INTRODUCCION

IDENTIFICACION DEL PROBLEMA

Las organizaciones dependen cada vez más del buen funcionamiento de los sistemas de comunicaciones. Cada vez es menos justificable la expresión **" la red no funciona bien "** al interior de la empresa, o la expresión **" la línea está caída"** frente al cliente.

Debido a la competencia de servicios, las organizaciones y empresas que no disponen de una buena gestión de sus redes y servicios de comunicaciones son cautivas de la tecnología y en lugar de emplear los recursos informáticos para hacer negocios, éstos pueden estar impidiendo el progreso de su negocio.

Los fallos en los sistemas de comunicaciones son inevitables y el tiempo de no-funcionamiento de los mismos es muy costoso para las organizaciones. Para evitar esto en la red de datos de la UTN, se ha propuesto el presente tema de tesis, que evalúa los sistemas de gestión de redes existentes en

nuestro medio y propone un sistema que se adapte mejor a las necesidades de gestión de la REDUTN.

Se desarrolló también el ***prototipo Net-Manager que permite realizar funciones básicas de configuración, visualizar estadísticas de rendimiento, detectar fallos y errores en los elementos activos de la REDUTN***, siendo éste el comienzo de la realización de un sistema modular de gestión de red creado en la **UNIVERSIDAD TECNICA DEL NORTE**.

Net-Manager permite saber si un dispositivo conectado a la red (computadoras, hubs, switchs) está funcionando correctamente, en caso de surgir algún fallo notificarlo al encargado de la gestión de la red además de almacenar los eventos ocurridos en un archivo de historial para un análisis posterior.

Como se ha podido determinar, este proyecto involucró una investigación pormenorizada de equipos activos, comunicación entre estos en tiempo real, análisis de algoritmos que permitan la detección de fallos y errores en una INTRANET y un sin número de actividades, por lo que se necesita un grupo de investigación que lleven a cabo el cumplimiento del proyecto planteado en el tiempo establecido.

Objetivos

Generales

- ✓ Obtener un estudio y evaluación de los principales sistemas comerciales de Gestión de Red existentes en nuestro medio.
- ✓ Configuración básica, visualización de estadísticas de rendimiento y detección de fallos y errores en los elementos activos de la REDUTN, con el desarrollo del prototipo Net-Manager.

Específicos

- ✓ Determinar los principales sistemas de gestión de red que puedan adaptarse a los requerimientos de gestión de la REDUTN.

- ✓ Analizar los SGR con los que cuentan las empresas o instituciones públicas y/o privadas, para emitir criterios de evaluación.

- ✓ Emplear las etapas de la Ingeniería del Software Orientada a Objetos en el diseño y desarrollo del software prototipo NetManager.

CAPITULO I

CONCEPTOS GENERALES DE REDES

Introducción

La difusión de las computadoras ha impuesto la necesidad de compartir información, programas, recursos, acceder a otros sistemas informáticos dentro de la empresa y conectarse con bases de datos situadas físicamente en otras computadoras. En la actualidad, una adecuada interconexión entre los usuarios y procesos de una empresa u organización, puede constituir una clara ventaja competitiva. La reducción de costes de periféricos, o la facilidad para compartir y transmitir información son los puntos claves en que se apoya la creciente utilización de redes.

1.1 Concepto de Red

Una red es un conjunto de computadoras conectados entre sí, que pueden comunicarse compartiendo datos y recursos sin importar la localización física de los distintos dispositivos (ver **Fig. 1.1**). Cada dispositivo activo conectado a la red se denomina nodo. Un dispositivo activo es aquel que interviene en la comunicación de forma autónoma, sin estar controlado por otro dispositivo.

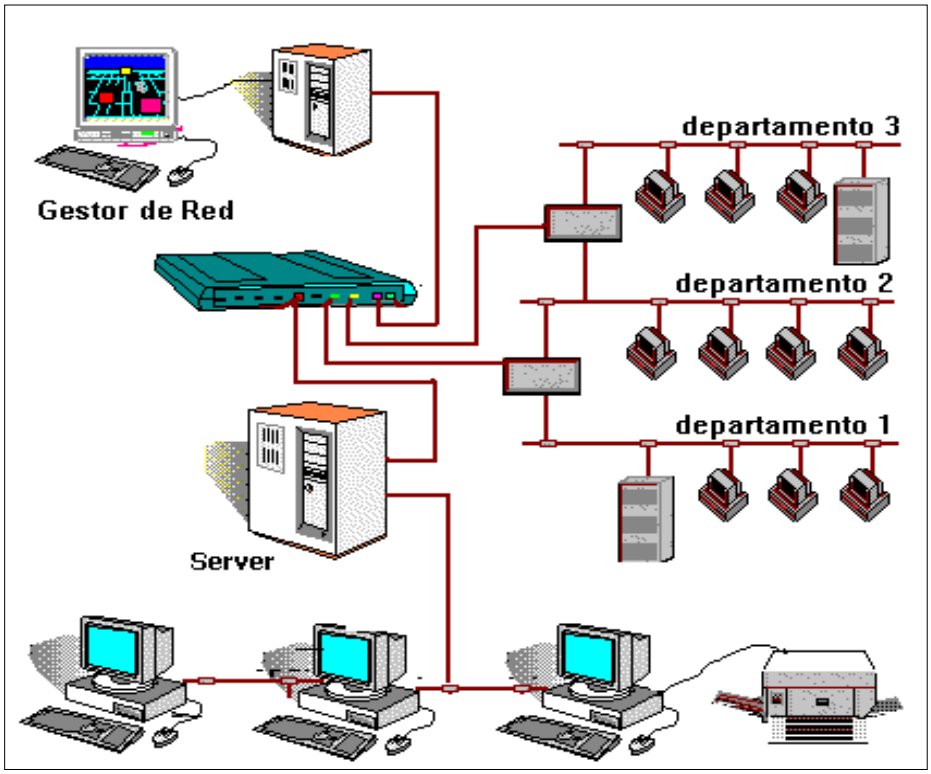


Fig. 1.1 **Esquema de una Red de Computadoras**

1.2 Ventajas de una Red de Computadoras

Dependiendo de la topología de red que se estudie, se tienen las siguientes ventajas:

- Necesidad de compartición de recursos (equipamientos e información).
- Proceso Distribuido.
- Sistemas de Mensajería.
- Bases de Datos.
- Creación de grupos de trabajo.
- Gestión centralizada.
- Seguridad.
- Acceso a otros sistemas operativos.
- Mejoras en la organización de la empresa.

1.3 Conceptos y Funcionalidades Básicas

1.3.1 Modelo de referencia OSI

Con objeto de proporcionar un estándar de comunicación entre diversos fabricantes, la Organización Internacional de Estándares (**ISO**, *International Standards Organization*) ha establecido una arquitectura como modelo de referencia para el diseño de protocolos de Interconexión de Sistemas Abiertos (**OSI**, *Open Systems Interconnection*).

Este ***modelo de siete niveles*** proporciona un estándar de referencia para la intercomunicación entre sistemas de computadoras a través de una red utilizando protocolos comunes.

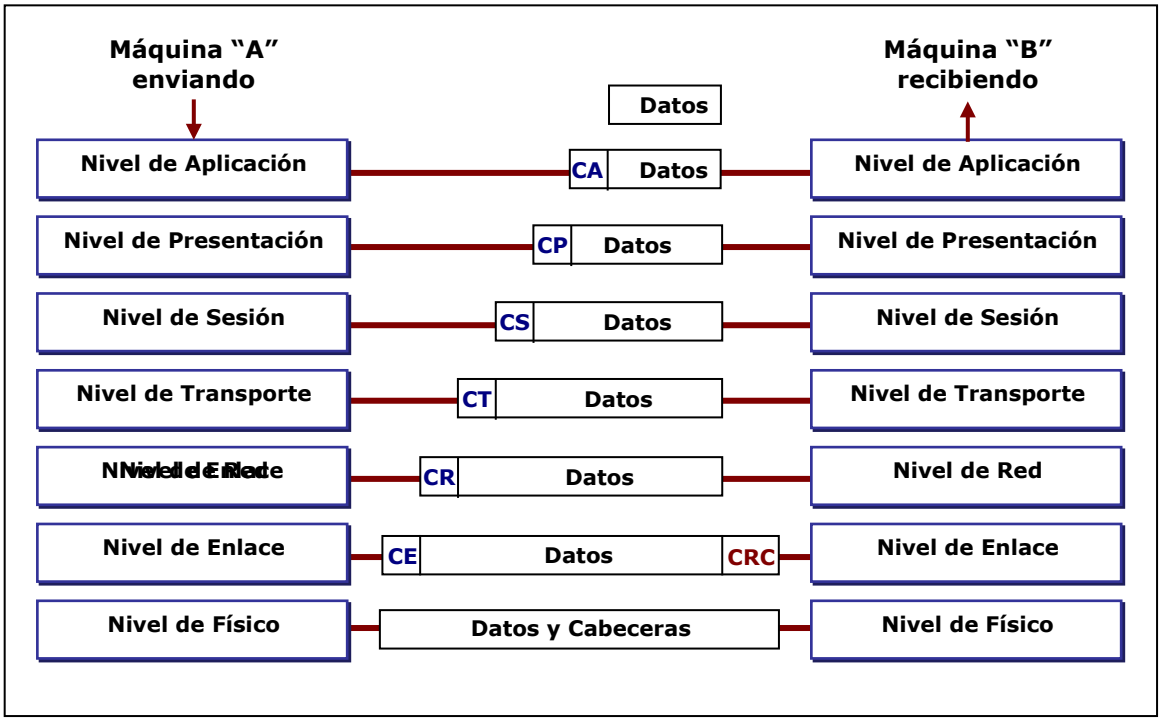


Fig. 1.2 **Modelo OSI**

1) **<u>Nivel Físico</u>:** especifica un conjunto de estándares que definen aspectos mecánicos, eléctricos y funcionales para la conexión de los equipos al

medio físico empleado. Su función es la transmisión de una cadena continua de bits a través de un canal básico de comunicación.

2) **Nivel de Enlace:** a partir del servicio de transmisión de bits ofrecido por el Nivel Físico, la tarea del Nivel de Enlace es ofrecer un control de errores al Nivel de Red. Además de la detección y corrección de errores, este nivel fragmenta y ordena en paquetes los datos enviados, también realiza funciones básicas de control de flujo.

3) **Nivel de Red:** este nivel proporciona los medios adecuados para establecer, mantener y terminar conexiones entre sistemas. El Nivel de Red principalmente permite direccionar los paquetes de datos que recibe del nivel de transporte.

4) **Nivel de Transporte:** se encarga de facilitar una transferencia de datos fiable entre nodos finales, proporcionando una integridad de los datos y una calidad de servicio previamente establecida.

5) **Nivel de Sesión:** Permite establecer, gestionar y terminar sesiones entre aplicaciones. Realiza la gestión y recuperación de errores y en algunos casos proporciona múltiples transmisiones sobre el mismo canal de transporte.

6) **Nivel de Presentación:** proporciona a las aplicaciones transparencia respecto del formato de presentación, realizando conversión de caracteres, códigos y algunas funciones de seguridad (encriptación).
7) **Nivel de Aplicación:** se denomina también ***"nivel de usuario"*** porque proporciona la interfaz de acceso para la utilización de los servicios de alto nivel.

1.3.2 Topologías

La topología de una red es la configuración formada por sus *nodos* (estaciones) y las *interconexiones* existentes entre ellos (bus, estrella, anillo, etc.).

1.3.3 Protocolos de comunicaciones

Los protocolos de comunicaciones son reglas y procedimientos utilizados en una red para establecer la comunicación entre los nodos. En los protocolos se definen distintos niveles de comunicación. Las reglas de nivel más alto definen ¿cómo se comunican las aplicaciones?, mientras que las de nivel más bajo definen ¿cómo se transmiten? las señales por el cable.

Los protocolos de comunicaciones se pueden clasificar en cuatro tipos:

- PROPIETARIOS
- XNS
- OSI
- TCP/IP

1.4 Tipos de Redes

Dependiendo del territorio que una red abarca se clasifica en:

1.4.1 Red de Area Local (**LAN**, *Local Area Network*)

Una Red de Area Local está normalmente restringida a un área geográfica de tamaño limitado, como un edificio de oficinas y depende de un canal físico de comunicaciones con una velocidad media/alta y con una tasa de errores reducida.

1.4.2 **Red de Area Extensa (WAN, *Wide Area Network*)**

Una Red de Area Extensa es una red que ofrece servicios de transporte de información entre zonas geográficamente distantes. Es el método más efectivo de transmisión de información entre edificios o departamentos distantes entre sí.

1.4.3 **Red de Area Metropolitana (MAN, Metropolitan Area Network)**

Una red de área metropolitana es una red de alta velocidad (banda ancha) que dando cobertura en un área geográfica extensa, proporciona capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y vídeo, sobre medios de transmisión tales como fibra óptica y par trenzado de cobre a velocidades que van desde los 2 Mbps hasta 155 Mbps (Megabits por segundo).

El concepto de red de área metropolitana representa una evolución del concepto de red de área local a un ámbito más amplio, cubriendo áreas de una cobertura superior que en algunos casos no se limitan a un entorno metropolitano sino que pueden llegar a una cobertura regional e incluso nacional mediante la interconexión de diferentes redes de área metropolitana.

1.5 **Dispositivos de Interconexión**

1.5.1 **Funciones básicas**

Para superar las limitaciones físicas de los elementos básicos de una red, existen dispositivos cuyas funciones son las de extender las topologías de red. Estos elementos son: *concentradores o hubs*, *repetidores*, *bridges o puentes*, *routers o encaminadores* y *gateways o pasarelas*.

Los dispositivos de interconexión de redes proporcionan algunas (o todas) de las siguientes funciones básicas:

a) **Extensión de la red:** Permite ampliar el rango de distancia que puede alcanzar una red.

b) **Definición de segmentos dentro de la red:** Al dividir la red en segmentos se consigue aumentar las prestaciones de la red ya que cada tramo soporta sólo su propio tráfico y no los de los otros segmentos.

c) **Separación entre redes:** Mediante estos dispositivos las grandes redes se pueden componer de otras más pequeñas interconectadas entre sí, de forma transparente para el usuario. Varias redes físicas pueden combinarse para formar una única red lógica.

1.5.2 Características Principales

Los dispositivos de interconexión deben funcionar para cualquier tipo de red y tener una arquitectura estándar para los protocolos de comunicación de las redes.

La **figura 1.2** muestra la relación de los dispositivos de interconexión con los niveles del modelo de referencia OSI.

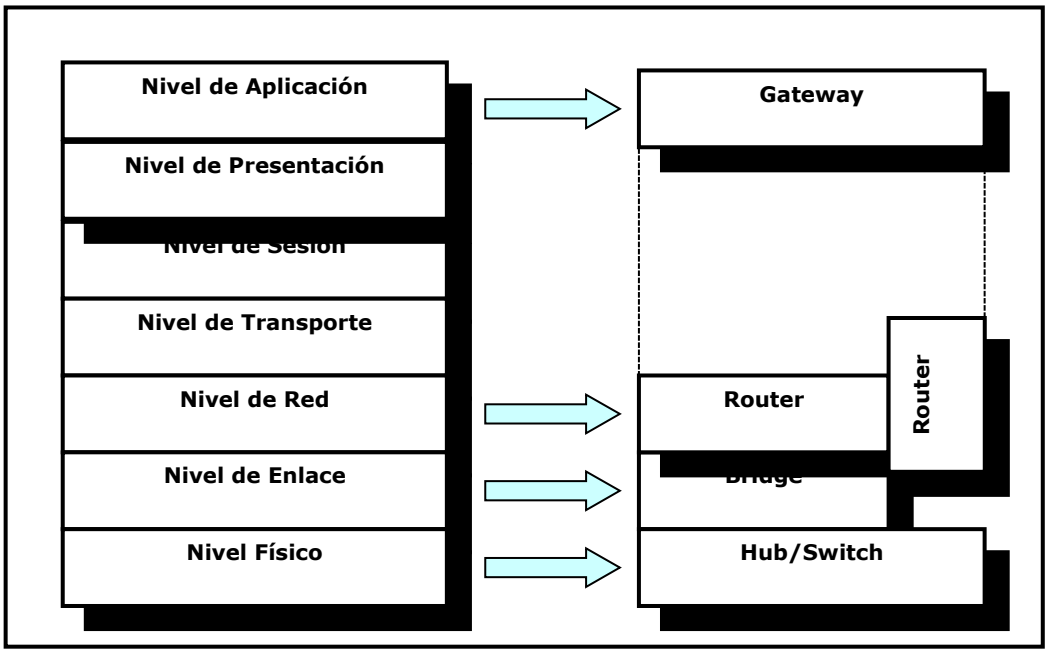


Fig 1.2 **Relación entre los dispositivos de interconexión y los niveles del modelo OSI**

Referencias Bibliográficas

1. **GARCIA Jesús., "Redes para Procesos Distribuidos"**, Editorial RA - MA, Madrid España.

2. **TANENBAUM Andrew., "Redes de Computadoras"**, Tercera Edición, Prentice Hall Hispanoamericana, S. A.

CAPITULO II

GESTION DE REDES

Introducción

En el campo de la tecnología de la información, la tendencia más importante está constituida por los sistemas distribuidos y las computadoras, los cuales se encuentran conectados por redes, mediante las que los usuarios pueden acceder a varios recursos conectados remotamente.

Llega entonces el momento de aplicar algunas técnicas y herramientas que permitan llevar a cabo la gestión de manera controlada y automatizada, garantizando que los sistemas funcionen, optimizando la fiabilidad y la disponibilidad de los mismos.

2.1 Conceptos Generales de Gestión

2.1.1 Gestión

Es una actividad fundamental que asegura la coordinación de los esfuerzos individuales para cumplir con las metas de grupo.

2.1.2 Actividades de Gestión

Los conocimientos se agrupan en diversas funciones administrativas entre las que se puede citar: planeación, organización, integración, dirección y control.

Los administradores persiguen el objetivo de establecer un medio en el cual las personas puedan cumplir con las metas del grupo en un lapso mínimo de tiempo. Estos a la vez buscan la productividad, que se mide en los resultados/producción que se tienen en un determinado período.

La productividad implica efectividad para el cumplimiento de las metas y eficiencia para el cumplimiento de las mismas con un mínimo de recursos.

Dentro de la gestión existen diversos enfoques uno de ellos es el de sistemas (ver **Fig. 2.1**), el que añade conceptos de base de aplicación muy amplia. Los sistemas tienen límites pero también actúan recíprocamente con el medio externo, es decir las organizaciones son sistemas abiertos. De ahí que es importante estudiar la relación existente entre las funciones de gestión que existen en una organización y sus diferentes subsistemas.

Un **"sistema"** es esencialmente un conjunto de elementos interrelacionados e interdependientes, que forman una unidad compleja.

Los sistemas también desempeñan un papel importante en el campo mismo de la administración, existen sistemas de planeación, de organización y de control, dentro de ellos es posible descubrir muchos subsistemas, como el de planeación de redes y de presupuestos.

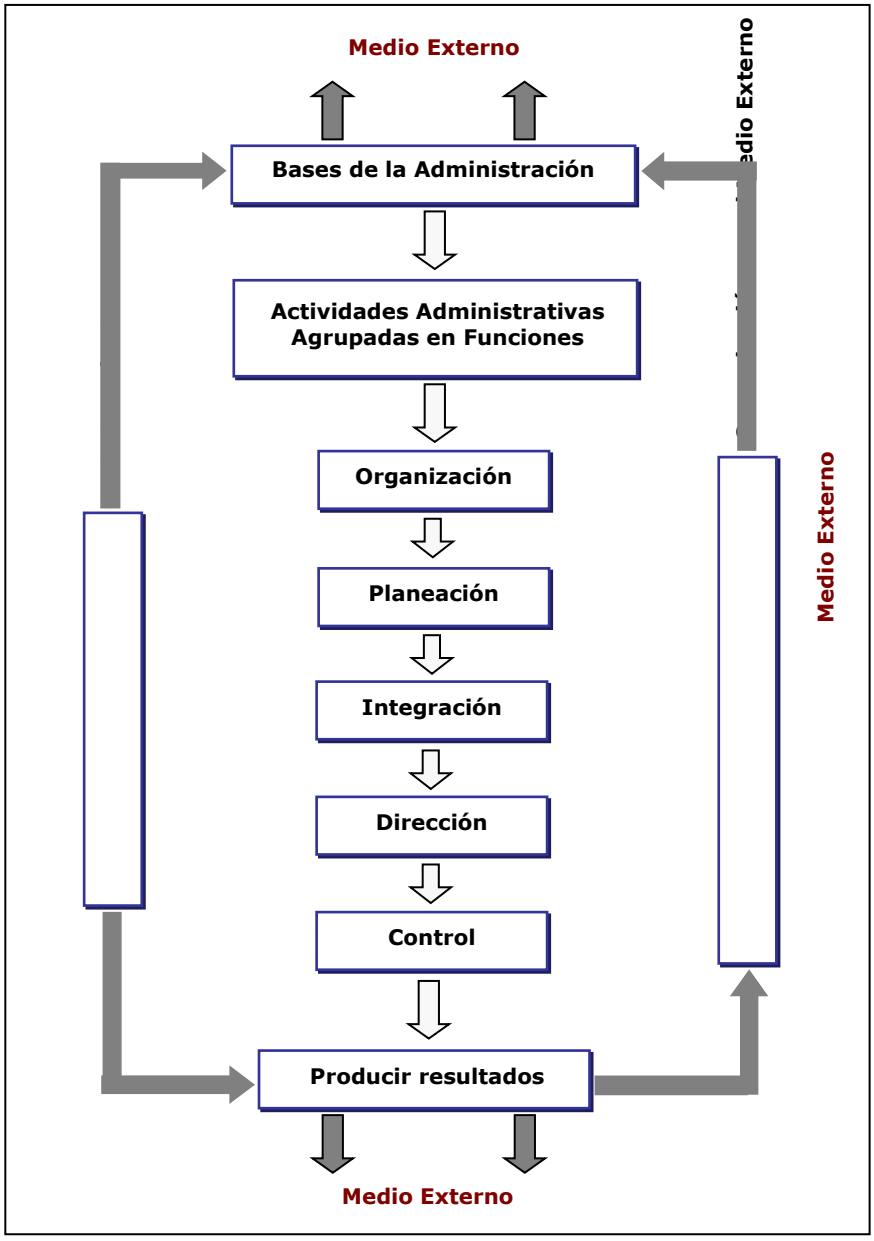


Fig. 2.1 **Enfoque de Sistemas en la Administración**

Las funciones de los administradores representan el trabajo práctico para organizar los conocimientos de la gestión, los elementos esenciales para que la gestión se desarrolle de mejor manera son:

- **Planificación:** selección de misiones y objetivos, estrategias, políticas, programas y procedimientos para lograr la toma de decisiones. La

planeación establece el puente entre el punto donde se encuentre en ese momento y el punto al cual se desea llegar en el futuro.

- **Organización:** consiste en la agrupación de las actividades necesarias para el cumplimiento de los objetivos.

- **Dirección:** implica el proceso de influir en las personas de modo que contribuyan al logro de las metas de la organización y del grupo.

- **Control**: consiste en medir y corregir la realización de las actividades con el fin de asegurar que se logren los planes y los objetivos de la empresa.

- **Integración:** implica mantener cubiertos los puestos de la estructura establecida por la organización, para fijar los requisitos de la labor por desempeñar, entre otras actividades que ayuden con su efectividad al desarrollo de la organización.

2.2 Gestión de Redes

2.2.1 ¿Qué es la Gestión de Redes?

Los recursos informáticos están interconectados mediante medios de transmisión y protocolos de comunicaciones organizados en las conocidas arquitecturas de computadoras y que se pueden denominar **"sistemas de comunicaciones"**.

Estos sistemas están implementados mediante una infraestructura de equipos de comunicaciones (módems, conmutadores, multiplexores, etc.) y facilidades de transmisión, estos son los que prestan los servicios finales, que los usuarios utilizan en la actividad diaria en las empresas y organizaciones.

El tamaño y la complejidad de las redes han ido creciendo sin cesar debido en gran parte a la aparición de las redes públicas de datos y a la creciente oferta de servicios de comunicaciones de valor agregado.

Actualmente los Sistemas de Comunicaciones prestan servicios a los usuarios utilizando redes Privadas y Redes Públicas. La interconexión entre las mismas proporciona mejores posibilidades en la provisión de servicios pero complica el control de las redes.

Habiendo conseguido la transferencia de información a través de esta complejidad de redes, surge la necesidad de gestionarlas, es decir, de controlar los recursos que le componen en términos de rendimiento, capacidad, utilización, reconfiguración, diagnósticos, planificación, entre otras.

El objetivo de la gestión de redes es mantener los sistemas de una organización en un estado óptimo de funcionamiento el tiempo máximo posible, minimizando la pérdida que ocasionará si existe una parada del mismo.

La **Gestión de Redes** es el conjunto de actividades destinadas a garantizar el control, la supervisión y la administración de los diferentes elementos que constituyen una red para que la comunicación tenga lugar.

La **gestión de red** toma la forma de seguimiento, coordinación y control de los recursos informáticos y de comunicaciones.

Las organizaciones dependen cada vez más del buen funcionamiento de los sistemas de comunicaciones dado que un gran número de los empleados utilizan recursos informáticos para la realización de su actividad diaria.

2.3 Arquitecturas de Gestión de Red

2.3.1 Modelo OSI

El modelo de gestión OSI se encuentra publicado en el conjunto de recomendaciones del Sector de Normalización de las Telecomunicaciones de la Unión Internacional de las Telecomunicaciones (**ITU-T**, *ITU Telecommunication Standarization Sector*) conocidas como Serie **X.700**.

La arquitectura OSI define los elementos básicos de los sistemas abiertos abstractos, es decir, de que manera debe verse un sistema desde el exterior.

Esta arquitectura define un objeto gestionable como la interfaz conceptual que han de presentar los dispositivos que ofrecen funciones de gestión. El proceso de supervisión y control de un objeto gestionable se realiza mediante una serie de interacciones.

Estas interacciones son de dos tipos:

- **De operación:** el gestor solicita algún dato al objeto gestionable o desea realizar alguna acción sobre él.

- **De notificación:** cuando el objeto gestionable intenta enviar algún dato al gestor como consecuencia de algún evento ocurrido en el dispositivo.

Un **"objeto gestionable"** se caracteriza además por un conjunto de atributos que son las propiedades y/o características del objeto y un comportamiento en respuesta a las operaciones solicitadas.

La comunicación entre el gestor y el objeto gestionable no es directa, se realiza mediante un intermediario: el agente de gestión (esto se corresponde con un modelo centralizado *gestor-agente*).

La función del agente es controlar el flujo de información de gestión entre el gestor y el objeto. Este control lo realiza comprobando una serie de reglas de gestión (por ejemplo que el gestor tenga la capacidad para solicitar una determinada operación), que han de cumplirse para poder realizar la operación. Estas reglas se incluyen en los datos como parte de la solicitud de una operación.

El flujo normal de información de gestión y control entre el gestor y el agente se realiza mediante el *Protocolo Común de Información de Gestión* (**CMIP**, *Common Management Information Protocol*), perteneciente al nivel de aplicación OSI.

CMIP permite que un sistema se pueda configurar para que opere como gestor o como agente. La mayoría de las realizaciones prácticas de sistemas gestionados se configuran con unos pocos sistemas operando en modo gestor, controlando las actividades de un gran número de sistemas operando en modo agente.

Cuando dos procesos se asocian para realizar una gestión de sistemas, deben establecer en qué modo va a operar cada uno de ellos (en modo agente o en modo gestor). Los procesos indican las funcionalidades y estándares de gestión que se utilizarán durante la asociación.

Otros componentes de la arquitectura de gestión OSI son:

Los objetos gestionados, en el modelo de arquitectura OSI se caracteriza por seguir la orientación a objetos, en el sentido de que la *Base de Información de Gestión* (**MIB**, *Management Information Base*) contiene más variables que el

modelo **SNMP** (tratado en **2.3.3**), constituida por objetos a los que se puede invocar operaciones y se los puede crear y destruir de manera dinámica.

Los objetos gestionados se los puede definir como una entidad intermedia entre el objeto real y el protocolo de comunicación utilizado.

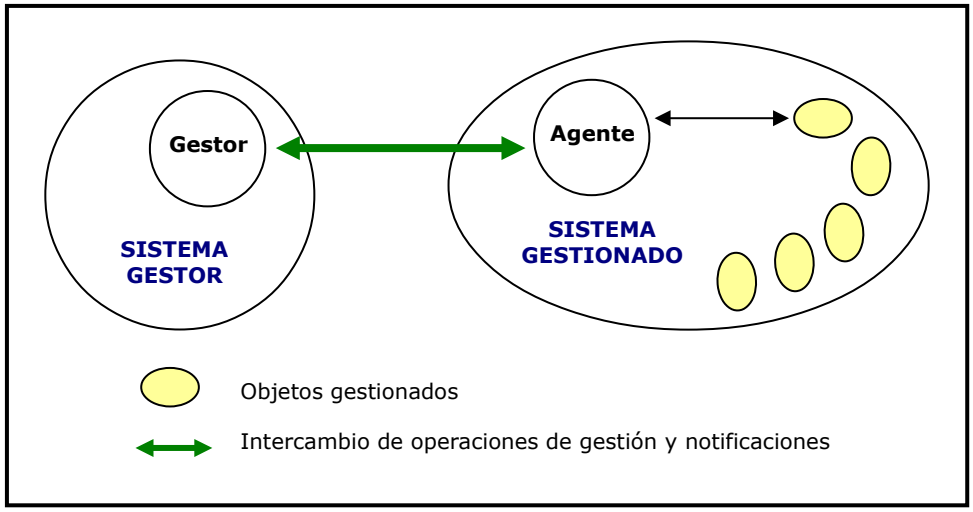


Fig. 2.2 Arquitectura de un sistema de gestión OSI

La arquitectura de información OSI se define basándose en los siguientes conceptos:

- **Modelo de Información de Gestión** (**MIM**, *Management Information Model*): modelo de la información de gestión manejada por las aplicaciones de gestión.

- **Definición de la Información de Gestión** (**DMI**, *Definition of Management Information*): define un objeto gestionado por el sistema y plantillas que pueden ser reutilizadas al definir nuevos objetos.

- **Directivas para la definición de Objetos Gestionados** (**GDMO**, *Guidelines for the Definition of Managed Objects*): proporciona métodos y guías para la definición de clases de objetos gestionados.

- **Estructura de la Información de Gestión** (**SMI**, *Structure of Management Information*): define la estructura lógica de la información de gestión OSI. Establece las reglas para nombrar a los objetos gestionables y a sus atributos. Define un conjunto de subclases y tipos de atributos que son en principio aplicables a todos los tipos de clases de objetos gestionables.

- **Base de Información de Gestión** (**MIB**, *Management Information Base*): representa la información que se está utilizando, modificando o transfiriendo en la arquitectura de los protocolos de gestión OSI. La MIB conoce todos los objetos gestionables y sus atributos. No es necesario que este centralizada físicamente en un lugar concreto, puede estar distribuida a través del sistema y en cada uno de sus niveles.

- **Servicios de Información Común de Gestión** (**CMIS**, *Common Management Information Services*): son un conjunto de reglas que identifican las funciones de una interfaz OSI entre aplicaciones, utilizado por cada aplicación para intercambiar información y parámetros. CMIS define la estructura de la información que es necesaria para describir el entorno.

Prácticamente todas las actividades de la gestión de red OSI están basadas en primitivas de servicio CMIS, entre ellas tenemos:

- **M-GET** obtiene la información de un objeto gestionado (*OG*).
- **M-SET** modifica la información contenida en un OG.
- **M-ACTION** invoca una operación sobre un OG.

- **M-CREATE** crea un nuevo OG de una clase determinada.
- **M-DELETE** elimina un OG.
- **M-CANCEL-GET** cancela una petición M-GET previa.
- **M-EVENT-REPORT** notifica un evento de manera asíncrona.

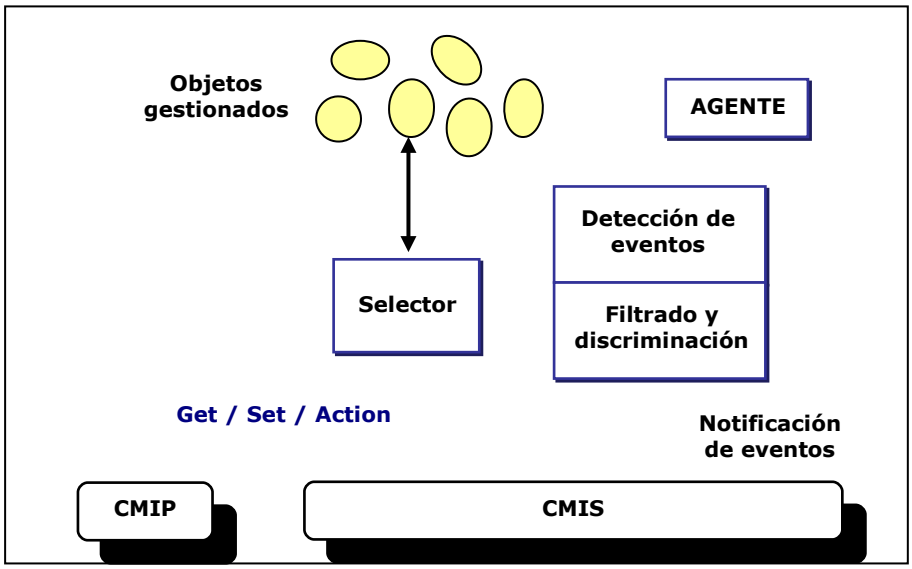


Fig. 2.3 **Arquitectura CMIS/CMIP**

Areas Funcionales de la Gestión OSI

De acuerdo con la clasificación establecida por la Organización Internacional de Estándares **(ISO**, *International Standard Organization***)**, las Areas Funcionales de la Gestión de Red se engloban en cinco grandes grupos: Gestión de Fallos y Recuperación, Gestión de la Configuración, Gestión del Rendimiento, Gestión de la Contabilidad y Gestión de la Seguridad.

1) Gestión de Fallos y Recuperación

La Gestión de Fallos y Recuperación comprende el conjunto de facilidades que permiten la detección, el aislamiento y la corrección de las operaciones anormales de las redes o sistemas de comunicaciones.

La Gestión de Fallas consiste en:

- La detección de la ocurrencia de fallas.
- El aislamiento de la causa de la falla.
- La corrección de la falla.

La Gestión de Fallas se encarga de:

- La supervisión de alarmas: indicación de fallas, su naturaleza y gravedad.
- Localización de fallas: rutinas para la localización.
- Corrección de Fallas: emitir reportes de las fallas ocurridas.

Las funciones de la Gestión de Fallas son:

- Detección e informe de problemas: este proceso, por medio de dispositivos activos y pasivos, detecta fallos e informa de los mismos a los operadores de red o a los procesos designados al efecto.
- Determinación de problemas: se encarga de aislar el problema en un recurso determinado, hardware, software, medio de transporte, o en una causa externa, para así poder identificar al personal específico responsable de su diagnóstico y resolución.
- Puenteo o recuperación de problemas: permite minimizar o eliminar el efecto del problema en la red hasta que éste pueda ser resuelto.
- Diagnóstico y resolución de problemas: determina la causa precisa del problema y las acciones requeridas para su resolución.
- Seguimiento y control del problema: conocido como ***"trouble ticketing"***, proporciona los mecanismos necesarios para el seguimiento del problema desde su detección hasta su resolución.

2) Gestión de la Configuración

El área funcional de la gestión de la configuración incluye al conjunto de facilidades pensadas para monitorizar y controlar la información necesaria para identificar física y lógicamente los recursos de red, incluyendo: nombre, dirección, estado, localización, responsable e información de identificación del producto.

Las funciones de la Gestión de la Configuración son:

- Construcción de la topología de la red de acuerdo con la visión del usuario. Incluir y dar de baja dispositivos.
- Establecimiento de los parámetros de funcionamiento, es decir, inicialización y modificación de la configuración de todos los recursos de la red.
- Mantenimiento de un inventario de los dispositivos instalados y de las líneas que los conectan.
- Gestión de la correspondencia entre nombres de dispositivos y sus direcciones de red para que los usuarios manejen los recursos según su visión de la red.
- Gestión racional de los cambios de configuración.

A continuación se exponen en más detalle el conjunto de funciones incluidas en esta área funcional:

- Definición de nuevos recursos a gestionar.
- Asignación y gestión de nombres a los recursos gestionados.
- Creación, modificación y destrucción de relaciones entre los recursos.

- Establecimiento y modificación de las características de operación.
- Borrado de recursos gestionados.
- Obtención de informes a voluntad de la identidad, condiciones de funcionamiento, etc. de los objetos gestionados.
- Reflejo en tiempo real de los cambios significativos en los modos de operación de los recursos gestionados.

3) Gestión del Rendimiento

Es el conjunto de actividades requeridas para que se evalúe continuamente los principales indicadores del rendimiento de operación de la red para verificar como son mantenidos los niveles de servicio.

La Gestión del Rendimiento consiste en:

- Colectar datos de la utilización actual de la red, dispositivos y enlaces.
- Analizar datos relevantes para visualizar tendencia de alta utilización.
- Definir límites de utilización de la red.
- Usar simulaciones para determinar como la red puede alcanzar un máximo rendimiento.

La Gestión del Rendimiento se encarga de:

- Monitoreo del desempeño.
- Control de gerencia del desempeño: manipulación de límites y parámetros de medición del tráfico en la red.
- Análisis del desempeño: procesamiento y análisis de datos, y la observación de la calidad del servicio.

Las funciones de la Gestión del Rendimiento son:

- Definición de indicadores de rendimiento:

  Indicadores como:

  - *Disponibilidad*: estado de los dispositivos gestionados.
  - *Tiempo de respuesta*: tiempo total, retardos en la red y en los nodos.
  - *Exactitud*: calidad del enlace.
  - *Grado de utilización*: mediciones dinámicas de la utilización de la red.
  - *Demanda*: utilización de recursos de red por parte de dispositivos y/o aplicaciones.
  - *Throughtput*: mide la relación entre la utilización y la demanda de un recurso de la red.

- Monitoreo del rendimiento

  Captura información de fallas, genera acciones en lugar de reacciones, almacena gran cantidad de información.

- Análisis y afinamiento

  Consiste en el análisis y evaluación del problema, proporcionar soluciones hipotéticas como el cambio de equipo o la expansión del ancho de banda, y determinar los impactos de la solución propuesta.

4) Gestión de la Contabilidad

Es el proceso de recopilación, interpretación y reportes del coste e información de carga orientada al uso de los recursos. Proporciona las herramientas

necesarias para mantener informados a los usuarios de la red sobre el grado de utilización de los recursos.

La Gestión de la Contabilidad consiste en:

- Obtener datos sobre la utilización de los recursos y servicios del sistema.
- Asociar el uso de los recursos con escalas de tarifación, combinando costos.
- Tarifar a los usuarios por el uso del sistema.

La Gestión de la Contabilidad se encarga de:

- Facturación: colección de datos, determinación de los valores contables.
- Tarifación: determinación de valores de los servicios utilizados.

Las funciones de la Gestión de la Contabilidad son:

- Identificación de los componentes de costos

  Hardware; software; servicios (voz, datos, vídeo); personal que trabaja en la red; otros (utilidades, mantenimiento, seguros, impuestos, costos de instalaciones, etc.).

- Establecer políticas de recargo a usuarios

  Reflejar una realidad económica, definir el uso de indicadores que serán la base del sistema de recargo, definición clara de las relaciones y reglas.

- Definición de procedimientos de recargos

  Los procedimientos tienen que ser definidos, desarrollados e implementados con simplicidad, exactitud, responsabilidad, deben poseer estabilidad y ser visibles.

- Procesamiento de facturas del vendedor

5) Gestión de la Seguridad

Es un conjunto de funciones que aseguran la protección de la red y sus componentes en todo aspecto de seguridad.

El punto de partida del diseño de la seguridad de un sistema es la identificación de las vulnerabilidades del mismo. Las actuales comunicaciones son vulnerables porque corren el riesgo de ser escuchadas y modificadas de forma impune. En general una comunicación es vulnerable si existe la posibilidad de que se produzca un efecto desautorizado en la misma.

La ***"Política de Seguridad"*** establece en rasgos generales lo que está o no permitido, luego cualquier posibilidad de comportamiento no autorizado en una red es un riesgo para el sistema.

La Gestión de la Seguridad consiste en:

- Identificar información delicada.
- Identificar, proporcionar seguridad y mantener los puntos de acceso.

La Gestión de la Seguridad se encarga de:

- Autentificación: integridad o autenticidad de usuarios.

- Control de accesos: asegurar que los recursos son utilizados por usuarios autorizados.

- Privacidad: secreto o confidencialidad.

Las funciones de la Gestión de la Seguridad son:

- Análisis de riesgos

  Incluyen todas las partes relevantes y vulnerables de la red.

- Evaluación de los servicios de seguridad

  - Comprobación de la autenticidad de la información.
  - Control de acceso mediante cuentas de usuario y protección de archivos y directorios.
  - Evitar el acceso no autorizado a datos.
  - Protección del análisis del flujo de tráfico.
  - Protección contra inserción, cambio y duplicación de segmentos de datos.

- Evaluación de las soluciones de gestión de seguridad

  - Encriptación de la información.
  - Utilización de claves para identificación de usuarios.
  - Control de ruteo mediante manejo de ancho de banda dinámico.

2.3.2 Modelo TMN

El término Red de Gestión de Telecomunicaciones (**TMN**, *Telecommunications Management Network*) fue introducido por el Sector de Normalización de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones (**ITU-T**, *ITU Telecommunication Standarization Sector*), y está definido en la recomendación M.3010 (define el concepto de Red de Gestión de Telecomunicaciones, su alcance, se describen las arquitecturas funcional y de información y se ofrecen ejemplos de arquitecturas físicas, además se expone un modelo de referencia funcional y se identifican conceptos para soportar la arquitectura de TMN). Aunque en un principio no hubo mucha colaboración entre los grupos de gestión de red de la ISO y el CCITT (*Comité Consultivo Internacional para Telefonía y Telegrafía*), posteriormente fueron incorporados varios conceptos del modelo OSI al estándar TMN. En concreto, se adoptó el ***"modelo gestor-agente"*** del modelo OSI.

Se siguió el paradigma de la orientación a objetos de la arquitectura OSI, se trabajó conjuntamente en el desarrollo del concepto de dominios de gestión, un aspecto diferenciador de ambos modelos consiste en la introducción, en el modelo TMN, de una red separada de aquella que se gestiona, con el fin de transportar la información de gestión.

A diferencia del modelo OSI, que define cinco áreas funcionales, el estándar TMN no entra en consideraciones sobre las aplicaciones de la información gestionada. Por el contrario, se define la siguiente funcionalidad:

- El intercambio de información entre la red gestionada y la red TMN.
- El intercambio de información entre redes TMN.

- La conversión de formatos de información para un intercambio consistente de información.
- La transferencia de información entre puntos de una TMN.
- El análisis de la información de gestión y la capacidad de actuar en función de ella.
- La manipulación y presentación de la información de gestión en un formato útil para el usuario de la misma.
- El control del acceso a la información de gestión por los usuarios autorizados.

La Arquitectura del modelo TMN se define en tres partes bien diferenciadas:

1. **Arquitectura funcional TMN**, describe la distribución de la funcionalidad dentro de la TMN, con el objeto de definir los bloques funcionales a partir de los cuales se construye la TMN (ver **Fig. 2.10**).

   Se definen cinco tipos de bloques funcionales. Estos bloques proporcionan la funcionalidad que permite a la TMN realizar sus funciones de gestión. Dos bloques funcionales que intercambian información están separados mediante puntos de referencia.

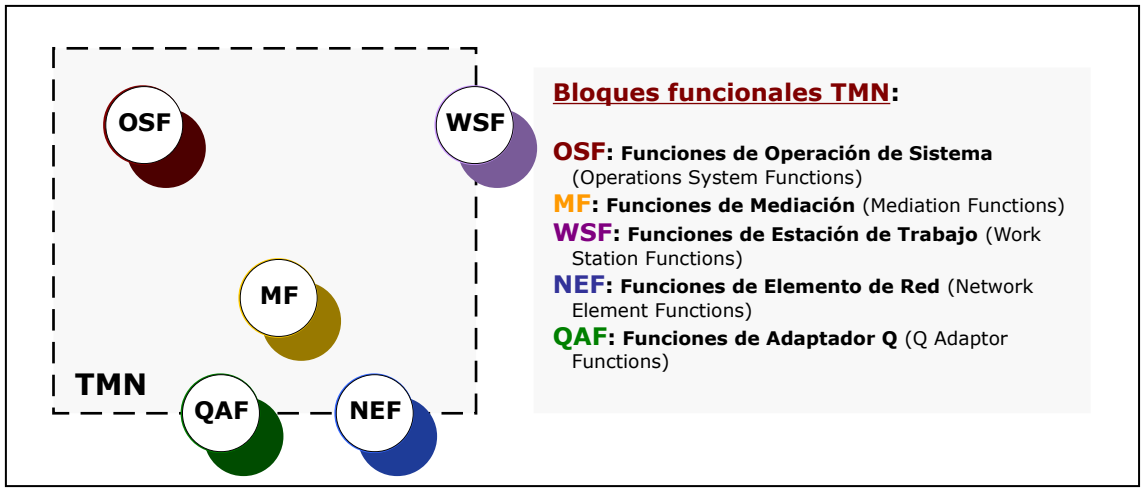


Fig. 2.4 Bloques Funcionales TMN

En la **figura 2.5** se especifican los puntos de referencia posibles entre los distintos bloques funcionales.

- El punto de referencia **x** solo aplica cuando cada Función de Operación de Sistema (**OSF**, *Operation System Function*) está en una TMN diferente.

- El punto de referencia **g** se sitúa entre la Función de Estación de Trabajo (**WSF**, *Work Station Function*) y el usuario, quedando fuera del estándar.

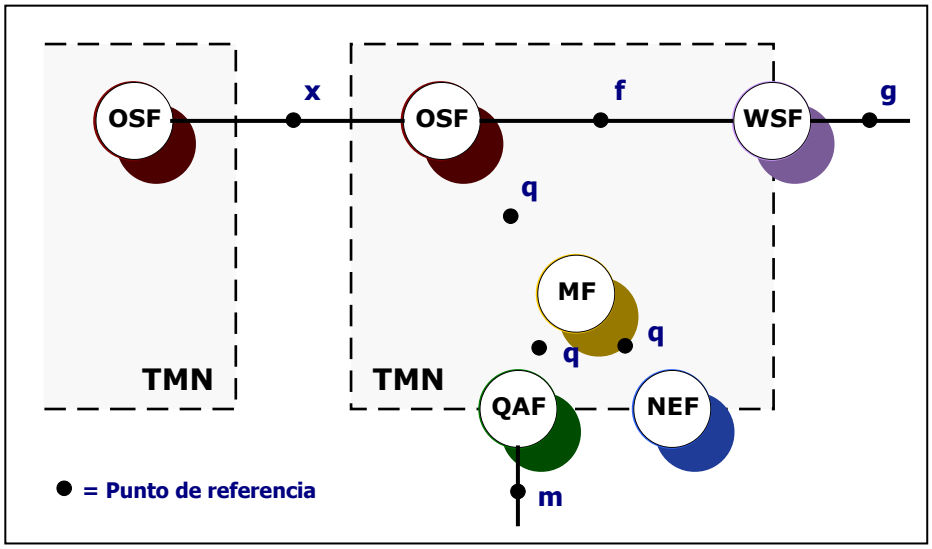


Fig. 2.5 Ejemplo de puntos de referencia entre bloques funcionales

A continuación se describen los distintos tipos de bloques funcionales:

- Función de operación de sistemas (**OSF**, *Operation System Fuction*): Los **OSF** procesan la información relativa a la gestión de la red con el objeto de monitorizar y controlar las funciones de gestión (ver **Fig. 2.6**). Cabe definir múltiples OSF dentro de una única TMN.

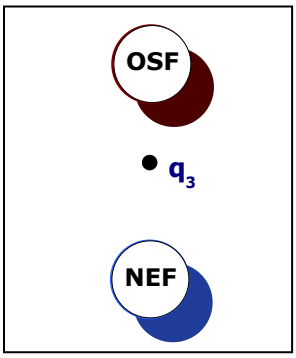


Fig. 2.6 Bloques funcionales OSF y NEF

La Función de Operación de Sistemas (**OSF**, Operation System Function) bloquea inicialmente las operaciones de gestión y recibe las notificaciones, desde el punto de vista del modelo gestor-agente (ver **Fig. 2.7**), la OSF puede verse como una función específica de la gestión.

