UNIVERSIDAD NACIONAL DE INGENIERÍA
FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE RED PARA UN CAMPUS UNIVERSITARIO

INFORME DE COMPETENCIA PROFESIONAL

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

RUBÉN ARTURO BORJA ROSALES

PROMOCIÓN
1992 - II
LIMA – PERÚ
2006

IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE RED PARA UN CAMPUS UNIVERSITARIO

Dedico este trabajo a: Clara, mi esposa amada por alentarme permanentemente, a mis hermosos hijos Yelena y Rodrigo por ser una de las razones más importante de mi existencia, a mis hermanas por darme entusiasmo a seguir superándome y mis padres que sin ellos no sería lo que soy.

SUMARIO

El presente informe pretende describir y abordar las implicancias de la implementación de un sistema de gestión de red, en la primera parte se realiza un análisis de las necesidades de gestionar la red y los servicios que a través de la red se brindan. Se concluye de este análisis que la gestión de red depende del tipo de red gestionada, tipo de equipos gestionados, y objetivos específicos de la gestión de red y que a bajo nivel, todos los métodos se basan en monitorización de red y control de red.

Se hace un análisis de las arquitecturas de gestión OSI, TMN e INTERNET/SNMP. Considerando las arquitectura de gestión de red basada en SNMP, llevamos a cabo un análisis de requerimientos sobre la base de una infraestructura existente, un modelo de negocio; para luego plantear un diseño del sistema de gestión de red listando los componentes y funciones de cada uno de ellos. Finalmente se describe el proceso de implementación del sistema de gestión de red y las acciones inmediatas y más frecuentes a realizar en la tarea de gestionar la red.

INDICE

PRÓLOGO

El propósito del presente trabajo es desarrollar un método de implementación de un sistema de gestión de red, el capitulo I se inicia realizando una revisión de los conceptos de gestión de red, motivaciones y requerimientos. Aún cuando las características cualitativas son útiles y pueden guiar el desarrollo de una facilidad de gestión de red, se hace necesario una composición funcional para estructurar el proceso global de diseño. Se describe el propósito de cada área funcional (FCAPS) y los requerimientos de usuario en cada una de las áreas funcionales, también se caracteriza al sistema de gestión de red en términos de sus componentes y las funciones que desempeña, así como las arquitecturas posibles del sistema y del software de gestión de red.

Se realiza la descripción de cada una de las dos partes que se debería tomar en cuenta cuando se realiza un proyecto de gestión de red: enfoque de negocio y enfoque técnico, a partir de este enfoque se identifica cada uno de los recursos implicados en el proyecto de gestión de red, así como las funciones que cumplirán. Debido a ausencia de funcionalidad de la gestión de red ya que depende del tipo de red gestionada, tipos de equipos, objetivos específicos de la gestión de red. Se puede concluir que todos los métodos se basan en monitorización y control de red. Se hace por tanto una revisión de la arquitectura de monitorización de red, esta tiene en consideración el tipo de información a monitorizar. Se describe luego la composición funcional de un sistema de monitorización, destacándose las funciones de gestor, función de agente, objetos gestionados, agente de monitorización y aplicación de monitorización, la monitorización implica obtención de información de gestión (objetos gestionados) desde los elementos de red, dos métodos son usados: sondeo y reporte de eventos. A continuación se describe la monitorización de rendimiento a través de los indicadores de rendimiento, considerando los orientado a servicio y los orientados a eficiencia así como las dificultades para la obtención de tales indicadores. Se aborda del mismo modo la monitorización de fallas, y de contabilización; considerando las interrogantes y dificultades en el cumplimiento de la función.

Se describe luego la parte de control de red, la cual esta comprometida con la modificación de parámetros y causan acciones a ser tomados por los sistemas finales, sistemas intermedios y subredes que construyen la configuración a ser administrada. El análisis esta centrado en el control de red de la gestión de configuración y seguridad. Para finalizar el capitulo se realiza una revisión de un conjunto de herramientas de gestión de red, sus características y ámbitos de aplicación.

En el capitulo II, se hace una revisión crítica de las arquitecturas de gestión de red y al ámbito de aplicación de cada una de ellas, justificándose el uso de la gestión INTERNET/SNMP debido a su simplicidad y bajo costo de implementación para las Interredes y las LAN.

En el capitulo III se inicia la planificación del sistema de gestión de red para un campus universitario, se realiza una descripción de la topología de la red, los diferentes equipos usados en la implementación de la red de campus a gestionar. La particularidad de que la red de campus este soportada por ATM en el backbone, obliga a una revisión del estándar LAN EMULATION. Se concluye identificando los equipos que componen el backbone ATM y las acciones para su configuración. Se prosigue realizando una análisis del modelo de negocio a partir del cual identificamos los recursos de red críticos para los procesos de la organización y por tanto prioritarios para el monitoreo y control (gestión).

Se debe indicar que la cantidad y los indicadores a considerar como relevantes deberán ser seleccionados dinámicamente, así como los valores de los indicadores que activaran las alertas y alarmas variarán dinámicamente según varía el patrón de tráfico de la red.

Dadas las características de la red a gestionar el proceso de diseño implicará determinar los componentes del sistema de gestión, dado la cantidad de recursos y usuarios de la red se opta por una arquitectura centralizada, será necesario como software de gestión, una plataforma de gestión debido a la heterogeneidad de componentes de red, es necesario considerar una comparación de funcionalidad/arquitectura/robustez/escalabilidad/costo entre las diferentes plataformas del mercado. Se proporciona una descripción de las plataformas de gestión de elementos de red (SPECTRUM) y VLAN (VLAN MANAGER) se resalta sus características: arquitecturales y funcionalidades. Se concluye este capitulo con el diseño del plan de direccionamiento IP y las VLAN a crearse y la pertenecía de los hosts siguiendo un criterio funcional de la actividad que realiza el usuario.

En el capitulo 4 se describe secuencialmente los procedimientos a seguir para el despliegue del sistema de gestión de red, desde la fase de preparación de los componentes del sistema de gestión de red, así como de los elementos de red. El descubrimiento de los elementos de red por parte del software de gestión es de particular importancia, ya que es a partir de este modelo de red, que obtiene el software de gestión, que el administrador de red llevará a cabo su tarea de monitorización y control. Se termina este capitulo listando un conjunto de acciones operativas de gestión de red.

CAPITULO I

GESTIÓN DE RED

1.1 Requerimientos y motivaciones de Gestión de red.

Las redes y los sistemas de procesamiento distribuidos son de importancia creciente y, ciertamente, han llegado a ser críticos en el mundo comercial. Dentro de una organización dada, la tendencia es mayor, más redes complejas dando soporte a más aplicaciones y más usuarios. Como estas redes crecen rápidamente, dos hechos quedan de manifiesto:

- La red, sus recursos asociados y aplicaciones distribuidas comienzan a ser indispensables para la organización.
- Muchas cosas pueden ir mal, inhabilitación total o parcial de la red, degradando el desempeño a un nivel inaceptable.

Una gran red no puede ser manejada solo bajo el esfuerzo humano aislado. La complejidad de tal sistema señala la necesidad de herramientas automatizadas de gestión de red. La necesidad urgente de tales herramientas y la dificultad en suministrarlos se incrementa si la red incluye equipos de múltiples fabricantes.

Como las instalaciones de red comienzan a ser más grandes, más complejas, y más heterogéneas, el costo de gestión de red aumenta. Para controlar costos, son necesarias herramientas estandarizadas, las que puede ser usados a través de un amplio espectro de tipos de productos, incluyendo sistemas finales, puentes, ruteadores, equipamiento de telecomunicaciones, y estos pueden ser usados en un entorno compuesto por equipos de diferentes fabricantes. En respuesta a esta necesidad, el Protocolo de gestión de Red Simple (SNMP) fue desarrollado para proveer una herramienta de gestión de red ínter operable para entornos constituidos por equipos de diferentes fabricantes.

SNMP realmente se refiere a un conjunto de estándares para la gestión de red, incluye un protocolo, una especificación de estructura de base de datos, y un conjunto de objetos de datos. SNMP fue adoptado como el estándar para Internets basados en TCP/IP en 1989.

Por tanto la gestión de red podemos definirlo como un conjunto de acciones que conllevan: Planificación, organización, supervisión y control de elementos de comunicaciones para garantizar un nivel de servicio, y de acuerdo a un costo

En cualquier diseño, es mejor comenzar con una definición de requisitos de los usuarios. Esto es ciertamente verdadero en un área tan compleja como la gestión de red. Una forma de hacer esto es considerar las características que son más importantes para el usuario. La Figura 1.1 muestra los resultados de una encuesta. Dado el costo de gestión de red y la magnitud de la tarea, no debería ser ninguna sorpresa que la facilidad de uso sea de importancia crítica para los usuarios.

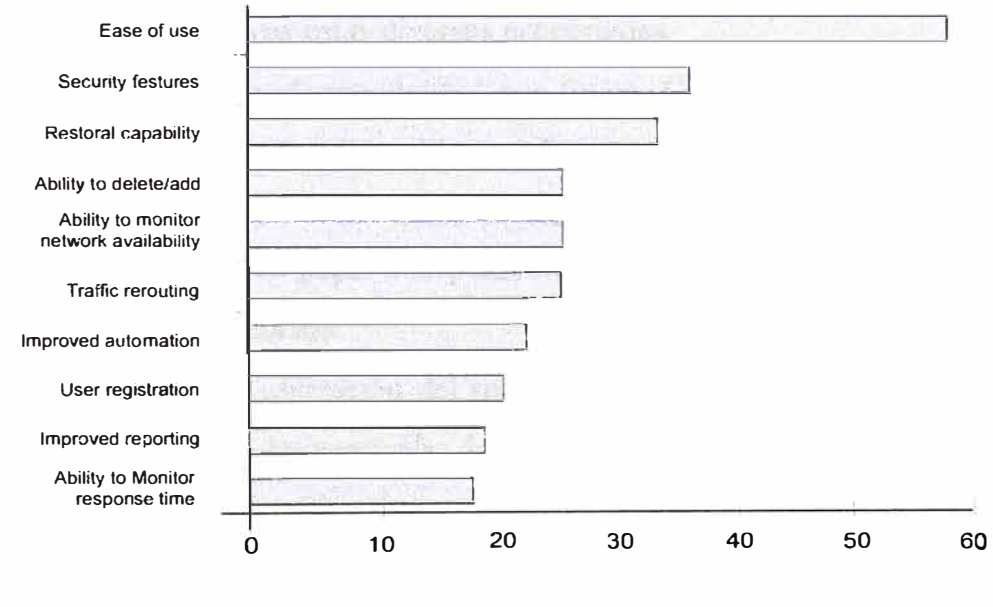


Figura 1.1 Características importantes de la gestión de red

Otra composición de requisitos de usuarios es proporcionada en (Terplan 1992), el cual lista lo siguiente como fuerzas motrices principales para justificar una inversión en la gestión de red:

- *Control Corporativo de activos estratégicos:* Las redes y los recursos distribuidos de computación son recursos progresivamente vitales para la mayoría de organizaciones. Sin control efectivo, estos recursos no proveen el retorno que la gestión corporativa requiere.

- *Control de complejidad:* El crecimiento sostenido del número de componentes de la red, usuarios finales, interfaces, protocolos, y fabricantes amenaza la gestión con perder el control sobre lo que está conectado a la red y cómo los recursos de red son usados.
- *Mejora de servicio:* Los usuarios finales esperan lo mismo o servicios mejorados conforme los recursos de cómputo e información crecen y se distribuyen en la organización.
- *Balance de necesidades diversas:* La información y recursos de cómputo de una organización deben ser puestas al alcance de un espectro de usuarios finales con aplicaciones diversas a un nivel dado de soporte, con requisitos específicos en las áreas de desempeño, disponibilidad, y seguridad. El gestor de la red debe asignar y controlar los recursos para balancear estas diversas necesidades.
- *Reducción del periodo de inactividad por fallas:* Como los recursos de red de una organización se convierten en requisitos cada vez más importantes, los requerimientos mínimos de disponibilidad se acercan al 100 por ciento. Además de diseño redundante, la gestión de red tiene un papel indispensable que desempeñar, asegurando la mas alta disponibilidad de sus recursos.
- *Control de costos:* La utilización del recurso debe ser monitoreada y controlada para responder a las necesidades esenciales de usuarios finales a costos razonables.

En la figura 1.2 podemos identificar las causas de la no utilización de la capacidad completa de la red, las acciones de la gestión de red estarán orientadas a mejorar la disponibilidad de la red y a incrementar su efectividad.

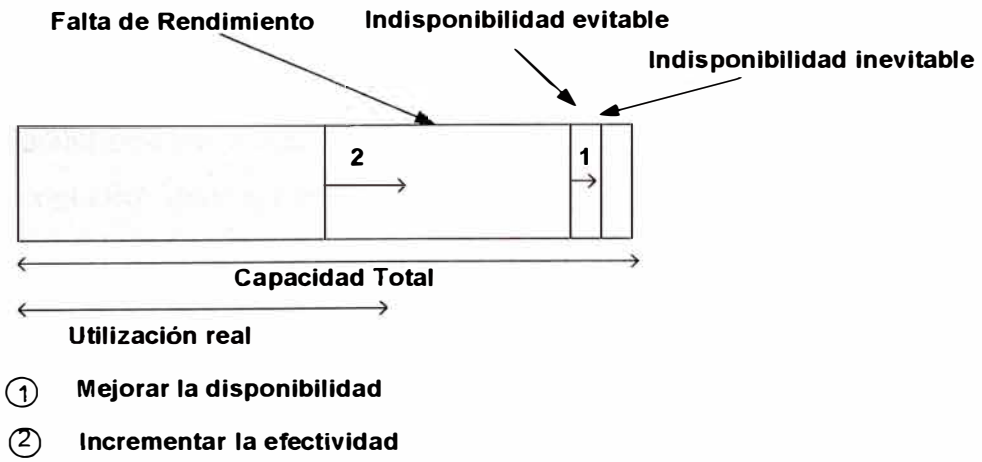


Figura 1.2 Objetivos de gestión de red

Aún cuando tales encuestas y citas cualitativas son útiles y pueden guiar en desarrollar los detalles para una facilidad de gestión de red, una composición funcional de requisitos es necesaria para estructurar el proceso global del diseño. Tabla 1.1 lista las áreas funcionales claves de gestión de red tal como lo definió la organización Internacional para la estandarización (ISO). Aunque esta clasificación funcional fueron desarrolladas para el entorno OSI, ha ganado amplia aceptación en los fabricantes de sistemas de gestión de red estandarizadas y propietarios.

TABLA 1.1. Áreas Funcionales de Gestión OSI

Gestión de Fallas

Las facilidades que posibilitan la detección, aislamiento, y la corrección de operación anormal del entorno OSI.

Gestión de Cuentas.

Las facilidades que posibilitan cargos a ser establecidos por el uso de objetos gestionados y costos a ser identificados por el uso de esos objetos gestionados.

Gestión de Nombre y Configuración.

Las facilidades que ejercen el control, identificación, recolección de datos, y proveen datos para objetos gestionados con el propósito de asistir en proveer operación continua de servicios de interconexión.

Gestión de Desempeño.

Las facilidades necesarias para evaluar el comportamiento de los objetos gestionados y la efectividad de actividades de comunicación.

Gestión de Seguridad.

Las facilidades que identifican los aspectos de seguridad OSI esenciales para operar la gestión de red OSI correctamente y proteger objetos gestionados.

1.1.1 Gestión de Fallas

a) Visión General.

Para mantener la operación correcta de una red compleja, un gestor de red debe tener cuidado en considerar el sistema como un todo, y cada componente esencial individualmente, y que estén en un orden de funciones apropiadas. Cuando una falla ocurre, para el gestor de red, es importante tan rápido como sea posible:

- Determinar exactamente donde esta el defecto
- Aislar la falla del resto de la red de modo que pueda continuar funcionando sin interferencia.
- Reconfigurar o modificar la red de tal manera que se minimice el impacto de operación sin el (los) componente (s) fallado(s).
- Reparar o reemplazar el (los) componente(s) fallado(s) para restituir la red a su condición inicial.

Tan importante como la definición de gestión de fallas, es el diferenciar fallas de errores. Una falla es una condición anormal que requiere atención de gestión (o la acción) para repararla, mientras que un error es solo un evento. Una falla es usualmente la imposibilidad de operar correctamente o con errores excesivos. Por ejemplo, si una línea de comunicaciones es fisicamente cortado, entonces ninguna señal puede ser recibida. O una corrugación en el cable puede causar distorsiones fuera de control tal que haya una alta tasa de errores persistentemente. Ciertos errores (Ejemplo: Un único error de bit en una línea de comunicación) puede ocurrir ocasionalmente y normalmente no será considerado falla. Se logra usualmente sobreponerse a errores usando los mecanismos de control de error de los protocolos de comunicaciones diversos.

b) Requerimientos de Usuario.

Los usuarios finales esperan soluciones a los problemas rápida y confiablemente. La mayoría de usuarios finales tolerarán una interrupción ocasional. Cuando estas interrupciones infrecuentes ocurren, sin embargo, el usuario final generalmente espera recibir notificación inmediata y tener el problema corregido inmediatamente. Proveer este nivel de resolución de falla requiere detección muy rápida, confiable y funciones de gestión de diagnóstico. El impacto y la duración de fallas también pueden ser minimizados por el uso de componentes redundantes y rutas de comunicación alternas,

para darle a la red un grado de "tolerancia a fallas." La capacidad de gestión de fallas en si misma debería ser redundante para aumentar fiabilidad de la red.

Los usuarios esperan estar informados en todo momento del estado de la red, incluyendo las actividades de mantenimiento programado y mantenimiento correctivo no programado. Los usuarios esperan tomar conocimiento de la correcta operación de la red a través de pruebas confiables o análisis de datos almacenados, registros de eventos, alertas, o estadísticas.

Después de corregir una falla y restaurar el sistema a su estado completamente operacional, el servicio de gestión de fallas debe asegurar que el problema esta verdaderamente resuelto y que no traerá nuevos problemas. Este requerimiento es llamado "rastreo y control del problema".

Al igual que con otras áreas de gestión de red, la gestión de fallas debería tener un impacto mínimo en el rendimiento de la red.

1.1.2 Gestión de Contabilización

a) Visión General.

En muchas redes corporativas, las divisiones individuales o centros de costo, aun proyectos con cuentas individuales, son cargados por el uso de servicios de red. Estos son procedimientos de contabilidad internas mas que una transferencia real de efectivo, que no obstante son importantes para los usuarios finales participantes. Además, aun si no hay tal carga de costo interno, el gestor de la red necesita poder rastrear el uso de recursos de la red por el usuario final, o clase de usuario final por un número de razones, incluyendo las siguientes:

- Los usuarios finales o grupo de usuarios finales abusan de sus privilegios de acceso y sobrecargan la red a costa de otros usuarios finales.
- Los usuarios finales pueden hacer uso ineficiente de la red, y el gestor de la red puede asistirlos cambiando procedimientos para mejorar el desempeño.
- El gestor de la red está en una mejor posición para prever el crecimiento de la red si la actividad de usuario final es conocida en detalle suficientemente.

b) Requerimientos del Usuario.

El gestor de red necesita poder especificar los tipos de información de contabilidad a ser registrados en diversos nodos, el intervalo deseado entre enviar la información registrada a los nodos de gestión del nivel más alto, y los algoritmos a ser usado en el calculo del cargo. Los reportes de cuentas deberían ser generados bajo el control del gestor de la red.

En orden a limitar el acceso a información contable, las facilidades de contabilidad deben proveer la capacidad para verificar autorización de los usuarios finales para acceder y manipular esa información.

1.1.3 Gestión de Configuración y Nombre.

a) Visión General.

Las redes de comunicación de datos modernas están compuestas de componentes individuales y subsistemas lógicos (Ejemplo., El controlador del dispositivo en un sistema operativo) que puede ser configurado para ejecutar aplicaciones diversas. El mismo dispositivo, por ejemplo, puede ser configurado para actuar ya sea como un ruteador o como un nodo de sistema final, o ambos. Una vez que está decidido cómo debe un dispositivo ser usado, el gestor de configuración puede escoger el software apropiado y el conjunto de atributos y valores (Ejemplo: Un temporizador de retransmisión de la capa de transporte) para ese dispositivo.

La gestión de configuración está relacionada con la inicialización de una red y la desactivación de una parte o la red completa. También esta relacionado con el mantenimiento, adición , y actualización de las relaciones entre componentes y el estado de los componentes mismos durante la operación de la red.

b) Requerimientos del usuario.

El arranque y las operaciones de cierre en una red son responsabilidades específicas de gestión de configuración. Esto es deseable a menudo para operaciones a ser realizadas sobre ciertos componentes; que estos sean deshabilitados (Ejemplo: Arranque o inhabilitación de una unidad de interfaz de red).

El gestor de red necesita capacidad para identificar los componentes que comprenden la red y definir la conectividad deseada de estos componentes. Esos que regularmente configuran una red con lo mismo o un conjunto similar de atributos del recurso en forma necesaria para definir y modificar atributos predeterminados y cargar estos conjuntos de atributos predefinidos en los componentes de red específicos. El gestor de la red debe poder cambiar la conectividad de componentes de la red cuando las necesidades de los usuarios finales cambien. La reconfiguración de una red es deseable a menudo en respuesta a la evaluación del desempeño o en soporte de actualizaciones de red, recuperación de fallas, o chequeos de seguridad.

Los usuarios a menudo tienen la necesidad o quieren estar informados del estado de los recursos y los componentes de la red. Por consiguiente, los usuarios finales deberían ser notificados cuando ocurren los cambios en la configuración. Los reportes de configuración pueden ser generados ya sea en alguna rutina periódica o en respuesta a solicitudes de tales informes. Antes de la reconfiguración, los usuarios finales a menudo quieren preguntar por el estado próximo de sus recursos y sus atributos.

Los gestores de la red usualmente desean sólo a usuarios finales autorizados (los operadores) para gestionar y controlar la operación de la red.

1.1.4 Gestión de desempeño.

a) Visión General.

Las redes modernas de comunicaciones de datos están compuestas de muchos y variados componentes, los cuales deben intercomunicarse y debe compartir datos y recursos. En algunos casos, es crítico para la efectividad de una aplicación que la comunicación sobre la red esté dentro de ciertos limites de rendimiento.

La gestión de rendimiento de una red de computadoras comprende dos categorías funcionales monitoreo y control. El monitoreo es la función que rastrea actividades en la red. La función de control posibilita la gestión de rendimiento para hacer ajustes, mejorar el desempeño de la red. Algunas de las interrogantes de interés para el gestor de la red relacionadas al rendimiento son como sigue:

- ¿Cuál es el nivel de utilización de la capacidad ?.
- ¿Hay tráfico excesivo?.
- ¿ Se ha reducido el rendimiento específico a niveles inaceptables?.
- ¿Hay cuellos de botella?.

- ¿Está aumentando el tiempo de respuesta?.

Para lidiar con estos cuestionamientos, el gestor de la red debe enfocarse en algún conjunto inicial de recursos a ser monitoreados, en orden a evaluar niveles de desempeño. Esto incluye asociar métricas apropiadas y valores con recursos de red relevantes como indicadores de diferentes niveles de rendimiento. ¿Por ejemplo, qué cantidad de retransmisiones en una conexión de transporte es considerada un problema de desempeño, requiriendo atención?. La gestión de desempeño, por consiguiente, debe monitorear muchos recursos para aportar información en determinado nivel operativo de red. Coleccionando esta información, analizándolo, y entonces usando el análisis resultante como retroalimentación al conjunto de valores prescritos, el gestor de la red puede llegar a ser mas diestro en el reconocimiento de situaciones indicativas de degradación presente o inminente de desempeño.

b) Requerimientos del usuario

Antes de usar una red para una aplicación particular, un usuario final puede querer saber algunas cosas como los tiempos de respuesta promedio y la confiabilidad de los servicios de red. Así el rendimiento debe ser conocido en suficiente detalle para responder consultas específicas de los usuarios finales. Los usuarios finales esperan que los servicios de red sean gestionados en una forma consistente tal que ofrecescan a sus aplicaciones en buen tiempo de respuesta.

Los gestores de red necesitan estadísticas de rendimiento para ayudarles a planear, gestionar, y mantener grandes redes. Las estadísticas de desempeño pueden usarse para reconocer potenciales sobrecargas de la red antes de que causen problemas a fin de que la acción correctiva apropiada puede ser tomada. Por ejemplo, el gestor de la red puede cambiar rutas que balanceen o redistribuyan la carga de tráfico de uso durante el embotellamiento o cuando un embotellamiento es identificado por una carga rápidamente creciente en un área. Sobre un periodo largo, la capacidad de planear basado en tal información de rendimiento pueden indicar las decisiones correctas a tomar, para ese caso, al menos con una expansión de líneas en esa área.

1.1.5 Gestión de Seguridad

a) Visión General.

La gestión de seguridad está relacionada con la gestión de protección de la información y facilidades de control de acceso. Estos incluyen: a generación,

distribución, y almacenamiento de claves de encriptación. Las contraseñas y otras autorizaciones o información de control de acceso deben ser mantenidas y distribuidas. La gestión de seguridad está también relacionada con el monitoreo y control de acceso a las redes de computadoras y a todo o parte de la información de gestión de red obtenida de los nodos de la red. Los registros de eventos (logs) son una herramienta importante de seguridad, y la gestión de seguridad esta por consiguiente muy involucrado con la recolección, almacenamiento, y examinación de registros de auditoria y eventos de seguridad, así como también con la habilitación y deshabilitacion de estas facilidades de registro.

b) Requerimientos de usuario.

La gestión de seguridad provee facilidades para la protección de recursos de la red y la información de usuario final. Las facilidades de seguridad de red deberían estar disponibles solo para usuarios autorizados. Los usuarios finales quieren saber que las políticas correctas de seguridad están aplicadas y son efectivas y que la gestión de facilidades de seguridad son en sí mismo seguros.

1.2 Sistemas de Gestión de red

Un sistema de gestión de red es una colección de herramientas para monitoreo y control de la red que esta integrada de la siguiente forma:

- Contiene una sola interfaz del operador con un potente pero amigable conjunto de comandos para realizar la mayoría de las tareas de administración de red.
- Tiene una cantidad mínima de equipos separados. Esto es, la mayoría del hardware y el software requerido para la gestión de red esta incorporada en el equipo del usuario.

Un sistema de Gestión de la red consiste de hardware y software adicional que se suma a los componentes existentes de la red. El software usado para lograr las tareas de gestión de red que reside en los computadores hosts y en los procesadores de comunicaciones (Ejemplo., Los procesadores front-end, controladores del grupo de terminales, los puentes, y los ruteadores). Un sistema de gestión de red esta diseñado para observar la red entera como una arquitectura unificada, con direcciones y etiquetas asignadas a cada punto y atributos específicos de cada elemento y enlaces conocidos al sistema. Los elementos activos de la red proveen retroalimentación regular de información de estado al centro de control de red.

1.2.1 Configuración de Gestión de red.

Figura 1.2 sugiere una arquitectura posible de un sistema de gestión de red. Cada nodo de la red contiene una colección de software asignado a la tarea de gestión de red, referida en el diagrama como una entidad de gestión de red (NME). Cada NME realiza las siguientes tareas:

- Recolecta estadísticas sobre comunicaciones y actividades relativas a la red.
- Almacena estadísticas localmente.
- Responde a comandos del centro de control de red, incluyendo comandos para: .
  1. Transmitir estadísticas recogidas para el centro de control de red.
  2. Cambiar parámetros (Ejemplo., Un temporizador usado en un protocolo de transporte).
  3. Proveer información de estado (Ejemplo., Valor de parámetros, enlaces activos).
  4. Generar tráfico artificial para realizar pruebas.

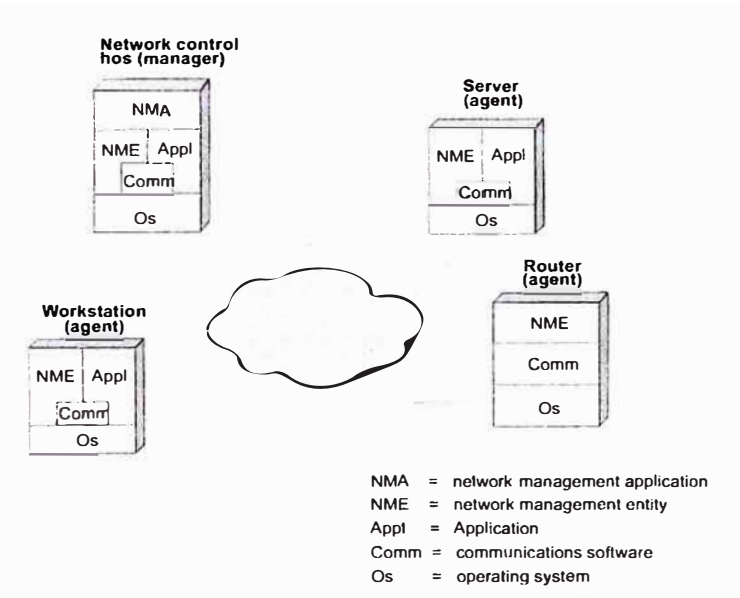


Figura 1.2 Elementos de un sistema de gestión de red

Al menos un host en la red es designado como el host de control, o administrador de red. Además del software NME, el host de control de la red incluye una colección de software denominado aplicación de gestión de red (NMA). La NMA incluye una interfaz del operador a permitir a un usuario autorizado operar la red. La NMA responde a las órdenes del usuario exhibiendo información y/o mediante el uso de comandos para el NME en toda

la red. Esta comunicación es transportada usando un protocolo de gestión de red a nivel de aplicación en la misma forma que cualquier otra aplicación distribuida.

Otros nodos en la red que son parte del sistema de gestión de red incluyen un NME que responde a las solicitudes de un sistema gestor. El NME en tales sistemas manejados es generalmente llamado módulo agente, o simplemente agente. Los agentes son implementados en sistemas finales que soportan aplicaciones de usuarios finales así también como los nodos que proveen servicios de comunicaciones, tales como procesadores frontales, conjunto de terminales, puentes, y ruteadores.

Algunas observaciones están en orden:

1. Debido a que el software de gestión de red se soporta en el sistema operativo del host y en la arquitectura de comunicaciones, la mayoría de ofertas a la fecha son diseñadas para equipamiento de un solo vendedor. Los últimos años han visto el surgimiento de sistemas de gestión de red estándar diseñados para administrar una red conteniendo equipos de diferentes fabricantes.
2. Como se muestra en la Figura 1.2, el host de control de la red comunica y controla los NMEs en otros sistemas.
3. Para mantener alta disponibilidad de la función de gestión de red, dos o más hosts de control de red son usados para controlar la red. En operación normal, uno de los centros esta sin uso o simplemente recolectando estadísticas, mientras el otro es usado para control. Si el host de control de red primario falla, el sistema del respaldo puede ser usado.

1.2.2 Arquitectura del Software de Gestión de red.

La arquitectura actual del software de gestión de red de un gestor agente varía generalmente, dependiendo de la funcionabilidad de la plataforma y los detalles de la capacidad de gestión de red. Figura 1.3 presenta una vista genérica de tal arquitectura. El software puede ser dividido en tres amplias categorías:

- software de presentación de usuario.
- software de gestión de red.
- software de comunicaciones y base de datos de soporte.

a) Software de Presentación del usuario.

La interacción entre un usuario de gestión de red y el software de gestión de red tiene lugar a través de una interfaz del usuario. Tal interfaz es necesaria en cualquier sistema administrador, para permitir a un usuario monitorear y controlar la red. También puede ser útil tener tal interfaz en algunos sistemas agente para los propósitos de prueba y depurado y para permitir algunos parámetros a ser observado o fijados localmente.

La clave para un sistema efectivo de gestión de red es una interfaz del usuario *unificada*. La interfaz debería ser el mismo en cualquier nodo, a pesar del fabricante. Esto permite a un usuario manejar una configuración heterogénea con un mínimo de entrenamiento.

Un peligro en cualquier sistema de gestión de red es la sobrecarga de información. Es posible para instrumentar una configuración que gran cantidad de información esté disponible para el usuario administrador de red. Las herramientas de presentación son necesarias para organizar, resumir, y simplificar esta información lo más posible. Idealmente, se da énfasis a presentaciones gráficas en vez de salidas textuales o tabulares.

b) El software de Gestión de red.

El software que específicamente provee la aplicación de gestión de red puede ser muy simple, como en el caso de SNMP, o muy complejo, como en caso de la gestión de sistemas OSI. La caja central en la figura 1.3 muestra más bien una estructura compleja que refleja la arquitectura de gestión de sistemas OSI y también sugiere un sistema de gestión de red propietario típica.

El software de gestión de red de la Figura esta organizado en tres capas. La capa más alta consiste de una colección de aplicaciones de gestión de red que proveen los servicios de interés para los usuarios. Por ejemplo, estas aplicaciones podrían corresponder a las áreas funcionales de la gestión OSI: gestión de fallas, gestión de contabilidad, gestión de configuración, gestión de desempeño, y gestión de seguridad.

Cada aplicación cubre un área amplia de gestión de red y debería exhibir consistencia sobre varios tipos de configuraciones, aunque pueden haber diferencias dependiendo de la naturaleza de las conexiones de red (por ejemplo, LAN, WAN, T1, multiplexores).

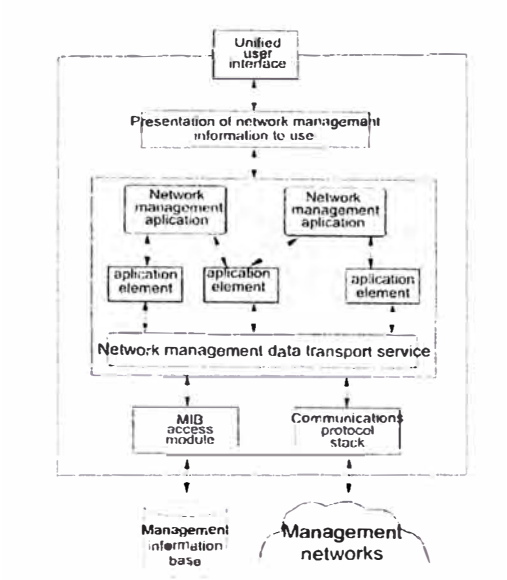


Figura 1.3 Modelo arquitectural de un sistema de gestión de red.

El pequeño número de aplicaciones de gestión de red es soportado por un número mayor de elementos de aplicación. Esos son módulos que implementan primitivas y funciones de gestión generales tales como generar alarmas o resumir datos. Los elementos de aplicación implementan herramientas básicas que son necesarias para unas o más de las aplicaciones de gestión de red. Organizando el software en términos de elementos de aplicaciones y siguiendo principios de diseño modulares tradicionales y posibilitan una implementación más eficiente a ser desarrollado basado en rehúso de software.

El nivel más bajo del software específico de gestión es un servicio de transporte de datos de gestión de red. Este módulo consta de un protocolo de gestión de red usado para intercambiar información de gestión entre administradores y agentes y una interfaz de servicio para los elementos de aplicación. Típicamente, la interfaz de servicio provee funciones muy primitivas, tales como obtener información, fijar parámetros, y generar notificaciones.

c) Software de Soporte de Gestión de red.

Para realizar sus funciones indicadas, el software de gestión de red necesita acceso a una base de información de gestión (MIB) local y agentes remotos y administradores. El MIB local en un agente contiene información de uso, para la gestión de red, incluyendo información que refleja la configuración y comportamiento de este nodo, y los parámetros que pueden usarse para controlar la operación de este nodo. El MIB local en el administrador contiene información específica del nodo así como también tal información sumaria acerca de los agentes bajo el control del administrador. El módulo

de acceso MIB incluye software básico de gestión de archivos que posibilita el acceso a la MIB. En suma el módulo de acceso puede necesitar convertir del formato local MIB a un formato que es estándar a través del sistema de gestión de red.

Las comunicaciones con otros nodos (los agentes y los administradores) son soportados por una pila de protocolos de comunicaciones, tales como OSI o la pila TCP/IP. La arquitectura de comunicaciones así soporta el protocolo de gestión de red, que esta a un nivel de aplicación.

1.2.3 Gestión de red distribuida.

La configuración mostrada en la Figura 1.2 sugiere una estrategia centralizada de gestión de red, con un solo centro de control de la red y quizá un centro de relevo. Esto es la estrategia que ambos vendedores de MainFrames y ejecutivos de sistemas de información tradicionalmente han favorecido. Un sistema centralizado de gestión de red significa control central. En el mismo sentido que en una configuración dominada de computadora central (MainFrame), donde los recursos cruciales residen en un centro de computo y el servicio es provisto para los usuarios remotos. La estrategia también se hace extensivo para los administradores responsables de los activos del sistema de información total de una organización. Un sistema centralizado de gestión de red habilita al administrador a mantener el control sobre la configuración entera, balanceando recursos contra necesidades y optimizando la utilización global de recursos.

Sin embargo, tal como un modelo de cómputo centralizado ha dejado paso a una arquitectura de computación distribuida, con aplicaciones desplazadas de los centros de datos a departamentos remotos, la gestión de red está también llegando a ser distribuida. Los mismos factores entran en juego: la proliferación de PCs de alta potencia y bajo costo y estaciones de trabajo; el amplio uso común de LANs departamentales; y la necesidad de control local y optimización de aplicaciones distribuidas.

Un sistema distribuido de gestión reemplaza al centro de control de red único con estaciones de trabajo interoperable, localizadas en LAN´s distribuidas en toda la empresa. Esta estrategia da a los administradores de nivel departamental, quienes deben observar sobre aplicaciones reducidas de tamaño y PC sobre las LAN, las herramientas que necesitan para mantener redes ágiles, sistemas, y aplicaciones para sus usuarios finales locales. Para prevenir la anarquía, una arquitectura *jerárquica* es típicamente usada, con los siguientes elementos:

- Las estaciones de gestión distribuidas tienen acceso limitado dado para monitorear y controlar la red, usualmente definidas por los recursos departamentales que ellos sirven.
- Una estación central y su respaldo, tienen derechos de acceso globales y la habilidad para manejar todos los recursos. También puede interactuar con estaciones de gestión menos capaces para monitorear y controlar sus operaciones.

Manteniendo la capacidad de control central, la aproximación distribuida ofrece un número de beneficios:

1. El sobre tráfico de gestión de red es minimizado. La mayor parte del tráfico esta confinado al entorno local.
2. La gestión distribuida ofrece mayor escalabilidad. Añadir capacidad adicional de gestión es simplemente una cuestión de desplegar otra estación de trabajo barata en la localización deseada.
3. El uso de múltiples estaciones en red elimina el único punto de falla que existe con esquemas centralizados.

La Figura 1.4 ilustra la estructura básica usada por la mayoría de sistemas de gestión de red distribuidos existentes hoy en el mercado. Los clientes de gestión están más cercanos a los usuarios. Estos clientes dan acceso a los usuario a los servicios de gestión e información y proveen una interfaz gráfica del usuario fácil de usar. Dependiendo de los privilegios de acceso, una estación de trabajo cliente puede acceder a uno o más servidores de administración. Los servidores de gestión que son el corazón del sistema. Cada servidor soporta un conjunto de aplicaciones de gestión y una base de información de gestión (MIB). También almacenan modelos comunes de datos de gestión e información de gestión de rutas para las aplicaciones y los clientes. Esos dispositivos a ser administrados que comparten los mismos protocolos de gestión de red como los servidores de gestión contienen agente software y son administrados directamente por uno o mas servidores de gestión. Para otros dispositivos, los servidores de gestión pueden alcanzar los recursos sólo a través de un administrador de elementos de un vendedor específico, o el *Proxy*. El concepto de Proxy es explorada en la siguiente sección.

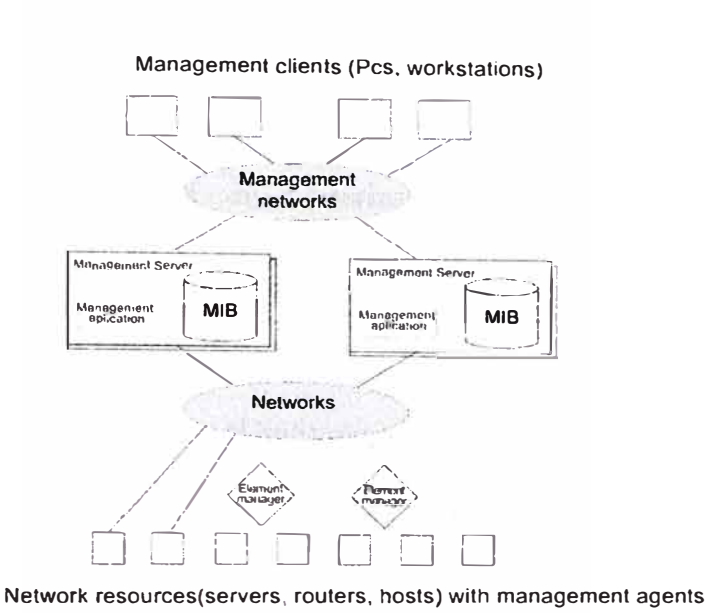


Figura 1.4 Arquitectura típica de un Sistema de gestión distribuido

La flexibilidad y la escalabilidad del modelo de gestión distribuido son evidentes en la Figura 1.4. Como los recursos adicionales son añadidos a la configuración, cada uno está equipada con el software agente o enlazado a un Proxy. En un sistema centralizado, este crecimiento eventualmente podría sobrecargar a una estación central. Pero en un sistema distribuido, los servidores adicionales de gestión y las estaciones de trabajo cliente pueden agregarse para cubrir los recursos adicionales. Además, el crecimiento de la configuración global ocurrirá en una forma estructurada (Ejemplo., Añadiendo a una LAN adicional con un número de PCs en red); el crecimiento del sistema de gestión refleja este crecimiento subyacente del recurso, con servidores y los clientes añadidos donde los recursos nuevos están ubicados.

1.3 Proyecto de Gestión de Red

La realización de un proyecto de gestión de red consta de dos partes, un enfoque de negocio y otro técnico. El enfoque de negocio recoge los requerimientos que la empresa tiene con respecto a las facilidades de red, como cada uno de los procesos de negocio se soporta en los diferentes servicios que esta provee, identifica los procesos de negocio críticos, y su dependencia de los recursos de red, el nivel de dependencia de los procesos de

negocio con los recursos de red nos indicará si los servicios de mantenimiento deberán ser realizados por personal de planta de la empresa o deberán ser tercerizados. Una baja dependencia dan la posibilidad de tercerizar los servicios, una alta dependencia recomendaría que los servicios de gestión de red deberían hacerse por parte de la misma empresa.

La figura 1.5 muestra un diagrama del desarrollo de un proyecto de gestión de red, se muestra las acciones a realizarse en el enfoque de negocio y el enfoque técnico.

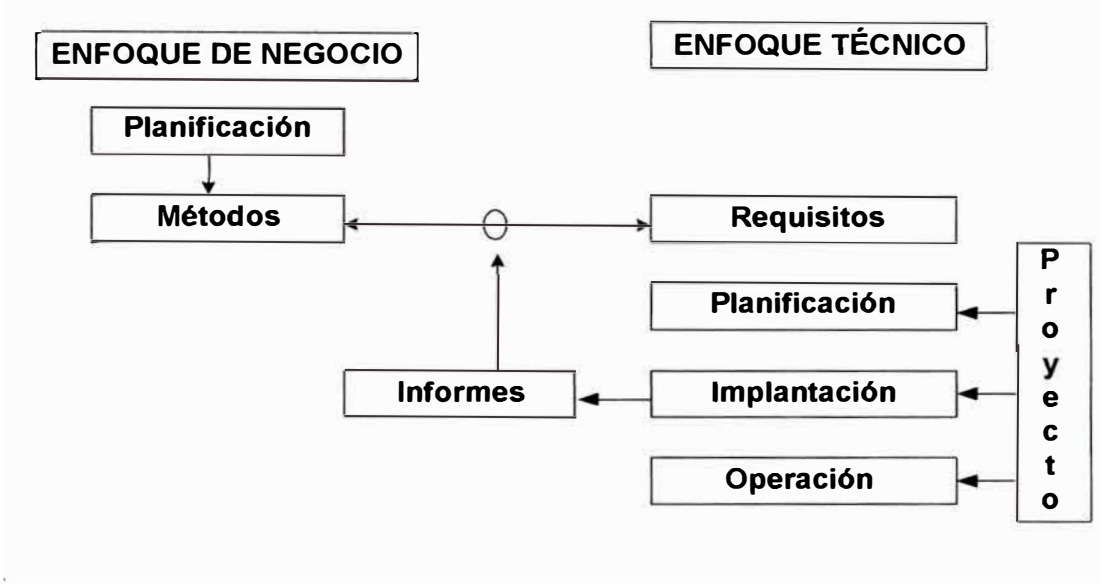


Figura 1.5 Proyecto de gestión de red

El enfoque técnico parte de los requerimientos de gestión, estos están constituidos por un conjunto de requisitos globales tales como los servicios que serán brindados (conexión a bases de datos, correo electrónico, transferencia de archivos, acceso a Internet vía WWW, así como las calidades objetivo (disponibilidad del 98%, tiempo de respuesta menor de 2 segundos, etc.). Guiados por esto se realiza la planificación en el cual se dispondrá de todo lo necesario para una gestión efectiva y eficiente. En esta fase se contempla la identificación de todos los elementos a utilizarse y la conformación del sistema de gestión de red: hardware, software, recursos humanos, procesos de gestión, operaciones de gestión y el presupuesto. También los detalles como el direccionamiento de los dispositivos de red gestionados y gestores, autenticación para la gestión, manual de operaciones.

La implantación esta relacionada con la instalación y configuración del sistema de gestión en la estación gestora, inicialización de los componentes gestionados del sistema, así como la distribución de funciones y responsabilidades del staff de gestión de red.

La operación esta relacionada con las tareas de gestión de red, como el monitoreo, resolución de fallas mediante cambios de equipos o cambios en la configuración de los mismos.

Todo proyecto de gestión de red implicará: recursos humanos (tales como operadores, gestores, analistas y planificadores), Procesos y procedimientos, herramientas.

1.4 Recursos Humanos

a.- Operadores

Soporte a usuarios (Help Desk): Recepción de incidencias reportados por el usuario final, asistencia inicial.

Soporte Técnico:

- Recogida y evaluación de alarmas.
- Recogida de datos sobre prestaciones y utilización
- Diagnosis dirigida de problemas.
- Arranque y parada de los componentes de red.
- Ejecución programada de pruebas preventivas.
- Modificación de configuraciones.
- Carga de nuevas versiones de software.

b.- Administradores

Control de Operadores: Herramientas de Seguimiento de Incidencias que permitan conocer el estado actual de incidencias y elaborar informes de actividad operacional para su posterior análisis.

- Gestión de inventario.
- Gestión de configuraciones
- Gestión de contabilidad
- Gestión de seguridad: control de acceso, etc.
- Mantenimiento de registro histórico de problemas.
- Evaluación de tráfico y calidad de servicio actuales

c.- Analistas

Su objetivo es garantizar la calidad de servicio

- Definición de indicadores de prestaciones: calidad de servicio.
- Análisis global de la calidad de servicio.
- Toma de decisiones para corregir desviaciones de la calidad de servicio.
- Preparación de procedimientos de operadores y administradores

d.- Planificadores

Decisiones dependientes del negocio al que se dedica la empresa

- Análisis de informes técnico – económicos (anuales).
- Establecimiento de política de telecomunicaciones
- Asignación de presupuesto.
- Selección de criterios de distribución de costes o facturación

1.5 Procesos y procedimientos

Con respecto a los aspectos funcionales de la gestión de red podemos notar que no existe funcionalidad común. Depende del tipo de red gestionada, tipo de equipos gestionados, objetivos específicos de la gestión de red. A bajo nivel, todos los métodos se basan en monitorización y control de red.

1.5.1 Monitorización de red

El componente de monitorización de red de la gestión de red esta comprometido con la observación y el análisis del estado y comportamiento de los sistemas finales, sistemas intermedios, y subredes que construyen la configuración a ser administrada.

(Chiu y Sudama 1991) sugieren que el monitoreo de red consiste de tres áreas de diseño principales:

- Acceso a información de monitoreo: como definir información de monitoreo, y como obtener esa información desde un recurso para un gestor.
- Diseño de mecanismos de monitoreo: como obtener mejor información de los recursos.
- Aplicación de la información monitoreada: como la información monitoreada es usada en las diversas áreas funcionales de gestión.

a) Arquitectura de monitorización de red

Antes de considerar el diseño de un sistema de monitorización de red, es mejor considerar el tipo de información que es de interés para un monitor de red. Luego podemos observar las alternativas para la configuración de las funciones de monitorización de la red.

1) Información de monitorización de la red

La información que debería estar disponible para monitorización de la red puede ser clasificada como sigue:

- Estática: Esta es información que caracteriza la configuración actual y los elementos en la actual configuración, tal como el número e identificación de puertos en un ruteador. Esta información cambiará con poca frecuencia.
- Dinámica: Esta información esta relacionada a eventos en la red, tal como un cambio de estado de un protocolo o la transmisión de paquetes sobre una red.
- Estadística: Esta es la información que puede ser derivada de información dinámica, tal como el número promedio de paquetes transmitidos por unidad de tiempo por un sistema final.

Un ejemplo de una estructura de información, para usar en sistemas de monitorización de tiempo real, es sugerido en (Mazumdar y Lazar 1991). En este esquema, la base de datos estática tiene dos componentes principales: una base de datos de configuración con información básica acerca del computador y elementos en red, y una base de datos sensor, con información acerca de sensores usados para obtener lecturas en tiempo real. La base de datos dinámica esta primariamente comprometido con la recolección de información acerca del estado de diferentes elementos de red y eventos detectados por los sensores. La base de datos estadística incluye medidas agregadas útiles. La figura 2.1 sugiere la relación entre esos componentes.

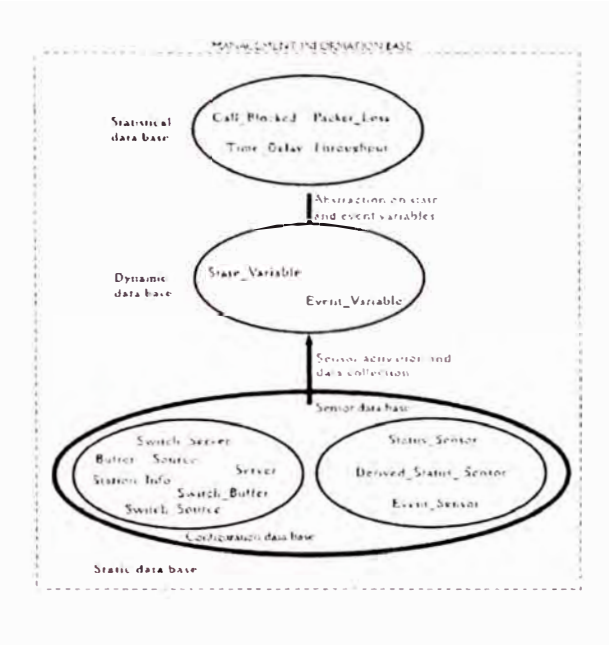


Figura 1.6 Organización de una Base de Información de Gestión.

La naturaleza de la información monitoreada tiene implicaciones como donde es recolectado y almacenado para propósitos de monitorización. La información estática es típicamente generada por los elementos involucrados.

Así un ruteador mantiene su propia información de configuración. Esta información puede ser hecha disponible directamente a un monitor si el elemento tiene el software agente apropiado. Alternativamente, la información puede ser hecha disponible a un Proxy que en respuesta hará disponible a un monitor.

Demasiada información dinámica, generalmente es recolectada y almacenada por elemento de red responsable por los eventos subyacentes. Sin embargo, si un sistema esta conectada a una LAN, entonces muchos de sus actividades pueden ser observadas por otro sistema en la LAN. El termino monitor remoto refiere a un dispositivo sobre una LAN que observa todo el tráfico en la LAN y recolecta información acerca de ese tráfico. Por ejemplo, el número total de paquetes usados por un elemento en la LAN podría ser registrado por el mismo elemento o por un monitor remoto que esta escuchando en la misma LAN. Alguna información dinámica, sin embargo, puede ser generado solo por el mismo elemento, tal como el número actual de conexiones del nivel de red.

Información estadística puede ser generada por cualquier sistema que tiene acceso a la información dinámica. La información estadística podría ser generado atrás en el mismo monitor de red. Esto requeriría que todos los datos sin procesar, sea transmitida al monitor, donde sería analizado y resumido. Si el monitor no necesita acceder a todos los datos sin procesar, entonces el tiempo de procesamiento del monitor y la capacidad de la red podría ser ahorrada si el sistema que contiene los datos dinámicos resumen y envían los resultados al monitor.

2) Configuración de la monitorización de red

La figura 1.7, basado en un grafico en (Chiu y Sudama 1992), se ilustra la arquitectura para la monitorización de red en términos funcionales. Parte (a) de la figura muestra los cuatro principales componentes de un sistema de monitorización de red:

- Aplicación de monitorización: Este componente incluye las funciones de monitorización de red que son visibles a los usuarios, tales como monitorización de rendimiento, monitorización de fallas, y monitorización de contabilidad.
- Función de gestor: Este es el módulo en el monitor de red que realiza las funciones de monitorización básica de recuperación de información desde otros elementos de la configuración.
- Función de agente: este módulo recolecta y registra información de gestión para uno o más elementos de red y comunica la información al monitor.

- Objetos gestionados: Esto es la información de gestión que representa recursos y sus actividades.
- Agente de monitorización: Este modulo genera resúmenes y análisis estadístico de información de gestión. Si es remoto desde el gestor, este modulo actúa como un agente y comunica la información resumida al gestor.

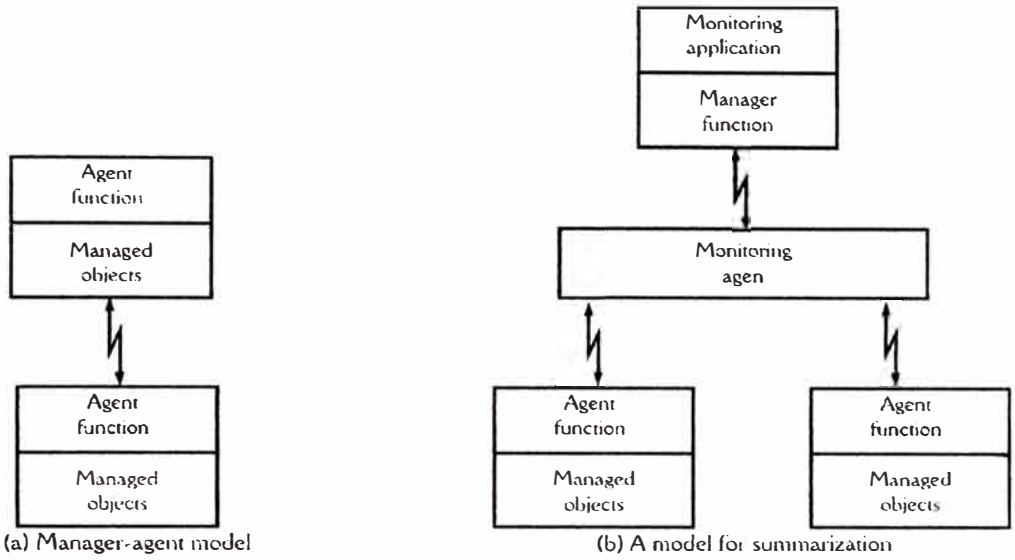


Figura 1.7 Arquitectura funcional para la monitorización de red

Esos módulos funcionales pueden ser configurados en un número de formas. Las estaciones que alojan las aplicaciones de monitorización son en si mismos elementos de red y sujetos a monitorización. Así, el monitor de red generalmente incluye software agente y un conjunto de objetos gestionados (figura 1.8 (a)). De echo es vital, para el monitor el estado y el comportamiento del monitor de red para asegurar que continua realizando su función y que evalúa la carga sobre si mismo y sobre la red. Un requerimiento clave es que el protocolo de gestión de red sea instrumentado para monitorear la cantidad de tráfico de gestión de red dentro y fuera del monitor de red.

La figura 1.8 (b) ilustra la configuración más común para la monitorización de otros elementos de red. Esta configuración requiere que el gestor y sistemas

agentes compartan el mismo protocolo de gestión de red y MIB (Base de Información de Gestión) sintaxis y semántica.

Un sistema de monitorización de red puede incluir también uno o más agentes que monitorean tráfico sobre una red. Esos son a menudo referidos como monitores externos o remotos; la configuración es mostrada en la figura 1.8(c).

Finalmente, como fue discutido en la sección 1.2.4, para elementos de red que no comparten un protocolo de gestión de red común con el monitor de red, un agente Proxy es necesario (figura 1.8(d)).

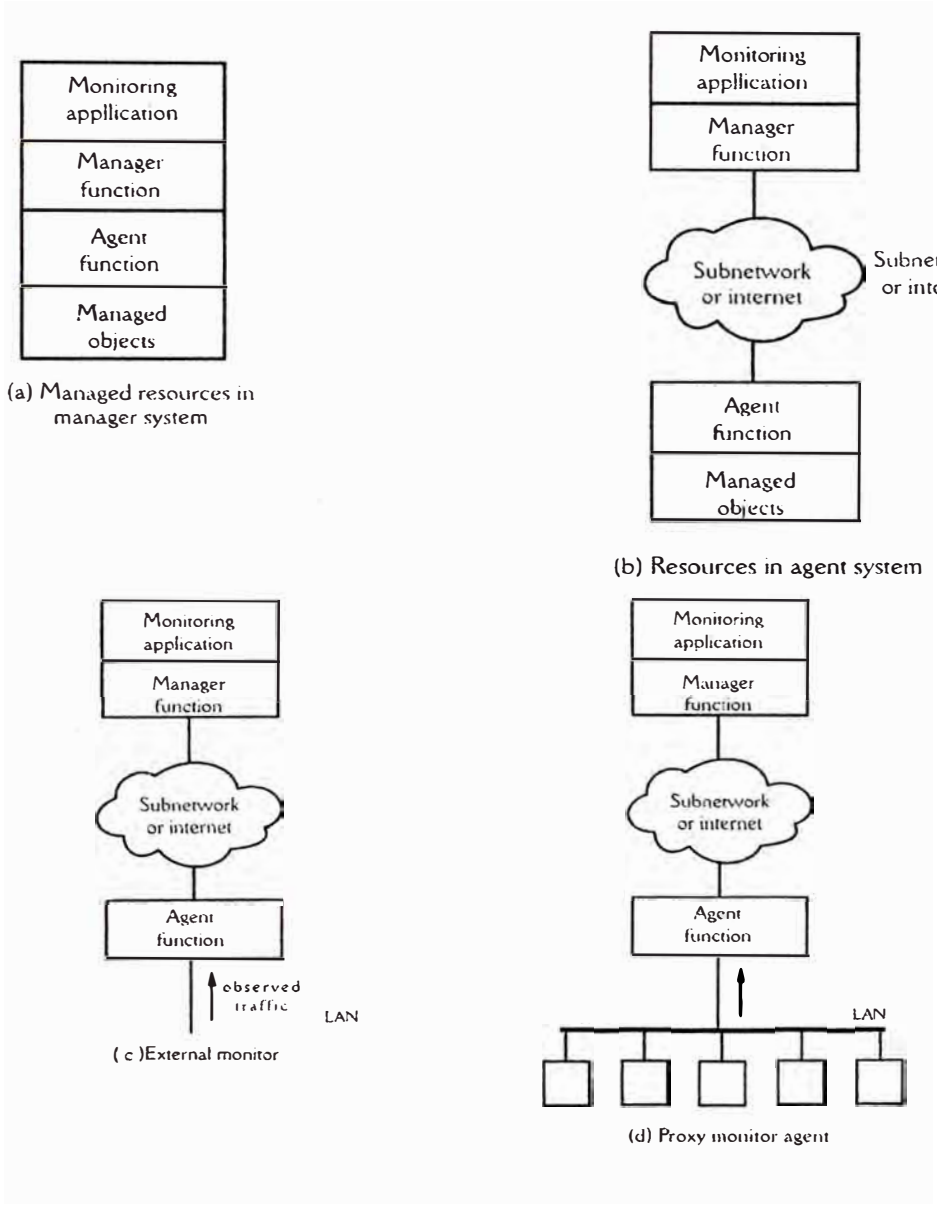


Figura 1.8 Configuraciones de Monitorización de red

3) Sondeo y reporte de eventos

La información que es útil para la monitorización de la red es recolectada y almacenada por agentes y hecho disponibles a uno o más sistemas gestores. Dos técnicas son usadas para hacer que información del agente sea disponible para el gestor: sondeo y reporte de eventos.

Sondeo es una interacción solicitud- respuesta entre un gestor y agente. El gestor puede consultar cualquier agente (para el cual este tenga autorización) y solicitar los valores de diferentes elementos de información; el agente responde con información de su MIB. La solicitud puede ser especifica, listado de uno o mas variables nombradas. Una solicitud puede también ser de naturaleza de una búsqueda, preguntando al agente por reporte de información que cumple ciertos criterios, o para suministrar al gestor con información acerca de la estructura de la MIB en el agente. Un sistema gestor puede usar sondeo o aprender acerca de la configuración que esta administrando, para obtener periódicamente una actualización de condiciones, o para investigar un área en detalle después de ser alertado por un problema. El sondeo también es usado para generar un reporte para ayudar a un usuario y para responder a consultas especificas de usuario.

Con reporte de eventos, la iniciativa es del agente y el gestor en el rol de un oyente, esperando por la llegada de información. Un agente puede generar un reporte periódicamente para dar al gestor su estado actual. El periodo de reporte puede ser pre configurado o fijado por el gestor.

Un agente puede también generar un reporte cuando ocurre un evento significativo (ejemplo, un cambio de estado) o un evento inusual (ejemplo una falla). Reporte de eventos son útiles para detectar problemas tan pronto como ocurran. Es mas eficiente que sondeo para la monitorización de objetos cuyos estados o valores cambian con relativa baja frecuencia.

