xx (101 594.1)

CINVESTAV - IPN

Centro de Investigación y de Estudios Avanzados del IPN
Unidad Guadalajara

Sistemas de gestión de redes de telecomunicaciones para pequeñas y medianas empresas

TESIS QUE PRESENTA
HECTOR CASTILLO HERNANDEZ

PARA OBTENER EL GRADO DE
MAESTRO EN CIENCIAS

EN LA ESPECIALIDAD DE
INGENIERÍA ELÉCTRICA

Guadalajara, Jal., Febrero de 2002

Sistemas de gestión de redes de telecomunicaciones para pequeñas y medianas empresas

Tesis de Maestría en Ciencias
Ingeniería Eléctrica

por:

Héctor Castillo Hernández

Ingeniero en Sistemas Computacionales
Instituto Tecnológico de Estudios Superiores de Occidente, 1991–1995
Becario del CONACYT, expediente no. **142657**

Directores de Tesis:

Dr. Deni Librado Torres Román

CINVESTAV del IPN Unidad Guadalajara, Febrero de 2002.

Si puedes tener cordura cuando otros la pierden,
si puedes confiar en ti cuando todos dudan de ti, pero tomas en cuenta sus dudas,
si puedes esperar sin que te canse la espera,
o soportar calumnias sin pagar con la misma moneda,
o ser odiado sin dar cabida al odio, y no por eso parecer demasiado bueno o sabio.

si puedes soñar sin que tus sueños te dominen,
si puedes pensar sin que tus pensamientos sean tu meta,
si puedes habértelas con triunfo o con desastre y tratar por igual a ambos farsantes,
si puedes tolerar que se tergiverse la verdad que has expresado,
y la conviertan en trampa para necios,
o ver en ruina la obra de tu vida y agacharte y reconstruirla con viejas herramientas.

si puedes hacer un atadijo con todas tus ganancias y arrojarlas al capricho del azar,
perderlas y volver a empezar sin que salga de tus labios una queja,
si puedes poner al servicio de tus fines, corazón entusiasmo y fortaleza,
y resistir aunque no te quede nada, salvo la voluntad que les diga: Adelante!

si puedes dirigirte a la multitud sin perder tu virtud,
si todos cuentan contigo pero no en demasía.
si puedes llenar el implacable minuto con 60 segundos de esfuerzo denotado,
entonces, tuya es la tierra y cuanto hay en ella y...Serás un hombre, hijo mío!

Anónimo

Tabla de Contenido

Agradecimientos:

Este trabajo lo dedico a Josefina Aguilar, Carmelo Hernández, Laura Lerma y Armando Castillo, cimientos y raiz de mi familia, cuyos consejos y platicas amenas quedarán en mi.

A Isabel y a Héctor, mis padres, por su apoyo incondicional, con quienes los momentos dificiles terminan siendo buenos momentos, tambien a Paty y a Ma. Isabel por contribuir a estos.

A Blas Castañeda y al Dr. Leonardo Soto por sus comentarios, aportaciones y apoyo al desarrollo de este trabajo.

al Dr. Deni quien me asesoró tanto con el trabajo de maestría como en el proceso de titulacion de licenciatura.

Al Consejo Nacional de Ciencia y Tecnología (CONACyT), por brindarme el apoyo económico, durante dos años, para dedicarme por completo al estudio de esta maestría.

A mis compañeros, por su buena actitud de trabajo.

Y por último, pero definitivamente el mas importante a Dios por permitir todo lo anterior.

1 Introducción

1.1 La necesidad de la gestión de redes de telecomunicaciones

Las redes de telecomunicaciones se han convertido en elementos esenciales en las actividades de las personas que laboran tanto en instituciones estatales y privadas como en sus propios domicilios, utilizando servicios de voz, datos y vídeo. En la mayoría de los casos, estas redes aseguran el crecimiento y supervivencia de las organizaciones.

De forma paralela al avance de los servicios de telecomunicaciones, nuevas tecnologías de red continúan evolucionando, tal es el caso de tecnologías de transporte (SONET/SDH), de acceso (CDMA) y de conmutación (switches ATM o Frame Relay). Estos constantes avances de servicios y tecnología como respuesta a expectativas de los usuarios, han creado la necesidad de verificar que los servicios proporcionados por la red sean confiables, que sea posible detectar fallas rápidamente, monitorear desempeño de resursos y servicios, utilizar eficientemente los recursos de red, administrar la seguridad, añadir nuevas tecnologías de red minimizando tiempo y costo. Es decir, surge la necesidad de gestionar la red de telecomunicaciones, de tal forma que los proveedores de servicios, clientes corporativos y usuarios finales puedan alcanzar sus objetivos.

1.2 Características de la gestión tradicional

Las redes de telecomunicaciones se caracterizan por contar con *elementos de red* de diferentes proveedores, los cuales pueden contar con *soluciones de gestión propietarias*. El resultado es un ambiente de gestión formado por múltiples administraciones con poca interacción entre ellas. Estas soluciones parciales independientes y consumidoras de recursos contribuyen a un ambiente de gestión deficiente, complejo y costoso.

La gestión tradicional cuenta con procedimientos, herramientas de configuración, detección de fallas, monitoreo de desempeño, seguridad, contabilidad entre otras funciones de gestión basadas en una relación maestro - esclavo entre el sistema de gestión o sistema de operación (OS, Operation System) y los elementos de red (NE, Network Element), estos últimos realizaban solamente operaciones básicas con poca habilidad para controlar actividades o tomar decisiones diferentes de transmitir información o invocar algún proceso, por el contrario los OSs realizaban toda la carga de trabajo de OAM&P (Operation, Administration, Maintenance & Provisioning).

Las diferentes configuraciones e interfaces de gestión aumentan la complejidad y especializan las operaciones de gestion, debido a las implementaciones específicas de elementos de red de los diferentes proveedores de equipo. Provocando que la adición de nuevos servicios y tecnologías fuera un proceso más tardado y complejo, además que se creaba la necesidad de contar con recursos humanos especializados en estas implementaciones.

Como resultado, ha sido difícil para el proveedor de servicios de telecomunicaciones englobar los servicios, tecnologías y procesos de gestión de red de manera no costosa,

rápida y competitiva en respuesta a los rápidos cambios de la industria de las telecomunicaciones.

A raíz de los problemas antes mencionados, surge la necesidad de realizar una estandarización con la finalidad de desarrollar las funciones de gestión de forma óptima en el sentido de recursos utilizados, personal especializado y complejidad de gestión. La estandarización incluyó interfaces, representación de la información, protocolos de acceso a esta información y la definición de funciones de gestión.

Algunos organismos y grupos de desarrollo encargados de las estandarizaciones son: ANSI (American National Standards Institute), ITU (International Telecommunications Union antes CCITT), IEEE (Institute of Electrical and Electronics Engineers), ISO/IEC (International organization for Standardization/ International Electrotechnical Commission), IETF (Internet Engineering Task Force).

1.3 Contribuciones de esta tesis

Un sistema de gestión, es una herramienta para el administrador de red, quien es responsable de garantizar el buen funcionamiento de las redes locales y de área amplia; además, evalúa las tecnologías existentes y diseña las modificaciones necesarias para la evolución de la red. Estos sistemas por lo general son muy costosos y son desarrollados para un sistema operativo específico (plataforma), razones por lo que éstos se encuentran económica y operacionalmente fuera del alcance muchas empresas pequeñas y medianas.

Los objetivos del presente trabajo son:

- Realización de un estudio crítico de la gestión de redes de telecomunicaciones.
- Diseñó e implementación de un sistema de gestión para pequeñas y medianas empresas.
- Que el sistema desarrollado sea no costoso e independiente de la plataforma.

La finalidad es que el sistema desarrollado disminuya las desventajas económicas y operacionales que imponen los grandes sistemas de plataforma y permita, además de gestionar la red, ayudar a su planeación y dimensionamiento.

El proyecto se basa en la especificación de las funciones de gestión de la RGT (Red de Gestión de Telecomunicaciones) definidas por la Unión Internacional de Telecomunicaciones (ITU) asi como en las propuestas de gestion desarrolladas para Internet (IETF).

1.4 Estructura de la tesis

Este trabajo se divide en 2 partes: en la primera se realiza un estudio de las diferentes propuestas y estándares para la gestión de redes de telecomunicaciones desde el punto de vista de la arquitectura e implementación de la misma.

En la segunda parte se realiza el ciclo de desarrollo de software; análisis, diseño e implementación para un sistema de gestión centralizado.

Parte I: Revisión de los estándares, arquitecturas y propuestas para la gestión de redes

2 Propuestas de Arquitecturas para la gestión de redes de telecomunicaciones

Existen dos propuestas de arquitecturas de gestión definidas por diferentes organismos:

- La ITU(International Telecommunications Union) quien define la red de gestión de telecomunicaciones (RGT, TMN Telecommunications Management Network) y utiliza CMIS/CMIP (Common Management Information Services / Common Management Information Protocol) como protocolo y modelo de información de gestión, especificado por la ISO, pero adoptado por la ITU.
- IETF (Internet Engineering Task Force) e IAB (Internet Architecture Board) definen a SNMP (Simple Network Management Protocol) y su arquitectura como propuesta de gestión.

Ambas propuestas buscan la interoperabilidad tanto entre los dispositivos de diferentes proveedores como entre administraciones de gestión (p.e. una red privada tiene acceso restringido de gestión a los elementos de la red publica que utiliza). Cada propuesta define su estructura de información de gestión de manera muy diferente, estos protocolos definen un conjunto de mensajes y servicios para realizar consultas en los dispositivos gestionados y notificación de eventos ocurridos en los mismos. Las diferentes propuestas fueron desarrolladas bajo diferentes filosofías.

La propuesta ITU/ISO plantea una arquitectura con diferentes niveles de abstracción con una estructura de información de gestión dinámica orientada a objetos sin preocuparse por la implementación, de aquí que actualmente muchas especificaciones de la RGT con CMIS/CMIP no se hayan implementado aún.

Por otro lado las características de los estándares de IETF es que son simples, implementables y se van modificando y mejorando según las necesidades del mercado. SNMP nació como una propuesta a corto plazo pero la simplicidad de éste tanto en concepto como en implementación lo ha hecho más popular que CMIS/CMIP. Esto no significa que SNMP sea mejor que CMIP. A continuación se describen las propuestas con más detalle.

2.1 Red de Gestión de Telecomunicaciones (ITU)

El objetivo de las especificaciones de la RGT es proporcionar un marco para el monitoreo y control de las funciones de red primarias mediante el concepto de modelo genérico de red para gestión, aplicable a diferentes equipos empleando modelos genéricos de información e interfaces normalizadas.

La RGT trata de hacer que las capacidades de las funciones de gestión se apliquen tanto entre los dispositivos de diferentes proveedores como entre administraciones de gestión diferentes, usando interfaces normalizadas, y que puedan operar en conjunto para realizar la gestión de la red.

La recomendación M.3010 [3] define el concepto de RGT en diferentes niveles de abstracción:

- Arquitectura funcional.
- Arquitectura física.
- Arquitectura de información.
- Arquitectura lógica estratificada.
    - Capa de gestión de elemento.
    - Capa de gestión de red.
    - Capa de gestión de servicio.
    - Capa de gestión empresarial.

La Arquitectura funcional describe la distribución apropiada de la funcionalidad dentro de la RGT, con la posibilidad de definir bloques, con diferentes tareas, usados para realizar una RGT de cualquier grado de complejidad.

Arquitectura física, define cómo las funciones de gestión pueden ser implementadas en equipos físicos, en esta arquitectura se definen y describen las interfaces que unen a los bloques funcionales especificados en la arquitectura funcional.

Arquitectura de información, describe la estructura de la información de gestión, conceptos que han sido adoptados de la propuesta de gestión OSI (CMIS/CMIP).

Arquitectura lógica estratificada, considerada como la aportación más importante de esta propuesta. Es un modelo que muestra como la gestión puede ser estructurada de acuerdo a las diferentes responsabilidades y propone los siguientes estratos: *gestión de elemento, de red, de servicio y de empresa*. Muchas veces ésta última se relaciona más con la gestión estratégica y táctica que con la operacional.

2.1.1 Requerimientos de una arquitectura de gestión

La RGT debe percibir las redes de telecomunicaciones y los servicios como colecciones de sistemas cooperantes. La *arquitectura* es el concepto que controla la gestión de distintos sistemas a fin de obtener un efecto coordinado con respecto a la red. La introducción de la RGT ofrece a las administraciones la posibilidad de lograr una diversidad de objetivos de gestión, en particular:

- minimiza los tiempos de reacción de gestión ante eventos de la red
- minimiza la carga causada por el tráfico de gestión cuando se utiliza la red de telecomunicaciones para transmitir información de gestión;
- posibilita la dispersión geográfica del control sobre aspectos de la operación de red
- proporciona mecanismos de aislamiento para minimizar los riesgos de seguridad
- proporciona mecanismos de aislamiento para localizar y contener los fallos de red
- mejora la asistencia de servicio y la interacción con los clientes

A fin de poder tener en cuenta al menos estos objetivos, la arquitectura de la RGT deberá cumplir los siguientes requisitos:

- posibilitar la gestión de redes, equipos y servicios heterogéneos en un entorno de telecomunicaciones;
- hacer posibles diversas estrategias de implementación y diversos grados de distribución de la funcionalidad de gestión;
- prever una estructura dividida pero compartida en la que las funciones de gestión puedan operar autónomamente dentro de cada división;
- prever posibles cambios tecnológicos y funcionales, introducir flexibilidad a la arquitectura;
- proporcionar un grado apropiado de confiabilidad en el soporte de funciones de gestión;
- proporcionar una funcionalidad de seguridad apropiada en el soporte de funciones de gestión;
- posibilitar a los clientes, proveedores de servicios de valor añadido y otras administraciones el acceso a funciones de gestión, de manera restringida y controlada;
- atender a los requisitos impuestos por un número grande o pequeño de objetos gestionados;
- posibilitar el funcionamiento cooperativo entre redes gestionadas por separado, de modo que sea posible prestar servicios entre administraciones (redes);
- hacer posible la gestión de redes híbridas constituidas por equipos de red mixtos;
- proporcionar mecanismos destinados a mantener la información necesaria para la comunicación entre sistemas (CMIP).

2.1.2 Principios para una red de gestión de las telecomunicaciones

Definición: *Las funciones de red primarias* son aquellas que directamente soportan los requerimientos del usuario (p.e. acceso a la red, intercambio de datos).

Definición: *La gestión de redes* es el acto de reinicializar, monitorear y modificar la operación de las funciones de red primarias[35].

Una red de telecomunicación consta de equipos de telecomunicaciones y considera disciplinas, medios y metodologías para comunicar a distancia. En este contexto, un servicio de telecomunicación consta de una gama de capacidades proporcionadas a los clientes que pueden ser desde servicio telefónico, Internet, videoconferencia, televisión por cable hasta enlaces privados de comunicación de diversos anchos de banda.

En el contexto de la RGT, se entiende por gestión un conjunto de capacidades que permiten el intercambio y procesamiento de información, con el fin de ayudar a las administraciones a realizar sus *funciones primarias* eficientemente [3]. El término "administración" abarca las EER (Empresa de Explotación Reconocida), las administraciones públicas y privadas (clientes y terceras partes) y/u otras organizaciones que operan o utilizan una RGT, más

aun es posible tener múltiples RGT en una administración o una única RGT establecida entre administraciones.

Una RGT proporciona funciones de gestión para redes y servicios de telecomunicación, y ofrece comunicaciones entre ella misma y las redes y servicios de telecomunicación, es decir, ofrece comunicaciones tanto entre los sistemas de operaciones (OSs), entre éstos y las diversas partes de la red de telecomunicaciones como a otras entidades de la RGT o similares.

Las RGT son redes de complejidad variable. Desde el punto de vista conceptual, es una red independiente de la de transporte, que asegura diversos puntos de interfaz con ésta para el envío/recepción de información y así realizar el control de sus operaciones. Una RGT puede utilizar partes de la red de telecomunicaciones para proporcionar sus comunicaciones, por esta razón, debe cumplir ciertos requisitos para la gestión. En la figura 1 se muestra la relación entre la RGT con la red de transporte de telecomunicaciones.

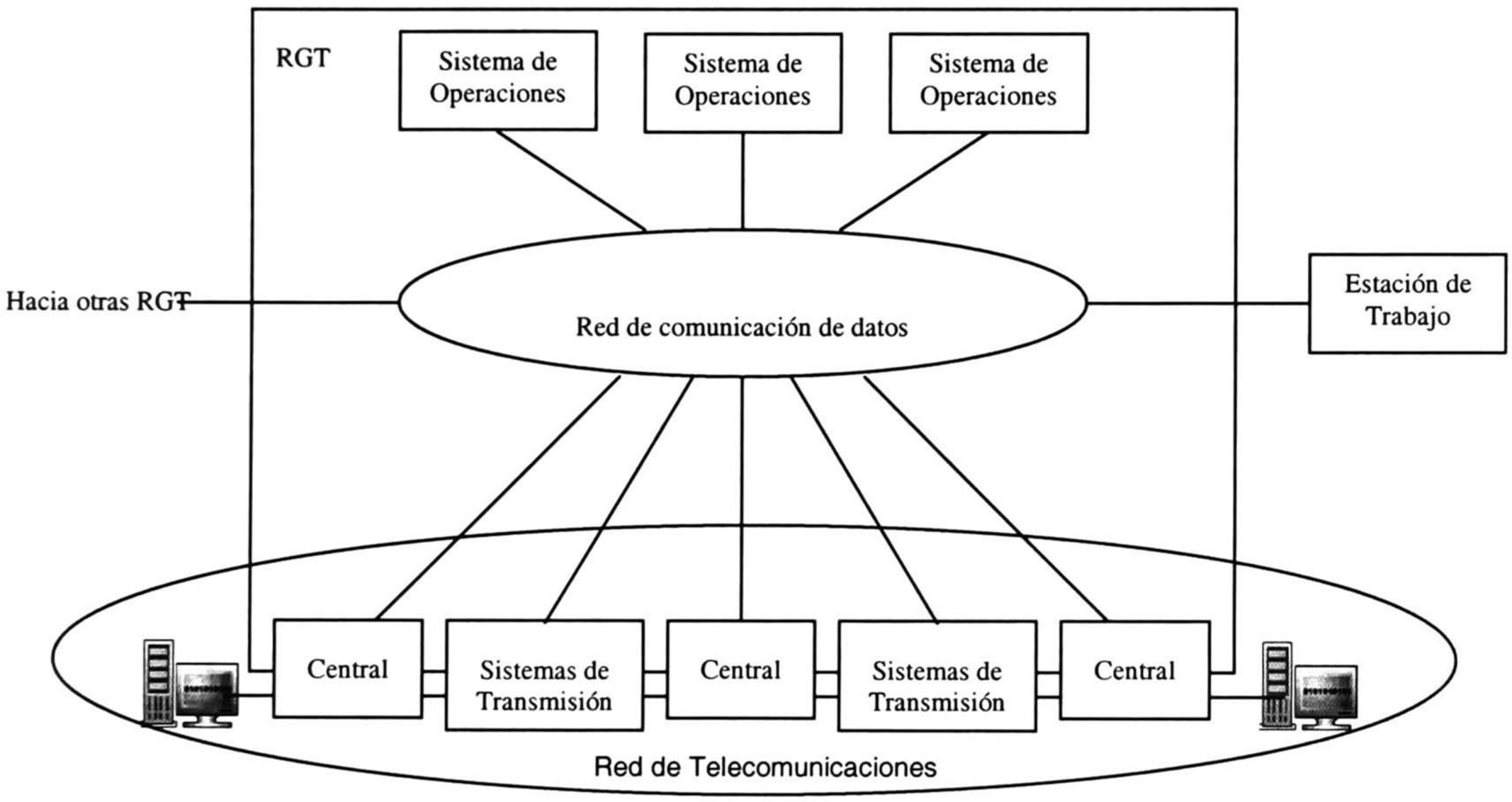


Figura 1. Relación entre la RGT con la red de telecomunicaciones

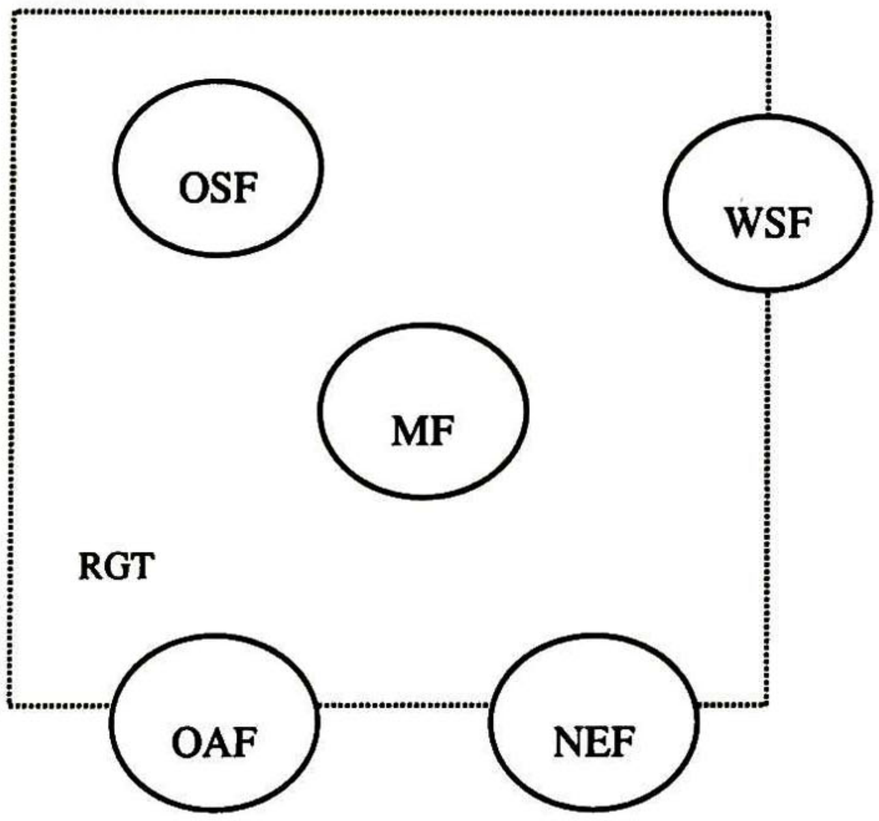
Enseguida se describen los diferentes niveles de abstracción de la arquitectura de la RGT, pero para una descripción más detallada se sugiere referirse al documento M3010 (1996) de la ITU.

2.1.3 Arquitectura funcional de la RGT

En la arquitectura funcional de RGT se definen 5 tipos diferentes de bloques. No es necesario que todos estén presentes en cada posible configuración de esta red, pero la mayoría de las RGT soportarán múltiples bloques funcionales del mismo tipo. Los cinco tipos de bloques funcionales son:

- Funciones de sistema de operación (OSF, Operating System Functions)

- Funciones de mediación (MF, Mediation Functions)
- Funciones adaptador Q (QAF, Q Adaptor Functions)
- Funciones de elemento de red (NEF, Network Element Functions)
- Funciones de estación de trabajo (WSF, Work Station Functions)



Bloques funcionales de la RGT:

OSF

MF

QAF

NEF

WSF

Figura 2. Bloques funcionales en la RGT

En la figura 2 se observa que los bloques OSF y MF se encuentran completamente dentro de la región RGT, esto significa que estos bloques se encuentran completamente especificados en las recomendaciones de RGT. Los tres bloques restantes (QAF, NEF y WSF) se encuentran en los bordes de la región y significa que solo parte de estos bloques funcionales se encuentran especificados en las recomendaciones de RGT.

Definición: Los *puntos de referencia* definen fronteras de servicio entre dos bloques de función de gestión.

Se pueden identificar cinco clases de puntos de referencia. Tres de ellos (**q, f , x**) están completamente descritos en las recomendaciones de RGT, el resto (**g, m**) se localizan fuera de la RGT y se describen solo parcialmente. La figura 3 muestra un ejemplo de los puntos de referencia y los bloques funcionales.

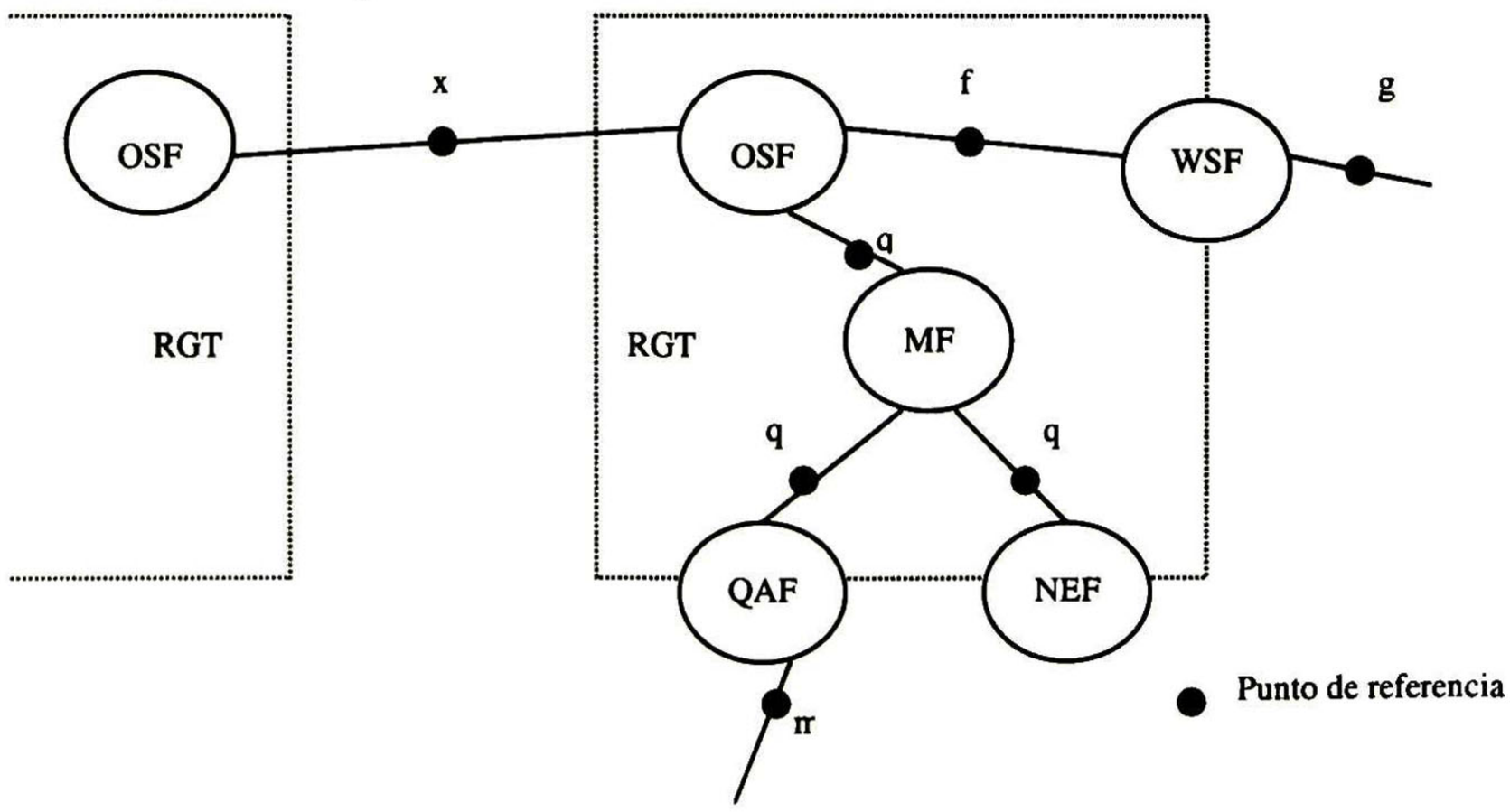


Figura 3. Ejemplo de puntos de referencia entre los bloques funcionales

2.1.3.1 Funciones de elemento de red (NEF)

Una típica red de telecomunicaciones consiste de sistemas de transmisión e intercambio de información. En la terminología de la RGT, estos sistemas son ejemplos de elementos de red (NEs), los cuales realizan funciones de elementos de red (NEFs), estas funciones incluyen:

- *Funciones primarias* (funciones de telecomunicaciones). Estas funciones son el sujeto de la gestión y soportan el intercambio de datos entre los usuarios de la red de telecomunicaciones.
- *Funciones de gestión*, las cuales permitirán al bloque NEF operar como agente.

El primer tipo de funciones no está definido por la RGT, lo cual explica que el bloque NEF se encuentra en el borde de la RGT.

2.1.3.2 Funciones del sistema de operaciones (OSF)

El bloque de funciones del sistema de operaciones inicia las operaciones de gestión y recibe notificaciones. En términos del modelo gestor – agente (manager – agent), el bloque OSF se puede ver como las funciones específicas del gestor. Un OSF se comunica con un NEF utilizando un punto de referencia $\mathbf{q_3}$ como se muestra en la figura 4.

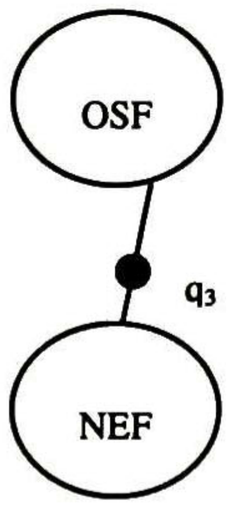


Figura 4 OSF y NEF

En la versión inicial de ésta recomendación (M.30 en 1988) define tres diferentes puntos de referencia q: $\mathbf{q_1}$, $\mathbf{q_2}$ y $\mathbf{q_3}$. El punto de referencia $\mathbf{q_3}$ es usado cuando la información de gestión debe ser intercambiada vía un protocolo de gestión de la capa de aplicación como CMIP (Common Management Information Protocol) de OSI. Los otros dos puntos de referencia se intentaron usar para casos en donde la información de gestión debe ser intercambiada vía protocolos de gestión de capas inferiores (p. e. capa de enlace de datos). Después de un tiempo parecía imposible hacer una distinción entre $\mathbf{q_1}$ y $\mathbf{q_2}$, éstos dos puntos de referencia fueron entonces reemplazados por un punto de referencia genérico $\mathbf{q_x}$.

La figura 5 muestra la relación entre NEF, OSF y $\mathbf{q_3}$ expresado en términos de servicio OSI y conceptos de protocolos.

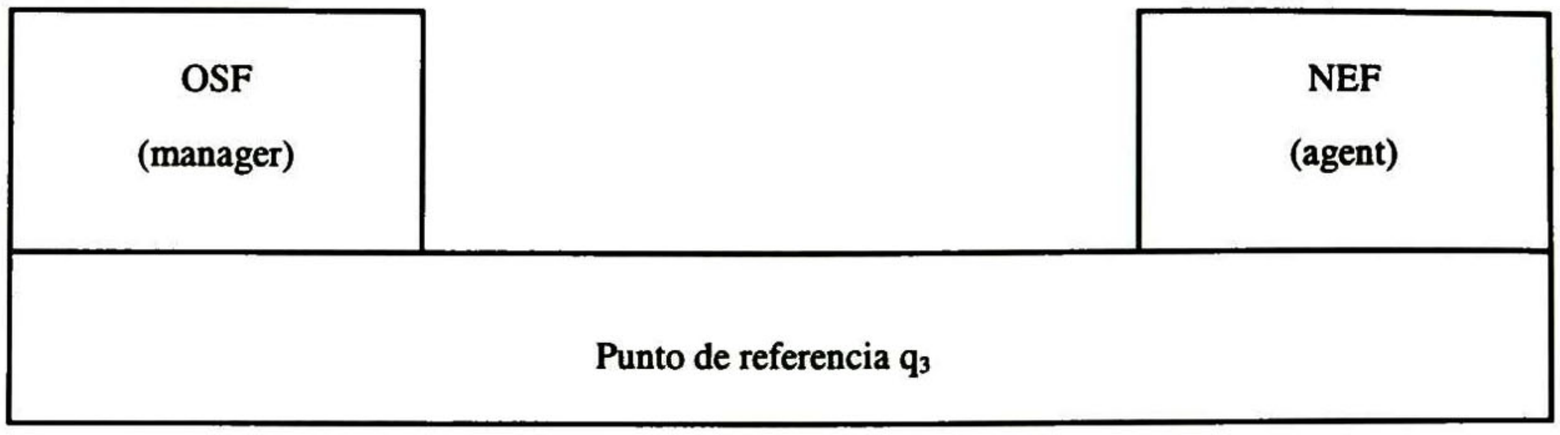


Figura 5 relación entre NEF, OSF y q_3 expresado en términos de servicio OSI

El servicio proporcionado por el punto de referencia **q_3** es generalmente el CMIS (Common Management Information Service). En una RGT, operada por una sola administración, se pueden definir múltiples OSFs y si es necesario se pueden comunicar entre ellas mediante puntos de referencia **q_3**. Es también posible que se puedan comunicar OSFs de diferentes administraciones (diferentes RGTs) utilizando los puntos de referencia **x**.

2.1.3.3 Funciones de estación de trabajo (WSF)

El bloque de *funciones de estación de trabajo* proporciona los medios para interpretar la información de la RGT para la de gestión del usuario. Las WSF proporcionan la interface al usuario utilizando el punto de referencia **g**. Tal soporte no se considera parte de la RGT, por ésta razón las WSF se localizan en el borde de la RGT con el punto de interface **g** en el exterior.

2.1.3.4 Funciones de adaptador Q (QAF)

Definición: *Un elemento de gestión RGT conforme*, es aquel que considera las especificaciones M3000 a M3599 de la ITU-T para su diseño e implementación.

El bloque de funciones de adaptador Q es usado para conectar a la RGT aquellas entidades que no soportan los puntos de referencia estándares de la RGT. En la Figura 6 se presenta un ejemplo, donde un OSF no RGT conforme y un NEF no RGT conforme están conectadas a RGT.

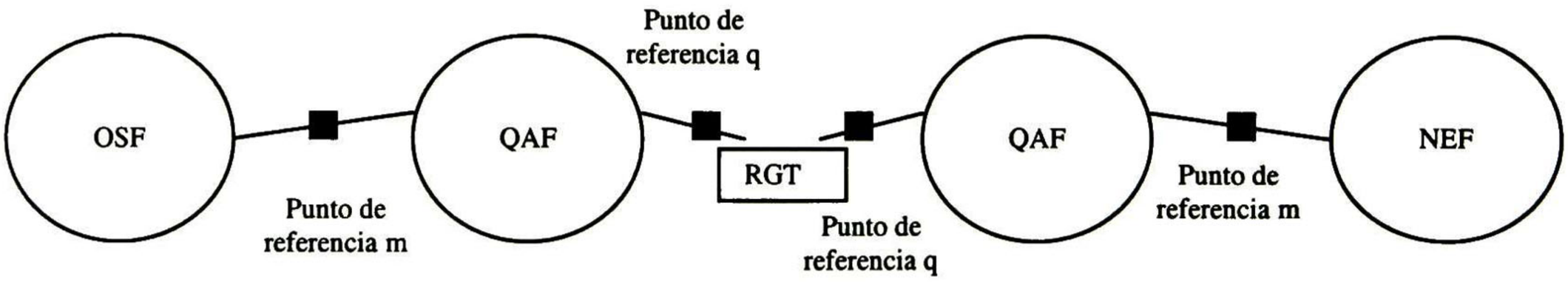


Figura 6. Funciones de adaptador Q

La responsabilidad de ambos QAF es traducir entre los puntos de referencia **q** (pertenecientes a la RGT) y los puntos de referencia **m**. Dado que los puntos de referencia son no – RGT conformes (p.e. propietarios), las QAF se encuentran en el borde de la RGT en la figura 2.

2.1.3.5 Funciones de mediación (MF)

El bloque de funciones de mediación se encuentra dentro de la RGT y transfiere la información entre NEFs o QAFs y OSFs . Un bloque MF puede ser usado para conectar uno o más NEFs y QAFs a un OSF [Figura 7]. Las MF se pueden conectar también en cascada.

Entre los tipos de MFs se encuentran aquellas que:

- Aumentan las funciones del sistema de operaciones (OSFs), por ejemplo el almacenamiento y filtrado de la información de gestión.
- Aumentan las funciones de los elementos de red (NEFs), por ejemplo la transformación de la representación local de la información de gestión a una forma estandarizada.

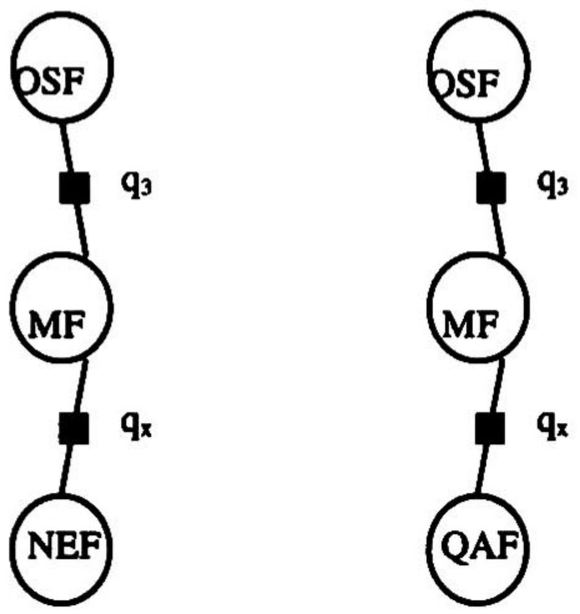


Figura 7. Relación del bloque funcional MF con OSF, NEF y QAF.

2.1.3.6 Relación entre los bloques funcionales

Un bloque funcional en la parte superior de las columnas puede intercambiar información de gestión con un bloque funcional a la izquierda de las filas con el punto de referencia en la intersección de la columna con la fila. En el caso de que la intersección esté vacía, los bloques funcionales asociados no pueden intercambiar directamente entre ellos información de gestión.

Tabla 1. Puntos de referencia que permiten la interacción entre bloques funcionales

	NEF	OSF	MF	QAF q_3	QAF q_x	WSF	No – RGT
NEF		q_3	qx				
OSF	q_3	x ,q_3	q_3	q_3		f	
MF	qx	q_3	qx		qx	f	
QAF q_3		q_3					m
QAF q_x			qx				m
WSF		f	f				g **
No – RGT				m	m	g **	

m, g son puntos de referencia que no están definidos en la RGT

* punto de referencia **x** aplica solamente cuando cada OSF se encuentra en otra RGT

* * punto de referencia **g** se ubica entre WSF y el usuario (humano).

Aparte de los bloques funcionales y los puntos de referencia, la arquitectura funcional de la RGT introduce otros conceptos:

- Funciones de comunicación de datos de las RGTs.
- Componentes funcionales de las RGTs.

De acuerdo con las recomendaciones M.3010, "las funciones de comunicación de datos de las RGTs (DCF, Data Communication Function) serán usadas por los bloques funcionales para intercambiar información. Las DCFs proporcionan las capas 1 a 3 del modelo de referencia OSI"

Cada bloque funcional de la RGT está a su vez formado de componentes funcionales y se definen los siguientes:

- Función de aplicación de gestión
- Base de información de gestión (MIB/MIT, Manage Information Base / Manage Information Tree)
- Función de conversión de información
- Adaptación hombre – máquina.
- Función de presentación.
- Función de comunicación de mensajes (MCF, Message Communication Function).

