

## **CAPÍTULO II**

El presente capítulo consta de: antecedentes de la investigación, marco teórico, definición de términos básicos, definición conceptual y operacional de la variable.

### **MARCO TEÓRICO**

#### **1. Antecedentes de la Investigación**

Al lograr definir el planteamiento del problema, precisados los objetivos generales y específicos que regirán los lineamientos de esta investigación, se hace necesario señalar trabajos realizados por investigadores independientes que sustentarán el objeto de estudio, a tal efecto se indican antecedentes hasta el momento relacionados al tema de investigación del modelo de gestión de redes.

Sabino (1998), El punto de partida de una investigación para construir el marco teórico lo constituyen los conocimientos previos de los fenómenos que se abordan en la que se exponen las características dentro de lo que se denomina "Antecedentes".

En otras ocasiones, cuando se trata de indagaciones se reduce en realidad de estudios aplicados o de investigaciones que buscan extender nuevos casos de estudio.

Bravo (1995). **Modelo integral de una red de gestión para administrar los sistemas de telecomunicación en la central de transmisión digital de Lagunilla Maraven**, tesis de grado para optar a la Licenciatura de Informática de la Universidad Rafael Beloso Chacín.

En función de su objetivo principal proponer un modelo integral de una de red de gestión permitir establecer controles en áreas funcionales; fallas, desempeño, seguridad y configuración de acuerdo a la cantidad de información que se maneja, una investigación descriptiva documental con un diseño no experimental transversal descriptivo; como resultado se demostró su aplicabilidad sobre los procesos y equipos para permitir que se establezca un servicio de red en forma optima .

Palma (2000), **Configuración e instalación del Netview como herramienta de control centralizado para el monitoreo de redes LAN y WAN. Estudio de Caso: IBM de Venezuela. e IBM Andino.** De la Universidad Nueva Esparta Escuela Electrónica como objetivo principal configuración de un software de monitoreo utilizando el Netview, fue implantado para cumplir con las tareas de supervisión, control y monitoreo de los equipos conectados a la red de IBM para llevar a cabo la gestión de red.

En la investigación se demostró que gracias a esta herramienta el personal de IBM que esté conectado a la red de la empresa estará lejos de apreciar un desperfecto de las capacidades que le ofrece la Red LAN y WAN, para el monitoreo de toda la estructura de la red usando el protocolo SNMP.

Morales, (2002). **Modelo de Gestión del conocimiento en empresas de telecomunicaciones de ciudad Maracaibo**, tesis de grado para optar a la Maestría en Gerencia de Proyectos Industriales de la Universidad Rafael Beloso Chacín, con el objetivo principal de proponer un modelo de gestión para administrar servicios de telecomunicaciones, se sustentó en los principios de Nonaka y Taveuchi (1995).

Investigación descriptiva de campo, como proyecto factible, diseño no experimental transversal, con una población de 10 empresas de la ciudad de Maracaibo, como resultado se tuvo la propuesta contribuiría a mejorar el tiempo de supervisión de las redes digitales, efectividad, competitividad tecnológica acorde a las exigencias del mercado.

Hernández, (2003), **Propuesta de un modelo de gestión de recursos de red para la administración de la seguridad y detección de fallas** tesis de grado para optar a la Maestría en Telemática de la Universidad Rafael Beloso Chacín, con el objetivo principal proponer un modelo de gestión de recursos de red para monitoreo y control...para la empresa Procedatos. Su propósito fue mejorar la capacidad y tiempo de respuesta frente a las demandas de los clientes de la empresa.

Investigación descriptiva de campo, proyecto factible, diseño no experimental, transversal, con una población de 1754 sujetos a una muestra de 325, la confiabilidad se ubicó en 0.90, se llegó a la conclusión de proponer un modelo de gestión de red para el uso de los recursos tecnológicos de la organización ofreciendo disponibilidad, confiabilidad,

rapidez y seguridad a sus clientes.

## **2. Bases Teóricas**

### **Fundamentación Teórica**

Sabino (1998), El propósito de definir las bases de diversas teorías y conceptos relevantes de la investigación es dar un enfoque coordinado y coherente que permita integrar a la investigación en un ámbito donde se cobre sentido el objeto de estudio.

Las consideraciones y el carácter teórico práctico del proceso de conocimiento son la base teórica en un conjunto de conocimientos con el fin de ofrecer una conceptualización adecuada de los términos utilizados.

A tal efecto, la investigación se orientó a partir de los modelos de gestión de red, red de gestión de telecomunicaciones, plataformas para gestión de red, técnicas basadas en modelo de gestión de red, entre otros.

#### **2.1 Sistema de Gestión de Redes (Network Management Systems)**

El autor Thornton (1998) señala, los proveedores de las redes están continuamente buscando hacia el futuro los sistemas de gestión de redes que poseerán la capacidad de configuraciones cambiantes proactivas de las redes y de enrutamiento de tráfico en tiempo real, con el fin de optimizar el ancho de banda del tráfico, y por lo tanto maximizar su margen de beneficio.

Según Chernand (1999) la interconexión de computadoras originó la creación de las LANs, permitiendo que varios usuarios ubicados en un área geográfica se conectaran a servidores de archivos, de aplicaciones, intercambiar mensajes, archivos, entre otros recursos.

Las interconexiones trajo la necesidad de resolver ciertos retos tecnológicos en área de conectividad, confiabilidad, administración de redes y flexibilidad para ser eficientes y efectivas las redes.

Los problemas que se presentan en las interconexiones se debe a:

- Dispositivos diferentes, por la gran variedad de marcas en el mercado en ocasiones las LANs tienen diferentes dispositivos
- Administraciones diferentes; la interconexión entre redes de distinto propósito se administraban y gestionaban de manera distinta
- Tecnologías de interconexión diferentes, diferentes topologías, diferentes tecnologías

Sin embargo, la principal barrera a la producción de verdaderos sistemas de gestión de redes en tiempo real es la tecnología, o la técnica, que permitirá la gran cantidad de datos de rendimiento de la red, son recogidos rutinariamente analizados, y que se puedan hacer los cambios en tiempo real.

Por la diversidad de tecnologías surgió la necesidad de implementar metodologías para la gestión de redes que fuera capaz de gestionar la configuración de sus componentes, la seguridad, las fallas, el desempeño.

El rápido cambio emergente de modelos de gestión de redes parece ofrecer una solución a los problemas que suministrará la base para la provisión de un sistema de gestión de redes en tiempo real en virtud de su posibilidad de estudiar rápidamente las grandes cantidades de datos.

El autor Thornton (1998) sigue señalando que hay dos barreras que excluyen normalmente el uso día a día de los sistemas de gestión.

La primera barrera es la falta de bases de conocimiento fiables y completamente suministrando información en cuanto a la acción correcta preventiva o paulatina, cuando una red presenta varias condiciones p.e. pérdida de celdas en un determinado conmutador.

La segunda barrera es la velocidad de procesado de la información.

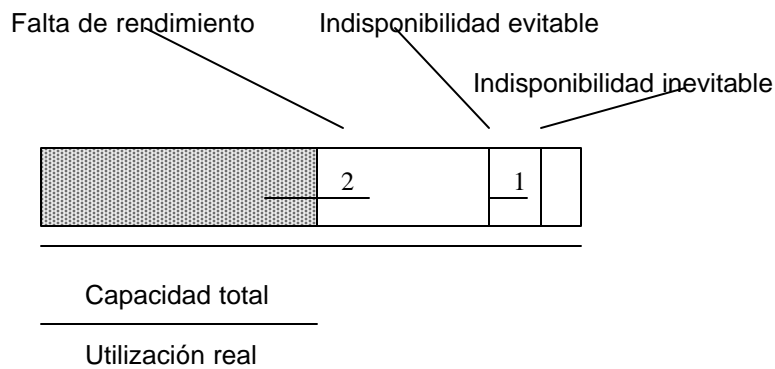
Una gran cantidad de información de rendimiento se recoge rutinariamente de las redes, normalmente 15 MB en 15 minutos en una red ATM, BURN (1996).

Con el fin de determinar los eventos que suceden en la red, un operador debe poder buscar rápidamente a través de grandes cantidades de información de rendimiento con el fin de hacer los cambios en la base de conocimiento de la red. La técnica usada para procesar los datos de rendimiento de la red necesitará ser tan rápida como sea posible.

La mayoría de los trabajos que se ha llevado a cabo hacia la meta final de suministrar sistemas de gestión de redes se ha focalizado en poder gestionar proactivamente una red usando el soporte de un sistema basado en el conocimiento, LAUFMANN (1997), p.e. superando la primera barrera,

se debe buscar superar la segunda, a saber estableciendo la técnica óptima que permite conseguir la gestión del sistema en verdadero tiempo real, determinando rápidamente la información a partir de las grandes cantidades de datos de rendimiento.

De acuerdo al objetivo de gestión se garantiza un nivel de servicio de acuerdo a un coste, según Figura 1.



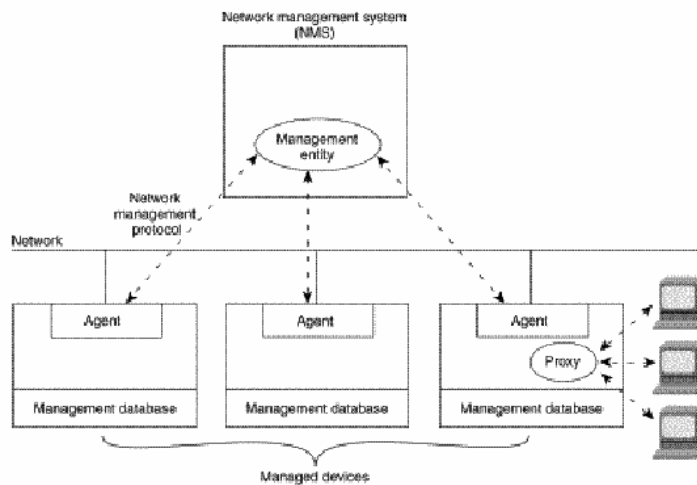
- 1) mejorar la disponibilidad
- 2) incrementar la efectividad

Figura 1 Objetivo de la Gestión  
Fuente: Thortonm (1998)

Las redes del mundo de las telecomunicaciones de hoy en día están basadas en diferentes tecnologías para transmitir datos, telefonía, videoconferencia y otros servicios, utilizan sistemas de gestión que actualmente implican altos costos y una complejidad extremadamente elevada en cuanto a la utilización y a la gestión, es por ello que se buscan

Modelos de gestión para sistemas heterogéneos de redes.

La gestión de redes basada en modelos , propuestas resuelve los problemas de gestión de los sistemas tradicionales dado que resulta evidente la necesidad de utilizar lenguajes que soporten la especificación de gestión, de seguridad, etc.



Arquitectura de gestión de red típica

Figura 2 Arquitectura de gestión de red  
Fuente: Thortonm (1998)

Con formato: Español (México)

## 2.2 Concepto de Gestión de Redes

ISO (Internacional Organization for Standardization) define la gestión de red como el conjunto de elementos de control y supervisión de los recursos que permiten que la comunicación tenga lugar sobre la red (Cisco, 2001).



Según Mendiola (1997), se entiende por gestión de redes al conjunto de actividades destinadas a garantizar los servicios que prestan las redes.

El uso de las redes en la actualidad han permitido relacionarse en el mundo de lo que llaman el uso de las nuevas tecnologías permitiendo a través de ellas comunicación a largas distancias con distintas empresas.

Las redes de datos y comunicaciones son la base de los sistemas de información y uno de los elementos críticos del engranaje corporativo.

La gestión de redes se convierte en un factor muy importante ya que contribuye a su mantenimiento, la resolución, prevención de incidencias y en definitiva a asegurar la máxima disponibilidad de la red de comunicación.

Mejora el rendimiento de la red detectando "Cuellos de botella", debido a saturación de tráfico en ciertos segmentos, o a un dimensional inadecuado de algún componente de la red.

La gestión de red permite la definición de alarmas que actúan en respuestas a eventos específicos (caídas de nodos, superación de umbrales error o tráfico), estas alarmas pueden asociarse a acciones que pueden automatizar parte de la gestión, facilitando en gran medida el trabajo del administrador de la red al permitir la rápida detección y resolución de las incidencias. (Tobal. 1999)

Los aspectos funcionales de la gestión de red indican:

- No existe funcionalidad común, depende de: tipo de red gestionada, tipo de equipos gestionados y objetivos específicos de la gestión de red

- A bajo nivel, todos los métodos se basan en: monitorización de la red (gestión de prestaciones, fallos, contabilidad, configuraciones) y Control de la red (gestión de configuraciones)

Thortonm (1998), señala un sistema de gestión de red es una colección de herramientas para monitorizar y controlar la red integrado en los siguientes sentidos:

- Una interfaz de operador única con un conjunto de órdenes potente, pero agradables para el usuario, para llevar a cabo la mayoría o todas las tareas de la gestión de red.

- Una cantidad mínima de equipamiento separado del sistema de gestión, esto es, la mayor parte del hardware y software requeridos para la gestión de red están incorporados en el equipamiento del usuario.

Las funciones de red se suelen agrupar en dos categorías:

**Supervisión de la red**, se considera una función de lectura y se encarga de observar y analizar el estado y comportamiento de la configuración de la red acompañado de sus componentes.

Para Cisco (1999), normalmente la supervisión se divide en tres áreas de diseño las cuales comprende:

- Acceso a la información supervisada, trata de cómo definir la información supervisada y como trasladarla desde un recursos a un gestor

- Diseño de los mecanismos de supervisión, trata de determinar la mejor forma de obtener la información de un recurso.