Ambos sondeo y reporte de eventos son útiles, y un sistema de monitorización de red típicamente empleará ambos métodos. El énfasis relativo fijado en los dos métodos varía grandemente en sistemas diferentes. Los sistemas de gestión de telecomunicaciones han tradicionalmente fijado una muy alta dependencia en reporte de eventos. En contraste, la aproximación SNMP pone muy poca dependencia en reporte de eventos. Los sistemas de gestión OSI tienden a caer en

algún lugar entre esos dos extremos. Sin embargo, sistemas de gestión SNMP y OSI, también la mayoría de esquemas propietarios, permiten al usuario considerable libertad en la determinación del énfasis relativo en las dos aproximaciones. La elección del énfasis depende de un número de factores, incluyendo los siguiente:

- La cantidad de tráfico de red generado por cada método
- Robustez en situaciones críticas
- El tiempo de retardo en la notificación al gestor de red
- La cantidad de procesamiento en el dispositivo administrado
- La negociación de transferencia confiable versus no confiable
- Las aplicaciones de monitorización de red que están siendo soportadas
- Las contingencias requeridas en caso que un dispositivo notifique fallas antes de enviar un reporte.

b) Monitorización de rendimiento

1) Indicadores de rendimiento

Un pre-requisito absoluto para la gestión de una red de comunicaciones es la habilidad para medir el rendimiento de la red, o monitorización de rendimiento. No podemos esperar gestionar y controlar un sistema o actividad a menos que podamos monitorear su rendimiento. Una de las duras dificultades del gestor de red esta en la elección y uso de los indicadores apropiados que miden el rendimiento de la red. Entre los problemas que pueden aparecer están los siguientes:

- Hay demasiados indicadores en uso
- El significado de la mayoría de indicadores no son claramente entendidos
- Algunos indicadores son introducidos y soportados solo por algunos fabricantes.
- La mayoría de los indicadores no están disponibles para la comparación con otros.
- Frecuentemente, los indicadores son precisamente medidos pero incorrectamente interpretados.

- En muchos casos, el calculo de indicadores toma demasiado tiempo, y el resultado final puede dificultosamente ser usada para el control del entorno.

En esta sección, daremos algunas ideas generales de los tipos de indicadores que son útiles para la gestión de red. Esos caen dentro de dos categorías: medidas orientadas a servicios y medida orientadas a eficiencia; la tabla 1.2, basado en (Terplan 1992), da una división de los principales indicadores en cada categoría. El principal medio de juzgar si una red esta cumpliendo sus requerimientos es que los niveles de servicios especificados sean mantenidos para la satisfacción de los usuarios. Así, los indicadores orientados a servicio son los de prioridad más alta. El gestor esta también comprometido con el logro de esos requerimientos al menor costo, por esta razón la necesidad de mediciones orientadas a eficiencia.

Tabla 1.2 Indicadores de rendimiento de red

Orientados a servicio	
Disponibilidad	El porcentaje de tiempo que un sistema de red, un componente, o una aplicación esta disponible para el usuario.
Tiempo de respuesta	Cuanto tiempo toma para que una respuesta aparezca en el Terminal después que el usuario realizo una invocación desde este.
Precisión	El porcentaje de tiempo que no ocurren errores en la transmisión y entrega de información.
Orientados a servicio	
Throughput	La tasa al cual ocurre eventos orientados a aplicación (ejemplo: mensajes de transacción, transferir archivos).
Utilización	El porcentaje de la capacidad teórica de un recurso que esta siendo usado (ejemplo: multiplexores, líneas de transmisión. Conmutadores).

1. Disponibilidad

La disponibilidad puede ser expresada como el porcentaje de tiempo que un sistema de red, componentes, o aplicaciones están disponibles para un usuario. Dependiendo de la aplicación, alta disponibilidad puede ser significativo. Por ejemplo, en una red de reservaciones de una aerolínea un minuto de fuera de servicio puede causar $10000 en perdidas; en una red bancaria, una hora de fuera de servicio puede introducir perdidas en el orden de millones de dólares.

La disponibilidad esta basado en la confiabilidad de los componentes individuales de una red. La confiabilidad es la probabilidad que un componente realizará su función especificada en un tiempo especificado bajo condiciones especificadas. La falla de componentes es usualmente expresado mediante el tiempo promedio entre fallas (MTBF). La disponibilidad, A, puede ser expresado como:

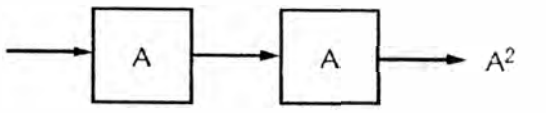
$$A = MTBF/(MTBF+MTTR)$$

Donde MTTR es el tiempo medio de reparación luego de la falla.

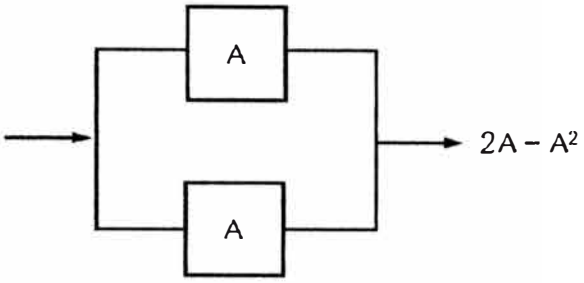
La disponibilidad de un sistema depende de la disponibilidad de sus componentes individuales mas la organización del sistema. Por ejemplo, algunos componentes pueden ser redundantes, tal que la falla de un componente no afecta la operación del sistema. O la configuración puede ser tal que la perdida de un componente resulta en la reducción de la capacidad, pero el sistema esta aún funcionando.

La figura 2.4 muestra dos simples configuraciones. En la parte (a), dos componentes están conectados en serie, y ambos deben funcionar apropiadamente para la función en cuestión a ser disponible. Por ejemplo, esos podrían ser dos módems en los extremos opuestos de un enlace de comunicaciones. Cuando dos componentes son conectados en serie, en esta forma, entonces la disponibilidad de la combinación es A^2 , si la disponibilidad de cada componente es A. Así si la disponibilidad de cada MODEM es 0.98, entonces la disponibilidad del enlace con los dos módems es 0.98*0.98 = 0.96. La segunda parte de la figura muestra dos dispositivos en paralelo. Por ejemplo, esos podrían ser dos enlaces conectando un Terminal a un host;. Si un enlace falla, el otro es automáticamente usado de

respaldo. En este caso, el enlace dual esta indisponible solo si ambos enlaces individuales están indisponibles. Si la disponibilidad de cada enlace es 0.98, entonces la probabilidad que uno de ellos este indisponible es 1-0.98=0.02. La probabilidad que ambos estén indisponibles es 0.02*0.02 = 0.004. Así la disponibilidad de la unidad combinada es 1-0.004=0.996.



(a) Serial



(b) Parallel

El análisis de disponibilidad llega a ser mas o menos compleja conforme la configuración llega a ser más complicada y conforme tenemos en cuenta no solo la disponibilidad de los componente sino también la carga esperada en el sistema. Como ejemplo, considere un sistema de enlace dual, tal como es mostrado en la figura 2.4(b). Los dos enlaces son usados para conectar un multiplexor a un sistema host. Durante periodos no pico una contabilidad de 40 por ciento de solicitudes de servicio, y durante esos periodos, cada enlace puede manejar la carga de tráfico. Durante periodos pico, ambos enlaces son requeridos para manejar la carga completa, pero un enlace puede manejar el 80 por ciento de la carga pico. La disponibilidad funcional para el sistema puede ser expresado como:

A_f = (capacidad cuando un enlace esta operativo)*Pr[1 enlace operativo] +
(capacidad cuando los dos enlaces están operativos)*Pr[2 enlaces operativos]

Donde Pr[ ] significa la probabilidad de.

La probabilidad que ambos enlaces estén operativos es A^2, donde A es la disponibilidad de cada enlace. La probabilidad que exactamente un procesador este operativo es $A(1-A)+(1-A)A=2A-2A^2$. Usando un valor para A de 0.9, entonces Pr[1 enlace este activo] = 0.9*0.9 = 0.81, y Pr[2 enlaces estén activos] = 0.18. Recordando que un enlace es suficiente para cargas no pico, tenemos:

A_f(no pico) = (1.0)(0.18) + (1.0)(0.81 = 0.99

y, para periodos picos,

A_f(pico) = (0.8)(0.18) + (1.0)(0.81) = 0.954.

La disponibilidad funcional total, entonces, es

$A_f = 0.6*A_f$(pico) + $0.4*A_f$(no pico) = 0.9684.

Así, un promedio, de cerca de 97 por ciento de solicitudes de servicio pueden ser manejados por el sistema.

ii. Tiempo de respuesta

El tiempo de respuesta es el tiempo que toma un sistema para reaccionar a una entrada dada. En una transacción interactiva este puede ser definido como el tiempo entre la presión de la ultima tecla por el usuario y el inicio de la visualización de los resultados por el computador. Para diferentes tipos de aplicaciones, una definición un poco diferente es necesario. En general este es el tiempo que toma para el sistema responder a una solicitud para realizar una tarea particular.

Idealmente, uno desearía que el tiempo de respuesta para cualquier aplicación sea corta. Sin embargo, en este caso invariablemente un tiempo de respuesta mas corto significa incremento de costo. Este costo viene de dos fuentes:

- Potencia de procesamiento del computador: las computadoras más rápidas, tienen tiempo de respuesta mas bajos. Por tanto, incremento de potencia de procesamiento significa incremento de costo.

- Competencia de requerimientos: proveer tiempo de respuesta rápido a algunos procesos puede penalizar otros procesos.

Así, el valor de un nivel dado de tiempo de respuesta debe ser evaluado versus el costo de lograr ese tiempo de respuesta.

La tabla 2.2, basado en (Martín 1988), lista seis rangos generales de tiempos de respuesta. Las dificultades de diseño son mostrados cuando el tiempo de respuesta requerido es menor que un segundo. El tiempo de respuesta es clave para la productividad en aplicaciones interactivas, esto ha sido confirmado en varios estudios (Guynes 1988; Shneiderman 1984; Tañan 1981). Esos estudios muestran que cuando un computador y un usuario interactúan en un escenario que asegure que ninguno tiene que esperar al otro, la productividad se incrementa significativamente, el costo del trabajo realizado en el computador por tanto cae, y la calidad tiende a mejorar. Comúnmente se acepta ampliamente que el tiempo de respuesta sea relativamente corto – hasta dos segundos- fue aceptable para la mayoría de aplicaciones interactivas porque el usuario estuvo pensando en la próxima tarea. Sin embargo, ahora parece que la productividad se incrementa tanto como tiempos de respuesta mas cortos sean alcanzados.

Tabla 2.2 Rangos de tiempo de respuesta

Mayor que 15 segundos Esta fuera de las reglas de interacción fluida. Para ciertos tipos de aplicaciones, ciertos tipos de usuarios podrían estar satisfechos de permanecer en un Terminal esperando por mas de 15 segundos por la respuesta a una consulta. Sin embargo, para personas ocupadas, la permanencia por mas de 15 segundos resulta intolerable. Si tales retardos ocurren, el sistema debería ser diseñado tal que el usuario puede cambiar a otras actividades y solicitar la respuesta mas adelante.
Mayor que 4 segundos Esos son generalmente demasiado tiempo para una fluidez requiere que el operador retenga información en la memoria de corto plazo. Tales retardos serían desalentadores en actividades de resolución de problemas y frustrante en actividades de entrada de datos. Sin embargo, en cierre de sistemas importantes, retardos de 4 a 15 segundos pueden ser tolerados.
De 2 a 4 segundos Retardos superiores a 2 segundos pueden inhibir operaciones de Terminal que demandan un alto nivel de concentración. Una espera de 2 a 4 segundos en el Terminal puede sentirse sorprendentemente largo cuando el usuario esta concentrado y emocionalmente comprometido a completar aquello que esta haciendo. Nuevamente, un retardo en este rango puede ser aceptable después que un cierre de sistema menor ha ocurrido.
Menor que 2 segundos Cuando el usuario del Terminal tiene que recordar información durante algunas respuestas, el tiempo de respuesta debe ser corto. En la mayoría de lo detallado, la mayoría lo necesita para respuestas menores que 2 segundos. Para elaboradas actividades de Terminal, 2 segundos representa un limite de tiempo de respuesta importante.
Tiempo de respuesta debajo de un segundo Cierto tipo de trabajo de pensamiento intensivo, especialmente con aplicaciones graficas, requiere tiempos de respuesta muy cortos para mantener el interés del usuario y la atención por largos periodos de tiempo.
Tiempo de respuesta debajo de una décima de segundo Una respuesta a la presión de una tecla y ver el carácter displayado en la pantalla o hacer clic en un objeto en la pantalla con un Mouse necesita ser instantáneo – menos que 0.1 segundo después de la acción. La interacción con un Mouse requiere interacción extremadamente más rápido si el diseñador esta evitando el uso de sintaxis extrañas (uno con comandos, selección de nemonicos, etc.)

El resultado reportado acerca de tiempos de respuesta están basados en un análisis de transacciones en línea. Una transacción consiste de un comando de usuario desde un Terminal y la respuesta del sistema. Es la unidad fundamental del trabajo en línea

de los usuarios de sistemas en línea. Este puede ser dividido en dos secuencias de tiempo:

- Tiempo de respuesta de usuario: el tiempo que transcurre entre el momento que el usuario recibe una respuesta completa a un comando e ingresa el siguiente comando; a menudo referido como "tiempo de pensamiento".
- Tiempo de respuesta del sistema: el tiempo que transcurre entre el momento que el usuario ingresa un comando y el momento en que se visualiza de manera completa la respuesta en el Terminal.

Como un ejemplo del efecto de reducidos tiempo de respuesta de los sistemas , la figura 2.5 muestra los resultados de un estudio realizado con ingenieros usando programas gráficos de diseño asistido por computador para el diseño de chips de circuitos integrados y circuitos impresos (Smith 1983). Cada transacción consiste de un comando efectuado por el ingeniero que altera en algún modo la imagen grafica que esta siendo visualizada en la pantalla. Los resultados muestran que la tasa de transacciones se incrementa en la medida que el tiempo de respuesta del sistema cae y se incrementa dramáticamente cada vez que el tiempo de respuesta cae debajo de un segundo. Lo que ocurre es que como el tiempo de respuesta del sistema cae, así como el tiempo de respuesta del usuario. Esto tiene que ver con el efecto del transcurso de la memoria de corto tiempo y atención humana.

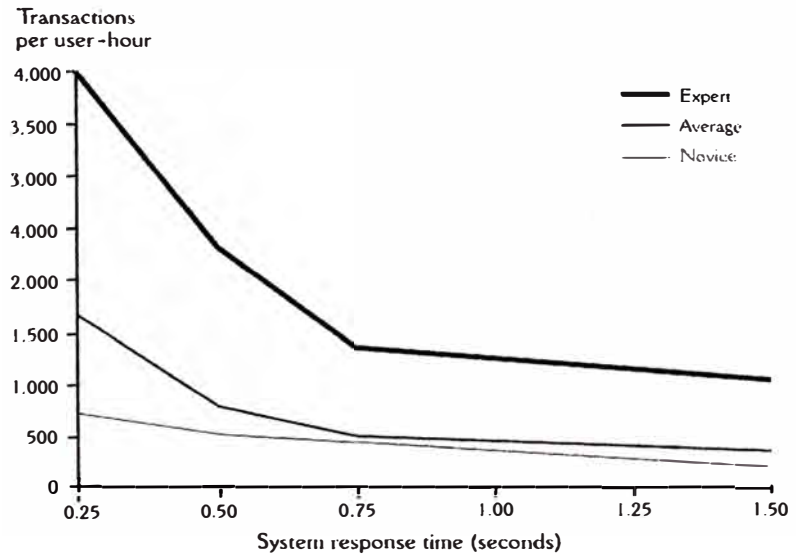


Figura 1.10 Tiempo de respuesta resultantes para funciones de alto contenido grafico

Para medir el tiempo de respuesta, un número de elementos necesitan ser examinados. En particular, mientras que pueda ser posible medir directamente el tiempo total de respuesta en un entorno de red dado, esta figura independiente es de poco uso en la corrección de problemas o planificación del crecimiento de la red. Para esos propósitos, una división detallada del tiempo de respuesta es necesario para identificar cuellos de botella y potenciales cuellos de botella.

La figura 2.6 ilustra una situación de red típica e indica los siete elementos del tiempo de respuesta comunes a la mayoría de aplicaciones interactiva. Cada uno de esos elementos es un paso en la ruta completa que sigue una consulta a través de una configuración de comunicaciones, cada elemento contribuye con una parte del tiempo de respuesta total:

- Retardo del Terminal de entrada: el retardo en obtener una consulta desde el Terminal hacia la líneas de comunicaciones. Asumimos que no hay retardo notable en el Terminal mismo, tal que el retardo es directamente dependiente de la tasa de transmisión del Terminal al controlador. Por ejemplo, si la tasa de datos en la línea es 2400 bps =300 caracteres por segundo, entonces el retardo es 1/300 =3.33 milisegundos por carácter. Si el promedio de la longitud del mensaje es 100 caracteres, el retardo será 0.33 segundos.
- Tiempo de encolamiento de entrada: el tiempo requerido para el procesamiento del controlador o dispositivo PAD. El controlador esta atendiendo con entradas desde un número de terminales también como entradas desde la red a ser entregada a los terminales. Así, un mensaje que llega será ubicado en un buffer a ser servido a su turno. Si el controlador esta muy ocupado el retardo de procesamiento será más grande.
- Tiempo de servicio de entrada: el tiempo para trasmitir por el enlace de comunicaciones, red u otra facilidad de comunicaciones desde el controlador al procesador front-end de host. Este elemento esta en si mismo compuesto de un número de elementos basados en la estructura de la facilidad de comunicaciones.
- Si la facilidad es una red publica de conmutación de paquetes, debe ser tratado como un único elemento.

- Sin embargo, si es una red privada (WAN o LAN), línea dedicada, u otra facilidad instalada de usuario, entonces una división de este elemento será necesario para el control y planificación de la red.
- Retardo de procesador: el tiempo que el procesador front-end, los hosts procesadores, las unidades de disco, y como el centro de computo tarda preparando la respuesta a una consulta. Este elemento esta usualmente fuera del control del gestor de red.
- Tiempo de encolamiento de salida: el tiempo que tarda la respuesta de un puerto del procesador front-end esperando a ser despachado por la red o línea de comunicaciones. Así como con el controlador, el procesador front-end tendrá una cola de respuestas a ser atendidas, y el retardo es mas grande conforme se incrementa el número de respuestas en espera.
- Tiempo de servicio de salida: el tiempo a transmitir por las facilidades de comunicaciones desde los procesadores front-end de los hosts hacia el controlador.
- Retardo de Terminal de salida: el retardo en el Terminal mismo. Nuevamente, este es debida principalmente a la velocidad de la línea.
- El tiempo de respuesta es relativamente fácil de medir y es uno de las clases mas importantes de información necesaria para la gestión de red.

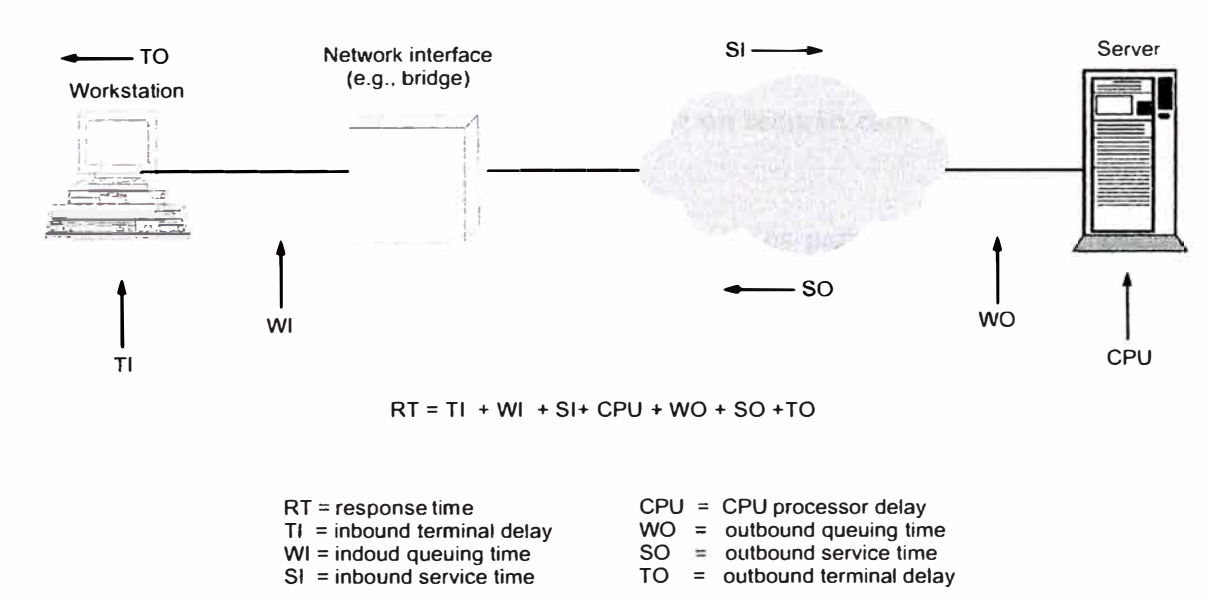


Figura 1.11 Elementos del tiempo de respuesta

iii. Precisión

Transmisiones precisas de datos entre usuarios y hosts o entre dos hosts es esencial para cualquier red. Como los mecanismos de control de error implementados en los protocolos, tales como los protocolos de enlace de datos y protocolos de transporte, precisamente este no le concierne generalmente al usuario. A pesar de esto es útil monitorear la tasa de errores que deben ser corregidos. Esto puede dar una indicación de una falla intermitente en la línea o la existencia de una fuente de ruido o interferencias que deberían ser corregidos.

iv. Throughput

El Throughput es una medida orientada a aplicación. Algunos ejemplos incluyen:

- El número de transacciones de un tipo dado en cierto periodo de tiempo.
- El número de sesiones de clientes para una aplicación dada durante un cierto periodo de tiempo.
- El número de llamadas en un entorno de conmutación de circuitos.

Es útil supervisar esas mediciones todo el tiempo para tener una referencia de la demanda proyectada e identificación de probables problemas de rendimiento.

v. Utilización

La utilización es una medida más refinada que el throughput. Este refiere a la determinación del porcentaje de tiempo que un recurso esta en uso en un periodo de tiempo dado.

Tal vez el uso más importante de la utilización es para la búsqueda de potenciales cuellos de botella y áreas de congestión. Esto es importante porque el tiempo de respuesta usualmente se incrementa exponencialmente conforme la utilización de los recursos se incrementa; esto es un resultado bien conocido de la teoría de colas. Debido a este comportamiento exponencial. La congestión puede rápidamente escapar del manejo si no se identifica rápidamente y resuelve con rapidez.

Viendo en el perfil del recurso, cuales recursos están en uso en cualquier tiempo dado y cuales están desocupados, el analista puede ser capaz de encontrar recursos que están sobre utilizados o subutilizados y ajustarlos de acuerdo a la red. Considere

los siguientes ejemplos de una simple pero efectiva técnica de evaluación de eficiencia de la red. Esta técnica es útil para evaluar la capacidad de varios enlaces de comunicaciones en una red. La idea básica es observar diferencias entre carga planeada y carga actual de los diferentes enlaces en la red. La carga planeada esta reflejada por la capacidad, en bits por segundo, de cada enlace. Una analogía puede ser realizada con la técnica de contabilidad de costos que observa la relación de gasto actual a gastos planeados por la división dentro de la compañía. Divergencias significativas entre divisiones puede llevar a información de utilización, porque ellos esperan cuestionar y rechazar la precisión del proceso de planificación del presupuesto en cada división.

Considere, por ejemplo, la simple configuración de red mostrada en la figura 1.12 (a). Expresamos la carga de cada canal como el porcentaje del total de carga en la red y el flujo de cada canal como el porcentaje del flujo total. La tabla 1.4 contiene resultados numéricos, y la figura 1.12 (b) provee una ilustración grafica. Como podemos ver, la capacidad total de la red provee un margen confortable sobre la carga total de la red, y de acuerdo ningún enlace esta transportando una carga más grande que su capacidad. Sin embargo, mediante observación de la capacidad y carga relativa, podemos ver que algunos enlaces están transportando una proporción de carga compartida menos que otras. Esto indica una distribución ineficiente de recursos. Mediante el ajuste de esas tasas (cada uno mediante redirección de tráfico o mediante el cambio de la tasa de datos relativa de los diferentes enlaces) un rápido balance entre la carga planeada y la carga actual puede ser lograda, reduciendo la capacidad total requerida y usando los recursos mas eficientemente.

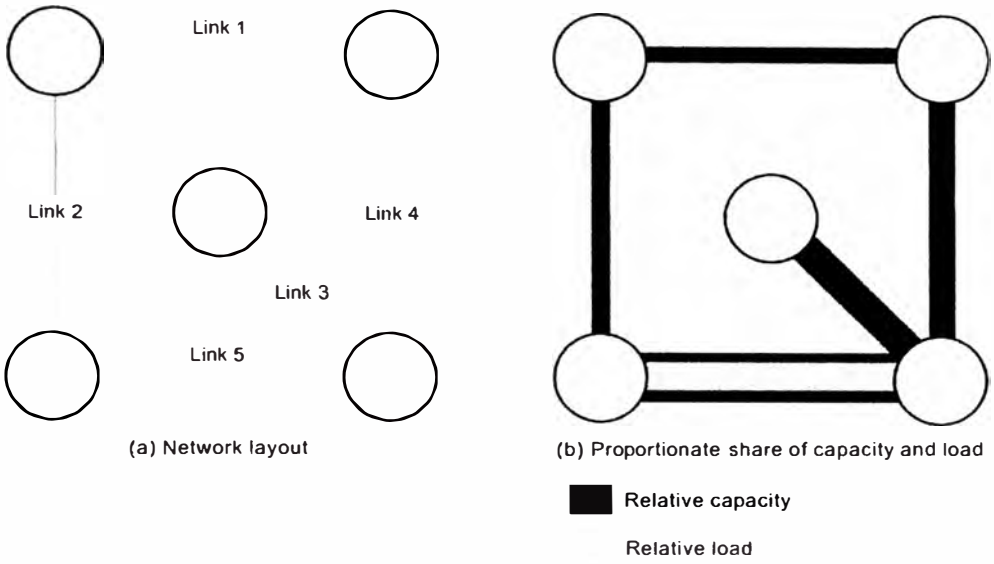


Figura 1.12 Análisis simple de eficiencia

Tabla 1.4 Análisis de capacidad y carga para la red mostrad en la figura 1.12 (a)

	Enlace 1	**Enlace 2**	**Enlace 3**	**Enlace 4**	**Enlace 5**	**Total**
Carga (Kbps)	30	30	50	40	50	200
Capacidad (Kbps)	40	40	60	80	180	400
Porcentaje de carga total	15	15	25	20	25	100
Porcentaje de capacidad total	10	10	15	20	45	100
Tasa	1.5	1.5	1.67	1.0	0.55	-

2) Función de monitorización de rendimiento

La monitorización de rendimiento incluye tres componentes: medición de rendimiento, el cual es el actual recolector de estadística acerca del tráfico de la red y temporización; análisis de rendimiento, el cual consiste de software para reducir y presentar los datos; y generación de tráfico sintético, el cual permite que la red sea observada bajo carga controlada.

La medición de rendimiento es a menudo exitosamente realizado por el modulo agente dentro del dispositivo en la red (hosts, ruteadores, bridges, etc.). Esos agentes están en posición de observar la cantidad de tráfico que ingresa y sale de un nodo, el número de conexiones (nivel de red, nivel de transporte, nivel de aplicación) y el tráfico por conexión y otras mediciones que provee una descripción detallada del comportamiento de ese nodo. De acuerdo, todas estas mediciones tienen un precio de recurso de procesamiento dentro del nodo.

En una red compartida, tal como una LAN, muchas de las necesidades de información pueden ser recolectadas por un monitor externo o remoto que simplifica la observación del tráfico en la red. Esta disposición descarga de los requerimientos de procesamiento de los nodos operacionales a un sistema dedicado.

La tabla 1.5 lista los tipos de mediciones reportadas en una facilidad de LAN típica y da algunas ideas de las clases de mediciones que son de interés. Esas mediciones pueden ser usadas para responder un número de preguntas. A un área le concierne consultas posibles acerca de errores o ineficiencias:

- Es el tráfico eventualmente distribuido entre los usuarios de la red o hay pares origen destino con inusual tráfico pesado?
- Cual es el porcentaje de cada tipo de paquete?. Hay algún tipo de paquete de frecuencia inusual alta, indicando un error o un protocolo ineficiente?
- ¿Cuál es la distribución del tamaño de los paquetes de datos?
- ¿Cuáles son los canales de adquisición y distribución de retardo de comunicación?. ¿Son esos tiempos excesivos?
- ¿Son las colisiones un factor en la obtención de paquetes transmitidos, indicando posibles fallas de hardware o protocolos?
- ¿Cuál es el throughput y la utilización del canal?

Una segunda área tiene que hacer con el incremento de la carga de tráfico y la variación de los tamaños de los paquetes:

- ¿Cuál es el efecto de carga de tráfico sobre la utilización, throughput, y retardos de tiempo?. ¿Cuándo la carga de tráfico empieza a degradar el rendimiento del sistema?
- Definiendo una red estable como una cuya utilización tiene una función no decreciente de carga de tráfico, ¿Cuál es la negociación entre estabilidad, throughput y retardo?
- ¿Cuál es la máxima capacidad del canal bajo condiciones de operación normal? ¿Cuántos usuarios activos son necesarios para alcanzar este máximo?
- Los paquetes grandes incrementan o disminuyen el throughput y retardo?
  - Como afectan los paquetes de tamaño constante la utilización y el retardo?
  - Esas áreas son de interés para el gestor de red. Otras preguntas de compromiso tienen que hacer con tiempos de respuesta o throughput por clases de usuario y la determinación de cuanto crecimiento puede absorber la red antes de cruzar cierto umbral de rendimiento.

Tabla 1.5 reportes de medidas de rendimiento

Nombre	**Variables**	**Descripción**
Matriz de comunicación de hosts	Origen X destino	(Número,%) de (paquetes, datos de paquetes, octetos de datos)
Matriz de comunicación de grupos	Origen X destino	Como el anterior, consolidado en grupos identificados.
Histograma de tipo de paquetes	Tipo de paquete	(número, %) de (paquetes, paquetes originales) por tipo
Histograma de tamaño de paquetes de datos	Tamaño de paquete	(Número, %) de paquetes de datos por longitud de octetos de datos.
Distribución de utilización	Origen	(Total de octetos, octetos de datos) transmitidos
Histograma de tiempo entre llegada y llegada de paquetes	Tiempo entre llegada y llegada	Tiempo entre señales de portadoras consecutivas (ocupación de red)
Histograma de retardo de adquisición del canal	Retardo de adquisición de la unidad de interfaz de red (NIU)	(Número, %) de paquetes retardados en la NIU por cantidades dadas
Histograma de retardo de comunicación	Retardo de paquete	Tiempo que el paquete original tarda del origen a receptor
Histograma de cuenta de colisiones	Número de colisiones	Número de paquetes por número de colisiones
Histograma de cuenta de transmisión	Número de transmisiones	Número de paquetes por intento de transmisión.

3) Estadísticas versus medición exhaustiva

Cuando un agente en un nodo o un monitor externo esta monitoreando un tráfico de carga pesado, podría no ser practico recolectar datos exhaustivamente. Por ejemplo, en la operación de un monitor externo para construir una matriz que muestre precisamente el número total de paquetes en un periodo de tiempo dado entre cada par origen- destino, el monitor necesitaría capturar cada paquete transmitido en la LAN bajo observación y leer las direcciones origen y destino en la cabecera de cada paquete. Cuando la LAN esta cargada fuertemente, el monitor simplemente podría no ser capaz de hacerlo.

La alternativa es tratar cada parámetro como una variable aleatoria y muestrear el flujo de tráfico en orden a estimar el valor de la variable aleatoria. Sin embargo, debe tener cuidado en el empleo e interpretación de las estimaciones estadísticas de los resultados. Los método estadísticos tradicionales fueron desarrollados para áreas como agricultura y biología, donde pueden ser a menudo que la probabilidad de interés sea relativamente grande (típicamente 10^{-2} o superior) y que hay una independencia entre observaciones(donde la salida de una observación no indica nada acerca de otra observación). Ninguna de esas asunciones permanecen ciertas para comunicaciones de datos, donde algunos eventos de interés, tales como errores, pueden ocurrir a tasas de 10^{-6} o inferiores, y donde agrupaciones o ráfagas son comúnmente observados. La responsabilidad individual de diseño de las funciones de muestreo y de interpretación de los resultados necesita tener alguna familiaridad con principios estadísticos.

c) Monitorización de fallas

El objetivo de la monitorización de fallas es identificar fallas tan rápido como ellos ocurren e identificar la causa de la falla y las acciones de remediación que deberán ser tomadas.

1) Problemas de monitorización de fallas

En un entorno complejo, la localización y diagnostico de fallas puede ser dificultoso. (Dupuy et al. 1989) lista los problemas específicos siguientes asociados con la observación de fallas:

- Fallas no observables: ciertas fallas son inherentemente localmente no observables. Por ejemplo, la existencia de un conflicto entre procesos distribuidos cooperativos pueden ser no observables localmente para registrar la ocurrencia de una falla.
- Fallas observables parcialmente: la falla de un nodo podría ser observable, pero la observación podría ser insuficiente para puntualizar el problema. Por ejemplo, escasa respuesta desde un dispositivo remoto podría significar que el dispositivo esta trabado, la red esta particionada, la congestión causa que la respuesta sea retardada, o el temporizador local este fallando.

Para Cada falla observada, es necesario aislar la falla a un componente particular. Los problemas ocurren aquí también, incluyendo los siguientes sugeridos en (Fried y Tjong 1990):

- Múltiples causas potenciales: cuando múltiples tecnologías son involucradas, los puntos de falla potencial y los tipos de fallas se incrementan. Esto hace arduo localizar la fuente de falla.
- En la figura 1.13, por ejemplo, los datos transmitidos entre la estación de trabajo cliente y el servidor debe atravesar la LAN, ruteador, multiplexor, y el subsistema de transmisión. Si la conectividad es perdida o si la tasa de error es alta, el problema podría ser debido a problemas en cualquiera de esos subsistemas.
- Demasiado observaciones relativas: una falla única puede afectar a muchas rutas de comunicaciones activas. La falla de una línea T1 en la figura 1.13 afectará todas las comunicaciones activas entre las estaciones token-ring y estaciones de las dos LAN ethernet, también como las comunicaciones de voz entre las PBX. Además, una falla en la capa uno de la arquitectura de comunicaciones puede causar degradaciones o fallas en todas las capas superiores dependientes, como se ilustra en la figura 1.14. Así, una falla en

la línea T1 será detectada en los ruteadores como una falla de enlace y en las estaciones como de transporte y fallas de aplicación. Porque una falla simple puede generar muchas fallas secundarias, la proliferación de datos de monitorización de fallas que pueden ser generados en esta forma puede oscurecer el único problema subyacente.

- Interferencia entre las causas del problema y procedimientos de recuperación local: los procedimientos de recuperación local pueden destruir importantes evidencias concernientes a la naturaleza de la falla, imposibilitando el descubrimiento de las causas.
- Ausencia de herramientas de pruebas automatizadas: las pruebas para aislar fallas es dificultoso y costoso de gestionar.

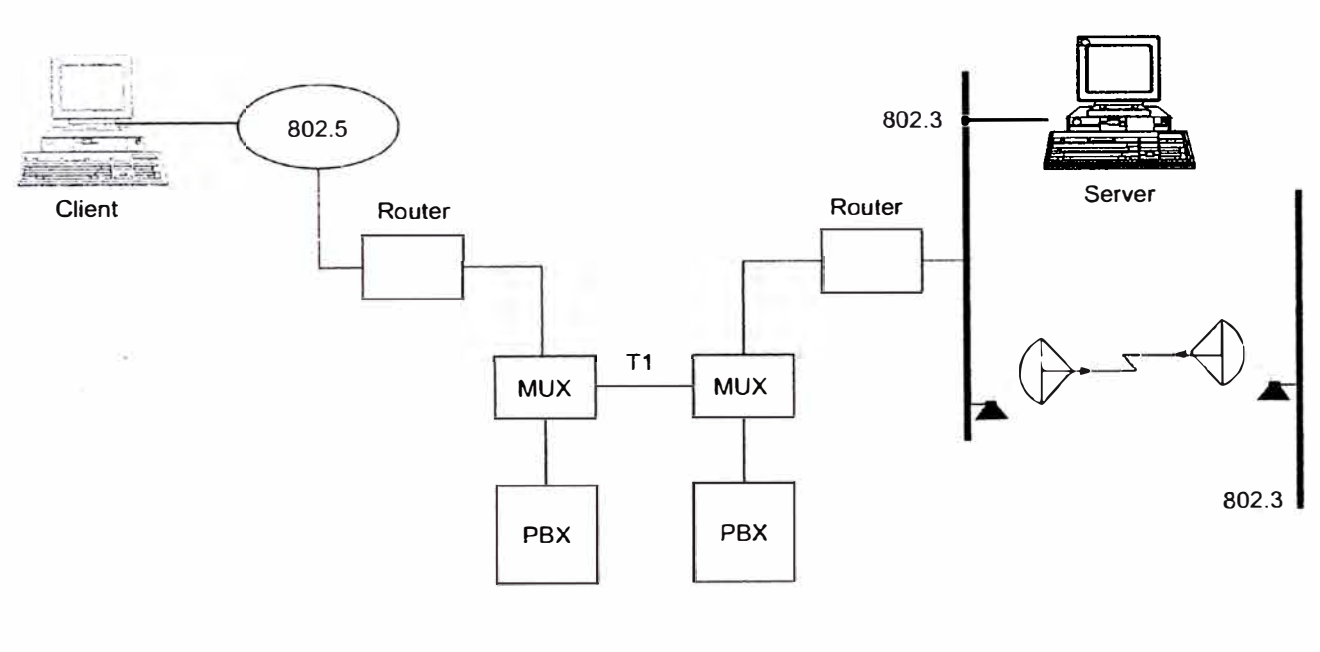


Figura 1.13 Entorno de red heterogéneo

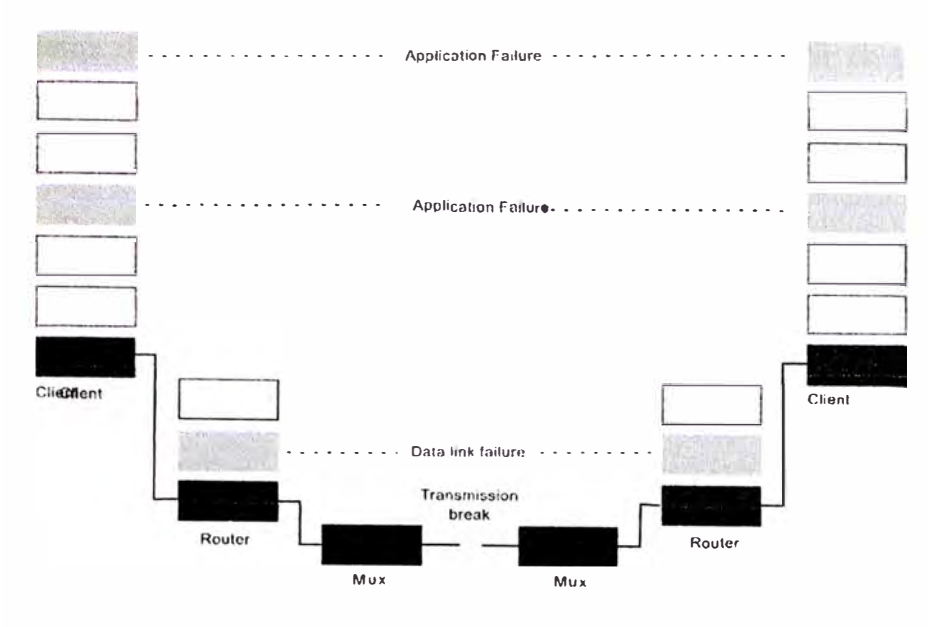


Figura 1.14 Propagación de las fallas a las capas superiores

2) Funciones de monitorización de fallas

Los primeros requerimientos de un sistema de monitorización de fallas es que sea capaz de detectar y reportar fallas. Al menos, un agente de monitorización de fallas mantendrá un registro de eventos y errores significativos. Esos registros, o resúmenes, están disponibles a los sistemas del gestor autorizado. Así, un sistema que opera primariamente mediante sondeo dependería de esos registros (logs). típicamente, el agente de monitorización de fallas tiene la capacidad de reportar errores independientemente a uno o mas gestores. Para evitar sobrecargar la red, el criterio para usar un reporte de falla es que debe ser razonablemente conciso.

En adición a reportar las fallas existentes conocidas, un buen sistema de monitorización de fallas será capaz de anticipar fallas. Generalmente, esto involucra configuración de umbrales y uso de reportes cuando una variable monitoreada cruza los umbrales. Por ejemplo, si la fracción de paquetes transmitidos que sufre errores que exceden cierto valor, esto podría indicar que un problema se esta desarrollando a lo largo de la ruta de comunicaciones. Si el umbral es fijado los suficientemente bajo, el gestor de red puede ser alertado en el momento para tomar acciones que eviten una falla mayor en el sistema.

El sistema de monitorización de fallas debería también asistir en el aislamiento y determinación de las causas de la falla. Ejemplos de pruebas que un sistema de monitorización de fallas debería incluir comandos para:

- Prueba de conectividad
- Prueba de integridad de datos
- Prueba de integridad de protocolos
- Prueba de saturación de datos
- Prueba de saturación de conexión
- Prueba de tiempo de respuesta
- Prueba de loopback
- Prueba de función
- Prueba de diagnostico

Tal vez más que en otras áreas de monitoreo de red, un interfaz de usuario efectiva es requerido para monitorización de fallas. En situaciones compleja, las fallas serán aisladas, conocido su origen, y finalmente corregida solo por el esfuerzo cooperativo de un usuario humano y el software monitor.

d) Monitorización de contabilidad

Monitorización de contabilidad es primariamente una materia de seguir la pista del uso de los recursos de la red por parte de los usuarios. Los requerimientos para esta función varían ampliamente. En algunos entornos, la contabilización puede ser de una naturaleza mas o menos general. Por ejemplo, un sistema de contabilización interno puede ser usado solo para evaluar el uso total de los recursos y para determinar que porción del costo de cada recurso compartido debería ser cargado a cada departamento. En otros casos, particularmente para sistemas que ofrecen un servicio publico, pero también para muchos sistemas con solo usuarios internos, se requiere que la utilización sea dividido por cuentas, por proyectos, o aun por usuarios individuales para el propósito del pago. En este ultimo caso, la información recolectada por el sistema monitor debe ser más detallado y más preciso que esos requeridos para un sistema general.

Ejemplos de recursos que pueden ser sujetos a contabilización incluyen los siguientes:

- Facilidades de comunicación: LANs, WANs, líneas arrendadas, líneas conmutadas, y sistemas PBX.
- Hardware de computador: estaciones de trabajo y servidores
- Software y sistemas: aplicaciones y software de utilidad en servidores, data center y sites de usuarios finales.
- Servicios: incluye todos los servicios de información y comunicación disponibles a los usuarios en la red.

Para cualquier tipo de recursos, datos de contabilización son recolectados, basados en requerimientos de la organización. Por ejemplo, los siguientes datos de contabilización relativo a las comunicaciones podrían ser recolectados y mantenidos para cada usuario:

- Identificación de usuario: provisto por el originador de la transacción o solicitud de servicio
- Receptor: identifica el componente de red al cual se intento o realizo la conexión.
- Número de paquetes: cuenta de datos transmitidos.
- Nivel seguridad: identifica la transmisión y prioridades de procesamiento
- Registro de tiempo: asociado con cada transmisión principal y evento de procesamiento (ejemplo: hora de inicio y parada de la transacción).
- Códigos de estados de la red: indica la naturaleza de cualquier error o malfuncionamiento detectado.
- Recursos usados: indica cual recursos son invocados mediante esta transacción o evento de servicio.

1.5.2 Control de red

La parte de control de red de la gestión de red, esta comprometida con la modificación de parámetros y causan acciones a ser tomados por los sistemas finales, sistemas intermedios, y subredes que construyen la configuración a ser administrada.

De todas las cinco principales áreas funcionales de gestión de red (rendimiento, fallas, contabilización, configuración, y seguridad) involucran monitoreo y control. Tradicionalmente, sin embargo, el énfasis de las tres primeras áreas funcionales ha sido

monitorización, mientras las dos ultimas áreas están más involucrados con el control. Por esta razón, el capitulo 1.5.1 se concentro en monitorización de rendimiento, fallas y contabilización. Este capitulo examina los aspectos de control de red de la gestión de configuración y seguridad.

a) Control de configuración

La gestión de configuración esta involucrada con la inicialización, mantenimiento, y la desactivación de componentes individuales y subsistemas lógicos de la configuración total del computador y recursos de comunicaciones de una instalación. La gestión de configuración puede ordenar el proceso de inicialización mediante la identificación y especificación de las características de los componentes de red y recursos que constituirán la red. Los recursos gestionados incluyen recursos fisicos identificables (ejemplo: servidor o un ruteador) y objetos lógicos de bajo nivel (ejemplo: temporizador de retransmisión de la capa de transporte). La gestión de configuración puede especificar valores iniciales o por omisión de atributos tal que los recursos gestionados comiencen la operación en el estado deseado, poseer los parámetros con valores apropiados, y formar la relación deseada con otros componentes de la red.

Mientras la red esta en operación, la gestión de configuración es responsable de la monitorización de la configuración y realización de cambios en respuesta a los comando de usuario o en respuesta a otras funciones de gestión de red. Por ejemplo, si las funciones de monitorización de rendimiento detectan que el tiempo de respuesta esta degradando debido a un desbalance de carga, la gestión de configuración puede ajustar la configuración para lograr nivelar la carga. Similarmente, si gestión de fallas detecta y aísla la falla, gestión de configuración puede alterar la configuración para saltar la falla.

Gestión de configuración incluye las siguientes funciones:

- Definir información de configuración.
- Fijar y modificar valores de los atributos.

1) Definir Información de Configuración

La información de configuración describe el estado y naturaleza de los recursos que son de interés para la gestión de red. La información de configuración incluye una especificación de los recursos bajo gestión y los atributos de esos recursos.

Los recursos de red incluyen recursos fisicos (Ejemplo: sistemas finales, ruteadores, bridges, servicios y facilidades de comunicaciones, medios de comunicación y modems) y recursos lógicos (ejemplo: temporizadores, contadores y circuitos virtuales). Los atributos por ejemplo, incluyen: nombre, dirección, número de identificación, estados, características operacionales, número y nivel de revisión de versión software.

La información de configuración (ciertamente, toda la información de gestión) puede ser estructurado en un número de formas:

- Como una lista de campos de datos estructurados, cada campo conteniendo un único valor. Esta es la aproximación tomada por SNMP.
- Como una base de datos orientado a objetos. Cada elemento de interés para la gestión es representado por uno o mas objetos. Cada objeto contiene atributos cuyos valores representan las características del objeto representado. Un objeto también puede contener comportamientos, tal como notificaciones a ser usados si ocurren ciertos eventos relativos a este elemento. El uso de relaciones de herencia y contenido permite que sea definido relaciones entre objetos. Esta es la aproximación tomada por la gestión de red OSI.
- Como una base de datos relacional. Campos individuales en la base de datos contienen valores que reflejan características de elementos de red. La estructura de la base de datos refleja las relaciones entre elementos de red.

Aunque si bien esta información es accesible a la estación del gestor, este es generalmente almacenado cerca de los recursos en cuestión, cada uno en un nodo agente, si el recurso es parte de ese nodo, o en un nodo Proxy, si el nodo que contiene el recurso no soporta el software agente.

Las funciones de control de red deberían habilitar al usuario, especificar el rango y tipo de valores para el cual puedan ser fijados los atributos del recurso especificado en un agente particular. El rango puede ser una lista de todos los posibles estados o los limites superiores e inferiores para los parámetros y atributos. Pueden también ser especificados el tipo permitido de valores para un atributo.

Las funciones de control de red deberían también ser capaces de definir nuevos tipos de objetos o tipos de elementos de datos, dependiendo del tipo de base de datos. Idealmente, debería ser posible definir esos nuevos objetos en línea y tener creado tales objetos en los agentes y Proxy apropiados. Virtualmente todos los sistemas de hoy, realizan esta función fuera de línea. Como parte de la configuración de un elemento de red, mas que siendo posible dinámicamente.

2) Fijar y modificar valores de los atributos

Las funciones de control de configuración deberían a habilitar a una estación gestora para configurar y modificar remotamente valores atributos en agentes y praxis. Hay dos limitaciones en esta capacidad:

i.- Un gestor debe estar autorizado a realizar las modificaciones de un atributo en particular en un agente o Proxy particular en un momento particular. Esto es una compromiso de seguridad, identificado en la sección b).

ii.- Algunos atributos reflejan la realidad de un recurso y no puede por su naturaleza, ser modificado remotamente. Por ejemplo, un ítem de información sería el número de puertos físicos en un ruteador. Aunque si bien cada puerto puede ser habilitado o deshabilitado en un instante particular, el número de puertos solo puede cambiar por una acción física en el ruteador, no por una acción de configuración de parámetros.

La modificación de un atributo obviamente modificaría la información de configuración en el agente o Proxy. En general, en general las modificaciones caen dentro de las tres categorías:

- Solo actualización de bases de datos: Cuando un gestor usa un comando en un agente, son cambiados uno o mas valores en la base de datos de la configuración del agente (si la operación es exitosa). En algunos casos, no hay respuestas inmediatas por el lado del agente. Por ejemplo, un gestor puede cambiar información del contacto (nombre e identificación de personas responsables por este recurso).

  El agente responde actualizando los valores de datos apropiados y retorna un acuse de recibo al gestor.

- Actualización de la base de datos mas modificación del recurso: Adicional a la actualización de valores en la base de datos de configuración en el agente, un comando de modificación puede afectar un recurso subyacente. Por ejemplo, si el atributo estado de un puerto fisico es configurado a deshabilitado, el agente no solo actualiza el atributo estado sino también deshabilita el puerto, tal que este no esta mas tiempo en uso.
- Actualización de base de datos mas acción: En algunos sistemas de gestión de red, no hay comandos de acción directa disponibles para los gestores. Mas bien, hay parámetros en la base de datos que, cuando son configurados, causan que el agente inicie una cierta acción. Por ejemplo, un ruteador podría mantener un parámetro de reinicio en la base de datos. Si un gestor autorizado configura este parámetro a **verdadero**, el ruteador podría iniciar un proceso de reinicio, el cual podría fijar el parámetro en **falso** y reiniciar el ruteador.

El usuario debería ser capaz de cargar valores de atributos por omisión como estados por omisión, valores, y características operacionales del recurso en el sistema completo, nodo individual o capa individual.

3) Definir y modificar relaciones

Una relación describe una asociación, conexión, o condición que existe entre los recursos o componentes de red. ejemplo de relación son topología, una jerarquía, una conexión lógica o fisica, o un dominio de gestión. Un dominio de gestión es un conjunto de recursos que comparten un conjunto de atributos de gestión o un conjunto de recursos comunes que comparten la misma autoridad de gestión.

Configuración de gestión debería permitir modificaciones en línea de recursos sin deshabilitar una parte o la red completa. Los usuarios deberían ser capaces de adicionar, borra y modificar la relación entre los recursos de red.

Un ejemplo de uso de las relaciones es gestionar la conexión de la capa de enlace entre los nodos LAN, en el nivel de los puntos de acceso al servicio (SAP) del control de enlace lógico (LLC). Una conexión LLC puede ser configurada en una de dos formas. Primero, el protocolo LLC es un nodo que puede usar una solicitud de conexión a otro nodo, cada uno en respuesta al software de la capa superior o

un comando de Terminal de usuario; esos podrían ser referidos como conexiones conmutadas. Segundo, una estación gestora de red podría configurar una conexión LLC fija o permanente entre dos nodos. Esta configuración de conexión designaría el SAP en cada nodo que sirvió como un punto final para la conexión. El software gestor, bajo comando del operador, debería también ser capaz de romper una conexión, permanente o conmutada. Otra característica útil es ser capaz de designar un respaldo o dirección alterna a ser usado en el caso que el destino primario falle en responder a una solicitud de conexión.

4) Inicializar y terminar operaciones de red

Gestión de configuración debería incluir mecanismos que habiliten a los usuarios a inicializar y cerrar las operaciones de red u subred. La inicialización incluye verificación de todos los atributos configurables de los recursos y relaciones que han sido apropiadamente configurados, notificación a usuarios de cualquier recurso, atributo, o relación aun necesaria a ser configurada, y validación de comandos de inicialización de usuarios. Para la terminación, mecanismos son necesarios para permitir a usuarios recuperar solicitudes de estadísticas especificadas, bloques, o estado de información antes que los procedimientos de terminación hayan completado.

5) Distribuir software

Gestión de configuración debería proveer la capacidad de distribuir software en cada parte de la configuración a los sistemas finales (hosts, servidores, y pasarelas de nivel de aplicación). Esta facilidad requiere permitir solicitar carga de software, para transmitir la versión especificada de software, y actualizar el sistema de seguimiento de configuración.

En adición al software ejecutable, las funciones de distribución de software debería también acompañar tablas y otros datos que manejen el comportamiento de un nodo. Lo más importante en esta categoría es la tabla de ruteo, usado por los bridges y ruteadores. Podría ser que aspectos concernientes a contabilización, rendimiento o seguridad requieran intervención de gestión en las decisiones de enrutamiento que no puedan ser resueltos solo por los algoritmos matemáticos.

Los usuarios necesitan mecanismos para examinar, actualizar y gestionar diferentes versiones de software e información de enrutamiento. Por ejemplo, los usuarios deberían ser capaces de especificar la carga de diferentes versiones de software o tablas de enrutamiento basado en condiciones particulares, tales como tasas de errores.

b) Control de seguridad

Los requerimientos de seguridad de información dentro en una organización han experimentado dos cambios importantes en las ultimas décadas. Antes al uso extendido de equipamiento de procesamiento de datos, la seguridad de la información valiosa de una organización fue provista primariamente mediante medios físicos y administrativos. Un ejemplo de los inicios es el uso gabinetes de archivos de información con una combinación de bloqueo para el almacenamiento de documentos sensibles. Un ejemplo de lo ultimo es el procedimiento de selección de personal usado durante el proceso de contratación.

Con la introducción del computador, la necesidad por herramientas automatizadas para la protección de archivos y otra información almacenada en el computador llega a ser evidente. Este es especialmente el caso de un sistema compartido, tal como un sistema de tiempo compartido, y la necesidad es más aun serio para sistemas que pueden ser accedidos sobre una red de datos o telefonía publica. El nombre genérico para la colección de herramientas diseñado para proteger datos y prevenir de hackers es seguridad de computadores.

El segundo cambio importante que afecta la seguridad es la introducción de sistemas distribuidos y el uso de redes y facilidades de comunicaciones para transportar datos entre terminales de usuario y computadores y entre computadores y computadores. Las medidas de seguridad de red son necesarias para proteger los datos durante su transmisión.

El componente gestión de seguridad de la gestión de red se sustenta en la provisión de seguridad de red y computador. Para los recursos bajo gestión, incluyendo de acuerdo el sistema de gestión de red mismo. Antes de examinar algunos de los detalles de gestión de seguridad, será útil caracterizar las amenazas de seguridad.

1) Amenazas de seguridad

En orden a ser capaz de entender los tipos de amenazas a la seguridad que existen, necesitamos tener una definición de requerimientos de seguridad. La seguridad de red y computadores identifica tres requerimientos:

- Secreto: requiere que la información en un sistema de computadores sea accesible para ser leído solo por partes autorizadas (este tipo de acceso incluye impresión, visualización, y otra forma de revelación, incluyendo la simple revelación de la existencia de un objeto)
- Integridad: requiere que los activos del sistema de computadoras puedan ser modificados solamente por partes autorizadas; la modificación incluye escritura, cambio, cambio de estado, borrado, y creación.
- Disponibilidad: requiere que los activos del sistema de computadoras estén disponibles a las partes autorizadas.

i. Tipos de amenazas

Los tipos de amenazas a la seguridad de un sistema de computadoras o red esta mejor caracterizado mediante la visualización de la función del sistema de computador para ser proveedor de información, En general, hay un flujo de información desde una fuente, tal como un archivo o región de la memoria principal, hacia un destino, tal como otro archivo o un usuario. Este flujo normal es descrito en la figura 1.15(a). Las figuras restantes muestran cuatro categorías generales de amenazas:

- Interrupción: Un activo del sistema es destruido o llega a ser indisponible o inutilizable. Esto es una amenaza la disponibilidad. Ejemplos incluyen la destrucción de una pieza de hardware, tal como un disco duro, el corte de una línea de comunicaciones, o la deshabilitación del sistema de gestión de archivos.
- Interceptación: una parte no autorizada gana acceso a un activo. Este es una amenaza al secreto. La parte no autorizada podría ser una persona, un programa, o un computador. Ejemplos incluyen conexiones para capturar datos en una red, y la copia ilícita de archivos o programas.
- Modificación: una parte no autorizada no solo gana acceso si no también estropea el activo. Esto es una amenaza a la integridad. Ejemplos incluyen

cambio de valores en un archivo de datos, alteración de un programa que se comportara diferente, y la modificación del contenido de mensajes que están siendo transmitidos en una red.

- Fabricación: una parte no autorizada inserta objetos falsos en el sistema. Esto es también una amenaza a la integridad. Ejemplos incluyen la inserción de mensajes espurios en una red o la adición de registros a un archivo.

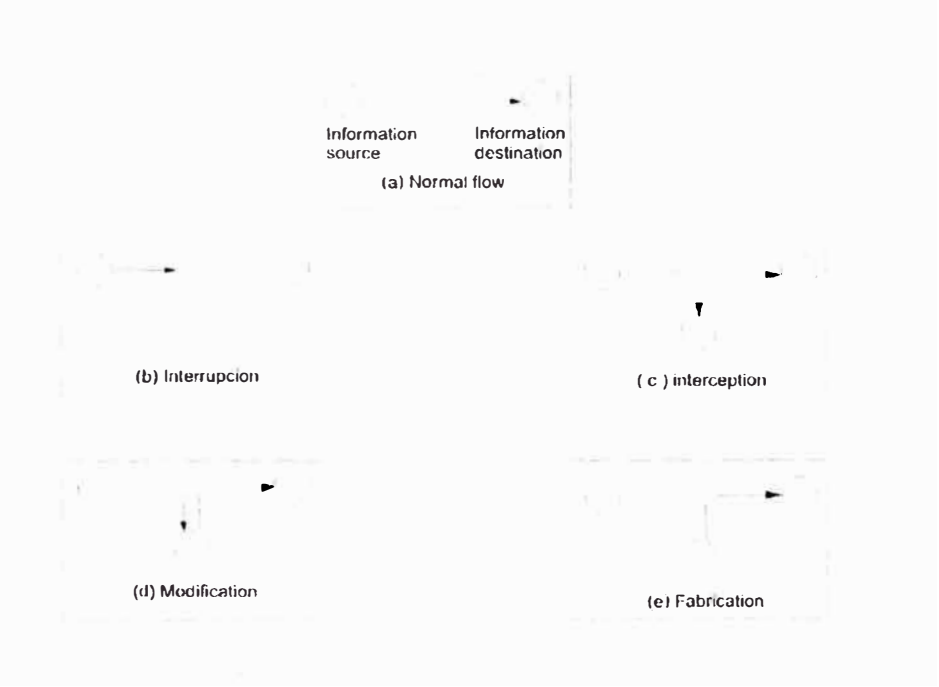


Figura 1.15 Amenazas de seguridad

Los activos de un sistema de computadoras puede ser categorizado como hardware, software, datos, y líneas de comunicaciones y redes. La figura 1.16 y la tabla 1.6 indican la categoría de cada amenaza de diversos activos. Permítanos considerar cada uno de esos a continuación:

ii. Amenaza al hardware

La principal amenaza al hardware de un sistema de computadoras esta en el área de disponibilidad. El hardware es el mas vulnerable a ataques y el menos dócil a control automático. Las amenazas incluyen daño accidental o deliberado al equipamiento así como también el robo. La proliferación de computadoras personales y estaciones de trabajo y el incremento del uso de redes de área local incrementa el potencial de

perdida en esta área. Las medidas de seguridad fisica y administrativa son necesarios para contrarrestar esas amenazas.

iii. Amenazas al software

Los sistemas operativos, utilidades, y programas de aplicación son los que hacen que sea útil el hardware del sistema de computadoras para los individuos o el negocio. Algunas amenazas distintivas necesitan ser consideradas.

Una amenaza clave al software es la disponibilidad. El software, especialmente aplicaciones software, es sorprendentemente fácil de borrar. El software puede también ser alterado o dañado para hacerlo inutilizable. El cuidado de la gestión de configuración software, los cuales incluyen hacer copias de respaldo de las versiones más recientes de software, pueden mantener una alta disponibilidad.

Un problema más dificultoso a enfrentar es la modificación del software que resulta en un programa que aun funciona pero que se comporta diferente que antes. Los virus de computadora y ataques relativos caen en esta categoría.

Un problema final es el secreto del software. Aun si ciertas contramedidas están disponibles, para y el gran problema de la copia no autorizada de software no ha sido resuelta.

iv. Amenaza a los datos

La seguridad de hardware y software son típicamente concernientes a los profesionales de centro de computo, o concierne a individuos usuarios de computadoras personales. Un problema mucho mas grande es la seguridad de datos, el cual involucra archivos y otras formas de datos controlados por individuos, grupos, y organizaciones de negocios.

Lo concerniente a la seguridad con respecto a los datos es amplio, asegurar disponibilidad, secreto, e integridad. En el caso de la disponibilidad, concierne esto a la destrucción de archivos de datos los cuales pueden ocurrir accidental o maliciosamente.

La concernencia es obvia con el secreto, de acuerdo, esto es la lectura no autorizada de archivos de datos o bases de datos, y esta área ha sido objeto de tal vez más investigación y esfuerzos que cualquier otra área de la seguridad de computadoras.

Una menos obvia amenaza al secreto, involucra el análisis de los datos y en si mismo manifiesto el uso de tal llamado bases de datos estadísticas, el cual provee resumen o información agregada. Presumiblemente, la existencia de información agregada no amenazan la privacidad de los individuos involucrados. Sin embargo, como el uso de las bases de datos estadísticas crece, el potencial de develar información personal se incrementa. En esencia, las características del constituyente individual puede ser identificado a través de un análisis cuidadoso. Para tomar un simple ejemplo, si una tabla de registra los agregados de las entradas que corresponden a A, B, C, y D y otros registros de las entradas de A, B, C, D, y E, la diferencia entre los dos agregados sería la entrada de E. este problema es exacerbado por el incremento deseado de combinar conjunto de datos. En muchos casos, la correspondencia de algunos conjuntos de datos para la consistencia al nivel de agregación apropiado para el problema requiere un aislamiento a unidades elementales en el proceso de construcción de los agregados necesarios. así, la unidad elemental, el cual es el objeto de la privacidad concerniente, están disponibles en varios estados en el procesamiento del conjunto de datos.