Estos componentes funcionales pueden estar divididos en dos categorías:

Los primeros cinco componentes pertenecen a la primera categoría. Estos componentes realizan las acciones de gestión y no manejan los problemas relacionados con el intercambio de información de gestión.

MCF pertenece a la segunda categoría. Este componente esta asociado con todos los bloques funcionales que requieren un servicio para el intercambio de su información de gestión. "La MCF está compuesta de un protocolo que permite la conexión de bloques funcionales con las DCFs". En muchos casos las MCF proporcionan funciones extremo a extremo, como las proporcionadas por las capas 4 a 7 del modelo de referencia OSI.

En la figura 8 se muestra la relación entre los bloques funcionales, componentes funcionales, las funciones de comunicación de mensajes (MCF) y las de comunicaciones de datos (DCF).

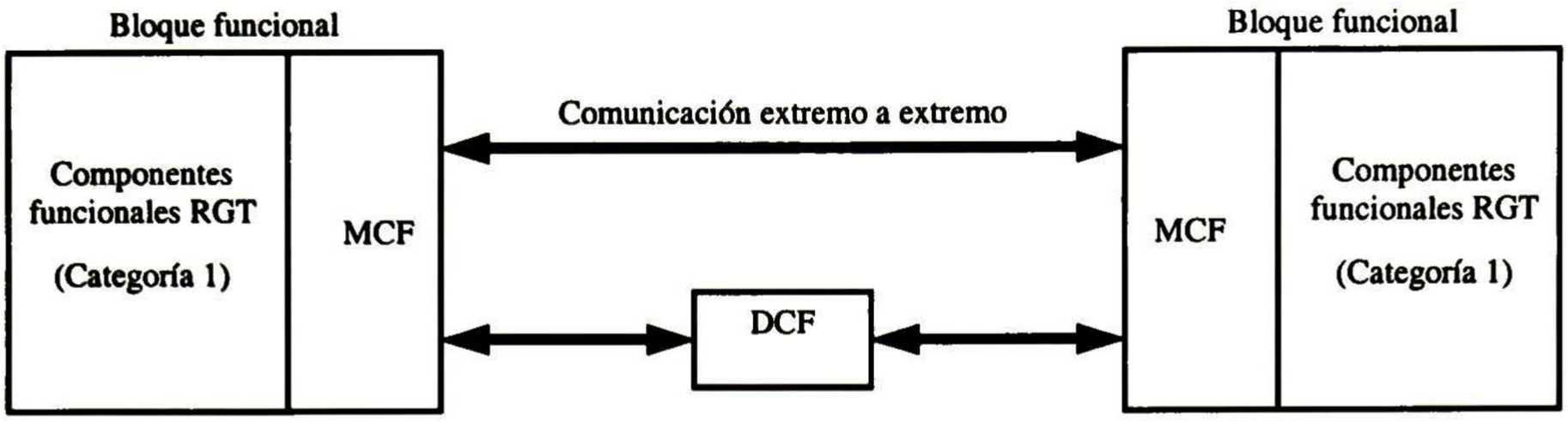


Figura 8. Elementos de comunicación entre bloques funcionales.

2.1.4 Arquitectura física de la RGT

La RGT define la arquitectura física después de la funcional. En la que se muestra como las funciones de la RGT pueden ser implementados en equipos físicos. En otras palabras, la implementación de funciones de la RGT puede tener muy diversas configuraciones físicas. La arquitectura física está definida en un nivel de abstracción inferior al de la funcional.

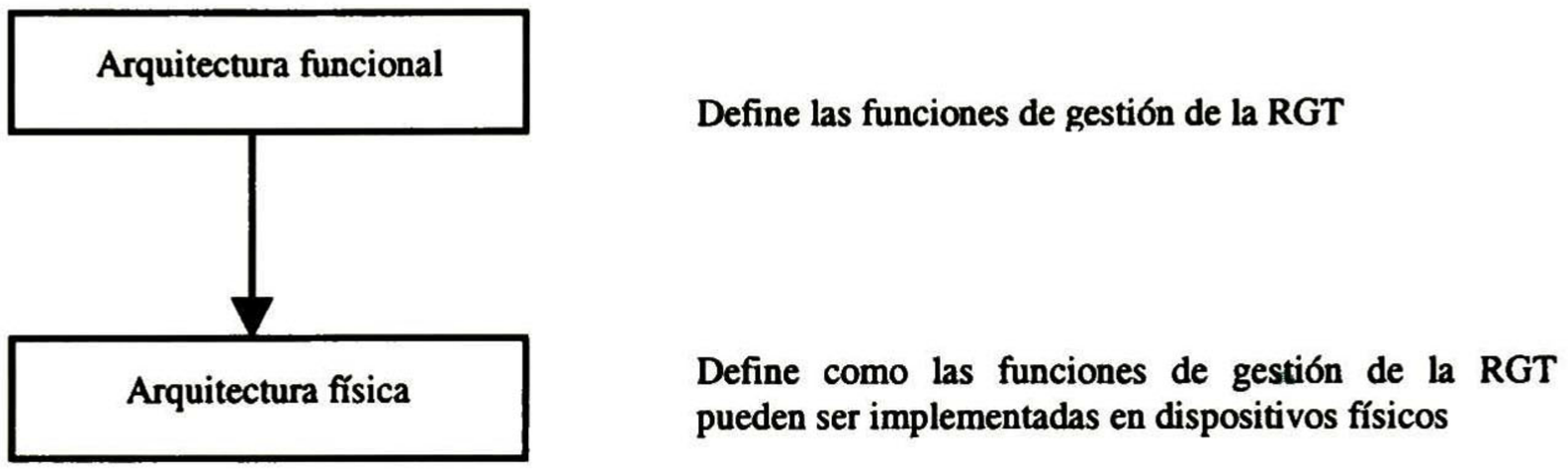


Figura 9. RGT ha definido múltiples arquitecturas relacionadas

La arquitectura física muestra como los bloques funcionales deben ser mapeados en bloques constitutivos y los puntos de referencia en interfaces, es decir, se refiere a la implementación. Se debe tomar en cuenta que un bloque funcional puede estar formado de varios componentes funcionales y un bloque constitutivo puede implementar múltiples bloques funcionales.

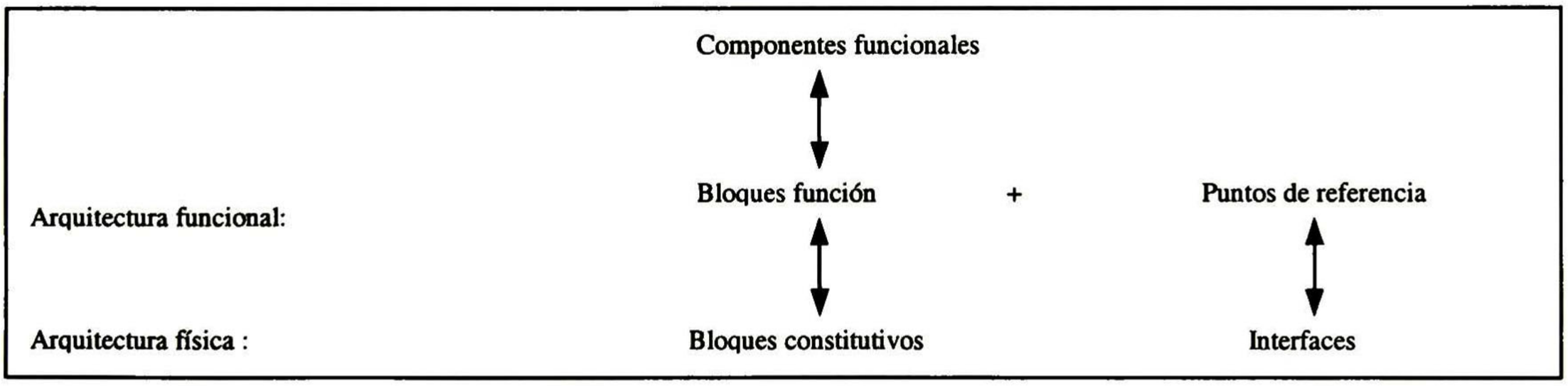


Figura 10. Relación entre arquitecturas de la RGT

Para evitar confusiones entre la arquitectura física y la funcional, se realizan las siguientes convenciones. Los nombres de puntos de referencia se escriben en minúscula y se representan como pequeños círculos rellenos y los de las interfaces en mayúscula y como círculos sin rellenar. Los bloques funcionales se muestran como círculos o elipses y los bloques constitutivos como rectángulos.

Figura 11. Convención de figuras

2.1.4.1 Bloques constitutivos

La arquitectura física de la RGT define los siguientes bloques constitutivos:

- Elemento de red (NE, Network Element).
- Dispositivo de mediación (MD, Mediation Device).
- Adaptador Q (QA, Q Adapter).
- Sistema de operación (OS, Operation System).
- Estación de trabajo (WS, Work Station).
- Red de comunicación de datos (DCN, Data Communication Network).

Los bloques constitutivos siempre implementan los funcionales del mismo nombre (por ejemplo, los elementos de red realizan las funciones de elementos de red, dispositivos de mediación realizan las funciones de mediación, etc.).

Es posible implementar múltiples bloques funcionales diferentes o del mismo tipo en un solo bloque constitutivo. El sistema de operaciones por ejemplo puede ser usado para implementar múltiples OSFs, pero también se puede usar para implementar una OSF, MF y una WSF. En el caso donde un bloque constitutivo implementa múltiples bloques función de diferentes tipos, la selección del bloque constitutivo está determinado por el uso predominante del bloque.

La Tabla 2 muestra cual bloque funcional puede ser implementado en cuales bloques constitutivos.

Tabla 2. Relación entre los bloques funcionales y los constitutivos

	NEF	MF	QAF	OSF	WSF
NE	M	O	O	O	O*
MD		M	O	O	O
QA			M		
OS		O	O	M	O
WS					M
DCN					

Una clase especial de bloque constitutivo es la red de comunicación de datos DCN (Data Communication Network), el cual no implementa ningún bloque función de la RGT. De

hecho, DCN es usado por otros bloques constitutivos para el intercambio de información de gestión, la tarea de DCN es actuar como una red de transporte.

A primera vista parece extraño que la RGT defina un bloque constitutivo que no implemente ningún bloque función. La existencia de la red de comunicación de datos se puede entender dado que en versiones anteriores de la RGT modelaban funciones de comunicación de datos (DCF, Data Communication Function) como bloque función y éstas tenían que ser implementadas por una DCN. En 1990 se decidió no modelar DCF como bloque función. Después de ésta decisión el estándar no se volvió a escribió de manera consistente y la DCN se modela como un bloque constitutivo.

2.1.4.2 Interfaces

Las interfaces se pueden ver como la implementación de los puntos de referencias. Los puntos de referencia se pueden comparar con servicios y protocolo que implementan éstos servicios.

En la mayoría de los casos los puntos de referencia y las interfaces tienen un mapeo uno a uno. No existe interfaz para aquellos puntos de referencia que:

- Cuya interconexión de bloque función está implementado dentro de un solo bloque funcional.
- Se encuentran fuera de la RGT (**g, m**). La implementación de estos puntos de referencia está fuera del alcance de la RGT.

El nombre de las interfaces es también directo: una interfaz obtiene su nombre (escrito en mayúsculas) del punto de referencia relacionado. La figura 12 muestra los posible mapeos.

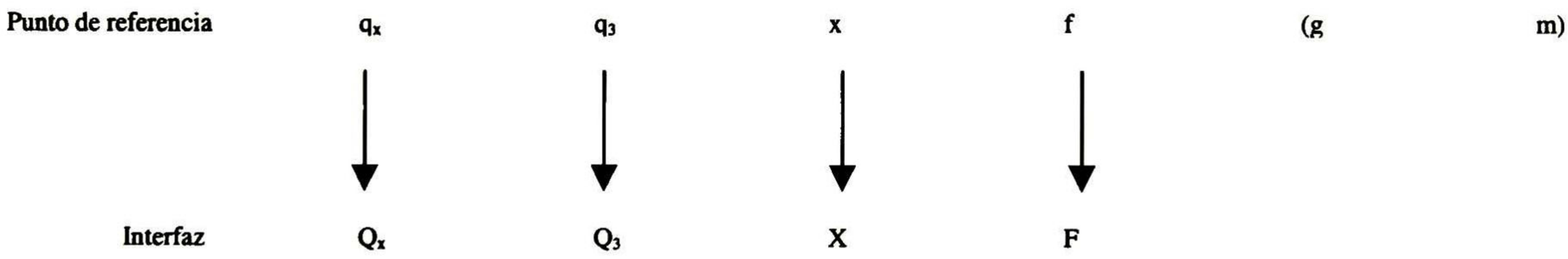


Figura 12. Mapeo de puntos de referencia a interfaces

2.1.5 Arquitectura de información

2.1.5.1 Planteamiento orientado a objeto

La arquitectura de información de la RGT utiliza una propuesta orientada a objetos y está basado en el modelo de información de gestión de OSI (CMIS/CMIP).

De acuerdo con este modelo, la gestión de un objeto es visible en la asociación del objeto mismo. En ésta asociación, la vista de gestión se describe en términos de:

- Atributos, que son propiedades o características del objeto.
- Operaciones, que son realizadas sobre el objeto.

- Comportamiento, que es exhibido en respuesta a operaciones.
- Notificaciones, que son emitidas por el objeto.

Figura 13. Objeto gestionado

2.1.5.2 Concepto de gestor – agente

La gestión de un entorno de telecomunicaciones es una aplicación de procesamiento de información. Debido a que el entorno sujeto a gestión es distribuido, la gestión de red es una *aplicación distribuida.*

Definición: un sistema gestor, es parte de una aplicación distribuida que tiene la función de enviar directivas de operación de gestión a uno o más agentes y recibir notificaciones de éstos.

Definición: sistema gestionado es aquel que cuenta con un *agente*.

Definición: el agente es parte de los procesos de aplicación que maneja los *objetos gestionados* asociados (p.e. interfaces, protocolos, ancho de banda, memoria). La tarea del agente es la de responder a las directrices expedidas por un gestor y reflejarán hacia éste una visión de estos objetos y emitirá notificaciones que reflejen el comportamiento de dichos objetos.

En la Figura 14 se muestra la relación existente entre gestor, agente y objetos gestionados.

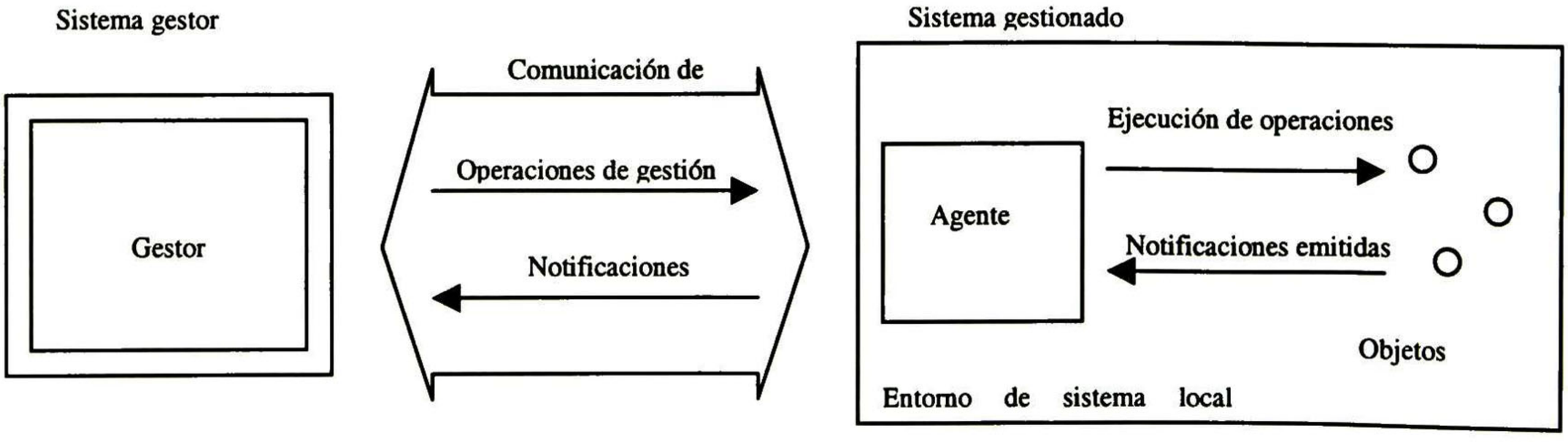


Figura 14. Relación gestor, agente y objetos gestionados

Es importante señalar que normalmente existirá una relación muchos a muchos entre gestores y agentes, es decir, un gestor puede estar involucrado en un intercambio de

información con varios agentes y viceversa. Un agente denegará directrices de un gestor por diversas razones como seguridad o coherencia del modelo de información.

La información, que puede ser transferida o afectada al utilizar protocolos de gestión OSI (CMIS/CMIP), es un conjunto de objetos gestionados denominado *base de información de gestión* (MIB, Management Information Base, MIT Management Information Tree).

2.1.6 Arquitectura lógica estratificada de la RGT

La RGT reconoce la existencia de una jerarquía de responsabilidades de gestión. Tal jerarquía se puede describir en términos de capas de gestión y una arquitectura lógica estratificada que las describe. Las ideas detrás de ésta arquitectura fueron descritas en 1989 por Boyd y Brodrick [25] como parte de su ONA (Open Network Architecture).

Para manejar la complejidad, la funcionalidad de la gestión con su información correspondiente, puede ser descompuesta en varias capas lógicas. El principio de tal estratificación se muestra en la figura 15.

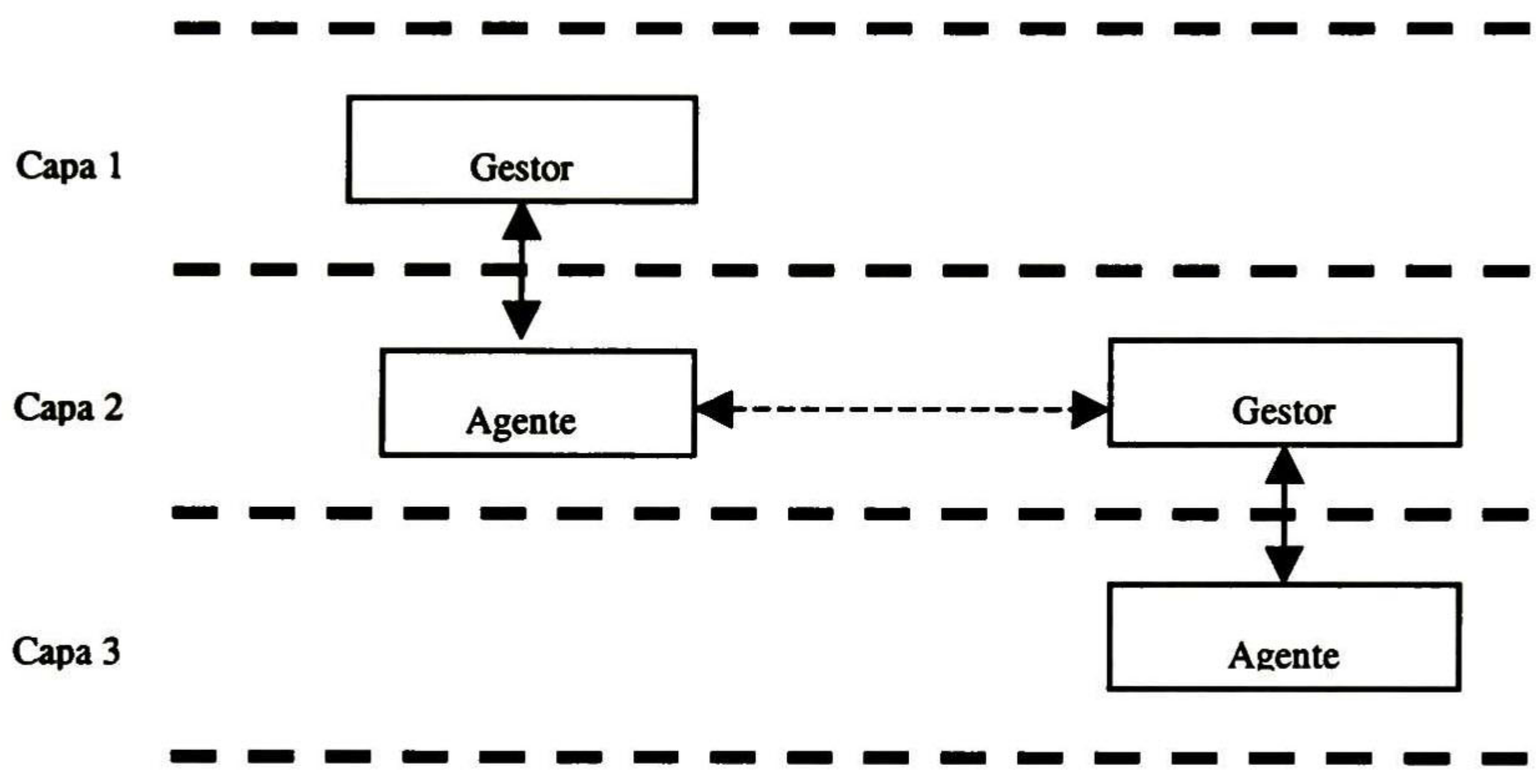


Figura 15. Descomposición de la funcionalidad de gestión

En la frontera entre la capa 1 y la capa 2 la vista de gestión de la capa 2 se presenta a la capa 1 como información contenida en el agente en la capa 2. Es importante notar que la vista de gestión presentada a la capa 1 no necesita revelar detalles de la capa 2; el agente en la capa 2 proporcionará solamente información necesaria en la capa 1. Este principio de estratificación puede ser usado de manera recursiva, es decir, la información de la capa 3 presentada a la capa 2, etc.

Una descomposición de la funcionalidad de gestión es la siguiente:

- capa de gestión de elementos
- capa de gestión de red
- capa de gestión de servicio
- capa de gestión empresarial

Estas capas sus bloques función y sus puntos de referencia se muestran en la figura 16.

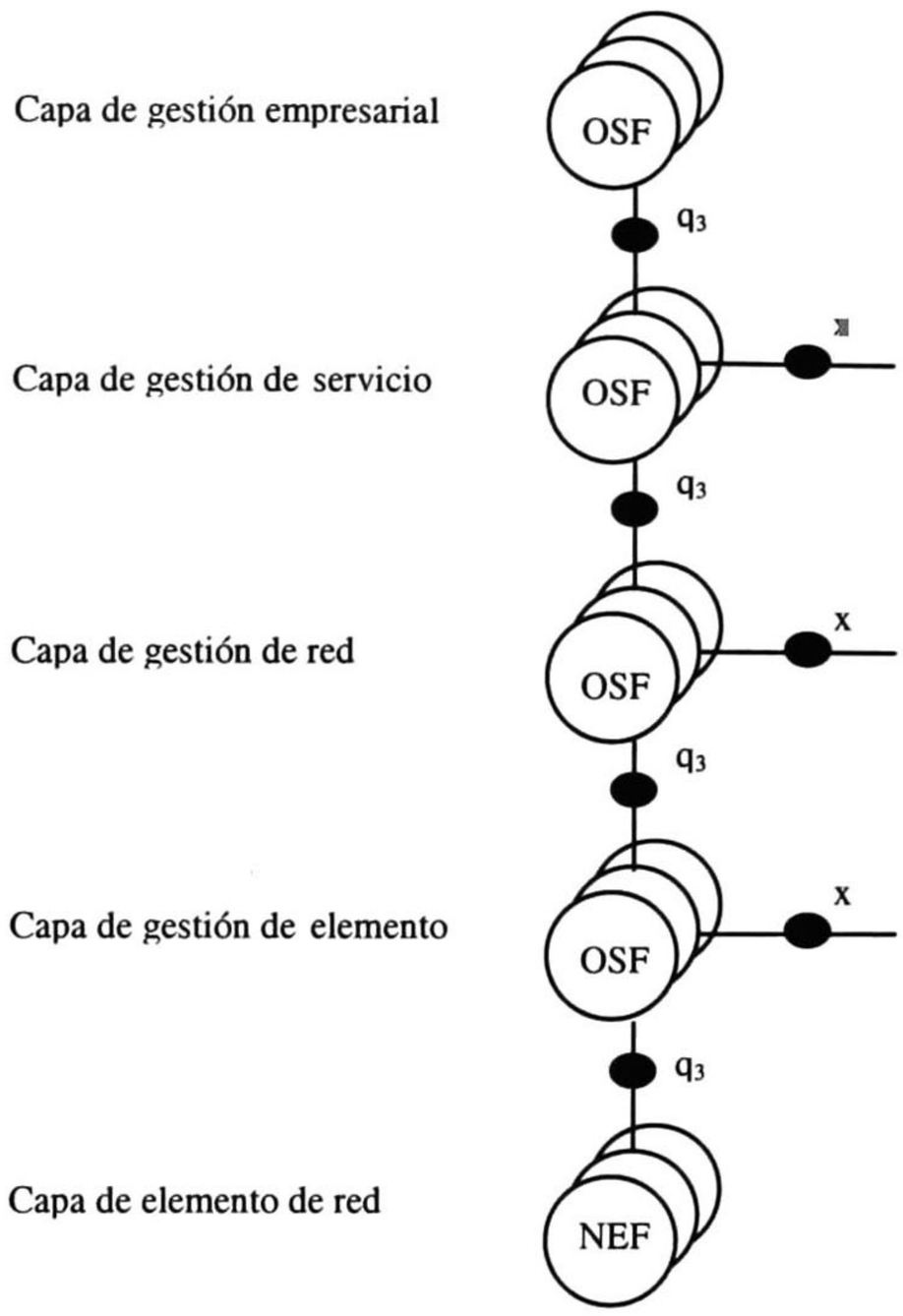


Figura 16. Arquitectura lógica estratificada de la RGT

2.1.6.1 Capa de gestión de elementos

Las funciones de los elementos de red individuales son gestionadas por las funciones de sistemas de operaciones en la capa de gestión de elemento. Esta capa trata con las funciones de gestión específicas de diversos proveedores de equipo y oculta estas funciones a las capas superiores como la capa de gestión de red.

Ejemplos de funciones ejecutadas en la capa de gestión de elemento son:

- detectar errores de equipo,
- medir el consumo de energía,
- medir la temperatura del equipo,
- medir los recursos utilizados como tiempo CPU, espacio en buffer, etc.,
- registrar datos estadísticos,
- actualizar firmware.

2.1.6.2 Capa de gestión de red

La responsabilidad de la capa de gestión de elemento es la de gestionar las NEFs implementadas en equipos de manera aislada, la responsabilidad de la capa de gestión de red es gestionar las funciones relacionadas a la interacción entre múltiples equipos. En la capa de gestión de red la estructura interna de los elementos de red no es visible, es decir, el

espacio de buffer en los ruteadores, la temperatura de los switches, etc., no puede ser directamente gestionada en éste nivel.

Los siguientes son ejemplos de funciones ejecutadas en esta capa:

- creación de una vista completa de la red,
- creación de caminos dedicados en la red para soportar la calidad de servicio (QoS) que demanda el usuario final,
- modificación de tablas de ruteo,
- monitoreo de la utilización del enlace,
- optimización el desempeño de la red y
- detección de fallas.

Las OSFs en la capa de gestión de red utilizan la información de gestión independiente del proveedor, que es proporcionada por las OSFs de la capa de gestión de elemento. En ésta interacción la capa de gestión de red actúa en un papel de gestor y la capa de gestión de elemento en un papel de agente.

2.1.6.3 Capa de gestión de servicio

La capa de gestión de servicio se dedica a la gestión de aquellos aspectos que pueden ser observados por el usuario de la red de telecomunicaciones. Estos usuarios pueden ser usuarios finales (clientes) u otros proveedores de servicios (administraciones). La gestión de servicio se construye sobre la información de gestión que proporciona la capa de gestión de red, pero no ve la estructura interna de la red.

Ejemplos de funciones ejecutadas en la capa de gestión de servicio son:

- gestión de la calidad del servicio (QoS, retardos, pérdidas, etc.),
- contabilidad y facturación,
- añadir o eliminar usuarios,
- asignación de direcciones,
- mantenimiento de direcciones de grupo.

La noción de la gestión de servicio es una valiosa contribución de la RGT y otros marcos de gestión como la de Internet (IETF) puede tomar ventaja de ésta idea y extender su gestión.

2.1.6.4 Ejemplos de gestión de servicios

A continuación se exponen algunos casos donde la gestión de servicio puede ser útil.

En el caso en el que dos operadores intercambian información de gestión para gestionar sus redes interconectadas (inter – operator management). Por razones comerciales y de seguridad cada operador tratará de ocultar la estructura interna de su red del otro solamente

aquella información de gestión que absolutamente necesaria intercambiar estará disponible para ser intercambiada.

Otro caso es donde un operador, que proporciona servicios de transporte de extremo a extremo, usa la red de otro operador para conectar sus elementos de red. Un ejemplo típico es un proveedor de servicio IP, que usa enlaces ATM (SDH o DWDM) de otro operador para conectar sus ruteadores. Este caso se muestra en la figura 17.

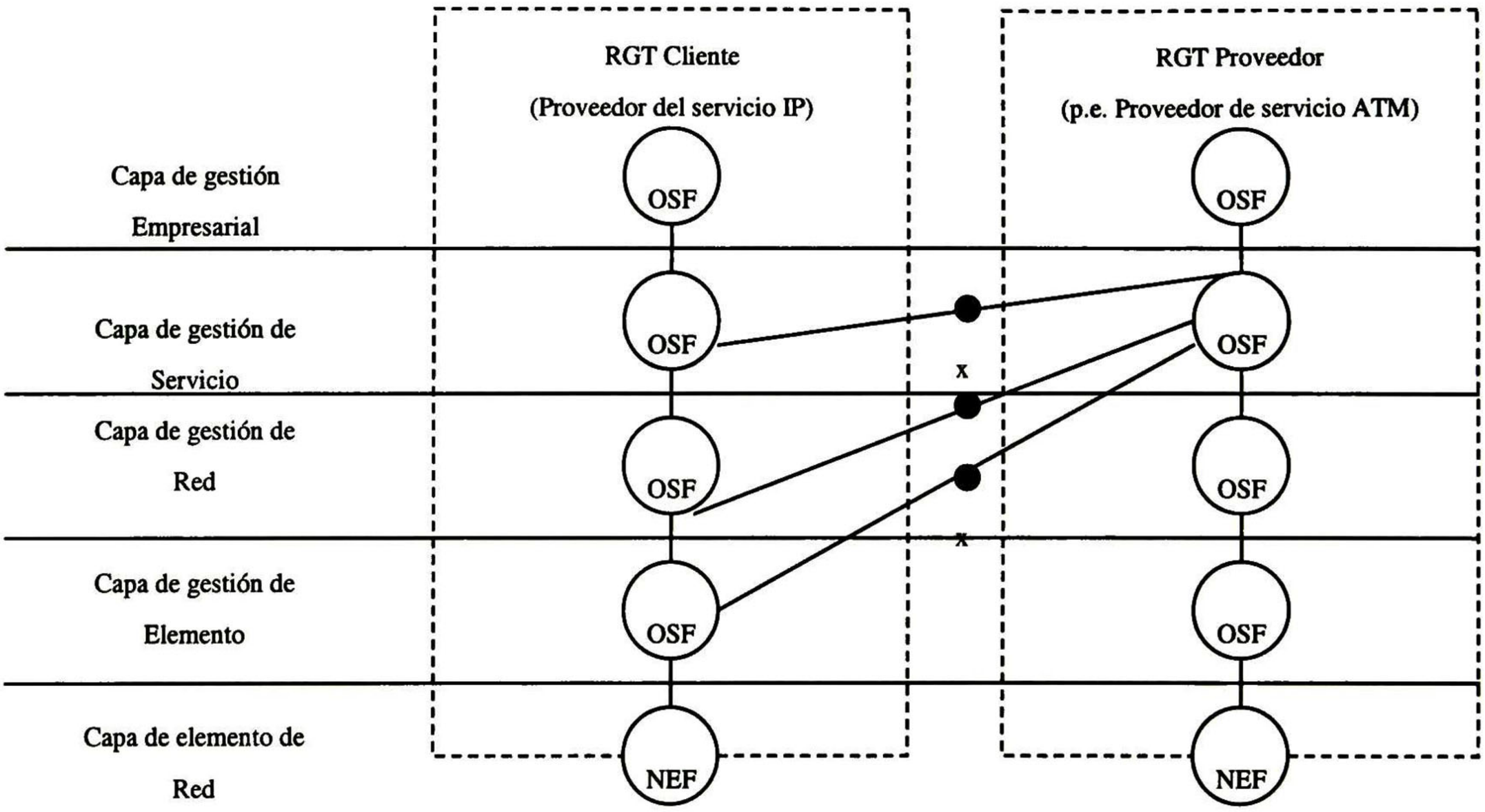


Figura 17. Ejemplo de proveedor de servicio IP que usa enlaces ATM

En el lado del proveedor de servicio ATM todos los puntos de referencia **x** están conectados a las OSFs de la capa de gestión de servicio, ya que el proveedor de servicio ATM no permitirá a la otra administración monitorear y modificar su red ATM; solo información de alto nivel será disponible al proveedor de servicio IP. Para el proveedor de servicio IP el enlace ATM será visto como un solo elemento en la red IP. En el caso de que el proveedor de servicio IP tuviera la opción de elegir ruta alternativas para el enlace ATM, existiría un punto de referencia en la capa de gestión de red. Finalmente el desempeño del enlace ATM tiene un impacto en QoS de la red IP esa es la razón del punto de referencia a la capa de gestión de servicio.

Un tercer caso es el de los servicios de valor agregado (VAS, Value Added Service). En este caso se puede usar una OSF para la gestión del VAS y otra OSF puede ser responsable de la gestión de la red de telecomunicaciones que se debe cruzar para usar el servicio. Ambas OSFs se deben comunicar entre sí. Si las OSFs pertenecen a la misma RGT (Administración), la comunicación se realiza mediante puntos de referencia **q** y si pertenecen a diferentes RGT se usará un punto de referencia **x**, como se muestra en la figura 18.

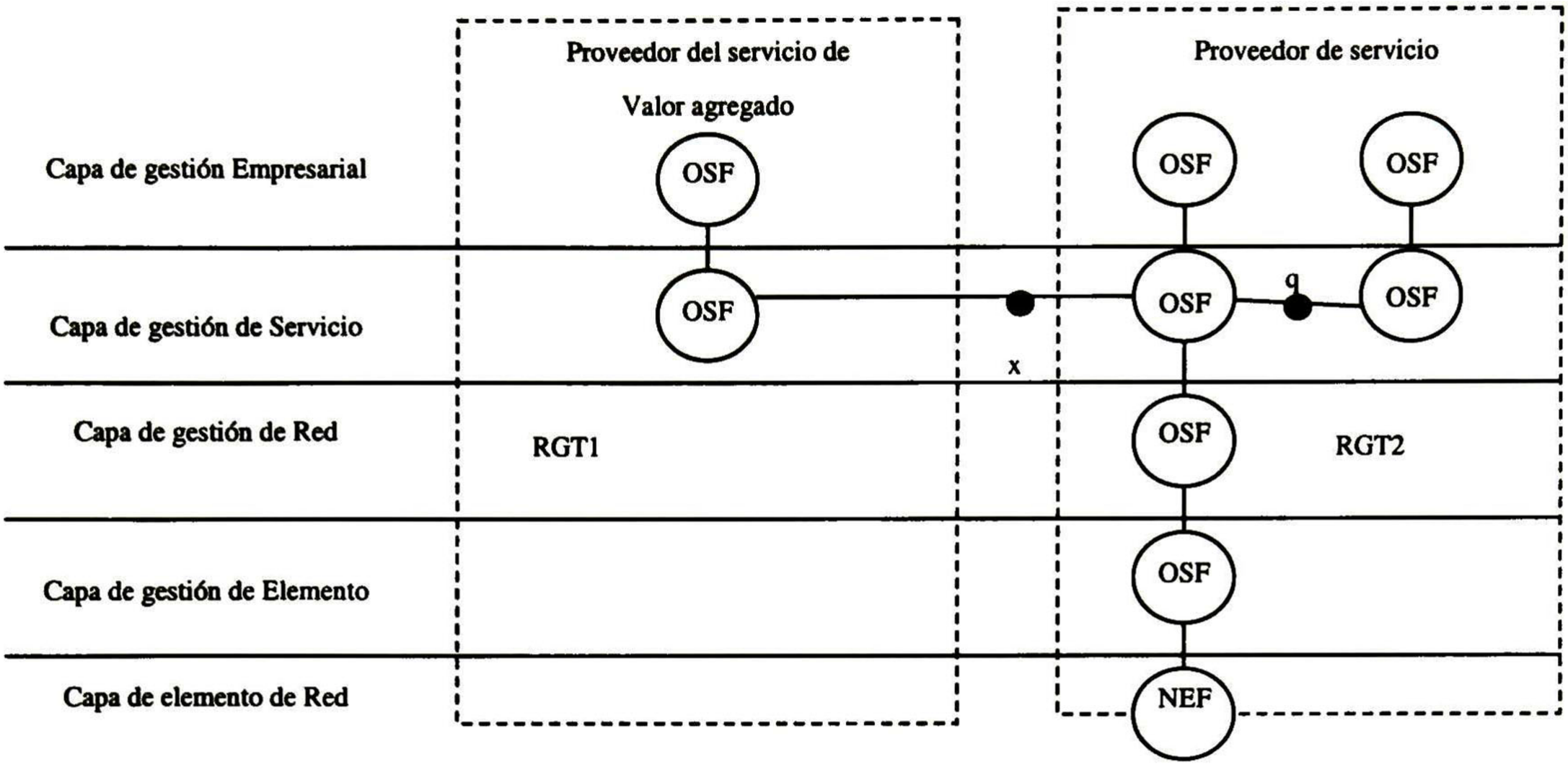


Figura 18. Ejemplo de servicios de valor agregado

2.1.6.5 Capa de gestión empresarial

La capa empresarial es responsable para la gestión de toda la empresa. Esta tiene un alcance muy amplio, donde la gestión de las comunicaciones es sólo una parte de las tareas que debe realizar. Esta capa se puede ver más como el hecho de fijar objetivos sin tomar en cuenta como alcanzarlos, es decir, la capa empresarial se relaciona mejor con la planeación estratégica y táctica, y no tanto con la operacional, como los otros estratos de gestión de la RGT.

2.1.7 Relación con otras propuestas de gestión

Aunque la recomendación M.3010 no hace ninguna referencia a la gestión de Internet (IETF) ni a su protocolo SNMP, es posible explicar la relación entre RGT y SNMP.

Existe una relación estrecha entre RGT y la gestión de OSI. La arquitectura funcional de la RGT, definida en términos de bloques función y puntos de referencia, puede ser explicada en términos de conceptos OSI. Los bloques función contienen componentes funcionales (funciones de presentación o MIBs), comparables a entidades de protocolo OSI. Los puntos de referencia son utilizados para interconectar bloques función, los cuales en terminología OSI son comparables a los subyacentes proveedores de servicios, como es muestra en la Figura 19.