- Aplicaciones con la información supervisada, cómo se usa la información en las distintas áreas funcionales

La supervisión de red se dirige hacia tres áreas funcionales;

1. Supervisión de rendimiento: es imposible una gestión de red sin medir el rendimiento de la misma, las medidas a cabo son: Disponibilidad, Tiempo de respuesta, Eficiencia, Rendimiento, Utilización
2. Supervisión de fallos; pretende descubrir los fallos del sistema, identificarlos lo antes posible su causa y llevar a cabo las acciones para poder remediarlos
3. Supervisión de cuentas, lleva a cabo el control del uso de los distintos recursos de la red por parte de los usuarios. Algunos recursos sujetos a supervisión pueden ser: Facilidades de comunicación, hardware como estaciones de trabajo y servidores y servicios.

**Control de red;** se considera como una función de escritura y se encarga de alterar los parámetros de los distintos componentes de la configuración y hacer a cabo las acciones que se determinen

El control de la red, se encarga de la supervisión de red, modificación de parámetros y hacer que se lleven a cabo las acciones por parte del sistema final, intermedio y las subredes que constituyen la configuración que debe ser gestionada.

El control de red se divide en áreas funcionales como:

1. Configuración, trata de la inicialización, mantenimiento y apagado de los componentes individuales, los subsistemas digitales del sistema.

Algunas funciones que se debe llevar a cabo en la gestión son las siguientes

- Floración de la información de la configuración
- Establecer y modificar los valores de configuración
- Definir y finalizar operaciones de red
- Distribución de software
- Informar el estado de la configuración

2. Control de seguridad, se encarga de cumplir los siguientes requisitos

- Privacidad, la información sólo debe acceder aquel que este autorizado
- Integridad, las características del sistema sólo deben poder modificarse por personas autorizadas
- Disponibilidad, los recursos deben ser efectivos para uso de aquellos a los que se les permita

En conclusión la gestión de redes se divide en cinco áreas funcionales. En la siguiente figura se señala como es el flujo de información de gestión en una red.

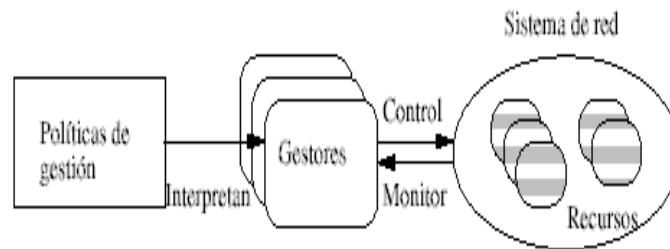


Figura 3 Flujo de información de gestión  
Fuente: Thortonm (1998)

El esquema de funcionamiento que sigue un sistema de gestión Figs.3 y 4, parte de las mediciones que se realizan de los recursos de la red a partir de los agentes que los mismos nodos contienen. Estos nodos, a través de sus agentes, proporcionan la información a los gestores de la red.

Los gestores, a partir de los parámetros definidos en sus políticas de gestión, actúan sobre la red mediante mensajes de control sobre los agentes de los nodos, optimizando el funcionamiento a través de cambios de configuración, etc.

Este control realizado sobre la red modifica las condiciones del tráfico y el ciclo se repite realizando nuevas mediciones sobre los recursos.

La información recabada por las funciones de gestión es útil para determinar si se están alcanzando los objetivos de desempeño de la red o si, con base en el desempeño se deben iniciar procedimientos de determinación de problemas. Trabajando con un gestor de rendimiento se podrá garantizar que se satisfagan las normativas de nivel de servicio de la red.

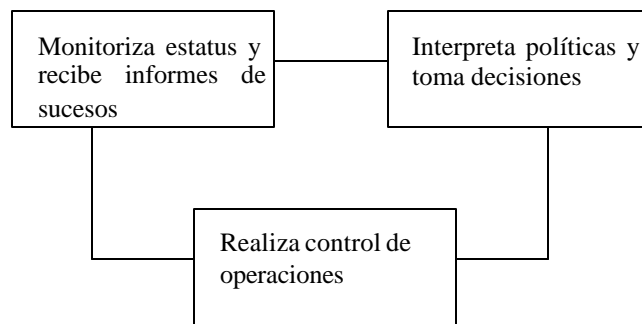


Figura 4 Bucle de actividades de gestión  
Fuente: Thortonm (1998)

Thortonm (1998) muestra el esquema de funcionamiento general de una plataforma de gestión en la siguiente figura 5. En este esquema, el usuario a través de una interfaz unificada tiene acceso a la información procedente de diversas aplicaciones de gestión (gestores).

Esto se requiere así puesto que la diversidad de elementos de red procedentes de diferentes fabricantes junto con la enormidad de funciones de gestión definidas por los estándares aconseja el procesado en paralelo.

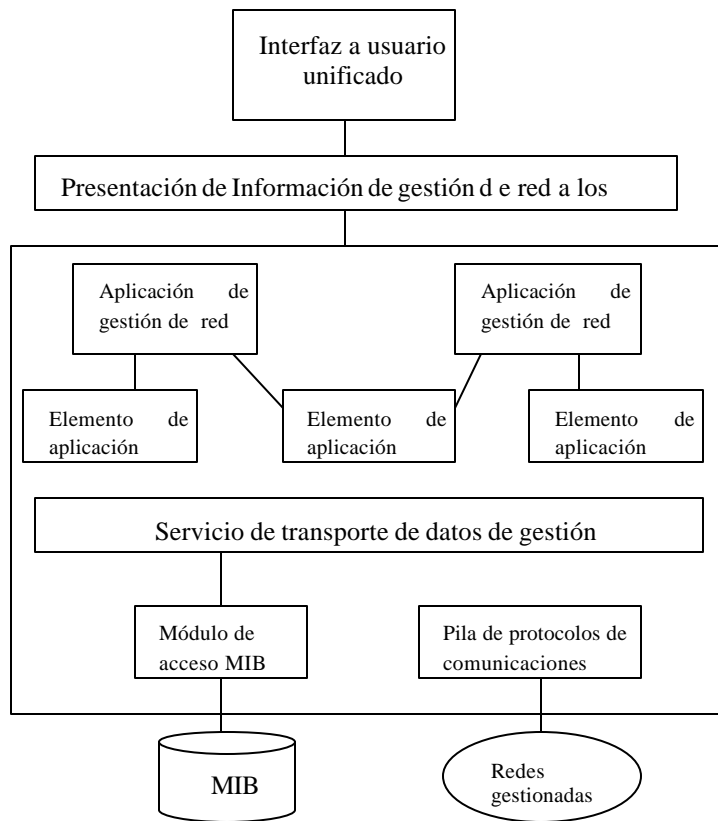


Figura 5 Modelo de referencia de un sistema de gestión de red  
Fuente: Thortonm (1998)

## **2.3 Áreas funcionales del modelo de Gestión de Redes**

Thortonm (1998), partiendo de definir la gestión de red como la planificación, la organización, la supervisión y el control de elementos de comunicaciones se garantiza un adecuado nivel de servicio, de acuerdo con un determinado coste, y según las recomendaciones de la OSI, recogidas por la ITU, definen las siguientes áreas funcionales para la gestión de red.

### **2.3.1 Gestión de fallas o Supervisión de fallos:**

Según Sherman (1997) el objetivo de la gestión de fallas es manejar las condiciones de error que hacen que los usuarios pierdan toda o parte de las funcionalidad de un recurso de la red.

Esta gestión establece la generación de notificaciones específicas de error (alarmas), el registro de las notificaciones de error y la verificación de los recursos de red para trazar e identificar fallas. También el conjunto de facilidades que permiten la detección, aislamiento y corrección de una operación anormal.

Una falla puede ser originada por:

- La degradación del desempeño de algún componente de la red, sobrepasando el umbral establecido.
- Por la presencia de algún evento controlado o inesperado
- Por la intervención planificada o inesperada de algún individuo.

De acuerdo a Mendiola (1997) la gestión de fallas se lleva a cabo en los siguientes pasos:

**1) Detectar o recibir notificaciones del problema;** lo ideal dentro del sistema de gestión de redes es que exista un mecanismo que permita detectar la presencia de algún problema antes que el usuario en todo caso, ante la complejidad de una infraestructura de redes y las limitaciones de los administradores de redes se debe implementar un proceso que permita al usuario notificar la presencia de una posible falla.

**2) Registrar el problema y posteriormente su solución;** El problema detectado por el administrador de red o notificado por el usuario debe ser registrado y almacenado en una base de datos de conocimientos que adicionalmente contendrá información relacionada con los pasos y detalles de la solución implementada para dicho problema.

En la medida que esta base de conocimientos va enriqueciendo con las vivencias y experiencias surgidas ante cada problema en esa medida la capacidad para gestionar las fallas más eficientemente se va incrementando.

**3) Diagnosticar y valorar el problema;** para diagnosticar y valorar el problema se debe resolver las siguientes interrogantes:

- ¿Cuáles son los componentes físicos y/o lógicos afectados directamente?
- ¿Cómo se manifiesta el problema?
- ¿Quiénes son los usuarios afectados?
- ¿Cuáles son las posibles causas del problema y orden de prioridad?



- ¿Qué componentes afecta indirectamente?
- ¿Cuál es el nivel o magnitud de la falla?
- ¿Qué recursos son necesarios para implementar la solución?
- ¿Cuál es el tiempo estimado de solución de la falla?
- ¿Es posible implementar una solución temporal alternativa?
- ¿Hay algún problema similar registrado en la base de datos?

**4) Resolver o aislar el problema:** Una vez culminado el diagnóstico de la falla, consiste en la implementación de las acciones correctivas para cada una de las posibles causas, hasta dar con la solución definitiva.

Los gestores de fallos tienen un Event Browser que filtra los eventos de acuerdo a una combinación configurable del tipo de evento, origen, cadena de mensaje, periodo de tiempo recibido e importancia.

El gestor agrupa los eventos en categorías basadas en la importancia y actúa sobre ellas por medio de acciones que el usuario puede definir, pueden realizarse operaciones de búsqueda, ordenación y filtrado.

Por ejemplo, puede avisar a alguien cuando recibe un determinado tipo de interrupción SNMP, este componente proporciona monitorización en tiempo real de elementos de la red y resolución de problemas.

Los contadores de estadísticas en tiempo real pueden extraerse y convertirse en gráficos dinámicos utilizando la consulta SNMP, entidades como son los puertos pueden configurarse mediante ventanas de fácil manejo, las visualizaciones de los paneles frontales y posteriores de los elementos de la red muestran gráficamente el estado actual de las tarjetas y

los subsistemas

El objetivo de la gestión de fallos es mantener dinámicamente el nivel de servicio evaluado

- Gestión proactiva: evitar fallos detectando tendencias hacia fallos, caracterización de tendencias a determinación de umbrales de ciertos parámetros y con la monitorización detectar los umbrales o programar notificaciones automáticas
- Gestión reactiva, asumir que existen fallos inevitables detectando lo antes posible el fallo y monitorizando periódicamente (no es posibles notificaciones).

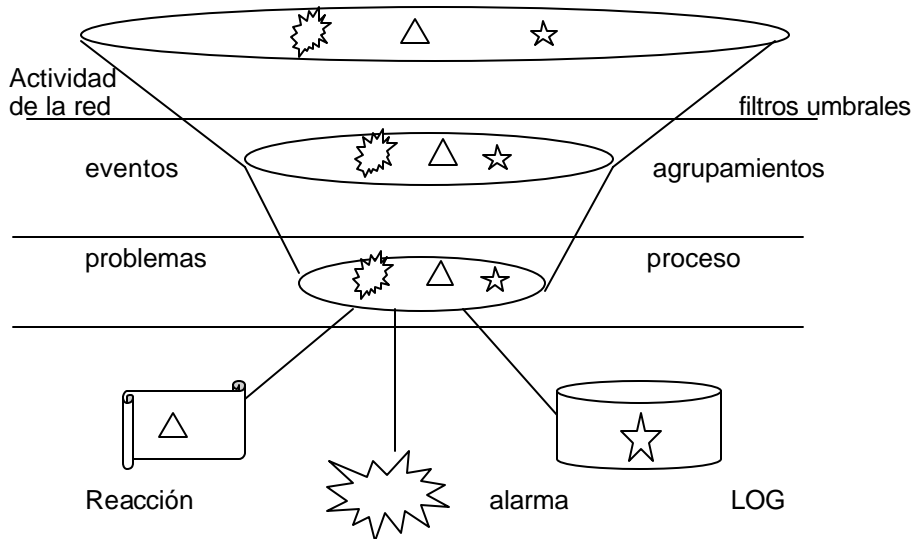


Figura 6 Gestión de red: fallos  
Fuente: Thortonm (1998)

En la gestión de fallas se evalúa

- Gestión del ciclo de vida de incidencias en la que se considera:

Detección de problema: Alarma de usuarios, Alarma de herramientas

Determinación del problema: La información sobre el fallo puede no ser fiable en cuanto a la fuente de fallo

Diagnóstico del problema, procedimiento

Resolución del problema

Por operadores de help-desk (80-85%)

Por operadores técnicos (5-10%)

Por especialistas en comunicaciones (2-5%)

Por especialista en aplicaciones (1-3%)

Por fabricante (1-2%)

- Gestión de pruebas preventivas, pruebas por conectividad, integridad de datos, integridad de protocolos, saturación de datos, saturación de conexiones, tiempo de repuestas, bucle y diagnósticos.

### **2.3.2 Gestión de configuración**

Se distribuye en actividades de inicialización, instalación, abastecimiento, permite la colección de información de configuración y estado en demanda, proporcionando facilidades de inventario,

Soporta el anuncio de cambios de configuración a través de notificaciones relevantes, facilidades que permiten controlar, identificar, recoger y proporcionar datos a objetos gestionados, con el propósito de

asistir a operar servicios de interconexión.

Para Cisco (1999), el objetivo de la gestión de configuración es controlar la información que describe las características físicas y lógicas de los recursos de la red, así como las relaciones entre dichos recursos.

Cada componente de la red tiene una amplia gama de información respecto a su marca, modelo, capacidad, versión, velocidad, seriales, entre otros, que son almacenados en una base de datos controlada por el módulo de gestión de la configuración.