Finalmente, la integridad de los datos es una principal concernencia en la mayoría de las instalaciones. La modificación de los archivos de datos pueden tener consecuencias en un rango de menores a desastrosas.

Tabla 1.6 Los activos y las amenazas de seguridad

	Disponibilidad	Secreto	Integridad
Hardware	Equipamiento es intervenido o deshabilitado, por tanto denegado el servicio.	-	-
Software	Los programas son borrados, denegando el acceso a los usuarios.	Copias no autorizadas son realizadas.	Un programa de trabajo es modificado, para causar fallas durante su ejecución o no realizar la tarea intentada.
Datos	Los archivos son borrados, denegando el acceso a los usuarios.	Lectura no autorizada de datos es realizado. Un análisis de datos estadísticos revela los datos subyacentes.	Los archivos existentes son modificados, o nuevos archivos son fabricados.
Líneas de comunicaciones	Los mensajes son destruidos o borrados. Las líneas de comunicación o redes son imposibles de usar	Los mensajes son leídos. El patrón de tráfico de mensajes es observado.	Los mensajes son modificados, retardados, reordenados, o duplicados. Mensajes falsos son fabricados.

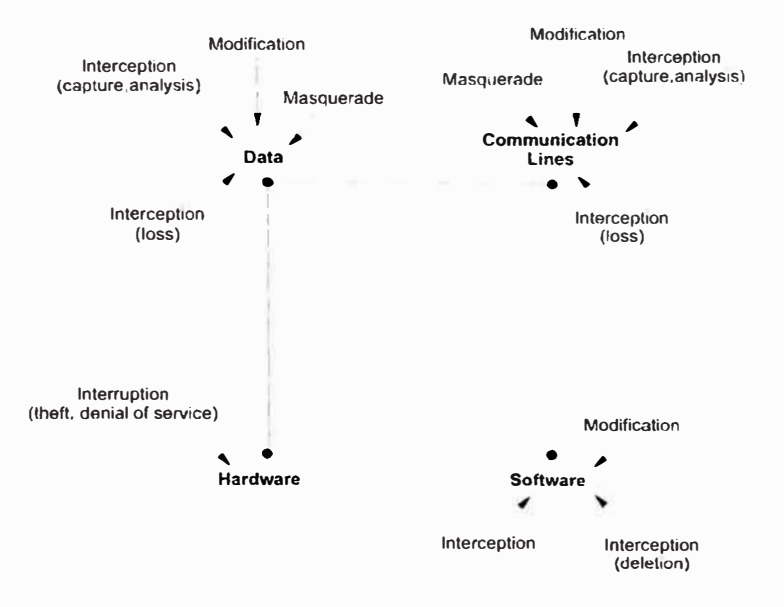


Figura 1.16 Activos del sistema de computadoras y las amenazas de seguridad

v. Amenazas a las líneas de comunicaciones y la red

Los sistemas de comunicaciones son usados para transmitir datos. así, lo concerniente a disponibilidad, seguridad e integridad que son relevantes para la seguridad de los datos aplican también a la seguridad de red. En este contexto, las amenazas son convenientemente categorizadas como pasivas o activas (figura 1.17).

Amenazas pasivas son de naturaleza similar a la escucha a escondidas o monitorización de las transmisiones de una organización. El objetivo del atacante es obtener información que esta siendo transmitida. Dos tipos de amenazas están involucradas aquí, revisión del contenido de mensajes y análisis de tráfico.

La amenaza de revisión de contenidos de mensajes es claramente entendido por la mayoría de los observadores. Una conversación telefónica, un mensaje de correo electrónico, o un archivo transferido puede contener información sensible confidencial. Desearíamos prevenir que el atacante aprenda el contenido de esas transmisiones.

La segunda amenaza pasiva, análisis de tráfico, es mas sutil y a menudo menos aplicable. Supone que tenemos una forma de enmascara el contenido de mensajes u otra información de tráfico tal que un atacante, aún si el o ella captura el mensaje, debería ser incapaz de extraer la información del mensaje. La técnica común de hacer esto es encriptación, discutido en extenso mas adelante. Si tenemos tales protecciones

en el lugar, podría aún ser posible para el atacante observar el patrón de esos mensajes. El atacante puede determinar la localización e identidad de los hosts en comunicación y puede también observar la frecuencia y longitud de los mensajes que están siendo intercambiados. Esta información puede ser útil en la determinación de la naturaleza de las comunicaciones que están teniendo lugar.

Las amenazas pasivas son muy dificultosas de detectar ya que ellos no involucran una alteración de los datos. Sin embargo es posible prevenir estos ataques sean exitosos. Así, el énfasis en contrarrestar amenazas pasivas es la prevención y no la detección.

La segunda categoría más importante de amenazas son las amenazas activas. Esos involucran algunas modificaciones del flujo de datos o la creación de un falso flujo. Podemos subdividir esas amenazas en tres categorías: modificación del flujo de mensajes, denegación del servicio de mensajes, y enmascaramiento.

Modificación del flujo de mensajes simplemente significa que alguna parte de un mensaje legitimo es alterado, o que mensajes son retardados, reconstruidos, o reordenados, en orden a producir un efecto no autorizado. Por ejemplo, un mensaje contiene "Permitir a John Smit leer archivos confidenciales de contabilidad" es modificado por el contenido "permitir a Fred Brown leer archivos confidenciales de contabilidad".

La denegación de servicio previene o inhibe el normal uso o gestión de las facilidades de comunicaciones. Este ataque puede tener un destino especifico; por ejemplo, una entidad puede suprimir todos los mensajes dirigidos a un destino particular. (ejemplo: el servicio de auditoria de seguridad). Otra forma de denegación de servicio es la disrupción de una red entera, mediante la deshabilitación de la red o mediante sobrecarga con mensajes tal que degraden el rendimiento.

Un enmascaramiento toma lugar cuando una entidad pretende ser una entidad diferente. Un ataque por enmascaramiento usualmente incluye uno o de las otras dos formas de ataques activos. Tales como un ataque puede tener lugar, por ejemplo, mediante la captura y reconstrucción de una secuencia de autenticación.

Las amenazas activas presentan las características opuestas de las amenazas activas. Mientras que ataques pasivos son dificiles de detectar, las medidas están disponibles para prevenir sus sucesos. Por otro lado, es mas o menos dificultoso prevenir de manera absoluta ataques activos, ya que este podría requerir la protección fisica de

todas las facilidades de comunicaciones y rutas todo el tiempo. En vez de esto, el objetivo con respecto a los ataques activos es detectar esos ataques y recuperar de cualquier disrupción o retardo causado por el ataque. Porque la detección tiene un efecto disuasivo, este puede también contribuir a la prevención.

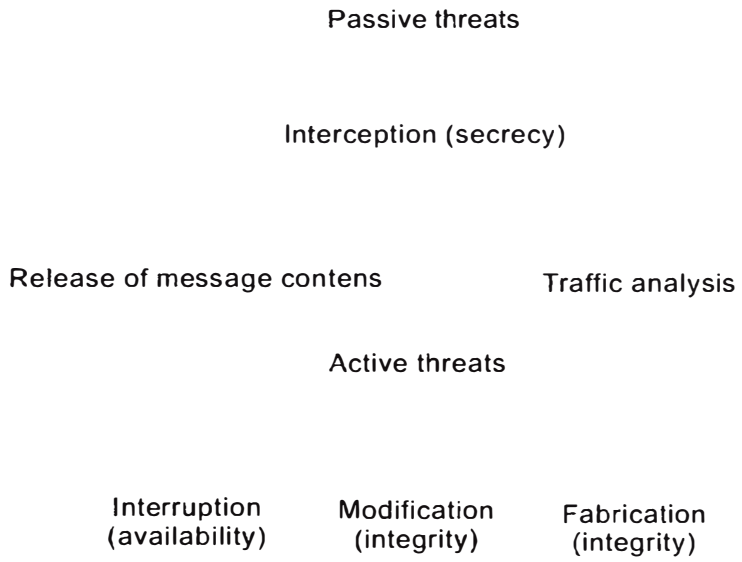


Figura 1.17 Amenazas de seguridad de red activas y pasivas

vi. Amenazas al sistema de gestión de red

Ya que la gestión de red es un conjunto de aplicaciones y bases de datos sobre varias plataformas hardware distribuida en cada parte de la configuración, todas las amenazas discutidas al inicio en este capitulo pueden ser consideradas amenazas al sistema de gestión de red. En adición, tres seguridades concernientes específicamente a gestión de red pueden ser citados:

- Enmascaramiento de usuario: un usuario quien no esta autorizado a realizar funciones de gestión de red puede intentar acceder a aplicaciones e información de gestión de red.
- Enmascaramiento del gestor de red: un sistema computador puede enmascarar como una estación gestora de red (un servidor de gestión en la figura 1.5).

- Interferencias en el intercambio gestor – agente: una amenaza es la observación del tráfico del protocolo gestor – agente para extraer información de gestión sensitiva. Mas dañino sería la modificación de tal tráfico para interrumpir la operación del agente o los recursos que esta administrando.

2) Funciones de gestión de seguridad

Las facilidades de seguridad de un sistema o red de sistemas consiste de un conjunto de mecanismos y servicios de seguridad. La función de gestión de seguridad puede ser agrupado en tres categorías:

- Mantenimiento de la información de seguridad.
- Control del servicio de acceso a los recursos.
- Control del proceso de encriptación

i. Mantenimiento de la información de seguridad

Como en otras áreas de gestión de red, la gestión de seguridad esta basado en el uso de información de gestión intercambiada entre gestores y agentes. La misma clase de operaciones son empleados para la gestión de seguridad como para otras áreas de gestión de red; la diferencia esta solo en la naturaleza de la información de gestión usada. Ejemplos de objetos apropiados para la gestión de seguridad incluye claves, información de autenticación, información de derechos de acceso, y parámetros operativos de servicios de seguridad y mecanismos.

La gestión de seguridad mantiene la contabilidad de actividades, o intentos de actividades, con esos objetos de seguridad en orden a detectar y recuperar del intento o ataque de seguridad exitoso. Esto incluye las siguientes funciones relativas al mantenimiento de la información de seguridad:

- Registro de eventos (logging)
- Monitorización del seguimiento de auditorias de seguridad
- Monitorización del uso y los usuarios de los recursos relativos a la seguridad
- Reporte de violaciones de seguridad
- Recepción de notificaciones de violaciones de seguridad

- Mantenimiento y examen de logs de seguridad
- Mantenimiento de copias de respaldo de todo o parte de los archivos relativos a seguridad
- Mantenimiento general de perfiles de usuarios de red, y uso de perfiles para recursos específicos, habilitar referencias de conformidad a los perfiles de seguridad designados.

ii. Control de servicios de acceso a los recursos

Uno de los servicios centrales de cualquier facilidad de seguridad es acceso y control. Acceso y control involucra servicios de autenticación y autorización y la actual decisión para conceder o denegar acceso a recursos específicos. El servicio de control de acceso se diseña para proteger un amplio rango de recursos de red. Entre esos recursos que concierne particularmente a las funciones de gestión de red son:

- Códigos de seguridad
- Origen de enrutamiento y registro de información de ruta
- Directorios
- Tablas de enrutamiento
- Niveles umbrales de alarmas
- Tablas de contabilización

La gestión de seguridad gestiona el servicio de control de acceso mediante un mantenimiento general de los perfiles de usuarios de red y perfiles de uso para recursos específicos y mediante la configuración de prioridades de acceso. Las funciones de gestión de seguridad habilitan a los usuarios a crear y borrar objetos relativos s seguridad, cambiar sus atributos o estados, y afectar la relación entre objetos de seguridad.

iii. Control del proceso de encriptación

La gestión de seguridad debe ser capaz de encriptar cualquier intercambio entre gestores y agentes, como sea necesario. En adición, la gestión de seguridad debería facilitar el uso de encriptación mediante otras entidades de red. Esta función es también responsable por la designación de los algoritmos de encriptación y proveer la distribución de claves.

1.6 Herramientas de gestión de red

A lo largo de los años se han requerido diversas soluciones, generalmente de tipo propietario, para la gestión de las redes de comunicaciones. Actualmente, con el mayor número y heterogeneidad de elementos junto a la mayor importancia que han adquirido las redes de comunicaciones para la empresa, se exigen nuevos enfoques.

1.6.1 Evolución de las redes de telecomunicaciones

Las redes de telecomunicaciones dentro del ámbito informático han evolucionado a partir de la necesidad de compartir información y procesos con usuarios remotos. En una primera fase se desarrollaron los grandes ordenadores: éstos eran extremadamente engorrosos de utilizar y caros. Estos primeros ordenadores tenían un uso local y eran manejados por una única persona o interfaz. Posteriormente, los sistemas operativos permitieron el acceso de múltiples usuarios que interactuaban en principio también en un modo local. La gestión de los equipos, cuando existía, era pues necesariamente local, y los mecanismos específicos de cada fabricante de ordenador. Ver figura 1.18

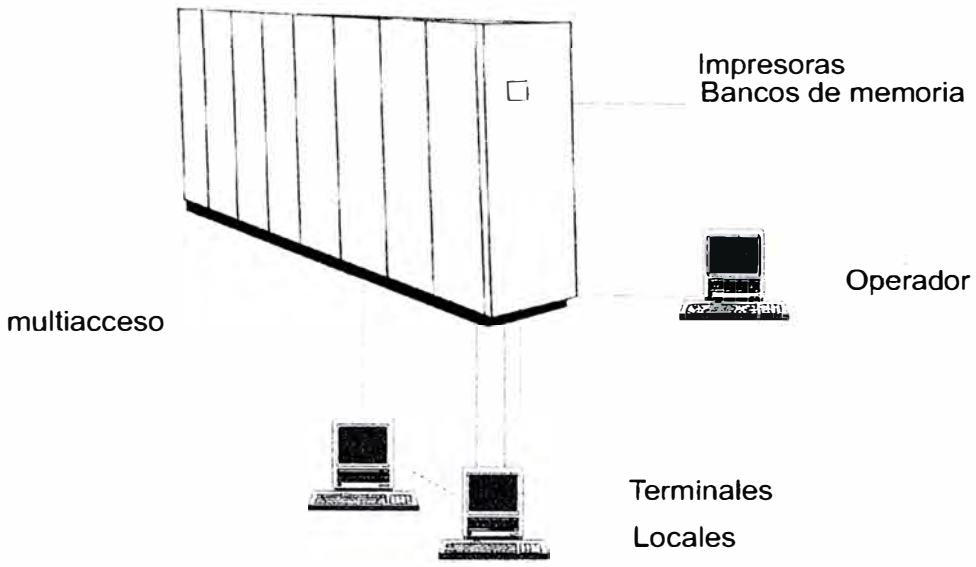


Figura 1.18 Esquema de un sistema formado por un único computador multiacceso y con gestión local

Más adelante, el uso de redes de telecomunicaciones permitió el acceso remoto de equipos terminales a los grandes ordenadores. Las redes de tecnología conmutada y el uso de módems eran más baratos de utilizar que el coste que comportaba la disposición de múltiples ordenadores. El único era de tipo multiacceso y se accedía a éste de modo local, o remotamente mediante el uso y equipos terminales (inicialmente teletipos). La gestión de red seguía siendo básicamente centralizado y basada en métodos del fabricante del mismo ordenador. Si bien esa gestión ya no cubría todos los elementos que entraban en la red de comunicaciones. Ver figura 1.19.

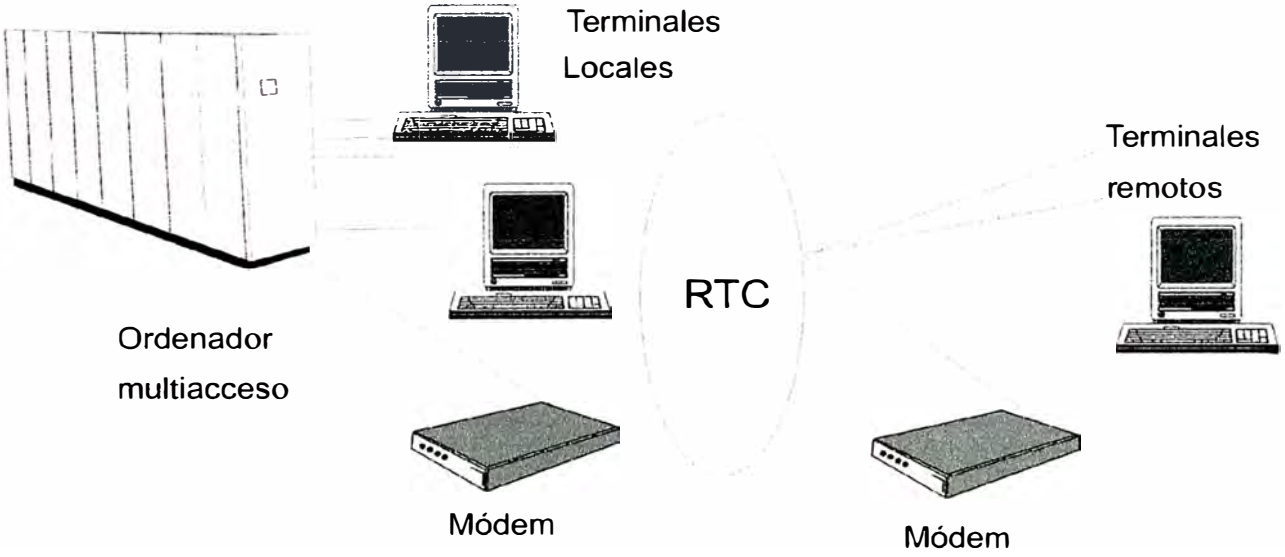


Figura 1.19 Esquema de un sistema formado por un único computador multiacceso y con conexión a terminales de acceso remoto mediante el uso de módems

A medida que creció el uso del ordenador y aumentó el número de conexiones de equipos terminales éste, fue necesario reducir la cantidad de módems utilizados debido a sus elevados costes. La solución fue la introducción del multiplexor que permitía integrar múltiples conexiones de equipos terminales en una sola línea de comunicación con lo que aumentaba el rendimiento. De esta forma, no eran necesarios tantos módems y se reducía el coste de las telecomunicaciones. Ver figura 1.20.

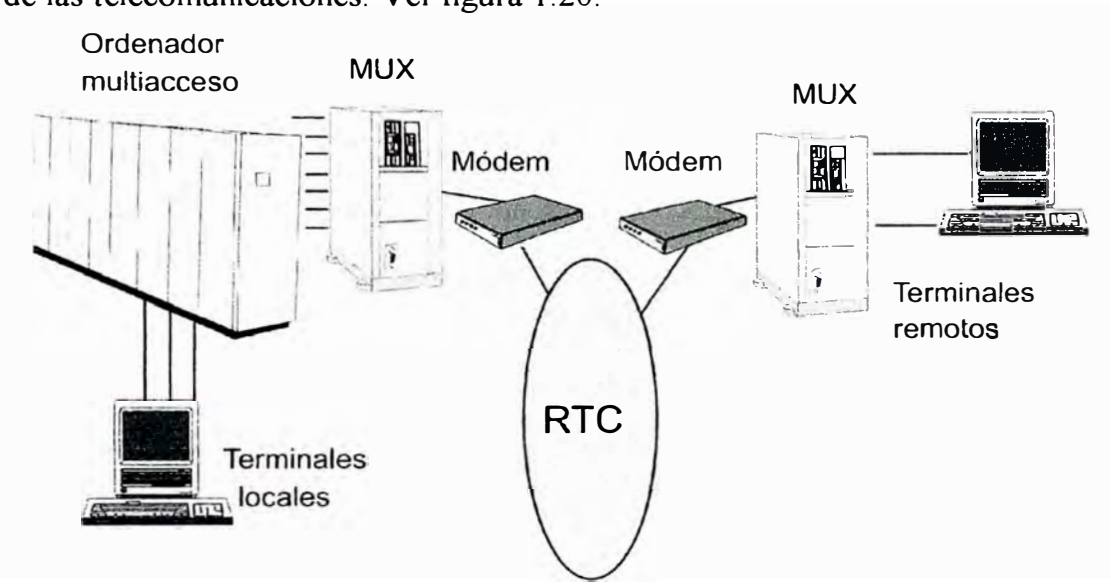


Figura 1.20 Esquema de un sistema formado por un único computador con conexión de terminales de acceso remoto a través de multiplexores

A medida que el progreso tecnológico abarataba los costes de la introducción de ordenadores en la empresa, las redes pasaron de tener configuraciones centralizadas a configuraciones de tipo distribuido con múltiples ordenadores. De esta forma, si bien en un principio se seguían utilizando redes RTC con módems, eran los ordenadores multiacceso quienes se interconectaban de forma interna. La gestión de red empezó a pasar de modelos centralizados a plantearse de modo distribuido o jerárquicamente distribuido en función del rango de los ordenadores en la red. Ver figura 1.21.

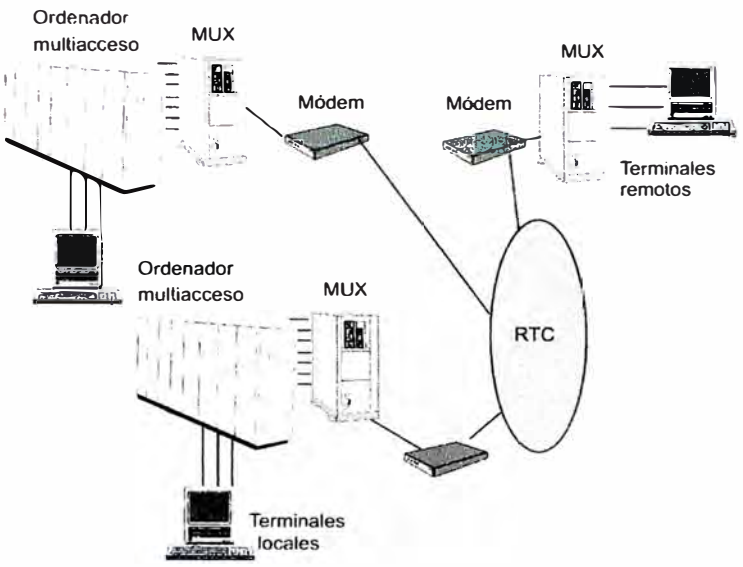


Figura 1.21 Esquema de un sistema formado por un conjunto de ordenadores actuando de forma distribuida conectados a través de una RTC

Conforme la interacción mutua del sistema distribuido de ordenadores iba aumentando fue haciéndose más necesario el uso de líneas dedicadas que permitieran reducir el coste debido al tráfico de información por las redes. Las empresas alquilaban líneas a los operadores de redes y eso permitía ofrecer costes menores en comunicaciones. La gestión de red se plantea de forma distribuida.

A raíz del crecimiento del tráfico telefónico en las redes de ordenadores se hace cada vez más necesario el empleo de líneas telefónicas privadas en las grandes corporaciones. A medida que la tecnología avance, se introducirán, además, líneas digitales que se adecuen mejor al tráfico generado por las comunicaciones entre ordenadores. Ver figura 1.22 y 1.23

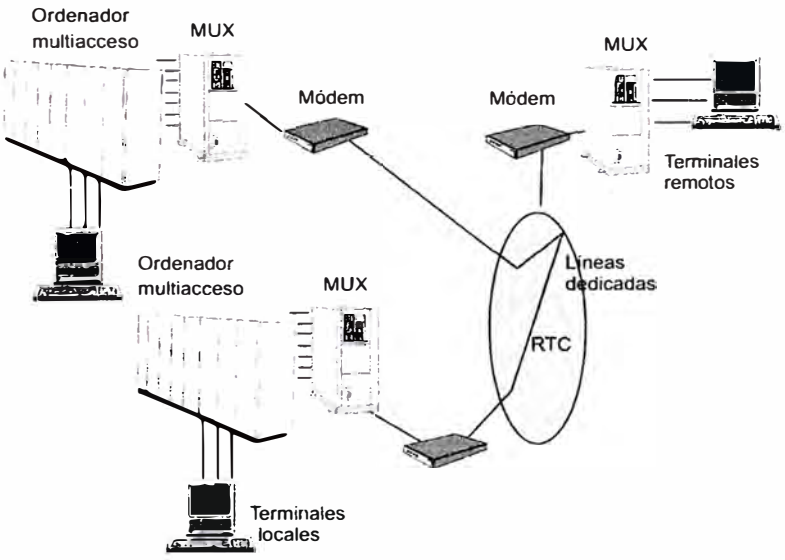


Figura 1.22 Esquema de un sistema formado por un conjunto de ordenadores que actúan de forma distribuida, conectados vía líneas dedicadas

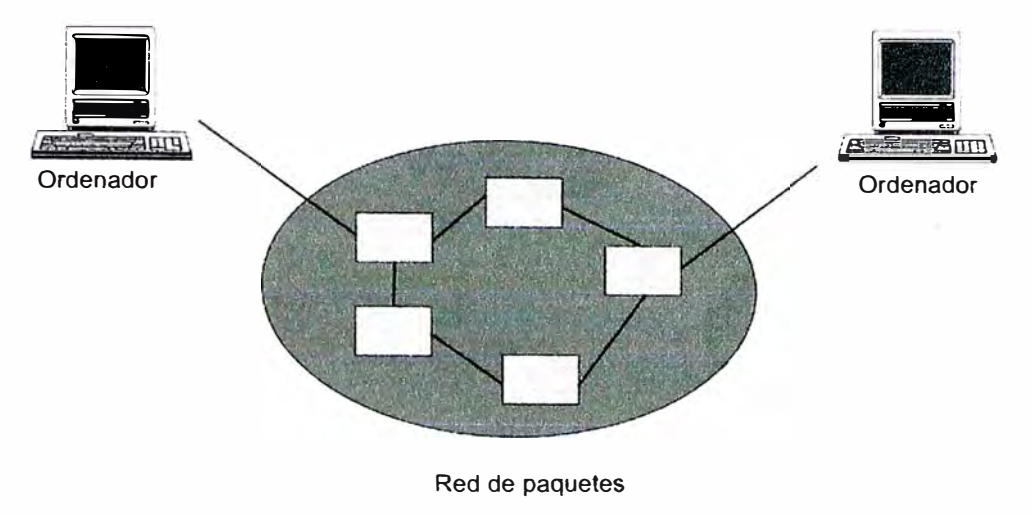


Figura 1.23 Esquema de un sistema formado por un conjunto de ordenadores que actúan de forma distribuida,conectados según una red digital o de paquetes

La entrada de las comunicaciones de tipo digital permitió optimizar la transferencia de información entre ordenadores. Nacieron redes como RDSI de conmutación de circuitos para terminales multimedia y otras redes basadas en conmutación de paquetes como la que utiliza la norma X.25.

Más adelante, con el empleo masivo de terminales tipo PC en las grandes corporaciones, se desarrollaron redes locales en conexión con redes de área extendida para poder cubrir las distancias correspondientes a campus o ciudades. Otros estándares como Frame Relay o ATM se han desarrollado para permitir esa interconexión de redes locales que pueden estar situadas de forma remota. En estos casos la proliferación de múltiples fabricantes distintos en el desarrollo de los terminales y dispositivos de interconexión de red hace complicada la gestión de este tipo de redes heterogéneas. Es por ello que a partir de esos momentos, resulta evidente la necesidad de diseñar mecanismos de estandarización para poder gestionar la creciente complejidad de los sistemas de redes. Ver figura 1.24

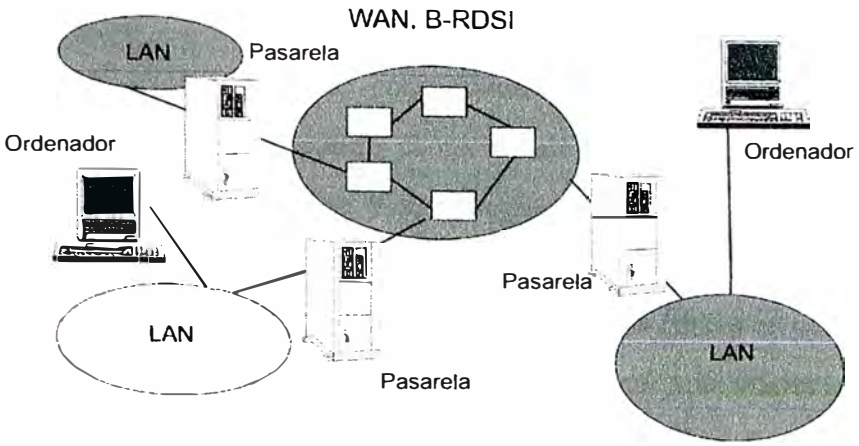


Figura 1.24 Esquema de un sistema formado por un conjunto de redes locales interconectadas por una red de paquetes, una red de área amplia (WAN) o una red de tipo B-RDSI

De esta forma, surgieron diversos organismos de estandarización que trataron de solucionar el problema de la gestión en redes heterogéneas, como IETF que definió el protocolo SNMP o como **ISO,** que hizo lo propio con el protocolo CMIP.

Se puede, pues, hablar de distintos tipos de gestión según las configuraciones de los escenarios, es decir, una gestión autónoma donde las redes tienen gestión local en cada nodo; una gestión homogénea con redes homogéneas con un único nodo de gestión centralizado; finalmente, una gestión heterogénea, con la ampliación de las redes con la interconexión de productos heterogéneos. Este sería el caso del siguiente ejemplo: una organización que interconecta sus sistemas de información con diferentes redes de comunicaciones.

El caso de utilizar sistemas de gestión de red propietarios trae consigo las siguientes consecuencias:
un plano de usuario (operador de red) con una multiplicidad de interfaces de usuario; un plano de aplicación (de gestión) con distintos programas de aplicación con funcionalidad similar; y, finalmente, un plano de información (de gestión): con una duplicidad y posible inconsistencia de la información almacenada en las bases de datos. Todo ello, dificulta el cumplimiento de que la gestión de red sea efectiva desde el punto de vista del coste.

Como solución se plantea una gestión integrada, en la que se normalizan las comunicaciones con la especificación de un protocolo entre elemento de red y centro de gestión, y la normalización de la información donde el centro de gestión debe poder conocer a los elementos de red mediante su nombre y sus propiedades visibles. Por tanto, debe haber también una definición sintacticamente uniforme de los elementos de red.

Existen una serie de modelos de gestión normalizados, en los cuales es posible el acceso los recursos gestionados. Se normaliza el protocolo de comunicaciones, el modelo de información de gestión y las definiciones de información de gestión. Los modelos de gestión de red tradicionales más importantes son la arquitectura TMN (ITU-T), el modelo de gestión OSI (ISO) con el protocolo CMIP y el modelo de gestión Internet (IETF), basado en el protocolo SNMP. Más recientemente han adquirido importancia el modelo DM1 (DMTF), la gestión por agentes inteligentes y la gestión por Web.

1.6.2 Modelos para la monitorización y el control de red

La gestión de red ha evolucionado desde la gestión basada en arquitecturas de red de tipo propietario hasta el uso, hoy ya masivo, de plataformas de gestión basadas principalmente en sistemas operativos UNIX o NT/WIN2000/WIN2003. Estas plataformas de gestión se implementan según una integración de aplicaciones compatibles y que permiten una gran flexibilidad de uso en la gestión de redes heterogénea (GHEI).

Existen también los productos específicos para la gestión de redes de área local, tanto para segmentos independientes como específicos, para redes de PCs o para determinados elementos de red. Finalmente, existen también los integradores de sistemas de gestión.

a) Arquitecturas propietarias

Desde siempre los fabricantes líderes en sistemas de gestión han tratado de imponer estándares de facto. Actualmente se trata de una tendencia que está cayendo en desuso. Las razones principales se basan en la cada vez menor cuota de mercado de estos fabricantes líderes y de la cada vez mayor complejidad de los entornos de red, formados por extensas interconexiones de redes y servicios que dificultan su control y gestión por parte de unos pocos fabricantes.

Entre las arquitecturas de red más importantes se encuentran: IBM, Xerox, Novell, Ungerman- Bass, 3 COM, Banyan, Proteon y AT&T. A continuación se describen algunas de ellas.

IBM network management architecture:

Open network management (ONA) es el marco de trabajo para los sistemas de gestión IBM (ver figura 1.25). Se definen tres grandes tipos de elementos que realizan funciones de gestión:

- Puntos focales, que proporcionan control centralizado, p. e. Netview.
- Puntos de entrada, que pueden ser dispositivos SNA en general.
- Puntos de servicio, que proporcionan servicios de gestión SNA.

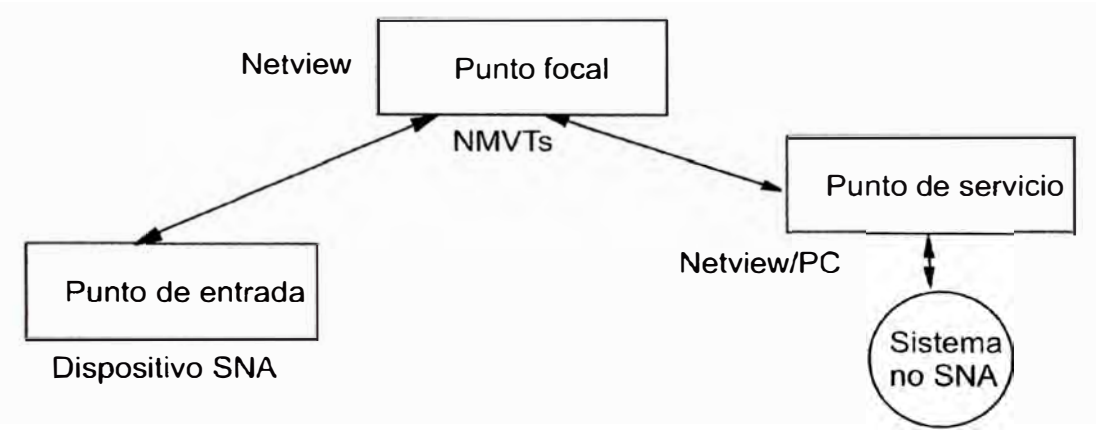


Figura 1.25 Esquema de la arquitectura de gestión de red IBM. Las plataformas de gestión que utilizan la arquitectura de red IBM pueden ser: Netview para la gestión de redes SNA, LAN Network Manager para la gestión de redes Token Ring y Netview/6000 para la gestión SNMP (Karat).

Novell:

Novell utiliza un sistema operativo de red, basado en una evolución del Netware. Recientemente Novell ha introducido CMISE y CMIP en sus sistemas de gestión de red. Actualmente Novell está migrando su torre de protocolos IPX al estándar IP.

Arquitectura de gestión de red AT&T:

La arquitectura del sistema de gestión múltiple de red, *UNMA (Unified Network* Management Architecture) de AT&T está basada en OSI (Ver figura 1.26). UNMA consiste de una arquitectura en tres capas ligadas. El nivel más bajo está formado por los elementos de la red, es decir, componentes fisicos y lógicos que comprende la red

que se quiere gestionar. El segundo nivel lo forman Element Management Systems (EMS), que administran y gestionan elementos de red. El tercer nivel consiste de sistemas de gestión integrados que unen conjuntamente los EMSs de los tres niveles.

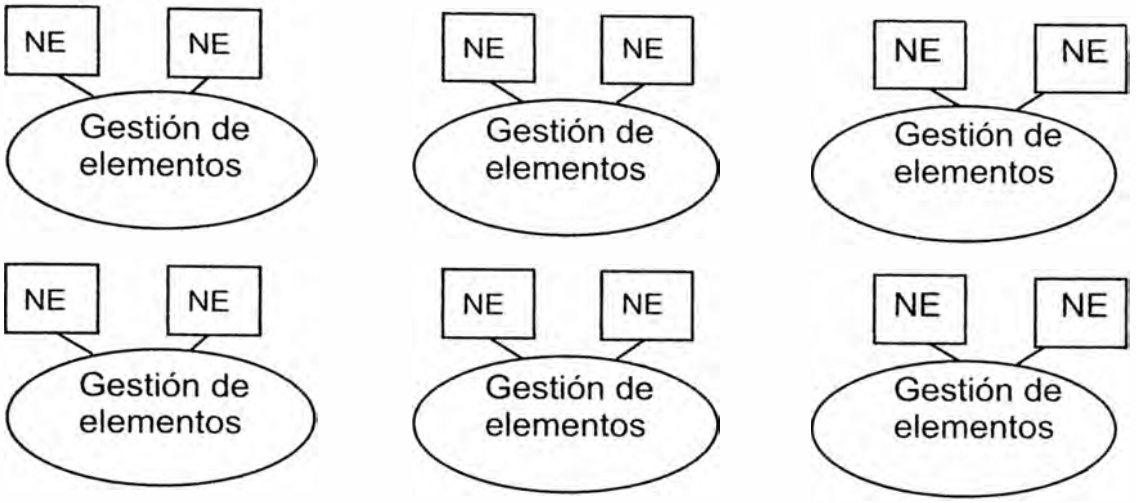


Figura 1.26 Esquema de arquitectura de red de AT&T

b) Plataformas de gestión

Las plataformas de gestión utilizan una integración de aplicaciones para poder adaptarse al entorno cambiante y complejo de los elementos de red que se quieran gestionar. Entre las aplicaciones más usuales que se incorporan, destacan los *MIB browser* (navegadores u hojeadores de MIB) como interfaces de usuario del protocolo SNMP; el *discover,* que permite autodescubrir equipos y topologías de la red; la programación de sondeos de variables de la MIB; la programación de acciones ante alarmas; y, finalmente, los visualizadores gráficos de valores de variables de MIB.

Dentro de la categoría de sistemas basados en UNIX podemos encontrar los siguientes:

- Enterprise Management Architecture de Digital (PolyCenter)
- OpenView Network Management server de HP
- SunNet Manager de Sun Microsystems (Solstice)
- Spectrum de Cabletron
- Dual Manager de Netlabs (OverLord)
- NMC 3000 de Network Gestores

- NetExpert de Objetive Systems Integrators
- NMS/Core de Teknekron Communications Systems
- Network Knowledge Systems de Applied Computing Devices
- IBM Netview/6000 para AIX
- TME 10 de Tivoli.

Las plataformas de gestión posibilitan mayor grado de integración multifabricante que el esquema gestor de gestores. Las interacciones con otros sistemas de gestión de diferentes fabricantes se realizan a través de un interfaz de programación de aplicaciones estándares (API) y un conjunto estándar de definiciones de datos de gestión.

c) Clases de productos de gestión

Se pueden distinguir las siguientes clases de productos de gestión para LANs:

- Productos *standalone*, dirigidos especialmente a monitorización, análisis de Tes., seguridad y necesidades de tarificación.
- Plataformas de gestión de red que proporcionan un entorno en el cual las aplicaciones pueden ser desarrolladas, mejoradas e intercambiadas.
- Herramientas de gestión de LANs de PCs, que incluyen soluciones de propósito especial como una combinación de funciones de sistemas operativos en LANs y añadidos especiales.
- Sistemas de gestión de elementos LAN basados en estándares abiertos o *de facto* que ofrecen una aceptable funcionalidad a elementos LAN, tales como segmentos LAN, *hubs* cableados, dispositivos de interconexión LAN, FDDI, PBXs y conexión a integradores de gestores de red.
- Integradores que probablemente soportan elementos de gestión de sistemas LAN, MAN, y WAN en la misma plataforma.

d) Productos de gestión de LANs standalone

Los productos *standalone* sirven áreas funcionales especiales sin intención de aplicabilidad a la integración de gestión de LANs. Esto es, instrumentos de test de LANs, analizadores de LAN, sistemas de monitorización de LAN, u otros instrumentos especiales.

Los productos standalone suelen evaluarse de acuerdo a los siguientes criterios:

- interfaz de usuario
- protocolos que son soportados
- nivel de decodificación
- el tipo de LANs / WANs soportadas
- buffers de captura
- filtros
- soporte para monitorización distribuida
- niveles de disparo
- búsquedas
- etiquetas temporales
- generadores de tráfico
- chequeo de cables
- convención en el nombrado
- diagnóstico por sí mismo
- impresión por hard-copy
- protección de passwords

Entre los instrumentos más importantes para tests de LANs se incluyen: óhmetros, *testers*, conectores coaxiales, conectores en T, terminadores, osciloscopios y reflectores en el dominio temporal.

Los analizadores de LANs tienen como fin el soporte de gestión de prestaciones y de fallos. En general ofrecen indicaciones sobre:

- Servicio: retardos, tiempo de transferencias, tiempo de diálogo.
- Uso: uso global del ancho de banda, uso específico por aplicaciones y/o usuarios.
- Perfiles de usuario: qué aplicaciones y qué actividades.
- Perfiles de servidores: uso interno, colas..

Los sistemas analizadores de LANs, suelen permitir la monitorización de precisión y disponer de herramienta de diagnóstico para gestores de red. Analizan tanto redes Ethernet como Token Ring (entre otros protocolos). Verifican tráfico en tiempo real, conectividad y problemas asociados, actividades de ficheros en tiempo real,

conectividad con bridges y retardos asociados, test de *hardware* para servidores y simulación de cargas.

Los sistemas de monitorización de LANs forman una familia de herramientas que soportan monitorización continua, ofreciendo una unidad de colección de datos en cada segmento LAN. Las funciones que suele realizar el *software* son del tipo: número de canales de entrada, filtros, etiquetas temporales, estaciones de monitorización, buffers (colas), niveles de disparo, presentación, lista de alarmas, protocolos medidos, encabezamientos, estadísticas y informes de errores, interfaz a bases de datos u otros y soporte SNMP. Entre los productos más representativos, se suele citar el Sniffer (llamado Watchdog) de Network General. Existen equipos más recientes como el Network Advisor de HP o el Trakker de Concord Communications.

Existen también instrumentos especiales de LANs. Estos instrumentos especiales soportan áreas de gestión de LANs específicas. Por ejemplo, la tarificación utiliza en particular dos tipos de productos:

medidores de *software* y herramientas de gestión de pruebas de auditabilidad, así como herramientas de documentación.

Gestión de LANs de PCs

Los sistemas de gestión de LANs de PCs están orientados a supervisión de eestatus, determinación de fallos y muy básicas capacidades de administración. Actualmente las últimas versiones de Windows NT /2000/2003 (Microsoft) está aportando interesantes novedades para la administración y monitorización de las redes locales de PCs. Además, y aparte de IBM, han dominado el mercado otras compañías como Novell, 3Com y Banyan. Otros productos interesantes en el área de LANs de PC son StarLAN de AT&T y LocalTalk de Apple. Como resultado de la tremenda presión de los usuarios hacia aplicaciones multiprotocolo, interoperabilidad, etc. las compañías líderes han reaccionado hacia:

- Abrir gateways a TCP/IP.
- Acuerdos de cooperación (p.e. IBM y Novell, IBM y 3Com, Banyan y Novell).
- Soporte de SNMP sobre redes locales.
- Soporte de CMOT sobre redes con muchos nodos.

Adquisición de productos de monitorización para proporcionar a los usuarios

con monitorización mejorada y gestión.

Actualmente son las plataformas abiertas de gestión de red las que constituyen la base común para que a través de APIs (interfaces de programación de aplicaciones) las aplicaciones de gestión puedan realizar la recogida de datos de los elementos de red. Estas aplicaciones son accesibles normalmente por medio de lenguaje C y permiten que una aplicación pueda invocar una función de otra.

DMI (Desktop Management Interface) fue el primer API de gestión de PCs independiente de protocolos y sistemas operativos (abril 1994). Es uno de los principales componentes de la solución de gestión de DMTF (Desktop Management Task Force), consorcio industrial que persigue proveer una plataforma PC susceptible de ser gestionada en modo flexible. Los ficheros MIF (Management Information Format) provistos con cada producto gestionable definen, por su parte, los atributos gestionables del estándar en categorías tales como sistemas PC, servidores, impresoras, adaptadores LAN, módems y aplicaciones *software*. La arquitectura DMI incluye el nivel de servicio, un programa local que recoge información de los productos, gestiona esa información en bases de datos MIF, y la pasa a las aplicaciones de gestión cuando es solicitada. Controla, además, su comunicación con las aplicaciones de gestión de MI (Management Interface) y con los productos gestionables a través de CI (Component Interface).

SMS (Systems Management Server) de Microsoft es otra plataforma diseñada para soportar tareas de gestión de sistemas, tales como inventarios *hardware* y *software* LAN y distribución electrónica de *software,* en entornos LAN Manager y Windows NT Advanced Server (NTAS) de Microsoft, Netware de Novell, Pathworks de Digital y LAN Server de IBM. Sobre plataformas Window NTAS, SMS utiliza DM1. La estrategia de gestión LAN de Microsoft se centra fundamentalmente en el control de los sistemas conectados a la LAN, dejando la gestión de dispositivos de red, como *ruteadores* y *hubs,* a soluciones de mayor nivel que incluyan estaciones basadas en SNMP.

NMS (Netware Management System) de Novell es una familia de productos software que constituye una solución abierta para la gestión de LANs NetWare y dispositivos de internetworking como ruteadores y hubs. NMS comprende tres productos software que corren sobre una consola central y agentes que residen en los

dispositivos de la red. El *software* de gestión de NMS corre bajo PCs Windows y sus funciones clave son la exploración y mapeo de dispositivos de ínter conectividad, gestión de direcciones de red, rastreo de condiciones de alarmas y su almacenamiento en una base de datos. Dispone de una herramienta de análisis experto para la solución de problemas y dispone de la capacidad de gestionar cualquier dispositivo SNMP.

e) Sistemas de gestión de elementos de red de área local (LAN)

Los sistemas de gestión de elementos de redes de área local gestionan LANs de propósito general. Los sistemas de gestión de elementos en esta sección están agrupados en:

- ethernet
- token Ring
- concentradores cableados, *hubs*
- dispositivos de interconexión
- backbones de LANs, como por ejemplo FDDI
- plataformas de gestión LAN

Los segmentos de redes de área local basados en Ethernet son todavía líderes en el mercado. Por ello, es extremadamente importante proporcionar capacidades de monitorización y gestión para esos segmentos. Las empresas líderes en este campo son DEC a través de Ethernim y HP, con LANProbe, Probeview y Openview.

IBM está liderando este mercado con herramientas de gestión token ring y con la gama de productos LAN Network Manager. Hay dos opciones de gestión básicas: gestión *standalone* de componentes conectados, o centralizados y gestión integrada vía Netview.

Los productos de gestión de redes LAN de IBM gestionan LANs al nivel de estación de trabajo, y con Netview como computador Host. Ellos hacen seguimiento y control de acceso a dispositivos en cada LAN. IBM tiene cinco grandes productos de gestión de redes Token-Ring:

- IBM LAN Network Management version 1.0.
- IBM LAN Network Management version 1.1.
- IBM LAN Network Management Entry.
- IBM LAN Station Manager.

- IBM 8230 Controlled Access Unit (CAU).

Se pueden distinguir las siguientes funciones en la gestión de elementos token ring como las más importantes:

- monitorización activa
- monitorización de errores en el anillo
- servidor de parámetros al anillo
- servidor de configuración del anillo
- servidor de puente LAN
- trazas y prestaciones
- gestor de estaciones
- unidad de acceso controlado
- gestor de LANs
- Netview (punto de control SNA)

Por otra parte, los concentradores cableados y hubs están llegando a ser el objetivo de la gestión de redes en LAN. Muchos analistas predicen que la gestión de red basada en bridges y ruteadores va encaminada a gestión basada en hubs. Uno de los sistemas de gestión más representativos es el que Cabletron presenta con el Spectrum Network Management.

Respecto a las redes de alta velocidad, se identifican casi exclusivamente como redes FDDI y Fast/Gigabit Ethernet. Los estándares de gestión en algunos tipos de redes todavía no están completamente definidos.

Los sistemas de gestión de elementos para LANs interconectados emplazan tanto gestión de LANs como gestión de WANs en el mismo lugar, el control del centro de gestión de red. Cada objeto gestionado individual, tales como repetidor, puente, *bruteador; ruteador,* y *gateway* es parte del segmento de LAN local. Pero al mismo tiempo, los mismos componentes son parte de la topología MAN y/o WAN. Como productos destacados se puede citar el CiscoWorks de Cisco.

Finalmente, la mayor parte de sistemas de gestión de elementos multisegmento tienen la capacidad de ofrecer gestión multisegmento desde plataformas estándares o propietarias. Estas combinan fast packet, conmutación, tecnologías de encaminamiento con FDDI, ethernet *y hubs token* ring que se gestionan desde una plataforma común y ofrecen mejores prestaciones por el menor coste.

f) Integradores para gestión de LANs

Para la gestión de redes heterogéneas se han adoptado diversas estrategias a lo largo del tiempo. Al principio era usual utilizar una integración de gestión de LANs jerárquica, mediante un esquema de gestor de gestores. Este esquema era válido pero no permitía suficiente flexibilidad en los cambios de configuración de la red, ya que exigía la modificación de los programas continuamente. El procesado de la información y la fiabilidad de un único nodo jerárquico superior (gestor de gestores) era también una limitación en redes de muchos nodos. Ver figura 1.27.

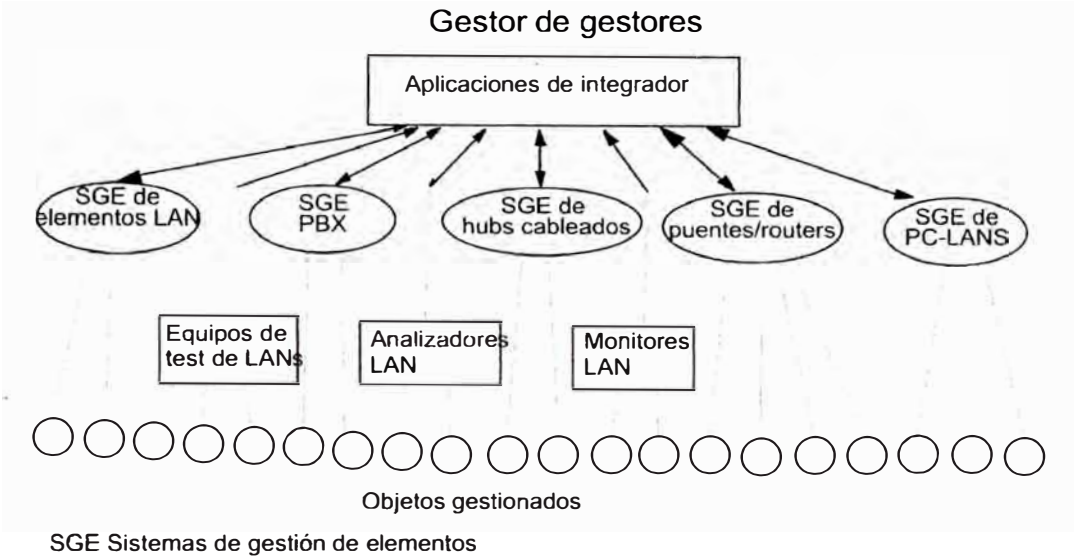
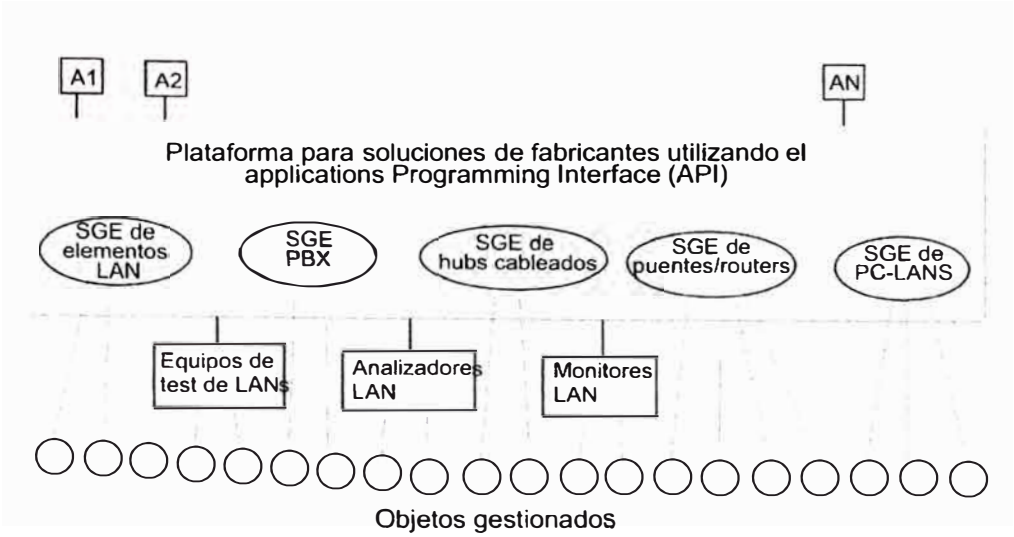


Figura 1.27 Configuración como gestor de gestores de redes

A medida que los fabricantes se fueron enfrentando con el problema de la gestión de gestores fueron adoptando otras soluciones como el uso de integración de gestión de LANs con plataformas. Actualmente el uso de plataformas de gestión que utilizan APIs *(Applications Programming Interfaces)* está muy extendido (ver figura 1.28). Finalmente, con el uso masivo de Internet, la gestión de red mediante Web y navegadores se está haciendo cada vez más normal, si bien los estándares están aún poco desarrollados.



SGE: Sistemas de gestión de elementos

Figura 1.28 Configuración como gestor que integra APIs para gestión de redes heterogéneas

Las aplicaciones sobre plataformas de gestión más frecuentes son las siguientes:

- gestión de equipos específicos
- gestión de incidencias a través de un Trouble Ticket System
- gestión de inventario
- gestión de cableado
- interacción con otros sistemas de gestión
- gestión de fallos mediante sistemas expertos
- gestión de sistemas,...

Por otra parte, las plataformas de gestión requieren de una integración entre esas aplicaciones. Existen tres tipos de integración entre aplicaciones: integración de comunicaciones, integración de interfaces de usuario e integración de información (ver figura 1.29). Sólo las dos primeras están solucionadas con el uso de una plataformas de gestión: las comunicaciones, dado que todas las aplicaciones usan los servicios de comunicaciones (API) de la plataforma y el interfaz de usuario, puesto que las aplicaciones comparten el interfaz de usuario de la plataforma.

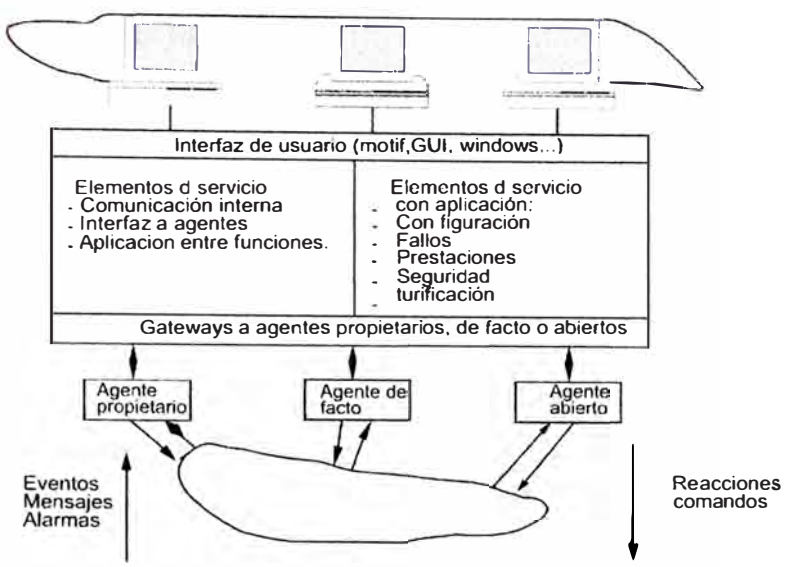


Figura 1.29 Arquitectura genérica de un producto de gestión de LANs actual

Respecto a la integración de información, se implementa una base de datos local de gestión dado que las aplicaciones de gestión requieren almacenar datos localmente, como datos de topología, datos administrativos, etc. Estos datos pueden formar parte de las MIB, pero no es frecuente. Las plataformas y algunas aplicaciones incorporan el uso de bases de datos relacionales para el almacenamiento local. Cada aplicación tiene necesidades de almacenamiento diferentes, pero con frecuencia existen datos comunes entre ellas. Como consecuencia, cada aplicación tiene su propia base de datos.

Dado que las plataformas actuales no permiten una integración de la información entre las aplicaciones (sólo admiten una emulación de consolas), se definen dos enfoques diferentes para su solución: un esquema universal de almacenamiento de datos, o bien el desarrollo de aplicaciones a la medida.

La integración puede realizarse de dos formas: mediante el uso de una plataforma o bien mediante el uso de un integrador. Con los productos de integración, se pueden identificar dos grandes grupos:

productos de emulación de consolas e integradores avanzados. Las soluciones más importantes basadas en productos de emulación de consolas son:

- Netview (IBM). Ver figura 1.30.
- Accumaster Integration (AT&T). Ver figura 1.31.

- DECmcc (DEC). Ver figura 1.32.

A continuación, en las siguientes figuras se presentan esquemáticamente las funcionalidades de estos integradores.

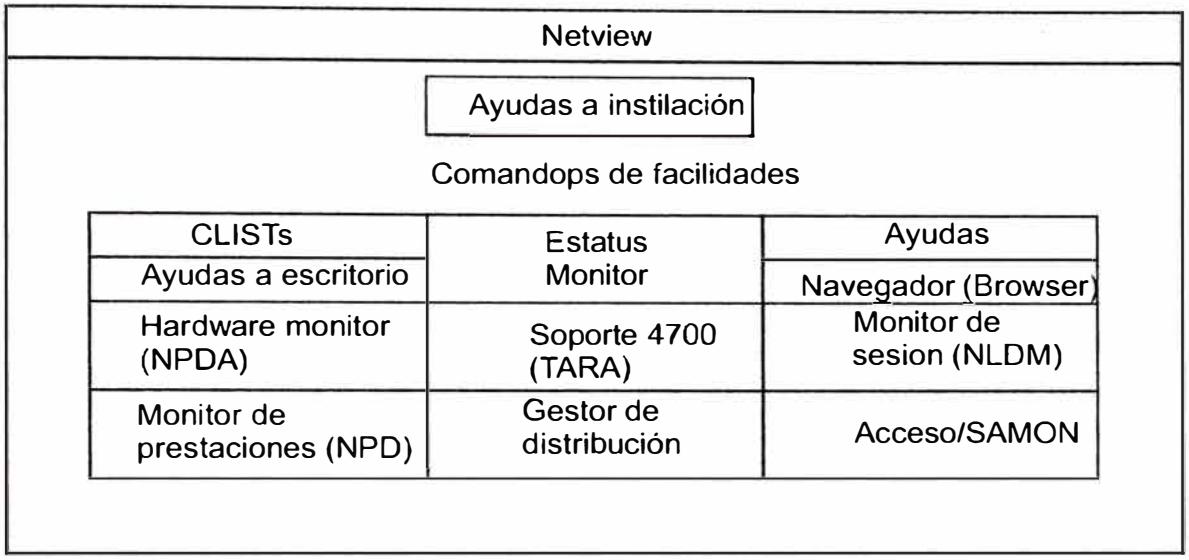


Figura 1.30 Estructura Netview (IBM)

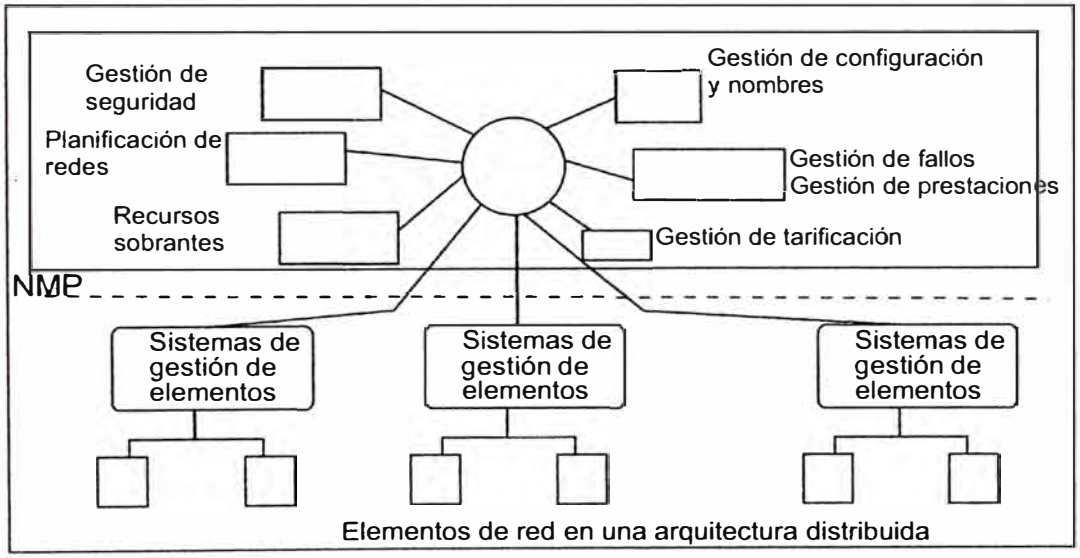


Figura 1.31 Accumaster Integrator Architecture

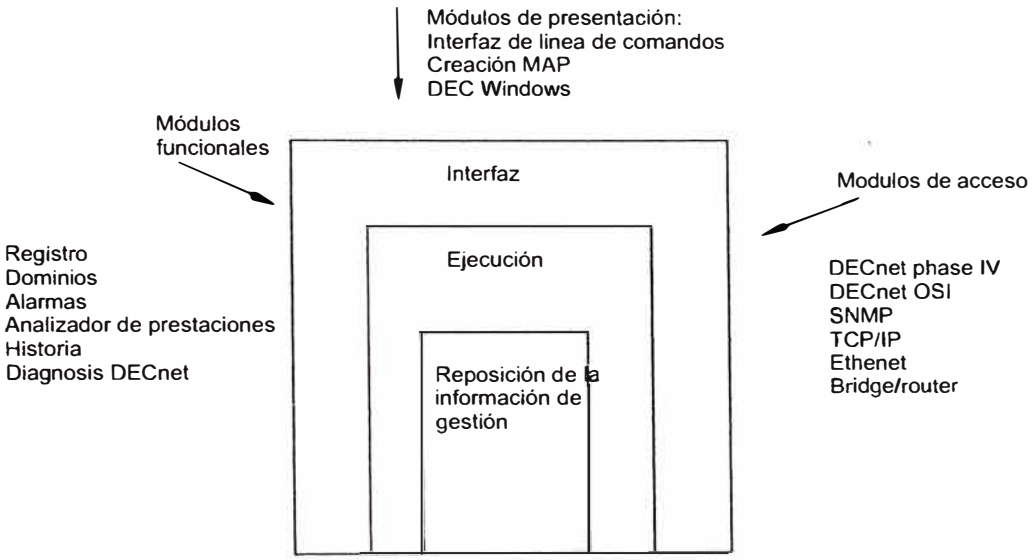


Figura 1.32 DECmcc Director

CAPITULO II

ARQUITECTURAS DE GESTIÓN DE RED

2.1 Conceptos de Arquitecturas de Gestión

Existen muchas propuestas de arquitecturas para gestión de sistemas distribuidos. Debido a la relativa madurez de la gestión de redes, y debido a que tanto la gestión de sistemas, como de aplicaciones requieren gestión de red, la mayoría de las arquitecturas de gestión integrada se basa en conceptos de gestión de redes.

