UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

GESTION DE REDES, ANALISIS COMPARATIVO DE LOS PROTOCOLOS DE GESTION

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRONICO

PRESENTADO POR:

WILMER VICENTE BERROSPI TAQUIRE

PROMOCIÓN
2002 - I

LIMA – PERÚ
2006

GESTION DE REDES, ÁNALISIS COMPARATIVO DE LOS PROTOCOLOS DE GESTIÓN

A Dios, mis padres y mi esposa, por el amor, la compresión y el apoyo incondicional.

SUMARIO

En muchas empresas informáticas e instituciones, incluso que cuentan con grandes estructuras informáticas y de gestión de datos, un tema poco tratado es el de los estándares y protocolos de gestión de redes.

La evolución de las tecnologías de las comunicaciones hacia redes de servicios integrados conlleva un aumento de complejidad en su gestión. Entendemos por redes de integración de servicios aquellas redes más dinámicas orientadas a la conexión con garantías de calidad de servicio, con un crecimiento en nodos, usuarios y sobretodo en tráfico. Los mecanismos existentes contemplan la gestión desde una óptica básicamente aislada en cuanto a la asignación de anchos de banda, encaminamiento, establecimiento de circuitos y de rutas de respaldo, etc. Por otro lado, dichas gestiones suelen actuar de forma estática, como procesos activados de forma manual y esporádica.

Así pues, nos encontramos ante un nuevo escenario donde se requieren nuevas estrategias que proporcionen a la red el control y el dinamismo que los nuevos servicios requieren.

INDICE

CAPITULOI

INTRODUCCIÓN A LOS ESTÁNDARES DE GESTIÓN DE REDES

1.1 Definición de Gestión de Redes. 2

1.2 ¿Porqué los Estándares de Gestión de Redes Son Necesarios? 2

1.3 Estructura de Gestión OSI. 2

1.4 Base de Infromacion de Gestion (Mannagment Information Base - MIB). 4

1.5 Capas de Arquitectura de Gestión de Red OSI. 5

1.6 Capas de la Arquitectura de Gestión de Red de Internet. 6

1.7 Capas de la Arquitectura de Gestión de Red IEEE (Institute of Electrical and Electronics Engineers). 6

1.8 Gestión de Redes de Telecomunicaciones (Telecommunications Network Management - TMN). 7

CAPITULO II

ESTÁNDAR DE GESTIÓN OSI

2.1 Áreas Funcionales de la Gestión OSI. 9

2.2 La Gestión de Sistemas. 10

2.3 Estructura de Información de Gestión. 11

2.4 La International Telecommunications Union – Telecommunication (Itu-T) y los Estándares de Gestión de Redes. 12

2.5 Los Estándares de la Gestión de Redes Internet. 13

CAPITULO III

SERVICIOS DE LA GESTION OSI

3.1 Uso de los Servicios de la Gestión de Redes OSI. 14

3.2 Definición de Servicios y Especificación de Protocolos. 14

3.3 Protocolos de Internet. 16

CAPITULO IV

LIBRERIA DE OBJETOS Y LA BASE DE INFORMACION DE GESTION (MIB)

4.1 El Propósito de una Base de Información de Gestión (Mib – Management Information Base) 17

4.2 LA MIB de Internet 17

4.3 La MIB RMON (Remote Monitoring). 19

4.4 Manejo de librería de objetos en OSI 21

CAPITULO V

PROTOCOLOS DE GESTIÓN

5.1 Propósito de CMISE y CMIP. 28

5.2 Common Management Information Service Element (CMISE/9595) Y Common Management Information Protocol (CMIP/9596). 28

CAPITULO VI

GESTION DE REDES DE TELECOMUNICACIONES

(TELECOMMUNICATONS MANAGEMENT NETWORK – TMN)

6.1 Introducción. 30

6.2 El Modelo de Gestión Tmn. 32

6.3 El Nuevo Entorno de Gestión. 38

6.4 Nuevos Sistemas De Gestión. 45

6.5 Conclusiones. 56

6.6 Referencias del Capitulo. 57

CAPITULO VII

PROTOCOLOS DE GESTIÓN DE INTERNET

7.1 Modelo de Gestión de Internet. 58

7.2 El Protocolo Simple de Gestion de Redes (Snmp – Simple Network Management Protocol) 59

7.3 El Protocolo de Gestion Snmpv2(Simple Network Management Protocol, Version 2) 65

7.4 El Nuevo Modelo Administrativo. 74

CAPITULO VIII

ANÁLISIS DE PROTOCOLOS DE GESTIÓN

8.1 Protocolo SNMP 76

8.2 Protocolo CMIP/CMIS 77

CONCLUSIONES 78

GLOSARIO DE ACRÓNIMOS 79

BIBLIOGRAFIA 81

PROLOGO

Las redes de telecomunicaciones se han convertido en elementos esenciales en las actividades de las personas que laboran tanto en instituciones estatales y privadas como en sus propios domicilios, utilizando servicios de voz, datos y vídeo. Estas redes aseguran el crecimiento y supervivencia de las organizaciones. Debido a su importancia, surge la necesidad de hacer que los servicios proporcionados por la red sean confiables, que sea posible detectar fallas rápidamente, monitorear desempeño, utilizar eficientemente los recursos de red, administrar la seguridad, entre otras. Es decir, surge la necesidad de gestionar la red de telecomunicaciones.

En el presente informe se describe lo que es la gestión de redes los puntos que debemos tener en cuenta asi como los protocolos que se utilizan para ello, como por ejemplo el protocolo de gestión SNMP (Simple Network Management Protocol).