Las funciones que ofrece la configuración son:

- Obtener inventario de los recursos o componentes de la red, tanto físicos como lógicos (servidores, enrutadores, concentradores)
- Obtener los valores de las variables de cada uno de los componentes (memoria RAM, disco duro, CPU, tarjeta de red, versión del sistema operativo).
- Obtener un datagrama de interconexión de los componentes
- Detectar cambios inesperados en características de los componentes físicos y lógicos
- Detectar cambios inesperados de interconexión de los componentes

El gestor cubre automáticamente elementos de la red y muestra un mapa topológico gráfico que soporta bien visualizaciones autónomas de mapas topológicos o bien mapas Hp OpenView.

Las pantallas multicolor se actualizan a tiempo real, en respuestas a los eventos que estén ocurriendo en la red.

El interfaz que muestra la topología soporta arrastre interactivo, selecciones múltiples, zoom de acercamiento/alejamiento, agrupaciones de nodos submapas entre otros.

En la gestión está:

- Gestión de SLAs (Service Level Agreements). Contrato entre cliente/proveedor o entre proveedores sobre servicios a proporcionar y calidades asociadas.

Identificación de las partes contractuales,

Identificación del trabajo a realizar,

Objetivos de niveles de servicio,

Niveles de servicios proporcionados,

Multas por incumplimiento,

Fecha de caducidad,

Cláusulas de renegociación y

Prestaciones actuales proporcionadas.

- Gestión de Incidencias, TTS (Trouble ticket systems),

Fecha y hora de informe de incidencia,

Resolución de incidencia,

Usuario/localización, equipo afectado, descripción del problema, estado, operador(es), grado de severidad, historial de incidencia, comentarios.

- Gestión de proveedores externos (órdenes de procesamiento / aprovisionamiento) y Gestión de cambios (reconfiguraciones)

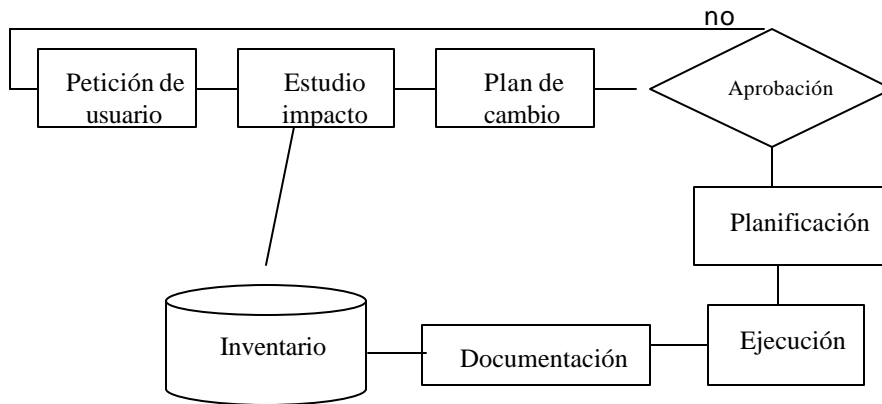


Figura 7 Gestión de red: configuración  
Fuente: Thortonm (1998)

### 2.3.3 Gestión de contabilidad

Consiste en actividades de recolección de información de contabilidad y su procesamiento para propósitos de cobranza y facturación.

Estas actividades establecen un límite contable para que un conjunto de costos se combinen con recursos múltiples y se utilicen en un contexto de servicio, facilidades que permiten establecer cargos por el uso de determinados objetos e identificar costes por el uso de éstos.

Para Computer Associates (1999) el objetivo de la gestión es medir los parámetros de la utilización de la red, para el uso de la misma por parte de los individuos o los grupos y pueda regularse de manera adecuada.

Con dicha regulación se reducen los problemas de la red ya que los recursos de las redes pueden dividirse en cantidades iguales dependiendo

de la capacidad de los recursos y se hace más justo el acceso a la red para todos los usuarios.

Por otro lado Cisco (1999) afirma que la gestión de contabilidad controla los cambios en la red, los cambios en las variables de cada uno de sus componentes, donde estos son originados principalmente por las siguientes razones:

- Requerimiento del usuario, se debe a las actualizaciones en hardware y software, instalaciones de nuevas aplicaciones y/o servicios solicitados por los usuarios de la red, debido a las nuevas necesidades de la red.
- Para evitar un problema que se ejecuta cuando alguna de las variables de componentes de la red llega al valor del umbral establecido en los parámetros de desempeño
- Para eliminar un problema que son necesarios para enfrentar cambios inesperados producidos como resultado de la falla de hardware, software u otro componente.
- Para mejorar el desempeño que se aplica cuando alguna de las variables de componentes mantiene sus valores cerca del umbral establecido en los parámetros de desempeño.

La gestión de la contabilidad evita, minimiza y/o elimina los problemas de la red promoviendo y administrando en forma ordenada los cambios en sus componentes.

La gestión abarca los siguientes pasos:

- Medir la utilización de todos los recursos importantes de la red
- Analizar los resultados para determinar los patrones de uso actuales
- Establecer cuotas de uso
- Efectuar subsecuencias mediciones y correcciones hasta establecer la utilización óptima y justa de los recursos

#### **2.3.4. Gestión de desempeño**

Proporciona información en forma ordenada para determinar la carga del sistema y de la red bajo condiciones naturales y artificiales, proporcionando estadísticas, permitiendo actividades de planeación de configuración.

De acuerdo a Cisco (1999), esta gestión permite medir y hacer disponible diferentes aspectos del desempeño de la red para que el desempeño total de la interred se pueda mantener a un nivel aceptable. Entre las actividades que se incluyen en una gestión de desempeño se encuentra el monitoreo de los tiempos de respuesta de los sistemas (hardware y Software), la medición de los recursos disponibles, rastreo y control del desempeño de la red.

La información recabada por las funciones de gestión de desempeño es útil para determinar si se están alcanzando los objetivos de la red o si con base en el desempeño se deben iniciar procedimientos de determinación de problemas.

La gestión de desempeño abarca los siguientes pasos:



- Establecer cuales son los componentes físicos y lógicos de interés para los administradores de la red, ejemplo un servidor de red.
- Establecer las variables de desempeño para cada uno de los componentes seleccionados, p.e. capacidad de memoria RAM, de disco duro
  - Reunir los datos de funcionamiento de los componentes seleccionados, registrando los valores para cada una de sus variables
  - Analizar los datos para determinar los niveles normales de capacidad, funcionamiento, operación, etc., y establecer así los parámetros normales de comportamiento.
- Determinar el umbral de desempeño máximo permitido para cada una de las variables y establecer los parámetros de desempeño
  - Implementar mecanismos de alertas que deben activarse cuando los parámetros llegan a los valores umbrales como mensajes emergentes, registro de eventos, avisos sonoros. Monitorear las alertas.

Cada uno de los pasos que se acaban de describir son parte de un sistema de gestión de desempeño reactivo, es decir cuando el desempeño de la red se hace inaceptable por haberse excedido un valor umbral definido por administrador de red el sistema reacciona enviando un mensaje. La gestión de desempeño puede implementarse bajo un sistema proactivo a través de la simulación de eventos, p.e. se podría usar una simulación de la red para hacer una proyección de cómo se verán afectados los parámetros de desempeño por el crecimiento de la red.

Se puede gestionar el rendimiento de la red utilizando un software que facilita la comprensión del funcionamiento interno de la red de manera que pueda resolver problemas con rapidez y optimizar el rendimiento.

La gestión de rendimiento permite definir, monitorear y optimizar los niveles de servicio, hacer el uso más eficiente posible de los recursos de la red, diagnosticar y resolver problemas de rendimiento, ajustar la red, y planificar cambios.

Cuando se ofrece un modelo exacto del transporte de encaminamiento y de flujo a través de dispositivos, puede analizar interacciones entre pérdidas de tráfico, topologías, parámetros de encaminamiento, configuraciones de router, etc.

Al trabajar con un gestor de rendimiento se podrá garantizar que se satisfacen las normativas de nivel de servicio, se resuelven problemas de la red, se reduce la optimización de los recursos, la empresa estará lista para enfrentarse a futuros planes de migración de equipos, protocolo y requisitos de rendimiento para aplicaciones.

Mendiola (1997) dice que el gestor de rendimiento ofrece una representación gráfica de la red, se logra recogiendo datos de configuraciones generando rápidamente las bases de topología multiprotocolo, rendimiento, tráfico, los resultados permite al administrador tomar decisiones fundamentales, eficaces para mejorar el rendimiento general y optimizar las cargas de tráfico.

### **2.3.5 Gestión de seguridad**

Está relacionada con 2 aspectos de la seguridad del sistema: aspectos que son esenciales en la gestión de red y que permiten proteger los objetos gestionados.

La gestión de seguridad requiere la habilidad para supervisar, controlar la disponibilidad de facilidades de seguridad, reportar amenazas y rupturas en la seguridad.

La seguridad de la gestión requiere la habilidad para autenticar usuarios y aplicaciones de gestión, con el fin de garantizar la confidencialidad e integridad de intercambios de operaciones de gestión y prevenir accesos no autorizados a la información.

Existen varias formas de abordar la seguridad de un sistema, un punto de vista es entenderla como una forma de prevenir futuras pérdidas una manera de gestionar los riesgos relacionados con la tecnología. Otros consideran que es algo innecesario para evitar que usuarios maliciosos entre al sistema.

La seguridad en sistemas de ordenadores es la protección de la integridad, disponibilidad y si es necesaria la confidencialidad de información y recursos que se usan para: Entrada, almacenamiento, proceso y comunicación de los mismos (Mendiola: 1998, p.51)

Existe una serie de compromisos básicos sobre la seguridad de sistemas de red:

- No dificultar las labores de los usuarios; el propósito es la protección de recursos considerados importantes dentro de la organización donde el sistema de seguridad está activo.

- La seguridad es responsabilidad de la gestión de riesgos; una de las responsabilidades en la gestión de un sistema es el control de riesgo, control de toda la información. Se debe conseguir que la información este disponible, sea correcta y esté completa.

- Se deben especificar claramente las responsabilidades en seguridad, es necesario que se haga de forma precisa los grupos a los que se le asigna esta tarea suelen ser los gestores de seguridad, operadores del sistema, gestores de aplicaciones, el encargado de la seguridad física, la oficina de recuperación de desastres, los usuarios y los encargados de los informes de supervisión.

- La seguridad requiere una estructura clara, la eficiencia de la seguridad precisa que distintos grupos, áreas dentro y fuera de la organización colaboren, la arquitectura o programa de seguridad se suele dividir en bloques que denominan controles agrupados en controles técnicos, de operaciones y de servicio. Para que sea la seguridad óptima hay que conocer esta estructuración y la interacción entre cada uno de ellos.

- La protección del sistema debe tener un coste soportable, hay que tener en cuenta que una inversión en seguridad puede suponer disminuir el número de pérdidas debido a fallos del sistema, o por manipulación fraudulenta de los recursos. Los beneficios de la seguridad no son sólo

monetarios, evita hackers así como otros elementos hostiles a nuestro sistema ayudando a ofrecer una buena imagen hacia el público.

Según Mendiola (1997), la labor principal en seguridad es el aislamiento de los actos no deseables y la prevención de aquellos que no se hayan considerado, de forma que si se producen hagan el menor daño posible, entre las distintas actividades que debe llevar a cabo se puede detectar las siguientes:

- Identificación de los usuarios; existe varias técnicas entre las que se encuentran contraseñas (password) o sistemas más sofisticados como reconocimiento de habla, huella dactilar o la retina del ojo.
- Detección de intrusos en la red; hay que detectar y actuar sobre cualquier acceso no autorizado a nuestro sistema, el objetivo es la detección de intrusos en tiempo real.
- Análisis de riesgo; intenta cuantificar los beneficios obtenidos con la protección contra amenazas de seguridad, el riesgo es función de la frecuencia con la que se producen dichas amenazas, vulnerabilidad de la protección contra las mismas y las pérdidas potenciales que se produjesen en el caso de que se diese una.
- Clasificación apropiada de los datos; en la gestión de seguridad llegan gran cantidad de datos provenientes de los distintos programas de control generados a partir de la actuaciones que llevan a cabo los usuarios en el sistema; es importante para una buena supervisión en la seguridad se debe clasificar los datos convenientemente de tal forma que se ahorre

tiempo en su análisis.

- Control de las nuevas aplicaciones; cuando se instala una nueva aplicación hay que comprobar que no introduzcan nuevas brechas de seguridad especialmente si se ejecuta con permisos de administrador.

- Análisis de los accesos de los usuarios; es necesario tener un control para poder detectar intentos de acceso no autorizados

La gestión de seguridad proporciona continuidad de la red y sus componentes en los distintos aspectos de seguridad:

- acceso a las redes, a los sistemas, a la información en tránsito en las funciones de la gestión de seguridad esta:

- definición de análisis de riesgos y política de seguridad
- implantación de servicios de seguridad e infraestructura asociada
- definición de alarmas registros e informes de seguridad.

## **2.4 Arquitectura de la Gestión de Redes**

Para Computer Associates (1999) y Cisco (1999) la mayoría de las arquitecturas de gestión de redes utilizan el mismo conjunto de relaciones y estructura básica.