Un modelo de referencia de gestión de sistemas tiene cuatro componentes principales:

- Gestores
- Objetos gestionados
- Servicios
- Entorno de mediación

2.1.1 Gestores

Los gestores son aplicaciones que implementan la funcionalidad de gestión. Proveen los servicios que interesan a los usuarios. Cada aplicación cubre un amplia área de gestión y debe exhibir un comportamiento consistente sobre varios tipos de configuraciones. Por ejemplo, las áreas funcionales de la arquitectura de gestión OSI.

2.1.2 Servicios

Los servicios proveen las facilidades comunes que las aplicaciones de gestión necesitan. Los tipos de servicios varían de acuerdo a la arquitectura. La arquitectura de gestión OSI especifica 13 servicios de gestión, los cuales soportan requerimientos en una o más áreas de aplicación. La arquitectura de gestión de Internet en cambio, no especifica servicios de gestión.

Algunos servicios de gestión incrementan la funcionalidad entre las aplicaciones de gestión y la información de gestión. Por ejemplo, algunas arquitecturas proveen un servicios de repositorio de información, el cual presenta las aplicaciones de gestión con un punto de vista lógico centralizado de la información de gestión.

Otros servicios de gestión incrementan la funcionalidad entre las aplicaciones de gestión y los usuarios finales. Por ejemplo, algunas arquitecturas proveen servicios de interfaz de usuario para las aplicaciones de gestión.

2.1.3 Objetos Gestionados

Un objeto gestionado es la información de gestión, desde el punto de vista de gestión, describe un recurso a ser gestionado, monitoreado y controlado. En otras palabras, un objeto gestionado es una representación abstracta de un recurso real a ser gestionado. Los recursos reales en sistemas distribuidos necesitan ser capturados y representados como objetos gestionados. Algunos puntos importantes acerca de objetos gestionados deben ser recalcados:

- Un objeto gestionado es una abstracción que esta disponibleal gestor y a los servicios. Algunos otros mecanismos, fuera del alcance de una arquitectura de gestión, mantienen las relaciones entre el objeto gestionado y el recurso.
- Un objeto gestionado puede representar uno o varios recursos.
- El mismo recurso puede ser representado por uno o varios objetos diferentes, cada uno representando un aspecto particular del recurso.
- No todos los recursos necesitan ser representados por objetos gestionados. Esto no significa que dicho recurso no exista, únicamente significa que no está disponible al sistema de gestión.

Los conceptos para describir objetos y la información relevante en la gestión se denominan en conjunto Modelos de Información. La aproximación del Modelo de Información usado para describir objetos gestionados podría ser entidad – relación, tipos de datos, o orientado a objetos. Por ejemplo, la gestión de Internet utiliza tipos de datos simples (escalares y arreglos bidimensionales de escalares) para representar los objetos gestionados. De otro lado, la gestión OSI, utiliza una aproximación orientada a objetos para su Modelo de Información.

2.1.4 Entorno de Mediación

El entorno de mediación gestiona la interacción entre aplicaciones dispares a través de un sistema heterogéneo.

El entorno de mediación puede proveer al cliente de un punto de vista del sistema a nivel de protocolo, como ocurre con CMIP o SNMP, o puede proveer un punto de vista a nivel de interfaz como en el caso de CORBA. La última aproximación define objetos computacionales independientes del protocolo que los sustenta, mientras que en los anteriores se define un protocolo que los clientes (aplicaciones, servicios, objetos gestionados) tienen que seguir para comunicarse.

El entorno de mediación usado para implementar un sistema es algunas veces diferente del utilizado para gestionarlo. Por ejemplo un sistema distribuido puede ser implementado utilizando llamadas a procedimientos remotos (RPC) mientras que podría ser gestionado utilizando agentes SNMP o CMIP. Con el advenimiento de sistemas distribuido orientados a objeto como CORBA, los modelos de implementación y de gestión tienden a compartir la misma infraestructura. Por ejemplo, CORBA podría ser usada para implementar y gestionar un sistema, bien adicionando objetos al sistema cuya tarea es gestionar otros objetos, o adicionando operaciones a las interfaces CORBA existentes para hacerlas gestionables.

2.2 Arquitecturas de gestión abiertas

2.2.1 Gestión de sistemas OSI

Aunque el origen de la gestión OSI puede decirse que ha sido encontrado en lo que establece ISO, la mayoría del trabajo se ha realizado en colaboración con la ITU-T (el anterior CCITT). Los estándares, que son el resultado de tal labor realizada, han sido publicados por estas organizaciones sin tener en cuenta las diferencias técnicas. Dentro del ITU-T, las recomendaciones de la Gestión OSI han sido publicadas como parte de la serie X.700.

El primer estándar que describe la Gestión OSI, es el Modelo OSI de Referencia. Esta norma identifica a la Gestión OSI como una área importante de trabajo y proporciona o provee las definiciones iniciales. Alrededor de los 80's, el Grupo de Trabajo Especial (ISO / TC 97/SC 21/WG 4 1) se formó dentro de ISO para llevar a cabo desarrollos de Gestión OSI. El primer resultado de este WG (WorkGroup) fue la Infraestructura de Gestión. Aunque la producción de esta infraestructura tomó considerable tiempo, generalmente no se

admitió como un punto de arranque adecuado. Se decidió por consiguiente producir un estándar adicional que se denominó Apreciación global de la Gestión OSI. Juntos estos estándares son los que proveen la base de la gestión OSI (Figura).

Titulo	ISO/IEC	ITU-T	Año de Publicación
OSI Management Framework	7498/4	X.700	1989
OSI Systems Management Overview	10040	X.701	1992

Figura 2.1 Base de la Gestión OSI

Aunque los Estándares de Gestión de Sistemas OSI están basados en conceptos de OO, los modelos MO no representan especificaciones completas de objeto. Los Modelos MO son esencialmente análisis de modelos de datos que son visibles externamente y de comportamientos, los cuales a través de la misma naturaleza de Análisis y Diseña en OO, forman la base o el fundamento del diseño de una interfaz. El paso de Mensajes a través de los objetos y el funcionamiento interno (privado) de estos (los objetos) aun no está especificado.

Esto tiene implicaciones importantes para el especificador del modelo MO y el diseñador/implementador (designer/implementor) quienes son los que deben desarrollar o implementar al modelo MO. El especificador del modelo MO está sólo relacionado con un conjunto restringido de (información) requisitos o requerimientos funcionales, pero el diseñador/implementador (designer/implementor) deben acomodar otros requisitos o requerimientos funcionales (incluyendo el mapeo de recursos reales) y los requisitos no funcionales. Claramente, la calidad del modelo MO tiene un impacto muy real en el diseñador/implementador (designer/implementor).

Es importante que el especificador del modelo MO reconozca las debilidades inherentes de usar GDMO y ASN.1 sin otras herramientas de especificación. Una sola especificación GDMO/ASN.1 proporciona, una manera razonable precisa e inequívoca, un conjunto de mensajes CMIP y estructuras de datos asociadas que pueden pasarse por una interfaz, en

una clase base por MO. Es sumamente dificil tratar a un diseño de interfaz como un conjunto cooperativo de clases MO dentro del contexto de GDMO.
Si la calidad de los modelos MO es mejorada, entonces deben usarse herramientas de la especificación adicionales. Naturalmente, el uso de las herramientas de Análisis y Diseño de OO existentes probablemente nos proporcionarán los beneficios deseados. También debe dársele consideración a proporcionar la métrica de calidad.

a) Arquitectura

La arquitectura de sistemas OSI incluye los siguientes elementos clave:

- Áreas Funcionales de Gestión
- Entorno de mediación
- Funciones de Gestión del Sistema
- Agente CMIP
- MIB de Agente
- CMIS/CMIP

La Gestión de las Áreas Funcionales corresponden al componente gestor en el modelo de referencia. Las Funciones de Gestión de Sistemas corresponden al componente de servicios en el modelo de referencia. El Entorno de Mediación Operacional y CMIS/CMIP juntos corresponden al componente del Entorno de Mediación en el modelo de referencia, y el Agente CMIP y el MIB de Agente corresponden juntos al componente de objeto gestionado en el modelo de referencia.

b) Áreas Funcionales

Los primeros trabajos de la Infraestructura de Gestión están contenidos en las secciones de las funciones de gestión. Éstas funciones de gestión evolucionaron gradualmente a lo que se conoce actualmente como las cinco áreas funcionales de OSI. Para denotar estas áreas, se usa normalmente el término `FCAPS ' (este término es una reducción de las cinco letras iniciales de las áreas funcionales).

1) Gestión de Fallas

La gestión de fallas es el conjunto de medios que permiten la detección, aislamiento y corrección de operaciones en modo de falla. Las posibles causas para que el funcionamiento sea anormal son: los errores dados en el diseño y la implementación, errores de sobrecarga, perturbaciones externas, y la expiración de acuerdo a su ciclo de vida de un componente. La gestión de fallas incluye funciones tales como:

- Mantenimiento y examinación de los registros de error.
- Aceptar y actuar ante las notificaciones de error.
- Rastrear e identificar las fallas.
- Llevar a cabo pruebas de diagnóstico.
- Corrección de fallas.

2) Gestión de Configuración

La gestión de configuración es el conjunto de medios que:

- Archivan o guardan la configuración actual del sistema.
- Registran los cambios en la configuración.
- Identifican los componentes de red (entrega las direcciones para los Puntos del Acceso al Servicio y los medios para conectarse a unas entidades de computadoras).
- Inicializan y cierran los sistemas de la red.
- Cambian los parámetros de la red (ejemplo: tablas de enrutamiento).

Un aspecto importante de gestión de configuración, es la asignación de nombres. Para enfatizar esta importancia algunas veces es usado, el término configuración y gestión de nombres.

3) Gestión de Contabilidad

La gestión de contabilidad es el conjunto de facilidades que permiten establecer los cargos y los costos que son identificados por un gestor (de red y/o del sistema), los cuales le permiten medir el uso de los recursos de la red (y/o del sistema). Estos recursos pueden ser:

- Servicios de red, el proveedor es responsable por la transferencia de los datos del usuario (ejemplo: la red pública).

- Aplicaciones de red (ejemplo: servicios de directorio).

La gestión de contabilidad permite:

- Informar a los usuarios de los costos, así estén lejos.
- Informar a los usuarios de los costos esperados en el futuro.
- Fijar el límite en los costos (ejemplo: desactivar el 0X en las conexiones de un teléfono).
- Combinar los Costos (prevenirle al usuario el recibir facturas separadas por cada conexión o servicio individual o en caso de haber realizado conexiones internacionales cada vez cruce o visite un determinado país).

4) Gestión del Rendimiento

La Gestión del Rendimiento es necesario para optimizar/perfeccionar la Calidad de Servicio (QoS). Para detectar y/o descubrir cambios de Rendimiento de la red, los datos estadísticos (ejemplo: lo valores de los temporizadores y de ciertos contadores) debe coleccionarse y/o almacenarse y además deben ser registrados periódicamente o cada vez que se produce algún evento. El uso de tales registros (logs) no está restringido para la Gestión del Rendimiento; también existen otras áreas de gestión que aprovechan estos registros (logs):

- Los registros del Rendimiento pueden ser usados por la Gestión de Fallas para la detección y/o descubrimiento de estas mismas.
- Los registros del Rendimiento pueden ser usados por la Gestión de Configuración para decidir cuando se necesitan cambios en la configuración.
- Los registros del Rendimiento pueden ser usados por la Gestión de Contabilidad para facturar.

Para Permitir que se haga una comparación significativa de los registros del Rendimiento, debe conocerse que existe y que ha existido la configuración y que los respectivos registros fueron hechos en el momento indicado. La información de la configuración debe también ser registrada.

5) Gestión de Seguridad

La Gestión de Seguridad es el conjunto de medios que le permiten al gestor inicializar y modificar aquellas funciones que aseguran la red de accesos

desautorizados y de comportamientos anómalos del usuario. Las partes importantes de la Gestión de Seguridad son la gestión de las claves (para la autorización, encriptación y autenticación), mantenimiento de firewalls (cortafuegos) y la creación de registros de seguridad (security logs).

6) Entorno de Mediación Operacional

Las cinco áreas funcionales mencionadas hacen uso de los servicios provistos por las funciones de gestión del sistema. Algún Entorno de Mediación, fuera del alcance de la arquitectura de gestión OSI, facilita la interacción entre las áreas funcionales y las funciones de gestión. Por ejemplo, las funciones de gestión del sistema podrían ser invocadas utilizando llamadas a procedimientos remotos.

7) Funciones de Gestión de Sistemas

Las funciones de Gestión de Sistemas (SMFs) son herramientas que soportan una o más de las cinco áreas funcionales de gestión. Cada área funcional puede ser implementadas como una aplicación que confia en algún subconjunto de funciones de Gestión del Sistema.

Algunas SMFs especificadas son:

- La Gestión de Objeto, soporta la creación y eliminación de objetos gestionados y la lectura y modificación de atributos del objeto. También especifica notificaciones ha ser emitidas cuando el valor de un atributo cambia.
- La Gestión de Estado, especifica servicios que permiten monitorear el estado pasado de objetos gestionados y reciben avisos, o alarmas, en respuesta a los cambios de estado de los objetos gestionados.
- La Gestión de la Relación, especifica a un modelo para representar y gestionar relaciones entre los objetos gestionados. En general, una relación es un conjunto de reglas que describen cómo el funcionamiento de un objeto gestionado afecta los la operación de otro objeto gestionado dentro de un sistema abierto.
- Reporte de Alarmas, que soporta la definición de alarmas de fallas y las notificaciones utilizadas para informarlas.

- La Gestión de Reporte de Eventos, soporta el control de informes de eventos, incluyendo las especificaciones de destinatarios de informes, la definición de informes, y la especificación de criterios por generar y distribuir informes.
- El Control de Registro soporta la creación de registros, la creación y almacenamiento de grabaciones de registros, y la especificación de criterio para logging.
- Reporte de Alarmas de Seguridad, que soporta la definición de alarmas de seguridad y las notificaciones usadas para informarlas.
- El Seguimiento de Revisión de Alarmas, especifica los tipos de informes de evento que deben estar contenidos en un registro usado para la evaluación de seguridad.
- El Control de Acceso, soporta el control de acceso a la operaciones e información de gestión.
- El Registro de Tarificación, provee información de la utilización de los recursos del sistema.
- Monitoreo de Carga de Trabajo, soporta la supervisión de los atributos de los objetos gestionados que se relacionan con el rendimiento de un recurso.
- La Gestión de Pruebas, soporta la gestión de confiabilidad y procedimientos de diagnóstico.
- Totalización, soporta la definición de medidas estadísticas para ser aplicadas a los atributos y el reporte de información resumida.

Estas funciones, a su vez, confian en el servicio de información de gestión común (CMIS) para el intercambio básico de información de la gestión.

8) Agente de CMIP

El agente CMIP mantiene información (en la forma de instancias de objeto gestionado) acerca del estado de una parte particular de la red de la cual él es responsable. El Agente CMIP responde a las peticiones de información y hace peticiones de acción desde la estación de gestión, y puede proporcionar información no solicitada a la estación de gestión asincrónicamente. El protocolo

usado para comunicarse con el agente es el Protocolo de Información de Gestión Común (CMIP).

9) MIB de Agente

El MIB de Agente (base de información de gestión) contiene los objetos gestionados que el agente hace disponibles al gestor. El tipo y estructura de la información de la gestión son determinadas por el OSI SMI (Estructura de Información de Gestión). La especificación del OSI SMI y MIB se apoya fuertemente en los conceptos de diseño orientado a objetos. La unidad básica de información en un MIB es el objeto. Un objeto puede incluir:

- **Atributos:** variables que representan características de recursos gestionados.
- **Comportamientos:** acciones que pueden ser activadas por un gestor.
- **Notificaciones:** informes de evento que pueden ser activados por eventos definidos.

Debe tenerse presente que las característica técnicas no dictaminan que tal MIBs sea implementada usando sistemas de gestión de bases de datos orientados a objetos o tecnología orientada a objetos. El único requisito es que la especificación de información comunicada entre sistemas abiertos en protocolos de Gestión de Sistemas (ej. CMIP) use principios de diseño orientados a objetos.

c) Intercambio de Información de Gestión

Se han identificado tres diferentes maneras para intercambiar información de gestión en el Modelo de Referencia OSI:

- La gestión de sistemas.
- La gestión de aplicaciones.
- La gestión de capa.

Aunque uno esperaría que el SC 21/WG 4 usaría estos tres acercamientos para empezar como punto de partida en el desarrollo de la Gestión de OSI. En la Infraestructura de Gestión, esto no sucedió, y en cambio, el SC 21/WG 4 decidió quitar gestión de aplicaciones e incluir la operación de capas.

1) Gestión de los Sistemas

La definición inicial de la gestión de sistemas, tal como se encuentra en el Modelo de Referencia OSI, se distingue entre dos propiedades diferentes:

- La Gestión de Sistemas está relacionada con la gestión de recursos de OSI y su estado a través de todas las capas de la arquitectura de OSI.
- Los protocolos para la Gestión de Sistemas residen en la capa de aplicación.

La primera propiedad explica que es lo que está siendo gestionado, lo segundo explica y dice cómo la información de gestión debe intercambiarse.

Es interesante ver que la Infraestructura de Gestión OSI se enfoca en el aspecto del intercambio de información de gestión de la gestión de sistemas (e ignora el aspecto para el cual se está gestionando). La gestión de sistemas puede ser caracterizada por el hecho de que los protocolos de aplicación deben usarse para el intercambio de información de gestión. Los protocolos de aplicación se construyen con base en los servicios asociados que deben ser fiables y orientados a conexión (el término `Royal Route` (Ruta Real) tiene que ser usado algunas veces para caracterizar esta manera de intercambio de información de gestión).

La decisión para usar los protocolos de la capa de aplicación está basada en asumir que se debe intercambiar información de gestión de la misma manera como con todas las otras formas de información. Según este punto de vista, la gestión debe considerarse como simplemente otra aplicación en alguna parte de la red (más precisamente en su capa de aplicación).

Para modelar el intercambio de información de gestión, se introduce el concepto de Entidades de Aplicación de Gestión de Sistemas (SMAE´s). Estas (las SMAE`s) residen en la capa de aplicación y realizan (y/o se encargan) los aspectos de comunicación de las funciones de gestión de sistemas (Figura 2.2).

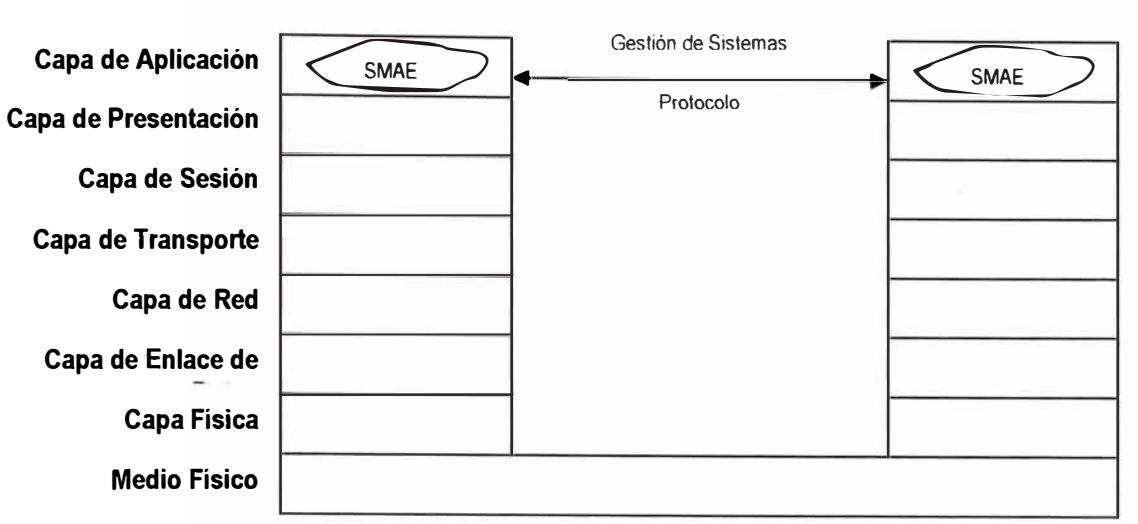


Figura 2.2 La Gestión de los sistemas debe verse como una aplicación de protocolos.

Los defensores de los intercambios de gestión en el nivel de aplicación usan los siguientes los argumentos:

- Los protocolos de la capa de aplicación son en su mayoría un tipo de protocolos potentes (`Powerful`). Un solo protocolo de la capa de aplicación debe ser capaz de transferir muchos tipos de información de gestión. Cuando se esté definiendo un protocolo de gestión poderoso será mucho mejor tener en cuenta que se deben definir muchos protocolos de gestión relacionados entre si.
- Los Servicios que son proporcionados por las capas más bajas normalmente no son bastante buenos para satisfacer todas las necesidades de gestión. Por ejemplo, para intercambiar grandes tablas de enrutamiento, pueden ser requeridas las capacidades completas de todas las capas de OSI (ejemplo: detección de errores, corrección del error, segmentación, re-ensamblaje, y la negociación del contexto etc.).
- La gestión se ve como una aplicación en la "parte alta" (desde el punto de vista protocolar) de una red. Si ISO no modelara a una aplicación dentro de la capa de aplicación, minaría su propia aproximación.

Los antagonistas de los intercambios de gestión en el nivel de aplicación usan siguientes argumentos:

- La implementación de todas las siete capas del Modelo de Referencia es costosa. Hay muchos sistemas que para su normal funcionamiento, no necesita implementar todas las siete capas (ejemplo: puentes (bridges) y enrutadores (ruteadores)). En estos sistemas puede darse una pérdida de dinero al implementar las capas restantes, sólo para permitir gestión.
- Después de un colapso en la red, una parte importante de la gestión tiene la responsabilidad de restaurar los servicios de y en la red. Como resultado de una falla o un colapso, los protocolos de la capa de aplicación ya no pueden funcionar bien. En caso de que el intercambio de información de la gestión cuenta con el funcionamiento correcto de estos protocolos, las funciones de la gestión ya no pueden ser logradas.
- Los protocolos de capa de aplicación involucran una cantidad de procesamiento y son relativamente lentos.
- Los protocolos de capa de aplicación no tienen facilidades de multicast o de broadcast.

2) La Gestión de Capa.

Mientras la gestión de los sistemas ha sido definida como la forma preferida para intercambiar información de gestión, de todas maneras no es la única forma. La Infraestructura de Gestión OSI alternativas, por ejemplo la gestión de capa que tiene las siguientes propiedades:

- La Capa-(N) de Gestión soporta el monitoreo, control y coordinación de los objetos gestionados de la capa-(N).
- Los Protocolos de Gestión de la Capa-(N) son soportados por los protocolos de capas-(N-1) y los de abajo.

El primer ítem relaciona la gestión de capa con lo que está gestionándose, el segundo nos dice cómo debe intercambiarse la información de gestión de la capa-(N). La Figura 2.3 muestra el ejemplo de la información de gestión de la capa de Red de OSI, la cual se intercambia por medio de un protocolo con propósito

especial en la gestión de capa localizado encima de los protocolos de comunicación normales.

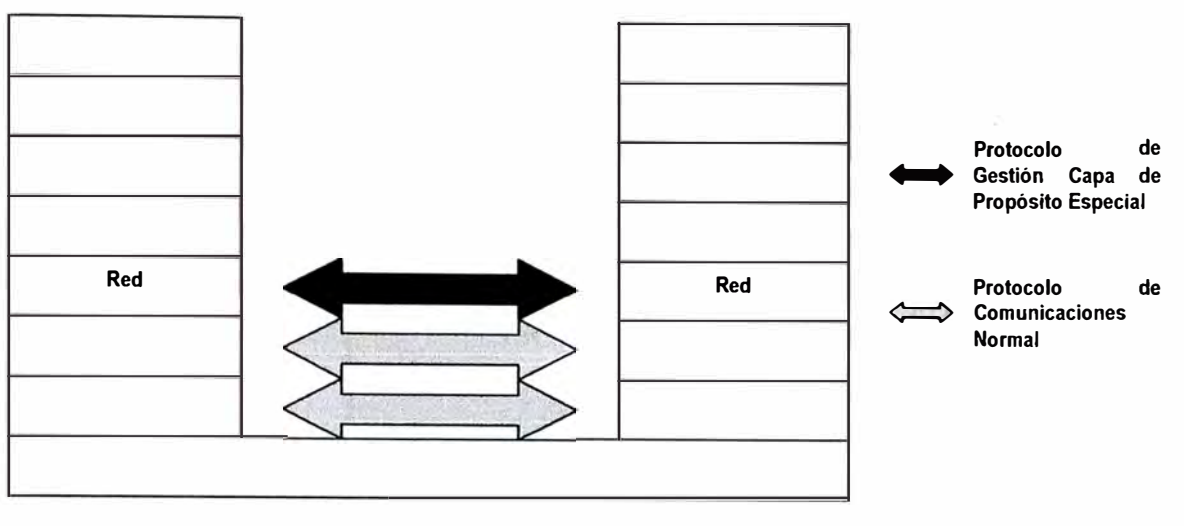


Figura 2.3 La Gestión de Capa en contra de los protocolos de comunicación normales.

Una importante diferencia entre la gestión de sistemas y la gestión de capa, es que la gestión de sistemas usa el servicio de la presentación para el intercambio de información de gestión, considerando que la gestión de la capa-(N) usa el servicio-(N-1). De acuerdo con la Infraestructura de Gestión, "el uso de la gestión de capa está restringida a los casos donde el uso de la gestión de sistemas es inapropiada".

Por ejemplo: la gestión de Capa normalmente se usa normalmente para el intercambio de información de enrutamiento. En varios casos, la información de enrutamiento deben transmitirse sobre un dominio de enrutamiento entero. Puesto que el servicio de presentación no tiene capacidades de broadcast, puede ser ineficaz el usar la gestión de sistemas. Varias estrategias de enrutamiento existentes cuentan por consiguiente, con protocolos de gestión de capa.

Se proporcionan otros ejemplos de gestión de capa en Figura 2.4 . Los estándares que son mencionados en esta Figura, son implementados en muchas redes que soportan el Protocolo de Red Sin Conexión de OSI (CLNP) . La figura es incluida

para demostrar que contrariamente a lo que a veces se sugiere, en las redes, con la gestión de capa los intercambios ocurren frecuentemente.

Tipo de PDU	Definido por	Cuando es Generado
Bridge PDU's	ISO 10038	Generado por todos los bridges después que expire el Hello timer (valor por defecto: 2 segundos)
Configuration PDU's	ISO 9542	Generado por todas las entidades de red después que expire el Configuration timer (mínimo valor: varios segundos; máximo valor: varios minutos)
Hello PDU's	ISO 10589	Generado por todos los ruteadores después que expire el Hello timer (valor por defecto: 10 segundos)

Figura 2.4 Ejemplos de Intercambios en la Gestión de Capa

3) Operación de la capa

El último tipo de intercambio de información de gestión es la Operación de capa. Esta forma primero fue definida por la Infraestructura de Gestión y no se ha mencionado en el Modelo de Referencia OSI. La Operación de Capa se define como "El Monitoreo y Control de una simple instancia de comunicación". En el caso de la Operación de capa, la información de gestión se toma como una parte de un protocolo de capa normal. Así como con la gestión de la capa-(N), la operación de la capa-(N) usa los protocolos (N-1) asociados para el intercambio de información de gestión (Figura 2.5).

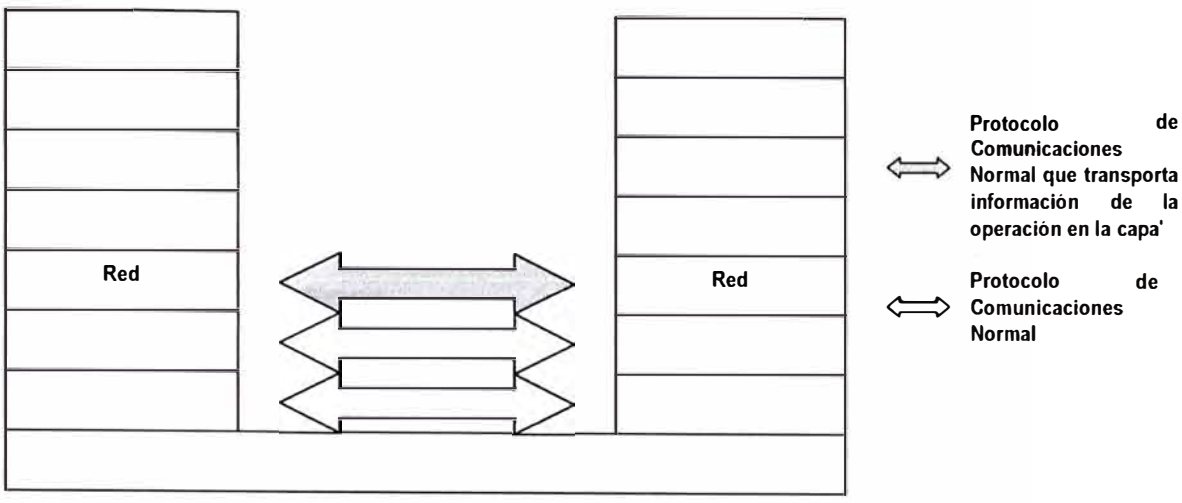


Figura 2.5 La Operación de Capa ante los protocolos de comunicación normales.

d) Objetos Gestionados, Información de Gestión y la MIB.

Para entender la relación entre los objetos gestionados, la información de gestión y la `Base de Información de Gestión' (MIB), puede ser útil echarle una mirada al desarrollo del Estándar de la Infraestructura de Gestión. Algunas versiones de este Estándar contienen las siguientes definiciones:

- **Objeto Gestionado:** "Son aquellos datos que representan datos de procesamiento y datos de recursos de comunicaciones (así sean recursos OSI o no) que pueden ser gestionados a través del uso de un protocolo de gestión OSI".
- **Información de Gestión:** "Es la Información asociada con un objeto gestionado que es operado por medio de un protocolo de Gestión OSI, para controlar y supervisar dicho objeto".

Estas definiciones sugieren que hay una diferencia entre los objetos gestionados y la información de gestión. Aunque los proyectos realizados acerca de la Infraestructura de Gestión a veces son difíciles de entender, también salta a la vista lo siguiente:

- Los objetos gestionados residen en varias capas del OSI RM (OSI Reference Model).
- La información de la gestión reside en la Base de Información de Gestión (MIB).

La MIB puede verse como un tipo de base de datos. Los contenidos de esta base de datos no son un conjunto de objetos gestionados, pero es la información que está asociada con los objetos gestionados. Los Gestores de capa (LM's) son responsables

mantener la asociación entre la información de la MIB y los objetos gestionados (Figura 2.6). En caso de presentarse problemas con Gestores de Capa, podría ocurrir que la información en la MIB no refleje más y con la precisión del caso, el estado de los objetos gestionados.

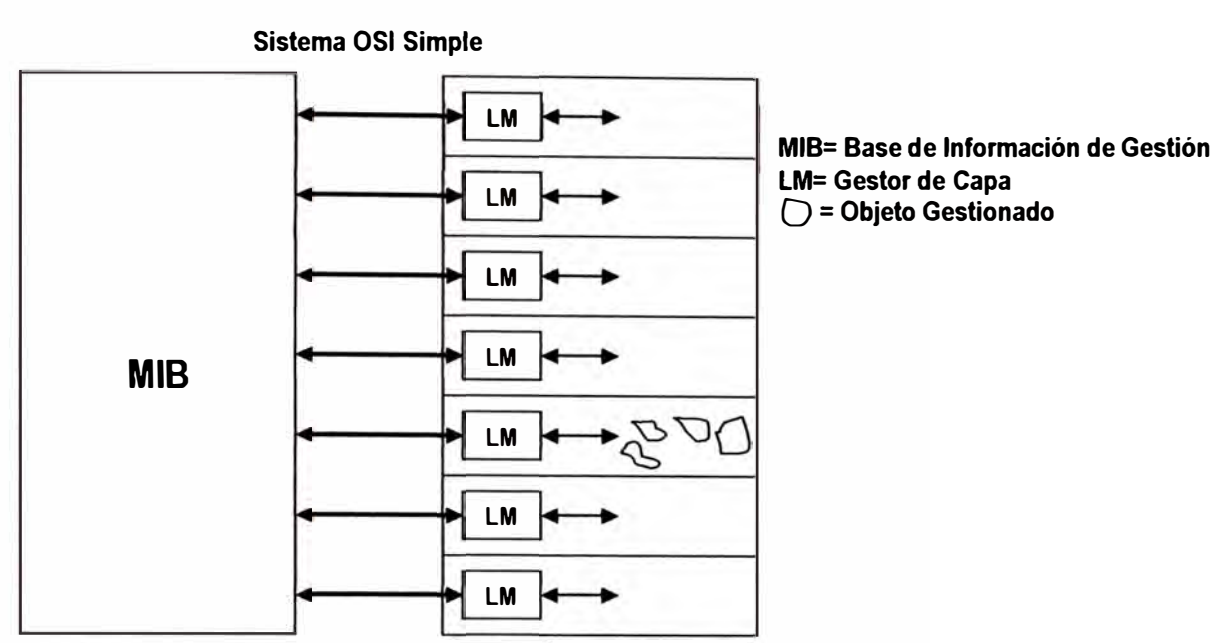


Figura 2.6 Abstracción de la MIB, los Objetos Gestionados y los Gestores de Capa

Como resultado de ciertos análisis, no existe una gran diferencia entre la información de gestión que puede guardarse dentro de una MIB, y los propios objetos gestionados. Según la versión final de la Infraestructura de Gestión "el conjunto de objetos gestionados dentro de un sistema, constituye la MIB de ese sistema". Puesto que esta definición hace implicar conceptualmente que una MIB no es más que la colección de todos los objetos gestionados dentro de un determinado sistema, por ello, el concepto de MIB no parece tener otra utilidad .

e) Apreciación global de los Sistemas de Gestión OSI

La definición de los Sistemas de Gestión OSI, está consignada en un trabajo hecho a manera de una apreciación global y se encuentra como Systems Management Overview (SMO), realizado alrededor de 1987 y finalizado en Junio de 1991.

El SMO incluye una descripción extensa de la gestión de sistemas. Esta descripción incluye los siguientes aspectos:

- Información.
- Organizacional.
- Funcional
- De Comunicación.

A continuación se discuten cada uno de estos aspectos; cada uno de estos incluyen referencias a los estándares de ISO/ITU-T y partes de estos estándares derivados son explicados también. La Figura 2.7 muestra como se relacionan los aspectos que se han mencionado.

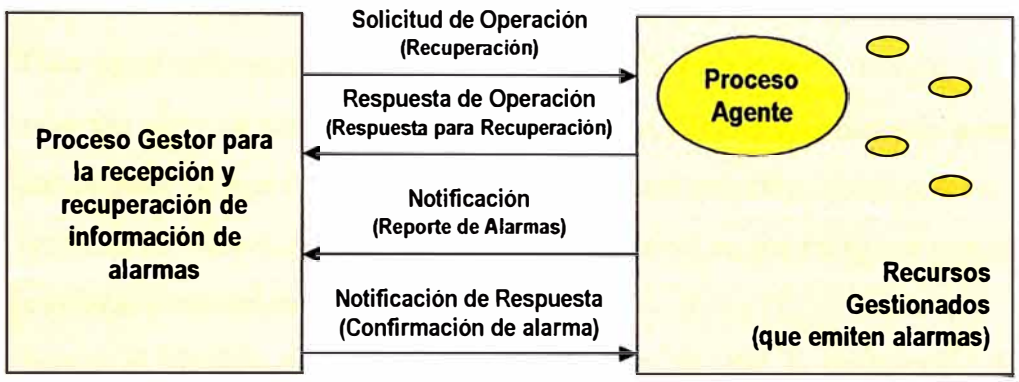


Figura 2.7 Visión Global de la Gestión de Sistemas OSI

1) Aspecto de Información

Los aspectos de información del modelo de gestión de sistemas se indican con los recursos que están gestionándose. Estos recursos se abstraen como ´ objetos gestionados ´.

El concepto de objetos gestionados se introdujo como parte de la Infraestructura de Gestión de OSI. Inicialmente se consideraba que esta introducción era suficiente; el concepto de objetos gestionados no fue elaborado aún más porque se pensó que era algo obvio y que violaba en algo el principio de OSI, que había sido establecido a partir sólo del comportamiento externo de los sistemas que podían estandarizarse. Posteriormente, se dio en el ámbito de las telecomunicaciones que algunas personas interpretaron el concepto del objeto gestionado de diferentes maneras: lo asumido inicialmente del concepto era obvio, pero resultó estar

equivocado en algunos aspectos. Después de ciertas deliberaciones, este problema fue abordado y se decidió refinar la descripción de objetos gestionados como sigue:

"Un objeto gestionado es, desde el punto de vista de la Gestión OSI, un recurso que está sujeto a la gestión, tal como una entidad de capa, una conexión o un ítem de equipo fisico de comunicaciones. Así, un objeto gestionado es la abstracción de tal recurso como lo que representa sus propiedades y que es vista por (y con el propósito de) la gestión. Una parte esencial de la definición de un objeto gestionado es la relación entre estas propiedades y el comportamiento operacional del recurso. Esta relación no está modelada de una forma general".

Una parte interesante de esta descripción es la última frase, la cual establece que la relación entre el comportamiento operacional y las propiedades de gestión no están modeladas de una forma general. Sin semejante relación, no es posible sin embargo expresar el efecto de las operaciones de gestión en los recursos gestionados. Esto es claramente indeseable.

Según el Modelo de Información de Gestión de OSI, la abstracción de gestión de un objeto gestionado es visible en el límite del objeto gestionado. En este límite, la abstracción de gestión se describe en términos de (ver Figura 2.5):

- **Atributos**, que son las propiedades o características del objeto.
- **Operaciones**, las cuales se realizan en el objeto.
- **Comportamiento**, el cual se exhibe en respuesta a las operaciones.
- **Notificaciones**, que son emitidas por el objeto.

Próximos a los objetos gestionados que representan recursos, hay o existen también ´Objetos de Soporte de Gestión`. Tales objetos pueden ser introducidos por el diseñador de funciones de gestión durante la fase de implementación. Un ejemplo de un objeto de soporte de gestión es un `registro de Log´ que puede usarse para guardar la información de gestión.

Figura 2.8 Un Objeto Gestionado

El concepto de objeto gestionado es refinado en varios estándares adicionales, los cuales se denominan estándares de la Estructura de Información de Gestión (SMI) (las primeras seis entradas de Figura 2.9). Los estándares de SMI no especifican los Objetos Gestionados reales; los objetos gestionados son definidos por los grupos de trabajo responsables del funcionamiento de varias capas del Modelo de Referencia OSI (se dan ejemplos de tales normas en las últimas cuatro entradas de Figura 2.9).

Título	ISO/IEC	ITU-T
Modelo de Información de Gestión	10165 –1	X.720
Definición de Información de Gestión	10165-2	X.721
Guías para la definición de Objetos Gestionados	10165-4	X.722
Información de Gestión Genérica	10165-5	X.723
Guías para Proformas de Conformidad	10165-6	X.724
Modelo de Relación General	10165-7	X.725
Información de Gestión relacionada con la capa de transporte	10737	X.284
Información de Gestión relacionada con la capa de red	10733	X.283
Información de Gestión relacionada con la capa de enlace de datos	10742	X.282
Información de Gestión relacionada con la capa fisica	13642	X.281

Figura 2.9 Estándares para Objetos Gestionados

2) Aspecto Organizacional

La Gestión de Sistemas OSI es organizada en una forma centralizada. De acuerdo a este esquema, un solo Gestor puede controlar a varios agentes. El Gestor realiza operaciones en (los objetos gestionados incluidos) los agentes, los agentes re-envían las notificaciones a sus Gestores. La Figura 2.10 ilustra este concepto del Gestor - Agente. El entorno de gestión OSI puede dividirse en varios dominios de gestión. El particionamiento puede estar basado en requisitos funcionales (ejemplo: seguridad, contabilidad y gestión de fallas), pero también en otros requisitos (ejemplo: geográficos y tecnológicos). La idea de los dominios de gestión aún está bajo desarrollo por la ISO.

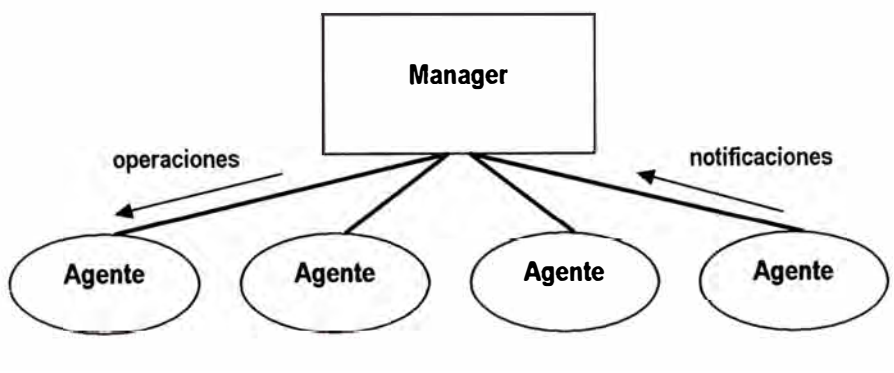


Figura 2.11 El concepto de Gestor - Agente

3) Aspecto Funcional

Poco después de que los primeros proyectos sobre la Infraestructura de Gestión aparecieron, ISO empezó a definir estándares de protocolos para cada una de las cinco áreas funcionales. (Figura 2.12).

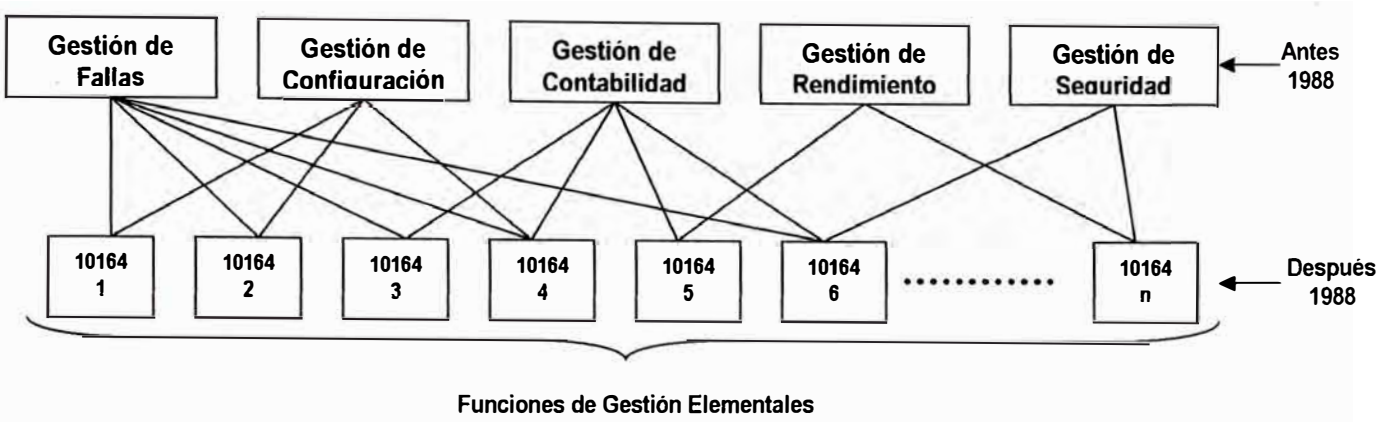


Figura 2.12 Las áreas Funcionales y las funciones de gestión elementales

4) Aspecto de Comunicación

OSI ha definido el `Servicio de Información de Gestión Común' (CMIS), como el servicio preferido para el intercambio de información de gestión (aunque el uso de otros servicios de intercambio todavía se permite, como servicios proporcionados por TP y FTAM). El rol de CMIS está restringido al traslado de información de gestión; el control actual de los sistemas se le deja a los usuarios-MIS que se localiza encima de CMIS (Figura 2.12).

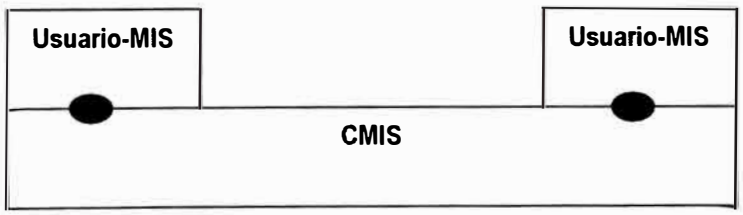


Figura 2.12 Usuarios-MIS encima de CMIS

El Proveedor del Servicio CMIS puede ser descompuesto, en el que caso en que dos o más Entidades de Aplicación de Sistemas de Gestión (SMAE's) aparezcan. Estas entidades contienen varios Elementos de Servicio de Aplicación (ASE's) y usa el proveedor de servicio de presentación para transferir sus datos (Figura 2.13). La interacción entre SMAE's es definida por el 'Protocolo de Información de Gestión Común' (CMIP]).

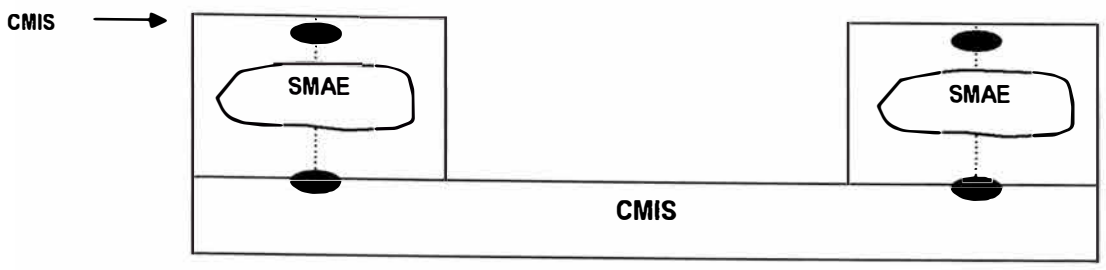


Figura 2.13 La Descomposición de CMIS

El estándar CMIS define las siguientes primitivas del servicio:

- **M-GET:** Se usa para recuperar información de gestión. Puede por ejemplo ser usado por un gestor para recuperar direcciones de agentes de red.
- **M-CANCEL-GET:** Se usa para cancelar un M-GET previamente invocado. Es útil en esos casos donde el M-GET entrega demasiada información o consume demasiados recursos. Esto puede pasar si por ejemplo, un gestor le pide a un agente que presente su tabla completa de enrutamiento.
- **M-SET:** Es para modificar los atributos de un objeto gestionado. Puede ser usado por ejemplo por un gestor para cambiar la dirección de red de un agente.
- **M-ACTION:** Para realizar alguna acción en un objeto gestionado. Puede por ejemplo ser usado por un manager para reinicializar algún sistema de red.
- **M-CREATE:** Para crear una nueva instancia de un objeto gestionado. Puede por ejemplo usarse para agregar una entrada a una tabla de enrutamiento.
- **M-DELETE:** Se usa para borrar una instanciación de objeto gestionado. Esta es la función antagónica o inversa de M-CREATE y puede por ejemplo ser usada para remover una entrada de una tabla de enrutamiento.
- **M-EVENT-REPORT:** Se usa para informar o reportar la ocurrencia de algún tipo de evento. Esto por ejemplo puede ser invocado por un agente para informar al gestor que uno de los enlaces de salida del agente no puede usarse más.

Las primeras seis primitivas definen operaciones, la primitiva M-EVENT-REPORT define una notificación (ver Figura 2.8). Mientras todas las primitivas pueden usarse de una forma confirmada, algunos (como M-SET, M-ACTION y M-EVENT-REPORT), son también usadas de una forma no confirmada.

La Figura 2.14 lista los estándares ISO/ITU-T que definen cómo la información de gestión de sistemas debe intercambiarse; la lista no incluye las enmendaduras y adiciones a estos estándares.

Título	ISO/IEC	ITU-T
Servicio de Información de Gestión Común **(CMIS)**	9595	X.710
Protocolo de Información de Gestión Común **(CMIP)**	9596	X.711

Figura 2.14 Estándares para los Aspectos de Comunicación

5) Protocolo de Gestión

Estructura De Aplicación de Gestión de Sistemas (SMAS).

La capa de aplicación del Modelo de Referencia OSI puede ser aun mas estructurada, a partir de los requerimientos de la aplicación. Los estándares OSI se han definido de una forma modular, para que así el máximo re-uso pueda ser posible a través de las diferentes aplicaciones. La unidad re-usable se denomina Elemento de Servicio de Aplicación (ASE).

Varios de los ASE's son combinados de acuerdo a las necesidades de la aplicación. Para las Aplicaciones de Gestión de Redes la estructura se muestra en la Figura 2.15 .

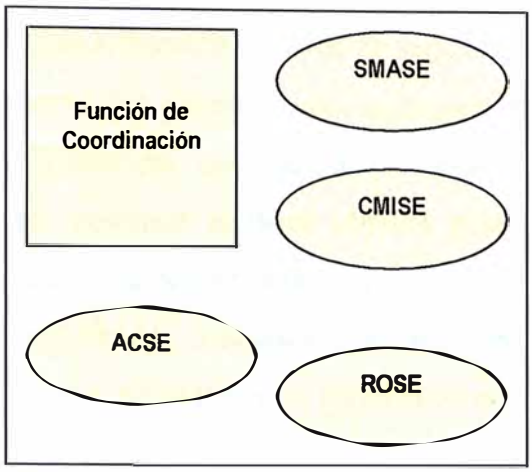


Figura 2.15 Estructura de Aplicación de Gestión de Sistemas: El ACSE (Elemento del Servicio de Control de Asociación); CMISE (Elemento del Servicio de Información de Gestión Común; ROSE (Elemento del Servicio para Operaciones Remotas); SMASE (Elemento del Servicio de Aplicación de Gestión de Sistemas)

Los bloques de construcción requeridos son: ACSE para fijar un tipo de asociación entre las entidades de aplicación pares; y la combinación de ROSE, CMISE y SMASE, que incluyen los modelos de información para la transferencia de los datos de información de gestión. Las funciones de coordinación representan la lógica requerida para que estas ASE's puedan trabajar en conjunto y de manera cooperativa.

f) Análisis

A continuación se discute algunos de los problemas principales de la Gestión OSI. No está hecha de forma exhaustiva.

1) Integridad Arquitectural

Un problema importante de la arquitectura de gestión OSI, es que no se aplican los principios de modelamiento del Modelo de Referencia OSI de una manera apropiada. La gestión de OSI viola, por ejemplo, el principio del layering (del particionamiento en capas), el cual dice que los usuarios de una capa en particular no necesitan conocer la estructura interna de su proveedor de servicio asociado. Según el principio de arquitectura basada en capas, las entidades pueden interactuar sólo con entidades en capas adyacentes por medio de las primitivas del

servicio; no es posible que las entidades accesen desordenadamente a los componentes en capas arbitrarias a través de algunos otros medios.

Por ejemplo, considere dos sistemas: uno en un gestor y otro en un papel de agente (Figura 2.16). El sistema que opera en el rol del agente es el que está gestionándose; este contiene algunos objetos gestionados para representar los recursos que pueden gestionarse. Los objetos gestionados pueden ser accedidos por un SMAE. Este SMAE comunica por medio de un protocolo de gestión de sistemas (CMIP) con un SMAE que se localiza en el sistema del gestor.

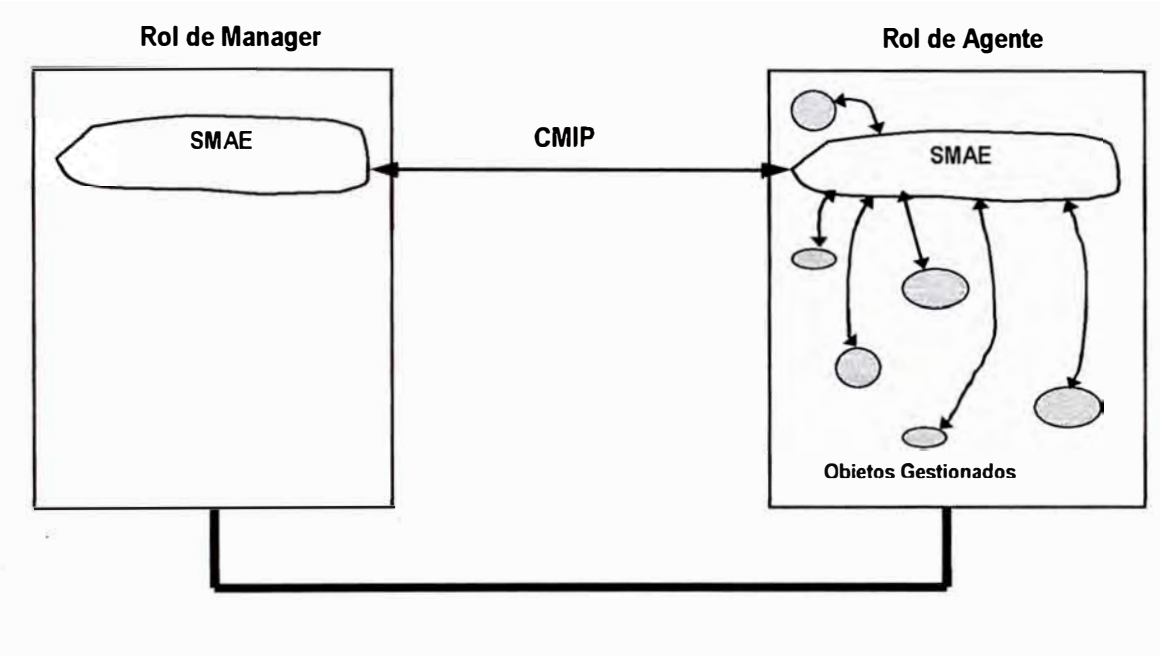


Figura: 2.16 Gestión de Sistemas OSI

Cada capa del Modelo de Referencia OSI puede necesitar gestión. Los objetos gestionados pueden encontrarse, de esta manera, en todas las capas del Modelo de Referencia OSI. El SMAE está, por definición, localizado en la capa de aplicación (Figura 2.17). Según la gestión OSI, el SMAE podrá sin embargo manipular objetos gestionados, independiente de la capa en la que estos objetos estén localizados. La implicación de esto es que el SMAE debe tener conocimiento sobre la estructura interna del proveedor de servicio asociado y debe poder acceder a los componentes dentro de este proveedor por medio de algún mecanismo de interacción 'Mágico'. Esto está en contra los principios del modelamiento, que han sido definidos por el Modelo de Referencia OSI.

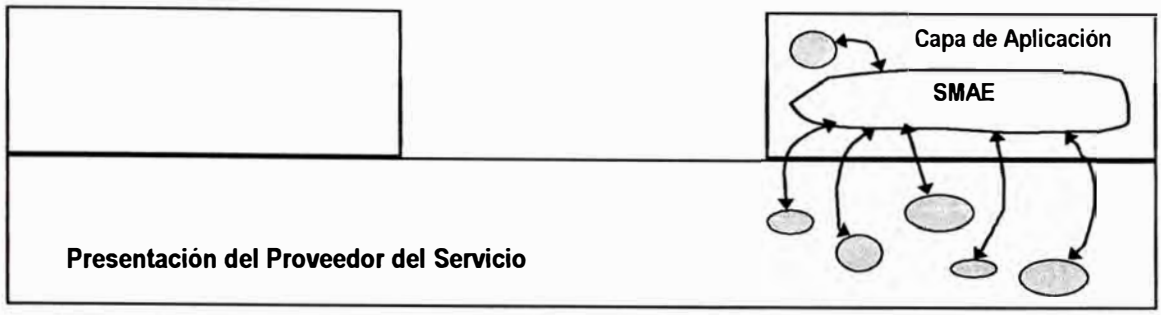


Figura 2.17 El SMAE conoce la estructura del proveedor asociado

2) Problemas con la Gestión de Fallas

Otro punto débil de la aproximación de la gestión de OSI, es que (implícitamente) los protocolos de capa que están gestionándose, también se usan para el intercambio de información de gestión. La Figura 2.18 se usa para ilustrar esta relación.

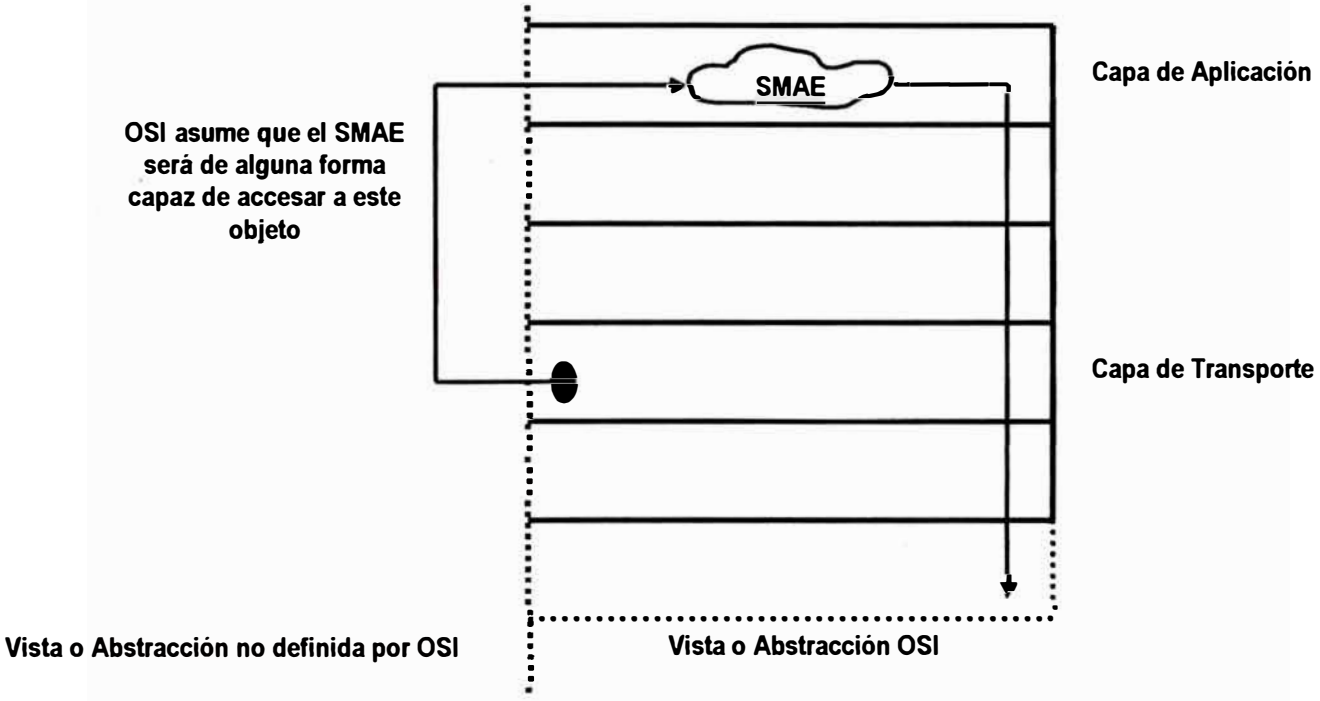


Figura 2.18 Ejemplo que muestra el doble papel de los protocolos de capa en la capa de aplicación y en la capa transporte

La figura muestra que un objeto gestionado de la capa de transporte, tal como un contador, refleja el número de errores CRC. Este contador CRC puede ser leído por el SMAE que reside dentro de la capa de aplicación. OSI no describe cómo el SMAE accede al objeto gestionado en la capa de transporte; la gestión OSI asume, sin embargo, que alguna forma de interacción puede ser posible. Después de que el SMAE ha leído al contador, se puede decidir enviar información CRC a otros sistemas. Para este propósito, el SMAE presenta la información como datos de usuario al proveedor de servicio de presentación asociado. El protocolo de la capa de transporte es parte de este proveedor, sin embargo, el protocolo de capa de transporte se usa así también para el intercambio de información de gestión.

Los protocolos que están gestionándose, también se usarán para intercambiar información de gestión. El problema con esta dependencia es que esa gestión de fallas puede tornarse imposible. Por ejemplo, considere un sistema en el que la entidad de transporte repentinamente se interrumpe. En caso de que todas las otras entidades dentro de ese sistema permanezcan operacionales, la falla puede ser detectada por el SMAE, el cual que puede decidir generar un reporte de alarma. Este (el reporte de alarma) no puede ser transmitido, debido a las fallas dentro de la entidad de transporte local.

3) Otros Problemas

Además de los dos problemas que se han mencionado, la gestión OSI se enfrenta con otros varios problemas:

- La gestión OSI explica cómo las operaciones de gestión individuales, tales como GET's y SET's, deben realizarse. Los estándares de gestión actuales no especifican la sucesión en la que estas operaciones deben realizarse para resolver problemas de gestión específicos. Hasta ahora, las soluciones para los problemas de la gestión reales apenas existen.
- La gestión OSI es bastante complicada. El SC 21/WG 4 ha introducido varios conceptos nuevos que a veces son dificiles comprender. Otras barreras son el número grande de estándares de gestión y el tamaño de estos estándares.

- Durante el proceso de estandarización se hicieron cambios considerables en algunos de los principales conceptos de gestión OSI. Los ejemplos de tales cambios son la re-definición de 'objetos gestionados', la remoción de la 'gestión de aplicación' y la introducción de la 'operación de capa'.
- La estandarización de la gestión OSI ha tomado demasiado tiempo. Existen otras aproximaciones, tales como SNMP, que surgen por consiguiente.
- Aunque la mayoría de fabricantes han declarado su apoyo por la gestión OSI, sólo se tienen unas aplicaciones en oferta.
- Los Sistemas de gestión que están basados en la arquitectura OSI son actualmente más caros que los sistemas de gestión que están basados en la Arquitectura de Gestión Internet (SNMP).

4) Aspectos Prácticos

La arquitectura de gestión de red OSI es una arquitectura muy poderosa comparado con la arquitectura de gestión Internet, pero también es muy compleja. Parea hacer factible la gestión OSI, es esencial emplear un número pequeño de funciones en un MIB manejable. Un acercamiento práctico es confiar en la gestión y empezar con un número modesto de objetos (un MIB pequeño) y una modesta cantidad de funcionalidad.

