plataformas Win32. La interfaz de programación de WinPcap puede ser utilizada por muchas tipos herramientas de red para el análisis, localización de fallas, seguridad y control.

- **Net-SNMP 5.3.0.1**

  Net-SNMP es una serie de aplicaciones utilizadas para la implementación del protocolo SNMP en sus diferentes versiones SNMP v1, SNMP v2c y SNMP v3 que utilizan IPV4 al igual que

IPV6. La serie debe compilar y debe correr en plataformas Win32, inclusive la biblioteca, la línea de comandos ordena-línea y la estructura básica del agente. El agente utilizado incluye actualmente apoyo para el módulo MIB-II, pero se requiere la previa instalación de la Plataforma Central SDK de Microsoft.

- **WiNmap**

Diseñada para plataformas Win32, WiNmap permite el análisis rápido de redes de gran tamaño mediante una interfaz amigable como las aplicaciones basadas en ventanas, se debe instalar Nmap previo a la utilización de esta herramienta.

- **MySQL**

MySQL uno de los Sistemas Gestores de bases de Datos (SQL) más populares desarrolladas bajo la filosofía de código abierto. La desarrolla y mantiene MySQL AB, pero puede utilizarse gratuitamente y su código fuente está disponible

HARDWARE

- Espacio libre en Disco Duro: 50MB
- Velocidad de procesador: 1GHz o superior
- Memoria RAM: 128MB o superior
- CD-ROM o unidad de DVD

4.3 DESCRIPCIÓN DEL FUNCIONAMIENTO DEL SISTEMA

4.3.1 PROCESO DE SUBNETEO

El primer paso que el sistema realiza para el descubrimiento de los dispositivos de red es obtener el rango que direcciones en las cuales este se encuentra. Para ello el formulario inicial del sistema permite al usuario introduzca una dirección IP y una máscara de red, con estos datos el sistema automáticamente genera el rango de direcciones a analizar.

Por ejemplo si se introduce la dirección IP 192.168.1.2 y una máscara 255.255.255.240 se realiza una operación AND para obtener la dirección de sub red y a la vez determinar la cantidad de direcciones que se han de revisar; para este caso se debe convertir la esta máscara de red a formato binario con lo que el valor 240 se vuelve 11110000 lo cual indica 2^4 direcciones de host, si extraemos la dirección de red y la de broadcast tendremos 14 direcciones asignables las cuales serán las que se utilizarán en el proceso de descubrimiento, es decir será analizado el rango desde 192.168.1.1 hasta 192.168.1.14.

4.3.2 DETECCIÓN DE DISPOSITIVOS EN LA RED ETHERNET

Para realizar el proceso de descubrimiento de los dispositivos de red se utilizan los protocolos ARP e ICMP. A continuación se presenta diagrama de flujo en el que se describe dicho proceso.

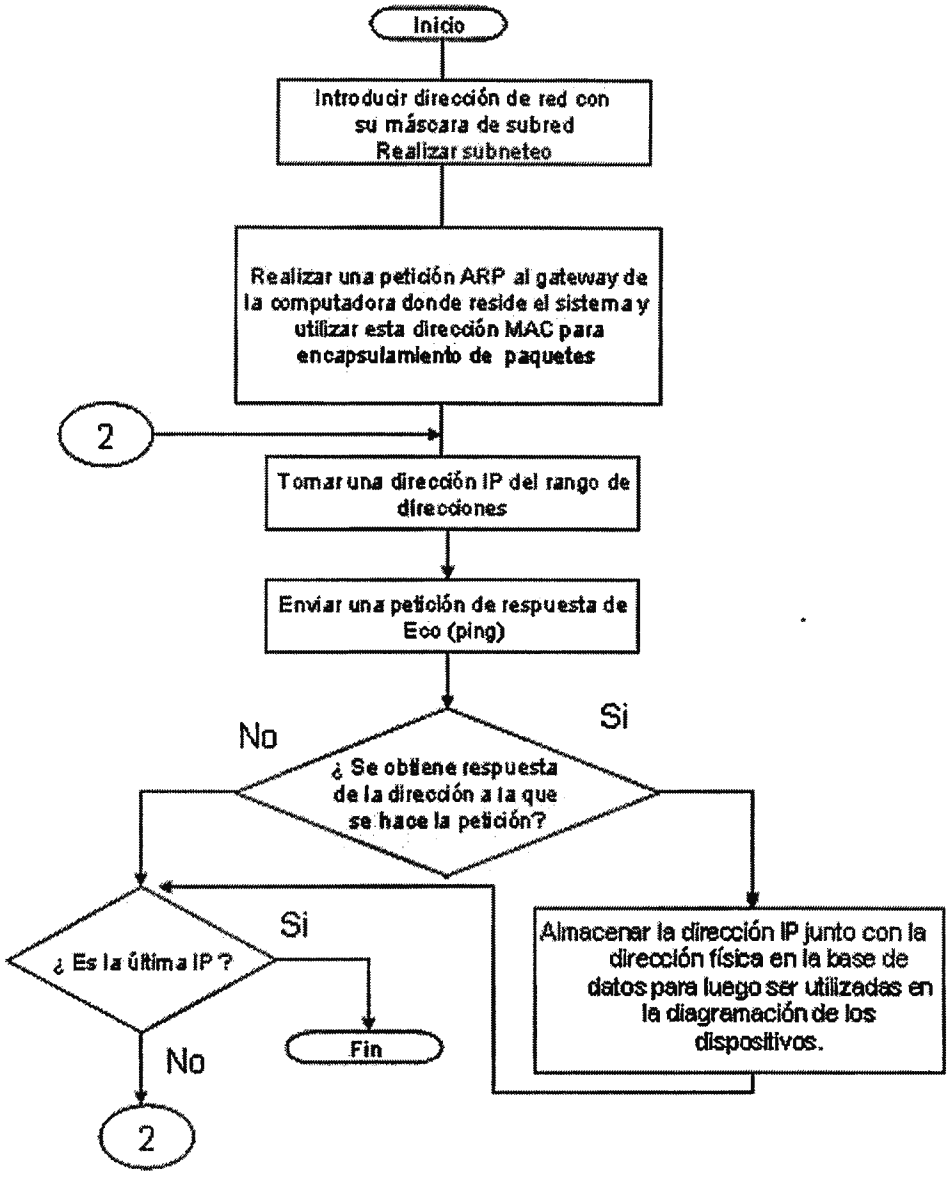


Fig. 14 – Diagrama de descubrimiento de red

4.3.3 DESPLIEGUE DE LOS DISPOSITIVOS DE RED DESCUBIERTOS

Cuando se han descubierto todas las direcciones IP que se encuentran asignadas, el sistema muestra un icono genérico para cada una de ellas pero si estos tienen el agente SNMP levantado entonces es posible colocar un icono que represente lo que realmente es por ejemplo un host, switch o un router.

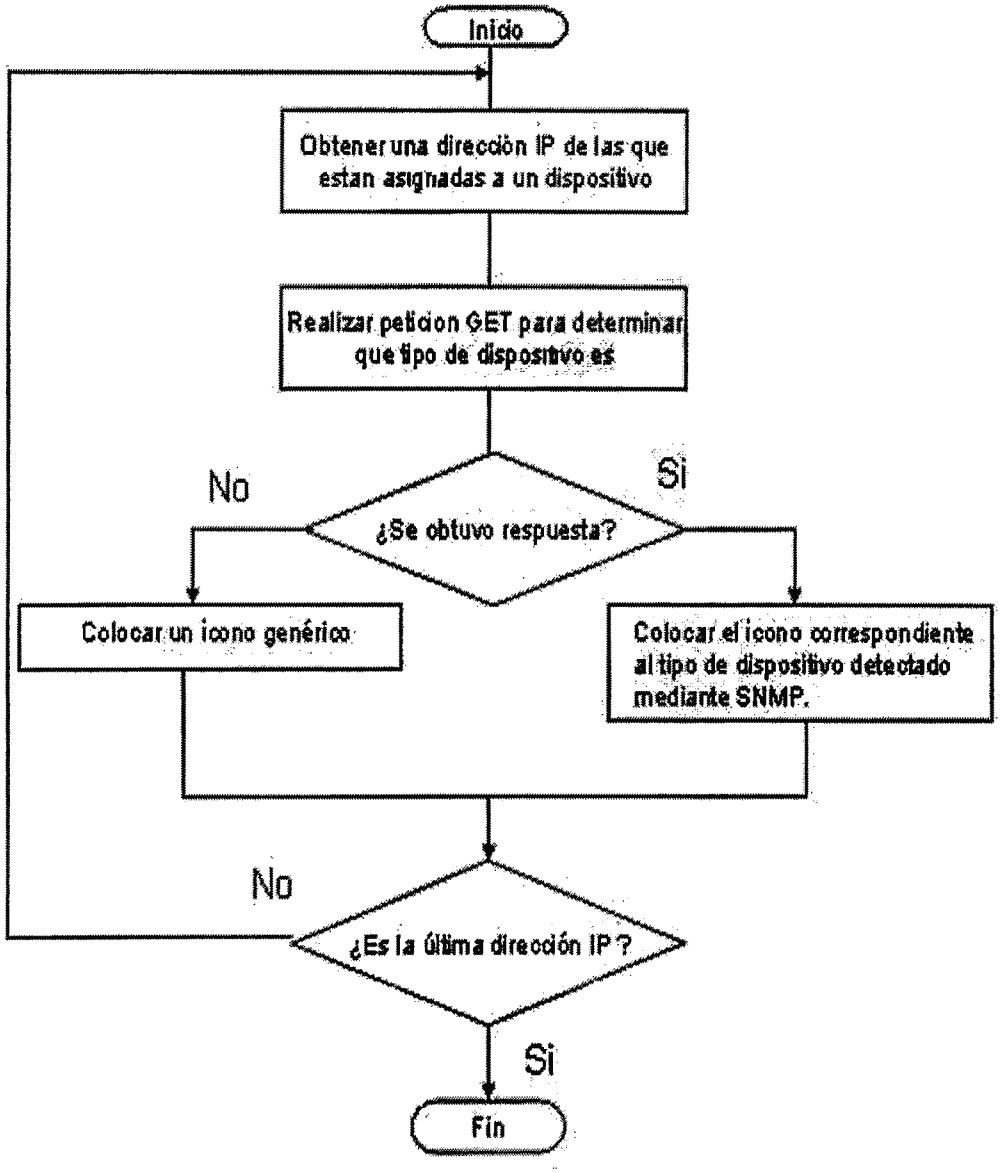


Fig. 15 – Diagramación de dispositivos

4.3.4 DESPLIEGUE DE DATOS DE DISPOSITIVOS DESCUBIERTOS

Para obtener la información referente a cada dispositivo detectado se utiliza el protocolo SNMP mediante el cual se realizan peticiones GET, GETNEXT y GETBULK según sea el caso con el fin de obtener los valores deseados, a continuación se presenta el algoritmo que se sigue para llevar a cabo esta acción:

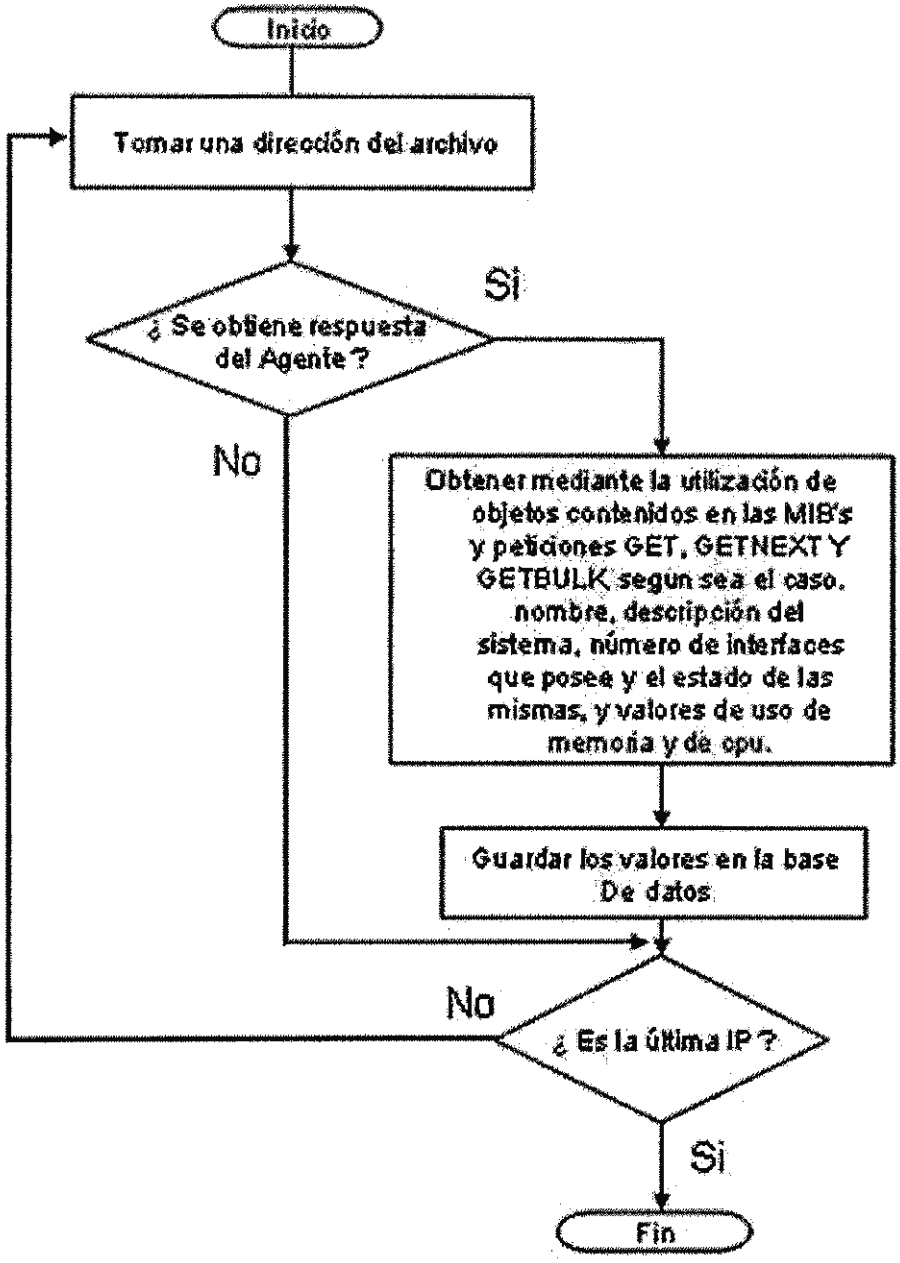


Fig. 16 – Obtención de datos mediante SNMP

4.3.5 REVISIÓN DE ESTADOS DE PUERTOS

Para el desarrollo de este modulo del sistema se utilizo la herramienta de código abierto para exploración de red y auditoria de seguridad *Nmap*. De dicha herramienta se utilizan los recursos para realizar el escaneo de puertos sobre el dispositivo deseado, con ello podemos conocer los puertos que se encontraban abiertos en el dispositivo estudiado al momento de realizar la solicitud de análisis.

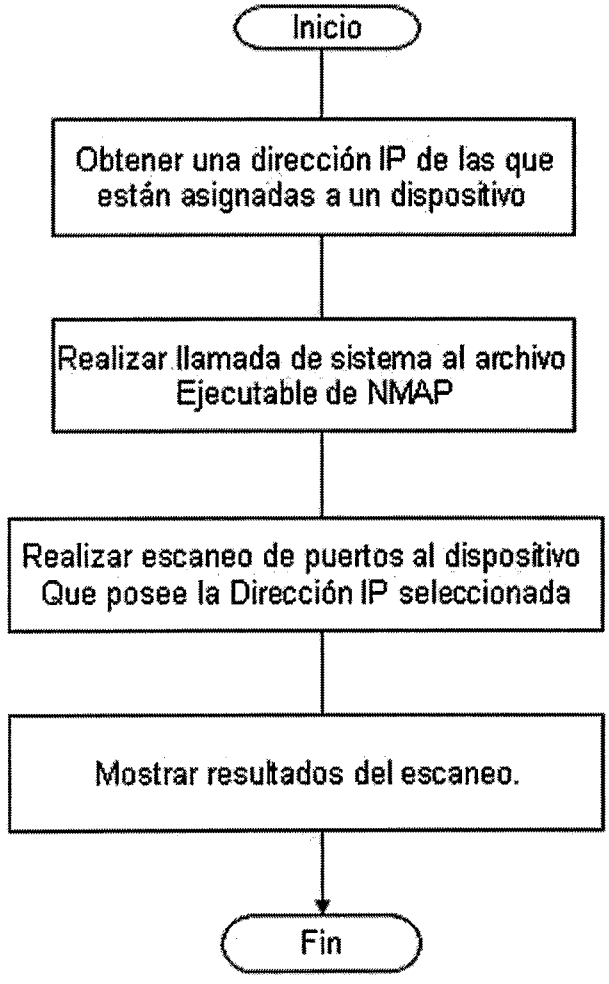


Fig. 17 – Revisión de estado de puertos

4.3.6 CÁLCULO DE ESTADÍSTICAS

La aplicación presenta datos estadísticos determinados por el usuario. Los valores a calcular son: memoria, uso de cpu y paquetes recibidos. El diagrama mostrado a continuación es el procedimiento a seguir para la obtención de estadísticas.

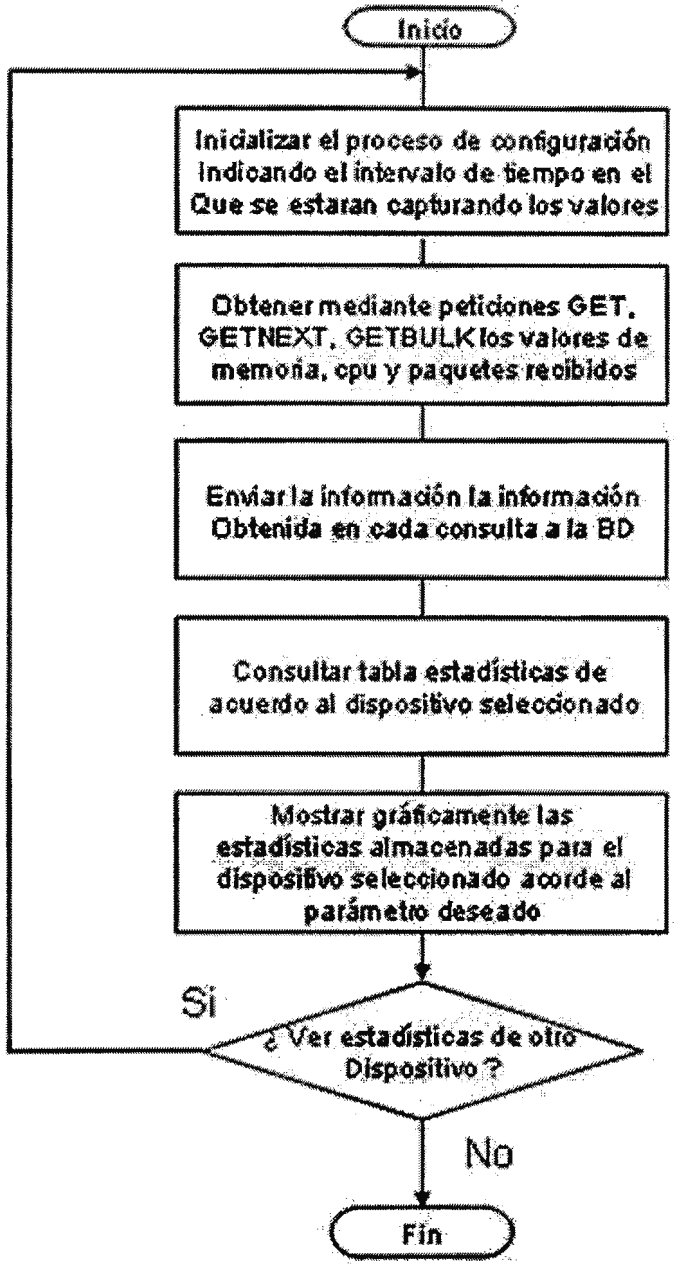


Fig. 18 – Cálculo de estadísticas

4.3.7 MAPEO DE DISPOSITIVOS

La realización del mapeo de los diferentes elementos de la red se basa en la ejecución del proceso descrito a través del diagrama que se presenta a continuación.

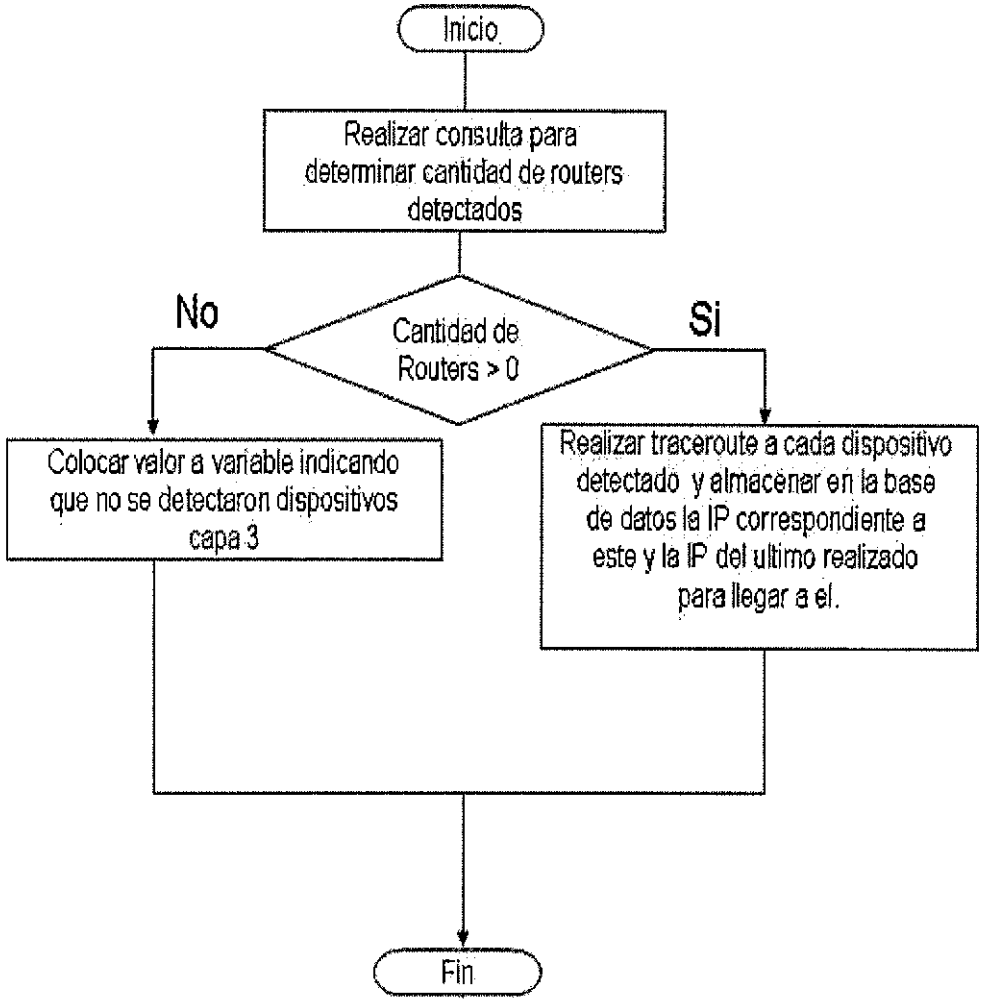


Fig. 19 – Mapeo de Dispositivos

4.3.8 ESTABLECIMIENTO DE ALARMAS

El sistema de monitoreo determina cuando uno de los elementos de la red tiene un comportamiento que pueda interferir con el funcionamiento correcto de la misma. El estableciendo de alarmas se basa en el envió permanente de peticiones de eco (PING) a los dispositivos presentes para determinar su existencia en la red en todo momento, esto se logra con el procedimiento mostrado a continuación.

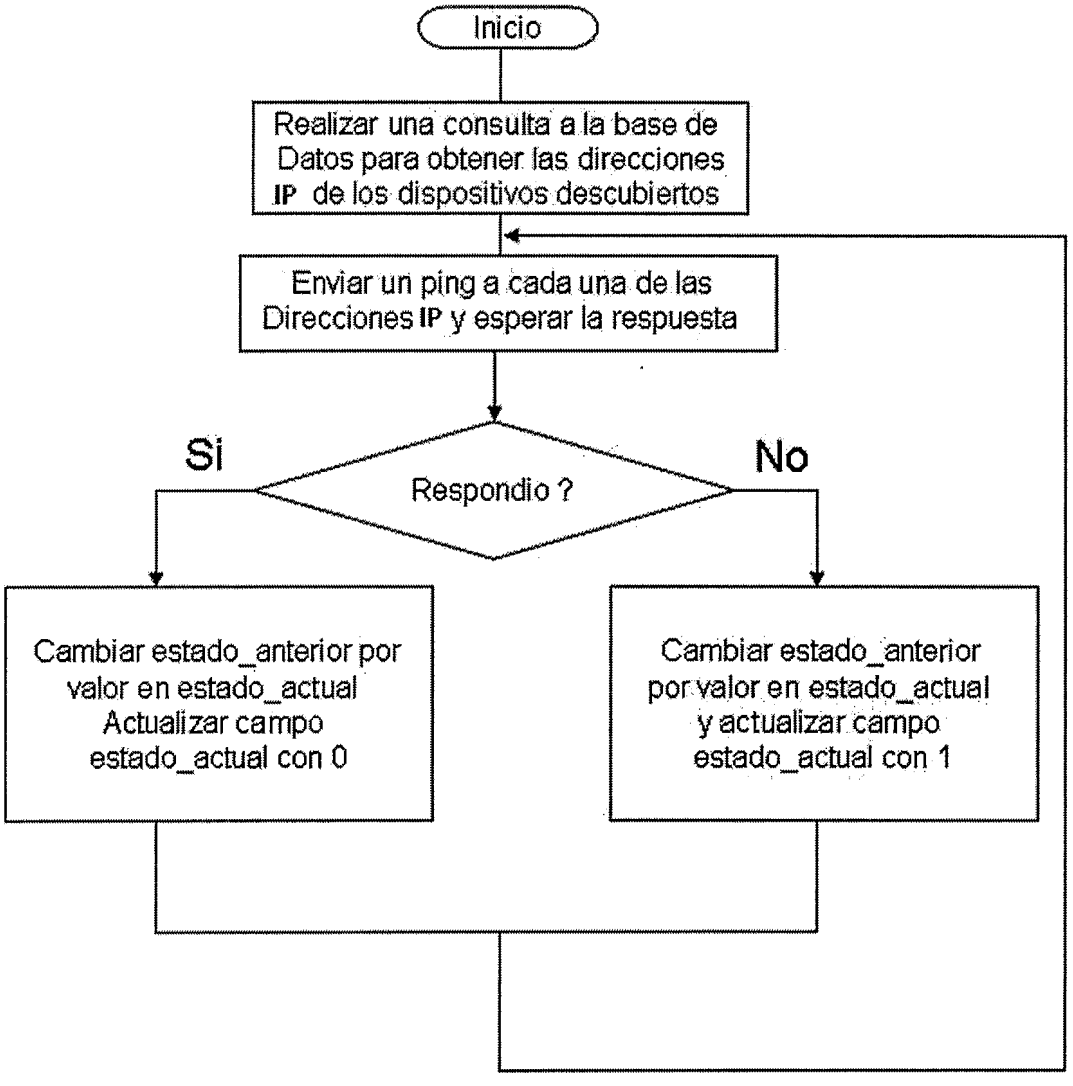


Fig. 20 – Establecimiento de alarmas por PING

Si existen cambios en el estado de los dispositivos en la petición realizada anteriormente el sistema cambiara el estado del elemento en la red según sea el caso. Si no se obtiene respuesta a las peticiones de eco un dispositivo detectado anteriormente se establece un valor de inalcanzable (1); por otra parte si el elemento en cuestión responde posteriormente a las peticiones siguientes reestablece su estado a normal (0). Lo anterior se demuestra en el diagrama siguiente.

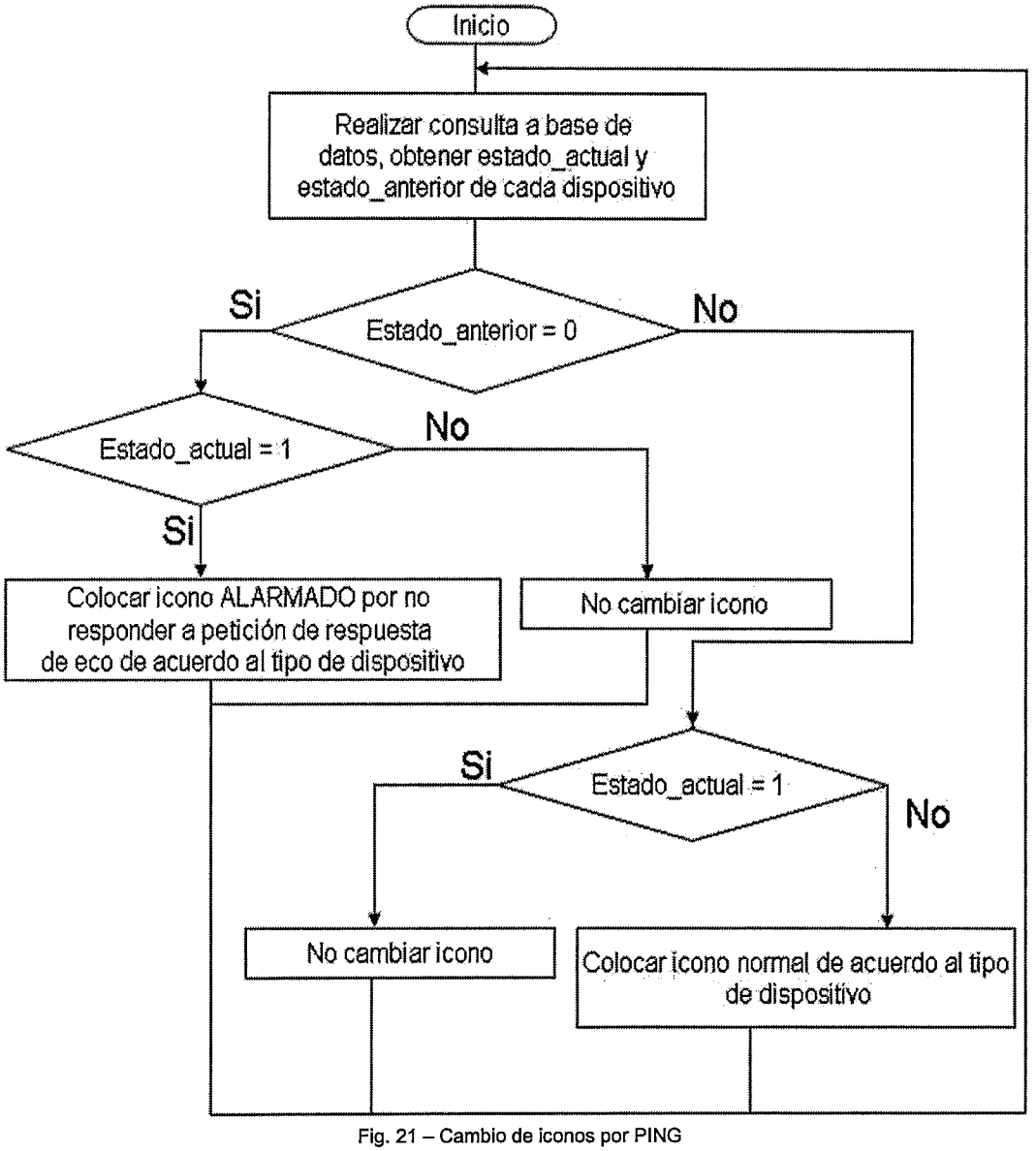


Fig. 21 – Cambio de iconos por PING

Por otra parte indica el sistema también informara si el funcionamiento de una estación de trabajo supera los valores tolerables por el procesador de estas (CPU), por lo que se activara una alarma si dicho valor supera el establecido por el administrador de red, 50% como valor por defecto, este valor se obtendrá al realizar el envió de peticiones de eco tal como se presenta en el diagrama de flujo siguiente.

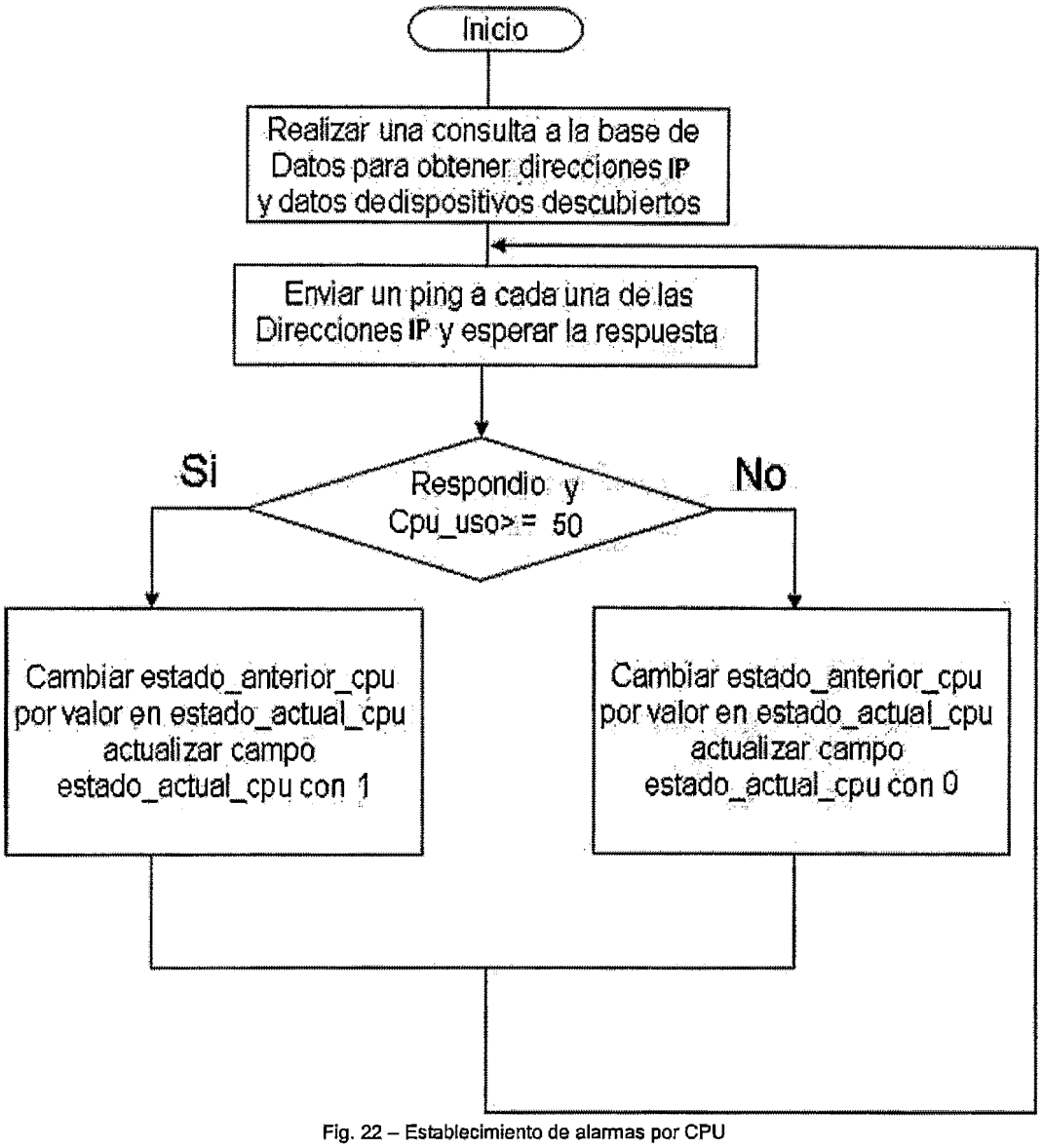


Fig. 22 – Establecimiento de alarmas por CPU

Si el valor de los uso del procesador es mayor al establecido por el administrador de red, como por ejemplo 50%, el sistema cambiara el estado del elemento en la red según sea el caso. Si el valor excede el uso tolerado se establece un valor de alarmado (1); por otra parte si el elemento en cuestión a disminuido el uso del procesador su estado vuelve a ser normal (0). Lo anterior se demuestra en el diagrama siguiente.