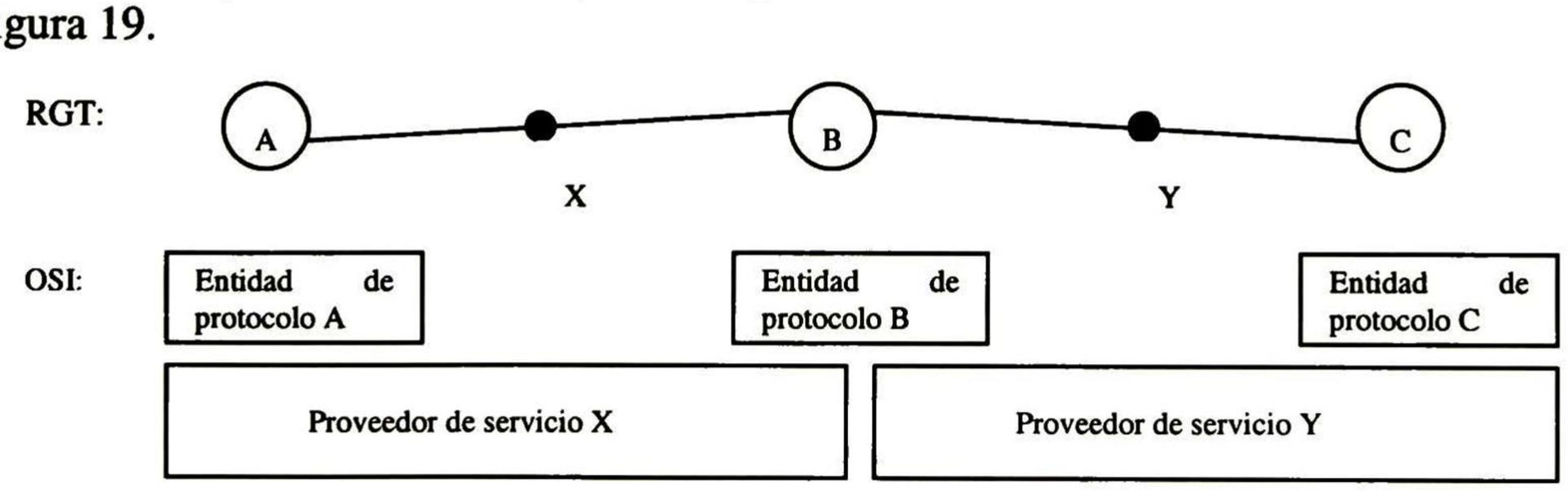


Figura 19. Relación entre los conceptos RGT y OSI

La RGT maneja conceptos que pueden ser importantes para la comunidad de gestión de Internet (IETF).

2.1.8 RGT y la gestión de IETF (Internet)

Una diferencia importante entre la RGT y la gestión de IETF es que la primera se concentra en la especificación de arquitecturas de gestión y la segunda en la implementación de protocolos de gestión. Como resultado existe un número limitado de productos RGT en el mercado y existe una gran cantidad de productos comerciales y públicos con la propuesta de gestión de la IETF. Es hasta la versión 3 de SNMP en la que se introduce una arquitectura modular que comparándola con la RGT permanece simple.

La integración entre RGT y SNMP ha sido un tópico de investigación. Esta integración se obtiene mediante QAF (Función de adaptador Q). La QAF traduce entre el punto de referencia $\mathbf{q_3}$, el cual es implementado como un protocolo de gestión OSI (CMIP) y el punto de referencia **m**, el cual es implementado como una pila de protocolo SNMP. La tarea más crítica de la QAF es la traducción del modelo de información de la RGT, la cual usa las directrices para la definición de objetos gestionados de OSI (GDMO, Guidelines for the definition of managed objects) y la estructura de la información de gestión (SMI, Structure of Managed Information) de IETF.

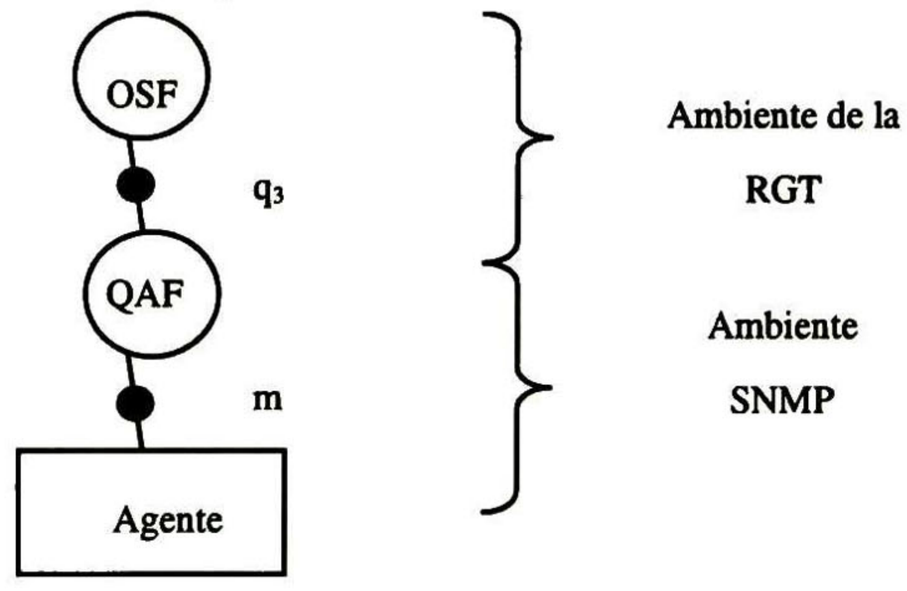


Figura 20. Integración de RGT con SNMP

La RGT sugiere una separación conceptual entre la red que está siendo gestionada y la red que transfiere la información de gestión. Por otra parte IETF no hace ésta distinción.

Probablemente el concepto más valioso de la RGT es el de la arquitectura lógica estratificada donde se distinguen gestiones de: *elemento, red, servicio y empresa*. La gestión de la IETF se ha enfocado en la gestión de elemento y red, pero necesita extenderse en la gestión de servicio para permitir el intercambio de información de gestión entre diferentes operadores y entre clientes y operador.

2.1.9 La RGT y la propuesta de gestión OSI

La cooperación de grupos de CCITT y ISO/IEC ha dado como resultado la incorporación de muchas ideas de gestión de OSI a la RGT, los cambios más importantes de la RGT en el documento M.30 hasta el M.3010 más reciente son:

- El concepto gestor – agente, desarrollado originalmente por OSI.
- La propuesta orientada a objetos de la OSI también fue copiada.

- La idea de dominios de gestión fue incluida.

A pesar de la cooperación de la ITU-T y grupos de gestión de OSI, existen aún diferencias:

OSI ha definido una sola arquitectura de gestión, mientras que la RGT define múltiples arquitecturas en diferentes niveles de abstracción.

La RGT define una arquitectura lógica estratificada para los múltiples niveles de responsabilidad de gestión que existe en las redes reales, mientras que OSI no proporciona tal estructura.

La ITU opuesto a OSI sugiere una separación conceptual entre la red gestionada y la red de gestión, la que transmite la información de gestión.

2.2 Funciones de gestión

En lo referente a las funciones de gestión de la RGT el documento M.3020 define lo que es una función de gestión y las directrices para la definición de funciones de gestión. El documento M.3400 define las 5 áreas funcionales de la RGT.

Las funciones de gestión son interacciones cooperativas entre procesos de aplicación en los sistemas gestores y gestionados, para la gestión de los recursos de telecomunicaciones. "Los conjuntos de funciones de gestión de la RGT se describen desde el punto de vista de los usuarios de la RGT y son independientes de los protocolos individuales y del modelado de la información de gestión"[M.3400][4].

2.2.1 Gestión de calidad de funcionamiento

Esta gestión involucra un conjunto de funciones para evaluar el comportamiento de los dispositivos y equipos de telecomunicaciones en relación con la efectividad de la red e informar al respecto. La meta de ésta gestión es supervisar y corregir la efectividad de la red y facilitar la planificación, provisión, mantenimiento y la evaluación de la calidad.

La *gestión de la calidad del funcionamiento* comprende los siguientes grupos de funciones:

1. *Garantía de la calidad de funcionamiento*; son procesos de decisión que establecen medidas de calidad apropiadas al área de gestión de la calidad de funcionamiento. Ejemplos de éstos procesos son; establecer objetivos de la calidad del servicio, objetivos de la calidad del funcionamiento de la red, criterios de calidad de servicio al abonado, etc.

2. *Supervisión de la calidad de funcionamiento* (PM, Performance monitoring); implica la recolección continua de datos sobre la calidad del funcionamiento de los elementos de red. Las condiciones de falla grave son detectadas por los métodos de vigilancia de alarmas, pero las condiciones de error de escasa frecuencia o intermitentes pueden provocar la degradación de la calidad de servicio y no detectadas por la vigilancia de alarmas. Se hace uso de parámetros supervisados para detectar las tendencias antes de que PM descienda por debajo de un nivel aceptable. Algunos procesos relacionados con PM son, políticas de supervisión de PM, correlación y filtrado de eventos de supervisión de PM, acceso a información para pronóstico y situación del tráfico.

3. *Control de la gestión de la calidad de funcionamiento*; se relaciona a la transferencia de la información para controlar el funcionamiento de la red en el área de gestión de la calidad de funcionamiento. Ejemplos de éstas funciones son, políticas de gestión del tráfico de la red, funciones de control del tráfico, funciones de administración del tráfico, etc.

4. *Análisis de la calidad de funcionamiento*; todos los datos de la calidad de funcionamiento son procesados y analizados para evaluar el nivel de calidad de funcionamiento de la entidad. Algunos ejemplos de funciones para analizar la calidad de funcionamiento son; políticas de umbrales de excepción y recomendaciones para la calidad de funcionamiento, previsión del tráfico, análisis de la capacidad de tráfico, etc. Mediante la gestión de la calidad de funcionamiento se puede asegurar que la red tiene la capacidad de cumplir con las necesidades de los usuarios.

2.2.2 Gestión de fallas

La gestión de fallas es un conjunto de procesos para localizar problemas, o fallas en la red de telecomunicaciones e involucra los pasos de descubrir el problema, aislarlo para posteriormente arreglarlo.

La evaluación de la protección de la calidad del servicio para la gestión de fallas involucra mediciones de los componentes de confiabilidad, disponibilidad y supervivencia (RAS).

La gestión de fallas comprende los siguientes conjuntos de funciones:

1. *Garantía de la calidad de RAS*; establece criterios de confiabilidad que orientan las políticas de diseño de equipos redundantes y otras como; fijar objetivos RAS de la red, fijar objetivos de disponibilidad de servicio, evaluación de RAS, notificación de interrupción de servicio.

2. *Vigilancia de alarmas*; cuando se produce un fallo en la red los elementos de red involucrados envían las indicaciones necesarias para que la RGT determine la naturaleza y la gravedad. La información referente a la alarma puede comunicar en el momento mismo de la ocurrencia y/o se puede registrar para una consulta futura. Algunas funciones relacionadas a la vigilancia de alarmas son; política de alarmas, señalamiento de alarmas, criterios de eventos de alarma, gestión de indicaciones de alarma, etc. Para que la RGT efectúe la vigilancia de alarmas, los NEs deberán permitir:

   - Supervisar las condiciones de alarma casi en tiempo real o con arreglo a un plan.
   - La consulta de las condiciones de alarma existentes en el NE.
   - El registro y recuperación del historial de información sobre alarmas.

3. *Localización de fallas o averías*; cuando la información inicial sobre la falla sea insuficiente para localizarla, será necesario usar programas que realicen ésta tarea. Estos programas pueden emplear sistemas de prueba internos o externos o pueden ser controlados por una RGT. Ejemplos de estas funciones son; política de localización de fallas, verificación de parámetros y conectividad, localización de fallas de la red, localización de fallas en los elementos de red (NE), realización de diagnóstico.

4. *Reparación de averías*; la cual se encarga de transferir datos relativos a la reparación de una falla y para controlar los procedimientos que usan recursos redundantes para remplazar equipos o facilidades que hayan fallado. La reparación de averías comprende funciones como; gestión del proceso de reparación, acuerdo de reparación con el cliente, restablecimiento automático, reparación de fallas de NE, despacho del personal de reparación.

5. *Pruebas*; se pueden realizar de dos formas, una es cuando la RGT indica a un NE que realice pruebas sobre el mismo (análisis de características de circuitos o equipos, procesamiento que se ejecuta internamente en el NE) y los resultados son comunicados a la RGT inmediatamente o con un retardo. La otra forma de realizar pruebas es hacer el análisis dentro de la RGT, en cuyo caso la RGT solamente pide a los NEs que aseguren el acceso al circuito o equipo a probar. Ejemplos de funciones de pruebas son, política de puntos de prueba, prueba de servicio, selección de circuitos, correlación de pruebas y localización de averías, control de prueba de NE, informe de resultados y situaciones.

6. *Administración de anomalías*; se encarga de transferir los informes de anomalías producidas por los clientes y las anomalías producidas por las pruebas dinámicas de detección de fallos. Se encarga de las acciones para investigar y eliminar anomalías. Ejemplos de estas funciones son; política de informe de anomalías, señalamiento de anomalías, indagación de información sobre anomalías, etc.

2.2.3 Gestión de la configuración

La gestión de la configuración provee las funciones necesarias para identificar, controlar, recolectar y proporcionar información a los NEs.

Los grupos de funciones relacionadas a la gestión de configuración son:

1. *Planificación e ingeniería de la red*; se refiere a las funciones asociadas con la determinación de la necesidad de aumentar la capacidad de la red y la introducción de nuevas tecnologías. Esto implica la evaluación de diversos planes y los seleccionados serán implementados por las funciones de aprovisionamiento. Funciones relacionadas a la planificación e ingeniería de la red son; presupuesto de línea de producto, política sobre tecnología y proveedores, planificación de infraestructura, gestión de planificación y del proceso de ingeniería, etc.

2. *Instalación*; se refiere a la instalación de los equipos y software (NEs) que forman parte de la red de telecomunicaciones tanto para ampliar o reducir la infraestructura o sistema. Algunas funciones relacionadas son; adquisiciones, gestión de instalación, contratación, acuerdo de instalación con el cliente, administración de las instalaciones de la red, gestión del material, instalación de elementos de red, etc.

3. *Planificación y negociación de servicios*; se refiere a la planificación de la introducción de nuevos servicios, cambiar características de servicios y desconectar servicios. Funciones relacionadas son; planificación de servicios, definición de características de servicios, funciones de mercadeo, gestión del proceso de ventas, planificación del servicio al cliente, etc.

4. *Provisión*; consiste de un conjunto de procedimientos para poner en servicio un equipo sin contar la instalación. La inicialización y estado del nuevo equipo se controla mediante funciones de provisión. Algunas funciones de provisión son; funciones de política de provisión, política de gestión del material, petición de servicio, diseño de circuito entre centrales, diseño de facilidad, gestión de conexión de red, etc.

5. *Situación y control*; se refiere a la capacidad para supervisar y controlar determinados aspectos de los NEs (servicio, fuera de servicio, reserva activa, pruebas de diagnóstico). Las aplicaciones de éstas funciones son; mantenimiento rutinario (ejecutan automáticamente o periódicamente), para retirar de funcionamiento algún equipo averiado y reenrutar el tráfico, para introducir una configuración propuesta para analizar su viabilidad antes de implementarla. Algunas funciones relacionadas son; política de servicios prioritarios, restablecimiento de servicios prioritarios, situación de red de circuitos arrendados, situación de red de transporte, situación y control de elementos de red, etc.

2.2.4 Gestión de seguridad

La gestión de seguridad comprende los servicios que aseguran las comunicaciones y el manejo de los dispositivos gestionados contra intrusos mediante la detección y notificación de eventos de seguridad (usuario no autorizado, manipulación indebida del equipo, etc.). La gestión de seguridad comprende el siguiente grupo de funciones:

1. *Prevención*: son funciones necesarias para evitar una intrusión. Ejemplos de éstas funciones son; seguridad de acceso físico, análisis del riesgo con el personal.

2. *Detección*: son funciones necesarias para detectar una intrusión. Algunas funciones relacionadas son; alarma de seguridad del cliente, perfiles del cliente, investigación de robo del servicio, alarmas de seguridad de la red, etc.

3. *Contenencia y recuperación:* son funciones necesarias para denegar el acceso a un intruso, repara los daños causados por el intruso. Funciones relacionadas a éste grupo son; protección de almacenamiento de datos empresariales, acciones por informe de excepción, recuperación del servicio tras una intrusión, administración de la lista de revocaciones de la red, etc.

4. *Administración de la seguridad*: son funciones necesarias para planificar y administrar las políticas de seguridad y gestionar la información relacionada con la seguridad. Algunas funciones relacionadas a éste grupo son; política de seguridad, planificación de la recuperación tras un desastre, gestión de dispositivos de seguridad, pistas de verificación, análisis de alarmas de seguridad, etc.

La gestión de seguridad controla el acceso a la información de la red, protege a la red y al sistema de gestión contra acciones accidentales o intencionales que puedan provocar daños. Los mecanismos de seguridad deben de ser flexibles para contemplar rangos de privilegios de control y búsqueda y definir modos de acceso ya sea por OS, grupos o por perfiles de usuario.

2.2.5 Gestión de contabilidad

Esta gestión se encarga de los procesos de tarificación por la utilización de los recursos de la red de forma individual o por grupos de usuarios por los servicios que la red de telecomunicaciones proporciona. La gestión de contabilidad comprende el siguiente grupo de funciones:

1. *Medición de utilización*; ésta se refiere a recolectar datos de los NEs que sirve para determinar los importes que deben cargarse a las cuentas de los clientes y por lo general se deben realizar estas funciones en tiempo real y para un gran número de clientes. Algunas funciones relacionadas a la medición de utilización son; planificación del proceso de medición de la utilización, proceso de medición de la utilización, correlación de la utilización del servicio, validación de la utilización del servicio, identificación de las reglas de medición, etc.

2. *Tarificación / fijación de precios:* una tarifa es un conjunto de datos de un elemento de red, que pueden estar centralizados, distribuidos o en sistemas de operaciones y son utilizados para determinar el importe del pago por los servicios utilizados. La tarifa puede ser afectada por varias variables como la clase de tarifa, origen o destino del servicio, periodo de tarificación o categoría del día y estos atributos pueden cambiar durante el transcurso del servicio. Funciones relacionadas son; estrategia de fijación de precios, administración de tarifas y precios, cálculo de costos, política de liquidaciones, tasación de la utilización, totalización de las tasas de utilización, etc.

3. *Cobros y finanzas*: se refiere a la funcionalidad de transferencia de datos financieros para la RGT para, administrar cuentas de clientes, informar a los clientes sobre saldo, fecha de pago y recepción de los pagos. Ejemplos de funciones de cobro y finanzas son, planificación del proceso de facturación, gestión del proceso de facturación, operación de contabilidad general, nómina, cobros, etc.

4. *Control de la empresa*; éstas funciones sustentan el flujo de datos necesarios para tomar decisiones sobre el flujo de fondos apropiado dentro de la empresa y entre la empresa y sus propietarios y acreedores (responsabilidades fiduciarias de los directivos de la empresa). Algunos ejemplos de ésta funciones son; presupuestación, auditoría, gestión del efectivo, ampliación del capital, reducción de costos, análisis de rentabilidad, funciones de información financiera, etc.

2.2.6 La funcionalidad de la RGT para la interoperabilidad

Aspectos que incluye la RGT para la interoperabilidad son:

- intercambiar información de gestión a través de la frontera entre el entorno de telecomunicaciones y el entorno RGT;
- intercambiar información a través de las fronteras entre entornos RGT;
- convertir información de gestión de un formato a otro, con objeto de que la información de gestión que fluya dentro del entorno de la RGT sea coherente;
- transferir información de gestión entre ubicaciones internas al entorno RGT;
- analizar y reaccionar apropiadamente a la información de gestión;

- manipular información de gestión de modo que adquiera una forma útil y/o apropiada para el usuario de información de gestión;
- entregar información de gestión al usuario de dicha información, y para presentarla en una forma de representación apropiada;
- asegurar a los usuarios de información de gestión autorizados un acceso seguro a dicha información.

Parte de la información intercambiada en la RGT puede ser utilizada como soporte de más de una área de gestión.

2.3 Propuesta OSI

2.3.1 CMIS/CMIP

CMIS/CMIP (Common Management Information Service / Common Management Information Protocol) es el protocolo de gestión de las redes OSI, CMIS define los servicios generales que proporciona cada elemento de red (NE) para la gestión y CMIP es el protocolo que implementa estos servicios. Los protocolos de red OSI intentan proporcionar una arquitectura de red común para todos los dispositivos en cada capa del modelo de referencia OSI, de la misma forma CMIS/CMIP intentan proporcionar un protocolo de gestión de red completo para usarse con cualquier dispositivo de red.

Una diferencia entre CMIS/CMIP y ambas versiones de SNMP es que CMIS/CMIP requiere que el dispositivo gestionado realice más tareas que los dispositivos gestionados por SNMP cuyos agentes permanecen simples y la carga de trabajo se encuentra en la estación donde corre el sistemas de gestión, CMIS/CMIP distribuye esta carga de trabajo más equitativamente, requiriendo para esto significativos recursos y capacidades del dispositivo gestionado.

Un sistema en la terminología OSI, que puede ser un elemento de red o una estación de trabajo que usa el protocolo OSI es llamado sistema abierto "open system". Dos dispositivos que se comunican usando el protocolo OSI, en la misma capa del modelo de referencia, son sistemas abiertos punto "peer open systems".

2.3.2 Arbol de información de gestión(MIT)

El MIT (Management Information Tree) en CMIS/CMIP contiene instancias de objetos gestionados organizados en una base de datos jerárquica:

- La información es almacenada tanto en las hojas como en los nodos internos del árbol.
- La estructura del MIT puede cambiar dinámicamente, es decir, se pueden añadir y borrar nodos.
- Las instancias de los objetos gestionados se almacenan en nodos individuales.
- El MIT proporciona identificación única a las instancias de los objetos gestionados los cuales tienen atributos que sirven como nombre distintivo relativo (RDN, Relative Distinctive Name). El RDN identifica una instancia entre las posibles de un nodo padre.

Concatenando el RDN con el camino desde la raíz del árbol a un nodo dado se obtiene un nombre distintivo único (DN, Distinctive Name). El DN es usado por CMIP para identificar un nodo y accesar la información de gestión que contiene.

- Debido a que MIT es dinámico en su estructura, la forma de accesarlo es realizando búsquedas en los subárboles por la información de interés, es decir, extraer toda la información de un subárbol que cumple con ciertas condiciones.

En el modelo de información de gestión, los objetos gestionados están formados de atributos y métodos, estos métodos pueden realizar una operación como la notificación de eventos a los sistemas de gestión. El MIT que se muestra en la figura 21 pertenece a un concentrador con diferentes interfaces.

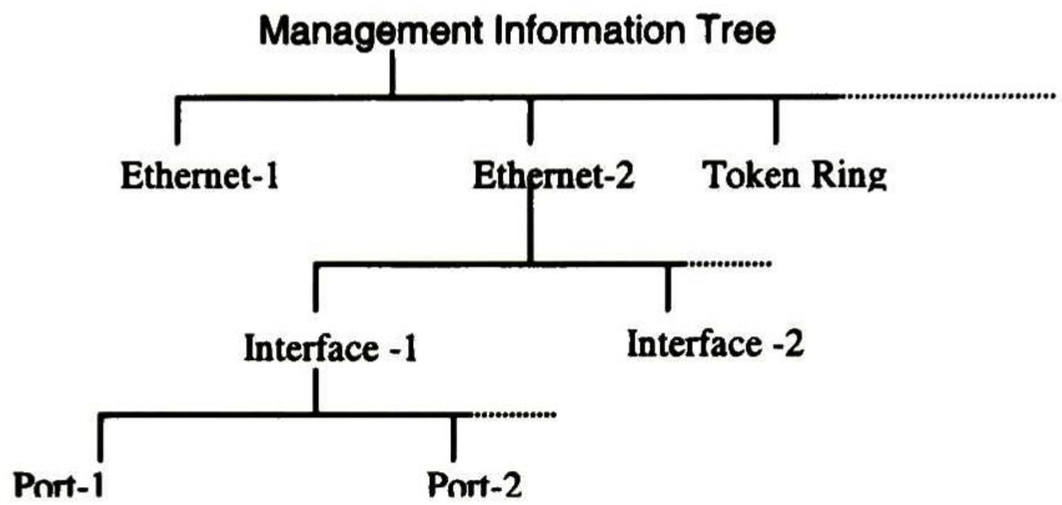


Figura 21. MIT

2.3.3 Estructura de protocolo OSI

La estructura de los protocolos de gestión OSI sigue a la del modelo de referencia OSI. Los procesos de la aplicación de gestión usan la capa de aplicación del modelo de referencia, en esta misma capa, CMISE (Common Management Information Service Element) el elemento servicio de información común de gestión provee a la aplicación de gestión los medios necesarios para que pueda usar el CMIP. CMISE usa dos protocolos de aplicación OSI mas:

ACSE (Association Control Service Element) elemento de servicio de control de asociación, el cual se encarga de establecer y cerrar asociaciones entre aplicaciones.

ROSE(Remote Operation Service Element) el elemento de servicio de operación remota, maneja las interacciones de requerimiento y respuesta entre las aplicaciones.

Estos protocolos y las aplicaciones que los usan son el marco de trabajo del esquema de gestión OSI. La figura 22 muestra los protocolos CMIP en el modelo de referencia OSI.

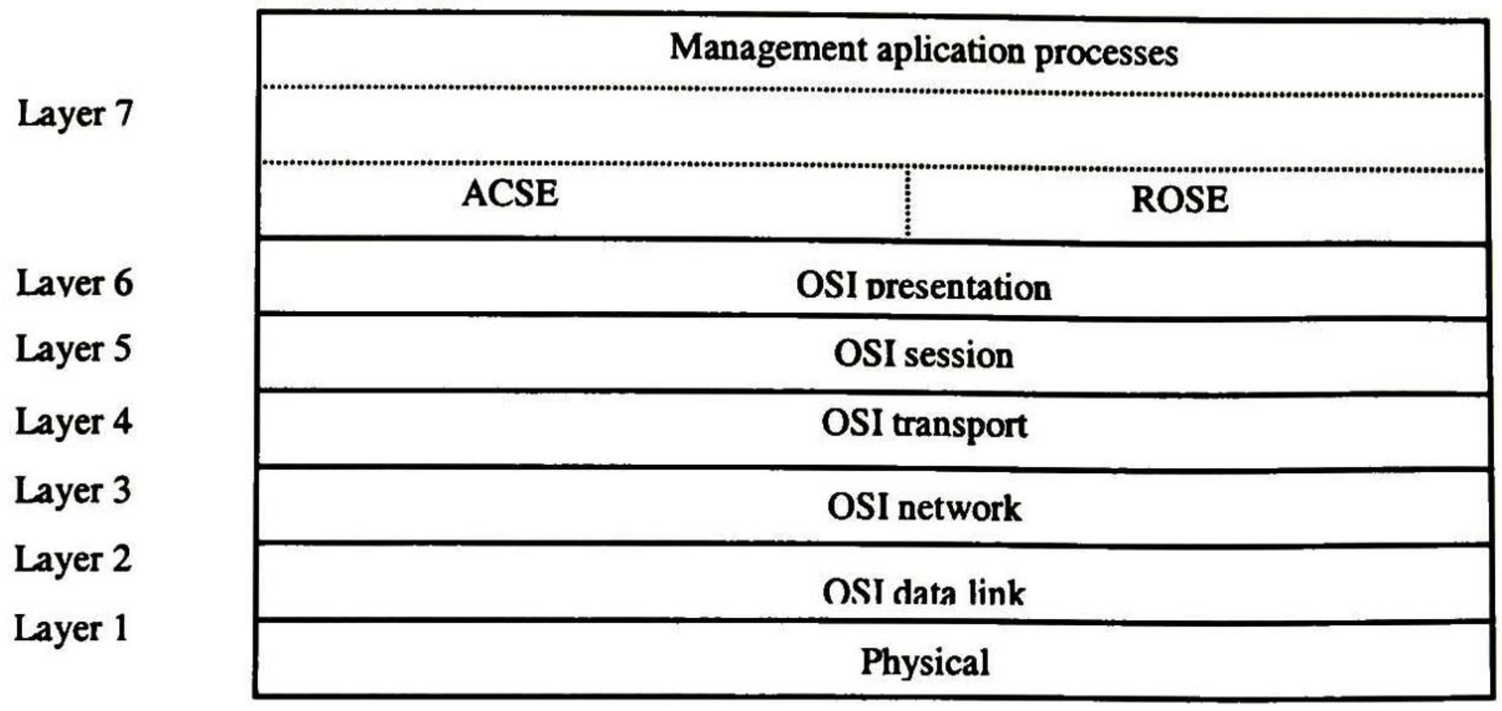


Figura 22. Protocolos CMIP en el modelo de referencia OSI

2.3.4 Servicios de información de gestión comunes (CMIS)

Cada servicio CMIS (Common Management Information Services) es una operación que puede ejecutar una aplicación de gestión y ésta es un usuario del CMISE. CMIS ha definido tres clases de servicios:

Servicios de asociación de gestión (Management Association Services), controlan la asociación de los sistemas abiertos de extremo, controlando la inicialización, terminación y terminación anormal de una conexión de asociación de gestión con los siguientes servicios:

- M-INITIALIZE: crea una asociación con un usuario CMISE para sistemas de gestión.
- M-TERMINATE: termina una conexión entre usuarios de servicio CMISE.
- M-ABORT: usado cuando una conexión entre usuarios de servicio CMISE termina anormalmente.

Estos servicios asumen el uso de ACSE para establecer y cerrar conexiones entre aplicaciones.

Servicios de notificación de gestión (Management Notification Services); proveen información sobre eventos en la red. El servicio M-EVENT-REPORT le dice a un usuario de servicio CMISE sobre un evento que ha ocurrido en otro usuario de servicio CMISE.

Servicios de operación de gestión (Management Operation Services) son:

- M-GET, es usado por un usuario CMISE para obtener información de gestión de un usuario CMISE de extremo, este servicio es análogo al mensaje de Get-Request en SNMP.
- M-CANCEL-GET, cancela un requerimiento de M-GET cuando la información ya no se necesita.
- M-SET, este servicio permite a un usuario de CMISE modificar información de gestión de un usuario CMISE de extremo, similar al mensaje de Set-Request en SNMP.
- M-ACTION, este servicio es invocado por un usuario CMISE para instruir a un usuario CMISE de extremo que ejecute una acción específica relacionada al funcionamiento del dispositivo.

- M-CREATE, este servicio es utilizado por un usuario CMISE para instruir a un usuario CMISE de extremo para crear otra instancia de un objeto gestionado. CMIS permite múltiples instancias del mismo objeto pero una sola definición del objeto, similar al concepto de programación orientada a objetos (Clases e instancias de clases). Este servicio permite a los objetos gestionados intruirse entre ellos sobre la presencia de nuevos objetos.
- M-DELETE, es la operación inversa de M-CREATE.

2.3.5 Asociaciones de gestión

Las conexiones entre sistemas abiertos de punta para los sistemas de gestión pueden ser de 4 tipos:

1. De evento

Una asociación de eventos permite a dos sistemas abiertos enviarse mensajes M-EVENT-REPORT, es decir, cuando únicamente se necesita enviar eventos de gestión. Para una asociación de evento dos sistemas abiertos necesitarán servicios de asociación de gestión y servicios de notificación de gestión.

2. De evento / monitor

Este tipo de asociación es igual a la de evento excepto que en éste cada sistema puede usar también mensajes M-GET, permite a los sistemas abiertos de extremo buscar información de gestión y recibir eventos de la red. Esta asociación es útil para usuarios CMISE interesados en saber el estado de ciertos sistemas abiertos de extremo sin acceso a modificarlos ya que este puede pertenecer a otra organización.

Para una asociación evento monitor dos sistemas abiertos de extremo necesitarán servicios de asociación, notificación y un subconjunto de los servicios de operación de gestión.

3. De monitor / control

Las asociaciones monitor /control permiten los servicios de M-GET, M-CANCEL-GET, M-SET, M-CREATE, M-DELETE y M-ACTION pero no se permite reporte de eventos, un usuario CMISE utilizaría esta asociación para modificar la configuración de un sistema abierto de extremo, en este caso los servicios de notificación no son tan importantes ya que la tarea principal es la configuración. Para la asociación monitor /control dos sistemas abiertos de extremo necesitan los servicios de asociación, un subconjunto de los servicios de operación de gestión. Idealmente otro usuario CMISE tiene la habilidad de procesar las notificaciones de eventos de la red.

4. De gestión completa / agente

Esta asociación soporta todos los servicios CMIS

2.3.6 Seguridad en CMIS

CMIS utiliza listas de acceso para cada sistema abierto en estas listas de acceso explícitamente se define el acceso de otro sistema abierto.

2.3.7 Protocolo de información de gestión común (CMIP)

CMIP (Common Management Information Protocol) es el protocolo que implementa CMIS. El protocolo CMIP requiere una máquina CMIP (CMIPM) para funcionar de acuerdo a la especificación definida. CMIPM es software con dos funciones:

Acepta operaciones enviadas por un usuario CMISE e inicia el procedimiento para realizar la operación asociada. Usa ROSE para enviar mensajes por de la red. La Figura 23 muestra el flujo del requerimiento de servicios CMIS entre 2 usuarios CMISE.

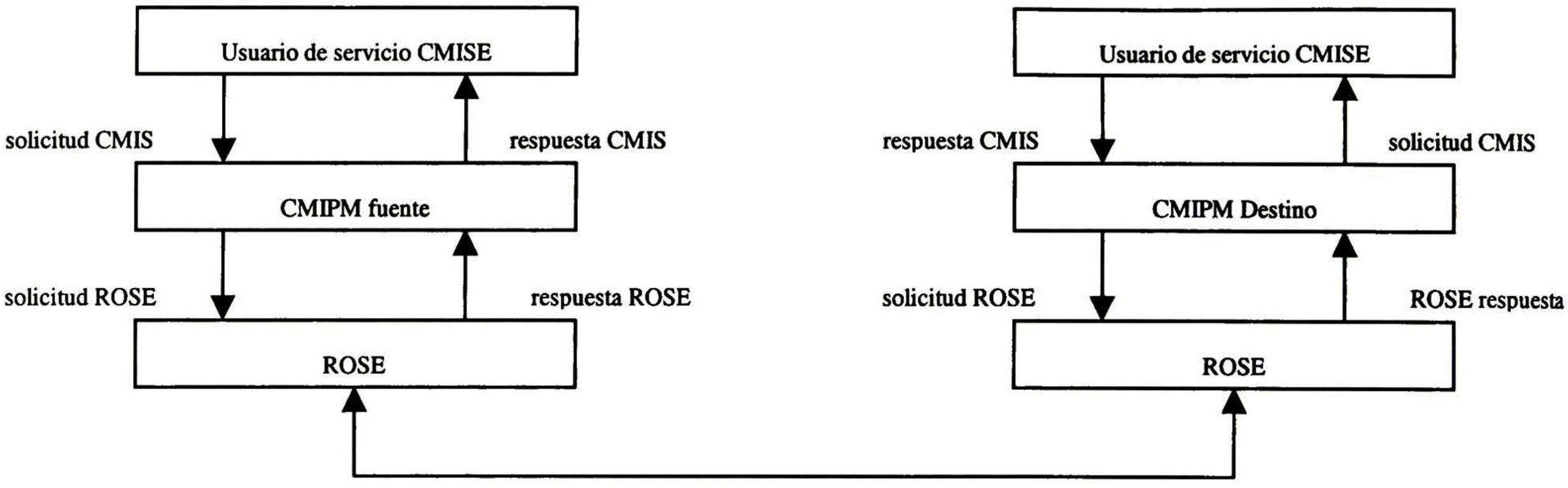


Figura 23. Flujo de solicitudes y respuestas entre 2 CMISE

CMIPM usa un conjunto de unidades de datos bien definidos para implementar los servicios CMIS, cada servicio CMIS usa un conjunto de estas unidades de datos como se muestra en la Tabla 3.

Tabla 3. Unidades de datos CMIP usados por servicio CMIS

CMIS servicio	***CMIP unidades de datos***
M-EVENT-REPORT	m-EventReport, m-EventReport-Confirmed
M-GET	m-Get, m-Linked-Reply
M-CANCEL-GET	m-Cancel-Get-Confirmed
M-SET	m-Set-Confirmed, m-Linked-Reply
M-ACTION	m-Action, m-Action-Confirmed, m-Linked-Reply
M-CREATE	m-Create
M-DELETE	m-Delete

Como ejemplo podemos ver a 2 CMIPM que usan m-Get y m-Linked-Reply; m-Get obtiene una parte de datos de una MIT de un usuario CMISE y m-Linked-Reply es usado

para responder a las unidades de datos de m-Get y proporciona una forma al usuario CMISE de correlacionar y responder mensajes que pueden utilizar múltiples paquetes.

CMIP define como descifrar la información en un paquete no en la forma en la que un usuario CMISE debe utilizar la información requerida de un objeto gestionado. CMIP no infringe en la funcionalidad de un sistema de gestión, este puede solicitar la información que necesite e interpretarla y manejarla de cualquier manera.

2.3.8 Ventajas y desventajas de CMIS/CMIP

Tabla 4 Ventajas y desventajas de CMIS/CMIP

Ventajas	Desventajas
Es posible distribuir los procesos de gestión a los dispositivos	Los dispositivos necesitan más capacidad de procesamiento y memoria.
La estructura de la información de gestión es dinámica orientada a objetos (MIT Management Information Tree)	La creación y borrado de objetos gestionados en los agentes, puede crear inconsistencias.
Proporciona un protocolo de gestión de red completo para cualquier dispositivo de red	El dispositivo gestionado necesita el stack de protocolo OSI completo (se necesitan recursos de memoria y procesamiento en el dispositivo).
El protocolo de gestión es orientado a conexión (gestor – dispositivo gestionado).	En situaciones cuando la red transporta mucho tráfico, ésta conexión de gestión se puede saturar cuando más se necesita, en situaciones difíciles.
	Utiliza mucho overhead y es difícil de implementar
El modelo OO proporciona una mejora en el manejo de notificación de eventos	
La información de gestión (MIT) colectada por el agente, se encuentra tanto en las hojas del árbol como en los nodos.	

2.4 Propuesta IETF

2.4.1 Base de información de gestión (MIB)

La MIB (Management Information Base) contiene información accesible mediante un protocolo de gestión de red, tiene estructura jerárquica y define la información disponible de un dispositivo. Cada dispositivo debe usar el formato para desplegar la información definido por la MIB para cumplir con el protocolo estándar de gestión. La estructura e identificación de la información de gestión (SMI, Structure and identification of Management Information) de diferentes MIBs (MIB, MIBII, RMON) se encuentran especificadas en RFCs (Request For Comments), donde se describe la sintaxis y tipo de información disponible en las MIBs. ASN.1 (Abstract Sintax Notation One)[31] es la entidad de ISO que define la sintaxis para la MIB. Actualmente existen MIBs específicas de los proveedores de equipo, estos dispositivos cuentan con un software agente que soporta la MIB estándar y la propietaria.

