ESCUELA SUPERIOR POLITECNICA DEL LITORAL

FACULTAD DE INGENIERIA EN ELECTRICIDAD Y COMPUTACIÓN

"IMPLEMENTACIÓN DE FUNCIONES DE GESTIÓN A LA RED LAN DE LA COMPAÑÍA MAINT USANDO HP OPENVIEW NODE MANAGER"

TOPICO DE GRADUACIÓN

"GESTION DE REDES Y SERVICIOS DE TELECOMUNICACIONES"

PREVIO A LA OBTENCIÓN DEL TITULO DE:

INGENIERO EN ELECTRICIDAD

ESPECIALIZACIÓN: ELECTRÓNICA

REALIZADO POR:

FERNANDO BOZA GAIBOR

GIOVANNI LOPEZ POTES

CHRISTIAN PERUGACHI BENALCAZAR

GUAYAQUIL – ECUADOR

2002

AGRADECIMIENTO

Primero a Dios, por otorgarnos el don maravilloso de la vida, salud y fortaleza; a nuestros padres por habernos dado el temple necesario para lograr nuestros propósitos; a la ESPOL por entregarnos los conocimientos necesarios para llegar a esta etapa tan importante para nosotros; a nuestro profesor de tópico el Ing. Edgar Leyton quien siempre nos guió y apoyó brindándonos su entera confianza; y en general a todas las personas e instituciones que de una u otra forma colaboraron en la elaboración de este proyecto.

DEDICATORIA

A mis padres, hermanos, y a esa persona que me impulsa a seguir adelante.

Fernando Boza Gaibor.

A Dios, a mis padres, a mi esposa y demás seres queridos y amigos que me apoyaron incondicionalmente en todo momento en la realización de este proyecto.

Giovanni López Potes.

A Dios, a mis padres, a mis hermanos, a mi abuelo, a mi esposa y demás seres queridos y amigos que siempre estuvieron presentes para darme el ánimo y la fuerza para triunfar profesionalmente en la vida como ingeniero.

Cristhian Perugachi Benalcázar.

TRIBUNAL DE GRADUACIÓN

Ing. Carlos Monsalve.

Subdecano de la FIEC

Ing. Edgar Leyton.

Profesor del Tópico

Ing. José Escalante.

Miembro del tribunal

Ing. Pedro Vargas.

Miembro del tribunal

DECLARACIÓN EXPRESA

"La responsabilidad por las ideas, hechos y doctrinas expuestas en esta tesis nos corresponden exclusivamente y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral"

(Reglamento de Graduación de la ESPOL)

Fernando Boza Gaibor

Giovanni López Potes

Christian Perugachi Benalcázar

RESUMEN

La gestión de redes y servicios de telecomunicaciones ha tenido un gran desarrollo, es así que la mayoría de empresas cuentan con su propia red de gestión la cual puede definirse en términos generales como la habilidad de tener un punto de control que nos permita las actividades de operar y administrar una red. Hp OpenView Network Node Manager provee al administrador de una red una herramienta integral para controlar y gestionar múltiples sistemas de red y aplicaciones desde una representación gráfica de la red, permitiéndole realizar tres de las cinco funciones de gestión, gestión de fallos, de rendimiento y de configuración.

En el Capítulo 1 se describen los conceptos básicos de un sistema de gestión de redes, sus componentes y se describe el protocolo SNMP (Simple Network Management Protocol), protocolo con el que trabaja el Hp OpenView Network Node Manager.

En el Capítulo 2 se analiza la red de la compañía Maint, su estructura, topología y además se detallan los equipos de red que pueden gestionarse por medio del Hp OpenView Network Node Manager.

En el Capítulo 3 se realiza una visión general del Hp OpenView Network Node Manager para mostrar sus características, su modo de

funcionamiento para descubrir los dispositivos de la red, se define la diferencia entre mapas y submapas y entre objetos y símbolos. Se analiza la correlación de eventos y se detallan las categorías de las alarmas.

En el Capítulo 4 se describe la implementación del Hp OpenView Network Node Manager en la red de Maint, los requisitos de instalación, su instalación paso a paso y como se establecen los dominios de gestión.

En el Capítulo 5 se realiza un análisis de las prestaciones de gestión del Hp OpenView Network Node Manager en la red de Maint, para esto se divide a la gestión de red en sus cinco grupos funcionales.

Del análisis de esta información se obtienen diferentes conclusiones, comprobándose que tan efectivo es tener implementado un sistema de gestión dentro de una compañía sin importar su complejidad o dimensión, ya que los servicios brindados por el Hp OpenView Network Node Manager realizan una monitorización interactiva de todos los nodos de la red, facultándole inclusive al administrador de la red determinar los recursos que se consideren críticos y merezcan un mayor control.

INDICE GENERAL

INDICE DE FIGURAS

CAPITULO 1

GESTION DE REDES BASADA EN SNMP

CAPITULO 2

ANÁLISIS DE LA RED DE MAINT

CAPITULO 3

VISION GENERAL DEL HP OPENVIEW NETWORK NODE MANAGER

CAPITULO 4

IMPLEMENTACION DEL HP OPENVIEW NETWORK NODE MANAGER EN LA RED DE MAINT

CAPITULO 5

ANALISIS DE PRESTACIONES DE GESTION EN LA RED DE MAINT

INTRODUCCION

Actualmente es de gran importancia para las empresas mantener el control sobre los equipos que forman parte de sus redes y los servicios que estos ofrecen, ya que las tendencias son hacia redes más grandes, más complejas y que dan soporte a más aplicaciones y a más usuarios.

Por estas razones es que la gestión de redes y servicios de telecomunicaciones ha tenido mayor auge en los últimos años, organizaciones internacionales han establecido estándares para la gestión de redes de telecomunicaciones siendo la gestión basada en SNMP *(Simple Network Management Protocol)* la más utilizada por ser fácil y sencilla de usar.

Debido a esta gran necesidad que tienen las empresas, ha aumentado la demanda de implementar sistemas de gestión que permitan supervisar el estado de la red mediante el monitoreo de parámetros que muestran la calidad de servicio, el estado de la red, la necesidad de ampliación, etc.

Muchos son los programas que se han elaborado con este fin pero hemos encontrado en el HP OPENVIEW NETWORK NODE MANAGER una herramienta de gestión muy amigable que nos permite supervisar la red mediante la generación automática de mapas en colores que nos

muestren el estado de la red, identificar rápidamente problemas en la red mediante la correlación de eventos, pudiéndose definir eventos y respuestas a los mismos; y el almacenamiento de datos de gestión para su posterior análisis identificando sus tendencias evitando de esta manera posibles problemas en la red.

Este proyecto está orientado a mostrar los beneficios que se obtienen al gestionar una red, para lo cual hemos aplicado el software de gestión HP OPENVIEW NETWORK NODE MANAGER a la red de la compañía Maint de la ciudad de Guayaquil, por medio de este software podremos realizar las funciones de gestión de fallos, de rendimiento y de configuración.

CAPITULO 1

GESTION DE REDES BASADA EN SNMP

Para entender el modelo de gestión de redes SNMP *(Simple Network Management Protocol)* debemos conocer ciertas definiciones básicas que nos ayudarán a familiarizarnos con la gestión de redes y servicios de telecomunicaciones.

1.1 Conceptos básicos de la gestión de redes.

Definiremos Gestión de Redes y servicios de Telecomunicaciones al conjunto de actividades como son planificar, instalar, mantener, operar y administrar, acciones que nos garantizarán la calidad de los servicios que prestan las redes.

Se entiende por gestión al conjunto de capacidades que nos permiten el intercambio y procesamiento de información con el fin de ayudar a cualquier organización que opera o utiliza una red de telecomunicaciones a realizar sus actividades de planificación, instalación, operación, mantenimiento y administración con eficacia.

1.2 Elementos de la gestión de redes.

Los términos que se aprecian en la *Figura 1.1* son clave en el funcionamiento del protocolo de gestión de redes SNMP.

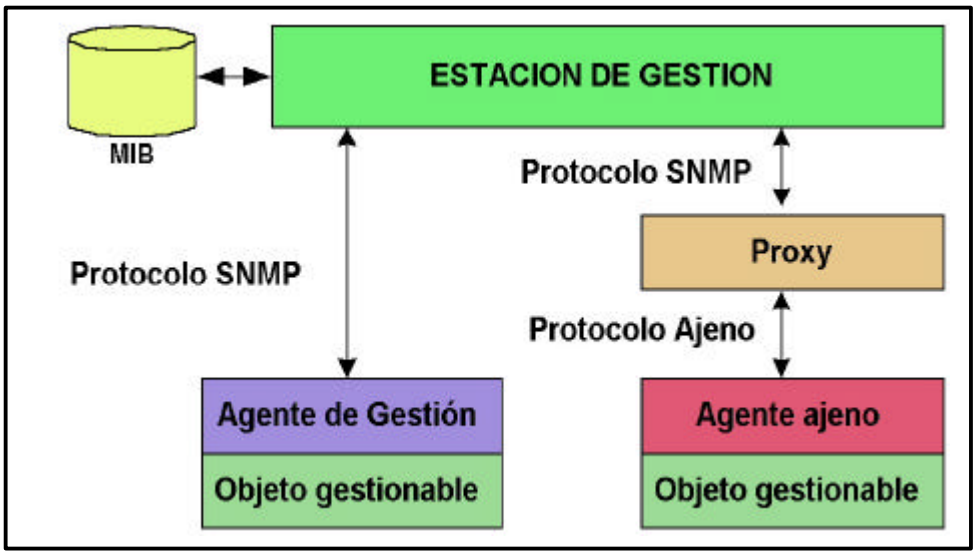

Figura 1.1 Elementos de la gestión de redes.

1.2.1 Estación de gestión.

Es un elemento de la red dedicado a las tareas de gestión, aunque también puede dedicarse a otras tareas. Sirve como interfaz entre el administrador de la red y el sistema de gestión de red.

En la estación de gestión se encuentra el software de gestión SNMP, que es una herramienta que proporciona una interfaz gráfica que permite pedir datos o visualizar alarmas por medio de mapas. Además, almacena los datos permitiendo analizar sus tendencias. La estación de gestión tendrá como mínimo:

- Un conjunto de aplicaciones de gestión para el análisis de datos, recuperación de fallos, etc.

- Una interfaz mediante el cual el gestor de la red pueda monitorizar y controlar la red.

- La capacidad de traducir los requerimientos del gestor de la red a las tareas de monitorización y control de los elementos remotos en la red.

- Una base de datos de información extraída de las MIBs (Management Information Base) de todas las entidades gestionadas en la red.

1.2.2 Agente de gestión.

Es un software que proporciona acceso a los datos de gestión de un dispositivo de red particular ***(objeto gestionable)***, responde a peticiones de información y acciones de parte de la estación de gestión y puede enviar a la estación cierta información importante no solicitada de un modo asíncrono.

Los dispositivos situados en la red son gestionados mediante transacciones entre el gestor y el agente SNMP. El protocolo SNMP proporciona dos clases de transacciones de gestión:

- Petición por parte del gestor SNMP y respuesta por parte del agente SNMP.

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

1.2.3 Base de información de gestión (MIB).

La MIB (Management Information Base), es una base de datos que contiene información sobre los elementos de la red a gestionar, cada recurso que se quiere gestionar se representa mediante un objeto. La MIB es un conjunto estructurado de tales objetos.

La MIB funciona como un conjunto de puntos de acceso al agente desde la estación de gestión. Una estación de gestión realiza la función de monitorización leyendo el valor de los objetos de la MIB. Una estación de gestión puede forzar a que tenga lugar una acción en un agente o puede cambiar la configuración de un agente modificando el valor de variables específicas.

1.2.4 Protocolo de gestión de redes.

Sirve para comunicar a la estación de gestión con los agentes de gestión. El protocolo utilizado es el SNMP (Simple Network Management Protocol), el cual incluye las siguientes capacidades:

- GET: permite a la estación de gestión recuperar el valor de los objetos en el agente.

- SET: permite a la estación de gestión modificar el valor de los objetos en el agente.

- TRAP: permite al agente notificar a la estación de gestión que ocurren eventos significativos.

SNMP es un protocolo no orientado a conexión, pues utiliza UDP (User Datagram Protocol), por lo que no se mantienen las conexiones entre la estación de gestión y sus agentes. Por lo tanto, cada intercambio es una transacción separada entre la estación de gestión y un agente.

Por ser SNMP un protocolo de sondeo, el gestor sondea periódicamente a los agentes para ver si hay algo que necesite atención. Si la petición o respuesta se pierde, es el gestor quien controla la situación.

Si una estación de gestión es responsable de un gran número de agentes, y cada agente tiene un gran número de objetos, entonces se vuelve poco práctico para la estación de gestión el sondear regularmente a todos los objetos de los agentes. La estrategia recomendada es que en el tiempo de inicialización y quizás a intervalos poco frecuentes, como una vez al día, una estación de

gestión puede sondear a todos los agentes que conozca, pidiendo alguna información clave.

Una vez que se ha realizado este sondeo la estación de gestión se abstiene de sondear. En su lugar, cada agente se responsabiliza de avisar a la estación de gestión en el caso de que ocurra algún evento anormal. Estos eventos son comunicados en mensajes SNMP conocidos como *Traps.*

Una vez que la estación de gestión ha sido alertada de la condición de excepción, ésta puede llevar a cabo una determinada acción, como encuestar directamente al agente que notificó el suceso o algún otro agente próximo para diagnosticar el problema y obtener más información sobre el mismo.

En resumen, la red no está pensada para llevar información de gestión que la estación de gestión no necesita, y los agentes no están diseñados para responder a frecuentes peticiones de información poco interesante.

1.2.5 Proxies (Apoderados).

El uso de SNMP requiere que todos los agentes, así como estaciones de gestión, soporten UDP e IP (Internet Protocol), estas restricciones

permiten la gestión a unos dispositivos y excluyen a otros. Como algunos bridges y módems que no soportan ninguna parte de la familia de protocolos TCP/IP (Transport Control Protocol/Internet Protocol).

Para acomodar dispositivos que no tienen implementado SNMP, se desarrolló el concepto Proxy. En este esquema, un agente SNMP actúa como un representante de uno o más dispositivos, es decir el agente SNMP actúa en nombre de los dispositivos representados.

Un Proxy SNMP es un software que permite que una consola SNMP gestione dispositivos no SNMP, es decir, actúa como conversor de protocolos, traduciendo comandos de la estación SNMP al protocolo propietario.

En la *Figura 1.2* se representa el concepto Proxy. La estación de gestión, en lugar de enviar los mensajes al propio dispositivo, los envía a su agente representante. Este convierte cada mensaje SNMP al protocolo de gestión utilizado por el dispositivo, cuando se recibe una respuesta, éste pasa dicha respuesta a la estación de gestión. De forma similar, si una notificación de algún tipo es transmitida al proxy, éste la envía a la estación de gestión en la forma de un mensaje *Trap*.

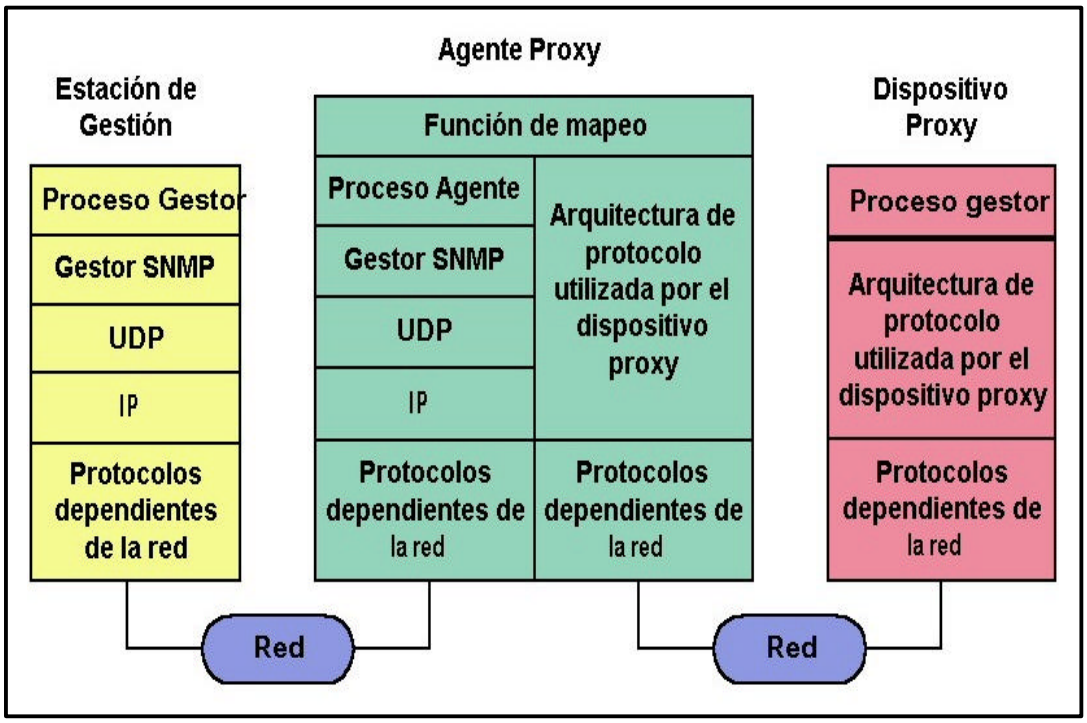

Figura 1.2 Representación de concepto Proxy.

1.3 Arquitectura del SNMP.

El modelo de arquitectura del SNMP consiste en una colección de estaciones de gestión de red y de elementos de red. Las estaciones de gestión de red ejecutan aplicaciones de gestión que monitorizan y controlan los elementos de red.

Los elementos de red son dispositivos como hosts, gateways, servidores de terminal y parecidos, que poseen agentes de gestión para realizar las funciones de gestión de red solicitadas por las estaciones de gestión de red. El SNMP es usado para comunicar información de gestión entre las estaciones de gestión de red y los agentes en los elementos de red.

La *Figura 1.3* sugiere la típica configuración de protocolos para SNMP. En una estación de gestión dedicada, hay un proceso gestor que controla el acceso a la MIB central en la estación de gestión y proporciona una interfaz al gestor de la red.

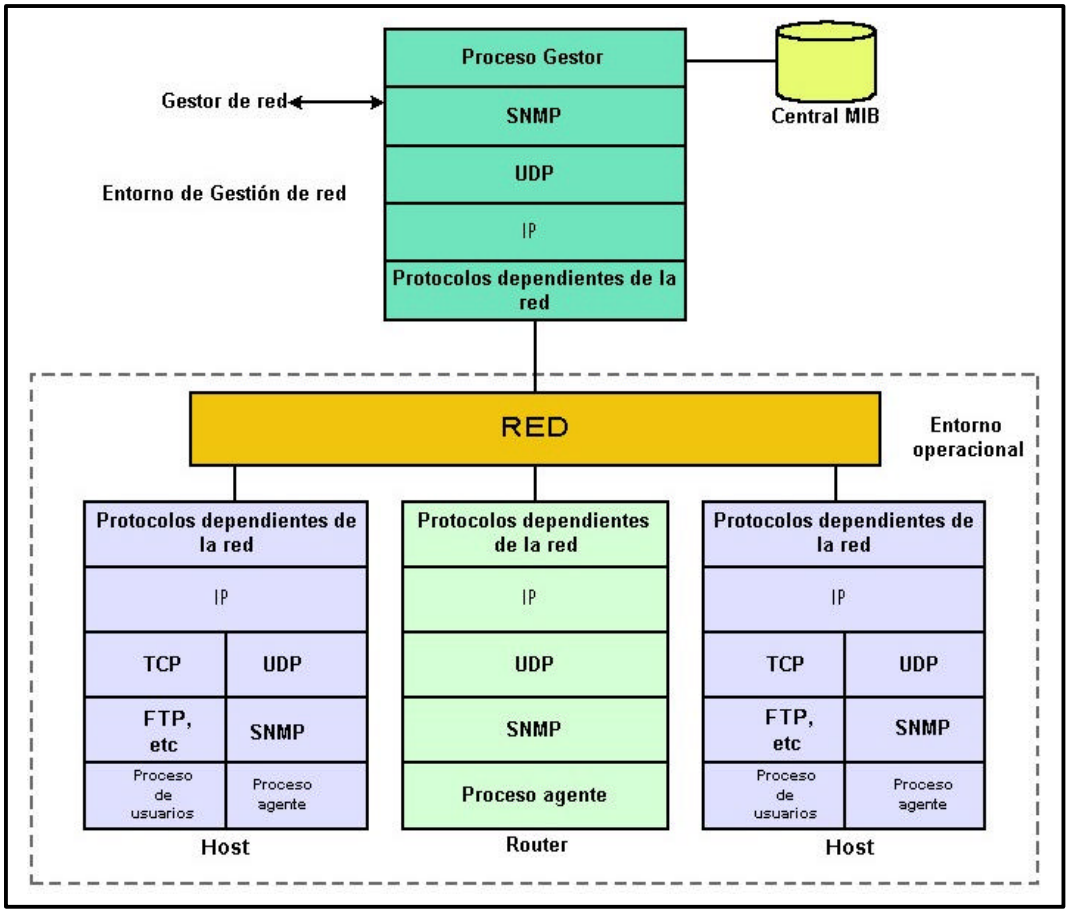

Figura 1.3 Configuración de protocolos para trabajar con SNMP.

El proceso gestor realiza la gestión de red usando SNMP, el cual está implementado por encima de UDP, IP, y los protocolos relevantes dependientes de la red (ej.: Ethernet, FDDI, X.25).

Como se ve en la *Figura 1.3* cada agente también debe implementar SNMP, UDP e IP. Además hay un proceso agente que interpreta los mensajes SNMP y controla la MIB (Management Information Base) del agente. Para un dispositivo agente que soporta otras aplicaciones, como FTP o TELNET, se requiere TCP además de UDP.

1.3.1 Propósitos de la arquitectura.

El SNMP explícitamente minimiza el número y complejidad de las funciones de gestión realizadas por el propio agente de gestión. Esta meta es atractiva al menos en cuatro aspectos:

1. El costo de desarrollo del software del agente de gestión necesario para soportar el protocolo se reduce acordemente.

2. El grado de funciones de gestión soportado remotamente se incrementa, posibilitando un uso completo de los recursos del Internet en la tarea de gestión.

3. El grado de funciones de gestión soportado remotamente se incrementa, imponiendo así las mínimas restricciones posibles en la forma y sofisticación de herramientas de gestión.

4. Los conjuntos simplificados de funciones de gestión son fácilmente entendibles y usados por los creadores de herramientas de gestión de red.

1.3.2 Especificaciones del protocolo.

El protocolo de administración de red SNMP es un protocolo de aplicación por el cual las variables de la MIB de un agente pueden ser inspeccionadas o alteradas.

Las entidades de protocolo se comunican entre sí mediante mensajes, cada uno formado únicamente por un datagrama UDP. Cada mensaje está formado por un identificador de versión, un nombre de comunidad SNMP y una PDU (Protocol Data Unit).

Todas las implementaciones del SNMP soportan 5 tipos de PDU:

- GetRequest-PDU
- GetNextRequest-PDU
- GetResponse-PDU
- SetRequest-PDU
- Trap-PDU

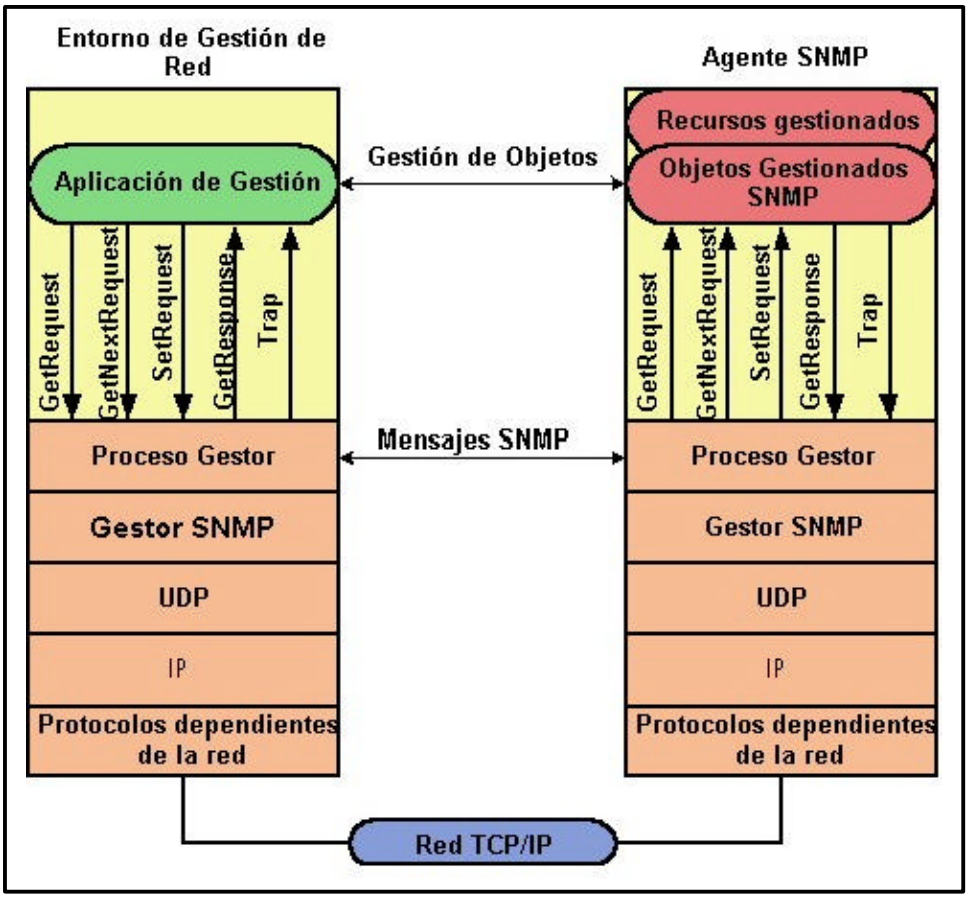

Figura 1.4 Representación del agente y del gestor SNMP.

La *Figura 1.4* proporciona una panorámica más detallada del contexto del protocolo de SNMP. Desde una estación de gestión se pueden enviar tres tipos de mensajes: *GetRequest, GetNextRequest y SetRequest*. Los dos primeros son variaciones de GET.

Los tres mensajes son reconocidos por el agente mediante un mensaje *GetResponse*, el cual es pasado a la aplicación de gestión. Además un agente puede emitir un mensaje *Trap* en respuesta a un evento que afecte a la MIB y a los recursos gestionados.

1.3.2.1 Elementos de procedimiento.

Se describirán a continuación las acciones que realiza una entidad de protocolo en una implementación SNMP. Definiremos dirección *de* transporte como una dirección IP seguida de un número de puerto UDP.

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

1. Construye la PDU apropiada como un objeto definido con el lenguaje ASN.1 (*Abstract Syntax Notation number One).*

2. Pasa esta PDU, junto con un nombre de comunidad y las direcciones de transporte de fuente y destino, a un servicio de autenticación. 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 autenticación 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 pequeño análisis para ver si el datagrama recibido corresponde con un mensaje en ASN.1. Si no lo reconoce, 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 autenticación. 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 un mensaje (trap), descarta el datagrama y no realiza más acciones.

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

1.3.2.2 Seguridad en SNMP.

El sistema de seguridad de SNMP, está basado en el concepto de *community* (comunidad). Una comunidad es una relación entre un agente SNMP y un conjunto de estaciones de gestión SNMP que define unas características de autentificación y control de acceso.

El agente establece una comunidad para cada combinación deseada de autentificación y control de acceso, y a cada comunidad se le da un nombre *(community name),* que es único dentro del agente. Las estaciones de gestión pertenecientes a una comunidad deberán emplear ese *community name* (nombre de comunidad) en todas las operaciones get y set. El agente puede establecer cualquier número de comunidades, pudiendo pertenecer una misma estación de gestión a varias comunidades.

Cuando un agente define una comunidad, está limitando el acceso a su MIB a un cierto conjunto de estaciones de gestión. Si utiliza más de una comunidad, el agente puede proporcionar diferentes categorías de acceso a las estaciones de gestión. Este control de acceso tiene dos vertientes:

- **Vista de la MIB SNMP:** Es un subconjunto de los objetos de una MIB. Se pueden definir diferentes vistas de la MIB para

las distintas comunidades. Estos Objetos no necesitan pertenecer a la misma rama del árbol.

- **Modo de acceso SNMP:** Este podrá ser READ-ONLY o READ-WRITE. Para cada comunidad se definirá un método de acceso.

A la combinación de una vista de la MIB y de un modo de acceso se le denomina SNMP *community profile* (perfil de comunidad de SNMP).

Cualquier petición realizada por la estación de gestión únicamente es atendida si el *community name* es correcto. En caso de que sea incorrecto, el agente SNMP no envía respuesta. Si no se especifica el community name, por defecto suele ser ***public***, permitiendo cualquier acceso.

1.3.2.3 Estructura de una PDU.

Cada PDU contiene los siguientes campos:

- **Versión:** indica la versión del SNMP.

- **Community Name:** Nombre de la comunidad para autentificar un mensaje SNMP.

Los datos que incluyen todas las PDUs excepto la PDU Trap son los siguientes:

- **RequestID:** 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.

- **ErrorStatus:** Entero que indica si ha existido un error. Puede tomar los siguientes valores:

  - noError (0)
  - tooBig (1)
  - noSuchName (2)
  - badValue (3)
  - readOnly (4)
  - genErr (5)

- **ErrorIndex:** entero que en caso de error indica qué variable de una lista ha generado ese error.

- **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.

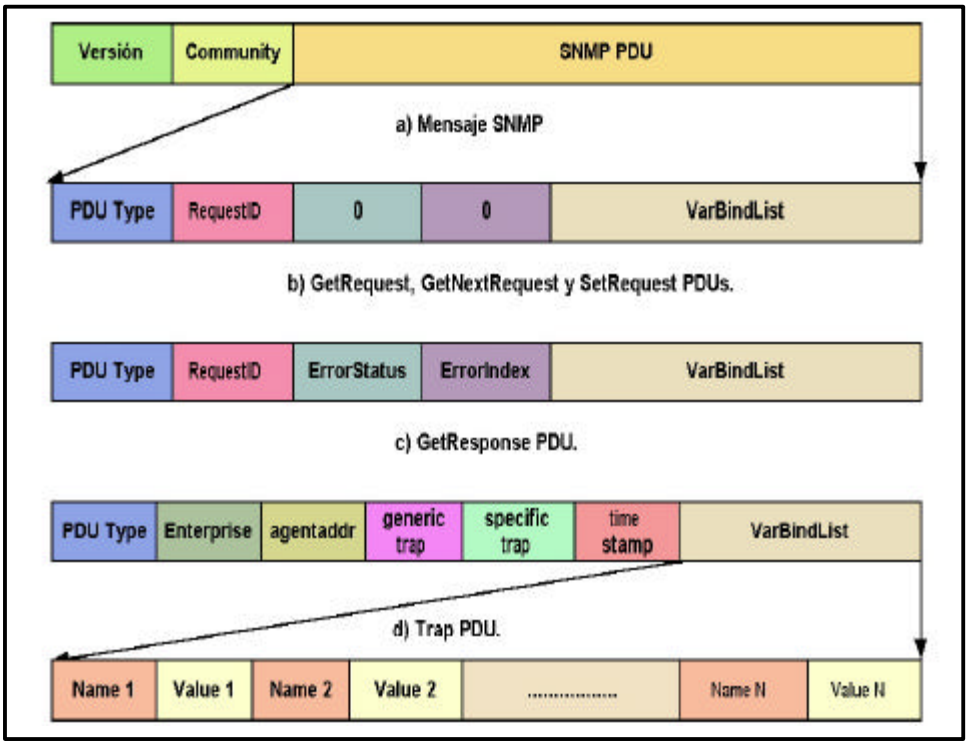

Figura 1.5 Formatos de las PDUs SNMP.