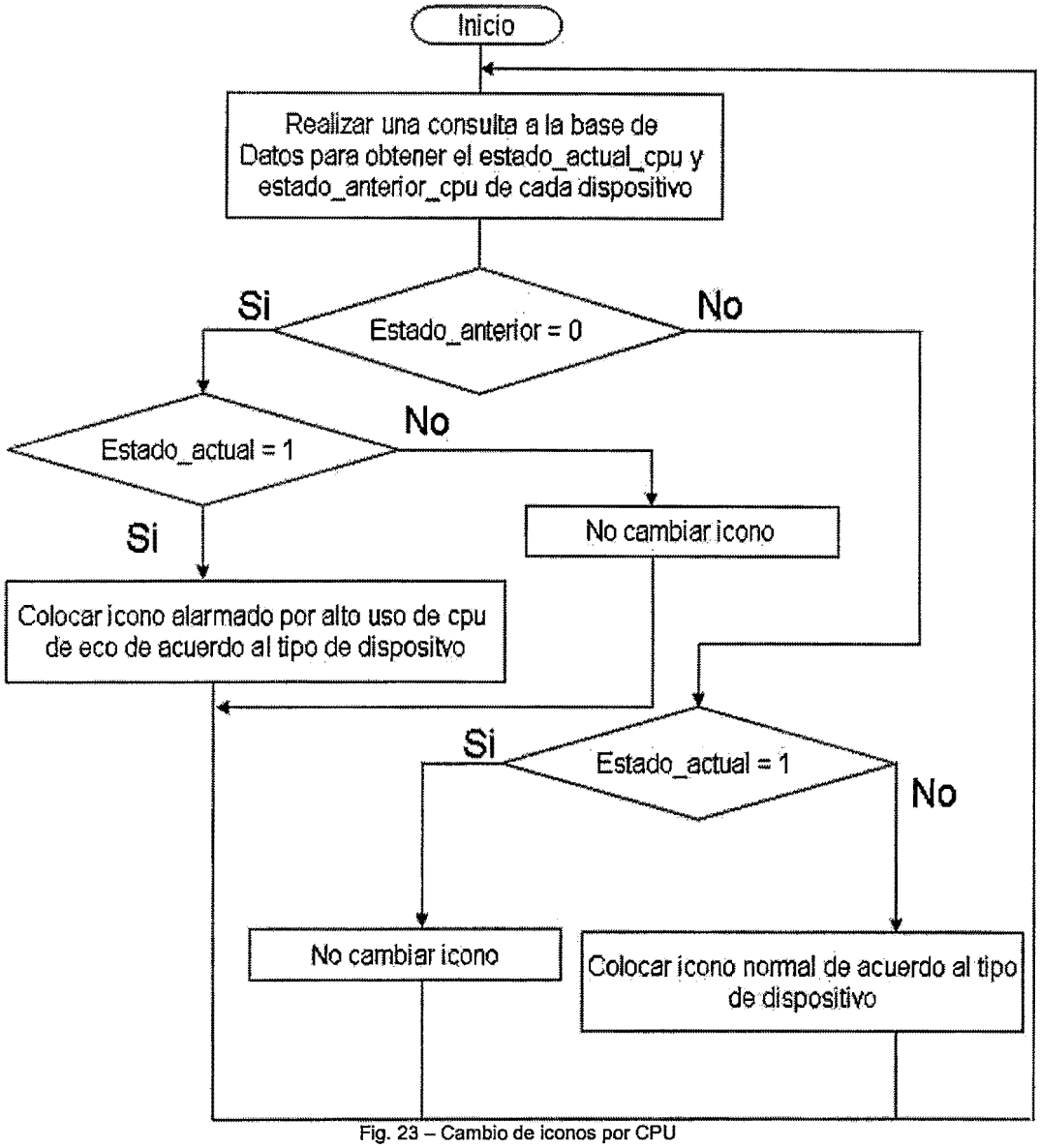


Fig. 23 – Cambio de iconos por CPU

4.3.9 DISEÑO DE LA BASE DE DATOS

DIAGRAMA ENTIDAD – RELACIÓN DE LA BASE DE DATOS

A continuación se muestran la estructura de la base de datos utilizada por la aplicación desarrollada así como los diferentes campos en cada una de ellas:

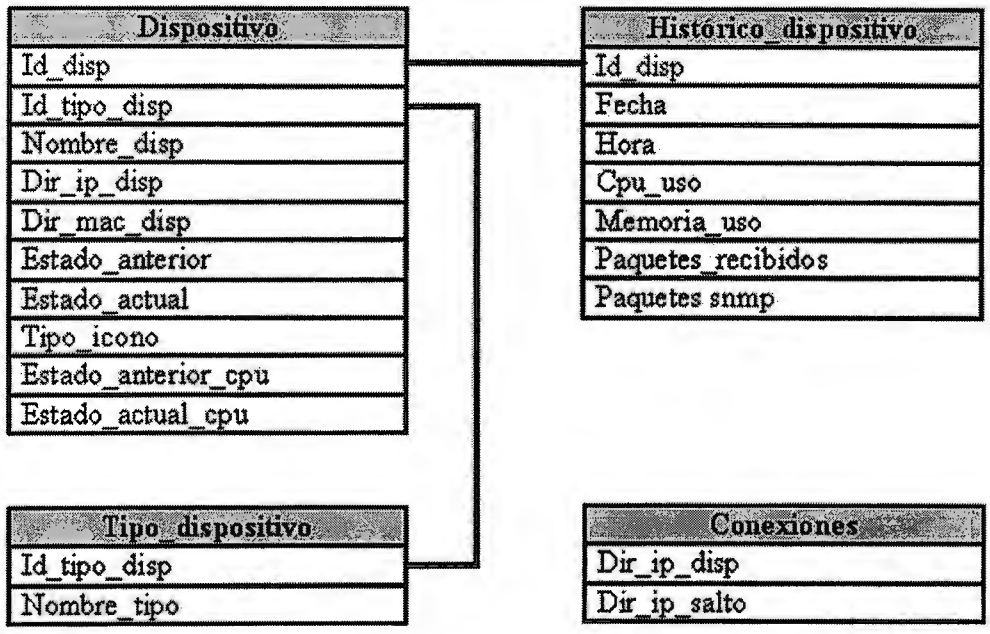


Fig. 24 – Diagrama Entidad-Relación

Dispositivos

Id_disp	Identificador único para cada dispositivo detectado soportado por el sistema
Id_tipo_disp	Identificador de los tipos de dispositivos existentes y en particular el tipo detectado
Nombre_disp	Nombre asociado al dispositivo detectado el cual se obtiene mediante una consulta SNMP, si el agente de este protocolo no esta ejecutándose en el dispositivo se colocara un nombre genérico "unknown"

Dir_ip_disp	Dirección IP asociada al dispositivo detectado
Dir_mac_disp	Dirección física, MAC, asociada al dispositivo descubierto
Est_anterior	Contiene el estado anterior en lo respectivo a alarmas de petición de respuesta de eco, si el valor es 0 su estado era normal pero si es 1 el dispositivo se encuentra alarmado.
Est_actual	Posee el estado actual en correspondiente a alarmado por petición de respuesta de eco, si el valor es 0 está normal, pero si es el valor es 1 está alarmado.
Tipo_icono	Este campo permite determinar que tipo de icono se colocara si un elemento se encuentra alarmado o su estado se normalice. Este valor puede modificarse al cambiar el icono que representa el dispositivo de red cuando se selecciona la opción propiedades del menú emergente.
Estado_anterior_cpu	Almacena el estado anterior correspondiente a alarmado de cpu, si el valor es 0 se encontraba en estado normal, sin embargo si el valor es 1 su estado fue alarmado.
Estado_actual_cpu	Este campo almacena el estado actual correspondiente a alarmado por CPU, el valor 0 indica que el dispositivo esta en estado normal, pero si dicho valor es 1 este dispositivo se encuentra alarmado.

Tipo Dispositivo

Id_tipo_disp	Identificador único para cada tipo de dispositivo detectado soportado por el sistema
Nombre_tipo	Nombre único asignado a cada tipo de dispositivo soportado

Histórico Dispositivo

Id_disp	Relaciona el registro con un dispositivo específico
Fecha	Almacena la fecha en la que el dato fue capturado
Hora	Almacena la hora en la que el dato fue capturado
Cpu_uso	Registra el porcentaje la unidad central de procesamiento, CPU, utilizado por el dispositivo analizado
Memoria_uso	Registra el porcentaje de memoria RAM utilizado por el dispositivo analizado
Paquetes_snmp	Almacena el número de paquetes en conjunto de los protocolos TCP, UDP e IP

Conexiones

Dir_ip_disp	Campo que almacena la dirección IP del dispositivo detectado a partir de la información de los router descubiertos que indican hacia cual de ellos se encuentra conectado.
Dir_ip_salto	Contiene la dirección IP del router desde el cual ha sido detectado el dispositivo al cual se encuentra conectado.

4.3.10 DIAGRAMACIÓN BÁSICA DE PROCESOS DE LA APLICACIÓN

A continuación se presentan los procesos básicos de la aplicación utilizados para la detección de los elementos de red:

La figura 20 presenta las entradas requeridas para la ejecución de la aplicación:

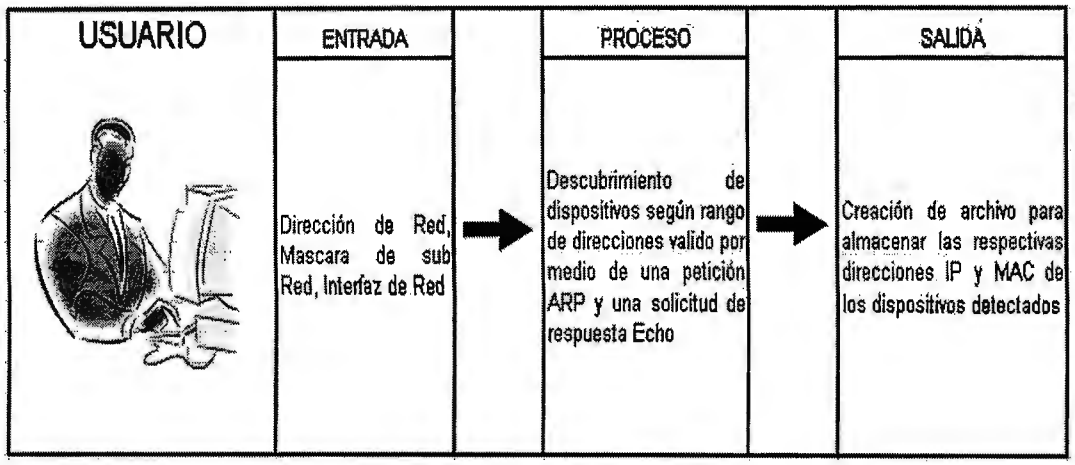


Fig. 25 – Entrada previas a la ejecución de la aplicación

Una vez se cuenta con las entradas del programa se prueba la conectividad con las diferentes direcciones IP del rango valido mediante una petición de echo:

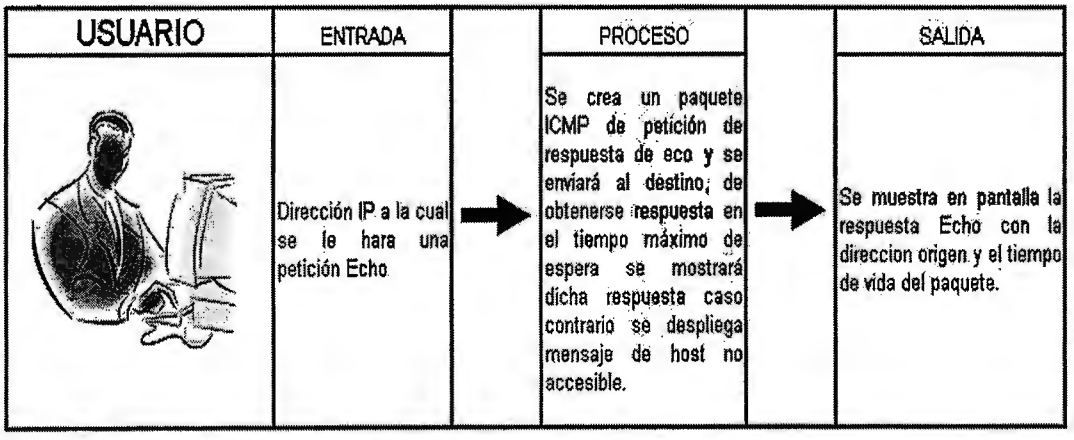


Fig. 26 – Prueba de conectividad mediante *ping*

Se posee la capacidad de detectar los saltos que deben realizarse para poder alcanzar un destino específico.

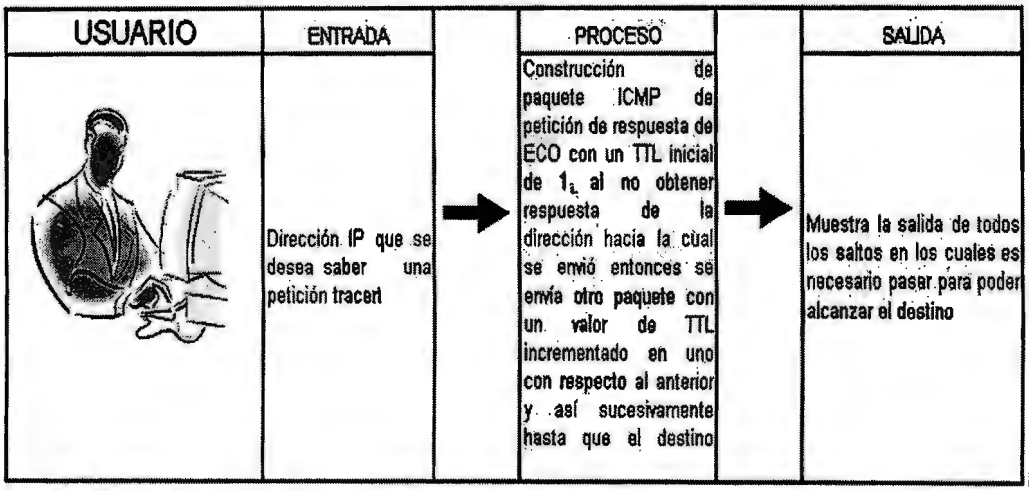


Fig. 27 – Detección de la ruta a un dispositivo

Cuando se detecten las direcciones IP en las cuales se encuentra un host, se procederá a la solicitud de información de este si el agente SNMP se encuentra activo.

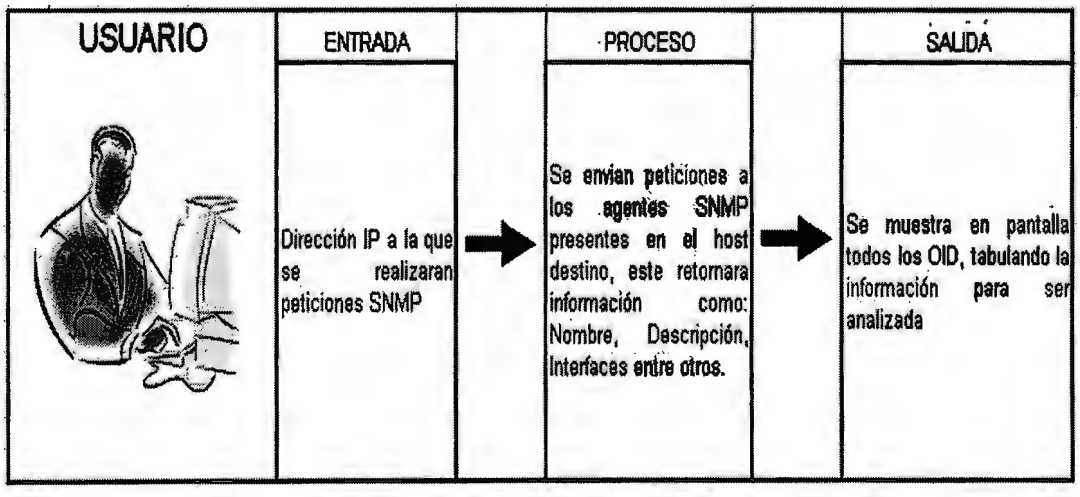


Fig. 28 – Solicitudes de datos a agentes SNMP

Finalmente cuando se posee la información deseada se procede al despliegue de los diferentes host en pantalla y el usuario podrá acceder a la información de ellos mediante los diferentes métodos

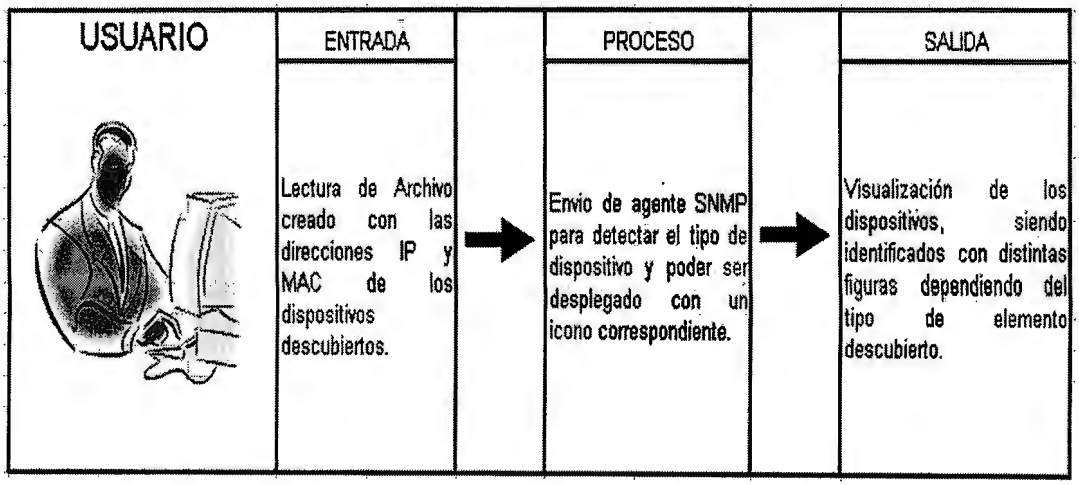


Fig. 29 – Despliegue de datos en pantalla

4.4 MÓDULOS A UTILIZAR

4.4.1 MÓDULO DE SUBNETEO

Para el desarrollo de este módulo se utilizó programación básica de C++ en la cual se incluyó el manejo de arreglos y de operaciones lógicas con el fin de realizar las operaciones que el procedimiento requería.

4.4.2 MODULO DE DETECCION DE DISPOSITIVOS EN LA RED ETHERNET

Para el desarrollo de este módulo se utilizó la librería Winpcap 5.1 la cual permite el encapsulamiento y envío de paquetes, así mismo el Ethereal ya que un programa de captura de tramas de red, permite conocer la estructura completa de un paquete, en este caso fue de suma importancia para comprender la estructura que poseen los paquetes de los protocolos ARP e ICMP. Estos son los que hacen posible el descubrimiento de los dispositivos.

Inicialmente se encapsula una petición ARP tomando la dirección IP que se desea saber, una de las que se encuentran en el rango previamente calculado; al obtenerse una respuesta se procede al envió de una petición de respuesta de eco y si en esta dirección IP que responde es a la que se le hizo la solicitud se obtiene un "*nuevo dispositivo descubierto*". Una vez completo el proceso para este host se procede a recopilar los datos, dirección IP y dirección física (MAC), en un archivo de texto. Este proceso se repite hasta agotar el rango de direcciones.

4.4.3 DESPLIEGUE DE INFORMACIÓN BÁSICA DE DISPOSITIVOS DESCUBIERTOS

Para realizar este procedimiento se utiliza el protocolo SNMP ya que mediante el se puede acceder al valor de los objetos contenidos en las MIB de los sistemas. Para esto se ha utilizado la librería Net SNMP 5.3.0.1-1 la cual es de licencia GPL y presenta las estructuras necesarias para la realización de todo tipo de procedimientos utilizando el protocolo SNMP.

En este sistema se han utilizado las peticiones GET, GETNEXT y GETBULK de acuerdo al objeto que se requiera. A continuación se presenta una tabla con las MIB y los objetos que se han utilizado en esta parte del sistema.

AGENTE	DESCRIPCION
sysName .1.3.6.1.2.1.1.5.0	Contiene el nombre del dispositivo
sysDescr .1.3.6.1.2.1.1.1.0	Contiene una descripción completa del sistema: nombre, tipo de hardware, sistema operativo y software de networking.
sysUptime .1.3.6.1.2.1.1.3.0	Devuelve el tiempo de ejecución del agente SNMP en el dispositivo monitoreado.
hrMemorySize .1.3.6.1.2.1.25.2.2.0	Permite obtener la cantidad de memoria de RAM de un dispositivo
hrSystemProcesses .1.3.6.1.2.1.25.1.6.0	Contiene la cantidad de procesos que se están ejecutado en el sistema
ifNumber .1.3.6.1.2.1.2.1.0	Contiene el numero de interfaces que posee el dispositivo
IfAdminStatus .1.3.6.1.2.1.2.2.1.7.1 ó .2	Designa el estado en el cual se encuentra la interfase del dispositivo
IfType .1.3.6.1.2.1.2.2.1.3.2 ó .1	Tipo de interfase que posee un dispositivo (Ethernet, loopback entre otras)
hrSWRunPerfMem .1.3.6.1.2.1.25.5.1.1.2	Contiene la cantidad de memoria que consume cada proceso ejecutado en el sistema
IfPhysAddress .1.3.6.1.2.1.2.2.1.6.1 ó .2	contiene la dirección MAC los dispositivos si en un caso no tuviera una dirección IP
1.3.6.1.4.1.9.2.1.58 avgBusy5	CISCO-PROCESS-MIB, permite tener el porcentaje de uso de CPU de un equipo cisco durante los últimos 5 minutos
ciscoMemoryPoolFree .1.3.6.1.4.1.9.9.48.1.1.1.6	Indica el número de bytes de memoria que son actualmente disponibles en el dispositivo manejado
ciscoMemoryPoolLargestFree .1.3.6.1.4.1.9.9.48.1.1.1.7	Indica los bytes contiguos de memoria que son actualmente disponibles en el dispositivo manejado
ciscoMemoryPoolUsed .1.3.6.1.4.1.9.9.48.1.1.1.5	Indica el número de bytes de memoria actualmente usados por aplicaciones en el dispositivo manejado

Tabla 19 – MIBs utilizadas para despliegue de datos

4.4.4 REVISIÓN DE ESTADOS DE PUERTOS

Para el desarrollo de este modulo del sistema se utilizo la herramienta de código abierto para exploración de red y auditoria de seguridad *Nmap* a través de la interfaz WinNmap. De dicha herramienta se utilizan los recursos para realizar el escaneo de puertos sobre el dispositivo deseado, con ello podemos conocer los puertos que se encontraban abiertos en el dispositivo estudiado al momento de realizar la solicitud de análisis.

4.4.5 CÁLCULO DE ESTADÍSTICAS

Para la obtención de las estadísticas se utilizaran peticiones periódicas en un intervalo de tiempo que el usuario determine de los objetos correspondientes a memoria, CPU y paquetes recibidos de cada dispositivo. Para ello se utiliza la librería Net SNMP 5.3.0.1-1 en conjunto con la librería *time.h* propia de C/C++. A continuación se presenta una tabla con las MIB y los objetos que se han utilizado en esta parte del sistema.

OID	MIB	Función
hrSystemProcesses .1.3.6.1.2.1.25.1.6.0	Host Resources	Obtener el número de procesos que se están ejecutando en el sistema.
hrSWRunPerfMem .1.3.6.1.2.1.25.5.1.1.2	Host Resources	Obtener la cantidad de memoria consumida por cada proceso que se está ejecutando en el sistema.
hrMemorySize .1.3.6.1.2.1.25.2.2.0	Host Resources	Obtener la cantidad de memoria que posee el sistema.
tcpInSegs .1.3.6.1.2.1.6.10	RFC-1213	Obtener la cantidad de paquetes TCP recibidos desde que se inicializó el agente SNMP.
udpInDatagrams .1.3.6.1.2.1.7.1	RFC-1213	Obtener la cantidad de paquetes UDP recibidos desde que se inicializó el agente SNMP.
ipInReceives .1.3.6.1.2.1.4.3	RFC-1213	Obtener la cantidad de paquetes IP recibidos desde que se inicializó el agente SNMP.

Tabla 20 – MIB utilizadas para el calculo de estadísticas

4.4.6 DIAGRAMACIÓN DE LOS DISPOSITIVOS DE RED DETECTADOS

Para determinar que icono colocar al momento de desplegar gráficamente los dispositivos detectados el sistema se realiza una petición SNMP con el fin de obtener que tipo de dispositivo es el que se ha detectado, si se obtiene respuesta se coloca el icono correspondiente pero si no se obtiene respuesta entonces se coloca un icono genérico.

4.4.7 HERRAMIENTAS QUE POSEE EL SISTEMA

Con el fin de proveer herramientas de monitoreo al sistema, se han implementado formularios capaces de realizar peticiones de respuesta de eco (ping) así como también la opción de poder detectar la ruta de llegada hacia cualquier dispositivo de los que se han detectado a la red (traceroute).

4.4.7.1 HERRAMIENTA ICMP

El sistema es capaz de realizar una petición de respuesta de eco a cualquiera de los dispositivos detectados. A esta herramienta puede accederse por medio de dos métodos, la primera realizando un clic derecho sobre el icono del dispositivo al que se le quiere hacer ping, luego seleccione herramientas y finalmente elija *ping*; el segundo método consiste en acceder al menú herramientas que se encuentra en la parte superior del formulario principal y seleccionando ping de las opciones desplegadas.

Para su implementación se utilizó la librería Winpcap 3.1 mediante la cual se encapsula el paquete de petición de respuesta de eco y se envía al dispositivo destino, así mismo se verifican las respuestas que de este se obtienen.

4.4.7.2 HERRAMIENTA TRACER

El sistema es capaz de detectar la ruta utilizada para alcanzar cualquiera de los dispositivos detectados, para su implementación se utilizó la librería Winpcap 3.1 mediante la cual se encapsula el paquete de petición de respuesta de eco inicialmente con un tiempo de vida (TTL) de uno. Si no se obtiene respuesta del dispositivo al cual se realizó la petición se obtendrá en su lugar un valor de tiempo de vida excedido del cual se obtiene la dirección IP del

router que envía ese paquete, se procede a enviar otro paquete pero esta vez con el valor de TTL incrementado en uno y así consecutivamente hasta que se obtenga respuesta del dispositivo o se llegue a un límite de 30 paquetes enviados.

4.4.7.3 ESCANEO DE PUERTOS

El sistema es capaz de realizar un escaneo de puertos en los dispositivos detectados durante el sondeo inicial, para ello se utiliza la herramienta de código abierto para exploración de red y auditoria de seguridad *Nmap* en una de sus versiones para Windows WiNmap v1.2.

De dicha herramienta se utilizan los recursos para realizar el escaneo de puertos sobre el dispositivo deseado, con ello podemos conocer los puertos que se encontraban abiertos en el dispositivo estudiado al momento de realizar la solicitud de análisis.

CAPITULO V
FORMULARIOS

5.1 DISEÑO DE LOS FORMULARIOS A UTILIZAR

5.1.1 FORMULARIO DE INICIO

Al ejecutar la aplicación se presenta la ventana principal con el menú Archivo, figura 30, desde este menú podrá seleccionar la opción de ingreso de datos para descubrimiento de la red o salir de la aplicación en el momento en que se desee.

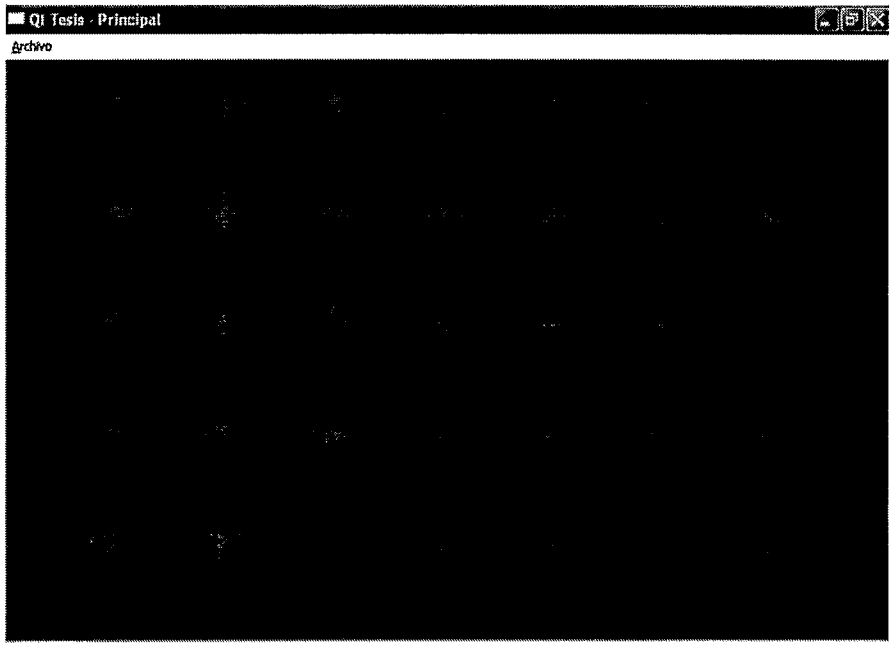


Fig. 30 – Formulario inicial

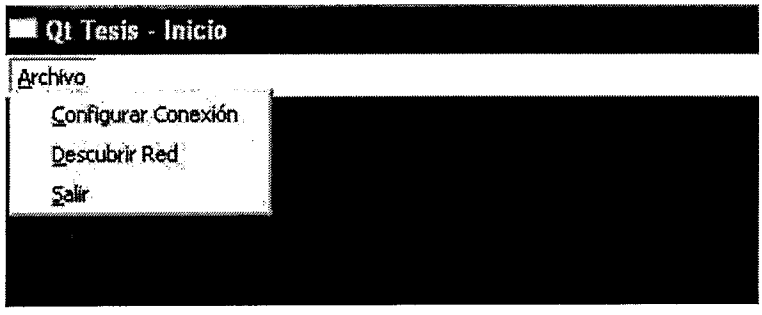


Fig. 31 – Menú Archivo en la ventana inicial

Como puede apreciarse en la imagen 31, el menú archivo de la ventana inicial cuenta con tres opciones:

- *Configurar Conexión*
- *Descubrir Red*
- *Salir*

La primera de ellas, *Configurar conexión*, permite establecer comunicación con el servidor que ejecuta la base de datos de la aplicación, para realizar dicha conexión deberán ingresarse los siguientes datos:

- *Servidor*, nombre del servidor MySQL
- *Usuario*, nombre establecido al configurar MySQL
- *Password*, consiste en establecida para limitar el acceso a la base de datos mediante una palabra clave conocida solamente por el administrador
- *Base de Datos*, nombre de la base de datos en la cual se almacena la información

La ventana de configuración del servidor se muestra a continuación en la figura 32:

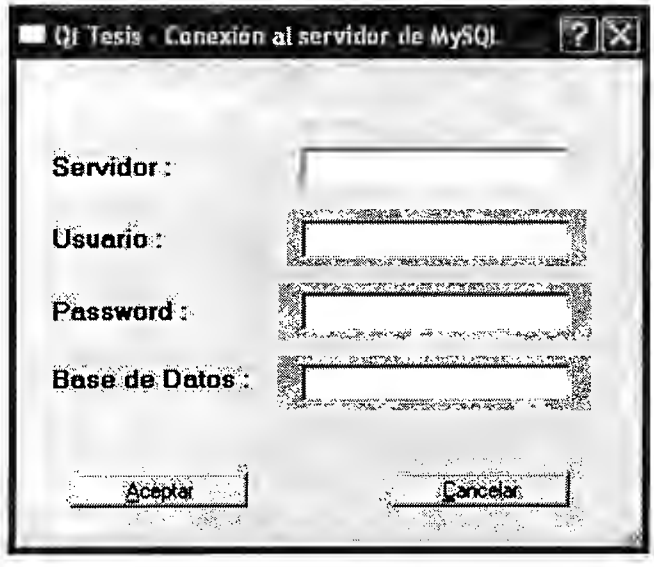


Fig. 32 – Ventana de conexión al servidor MySQL

Nota: La conexión con el servidor es esencial para el funcionamiento del monitor de red. Si esta conexión se pasa por alto no será posible detectar los elementos de la red y posteriormente mostrar su estado.

Posterior al establecimiento de una conexión a la base de datos será necesario especificar una dirección IP y la mascara de subred a utilizar, con estos datos la aplicación detectara el rango de direcciones IP con las cuales se trabajara; por otra parte el sistema detectara las interfaces presentes en computadora en la que se ejecuta la aplicación, deberá elegir una interfaz alámbrica.

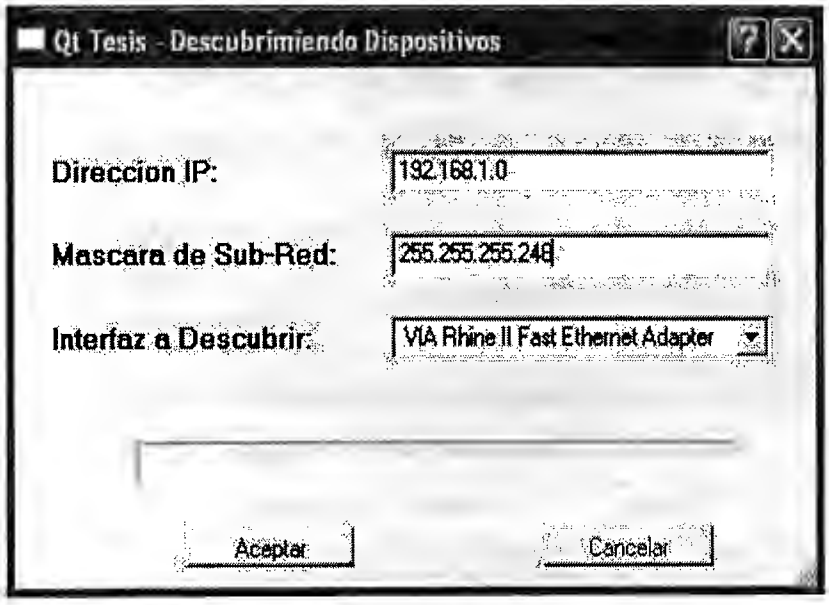


Fig. 33 – Ventana de introducción de datos

Una vez concluida la etapa de estudio de las direcciones IP del rango calculado se procede a identificar que tipo de dispositivo ha sido encontrado, esto se logra como se menciono anteriormente con el análisis de agentes SNMP que puedan existir en dichos dispositivos, durante este proceso se despliega la pantalla de metadatos, figura 34, presentada a continuación.