Cada MIB utiliza la estructura de árbol definida por ASN.1, para organizar toda la información disponible, cada nodo se etiqueta con un texto de descripción y con un identificador de objeto (OID) que es una serie de enteros, utilizado para atravesar el árbol y accesar el nodo, un nodo puede tener subárboles, numerados en orden ascendente. Si un nodo no contiene subárboles ni nodos hoja, este contiene un valor y es un objeto.

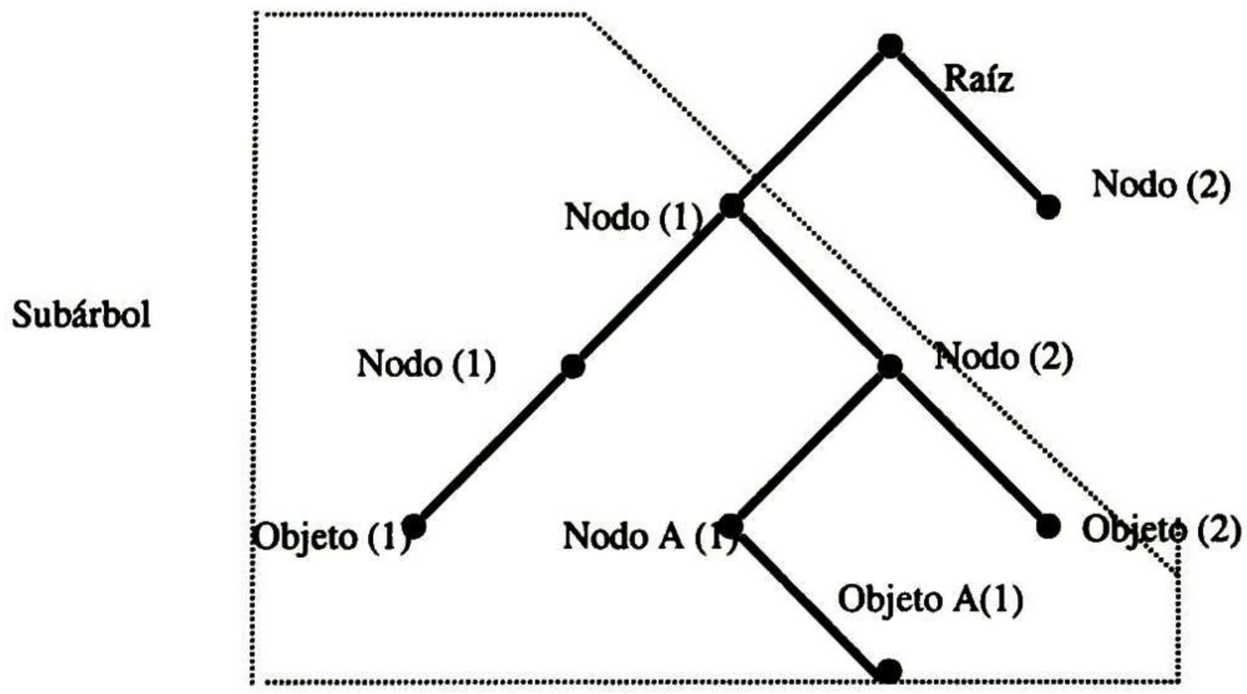


Figura 24. MIB

La Figura 24 muestra un ejemplo de un árbol MIB, en donde el objeto A se puede referenciar por el OID = 1.2.1.1 o [nodo A 1]

2.4.2 SNMP V.1

SNMP (Simple Network Management Protocol) es el protocolo de gestión más usado. Este se encuentra especificado en el RFC 1157 [5], donde se describe el modelo agente / estación usado en SNMP. Un agente SNMP es software capaz de responder a consultas válidas de una estación SNMP, sobre información definida en el MIB, el agente es parte del elemento de red (NE).

Agentes y estaciones SNMP se comunican con mensajes estándares, estos mensajes son empaquetados en PDUs (Protocol Data Units). SNMP usa UDP (User Datagram Protocol) como protocolo de capa de transporte, debido a que el mismo proporciona un servicio sin conexión, el agente y las estaciones no necesitan una conexión para transmitir los mensajes. UDP proporciona un servicio de transporte rápido con el mínimo de recursos necesarios, pero no es confiable. La figura 25. muestra la localización de SNMP en el modelo de referencia OSI.

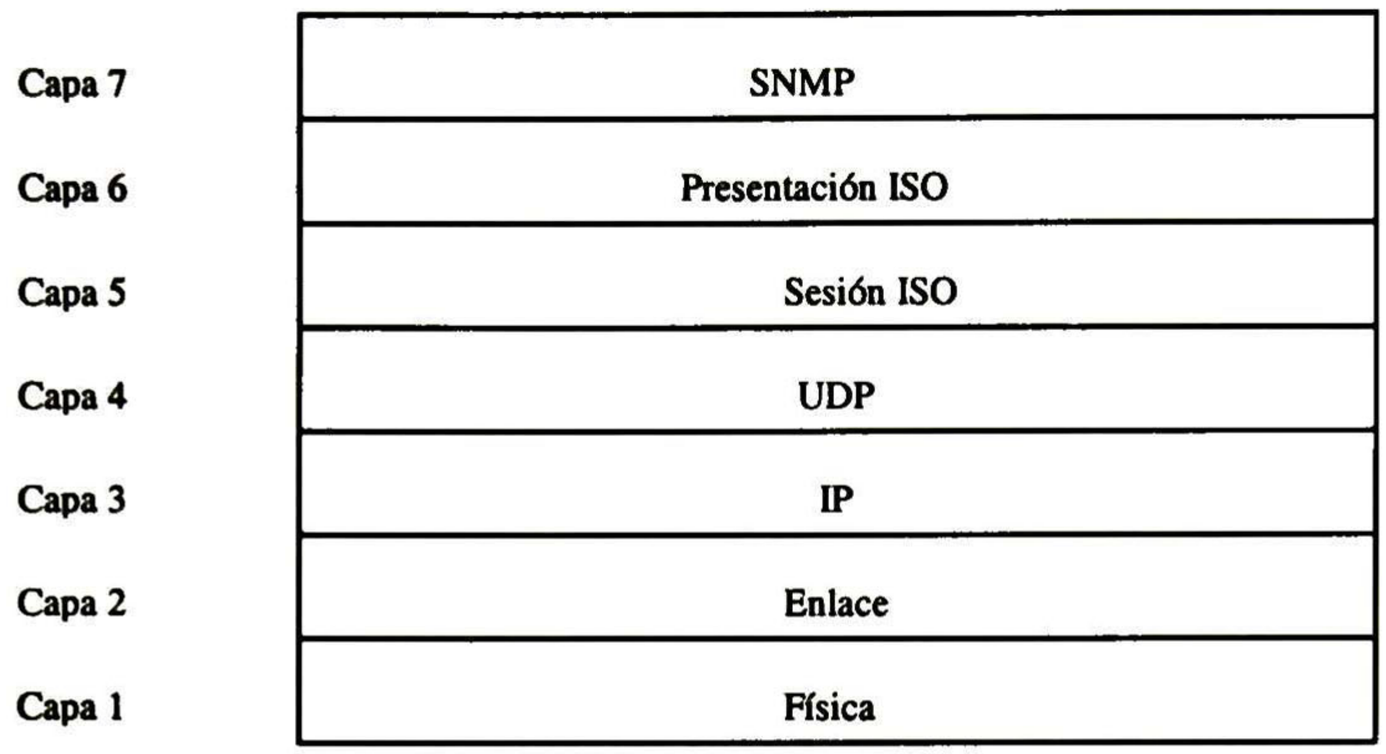


Figura 25. Relación de SNMP con el modelo de referencia OSI

SNMP tiene 5 tipos de mensajes:

- GetRequest; usado para obtener información de un NE que tiene un agente SNMP.
- GetResponse; mensaje que utiliza el agente para responder al mensaje GetRequest.
- GetNextRequest; usado en conjunto con GetRequest cuando el objeto consultado es una tabla.
- SetRequest; es un mensaje que permite la configuración remota de un NE.
- Trap; es un mensaje no solicitado enviado por un agente SNMP a la estación, este mensaje informa sobre la ocurrencia de un evento específico.

La figura 26 muestra los formatos de los mensajes SNMP.

Version	Community	PDU type	Request ID	0	0	Name X	Value X	-------

GetRequest, GetNextRequest, SetRequest

Version	Community	PDU type	Request ID	Error Status	Error Index	Name X	Value X	-------

GetResponse

Version	Community	PDU type	Enterprise	Agent Addr	Generic	Specific trap	Time	Name X	Value X

Trap

Figura 26. Mensajes SNMPv.1

2.4.2.1 Seguridad en SNMPV1

El agente SNMP puede requerir que los sistemas gestores envíen una clave particular con cada mensaje, para que el agente verifique que éstos están autorizados para accesar la MIB, esta clave se denomina "*community string*". Algunas implementaciones de agentes SNMP permiten diferentes niveles de seguridad usando "*community strings*".

2.4.2.2 Ventajas y desventajas de SNMP V1

Tabla 5 Ventajas y desventajas de SNMP

Ventajas	Desventajas
Es un protocolo simple, con MIBs[9][6] en los agentes, como bases de datos de la información de gestión.	Limitado en capacidad de gestión, por lo que han salido nuevas versiones SNMP V2 y V3.
Nuevos MIB´s han salido recientemente (MIBII, RMON) que han mejorado las limitaciones de SNMP contra CMIP.	La estructura de la información de gestión (MIB) es estática y está estandarizada en RFC´s, es decir, la estructura de los MIBs ya está definida en el momento de su diseño.
La simplicidad de éste lo ha hecho muy popular en el mercado.	
Es posible crear MIBs propietarios, en el caso de que los existentes no sean apropiados para representar la información de gestión del dispositivo.	MIBs propietarios originan problemas de interoperabilidad.
La estructura jerárquica del MIB permite agrupar variables relacionadas (OSI, Internet, Mangement).	La información se almacena únicamente en las hojas del árbol, los nodos internos (ramas) son usados para clasificar y agrupar variables.
El manejo de notificación de eventos se realiza mediante mensajes no solicitados por el sistema de gestión (Traps), generados por los agentes.	
La comunicación gestor – agente es mediante datagramas (UDP/IP), lo cual mejora el desempeño respecto a CMIP en condiciones difíciles de la red.	El uso de datagramas implica entrega no confiable de paquetes, por lo que el protocolo de gestión o el gestor se deben encargar de la confiabilidad de la comunicación.

2.4.3 SNMP V.2

Para superar algunas limitaciones de SNMP se desarrolló SNMP v.2 cuya funcionalidad sigue siendo accesar los MIBs de los NEs para obtener o cambiar la información de gestión. Posterior a SNMP se desarrollaron Secure SNMP y SMP (Simple Management Protocol), la comunidad de Internet acordó unir las ventajas de estas implementaciones para formar SNMP v.2 al cual se le añadieron nuevos tipos de mensajes, soporte multiprotocolo estandarizado, nuevos objetos en la MIB, extensiones en seguridad y en la estructura de la información de gestión (SMI, *Structure and identification of Management Information*) y puede coexistir con SNMPv.1.

Las extensiones realizadas en la estructura e identificación de la información de gestión 0(SMI) en SNMPv.2 son:

- Permite enteros de 64 bits (Counter64), contra los de 32 bits de SNMPv.1 que se renombraron (Counter32, Gauge32). Los valores que pueden generar estos tipos de datos necesitarán el doble de memoria, que muchos tipos de dispositivos no tienen, es por esto muchos MIBs estándar tienen un número limitado de objetos que se representan con enteros sin signo de 64 bits.
- Se añade un bit de signo a los números binarios.
- Se añade también un nuevo tipo de dato para representar direcciones OSI NSAP (Network service access point) llamado NsapAddress. Una NSAP es una dirección de red jerárquica usada por la capa de red OSI.
- SNMPv.2 incorpora todos los mensajes que maneja la versión anterior pero con diferente formato, es decir, los mensajes SNMPv.1 tienen los mismos campos excepto para GetResponse y Trap, ahora en SNMPv.2 usa un solo formato para todos los mensajes excepto GetBulkRequest y GetResponse. Otra diferencia entre los dos protocolos es la forma de crear sus tablas y mensajes de error. Se añaden 2 nuevos tipos de mensajes:
  - *InformRequest*; el cual permite que una aplicación de gestión envíe información a otra, es decir comunicación entre sistemas de gestión, este nuevo tipo de mensaje puede ser usado para proporcionar comunicación entre sistemas de gestión de redes jerárquica o distribuida.
  - *GetBulkRequest*; es un mensaje que ayuda a optimizar la extracción de cantidades grandes de información de gestión, que es uno de los principales problemas de SNMPv.1. Este mensaje trabaja de forma similar a GetNextRequest con la diferencia que GetBulkRequest extrae tanta información como sea posible del MIB para una consulta determinada.

La estructura de los mensajes SNMPv.2 es la siguiente:

PDU type	Request ID	0	0	Name X	Value X	-------

a) GetRequest, GetNextRequest, SetRequest,Trap, InformRequest

PDU type	Request ID	Error Status	Error Index	Name X	Value X	-------

b)GetResponse

PDU type	Request ID	Non-repeaters	Max repetitions	Name X	Value X	-------

c)GetBulkRequest

Figura 27. Mensajes SNMPv.2

SNMPv.1 se estandarizó para trabajar en redes IP solamente, ahora SNMPv.2 puede trabajar en protocolos como Appletalk de Apple, IPX de Novell, CLNS (Connectionless network service) de OSI, lo que habilitaría al protocolo a poder ser manejado en casi cualquier red. Sin importar el protocolo que soporte SNMPv.2 la operación de los mensajes y el protocolo permanece igual, en el modelo de referencia OSI SNMPv.2 esta en la capa de aplicación y usa la capa de red para la entrega, esto hace posible cambiar la capa de red sin modificar el protocolo SNMPv.2.

2.4.3.1 Seguridad en SNMPv.2

En el aspecto de seguridad los *"community strings"* en SNMPv.1 proporcionan un nivel débil de seguridad, ya que alguien con conocimientos en redes y con el equipo apropiado podría descifrar los *"community strings"*

Los mecanismos de seguridad implementados para SNMPv.2 proveen autorización y encripción para sus mensajes, la información de seguridad se encuentra fuera del mensaje, como se muestra en la figura 28.

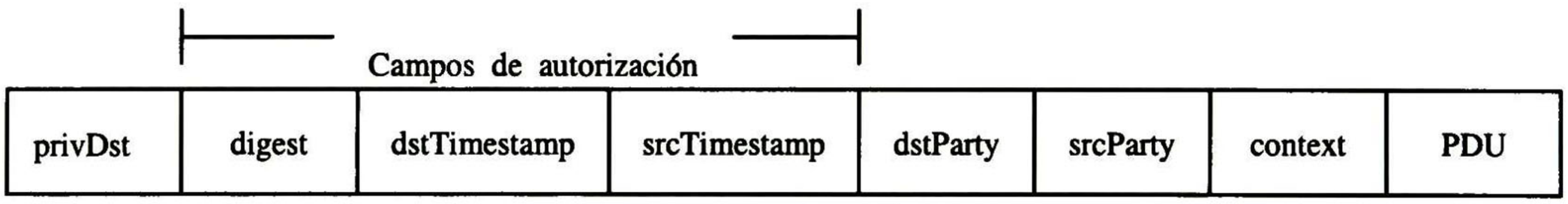


Figura 28. Campos de seguridad en SNMPv.2

El campo srcParty identifica al agente o sistema de gestión fuente que envía el mensaje, el campo dstParty indica el agente o sistema de gestión destino, el cual se repite en el campo privDst, esto se debe a que el mensaje SNMPv.2 puede estar encriptado en todos los campos siguientes a privDst, el cual permanece en texto claro para poder identificar fácilmente el destino del mensaje. Si el mensaje requiere autorización este contendrá los campos digest, dstTimestamp y srcTimestamp. Una parte (party) SNMPv.2 es un grupo de entidades que se comunican con información de gestión, pueden ser solo 2 entidades, cada parte tiene un conjunto de propiedades que controlan acceso y privilegios a la información de los MIB, estas propiedades son:

- Autorización, cuando se activa esta propiedad se utiliza un protocolo de autorización.
- Cifrado, esta propiedad se lleva a cabo por el algoritmo DES (Data Encryption Standard).
- Vistas de MIB, esta propiedad se refiere a partes de la MIB a los que el agente controla el acceso, la porción de la MIB que es accesible a un sistema de gestión se llama vista de la MIB.
- Contextos, en SNMPv.2 un contexto es un conjunto de objetos gestionados que un sistema de gestión o agente puede accesar.

2.4.3.2 MIBs relacionados a SNMPv.2

Se definen tres MIBs que ayudan a la gestión con SNMPv.2:

MIB SNMPv.2, en la que se definen objetos que describen el funcionamiento de SNMPv.2, esta formado por cinco grupos:

- *Grupo de estadísticas SNMPv.2*, el cual proporciona objetos que dan información sobre sistemas de gestión o agentes SNMPv.2
- *Grupo de estadísticas SNMPv.1*, el cual proporciona objetos que dan estadísticas sobre sistemas de gestión o agentes SNMPv.2 que se comunican con SNMPv.1.
- *Grupo de objetos recurso*, el cual proporciona información sobre los objetos que un agente SNMPv.2 puede crear dinámicamente.
- *Grupo de traps*, que contiene una tabla de información de cada trap que un agente envia.
- *Grupo de set*, el cual proporciona un solo objeto que permite a múltiples sistemas de gestión enviar mensajes de set a un agente sin tener problemas de coordinación, es decir, cuando 2 sistemas de gestión contradigan mensajes en la actualización del valor de algún objeto de un agente.

Manager to Manager MIB; los objetos que se encuentran en éste MIB proveen información sobre el desempeño de un sistema de gestión SNMPv.2. Esta formado por 2 grupos:

- Grupo de alarmas
- Grupo de eventos

Party MIB, contiene objetos que describen y configuran las partes asociadas a una entidad SNMPv.2, los grupos que contiene este MIB son:

- Grupo de base de datos de las partes, el cual contiene información sobre todas la partes locales o remotas conocidas, información que se almacena en el dispositivo.
- Grupo de base de datos de contextos.
- Grupo de base de datos de privilegios de acceso.
- Grupo de base de datos de vistas de la MIB.

Los tres grupos restantes se ocupan de los privilegios entre el sistema de gestión y el agente. Estos grupos permiten el control de contextos locales y remotos en la entidad SNMPv.2.

2.4.3.3 Coexistencia con SNMPv.1

Definición: un agente "proxy" es un elemento (hardware o software) de mediación entre sistemas gestores y agentes que no manejan el mismo protocolo. Realiza una traducción entre los protocolos de ambos para su comunicación.

Todas las definiciones de la MIB SNMPv1 son compatibles con los agentes y sistemas de gestión para SNMPv.2, los mensajes son muy similares entre ambos protocolos, de tal forma que hay dos posibles soluciones para la coexistencia:

Tener un agente "proxy" que realice la traducción de mensajes, un agente "proxy" tiene la función también de recopilar información sobre sistemas remotos y pasar esta información a una estación de gestión mediante un protocolo (SNMP).

Otra solución es tener un sistema de gestión que maneje ambos protocolos y que éste pueda decidir sobre el protocolo que debe usar con cada agente.

3 Sistemas de gestión

3.1 Características de los sistemas de gestión

Los sistemas de gestión contienen 3 tipos de componentes que trabajan juntos:

- *Gestores*; los cuales toman las decisiones sobre la información de gestión recolectada.
- *Agentes de gestión*; los cuales recolectan la información de gestión.
- *Objetos gestionados*; representan a sistemas o recursos de red gestionados.

Los agentes de gestión son usados en sistemas distribuidos y gestión de redes para reunir información, crear, borrar y cambiar el estado de los objetos gestionados, enviar notificaciones de eventos de los objetos gestionados a los sistemas gestores, esta interacción se muestra en la Figura 29. Los agentes operan a favor de los sistemas gestores, quitándoles carga de trabajo, ya que ésta se distribuye por el sistema o red y la eficiencia incrementa.

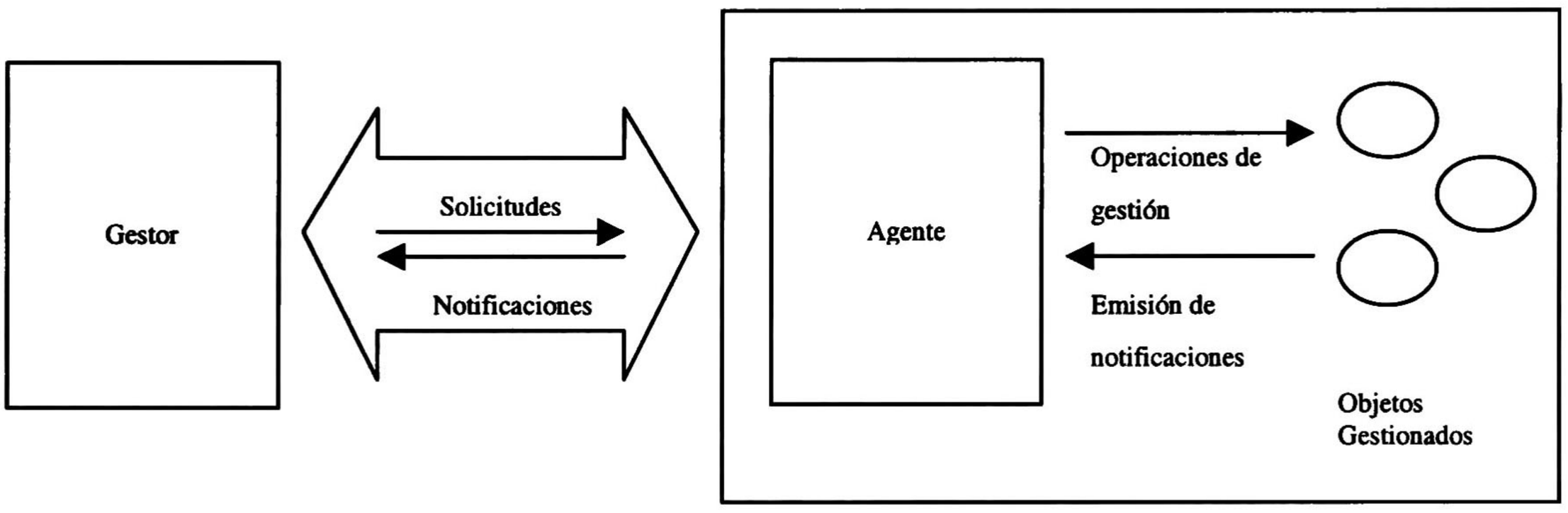


Figura 29. Relación gestor, agente y objetos gestionados.

Para facilitar el desarrollo de agentes se ha identificado una arquitectura genérica para agentes. En la misma se describen los servicios que los agentes pueden o deben proporcionar, los componentes que comprenden un agente y como éstos satisfacen los servicios. Una vez teniendo las capacidades de un agente de gestión genérico el desarrollador del agente se puede concentrar en la optimización de éste.

3.1.1 Requerimientos funcionales de agentes de gestión

Dado que un agente debe responder a solicitudes de los gestores, a otros agentes y objetos gestionados, el agente debe soportar los siguientes tipos de operaciones:

1. *Operaciones de auto descripción*: Un Agente debe ser capaz de describirse ante otras entidades (gestores y otros agentes) para que éstas últimas puedan descubrir que operaciones realiza y que recursos gestiona.

2. *Operaciones comunes de gestión*: Relacionadas al protocolo de gestión, operaciones como obtener/enviar información de/hacia los recursos gestionados, crear/borrar objetos gestionados, etc.
3. *Operaciones definidas por el usuario*: Diferentes tipos de análisis de la información recolectada, ejecutar servicios periódicamente.
4. *Operaciones de registro*: Los agentes deben ser capaces de registrar solicitudes, notificaciones e información de gestión para propósitos de análisis estadísticos y seguridad.

3.1.2 Componentes de un agente genérico

Los componentes de un agente de gestión genérico se muestran en la Figura 30. Cuando una solicitud llega y pasa al coordinador, donde se analiza su formato (parser) posteriormente pasa al componente de verificación de solicitud para después enviarse al componente apropiado donde la solicitud se ejecuta y cualquier resultado se envía de regreso a quien lo solicitó. Enseguida se realiza una explicación de los componentes de un agente genérico.

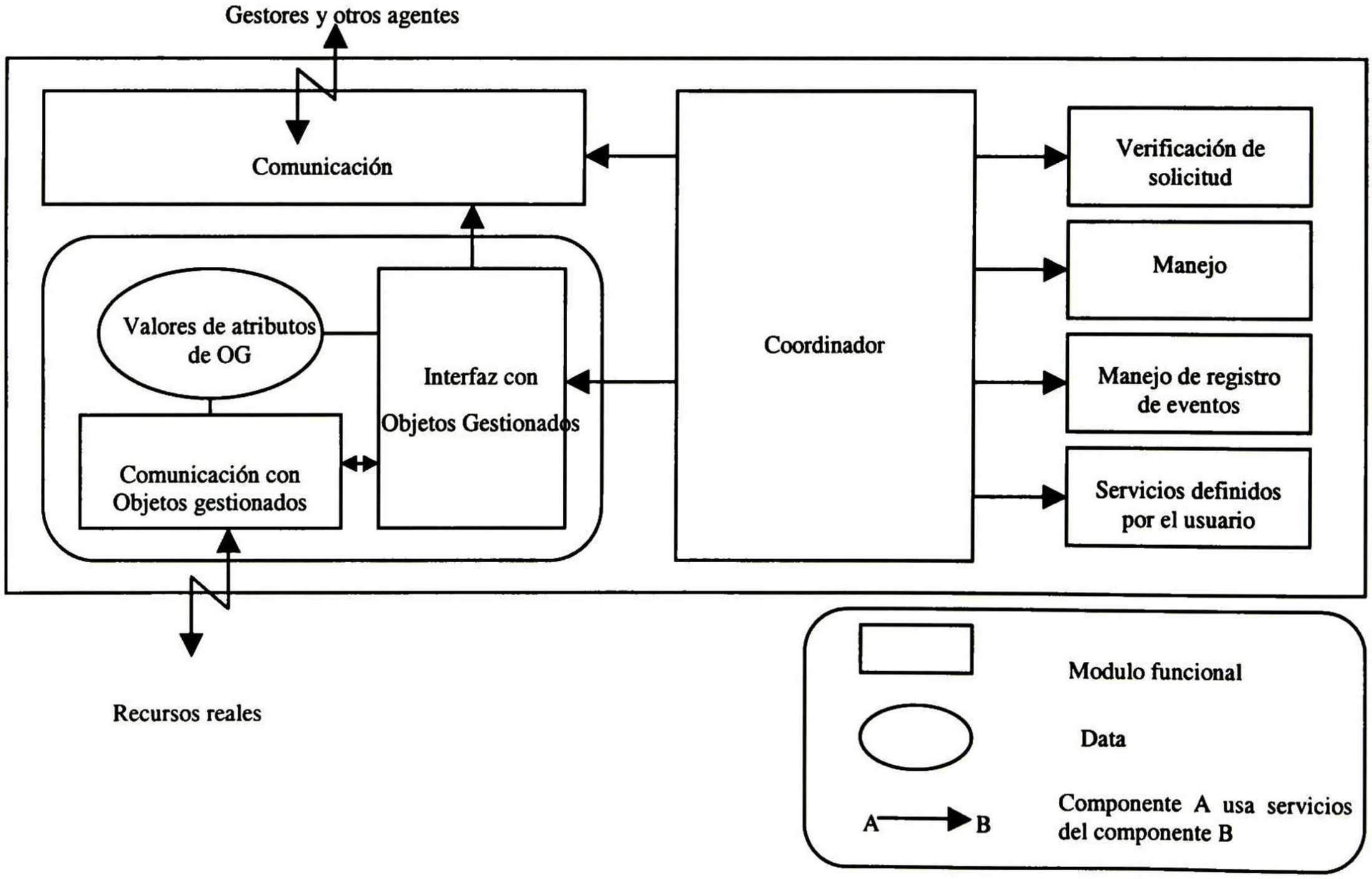


Figura 30. Agente genérico

1. *Coordinador*: es el componente central del agente, analiza la solicitud de acuerdo con el protocolo de gestión usado (parser) y conoce los servicios que proporciona el agente, para poder describir el agente a otras entidades.

2. *Comunicación*: proporciona servicios de comunicación para recibir solicitudes y enviar repuestas y notificaciones. Este componente necesita conocer el protocolo de gestión usado.
3. *Verificación de solicitud*: para asegurarse que las siguientes condiciones se mantiene que:
   - el agente soporta la solicitud,
   - cualquier objeto gestionado al que se hace referencia, existe,
   - quien solicita está autorizado para hacerlo y
   - quien solicita, tiene permiso para realizar la solicitud sobre los objetos gestionados destino.

   Para verificar estas condiciones, este componente debe conocer los servicios que proporciona el agente, así como las clases de objetos gestionados.
4. *Interfaz de objeto gestionado*: este componente contiene los objetos gestionados (abstracciones de los recursos gestionados) que pueden ser recursos físicos o procesos de una aplicación. Este componente proporciona la interfaz para que el agente interactúe con los recursos reales que representa. La comunicación con los recursos gestionados es decisión del desarrollador de los objetos gestionados. Este componente deberá conocer las operaciones de gestión que serán soportadas
5. *Manejo de registro de eventos*: este componente contiene servicios que permiten al agente registrar información de gestión, ejecución de servicios dinámicos o notificaciones recibidas de los objetos gestionados. Este componente puede ser automatizado.
6. *Servicios definidos por el usuario*: este componente almacena los servicios que han sido añadidos al agente y ejecuta estas solicitudes.
7. *Manejo de errores*: este componente esconde algunos detalles del protocolo de gestión del resto de los componentes del agente. Realiza diagnóstico y posible corrección de errores. Este componente conoce el protocolo de gestión.

La ventaja de tener componentes modulares es que cada componente no depende de los detalles de implementación de los otros, por ejemplo para el manejo de errores, solo se tiene que tener conocimiento del protocolo de gestión. El mismo código de manejo de errores es usado para todos los agentes que usan el mismo protocolo sin importar los servicios ofrecidos y los objetos gestionados localizados en otros componentes.

3.1.3 Servicio de interfaz del agente

Esta sección describe las operaciones que comprenden el servicio de interfaz. Estas operaciones representan la mayoría de las operaciones que los agentes de gestión proporcionan a otras entidades de gestión (gestores). Podemos distinguir cuatro tipos de operaciones ofrecidas por un agente:

- auto descripción, que son operaciones de gestión que permiten al agente describirse con sus capacidades a otras entidades de gestión,

- comunes de gestión, que son operaciones usadas para manipular los objetos gestionados,
- definidas por el usuario, operaciones que permiten extender las capacidades de los agentes,
- registro de eventos, las cuales permiten al agente registrar solicitudes, notificaciones e información de gestión.

Información detallada sobre las interfaces se describe enseguida.

3.1.3.1 Operaciones de auto descripción

Estas operaciones pueden ser usadas por gestores, objetos gestionados u otros agentes que solicitan al agente información del dispositivo o aplicación que en el que se encuentra.

1. *DescribeMyself*: permite al agente describirse a si mismo y sus capacidades incluidas.
2. *GetMOList*: Lista los objetos gestionados. Esta operación realiza un recorrido del árbol de objetos gestionados y regresa una lista. Quien solicita puede limitar o controlar el recorrido del árbol de objetos gestionados.
3. *ListPeriodicServices*: permite a una entidad de gestión consultar un agente por los servicios que se han planificado para correr como servicios periódicos. Un servicio periódico es aquel que ha sido añadido dinámicamente y se ha planificado para ejecutarse periódicamente (p.e. cada 5 minutos).
4. *ListServices*: permite a un gestor consultar a un agente por los servicios que se le han añadido.

3.1.3.2 Operaciones de gestión comunes

Estas operaciones son usadas por los gestores y otros agentes para borrar y crear objetos gestionados, realizar acciones sobre éstos, así como obtener y modificar valores de atributos en los objetos gestionados. También es usado por los objetos gestionados para enviar notificaciones de eventos a los gestores.

1. *Action*: envía un comando de acción a uno o más objetos gestionados. Las acciones están definidas en los objetos gestionados y se ejecutan sobre ellos mismos.
2. *Create*: crea un nuevo objeto gestionado de una clase, nombre y parámetros especificados.
3. *Delete*: borra el objeto gestionado especificado.
4. *ForwardNotification*: permite a un objeto gestionado enviar una notificación a un gestor.
5. *Get*: regresa valor(es) de atributo(s) de objeto(s) gestionado(s) especificado(s).
6. *Set*: modifica valor(es) de atributo(s) de objeto(s) gestionado(s) especificado(s).

3.1.3.3 Operaciones definidas por el usuario

Estas operaciones permiten extender la funcionalidad de los agentes. Nuevos servicios pueden ser añadidos estática o dinámicamente y ejecutados después bajo solicitud o periódicamente.

1. *AddNewService*: añade dinámicamente funcionalidad a el agente. Cada agente tiene tres tipos de operaciones que puede realizar:

   - Operaciones estáticas, un ejemplo de estas operaciones es esta lista o las operaciones de gestión comunes.
   - Operaciones estáticas definidas por el usuario; que es código escrito por el usuario y encadenado al agente en tiempo de construcción del mismo (p.e. cuando se optimiza un agente generalizado).
   - Operaciones dinámicas definidas por el usuario; llamadas servicios, que es código escrito por el usuario añadido al agente dinámicamente en tiempo de ejecución.

   Esta operación permite a una entidad de gestión enviar un programa a un agente y que éste lo añada en su lista de servicios.

2. *ExecuteService*: ejecuta el servicio especificado y regresa los resultados.
3. *StartPeriodicService*: planifica el servicio especificado a ser ejecutado periódicamente. Cualquier servicio que ha sido añadido con AddNewService puede ser usado en un servicio periódico. Si el servicio especificado regresa un valor.
4. *StopPeriodicService*: saca de planificación el servicio periódico especificado.

3.1.3.4 Operaciones de registro de eventos

DescribeLog: esta operación permite a una entidad de gestión para consultar un archivo de registro (Log file) por su estado actual, tamaño, etc.

LockLog: bloquea o desbloquea un archivo de registro, para que sus registros pueda ser leídos y no se pueden añadir nuevos registros.

StartLog: crea un nuevo archivo de registro (Log) habilitado y desbloqueado.

StopLog: detiene un archivo de registro y no puede ser reiniciado.

3.2 Arquitecturas de los sistemas de gestión

Un sistema de gestión de red puede usar varias arquitecturas para proveer su funcionalidad, como:

- Centralizada
- Jerárquica
- Distribuida

No hay una arquitectura mejor que otra, cada una tiene sus características específicas que trabajan bien en ciertos ambientes y en muchos casos la red de telecomunicaciones está estructurada de la misma manera que la arquitectura.

3.2.1 Arquitectura centralizada

Una arquitectura centralizada tiene la plataforma de gestión en un lugar y en un sistema y es responsable por todas las labores de gestión, con una base de datos centralizada, la cual esta respaldada por razones de seguridad y redundancia.

Aunque el sistema central realiza la gestión, este puede permitir acceso y mandar eventos a otras consolas de la red. El sistema con arquitectura centralizada es usado para:

- Todos los eventos y alertas de la red.
- Toda la información de la red.
- Para acceso a todas las aplicaciones de gestión.

Una desventaja significante de esta arquitectura es el hecho de realizar consultas a todos los dispositivos de la red desde un solo lugar, ya que se añade carga de tráfico en todos los enlaces conectados al sitio de gestión y en toda la red. Si la conexión de la estación de gestión se daña, todas las capacidades de gestión se pierden. Ejemplos de productos con arquitectura de gestión centralizada son Netview de IBM para una red SNA (Systems Network Architecture).

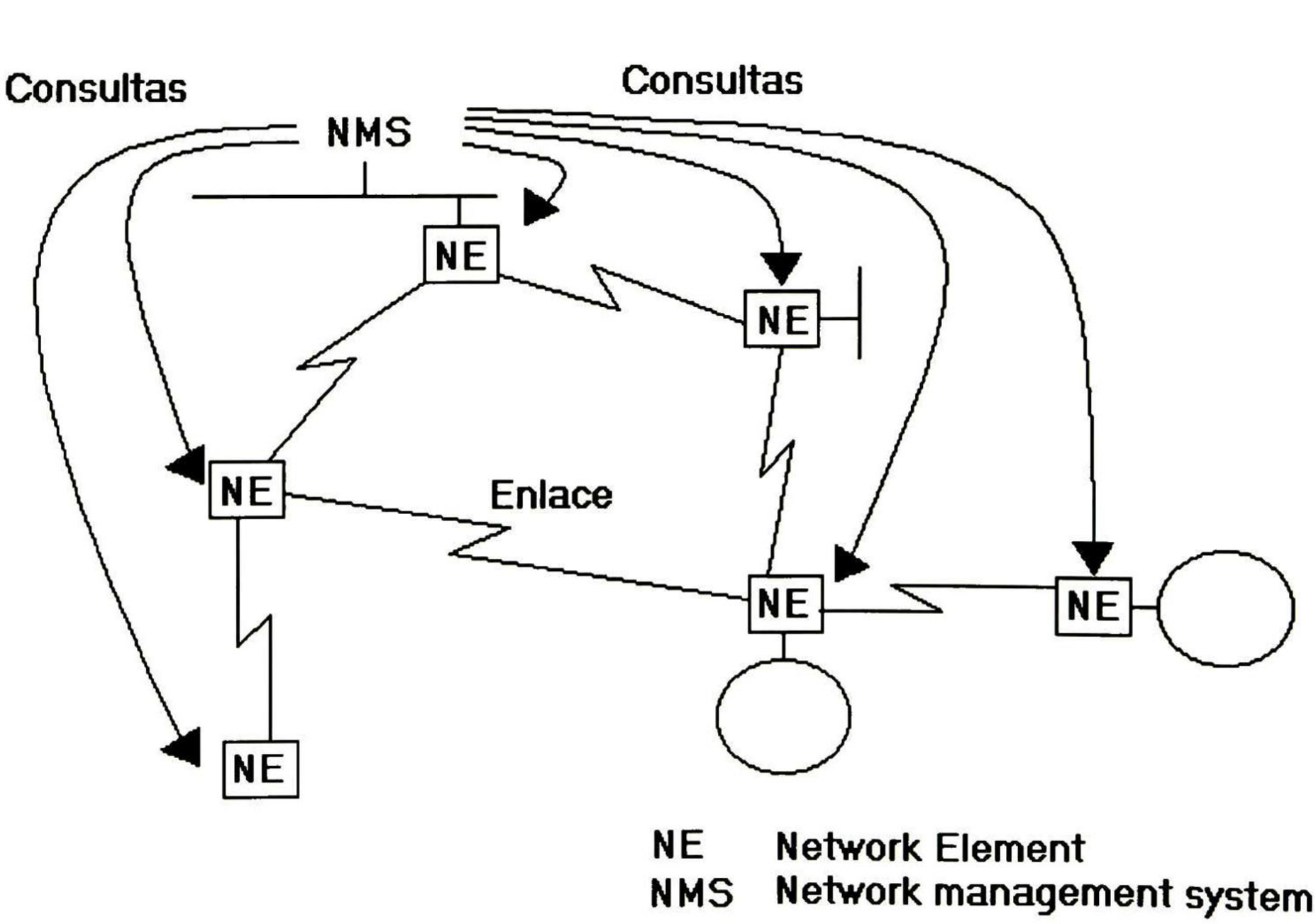


Figura 31. Arquitectura de gestión centralizada

3.2.2 Arquitectura jerárquica

Se caracteriza por usar múltiples sistemas, uno como servidor central y otros trabajando como clientes, distribuyéndose así las labores de gestión. La plataforma usa bases de datos cliente / servidor, los clientes consultan una sola base de datos en toda la red, las principales características de esta arquitectura son:

- No depende de un solo sistema.
- Distribución de tareas de gestión.
- Monitoreo de red distribuido.
- Almacenamiento de información centralizada.