La PDU Trap posee los siguientes campos:

- **Enterprise:** identifica el subsistema de gestión de red que ha emitido el TRAP. Su valor se toma de sysObjectID en el grupo System.

- **Agent address:** indica la dirección IP del objeto que genera el TRAP.

- **Generic Trap:** indica uno de los tipos de TRAP predefinidos.

  - coldStart (0).
  - warmStart (1).
  - linkDown (2).
  - linkUp (3).
  - authenticationFailure (4).
  - egpNeighborLoss (5).
  - enterpriseSpecific (6).

- **Specific Trap:** este código específica la naturaleza del TRAP.

- **Time stamp:** es el intervalo de tiempo entre la última reinicialización de la entidad que ha emitido el TRAP y la generación del mismo.

- **Variable bindings:** proporcionan información adicional relativa al TRAP. El significado de este campo depende de cada implementación en particular.

1.3.2.4 Tipos de PDU.

Como se mencionó anteriormente existen 5 tipos de PDU definidas en SNMP:

1. **GetRequest.-** Primitiva para la obtención del valor de la variable de la MIB de un dispositivo de red.

2. **GetNextRequest.-** Primitiva para la obtención del valor siguiente (en orden lexicográfico) al solicitado en la anterior primitiva GetRequest.

3. **SetRequest.-** Primitiva para la modificación de las variables en la MIB del agente SNMP.

4. **GetResponse.-** Primitiva empleada por el agente SNMP para devolver al gestor los datos solicitados.

5. **Trap.-** Esta es una primitiva especial que los agentes pueden enviar asincrónicamente a un gestor para notificar determinadas condiciones o estados, previamente definidos.

1.4 Estructura de la MIB.

SNMP utiliza el esquema jerárquico de nombrado desarrollado por ISO. En este esquema, *Figura 1.6,* el espacio de nombres (conjunto de todos los nombres disponibles) forma un árbol como se indica a continuación:

- El árbol consiste en una raíz conectada a un conjunto de nodos etiquetados.

- Cada nodo, a su vez, puede estar conectado a otros subnodos también etiquetados.

- Una etiqueta es un par formado por una breve descripción textual y un entero, por ejemplo: iso(1). La descripción textual se utiliza para ser interpretada por las personas, y nunca es transmitida en una PDU.

- El nombre de un nodo, denominado Identificador de Objeto, es la secuencia de los enteros de las etiquetas de cada nodo, desde la raíz hasta el nodo en cuestión. Un identificador de objeto es un identificador único para un objeto en concreto.

La *Figura 1.6* ilustra la estructura de la MIB, como se ve todos los objetos de interés para SNMP están en la parte del árbol correspondiente a iso y de hecho cuelgan del nodo internet. Así el nodo internet tiene el valor de identificador de objeto 1.3.6.1. Este valor sirve como prefijo para los nodos de niveles inferiores.

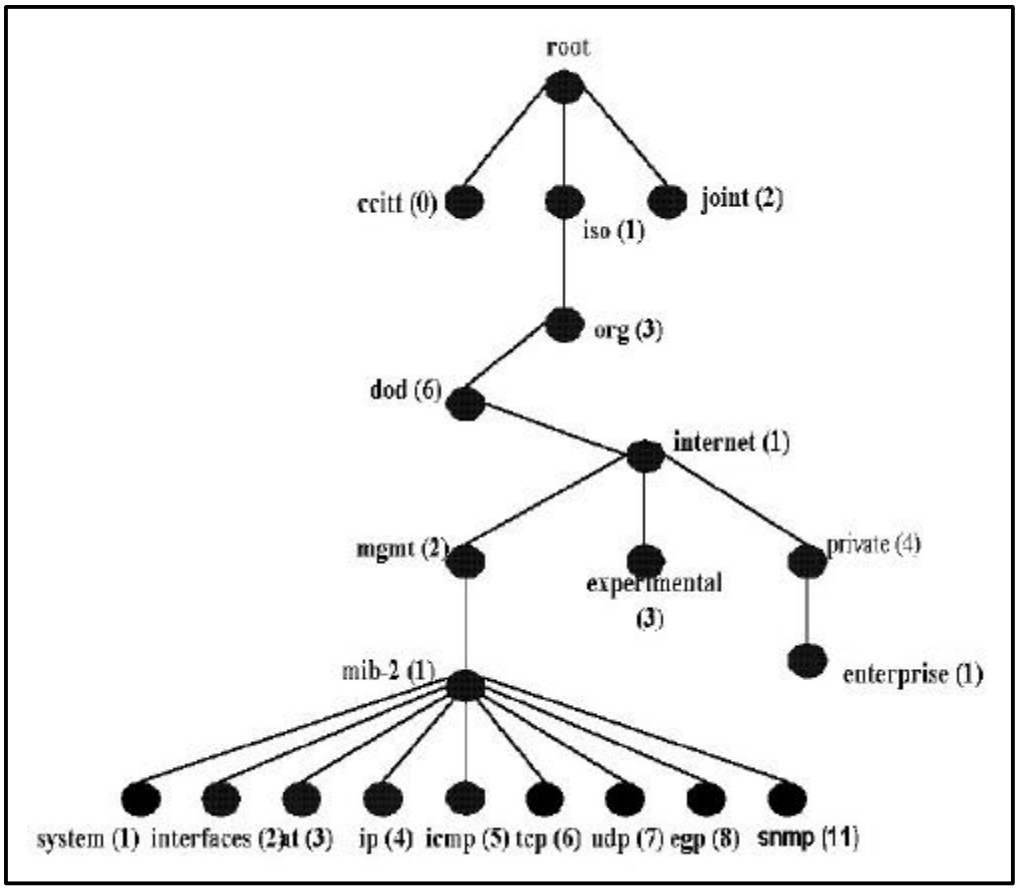

Figura 1.6 Esquema jerárquico de nombrado utilizado en la MIB.

Como se muestra en la *Figura 1.6* la MIB-2 está dividida en varios grupos, de manera que los nodos deben implementar o todos o ninguno de los objetos dentro del mismo grupo. A continuación se describen cada uno de los grupos:

- **Grupo System:** proporciona información general sobre el sistema gestionado. Dentro de este grupo destacaremos algunos de sus objetos:

- sysDescr: proporciona una descripción de la entidad, tal como el hardware, sistema operativo, etc.

- sysLocation: proporciona la localización física del nodo.

- sysServices: el valor de este objeto es interpretado como un código de 7 bits. Cada bit del código corresponde a un nivel de la arquitectura TCP/IP u OSI, donde el bit menos significativo representa el nivel 1. Cuando un sistema ofrece un servicio de un cierto nivel jerárquico, el bit correspondiente se pondrá a 1.

- sysUpTime: indica el tiempo total que ha transcurrido desde que el sistema fue reinicializado por última vez. Este objeto es útil para monitorización de fallos.

- **Grupo Interfaces:** Este grupo contiene información genérica sobre las interfases físicas de la entidad, incluyendo información de configuración y estadísticas de los eventos ocurridos en cada interfaz. Este grupo incluye los objetos:

  - ifNumber: que almacena el número total de interfaces, independientemente de sus estados actuales.

- ifTable: incluyendo una fila para cada interfaz. Dentro de cada fila distinguiremos entre otros:

  - ifIndex: se trata de un valor único para cada interfaz, y se emplea como índice de la tabla. Su valor está comprendido entre 1 y el valor de ifNumber.

  - ifType: indica el tipo de interfaz. Cada interfaz se identifica mediante un número único.

  - ifPhysAddress: indica la dirección física del interfaz. Para el caso de LANs, proporciona la dirección MAC del interfaz.

  - ifAdminStatus: permite al gestor especificar el estado operacional deseado de un interfaz.

  - ifOperStatus: refleja el estado operacional real de un interfaz.

    Si estos dos objetos tienen el valor down (2), el interfaz ha sido inhabilitado por el gestor. Si ifAdminStatus toma el valor up (1) e ifOperStatus toma el valor down (2), el

interfaz ha fallado o bien se ha desconectado localmente.

- ifSpeed: muestra la capacidad actual en bit/s del interfaz.

Toda la información de este grupo es genérica y aplicable a cualquier tipo de interfaz. Dicha información es útil como punto de partida de cualquier función de gestión de red, tal como la monitorización del rendimiento o el control de fallos.

- **Grupo at:** Este grupo se compone de una sola tabla, y cada fila de la misma corresponde a uno de las interfases físicas del sistema. Cada fila proporciona una traslación (mapping) desde una dirección de red a una dirección de red física. Este grupo está desfasado (deprecated) en la MIB-II y sólo está incluido en ella para compatibilizarla con los nodos MIB-I.

- **Grupo ip:** Proporciona información sobre la implementación y ejecución de IP sobre el sistema. Entre los objetos de este grupo existen tres tablas que son importantes:

  - ipAddrTable: contiene información relevante de direcciones IP asignadas a esta entidad, con una fila para cada dirección

IP. Cada dirección está asignada unívocamente a un interfaz físico, indicado por la variable ipAdEntIfIndex, cuyo valor coincide con el de ifIndex (grupo interfaces). Esta información es útil para la monitorización de la configuración de la red en términos de direcciones IP.

- ipRouteTable: contiene información usada en el enrutamiento. La información de esta tabla es útil para la monitorización de la configuración y puesto que los objetos de la tabla son de lectura/escritura, se puede utilizar ésta para el control del proceso de enrutamiento.

- ipNetToMediaTable: Es una tabla de traducción de direcciones que proporciona una correspondencia entre la dirección física y la dirección IP. La información contenida aquí es la misma que la del grupo at, incluyendo además, la variable ipNetToMediaType.

- **Grupo icmp:** Este grupo contiene información relevante de la implementación y operación de ICMP (*Internet Control Message Protocol*) en un nodo. Consta únicamente de contadores para los diferentes tipos de mensajes ICMP enviados o recibidos.

- **Grupo tcp:** Este grupo contiene información relevante de la implementación y operación de TCP en un nodo. El objeto más importante dentro de este grupo es la tabla tcpConnTable.

- **Grupo udp:** Este grupo contiene información relevante de la implementación y operación de UDP en un nodo. Además de la información de los datagramas recibidos y transmitidos, este grupo incluye la tabla udptable, que contiene información sobre los puntos finales UDP de esta entidad sobre los que una aplicación local está aceptando datagramas. Para cada uno de los usuarios UDP, la tabla contiene la dirección IP del usuario y el puerto UDP.

- **Grupo egp:** Este grupo contiene información relevante de la implementación y operación de EGP (*External Gateway Protocol*) en un nodo.

  Además de la información sobre los mensajes EGP enviados y recibidos, este grupo incluye la tabla *egpNeighTable*, que contiene información sobre cada uno de los routers vecinos conocidos por esta entidad. La tabla está indexada por *egpNeighAddr*, que contiene la dirección IP del router vecino.

- **Grupo transmission:** Este grupo contiene objetos que proporcionan información sobre el medio de transmisión subyacente para cada interfaz del sistema.

  Actualmente no se han definido ninguno de estos objetos en la MIB-II. Sin embargo, se han desarrollado una serie de definiciones específicas del medio como RFC *(Request For Comment)* en la parte experimental de la MIB. Con el tiempo, estas definiciones se moverán al grupo transmisión.

  Entre las MIBs experimentales definidas, destacamos:

  - IEEE 802.4 Token Bus (RFC 1230).
  - IEEE 802.5 Token Ring (RFC 1231).
  - FDDI Fiber Distributed Data Interface (RFC 1285).

  No hay que confundir la información de este grupo con la presentada en el grupo interfaces. El grupo interfaces contiene información genérica aplicable a todas las interfaces, mientras que la información de este grupo contiene información relativa a un tipo específico de subred.

- **Grupo snmp:** Este grupo, definido como parte de MIB-II contiene información relevante sobre la implementación y funcionamiento de SNMP. Algunos de los objetos definidos en el grupo presentan el valor 0 para aquellas implementaciones que soportan sólo funciones de estación de gestión o sólo funciones de agente SNMP.

  A excepción del último objeto en el grupo, todos los objetos son contadores de sólo lectura. El *snmpEnableAuthenTraps* es fijado por la estación de gestión, e indica si el agente puede enviar *TRAPs* cuando se produce un fallo de autenticación, es decir cuando recibe un PDU con un *community name* incorrecto.

CAPITULO 2

ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA RED DE MAINT

La compañía Maint en la ciudad de Guayaquil cuenta con una red LAN la cual se encuentra distribuida en los distintos departamentos que conforman la empresa tales como:

- Contabilidad.
- Tesorería y Cobranzas.
- Recursos Humanos.
- Marketing.
- Sistemas y desarrollo.
- Mantenimiento.
- Cableado Estructurado.
- Soluciones de Hardware.
- Soluciones de Software.
- Soluciones de Redes.

A continuación en la *Figura 2.1* mostramos el organigrama de la empresa para dar una mejor idea de cómo está conformada la compañía.

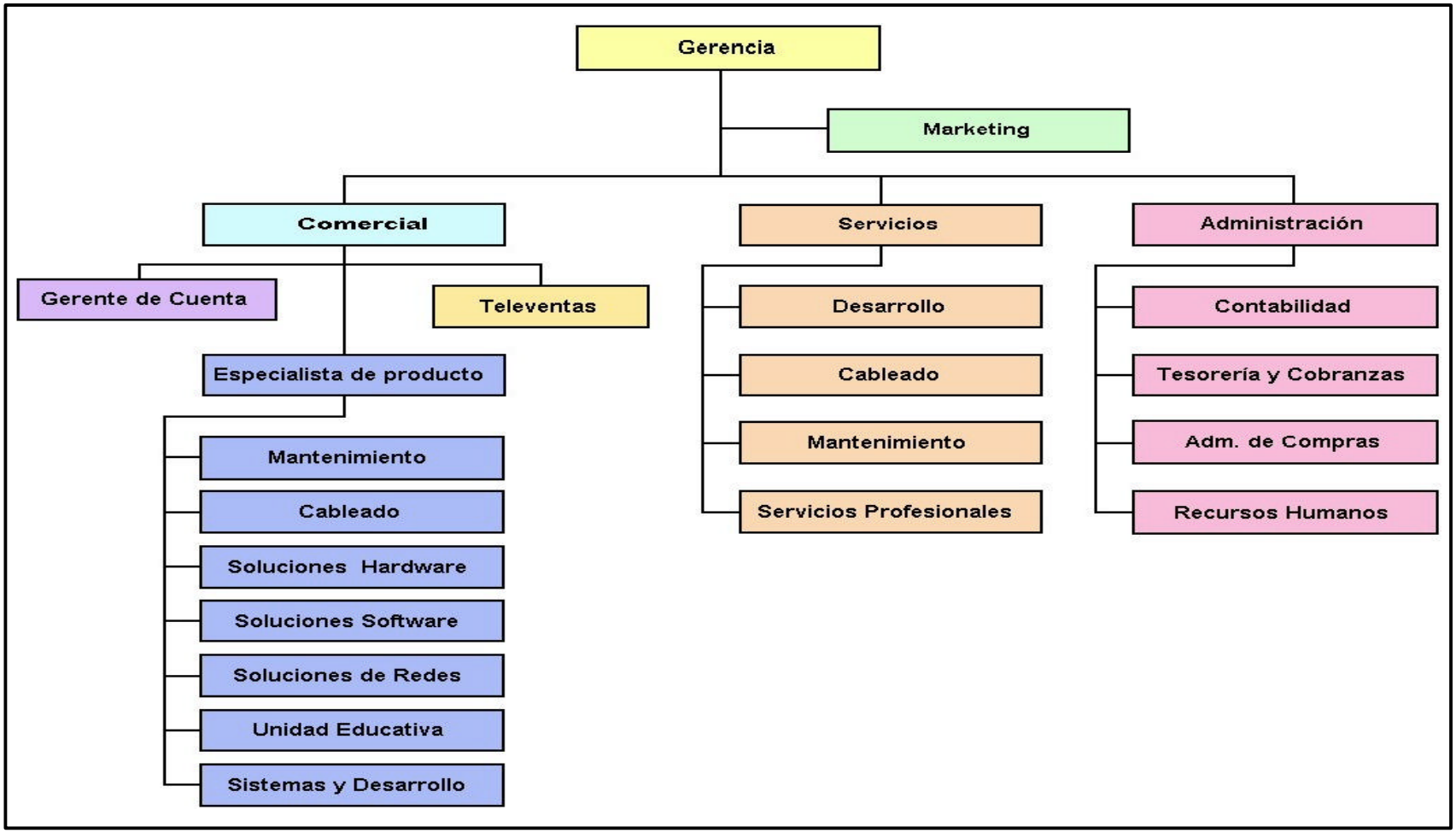

Figura 2.1 Organigrama de la compañía Maint.

2.1 Estructura y topología de la red.

La red LAN de la compañía Maint cuenta en total con 78 computadoras que se encuentran distribuidas en los distintos departamentos que conforman la red de la empresa. Esta red es una red centralizada pues todos los servidores se encuentran agrupados en un segmento, además toda la red utiliza tecnología Ethernet a 10 Mbps.

2.2 Análisis de la red.

La red de la compañía Maint cuenta con 7 servidores, que se encuentran conectados directamente al Switch Catalyst (2900 XL), al que se encuentran conectados también el Switch Newlink (6020) y otro Switch Catalyst (2900 XL). Al Switch Newlink (6020) se conectan el Hub Bay Networks (10 Base T) y el Switch Cabletron (System 2000) de los que se desprenden la porción de la red que pertenece a la parte comercial y los niveles de gerencia.

Al Switch Catalyst (2900 XL) se conectan los siguientes equipos: 3Com (3C16270), 3Com Link Builder (FMS II), Hub Bay Networks (10 Base T), 3Com Link Builder (10 Base T) a los que se conectan los diferentes equipos que forman la parte de la red LAN que pertenece a los distintos departamentos de soporte. En la *Figura 2.2* se muestra la red LAN de la compañía Maint de forma detallada.

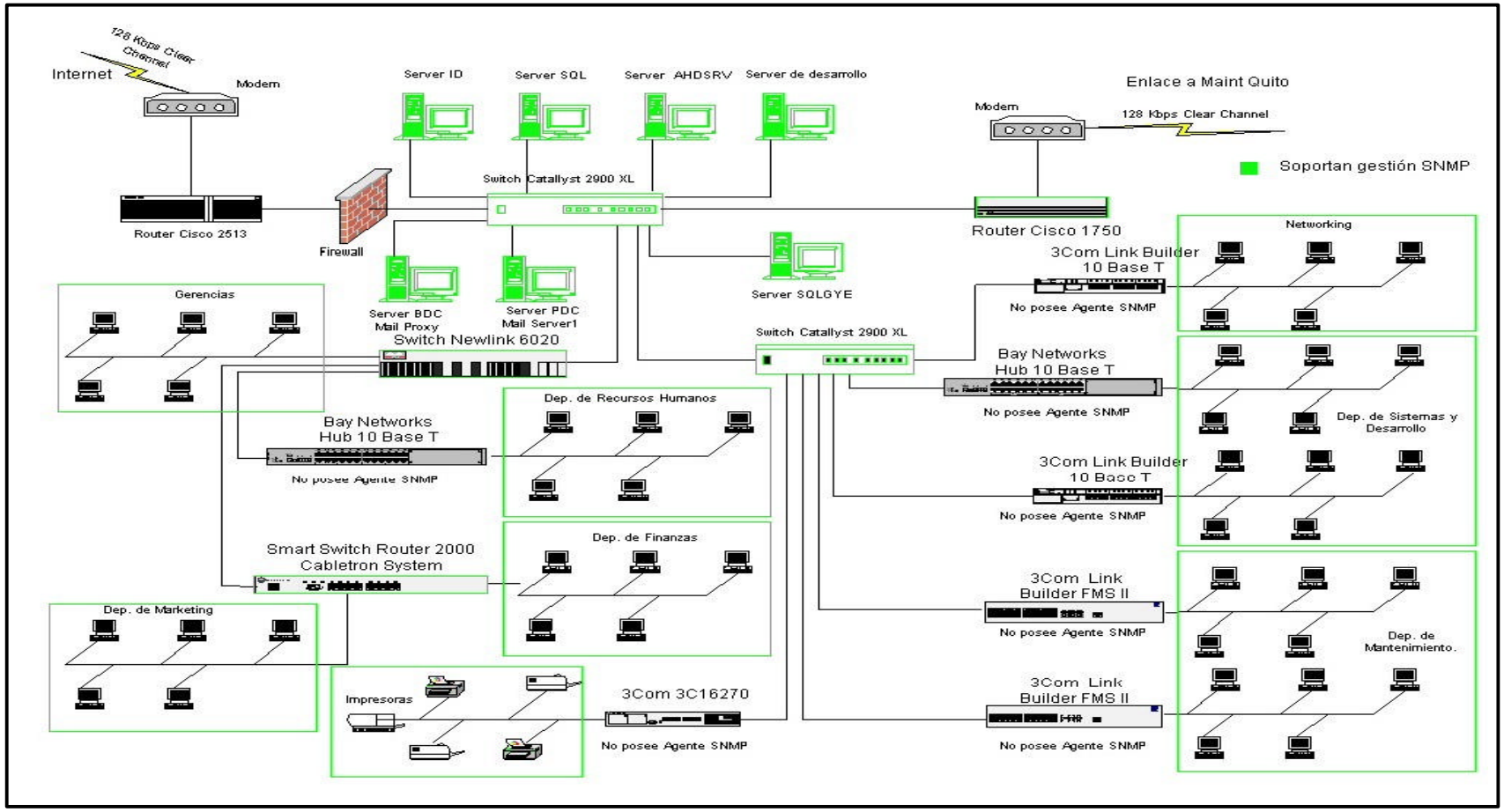

Figura 2.2 Diagrama de la red LAN de la compañía Maint.

2.3 Dispositivos de red que se pueden gestionar.

La red de la compañía Maint en la ciudad de Guayaquil, cuenta con los siguientes elementos de red que pueden ser gestionados directamente mediante el Hp OpenView Network Node Manager, además de los distintos servidores y computadoras que conforman la red.

- **Router Cisco 1750.**

  El router Cisco 1750 proporciona una solución rentable para el soporte de aplicaciones, que incluye:

  - Acceso seguro a Internet, intranet y extranet con firewall opcional.
  - Integración multiservicio de voz, fax y datos.
  - Acceso VPN (Virtual Private Network).
  - Cenectividad de banda ancha DSL y cable.

  Dispone de tres ranuras modulares para tarjetas de interfaz de voz y datos, un puerto de detección automática Ethernet 10/100 BaseT, un puerto de consola y un puerto auxiliar.

  Posee enrutamiento multiprotocolo (IP, IPX y AppleTalk), IBM/SNA y bridging transparente a través de ISDN (Integrated Service Digital Network), transmisión serial síncrona y asíncrona

como por ejemplo, líneas dedicadas, Frame Relay, SMDS, Switched 56, X.25.

Figura 2.3 Router Cisco 1750

- **Router Cisco 2513.**

  Está diseñado para usarlo en ambientes de oficina que necesitan incrementar su densidad mediante la segmentación de la red LAN existente.

  Posee interfaces Ethernet, Token Ring, dos interfaces seriales síncronas que operan a 4 Mbps, y una interface serial asíncrona de baja velocidad para acceso WAN. Soporta los protocolos IP, IPX, AppleTalk y DECnet.

Figura 2.4 Router Cisco 2513

- **Switch Cisco Catalyst 2900 XL.**

  Este switch ofrece rendimiento en la red, modularidad y una gestión flexible. Además tiene las siguientes características:

  – 24 puertos con detección automática para 10 o 100 Mbps y 2 ranuras de expansión para puertos 100 BaseFX.
  – Autonegociación de velocidad y operación en half o full duplex.
  – Soporta aplicaciones de gestión SNMP.
  – Posee conexión para un sistema redundante de poder.

Figura 2.5 Switch Cisco 2900 XL

- **Smart Switch Router 2000 Cabletron System.**

  Este switch nos brinda las siguientes propiedades:

  – Soporta protocolos IP e IPX.

- Posee 24 puertos con velocidades de 16 – 10/100Base TX.
- Flexibilidad de expansión y conectividad WAN mediante 2 ranuras.
- Posee conexión para fuente de poder redundante.
- Soporta la gestión SNMP directamente.

Figura 2.6 Smart Switch Router 2000.

- **Switch NewLink 6020.**

  Este switch tiene las siguientes características:

  - Posee 24 puertos, con velocidades de 10 o 100 Mbits/seg.
  - Soporta protocolos IP o IPX.
  - Posee agente SNMP.

Figura 2.7 Switch NewLink 6020.

- **Bay Networks 10 Base-T Hub.**

  Este Hub posee 12 puertos 10 BaseT, soporta cable UTP hasta 100 metros. En la parte frontal posee indicadores de estado. Este equipo no posee agente SNMP por lo tanto no puede ser gestionado por el Hp OpenView Network Node Manager.

Figura 2.8 Hub Bay Networks 10 Base-T.

- **3Com Link Builder FMS II 3C16671A.**

  Este Hub posee las siguientes características:

  - Soporta los protocolos IP e IPX.
  - Posee 24 puertos de 10 Mbits/seg.
  - Puede conectarse a otro Hub, por medio del puerto 24.
  - Posee conexión para fuente de poder redundante.
  - No puede soportar la gestión directamente, para esto deben implementarse el modulo de gestión 3C16630 o el módulo de gestión avanzada RMON 3C16632.

Figura 2.9 Hub 3Com Link Builder FMS II.

- **3Com Link Builder 3C16670.**

  Este Hub posee las siguientes características:

  - Soporta los protocolos IP e IPX.
  - Posee 12 puertos de 10 Mbits/seg.
  - Posee conexión para fuente de poder redundante.
  - No puede soportar la gestión directamente, para esto deben implementarse el modulo de gestión 3C16630 o el módulo de gestión avanzada RMON 3C16632.

Figura 2.10 Hub 3Com Link Builder 3C16670.

- **3Com Link Builder 3C16270.**

  Este Hub posee las siguientes características:

  - Soporta los protocolos IP e IPX.
  - Posee 12 puertos de 10 Mbits/seg.
  - Posee conexión para fuente de poder redundante.
  - No puede soportar la gestión directamente, para esto deben implementarse el modulo de gestión 3C162230.

Figura 2.11 3Com Link Builder 3C16270.

CAPITULO 3

VISION GENERAL DEL HP OPENVIEW NETWORK NODE MANAGER

3.1 Características del HP OpenView Network Node Manager.

Hp OpenView Network Node Manager comprende una extensa gama de herramientas que nos permiten controlar los elementos de una red LAN de manera individual, orientándonos a un mejor tiempo de respuesta garantizándonos de esta forma la disponibilidad de la red.

Entre las principales características tenemos:

- Consiste en soluciones dirigidas a diferentes aspectos del proceso.

- Diseñado para gestionar eficaz y eficientemente una red de equipos de cualquier marca que tengan agentes SNMP.

- Hp Openview Network Node Manager provee apertura para que aplicaciones específicas de gestión operen de una manera consistente.

- Nos muestra el estado actual de la red, que dispositivos están presentes y como están configurados, como están comportándose y si algo anda mal.

- Nos permite identificar tendencias por medio de lo cual podemos optimizar la red, cambiando la configuración o cambiando elementos en la red.

- Por medio del Hp OpenView Network Node Manager podemos establecer umbrales en los dispositivos de red críticos para predecir que puede salir mal y evitar que ocurran problemas mayores.

3.2 Modo de funcionamiento del Hp OpenView Network Node Manager.

Una vez que el Hp OpenView Network Node Manager ha sido instalado reconocerá automáticamente todos los dispositivos IP y de nivel 2 del modelo OSI (Open System Interconection) que se encuentren en la red para luego establecer un mapa de la red LAN, el cual podremos ver en la pantalla de la estación de gestión. Este mapa es una representación visual de los canales de comunicación establecidos entre el Hp OpenView Network Node Manager y los recursos de la red. Hay que estar

conscientes de que esta no es una representación física sino una representación lógica.

Otra cosa que hay que tomar en cuenta es la diferencia que debemos hacer entre Servicios y Aplicaciones que componen el Hp OpenView Network Node Manager.

- **Servicios:** son aquellos que continuamente monitorizan el estado y configuración de los dispositivos gestionados. Se encargan también de mantener una base de datos con información acerca de la red, y de actualizarla conforme hay cambios en la red. Los servicios deben estar activos para poder ejecutar las aplicaciones.

- **Aplicaciones:** Se encargan de organizar y presentar la información recogida por los servicios. También organiza y presenta las alarmas que responden a cambios en la red, en cuanto se detectan. Finalmente, puede obtener y recoger información de los dispositivos que soportan SNMP.

Los servicios se pueden arrancar y detener interactivamente, aunque lo más habitual es que se activen automáticamente cuando el sistema arranca. La aplicación se arranca interactivamente, pero para ello primero tienen que estar activos los servicios.

3.2.1 Método para descubrir dispositivos.

El Servicio *Netmon* (proceso en background), usa una combinación de peticiones SNMP y de pings ICMP (Internet Control Message Protocol) transmitidos sobre UDP (User Datagram Protocol) e IPX (Internet Packet Exchange) para encontrar los nodos de la red.

- **Descubrimiento de Nodos IP.**

  Para descubrir los nodos IP de la red, *Netmon* necesita tener acceso a la siguiente información:

  - La máscara de subred.
  - La dirección del router predefinido en la tabla de ruteo de la estación de gestión.
  - Información SNMP del router predefinido y de los otros routers y nodos de la red.

  Para trabajar, el Servicio *Netmon* requiere lo siguiente:

  - Que la estación de gestión esté correctamente configurada para trabajar en red.

- En la estación de gestión debe estar un agente SNMP

- Los nodos deben de estar activos y responder a la petición de ping para poder ser descubiertos.

- Todos los gateways/routers y la estación de gestión deben tener correctamente configurada la máscara de subred.

La información sobre los nodos descubiertos se almacenan en la base de datos del Network Node Manager y este la usa para generar automáticamente el mapa de la red.

Si Network Node Manager no encuentra el Nodo, se puede mandar un ping ICMP que fuerce su descubrimiento, o se lo puede adherir manualmente.

- **Descubrimiento de Nodos IPX.**

  Para descubrir nodos IPX, el Servicio *Netmon* utiliza un método diferente, emite varias versiones del protocolo IPX para descubrir los nodos y luego SNMP para rellenar información adicional sobre el nodo.

Para descubrir los nodos IPX en la red, el Servicio *Netmon* requiere de lo siguiente:

- La estación de gestión debe estar correctamente configurada para trabajar sobre IPX.

- Al menos un servidor o router IPX debe estar conectado a la misma red de la estación de gestión.

- Los nodos deben estar activos y responder el diagnostico IPX para ser descubiertos.

Tal como con el descubrimiento en IP, la información de los nodos es almacenada en la base de datos del Network Node Manager y se usa automáticamente para generar el mapa de la red.

Network Node Manager toma la información provista por tres estándares MIB para descubrir bridges, switches y hubs. Estos tres estándares MIB son el *RFC 1493*, el *RFC 2108* y el *802.3 MAU*. Si un dispositivo de red soporta cualquiera de estos estándares, el Servicio *Netmon* deberá usar la información proporcionada para desarrollar un modelo de la topología que

representa mejor, como y a que dispositivos están conectados. La *Figura 3.1* muestra un submapa de la red LAN de la compañía Maint, luego del proceso de descubrimiento.