CAPITULOI

INTRODUCCIÓN A LOS ESTÁNDARES DE GESTIÓN DE REDES

1.1 Definición de Gestión de Redes.

La ISO (*International Organization for Standardization)* define la gestión de red como: "El conjunto de elementos de control y supervisión de los recursos que permiten que la comunicación tenga lugar sobre la red"

La gestión de redes comprende las herramientas necesarias para realizar las siguientes funciones:

- Supervisión de la red.
- Control de los dispositivos de la red.
- Administración de la red

1.2 ¿Porqué los Estándares de Gestión de Redes Son Necesarios?

La gestión de redes juega un papel importante en el buen funcionamiento de las redes y se hace imprescindible su aplicación por las siguientes razones:

- Los sistemas de información, son vitales y están soportados sobre redes.
- La información manejada, tiende a ser cada día mayor y a estar más dispersa.
- Las nuevas tecnologías de red, requieren de una gestión cada vez más especializada, que le permita el empleo eficiente de sus recursos de telecomunicaciones.
- El adecuado empleo de las tecnologías de gestión de red, permite mejorar la eficiencia, disponibilidad y el rendimiento de las redes, aumentar la relación calidad / costo en el diseño de las redes, así como aumentar la satisfacción de los usuarios por el servicio de red proporcionado.

1.3 Estructura de Gestión OSI.

Veremos dos tipos de estructura:

1.3.1 Estructura Estática

Cada factor, criterio o métrica puede tener una sub-descomposición. En la Figura 1.1 veremos la posición de cada una.

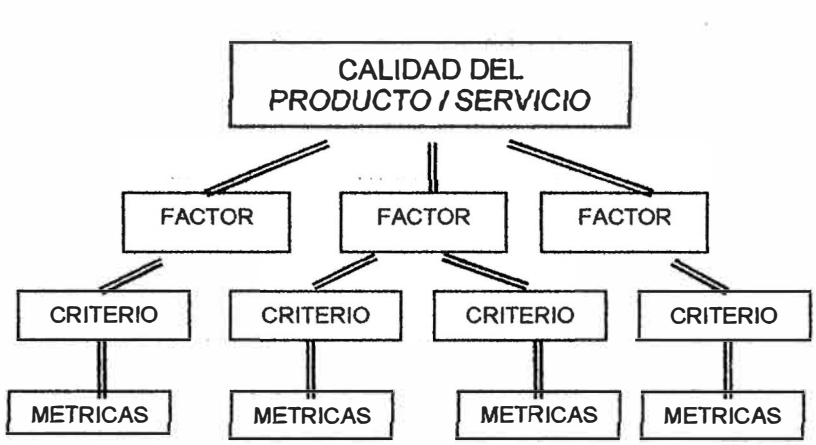

Figura 1.1. Estructura estática de la gestión OSI.

- *Cálculo del valor de calidad*
  - Obtiene dos valores cuantitativos normalizados de métricas.
  - Criterios cuantificados por función de ponderación aplicada a métricas:

    $Ci = c(m1, m2,...,mk)$
  - Factores cuantificados por la función aplicada a los criterios:

    $Fi = f(C1, C2,...,Cl)$
  - Cualidades globales cuantificada por la función aplicada a los factores:

    $Qi = q(F1, F2,...,Fm)$
- Problemas.
  - Gama de valores de métricas y unidades de medición.
  - Utilización de funciones cualesquiera mas fórmulas.
  - Normalización de valores brutos de métricas.
  - Gama de valores muy extensa = poco o ningún significado realista para las cualidades.
  - Normalización dentro de un intervalo finito, por ejemplo [0, 2].
  - Sin intervalo, son escogidos similares para los cuales son atribuidos significados precisos relativos a calidad.

1.3.2 Estructura Dinámica

i. ***Objetos,*** la calidad del modelo son evaluados periódicamente durante el ciclo de vida del producto o servicio.

ii. ***Memoria,*** la calidad en determinado momento es influenciada por la calidad en los momentos anteriores del ciclo de vida.

iii. ***Evaluaciones periódicas de los objetos del modelo***.

iv. ***Validación de la estructura estática***, validación de las métricas y de las heurísticas del modelo.

v. ***Planificación de la gerencia de la calidad,*** control de los costes. Aquí se tiene en cuenta lo siguiente:

- Análisis de tendencias.
- Modulación de los esfuerzos de seguridad y control de calidad, evitando perdida de costos.

vi. ***Costo mínimo,*** el coste mínimo no debe ser necesariamente el único criterio para la adopción de un nivel de calidad de gestión.

vii. ***Costo total,*** el coste total puede ser descompuesto en una estructura arborescente amorfa a la estructura dinámica del modelo de cuantificación de la calidad.

1.4 Base de Información de Gestión (Mannagment Information Base - MIB).

A través del MIB se tiene acceso a la información para la gestión, contenida en la memoria interna del dispositivo en cuestión. MIB es una base de datos completa y bien definida, con una estructura en árbol, adecuada para manejar diversos grupos de objetos (información sobre variables/ valores que se pueden adoptar), con identificadores exclusivos para cada objeto.

La arquitectura SNMP(Simple Network Management Protocol) opera con un *reducido* grupo de objetos que se encuentran definido con detalle en la RFC 1066 "Base de información de gestión para la gestión de redes sobre TCP/IP".

Los 8 grupos de objetos habitualmente manejados por MIB (MIB-I), que definen un total de 114 objetos (recientemente, con la introducción de MIB-II se definen hasta un total de 185 objetos), son:

i. Sistema.
ii. Interfaces.
iii. ATT (Address Translation Table).
iv. IP (Internet Protocol).
v. ICMP (Internet Communication Management Protocol).
vi. TCP (Transmission Control Protocol).
vii. UDP (User Datagram Protocol).
viii. EGP (Exterior Gateway Protocol).