Comparado con la centralizada, en ésta se distribuyen tanto tareas como monitoreo y se ahorra ancho de banda en la red, ya que los clientes pueden no requerir funcionalidad completa del servidor. Un cliente RMON (Remote network Monitoring device) es un ejemplo de ésta propuesta.

La desventaja de esta arquitectura reside en que debido a que se requieren de múltiples sistemas distribuidos para gestionar la red, reunir información de gestión completa de la red puede ser difícil y tardado.

Otro aspecto es que la lista de dispositivos gestionados por los clientes necesita ser lógicamente predeterminado y manualmente configurado, tarea que se debe hacer con control y cuidado para evitar que dos clientes realicen monitoreo del mismo dispositivo y se genere tráfico innecesario.

Ejemplos de productos que usan una arquitectura de gestión jerárquica son SunConnect SunNetManager, HP OpenView, IBM Netview/AIX y AT&T StarSentry, estos productos permiten configurar plataformas corriendo concurrentemente que operen de manera jerárquica.

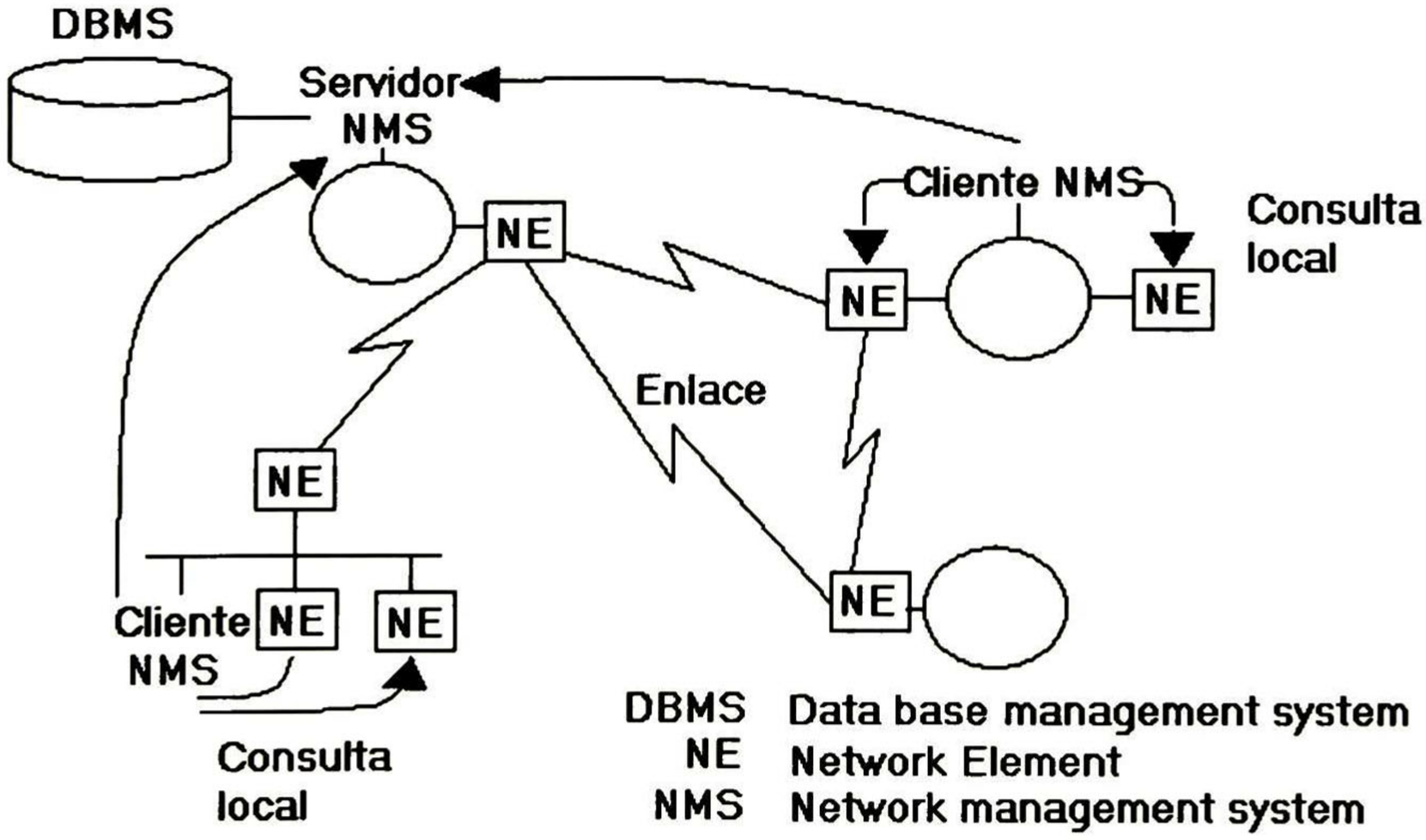


Figura 32. Arquitectura de gestión jerárquica

3.2.3 Arquitectura Distribuida

La arquitectura distribuida combina la centralizada y la jerárquica, esta propuesta usa múltiples plataformas, cada una de las cuales dirige un conjunto de sistemas de gestión de punto (peer NMS) y puede tener una base de datos para almacenar información de todos los dispositivos de la red, lo que permite realizar varias tareas y reportar el resultado al sistema central. Las características de esta arquitectura son:

- la información, alertas y eventos de toda la red se encuentra en un solo lugar,
- un lugar para acceso de todas las aplicaciones de gestión,
- no depende de un solo sistema,
- distribución de tareas de gestión,
- distribución monitoreo en toda la red.

Debido al manejo de múltiples bases de datos, es necesario mantener a las bases de datos de los diferentes sistemas completamente sincronizados, que es una labor compleja y el "overhead" asociado con la sincronización consume más recursos que una tecnología de base de datos cliente / servidor.

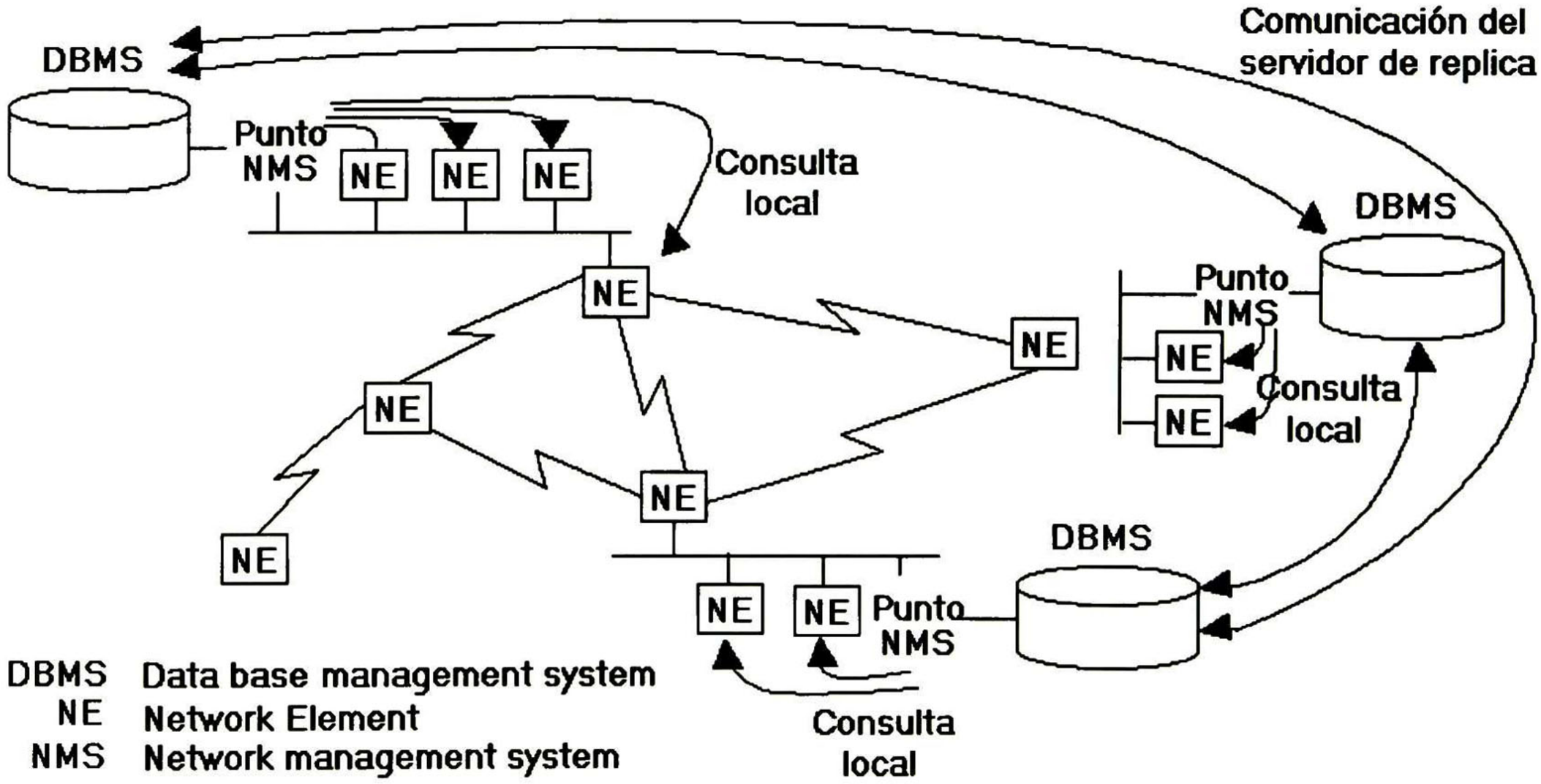


Figura 33. Arquitectura de gestión distribuida

Con independencia de la arquitectura se ha hecho necesario la unificación de las tareas de gestión mediante la estandarización de:

- Protocolos de gestión (SNMP, SNMPv.2, CMIP).
- Estructuras de la base de información de gestión en los agentes (MIB,MIT).
- Semántica de la información en las bases de datos (SMI, Structure of Managed Information).

- Plataformas de gestión.

Por lo que el reto por afrontar en la gestión de redes consiste en desarrollar respuestas efectivas y sistemáticas a:

¿Qué debe ser monitoreado?

¿Cómo debe ser interpretado?

¿Cómo debe ser usado éste análisis para controlar el comportamiento de la red?

3.3 Sistemas de gestión basados en plataforma (Platform based)

Una plataforma de gestión de red es un paquete de software que provee la funcionalidad básica de gestión para múltiples y diferentes elementos de red y está formada por:

- Una interfaz gráfica de usuario (GUI).
- Un mapa de la red.
- Un sistema manejador de base de datos (DBMS)
- Un método estándar para realizar consultas a los dispositivos.
- Un registro de eventos (Event log).

3.3.1 Interfaz Gráfica de usuario

Los sistemas de gestión desarrollados para un sistema operativo específico (plataforma) tienen la característica de tener interfaces amigables, completamente gráficas, con múltiples ventanas, con un sistema menús para desplegarlas y accesibilidad para realizar una determinada operación de diversas formas (p. e. Desplegar información de dispositivos mediante el uso del menú o mediante alguna acción del mouse).

Una característica importante de éstos sistemas es que proporcionan al usuario (administrador de red) un mapa de la red que se está gestionando, éste cuenta con iconos que representan a los dispositivos o entidades gestionadas y líneas que pueden representar enlaces o flujo de tráfico de datos de algún protocolo. En general la idea es que este mapa represente concierta precisión el estado actual de la red, de tal forma que el administrador pueda verificar el buen funcionamiento de los dispositivos en un solo lugar.

3.3.2 Sistema manejador de base de datos (DBMS)

Un sistema de gestión de plataforma hace uso de una o varias bases de datos donde registra la información de gestión relevante una vez que ésta ha sido recolectada de los dispositivos gestionables y procesada por los OSs del sistema gestor.

3.3.3 Un método estándar para realizar consultas a los dispositivos

Parte esencial de los sistemas de gestión es la habilidad para obtener información de los elementos de red (NE) y mandar información que efectúe cambios en estos. Un protocolo de gestión de redes:

- provee formatos de datos y parámetros comunes,
- permite extraer información de los elementos de red,
- permite enviar información, que activen cambios en los dispositivos,
- cuenta con mecanismos de seguridad, para proteger la información requerida y evitar que se realicen cambios no autorizados,
- puede ejecutar remotamente tareas de gestión,
- puede ser totalmente independiente de la capa de protocolo de red, para que todos los dispositivos sin importar el protocolo sean gestionables,

Existen protocolos simples, más complejos y avanzados. Los protocolos de gestión más comunes son:

- Simple Network Management Protocol (SNMPv.1 y SNMPv.2).
- Common Management Information Services / Common Management Information Protocol (CMIS /CMIP).

Los cuales fueron estudiados en el capítulo 2.

3.3.4 Un registro de eventos (Event log)

Un *registro de eventos* es utilizado por el administrador de la red para rastrear ciertos eventos como errores sobre algún dispositivo, tráfico excesivo, estadísticas de errores por protocolo utilizado, entre otros.

3.4 Sistemas de gestión basados en tecnologías de Internet (Web based)

Generalmente las redes son gestionadas por sistemas de plataforma, los cuales proporcionan la integración de herramientas de gestión, pero cuentan con algunas desventajas:

- Las plataformas de gestión son costosas en términos de software y del hardware requerido.
- Son complejas de instalar, correr y mantener
- Las plataformas de gestión se basan en el paradigma centralizado, lo cual crea cuellos de botella y provoca retardos para reaccionar ante problemas de la red.

Las recientes tecnologías de Internet como World Wide Web (WWW) y el lenguaje Java proporcionan medios para contrarrestar algunas de las desventajas de las plataformas de gestión.

WWW ha cambiado la forma en la que la gente trabaja y se comunica, muchas interfaces de usuario se han modificado a favor de la interface web y se ha adoptado como la forma privilegiada de interactuar con el usuario sin importar el sistema operativo ni la aplicación que se usa. Por otro lado el lenguaje Java proporciona medios para crear aplicaciones de software portable entre plataformas, distribuidas y accesibles mediante un navegador.

Los beneficios de la interface web en aplicaciones de gestión:

- Los navegadores se proporcionan con casi cualquier sistema operativo y están basados en estándares (HTML, HTTP).
- Las facilidades de Hipertexto son aprovechadas para ayuda en línea y documentación.
- Anterior a la arquitectura cliente –servidor de la web, los servidores web funcionaban como contenedores centrales de software y los navegadores se usaban como aplicaciones cliente.
- Las páginas HTML pueden integrar múltiples servicios heterogéneos (Applets).

Uno de los desarrollos más completos de sistemas de gestión basados en tecnologías de Intenet es el desarrollado por L. Deri [11][19][23]el cual tiene las siguientes características:

- Conocer los recursos de red SNMP o CMIP usando un navegador.
- Desplegar la topología de la red en 3D usando VRML [21](Virtual Reality Markup Language).
- Realizar operaciones de procesamiento usadas por elementos de software externos (C, C++, Java) que permiten la creación de aplicaciones de gestión simples explotando un conjunto de servicios (RAD, Rapid Application Development[20]).
- Gestionar instancias SNMP y CMIP desde Corba, explotando las asociaciones externas de software del punto anterior [22].

Otros esfuerzos por usar las tecnologías de Internet en la gestión se han desarrollado tal es el caso de extensiones del lenguaje tcl/tk llamada Scooty. En la cual se añade el manejo de mensajes SNMP. Las aplicaciones tcl/tk se pueden enlazar con un navegador.

3.5 Sistemas de gestión basados en escritorios de sistemas operativos modernos (Desktop Based)

El escritorio (desktop) es un ambiente gráfico que permite al usuario interactuar con el sistema operativo mediante iconos, ventanas y el "mouse" En algunos ambientes de escritorio modernos (Windows98) se ha incluido al navegador (IE, Netscape) como parte del escritorio (webtop), básicamente cada aspecto del SO se ha basado en la web y se ha usado como un reemplazo del escritorio del SO.

A pesar de todos los beneficios que ofrecen las tecnologías de Internet, las aplicaciones basadas en la web no se han integrado al escritorio.

El uso de interfaces web como plataforma nativa de aplicaciones tiene las siguientes desventajas;

- *Integración limitada al SO* (Sistema Operativo). Los ambientes de escritorio tienen un URL único para cada recurso accesible con el navegador, por lo que no es posible accesar el mismo recurso utilizando una aplicación no basada en la web, como un shell o un editor de texto (no es posible more http://www.erw.....).
- *Falta de automatización de tareas o manejo de scripts*. Una ventaja de los sistemas operativos basados en shell es la capacidad de escribir pequeños programas usando lenguajes de script, por lo que cuando se usa un navegador cada actividad se tiene que realizar gráficamente, llenando formas y navegando, no es fácil crear un programa de notificación de eventos. Esto se debe a que HTML es para desplegar no para procesar.
- *Integración de recursos contra composición de recursos*. HTML permite integrar información heterogénea y aplicaciones Java en una sola página, además del uso de "scripts" de java con capacidades limitadas para interactuar y comunicar. La composición de recurso por otro lado permite a los desarrolladores componer diferentes recursos como software y documentos y generar otro recurso que puede ser parte de otro a su vez.

Desktop Based Management es la actividad de gestionar redes y sistemas usando herramientas, métodos y paradigmas estándares del escritorio (Desktop) del sistema operativo. Los principios son:

- Toda información/ recurso de gestión debe poder ser accesible desde el escritorio.
- Cualquier aplicación pueda desplegar información de gestión.
- Los recursos de gestión deben ser visibles al nivel del escritorio y accesible de diferentes aplicaciones.

Las ventajas que ofrece la gestión basada en el escritorio del sistema operativo:

- *Fácil uso*, debido a que cada detalle de implementación esta oculto por el esritorio que presenta los recursos de gestión de forma amigable. Por ejemplo, un trap de SNMP puede ser notificado añadiendo un archivo con información del trap en un directorio compartido que apunte al host donde el demonio del trap SNMP está corriendo.
- *Integración completa al SO*, esto permite a diversas aplicaciones accesar información de gestión. Por ejemplo, un usuario podría usar una hoja de cálculo para escribir una macro que realice un gráfico de desempeño leyendo algunos archivos.
- *No se necesita software especializado* en el host cliente (navegador o aplicación de plataforma).

3.6 Modelo de la información de gestión con el paradigma orientado a objetos

El paradigma orientado a objetos fue aplicado al análisis y diseño por los analistas de ITU (sector telecomunicaciones) ANSI T1 por cumplir éste con requerimientos que otros métodos no tenían.

3.6.1 Descomposición algorítmica (estructurada) contra orientada a objetos

El descomponer el espacio del problema en piezas manejables y entendibles se puede realiza normalmente de dos formas ya sea:

- *Estructurada*, la cual se concentra en el ordenamiento de los eventos en un proceso usando por ejemplo el análisis estructurado Top-Down en el cual se realiza una descomposición sucesiva de procesos mayores en subprocesos de complejidad menor.
- *Orientada a objetos*, el cual detecta abstracciones clave en el dominio del problema, es decir, se enfatiza a los elementos que causan o que son sujetos de acciones.

La metodología orientada a objetos trabaja bien en el problema de la integración de sistemas de gestión bajo los siguientes criterios:

- El sistema resultante debe ser capaz de proporcionar diferentes perspectivas o vistas del mismo objeto o grupo de objetos; por ejemplo un contador puede ver al sistema como una herramienta para calcular la depreciación, un analista de seguridad como un detector de intromisión, un administrador de red como una herramienta para monitorear el comportamiento de la red, etc.
- El diseño se debe realizar sin tomar en cuenta aspectos de la implementación. Esperar implementaciones comunes es imposible a causa de las limitaciones físicas de diferentes dispositivos.
- El diseño debe explotar la similitud y aspectos comunes que existan, es decir, se deben detectar las características comunes, para evitar repetición de módulos.
- Un buen diseño permitirá que objetos diferentes puedan realizar acciones comunes.

Diseño orientado a objetos es una herramienta poderosa para manejar la complejidad, Booch [26] menciona que los sistemas de software son inherentemente complejos, pero utilizando técnicas de análisis y diseño OO, la complejidad se pueden simplificar usando los principios de descomposición, abstracción, jerarquía (herencia) y asociación.

3.6.2 Objetos

Humanos intuitivamente perciben el mundo como una colección de objetos que interactuan, un conmutador, un módem, un cable, una persona, etc. Los objetos:

- Tienen atributos; cable desconectado, interfaz activa, dispositivo fuera de servicio, etc.
- Pueden realizar acciones o se pueden ejercer acciones sobre ellos; un cable transmite datos, un dispositivo conmuta paquetes en la red, un puerto rechaza paquetes bajo ciertas circunstancias.
- Pueden estar formados por otros objetos; un conmutador está formado por circuitos integrados y cables.
- Pueden tener propiedades comunes; ambos conmutador y módem tienen interfaces.

- Pueden operar con acciones comunes; conmutador y concentrador distribuyen tráfico a la red.

Un objeto se puede definir como la representación de una entidad física o lógica de interés para el diseño.

3.6.3 Objetos Gestionados

Un objeto gestionado es un recurso físico o lógico de interés y se define en términos de:

- *Atributos*, que son características de los objetos, expresadas como datos de interés para la gestión.
- *Operaciones*, que pueden ser realizadas sobre él.
- *Notificaciones,* que puede realizar sin solicitud previa.
- *Relación con otros objetos gestionados* y otras formas de comportamiento que presente.

El modelo de objetos se construye basándose en los principios de encapsulamiento, abstracción, herencia y polimorfismo.

3.6.4 Principios del análisis y diseño orientado a objetos.

Es importante distinguir la perspectiva que tiene la persona que implementa / desarrolla a la que tiene el analista / diseñador, éste último intenta integrar sistemas de diferentes proveedores descomponiendo el problema y creando un diseño que pueda ser ampliamente entendido e implementado de diferentes formas. El que implementa / desarrolla normalmente ve el problema de la perspectiva de algún método particular de implementación.

3.6.4.1 Abstracción

Este principio proporciona diferentes vistas del objeto gestionado a diferentes personas, es decir, cualquier detalle que no sea de interés para la vista del usuario se oculta. Los diseñadores de sistemas de gestión integrados utilizan este principio de dos formas:

- Para realizar una descomposición jerárquica del problema y así agrupar características comunes en clases de objetos.
- Para construir objetos gestionados con características que representen ampliamente la vista del recurso de red, esta tarea se apoya también del principio de herencia.

3.6.4.2 Encapsulamiento

Este principio esta muy ligado a la abstracción, esta última nos da una interfaz simple de un objeto complejo y el encapsulamiento oculta la complejidad y los detalles de implementación. La meta de aplicar este principio es especificar módulos que son independientes y por eso se pueden modificar o reutilizar, sin tener que realizar cambios donde estos objetos son utilizados. Principio que es importante para la integración de

sistemas ya que estos entenderán la información de la misma forma con una variedad de aplicaciones de agente construidos en el mismo modelo.

3.6.4.3 Jerarquía / Herencia

La abstracción se asiste de la descomposición jerárquica y del concepto de herencia o especialización. Cuando se identifica una abstracción que agrupa a cierta clase de objetos para posteriormente especializarlos creando subclases, de tal manera que la especialización defina mejor a un tipo particular de objeto, tenemos como resultado una descomposición jerárquica que presenta una abstracción entendible y expansible.

En el más alto nivel de abstracción se identifica el objeto del cual se derivarán otras subclases de objetos y este nivel más alto contendrá información que deseamos hacer común a todos los objetos que se deriven. Estos no repiten esas características pero si especifican las diferencias que los hacen especializaciones de la superclase e indican de cual superclase son derivados, por lo tanto heredan las características de la superclase. Esto implica que un modelo orientado a objetos puede ayudar a realizar un diseño de larga vida cuando se realiza una buena abstracción jerárquica aún con la rápida evolución de la tecnología.

Las clases y subclases pueden ser instanciables o no instanciables, estas últimas son usadas cuando se desea que ciertas características no sean implementadas sin la debida especialización.

Existen también dos formas del principio de herencia, la herencia estricta y la herencia múltiple. Para asegurar la claridad de la descomposición del dominio del problema, analistas de sistemas de gestión usan la herencia estricta únicamente en donde una subclase hereda las características de todas sus superclases. La herencia múltiple se refiere a la habilidad de una clase para heredar características de más de una superclase.

3.6.4.4 Polimorfismo

La evolución de la tecnología provocará que recursos y sistemas de gestión que se desarrollen tengan diferentes versiones del modelo implementado y por lo tanto diferente comportamiento. El polimorfismo es el principio usado para manejar la complejidad provocada por la coexistencia de versiones diferentes. El polimorfismo permite a dos instancias de una clase a comportarse diferente a un mismo mensaje como si fueran derivadas de supercalses diferentes. Este principio ayuda al control de versión en la gestión, así como nos permite añadir nuevo código al sistema sin tener que cambiar el viejo.

Los principios del análisis y diseño orientado a objetos cuentan con la suficiente flexibilidad que nos proporciona la abstracción, herencia y el polimorfismo y la simplicidad y protección del encapsulamento para poder diseñar la estructura de un modelo de información y un sistema de gestión robusto y de larga duración.

Podemos ver que los principios de la RGT en el sentido del modelado de la estructura de la información de gestión son aplicables de forma más directa usando Common Management Information Services / Common Management Information Protocol (CMIS/CMIP) ya que éste marco de trabajo hace un uso más completo del paradigma orientado a objetos. Por

otro lado las versiones recientes de SNMP han presentado mejoras tanto en la estructura de la información con los diferentes tipos de MIBs (MIBII, RMON) como en el desempeño del protocolo.

Parte II: Análisis, diseño e implementación de un sistema de gestión

4 Desarrollo de un sistema de gestión enfocado a pequeñas y medianas empresas

4.1 Convenciones para el desarrollo de este proyecto

Definición: *Artefacto* es una pieza de información que es usada o producida durante el proceso de desarrollo de un software [28].

Para modelar el sistema se ha elegido utilizar UML (Unified Modeling Language)[27][28] debido a que UML es un lenguaje estándar para la construcción de modelos y ha sido producto de mejoras realizadas a metodologías de diseño como OMT[32], Booch[26] y OOSE[33]. Sin embargo, UML no es considerado por si mismo como una metodología de análisis y diseño, esto se debe a que UML define un conjunto de diagramas y modelos (artefactos), pero no especifica un *proceso de desarrollo de software* en particular, el cual:

Proporciona una guía para ordenar las actividades de un equipo de desarrollo. Especifica los artefactos que deben ser desarrollados dependiendo del dominio del problema. Ofrece criterios para monitorear y evaluar las actividades y productos del proyecto.

Entre los tipos de diagramas que define UML están:

- Diagramas de casos de uso.
- Diagramas de clases.
- Diagramas de comportamiento:
    - Diagramas de estados.
    - Diagramas de actividades.
- Diagramas de interacción:
    - Diagramas de secuencias.
    - Diagramas de colaboración.
- Diagramas de implementación:
    - Diagramas de componentes.
    - Diagramas de desarrollo.

Por lo tanto es necesario, especificar un proceso de desarrollo de software, el cual se describe a continuación.

4.2 Proceso de desarrollo de software

En un alto nivel, podemos distinguir 3 pasos:

1. Planeación y elaboración de prototipos.
2. Construcción.

3. Aplicación.

Planeación y elaboración de prototipos; se refiere a la definición de requerimientos necesarios para la planeación y el posterior desarrollo de prototipos, los cuales se presentan al cliente para involucrarlo en el proceso de desarrollo de tal forma que se genere retroalimentación que ayude al buen desarrollo del proyecto. Las tareas que pueden formar parte de éste paso son:

- Investigar del dominio del problema y realizar un informe al respecto.
- Especificar los requerimientos.
- Implementar prototipo (opcional).
- Definir los casos de uso de alto nivel y esenciales.
- Definir el modelo conceptual preliminar (esta tarea se puede aplazar).
- Definir la arquitectura preliminar del sistema (esta tarea se puede aplazar).
- Perfeccionar el plan.

Construcción; es una fase iterativa en el proceso cuyo objetivo es obtener un sistema funcional de software que cumpla con los requerimientos acordados. Para simplificar la posible complejidad que pueda tener el sistema en desarrollo este proceso se elabora en ciclos iterativos. En cada ciclo iterativo la construcción se centra en un caso de uso (o varios, cuando no son muy complejos) o un caso de uso se puede desarrollar en varias iteraciones debido a su complejidad. Las tareas que se realizan son:

- Perfeccionamiento del plan.
- Análisis y diseño
    - Definir los casos de uso
    - Perfeccionar los diagramas de casos de uso
    - Perfeccionar el modelo conceptual
    - Definir los diagramas de secuencia.
    - Definir los diagramas de estado (aplazable)
    - Definir reportes, interfaz del usuario y la secuencia de las pantallas
    - Perfeccionar la arquitectura del sistema
    - Definir los diagramas de interacción
    - Definir los diagramas de diseño de clases (si no se ha hecho).
    - Definir el esquema de la base de datos.
- Implementación.
- Pruebas.

Aplicación; que es la transición de la implantación del sistema a la utilización del mismo.

4.3 Análisis y Diseño

4.3.1 Análisis de Requerimientos

Panorama general

Este proyecto tiene la finalidad de crear un sistema de gestión de redes, que utilice SNMP como protocolo de gestión y que implemente el máximo número posible de funciones de gestión especificadas en la RGT.

Clientes

Pequeñas y medianas empresas.

Metas

En términos generales la meta es lograr tener un mayor control sobre la red de datos utilizando un software especializado, el cual deberá:

- Realizar monitoreo de los diferentes dispositivos de red y verificar su estado.
- Contar con un mapa gráfico de la red.
- Controlar la generación de alarmas visibles en el mapa, cuando eventos que afecten negativamente el desempeño de la red se presenten (fallas, aspectos de desempeño).
- Realizar análisis de desempeño de la red (tráfico, utilización de servidores).
- Generar el menor tráfico de gestión posible.

Funciones del sistema

En la siguiente tabla se describen las funciones clasificándose en categorías, que pueden ser:

- *Evidente*; es decir, que debe realizarse y el usuario debe saber que se ha realizado.
- *Oculta*; es decir, es transparente para el usuario pero debe realizarse (p.e. guardar información en mecanismos persistentes de almacenamiento).
- *Superflua*, ésta es opcional, ya que no repercute significativamente en el costo ni a otras funciones.

Los atributos del sistema son sus características o dimensiones y éstos pueden afectar a todas las funciones o pueden existir atributos por función, en la tabla se toman en cuenta estas últimas y su categoría que puede ser atributos opcionales u obligatorios.

Tabla 6 Funciones Básicas [F1]

Ref.	Función	Categoría de Función	Atributo	Detalles y Restricciones	Categoría de Atributo
F1.1	Manejo del protocolo SNMP v1	Oculta			
F1.2	Exploración de la red en busca de NEs gestionables.	Evidente	Interfaz	Mapa gráfico de la red	Obligatorio

F1.3	Registrar Información de los NEs encontrados como monitoreables	Oculta			
F1.4	Realizar consultas periódicas a los NE por información de gestión.	Oculta			
F1.5	Almacenamiento de información de gestión antes de ser procesada, es decir, los datos brutos obtenidos de los muestreos periódicos sobre los NEs.	Oculta			
F1.6	Procesar información de gestión (Obtener información estadística de datos brutos obtenidos de los muestreos periódicos a los NEs)	Oculta			
F1.7	Presentar información de gestión procesada al administrador de la red.	Evidente	Actualiza-da	Tomar siempre la información de gestión más reciente	Obligatorio
			Interfaz	Usar gráficas o formas que re-presenten cla-ramente el sig-nificado de la información	Obligatorio

Tabla 7 Funciones de gestión de configuración [F2]

Ref.	Función	**Categoría de Función**	**Atributo**	**Detalles y Restricciones**	**Categoría de Atributo**
F2.1	Manejo de la configuración de los parámetros de gestión de desempeño, fallas, seguridad y configuración (p.e.tiempo de espera entre consultas a los NEs, activación / desactivación de alarmas, establecer umbrales de desempeño, etc.)	Evidente	Interfaz	Pantallas basa-das en formas con campos modificables	Obligatorio
F2.2	Registro de parámetros de configuración	Oculta			
F2.3	Control, instalación y puesta en servicio de nuevos elementos de red (Activar, desactivar, realizar pruebas y ordenar autopruebas en NEs)	Evidente			

Tabla 8 Funciones de gestión de desempeño[F3]

Ref.	Función	**Categoría de Función**	**Atributo**	**Detalles y Restricciones**	**Categoría de Atributo**
F3.1	Monitoreo de desempeño de los elementos de red (NEs) mediante la consulta de variables relacionadas con el desempeño (p.e. número de colisiones, número de paquetes perdidos, número de paquetes transmitidos por unidad de tiempo).	Evidente	Interfaz (Bajo solicitud)	Esta informa-ción puede se consultada por el administra-dor cuando lo desee.	Obligatorio

F3.2	Monitoreo de desempeño de la red, mediante la correlación de variables de desempeño de los elementos de red (p.e. ancho de banda utilizado en función del tiempo en diversos segmentos de la red).	Evidente	Interfaz (Bajo solicitud)	Esta información puede se consultada por el administrador cuando lo desee.	Obligatorio
F3.3	Administración y control del tráfico, para asegurar la calidad del funcionamiento (activar/desactivar puertos de un NE, reenrutar el tráfico, etc.)	Evidente			

Tabla 9 Funciones de gestión de fallas y averías [F4]

Ref.	Función	**Categoría de Función**	**Atributo**	**Detalles y Restricciones**	**Categoría de Atributo**
F4.1	Vigilancia de las alarmas configuradas en la función F1.3	Evidente	Interfaz	Alarma visible en el mapa de la red mediante algún cambio de color en el NE en alarma	Obligatorio
F4.2	Localización de fallas, mediante verificación de parámetros, conectividad y pruebas en los elementos de red	Evidente	Interfaz	Localización visible en el mapa de la red	Obligatorio
F4.3	Reparación de fallas (reinicializar enlaces, activar equipo redundante, reenrutar trafico, etc.), cuando sea posible o programar envío de personal	Evidente			
F4.4	Registro de historial de reparación de fallas, para agilizar la solución de fallas similares y llevar control de las fallas de los dispositivos.	Oculta			

Tabla 10 Funciones de gestión de seguridad [F5]

Ref.	Función	**Categoría de Función**	**Atributo**	**Detalles y Restricciones**	**Categoría de Atributo**
F5.1	Prevención de intrusos a los NE y al mismo sistema de gestión	Evidente	Interfaz	Usar clave de autorización de acceso a los NEs	Obligatorio
F5.2	Detección de intrusos a los NE y al mismo sistema de gestión e indicar al administrador de la red sobre manipulaciones indebidas del equipo	Evidente	Interfaz	Usar alarmas de seguridad	Obligatorio
F5.3	Contención de intrusos a los NE y al mismo sistema de gestión.	Evidente	Interfaz	Usar alarmas de seguridad	Obligatorio

Tabla 11 Funciones de gestión de contabilidad [F6]

Ref.	Función	Categoría de Función	Atributo	Detalles y Restricciones	Categoría de Atributo
F6.1	Subscripción / Eliminación de clientes	Evidente			
F6.2	Medición de utilización de servicios por usuario (cliente)	Oculta			
F6.3	Tarificación y fijación de precios de los servicios.	Evidente			
F6.4	Facturación mensual para cada usuario	Evidente			

4.3.2 Casos de uso

Los casos de uso son artefactos del análisis para describir la secuencia de eventos de un actor (agente externo al sistema) que utiliza un sistema para completar un proceso específico. Se describirán los siguientes casos de uso:

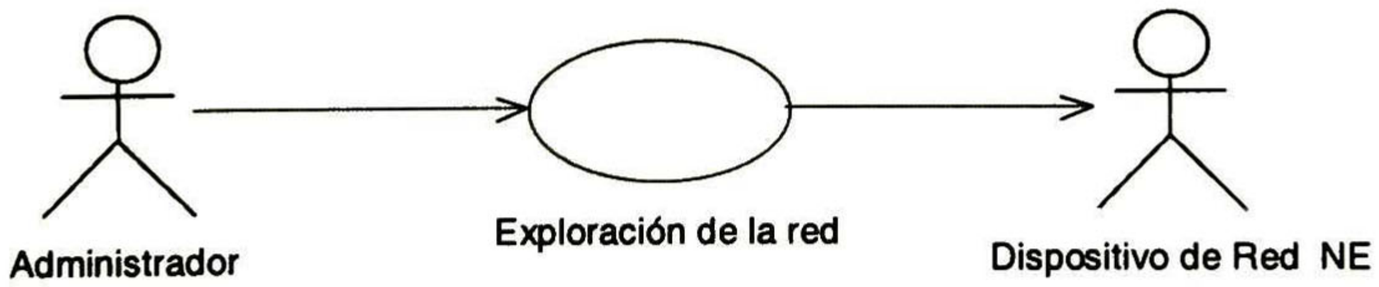
- Iniciar el sistema de gestión.
- Explorar la red.
- Recolectar información de gestión periódicamente de los dispositivos de red.
- Gestionar la calidad de desempeño de la red.
- Gestionar fallas de la red.
- Gestionar configuración de los elementos de red.
- Gestionar la seguridad de la red.
- Gestionar la contabilidad de los servicios ofrecidos por la red.

4.3.2.1 Caso de uso: Iniciar el sistema de gestión.

Actores: Administrador, elementos de red (NEs).

Propósito: La creación de los objetos (instancias de clases) necesarios para que el sistema funcione bien. Inicializar la configuración de parámetros básicos de gestión, bases de datos de NEs monitoreables.

4.3.2.2 Caso de uso: Explorar la red.



Actores: Administrador, elementos de red (NEs).

Propósito: Localizar los elementos de red gestionables, para iniciar los procesos de gestión o para actualizar la lista de NEs gestionables.

Resumen: El administrador de la red realiza una exploración sobre la red que desea gestionar, para localizar NEs monitoreables y les consulta información que generalmente no cambia (Descripción del sistema, dirección IP, localización, etc.) almacena esta información y se genera un mapa gráfico de la red. El administrador también puede modificar algunos parámetros básicos de gestión o dejar los valores asignados por omisión.