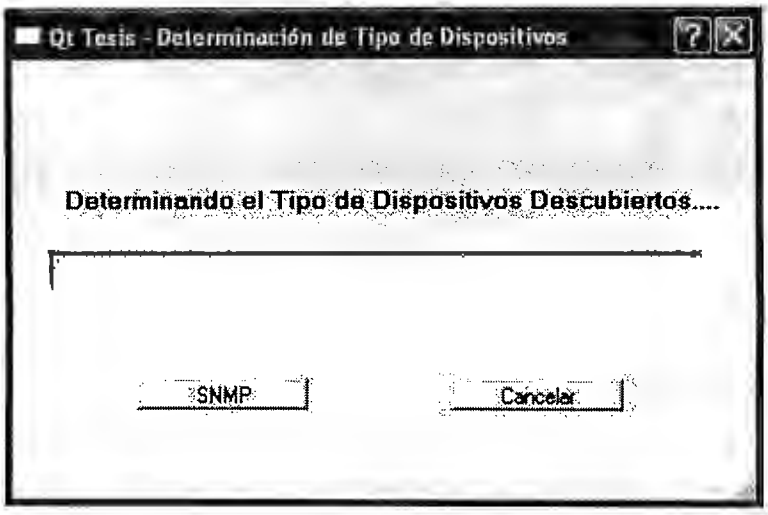


Fig. 34 – Ventana Metadatos

Una vez han sido detectadas las direcciones IP utilizadas y posterior determinación de los diferentes dispositivos aparece la ventana presentada en la figura numero 35; esta permite activar el proceso de mapeo de los dispositivos mediante el cual se activa la diagramación de los elementos red.

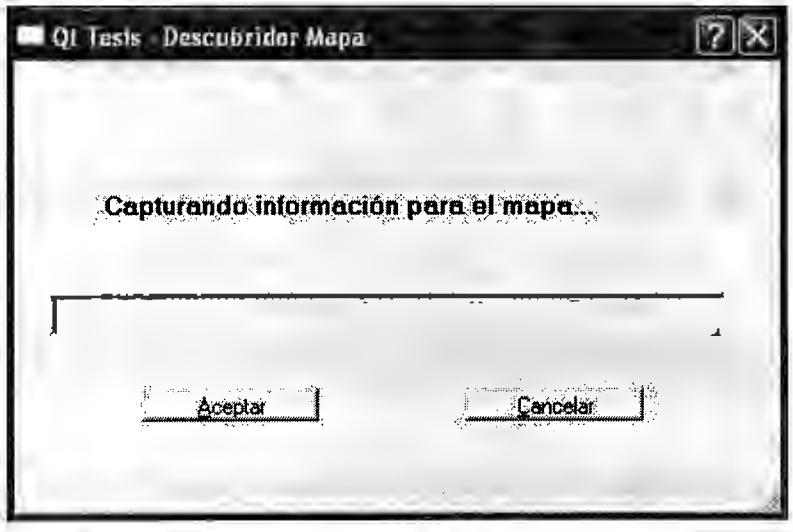


Fig. 35 – Activación de mapa de datos

Nota: El sistema de Administración y Monitoreo de red asume que la primera dirección IP correspondiente a la subred donde se encuentra la estación monitora corresponde al gateway de la misma, esto puede apreciarse gráficamente en la imagen 38, pág. 113.

5.1.2 FORMULARIO DE PANTALLA PRINCIPAL

Una vez realizados los diferentes procesos para el funcionamiento correcto del monitor de red, el sistema muestra la pantalla principal en la cual inicialmente no se muestran dispositivos hasta seleccionar la opción Cargar Red del menú archivo de la barra de menú.

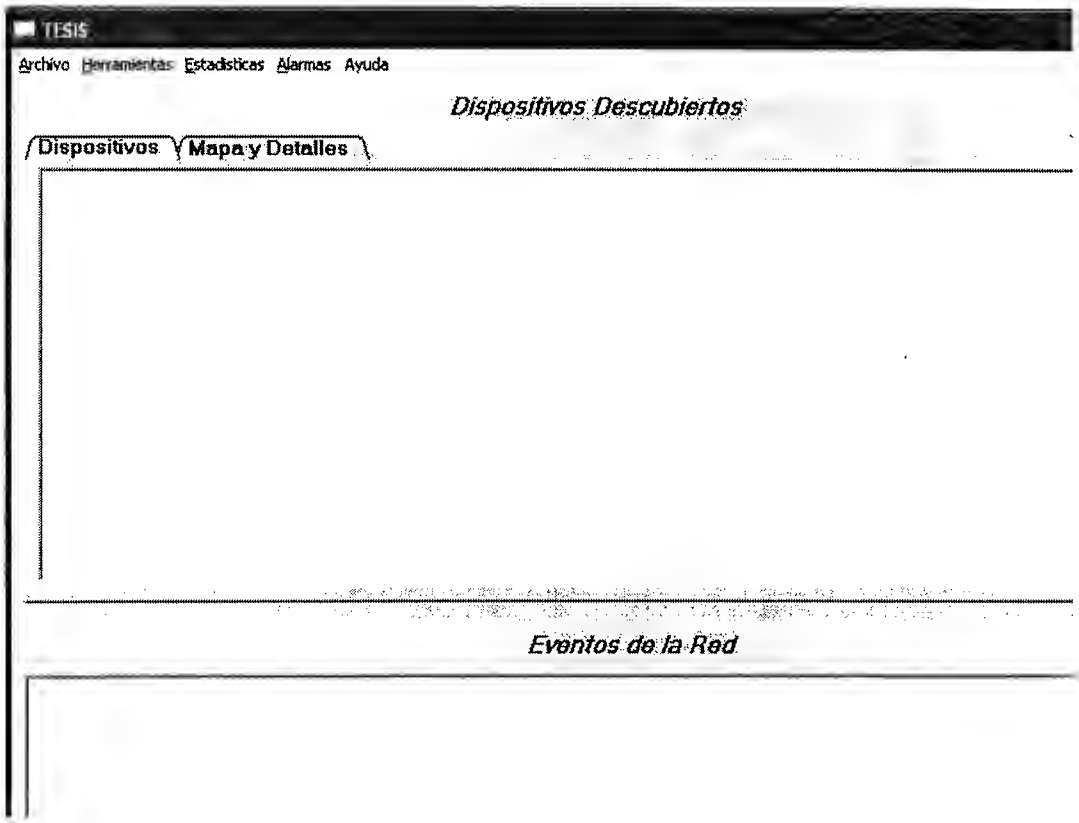


Fig. 36 – Formulario principal

La figura anterior cuenta con dos áreas principales, en la parte superior se encuentra la sección de Dispositivos Descubiertos, esta a su vez posee dos fichas para el análisis de red: *Dispositivos, Mapa y Detalles.* La parte inferior contendrá los acontecimientos de la red por fecha y descripción del suceso.

5.1.2.1 FICHAS EN DISPOSITIVOS DESCUBIERTOS

5.1.2.1.1 DISPOSITIVOS

La ficha Dispositivos, muestra las direcciones IP utilizadas y los diferentes tipos de dispositivos presentes en la red, de igual forma presentada el estado actual de estos, figura 37.

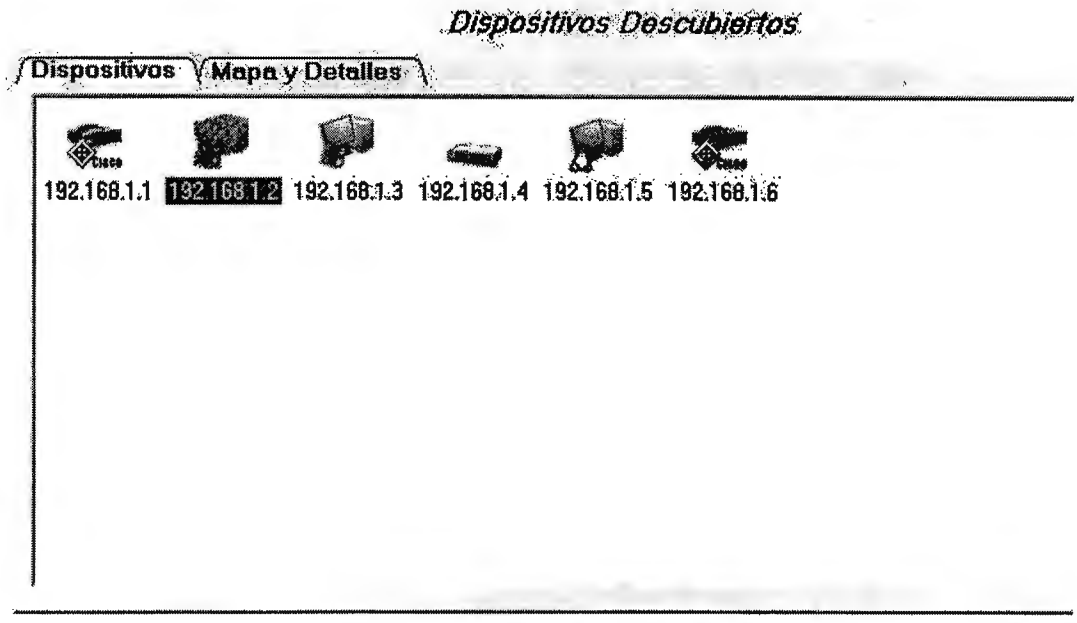


Fig. 37 – Ficha Dispositivos

Nota: Para desplegar los dispositivos de la red primero deberá seleccionar la opción Cargar red del menú archivo, Pág. 129.

5.1.2.1.2 MAPA Y DETALLES

En la figura 38, se presenta la ficha *Mapa y Detalles* esta ventana se divide en dos partes principales; el panel izquierdo que presenta la conexión entre los routers y diferentes dispositivos de la red, el panel derecho mientras tanto presenta la red a través de los datos básicos de los elementos detectados entre los cuales se mencionan:

- Nombre del equipo
- Tipo de dispositivo (router, switch, estación de trabajo)
- Su dirección de red (IP)
- Dirección física (MAC)

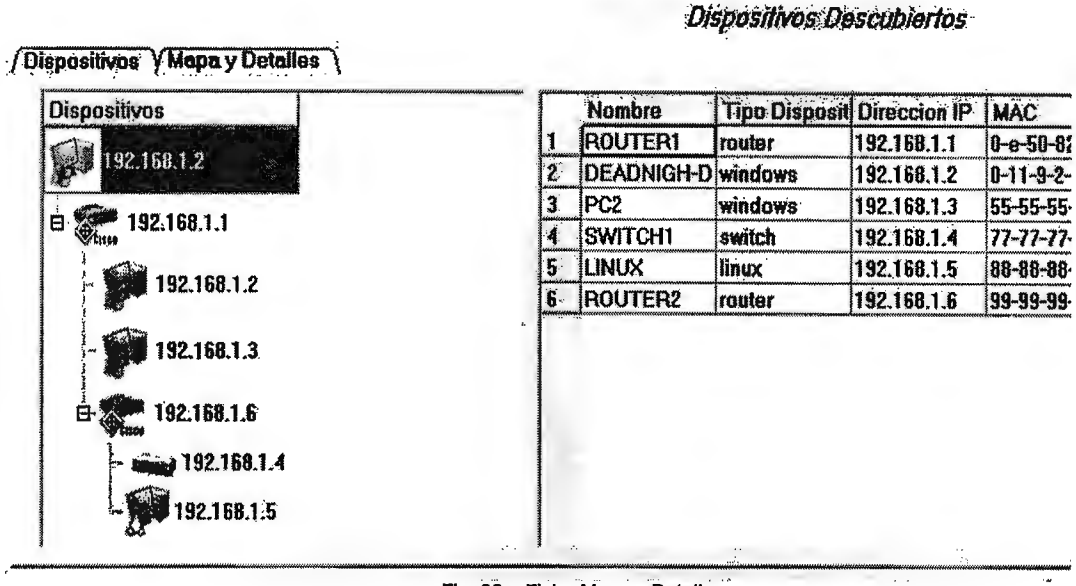


Fig. 38 – Ficha Mapa y Detalles

Nota: La primera estación de trabajo presentada en el panel izquierdo, Dispositivos, será aquella sobre la que se este ejecutando el monitor de red

5.1.3 BARRA DE MENÚ

La parte superior de la pantalla principal de la aplicación se cuenta con una barra de menú que permite acceder a diferentes opciones según sea necesario.

Fig. 39 – Barra de Menú

5.1.3.1 AYUDA

El menú *Ayuda* le permite al usuario acceder a un tutorial del uso de la aplicación para ello deberá seleccionar la opción *Ver Ayuda*. Seleccionando la opción *Acerca de Descubridor*, obtendrá una la información de los desarrolladores de la aplicación así como las herramientas utilizadas para lograr su funcionamiento.

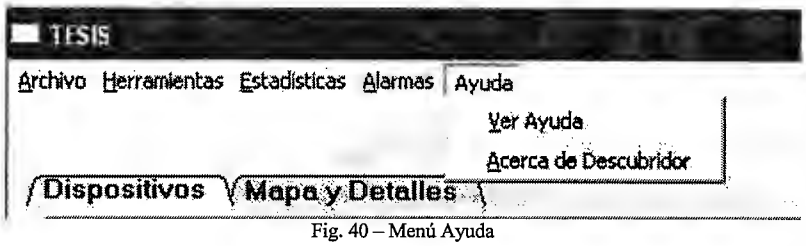


Fig. 40 – Menú Ayuda

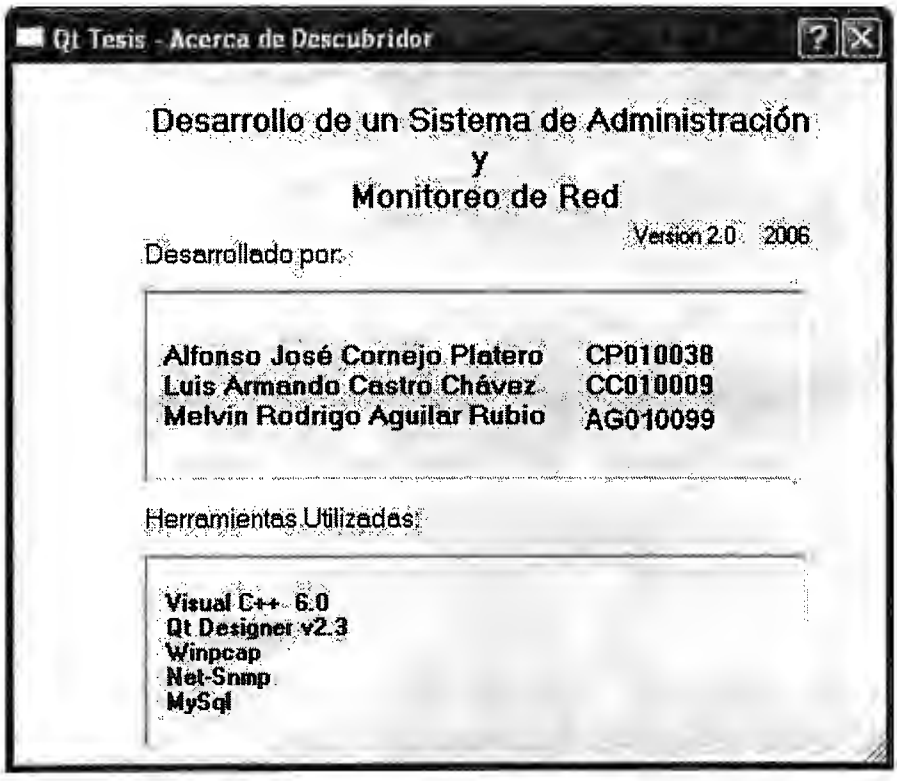


Fig.41 – Formulario Acerca del Descubridor de Redes

5.1.3.2 ARCHIVO

El menú *Archivo* cuenta con las opciones: *Cargar Red* y *Salir*. Cuando se han obtenido todos los datos acerca de las direcciones IP en el rango en estudio y se analiza el tipo de dispositivo presente en estas, el sistema no desplegara dichos elementos, para ello debe seleccionarse la opción *Cargar Red* de la barra de menú y podrán observar la red bajo estudio.

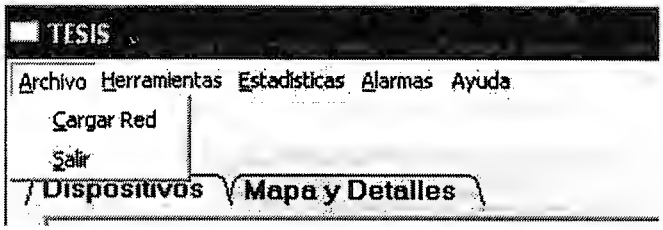


Fig. 42 – Menú Archivo

5.1.3.3 HERRAMIENTAS

El menú de *Herramientas* permite acceder a diferentes opciones para verificar el correcto funcionamiento de los equipos presentes en la red, como puede apreciarse en la figura 43, las opciones a las cuales puede accederse desde acá son:

- *Ping*, herramienta ICMP basada en peticiones de respuesta de eco
- *Trace Route*, herramienta Tracer que efectúa el trazado de ruta de un dispositivo a otro
- *Nmap*, escaneo de los puertos de una estación de trabajo

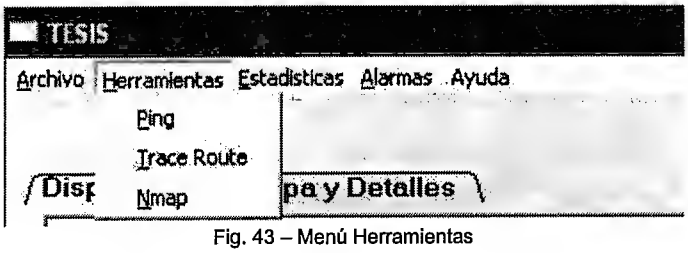


Fig. 43 – Menú Herramientas

5.1.3.4 ESTADÍSTICAS

El menú de estadísticas permite acceder a la configuración del intervalo de tiempo respecto al cual se desean obtener las diferentes estadísticas de:

- CPU
- Memoria
- Numero de paquetes

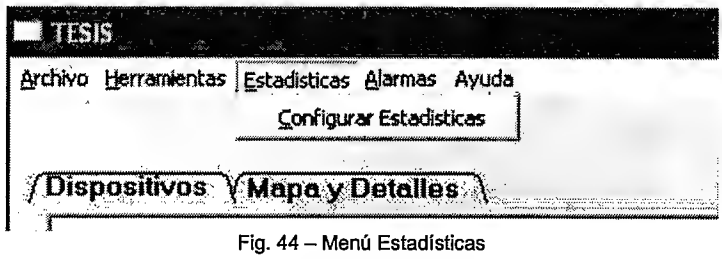


Fig. 44 – Menú Estadísticas

5.1.3.5 ALARMAS

El monitor de red cuenta con un menú que permite la configuración de alarmas para la detección de cambios de estado de un elemento de la red. Dicho cambio consiste en reportar si un elemento deja de formar parte de la red por falta de respuesta a peticiones de eco o la respuesta a ellas si anteriormente no respondió; por otra parte informa si existe un elevado uso del procesador por parte de una estación de trabajo. Para acceder a estas opciones deberá seleccionar *Configurar Alarmas* como en la figura 45.

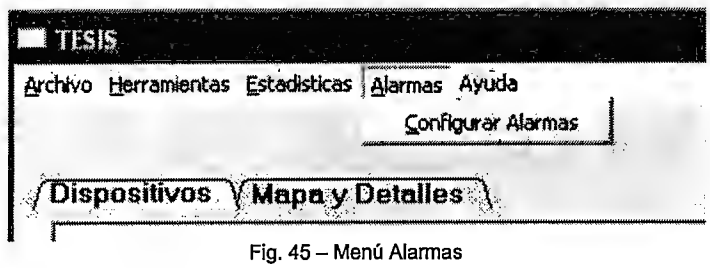


Fig. 45 – Menú Alarmas

5.1.4 ICONOS

Cuando los elementos de la red son presentados en pantalla el usuario tendrá una serie de símbolos para determinar que tipo de dispositivos han sido detectados por el sistema, los diferentes símbolos son presentados en la tabla 21 mostrada a continuación:

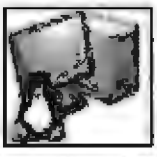
	**Estación Genérica** Este es el icono por defecto en caso que el sistema no logre determinar que tipo de equipo ha sido encontrado.
	**Estación Windows** Símbolo a asignar cuando el elemento detectado en una dirección IP sea una estación de trabajo personal que utiliza el sistema operativo Microsoft Windows en sus diferentes versiones.
	**Estación Linux** Símbolo a asignar cuando el elemento detectado en una dirección IP sea una estación de trabajo personal que utiliza alguna de las versiones del sistema operativo Linux.
	**Switch Cisco** Este icono se colocara cuando el elemento presente en una dirección IP del rango en estudio sea un switch.
	**Router Cisco** Este icono se colocara cuando el elemento detectado en la dirección IP estudiada sea un dispositivo de ruteo de paquetes

Tabla 21 - Iconos

Si el dispositivo evaluado supera el valor del procesador (CPU) establecido por el administrador de red, el icono aparecerá rodeado de color amarillo; por otra parte si uno de los dispositivos detectados inicialmente deja de responder a las constantes peticiones de eco enviadas por el monitor de red, su icono representativo aparecerá rodeado del color rojo y regresara a estado activo si responde a la siguiente petición de respuesta de eco.

A continuación se presenta la figura 46 con un ejemplo de los posibles estados de un dispositivo alarmado, en esta ocasión el ejemplo corresponde a una estación de trabajo con el sistema operativo Microsoft Windows:

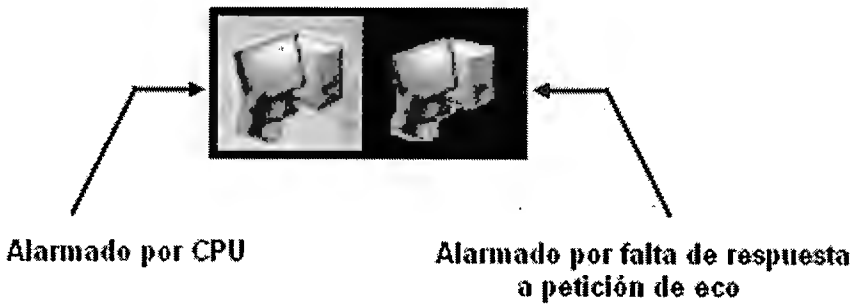


Fig. 46 – Dispositivos Alarmados

5.2 MENÚS EMERGENTES

Al dar un clic derecho sobre de los diferentes host detectados podrá acceder a las diferentes opciones disponible en la barra de menú mediante ventanas emergentes, esto vuelve el uso de la aplicación mas sencillo y agradable al usuario. Los diferentes menús a los que puede accederse se describen a continuación:

Fig. 47 – Menú emergente principal

5.2.1 SNMP

Si el dispositivo a evaluar posee un agente activo del protocolo de gestión SNMP será posible obtener datos del funcionamiento del sistema, entre ellos una descripción general del equipo y el estado de sus diferentes interfaces.

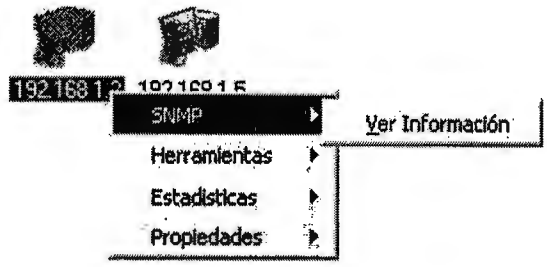


Fig. 48 – Submenú SNMP

Como puede observarse en la figura anterior, la selección del submenú *Ver Información* muestra una nueva ventana en la cual se encuentran los datos del elemento en estudio:

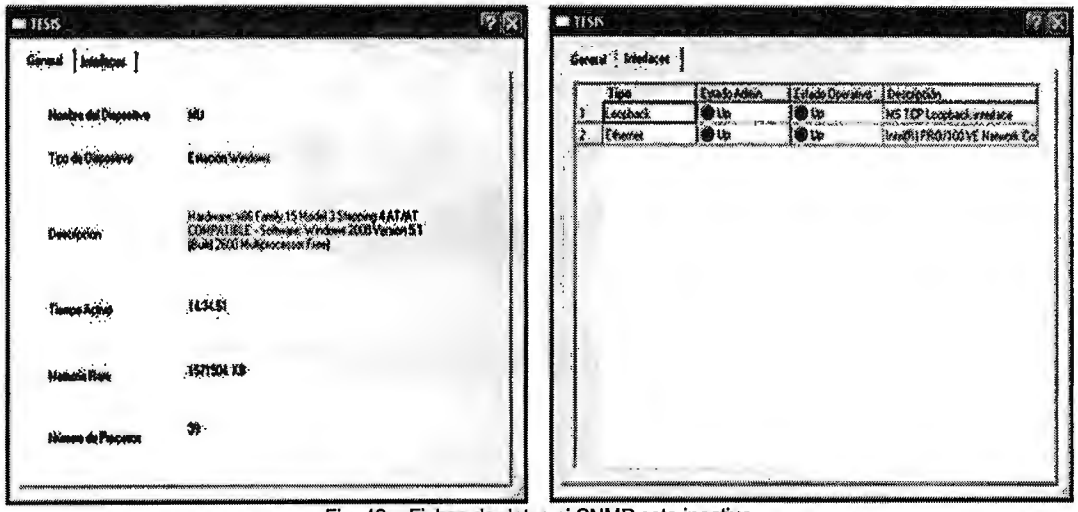


Fig. 49 – Fichas de datos si SNMP esta inactivo

Si no se cuenta con actividad del agente SNMP esta opción todavía podrá ser seleccionada del menú desplegable, sin embargo no se obtendrán datos en ninguna de las fichas de información, esto se muestra en la figura 50.

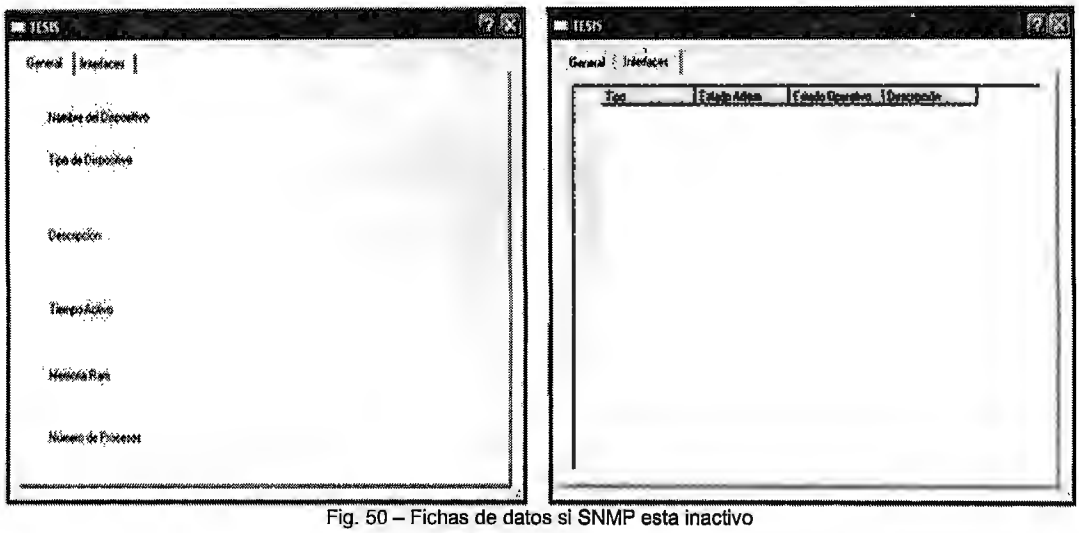


Fig. 50 – Fichas de datos si SNMP esta inactivo

Nota: Si el agente SNMP no se encuentra activo en el dispositivo puede revisar la información básica acerca de este en la opción *Propiedades* al final del menú emergente. Para mas detalles, *Propiedades* pagina 136.

5.2.2 HERRAMIENTAS

El submenú de *Herramientas* permite acceder a las opciones para estudiar el comportamiento de la red, al igual que la desde la barra de menú principal permite seleccionar:

- *Ping*, herramienta ICMP basada en peticiones de respuesta de eco
- *Traceroute*, , herramienta Tracer que efectúa el trazado de ruta de un dispositivo a otro
- *Port Scan*, escaneo de los puertos de una estación de trabajo

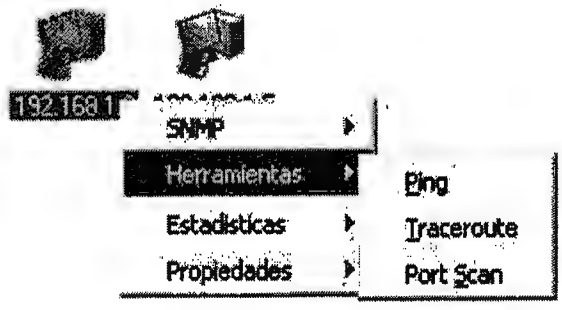


Fig. 51 – Submenú Herramientas

5.2.3 ESTADÍSTICAS

Este menú emergente permite acceder rápidamente a los diferentes valores de los cuales se pueden generar estadísticas presentadas de forma grafica. Los valores a evaluar pueden ser:

- Memoria
- Procesador
- Recepción de Paquetes.

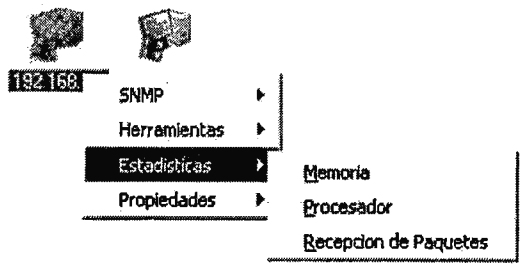


Fig. 52 – Submenú Estadísticas

5.2.4 PROPIEDADES

El menú emergente de *Propiedades* cuenta con dos opciones. La primera de ellas *Cambiar Icono*, es de gran utilidad cuando el sistema no pudo determinar que tipo de dispositivo se encuentra en una dirección IP al no existir un agente SNMP activo, permitiendo seleccionar uno de los iconos predeterminados para representar el equipo de forma mas precisa.

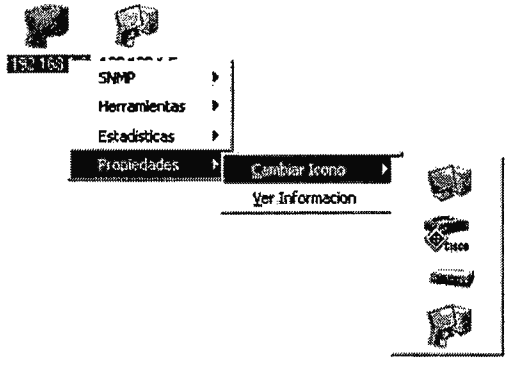


Fig. 53 – Submenú Propiedades, opción Cambiar Icono

La segunda de las opciones, *Ver Información*, permite obtener datos básicos del elemento en estudio; cuando el agente SNMP no se encuentra activo puede seleccionarlo para obtener datos básicos acerca del dispositivo.

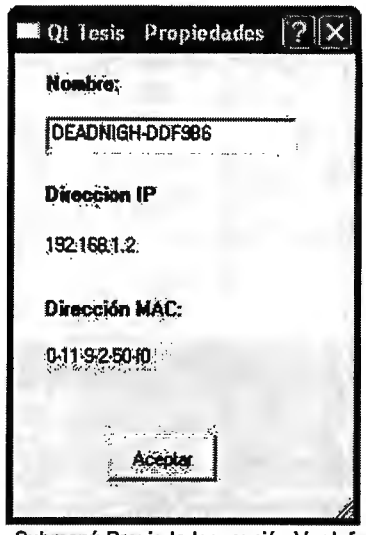


Fig. 54 – Submenú Propiedades, opción Ver Información

5.3 HERRAMIENTAS

5.3.1 HERRAMIENTA ICMP

En una red de computadoras es importante determinar la existencia de conectividad entre los diferentes dispositivos interconectados, por tal razón se provee al sistema la capacidad de realizar peticiones de respuesta de eco desde cualquiera los equipos detectados hacia cualquier otro.

Una petición de respuesta de eco es útil para diagnosticar errores en la red, la mayoría de veces es utilizada para medir la latencia o tiempo que tardan en comunicarse dos puntos remotos.

A esta herramienta puede accederse por medio de dos métodos:

- El primer método consiste en seleccionar la opción *Herramientas* de la barra de menú la cual se ubica en la parte superior del formulario principal, seleccione la herramienta *Ping* de entre las opciones desplegadas.

- El segundo consiste en realizar clic derecho sobre el icono del dispositivo con el cual se desea comprobar conectividad y luego seleccione *Herramientas* del menú emergente con lo que se observaran las diferentes alternativas con las cuales se cuenta, elija en este caso *Ping*.

La figura 55 presenta la interfaz de la herramienta ICMP en la cual puede realizar una prueba de *Ping*, en ella seleccione la dirección IP del dispositivo con el cual desea comunicarse del menú desplegable, posteriormente el numero de paquetes que desea utilizar para dicha prueba así como el tamaño de estos.

Fig. 55 – Herramienta ICMP

5.3.2 HERRAMIENTA TRACER

El sistema es capaz de detectar la ruta que debe ser recorrida para que un paquete se traslade de un elemento detectado en la red a otro, esta herramienta es útil para determinar en que segmento de la red existen retrasos cuando se realiza un intercambio de datos entre dos dispositivos.

El sistema envía un paquete de petición de respuesta de eco inicialmente con un tiempo de vida (TTL) de forma encapsulada, si no se obtiene respuesta del dispositivo al cual se realizó la petición se obtendrá en su lugar un valor de tiempo de vida excedido del cual se obtiene la dirección IP del router que envía ese paquete, se procede a enviar otro paquete pero esta vez con el valor de TTL incrementado en uno y así consecutivamente hasta que se obtenga respuesta del dispositivo o se llegue a un límite de paquetes enviados.

A esta herramienta puede accederse por medio de dos métodos:

- El primer método consiste en seleccionar la opción *Herramientas* de la barra de menú la cual se ubica en la parte superior de la ventana principal, seleccione *Trace Route* de entre las opciones desplegadas.

- El segundo consiste en realizar clic derecho sobre el icono del dispositivo con el cual desea comunicarse y luego seleccione *Herramientas* del menú emergente con lo que se observaran las opciones con las cuales se cuenta, elija en este caso *Trace Route*.