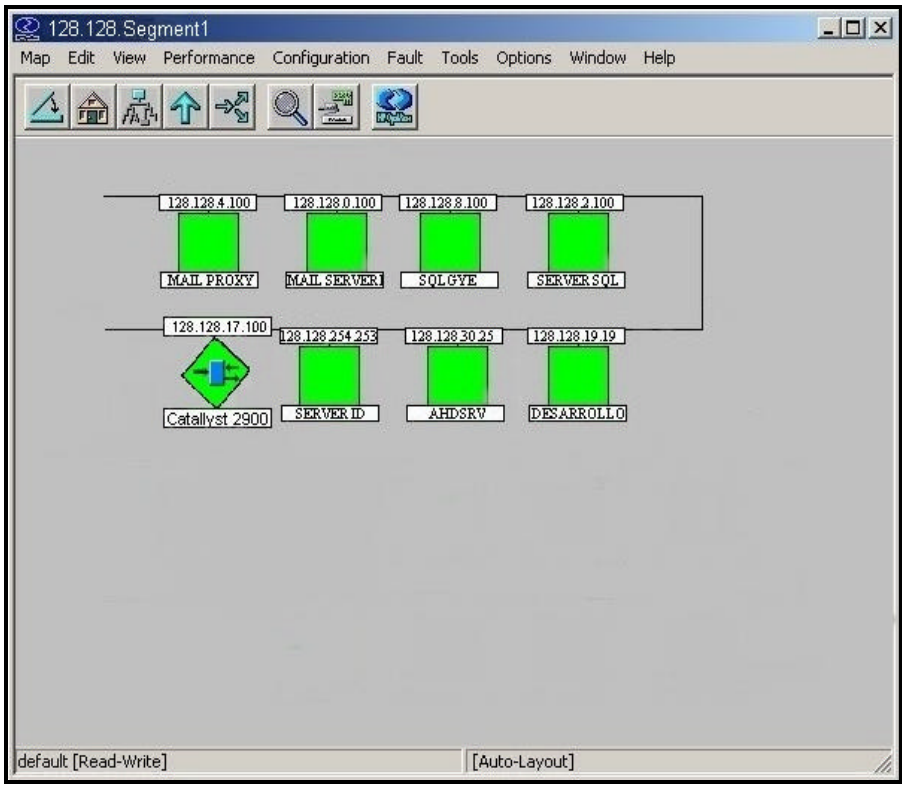

Figura 3.1Visualización del Segmento 1 de la red de Maint.

3.2.2 Bases de datos.

Hp OpenView Network Node Manager provee algunas bases de datos diseñadas para almacenar datos específicos y utilizarlos para varios propósitos, incluyendo una base de datos que almacena datos históricos de la red.

Las bases de datos operacionales son:

- Base de datos de objetos.
- Base de datos de mapas.
- Base de datos de topología.
- Base de datos de eventos.
- Base de datos de tendencias.

3.2.2.1 Base de datos de objetos.

Esta base de datos contiene información específica acerca de los símbolos de los mapas. La información es genérica, no puede ser personalizada. Contiene información tales como sysObjectID, vendedor y el agente SNMP.

3.2.2.2 Base de datos de mapas.

Contiene información específica de cada mapa tales como la ubicación exacta de cada símbolo en el mapa, el símbolo asociado con cada objeto, y la etiqueta de cada símbolo.

3.2.2.3 Base de datos de la topología.

Es la que maneja información crítica de gestión de los nodos IP, incluye información de estado que indica cuando fue la última vez

que cambió la configuración y cuando debe ser el siguiente sondeo.

Esta información ayuda a detectar cambios y comunicarlos a los diferentes servicios del Network Node Manager.

3.2.2.4 Base de datos de eventos.

Esta base de datos almacena los Traps SNMP y los eventos propios del Hp OpenView que son recibidos por el programa, también almacena eventos manejados por el Servicio de Correlación de Eventos (ECS) por sus siglas en inglés.

3.2.2.5 Base de datos de tendencias.

También llamada *snmpCollect*, guarda información de la MIB y los umbrales generados por el servicio snmpCollect (proceso). La información de la base de datos de tendencias se la utiliza en los reportes y puede verse de manera gráfica en la estación de gestión.

3.2.3 Visualización de mapas.

En el Network Node Manager cuando se ve una parte de la red, entonces se está viendo un submapa. La vista puede representar una

visión amplia de la red o un submapa detallado de alguna porción de la red.

3.2.3.1 Diferencia entre mapas y submapas.

Un mapa es un conjunto de objetos, símbolos y submapas relacionados que nos muestra una representación gráfica y jerárquica de la red. Se pueden crear múltiples mapas, pero solo uno puede estar abierto en una sesión del Network Node Manager.

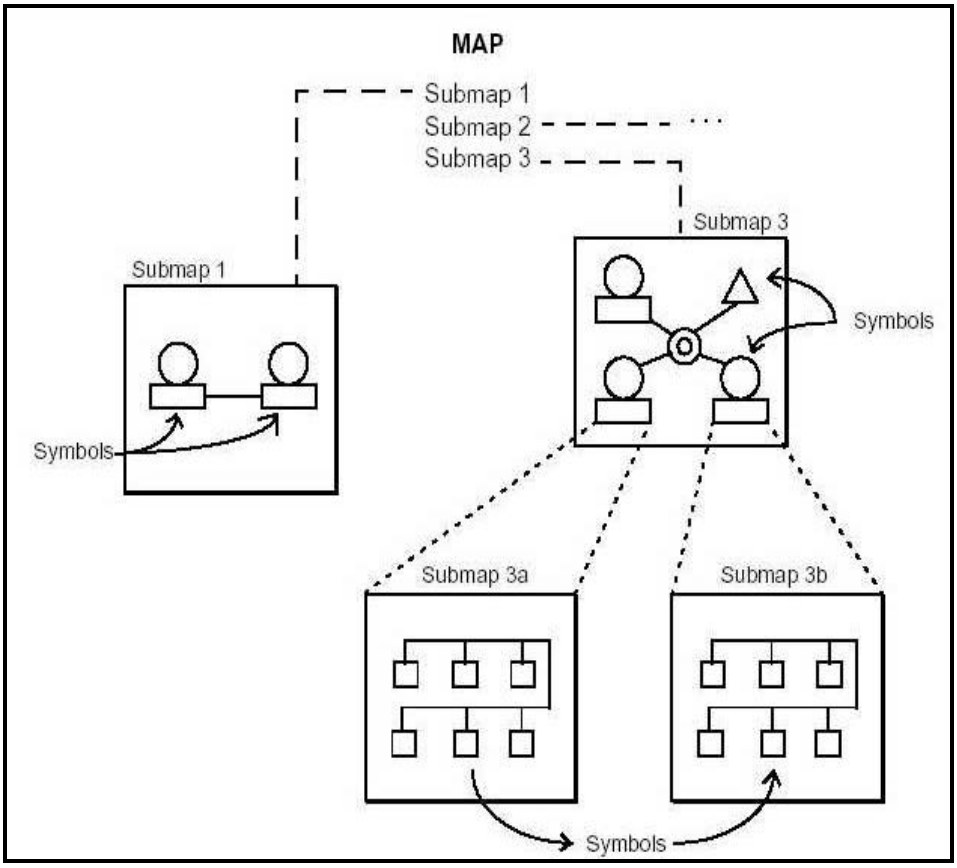

Figura 3.2 Relación entre mapas y submapas.

La *Figura 3.2* nos muestra como los submapas y sus símbolos pueden gráficamente ayudarnos con la información de gestión de la red.

No se ve directamente un mapa, sino los submapas que lo comprenden, pudiéndose desplegar múltiples submapas a la vez. Los submapas se organizan jerárquicamente para mostrarnos sus niveles con detalle. Se pueden definir diferentes mapas para diferentes regiones de gestión o diferentes presentaciones para la misma región de gestión.

Al poder crear múltiples mapas se puede personalizar la información que se mostrará en cada uno. La información de un mismo objeto puede mostrarse en diferentes mapas debido a que todos obtienen la información desde la misma fuente, la base de datos de los objetos.

Se pueden ver varios mapas a través de múltiples sesiones con el Network Node Manager, sin embargo como ya se mencionó solo un mapa a la vez por sesión. De esta manera un usuario puede abrir múltiples mapas abriendo múltiples sesiones. Diferente usuarios pueden abrir el mismo mapa al mismo tiempo por medio

de diferentes sesiones, pero todos los usuarios excepto el primero estarán limitados al acceso de solo lectura.

Un submapa es una vista particular de la red, consiste en símbolos relacionados que se muestran en una ventana. Network Node Manager crea un submapa raíz para cada mapa, este submapa raíz provee organización de niveles para cada mapa, es decir de manera jerárquica con el submapa raíz a la cabeza. Pero también se puede crear mapas independiente de esta jerarquía.

Se pueden abrir y desplegar múltiples submapas de un mapa al mismo tiempo, navegando de un submapa a otro por medio de los símbolos explorables, obteniendo información más detallada. La relación de jerarquía de los submapas crea una relación padre-hijo entre ellos. Esta relación nos ayudará a mantener un buen control sobre la organización de la red y poder ver cualquier lugar en particular, es decir seleccionar departamento específico de un nodo en particular, pudiendo personalizar esta organización para satisfacer nuestros propósitos.

3.2.3.2 Diferencia entre objetos y símbolos.

Un Objeto representa una entidad o dispositivo particular en un sistema o red de computadoras, puede representar una pieza física

del equipo de red, componentes de un nodo o partes de la red, como por ejemplo una estación de trabajo, un router, una interfase o una conexión RS-232.

El objeto representa el dispositivo modelando sus atributos. Un objeto está representado por símbolos en mapas y submapas de la red.

Todo objeto almacenado en la base de datos posee atributos o propiedades que los definen. Un atributo es una característica de un objeto cuyos valores pueden ser asignados tales como:

- Hostname
- Dirección
- Estado
- Descripción
- Propietario

Todos los objetos tienen un atributo especial llamado *selection name*, el cual identifica únicamente a un objeto. Las operaciones que se pueden realizar con los objetos son:

- Agregar un objeto.

- Seleccionar uno más objetos.
- Localizar objetos.
- Agregar atributos al objeto.
- Cambiar descripción del Objeto.
- Cambiar valores SNMP.
- Borrar objetos.
- Ocultar objetos.
- Mostrar objetos ocultos.

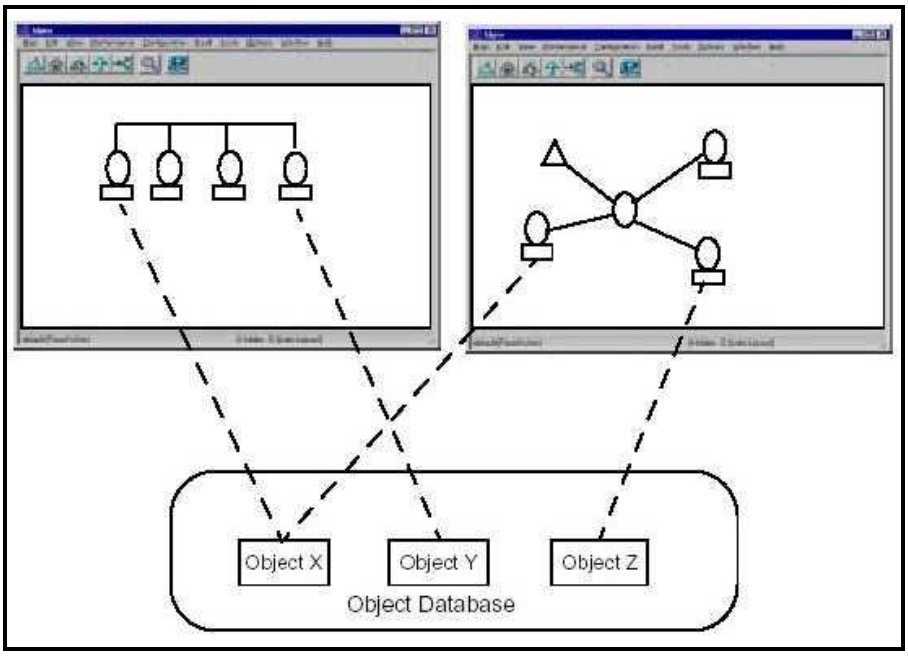

Figura 3.3 Relación entre objetos y símbolos.

Un símbolo es una representación gráfica de un objeto. Un objeto puede ser representado por múltiples símbolos que pueden existir en el mismo submapa, en múltiples submapas de un mismo mapa

o en diferentes mapas. Un símbolo nunca representa más de un objeto a la vez. La *Figura 3.3* muestra la relación entre objetos y símbolos.

Además de representar objetos, los símbolos realizan las siguientes funciones:

- Permiten navegar a través de submapas en un mapa.

- Algunos símbolos realizan acciones predefinidas.

- Puede ser configurado para mostrar el estado del objeto al cual representa.

Existen dos variedades el símbolo icono y el símbolo conexión.

- **El símbolo icono:** usualmente referido simplemente como símbolo consiste en una forma geométrica en la cual aparece dentro un símbolo o icono. Cada símbolo consiste de clases y subclases, la clase se indica fuera de la forma del símbolo y cada clase se divide en subclase. La *Figura 3.4* muestra las subclases del símbolo Connector.

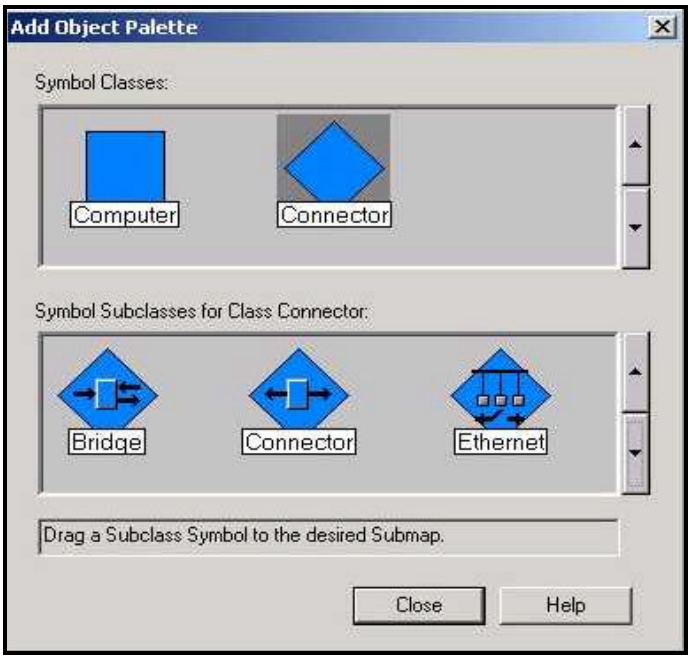

Figura 3.4 Subclases del Símbolo Icono (Connector.)

- **El símbolo conexión:** es una línea que gráficamente representa la conexión entre dos símbolos iconos, que nos muestra el estado de conexión entre dos objetos. Ver *Figura 3.5.*

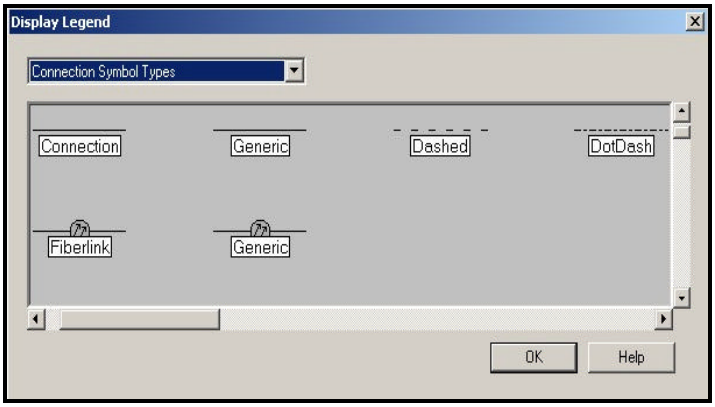

Figura 3.5 Tipos de Símbolo Conexión.

Las operaciones que se pueden realizar con los símbolos son:

- Añadir símbolos (icono o de conexión)
- Añadir un símbolo ejecutable.
- Cambiar las funciones del símbolo.
- Cambiar la etiqueta del símbolo.
- Cambiar el tipo de símbolo.
- Cortar y pegar símbolos.
- Copiar símbolos.

3.2.4 Correlación de eventos.

Network Node Manager incluye el Servicio de Correlación de Eventos (ECS) por sus siglas en inglés, el cual nos ayudará a gestionar una eventual lluvia de eventos y definir relaciones entre los diferentes tipos de eventos. El servicio de correlación de eventos mejora la generación de alarmas suprimiendo las no deseadas y las redundantes, dando prioridad a las más significativas.

Esto produce menos alarmas pero con mayor información, mostrándonos las relaciones y dependencias entre eventos de la red. Lo que da como resultado la facilidad para identificar tendencias, aislar eventos importantes y reaccionar rápidamente a los problemas.

El servicio de correlación de eventos procesa eventos basándose en la relación entre eventos individuales, analizando eventos anteriores, actuales o subsecuentes, pudiendo inclusive crear nuevos eventos.

3.2.5 Sondeos y alarmas.

Existen muchos servicios dentro del Network Node Manager que recogen y generan información de eventos que se remiten a este. Estos eventos pueden ser emitidos desde agentes en nodos gestionados, de aplicaciones de gestión en diferentes estaciones de gestión, de algún nodo específico de la red o los eventos SNMP no solicitados llamados Traps.

Para gestionar esta alarmas Network Node Manager nos ofrece un servicio, el visor de alarmas, por medio del cual podemos ver todos los Eventos y Traps que se generen, teniendo el control sobre todos ellos y de esta manera determinar cuales debemos considerar lo suficientemente importantes como para definirlos como alarmas, facilitándonos la tarea de monitorización de las alarmas, para tomar decisiones apropiadas que nos garanticen el buen funcionamiento de la red.

Network Node Manager nos permite las siguientes operaciones relacionadas con las alarmas:

- Nos muestra la información útil de una alarma.

- Nos permite agrupar alarmas por categorías.

- Nos ayuda a reconocer que problema causó la alarma.

- Nos facilita obtener información particular mediante el filtrado de alarmas de distintas maneras.

- Nos permite ejecutar acciones adicionales una vez que se selecciona la alarma.

Para visualizar las alarmas existe el visor de alarmas el cual nos permite ver las alarmas por categorías, si deseamos ver las alarmas de cualquier símbolo en algún submapa, basta con seleccionarlo y filtrar sus alarmar por categoría.

3.2.5.1 Categorías de Alarmas.

Por conveniencia Network Node Manager ordena las alarmas en categorías, por defecto son las siguientes:

- Alarmas de errores.
- Alarmas de umbrales.
- Alarmas de estados.

- Alarmas de configuración.
- Alarmas de aplicaciones.
- Todas la alarmas.

Figura 3.6 Ventana de alarmas por categoría.

Para acceder a ellas cada una posee un botón el cual cambia de color según sea el estado de los dispositivos que la generan, como se muestra en la *Figura 3.6.* Así los colores que indican la severidad de cada evento son los siguientes:

- Verde normal
- Cian advertencia
- Amarillo problema menor
- Naranja problema mayor
- Rojo problema crítico

Al acceder a cualquiera de las categorías se mostrarán listadas en orden cronológico las alarmas pertenecientes a la categoría

seleccionada, indicando la severidad, fecha, hora, que dispositivo la produjo y una breve descripción de la alarma, como se muestra en la *Figura 3.7.*

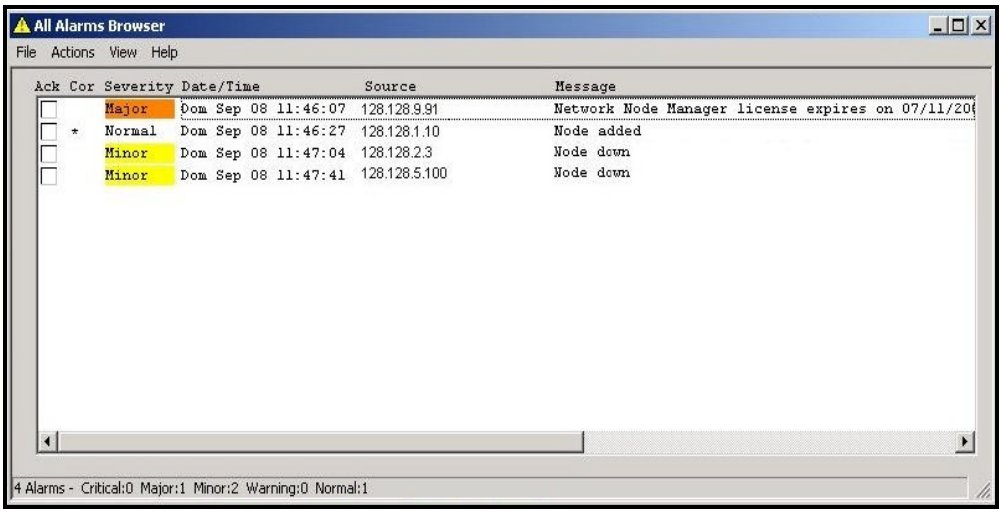

Figura 3.7 Visor de alarmas.

Otra cosa que hay que indicar es que en cada submapa se muestra el estado de cada dispositivo de red. Hay dos categorías de condición de estado: administrativo y operacional. El Hp OpenView Network Node Manager reconoce diez condiciones de estado que mencionamos a continuación:

Estados Administrativos

- **Administrative Unmanaged:** Este estado indica que el objeto no puede ser monitorizado y el estado operacional puede ser ignorado.

- **Administrative Testing:** Indica que el objeto está temporalmente en diagnóstico o ha sido sometido a mantenimiento.

- **Administrative Restricted:** Indica que el objeto funciona normalmente pero no está disponible para otros usuarios.

- **Administrative Disabled:** Indica que el objeto está inactivo aunque no necesariamente tenga algún daño.

La *Figura 3.8* muestra los colores usados para representar los diferentes estados administrativos.

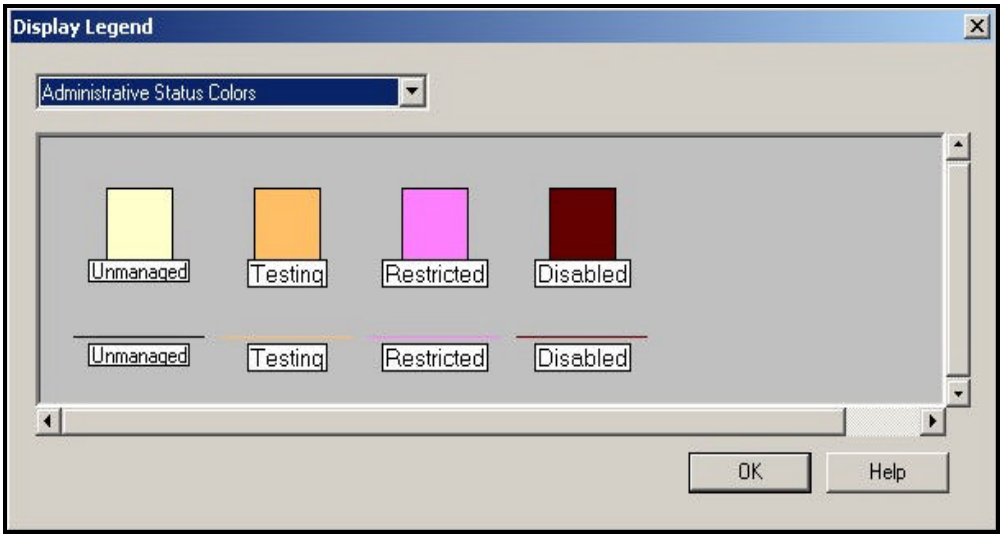

Figura 3.8 Colores de los diferentes estados Administrativos.

La *Figura 3.9* muestra los colores usados para representar los diferentes estados operacionales.

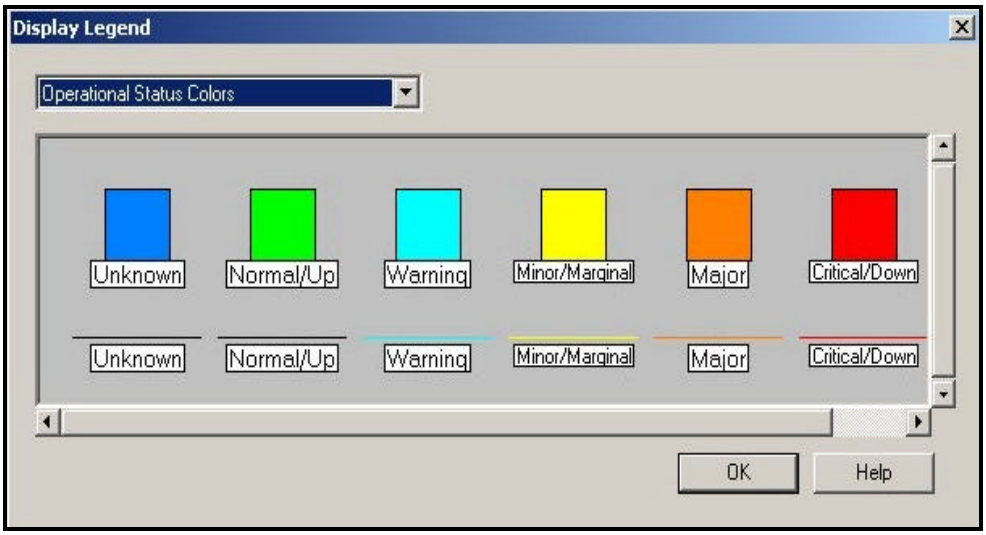

Figura 3.9 Colores de los diferentes estados operacionales.

Estados Operacionales

- **Operacional Unknown:** cuando el estado de un objeto no puede ser determinado.

- **Operacional Normal:** indica que el objeto está en estado de operación normal.

- **Operacional Warning:** cuando un objeto puede tener un problema potencial.

- **Operacional Minor/Marginal:** cuando un objeto tiene un problema menor, pero puede seguir operando normalmente.

- **Operacional Major:** indica que el objeto tiene un problema serio y en cualquier momento deje de operar normalmente.

- **Operacional Critical:** indica que el objeto no está funcionando.

CAPITULO 4

IMPLEMENTACION DEL HP OPENVIEW NETWORK NODE MANAGER EN LA RED DE MAINT

4.1 Requisitos para la instalación del HP OPENVIEW NODE MANAGER.

Antes de proceder a instalar el software de gestión, debemos revisar los requisitos que debe cumplir la estación de gestión, los cuales son:

- Procesador Intel Pentium de 333 MHz o superior.
- Microsoft Windows NT o Windows 2000 Workstation o Server versión 4.0 y además tener instalado y configurado el protocolo TCP/IP.
- 256 MB de memoria RAM.
- Monitor 800x600 con tarjeta gráfica SVGA.
- 650 MB de espacio libre en el disco duro.
- Tarjeta de Red.

Para instalar el Hp OpenView Network Node Manager debemos instalar primero ciertos servicios, algunos requeridos y otros que son opcionales según el ambiente de la red.

- Paging File setup depende del ambiente de la red.
- Servicio TCP/IP requerido.
- Microsoft SNMP Agent requerido.
- DHCP setup depende del ambiente de la red.
- Servicio IPX opcional.
- Web Browser requerido.
- Web Server requerido.
- Microsoft data access components check requerido.
- Microsoft Terminal Services opcional.
- Windows NT Service Pack reinstallation requerido.

Además se tiene que poseer la licencia del software que para el caso de la compañía Maint debe ser una para 250 nodos cuyo costo es de $4000.

4.2 Instalación del Hp OpenView Network Node Manager.

Una vez que se ha instalado todos los servicios anteriormente mencionados se procede a instalar el software Hp OpenView Network Node Manager de la siguiente manera:

1. Se inserta el CD de instalación, si no se ejecuta el programa de instalación automática se debe hacer lo siguiente:

- En el Menú inicio de la barra de tareas del sistema operativo Windows NT se selecciona configuración, y luego panel de control.

- Se selecciona agregar o quitar programas.

- Luego en el cuadro de dialogo Instalar o desinstalar, se selecciona instalar.

2. Una vez que se ejecuta el programa de instalación, este guiará con los pasos que se deben seguir.

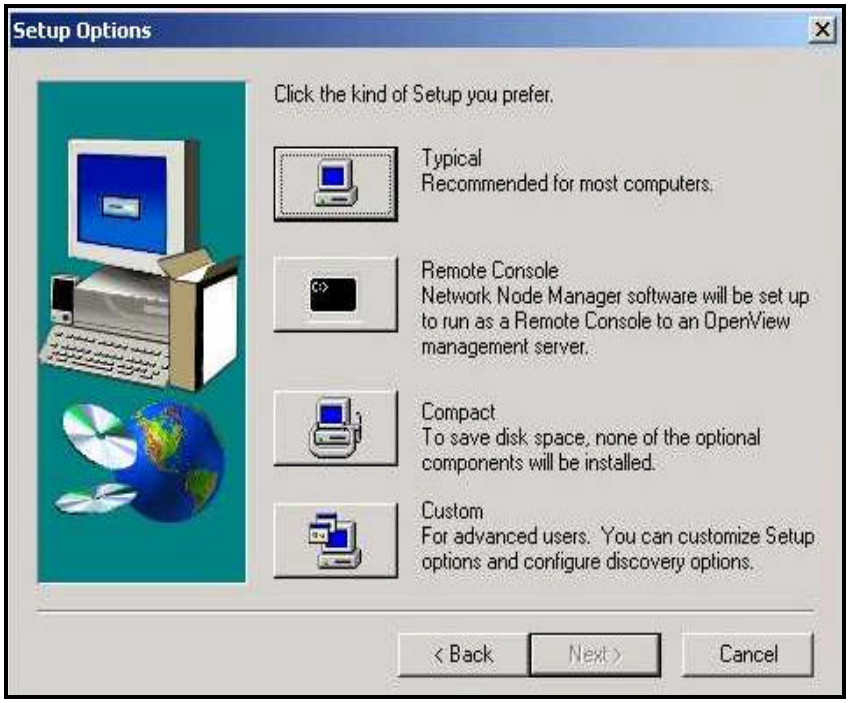

Figura 4.1 Tipos de instalación.

- En el cuadro de diálogo de instalación aparecerán cuatro tipos de instalaciones que se muestran en la *Figura 4.1*

3. Se escoge uno que este de acuerdo a las necesidades. A continuación el programa de instalación mostrará algunos gráficos que indican el progreso de la instalación.

4. Una vez terminada la instalación se presentarán dos opciones:

   - Ver notas
   - Comenzar Network Node Manager automáticamente.

5. Si no se eligió comenzar Network Node Manager automáticamente al final del proceso de instalación, se puede hacer lo siguiente:

   - Primero se debe lanzar la interfaz gráfica de usuario (GUI), seleccionando el botón inicio de la barra de tareas del sistema operativo Windows NT, luego Programas, Hp OpenView, Network Node Manager, Admin, Services, Start.

   - Después para comenzar con el Hp OpenView Network Node Manager se selecciona el botón inicio de la barra de

tareas del sistema operativo Windows NT, luego Programas, Hp OpenView, Network Node Manager.

El Hp OpenView Network Node Manager comienza a recoger la información que necesita para establecer el mapa de la red en cuanto se empiezan sus servicios (procesos en background). Estos servicios monitorizan continuamente la red y su actividad; y deben ser activados la primera vez que se ejecuta el Hp OpenView Network Node Manager, después de esto ellos correrán continuamente así no se tenga abierta la interfase del usuario.

Para saber el estado de los servicios que forman parte del Hp OpenView Network Node Manager se debe seleccionar el botón inicio, Programas, Hp Openview, Network Node Manager, Admin, Services, Status.

4.3 Descubrimiento de dispositivos.

Como se mencionó anteriormente el Hp OpenView Network Node Manager puede reconocer automáticamente cada dispositivo en la red y la relación entre ellos. Esta información es almacenada en las bases de datos de objetos y topología para luego usarse en la creación del mapa predefinido y en el sistema de rastreo de eventos, los cuales nos ayudaran a identificar y arreglar los problemas en la red.

Una vez de que se comenzaron los servicios del Hp OpenView Network Node Manager (procesos en background), se genera un intenso tráfico en la red debido al sondeo realizado por el Servicio *Netmon*, servicio de monitoreo, el cual trabaja tan rápido como le es posible para descubrir cada uno de los dispositivos de la red.