Tipo: Primario

Referencias Cruzadas:

- *Funciones*: F1.1, F1.2, F1.3, F1.4, F1.5, F1.6, F1.7. ver [Tabla 6]

Pantalla: Figura 34.

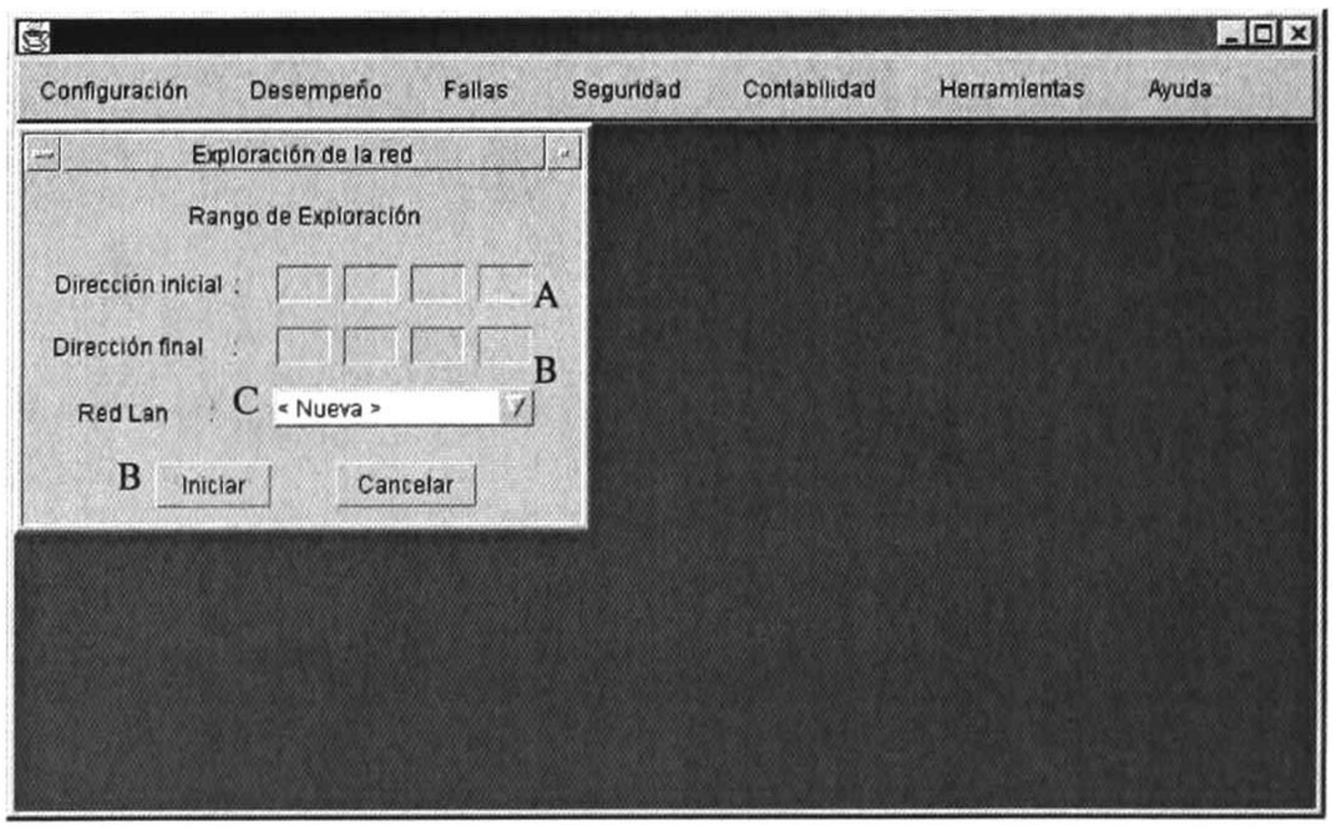


Figura 34. Ventana de exploración de la red

Tabla 12 Curso normal de los eventos exploración de la red

	Acción de los actores	Respuesta del sistema
1	Este caso de uso comienza cuando el Administrador solicita la exploración de la red por elementos que sean monitoreables, introduciendo las direcciones IP inicial [A] y final [B] sobre las cuales se realizará la exploración y si se trata de una nueva LAN o actualizar una LAN existente [C]	
2	El Administrador presiona el botón iniciar [D]	Se planifican todas las direcciones en el rango propuesto
3		Para cada dirección, se crea un mensaje SNMP y se envía, solicitando información de identificación del dispositivo
4	El Administrador puede organizar los iconos que representan los elementos de red.	Por cada NE monitoreable encontrado se despliega un icono que lo represente. Registra los NEs encontrados.

5		Se Registran los NEs encontrados en una base de datos.

Diagrama de colaboración

Los diagramas de interacción explican gráficamente como los objetos interactuan a través de mensajes para realizar las tareas. El siguiente diagrama de colaboración corresponde al de la exploración de la red.

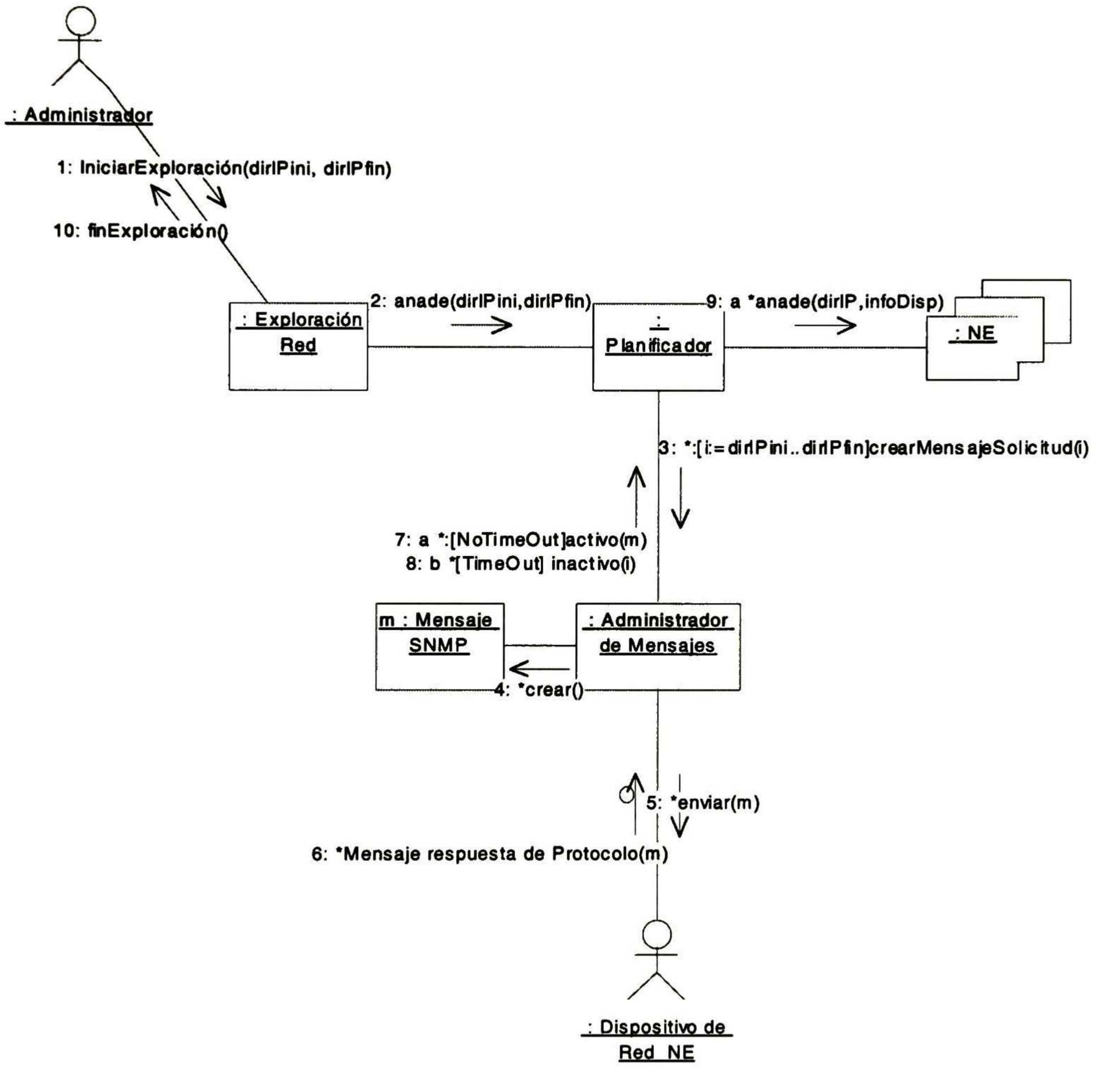


Figura 35. Diagrama de colaboración para exploración de la red

Descripción del diagrama de colaboración:

1- El usuario define el rango de exploración.

2- Se manda un mensaje al planificador con el rango, para que éste envíe solicitudes de descripción a los dispositivos en el rango.

3- Se pasa cada dirección en el rango al administrador de mensajes.

4- El administrador crea un nuevo mensaje SNMP.

5- Envía el mensaje creado al dispositivo.

6- Si el dispositivo responde.

7- El administrador de mensajes informa al planificador que el dispositivo si es gestionable.

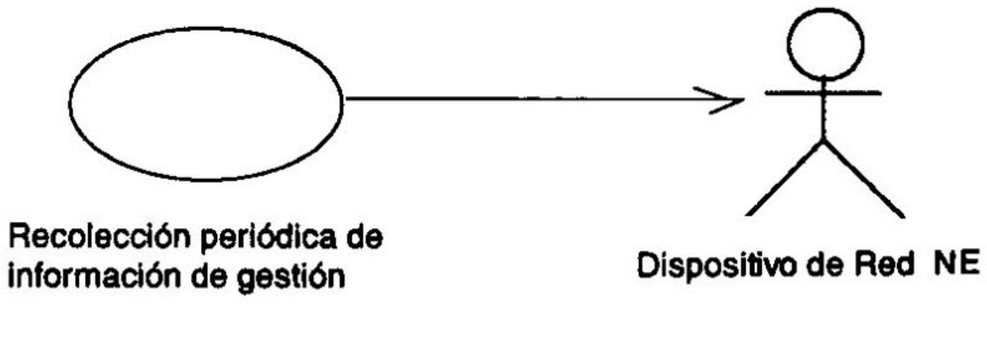
8- Si el dispositivo no responde (time out al mensaje SNMP), se obtiene la siguiente dirección a consultar.

9- Se crea un nuevo NE, con la dirección IP y la información de descripción solicitada.

La interfaz del usuario resultado es: Figura 36.

Figura 36. Mapas de red resultado de la exploración

4.3.2.3 Caso de uso: Recolectar información de gestión periódicamente de los dispositivos de red.



Actores: Elementos de red (NEs).

Propósito: Mantener la información sobre los dispositivos de red, actualizada.

Resumen: Una vez localizados los elementos de red gestionables, el sistema los planifica, es decir, les asigna un orden en el cual estos serán consultados por su información de gestión más reciente y esta información se procesa y/o almacena en la base de datos del sistema de gestión.

Tipo: Primario

Referencias Cruzadas:

- *Funciones*: F1.4, F1.5. ver [Tabla 6]
- *Casos de uso*: El Administrador debe haber terminado el caso de uso Iniciar el sistema de gestión y el de exploración de la red.

Pantalla: Este caso de uso no cuenta con una interfaz, ya que es un proceso interno del sistema.

Tabla 13 Curso normal de los eventos para recolección periódica de información

	Acción de los actores	**Respuesta del sistema**
1		Este caso de uso comienza cuando el proceso de exploración de la red ha terminado o cuando se reinicia el sistema de gestión y se hace una consulta al la base de datos por los elementos de red a planificar
2		El planificador indica al administrador de mensajes el siguiente dispositivo a consultar y que información consultar de el.
3		El administrador de mensajes crea el mensaje de protocolo y lo envía al dispositivo especificado.
4	El dispositivo recibe el mensaje, verifica la autorización, versión, formato y si está correcto asigna valores a las variables contenidas en el mensaje. Envía el mensaje respuesta.	El administrador de mensajes recibe el mensaje respuesta, lo procesa y regresa la lista de variables con sus valores.
5		El planificador indica al administrador de mensajes el siguiente dispositivo a consultar

Cursos alternos:

Línea 4: El dispositivo no recibe el mensaje solicitud o el mensaje respuesta se pierde o si el dispositivo encuentra algún error en el mensaje, el caso de uso termina.

Diagrama de colaboración:

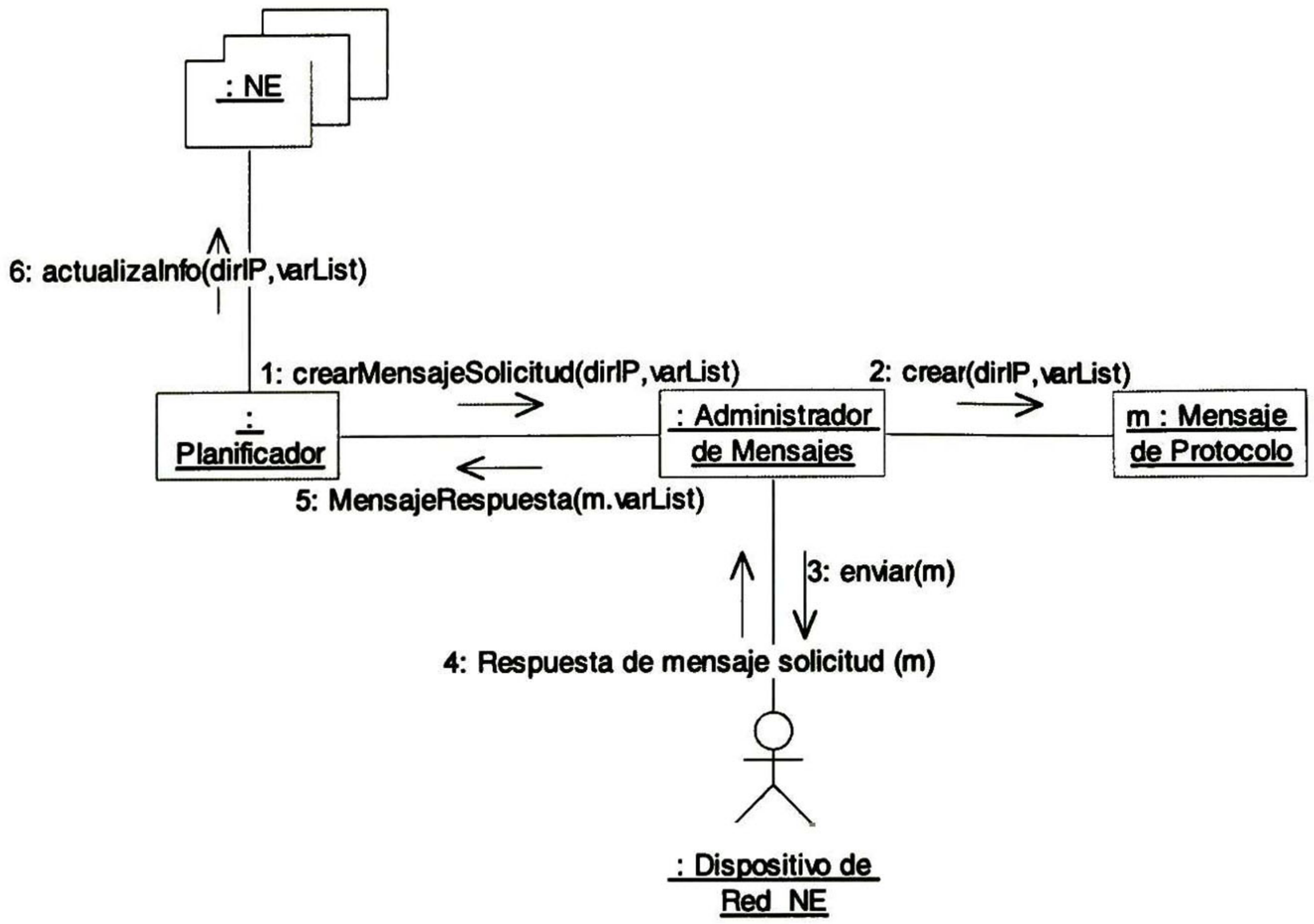


Figura 37. Diagrama de colaboración para la recolección periódica

Descripción del diagrama de colaboración:

1- El planificador solicita al administrador de mensajes solicitar las variables de gestión varList del dispositivo con la dirección IP dirIP.

2- El administrador de mensajes crea un nuevo mensaje SNMP con los valores (dirIP,varList).

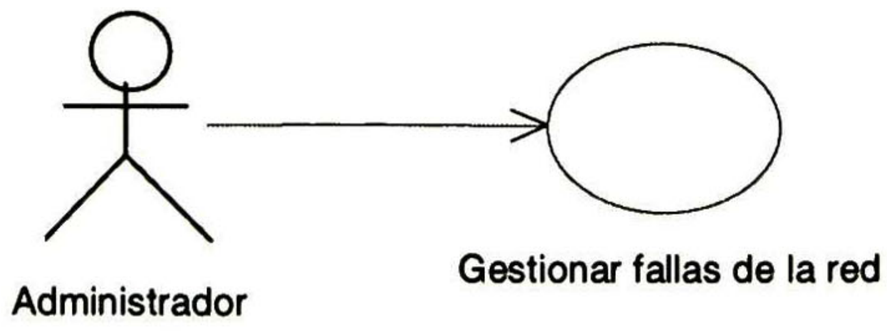
3- El nuevo mensaje SNMP es enviado al dispositivo planificado.

4- El dispositivo responde el mensaje.

5- Los valores de la variables de gestión las obtiene el planificador.

6- Los nuevos valores son actualizados en el elemento de software que representa a los dispositivos.

4.3.2.4 Caso de uso: Gestionar fallas de la red.



Actores: Administrador, NEs.

Propósito: Localizar, aislar y arreglar fallas en la red.

Resumen: Cuando ocurre una falla en la red (algún NE no responde, genera mucho tráfico, algún enlace está saturado o está por saturarse) el sistema de gestión genera alarmas, posteriormente el Administrador se da cuenta de las alarmas, localiza la falla trata de aislarla para tratar de solucionarla (reenrutar tráfico, activar equipo redundante si existe, activar/desactivar puestos de algún dispositivo).

Referencias Cruzadas:

- *Funciones*: F4.1, F4.2, F4.3, F4.4, F1.4, F1.7 ver [Tabla 6][Tabla 9]
- *Casos de uso*: El Administrador debe haber terminado el caso de uso Iniciar el sistema de gestión.

Interfaz: En la Figura 38. se pueden ver los dispositivos en alarma (Amarillo) o en error (Naranja).

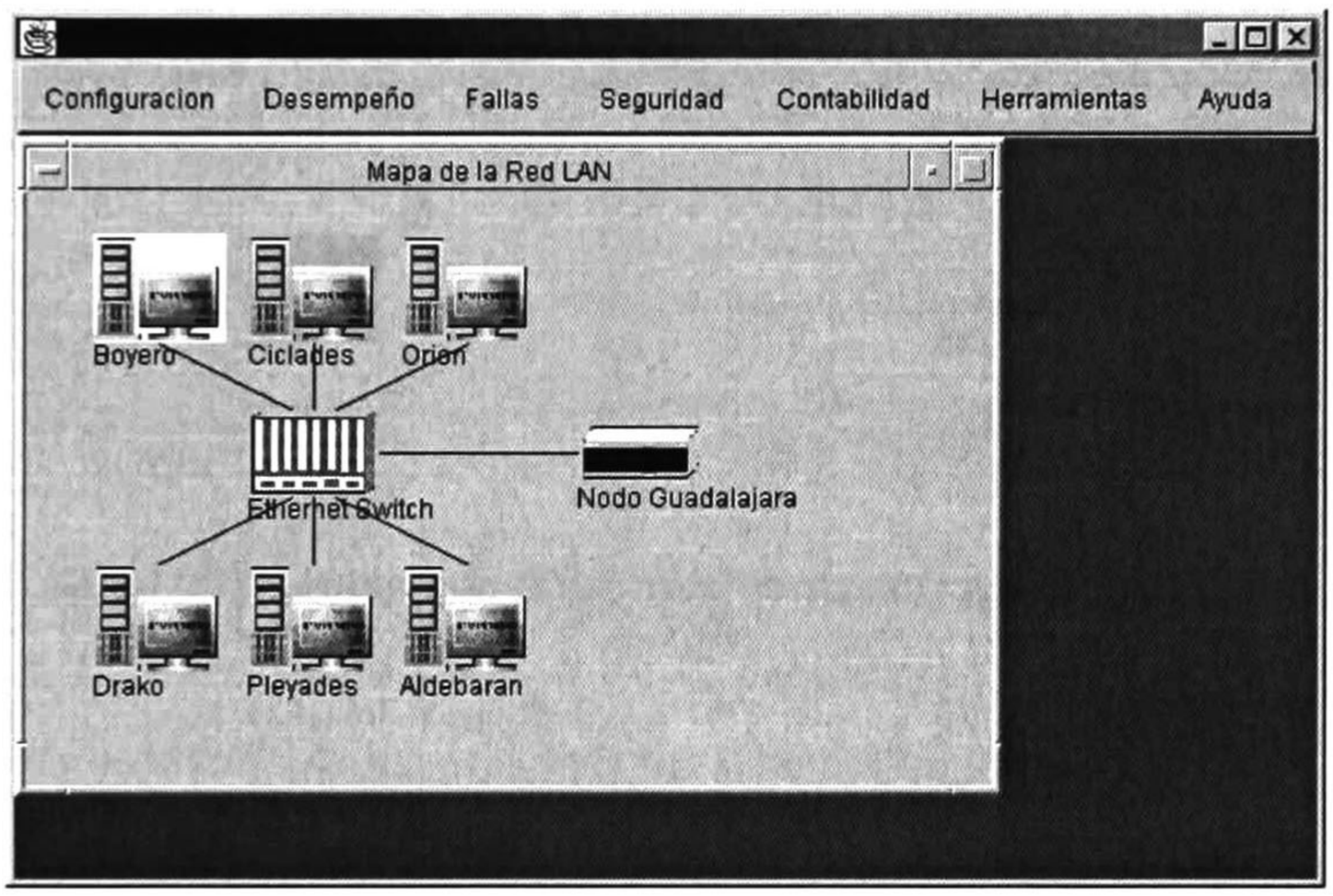


Figura 38. Ventana de fallas y alarmas

Tabla 14. Curso normal de los eventos en gestión de fallas

	Acción de los actores	*Respuesta del sistema*
1		El caso de uso comienza cuando se presenta una falla en algún elemento de red monitoreable, el cual genera un mensaje SNMP Trap y lo envía al sistema gestor. El receptor de traps lo captura, extrae la alarma y lo envía al gestor de fallas el cual posteriormente registra el evento en la LAN a la que pertenece el dispositivo. Este evento se representa gráficamente en el mapa de la LAN correspondiente.
2	El Administrador se da cuenta de las alarmas, localiza la falla y realiza acciones para tratar de aislar la falla (segmentar la red y hacer pruebas en enlaces y NEs).	

3	El administrador verifica que se aisló la falla	
4	El administrador realiza acciones para tratar de arreglar la falla (reenrutar tráfico, activar equipo redundante si existe, activar/desactivar puestos de algún dispositivo).	Confirma la realización de acciones de solución de fallas. Desactiva alarmas (Si se soluciona el problema).
5	El administrador verifica que se solucionó la falla	

Cursos alternos:

Línea 3: El Administrador no logró aislar la falla, programa envío de personal y finaliza el caso de uso.

Línea 5: El Administrador no logró solucionar la falla, programa envío de personal y finaliza el caso de uso.

Diagrama de colaboración:

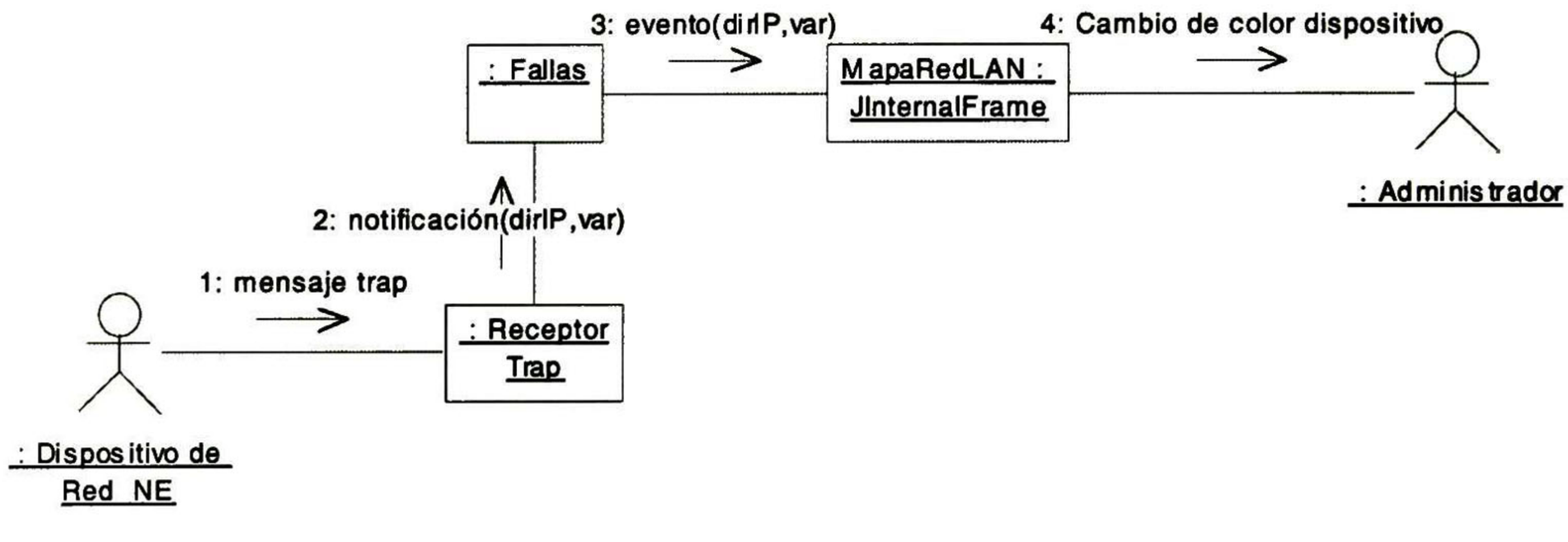
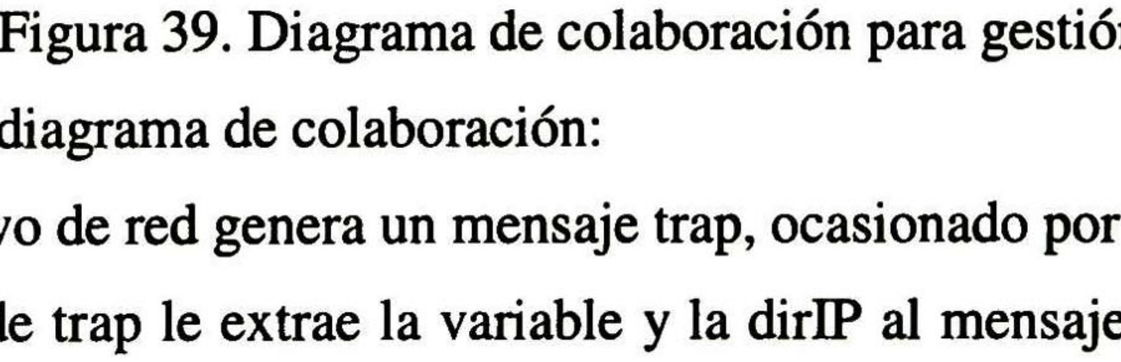


Figura 39. Diagrama de colaboración para gestión de fallas

Descripción del diagrama de colaboración:

1- Un dispositivo de red genera un mensaje trap, ocasionado por un problema en el mismo.
2- El receptor de trap le extrae la variable y la dirIP al mensaje y lo notifica a gestión de fallas.
3- Fallas lo añade a la lista de eventos de la LAN a la que corresponde.
4- El mapa de red LAN muestra gráficamente con un cambio de color en el dispositivo en el que ocurrió la alarma o error.

4.3.2.5 Caso de uso: Gestionar desempeño de la red.



Actores: Administrador, NEs.

Propósito: Monitorear el desempeño de la red y elementos de la red, para poder evaluarlo y controlarlo cuando sea posible. La información que generada por la gestión de la calidad de desempeño de la red ayuda al administrador a la planificación de la misma.

Resumen: El administrador de la red solicita información (información que periódicamente el sistema consulta y procesa, para monitorear los NEs) sobre el desempeño de la red y toma decisiones (reenrutar tráfico, activación / desactivación de puertos de NEs) para controlarlo cuando sea posible.

Referencias Cruzadas:

- *Funciones*: F3.1, F3.2, F3.3, F1.4, F1.7 ver [Tabla 6][Tabla 8]
- *Casos de uso*: El Administrador debe haber terminado el caso de uso Iniciar el sistema de gestión.

Interfaz: En la Figura 38. se puede ver el desempeño de 2 interfaces de un dispositivo

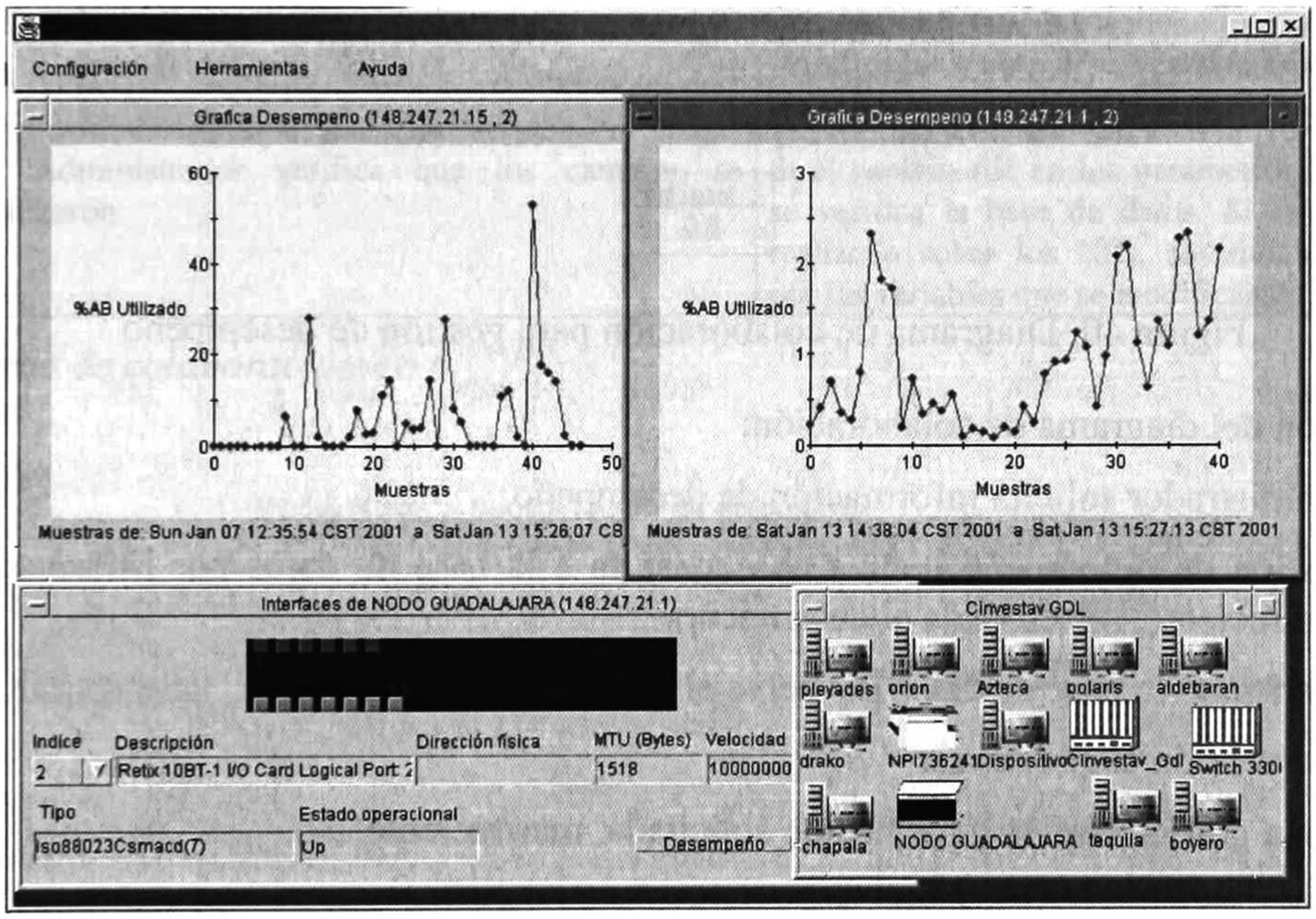


Figura 40. Pantalla de desempeño, ancho de banda utilizado

Tabla 15. Curso normal de los eventos para gestión de desempeño de la red

	Acción de los actores	Respuesta del sistema
1	Este caso de uso comienza cuando el administrador solicita información de desempeño de la red.	Presenta gráficas y datos de desempeño de la red.
2	El Administrador evalúa las gráficas y decide solicitar información de desempeño de algún(os) NEs.	Presenta gráficas y datos de desempeño de los elementos de red requeridos.
3	El Administrador decide cambiar algunos parámetros relacionados al desempeño de la red (umbrales, acciones sobre NEs, reenrutar tráfico)	Registra los cambios y los aplica a las siguientes consultas periódicas que continuamente el sistema realiza para monitorear el desempeño.

Cursos alternos:

Línea 2: El Administrador no desea más información de desempeño y termina el caso de uso.

Línea 3: El Administrador no desea modificar parámetros de gestión de desempeño y termina el caso de uso.

Diagrama de colaboración:

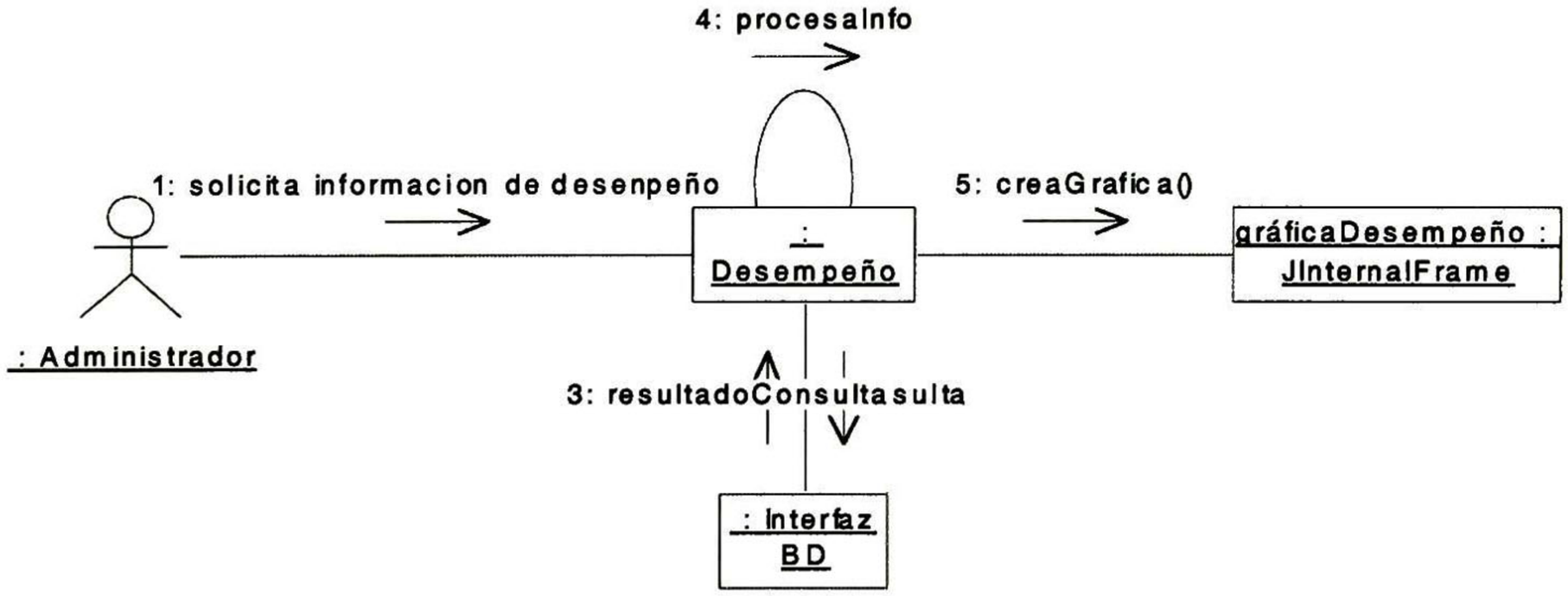
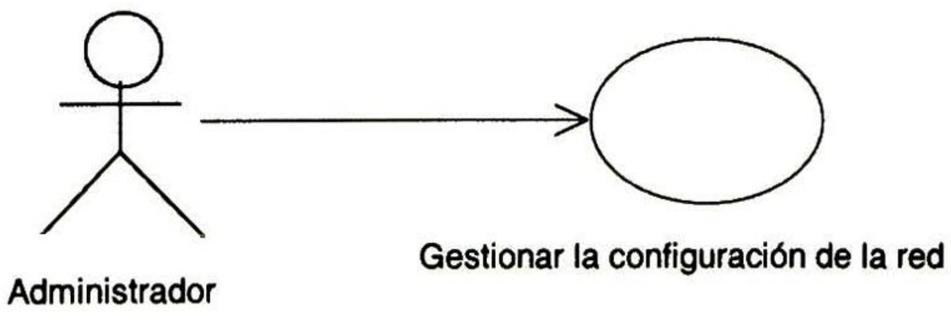


Figura 40. Diagrama de colaboración para gestión de desempeño

Descripción del diagrama de colaboración:

1- El administrador solicita información de desempeño.
2- La gestión de desempeño realiza una consulta a la base de datos por información de gestión reciente, relacionada al desempeño.
3- La interfaz de la base de datos devuelve el resultado de la consulta
4- La información es procesada.
5- Crea una gráfica con la información solicitada, mas reciente.

4.3.2.6 Caso de uso: Gestionar configuración.



Actores: Administrador, NEs.

Propósito: Gestionar los parámetros de configuración de los NEs (parámetros que controlan el estado de los NEs).

Resumen: El administrador realiza algún cambio en la configuración actual de la red (añadir o quitar NEs, añadir o suspender servicios) o de los parámetros de gestión (periodo de consulta a los elementos de red), los cambios son registrados en el sistema y aplicados.

Referencias Cruzadas:

- *Funciones*: F2.1, F2.2, F2.3, F1.4, F1.7 ver [Tabla 6] [Tabla 7]
- *Casos de uso*: El Administrador debe haber terminado el caso de uso Iniciar el sistema de gestión.