La recomendación **M.3010**, aprobada en 1988 en Melbourne como recomendación **M.30**, define tres diferentes puntos de referencia **q**: q1, q2, q3. El punto de referencia **q3** es usado cuando la información de gestión debería ser cambiada por el protocolo de gestión de la capa de aplicación, tal como el Protocolo de Información Común de Gestión (**CMIP**, *Common Management Information Protocol*) de OSI.

Los otros dos puntos de referencia son destinados para casos en que la información de gestión deba cambiarse por medio de capas inferiores (*ejemplo*: enlace de datos) de los protocolos de gestión.

El servicio proveído para el punto de referencia **q3** se lo hace generalmente por el Servicio de Información Común de Gestión (CMIS).

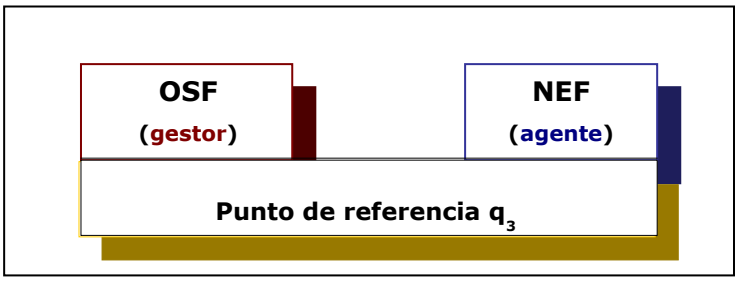


Fig. 2.7 **Relación entre OSF, NEF y q3, expresado en términos de los conceptos OSI**

- Función de estación de trabajo (**WSF**, *Work Station Function*): este bloque funcional proporciona los mecanismos para que un usuario pueda interactuar con la información gestionada por la TMN.

- Función de elemento de red (**NEF**, *Network Element Function*): es el bloque que actúa como agente, susceptible de ser monitorizado y controlado. Estos bloques proporcionan las funciones de intercambio de datos entre los usuarios de la red de telecomunicaciones gestionada.

- Función adaptador Q (**QAF**, Q Adaptor Function): este tipo de bloque funcional se utiliza para conectar a la TMN aquellas entidades que no soportan los puntos de referencia estandarizados por TMN (ver **Fig. 2.8**).

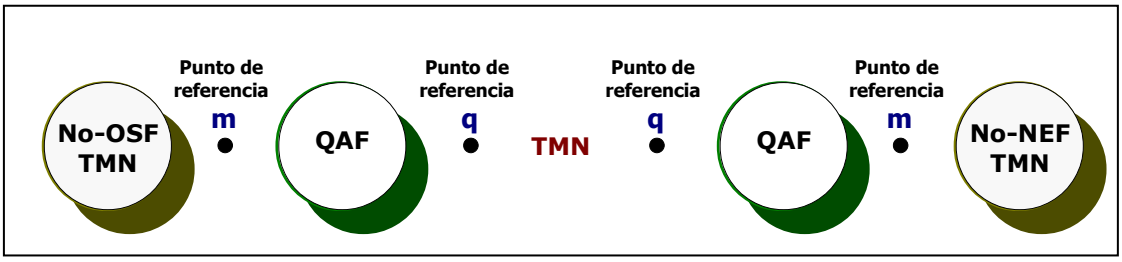


Fig. 2.8 **Funciones Adaptador Q**

- Función de mediación (**MF**, Mediation Function): se encarga de garantizar que la información intercambiada entre los bloques del tipo OSF o NEF cumple los requisitos demandados por cada uno de ellos. Puede realizar

funciones de almacenamiento, adaptación, filtrado y condensación de la información.

Cada bloque funcional se compone a su vez de un conjunto de componentes funcionales, considerados como los bloques elementales para su construcción. Estos componentes se identifican en la norma pero no están sujetos a estandarización.

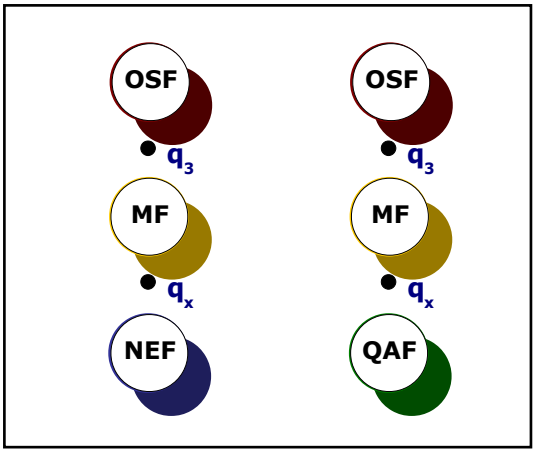


Fig. 2.9 Relación de las funciones de mediación (MF) con otros bloques funcionales TMN

2. **Arquitectura física TMN**, describe las interfaces y el modo en que los bloques funcionales se implementan en equipos físicos (ver **Fig 2.10**).

Se encarga de definir como se implementan los bloques funcionales mediante equipamiento físico y los puntos de referencia en interfaces.

TMN también define una arquitectura física, al igual que la arquitectura funcional se encuentra dentro de un equipamiento físico, la arquitectura física

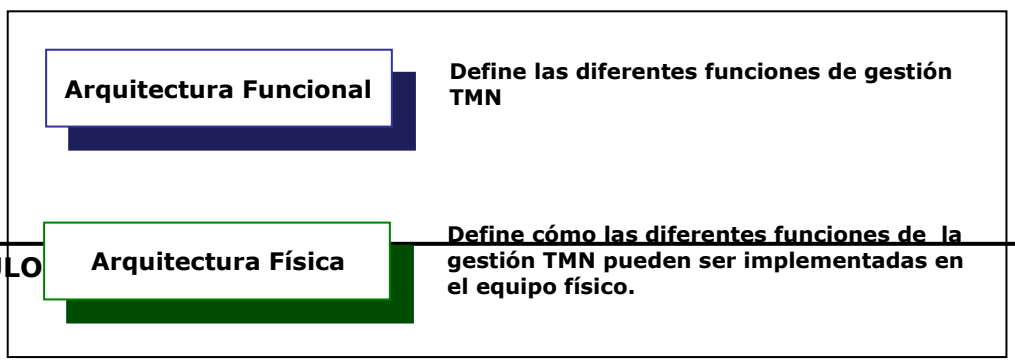


Fig. 2.10 Arquitecturas TMN

de TMN está definida por un nivel inferior de abstracción que el de la funcional.

La arquitectura física muestra como los bloques de función que deberían combinarse sobre la construcción de los bloques (equipamiento físico) y los puntos de referencia sobre las interfaces. De hecho, la arquitectura física definida como bloques de función y puntos de referencia pueden implementarse. Se debe anotar sin embargo que cada bloque de función puede contener múltiples componentes funcionales y un bloque de construcción puede implementar múltiples bloques de función.

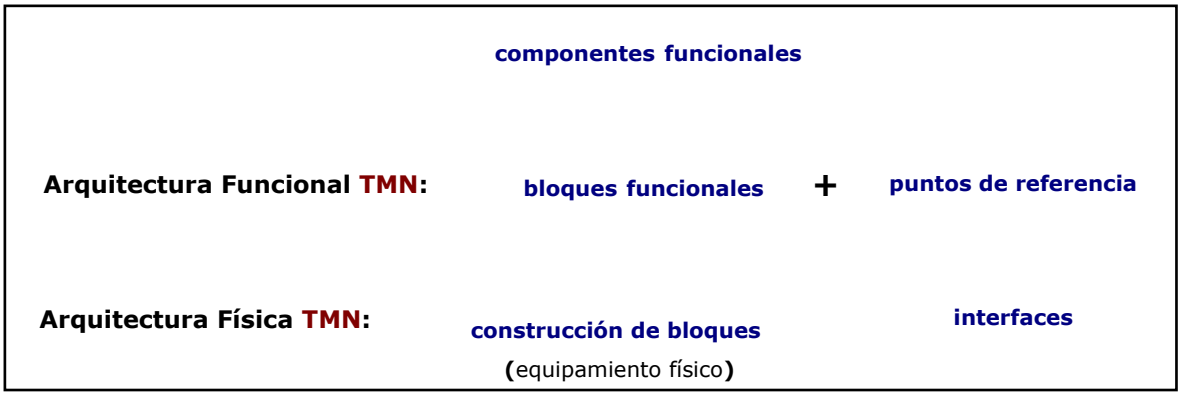


Fig. 2.11 Relación entre las Arquitecturas TMN

En la arquitectura física se construyen los siguientes bloques:

- Elemento de red (NE, Network Element).
- Dispositivo de mediación (MD, Mediation Dispositive).
- Adaptador Q (QA, Q Adaptor).
- Sistema de operaciones (OS, Operations System).
- Estación de Trabajo (WS, Work Station).
- Red de comunicación de datos (DCN, Data Communication Network).

Cada uno de estos bloques puede implementar uno o más bloques funcionales (excepto la DCN que se encarga de realizar el intercambio de información

entre bloques), pero siempre hay uno que ha de contener obligatoriamente y que determina su denominación (ver **tabla 2.1**).

NEF
Funciones de Elemento de Red **MF**
Funciones de Mediación **QAF**
Funciones de Adaptador Q **OSF**
Funciones de Operación de Sistema **WSF**
Funciones de Estación de Trabajo
NE
(elemento de red**)** Obligatorio Opcional Opcional Opcional **Opcional**
Si **OSF** o **MF** están presentes **MD**
(dispositivo de mediación**)** Obligatorio Opcional Opcional Opcional **QA**
(adaptador Q**)** Obligatorio **OS**
(sistema de operaciones**)** Opcional Opcional Obligatorio Opcional **WS**
(estación de trabajo**)** Obligatorio **DCN**
(red de comunicación de datos**)**

Tabla 2.1 Relación entre la construcción de bloques y los bloques funcionales

- Interfaces: son implementaciones de los puntos de referencia, y son comparables a las pilas de protocolos. Existe una correspondencia uno a uno entre los puntos de referencia y las interfaces, excepto para aquellos que están fuera de la TMN, es decir, los puntos de referencia **g** y **m**.

Punto de referencia:	q_x	q_3	**x**	**f**	**(g**	**m)**
interfaz:	Q_x	Q_3	**X**	**F**		

Fig. 2.12 Mapeo de puntos de referencia para cada interfaz

3. **Arquitectura lógica de niveles TMN**, sigue los principios de los modelos OSI de gestión (CMIS y CMIP) y directorio (X.500) (ver **Fig. 2.13**).

En el estándar TMN define una serie de capas o niveles de gestión mediante las cuales se pretende abordar la gran complejidad de la gestión de redes de

telecomunicación. Cada uno de estos niveles agrupa un conjunto de funciones de gestión. El estándar **LLA** (*Logic Level Architecture*) define cuáles son esos niveles y las relaciones entre ellos.

Se definen los siguientes niveles, de abajo hacia arriba como indica la **figura 2.13**:

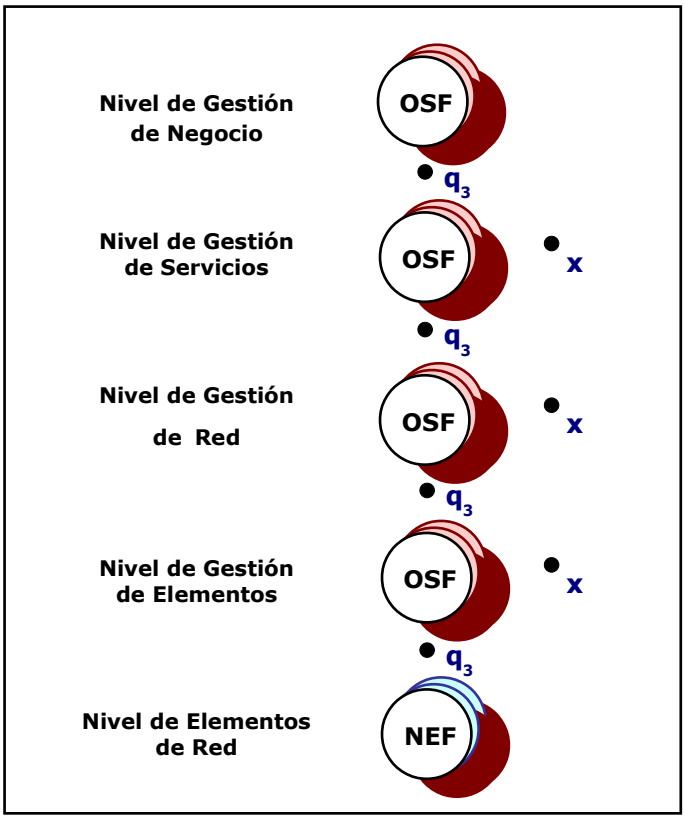


Fig. 2.13 Jerarquía funcional de la Arquitectura Lógica de Niveles TMN

- Nivel de Elementos de Red: incluye las funciones que proporcionan información en formato TMN del equipamiento de red así como las funciones de adaptación para proporcionar interfaces TMN a elementos de red no - TMN.

- Nivel de Gestión de Elementos: incluye la gestión remota e individual de cualquier elemento de red que se precise para el establecimiento de conexiones entre dos puntos finales para proporcionar un servicio dado.

Este nivel proporcionará funciones de gestión para monitorizar y controlar elementos de gestión individuales en la capa de elemento de red.

- Nivel de Gestión de Red: Incluye el control, supervisión, coordinación y configuración de grupos de elementos de red constituyendo redes y subredes para la realización de una conexión.

- Nivel de Gestión de Servicios: Incluye las funciones que proporcionan un manejo eficiente de las conexiones entre los puntos finales de la red, asegurando un óptimo aprovisionamiento y configuración de los servicios prestados a los usuarios.

- Nivel de Gestión de Negocio: Incluye la completa gestión de la explotación de la red, incluyendo contabilidad, gestión y administración, basándose en las entradas procedentes de los niveles de Gestión de Servicios y de Gestión de Red.

2.3.3 Modelo Internet (SNMP)

El organismo encargado de la estandarización de la Gestión Internet es la Fuerza de Trabajo de Ingeniería del Internet (**IETF**, *Internet Engineering Task Force*)

En 1988, el **IAB** (*Internet Activities Board*) determinó la estrategia de gestión para **TCP/IP** (*Transfer Control Protocol/Internet Protocol*). Esto significó el *nacimiento de dos esfuerzos paralelos*: la solución a corto plazo, el Protocolo Simple de Gestión de Red (**SNMP**, *Single Network Management Protocol*) y la solución eventual a largo plazo, el Protocolo de Información Común de Gestión sobre TCP/IP (**CMOT**, *CMIP Over TCP/IP*).

CMOT pretendía implantar los estándares del modelo de gestión OSI en el entorno Internet (TCP/IP). CMOT tuvo que afrontar los problemas derivados de la demora en la aparición de especificaciones y la ausencia de implementaciones prácticas. Como consecuencia de ello, la iniciativa CMOT fue paralalizada en 1992.

El Protocolo Simple de Gestión de Red (**SNMP**, *Simple Network Management Protocol*) es una ***extensión*** del Protocolo Simple de Supervisión de Pasarelas (**SGMP**, *Simple Gateway Monitoring Protocol*), que se convirtió en 1989 en el estándar recomendado por Internet.

Está dirigido a proporcionar una gestión de red centralizada que permita la **observación**, el **control** y la **gestión de las instalaciones**. Utilizando **SNMP**, un administrador de red puede direccionar preguntas y comandos a los dispositivos de la red.

SNMP se ha convertido, debido al enorme éxito que ha tenido desde su publicación, en el estándar de la gestión de redes. Prácticamente todo el equipamiento de redes puede ser gestionado vía SNMP.

Algunas de las funciones que proporciona SNMP son:

- Supervisión del rendimiento de la red y su estado.
- Control de los parámetros de operación.
- Obtención de informes de fallos.
- Análisis de fallos.

El protocolo SNMP incorpora varios elementos presentes en otros estándares como el modelo gestor-agente, la existencia de una base de datos de información de gestión (MIB) o el uso de primitivas para manipular dicha información (ver **Fig. 2.16**):

- Agente: equipamiento lógico alojado en un dispositivo gestionable de la red. Almacena datos de gestión y responde a las peticiones sobre dichos datos (ver **Fig. 2.14**).

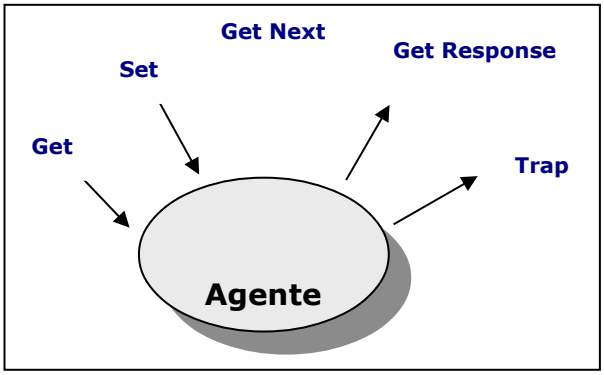


Fig. 2.14 Primitivas SNMP

- Gestor: equipamiento lógico alojado en la estación de gestión de red. Tiene la capacidad de preguntar a los agentes utilizando diferentes comandos SNMP.

- Base de Información de Gestión (**MIB**, *Management Information Base*): es una base de datos virtual de los objetos gestionables, accesible por un agente, que puede ser manipulada vía SNMP para realizar la gestión de red.

El protocolo SNMP realiza las funciones descritas anteriormente llevando información de gestión entre los gestores y los agentes.

El protocolo SNMP es un aspecto dentro de toda la estructura de gestión, compuesta de los siguientes elementos (ver **Figuras 2.15** y **2.16**):

- **Estación de Gestión de Red** (**NMS**, *Network Management Station*): es el elemento central que proporciona al administrador una visión del estado de

la red y unas funciones de modificación de este estado (puede ser una estación de trabajo o un ordenador personal).

Nodos Gestionados (**MN**, *Managed Nodes*): son elementos como los gateways, routers, etc. Estos nodos residen en el agente gestor que es el encargado de llevar a cabo las funciones requeridas por la estación gestora.

- **Protocolo de Gestión de Red** (*Protocolo SNMP*): es aquel que define la comunicación entre los nodos gestionados y las estaciones gestoras.

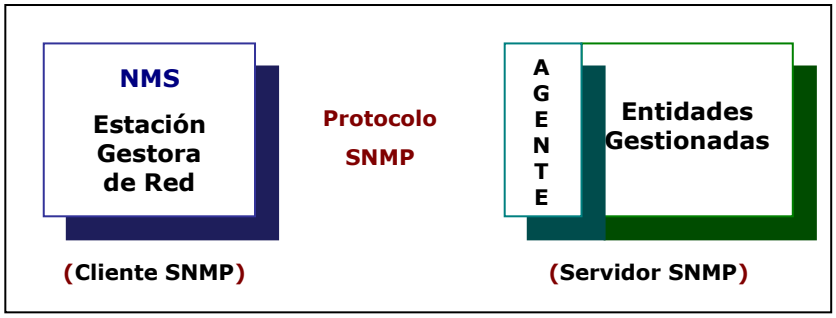


Fig. 2.15 Modelo SNMP

Algunas de las claves de flexibilidad del protocolo SNMP son el uso de las variables así como la forma de representación de los recursos, tanto lógicos como físicos.

Para cada nodo gestionado el agente SNMP proporciona una base de datos llamada **MIB** (*Base de Información de Gestión*) que es una colección de objetos, que representan de forma abstracta los dispositivos de la red y sus componentes internos. Estos objetos incluyen direcciones de red, tipos de interfaz, contadores y datos similares.

Dentro del SNMP existen cinco mandatos (ver **Fig. 2.17**):

- **Get**, obtiene las variables MIB especificas de un nodo gestionado, el agente responde con un **Get-Response** conteniendo las variables o un mensaje de error.

- **Get-Next**, obtiene la variable MIB siguiente a la especificada, el agente responde con un **Get-Response** conteniendo las variables o un mensaje de error.

- **Get-Response**, enviado por el nodo gestionado a la estación gestora como respuesta a **Get**, **Get-Next**, o **Set**.

- **Set**, enviado por la estación gestora para dar un valor determinado a la variable MIB de un nodo gestionado.

- **Trap**, enviado por el nodo gestionado a la estación gestora de forma no solicitada para informar de los eventos o cambios de estado de las variables.

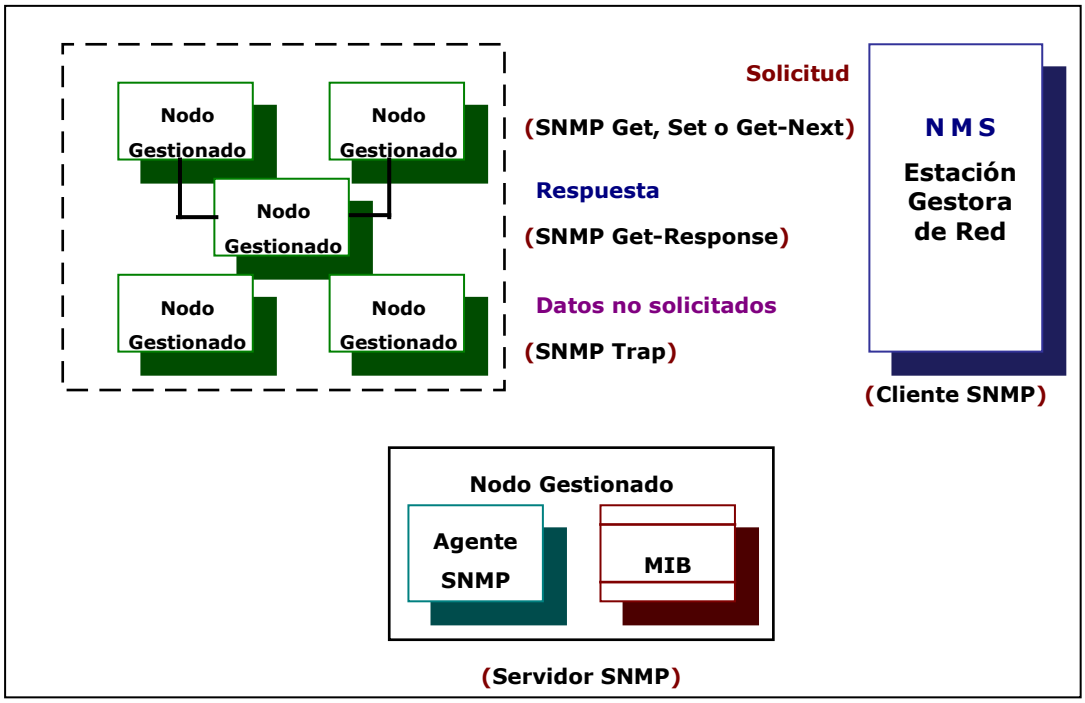


Fig. 2.16 **Protocolo SNMP**

A parte de la MIB, existe la ***"Base de Datos de Estadísticas de Red"*** (**NSD**, *Network Statistics Database*) que está en la estación de trabajo de gestión. En

esta base de datos se recoge información de los agentes para realizar funciones de correlación y planificación.

Las limitaciones de SNMP se deben a no haber sido diseñado para realizar funciones de gestión de alto nivel. Sus capacidades lo restringen a la supervisión de redes y a la detección de errores. Como todos los elementos TCP/IP, han sido creados pensando más en su funcionalidad y dejando a un lado la seguridad.

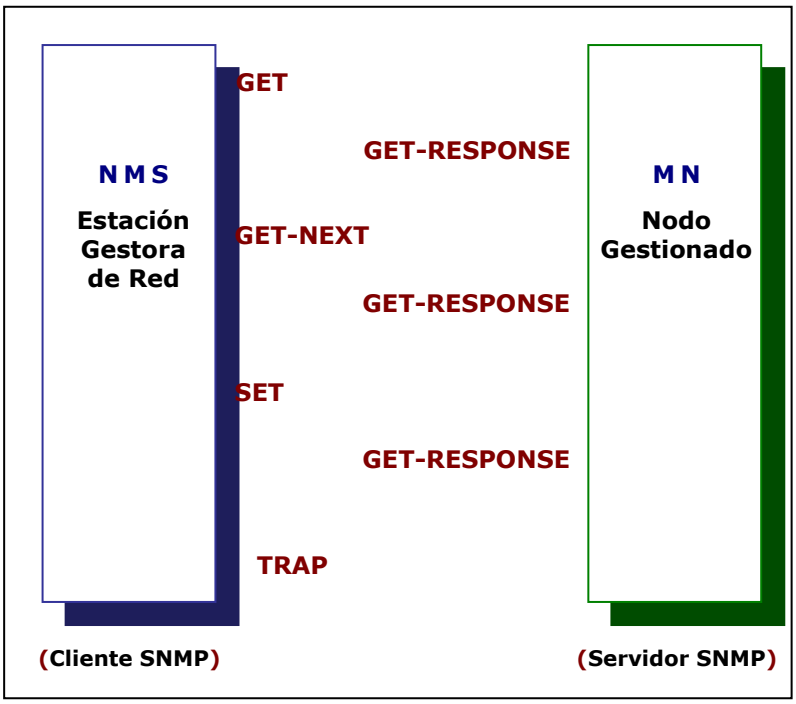


Fig. 2.17 Flujo de mandatos SNMP

- ## SNMP v2 y v3

En 1996 se publicó un nuevo estándar, el protocolo SNMPv2, resultado de una serie de propuestas para mejorar las características de SNMP. Los cambios se traducen fundamentalmente en una mejora de las prestaciones, un aumento de la seguridad y en la introducción de una jerarquía de gestión.

Las prestaciones del SNMPv2 mejoran el mecanismo de transferencia de información hacia los gestores, de forma que se necesitan realizar menos peticiones para obtener paquetes de información grandes.

En la seguridad, a diferencia de SNMP que no incorpora ningún mecanismo de seguridad, SNMPv2 define métodos para controlar las operaciones que están permitidas como privacidad, autentificación y control de acceso.

En cuanto a la gestión jerárquica:

- Cuando el número de agentes a gestionar es elevado, la gestión mediante el protocolo SNMP se vuelve ineficaz debido a que el gestor debe sondear periódicamente todos los agentes que gestiona.
- SNMPv2 soluciona este inconveniente introduciendo los gestores de nivel intermedio. Son estos últimos los que se encargan de sondear a los agentes bajo su control. Los gestores intermedios son configurados desde un gestor principal de forma que solo se realiza un sondeo de aquellas variables demandadas por este último, y solo son notificados los eventos programados.
- SNMPv2 también introduce un vocabulario más extenso, permite comandos de agente a agente y técnicas de recuperación de mensajes

Algunas de las primitivas del SNMP v2 son (ver **Fig. 2.18**):

- **GetRequest** incluye una lista de uno o más identificadores de variables cuyos valores desea conocer el gestor.
- **GetNextRequest** incluye una lista de variables, permite obtener los valores de las variables cuyos nombres siguen un orden lexicográfico.

- **GetBulkRequest** obtiene gran cantidad de información de una sola vez.
- **SetRequest** indica al agente que el gestor desea modificar el valor de una o más variables.
- **Response** emitida por el agente para enviar la información solicitada por el gestor.
- **Trap** emitida por el agente de manera asíncrona para indicar al gestor que se ha producido un evento no esperado.
- **InformRequest** emitida por el gestor para solicitar información a otro gestor.

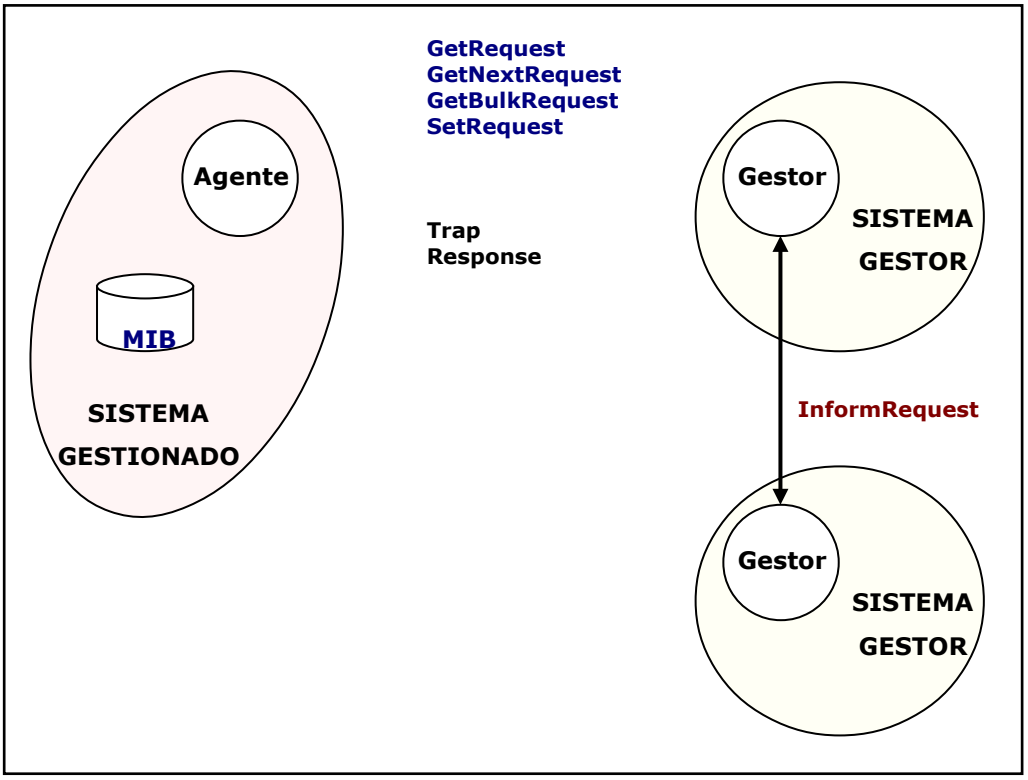


Fig. 2.18 Intercambio de primitivas SNMP v2

La información de gestión usada por el protocolo SNMP se encuentra almacenada en la MIB que contiene una gran cantidad de objetos clasificados de la siguiente manera:

- **Sistema**, contiene información sobre la entidad, como el hardware, software del sistema, versión, el tiempo de la última iniciación, la localización física, etc.

- **Interfaces**, contiene todas las interfaces por las que los nodos pueden enviar/recibir datagramas, contiene además contadores para paquetes enviados y recibidos.

- **Traducción de direcciones**, contiene información para traducir una dirección de red en una dirección de subred o física.

- **IP**, contiene información del nivel de IP, como el número de datagramas enviados, recibidos y propagados. Incluye dos tablas: la tabla de direcciones IP, que tiene la información de direccionamiento IP para la entidad y la tabla de encaminamiento IP que tiene una entrada para cada ruta actualmente conocida.

- **ICMP**, contiene estadísticas de entrada y salida del Internet Control Message Protocol.

- **TCP**, contiene información sobre las conexiones TCP, así como el número máximo de conexiones que puede soportar una entidad, etc.

- **UDP**, contiene información sobre el nivel UDP, como contadores de datagramas enviados y recibidos.

- **EGP**, estadísticas de configuración de las funciones **EGP** (*External Gateway Protocol*) soportadas, número de mensajes, contadores de error, etc.

- **Transmisión**, información específica de cada medio de transmisión.

- **SNMP**, contiene información acerca del agente SNMP, número de paquetes SNMP recibidos, número de peticiones, etc.

El proceso encargado de mantener a la MIB privada se conoce con el nombre de ***"subagente"*** o ***"agente proxy"***, y mantiene una interacción con el proceso SNMP local o remoto para comunicarse con uno o más gestores.

- **RMON**

La especificación **RMON** (*Remote MONitor, Monitorización Remota*) es una Base de datos de información de gestión (**MIB**, *Management Information Base*) desarrollada por el organismo IETF (Internet Engineering Task Force) para proporcionar capacidades de monitorización y análisis de protocolos en redes de área local (segmentos de red). Esta información proporciona a los gestores una mayor capacidad para poder planificar y ejecutar una política preventiva de mantenimiento de la red.

Las implementaciones de RMON consisten en soluciones cliente/servidor. El cliente es la aplicación que se ejecuta en la estación de trabajo de gestión, presentando la información de gestión al usuario. El servidor es el agente que se encarga de analizar el tráfico de red (ver **Anexo A**) y generar la información estadística. La comunicación entre aplicación y agente se realiza mediante el protocolo SNMP.

RMON es una herramienta muy útil para el gestor de red pues le permite conocer el estado de un segmento de red sin necesidad de desplazarse físicamente hasta el mismo y realizar medidas con analizadores de redes y protocolos. Las iniciativas se dirigen en estos momentos hacia la obtención de una mayor y más precisa información. En concreto, se trabaja en la línea de analizar los protocolos de nivel superior, monitorizando aplicaciones concretas y comunicaciones extremo a extremo (niveles de red y superiores). Estas

facilidades se incorporarán en versiones sucesivas de la especificación (RMON II).

2.4 Normas y estándares aplicables a la Gestión de Redes

Las normas y estándares aplicables a la gestión de redes se muestran a continuación:

GESTION DE INTERCONEXION DE SISTEMAS ABIERTOS (Gestión OSI)	Recomendación
Marco y Arquitectura de la Gestión de Sistemas:	
Marco de la Gestión OSI – Arquitectura de Gestión OSI	**ITU-T X.700**
Visión General de la Gestión de Sistemas OSI	**ITU-T X.701**
Servicio y Protocolo de Comunicación de Gestión:	
Servicio Común de Información de Gestión (CMIS)	**ITU-T X.710**
Protocolo Común de Información de Gestión (CMIP)	**ITU-T X.711**
Estructura de la Información de Gestión:	
Modelo de Información de Gestión	**ITU-T X.720**
Definición de la Información de Gestión	**ITU-T X.721**
Directrices para la Definición de Objetos Gestionados (GDMO)	**ITU-T X.722**
Información de Gestión Genérica	**ITU-T X.723**
Directrices para la implantación de Proformas relacionadas con la Gestión OSI	**ITU-T X.724**
Modelo General de Relación	**ITU-T X.725**
Funciones de Gestión de Sistemas:	
Función de Gestión de Objetos	**ITU-T X.730**
Función de Gestión de Estados	**ITU-T X.731**
Atributos para la Representación de Relaciones	**ITU-T X.732**
Función Señaladora de Alarmas	**ITU-T X.733**
Función de Gestión de Informes de Evento	**ITU-T X.734**
Función de Control de Archivos de Registro Cronológico	**ITU-T X.735**
Función Señaladora de Alarmas de Seguridad	**ITU-T X.736**
Categorías de Prueba de Confianza y de Diagnóstico	**ITU-T X.737**
Función de Sumario	**ITU-T X.738**
Objetos Métricos y Atributos	**ITU-T X.739**
Función de Pista de Auditoría de Seguridad	**ITU-T X.740**
Objetos y Atributos para el Control de Acceso	**ITU-T X.741**
Función de Cómputo de Utilización para la Contabilidad	**ITU-T X.742**
Función de Gestión del Tiempo	**ITU-T X.743**
Función de Gestión del Soporte Lógico	**ITU-T X.744**
Función de Gestión de Prueba	**ITU-T X.745**
Función de Planificación	**ITU-T X.746**
Función de Monitorización del Tiempo de Respuesta	**ITU-T X.748**

Tabla 2.2 Normas y estándares aplicables a la Gestión OSI

GESTION DE LA RED DE GESTION DE LAS TELECOMUNICACIONES (Modelo TMN)	Recomendación
Arquitectura del Modelo TMN:	
Visión de Conjunto de las Recomendaciones Relativas a la Red de Gestión de las Telecomunicaciones	**ITU-T M.3000**

Principios para una Red de Gestión de las Telecomunicaciones	**ITU-T M.3010**
Consideraciones sobre una Red de Gestión de las Telecomunicaciones	**ITU-T M.3013**
Metodología de Especificación de Interfaces TMN:	
Metodología de especificación de interfaz de la Red de Gestión de las Telecomunicaciones.	**ITU-T M.3020**
Modelos y Catálogo de Información de Gestión:	
Modelo Genérico de Información de Red	**ITU-T M.3100**
Catálogo de Información de Gestión de la Red de Gestión de las Telecomunicaciones	**ITU-T M.3180**
Servicios de Gestión:	
Introducción a los Servicios de Gestión de las Telecomunicaciones	**ITU-T M.3200**
Requisitos de la Interfaz F de la Red de Gestión de las Telecomunicaciones	**ITU-T M.3300**
Funciones de Gestión:	
Funciones de Gestión de la Red de Gestión de las Telecomunicaciones	**ITU-T M.3400**
Protocolos de Comunicación:	
Perfiles de Protocolo de capa inferior para las Interfaces Q3 y X	**ITU-T Q.811**
Perfiles de Protocolo de capa superior para las Interfaces Q3 y X	**ITU-T Q.812**
Servicios de Gestión de Sistemas y Mensajes de Gestión:	
Descripción de la etapa 2 y la etapa 3 para la interfaz Q3: **Vigilancia de Alarmas**	**ITU-T Q.821**
Descripción de la etapa 1, la etapa 2 y de la etapa 3 para la interfaz Q3: **Gestión de la calidad de funcionamiento**	**ITU-T Q.822**

Tabla 2.3 **Normas y estándares aplicables a la Gestión TMN**

GESTION INTERNET (**Modelo SNMP**)	**Recomendación**
Recomendaciones del IAB (Internet Activities Board) para el desarrollo de estándares de gestión de red para Internet.	**RFC 1052**
Base de Información de gestión para Redes basadas en TCP/IP	**RFC 1066**
Estructura e Identificación de la Información de Gestión para Redes basadas en TCP/IP	**RFC 1155**
Protocolo SNMP	**RFC 1157**
Definición concisa de MIB	**RFC 1212**
Base de la Información de Gestión para Redes basadas en TCP/IP: MIB-II	**RFC 1213**
Definición de Traps para uso en SNMP	**RFC 1215**
Estructura de información de gestión SNMPv2	**RFC 1902**
Nomenclatura en SNMPv2	**RFC 1903**

Reglas de conformidad para SNMPv2	**RFC 1904**
Operaciones del protocolo SNMPv2	**RFC 1905**
Mapeados de transporte SNMPv2	**RFC 1906**
MIB para SNMPv2	**RFC 1907**
Compatibilidad entre las versiones 1 y 2 de SNMP	**RFC 1908**
Arquitectura de las plataformas SNMP	**RFC 2271**
Procesamiento y envío de mensajes en SNMP	**RFC 2272**
Aplicaciones SNMPv3	**RFC 2273**
Modelo de seguridad basado orientada al usuario en SNMPv3	**RFC 2274**
Modelo de control de acceso SNMP	**RFC 2275**

Tabla 2.3 **Normas y estándares aplicables a la Gestión Internet**

Referencias Bibliográficas

1. **KOONTZ, O'DONELL, WEIHRICH., "Elementos de Administración"**, Editorial Mc-Graw Hill, Cuarta Edición.
2. **REINOSO Víctor., "El Proceso Administrativo de las Empresas"**, Editorial Pedagógica, Cuarta Edición.
3. **GARCIA Jesús., "Redes para Procesos Distribuidos"**, Editorial RA - MA, Madrid España.
4. **TANENBAUM Andrew., "Redes de Computadoras"**, Tercera Edición, Prentice Hall Hispanoamericana, S. A.
5. **PRAS Aiko, VAN-BEIJNUM Bert y SPRENKELS Ron., "Introduction to TMN"**, CTIT Technical Report 99-09, University of Twente – The Netherlands, April 1999.
6. **PRAS Aiko., "SNMP Goals",** Slides, University of Twente – The Netherlands, 2000.
7. **PRAS Aiko., "Network Management Standards"**, Slides, University of Twente – The Netherlands, 2000.
8. **DaSILVA Luis., "Network Management"**, Slides, University of Virginia, Virginia – USA, 1996.
9. **STALLINGS William., "SNMP, SNMPv2, and RMON Practical Network Management"**, Segunda Edición, Addison Wesley Professional Computing and Engineering 1996.
10. **HARNEDY Sean., "Total SNMP, Exploring the Simple Network Management Protocol"**, Segunda Edición, Editorial Prentice Hall, 1998.

CAPITULO III

SISTEMAS DE GESTION DE RED

INTRODUCCION

La gestión de redes se está convirtiendo en un elemento esencial para asegurar la disponibilidad tanto física como lógica de las redes locales. La complejidad de las actuales redes impone la necesidad de utilizar sistemas de gestión capaces de controlar, administrar y monitorear redes locales y extensas, dispositivos de interconexión, servidores y sus clientes.

En la actualidad existen diferentes niveles en la concepción de las herramientas de ayuda a la gestión, cada uno de estos niveles permite atender una problemática particular del entorno de redes que en general no están integrados en un único sistema capaz de proporcionar una visión completa de los subsistemas que conforman las redes.

La tendencia en la evolución de la tecnología de gestión de redes se encamina hacia el desarrollo de productos integrados capaces de gestionar conjuntamente subsistemas de voz, datos e imagen en sus diferentes niveles: medio físico de transmisión, redes, aplicaciones, etc.

3.1 ¿Qué es un Sistema de Gestión de Red?

Un sistema de gestión de red (SGR) es un conjunto de dispositivos físicos y programas informáticos, mediante los cuales se puede controlar y supervisar el estado y funcionamiento global de una red de área local, metropolitana, extendida o de una interconexión entre ellas, y en particular, el estado y funcionamiento de algún componente de la red.

Los elementos que pueden ser objeto de control por estos sistemas son:

- Redes y subredes.
- Cableado.
- Equipos de interconexión.
    - Concentradores.
    - Repetidores.
    - Puentes.
    - Dispositivos de encaminamiento (routers).
- Equipos finales.
    - Hosts.
    - Terminales.
    - Computadoras personales (PC).
    - Estaciones de trabajo.
    - Servidores.

3.2 Funcionalidades básicas de un SGR

A continuación se describen las funciones básicas que contempla un sistema de gestión de red, dependiendo del tipo de red en dónde se utilice (redes pequeñas, medianas y/o grandes).

3.2.1 SGR para redes pequeñas

En redes con pocos usuarios, con un bajo número de dispositivos de red, es suficiente con un sistema de gestión que ofrezca las funciones básicas de supervisión:

- Supervisión y presentación en tiempo real de los componentes individuales de la red.
- Presentación de la información de la configuración.
- Representación gráfica de los nodos instalados en la red.
- Indicación del estado de los componentes individuales (cuáles están activos y cuáles inactivos).
- En caso de avería, indicación del tipo de ésta.
- Notificación automática de errores.
- Posibilidad de acceso automático a los elementos de la red desde la consola de gestión de red.
- Filtrado de alarmas.
- Supervisión y determinación de los valores de rendimiento para la totalidad de la red, así como en los diversos componentes de la red.
- Modificación de la configuración de la red y establecimiento de los derechos de accesos a los diversos sistemas.

- Aislamiento de errores de equipo físico respecto a los errores de equipo lógico.

Es importante que los sistemas de gestión sean fáciles de instalar, operar, y que cuenten con interfaz gráfica (menús, iconos, campos de texto, ayudas, etc.). Es conveniente que se presenten los resultados de forma comprensible y que los procedimientos de consulta sean sencillos.

3.2.2 SGR para redes medianas y grandes

En redes de mayor complejidad, al estar formadas por diferentes tipos de redes con diferentes protocolos y con elementos de diversos fabricantes, son necesarias funciones de gestión más avanzadas.

A las funciones descritas anteriormente hay que añadir las siguientes:

- Capacidad de supervisar el rendimiento y generar estadísticas dando una valoración de los resultados.
- Evitar averías, pérdidas de rendimiento y problemas de configuración mediante políticas de gestión preventivas.
- Recuperación automática ante fallos.
- Proveer los mecanismos avanzados para la seguridad de la red y de los datos.
- Capacidad para representar gráficamente en tiempo real la totalidad de la red, partes de la misma y los sistemas conectados en cada punto, de forma que la gestión no se convierta en una tarea excesivamente compleja.
- Capacidad para supervisar desde una única estación la totalidad de los tipos de red que puedan existir (Ethernet, Token Ring, FDDI, etc.).

- Posibilidad de intercomunicación local y remota con cualquier elemento de la red.
- Proporcionar interfaces con otros entornos.
- Recogida y análisis de datos de gestión.
- Escalabilidad del sistema de gestión para responder adecuadamente al crecimiento de la red.
- Capacidad para integrar equipos de múltiples fabricantes y que soportan diversos protocolos.

3.3 Componentes de un SGR

Los componentes de un sistema de gestión de red son los siguientes:

- **Objeto gestionable (OG):** representa cualquier dispositivo físico o lógico de la red y el equipamiento lógico relacionado con él que permita su gestión.
- **Agente:** es el equipamiento lógico de gestión que reside en el objeto gestionable.
- **Protocolo:** utilizado por el agente para pasar información entre el objeto gestionable y la estación de gestión.
- **Objeto ajeno:** se define como un objeto gestionable que utiliza un protocolo ajeno, es decir un protocolo distinto al de la estación de gestión.
- **Agente Conversor:** actúa de conversor entre el protocolo ajeno y el protocolo utilizado por la estación de gestión.
- **Estación de Gestión:** está formada por varios módulos o programas corriendo en una estación de trabajo o computador personal.

La relación que existe entre los diferentes componentes de un SGR se representa en el siguiente diagrama:

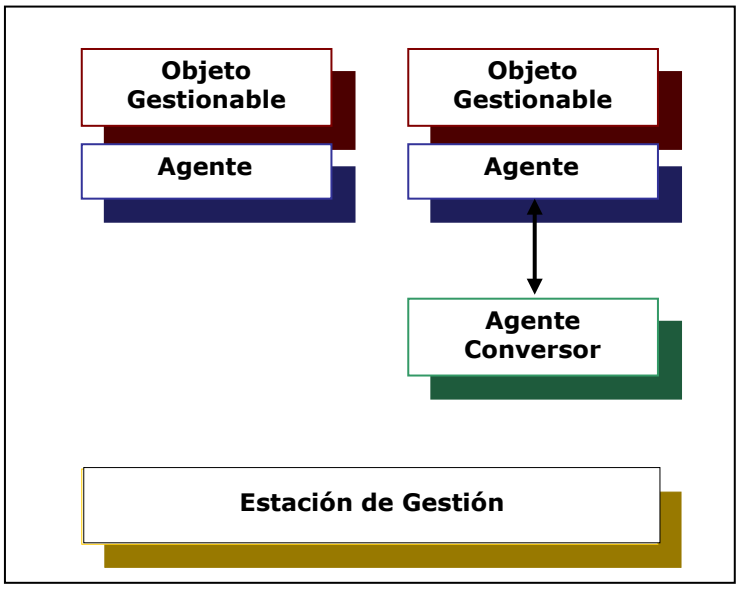


Fig. 3.1 Componentes de un SGR

A continuación se hace una descripción de los ***componentes de la estación de gestión***:

- **Interfaz de usuario:** es la interfaz entre el usuario y el sistema puede ser en modo carácter o gráfico.
- **Base de datos:** mantiene cualquier información de la red (descripciones de diferentes parámetros, configuración de contadores...), almacenando el historial de eventos y permitiendo la realización de seguimientos.
- **Programa monitor:** supervisa las condiciones actuales y permite la inspección futura. Visualiza las alarmas activadas por los agentes, y realiza actualizaciones mediante sondeos regulares.
- **Arranque y configuración:** comprueba que cada estación pueda ser atendida enviándole los parámetros actuales de configuración y el equipamiento lógico de arranque.

- **Protocolo de gestión:** controla las operaciones de gestión entre el gestor y el agente.

La estación de gestión puede acceder a los objetos gestionables de cuatro maneras diferentes:

1) **En banda** (***In-band***): la gestión del objeto se realiza utilizando la red.

2) **Fuera de banda** (***Out-of-band***): el sistema de gestión accede a los objetos gestionables a través de otros canales. Esto se puede realizar mediante un terminal conectado directamente a un puerto del objeto gestionable o que el objeto gestionable tenga algún tipo de visualizador o panel de control.

3) **Remotamente:** la gestión se realiza desde otra estación que no es la estación principal de gestión. Existen varias posibilidades:

   Mediante una estación adicional operadora que permite a varios operadores gestionar todo el sistema o partes de él.

   Utilizando una estación remota conectada a otro segmento de la red que da servicio a estaciones locales.

