UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

GESTIÓN Y OPERACIÓN DE REDES DE COMUNICACIÓN

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

RICHARD ESTEBAN CRUZ RAMOS

PROMOCIÓN
1999–I

LIMA – PERÚ
2003

Dedico este trabajo a:

Mi Madre, por el apoyo incondicional

durante toda mi carrera,

Mis hermanas, por brindarme la esperanza de

superación.

GESTIÓN Y OPERACIÓN DE REDES DE COMUNICACIÓN

SUMARIO

El presente informe tiene como objetivo informar como optimizar el manejo e intercambio de información a través de una red IP en la actualidad, del mismo modo identificar sistemas, elementos y actividades que componen una estructura de administración de red.

El capitulo I ofrece un panorama general sobre lo que significa disponer de un sistema de gestión de red, aspectos básicos de administración que componen dicho sistema, así como el equipamiento necesario en hardware y software.

El capitulo II describe la evolución de las diferentes arquitecturas y plataformas conforme la madurez que han alcanzado las redes, se discute los elementos que las componen, así como sus ventajas y desventajas; se presentan aplicaciones de amplio uso hoy en día. Se da un alcance sobre los planes y contingencias a considerar en una red en proceso de cambio.

El capitulo III discute las actividades y elementos estándares para lograr un alto rendimiento en el mantenimiento, monitoreo de toda una red, a través de los centros de

operación e información de red, logrando una alta disponibilidad y un mejor control de los cambios.

El capitulo IV describe en detalle los diversos protocolos para la gestión y operación de red, enfatizando el SNMP como estándar universal.

El capítulo V proporciona aspectos a tomar en cuenta para administrar una red TCP/IP en ambientes corporativos e Internet.

El capítulo VI discute las bases para lograr un sistema de gestión de red con éxito y calidad.

ÍNDICE

PRÓLOGO

Un aspecto clave del rápido crecimiento de Internet y las redes en general ha sido el acceso libre y abierto a los documentos básicos, especialmente a las especificaciones de los protocolos. Los comienzos de Arpanet y de Internet en la comunidad de investigación universataria estimularon la tradición académica de la publicación abierta de ideas y resultados. Una serie de memorándums llamados RFC (Request For Comments) pretendieron ser una vía informal y de distribución rápida para compartir ideas con los investigadores en redes, hoy en día se encuentran difundidos en el World Wide Web en decenas de emplazamientos. El crecimiento en el mundo empresarial trajo como consecuencia un incremento de la preocupación por el propio proceso de estándares y por ende surgieron las necesidades de gestionar y operar de manera adecuada una red para evitar complicaciones en el largo plazo. En paralelo con los esfuerzos de comercialización amparados por las actividades de interoperabilidad, los fabricantes comenzaron a acudir a las reuniones del IETF que se convocaban tres o cuatro veces al año para discutir nuevas ideas para extender el conjunto de protocolos relacionados con TCP/IP. Comenzaron con unos cientos de asistentes procedentes en su mayor parte del mundo académico y financiados por el sector público; actualmente estas

reuniones atraen a varios miles de participantes, en su mayor parte del sector privado y financiados por éste. Los miembros de este grupo han hecho evolucionar el TCP/IP cooperando entre sí. La razón de que estas reuniones sean tan útiles es que acuden a ellas todas las partes implicadas: investigadores, usuarios finales y fabricantes. La Gestión de Redes nos da un ejemplo de la beneficiosa relación entre la comunidad investigadora y los fabricantes. En los comienzos de Internet, se hacía hincapié en la definición e implementación de protocolos que alcanzaran la interoperación. A medida que crecía lared aparecieron situaciones en las que procedimientos desarrollados "ad hoc" para gestionar la red no eran capaces de crecer con ella. La configuración manual de tablas fue sustituida por algoritmos distribuidos automatizados y aparecieron nuevas herramientas para resolver problemas puntuales. En 1987 quedó claro que era necesario un protocolo que permitiera que se pudieran gestionar remota y uniformemente los elementos de una red, como los routers. Se propusieron varios protocolos con este propósito, entre ellos el SNMP (Single Network Management Protocol, protocolo simple de gestión de red) diseñado, como su propio nombre indica, buscando la simplicidad; HEMS, un diseño más complejo de la comunidad investigadora; y CMIP, desarrollado por la comunidad OSI. Dándose lugar a desestimar HEMS como candidato para la estandarización, dejando como solución inmediata al SNMP mientras el CMIP pasará a ser una aproximación a largo plazo: El mercado podría elegir el que resultará más apropiado. Hoy SNMP se usa casi universalmente para la gestión de red.

CAPÍTULO I

GESTIÓN DE RED: GENERALIDADES

1.1 ADMINISTRACIÓN Y GESTIÓN DE RED

El objetivo principal de la administración de red es mantener operativa la red satisfaciendo las necesidades de los usuarios. La utilización de herramientas adecuadas permite realizar de forma centralizada la administración de múltiples redes de gran tamaño compuestos de cientos de dispositivos tales como routers, switches, transductores, servidores, puestos de trabajo, periféricos, etc.

Normalmente las herramientas de administración de red forman un conjunto muy heterogéneo de aplicaciones proveniente de, por ejemplo, el sistema de gestión de red, el Help Desk, herramienta de los fabricantes de los dispositivos, herramientas autónomas e independientes. Además muchas de estas herramientas suelen tener APIs (Application Program Interface) que permiten el acceso por programación. Hoy en día estas herramientas corren sobre diferentes sistemas operativos y suelen tener la característica de disponer de un interfaz gráfico de usuario basado en ventanas.

No importando cuan grande o pequeña es tu ambiente de red, los cambios son inevitables. Contratando nuevos empleados, adicionando nuevas oficinas, soportando nuevos servicios de red, reparando defectos de sistema, todas estas actividades resultan en un cambio, especialmente tus dispositivos de infraestructura de red, tal como routers, switches, hubs, firewalls, y así sucesivamente. A pesar de que el cambio es casi siempre una cosa buena, pueden causar cosas malas a la larga. De modo que no importando cuan menor o beneficioso puede ser un cambio, siempre se debe realizar con dosis saludable de precaución. De modo gestionar los cambios de la red implica tener un conjunto de políticas y procedimientos que se adopten y se cumplan para formalizar tal precaución dentro de un proceso consistente.

1.2 ROL DE UN ADMINISTRACIÓN DE RED

Dentro de los muchos roles a la que esta sujeto un administrador de red, hay que considerar el mantenimiento de la documentación que describe las configuraciones actuales de todos los dispositivos de la red, el propósito y detalles de cualquier cambio, para ser usado en caso de cualquier emergencia, implementando políticas que controlen la tasa de cambio, así como de quienes intervinieron en todas las implementaciones del sistema que fueron planeadas.

1.2.1 Gestión de usuarios

La gestión de usuarios es la actividad referida a la creación y mantenimiento de cuentas de usuarios, así como la de asignación de recursos y mantenimiento de la seguridad en los accesos a la red. Las tareas principales en la gestión de usuarios son:

- Altas, bajas y modificaciones de usuarios en la red.
- Establecimiento de políticas de passwords como su longitud, tiempo de vida, seguridad de la base de datos de passwords, etc.
- Asignación de permisos para la utilización de recursos de red.
- Monitorización de la actividad de los usuarios.
- Establecimiento de políticas generales y de grupo que faciliten la configuración de usuarios.

1.2.2 Gestión del hardware

La gestión del hardware es una actividad esencial para el control del equipamiento y sus costes asociados así como para asegurar que los usuarios disponen del equipamiento suficiente para cubrir sus necesidades.

Para evitar visita física a los equipos, se utilizan agentes que se ejecutan en los puestos de trabajo y que realizan el inventario del hardware de forma autónoma y remota.

Una vez que la información de inventario es recogida, la administración de red puede hacer las siguientes funciones:

- Añadir información relativa a puestos de trabajo no instalados en red.
- Añadir información sobre otros aspectos como la localización física, condiciones en que se encuentra, etc.
- Establecimiento de parámetros de configuración en los ficheros de configuración del sistema operativo.
- Realizar el seguimiento de averías de los componentes de las estaciones de trabajo.
- Anotar información al inventario referente a los componentes que forman la estación de trabajo (tarjetas, discos, etc).

El inventario se realiza periódicamente bien cada vez que se ponen en marcha los puestos, bien durante su tiempo de funcionamiento. Normalmente los datos que se recogen son variados:

- BIOS del sistema.
- Ficheros de configuración del sistema operativo.
- Parámetros del sistema operativo.
- Características de los discos duros.
- Drivers cargados en memoria durante el funcionamiento de la estación.
- Otras características establecidas por el administrador.

En los servidores, además se suelen realizar un seguimiento de los parámetros de funcionamiento como pueden ser actividad de la CPU, de los discos, espacios disponibles, número de conexiones, etc. Este seguimiento permite analizar el

comportamiento y, en su caso, detectar nuevas necesidades y adaptar las características hardware de los servidores.

1.2.3 Gestión del software

Las actividades relativas a la gestión de software permiten a la administración de red determinar si las aplicaciones necesitadas por los usuarios se encuentran instaladas y donde están localizadas en la red, además permiten el seguimiento de número de licencias existentes y el cumplimiento de su uso en la red. De igual forma que en el hardware, se utilizan agentes que realizan la función de obtener toda la información acerca del software en la red. Sus características particulares son:

- Obtienen su información chequeando todos los discos de los puestos de trabajo en la red.
- Normalmente son capaces de identificar cientos de paquetes comerciales y se les puede añadir nuevos paquetes particulares de la empresa.
- Realizan mediciones del número de copias de un paquete que se están usando en la red de forma simultánea con objeto de comprobar su adecuación al número de licencias adquiridas.

Las tareas que normalmente realiza la administración de red en este área son:

- Creación y mantenimiento del inventario de software instalado.
- Especificación y requerimiento del número de copias disponibles de los distintos paquetes.

- Seguimiento de la instalación no autorizada de software y de otros ficheros en prevención de introducción de virus.
- Autorización a los usuarios para la utilización de los paquetes de software.

La información que se suele extraer es la siguiente:

- Información general del paquete: fabricante, versión, nº de licencias, etc.
- Disponibilidad: quién usa el software, quién lo puede usar, etc.
- Ficheros que componen el paquete.
- Información adicional establecida por el administrador.

1.2.4 Distribución de ficheros

Debido a la enorme dispersión de puestos en red, la distribución de software y otros ficheros se realiza mediante la utilización de agentes de distribución de ficheros. Las características de los agentes de distribución de ficheros son:

- Las funciones que realizan son instalación y actualización de software, descargas y eliminación de ficheros.
- Pueden aplicarse a puestos individuales o a grupos de estaciones simultáneamente.
- Recoger información sobre el estado de la distribución presentando la información en la consola de administración.
- Tienen en cuenta los permisos de accesos de los usuarios a más de una máquina para instalar el software en cada una de las máquinas a las que se accede.

En la mayoría de los casos se utilizan lenguajes de scripts para realizar las tareas de distribución de software. Otros paquetes más sofisticados disponen de herramientas que guían el proceso de creación de scripts generando paquetes completos que contienen scripts, ficheros y reglas de dependencias para su correcta distribución. Normalmente estos paquetes se comprimen para ahorrar tráfico de red. Los momentos de distribución suelen ser cuando los puestos inician su funcionamiento aunque los usuarios a veces puedan posponer la instalación de paquetes.

1.2.5 Monitorización de la actividad de red

Las funciones de la monitorización de red se llevan a cabo por agentes que realizan el seguimiento y registro de la actividad de red, la detección de eventos y la comunicación de alertas al personal responsable del buen funcionamiento de la red. Los eventos típicos que son monitorizados suelen ser:

- Ejecución de tareas como pueden ser realización de copias de seguridad o búsqueda de virus.
- Registro del estado de finalización de los procesos que se ejecutan en la red.
- Registro de los cambios que se producen en el inventario de hardware.
- Registro de las entradas y salidas de los usuarios en la red.
- Registro del arranque de determinadas aplicaciones.
- Errores en el arranque de las aplicaciones, etc.

En función de la prioridad que tengan asignados los eventos y de la necesidad de intervención se pueden utilizar diferentes métodos de notificación como son:

- Mensajes en la consola: se suelen codificar con colores en función de su importancia.
- Mensajes por correo electrónico: conteniendo el nivel de prioridad y el nombre e información del evento.
- Mensajes a móviles: cuando el evento necesita intervención inmediata se suele comunicar a los técnicos de guardia a través de este método.

Además de los eventos, otra característica importante es la monitorización del tráfico de red:

- Se toman nuevas medidas sobre aspectos de los protocolos, colisiones, fallos, paquetes, etc.
- Se almacenan en BBDD para su posterior análisis.
- Del análisis se obtienen conclusiones, bien para resolver problemas concretos o bien para optimizar la utilización de la red.

1.2.6 Seguridad

La seguridad es un aspecto que afecta a todas las áreas de administración que se han comentado anteriormente. Para cada recurso en la red, el administrador dispone de los mecanismos para establecer permisos de utilización, así como monitorizar el uso que se hace de los recursos.

Todas estas tareas son muy complejas por lo que se utiliza actualmente son políticas de seguridad. Las políticas de seguridad permiten establecer aspectos de seguridad en forma de perfiles que afectan a grupos de usuarios. Una vez definidas las políticas, el administrador sólo tiene que añadir los usuarios a los grupos establecidos con lo que adquieren los perfiles de seguridad. De esta forma la actualización de medidas de seguridad se hace sobre las políticas y no sobre los usuarios directamente.

Otro aspecto a considerar es el de la monitorización y registro de las actividades de los usuarios pudiendo denegar el acceso de los usuarios en función de que intenten realizar actividades para los que no tienen permiso.

1.3 EQUIPAMIENTO DE UNA RED DE DATOS

1.3.1 Agentes y consolas

Los agentes y consolas son los conceptos claves en la administración de redes.

- Consola: es una estación de trabajo convenientemente configurada para visualizar la información recogida por los agentes.
- Agentes: son programas especiales que están diseñados para recoger información específica de la red.

Entre las características de los agentes cabe destacar:

- Están basados en software frente a monitores y analizadores basados en hardware.

- Son transparentes a los usuarios. Se ejecutan en los puestos de trabajo sin afectar al rendimiento de los mismos.
- La información que recogen la almacenan en bases de datos relacionales que después son explotadas a través de las consolas.
- Los agentes son configurados de forma remota a través de la consola para su correcta operación.
- Al ser software pueden realizar las mismas tareas que los analizadores y hacen un mayor procesamiento de la información que obtienen.

Las funciones que soportan los agentes son entre otras:

- Visualizar y manipular información de la red.
- Automatizar la distribución de ficheros.
- Mantener el inventario del hardware.
- Gestión y configuración del software remoto.
- Recibir notificación de alarmas de red.
- Soportar y gestionar la impresión en red.
- Automatizar tareas como copias de seguridad y detección de virus.
- Monitorizar la utilización de discos y de ficheros.
- Establecer y gestionar la seguridad en la red.
- Procesar scripts.

1.3.2 Protección contra virus

La protección contra la entrada de virus en la red se suele hacer mediante la utilización de paquetes especiales basados en una parte servidora y un conjunto de agentes distribuidos en los puestos de trabajo. La parte servidora realiza las tareas de actualización contra nuevos virus, realiza tareas de registro de virus, comunicación de alarmas al administrador, comunicación con otros servidores distribuidos en la red con software antivirus, protección de los discos y ficheros de los propios servidores, etc.

Los agentes por su parte evitan la entrada de virus en los propios puestos de trabajo comunicando al servidor la detección de los virus y eliminándolos automáticamente siempre que sea posible.

1.3.3 Soporte de impresoras

La gestión centralizada de impresoras en la red permite reducir el tiempo y el esfuerzo que necesitan los usuarios para configurar la impresión desde unos puertos de trabajo y también permiten al administrador realizar una gestión unificada de todas las impresoras de la red.

Las actividades relacionadas con el soporte de impresoras son dos:

- Las relacionadas con el manejo de las impresoras por parte del administrador.
- Las relacionadas con la selección de impresoras e impresión por parte de los usuarios.

El modo de operar suele ser el siguiente:

- El administrador da de alta las impresoras en la red seleccionando los servidores que actuarán de spoolers, identificándolos con un nombre y asociando el driver correspondiente para su utilización.
- Posteriormente el administrador, establece las condiciones de acceso como permisos a los usuarios, horario de acceso a las impresoras, etc.
- El usuario después selecciona las impresoras de las que tiene acceso permitido y las instala en un puerto de trabajo de forma remota y transparente.
- Cuando el usuario imprime también tiene acceso a las colas de impresión de forma que puede añadir o eliminar trabajos de su propiedad.
- El administrador a través de la consola y los agentes de impresión monitoriza la actividad de las impresoras y soluciona problemas que puedan surgir.

1.3.4 Gestión del espacio de almacenamiento

La utilización masiva de servidores de ficheros y BBDD en las redes actuales han hecho del espacio de almacenamiento un recurso común a los usuarios y un elemento escaso que hay que optimizar. El administrador utiliza agentes que recolectan información sobre el grado de ocupación de los discos con objeto de tomar decisiones al respecto de la redistribución de ficheros y de la adquisición de nuevos discos.

La extracción de información que realiza el agente suele ser a nivel de:

- Partición: utilización del espacio de la partición (poco nivel de detalle).

- Directorios: grado de utilización del espacio para los directorios.
- Ficheros: tamaño que ocupan los ficheros.

Al igual que con otras actividades de administración se suelen programar una serie de eventos consistente en ciertos límites que cuando son sobrepasados elevan una alarma que es comunicada al administrador a través de un mensaje en la consola, un correo electrónico o un mensaje a un móvil por ejemplo. La tarea de recoger la información normalmente se puede hacer en background sin afectar a los procesos en ejecución aunque también pueden ser planificados para su posterior ejecución.

CAPÍTULO II

SISTEMA DE GESTIÓN DE LA RED

2.1 ARQUITECTURAS

Arquitecturas de Gestión de Red da un revisión acerca de las tecnologías de gestión de red actualmente disponibles y explica como el protocolo SNMP esta altamente relacionado.

2.1.1 Evolución de Redes hacia el Nuevo Milenio

Los 70's fue la década de red centralizada, dominada por el procesamiento del supercomputador, la comunicación de datos permitió a los terminales comunicarse a los supercomputadores. Baja velocidad, transmisión asíncrona fue la norma. Proveedores de supercomputador tal como IBM y proveedores de circuitos de comunicación tal como AT&T o la compañía de teléfonos local administró la red para esos sistemas.

Los 80's dieron los cambios considerables en la comunicación de datos. Los microprocesadores llegaron y ofrecieron precios significantes y ventajas de

rendimiento sobre los supercomputadores. El número de LANs basados en microcomputadores creció.

En los 90's las facilidades de transmisión de área amplia de alta velocidad, tal como circuitos en Frame Relay, emergieron para conectar LANs basados en microcomputadores. La proliferación de LANs elevó el procesamiento distribuido y cambió las aplicaciones en el supercomputador y en el ordenador de escritorio.

Mientras estamos en el nuevo milenio, Gigabit Ethernet en la LAN y la red óptica sincrónica (SONET) en la WAN ayudan a satisfacer la necesidad para el constante incremento de cantidades de BW. Y como la transmisión de datos desplazó a las redes distribuidas, la gestión de red llegó a ser distribuida también. Adicionales cambios son resultado del uso de tecnologías basadas en WWW, el cual usan ampliamente buscadores Web disponibles para acceder a información de gestión de red. Como los requerimientos de transporte de información han crecido tanto en complejidad y velocidad, las capacidades de gestión de redes también de madurar.

2.1.2 El reto de la gestión de red distribuida

Alguna veces la gente olvida que la gestión de red tiene dos partes: la Red y la Gestión. Para que una red sea manejado propiamente, todos deben estar de acuerdo en este significado y en sus objetivos. La gestión de red puede significar cosas diferentes para individuos diferentes en una organización; por ejemplo, para un CEO (Chief Executive Officer) es visto como una gestión financiera de la

red de comunicaciones corporativo que implica gestionar ordenes, inventario, información acerca de cuentas, etc. Para un CIO (Chief Information Officer) la perspectiva es tanto el presupuesto corporativo teórico como la perspectiva práctica de los usuarios finales. El reto es mantener la red corporativa trabajando el 99.99% del tiempo y organizar periodos de corte los fines de semana y feriados cuando pocos pueden notarlo. Entonces el CIO definiría la gestión de red como la habilidad de balancear los crecientes requerimientos del usuario final con menos recursos; esto es, mas servicio con menos dinero.

Los usuarios realizan trabajos dependiendo de la operatividad de la red. Ellos definirían la gestión de red como algo que mantiene la infraestructura de comunicación de datos, el cual ellos dependen trabajando todo el tiempo. Una falla en la red amenazaría sus trabajos cotidianos. Considerando el beneficio económico de la corporación, sus clientes y sus empleados, una definición compacta para gestión de red que los involucre sería: Las redes de comunicaciones es el enlace vital entre clientes y productos. Nuestro objetivo es mantener el enlace operativo todo el tiempo, porque cuando falla nuestro capital financiero sufre.

2.1.3 El sistema a ser administrado

Ahora veamos el alcance de la gestión de redes desde la perspectiva de la ingeniería de sistemas. Tenemos aplicaciones centralizadas tal como un sistema de control de inventario o la base de datos financiera de la corporación. Aplicaciones distribuidas, tales como los que corren sobre LANs cliente-servidor. Y los diferentes tipos de sistemas de transporte de área amplia: el transporte puede

consistir de redes públicas provistas por Inter-Exchange Carriers (IXCs), Local Exchange Carriers (LECs), Internet Service Providers (ISPs), e Internet Telephony Service Providers (ITSPs); las redes privadas pueden incluir tecnologías punto a punto, conexiones backbone, redes privados virtuales (VPN) y otros.

2.1.4 Elementos de una Arquitectura de Gestión de Red

El sistema de gestión de red, llamado el modelo gestor/agente, consiste de un gestor, un sistema gestionado, una base de datos de información de gestión, y el protocolo de red.

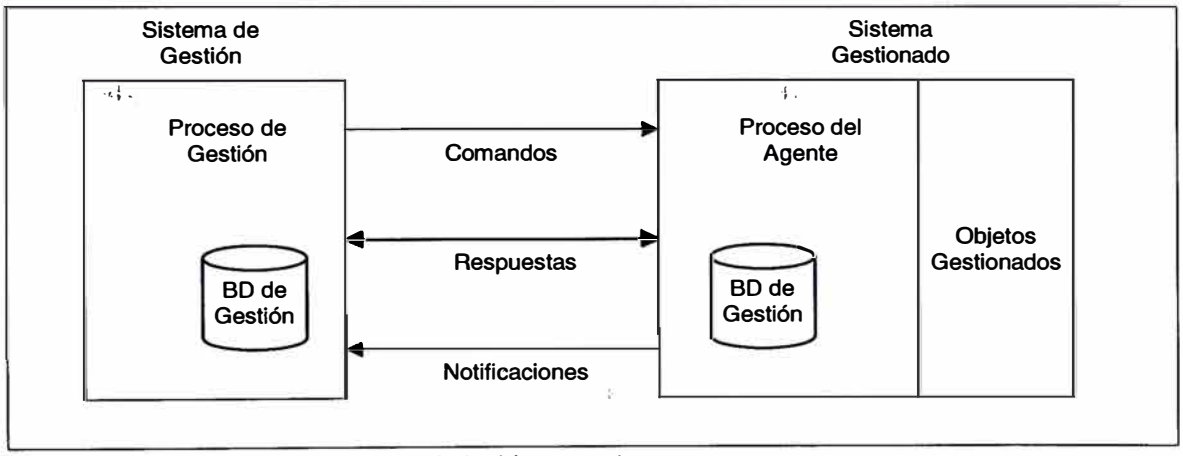

Fig. 2.1 Relación gestor/agente en una red

El gestor proporciona la interfaz entre administrador de red humana y los dispositivos a ser gestionados. También proporciona el proceso de gestión de red. El proceso de gestión realiza tareas tal como medición de tráfico de un segmento de LAN remoto o reproducir la velocidad de transmisión y dirección física de una interfaz LAN de un router. El gestor también incluye algunos tipos de salidas, usualmente gráficas, para mostrar la data gestionada, estadísticas históricas, y

otros. Un ejemplo común de una visualización gráfica es un mapa de la topología de una internetwork mostrando las ubicaciones de los segmentos LAN; seleccionando un segmento particular podría mostrar su actual estado de operación.

Como la Fig. 2.1 muestra, el sistema gestionado consiste del proceso del agente y los objetos gestionados. El proceso del agente realiza operaciones de gestión de red tales como fijar la configuración de parámetros y estadísticas operacionales actuales para un router en un segmento dado. Los objetos gestionados incluyen estaciones de trabajo, servidores, hubs, circuitos de comunicación, y otros. Asociado con los objetos gestionados son atributos, los cuales pueden ser definido estáticamente (tal como la velocidad de una interfaz), dinámico (tal como entradas en una tabla de rutas), o requiere medición continua (tal como el número de paquetes transmitidos sin errores en un periodo de tiempo dado).

Una base de datos de información de gestión de red, llamado el MIB (Management Information Base), esta asociado con ambos el gestor y el sistema gestionado. Tal como una base de datos numérica tiene una estructura para almacenar y recuperar datos, un MIB tiene una organización definida. Esta organización lógica es llamada la estructura de información de gestión o SMI (Structure of Management Information). El SMI esta organizado en una estructura árbol, empezando en la raíz, con ramas que organizan los objetos gestionados por categorías lógicas. El MIB representa los objetos gestionados como las hojas de las ramas.

El protocolo de gestión de red proporciona una manera de comunicación para el gestor, los objetos gestionados, y sus agentes. Para estructurar el proceso de comunicación, el protocolo define mensajes específicos, referidos como comandos, respuestas, y notificaciones. El gestor usa estos mensajes para requerir información de gestión específica, y el agente los usa para responder. Los bloques construidos de los mensajes son llamados unidades de datos de protocolo ó PDUs (Protocolo Data Units). Por ejemplo, un gestor envía un GestRequest PDU para recuperar información, y el agente responde con un GetResponse PDU.

Como se observa en la Fig. 2.2, una consola, tal como una estación SPARC de Sun Microsystems, Inc., típicamente realiza las funciones de gestor de red. Los dispositivos en la internetwork, tales como routers y computadores, contienen agentes de gestión de red. MIBs están asociados con ambos el gestor y los agentes, pero los MIBs del router y los MIBs del host probablemente no son los mismos por dos razones. Primero, estos dispositivos usualmente vienen de diferentes fabricantes quienes tienen implementados funciones de gestión de red en diferente, pero complementario maneras. Segundo, los routers y hosts realizan diferentes funciones de internetworking y pueden no necesitar almacenar la misma información. Por ejemplo, el host puede no requerir tablas de rutas, y así no necesitará almacenar parámetros relacionado a tablas de rutas tal como el próximo salto hacia un destino particular en sus MIBs. Contrariamente, un MIB de un router podría no contener una estadística tal como la utilización de CPU que puede ser significante para un host.

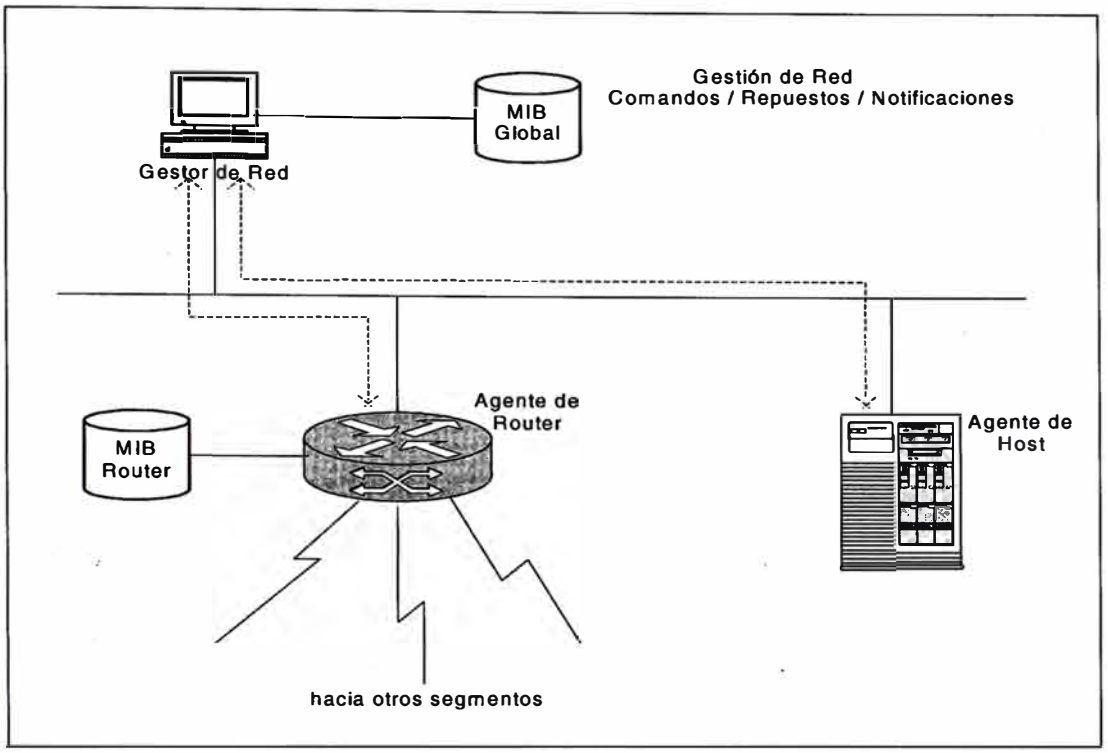

Fig. 2.2 Realización gestor/agente en la red

Un protocolo tal como SNMP permite comunicarse al gestor y los agentes. Este protocolo proporciona la estructura de comandos desde el gestor, notificar al gestor de eventos significantes desde el agente, y responder tanto al gestor o al agente.