- Gestores de redes,
- Consola de administración,
- Agentes,
- Dispositivos Administrados,
- Base de datos de administración,

- Protocolo de gestión

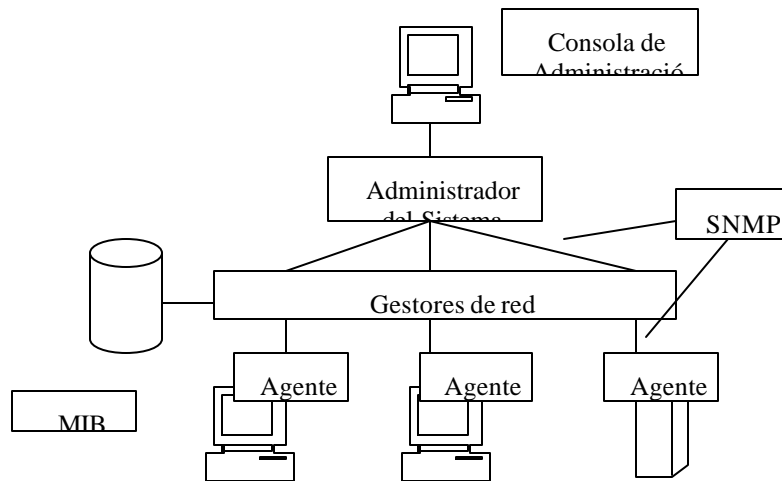


Figura 8 Arquitectura de la gestión de redes  
Fuente: Cisco (1999)

## 2.5 Elementos de un sistema de Gestión de Redes

Thortonm (1998), los elementos activos de la red proporcionan una realimentación regular de información de estado al centro de control de red.

Un sistema de gestión de red tiene los siguientes elementos claves:

- Estación de gestión o gestor
- Agente
- Base de información de red
- Protocolo de gestión de red

**La estación de gestión de red** es un dispositivo autónomo pero puede ser implementado en un sistema compartido, la gestión de servicio

sirve como interfaz entre el gestor de red humano y el sistema de gestión de red. La estación de gestión tendrá como mínimo:

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

- Una interfaz a través de la cual el gestor de red puede monitorizar y controlar la red.

- La capacidad de trasladar los requerimientos del gestor de red a la monitorización y control de red de los elementos.

- Una base de datos de información de gestión de red extraída de las bases de datos de todas las entidades gestionadas en la red.

Es un nodo que activamente participa en la administración de una red, solicita e interpreta datos acerca de dispositivos de red y tráfico, típicamente interactúa con los usuarios para llevar a cabo sus intenciones.

Un administrador puede provocar cambios en un agente alternando el valor de una variable en el nodo agente, los administradores o managers son frecuente implementados como aplicaciones de red. (Computer Associates. 1999).

Según Cisco (1999) es localizado en el host principal de la red, su principal función es encuestar a los agentes acerca de cierta información solicitada.

El gestor es la parte de la aplicación que emite las directivas de operaciones de gestión, recibe notificaciones y respuestas. Este se



implementa en una estación de gestión en la cual se debe disponer de la MIB del dispositivo en gestión y una interfaz de usuario.

**Agente**, las plataformas claves como los computadores, puentes, dispositivos de encaminamiento y concentradores pueden ser equipados con software de agente área que puedan ser gestionados desde la estación de gestión.

El agente tiene la función de responder a las directivas enviadas por el gestor y lo realiza accedendo a la MIB para manipular los objetos involucrados en la operación, se encuentra ubicado en el dispositivo de telecomunicaciones gestionado.

De acuerdo con Mendiola (1997) un agente es un software que reside en un nodo de red y es responsable de comunicarse con los managers o administradores considerando el nodo, el nodo es representado como un objeto teniendo varios campos o variables que están definidos en el MIB apropiado.

El agente tiene dos propósitos:

- Responder a las solicitudes de los manegers, suministrando o cambiando los valores de las variables de los objetos según se solicitaron
- Generar traps para alertar a los managers de los eventos notables que ocurren en el nodo, tales como una falla en un componente.

El agente corre en cada nodo de la red, colecciona información de red y terminal como esté especificado en el MIB. El manager se comunica con el agente por mensajes del protocolo de gestión los cuales están en forma de

solicitudes. Los managers no necesitan saber ningún detalle interno acerca del objeto administrado por el agente (Cisco 1999).

Además, un agente puede servir solicitudes de muchos administradores, el agente no necesita saber el contenido de la solicitud o la estructura del manager que está haciendo la solicitud, el agente valida la solicitud, los servicios y entra en el estado pasivo – esperando la siguiente solicitud.

**Base de Información de gestión (MIB. Management Information Base),:** El medio por el cual se pueden gestionar los recursos de una red es representando estos recursos como objetos. La colección de objetos se conoce como base de información de gestión (MIB. Management Information Base), el cual funciona como una colección de puntos de accesos al agente por parte de la estación de gestión. La estación de gestión lleva a cabo la función de monitorización mediante el acceso a los valores de los objetos MIB.

La MIB es el conjunto de objetos gestionados (el concepto de objeto es diferente al empleado en la programación orientada a objetos) que representan a los recursos de la red que permiten algún tipo de gestión en una forma abstracta. La MIB se encuentra ubicada en el dispositivo de telecomunicaciones, y una referencia de ésta es necesaria en el gestor.

Las características de los componentes de la red son representadas mediante objetos. Cada objeto es en esencia una variable de datos que representa un aspecto del agente en cuestión (Computer Associates 1999).

Las estaciones de gestión ejecuta las funciones de monitoreo recuperando el valor de los objetos MIB, además la estación de gestión puede ejecutar una acción que se ejecute en un agente, o puede cambiar la configuración original de un agente modificando el valor de variables específicas.

**El protocolo** es el conjunto de especificaciones y convenciones que gobiernan la interacción de procesos y elementos dentro de un sistema de gestión.

En la actualidad SNMP (Simple Network Management Protocol), forma parte del modelo de gestión de internet, y CMIP (Common Management Information protocol), es parte del modelo de gestión OSI son los protocolos predominantes.

Para Cisco (1997), Stalling (1997) es el encargado de enlazar la estación de gestión y los agentes.

El protocolo utilizando para las gestiones de redes TCP/IP es el SNMP, para redes en OSI se usa el CMIP.

Por otro lado, según Soriano (2000), La gestión de un entorno de telecomunicaciones es una aplicación de procesamiento de información, en la cual intervienen elementos fundamentales como son:

El gestor, el agente, el protocolo de gestión, y la base de información de gestión (MIB, Management Information Base), los cuales interactúan entre sí empleando el modelo gestor-agente como se muestra en la siguiente figura 9

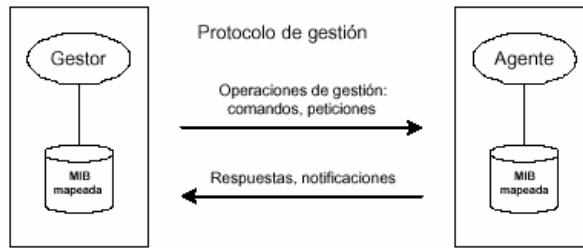


Figura 1. Modelo gestor-agente

Figura 9. Modelo Gestor - Agente  
Fuente: Soriano (2000)

Los Sistemas de Gestión permiten reducir los costes de explotación mediante la centralización de la operación y mantenimiento de las distintas redes y de los servicios que se apoyan en las mismas, la reducción de los tiempos de formación de los operadores y la simplificación en el manejo de la creciente complejidad de la tecnología. Así mismo, contribuyen a rentabilizar al máximo las inversiones realizadas en infraestructuras de red.

Burn (1996), A partir de medidas estadísticas de tráfico, se puede analizar con detalle el uso real de las infraestructuras, y poner de manifiesto tanto aquellas con capacidad ociosa como las que presentan cuellos de botella que suponen pérdida de oportunidad de ingresos y deterioro de imagen ante los clientes.

Por otro lado, Góngora (1998), los Sistemas de Gestión permiten acortar, en buena medida, los plazos de provisión de nuevos servicios, gracias a la automatización de los procesos administrativos que intervienen en el alta y/o baja de los mismos y a la posibilidad de activar dichos servicios

en los elementos de la red con seguridad e inmediatez.

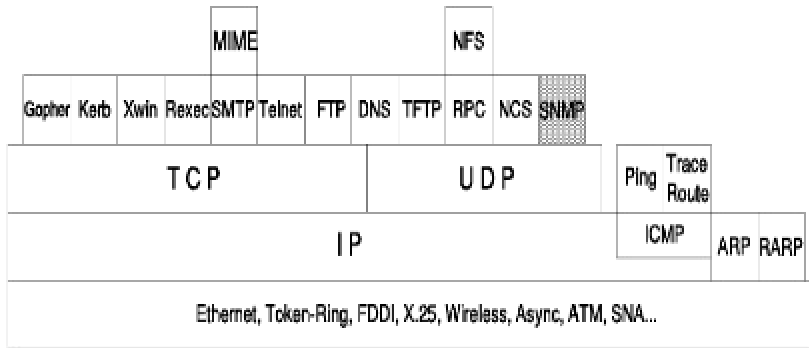


Figura 10. Gestión de Red  
Fuente: Soriano (2000)

## 2.6. Importancia de la gestión de redes

Según Soriano (2000), expresa lo siguiente; Las redes de comunicaciones han evolucionado con el paso del tiempo ante la necesidad de satisfacer las demandas de los diferentes servicios de telecomunicaciones, que día a día necesitan un mayor ancho de banda y una mejor calidad de servicio para las nuevas aplicaciones que se han venido desarrollando hasta la actualidad.

La tecnología de redes ha incrementado su complejidad generándose la necesidad de contar con una mejor administración de los recursos de estos sistemas, lo cual ha favorecido la evolución conjunta de la gestión de redes.

La gestión de redes tiene como propósito la utilización y coordinación de los recursos para planificar, organizar, mantener, supervisar, evaluar, y controlar los elementos de las redes de comunicaciones para adaptarse a la calidad de servicio necesaria a un determinado costo.

Su campo de aplicación es amplio y de gran importancia dadas las características tecnológicas que poseen los sistemas de telecomunicaciones y los servicios que ofrecen, mantiene un cierto grado de complejidad al interactuar con sistemas heterogéneos que involucran diversos fabricantes con productos eminentemente propietarios, así como productos apegados a estándares en forma total o parcial.

Gervás (2002), La gestión de red juega un papel importante en el buen funcionamiento de las redes y se hace imprescindible su aplicación por las siguientes razones:

- Los sistemas de información son vitales y están soportados sobre redes
- La información manejada tiende a ser cada día mayor más dispersa
- Las nuevas tecnologías de red requieren de una gestión cada vez más especializada, que le permita el empleo eficiente de sus recursos de telecomunicaciones.

El adecuado empleo de las tecnologías de gestión de red permite mejorar la eficiencia, disponibilidad y el rendimiento de las redes, aumentar la relación calidad/costo en el diseño de las redes, así como aumentar la satisfacción de los usuarios por el servicio de red proporcionado.

Góngora (1998), Para lograr una gestión de red eficiente es necesario contar con un sistema integrado de gestión que conlleve a mejorar la eficiencia en la operación de la red.

Un sistema integrado de gestión de red debe contar con los siguientes elementos: Recursos humanos, métodos de trabajo y desarrollo tecnológico.

La gestión de redes es una necesidad primordial en las organizaciones.

De la gestión de red se espera que:

- Asegure un servicio casi continuo a los usuarios finales descrito por la disponibilidad y velocidad de respuesta, sin que se vean afectados por las actualizaciones tecnológicas en la red.

- Incremente el desempeño de una red con el empleo de la mejor tecnología de redes, recursos humanos adecuados, métodos de trabajo probados y herramientas integradas que automaticen las operaciones de gestión.

- Controle los costos dedicados a las comunicaciones y a la seguridad de la información.

Millán (2000), La gestión de las redes representa ya un aspecto de importancia fundamental en el mundo de las telecomunicaciones, sea por los operadores públicos o privados, sea por las empresas que utilizan redes locales y geográficas.

A fin de efectuar las adecuadas elecciones a nivel proyectivo, es fundamental tener buenos conocimientos sobre los modelos estándares

utilizados en los sistemas de gestión y sobre las nuevas tecnologías habilitadoras (CORBA, Java, Web).

Reyes (2000), Los administradores de red no sólo deben gestionar una infraestructura cada vez más compleja, sino también debe cumplir objetivos específicos sobre el nivel de servicio ofrecido.

Los administradores de grandes redes distribuidos necesitan una herramienta de gestión que les permita analizar mediante una interfaz gráfica e intuitiva la red y sus dispositivos.

Estos administradores requieren una alternativa de bajo coste que les permita acceder de forma remota y segura en su entorno de gestión de red.

Al momento de planificar una red hay que tomar en consideración el aspecto de seguridad para efectuar una administración en forma efectiva.

Reyes (2000), El control de situaciones conflictivas en el tráfico de red y del rendimiento alcanzado en su utilización son dos funciones primordiales:

- Cubrir la infraestructura de comunicación de datos LANs basados en tecnologías como Ethernet, Token Ring, ATM, FDI, al mismo tiempo ofrece soluciones para redes conmutadas.

Cabe destacar que un gestor de redes permite la planificación, organización, supervisor y control de elementos de comunicación para garantizar el servicio de acuerdo a un coste.



## 2.7 Motivación de la gestión de red

- Control de activos estratégicos, Control de complejidad, Mejorar servicio, Equilibrar necesidades, Reducir indisponibilidad, Control de costes.

Race (1994), La pirámide de la gestión señalada en la figura 11

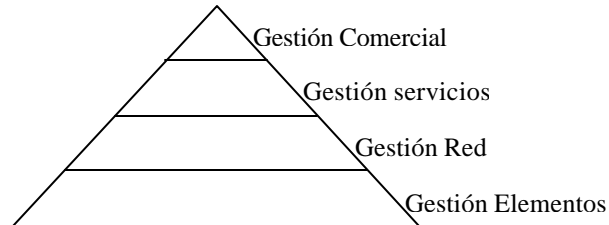


Figura 11 Ubicación de sistemas de gestión actuales  
Fuente: Foro CITEI/CCP.I.(1998)

La figura 12 indica los sistemas reales no operan a todos los niveles, el éxito económico de la gestión se cuantifica en el vértice. Los niveles inferiores son facilitadores, el nivel N no puede funcionar si el N- 1 no opera satisfactoriamente. .