1.5 Capas de Arquitectura de Gestión de Red OSI.

a. Capa aplicación

   Medio para que los programas de aplicación accedan al entorno OSI.

b. Capa de presentación:

   Codificación y formato de los datos, compresión de los datos, cifrado de datos.

c. Capa de sesión:

   Control de diálogo entre aplicaciones, disciplina de diálogo, agrupamiento, recuperación.

d. Capa de transporte:

   Intercambio de datos entre los sistemas finales, libre de errores, en orden, sin pérdidas, sin duplicaciones, calidad de servicio o *QoS.*

e. Capa de red:

   Transferencia de información hasta el destino, las capas superiores no necesitan conocer la transmisión de datos subyacente.

   Tampoco necesitan conocer las tecnologías de conmutación utilizadas para conectar los sistemas.

f. Capa del enlace de datos:

   Proporciona los medios para activar, mantener y desactivar el enlace, detección y control de errores, la capa adyacente superior puede suponer que la transmisión está libre de errores.

g. Capa física:

   Se encarga de la interfaz física entre los dispositivos: mecánica, eléctrica, funcional y de procedimiento.

Figura 1.2. Capas de arquitectura de gestión OSI

1.6 Capas de la Arquitectura de Gestión de Red de Internet.

a. Capa de aplicación:
   Comunicación entre procesos o aplicaciones de computadores separados.
b. Capa de transporte extremo-a-extremo (TCP/UDP):
   Transferencia de datos extremo-a-extremo, puede incluir mecanismos de seguridad (TCP), Oculta los detalles de la red, o redes subyacentes.
c. Capa Internet (IP):
   Encaminamiento de los datos hasta su destino.
d. Capa de acceso a la red:
   Sirve de interfaz lógica entre un sistema final y una subred.
e. Capa física:
   Medio de transmisión, tasa de señalización y codificación.

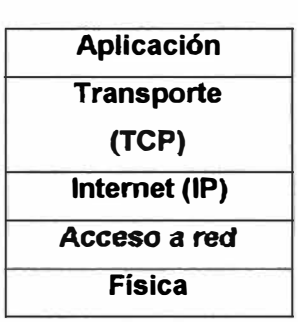

Figura 1.3. Capas de la arquitectura de gestión de Internet.

1.7 Capas de la Arquitectura de Gestión de Red IEEE (Institute of Electrical and *Electronics Engineers*).

a. Físico:
   - Codificación / Decodificación.
   - Generación / Eliminación del preámbulo.
   - Transmisión / Recepción de bits.
   - Especificación del medio de transmisión.
   - *Topología de red.*

b. Control de Acceso al medio-MAC:
   - Ensamblado de datos en tramas (Tx).
   - Desensamblados de tramas (Rx).
   - Control de acceso al medio de Transmisión Lan.

c. Control de Enlace Lógico-LLC:
   - Interfaz con la capa superior.
   - Control de error y de flujo.

d. Protocolos de las capas superiores:

Figura 1.4. Capas de la arquitectura de gestión de red IEEE.

1.8 Gestión de Redes de Telecomunicaciones (Telecommunications Network Management - TMN).

TMN es un estándar de arquitectura, para la gestión de una red telemática, este término fue introducido por la ITU-T en la recomendación M.3010.

El concepto TMN, ha ido evolucionando, en un principio, este estándar no estaba muy bien coordinado / integrado con anteriores documentos como las publicados por otros organismos como ISO o la CCITT (organismo predecesor del ITU-T), no obstante hoy en día TMN ha adquirido y adaptado varios conceptos de la estructura OSI para la gestión de redes, convirtiéndose en prácticamente un estándar de facto en lo que se refiere a herramientas de soporte y mantenimiento de redes en las grandes compañías del sector.

El modelo TMN define tres arquitecturas diferenciadas:

i. ***Arquitectura funcional***, que describe la distribución de la funcionalidad dentro de la TMN, con el objeto de definir los bloques funcionales a partir de los cuales se construye la TMN.

ii. ***Arquitectura física***, que describe los interfaces y el modo en que los bloques funcionales se implementan en equipos físicos.

iii. ***Arquitectura de la información***, que sigue los principios de los modelos OSI de gestión (CMIS y CMIP) y directorio (X.500).

CAPITULO II
ESTÁNDAR DE GESTIÓN OSI

2.1 Áreas Funcionales de la Gestión OSI.

En la Tabla 2.1. se muestra un listado el cual es siempre visto cuando se toca el tema de gestión en OSI.

Tabla 2.1. Comparación entre áreas y funciones

AREAS	FUNCIONES
CONFIGURACIÓN	- Control de las configuraciones Física y lógica - Identificación de los elementos de red - Manipulación de los estados de red - Establecer los parámetros de operación. - Asociar nombres a objetos. - Activar y desactivar objetos. - Recoger información sobre el estado igual. - Recoger avisos de cambios significativos. - Cambiar la configuración del sistema.
FALLAS	- Detección del comportamiento anómalo de redes - Aislamiento de problemas de red y diagnostico - Control y solución de problemas de red - Mantener y examinar registro de errores - Aceptar y actuar ante notificaciones de registro de errores. - Localizar e identificar las averías. - Llevar a cabo secuencias de pruebas de diagnostico. - Corregir las averías.
DESEMPEÑO	- Análisis de la tasas de error en la red - Análisis de la capacidad de la red - Obtención del desempeño óptimo de la red