2.1.5 La Arquitectura de Gestión de Red OSI

El sistema de gestión de red para el modelo de Interconexión de Sistemas Abiertos de la Organización de Estándares Internacional ó ISO/OSI (International Standars Organization's Open Systems Interconection) ha sido aplicado para redes de computadores desde que fue primera vez publicado en 1978. La Fig. 2.3 muestra la estructura familiar de 7 capas. A continuación un resumen de las 7 capas:

Capa	Descripción
Física	Proporciona el medio de transmisión físico para portar una fila de datos, tales como impulsos eléctricos u ópticos, desde un modo de red a otro.
Enlace de Datos	Proporcionar una comunicación confiable del enlace; esto es, crea el canal entre los nodos adyacentes en una LAN, MAN ó WAN. Tiene funciones de direccionamiento, trama y control de error en el enlace.
Red	Proporciona funciones de comunicación para un internetwork. Tareas como direccionamiento global, ruteo, y switching que toma los datos desde su fuente a su destino vía una internetwork de LANs, MANs y WANs.
Transporte	Asegura la confiabilidad de entrega de datos de extremo a extremo. Incluye funciones de control de error y control de secuencia.
Sesión	Establece la conexión lógica entre aplicaciones de usuario final. Estas funciones incluyen mecanismos que sincronizan la transferencia de datos una vez que una conexión sea establecida.
Presentación	Representa los datos de aplicación para ser propiamente interpretado en la ubicación distante. Ejemplo de estas funciones incluyen compresión/descompresión de datos, encriptación, o conversión de código ASCII a EBCDIC.

Aplicación	Incluye las funciones responsable para aplicaciones de usuario final, tales como transferencia de archivos, correo electrónico, o acceso de terminal remoto. SNMP es un protocolo de Capa de Aplicación.

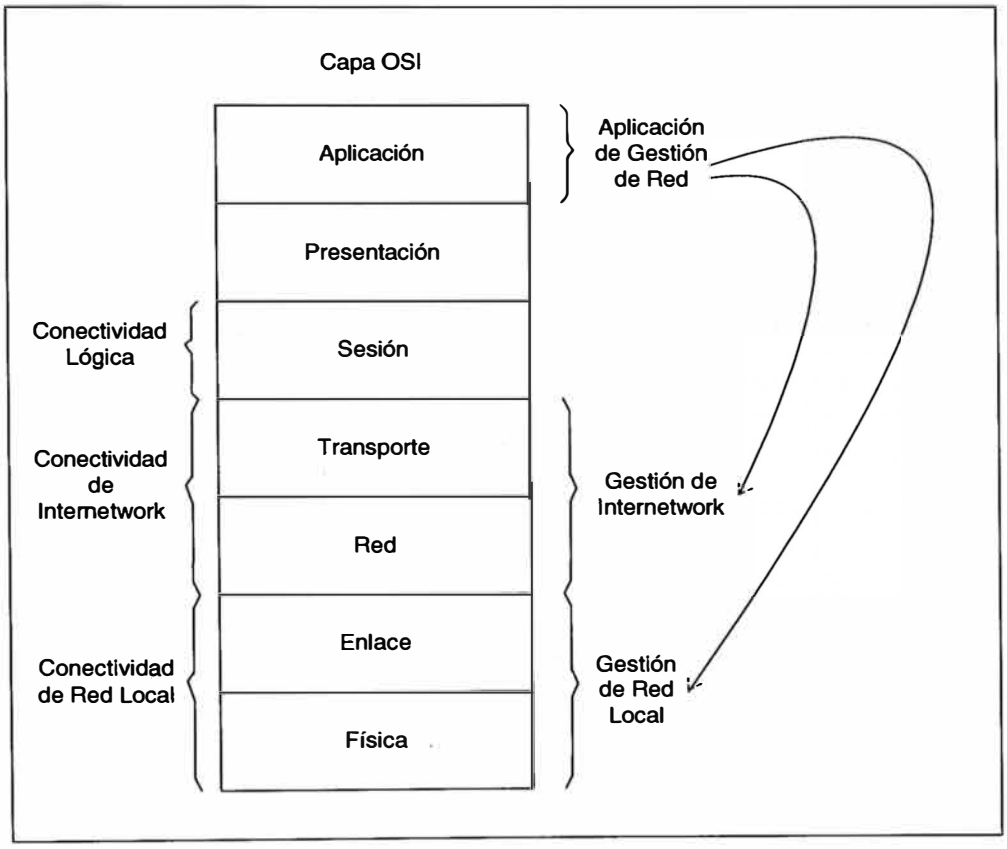

Fig. 2.3 Gestión de red dentro de la estructura de OSI

- El Modelo de Gestión OSI

El modelo gestor/agente incluye un numero de componentes interactivos. La estructura de trabajo de red OSI define los roles de estos componentes. El modelo organizacional usa un dominio de gestión. (ver Fig. 2.4). El dominio puede contener uno o mas sistemas de gestión, sistemas gestionados, y sub-dominios. El sistema gestionado puede, a su vez, contener una o mas objetos gestionados. Cada

objeto es un recurso de red que uno de los sistemas gestionados puede monitorear y/o controlar. De este ejemplo, nosotros podemos hacer diversas observaciones. Primero, la aplicación de gestión de red del gestor debe ser compatible con la del agente. Desde que este ejemplo usó un esquema de gestión de red basado en OSI, el CMIP (Common Management Information Protocol) podría proporcionar comunicación compatible. Segundo, las otras capas de las otras arquitecturas computadas deben también ser compatibles. Si la capa de red de la consola usa el CLNP de OSI (Connectionless Network Protocol) definido por ISO 8473, el router debe también entender ese protocolo. Finalmente, la misma camino física debe conectar al gestor y al agente, aunque ese camino no tiene que estar en la misma LAN o aún en el mismo país.

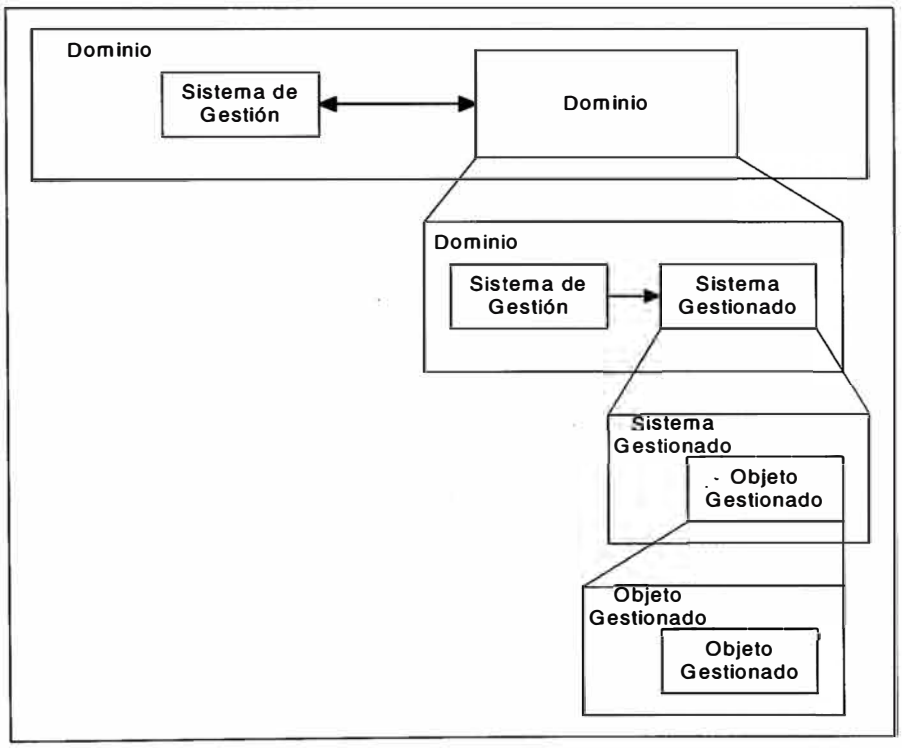

Fig. 2.4 Modelo organizacional abstracto del ambiente de Gestión

Un modelo de información asociado con el modelo organizacional define la estructura de gestión de información y la base de información de gestión (MIB). Como puede verse en la Fig. 2.5, una estructura de árbol agrupa objetos que comparten similares características en clases. Estos objetos son representados como una entrada en el árbol de información de gestión, cada entrada ha definido atributos y valores.

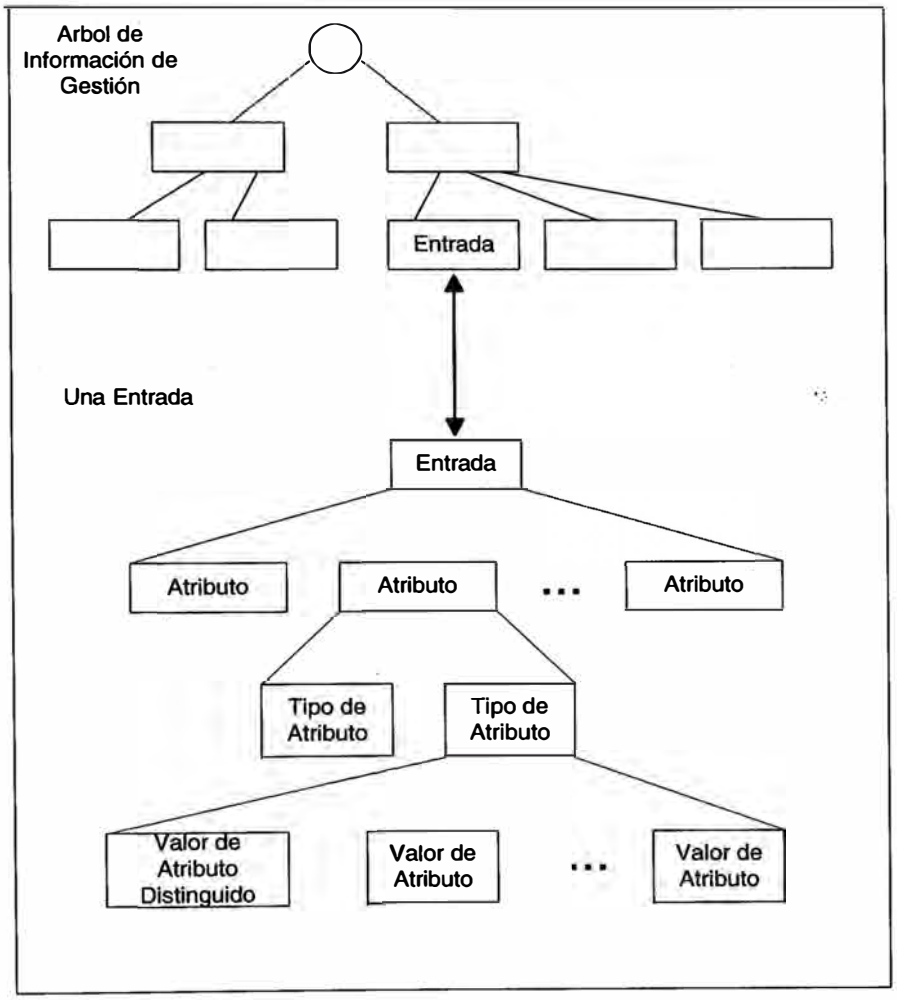

Fig. 2.5 Árbol de información de Gestión

El modelo funcional define cinco áreas de gestión de red usados para propósitos específicos. La siguiente sección explora estos cinco áreas en detalle.

La Fig. 2.6 demuestra como los varios elementos trabajan juntos. Este modelo relaciona el proceso de aplicación de gestión del sistema (SMAP) a una base de información de gestión (MIB) y las 7 capas del sistema de gestión de red. Define interfaces para el sistema de gestión (SMI) y la capa de gestión (LMI). Las funciones de gestión de capa son específicas para una entidad de capa de OSI. Ejemplos de estas funciones incluirían parámetros específicos de capa, pruebas, o servicios los cuales residirían en una entidad de capa de gestión (LME). El modelo también especifica un protocolo para comunicación de gestor/agente, conocido como Protocolo de Información de Gestión Común o CMIP.

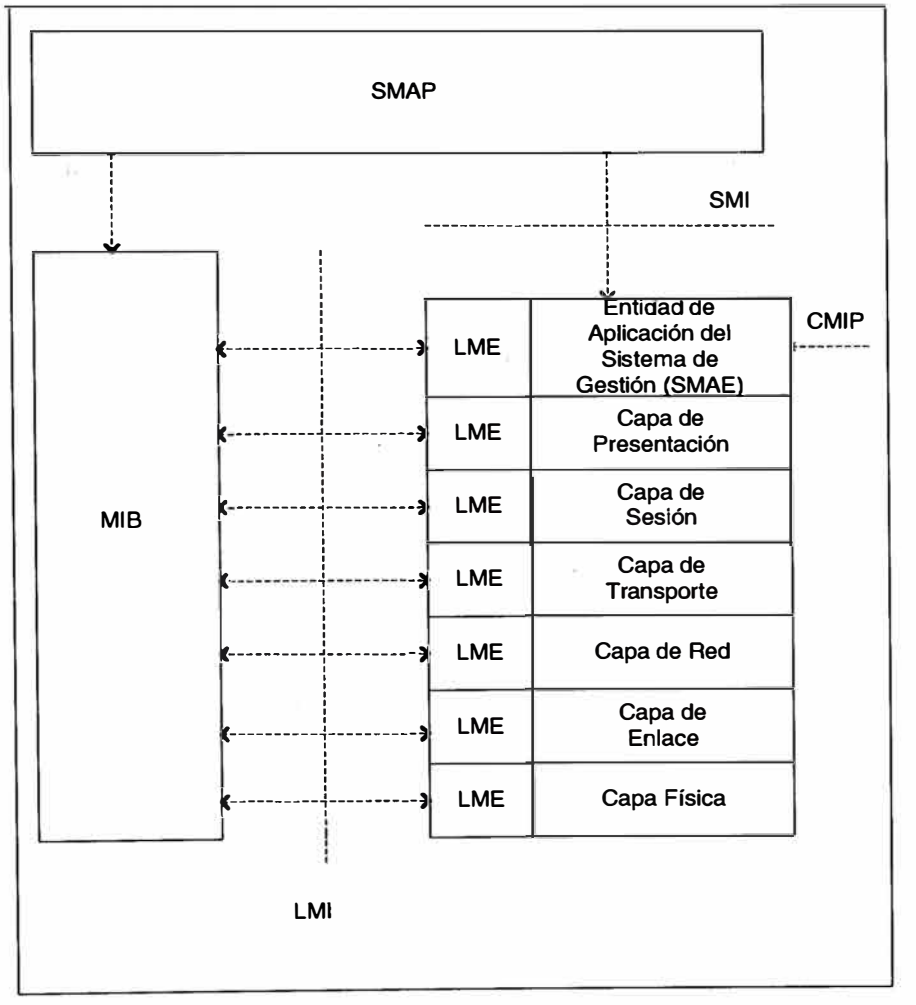

Fig. 2.6 Modelo de arquitectura de Gestión de OSI

2.1.6 La Arquitectura de Gestión de Red IEEE

IEEE (Institute of Electrical and Electronics Engineers), el mejor conocido en el campo de comunicaciones de datos por desarrollar las series 802 de estándares LAN. Estos incluyen especificaciones para acceso múltiple por sentido de portadora con detección de colisiones (CSMA/CD) en LANs tales como 802.3 10BASE-T y 802.5 token-ring. Pero los estándares de gestión IEEE 802.1B LAN/WAN son otros elementos claves del trabajo IEEE.

El proyecto IEEE 802 guía las capas física y de enlace y se extiende en capas mas altas de la arquitectura donde es apropiado. El estándar de gestión IEEE LAN/MAN usa CMIP de ISO, el cual fue expuesto en la arquitectura con OSI, para extender hacia las capas mas altas. Esta arquitectura incluye tres elementos (ver Fig. 2.7): el servicio de gestión de LAN/MAN (LMMS), la entidad de protocolo de gestión de LAN/MAN (LMMPE), y la entidad de protocolo de convergencia (CPE). El LMMS define la disponibilidad de servicio de gestión para el usuario de gestión LAN/MAN (LMMU). El LMMPE comunica la información de gestión vía intercambio de protocolo. LMMS y LMMPE usan los estándares CMIS y CMIP de ISO y habilita dos LMMUs para intercambiar la información de gestión. El CPE permite al ambiente LAN/MAN proporcionar LMMS. El CPE adiciona funciones de confianza y entrega de datos secuencial sobre el servicio de no reconocimiento sin conexión provista por la capa de enlace según IEEE 802.2 LLC. El servicio de no reconocimiento sin conexión es conocido como LLC de tipo 1.

Fig. 2.8 ilustra la interacción entre estas operaciones de gestión de red. Diversos procesos cooperativos hacen la solicitud desde un gestor (un LMMU) hacia un agente (otro LMMU). El LMMS del gestor lo solicita (REQ) usando el protocolo LMMP. El agente recibe esta solicitud como una indicación (IND). El agente realiza operaciones en los objetos gestionados y luego retorna los resultados como un respuesta (RSP). Finalmente, el LMMPE devuelve la confirmación (CONF) al gestor.

Un objeto gestionado realiza una serie de pasos similares para notificar al gestor de eventos (Fig. 2.9). El objeto gestionado envía una notificación al agente, generando un solicitud (REQ) al LMMS. El LMMPE comunica ese requerimiento a lo largo de la LAN, produciendo una indicación (IND) al gestor. Finalmente, el gestor aclara una respuesta (RSP), el cual el agente recibe como una confirmación (CONF).

La Fig. 2.10 compara la arquitectura IEEE con el modelo OSI. La complejidad de los protocolos varía significantemente. Mientras CMIP usa todas las 7 capas del modelo ISO, el modelo IEEE corre CMIP y el CPE directamente sobre la capa LLC – con el acrónimo CMOL, el cual es para referirse a CMIP sobre LLC. Debido a que LLC proporciona servicio sin conexión a una aplicación de gestión, algunos de las funciones ACSE (Association Control Service Element) en el paquete completo del CMIP son innecesarios. El CPE completa y realiza algunos, pero no todo, las funciones de capa de Presentación a través de la red. El beneficio de un CMOL reducido es que minimiza los requerimientos de memoria para los

agentes. La desventaja es que no puedes encaminar CMOL a lo largo de una internetwork por la falta de funcionalidad de la capa de red. Esto no es sorprendente, desde que CMOL fue diseñado desde una perspectiva LAN y no una internetwork.

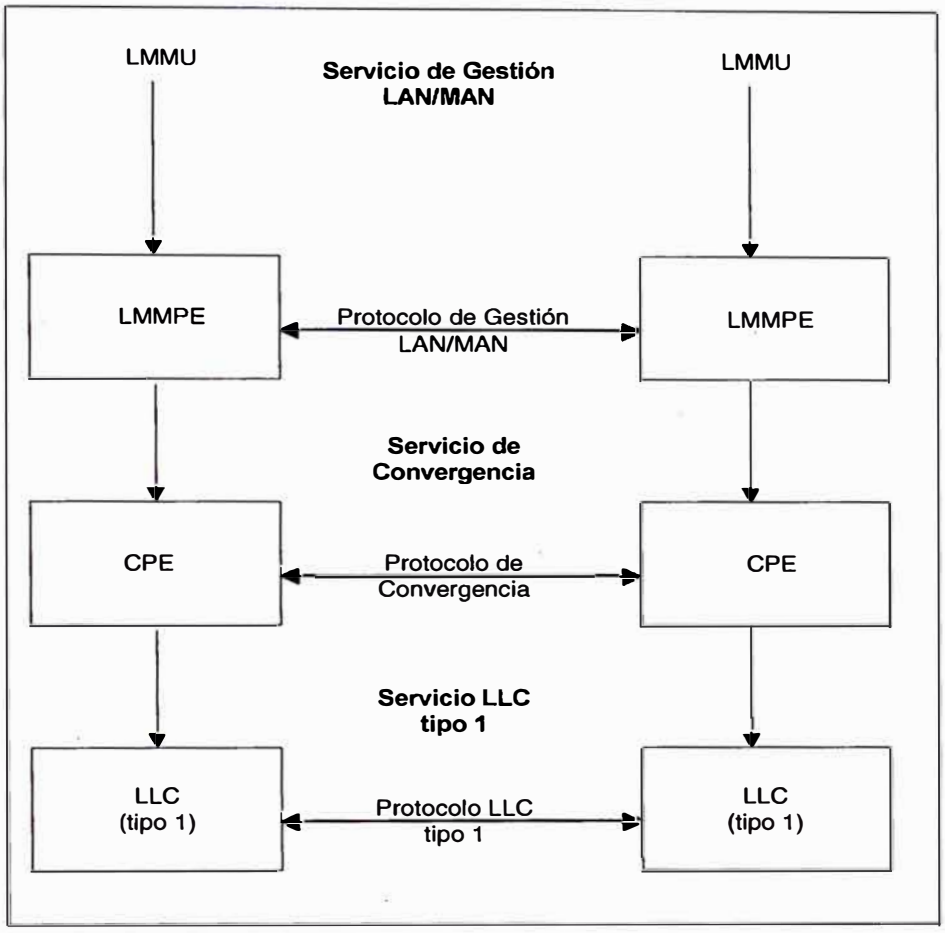

Fig. 2.7 Arquitectura de comunicación de Gestión LAN/MAN

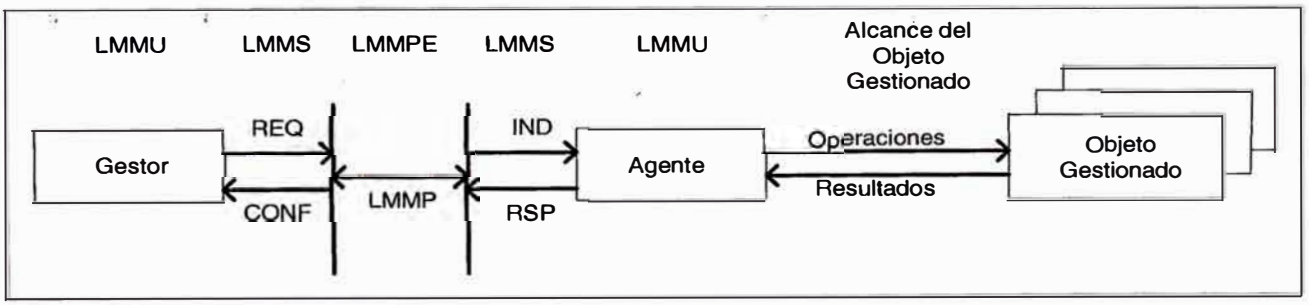

Fig. 2.8 Intercambio de Información de Gestión LAN/MAN: Operaciones

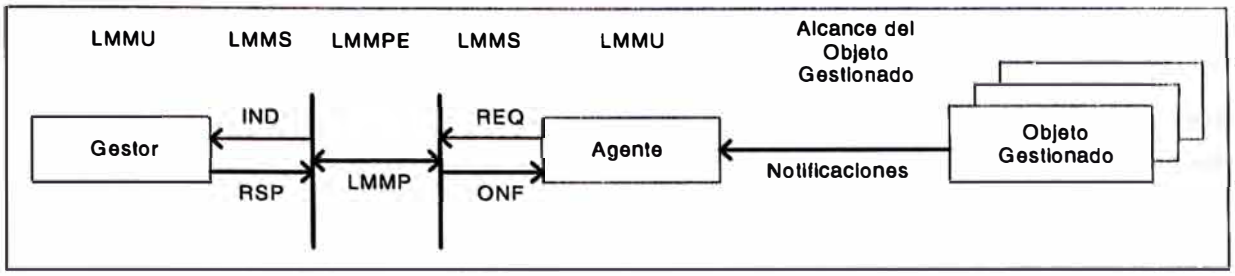

Fig. 2.9 Intercambio de Información de Gestión LAN/MAN: Notificaciones

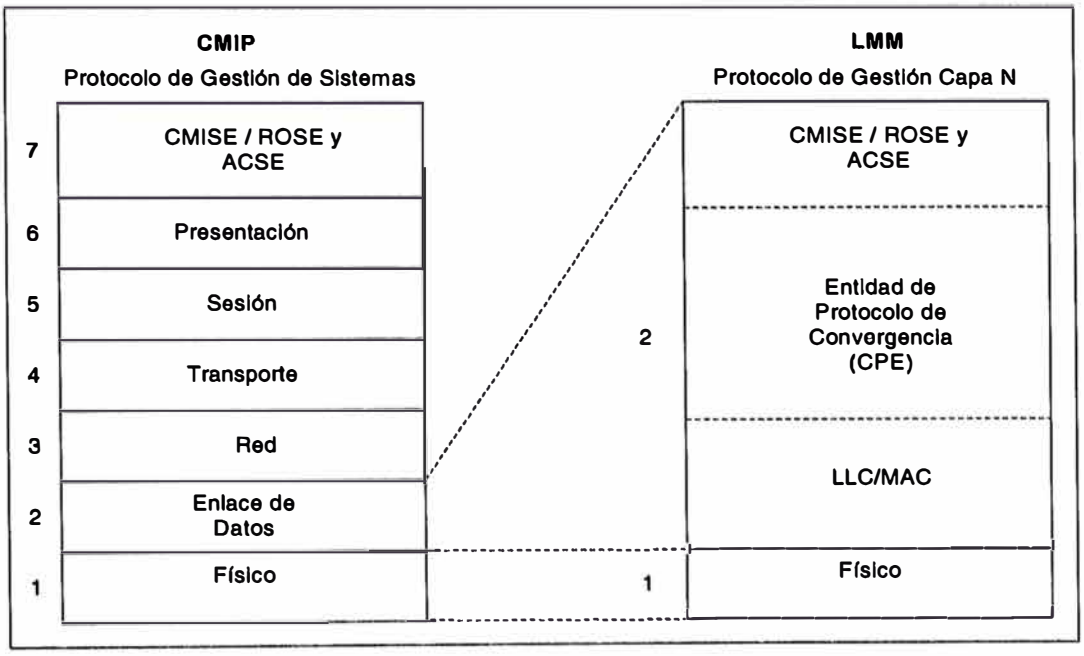

Fig. 2.10 Comparación de protocolos CMIP y LMMP

2.1.7 Comisión de Investigación de Gestión de Ordenador

La comisión de Investigación de Gestión Distribuida (DMTF) fue fundado en 1992 por Digital Equipment, Hewlett-Packard, IBM, Intel, Microsoft, Novell, SunSoft, y SynOptics Communications (ahora parte de Nortel Networks). El propósito de DMTF es desarrollar un conjunto de estándares de interfaces de aplicaciones programables (APIs) que acceden y gestionan sistemas de ordenadores, componentes y periféricos relacionados. Actualmente, mas de 300 organizaciones son miembros de DMTF. El DMTF también esta involucrado en la

gestión de red basada en web, el cual será descrito posteriormente. La tecnología de Interfaz de Gestión de Ordenador (DMI) es una arquitectura de gestión desarrollado por el DMTF (ver Fig. 2.11). El DMI esta enfocado en la gestión de Ordenar y LAN, independiente del sistema, sistema operativo, o sistema de operación de red. DMI esta diseñado para integrarse con todos los protocolos y consolas de gestión de red, tal como SNMP o CMIP. La arquitectura DMI esta dividida en tres capas: la capa de aplicaciones de gestión, los cuales interactúan con varios agentes; la capa de servicio, el cual incluye el archivo de base de datos de información de gestión (MIF); y la capa de componentes de hardware y software, los cuales interactúan con los componentes actuales a ser gestionados.