El Hp OpenView Network Node Manager utiliza la información que le proporciona el Servicio *Netmon* para determinar el símbolo más apropiado para la representación de cada dispositivo en la red. Si no se encuentra un símbolo específico entonces se representa utilizando un símbolo genérico en el mapa.

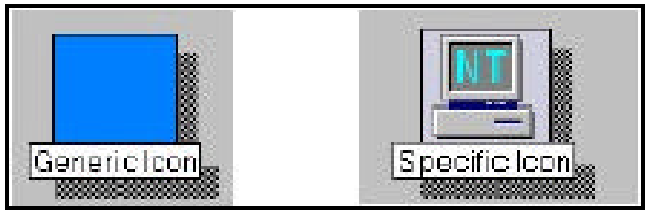

Figura 4.2 Icono genérico versus icono específico.

La *Figura 4.2* muestra la diferencia entre el símbolo genérico y el específico, cabe recalcar como el símbolo específico nos indica mucha más información que el símbolo genérico como por ejemplo el sistema operativo que posee el dispositivo de red.

El proceso inicial de descubrimiento toma tiempo por lo que se recomienda que se le permita al Hp OpenView Network Node Manager trabajar toda la noche para obtener la mayoría de la información disponible de la red. Luego de que se completa el descubrimiento de los dispositivos se debe verificar la precisión o exactitud del mapa, para estar seguros de que cualquier dispositivo que se haya definido como crítico aparezca en el mapa.

4.4 Establecimiento de los dominios de gestión.

Como ya se ha indicado, al terminar de descubrir los dispositivos el Hp OpenView Network Node Manager crea un mapa de la red con todos los dispositivos que fueron descubiertos.

Por medio del Hp OpenView Network Node Manager podremos definir cuales dispositivos serán gestionados directamente por sus servicios de sondeo y cuales no. Y aunque un dispositivo no se gestione directamente podemos configurar el agente SNMP del dispositivo para que envíe algún trap a la estación de gestión cuando ocurra algún evento relevante para el funcionamiento de la red.

El poder de personalizar la magnitud del dominio de gestión nos permite gestionar la red de manera interactiva, decidiendo que dispositivos no son críticos lo que nos ayudará a disminuir el tráfico de gestión.

A continuación se describen los procedimientos para habilitar y deshabilitar un dispositivo como gestionable.

4.4.1 Habilitar o deshabilitar un dispositivo para la gestión.

Para cambiar el estado de un dispositivo de no gestionable a gestionable o viceversa se deben realizar los siguientes pasos:

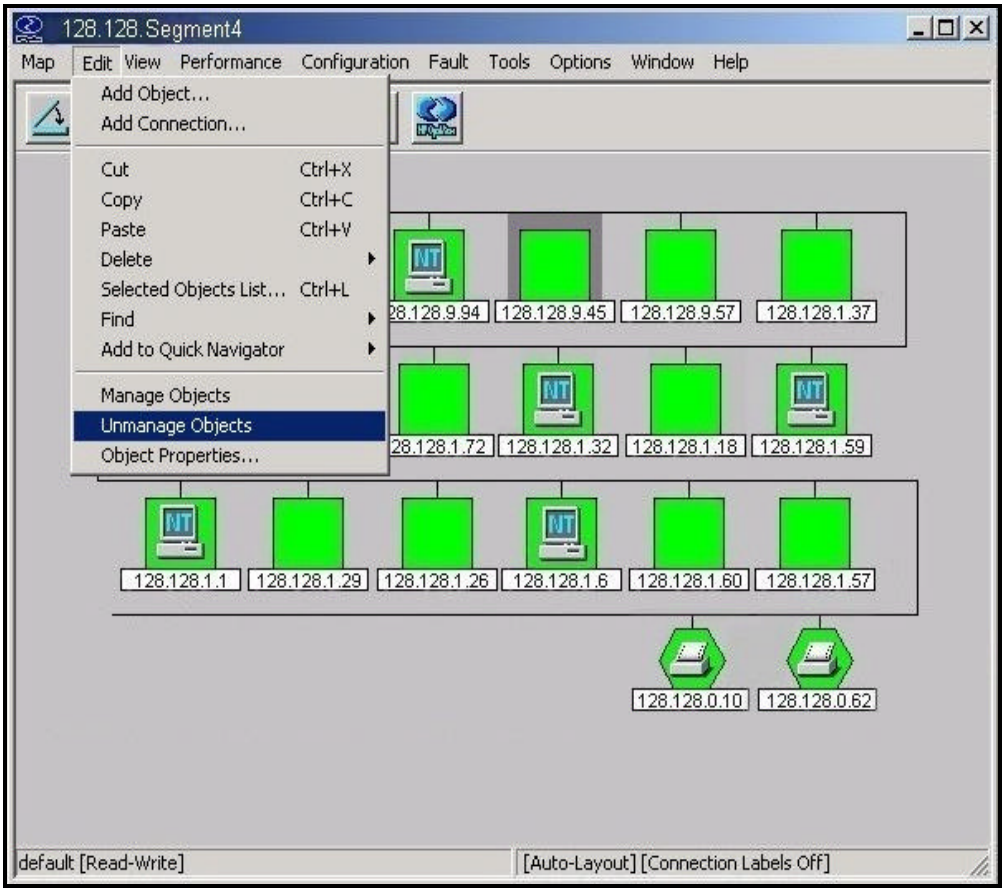

Figura 4.3 Método para habilitar o deshabilitar un dispositivo para la gestión.

1. Se selecciona del Mapa el símbolo del dispositivo que se desea habilitar o deshabilitar para la gestión, en este caso se ha seleccionado la computadora con dirección IP 128.128.9.45 de la red LAN de la compañía Maint.

2. Luego se elige del *Menú Edit* la opción *Manage Objets* o *Unmanage Objects*, para habilitar o deshabilitar el dispositivo para la gestión respectivamente, tal como se muestra en la *Figura 4.3.*

Hp OpenView Network Node Manager se encarga de actualizar el mapa, las bases de datos y el servicio de monitoreo de eventos para incluir o excluir el dispositivo.

CAPITULO 5

ANALISIS DE PRESTACIONES DE GESTION DE LA RED DE MAINT

La gestión de red puede definirse en términos generales como la habilidad de tener un punto de control que nos permita las actividades de manejar una red. El Hp OpenView Network Node Manager provee al administrador de una red de una herramienta integral para controlar y gestionar múltiples sistemas de red y aplicaciones desde una representación gráfica (Mapas).

Una estación de gestión debidamente implementada nos ayudará a:

- Reducir el tiempo fuera de servicio de una red o de algún elemento de ésta.

- Una rápida detección y corrección de problemas evitando el rompimiento del servicio de red.

- Tener habilidad de supervisar datos para anticipar problemas.

- Tener habilidad de guardar información histórica para su análisis.

- Tener la habilidad de realizar alguna acción cuando se presenta un evento o situación predefinida.

Para comprender como el Hp OpenView Network Node Manager maneja estos problemas, debemos dividir la gestión en cinco categorías que listamos a continuación:

- Gestión de Fallos.
- Gestión de Rendimiento.
- Gestión de Configuración.
- Gestión de Contabilidad.
- Gestión de Seguridad.

Cabe mencionar aquí que el Hp OpenView Network Node Manager nos permite de manera directa realizar las tres primeras funciones de gestión: Fallos, Rendimiento y Configuración que detallamos a continuación.

5.1 Gestión de fallos.

La función de gestión de fallos comprende el conjunto de facilidades que permiten detectar, aislar, controlar y corregir problemas o fallas en la red. Esto se lleva a cabo por el monitoreo de alarmas, alertas, reportes y por herramientas de predicción.

Un fallo en la red trae como consecuencia que el usuario no pueda utilizar algún servicio, por lo que es deseable su pronta detección y resolución.

La gestión de Fallos consta de los siguientes pasos:

- Determinar donde está el problema exactamente.

- Aislar el resto de la red del elemento que ha fallado para que pueda seguir funcionando sin interferencias.

- Reconfigurar la red para minimizar el impacto de la operación sin el componente que ha fallado.

- Reparar o sustituir los componentes para restablecer la red a su estado inicial.

Después de solucionar el problema y restablecer el sistema a su estado operacional el servicio de gestión de fallos debe asegurarse de que el problema este resuelto por completo.

Otros aspectos a tener en cuenta son las medidas preventivas, es decir la predicción de fallos al identificar una degradación del rendimiento, y su solución si es posible antes de que se produzca y el usuario se vea afectado.

La mayoría de las veces la tarea más difícil para el administrador de la red es identificar la fuente del problema cuando este ocurre. El Hp OpenView Network Node Manager nos ayuda a identificar problemas, errores y reconocer tendencias para evitar posibles fallas. Nos permite:

- Descubrir automáticamente los nodos IP e IPX en la red.

- Monitorear automáticamente el estado de la red a través de una interfase gráfica (mapa) y por la generación de eventos, lo que nos permite su debido control.

- Gestionar dispositivos de diferentes marcas que soporten el Protocolo Simple de Gestión de Red (SNMP).

- Ingresar a la Base de información de gestión (MIB). Una vez que se ha cargado la MIB en la estación de gestión se podrá tener acceso a cualquier objeto definido en esta MIB.

- Definir umbrales de eventos para los objetos de la MIB; por ejemplo un evento puede ser generado cuando el disco en un dispositivo exceda un límite.

- Definir acciones que se deben tomar al recibir una alarma (Trap) SNMP.

- Gestionar eventos y mejorar el volumen de información suprimiendo eventos no deseados y redundantes mediante el Servicio de Correlación de Eventos.

- Diagnosticar fallas en la red y problemas en el desempeño de dispositivos analizando sus tendencias, permitiendo personalizar y automatizar el monitoreo de la red y la respuesta de la estación de gestión a los eventos.

- Administrar o ver las propiedades de un nodo por medio del Servidor de Gestión de Sistemas (SMS por sus siglas en inglés).

Las opciones que brinda el Hp OpenView Network Node Manager dentro de la Función de Gestión de Fallos son las siguientes:

- Configuración de Eventos.
- Configuración de Umbrales.
- Correlación de Eventos.
- Control de Alarmas.

5.1.1 Configuración de eventos.

Los eventos SNMP son la base de la gestión de redes, ya que las alarmas se generan cuando el Hp OpenView Network Node Manager

recibe notificaciones provenientes de los agentes de gestión. Una buena planificación y el uso de la configuración de eventos permitirán al Hp OpenView Network Node Manager supervisar la red LAN de la compañía Maint de una manera eficaz, ya que de esta forma se puede controlar y reforzar la manera en que se manejan las alarmas.

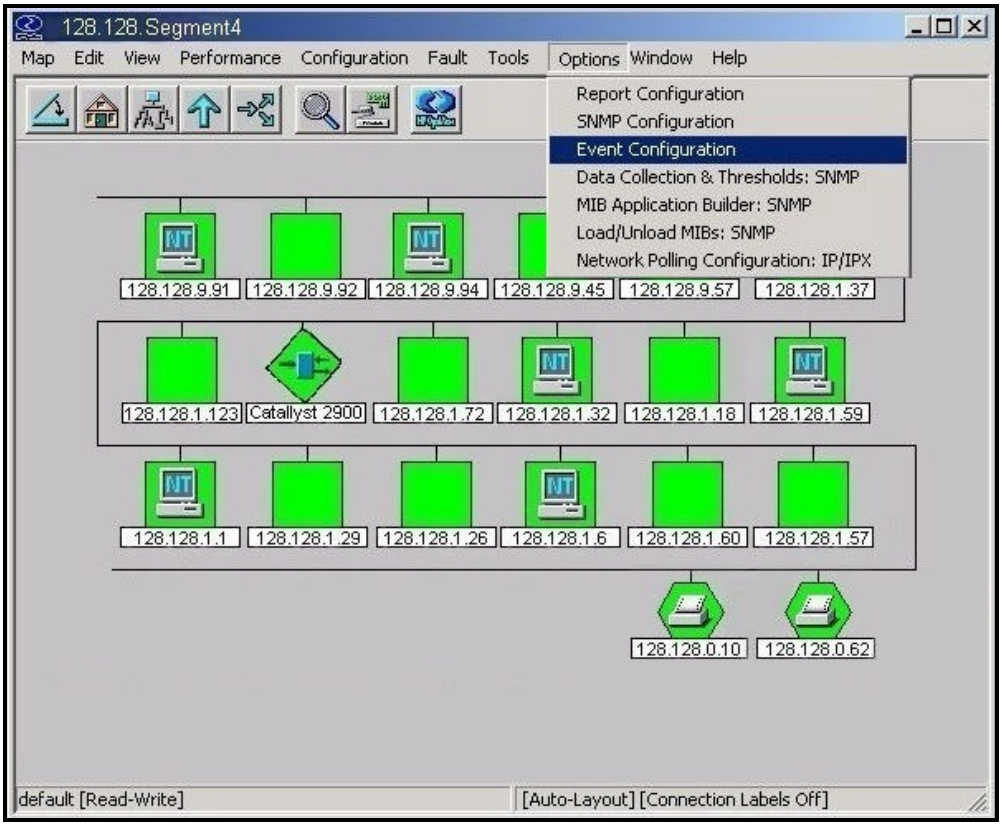

Figura 5.1 Método para abrir la ventana de configuración de eventos.

A continuación procedemos a describir la ventana de configuración de eventos, para visualizarla se debe ubicar en cualquier submapa de la red y luego seleccionar del *Menú Options,* la alternativa *Event Configuration*, tal como se muestra en la *Figura 5.1.*

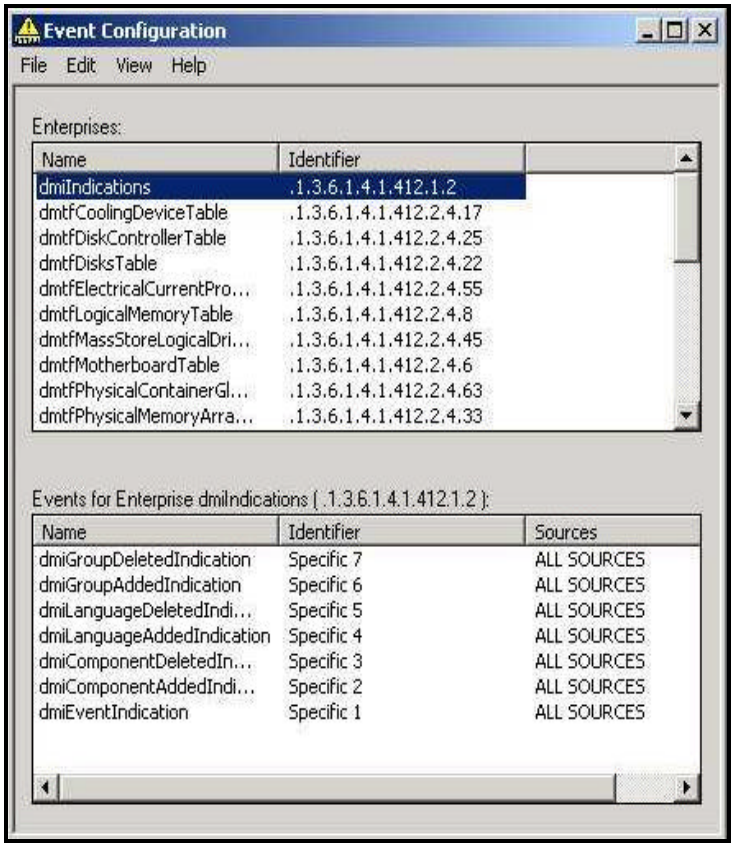

Figura 5.2 Ventana de configuración de eventos.

La ventana de configuración de eventos *Figura 5.2* tiene una Sección de Identificación de Empresa (parte superior), y una Sección de Identificación de Eventos (parte inferior).

En la Sección de Identificación de Empresa están definidos eventos específicos que son proporcionados por varios vendedores (empresas) y que se encuentran en la MIB. En esta sección se puede seleccionar la empresa asociada con los eventos que se quieren configurar, cada elemento en la lista contiene:

- **Nombre de la empresa:** es una representación conveniente y significativa del identificador de empresa usado por la aplicación configuración de eventos. Esta etiqueta usualmente corresponde al nombre de la empresa definido en la MIB.

- **Identificador de empresa:** corresponde al valor proporcionado con los traps.

La Sección de Identificación de Eventos consiste en una lista que identifica los eventos asociados con la empresa seleccionada en la parte superior. Esta lista consta de los siguientes campos:

- **Nombre del evento:** es el nombre que se usa para hacer referencia al evento.

- **Identificador del evento:** se puede mostrar como traps genéricos y específicos o como identificadores de objeto.

- **Fuentes:** son las fuentes potenciales del evento tales como nodos o Todas las fuentes (ALL SOURCES) si el evento se usa sin tener en cuenta la fuente del evento.

Mediante la configuración de eventos tenemos las siguientes posibilidades:

- Notificación de eventos.
- Definición de nuevos eventos.

5.1.1.1 Notificación de eventos.

Es importante tener en cuenta que el Hp OpenView Network Node Manager nos faculta seleccionar los eventos que nosotros consideremos necesarios para la gestión de la red LAN de la compañía Maint. Para esto podemos ingresar a la ventana de configuración de eventos y modificar según nuestros requerimientos de gestión las características de los eventos definidos en esta ventana, con la finalidad de tener un mejor control sobre dispositivos de red que se consideren primordiales para el buen funcionamiento de la red LAN de la compañía Maint.

A continuación se detalla el procedimiento para configurar el evento *OV_Connection_Down,* el cual nos alerta cuando un dispositivo de red ha caído. Este procedimiento puede utilizarse para modificar cualquier otro evento definido en la ventana de configuración de eventos.

1. Se abre la ventana de configuración de eventos desde cualquier submapa eligiendo del *Menú Options*, la alternativa *Event Configuration*.

2. En la parte superior de la ventana de configuración de eventos, se selecciona la empresa que proporciona la MIB, en este caso *OpenView*, y en la parte inferior se especifica el evento SNMP, en este caso se ha escogido *OV_Connection_Down*, tal como se muestra en la *Figura 5.3*, luego se escoge *Modify* de la opción *Events* del *Menú Edit* para modificar las características de la configuración del evento *OV_Connection_Down*.

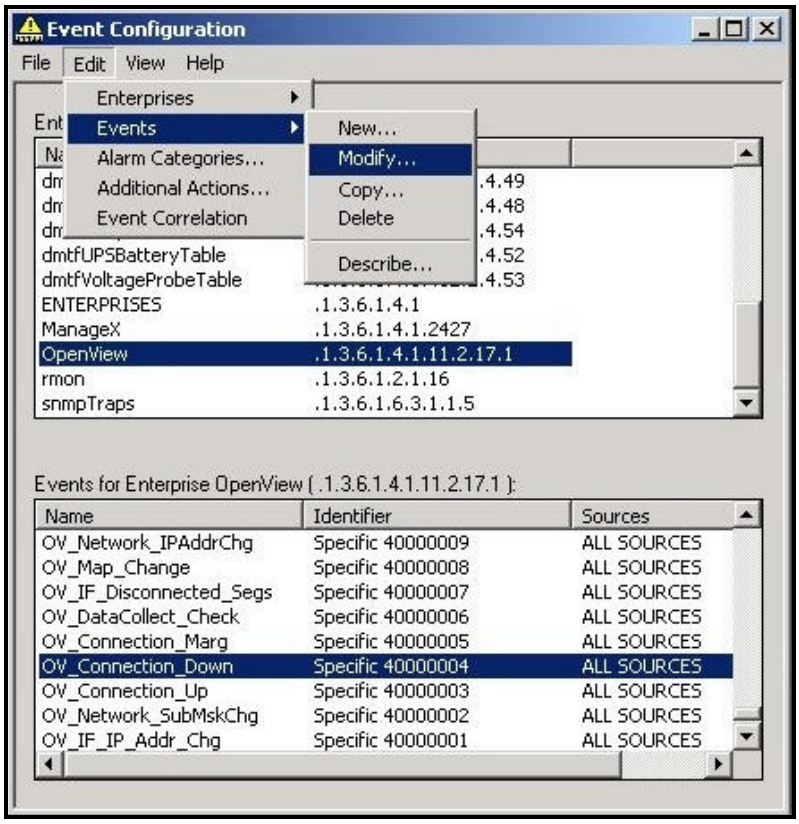

Figura 5.3 Ventana para modificar la configuración del evento OV_Connection_Down.

3. Se realiza la configuración del evento seleccionando la fuente a la que se le desea aplicar, especificando el nombre de host o la dirección IP, como se muestra en la *Figura 5.4,* en este caso hemos escogido el router Cisco 1750 de la red LAN de la compañía Maint cuya dirección IP es 10.1.1.1.

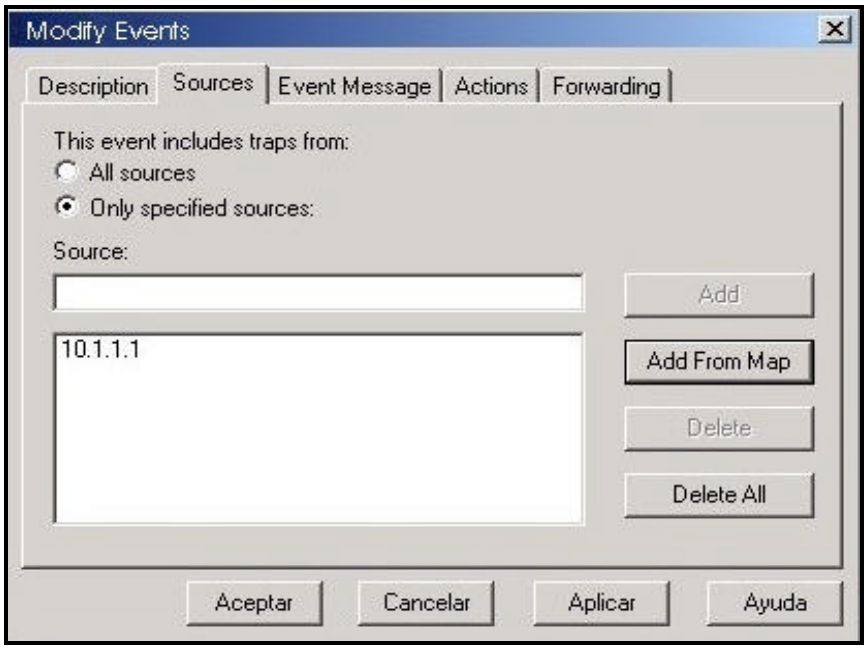

Figura 5.4 Especificaciones del evento OV_Connection_Down

4. Una vez que se han hecho las especificaciones necesarias para el evento *OV_Connection_Down*, se presiona *Aceptar* y luego se graba el evento por medio de la opción *Save* del menú *File*.

De esta manera obtenemos un evento que se activará solo cuando se produzca un fallo en la conexión de red del router Cisco 1750 de la red LAN de la compañía Maint.

5.1.1.2 Definición de nuevos eventos.

Mediante el Hp OpenView Network Node Manager podemos crear nuevos eventos que nosotros consideremos necesarios para hacer más eficiente la gestión de la red LAN de la compañía Maint.

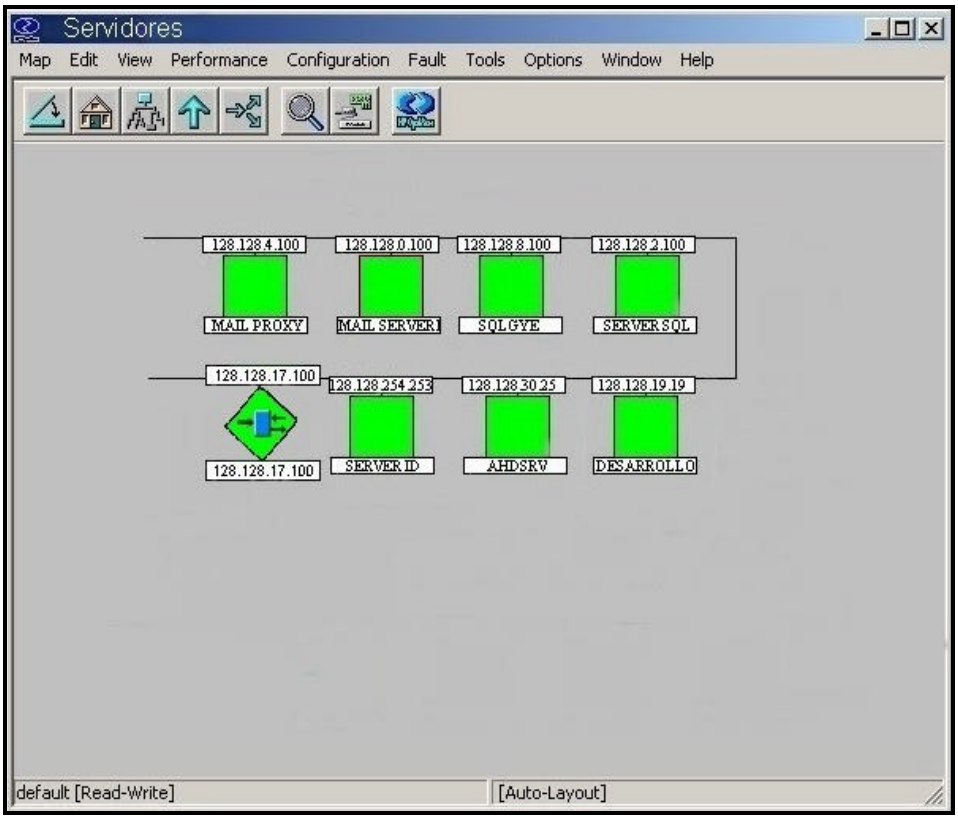

Figura 5.5 Mapa con los servidores de la compañía Maint.

Por ejemplo, hemos creado un mapa con todos los servidores que posee la compañía Maint, los cuales se aprecian en la *Figura 5.5* y a continuación hemos creado un evento de nombre OV_Servidor_Down para que se active cuando ocurra un fallo en la conexión de red de cualquiera de los servidores de la compañía Maint.

A continuación se describe el procedimiento para crear el evento *OV_Servidor_Down,* este procedimiento puede ser usado para crear cualquier otro evento.

1. Se abre la ventana de configuración de eventos desde cualquier submapa seleccionando del *Menú Options*, la alternativa *Event Configuration*.

2. En la parte superior de la ventana de configuración de eventos, se selecciona *OpenView*, y en la parte inferior se escoge el evento *OV_Connection_Down*, como se muestra en la *Figura 5.6,* luego se selecciona del *Menú Edit,* la alternativa *Events y* después la opción *Copy*, para copiar las características del funcionamiento del evento *OV_Connection_Down* y que va a ser usado por el nuevo evento *OV_Servidor_Down*.

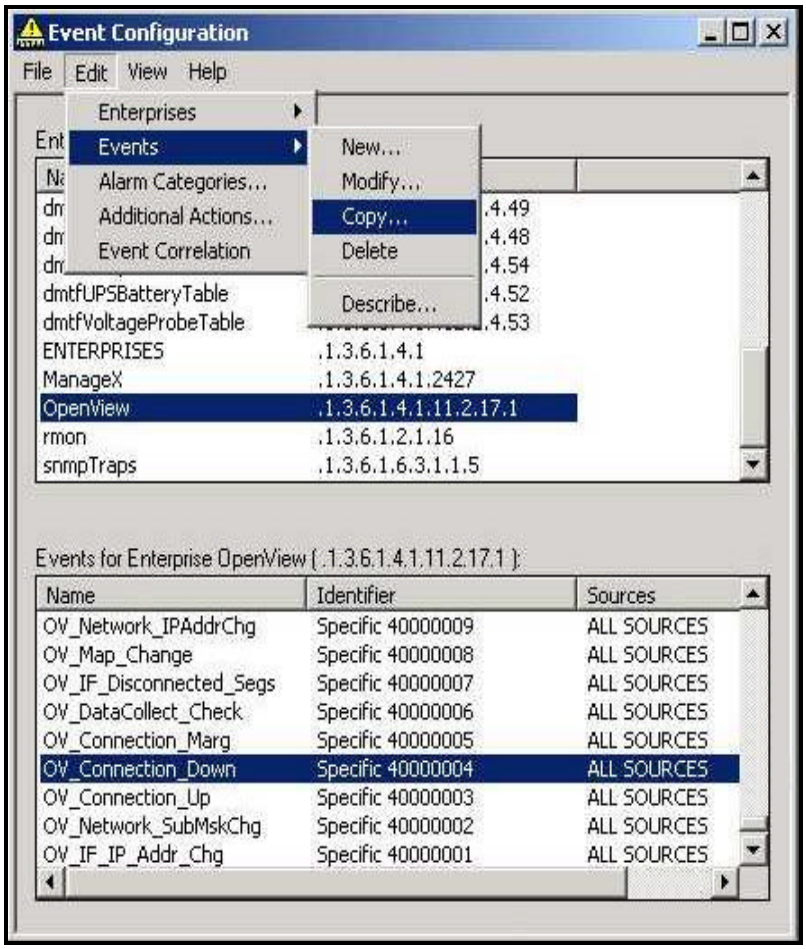

Figura 5.6 Método para crear el evento OV_Servidor_Down.

3. A continuación se procede a configurar el evento *OV_Servidor_Down* como se observa en la *Figura 5.7*, especificando la fuente o dispositivo al cual se le aplicará el evento, por medio de la dirección de red del dispositivo, en este caso ponemos la dirección IP de todos los servidores de la compañía Maint.

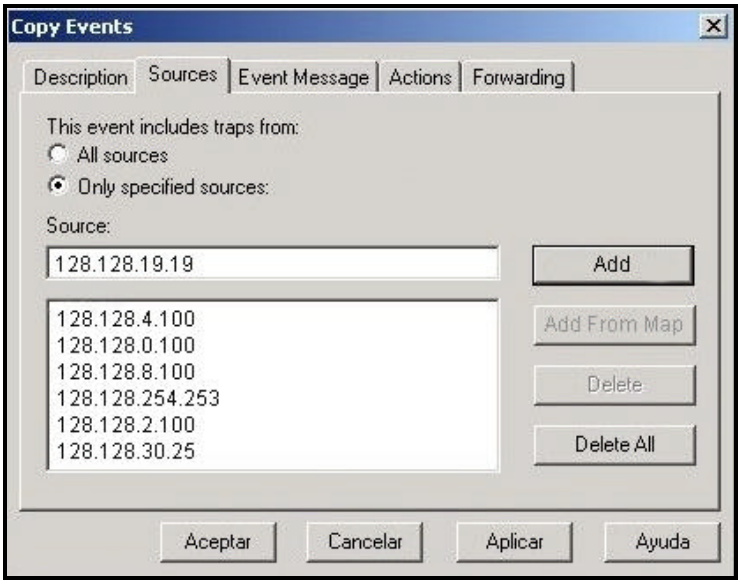

Figura 5.7 Ventana para configurar el evento OV_Servidor_Down.

4. Una vez que se ha configurado al evento *OV_Servidor_Down*, se presiona *Aceptar* y luego se graba el evento para que los cambios tengan efecto, por medio de la opción *Save As* del *Menú File*.

Luego de lo descrito, procedimos a realizar la prueba del evento, por lo que desconectamos el Servidor Mail y como resultado obtuvimos que en el mapa de servidores, los símbolos que representan la conexión a la red y el servidor Mail cuya dirección IP es 128.128.0.100 tomaron un color rojo como se muestra en la *Figura 5.8*, con lo cual se verificó el buen funcionamiento de la

configuración del evento *OV_Servidor_Down*. De esta manera tenemos un mejor control sobre los servidores de la red LAN de la compañía Maint.