La interfaz de la herramienta Tracer se muestra en la figura 56 presentada a continuación:

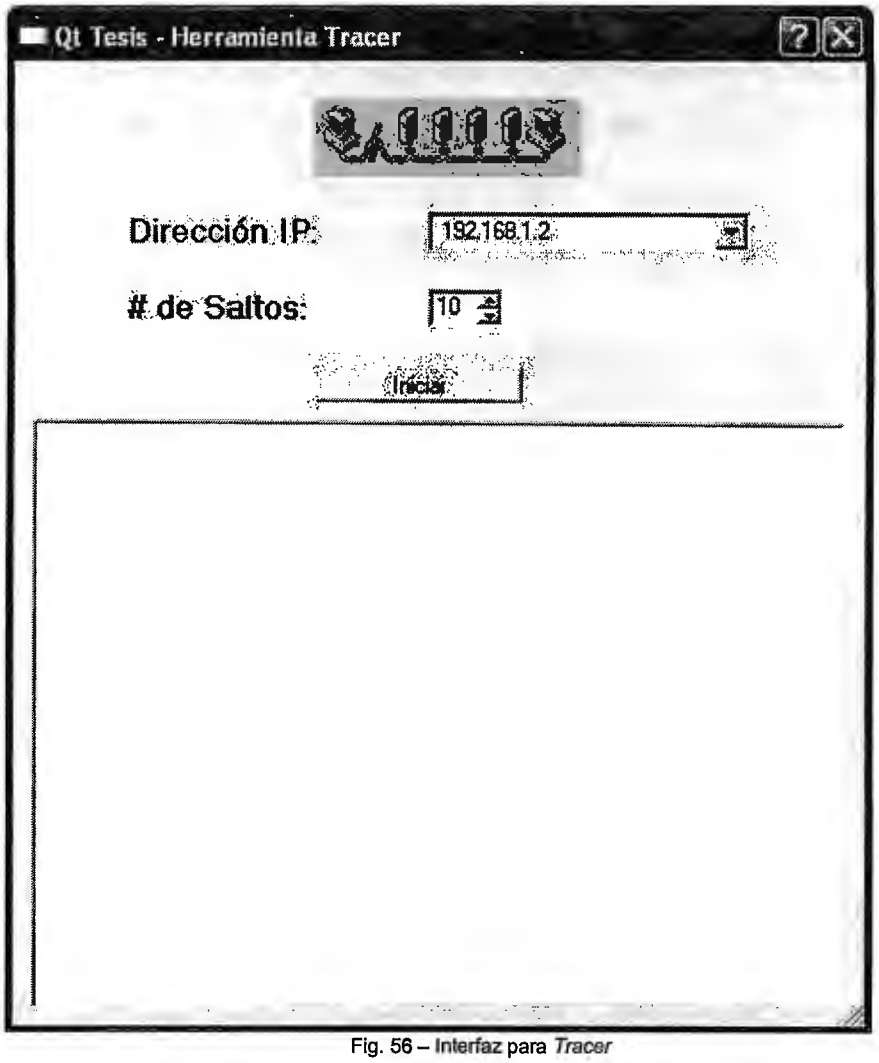


Fig. 56 – Interfaz para *Tracer*

5.3.3 ESCANEO DE PUERTOS

El sistema es capaz de realizar un escaneo sistemático de puertos en las estaciones de trabajo detectados durante los sondeos de la red. Dado que un puerto es un lugar donde la información entra y sale constantemente de una computadora, analizar el estado de estos identifica puertas abiertas que constituyan un punto débil para irrumpir en la seguridad del dispositivo y consecuentemente en toda la red supervisada.

Para realizar esta operación se utiliza la herramienta de código abierto para exploración de red y auditoria de seguridad *Nmap* para Windows,

WiNmap. De dicha herramienta se utilizan los recursos para realizar el escaneo de puertos sobre el dispositivo deseado, con ello puede conocerse el estado de los puertos en el dispositivo estudiado al momento de realizar la solicitud de análisis.

A esta herramienta puede accederse por medio de dos métodos:

- El primer método consiste en seleccionar la opción *Herramientas* de la barra de menú la cual se ubica en la parte superior de la ventana principal, posteriormente seleccione *Nmap* de entre las opciones desplegadas.

- El segundo consiste en realizar clic derecho sobre el icono del dispositivo en el cual se desea analizar sus puertos y luego seleccione *Herramientas* del menú emergente con lo que se observaran las opciones con las cuales se cuenta, elija en este caso *Port Scan*.

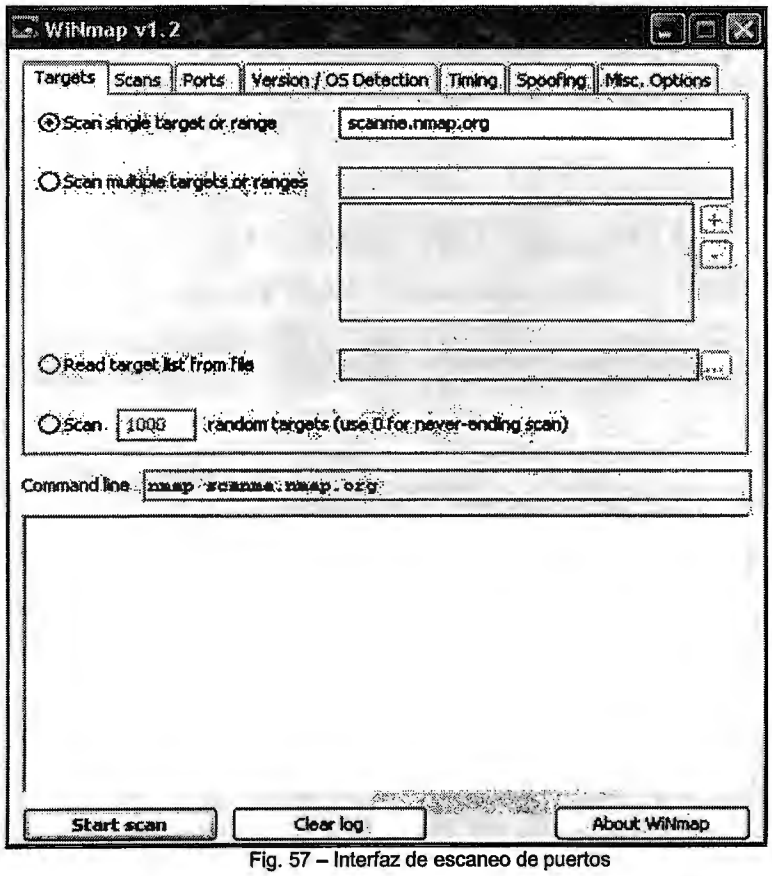


Fig. 57 – Interfaz de escaneo de puertos

5.3.4 ESTABLECIMIENTO DE ALARMAS

En una red de computadoras es esencial estar al tanto de los diferentes acontecimientos que se presentan en una red. La detección de comportamientos anormales en la red es una necesidad primordial por lo que se provee al sistema la capacidad de detectar tanto la falta de comunicación de con uno de los dispositivos o el reestablecimiento de esta a través de peticiones de respuesta de eco, de igual forma se identifica si el nivel de desempeño de una estación de trabajo es un valor que supera los considerados como aceptables.

Para activar el sistema de alarma deberá seleccionar la opción *Configurar Alarmas* del menú *Alarmas* en la ventana principal, con ello obtendrá la ventana siguiente:

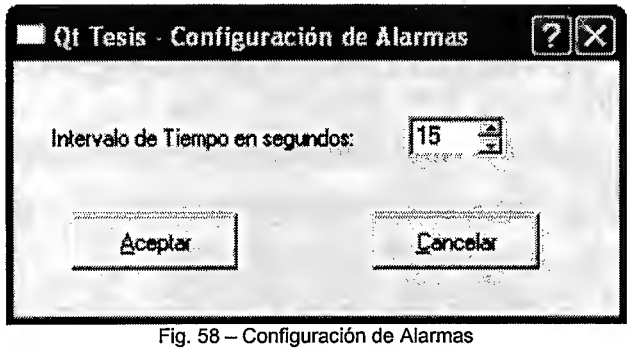


Fig. 58 – Configuración de Alarmas

Al establecer el intervalo de tiempo se activa el proceso mediante el cual el sistema indicara si uno de los elementos deja de responder a las peticiones de eco o si sobrepasa el valor establecido respecto al uso del procesador. El establecimiento del valor de CPU es configurable en la ventana *Configuración de Estadísticas*.

5.3.5 ESTADÍSTICAS

El sistema de monitoreo permite realizar análisis estadísticos respecto a diferentes valores de importancia de una estación de trabajo, los datos se muestran gráficamente y los valores a evaluar consisten en:

- Dirección IP en estudio
- Intervalo de fecha y hora a evaluar
- Valores a evaluar
    - CPU
    - Memoria
    - Numero de paquetes recibidos

El uso de esta herramienta consiste en el proceso siguiente:

I. El primer paso es la selección de la opción Configurar Estadísticas de la barra de menú con lo que obtendrá la ventana de la figura 59, acá establecerá el intervalo de tiempo a utilizar (segundos) para el desligue de los gráficos.

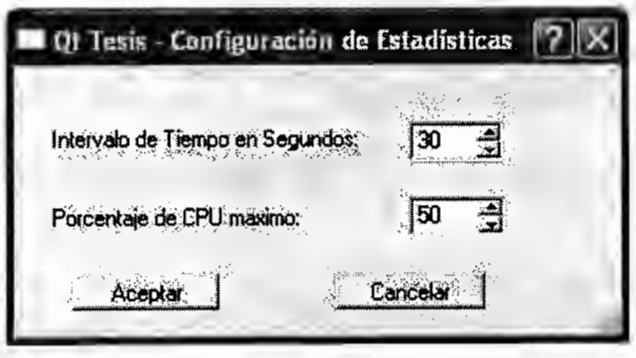


Fig. 59 – Configuración de Estadísticas

II. Realice un clic derecho sobre el icono del dispositivo del cual se desean obtener datos de estudio y luego seleccionar que tipo de dato desea que sean presentados. Puede elegir entre uso de CPU, Memoria y numero de paquetes recibidos en la estación deseada.

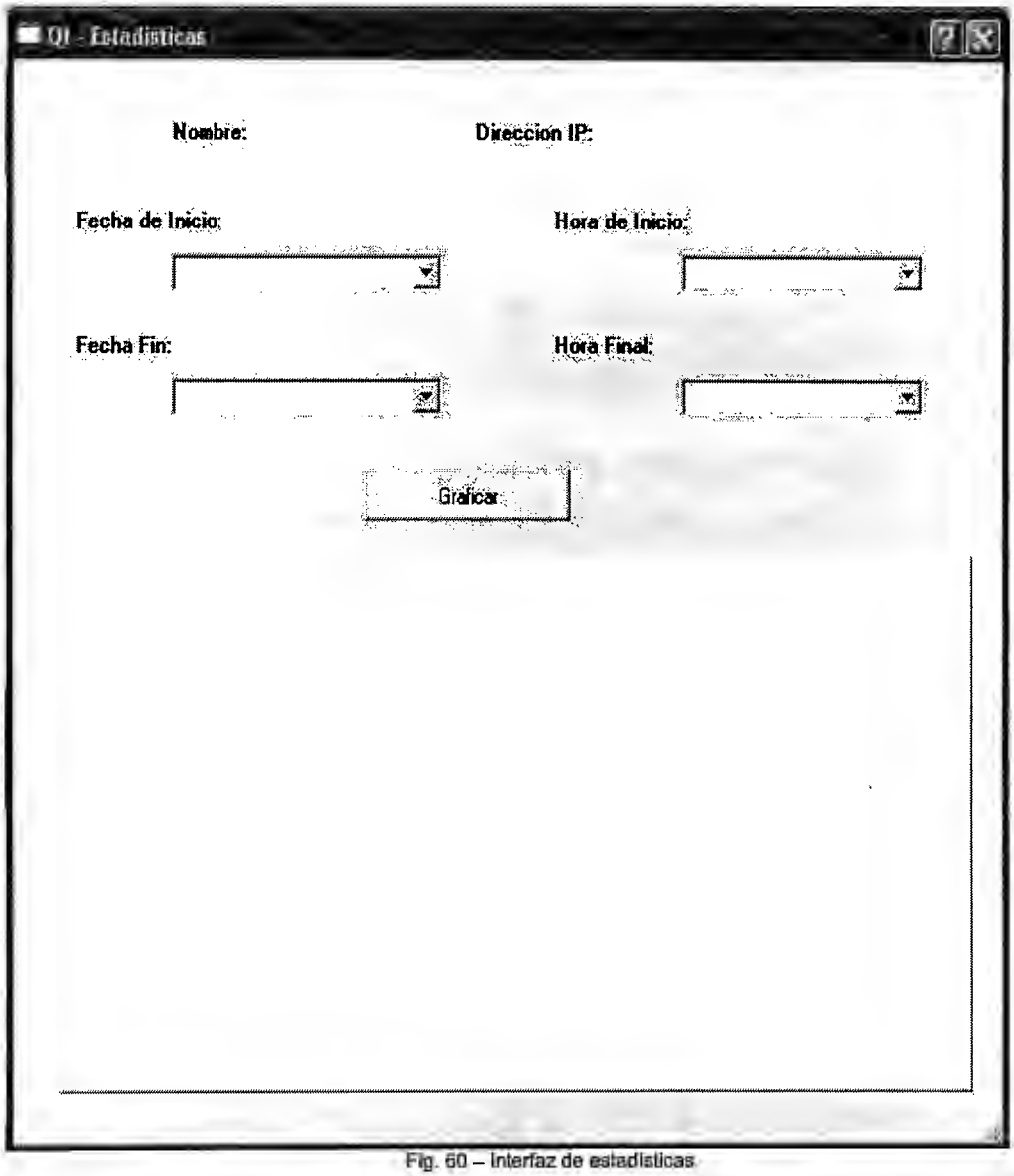


Fig. 60 – Interfaz de estadisticas

CONCLUSIONES

Finalizada el desarrollo del Sistema de Administración y Monitoreo de Red nos complace presentar las siguientes conclusiones:

- Se realizaron profundas investigaciones teóricas con el fin de comprender los posibles procedimientos que podrían hacer posible la detección de los diferentes dispositivos de red. La búsqueda condujo a la utilización de protocolos de administración de red como el SNMP, ICMP, entre otros. Gracias a dicho análisis se determino que tipo de información debía obtenerse de estos y los procedimientos para extraer y utilizar dicha información, de igual forma se establecieron las diferentes herramientas a utilizar para ponerlos en practica tal es el caso del Net-SNMP, WinPcap y MySQL.

- La arquitectura del sistema se realiza en el lenguaje de programación C++ en ambiente Windows y la interfaz grafica mediante la librería QT, a través de ambas se diseña una interfaz amigable al usuario desde la cual se manipulan las diferentes herramientas y procesos para llevar a cabo la correcta detección de equipos y posteriormente el estado de estos, esta fase se acompaño de constantes pruebas de laboratorio que permitieron la determinación de fallas para su posterior corrección y mejoras sobre la aplicación.

- La realización del Sistema de Administración y Monitorio de Red se convierte en una herramienta de gran utilidad capaz de agilizar la realización de tareas cotidianas a las que se enfrenta el personal de administración de red; de igual forma proporciona la oportunidad a estudiantes de apreciar el funcionamiento de redes en ambiente ethernet TCP/IP mediante los diferentes protocolos de red utilizados para el funcionamiento del sistema.

- El área de desarrollo no a sido explotada a nivel nacional por lo que el grado de complejidad aumento por falta de investigaciones previas, con la puesta en practica de los diferentes métodos de investigación y conocimientos adquiridos durante nuestros estudios universitarios se superaron las adversidades y se presenta este sistema como un estimulo a futuras generaciones estudiantiles a continuar con este tipo de investigaciones que contribuyan al enriquecimiento de conocimientos en este campo.

RECOMENDACIONES

A medida evoluciona el desarrollo del campo computacional se vuelve indispensable la constante investigación y actualización que permitan manejar las redes de datos de forma mas eficiente. Se anima a los estudiantes universitarios a la continuación de esta aplicación mediante la adición de diferentes herramientas que puedan facilitar aun más la administración de redes de datos.

El sistema de Administración y Monitoreo de Red realiza funciones básicas para estar al tanto del funcionamiento de una red de datos, sin embargo se sugiere la investigación del protocolo de administración de red SNMPv3 para lograr la obtención de datos de dispositivos de Capa Tres mas recientes. De igual forma es conveniente realizar estudios sobre el impacto de IPV6 sobre las diferentes topologías de red y como realizar modificaciones sobre esta aplicación para que logre compatibilidad con el nuevo formato de direcciones IP.

La aplicación se diseña para redes Ethernet TCP/IP por lo que podría extenderse a diferentes tipos de red como las tipo Token Ring o FDDI.

Sobre la aplicación final se sugiere la mejora de algunos procesos específicos para incrementar la funcionalidad de la misma, estos se listan a continuación:

1. Posterior al proceso de Descubrimiento de la Red se sugiere la adición de un procedimiento que permita establecer la detección de nuevos elementos que se incluyan a la red o proveer al sistema la capacidad de agregar y personalizar nuevos dispositivos a esta de forma manual.

   - Para desarrollar el proceso anteriormente mencionado se recomienda el desarrollo de un hilo que se encargue de la realización de consultas a las direcciones IP que no fueron detectadas como asignadas al inicio del procedimiento del Descubrimiento de la red, al detectar actividad en una de estas se indicara la aparición de un nuevo elemento en la red y al

mismo tiempo se realicen procesos procedimiento para determinar el tipo de dispositivo que a sido detectado.

- Respecto a la adición de dispositivos a la red de forma manual puede diseñarse un formulario desde el cual puedan ser agregados los nuevos dispositivos a la red especificando la dirección IP de estos así como también la determinación de tipo de dispositivo para finalmente agregarlo al mapa; se sugiere la realización de una petición de respuesta de eco, PING, a la dirección IP establecida para el dispositivo, si se obtiene respuesta la base de datos se actualizará con dichos valores, se deberá detectar el tipo de dispositivo y trazar la ruta para identificar a que dispositivo se encuentra conectado.

2. Se sugiere agregar al sistema la capacidad de actualizar el valor de las direcciones IP con la que se detectaron los elementos de la red.

   Para realizar dicha tarea se sugiere consultar a la base de datos con el fin de detectar si la dirección IP que se desea situar no fue previamente asignada y actualizar el campo IP con la nueva dirección.

3. El sistema de Administración y Monitoreo de red asume que la primera dirección IP correspondiente a la subred donde se encuentra la estación monitora corresponde al gateway de la misma.

   Si esta condición no se cumple puede desarrollarse un proceso alterno que permita obtener el gateway de la estación monitora.

4. Con el fin de disminuir el trafico generado por el sistema de administración se sugiere el establecimiento de alarmas mediante trampas, traps, para los dispositivos con un agente SNMP activo y el envió de peticiones de respuesta de eco a los elementos de red en los cuales no fue detectado protocolo SNMP.

5. Puede incorporarse al sistema opciones que permitan el almacenamiento de de la base de datos y desarrollo de procesos para su posterior ejecución.

6. Actualmente el registro de eventos de la red es almacenado en un archivo de texto creado cada vez que se ejecuta el sistema borrando así los datos existentes, se sugiere un cambio a la forma de almacenamiento del registro de eventos de forma que si el sistema se reinicia los nuevos datos sean adheridos a dicho archivo.

7. El establecimiento de alarmas por nivel de uso de CPU se realiza de forma global; es decir el valor de CPU especificado como nivel critico es el mismo para cada dispositivo.

   Se sugiere establecer el porcentaje de CPU por cada dispositivo agregando un campo a la base de datos mediante el formulario de Propiedades en el que sea posible establecer el porcentaje a considerar como critico.

Para un estudio mas completo de los diferentes protocolos de red utilizados y para la planificación de herramientas que aumenten la funcionalidad de este sistema es beneficioso el referirse a las diferentes RFC (Request For Comments) las cuales son un conjunto de notas técnicas y organizativas donde se describen los estándares o recomendaciones de Internet.

BIBLIOGRAFIA

BIBLIOGRAFIA.

El desarrollo de la presente investigación se basa en la investigación y aplicación de conceptos, procesos e información respecto a las diferentes áreas de estudio de las siguientes fuentes de datos:

- http://www.trolltech.com/
  Pagina principal de QT, desde acá se tiene acceso a la descarga de esta librería grafica en sus versiones gratuita y comercial.
  Actualización 2006.

- http://doc.trolltech.com/3.2/index.html
  Documentación para QT edición gratuita. En este sitio puede accederse a ejemplos desarrollados con esta librería al igual que una explicación detallada de cada uno de las opciones que pueden utilizarse.
  Actualización 2006.

- http://www.tcpipguide.com/free/t_TCPIPMIBObjectDescriptorsandIdentifiersandtheObjec.htm
  Descripción del protocolo TCP/IP y su funcionamiento el cual el cual es indispensable conocer para el desarrollo de la aplicación y su interacción con SNMP.
  Actualización 2005

- http://www.tcpipguide.com/free/t_SNMPProtocolMessagingandMessageFormats.htm
  Contiene información consistente respecto a SNMP y las MIBs utilizadas por dicho protocolo de gestión de datos.
  Actualización 2005

- http://wiki.ethereal.com/WinPcap
  Información General sobre la liberaría para el análisis de paquetes Winpcap, esta librería es esencial en el funcionamiento de Ethereal por lo que se le otorga una sección muy detallada en este enlace.
  Actualización 2006.

- http://www.winpcap.org/
  Sitio de descarga de la librería de captura de paquetes para Windows, WinPcap. En este sitio se encuentran todas las noticias referentes a las versiones mas recientes de esta así como enlaces a sitios de descarga de herramientas que hacen uso de WinPcap.
  Actualización 2006.

- http://www2.rad.com/networks/1995/snmp/snmp.htm
  Información General de estructura y funcionamiento del protocolo SNMP
  Actualización 1995.

- http://net-snmp.sourceforge.net
  Net SNMP, Librería de en c++ para poder acceder a la información de los agentes SNMP
  Actualización 2006.

- http://www.snmplink.org/
  Información General de SNMP, contiene enlaces a sitios referentes a SNMP así como diferentes herramientas como descarga de MIB y buscador de estas.
  Actualización 2005

- http://snmp.cs.utwente.nl/ietf/mibs/
  Simple Web es una fuente de RFCs en la cual puede encontrarse una amplia gama de OIDs y MIBs.
  Actualización 2003.

- www.cisco.com
  Sitio en el cual se obtuvo la información referente a los OID propios de dispositivos cisco
  Actualización 2006.

- http://www.comptechdoc.org/independent/networking/guide/netnetbeui.html
  Descripción de estructura y funcionamiento del protocolo Netbios.
  Actualización 2000.

- http://insecure.org/nmap/
  El sitio de descarga de la aplicación NMAP para Linux y Windows en modo consola; de igual forma contiene información acerca del funcionamiento de este. El Nmap es utilizado para el análisis de puertos de los dispositivos en la red.
  Actualización 2006.

- http://www.philippsworld.net/software_winmap.htm
  Enlace para descargar la interfaz grafica de Nmap para plataformas Windows, WinNmap v1.2. Para la utilización de esta interfaz grafica debe descargarse e instalarse la versión de consola descrita en el enlace anterior.

- http://www.infor.uva.es/~jvegas/cursos/bd/sqlplus/sqlplus.html
  Documentación sobre lenguaje de administración de bases de datos SQL,
  Actualización 1998.

- http://www.mysql.com/
  Sitio principal de MySQL, desde el cual puede accederse a las versiones gratuitas y comerciales de MySQL, al mismo tiempo cuenta con diferentes artículos de soporte de esta aplicación. Esta herramienta fue utilizada para el desarrollo de la base de datos utilizada por la aplicación.
  Actualización 2006.

- http://wiki.ethereal.com/
  Sitio en el cual se puede descargar y encontrar información de funcionamiento del analizador de tramas de red Ethereal, esta herramienta fue de de suma importancia para la compresión de los paquetes a capturar y utilizar en la aplicación.
  Actualización 2006

GLOSARIO

GLOSARIO

BROADCAST

Paquete de datos que se envía a todos los nodos de una red. Se identifican a través de una dirección de broadcast. Comparar con *multicasty unicast.*

DIRECCIÓN INDIVIDUAL

Se refiere a múltiples dispositivos de red. Sinónimo de *dirección de grupo.*

DIRECCIÓN DE UNICAST

Dirección que especifica un solo dispositivo de red.

DATAGRAMA

Agrupación lógica de información que se envía como una unidad de capa de red a través de un medio de transmisión sin establecer con anterioridad un circuito virtual. Los datagramas IP son las unidades principales de información de Internet. Los términos *trama, mensaje, paquete* y *segmento* también se usan para describir las agrupaciones de información lógica en las diversas capas del modelo de referencia OSI y en los diversos círculos tecnológicos.

DIRECCIÓN FÍSICA / MAC

Dirección de capa de enlace de datos estandarizada que se requiere para cada puerto o dispositivo que se conecta a una LAN. Otros dispositivos de la red usan estas direcciones para localizar puertos específicos en la red y para crear y actualizar tablas de enrutamiento y estructuras de datos. Las direcciones MAC tienen 6 bytes de largo y se controlan a través de la IEEE. Comparar con *dirección de red.*

DIRECCIÓN LÓGICA/ DIRECCIÓN DE RED

Dirección de capa de red que se refiere a un dispositivo de red lógico, más que físico. También denominada dirección de protocolo. Comparar con *dirección MAC.*

DIRECCIÓN IP

Dirección de 32 bits asignada a los hosts que usan TCP/IP. Una dirección IP pertenece a una de las cinco clases (A, B, C, D o E) y se escribe como 4 octetos separados por puntos (formato decimal separado por puntos). Cada dirección está compuesta por un número de red, un número de subred opcional y un número de host. Los números de red y subred de forma conjunta se usan para el enrutamiento, mientras que el número de host se usa para direccionar a un host individual dentro de la red o subred. La máscara de subred se usa para extraer información de red y subred de la dirección IP. También denominada dirección Internet.

HOST

Sistema computacional ubicado en una red. Es similar al término nodo, salvo que el host generalmente implica un sistema computacional, mientras que el nodo generalmente se aplica a cualquier sistema conectado a la red, incluyendo servidores de acceso y routers.

INTERNET

Abreviatura de internetwork. No se debe confundir con la Internet.

INTERNETWORKING

Conjunto de redes interconectadas por routers y otros dispositivos que funcionan (generalmente) como una sola red. A veces denominada *Internet*, que no se debe confundir con la *Internet*.

IP

Protocolo Internet. Protocolo de capa de red en la pila TCP/IP que brinda un servicio de internetworking no orientado a conexión. El IP suministra características de direccionamiento, especificación de tipo de servicio, fragmentación y reensamblaje y seguridad.

LAN

Red de área local. Redes de datos de alta velocidad y bajo nivel de errores que abarcan un área geográfica relativamente pequeña (hasta unos pocos miles de metros). Las LAN conectan estaciones de trabajo, dispositivos periféricos, terminales y otros dispositivos que se encuentran en un mismo edificio u otras áreas geográficas limitadas. Los estándares de LAN especifican el cableado y la señalización en las capas física y de enlace de datos del modelo OSI. Ethernet, FDDI y Token Ring son tecnologías LAN de uso muy difundido

MAN

Red de área metropolitana. Red que abarca un área metropolitana. Por lo general, una MAN abarca un área geográfica más grande que una LAN, pero más pequeña que una WAN.

NETWORKING

Conexión de cualquier conjunto de computadores, impresoras, routers, switches y otros dispositivos con el propósito de comunicarse a través de algún medio de transmisión.

MODELO DE REFERENCIA OSI

Modelo de referencia de interconexión de sistemas abiertos. Modelo de arquitectura de red desarrollado por la ISO y la UIT-T. El modelo está compuesto por siete capas, cada una de las cuales especifica funciones de red particulares como, por ejemplo, direccionamiento, control de flujo, control de error, encapsulamiento y transferencia confiable de mensajes. La capa superior (la capa de aplicación) es la más cercana al usuario; la capa inferior (la capa física) es la más cercana a la tecnología de medios. La capa que le sigue a la capa inferior se implementa en el hardware y software, mientras que las cinco capas superiores se implementan sólo en el software. El modelo de referencia OSI se usa de forma universal como método para la enseñanza y la comprensión de la funcionalidad de la red.

TCP/IP

Protocolo de control de transmisión/Protocolo Internet. Nombre común para el conjunto de protocolos desarrollado por el DoD de EE.UU. en la década de los años 70 para permitir la creación de redes interconectadas a nivel mundial. El TCP y el IP son los dos protocolos más conocidos del conjunto Ver también IP y TCP.

TCP

Protocolo de control de transmisión. Protocolo de capa de transporte orientado a conexión que suministra transmisión de datos full-duplex confiable. El TCP forma parte de la pila de protocolo TCP/IP.

PLATAFORMA

Base sobre la cual de desarrolla una aplicación.

PROTOCOLO

Descripción formal de un conjunto de normas y convenciones que rigen la forma en que los dispositivos de una red intercambian información.

ROUTER

Dispositivo de capa de red que usa una o más métricas para determinar la ruta óptima a través de la cual se debe enviar el tráfico de red. Los routers envían paquetes desde una red a otra basándose en la información de la capa de red.

SWITCH

Dispositivo de red que filtra, reenvía o inunda tramas basándose en la dirección destino de cada trama. El switch opera en la capa de enlace de datos del modelo OSI.

TARJETA DE INTERFAZ DE RED / NIC

Tarjeta de interfaz de red. Placa que suministra capacidades de comunicación de red hacia y desde un sistema computacional.

TOKEN

Trama que contiene información de control. La posesión del token permite que un dispositivo transmita datos en la red.

TOPOLOGÍA

Disposición física de los nodos y medios de red dentro de una estructura de networking empresarial.

TOPOLOGIA LÓGICA

La forma en que los hosts acceden a los medios para enviar datos.

TOPOLOGÍA FÍSICA

Disposición real de los cables o medios de red.

TROUBLESHOOTING

Análisis y solución de problemas técnicos de red.

WAN

Red de área amplia. Red de comunicación de datos que sirve a usuarios dentro de un área geográficamente extensa y a menudo usa dispositivos de transmisión provistos por un servicio público de comunicaciones.

ANEXOS

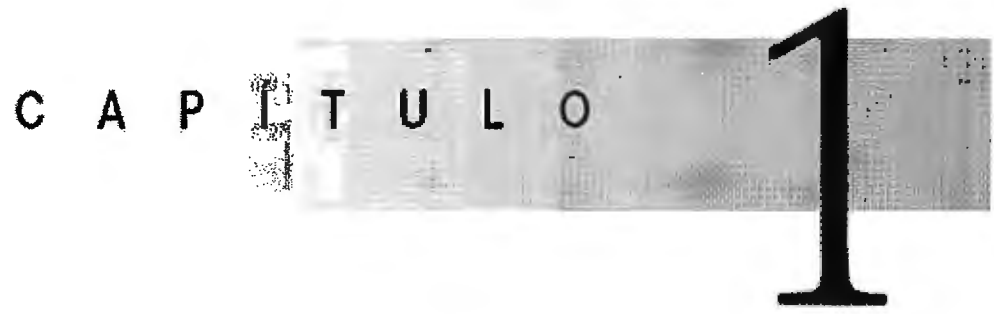
Manual del usuario de Sistema de Administración y Monitoreo de Red

Universidad
Don Bosco

2006

C O N T E N I D O

INSTALACIONES ADICIONALEs



INTRODUCCIÓN AL SISTEMA DE ADMINISTRACIÓN Y MONITOREO DE RED

El sistema de administración y monitoreo de red proporciona un completo software de:

- Detección de elementos presentes en redes Ethernet de TCP/IP y permite determinar las características generales de dichos elementos; al mismo tiempo presenta estadísticas del comportamiento de los dispositivos detectados y delata fallas en el funcionamiento de estos.

- Herramientas de detección de conectividad, trazado de rutas de un punto a otro y escaneo general de puertos en estaciones de trabajo personales.

Esta guía esta diseñada para todos aquellos que deseen utilizar este sistema como herramienta para manejar redes de computadoras con motivos de aprendizaje de acerca del funcionamiento de las mismas.

CARACTERÍSTICAS GENERALES

El Sistema de Administración y Monitoreo de red se presenta como una herramienta para monitoreo de red de libre distribución. Diseñado para facilitar el proceso de administración de redes de TCP/IP con objetivos educativos, permite observar el correcto funcionamiento y rendimiento de la red mediante la utilización de técnicas de networking y análisis de datos por medio de protocolos de red, al mismo tiempo obtiene la distribución de los dispositivos presentes en la misma con sus características esenciales y permite el análisis de ellos mediante diferentes herramientas.

- Herramienta ICMP

  En una red de computadoras es importante determinar la existencia de conectividad entre los diferentes dispositivos. El sistema es capaz de realizar peticiones de respuesta de eco desde cualquiera los equipos detectados hacia cualquier otro, es posible acceder a esta herramienta por diferentes métodos.

- Herramienta Tracer

  El sistema es capaz de detectar la ruta que debe ser recorrida para que un paquete se traslade de un elemento detectado en la red a otro, esta herramienta es útil para determinar en que segmento de la red existen retrasos cuando se realiza un intercambio de datos entre dos dispositivos.

- Escaneo de puertos

  El sistema puede capaz de realizar un escaneo sistemático de puertos en las computadoras detectados durante los sondeos de la red. Dado que un puerto es un lugar donde la información entra y sale constantemente de una computadora, analizar el estado de estos identifica puertas abiertas que constituyan un punto débil para irrumpir en la seguridad del dispositivo y consecuentemente en toda la red supervisada.

- Establecimiento de alarmas

  La detección de comportamientos anormales en la red es esencial por lo que se provee al sistema la capacidad de detectar si un dispositivo detectado deja de responder a las peticiones de respuesta de eco del sistema, de igual forma se identifica el nivel de desempeño de una estación de trabajo.

- Estadísticas

  Esta aplicación permite realizar análisis estadísticos respecto a CPU, Memoria y Número de Paquetes recibidos de un dispositivo. Estos datos se muestran de forma grafica y en base a parámetros de tiempo determinados por el usuario

INTRODUCCIÓN A LAS REDES DE COMPUTADORAS

No hay manera fácil de describir una red a causa de su naturaleza diversa, sin embargo diremos que los equipos se conectan a ellas de forma directa a un segmento de son denominados dispositivos. Estos se clasifican en dos grandes grupos.

El primer grupo está compuesto por los dispositivos de usuario final, los cuales incluyen las computadoras, impresoras, escáneres, y demás dispositivos que brindan servicios directamente al usuario.

El segundo grupo está formado por los dispositivos de red estos son todos aquellos que conectan entre sí a los dispositivos de usuario final transportando los datos que deben transferirse entre estos y posibilitando así su intercomunicación.

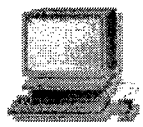
Los dispositivos de usuario final que conectan a los usuarios con la red se conocen con el nombre de hosts; permiten a los usuarios compartir, crear y obtener información.

Los host pueden existir sin una red, pero sin esta sus capacidades se ven sumamente limitadas. Los host están físicamente conectados con los medios de red mediante una tarjeta de interfaz de red (NIC). Utilizan esta conexión para realizar las tareas de envío de correo electrónico, impresión de documentos, escaneado de imágenes o acceso a bases de datos.

No existen símbolos estandarizados para los dispositivos de usuario final en la industria de networking. Son similares en apariencia a los dispositivos reales para permitir su fácil identificación.

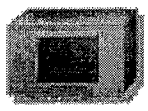
A continuación se muestran algunos de los símbolos utilizados con mayor frecuencia para representar los diferentes dispositivos presentes en una red.

Computadora Personal.



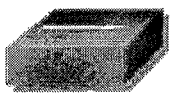
Sistema digital con tecnología microelectrónica capaz de procesar datos a partir de un grupo de instrucciones denominado programa. Su estructura básica incluye microprocesador (CPU), memoria y dispositivos de entrada/salida (E/S), junto a los buses que permiten la comunicación entre ellos.

Repetidor.



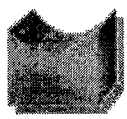
Dispositivo de red que regenera una señal analógica o digital que se distorsionan a causa de pérdidas en la transmisión producidas por la atenuación.

Hub.



Es un concentrador de conexiones. Permite que la red trate un grupo de hosts como si fuera una sola unidad. Esto sucede de manera pasiva, sin interferir en la transmisión de datos. Los hubs además son capaces de regenerar señales.

Puentes.



Convierten los formatos de transmisión de datos de la red además de realizar la administración básica de la transmisión de datos. Los puentes, proporcionan las conexiones entre LAN.

Switch.

Agrega inteligencia a la administración de transferencia de datos. No sólo son capaces de determinar si los datos deben permanecer o no en una LAN, sino que pueden transferir los datos únicamente a la conexión que necesita esos datos. Un switch no convierte formatos de transmisión de datos.

Router.