   Empleando un terminal remoto conectado mediante un modem.

   Un dispositivo de gestión dedicado que puede llamar al operador a través de un servicio de "buscapersonas" o correo electrónico.

4) **El sistema de gestión puede ser un elemento dentro de un gran sistema** supervisado por un gestor de sistemas.

3.4 Arquitectura Funcional de un SGR

Los Sistemas de Gestión de Red poseen cuatro niveles de funcionalidad. Cada nivel tiene un conjunto de tareas definidas que permiten proporcionar, formatear o recolectar datos necesarios para gestionar los objetos.

3.4.1 Objetos Gestionados

Son los dispositivos, sistemas y/o cualquier dispositivo que requiera de alguna forma de monitoreo o gestión. Es importante hacer notar que el objeto gestionado no debe ser necesariamente un equipo, sino que debe ser tomado en cuenta como una función que se proporciona en la red.

3.4.2 Sistemas de Gestión de Elementos

Permite administrar una porción o segmento específico de la red. Pueden gestionar líneas asíncronas, multiplexores, PBX's, sistemas propietarios, o aplicaciones determinadas.

3.4.3 Gestor de Sistemas de Gestión

Integran la información asociada con varios sistemas gestores de elementos, usualmente ejecuta una correlación de alarmas entre los diversos gestores de elementos. En estos sistemas se debe recolectar la información necesaria acerca de la fuente (objeto gestionado), reducirla a algo significativo y presentarla en la consola central para su análisis.

3.4.4 Interfaz de Usuario

Es la parte principal al desarrollar un SGR, ya que permitirá visualizar: alarmas en tiempo real, alertas o gráficas de análisis de tendencia y/o informes. La información obtenida debe ser difundida a todos los miembros de la organización para mantenerlos informados y para establecer una comunicación con los equipos.

Los datos no significan nada si no se usan para tomar decisiones adecuadas sobre la optimización y funcionalidad de los sistemas.

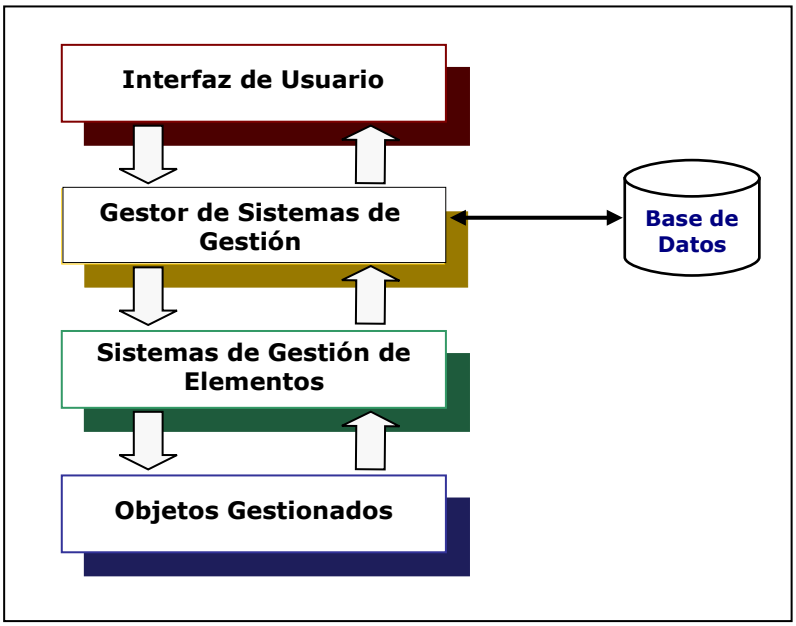


Fig. 3.2 Niveles de Funcionalidad de los SGR

3.5 Tendencias Tecnológicas y del Mercado

Las redes de comunicaciones de datos se han convertido en un componente fundamental dentro de la infraestructura corporativa, imponiendo a su vez unas exigencias muy altas a los sistemas de gestión de dichas redes. Las plataformas de gestión actuales se quedan cortas a la hora de responder a estas necesidades, especialmente cuando se aplican a redes a gran escala y en aplicaciones críticas.

A continuación se analizan las principales tendencias que se detectan en el segmento de la gestión de redes para dar solución a estos problemas.

3.5.1 Sistemas de Gestión de Red Distribuidos

Con el fin de evitar que toda la información de gestión confluya en un único puesto central, la tendencia hoy en día se dirige hacia la distribución de la inteligencia y la información por toda la red. Se pretende de este modo simplificar la gestión por medio de la automatización, de forma que las decisiones básicas se tomen cerca del origen del problema. Mediante la gestión distribuida es posible controlar redes de gran extensión de una manera más efectiva, dispersando entre varias estaciones de gestión las tareas de monitorización, recogida de información y toma de decisiones (ver **Fig. 3.3**).

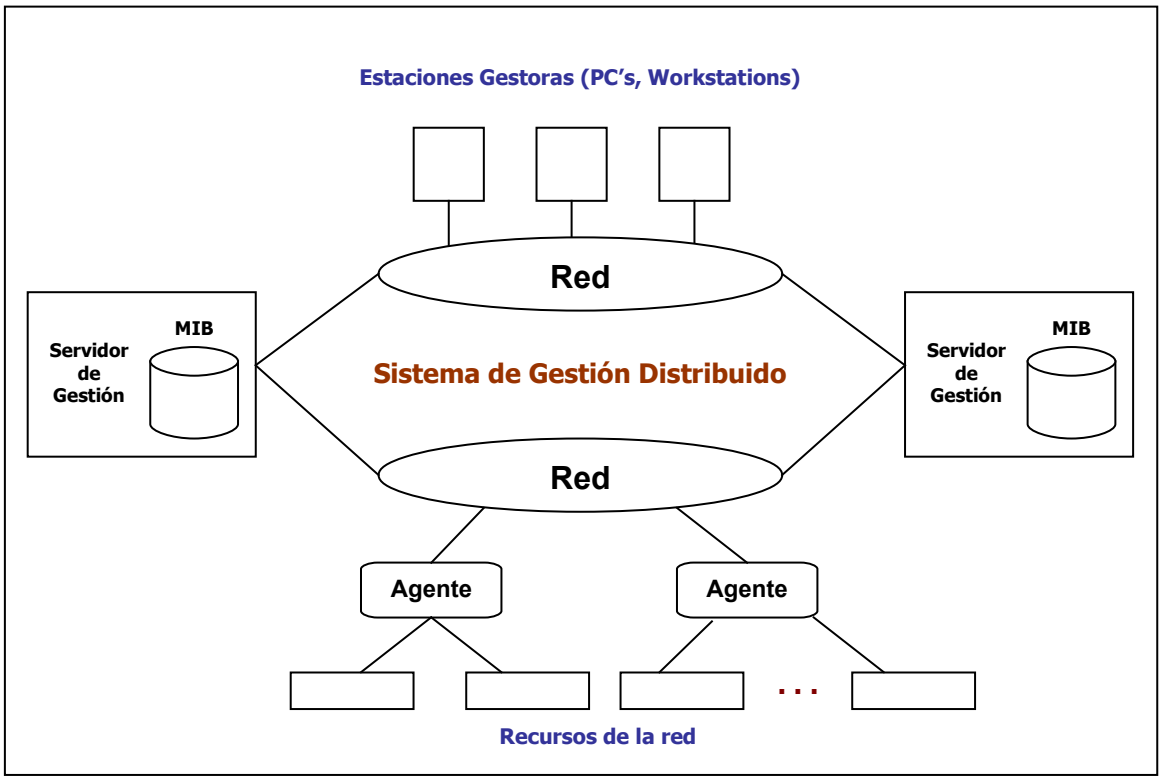


Fig. 3.3 Sistema de Gestión de Red Distribuido

La funcionalidad básica que ha de ofrecer un sistema distribuido es la siguiente:

- Escalabilidad para poder satisfacer las necesidades de gestión de redes de complejidad creciente en recursos y en información almacenada.
- Capacidad para distribuir entre distintas estaciones remotas de la red las funciones de supervisión, recogida de datos y sondeo de estado.

- Capacidad para gestionar entornos enormemente heterogéneos en el tipo de recursos de red y sistemas que los componen.
- Alta disponibilidad del sistema de gestión y tolerancia a fallos de componentes.
- Capacidad para incorporar nuevos servicios e integrarlos con los existentes.
- Capacidad para interoperar con diversos entornos.

En esta línea se están realizando esfuerzos para integrar la arquitectura de intermediario de petición de objetos común (**CORBA**, *Common Object Request Broker Architecture*) en los modelos de gestión tradicionales (CMIP/SNMP). CORBA es más potente que SNMP y menos complejo que CMIP. A esto se añade la ventaja que supone su proximidad a C++ y Java, dos lenguajes de gran difusión.

La mayor dificultad que presenta la integración de CORBA con los sistemas tradicionales de gestión es el modelo de objetos. **SNMP es completamente no orientado a objetos** mientras que CMIP, a pesar de serlo, utiliza una aproximación que difiere mucho de la empleada en CORBA.

A la hora de integrar CORBA y SNMP la opción natural es la adopción de una estrategia de pasarela (gateway) que mapee los paquetes SNMP en tipos de datos del lenguaje de definición de interfaz de CORBA (**IDL**, *Interface Definition Language*).

En el caso de CMIP se han planteado dos aproximaciones posibles:

- La estrategia de pasarela, similar a la seguida en el caso anterior y que consiste en mapear cada objeto del modelo CMIP (GDMO) y cada operación

dentro del entorno CORBA. La desventaja de esta aproximación radica en que, al existir una correspondencia uno a uno entre uno y otro entorno, no se obtiene ningún valor añadido de la integración.

- La aproximación mediante la definición de objetos abstractos. En este caso, un grupo de objetos del entorno CMIP se mapea mediante un único objeto CORBA, el cual representa entidades de gestión de nivel superior. Mediante este modelo se saca el mejor partido de ambas tecnologías.

CORBA también se perfila como alternativa de implantación de los objetos de nivel de servicio del modelo TMN, todavía por definir.

3.5.2 Sistemas de Gestión de Red Orientados a Servicios

La aproximación tradicional a la problemática de la gestión de redes se ha centrado en los dispositivos de red. Esto ha dado lugar en muchos casos, a situaciones en las que a pesar de mantener un alto nivel de rendimiento en los componentes aislados, no se obtenía la calidad del servicio requerido. En gran medida esto se debe a que resulta difícil establecer una conexión entre la gestión de dichos componentes de red y los procesos de negocio a los que están dando soporte dentro de la empresa.

La arquitectura de gestión de redes TMN, que contempla en su modelo de niveles de gestión una capa específica de gestión de negocio, parece la mejor posicionada para dar respuesta a estas necesidades.

3.5.3 Sistemas de Gestión de Red basados en Web

El gran crecimiento de Internet y la introducción en las redes empresariales de las tecnologías que le son propias, está llegando también al ámbito de la gestión de redes. Mediante la adopción de este paradigma se posibilita un acceso universal a los sistemas de gestión desde cualquier plataforma que soporte los estándares de Internet (HTML, Java).

En esta línea, los fabricantes de dispositivos de red (routers, conmutadores, etc.) están integrando en sus equipos el software que permite actuar como servidores web. Del mismo modo, se están realizando esfuerzos para la definición de nuevos estándares de gestión que, integrando protocolos como SNMP, HTTP y otros en una misma arquitectura, permita la gestión desde cualquier plataforma.

Los esfuerzos para definir un interfaz programático de gestión basado en Java, también se enmarcan dentro de esta estrategia unificadora. Se trata en este caso de aprovechar la característica de que los módulos de software desarrollados en este lenguaje puedan ser ejecutados en cualquier plataforma.

3.5.4 Sistemas de Gestión de Red Inteligentes

Los nuevos sistemas de gestión de red están basados en desarrollos de inteligencia artificial, de forma que el sistema de gestión permita descargar de trabajo al administrador de la red. Existen dos técnicas básicas de inteligencia artificial que pueden emplearse en la gestión de redes:

- **Sistemas Expertos:** los sistemas expertos de gestión de red simulan el proceso humano de toma de decisiones, aplicando una serie de reglas para escoger la mejor respuesta a un conjunto de circunstancias o eventos. La base de conocimiento y las reglas que utiliza un sistema experto están suministrados por seres humanos, y deben adaptarse a cada red concreta

antes de poder usarse con confianza. Estos sistemas no son, por el momento, capaces de aprender por sí mismos cómo gobernar una red, pero han mejorado mucho las capacidades de los gestores de la red.

- **Modelado Inductivo:** cada parte del sistema se modela por separado, representándola mediante estructuras de datos y código que representa la función del elemento. Cada elemento interacciona con los demás intercambiando señales y datos. Para realizar este modelado se utiliza la tecnología de orientación a objetos. La característica de herencia de la orientación a objetos permite la creación de nuevos objetos basados en los ya existentes. A los datos se les asocian deducciones que se activan cuando se produce un cambio en sus valores. Los eventos activan deducciones que reaccionan con los modelos de los elementos la red, originando otras deducciones sobre el nuevo estado de la red. La estación de gestión no tiene conocimiento de todos los eventos posibles, sólo responde por deducción a cada nuevo conjunto de condiciones.

3.6 Aspectos Técnicos en el Proceso de Adquisición de SGR

Con el propósito de que el proceso de adquisición de un SGR se realice de una manera versátil para el comprador, se han propuesto los siguientes aspectos:

Se realiza en primer lugar un análisis de las necesidades del comprador, a continuación se recogen los factores relevantes a tener en cuenta en el proceso de adquisición y, finalmente, se describe cómo deben ser planteadas las especificaciones técnico - funcionales para la elaboración del Pliego de Prescripciones Técnicas que pueden ser de aplicación, y cuál es el cuestionario técnico diseñado para normalizar las ofertas y facilitar su evaluación.

3.6.1 Análisis de las necesidades del comprador

Las razones para proceder a la adquisición de un sistema de gestión de redes pueden estar determinadas por diferentes factores. Es labor del responsable de la administración de la red la realización de un análisis de necesidades existentes dentro de su organización que permita determinar las necesidades actuales y futuras de los usuarios y las limitaciones o restricciones que ha de plantearse respecto al dimensionamiento del sistema. Es necesario tener en cuenta y analizar a profundidad los costos y beneficios asociados para obtener argumentos de peso en la toma de decisiones.

En la fase de análisis de necesidades, fase inicial del proceso de adquisición, hay que tener en cuenta todos aquellos requisitos, limitaciones y restricciones que afecten, entre otros, a los siguientes puntos:

- **Elementos gestionables:** el comprador debe analizar los tipos de elementos que deben ser gestionados:

  Cables físicos.

  Dispositivos de red.

  Topologías de red.

  Sistemas operativos de red.

- **Interoperatividad de protocolos:** en el momento de comprar un sistema de gestión de red, el usuario debe analizar cuáles son sus necesidades relativas, qué protocolos deben ser soportados, de modo que el sistema que se adquiera ofrezca los máximos niveles en cuanto a flexibilidad, adaptabilidad y capacidad de expansión. Se deben realizar estimaciones de crecimiento de la red y tenerlas en cuenta durante esta fase.

Si en el entorno de gestión existen protocolos propietarios, el nuevo sistema de gestión debe tener, asimismo, facilidades para la gestión de estos últimos.

- **Facilidades de detección y recuperación ante fallos:** ante fallos en la red, el usuario debe analizar cuáles son sus necesidades relativas a:

  Capacidad para aislar los segmentos de red.

  Facilidades de mantenimiento y recuperación ante errores.

- **Interfaz gráfica de usuario:** si las redes que van a ser gestionadas se encuentran geográficamente dispersas por un campus, conectan varias plantas de un edificio, interconectan diferentes edificios, resulta muy interesante que el sistema de gestión que se vaya a adquirir disponga de una interfaz gráfica de usuario con facilidades para el dibujo de mapas, planos de edificios (sobre los que se podrá situar los equipos de comunicaciones), facilidades de zoom (con las que se puedan observar diferentes niveles de detalle de la red) y capacidades para añadir y configurar nuevos iconos (especialmente cuando se trate de un sistema de gestión de diseño a medida).

- **Facilidades de gestión remota:** en ocasiones puede ser de gran utilidad disponer de un sistema de gestión que permita configurar la red remotamente y que la información disponible sobre la red sea consistente, independientemente de la ubicación física desde la que se accede a la misma.

- **Características del equipo físico que soporte el sistema de gestión:** el sistema de gestión requerirá de una plataforma física sobre la que este pueda ejecutarse, con requisitos de compatibilidad respecto al equipo físico (memoria, disco, resolución gráfica, etc) y lógico (sistema operativo, interfaz gráfico, etc).

3.6.2 Factores relevantes en el proceso de adquisición de SGR

Es de suma importancia que todos los factores relevantes que intervienen en el proceso de adquisición queden debidamente recogidos en el pliego de prescripciones técnicas.

No obstante se hace mención de aquellos factores que pueden intervenir en el proceso de adquisición de Sistemas de Gestión de Redes y cuyo seguimiento debe efectuarse exhaustivamente:

- **Capacidad para soportar todos los elementos de la red:** el sistema de gestión debe permitir la integración de diferentes componentes y sistemas de interconexión. Cuando se dispone de diferentes redes, protocolos y dispositivos de red de diferentes fabricantes, se hace necesario que el sistema de gestión permita la gestión y supervisión de los diferentes elementos de la red.

- **Diseño a medida:** es muy importante que el sistema de gestión tenga capacidades de incorporación dinámica de nuevos elementos (nodos, enlaces, dispositivos, etc) a la medida de las necesidades del usuario, de forma que se puedan definir, o programar, las características de cada elemento. El usuario debe poder adaptar la representación gráfica en caso de producirse cambios en la red, permitiéndosele realizar altas, bajas y modificaciones de cada uno de los elementos que forman parte de la red.

En conclusión, la solución de software elegida deberá cubrir en el mayor grado posible todos y cada uno de los apartados anteriormente expuestos, sin que el coste final de la aplicación condicione fuertemente nuestra elección. Aunque el

factor precio influye notablemente en las aspiraciones de cualquier administrador, cabe plantearse la siguiente pregunta: **¿**De qué sirve una solución que no ofrece las opciones y posibilidades necesarias demandadas en cualquier entorno de red, limitándose a cubrir las facetas más generales de la administración de redes, sin entrar en los detalles y puntos de conflictividad donde realmente se distinguen las facultades de las herramientas más potentes**?**

3.6.3 Cuestionario Técnico para la adquisición de un SGR

(Marque con una **X**)

1. Elementos a ser gestionados

- Cables físicos ☐
- Dispositivos de red ☐
- Topologías de red ☐
- Sistemas operativos de red ☐

2. Protocolos soportados

- ICMP ☐
- SNMP ☐
- SNMPv2 ☐
- SNMPv3 ☐
- RMON ☐
- CMIP ☐
- Otro ☐ Detalle: _____

3. Facilidades de detección y recuperación ante fallos

- Permite aislar segmentos de red en los que se ha detectado fallos graves?
  Sí ☐ No ☐

4. Interfaz gráfica de usuario (GUI)

- Tipo de interfaz:
  - Modo Texto ☐
  - Modo Gráfico ☐
- Tipo de entorno gráfico:
  - MS-Windows ☐
  - X-Window ☐
  - Web Browser ☐

5. Facilidades de Gestión Remota

- El SGR permite configurar la red independientemente de la ubicación física desde dónde se acceda a la misma? Sí ☐ No ☐

6. Características del equipo físico que soporte al SGR

Características físicas

Tipo de procesador

- Pentium ☐
- AMD ☐
- Cyrix ☐
- Otro ☐ Detalle: _____

Velocidad del procesador

- 100 MHz ☐
- 133 MHz ☐
- 233 MHz ☐
- Superior a 233 MHz ☐

Memoria principal

- 32 MB ☐
- 64 MB ☐
- 128 MB ☐
- Superior a 128 MB ☐

Resolución gráfica

- 640 x 480 ☐
- 800 x 600 ☐
- 1200 x 720 ☐
- Otra ☐

Disponibilidad

- CPU redundante Sí ☐ No ☐
- Fuente de alimentación redundante Sí ☐ No ☐

Características lógicas

Sistema operativo

- UNIX ☐
- Linux ☐
- Windows 9x ☐
- Windows NT ☐
- Windows 2000/ Me ☐
- Otro ☐

7. Factores relevantes en la adquisición de un SGR

Capacidad para soportar todos los elementos de red

Tipos de redes gestionadas / por su ubicación

- LAN ☐
  - 802.3 (Ethernet) ☐
  - 802.5 (Token Bus) ☐
  - 802.6 (Redes Metropolitanas) ☐
- WAN ☐

Topología

- Bus ☐
- Anillo ☐
- Estrella ☐
- Estrella jerárquica ☐

¿El SGR indica el estado individual de los elementos gestionados?

Sí ☐ No ☐

Diseño a medida

Operaciones de red

- ¿Gestión, supervisión y actualización de los nodos de red?

  Sí ☐ No ☐
- Brinda el establecimiento de derechos de acceso:
  - Identificación ☐
  - Detección de violación de seguridad ☐
- ¿Permite un Filtrado y gestión de eventos?

  Sí ☐ No ☐
- Permite configurarse para una gestión:
  - Centralizada ☐
  - Distribuida ☐
- ¿Permite realizar tareas de configuración de los dispositivos de red?

  Sí ☐ No ☐
- ¿Brinda facilidades de gestión de base de datos y aplicaciones?

  Sí ☐ No ☐

- ¿Permite realizar una distribución de software?

  Sí ☐ No ☐

- ¿Genera estadísticas de utilización de ancho de banda?

  Sí ☐ No ☐

- ¿Permite tener una visión panorámica de los nodos gestionados?

  Sí ☐ No ☐

- Facilita una representación gráfica en tiempo real de:
  - Partes de la red ☐
  - La totalidad de la red ☐

- Permite tarifar el uso de un determinado servicio de manera:
  - Individual ☐
  - Por grupos ☐

- Brinda una automatización de:
  - Tareas ☐
  - Mensajes ☐
  - Alarmas ☐

Mantenimiento

- ¿Permite tener el control sobre los dispositivos gestionados?

  Sí ☐ No ☐

- ¿Brinda notificaciones automáticas de errores?

  Sí ☐ No ☐

- ¿Permite un acceso automático desde la consola de gestión?

  Sí ☐ No ☐

- ¿Realiza un filtrado de alarmas?

  Sí ☐ No ☐

- Realiza un aislamiento de fallos:
  - Lógico ☐
  - Físico ☐

- ¿Permite una recuperación ante fallos automática?

  Sí ☐ No ☐

3.6.4 Características de Funcionamiento de los SGR por cada Area de Gestión del Modelo Funcional OSI

A continuación se presentan unos formularios que servirán de ayuda adicional en el proceso de elección de un SGR. Estos resumen las características de las áreas del modelo funcional OSI, quizá no pueda conseguirse todas las características expuestas en un SGR comercial, pero vale la pena hacer un análisis de prestaciones, en base a dichos formularios, para tomar una decisión final.

Cabe indicar que no se ha incluido formulario alguno sobre el Area Funcional de la Gestión de la Contabilidad, para el proceso de elección del SGR, debido a que no existe por el momento en el mercado implementación alguna que proporcione funciones de tipo contable.

Funcionamiento de los SGR por cada Area de Gestión del Modelo Funcional OSI

Area: **Gestión de Fallos y Recuperación**

	SGR a evaluar		
Características Funcionales	**SGR1**	**SGR2**	**SGR3**
1. Detección e informe de problemas			
1.1. Presentación del estado de la red, e indicación de la falla, su naturaleza y gravedad			
1.2. Empleo de rutinas para la localización de la falla			
1.3. Almacenamiento de los eventos generados en los recursos gestionados en una BDD de reportes históricos			
1.4. Generación de alarmas para indicar el mal funcionamiento			
2. Aislamiento de la causa del problema			
2.1. Determinación de la ubicación exacta de cuellos de botella y problemas de red			
2.2. Aislamiento del recurso hardware, medio de transporte o causa externa causante de la falla			
3. Diagnóstico y resolución del problema			
3.1. Seguimiento y control del problema desde su detección hasta su resolución (Trouble Ticketing)			
3.2. Determinación de las posibles soluciones para el problema detectado			
3.3. Respaldo y reconfiguración para mantener la integridad de la topología de red			
3.4. Puenteo o recuperación de problemas para minimizar o eliminar temporalmente los efectos de los fallos en la red			

Funcionamiento de los SGR por cada Area de Gestión del Modelo Funcional OSI

Area: **Gestión de la Configuración**

	SGR a evaluar		
Características Funcionales	**SGR1**	**SGR2**	**SGR3**
1. Construcción de la topología de red de acuerdo a la visión del usuario			
1.1. Definición de nuevos recursos a gestionar			
1.2. Manejo de correspondencia de nombres entre dispositivos y sus direcciones de red			
1.3. Asignación y gestión de nombres a los recursos gestionados			
1.4. Creación, modificación y destrucción de relaciones entre los recursos			
1.5. Determinación de los conflictos reales y potenciales al realizar cambios en las configuraciones			
1.6. Descubrimiento automático de dispositivos			
2. Establecimiento de los parámetros de funcionamiento (inicialización y modificación de la configuración) de todos los recursos de la red			
2.1. Establecimiento y modificación de las características de operación de los dispositivos			
2.2. Reflejo en tiempo real de los cambios en los modos de operación de los recursos gestionados			
2.3. Determinación del espacio libre en disco de las estaciones de trabajo y servidores			
3. Mantenimiento de inventario de los dispositivos instalados			
3.1. Borrado y actualización de los dispositivos instalados			
3.2. Obtención de informes de la identidad, condiciones de funcionamiento, de los objetos gestionados			
3.3. Determinación de cambios en el software instalado			
3.4. Identificación de cambios en los archivos de configuración			
3.5. Recopilación de datos hardware y software			
3.6. Distribución electrónica de software			

Funcionamiento de los SGR por cada Area de Gestión del Modelo Funcional OSI

Area: **Gestión del Rendimiento**

	SGR a evaluar

Características Funcionales	SGR1	SGR2	SGR3
1. Recolección de información del estado de la red y determinación de indicadores de rendimiento			
1.1. Almacenamiento de información de la utilización actual de la red, dispositivos y enlaces en una BDD histórica			
1.2. Determinación de los siguientes indicadores del desempeño:			
1.2.1. Estado de los dispositivos gestionados (**Disponibilidad**)			
1.2.2. Tiempo total, retardos en la red y en los nodos (**Tiempo de respuesta**)			
1.2.3. Calidad del enlace (**Exactitud**)			
1.2.4. Mediciones dinámicas de la utilización de la red (**Grado de utilización**)			
1.2.5. Utilización de recursos de red por parte de los dispositivos y/o aplicaciones (**Demanda**)			
1.2.6. Relación entre la utilización y la demanda de un recurso de la red (**Throughput**)			
2. Monitoreo del rendimiento de la red			
2.1. Almacenamiento de información de fallas			
2.2. Definición de límites/umbrales de utilización de la red			
2.3. Manipulación de límites e indicadores del rendimiento en la red			
3. Análisis y afinamiento			
3.1. Analizar datos relevantes de la información almacenada para visualizar tendencia de alta utilización			
3.2. Usar simulaciones para determinar cómo la red puede alcanzar máximo rendimiento			

Funcionamiento de los SGR por cada Area de Gestión del Modelo Funcional OSI

Area: **Gestión de la Seguridad**

	SGR a evaluar		
Características Funcionales	**SGR1**	**SGR2**	**SGR3**
1. Análisis de riesgos			
1.1. Creación, eliminación y mantenimiento de servicios y mecanismos de seguridad de acuerdo a una política de seguridad establecida			
1.2. Distribución de información de seguridad			
1.3. Información de los intentos de violación de la seguridad en los equipos activos de comunicación			
2. Evaluación de los servicios de seguridad			
2.1. Comprobación de la autenticidad de la información			
2.2. Control de acceso hacia los objetos gestionados			
3. Evaluación de las soluciones de gestión de seguridad			
3.1. Encriptación			
3.2. Utilización de claves para la identificación de usuarios			

La mayor parte de las aplicaciones de gestión de redes solamente se refieren a la seguridad aplicable al equipo de red, tal como el acceso a un ruteador o puente. Algunas herramientas cuentan con alarmas y capacidades de reporte que forman parte de la seguridad física del equipo (interfaz con la alarma contra incendios, etc), pero ninguna trabaja con la seguridad del sistema de información, debido a que se piensa que ésta es una tarea del Administrador del Sistema de Información.

Referencias Bibliográficas

1. **ISLAS Carlos, MENDOZA Alfredo.,** "**Administración de Redes Informáticas Empresariales**", Centro de Investigación en Informática., ITESM, México 1997.

2. **EGAS Carlos.,** "**Gestión de Redes**", CLEI 1998, Quito – Ecuador.

3. **FLATIN Jean Philippe, ZNATY Simon, HUBAUX Jean Pierre.,** "**A Survey of Distributed Network and Systems Management Paradigms**", Communication System Division (SSC), CH-1015 Technical Report , Lausanne-Switzerland 1998.

CAPITULO IV

SISTEMAS DE GESTION DE RED COMERCIALES

INTRODUCCION

En nuestro medio las únicas instituciones que están en la capacidad de adquirir un SGR comercial son las instituciones bancarias y aquellas que manejen sistemas de telecomunicaciones debido a su elevado costo.

En este capítulo se van a estudiar tres Sistemas de Gestión de Red Comerciales: Tivoli Netview (IBM), Spectrum Enterprise Manager (Cabletron) y System Management Server (Microsoft), que en el mercado actual son considerados los mejores Sistemas de Gestión de Red.

El estudio se enmarcará en las funciones de Gestión de Red del modelo funcional OSI que realicen cada uno de estos, así como también la seguridad, arquitectura y tipos de redes que soporten.

La evaluación de los SGR Comerciales, empleando el cuestionario técnico para la adquisición de un SGR y los formularios descritos al final del capítulo anterior, está documentada en el **Anexo B** .

4.1 Tivoli NetView

NetView es una herramienta de gestión de redes para ambientes heterogéneos, que provee funciones de gestión de la configuración, fallos, seguridad, y desempeño (rendimiento), a lo largo de muchos aspectos que lo hacen fácil de instalar y usar.

NetView permite descubrir las redes TCP/IP, las topologías de redes, correlacionar y administrar los sucesos, el monitoreo de la red, y el desempeño de los datos. También permite la integración de aplicaciones multi-protocolos con submapas TCP/IP.

Además, NetView provee una plataforma abierta de gestión de red que permite la integración de SNMP y aplicaciones que usan el Protocolo de Información Común de Gestión (CMIP). Añadir un objeto MIB a la base de datos MIB SNMP existente, significa que un administrador de NetView puede administrar multi-entradas, los dispositivos heterogéneos de red y también proveer de soporte para la gestión de dispositivos que no tienen una dirección IP.

NetView es una herramienta que provee gestión centralizada o distribuida para su red.

NetView ha extendido su capacidad de gestión tanto en administración de redes y gestión de sistemas que puede seguirse integrando con otras aplicaciones de Tivoli.

4.1.1 Características de Tivoli NetView

NetView posee las siguientes características:

- Administración heterogénea, redes multivendedor.
- Configuración de la red, fallas, seguridad, y administración de rendimiento.
- Descubrimiento dinámica de dispositivos.
- Interfaz gráfica fácil de usar.

- Integración con bases de datos relacionales.
- Soporte de muchas aplicaciones de terceros.
- Administración distribuida.
- Distribución de interfaz gráfica TME 10 de NetView para los clientes.
- Monitorización de IP y administración de SNMP.
- Administración y supervisión multiprotocolo.
- Administración de las herramientas MIB (Management Information Base).
- Interfaz de aplicaciones programables (APIs).
- Fácil instalación y mantenimiento.
- Conectividad a Host e información On-Line.

4.1.2 Plataformas soportadas

Tivoli NetView para UNIX

NetView para UNIX debe instalarse en un ambiente que posea Tivoli Framework.

El Tivoli Framework soporta instalación y administración remota de este producto desde un servidor TMR (TME 10 Management Region) a un nodo de recursos manejado por Tivoli. En la tabla siguiente (**Tabla 4.1**) se muestran las plataformas que pueden ser usadas para la administración, instalación y ejecución de NetView de manera local y remota.

Plataforma	Instalación y Administración remota	Instalación y administración local
IBM RS/6000 AIX4.1.4+, 4.2.x, 4.3.x	Sí	Sí
Digital UNIX 4.0 (A-D)	Sí	Sí
SUN SPARC Solaris 2.5, 2.5.1, 2.6	Sí	Sí
HPUX 10/11	Sí	No
Windows NT 4.0	Sí	No

Tabla 4.1 Plataformas soportadas por Tivoli NetView

Tivoli NetView para Microsoft Windows NT

Hardware: los requisitos de NetView para Windows NT son los siguientes:

- CPU: Intel PC o Alfa PC. Para PCs Intel, mínimo Pentium de 90 Mhz.
- Memoria: 48MB de RAM para PCs Intel, 64MB de RAM para PCs Alfa.
- Espacio de página: 128MB (mínimo).
- Sistema de archivos: partición NTFS o una partición FAT que soporte nombres de archivos largos.
- LAN: Conexión de red.
- Vídeo: tarjeta gráfica SVGA y monitor (mínimo 800x600 pixels x 16 colores). Se recomienda 1024x768 pixels.

Software: los requisitos del software para el cliente o modo del servidor, así como para el Servicio de Cliente Web son:

- Windows NT Versión 4.0 con Service Pack 3 o superior.
- Instalado y configurado TCP/IP.
- Instalado y configurado el servicio SNMP.

4.1.3 Arquitectura de Tivoli NetView

En el ambiente actual las redes tienen una sobrecarga de información debido a un ascendente aumento de recursos SNMP en la red provocados por el envío de paquetes de información desde el punto central de gestión.

NetView permite una distribución de la gestión de la red usando el Administrador de Nivel Medio (**MLM**, *Mid Level Manager*).

El administrador de nivel medio permite que se pueda controlar el sistema, la verificación de la red, y la gestión de red desde una plataforma central de administración de red (el nodo administrador Tivoli con NetView instalado) con un gestor intermedio basado en SMNP, (el administrador de nivel medio) instalado sobre cualquier máquina TCP/IP en su red.

Las tareas desempeñadas por el administrador de nivel medio incluyen lo siguiente:

- Descubrimiento de nuevos nodos y estadísticas de los nodos concurrentes.
- La automatización de sucesos.
- Detección automática de nuevos dispositivos recientemente borrados o añadidos.

Estos aspectos de gestión reducen la cantidad del tránsito creado en la red por el sistema de gestión y minimiza la asociación administrativa que va con los sistemas de gestión de red. Además, muchos problemas se resuelven mediante la automatización local, así, reduciendo la carga de trabajo administrativo de agregar y borrar nodos.

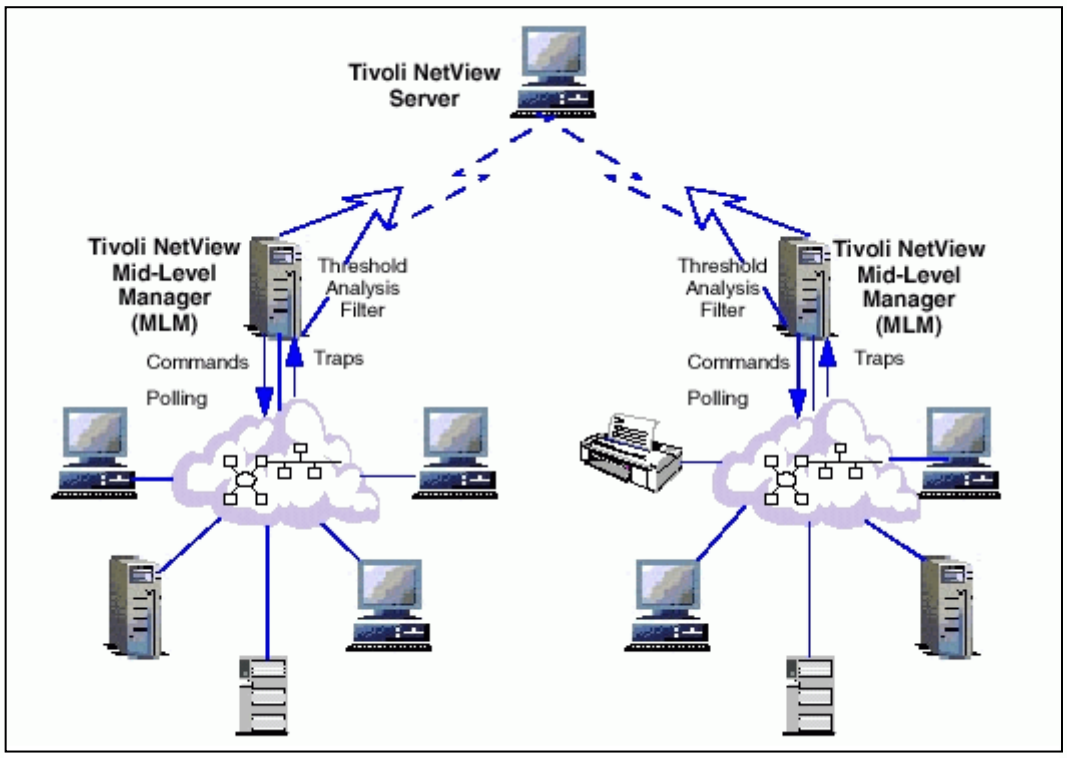


Fig. 4.1 Arquitectura Distribuida de Gestión de Tivoli NetView

4.1.4 Gestión de la Seguridad

La gestión de la seguridad de NetView crea servicios seguros de contexto para la comunicación entre el servidor y el administrador de nivel medio. Se puede usar estos servicios para definir políticas de seguridad para su red y de control para los usuarios que acceden a NetView y a sus aplicaciones.

Los servicios de seguridad de NetView proveen los controles siguientes:

- La identificación y autenticación de red.
- La comunicación protegida de red entre el servidor NetView y el administrador de nivel medio.
- La protección de contraseña.
- Auditoría continua de la gestión de red.
- Control de acceso a los recursos de NetView en la red.

- Interfaz gráfica personalizada de NetView según los derechos del usuario.
- Auditoria de gestión.

Los servicios de seguridad para cada usuario son auténticos. Los usuarios emiten un login que será identificado como un usuario válido ID, grupo ID, y contraseña. Si la contraseña proporcionada por el usuario es igual a la contraseña de seguridad en la base de datos, el usuario tiene el acceso a las funciones predefinidas en NetView. Para definir adecuadamente una política de seguridad, se controla el acceso a los usuarios a las funciones, aplicaciones mapas y submapas de NetView.

4.1.5 Gestión de Configuración

La gestión de configuración de NetView provee aplicaciones dinámicas para las actualizaciones de las diferentes topologías de la red. NetView descubre automáticamente y actualiza los mapas y submapas de la red.

Algunas de las funciones que puede realizar la configuración de NetView son:

- Configuración y despliegue de eventos.
- Navegación y consultas de objetos MIB.
- Permite ver y modificar las descripciones de los nodos.
- Localización de los objetos en los mapas.

Descubrimiento Dinámico de dispositivos

Este atributo de NetView lo realiza de algunas formas:

- Puede descubrir todos los elementos de la red que contengan IP.

- NetView hace uso de un archivo de semilla que define el conjunto inicial de nodos de IPs para ser descubiertos. Usando el archivo de semilla fuerza o restringe el proceso de descubrimiento para generar el mapa topológico comenzando con nodos como el servidor de gestión.
- Se puede limitar el descubrimiento de los nodos seleccionados de la red o de las sub-redes.

El programa de descubrimiento permite encontrar nuevos dispositivos agregados a la red y determina aquellos dispositivos borrados desde la red. El proceso de descubrimiento asegura que el mapa topológico de la red se completará y se verá en la Consola de NetView.

Cuando un nuevo nodo se descubre, se agrega a la base de datos y la lista de nodos que están siendo controlados. Si el nodo descubierto soporta un agente SNMP, la información sobre su configuración de sistema es recobrada por obtención de la MIB de valores y del almacenamiento en la base de datos.

NetView puede configurarse para trabajar con una base de datos relacionada. Desde la base de datos relacionada, usted puede usar cualquier de las herramientas disponibles para crear informes desde la base de datos sobre los datos de IP y los nodos en su configuración de red.

Edición de Mapas de red

Puede haber dispositivos que no pueden dinámicamente descubrirse en la red, para permitir representar estos dispositivos, NetView soporta la edición manual en el mapa de la red. Se puede agregar, borrar, mover, o trasladar objetos entre mapas (ver **Fig. 4.2**). Estas alteraciones en los mapas pueden ser grabadas para

futuras planificaciones de las configuraciones y diagnósticos de problemas en la red.

Configuración y presentación de eventos

NetView proporciona un estado de configuración para cambios que permiten especificar el significado del estado de los eventos para las tramas especificadas. Se puede identificar parámetros para decir cuando un nodo esta abajo o arriba en su funcionamiento. Los cambios de estado se reflejan dinámicamente por un cambio en color desplegado en la topología de la red.

Los cambios de la configuración generan eventos en los que pueden presentarse en la

Interfaz gráfica o en las tarjetas de eventos o lista de eventos.

Navegar y consultar objetos MIB

Las consultas a los valores MIBs se las puede realizar a través de interfaces gráficas que se representan en tiempo real. Se puede crear una aplicación de datos MIB y puede agregarlo al menú de NetView. La función de consultas ayudará a recuperar uno o más valores de los objetos MIB en una tabla o en una forma gráfica en tiempo real.

Localización de objetos en el mapa

Para encontrar objetos en los mapas se pueden tener algunos atributos para encontrarlos como por el nombre de la máquina, la dirección IP, enlaces de direcciones, el tipo de objeto, o agrupaciones de objetos (ver **Fig. 4.2**).

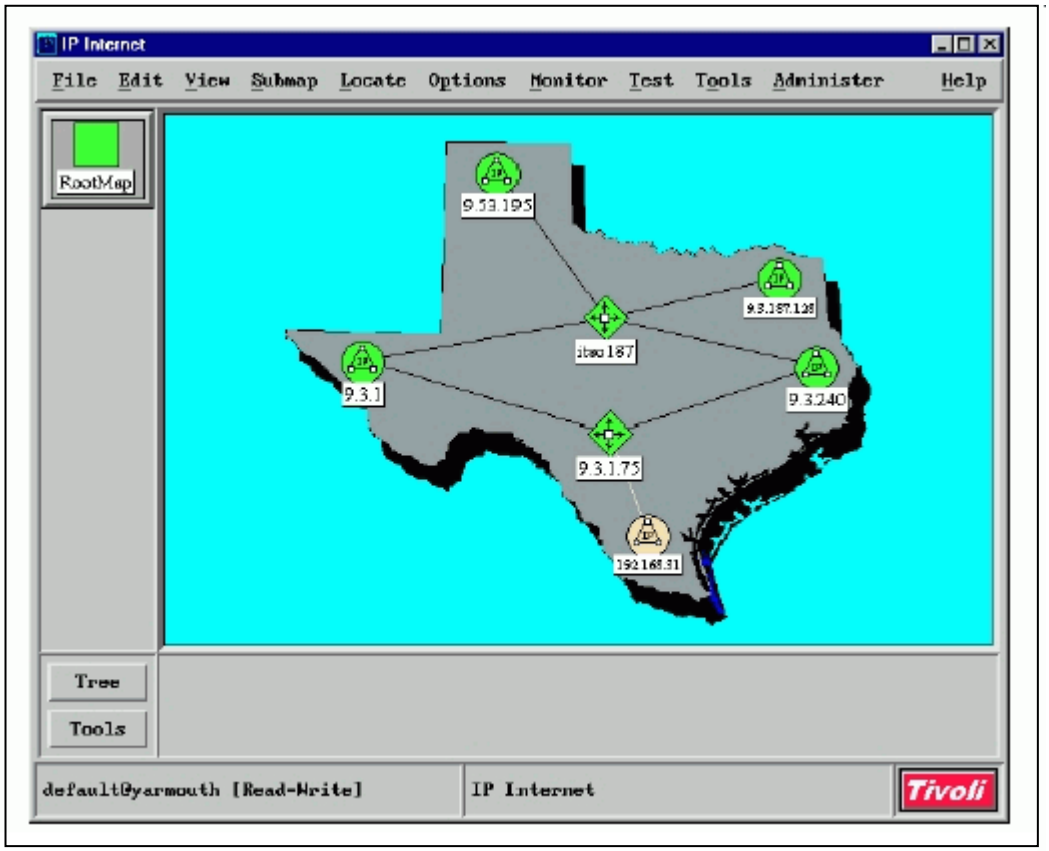


Fig. 4.2 **Consola de Tivoli NetView**

4.1.6 Gestión de Fallas y Recuperación

NetView tiene funciones de ayuda para usted, ayuda a la determinación de problemas, identifica problemas en la red, y provee mecanismos para la recuperación de errores a la brevedad posible.

Algunas de sus funciones son:

- Supervisión en el mapa de la red para detectar problemas.
- Eventos supervisados para detectar problemas.
- Localización de problemas en la red.
- Solución de problemas en la red.

Las siguientes son las definiciones de sucesos usadas por NetView:

- **Sucesos de mapa**: son las notificaciones enviadas por el servidor de NetView por causa de un usuario o una acción de una aplicación que afecta la condición de la red sobre la interfaz gráfica de NetView.
- **Sucesos de red:** Son los mensajes enviados por un agente al servidor de NetView para proveer la notificación de la ocurrencia de una actividad que afecta a un objeto de la red.

Eventos supervisados para detectar problemas

NetView recibe sucesos por cada dispositivo de la red. Los sucesos se muestran cuando los errores ocurren sobre la red, cuando la topología de la red cambia, cuando hay cambios en la configuración de los nodos, o cambios de condición de la red, y estos sucesos son recibidos por NetView (ver **Fig. 4.3**). NetView puede detectar la condición de dispositivos enviados por el eco de peticiones del Protocolo de Control de Mensajes de Internet (ICMP) mediante (pings) y peticiones de SNMP a dispositivos.

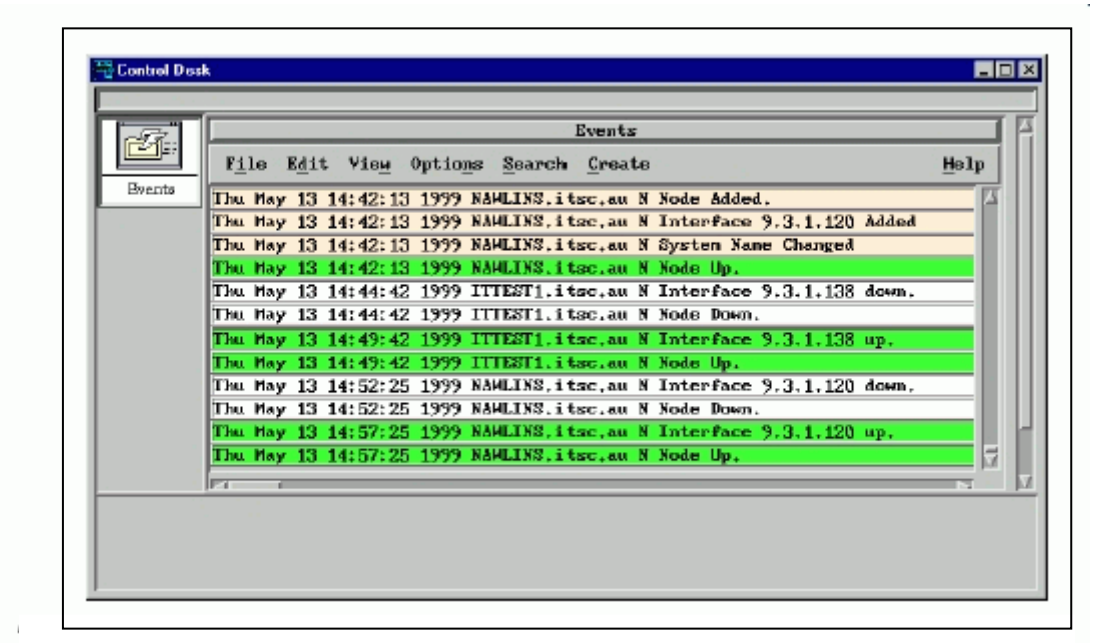


Fig. 4.3 Control de Eventos en Tivoli NetView

En redes grandes con muchos objetos y agentes, muchos sucesos que el servidor de NetView puede recibir y procesarlos para luego enviar repuestas. Se puede significativamente reducir la cantidad de tiempo requerido por el servidor de NetView para procesar los sucesos entrantes por filtradores afuera y desechar esos sucesos que no son importantes para su operación.