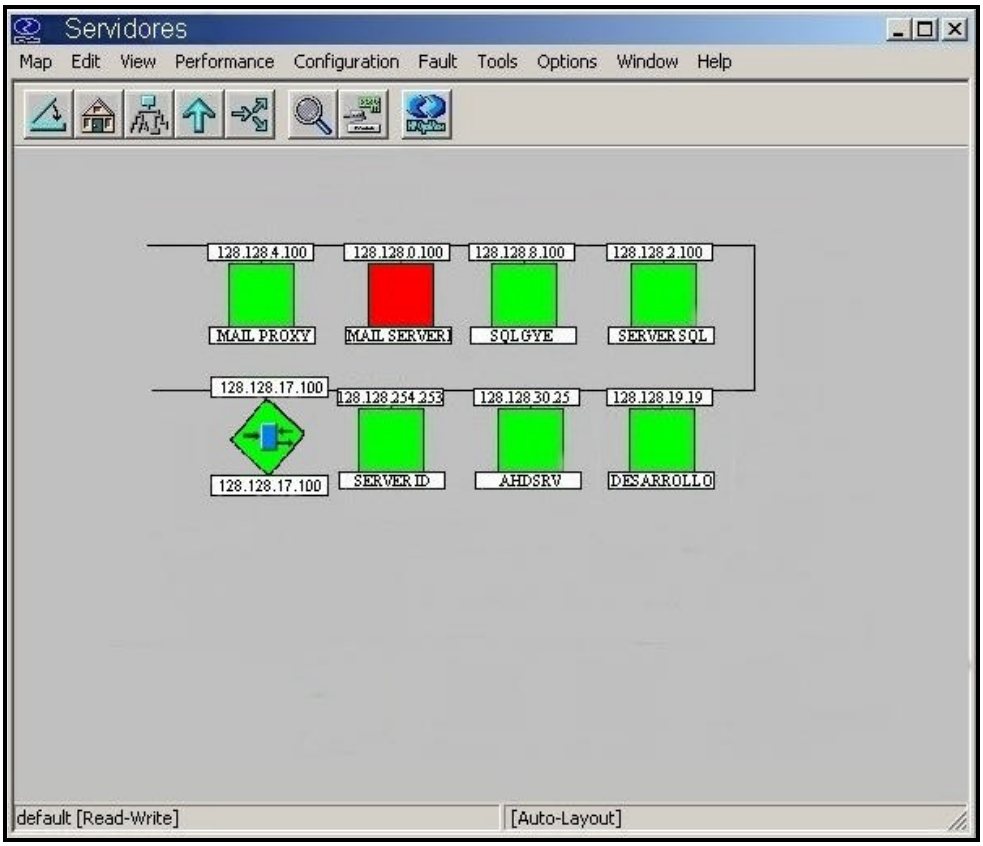

Figura 5.8 Mapa que representa el fallo en el servidor Mail de la compañía Maint.

5.1.2 Configuración de umbrales.

El Hp OpenView Network Node Manager nos permite definir umbrales asociados a objetos específicos de la MIB, y configurar sucesos que

se enviarán al Visor de Alarmas, así como acciones que se llevarán a cabo si los umbrales definidos se superan. Los umbrales se pueden especificar únicamente sobre objetos de la MIB definidos como numéricos, como por ejemplo *ifOutOctets* o *IfOutErrors*.

A continuación procedemos a detallar el procedimiento para definir un umbral para el objeto de la MIB *IfOutOctets*, el cual nos indica el número de octetos que transmite la interfase de red de un dispositivo, información que nos puede ser de utilidad para medir el tráfico de datos generado por la interfase de red de cualquier elemento de la compañía Maint, este umbral se probó sobre la máquina de dirección IP 128.128.19.19, la cual es el Servidor de Desarrollo de la compañía Maint. Este procedimiento puede ser empleado para definir otro tipo de umbrales que involucren otros objetos de la MIB.

1. Se selecciona en el submapa el elemento de red que será analizado, en este caso el servidor de desarrollo de la compañía Maint.

2. Luego para abrir la ventana de configuración de umbrales se escoge del *Menú Options* la alternaniva *Data collection & thresholds: SNMP*, como se muestra en la *Figura 5.9.*

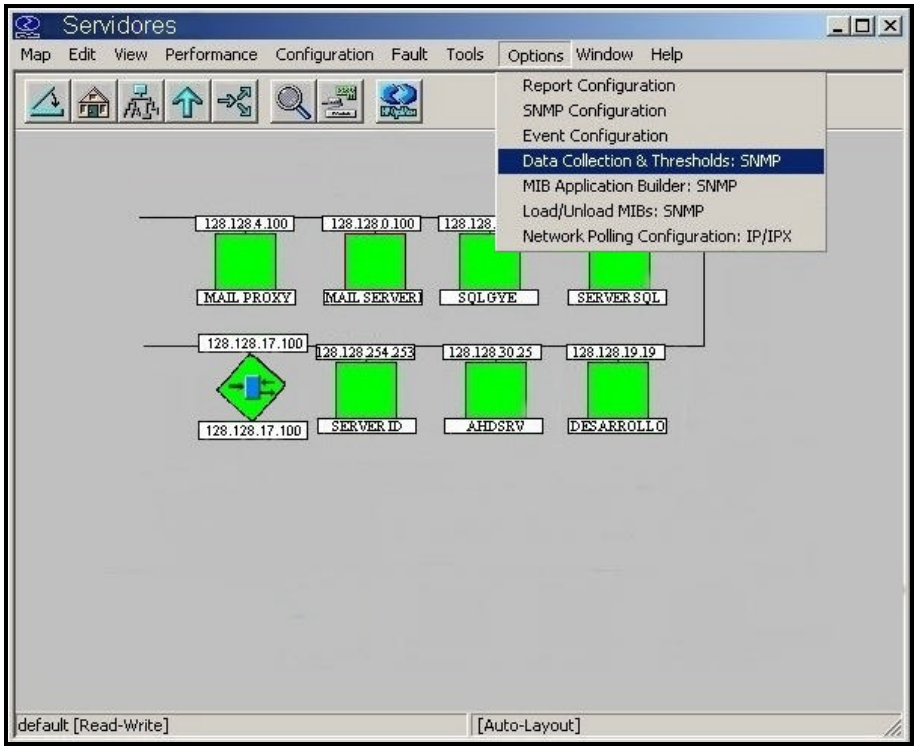

Figura 5.9 Método para abrir la ventana de configuración de umbrales.

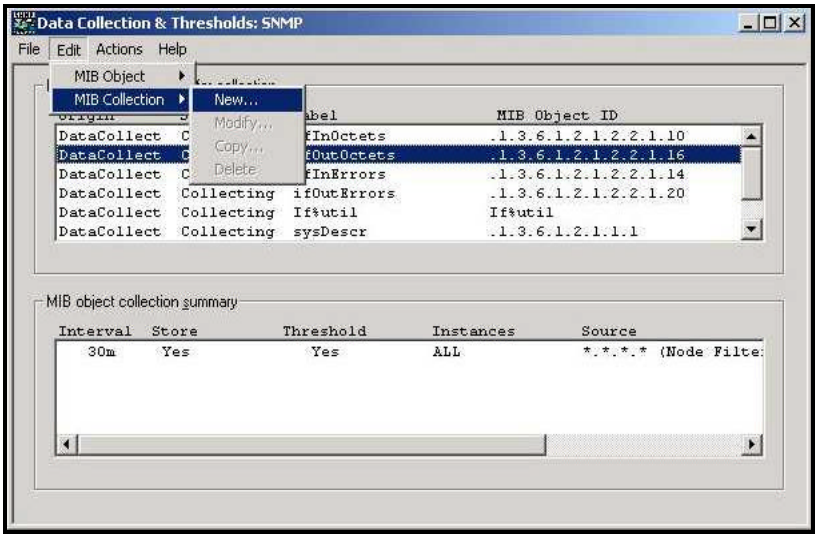

Figura 5.10 Ventana para seleccionar la recolección de datos.

3. A continuación aparece la ventana que se observa en la *Figura 5.10*, se hace click en la línea en la que aparece el objeto de la MIB, *ifOutOctets,* y cuando esté seleccionado, se escoge del *Menú Edit* la opción *MIB Collection* y luego *New*.

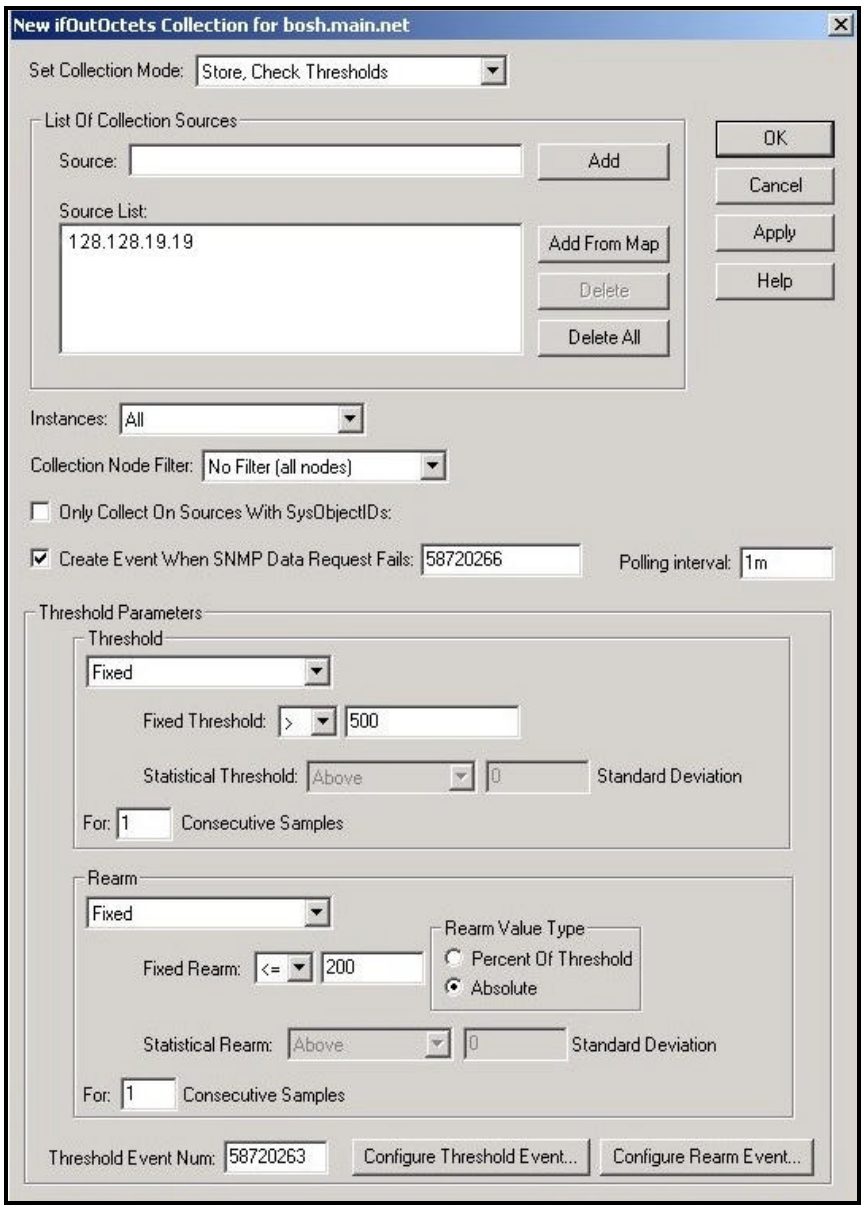

Figura 5.11 Cuadro de diálogo para definir umbrales.

4. En la ventana de diálogo para definir umbrales, *Figura 5.11*, se selecciona *Add from map*, con lo que deberá aparecer el elemento de red anteriormente seleccionado del mapa, es decir el servidor de Desarrollo de la compañía Maint cuya dirección IP es 128.128.19.19. Se escoge también un intervalo de recogida de datos de por ejemplo 1 minuto (1m) y como modo de recogida (Collection Mode) *Store, check thresholds*, esto hace que los campos *Threshold* y *Rearm* de la ventana estén disponibles.

   En el campo *Threshold* se introduce el valor de por ejemplo 500, que cuando se exceda, provocará que se envíe una alarma al Visor de Alarmas. El campo *Rearm* indica cuándo se considera que el dispositivo ha vuelto a un estado no crítico, se pone por ejemplo el valor de 200, esto también provocará que se envíe una alarma al Visor de Alarmas.

   Se acepta la configuración y se vuelve a la ventana de Data collection & thresholds, *Figura 5.10,* se debe guardar siempre la configuración de Data Collection & Threshold para activar los cambios.

5. Una vez que configuramos el umbral para el objeto de la MIB *IfOutOctets* del servidor de Desarrollo de la compañía Maint,

verificamos el funcionamiento de éste realizando un FTP anónimo al servidor mencionado y haciendo una operación GET sobre alguno de sus ficheros disponibles.

Tal como se muestra en la *Figura 5.12*, hemos obtenido los eventos *Threshold* y *Rearm* asociados a la máquina cuya dirección IP es 128.128.19.19 y que representan que se ha trabajado fuera de los límites definidos anteriormente.

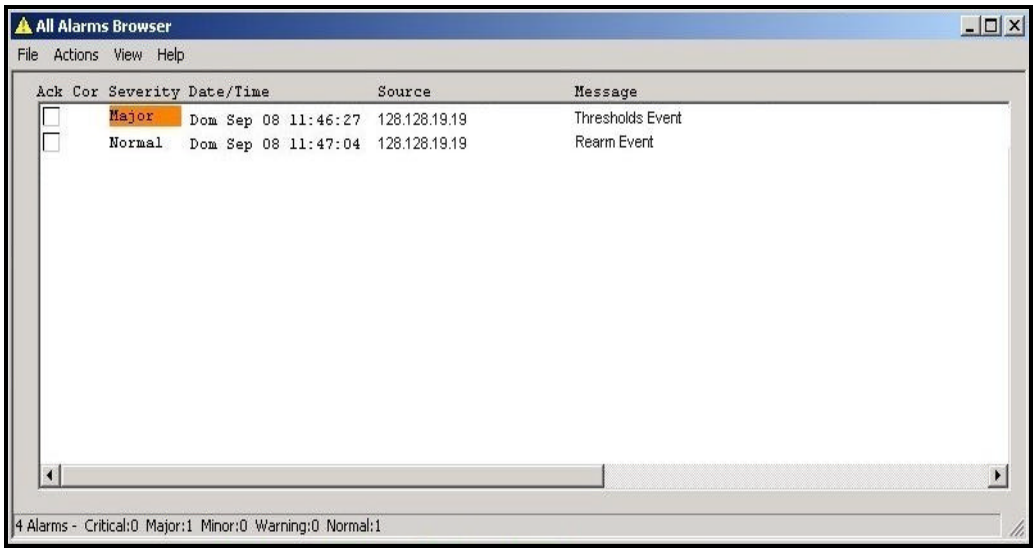

Figura 5.12 Visor de alarmas con los eventos Threshold y *Rearm.*

5.1.3 Correlación de eventos.

Como mencionamos en el Capítulo 3, el Servicio de Correlación de Eventos del Hp OpenView Network Node Manager nos permite cambiar un conjunto de eventos redundantes generados en

determinadas situaciones, por otros que nos den una mejor idea del estado de la red LAN de la compañía Maint.

Un ejemplo típico de esta aplicación es la caída de un router. Dicho suceso provocará una alarma de caída asociada al router, pero también provocará una alarma cada uno de los nodos que son alcanzables a través de dicho router.

Es claro que el suceso más importante es el primero, y es el que da lugar a los siguientes, aunque los nodos en cuestión no hayan caído. Otra aplicación sería cuando hay previstas tareas de mantenimiento que suponen que algunos nodos estarán fuera de servicio en intervalos de tiempo previamente conocidos.

Esta situación va a provocar dos alarmas: la de nodo caído (down) al empezar el mantenimiento, y la de nodo operativo (up) al terminar el mantenimiento.

Es posible instruir al Hp OpenView Network Node Manager para que sustituya esas alarmas por una que identifique esa tarea de mantenimiento mediante una alarma de *Scheduled Maintenance (Mantenimiento Planificado)*.

Un ejemplo claro se muestra en la *Figura 5.13*, en la cual ocurren dos situaciones, la primera un mantenimiento planificado al router A, en este caso se lo está moviendo a un nuevo rack, y la segunda una caída de un nodo (router B). En la parte **superior** de la figura **no** se han correlacionado los eventos por lo que vemos en el Visor de Alarmas tres alarmas asociadas a tales eventos.

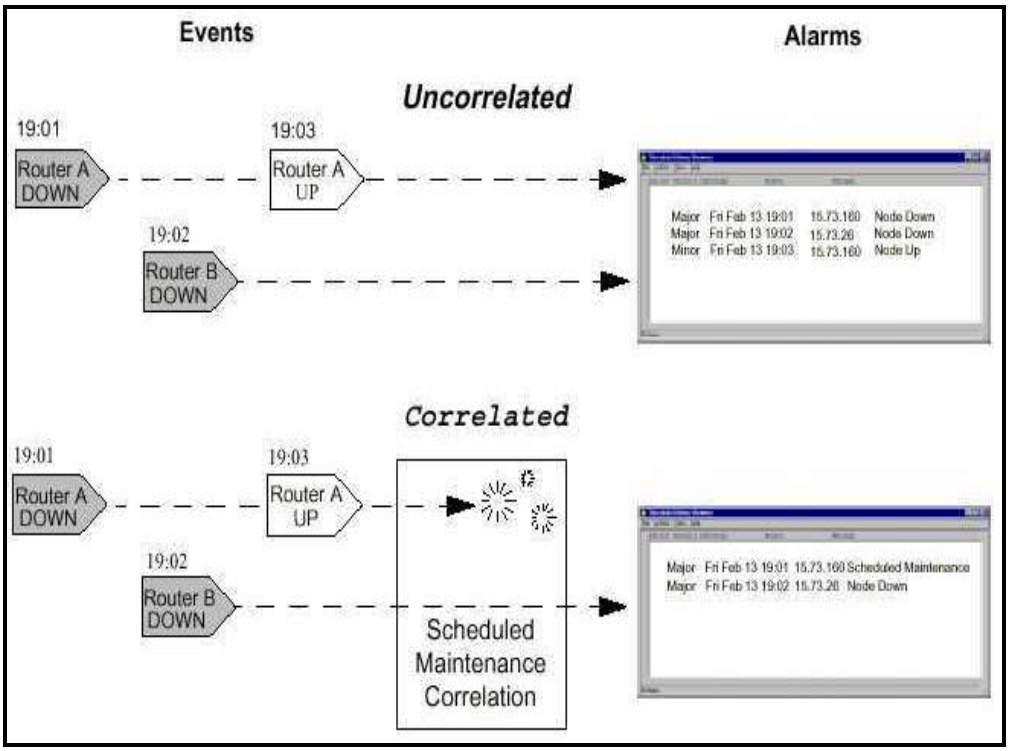

Figura 5.13 Eventos correlacionados y no correlacionados.

Mediante la correlación “Scheduled Maintenance” podemos configurar una alarma que notifique el mantenimiento y suprimir todos los demás eventos generados por este dispositivo durante el período de

mantenimiento, tal como se aprecia en la parte **inferior** de la *Figura 5.13*. Al apagarse el router A durante el período de mantenimiento, la correlación suprime ambos eventos del router A, sin embargo el evento del router B si es anunciado debido a que no se encuentra dentro de las especificaciones del mantenimiento. Como resultado se obtienen dos eventos con un nivel de confianza más alto, ayudándonos de esta manera a prestar una mejor atención a las alarmas que lo requieren.

A continuación mostramos las correlaciones que nos brinda el Hp OpenView Network Node Manager y que pueden ser de gran ayuda.

- **Correlación "Connector Down"**

  Esta correlación puede prevenir una tormenta de eventos cuando un router o algún otro equipo de conexión deja de funcionar, en este caso el Hp OpenView Network Node Manager puede determinar automáticamente:

  - El equipo que se encuentra con problemas.

  - Que otros dispositivos de red han sido impactados por esta falla. Es decir qué equipos son ahora inaccesibles para la estación de gestión.

- **Correlación “Scheduled Maintenance”**

  Como se mencionó anteriormente los equipos de red suelen ser sometidos regularmente a algún tipo de mantenimiento, para lo cual son apagados, esto significaría un buen número de alarmas innecesarias que serían generadas debido a este evento durante el mantenimiento. Pero al configurar la correlación “Scheduled Maintenance” podemos especificar el día, la hora y el tiempo que tomará el mantenimiento, evitando de esta manera llenarnos de alarmas que no deben ser anunciadas.

- **Correlación “Repeated Event”**

  Esta correlación permite que múltiples alarmas que están asociadas a un solo evento puedan ser reemplazadas por una sola alarma.

- **Correlación “Par Wise”**

  Esta correlación empareja un evento (evento padre) a uno o más eventos (eventos hijos) que ocurren de una misma fuente o nodo.

No podemos mostrar la utilización de esta herramienta en la red LAN de la compañía Maint, porque ésta solo se habilita al poseer la

licencia del software, pero debido a su importancia en la gestión la hemos mencionado.

5.1.4 Control de alarmas.

Como mencionamos en el Capitulo 3, el Hp OpenView Network Node Manager nos permite tener un control total sobre todas las alarmas que se producen en la red LAN de la compañía Maint, basta tan solo seleccionar el Visor de alarmas para conocer si ha ocurrido algún evento que pueda perjudicar el buen funcionamiento de la red LAN.

De esta manera tenemos la oportunidad de gestionar las alarmas que en determinado momento se activen al producirse cualquier evento en la red LAN de la compañía Maint, por medio del filtrado de alarmas lo cual es una herramienta muy útil que nos brinda el Visor de Alarmas.

5.1.4.1 Filtrado de Alarmas.

Con el fin de ayudar a clasificar la presentación, en el caso de que las alarmas presentadas sean muy numerosas el Visor de alarmas nos permite filtrar las alarmas producidas por la red LAN de la compañía Maint según varios criterios:

- Severidad.
- Dirección IP del objeto que ha fallado.

- Tipo de alarma.
- Mensaje.
- Intervalo de tiempo en el que se ha producido.

Por ejemplo: si queremos determinar las alarmas de severidad menor que se han producido en la red LAN de la compañía Maint procedemos a realizar un filtro de la siguiente manera:

1. Del Visor de alarmas se escoge la opción *Set Filters* del Menú *View*, como se muestra en la *Figura 5.14.*

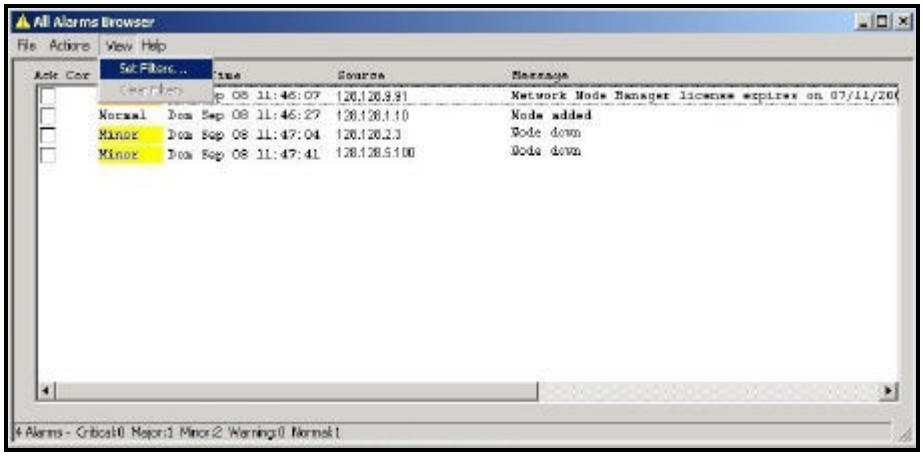

Figura 5.14 Método para definir filtros de Alarmas.

2. A continuación aparece la ventana que se observa en la *Figura 5.15,* en la cual se especifica el filtro, en este caso para ver sólo las alarmas de severidad menor que han ocurrido seleccionamos el casillero *Minor* y luego presionamos *Aceptar*. Podemos observar también en esta figura que es

posible filtrar las alarmas según su severidad, período de tiempo o según el dispositivo de red que ha provocado el fallo.

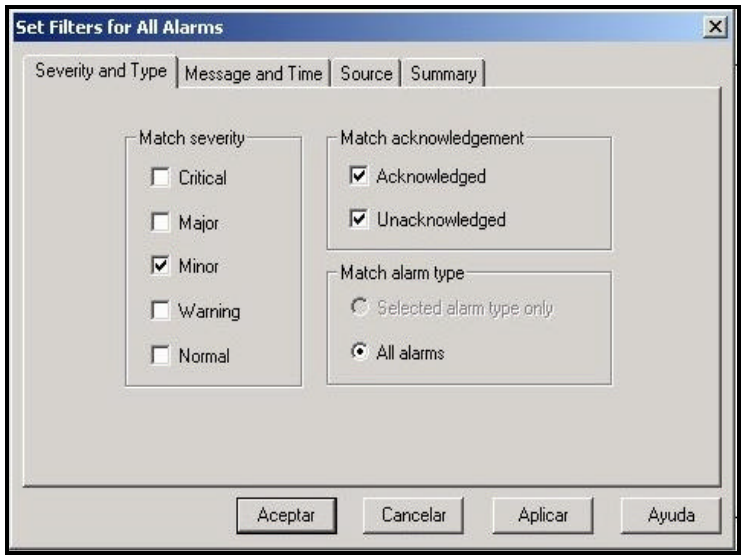

Figura 5.15 Ventana para especificar el filtro de Alarmas.

De esta manera obtenemos solo las alarmas de severidad menor tal como se muestra en la *Figura 5.16.*

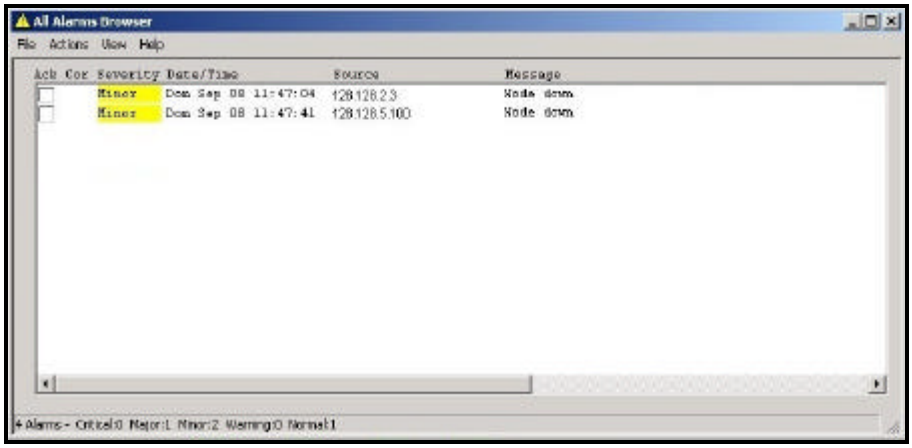

Figura 5.16 Listado de alarmas de severidad menor.

5.2 Gestión de Rendimiento.

Esta área comprende el conjunto de funciones destinadas a evaluar el comportamiento de equipos de telecomunicaciones e informar al respecto, midiendo el desempeño de la red como puede ser según el porcentaje de utilización, tasa de error, y el tiempo de respuesta, a través de la recolección y análisis de datos de la red.

Mediante la medida y gestión del rendimiento se puede asegurar que la capacidad y prestaciones de la red de telecomunicaciones corresponden a las necesidades de los usuarios.

Fundamentalmente la gestión de rendimiento consta de dos categorías funcionales: Monitorización y Control. La Monitorización realiza el seguimiento de las actividades de la red. La función de Control permite realizar los ajustes necesarios para mejorar el rendimiento.

La gestión de rendimiento debe monitorizar muchos recursos para conseguir información y determinar el nivel de operación de la red. Con las estadísticas sobre el rendimiento obtenidas se pueden predecir cuellos de botella antes que causen problemas a los usuarios, seguidamente se pueden tomar las acciones correctivas apropiadas como por ejemplo balancear o distribuir el tráfico.

Calcular como poner a punto el desempeño de una red puede ser un gran desafío. Para ayudar en esta tarea, Network Node Manager recoge información de la red que puede ser analizada para saber su tendencia.

A continuación los rasgos de la información que recolecta Network Node Manager.

- Monitorea automáticamente el estado de la red.

- Recopila información histórica de los objetos de la MIB y de los eventos, guardando los datos para el análisis de sus tendencias.

- Permite establecer umbrales de trabajo basados en los datos históricos recolectados.

- Diagnostica fallas y problemas en el desempeño en la red analizando sus tendencias en el tiempo, permitiendo personalizar y automatizar el monitoreo de la red y la respuesta de la estación de gestión a los eventos.

Las funciones que nos brinda la Gestión de Rendimiento son las siguientes:

- Definición automática de acciones.
- Recogida automática de datos.
- Visualización de los objetos de la MIB.

5.2.1 Definición automática de acciones.

Una de las características del Hp OpenView Network Node Manager es que nos permite definir acciones automáticas que se llevan a cabo si ocurre determinado evento. Para definir las acciones automáticas que tendrán lugar si ocurre un fallo en la red LAN de la compañía Maint se siguen los siguientes pasos:

1. Se abre la ventana de configuración de eventos desde la ventana del visor de alarmas seleccionando la opción *Event Configuration* del *Menú Actions*; o desde cualquier submapa seleccionando del *Menú Options*, la alternativa *Event Configuration*.

2. Luego en la parte superior de la ventana, se selecciona la empresa que proporciona la MIB por ejemplo OpenView y en la parte inferior se especifica el evento SNMP, en este caso hemos escogido *OV_Connection_Down*, se selecciona *Copy* o *Modify Event* del *Menú Edit* tal como se muestra en la *Figura 5.17.*

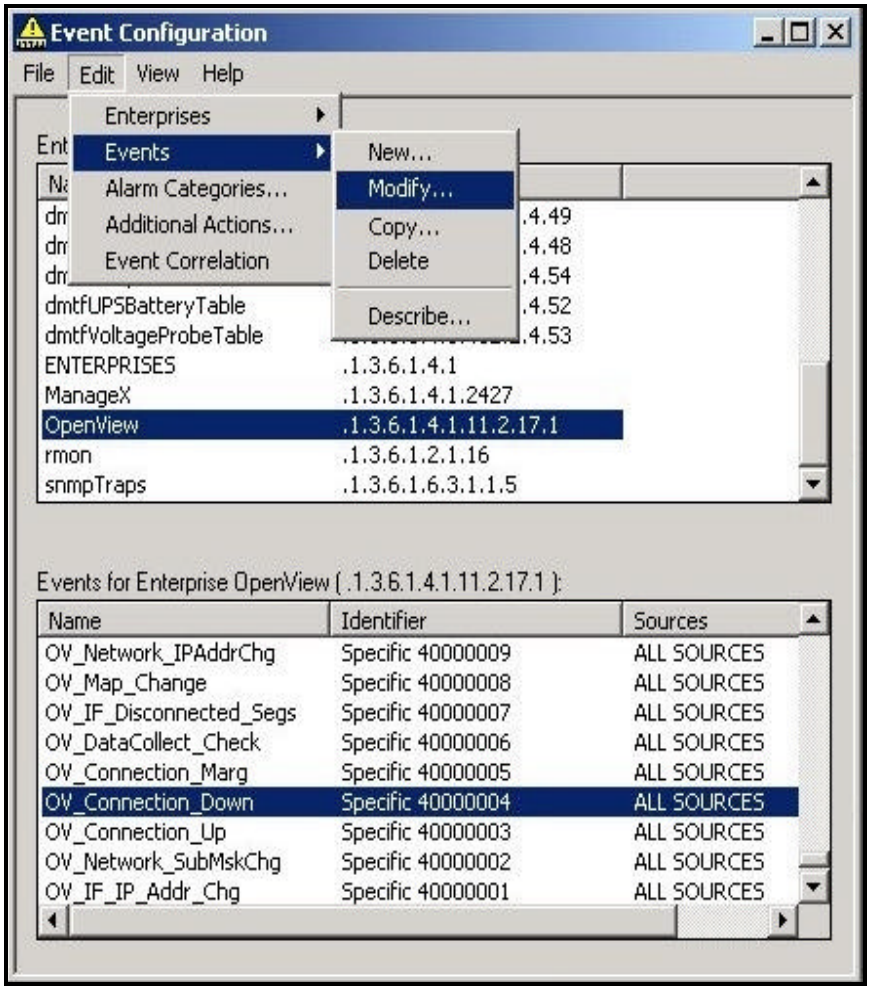

Figura 5.17 Selección del evento OV_Connection_Down.