Dispositivo capaz de regenerar señales, concentrar múltiples conexiones, convertir formatos de transmisión de datos, y manejar transferencias de datos. También pueden conectarse a una WAN, lo que les permite conectar LAN que se encuentran separadas por grandes distancias.

TOPOLOGÍA DE REDES

La topología de red define la estructura de esta. Una parte de la definición topológica es la topología lógica, que define la forma en que los hosts acceden a los medios para enviar datos es decir consiste en describir la forma en que las máquinas se comunican a través del medio físico. Existe también la topología física, la cual consiste en la disposición real de las maquinas, dispositivos de red y los cables o medios para realizar la comunicación entre los equipos.

TOPOLOGÍAS LÓGICAS

Los dos tipos más comunes de topologías lógicas son redes de broadcast y transmisión de tokens.

La topología de broadcast simplemente significa que cada host envía sus datos hacia todos los demás hosts del medio de red. Las estaciones no siguen ningún orden para utilizar la red, sino que cada máquina accede a la red para transmitir datos en el momento en que lo necesita. Esta es la forma en que funciona Ethernet.

En cambio las topologías lógicas que trabajan por transmisión de tokens, como Token Ring y FDDI, controlan el acceso a la red al transmitir un token eléctrico de forma secuencial a cada host. Cuando un host recibe el token es su señal para enviar datos a través de la red. Si el host no tiene ningún dato para enviar, transmite el token hacia el siguiente host y el proceso se vuelve a repetir.

El Sistema de Administración y Monitoreo de Red esta diseñado para detectar redes lógicas del tipo Ethernet y para protocolos TCP/IP.

TOPOLOGÍAS FÍSICAS

TOPOLOGÍA DE BUS

En este tipo de distribución todos los nodos se encuentran conectados directamente a un enlace y no existe ningún otro tipo de conexión entre ellos. Físicamente cada host está conectado a un cable común, por lo que se pueden comunicar directamente, por otra parte la ruptura del cable hace que los hosts queden incomunicados.

La topología de bus permite que todos los dispositivos en la red puedan ver todas las señales que son transmitidas por todos los demás dispositivos, lo que puede considerarse como una ventaja si el objetivo de la red sea que todos los dispositivos obtengan esta información. Sin embargo, por la misma causa puede representar una desventaja, pues comúnmente se producen problemas de tráfico y colisiones, que se pueden disminuir los niveles de conectividad. Es la topología más común en pequeñas LAN y se emplean hubs o switches en uno de los extremos.

TOPOLOGÍA DE ANILLO

Una topología de anillo se compone de una trayectoria cerrada conformada por nodos y enlaces, en ella cada nodo se encuentra conectado solamente con sus dos nodos adyacentes.

Los dispositivos se conectan directamente entre sí por medio de cables en lo que se denomina una cadena. Para que la información pueda circular, cada estación debe transferir la información a la estación adyacente.

TOPOLOGÍA DE ESTRELLA

Esta topología tiene un nodo central desde el que divergen todos los enlaces hacia el resto de los nodos. Por el nodo central circula toda la información que se transmite por la red; para la función de nodo central generalmente son utilizados dispositivos como switches.

La ventaja principal es que permite que todos los nodos se comuniquen entre sí de manera conveniente. Su desventaja radica en la existencia de fallas en el nodo central, lo que conllevaría a que toda la red se desconecte.

TOPOLOGÍA DE ÁRBOL

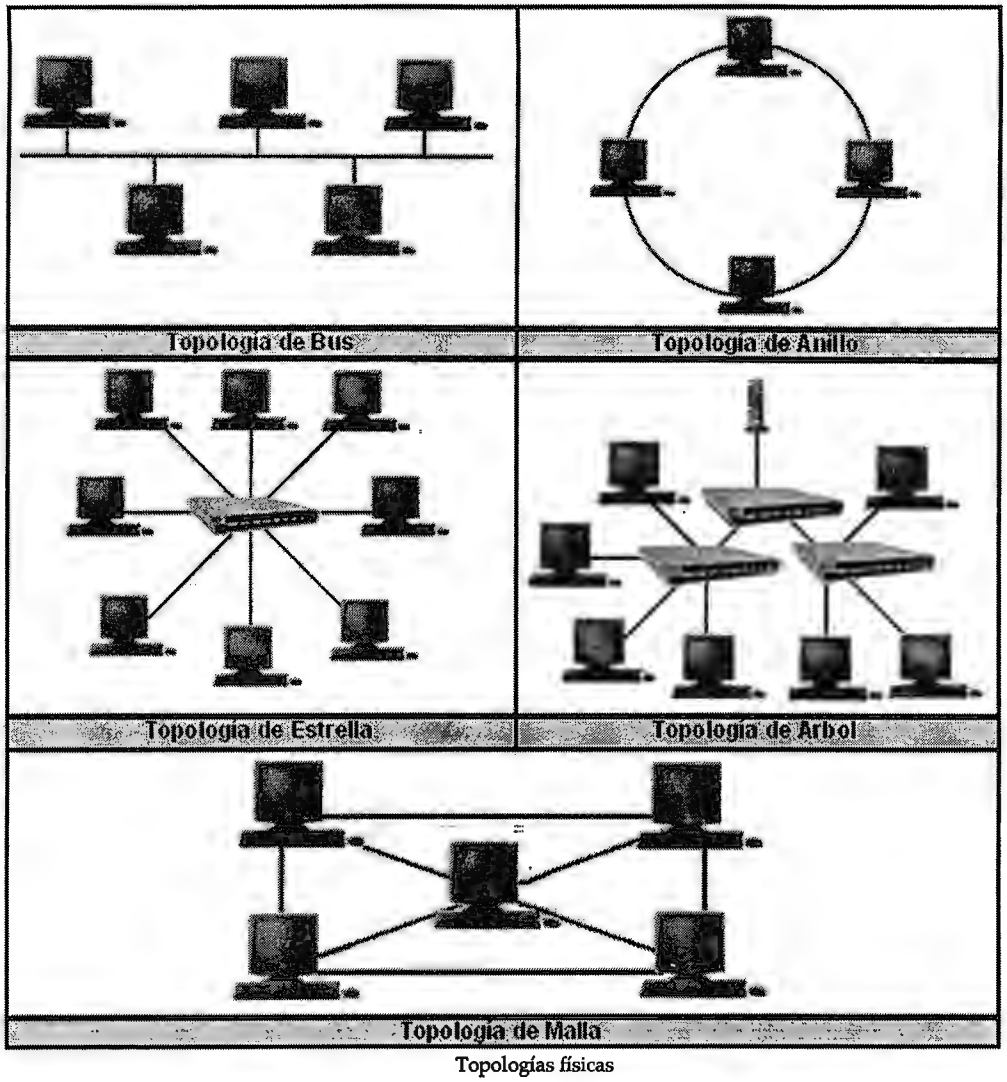
La topología de árbol es similar a la topología en estrella, salvo que no tiene un nodo central. En cambio se cuenta con un nodo de enlace troncal, generalmente ocupado por switches, desde el que se ramifican los demás nodos.

El enlace troncal es un cable con varias capas de ramificaciones, y el flujo de información es jerárquico. Conectado en el otro extremo al enlace troncal generalmente se encuentra un host servidor.

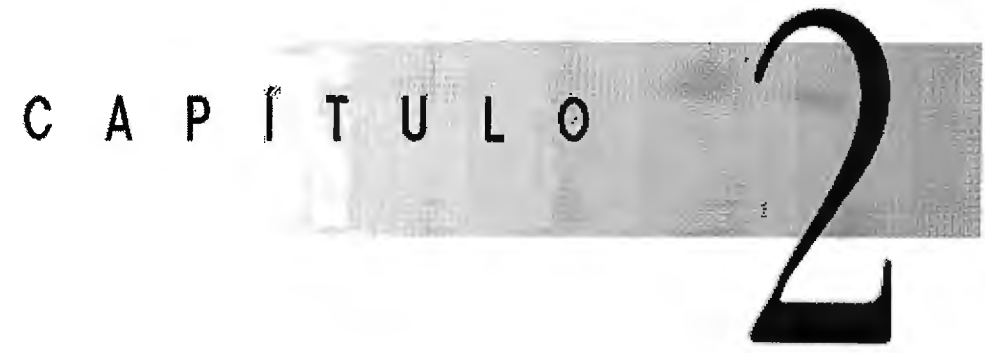
TOPOLOGÍA DE MALLA

En esta clase de topología, cada nodo es enlazado directamente con los demás nodos en la red. Tiene como ventajas una conexión redundante entre los elementos de la red, por lo que si algún enlace deja de funcionar la información aun podrá circular hacia cualquier estación designada como destino utilizando alguno de los enlaces funcionales.

La desventaja física principal radica en que es funcional solo para redes con un una pequeña cantidad de nodos, ya que de lo contrario la cantidad de medios necesarios para los enlaces, y la cantidad de conexiones con los enlaces se torna abrumadora.



Topologías físicas



INSTALACIÓN DEL SISTEMA DE ADMINISTRACIÓN Y MONITOREO DE RED

REQUISITOS DE SISTEMA

Para utilizar el Sistema de Administración y Monitoreo de Red, el equipo debe tener contar con los siguientes requerimientos:

HARDWARE

- Espacio libre en Disco Duro: 50MB
- Velocidad de procesador: 1GHz o superior
- Memoria RAM: 128MB o superior
- CD-ROM o unidad de DVD

SOFTWARE

- Sistema Operativo Microsoft Windows XP Profesional
- WinPcap 3.1
- Net-SNMP 5.3.0.1
- WiNmap
- MySQL

Si alguna de las aplicaciones aun no ha sido instalada se instalaran automáticamente con el sistema. Si ya se encuentran instaladas deberán removerse del equipo de trabajo previo a la instalación, para mayor información puede referirse a la sección Instalaciones Adicionales, pág. 41.

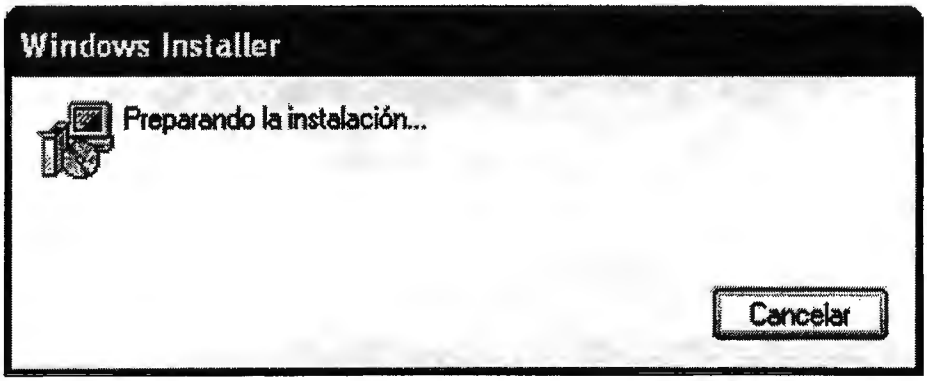
PREPARACIÓN DEL EQUIPO

Es recomendable cerrar todos los programas de Windows que estén abiertos antes de instalar el Sistema de Administración y Monitoreo de Red.

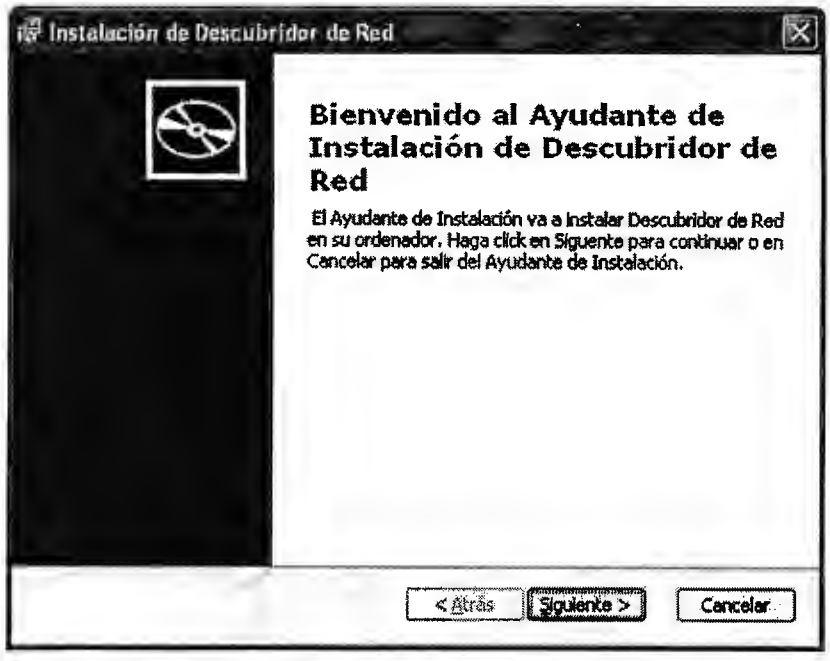
Instale el sistema desde el CD del programa.

INSTALACIÓN

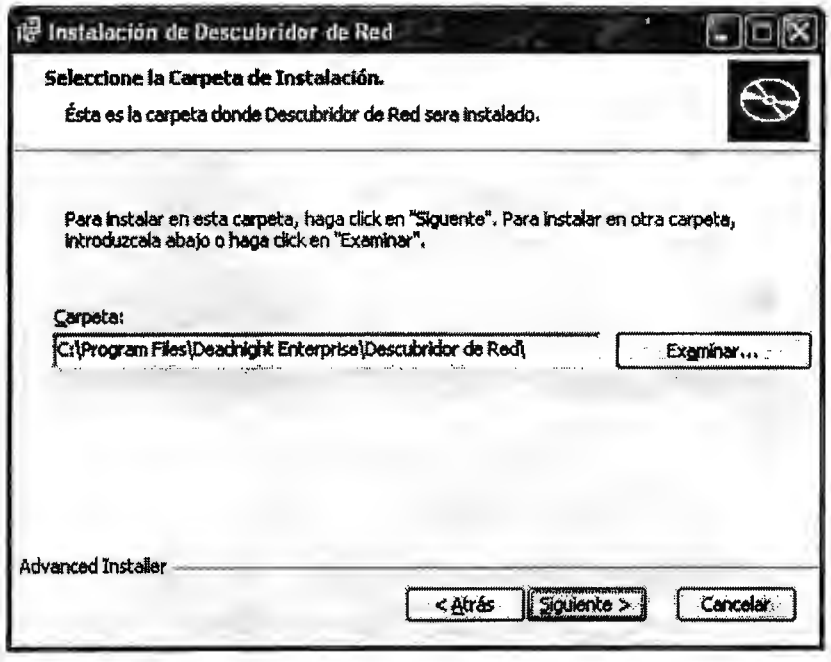
1. Introduzca el CD del Sistema de Administración y Monitoreo de Red en la unidad de CD-ROM.
2. Abra el CD desde "Mi Computadora" y seleccione el instalador que encontrara en la unidad de CD.
3. El instalador de Windows indicara que el sistema se prepara para la instalación del sistema.



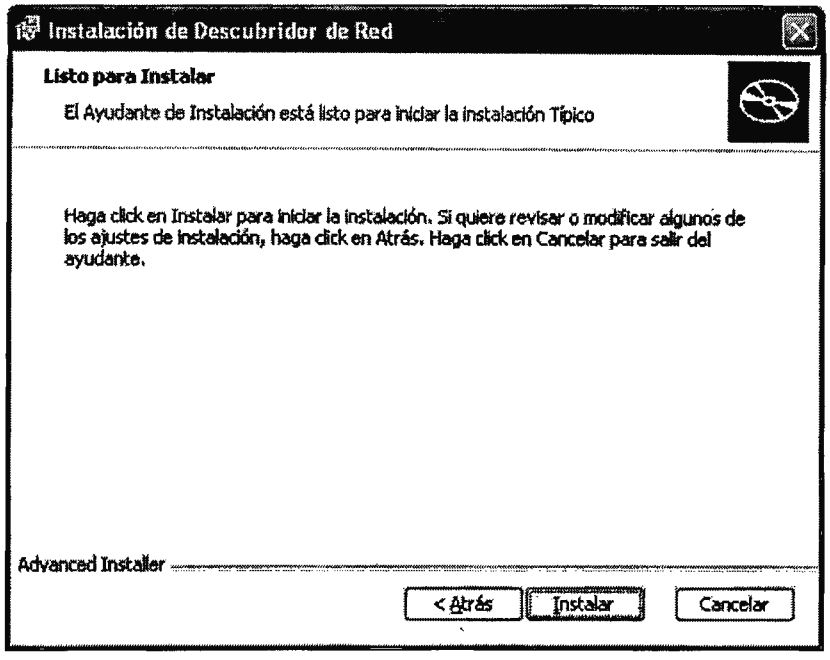
4. Espere breves segundos para obtener la ventana de bienvenida del instalador. Haga clic en Siguiente.



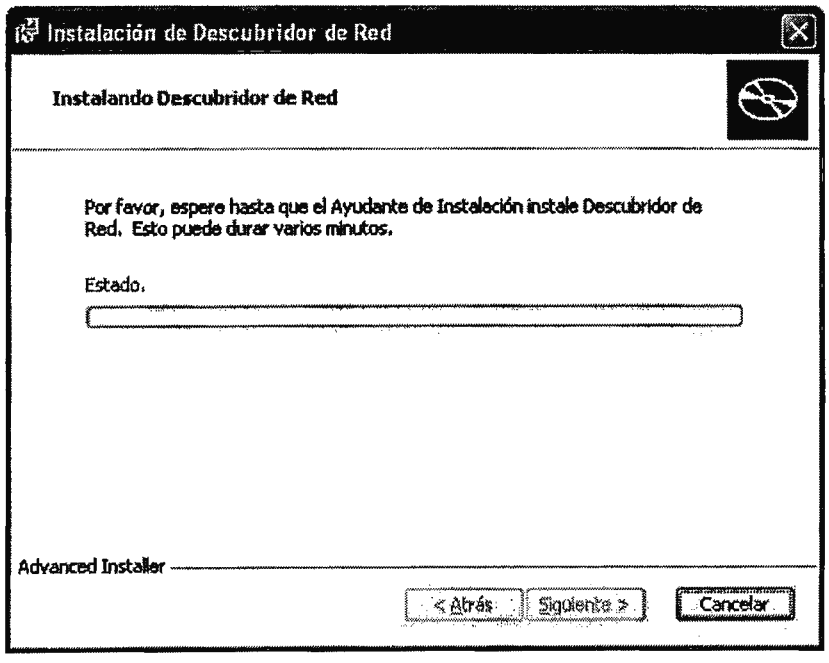
5. Seleccione la carpeta en la que desee instalar la aplicación, si lo prefiere puede utilizar la ruta sugerida, haga clic en Siguiente.

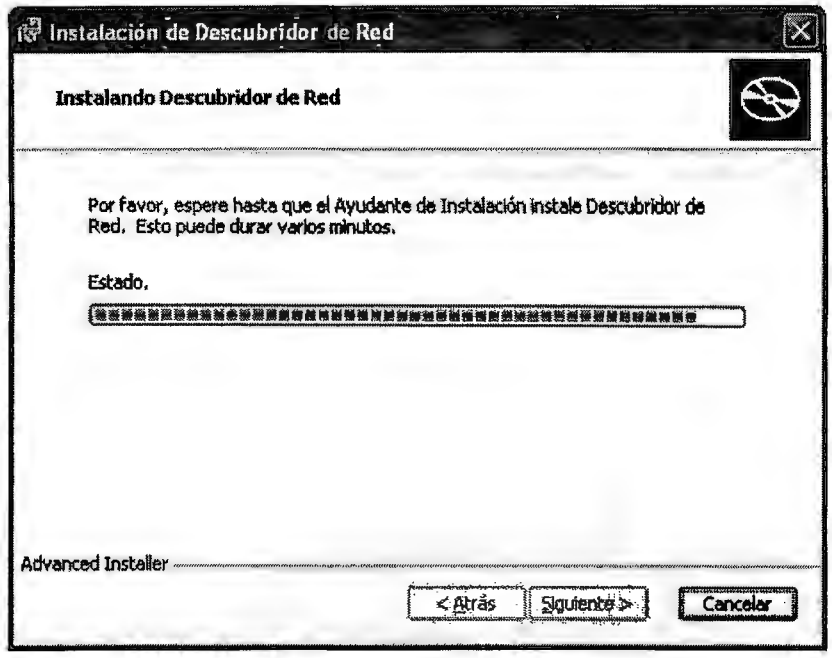


6. Obtendrá la confirmación para iniciar el proceso de instalación, clic en instalar.



7. Aparecerá a continuación el proceso de instalación, esta fase puede tardar varios minutos.





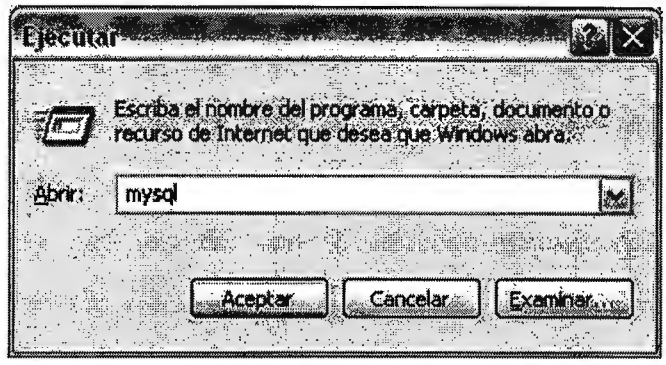
8. En este momento comenzara la instalación de las aplicaciones necesarias para la ejecución del sistema, ver Instalaciones Adicionales pág. 41, finalmente obtendrá el siguiente formulario. Haga clic en Finalizar para salir del programa de instalación.

INSTALACIÓN DE BASE DE DATOS

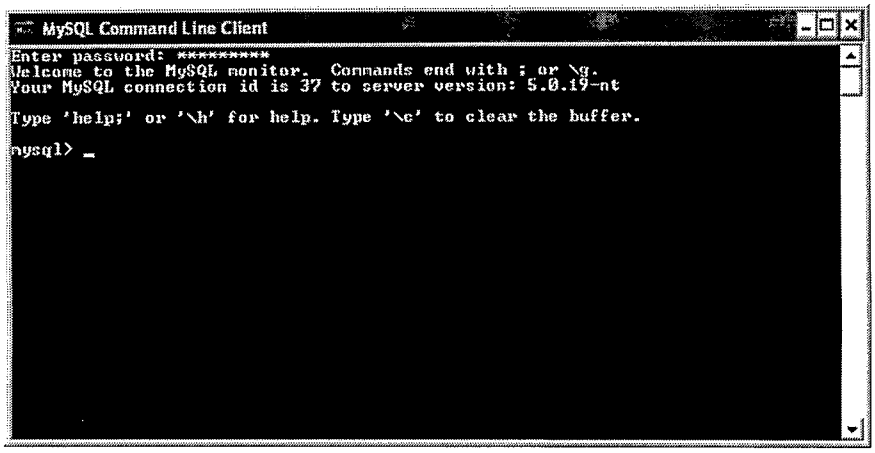
Finalizado el proceso de instalación del Sistema de Administración y Monitoreo de Red y las aplicaciones adicionales deberá instalarse la base de datos que permita almacenar los datos a obtener con la aplicación.

Nota: Para realizar el proceso siguiente deberá estar instalada la aplicación MySQL, si este paso no se ha realizado todavía por favor revise la sección Instalaciones Adicionales, MySQL 5.0

1. Presione el botón Inicio de la esquina inferior izquierda y elija Ejecutar, ingrese el comando mysql



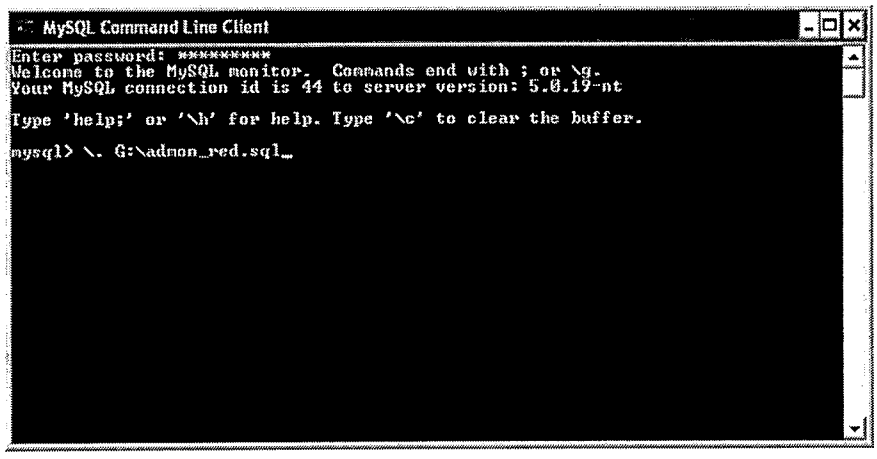
2. Se solicitara el ingreso de la contraseña establecida para acceder al servidor de MySQL



3. Finalmente digite el la siguiente línea de comando para instalar la base de datos y pueda utilizar la aplicación satisfactoriamente.

mysql> \. G:\admon_red.sql

Donde *G* representa la unidad de almacenamiento en que se instalara MySQL



CAPÍTULO 3

UTILIZANDO EL SISTEMA DE ADMINISTRACIÓN Y MONITOREO DE RED

La aplicación permite observar el correcto funcionamiento y rendimiento de la red mediante la utilización de técnicas de networking y análisis de datos por medio de protocolos de red, al mismo tiempo obtiene la distribución de los dispositivos presentes en la misma con sus características esenciales y permite el análisis de ellos mediante diferentes herramientas.

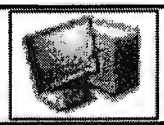
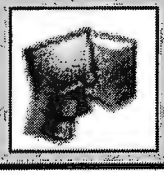
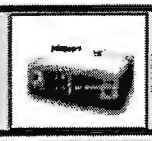
Esta sección esta diseñada para aprender acerca de la utilización del Sistema de Administración y Monitoreo de Red y sus diferentes herramientas

ICONOS EN EL SISTEMA DE ADMINISTRACIÓN Y MONITOREO DE RED

Esta herramienta es capaz de de detectar los elementos dentro de un rango de direcciones especifico, una de los principios básicos para la determinar que tipo de dispositivo ha sido encontrado radica en que dicho dispositivo deberá tener activo un agente SNMP del cual se extrae la información necesaria para representarlo como lo que en realidad es.

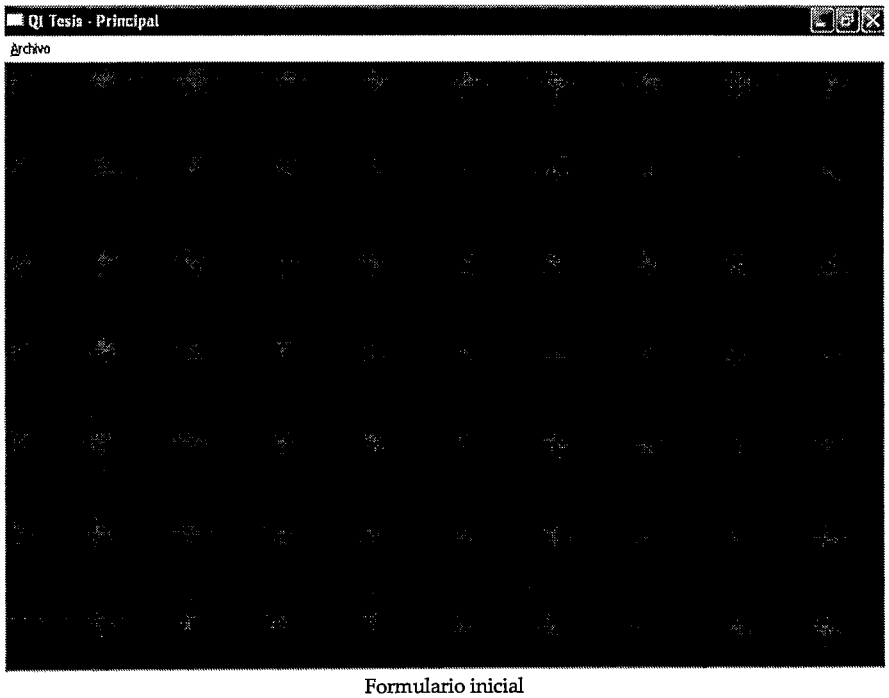
Si el agente SNMP no esta activo, o el dispositivo en estudio no soporta este protocolo de gestión, se asignara un icono genérico que indique la existencia de un objeto en un punto especifico de la red. Este símbolo podrá ser cambiado por el usuario por uno de los que se encuentran en las muestras del programa que logre representar la función de dicho equipo.

Los símbolos utilizados en son presentados en la siguiente tabla.

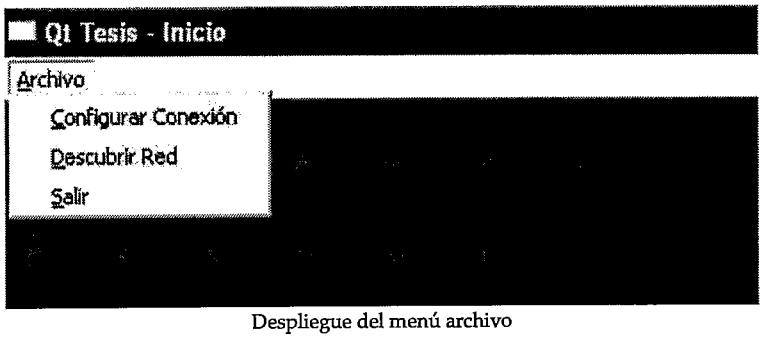
	**Estación Genérica** Este es el icono por defecto en caso que el sistema no logre determinar que tipo de equipo ha sido encontrado.
	**Estación Windows** Símbolo a asignar cuando el elemento detectado en una dirección IP sea una estación de trabajo personal que utiliza el sistema operativo Microsoft Windows en sus diferentes versiones.
	**Estación Linux** Símbolo a asignar cuando el elemento detectado en una dirección IP sea una estación de trabajo personal que utiliza alguna de las versiones del sistema operativo Linux.
	**Switch Cisco** Este icono se colocara cuando el elemento presente en una dirección IP del rango en estudio sea un switch.
	**Router Cisco** Este icono se colocara cuando el elemento detectado en la dirección IP estudiada sea un dispositivo de ruteo de paquetes

FUNCIONAMIENTO DEL SISTEMA DE ADMINISTRACIÓN Y MONITOREO DE RED

Al ejecutar el programa se presenta la ventana principal con el menú *Archivo*, desde este menú podrá seleccionar la opción de ingreso de datos para descubrimiento de la red o salir de la aplicación en el momento en que se desee.



Formulario inicial

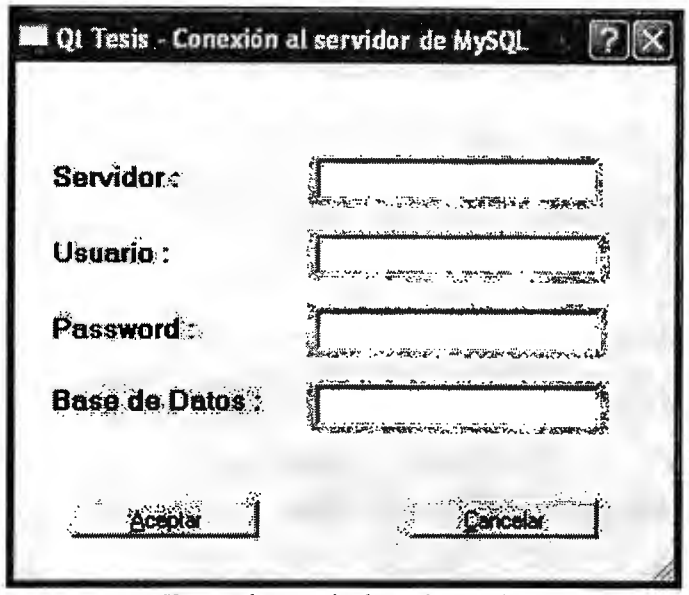


Despliegue del menú archivo

La primera de las opciones, *Configurar conexión*, permite establecer comunicación con el servidor que ejecuta la base de datos de la aplicación, para realizar dicha conexión deberán ingresarse los siguientes datos:

- *Servidor*, nombre del servidor MySQL
- *Usuario*, nombre establecido al configurar MySQL
- *Password*, consiste en establecida para limitar el acceso a la base de datos mediante una palabra clave conocida solamente por el administrador
- *Base de Datos*, nombre de la base de datos en la cual se almacena la información

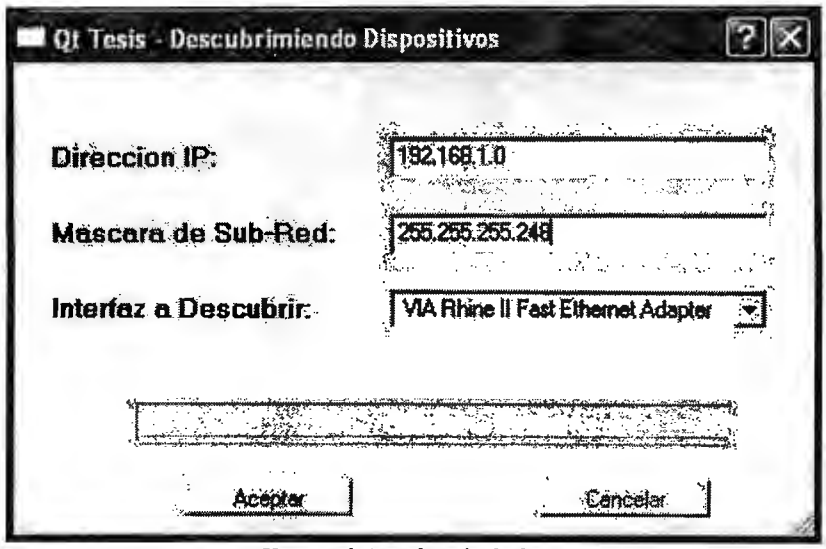
La ventana de configuración del servidor se muestra a continuación:



Ventana de conexión al servidor MySQL

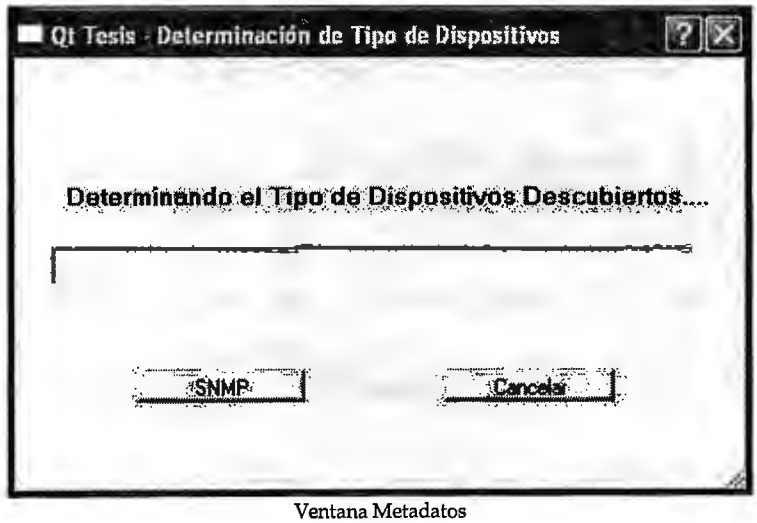
Nota: La conexión con el servidor es esencial para el funcionamiento del monitor de red. Si esta conexión se pasa por alto no será posible detectar los elementos de la red y posteriormente mostrar su estado.

Posterior al establecimiento de una conexión a la base de datos será necesario especificar una dirección IP y la mascara de subred a utilizar, con estos datos la aplicación detectara el rango de direcciones IP con las cuales se trabajara; por otra parte el sistema detectara las interfaces presentes en computadora en la que se ejecuta la aplicación, deberá elegir una interfaz alámbrica.