También, con estos filtros y capacidades de correlación, se puede seleccionar los sucesos que se quiere mostrar sobre la consola (ver **Fig. 4.4**). Filtrar los criterios puede ser aplicado a la información del suceso recibido desde la red que ha seleccionando, solamente sucesos para ser presentados sobre la interfaz gráfica.

Estas acciones pueden incluir una ejecución de un shell script o un comando para comenzar una aplicación particular. Dependiendo del resultado de la correlación de los sucesos, NetView emitirá un comando para paginar soporte técnico o envía un suceso resultante.

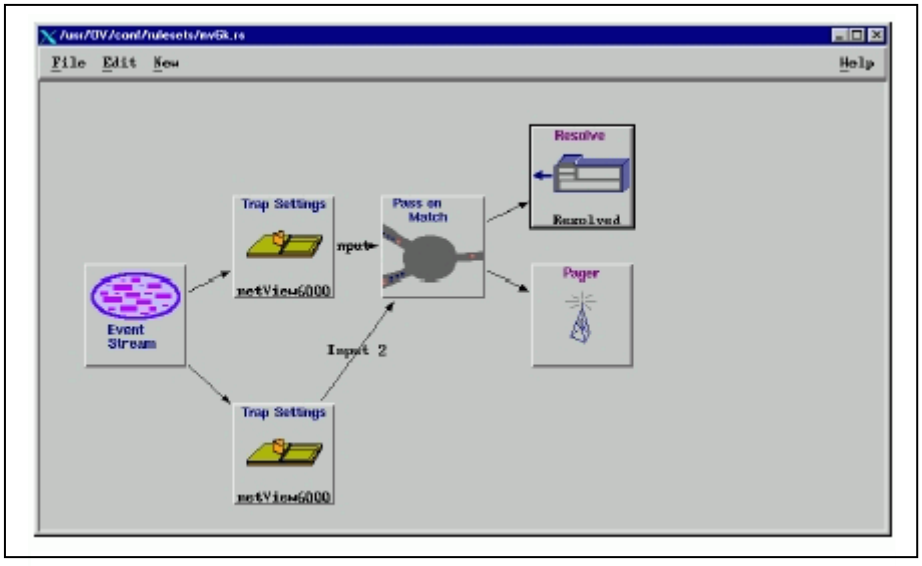


Fig. 4.4 Reglas de Correlación de alarmas

NetView tiene varias herramientas para diagnosticar los problemas en la red. Estas herramientas pueden ayudar rápidamente a resolver los problemas. Puede seleccionar el suceso apropiado, donde se pueda ver información relevante del dispositivo que se encuentra fallando, es decir la descripción del problema, ubicación, y contacto del proveedor. En la adición a un mapa topológico, se puede seleccionar el nodo y escoger los ítems de menú, si se necesita información adicional.

Por lo general NetView tiene varios colores con los que se puede identificar los estados en los que se encuentran los objetos (ver **Tabla 4.2**):

Estado	Significado del estado	Color por defecto del icono	Color por defecto de la conexión
Desconocido	Estado no determinado	Azul	Negro
Normal	Estado de operación normal	Verde	Negro
Marginal	Daño, pero todavía funciona	Amarillo	Amarillo
Critico	No funciona	Rojo	Rojo
No manejado	No esta monitoreado, el usuario a definido el símbolo	Trigo	Negro
Inalcanzable	Actualmente no identificado por la estación administradora.	Blanco	Negro
Reconocido	No esta monitoreado, el usuario a definido el símbolo	Verde obscuro	Negro
Usuario1	Un nodo está abajo para ser reconfigurado. Este estado se aclara cuando el nodo se pone en operación de nuevo.	Rosado	Negro
Usuario2	Indica un fracaso que no puede ser restablecido. Si el usuario2 esta asociado con un estado de netmon, los estados del netmon serán atendidos por el usuario2.	Violeta	Negro

Tabla 4.2 Colores asociados para la detección de fallas en Tivoli NetView

4.1.7 Gestión de Rendimiento de Tivoli NetView

NetView tiene varias funciones que permiten verificar el desempeño de una red, tal como:

- Coleccionar estadísticas en tiempo real y presentarlas en forma gráfica.
- Colocar las entradas para las áreas críticas del desempeño de la red, NetView configura para verificar estas entradas por nodos especificados en intervalos y generan una trampa si la entrada se ha excedido.
- El uso de los datos MIB en NetView son para obtener información específica, tal como la utilización del CPU y el tráfico de la red, desde nodos que tienen un agente SNMP corriendo.

Los datos de la MIB pueden ayudar a planificar el uso de la red y los recursos de la computadora así como también aislar los errores y problemas de desempeño en la red.

El conjunto de datos de la MIB de NetView continuamente se actualizan y controlan dispositivos o agrupaciones de dispositivos en la red basados en ciertos parámetros de configuración. NetView encuesta nodos de la red para obtener información acerca del número de elementos MIB de dispositivos SNMP. Se puede acceder a esta información tan pronto como se haya agrupado (ver **Fig. 4.5**). El conjunto de datos MIB verifica las entradas para la agrupación de datos MIB y pueden emitir un suceso si una entrada se ha excedido.

NetView provee aplicaciones que permiten controlar el desempeño de la red en tiempo real. También provee una herramienta, el constructor de aplicaciones MIB, que permite construir una aplicación propia de monitoreo de red.

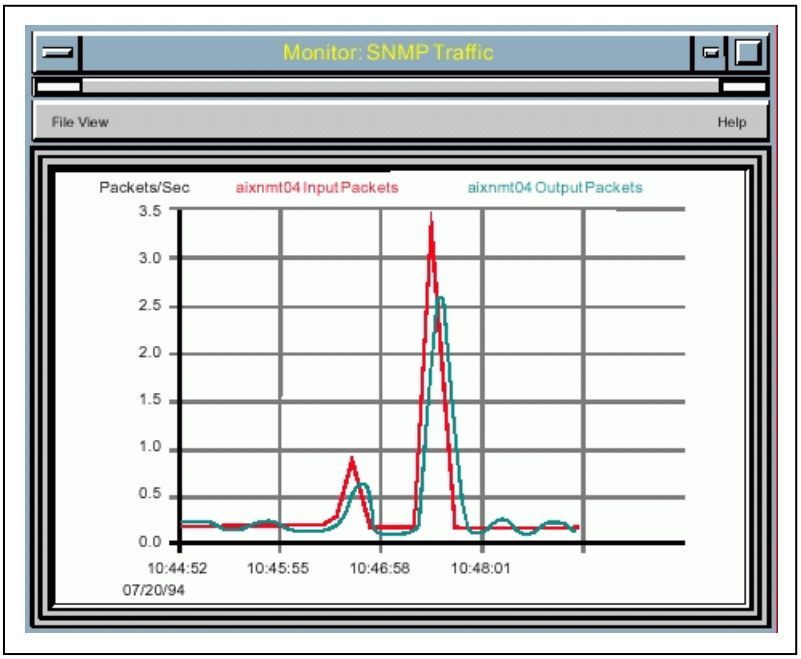
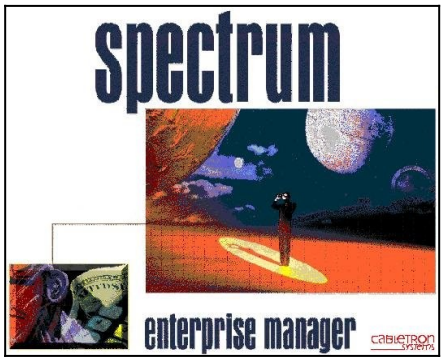


Fig. 4.5 **Monitoreo de Tráfico SNMP**

4.2 Spectrum Enterprise Manager



SPECTRUM es un conjunto integrado de aplicaciones de gestión de red apoyado por una plataforma de inteligencia artificial. En combinación con el diseño cliente/servidor de SPECTRUM, esta inteligencia permite un monitoreo remoto e incluso gestiona el conjunto más grande de redes multivendedores usando modelos de software que representan dispositivos reales y mantienen un conocimiento sobre sus conexiones y relaciones (ver **Fig. 4.6**).

Estos modelos inteligentes se representan a su vez en la interfaz gráfica de usuario de SPECTRUM por íconos que indican el estado del dispositivo "de una ojeada" y proporciona fácil acceso a información más detallada sobre la configuración, rendimiento, y aplicaciones soportadas.

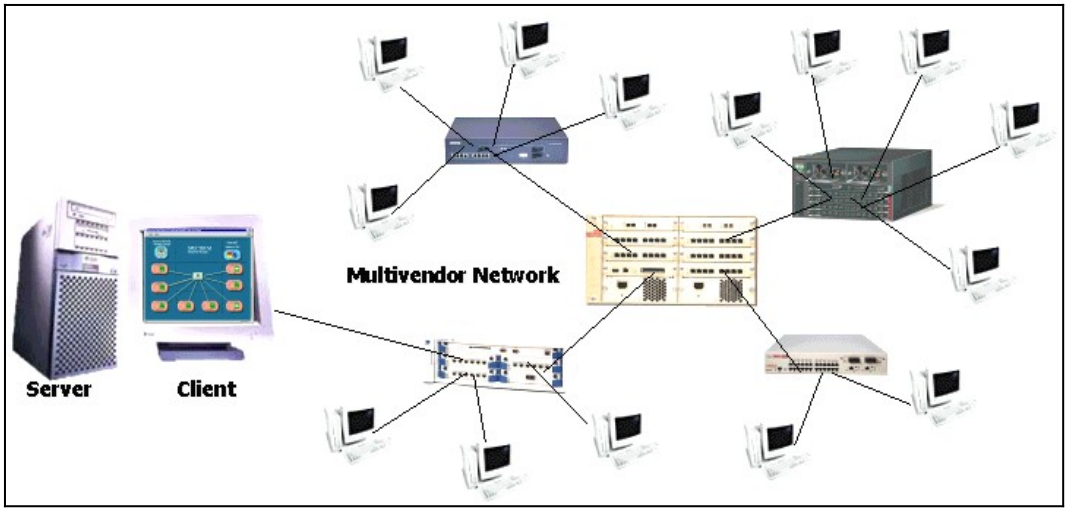


Fig. 4.6 Gestión de una red multivendedor mediante SPECTRUM

La base de conocimiento que SPECTRUM puede ser entonces empleado por otras aplicaciones de SPECTRUM y por otras aplicaciones integradas para una total gestión empresarial, incluyendo sistemas, procesos comerciales, servicios, etc.

4.2.1 Características de Spectrum

- **Cliente/Servidor**: SPECTRUM utiliza la verdadera arquitectura cliente/servidor. Todos los gráficos se producen localmente en la estación que ejecuta el cliente, salvaguardando el ancho de banda. Todos los clientes pueden acceder al servidor y usar los diferentes derechos de acceso. Las opciones de acceso disponibles para cualquier usuario concurrente son SOLO-LECTURA, y LECTURA/ESCRITURA/ EJECUCION y Ningún Acceso.

- **Distribuido:** SPECTRUM puede tener múltiples clientes por servidor, así como múltiples servidores por red. Cada servidor debe estar consciente de

otros servidores en la red. La tarea de gestión de red puede distribuirse a donde ellos la realizan eficazmente, mientras se continua manteniendo un control centralizado.

- **Escalable:** SPECTRUM descascara bien a redes de cualquier tamaño sin una pérdida en el rendimiento o retardo en la notificación del problema.

- **Multivendedor:** SPECTRUM manejará virtualmente cualquier dispositivo a través de su tecnología de modelamiento orientada a objetos.

- **Multiprotocolo:** SPECTRUM soporta SNMP, ICMP, RPC, y 802.1D. Usando la Interfaz de Protocolo Externa, API abierto de SPECTRUM (EPI External Protocol Interface), cualquier pila de protocolos puede agregarse a través de personalización.

- **Proactivo:** SPECTRUM descubrirá síntomas del problema, analizará los síntomas y presentará una alarma para el origen, minimizando la cantidad de tiempo que gastan los operadores y técnicos aislando el problema. Pueden establecerse umbrales, o los atributos MIB compararse entre si; por ejemplo, las colisiones compararse con la carga o el tiempo.

- **Inteligente:** para determinar un Punto Simple de Aislamiento de Fallas, SPECTRUM usa una inteligencia artificial internamente desarrollada que puede ser empleada en cualquier tecnología modelada en SPECTRUM, si ésta es una LAN, WAN, ATM ó PBX.

- **Flexible:** SPECTRUM puede operar en Solaris y plataformas Windows NT en un ambiente mixto. (Es decir, un SpectroSERVER puede instalarse en una máquina de Solaris y puede ser accesada por un SpectroGRAPH instalado en una máquina NT.)

- **Basado en Web:** La consola Web Metrix permite visualización de la red desde cualquier explorador de html. Permite informes esenciales del negocio y la gestión para ser visualizados desde un explorador web.

- **Automatizado:** SPECTRUM tiene la capacidad de realizar acciones automáticamente, basado en eventos de la red o tiempo. El resultado obtenido minimiza el tiempo fuera de servicio, maximiza el rendimiento y una mínima intervención es necesitada para controlar la red mientras proporciona estadísticas para la gestión de la red y la planificación de capacidad.

4.2.2 Plataformas Soportadas

La siguiente subdivisión lista el hardware y el software requerido para el paquete básico de gestión de red SPECTRUM para cada una de las plataformas soportadas. SPECTRUM puede configurarse con más de un SpectroGRAPH, los requisitos de memoria sugeridos para la Interfaz Gráfica de Usuario y SpectroSERVER se presentan separadamente. La RAM mínima sugerida y los requerimientos mínimos de espacio disponible en Disco son presentados juntos y separadamente (ver Tablas **4.3** y **4.4**). Todas las cantidades son mostradas en megabytes.

Requerimientos para Sun Solaris

- SPECTRUM soporta los sistemas operativos Solaris 2.5.1 y 2.6 sobre las siguientes estaciones de trabajo: Sparc 5, Sparc 10, Sparc 20 y UltraSPARCs.
- SPECTRUM se instalará sobre Solaris 2.5.1 con OpenWindows 3.5.1 y CDE (Common Desktop Environment) 1.0.2.
- SPECTRUM se instalará sobre Solaris 2.6 con OpenWindows 3.6 y CDE 1.2., SPECTRUM está compilado con C++ versión 4.1.

Tipo de Instalación	RAM Mínima	Espacio mínimo de intercambio	Espacio mínimo disponible en disco
SpectroSERVER y SpectroGRAPH en la misma máquina	128MB	256MB	500MB
SpectroSERVER	96MB	192MB	250MB
SpectroGRAPH	64MB	128MB	250MB

Tabla 4.3 Requerimientos de SPECTRUM para Sun Solaris

Requerimientos para Microsoft Windows NT

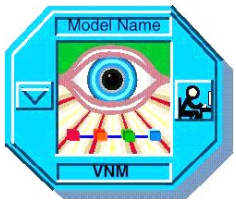
- SPECTRUM soporta Microsoft Windows NT 4.0 con el Service Pack 3 o superior, basados en sistemas Intel con procesadores Pentium de 150 Mhz (o superior).

Tipo de Instalación	RAM Mínima	Espacio mínimo de intercambio	Espacio mínimo disponible en disco
SpectroSERVER y SpectroGRAPH en la misma máquina	128MB	256MB	600MB
SpectroSERVER	96MB	256MB	300MB
SpectroGRAPH	96MB	128MB	300MB

Tabla 4.4 Requerimientos de SPECTRUM para Windows NT

4.2.3 Arquitectura de SPECTRUM

El diseño cliente/servidor de SPECTRUM es inherentemente flexible y escalable, permitiéndole configurar servidores múltiples (SpectroSERVERS Distribuídos) y fácilmente agrega nuevas aplicaciones cliente para reunir requisitos cambiantes como su empresa se extiende (ver **Fig 4.7**).



El servidor SpectroSERVER o máquina de red virtual (**VNM**, *Virtual Network Machine*) incluye la base de datos y proporciona la seguridad, capacidades de modelamiento y facilidades de gestión de dispositivos.

La base de datos proporciona almacenamiento para configuraciones específicas de dispositivos, estadísticas, eventos y contiene un catálogo de modelamiento (tipos de modelos y relaciones) que son la estructura para toda la información de red.

Las aplicaciones cliente incluyen SpectroGRAPH, usa la Interfaz de Programación de Aplicaciones SpectroSERVER (**SSAPI**, *SpectroSERVER Application Programming Interface*) para accesar a la información del servidor así como las utilidades para el descubrimiento automatizado y modelamiento, planeamiento, generación de reportes, establecimiento de umbrales, y gestión de alarmas y configuraciones.

Numerosas aplicaciones integradas de terceros también usan la inteligencia de SpectroSERVER para proporcionar soluciones para la Gestión de Nivel de Servicio, Distribución del Software, y otros desafíos de gestión importantes. SpectroGRAPH provee una interfaz gráfica de usuario para la gestión de la red.

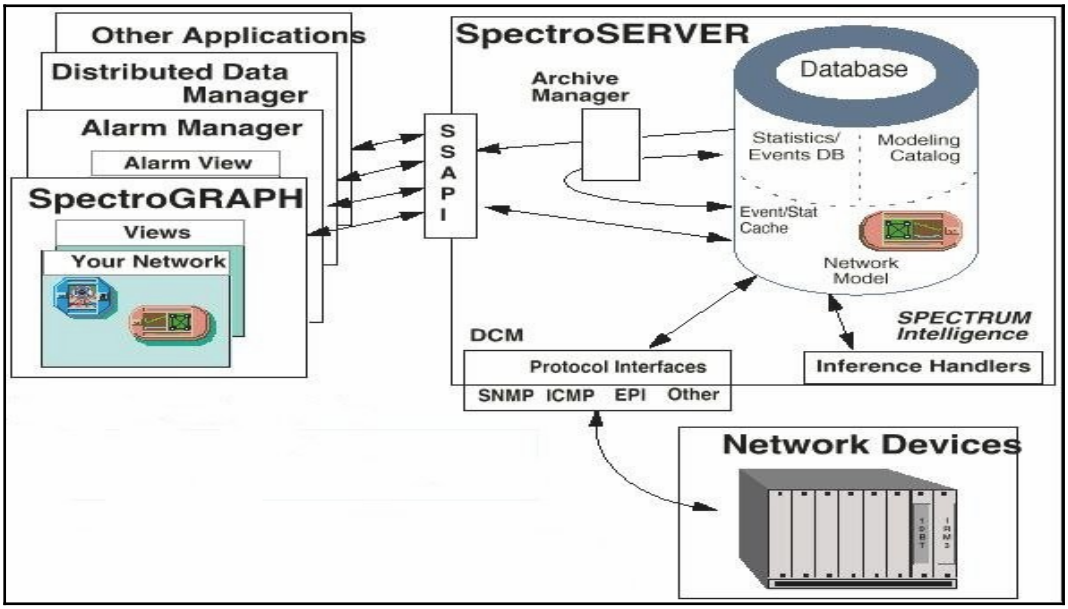


Fig. 4.7 Arquitectura de SPECTRUM Enterprise Manager

Sinopsis Funcional: Cómo trabaja SPECTRUM

El diseño de SPECTRUM está basado en un modelo cliente / servidor. El servidor, SpectroSERVER o Máquina de Red Virtual (**VNM**, *Virtual Network Machine*), incluye la base de datos de SPECTRUM y proporciona capacidades de seguridad, modelamiento, y facilita la administración de dispositivos. SpectroSERVER soporta un conjunto de aplicaciones cliente a través de su Interfaz de Programación de Aplicaciones (**SSAPI**, *Application Program Interface*). La primera aplicación cliente que se mira al iniciar SPECTRUM es SpectroGRAPH.

SpectroGRAPH proporciona la interfaz gráfica de usuario que utiliza para monitorear la red y cargar otras aplicaciones cliente. Las vistas de SpectroGRAPH's contienen una variedad de íconos que representan los diferentes elementos de su red, incluyendo dispositivos, usuarios, y elementos conceptuales como los segmentos de red. Cada ícono presenta información de estado y proporciona acceso para facilitar la administración específica del elemento de red representado. La información presentada por un ícono es recuperada desde un

modelo correspondiente que es mantenida en la base de datos del SpectroSERVER.

El Administrador de Comunicación entre Dispositivos de SPECTRUM (**DCM**, *Device Communications Manager*) proporciona el mecanismo para recuperar información de los dispositivos y administrarlos en la red. El **DCM** consulta cada dispositivo periódicamente para almacenar su último estado en la Base de Datos. El **DCM** es también el mecanismo que permite una administración de elementos. Por ejemplo, cambios administrativos que puede hacer en un modelo mostrado en una vista SpectroGRAPH, como habilitar o deshabilitar un puerto, son interpretadas por SPECTRUM y enviados al dispositivo mediante el DCM donde la acción administrativa es ejecutada. El estado del dispositivo es actualizado en la base de datos y el nuevo estado administrativo es presentado en la vista.

La inteligencia de SPECTRUM es implementada mediante *"manejadores de inferencia"* que añaden un valor a la información colectada. Estos están en capacidad de procesar estadísticas útiles, como paquetes por segundo. También son capaces de interpretar la información colectada de dispositivos individuales y presentar información de diagnóstico que puede ayudar a aislar y responder ante problemas de red.

Los manejadores de inferencia dependen de un adecuado modelamiento de red en la base de datos de SpectroSERVER para un efectivo análisis de los datos colectados.

El modelamiento de red básico debe consistir de modelos de cada dispositivo de red y modelos para los usuarios administrativos y operacionales. Luego, se puede expandir el modelo creando dispositivos adicionales, modelos de campus, como edificios y closets de RACKs y modelos para grupos organizacionales y usuarios.

Componentes de SPECTRUM

La **Figura 4.8** ilustra el sistema de gestión de la base de conocimiento de SPECTRUM. El triángulo más grande representa a SpectroSERVER e incluye la capa de acceso de SpectroSERVER representada por el área compartida, y la base de conocimiento representada en el triángulo más pequeño. La figura muestra información que ha sido añadida a la base de conocimiento mediante el Editor de Tipos de Modelos (**MTE**, *Model Type Editor*) y aplicaciones cliente. También muestra una aplicación cliente interactuando con SpectroSERVER, y la comunicación de los nodos gestionados con el Administrador de Comunicación entre Dispositivos (**DCM**, *Device Communications Manager*).

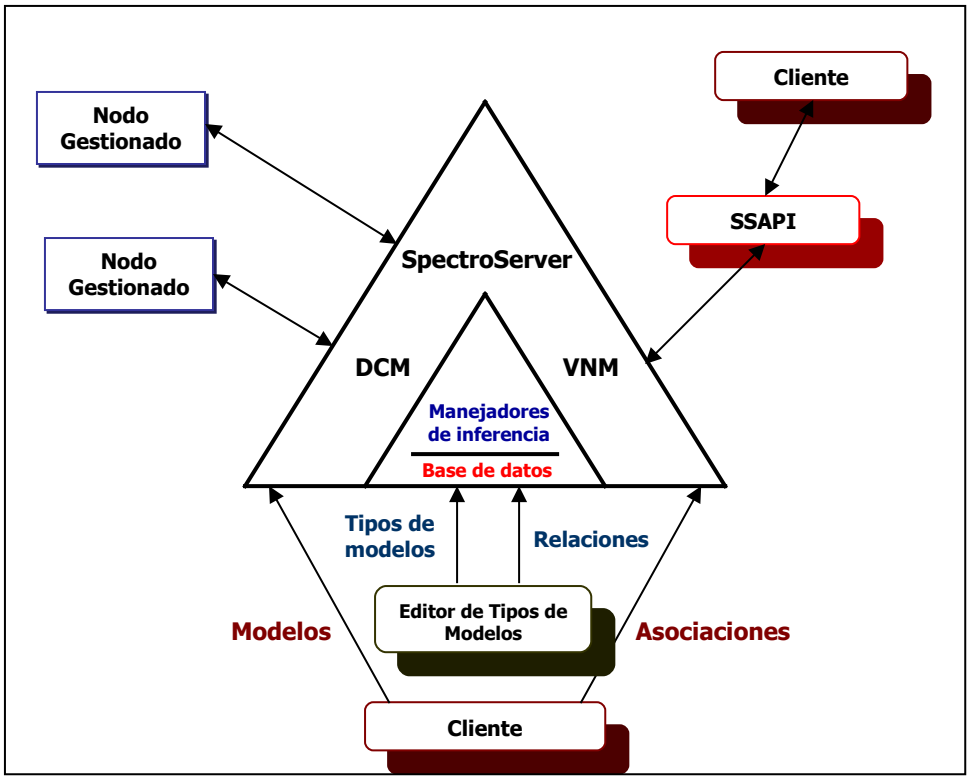


Fig. 4.8 Gestión de la base de conocimiento de SPECTRUM

4.2.4 Gestión de la Seguridad

La seguridad en SPECTRUM permite prevenir accesos no autorizados y edición de varias vistas y modelos. Esas medidas de seguridad también pueden impedir cambios no autorizados de los dispositivos de red descubiertos y modelados en SPECTRUM. La seguridad en SPECTRUM no reemplaza su sistema actual de seguridad de red, pero puede "cooperar" con él.

SPECTRUM proporciona mecanismos de seguridad que extiende la seguridad de las plataformas UNIX o Windows NT. Estos mecanismos establecen:

- Areas en el modelo de red que los usuarios pueden examinar o ver.
- Valores para atributos existentes que los usuarios pueden actualizar.
- Modelos y vistas existentes en SPECTRUM que los usuarios pueden editar.

Los siguientes términos describen conceptos que son la base de la seguridad en SPECTRUM:

1. **Comunidad de seguridad**: define áreas de acceso, proporciona un mecanismo para agrupar vistas y modelos de red para el control de acceso de los usuarios. El acceso hacia una comunidad de seguridad se determina comparando un modelo de cadena de seguridad con un modelo de cadena de comunidad.

2. **Cadena de seguridad**: define los requerimientos para accesar hacia un modelo para usuarios de SPECTRUM. Cada cadena de seguridad consiste de una o más entradas de comunidad.

3. **Cadena de comunidad**: define comunidades de seguridad que permiten a un usuario el acceso, establecimiento y edición de privilegios. Cada entrada define una o más comunidades de seguridad específicas y los niveles de privilegios de acceso asociados a cada uno.

La comunidad ADMIN contiene a todos los modelos en SPECTRUM. Se debe determinar la estructura de las comunidades como parte de la planificación para la seguridad de la red. Las comunidades pueden ser establecidas como únicas o como parte de otras comunidades. Los nombres de las comunidades de seguridad las determina el Administrador de la red.

SPECTRUM compara el valor de la cadena de comunidad con el valor de la cadena de seguridad para determinar cuando un modelo de usuario ha visualizado o editado privilegios en los modelos de red o vistas.

Niveles de privilegio de acceso:

0-4 Vizualización, actualización y privilegios de edición.

5.9 Solamente visualización (no permite edición o actualización de privilegios).

ADMIN,0	Todos los privilegios administrativos
ADMIN,5	Todos los privilegios para visualizar
ADMIN,6:Local,0	Todos los privilegios para vizualizar y actualizar con limitación de privilegios de edición. Este usuario puede navegar en todas las vistas y puede editar los modelos de la comunidad **Local**.

4.2.5 Gestión de la Configuración

Descubrimiento de equipos

El proceso de descubrimiento de equipos (ver **Fig 4.9**) se realiza en tres fases utilizando varios métodos de descubrimiento (Descubrimiento de Routers, Descubrimiento de LANs, Descubrimiento de prueba de rango, descubrimiento en base a NIS y descubrimiento de tablas ARP) y utilizando los protocolos ICMP y SNMP:

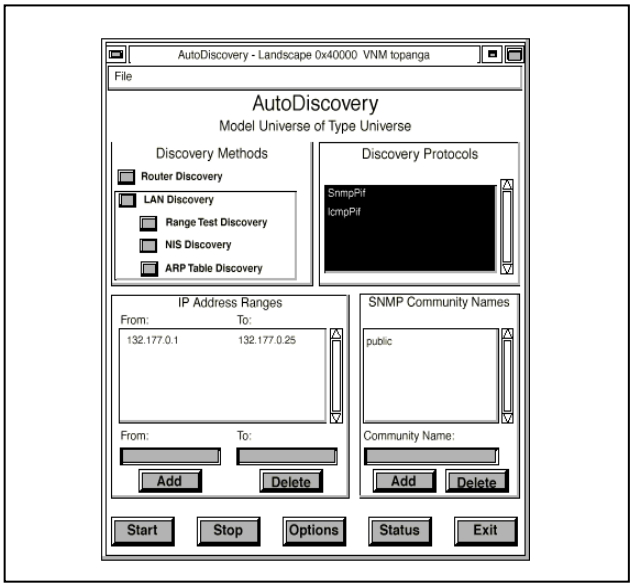


Fig. 4.9 Descubrimiento de equipos en SPECTRUM

- **Fase Uno - El nivel Router/Red:** AutoDiscovery lee las tablas de ruteo para identificar los routers más cercanos. Las direcciones son analizadas en términos del rango de búsqueda establecido en la sesión de descubrimiento. Siempre y cuando estén en el rango (o asociados con direcciones destino del rango) son añadidas a la lista de routers.

- **Fase Dos - El nivel LAN/Bridge:** aquí AutoDiscovery utiliza uno o más de tres métodos de descubrimiento selec-cionables por el usuario para examinar cada una de las LANs descubiertas en la Fase Uno. Durante el transcurso del

examinamiento de cada LAN, AutoDiscovery localiza y modela todos los bridges (puentes) y usa su información de interfaz para modelar y ubicar LANs discretas (802.3, 802.5, etc.) a las que los puentes interconectan. Si no se encuentran puentes, se examinarán los hubs, y si un hub muestra un tipo de interfaz que corresponda a una red LAN discreta, ésta se creará.

- **Fase Tres – El nivel LAN discreta/Hub:** en la tercera fase del descubrimiento, los métodos de descubrimiento seleccionados son usados para examinar cada una de las LANs descubiertas en la Fase Dos. Cada Hub es localizado y modelado, AutoDiscovery trata de identificar y modelar los dispositivos conectados a cada uno de sus puertos. Otros dispositivos multipuerto no-inteligentes, como los transceivers multipuerto con varios usuarios conectados, son modelados como fanouts.

Métodos de descubrimiento

- **Descubrimiento de Routers:** cuando este método es seleccionado, AutoDiscovery busca en la base de datos de SPECTRUM un modelo de router "semilla" que es usado como base en el descubrimiento de la Fase Uno. Por defecto, este método utiliza las Tablas de Ruteo IP de los routers semilla para buscar y modelar los routers más cercanos.

- **Descubrimiento de LANs:** este método permite el mapeo de modelos de dispositivos existentes (por ejemplo, aquellos dispositivos descubiertos durante una sesión de descubrimiento en segundo plano) en el nivel LAN/bridge. También puede correr AutoDiscovery solamente con este método seleccionado, éste se selecciona automáticamente al seleccionar cualquiera de estos tres métodos: Range Test, NIS, o ARP Table.

- **Descubrimiento con Prueba de Rangos (Range Test Discover)**: cuando este método está habilitado, AutoDiscover usa peticiones de eco ICMP (pings) para probar que cada una de las direcciones IP están en el rango o rangos especificados. Una dirección que responde a un ping es sujeta a los protocolos ICMP y SNMP para ser identificada y modelada. También este método proporciona cobertura para un rango dado, pero en términos de uso de ancho de banda su uso no debe considerarse en rangos muy extensos.

- **Descubrimiento NIS:** (solamente en Solaris) este método limita el descubrimiento a los dispositivos direccionados en la tabla host del sistema Solaris NIS (Network Information Service).

- **Descubrimiento de tablas ARP (ARP Table Discover):** este método permite al AutoDiscover asociar una dirección IP descubierta a una dirección física MAC.

Edición de Mapas/Modelamiento de la Red

Modelamiento de la Red: proceso de creación y ubicación de modelos que representan entidades de la red en vistas específicas.

Existen tres jerarquías de modelamiento que son usadas para modelar una red: *topología, localización y organización*.

Una vez creado el modelo topológico, las jerarquías restantes pueden ser modificadas manualmente.

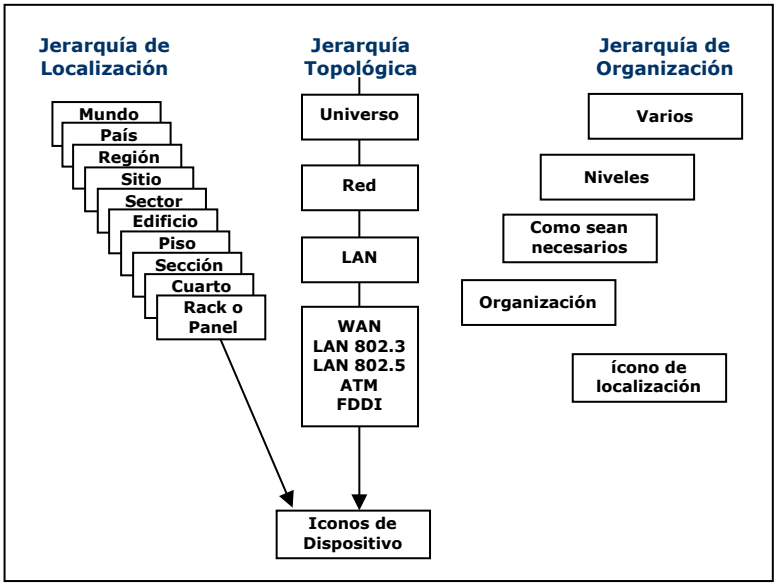


Fig. 4.10 **Jerarquías de modelamiento en SPECTRUM**

Localización de modelos

Para ubicar los modelos (entidades que representan la red en vistas específicas) se pueden tener algunos atributos para encontrarlos como: la MAC, nombre del modelo, tipo del modelo, direcciones de red, direcciones de puerto o interfaz, número de serie, fecha de creación del modelo, condición de estado del modelo, etc.

Presentación de Variables MIB

SPECTRUM posee vistas que utilizan variables MIB sobre la configuración de dispositivos SNMP genéricos, información de monitoreo, como el flujo del tráfico y errores de datos, estado actual de las interfaces, etc.

Representación física / lógica de los dispositivos

SPECTRUM posee vistas que permiten ver las Interfaces y los Chassis de los dispositivos con módulos genéricos de gestión SNMP (ver **Fig. 4.11**).

Las características de las vistas de un dispositivo típico incluyen:

- LEDs que representan el cambio de estado de acuerdo con la actividad del dispositivo.
- Dispositivos Multi-slot, como hubs, muestran tarjetas individuales para cada slot.
- Algunos tipos de modelos tienen vistas específicas de puerto, como Rendimiento.
- Al hacer Doble-click en un conector de puerto se tiene acceso a la vista de rendimiento del mismo.
- Los menús permiten mostrar una vista Física o Lógica del dispositivo MIM (Media Interface Module, Módulo de Interfaz de Medios).

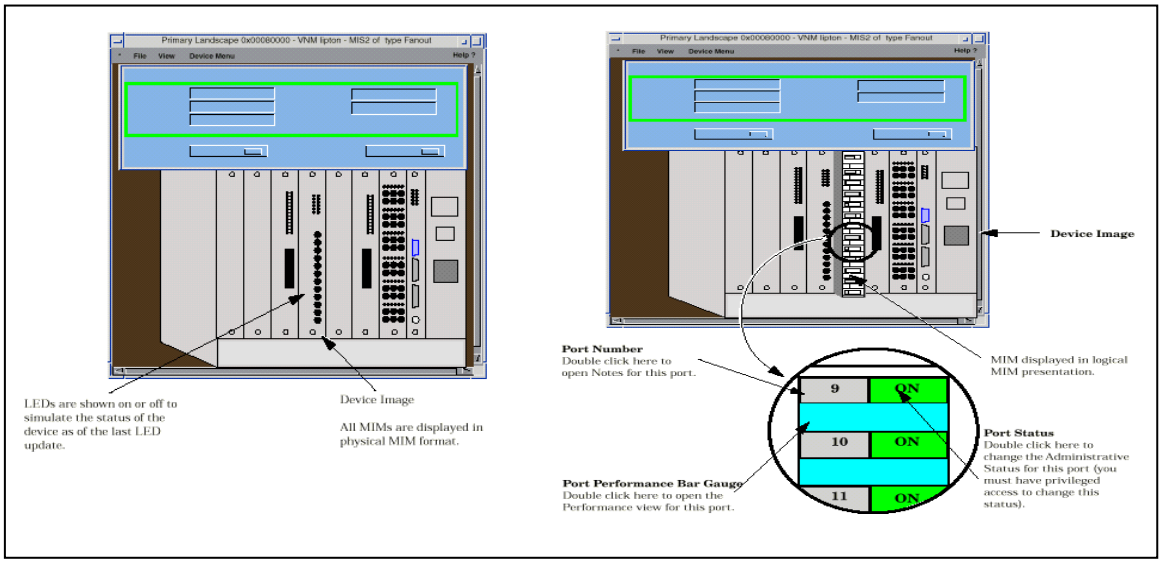


Fig. 4.11 Representación física / lógica de los dispositivos gestionados por SPECTRUM

4.2.6 Gestión de Fallas y Recuperación

Cuando existe un problema en la red, SPECTRUM realiza varias cosas para alertar al administrador sobre los sucesos ocurridos, y le permite aislar e identificar el problema. Como se muestra en la **Figura 4.12**, los iconos de SPECTRUM cambian de color inmediatamente para indicar el tipo y severidad de la alarma. También produce una alarma audible. El cambio de la alarma e información detallada

aparece automáticamente en el Administrador de Alarmas (Alarm Manager). Apartir de aquí, la responsabilidad en la solución de los problemas en la red depende de las instrucciones del encargado de la gestión de la red.

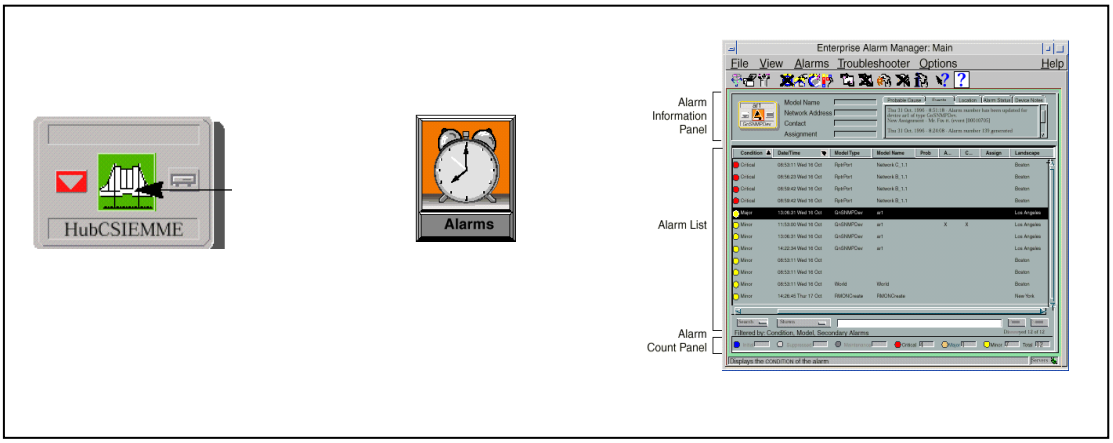


Fig 4.12 Gestión de fallas en SPECTRUM

Detección de Fallas

Las fallas son detectadas a través de Traps recibidas del dispositivo o configuradas a través de SPECTRUM (ver **Fig. 4.13**). Estas traps son utilizadas para generar condiciones RollUp, condiciones de los dispositivos, alarmas, y mensajes de eventos para cualquier puerto o dispositivo.

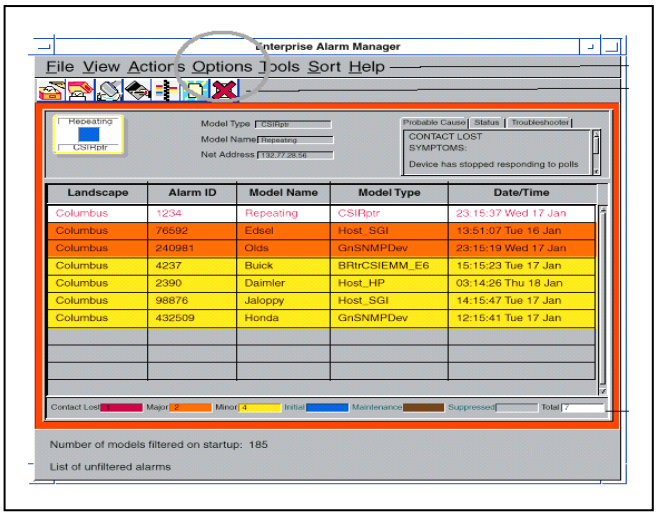
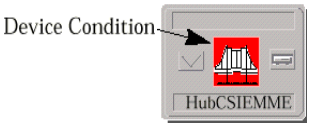


Fig. 4.13 Detección de fallas en SPECTRUM

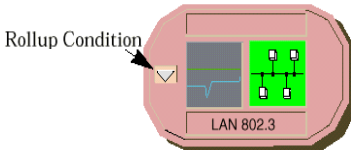
Qué indican los Colores de Condición de Dispositivo



Los colores de condición del dispositivo reflejan el estado de un modelo representado por un icono. Si un evento causa el cambio del color de condición, este es registrado en el Historial de Eventos (Event Log). El Alarm Manager indicará el Síntoma/Probable Causa y recomendará acciones para el evento.

- **Verde:** bien, contacto establecido, operación normal.
- **Amarillo:** alarma menor, primer nivel de operación marginal (una situación ha ocurrido pero no requiere una acción inmediata) o dirección IP duplicada.
- **Anaranjado**: alarma mayor, el dispositivo está funcionando pero no responde ante solicitudes de gestión. Pérdida del servicio (SNMP). Una acción es requerida en corto tiempo.
- **Rojo:** crítico, el contacto con el dispositivo se ha perdido. Requiere una acción inmediata.
- **Gris:** desconocido, este dispositivo no puede ser accedido debido a una condición de error que existe en otro dispositivo.
- **Azúl:** inicial, el contacto con el dispositivo todavía no se ha establecido.
- **Marrón:** el dispositivo ha sido puesto fuera de servicio para propósitos de mantenimiento.

Qué indica el color de una condición Rollup



Cuando ocurre una falla con un dispositivo, una Trap es generada por el dispositivo o por SPECTRUM para propósitos de gestión de red. SPECTRUM recibe la trap y genera un color de condición del dispositivo que indica su estado. La importancia del dispositivo en la red determina el valor de significancia que tendrá en la condición.

- **Amarillo:** alarma de información.
- **Anaranjado:** falla menor del sistema o subsistema.
- **Rojo:** falla mayor del sistema o subsistema.

Aislamiento de la Falla

La detección de fallas es el primer paso en el aislamiento de fallas. SPECTRUM detecta que una falla ha ocurrido y genera una alarma. Una vez que la falla ha sido detectada, puede usar las características de SPECTRUM para navegar en las vistas e identificar la red específica, dispositivo, canal, o puerto que generó la alarma.

4.2.7 Gestión del Rendimiento

Cada sistema de red tiene cuatro componentes centrales: Disco, E/S, memoria, y CPU. SPECTRUM posee un conjunto de vistas que permiten visualizar estadísticas del rendimiento en los componentes antes mencionados (ver **Fig. 4.14**).

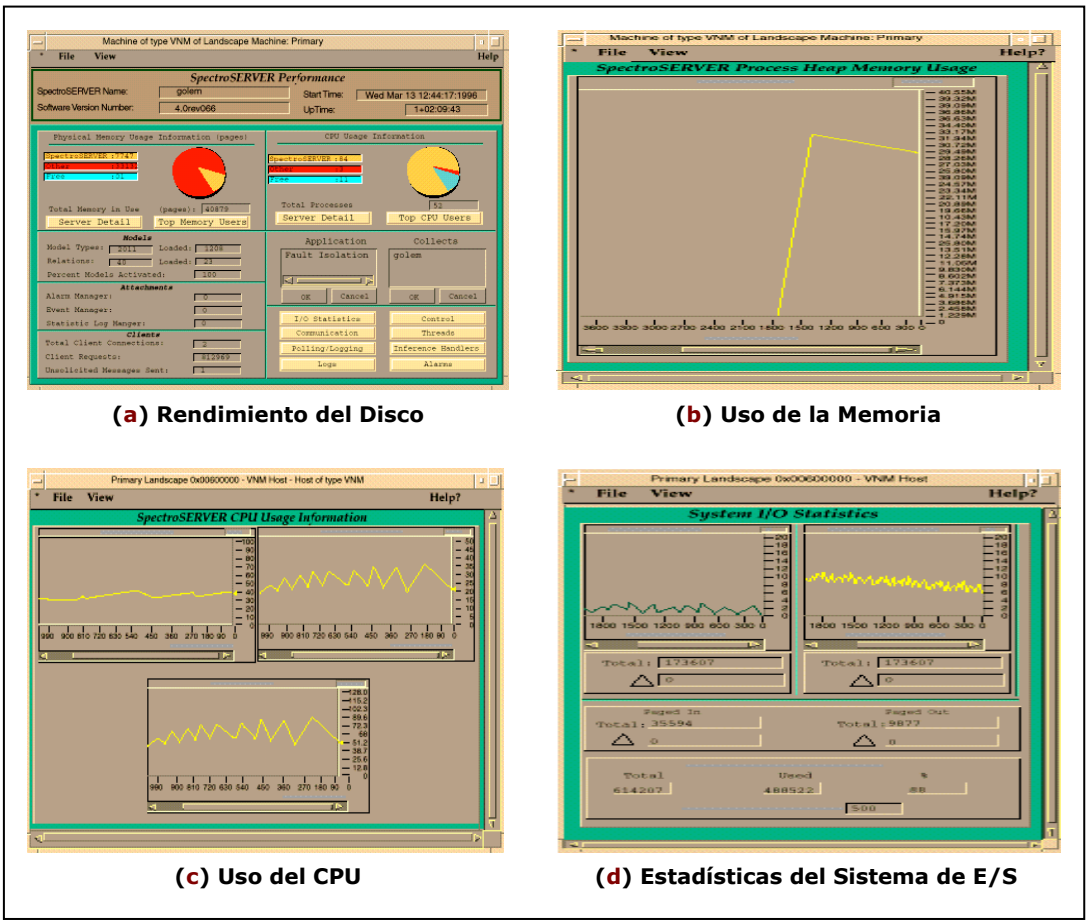


Fig. 4.14 Vistas de Rendimiento de los componentes centrales de SPECTRUM

Las vistas de Rendimiento de SPECTRUM (ver **Fig. 4.15**) proporcionan estadísticas de red detalladas para cada interfaz. La vista sumariza el flujo de tráfico en paquetes. Permiten visualizar El uso de la memoria y CPU de las estaciones de trabajo en dónde se encuentra instalado SpectroSERVER.

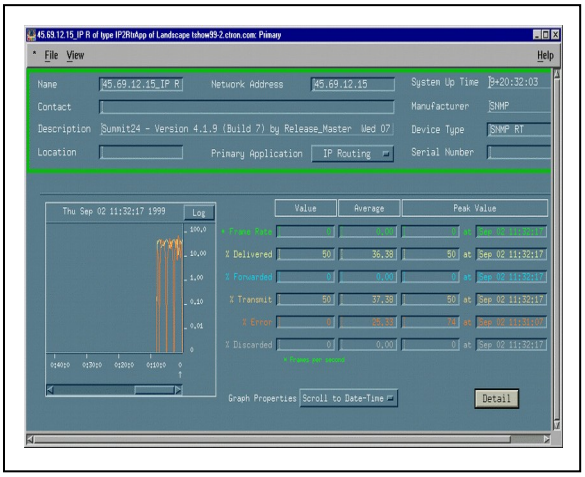


Fig. 4.15 Vista de Rendimiento de interfaz

4.3 Microsoft Systems Management Server 2.0

Microsoft Systems Management Server (**MSMS**) 2.0 es una herramienta para la gestión de redes locales así como de redes de área extensa, entre sus principales servicios incluye el inventario detallado de hardware, medición e inventario de software, distribución e instalación de software y herramientas para la solución de problemas a distancia. Además es un software creado bajo los protocolos estándar de administración de redes, asegurando la compatibilidad con herramientas de administración complementarias así como equipos activos de casas diferentes que conforman una red.