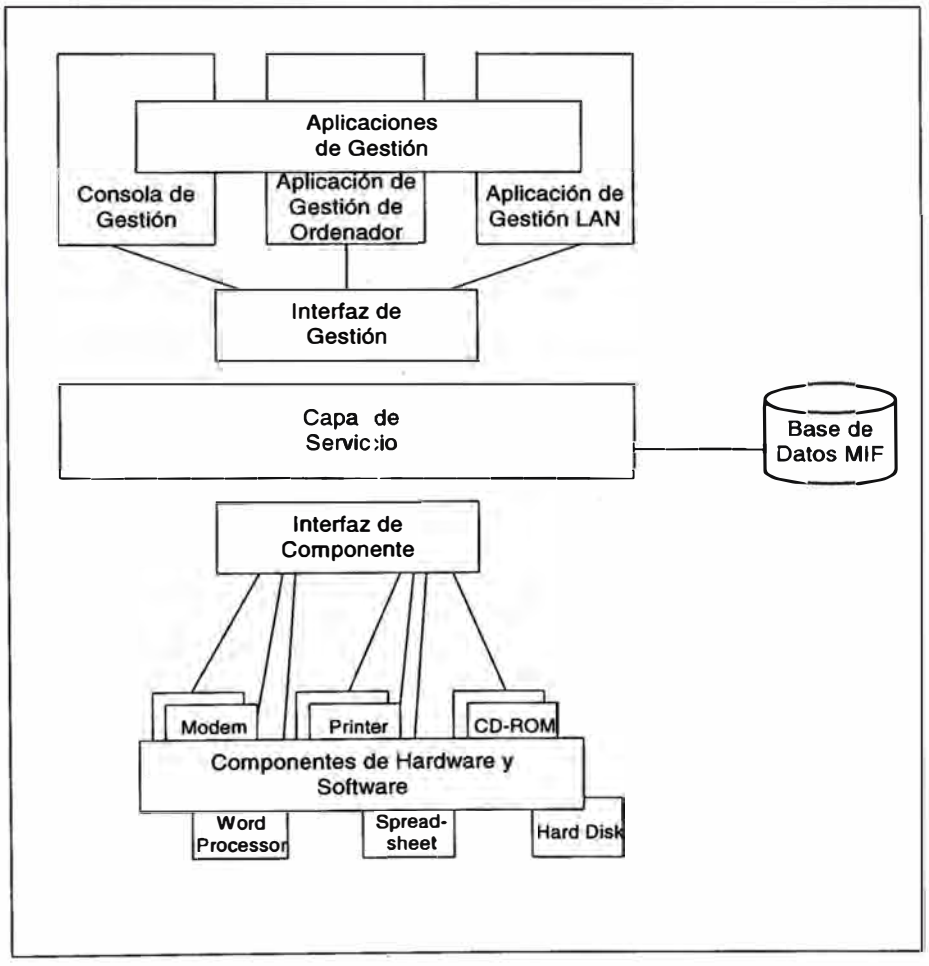

Fig. 2.11 Interfaz de Gestión de Ordenador

2.2 PLATAFORMAS

Las plataformas de gestión de red han evolucionado en los pocos últimos años, como los sistemas clientes han llegado a ser mas distribuidos y complejos. Por ejemplo, los sistemas de gestión a fines del 80, frecuentemente fueron llamados gestores de dispositivos, fueron enfocados en un simple dispositivo o sistema, tal como un multiplexor o un módem de alta velocidad. La primera progresión revolucionaria ocurrió a comienzos de los 90 mientras las plataformas de gestión de red intentaron integrar múltiples gestores de dispositivos en un ambiente cohesivo y comunicativo. Integración adicional llegó a ser posible cuando la industria comenzó a usar SNMP como el estándar de comunicación entre agentes y gestores, y así se asegura la interoperabilidad de los vendedores entre componentes. Otros cambios hacia la integración involucró el compartimiento de la información de base de datos entre varias aplicaciones de modo que, por ejemplo, una alarma de un agente podría activar automáticamente una página para el gestor de red y poner en bitácora una entrada en la aplicación de reporte del ticket de problema. Sin embargo, todos estos mejoramientos han enfocado en los sistemas de gestión de red y su interacción con agentes y aplicaciones, mas que en la interfaz del usuario hacia la información de gestión de red.

Una de las interfaces mas comunes que ha evolucionado en años recientes es el WWW (World Wide Web), o simplemente la Web. Los sistemas basados en web consisten en un servidor que almacena "páginas" o información que son típicamente formateados usando el HTML (HyperText Markup Language). El cliente accede a la información usando software llamado un buscador Web, el cual

puede haber integrado potenciales para impresión, recuperación y almacenamiento de archivo, correo electrónico, y así sucesivamente. El protocolo de comunicación entre el servidor y el cliente es el HTTP (HyperText Transfer Protocol), el cual es un protocolo orientado a la transacción que hace use del TCP (Transmission Control Protocol). Una de las ventajas de esta arquitectura es su independencia de plataforma, mientras los buscadores de Web de un número de plataformas de clientes, incluyendo Macintosh, Windows, UNÍS, y otras estaciones de trabajo, pueden acceder al servidor Web de manera similar. El tráfico basado en Web ahora consume una larga porción del tráfico en Internet.

La popularidad de estos sistemas basados en Web han creado otra aplicación para esta tecnología – almacenamiento de información de gestión de red en un servidor Web de modo que ello puede ser accedido y propagado a usuarios distribuidos en una moda independiente de plataforma. La gestión de red basado en Web puede tomar una de las diversas formas:

- Los agentes habilitados en Web que pueden ser gestionados a través de un buscador usando el HTTP para comunicación.
- Los gestores habilitados en Web, los cuales pueden incluir un servidor de Web frontal hacia una plataforma existente o gestor único corriendo en un servidor Web, y el cual también puede usar el HTTP para comunicación.
- La propuesta de gestión de empresa basado en Web (WBEM), de un consorcio de vendedores el cual incluye Microsoft, Compaq Computer, Cisco Systems, y muchos otros, el cual es ahora parte de la labor del DMTF.

- La interfaz de programación de aplicación de gestión Java (JMAPI) propuesta de SunSoft.

En cualquier evento, sin embargo, el SNMP aún entra en la igualdad, ya sea desde la perspectiva de comunicación con existencia legal de gestores y/o agentes SNMP, o de la necesidad de proveer funcionalidad técnica que otras soluciones no cubren adecuadamente. Por ejemplo, el HTML que es usado para definir el formato de las páginas Web – y es entonces transmitido con el http – no es bien apropiado para el monitoreo del gestor/agente. Esto es porque existe un requerimiento para el "humano local" para presionar un botón para inicializar la secuencia de comunicación. La comunicación del gestor/agente usando métodos de comunicación con SNMP existente son probablemente a ser prevalecientes hacia otras propuestas, tal como JMAPI y WEBM, alcanzar madurez.

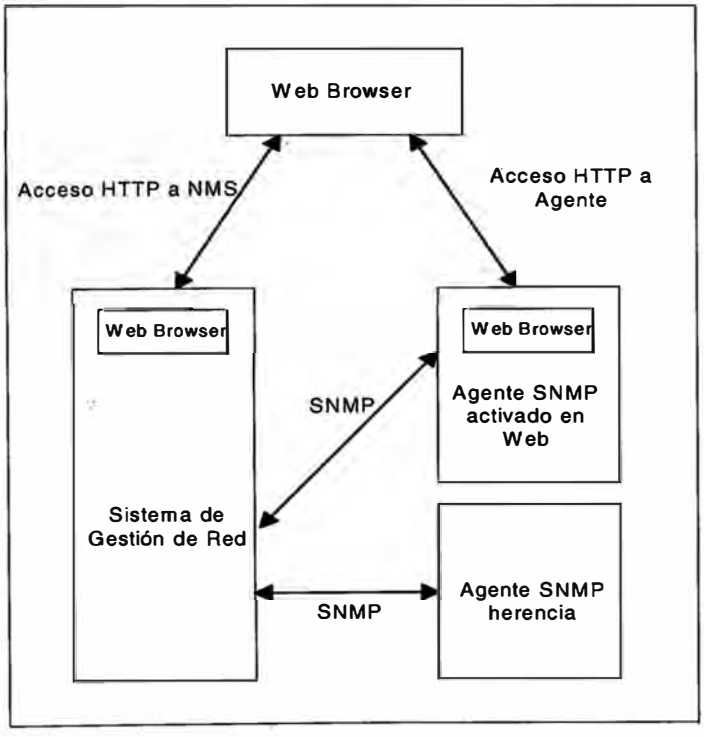

Fig. 2.12 Arquitectura de Gestión basada en Web

2.2.1 Gestión de Empresa basado en Web

La iniciativa de WBEM dirige el reto de redes distribuidas usando tecnologías emergentes basado en Web. Otras metas incluyen la integración de red, sistemas, y aplicación de gestión; independencia de ambiente de gestión y plataforma; escalabilidad para crecer mientras las redes se expanden; y balancear el bajo costo de clientes habilitados en Web. La propuesta de WBEM consiste de diversos elementos (ver Fig. 2.13):

- HMMS (HyperMedia Management Schema), un modelo de datos expansible el cual puede ser usado para describir los objetos gestionados. El DMTF fue autenticado con definición adicional del HMMS.
- HMMP (HyperMedia Management Protocol), el cual es un protocolo de comunicación que involucra el HMMS y corre sobre el http, con interfaces para SNMP y DMI en el futuro. El HMMP permite los datos agregados a ser buscados a lo largo de la red y compartido entre aplicaciones de alto nivel. El IETF fue autenticado con refinamiento adicional del HMMP.
- HMMO (HyperMedia Managed Object) es una entidad gestionada, contiene al menos un URL, que contiene datos que pueden ser gestionados por un buscador cliente, bien directamente o a través de algún tipo de esquema de gestión.
- HMOM (HyperMedia Object Manager) es una definición genérica para aplicaciones de gestión que combina información de múltiples fuentes y usa un protocolo de comunicación para presentar esa información al cliente (buscador) usando el HTML. Es anticipado que el HMOM podría ser implementado usando un número de plataformas de desarrollo, tal como Java, Active X, CGI (Common

Gateway Interface), CORBA (Common Object Request Broker Architecture), y otros.

En Junio de 1998, trabajo continuo sobre iniciativas WBEM y DMI fue cedido al DMTF. Este es visto como un esfuerzo para proporcionar alguna cohesión entre estas especificaciones y algún trabajo en curso en el DMTF. WBEM llega a ser el paraguas bajo el cual una variedad de especificaciones DMTF, tal como DMI, son ubicados. Dos iniciativas adicionales, el CIM (Common Information Model) y DEN (Directory-Enabled Networking), están también bajo el global WBEM.

CIM proporciona la base para WBEM. CIM define los esquemas que son usados para representar los objetos del mundo real que están siendo gestionados, usando un paradigma orientado al objeto. Describe un método común de estructuración de datos de gestión a través de diferentes sistemas de gestión, y facilita la integración de información de gestión desde estas diferentes fuentes. Así, datos de diferentes elementos de red y sistemas, tales como CMIP, SNMP, y DMI, podrían ser descritos y relatados en un formato estándar. El protocolo de aplicación a aplicación definido bajo CIM es el XML (Extensible Markup Language), el cual define un formato común para el intercambio de información de gestión. DEN es también un elemento del modelo CIM; integra directorios y servicios para funciones de gestión a nivel de empresa.

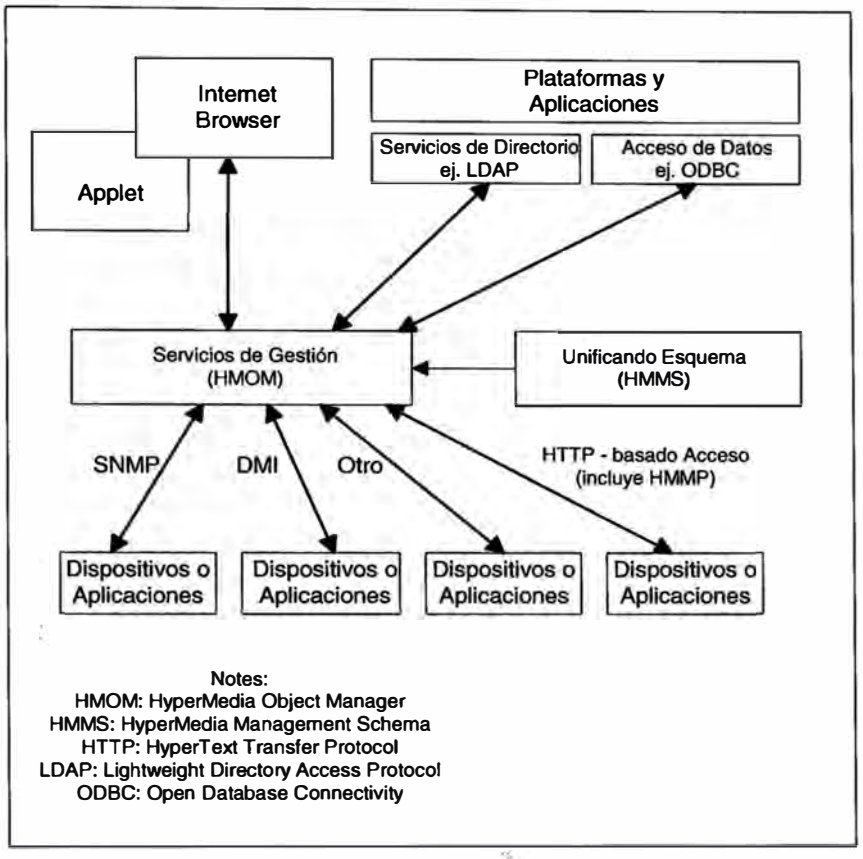

Fig. 2.13 Arquitectura WBEM

2.2.2 Interfaz de Gestión Java

Java de SunSoft es un simple pero robusto lenguaje de programación orientado a objetos que ha sido implementado a través de una amplia variedad de plataformas y sistemas operativos. El JMAPI es un conjunto de objetos y herramientas desarrolladas para crear soluciones de gestión de red que pueden ser usados por una amplia variedad de redes heterogéneas. Así, el JMAPI apalanca la independencia de plataforma del ambiente de computación Java, extendiendo las capacidades "escribir una vez, correr en cualquier lugar" de Java a las tradicionalmente arquitecturas propietarias de sistemas de gestión de red y consolas. En suma, el JMAPI permite para la integración de información del

agente SNMP en el ambiente Java, así apalancando soluciones de gestión de red clásico con la emergente tecnología de gestión de red basada en Web.

El JMAPI consiste de tres componentes funcionales: un BUI (Browser User Interface), un ARM (Admin Runtime Module), y accesorios.

El BUI es el medio por el cual el administrador de red publica los comandos y pedidos de gestión. El BUI requiere un buscador de Web habilitado en Java que tiene las capacidades para correr applets de Java. Los applets son programas Java que pueden ser incluidos en una página HTML tan igual que las gráficas, tal como archivos .GIF, pueden ser incluidos en una página. Cuando un buscador compatible con Java visualiza una página conteniendo un applet, el código applet es transferido, y luego ejecutado, el buscador. El BUI usa el http para comunicación con un servidor http con un ARM (Admin Runtime Module), el cual carga el applet Java inicial y objetos JMAPI. Otra comunicación a lo largo de los límites de máquina usa el RMI (Remote Method Invocation). El applet JMAPI consiste del AVM (Administrative View Module), el cual provee un conjunto de bloques para interfaz de usuario y funcionalidad a nivel de aplicación. Las interfaces de objetos gestionados realizan funciones de gestión remota.

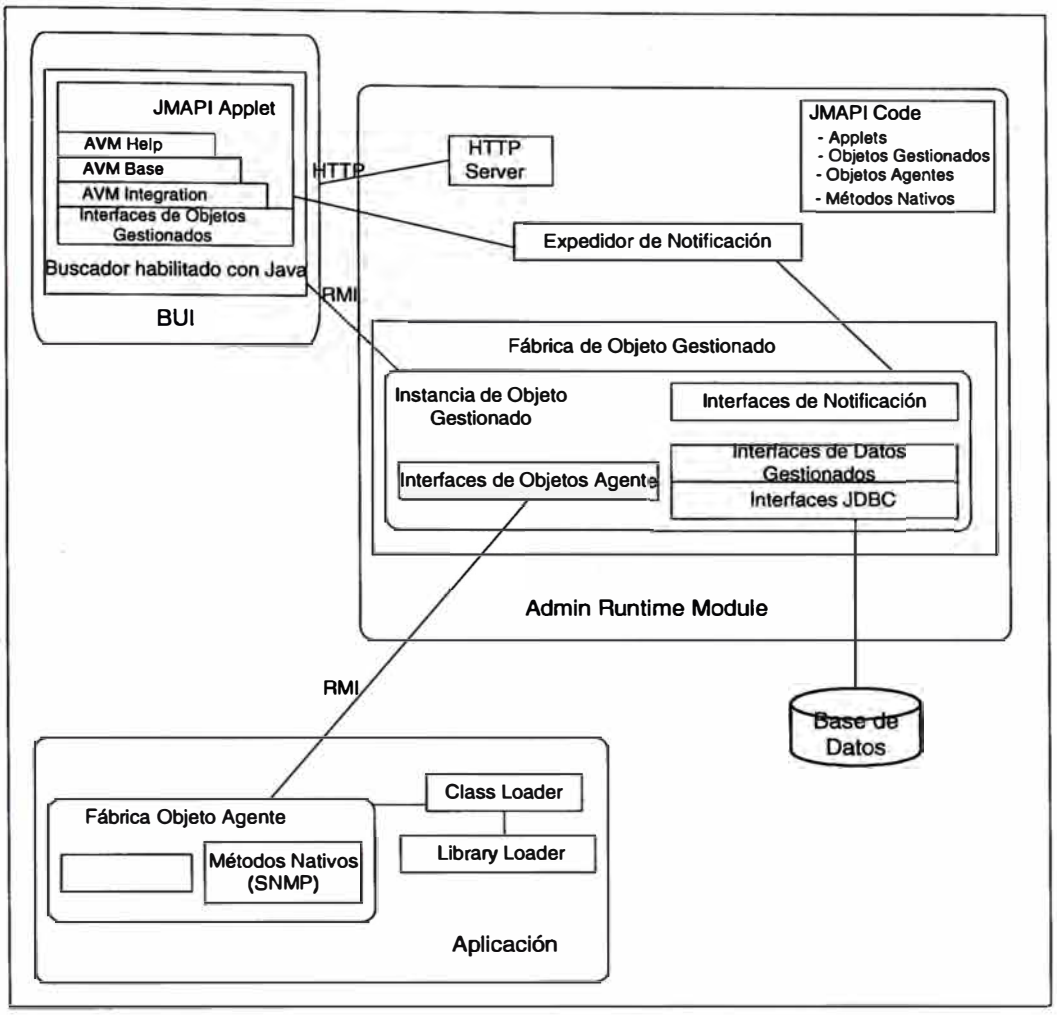

Fig. 2.14 Componentes de Arquitectura API de Gestión Java

El ARM es el centro de fuerza de administración; consiste de diversos elementos. El servidor http provee servicios de recarga para elementos Java. Después de que los applets Java toman control, las interfaces de objetos gestionados en el BUI proveen el enlace de comunicación al ARM. La fábrica de objetos gestionados implementa operaciones de gestión e interactúa con las interfaces de objetos de agentes y las interfaces de datos gestionados. Las interfaces de datos gestionados acceden una base de datos relacionado a través de la interfaz JDBC (Java Database Connectivity), el cual proporciona el depósito de información de gestión.

Las aplicaciones son los dispositivos siendo gestionados por el ARM. Una aplicación contiene una fábrica de objeto agente que crea y mantiene instancias de objetos agentes. Cuando los objetos son invocados, ellos pueden bajar código Java para implementar operaciones de gestión. Integración con agentes SNMP, el cual puede implementar el protocolo y manejar traps, también ha sido diseñado en el sistema.

Así, el API de gestión de Java proporciona las herramientas para desarrollar sistemas de gestión de red y servicio que pueden operar a lo largo de una diversidad de sistemas y plataformas.

2.3 APLICACIONES

Ahora que hemos considerado los elementos de un sistema de gestión de red, describiremos arquitecturas a nivel de aplicación de vendedores prominentes que soportan sistema de gestión basado en SNMP. Esta sección aborda, en orden alfabético, presenta desde Cabletron Systems, Inc., Hewlett-Packard Company, SunSoft, Inc., y Tivoli Systems.

2.3.1 Cabletron Systems' SPECTRUM

El gestor de empresa Cabletron Systems' SPECTRUM Enterprise Manager es diseñado como un sistema abierto para ser implementados en ambientes de diversos vendedores. La arquitectura esta basada en un paradigma cliente/servidor, con varias interfaces hacia otros sistemas. SPECTRUM consiste de dos elementos principales. Una interfaz de usuario gráfica (GUI), llamado

SpectroGRAPH, proporciona una interfaz basado en Motif para el usuario final. El servidor de gestión, llamado SpectroSERVER, consiste de dos secciones. La máquina de Red Virtual (VNM) crea modelos de varias entidades de red, tales como cables o dispositivos de red. El gestor de comunicación de dispositivo (DCM) es una máquina de comunicaciones de varios protocolos con protocolo soporte para SNMP, IEEE 802.1, y comandos ICMP/PING, con soporte futuro planeado para CMIP tanto como extensiones (vía un conjunto de herramientas) para cualquier protocolo propietario (ver Fig. 2.15).

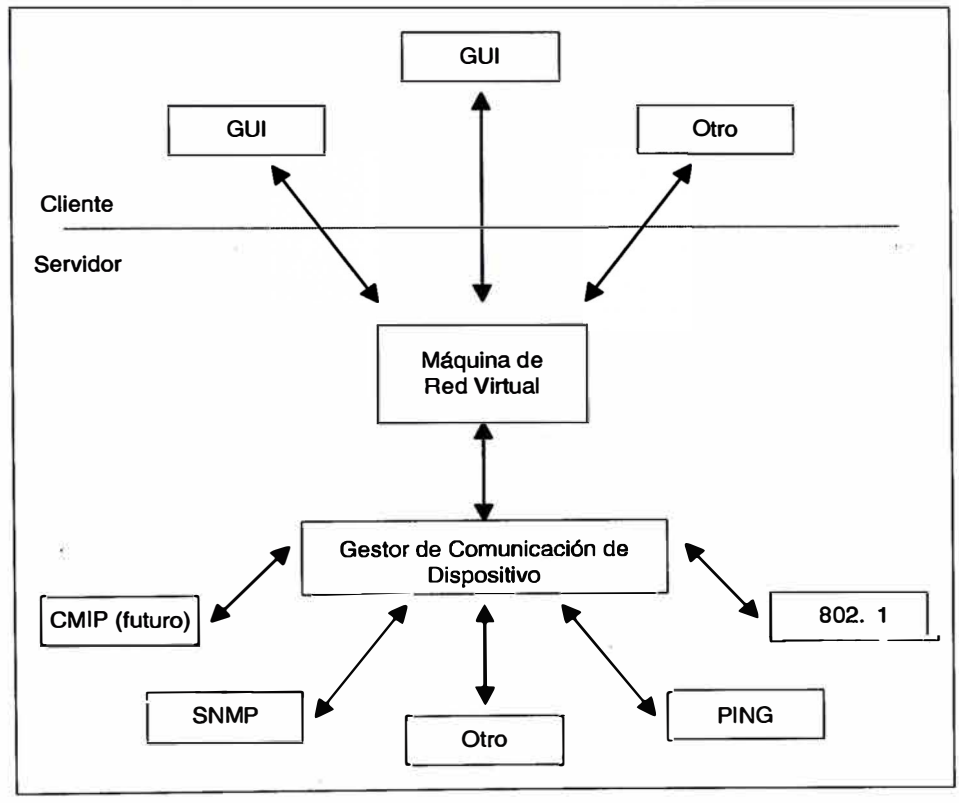

Fig. 2.15 Arquitectura de Cabletron Systems' SPECTRUM

En una implementación típica, el SpectroGRAPH y SpectroSERVER corren sobre diferentes hosts en la red. Los dos sistemas son típicamente conectados vía un socket BSD UNÍX. La arquitectura cliente/servidor del SPECTRUM ha permitido

alcanzar altos de niveles de escalabilidad, incluyendo ambientes con cientos y aún miles de SpectroSERVERs trabajando en paralelo.

El gestor de empresa SPECTRUM puede soportar ambos el UNIX y estaciones de trabajo NT con completa fluidez. Por ejemplo, un SpectroGRAPH basado en NT puede interactuar completamente con un SpectroSERVER basado en UNIX. Es aún posible para un SpectroGRAPH basado en UNIX interactuar con un SpectroSERVER basado en NT. SPECTRUM sobre NT tiene todas las características, funciones, y la mayoría de aplicaciones actualmente disponible en UNIX.

SPECTRUM usa dos base de datos. El gestor de base de datos distribuida DDM contiene un archivo de estadísticas y eventos de red. La base de datos de la tecnología de modelo inductivo IMT modela la relación red desde una variedad de perspectivas, tal como topología, jerarquía, e incluso organizaciones. Ambas bases de datos están residentes con el SpectroSERVER pero pueden proporcionar amplios reportes de empresa integrados, vista de alarmas, notificación de aplicación automatizado, y otras características del mundo empresarial.

Muchas de las aplicaciones avanzadas de SPECTRUM sacan provecho de su IMT para construir grandes niveles de automatización. Por ejemplo, SpectroRx Resolution Expert proporciona a los clientes con resolución de falla automatizada una tecnología de inteligencia artificial llamado argumento basado en el caso. Esta

tecnología ayuda a diagnosticar problemas de red y sistemas usando el mismo paradigma que los abogados usan cuando intentan probar un caso del pasado.

2.3.2 Hewlett-Packard OpenView

La familia Hewlett-Packard OpenView proporciona una solución de gestión de red y sistemas integrada para gestión de servicio end-to-end del ambiente de tecnología de información completa. Las soluciones consisten de un amplio portafolio de productos de gestión de HP y OpenView Solutions Partners, y un conjunto completo de servicios que ayudan al cliente a mejorar el servicio y reducir los costos de operación (ver Fig. 2.16). Las soluciones incluyen:

- Network Node Manager: tiene los requerimientos para una solución de gestión de red poderosa que proporciona una vista espontánea de la red para monitorear y controlar el ambiente de cómputo entero.
- IT/Operaciones: operaciones avanzadas y solución de problemas de gestión que permite al gestor de red mantener una distribuida, ambiente de cómputo de varios vendedores activa y corriendo.
- IT/Administración: una solución efectiva para inventario, software, y gestión de usuario que mejorará la seguridad, proporcionará un mejor control de dispositivos gestionados, y soportará estándares de fabricación para distribución de software.
- PerfView/MeasureWare and NetMetrix: soluciones de gestión de recursos y rendimiento que proporciona la base para gestión a nivel de servicio, incluye objetivos para medición de tiempo de respuesta, latencia de enlace WAN/LAN, y monitoreo continuo de disponibilidad de recursos de cómputo.

- OmniBack II and OmniStorage: para gestión de datos y almacenamiento, proporcionan respaldo de rendimiento de alta confiabilidad para proteger los datos de la empresa.

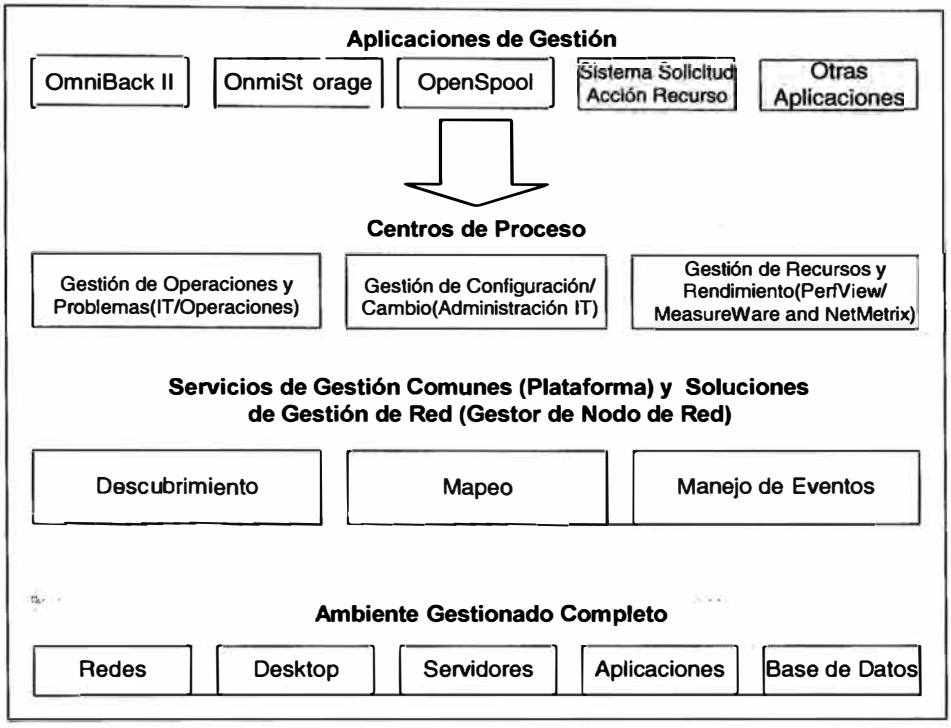

Fig. 2.16 Hewlett-Packard OpenView Solution Framework

2.3.3 Sun Microsystems' Solstice Enterprise Manager

La solución de gestión de red Sun Microsystems es llamada EM(Solstice Enterprise Manager), el cual es diseñado como una arquitectura altamente flexible y escalable. Solstice EM esta basado una arquitectura distribuida, orientada a objeto, cliente/servidor que permite escalar para manejar redes grandes, distribuidas, o de misión crítica. Esta especialmente enfocada en los requerimientos de los portadores de telecomunicaciones y proveedores de servicio de Internet (ISPs), e incluye soporte para el estándar TMN en suma al CMIP y SNMP. La arquitectura cliente/servidor proporciona verdadero soporte de varios

usuarios. La seguridad esta basada en usuarios y grupos definidos. Controles de acceso puede ser especificado en una plataforma (todas las aplicaciones), en aplicaciones seleccionadas, o en una base con característica de aplicación. Por ejemplo, el buscador SNMP puede permitir GETs pero no SETs. Servidores de gestión múltiple, llamado MIS (Management Information Servers), pueden ser destacado para escalabilidad. MIS pueden comunicarse uno con otro para presentar una vista consistente para el operador de red.