2.2.2 RED DE GESTIÓN DE TELECOMUNICACIONES TMN (UIT)

Con la introducción de nuevos elementos en los sistemas de Telecomunicaciones, nuevas tecnologías para prestar nuevos servicios de comunicaciones y mayor demanda de los mismos a aumentado la complejidad de los sistemas de Operaciones y Mantenimiento tradicionales. Ahora se tiene un concepto de gestión mucho más amplio que involucra otros componentes con miras a obtener la calidad del servicio deseada por los usuarios, en este proceso de evolución se ha definido las actividades de gestión al conjunto de OAM&P (Operación, Gestión, Mantenimiento y Suministro) que aseguran la cobertura total de las áreas de gestión definida por el estándar OSI de la ITU-T (Fallas, Configuración, Contabilidad, Desempeño y Seguridad). Con esta problemática actual muchos organismos

han creado sistemas de gestión propietarios, pero estos complican aún mas el problema, de esto surge la idea de la TMN (Telecomunication Management Network), que está en proceso de estandarización y define las reglas de juego en todos las áreas de gestión de telecomunicaciones. La TMN es el conjunto de capacidades que permiten el intercambio de información de gestión para que las empresas operadoras puedan realizar sus actividades de OAM&P, esta siendo estudio de estandarización con las siguientes organizaciones: OSI, ITU-T, ETSI, IEEE, ISO y el Network Management Forum, de donde se extrae la definición dada por la ITU-T en la recomendación M.3010: La TMN proporciona una estructura uniforme de gestión de redes de telecomunicaciones, a través de la introducción de modelos genéricos de gestión en diversos tipos de equipos, soportando modelos genéricos de información en interfaces estandarizadas.

Lo mencionado anteriormente toca de manera especial a la gestión de redes de telecomunicaciones y a los servicios que involucra. Gestión orientada al servicio, a la satisfacción del cliente, es más, servicios de gestión de servicios para involucrar aún más al cliente con la red es la tendencia del mercado. La Red de Gestión de Telecomunicaciones TMN ha tenido cierto impacto en el desarrollo de plataformas para la gestión de elementos de red y para gestión de la red en sí y ha servido como base para la especificación de arquitecturas *software* globales como TINA y la definición de servicios avanzados de gestión para Redes Inteligentes (CS2). Siendo TMN una tecnología diversificada, la cual tiene una estructura jerárquica por niveles para permitir una gestión integral de una red de telecomunicaciones, es lo suficientemente flexible para permitir abordar el problema de la gestión de servicios sin haber resuelto totalmente los problemas de gestión de elementos de red y de gestión de red.

Los principios de la red de gestión de telecomunicaciones TMN, apuntan a la operación, gestión, mantenimiento y provisión de las redes y servicios de telecomunicaciones en el ambiente abierto y multipropietario actual. Los elementos de las redes de telecomunicaciones (redes gestionadas) se comunican con los sistemas de gestión (en redes de gestión) a través de interfaces bien definidas y estandarizadas. Estas interfaces son más que protocolos porque incluyen modelos de información. Existe hoy un conjunto creciente de estándares TMN para las interfaces entre elementos de red y los sistemas de gestión. Sin embargo, muy pocos elementos instalados soportan esas interfaces.

a) Principios Básicos

El objetivo de la TMN es soportar las actividades de planificación, suministro, instalación, mantenimiento, operación y gestión de los elementos que conforman las redes, de las redes mismas y de los servicios de telecomunicaciones que ellas soportan, de una manera flexible, eficiente e integrada; para lo cual provee una estructura organizada de red que posibilita el interconectar e interoperar diferentes sistemas de apoyo a las actividades de OAM&P (Operation Accouting Management & Performance), entre sí y con equipos de telecomunicaciones para el intercambio de información de gestión, utilizando una arquitectura común, con interfaces estandarizadas (incluidos mensajes y protocolos). Además, la separación lógica de la TMN y las redes de telecomunicaciones posibilita una mayor flexibilidad en la implantación de arquitecturas de gestión centralizadas o descentralizadas, es así como una operadora podrá gestionar un amplio conjunto de equipos y/o sistemas distribuidos a partir de un número limitado de centros de gestión, sin que ello implique que la TMN no utilice recursos de la red de telecomunicaciones para realizar sus comunicaciones.

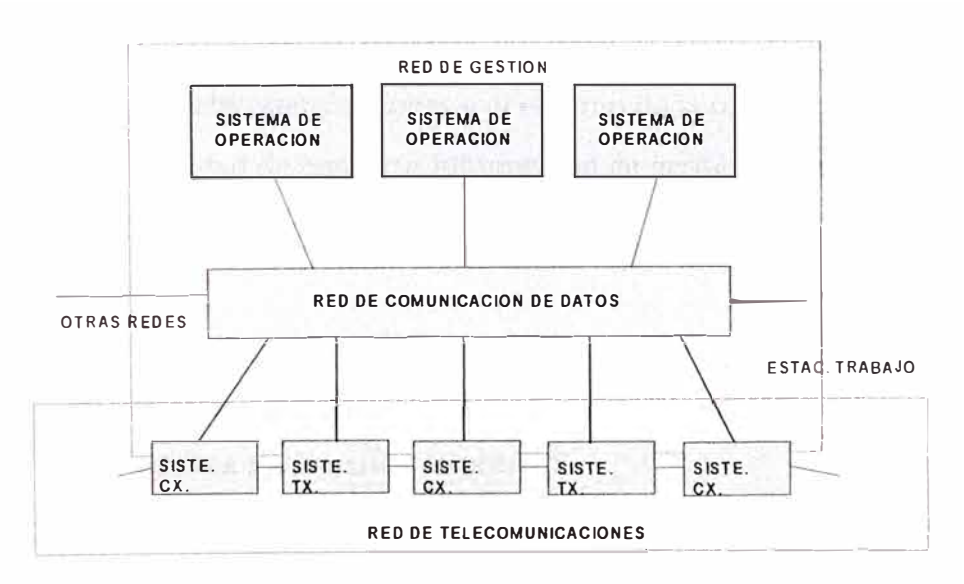


Figura 2.19 Relación Entre Una TMN Y Una Red De Telecomunicaciones.

Desde el punto de vista conceptual, la TMN es una red aparte que asegura la interfaz con una red de telecomunicaciones para el envío/recepción de información hacia o desde la segunda red y para el control de sus operaciones.

Dentro del contexto de TMN, la gestión hace referencia a un conjunto de capacidades orientadas a permitir el intercambio y procesamiento de información con el fin de apoyar a la gestión en el logro de una mayor eficiencia en el negocio. Como se conoce, una red de telecomunicaciones puede componerse tanto de equipos digitales como analógicos, tales como sistemas de transmisión, sistemas de conmutación, multiplexores, terminales de señalización, servidores de redes de datos, etc. y cuando estos componentes pasan a ser gestionados se les refiere como Elementos de Red (NE, Network Element).

La red de gestión de telecomunicaciones puede gestionar servicios y sistemas de telecomunicaciones, diferentes clases de equipos y diferentes redes entre las cuales se encuentran públicas y privadas, de banda estrecha y de banda ancha, móviles, redes telefónicas privadas, redes privada virtuales y redes inteligentes.

1) Funciones Asociadas a una TMN

Entre las funciones generales que debe soportar una TMN se cuentan:

- La capacidad de intercambiar información de gestión entre el entorno de la Red de Telecomunicaciones y el entorno de la red de gestión.
- La capacidad de convertir información de gestión de un formato a otro.
- La capacidad de transferir información entre localidades diferentes de la TMN.
- La capacidad de manipular información de gestión de tal manera que se presente de manera adecuada y de forma consistente al usuario, así como distribuirla a los usuarios respectivos.
- La capacidad de analizar y reaccionar debidamente ante la información de gestión obtenida.
- La capacidad de garantizar sólo a los usuarios autorizados el acceso a los diferentes tipos de información de gestión.

Es así como la TMN se ha orientado a soportar una gran diversidad de áreas de gestión que van desde la planeación y gestión hasta la operación y el

mantenimiento de las redes y los servicios que ellas soportan, pero corresponde a las empresas operadoras definir qué funciones de aplicación deberá soportar su red de gestión de acuerdo con sus proyecciones, sus prioridades, problemas y conveniencias; pero el CCITT ha definido una guía, clasificando la gestión en cinco grandes áreas funcionales (recomendación X.700) así:

- Gestión de rendimiento o de la calidad de funcionamiento (o rendimiento).
- Gestión de fallas.
- Gestión de la configuración.
- Gestión de la Tarificación
- Gestión de la seguridad

2) Gestión de Rendimiento

Evalúa y reporta sobre el comportamiento de los equipos de telecomunicaciones y la efectividad de la red o de elementos de red. Su función es recoger datos estadísticos para propósitos de monitoreo, corrección del comportamiento y para ayudar en la planeación y el análisis sobre la red, los elementos de red o sobre los equipos.

En términos generales, la gestión de la calidad de funcionamiento debe proporcionar los medios para efectuar tareas como las siguientes:

- Funciones de monitoreo de rendimiento, siguen la pista de las actividades del sistema, la red o el servicio para reunir los datos apropiados que determinen su calidad de funcionamiento, lo que permite detectar deterioros en los equipos y sistemas.
- Funciones de gestión de red y de tráfico, son las funciones relacionadas con la aplicación, modificación y eliminación de controles de tráfico automáticos y manuales, así como de gestión de red. La TMN recoge los datos de tráfico desde los elementos de red (Network Element, NEs), los analiza y decide reconfigurar o no la red de telecomunicaciones, o modificar su operación para ajustarla a un tráfico extraordinario.
- Funciones de observación de la Calidad del Servicio (Quality Of Service QOS). Estas funciones miden la eficacia con la que se presta un servicio, e

incluye tanto el monitoreo como el almacenamiento de parámetros relacionados con conexiones, la evaluación de registros históricos, etc.

3) Gestión de Fallas

Es un conjunto de funciones que permite detectar, aislar y corregir el funcionamiento anormal de la red de telecomunicaciones y de su entorno. La TMN proporciona la capacidad de monitorear fallas de los elementos de red casi en tiempo real. Cuando una falla ocurre el NE hace una indicación para que la TMN determine la naturaleza y severidad de la falla al establecer los efectos que ocasiona en los servicios que están siendo prestados por el equipo que presenta la avería.

En términos generales, la gestión de fallas debe proporcionar los medios para efectuar tareas específicas como: Localización de fallas y realización de pruebas.

4) Gestión de Configuración

Proporciona funciones para ejercer control sobre los elementos de red, así como recoger y enviar datos desde y hacia dichos elementos, comprende las siguientes funciones:

- Funciones de Aprovisionamiento, estas consisten en los procedimientos requeridos para que un equipo entre en servicio, sin incluir la instalación. Cuando la Unidad está lista para el servicio, los programas de soporte se inicializan a través de la TMN. El estado de la unidad, es decir si se encuentra en servicio, reserva, fuera de servicio, etc., y los parámetros seleccionados también pueden ser controlados por funciones de aprovisionamiento.
- Funciones de Control y Estado. TMN proporciona la capacidad de monitorear y controlar ciertos aspectos de algún elemento de red. Por ejemplo se puede cambiar o revisar el estado del servicio de un NE o de alguna de sus partes, así como realizar pruebas de diagnóstico. Cuando un equipo presenta fallas, la TMN puede excluirlo y reenrutar el tráfico reconfigurando la red si es necesario.

- Funciones de Instalación, TMN facilita la instalación de nuevos equipos dentro de la red de comunicaciones, o su remoción si es necesario. Se pueden instalar programas en los NE desde sistemas de base de datos de la TMN, además pueden intercambiarse datos administrativos entre los NEs y la TMN.

5) Gestión de Facturación

Esta proporciona un conjunto de funciones de soporte que permiten medir la utilización del servicio de red y determinar el costo de dicha utilización y además proporciona facilidades como: la recolección de registros de facturación y el establecimiento de parámetros de tarificación para el uso de los servicios.

6) Gestión de Seguridad

La definición de los aspectos de la gestión de seguridad todavía se encuentran en estudio, por lo tanto estos parámetros pueden diferir de una gestión a otra.

7) Requisitos de la Arquitectura TMN

Para la planificación y la construcción de la TMN, deben tenerse en cuenta cuatro aspectos fundamentales: Flexibilidad, Interoperabilidad entre Sistemas Distribuidos, Integración de las Actividades de OAM&P y Especificación clara y precisa de la Gestión de Redes.

Flexibilidad para hacer posible la gestión de redes heterogéneas de variada complejidad, adaptarse a los diferentes esquemas de organización y facilitar la evolución en servicios, tecnologías, políticas, mercados, etc.

Interoperabilidad para soportar un esquema multiproveedor y evitar la dependencia.

Integración para posibilitar de manera eficiente la cooperación entre sistemas y lograr una plena gestión de la red.

Claridad para facilitar la interoperabilidad y la posibilidad de la reutilización de especificaciones.

b) Modelos de Arquitectura TMN

Según la descripción de TMN, el propósito de la arquitectura de la red de gestión es permitir a los operadores minimizar los tiempos de reacción a los eventos que se presentan en la red, optimizar el flujo de información de gestión, permitir la distribución del control y mejorar el servicio de asistencia y las interacciones con los clientes; es decir, dar soporte a numerosas aplicaciones de gestión de redes y servicios de telecomunicaciones. Una aplicación de gestión es una actividad de procesamiento distribuido de información, que se caracteriza por la cooperación de dos o más procesos de gestión ubicados en diferentes entidades que componen la TMN y que necesitan comunicarse entre sí.

Dentro de la arquitectura TMN general existen tres aspectos básicos de ésta que pueden ser considerados por separado al planificar y diseñar una TMN que son:

- Arquitectura funcional (lógica)
- Arquitectura de la información
- Arquitectura física

1) Arquitectura Funcional de la TMN

La arquitectura funcional TMN se define desde el punto de vista de los bloques de función, que a su vez proveen las funciones que permiten a la TMN realizar la gestión (almacenamiento, transporte y procesamiento de información).

La arquitectura funcional de la TMN se basa en tres conceptos fundamentales: el bloque funcional, el componente funcional y el punto de referencia.

Los bloques funcionales representan agrupaciones de funciones generales de la TMN, lo que permite un tratamiento modular de la red y con ello la flexibilidad requerida por ella.

Los puntos de referencia caracterizan las fronteras entre los bloques funcionales, a través de las cuales ocurren los intercambios de información.

Los componentes funcionales son desagregados de los bloques funcionales y a su vez agrupan funciones de carácter más específico.

La figura 2.20 presenta la arquitectura funcional de la TMN, con los bloques funcionales y los puntos de referencia asociados.

i. Bloques Funcionales

Bloque Funcional Del Sistema De Operaciones (OSF). Procesa información asociada a alguna aplicación de gestión con objeto de monitorear, coordinar y/o controlar funciones de telecomunicaciones y/o funciones de gestión (es decir, la propia TMN).

Bloque Funcional De Elemento De Red (NEF). Representa las funciones desempeñadas por los recursos de telecomunicaciones, se comunica con una TMN con el propósito monitorear y controlar los recursos que aunque no hacen parte de ella son representados por el NEF.

Bloque Funcional De Adaptador Q (QAF). Permite conectar a la TMN aquellas entidades funcionales no-TMN con funcionalidades análogas a los bloques funcionales NEF y OSF, realizando la conversión entre un punto de referencia no-TMN y un punto de referencia "q3" o "qx" de la TMN.

Bloque Funcional De Mediación (MF). Actúa sobre la información que pasa entre un OSF y un NEF (o QAF), adaptándola, filtrándola o condensándola, a fin de asegurar que sea conforme a las expectativas de los bloques de función enganchados al MF.

Bloque Funcional De Estación De Trabajo (WSF). Representa la funcionalidad que permite el intercambio de información de gestión con el usuario de la TMN, e incluye el soporte para la interfaz hombre-máquina, aunque no se considera que estos aspectos formen parte de la TMN, por lo que esta parte del WSF aparece representada en el exterior de la frontera de TMN. El bloque WSF proporciona los medios para la comunicación entre los bloques funcionales (OSF, MF, DCF, NEF) y el usuario.

Una función no considerada como bloque funcional pero de vital importancia para la TMN es la DCF - Función de Comunicación de Datos, que se utiliza para transportar, de manera pasiva, la información de gestión intercambiada entre los demás bloques funcionales ya que es la encargada de proveer las funciones de los tres primeros niveles del modelo de referencia OSI.

ii. Puntos de Referencia.

- Puntos de referencia q: Estos puntos conectan los bloques funcionales NEF a los MF, MF a MF, MF a OSF y OSF a OSF, directamente o a través del DCF.
- Puntos de referencia f: Estos puntos conectan los bloques funcionales OSF, MF, al WSF.
- Puntos de referencia g: Son los puntos entre el WSF y el usuario.
- Puntos de referencia x: Conectan una TMN a redes de gestión de otro tipo (OSFs de dos TMNs) incluyendo otras TMN.

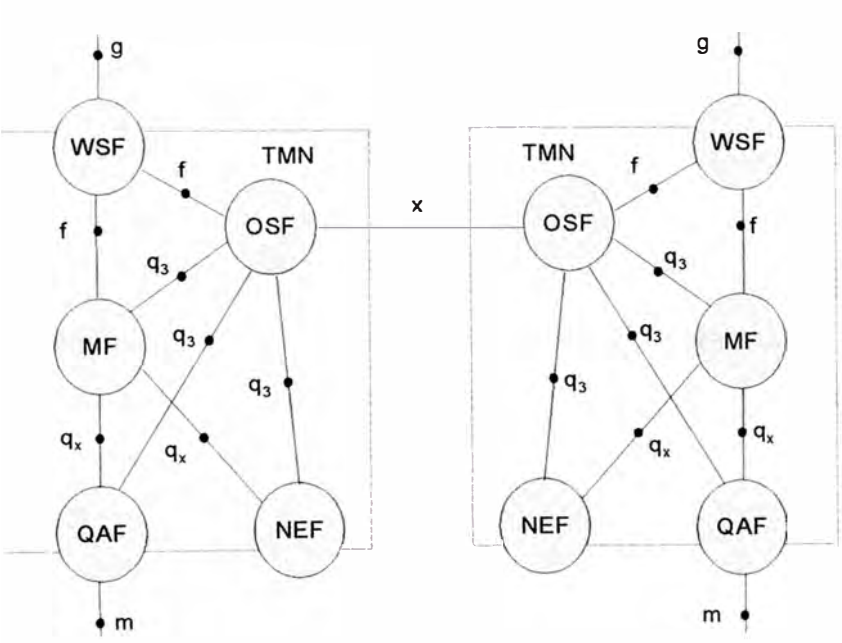


Figura 2.20 Arquitectura Funcional De TMN

TABLA 2.1 Relación entre Bloques Funcionales y Puntos de Referencia

DESCRIPCIÓN DE LOS BLOQUES		DESCRIPCIÓN DE LOS PUNTOS DE REFERENCIA	
OSF	Función de sistema de operaciones	q3	Entre OSF y MF, QAF o NEF
MF	Función de Mediación	qx	Entre MF y QAF o NEF
QAF	Función de adaptador Q	f	Para conectar una WSF
WSF	Función de Estación de Trabajo	x	Entre dos OSF de dos TMN
NEF	Función de Elemento de Red	g	Entre la WSF y el usuario
		m	Entre la QAF y entidades no TMN

iii. Componentes Funcionales

- Función De Aplicación De Gestión (MAF). Representa la funcionalidad de aplicación de gestión o parte de ella y recibe su denominación según el bloque al que pertenece, es decir, OSF-MAF, NEF-MAF, QAF-MAF, MF-MAF.
- Base De Información De Gestión (MIB). Almacén de datos donde se deposita toda la información de gestión y representa al conjunto de objetos gestionados que pertenecen a un sistema gestionado.
- Función De Comunicación De Mensajes (MCF). Asociada a todos los bloques funcionales que tienen una interfaz física, se usa exclusivamente para el intercambio de información de gestión contenida en mensajes entre pares de bloques de la TMN y eventualmente puede proveer funciones de convergencia de protocolos. Dependiendo de cual sea la pila de protocolo soportada por el punto de referencia, la MCF recibe su denominación

(MCFq3, MCFqx, MCFf, MCFx, MCFm). Este componente provee los protocolos y servicios de los siete niveles del modelo OSI.

- Función De Conversión De Información (ICF). Componente Funcional encargado de traducir el modelo de Información entre dos interfaces diferentes. Transforma los mensajes intercambiados a nivel sintáctico o a nivel semántico y es un componente obligatorio de los bloques MF y QAF.
- Función De Presentación (PF). Traduce la información que cursa entre el modelo de información de la TMN y la interfaz de Usuario y viceversa. Brinda un entorno amigable que permite al usuario introducir, visualizar y modificar los objetos de gestión.
- Función De Adaptación Hombre Máquina (HMA). Componente funcional que traduce la información que cursa entre el modelo de información de la MAF y el modelo de información que la TMN presenta a la PF y viceversa.

2) Arquitectura Física de la TMN

Este modelo genérico define los elementos fisicos que conforman la TMN y las interfaces que permiten interconectarlos. Estos elementos fisicos constituyen los bloques que representan implementaciones de las funcionalidades de la TMN. Bajo este punto de vista, los bloques funcionales de gestión se convierten en bloques de construcción de TMN y los puntos de referencia se convierten en interfaces. La figura 2.21 muestra una forma de implementar la arquitectura fisica TMN.

La arquitectura fisica debe agrupar los bloques funcionales en entidades fisicas con el objeto de alcanzar los requisitos de flexibilidad.

Las entidades fisicas mediante las cuales se implementa la TMN van desde los Sistemas de Operaciones hasta la Red de Comunicación de Datos (Data Communication Network, DCN), que es la encargada de transportar la información de gestión alrededor de la red. Los componentes de la arquitectura fisica incluyen:

- Sistemas de Operaciones.
- Dispositivos de Mediación.
- Estaciones de Trabajo.

- Red de Comunicación de Datos.
- Elementos de Red.

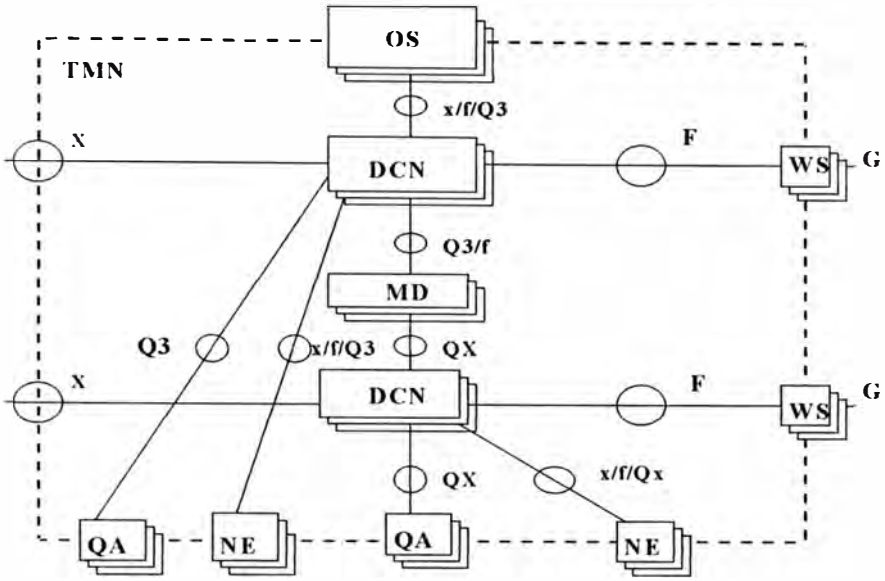


Figura 2.21 Arquitectura Física De La TMN

Sistema De Operaciones (OS). Componente de la Arquitectura Física de la TMN que ejecuta las funciones de sistemas de operaciones y que eventualmente puede proporcionar funciones de mediación, de adaptador Q y de estación de trabajo.

Elemento De Red (NE). Equipos de telecomunicaciones (o grupos de ellos) y de soporte que pertenecen al entorno y sobre los cuales se ejecutan funciones de elemento de red.

Adaptador Q (QA). Dispositivo utilizado para conectar con la TMN entidades semejantes a NEs y a OSs que no proporcionan interfaces TMN normalizadas.

Estación De Trabajo (WS). Elemento de la Arquitectura Física de la TMN que permite al usuario visualizar la información de gestión, facilitando además la entrada y edición de datos a fin de gestionar objetos.

Dispositivo De Mediación (MD). Este elemento ejecuta las funciones de mediación y eventualmente las funciones de sistemas de operaciones, de adaptador Q y de estación de trabajo.

Red De Comunicación De Datos (DCN). Es la red encargada de soportar la función de comunicación de datos y representa una realización de los niveles 1 a 3 del sistema OSI (incluye las normas OSI para estos niveles). La DCN no proporciona funcionalidad alguna de los niveles 4 a 7 OSI y puede constar de sub-redes individuales, o redes diferentes interconectadas entre si.

Se aclara que la DCN es una red conceptual, la recomendación M.3010 de la ITU-T afirma "...una TMN es conceptualmente una red separada que tiene interfaces con una red de Telecomunicaciones para recibir información desde ella y para controlar sus operaciones". Esto permite que la DCN pueda ser implementada como una red superpuesta separada, por ejemplo X.25, o una red TCP/IP, siendo este último el estándar acogido.

Como otro componente de la arquitectura fisica de la TMN se encuentran las interfaces, que se asocian a los puntos de referencia del modelo funcional:

- Interfaz Q: aplicada en puntos de referencia q. Puede ser Qx (entre MD y EN) y Q3 (entre OS y los elementos TMN).
- Interfaz F: Aplicada en puntos de referencia f.
- Interfaz X: Aplicada en puntos de referencia x.
- Interfaz G: Aplicada en puntos de referencia g.

3) Arquitectura de Información de la TMN

La arquitectura de la información de la TMN describe la naturaleza de la información que necesita ser intercambiada entre los bloques de función de gestión (OSF y OSF, OSF y MF, OSF y WSF, OSF y QAF, OSF y NEF, MF y NEF, MF y QAF). Esta arquitectura describe un modelo de información orientado a objetos, presentados como abstracciones de las propiedades de los recursos (fisicos o lógicos) que están siendo gestionados (así, un recurso puede ser representado por más de un objeto), y además se basa en los conceptos manejados por el modelo de gestión de los sistemas OSI; así, todo intercambio de información de gestión involucra un "sistema gestionador" (GESTOR) que controla y/o hace el monitoreo remoto de los recursos de un "sistema gestionado" (AGENTE), intercambio que para ser efectivo necesita una visión compartida de la información y de las reglas de comunicación usadas.

Un objeto gestionado también puede representar una relación entre recursos, o combinaciones de ellos.

Para interactuar, los sistemas de gestión deben compartir una visión o entendimiento del medio, que incluye cuales son las funciones y objetos gestionados soportados, las capacidades de gestión autorizadas, las capacidades de protocolo soportadas, los ejemplares de objetos gestionados disponibles, y las relaciones de continencia entre objetos, entre otros, a toda esta información se le conoce como SMK Conocimiento de Gestión Compartido. EL modelo de Información de la TMN define la sintaxis y la semántica de toda esta información intercambiada entre los sistemas de gestión que se comunican, constituyéndose en el elemento esencial para garantizar la interoperabilidad.

Los objetos gestionados poseen atributos que representan sus características más relevantes, son caracterizados también por las operaciones que pueden soportar y por las notificaciones que pueden emitir. Además, el objeto gestionado tiene un comportamiento, que representa la manera cómo reacciona a una operación y las condiciones bajo las cuales genera una notificación.

El conjunto de todos los objetos definidos en un sistema gestionado, junto con sus propiedades, atributos, operaciones, notificaciones y comportamiento constituye la MIB (Base de Información de Gestión) del sistema

La interacción entre gestor, agente y objetos es mostrada en la siguiente figura 2.22.

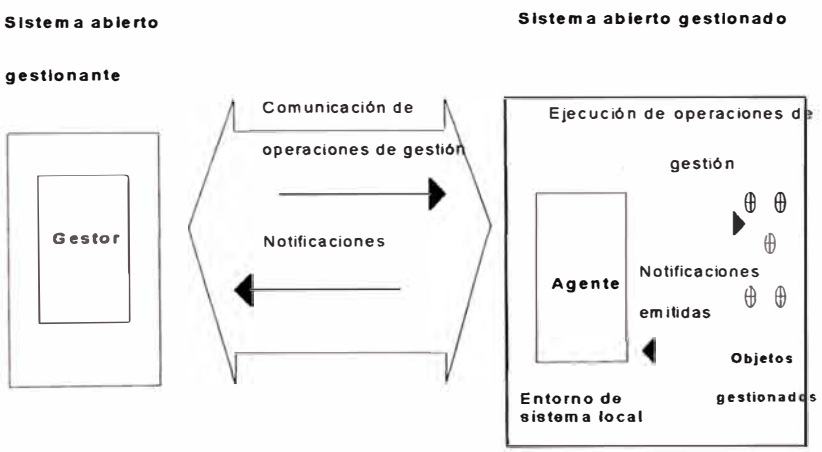


Figura 2.22 Interacción Entre Gestor, Agente Y Objetos

El agente procesa las operaciones emitidas por el gestor sobre sus objetos contenidos en la MIB, además filtra y/o concentra las notificaciones emitidas por los objetos reflejando sus comportamientos al gestor. Es así como un gestor puede verse involucrado en el intercambio de información con muchos agentes, y un agente con muchos gestores.

Los intercambios de operaciones y notificaciones entre gestor y agente se realizan a través del uso de los servicios CMIS (Sistema Común de Información de Gestión) y se transportan a través del protocolo CMIP (Protocolo Común de Información de Gestión).

La información de gestión se considera desde dos puntos de vista:

- MODELO DE INFORMACIÓN DE GESTIÓN: Es una abstracción de los aspectos de gestión involucrados con la red fisica y con las actividades de gestión que de ella se derivan. Este modelo determina el tipo de información que se puede intercambiar de forma normalizada. Esta actividad de soporte del modelo de información tiene lugar a nivel de aplicación, e involucra una variedad de funciones de aplicación de gestión, tales como el almacenamiento, la consulta y el procesamiento de información.
- INTERCAMBIO DE INFORMACIÓN DE GESTIÓN: Involucra las funciones de comunicación de datos (DCFs) a través de una red de comunicaciones , y las funciones de comunicación de mensajes (MCFs), que permiten conectar distintos componentes fisicos a la red de telecomunicaciones en una interfaz dada. Este nivel de actividad involucra solamente mecanismos de comunicación tales como pilas de protocolos.

c) Modelo Lógico de TMN

La TMN puede considerarse desde el punto de vista de niveles que agrupan las responsabilidades de gestión lo que permite establecer una jerarquía de los OSFs para llevar a cabo las actividades de gestión.

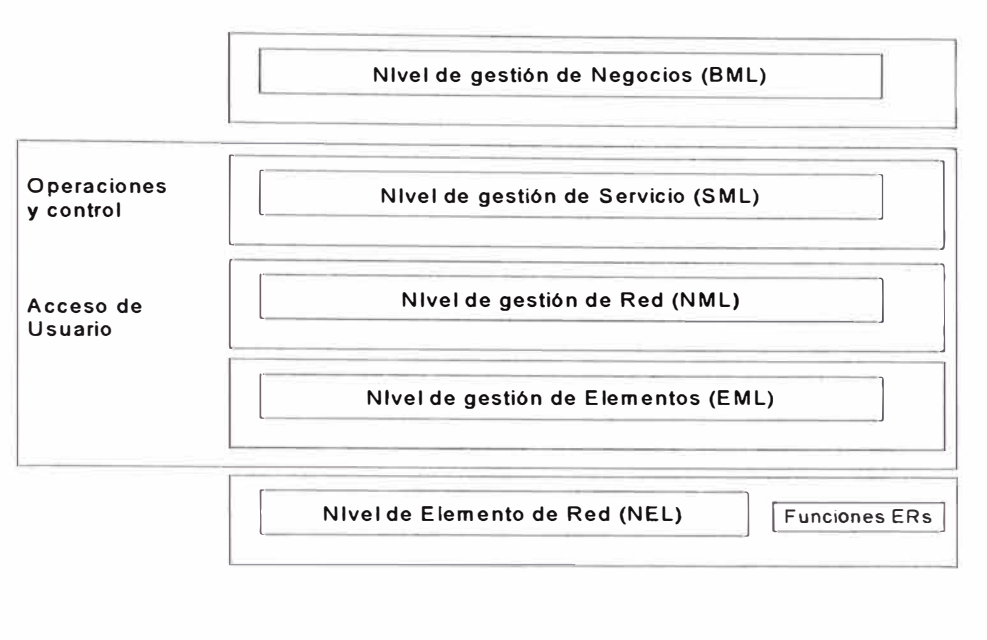


Figura 2.23 Estructura De Múltiples Niveles TMN

En esta jerarquía, cada Nivel restringe las actividades de gestión con limites que definen claramente el rango que es concerniente con algunos subgrupos de las actividades totales de gestión.

1) **Nivel de Gestión Comercial (BML)**

   Es responsable de gestión de la totalidad de la empresa. En el realizan los acuerdos entre operadores, se definen los objetivos de la compañía asignando tareas específicas, presupuestos, etc., siendo necesarias muchas interacciones con otros sistemas de gestión.

2) **Nivel de Gestión de Servicios (SML)**

   Este Nivel es la encargada de gestionar los aspectos contractuales de los servicios prestados o disponibles para los clientes y cuenta con el Nivel de gestión de red para el aprovisionamiento técnico de dichos servicios. La SML tiene seis tareas principales de gestión:

   - Asegurar el contrato con el cliente y la interfaz con otros proveedores de servicios de red.
   - Interactuar con proveedores de servicios.
   - Interactuar con el Nivel NML.
   - Mantenimiento de datos estadísticos.
   - Interacción entre servicios.
   - Interactuar con el Nivel comercial.

3) Nivel de Gestión de Red (NML)

Es responsable de los aspectos de red y de los requisitos de servicios solicitados por el Nivel de gestión de servicios, conoce plenamente qué recursos están disponibles en la red y cómo pueden ser controlados. La NML tiene una vista global de la red y también es responsable de proveer el rango y la cantidad inicial de recursos de red que encuentra para ofrecer el servicio.

Tiene la responsabilidad de la gestión de todos los elementos de red, ya sea individualmente o en grupo. Realiza la gestión de una amplia área geográfica localizada en este Nivel.

La NML tiene 3 tareas principales:

- Control y coordinación de la red examinando todos los elementos de ella con su alcance y dominio.
- Aprovisionamiento de capacidades de red para soportara los servicios.
- Interacción con el Nivel de gestión de servicios en cuanto ejecución, uso, disponibilidad, etc.

Así el Nivel NML provee la funcionalidad para manejar la red coordinado actividades a través de ella, y soportando la demanda hecha por el Nivel SML.

4) Nivel de Gestión de Elementos de Red (EML)

Gestiona cada elemento de red por separado y soporta una abstracción de las funcionalidades proporcionadas por el Nivel de elemento de red. Este tiene elementos gestionadores o OS´s (Sistemas de Operaciones), donde cada uno de los cuales se responsabiliza por la información gestionable propia de la TMN, acerca de algún elemento de red. En general un elemento de gestión o gestionador de red es responsable de un subconjunto de elementos de red, este se encarga de gestionar los datos, accesos, actividades, etc. de cada uno de estos. Lógicamente, los dispositivos de mediación (MD´s), están en el EML, aun si estos están localizados fisicamente en algún otro nivel lógico, tales como el NML o el SML. Un dispositivo MD se comunica con un EML OS (Sistema de Operaciones de un EML) por medio de una interfaz Q3. Además, un EML OS presenta su

información de gestión desde un subconjunto de elementos de red s un OS en el NML a través de una interfaz Q3.

Los datos de gestión específicos se almacenan y se convierten en formatos uniformes.

La EML tiene 3 principales funciones:

- Control y coordinación de un grupo de elementos de red.
- Provee una función de mediación que permite que el Nivel de gestión de red interactúe con los elementos de red.
- Mantenimiento de estadísticas, registros y otros datos acerca de los elementos.

En este Nivel se encuentran lógicamente todas las funciones de mediación, incluyendo las localizadas fisicamente en otras partes.

5) Nivel de Elemento de Red (NEL)

Este Nivel contiene funciones que son enlazadas a la tecnología o arquitectura de los elementos de red que proveen el transporte de la información básica y el procesamiento de los servicios, y que son accesadas por las funciones de EML usando estándares o modelos de información abiertos.

2.2.3 GESTIÓN EN INTERNET / SNMP (V.1, V.2 Y V.3)

Este capítulo discute y analiza la aproximación de gestión que estandarizada por la Fuerza o Grupo de Labores en Ingeniería de Internet (IETF). Esta aproximación también es conocido como el Protocolo de Gestión de Red Simple (SNMP) o como la aproximación de Gestión TCP/IP.

El término Simple Network Management Protocol (SNMP) se refiere a una colección de especificaciones para gestión de red que incluye el mismo protocolo, la definición de una base de datos, y los conceptos asociados.

a) Cronología

En la década pasada Internet creció vertiginosamente a un tamaño en el que la gestión no cubría eficientemente el entorno, por ello fue solicitada una aproximación estructurada y estandarizada para la gestión de Internet. Por consiguiente, en 1987 tres propuestas de gestión aparecieron. Una de éstas, la **High - level Entity System /**

Protocol (HEMS / HEMP), que fue retirada demasiado pronto, y tan sólo permanecieron dos: el **Protocolo de Gestión de Red Simple (SNMP)** y la **Gestión Común Sobre TCP/IP (CMOT)**. Pero para marzo de 1988, se hizo una reunión del equipo de ingeniería encargado de Internet, la cual tomó la decisión de usar SNMP en un corto término y CMOT en un largo término.

En 1988, reconociendo la necesidad de una gestión de red distribuida e interoperable, el Internet Activities Board (IAB) revisó algunas propuestas y aprobó SNMP como una solución a corto plazo, y CMOT (CMIP over TCP/IP) como la solución a largo plazo. En aquel tiempo se pensó que en un tiempo razonable, las instalaciones TCP/IP migrarían a protocolos basados en OSI. De esta forma no se quiso invertir mucho esfuerzo el desarrollo de protocolos de nivel de aplicación que probablemente tendrían que ser abandonados pronto. Para ayudar la transición desde SNMP hacia CMOT, el IAB dictaminó que ambos deben utilizar la misma base de datos de objetos gestionados. Sin embargo pronto llegó a ser evidente que este ligamiento fue impráctico. En la gestión de redes OSI, los objetos gestionados han sido vistos como entidades sofisticadas con atributos, procedimientos asociados, capacidades de notificación, y otras características complejas asociadas con la tecnología orientada a objetos. Para mantener a SNMP simple, no se diseño para trabajar con objetos. De hecho los objetos SNMP no son realmente objetos desde el punto de vista de la tecnología orientada a objetos; en lugar de ello, los objetos en SNMP son simplemente variables con unas pocas características básicas, tales como tipo de dato, y atributos de solo – lectura o lectura – escritura. De acuerdo a esto, el IAB permitió que el desarrollo de SNMP y CMOT procediera de manera independiente y en paralelo.

CMOT estaba indicado para hacer uso de los estándares de gestión de sistemas OSI (tales como CMIP) en el Entorno Internet. CMOT enfrentó los mismos problemas que la gestión de OSI: las especificaciones técnicas no aparecían a tiempo, no había virtualmente experiencia operacional en aplicaciones ni implementaciones de las cuales hubiesen podido obtenerse. Como resultado, el soporte para CMOT disminuyó lentamente. En 1992 todo el trabajo en CMOT se detuvo.

SNMP actualmente es un desarrollo ampliado de SGMP (Simple Gateway Monitoring Protocol). SGMP fue elegido para la gestión de Sistemas Intermedios

(gateways). Debido al éxito de SGMP, se decidió extender su alcance e incluirlo en la Gestión los Sistemas Terminales. Para reflejar este cambio, el protocolo se renombró como SNMP.

Una interesante diferencia entre el IETF y la ISO es que el IETF toma una aproximación más pragmática que ISO. En el IETF es por ejemplo raro dedicar mucho tiempo en discusiones arquitecturales; la gente prefieren usar su tiempo en el desarrollo de protocolos y aplicaciones. Esta actitud diferente explica el por qué no hay ningún estándar especial que se haya definido para la Arquitectura de Gestión Internet; únicamente se han estandarizado protocolos y MIB's. Afortunadamente se tiene escrito mucha literatura que describen los principios de gestión de Internet. De estos escritos se han extractado las siguientes ideas:

- Todos los sistemas conectados a la red deben ser gestionados con SNMP.
- El costo de agregar la gestión de red a los sistemas existentes debe ser mínimo.
- Debe ser relativamente fácil extender las capacidades de gestión de los sistemas existentes (por medio de la extensión de la Base de Información de Gestión).
- La gestión de red debe ser robusta. Incluso en caso de fallas, debe estar aún disponible un pequeño conjunto de capacidades de gestión.

Al parecer SNMP fue la solución correcta en el momento correcto. Y Pocos años después de la publicación del estándar la mayoría de equipos de comunicación de datos podían ser gestionados por medio de SNMP; este (SNMP) se había convertido en el estándar de facto para la gestión de redes de comunicación de datos. Aún SNMP tiene un poco de deficiencias. En 1992 empezó el trabajo de desarrollar una versión mejorada de SNMP y por consiguiente esta nueva versión se llamó SNMPv2.

b) Arquitectura

La arquitectura utilizada para gestión de redes TCP/IP incluye los siguientes elementos:

- Gestor
- Agente SNMP
- MIB de Agentes
- Protocolo SNMP

El agente SNMP y la MIB de Agente juntos corresponden al objeto gestionado en el modelo de referencia, y el protocolo SNMP corresponde al entorno de mediación. La arquitectura SNMP no especifica servicios.

1) Gestor

El gestor sirve como interfaz para el gestor humano, y debe tener como mínimo:

- Un conjunto de aplicaciones de gestión para análisis de datos, recuperación de fallas, etc.
- Una interfaz mediante la cual el gestor de red puede monitorear y controlar la red.
- La capacidad de trasladar los requerimientos del gestor de red dentro del control y monitoreo actual de los elementos remotos.
- Una base de datos de información extraída a partir de las MIBs de todas las entidades gestionadas en la red.

Únicamente los dos últimos elementos son tema de SNMP.

2) Agente SNMP

El otro elemento activo en el sistema de gestión de red es el agente de gestión. Plataformas claves como hosts, bridges, ruteadores y hubs pueden ser equipados con agentes SNMP de tal forma que ellos puedan ser gestionados por el elemento gestor. El agente de gestión responde a las peticiones de información y de acción provenientes de las funciones de gestión del sistema y pueden proveer información importante pero no solicitada de manera asincrónica.

La utilización de SNMP requiere que todos los agentes, tal como las estaciones gestionadas, soporten UDP e IP. Esto excluye algunos dispositivos como bridges y modems, que no soportan alguna parte de la suite de protocolos TCP/IP. Además puede haber varios sistemas más pequeños que soportan TCP/IP pero para los cuales no es deseable adicionar carga extra de SNMP, lógica de agente o soporte MIB.

Para acomodar tales dispositivos, se desarrollo el concepto de proxy. En este esquema, un agente SNMP actúa como un representante para uno o varios

dispositivos, es decir el agente SNMP actúa en nombre de los dispositivos representados.

3) MIB de Agente

La MIB (Management Information Base) contiene los objetos gestionados que el agente hace disponibles al gestor. El tipo y estructura de la información de gestión es determinada por el SMI (Structure of Management Information) de Internet. En el caso de SNMP, un objeto es una variable de tipo escalar, y la MIB esta conformada por una estructura jerárquica simple de objetos.

El modelo de información de Internet prescribe que únicamente una instancia de objeto puede existir para cada tipo de objeto. La forma en la cual cada instancia de objeto es referido, no es asunto del modelo de información. Es la responsabilidad de cada protocolo de gestión ceñirse al SMI para definir este mecanismo. Uno de tales protocolos el Simple Network Management Protocol (SNMP).

4) Protocolo de Gestión de red Simple

La importancia de SNMP radica en su popularidad y propagación en el mundo Internet. En SNMP las únicas operaciones que son soportadas son alteraciones o inspecciones de variables. Específicamente, cuatro operaciones pueden se realizadas:

- **Get:** Una estación de gestión recupera un valor de objeto escalar desde el agente.
- **GetNext:** Una estación de gestión recupera la siguiente pieza de información desde una tabla o lista dentro de un agente.
- **Set:** Un estación de gestión actualiza un valor de objeto escalar en un agente.
- **Trap:** Un agente envía un valor de objeto escalar no solicitado hacia la estación de gestión.

c) El Protocolo Original de SNMP

Las ideas detrás de SNMP son relativamente fáciles de entender. Hay una pequeña diferencia de hecho, entre las ideas detrás de SNMP y las ideas que han existido en

ISO desde 1987; eso fue antes de que ISO adoptara la aproximación de la Orientación a Objetos (OO) para la gestión. Los ejemplos de tales ideas comunes son:

- El concepto de Gestor/Agente.
- La idea de también usar las funciones de gestión para el intercambio de información de gestión.
- La idea para usar las PDU's GET y SET para operaciones sobre la información de gestión.
- La idea de usar ASN.1 para la definición de la información de gestión y de la MIB.

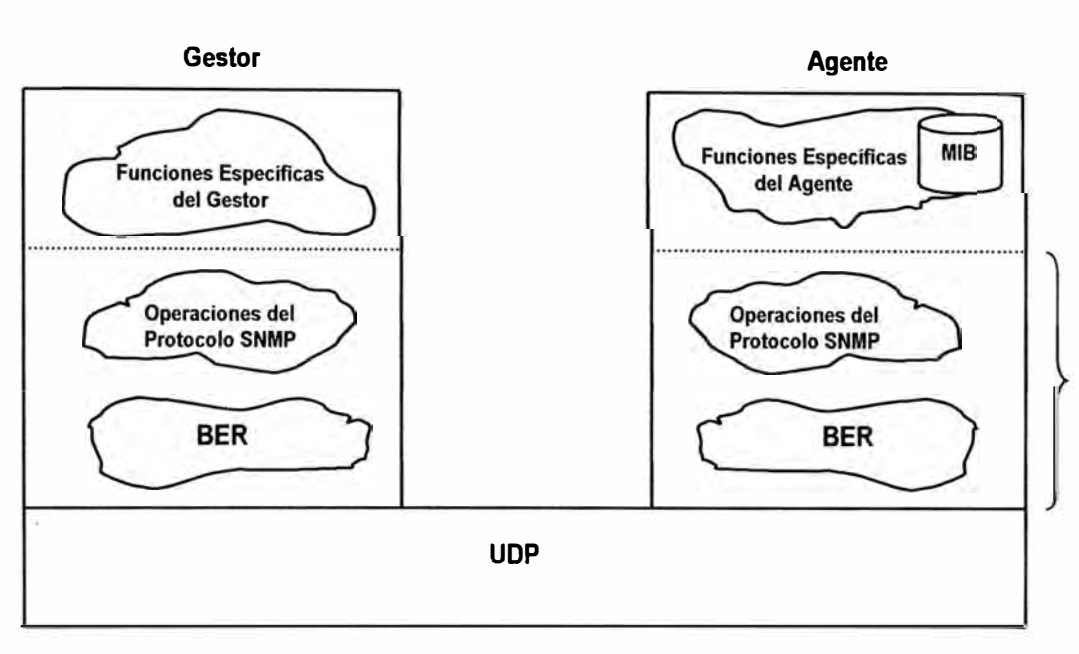


Figura 2.24 Estructura de Gestión Internet

SNMP fue diseñado para ser un protocolo del nivel de aplicación que es parte de la Suite de protocolos de TCP-IP. Como se muestra en la Figura 2.25, SNMP opera típicamente sobre un Protocolo de Datagramas de Usuario (UDP), aunque también puede operar sobre TCP. Para una Estación de Gestión Autosuficiente, un proceso Gestor controla el acceso a la MIB central en la estación de gestión y proporciona una interfaz al Gestor de red. El proceso Gestor realiza la gestión de red por medio de SNMP, el cual es implementado en la parte alta de UDP, IP y en los relevantes protocolos dependientes de red (ejemplo: Ethernet, FDDI, X.25).

Cada agente debe también implementar SNMP, UDP e IP. Además hay un proceso Agente que interpreta los mensajes SNMP y controla el acceso remoto a la MIB del Agente. Para un dispositivo Agente que soporte otros tipos de aplicaciones, tales como FTP, se requiere de igual forma a TCP como a UDP.

Desde una Estación de Gestión, hay tres tipos de mensajes SNMP que son emitidas en nombre de una aplicación de gestión: GetRequest, GetNextRequest y SetRequest. Las dos primeras son variaciones de la función get; todos los tres mensajes son reconocidos y confirmados por el Agente en la forma de un mensaje GetResponse, el cual es pasado a la aplicación de gestión. Además un Agente puede emitir un mensaje trap en respuesta a un evento que afecte la MIB y los recursos de gestión asociados.

SNMP se fia sobre UDP, el cual es un protocolo sin conexión, SNMP es en si sin conexión. Ninguna clase de continuas conexiones se mantienen entre las Estaciones de Gestión y sus Agentes. En cambio cada intercambio es una transacción separada entre una Estación de Gestión y un Agente.

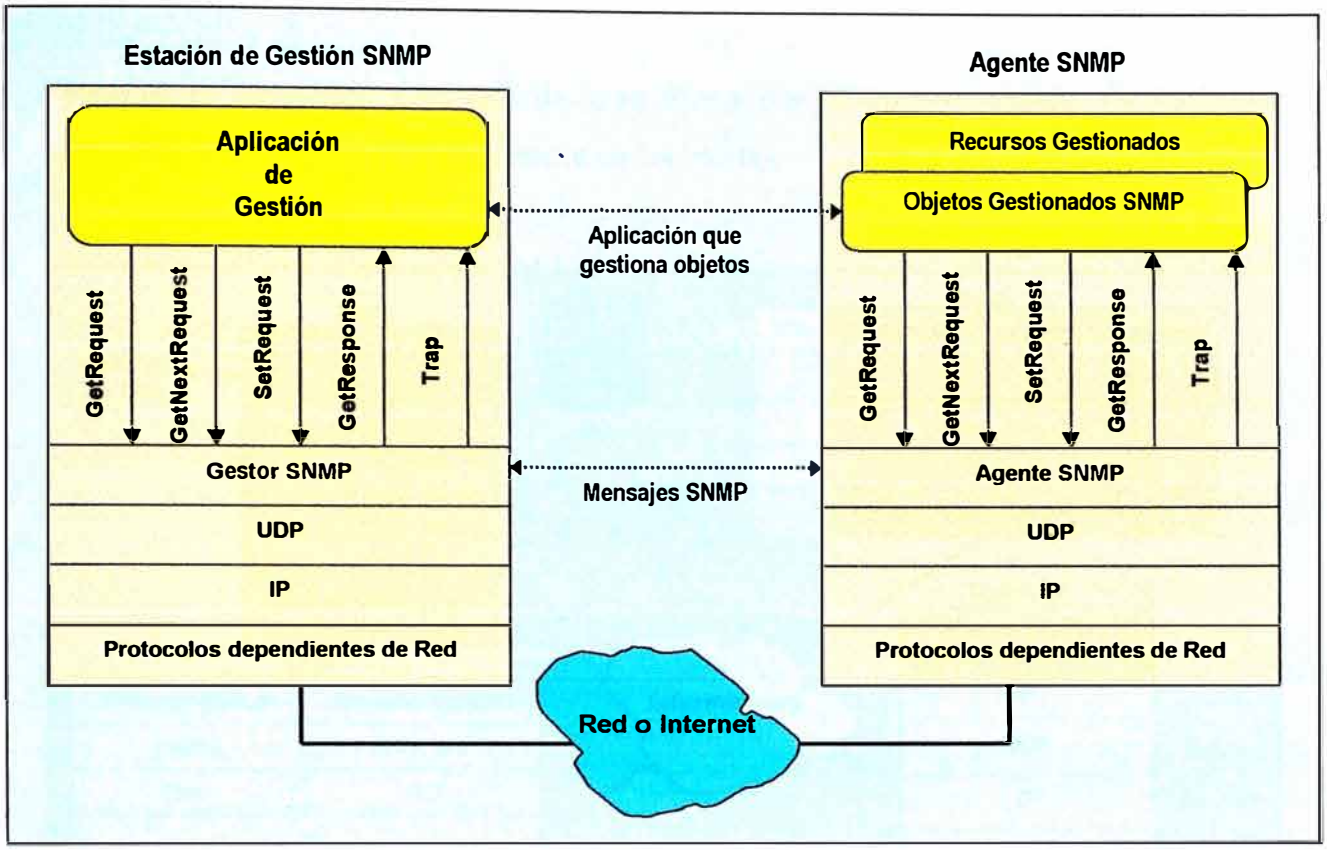


Figura 2.25 El Rol de SNMP

Con SNMP, un solo gestor puede controlar a muchos agentes. Como muestra en la Figura2.24. El protocolo SNMP se construye sobre el Protocolo de Datagramas de Usuario (UDP), que es un protocolo de transporte sin conexión. Desde que la información de gestión Internet así como los formatos de las PDU's de SNMP se definen según (un subconjunto de) la sintaxis ASN.1, se requieren las funciones de codificación inmediatamente encima de UDP. Estas funciones operan según las Reglas de Codificación Básicas (BER) que aplique un gestor con funciones específicas. Se definen cinco tipos de PDUs de SNMP: GetRequest, GetNextRequest, SetRequest, Response y Trap. El Estándar del Protocolo SNMP no dice cuales son las funciones que son específicas para gestores o agentes; el estándar SNMP se restringe así a las funciones que están debajo de la línea punteada (Figura 2.24). Esto implica que el alcance de SNMP es equivalente al de CMIP; no existe un estándar opuesto a CMIP, que defina el servicio que se proporciona en el tope de SNMP. El modelo de Gestión de SNMP se aprecia en la Figura 2.26.

El IETF no tiene aún definidas las funciones específicas del gestor; por consiguiente, se necesita urgentemente un trabajo extenso en esta área. La falta de las funciones

específicas del gestor contrasta de gran forma con al número grande de funciones específicas del agente (principalmente en las MIBs).

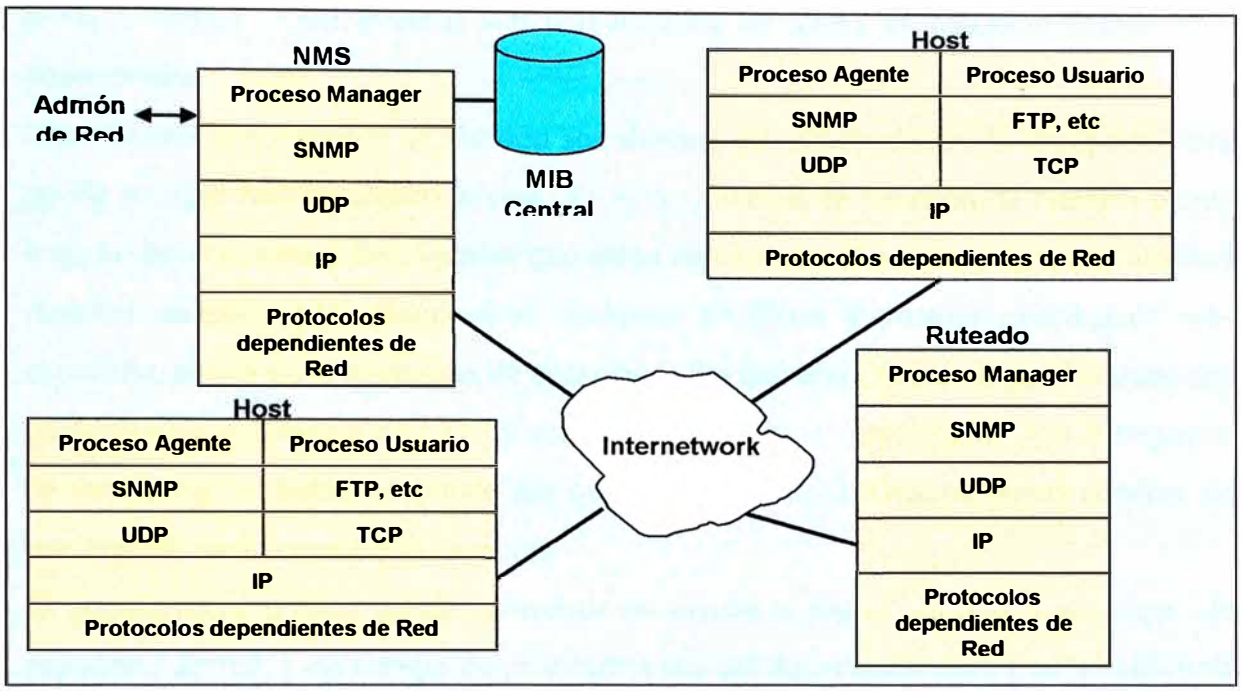


Figura 2.26 Modelo de Gestión de SNMP

Si una estación de Gestión es responsable de un gran número de Agentes, y si cada Agente mantiene un gran número de objetos, estos es impráctico para la Estación de Gestión para sondear regularmente a todos los agentes y a todos sus datos que representan objetos y que pueden ser leídos. En cambio, SNMP y la MIB asociada son diseñadas para fomentar que el Gestor use una técnica conocida como *trap-directed polling.*

La estrategia recomendada es; en el momento de la inicialización, y quizás a intervalos irregulares (sin frecuencia), como una vez al día, una Estación de Gestión puede hacerle poll a todos los agentes sí sabe o conoce información clave, tal como las características de la interfaz, y quizás algunas estadísticas de rendimiento básicas, tales como número promedio de paquetes enviados y recibidos sobre cada interfaz en un periodo determinado de tiempo. Cuando esta base es establecida, la Estación de Gestión es detenida desde el polling. En cambio, cada Agente es responsable de

notificar a la Estación de Gestión de cualquier evento inusual. Ejemplos de esto son sí el Agente colapsa o falla y es re-iniciado, la falla de un enlace, o una condición de sobrecarga tal como la que se define cuando la carga de paquetes sobrepase algún límite o umbral. Tales eventos son comunicados en forma de mensajes SNMP y se conocen como *traps*.

Una vez que una Estación de Gestión sea alertada de una condición de excepción, esta puede escoger realizar alguna acción. En esta situación, la Estación de Gestión puede hacerle directamente a los Agentes que estén reportando el evento y quizás a algunos Agentes cercanos para diagnosticar cualquier problema y obtener información más específica acerca de la condición de excepción. Sin embargo, debido a que los traps son comunicados por medio de UDP y son por consiguiente despachados y/o entregados de una forma no fiable, se puede dar que una Estación de Gestión pueda sondear de una manera no frecuente a los agentes.

El trap-directed polling puede repercutir en ayudar a lograr ahorros sustanciales de capacidad de red, y de tiempo de procesamiento del Agente. Es claro que las redes no están hechas para transportar información de gestión, que una Estación de Gestión no esté necesitando, y los Agentes no están hechos para responder a solicitudes frecuentes que representen información sin interés.

En cuanto a los Proxies, el uso de SNMP requiere que todos los Agentes, así como las Estaciones de Gestión, soporten UDP e IP. Esto limita a que la gestión se encargue de tales dispositivos y excluya a otros, tales como algunos bridges y modems, que no estén en capacidad de soportar parte de la suite de protocolos TCP/IP. Además, pueden haber numerosos sistemas pequeños (computadores personales, estaciones de trabajo, controladores programables), que implementan TCP/IP para soportar sus aplicaciones, pero para los cuales no es deseable agregar una carga adicional de SNMP, lógica del agente, y mantenimiento de la MIB.

Entonces el concepto de proxy se desarrolló para acomodar a estos dispositivos que no implementan TCP/IP. En este esquema un Agente SNMP actúa como un proxy para uno o más dispositivos, esto quiere decir que el Agente SNMP actúa en nombre de los dispositivos manejados por el uso de los proxies. La Figura 2.27 indica el tipo de arquitectura de protocolo que se usa a menudo. La estación de gestión envía consultas acerca de un dispositivo a su Agente proxy. El Agente proxy convierte cada consulta

en un protocolo de gestión que es usado por el dispositivo. Cuando una respuesta a una consulta es recibida por el Agente, se le pasa de nuevo una respuesta a la Estación de Gestión. Similarmente, sí una notificación de alguna clase de evento del dispositivo es transmitida al proxy, este lo envía sobre la estación de gestión en la forma de un mensaje trap.

1) Mapeos de Transporte

La opción para operar SNMP sobre UDP (connection less), tiene varias implicaciones. En primer lugar UDP es inestable, lo cual significa que los datos de usuario pueden perderse. La decisión de usar un proveedor de servicio de transporte inestable, se ha tomado deliberadamente. La razón es que en caso de fallos repetidos del proveedor, todavía debe ser posible intercambiar parte de la información de gestión. Con un proveedor fiable (orientado a conexión) no puede ser posible ni pasar. Los proveedores orientados a conexión son diseñados de acuerdo a un 'todo o nada' de la aproximación: o todos los datos se entregarán o ninguno se entregará. Si no pueden entregarse datos, la conexión se liberará. Los proveedores no orientados a conexión Se diseñan según la aproximación 'mejor esfuerzo' : aún en caso de fallas, algunos de los datos pueden llegar al destino. La gestión, por consiguiente, puede ser todavía posible, aunque de una manera limitada. Es interesante ver que el protocolo SNMP no realiza retransmisiones. La responsabilidad para detectar la pérdida de datos y el iniciar retransmisiones le queda al gestor, esto es debido a que normalmente los gestores se equipan mejor para determinar cuando se requieren las retransmisiones.

Una segunda implicación de usar un protocolo de transporte sin conexión, es que los gestores deben realizar algún tipo de sondeo para detectar si los agentes todavía son operacionales. Con los proveedores orientados a conexión (ejemplo: El servicio de presentación de OSI) esto no sería necesario, porque tales proveedores incluyen funciones de control del ciclo de vida. Tales funciones chequean periódicamente si los sistemas remotos (en nuestro caso los agentes) están todavía operacionales. En caso de que estén inactivos, el proveedor toma la iniciativa de liberar la conexión e informar al usuario (en nuestro caso el gestor).

Una característica de UDP es que los paquetes no pueden exceder un cierto tamaño. Para asegurar eso, solamente, se generarán paquetes de tamaño limitados, para ello el protocolo de SNMP ha definido varios reglas. Uno de estas reglas es que, si la respuesta a cierta solicitud SNMP excediera el tamaño de paquete máximo, ninguna información sería retornada. Los Gestores deben ser conscientes de esta regla y en lugar de emitir una sola solicitud que comprenda todo, se deben emitir múltiples solicitudes más pequeñas para conseguir una forma de información parte por parte, y por ende ser recuperada de la misma manera. Desafortunadamente los gestores, en muchos de los casos, no pueden predecir la cantidad de información que puede obtenerse por medio de una sola solicitud.