MSMS está estrechamente integrado con Microsoft SQL Server y el sistema operativo Microsoft Windows NT Server, lo que permita que sea un software muy seguro y le permita trabajar en cualquier tipo de redes Windows, además de proveer permisos de administración a usuarios o grupos de usuarios específicos para tareas específicas.

4.3.1 Características de MSMS

- Administración de equipos basada en directivas: mediante la utilización de las directivas de sistema de Microsoft para Windows NT Workstation, Windows 95, Windows 98, Office 97 e Internet Explorer.
- Integración con Microsoft SQL Server y Windows NT Server.
- Administración de cambios en la configuración de equipos de escritorio Windows.
- Inventario detallado de hardware y software.

- Distribución programada de software.
- Solución remota de problemas.

4.3.2 Plataformas Soportadas

Microsoft Systems Management Server soporta la plataforma Windows NT.

Requerimientos para Windows NT

- Microsoft Windows NT 4.0 con Service Pack 4 o superior.
- Microsoft SQL Server 6.5 con Service Pack 4 o superior (requerido para el servidor principal).
- Procesador Intel Pentium de 133 Mhz o superior.
- De 64 a 96 MB de RAM (se recomienda 128 MB).
- Se requiere un GB de espacio disponible en el disco duro.

4.3.3 Arquitectura del MSMS

El diseño de Microsoft Systems Management Server se basa en componentes.

Existe una estrecha relación entre los componentes y la base de datos. MSMS puede ser configurado para que pueda gestionar redes LAN o WAN con Servidores llamados Servidores de Sitio (**SS**, *Site Servers*), creando de esta forma árboles jerárquicos (ver **Fig. 4.16**).

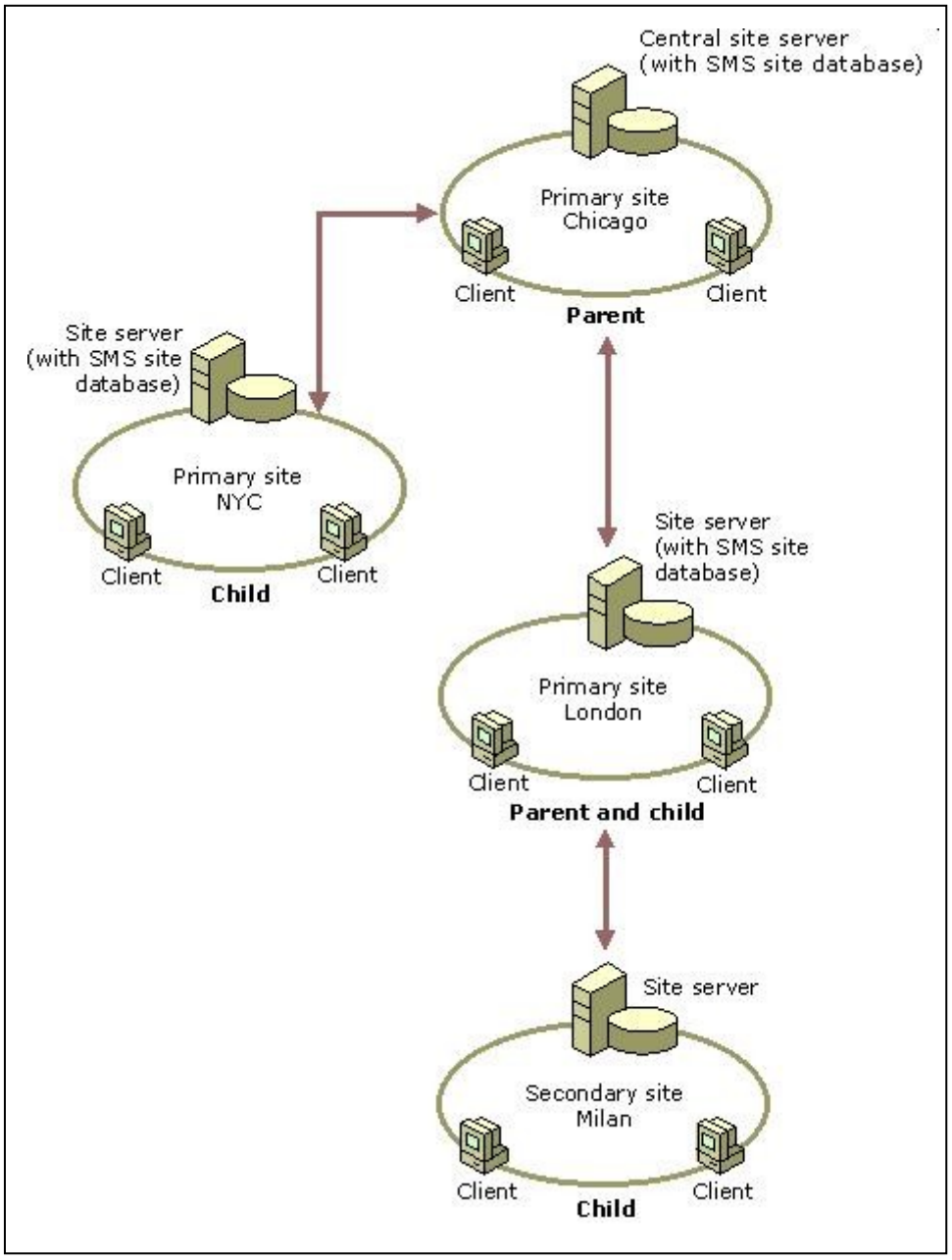


Fig. 4.16 **Arbol jerárquico de Servidores de Sitios**

La gestión se descentraliza para una mayor velocidad del monitoreo, los Servidores Primarios de Sitio (**PSS**, *Primary Site Server*) configuran y controlan a los Servidores Secundarios de Sitio (**SSS**, *Secondary Site Server*), de esta manera los eventos que sucedan debajo del Servidor Secundario de Sitio se reportan a éste y dependiendo de su configuración, se replican al Servidor Primario de Sitio.

A continuación, en la **figura 4.17**, se muestra la arquitectura de Microsoft Systems management Server.

Los componentes principales del Servidor SMS son servicios que se instalan en un Servidor de Sitio.

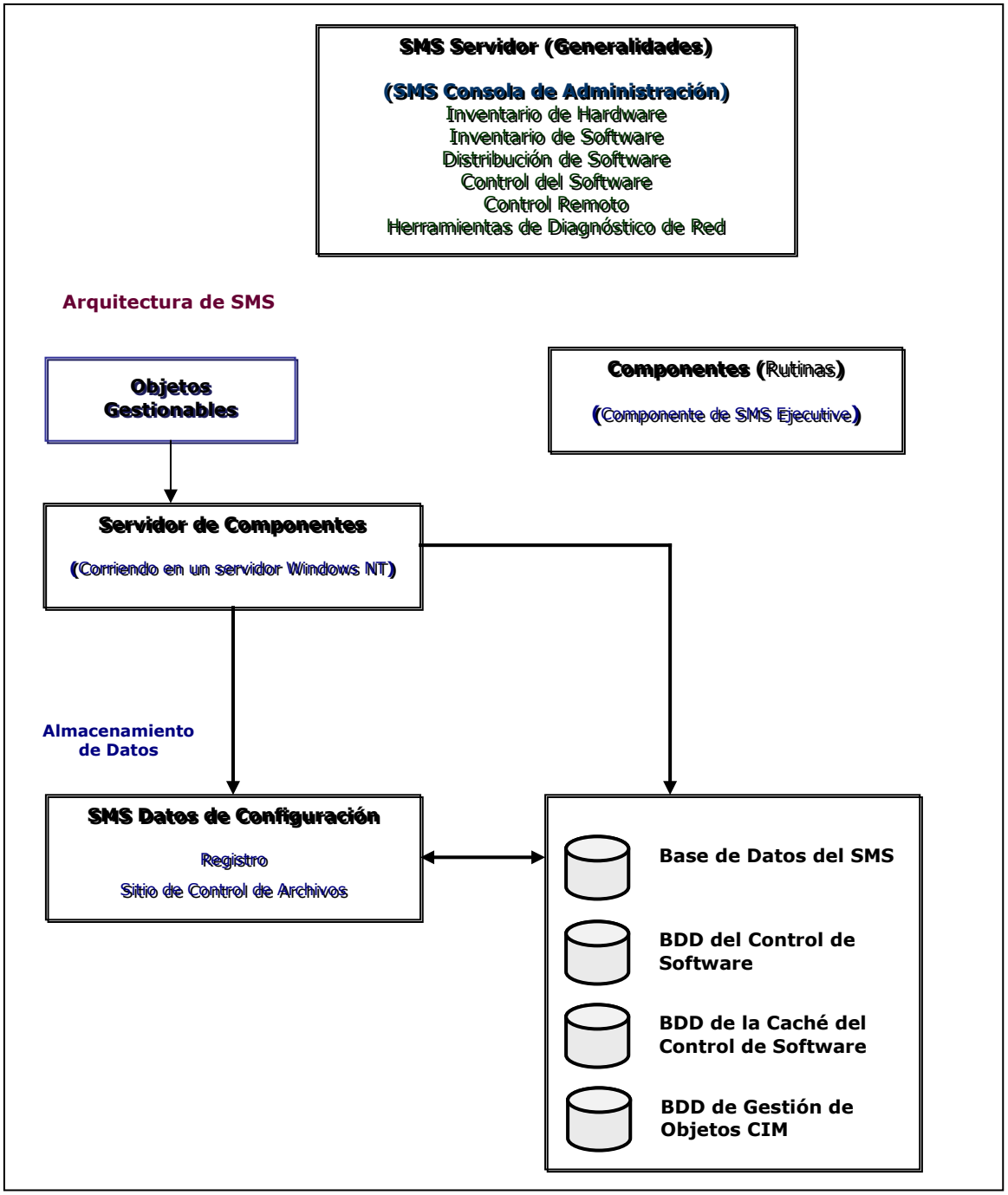


Fig. 4.17 **Arquitectura de Microsoft System Management Server**

El servidor de componentes contiene programas que funcionan en conjunto para que el SMS realice tareas especificas. Cuando SMS es instalado, el servicio de componentes se ejecuta automáticamente, este servicio puede ser iniciado o detenido desde el Panel de Control -> Servicios de Windows NT.

El número de componentes de servicio activos en cada servidor depende de las opciones que SMS le ofrece al instalar en el servidor.

Las peticiones de los objetos gestionados o recién descubiertos llegan a un Servidor de Sitio, que valida los datos como usuario, dominio, características, etc, una vez validada la información y dependiendo de las peticiones del Administrador se llama a cada uno de los componentes para ejecutar dicha tarea y si es preciso ingresa a la base de datos de configuración o directamente a la base de datos del Servidor de Sitio.

Los principales componentes (rutinas) de un Servidor de Sitio son:

- **Comunicación:** estos componentes proporcionan a SMS toda la conectividad entre componentes. Ellos también replican y copian archivos y datos en directorios donde se encuentra el Servidor SMS y por todos los sitios y clientes dentro de la jerarquía.

- **Configuración/Control:** estos componentes se instalan en clientes, y se monitorean desde el Servidor SMS.

- **Descubrimiento:** estos componentes identifican y capturan información básica sobre los recursos de la red. La meta de descubrimiento es identificar y recoger datos (nombres de NetBIOS, información del sistema, y así sucesivamente) sobre los dispositivos de la red. Específicamente, SMS descubre computadoras para que ellos puedan instalarse como clientes.

- **Mantenimiento:** estos componentes supervisan acciones de SMS que se unen con la base de datos y proporcionan ayuda apropiada manteniendo la integridad de los datos y las operaciones, SMS guarda toda esta información en la Base de Datos del Servidor SMS.

- **Estado:** estos componentes supervisan las acciones que ocurren en un Servidor de Sitio de SMS e informan su estado a través de la Consola de Administración del SMS.

- **Tareas:** estos componentes crean un proceso para cada una de las tareas principales de SMS como inventario del hardware y software, distribución y control del software.

- **Almacén de datos:** un ambiente de información dinámica debe tener un sitio central donde la información crítica y operaciones se guarden, los componentes de servicio y subcomponentes necesitan acceso a sus datos de configuración, tiempos establecidos de funcionamiento y los datos en sí del SMS. Por ejemplo, datos que el Administrador necesita saber, datos a evaluar, cuándo evaluarlos, y qué recursos pertenecen a cada dispositivo específico. Para hacer esto, necesita acceso a los datos de la configuración así como los datos guardados en la base de datos del Servidor SMS.

  Existen dos tipos básicos de Almacén de datos.

  a) **Datos de configuración:** se recogen de escenas predefinidas instaladas con SMS, los cambios se realizan a través de la consola de administración del SMS.

     SMS es un sistema dinámico que le permite que tome decisiones sobre cómo y cuándo el sitio operará. Cuando la configuración cambie, SMS pone al día el archivo de mando de sitio y el registro. La mayoría

de los servicios de SMS trabajan en función de un horario. Así, después de que los servicios y componentes se inician, ellos verifican el archivo de mando de sitio periódicamente para su configuración.

b) Datos del sistema: se recogen de los recursos de la red. Se actualizan de acuerdo a los cambios que se realizan dentro de esta, por ejemplo cuando en una empresa se cambia el hardware, software, se adquieren nuevas computadoras, sistemas viejos que necesitan ser actualizados. SMS guarda esta información en la base de datos del Servidor SMS.

4.3.4 Gestión de la Seguridad

Systems Management Server hace uso de la seguridad integral de Windows NT Server, permitiendo la otorgación de privilegios a usuarios específicos para realizar tareas como la distribución programada de software en las PCs de los clientes.

MSMS utiliza la administración basada en directivas. Aunque no forma parte de Systems Management Server 2.0, merece la pena investigar este método. El método de utilización de directivas (ver **Fig. 4.18**) se describe a continuación:

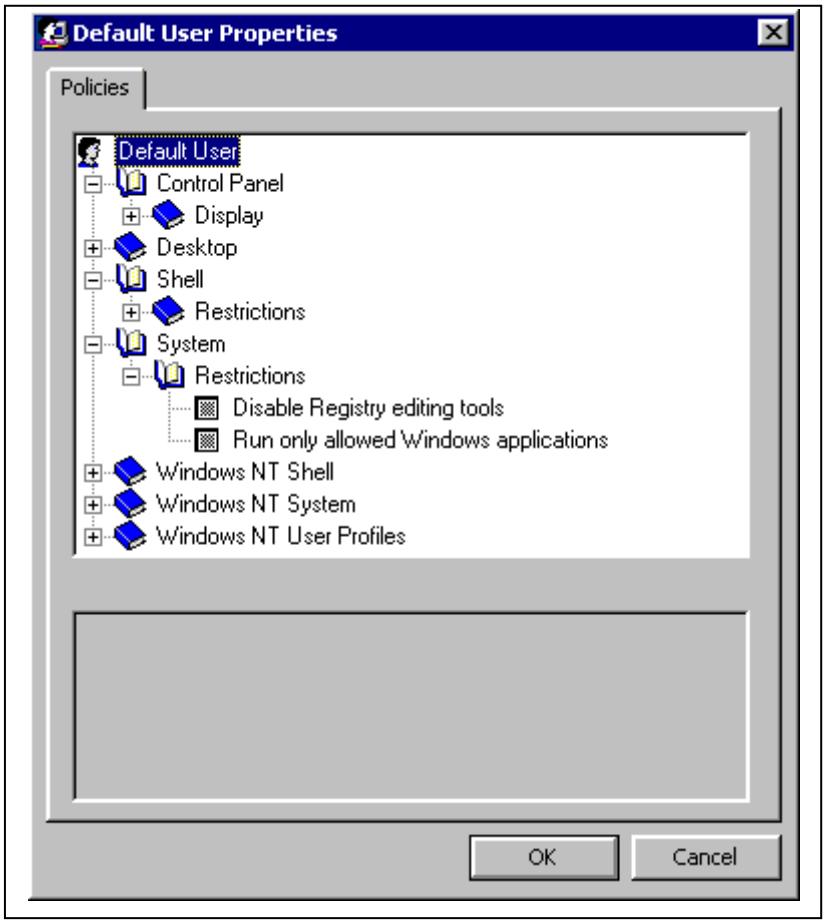


Fig. 4.18 **Herramienta Editor de Directivas**

- La administración de directivas comienza con un subprograma llamado Editor de directivas.

- El administrador abre este subprograma y crea un archivo de directiva que contiene restricciones para todos los usuarios, grupos y estaciones de trabajo de una empresa.

- Estas restricciones pueden incluir elementos en los que los cambios de los usuarios pueden ser perjudiciales para el sistema, como las herramientas de modificación del Registro y otros valores de configuración del sistema.

- Estas restricciones también pueden incluir la apariencia del escritorio y la disponibilidad de las aplicaciones.

- Estas restricciones se han ampliado para que incluyan también restricciones de Office 97 e Internet Explorer.

- Este archivo se almacena en el controlador principal de dominio y se duplica en todos los controladores de reserva para garantizar la disponibilidad independientemente de dónde se autentique al usuario.

- Cuando un administrador cambia este archivo, el proceso de duplicación natural actualiza el archivo en toda la empresa.

- El usuario recobra la configuración en su próximo inicio de sesión.

4.3.5 Gestión de la Configuración

Existe una herramienta nueva en Microsoft Systems Management Server 2.0 que ayuda en la gestión general de la infraestructura de una red. Se trata de la herramienta Network Trace, la cual permite al administrador crear una vista gráfica de todos los recursos de la red, incluidos los ruteadores, impresoras, estaciones de trabajo y servidores (ver **Fig. 4.19**). Esta utilidad realiza el seguimiento de las rutas de comunicación entre el servidor y todos los sistemas del sitio para mostrar los dispositivos de red con los que el servidor del sitio se puede comunicar, sus funciones en el sistema, las direcciones IP y otra información.

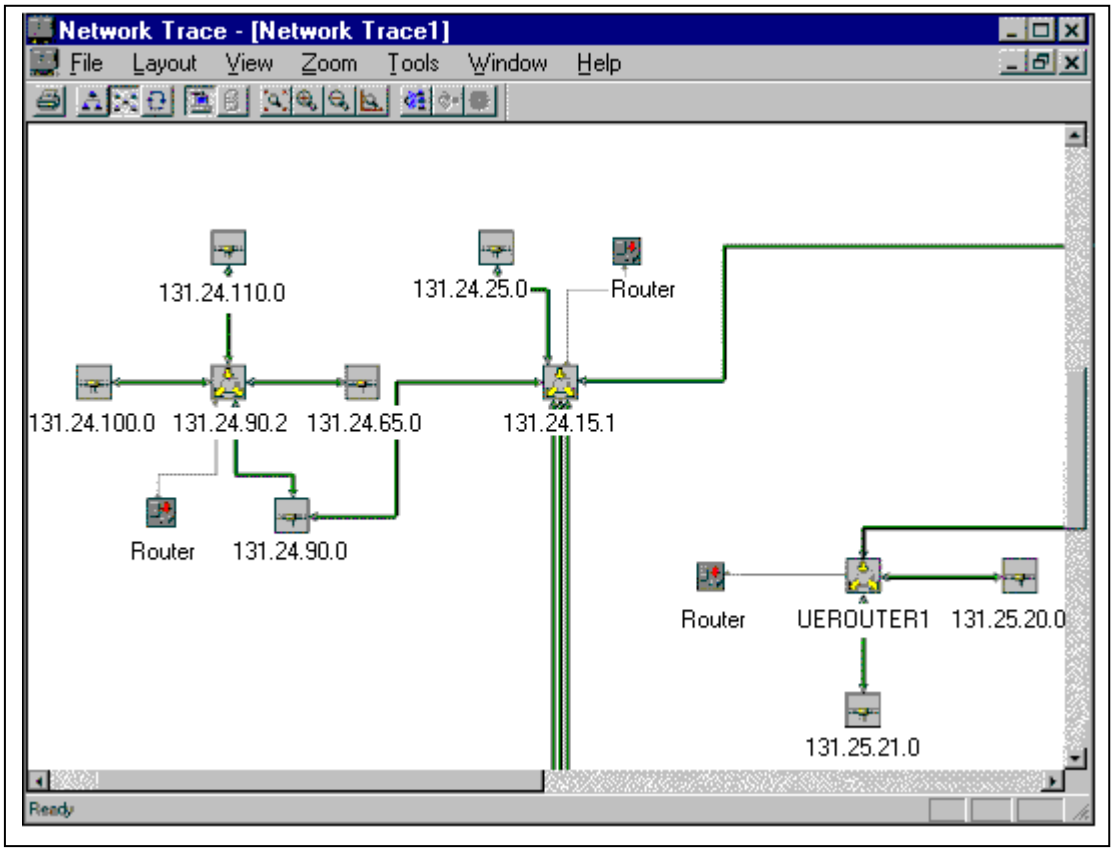


Fig. 4.19 **Herramienta Network Trace**

Configuración del Inventario de Hardware

La configuración del inventario de hardware de Systems Management Server resulta sencilla. A continuación se muestran los pasos:

- Descubrir recursos de la empresa según la configuración IP, configuración de usuarios y grupos de NT o Novell, o un conjunto de otros métodos de descubrimiento.

- Convertir estos recursos en recursos de MSMS mediante secuencias de comandos que Systems Management Server configura automáticamente o incluso incluir las partes de cliente automáticamente en el caso de Windows NT.

- El software de cliente de MSMS se distribuye automáticamente al cliente, incluido el agente de inventario de hardware que se basa en la especificación Modelo de Información Común (CIM, *Common Information Model*) desarrollada por el Grupo de Trabajo para la Gestión de Equipos de Escritorio (**DMTK**, *Desktop Management Task Force*), como parte de la iniciativa de Gestión Empresarial Basada en Web.

- Los agentes de cliente recopilan un inventario del hardware del cliente y almacenan los resultados en el cliente.

- Esta información se pasa a través de un punto de acceso de cliente (CAP) a la base de datos del sitio.

Se recopila e informa de más de 200 propiedades, y se incluyen detalles como los siguientes: número de unidades de disco, tipo de procesador, cantidad de memoria, sistema operativo, configuración de monitor y de pantalla, nombre de equipo y dirección IP, información acerca de los periféricos conectados al recurso, tipo de red e información del BIOS.

Se realiza un seguimiento del historial de toda la información del inventario para ayudar a solucionar problemas en el futuro.

Configuración del Inventario de Software

Para proporcionar el inventario de software, Systems Management Server 2.0 busca información de recursos de versión en cada archivo ejecutable (de forma predeterminada) del equipo cliente. Esta configuración se puede ampliar para descubrir cualquier tipo de archivo de una estación de trabajo. A continuación, la información de recursos se organiza por fabricante para facilitar la elaboración de informes (ver **Fig. 4.20**).

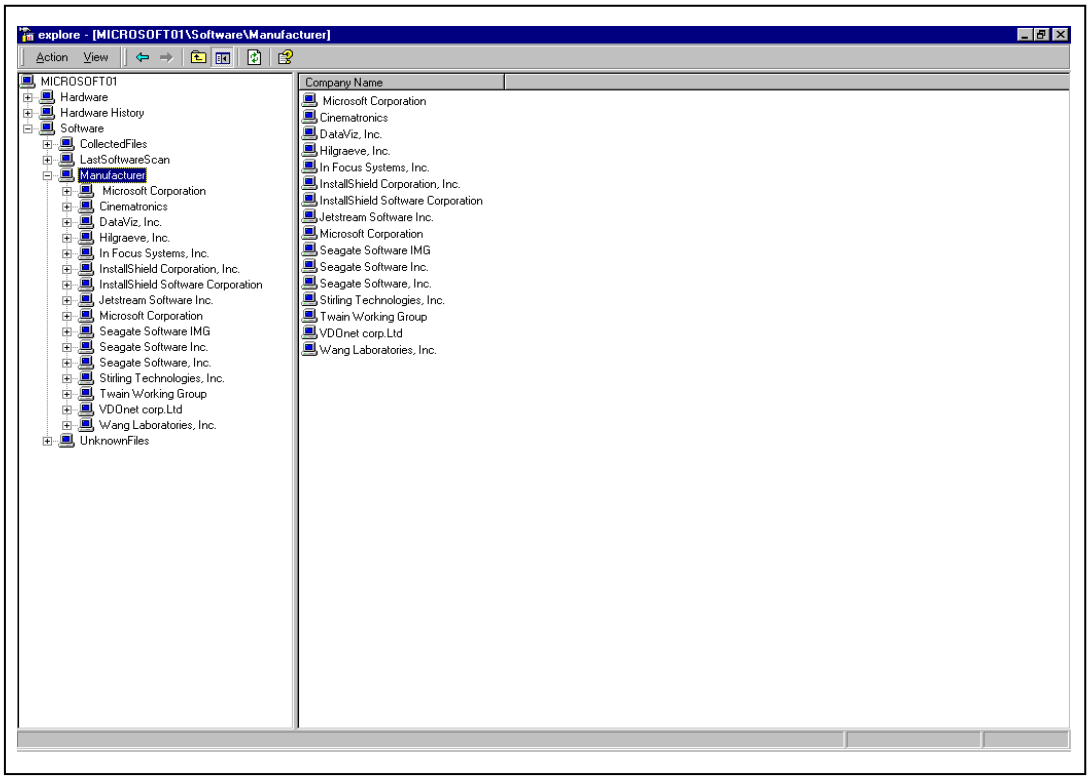


Fig. 4.20 Inventario de Software

Administración Remota de Estaciones de Trabajo

El agente de control remoto de Systems Management Server posee las características mencionadas a continuación:

- Reconciliación de seguridad para varios sitios: de esta forma se evita que se utilice la consola de administrador para tomar el control ilegalmente de un cliente.

- Detección inteligente de anteriores iteraciones o versiones inferiores del software de control remoto. El agente de Systems Management Server 2.0 detecta al agente anterior en el cliente, deniega la instalación y notifica al administrador que se ha producido un conflicto en lugar de comprometer la funcionalidad de control remoto en el cliente.

- Capacidad para administrar la instalación y desinstalación del control remoto en todos los clientes de la empresa desde la consola de Administrador de Systems Management Server.

- De forma similar, todos los clientes de una empresa pueden administrarse según la configuración que dicta el administrador. No es necesario realizar cambios en la configuración de cada cliente.

- Configuración segura del Registro: si el usuario realiza cambios en el Registro que entran en conflicto con la configuración del sitio, un proceso de seguridad interno sobrescribirá los cambios con la configuración del administrador.

- Reinicio mejorado de clientes de Windows 95 y Windows 98 con resolución de 16 colores.

4.3.6 Gestión de Fallas y Recuperación

Mediante el Monitor de red se puede observar el estado de cada dispositivo conectado a ella. En caso de una falla MSMS alerta al encargado de la gestión de la red del mal funcionamiento, o falla, del dispositivo y almacena esta información en la base de datos de MSMS para tener una bitácora del funcionamiento de la red.

También se pueden identificar problemas como protocolos no deseados, direcciones duplicadas de IP e intentos de irrumpir en Internet al monitorear el tráfico de la red.

La consola de administración de HealthMon es un componente de Systems Management Server que proporciona una vista central, gráfica y en tiempo real

del estado de servidores Windows NT 4.0 y BackOffice. A partir de grados de gravedad marcados con colores, se pueden ver las condiciones de funcionamiento, que incluyen tanto los estados normal como de excepción.

El componente de supervisión de HealthMon contiene un conjunto de directivas de supervisión predefinidas que identifican la métrica y criterios de las condiciones normal, anormal (advertencia y crítica) y desconocida.

4.3.7 Gestión del Rendimiento

Mediante la herramienta Monitor de Red se puede obtener una supervisión del tráfico de la misma, ya que permite: capturar, filtrar, decodificar, analizar y editar los paquetes de protocolos de red, incluyendo TCP, IPX/SPX, NetBIOS y SNMP. Esto impide que se saturen las conexiones de red al regular el tráfico por el ancho de banda usado (reducción de los cuellos de botella).

La herramienta Crystal Info posee una gran cantidad de informes que permiten, a los encargados de la gestión de la red, realizar una adecuada planificación del uso de los recursos. Con la interpretación de los informes se puede controlar la instalación de aplicaciones, realizándolas en fechas que no saturen la utilización del ancho de banda de la red y que no interfieran con la ejecución de aplicaciones cruciales de la organización.

Referencias Bibliográficas

1. **IBM Corporation., "TME 10 NetView Concepts – A General Information Manual - Version 5"**, IBM Corporation., Thornwood New York - USA 1997.
2. **COOK Catherine, DARWAMAN Budi, FOSTER Mike y otros., "An Introduction to Tivoli Enterprise"**, Redbook, International Technical Support Organization - IBM Corporation., Austin Texas - USA 1999.
3. **FEARN Paul, OLSSON Arne, BAJUK Larry y otros., "Integrated Management Solutions Using NetView Version 5.1"**, Redbook, International Technical Support Organization - IBM Corporation., Austin Texas - USA 1999.
4. **UELPENICH Stefan, ANDERS Karl, FRANKE Martin y otros., "A Project Guide for Deploying Tivoli Solutions"**, Redbook, International Technical Support Organization - IBM Corporation., Austin Texas - USA 1999.
5. **HAWES Richard, MAYERHOFFER Guenther, SCHUSTER Thomas., "Tivoli Security Management Design Guide"**, Redbook, International Technical Support Organization - IBM Corporation., Austin Texas - USA 1998.
6. **DARMAWAN Budi, KÖPPE Adelbert., "Using Tivoli NetView Performance Monitor (NPM)"**, Redbook, International Technical Support Organization - IBM Corporation., Austin Texas - USA 2000.
7. **CABLETRON Systems., "Getting Started with Spectrum for Administrators"**, Cabletron Systems., Rochester NH - USA 1998.
8. **CABLETRON Systems., "Getting Started with Spectrum for Operators"**, Cabletron Systems., Rochester NH - USA 1998.
9. **CABLETRON Systems., "SPECTRUM Concepts Guide"**, Cabletron Systems., Rochester NH - USA 1996.
10. **CABLETRON Systems., "SPECTRUM Knowledge Base Guide"**, Cabletron Systems., Rochester NH - USA 1996.
11. **CABLETRON Systems., "Database Management"**, Cabletron Systems., Rochester NH - USA 1998.

12. **CABLETRON Systems.,** "**Distributed SpectroSERVER**", Cabletron Systems., Rochester NH - USA 1998.

13. **CABLETRON Systems.,** "**SPECTRUM Icons**", Cabletron Systems., Rochester NH - USA 1998.

14. **CABLETRON Systems.,** "**SPECTRUM Views**", Cabletron Systems., Rochester NH - USA 1998.

15. **CABLETRON Systems.,** "**How to Manage Your Network with SPECTRUM**", Cabletron Systems., Rochester NH - USA 1996.

16. **CABLETRON Systems.,** "**AutoDiscovery User's Guide**", Cabletron Systems., Rochester NH - USA 1998.

17. **CABLETRON Systems.,** "**Performance**", Cabletron Systems., Rochester NH - USA 1998.

18. **CABLETRON Systems.,** "**Report Generator User's Guide Version 5.0rev1**", Cabletron Systems., Rochester NH - USA 1998.

19. **CABLETRON Systems.,** "**Performance**", Cabletron Systems., Rochester NH - USA 1998.

20. **CABLETRON Systems.,** "**Security and User Maintenance**", Cabletron Systems., Rochester NH - USA 1998.

21. **MICROSOFT Corporation.,** "**Systems Management Server Version 2.0 – Reviewer's Guide**", Microsoft Corporation, Redmond – USA 1998.

CAPITULO V

APLICACION PROTOTIPO

Software de Características Resumidas para la Gestión de Redes "Net Manager"

Introducción

En este capítulo se realizan las fases de análisis, diseño de los módulos de Gestión de la Seguridad, Gestión de la Configuración, Gestión de Fallos, Gestión del Rendimiento y Gestión Remota del Sistema Prototipo de Gestión de Red "Net Manager". Las fase de implementación se realizó en el lenguaje Visual Basic 6.0 y se detalla en el **Anexo C**.

Este Software Prototipo se enmarca dentro de los Sistemas de Gestión Centralizada y hace uso del Protocolo Simple de Gestión de Red (**SNMP**, *Simple Network Management Protocol*) y del Protocolo de Control de Mensajes de Internet (**ICMP**, *Internet Control Message Protocol*).

5.1 Módulo de Gestión de la Seguridad (MGS)

La seguridad es un aspecto importante dentro de la Gestión de Red ya que le permite al encargado de la gestión realizar un control de acceso a las herramientas del sistema.

5.1.1 Estudio de Factibilidad

Realizar una aplicación que permita controlar el acceso de usuarios hacia el sistema es totalmente factible mediante la autenticación por clave, permitiendo que usuarios registrados en el sistema puedan tener acceso a las herramientas y utilidades de gestión.

5.1.2 Análisis y Diseño

Para el Módulo de Gestión de la Seguridad será necesario la utilización de cuatro procesos que ayudarán a facilitar el proceso de autenticación de usuarios para el ingreso al SGR. Estos procesos se explican a continuación:

- **Proceso "Obtener Información":** permite obtener información del usuario que intenta ingresar al sistema (ver **Fig. 5.1**).

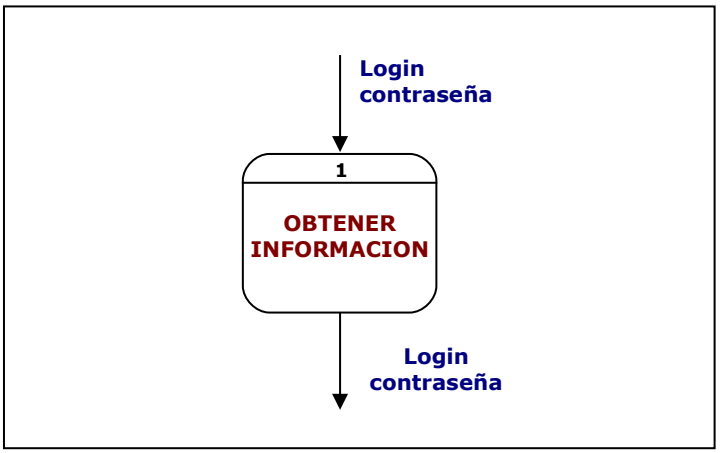


Fig. 5.1 MGS - Proceso "Obtener Información"

- **Proceso "Verificar Usuario":** permite determinar si el usuario que ingreso su login y password es un usuario registrado del sistema. Si es así devuelve el código asignado para él (Administrador u operador) (ver **Fig. 5.2**).

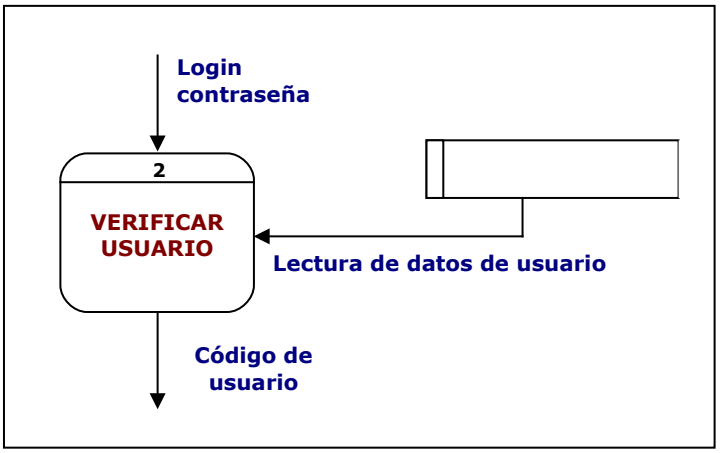


Fig. 5.2 MGS - Proceso "Verificar Usuario"

- **Proceso "Verificar Contraseña":** permite determinar si el usuario registrado ingreso su password correctamente para ingresar al sistema. Si es así devuelve el código asignado para él (Administrador u operador) y se le permite el acceso al SGR, caso contrario incrementa el número de intentos fallidos. Si el número de intentos fallidos es mayor que tres retorna al proceso "Obtener Información" (ver **Fig. 5.3**).

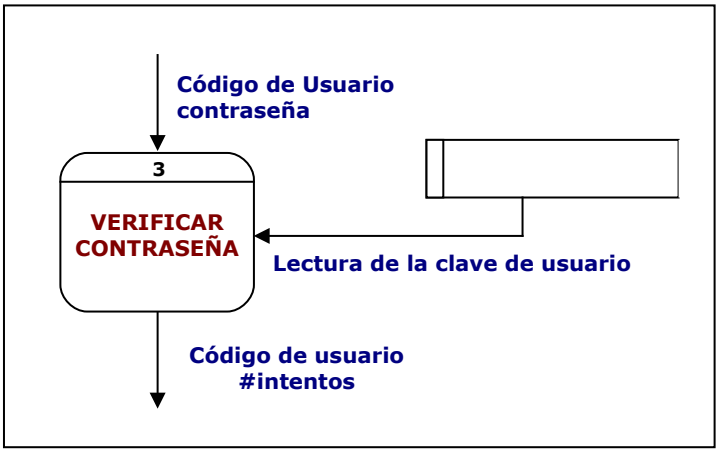


Fig. 5.3 MGS - Proceso "Verificar Contraseña"

- **Proceso "Habilitar/Deshabilitar Seguridad":** permite conceder o denegar permiso de ejecución de las diferentes opciones del Menú del Sistema dependiendo del código del usuario que ingresó al sistema. Si el usuario tiene código de Administrador actualiza los permisos para las opciones del menú y si el usuario tiene código de Operador simplemente se habilitan las opciones de Menú por defecto (ver **Fig. 5.4**).

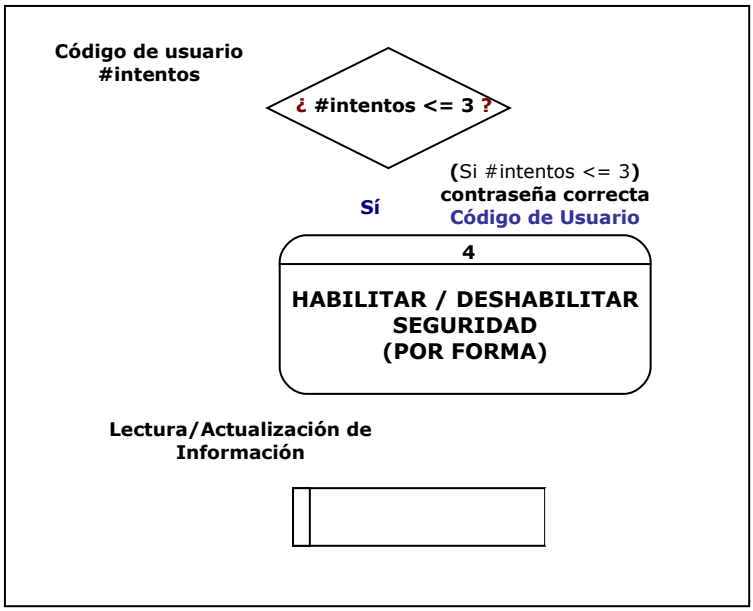


Fig. 5.4 MGS - Proceso "Habilitar/Deshabilitar Seguridad"

A continuación se detallan los Diagramas de Flujo de Datos de Nivel 0, Nivel 1 y Nivel 2 y el Diagrama de Flujo de Objetos para el Módulo de Gestión de la Seguridad.

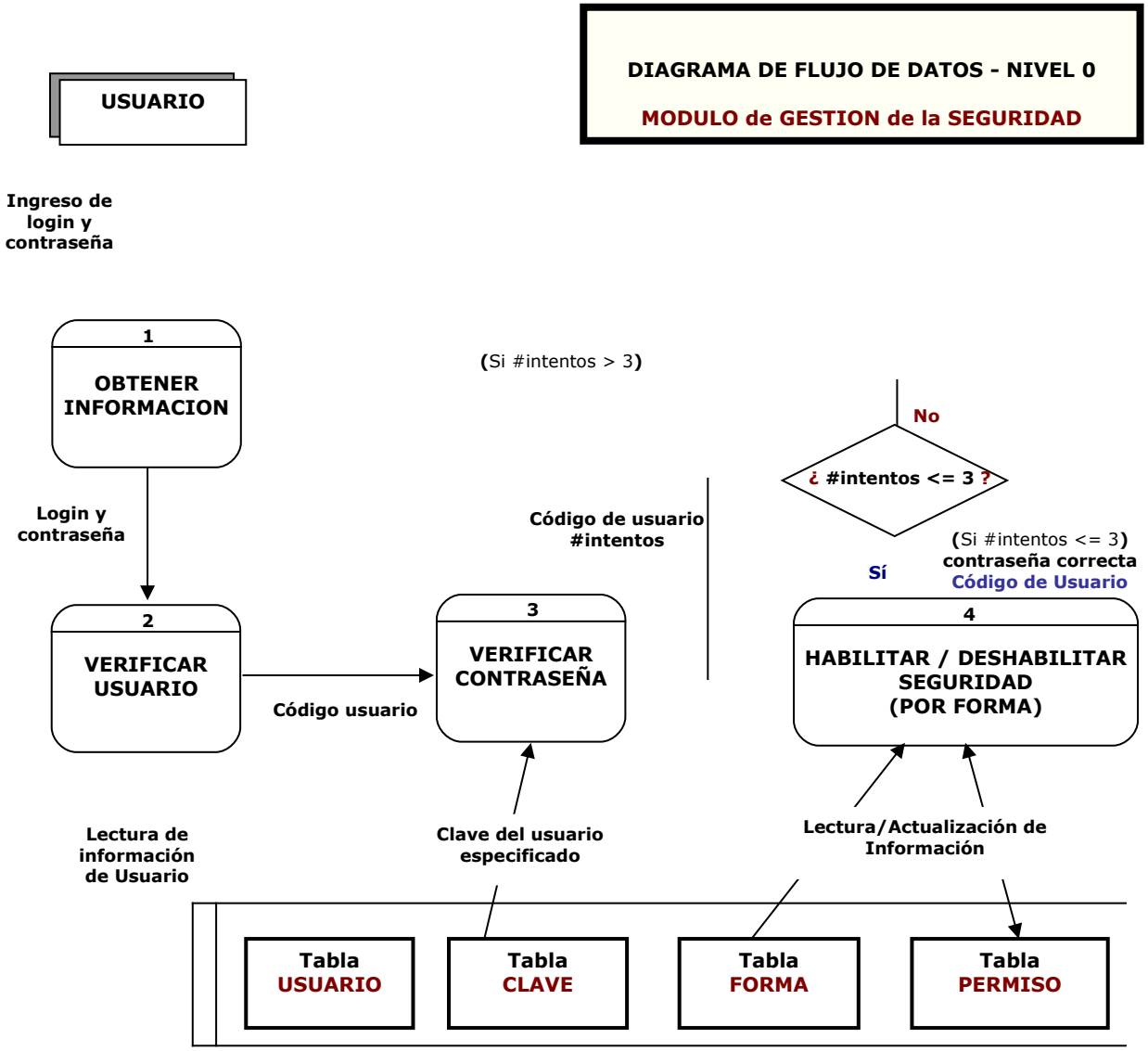
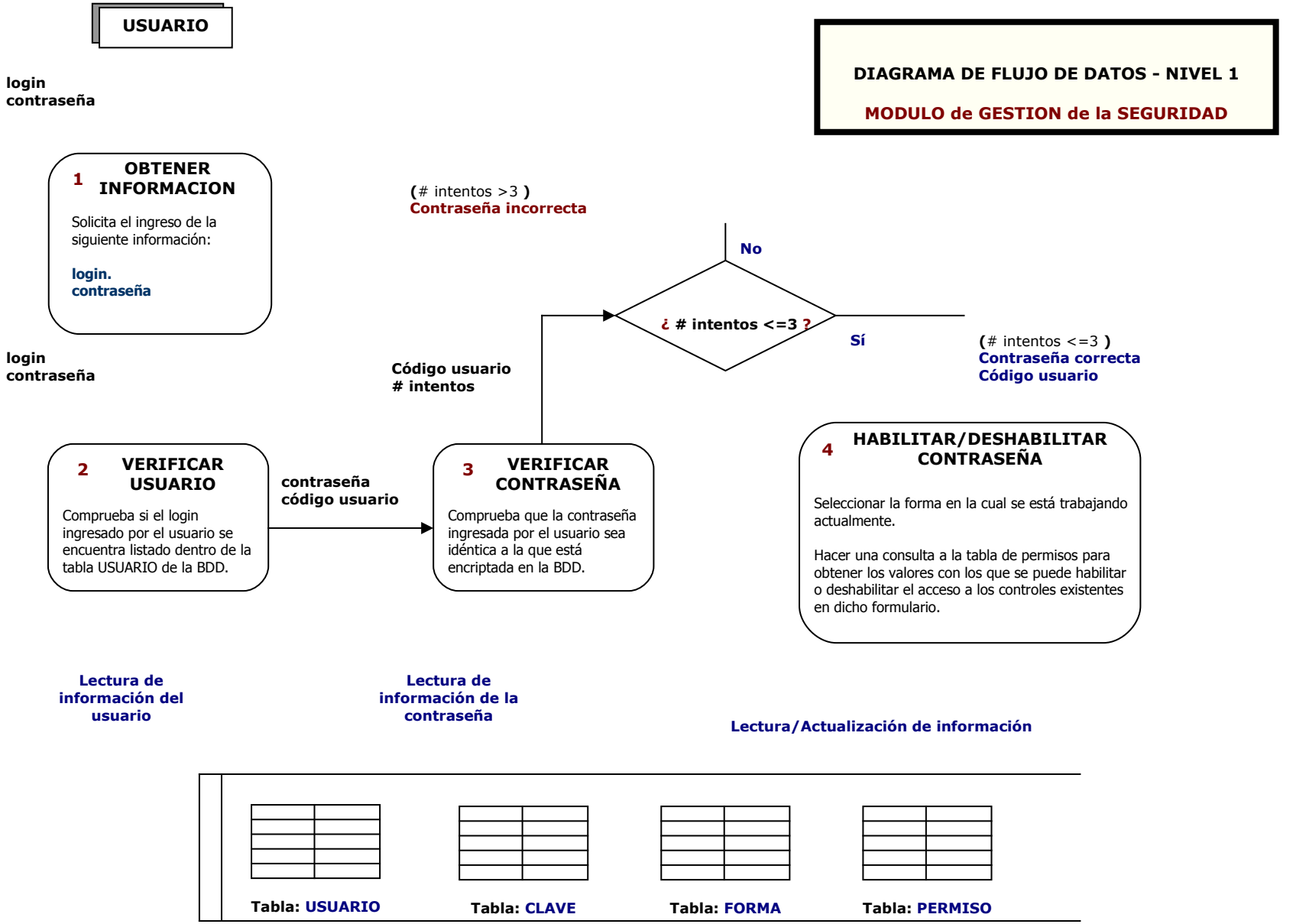
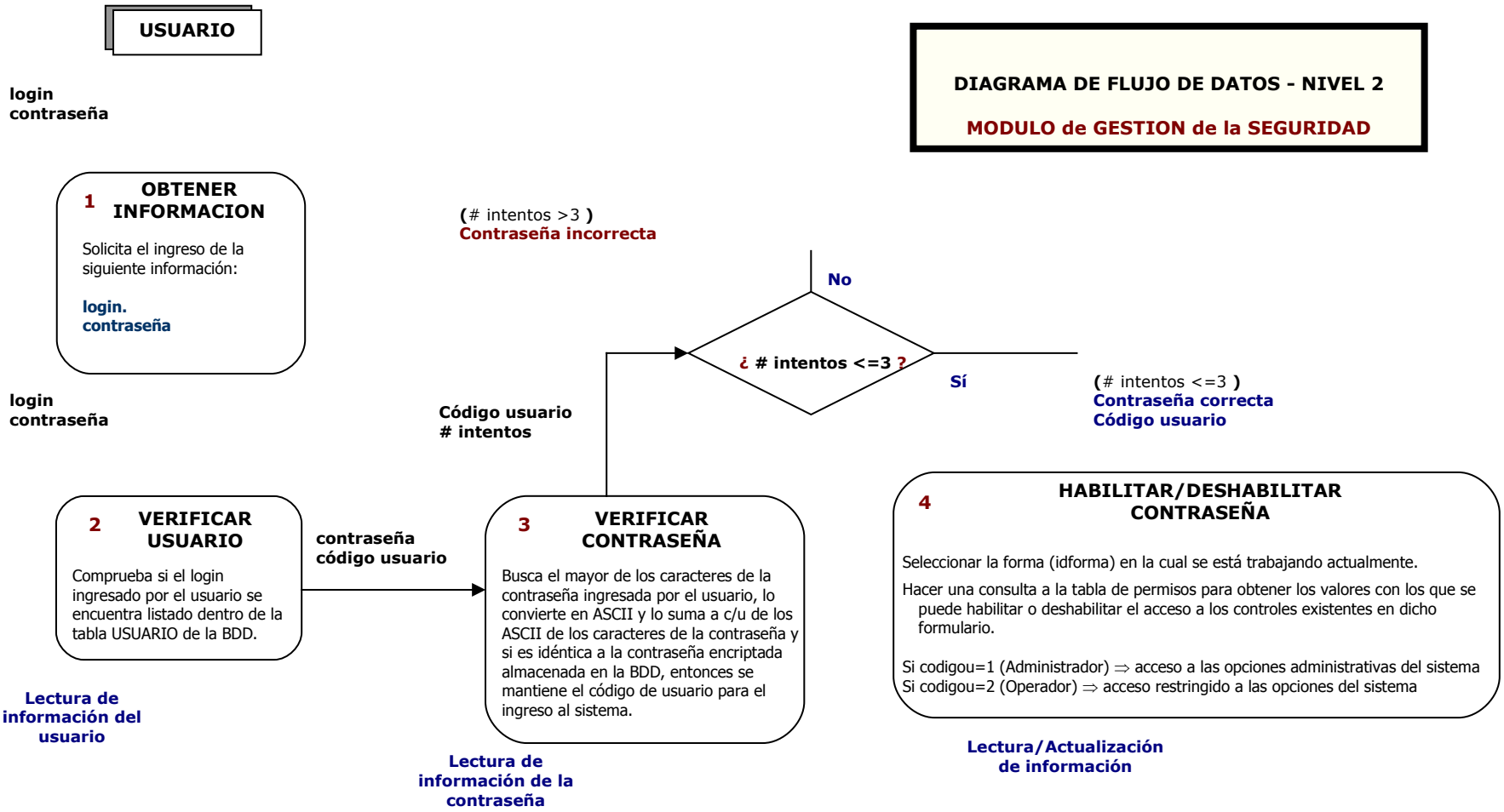