La Fig. 2.17 muestra los servicios claves proporcionado por el MIS del EM. Empezando en la capa mas baja, el MIS usa MPAs (Management Protocol Adapters) para acotar entre varios protocolos de gestión, tal como el SNMP, y varios servicios de gestión. El PMI (Portable Mangement Interface) proporciona un mecanismo para aplicaciones de gestión, incluyendo aplicaciones de terceros, para acceder los servicios del MIS.

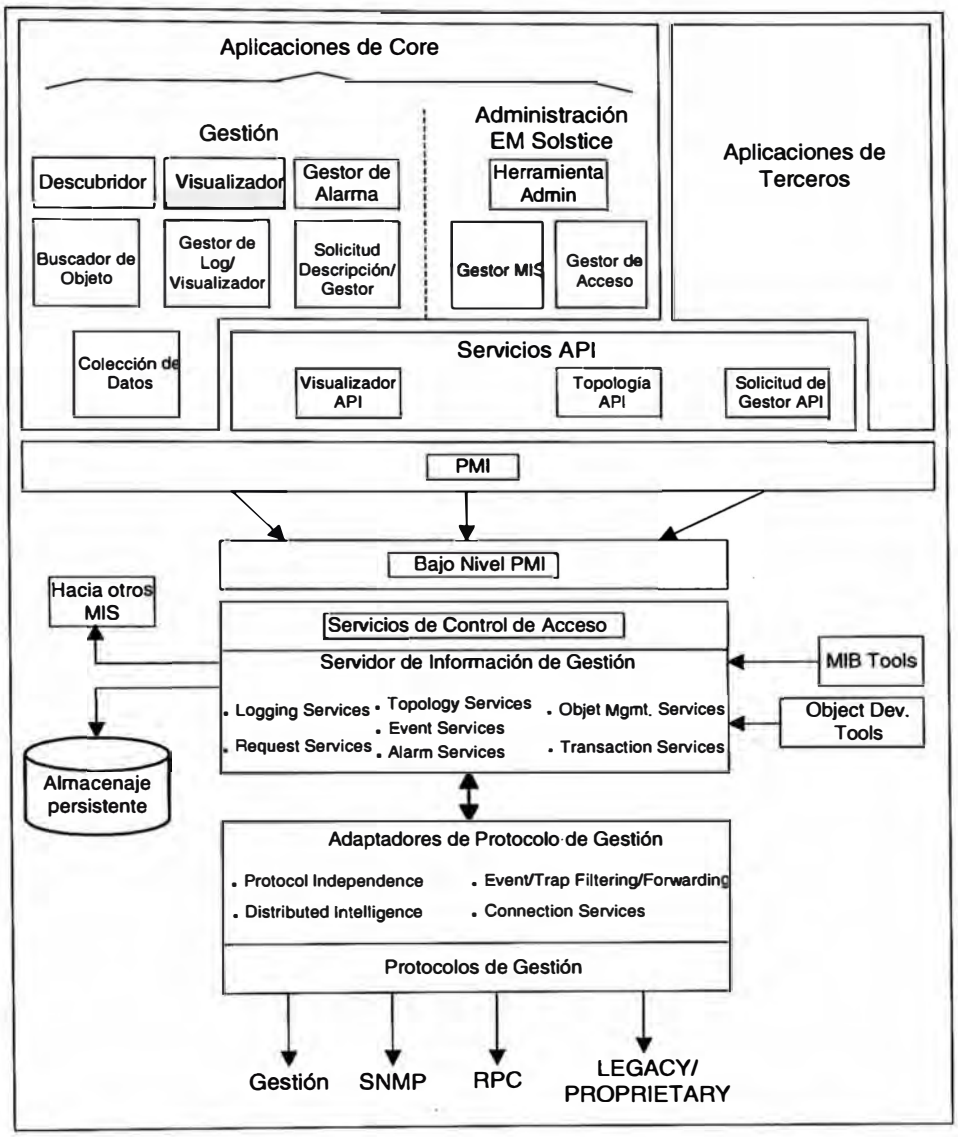

Fig. 2.17 Sun Microsystems' Solctice Enterprise Manager Core Applications and Services

2.3.4 Tivoli Systems' TME NetView

TME NetView destruyó la barrera tradicional entre gestión de red y gestión de sistemas al proporcionar fuerte integración con aplicaciones de gestión TME complementarios de Tivoli. Combinado con su habilidad para fácilmente efectuar cambios en muchos dispositivos, una infraestructura de soporte global, y el respaldo de cientos de terceros vendedores, TME NetView de Tivoli es una

plataforma de gestión implementado ampliamente (ver Fig. 2.18). Por otro lado, TME NetView no solamente te habilita a gestionar tu red; también te ubica para planear y crecimiento futuro con una solución de gestión de sistemas completo. TME NetView habilita usuarios para descubrir redes TCP/IP, mostrar topologías de red, correlacionar y manejar eventos y traps SNMP, monitorear la vitalidad de la red, y recolectar datos de rendimiento. TME NetView encuentra la necesidades de gestores de redes pequeñas y pueden crecer contigo para gestionar aún las redes mas grandes. Al usar el MLM (Mid-Level Manager) de TME NetView a través de tu empresa, puedes escalar TME NetView en una verdadera manera distribuida, proporcionando un medio efectivo para reducir tus costos totales de propiedad y mantener el tráfico de gestión de red cerca de la fuente.

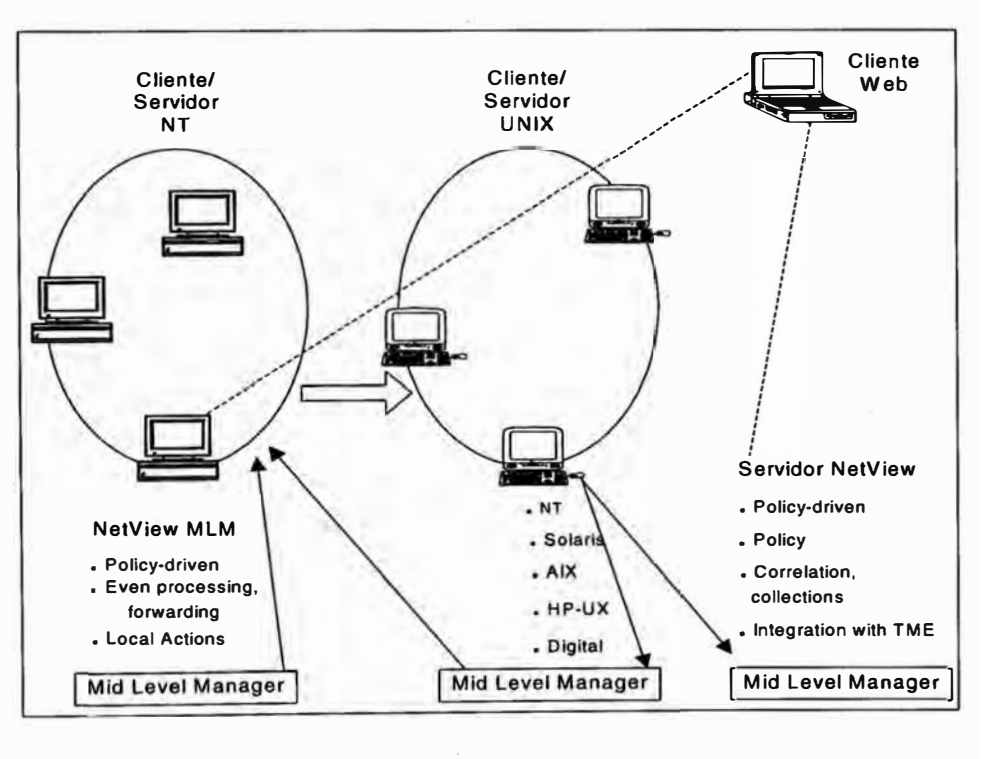

Fig. 2.18 Gestión Distribuida Tivoli NetView

TME NetView es rico en características poderosas que te proporcionan con relevante, información al minuto. Por ejemplo, la colección de objetos de TME NetView te habilita agrupar dinámicamente recursos por características comunes tal como tipo de recurso o ubicación. Usando colección de objetos, puedes monitorear grupos de dispositivos sin búsqueda manual de ellos. La colección de objetos te habilita agrupar dinámicamente objetos de red de acuerdo a cualquier esquema lógico. Puedes ver, por ejemplo, todos los routers caídos (información de excepción), todos los routers de un fabricante específico (todos los routers de marca x), o todos los routers de una subred específica. Distinto a algunas facilidades de colección, la colección de objetos del TME NetView son dinámicamente actualizados en tiempo real, eliminando el error humano e información no actualizada.

En una acción simple, puedes centralmente fijar e implementar política para multiplicar dispositivos de red usando el gestor de política de agente. Cambios en cientos o miles de dispositivos remotos ocurren en minutos en lugar de horas o días.

Una sofisticada máquina de correlación de eventos basada en reglas te permite construir gráficamente reglas que definen como quieres implementar políticas de negocios. Eventos pueden ser manejados localmente, centralizado, o a través de otras aplicaciones de Tivoli para correlación adicional. En esencia, la habilidad para implementar políticas de negocios en forma de reglas te habilita para diagnosticar rápidamente problemas de raíz mas que reportar solamente eventos

sintomáticos. Además, reporte de excepción declara problemas serios con específicos dispositivos de red cuando niveles definidos son violados.

2.4 MÉTODO DE SELECCIÓN Y PLANEACIÓN

2.4.1 Planificación de Procesos

En vez de tener que recordar y realizar trabajos periódicos o en horas no laborables, el administrador puede programar un agente que realiza las tareas programadas en los momentos previstos. Además, estos agentes recogen información sobre el estado de finalización de los procesos para un posterior análisis por el administrador.

Los procesos típicos que se suelen planificar son: copias de seguridad, búsqueda de virus, distribución de software , impresiones masivas, etc.

La planificación de procesos permite también aprovechar los períodos en que la red está más libre como las noches y los fines de semana.

Los planificadores como AT de Windows NT y CRON de Unix permiten procesos especificando un momento determinado y una frecuencia.

Normalmente también se suelen usar scripts para programar a los agentes planificadores.

2.5 DESARROLLO Y PLANES DE CONTINGENCIA

Garantizar la disponibilidad y calidad de los servicios en la red implica evitar cambios no autorizados o no planeados. Ya estos aspectos causan fallas del equipamiento de red y una perdida de tiempo no planeada para las organizaciones. Fallar al documentar configuraciones actuales lo hace difícil, sino imposible, para recuperar airosamente de un procedimiento de cambio fallado. Fallar al controlar la tasa de cambios así como quien hizo los cambios resulta en un ambiente inconsistente que es difícil de mantener a largo plazo. En lugar de pensar la gestión como un trabajo extra, me gustaría pensar de la gestión como salvar mi trabajo. Simplemente siguiendo algunas metodologías simples y procesos, podemos asegurar que los cambios a los dispositivos de red nunca llegarán a ser una pesadilla. O al menos, si llegaran a ser una pesadilla, podemos rápidamente recuperar sin tener que pasar toda la noche en la oficina.

Los mecanismos actuales de gestión de cambio dependen en cuales tipos de dispositivos y herramientas tienes en tu red; las formas en el cual debes conducir un programa de gestión de cambio, sin embargo, son universales. Uno de los principales pasos a seguir para un programa de gestión es el planeamiento. Muchas metodologías de gestión de cambio ignoran la fase de planeamiento, el cual es quizás el mas importante. Planear te permite identificar y reducir riesgo, proporciona un medio para recuperación en caso de desastre, y así sucesivamente. Esencialmente, planear requiere que:

- Identifiques cada cosa que podría posiblemente ir mal como resultado de una mala gestión.

- Asignes un nivel de probabilidad y severidad a cada riesgo potencial.
- Identifiques medios de aplacar riesgos o, al menos, proporcionar un medio de recuperación debe el riesgo llegar a ser una realidad.

Una metodología de planeamiento de gestión de cambio sólido lo haría mas fácil para ti para priorizar cambios de acuerdo al impacto de sus negocios. Por ejemplo, si tu mismo encuentras que haciendo diversos cambios de alto riesgo, bajo beneficio, puedes implementar políticas para reducir tal actividad, por ejemplo, adoptando una política de solamente hacer cambios de bajo beneficio durante un ciclo de actualización regular, tal como al fin de cada mes.

Como tu actualmente conduzcas cada paso del proceso de planeamiento depende de tu ambiente y tus preferencias personales. En las cuatro próximas secciones, se proporcionarán algunos ejemplos para empezar.

2.5.1 Identificar riesgos

Que podría ir mal cuando actualices una tabla de rutas en uno de tus routers? Muchas posibilidades saltan a la mente:

- Podrías errar al teclear algo y corromper toda la tabla de rutas, haciendo el router inútil funcionalmente.
- Podrías ingresar información incorrecta, previendo el cambio de trabajar propiamente.

- Podrías ingresar información incorrecta que hace las rutas existentes dejar de trabajar correctamente.
- Mientras actualices cambios al router, podrías perder tu conexión de red, resultando en un cambio parcial para el router.
- Podrías actualizar cambios al router equivocado, causando problemas de rutas a través de la red.
- Cualquier cambio incorrecto que tu hagas podría replicar a través de tu red dentro de los protocolos de rutas, corrompiendo todos tus dispositivos de red.

El objetivo con tu lista de riesgo es identificar cada cosa que podría posiblemente ir mal, no solo las cosas que son probables para ir mal. Ten en mente que cambiar la configuración de cualquier dispositivo de red, no solo un router, crea un conjunto de riesgos potenciales.

2.5.2 Categorizar riesgos

Después que hayas obtenido una lista de cada cosa que podría fallar, asignar probabilidad y severidad a cada ítem. Por ejemplo un escala simple de 1 a 3, donde 1 representa riesgos altamente improbables, o riesgos que serían muy menores si ocurrieron. Trabajando con la lista de riesgos potenciales creada previamente, podrías asignar los siguientes calificaciones:

- Podrías errar al teclear algo y corromper toda la tabla de rutas, haciendo el router inútil funcionalmente—probabilidad es 2, severidad. La probabilidad es alta porque tecleas manualmente toda la información de configuración del router y a

pesar de que siempre eres cuidadoso, no hay un proceso de validación de data en el lugar.

- Podrías ingresar información incorrecta, previendo el cambio de trabajar propiamente—probabilidad es 2, severidad es 1. Severidad es menos que lo del primer riesgo porque simplemente estas fallando al implementar el cambio, sin afectar algo adicional.

- Podrías ingresar información incorrecta que hace las rutas existentes dejar de trabajar correctamente—probabilidad es 2, severidad es 2. La severidad es 2 para el riesgo porque estas afectando un dispositivo entero.

- Mientras actualices cambios al router, podrías perder tu conexión de red, resultando en un cambio parcial para el router—probabilidad es 1 porque cuentas con fuente de alimentación backup en cualquier lugar y una red muy confiable; severidad es 2 porque si el riesgo ocurriera, arruinaría un router entero.

- Podrías actualizar cambios al router equivocado, causando problemas de rutas a través de la red—probabilidad es 1 porque eres cuidadoso; severidad es 2 porque si harías este disparate, arruinarías un router entero.

- Cualquier cambio incorrecto que tu hagas podría replicar a través de tu red dentro de los protocolos de rutas, corrompiendo todos tus dispositivos de red—probabilidad es 3 porque si haces un cambio incorrecto, se propagaría apenas rápidamente; severidad de 3 porque esta equivocación podría potencialmente llevar toda tu red fuera de línea.

El propósito de esta lista es ayudar identificar los riesgos que son en la mayoría necesarios de compensación específica. La lista de riesgo para una configuración

de switch podría incluir similares ítems, pero los riesgos listados serían únicos para los switches; lo mismo puede decirse de los firewalls, hubs gestionados, o cualquier otro dispositivo de red. Una manera simple de clasificar tus riesgos es adicionar a tus dos calificaciones, dando a ti una lista prioridad de cosas que no funcionarían:

- Cualquier cambio incorrecto que tu hagas podría replicar a través de tu red dentro de los protocolos de rutas, corrompiendo todos tus dispositivos de red—riesgo: 6.
- Podrías errar al teclear algo y corromper toda la tabla de rutas, haciendo el router inútil funcionalmente—riesgo: 5.
- Podrías ingresar información incorrecta que hace las rutas existentes dejar de trabajar correctamente—riesgo: 4.
- Podrías ingresar información incorrecta, previendo el cambio de trabajar propiamente—riesgo: 3.
- Mientras actualices cambios al router, podrías perder tu conexión de red, resultando en un cambio parcial para el router—riesgo: 3.
- Podrías actualizar cambios al router equivocado, causando problemas de rutas a través de la red—riesgo: 3.

2.5.3 Mitigar riesgos

Mitigación de riesgo es un proceso de planeamiento en el cual intentas pensar formas para prevenir tus riesgos identificados de cualquier ocurrencia; mientras al mismo tiempo obteniendo ideas de recuperación el riesgo debe llegar a ser una

realidad a pesar de tus esfuerzos. Adiciona la mitigación e ideas de recuperación a tu lista para crear una lista de comprobación de evasión de riesgo y recuperación.

- Cualquier cambio incorrecto que tu hagas podría replicar a través de tu red dentro de los protocolos de rutas, corrompiendo todos tus dispositivos de red.

Evasión—Deshabilitar protocolos de rutas en el router hasta que el cambio sea verificado por un administrador mayor.

Recuperación—Asegurar que un backup de todas las configuraciones del router estén disponibles antes de que hagas algún cambio. En el evento de que se propagasen datos incorrectos, recuperar inmediatamente configuraciones del dispositivo del backup.

- Podrías errar al teclear algo y corromper toda la tabla de rutas, haciendo el router inútil funcionalmente.

Evasión—Usar herramientas dotadas por el proveedor para hacer los cambios en ves de cambios enteramente manuales. Las herramientas del proveedor proporcionan alguna validación de datos para ayudar prevenir errores en el ingreso de datos. Además, documentar todos los cambios y tener otra revisión de administrador y aprobarlos para exactitud. El otro administrador tiene que verificar la precisión de los cambios después de ellos son hechos.

Recuperación—Realizar el backup de la configuración del dispositivo antes de hacer un cambio. Restaurar inmediatamente la configuración del dispositivo si los cambios hechos no cumplen con la documentación de cambio.

- Podrías ingresar información incorrecta que hace las rutas existentes dejar de trabajar correctamente o previendo el cambio de trabajar propiamente.

Evasión—Usar herramientas dotadas por el proveedor para hacer los cambios en ves de ingresar cambios directamente en el router. Herramientas de proveedor proporcionan alguna validación de data para ayudar prevenir errores de ingreso de data. Además, documentar todos los cambios en un papel hacer que otro administrador los revise y apruebe para precisión. El otro administrador tiene que verificar la precisión de los cambios después de ellos son hechos.

Recuperación—Realizar el backup de la configuración del dispositivo antes de hacer un cambio. Restaurar inmediatamente la configuración del dispositivo si los cambios hechos no cumplen con la documentación de cambio. Tener siempre una estación de trabajo disponible que puede hacer una conexión serial directa al router en caso un cambio incorrecto deshabilite la habilidad del router para comunicar vía la interfaz de red.

- Mientras actualices cambios al router, podrías perder tu conexión de red, resultando en un cambio parcial para el router.

Evasión—Asegurar que el router, estación administrativa, y dispositivos intermedios (hubs y switches) están en un backup mecánico. Si es posible, ubica una estación administrativa en el mismo segmento de red como el router a ser cambiado para eliminar la posibilidad de una falla de router intermedio durante la carga.

Recuperación—Realizar el backup de la configuración del dispositivo antes de hacer un cambio. Asegurar que el router a ser cambiado es accesible a una estación de segmento local en el cual reside el backup, permitiendo una recuperación mas fácil. Tener siempre una estación de trabajo disponible que puede hacer una conexión serial directa al router en caso un cambio incorrecto

deshabilite la habilidad del router para comunicar vía la interfaz de red. Como un método de recuperación de última opción, muchos dispositivos de red ofrecen un switch de restablecimiento de hardware que recupere la configuración de fábrica de dispositivo. Combinado con un backup de configuración reciente, puedes usar esta función de restablecimiento para poner rápidamente en pie al dispositivo y corriendo nuevamente.

- Podrías actualizar cambios al router equivocado, causando problemas de rutas a través de la red.

Evasión—Tener otro administrador para confirmar tus cambios y escenario previo a la carga.

Recuperación—Realizar el backup de la configuración del dispositivo antes de hacer un cambio. Si la data es cargada al dispositivo equivocado, recupera la configuración del dispositivo del backup. Tener siempre una estación de trabajo disponible que puede hacer una conexión serial directa al router en caso un cambio incorrecto deshabilite la habilidad del router para comunicar vía la interfaz de red.

Algunos dispositivos de red, tales como los hubs o switches gestionados, podrían ofrecer métodos de recuperación mas simples. Algunos hubs gestionados, por ejemplo, pueden crear un backup de la configuración buena última conocida a un módulo RAM de instante inherente, y permitirte recuperar esa configuración con un switch de restablecimiento de hardware. Otros dispositivos de red, tal como los firewalls, podrían requerir planeamiento mas extenso para asegurar que una recuperación rápida es posible.

En resumen, después que has desarrollado un lista completa, incluyendo mitigaciones, para un tipo particular de cambio en la gestión, grábalo. Esta lista puede llegar a ser una lista de comprobación para todos los cambios futuros del mismo tipo. Siguiendo la lista de comprobación cada vez que haces ese tipo de cambio, mitigarás automáticamente los riesgos potenciales así como haber preparado opciones de recuperación en caso ocurra lo peor. Si tu administración de red es logrado primordialmente por administradores jóvenes, estas listas de mitigación pueden llegar a ser una parte obligatorio de los procedimientos que siguen los administradores, ayudando asegurar que eres un tipo de vigilante, aún cuando no estés.

CAPÍTULO III

ACTIVIDADES Y ELEMENTOS DE LA GESTIÓN DE REDES

3.1 ACTIVIDADES DEFINIDAS POR EL MODELO OSI

3.1.1 Gestión de fallas

El estándar dice que la gestión de falla engloba la detección de falla, aislamiento y corrección de la operación anormal del ambiente OSI. El estándar también considera reporte de errores, identificación de fallas, y pruebas de diagnóstico.

En otras palabras, gestión de falla significa que tu necesitas primero identificar, luego reparar fallas de red. Hay dos maneras de gestionar fallas: re-activamente o pro-activamente. Un gestor reactivo espera por un problema y luego lo analiza. Un gestor pro-activo examina el gestor y agentes para determinar si ellos están excediendo niveles operacionales críticos, tal como utilización de red. Si ocurre excesos, el administrador pro-activo determina su fuente y los reduce en acuerdo.

3.1.2 Gestión de cuentas

El estándar dice que la gestión de cuentas "habilita cargas a ser establecidas por el uso de recursos en el ambiente de OSI, y por costo a ser identificado para el uso de esos recursos." Otras consideraciones incluyen informar a los usuarios de los costos y recursos consumidos, fijar límites de cuentas, e incorporar información de tarifas en todo el proceso de cuentas.

En el mundo real, cuenta significa tratar con gente real usando recursos de red reales con gastos de operación real. Ejemplos de estos costos incluyen uso de disco y archivo de datos, gastos de telecomunicaciones para acceso remoto de datos, y cargas por envío de mensajes de correo electrónico. Tu también puedes usar cuentas de gestión para determinar si la utilización de recursos de red esta incrementando debido a un crecimiento, el cual podría indicar la necesidad para adicionar o mantener en un futuro cercano.

3.1.3 Gestión de configuración

El estándar dice que la gestión de configuración "identifica, controla la práctica, colecciona datos, y proporciona datos a sistemas abiertos para el propósito de prepararlos, inicializar, empezar, proveer para una operación continua, y terminar servicios de interconexión." Estos servicios podrían incluir la colección de información dependiendo del sistema, alertas de acuerdo a los cambios en el sistema, y cambios de configuración del sistema.

En el mundo real, los movimientos, adiciones y cambios, tipifican el trabajo de gestión. Las redes son sistemas dinámicos, y los administradores de red necesitan desplazar personal y arreglar sus necesidades de procesamiento. Este aspecto de gestión de red puede ser tan simple como acomodar conectores modulares en un cableado, o tan complejo como instalar una LAN y sus servidores asociados, comunicación de circuitos, y así sucesivamente, en una ubicación remota. Por lo tanto, un aspecto significante de la función de gestión de red involucra seguir todos estos cambios usando algún tipo de base de datos.

3.1.4 Gestión de rendimiento

En el estándar, gestión de rendimiento "habilita el comportamiento de recursos en el ambiente OSI y la efectividad de actividades de comunicación a ser evaluados." Estas funciones incluyen recolección estadística e información histórica y evaluación de rendimiento del sistema bajo una variedad de condiciones reales y hipotéticas.

Prácticamente, gestión de rendimiento asegura que el administrador satisface las necesidades finales de los usuarios todo el tiempo. Para hacer esto, el administrador debe seleccionar el hardware y software de acuerdo a las necesidades de la interred, luego ejercitar estos sistemas a su máximo potencial. En algunos casos, políticas administrativas son desarrolladas los cuales delinean estos requerimientos de rendimiento en la red. Adicionalmente, rendimiento y gestión de fallas esta

cercanamente relacionados, desde que necesitas eliminar, o al menos minimizar, fallas para obtener óptimo rendimiento. Muchas herramientas están disponibles para medir rendimiento. Estos incluyen analizadores de protocolo, software de monitoreo de red, y varias utilidades que vienen con programas de consola de sistemas operativos de red.

3.1.5 Gestión de seguridad

Académicamente, "el propósito de gestión de seguridad es soportar la aplicación de políticas de seguridad por medio de funciones el cual incluye la creación, borrado, y control de servicios de seguridad y mecanismos; la distribución de información de seguridad relevante; y el reporte de eventos relacionados con seguridad."

En otras palabras, seguridad protege la red. Lo defiende contra virus, asegura la autenticación de usuarios locales y remotos, e instala sistemas de encriptación en cualquier circuito de comunicación que conecta a un lugar remoto.

3.2 SIMULACIÓN Y MONITOREO DE TODOS LOS EQUIPOS DE LA RED

Abatidamente, no muchas redes son construidas sobre la solución de un proveedor. Puedes simplemente implementar la solución de cada proveedor, y tratar con diferentes técnicas cada una usa para lograr tales como realizar backup de la configuración de un

dispositivo. Una mejor alternativa, sin embargo, es implementar una solución que puede simplificar la gestión de configuración de red al manejar todos tus dispositivos de red, indiferente de su fabricante. Una de esas soluciones esta disponible en AlterPoint http://www.alterpoint.com. El producto de AlterPoint puede automáticamente guardar las configuraciones de un dispositivo, alertarte de cambios, mostrarte exactamente cuales cambios fueron hechos, y aún recuperar configuraciones de dispositivos si un desastre ocurre. Aún otra solución es ReadyRouter http://readyrouter.com, un producto designado para salvar automáticamente configuraciones de dispositivo, recuperarlos cuando sea necesario, y rastrear cambios hechos a ellos.

Si eres bastante afortunado que todos tus dispositivos de red vengan de algún fabricante, el fabricante probablemente proporciona algún tipo de software para ayudar automatizar los backups de los dispositivos, el cual es una parte clave de gestión de cambio. Cisco Systems http://www.ciscosystems.com, por ejemplo, ofrece una gran pieza de software llamado el Cisco Works Resource Manager Essentials (RME), el cual proporciona una interfaz basada en web para gestión de inventario, auditoria de cambio, configuración de dispositivo, y mucho mas. RME trabaja con la mayoría de dispositivos Cisco, desde routers a switches. RME puede inventariar y monitorear tus dispositivos Cisco, y reportar cualquier cambio que les ocurre a su configuración, y mucho mas.