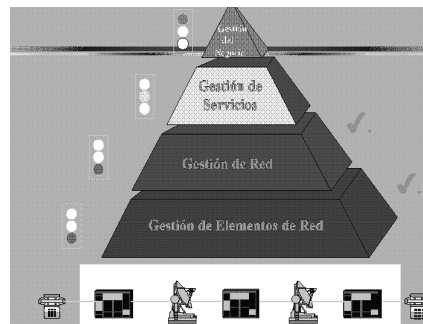


Figura 12 Estado Actual de la implementación de red de Gestión  
Fuente: Foro CITEI/CCP.I.(1998)

## **2.8 Definición y Desarrollo de Técnicas basadas en el Conocimiento para la Aplicación de Gestión de Redes y Servicios: Gestión Semántica.**

Salavert (1998) Ante la heterogeneidad de modelos de Gestión de Red Integrada (SNMP, OSI, DMI, WBEM), y teniendo en cuenta que es muy probable el hecho de que en un mismo dominio de gestión necesite aplicar múltiples modelos simultáneamente.

Ha sido necesario tradicionalmente establecer mecanismos que posibiliten la interoperabilidad entre los distintos dominios implicados, siendo ésta posible si se consigue definir un conjunto de reglas que traduzcan el protocolo de comunicaciones y modelo de información de gestión.

Sin embargo, un aspecto que todavía no tiene fácil solución se presenta cuando en dos dominios distintos de gestión se representa un mismo concepto de distinta manera: una traducción meramente sintáctica del modelo de información de gestión origen no proporciona el concepto existente en el modelo destino. Se hace por tanto necesaria una traducción semántica que haga corresponder directamente los conceptos de ambos dominios.

La aplicación de gestión de red y servicios tiene como objetivo proponer soluciones que permitan perfeccionar la interoperabilidad en lo que se refiere a los modelos de información de gestión, ahondando en las posibilidades que existen para llevar a cabo la traducción semántica. Para ello, la técnica de representación del conocimiento conocida como ontología

es una de las respuestas más adecuadas a este problema, dado que proporciona las construcciones necesarias para añadir semántica a la información representada.

Salavert (1998), en su investigación señala que la aplicación de esta tecnología al campo de la gestión de red puede ser la clave que permita realizar una gestión realmente integrada e inteligente de los diversos recursos que posee una empresa, que normalmente pertenecen a distintos dominios de gestión:

Conmutadores y encaminadores gestionados con SNMP, Ordenadores con DMI o servicios de comercio electrónico accesibles con una interfaz CORBA se gestionarían de manera unificada desde un gestor con un único modelo de información. El empleo de ontologías puede permitir la definición de reglas que definan el comportamiento del gestor, de forma añadida al modelo de información de gestión que se haya especificado, definiendo así toda la información relativa a la gestión de manera unificada.

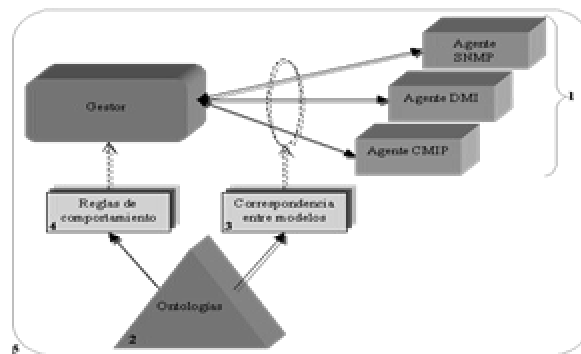


Figura 13 Modelo de gestión de red y servicio  
Fuente: Salavert (1998)

La figura anterior señala los siguientes parámetros

- Formalizar los distintos modelos de información de gestión existentes, capturando aquellas características que debe poseer un modelo de información de gestión de red para que permita trabajar con dicha información a un nivel semántico, basándose en las posibilidades que ofrecen las ontologías.

- Definir una ontología para la gestión de red proporcionará la base de información de gestión necesaria para la gestión de redes, sistemas, servicios y aplicaciones, modelará y declarará el comportamiento de un gestor de red.

- Establecer correspondencias entre esta ontología y los modelos de gestión existentes. Esto permitirá a una entidad gestora obtener información de los distintos dominios gestionados desde un punto de vista de información único.

- Aplicar las reglas de comportamiento definidas a un sistema inteligente de gestión. Esto permitiría comprobar la posibilidad de integrar la totalidad de la información que necesita un gestor en una misma ontología.

- Experimentar un caso de gestión integrada utilizando las correspondencias previamente definidas para la gestión de un servicio.

Esto permitirá validar el trabajo realizado, aplicándolo a un caso en el que intervienen varios dominios de gestión:

SNMP para la red de datos, WBEM o DMI para el servidor y CORBA para el servicio electrónico.

## 2.9 Gestión de Telecomunicaciones

Millán (2000), Tradicionalmente, las redes de telecomunicaciones tienen separados el nivel de gestión del nivel de comunicación; existen diferentes infraestructuras para la entrega de los datos del usuario y la entrega de la información, comandos intercambiados entre las entidades de gestión y los objetos gestionados.

La industria de telecomunicaciones es dinámica. Los operadores y proveedores de servicios están operando en un mercado ultra - competitivo que posee un apetito insaciable por nuevos servicios y aplicaciones.

El poder combinado entre la movilidad e Internet permitirá el acceso a toda hora y en cualquier lugar. La migración desde redes "circuit switched" hacia "packet switched" significa que los operadores deben agregar nuevas tecnologías tales como ADSL, Media Gateways, ATM, etc., mientras mantienen las redes y servicios existentes que generan las actuales utilidades.

En varias situaciones esto significa aumentar el equipamiento acudiendo a varios proveedores.

Sánchez (2000), La feroz competencia no permite que los movimientos rápidos para introducir nuevos servicios en el mercado sean sacrificados. La creciente complejidad de las redes genera un aumento en la necesidad de contar con flexibles soluciones de gestión. Varios operadores actuarán como "carriers", vendiendo capacidad a los proveedores de

servicios y proveedores de acceso. La activación del servicio, la inter-operación y facturación será crucial utilizada frecuentemente.

Para cubrir la demanda del mercado se utiliza los mejores componentes, aplicaciones para proveer soluciones completas de gestión con flexibilidad para adaptar los cambios en la demanda de servicios y tecnología de redes. La migración hacia redes multi-servicio completa es soportada con soluciones para el portafolio ENGINE, con alternación de circuitos AXE y convergencia IP.

Soluciones ofrecidas para la Seguridad en la Operación de las Redes y Servicios, brindando gestión en la performance, routing, configuración y tráfico. Las soluciones brindan calidad superior en los servicios a los usuarios finales, reducción de costos, planeación de redes y permite la creación de nuevos volúmenes de utilidad.

**Gestión del Cliente**, ofrece soluciones end-to-end en las áreas de facturación, atención al cliente, pre-pago, fraude y mediación, mientras que la rentabilidad puede ser incrementada con mejoras en el "time-to-market," atención al cliente y performance.

Abastecimiento en la **Gestión de Servicios de Telecomunicaciones**, soluciones que soportan el servicio de abastecimiento de servicios de próxima generación, como "banking", " e-payment" y "unified messaging" pueden ser suministradas rápidamente, con alta calidad y bajo costo para los clientes. Mediación en la utilización ofrece una colección flexible, pre -procesamiento,

y distribución de valiosos usos de datos para aplicaciones "downstream".

E-Management, soluciones que permiten la gestión de la atención del cliente en la web y el soporte en la administración de servicios digitales.

Soluciones completas para la gestión de servicios para redes multi-servicio:

- Maximiza la performance de las redes multi-servicio en términos de capacidad y relanzamiento de servicios - maximizando la utilidad.

- Maximiza la satisfacción del cliente a través de eficientes servicios de facturación de servicios y fulfillment.

- Simplifica los procesos del operador, dando acceso a información relevante más fácil y rápidamente acortando los tiempos de respuesta.

- Asegura la calidad consistente de los servicios provistos.

- Permitirá la continua evolución y gestión para cubrir los requerimientos futuros.

- Basado en los requerimientos específicos del negocio del operador y en los requerimientos del mercado local. p.e Ericsson maneja las mejores soluciones para alcanzar sus necesidades. "One-stop-shopping" y total y "turn-key solutions" reducen la complejidad de las decisiones técnicas, modularidad, pre-integración y capacidad "multi-vendor compatibility" son el eje de la Gestión de Telecomunicaciones

Race (1994), Las soluciones de Gestión en Telecomunicaciones no solo brindan el comando, control, inteligencia, comprensión y simplicidad

para resolver los problemas de la red del operador, sino que también tienen en cuenta el potencial de sus redes.

La seguridad en las redes está relacionada con la seguridad de los sistemas, programas y datos cuantos éstos existen en una red establecida. Los efectos de compartir en las redes tiene como resultado la existencia de más usuarios potenciales (simpáticos o no) accediendo a los sistemas, las redes aumentan la vulnerabilidad de los sistemas informáticos.

El autor Méndez (2000) señalan el término TMN (Telecommunications Management Network) fue introducido por la ITU-T, y está definido en la recomendación M.3010. Aunque en un principio no hubo mucha colaboración entre los grupos de gestión de red de la ISO y el CCITT (germen de la ITU-T), posteriormente fueron incorporados varios conceptos del modelo OSI al estándar TMN. En concreto:

- Se adoptó el modelo gestor-agente del modelo OSI
- Se siguió el paradigma de la orientación a objetos de la arquitectura OSI
- Se trabajó conjuntamente en el desarrollo del concepto de dominios de gestión

Un aspecto diferenciador de ambos modelos consiste en la introducción, en el modelo TMN, de una red separada de aquella que se gestiona, con el fin de transportar la información de gestión.

A diferencia del modelo OSI el cual se definen cinco áreas funcionales, el estándar TMN no entra en consideraciones sobre las



aplicaciones de la información gestionada. Por el contrario, se define la siguiente funcionalidad:

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

### **2.9.1 Arquitectura TMN**

El objetivo es proporcionar una estructura de la red organizada para conseguir la interconexión de los diversos tipos de sistemas de operación y equipos de telecomunicaciones usando una arquitectura estándar e interfaces normalizados.

Arquitectura física, estructura y entidades de la red

Modelo organizativo, niveles de gestión

Modelo funcional, servicios, componentes y funciones de gestión

Modelo de información, definición de recursos gestionados

La motivación de una arquitectura de TMN es por la heterogeneidad en la tecnología de redes de telecomunicaciones, redes analógicas, digitales banda estrecha, banda ancha, demandas sobre posibilidad de introducir nuevos servicios, alta calidad de servicios, posibilidad de reorganizar las redes, métodos eficientes de trabajo para operar las redes y competencia entre empresas operadoras privadas.

ITU-T (1992), El modelo TMN define tres arquitecturas diferenciadas:

- **Arquitectura funcional**, describe la distribución de la funcionalidad dentro de la TMN, con el objeto de definir los bloques funcionales a partir de los cuales se construye la TMN.
- **Arquitectura física**, describe los interfaces y el modo en que los bloques funcionales se implementan en equipos físicos.
- **Arquitectura de la información**, sigue los principios de los modelos OSI de gestión (CMIS y CMIP) y directorio (X.500).

**Arquitectura funcional** Estos bloques proporcionan la funcionalidad que permite a la TMN realizar sus funciones de gestión.

A continuación se describen los distintos tipos de bloques funcionales:

**Función de operación de sistemas (OSF):** Los OSF procesan la información relativa a la gestión de la red con el objeto de monitorizar y controlar las funciones de gestión.

**Función de estación de trabajo (WSF)** Este bloque funcional proporciona los mecanismos para que un usuario pueda

interactuar con la información gestionada por la TMN.

**Función de elemento de red (NEF)** Es el bloque que actúa como agente, susceptible de ser monitorizado y controlado.

Estos bloques proporcionan las funciones de intercambio de datos entre los usuarios de la red de telecomunicaciones gestionada.

**Adaptadores Q (QAF)** Este tipo de bloque funcional se utiliza para conectar a la TMN aquellas entidades que no soportan los puntos de referencia estandarizados por TMN.

**Función de mediación (MF)** La función de mediación se encarga de garantizar que la información intercambiada entre los bloques del tipo OSF o NEF cumple los requisitos demandados por cada uno de ellos.

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

Cada bloque funcional se compone a su vez de un conjunto de componentes funcionales, considerados como los bloques elementales para su construcción.

Estos componentes se identifican en la norma pero no están sujetos a estandarización.

**Arquitectura Físicas**, se encarga de definir como se implementan los bloques funcionales mediante equipamiento físico y los puntos de referencia en interfaces. En la arquitectura física se definen los siguientes bloques constructivos:

- Elemento de red (NE)

- Dispositivo de mediación (MD)
- Adaptador Q (QA)
- Sistema de operaciones (OS)
- Red de comunicación de datos (DCN)

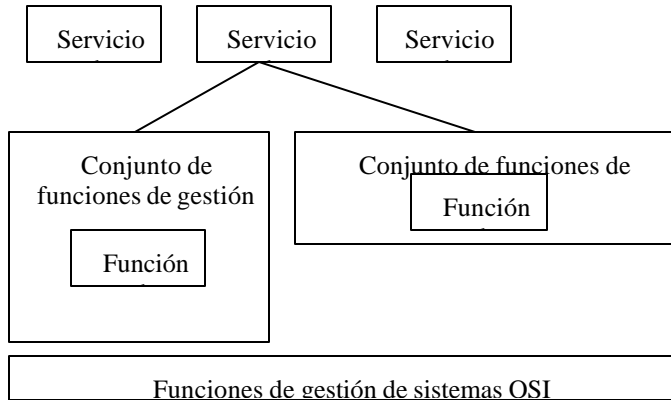


Figura 14 Modelo funcional de TMN  
Fuente: Salavert (1998)

Cada uno de estos bloques puede implementar uno o más bloques funcionales (excepto el DCN que se encarga de realizar el intercambio de información entre bloques), pero siempre hay uno que ha de contener obligatoriamente y que determina su denominación.

Los interfaces son implementaciones de los puntos de referencia, y son comparables a las pilas de protocolos.