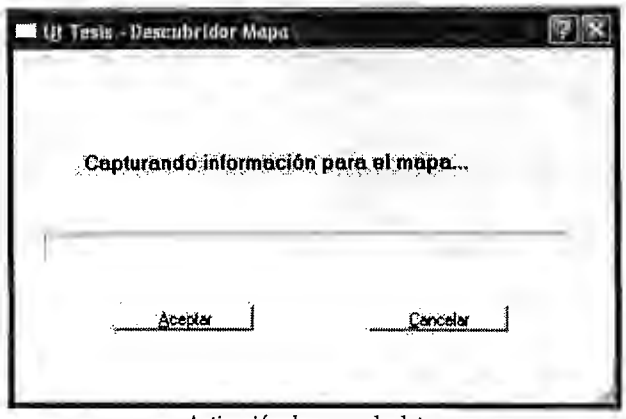
Ventana de introducción de datos

Una vez concluida la etapa de estudio de las direcciones IP del rango calculado se procede a identificar que tipo de dispositivo ha sido encontrado, esto se logra como se menciono anteriormente con el análisis de agentes SNMP que puedan existir en dichos dispositivos, durante este proceso se despliega la pantalla de metadatos.



Ventana Metadatos

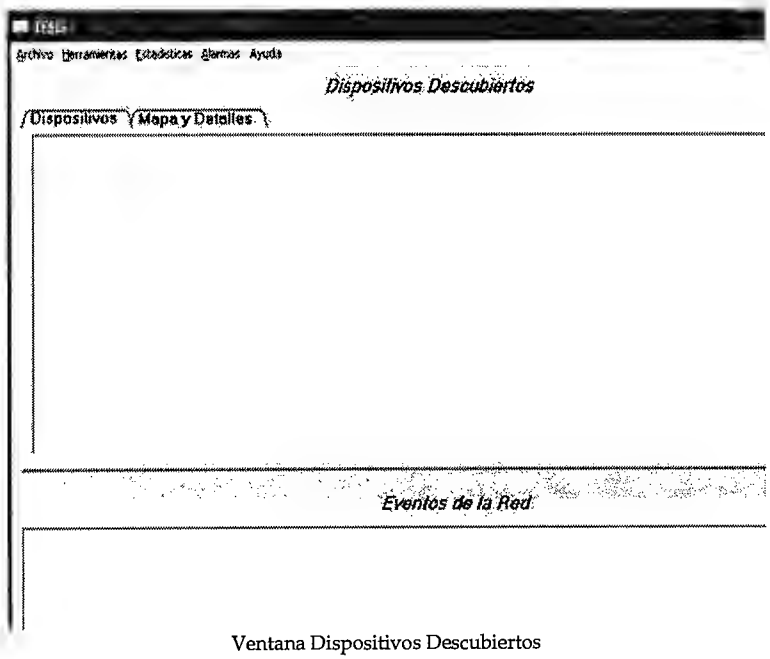
Una vez han sido detectadas las direcciones IP utilizadas y la posterior determinación los diferentes dispositivos aparece la ventana presentada que permite activar el proceso de mapeo de los dispositivos mediante el cual se activa la diagramación de los elementos de la red.



Activación de mapa de datos

Nota: El sistema de Administración y Monitoreo de red asume que la primera dirección IP correspondiente a la subred donde se encuentra la estación monitora corresponde al gateway de la misma, esto puede apreciarse gráficamente en la imagen *Ficha Dispositivo*, pág. 27.

Una vez realizados los diferentes procesos para el funcionamiento correcto del monitor de red, el sistema muestra la pantalla principal en la cual inicialmente no se muestran dispositivos hasta seleccionar la opción Cargar Red del menú archivo de la barra de menú.



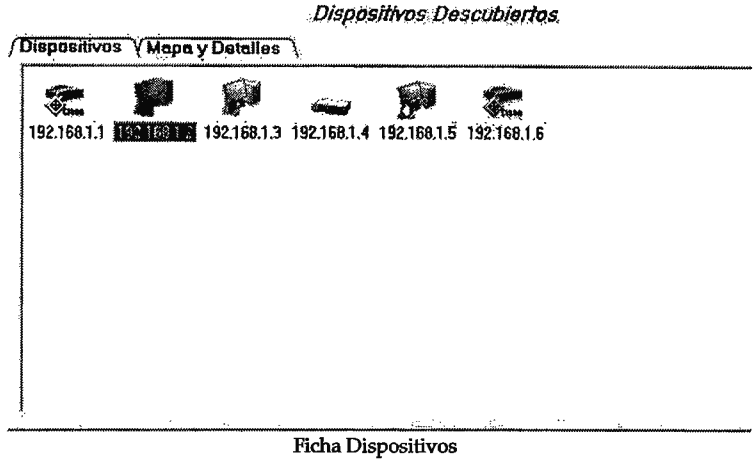
Ventana Dispositivos Descubiertos

La figura anterior cuenta con dos áreas principales, en la parte superior se encuentra la sección de Dispositivos Descubiertos, esta a su vez posee dos fichas para el análisis de red: *Dispositivos, Mapa y Detalles.* La parte inferior contendrá los acontecimientos de la red por fecha y descripción del suceso.

FICHAS EN DISPOSITIVOS DESCUBIERTOS

DISPOSITIVOS

La ficha Dispositivos, muestra las direcciones IP utilizadas y los diferentes tipos de dispositivos presentes en la red, de igual forma presentada el estado actual de estos.



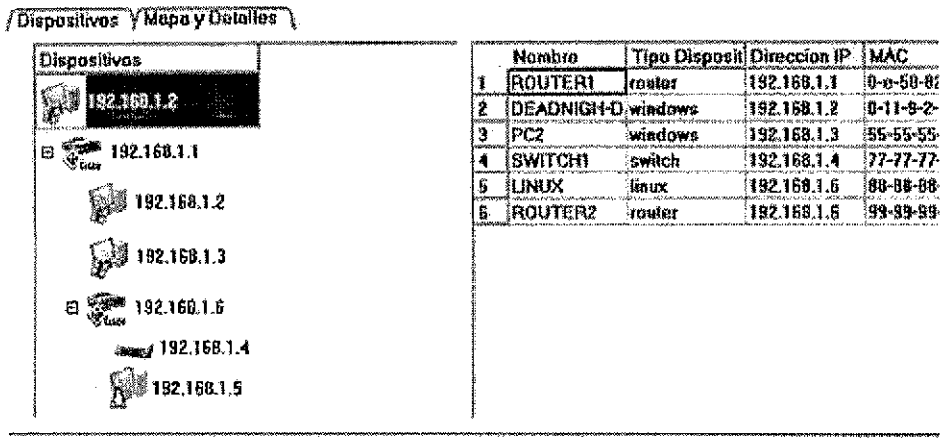
Ficha Dispositivos

Nota: Para desplegar los dispositivos de la red primero deberá seleccionar la opción Cargar Red del menú archivo

MAPA Y DETALLES

A continuación se presenta la ficha *Mapa y Detalles* esta ventana se divide en dos partes principales; el panel izquierdo que presenta la conexión entre los routers y diferentes dispositivos de la red, el panel derecho mientras tanto presenta la red a través de los datos básicos de los elementos detectados entre los cuales se mencionan:

- Nombre del equipo
- Tipo de dispositivo (router, switch, estación de trabajo)
- Su dirección de red (IP)
- Dirección física (MAC)



Ficha Mapa y Detalles

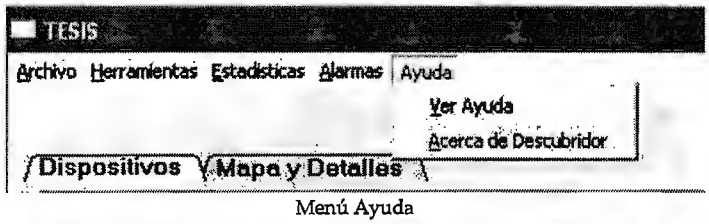
BARRA DE MENÚ

La parte superior de la pantalla principal de la aplicación se cuenta con una barra de menú que permite acceder a diferentes opciones según sea necesario.

Barra de Menú

AYUDA

El menú *Ayuda* le permite al usuario acceder a un tutorial del uso de la aplicación para ello deberá seleccionar la opción *Ver Ayuda.* Seleccionando la opción *Acerca de Descubridor,* obtendrá una la información de los desarrolladores de la aplicación así como las herramientas utilizadas para lograr su funcionamiento.

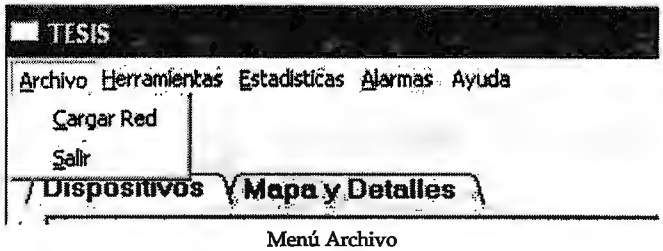


Menú Ayuda

Formulario Acerca del Descubridor de Redes

ARCHIVO

El menú *Archivo* cuenta con las opciones: *Cargar Red* y *Salir*. Cuando se han obtenido todos los datos acerca de las direcciones IP en el rango en estudio y se analiza el tipo de dispositivo presente en estas, el sistema no desplegara dichos elementos, para ello debe seleccionarse la opción *Cargar Red* de la barra de menú y podrán observar la red bajo estudio.

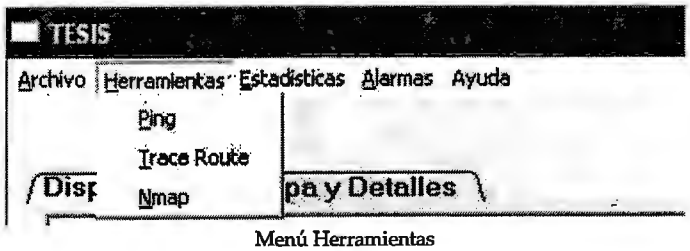


Menú Archivo

HERRAMIENTAS

El menú de *Herramientas* permite acceder a diferentes opciones para verificar el correcto funcionamiento de los equipos presentes en la red, como puede apreciarse en la imagen siguiente, las opciones a las cuales puede accederse desde acá son:

- *Ping*, herramienta ICMP basada en peticiones de respuesta de eco
- *Traceroute*, , herramienta Tracer que efectúa el trazado de ruta de un dispositivo a otro
- *Port Scan*, escaneo de los puertos de una estación de trabajo

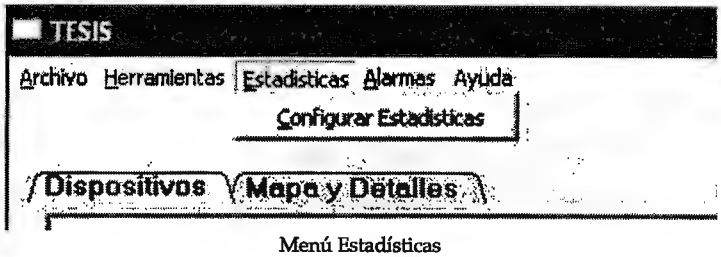


Menú Herramientas

ESTADÍSTICAS

El menú de estadísticas permite acceder a la configuración del intervalo de tiempo respecto al cual se desean obtener las diferentes estadísticas de:

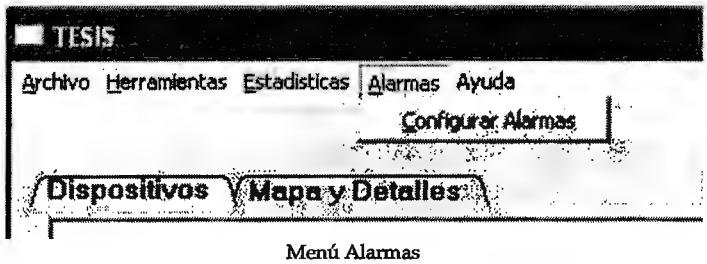
- Dirección IP en estudio
- Intervalo de fecha y hora a evaluar
- Valores a evaluar
  - CPU
  - Memoria
  - Numero de paquetes recibidos



Menú Estadísticas

ALARMAS

El monitor de red cuenta con un menú que permite la configuración de alarmas para la detección de cambios de estado de un elemento de la red. Dicho cambio consiste en reportar si un elemento deja de formar parte de la red por falta de respuesta a peticiones de eco o la respuesta a ellas si anteriormente no respondió; por otra parte informa si existe un elevado uso del procesador por parte de una estación de trabajo. Para acceder a estas opciones deberá seleccionar *Configurar Alarmas* como en la siguiente imagen.

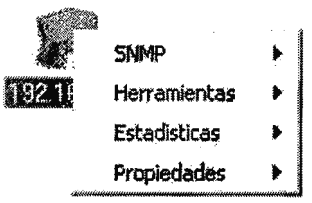


Menú Alarmas

UTILIZANDO LA PANTALLA PRINCIPAL

Una vez que los elementos detectados en la red se presentan en la ventana principal es posible utilizarlos para acceder a las diferentas herramientas del sistema así como a las características de un dispositivo especifico, esto se logra mediante un clic derecho sobre el icono que desee utilizar como objeto de estudio.

Las opciones a las que será posible acceder al realizar un clic derecho sobre un icono específico se muestran a continuación:

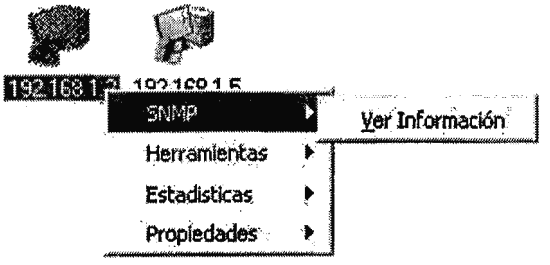


Menú emergente principal

Cada una de las opciones de la imagen anterior brindan acceso a submenús desplegables que cuentan con diferentes opciones, estudiemos cada uno de ellos con las siguientes imágenes.

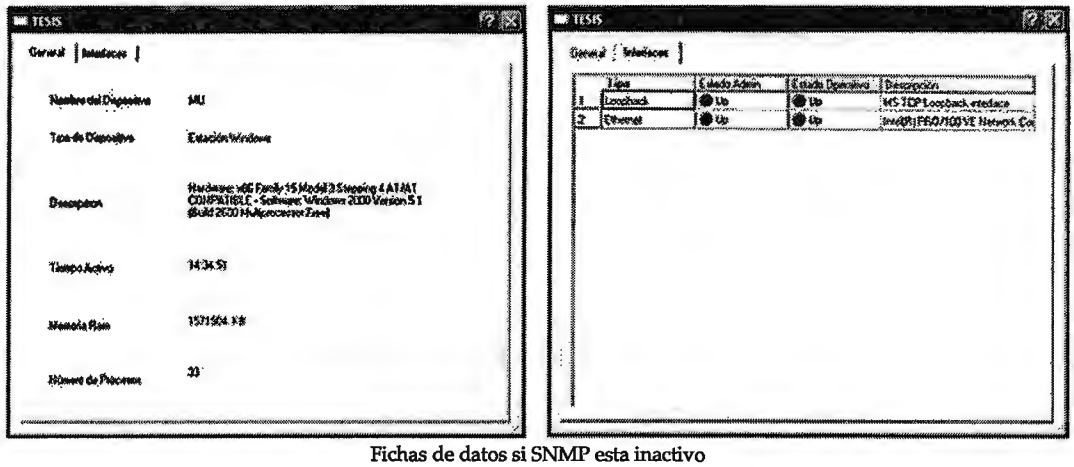
SNMP

Si el dispositivo a evaluar posee un agente activo del protocolo de gestión SNMP será posible obtener datos del funcionamiento del sistema, entre ellos una descripción general del equipo y el estado de sus diferentes interfaces.



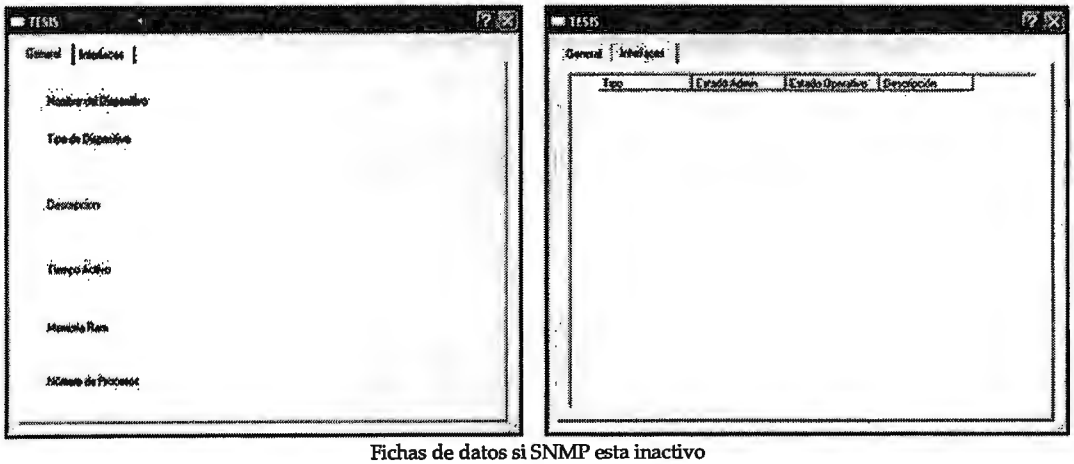
Submenú SNMP

Como puede observarse en la figura anterior, la selección del submenú *Ver Información* muestra una nueva ventana en la cual se encuentran los datos del elemento en estudio



Fichas de datos si SNMP esta inactivo

Si no se cuenta con actividad del agente SNMP esta opción todavía podrá ser seleccionada del menú desplegable, sin embargo no se obtendrán datos en ninguna de las fichas de información, esto se muestra en la imagen siguiente.



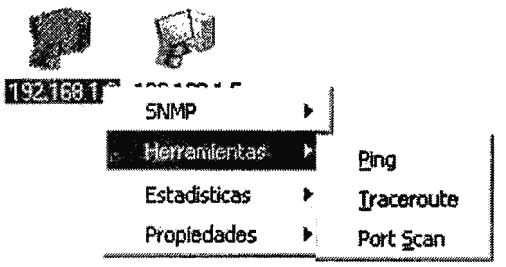
Fichas de datos si SNMP esta inactivo

Nota: Si el agente SNMP no se encuentra activo en el dispositivo puede revisar la información básica acerca de este en la opción *Propiedades* al final del menú emergente. Para mas detalles, *Propiedades* pagina 34.

HERRAMIENTAS

El submenú de *Herramientas* permite acceder a las opciones para estudiar el comportamiento de la red, al igual que la desde la barra de menú principal permite seleccionar:

- *Ping,* herramienta ICMP basada en peticiones de respuesta de eco
- *Traceroute,* , herramienta Tracer que efectúa el trazado de ruta de un dispositivo a otro
- *Port Scan,* escaneo de los puertos de una estación de trabajo

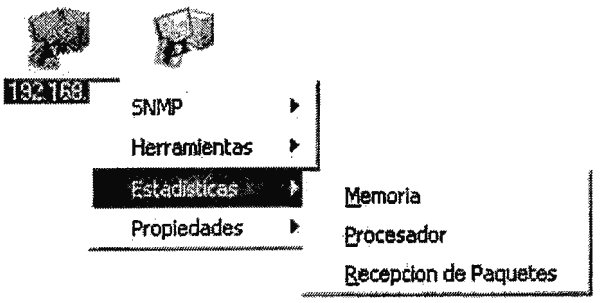


Submenú Herramientas

ESTADÍSTICAS

Este menú emergente permite acceder rápidamente a los diferentes valores de los cuales se pueden generar estadísticas presentadas de forma grafica. Los valores a evaluar pueden ser:

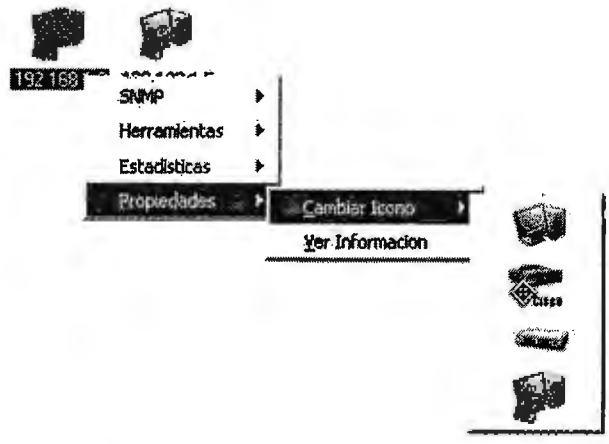
- Memoria
- Procesador
- Recepción de Paquetes.



Submenú Estadísticas

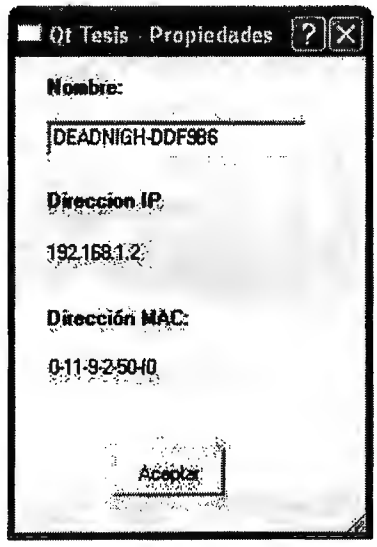
PROPIEDADES

El menú emergente de *Propiedades* cuenta con dos opciones. La primera de ellas *Cambiar Icono,* es de gran utilidad cuando el sistema no pudo determinar que tipo de dispositivo se encuentra en una dirección IP al no existir un agente SNMP activo, permitiendo seleccionar uno de los iconos predeterminados para representar el equipo de forma mas precisa.



Submenú Propiedades, opción Cambiar Icono

La segunda de las opciones, *Ver Información,* permite obtener datos básicos del elemento en estudio; cuando el agente SNMP no se encuentra activo puede seleccionarlo para obtener datos básicos acerca del dispositivo.



Submenú Propiedades, opción Ver Información

HERRAMIENTAS DEL SISTEMA DE ADMINISTRACIÓN Y MONITOREO DE RED

La aplicación cuenta con diferentes herramientas para verificar el funcionamiento de la red y estudiar el comportamiento de los elementos que la componen.

HERRAMIENTA ICMP

En una red de computadoras es importante determinar la existencia de conectividad entre los diferentes dispositivos interconectados, por tal razón se provee al sistema la capacidad de realizar peticiones de respuesta de eco desde cualquiera los equipos detectados hacia cualquier otro.

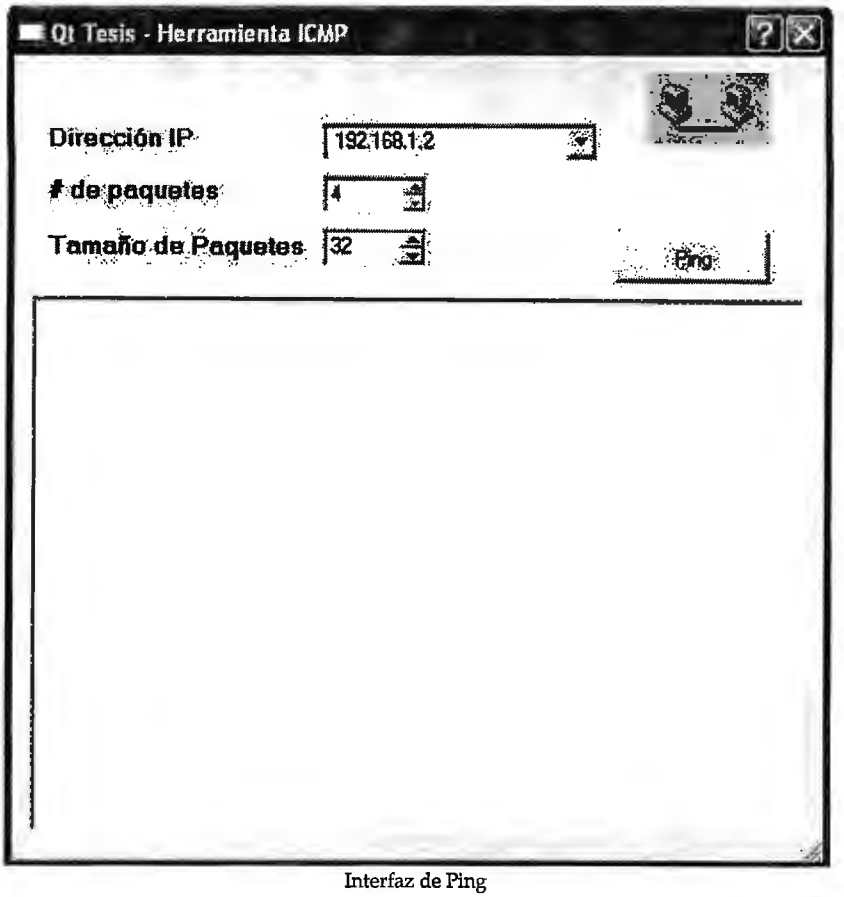
Una petición de respuesta de eco es útil para diagnosticar errores en la red, la mayoría de veces es utilizada para medir la latencia o tiempo que tardan en comunicarse dos puntos remotos.

A esta herramienta puede accederse por medio de dos métodos:

- El primer método consiste en seleccionar la opción *Herramientas* de la barra de menú la cual se ubica en la parte superior del formulario principal, seleccione la herramienta *Ping* de entre las opciones desplegadas.

- El segundo consiste en realizar clic derecho sobre el icono del dispositivo con el cual se desea comprobar conectividad y luego seleccione *Herramientas* del menú emergente con lo que se observaran las diferentes alternativas con las cuales se cuenta, elija en este caso *Ping*.

La figura siguiente presenta la interfaz de la herramienta ICMP en la cual puede realizar una prueba de *Ping*, en ella seleccione la dirección IP del dispositivo con el cual desea comunicarse del menú desplegable, posteriormente el numero de paquetes que desea utilizar para dicha prueba así como el tamaño de estos.



Interfaz de Ping

HERRAMIENTA TRACER

El sistema es capaz de detectar la ruta que debe ser recorrida para que un paquete se traslade de un elemento detectado en la red a otro, esta herramienta es útil para determinar en que segmento de la red existen retrasos cuando se realiza un intercambio de datos entre dos dispositivos.

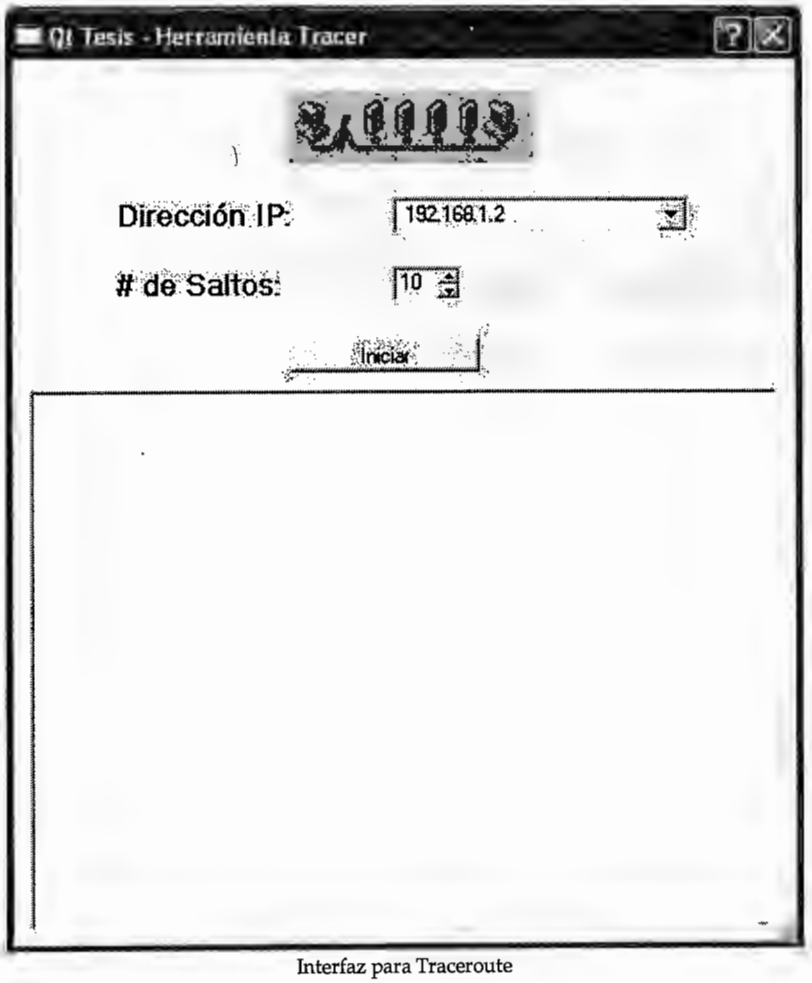
El sistema envía un paquete de petición de respuesta de eco inicialmente con un tiempo de vida (TTL) de forma encapsulada, si no se obtiene respuesta del dispositivo al cual se realizó la petición se obtendrá en su lugar un valor de tiempo de vida excedido del cual se obtiene la dirección IP del router que envía ese paquete, se procede a enviar otro paquete pero esta vez con el valor de TTL incrementado en uno y así consecutivamente hasta que se obtenga respuesta del dispositivo o se llegue a un límite de paquetes enviados.

A esta herramienta puede accederse por medio de dos métodos:

- El primer método consiste en seleccionar la opción *Herramientas* de la barra de menú la cual se ubica en la parte superior de la ventana principal, seleccione *Trace Route* de entre las opciones desplegadas.

- El segundo consiste en realizar clic derecho sobre el icono del dispositivo con el cual desea comunicarse y luego seleccione *Herramientas* del menú emergente con lo que se observaran las opciones con las cuales se cuenta, elija en este caso *Trace Route.*

La interfaz de la herramienta Tracer se muestra en la imagen presentada a continuación:



Interfaz para Traceroute

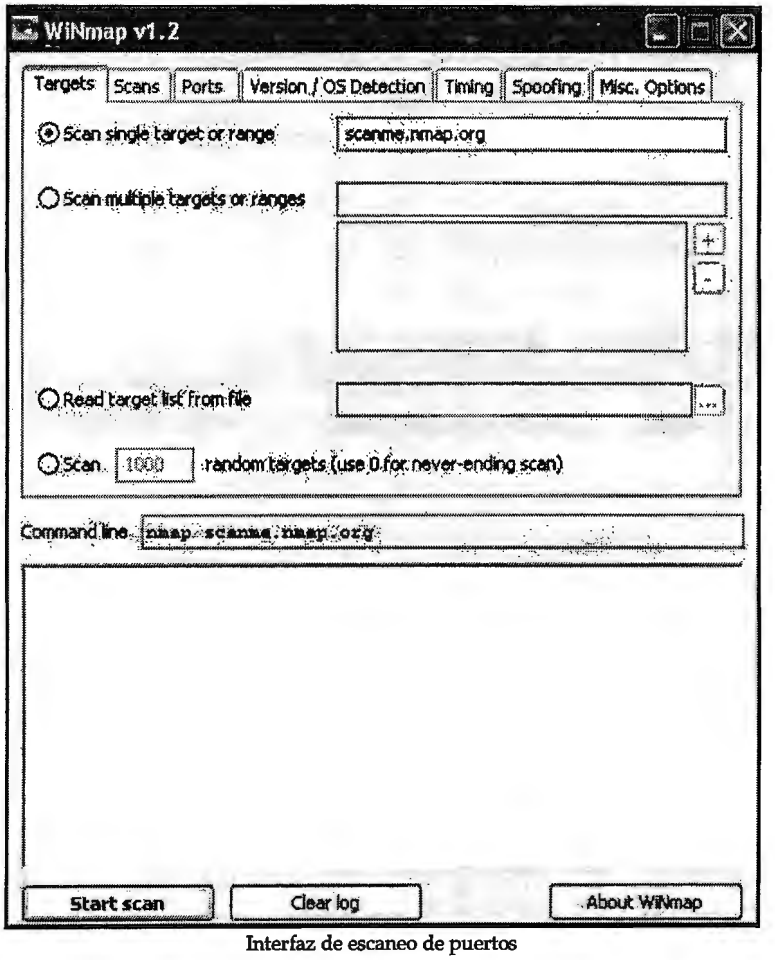
ESCANEO DE PUERTOS

El sistema es capaz de realizar un escaneo sistemático de puertos en las estaciones de trabajo detectados durante los sondeos de la red. Para realizar esta operación se utiliza la herramienta de código abierto para exploración de red y auditoria de seguridad *Nmap* para Windows, *WiNmap*.

A esta herramienta puede accederse por medio de dos métodos:

- El primer método consiste en seleccionar la opción *Herramientas* de la barra de menú la cual se ubica en la parte superior de la ventana principal, posteriormente seleccione *Nmap* de entre las opciones desplegadas.

- El segundo consiste en realizar clic derecho sobre el icono del dispositivo en el cual se desea analizar sus puertos y luego seleccione Herramientas del menú emergente con lo que se observaran las opciones con las cuales se cuenta, elija en este caso Port Scan.

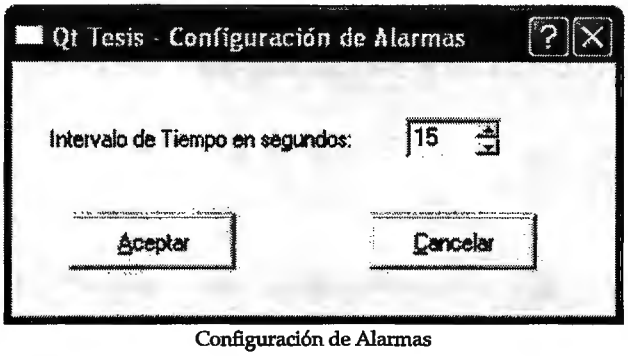


Interfaz de escaneo de puertos

ESTABLECIMIENTO DE ALARMAS

En una red de computadoras es esencial estar al tanto de los diferentes acontecimientos que se presentan en una red. La detección de comportamientos anormales en la red es una necesidad primordial por lo que se provee al sistema la capacidad de detectar tanto la falta de comunicación de con uno de los dispositivos o el reestablecimiento de esta a través de peticiones de respuesta de eco, de igual forma se identifica si el nivel de desempeño de una estación de trabajo es un valor que supera los considerados como aceptables.

Para activar el sistema de alarma deberá seleccionar la opción *Configurar Alarmas* del menú *Alarmas* en la ventana principal.



Configuración de Alarmas

Al establecer el intervalo de tiempo se activa el proceso mediante el cual el sistema indicara si uno de los elementos deja de responder a las peticiones de eco o si sobrepasa el valor establecido respecto al uso del procesador. El establecimiento del valor de CPU es configurable en la ventana *Configuración de Estadísticas*.