	- Reunir información estadística. - Mantener y explotar registros históricos del estado del sistema. - Determinar las prestaciones del sistema en condiciones naturales y artificiales. - Modificar la operación del sistema para una correcta gestión de prestaciones.
CONTABILIZACIÓN	- Colecta de datos de utilización de recursos - Procesamiento de los datos de utilización - Informar a los usuarios de los costes en los que han incurrido y de los recursos consumidos. - Establecer limites de coste y programas de tarifas asociados con el uso de los recursos. - Combinar costos de varios recursos cuando un servicio se presta en base a múltiples elementos.
SEGURIDAD	- Control del acceso a la red para operaciones de gerencia. - Activación de servicios y mecanismos de seguridad - Colecta de datos para la auditoria de la seguridad - Crear, borrar y controlar los servicios y mecanismos de seguridad. - Distribuir la información de seguridad. - Informar de los sucesos relativos a la seguridad del sistema.

2.2 La Gestión de Sistemas.

Lo trataremos a partir de sus componentes

Los componentes de un sistema de gestión de red y las relaciones entre ellos se representa en la figura 2.2.

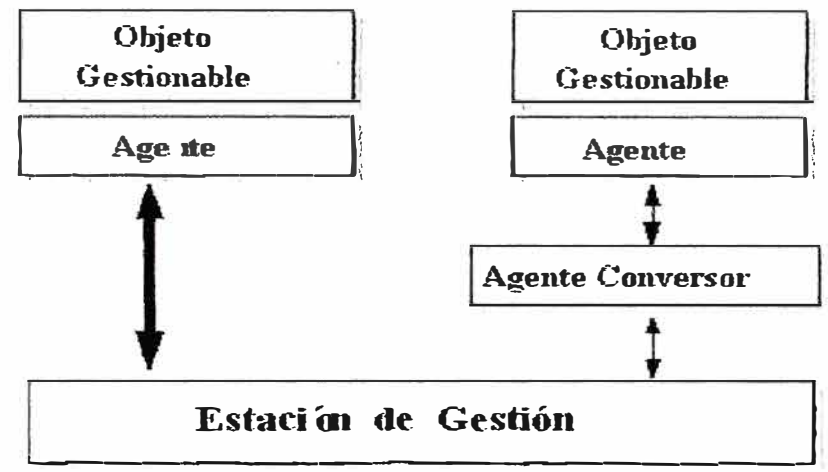

Figura 2.2 Componentes de gestión.

Cada uno de los elementos mostrados en la figura anterior tiene el siguiente significado:

i. ***Objeto Gestionable.***

Representa cualquier dispositivo físico o lógico de la red y el equipamiento lógico relacionado con él, que permita su gestión.

ii. ***Agente.***

Es el equipamiento lógico de gestión que reside en el objeto gestionable.

iii. ***Protocolo.***

Utilizado por el agente para pasar información entre el objeto gestionable y la estación de gestión.

iv. ***Objeto Ajeno.***

Se define como un objeto gestionable que utiliza un protocolo ajeno, es decir un protocolo distinto al de la estación de gestión.

v. ***Agente Conversor.***

Actúa de conversor entre el protocolo ajeno y el protocolo utilizado por la estación de gestión.

vi. ***Estación de Gestión.***

Está formada por varios módulos o programas corriendo en una estación de trabajo u ordenador personal.

2.3 Estructura de Información de Gestión.

SMI("Structure and Identification of Management Information"), SMI define las reglas para describir los objetos gestionados y cómo los protocolos sometidos a la gestión pueden acceder a ellos. La descripción de los objetos gestionados se hace utilizando un subconjunto

de ASN.1("Abstract Syntax Notation 1, estándar *ISO 8824*), un lenguaje de descripción de datos. La definición del tipo de objeto consta de cinco campos:

i. **Objeto**: nombre textual, llamado *descriptor del objeto*, para el tipo del objeto, junto con su correspondiente *identificador de objeto*, definido abajo.

ii. **Sintaxis**: la sintaxis abstracta para el tipo **objeto**. Las opciones son SimpleSyntax (entero, octeto de caracteres, identificador de objeto, Null), ApplicationSyntax (dirección de red, contador, escala, ticks, opaco) u otro tipo de sintaxis de aplicación(ver el RFC 1155 para más detalles).

iii. **Definición**: descripción textual de la semántica del tipo.

iv. **Acceso**: sólo lectura, sólo escritura, lectura - escritura o inaccesible.

v. **Status**: obligatorio, opcional u obsoleto.

2.4 La International Telecommunications Union – Telecommunication (Itu-T) y los Estándares de Gestión de Redes.

La International Telecommunications Union – Telecommunication antes conocida como CCITT (Comite Consultatif Internationale de Telegraphie et Telephonie).Agencia de la Organización de las Naciones Unidas que trata lo referente a telecomunicaciones: crea estándares, reparte frecuencias para varios servicios.

El grupo ITU-T recomienda estándares para telecomunicaciones y está en Génova (Suiza). También se encarga de elaborar recomendaciones sobre *codecs* (compresión / descompresión de audio) y *modems*.

SG2. Grupo de Estudio Líder para definición de Servicio, numbering y routing. Es responsable de estudios que se relacionan con:

i. Los principios de provisión de servicio, definición y las exigencias operacionales de emulación de servicio.

ii. Enumeración, nombramiento, dirección de exigencias y asignación de recurso incluyendo criterios y procedimientos para reserva y asignación.

iii. Encaminamiento e interfuncionalidad de exigencias.

iv. Factores humanos.

v. Los aspectos operacionales de redes y exigencias de funcionamiento asociadas incluyendo dirección de tráfico de red, calidad de servicio (ingeniería de tráfico, funcionamiento operacional y medidas de servicio).

vi. Los aspectos operacionales de interfuncionamiento entre la telecomunicación tradicional conectan una red y el desarrollo de redes.

vii. Evaluación de regeneración de operadores, empresas de la fabricación y usuarios sobre los aspectos diferentes de operación de red.