Si no quieres invertir en una solución comercial, puedes probablemente empedrar juntos alguna cosa propio de ti. Por ejemplo, la mayoría de dispositivos de red soportan el

TFTP (Trivial File Transfer Protocol) para recuperar sus archivos de configuración; puedes fácilmente escribir una plantilla de línea de comandos que interroga cada uno de tus dispositivos por sus archivos de configuración y los graba en un servidor de archivos. Puedes aún organizar el script (usando cron en el sistema UNÍS y un Task Scheduler en sistemas Windows) para correr en una base regular, asegurando que tu obtienes un backup semanalmente o aún cada noche de tus configuraciones de dispositivo.

Desafortunadamente, muchos dispositivos no soportan TFTP. Para esos que no lo hacen, tendrás que entrar en el dispositivo y manualmente obtener su configuración, tal vez tomando nota de los resultados de cada pregunta o grabando ellos en un archivo texto para referencia futura. Un beneficio del producto de AlterPoint y soluciones similares es que ellos pueden automáticamente realizar la tediosa tarea de colectar los datos de configuración de dispositivos que no soportan TFTP o algún otro método de transferencia de volumen.

3.3 MANTENIMIENTO

Desde el punto de vista de darle solución a un dispositivo, por ejemplo un router gestionado cuando no esta operando es preguntarse que cambió. Muy pocos dispositivos de red se alteran solos; encontrarás que usualmente requiere implicación humana para realmente errar las cosas. Asumiendo que has eliminado algún tipo de falla de hardware como la causa del problema, el culpable es mayormente probable un cambio reciente

hecho a la configuración del dispositivo. Por supuesto, si el hardware es la falla, simplemente necesitas remplazar el hardware y recuperar la configuración del backup.

Recuperando desde un backup que tu haces es un buen primer paso aún si el hardware es fino. Idealmente, la configuración backup resolverá el problema, y puedes usar una herramienta para comparar la antigua y nueva configuración para determinar las diferencias. Esto no es exactamente solucionar el problema, pero al menos estas trabajando en un laboratorio, tu meta debe ser recuperar el dispositivo a operación primero, y resolver que causó el problema luego.

Si realmente no tienes un backup reciente, es irresponsabilidad. Optimistamente tu tienes documentación de gestión de cambio que describe los cambios que han sido hechos al router en una memoria reciente. Comienza examinando esos cambios para ver cuales podrían aplicar al problema tu estas teniendo. Si es necesario, deshacer manualmente cada cambio, uno a la vez, hasta que el problema se vaya.

Otros cambios podrían involucrar un aumento del sistema operativo al dispositivo o parche. En tales casos, nunca debes hacer un cambio sin conocer como puedes regresar a la versión de sistema operativo anterior a la cual estuvo trabajando. Si es necesario, cuenta con un router de respaldo a la mano en caso que el cambio de sistema operativo o los parches liquiden tu unidad en producción. La meta, en cual evento, es no preocuparse

demasiado sobre como darle solución al problema actual, y simplemente retroceder a la última configuración que trabajaba.

Ten en cuenta que no todos los cambios necesitan involucrar los archivos de configuración de un router o el sistema operativo. Por ejemplo, quizás tu compañía recientemente contrató alguien para alinear el armario de cables eléctricos, y esa persona accidentalmente atascó el router en la subred incorrecta cuando el o ella repuso el armario junto. El cambio en el armario eléctrico debió haber sido documentado como un cambio en la red, y te daría una información que tu necesitas chequear las interfaces del router para ver que ello están atascados. Concluyendo que no hay cambio que sea simple o menor que no deba ir a través del proceso de gestión de cambio.

Por supuesto, si no tienes un programa de gestión de cambio en su lugar o, al menos, un backup de la configuración del router, estas fuera de las opciones simples. Necesitarás comenzar dándole solución al problema de una manera dura, el cual podría eventualmente involucrar completamente recargar la configuración de fábrica del router y reconstruir tu configuración de chiripa. Tales medidas drásticas dan relevancia la importancia de ambos backups y una metodología de gestión de cambio sólida.

3.4 CENTRO DE OPERACIÓN DE RED

El NOC (Network Operation Center) o Centro de Operación de Red, es el encargado de mantener funcionando de manera eficiente la interconexión de las redes locales, los enlaces de área amplia y el backbone de toda una red. Se dedica a proporcionar apoyo a los administradores de redes a solucionar sus problemas de intercomunicación, respondiendo así la problemática que se presenta en la red y clientes. Es importante señalar también que el NOC se encarga de estudiar el desempeño de la red y participar en las tareas de configuración, mantenimiento e implementación de las nuevas tecnologías en el backbone, manteniendo así un buen servicio y buena infraestructura. El NOC tiene varias líneas telefónicas para recepción y atención por personal facultada para brindar solución de manera inmediata. El NOC interactúa con las áreas adyacentes para conseguir una solución satisfactoria transparente para el cliente.

Para mantener un buen nivel de servicio en una red se requiere un esquema de operación jerárquico, en el cual la Subdirección de Redes y Comunicaciones se ubica en el nivel más alto. Debajo de esta se encuentra el Departamento de Operación de Red, cuya tarea principal es la de administrar y operar la parte medular, o backbone, de la red, y a su vez mantener operando la interconexión de todas las redes locales y enlaces dedicados WAN de sus clientes, los cuales conforman organismos o empresas que se enlazan a través de la red.

Un NOC cuenta con sistemas automatizados que constantemente verifican el estado de los dispositivos más importantes de la red (como los que forman el backbone), y recolectan información que posteriormente será procesada para su análisis minucioso. Dichos sistemas trabajan 24 horas del día, los 365 días del año, con lo cual se logra ofrecer un servicio de calidad que se traduce en una alta disponibilidad de los recursos de información, los cuales pueden incluso ser ofrecidos a los clientes por medio de su servidor de web. El funcionamiento de un sistema automatizado permite enviar las alarmas más importantes hacia la vista del personal del NOC. Con esto se logra minimizar de manera considerable el tiempo de atención de fallas en sus equipos.

Las responsabilidades y actividades más importantes que desarrolla el Centro de Operación de Red son: monitoreo, tarifación, generación de estadísticas, administración de equipos de rutas, seguimiento de reportes (detección, diagnóstico, determinación, y resolución de la falla), documentación.

3.5 DISPONIBILIDAD DE RED

No existen reglas estrictas y rápidas, pero un servidor de doble procesador se utiliza frecuentemente para Internet e intranets, y también para correo electrónico (conocidos también como servidores de mensajería). Los servidores de doble procesador se utilizan también para aplicaciones empresariales en un departamento (finanzas, recursos humanos, etc.), Mientras que los servidores de cuatro procesadores se utilizan para ejecutar aplicaciones para toda una empresa. Entre las aplicaciones para servidores de

cuatro procesadores se cuenta con productos de sap, oracle y peoplesoft. Los servidores de cuatro procesadores suelen ser también la plataforma para servidores de trabajo en grupo. Lotus notes* fue uno de los ejemplos iniciales de este entorno. Estos servidores se encargan del manejo de información semiestructurada, como texto, imágenes, correo, pizarras electrónicas y flujo de trabajo.

Sin embargo, uno de los campos de más rápido crecimiento para los servidores snmp es el de las aplicaciones centradas en bases de datos. Las aplicaciones cliente/servidor centradas en bases de datos se clasifican en dos categorías: decision support systems (dss, sistemas de soporte a decisiones) y online transaction processing (oltp, procesamiento de transacciones en línea).
Los sistemas de soporte a decisiones se ejecutan en servidores de bases de datos y se utilizan para analizar datos y crear informes.

Estos sistemas proporcionan a los profesionales de las empresas y buscadores de información los medios para obtener la información que necesitan. Los usuarios deben poder crear consultas elaboradas, responder a preguntas "circunstanciales (what-if)", buscar correlaciones en los datos, graficar los datos y trasladarlos a otras aplicaciones como hojas de cálculo y documentos de procesadores de textos.

Los sistemas oltp se ejecutan en servidores de transacciones y se utilizan para crear aplicaciones en todos los tipos de empresas. Entre estas aplicaciones se encuentran

sistemas de reservaciones, sistemas de punto de venta, sistemas de seguimiento, control de inventario, estaciones de trabajo de corredores de bolsa y sistemas de control de plantas de manufactura. Por lo general son aplicaciones de misión crítica que requieren un tiempo de respuesta de 1 a 3 segundos el 100% de las veces.

3.6 SEGURIDAD Y CONTROL DE CAMBIOS DE LA RED

Nosotros gestionamos dispositivos usando el protocolo SNMP, la pregunta es si habrá algún riesgo en la parte de seguridad. El protocolo SNMP puede ser usado para leer o escribir información sobre los dispositivos de red. Aparentemente no hay algún riesgo de seguridad en la lectura, pero si lo hay. Los hackers pueden usar la información recabada del SNMP para aprender mas sobre la infraestructura de tu red, construyendo efectivamente un diseño completo de tu red. Cada cinta que incluye irrumpir el banco de memoria nos enseña que un diseño es la mejor manera de planear tu ataque, así que denegando a los hackers tu diseño de red es una primera defensa maravillosa. Por supuesto, la habilidad del SNMP para cambiar los escenarios de configuración de los dispositivos de red pueden, por supuesto, ser letales. Aquí hay algunos consejos para mantener SNMP de llegar a ser un peligro:

- Deshabilitar SNMP completamente, si pudieras. Otros, mas seguros, protocolos de gestión están disponibles (la mayoría de ellos propietarios, tal como el protocolo Insight de Hewlett-Packard). Al fin de todo, configura tus dispositivos para SNMP de sólo lectura, y realiza cambios de configuración a través de otros medios, si es posible.

- Si no estas usando el SNMP, definitivamente necesitas deshabilitarlo de tus dispositivos. Podrías pensar que tu firewall previene intrusos Internet de usar SNMP para atacar tus dispositivos, pero no olvides acerca de los intrusos internos o precisamente aparentes usuarios traviesos.

- Cambia con frecuencia tu cadena de comunidad de SNMP. Una vez a la semana no es tan frecuente. Por supuesto, cambiar las cadenas en todos tus dispositivos sería un tormento, así que ve si tus proveedores de dispositivos de red ofrecen cualquier herramienta para automatizar el proceso. Nuevamente, no asumas que tus dispositivos están seguros de ataques sólo porque ellos están detrás de un firewall. Nunca dejes tu comunidad SNMP como "public", el cual es frecuentemente común y por tanto conocido por cualquier hacker.

- La especificación SNMP requiere cadenas de comunidad para ser sensibles a la diferencia entre letras mayúsculas y minúsculas, usa una combinación de estos así como números. Adicionalmente, no uses cadenas de comunidad agradables; usa completamente aleatorios, justo como te gustaría para un password especialmente seguro. Por ejemplo, e3N7$ft8eH9H sería una gran cadena de comunidad.

- Configura dispositivos frontera, tales como firewalls, para bloquear tráfico SNMP de ingreso o salida a tu red.

- Idealmente, construye una red separada para transportar tráfico SNMP, y físicamente separarlo de tu red de producción. Esta técnica lo hará mas duro para los hackers obtener tráfico SNMP de tus dispositivos. Y nunca olvides que los hackers pueden venir de adentro; simplemente bloqueando el SNMP en tu firewall no es suficiente para proteger

tus dispositivos. Una red separada también te ayudará proteger contra ataques DoS (Denial of Service) de SNMP, lo cual es cuando un hacker dispara paquetes SNMP inválidos a dispositivos en un intento de retrasarlos y prevenirlos de responder solicitudes legítimas. Una red separada es definitivamente una propuesta cara; sin embargo, proporciona lo último en seguridad para tus dispositivos de red. Organizaciones que tienen especialmente requerimientos de seguridad rigurosos, tal como bancos y entidades gubernamentales, podrían buscar una inversión valedero.

- Dispositivos de alta capacidad pueden ser configurados para aceptar instrucciones SNMP solamente de una dirección IP específica o rango de dirección. Averiguar si tus dispositivos soportan esta capacidad, y si ellos cumplen, usarlo. Establecer tus estaciones administrativas y consolas de gestión con dirección IP fijo (ya sea una dirección IP estática o reservaciones DHCP) e instruye tus dispositivos para ignorar instrucciones SNMP que vienen de cualquier otra dirección IP.
- Permanecer al día con las actualizaciones del sistema operativo de tu dispositivo. La mayoría de los fabricantes de dispositivos de red publican parches regulares y boletines de seguridad para ayudar hacer sus dispositivos tan seguros como sea posible. Muchos fabricantes proporcionan listas de correo electrónico al cual te puedes inscribir y usar estas listas para que te notifiquen de los últimos arreglos.
- Poner en bitácora el tráfico SNMP. Algunos dispositivos proporcionan una opción para automáticamente poner en bitácora las solicitudes de SNMP recibidas. Si ellos no lo hacen, puedes usar dispositivos husmeadores de red para monitorear tráfico SNMP y

capturar cualquiera que ve pasar en tu red. Aún si tu solamente corres ocasionalmente el software de monitoreo, ayudará detectar cualquier tráfico SNMP no autorizado en tu red.

SNMP puede ser útil, si tu eres conciente de los riesgos y tomas los pasos necesarios para hacer SNMP más seguro.

3.7 SOPORTE REMOTO A LAS INSTALACIONES

El servicio de soporte a las instalaciones de forma remota consiste en acceder a los equipos que son parte de la topología de un proyecto establecido para brindar un servicio, y por ende realizar las configuraciones necesarias para la puesta en servicio o reconfiguraciones, cualesquiera que sea el trabajo y no implique desplazamiento de personal de campo. Desde que todos los equipos de red son administrados debidamente, se pueden gestionar recursos de red y clientes; esto es realizar cambios de software, ejecución de comandos para ampliaciones y reducciones de ancho de banda, agregar servicios, filtrar paquetes y protocolos, verificar el monitoreo de los equipos de los clientes y red.

El personal que realiza el soporte debe contar con herramientas de gestión tal como los gestores provistos por los fabricantes de los equipos que conforman la red, tener las listas de chequeo para cada caso que se presente al realizar una instalación o cambio. Debe garantizar el transporte y para esto requiere hacer las pruebas pertinentes sobre

todo el circuito. Asimismo, cuenta con el sistema de base de datos donde actualiza y registra los cambios, por ejemplo a través de un inventario de red y clientes.

El aspecto de coordinación es muy importante cuando se trata de una red que involucra varios operadores, donde se requiere realizar configuraciones en muchos tramos, por ejemplo a nivel internacional. Entonces el soporte remoto se maneja a nivel lógico, en cambio la parte física requiere de un instalador en sitio.

CAPÍTULO IV

PROTOCOLOS DE ADMINISTRACIÓN DE RED

4.1 PROTOCOLO SIMPLE DE GESTIÓN DE RED

Desde que fue desarrollado en 1988, SNMP (Simple Network Management Protocol) ha llegado a ser el estándar de facto para gestión de redes. Debido a la relativa facilidad para implementar y adicionar funciones de gestión, los diversos proveedores pueden fácilmente construir agentes SNMP en sus productos.

Un sistema de administración de red contiene dos elementos primarios: un gestor y los agentes. El gestor o administrador es la consola a través del cual el administrador de red (humano) realiza funciones de gestión de red. Los agentes son las entidades que interactúan con los dispositivos actuales que están siendo administrados. Bridges, routers, switches, o servidores de red son ejemplos de estos dispositivos que contienen objetos administrados. Estos objetos podrían ser hardware, parámetros de configuración, estadísticas de rendimiento, y otros, que se relacionan directamente a la actual operación del dispositivo en cuestión. Estos objetos son arreglados en lo que es denominado como una base de datos de información virtual, llamado una base de información de

administración (MIB). SNMP permite a los gestores y agentes comunicarse con el propósito de acceder estos objetos.

Existen tres elementos en la estructura de gestión de Redes en Internet, estructura de gestión de información (SMI), las bases de información de administración (MIBs), y el protocolo (SNMP).

Con el crecimiento de tamaño y complejidad de las interredes basadas en TCP/IP la necesidad de la administración de redes comienza a ser muy importante. El espacio de trabajo de la administración de redes actual para las interredes basadas en TCP/IP consiste en:

- SMI (RFC 1155) - describe cómo se definen los objetos administrados contenidos en el MIB.
- MIB-II (RFC 1213) - describe los objetos administrados contenidos en el MIB.
- SNMP (RFC 1098) - define el protocolo usado para administrar estos objetos.

El IAB emitió un RFC detallando su recomendación, que adoptó dos enfoques diferentes:

- A corto plazo debería usarse SNMP. IAB recomienda que todas las implementaciones IP y TCP sean redes que puedan administrarse. En el momento actual, esto implica la implementación de MIB-II Internet (RFC 1213), y al menos el protocolo de administración recomendado SNMP (RFC 1157).

- A largo plazo, se podría investigar el uso del protocolo de administración de redes OSI emergente (CMIP). Esto se conoce como CMIP sobre TCP/IP (CMOT).

SNMP y CMOT usan los mismos conceptos básicos en la descripción y definición de la administración de la información llamado Estructura e Identificación de Gestión de Información (SMI) descrito en el RFC 1155 y Base de Información de Gestión (MIB) descritos en el RFC 1156.

Por lo general, SNMP se utiliza como una aplicación cliente/servidor asincrónica, lo que significa que tanto el dispositivo administrado como el software servidor SNMP pueden generar un mensaje para el otro y esperar una respuesta, en caso de que haya que esperar una.

Ambos lo empaquetan y manejan el software para red (como el IP) como lo haría cualquier otro paquete. SNMP utiliza UDP como un protocolo de transporte de mensajes. El puerto 161 de UDP se utiliza para todos los mensajes, excepto para las trampas, que llegan el puerto 162 de UDP. Los agentes reciben sus mensajes del administrador a través del puerto UDP 161 del agente.

SNMP v2 añade algunas nuevas posibilidades a la versión anterior de SNMP, de las cuales, la más útil para los servidores es la operación get-bulk. Ésta permite que se envíen un gran número de entradas MIB en un solo mensaje, en vez de requerir

múltiples consultas get-next para SNMP v1. Además, SNMP v2 tiene mucho mejor seguridad que SNMP vl, evitando que los intrusos observen el estado o la condición de los dispositivos administrados. Tanto la encriptación como la autentificación están soportadas por SNMP v2. SNMP v2 es un protocolo más complejo y no se usa tan ampliamente como SNMP vl.

El SNMP reúne todas las operaciones en el paradigma obtener-almacenar (fetch store paradigm) . Conceptualmente, el SNMP contiene sólo dos comandos que permiten a un administrador buscar y obtener un valor desde un elemento de datos o almacenar un valor en un elemento de datos. Todas las otras operaciones se definen como consecuencia de estas dos operaciones.

La mayor ventaja de usar el paradigma obtener-almacenar es la estabilidad, simplicidad flexibilidad. El SNMP es especialmente estable ya que sus definiciones se mantienen fijas aun cuando nuevos elementos de datos se añadan al MIB y se definan nuevas operaciones como efectos del almacenamiento de esos elementos.

Desde el punto de vista de los administradores, por supuesto, el SNMP se mantiene oculto por usuario de una interfaz para que el software de administración de red puede expresar operaciones como comandos imperativos (por ejemplo, arrancar). Así pues, hay una pequeña diferencia visible entre la forma en que un administrador utiliza SNMP y otros protocolos de administración de red.

A pesar de su extenso uso, SNMP tiene algunas desventajas. La más importante es que se apoya en UDP. Puesto que UDP no tiene conexiones, no existe contabilidad inherente al enviar los mensajes entre el servidor y el agente. Otro problema es que SNMP proporciona un solo protocolo para mensajes, por lo que no pueden realizarse los mensajes de filtrado. Esto incrementa la carga del software receptor. Finalmente, SNMP casi siempre utiliza el sondeo en cierto grado, lo que ocupa una considerable cantidad de ancho de banda.

Un paquete de software servidor SNMP puede comunicarse con los agentes SNMP y transferir o solicitar diferentes tipos de información. Generalmente, el servidor solicita las estadísticas del agente, incluyendo el número de paquetes que se manejan, el estado del dispositivo, las condiciones especiales que están asociadas con el tipo de dispositivo (como las indicaciones de que se terminó el papel o la pérdida de la conexión en un módem) y la carga del procesador.

El servidor también puede enviar instrucciones al agente para modificar las entradas de su base de datos MIB(la Base de Información sobre la Administración). El servidor también puede enviar los límites o las condiciones bajo las cuales el agente SNMP debe generar un mensaje de interrupción para el servidor, como cuando la carga del CPU alcanza el 90 por ciento.

Las comunicaciones entre el servidor y el agente se llevan a cabo de una forma un tanto sencilla, aunque tienden a utilizar una notación abstracta para el contenido de sus mensajes. Por ejemplo, el servidor puede enviar un mensaje what is your current load y recibir un mensaje del 75%. El agente nunca envía datos hacia el servidor a menos que se genere una interrupción o se haga una solicitud de sondeo. Esto significa que pueden existir algunos problemas constantes sin que el servidor SNMP sepa de ellos, simplemente porque no se realizó un sondeo ni se generó interrupción.

4.1.1 Arquitectura y Objetivos del SNMP

El RFC 1157 declara que "SNMP explícitamente minimiza el número y complejidad de funciones de gestión realizado por el mismo agente de gestión". En otras palabras, el SNMP es diseñado para ser simple. Esto lo hace de tres maneras. Reduciendo el costo de desarrollo del software del agente, SNMP ha disminuido la carga a proveedores quienes desean soportar el protocolo, consecuentemente incrementando la aceptación del protocolo. Segundo, SNMP es extensible, permitiendo a los proveedores adicionar funciones de gestión de red. Tercero, separa la arquitectura de gestión de la arquitectura de dispositivos hardware, tales como hosts y routers, extendiéndose la base de soporte de varios proveedores.

SNMP tiene una arquitectura muy directa. La Fig. 4.1 compara la arquitectura SNMP al modelo ISO/OSI y el modelo ARPA, en torno de los cuales los protocolos de Internet y

TCP/IP fueron desarrollados. Notar que las cuatro capas del modelo ARPA no trazan equitativamente a las siete capas del modelo OSI.

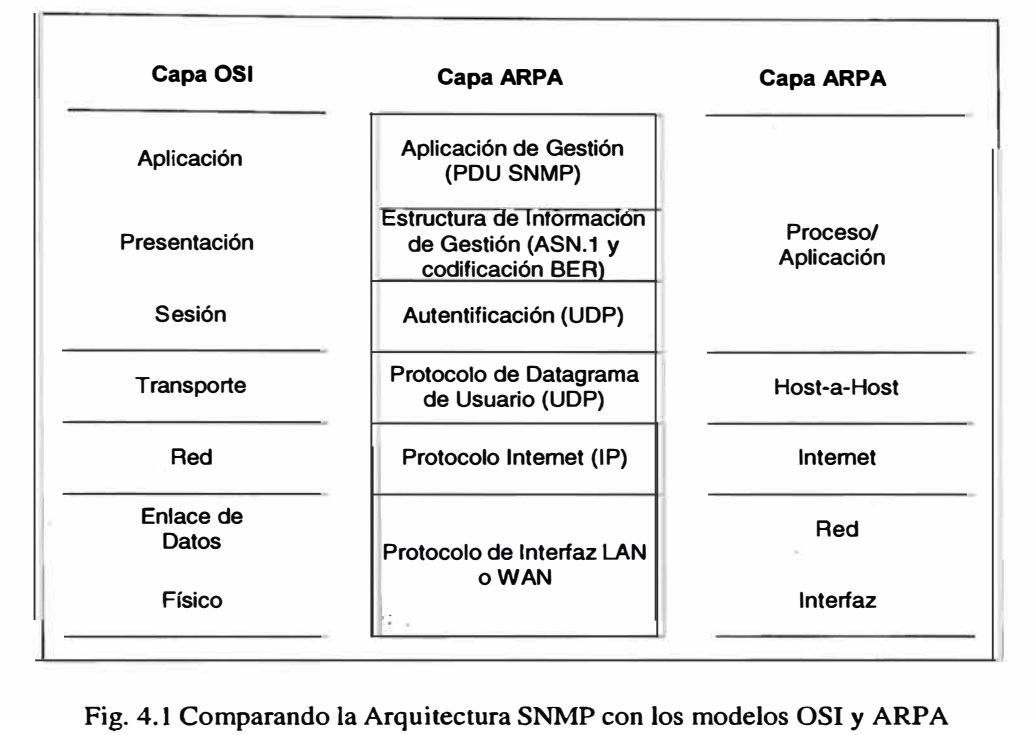

Fig. 4.1 Comparando la Arquitectura SNMP con los modelos OSI y ARPA

Usemos un ejemplo para ver como los procesos dentro de la arquitectura SNMP interactúan. Supón una consola de gestión requiere información sobre uno de los nodos gestionados. Los procesos del SNMP en ambos el gestor y el agente responden a la consola. La codificación ASN.1 en la capa de Aplicación proporciona la sintaxis propia para el mensaje SNMP. El resto de funciones autentifica la data (adosar la cabecera SNMP) y comunica la información de solicitud.

Debido a que la mayoría de información de gestión no demandan la entrega confiable que proporcionan los sistemas orientados a la conexión, el canal de comunicación entre el gestor SNMP y el agente es sin establecimiento de la conexión. Cuando comparas el

modelo SNMP con el modelo ISO/OSI, el mecanismo de comunicación sin conexión del SNMP desplaza algo de la necesidad para una capa de Sesión y reduce las responsabilidades de las cuatro capas mas inferiores. Para la mayoría de las implementaciones, el UDP realiza las funciones de capa de Transporte, el IP proporciona las funciones de capa de Red, y LANs tales como Ethernet o token ring o WANs tales como una línea arrendada o una conexión frame relay proporcionan las funciones de capa Física y Enlace de Datos. (Hay algunas excepciones a esta regla. RFCs 1418, 1419, y 1420 describen implementaciones que usan otros mecanismos de transporte, tales como OSI Apple Computer's AppleTalk, o protocolos Novell Inc.'s IPX. Sin embargo, RFC 1270, llamado "Servicios de comunicación de SNMP", declara que UDP/IP son los protocolos de elección para mayoría de circunstancias.

Si comparas SNMP con el modelo arquitectural Internet (o ARPA), ver Fig. 4.2, notarás que el modelo ARPA usa cuatro capas para describir la función de comunicación completo. En el modelo ARPA, SNMP residiría en la capa Proceso/Aplicación. Sin embargo, mientras la capa Host-to-Host de ARPA proporciona la confiabilidad de comunicación punto a punto, el uso de SNMP de UDP asegura solamente el correcto puerto de direccionamiento y una suma de chequeo; no proporciona un control de error octeto por octeto. IP proporciona las funciones de capa de Internet, tales como direccionamiento y fragmentación, que son necesarios para entregar un mensaje SNMP de la fuente al destino. Finalmente, la capa de interfaz de red trata con el hardware LAN o WAN, tal como una interfaz a una conexión de red FDI o Frame Relay. Notar que la

Fig. 4.2 también muestra las complejidades relativas de las funciones de host y router. Los hosts implementan todas las cuatro capas del modelo ARPA, mientras que los routers implementan solamente las dos inferiores. Comparando la arquitectura SNMP con los modelos arquitecturales de ISO/OSI y ARPA proporciona una base teórica para esta discusión. Pero de una perspectiva práctica, el modelo SNMP trabaja como se muestra en la Fig. 12. Este modelo contiene diversos elementos discutidos en el Capítulo 2. Incluye un sistema de gestión que usa el gestor SNMP, un agente SNMP, y recursos gestionados, y los mensajes SNMP comunican la información de gestión vía cinco unidades de data de protocolo SNMP (PDUs). La aplicación de gestión emite los PDUs Get, GetNext, o Set. El sistema gestionado retorna un PDU GetResponse. El agente puede iniciar un PDU Trap (algunas veces llamado un Evento) cuando condiciones predefinidas son encontradas. La sección 4.1.3 discute estas cinco PDUs en detalle.