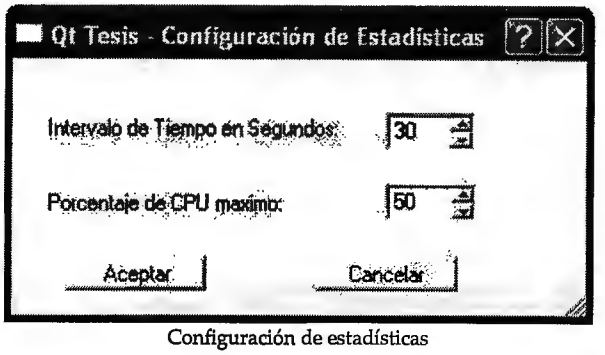
ESTADÍSTICAS

El sistema de monitoreo permite realizar análisis estadísticos respecto a diferentes valores de importancia de una estación de trabajo:

- Dirección IP en estudio
- Intervalo de fecha y hora a evaluar
- Valores a evaluar
    - CPU
    - Memoria
    - Numero de paquetes recibidos

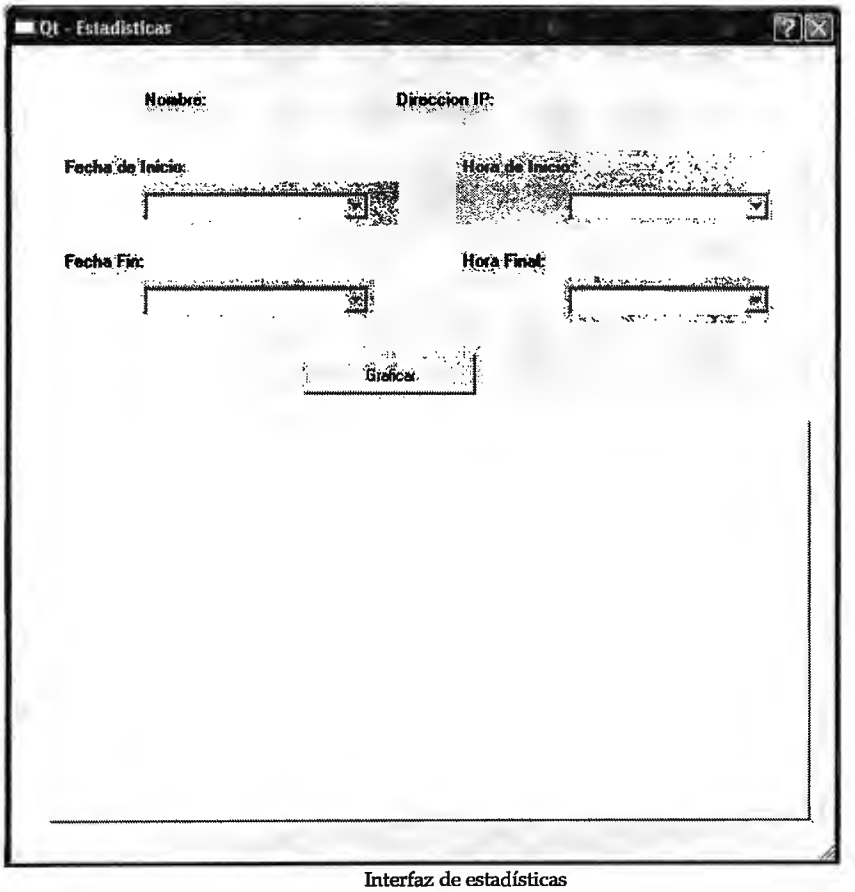
El uso de esta herramienta consiste en el proceso siguiente:

I. El primer paso es la selección de la opción Configurar Estadísticas de la barra de menú con lo que obtendrá la ventana de la imagen siguiente, establezca el intervalo de tiempo a utilizar.



Configuración de estadísticas

II. Realice un clic derecho sobre el icono del dispositivo del cual se desean obtener datos de estudio y luego seleccionar que tipo de dato desea que sean presentados.



Interfaz de estadísticas

INSTALACIONES ADICIONALES

Posterior a la copia de los archivos del sistema el asistente de instalación del Sistema de Administración y Monitoreo de red iniciara automáticamente el proceso de instalación de las aplicaciones requeridas para utilizar el sistema.

Si las aplicaciones ya se encuentran instaladas remuévalas de su equipo de trabajo previo a continuar con la instalación del sistema.

Posterior a la finalización de este proceso siga los pasos de ***Instalación de Base de Datos,*** Pág. 18.

NET-SNMP 5.3.0.1

Net-SNMP es una serie de aplicaciones utilizadas para la implementación del protocolo SNMP en sus diferentes versiones SNMP v1, SNMP v2c y SNMP v3 que utilizan IPV4 al igual que IPV6.

Este paquete se baso originalmente en la implementación de la Universidad de Carnegie Mellon SNMP (la versión 2.1.2.1), pero ha desarrollado apreciablemente desde entonces.

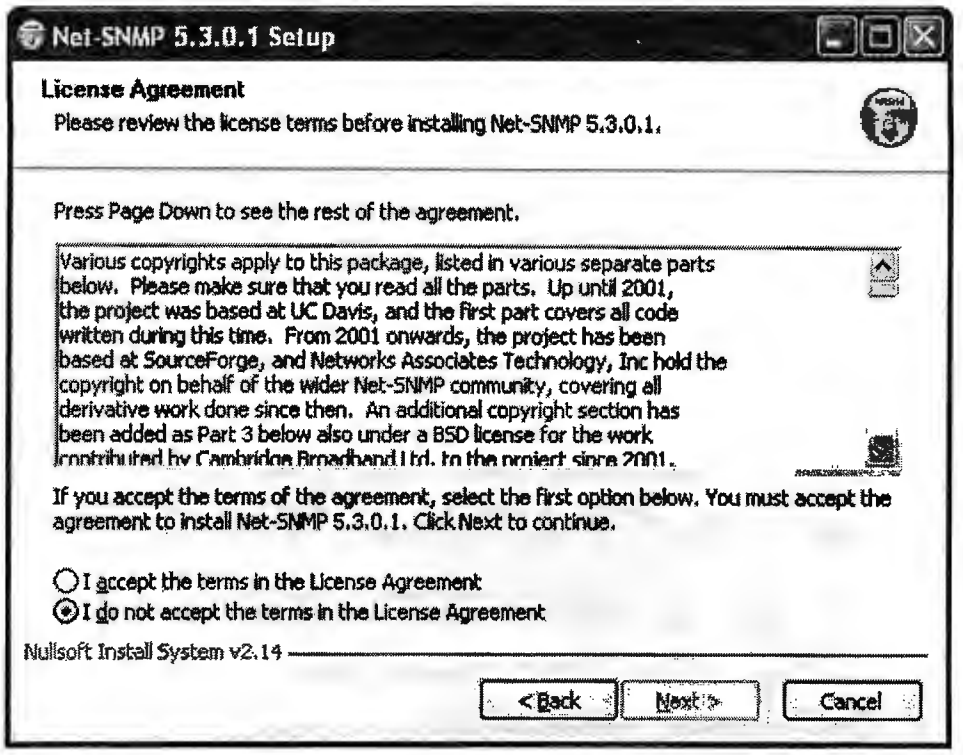
Puede obtener esta aplicación gratuitamente de:

http://net-snmp.sourceforge.net/download.html

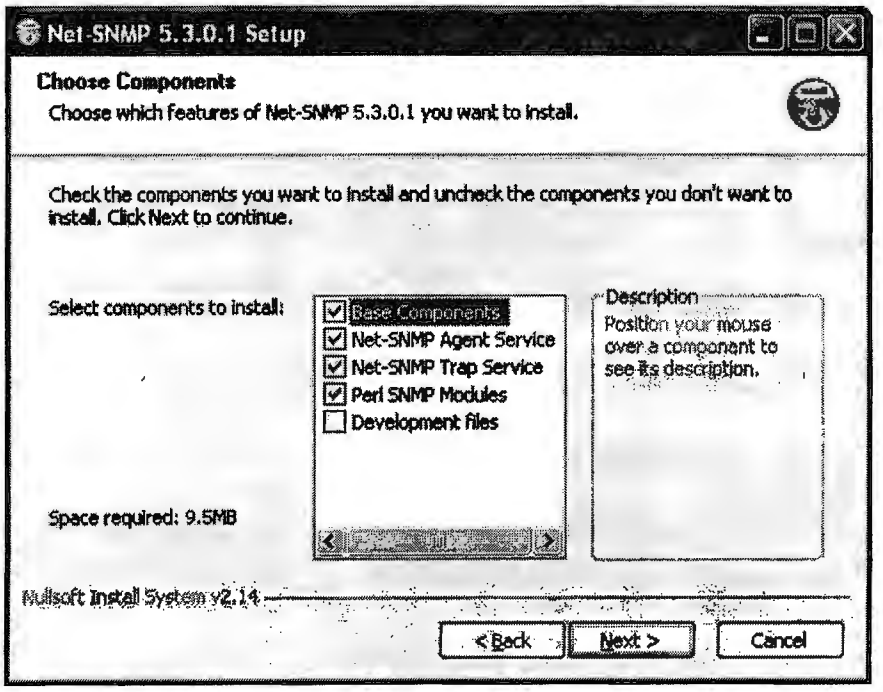
Finalizado el asistente de instalación del Sistema de Administración y Monitoreo de red iniciara automáticamente el instalador de Net-SNMP 5.3.0.1

1. Obtendrá la siguiente pantalla de bienvenida.

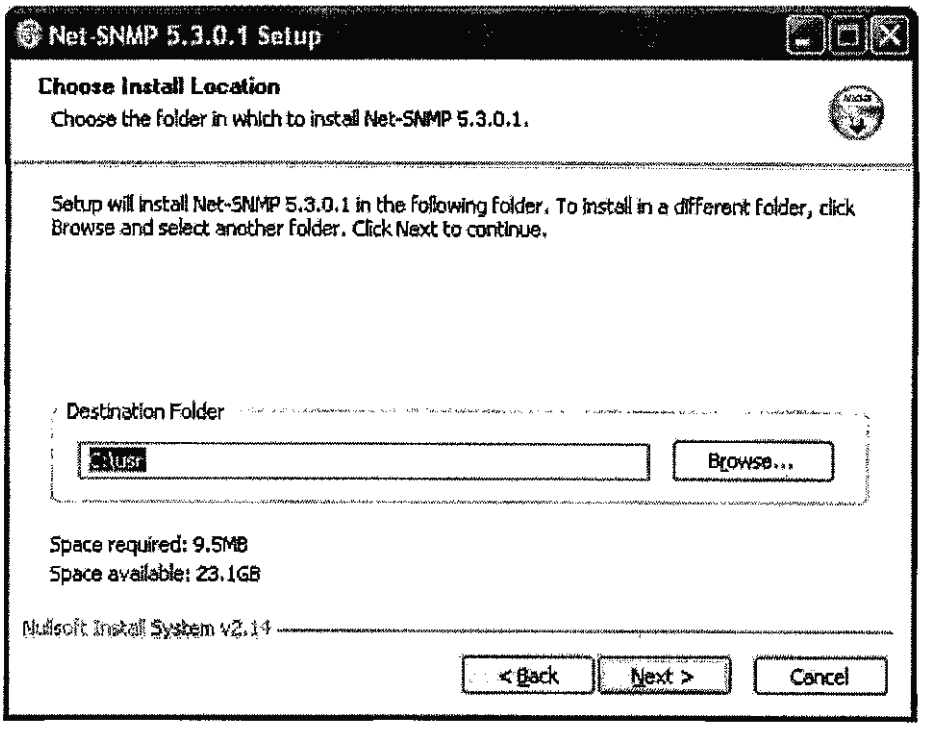
2. Acepte la licencia de uso de esta instalación y seleccione Siguiente



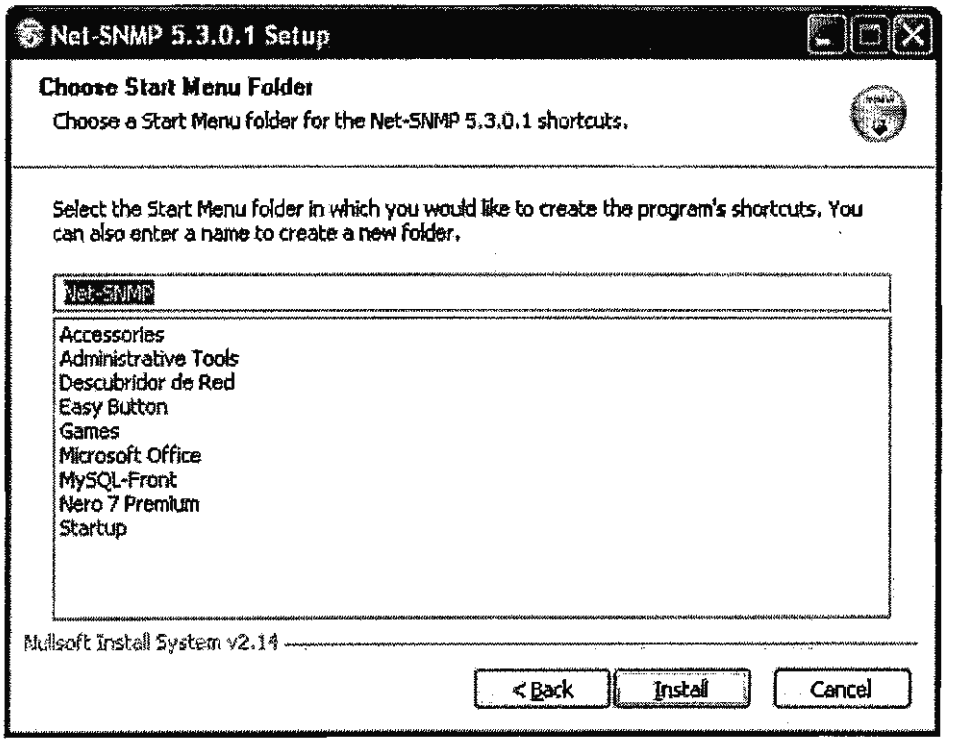
3. Elija los componentes que desea instalar de Net-SNMP, puede dejar las opciones seleccionadas por defecto.



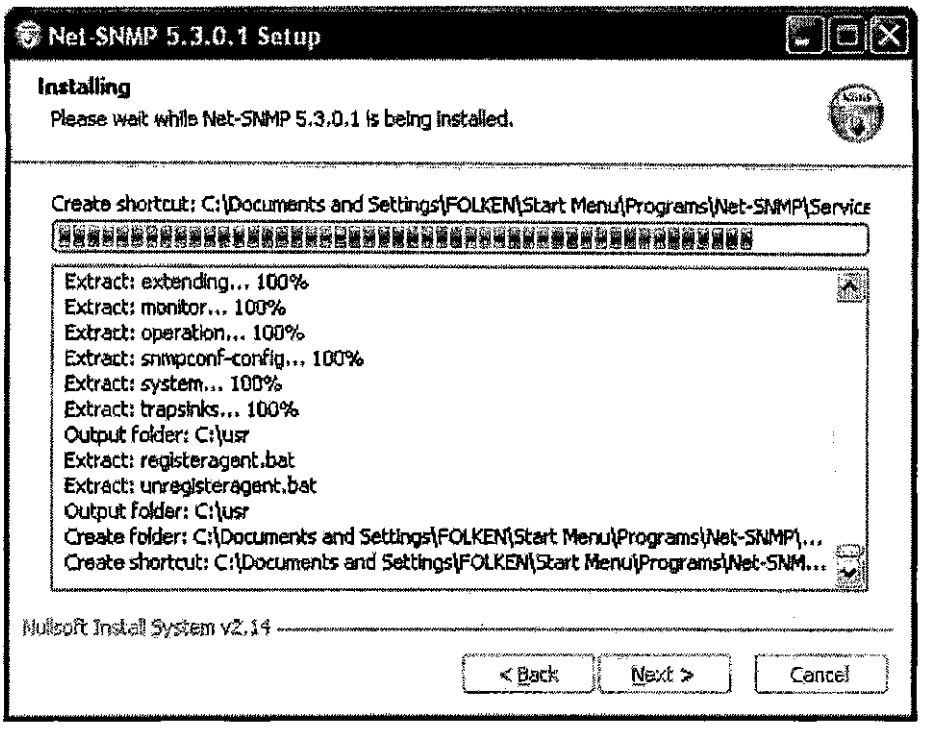
4. Escoja la ruta de instalación, o de clic en siguiente para utilizar el directorio sugerido



5. Elija el fólder en el cual se cree el acceso a esta librería. Oprima la opción Instalar.



6. Aparecerá el indicador de progreso de instalación de Net-SNMP, espere breves minutos para finalizar con este proceso.



7. Espere la confirmación de la instalación satisfactoria de la aplicación y cierre el asistente.

WINMAP v1.2

WiNmap es una herramienta del GUI de Windows para el nmap. Se basa en el Nmap v3.95. Para que fuese una herramienta fácil de utilizar WinNmap se diseñó con un esquema similar al del front-end para GTK, pero con más opciones. Como herramienta GUI el usuario podrá utilizarla con simplemente la selección de opciones. Esta versión de Nmap vuelve fácil el uso de este en ambiente Win32.

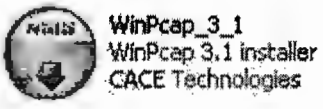
Puede descargar esta aplicación de forma gratuita del sitio web:

http://www.philippsworld.net/software_winmap.htm

WINPCAP 3.1

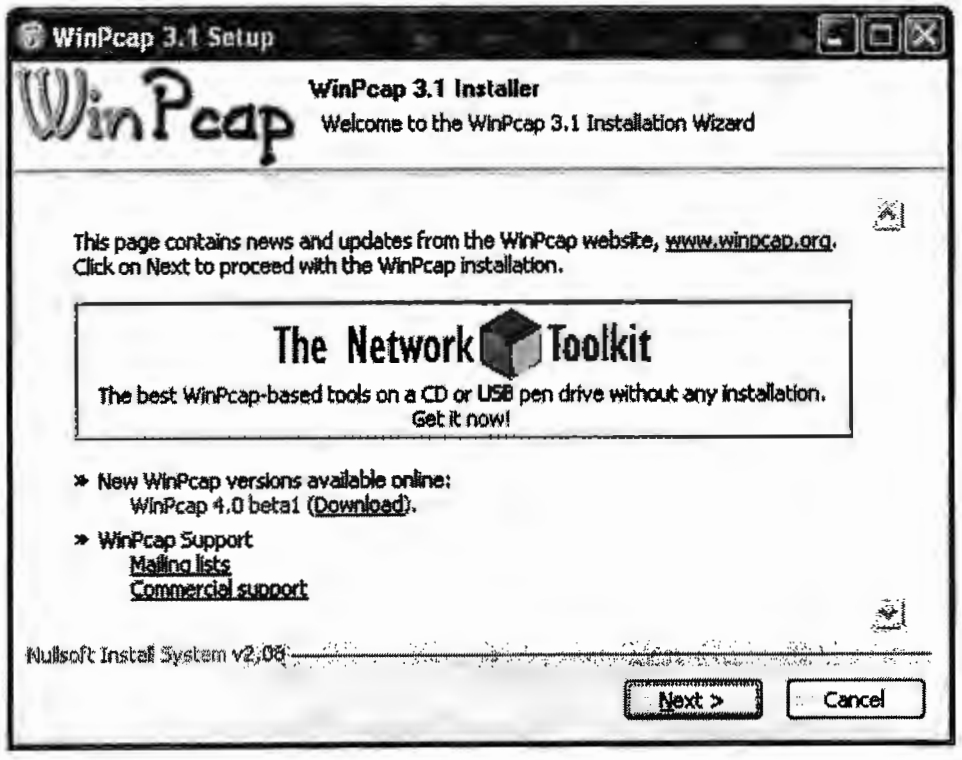
WinPcap es una biblioteca abierta para la captura de paquete y análisis de red para las plataformas Win32. La versión para el sistema operativo Linux es libpcap. Puede obtener esta aplicación de:

http://www.winpcap.org/

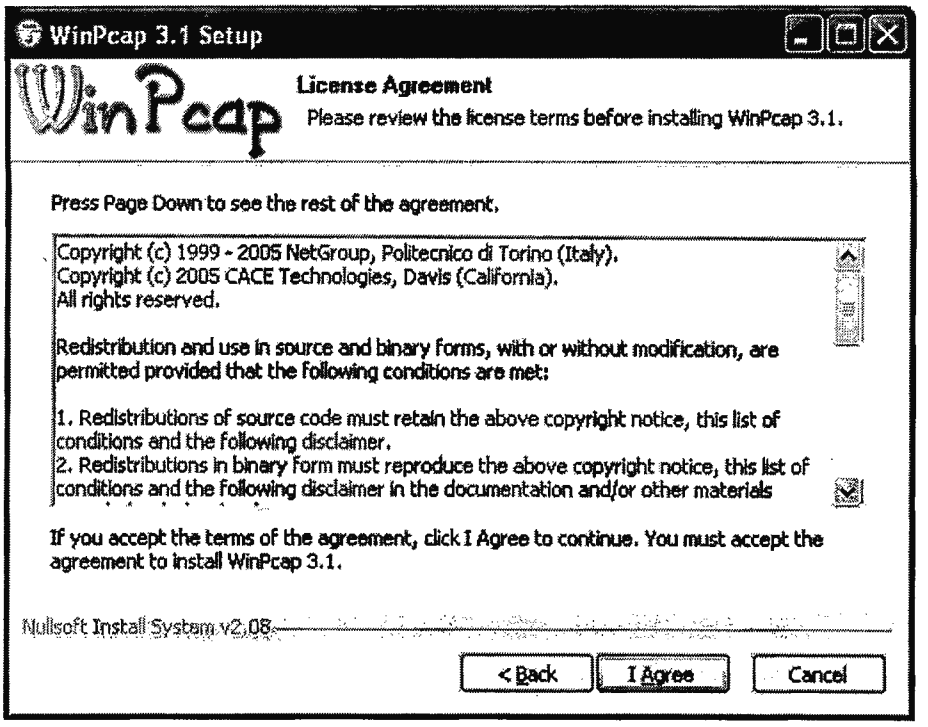


Finalizado el asistente de instalación de Net-SNMP 5.3.0.1 iniciara automáticamente el instalador de WinPcap 3.1.

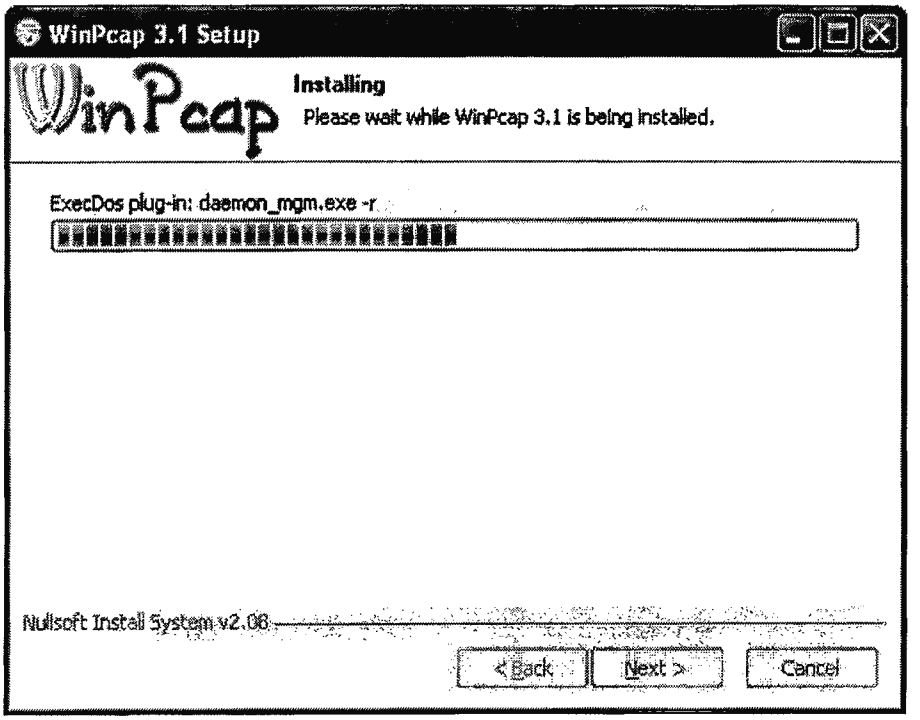
1. Obtendrá la siguiente pantalla de bienvenida, clic en siguiente



2. Debe estar de acuerdo con los términos de uso para continuar con el proceso de instalación.



3. Aparecerá el indicador de progreso de instalación de WinPcap, espere breves minutos para finalizar con este proceso.



4. Espere la confirmación de la instalación satisfactoria de la aplicación y cierre el asistente.

NOTA: Si WinPcap 3.1 fue instalado previamente en la estación de trabajo previamente deberá ser descargado el archivo **3.1beta4-WpdPack.zip** del sitio **http://www.winpcap.org/archive/** finalmente libere los archivos contenidos en el archivo zip en la misma carpeta de instalación que eligió para WinPcap.

MySQL SERVER 5.0

MySQL es un sistema de administración relacional de bases de datos. Una base de datos relacional archiva datos en tablas separadas en vez de colocar todos los datos en un gran archivo. Esto permite velocidad y flexibilidad. Las tablas están conectadas por relaciones definidas que hacen posible combinar datos de diferentes tablas sobre pedido.

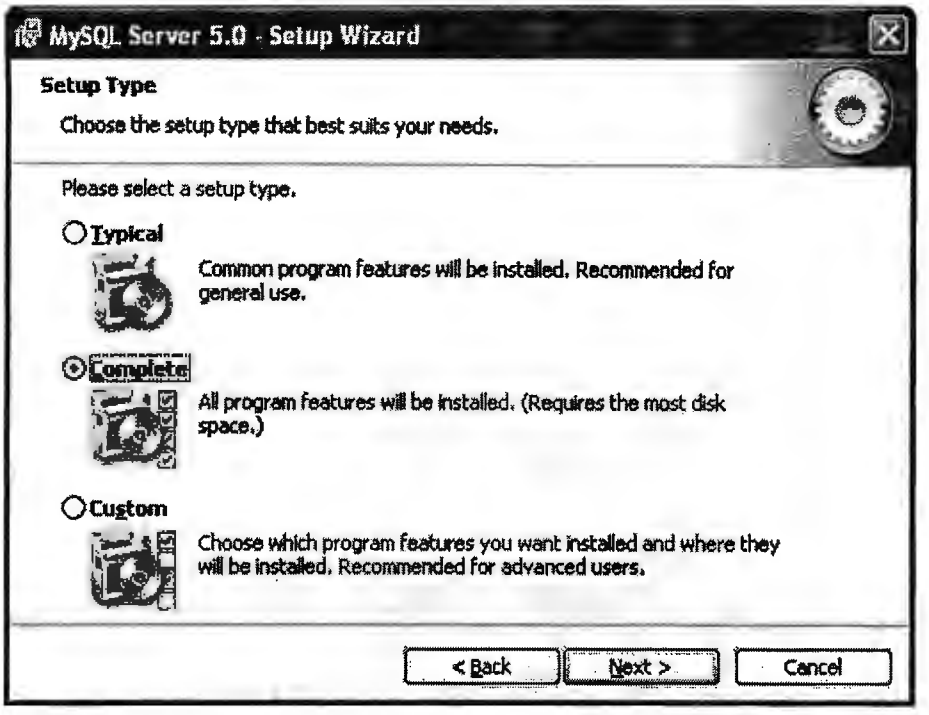
Puede obtener esta aplicación gratuitamente de:

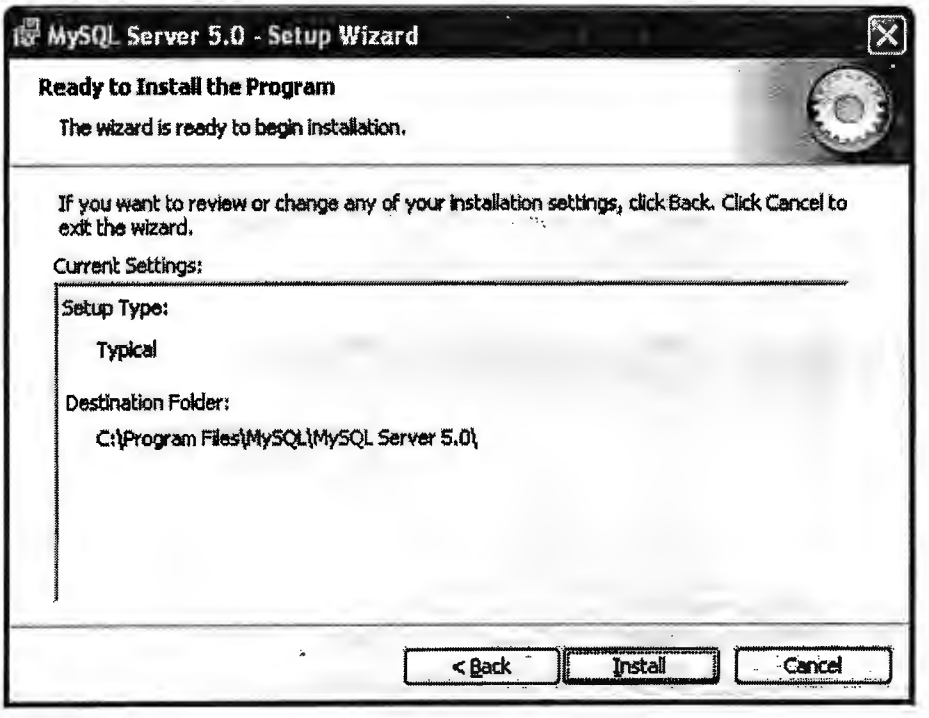
http://dev.mysql.com/downloads/mysql/5.0.html

Finalizado el asistente de instalación de WinPcap 3.1 iniciara automáticamente el instalador de MySQL 5.0.

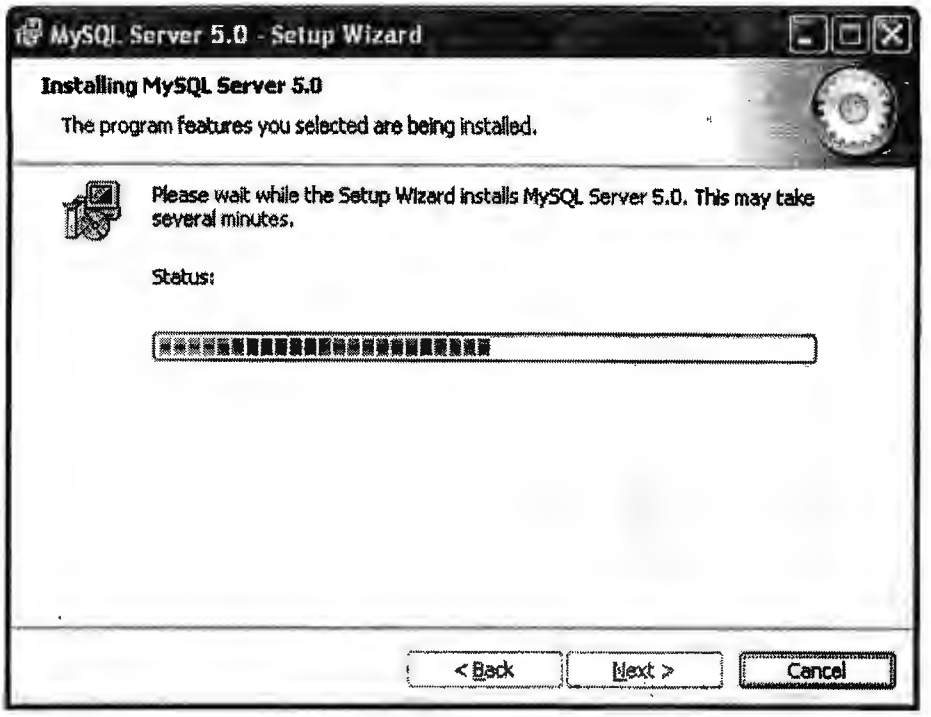
1. Obtendrá la siguiente pantalla de bienvenida, clic en siguiente.

2. Elija el tipo de instalación a realizar y confírmela en la siguiente ventana.

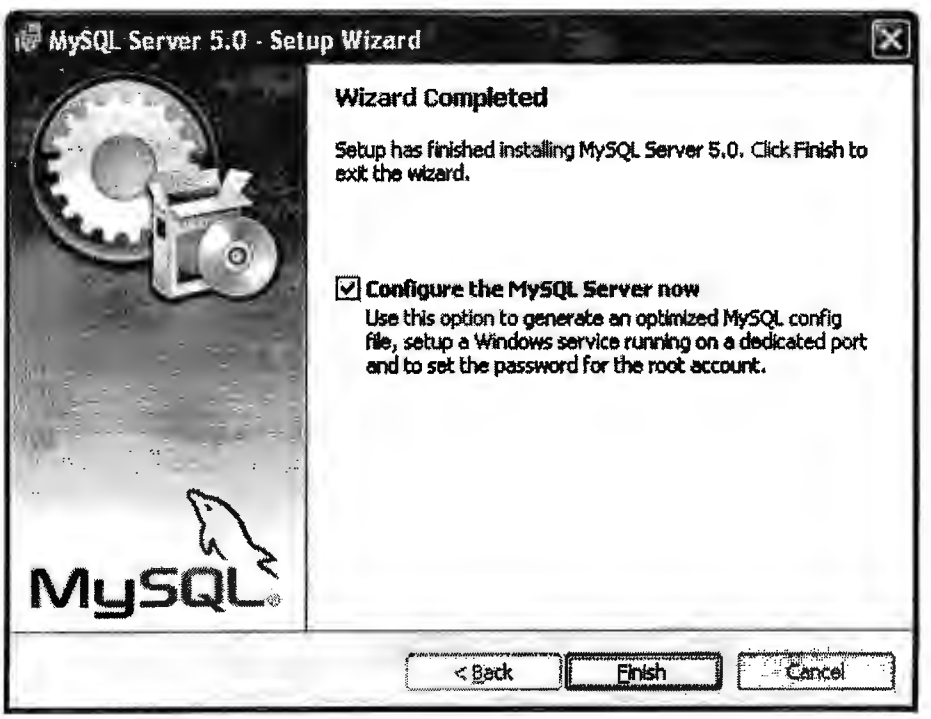




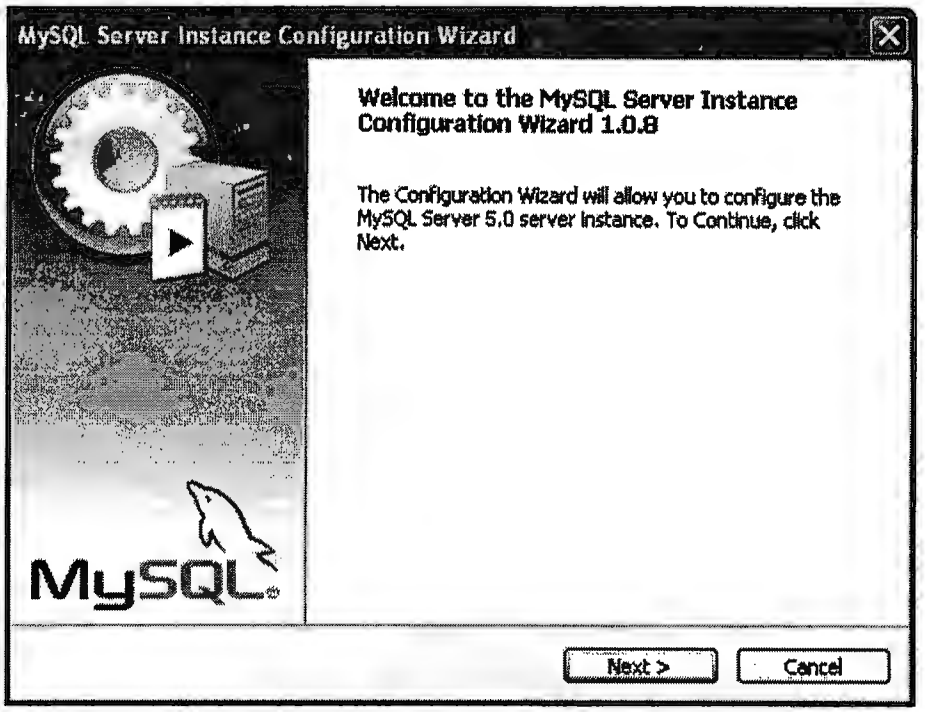
3. Aparecerá el indicador de progreso de instalación de MySQL, espere breves minutos para finalizar con este proceso.