2.5 Los Estándares de la Gestión de Redes Internet.

Los estándares propuestos, provisionales, y los protocolos estándar figuran en el "Internet Standards Track"("Seguimiento de estándares de Internet"). El seguimiento de estándares es controlado por el *IESG("Internet Engineering Steering Group")* del IETF. Cuando un protocolo alcanza el estado de estándar, se le asigna un número de estándar(STD). El propósito del STD es indicar claramente que RFCs describen estándares de Internet.

Los números STD, referencian múltiples RFCs, cuando la especificación de un estándar está repartida entre varios documentos. A diferencia de los RFCs, donde el número se refiere a un documento específico, los números STD no cambian, cuando un estándar es actualizado.

Sin embargo, los STD carecen de número de versión ya que todas las actualizaciones se hacen a través de RFCs los cuales son únicos. De este modo, para especificar sin ambigüedades a que estándar se refiere uno, el número de estándar y todos los RFCs que incluye deberían ser mencionados.

Por ejemplo, el DNS("Domain Name System") tiene el STD 13, y se describe en los RFCs 1034 y 1035. Para referenciar un estándar, se debería usar una forma como "STD-13/RFC-1034/RFC-1035". Para una descripción de los procedimientos para estándares, remitirse al *RFC 1602 -- Los procedimientos para estándares de Internet - Revisión 2*. Para el seguimiento de algunos estándares, el status del RFC no siempre contiene suficiente información, como para ser útil. Por ello se le añade un *descriptor de aplicabilidad*, dado bien en la forma de STD 1 en un RFC separado; este descriptor lo dan particularmente los protocolos de encaminamiento.

Cuatro estándares de Internet son de particular importancia:

i. STD 1 - Estándares de protocolo oficiales en Internet.

ii. STD 2 - Números asignados de Internet.

iii. STD 3 - Requerimientos de host.

iv. STD 4 - Requerimientos de pasarela.

CAPITULO III

SERVICIOS DE LA GESTION OSI

3.1 Uso de los Servicios de la Gestión de Redes OSI.

i. Nivel de servicio de red

a. Acuerdo / contrato entre A&G de Red y Representación de los Usuarios.

- Acuerdo de Nivel de Servicio.
- Calidad del servicio cuantificada: disponibilidad aceptable = un 90%, tiempo de respuesta < 10 s en un 90% del tiempo.
- Contrapartidas del usuario definidas: nivel de entrenamiento, conocimiento de los procedimientos de registro de incidentes, participación financiera.

b. Mecanismos de evaluación y verificación.

ii. Panel del Nivel de Servicio.

a. Comparar el nivel de servicio cadena con el nivel de servicio previsto en el acuerdo con el usuario.

b. Tener una visión de conjunto de la red en el estado actual.

c. Analizar tendencias.

3.2 Definición de Servicios y Especificación de Protocolos.

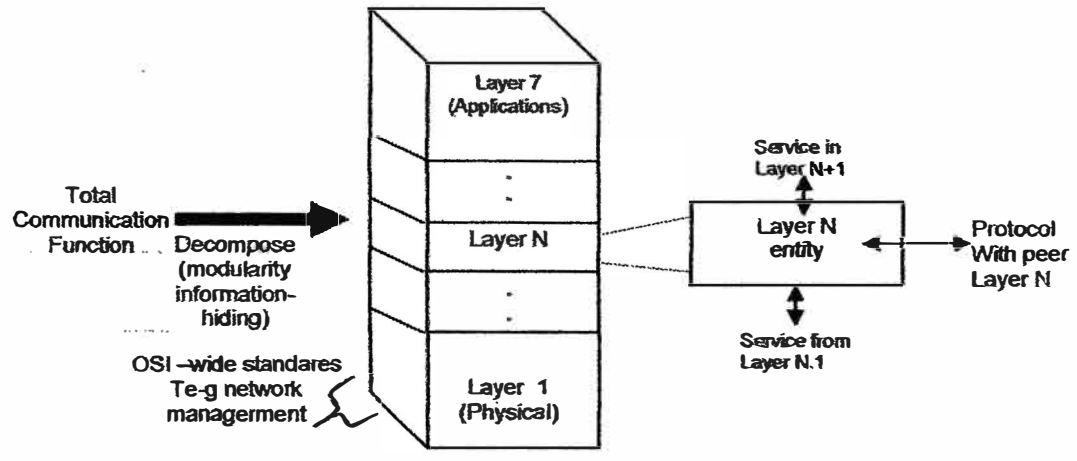

Figura 3.1 Capas

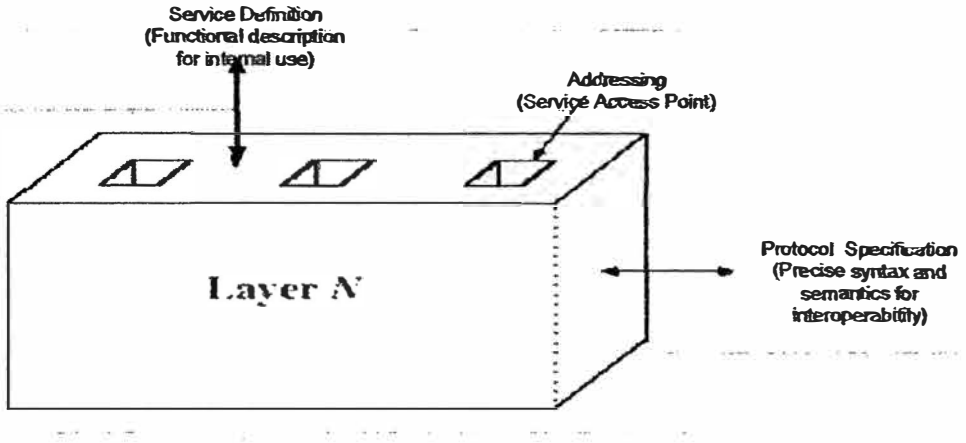

Figura 3.2. servicios

i. Servicio orientado a conexión:
   - Se basa en el modelo telefónico.