3. A continuación se selecciona la etiqueta *Actions* para editar las acciones que se llevarán a cabo cuando ocurra el evento. Para que el Hp OpenView Network Node Manager tome una acción automática si el evento ocurre se debe poner las instrucciones dentro del campo *Command for Automatic Actions*.

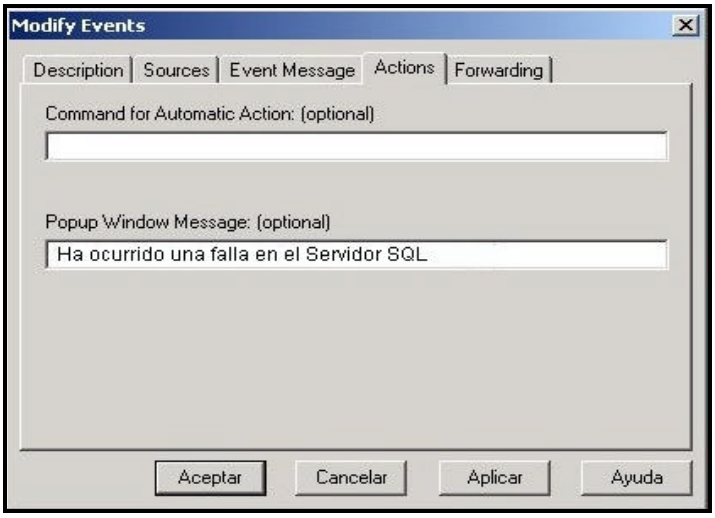

Figura 5.18 Ventana para definir acciones Automáticas.

En este caso se utilizó el campo *Popup Window Message* tal como se observa en la *Figura 5.18* para que, en el caso de que ocurra el evento se mande el mensaje a través del servicio de mensajería instantánea de Windows NT a la estación de gestión.

Esta acción es muy útil cuando por ejemplo, se tiene cerrada la interfaz gráfica del Hp OpenView Network Node Manager por lo que no se puede apreciar el fallo en el mapa que representa la red LAN de la compañía Maint.

4. Luego se selecciona la etiqueta *Sources* para especificar el o los dispositivos de la red LAN de la compañía Maint que van a formar parte del evento, especificando el nombre de host o

la dirección IP, por ejemplo el Servidor SQL de la red LAN de la compañía Maint cuya dirección IP es 128.128.2.100, como se aprecia en la *Figura 5.19*.

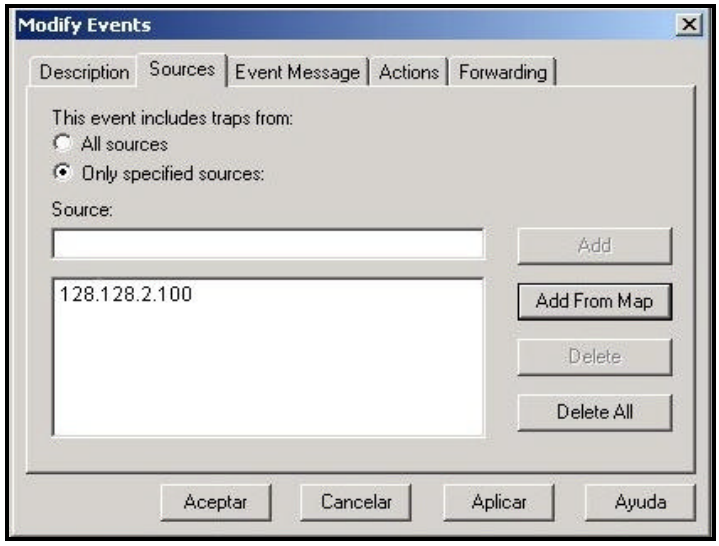

Figura 5.19 Ventana de especificaciones del evento OV_Connection_Down.

Una vez concluida la configuración del evento *OV_Connection_Down*, se presiona Aceptar y se graba el evento mediante la opción *Save* del *Menú File* para que los cambios tengan efecto.

5.2.2 Recogida automática de datos.

Con esta posibilidad podemos pedir que el Hp OpenView Network Node Manager se encargue de obtener datos de cualquier objeto de

la red LAN de la compañía Maint, con una cierta periodicidad y que los almacene o los presente de forma gráfica.

Por ejemplo para saber cual es el número de errores producido por la interfase del router Cisco 1750 de la red LAN de la compañía Maint, se puede interrogar al objeto de la MIB *ifOutErrors* de la siguiente manera:

1. Se selecciona en el submapa el símbolo que representa al router Cisco 1750 de la red LAN de la compañía Maint.

2. A continuación del *Menú Options* se escoge *Data collection & thresholds: SNMP*, para abrir la ventana de configuración para la recogida automática de datos.

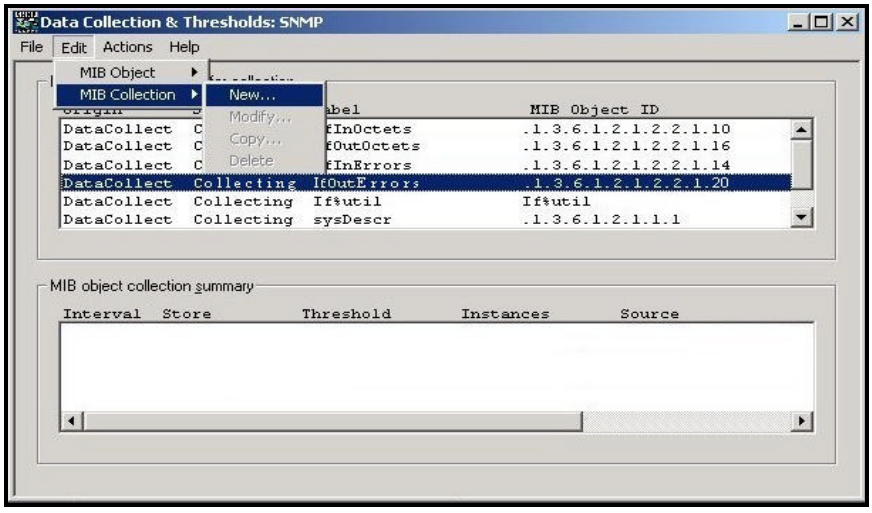

Figura 5.20 Selección del objeto ifOutErrors para obtener sus datos automáticamente.

3. Se hace click en la línea en la que aparece el objeto de la MIB *ifOutErrors* y cuando esté seleccionada, se escoge del *Menú Edit* la opción *MIB Collection* y luego New, como se muestra en la *Figura 5.20*.

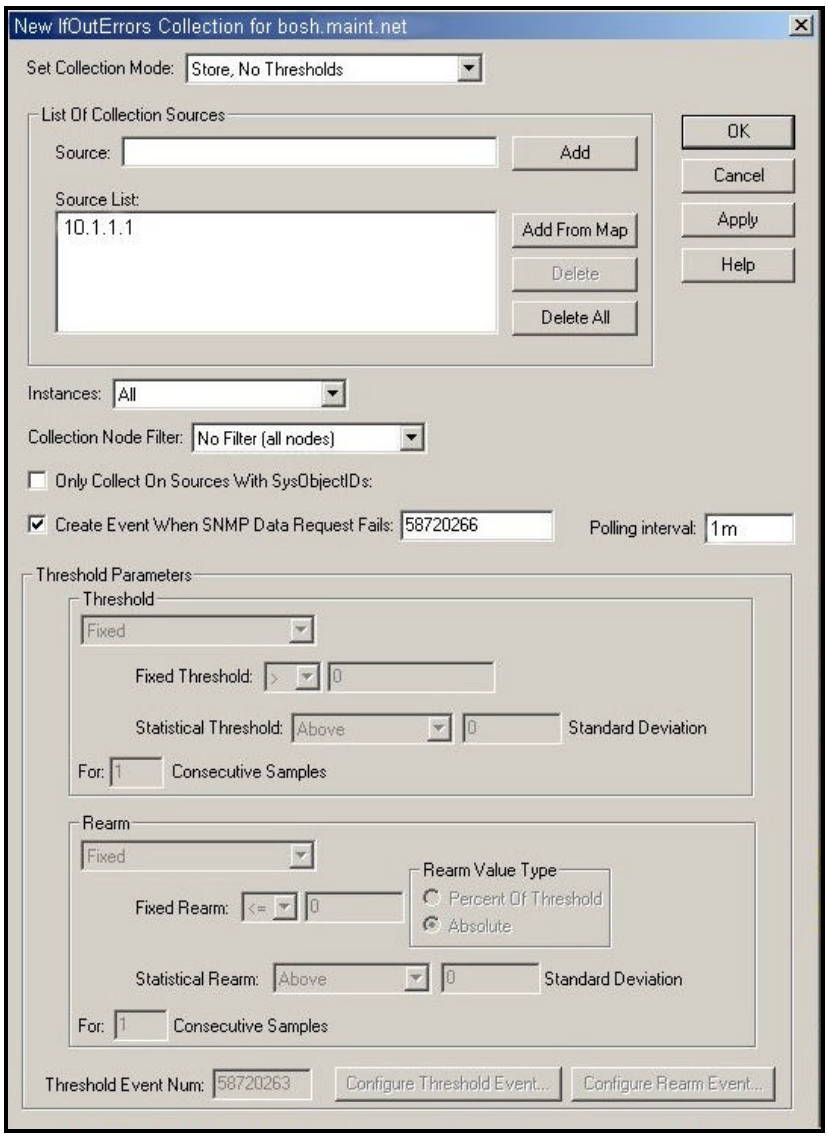

Figura 5.21 Ventana para configurar la recogida automática de datos.

4. En la ventana de diálogo que aparece a continuación, *Figura 5.21*, se selecciona Add from map, con lo que deberá aparecer la dirección IP del router Cisco 1750 la cual es 10.1.1.1. A continuación se escoge también un intervalo de recogida de datos por ejemplo de 1 minuto (1m) y como modo de recogida (Collection Mode) *Store, No Thresholds*.

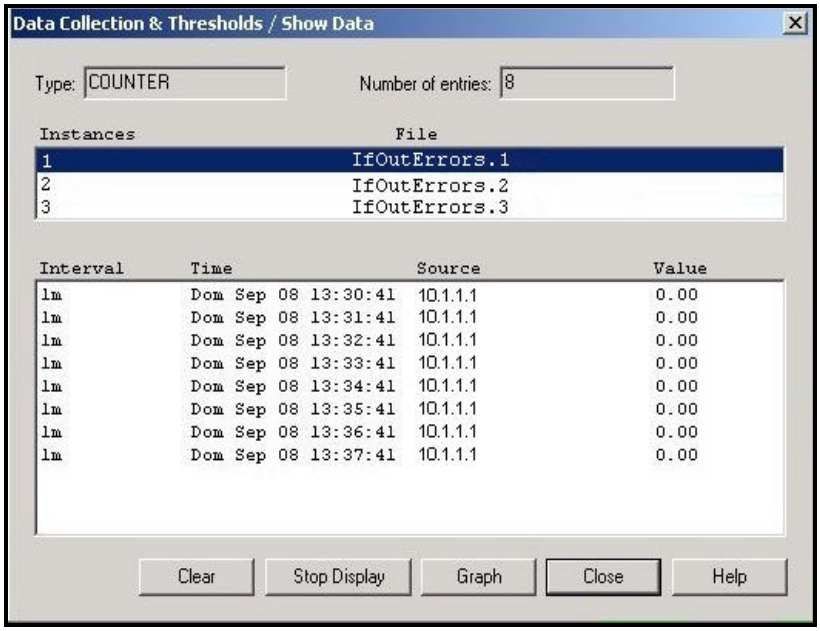

Figura 5.22 Método para graficar los datos obtenidos del Router Cisco 1750.

5. Se acepta la configuración y se vuelve a la ventana de *Data collection & thresholds*, *Figura 5.20*, y se escoge del *Menú Actions* la opción *Show data*, y en el cuadro que aparece se selecciona con el mouse la instancia de la interfaz

correspondiente, en este caso hemos escogido *ifOutErrors.1* y luego se selecciona *Graph*, tal como se muestra en la *Figura 5.22*.

Mediante este procedimiento hemos obtenido la gráfica que se muestra en la *Figura 5.23*, donde se observa que el número de errores producidos por la interfaz del router Cisco 1750 de la compañía Maint es despreciable.

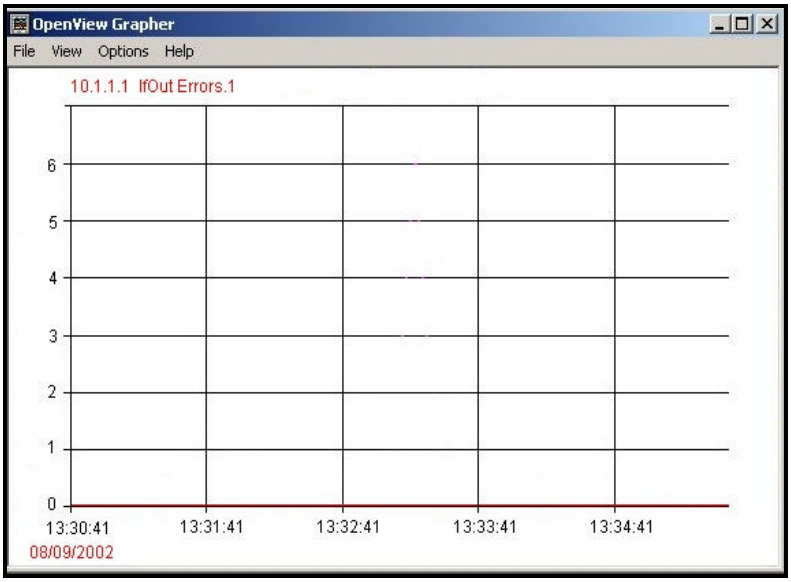

Figura 5.23 Número de errores producidos por el Router 1750.

5.2.3 Visualización de los objetos de la MIB.

Esta herramienta del Hp OpenView Network Node Manager nos permite examinar y consultar los valores de cualquier objeto de la MIB, de forma interactiva. Para navegar en el Visor de la MIB basta

con expandir o contraer el árbol de la MIB y seleccionar cualquier objeto de la MIB e iniciar una consulta.

Por ejemplo si deseamos obtener la información del objeto de la MIB ***sysDescr***, el cual nos muestra el nombre completo, la versión del software, el tipo de hardware, el sistema operativo y el software de red, de la máquina cuya dirección IP es 128.128.9.91, se procede de la siguiente manera:

1. Se selecciona en el submapa de la red LAN de Maint la máquina que deseamos interrogar (128.128.9.91).

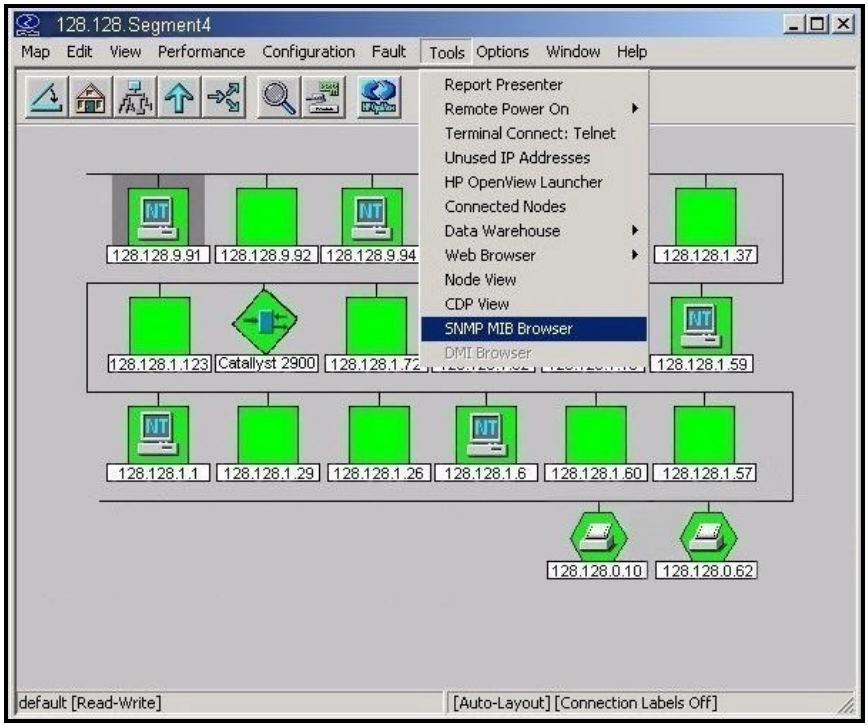

Figura 5.24 Procedimiento para abrir el Visor de la MIB.

2. Se abre el visor de la MIB seleccionando del *Menú Tools* la opción *MIB browser* tal como se observa en la *Figura 5.24*.

3. En el árbol de la MIB se busca *sysDescr* tal como se aprecia en la *Figura 5.25* y a continuación se presiona *Start Query*, para comenzar la interrogación del objeto.

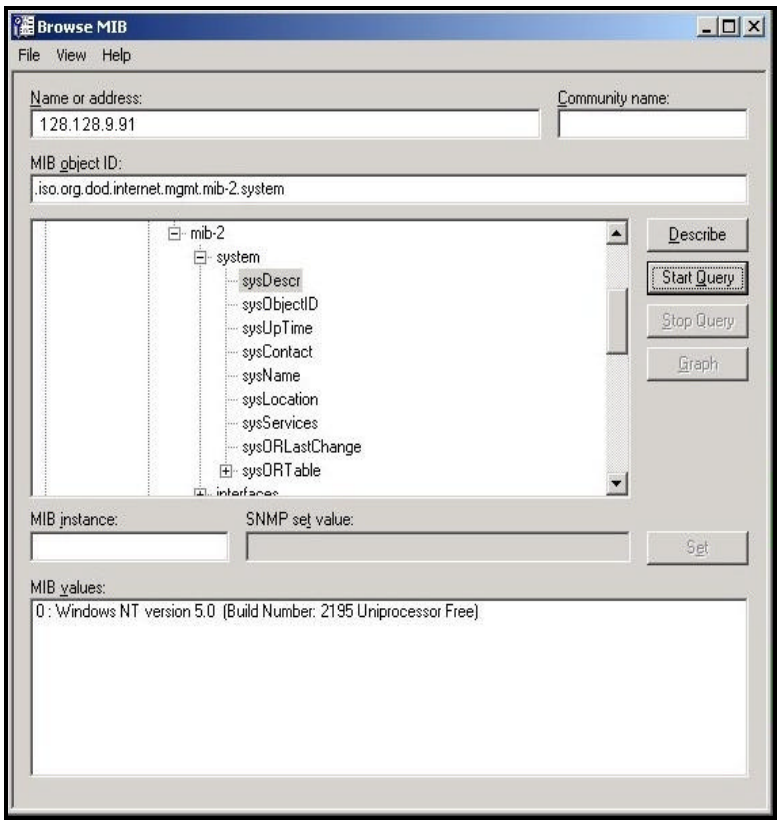

Figura 5.25 Información del objeto sysDescr obtenida del visor de la MIB.

Tal como se aprecia en la Figura 5.25 parte inferior (*MIB values*), hemos obtenido mediante la interrogación del objeto *sysDescr* de la

máquina con dirección IP 128.128.9.91, el sistema operativo, su versión e información relativa al hardware.

Mediante el Visor de la MIB podemos interrogar a cada uno de los objetos de los diferentes grupos que componen la MIB y que fueron explicados en el Capítulo 1.

5.3 Gestión de configuración.

La gestión de configuración está relacionada por una parte, con la inicialización de la red y la desconexión ordenada de la misma o parte de ella, y por otro lado del mantenimiento, la adición de componentes y la actualización de las relaciones entre los componentes.

Esta función es responsable de encontrar y preparar los dispositivos de la red para poder controlar el comportamiento de ésta. El Hp OpenView Network Node Manager nos ayuda a mantener un registro de la información de configuración permitiéndonos lo siguiente:

- Guardar información de configuraciones críticas tales como routers y switches.

- Llevar un inventario de los dispositivos de la red.

Las acciones que nos brinda la Gestión de Configuración son las siguientes:

- Visualización de las propiedades de configuración de la red.
- Personalización de mapas.

5.3.1 Visualización de las propiedades de configuración de la red.

Como ya hemos mencionado anteriormente la característica más importante del Hp OpenView Network Node Manager es que permite ver toda la red LAN de la compañía Maint por medio de mapas, que nos muestran el estado de cada uno de los dispositivos que conforman la red. A continuación mostramos cada uno de los submapas que especifican la configuración de la red LAN de la compañía Maint en la ciudad de Guayaquil.

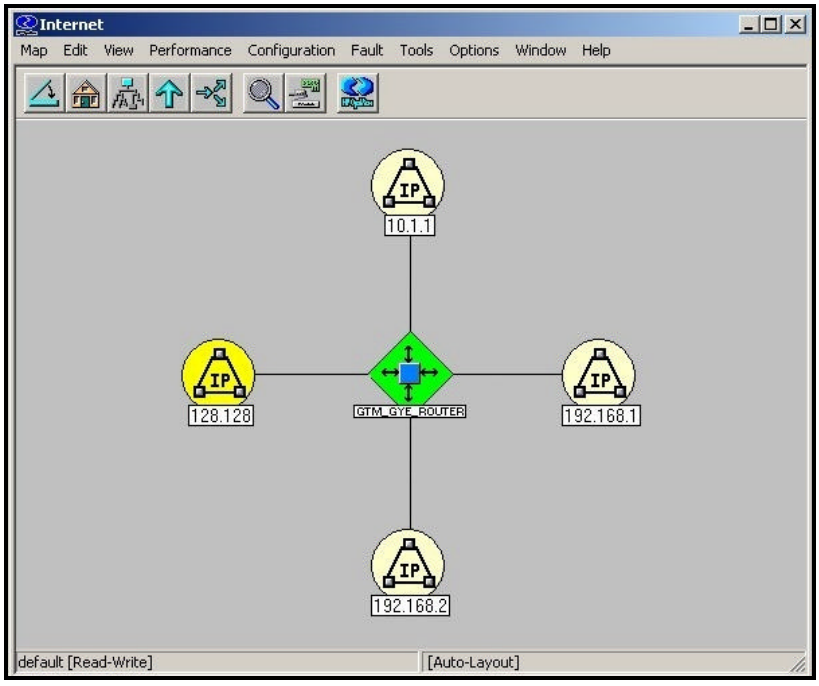

Figura 5.26 Mapa de la red IP de la compañía Maint.

La *Figura 5.26*, muestra cuatro redes IP siendo la red 128.128.0.0 la que pertenece a la red LAN de la compañía Maint en la ciudad de Guayaquil.

Al ingresar a la red IP 128.128.0.0 se obtiene la *Figura 5.27* en la que se puede observar como se encuentra configurada la red LAN de la compañía Maint.

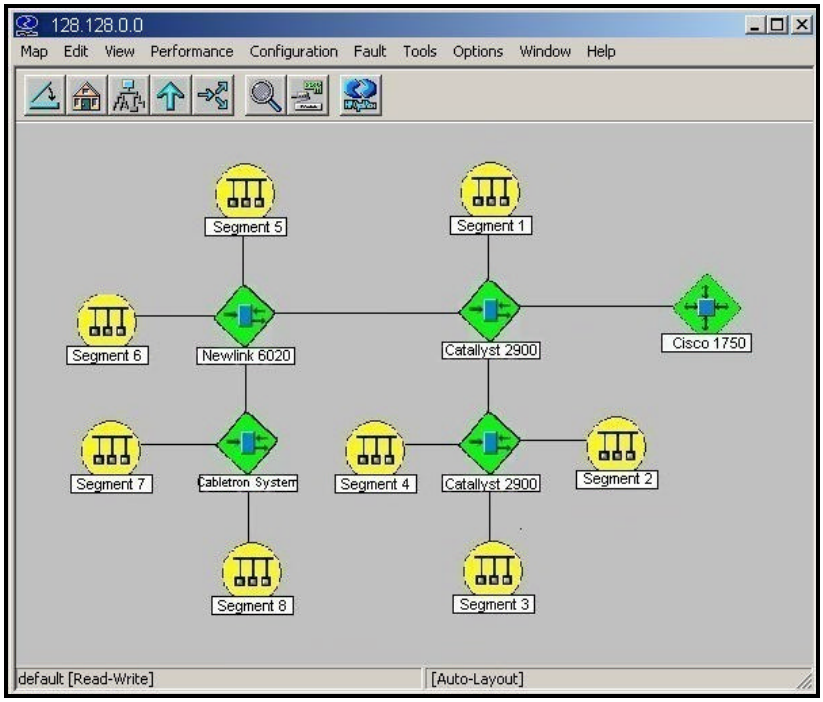

Figura 5.27 Segmentos que forman la red LAN de Maint.

Haciendo doble click en cada uno de los símbolos que representan los diferentes segmentos que forman la red LAN de la compañía Maint en la ciudad de Guayaquil, podremos ver los distintos nodos que

componen cada uno de los segmentos, tal como se muestra en las *Figuras 5.28 a 5.35.*

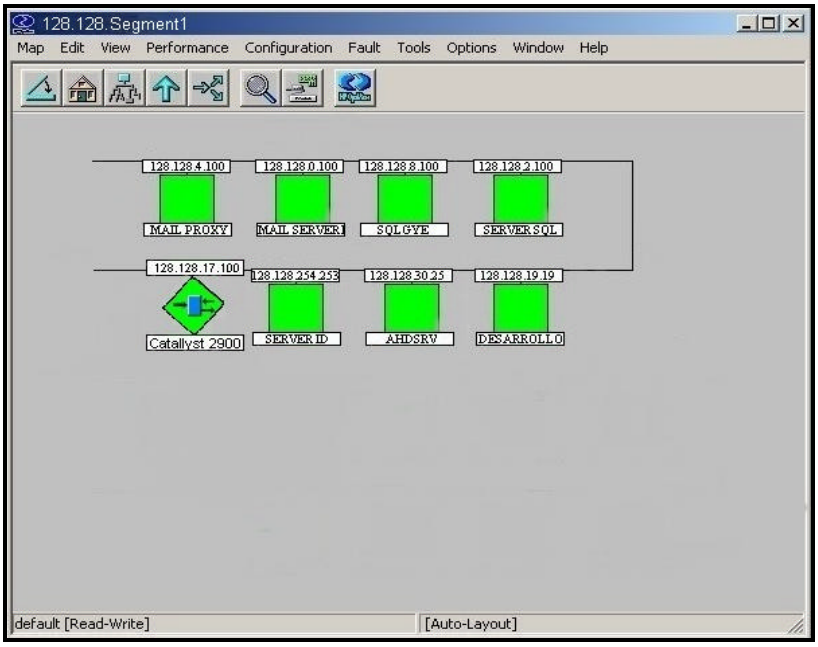

Figura 5.28 Nodos del Segmento 1 de la red LAN de Maint.

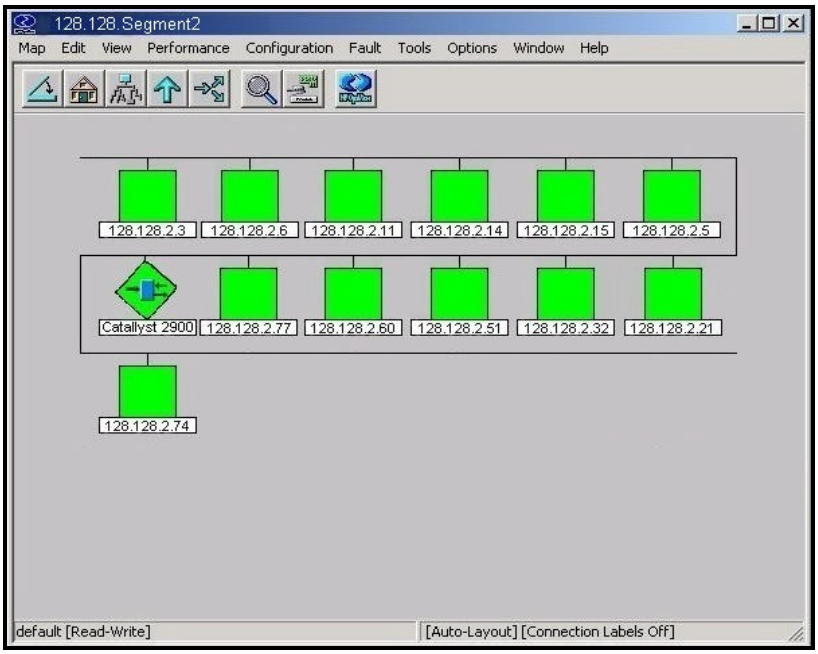

Figura 5.29 Nodos del Segmento 2 de la red LAN de Maint.

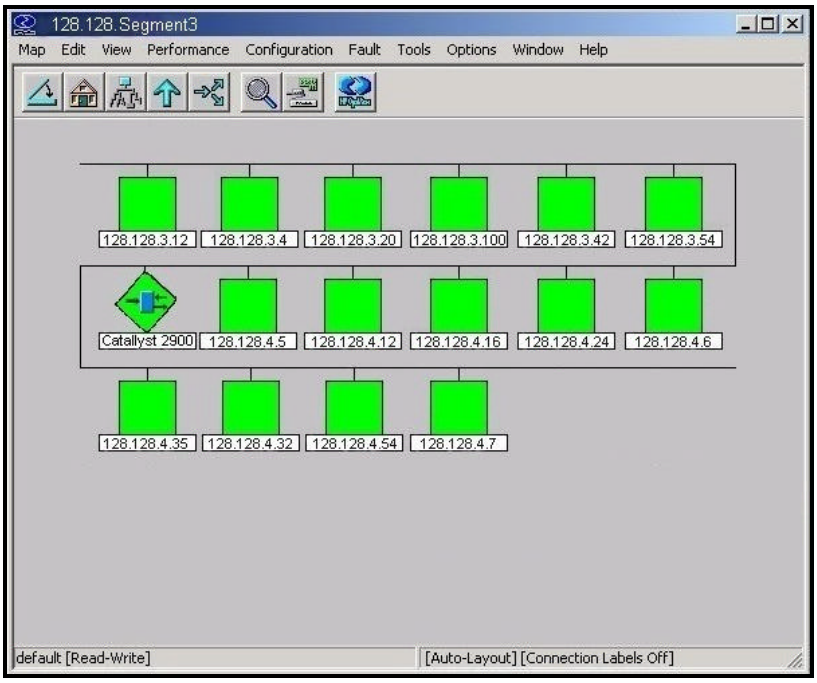

Figura 5.30 Nodos del Segmento 3 de la red LAN de Maint.