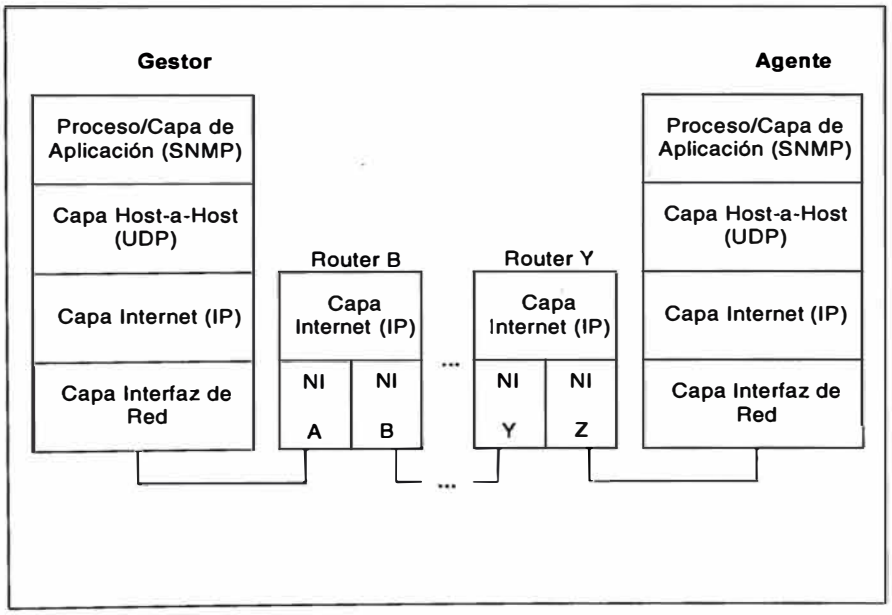

Fig. 4.2 Conexión Aplicación a Aplicación

4.1.2 Operación del SNMP

Los procesos descritos en la sección previa debe ocurrir en dispositivos físicos. Por ejemplo, un router debe tener un procesador físico que implementa el software activo como un agente SNMP. Dos conjuntos de procesos lógicos ocurren dentro de estos elementos físicos: las relaciones que son especificados entre varias entidades de gestión de red, y la forma como la información de gestión de red es comunicado.

- Relaciones de Gestión de Red

El estándar SNMP, RFC 1157, y el "Modelo Administrativo SNMP," RFC 1351, define un número de términos. Muchas de estas definiciones describen las relaciones entre las entidades de gestión:

- Estaciones de gestión de red son dispositivos que ejecutan las aplicaciones de gestión que controlan y monitorean los elementos de red.
- Elementos de red son dispositivos tales como hosts, switches, routers, y hubs que contienen un agente y realizan funciones de gestión de red que solicitan las estaciones de gestión de red.
- El SNMP permite comunicar las estaciones de gestión de red y los agentes en los elementos de red.
- Las entidades de aplicación SNMP residen ya sea en una estación de gestión o un nodo gestionado, y usan SNMP como un mecanismo de comunicación.
- La comunidad SNMP parea un agente SNMP con un conjunto arbitrario de entidades de aplicación SNMP. El administrador de red asigna la comunidad un nombre (llamado

el nombre de comunidad), que es esencialmente un password con derechos y privilegios asociados. Una aplicación de gestión con nombres de comunidades múltiples puede pertenecer a múltiples comunidades.

- Mensajes SNMP autorizados son mensajes SNMP enviados desde una entidad de aplicación a una comunidad SNMP específica. El mensaje contiene el nombre de la comunidad de interés.

- El esquema de autentificación es el método por el cual un mensaje SNMP es identificado como perteneciente a una comunidad SNMP específica.

- El MIB View es el subconjunto de objetos MIB, los cuales pueden estar contenidos dentro de diversos subárboles que pertenecen a un elemento de red.

- El modo de acceso SNMP determina el nivel de acceso para objetos que una entidad de aplicación particular es permitida. Las opciones son solamente lectura y lectura-escritura.

- El perfil de comunidad parea el modo de acceso SNMP con el MIB View de SNMP. El perfil de comunidad representa privilegios de acceso específicos para las variables en un MIB View.

- La política de acceso SNMP parea una comunidad SNMP con un perfil de comunidad SNMP. La política de acceso representa el perfil de comunidad específica que un agente permite tener a los otros miembros de la comunidad.

- El agente proxy SNMP proporciona funciones de gestión en beneficio de elementos de red que de otra manera sería inaccesible.

La Fig. 4.3 ilustra algunas de las definiciones descritas arriba.

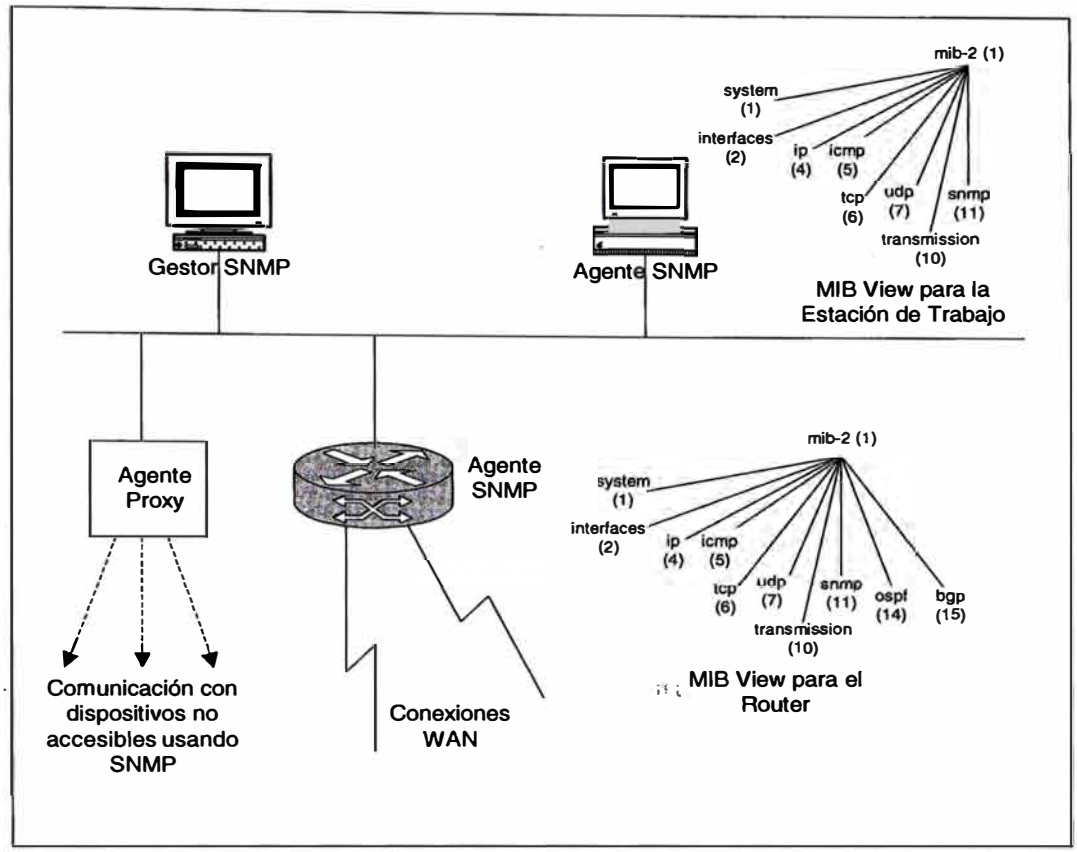

Fig. 4.3 Relaciones de Gestión de Red

- Identificación y Comunicación de Instancias de Objetos

Los tipos de objetos SMI gestionados tienen un identificador de objeto (OID) que únicamente los nombra y ubica sus lugares en un árbol de objeto. Una *instancia* de un tipo de objeto es una ocurrencia de este tipo de objeto y tiene un valor asignado. Por ejemplo, el objeto sysDescr {1.3.6.1.2.1.1.1.0} podría tener un valor de "Retix Remote Bridge Model 2265M".

Supón una estación de gestión de red desea recuperar una instancia de un objeto específico. La estación de gestión debe usar SNMP para comunicar su pregunta al agente.

Ahora, supón múltiples instancias (u ocurrencias) de este objeto son posibles. Por ejemplo, decir una tabla de rutas de un router contiene un número de entradas. Como la estación de gestión de red recuperaría justo el valor de la tercera entrada en la tabla?.

RFC 1157, páginas 12-15, especifica estas tareas. Para estas operaciones SNMP, un *nombre variable* únicamente identifica cada instancia de un tipo de objeto. Este nombre consiste de dos partes de la forma x.y. La porción *x* es el tipo de objeto definido en el MIB, y la porción *y* es un fragmento OID que identifica la instancia deseada. Los siguientes deben clarificar esto.

Considerar un objeto escalar que tiene una instancia. Los objetos contenidos en el grupo System son todos objetos escalares. Por ejemplo, el objeto sysServices tiene un OID de {1.3.6.1.2.1.1.7} y ocurre una vez. La porción *x* del nombre variable es el OID y la porción *y* ha sido asignado a 0. Puedes derivar esto al seguir el árbol OID bajo el objeto sysServices y adicionar el sufijo de instancia apropiado (con el sufijo, o porción *y*):

iso	org	dod	internet	mgmt	mib-2	system	sysServices	Instance
1	3	6	1	2	1	1	7	0

Así, el nombre de variable para sysServices es {1.3.6.1.2.1.1.7.0}.

El nombre variable para un objeto de forma de columna es mas complicado porque debe identificar la posición de un objeto dentro de una estructura de data de dos dimensiones, tal como una tabla que tiene ambas filas y columnas. (Dentro del RMON MIB, las estructuras de datos de tres dimensiones son añadidas, haciendo la identificación aún mas compleja.) Usando la hoja de cálculo familiar como un ejemplo, la identificación de una celda particular requiere dos coordinadas, X e Y, el cual describe las posiciones horizontal y vertical, respectivamente. Con objetos en forma de columna, un esquema de indexado, especificado en la cláusula INDEX en la definición ASN.1 para ese objeto, proporciona un medio para identificar la instancia específica. La cláusula INDEX entonces además identifica la sintaxis a ser usada. Y como uno podría esperar, algunos de los esquemas de indexado son mas complicados que otros. RFC 1212, páginas 8-10, lista muchas de las cláusulas INDEX que son encontrados dentro del MIB-2. Miremos algunos ejemplos para claridad adicional.

Considerar el objeto IP Address Table, ipAdEntBcastAddr, el cual especifica el valor del bit menos significante (LSB) de la dirección IP broadcast (ver Fig. 4.4 y Fig. 4.5). Para comenzar, sigue el árbol OID para ipAdEntBcastAddr:

iso	org	dod	internet	mgmt	mib-2	ip	ipAddrTable	ipAddrEntry	ipAdEntBcastAddr
1	3	6		2	1	4	20	1	4

El OID es {1.3.6.1.2.1.4.20.1.4}, consiste del Grupo IP {1.3.6.1.2.1.4}, el IP Address Table (20), el ipAddrEntry (1),y el objeto ipAdEntBcastAddr (4), mostrado en la Fig. 4.4.

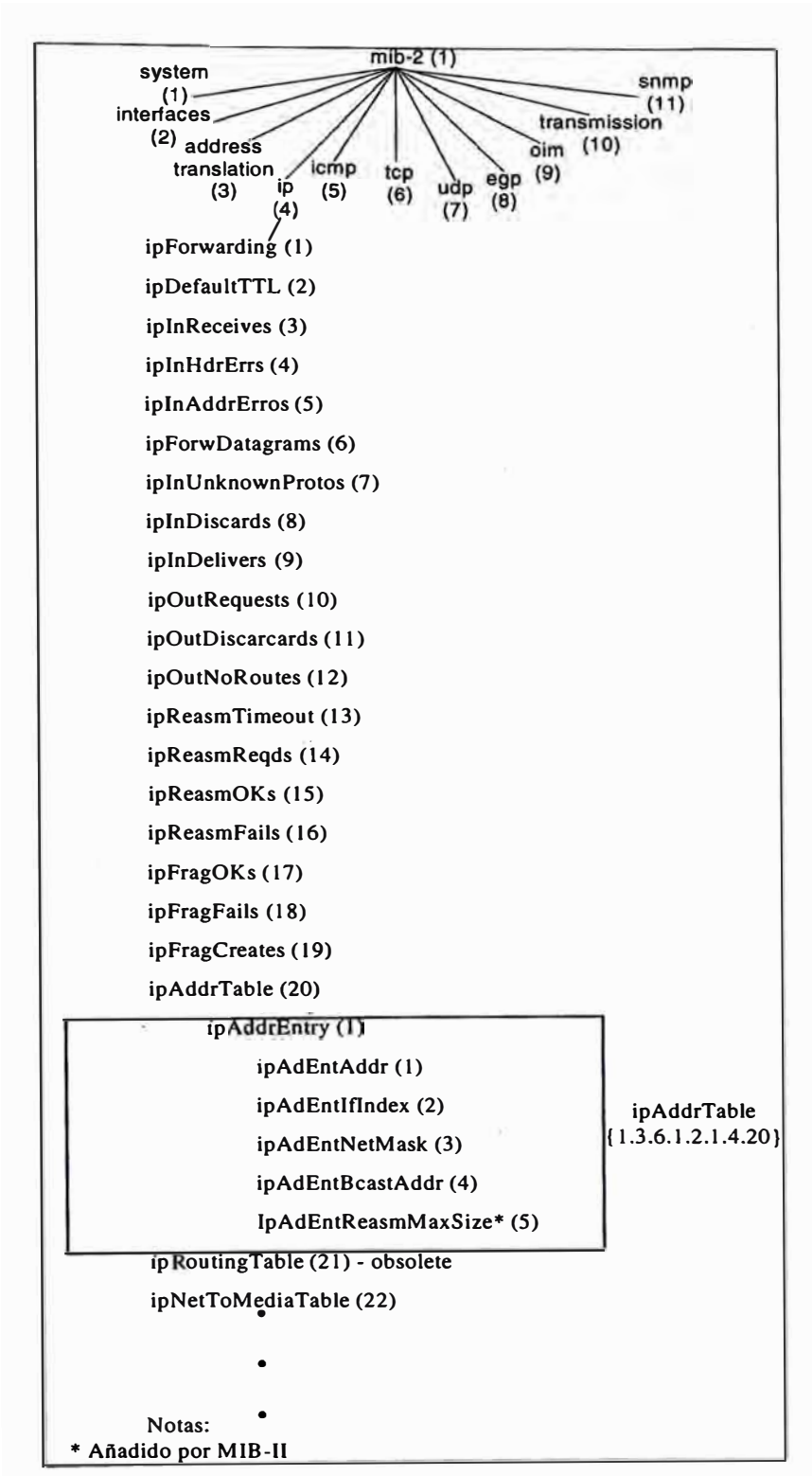

Fig. 4.4 La Tabla de Dirección IP dentro del Árbol OID

Consultando MIB-2, RFC 1157 página 31, la definición ASN.1 para el objeto ipAddrEntry incluye una cláusula INDEX que especifica el objeto ipAdEntAddr. Unas líneas abajo en el RFC 1157, vemos que el objeto ipAdEntAddr tiene un SYNTAX de IpAddress. Así, preveríamos el índice para este objeto a ser definido por una dirección IP y mostrado en notación decimal punteado: a.b.c.d. Retornando a nuestro ejemplo, para completar el nombre de variable, el sufijo (o porción *y*) es añadido, el cual consiste de una dirección IP: a.b.c.d. El nombre de variable para ipAdEntBcastAddr asociado con dirección IP a.b.c.d sería por lo tanto {1.3.6.1.2.1.4.20.1.4.a.b.c.d}. La Fig. 4.5 es una tabla de direcciones IP completada, construida al recuperar todas las variables del IP Address Table. Las cabeceras de las columnas muestran los cinco objetos, ipAdEntAddr hasta ipAdEntReasmMaxSiza. Cada fila contiene los valores de las cicos variables: ipAdEntAddr [XXX.YYY.150.2], ipAdEntIfIndex (1), y así sucesivamente. Un índice diferente (2) identifica la segunda fila y contiene valores diferentes. Entradas de filas adicionales son creadas, como necesarias, hasta que la tabla es completada.

IpAddrTable {1.3.6.1.2.1.4.20}

	ipAdEntAddr {1.3.6.1.2.1.4.20.1.1}	ipAdEntIfIndex {1.3.6.1.2.1.4.20.1.2}	ipAdEntNetMask {1.3.6.1.2.1.4.20.1.3}	ipAdEntBcastAddr {1.3.6.1.2.1.4.20.1.4}	ipAdEntReasmMaxSiz {1.3.6.1.2.1.4.20.1.5}
Fila 1	XXX.YYY.150.2	1	255.255.255.0	0	12000
Fila 2	XXX.YYY.1.1	2	255.255.0.0	1	12000
Fila n		. . .			

Fig. 4.5 Instancia de Objeto en las Tablas de Direcciones IP

Un ejemplo final (derivado del RFC 1157, sección 3.2.6.3) es de TCP Connection Table, tcpConnTable. Supón que deseas recuperar el estado de la conexión entre el puerto 575 de una dirección local {a.b.c.d} y el puerto 441 de dirección remota {w.x.y.z}. El OID para tcpConnState es {1.3.6.1.2.1.6.13.1.1}. La cláusula INDEX consiste de cuatro partes: tcpConnLocalAddress, tcpConnLocalPort, tcpConnRemAddress, y tcpconnRemPort. El sufijo *y* por lo tanto sería expresado como {a.b.c.d.575.w.x.y.z.441}. Por lo tanto, el nombre de la variable completa sería:

{1.3.6.1.2.1.6.13.1.1.a.b.c.d.575.w.x.y.z.441}

Los siguientes ejemplos muestran los nombres de las variables especificas para ambos tipos de objetos escalares o de forma de columnas:

- La descripción de servicios de este sistema:

SysServices ::=

{1.3.6.1.2.1.1.7.0}

- La velocidad de interfaz 3:

IfSpeed.3 ::=

{1.3.6.1.2.1.2.2.1.5.3}

- La dirección física asociada con interfaz 2 y dirección IP {a.b.c.d} (Notar que el primer componente es un *.1* el cual indica una dirección IP [ver RFC 1157, página 13]):

AtPhysAddress.2.1.a.b.c.d ::=

{1.3.6.1.2.1.3.1.1.2.2.1.a.b.c.d}

- El máximo tamaño de reagrupación del datagrama IP asociado con una dirección IP {a.b.c.d}:

ipAdEntReasmMaxSize.a.b.c.d ::=

{1.3.6.1.2.1.4.20.1.5.a.b.c.d}

- El número de mensajes ICMP Echo (solicitud) recibidos en este dispositivo:

icmpInEchos ::=

{1.3.6.1.2.1.5.8.0}

- El estado de una conexión TCP entre el puerto local e, dirección local {a.b.c.d} y puerto remoto j, dirección remota {f.g.h.i}:

tcpConnState.a.b.c.d.e.f.g.h.i.j ::=

{1.3.6.1.2.1.6.13.1.1.a.b.c.d.e.f.g.h.i.j}

- Verificación de que un escuchador UDP es operacional en el puerto e de la dirección IP local a.b.c.d:

udpLocalAddress.a.b.c.d.e ::=

{1.3.6.1.2.1.7.5.1.1.a.b.c.d.e}

- El estado del vecino por la dirección IP a.b.c.d:

egpNeighState.a.b.c.d ::=

{1.3.6.1.2.1.8.5.1.1.a.b.c.d}

- El número de mensajes SNMP entregados a este dispositivo con nombres de comunidad desconocidos (un escalar):

SnmpInBadCommNames ::=

{1.3.6.1.2.1.11.4.0}

RFC 1157, páginas 12-15, y RFC 1212, páginas 8-10, proporciona otros ejemplos que son válidos para un estudio adicional.

4.1.3 Unidades de data del protocolo SNMP (PDUs)

Comenzaremos la discusión de PDUs describiendo la posición del mensaje SNMP dentro de un frame transmitido. El *frame* es una unidad de información transmitida entre nodos de red. Por ejemplo, un formato de frame de IEEE 802.5 define la transmisión entre nodos token ring, y un formato ANSI T1.617 define la transmisión entre nodos Frame Relay.

La cabecera de red local y colas definidas por el protocolo LAN o WAN delimitan el frame (ver Fig. 4.6). Los data transmitida es llamada un *datagrama* del Protocolo Internet (IP). El datagrama IP es una unidad de información enviada desde el host fuente a su destino deseado vía la interred. Dentro del datagrama esta una dirección IP destino que guía el datagrama hacia el receptor deseado. Luego, la cabecera del UDP identifica el proceso del protocolo de capa mas alta (SNMP) que procesará el datagrama, y proporciona control de error usando una suma de chequeo. El mensaje SNMP es la parte intima del frame, lleva la data actual entre el gestor y el agente.

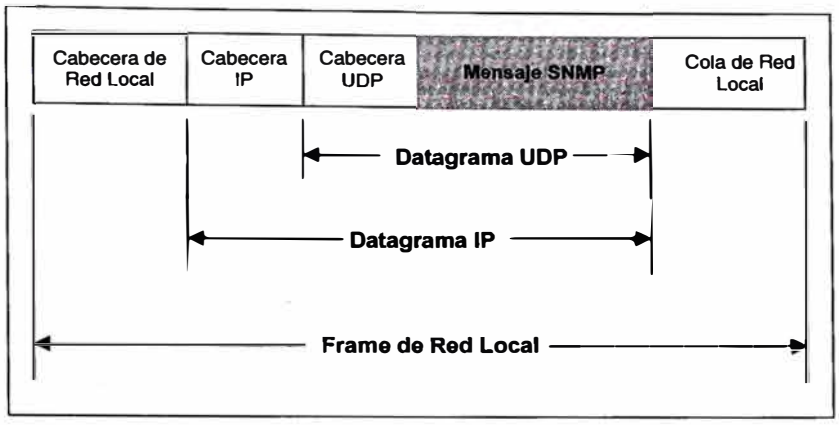

Fig. 4.6 Mensaje SNMP dentro de un Frame de Transmisión

Cuando el IP es demasiado grande para caber dentro de un frame, podría ser dividido (o fragmentado) en diversos frames para transmitir en la LAN. Por ejemplo, una datagrama conteniendo 2500 octetos requiere dos frames Ethernet, cada una de ellos puede contener un máximo de 1500 octetos de datos de la capa mas alta. La estructura general de cada frame, como el mostrado en la Fig. 4.6, restaría lo mismo.

El mensaje SNMP en si mismo es dividido en dos secciones: un identificador de versión mas nombre de comunidad, y un PDU. El identificador de versión y nombre de comunidad son algunas referidos como la *cabecera de autentificación del SNMP*. Hay cinco tipos de PDU diferentes: GetRequest, GetNextRequest, GetResponse, SetRequest, y Trap. Los PDUs Get, Set, y Response tienen un formato común (ver Fig. 4.7), mientras el PDU Trap es único.

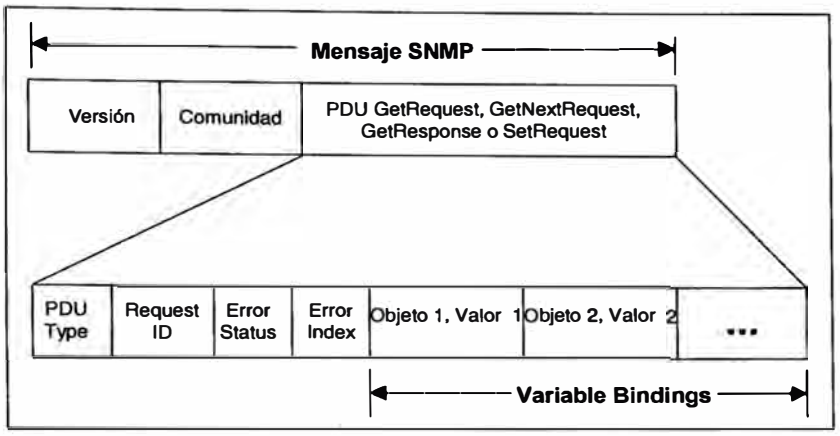

Fig. 4.7 Las Estructuras de los PDU SNMP GetRequest, GetNextRequest, GetResponse, y SetRequest

El número de versión (un tipo INTEGER) asegura que ambos el gestor y agente están usando la misma versión del protocolo SNMP. Los mensajes entre gestor y agente contienen diferentes números de versión son descartados sin procesamiento adicional. El nombre de la comunidad (un tipo OCTET STRING) autentifica el gestor antes de permitir el acceso al agente. El nombre de comunidad, junto con la dirección IP del gestor, es almacenado en el perfil de comunidad del agente. Si hay alguna diferencia entre los valores del gestor y el agente para el nombre de comunidad, el agente enviará un mensaje trap de falla de autentificación hacia el gestor. Si ambos el número de versión y el nombre de comunidad del gestor coinciden con los almacenados en el agente, el PDU SNMP empieza a procesar.

En las siguientes secciones veremos los campos de los dos formatos PDU y la operación de los cinco PDUs.

- Formatos PDU Get, Set y Response

El primer campo (ver Fig. 4.7), PDU Type, especifica el tipo de PDU el mensaje contiene.

PDU	**Valor del campo Tipo de PDU**
GetRequest	0
GetNextRequest	1
GetResponse	2
SetRequest	3
Trap	4

El campo Request ID es un tipo INTEGER que correlaciona la solicitud del gestor a la respuesta del agente. El campo Error Status es un tipo INTEGER enumerado que indica operación normal (noError) o un de las cinco condiciones de error. Los valores posibles son:

Error	**Valor**	**Significado**
noError	0	Operación adecuada gestor/agente.
tooBig	1	El tamaño del PDU GetResponse requerido excede un limitación local.
noSuchName	2	El nombre del objeto solicitado no coincidió con los nombres disponibles en el relevante MIB View.
badValue	3	Un SetRequest contuvo un tipo, longitud, y valor inconsistente para la variable.

readOnly	4	No definido en RFC 1157.
GenErr	5	Otros errors, no definidos explícitamente, han ocurrido.

Cuando ocurre un error, el campo Error Index identifica la entrada de la lista Variable Bindings que causó el error. Por ejemplo, si la cuarta Variable Binding fue mal formateada, o de alguna manera no entendible por el receptor, un Error Index = 4 sería retornado. Una Variable Binding (VarBind) parea un nombre de variable con su valor. Un VarBindList es una lista de tales pares. Notar que dentro de los campos del Variable Bindings de los PDUs SNMP (ver Fig. 4.7 a Fig. 4.12), la palabra identifica el nombre de variable (OID codifica el tipo de objeto mas la instancia) por el cual un valor esta siendo comunicado. También notar que los PDUs GetRequest o GetNextRequest usan un valor de NULL, el cual es un tipo de data especial de ASN.1.

- Usando el PDU GetRequest

El gestor usa el PDU GetRequest para recuperar el valor de uno o mas objetos desde el agente. En la mayoría de casos, estos son escalares, no de forma columnas, objetos. Para generar el PDU GetRequest, el gestor asigna PDU Type = 0, especifica un Request ID definido localmente, y fija ambos el Error Status y Error Index a 0. Un VarBindList, conteniendo las variables solicitadas y valores NULL correspondientes, completa el PDU. Bajo condiciones de libre error, el agente genera un PDU GetResponse, el cual es asignado PDU Type = 2, el mismo valor de Request ID, Error Status = noError, y Error

Index = 0. La Variable Bindings ahora contiene los valores asociados con cada valor anotado en el PDU GetRequest (ver Fig. 4.8). Recordar que el término variable se refiere a una instancia de un objeto gestionado.

Cuatro condiciones de error son posibles:

- Si una variable en el campo de Variable Bindings no coincide exactamente un objeto disponible, el agente retorna un PDU GetResponse con Error Status = noSuchName, y con el Error Index indicando el índice de la variable en cuestión.
- Si una variable es un tipo agregado, tal como un objeto fila, el agente retorna un PDU GetResponse con Error Status = noSuchName, y con el Error Index indicando el índice de la variable en cuestión.
- Si el tamaño del PDU GetResponse apropiado excediera una limitación local, entonces el agente retorna un PDU GetResponse de forma idéntica, con Error Status = tooBig, y Error Index = 0.

Si el valor de una variable solicitada no puede ser recuperada por cualquier otra razón, entonces el agente retorna un PDU GetResponse con Error Status = genErr, y el Error Index indicando el índice de la variable en cuestión.