Existe una correspondencia uno a uno entre los puntos de referencia y los interfaces, excepto para aquellos que están fuera de la TMN, es decir, los puntos de referencia g y m.

**Arquitectura lógica de niveles** En el estándar TMN define una serie de capas o niveles de gestión mediante las cuales se pretende abordar la gran complejidad de la gestión de redes de telecomunicación. Cada uno de estos niveles agrupa un conjunto de funciones de gestión. El estándar LLA define cuáles son esos niveles y las relaciones entre ellos.

Se definen los siguientes niveles:

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

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

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

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

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

- **Nivel de Gestión de Negocio.** Incluye la completa gestión de la explotación de la red, Contabilidad, Gestión y Administración, basándose en las entradas procedentes de los niveles de Gestión de Servicios y de Gestión de Red.

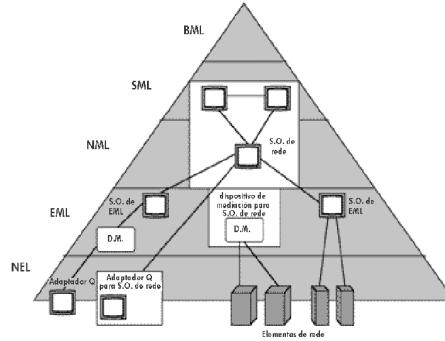


Figura 15 Modelo lógico de una pirámide TMN  
Fuente: Salavert (1997)

Diseñar una red permitirá interconectar los sistemas de operación con elementos de la red, todos los sistemas de operación deberán usar el mismo método de acceder a los recursos, respetando la heterogeneidad y capacidad de los recursos de telecomunicaciones, interconexión con otros dominios y estaciones de trabajo de operadores.

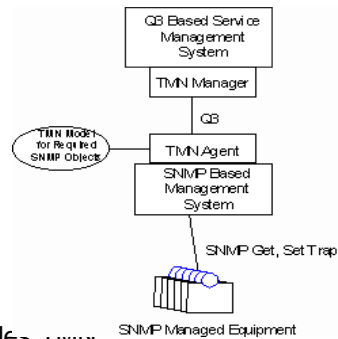


Figura 16 Bloques funcionales TMN  
Fuente: Salavert (1997)

J. Sánchez (2000), señala el operador de red debe disponer de sistemas de gestión que cumplan las recomendaciones estándares referentes a gestión de red.

De esta forma, tal como se muestra en la figura 17 la comunicación y cooperación entre sistemas actuando en diferentes dominios e incluso en un entorno multisuministrador se verá favorecida.

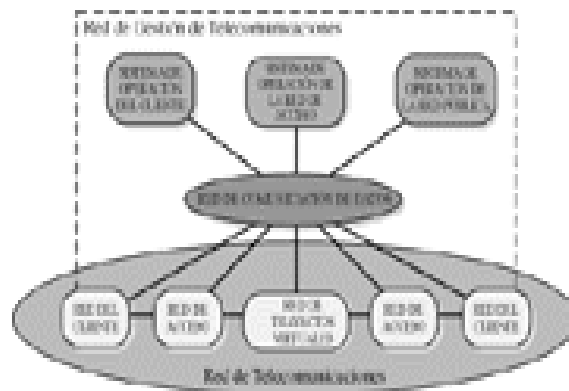


Figura 17: Relación entre la Red de Gestión y la Red de Telecomunicaciones  
Fuente: J. Sánchez (2000)

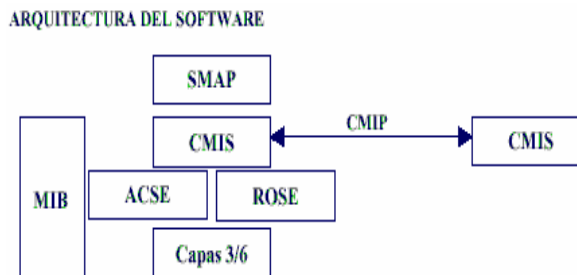


Figura 18 Arquitectura del software para TMN  
Fuente: Race (1994)

Se define un modelo de 7 capas para la TMN.

Las inferiores se han detallado. Las capas complementarias son las siguientes:

-Capa de Transporte (capa 4/ISO 8073): clase de servicio, retransmisión de datos.

-Capa de Sesión (capa 5/ITU-T X.215): aceptación, rechazo, desconexión, aborto, transporte y segmentación.

-Capa de Presentación (capa 6/ITU-T X.216/226): reglas de codificación para sintaxis de transferencia.

-Capa de Aplicación (capa 7/ITU-T X.217/227): sintaxis abstracta (protocolos CMIP y ROSE).

Las funciones generales de la TMN son:

-Transporte de información entre distintos elementos;

-Almacenamiento de la información;

-Seguridad para garantizar un control de acceso;

-Consulta para permitir el acceso a la información;

-Tratamiento para permitir el análisis;

-Soporte para garantizar la entrada/salida de datos.

Dichas funciones se estructuran en 4 niveles (es decir, cada tipo de gestión se realiza en estratos diferentes) de acuerdo con ITU-T M.3010:

De esta forma la función de gestión de averías en el elemento de red es detectar alarmas, las cuales son "filtradas" (seleccionada de acuerdo con prioridad y origen) en la gestión de avería de red y presentadas en gestión de



avería de servicio.

Tobal (1999) señala lo siguiente, en 1988, el IAB (Internet Activities Board, Comité de Actividades Inter-red) determinó la estrategia de gestión para TCP/IP (Transfer Control Protocol/Internet Protocol, Protocolo de Control de Transmisión/Protocolo de Inter-Red).

Esto significó el nacimiento de dos esfuerzos paralelos: la solución a corto plazo, SNMP, y la solución eventual a largo plazo, CMOT (CMIP Over TCP/IP, CMIP sobre TCP/IP).

## **2.10 Estado del Arte en Estandarización de Gestión de Red**

Millán (2000), manifiesta en su investigación diversos organismos están involucrados en el proceso de definición de estándares de gestión de red, entre los que cabe destacar a ISO, CCITT.

ISO y CCITT. ISO orienta sus trabajos a la gestión de sistemas abiertos, entendiendo por sistema abierto cualquier sistema que se comunica con otros mediante los protocolos de comunicación definidos en el modelo de referencia de interconexión de sistemas abiertos (Open System Interconnection Reference Model).

Se establece en las recomendaciones de ISO un marco de trabajo en el cual se describen los modelos de organización, de comunicación, de información y funcional que se emplean en la gestión de sistemas abiertos.

Stalling (1997), El modelo de organización indica cómo asignar los papeles de gestor y/o agente a los actores que participan en la gestión, cómo

modificar dinámicamente dichos papeles y cómo agrupar los objetos gestionados en dominios de gestión.

El modelo de comunicación señala cómo las interacciones entre sistemas gestores y sistemas gestionados se realizan a través del intercambio de información de gestión mediante protocolos OSI.

El modelo de información describe la abstracción en objetos de los recursos que están siendo gestionados y de los recursos necesarios para la gestión, y la definición de la base de información de gestión (MIB: Management Information Base) como el conjunto de los objetos necesarios para la gestión de un sistema.

El modelo funcional describe las distintas funciones necesarias para gestionar un sistema y las interrelaciones entre ellas, estas funciones se agrupan en las denominadas áreas funcionales (de fallos, de configuración, de contabilidad, de prestaciones y de seguridad) para satisfacer los requisitos del usuario para gestión,

A continuación se proporciona una clasificación de las recomendaciones de ISO organizadas de acuerdo a estos modelos.

Además de las recomendaciones en las que se describen el servicio y el protocolo de información de gestión común (CMIS, CMIP), y la guía para la definición de objetos gestionados (GDMO), son de especial relevancia las recomendaciones de ISO en las que se describen las Funciones de Gestión de Sistemas abiertos (FGS), recogidas en la serie 10164-X.

Millán (2000), Una FGS define la semántica de una funcionalidad de gestión general de sistemas abiertos y puede junto con otras FGSs, ser empleada por uno o más servicios de gestión para proporcionar la funcionalidad del servicio específico.

Un FGS define, la sintaxis abstracta de la información transferida mediante el servicio de comunicación ofrecido por distintos elementos de servicio de aplicación (CMISE, FTAM, TP,)

Dos o más de estas FGSs pueden agruparse para ofrecer sus funcionalidades de forma conjunta, en los denominados SMASEs. De esta forma, los servicios proporcionados por un SMASE (Systems Management Application Service Element) se basan en FGSs (es decir, un SMASE puede estar formado por varias FGSs). Estas últimas pueden ser negociadas entre los actores que intervienen en la gestión de sistemas.

Mientras que ISO trabaja en el campo general de la gestión de sistemas abiertos, CCITT centra su actividad de estandarización en la gestión de redes de telecomunicaciones.

El CCITT define en su recomendación M.3010, el concepto de TMN (Telecommunications Management Network) o en castellano RGT (Red de Gestión de Telecomunicaciones), una red separada de la red de telecomunicación que se conecta con esta última en diferentes puntos para intercambiar información para controlar las operaciones de la misma. Una RGT soporta los requisitos de gestión necesarios para planificar, instalar, mantener, operar, administrar redes y servicios de telecomunicación.

En la [figura 19](#) se muestra la arquitectura física simplificada de una RGT genérica.

Según se observa en ella los Sistemas de Operación (SO) encargados de procesar la información de gestión y de realizar las funciones de gestión se conectan con los Elementos de Red a gestionar (ER) a través de una interfaz denominada Q3.

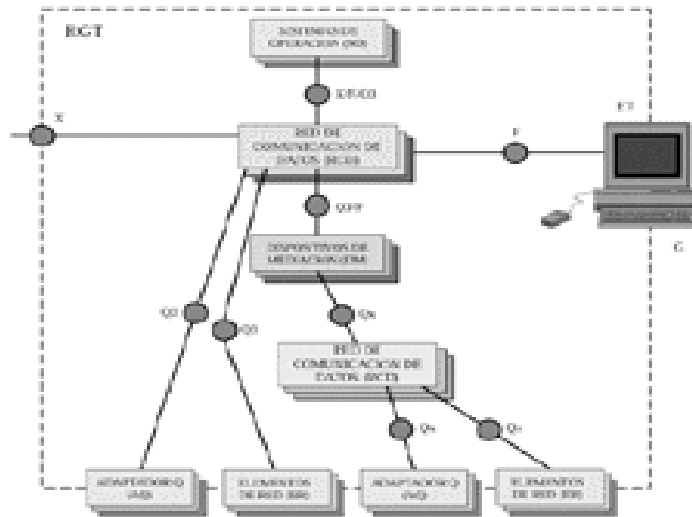


Figura 19. Estructura RGT  
Fuente: Millán (2000)

Si el ER no soporta dicha interfaz, es necesario emplear un Adaptador de interfaz Q (AQ). La conexión con los elementos de red puede ser directa a través de la Red de Comunicación de Datos (RCD) o se puede realizar a través de los dispositivos de Mediación (DM), los cuales pueden adaptar, filtrar y/o condensar la información recibida de los ERs vía

interfaz Qx.

La conexión entre la RGT se realiza a través de la interfaz X. Por último, los usuarios de la RGT acceden a la funcionalidad de ésta mediante las Estaciones de Trabajo (ET), las cuales se comunican con el resto de componentes de la RGT a través de la interfaz F.

Los sistemas de operación pueden encontrarse jerarquizados. En efecto, un SO puede responsabilizarse de la gestión:

- A nivel de elemento de red (gestión de un conjunto de ERs de un área geográfica determinada, diferenciado por la tecnología y las características de los ERs)
- A nivel de red (gestión global de una red en concreto, con visión completa de la misma)
- A nivel de servicio (gestión de un servicio concreto que puede necesitar varias redes, gestión de aspectos relacionados con el cliente y la personalización del servicio)
- A nivel de negocio (gestión de los aspectos estratégicos con influencia de factores macroeconómicos y legislativos)

## **2.11 Introducción a los Protocolos de Gestión de red**

### **2.11.1 Protocolos de Gestión ISO/IUT**

Race (1994), detalla las funciones previstas para la gestión de red, la posición en el modelo de capas de los protocolos RFC (ICMP y SNMP) y los

IUT-T (CMIP) para efectuar la gestión de redes. Los protocolos de capa 3 son IP y CLNS respectivamente, ambos protocolos funcionan sobre redes LAN o líneas X.25.

### **Funciones de la gestión de redes**

**Fallas**, permite detectar la localización de fallas, aislar partes de la red, correlacionar alarmas múltiples, administrar test de diagnósticos rutinarios o sobre la base de esto reconfigurar o modificar la red.

**Cobro** Se refiere a la determinación de costos de operación para cambiar procedimientos.

Permite detectar el uso abusivo o ineficiente por parte de componentes de la red.

**Configurar** Se trata de una comunicación hacia y desde los elementos de red. Permite el inventario, la asignación de recursos, la activación y el back-up para la restauración futura.

La información sobre configuración describe la naturaleza y el estado de los recursos involucrados en la red. Incluye la descripción de atributos de los recursos físicos (hardware) y lógicos (software: circuitos virtuales, contadores, temporizadores, etc).

**Performance** Se pueden obtener indicadores de performance orientados al servicio (disponibilidad, tiempo de respuesta, porcentaje de segundos sin errores EFS) e indicadores orientados a la eficiencia (cantidad de eventos de transacción ocurridos -Throughput- y la utilización como

porcentaje del recurso utilizado.

Esta gestión permite la colección de estadísticas, cambiar parámetros, generar tráfico artificial, etc.

**Seguridad** Permite la autenticación y control de acceso para protección contra intrusos no autorizados.

Sara (1993) La gestión de configuración puede realizarse mediante una lista de datos como en SNMP o mediante una base de datos orientado-al-objeto como en ISO.