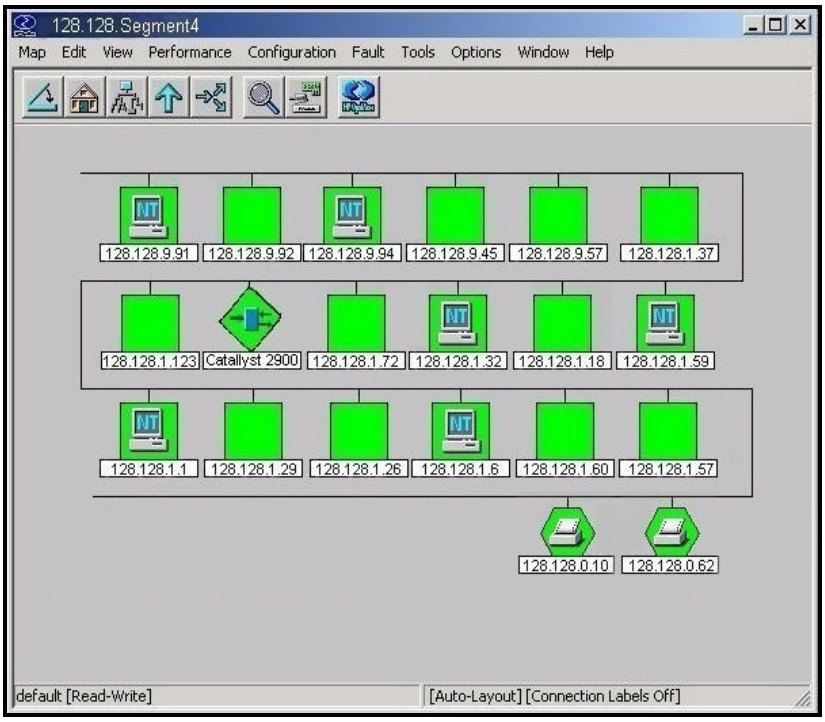

Figura 5.31 Nodos del Segmento 4 de la red de Maint.

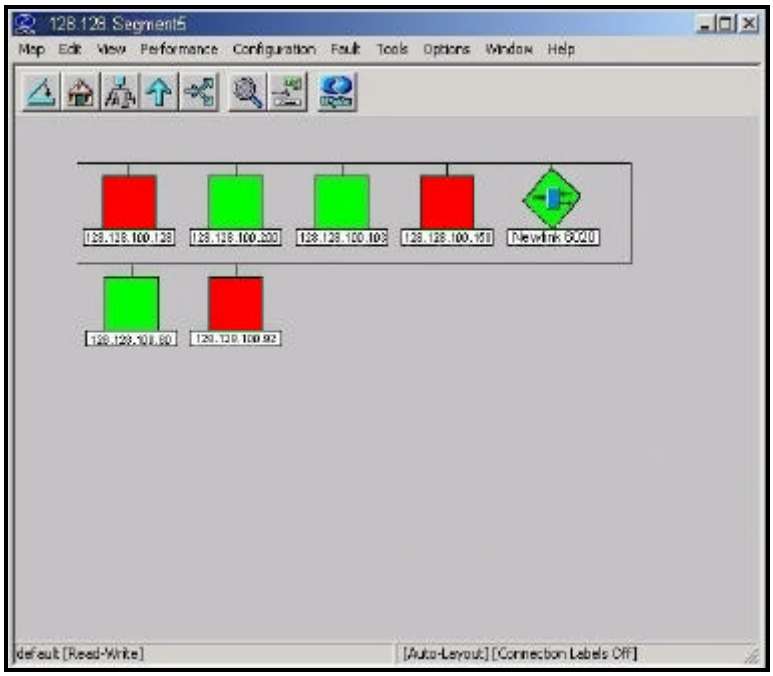

Figura 5.32 Nodos del Segmento 5 de la red de Maint.

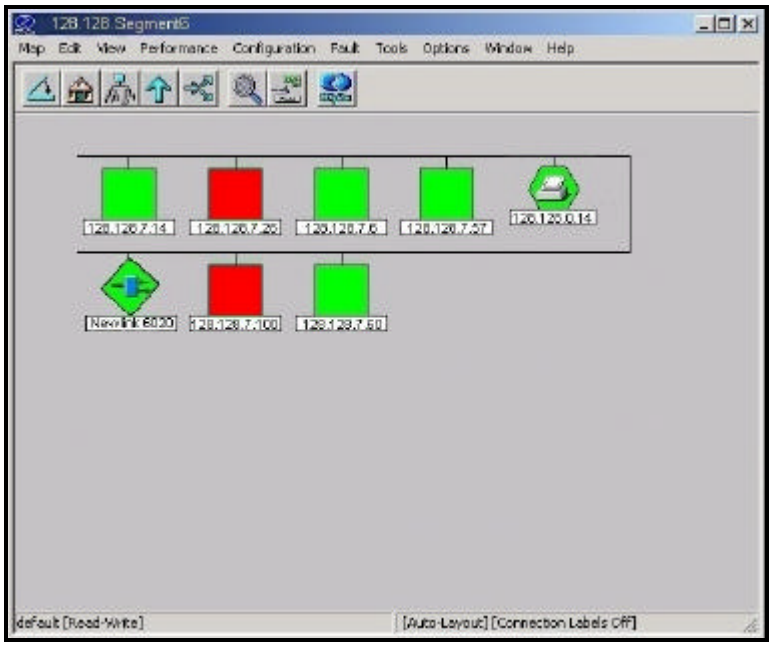

Figura 5.33 Nodos del Segmento 6 de la red de Maint.

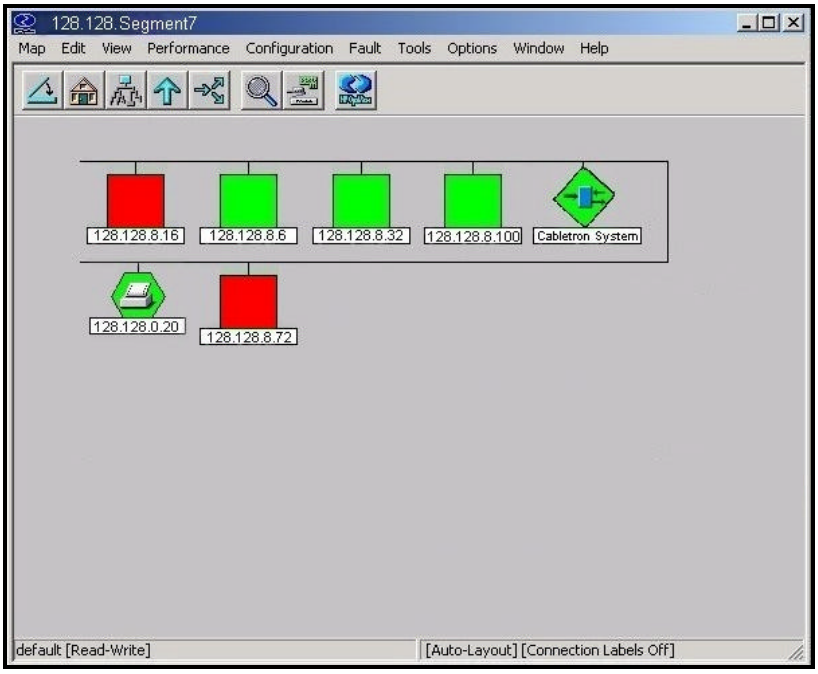

Figura 5.34 Nodos del Segmento 7 de la red de Maint.

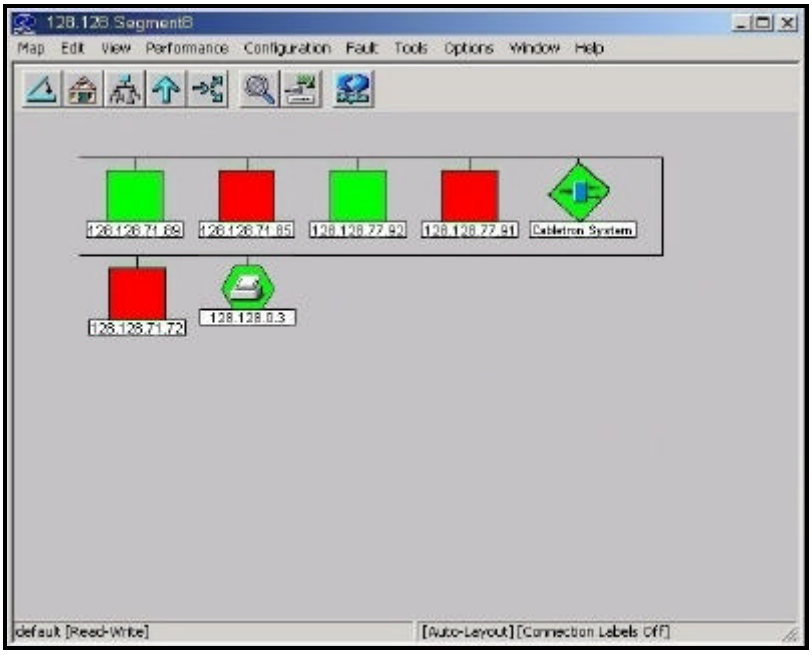

Figura 5.35 Nodos del Segmento 8 de la red de Maint.

Consideramos que la configuración actual de la red LAN de la compañía Maint es la más optima pues al encontrarse segmentada existe menor competencia por el medio y por consiguiente menor número de colisiones.

Se puede acceder rápidamente al servicio de información que describe la configuración de la red LAN de la compañía Maint. Los cuadros de diálogo que muestran las propiedades de los objetos pueden ayudarnos a determinar si todos los elementos se encuentran correctamente definidos en el mapa. El Hp OpenView Network Node Manager nos permite ver las propiedades de los objetos según:

- Descripción de un objeto red.
- Descripción de un objeto segmento.
- Descripción de un objeto nodo.
- Descripción de un objeto interfase.

5.3.1.1 Descripción de un objeto red.

Para saber las propiedades de configuración de la red LAN de la compañía Maint cuya dirección IP es 128.128.0.0, simplemente se selecciona en el submapa de la red el símbolo que la representa y luego se hace click con el botón derecho del mouse y después se

selecciona *Object Propertiers* y a continuación *IP Map*, tal como se muestra en la *Figura 5.36*.

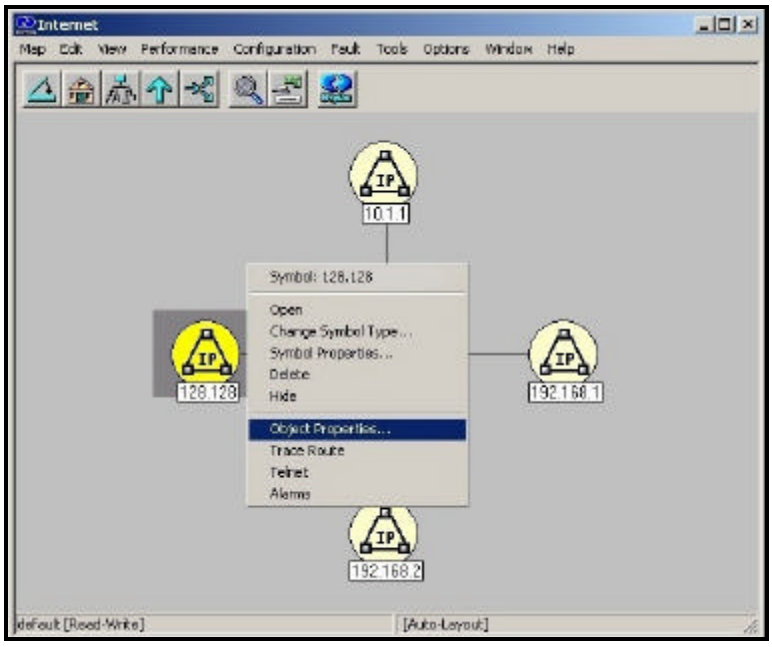

Figura 5.36 Método para obtener la descripción de la red LAN de la compañía Maint.

De esta forma obtendremos la siguiente información, tal como se muestra en la *Figura 5.37.*

- El nombre de la red tal como aparece en el mapa.
- La dirección de red.
- El estado de la red.
- Número de segmentos en la red.
- Número de nodos contenidos en la red.

- Cualquier mensaje de error o estado que pueda aparecer el campo de mensajes.

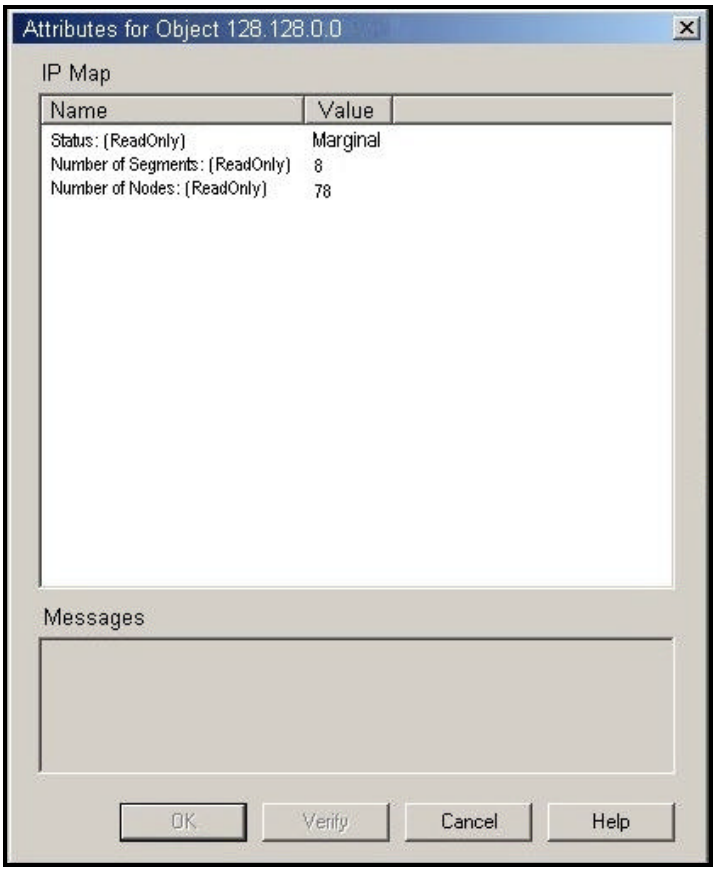

Figura 5.37 Descripción de la red LAN de la compañía Maint.

5.3.1.2 Descripción de un objeto segmento.

Para obtener la descripción de la configuración de cualquier segmento de red que conforma la red LAN de la compañía Maint se selecciona cualquier símbolo que represente cualquier segmento en el submapa, por ejemplo el Segmento 4 de la red

LAN de la compañía Maint y se hace click con el botón derecho del mouse y luego se selecciona *Object Propertiers* y después *IP Map*, tal como se aprecia en la *Figura 5.38.*

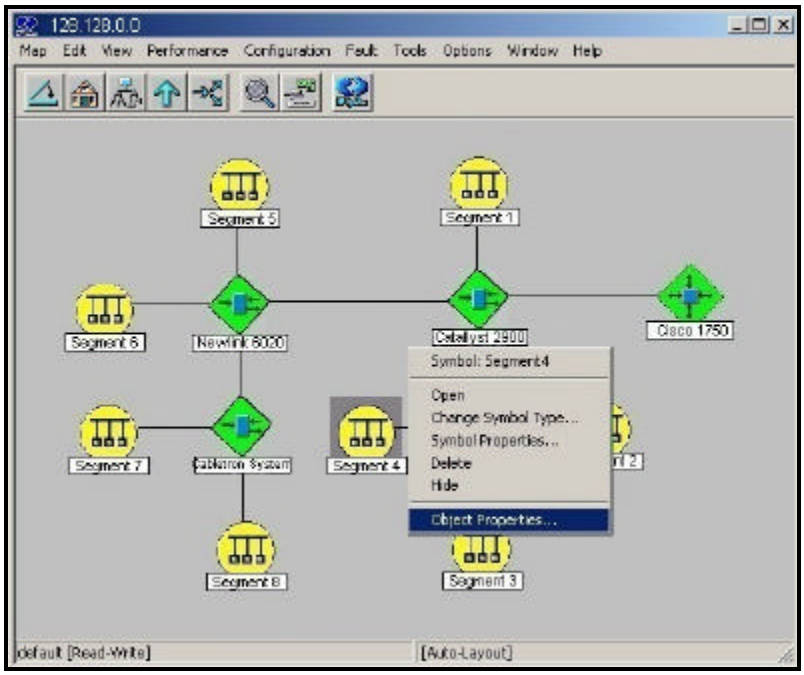

Figura 5.38 Método para obtener la descripción del Segmento 4 de la red LAN de Maint.

Por este procedimiento obtenemos la siguiente información, tal como vemos en la *Figura 5.39.*

- Estado del segmento.
- Número de nodos del segmento.

- Cualquier mensaje de error o estado que pueda aparecer el campo de mensajes.

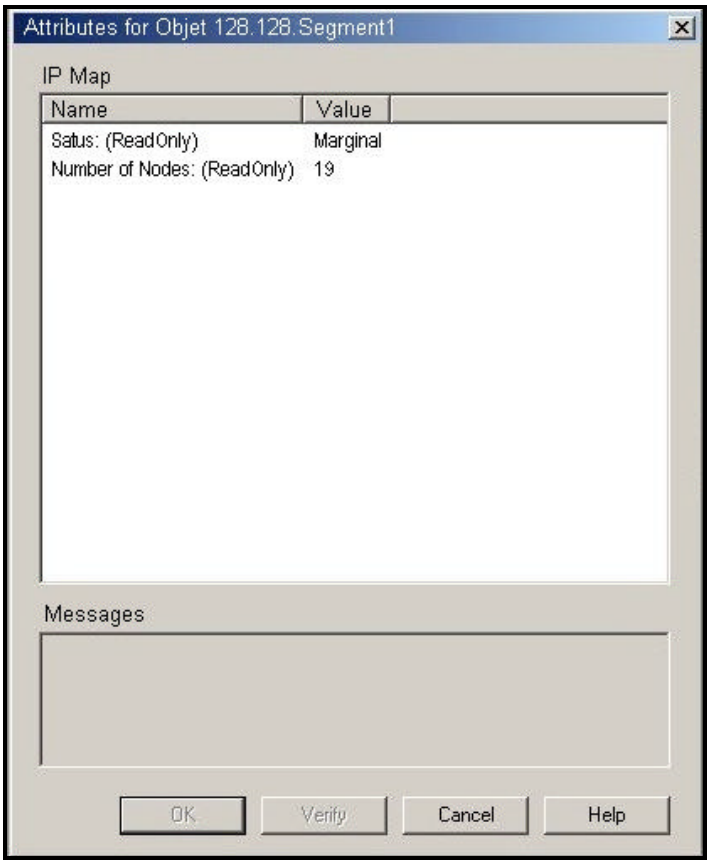

Figura 5.39 Descripción del Segmento 4 de la red LAN de Maint.

5.3.1.3 Descripción de un objeto nodo.

De igual manera para visualizar las propiedades de configuración de cualquier nodo que forma parte de la red LAN de la compañía Maint se selecciona cualquier símbolo de nodo en el mapa, por ejemplo la máquina cuya dirección IP es

128.128.9.91 y se hace click con el botón derecho del mouse y se selecciona *Object Propertiers* y a continuación *IP Map*, tal como se observa en la *Figura 5.40.*

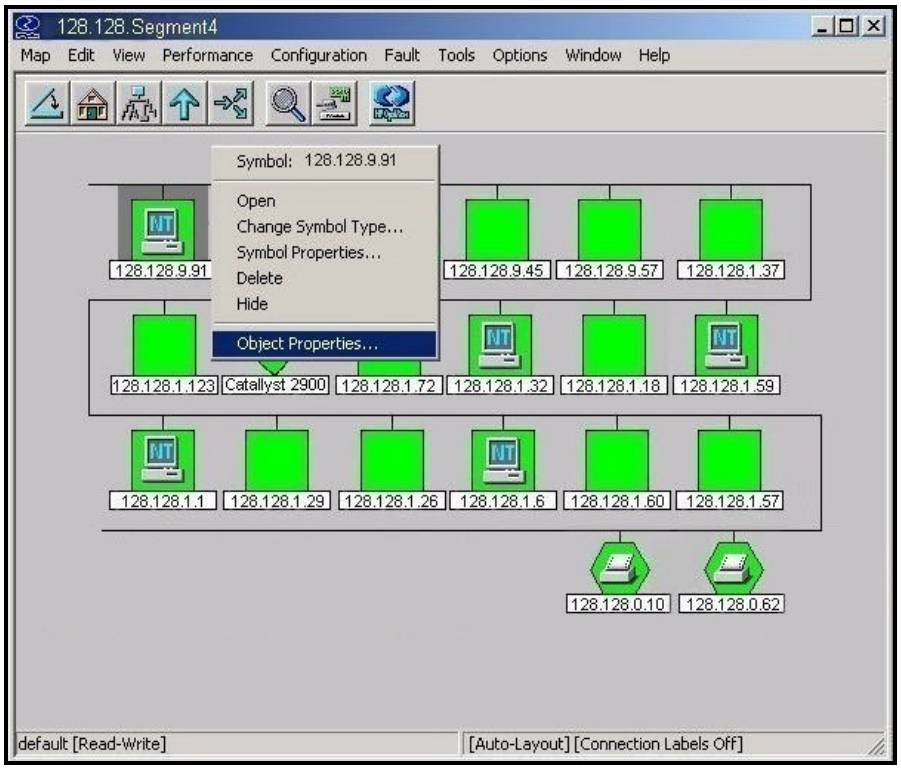

Figura 5.40 Método para obtener la descripción de la máquina 128.128.9.91.

De esta manera obtenemos la siguiente información, como se muestra en la *Figura 5.41.*

- El nombre del host que fue asignado cuando fue descubierto inicialmente.

- El estado del nodo.
- Información sobre el estado de cada interfase instalada en el nodo.
- Descripción del sistema dado por el agente SNMP.
- Situación del sistema dado por el agente SNMP.
- Identificador de objeto del nodo.
- Cualquier mensaje de error o estado que pueda aparecer en el campo de mensajes.

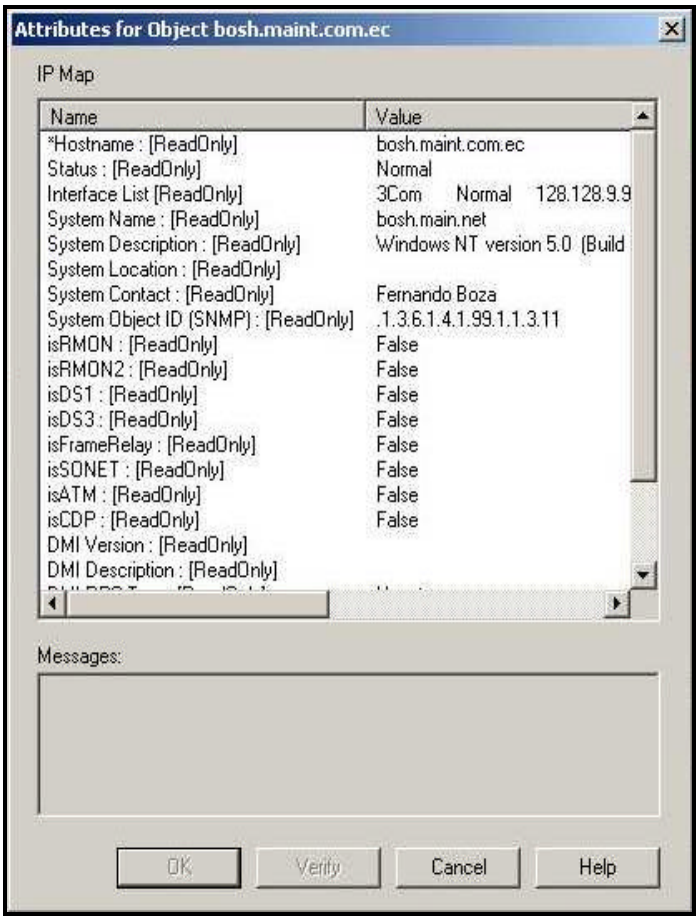

Figura 5.41 Descripción de la máquina 128.128.9.91.

5.3.1.4 Descripción de un objeto interfase.

Tal como en los anteriores casos podemos obtener la información de configuración de la interfase de red de cualquier dispositivo de la red LAN de la compañía Maint, simplemente se selecciona algún símbolo que represente alguna interfase en el submapa de la red, por ejemplo la interfaz Fa0 que pertenece al router Cisco 1750, se hace click con el botón derecho del mouse, luego se selecciona *Object Propertiers* y a continuación *IP map*, tal como se muestra en la Figura 5.42.

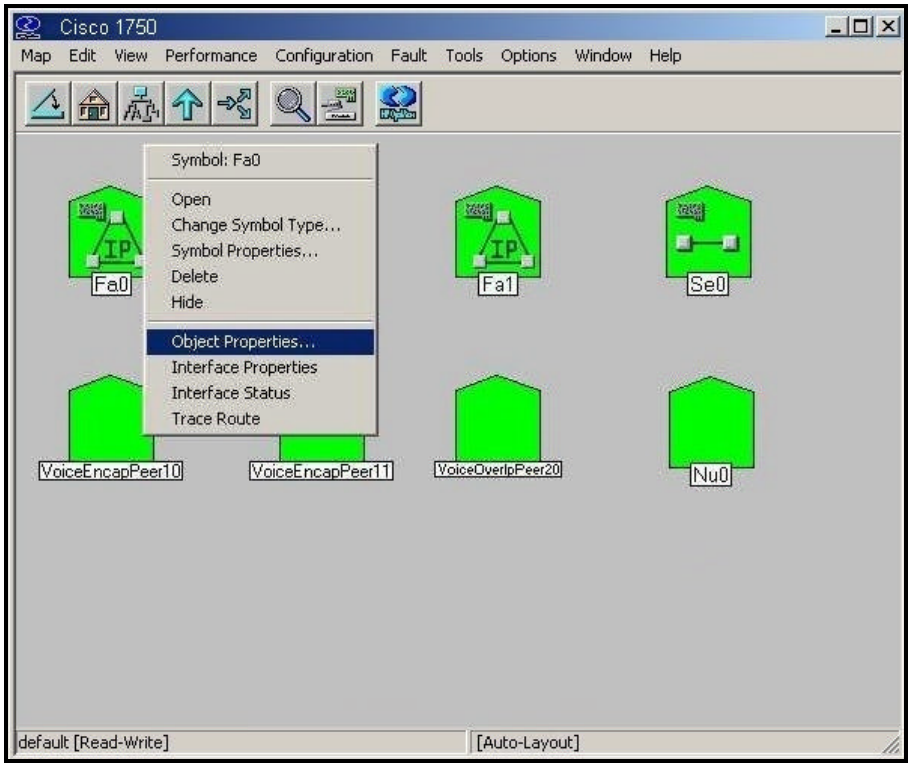

Figura 5.42 Método para obtener la descripción de la interfase Fa0 del router Cisco 1750.

De esta manera podremos acceder a la siguiente información, como se muestra en la *Figura 5.43.*

- Dirección de la interfase.
- Máscara de subred.
- Dirección Física.
- Tipo de interfase.
- Estado de la interfase.
- Cualquier mensaje de error o estado que pueda aparecer en el campo de mensajes.

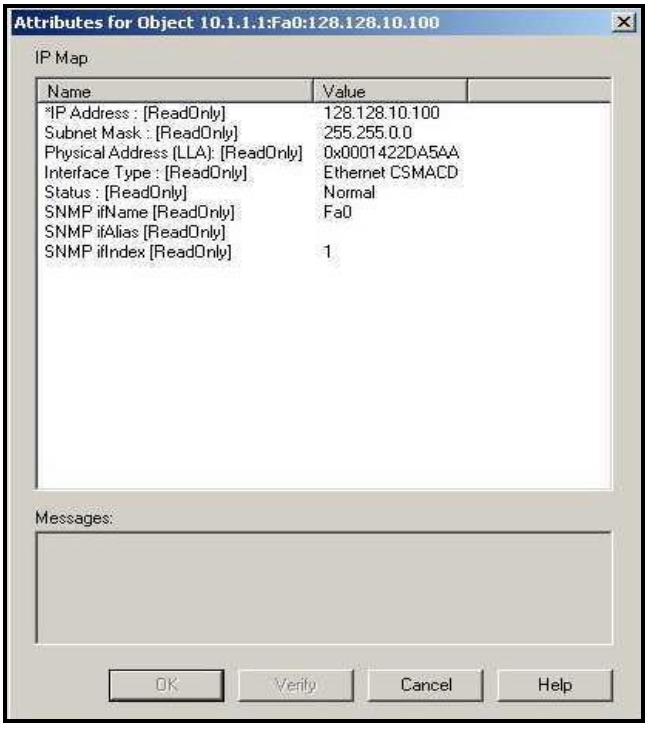

Figura 5.43 Descripción de la interfase Fa0 del router Cisco 1750.

5.3.2 Personalización de mapas.

Como se ha mencionado, el Hp OpenView Network Node Manager genera un mapa con todos los dispositivos que pudo descubrir, el propósito de este mapa es mostrar la red de una manera rápida una vez que se ejecute el programa. Pero debido a que muchas veces se desea personalizar la vista de este mapa se pueden hacer múltiples copias de éste.

Pueden existir múltiples mapas que visualicen información del mismo objeto ya que todos los mapas obtienen su información desde el mismo lugar, la Base de Datos de Objetos.

Gracias a esto se pueden tener múltiples vistas de la red, unos con mayor información que otros con la finalidad de distribuir la gestión de la red para un equipo de trabajo. Las opciones de personalización son:

- Copiar el mapa original.
- Controlar la visualización de dispositivos ligados a switches o bridges.
- Dar nombres significativos a los símbolos de la red.
- Visualizar las etiquetas de conexión.
- Controlar dispositivos que aparecen en el mapa.

5.3.2.1 Copiado del mapa original.

El Hp OpenView Network Node Manager nos permite copiar los objetos de los submapas de la red LAN de la compañía Maint y de esta manera crear nuevos submapas que nos posibilitan una visualización más ordenada de la red.

Gracias a esta propiedad hemos podido crear distintos submapas que nos permiten visualizar cada uno de los departamentos que posee la compañía Maint.

De esta forma tenemos acceso de una manera más organizada a cada uno de los nodos que conforman la red LAN de la compañía Maint, lo que nos facilita la gestión de configuración.

A continuación mostramos cada uno de los submapas de los diferentes departamentos que conforman la red LAN de la compañía Maint y los nodos que se encuentran contenidos en cada departamento.

Los submapas que representan los departamentos de la compañía Maint se muestran en las *Figuras 5.44* a *5.50.*

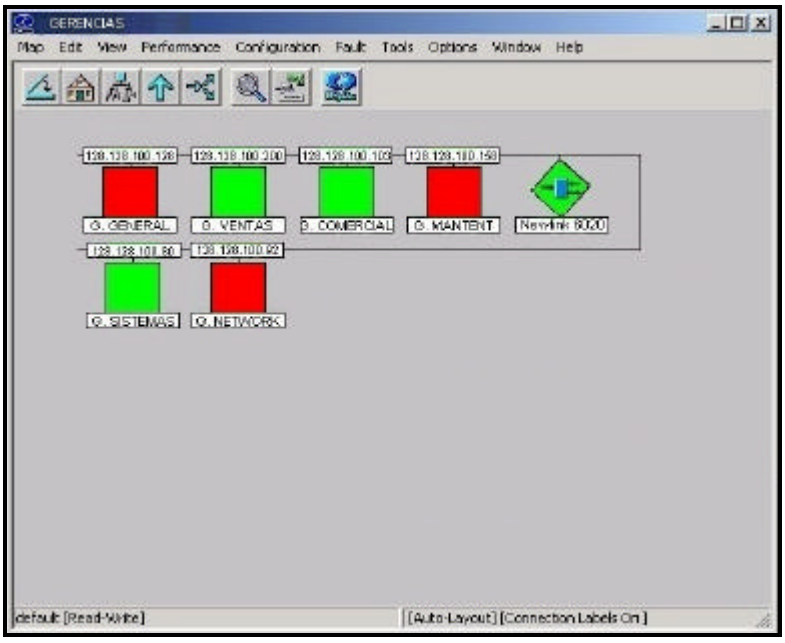

Figura 5.44 Submapa de Gerencias de la compañía Maint.