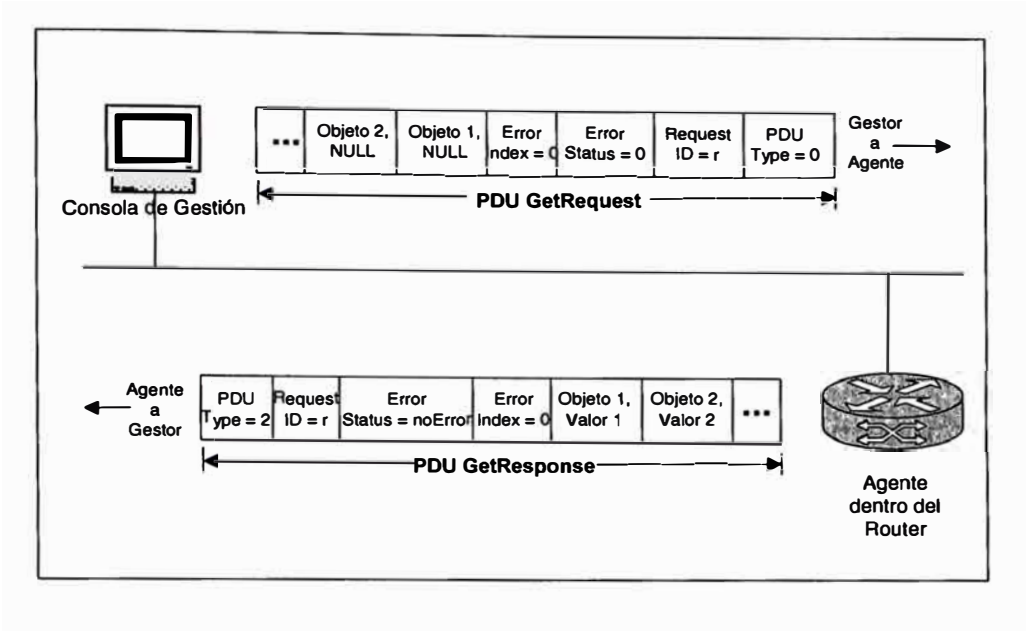

Fig. 4.8 Transmisión de PDU GetRequest/GetResponse (sin errores)

- Usando el PDU GetNextRequest

El gestor usa el PDU GetNextRequest para recuperar uno o mas objetos y sus valores desde un agente. En la mayoría de los casos, estos múltiples objetos residirán dentro de una tabla. Como puedes ver en la Fig. 4.9, para generar el PDU GetNextRequest el gestor asigna PDU Type = 1, especifica un Request ID definido localmente, y fija ambos el Error Stuts y el Error Index a 0. Un VarBind List, conteniendo los OIDs y correspondientes valores NULL, completan el PDU. Estos OIDs pueden ser cualquier OID (el cual puede ser una variable) que inmediatamente precede la variable y valor retornado. Bajo condiciones de libre error, el agente genera un PDU GetResponse, el cual es asignado PDU Type = 2, el mismo valor de Request ID, Error Status = noError, y Error Index = 0. La Variable Bindings contiene el nombre y valor asociado con el sucesor lexicográfico de cada uno de los OIDs anotados en el PDU GetNextRequest.

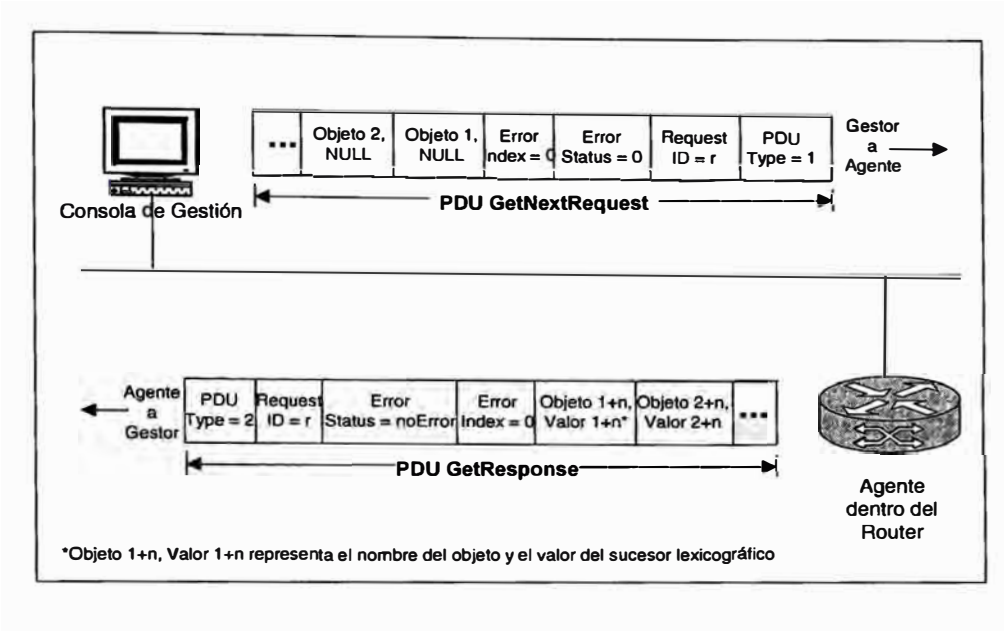

Fig. 4.9 Transmisión de PDU GetNextRequest/GetResponse (sin errores)

La diferencia clave entre los PDUs GetRequest y GetNextRequest es la palabra *lexicográfica*. Esto significa que el GetNextRequest recupera el valor del objeto próximo dentro del MIB View del agente.

Tres condiciones de error son posibles:

- Si una variable en el campo Variable Bindings no precede en forma lexicográfica el nombre de un objeto que puede ser recuperado (esto es, un objeto disponible para operaciones Get y dentro de el relevante MIB View), el agente retorna un PDU GetResponse con Error Status = noSuchName, y con el Error Index indicando el índice de la variable en cuestión. Esta condición es llamado "desterrando el fin del MIB View.".

- Si el tamaño del PDU GetResponse apropiado excede una limitación local, el agente retorna un PDU GetResponse de forma idéntica, con Error Status = tooBig y Error Index = 0.

- Si el valor del sucesor lexográfico a una variable solicitada en el campo de Variable Bindings no puede ser recuperado por alguna otra razón, el agente retorna un PDU GetResponse, con Error Status = genErr, y el Error Index indicando el índice de la variable en cuestión.

- Usando el PDU SetRequest

El gestor usa el PDU SetRequest para asignar un valor a un objeto residiendo en el agente. Como puedes ver en la Fig. 4.10, para generar ese PDU el gestor asigna PDU Type = 3, especifica un Request ID definido localmente, y fija ambos el Error Status y Error Index a 0. Un VarBindList, conteniendo las variables especificadas y sus correspondientes valores, completa el PDU. Cuando el agente recibe el PDU SetRequest, altera los valores de los objetos mencionados a los valores en la Variable Binding. Bajo condiciones de libre error, el agente genera un PDU GetResponse de forma idéntica, excepto que el asignado PDU Type = 2, Error Status = noError, y Error Index = 0.

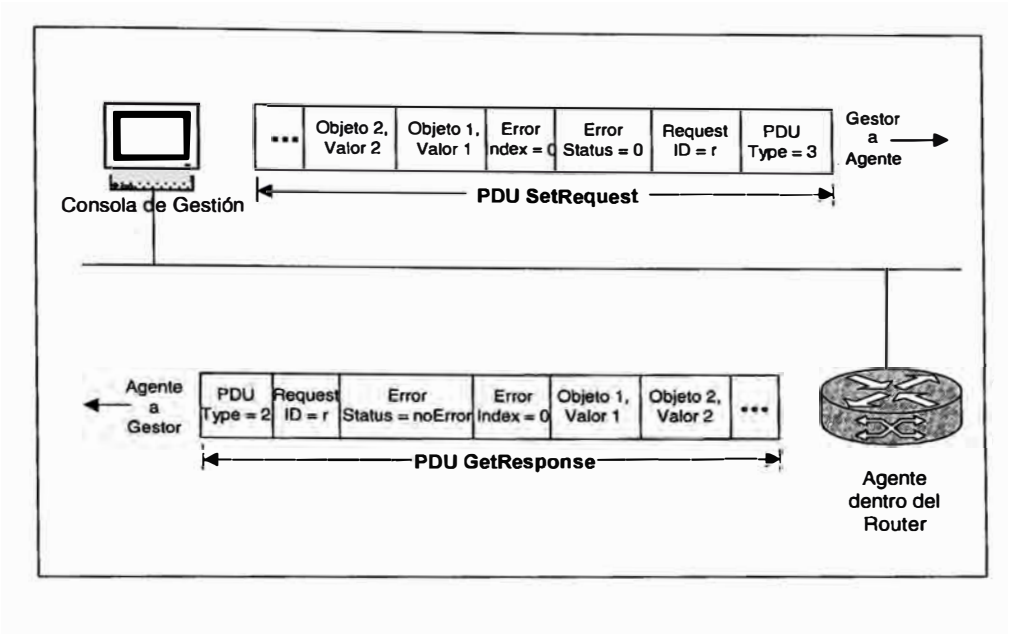

Fig. 4.10 Tranmisión de PDU GetNextRequest/GetResponse (sin errores)

Cuatro condiciones de error son posibles:

- Si una variable en el campo de Variable Bindings no esta disponible para operaciones Set dentro del relevante MIB View, el agente retorna un PDU GetREsponse de forma idéntica, con Error Status = noSuchName, y con el Error Index indicando el índice del nombre del objeto en cuestión. (Nota histórica: Algunas implementaciones de agente retornan Error Status = readOnly si el objeto existe, pero Access = read-only para esa variable.).

- Si el valor de una variable llamada, en el campo de Variable Bindings no adapta al ASN.1 Type, Length, y Value requerido, el agente retorna un PDU GetResponse de forma idéntica, con Error Status = badValue y el Error Index indicando el índice de la variable en cuestión.

- Si el tamaño del PDU GetResponse apropiado excede una limitación local, el agente retorna un PDU GetResponse de forma idéntica, con Error Status = tooBig, y Error Index = 0.

- Si el valor de una variable no puede ser alterado por alguna otra razón, el agente retorna un PDU GetResponse de forma idéntica, con Error Status = genErr y el Error Index indicando el índice de la variable en cuestión.

- El Formato PDU Trap

El PDU Trap tiene un formato distinto de los otros cuatro PDUs SNMP, como puedes ver en la Fig. 4.11. El primer campo indica el PDU Trap y contiene PDU Type = 4. El campo Enterprise identifica la empresa de gestión bajo cuya autoridad de registración el trap fue definido. Por ejemplo, el prefijo OID {1.3.6.1.4.1.110} identificaría Network General Corp. (ahora parte de Network Associtates, Inc.) como el Enterprise enviando un trap. El campo Agent Address, el cual contiene la dirección IP del agente, proporciona identificación adicional. Si un protocolo de transporte no IP es usado, el valor 0.0.0.0 es retornado.

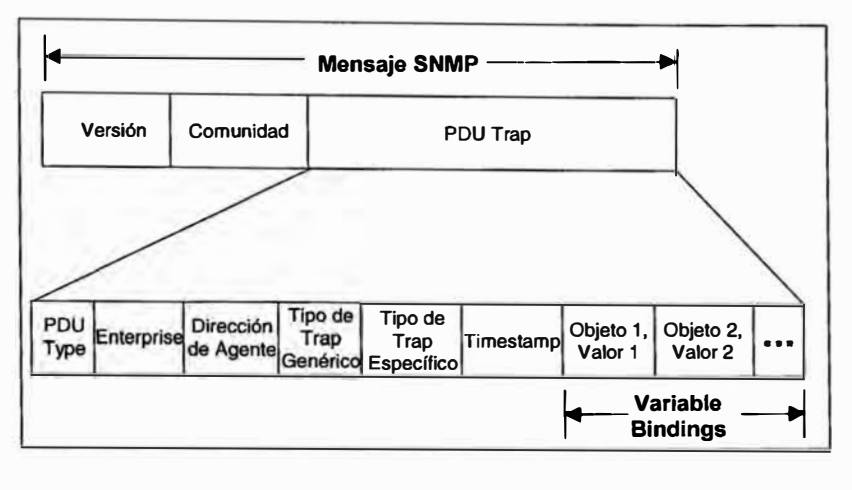

Fig. 4.11 Estructura del PDU Trap de SNMP

El Generic Trap Type proporciona mas información específica en el evento siendo reportado. Hay siete valores definidos (tipos INTEGER enumerados) para este campo.

Trap	**Valor**	**Significado**
ColdStart	0	La entidad de protocolo de envío (gestión de red de capa mas alta) ha reinicializado, indicando que la configuración del agente o implementación de entidad puede ser alterado.
WarmStart	1	El protocolo de envío ha reinicializado, pero ni la configuración del agente ni la implementación de la entidad de protocolo ha sido alterado.
LinkDown	2	Un enlace de comunicación ha fallado. La interfaz afectada es identificada como el primer elemento dentro del campo de Variable Bindings: nombre y

		valor de la instancia ifIndex.
linkUp	3	Un enlace de comunicación ha levantado. La interfaz afectada es identificada como el primer elemento dentro del campo de Variable Bindings: nombre y valor de la instancia ifIndex.
authenticationFailure	4	El agente ha recibido un mensaje SNMP de autentificación impropiamente desde el gestor; esto es, el nombre de comunidad fue incorrecto.
egpNeighborLoss	5	Un vecino par EGP esta caído.
enterpriseSpecific	6	Un trap no genérico ha ocurrido, el cual es identificado adicionalmente por el campo Specific Trap Type y el campo Enterprise.

Dos campos adicionales completan el PDU Trap. El campo Timestamp contiene el valor del objeto sysUpTime, representando la cantidad de tiempo transcurrido entre la última re-inicialización del agente y la generación de ese Trap. El último campo contiene la Variable Bindings.

- Usando el PDU Trap

El agente usa el PDU Trap para alertar el gestor que un evento predefinido a ocurrido. Para generar el PDU Trap el agente asigna un PDU Type = 4 y completa en los campos

Enterprise, Agent Address, Generic Trap Type, Specific Trap Type, y Timestamp, así como la lista de Variable Bindings.

Por definición (y convención), Traps son aplicación específica. Por lo tanto, sería difícil cubrir el rango de usos para este PDU. La Fig. 4.12 ilustra como un agente en un router podría usar un Trap para comunicar un evento significante al gestor.

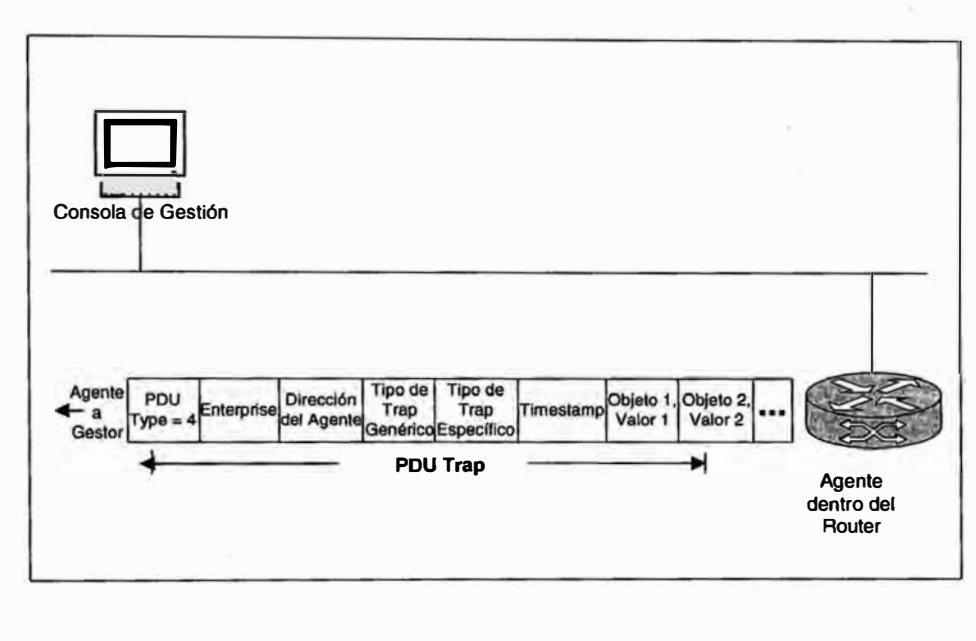

Fig. 4.12 Operación del PDU Trap

4.2 PROTOCOLO DE MONITOREO REMOTO

El MIB de monitoreo remoto (RMON) es usado para monitorear y manejar segmentos remotos de interredes distribuidas.

4.2.1 Monitoreo remoto de Interredes Distribuidas

En la última decada, LANs e interredes han llegado a ser mas complejos, y con eso, los métodos y procedimientos para manejar redes han madurado también. Por ejemplo, una

red consiste de un segmento simple, tal como la topología mostrada en la Fig. 4.13, no necesita mucho rigor en su estrategia de gestión de red. Primero, hay relativamente pocos dispositivos para gestionar, y lo mas importante, estos dispositivos están geográficamente localizados en una localidad central. Así esto sería un proceso directo para diagnosticar y reparar un problema con esta red.

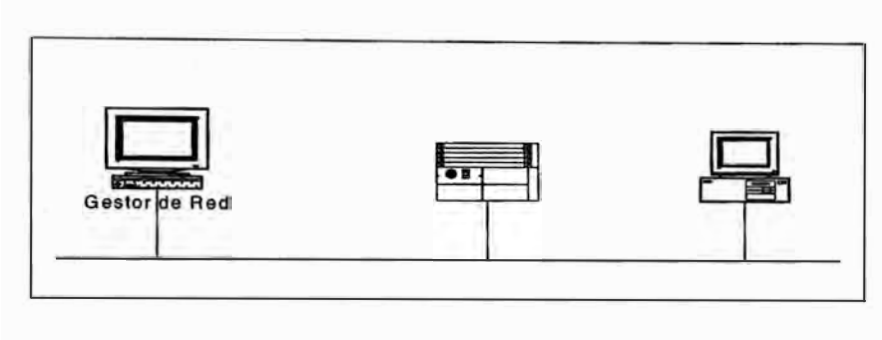

Fig. 4.13 Monitoreo de Red de un Segmento Simple

Interredes distribuidas son una historia diferente, sin embargo, por diferentes razones. Primero, hay mas dispositivos. Segundo, desde que hay múltiples segmentos, los dispositivos en estos segmentos son mas probablemente a ser adquiridos con el tiempo, a ser traídos de diferentes fabricantes, tener diferentes fechas de revisión de software, y así sucesivamente. (No demasiadas interredes son construidas todo a la vez. Es mas probablemente que ellos hayan evolucionado con el tiempo, con los retos típicos que la evolución de red trae). Lo mas importante, cuando dificultades de red ocurren, geografía no ayuda al administrador de red. No puedes estar en múltiples localidades al mismo tiempo, y si la ley de Murphy es cierta, el segmento que estas probando actualmente no es el segmente que debe ser probado. Y al menos que tengas un personal y recursos

ilimitados, no es probable que puedas afrontar enviar colegas a cada segmento para asistir con el problema. Así manejar segmentos de interredes dispersados geográficamente puede ser un reto. Los conceptos de *remote monitoring*, o RMON, son designados para dirigir esos retos. RMON ubica agentes, llamados detectores RMON, en ubicaciones estratégicas en la interred (ver Fig. 4.14). Estos detectores consisten de una interfaz de red (sea Ethernet o token ring), un procesador, y memoria, y son unidos a la red tan igual que otro dispositivo. La consola de gestión de red determina la información que los detectores están reportando, tales como las estadísticas a ser monitoreado, periodos de tiempo sobre el cual colectar información histórica, y así sucesivamente. En efecto, los detectores actúan como los ojos y oídos del sistema de gestión de red, proporcionando a los administradores con detalles de la operación de los segmentos distribuidos que de otra manera no serían accesibles sin algún tipo de interacción humana directa.

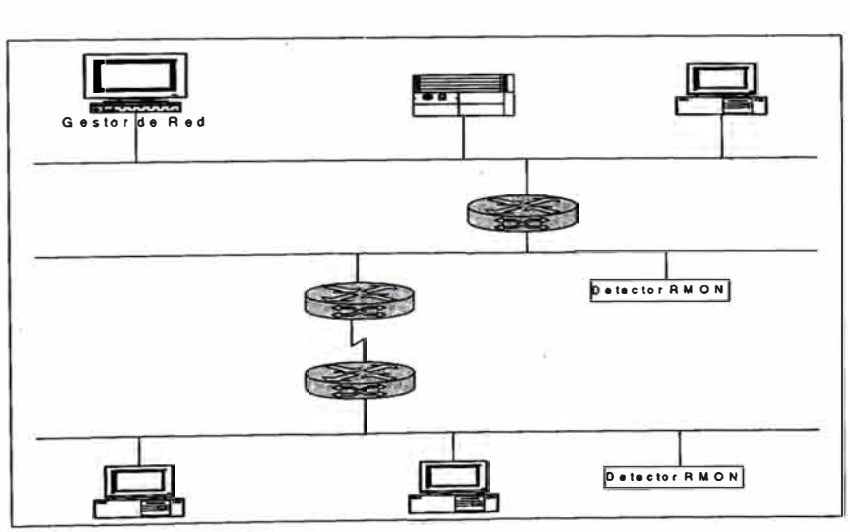

Fig. 4.14 Monitoreo de Segmento de Red Distribuido usando RMON

RMON ha sido desarrollado en tres escenarios, los cuales son descritos a continuación.

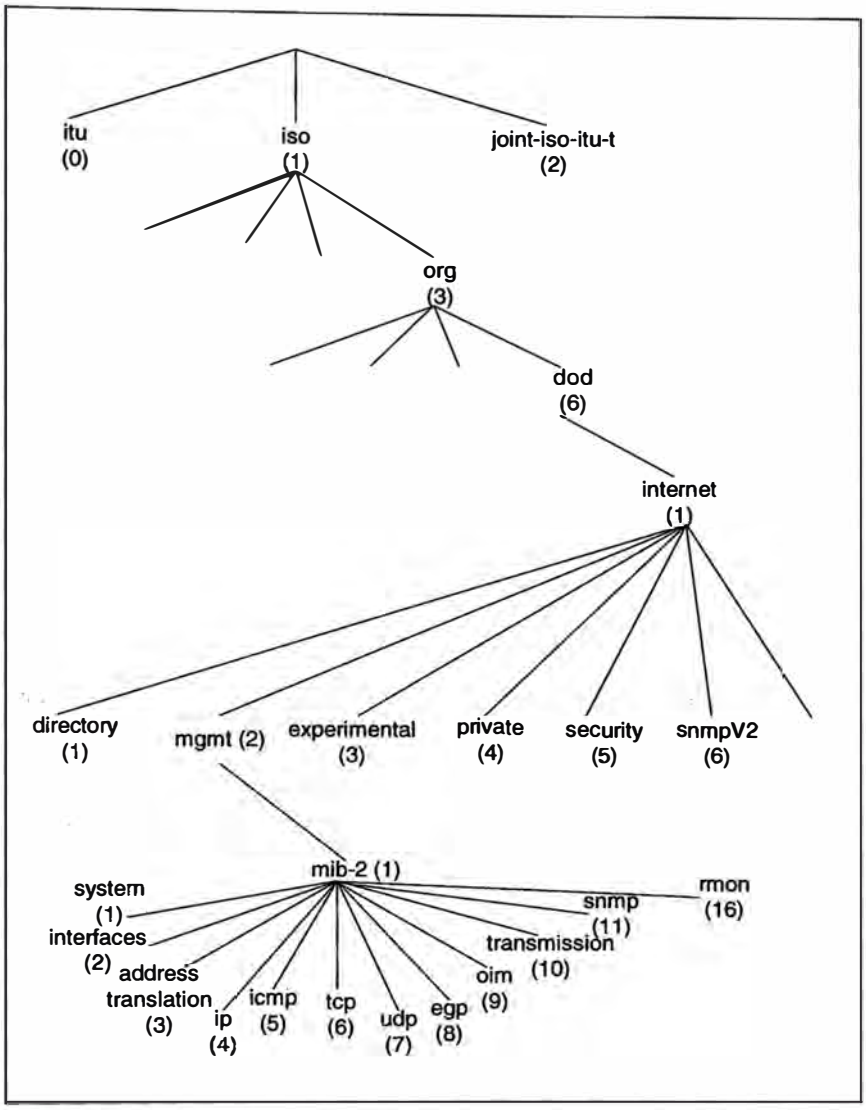

Fig. 4.15 Posición del MIB RMON en el Árbol OID de Internet

4.2.2 El MIB RMON Ethernet

El módulo MIB RMON Ethernet fue el primero en ser desarrollado. Este módulo estandariza la información de gestión enviado a y desde el detector RMON Ethernet y esta representado en el RFC 1757. El MIB RMON original es frecuentemente referido

como el MIB RMON Ethernet. Es asignado el OID {1.3.6.1.2.1.16} y contiene nuevo grupos. Todos estos grupos son opcionales (no mandatorios), pero la implementación de algunos grupos requiere otros grupos. Por ejemplo, el grupo Filter requiere el grupo Packet Capture. A continuación el resumen de los nueve grupos Ethernet:

Grupo	**Descripción**
Statistics (1)	Proporciona estadísticas medidas por el detector, tal como el número y tamaños de paquetes, broadcasts, colisiones, y así sucesivamente.
history (2)	Registra muestras estadísticas periódicas con el tiempo que puedes usar para analizar tendencias.
alarm (3)	Compara muestras estadísticas con niveles preseleccionados, generando alarmas cuando un nivel particular es pasado.
host (4)	Mantiene estadísticas de los hosts de la red, incluyendo las direcciones MAC de los hosts activos.
hostTopN (5)	Proporciona reportes almacenados por las estadísticas de tabla del host, indicando cuales de los hosts están al tope de la lista en una categoría particular.
matrix (6)	Almacena estadísticas en una matriz de tráfico que rastrea conversiones entre pares de hosts.
filter (7)	Permite paquetes a ser coincididos de acuerdo a una ecuación de filtro.

capture (8)	Permite paquetes a ser capturados después de que ellos pasen a través de un canal lógico.
event (9)	Controla la generación y notificación de eventos, el cual puede incluir mensajes de trap SNMP.

El estándar actual, RFC 1757, dirige solamente monitoreo de red Ethernet. La siguiente sección veremos las extensiones del token ring.

4.2.3 El MIB RMON Token Ring

Fue creado al adicionar tablas al MIB RMON Ethernet, y al adicionar un grupo décimo, tòdo en soporte de redes token ring. Recordar que el MIB RMON Ethernet define nueve grupos, desde Statistics hasta Events. El MIB RMON Token Ring extiende dos de estos grupos, Statistics e History, y adiciona un único grupo. Este grupo nuevo es llamad tokenRing, con identificado de objeto {rmon 10}.

Las extensiones de Statistics permiten un dispositivo compatible con RMON colectar errores de la capa MAC del token ring y errores promiscuos. Los errores de la capa MAC, tales como errores de token y errores de frame copiados, son específicos al protocolo token ring; los errores promiscuos, tal como número de contador de paquetes broadcast o paquetes de datos entre 512 y 1023 octetos de longitud, son mas generales. El grupo tokenRing contiene cuatro subgrupos: ring station, el cual monitorea eventos específicos de estación y anillo; ring station order, el cual rastrea la topología de red;

ring station configuration, el cual controla la eliminación y/o configuración de estaciones en el anillo; y source routing, el cual detalla información de rutas fuente.

4.2.4 RMON2

Los MIBs RMON originales para redes Ehternet y token ring son principalmente concernientes con la operación y gestión de las capas física y enlace de una red remota. Como tal, pueden compilar estadísticas e información histórica relativo a colisiones Ethernet, frame token ring con errores copiados, y así sucesivamente, pero no pueden ver dentro la operación de la red OSI hasta las capas de aplicación de esa red remota.

RMON2, definido en RFC 2021, extensiones de las capacidades de RMON para esas capas mas altas al adicionar diez nuevos grupos, designado {rmon 11} hasta {rmon 20}. Así, RMON2 permite los protocolos de capa mas altas, tal como TCP/IP o SPX/IPX, para ser monitoreado para visibilidad de gestión mas grande dentro de la interred. A continuación los diez grupos:

Grupo	**Descripción**
protocolDir (11)	Protocol Directory: lista, en una tabla, el inventario de protocolos que el detector tiene la capacidad de monitorear. Cada protocolo es descrito por una entrada en la tabla.

ProtocolDist (12)	Protocol Distribution: colecciona la cantidad relativa de octetos y paquetes para los diferentes protocolos que son detectados en un segmento de red. Cada protocolo es descrito por una entrada en una tabla, y la estación de gestión de red puede fácilmente determinar el ancho de banda consumido por protocolo accediendo la información en esa tabla.
addressMap (13)	Address Map: correlaciona direcciones de la capa de red y direcciones de la capa MAC, y almacena la información en tablas.
nlHost (14)	Network Layer Host: cuenta la cantidad de trafico enviado desde y hacia cada dirección de capa de red descubierto por el detector, y almacena la información en tablas.
nlMatrix (15)	Network Layer Matrix: cuenta la cantidad de tráfico enviado entre cada par de direcciones de red descubierta por el detector, y almacena la información en tablas de ambos fuente a destino y destino a fuente.
alHost (16)	Application Layer Host: cuenta la cantidad de tráfico, por protocolo y por host, que es enviado desde y para cada dirección de red descubierta por el detector.

alMatrix (17)	Application Layer Matrix: cuenta la cantidad de tráfico, por protocolo, enviado entre cada par de dirección de red descubierta por el detector, y almacena esta información en tablas. Este grupo es similar al grupo nlMatrix, pero el enfoque esta en el protocolo en operación.
usrHistory (18)	User History: combina mecanismos vistos en los grupos alarm (3) e history (2) para proporcionar colección histórica de usuario especificado, y almacena esa información en tablas.
probeConfig (19)	Probe Configuration: controla la configuración de varios parámetros operacionales por el detector, tal como los grupos RMON Ethernet y token ring que son soportados por el detector, números de revisión de software y hardware del detector, una tabla destino de trap, y así sucesivamente.
rmonConformance (20)	RMON Conformance: describe los requerimientos para conformidad al MIB RMON2.

4.3 OTROS PROTOCOLOS

Similar al protocolo SNMP entre otros protocolos estándares tenemos:

MIB-II es un protocolo estándar de Internet. Su estado es recomendado. La especificación actual se puede encontrar en RFC 1213 - Base de Información de Gestión para la Gestión de Redes basadas en Interredes TCP/IP: MIB-II.