ii. Servicio sin conexión:
   - Se basa en el sistema postal.

iii. Primitiva de servicio:
   - Un servicio está formalmente especificado por primitivas (operaciones).
   - Las primitivas indican al servicio que debe realizar una acción o notifican la acción realizada por una entidad par.

En la tabla 3.1 Se muestra algunas definiciones para una entidad, y se hace una lista de lo que significado una operación (primitiva).

Tabla 3.1. Entidad y Operaciones.

Significado	Primitiva
Una entidad	va a ser informada acerca de su solicitud Confirmación o *Confirm*
Una entidad	desea responder a un evento Respuesta o *Response*
Una entidad	es informada acerca de un evento Indicación o *Indication*
Una entidad	desea que el servicio realice un trabajo Solicitud o *Request*

3.3 Protocolos de Internet.

i. **SNMP** (*Simple Network Management Protocol*).es un *protocolo estándar* de Internet. Su status es *recomendado*. Su especificación actual se encuentra en el *RFC 1157 - SNMP("Simple Network Management Protocol")*.

ii. **MIB-II** es un *protocolo estándar* de Internet. Su status es *recomendado*. Su especificación actual se encuentra en el *RFC 1213 - MIB-II:Management Information Base for Network Management of TCP/IP-based Internets.*

iii. **CMIP** (*Common Management Information Protocol*) y CMIS (*Common Management Information Services*) se definen según los estándares ISO/IEC 9595 y 9596.

iv. **CMOT** (*CMIS/CMIP Over TCP/IP*) es un *protocolo propuesto como estándar de Internet*. Su status es *electivo*. Su especificación actual se encuentra en el *RFC 1189 - CMOT y CMIP("Common Management Information Services and Protocols for the Internet")*.

v. **OIM-MIB-II** es un *protocolo propuesto como estándar de Internet*. Su status es *electivo*. Su especificación actual se encuentra en el *RFC 1214 - Gestión OSI Internet Management: MIB("Management Information Base")*. Otros RFCs emitidos por el IAB sobre este tema son:

- RFC 1052 - *Recomendaciones del IAB para el desarrollo de estándares de gestión de red*.
- RFC 1085 - Servicios ISO de presentación sobre redes basadas en TCP/IP.
- RFC 1155 - *SMI("Structure and Identification of Management Information") para redes basadas en TCP/IP*.
- RFC 1156 - *MIB("Management Information Base") para la gestión de redes basadas en TCP/IP*.
- RFC 1215 - *Convenios de definición para SNMP*.
- RFC 1227 - *Protocolo SNMP MUX y MIB*.
- RFC 1228 - *SNMP-DPI("Simple Network Management Protocol Distributed Programming Interface"*.
- RFC 1230 - *IEEE 802.4 Token Bus MIB*.
- RFC 1231 - *IEEE 802.5 Token-Ring MIB*.
- RFC 1239 - *Reasignación de MIBs experimentales a MIBs estándares*.
- RFC 1351 - *Modelo administrativo de SNMP*.
- RFC 1352 - *Protocolos de seguridad SNMP*.

CAPITULO IV
LIBRERIA DE OBJETOS Y LA BASE DE INFORMACION DE GESTION (MIB)

4.1 El Propósito de una Base de Información de Gestión (Mib – Management Information Base)

MIB (Management Information Base) es una norma que define el conjunto de información, acerca de los recursos de la red, que un Sistema de Gestión puede visitar.

A ese conjunto de información se le da el nombre de variable. Cuando son leídas, ellas pasan información acerca de su estado para el sistema gestor (gerente). Este por su parte, puede cambiar sus estados para hacer ejecutar determinadas funciones de gerencia. Determinadas porque cada variable esta relacionada con ciertos detalles de los recursos. Las variables del MIB se encuentran en las unidades a que sean gestionadas.

El formato de la información contenida en las variables son determinadas por una norma denominada SMI.

4.2 LA MIB de Internet

Todos los objetos gestionados en el ambiente de SNMP están ordenados en una estructura de árbol. Las hojas del árbol son los verdaderos objetos gestionados, cada uno de los cuales representa algún recurso, actividad, o información relacionada que será gestionada. La estructura de árbol por sí misma define un agrupamiento de objetos dentro de grupos relacionados lógicamente.

Asociado con cada tipo de objeto dentro de una MIB hay un identificador de objeto (OID) del tipo OBJECT IDENTIFIER de ASN.1. El OID es único para cada tipo de objeto, y sirve para nombrar al objeto. Su valor consiste en una secuencia de enteros denominados sub indentificadores. Como es posible establecer un orden jerárquico a partir de los OID, además de servir para identificar los objetos, los OIDs sirven también para identificar la estructura del árbol.

Comenzando por la raíz (sin nombre) del árbol, cada subidentificador del OID identifica un nodo en el árbol. Hay tres nodos en el primer nivel:

ccitt (0), iso (1), joint-iso-ccitt (2).