Aunque se piensa que SNMP opera encima de UDP, hay también RFCs que definen cómo operar SNMP encima de otros protocolos (ejemplo: Ethernet, IPX o aún OSI).

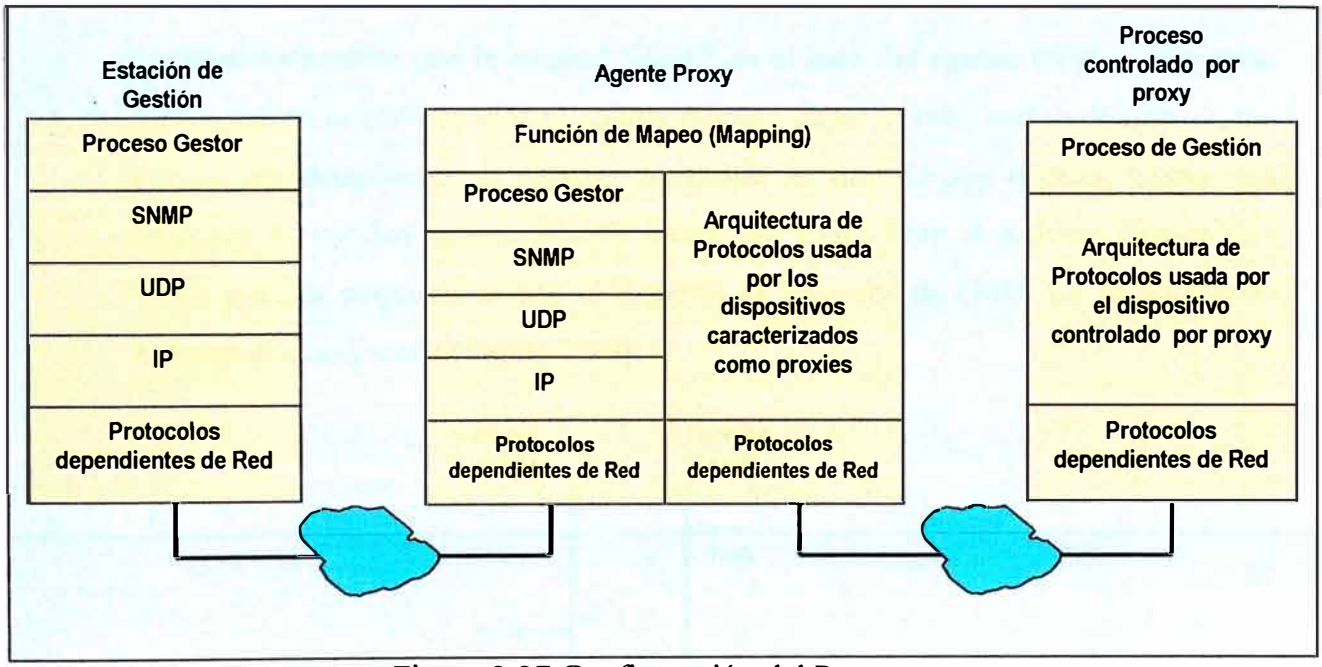


Figura 2.27 Configuración del Proxy

2) Operaciones de Protocolos

En SNMP, la comunicación del gestor al sistema del agente se realiza de forma confirmada. La entidad SNMP del lado Gestor toma la iniciativa de enviar una de

las siguientes PDU's: GetRequest, GetNextRequest o SetRequest. Se acostumbra usar a GetRequest y GetNextRequest para recuperar información de gestión del agente, el SetRequest es acostumbrado para guardar (o cambiar) la información de gestión.

Después de la recepción de una de estas PDU's, la entidad de SNMP en el lado del agente responde con una PDU (ver Figura 2.28). Esta PDU lleva la información pedida o indica la falla de la solicitud anterior.

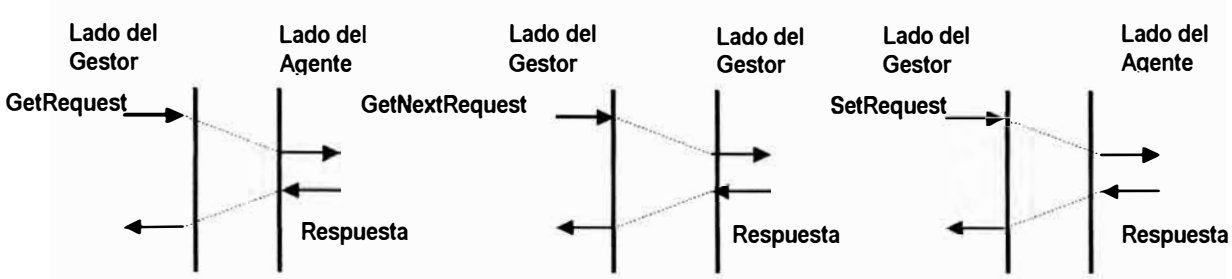


Figura 2.28 El Sistema Gestor Toma la Iniciativa

También es posible que la entidad SNMP en el lado del agente tome la iniciativa. Esto pasa en el caso en que el agente detecta algún evento extraordinario, como una re inicialización o un cambio de estado en uno de sus enlaces. Como una reacción, la entidad agente SNMP envía una PDU Trap al sistema Gestor (los Traps pueden compararse con el Reporte de Eventos de OSI). La recepción de Trap no es confirmada (Figura 2.29).

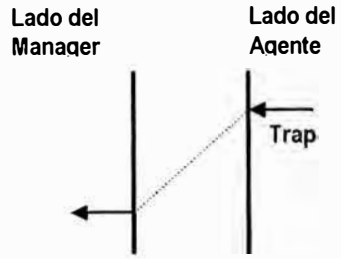


Figura 2.29 El sistema del Agente Toma la Iniciativa

SNMP no describe cómo relacionar varias interacciones Get, Set y Trap. Por ejemplo que hacer después de la recepción de un Trap no ha sido definido aún por

SNMP. En cambio, se considera que la determinación de esta relación es una responsabilidad de las funciones específicas del Gestor.

d) SNMPv2

Desde la publicación original de SNMP, se han presentado varias propuestas protocolares para mejorar a SNMP. En 1992 se decidió reunir todas estas propuestas y producir una nueva norma: SNMPv2. Desafortunadamente SNMPv2 se tornó más complejo que el SNMP original; considerando que la descripción del protocolo de SNMP original requirió, por ejemplo, de sólo 35 páginas, la descripción de SNMPv2 requirió aproximadamente 250 páginas.

Los logros principales de SNMPv2 son el Rendimiento mejorado (ver b), 1)), una mejor Seguridad (ver b), 2))y la posibilidad de construir una jerarquía de Gestores (ver b), 3)).

1) Rendimiento

Como se explicó, el protocolo original de SNMP incluye una regla que establece que si la respuesta a una solicitud Get o GetNext, excediera el tamaño máximo de un paquete, ninguna información será retornada. Puesto que los Gestores no pueden determinar de antemano, el tamaño preciso de los paquetes de respuesta, ellos normalmente toman una suposición conservadora y solicitan por PDU sólo una cantidad pequeña. Para obtener toda la información, puede ser que los Gestores emitan un número grande de solicitudes consecutivas.

Para mejorar el Rendimiento, SNMPv2 ha introducido la PDU GetBulk. En contraste con Get y GetNext, la respuesta a GetBulk siempre retorna tanta información como le sea posible. Si la información solicitada excede el tamaño del máximo de un paquete UDP, la información será truncada y sólo una parte que encaje dentro del paquete es retornada.

2) Seguridad

El protocolo original SNMP no tenía ninguna característica de seguridad, salvo por un simple mecanismo que involucró el intercambio de contraseñas (passwords) (el término 'Community string' fue usado para denotar esta contraseña (password)).

Para resolver esta deficiencia, SNMPv2 introdujo un mecanismo de seguridad completo. Este mecanismo esta basado en el uso de "Parties" y 'Contexts'; dos conceptos que no pueden encontrarse en otras aproximaciones de gestión. Aunque los estándares de SNMPv2 incluyen definiciones de ambos conceptos, estas definiciones son dificiles entender.

Las "Parties" (Sesiones) tienen algo de parecido con las entidades protocolares. Normalmente múltiples "Parties" están activas en un solo subsistema SNMPv2, y varias de estas "Parties" se configurarán de diferentes maneras. Una "Party" puede, por ejemplo, configurarse de tal forma de que se prepare para comunicarse con cada una de las otras "Parties" que están en cada uno de los otros sistemas.

Otra "Party" puede configurarse para que sólo sea predispuesta para interactuar con una "Party" remota particular. En tal caso, el mecanismo de autenticación MD5 se usa para asegurar la autenticación de la otra "Party". Finalmente las "Parties" pueden configurarse de una forma en la que ellas sólo estén dispuestas para interactuar con "Parties" remotas particulares y además requieren que toda la información de gestión este encriptada de acuerdo al algoritmo DES.

Una representación gráfica de las "Parties" se proporciona en la Figura 2.30. En esta figura se han configurado tres "Parties" en el sistema Gestor (Pa1, Pa2 y Pa3) y tres "Parties" en el sistema Agente (Pb1, Pb2 y Pb3).

Para controlar el acceso a las varias partes de una MIB, SNMPv2 han introducido el concepto de contexto. Cada contexto se refiere a una parte específica de una MIB. En el ejemplo de la Figura 2.30, el contexto C1 y el contexto C2 se refieren a las dos áreas punteadas en la MIB.

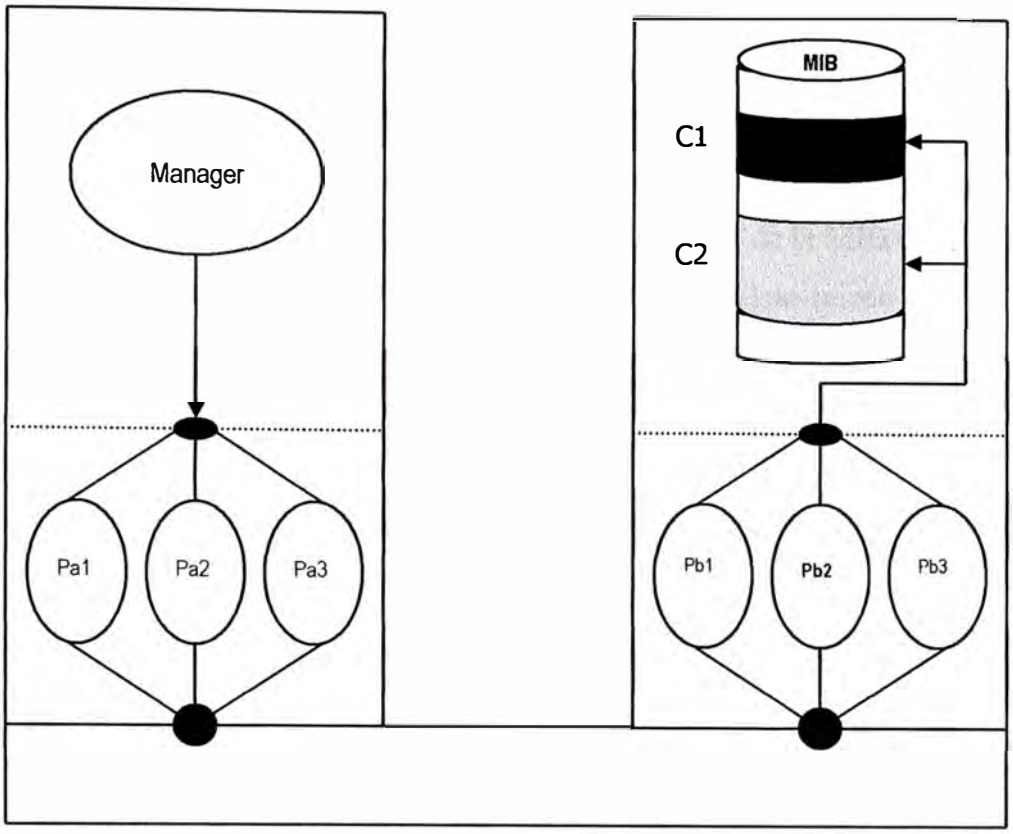


Figura 2.30 Las "Parties" y los Contextos

Los contextos pueden estar traslapados y pueden ser dinámicamente configurables, lo cual significa que los contextos pueden crearse, removerse o modificarse durante la fase operacional de la red. Los contextos diferentes pueden configurarse para diferentes sistemas.

Sesión ("Party") Remota	Sesión ("Party") Local	Contexto	Operación
Pa1	Pb1	C1	get
Pa2	Pb2	C1	get
Pa3	Pb3	C1	get + set
Pa3	Pb3	C2	get

Figura 2.31 El Ejemplo de una Lista de Control de Acceso (ACL)

Para determinar qué "Parties" están habilitadas para ejecutar operaciones sobre la MIB, SNMPv2 ha asociado con cada Agente una Lista de Control de Acceso (ACL). La Figura 2.31 muestra un ejemplo de tal lista. La primera fila indica que la "Party" Pa1 (en el sistema Gestor) puede realizar operaciones Get por medio de la "Party" Pb1 (en el sistema del Agente) en esa parte de la MIB que está identificada por el contexto C1. La tercera fila muestra que Pa3 lo puede hacer por medio de Pb3, para realizar operaciones Set en esta parte de la MIB.

3) Jerarquía de Gestión

La experiencia práctica con el protocolo original de SNMP ha mostrado que en muchos casos los Gestores son incapaces de gestionar más que unos pocos cientos de sistemas Agente. La causa para esta restricción está en la naturaleza de Polling de SNMP: el Gestor debe periódicamente realizar un sondeo a cada sistema bajo su control, lo cual toma tiempo. Para resolver este problema, SNMPv2 ha introducido la idea de los Gestores de nivel intermedio. El sondeo es ahora realizado a través de un número tal de Gestores de nivel intermedio que están bajo el control del Gestor de alto nivel.

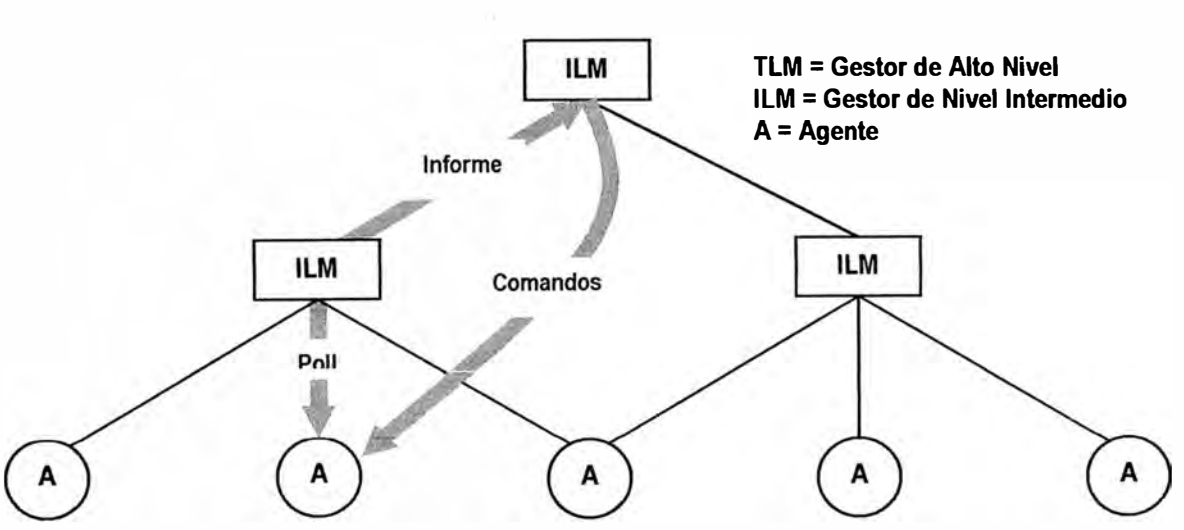


Figura 2.32 Los Gestores de Nivel Intermedio

La Figura 2.32 muestra un ejemplo. Antes de que los Gestores de nivel intermedio inicien el sondeo, el Gestor de alto nivel le dice a los Gestores de nivel intermedio cuales variables deben ser tomadas en sondeo en cuales agentes. Además, el Gestor de alto nivel le reporta a los Gestores de nivel intermedio de los eventos con los cuales él quiere ser informado. Después los Gestores de nivel intermedio son configurados, y ellos inician el sondeo. En caso de que un Gestor de nivel intermedio detecte en un agente particular un evento sobre el cual los Gestores de alto nivel quisieran ser informados, entonces se genera un informe especial PDU. Después de la recepción de esta PDU, el Gestor de alto nivel opera directamente sobre el agente que haya causado el evento.

e) MIB's

Para identificar todas las variables que puedan gestionarse, un gran número de Base de Información de Gestión (MIB) estándares ha sido desarrollado. Cercano a estos estándares, existe un estándar especial que define cómo describir variables de una MIB. Este estándar se denomina la Estructura de Información de Gestión (SMI). Por ejemplo, este define el subconjunto de ASN.1 de estructuras que pueden usarse para describir variables de gestión.

Para asegurar una única identificación de cada variable de gestión, SMI introduce el concepto de árbol de nombrado. Las hojas de este árbol representan la información de gestión actual. Un ejemplo (imaginario) de esto se muestra en la Figura 2.33; en esta figura el identificador del objeto de la dirección de red es root.1.1, el identificador del objeto del contador de colisión es root.2.2 y el identificador del "token holding timer" es root.3.4.

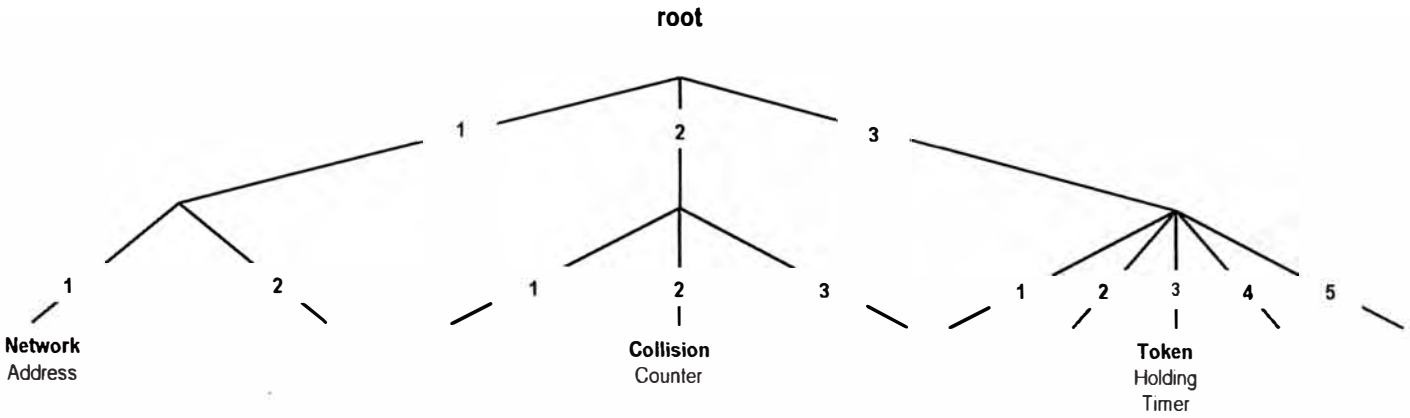


Figura 2.33 El Concepto del Árbol de Nombrado

La MIB-II es la más importante y probablemente mejor MIB conocida; contiene todas las variables para controlar la mayoría de los protocolos de Internet (ejemplo: IP, ICMP, UDP, TCP, EGP y SNMP). La estructura de esta MIB es simple: todas las variables de gestión que pertenecen al mismo protocolo son agrupadas (Figura 2.34). Dentro de un grupo de protocolos, hay estructuras adicionales que ayudan a entender las varias variables dentro de ese grupo.

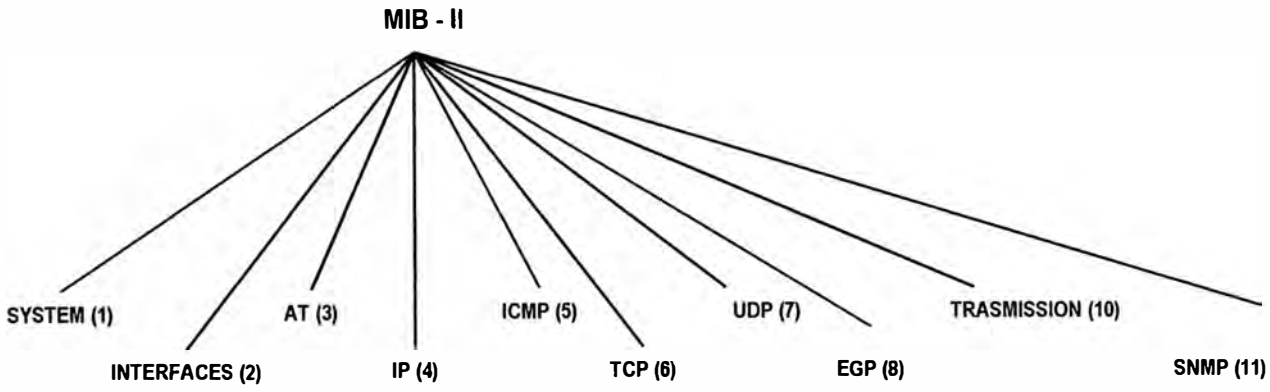


Figura 2.34 Los diferentes grupos de Protocolos de la MIB-II

Poco después de la definición de la MIB-II otros MIB's han aparecido; la Figura 2.35 muestra algunas de las estandarizadas.

Muy cercanas a estas MIB's estandarizadas, hay también un gran número de MIB's específicas de tipo empresarial. Todas estas MIB's en conjunto definen algo más de 20000 variables de gestión. Desafortunadamente no se tiene ninguna estructura desarrollada que sirva para explicar la relación entre estas MIB's; la única indicación del propósito de las MIB's es su nombre.

Título	**RFC**	**Fecha**
MIB-II	1213	March 1991
IEEE 802.5 Token Ring	1231	May 1991
Appletalk	1243	July 1991
OSPF version 2	1253	August 1991
Remote Network Monitoring	1271	November 1991
IP Forwarding Table MIB	1354	July 1992
RIP Version 2	1389	January 1993
DS1 and E1 Interface Types	1406	January 1993
DS3 and E3 Interface Types	1407	January 1993
X.25	1461	May 1993
Point to Point Protocol	1471-1474	June 1993
Bridges	1493	July 1993
FDDI	512	September 1993
Remote Network Monitoring - Token Ring	1513	September 1993
Host Resources	1514	September 1993
IEEE 802.3 Medium Attachment Units	1515	September 1993
IEEE 802.3 Repeater Devices	1516	September 1993
Source Routing Bridges	1525	September 1993
DECnet Phase IV Extensions	1559	December 1993

Network Services Monitoring	1565	January 1994
Mail Monitoring	1566	January 1994
X.500 Directory Monitoring	1567	January 1994
SNA APPN Node	1593	March 1994
SONET/SDH Interface	1595	March 1994
Frame Relay Service	1604	March 1994
Domain Name System	1611-1612	May 1994
Uninterrupted Power Supply	1628	May 1994
Ethernet - like Interface Types	1643	July 1994
Border Gateway Protocol	1657	July 1994
Character Stream Devices	1658	July 1994
RS-232-like Hardware Devices	1659	July 1994
Parallel-printer-like Hardware Devices	1660	July 1994
SNA NAU	1666	August 1994
SMDS - SIP Interface Type	1694	August 1994
ATM	1695	August 1994
Modem	1696	August 1994
Relational Database Management System	1697	August 1994

Figura 2.35 Algunas definiciones de MIB existentes

f) Análisis

La gestión Internet puede compararse con la gestión OSI. De hecho, la gestión Internet usa muchos de los conceptos que existen en OSI en el momento en que SNMP empezó (alrededor de 1988). En contraste con la gestión OSI, sin embargo, la gestión Internet usa sólo una pequeña parte de las funciones gestionadas para el intercambio de información de gestión. Los problemas con la gestión de fallas, es lo que por consiguiente probablemente ocurra.

1) La Arquitectura de la Gestión no ha sido Descrita

Ningún estándar se ha producido para definir la Arquitectura de Gestión Internet. Para conseguir una comprensión de los conceptos arquitectónicos detrás de la Gestión Internet, quien quiera entender tiene que derivar el significado de los diferentes conceptos de los Estándares del Protocolo. Aunque éste no puede ser un problema en el caso de la versión original de SNMP, es ciertamente un problema con SNMPv2. La experiencia ha mostrado que sin una buena comprensión de estos conceptos, es difícil implementar SNMPv2. Una recomendación para el IETF es por consiguiente desarrollar tal estándar.

Los conceptos que causan la mayoría de los problemas, son las "Parties" y los Contextos. Aunque la interpretación de estos conceptos dada (ver figura 2.30) puede ser suficiente para entender la mayoría de las partes de el estándar SNMPv2, ciertas partes de los estándares están basados en alguna otra interpretación. Un buen ejemplo de tal interpretación alternativa puede encontrarse en los estándares que definen cómo usar los Gestores de nivel intermedio. Según estos estándares, un contexto no sólo se refiere a la parte específica de una MIB, sino que también identifica a uno de los agentes que es controlado por el Gestor de nivel intermedio.

2) Demasiadas Variables de Gestión

Ahora que se han definido miles de variables de gestión, la falta de una buena estructura funcional para clasificar estas variables se ha convertido en un problema. Sin tal estructura, los Gestores se confrontarán con grandes listas de variables de gestión. Para determinar qué variables deben observarse y qué modificaciones deben hacerse, los Gestores deben entender el significado preciso de muchas variables.

En caso de que la gestión sea realizada por seres humanos, es improbable que hallan muchas personas con un conocimiento claro y suficiente. Como una consecuencia, puede esperarse que los Gestores necesitan mucho más tiempo antes de que ellos decidan qué hacer. La Gestión de Red puede convertirse en un factor que implique sólo consumo de tiempo, y por consiguiente sea una actividad costosa.

3) Las Funciones Específicas del Gestor aun no se han definido

Los estándares de Gestión de Internet explican cómo deben realizarse las operaciones de gestión individuales, tales como GET y SET. Actualmente ellos no especifican, sin embargo, la secuencia en la cual estas operaciones deben realizarse para resolver problemas de gestión particulares. Tales secuencias son parte de las 'Funciones Específicas del Gestor' (ver Figura); hasta ahora el IETF no ha definido tales funciones.

Ejemplo: Suponga que un Ruteador le sucede una avería. Las acciones deben ser iniciadas por la gestión para prevenir que los datos se pierdan. Estas acciones incluyen el cambio de las tablas de enrutamiento. Puesto que las redes consisten de miles de sistemas, la gestión debe decidir cuales tablas son para cambiar y cuales no. Por supuesto, la gestión también debe especificar los volúmenes o contenidos exactos de las tablas de enrutamiento modificadas. Los estándares de gestión Internet no describen ninguno de estas acciones. En cambio, la gestión Internet proporciona sólo una aproximación general para leer y modificar variables de gestión individuales.

La aproximación que se toma de Internet para gestionar redes es comparable a una aproximación en la cual los depuradores (debuggers) son usados para 'Gestionar' programas de computadora. Los depuradores (debuggers) ordinarios le permiten a los programadores ver y modificar las variables del programa. Un programa depurador no ayuda, sin embargo, a determinar cuales variables deben mirarse y cuales modificaciones deben hacerse. Tales decisiones deben ser tomadas por el programador; el debugger sólo ayuda a acceder a las variables.

Los Estándares de Gestión Internet definen 'Debuggers' distribuidos. Estos 'Debuggers' le permiten a los Gestores ver y modificar variables de gestión; ellos no dicen cuales variables deben verse y cuales modificaciones deben hacerse.

Las tales decisiones deben ser tomadas por las 'Funciones Específicas del Gestor' (ejemplo: el operador); Los Estándares de Gestión Internet sólo dicen cómo acceder a las variables de la gestión.

g) SNMPv3

En Septiembre de 1996, el IETF formo un Comité Asesor para analizar la competencia propuesta por algunas aproximaciones a la seguridad de SNMP. A comienzos de 1997, se produjo un análisis que describió a SNMPng (o SNMP next generation). SNMPng incluye las funcionalidades de SNMPv2 e incorpora características de seguridad sacadas de las aproximaciones propuestas. Con aún mas refinamiento y experiencia de implementación, SNMPng esta proyectado para convertirse en SNMPv3, los productos basados en este estándar están ya disponibles desde Abril de 1998.

SNMPv3 consiste de tres módulos, Módulo de Control y Procesamiento de Mensajes que maneja la creación de mensajes SNMP y análisis de funciones, y también determina si el proxy de manejo es requerido por algún mensaje SNMP. El Módulo de Procesamiento Local ejecuta los procesos de control de accesos para las variables de datos de enlace (variable binding data), el procesamiento de estos datos, y el procesamiento del Trap. El Módulo de Seguridad, que provee funciones de autenticación y encriptación, y chequea los horarios de ciertos mensajes SNMP.

La mayoría de las sustanciales mejoras que SNMPv3 ofrece sobre SNMPv1 y SNMPv2 son las características de seguridad que en este se han adicionado. Esto trata con una de las mayores preocupaciones que los usuarios de SNMP han expresado, y es la falta de una seguridad efectiva. Específicamente, los usuarios desean saber que sólo el personal autorizado es capaz de realizar las Funciones de Gestión de Red (ejemplo: habilitar/deshabilitar una línea), y que únicamente el personal autorizado sea capaz de leer la Información de Gestión de Red (ejemplo: el contenido de un archivo de configuración).

Las tres nuevas características de seguridad provistas por SNMPv3 son la Autenticación, Reserva (Secrecy) y Control de Acceso. La Autenticación permite a un Agente verificar que un comando que está entrando o introduciéndose, proviene desde un Gestor autorizado y que los contenidos del comando no ha sido alterado. Para lograr esto, cada Gestor y Agente que deseen comunicarse deben compartir una clave secreta (secret key). El Gestor usa esta clave para calcular el código de autenticación del mensaje, el cual es una función del mensaje para ser re-transmitido y añade el código para este mensaje. Cuando el Agente recibe el mensaje, éste usa el código nuevamente. Sí la versión del código del Agente señala que el valor añadido para el

mensaje entrante, entonces el Agente conoce que el mensaje puede solamente haber sido originado desde un Gestor autorizado, y que el mensaje no fue alterado durante su tránsito.

La facilidad de Reserva (Secrecy) permite a los Gestores y a los Agentes encriptar mensajes para prevenir indiscreciones por otras "Parties". De nuevo, un Gestor y un Agente comparten una clave secreta. En este caso, sí los dos son configurados para usar la facilidad de Reserva, todo el tráfico entre ellos es encriptado.

Finalmente, la facilidad del Control de Acceso hace posible configurar Agentes para proveer diferentes niveles de acceso a diferentes Gestores. El acceso puede estar limitado en términos de los comandos que el Agente vaya a aceptar desde un Gestor dado y también en términos de la porción de la MIB del Agente que un Gestor dado pueda acceder. La política de Control de Acceso que vaya a usar un Agente por cada Gestor debe ser preconfigurada y esencialmente debe consistir de una tabla que detalle los privilegios de acceso de cada un de lo Gestores que se hallen autorizados.

Con estas nuevas características de Seguridad, los Gestores de Red tienen un nivel más alto de comodidad en el uso de SNMPv3, particularmente en grandes instalaciones y/o en aquellas donde halla una población muy grande de usuarios.

CAPITULO III

PLANEAMIENTO DEL SISTEMA DE GESTIÓN DE RED DE CAMPUS

3.1 Análisis de Requerimientos de Gestión de una red de Campus

3.1.1 La red de campus

El campus Universitario, posee una extensión próxima a un kilómetro de longitud, en esta residen todas las facultades incluyendo las oficinas administrativas. Debido a la extensión del campus se contemplo la necesidad de un backbone enlazando nodos distribuidos estratégicamente para dar cobertura de acceso a la red a las zonas donde hay presencia humana comprometida con los objetivos de la organización. La figura 3.1 muestra el campus dividido en sectores, cada sector por lo general comprende una facultad, el cuadro 3.1 muestra la relación de sectores y las facultades respectivas.

TABLA 3.1 Lista de facultades y los sectores donde se ubican.

SECTORES	FACULTADES/DEPENDENCIAS
A	Ingeniería mecánica (FIM)
B	Pabellón Central (Oficinas Administrativas)
C	Ingeniería Química Manufacturera (FIQM)
D	Ingeniería Petrolera (FIP), Ingeniería Ambiental (FIA)
E	Teatro
F	Ingeniería Geológica Metalúrgica y Minera (FIGMM)
G	Ingeniería Civil (FIC)
H	Arquitectura Urbanismo y Arte (FAUA)
I	Ingeniería Geológica Metalúrgica y Minera (FIGMM)
J	Ingeniería Civil (FIC)
K	Hidráulica
M	Ingeniería Económica Estadística y Ciencias Sociales (FIECS)
N	Centro de Computo
Q	Ingeniería Eléctrica y Electrónica (FIEE)
R	Ciencias (FC)
S	Ingeniería Industrial y de Sistemas (FIIS)
T	Centro de Investigaciones Sísmicas y Mitigación de Desastres (CISMID)

a) El Backbone

El Backbone de la red esta compuesto por enlaces que salen del nodo principal ubicados en el pabellón central (B), hacia los nodos secundarios que se encuentran en la facultad de ingeniería civil, centro de computo, facultad de ingeniería electrónica en los sectores G, N y Q respectivamente; cada enlace esta compuesto por 12 pares de fibra óptica, 6 pares de fibra multimodo 62.5/125 y 6 pares de fibra monomodo 10/125. La cantidad de pares de fibra óptica en exceso se hace necesario para cubrir posibles ampliaciones o deterioro de algunos de los pares. La existencia de las fibras Monomodo sin conectorizar son en previsión de que la evolución tecnológica lo requiera en futuras actualizaciones de la red a velocidades más elevadas, que según las tendencias requieren de medios de transmisión de ancho de banda cada vez mayores como la fibra óptica monomodo.

La fibra óptica ha sido instalada a través de ducterias subterráneas, las líneas en verde en la figura 3.1a muestran el trayecto de estas ducterias, saliendo del nodo principal B, hacia cada uno de los nodos secundarios G, N y Q. Aunque la figura 3.1a muestra como si se tratara de un bus, en realidad desde el nodo B salen conexiones punto a punto hacia cada uno de los otros nodos. La tecnología usada para el transporte de datos a alta velocidad en el backbone es ATM operando a 155Mbps, en combinación con emulación LAN para hacer posible el transporte de datos proveniente de ethernet, tecnología usada para el acceso de los usuarios finales. La figura 3.1b muestra un diagrama lógico de interconexión de los diferentes nodos que componen la red de campus universitario.

CAMPUS UNIVERSITARIO

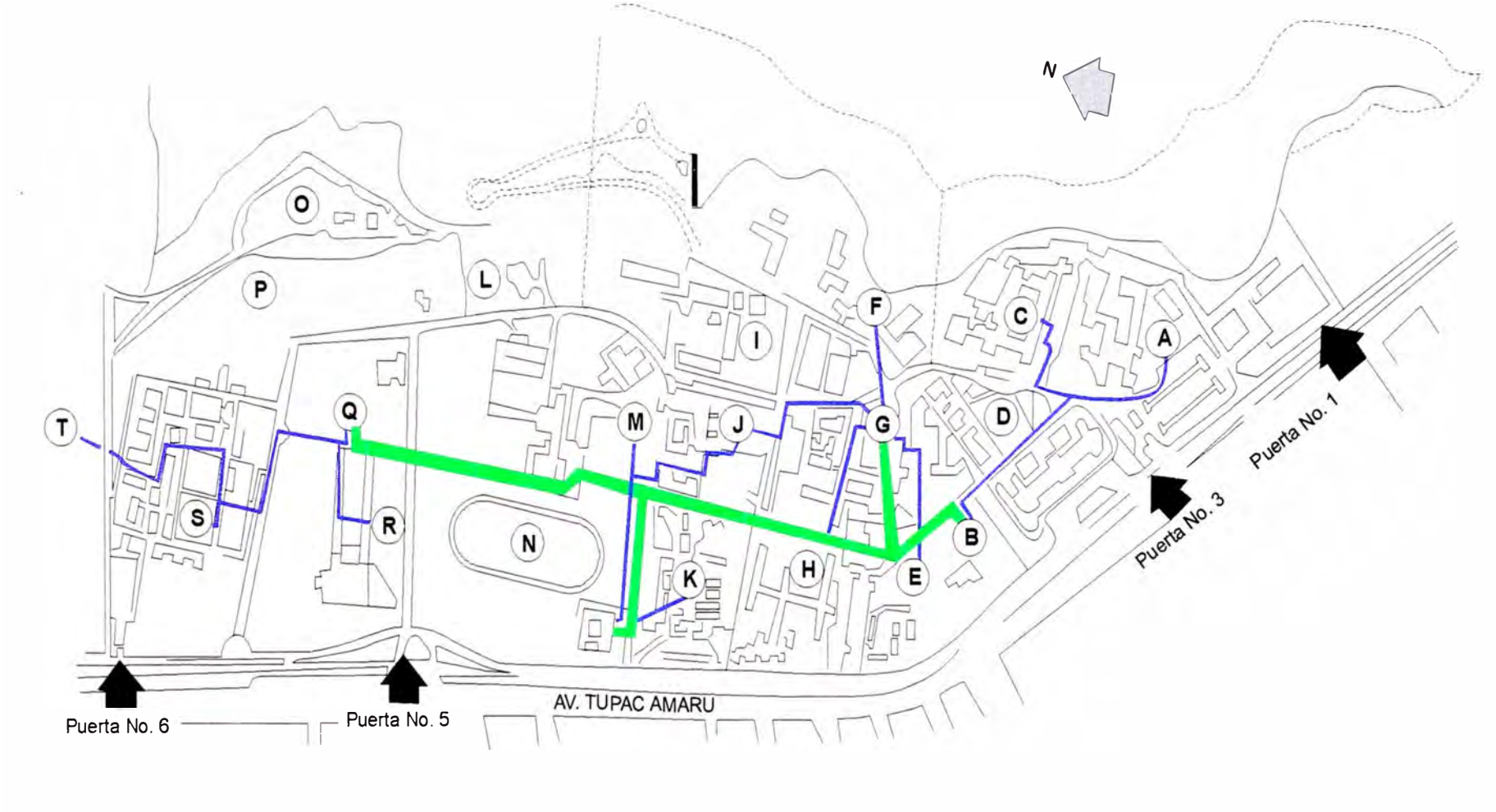


Figura 3.1a El campus Universitario dividido en Sectores

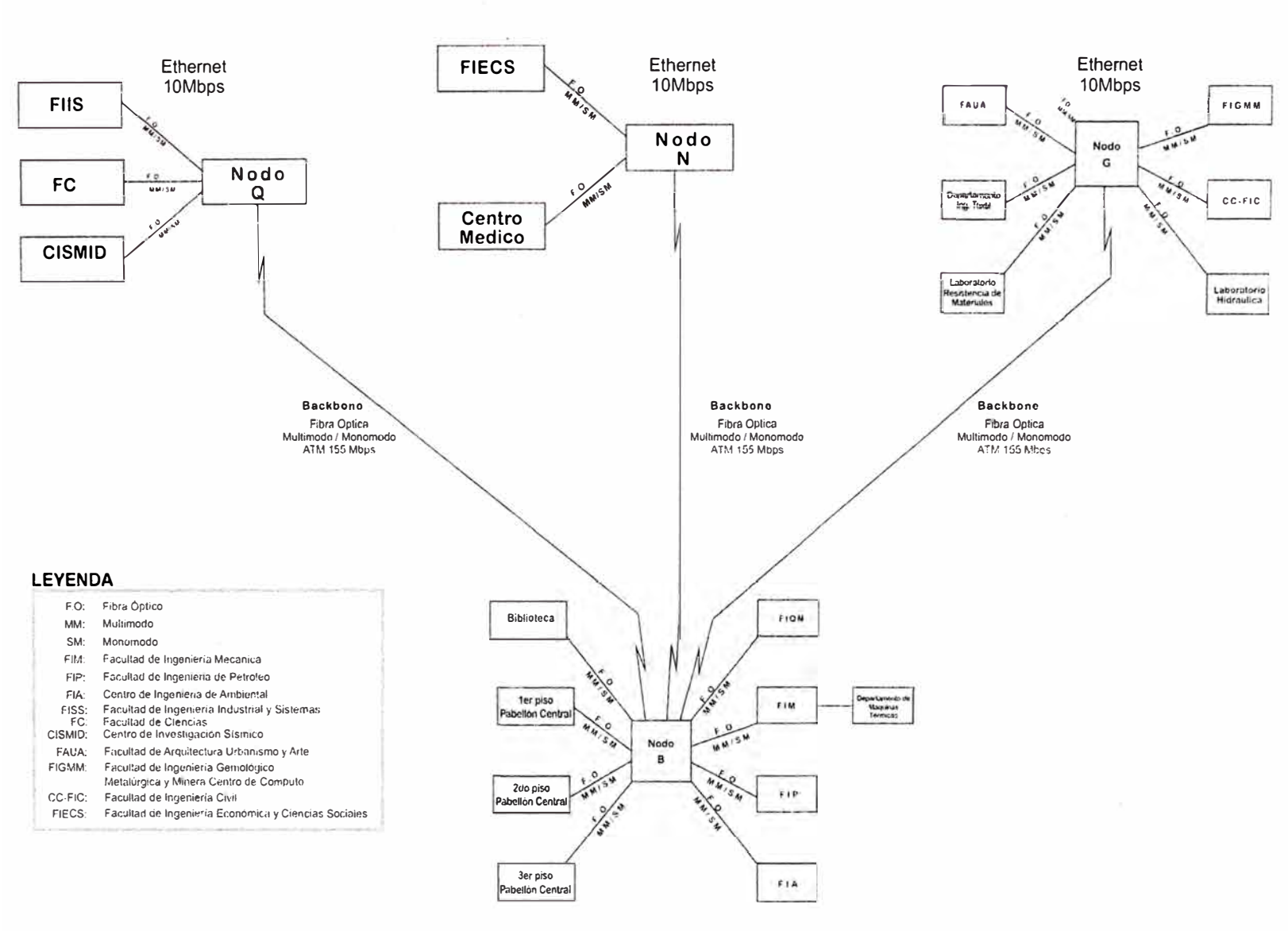


Figura 3.1 b Vista lógica de interconexión de los diferentes Nodos

La figura 3.2 muestra los enlaces entre los diferentes nodos secundarios con el nodo principal, existe una conexión punto a punto en cada caso, a partir de cada uno de los nodos secundarios y también del primario se extienden las conexiones hacia los nodos de acceso para la conexión de los dispositivos de usuarios finales.

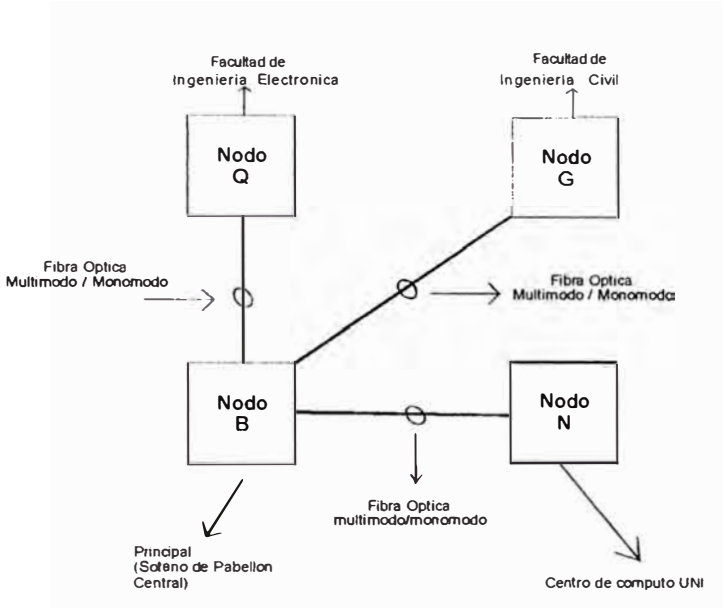


Figura 3.2 Interconexión de los nodos secundarios al nodo principal

En el grafico 3.1a estos enlaces son resaltados mediante las líneas de color verde.

b) Los enlaces de distribución

A partir de cada uno de los nodos primario y secundarios se extienden enlaces hacia los diferentes sectores de las diferentes facultades, las longitudes que deben cubrir cada uno de estos enlaces superan los 100 metros, no siendo factible el uso de cable par trenzado, siendo por tanto necesario la instalación de fibra óptica entre los nodos secundarios y los puntos de acceso, además la norma de cableado estructurado establece que toda conexión entre edificios debe hacerse usando fibra óptica, una de las razones para el uso de fibra óptica es evitar el problema de las diferencias de los potenciales a tierra de cada edificio, al no usarse señal eléctrica se produce un aislamiento perfecto.

Los enlaces interconectan dispositivos ethernet, en los nodos secundarios se encuentran los SWITCH´s (conmutadores) ethernet y en los puntos de acceso están los HUB´s,

para poder transmitir las señales de los switch´s a través de la fibra óptica se requiere una conversión del tipo de señal de eléctrico a óptico y viceversa, esto se realiza a través de los conversores de medios (media converter), en el lado receptor es necesario realizar la operación inversa, por tanto también es requerido conversores de medios (óptico/eléctrico).

1) El nodo B

El nodo principal (B) conecta a los nodos de acceso ubicados en las facultades de Ingeniería Química Manufacturera, Ingeniería Mecánica, Ingeniería de petróleo, Ingeniería ambiental, Biblioteca, pabellón central pisos 1, 2 y 3. Cada uno de los enlaces son de fibra óptica, estos constan de 3 pares de fibra multimodo y 3 pares de fibra monomodo. Ver figura 3.3.

En cada uno de los nodos de acceso reside un gabinete de comunicaciones que aloja un "patch panel" (panel de conexiones) de fibra óptica, HUB de 24 puertos que incorpora un EPIM (media converter), un "patch panel" de par trenzado y una fuente de alimentación ininterrumpida (UPS) . Desde estos puntos se distribuye la conexiones de usuario final en el área de trabajo mediante un cableado horizontal utilizando cable par trenzado. Cada uno de estos nodos de acceso por tanto constituyen un dominio de colisión.

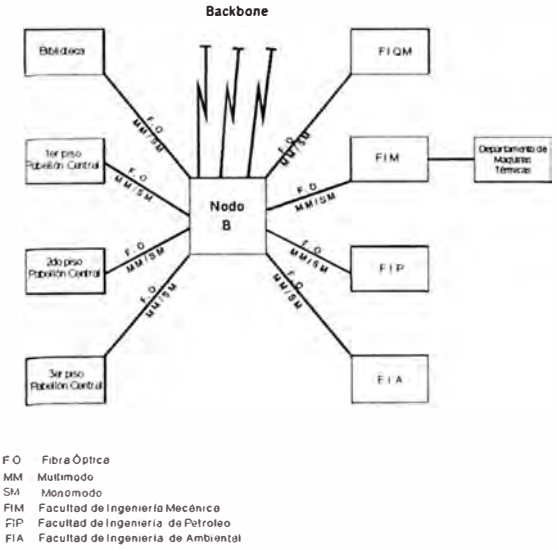


Figura 3.3 El nodo primario B y los puntos de acceso

2) El Nodo G

El nodo G conecta a las facultad de Arquitectura Urbanismo y Arte, facultad de Ingeniería Geológica y Minera, departamento de Ingeniería textil, laboratorio de resistencia de materiales, laboratorio de hidráulica, Centro de computo de la facultad de Ingeniería civil. Ver figura 3.4.

Cada uno de los enlaces son de fibra óptica, estos constan de 3 pares de fibra multimodo y 3 pares de fibra monomodo.

En cada uno de los nodos de acceso reside un gabinete de comunicaciones que aloja un "patch panel" (panel de conexiones) de fibra óptica, HUB de 24 puertos que incorpora un EPIM (media converter), un "patch panel" de par trenzado y una fuente de alimentación ininterrumpida (UPS) .

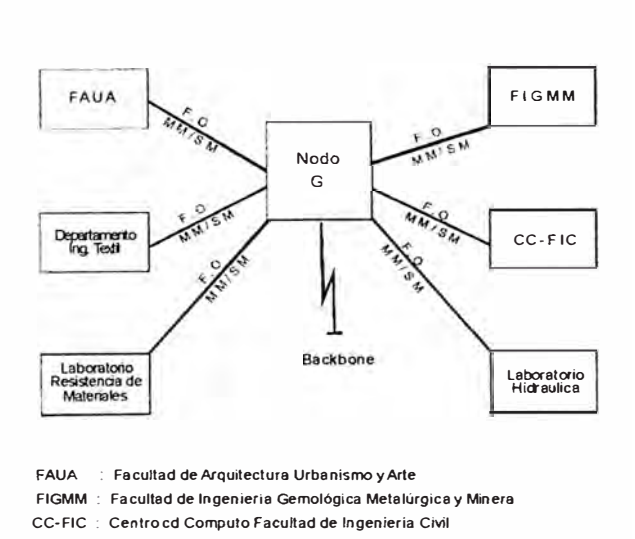


Figura 3.4 El nodo secundario G y los puntos de acceso.

3) El Nodo Q

El nodo Q ubicado en la facultad de ingeniería eléctrica y electrónica, conecta a las facultades de ingeniería industrial y de sistemas ubicado en el sector S, ciencias ubicado en el sector R y el CISMID ubicado en el sector T. Ver figura 3.5.

Cada uno de los enlaces son de fibra óptica, estos constan de 3 pares de fibra multimodo y 3 pares de fibra monomodo.

En cada uno de los nodos de acceso reside un gabinete de comunicaciones que aloja un "patch panel" (panel de conexiones) de fibra óptica, HUB de 24 puertos que incorpora un EPIM (media converter), un "patch panel" de par trenzado y una fuente de alimentación ininterrumpida (UPS).

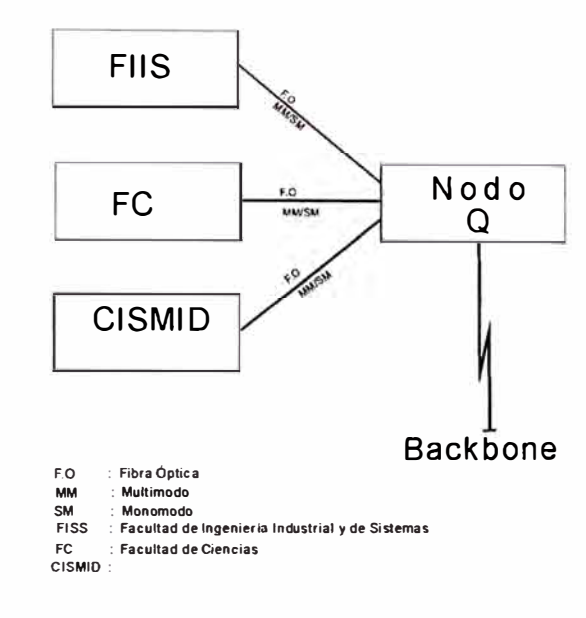


Figura 3.5 El nodo secundario Q y los puntos de acceso

4) El Nodo N

El nodo N ubicado en el centro de computo de la universidad conecta a los puntos de acceso ubicados en la Facultad de ingeniería económica estadística y de ciencias sociales ubicada en el sector M, el centro medico, laboratorio de hidráulica ubicada en el sector K y el laboratorio de topografía ubicado en el sector J. Ver figura 3.6.

Cada uno de los enlaces son de fibra óptica, estos constan de 3 pares de fibra multimodo y 3 pares de fibra monomodo.

En cada uno de los nodos de acceso reside un gabinete de comunicaciones que aloja un "patch panel" (panel de conexiones) de fibra óptica, HUB de 24 puertos que incorpora un EPIM (media converter), un "patch panel" de par trenzado y una fuente de alimentación ininterrumpida (UPS).

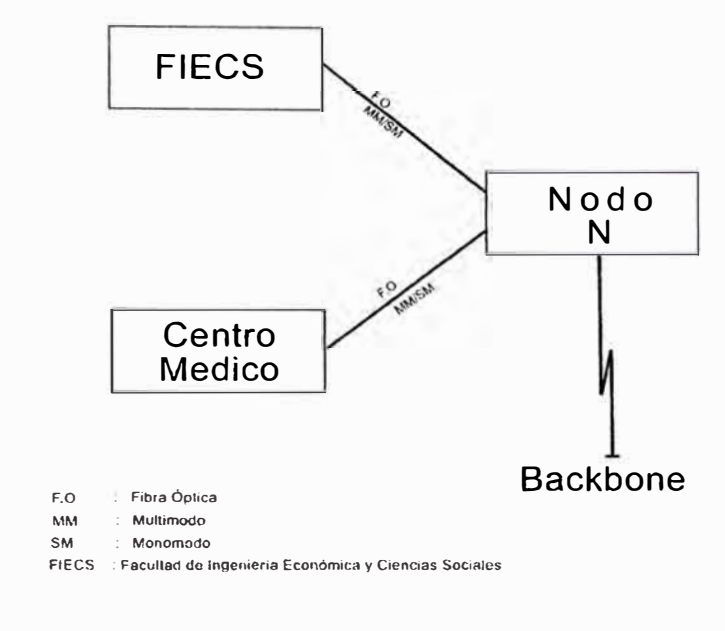


Figura 3.6 El nodo N y los puntos de acceso

c) Estructura de cada Nodo

El nodo principal cuenta con un chasis y módulo ambiental MMAC-PLUS que contiene los siguientes componentes: un switch ATM, un uplink implementando LANE (LAN Emulation), y un switch ethernet.

Los nodos secundarios cuentan con un chasis y modulo ambiental MMAC-Plus, conteniendo los siguientes componentes: un uplink implementando LANE y un switch ethernet. La figura 3.7 muestra una representación esquemática de cada uno de los nodos.

El switch ATM del nodo principal interconecta a los nodos secundarios a través de los uplinks. En cada nodo la comunicación entre los uplink y el switch ethernet se realiza mediante el backplane (bus interno proporcionado por el chasis).

La figura 3.7 muestra gráficamente una representación de la forma como se interconectan los nodos, para ser más preciso debemos añadir que las conexiones se realizan a través del panel de conexiones de fibra óptica en cada uno de los nodos.

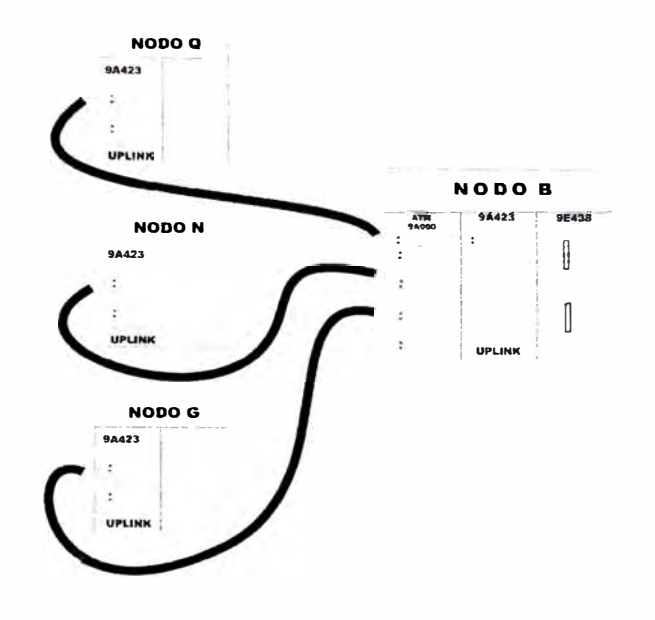


Figura 3.7 Composición de cada nodo y su interconexión.

De cada uno de los switchs ethernet, se conectan los HUB´s, convirtiéndose de este modo en los dispositivos de acceso a la red para los usuarios finales. De esta manera, los usuarios finales, desde sus PC´s acceden a los recursos de la red, que están en su mismo dominio de colisión (segmento), en el mismo switch ethernet o en un nodo remoto, en tal caso, las tramas serán entregados al switch, y este lo encaminará hacia el uplink, en este punto las tramas entregadas al uplink se convertirán en celdas ATM, el uplink es también responsable de la creación de los circuitos virtuales para el encaminamiento de las tramas, en forma de celdas ATM, el cual conmuta en base a los circuitos virtuales y los encamina hacia el uplink correspondiente, este a su vez ensambla las celdas obteniendo las tramas ethernet los cuales son pasados al switch ethernet, el cual se encarga de la entrega de la trama al usuario final. Una explicación con detalles técnicos más precisos es presentada en el capitulo siguiente. La figura 3.8 muestra una vista aproximada de la coexistencia ATM-ETHERNET.

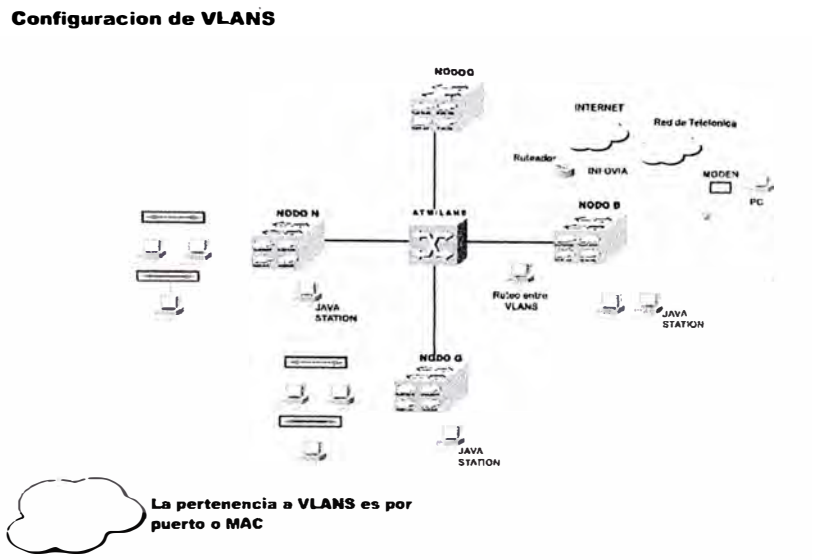


Figura 3.8 Diagrama lógico de Interconexión de ethernet sobre ATM

El Backbone (Nodo Principal B y Nodos Secundarios G, N y Q) están compuestos por:

1 SWITCH ATM (FORE 9A000), solo el nodo principal

3 UPLINK (FORE 9A423), uno en cada nodo

3 SWITCH ETHERNET (9E438), uno en cada nodo

El Switch ATM, realiza la conmutación de celdas y opera a 155 Mbps, esta compuesto por 8 puertos a cada uno de los 4 primeros puertos se conectan los UPLINK 9A423, cuya función es convertir las tramas ethernet recibidas a través del backplane del Chasis MMAC Plus en celdas ATM para que estos sean pasados a través del SWITCH 9A000, y viceversa en la dirección contraria recibirá las celdas y ensamblará las tramas.

El chasis MMAC-PLUS esta compuesto por un modulo ambiental que controla temperatura, humedad, niveles de consumo de voltaje y corriente, permite además un puerto de consola que permite el acceso a cada uno de los switch´s en forma de tarjetas insertos en el chasis, este también provee alimentación eléctrica redundante, para cada uno de los componentes del chasis.

En cada uno de los NODOS que componen el Backbone se encuentra instalado tarjetas 9E438, que son switchs Ethernet, a través de los cuales se conectan los SEHI´s, que son HUB´s ethernet, en los cuales se conectan las estaciones de trabajo de los usuarios finales, como se muestra en la figura 3.9

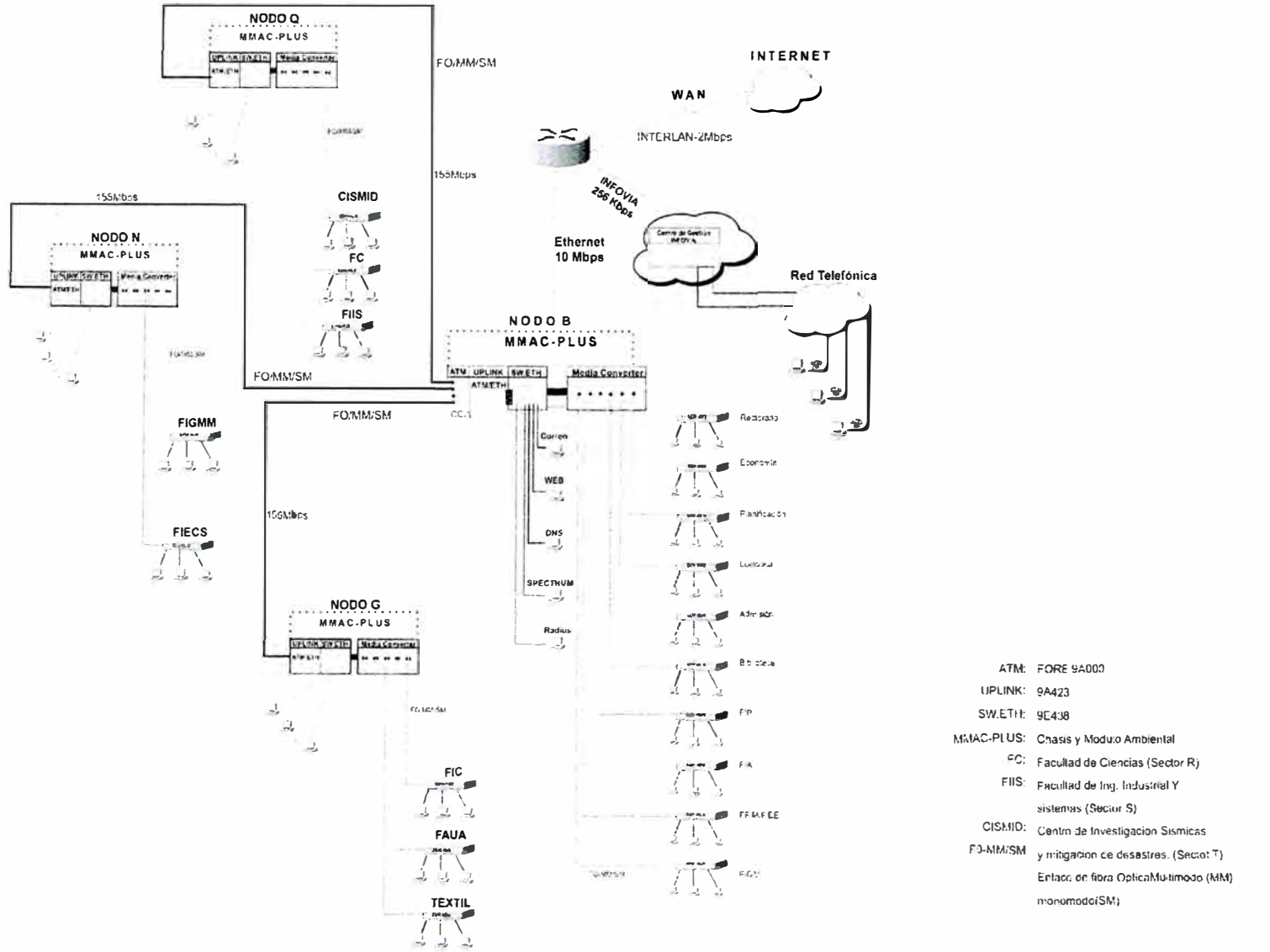


Figura 3.9 Representación de los componentes de cada nodo y su interconexión.