Tabla 16. Curso normal de los eventos para gestionar la configuración

	Acción de los actores	Respuesta del sistema
1	El caso de uso comienza cuando el Administrador realiza un cambio en la configuración de los elementos de red o en los parámetros con los que se realiza la gestión.	Si el cambio es en los parámetros de control del sistema, éste los aplica y los registra en la base de datos. Si se cambió la configuración de uno o más dispositivos, las solicitudes se mandan al planificador y éste a su vez al administrador de mensajes y las solicitudes de cambio se envían.
2	El Administrador verifica que los cambios se realizaron	Si el cambio fue en los parámetros del sistema, se verifica la base de datos. Si el cambio fue realizado sobre los NEs, se envían solicitudes por las variables que se modificaron.

Diagrama de colaboración:

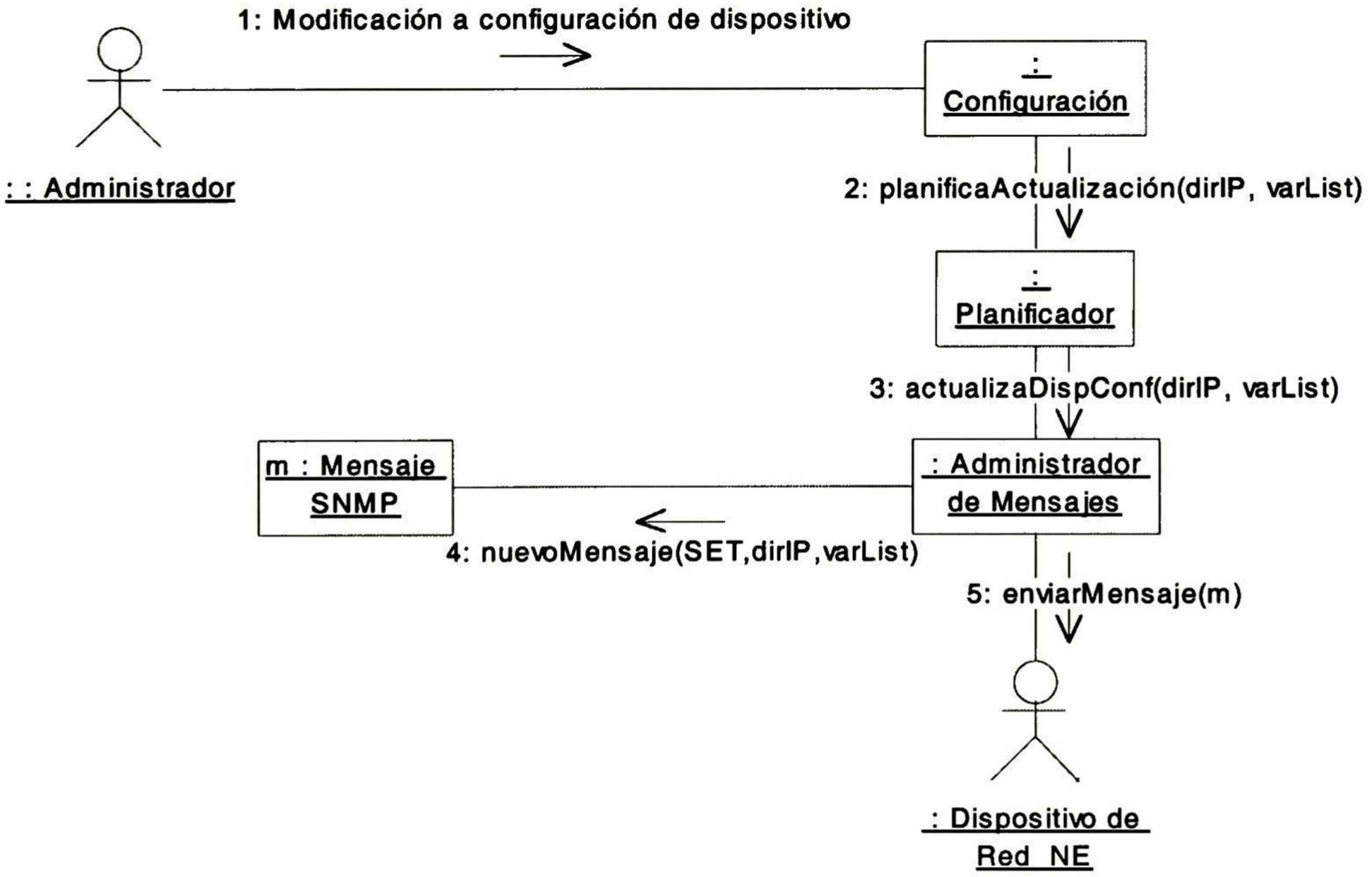


Figura 41. Diagrama de colaboración para la gestión de la configuración

Descripción del diagrama de colaboración:

1- El administrador realiza modificaciones a la configuración de los dispositivos (p.e. activar o desactivar una interfaz, modificaciones de ruteo), modificaciones que son manejadas por la función de gestión de configuración.

2- Se manda al planificador la solicitud para planificar las modificaciones al dispositivo con dirección IP y las variables a modificar en éste dispositivo.

3- El planificador pasa los parámetros al Administrador de Mensajes.

4- Este crea un nuevo mensaje SNMP.

5- El mensaje de modificación de variables se envía al dispositivo.

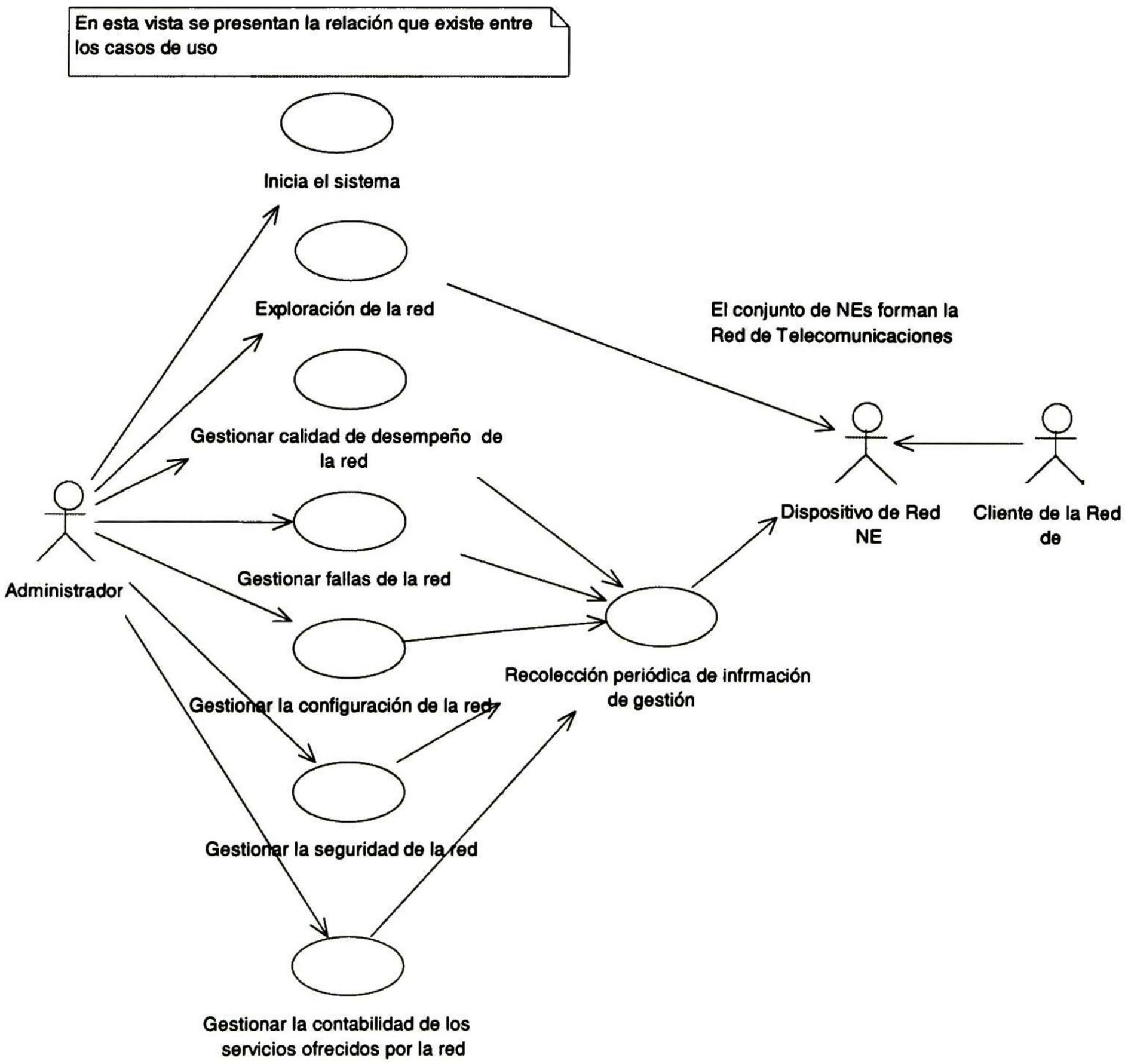


Figura 42. Relación entre los casos de uso

4.3.3 Modelo conceptual

Es una representación de los conceptos principales del problema y permite concentrarse en el dominio del mismo y no en las entidades de software. Un modelo conceptual muestra:

- Conceptos.
- Asociaciones entre los mismos; que indica alguna conexión significativa entre ellos.
- Atributos de éstos; que son valores lógicos de datos de los conceptos.
- Multiplicidad que los relaciona (p.e. 1 a 1,1 a muchos, etc.).

En UML se emplean los términos "clase" y "tipo" en lugar de "concepto". El término "interfaz" es usado para un conjunto de operaciones visibles en el exterior para las clases que la utilice (p.e. *Runnable* en Java). La finalidad principal de un modelo conceptual es, además de cumplir con los requerimientos establecidos, comunicar claramente una comprensión esencial de los conceptos importantes en el dominio del problema.

Las relaciones entre conceptos se leen de arriba hacia abajo o de izquierda a derecha (p.e. Mensaje de protocolo es usado por el administrador de mensajes).

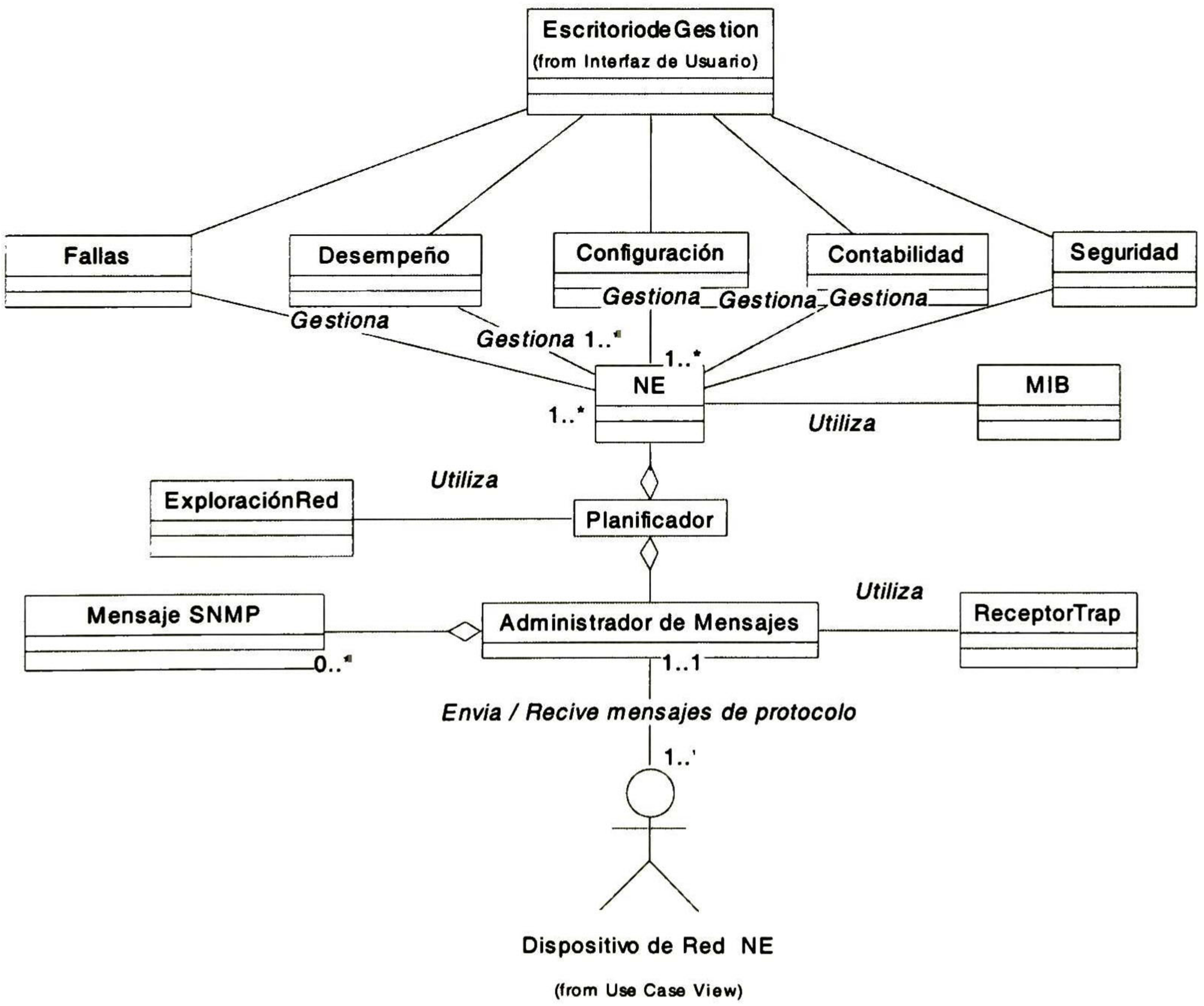


Figura 43. Modelo conceptual

En el diagrama anterior se puede ver el modelo conceptual al problema de gestión. Este modelo se basa en la separación de los conceptos relacionados con la interfaz gráfica, con el dominio del problema y la información manejada (modelo vista - controlador). En éste caso particular la vista esta representada en el modelo por la clase *Escritorio de Gestión* y el controlador por las funciones de gestión, el planificador y las clases que se relacionan con éstos.

Las clases fallas, desempeño, configuración, contabilidad, seguridad, gestionan a los elementos de red (NE, Network Elements), los cuales son consultados periódicamente en un orden manejado por el planificador. Este ultimo contiene un administrador de mensajes SNMP que oculta la complejidad del manejo del protocolo SNMP e inicia un hilo de programación para la recepción de traps (notificaciones).

La exploración de la red es solicitada por el usuario del sistema y se comunica directamente con el planificador para que realice la búsqueda de dispositivos gestionables.

4.3.4 Diagramas de clase y herencia

4.3.4.1 Clases relacionadas con la interfaz de usuario

La interfaz de usuario es completamente gráfica implementada por la clase EscritorioGestion, la cual hereda de la clase JFrame y contiene como atributo una instancia de la clase JDesktopPane. Esta última proporciona una presentación de escritorio (virtual desktop) como contenedor de múltiples documentos o ventanas internas (instancias de JInternalFrame), éstas son usadas tanto para desplegar como para pedirle información al usuario.

El mapa de la red WAN y los de las LANs hacen uso de iconos (instancias de la clase Image) para representar a los dispositivos gestionados y su estado actual (activo, alarmado o en error). De ésta forma el sistema proporciona al administrador de red, la localización de los problemas o fallas para posteriormente tomar una decisión.

La interfaz de usuario hace uso de otras clases como [10] JTextField, JComboBox, JMenuBar, JMenuItem, JPopupMenu, las cuales ayudan a que ésta sea más amigable. También se utilizan *oyentes de eventos* (event listeners) los cuales detectan acciones (de mouse, teclado, menús, abrir o cerrar ventanas) del usuario sobre las diferentes ventanas y sus componentes con la finalidad de realizar *validaciones*, *llamadas a otras ventanas, invocación de métodos* y mejoramiento la interacción hombre - sistema.

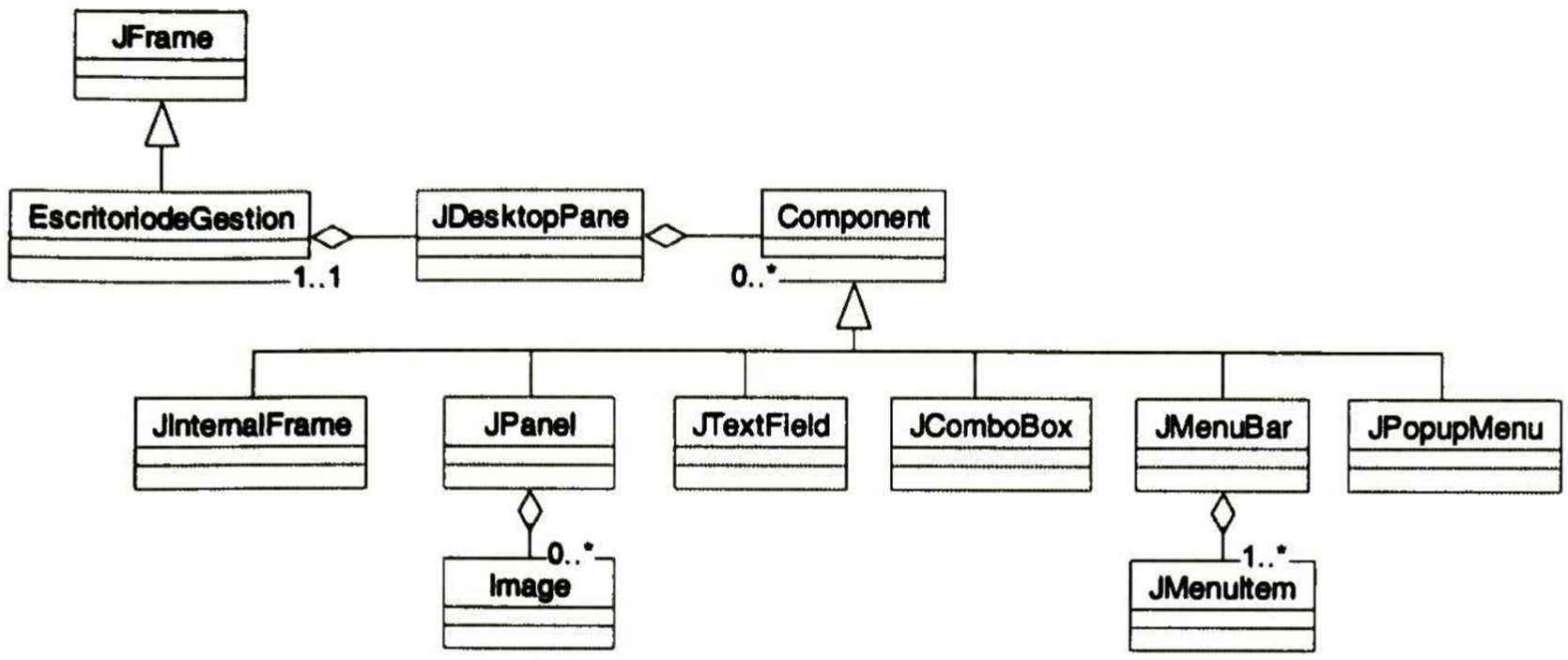


Figura 44. Diagrama de clases para el paquete de interfaz de usuario

4.3.4.2 Clases relacionadas con las funciones de gestión

Las funciones de gestión (fallas, configuración y desempeño), se encargan del procesamiento y correlación de la información de gestión consultada a los dispositivos de tal forma que pueda ser valiosa para el administrador en la toma de decisiones, ejemplo de esta información son los registros históricos de *ancho de banda* utilizado y *estadísticas referentes a mensajes de diferentes protocolos*, (IP, ICMP, UDP, TCP) que nos indican el total de mensajes manejados, mensajes desechados por contener errores en header o debido a que el buffer del dispositivo se encuentra lleno, en un determinado periodo de tiempo.

Las funciones de gestión utilizan a clases como *Planificador*, el cual lleva el control de quien es el siguiente elemento de red a ser consultado, las variables que deben ser consultadas y proporcionar los valores de éstas a la función de gestión correspondiente. La clase *AdministradorMensajes* oculta los detalles de implementación del protocolo y se encarga de crear, enviar y recibir mensajes de protocolo SNMP, esta clase está instanciada en la clase *Planificador*. Las funciones de gestión, el planificador y el receptor de traps serán hilos de programación.

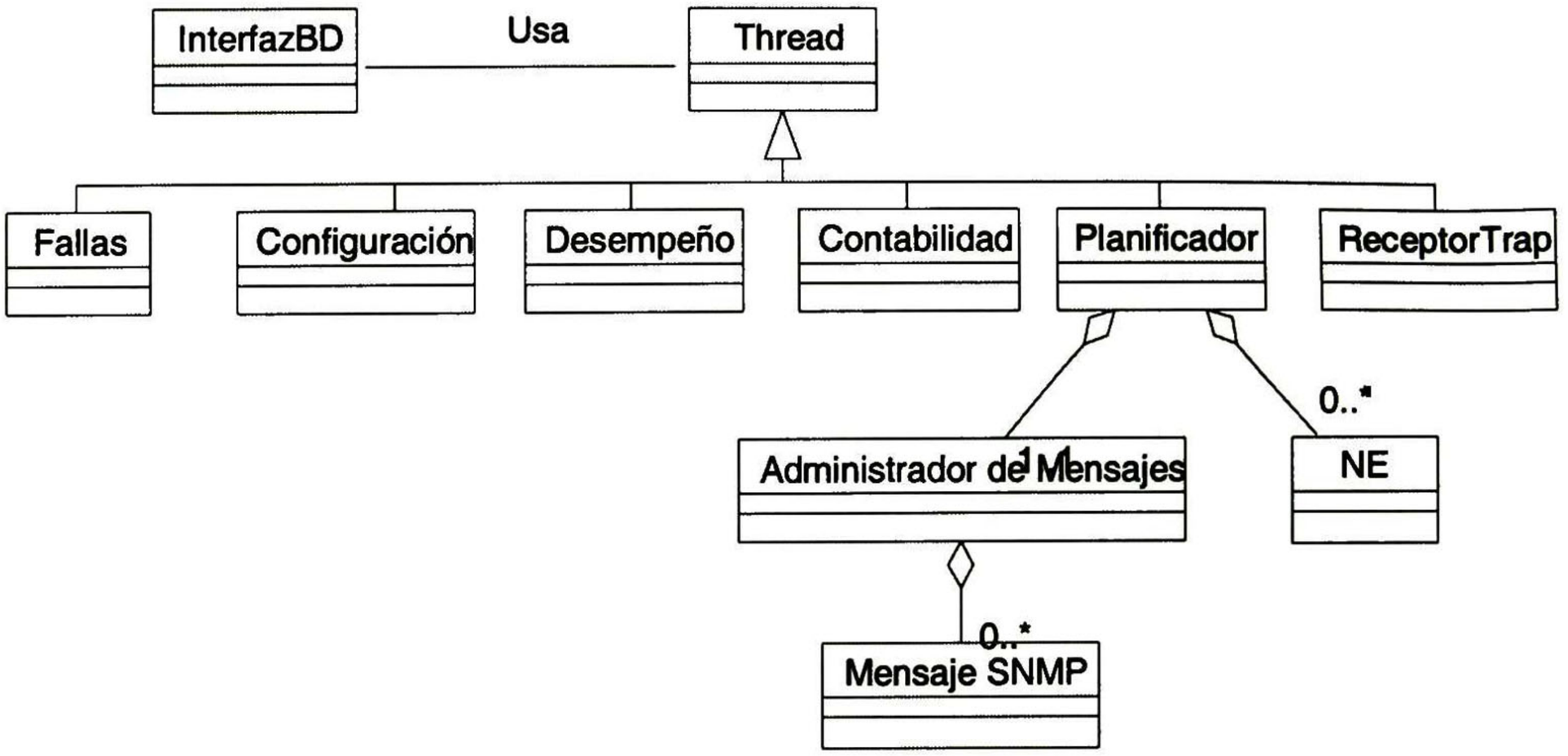


Figura 45. Diagrama de clases relacionadas con las funciones de gestión

4.3.4.3 Clases relacionadas con el protocolo SNMP

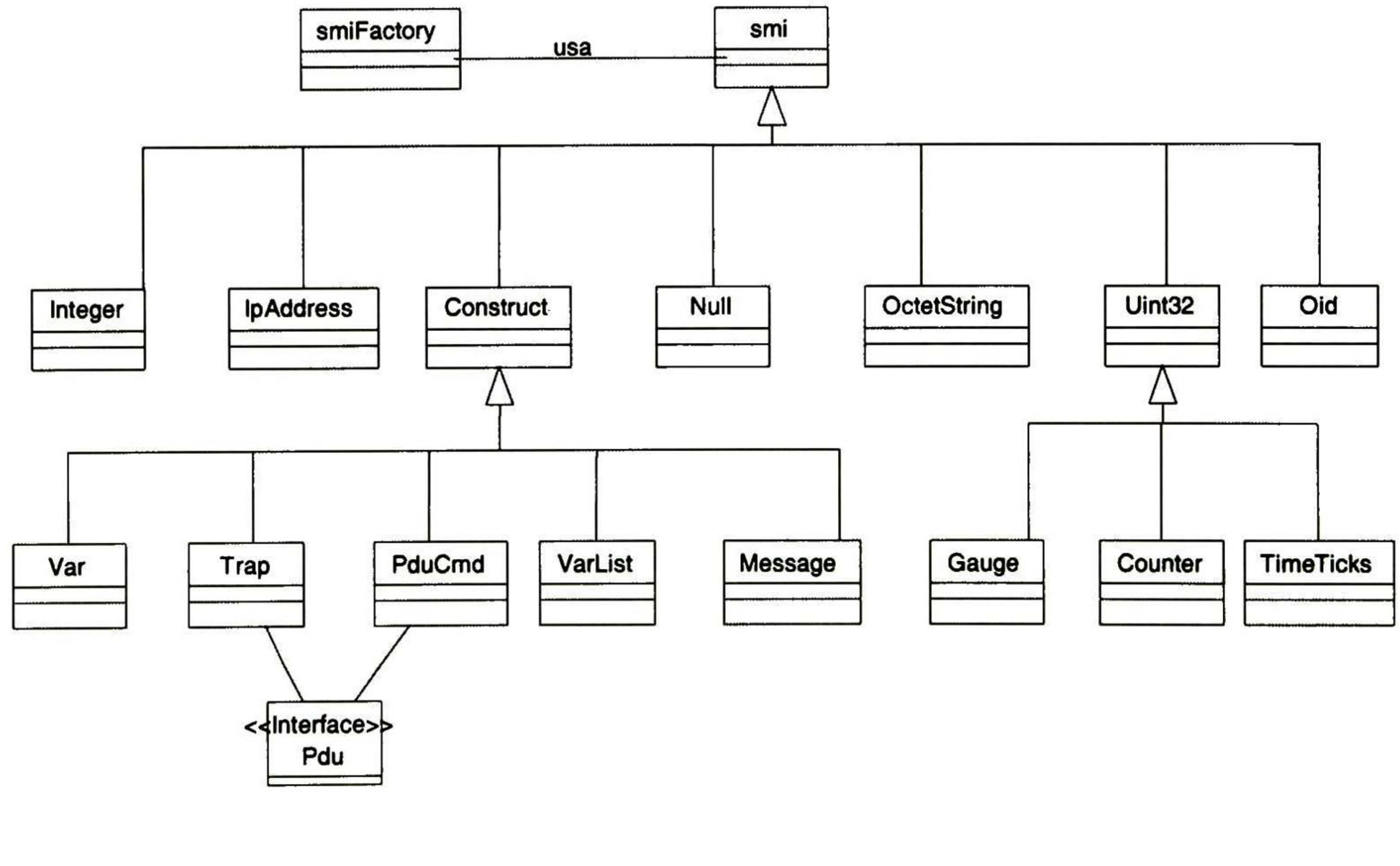


Figura 46. Diagrama de clases del protocolo SNMP

4.3.5 Esquema de la base de datos

4.3.5.1 Diseño de base de datos relacional para un sistema de gestión

En esta sección se describe el diseño de la *base de datos para un sistema de gestión*. Se hace uso de los *modelos entidad – relación y relacional* para describir la estructura lógica de la base de datos, es decir, primero se realiza el modelo entidad – relación para el sistema y posteriormente se hace una transformación al modelo relacional. Se eligieron éstos modelos debido a que son modelos muy flexibles, son los más comunes y no son tan complejos en su diseño e implementación como el modelo orientado a objetos. El proceso para el diseño de una base de datos es el siguiente [13]: se realiza una lista de relaciones de datos la información que deberá manejar el sistema, se realiza el proceso de normalización sobre las relaciones encontradas, se hace una transformación de éste modelo entidad relación que representa al sistema al modelo relacional, lo cual es casi directo, para posteriormente realizar el análisis, diseño e implementación de la aplicación que manejará ésta base de datos. En el presente documento se describe el modelo entidad – relación para poder entender el esquema lógico de la base de datos.

Tabla 17. Relaciones

Relación	Llave
DISPOSITIVOS	DirIP
INTERFACES	(DirIP , InterfazIdx)
DESCRIPCIONINTERFAZ	TipoInterfaz
ESTADOINTERFAZ	Estado
IP	(DirIP, Fecha)
ICMP	DirIP
TCP	DirIP
UDP	DirIP
EGP	DirIP
SNMP	DirIP
TABLARUTEO	DirIP
ESTADISTICASETHERNET	(DirIP, etherstatIdx, etherStatsFuente)
CONTROLHISTORICOS	(DirIP, histctlIdx, histctlFuente)
HISTORICOETHERNET	(DirIP , etherHistIdx)
ALARMA	(DirIP , alarmIdx)
CONTROLHOST	(DirIP, hostctlIdx)
HOST	(DirIP, hostIdx)
EVENTOS	(DirIP , eventIdx)

4.3.5.2 Modelo Entidad – Relación

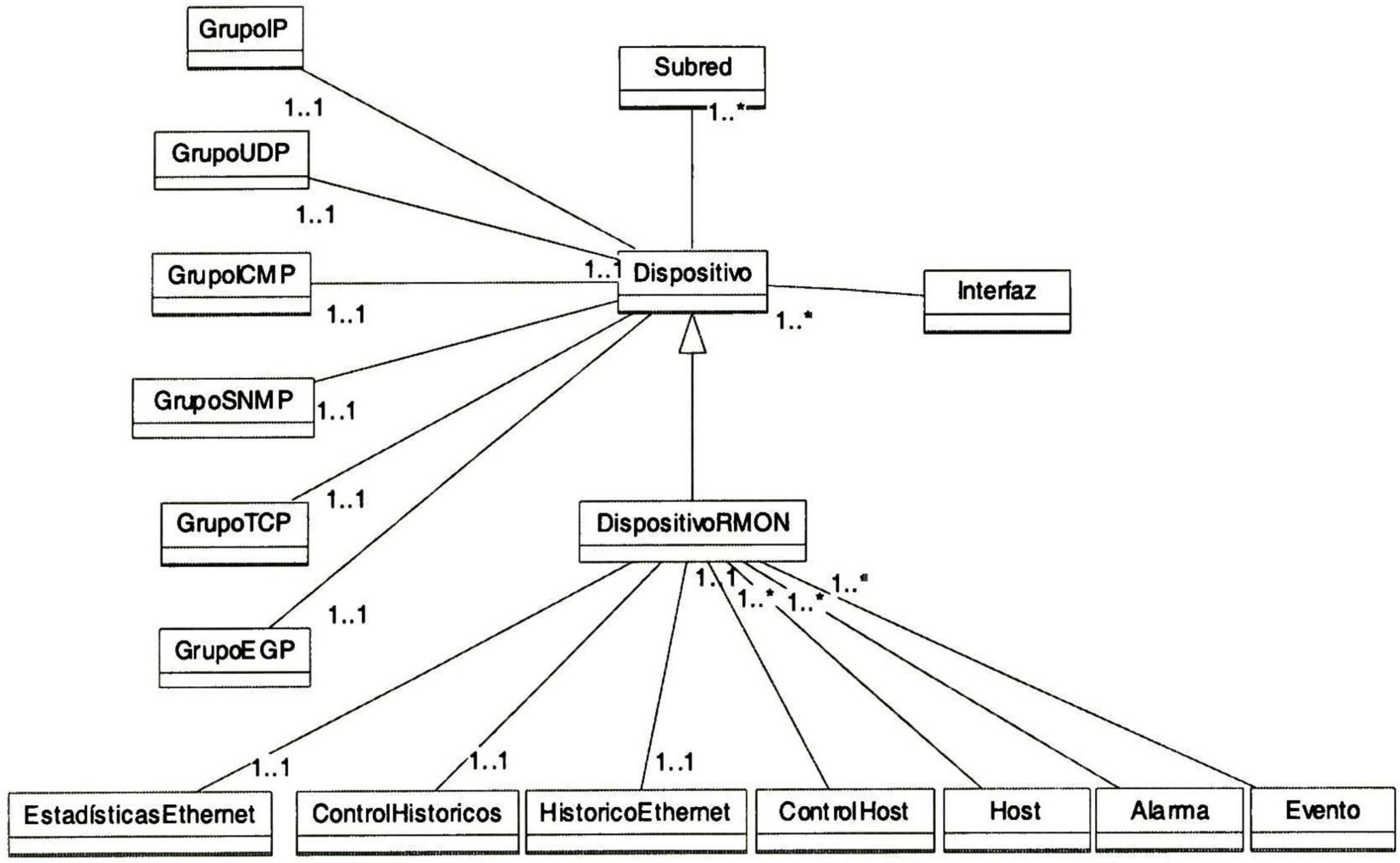


Figura 47. Modelo entidad - relación para un sistema de gestión

4.3.5.3 Relaciones que representan el modelo entidad relación

Los nombres de los campos en las relaciones están de acuerdo con los nombres de las variables encontradas en los MIB's de los dispositivos. Se subraya la llave y se añaden los atributos de las relaciones.