Bajo el nodo iso, un subárbol es para uso de otras organizaciones, una de las cuales es el *U.S.Departament of Defense* (dod). La RFC 1155 asume que un subárbol bajo el nodo dod será ubicado por el *Internet Activities Board* (IAB) como sigue:

internet OBJECT IDENTIFIER ::= {iso (1) org (3) dod (6) 1}.

Entonces, el nodo internet(1) tiene un valor de OID de 1.3.6.1. Este valor sirve como prefijo para los nodos del siguiente nivel inferior del árbol. El documento SMI define cuatro nodos bajo el nodo internet:

- directory(1): reservado para uso futuro con el OSI directory (X.500)
- mgmt(2): usado para objetos definidos en documentos aprobados por el IAB.
- experimental(3): usado para identificar objetos utilizados en experimentos de Internet.
- private(4): usados para identificar objetos definidos unilateralmente por los fabricantes.

En la Figura 4.1 vemos como el nodo internet está ubicado debajo del nodo dod.

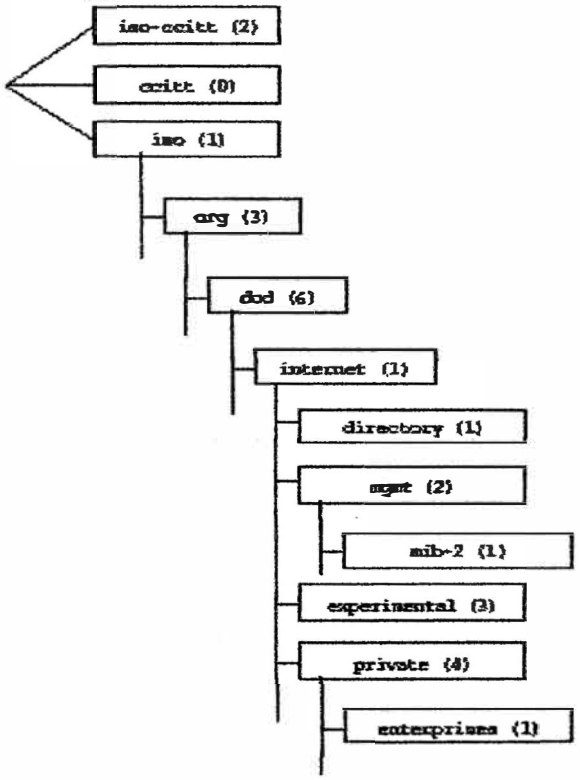

Figura 4.1. Parte del árbol del identificador de objetos (OIDs).

El subárbol mgmt contiene las definiciones de las MIBs que han sido aprobadas por el IAB. Actualmente, dos versiones de la MIB han sido desarrolladas, mib-1 y mib-2. La segunda es una extensión de la primera. Ambas fueron provistas con el mismo OID en el subárbol de modo que sólo puede haber una de las MIBs presentes en cualquier configuración.

Pueden definirse objetos adicionales para una MIB en una de las siguientes formas:

i. Los objetos usados para representar un recurso particular deben ser los mismos en todos los sistemas.

ii. Se debe usar un esquema común de representación de la información para lograr interoperabilidad.

iii. Se puede expandir el subárbol mib-2 o reemplazarlo por una nueva revisión (presumiblemente mib-3). Para expandir mib-2 se define un nuevo subárbol. Por ejemplo, la *remote networking monitoring* MIB se define como el decimosexto subárbol bajo mib-2 (mib-2 (16)).

iv. Puede construirse una MIB experimental para una aplicación particular. Los objetos definidos en ella pueden luego ser movidos hacia el subárbol mgmt. Ejemplos de este caso incluyen varias *media transmission* MIBs, una de las cuales es IEEE 802.5 token ring LAN (RFC 1231).

v. Pueden agregarse extensiones privadas al subárbol private. Una que esta documentada como RFC es la MUX MIB (RFC 1227).

El subárbol private tiene actualmente definido sólo un nodo hijo, el nodo enterprises(1). Esta porción del subárbol se usa para permitirle a los fabricantes mejorar la gestión de sus dispositivos y compartir esta información con otros usuarios y fabricantes quienes pueden necesitar interoperar con sus sistemas. Se asigna una rama dentro del subárbol enterprises a cada fabricante que se registre por un OID enterprises.

4.3 La MIB RMON (Remote Monitoring).

Además de los mencionados en la primera parte, ciertos fabricantes están cooperando para el desarrollo de extensiones particulares para ciertas clases de productos y la gestión remota de dispositivos, conocidas como **RMON (*Remote MONitor*)**, normas RFC 1757

(antes 1271) para Ethernet y RFC 1513 para Token Ring del IETF (*Internet Engineering Task Force*), que incluyen sobre unos 200 objetos clasificados en 9 grupos: Alarmas, Estadísticas, Historias, Filtros, Ordenadores, N Principales, Matriz de Tráfico, Captura de Paquetes y Sucesos. Con RMONv2 se decodifican paquetes a nivel 3 de OSI, lo que implica que el trafico puede monitorizarse a nivel de direcciones de red (puertos de los dispositivos) y aplicaciones específicas.

i. Configuración Interna de MIB – ROM

- Tabla de control: Especifica como funciona un dispositvo monitor.
- Tabla de datos: Contiene los propios datos recolectados.
- 9 grupos de información remota de monitores de implementación opcional.

ii. Grupos de información / Funciones.