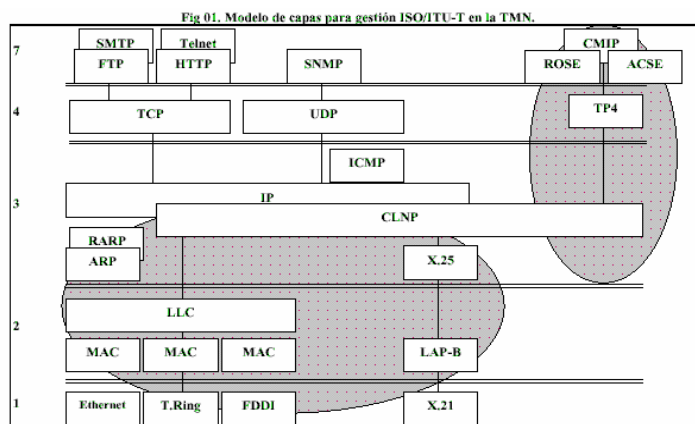


Figura 20 Modelo de Capas para gestión ISO/IUT  
Fuente: Race (1994)

### 2.11.2 Protocolos de comunicación.

ITU-T (1992). La ISO-7498 y ITU-T-X.700 han determinado un modelo de arquitecturas generales de estándar para la gestión de redes. En particular dan lugar a la red de management de telecomunicaciones TMN.

A continuación se indican los protocolos definidos en las normas ISO relacionados con funciones de gestión de redes.

-SMAP (System Management Application Process). Es el software local responsable de la gestión. Puede ser coordinado con SNMP. Permite normalmente una visualización en formato Windows (Open View).

-CMIP (Common Management Information Protocol). Protocolo a nivel de aplicación para comunicación entre funciones CMIS. CMIS (CMI Service). ISO-9595. Los servicios definidos en CMIS se efectúan mediante el protocolo de comunicación CMIP. Permite cambios de atributos o estado de objetos y recibe reportes (Trap). Opera sobre los protocolos ACSE y ROSE en la misma capa 7.

-ACSE (Association Control Service Element). ISO8649. ACSE permite iniciar y terminar una conexión entre 2 aplicaciones (capa 7).

-ROSE (Remote Operation Service Element). ISO 9072. ROSE permite realizar una operación en otro sistema (origen invoker y recipiente performer).

- LME (Layer Management Entity). Lógica incorporada a cada capa del modelo para permitir la gestión de la red. Estas entidades se encuentran distribuidas.

-MIB (Management Information Base). Colección de información que cada nodo entrega a la gestión de la red, MIB obtiene información de cada capa del modelo. Utiliza la técnica orientada-al-objeto OOD (Object Oriented Design) que data desde los años 70. En 1983 se crea el lenguaje Small-Talk



para comunicar objetos sin conocer su operación interna. Consiste en definir Objetos abstractos cuyas características dinámicas se modelan con un Comportamiento.

Se define al objeto gestionado en términos de atributos que son una variable a la cual se le asignan valores.

Los valores son: características operacionales, estado corriente, condiciones de operación, etc.

El objeto gestionado se describe mediante su comportamiento (Behavior). En una red real la función completa envuelve la interacción de todos los objetos asociados. La totalidad de los objetos se la conoce como base o modelo de datos MIB.

- CMIS/P (Common Management Information Service/Protocol). Event-Report Permite reportar un evento desde un manager a otro.

Es una indicación asincrónica de eventos importantes y lleva la información necesaria para reconocerlo. Puede ser confirmada la recepción de Event\_Report. Get Requiere un reporte desde un manager a otro.

## **2.12 Modelo Internet SNMP (Protocolo Sencillo de Administración de Redes).**

Stalling (1997), El protocolo sencillo de administración de redes (SNMP) es el protocolo de administración de redes estándar usado en Internet, define la comunicación de un administrador con un agente

Define el formato y el significado de los mensajes que intercambian el administrador y el agente<sup>1</sup>. En lugar de definir muchas operaciones, el SNMP utiliza el paradigma de obtención y almacenamiento, el administrador manda solicitudes de obtención y almacenamiento de valores en variables. Todas las operaciones se definen como efectos colaterales de las operaciones de almacenamiento.

El SNMP no define el grupo de variables que se pueden emplear, las variables y sus significados se definen en normas distintas, lo que permite la definición de diferentes grupos de variables MIB para cada dispositivo de hardware o protocolo.

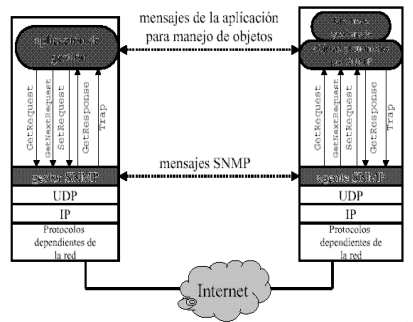


Figura: 21 Formato de mensaje de SNMP  
Fuente: Stallings, (1999)

Stalling (1997), también señala SNMP es una extensión del protocolo de gestión de red para gateways SGMP (Simple Gateway Monitoring Protocol, Protocolo Sencillo de Supervisión de Pasarelas), que se convirtió en 1989 en el estándar recomendado por Internet.

<sup>1</sup> Se usara el término agente, refiriéndose a un dispositivo que actúe como servidor

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

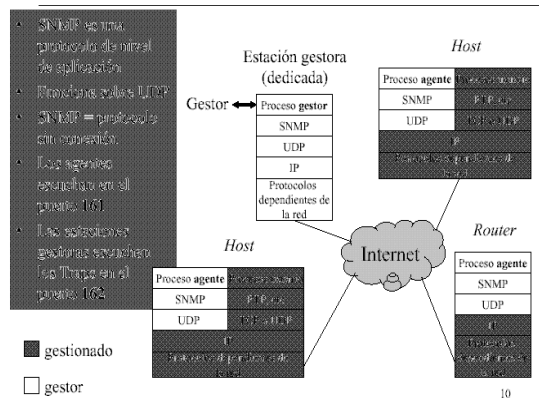


Figura: 22 Formato de mensaje de SNMP  
Fuente: Stallings, (1999)

SNMP debido al enorme éxito que ha tenido desde su publicación en el estándar de factor de gestión de redes.

Prácticamente todo el equipamiento de redes puede ser gestionado vía SNMP.

Algunas de las funciones que proporciona son:

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

Este protocolo incorpora varios elementos presentes en otros estándares como el modelo gestor-agente, la existencia de una base de datos de información de gestión (MIB) o el uso de primitivas de tipo PUT y GET para manipular la información. A continuación se describen dichos elementos:

- Agente: equipamiento lógico alojado en un dispositivo gestionable de la red, almacena datos de gestión y responde a las peticiones sobre dichos datos.

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

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

[Tobal](#) (1999), afirma que el protocolo realiza las funciones descritas anteriormente llevando información de gestión entre los gestores y los agentes. Es sólo un aspecto dentro de toda la estructura de gestión la cual está compuesta de los siguientes elementos:

- Estación de Gestión de Red (Network Management Station, NMS). Es el elemento central que proporciona al administrador una visión del estado de la red y unas funciones de modificación del estado (puede ser una estación de trabajo o un ordenador personal).

- Estructura de la Información de Gestión (SMI, Structure of Management Information). Es un conjunto de reglas que define las

características de los objetos de la red y cómo obtienen los protocolos de gestión información de ellos.

Aunque ha sido diseñado después del SMI de OSI, no es compatible con este.

- Base de Información de Gestión (MIB). Es una colección de objetos, que representan de forma abstracta los dispositivos de la red y sus componentes internos. La MIB es conforme a la SMI para TCP/IP. Cada agente SNMP contiene instrumentación que, como mínimo, debe ser capaz de reunir objetos MIB estándar. Estos objetos incluyen direcciones de red, tipos de interfaz, contadores y datos similares.

El estándar MIB de Internet define 126 objetos relacionados con los protocolos TCP/IP.

Los fabricantes que deseen pueden desarrollar extensiones del estándar MIB. Estas MIBs privadas incorporan un amplio rango de objetos gestionables, y algunas veces contienen objetos que son funcionalmente similares a los MIBs ya definidos, en otros casos el cambio de una variable en un objeto inicia una batería de funciones en el dispositivo gestionado (como por ejemplo un autodiagnóstico).

La carga de la gestión de todas las MIBs y de las extensiones privadas recae en el sistema de gestión escrita en una variante simple del lenguaje de definición OSI ASN.1. En 1990 se introdujo una nueva versión de MIB, MIB II donde la mayor aportación es la utilización de 185 nuevos objetos de extensiones privadas.

Aparte de la MIB, existe la Base de Datos de Estadísticas de Red (Network Statistics Databas, NSD) que está en la estación de trabajo de gestión, en esta base de datos se recoge información de los agentes para realizar funciones de correlación y planificación.

Las limitaciones de SNMP se deben a no haber sido diseñado para realizar funciones de gestión de alto nivel, sus capacidades lo restringen a la supervisión de redes y a la detección de errores.

Como todos los elementos TCP/IP, se ha ido creado pensando más en su funcionalidad y dejando a un lado la seguridad. SNMP opera en la capa de transporte del TCP/IP por lo que ignora los aspectos específicos del hardware sobre el que funciona.

### **2.13 SNMPv2 y v3**

Stalling( 1997), En 1996 se publicó un nuevo estándar, el protocolo SNMPv2, resultado de una serie de propuestas para mejorar las características de SNMP.

Los cambios se traducen fundamentalmente en una mejora de las prestaciones, un aumento de la seguridad y en la introducción de una jerarquía de gestión.

- Prestaciones: mejora el mecanismo de transferencia de información hacia los gestores, de forma que se necesitan realizar menos peticiones para obtener paquetes de información grandes.

- Seguridad: A diferencia de SNMP, no incorpora mecanismo de seguridad, define métodos para controlar las operaciones que están permitidas.

Desafortunadamente surgieron dos planteamientos diferentes en cuanto al modelo de seguridad, que han dado lugar a dos especificaciones conocidas como SNMPv2\* y SNMPv2u.

Soluciona este inconveniente introduciendo los gestores de nivel intermedio, son estos últimos los que se encargan de sondear a los agentes bajo su control.

Soriano L. (2000). Los gestores intermedios son configurados desde un gestor principal de forma que solo se realiza un sondeo de aquellas variables demandadas por este último, y solo son notificados los eventos programados, también introduce un vocabulario más extenso, permite comandos de agente a agente y técnicas de recuperación de mensajes.

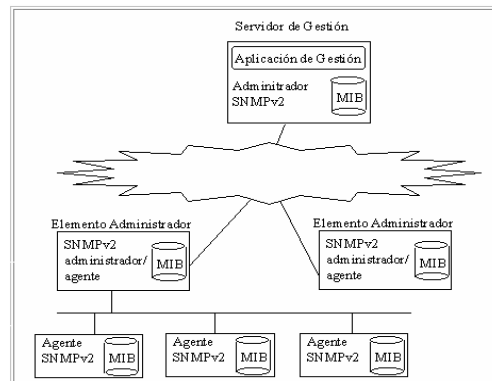


Figura 23 Configuración de Gestión de SNMPv2  
Fuente: Stalling (1997)

## **2.14 CMIP**

CMIP fue diseñado teniendo en cuenta a SNMP solucionando los errores y fallos de SNMP volviéndose un administrador de red mayor y más detallado, es un protocolo de administración de red implementado sobre OSI conviene introducir el marco de trabajo OSI en lo que respecta a administración.

En pocas palabras, es una arquitectura de administración de red que provee un modo de que la información de control y mantenimiento pueda ser intercambiada entre administrador y un elemento remoto de red, en efecto los procesos de aplicación llamados administradores residen en las estaciones de administración mientras que los procesos de aplicación llamados agentes residen en los elementos de red. (Mendiola, 1997).

## **2.15 Comparación SNMP/CMIP**

A continuación se hace una comparación entre los protocolos SNMP y CMIP:

- SNMP está basado en técnicas de sondeo, mientras que CMIP utiliza una técnica basada en eventos. Esto permite a CMIP ser más eficiente que SNMP en el control de grandes redes.
- CMIP es un protocolo orientado a conexión mientras que SNMP es un protocolo sin conexión.



Esto significa que la carga de proceso de SNMP es reducida, pero cuando se envía un mensaje nunca se puede asegurar que el mensaje llega a su destino.

- La seguridad de los datos no es prioritaria para SNMP.
- CMIP permite la implementación de comandos condicionales sofisticados, mientras que SNMP necesita el nombre de cada objeto.
- CMIP permite, mediante una única petición, la recogida de gran cantidad de datos de los objetos gestionables, enviando información de retorno en múltiples respuestas. Esto no está permitido en SNMP.
- CMIP está especialmente preparado para gestionar grandes redes distribuidas, mientras que SNMP está recomendado para la gestión inter-red.
- CMIP realiza una distinción clara entre los objetos y sus atributos. SNMP no permite esto, lo cual hace imposible la reutilización de atributos y definiciones.

## **2.16 Monitorización de red**

Para la monitorización se consideran cuatro fases de una red:

- Definición de la información de gestión que se monitoriza
- Acceso a la información de monitorización
- Diseño de mecanismos
- Procesado de la información de monitorización
- Control de red, fases de definición y acceso

De acuerdo a la naturaleza existe la siguiente información a monitorear, información estática que no cambia con la actividad de la red, información dinámica que evoluciona con la propia actividad de la red y por último la estadística postprocesado de la información dinámica que proporciona un mayor significado de gestión.

¿Qué información monitorizar?

Depende de la aplicación

- Para gestión de prestaciones: información estadística, generada a partir de información dinámica (tráfico, retardo, etc)
- Para gestión de fallos, información dinámica (cambios de estados)
- Para gestión de configuraciones; información estática (inventario de red)

El objetivo es monitorización remota de los recursos desde el centro de gestión, necesita una cooperación entre los gestores y los equipos gestionados, los equipos deben querer ser gestionados, instalación del software de gestión adecuado. El método común de acceso a la información gestionada independiente de la tecnología o fabricante del equipo monitorizado, los modelos de gestión de red integrada proporcionan la interoperatividad.