Los estándares ISO/IEC 9595 y 9596 definieron CMIP (Protocolo de Información de Gestión Común) y CMIS (Servicios de Información de Gestión Común).

CMOT (CMIS/CMIP sobre TCP/IP) es un protocolo estándar propuesto de Internet. Su estado es electivo. La especificación actual se puede encontrar en el RFC 1189 - Servicios de Información de Gestión Común y Protocolos para Internet (CMOT) y (CMIP).

OIM-MIB-II es un protocolo estándar propuesto de Internet. Su estado es electivo. La especificación actual puede encontrarse en el RFC 1214 - Gestión de Internet OSI: Base de Información de Gestión.

CAPÍTULO V

ADMINISTRACIÓN DE REDES TCP/IP

5.1 CENTRO DE INFORMACIÓN DE RED

El NIC (Network Information Center) tiene como principal actividad el mantenimiento de una Base de Datos en donde se concentra la información referente a cada una de las instituciones que conforman la red. Los servicios que ofrece el NIC están orientados básicamente a las necesidades generales de cada una de las redes locales, los cuales son descritos a continuación.

5.1.1 Servicio de Nombres

Actualmente todos los hosts deben contar con una dirección IP y un nombre, el cual esta asociado a un dominio (institución.país). Esto les permite ser identificados dentro de Internet y poder tener comunicación con otros hosts. Por ello es conveniente que cada uno de ellos este dado de alta en las Bases de Datos del Servicio de Nombres; esto se hace mediante una solicitud que envía el administrador de la red local al NIC.

5.1.2 Asignación de Direcciones IP

El NIC asigna a cada una de las dependencias que se conectan a la red un rango de direcciones IP. El administrador de red local es el responsable de hacer esta solicitud al NIC. La persona encargada de asignar una dirección IP a cada uno de los hosts que conforman la red de la dependencia. El NIC se reserva el derecho de ceder o retirar la administración total o parcial de las subredes a quien considere conveniente. Con base a las normas de uso aceptable buscando siempre el mejor desempeño de la administración de la misma

5.1.3 Solicitud y Asignación de Dominios

En el caso de las dependencias internas, el NIC le asigna a cada una de ellas un subdominio (por ejemplo: escuela.pe,lab.escuela.pe), previa solicitud del administrador local. Para las instituciones externas, el NIC hace la solicitud de dominios ante el NIC-Regional para aquellas que así lo requieran.

5.1.4 Servicio de Servidor Secundario

En muchas ocasiones, instituciones ajenas a la institución requieren de tener un servidor secundario para sus dominios; el NIC puede ofrecer este servicio a aquellas que estén directamente conectadas a ella.

5.1.5 Elaboración e Implementación de Políticas

Este es uno de los pilares para la administración de la red. El NIC elabora políticas de cada uno de los servicios que brinda y de acuerdo a las necesidades de administración. Se lleva a cabo en conjunto con los diversos grupos de trabajo que intervienen en la operación de la red. Para dar a conocer a los administradores de red los lineamientos que se deben seguir para hacer uso de los servicios. Los administradores deben d estar de acuerdo con estas políticas y es su responsabilidad hacerlas del conocimiento de sus usuarios.

5.2 GESTIÓN DE REDES CORPORATIVAS

La gestión de redes corporativas involucra un conjunto de actividades basadas en las funciones de gestión

5.2.1 Gestión de fallas y recuperación

Comprende el conjunto de facilidades que permiten la detención, el aislamiento y la corrección de las operaciones anormales de las redes o sistemas de comunicaciones. Esta función en general comprende el conjunto de actividades orientadas a detectar, diagnosticar, anular, reparar e informar sobre los fallos de los equipos que componen las redes o los servicios de telecomunicación utilizados. Un fallo en la red trae como consecuencia que el usuario no pueda utilizar algún servicio, por lo que es deseable su pronta detección y resolución. Se pueden seguir los siguientes pasos:

- Identificar el problema.

- Aislar el problema.

- Solucionar el problema.

El beneficio es incrementar la confiabilidad de la red dando herramientas para detectar problemas e iniciar procedimientos de recuperación más rápidamente.

5.2.2 Gestión de la configuración.

El área funcional de la gestión de la configuración incluye al conjunto de facilidades pensadas para la realización de los 5 grupos de actividades siguientes: - Construcción de la topología de la red de acuerdo con la visión del usuario. Incluir y dar de baja dispositivos.

- Establecimiento de los parámetros de funcionamiento, es decir, inicialización y modificación de la configuración de todos los recursos de la red.

- Mantenimiento de un inventario de los dispositivos instalados y de las líneas que los conectan.

- Administración de la correspondencia entre nombres de dispositivos y sus direcciones de red para que los usuarios manejen los recursos según su visión de la red.

- Gestión racional de los cambios de configuración.

Pasos:

- Obtener información del estado actual de la red (errores).

- Usar esos datos para modificar la configuración de los dispositivos de red.

- Almacenar los datos y tener un inventario de todos los dispositivos de la red.

El beneficios es permitir el acceso rápido a la configuración de todos los dispositivos de red.

5.2.3 Gestión del rendimiento.

Esta área funcional comprende el conjunto de funciones destinadas a la obtención de información para conocer en todo momento:

- El grado de utilización de los recursos de la red.
- El nivel de cumplimiento de servicio a los usuarios.

La recolección de estadísticas acerca del tráfico de los elementos de la red, es el método más empleado para el cálculo y conocimientos del grado de utilización de los recursos de la red. Estas estadísticas deben guardarse en bases de datos históricas para poder disponer de la historia de la red.

Del análisis comparativo de estas bases de datos históricas pueden obtenerse datos sobre el ritmo de crecimiento del tráfico con objeto de realizar ampliaciones, etc.

Pasos:

- Obtener información de la utilización actual de los dispositivos de la red y sus enlaces.
- Analizar la información más relevante para discernir las tendencias de utilización.
- Establecer límites de utilización.
- Simular tráfico para predecir su comportamiento y maximizar su rendimiento.

El beneficio es proporciona consistencia en el servicio y permite corregir problemas potenciales.

5.2.4 Gestión de la contabilidad

Esta área funcional proporciona las herramientas necesarias para mantener informados a los usuarios de la red de la utilización realizada de los recursos. Los procedimientos que permiten conseguir esta funcionalidad son:

- La identificación del uso de recursos y el intercambio de información entre diferentes sistemas de comunicaciones.
- La información sobre tarifas y límites para ciertos recursos, y la posibilidad de establecer estos límites.
- La posibilidad de compartir costos cuando dos o más sistemas de comunicaciones cooperan en la prestación de un servicio.

Pasos:

- Obtener información de la utilización de los recursos de la red.
- Establecer cuotas de utilización.
- Realizar el cobro por utilización de la red.

El beneficios es dar a conocer la utilización de la red para hacerla más productiva, permite medir y reportar la utilización de los recursos por los usuarios y determinar el costo por utilización.

5.2.5 Gestión de la seguridad

El propósito de esta área funcional es el de servir de soporte a la aplicación de políticas de seguridad. Los mecanismos que proporciona son:

- La creación, eliminación y mantenimiento de servicios y mecanismos de seguridad de acuerdo con la política de seguridad establecida.
- La distribución de información de seguridad.
- La información acerca de las violaciones de la seguridad. También de los intentos fallidos.

Los pasos a seguir son identificar la información a proteger, encontrar los puntos de acceso, proteger los puntos de acceso y mantener la seguridad. El beneficio es evitar malos manejos de información que pudieran afectar el desempeño de mi red o la integridad de ésta.

5.3 GESTIÓN DE UN AMBIENTE INTERNET

Las tres arquitecturas de gestión de red discutidas anteriormente tienen un denominador común: Su diseño fue un proceso formal involucrando participantes alrededor del mundo. Lo mas importante, la arquitectura de gestión de red fue puesto en primer plano, y los proveedores fueron entonces estimulados a implementarlo.

El Internet, sin embargo, fue una interred operacional mundial, así sus administradores no podían estudiar gestión de red por años antes de aparecer con una implementación. El Internet fue derivado de investigación del gobierno de U.S. que comenzó en 1969. El

objetivo fue desarrollar tecnologías de comunicación y protocolos de modo que las organizaciones gubernamentales, contratistas de defensa, e investigadores académicos usando sistemas de computadores similares puedan colaborar en proyectos. El resultado del proyecto de investigación del gobierno fue la Agencia de Investigación de Proyectos Avanzada de red (ARPANET), el cual usó tecnología de conmutación de paquetes para conectar sistemas diferentes. ARPANET llegó a ser en 1969 con nodos en cuatro localidades en los Estados Unidos. Desde ese inicio humilde, el Internet ahora conecta más de un millón de computadores servidores alrededor del mundo.

A finales de los 80's, el Internet Activities Board (IAB) se percató que este necesitaba un método para gestionar el crecimiento de Internet y las otras redes anexas. El tablero consideró tres propuestas: la entidad de sistema de gestión de alto nivel (HEMS); un sistema basado en OSI, usando CMIS y CMIP; y extensiones al existente protocolo de monitoreo de puerta simple (SGMP) que las redes regionales que adoptan el Internet estuvieron usando.

El IAB decidió tomar un alcance de dos pasos para la gestión de Internet. Mejoramientos al SGMP, el cual llegó a ser conocido como el protocolo de gestión de red simple (SNMP), facilitarían una solución a corto plazo. Una solución a largo plazo sería basado en la arquitectura CMIS/CMIP, y fue llamado CMOT (CMIP sobre TCP/IP).

Una solución CMOT a largo plazo, sin embargo, nunca ha recibido las arquitecturas ampliamente generalizadas. CMOT es actualmente denominado "histórico," significando que los estándares más recientes lo han reemplazado o que es considerado obsoleto por alguna otra razón. Sin embargo CMOT será discutido brevemente posteriormente.

5.3.1 SNMP, el Protocolo de Gestión de Red Simple

SNMP es basado en el modelo gestor/agente (ver Fig. 1). SNMP es referido como "simple" porque el agente requiere software mínimo. La mayoría de la fuente de procesamiento y almacenamiento de datos reside en el sistema de gestión, mientras un subconjunto complementario de estas funciones reside en el sistema gestionado.

Para lograr esta meta de ser simple, SNMP incluye un conjunto limitado de comandos y respuestas de gestión (ver Fig. 5.1). El sistema de gestión emite mensajes Get, GetNext, y Set para recuperar variables de objetos individuales o múltiples ó establecer el valor de una variable individual. El sistema gestionado envía un mensaje Response para completar el Get, GetNext, o Set. El sistema gestionado envía un evento de notificación, llamado un trap, al sistema de gestión para identificar la ocurrencia de condiciones tal como un umbral que excede un valor predeterminado.

SNMP asume que el camino de comunicación es una subred de comunicación sin conexión. En otras palabras, ruta de comunicación no planeado de antemano es

establecida previo a la transmisión de datos. Como resultado, SNMP no garantiza una entrega confiable de los datos; sin embargo, en la práctica la mayoría de mensajes consiguen pasar, y esos que no pueden ser retransmitidos. Reobservando la Fig. 5.1, los protocolos primordiales que SNMP implementa son el UDP (User Datagram Protocol) y el IP (Internet Protocol). SNMP también requiere protocolos de capa de enlace de datos, tal como Ethernet o tokeng ring, para implementar el canal de comunicación desde el sistema de gestión hasta el sistema gestionado. La simplicidad y comunicación sin conexión del SNMP también produce un grado de robustez. Ni el gestor ni el agente confía en el otro para su operación. Así, un gestor puede continuar funcionando aún si un agente remoto falla. Cuando el agente reactiva el funcionamiento, puede enviar un trap al gestor, notificándolo de su cambio a estado operacional.

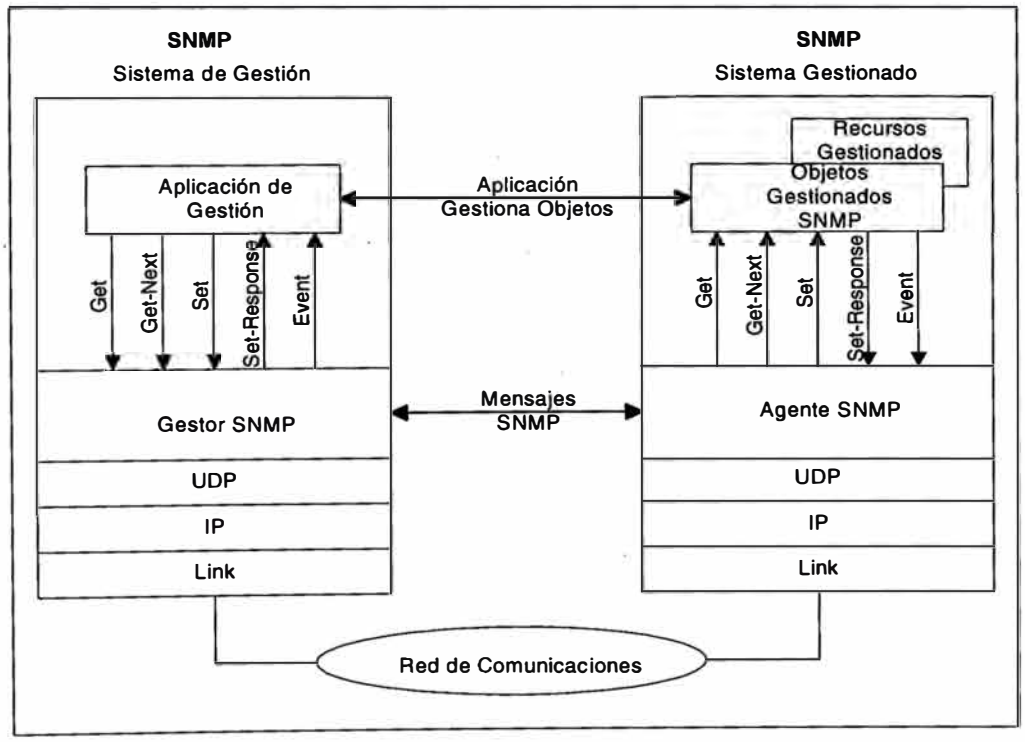

Fig. 5.1 Arquitectura SNMP

5.3.2 CMIP sobre TCP/IP (CMOT)

Como resultado del estudio de varias estrategias de gestión de interred, en 1990 el IAB desarrollo una estrategia para implementar CMOT. A pesar de que el IETF (el cuerpo de estándares en Internet) ha diseñado esto trabajo como "histórico", una cantidad de vendedores han incluido el CMOT en sus planes de arquitectura.

Arquitectónicamente, CMOT encaja en el paradigma gestor/agente (ver Fig. 5.2). Diferente al SNMP, el cual provee servicio sin conexión usando UDP/IP, sin embargo, CMOT asegura el transporte confiable de datos. Para garantizar el transporte confiable, los sistemas CMOT establecen las conexiones de capa de Aplicación antes de transmitir la información de gestión.

Los servicios de capa de Aplicación del CMOT están construidos sobre los tres servicios de OSI: CMISE (Common Management Information Service Element), ROSE (Remote Operation Service Element), y ACSE (Association Control Service Element). Un LPP (Lightweight Presentation Protocol) proporciona los servicios de la capa de Presentación.

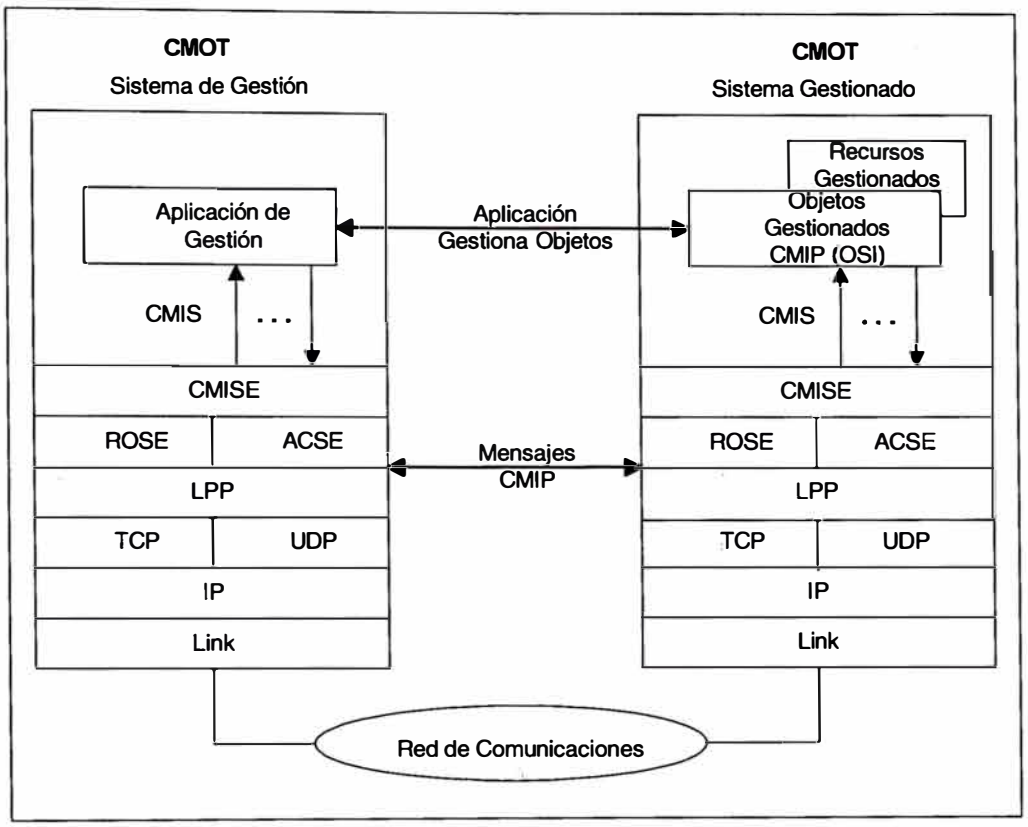

Fig. 5.2 Arquitectura CMOT

El modelo CMOT también es mas riguroso que el SNMP. La definición de objetos CMIP son mas comprensivos e incluyen atributos, eventos emitidos, y acciones imperativos. Como nosotros discutimos, SNMP define primariamente los objetos por grupos funcionales.

Sin embargo, SNMP es hoy, y muchos vendedores de ambos sistemas agente y gestión implementan SNMP. Como testimonio del amplio uso, el SNMP continua siendo mejorado.

5.4 FACTURACIÓN DE SERVICIOS

Otra tarea importante que se realiza en la gestión es la facturación de servicios, esto puede llevarse a cabo a través del centro de operaciones de la red. Se refiere a contabilizar el tráfico generado por todas las redes locales que se conectan a la red global. Los sistemas de monitoreo recolectan esta información diariamente para ser almacenada en una base de datos que será accedida por programas desarrollados por el área de sistemas conjuntamente con el NOC, con la finalidad de generar de manera condensada y verás la contabilidad de tráfico de cada enlace arrendado y emitir la factura correspondiente al servicio contratado.

CAPÍTULO VI

POLÍTICAS DE GESTIÓN DE REDES

6.1 ELABORACIÓN E IMPLEMENTACIÓN DE PROCEDIMIENTOS

Los modernos sistemas de administración y las herramientas son adquiridos principalmente de los programas diseñados por un equipo de consultores en la red con amplia experiencia en muchas empresas internacionales. Se logra una madurez del mismo luego de encontrar muchas dificultades y obstáculos en su desarrollo. Sin embargo, las principales fortalezas del sistema se alcanzan precisamente por la forma como se atacan los problemas.

6.1.1 El proceso de Adaptación

Uno de los principales problemas que se presenta en las primeras etapas de concatenar el proceso, es que el sistema puede parecer complejo, creando una respuesta negativa por parte de todos los participantes en todos los niveles de la organización. Por tanto, el sistema es rediseñado para simplificar el fácil entendimiento de cualquier persona. Los

siguientes requerimientos son usados como herramienta para la implementación de un sistema simplificado:

- Gran énfasis en los resultados.
- Fácil de usar.
- Todas las herramientas deben ser integradas como parte de un sistema completo.

Respeto por los valores humanos.

Otro de los grandes problemas es la adaptación de los valores Latino Americanos al sistema. Creemos que nuestra cultura tiene valores fuertes y creemos que deben ser considerados para la efectiva implementación del sistema. El entrenamiento inicial con las herramientas de control de calidad es otro de los problemas enfrentados, administración diaria, pero el entusiasmo de la gente es realmente relevante cuando se forma parte del desarrollo de todo un sistema en una empresa.

6.1.2 Los Elementos del Sistema

El objetivo del sistema es dar satisfacción a todos los consumidores de la Empresa. El primer consumidor es representado por los clientes, y la empresa debe de entender sus necesidades y satisfacerlos completamente con productos y servicios que sean atractivos para ellos con buenos niveles de calidad, precio, servicio y entrega. El segundo consumidor son los accionistas o propietarios de la empresa quienes deben de tener una buena retribución por el dinero que ellos han invertido y por el buen trabajo que han hecho por servir a sus clientes. Las ganancias deben ser reinvertidas en la empresa y

deben de ser compartidas con los empleados. El tercer consumidor son los empleados quienes deben de estar felices de trabajar en una empresa que se interesa por su desarrollo y cuida de todas las necesidades humanas. Finalmente el cuarto consumidor es la sociedad y la empresa no debe hacer nada que dañe el medio ambiente y debe contribuir al desarrollo de la armonía de la comunidad donde esta localizada.

Política básica (3 a 5 años) con una misión, visión y valores. La misión es el principal propósito de la empresa, donde toda la energía del equipo humano debe estar concentrada. La visión es adonde queremos llegar o lo que queremos ser en un tiempo determinado. Los valores son aquellos que rigen a la empresa, como la gente debe actuar.

Política anual (1 año), que contemple los principales objetivos para un año. Uno de los trabajos más importantes para lo líderes y directores de la empresa es tomar las decisiones correctas en orden de establecer prioridades para la asignación de los recursos y las mejoras que sean necesarias. Esto debe ser hecho a través de una política anual, por ejemplo usando la técnica Hoshin Kanri. Esta política debe contemplar los cuatro consumidores de la empresa, clientes, accionistas, empleados y el medio ambiente. Es muy conveniente también contemplar el desarrollo del sistema de gestión.

El mejoramiento continuo (1 a 3 meses) consiste en planear, ejecutar, revisar y actuar. Es la herramienta básica para un trabajo sistemático entre los directores y gerentes de la

empresa. Un plan tiene tres elementos principales: objetivo, meta y método. El método debe de ser desarrollado usando la técnica de 5W + 1H., qué, por qué, quién, cuando, dónde y cómo.

Todas las actividades que son llevadas a cabo diariamente para satisfacer la necesidades de los clientes, deben ser estandarizadas. PDCA y SDCA son usados simultáneamente en la empresa.

Las técnicas usadas en el sistema desde la política básica hasta la administración diaria son usadas para soportar estas actividades. Ellas pueden ser implementadas considerando la política anual en cada empresa, tales como investigación de mercado, shake down, evaluación de la competencia, auditorías al presidente, evaluación al del cliente, 5's, workshop, liderazgo, TPM, sistema de sugerencias, la ruta de la calidad, herramientas básicas, ISO 9000, círculos de control de calidad, sistema de administración interfuncional, justo a tiempo.

El sistema de documentación tiene tres niveles. Nivel Estratégico, deben ser considerados el Manual de Calidad, La Política Básica, y la información básica para establecer las estrategias de la empresa. Nivel Táctico, deben ser incluidos todos los documentos para los esfuerzos de mejoramiento del PDCA y el despliegue de la política. Nivel Operacional, deben de ser considerados todos los procedimientos estándar y las instrucciones para la administración diaria de la empresa.

6.2 ASIGNACIÓN Y AUTOMATIZACIÓN DE RECURSOS

Para prestar servicio a todas las dependencias de gestión y operación de la red se requiere mantener la asignación de recursos de las partes relacionadas al hardware y software a manera de realizar una planificación y distribución de estos recursos acorde con las necesidades de los productos vía un sistema automatizado.

Parte de los recursos con que cuenta una empresa, es la de recursos humanos, pueden reclutar, retener y formar a sus empleados de forma más eficaz, La optimización del personal laboral transforma las operaciones de recursos de red repetitivas y basadas en papel en procesos de autoservicio de la red. Esto significa que los empleados son capaces de ver y modificar los beneficios de los cambios proyectados. Para esto se asignan perfiles para reducir el tratamiento de muchas tareas de gestión mejorando la productividad del servicio y una alta tasa de disponibilidad de recursos de red.

Sin duda contar con servicios automatizados para gestionar y operar una red es de mucha utilidad porque ayuda a participar activamente y compartir diversos proyectos a la vez, ahorrando tiempo y dinero en los procesos técnicos. Disponer de inventario total de red y clientes, bajo una estructura de información en bases de datos automatizadas agiliza su actualización en línea de manera eficiente.

6.3 CONTRIBUCIÓN AL NEGOCIO: COSTOS, PRECIOS Y DISPONIBLIDAD

Definitivamente realizar gestión y operación a las redes tiene un costo importante. Implica contar con un personal distribuido por turnos de tal manera que cubra las 24 horas del día, los 365 días del año. Mantener la operatividad de la red en un 99.99% de disponibilidad, implica realizar un análisis detallado de los eventos reportados con el fin de reducir gastos futuros.

Disponer de un centro de operaciones de red es de alguna atractivo para los clientes porque brinda confiabilidad sobre el producto que contrata, desde donde se cuenta con la disponibilidad de corregir fallas en muchos de forma pro-activa y en otros tantos de manera preventiva. Garantizando al usuario de la red un mínimo por pérdida de enlace en caso ocurriera. Para lograr esto se debe tener conocimiento de todos los planes de contingencia y recursos disponibles al momento, esto a través de una base de datos sólida.

Por otro lado, como parte de la operación es cumplir con las solicitudes hechas por los clientes sobre un servicio específico, para esto se establecen precios que son calculados según el grado de complejidad y recurso implicado para recuperar lo invertido en los mantenimientos del equipamiento de red, así como el pago a empleados. Una opción de equilibrar los gastos al mantenimiento es recuperar en las ventas o alquileres de equipos de un proveedor socio. Con un buen servicio los beneficios a corto plazo son superiores.

Es prescindible identificar a los clientes potenciales haciendo un seguimiento más preciso de los logros con su servicio y ubicar las oportunidades que surgen.

CONCLUSIONES

1. Al término de este informe, se ha visto en que consiste un sistema de gestión de red y el papel importante que juega el administrador de red no interesando cuan grande o pequeña sea la red, el sistema a ser administrado tiene que ser una persona calificada y debe contar con el equipamiento necesario para el logro de una gestión exitosa.

2 Los principales elementos que participan en el intercambio de información son el gestor y el agente, estos interactúan a través de mensajes usando el protocolo SNMP. Existen otras arquitecturas que definen sus propias estructuras de trabajo tales como el OSI y el IEEE, además de las plataformas de alto nivel que se desarrollan con herramientas web tal como el Java. Así mismo en la actualidad se cuentan con aplicaciones de proveedores que soportan sistemas de gestión de red.

3. Las actividades y elementos estándares para la gestión y operación de redes están definidas por OSI, entre los cuales se tiene la gestión de fallas (identificar, clasificar, y mitigar), cuentas, rendimiento, seguridad. Dar el mantenimiento preventivo y correctivo a través del centro de operaciones de la red, así como cuidar la alta disponibilidad de los

recursos y servicios. Brindar el soporte remoto adecuado a las instalaciones de campo vía los gestores provistas por los proveedores.

4. Los protocolos de gestión como el SNMP tienen una amplia ventaja por la sencillez en el manejo de sus mensajes, cuyas instancias se encuentran localizadas bajo un árbol estandarizado. El SNMP consta principalmente de un número de versión y el nombre de comunidad para que pueda ser autentificado por su similar. El monitoreo remoto de redes con el RMON se logra con detectores Ethernet y token ring basadas en la operación y gestión a nivel físico y enlace, mientras queel RMON2 puede ver las capas más superiores de OSI.

5. La elaboración de procedimientos estableciendo políticas de calidad en la gestión favorece en el desempeño tanto del personal dedicado como el mantenimiento y la solución inmediata de los problemas de los clientes, para esto se requiere contar con las herramientas modernas, con una base de datos sólida, logrando una automatización de recursos y por ende un ahorro de costo de operación efectivo.

BIBLIOGRAFÍA

1. Mark A. Miller, P.E. "Managing Internetworks with SNMP" Ed. M&T Books, 1999.
2. Hewlett-Packard Company. "Managing Your Network with HP OpenView Network Nodo Manager" Ed. HP Company, 1999.
3. Paul L. DellaMaggiora. "Performance and Fault Management" Ed. Cisco Press, 2000.
4. David Perkins. "Understanding SNMP MIBs" Ed. Prentice Hall, 1999.
5. Douglas R. Mauro, Kevin J. Schmidt. "Essential SNMP" Ed. O'Reilly, 2000.