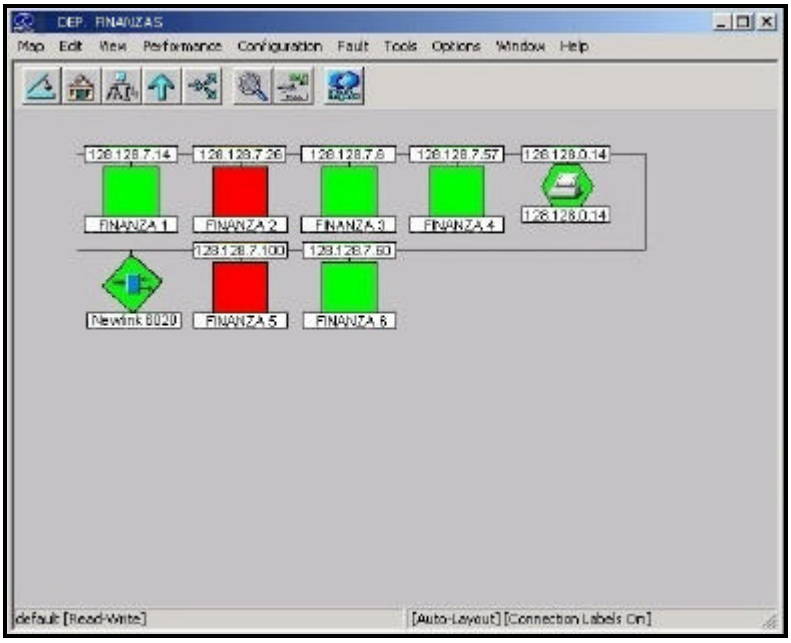

Figura 5.45 Submapa del área de Finanzas de la compañía Maint.

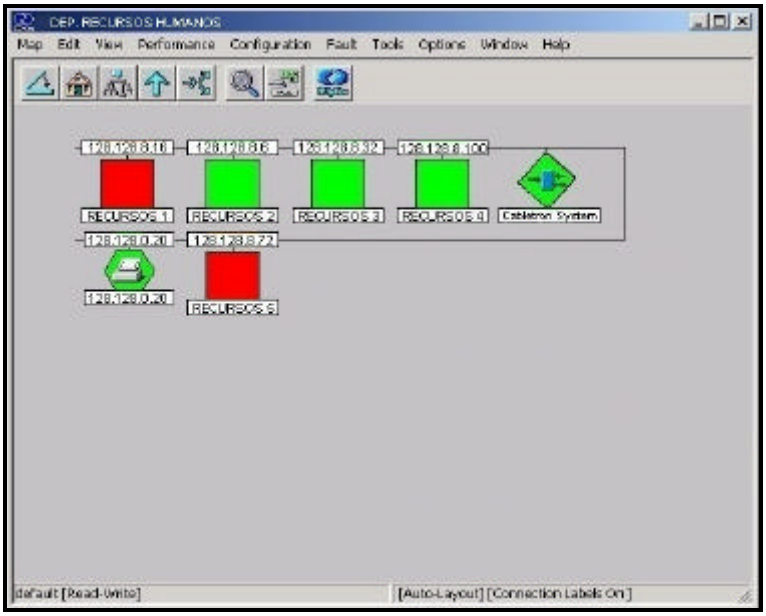

Figura 5.46 Submapa del área de Recursos Humanos de la compañía Maint.

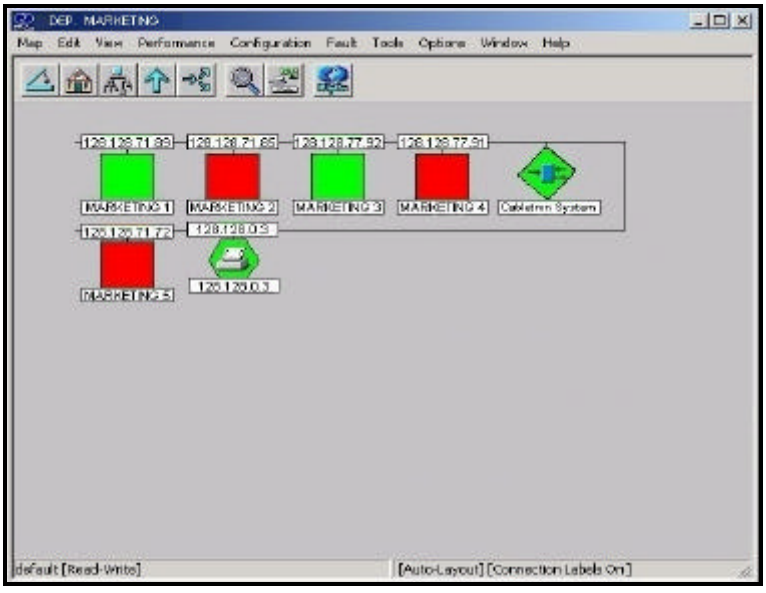

Figura 5.47 Submapa del área de Marketing de la compañía Maint.

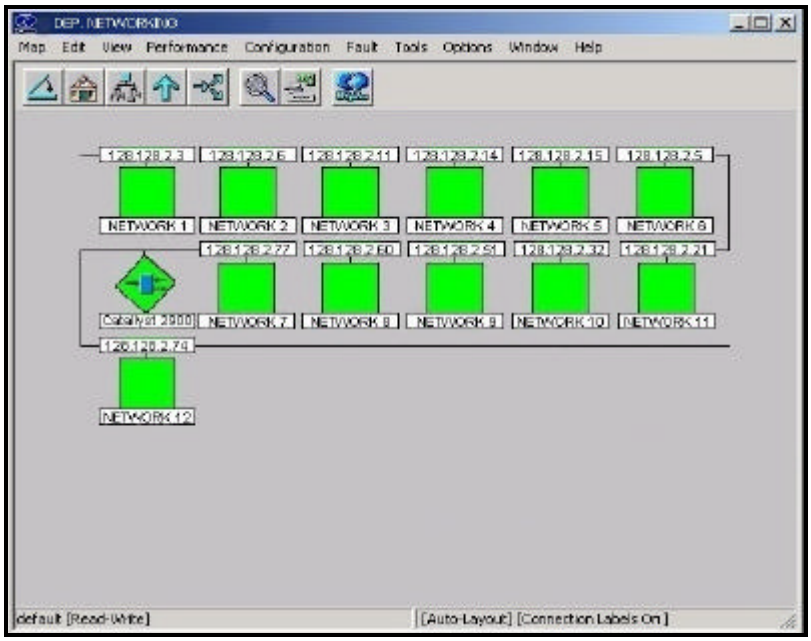

Figura 5.48 Submapa del área de Networking de la compañía Maint.

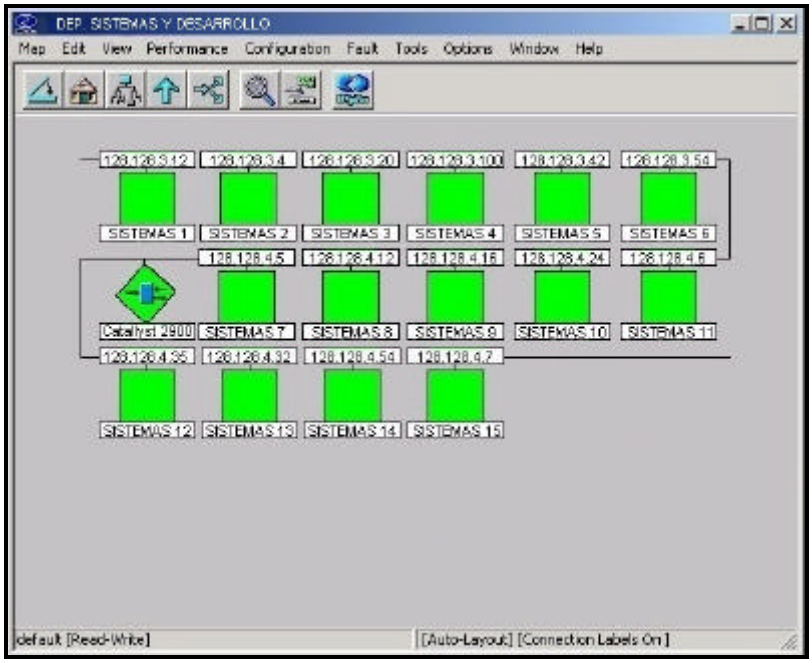

Figura 5.49 Submapa del área de Sistemas y Desarrollo de la compañía Maint.

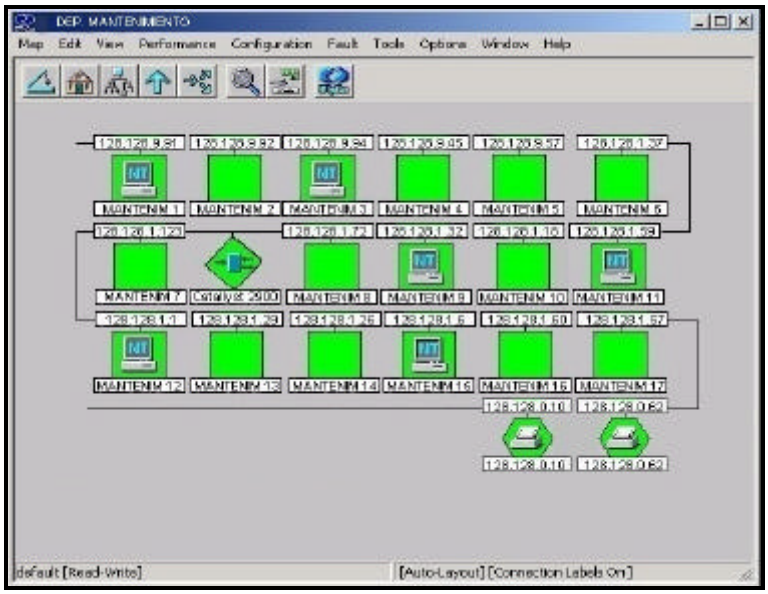

Figura 5.50 Submapa del área de Mantenimiento de la compañía Maint.

Consideramos que la gestión de la red LAN de la compañía Maint por departamentos es la más optima pues nos permite visualizar la máquina que ha fallado y su localización, lo que facilita su pronta recuperación.

5.3.2.2 Visualización de dispositivos ligados a switches o bridges.

Hp OpenView Network Node Manager tiene dos métodos para visualizar los dispositivos que están directamente vinculados a los puertos de switches y bridges de la red LAN de la compañía Maint:

1. Cada dispositivo vinculado es presentado como parte de una configuración estrella. Se hace doble click en el icono del segmento estrella para desplegar todos los dispositivos vinculados en un submapa. Esta presentación es la opción recomendada, por ser más ordenada y más fácil de usar para arreglar problemas. Ver *Figura 5.51*.

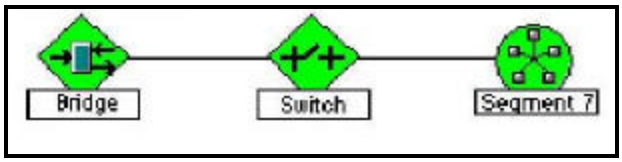

Figura 5.51 Presentación de objetos como configuración estrella.

2. Cada dispositivo vinculado es presentado como un segmento bus separado y para inspeccionar el estado de cada dispositivo se selecciona cada segmento. Ver *Figura 5.52.*

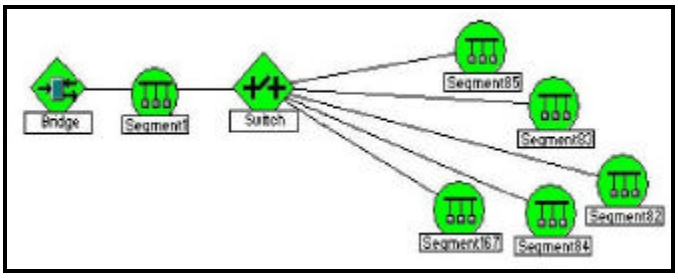

Figura 5.52 Presentación de objetos como segmento bus.

5.3.2.3 Nombrado significativo de los símbolos de la red.

Hp OpenView Network Node Manager permite proveer nombres significativos para los símbolos de la red LAN de la compañía Maint que estén de acuerdo al la función que desempeñan o al área que pertenecen, en lugar de sus direcciones IP, como por ejemplo: Finanzas, Gerencia, Mantenimiento, etc, tal como se muestra en la *Figura 5.53.* Esta manera de ver los elementos de la red LAN de Maint permite reconocerlos de una forma más rápida lo que nos facilita la gestión.

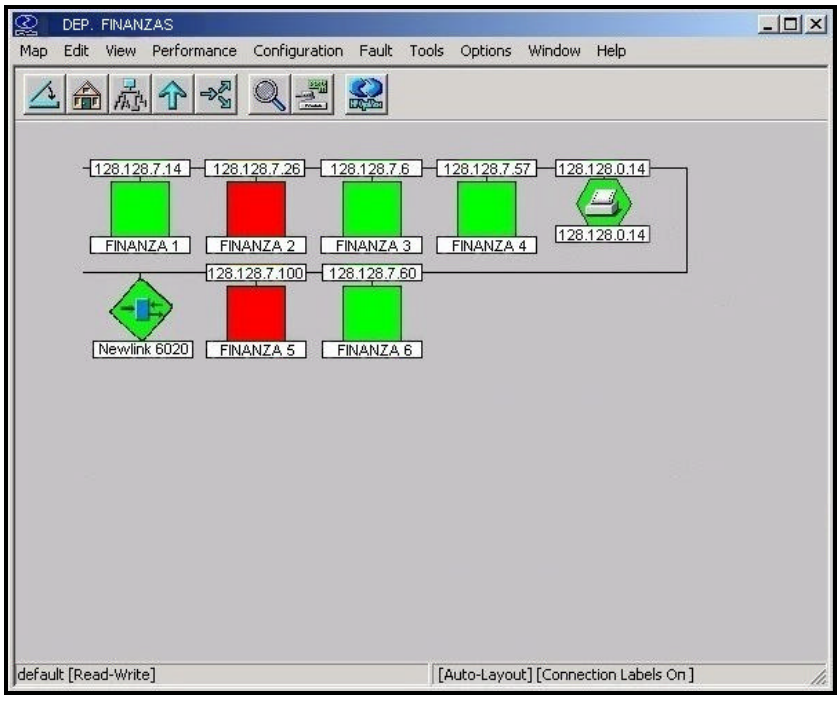

Figura 5.53 Submapas de la red LAN de Maint con nombres significativos.

5.3.2.4 Visualización de etiquetas de conexión.

Las etiquetas de conexión indican el puerto que se está usando para conectar una interfase de red a otra. Para poder ver las etiquetas se tienen dos opciones, por medio del *Menú View* seleccionando la opción *Show connection labels*, o mediante el botón *Toggle connection labels*. *Ver Figura 5.54.*

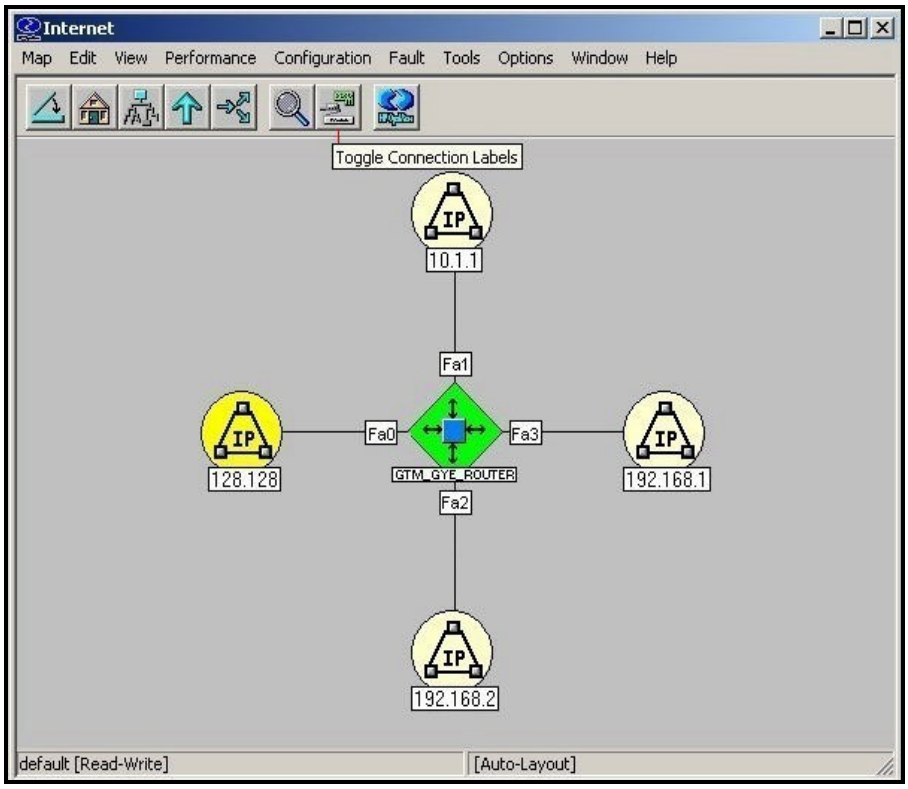

Figura 5.54 Submapa con etiquetas de conexión.

Es muy importante mencionar que las etiquetas de conexión se crean con la información disponible de los fabricantes de los equipos que forman parte de la red LAN de la compañía Maint, si

el Hp OpenView Network Node Manager no puede leer o entender la información de algún dispositivo no podrá etiquetar la conexión.

5.3.2.5 Control de dispositivos que aparecen en el mapa.

Mediante el Hp OpenView Network Node Manager se puede tener el control de cuales dispositivos serán visibles en el mapa. Es importante recordar que todos los mapas obtienen su información desde el mismo lugar, la base de datos de objetos, por lo que si se elimina un objeto (un dispositivo específico) desde la base de datos se eliminará de todos los mapas. Entonces en vez de borrar el dispositivo se tiene la siguiente opción:

- **Ocultar las características del Objeto.**

  Al ocultar las características del objeto se puede personalizar de manera individual cada submapa y todos los submapas de un mapa.

  Para ocultar un símbolo, se selecciona el símbolo o los símbolos que se desean ocultar y se selecciona del *Menú View, Hidden Objects* y luego se elige *Hide Selected From*

This Submap o Hide Selected From All Submap, tal como se muestra en la *Figura 5.55.*

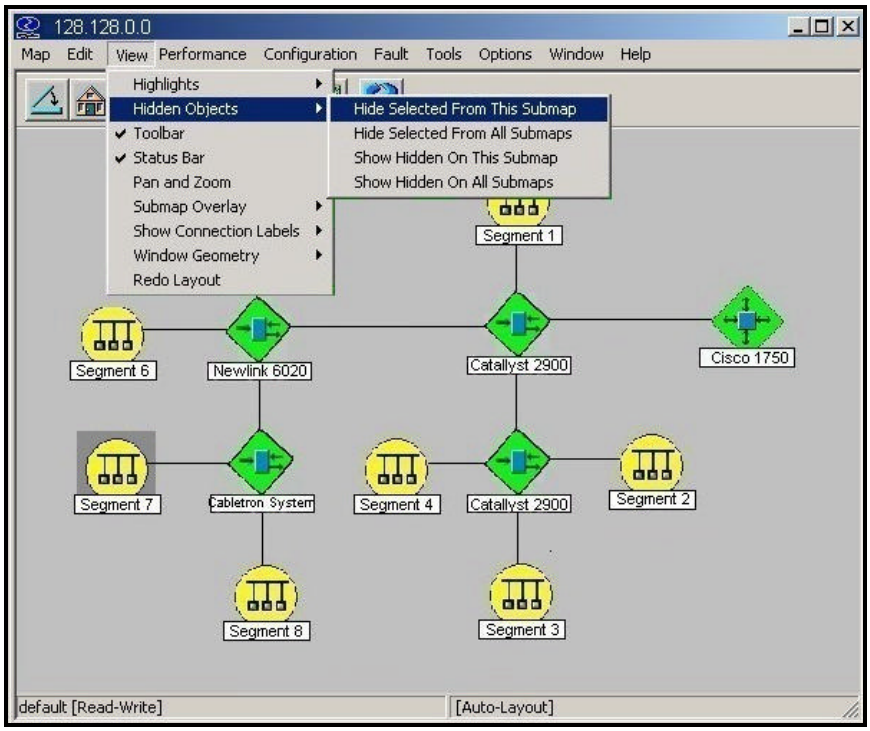

Figura 5.55 Método para ocultar símbolos de los segmentos de la red LAN de Maint.

Por ejemplo en la *Figura 5.56* se ve el procedimiento para esconder todos los símbolos de los segmentos que forman la red LAN de Maint para utilizar este mapa para monitorear exclusivamente los switches y el router que posee la compañía.

Tal como vemos en la Figura 5.56, en la parte inferior derecha se muestra el número de objetos ocultos en el submapa, en este caso el número de segmentos que forman la red LAN de la compañía Maint.

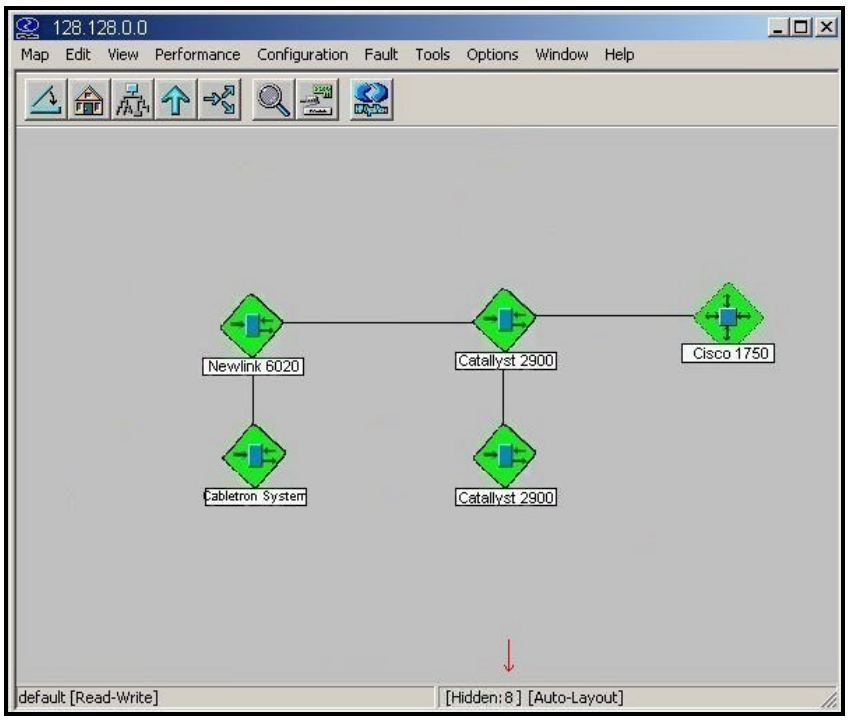

Figura 5.56 Submapa de la red LAN con objetos ocultos.

5.4 Gestión de Contabilidad.

Esta función obtiene información estadística del uso de la red. Permite recoger datos relacionados al consumo de los recursos de la red de manera individual o de grupo, y poder así identificar los costes de la

utilización de los recursos para en función de los mismos poder establecer los cargos por consumo a los usuarios.

Hp OpenView Network Node Manager no gestiona esta función directamente.

5.5 Gestión de seguridad.

Esta función protege la red y sus interconexiones, sistemas e información de gestión de la red de algún uso o acceso no autorizado u otro daño. De esta forma se puede impedir que una persona sin autorización pueda acceder a esta información por medio de la red.

La gestión de seguridad proporciona los medios para localizar la información importante, establecer los puntos desde los que se puede acceder y registrar a los usuarios que consultan dicha información y durante que períodos de tiempo, así como los intentos fallidos de acceso a dicha información o dispositivo que la contiene.

Hp OpenView Network Node Manager no gestiona esta función directamente.

CONCLUSIONES Y RECOMENDACIONES

Tal como hemos comprobado en este proyecto, el software de gestión Hp OpenView Network Node Manager pudo ser instalado y probado satisfactoriamente en la red LAN de la compañía Maint, todos los dispositivos fueron reconocidos correctamente lo que demostró su capacidad de gestionar una red compuesta por elementos de diferentes marcas que soportan agente SNMP.

Las herramientas proporcionadas por este software nos permitieron cumplir nuestro objetivo al comprobar que tan efectivo es tener implementado un sistema de gestión dentro de una compañía sin importar su complejidad o dimensión, ya que los servicios brindados por el Hp OpenView Network Node Manager realizan una monitorización interactiva de todos los nodos de la red, facultándole inclusive al administrador de la red determinar los recursos que se consideren críticos y merezcan un mayor control.

Tres de las cinco funciones de gestión que brinda el Hp OpenView Network Node Manager pueden ser explotadas en su totalidad por el administrador de la red mediante el monitoreo constante de la situación de los nodos de la red por medio de mapas interactivos que indican por

medio de colores el estado de cada dispositivos sean estos conexiones físicas o elementos activos.

Consideramos que el visor de alarmas constituye un instrumento fundamental para el administrador de la red ya que por medio de este se tiene absoluto control de todos los eventos que ocurren en la red, pudiendo inclusive configurar nuevos eventos con umbrales significativos que se consideren necesarios; y además gracias al servicio de correlación de eventos podemos descartar eventos redundantes lo que es de gran ayuda para establecer el origen exacto del problema.

Sin duda alguna el Hp OpenView Network Node Manager ha demostrado cumplir con las normas internacionales consolidándose como una plataforma comercial de gestión por su difusión y sus buenas posibilidades, y recomendamos se implementen las funciones de contabilidad y seguridad por medio del Hp OpenView IT/Administration para de esta manera tener completo el sistema de gestión.

Al terminar este proyecto no solo hemos aprendido lo valioso de tener implementado un sistema de gestión si no también cuan importante es tomar decisiones rápidas para evitar mayores inconvenientes que puedan afectar el rendimiento de una red de telecomunicaciones.

GLOSARIO

Agente de gestión.- Es un software que proporciona acceso a los datos de gestión de un dispositivo de red particular, responde a peticiones de información y acciones de parte de la estación de gestión y puede enviar a la estación cierta información importante no solicitada de un modo asíncrono.

Bridge.- Puente. Dispositivo que interconecta redes de área local (LAN) en la capa de enlace de datos OSI. Filtra y retransmite tramas según las direcciones a Nivel MAC.

Datagrama.- Usualmente se refiere a la estructura interna de un paquete de datos.

Estación de gestión.- Es un elemento de la red dedicado a las tareas de gestión, aunque también puede dedicarse a otras tareas. Sirve como interfaz entre el administrador de la red y el sistema de gestión de red.

Ethernet.- Diseño de red de área local normalizado como IEEE 802.3. Utiliza transmisión a 10 Mbps por un bus coaxial. El método de acceso es CSMA/CD.

FDDI (Fiber Distributed Data Interface).- Un estándar de transmisión de datos empleando fibra óptica con un rango de 100,000,000 bits por segundo *(10 veces más rápido que una red Ethernet, alrededor del doble de rápido que un T-3).*

Firewall.- Cortina de Fuego. Router diseñado para proveer seguridad en la periferia de la red. Se trata de cualquier programa (Software) ó router (Hardware) que protege a una red de otra red. El firewall da acceso a una maquina en una red local a Internet pero Internet no ve más allá del firewall.

FTP.- File Transfer Protocol. Protocolo de Transferencia de Archivos. Uno de los protocolos de transferencia de ficheros más usado en Internet.

Gateway.- Pasarela. Puerta de Acceso. Dispositivo que permite conectar entre si dos redes normalmente de distinto protocolo o un Host a una red.

Hub.- Dispositivo que ejerce de nodo central en redes en estrella; se puede utilizar en caso de administración central. Los nodos pueden aislarse contra colapsos.

ICMP (Internet Control Message Protocol).- Protocolo Internet de Control de Mensajes.

Interfase.- provee los medios para la interconexión de equipo o procesos localizados en un lugar específico. Ejemplos de interfaces lo son el RS232-C, RS449, X-21, etc.

IP (Internet Protocol).- aquella parte del TCP/IP que administra el envío de paquetes.

IPX (Internet Packet Exchange).- Intercambio de Paquetes entre Redes. Inicialmente protocolo de Novell para el intercambio de información entre aplicaciones en una red Netware.

ISDN (Integrated Services Digital Network).- Red Digital de Servicios Integrados. Servicio provisto por una empresa de comunicaciones que permite transmitir simultáneamente diversos tipos de datos digitales conmutados y voz.

ISO (International Standard Organization).- Organización Internacional de Estándares.

LAN (Local Area Network).- Red de Area Local. Una red de área local es un sistema de comunicación de alta velocidad de transmisión. Estos sistemas están diseñados para permitir la comunicación y transmisión de datos entre estaciones de trabajo inteligentes, comúnmente conocidas

como Computadoras Personales. Todas las PCs, conectadas a una red local, pueden enviar y recibir información. Como su mismo nombre lo indica, una red local es un sistema que cubre distancias cortas. Una red local se limita a una planta o un edificio.

MAC (Media Access Control).- Control de Acceso a Medio. Protocolo que define las condiciones en las cuales las estaciones de trabajo acceden al medio, su uso está difundido en las LAN; la capa MAC es la subcapa más baja del protocolo de la capa de enlace de datos.

MIB (Management Information Base).- Es una base de datos que contiene información sobre los elementos de la red a gestionar, cada recurso que se quiere gestionar se representa mediante un objeto. La MIB es un conjunto estructurado de tales objetos.

Nodo.- Por definición punto donde convergen más de dos líneas. A veces se refiere a una única máquina en Internet. Normalmente se refiere a un punto de confluencia en una red. Punto de interconexión a una RED.

OSI (Open Systems Interconnection).- Interconexión de Sistemas Abiertos. Modelo de referencia de interconexión de sistemas abiertos propuesto por la ISO. Divide las tareas de la red en siete niveles.

PING (Packet Internet Groper).- Rastreador de Paquetes Internet. Programa utilizado para comprobar si un Host está disponible. Envía paquetes de control para comprobar si el anfitrión está activo y los devuelve.

Protocolo.- Este es el procedimiento (conjunto de pasos, mensajes, forma de los mensajes y secuencias) que se utiliza para mover la información de una localización a otra sin errores.

Router.- Dispositivo conectado a dos o mas redes que se encarga únicamente de tareas de comunicaciones.

Servidor.- Un dispositivo de red que ofrece servicios a un PC cliente; por ejemplo, acceso a ficheros, cola de impresión o acceso remoto.

SNMP (Simple Network Management Protocol).- Protocolo que controla los dispositivos de conexión en red, entre los cuales se encuentran adaptadores, conmutadores, rutas, servidores y estaciones de trabajo; recogen información de diferentes agentes.

TCP/IP (Transport Control Protocol/Internet Protocol).- Protocolo de Control de Transporte / Protocolo Internet. Nombre común para una serie de protocolos desarrollados por DARPA en los Estados Unidos en los

años 70, para dar soporte a la construcción de redes interconectadas a nivel mundial. TCP corresponde a la capa (layer) de transporte del modelo OSI y ofrece transmisión de datos. El IP corresponde a la capa de red y ofrece servicios de datagramas sin conexión. Su principal característica es comunicar sistemas diferentes.

Telnet.- Protocolo y aplicaciones que permiten conexión como terminal remota a una computadora anfitriona, en una localización remota.

UDP (User Datagram Protocol).- Protocolo de Datagrama de Usuario. Protocolo abierto en el que el usuario (programador) define su propio tipo de paquete.

X.25.- Protocolo de transmisión de datos. Establece circuitos virtuales, enlaces y canales.

REFERENCIAS BIBLIOGRAFICAS

- Tutorial de Gestión de redes y servicios, Ing. Edgar Leyton.
- http://www.arrakis.es/~gepetto/redes/rog08p2.html
- http://www.disc.ua.es/asignaturas/rc/trabajos/snmp/tema1.html#principio
- http://www.map.es/csi/silice/Redges6.html
- http://ovweb.external.hp.com/ovnsmdps/pdf/j1240-90058.pdf