Los mecanismos de monitorización consideran:

- Sondeo o polling, acceso periódico a la información de gestión, su ventaja es que los objetos solo deben estar preparados para responder simplicidad

- Event reportong o notificaciones, los propios recursos envían notificaciones bajo ciertas condiciones, su ventaja minimiza el tráfico de gestión por la red

Las filosofías de gestión son descargar la complejidad hacia los gestores y balancear complejidad entre gestores y equipos gestionados.

Los administradores de red no sólo deben gestionar una infraestructura cada vez más compleja sino también debe cumplir objetivos específicos sobre el nivel de servicio ofrecido, el equipamiento de red debe ser monitorizado para detectar y resolver fallos, los datos deben ser analizados para identificar cuellos de botellas y predecir problemas, el flujo de datos debe ser optimizado para asegurar la utilización más efectiva de los recursos de la red (Mendoza, 2000)

Los administradores de grandes redes distribuidas necesitan una herramienta de gestión que les permita analizar mediante una interfaz gráfica e intuitiva, la red y sus dispositivos.

## **2.17 Algunas Plataformas de Administración**

Hay categorías de software que da un paso más allá en la tarea de gestión de redes ofreciendo una solución completa tanto para monitorizar como para configurar toda la red. Este tipo de solución permite obtener una compleja representaci ón gráfica de la red y ojear fácilmente los nodos que la componen verificando detalles de configuraciones específicas y otras cuestiones de interés. (Mendoza, 2000)

A este nivel se puede hablar de soluciones comerciales ampliamente utilizadas: Hp-openView de Hewlett-Packard, Sunnet Manager de Sun, entre otros.

Estas herramientas ofrecen una plataforma integrada para la gestión de los recursos de red a través de impresionantes interfaces gráficas, entre otras utilidades disponen de herramientas para localizar los nodos de la red en los que se están sujetando agentes SNMP.

Otro aspecto importante para la gestión de redes es la capacidad de integrar productos de otros fabricantes, como lo hace CiscoWorks de Cisco, permite al administrar mantener una base de datos con todas las configuraciones de los encaminadores e incluso monitorizar gráficamente los paneles traseros en los encaminadores con todas sus conexiones.

### **2.17.1 Tivoli Management Environmet**

Es una herramienta escalable abierta al mercado y capaz de desempeñarse en múltiples plataformas que permiten administrar redes empresariales desde un punto centralizado, la base de este producto es proveer un entorno gráfico.

Tivoli permite el monitoreo permanente de los recursos de la red asegurándose que estos estén disponible a los usuarios.

Esta herramienta hace posible implementar aplicaciones y software a cientos de estaciones de trabajo con una sola operación asegurándose que la misma versión este disponible para todos los usuarios, además provee a

los administradores de una detallada bitácora de operaciones referentes a plataformas específicas. Soporta proyectos como manejo de tareas automáticas para la detección de intrusos, monitoreo de los recursos, respaldo y recuperación de datos.

### 2.17.2 Hp Open View, servicio Hp de monitorización de la disponibilidad de redes

Hp Open View monitoriza todo tipo de evento en su entorno de red, ofrece una cobertura de soporte completa para la implantación y disponibilidad de red.

Explora la existencia de problemas en su entorno de red verificando si un conjunto de equipos que responde a una petición de eco ICMP (protocolo de mensajes de control para internet).

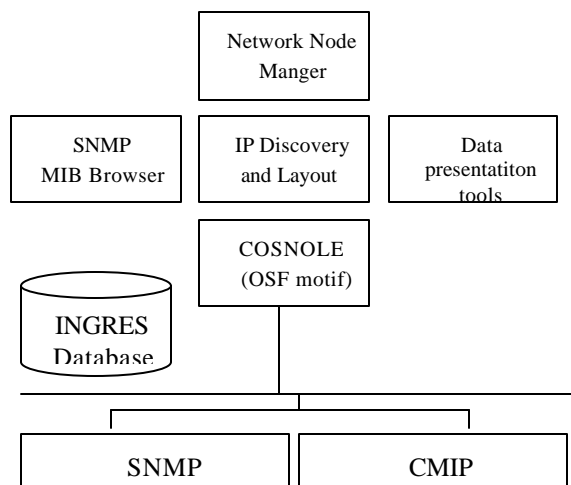


Figura: 24 Arquitectura Hp OpenView  
Autor: Mendoza (2000)

Hp sondea su entorno de red por términos medio cada 5 minutos, las 25 horas del día, los 7 días de la semana, los 365 días al año. Cuando detecta una incidencia en la red trabaja para aislar y resolver el problema, clasifica la incidencia en dos categorías urgente e informativo.

### **2.17.3 Novell Managewise**

Optimiza el funcionamiento de la red garantizando el cumplimiento de sus metas administrativas con un sorprendente rendimiento de inversión.

Es una solución integrada y de gran alcance que permite optimizar su manejo administrativo y gerencial, optimiza su heterogénea red informática.

Predice futuros cuellos de botellas y planifica la resegmentación de su LANS antes de que se presenten problemas.

Los beneficios principales se traducen en reducir el costo de adquisición y operación de la red, incrementa las operaciones de negocios, imprime efectividad al trabajo y dota de mayor productividad al usuario.

Con facilidad permite planificar los cambios y crecimiento futuro que experimentará la red, por otro lado posibilita la inspección de las tendencias de tráfico en la red sobre Ethernet y redes de señales circulares con lo cual podrá optimizar los senderos de tráfico en la red.

### **2.17.4 Unicenter TNG**

Es la solución al manejo inteligente de negocios permite supervisar, controlar y administrar diferentes plataformas, hardware, software desde un solo punto de mando

Una capacidad de extremo a extremo optimiza la disponibilidad del sistema y predice las posibles fallas.

TNG tiene un conjunto de herramientas de administración desarrolladas sobre una estructura muy flexible, su arquitectura esta bajada en objeto, tiene una base de datos que actúa como repositorio de las características de los objetos y una infraestructura del tipo manager/agent.

Visualiza los procesos que corren en cada máquina, con un golpe de vistas se puede conocer el estado de una impresora, si una torre de cintas necesita reemplazo de sus cintas o si un determinado usuario se encuentra bloqueado en la red.

#### **2.17.5 MTRG: Multi Router Traffic Grapher**

MTRG es una avanzada herramienta de utilidad gráfica para representar gráficamente los datos que los gestores SNMP leen de los agentes SNMP, produce unas vistosas páginas HTML con gráficos GIF sobre el gráfico entrante y saliente en las interfaces de red, prácticamente en tiempo real.

Con esta herramienta se evita el tener que trabajar directamente con las utilidades CMU-SNMP mediante línea de comandos, es una herramienta potente y fácil de utilizar.

MRTG utiliza una implementación de SNMP escrita completamente en Perl, por lo tanto no es necesario instalar otros paquetes, el programa principal está escrito en "C" para acelerar el proceso de toma de muestras y

la generación de imágenes GIF, los gráficos son generadores con la ayuda de la biblioteca GD escrita por Thomas Boutell, autor de la FAQ WWW.

El paquete contiene algunas utilidades para analizar las interfaces de enlace, extraer sus características y generar los ficheros de configuración base que luego se pueden modificar para adaptarlos a las necesidades concretas.

Otra característica importante de esta herramienta es la cantidad de información que produce, permite cuatro niveles de detalle para cada interfaz; tráfico en las últimas 24 horas, la última semana, el último mes y un gráfico anual, esto permite recoger información para realizar estadísticos, guarda toda la información en una base de datos utilizando algoritmos de consolidación que impide que los ficheros crezcan en forma desmesurada.

Genera una página principal que contiene las imágenes GIF de los detalles diarios de cada interfaz del encaminador lo que permite hacerse una idea general de que es lo que está pasando en el encaminador con un solo vistazo. (Rabin, 2000).

## **2.18 Definición de Términos**

**ANCHO DE BANDA** -- determina la tasa a la cual la información puede ser enviada a través de un canal - a mayor ancho de banda, mayor cantidad de información que puede ser enviada en un tiempo dado. (Boehm, 1981.)



**BRIDGES (puentes):** conectar dos o más redes entre sí, aún teniendo diferentes topologías, pero asumiendo que utilizan el mismo protocolo de red y segmentar una red en subredes. (Recio. 2001)

**CARRIERS** empresas que dan el servicio de comunicaciones locales (urbanas) no son las mismas que manejan las comunicaciones de larga distancia (interurbanas) (Sheldom. 1994)

**DIRECCIÓN:** Todos los nodos de la red deben tener una dirección que los identifique dentro de la red de forma única, La dirección de un nodo depende del protocolo de comunicación que se está utilizando. (Recio. 2001)

**GATEWAYS (Pasarelas):** Permiten interconectar redes de diferentes arquitecturas, topologías y protocolos. No sólo realiza funciones de encaminamiento, sino que también realiza conversiones de protocolos (Recio. 2001)

**GESTIÓN:** Todas las medidas que aseguran la efectiva y eficiente operación de un sistema adecuando sus recursos a un objetivo. (Recio. 2001)

**HUBS (Concentradores):** Se trata de un dispositivo que centraliza la conexión de los cables procedentes de las estaciones de trabajo. (Recio. 2001)

### **INSTITUTO NACIONAL AMERICANO DE ESTÁNDARES – (ANSI)**

Diseña y propone recomendaciones para los estándares de comunicaciones internacionales. (Jones, 1986)

**INTERCONEXIÓN DE REDES:** la necesidad de interconectar dos o más redes es compartir recursos o la división en dos subredes de una red, para mejorar el rendimiento de ésta. En ambos casos es necesaria la presencia de un dispositivo (que puede ser un hubs, un bridges, un routers, etc). (Recio. 2001)

**ISO** (International Organization for Standardization): organización de normalización reconocida mundialmente. Su objetivo es el de promover y desarrollar normas para el intercambio internacional. (Recio. 2001)

**LÍNEA DE ACCESO:** Una línea de comunicaciones (p.ej. circuito) que interconecta un dispositivo compatible (Jones, 1986)

**OSI** (Open Systems Interconection): Se trata de un modelo elaborado por la ISO que define los protocolos de comunicación en siete niveles diferentes. (Recio. 2001)

**PAQUETE:** Un paquete es básicamente el conjunto de información a transmitir entre dos nodos, añadiendo datos de control como la dirección de la máquina que envía la información y la dirección de la máquina a la que va destinada la información (dirección destino). (Recio. 2001)

**ROUTERS (Encaminadores):** Se trata de dispositivos que interconectan redes a nivel de red del modelo OSI de la ISO. Realizan funciones de control de tráfico, encaminamiento de paquetes por el camino más eficiente en cada momento. (Recio. 2001)

**SNMP:** Protocolo llamado Simple Network Management Protocol. Integra la gestión de diferentes tipos de redes mediante un diseño sencillo. (Jones, 1986)

**TCP/IP:** Son dos protocolos de comunicaciones: el protocolo TCP (Protocolo de control de transmisión) que se establece al nivel de transporte del modelo OSI y el protocolo IP (Internet protocolo) que pertenece al nivel de red. (Recio. 2001)

**TRAMA:** El concepto de trama es de más bajo nivel que el de paquete. Una trama es un paquete o parte de un paquete (a veces los paquetes se fragmentan si son muy grandes) al que se le añade información de control. Las tramas son los elementos que circulan por el medio físico. (Recio. 2001)

**TRAPS:** el manager solicita información del agente y este responde, es posible para un agente emitir mensajes sin una correspondiente solicitud, este mensaje es conocido como traps, existen bajo condiciones especiales. (Computer Associates 1999).

**UMBRAL DE DESEMPEÑO:** Aquel valor establecido para un parámetro específico. P.e. procesamiento de CPU  $>0$ }= 80%, indica cual es el límite de los niveles normales, sobre o debajo, el cual se estaría en presencia de un situación de problema. (Mendiola 1997)

## 2.19 Cuadro Operacionalización de Variables

A continuación se describe las variables de estudio a la presente investigación.

**Definición Conceptual:** Un modelo de gestión de redes se define como el conjunto de actividades destinadas a garantizar los servicios que prestan las redes, controlando el uso de los recursos convirtiéndose en un factor importante ya que contribuye al mantenimiento, resolución y prevención de incidencias para asegurar la máxima disponibilidad de la red de comunicaciones.(Mendiola, 1997)

**Definición Operacional:** Operacionalmente la variable "Modelo de Gestión de Red" será manipulada y estudiada a través de las dimensiones de los mecanismos de gestión de red mediante la elaboración de instrumento de recolección de datos aplicados en las empresas con tecnología en el Estado Trujillo, los cuales se consideraron indicadores relacionados con recursos para controlar y administrar la red, disponibilidad de monitoreo, tipos y recurrencias de fallas, herramientas para atención de fallas, tecnología de

gestión utilizada, modelo de gestión de red utilizado, estadísticas de gestión, entre otros.

Así mismo, fueron medidos aspectos como Parámetros y frecuencia para monitoreo, cantidad de equipos que monitorea, Gestión de Desempeño, Gestión de Configuración, Gestión de Fallas y Gestión de Seguridad.

### Operacionalización de la Variable

Cuadro N °1

Cuadro Operacional conceptual y operacional de las variables

Variable	Dimensiones	Indicadores	ítem
Modelo de Gestión de Red	Situación actual	- Recursos para controlar y administrar la red	1
		- Disponibilidad de Monitoreo	2
		- Tipo de Falla	3,8
		- Recurrencia de las fallas	6,7,10
		- Tiempo de repuestas de las fallas	11,12
	Mecanismos de gestión de red	-Herramientas para la atención de fallas	4,5,13
		- Tecnología de gestión de red utilizada	14
		-Modelo de gestión de red utilizado	15,16,17,22
		- Parámetros de monitoreo	18,19,20,21
		- Frecuencia de monitoreo	23,9
	- Cantidad de equipos que monitorea	24,25	
	- Protocolo	26	
	- Estadísticas de gestión	27,28	

Fuente: La autora