DIAGRAMA DE FLUJO DE DATOS - NIVEL 0
MODULO de GESTION de la SEGURIDAD
USUARIO
Ingreso de login y contraseña
1
OBTENER INFORMACION
Login y contraseña
2
VERIFICAR USUARIO
Código usuario
3
VERIFICAR CONTRASEÑA
(Si #intentos > 3)
Código de usuario
#intentos
No
¿ #intentos <= 3 ?
Sí
(Si #intentos <= 3)
contraseña correcta
Código de Usuario
4
HABILITAR / DESHABILITAR SEGURIDAD (POR FORMA)
Lectura de información de Usuario
Clave del usuario especificado
Lectura/Actualización de Información
Tabla USUARIO
Tabla CLAVE
Tabla FORMA
Tabla PERMISO


USUARIO
DIAGRAMA DE FLUJO DE DATOS - NIVEL 1
MODULO de GESTION de la SEGURIDAD
login
contraseña
1 OBTENER INFORMACION
Solicita el ingreso de la siguiente información:
login.
contraseña
(# intentos >3)
Contraseña incorrecta
No
¿ # intentos <=3 ?
Sí
(# intentos <=3)
Contraseña correcta
Código usuario
login
contraseña
Código usuario
intentos
2 VERIFICAR USUARIO
Comprueba si el login ingresado por el usuario se encuentra listado dentro de la tabla USUARIO de la BDD.
contraseña
código usuario
3 VERIFICAR CONTRASEÑA
Comprueba que la contraseña ingresada por el usuario sea idéntica a la que está encriptada en la BDD.
4 HABILITAR/DESHABILITAR CONTRASEÑA
Seleccionar la forma en la cual se está trabajando actualmente.
Hacer una consulta a la tabla de permisos para obtener los valores con los que se puede habilitar o deshabilitar el acceso a los controles existentes en dicho formulario.
Lectura de información del usuario
Lectura de información de la contraseña
Lectura/Actualización de información
Tabla: USUARIO
Tabla: CLAVE
Tabla: FORMA
Tabla: PERMISO



NombreDescripción1codigo# de usuario**2**descripcionCaracterística del usuario**3**loginNombre de usuario del SGR

Tabla: USUARIO

NombreDescripción1codigo# de usuario**2**claveContraseña encriptada**3**numero_diasCuándo caduca la contraseña**4**fecha_creadaFecha de creación del usuario y contraseña

Tabla: CLAVE

NombreDescripción1idformaId de cada formulario del proyecto**2**nombreDescripción del formulario

Tabla: FORMA

NombreDescripción1codigouCódigo de usuario**2**IdformauId. de la forma**3**objetoNombre del objeto contenido en la forma**4**nombreDescripción del objeto**5**permiso# que indica accesibilidad (1) o no (0) hacia el objeto

Tabla: PERMISO

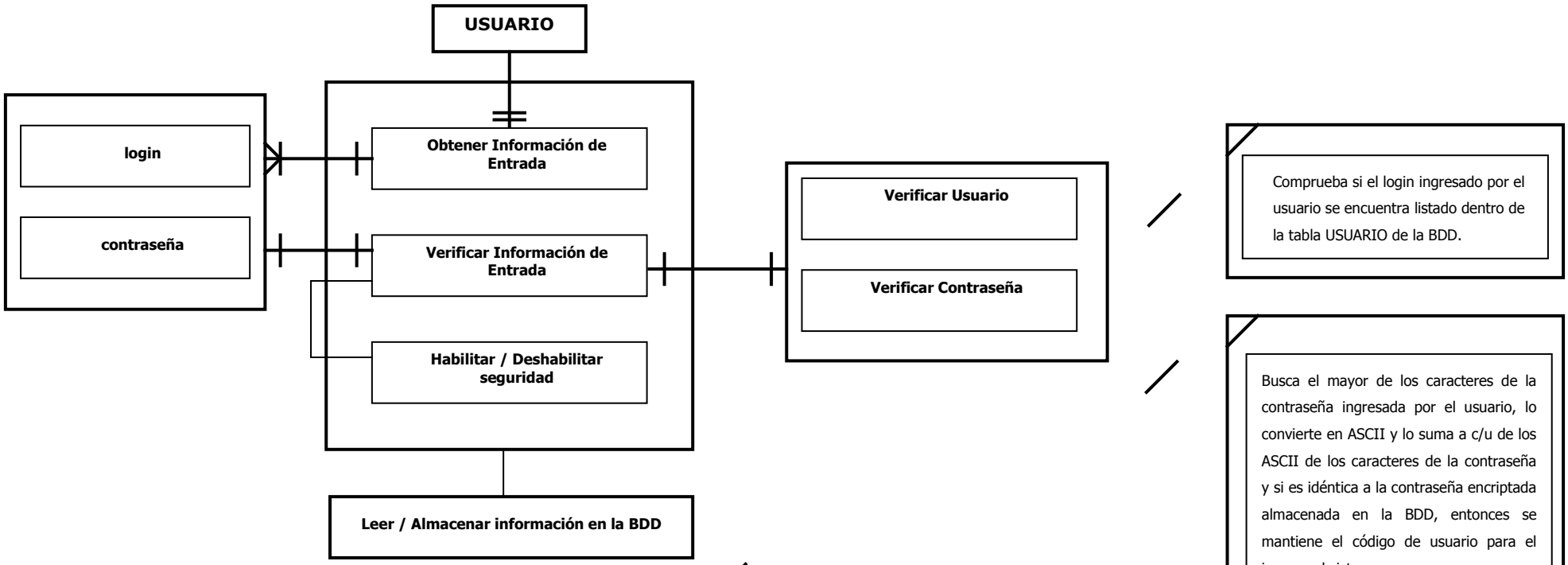


DIAGRAMA DE FLUJO DE OBJETOS
MODULO DE GESTION DE LA SEGURIDAD

5.2 Módulo de Gestión de la Configuración (MGC)

La Gestión de la Configuración implica un conjunto de procedimientos que constituyen la base de un SGR. Estos procedimientos deben permitir: el descubrimiento de los nodos que conforman la red, el agrupamiento dinámico de dispositivos descubiertos, la búsqueda de equipos deacuerdo a su descripción, consulta y despliegue de variables MIB, etc.

5.2.1 Estudio de Factibilidad

Realizar una aplicación que relacione los procedimientos de Gestión de la Configuración anteriormente descritos es factible realizando un diseño de Base de Datos que permita almacenar la información referente a los rangos de descubrimiento, nodos descubiertos, características de los nodos e información MIB. El proceso de descubrimiento de equipos puede realizarse utilizando ICMP – Ping para un rango de direcciones IP, mientras que la Consulta y navegación de variables MIB puede realizarse empleando SNMP, y su primitiva SNMP-Get conociendo el OID de la variable MIB a consultar.

5.2.2 Análisis y Diseño

Para el Módulo de Gestión de la Configuración será necesario la utilización de cuatro procesos que permitan realizar las tareas descritas anteriormente. Estos procesos se indican a continuación:

- **Proceso "Obtener Información":** permite obtener la dirección IP inicial y final para el descubrimiento, además de la cadena de comunidad de acceso SNMP (ver **Fig. 5.5**).

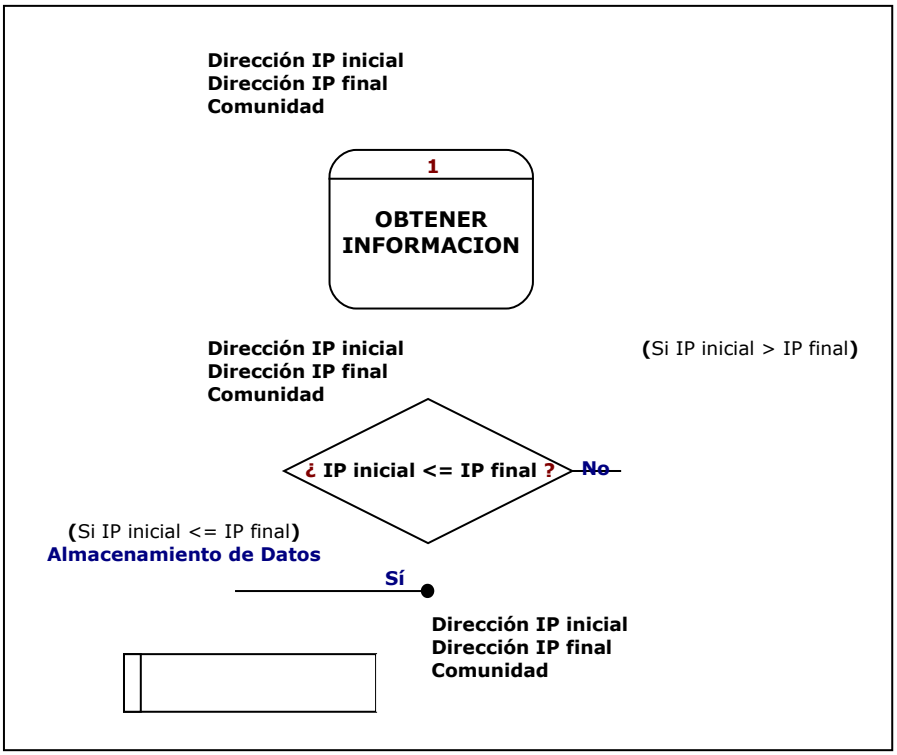


Fig. 5.5 MGC - Proceso "Obtener Información"

- **Proceso "Actualizar Rango":** permite obtener la dirección IP inicial y final para el descubrimiento, además de la cadena de comunidad de acceso SNMP (ver **Fig. 5.6**).

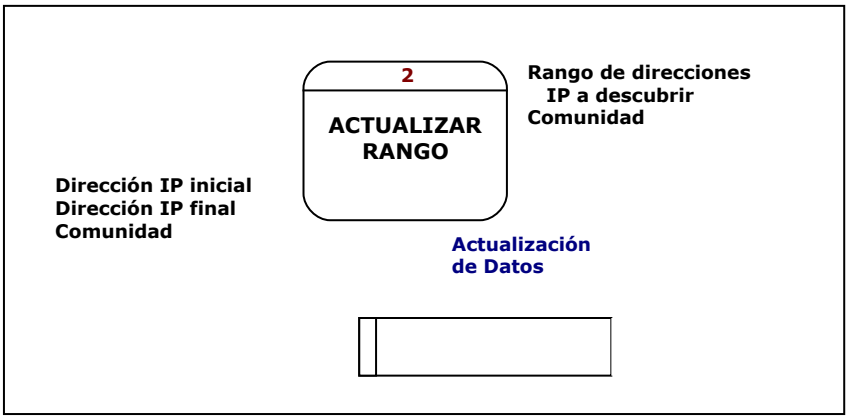


Fig. 5.6 MGC - Proceso "Actualizar Rango"

- **Proceso "Descubrir Nodos":** permite descubrir los nodos que se encuentran dentro de un rango de direcciones IP utilizando sondeos ICMP y SNMP (ver **Fig. 5.7**).

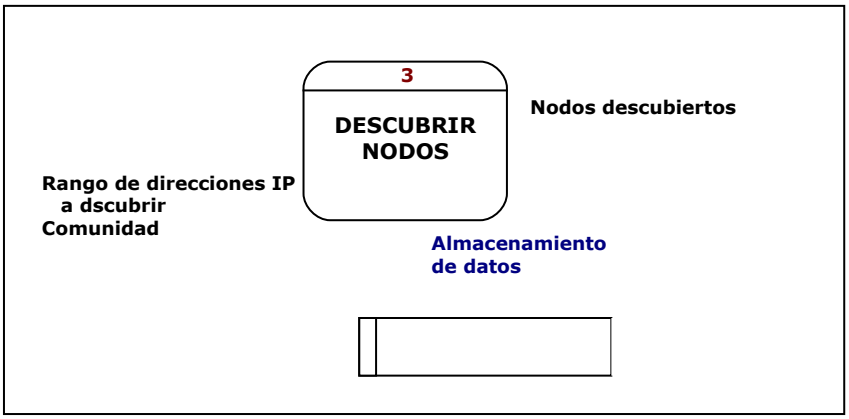


Fig. 5.7 MGC - Proceso "Descubrir Nodos"

- **Proceso "Manejar Nodos y Grupos":** permite realizar funciones de edición para grupos (crear, borrar, renombrar, cambiar imagen) y de edición y consulta para nodos (agrupar, ver propiedades, subir de nivel, borrar, renombrar, cambiar imagen) (ver **Fig. 5.8**).

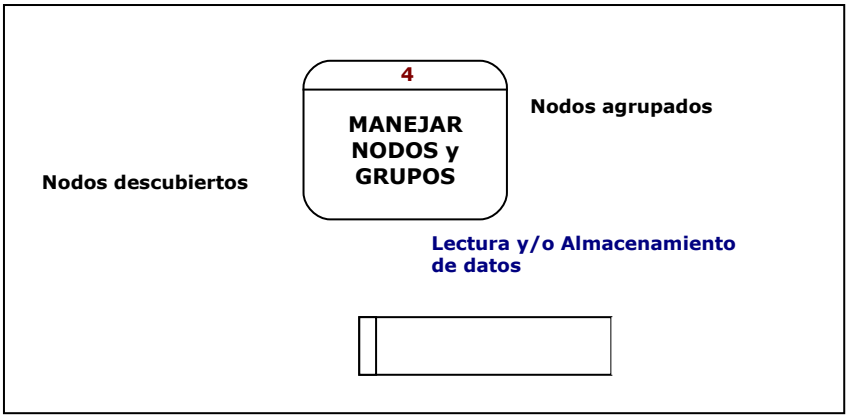


Fig. 5.8 MGC - Proceso "Manejar Nodos y Grupos"

A continuación se detallan los Diagramas de Flujo de Datos de Nivel 0, Nivel 1 y Nivel 2 y el Diagrama de Flujo de Objetos para el Módulo de Gestión de Fallos.

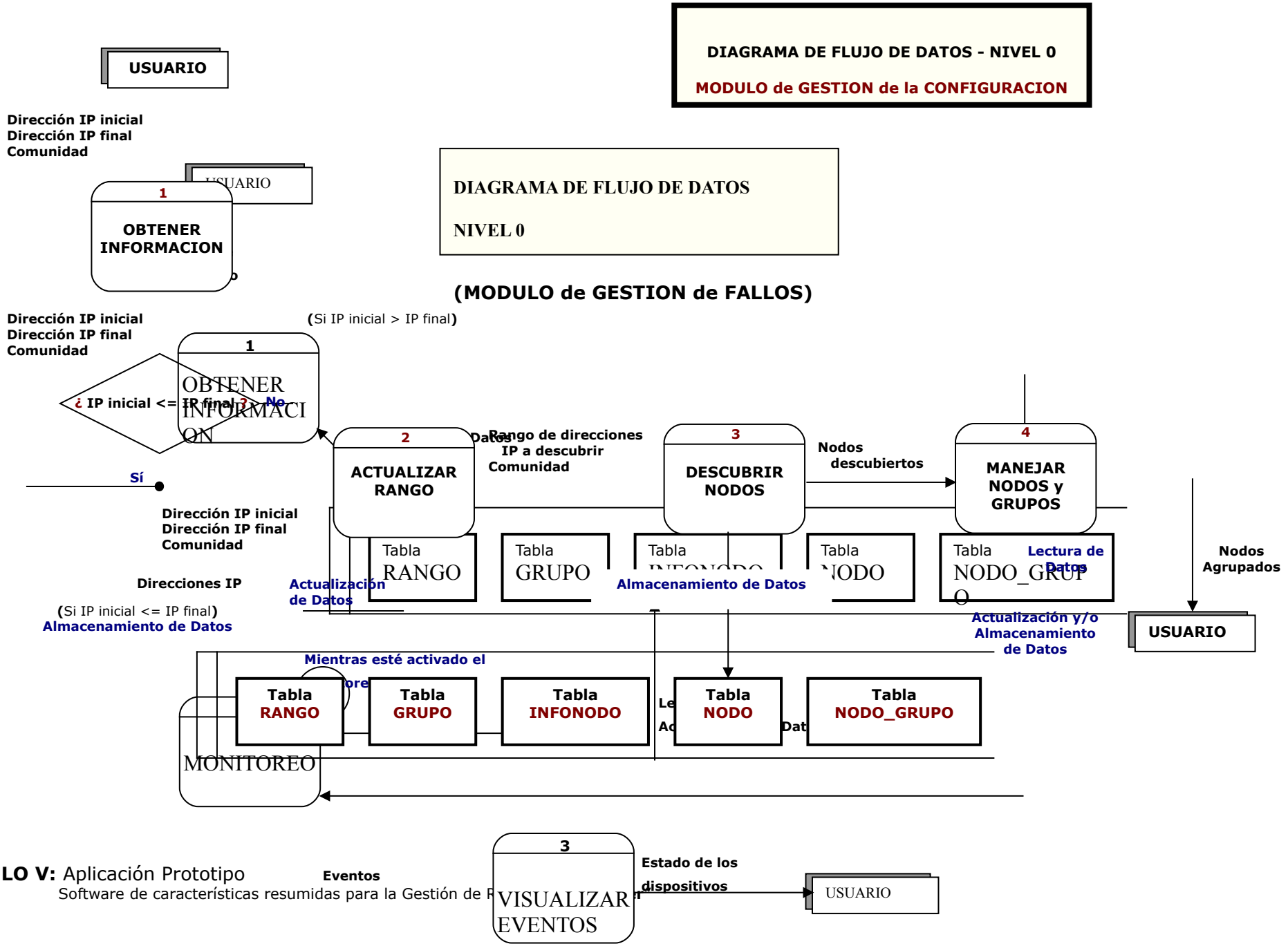


DIAGRAMA DE FLUJO DE DATOS - NIVEL 0
MODULO de GESTION de la CONFIGURACION
USUARIO
Dirección IP inicial
Dirección IP final
Comunidad
1
OBTENER INFORMACION
DIAGRAMA DE FLUJO DE DATOS
NIVEL 0
(MODULO de GESTION de FALLOS)
Dirección IP inicial
Dirección IP final
Comunidad
(Si IP inicial > IP final)
1
OBTENER INFORMACION
¿ IP inicial <= IP final ?
No
Sí
2
ACTUALIZAR RANGO
Datos
Rango de direcciones IP a descubrir
Comunidad
3
DESCUBRIR NODOS
Nodos descubiertos
4
MANEJAR NODOS y GRUPOS
Dirección IP inicial
Dirección IP final
Comunidad
Direcciones IP
(Si IP inicial <= IP final)
Almacenamiento de Datos
Tabla RANGO
Tabla GRUPO
Tabla INFONODO
Tabla NODO
Tabla NODO_GRUPO
Actualización de Datos
Almacenamiento de Datos
Lectura de Datos
Nodos Agrupados
Actualización y/o Almacenamiento de Datos
USUARIO
Mientras esté activado el
MONITOREO
Tabla RANGO
Tabla GRUPO
Tabla INFONODO
Tabla NODO
Tabla NODO_GRUPO
Eventos
3
VISUALIZAR EVENTOS
Estado de los dispositivos
USUARIO

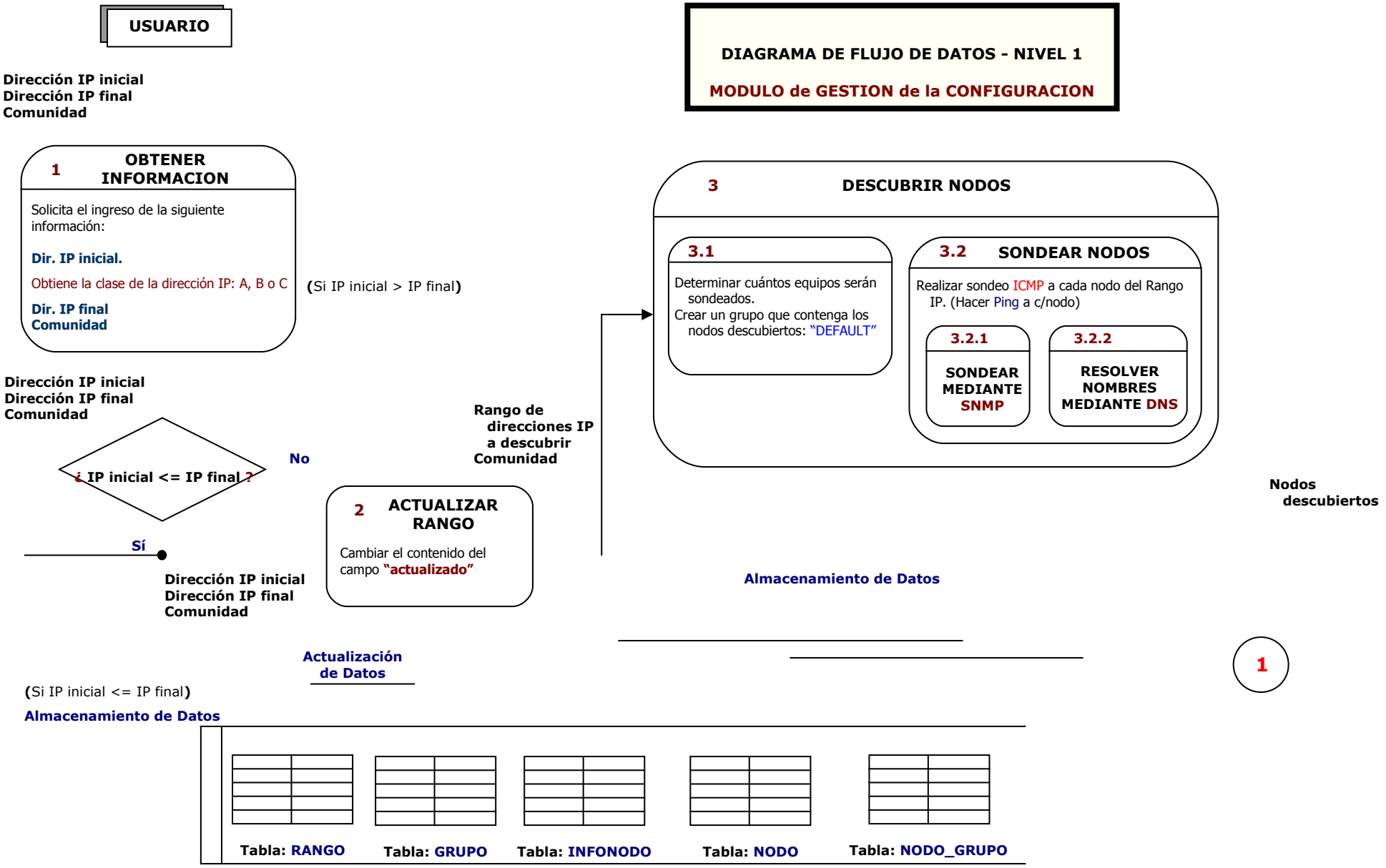
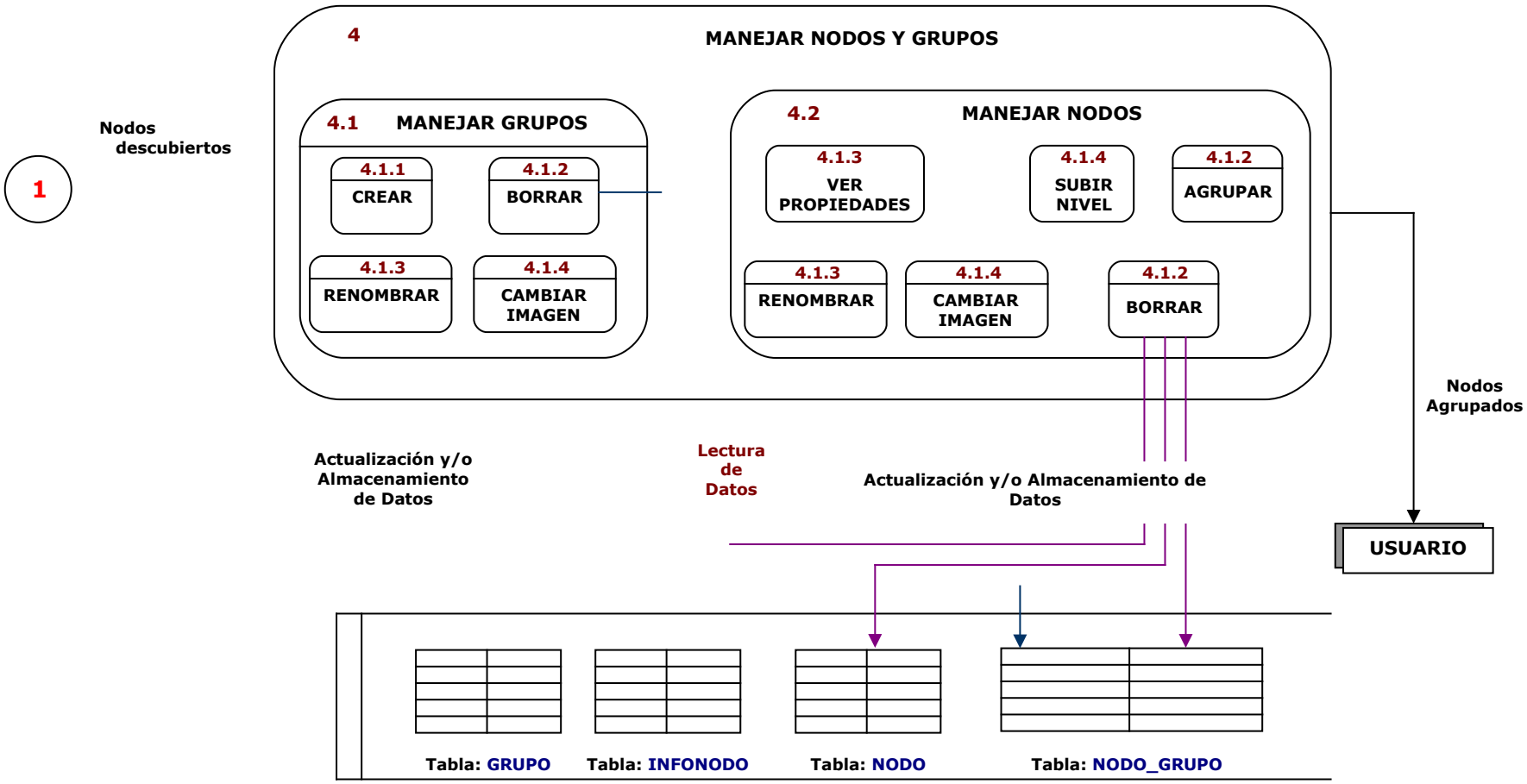

USUARIO
DIAGRAMA DE FLUJO DE DATOS - NIVEL 1
MODULO de GESTION de la CONFIGURACION
Dirección IP inicial
Dirección IP final
Comunidad
1 OBTENER INFORMACION
Solicita el ingreso de la siguiente información:
Dir. IP inicial.
Obtiene la clase de la dirección IP: A, B o C
Dir. IP final
Comunidad
(Si IP inicial > IP final)
3 DESCUBRIR NODOS
3.1
Determinar cuántos equipos serán sondeados.
Crear un grupo que contenga los nodos descubiertos: "DEFAULT"
3.2 SONDEAR NODOS
Realizar sondeo ICMP a cada nodo del Rango IP. (Hacer Ping a c/nodo)
3.2.1 SONDEAR MEDIANTE SNMP
3.2.2 RESOLVER NOMBRES MEDIANTE DNS
Dirección IP inicial
Dirección IP final
Comunidad
¿ IP inicial <= IP final ?
No
Rango de direcciones IP a descubrir
Comunidad
Nodos descubiertos
Sí
2 ACTUALIZAR RANGO
Cambiar el contenido del campo "actualizado"
Dirección IP inicial
Dirección IP final
Comunidad
Almacenamiento de Datos
Actualización de Datos
1
(Si IP inicial <= IP final)
Almacenamiento de Datos
Tabla: RANGO
Tabla: GRUPO
Tabla: INFONODO
Tabla: NODO
Tabla: NODO_GRUPO

DIAGRAMA DE FLUJO DE DATOS - NIVEL 1

MODULO de GESTION de la CONFIGURACION
(Continuación)



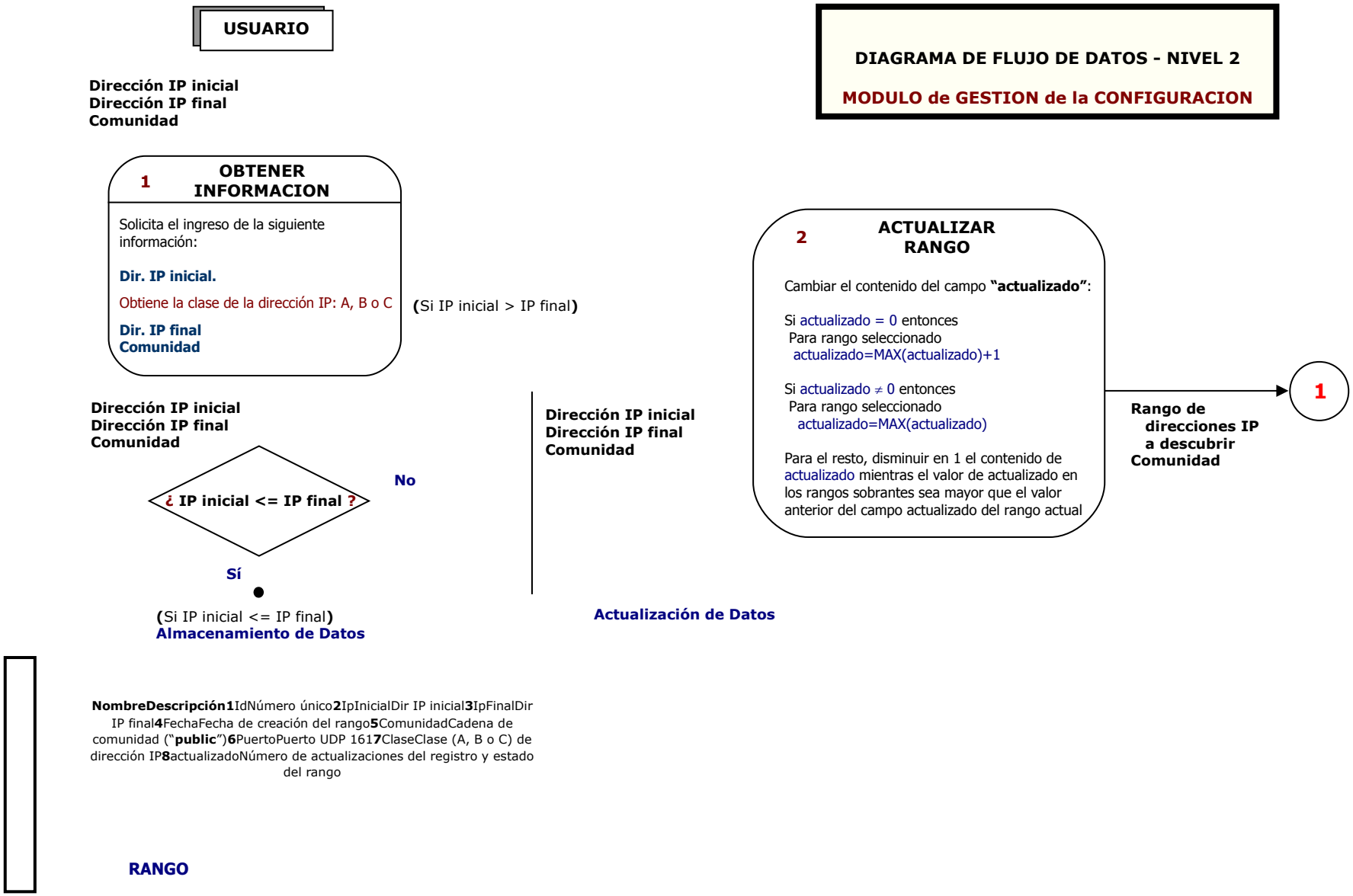
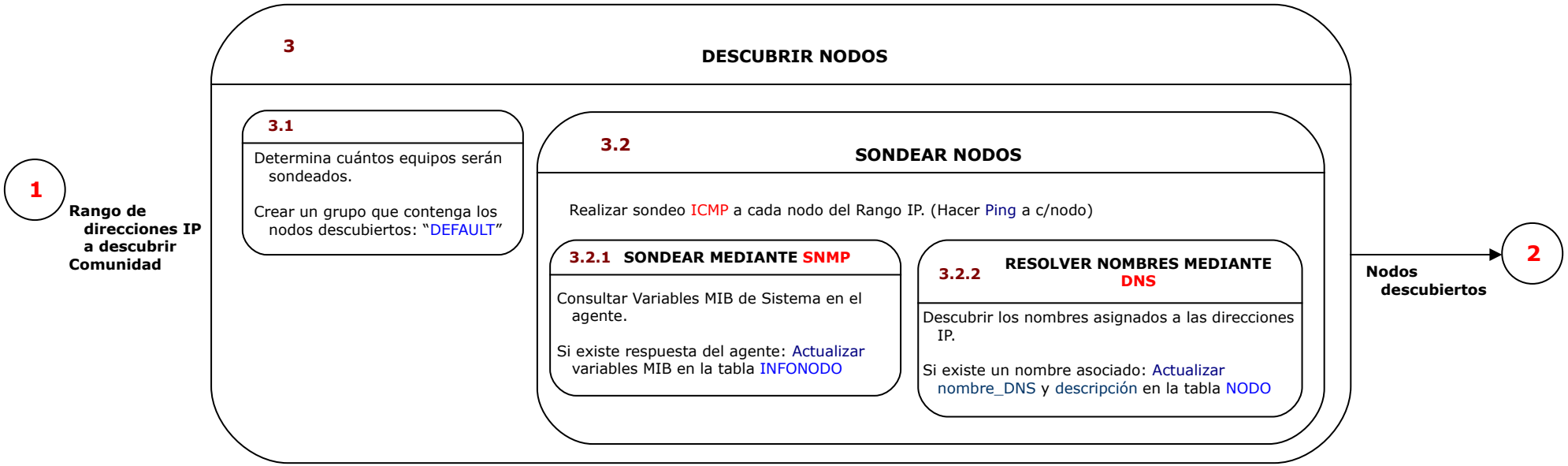

USUARIO
DIAGRAMA DE FLUJO DE DATOS - NIVEL 2
MODULO de GESTION de la CONFIGURACION
Dirección IP inicial
Dirección IP final
Comunidad
1
OBTENER INFORMACION
Solicita el ingreso de la siguiente información:
Dir. IP inicial.
Obtiene la clase de la dirección IP: A, B o C
Dir. IP final
Comunidad
(Si IP inicial > IP final)
2
ACTUALIZAR RANGO
Cambiar el contenido del campo "actualizado":
Si actualizado = 0 entonces
Para rango seleccionado
actualizado=MAX(actualizado)+1
Si actualizado ≠ 0 entonces
Para rango seleccionado
actualizado=MAX(actualizado)
Para el resto, disminuir en 1 el contenido de actualizado mientras el valor de actualizado en los rangos sobrantes sea mayor que el valor anterior del campo actualizado del rango actual
Rango de direcciones IP a descubrir
Comunidad
1
Dirección IP inicial
Dirección IP final
Comunidad
¿ IP inicial <= IP final ?
No
Sí
(Si IP inicial <= IP final)
Almacenamiento de Datos
Dirección IP inicial
Dirección IP final
Comunidad
Actualización de Datos
NombreDescripción1IdNúmero único2IpInicialDir IP inicial3IpFinalDir IP final4FechaFecha de creación del rango5ComunidadCadena de comunidad ("public")6PuertoPuerto UDP 1617ClaseClase (A, B o C) de dirección IP8actualizadoNúmero de actualizaciones del registro y estado del rango
RANGO

DIAGRAMA DE FLUJO DE DATOS - NIVEL 2

MODULO de GESTION de la CONFIGURACION
(Continuación)



Almacenamiento de Datos

NombreDescripción1 IdGrupoId. Único de grupo**2**IdRangoId de rango**3**IdSubGrupoId de sub grupo**4**NombreNombre del grupo**5**ImagenNúmero de imagen**6**Estado_ActualEstado: 1 Up, 0 Down

Tabla: GRUPO

Almacenamiento de Datos

NombreDescripción1 DirecciónIPDirección IP**2**ComunidadCadena de comunidad ("**public**")**3**ObjectIDVariable MIB SysOID**4**DescripciónVariable MIB SysDescripcion**5**ContactoVariable MIB SysContact**6**NombreVariable MIB SysName**7**LocalizaciónVariable MIB SysLocation**8**ServiciosVariable MIB SysServices**9**TiempoVariable MIB SysUpTime

Tabla: INFONODO

Almacenamiento de Datos

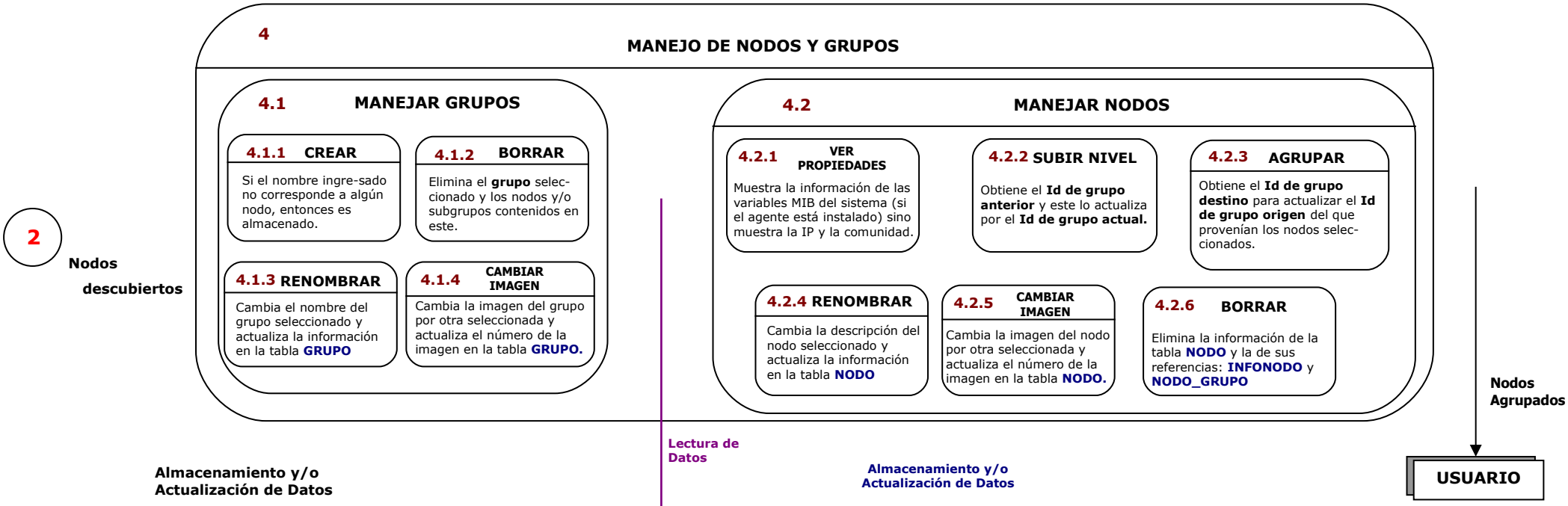
NombreDescripción1IPDir. IP**2**Nombre_DNSN. DNS**3**DescripciónDescripción**5**Imagen# de imagen**6**Estado_ActualEstado: 1 Up, 0 Down.º

Tabla: NODO

NombreDescripción1NG_IPDirección IP**2**NG_GrupoId de Grupo**3**IdrangoId de Rango

Tabla: NODO_GRUPO

DIAGRAMA DE FLUJO DE DATOS - NIVEL 2
MODULO de GESTION de la CONFIGURACION
(Continuación)



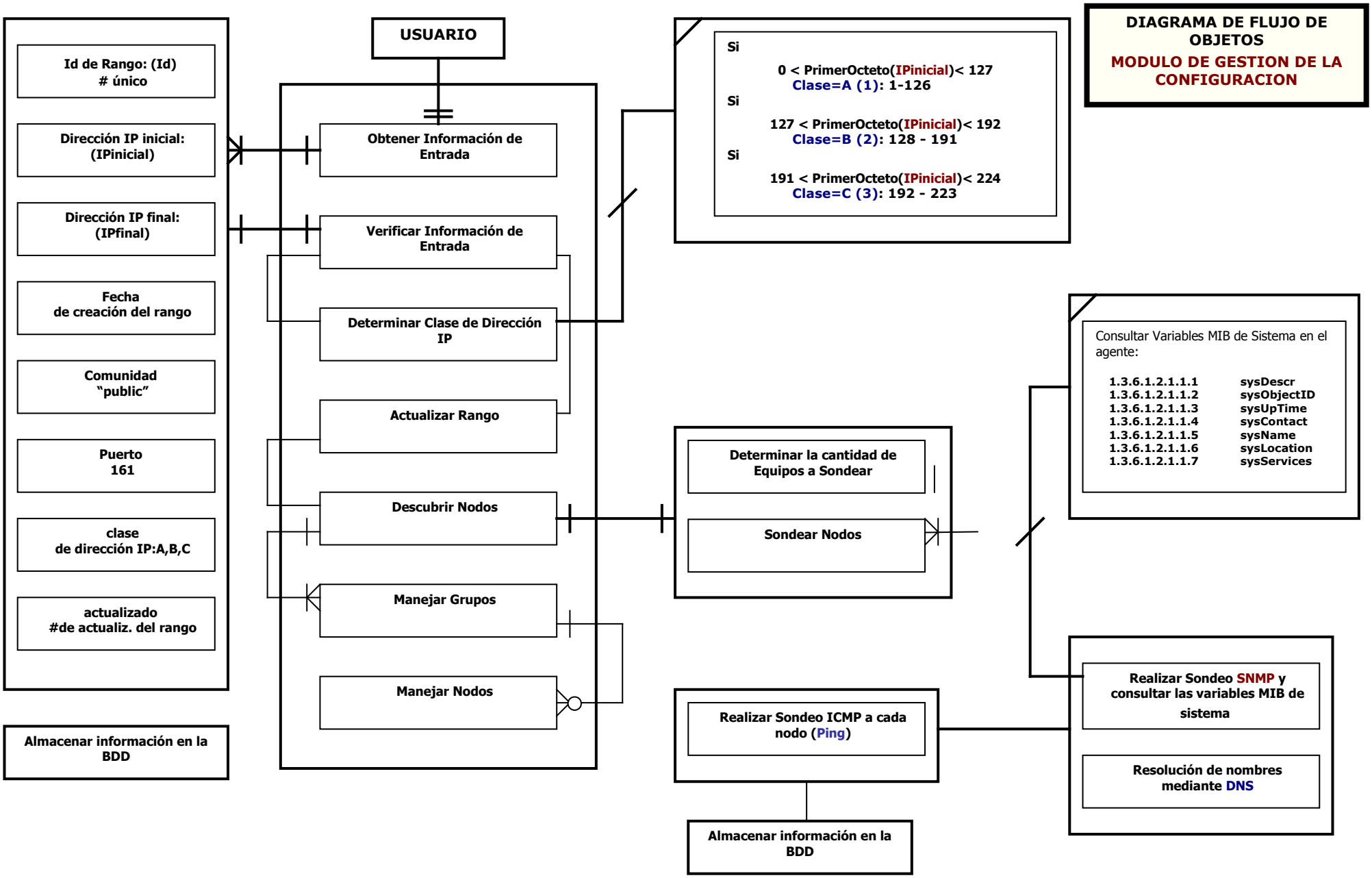


DIAGRAMA DE FLUJO DE OBJETOS
MODULO DE GESTION DE LA CONFIGURACION
USUARIO
Id de Rango: (Id)
único
Dirección IP inicial:
(IPinicial)
Dirección IP final:
(IPfinal)
Fecha
de creación del rango
Comunidad
"public"
Puerto
161
clase
de dirección IP:A,B,C
actualizado
#de actualiz. del rango
Almacenar información en la BDD
Obtener Información de Entrada
Verificar Información de Entrada
Determinar Clase de Dirección IP
Actualizar Rango
Descubrir Nodos
Manejar Grupos
Manejar Nodos
Si
0 < PrimerOcteto(IPinicial)< 127
Clase=A (1): 1-126
Si
127 < PrimerOcteto(IPinicial)< 192
Clase=B (2): 128 - 191
Si
191 < PrimerOcteto(IPinicial)< 224
Clase=C (3): 192 - 223
Determinar la cantidad de Equipos a Sondear
Sondear Nodos
Realizar Sondeo ICMP a cada nodo (Ping)
Almacenar información en la BDD
Consultar Variables MIB de Sistema en el agente:
1.3.6.1.2.1.1.1 sysDescr
1.3.6.1.2.1.1.2 sysObjectID
1.3.6.1.2.1.1.3 sysUpTime
1.3.6.1.2.1.1.4 sysContact
1.3.6.1.2.1.1.5 sysName
1.3.6.1.2.1.1.6 sysLocation
1.3.6.1.2.1.1.7 sysServices
Realizar Sondeo SNMP y consultar las variables MIB de sistema
Resolución de nombres mediante DNS

5.3 Módulo de Gestión de Fallos (MGF)

En una red de computadoras es muy común encontrarse con que no se puede acceder a un determinado recurso de red debido a la "falla" de uno o varios elementos activos, problema que incomoda al usuario y que requiere una pronta detección y solución por parte del personal de soporte técnico.

La detección y el traslado del personal de soporte hacia el lugar del problema conlleva cierto tiempo, de ahí que es necesario tener a la mano una herramienta que esté en capacidad de monitorizar los equipos o elementos activos para determinar cuál no funciona y en qué lugar se encuentra dentro de la organización para realizar una planificación que permita adoptar las medidas necesarias que reduzcan el impacto de la falta de uno de ellos en un período de tiempo no determinado y seguir brindando el servicio al usuario final.

5.3.1 Estudio de Factibilidad

Realizar una herramienta que permita monitorizar los equipos o elementos activos (nodos de red) para determinar cuál no funciona y en qué lugar se localiza dentro de la estructura organizacional de la red es totalmente factible, ya que mediante el uso del Protocolo de Control de Mensajes de Internet (**ICMP**, *Internet Control Message Protocol*), con el envío de una solicitud de respuesta de eco, es posible determinar si uno o más nodos de red se encuentran disponibles (al devolver el eco de la solicitud de respuesta) o no y es posible saber su ubicación consultando la información de las tablas de la base de datos creada en el proceso de descubrimiento.