La comunicación hacia el exterior (INTERNET), se realiza mediante un enlace punto a punto de 2Mbps a través de la red Frame Relay, servicio brindado por Telefónica del Perú, también esta presente el servicio de acceso a INTERNET a través de la red telefónica conmutada, para proporcionar este servicio se cuenta con una línea Frame Relay de 256 Mbps. Para la implementación de este servicio es necesario realizar la autenticación de usuario, esto es realizado mediante el servidor Radius.

d) Modelo Lógico: Interconexión via ATM mediante LAN EMULATION

El ATM Forum planteó en 1995 una alternativa de interconexión de redes ATM con redes de datos más flexible que Classical IP, a costa de introducir más ineficiencias.

El modelo Classical IP permitió el inmediato despliegue de las redes ATM en internets IP, en particular, en la Internet. A pesar de que IP es el protocolo más extendido actualmente en las redes corporativas de datos, la especificidad del modelo Classical IP obligó al ATM Forum, que no estaba condicionado por una plataforma determinada, a buscar una alternativa multiprotocolo de interconexión de las redes ATM con redes de datos tradicionales para acelerar la introducción de la nueva tecnología en el mercado.

El ATM Forum publicó en enero de 1995 la especificación LAN *Emulation versión* 1.0. Se trató de una solución de interconexión válida para el transporte tanto de paquetes IP como IPX, NetBEUI, etc. Como primera aproximación al modelo LAN *Emulation* (LANE) de interconexión, se puede afirmar que, si *Classical* IP asimilaba la red ATM a una subred IP, en LANE la red ATM se asimila a una red LAN IEEE 802.3/5.

1) MODELO LANE DE INTERCONEXIÓN

En el modelo LANE de interconexión, es fundamental el concepto de Red de Área Local Emulada *(Emulated* LAN, ELAN). Una red ELAN es una red ATM que incorpora un protocolo denominado LANE, que es responsable de ofrecer a las estaciones conectadas a la red ELAN un servicio de las mismas características que una red LAN IEEE 802.3/.5.

Este concepto se ilustra en la Figura 3.10. En una red LAN tradicional, por ejemplo, una red Ethernet/802.3, las estaciones:

- se encuentran conectadas a un bus compartido,
- tienen asignadas unas direcciones únicas de 48 bits y
- emplean el mecanismo CSMA/CD de acceso al medio compartido.

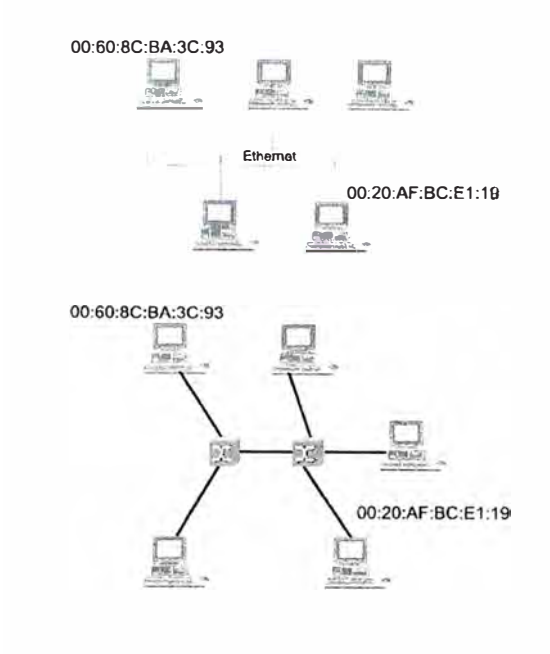


Figura 3.10 Red LAN emulada

Una red ELAN consiste en el mismo conjunto de estaciones:

- ahora conectadas a una red de conmutadores ATM,
- que tienen asignadas direcciones ATM de 20 bytes y
- que emplean los mecanismos de transporte y de señalización específicos de ATM para transmitir datos.

Sin embargo, al igual que las estaciones de la LAN tradicional:

- tienen también asignadas direcciones únicas de 48 bits y,
- además, a las aplicaciones residentes en las estaciones de la ELAN se les ofrece un servicio de red de las mismas características que en la red LAN tradicional.

El servicio que, a nivel MAC, ofrece una red LAN tradicional Ethernet/802.3 se caracteriza por:

- ser un servicio sin conexión;
- permitir la entrega unidestino *(unicast)* y multidestino *(multicast)* de datos;

- identificar los destinos mediante direcciones IEEE 802 de 48 bits.

Por otro lado, el servicio que, a nivel AAL, ofrece una red ATM con protocolo de adaptación AAL 5, se caracteriza por:

- ser un servicio orientado a la conexión;
- permitir únicamente la entrega unidestino de datos;
- identificar los destinos mediante direcciones ATM de 20 bytes.

Por tanto, el protocolo LANE, cuya función es emular el servicio MAC Ethernet/802.3 a partir del servicio AAL 5 de una red ATM, deberá adaptar las características del segundo para ofrecer a los protocolos de capa superior un servicio de las características del primero.

1. El protocolo LANE

Tres son las principales tareas que debe efectuar el protocolo LANE para cumplir su función:

- Definir un formato de trama LANE que permita ofrecer un servicio IEEE 802.3 a los protocolos de capa superior usuaria, tales como IP, IPX, etc.
- Definir un mecanismo de encapsulado de la trama LANE sobre red ATM para ser transportada entre dos estaciones de la misma ELAN.
- Definir un mecanismo de resolución de dirección MAC a ATM que permita averiguar la dirección ATM propia de una estación ELAN identificada por su dirección MAC.

El protocolo LANE emplea tramas de datos y de control para su operación. En la Figura 3.11 se muestra el formato de la trama LANE de datos. Los campos están dispuestos de arriba a abajo y de izquierda a derecha en filas de 4 bytes de longitud.

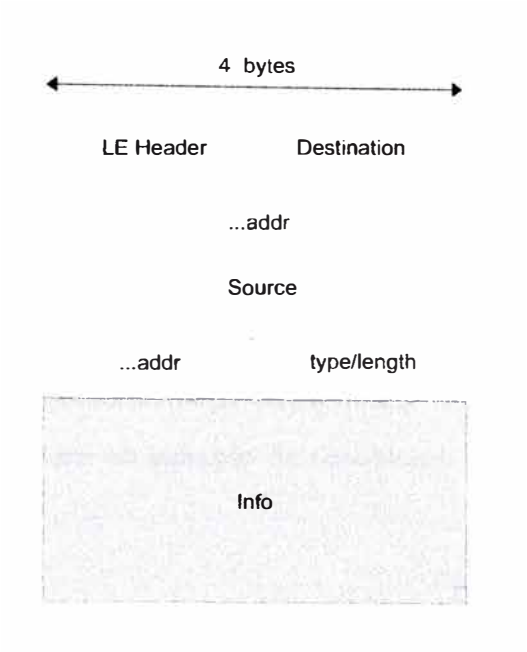


Figura 3.11 Formato de trama LANE

Obsérvese las siguientes características:

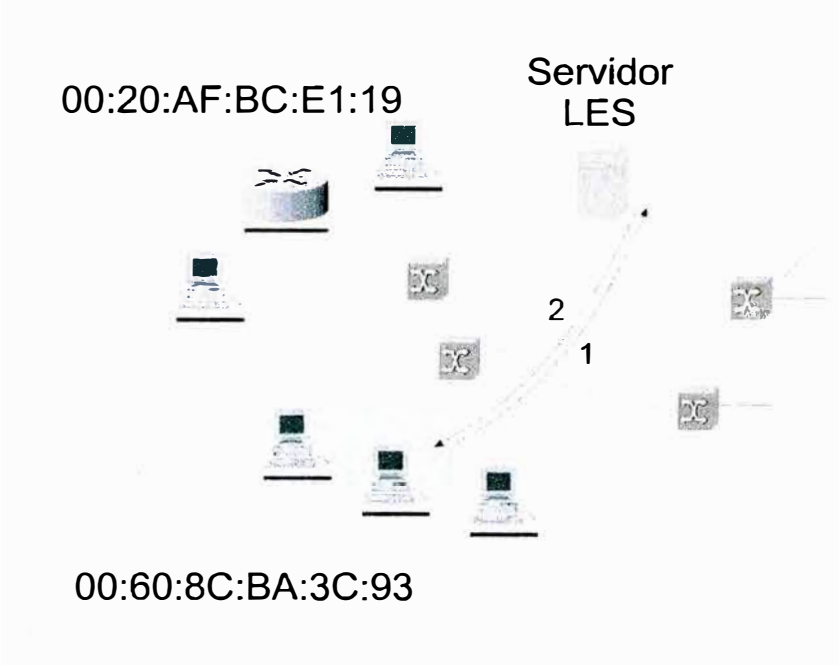
- Al igual que las tramas Ethernet e IEEE 802.3, la trama LANE dispone de un primer campo de dirección de destino y un segundo campo de dirección de origen, de 6 bytes cada uno.
- El campo *type/length* permite alternativamente emular el encapsulado Ethernet DIX, siendo campo *type*, y el encapsulado IEEE 802.3, siendo campo *length*.
- A diferencia de las tramas Ethernet e IEEE 802.3, la trama LANE no incluye un campo CRC de detección de errores de la transmisión. La razón es que esta tarea la realizará la subcapa CPCS-AAL5, por lo que se ha considerado redundante su inclusión.
- El campo LE *header*, específico de la trama LANE, desempeña funciones específicas del protocolo LANE, como la identificación del tipo de trama.

Para la transmisión de tramas LANE, tanto de datos como de control, se utiliza el servicio AAL 5 orientado a la conexión. Es decir, se establecen conexiones ATM conmutadas y, a través de ellas, se envían las tramas LANE. La identificación del protocolo LANE no se realiza mediante ningún mecanismo de encapsulado, sino mediante el identificador del punto de acceso al servicio.

Uno de los aspectos que el protocolo LANE debía adaptar para emular el servicio

IEEE 802.3 a partir del servicio AAL es la duplicidad de direcciones en una red ELAN. El envío de tramas a través del servicio IEEE 802.3 se realiza identificando el destino mediante direcciones IEEE 802, mientras que la transmisión efectiva de la trama se realiza a través de conexiones A TM conmutadas en las que el destino se identifica mediante direcciones A TM. Se plantea un problema de correspondencia de direcciones MAC y ATM que el ATM Forum ha resuelto mediante un mecanismo de resolución de direcciones.

En la Figura 3.12 se muestra un ejemplo de resolución de direcciones en una red ELAN.



Supóngase que la estación OO:60:8C:BA:3C:93 desea enviar una trama LANE de datos a la estación OO:20:AF:BC:El:19, para 10 cual necesita conocer la dirección A TM de esta última. El ATM Forum ha normalizado un protocolo denominado LE_ARP, que traslada el esquema de funcionamiento del protocolo ATMARP de ***Classical IP*** a la red ELAN.

Efectivamente, en cada ELAN hay un elemento denominado servidor LES (LAN *Emulation Server),* que conoce la correspondencia de todas las direcciones MAC a ATM de las estaciones de la ELAN. Cuando un miembro de la red ELAN, denominado genéricamente LEC (LAN *Emulation Client),* desea resolver una

dirección MAC, le envía una petición de resolución, en forma de trama LANE de control LE_ARP_REQUEST -paso designado por el dígito 1-. El servidor LES contesta a la petición con la dirección A TM requerida, en forma de trama LANE de control LE_ARP_RESPONSE -paso designado por el dígito 2-.

Para que el servidor LES tenga conocimiento de los pares MAC-ATM de las estaciones de la ELAN, se ha establecido un procedimiento de registro de direcciones. Durante la inicialización de cada cliente LEC, éste debe establecer una conexión A TM con su servidor LES, a través de ella y mediante las tramas LANE de control adecuadas, registra sus direcciones MAC y A TM. Esta conexión se denomina *control direct* VCC, y es punto a punto. Esta conexión es la utilizada, además, durante el procedimiento de resolución LE_ARP, para el envío de las tramas LE_ARP_REQUEST y LE ARP RESPONSE. Evidentemente, la dirección ATM del servidor LES debe ser conocida por todos los clientes LEC de la ELAN. La configuración de este parámetro es, como se verá más adelante, automática. Finalmente, se establece que los pares MAC-ATM que obtienen los clientes LEC caduquen a los 5 minutos.

Nótese cómo el procedimiento LE_ARP normalizado por el ATM Forum es análogo al procedimiento ATMARP normalizado por el IETF. En la tabla 3.2 se alinean los términos equivalentes entre LE_ARP y ATMARP:

Tabla 3.2 Equivalencia LE_ARP y ATMARP

	LE_ARP	ATMARP
Red Lógica	**ELAN**	LIS
Servidor de direcciones	LES	Servidor **ATMARP**
Dirección a Resolver	Dirección **MAC**	Dirección IP

ii. Comunicación *unicast* en LANE

Una vez especificados los procedimientos de encapsulado de trama LANE y de resolución de direcciones MAC, se puede especificar el procedimiento de comunicación unidestino entre estaciones de una ELAN, como el caso mostrado en la Figura 3.13

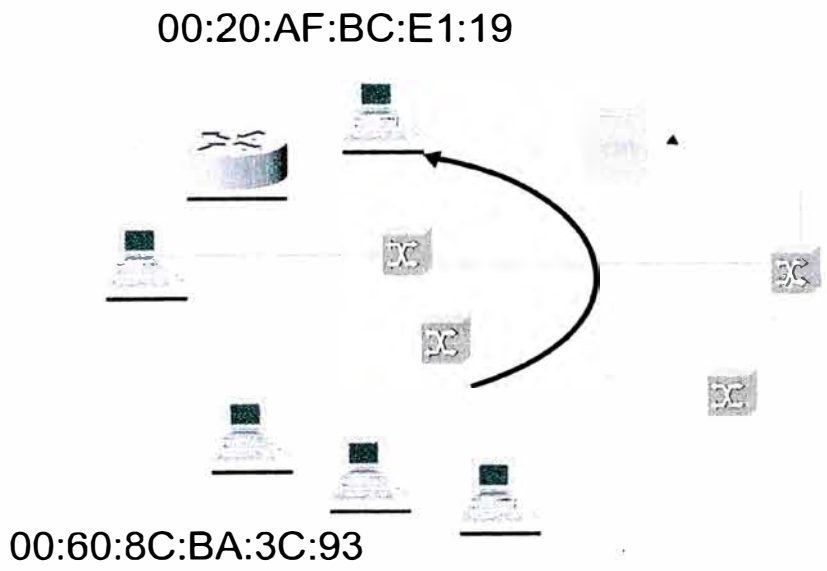


Figura 3.13 Funcionamiento LAN Emulation

En el ejemplo de la figura, para que la estación OO:60:8C:BA:3C:93 pueda enviar una trama LANE de datos a la estación 00:20:AF:BC:EI:19, son necesarios los siguientes pasos:

- La estación debe obtener la dirección ATM de OO:20:AF:BC:EI:19, mediante el protocolo LE_ARP.
- Deberá establecer una conexión A TM con el destino, utilizando los procedimientos de señalización UNI 3.1/4.0. Esta conexión ATM se denomina *data direct* VCC. .
- Debe, finalmente, enviar la trama LANE a través de la conexión *data direct* VCC.

iii. Comunicación *multicast* en LANE

La tercera característica que debe ser emulada en una red ELAN es, como se apuntó anteriormente, la capacidad de entregar datos a un grupo de destinatarios determinados.

En efecto, las redes LAN tradicionales permiten el envío de tramas con destino a un grupo determinado. Esta alternativa, denominada envío multidestino o simplemente *multicast,* es posible gracias, amén de la existencia de un medio fisico compartido, al esquema de direccionamiento IEEE 802, que reserva el bit menos significativo del primer byte para indicar si se trata de una dirección de grupo o individual -recuérdese el bit G/I-. Existe una dirección de grupo predefinida, que incluye a todas las estaciones conectadas a la red: se trata de la dirección de difusión o *broadcast.*

Existen dos posibilidades de conectividad que permiten las redes ATM: las conexiones punto a punto bidireccionales y las conexiones punto a multipunto unidireccionales. Este último caso es útil, como se verá a continuación, para conseguir difusión en una red ELAN, pero no es asimilable a la capacidad *multicast* de una red LAN tradicional. Nótese que una conexi6n punto a multipunto únicamente permite el flujo de datos desde una estación -la que se constituye en nodo raíz- hacia el resto. En cambio, cuando se habla de *multicast,* o más propiamente de un grupo *multicast,* se hace referencia a la posibilidad de enviar flujos de datos concurrentemente entre todos las estaciones incluidas en el mismo.

En LAN *Emulation,* se consigue emular la capacidad *multicast* mediante un elemento denominado servidor BUS *(Broadcast and Unknown Server),* que se

encarga de recibir las tramas LANE multidestino para reenviarlas al grupo correspondiente de estaciones.

Como se muestra en la Figura 3.14, en cada ELAN existe un servidor BUS, de igual manera que existía un servidor LES en cada ELAN.

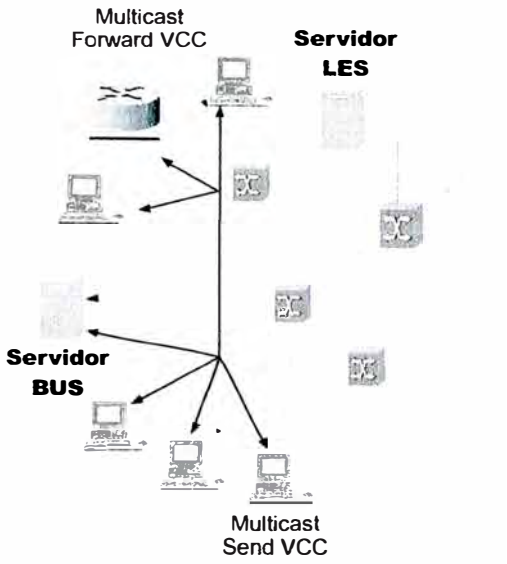


Figura 3.14 Comunicación multicast en LAN Emulation

Cuando un cliente LEC desea enviar una trama LANE a un grupo *multicast* de estaciones de su misma red ELAN, inserta la dirección de grupo correspondiente en la trama LANE y la envía al servidor BUS de su red ELAN. Para ello es necesario cumplir dos tareas previas:

- Averiguar la dirección ATM del servidor BUS. Para ello, el cliente LEC deberá resolver la dirección de grupo mediante el protocolo LE_ARP; es decir, el servidor LES de la red ELAN es el encargado de proporcionar tal dirección, siguiendo el procedimiento estándar de resolución de direcciones que se estudió para la comunicación *unicast.*
- Establecer una conexión ATM con el servidor BUS. Se trata de una conexión punto a punto bidireccional cuyo establecimiento inicia el cliente LEC. Esta conexión se denomina *multicast send* VCC.

Una vez recibida, por parte del servidor BUS, la trama LANE *multicast,* éste la entregará a los miembros del grupo *multicast* indicado por la dirección de grupo. Para ello, el servidor BUS mantiene una conexión punto a multipunto por cada

grupo *multicast*. El servidor BUS es el nodo raíz de esta conexión ATM, mientras que cada miembro del grupo *multicast* se constituye en hoja. El servidor BUS, por tanto, es el encargado de incorporar a los miembros del grupo. Esta conexión se denomina *multicast forward* VCC.

iv. Configuración ELAN

Se ha mencionado anteriormente que cada cliente LEC de una red ELAN debe conocer la dirección ATM del servidor LES de su red ELAN. De este modo, el cliente LEC sabe a quien dirigirse para resolver la dirección MAC de otro cliente LEC, o bien para conocer la dirección ATM del servidor BUS de la red ELAN. En el caso de *Classical* **IP,** era asimismo necesario que los miembros de una subred LIS conociesen la dirección ATM del servidor ATMARP de la LIS.

La necesidad de configurar manualmente la dirección A TM del servidor LES en cada una de las estaciones que implementen LANE en una red ATM es indeseable y, además, se trata de un procedimiento propenso a errores. Por añadidura, la pertenencia de una estación LANE a una determinada red ELAN de entre las configuradas en una red ATM es, en principio, una característica dinámica de la estación, lo que añade complejidad a la administración de la red.

Por las razones anteriores, el ATM Forum incluyó en la especificación LAN *Emulation* un procedimiento de configuración automático. Para ello, en cada red ATM que implemente LANE debe existir un servidor denominado LECS (LE *Configuration Server),* que será único independientemente del número de redes ELAN configuradas en la red ATM. La dirección ATM del servidor LECS debe ser conocida por todos los clientes LEC de la red ATM. Con estas premisas, durante la inicialización de un cliente LEC, éste solicita al servidor LECS que le proporcione la dirección ATM del servidor LES del que se servirá a partir de ese momento. El servidor LECS tiene atribuida de este modo la función de asignar cuál es la red ELAN a la que queda asignado cada cliente LEC de una red ATM.

Gracias al procedimiento descrito de asignación de ELAN mediante el servidor LECS, el administrador de la red puede configurar dinámicamente a qué ELAN pertenece cada estación. Esta tarea se simplifica al mantener una única base de datos residente en el servidor LECS.

2) COMUNICACIÓN FUERA DE ELAN

Una red ELAN, a diferencia de las redes LAN tradicionales, no viene limitada en su extensión por su propia tecnología. En efecto, la red ATM, que es la tecnología que subyace a la red ELAN, no impone límite a la extensión geográfica ni al número de estaciones conectadas. No" obstante, desde el punto de vista del administrador de la red corporativa, es conveniente limitar el número de estaciones conectadas a una misma ELAN. Piénsese en que una ELAN puede soportar un grupo de trabajo o un departamento de una empresa. Se impone, de igual modo que ocurría en el caso de las redes LAN tradicionales, determinar mecanismos para comunicar las estaciones de una ELAN con estaciones no pertenecientes a las mismas.

Se abordan a continuación dos aproximaciones para la comunicación fuera de la red ELAN. Ambas se basan en la utilización de unos u otros dispositivos de interconexión de redes. En efecto, en primer lugar, se estudiará la comunicación de una ELAN con el exterior mediante ruteadores IP; a continuación, se estudiará cómo posibilitar la misma comunicación mediante puentes IEEE 802.1d.

i. Comunicación mediante ruteadores IP

Una red ELAN, en cuanto que ofrece un servicio de idénticas características que una red LAN tradicional IEEE 802, puede ser interconectada con otras redes de la misma o de distinta tecnología si se adopta la solución de interconexión mediante ruteadores IP.

Cuando se interconecta una ELAN mediante IP hay que tener presente las siguientes consideraciones. En primer lugar, el ruteador IP no es consciente de la presencia de ATM, sino que presupone la existencia de una LAN IEEE 802. Por tanto, los mecanismos de encapsulado y de resolución de direcciones diseñados para este tipo de redes son los aplicables para el caso que nos ocupa. En segundo" lugar, la comunicación fuera de una ELAN a través de un ruteador no puede iniciada el protocolo LANE, sino el protocolo de interconexión en la estación de origen, esto es, el protocolo IP. En tercer lugar, al emplear IP, la red ELAN es tratada como una subred. Por tanto, deberá tener asignado un *netid.*

Con el fin de comprender el funcionamiento del protocolo IP cuando interconecta una red ELAN, se muestra un ejemplo en la Figura 3.15, Figura 3.16 y Figura 3.17. Se ha tomado la red ELAN de la Figura 3.13 y se ha asignado direcciones MAC e IP a los elementos relevantes en el ejemplo. En éste, la estación 158.42.2.16 desea enviar un datagrama con destino fuera de su ELAN, para lo cual debe entregárselo al ruteador 158.42.2.14.

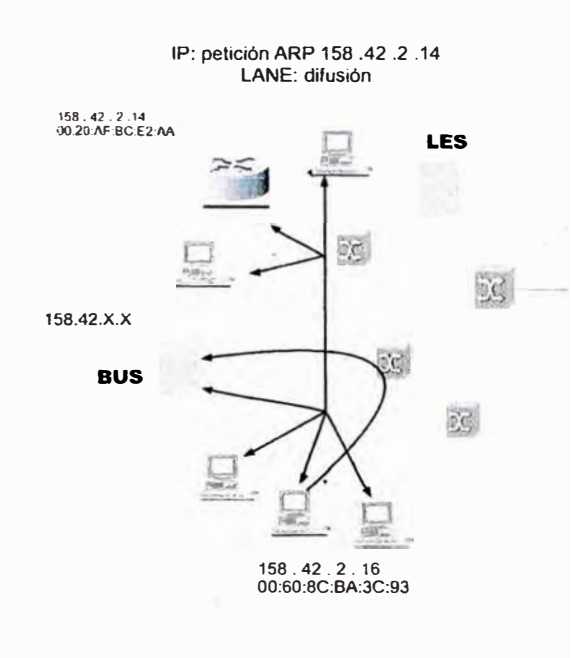


Figura 3.15 Ejemplo de funcionamiento IP sobre LANE (1)

El primer paso que se da para efectuar la entrega deseada del datagrama IP al ruteador 158.42.2.14 es resolver la dirección IP del ruteador. Para ello, se empleará el protocolo ARP. Tal como se indica en la Figura 3.15, la estación 158.42.2.16 envía un mensaje de petición ARP, que se difundirá a través de la red ELAN. Esta difusión la efectúa el protocolo LANE, el cual encapsulará el mensaje en una trama LANE de difusión y la enviará al servidor BUS de su ELAN. El servidor BUS, a su vez, la difundirá a todos los clientes LEC de su ELAN, a través de la conexión punto a multipunto correspondiente, con lo cual la trama -y, por tanto, el mensaje ARP- llegará al ruteador 158.42.2.14.

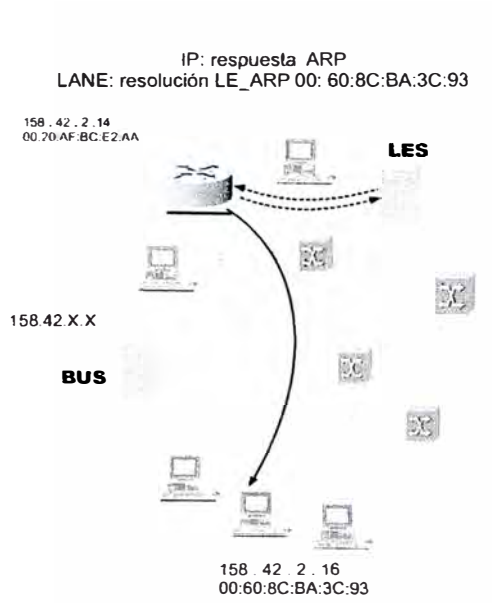


Figura 3.16 Ejemplo de funcionamiento IP sobre LANE (2)

Como se indica en la Figura 3.16, el ruteador, una vez recibe el mensaje de petición ARP, deberá devolver a la estación 158.42.2.16 un mensaje de respuesta ARP, en el que proporcionará su dirección fisica, es decir, la dirección MAC OO:20:AF:BC:E2:AA. Para ello, deberá entregar el mensaje ARP al protocolo LANE, quien lo encapsulará en una trama LANE de datos con dirección MAC de destino OO:60:8C:BA:3C:93. Para hacer llegar esta trama a la estación de destino, el protocolo LANE hace uso del protocolo de resolución LE_ARP, mediante el que solicita al servidor LES de su red ELAN cuál es la dirección ATM correspondiente a la dirección MAC OO:60:8C:BA:3C:93 -ver flechas en trazo discontinuo-. Una vez obtenida la dirección ATM, el ruteador enviará la trama a través de una conexión ATM punto a punto -ver flechas en trazo continuo-.

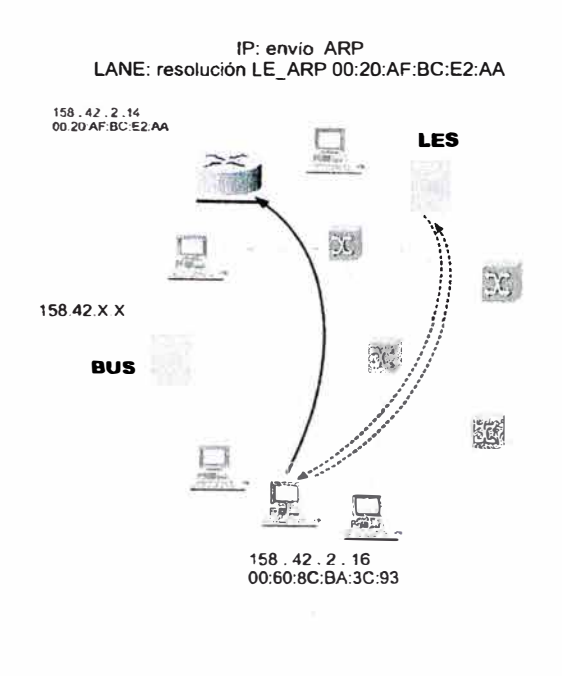


Figura 3.17 Ejemplo de funcionamiento IP sobre LANE (3)

El segundo paso, una vez que la estación 158.42.2.16 ha obtenido la dirección MAC del ruteador 158.42.2.14, es encapsular el datagrama y enviarlo a través de la red ELAN. Para ello, tal como se indica en la Figura 3.17, el datagrama IP se encapsula en una trama LANE de datos, cuya dirección de destino es 00:20:AF:BC:E2:AA. Para enviar la trama LANE, la estación 00:60:8C:BA:3C:9 deberá averiguar, haciendo uso del protocolo LE_ARP, la dirección ATM correspondiente a la dirección MAC 00:60:8C:BA:3C:93; en este proceso interviene el servidor LES de la red ELAN. Una vez obtenida la dirección ATM, se establece una conexión ATM punto a punto con el ruteador y se transmite la trama LANE.

Nótese cómo el protocolo LANE garantiza la transparencia requerida por el protocolo IP para operar sobre una red ELAN de manera idéntica a como lo haría sobre una red LAN IEEE 802.3.

ii. Comunicación mediante puentes

Para las redes IEEE 802.3 existe una alternativa de interconexión a la utilización del protocolo IP, tal y como se estudió en el capítulo 4. Tal alternativa consistía en la utilización de puentes transparentes, de acuerdo con la especificación IEEE 802.1d. Pues bien, las redes ELAN pueden interconectarse con otras redes IEEE

802.3 o con otras redes ELAN mediante puentes transparentes.

La interconexión de una red ELAN con una red LAN tradicional mediante un puente transparente es una alternativa muy apreciada por los administradores de redes corporativas. La pila de protocolos necesaria para conseguir la interconexión se muestra en la Figura 3.18.

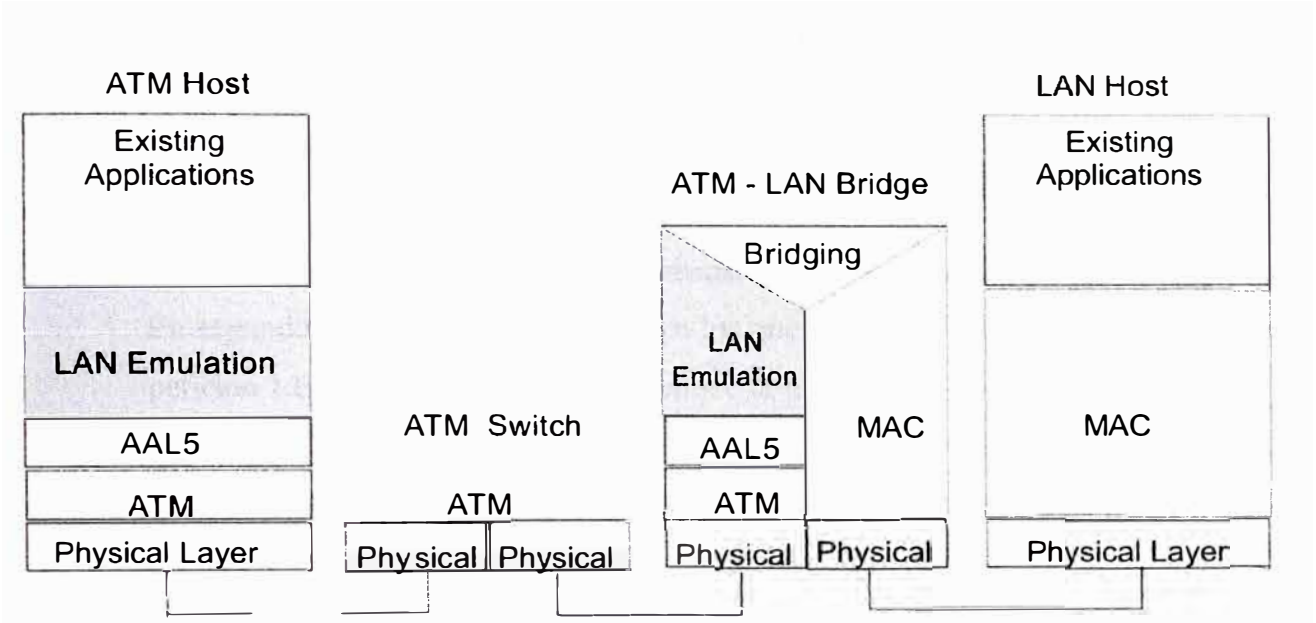


Figura 3.18 Interconexión de ELAN mediante puentes

Nótese cómo se consigue transparencia de protocolos a varios niveles. En primer lugar, la estación conectada a la red LAN tradicional no es consciente de la existencia de otras redes LAN, gracias a la operación del puente transparente. En segundo lugar, el puente transparente no es consciente de la existencia de una red A TM, gracias a la operación del protocolo LANE. Y en tercer lugar, el protocolo LANE no es consciente de la existencia de otras redes LAN, sean emuladas o no, gracias a la operación del puente transparente.

A pesar de la pretendida transparencia que se consigue con el puente IEEE 802.1d, existe una situación en la operación del protocolo LANE que requiere una consideración excepcional. Si una estación de la red ELAN desea enviar una trama a una estación de la red LAN tradicional, el protocolo LE_ARP deberá devolver la dirección ATM, no de la estación -dado que no la tiene-, sino del puente a través del cual es accesible.

Para tener en cuenta esta situación, se han previsto algunas modificaciones del

protocolo LE_ARP. En primer lugar, cada puente debe registrar en el servidor LES de la red ELAN a la que pertenece, la dirección A TM asociada a su dirección MAC, así como a todas las direcciones MAC de estaciones conectadas a redes LAN tradicionales a las que tenga alcance. Evidentemente no es factible registrar todas las estaciones LAN, por dos razones: en primer lugar, porque obligaría a mantener una tabla de resoluciones de gran tamaño; en segundo lugar, porque el puente desconoce en un momento dado la totalidad de las estaciones LAN a las que puede alcanzar, debido a que emplea el procedimiento de aprendizaje hacia atrás para rellenar su tabla caché de encaminamiento. Es por ello que se deja a criterio del administrador de la red la decisión de cuántas y cuáles registrar.

En segundo lugar, en aquellos casos en los que el servidor LES, cuando recibe una petición LE_ARP_REQUEST, no conoce la dirección ATM solicitada, reenvía la petición a todos los clientes LEC de la red ELAN. Con este propósito, el servidor LES mantiene una conexión punto a multipunto, denominada *control distribute* VCC, de la que es el nodo raíz. Esta posibilidad está prevista para el caso descrito en el párrafo anterior, pues de otro modo, todas las estaciones de la LAN tradicional deberán estar registradas en su servidor LES.

iii. Conclusión

Para configurar una ELAN en un switch FORE-9A000 se debe seguir tres pasos:

- Configurar un archivo de base de datos de configuración LECS
- Iniciar los servicios de LAN Emulation (LECS, LES, y BUS)
- Iniciar el LEC(s) y unir una ELAN.

Del mismo modo será necesario configurar los uplink 9A423, aquí también será necesario crear las ELAN´s.

Como se puede observar la puesta en operación desde cero de una LAN Emulada sobre ATM, demanda la realización de un trabajo complejo, totalmente contraria a la filosofía seguida por ethernet.

La configuración exitosa dará como resultado la operación de la red bajo LAN Emulation, según como se muestra en la figura 3.9.

3.2 Modelo de negocio

La red de campus de una entidad académica esta orientada a brindar el apoyo a las funciones administrativas y académicas.

Como soporte de las funciones administrativas tales como: logística, economía, personal, ORCE.

Como soporte a las actividades académicas tales como: Biblioteca, acceso a servicios a través de Internet (buscadores, bibliotecas virtuales, universidades virtuales, redes colaborativas, correo electrónico, etc.), realización de cursos a distancia soportados por TIC´s.

ORCE es una dependencia de la Universidad, dedicada a la administración de los records academicos de los estudiantes. Administra el estatus de los estudiantes, la información que posee es muy importante para llevar a cabo actividades tan importantes como la matrícula estudiantil. Cada una de las facultades a través de sus oficinas de registros academicos locales requiere conexión permanente a la base de datos ORCE. La figura 3.19 nos muestra un diagrama lógico de los elementos componentes de ORCE.

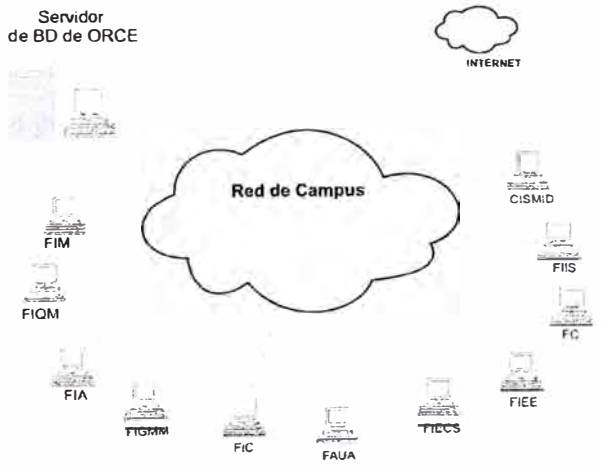


Figura 3.19 Interconexión de registros académicos.

La oficina de personal esta encargada de administrar la información de todo el personal que labora en la universidad. Cada una de las facultades tiene una oficina de personal que mantiene la información administrativa correspondiente al personal que trabaja en dicha facultad. Cada una de estas oficinas requiere acceder a información que la oficina central de personal posee, así como mantener actualizado la información. La figura 3.20 muestra las conexión a través de la red de campus de las oficinas de personal y la posibilidad de conexión exterior con entes de interes.

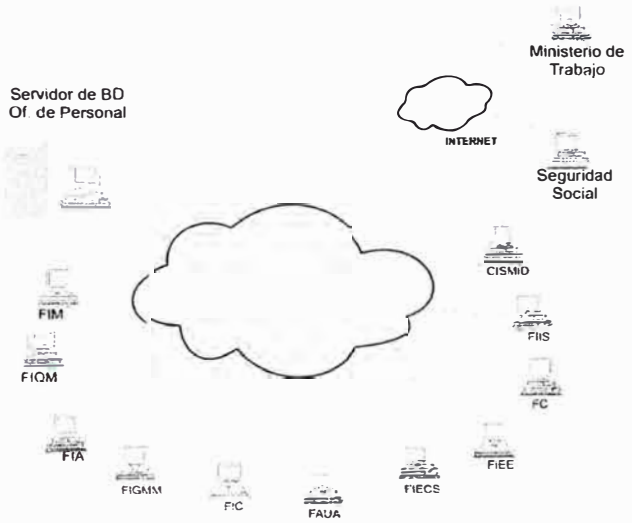


Figura 3.20 Interconexión de las oficinas de personal.

La Universidad cuenta con una base de datos bibliografica central, los cuales son mantenidos y consultados por las bibliotecas de cada facultad. Un conjunto de estaciones de consulta se han desplegado en todo el campus desde los cuales la comunidad universitaria puede acceder a realizar busquedas bibliograficas.

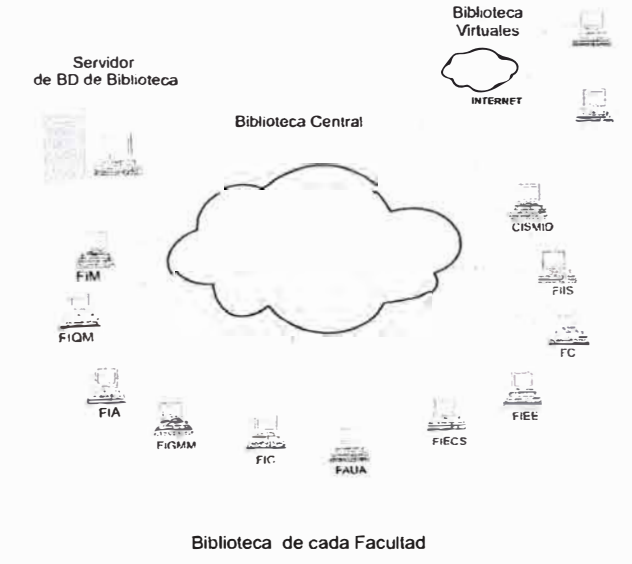


Figura 3.21 Interconexión de las bibliotecas

La figura 3.21 muestra los componentes de este sistema conectados por la red de campus.

La dependencia de la Universidad encargada de administrar las adquisiciones es la oficida de logistica. Cada facultad tiene una oficina de logistica que requiere interactuar con logistica central para administrar sus adquisiciones locales. La figura 3.22 muestra la interrelación de estos elementos y los agentes importantes mediante la red de campus.

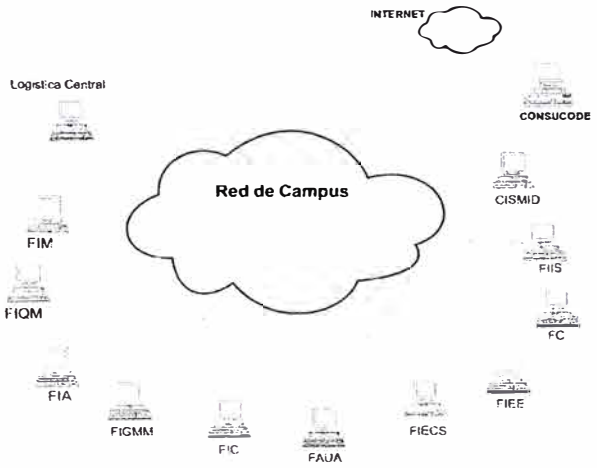


Figura 3.22 Interconexión de las oficinas de logistica

La oficina de economia y finanzas se encarga de la administración de los recursos financieros de la universidad. Cada una de las facultades posee una oficina de economia que administra localmente sus recursos financieros en estrecha coordinación con la oficina de economia central. La figura 3.23 muestra la interconexión de las oficinas de economia de cada facultad a través de la red de campus.

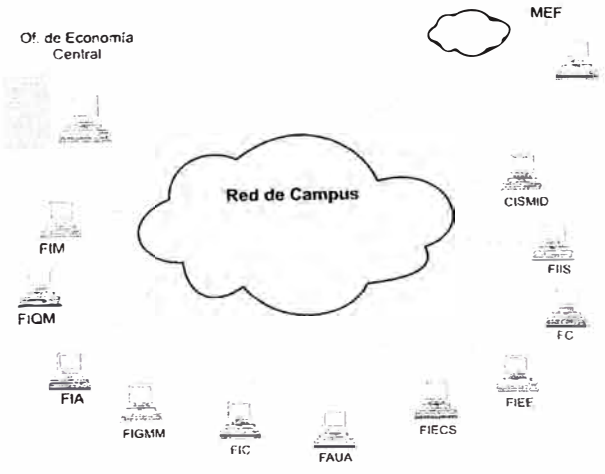


Figura 3.23 Interconexión de las oficinas de economia y finanzas

La universidad tiene implementado servicios que se brindan a la comunidad universitaria tales como: Servicio de Correo Electrónico, Servicio WEB, Sistema Integrado de Biblioteca. Estos servicios están al alcance desde el interior del campus universitario así como del exterior a través de la Internet. A traves de la red de campus tambien se ofrece el servicio de interconexión a Internet mediante un enlace de 2Mbps. Tambien se brinda un servicio de conexión dial-up para usuarios suscritos al servicio, se cuenta con un enlace de 256 Mbps para este proposito. La figura 3.24 muestra la accesibildad a estos servicios mediante la red de campus.

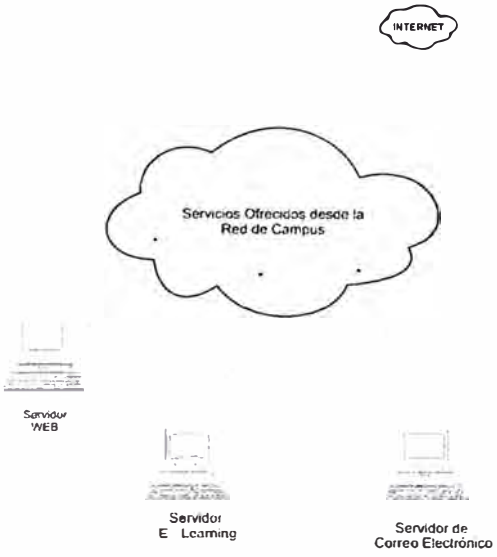


Figura 3.24 Algunos Servicios brindados a través de la red de campus

Producto del analisis del modelo de negocio, se puede establecer valores umbrales para determinados indicadores que permitan una eficaz monitorización de los recursos de red.

La table 3.2 registra los principales indicadores de desempeño, utilización y tiempo de respuesta. Sus valores serán establecidos analizando la tolerancia de los procesos iternos de cada entidad que soporte sus actividades en los ervicios de red.

TABLA 3.2 Recursos de red y sus indicadores de rendimiento

Recursos Implicados	Indicadores y rendimientos esperados			
	Disponibilidad	Tiempo de respuesta	Throughput	Utilización
SWITCH ATM	90%			<50%
UPLINK	90%			<50%
SWITCH ETHERNET	90%			<50%
HUB´s	90%			<30%
ENLACES F.O SWITCH-HUB	90%			<80%
ENLACES F.O UPLINK-SW-ATM	90%			<80%
ROUTER	95%			<50%
ENLACE A INTERNET	80%			<50%
ENLACE A INFOVIA	80%			<50%
SERVIDOR PROXI	90%			<50%
SERVIDOR DE CORREO	90%			<50%
SERVIDOR DNS	90%			<50%
SERVIDOR ESTACIONES JAVA SERVIDOR BD BIBLIOTECA	90% 90%			<70%

3.3 Diseño del sistema de gestión de red.

El sistema de gestión estará compuesta por una plataforma de gestión de red, para la gestión de los diferentes elementos de red orientado a monitorear y controlar el rendimiento de los diferentes elementos y sistemas de red, la elección de una plataforma de gestión de red es debido a que la red tiene equipos de diferentes fabricantes, y esta heterogeneidad tiende a incrementarse.

Por otro lado será necesario otra herramienta para la gestión de las VLAN, necesario para el control del tráfico de broadcast y multicast en la red conmutada.

3.3.1 Organización del sistema de gestión de red

El sistema de gestión de red estará conformada por una plataforma de gestión de red, un operador de las plataforma de gestión de red (administrador de red), un administrador de sistemas operativos y servicios de red, personal de soporte técnico, un helpdesk para recepcionar las incidencias.

Las incidencia en la red serán dados a conocer al centro de gestión de red a través de teléfono por un helpdesk, quienes tomaran el reporte de incidencia, lo registraran e intentarán una solución si esta a su alcance, si logra resolverlo la incidencia será cerrada.

Las incidencias que no pueden ser resueltas por el helpdesk deberán registrarse y asignarse a un personal de soporte, el estado de la incidencia será abierto, cuando el personal de soporte resuelva la incidencia el estado transitará a cerrado.

a) Plataforma de Gestión

Constituida por el gestor de elementos de red y el gestor de VLAN´s

1) Gestor de elementos de red

La herramienta de gestión que se dispone, es el SPECTRUM del fabricante Enterasys (Cabletron), cuyas características son las siguientes.

Características Generales:

Esta construida bajo la arquitectura Cliente – Servidor en este caso el servidor es SPECTROSERVER(VNM: Virtual Network Machine), y el cliente es SPECTROGRAPH(SG). La arquitectura del SPECTROSERVER, es mostrado en la figura 3.24.

El servidor realiza las siguientes funciones:

- Manejo de la Base de datos
- Lleva a cabo el sondeo
- Recibe los traps y los interpreta
- Obtener información de las BD y proveerlas a las aplicaciones

El Cliente realiza las siguientes funciones:

- Procesa la información recibida del servidor y la presenta en forma grafica al usuario.

Ventaja de la arquitectura Cliente Servidor

- Tanto el Servidor como el cliente pueden residir en la misma estación del trabajo, o en estaciones de trabajo independientes.

- Trabaja en forma distribuida.
  - oAyuda a tener redundancia
  - oSi la red es grande se puede monitorear parte de la red con otro servidor.
  - oLa arquitectura modular, facilita la ampliación de las funcionalidades y el soporte para la gestión de nuevos dispositivos.

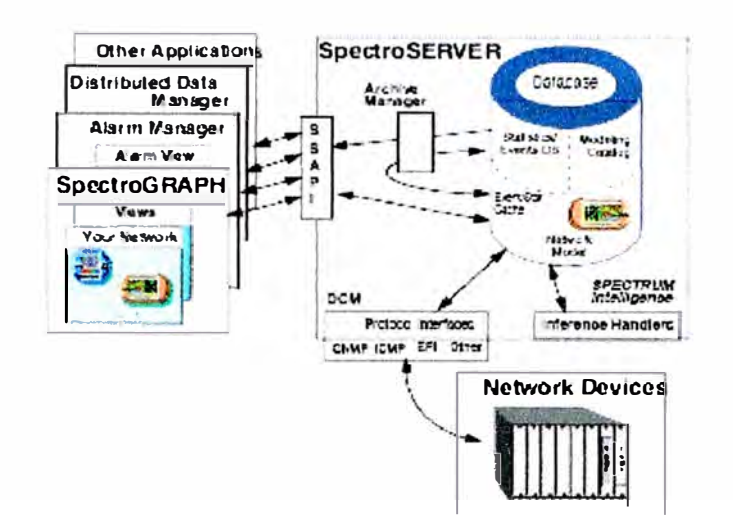


Figura 3.25 Estructura del Servidor (SpectroSERVER)

- Gestor de comunicaciones de dispositivos(DCM: Device Communications Manager): provee el mecanismo de recuperación de información y gestión de dispositivos sobre su red. El DCM periódicamente sondea cada dispositivo para recuperar el estado actual de los dispositivos guardados en la base de datos. El DCM es también el mecanismo de gestión del elemento de red. Los cambios administrativos que se realizan sobre un modelo de dispositivo en una vista del SpectroGraph, tal como habilitar o deshabilitar un puerto, son interpretadas por SPECTRUM y enviadas al dispositivo vía el DCM donde la acción administrativa es ejecutada. El estado del dispositivo es actualizado en la base de datos y el nuevo estado administrativo es presentado en la vista.
- Manejadores de Inferencia (Inference handlers): es la implementación de SPECTRUM Intelligence, este adiciona valor a los datos recolectados. Los manejadores de inferencia son capaces de procesar estadísticas muy útiles, tales como paquetes por segundo. También son capaces de interpretar la

información recolectada de los dispositivos individuales y presentar información de diagnostico que pueden ayudar a aislar y responder a problemas de red

- La base de datos SpectroSERVER: SPECTRUM recolecta una cantidad significativa de información. Una parte es recolectada mediante el sondeo de dispositivos; otra parte es recolectada de otros dominios de gestión SpectroSERVER , denominados LANDSCAPES. Estos datos son almacenados como en la base de datos de Eventos/estadísticas de SpectroSERVER como eventos y estadísticas. La figura 3.26 muestra la estructura de la BD.
- El Gestor de datos Distribuidos (DDM) provee facilidades para reducir y guardar la información recolectada y distribuir la información en una variedad de formatos a través de múltiples LANDSCAPES y aplicaciones externas.
- El gestor de archivos de DDM recupera eventos y datos estadísticas desde el SpectroSERVER, reduce y almacena el la base de datos Eventos/estadísticas. Una sobre posición es mantenida entre dos bases de datos para asegurar un registro preciso de eventos y estadísticas en caso de una falla del sistema.

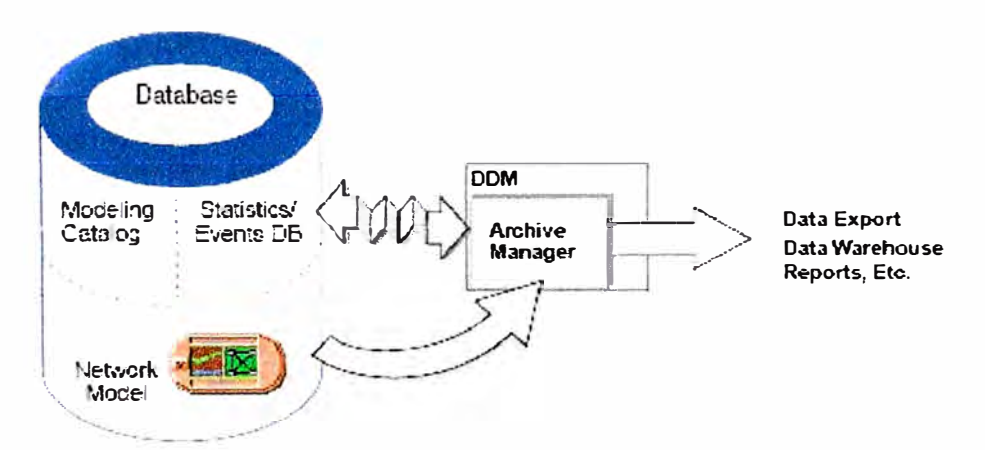


Figura 3.26 Estructura de la BD SpectroSERVER

- **Mantenimiento de bases de datos**

Copias de respaldo obtenidas de manera confiable y regular de sus bases de datos pueden ayudar a restaurar la integridad de las bases de datos.

SPECTRUM provee 2 formas de llevar acabo copias de respaldo, la primera es en línea mientras el SpectroServer esta en ejecución, alternativamente desde el control panel de SPECTRUM puede obtener una copia de respaldo, pero requiere que SpectroSERVER este desactivado.

- **Tipos de modelos, modelos y relaciones**

  La base de datos SpectroSERVER provee almacenamiento para cada configuración de dispositivo especifico, estadísticas y eventos. La base de datos también contiene el catalogo de modelos (tipos de modelos y relaciones) que determinan la estructura de toda la información de la red.

- **Tipos de modelos**: sirven como modelo base para la creación de otros similares. Ellos definen características (atributos) de los elementos que conforman su red, tales como estaciones de trabajo, hubs, redes, y usuarios. El catalogo de modelos contiene tipos que corresponden a los tipos de dispositivos encontrados en su red. Esos tipos de modelos de dispositivos proveen información especifica del dispositivo junto con el manejador de inferencias necesarias para la gestión de red.

  Un modelo representa una instancia particular de un tipo de modelo. Los modelos no son parte del catalogo de modelos, pero en ves de esto, ellos son creados desde los tipos de modelo provisto por los catálogos de modelos.

  Por ejemplo para crear un modelo de una estación de trabajo particular SPARCstation20 en la red (identificado por una única dirección IP y nombre de host), debería elegir el tipo de modelo Host_SUN como modelo predefinido de los tipos de modelo disponibles en el catalogo de modelos. Antes de crear el modelo, SPECTRUM pregunta por la identificación de la estación particular, esta compuesta por el IP y el nombre de host.. Esta información identifica únicamente el nuevo modelo como un particular SPARCstation 20.

  Las relaciones (conexión, contención, propiedad, etc.) define las relaciones que pueden existir entre dos o mas modelos. El tipo de relación que un modelo particular es capaz esta determinado por el tipo de modelo usado para crear un modelo. Por ejemplo, un modelo creado desde el tipo de modelo "Network" puede contener una variedad de dispositivos de red

(ruteadores, bridges, estaciones de trabajo, etc.) incluyendo modelos de red específicos tales como FDDI_Network, ATM_Network, etc. Las relaciones definen la estructura en el modelo de red.

El hardware necesario y el utilizado para la instalación de la plataforma de gestión de red Spectrum esta compuesto por:

SUN NETRA i (256Mbytes de RAM, 2 interfaces ethernet, 233Mhz de CPU, 2Gbytes de Disco Duro)

Monitor de 24 pulgadas de alta resolución

Sistema Operativo Solaris 5.0

2) El gestor de VLAN

A la gestión de red le concierne resolver problemas de la red tales como adicionar, mover y cambiar dispositivos de la red, controlar tráfico de broadcast y seguridad. Las VLANs ofrecen soluciones a esos problemas. Ver figura 3.27

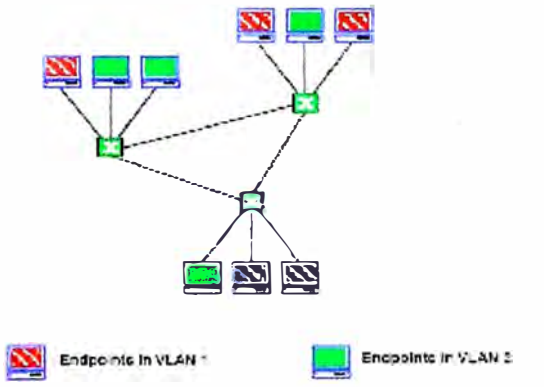


Figura 3.27 Vista de una LAN usando VLAN

Movimientos y cambios

Las VLANs incrementan su habilidad para gestionar su red dinámicamente sin frecuentes idas y vueltas al closet de cableado o reconfiguraciones manuales de las estaciones de trabajo. En una red ip por ejemplo, cuando un usuario se mueve de una subred a otra, una ida y vuelta al closet de cableado es usualmente requerido, y las direcciones ip de los usuarios deben ser manualmente actualizados. VLAN elimina ambos requerimientos porque la membresía no depende de de la

localización física del usuario en la red. Los usuarios retienen sus direcciones IP originales y la membresía de subred.

Los miembros de un grupo funcional, no importa cuan dispar, pueden aparecer como si ellos están en el mismo segmento LAN, con la mayoría de tráfico de broadcast de red permaneciendo dentro de esa VLAN del grupo. Esos grupos funcionales pueden ser imaginados como grupos virtuales. Aunque la localización física no es concerniente al entorno VLAN, un grupo miembro quien se mueve a otra localización no causa problemas particulares a la red y no tienen que ser realizado cambios a las estaciones de los usuarios. Si ese mismo miembro es transferido a otro grupo, puede asignar la membresía del usuario en el nuevo grupo, mediante un simple arrastre del icono del usuario de una VLAN y luego soltándolo en otra.

Tráfico de broadcast

Conmutadores operando en modo VLAN SecureFast hacen esto mediante la resolución de los paquetes broadcast a unicast. Esto es llevado a cabo por cada switch estando habilitado a resolver paquetes broadcast en el puerto de acceso del switch, mas que precisamente etiquetar e inundar los paquetes broadcast.

Para resolver, el switch hace una inspección de su directorio local y/o el directorio virtual (vía la solicitud de resolución inter switch) para el paso de la dirección MAC a la dirección de red (dirección alias). Mas que inundar broadcast ARP, el switch de acceso resuelve hacia la verdadera MAC destino y luego establece una conexión desde switch de ingreso y egreso para la dirección MAC origen a la dirección MAC destino.

Si el destino no puede ser resuelto a la verdadera dirección MAC, los paquetes son reenviados fuera de los puertos asociados con la VLAN origen.

Las VLAN se comportan en mucho de la misma forma que lo hacen los ruteadores, restringiendo el tráfico de broadcast a solo esos usuarios dentro de la misma VLAN. Esto también reduce grandemente el tráfico de broadcast mediante limitación de broadcast solo a los puertos de switch conectado a los puntos finales perteneciendo a una VLAN particular.

Características del gestor de VLANs

Plug and Play fácil de usar.- la comunicación entre puntos finales es posible aun antes que el VLAN MANAGER se instale. Antes de cualquier gestión de membresía de VLAN, cada VLAN en el dominio del switch emula una única LAN puenteada, donde todos os puntos conectados directamente en efecto son miembros de una VLAN común.

- Automatización de adición, movimiento y cambio de usuarios: el software soporta adición, movimiento y cambios dinámicos de usuarios.
- Capacidad de sostener alto throughput .- cada vez que una llamada es efectuada, el procesamiento procede velocidad cableada prácticamente.
- Control de tráfico de broadcast.- inundación basado en etiqueta de broadcast no resolvible.
- Conmutación o enrutamiento entre vlans .- conmutación capa 3 para la comunicación de host abierta o enrutamiento capa 3 para soportar control de acceso host.
- Llamada a re-enrutamiento automático.- Un VLPS especializado (Protocolo de estado de enlace virtual) provee rutas redundantes. La llamada a re-enrutamiento es hecho en el aire.
- Enlaces de red activos múltiples con balance de carga .- las conexiones agregadas para cada switch SecureFast es balanceado sobre múltiples enlaces de alta velocidad.
- Operación independiente de los protocolos de red.- todos los protocolos populares soportados con servicios especiales para IP, IPX, DHCP, etc.
- Operación independiente de tecnologías y topologías LAN.- todas las tecnologías LAN populares tales como ethernet y FDDI son soportados.
- Compatibilidad completa con adaptadores de red existentes, HUB´s, ruteadores y conmutadores .- protege su inversión actual en hardware.
- Criterio de membrecia VLAN flexible .- membresía de punto final por switch, puerto, dirección MAC, protocolo, dirección de red.