Tabla 18. Relaciones con atributos

Relaciones	Atributos
DISPOSITIVO	DirIP, disDescripcion, disNombre, disLocalizacion, disContacto, disServicios, disNumInterfaces
INTERFAZ	DirIP, ifidx, ifDescripcion,ifTipo, IfMtu, ifVelocidad, ifDirFisica, ifAdminEstado, ifOperEstado, ifUltimoCambio, ifOctetosEntrada, ifUcastPktsEntrada, ifNUcastPktsEntrada, ifDescartadosEntrada, ifErroresEntrada, ifProtocoloDescEntrada, ifOctetosSalida, ifUcastPktsSalida, ifNUcastPktsSalida, ifDescartadosSalida, ifErroresSalida, ifLongitudColaSalida, ifSpecific,
INTERFAZTIPO	TipoInterfaz, iftipoDescripcion
ESTADOINTERFAZ	EstadoInterfaz, ifEdoDescripción
IP	DirIP, EstampaTiempo,ipesGateway, ipTTL,ipRecividos, ipErrorHdr, ipErrorDir, ipDatagramasForw, ipProtoDesc, ipDescartadosEntrada,ipEntregados, ipDescartadosSalida, ipNoRuta,

	ipTiempoReensamble, ipSolicitudesReensamble, ipReensamblesOK, ipReensamblesFallos, ipFragsCreados, ipRuteosDescartados
TABLARUTEO	DirIP, ipRutDest, ipRutIfIndex, ipRutMetric1, ipRutMetric2, ipRutMetric3, ipRutMetric4, ipRutSigSalto, ipRutTipo, ipRutProto, ipRutAge, ipMascaraRuteo, ipRutMetric5
ICMP	DirIP, EstampaTiempo,icmpMensajesEntrada, icmpMensErrorEntrada, icmpDestNoEncontradoEntrada, icmpTiempoExecEntrada, icmpProbParamEntrada, icmpMensajesSalida, icmpMensErrorSalida, icmpDestNoEncontradoSalida, icmpTiempoExecSalida, icmpProbParamSalida
TCP	DirIP, EstampaTiempo,tcpAlgoritmoRto, tcpRtoMin, tcpRtoMax, tcpMaxConexiones, tcpActivoAbiertas, tcpPasivoAbiertas, tcpIntentosFallos, tcpEstabReset, tcpEstabActualmente, tcpSegEntrada, tcpSegSalida, tcpSegRetrans
UDP	DirIP, EstampaTiempo,udpDatagramasEntrada, udpSinPuertos, udpErroresEntrada, udpDatagramasSalida
EGP	DirIP, EstampaTiempo, egpMensajesEntrada, egpErroresEntrada, egpMensajesSalida, egpErroresSalida, egpAs
SNMP	DirIP, EstampaTiempo smnpPktsEntrada, snmpPktsSalida, snmpErrorVersEntrada, snmpErrorCommunityNameEntrada, snmpErrorCommunityUsesEntrada, snmpParseErrorEntrada, snmpTooBigEntrada, snmpNoSuchNameEntrada, snmpBadValuesEntrada, snmpReadOnlyEntrada, snmpGenErrEntrada, snmpTotVarsGetEntrada, snmpTotVarsSetEntrada, snmpGetRequestEntrada, snmpGetNextEntrada, snmpSetRequestEntrada, snmpGetResponsesEntrada, snmpTrapsEntrada, snmpTooBigSalida, snmpNoSuchNameSalida, snmpBadValuesSalida, snmpReadOnlySalida, snmpGenErrSalida, snmpGetRequestSalida, snmpGetNextSalida, snmpSetRequestSalida, snmpGetResponsesSalida, snmpTrapsSalida,snmpAutorizaTraps
ESTADISTICAS ETHERNET	DirIP, etherstatsIdx etherStatsFuente (relacionado con indice de interfaz), etherStatsEventosDrop, etherStatsOctetos, etherStatsPkts, etherStatsPktsBroadcast, etherStatsPktsMulticast, etherStatsErroresAlineacionCRC, etherStatsPktsUndesize, etherStatsPktsOversize, etherStatsFragmentos, etherStatsJabbers, etherStatsColisiones, etherStatsPkts64Octetos, etherStatsPkts65to127Octetos, etherStatsPkts128to255Octetos, etherStatsPkts256to511Octetos, etherStatsPkts512to1023Octetos, etherStatsPkts1024to1518Octetos, etherStatsPropietario, etherStatsEstado,
CONTROL HISTORICO	DirIP, histctlIdx, histctlFuente, histctlBucketsSolicitados, histctlBucketsAdmitidos, histctlIntervalo, histctlPropietario, histctlBucketsEstado
HISTORICO ETHERNET	DirIP etherHistIdx (Relacionado con histctlIdx), etherHistIdxMuestra, etherHistComienzoIntervalo, etherHistEventosDrop, etherHistOctetos, etherHistPkts, etherHistBroadcastPkts, etherHistMulticasPkts, etherHistErroresAlineacionCRC, etherHistPktsUndesize, etherHistPktsOversize, etherHistFragmentos, etherHistJabbers, etherHistColisiones, etherHistUtilizacion
ALARMA	DirIP , alarmIdx, alarmIntervalo, alarmVariable, alarmTipoMuestreo, alarmValor, alarmComiezoAlarma, alarmUmbralSuperior, alarmUmbralInferior, alarmEventoUmbralSuperior, alarmEventoUmbralInferior, alarmPropietario, alarmEstado

CONTROLHOST	DirIP, hostctlIdx , hostctlFuente, hostctlTamanoTabla, hostctlUltimoBorrado, hostctlPropietario, hostctlEstado
HOST	DirIP, hostIdx, hostDireccion, hostOrdenCreacion, hostPktsEntrada, hostPktsSalida, hostOctetosEntrada, hostOctetosSalida, hostErroresSalida, hostPktsBroadcastSalida, hostPktsMulticastSalida
EVENTOS	DirIP , eventIdx , eventDescripcion, eventTipo, eventCommunity, eventUltimoEnvio, eventPropietario, eventEstado

4.3.5.4 Diccionario de Datos

Tabla 19. Diccionario de datos

	Tipo	Descripción
DISPOSITIVO	Relación	Relación donde que contiene las características y descripción del dispositivo gestionable (Elemento de red)
DirIP	Atributo	Representa la dirección IP del dispositivo gestionable.
DisDescripcion	Atributo	Representa la descripción del dispositivo (nombre, versión, tipo de hardware).
DisNombre	Atributo	Representa el nombre asignado por el administrador a éste nodo
DisLocalizacion	Atributo	Localización física del nodo
DisContacto	Atributo	Identificación de la persona a contactar para éste nodo gestionado, junto con información de cómo contactarla.
DisServicios	Atributo	Representa un valor que indica el conjunto de servicios, que ésta entidad ofrece principalmente.
DisNumInterfaces	Atributo	Número de interfaz con las que cuenta esta entidad
INTERFAZ	Relación	Relación que agrupa las interfaces por dispositivo gestionable
Ifidx	Atributo	Valor que identifica una interfaz en un dispositivo
IfDescripcion	Atributo	Información sobre la interfaz
IfTipo	Atributo	Tipo de interfaz de acuerdo con el protocolo de enlace o físico
IfMtu	Atributo	Tamaño del datagrama más largo que puede ser enviado o recibido por esta interfaz (Maximun transfer unit)
if Velocidad	Atributo	Estimado del ancho de banda actual de la interfaz
IfDirFisica	Atributo	La dirección de la interfaz en la capa de protocolo inmediatamente inferior a la capa de red en el stack
IfAdminEstado	Atributo	El estado deseado de la interfaz (up, down, testing)
IfOperEstado	Atributo	El estado de operación actual de la interfaz
IfUltimoCambio	Atributo	El valor de SysUpTime cuando se modificó el estado de operación de la interfaz
ifOctetos Entrada	Atributo	El número total de octetos recibidos en la interfaz

IfUcastPktsEntrada	Atributo	El número de paquetes unicast entregados a un protocolo de más alto nivel
IfNUcastPktsEntrada	Atributo	El número de paquetes no unicast entregados a un protocolo de más alto nivel
IfDescartadosEntrada	Atributo	El número de paquetes descartados
IfErroresEntrada	Atributo	El número de paquetes de entrada con errores
IfProtocoloDescEntrada	Atributo	El número de paquetes descartados por usar protocolo desconocido
IfOctetosSalida	Atributo	El número total de octetos transmitidos fuera de la interfaz
IfUcastPktsSalida	Atributo	El número de paquetes que protocolos de más alto nivel solicitaron enviar a una dirección unicast
IfNUcastPktsSalida	Atributo	El número de paquetes que protocolos de más alto nivel solicitaron enviar a una dirección no unicast
IfDescartadosSalida	Atributo	El número de paquetes descartados en la salida
IfErroresSalida	Atributo	El número de paquetes de salida con errores
ifLongitudColaSalida	Atributo	Longitud de la cola de paquetes de salida del dispositivo
IfSpecific	Atributo	Referencia a MIB
INTERFAZTIPO	Relación	Describe el tipo de interfaz relacionada con el protocolo de la capa de enlace o físico.
TipoInterfaz	Atributo	Identificador del tipo de interfaz
IftipoDescripcion	Atributo	Descripción del tipo de interfaz
ESTADOINTERFAZ	Relación	Describe el estado en el que se encuentran las interfaces de un dispositivo
EstadoInterfaz	Atributo	Identificador de estado
IfedoDescripción	Atributo	Descripción del estado de la interfaz
IP	Relación	Relación con información de mensajes IP que ha manejado el dispositivo
ipesGateway	Atributo	Indica si esta entidad funciona como Gateway IP
IpTTL	Atributo	Representa el valor TimeToLive del encabezado del paquete IP
IpRecibidos	Atributo	El número total de datagramas recibidos por la interface
IpErrorHdr	Atributo	El número de datagramas de entrada descartados por errores en el encabezado (header)
IpErrorDir	Atributo	El número de datagramas de entrada descartados por errores en la dirección
IpDatagramasForw	Atributo	El número de datagramas para los que ésta entidad no ha sido el último destino
IpProtoDesc	Atributo	El número de datagramas recibidos, pero descartados debido a protocolo desconocido
ipDescartadosEntrada	Atributo	El número de datagramas descartados

IpEntregados	Atributo	El número de datagramas entregado exitosamente
ipDescartadosSalida	Atributo	El número de datagramas IP (sin problemas) de salida descartados por falta de recursos. (espacio en el buffer)
IpNoRuta	Atributo	Datagramas IP descartados por no encontrarse ruta para transmitirlos
ipTiempoReensamble	Atributo	El número máximo de segundos en los que los fragmentos recibidos se almacenan para reensamblarse
ipSolicitudesReensamble	Atributo	El número de fragmentos IP recibidos por la entidad para reemsamblarse
IpReensamblesOK	Atributo	El número de datagramas IP bien reensamblados.
ipReensamblesFallos	Atributo	El número de fallas detectadas por el algoritmo de reensamblado.
IpFragsCreados	Atributo	El número de fragmentos de datagramas generados por ésta entidad
ipRuteosDescartados	Atributo	El número de entradas de ruteo (sin problemas) descartados por falta de recursos (espacio en el buffer).
TABLARUTEO	Relación	Relación que representa entradas por cada ruta conocida actualmente por esta entidad.
IpRutDest	Atributo	El destino IP de esta ruta
IpRutIfIndex	Atributo	El valor índice (Tabla de Interfaces, ifIndex) que identifica unívocamente la interfaz local para el siguiente salto de esta ruta.
ipRutMetric1	Atributo	Representa la métrica de ruteo primaria (semántica especificada por el protocolo de ruteo).
ipRutMetric2	Atributo	Representa una métrica de ruteo alterna
ipRutMetric3	Atributo	Representa una métrica de ruteo alterna
ipRutMetric4	Atributo	Representa una métrica de ruteo alterna
IpRutSigSalto	Atributo	La dirección IP del siguiente salto de ésta ruta
IpRutTipo	Atributo	Representa el tipo de ruteo
IpRutProto	Atributo	Representa el mecanismo de ruteo mediante el cual esta ruta se aprendió
IpRutAge	Atributo	El número de segundos en los que ésta ruta se actualizó por última vez o se determinó correcta.
IpRutMascara	Atributo	Representa la máscara contra la cual se realiza una operación AND con la dirección destino antes de ser comparada con el campo ipRutDest.
ipRutMetric5	Atributo	Representa una métrica de ruteo alterna
ICMP	Relación	Relación que representa información de mensajes ICMP (Internet Control Message Protocol)
EstampaTiempo	Atributo	Representa el valor de SysUpTime al momento de la consulta de las variables del MIB del agente.

icmpMensajesEntrada	Atributo	El número total de mensajes ICMP recibidos por ésta entidad.
icmpMensErrorEntrada	Atributo	El número de mensajes ICMP recibidos con error
icmpDestNoEncontrado Entrada	Atributo	El número de mensajes ICMP "Destination Unreachable" recibidos
icmpTiempoExecEntrada	Atributo	El número de mensajes ICMP "Time Exceded" recibidos
icmpProbParamEntrada	Atributo	El número de mensajes ICMP "Parameter Problem" recibidos.
icmpMensajesSalida	Atributo	El número total de mensajes ICMP que ésta entidad intentó enviar.
icmpMensErrorSalida	Atributo	El número total de mensajes ICMP que ésta entidad no envió debido a problemas encontrados en ICMP.
icmpDestNoEncontrado Salida	Atributo	El número de mensajes ICMP "Destination Unreachable" enviados.
icmpTiempoExecSalida	Atributo	El número de mensajes ICMP "Time Exceded" enviados
icmpProbParamSalida	Atributo	El número de mensajes ICMP "Parameter Problem" enviados.
TCP	Relación	Relación que representa información sobre una conexión TCP particular (Transiente)
tcpAlgoritmoRto	Atributo	Representa el algoritmo usado para determinar el valor de timeout para retransmitir octetos sin acuse de recibo
TcpRtoMin	Atributo	Mínimo valor permitido para la retransmisión.
TcpRtoMax	Atributo	Máximo valor permitido para la retransmisión.
tcpMaxConexiones	Atributo	El límite en el total de conexiones TCP que la entidad puede soportar (si es dinámico el valor es -1)
tcpActivoAbiertas	Atributo	El número de ocasiones que conexiones TCP han hecho una transición directa a SYN-SENT a partir del estado CLOSED.
tcpPasivoAbiertas	Atributo	El número de ocasiones que conexiones TCP han hecho una transición directa a SYN-RCVD a partir del estado LISTEN.
tcpIntentosFallos	Atributo	El número de ocasiones que conexiones TCP han hecho una transición directa a CLOSED a partir del estado SYN-SENT o al estado SYN-RCVD, mas el número de ocasiones que una conexión TCP ha hecho una transición directa al estado LISTEN a partir del estado SYN-RCVD.
TcpEstabReset	Atributo	El número de ocasiones que conexiones TCP han hecho una transición directa a CLOSED a partir del estado ESTABLISHED o al estado CLOSEWAIT.
tcpEstabActualmente	Atributo	El número de conexiones TCP que se encuentran en estado ESTABLISHED o CLOSEWAIT.
TcpSegEntrada	Atributo	El número total de segmentos recibidos.
TcpSegSalida	Atributo	El número total de segmentos enviados.
TcpSegRetrans	Atributo	El número total de segmentos retransmitidos.
UDP	Relación	Relación que representa información sobre mensajes UDP

udpDatagramasEntrada	Atributo	El número total de datagramas UDP entregados.
UdpSinPuertos	Atributo	El número total de datagramas UDP recibidos para los que no hubo aplicación en el puerto destino.
udpErroresEntrada	Atributo	El número de datagramas UDP que no fueron entregados por errores diferentes al del udpSinPuertos
udpDatagramasSalida	Atributo	El número de datagramas UDP enviados por ésta entidad.
EGP	Relación	Relación que representa información sobre mensajes EGP (Exterior Gateway Protocol).
egpMensajesEntrada	Atributo	El número de mensajes EGP recibidos sin error.
egpErroresEntrada	Atributo	El número de mensajes EGP recibidos con error.
egpMensajesSalida	Atributo	El número total de mensajes EGP generados localmente
egpErroresSalida	Atributo	El número total de mensajes EGP generados localmente no enviados por falta de recursos.
egpAs	Atributo	El número de sistema autónomo de esta entidad.
SNMP	Relación	Relación que representa información sobre mensajes SNMP (Simple Network Management Protocol).
smnpPktsEntrada	Atributo	El número de mensajes SNMP entregados a la entidad SNMP del servicio de transporte.
snmpPktsSalida	Atributo	El número de mensajes SNMP pasados a la entidad de protocolo SNMP al servicio de transporte.
snmpErrorVersEntrada	Atributo	El número de mensajes SNMP pasados a la entidad de protocolo SNMP que fueron de versión no soportada.
snmpErrorCommunity NameEntrada	Atributo	El número de mensajes SNMP pasados a la entidad de protocolo SNMP que usaron un community name no conocido
snmpParseErrorEntrada	Atributo	El número total de errores encontrados por la entidad de protocolo SNMP en la decodificación de los mismos.
snmpTooBigEntrada	Atributo	El número total de PDU´s entregados a la entidad SNMP para los cuales el error-estatus es "tooBig"
snmpNoSuchName Entrada	Atributo	El número total de PDU´s entregados a la entidad SNMP para los cuales el error-estatus es "noSuchName"
snmpBadValuesEntrada	Atributos	El número total de PDU´s entregados a la entidad SNMP para los cuales el error-estatus es "badValue"
snmpReadOnlyEntrada	Atributo	El número total de PDU´s entregados a la entidad SNMP para los cuales el error-estatus es "readOnly"
snmpGenErrEntrada	Atributo	El número total de PDU´s entregados a la entidad SNMP para los cuales el error-estatus es "genErr"
snmpTotVarsGetEntrada	Atributo	El número total de objetos MIB que han sido accesados exitosamente por la entidad de protocolo SNMP
snmpTotVarsSetEntrada	Atributo	El número total de objetos MIB que han sido alterados exitosamente por la entidad de protocolo SNMP
snmpGetRequestEntrada	Atributo	El número total de PDU´s Get-Request que han sido

		aceptados y procesados por esta entidad.
snmpGetNextEntrada	Atributo	El número total de PDU´s Get-Next que han sido aceptados y procesados por esta entidad.
snmpSetRequestEntrada	Atributo	El número total de PDU´s Set-Request que han sido aceptados y procesados por esta entidad.
snmpGetResponses Entrada	Atributo	El número total de PDU´s Get-Responses que han sido aceptados y procesados por esta entidad.
snmpTrapsEntrada	Atributo	El número total de PDU´s Traps que han sido procesados por esta entidad.
snmpTooBigSalida	Atributo	El número total de PDU´s generados por la entidad SNMP para los cuales el error-estatus es "tooBig"
snmpNoSuchNameSalida	Atributo	El número total de PDU´s generados por la entidad SNMP para los cuales el error-estatus es "noSuchName"
snmpBadValuesSalida	Atributo	El número total de PDU´s generados por la entidad SNMP para los cuales el error-estatus es "BadValue"
snmpReadOnlySalida	Atributo	El número total de PDU´s generados por la entidad SNMP para los cuales el error-estatus es "readOnly"
snmpGenErrSalida	Atributo	El número total de PDU´s generados por la entidad SNMP para los cuales el error-estatus es "genErr"
snmpGetRequestSalida	Atributo	El número total de PDU´s Get-Request que han sido generados por esta entidad.
snmpGetNextSalida	Atributo	El número total de PDU´s Get-Next que han sido generados por esta entidad.
snmpSetRequestSalida	Atributo	El número total de PDU´s Set-Request que han sido generados por esta entidad.
snmpGetResponses Salida	Atributo	El número total de PDU´s Get-Responses que han sido generados por esta entidad.
snmpTrapsSalida	Atributo	El número total de PDU´s Trap que han sido generados por esta entidad.
snmpAutorizaTraps	Atributo	Indica si el proceso de agente SNMP genera Traps de fallas de autorización
ESTADISTICAS ETHERNET	Relación	Relación que representa información sobre estadísticas ethernet por interfaz de la entidad
etherstatsIdx	Atributo	Identifica unívocamente entradas de estadísticas ethernet
etherStatsFuente	Atributo	Este objeto identifica la fuente de datos que ésta entrada de estadísticas de ethernet analizará, esta puede ser una interfaz ethernet en el dispositivo (relacionado con el índice de la tabla de interfaces).
etherStatsEventosDrop	Atributo	El número de paquetes tirados por falta de recursos.
etherStatsOctetos	Atributo	El número total de octetos recibidos.
etherStatsPkts	Atributo	El número total de paquetes recibidos.

etherStatsPktsBroadcast	Atributo	El número total de paquetes recibidos dirigidos a una dirección broadcast.
etherStatsPktsMulticast	Atributo	El número total de paquetes recibidos dirigidos a una dirección multicast.
etherStatsErrores AlineacionCRC	Atributo	El número de paquetes con error de FCS (Frame Check Sequence).
etherStatsPktsUndesize	Atributo	El número total de paquetes con longitud menor a 64 octetos.
etherStatsPktsOversize	Atributo	El número total de paquetes con longitud mayor a 1518 octetos.
etherStatsFragmentos	Atributo	El número total de paquetes recibidos con longitud menor a 64 octetos de longitud y error en FCS.
etherStatsJabbers	Atributo	El número total de paquetes recibidos con longitud mayor a 1518 octetos de longitud y error en FCS.
etherStatsColisiones	Atributo	Estimado del total de colisiones en el segmento ethernet
etherStatsPkts64Octetos	Atributo	El número total de paquetes con longitud de 64 octetos
etherStatsPkts65to127 Octetos	Atributo	El número total de paquetes recibidos con longitud de entre 65 y 127 octetos.
etherStatsPkts128to255 Octetos	Atributo	El número total de paquetes recibidos con longitud de entre 128 y 255 octetos.
etherStatsPkts256to511 Octetos	Atributo	El número total de paquetes recibidos con longitud de entre 256 y 511 octetos.
etherStatsPkts512to1023Octetos	Atributo	El número total de paquetes recibidos con longitud de entre 512 y 1023 octetos.
etherStatsPkts1024to1518Octetos	Atributo	El número total de paquetes recibidos con longitud de entre 1024 y 1518 octetos.
etherStatsPropietario	Atributo	Describe a la entidad que configuró ésta entidad.
etherStatsEstado	Atributo	El estado de ésta entrada de estadísticas ethernet.
CONTROL HISTORICO	Relación	Relación con información sobre el muestreo periódico estadístico.
histctlIdx	Atributo	Indice que identifica unívocamente a las entradas de la tabla de control de histórico.
histctlFuente	Atributo	Este objeto identifica la fuente de datos para la cual se obtiene la información histórica. Esta puede ser cualquier interfaz en el dispositivo.
histctlBucketsSolicitados	Atributo	El número solicitado de intervalos de tiempo discreto sobre los que se salvarán datos.
histctlBucketsAdmitidos	Atributo	El número de intervalos de muestreo discreto sobre los que se salvarán datos.
histctlIntervalo	Atributo	Intervalo en segundos, con el cual los datos serán muestreados para cada bucket.

histctlPropietario	Atributo	La entidad que configuró esta entrada y utiliza los recursos asignados a ésta.
histctlBucketsEstado	Atributo	El estado de esta entrada de control de histórico.
HISTORICO ETHERNET	Relación	Relación con información histórica de ethernet por interfaz de dispositivos.
etherHistIdx	Atributo	Representa el histórico del que esta entrada es parte (relacionado con histctlIdx).
etherHistIdxMuestra	Atributo	Representa un índice que identifica unívocamente una muestra
etherHistComienzo Intervalo	Atributo	El valor de sysUpTime en el comienzo del intervalo sobre el cual se tomó la muestra.
etherHistEventosDrop	Atributo	El número de paquetes tirados por falta de recursos durante éste intervalo de muestreo.
etherHistOctetos	Atributo	El número total de octetos recibidos en la red.
etherHistPkts	Atributo	El número de paquetes recibidos durante el intervalo de muestreo.
etherHistBroadcastPkts	Atributo	El número de paquetes recibidos dirigidos a una dirección broadcast.
etherHistMulticasPkts	Atributo	El número de paquetes recibidos dirigidos a una dirección multicast.
etherHistErrores AlineacionCRC	Atributo	El número de paquetes recibidos en el intervalo de muestreo entre 64 y 1518 octetos con error en FCS
etherHistPktsUndesize	Atributo	El número de paquetes recibidos durante éste intervalo de muestreo de longitud menor a 64 octetos.
etherHistPktsOversize	Atributo	El número de paquetes recibidos durante éste intervalo de muestreo de longitud mayor a 1518 octetos.
etherHistFragmentos	Atributo	El número de paquetes recibidos durante éste intervalo de muestreo de longitud menor a 64 octetos y con error de FCS
etherHistJabbers	Atributo	El número de paquetes recibidos durante éste intervalo de muestreo de longitud mayor a 1518 octetos y con error de FCS.
etherHistColisiones	Atributo	Estimado del número total de colisiones sobre el intervalo de muestreo.
etherHistUtilizacion	Atributo	El mejor estimado de utilización de la capa de red de medio físico en ésta interfaz durante el intervalo de muestreo.
ALARMA	Relación	Relación con información de la configuración de alarmas
alarmIdx	Atributo	Indice que identifica unívocamente una entrada en la tabla de alarmas.
alarmIntervalo	Atributo	Intervalo en segundos sobre el cual se muestrean los datos y se comparan con los umbrales superior o inferior
alarmVariable	Atributo	El identificador de objeto de la variable a ser muestreada.
alarmTipoMuestreo	Atributo	Representa el tipo de muestreo y el cálculo del valor a ser

		comparado con los umbrales.
alarmValor	Atributo	El valor estadístico sobre el último periodo de muestreo.
alarmComiezoAlarma	Atributo	Representa la alarma que puede ser enviada cuando esta entrada es válida por primer vez(p.e. una sola alarma de que excedió el umbral).
alarmUmbralSuperior	Atributo	Un umbral para la muestra estadística.
alarmUmbralInferior	Atributo	Un umbral para la muestra estadística.
alarmEventoUmbral SuperiorIdx	Atributo	Indice de la entrada de evento usada cuando se cruza un umbral superior
alarmEventoUmbral InferiorIdx	Atributo	Indice de la entrada de evento usada cuando se cruza un umbral inferior.
alarmPropietario	Atributo	La entidad que configuró esta entrada y usa los recursos asignados a ésta.
alarmEstado	Atributo	El estado de ésta entrada de alarma
CONTROLHOST	Relación	Relación que guarda información sobre las interfaces que implementan estas funciones RMON para hosts. Información que se almacena en la tabla de HOST.
hostctlIdx	Atributo	Indice que identifica una entrada en la tabla de control de host.
hostctlFuente	Atributo	Este objeto identifica la fuente de datos para la instancia de la función de host. La fuente puede ser cualquier interfaz en éste dispositivo. (Relacionado con ifIdx de la tabla de interfaces).
hostctlTamanoTabla	Atributo	El número de entradas de host
hostctlUltimoBorrado	Atributo	El valor de sysUpTime cuando la última entrada fue borrada.
hostctlPropietario	Atributo	La entidad que configuró esta entrada y usa los recursos asignados a ésta.
hostctlEstado	Atributo	El estado de ésta entrada de control de host.
HOST	Relación	Relación que almacena información estadística de los hosts
hostIdx	Atributo	Valor que agrupa a un conjunto de hosts y está relacionado con hostctlIdx de la tabla de ControlHost
hostDireccion	Atributo	La dirección física del host
hostOrdenCreacion	Atributo	Indice que define el orden relativo de tiempo de creación
hostPktsEntrada	Atributo	El número de paquetes transmitidos a ésta dirección
hostPktsSalida	Atributo	El número de paquetes transmitidos por ésta dirección
hostOctetosEntrada	Atributo	El número de octetos transmitidos a ésta dirección
hostOctetosSalida	Atributo	El número de octetos transmitidos por ésta dirección
hostErroresSalida	Atributo	El número de paquetes erróneos transmitidos por ésta dirección
hostPktsBroadcastSalida	Atributo	El número de broadcast generados por ésta dirección
hostPktsMulticastSalida	Atributo	El número de multicast generados por ésta dirección

EVENTOS	Relación	Información sobre la generación y notificación de eventos de los dispositivos RMON.
eventIdx	Atributo	Indice de entradas en la tabla de eventos.
eventDescripcion	Atributo	Comentario sobre ésta entrada de eventos.
EventTipo	Atributo	Tipo de notificación que la prueba hará sobre éste evento
EventCommunity	Atributo	Community que utilizará el mensaje Trap.
EventUltimoEnvio	Atributo	El valor de sysUpTime cuando esta estrada generó un evento.
EventPropietario	Atributo	Entidad que configuró esta entrada.
EventEstado	Atributo	El estado de ésta entrada.

4.4 Implementación

Aunque en las secciones [4.3] se describe el análisis y diseño completo del sistema, existen elementos que se consideró dejar como trabajo futuro por razones de infraestructura que se comentarán más adelante. Enseguida se describen los alcances, limitaciones y aspectos concernientes a la implementación.

4.4.1 Lenguaje de implementación

El lenguaje de implementación utilizado fue Java[10] debido a que es un lenguaje transportable entre plataformas (Sistemas operativos) siempre y cuando se utilicen las librerías adecuadas (sun, swing, awt) para este fin. Se utilizó una herramienta visual para acelerar el aprendizaje del lenguaje (JBuilder ver.3) y para facilitar el manejo de base de datos relacionales. Un sistema de gestión independiente de la plataforma, y con requerimientos de hardware comunes (Pentium II, III y 40 MB RAM) como para cualquier otra aplicación, da la posibilidad operacional, a las empresas pequeñas y medianas de poder utilizarlo sin tener que invertir en hardware especial y costoso. El protocolo de gestión utilizado fue SNMPv.1 el cual fue muy aceptado por el mercado y por lo tanto el más común.

4.4.2 Arquitectura operacional

Debido a que SNMP es el protocolo que utiliza el sistema desarrollado para gestionar a los NEs, consultándoles principalmente 2 tipos de MIBs:

- MIB para gestión de redes basadas en TCP/IP [6] (Management Information Base for Network Management of TCP/IP-based internets: MIB-II)
- MIB de prueba de monitoreo remoto [7] (Remote Network Monitoring Management Information Base: RMON)

El sistema utiliza una arquitectura centralizada en la forma de gestionar [Sección 3.2] a los dispositivos cuyos agentes manejan la MIBII y jerárquica a los que manejan una prueba de monitoreo remoto (RMON), es decir, los configura de tal forma, que la prueba es capaz de realizar cierto procesamiento (p.e. ancho de banda utilizado en cada puerto) y la comunicación no es tan constante con el OS gestor, disminuyéndose así el tráfico generado por la gestión.

Tomando en cuenta el marco de la RGT en su arquitectura lógica estratificada [Sección 2.1.6] el sistema desarrollado se ubica en el estrato de gestión de elemento de red y de red debido a los MIBs que maneja el sistema (ver apéndice A).

4.4.3 Alcances

El sistema desarrollado toma en cuenta las funciones de gestión definidas en la RGT [Sección 2.2] e implementa aspectos relacionados con la configuración, fallas y calidad del desempeño, hasta donde lo permiten los MIBs que el sistema maneja.

4.4.4 Limitaciones

En el marco de la RGT, en específico las funciones de gestión no se implementaron las gestiones de contabilidad y seguridad.

4.5 Acrónimos

A Agente

A/M Agente/gestor (*Agent/Manager*)

CDMA (*Code Division Multiple Access*)

CMIP Protocolo común de información de gestión (*Common Management Information Protocol*)

CMIS Servicio común de información de gestión (*Common Management Information Service*)

CMISE Elemento común del servicio de información de gestión (*Common Management Information Service Element*)

CNM Gestión de red de cliente (*Customer Network Management*)

DCF Función de comunicación de datos (*Data Communication Function*)

DIB Base de información de directorio (*Directory Information Base*)

DO Objeto del directorio (*Directory Object*)

EER Empresa de explotación reconocida

EML Capa de gestión de elemento (*Element Management Layer*)

IN Red inteligente (*Intelligent Network*)

ISO Organización Internacional de Normalización (*International Organization for Standardization*)

LAN Red de área local (*Local Area Network*)

LLA Arquitectura lógica por capas (*Logical Layered Architecture*)

MAN Red de zona metropolitana (*Metropolitan Area Network*)

MIB Base de datos de información de gestión (Manage Information Base)

MIS Servicio de información de gestión (*Management Information Service*)

MIT Arbol de información de gestión (*Manage Information Tree*)

NE Elemento de red (*Network Element*)

NML Capa de gestión de red (*Network Management Layer*)

OA&M Operaciones, administración y mantenimiento (*Operations, Administration and Maintenance*)

OMG Grupo de metodología objeto (*Object Methodology Group*)

OS Sistema de operaciones (*Operations System*)

OSI Interconexión de sistemas abiertos (*Open Systems Interconnection*)

PBX Centralita privada (*Private Branch Exchange*)

PDU Unidad de datos de protocolo (*Protocol Data Unit*)

QoS Calidad de servicio (*Quality of Service*)

R Recurso (Resource)

DCN Red de comunicación de datos (Data Comunications Network)

ISDN Red digital de servicios integrados (Integrated service digital network)

TMN Red de gestión de las telecomunicaciones (RGT) (TMN, Telecomunications Management Network)

RMON Dispositivo de monitoreo remoto(*Remote Network Monitoring*)

RSE Entorno de sistema real (*Real System Environment*)

SDH Jerarquía digital síncrona (*Synchronous Digital Hierarchy*)

SMAE Entidad de aplicación de gestión de sistemas (*Systems Management Application Entity*)

SMASE Elemento de servicio de aplicación de gestión de sistema (*System Management Application Service Element*)

SMI Estructura e identificación de la información de gestión (*Structure and identification of Management Information*)

SMK Conocimiento de gestión compartido (*Shared Mmanagement Knowledge*)

SML Capa de gestión de servicios (*Service Management Layer*)

SONET Red óptica síncrona (*Synchronous Optical Network*)

SS N.º 7 Sistema de señalización N.º 7 (*Signalling System No. 7*)

STP Punto de transferencia de la señal (*Signal Transfer Point*)

TP Procesamiento de transacciones (*Transaction Processing*)

UISF Función de soporte de interfaz de usuario (*User Interface Support Function*)

UIT-R Sector de Radiocomunicaciones de la Unión Internacional de Telecomunicaciones

UIT-T Sector de Normalización de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones

UPT Telecomunicaciones personales universales (U*niversal Personal Telecommunications*)

VAS Servicio de valor añadido (V*alue Added Service*)

VASP Proveedor de servicio de valor añadido (V*alue Added Service Provider*)

WSF Función de estación de trabajo (W*orkstation Function*)

WSSF Función de soporte de estación de trabajo (W*orkstation Support Function*)

5 Conclusiones

En las contribuciones de esta tesis se menciona que el proyecto esta basado en las funciones de gestion de la RGT definidas por la ITU asi como en las propuestas de gestion desarrolladas por IAB e IETF para internet, en este sentido y analizando las propuestas vemos que la ITU tiene una propuesta mas completa, en su estructura de información y compleja, en la distribucion de tareas e inteligencia de gestion, con la desventaja de la necesidad de una conexión dedicada de gestor a dispositivo gestionado. Por otro lado la propuesta de gestión IETF tiene una arquitectura de gestion mas simple que ha ido mejorando con nuevas versiones, añadiendo distribución en los procesos de gestión. En este proyecto se utiliza SNMP como protocolo de gestion por lo que, hasta el momento no es posible abarcar toda la funcionalidad operativa que se describe en la RGT, pero lo que si se puede hacer es organizar la informacion de gestion de tal manera que el sistema de gestion proporcione una descomposicion de la funcionalidad en capas de:

- gestión de elementos
- gestión de red
- gestión de servicio
- gestión empresarial

En el trabajo desarrollado se logró lo siguiente:

- Se realizó un estudio crítico del problema de la gestión de redes de telecomunicaciones, con sus antecedentes, problemas, estándares, diferentes propuestas y las tendencias en éste campo.
- Se realizó el análisis y diseño del sistema.
- Se implementó un sistema que gestiona redes de pequeñas y medianas empresas.
- El sistema realiza las funciones de gestión de configuración, fallas y desempeño.
- La implementación se realizó en Java[10], lo que hace al sistema independiente de la plataforma y le da la posibilidad de ser accesible desde un navegador de internet.
- Ayuda a una mejor planeación y dimensionamiento de la red, basándose en la gestión de desempeño, la cual proporciona información al administrador sobre el volumen de tráfico en los enlaces. La gestión de fallas por otra parte, ayuda a la localización de errores y fallas, para que se pueda tomar una decisión.
- El sistema utiliza la red TCP/IP y
- SNMPV1 como protocolo de gestión (con gran aceptación en el mercado).

Pensando en la posibilidad de que el trabajo desarrollado sea puesto en el mercado y permanezca como un producto de buena calidad, el trabajo futuro es el siguiente:

- Implementar las versiones 2 y 3 de SNMP y así aprovechar la arquitectura distribuida de la versión 2 y las mejoras de seguridad de la versión 3. Dado que la arquitectura de las diferentes versiones de SNMP permiten su coexistencia.

- Implementar un analizador de protocolo, como complemento al MIBII respecto al flujo de mensajes por host y por protocolo.
- Utilizar CORBA o RMI para implementar el concepto de gestión por delegación [16][17].
- Utilizar CORBA o RMI para realizar un mapeo de mensajes SNMP a CMIP y con esto aumentar la capacidad del sistema para gestionar dispositivos de ambas propuestas IETF e ITU/OSI.
- Aumentar el número de MIBs soportados (ver apéndice A).
- Habilitar al sistema para que pueda utilizar los MIBs propietarios.
- Hacer que la información del sistema de plataforma pueda ser consultada también usando un navegador de Internet.

5.1 Apéndice A

TRANSMISSION MIBs

Title	RFC
IEEE 802.3 Repeater Devices	2108
Data Link Switching	2024
IEEE 802.5	1748
ATM	1695
SMDS	1694
Ethernet	1650
Frame Relay	1604
SONET / SDH	1595
FDDI	1512
Link Control Protocol of PPP	1471
Multiprotocol Interconnect over X.25	1461
DS3 / E3	1407
DS1 / E1	1406
Frame Relay DTEs	1315

NETWORK LAYER MIBs

Title	RFC
IP Forwarding Table	2096
RMON Version 2	2021
IP Mobility Support	2006
OSPF Version 2	1850
RMON	1757
RIP	1724
BGP Version 4	1657
Token Ring extensions to RMON	1513
Identification MIB	1414
BGP Version 3	1269
MIB-II	1213

APPLICATION LAYER MIBs

Title	RFC
WWW servers	2039
RDBMS	1697
DNS Resolver	1612
DNS Server	1611
X.500 Directory	1657
Mail	1566
Network Services	1565
Host Resources	1514

HARDWARE SPECIFIC MIBs

Title	RFC
Entity	2037
Printer	1759
Modem	1696
Parallel printer-like Hardware	1660
RS-232-like Hardware	1659
Character Stream Devices	1658
UPS	1628

6 REFERENCIAS

1. S. Aidarous, T. Plevyak. *Telecomunications Network Mamagement in to the 21st Century*, (IEEE Press), (1994).
2. K. Leinwand, C. Fang. *Network Management a practical perspective*. (Addison Wesley, USA,1996).
3. Recomendación UIT-T M.3010, *Principios para una red de gestión de las telecomunicaciones*, 1996.
4. Recomendación UIT-T M.3400, *Funciones de gestión de la red de gestión de las telecomunicaciones*, 1996.
5. J. Case, M. Fedor, M. Schoffstall y J. Davin. *A Simple Network Management Protocol (SNMP).* Internet Request for Comments 1157, Mayo (1990).
6. K. McCloghrie, M. Rose. *Management Information Base for Network Management of TCP/IP-based internets: MIB-II*. Internet Request for Comments 1213, Marzo (1991).
7. S. Waldbusser. *Remote Network Monitoring Management Information Base*. Internet Request for Comments 1757, Febrero (1995).
8. G. S. Perrow, J. W. Hong, H. L. Lutfiyya, M. y A. Bauer. *The Abstraction and Modeling of Management Agents*, http://www.simpleweb.org/
9. D. T. Perkins. *Understanding SNMP MIBs*. septiembre (1993), http://www.simpleweb.org/
10. M. Morgan. *Descubre Java 1.2.* (Prentice Hall, Madrid 1999).
11. L. Deri. *Network Management for the 90's*. Julio (1996), Proceedings of the ECOOP '96 Workshop on Systems and Network Management, Linz, Austria. http://www.simpleweb.org/
12. K. Terplan y J. Huntington – Lee. *Aplications for distributed systems and Network Management*, (John Wiley & Sons. Canada, 1995).
13. D. Kroenke. *Database Processing, fundamentals, design and implementation*. (Prentice Hall. USA 1997).
14. S. Lalani, K. Jamsa. *Java, biblioteca del programador*. (McGraw-Hill. México 1997).
15. M. Rinehart. *Desarrollo de bases de datos en Java*. (McGraw-Hill. Madrid 1998).
16. D. Zhang, W. Zorn. *Developing network management aplications in an aplication oriented way using mobile agent*. (1998). http://www.simpleweb.org/
17. J. Schonwalder. *Network Management by Delegation, from research prototypes towards standards*. Julio de (1997). http://www.simpleweb.org/
18. L. Deri, *Desktop vs. Web Based Network Management*. (1999) http://www.simpleweb.org/

19. L. Deri, *Sufin' network resources across the web* (1995). In Proceedings of the IEEE Workshop on Systems Management, Toronto, Canada. June 1996. http://www.simpleweb.org/

20. L. Deri, *Rapid Network Management Application Development* (junio 1997) http://www.simpleweb.org/

21. L. Deri, *VRML: Adding 3D to Network Management* IS&N'97, Como, Italia. Mayo 1997. http://www.simpleweb.org/

22. L. Deri, B. Bela *"Static vs. Dynamic CMIP/SNMP Network Management Using CORBA"*. Aceptada para publicarse en IS&N'97, Como, Italy. May 1997.

23. F. Barillaud, L. Deri, M. Feridun, *Network Management Using Internet Technologies*. (1997). http://www.simpleweb.org/

24. J. Reilly, P. Niska, L. Deri, and D. Gantenbein. *Enabling Mobile Network Managers*. (1997). http://www.simpleweb.org/

25. R. Boyd, K. Brodrick: *"Operational Support Systems for the future Local Network"*, BT Technology Journal, Vol. 7, No. 2, Abril 1989, páginas 136-150.

26. Booch, *Object oriented analysis and design with applications*, Addison – Wesley 1995.

27. P. Muller, *Instant UML*, Wrox Press, 1997 Canada.

28. *OMG Unified Modeling Language Specification*. Version 1.3, June 1999. http://www.omg.org/

29. S. Young-Chul, *Developing a Managed System in a Telecommunications Management Network* (1996). http://www.omg.org/

30. M. Schultze, G. Benko y C. Farrell, *A Prelude to Network Management.* (1993). http://www.omg.org/

31. *Information processing systems* Open Systems Interconnection Specification of Basic Encoding Rules for Abstract Notation One (ASN.1), International Organization for Standardization, International Standard 8825, December 1987.

32. J. Rumbaugh, *OMT Insights*, SIGS Books ,1996.

33. E. Yourdon, *Object Oriented Systems Design, an Integrated Approach*. Yourdon Press Computing Systems, 1994.

34. T. Quantrani, *Visual Modeling Whit Rational Rose and UML*, Addison – Wesley, 1998.

35. P. Aiko, *Network Management Architectures,* Ph.D. Thesis 1995, http://www.omg.org/

ANIVERSARIO
Cinvestav

Centro de Investigación y de Estudios Avanzados del IPN

Unidad Guadalajara

El Jurado designado por la Unidad Guadalajara del Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional, aprobó la tesis: SISTEMAS DE GESTIÓN DE REDES DE TELECOMUNICACIONES PARA PEQUEÑAS Y MEDIANAS EMPRESAS del(a) C. Héctor CASTILLO HERNANDEZ el día 15 de Febrero de 2002

Dr. Deni Librado Torres
Román
Profesor Investigador 3A
CINVESTAV GDL
Guadalajara

p.a.

Dr. Manuel Edgardo
Guzmán Renteria
Investigador Cinvestav 3A
CINVESTAV GDL
Guadalajara

Dr. Jesús Leonardo Soto
Sumuano
Investigador 2A
INSTITUTO TECNOLOGICO Y
DE ESTUDIOS SUPERIORES
DE MONTERREY Campus
Guadalajara
Guadalajara