5.3.2 Análisis y Diseño

Para el Módulo de Gestión de Fallos será necesario la utilización de tres procesos que ayudarán a realizar la monitorización de los nodos de red descubiertos. Estos procesos se explican a continuación:

- **Proceso "Obtener Información":** permite recuperar información de la base de datos referente a las direcciones IP del Rango que se encuentra actualmente seleccionado (ver **Fig. 5.9**).

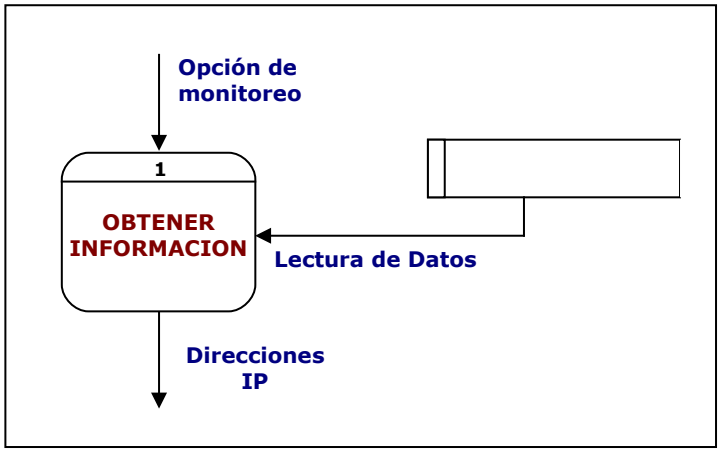


Fig. 5.9 MGF - Proceso "Obtener Información"

- **Proceso "Monitoreo":** permite sondear un listado de direcciones IP y obtener la ubicación del nodo monitoreado, en caso de una falla genera eventos que son visualizados en pantalla y almacenados en archivos de registro cronológico (ver **Fig. 5.10**).

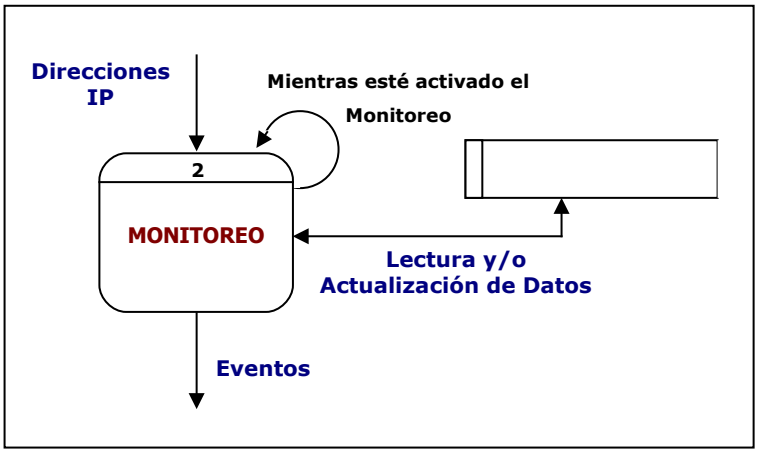


Fig. 5.10 **MGF – Proceso "Monitoreo"**

- **Proceso "Visualizar Eventos":** permite sondear un listado de direcciones IP y obtener la ubicación del nodo monitoreado, en caso de una falla genera eventos que son visualizados en pantalla y almacenados en archivos de registro cronológico (ver **Fig. 5.11**).

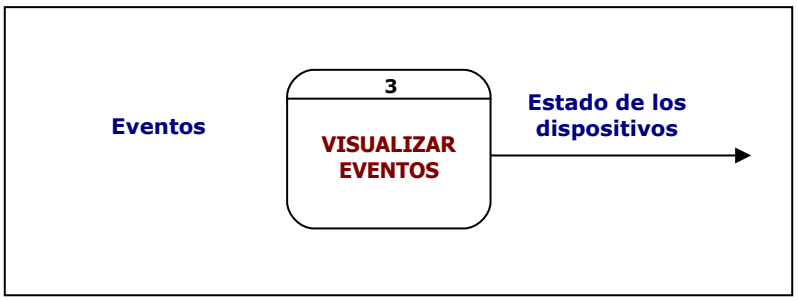
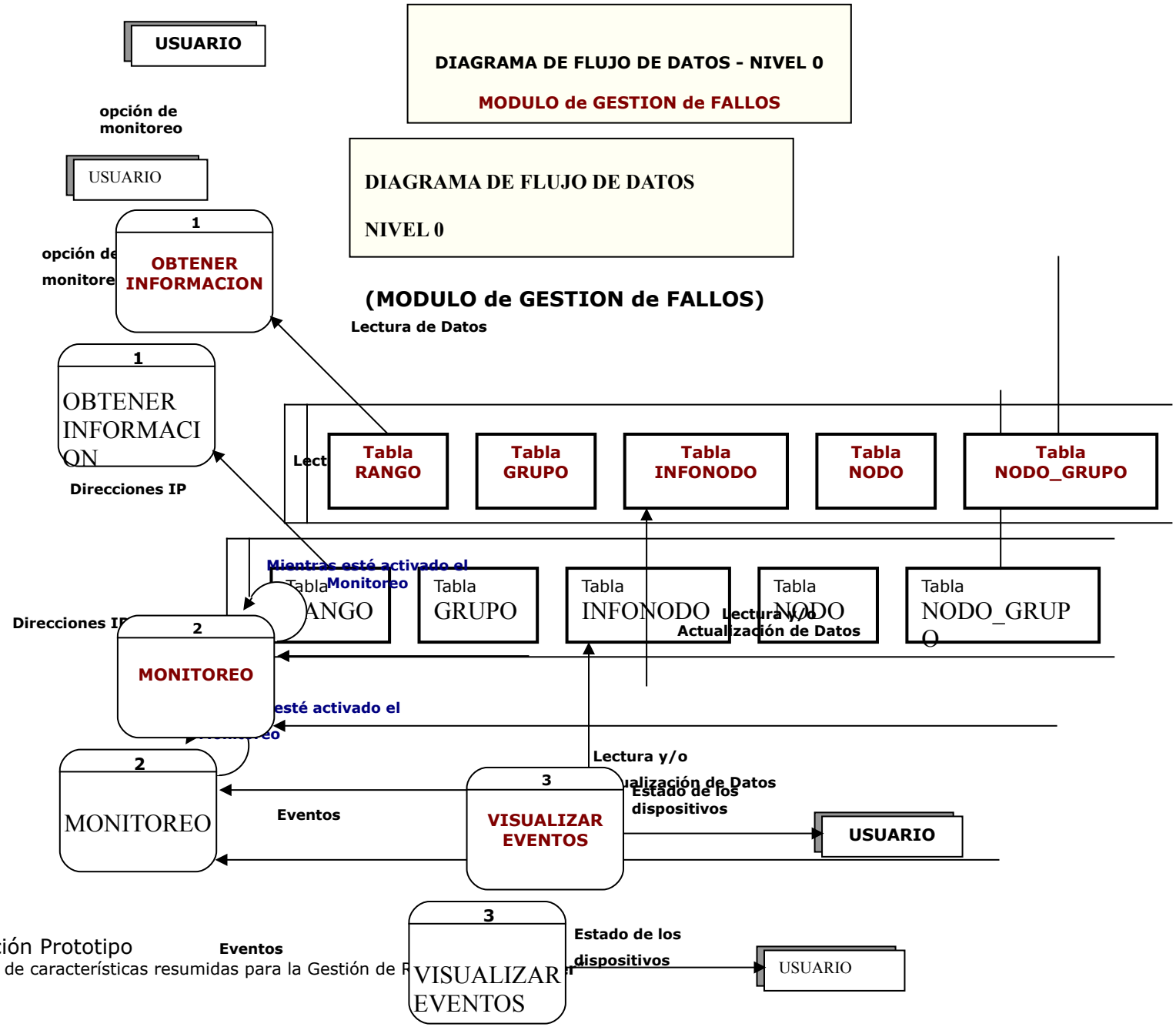


Fig. 5.11 **MGF –Proceso "Visualizar Eventos"**

A continuación se detallan los Diagramas de Flujo de Datos de Nivel 0, Nivel 1 y Nivel 2 y el Diagrama de Flujo de Objetos para el Módulo de Gestión de Fallos.


USUARIO
DIAGRAMA DE FLUJO DE DATOS - NIVEL 0
MODULO de GESTION de FALLOS
opción de monitoreo
USUARIO
DIAGRAMA DE FLUJO DE DATOS
NIVEL 0
1
OBTENER INFORMACION
(MODULO de GESTION de FALLOS)
Lectura de Datos
1
OBTENER INFORMACI ON
Direcciones IP
Tabla RANGO
Tabla GRUPO
Tabla INFONODO
Tabla NODO
Tabla NODO_GRUPO
Mientras esté activado el Monitoreo
Tabla ANGO
Tabla GRUPO
Tabla INFONODO
Tabla NODO
Tabla NODO_GRUP O
Lectura y/o Actualización de Datos
Direcciones IP
2
MONITOREO
esté activado el
2
MONITOREO
Lectura y/o
ualización de Datos
Eventos
3
VISUALIZAR EVENTOS
Estado de los dispositivos
USUARIO
3
VISUALIZAR EVENTOS
Eventos
Estado de los dispositivos
USUARIO

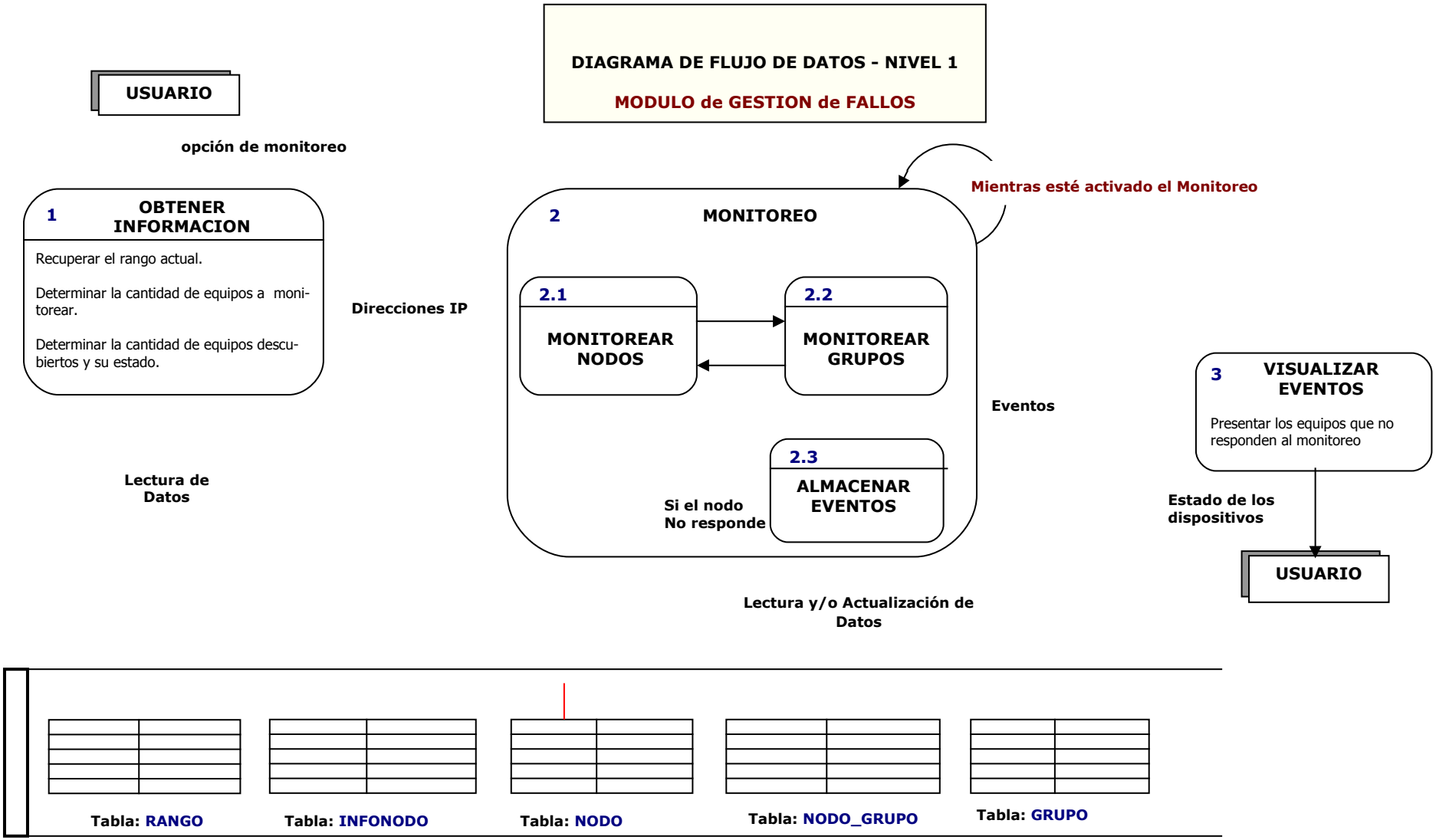


DIAGRAMA DE FLUJO DE DATOS - NIVEL 1
MODULO de GESTION de FALLOS
USUARIO
opción de monitoreo
1
OBTENER INFORMACION
Recuperar el rango actual.
Determinar la cantidad de equipos a monitorear.
Determinar la cantidad de equipos descubiertos y su estado.
Direcciones IP
Lectura de Datos
2
MONITOREO
Mientras esté activado el Monitoreo
2.1
MONITOREAR NODOS
2.2
MONITOREAR GRUPOS
2.3
ALMACENAR EVENTOS
Si el nodo No responde
Eventos
Lectura y/o Actualización de Datos
3
VISUALIZAR EVENTOS
Presentar los equipos que no responden al monitoreo
Estado de los dispositivos
USUARIO
Tabla: RANGO
Tabla: INFONODO
Tabla: NODO
Tabla: NODO_GRUPO
Tabla: GRUPO

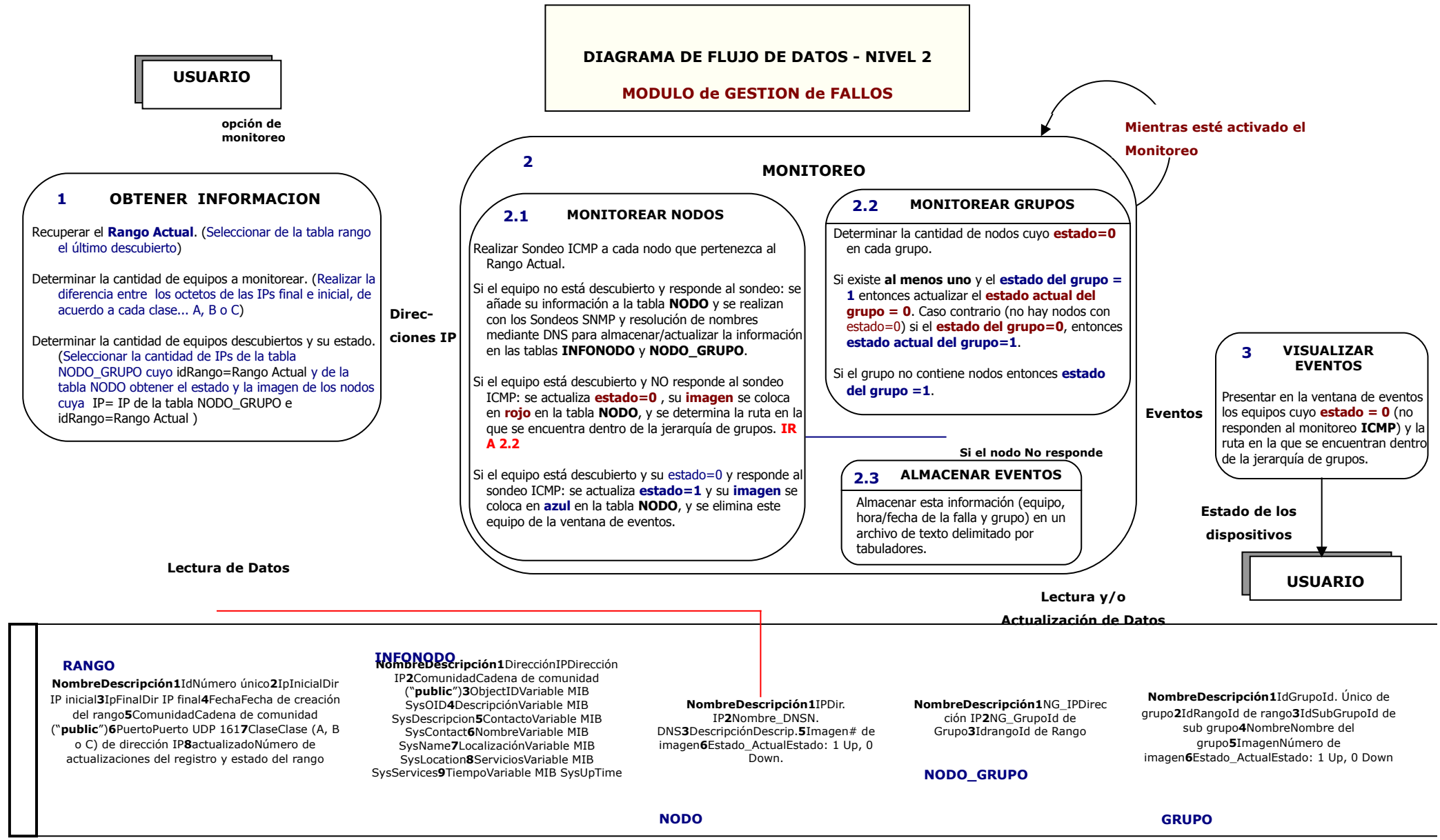


DIAGRAMA DE FLUJO DE DATOS - NIVEL 2
MODULO de GESTION de FALLOS
USUARIO
opción de monitoreo
Mientras esté activado el Monitoreo
1 OBTENER INFORMACION
Recuperar el Rango Actual. (Seleccionar de la tabla rango el último descubierto)
Determinar la cantidad de equipos a monitorear. (Realizar la diferencia entre los octetos de las IPs final e inicial, de acuerdo a cada clase... A, B o C)
Determinar la cantidad de equipos descubiertos y su estado. (Seleccionar la cantidad de IPs de la tabla NODO_GRUPO cuyo idRango=Rango Actual y de la tabla NODO obtener el estado y la imagen de los nodos cuya IP= IP de la tabla NODO_GRUPO e idRango=Rango Actual)
Direc-ciones IP
2 MONITOREO
2.1 MONITOREAR NODOS
Realizar Sondeo ICMP a cada nodo que pertenezca al Rango Actual.
Si el equipo no está descubierto y responde al sondeo: se añade su información a la tabla NODO y se realizan con los Sondeos SNMP y resolución de nombres mediante DNS para almacenar/actualizar la información en las tablas INFONODO y NODO_GRUPO.
Si el equipo está descubierto y NO responde al sondeo ICMP: se actualiza estado=0 , su imagen se coloca en rojo en la tabla NODO, y se determina la ruta en la que se encuentra dentro de la jerarquía de grupos. IR A 2.2
Si el equipo está descubierto y su estado=0 y responde al sondeo ICMP: se actualiza estado=1 y su imagen se coloca en azul en la tabla NODO, y se elimina este equipo de la ventana de eventos.
2.2 MONITOREAR GRUPOS
Determinar la cantidad de nodos cuyo estado=0 en cada grupo.
Si existe al menos uno y el estado del grupo = 1 entonces actualizar el estado actual del grupo = 0. Caso contrario (no hay nodos con estado=0) si el estado del grupo=0, entonces estado actual del grupo=1.
Si el grupo no contiene nodos entonces estado del grupo =1.
Si el nodo No responde
2.3 ALMACENAR EVENTOS
Almacenar esta información (equipo, hora/fecha de la falla y grupo) en un archivo de texto delimitado por tabuladores.
Eventos
3 VISUALIZAR EVENTOS
Presentar en la ventana de eventos los equipos cuyo estado = 0 (no responden al monitoreo ICMP) y la ruta en la que se encuentran dentro de la jerarquía de grupos.
Estado de los dispositivos
USUARIO
Lectura de Datos
Lectura y/o Actualización de Datos
RANGO
NombreDescripción1IdNúmero único2IpInicialDir IP inicial3IpFinalDir IP final4FechaFecha de creación del rango5ComunidadCadena de comunidad ("public")6PuertoPuerto UDP 1617ClaseClase (A, B o C) de dirección IP8actualizadoNúmero de actualizaciones del registro y estado del rango
INFONODO
NombreDescripción1DirecciónIPDirección IP2ComunidadCadena de comunidad ("public")3ObjectIDVariable MIB SysOID4DescripciónVariable MIB SysDescripcion5ContactoVariable MIB SysContact6NombreVariable MIB SysName7LocalizaciónVariable MIB SysLocation8ServiciosVariable MIB SysServices9TiempoVariable MIB SysUpTime
NombreDescripción1IPDir. IP2Nombre_DNSN. DNS3DescripciónDescrip.5Imagen# de imagen6Estado_ActualEstado: 1 Up, 0 Down.
NODO
NombreDescripción1NG_IPDirección IP2NG_GrupoId de Grupo3IdrangoId de Rango
NODO_GRUPO
NombreDescripción1IdGrupoId. Único de grupo2IdRangoId de rango3IdSubGrupoId de sub grupo4NombreNombre del grupo5ImagenNúmero de imagen6Estado_ActualEstado: 1 Up, 0 Down
GRUPO

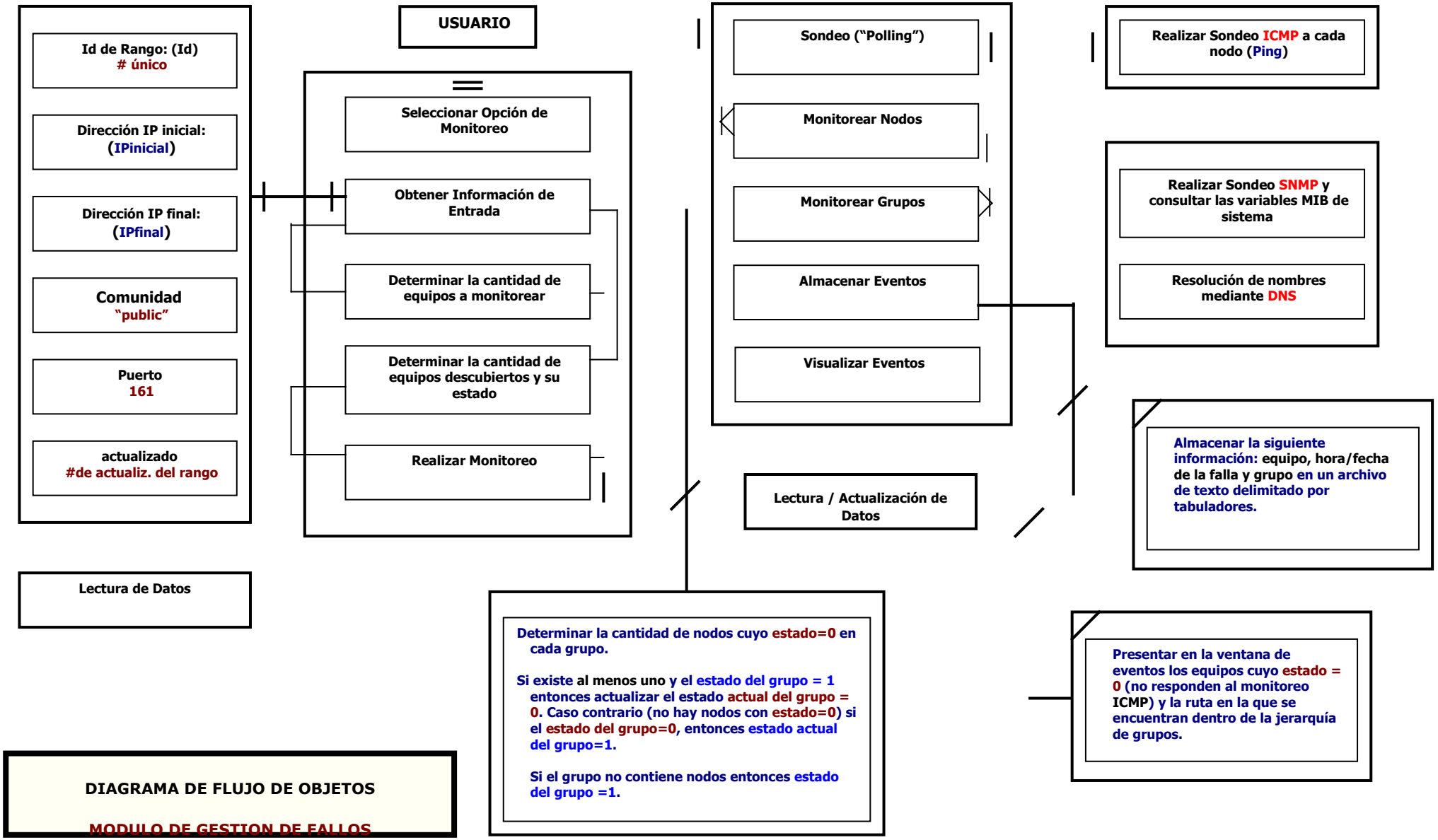


DIAGRAMA DE FLUJO DE OBJETOS

MODULO DE GESTION DE FALLOS

5.4 Módulo de Gestión del Rendimiento (MGDR)

Dentro de la Gestión del Rendimiento, la representación de información relacionada con el tráfico de la red en gráficos estadísticos y su análisis permiten tener una visión sobre el grado de utilización de los recursos de la red y otros indicadores del rendimiento.

5.4.1 Estudio de Factibilidad

Realizar una aplicación que permita recolectar y almacenar información sobre el tráfico de la red y representarla gráficamente es factible utilizando la primitiva SNMP-Get conociendo los OID de las variables MIB relacionadas con el tráfico (paquetes Unicast, No-Unicast y Multicast entrantes y salientes, paquetes descartados, tasa de errores).

5.4.2 Análisis y Diseño

Para el Módulo de Gestión del Rendimiento se requieren cinco procesos que permitirán la representación gráfica de la información relacionada con el rendimiento de la red. Estos procesos se explican a continuación:

- **Proceso "Obtener Información":** permite ingresar la dirección IP y la cadena de comunidad SNMP para consultar información relacionada con el rendimiento de una interfaz de dispositivo activo que soporte SNMP (ver **Fig. 5.12**).

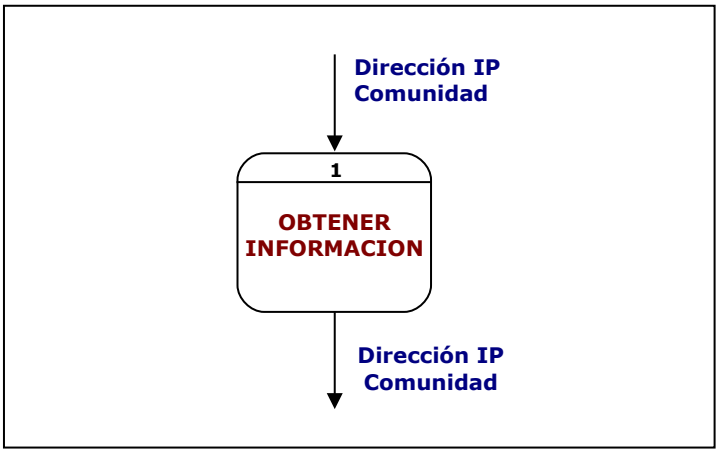


Fig. 5.12 MGDR - Proceso "Obtener Información"

- **Proceso "Navegar y Consultar Variables MIB":** permite ingresar la dirección IP, la cadena de comunidad SNMP y el OID de la(s) variable(s) MIB a consultar en el equipo activo seleccionado (ver **Fig. 5.13**).

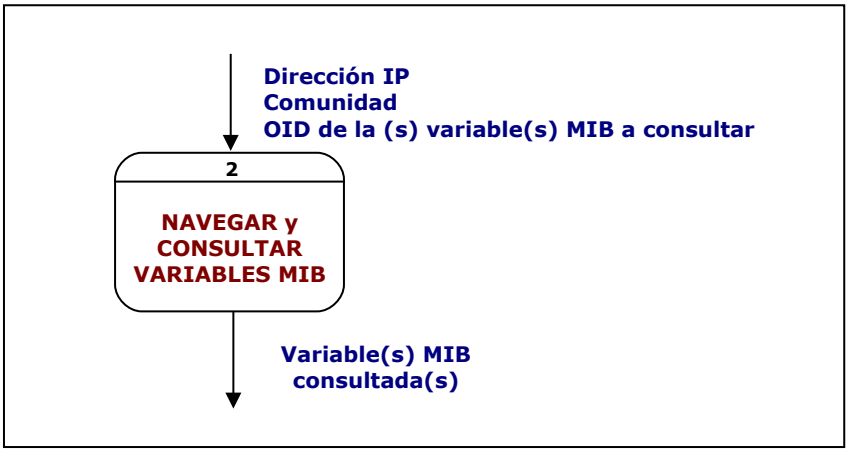


Fig. 5.13 MGDR - Proceso "Navegar y Consultar Variables MIB"

- **Proceso "Verificar Soporte SNMP":** permite determinar si un equipo tiene instalado o no el agente SNMP. Si el equipo seleccionado tiene instalado el agente SNMP se listan todas las interfaces para consultar información sobre el rendimiento, caso contrario se debe seleccionar otro equipo (ver **Fig. 5.14**).

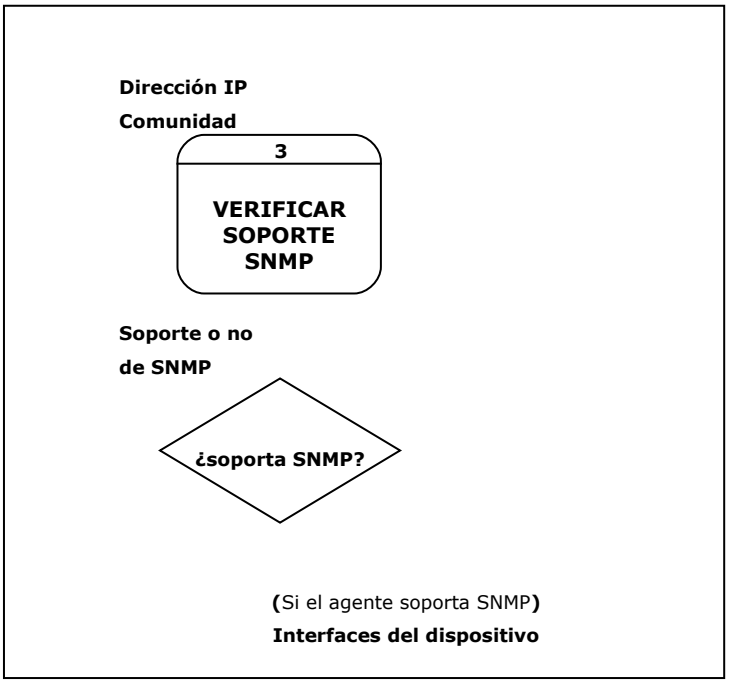


Fig. 5.14 MGDR - Proceso "Verificar Soporte SNMP"

- **Proceso "Consultar Información Estadística":** permite obtener información estadística sobre el rendimiento de la interfaz del dispositivo activo seleccionado que posee el agente SNMP. (ver **Fig. 5.15**).

Fig. 5.15 MGDR – Proceso "Consultar Información Estadística"

- **Proceso "Visualizar Información Estadística":** permite representar gráficamente en pantalla y almacenar en un archivo de texto la información estadística de las variables MIB relacionadas con el tráfico de la interfaz del dispositivo seleccionado. (ver **Fig. 5.16**).

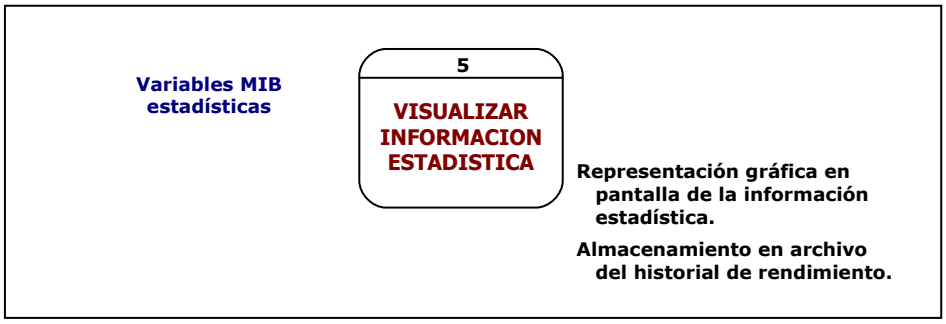


Fig. 5.16 MGDR – Proceso "Visualizar Información Estadística"

A continuación se detallan los Diagramas de Flujo de Datos de Nivel 0, Nivel 1 y Nivel 2 y el Diagrama de Flujo de Objetos para el Módulo de Gestión del Rendimiento.

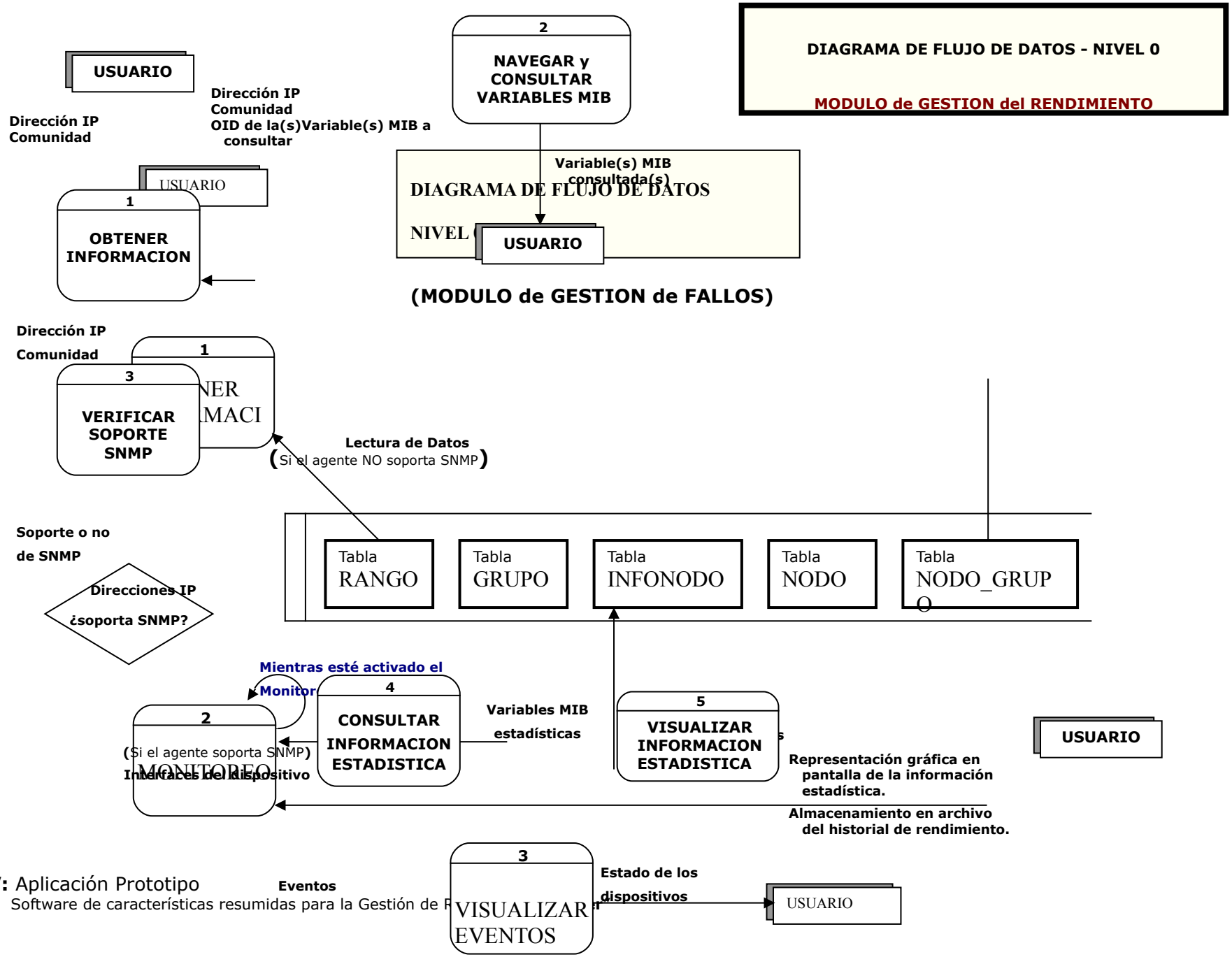


DIAGRAMA DE FLUJO DE DATOS - NIVEL 0
MODULO de GESTION del RENDIMIENTO
USUARIO
Dirección IP
Comunidad
OID de la(s)Variable(s) MIB a consultar
2
NAVEGAR y CONSULTAR VARIABLES MIB
Variable(s) MIB consultada(s)
DIAGRAMA DE FLUJO DE DATOS
NIVEL
USUARIO
1
OBTENER INFORMACION
(MODULO de GESTION de FALLOS)
Dirección IP
Comunidad
1
3
VERIFICAR SOPORTE SNMP
Lectura de Datos
(Si el agente NO soporta SNMP)
Soporte o no de SNMP
Direcciones IP
¿soporta SNMP?
Tabla RANGO
Tabla GRUPO
Tabla INFONODO
Tabla NODO
Tabla NODO_GRUPO
Mientras esté activado el Monitor
4
CONSULTAR INFORMACION ESTADISTICA
Variables MIB estadísticas
5
VISUALIZAR INFORMACION ESTADISTICA
USUARIO
2
(Si el agente soporta SNMP)
MONITOREO
Interfaces del dispositivo
Representación gráfica en pantalla de la información estadística.
Almacenamiento en archivo del historial de rendimiento.
Eventos
3
VISUALIZAR EVENTOS
Estado de los dispositivos
USUARIO

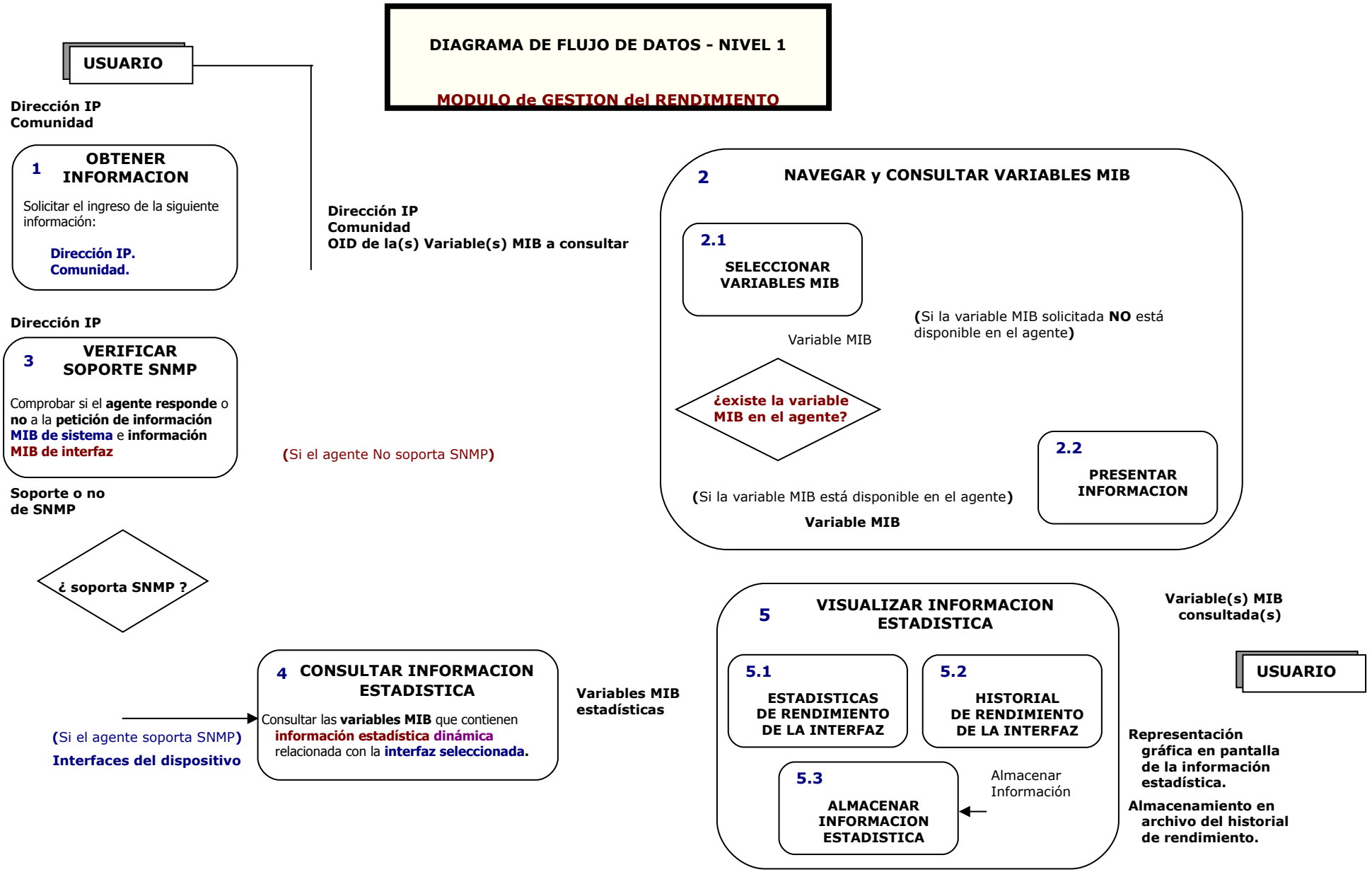


DIAGRAMA DE FLUJO DE DATOS - NIVEL 1
MODULO de GESTION del RENDIMIENTO
USUARIO
Dirección IP
Comunidad
1 OBTENER INFORMACION
Solicitar el ingreso de la siguiente información:
Dirección IP.
Comunidad.
Dirección IP
Comunidad
OID de la(s) Variable(s) MIB a consultar
2 NAVEGAR y CONSULTAR VARIABLES MIB
2.1 SELECCIONAR VARIABLES MIB
(Si la variable MIB solicitada NO está disponible en el agente)
Variable MIB
¿existe la variable MIB en el agente?
2.2 PRESENTAR INFORMACION
(Si la variable MIB está disponible en el agente)
Variable MIB
Dirección IP
3 VERIFICAR SOPORTE SNMP
Comprobar si el agente responde o no a la petición de información MIB de sistema e información MIB de interfaz
(Si el agente No soporta SNMP)
Soporte o no de SNMP
¿ soporta SNMP ?
(Si el agente soporta SNMP)
Interfaces del dispositivo
4 CONSULTAR INFORMACION ESTADISTICA
Consultar las variables MIB que contienen información estadística dinámica relacionada con la interfaz seleccionada.
Variables MIB estadísticas
5 VISUALIZAR INFORMACION ESTADISTICA
5.1 ESTADISTICAS DE RENDIMIENTO DE LA INTERFAZ
5.2 HISTORIAL DE RENDIMIENTO DE LA INTERFAZ
5.3 ALMACENAR INFORMACION ESTADISTICA
Almacenar Información
Variable(s) MIB consultada(s)
USUARIO
Representación gráfica en pantalla de la información estadística.
Almacenamiento en archivo del historial de rendimiento.