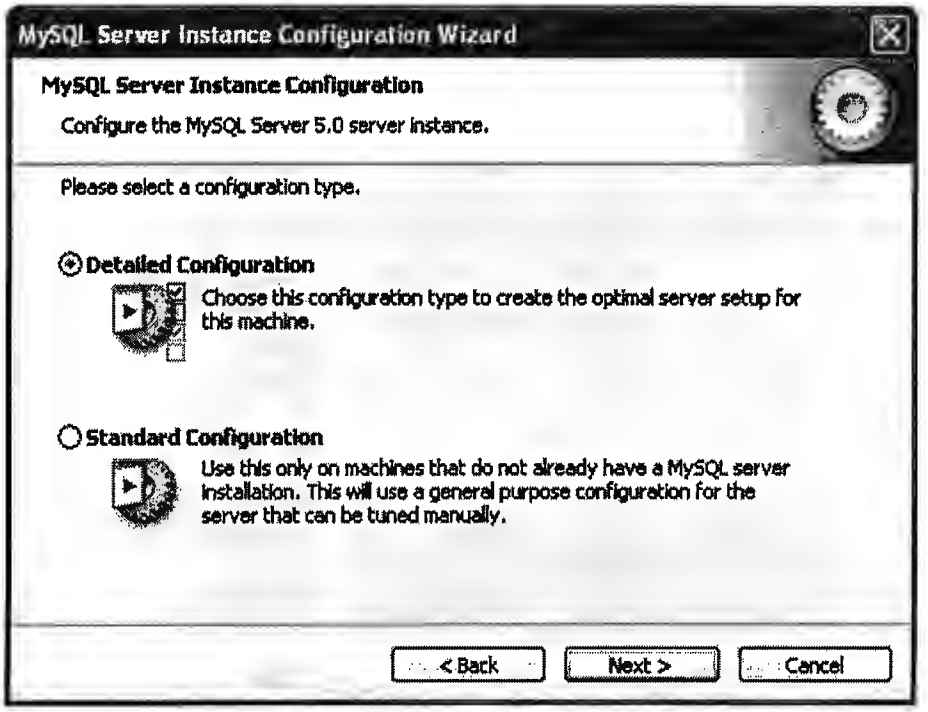
4. Espere la confirmación de la instalación satisfactoria de la aplicación y cierre el asistente.



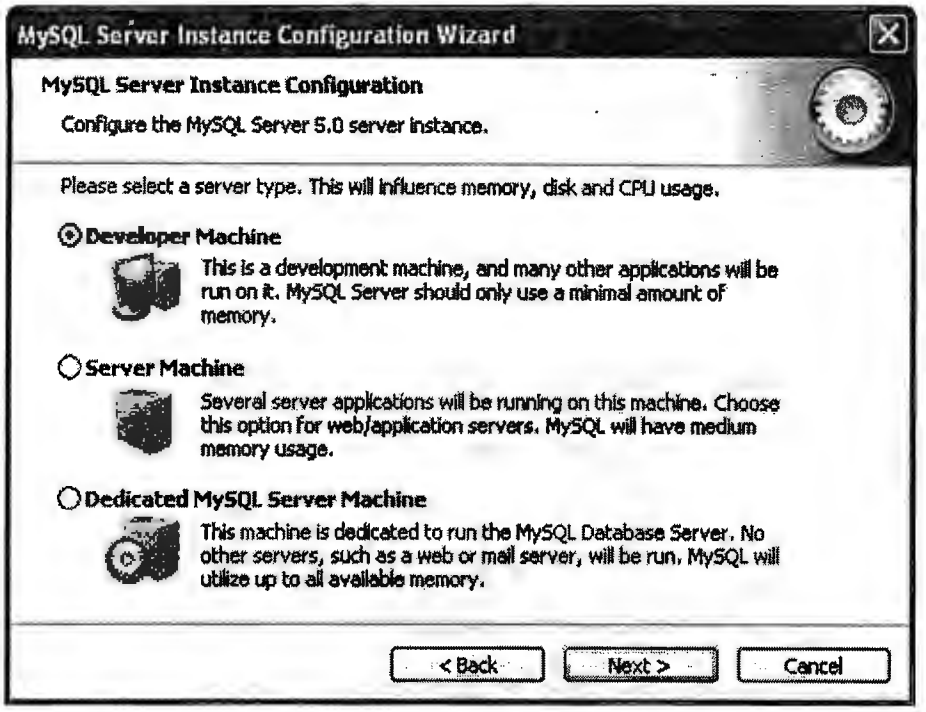
5. Al seleccionar la finalización del asistente, proceda a la configuración del servidor.



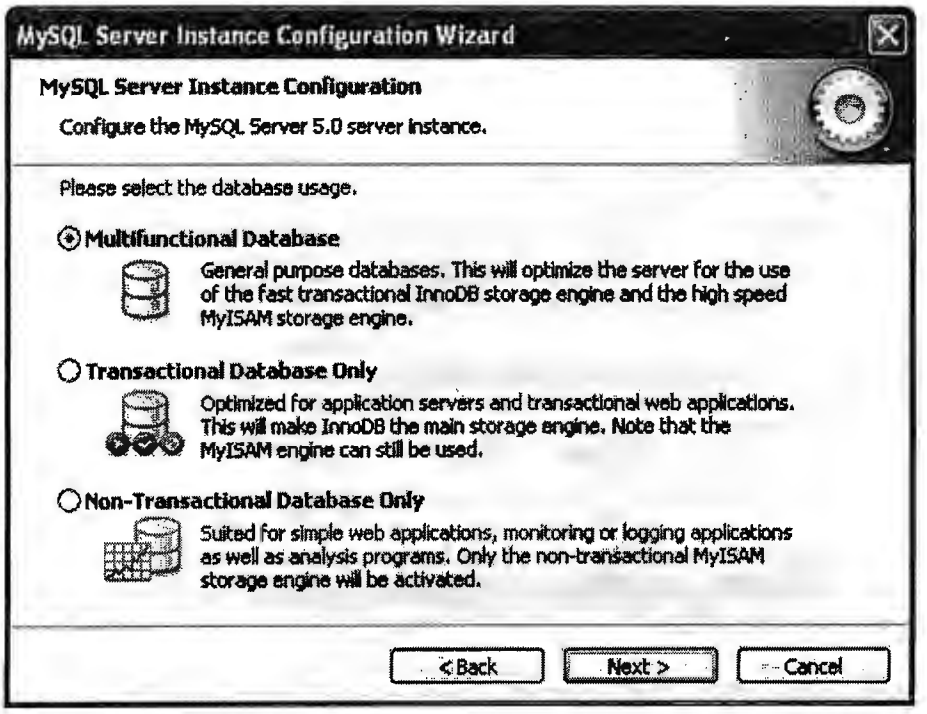
6. Siga las opciones del asistente para configurar el servidor de MySQL

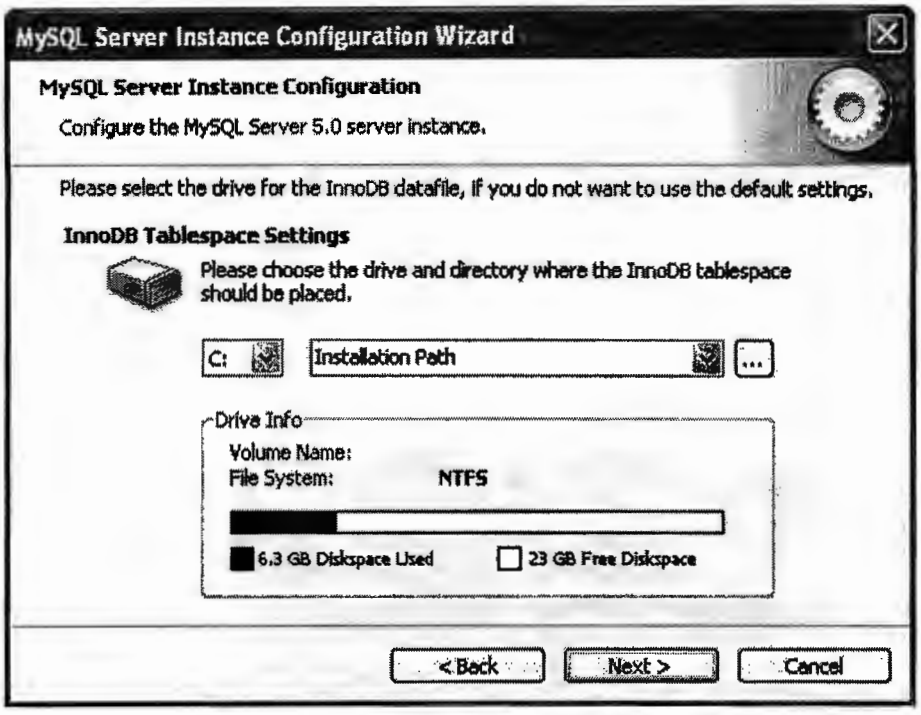


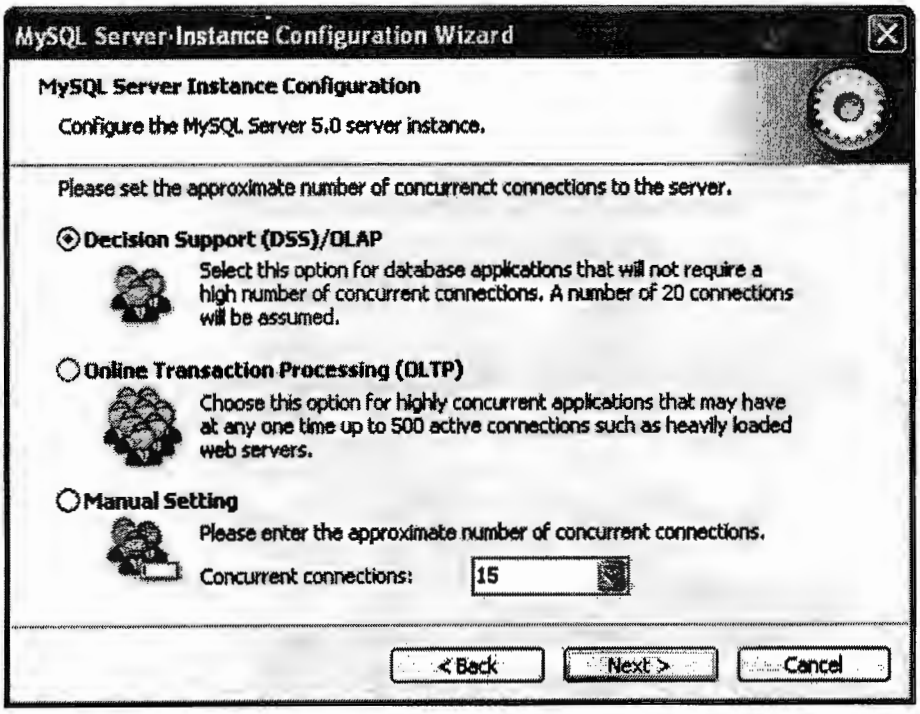
7. Elija la opción Estación de Desarrollo para que el servidor de MySQL utilice solo los recursos necesarios de la estación de trabajo.

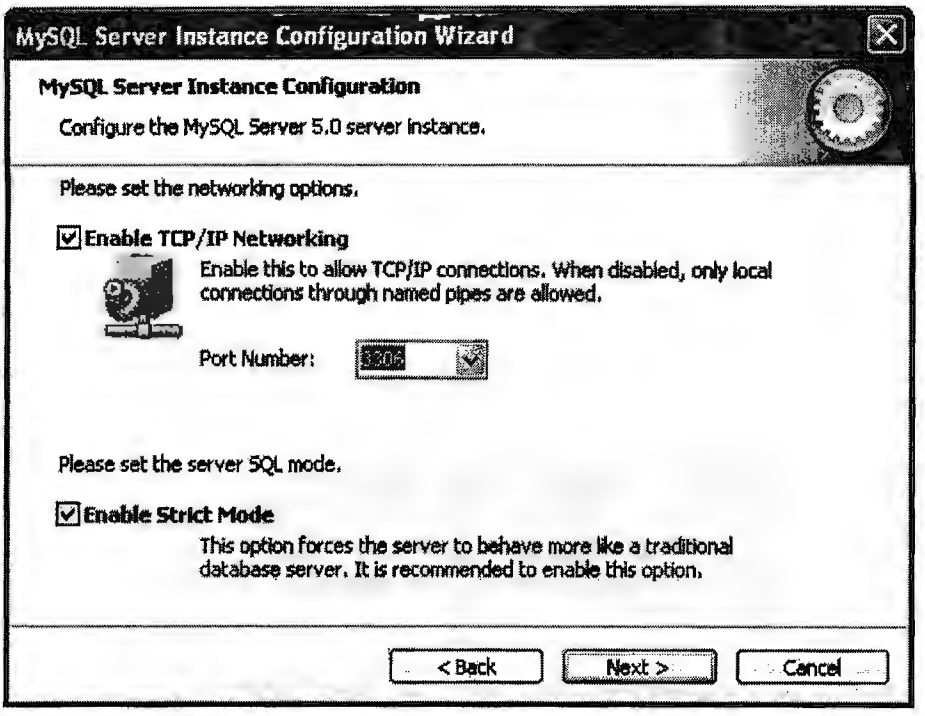


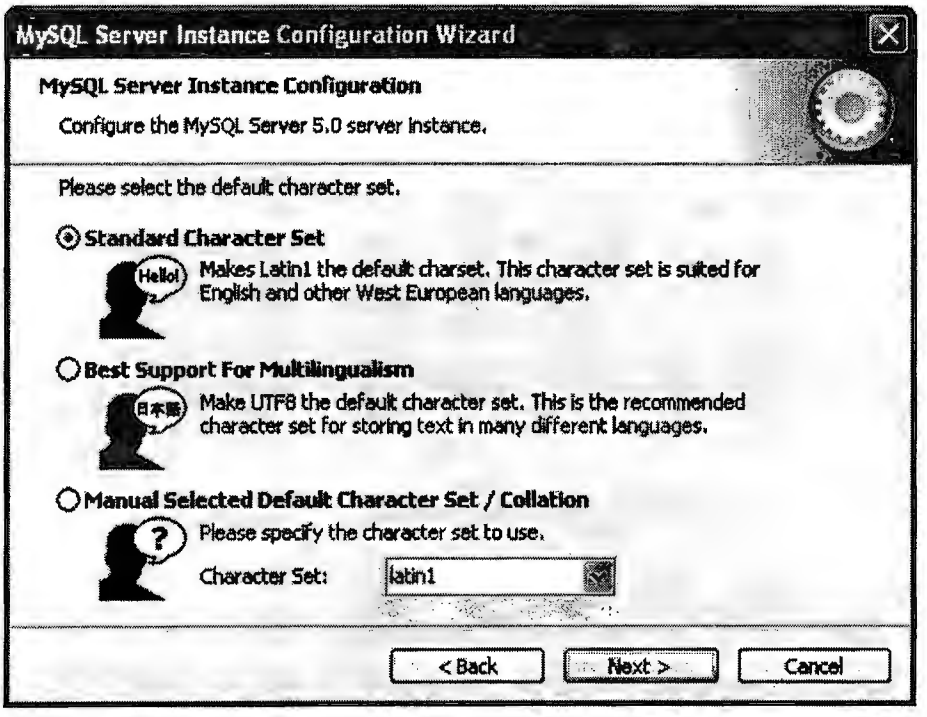
8. Continué con las opciones por defecto del asistente de instalación

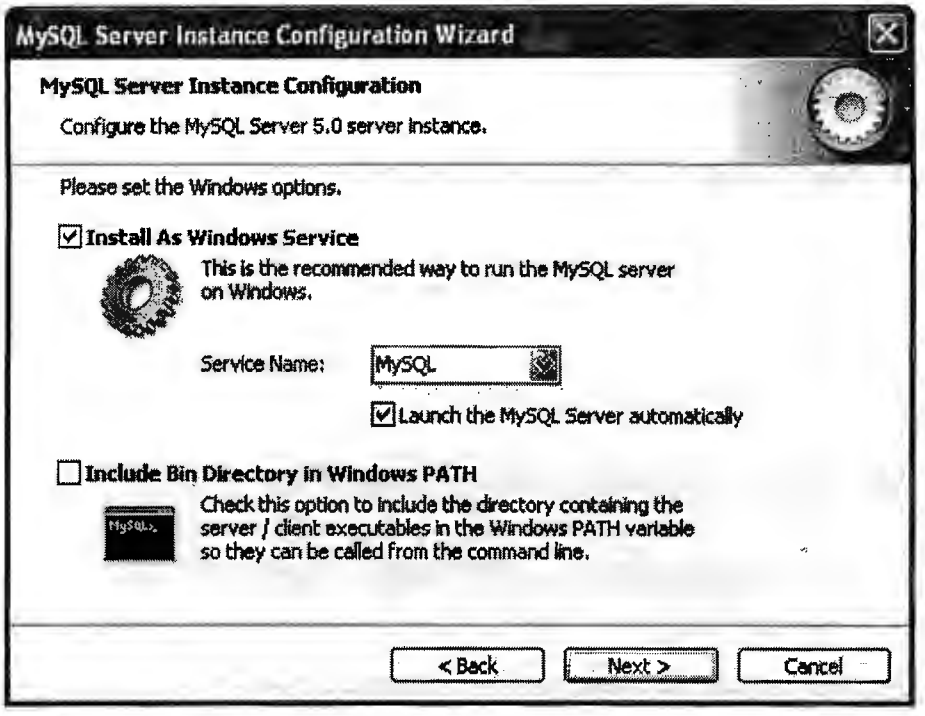



MySQL Server Instance Configuration Wizard
MySQL Server Instance Configuration
Configure the MySQL Server 5.0 server instance.
Please select the drive for the InnoDB datafile, if you do not want to use the default settings.
InnoDB Tablespace Settings
Please choose the drive and directory where the InnoDB tablespace should be placed.
C:
Installation Path
...
Drive Info
Volume Name:
File System: NTFS
6.3 GB Diskspace Used
23 GB Free Diskspace
< Back
Next >
Cancel

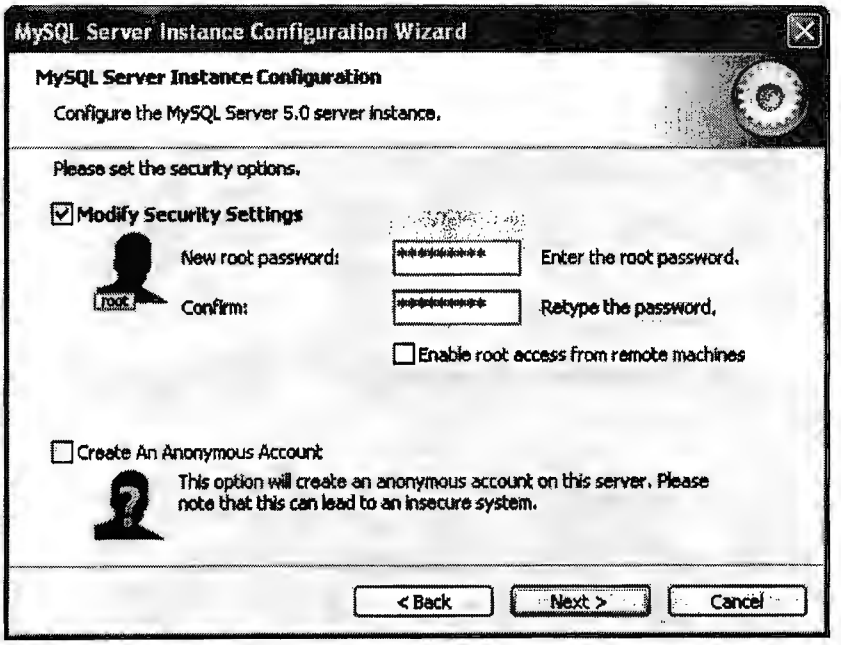

MySQL Server Instance Configuration Wizard
MySQL Server Instance Configuration
Configure the MySQL Server 5.0 server instance.
Please set the approximate number of concurrent connections to the server.
Decision Support (DSS)/OLAP
Select this option for database applications that will not require a high number of concurrent connections. A number of 20 connections will be assumed.
Online Transaction Processing (OLTP)
Choose this option for highly concurrent applications that may have at any one time up to 500 active connections such as heavily loaded web servers.
Manual Setting
Please enter the approximate number of concurrent connections.
Concurrent connections:
15
< Back
Next >
Cancel


MySQL Server Instance Configuration Wizard
MySQL Server Instance Configuration
Configure the MySQL Server 5.0 server instance.
Please set the networking options.
Enable TCP/IP Networking
Enable this to allow TCP/IP connections. When disabled, only local connections through named pipes are allowed.
Port Number:
Please set the server SQL mode.
Enable Strict Mode
This option forces the server to behave more like a traditional database server. It is recommended to enable this option.
< Back
Next >
Cancel

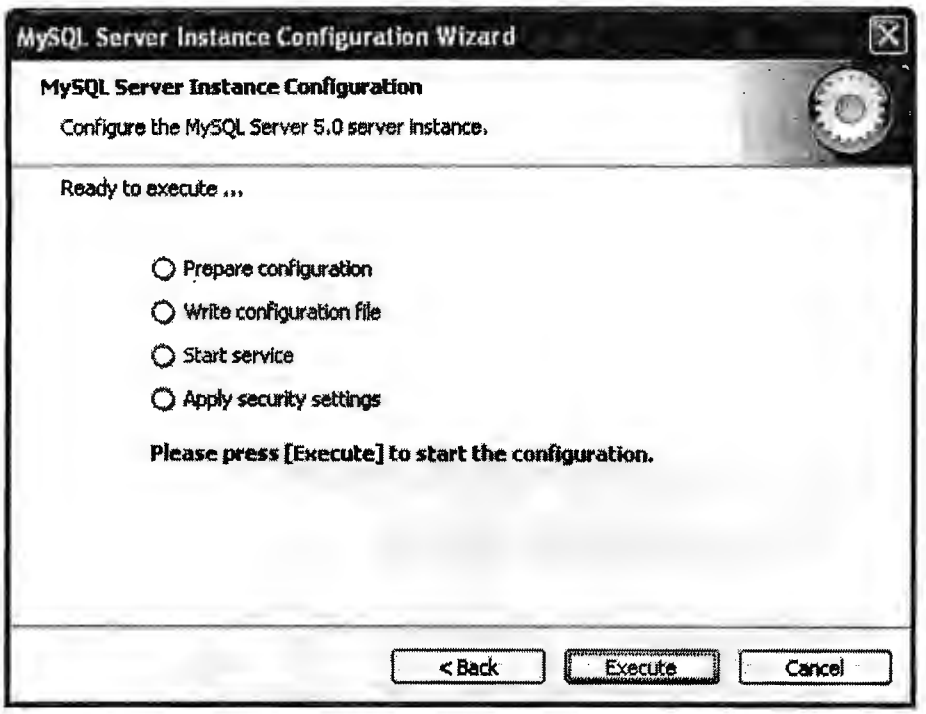

MySQL Server Instance Configuration Wizard
MySQL Server Instance Configuration
Configure the MySQL Server 5.0 server instance.
Please select the default character set.
Standard Character Set
Hello!
Makes Latin1 the default charset. This character set is suited for English and other West European languages.
Best Support For Multilingualism
日本語
Make UTF8 the default character set. This is the recommended character set for storing text in many different languages.
Manual Selected Default Character Set / Collation
?
Please specify the character set to use.
Character Set:
latin1
< Back
Next >
Cancel

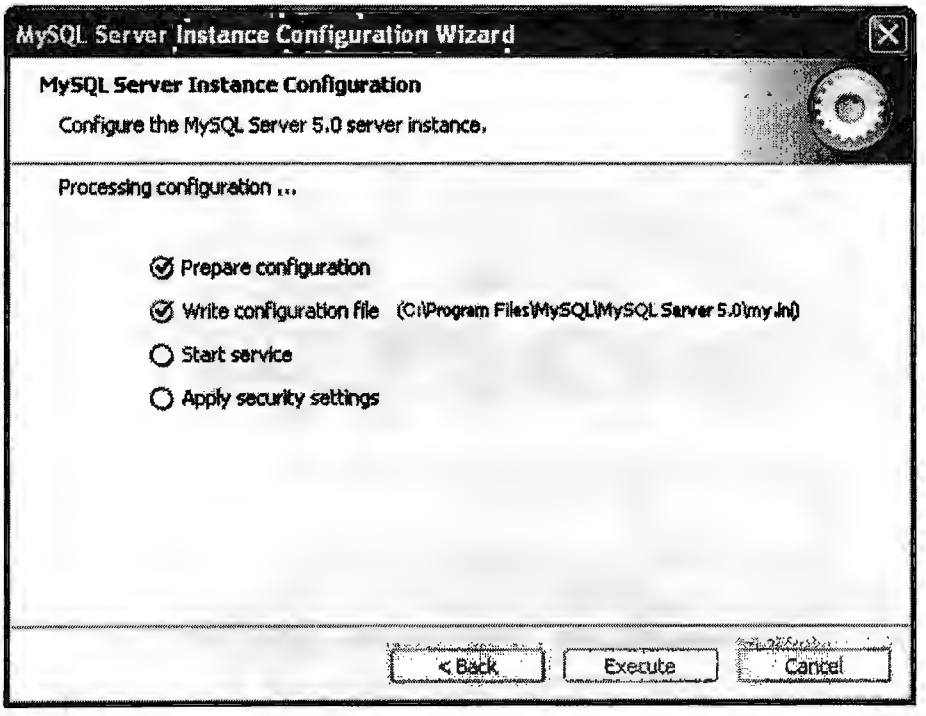


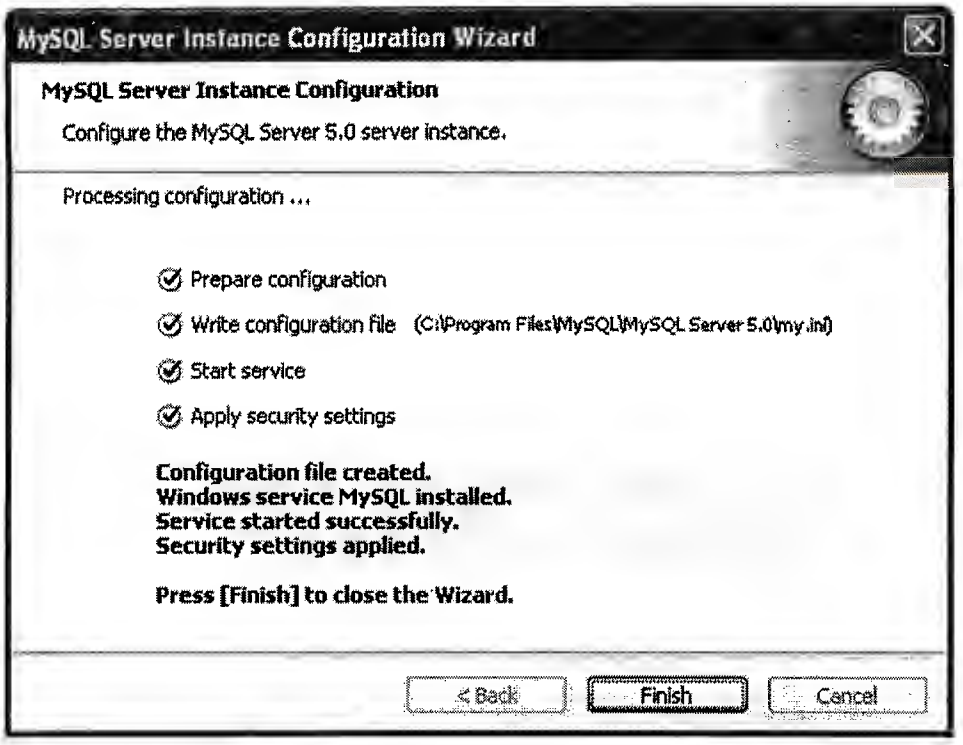
9. Realice las modificaciones de seguridad para el servidor según sus preferencias.



10. Observe la configuración final del servidor y cierre el asistente al concluir el proceso.






MySQL Server Instance Configuration Wizard
MySQL Server Instance Configuration
Configure the MySQL Server 5.0 server instance.
Processing configuration ...
Prepare configuration
Write configuration file (C:\Program Files\MySQL\MySQL Server 5.0\my.ini)
Start service
Apply security settings
Configuration file created.
Windows service MySQL installed.
Service started successfully.
Security settings applied.
Press [Finish] to close the Wizard.
< Back
Finish
Cancel

Guía del Programador
Sistema de Administración y Monitoreo de Red

Universidad
Don Bosco

2006

A continuación se presenta una referencia a los diferentes archivos desarrollados en el Sistema de Administración y Monitoreo de Red.

Cada archivo es asociado a cuatro tipos de extensiones.

Archivos ui (.ui)

Archivos creados por la librería grafica QT por cada uno de los formularios creados. Apartir de este tipo de archivos se generan otros con extensiones moc, h y cpp

Archivos moc (.moc)

Este tipo de archivos se encargan de realizar la reservación de la memoria a utilizar por los formularios desarrollados.

Archivos h (.h)

Los archivos h, conocidos como librerías contienen las variable a utilizar y la definición de diferentes procedimientos desarrollados en los archivos cpp.

Archivos cpp (.cpp)

Los ficheros cpp contiene la combinación de diferentes procesos para la realización de las tareas del Sistema de Administración y Monitoreo de Red. A continuación se describen los procesos desarrollados en estos últimos.

Tesiswindow.cpp

Este archivo es el formulario inicial del sistema. A través de el se tiene acceso al archivo que elabora y controla el formulario de descubrimiento de red. Por otra parte, *Tesiswindow*, posee los procesos de activación de alarmas mediante el envió de múltiples peticiones de respuesta de eco.

Iniciodescubridor.cpp

La función principal consiste en realizar el descubrimiento de los diferentes dispositivos de la red existentes en el rango de direcciones valido que se le proporcione.

Iniciodescubridor hace uso de la librería winpcap, mediante esta lleva a cabo procesos de encapsulamiento de paquetes de petición de respuesta de eco, con el propósito de obtener la información específica de cada dispositivo que ha sido detectado y posteriormente ingresarla a la base de datos activa en el servidor de MySQL.

En este momento aun no se determina que tipo de dispositivo se ha detectado, únicamente se conoce de la existencia de un elemento de red en cada una de las direcciones IP evaluadas. La información obtenida y almacenada en este proceso es utilizada en la siguiente fase para determinar los diferentes tipos de dispositivos presentes.

Iniciosnmp.cpp

El archivo *Iniciosnmp* se encarga de determinar los tipos de dispositivo en las direcciones IP utilizadas por la red, esto se realiza mediante una consulta a los elementos de red para comprobar si en ellos existe activo un agente SNMP, el cual contiene toda la información del sistema operativo a través de bases de datos de administración (MIBs) del protocolo SNMP.

Si dicho agente se encuentra activo se utilizaran los datos obtenidos anteriormente mediante *Iniciodescubridor*. La detección del agente se realiza utilizando la librería Net-SNMP, con la cual se adquiere la descripción del sistema operativo de los elementos detectados y a partir de un análisis de estos datos se determinara que tipo de dispositivo se encuentra en estudio.

Esta información es esencial puesto que a partir del conocimiento de los diferentes tipos de dispositivos el proceso de mapeo podrá posteriormente desplegar los elementos correctamente y determinara los identificadores de objetos (OIDs) correctos, de igual forma con esta información se realizan las peticiones adecuadas para las estadísticas de memoria, cpu y numero de paquetes, finalmente posibilita el monitoreo de la red en archivos posteriores. La información acerca de los tipos de dispositivo es actualizada en la tabla Dispositivos, de la base de datos.

Iniciomapa.cpp

Realiza el proceso de trazado de rutas hacia los elementos de red que no sean routers (es decir estaciones de trabajo, switch o elementos genéricos).
Mediante este archivo se almacena en la base de datos la dirección IP del último salto desde el cual es posible llegar a dicho dispositivo. La información almacenada en este procedimiento es utilizada posteriormente en el archivo de mapeo de la red.

Iconosdisplay.cpp

Este es uno de los archivos más complejos de la aplicación. En el se encuentran diferentes procesos para la detección de dispositivos en el mapeo de red, además obtiene los detalles de los elementos detectados y las diferentes estadísticas; los procedimientos efectuados en este archivo son:

- Mapeo
- Tabla detalles
- Despliegue de dispositivos descubiertos
- Captura de estadísticas
- Cambio de iconos por alarmado
    - Uso excesivo de procesador, CPU
    - No respuesta a peticiones de eco

Confalarms.cpp

Confalarms es el encargado de activar el procedimiento paralelo (hilo) para la ejecución de alarmas, esto se logra mediante el envió de peticiones de respuesta de eco así también por el establecimiento de intervalos de tiempo en el cual se desea sean envíen las peticiones.

Confestaisticas.cpp

Esta sección de la aplicación activa los procesos paralelos (hilos) de activación de alarmas al superar el nivel máximo aceptable respecto al uso de CPU, al mismo tiempo que permite establecer el intervalo de tiempo en el cual se desea realizar el envió de las peticiones de estadísticas.

Estadisticas.cpp

El despliegue de los valores correspondientes a las estadísticas de la aplicación es posible gracias a los diferentes pasos efectuados en este archivo, *Estadísticas*; los tipos de datos desplegados son:

- Memoria
- CPU
- Numero de paquetes

Ping.cpp

El archivo *Ping* permite ejecutar un envío constante de peticiones de respuesta de eco con variaciones en la longitud de los diferentes paquetes, al mismo tiempo realiza la interpretación de una diversidad de tipos de respuestas con lo cual proporciona información que permite determinar las posibles causas por la que las que el dispositivo en estudio no responda.

Propiedades.cpp

Esta sección de la aplicación provee al sistema la capacidad de desplegar información general de los diferentes elementos de la red. Mediante este archivo el usuario podrá verificar en pantalla los siguientes datos:

- Nombre del dispositivo
- Dirección IP
- Dirección física (MAC)

Tracer.cpp

Tracer es la conjunto de procedimientos del sistema que permite realizar el establecimiento de de la ruta hacia cualquiera de los dispositivo de la red. Este proceso tiene como finalidad primordial el fin de conocer que dispositivos de capa tres deben ser cruzados para llegar al equipo bajo estudio.

About.cpp

Muestra el formulario con información sobre los desarrolladores del sistema y un archivo de ayuda acerca de la utilización del Sistema de Administración y Monitoreo de red.

Snmp.cpp

Los procesos efectuados en este archivo permiten el despliegue de la información de los diferentes dispositivos mostrados en la red en los cuales se encuentra activo el agente SNMP, realizada la consulta a dicho agente se obtienen los siguientes datos:

- Nombre de Dispositivo
- Tipo de Dispositivo
- Descripción del sistema operativo
- Tiempo activo del agente
- Valor de Memoria RAM
- Numero de Procesos

El (la) Suscrito (a) Director (a) del Centro Educativo _____
_____, Municipio_____, Departamento de_____
Hace constar que:_____, alum
último año de Bachillerato _____, Opción_____
Jornada_____ egresado (a) durante el año _____obtuvc
asignaturas básicas, que se evalúan en la prueba de Aprendizaje y Aptit
Egresados de Educación Media (PAES) los siguientes resultados finales co
promocional:

ASIGNATURAS	PROMEDIO INSTITUCIONAL	80 %	PAES	20 %	RI
Lenguaje y Literatura					
Matemática					
Ciencias Naturales					
Estudios Sociales y Cívica					

Y para los usos que el (la) interesado (a) estime conveniente, se extiende la presente en de_____, a los _____, días de _____, año_____

F. _____
Licda. Narda Elizabeth Ramírez de Marin
Director (a) del Centro Educativo