- Capacidad de llamada a derivación .- conexiones direccionales o bidireccionales monitoreados hacia el puerto de salida de un analizador o vía la dirección fisica de un analizador. Las llamadas pueden ser derivadas a cualquier puerto dentro de la estructura del switch mediante la selección de cada una de las direcciones MAC de la sonda del analizador de red a través de las aplicaciones del VLAN Manager o cualquier puerto de switch dentro de la estructura del switch.
- Vista topológica editable.- Las conexiones de red son dinámicas. El número de usuarios conectados al switch se visualiza sobre el icono del switch. Puede filtrar sobre una VLAN especifica. Los iconos pueden ser movidos orientados a crear una vista personalizada.
- Control multidominio.- Un VLAN Server puede gestionar múltiples dominios VLAN.
- Movilidad de usuario completo.- Un usuario quien es estáticamente asignado a una VLAN retendrá el mapeo durante el proceso de movimiento de un puerto a otro o de un switch a otro.
- Tabla de conexión.- Displaya conversaciones de nodo final activo para los usuarios seleccionados.
- Servicios de directorio.- Directorio dinámico los cuales proveen localización fisica de cada punto final, dirección capa 3, nombre de host, y mapeo de VLAN.
- Determinación de mejor ruta.- enlaces óptimos son elegidos para establecer una conexión basado en costo del enlace.
- Convergencia topológica rápida.- detección de perdida eléctrica para enlaces de red ethernet y fastethernet. Detección de perdida SMT para enlaces de red FDDI.
- Políticas VLAN (open/secure).- en modo abierto, la comunicación inter VLAN es posible vía llamada a procesamiento y resolución dirección/VLAN. No es requerido un ruteador. En modo seguro, comunicación inter-VLAN es posible para usar un ruteador o mediante el uso de políticas avanzadas.
- Políticas VLAN avanzadas.- politicas inter-VLAN pueden ser configuradas por VLAN mas que globalmente.

- Membresía de múltiples VLAN por usuario - los usuarios pueden tener memebrecia en mas de una VLAN.
- Herencia de membresía VLAN por puerto para usuarios sin ninguna asociación VLAN previa.- los usuarios son asignados a la VLAN por defecto de los puertos a los que ellos se conectan.
- Puerto espejo.- provee la habilidad para redirecionar todos los datos a un puerto para el análisis de paquetes o diagnostico de red.
- Control de protocolo.- permite al gestor de red suprimir ciertos protocolos o tipos de tramas de protocolo sobre la base de dominio o switch.
- Restricciones User/port .- permite a los usuarios a ser restringidos a ciertos puertos y puertos a ser restringido a ciertos usuarios.
- Agente de reenvió DHCP.- Soporta múltiples DHCP (Dynamic Host Control Protocol) ámbitos servidos por un único servidor DHCP dentro de un dominio.

Componentes del VLAN MANAGER

El SPECTRUM VLAN MANAGER consiste del software VLAN MANAGER y los switchs (con firmware VLAN instalado) SmartSwitch de Cabletron trabajando en conjunción con puntos finales de red.

- El software VLAN Manager monitorea y controla la configuración y mantenimiento de las redes VLAN. Este consiste del VLANServer y el VLAN MANAGER Cliente. Ver arquitectura software VLAN en la figura 3.28 y modelo de interacción en la figura 3.29a.
- Los switchs SmartSwitch proveen intercepción de broadcast, resolución de dirección y procesamiento de llamado.
- Los puntos finales son dispositivos conectados a puertos de acceso en un dominio switch VLAN.

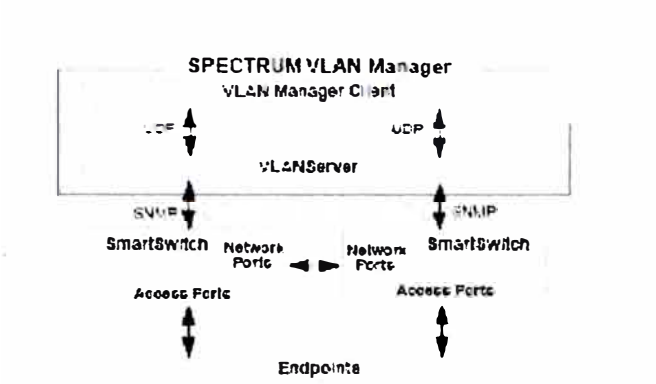


Figura 3.28 Arquitectura Sofware VLAN

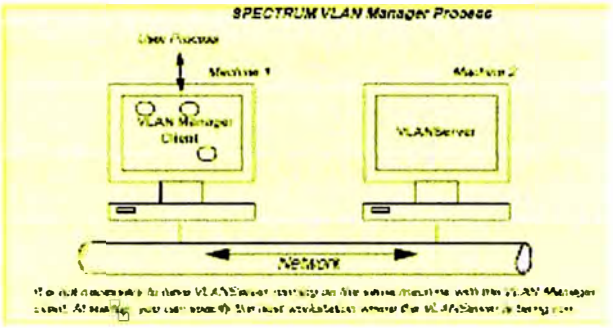


Figura 3.29a Modelo de Interacción del gestor de VLAN

Los Switchs VLAN SecureFast son dispositivos de interconexión orientados a conexión. Esos dispositivos usan pares de direcciones origen/destino (SA/DA) con servicios de enrutamiento virtual capa 3 para proporcionar intercepción , resolución y procesamiento de llamada. En una red orientada a conexión, la determinación de la ruta se realiza al momento de realizar la llamada. Una vez que la llamada es programada, no se requiere ninguna intervención software adicional. Este tipo de gestión de llamada opera de manera similar a la red de telefonía. El circuito es establecido, los datos son transferidos.

Los switchs reenvían los paquetes en la capa MAC y permiten conectividad de los puntos finales vía puertos de acceso basados en mapeo a VLANs. El primer paquete es ruteado y los paquetes restantes son conmutados siguiendo la misma ruta. Cada Switch VLAN mantiene un directorio local de MACs de puntos finales y direcciones de red encontradas en cada puerto de switch. La agregación de cada directorio local del switch VLAN forma una vista completa de un dominio VLAN entero. Esta información es usada por el gestor de VLAN para la asignación y verificación de VLANs.

El software gestor de VLAN esta basado en el modelo cliente/servidor. El programa cliente (VLAN MANAGER), es una interfaz grafica de usuario del gestor de VLAN. El programa servido (VLANServer) y la interfaz de usuario grafica es lanzada desde el panel de control SecureFast, desde el icono del VLANSERVER.

Tomando ventaja de esta relación cliente/servidor, múltiples interfaces de usuario pueden ser conectados a un único VLANServer. La interfaz de usuario puede ser ejecutado localmente, en la misma maquina del VLANServer o remotamente desde la red.

El cliente gestor de VLAN (VLAN MANAGER), y la puerta hacia la administración de VLANs. A través del cliente, puede iniciar todas las tareas de gestión de red VLAN, como :

- Crear, remover, abrir, configurar, y descubrir dominios, y visualizar detalles del dominio.
- Crear y borrar VLANs, ver detalles de las VLANs, habilitar o deshabilitar VLANs, y aplicar políticas de VLANs.
- Aplicar políticas avanzadas de VLANs.
- Adicionar y remover alias de usuario.
- Adicionar y borrar switchs y visualizar detalles del switchs.
- Crear nuevos usuarios y visualizar el directorio de todos los usuarios.
- Cambiar el estado y bloqueo y desbloqueo de los puertos de acceso.
- Realizar tareas administrativas y de descarga.
- Visualización de la topología de un dominio de vlan.
- Visualización activa de llamadas por usuario.
- Establecer escucha de llamada para analizar llamadas.
- Liberar las llamadas.
- Facilitar la realización de llamadas
- Crear circuitos virtuales permanentes (PVCs)
- Configurar parámetros del ruteador
- Crear y gestionar VLANs AMR.

- Crear y gestionar grupos IP Multicast.
- Configurar "Uplink switching" basado en chasis.
- Restringir usuarios a ciertos puertos o puertos a ciertos usuarios.
- Redirigir los datos de un puerto a otro puerto para el análisis de paquetes.
- Configurar puertos de acceso redundante.

Vlan Manager Usa comandos del protocolo SNMP para configurar y controlar todos los Switchs VLAN en un dominio VLAN. Un dominio VLAN consiste de un grupo de Switchs VLAN limitados por dispositivos de ruteo. Toda la información de los puntos finales es descubierto y usados por los Swiths VLAN durante el establecimiento de la llamada. El "VLAN Manager" recolecta esta información periódicamente usando SNMP.

El VLANServer provee de inteligencia al "VLAN Manager". Contiene los modelos de los dispositivos de red actual y sus interacciones. Esos modelos están recolectando datos continuamente relativo a los objetos que representa. Como resultado de este proceso de sondeo, la base de datos del VLANServer gana gran conocimiento acerca de cualquier red que gestiona. Mediante el análisis de esta información, se puede maximizar el rendimiento de sus sistemas minimizando costos.

El hardware necesario y el utilizado para la instalación de la plataforma de gestión de red Spectrum esta compuesto por:

SUN NETRA i (256Mbytes de RAM, 2 interfaces ethernet, 233Mhz de CPU, 2Gbytes de Disco Duro)

Monitor de 24 pulgadas de alta resolución

Sistema Operativo Solaris 5.0

b) El Administrador de Red

Estará encargado del monitoreo y control de los dispositivos que componen la red LAN y su Interconexión a la Internet.

Detección de fallos en la red, análisis del impacto, aislamiento y solución de las fallas, así como su reporte correspondiente.

Planificación de la estructura de VLANs, su interconexión, creación y pertenencia a VLANs.

Actualización de los firmware (sistemas operativos) de los switchs, hubs, ruteadores.

Planificación de las acciones de mantenimiento del equipamiento de la red y los servicios brindados por los carriers(servicios de interconexión). Coordinación con cada uno de los usuarios implicados en las acciones de mantenimiento.

Reporte de planes a llevarse a cabo, y ejecutados, Reportes de altas y bajas de servicio, tiempo de duración de los fuera de servicio, razones de la interrupción.

Administrará las plataformas de gestión. Sus funciones estarán fuertemente apoyadas en las plataformas de gestión y algunas herramientas independientes.

Perfil del administrador de red:

- Conocimiento avanzado de sistemas operativos UNIX, LINUX, WIN2000 SERVER.
- Conocimiento avanzado de la pila de protocolos TCP/IP, en particular del protocolo SNMP.
- Conocimiento de la arquitectura de gestión basada en SNMP.
- Conocimiento avanzado de conmutación ethernet, VLAN (IEEE802.1q), STP (IEEE802.1d), enrutamiento entre VLANs.
- Conocimiento avanzado de enrutamiento IP.

c) El administrador de sistemas operativos y servicios

Esta encargado del buen funcionamiento de los servidores, sus sistemas operativos y los servicios que estos brindan.

Dimensionar los recursos fisicos de los servidores para un servicio eficaz. Establecer el número máximo de conexiones concurrentes que es capaz de soportar con los recursos fisicos actuales, monitorizar este parámetro que no exceda el umbral.

Actualizar el sistema operativo, con nuevas versiones y/o parches, así como los servicios que aloja.

Realizar copias de respaldo periódicos, totales e incrementales.

Registro y análisis de eventos que se producen en los servidores.

Administrar el acceso al servidor, creando usuarios y otorgando privilegios, monitorizando las acciones que los diferentes usuarios realizan en el servidor.

Los servidores trabajarán bajo los sistemas operativos SOLARIS, LINUX, WIN2000-Server, los servicios que alojaran son:

DNS (Domain Name Service), http (WEB), correo, NAT/PAT, FTP, JAVA-Server, Radius, Bases de Datos Lotus Notes.

Perfil del administrador de sistemas operativos y servicios

- Conocimientos avanzados de Solaris, Linux, WIN2000-Server
- Conocimientos avanzados en la instalación y configuración de servicios DNS, WEB, CORREO, FTP, LOTUS NOTES, JAVA-SERVER, RADIUS, NAT/PAT.
- Capacidad para realizar copias de respaldo, y restablecimiento de los servicios a partir de estas copias de respaldo.
- Capacidad de realizar actualizaciones a nivel del sistema operativo y servicios. Asegurar sistemas operativos y servicios.

d) Los soportes Técnicos

Están encargados de realizar instalaciones de los sistemas operativos de PCs WIN95, 98, XP.

Configuración TCP/IP para su trabajo en red.

Instalación de aplicativos de usuario final.

Conexión de nuevas estaciones de trabajo a la red de campus.

Mantenimiento preventivo de los equipos que componen la red.

Reportar el estado de los incidentes recibidos.

Actualizar aplicativos de usuario final.

Perfil de soporte técnico

- Conocimiento de sistemas operativos WIN95, 98, XP, Linux.
- Instalación y configuración de interfaces de red
- Conocimiento de cableado estructurado.
- Capacidad de instalar nuevas interfaces a una PC y configurarlos.

e) El helpdesk

Es el punto de contacto entre el usuario final y el centro de gestión. Es el primer punto de soporte que encuentra el usuario final para reportar incidentes (fallas, alertas, solicitudes de nuevas configuraciones, accesos a nuevos servicios, etc.)

El helpdesk recibe y registra los incidentes reportados, también es responsable de la actualización de los estados de las incidencias.

Las incidencias pueden transitar a través de los diferentes estados: recibido, abierto, asignado, resuelto, cerrado.

El helpdesk clasifica los incidentes y los reporta al administrador de red, administrador de sistemas operativos y servicios y/o al personal de soporte.

El perfil técnico del help desk:

- Conocimiento de sistemas operativos de estaciones de usuario final WIN95, 98, XP, Linux.
- Configuración de interfaces de red.
- Configuración de impresoras.
- Configuración TCP/IP en estaciones WINDOWS y Linux.
- Configuración de clientes de correo: IMAP, POP3.
- Instalación, configuración y actualización de navegadores (clientes WEB)

La figura 3.29b muestra una vista logica de los componentes del sistema de gestión de red.

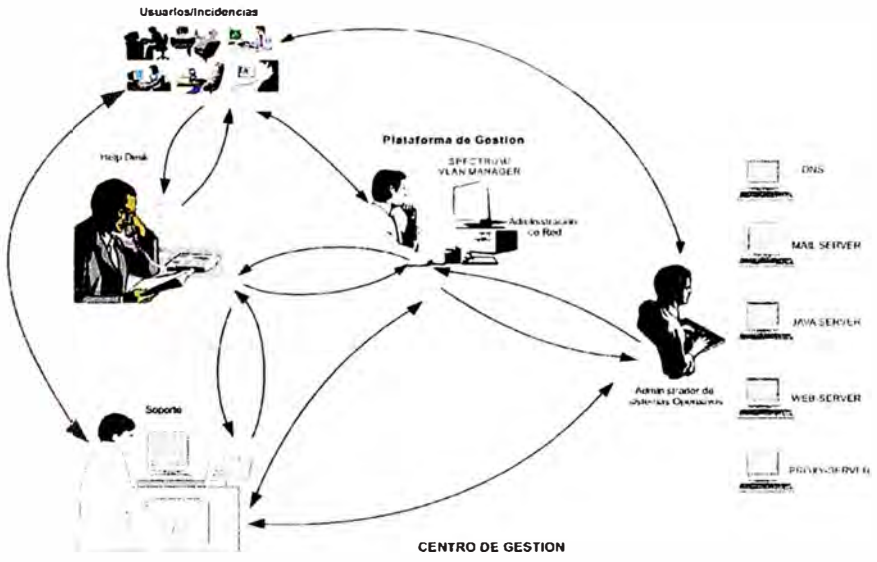


Figura 3.29b Componentes del sistema de gestión

3.3.2 Plan de Numeración del sistema de gestión de Red.

Plan de numeración de los dispositivos gestionados y estaciones de gestión.

SWITCH ATM (9A000): 134.141.0.10 /16

UPLINKs (9A423):

NODO B: 134.141.1.123/16

NODO G: 134.141.2.123/16

NODO N: 134.141.3.123/16

NODO Q: 134.141.4.123/16

SWITCH ETHERNET (9E438):

NODO B: 134.141.1.138/16

NODO G: 134.141.2.138/16

NODO N: 134.141.3.138/16

NODO Q: 134.141.4.138/16

SEHIS-HUB:

NODO B:

NODO G:

FAUA- Logística: 134.141.2.10/16

FAUA Proyección social: 134.141.2.50/16

FIGMM-Cabina: 134.141.2.32/16

FIGMM-Centro de Computo: 134.141.2.30/16

FIC-Centro de Computo: 134.141.2.60/16

FIC-Laboratorio de estructuras: 134.141.2.20/16

FIQM-Laboratorio: 134.141.2.40/16

NODO N:

FIECS: 134.141.3.10/16

FIC: 134.141.3.30/16

Laboratorio de Hidráulica: 134.141.3.40/16

Centro Medico: 134.141.3.20/16

NODO Q:

FC: 134.141.4.10/16

FIIS: 134.141.4.20/16

CISMID: 134.141.4.30/16

Estación de gestión: SPECTRUM

134.141.1.5

Estación de gestión: VLAN

134.141.1.4

Seguridad de acceso a los dispositivos gestionados.

Cada uno de los elementos administrables requieren de una configuración básica consistente en nombres de comunidades:

Solo lectura: unixyz

Lectura/Escritura: xyzuni

Parámetros para la conexión a través del puerto de consola:

Velocidad de transmisión=9600bps

Bits de datos=8

Bits de parada=1

Paridad=Ninguno

Control de Flujo=Ninguno

Topología lógica del sistema de gestión

Los equipos a gestionarse así como los gestores finalmente se encontraran en la VLAN "BASE", todos los equipos en un estado inicial están en la VLAN BASE (Alias de la VLAN 1, VLAN por omisión).

3.3.3 Plan de pertenencia a VLANs

Para evitar el aumento desmedido del tráfico de broadcast, se plantea una VLAN (dominio de broadcast) por cada grupo de usuarios. En especial las estaciones JAVA, son muy susceptibles al tráfico de broadcast y colisiones, debido a que todos los recursos que necesita para operar lo obtienen de los servidores a través de la red.

VLAN BASE: Todos los recursos descubiertos inicialmente se encontraran en esta VLAN.

VLAN ACADEMICA: contendrá a los recursos (PCs) de la comunidad estudiantil en general

VLAN SIB: contendrá las recursos del sistema de biblioteca

VLAN OCEF: contendrá a los recursos de la oficina de economía y finanzas

VLAN ORCE: contendrá a los recursos de la oficina de registros académicos

VLAN JAIL: contendrá a los recursos de los usuarios que hacen uso inapropiado de la red y los servicios

Las VLANs contempladas son mostrados en la figura 3.30, un modelo de la interconexión de VLANs es mostrado en la figura 3.31.

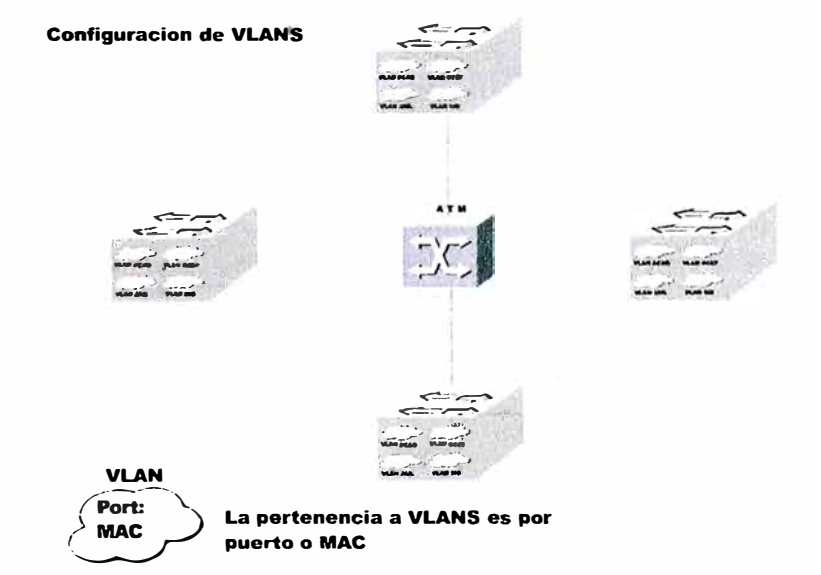
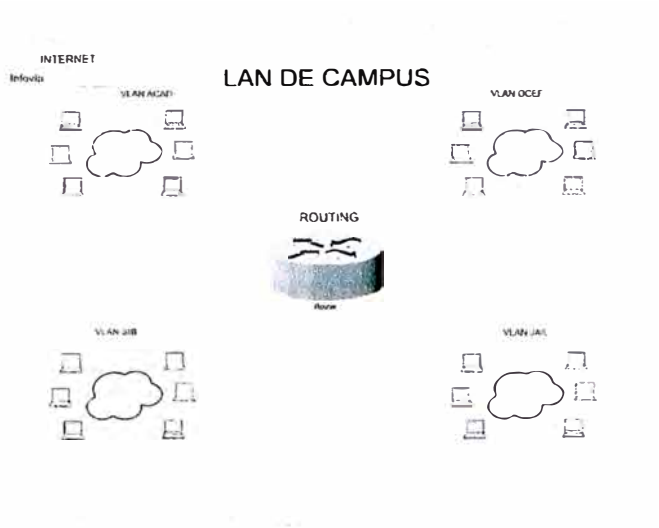


Figura 3.31 VLANs contempladas en la red de campus



VISTA LOGICA USANDO VLAN

Figura 3.31 Modelo de Interconexión de VLANs

CAPITULO IV

IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE RED DE CAMPUS

4.1 Configuración de los elementos gestionados

Configuración del switch ATM: mediante una conexión a través del puerto de consola con los parámetros indicados en la fase de planificación y haciendo uso del modo AMI realizar: Asignación de dirección IP, carga del archivo de configuración LECS, configuración del LEC, creación de un LES y un BUS. Esta configuración debe realizarse con el switch ATM sin conexión a los uplink.

Asignar la direcciones IP y el nombre de comunidad, configurar la clave de acceso al switch

Configuración de los UPLINK: a través del puerto de consola asignar la dirección IP, crear las ELANs, de acuerdo con la configuración del switch ATM. Crear las VLAN´s y luego unirlas a las ELAN´s.

Configurar las direcciones IP de cada uno de los UPLINK , el nombre de comunidad y las claves de acceso a la consola de cada dispositivo.

Configurar las direcciones IP de los switch 9E438, configurar los nombres de comunidades y claves de acceso a la consola del switch.

Conectar el switch ATM a los UPLINK en el nodo central, probar la conectividad hacia los diferentes UPLINK.

Configurar las direcciones IP de cada uno de los HUBs de acuerdo al plan de numeración, configurar el nombre de comunidad y las claves de acceso a cada uno de los HUBs.

Desde el nodo central realizar las pruebas de conectividad hacia cada uno de los HUBs.

Configurar el agente SNMP del Ruteador con el nombre de comunidad.

Desde el nodo central realizar las pruebas de conectividad.

4.2 Configuración de los gestores de red.

4.2.1 Preparación de las estaciones Gestoras

Las estaciones gestoras son estaciones donde se instalará y residirán los softwares de gestión para el monitoreo y control de los dispositivos de red y para la gestión de VLANs.

- Verificación de conformidad entre los requerimientos software y las características del equipo.
- Instalación del sistema operativo, y los parches correspondientes de acuerdo con los requerimientos del sistema operativo así como del software de gestión.
- Configuración de las direcciones IP de acuerdo con el plan de numeración. Pruebas de conectividad en la red lógica asignada para efectos de gestión de red.

4.2.2 Instalación de software de gestión

Los software de gestión correspondientes son: SPECTRUM V5.0 (SERVER y GRAPH) y VLAN V1.2 (SERVER y MANAGER).

Luego de la instalación se deberá proceder con la verificación de la operación de las aplicaciones Servidor y Cliente.

En el host SPECTRUM: prueba de ejecución del SPECTROServer, prueba de ejecución del SPECTROGraph, verificación de la conexión del cliente con el servidor.

a) SPECTRUM

   1) Estructura de directorios después de la instalación, ver figura 4.1.

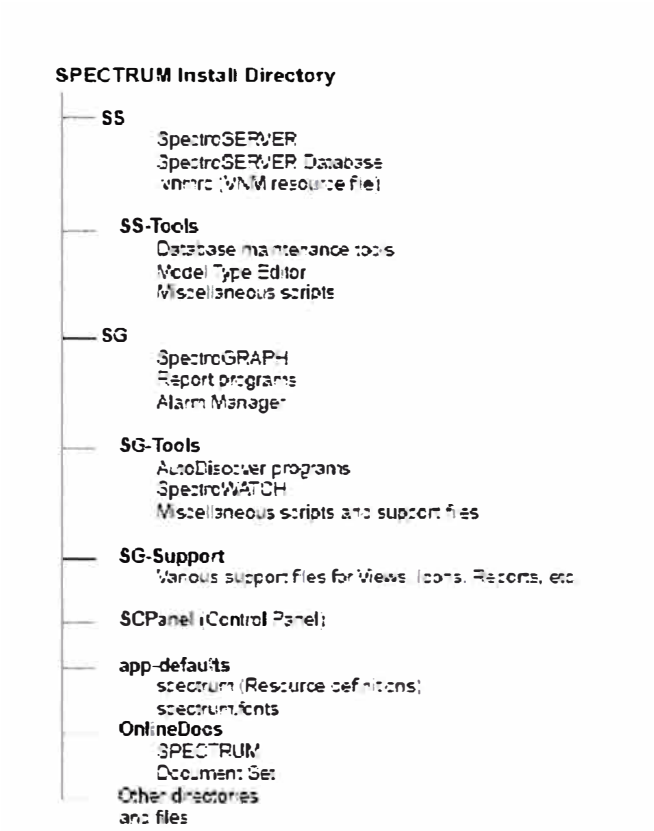


Figura 4.1 Estructura de directorios del SPECTRUM

2) Luego de la instalación, el lanzamiento del panel de control del SPECTRUM se realiza con el usuario y clave de acceso correspondiente a la instalación:

Spectrum > SPECTRUM

Esto producirá la aparición de la pantalla mostrada en la figura 4.2

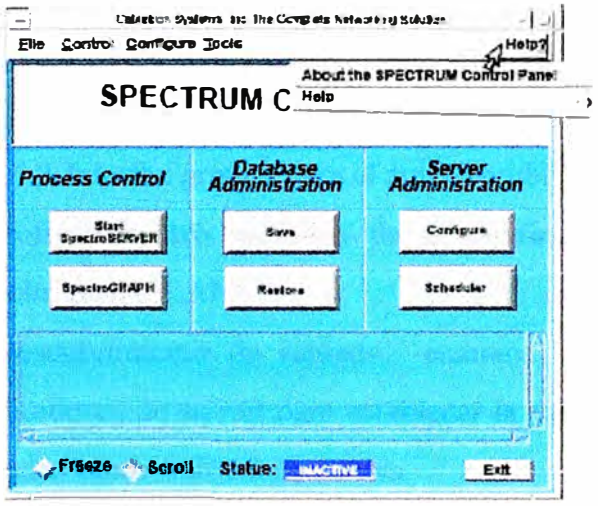


Figura 4.2 Interfaz grafica de lanzamiento del Servidor y Cliente

Desde este panel de control se puede lanzar el EspectroSERVER, también puede lanzarse desde la línea de comando del sistema operativo:

Spectrum> SpectroSERVER

3) Configuración de los nombres de comunidades y del rango de direcciones para la realización del "autodiscovery", descubrimiento automático vía SNMP de los elementos de red.

Desde el nodo central, donde se encuentran los servidores de gestión:

Mediante la herramienta de autodescubrimiento (ver figura 4.3) localizar cada uno de los elementos de red que contienen agentes SNMP configurados tales como: SWITCH ATM, UPLINKS, SWITCHs Ethernet, HUBs, Servidores.

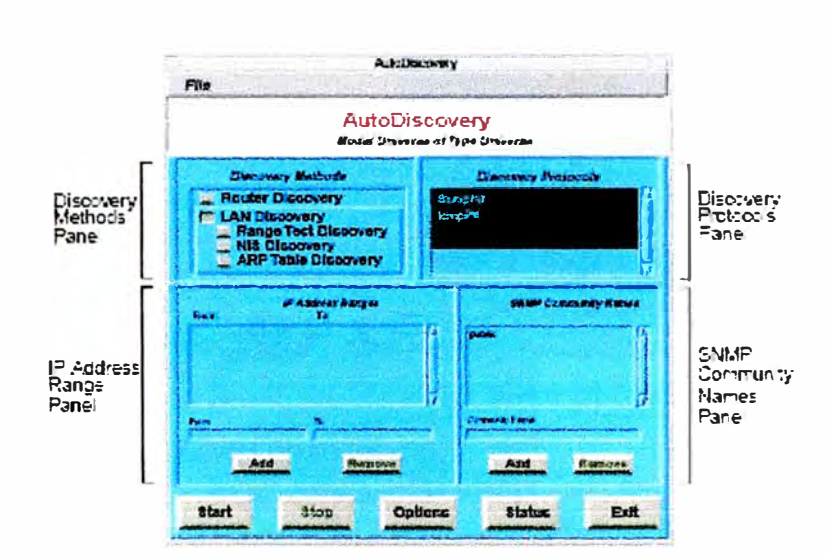


Figura 4.3 Interfaz grafica para el autodescubrimiento.

AutoDiscovery, ofrece cuatro métodos de descubrimiento de ruteador y tres métodos de descubrimiento LAN:

- Descubrimiento de ruteador: examina la tabla de rutas en los rutadores de su red para establecer la topología de alto nivel de su red creando subredes y LANs.
- Descubrimiento por prueba de rangos: usa "ICM ECHO REQUEST" (ping) para probar cada uno de las direcciones IP

dentro de su rango o rangos en el panel de rangos de direcciones IP.

- Descubrimiento NIS: limita el descubrimiento a los dispositivos identificados en la tabla host de su sistema servidor NIS(Network information Service).
- Descubrimiento de tablas ARP: mapea las direcciones IP de los dispositivos descubiertos a direcciones fisicas (MAC).

La herramienta de autodescubrimiento relacionará los diferentes elementos de de red formando una representación de la topología de la red, como muestra la figura 4.4.

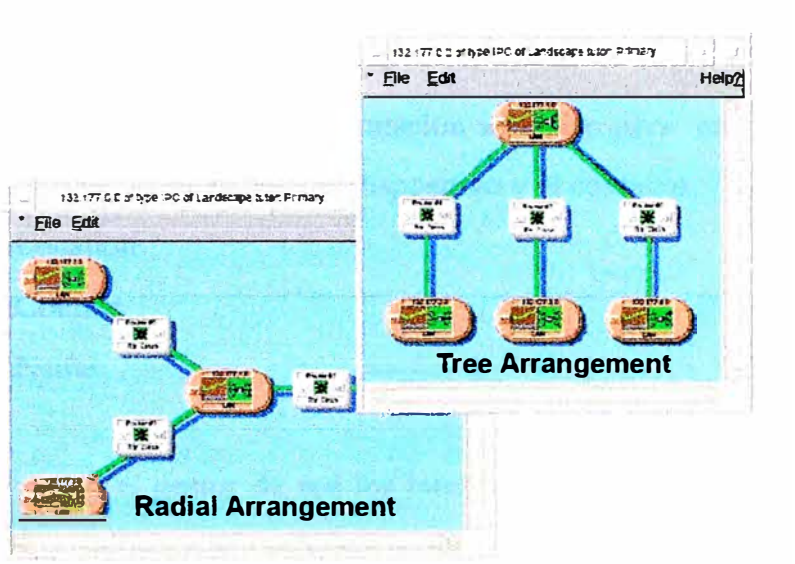


Figura 4.4 Vista de los elementos de red que son descubiertos

4) Verificar que todos los dispositivos de la red hayan sido descubiertos (hacer un checklist), para los dispositivos no descubiertos, haciendo uso de la herramienta de descubrimiento manual intentar descubrirlo, si no es posible inicie procedimiento de diagnostico y resolución de fallas relacionado con el agente SNMP del elemento de red que no ha sido descubierto. La figura 4.5 muestra una vista de la red de campus, luego de la operación de autodescubrimiento.

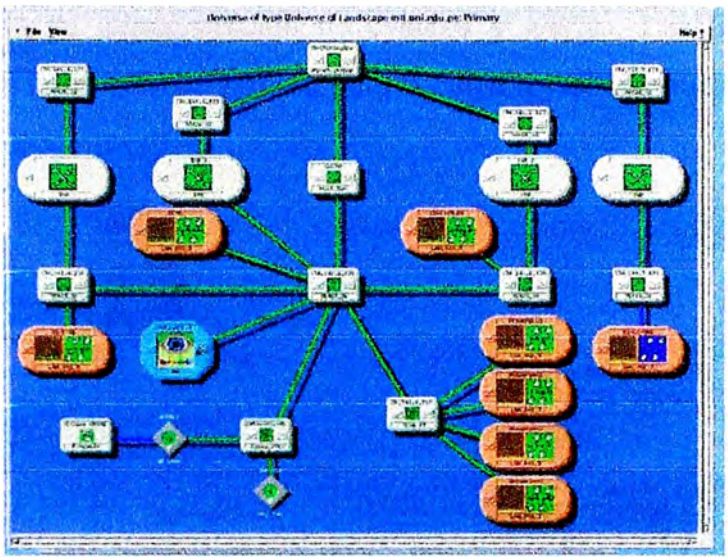


Figura 4.5 Modela Red de campus luego del Autodescubrimiento

5) Las relaciones no resueltas deberán ser realizadas manualmente por el administrador de la red.

Se procederá a completar la información administrativa en cada dispositivo, tal como el nombre, localización del dispositivo y el contacto.

- sysLocation
- sysContact
- sysName

6) Configurar en el gestor de red los intervalos de sondeo de cada elemento red, los traps, y valores umbrales de los objetos gestionados para el lanzamiento de las alarmas.

Se sugiere que los intervalos de sondeo por defecto no se cambien si no hay una razón técnicamente válida, un intervalo de sondeo pequeño podría producir una sobrecarga de tráfico en la red y un intervalo muy grande retardaría el conocimiento de los eventos que ocurren en la red y por tanto su tratamiento. El valor por omisión en el gestor SPECTRUM es de 300 segundos.

7) A partir de la identificación de los parámetros críticos, definir los valores umbrales de los objetos de gestión y las acciones que el sistema de gestión debe realizar, tales como generación de alarmas, y la comunicación a los elementos

técnicos humanos para el seguimiento de la incidencia. La figura 4.6 muestra la estructura de administración de eventos y alertas. Las figuras 4.7, 4.8, 4.9 muestran las interfaces graficas para la edición y configuración de TRAPS.

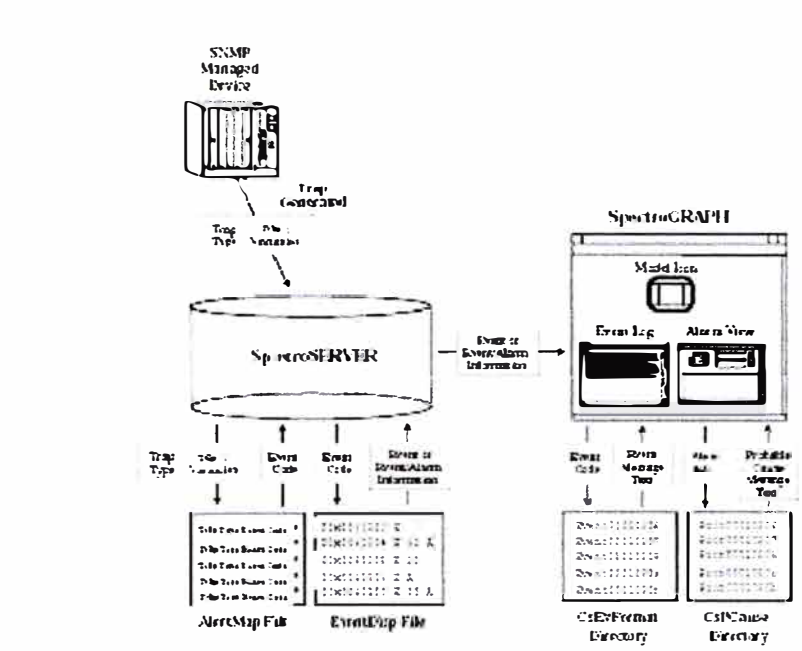


Figura 4.6 Arquitectura del subsistema de manejo de eventos y alertas

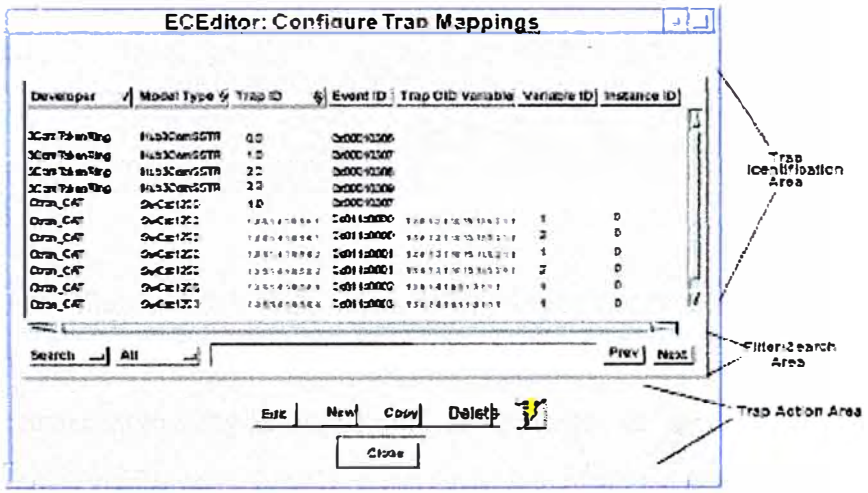


Figura 4.7 Vista grafica de los TRAPS definidos

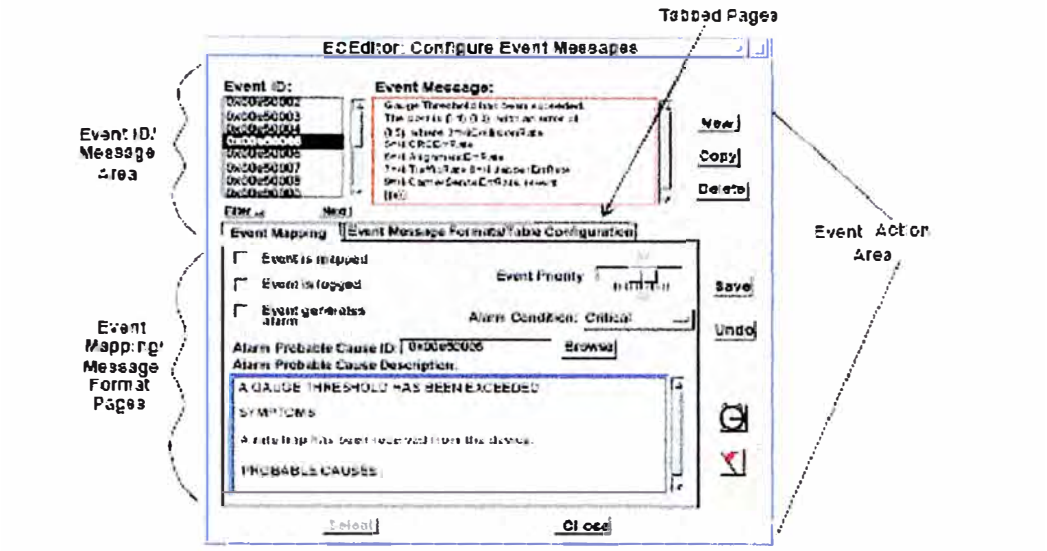


Figura 4.8 Vista grafica del mapeo Evento - Alarma

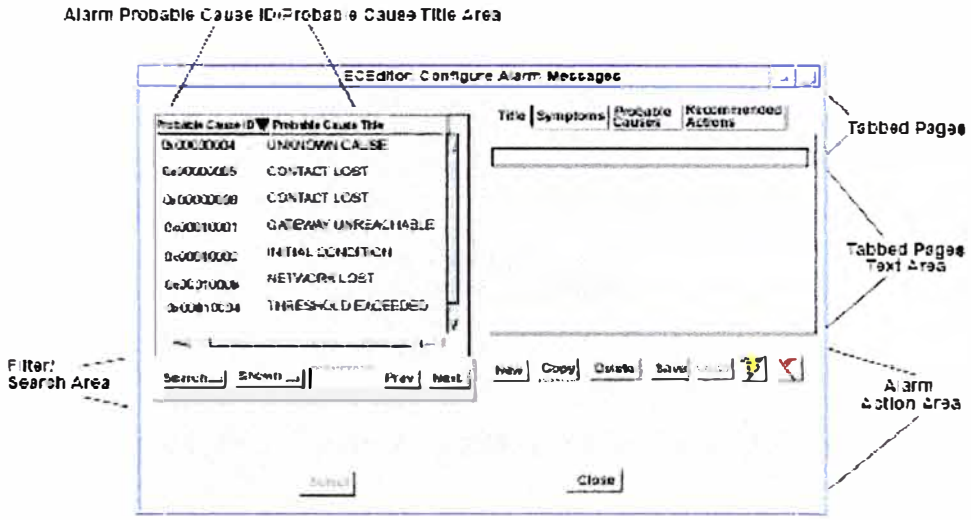


Figura 4.9 Vista grafica de la correlación de alarmas

8) Implementación de la seguridad del sistema de gestión de red: Creación de usuarios y grupos, y acceso a los recursos administrados, como se muestra en la figura 4.10a y 4.10 b.

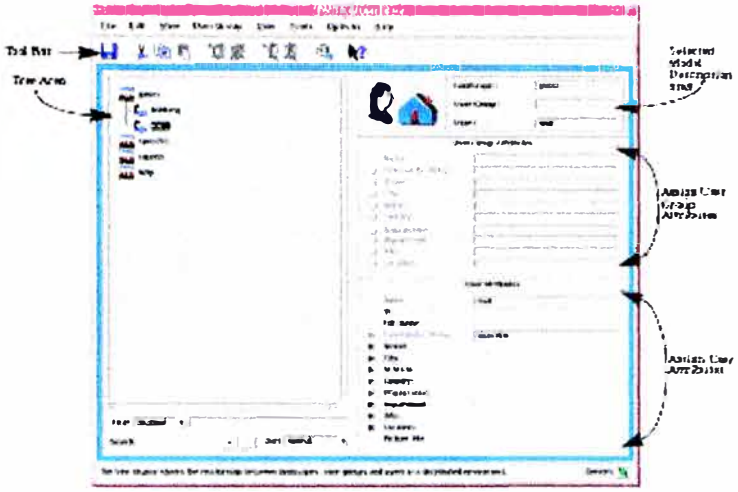


Figura 4.10a Interfaz grafica de creación de usuarios

Figura 4.10b Vista grafica de la estructura jerarquica de usuarios, basado en privilegios

9) Luego de culminar con la instalación y configuración del SPECTRUM, es recomendable realizar una copia de respaldo de las bases de datos. Considerar la arquitectura del sistema de BD que utiliza para realizar las copias de respaldo. La figura 4.11 y 4.12 muestran la arquitectura del software de gestión enfatizando la BD que maneja. Haga uso de la interfaz gráfica mostrada en la figura 4.13 para hacer la copia de respaldo.

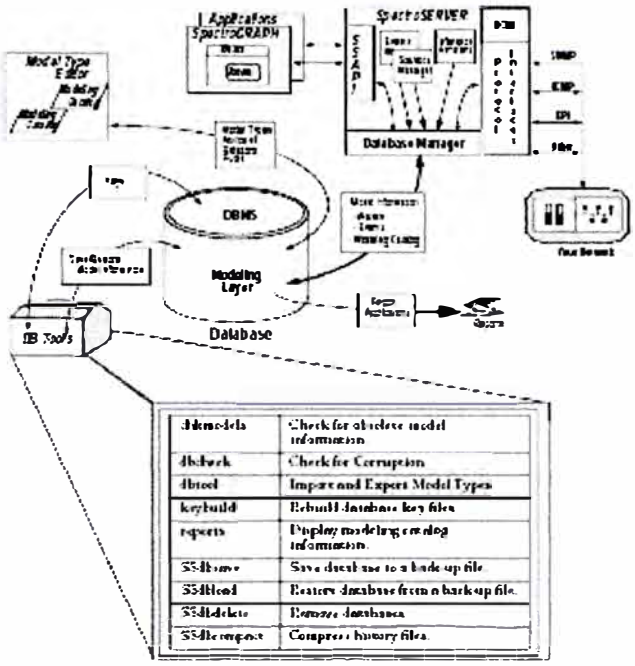


Figura 4.11 Arquitectura de la BD SPECTRUM

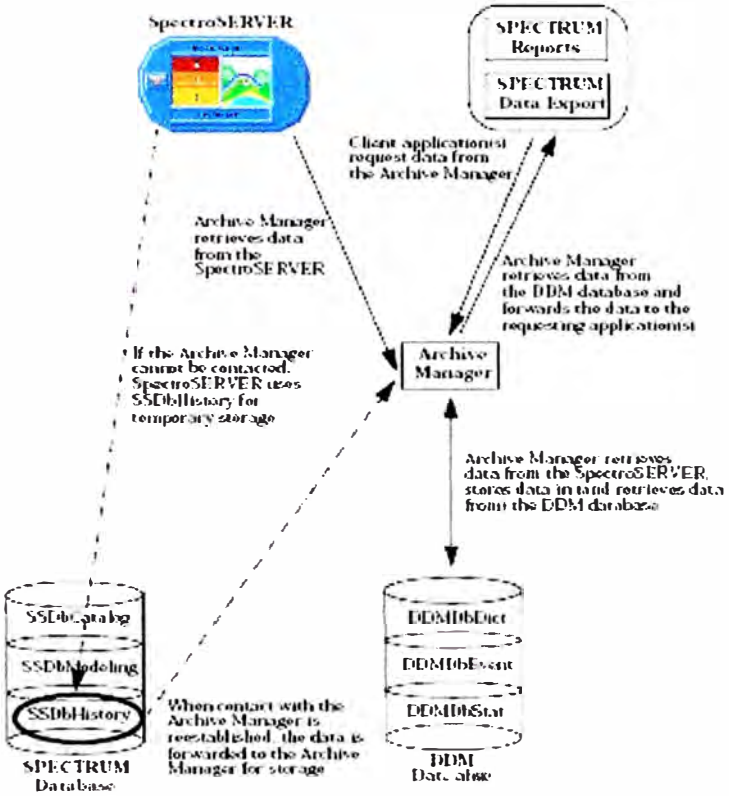


Figura 4.12 Modelo de acceso a las BD SPECTRUM

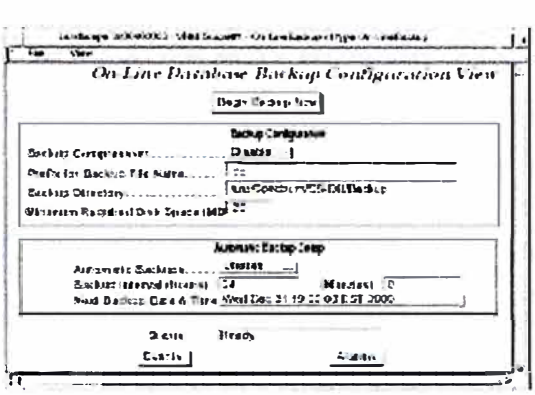


Figura 4.13 Interfaz gráfica para la realización de las copias de respaldo.

b) VLAN MANAGER:

1) Ejecutar la herramienta de autodescubrimiento, para descubrir a cada uno de los nodos UPLINK y SWITCH Ethernet.

El proceso de autodescubrimiento lograra descubrir a cada dispositivo ethernet conectado del switch ethernet tales como HUBs, servidores, y PCs de usuario final. Todos los dispositivos descubiertos inicialmente se encontraran en la VLAN BASE que es la VLAN por omisión.

La herramienta de autodescubrimiento descubrirá también las VLAN creadas previamente, si no hay una creación previa se podrá crear desde este punto. La figura 4.14 muestra las interfaces del gestor de VLANs, conteniendo la información gráfica relativa al descubrimiento realizado. Por un lado las VLANs y por otro los switchs descubiertos y los detalles de los dispositivos conectados a sus diferentes puertos.

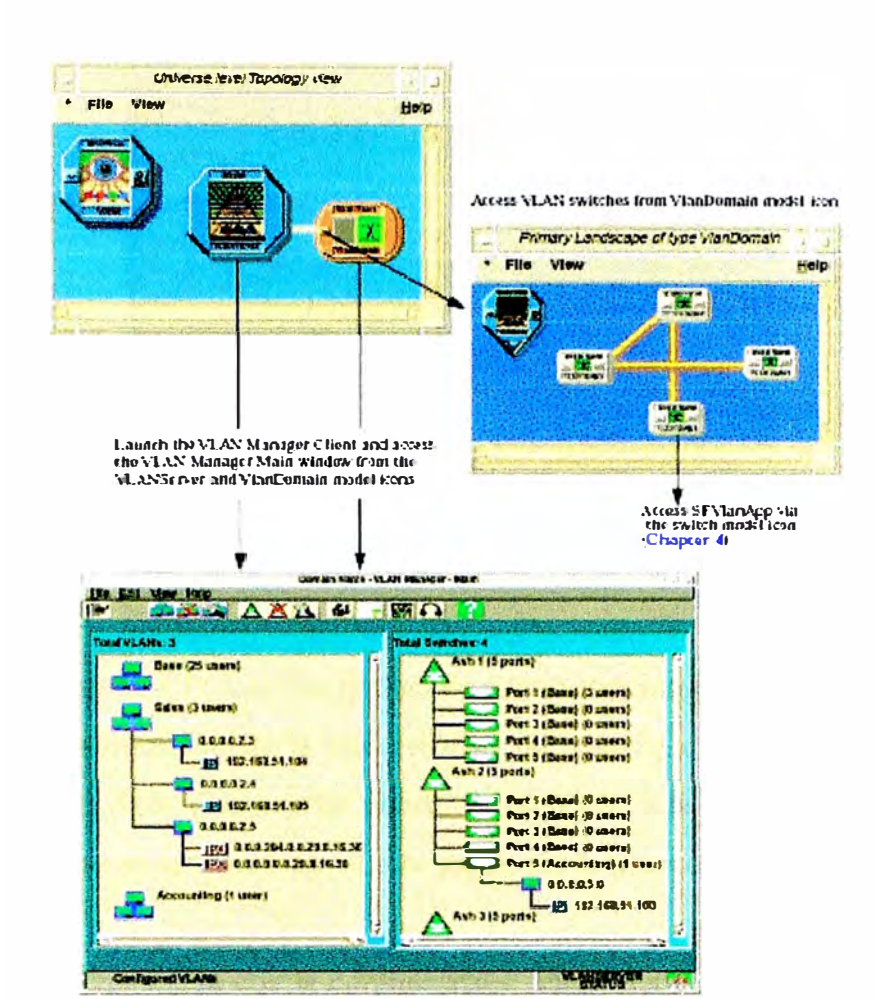


Figura 4.14 Descubrimiento de VLANs

2) Una vez que las VLAN han sido creadas o descubiertas, se debe realizar la configuración de la pertenencia de puertos a VLAN, de acuerdo con el plan de pertenencia a VLANs. En la interfaz gráfica mostrada en la figura 4.15, realizara la pertenecia a VLANs mediante la selección y arrastre del icono correspondiente.

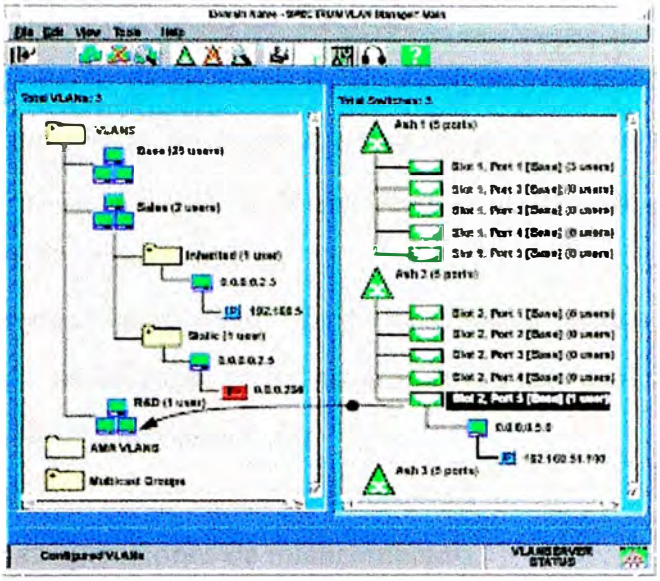


Figura 4.15 Interfaz gráfica de administración de VLANs

3) Para la verificación de la conectividad de hosts que se encuentran en la misma VLAN, de debe disponer un puerto de conexión a la red con una PC de prueba, este puerto se cambiará de VLAN según sea la prueba que se realice.

4) Una vez culminada con la configuración inicial del gestor de VLAN, se obtendrá una copia de respaldo, para poder realizar el restablecimiento a partir de esta copia en caso de corrupción de las Bases de datos. Las interfaces gráficas mostradas en la figura 4.16 nos permitiran las copias de respaldo.

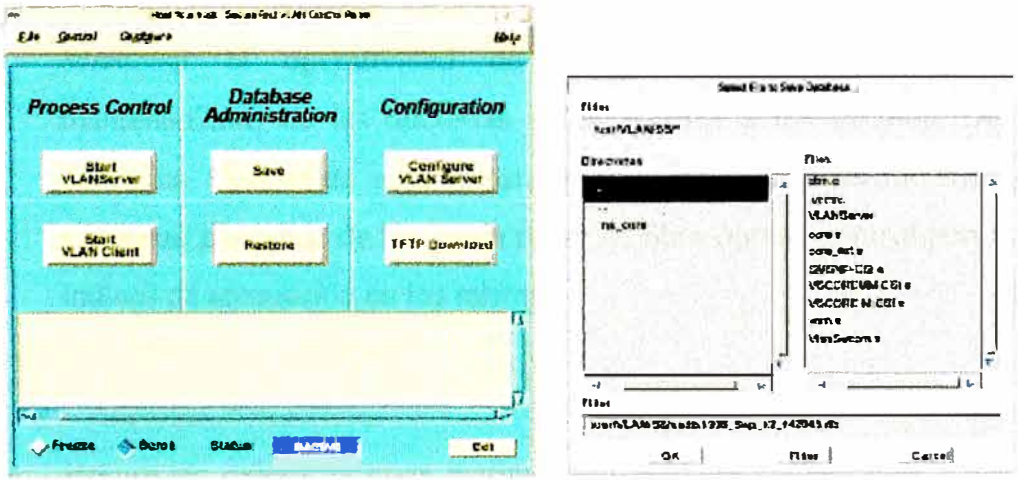


Figura 4.16 Interfaz de copia de respaldo.

4.3 Acciones Operativas en el Centro de Gestión.

- Monitoreo permanente de cada uno de los componentes constituyentes de la red de campus, siendo prioritario los equipos y enlaces que componen el backbone.
- Reporte cada 3 horas del estado de los equipos principales y sus parámetros más relevantes que definen su operación.
- Monitoreo permanente de cada uno de los servidores, verificación de :
    - Actividad: verificación de los estados de los procesos.
    - Carga: número de conexiones
    - Verificación de registros de eventos: logs.
    - Coordinar operaciones de mantenimiento.

- Atención permanente del helpdesk a través del teléfono y una dirección de correo electrónico. Para una posterior coordinación con el administrador de red, administrador de sistemas operativos y soporte técnico.
- Atención de los reportes de incidentes (interrupción de servicio, solicitud de nuevos servicios, etc.).

4.3.1 Planes operativos frecuentes

a) Medios de Transmisión

Fibra óptica

- Acciones Preventivas

  Mantener la operatividad de los mismos, mediante actividades de mantenimiento de las ducterias y los accesos a los mismos. Desratización periódica. Control de nuevas instalaciones que utilizan las ducterias.

  Limpieza periódica de los patch panel de fibra óptica, control periódico de los índices de atenuación en los mismos.

- Acciones correctivas

  Rotura de cables a nivel match panel: uso de los pares de fibra óptica de respaldo. Tiempo de solución estimado a partir del diagnostico: 30 minutos.

Rotura fuera de patch panel: empalme de la fibra óptica, transitoriamente, hasta que sea reemplazado como solución permanente. Tiempo de solución estimado a partir del diagnostico: 24 horas.

Monitoreo permanente de los enlaces que componen el backbone, que conectan los nodos principales (B, N, G, Q), así como los enlaces que unen a los nodos secundarios con los nodos principales.

Cable UTP

Monitoreo del estado, a través de la actividad del usuario, cada vez que un usuario se conecta a la red el sistema deberá mostrar la conexión establecida, la detección de falla se realizara luego de que este sea reportado.

- Acciones Preventivas:

  Limpieza periódica de los match panel y control de los rotulados.

  Control Periodicote pruebas de categoría.

- Acciones correctivas:

  Rotura de cables o desconexión a nivel de match panel y/o Jack RJ45 en el área de trabajo: 1 hora.

  Rotura de cables fuera de patch panel o Jack RJ-45 en el área de trabajo cambio de cableado: 6 horas.

b) Equipos

SWITCH ATM

Monitorear permanentemente:

Rendimiento del switch ATM

- Tasa de bits por segundo de cada puerto, tasa máxima 155Mbps(OC3).
- Número de circuitos virtuales
- Actividad del CPU

Condiciones ambientales

- Temperatura
- Humedad

Alimentación eléctrica del chasis donde reside el switch.

Configuración del Switch.

Acciones Preventivas:

- Limpieza periódica del chasis.
- Control periódico del potencial a tierra.
- Reboteo periódico programados de los switch´s.
- Actualización del FIRMWARE.
- Control periódico de las fuentes redundantes.

Acciones Correctivas:

- Corrupción del Firmware: recarga desde el servidor TFTP del sistema operativo, tiempo estimado 15 minutos.
- Corrupción o perdida del archivo de configuración: recarga desde el servidor TFTP, tiempo estimado 15 minutos.
- Corrupción de la tabla de conmutación ATM: reboteo del shitch al vació, sin los nodos conectados, tiempo estimado 5 minutos.
- Falla de la memoria Flash que almacena el FIRMWARE: reemplazo, tiempo de obtención de la memoria, 15 días. Temporalmente puede cargarse el sistema operativo y al archivo de configuración desde el servidor TFTP.
- Falla de la fuente de alimentación: automáticamente entra en operación la fuente redundante, cambiar la fuente dañada. Tiempo de reemplazo 15 días.

UPLINK ATM

Monitoreo permanente:

- Rendimiento del UPLINK
- Número de circuitos virtuales
- Número de entradas en la tabla circuitos virtuales, MAC address y pertenencia a VLAN.
- Porcentaje de carga del procesador.

Acciones preventivas

- Limpieza de las tarjetas insertadas en el chasis.
- Limpieza de las tablas de conmutación, periódicamente (cada mes o 3 meses).

Acciones Correctivas

- Corrupción del Firmware: iniciar recarga desde la red usando las copias de respaldo.
- Corrupción o perdida del archivo de configuración: iniciar recarga desde la red usando las copias de respaldo.
- Falla de la memoria Flash que almacena el FIRMWARE: Coordinar la obtención con telefónica y realizar los cambios correspondientes.
- Falla de la fuente de alimentación: reemplazo de la fuente dañada.

SWITCH ETHERNET

Monitorear permanentemente:

- Enlaces con los HUB´s, de acceso de usuario.
- Tasas de colisión en cada segmento.
- Tasas de Broadcast que ingresa y salen de cada puerto.
- Ancho de banda de cada puerto que se esta usando actualmente.
- Capacidad de CPU que se esta utilizando (tasa porcentual de la máxima capacidad).
- Número de entradas en la tabla MAC.

Acciones Preventivas:

- Limpieza de las tarjetas insertadas en el chasis.
- Limpieza de las tablas de conmutación, periódicamente (cada mes o 3 meses).
- Establecer el tiempo de tiempo de envejecimiento de las entradas en la tabla MAC.
- Establecer los umbrales máximos de la tabla de conmutación.

Acciones Correctivas.

- Corrupción del Firmware: iniciar recarga desde la red usando las copias de respaldo.
- Corrupción o perdida del archivo de configuración: iniciar recarga desde la red usando las copias de respaldo.
- Falla de la memoria Flash que almacena el FIRMWARE: Coordinar la obtención con telefónica y realizar los cambios correspondientes.

- Falla de la fuente de alimentación: reemplazo de la fuente dañada.

HUB ETHERNET

Monitorear permanentemente:

- Enlace que lo une al switch de borde
- Tasa de colisiones.
- Tasa de Broadcast.
- Tasa de paquetes (bytes) que ingresan y salen en cada puerto.

Acciones Preventivas:

- Limpieza interna del equipo, así como los puertos de conexión ethernet par trenzado y fibra óptica.
- Actualización de Firmware.

Acciones Correctivas:

- Reemplazo del HUB.

CONCLUSIONES Y RECOMENDACIONES

Podemos concluir que la tarea de diseñar un sistema de gestión de red se convierte en un arte, en que dependiendo del tipo de red gestionada, tipo de equipos, objetivos específicos de la gestión de red, las características del sistema de gestión de red pueden cambiar drásticamente, tanto en su arquitectura de operación así como del software. El modelo de red para el cual se diseño el sistema de gestión de red brinda estrechos márgenes de acción debido a la carencia de redundancia, de esto se desprende que la planificación del sistema de gestión de red va implicar en algunos casos cambios en la topología, número de equipos, características de los equipos con los que la red debe contar para poder satisfacer los requerimientos de rendimiento (disponibilidad, tiempo de respuesta, precisión, Throughput, utilización), elevando por tanto los costos de implementación y mantenimiento. Esto nos lleva a ver en la gestión de red una esencial motivación económica, la cual estará sujeto a una evaluación costo – beneficio. Esta es la razón por la cual en la mayoría de los caso debemos conformarnos con niveles aceptables de rendimiento, esta aceptabilidad esta relacionada con un costo beneficio positivo.

Las diferentes herramientas para la gestión de red están en evolución, por tanto cada vez es posible lograr una mayor precisión en el diagnostico de fallos, en un tiempo reducido.

En el caso de la red campus se recomienda tener redundancia a nivel de los enlaces en la red LAN interna, así como en los equipos que constituyen el nodo principal y en los enlaces hacia el Internet. Esto permitirá mayor rango de acción a los gestores de red, que podrían realizar acciones como redirección de tráfico, disminuyendo los periodos de indisponibilidad.

Bibliografía

1. William Stallings, "SNMP SNMPV2 and RMON", Addison Wesley, 1996
2. Antoni Barba Martí, "Gestión de Red", Alfaomega, 2001
3. Douglas R. Mauro & Kevin J. Schmidt, "Essential SNMP", O´REILLY, 2005
4. Heinz-Ger Hegering & Sebastian Abeck , "Integrated Management of Networked Systems", Morgan Kaufmann Publishers, 1998.
5. Aiko Pras, "Ph. D-thesis : Network Management Architectures", Centre Telematics and Information Tecnology, 1995.
6. Jose Arciniegas & Giovanny Arteaga & Fernando Velez, "Proyecto GETWeb", Universidad del Cauca – Popayán – Colombia, 1999.
7. Luis Guijarro Coloma, "Redes ATM", Ra-Ma, 2000.