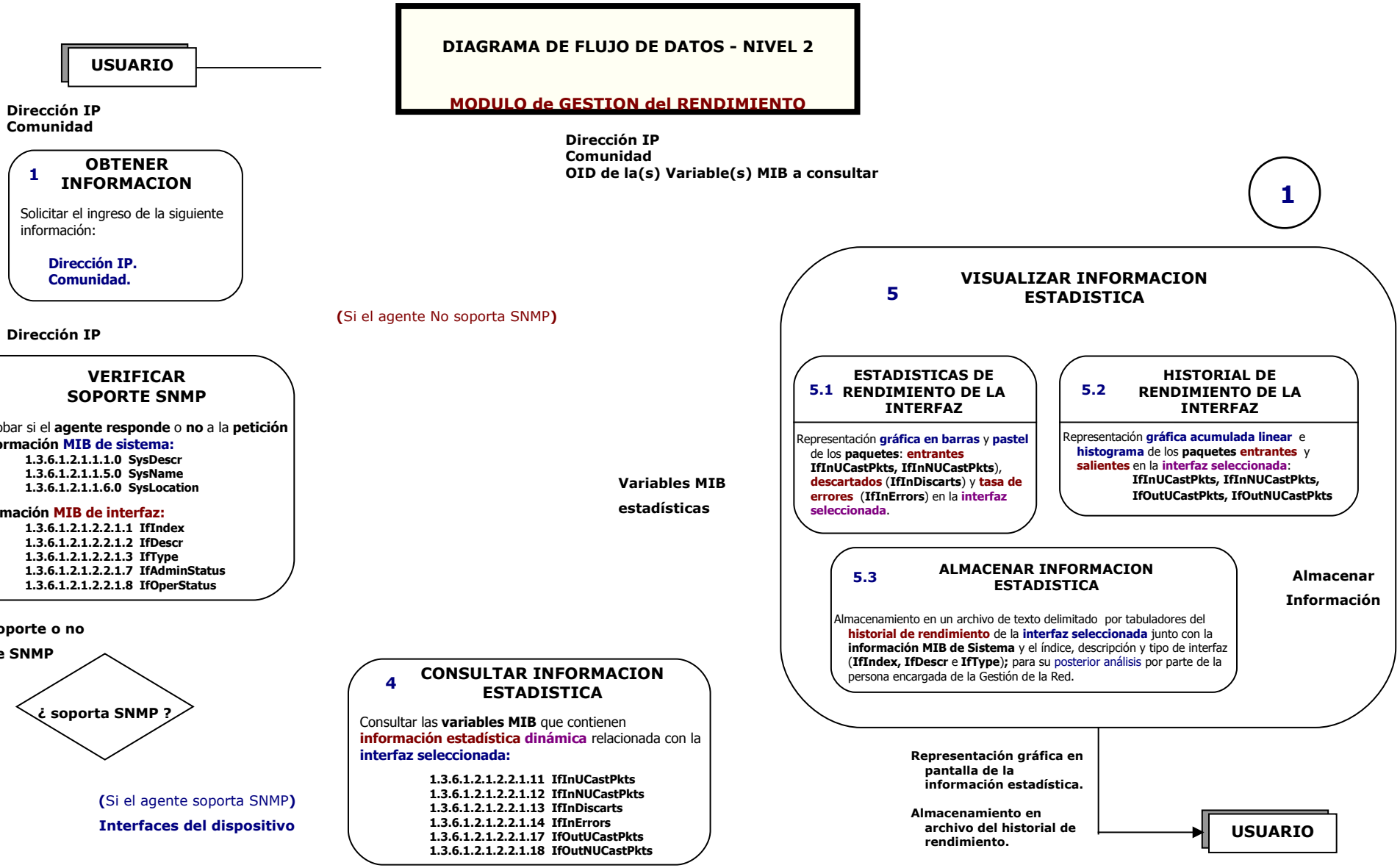


DIAGRAMA DE FLUJO DE DATOS - NIVEL 2
MODULO de GESTION del RENDIMIENTO
USUARIO
Dirección IP
Comunidad
1 OBTENER INFORMACION
Solicitar el ingreso de la siguiente información:
Dirección IP.
Comunidad.
Dirección IP
Comunidad
OID de la(s) Variable(s) MIB a consultar
1
(Si el agente No soporta SNMP)
Dirección IP
3 VERIFICAR SOPORTE SNMP
Comprobar si el agente responde o no a la petición de información MIB de sistema:
1.3.6.1.2.1.1.1.0 SysDescr
1.3.6.1.2.1.1.5.0 SysName
1.3.6.1.2.1.1.6.0 SysLocation
e información MIB de interfaz:
1.3.6.1.2.1.2.2.1.1 IfIndex
1.3.6.1.2.1.2.2.1.2 IfDescr
1.3.6.1.2.1.2.2.1.3 IfType
1.3.6.1.2.1.2.2.1.7 IfAdminStatus
1.3.6.1.2.1.2.2.1.8 IfOperStatus
Soporte o no de SNMP
¿ soporta SNMP ?
(Si el agente soporta SNMP)
Interfaces del dispositivo
Variables MIB estadísticas
4 CONSULTAR INFORMACION ESTADISTICA
Consultar las variables MIB que contienen información estadística dinámica relacionada con la interfaz seleccionada:
1.3.6.1.2.1.2.2.1.11 IfInUCastPkts
1.3.6.1.2.1.2.2.1.12 IfInNUCastPkts
1.3.6.1.2.1.2.2.1.13 IfInDiscarts
1.3.6.1.2.1.2.2.1.14 IfInErrors
1.3.6.1.2.1.2.2.1.17 IfOutUCastPkts
1.3.6.1.2.1.2.2.1.18 IfOutNUCastPkts
5 VISUALIZAR INFORMACION ESTADISTICA
5.1 ESTADISTICAS DE RENDIMIENTO DE LA INTERFAZ
Representación gráfica en barras y pastel de los paquetes: entrantes IfInUCastPkts, IfInNUCastPkts), descartados (IfInDiscarts) y tasa de errores (IfInErrors) en la interfaz seleccionada.
5.2 HISTORIAL DE RENDIMIENTO DE LA INTERFAZ
Representación gráfica acumulada linear e histograma de los paquetes entrantes y salientes en la interfaz seleccionada:
IfInUCastPkts, IfInNUCastPkts, IfOutUCastPkts, IfOutNUCastPkts
5.3 ALMACENAR INFORMACION ESTADISTICA
Almacenamiento en un archivo de texto delimitado por tabuladores del historial de rendimiento de la interfaz seleccionada junto con la información MIB de Sistema y el índice, descripción y tipo de interfaz (IfIndex, IfDescr e IfType); para su posterior análisis por parte de la persona encargada de la Gestión de la Red.
Almacenar Información
Representación gráfica en pantalla de la información estadística.
Almacenamiento en archivo del historial de rendimiento.
USUARIO

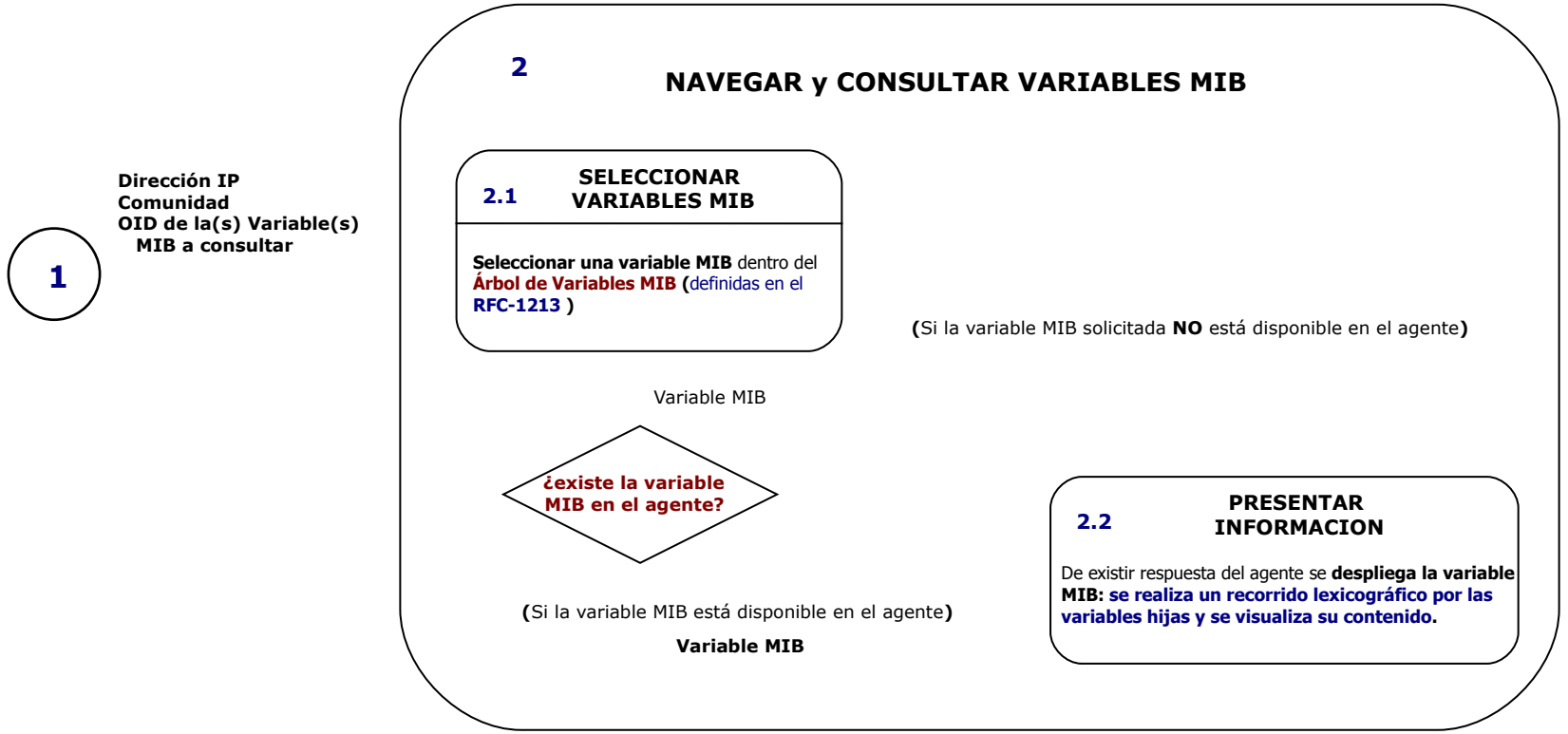


DIAGRAMA DE FLUJO DE DATOS - NIVEL 2

MODULO de GESTION del RENDIMIENTO
(Continuación)

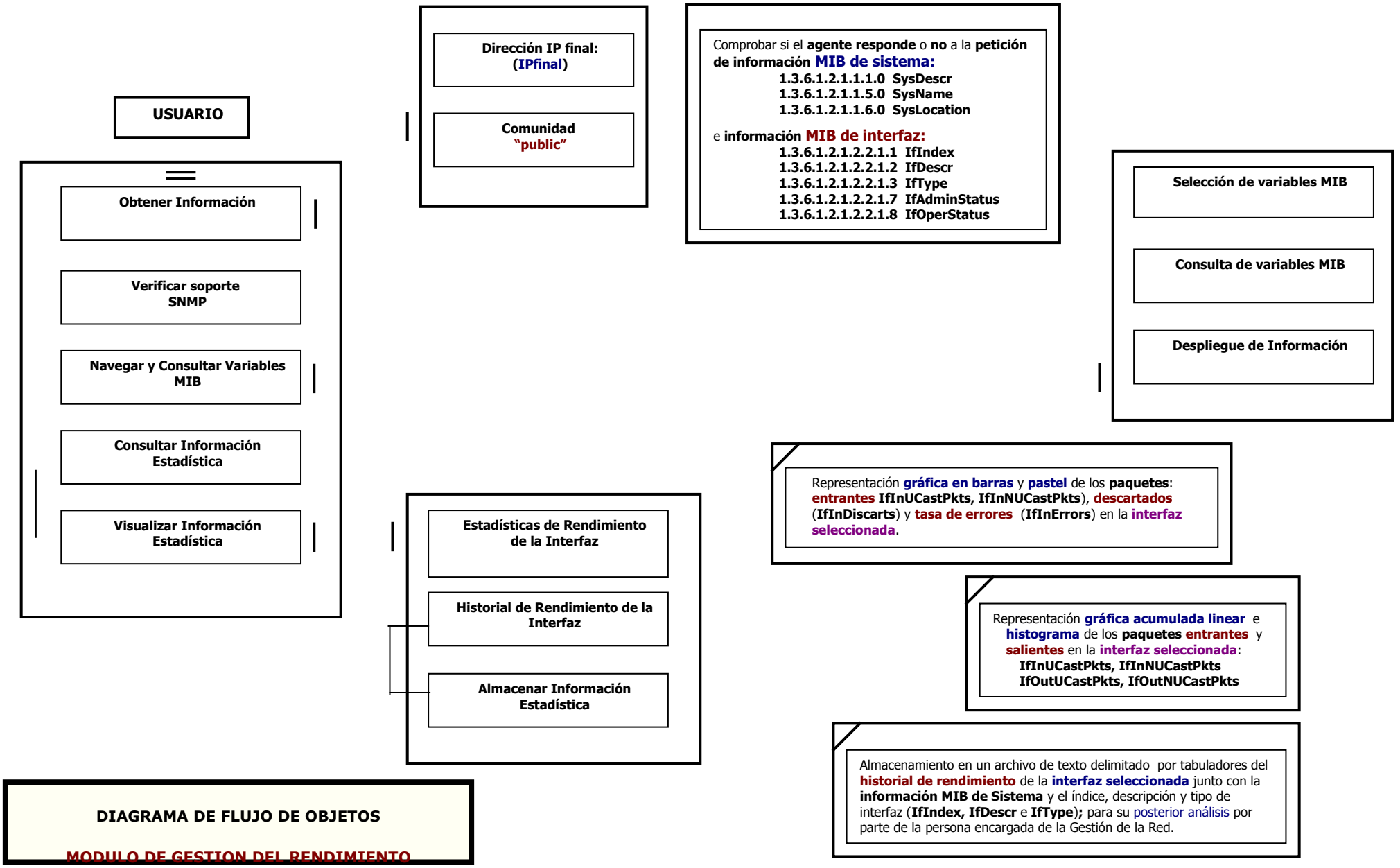


DIAGRAMA DE FLUJO DE OBJETOS

MODULO DE GESTION DEL RENDIMIENTO

5.5 Módulo de Gestión Remota (MGR)

La Gestión Remota de estaciones de trabajo Windows 9x, constituye una tarea muy importante dentro de la Gestión de Redes, ya que permite obtener información ampliada de los nodos finales gestionados, realizar una serie de tareas administrativas y brindar soporte desde un lugar centralizado.

5.5.1 Estudio de Factibilidad

Realizar una aplicación que permita obtener información ampliada de los nodos finales gestionados (Memoria utilizada, listado de procesos en ejecución, unidades de disco: etiqueta, espacio utilizado y disponible, recursos hardware, etc) es factible, ya que mediante el API de Windows se puede obtener dicha información y gracias a la utilización de SOCKET's enviarla hacia una aplicación de gestión.

5.5.2 Análisis y Diseño

Para el Módulo de Gestión Remota son necesarios tres procesos: dos de lado de la Estación Gestora y uno del lado de la Estación Gestionada. Los procesos se explican a continuación:

- **Proceso "Enviar Petición":** permite enviar una petición (token) solicitando información a la Estación Gestionada.
- **Proceso "Procesar Petición":** recibe el token enviado por la Estación Gestora, obtiene la información solicitada y la envía junto con un token (token + información solicitada).
- **Proceso "Recibir Información":** Recibe la información solicitada: separa el token de la información enviada por la Estación Gestionada y la presenta al encargado de la Gestión.

A continuación se describe el Flujo de Datos y se detallan los Diagramas de Flujo de Datos de Nivel 0, Nivel 1 y Nivel 2 y el Diagrama de Flujo de Objetos para el Módulo de Gestión Remota.

Consola de Gestión	Estación Gestionada
	• Crear una clave en el registro del sistema Operativo Windows 9x para que la aplicación de gestión se ejecute cada vez que se inicie el S.O. **HKEY_LOCAL_MACHINE** **SOFTWARE** **Microsoft** **Windows** **CurrentVersion** **Run** **"NetManager " "sgrserver.exe"** • Abrir la Base de Datos que contiene el listado de las aplicaciones restringidas, el intervalo de tiempo de reporte y el nombre del usuario. • Abrir el puerto UDP 1991 y dejarlo en escucha. (Puerto UDP Local 1991, Puerto UDP Remoto 1990)
• Se envía una petición (token) a todas las estaciones gestionadas solicitando nombre y dirección IP (host remoto **255.255.255.255**, puerto UDP Local 1990, Puerto UDP Remoto 1991).	
	• Se procesa la petición (token) de la consola de gestión y se devuelve la información solicitada. (token + inf. Solicitada)
• Recibe la información solicitada (se separa el token de la inf. Solicitada) de parte de todas las estaciones gestionadas. • Cierra el Socket UDP.	
• El usuario selecciona el equipo a monitorear • Se abre el puerto UDP 1990 y se establece una conexión con el puerto UDP 1991 del equipo remoto seleccionado. • Se envían peticiones (tokens) al equipo remoto seleccionado	
	• Se procesan las peticiones (tokens) de la consola de gestión y se devuelve la información solicitada. (token+inf solicitada)
• Se recibe la información solicitada (se separa el token de la inf. solicitada) y se muestra en la Consola.	
• Se cierra el Socket UDP	

Caso especial: opción "Escanear" (ver la pantalla del equipo remoto)

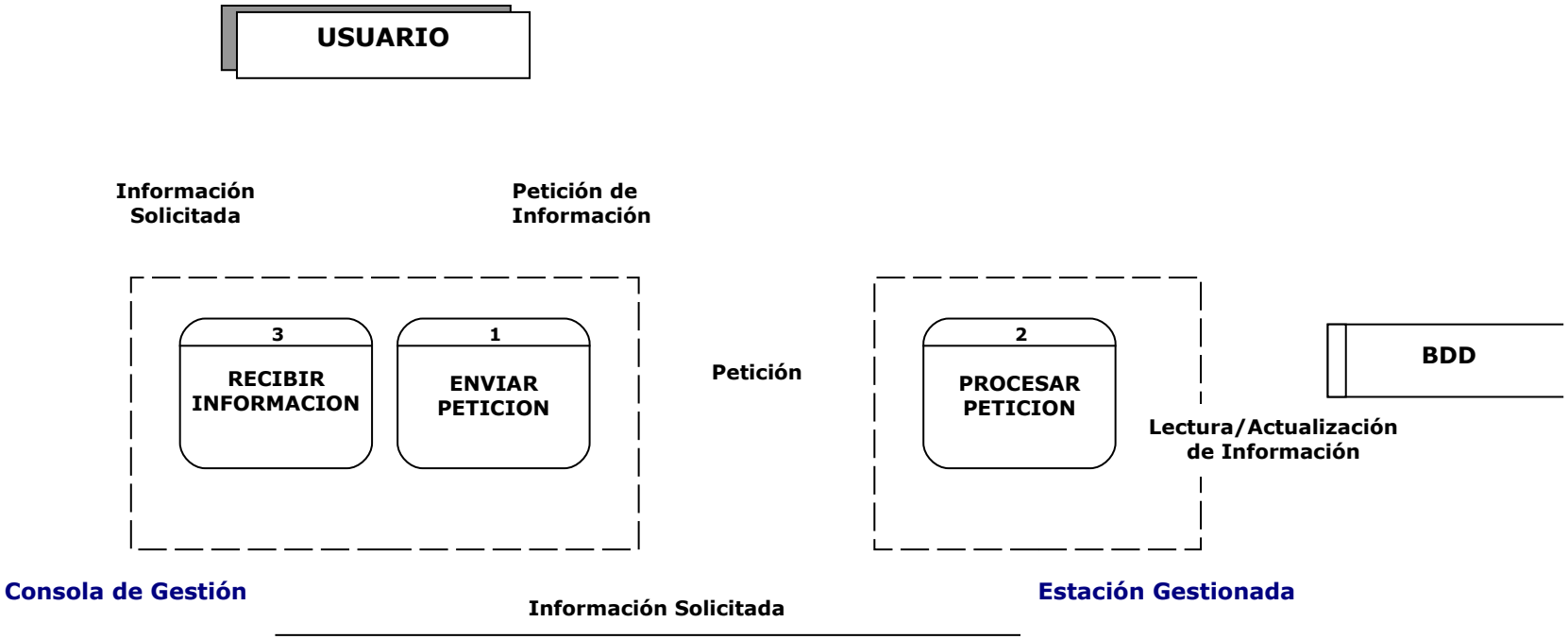
Consola de Gestión	Estación Gestionada
	• Abrir el puerto UDP 1991 y dejarlo en escucha. (Puerto UDP Local 1991, Puerto UDP Remoto 1990)
• El usuario selecciona el equipo a monitorear • Se abre el Socket UDP, puerto 1990 y se establece una conexión con el puerto UDP 1991 del equipo remoto seleccionado. • Se envía la petición de "escanear" (token) al equipo remoto seleccionado	

	• Se procesa la petición "escanear" : (token)
	  • Se cierra el puerto UDP
	  • Se abre un puerto TCP (8174)
	  • Se solicita petición de conexión al puerto TCP (8174).
	  • Se captura la imagen del escritorio en formato BMP
	• Se convierte el BMP en formato JPG.

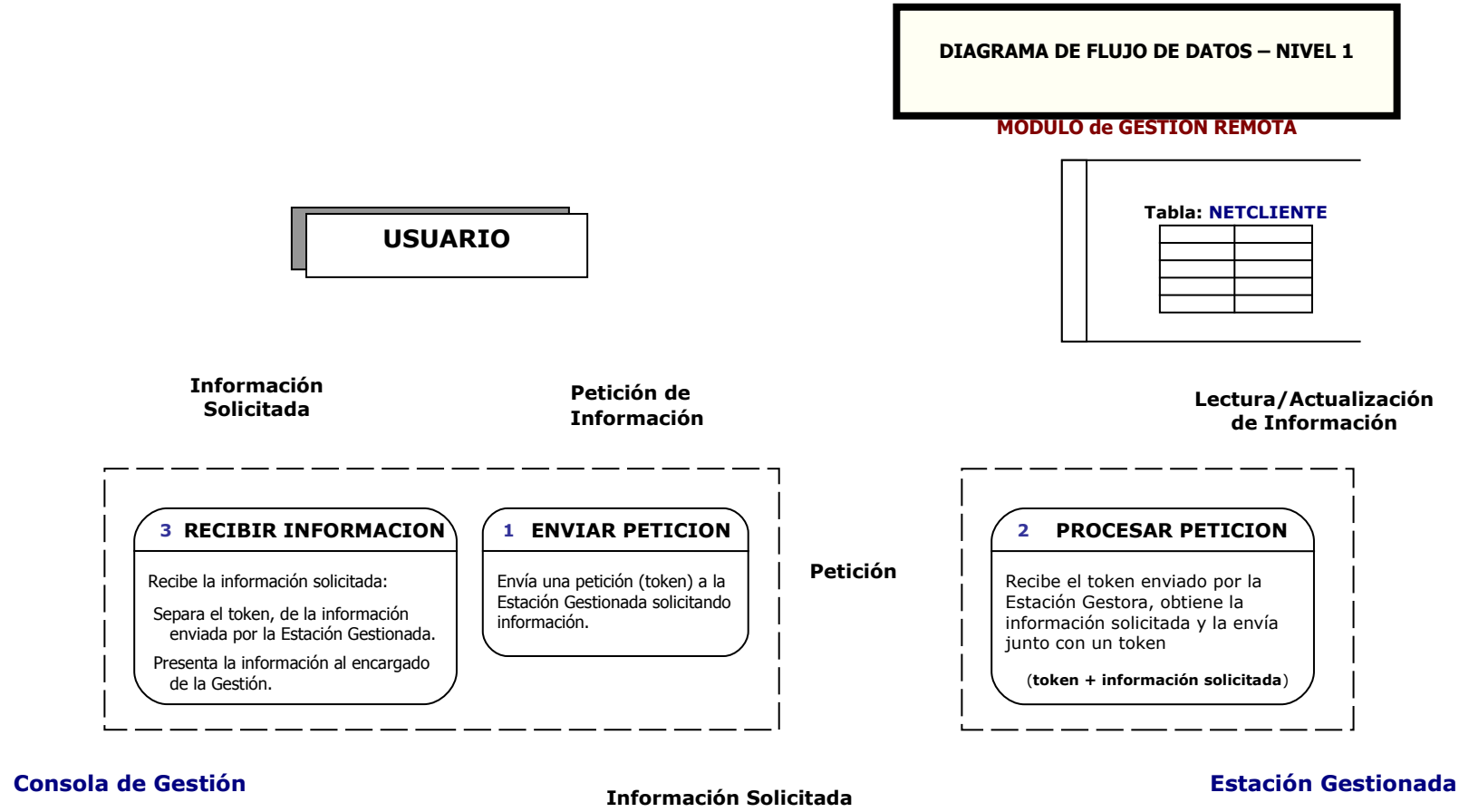
• Se acepta la petición de conexión al puerto TCP (8174). • Se esperan datos de la captura de imagen	
	• Se envía la imagen del escritorio (token+datos de la imagen)
• Se reciben los datos, se separa el token de la información • Se muestra la imagen capturada.	
NOTA Si la recepción de la imagen capturada demora más de cinco segundos (5 seg) se cierra el Socket TCP y se abre el Socket UDP para continuar con la administración remota.	**NOTA** Si el envío de la imagen capturada demora más de cinco segundos (5 seg) se cierra el Socket TCP y se abre el Socket UDP para continuar con la administración remota.

DIAGRAMA DE FLUJO DE DATOS - NIVEL 0

MODULO de GESTION REMOTA



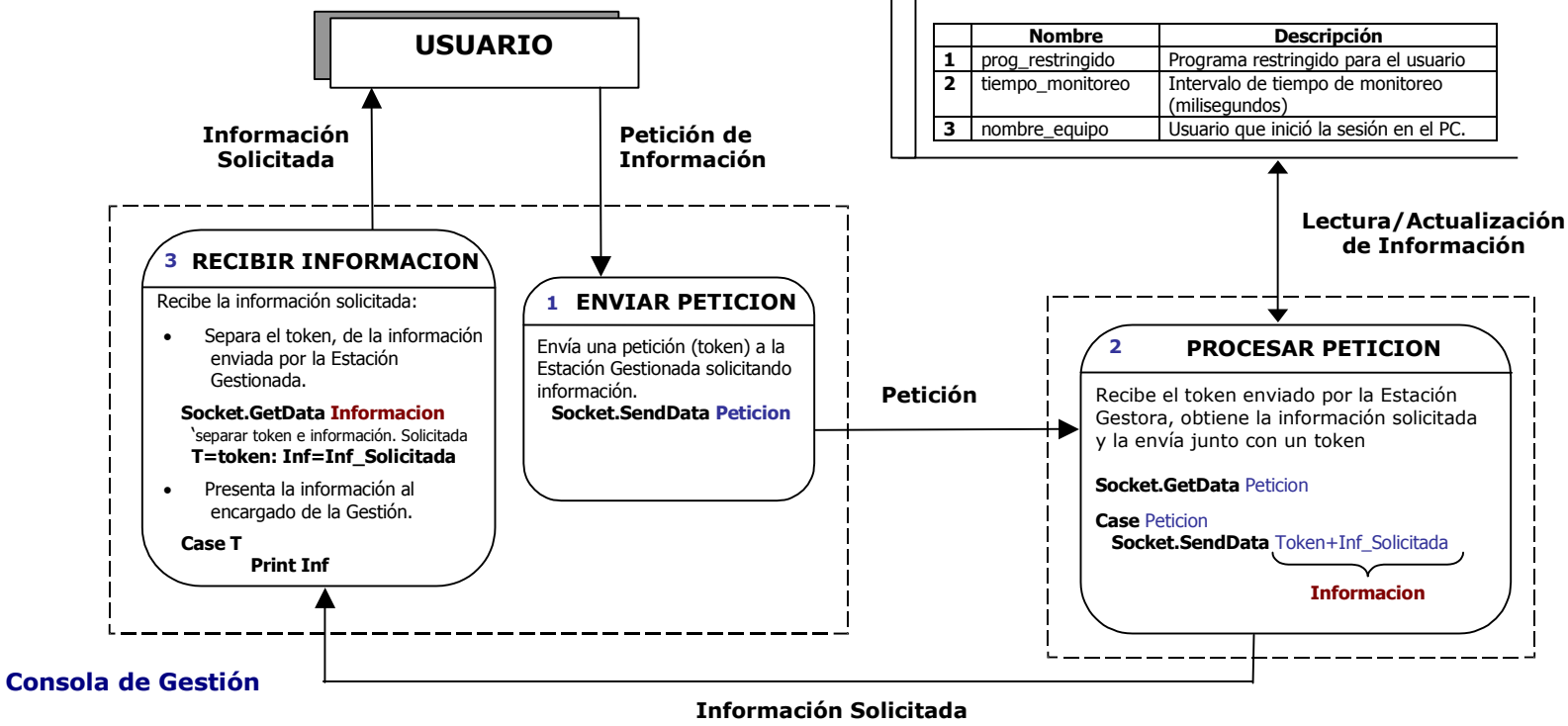
NOTA: Para este flujo de datos se requiere establecer una conexión mediante Socket UDP entre la Estación Gestionada y la Consola de Gestión



NOTA: Para este flujo de datos se requiere establecer una conexión mediante Socket UDP entre la Estación Gestionada y la Consola de Gestión

DIAGRAMA DE FLUJO DE DATOS – NIVEL 2

MODULO de GESTION REMOTA



NOTA: Para este flujo de datos se requiere establecer una conexión mediante Socket UDP entre la Estación Gestionada y la Consola de Gestión

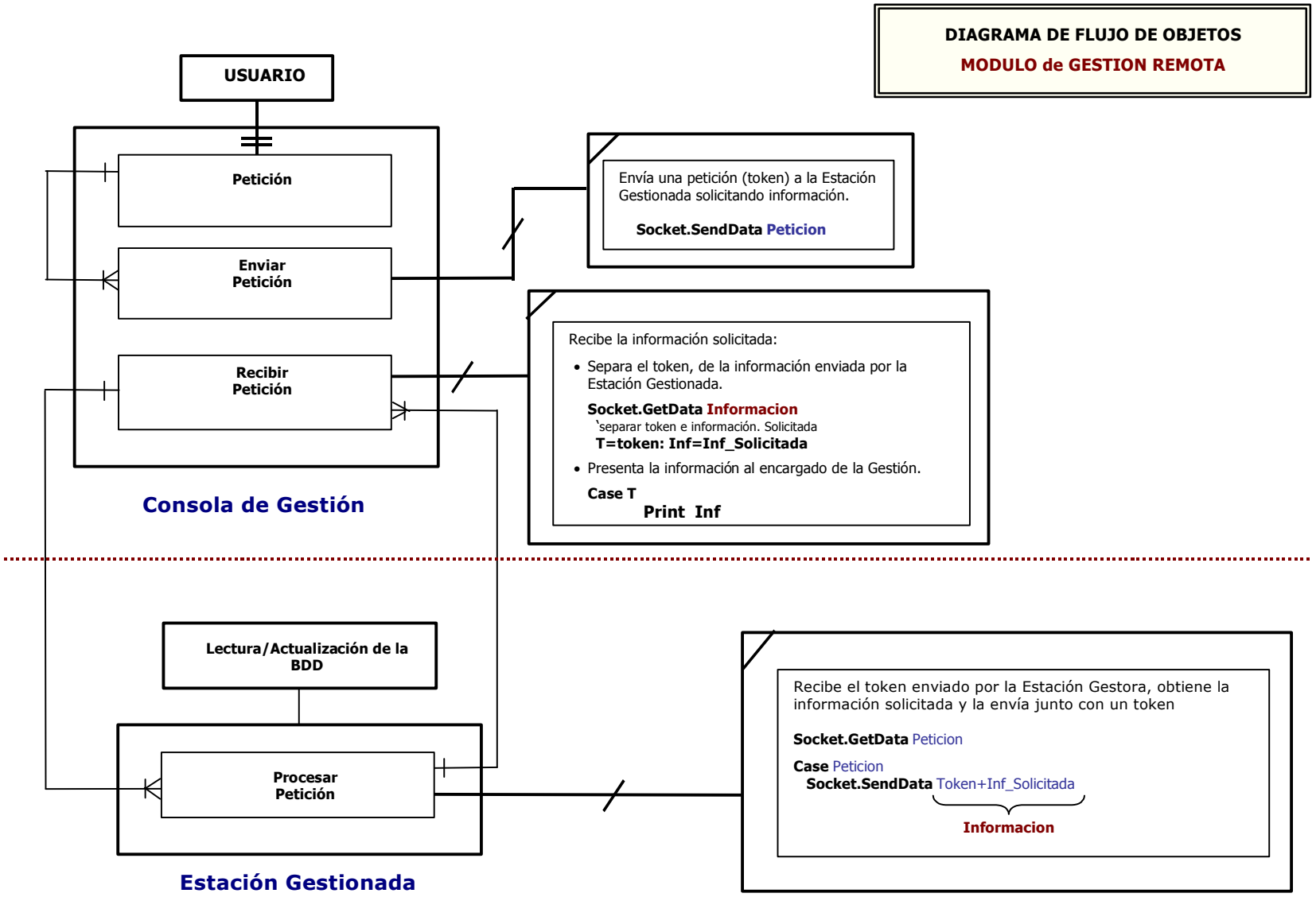
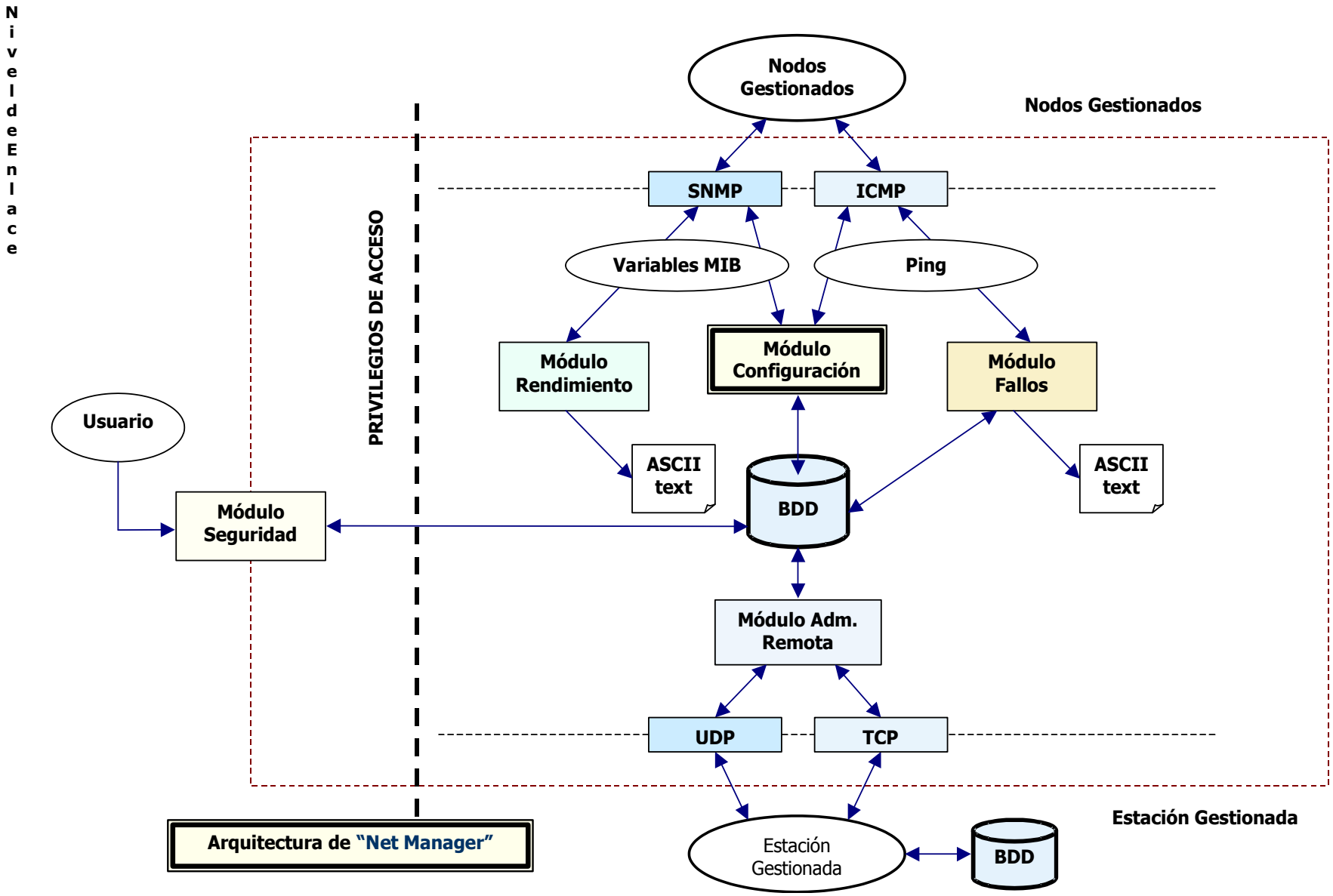


DIAGRAMA DE FLUJO DE OBJETOS
MODULO de GESTION REMOTA
USUARIO
Petición
Enviar Petición
Recibir Petición
Consola de Gestión
Envía una petición (token) a la Estación Gestionada solicitando información.
Socket.SendData Peticion
Recibe la información solicitada:
• Separa el token, de la información enviada por la Estación Gestionada.
Socket.GetData Informacion
'separar token e información. Solicitada
T=token: Inf=Inf_Solicitada
• Presenta la información al encargado de la Gestión.
Case T
Print Inf
Lectura/Actualización de la BDD
Procesar Petición
Estación Gestionada
Recibe el token enviado por la Estación Gestora, obtiene la información solicitada y la envía junto con un token
Socket.GetData Peticion
Case Peticion
Socket.SendData Token+Inf_Solicitada
Informacion


Nivel de Enlace
Nodos Gestionados
Nodos Gestionados
SNMP
ICMP
Variables MIB
Ping
PRIVILEGIOS DE ACCESO
Módulo Rendimiento
Módulo Configuración
Módulo Fallos
Usuario
ASCII text
BDD
ASCII text
Módulo Seguridad
Módulo Adm. Remota
UDP
TCP
Estación Gestionada
Arquitectura de "Net Manager"
Estación Gestionada
BDD

Referencias Bibliográficas

1. **HANSEN Gary, HANSEN James., "Diseño y Administración de Bases de Datos"**, Editorial Prentice Hall Hispanoamericana S.A., Segunda Edición, México, 1998.
2. **COHEN Daniel, ASIN Enrique., "Sistemas de Información - Enfoque para la toma de decisiones"**, Editorial Mc Graw Hill., Tercera Edición, México, 2000.
3. **KENDALL, Kenet., "Análisis y Diseño de Sistemas"**, Editorial Prentice Hall Hispanoamericana S.A., Tercera Edición, España, 1997.
4. **ODELL, James., "Análisis y Diseño Orientado a Objetos"**, Editorial Prentice Hall Hispanoamericana S.A., México, 1992.
5. **JAMES, Martin., "Métodos Orientados a Objetos"**, Editorial Prentice Hall Hispanoamericana S.A., México D.F., 1997.
6. **JONES Anthony, OHLUND Jim., "Network Programming for Microsoft Windows"**, Microsoft Press, 1999, **ISBN:** 0-7356-0560-2.
7. **MIRHO Charles, TERRISE Andre., "Communications Programming for Windows 95"**, Microsoft Press 1996. **ISBN:** 1-55615-668-5.
8. **NATALE BOB., "WINDOWS SNMP – An Open Interface for Programmig Network Management Applications using the Simple Network Management Protocol under Microsoft Windows"**, - **WinSNMP/Manager API** , ACE*COMM Corporation ., USA 1995 (http://www.winsnmp.com , http://www.acecomm.com).

CAPITULO VI

VERIFICACION DE LA HIPOTESIS, CONCLUSIONES y RECOMENDACIONES

6.1 Verificación de la Hipótesis

La hipótesis planteada al inicio de esta Tesis fue la siguiente:

"El análisis y evaluación de los Sistemas de Gestión de Red permitirá desarrollar el Software Net Manager que estará en capacidad de realizar funciones básicas de configuración, visualizar estadísticas de rendimiento, detectar los fallos y errores en los elementos activos de la REDUTN".

Al término de este trabajo se ha conseguido desarrollar un SGR prototipo que brinda las siguientes funcionalidades basándose en ciertas características obtenidas del estudio de los SGR Comerciales:

a) Funcionalidades Básicas de Configuración:

- Descubrimiento de los nodos que conforman la red mediante el ingreso de un rango de direcciones IP con la utilización de los protocolos SNMP e ICMP.
- Agrupamiento dinámico de los dispositivos descubiertos de acuerdo a la visión del administrador de la red.
- Asignación y Modificación de nombres e imágenes a los dispositivos descubiertos de acuerdo a la visión del administrador de la red.

- Búsqueda de los equipos descubiertos basándose en su descripción.
- Eliminación de cualquier dispositivo de la Consola de Administración.
- Consulta de variables MIB en los dispositivos que soportan SNMP.
- Despliegue de variables MIB de sistema de los nodos seleccionados.
- Uso de la utilidad Ping para los dispositivos descubiertos y acceso al servicio Telnet para los dispositivos que lo soporten.
- Despliegue de informes sobre los dispositivos descubiertos organizados en las siguientes categorías: rangos de direcciones, soporte SNMP, disponibilidad; además de las estaciones de trabajo Windows 9x en las que se encuentra instalada la aplicación cliente de administración remota (Net-Cliente).

b) Visualización de Estadísticas de Rendimiento:

- Despliegue en pantalla del historial de rendimiento, en gráficos de barras y líneas, de los paquetes unicast y no-unicast entrantes y salientes en la interfaz del dispositivo activo seleccionado, así como también de los paquetes unicast, multicast, descartados y errores entrantes, en gráficos de barras y pastel, durante un intervalo de tiempo.

c) Detección de Fallos:

- Mediante la monitorización del rango descubierto utilizando el sondeo ICMP - Ping – se obtiene un listado de los dispositivos que no responden a la solicitud de respuesta de mensaje de eco, su dirección IP, nombre resuelto mediante DNS, la hora en la que se generó dicho evento y su ubicación dentro del agrupamiento dinámico establecido por el encargo de la gestión de la red.

d) Administración Remota de Estaciones de Trabajo Windows 9x:

Al instalar el software cliente "NetCliente" en una Estación de Trabajo Windows 9x, se hace posible la comunicación con la Consola Central de Gestión permitiéndole al encargado de la gestión de la red realizar tareas como:

- Listar los procesos activos que se ejecutan en la estación remota, permitiendo restringir aquellos que infrinjan las políticas de utilización de los recursos de la red.
- Visualizar información general del sistema remoto (versión de Sistema Operativo, Memoria Física disponible, etc.).
- Visualizar la lista de recursos hardware disponibles en la estación remota.
- Listar los recursos restringidos y permitir o no su ejecución.
- Visualizar información de la(s) unidad(es) de disco de la estación remota (Etiqueta, Sistema de archivos, tamaño, espacio utilizado y disponible).
- Bloquear la estación remota, impidiendo su utilización.
- Cerrar la sesión, Reiniciar o Apagar la estación de trabajo remota.
- Enviar mensajes de aviso o advertencia al usuario de la estación gestionada.
- Capturar la imagen de la pantalla de la estación remota para observarla en la Consola Central de Gestión.

Por todo lo expuesto se considera que **se cumple en su totalidad la hipótesis**.

6.2 Conclusiones

Al finalizar el trabajo de investigación se concluye lo siguiente:

1. <u>Referente al aplicativo:</u>

- Visual Basic es una herramienta que facilita el uso de los objetos y eventos en cuanto a la incrustación de OCX personalizados.
- El descubrimiento de equipos con ICMP, SNMP y DNS es una implementación eficiente por que no ocupa mayor ancho de banda, ya que utiliza SNMP y DNS en caso de ser necesario (para rangos de descubrimiento pequeños).
- El manejo de UDP para manejar clientes remotos es liviano ya que utiliza datagramas no orientados a conexión.
- El monitoreo de equipos mediante ICMP para grandes redes no es aconsejable ya que genera tráfico, degradando el ancho de banda de la red.
- NetManager brinda un mejor desempeño gestionando redes pequeñas.
- Las bitácoras de historial de rendimiento generadas por NetManager pueden ser utilizadas en lo posterior para determinar el grado de utilización de ancho de banda de los equipos activos.
- El historial de eventos permitirá determinar el grado de disponibilidad de cada elemento gestionado.
- Con el modelo de comunicación gestor - agente se ha podido implementar una aplicación que facilita la gestión de escritorio (NetCliente), utilizando UDP y TCP.

2. <u>En cuanto al estudio realizado:</u>

- Se han podido conocer los entornos de gestión en los que se enmarcan los SGR.
  - Gestión empresarial
  - Gestión de escritorio

- Se han podido determinar que las necesidades de gestión de la REDUTN se enmarcan dentro de la gestión de escritorio.
- Se pudieron determinar las características funcionales necesarias con las que debe contar una aplicación de gestión de red.
- Ampliar los conocimientos sobre gestión de redes:
  - Modelos de gestión.
  - Protocolos al nivel de aplicación, transporte y red.
  - Variables MIB.
- Gracias a la documentación facilitada por las instituciones (Banco "La Previsora" Guayaquil, IBM-Ecuador y Microsoft-Ecuador) se pudo realizar el estudio de los SGR comerciales facilitando la elaboración de criterios para la evaluación y adquisición de SGR (Capítulo III).
- Con la evaluación de los SGR comerciales estudiados se concluye que el más adecuado para gestionar la REDUTN es el Microsoft Systems Managament Server, debido a que sus características funcionales abarcan la gestión de escritorio.
- Con el estudio y evaluación de los SGR y siguiendo las etapas de la ingeniería de software se ha desarrollado una aplicación prototipo para la gestión de redes (NetManager).

Se concluye además que el Centro de Cómputo de la UTN cuenta con la infraestructura y el personal calificado para realizar una gestión eficiente de la REDUTN.

6.3 Recomendaciones

Se recomienda lo siguiente:

1. **Referente al aplicativo:**

- Desarrollar un motor de inferencia con una base de conocimiento para determinar las causas y posibles soluciones a los problemas sucitados en las redes de computadores.
- Asignar una persona para que se capacite en el manejo de NetManager.
- Agregar otro método de descubrimiento de equipos.
- Se recomienda agregar un módulo de help desk para dar soporte a los usuarios remotos.
- Mejorar la aplicación de administración remota "NetCliente" para que permita el proceso de distribución de software, auditoría ampliada de hardware y software y la tarifación por el uso de aplicaciones en las estaciones Windows 9x, investigando a profundidad el API del sistema operativo Windows.

2. **Referente al estudio realizado:**

- Realizar un estudio pormenorizado sobre las normas y estándares aplicables a la gestión de redes.
- Realizar un estudio sobre la Notación de Sintaxis Abstracta Uno (ASN.1) y su utilización en la representación de la información de gestión en los modelos OSI e Internet y como aplicación realizar un intérprete de MIBs (que puede ser acoplado como utilidad para la consulta de variables MIB del prototipo NetManager).
- Realizar un estudio sobre RMON y la Ingeniería del Tráfico para la interpretación de las variables e indicadores del rendimiento de la red y su aplicación en la

implementación de un visor de estadísticas ampliadas de rendimiento en redes LAN.

- Realizar un estudio sobre las nuevas tendencias de la gestión de redes haciendo énfasis en la gestión WEB para la implementación de un SGR para la WEB empleando Java o CORBA.
- Profundizar el estudio sobre el modelo de gestión Internet, de manera especial en el protocolo SNMP (implementación de la primitiva SNMP-Set).

Indice de Contenidos

INTRODUCCION.....i

IDENTIFICACION DEL PROBLEMA.....i

Definición del problema.....i

Justificación.....i

Objetivos.....iii

GENERALES.....III
ESPECÍFICOS.....IV

CAPITULO I

CONCEPTOS GENERALES DE REDES.....1

1.1 Concepto de Red.....1

1.2 Ventajas de una Red de Computadoras.....2

1.3 Conceptos y Funcionalidades Básicas.....2

1.3.1 MODELO DE REFERENCIA OSI.....3
1.3.2 TOPOLOGÍAS.....4
1.3.3 PROTOCOLOS DE COMUNICACIONES.....5

1.4 Tipos de Redes.....5

1.4.1 RED DE AREA LOCAL (LAN, *LOCAL AREA NETWORK*).....5
1.4.2 RED DE AREA EXTENSA (WAN, *WIDE AREA NETWORK*).....6
1.4.3 RED DE AREA METROPOLITANA (MAN, METROPOLITAN AREA NETWORK).....6

1.5 Dispositivos de Interconexión.....6

1.5.1 FUNCIONES BÁSICAS.....6
1.5.2 CARACTERÍSTICAS PRINCIPALES.....7

Referencias Bibliográficas.....9

CAPITULO II

GESTION DE REDES.....10

2.1 Conceptos Generales de Gestión.....10

2.1.1 GESTIÓN.....10
2.1.2 ACTIVIDADES DE GESTIÓN.....10

2.2 Gestión de Redes.....13

2.2.1 ¿QUÉ ES LA GESTIÓN DE REDES?.....13

2.3 Arquitecturas de Gestión de Red.....15

2.3.1 MODELO OSI.....15

Areas Funcionales de la Gestión OSI.....19

2.3.2 MODELO TMN.....27

2.3.3 MODELO INTERNET (SNMP).....37

2.4 Normas y estándares aplicables a la Gestión de Redes.....47

Referencias Bibliográficas.....50

CAPITULO III

SISTEMAS DE GESTION DE RED.....51

INTRODUCCION.....51

3.1 ¿Qué es un Sistema de Gestión de Red?.....52

3.2 Funcionalidades básicas de un SGR.....52

3.2.1 SGR PARA REDES PEQUEÑAS.....53

3.2.2 SGR PARA REDES MEDIANAS Y GRANDES.....54

3.3 Componentes de un SGR.....55

3.4 Arquitectura Funcional de un SGR.....58

3.4.1 OBJETOS GESTIONADOS.....58

3.4.2 SISTEMAS DE GESTIÓN DE ELEMENTOS.....58

3.4.3 GESTOR DE SISTEMAS DE GESTIÓN.....58

3.4.4 INTERFAZ DE USUARIO.....58

3.5 Tendencias Tecnológicas y del Mercado.....59

3.6 Aspectos Técnicos en el Proceso de Adquisición de SGR.....64

Referencias Bibliográficas.....78

CAPITULO IV

SISTEMAS DE GESTION DE RED COMERCIALES.....79

4.1 Tivoli NetView.....80

4.1.1 CARACTERÍSTICAS DE TIVOLI NETVIEW.....80

4.1.2 PLATAFORMAS SOPORTADAS.....81

4.1.3 ARQUITECTURA DE TIVOLI NETVIEW.....82

4.1.4 GESTIÓN DE LA SEGURIDAD.....84

4.1.5 GESTIÓN DE CONFIGURACIÓN.....85

4.1.6 GESTIÓN DE FALLAS Y RECUPERACIÓN.....88

4.1.7 GESTIÓN DE RENDIMIENTO DE TIVOLI NETVIEW.....92

4.2 Spectrum Enterprise Manager.....93

4.2.1 CARACTERÍSTICAS DE SPECTRUM.....94

4.2.2 PLATAFORMAS SOPORTADAS....96
4.2.3 ARQUITECTURA DE SPECTRUM....98
4.2.4 GESTIÓN DE LA SEGURIDAD....102
4.2.5 GESTIÓN DE LA CONFIGURACIÓN....104
4.2.6 GESTIÓN DE FALLAS Y RECUPERACIÓN....108
4.2.7 GESTIÓN DEL RENDIMIENTO....111

4.3 Microsoft Systems Management Server 2.0....113

4.3.1 CARACTERÍSTICAS DE MSMS....113
4.3.2 PLATAFORMAS SOPORTADAS....114
4.3.3 ARQUITECTURA DEL MSMS....114
4.3.4 GESTIÓN DE LA SEGURIDAD....119
4.3.5 GESTIÓN DE LA CONFIGURACIÓN....121
4.3.6 GESTIÓN DE FALLAS Y RECUPERACIÓN....125
4.3.7 GESTIÓN DEL RENDIMIENTO....126

Referencias Bibliográficas....127

CAPITULO V

APLICACIÓN PROTOTIPO

Software de Características Resumidas para la Gestión de Redes "Net Manager"....129

Introducción....129

5.1 Módulo de Gestión de la Seguridad (MGS)....130

5.2 Módulo de Gestión de la Configuración (MGC)....137

5.3 Módulo de Gestión de Fallos (MGF)....147

5.4 Módulo de Gestión del Rendimiento (MGDR)....154

5.5 Módulo de Gestión Remota (MGR)....163

Referencias Bibliográficas....171

CAPITULO VI

VERIFICACION DE LA HIPOTESIS, CONCLUSIONES y RECOMENDACIONES. .172

6.1 Verificación de la Hipótesis....172

6.2 Conclusiones....175

6.3 Recomendaciones....177

ANEXO A: **Análisis del Rendimiento**

ANEXO B: **Evaluación de Sistemas de Gestión de Red Comerciales**

ANEXO C: **Implementación Sistema Prototipo "NetManager"**

ANEXO D: **Manual de Usuario**

ANEXO E: **Variables MIB**

ANEXO F: **Características de los Equipos Activos**