- ***Estadísticas***: paquetes (numero / tamaño), colisiones, errores, paquetes descartados.
- ***Histórico***: Contiene los propios datos recolectados.
- Alarmas: Condiciones limites de funcionamiento de la red para notificar (*Trap*), con mecanismo para no inundar de alarmas al gestor de alarmas.
- ***Hosts***: Contador de trafico Entrante/Saliente en las computadoras de la red remota.
- ***Hosts***-TopN: Clasificación de los hosts según cierto criterio, por ejem. Según el trafico saliente.
- ***Matriz***: Matriz de trafico o de errores en las comunicaciones entre pares de Hosts.
- ***Filtro***: condiciones de captura de paquetes para registrar estadísticas de la red remota.
- ***Captura de paquetes***: localización y control de *buffers* para almacenar paquetes.
- ***Eventos***: especificación de eventos que deben provocar envió de notificaciones a los gestores de registro en una tabla (*logTable*) interna del monitor.

4.4 Manejo de librería de objetos en OSI

El MIB define los objetos que pueden ser gestionados para cada capa en el protocolo TCP/IP. Hay dos versiones, MIB-I and MIB-II. MIB-I fue definida en el RFC 1156, y está clasificado ahora como protocolo *histórico con status no recomendado.*

Cada nodo gestionado soporta sólo los grupos apropiados. Por ejemplo, si no hay pasarela, el grupo EGP no tiene por qué estar incluido. Pero si un grupo es apropiado, todos los objetos en ese grupo deben estar soportados.

La lista de objetos gestionados definidos deriva de aquellos elementos considerados esenciales. Este enfoque, consistente en tomar sólo los objetos esenciales no es restrictivo, ya que el SMI proporciona mecanismos de extensibilidad tales como la definición de una nueva versión de MIB o de objetos privados o no estandarizados.

En la tabla de abajo hay algunos ejemplos de objetos. La lista completa está definida en el RFC 1213. Cabe señalar que cada fila representa a un grupo de objetos.

Tabla 4.1. MIB - II("Management Information Base II") - Definición de grupo donde #: Numero de objetos en el grupo.

Group	Objects for	#
system	basic system information	7
interfaces	network attachments	23
at	address translation	3
ip	internet protocol	38
icmp	internal control message protocol statistics	26
tcp	transmission control protocol	19
udp	user datagram protocol	7
egp	exterior gateway protocol	18
transmiss.	transmission. Media-specific	0
snmp	snmp applications entities	30

En la tabla 4.1 hay algunos ejemplos de objetos. La lista completa está definida en el RFC 1213. cabe señalar que cada fila representa a un grupo de objetos .

Cada objeto dentro de la SNMP MIB se define de un modo formal. La definición especifica el tipo de dato del objeto, sus estados permitidos y rangos de valores, y su relación con otros objetos dentro de la MIB. La notación ASN.1 se usa para definir cada

objeto individual y también para definir la estructura completa de la MIB. Para mantener la simplicidad sólo se usa un subconjunto de elementos y características de ASN.1. A continuación se describen los tipos de datos permitidos y se mencionan sus usos más comunes:

4.4.1 Tipos Universal.

La clase UNIVERSAL de ASN.1 está formada por tipos de datos independientes de la aplicación para uso general. Dentro de esta clase, sólo los siguientes tipos de datos están permitidos para definir objetos de MIB:

- integer (UNIVERSAL 2)
- octetstring (UNIVERSAL 4)
- null (UNIVERSAL 5)
- object identifier (UNIVERSAL 6)
- sequence, sequence-of (UNIVERSAL 16)

Los cuatro primeros son tipos primitivos que sirven como bloques de construcción básicos de otros tipos de objetos. El último ítem en la lista menciona los tipos constructores sequence y sequence-of, los cuales se usan para construir tablas, como veremos luego.

4.4.2 Tipos de Application-Wide.

La clase APPLICATION de ASN.1 consta de tipos de datos que son relevantes para una aplicación particular. Cada aplicación, incluyendo SNMP, es autora de sus propios tipos de datos APPLICATION. La RFC 1155 lista un conjunto de tipos de datos application-wide para SNMP; otros tipos podrán definirse en futuras RFCs. Los siguientes tipos están definidos:

- ***networkaddress***: este tipo se define usando el constructor CHOICE, permitiendo la selección de un formato de dirección dentro de un número de familias de protocolos. Actualmente, la única dirección definida es IpAddress.
- ***ipaddress***: es una dirección de 32 bits usando el formato especificado en IP.
- ***counter***: es un entero no negativo que se puede incrementar pero no decrementar. Se especifica un valor máximo de 232 – 1; cuando el counter alcanza su máximo, comienza a incrementarse nuevamente desde cero.
- ***gauge***: es un entero no negativo que puede incrementarse o decrementarse, con un valor máximo de 232 – 1. Si se alcanza el valor máximo, mantiene el mismo hasta ser reseteado.

- ***Instancia de Macro***: una instancia generada a partir de una definición de macro específica suministrando los argumentos para los parámetros en la definición de macro; especifica un tipo particular.
- ***Valor de una Instancia de Macro***: representa una entidad específica con un valor específico.

La macro usada para las MIBs SNMP fue definida inicialmente en la RFC 1155 (Structure of Management Information) y luego extendida en la RFC 1212 (Concise MIB Definitions). La versión en la RFC 1155 se usa para definir objetos en la MIB-I. La versión en la RFC 1212, que incluye más información, se usa para definir objetos en la MIB-II y otras adiciones recientes a la MIB. La figura 4.2 muestra la definición de la macro OBJECT-TYPE en la RFC 1212.

Los principales componentes son los siguientes:

- SYNTAX: la sintaxis abstracta para el tipo de objeto. Ésta debe determinar una instancia del tipo ObjectSyntax definido en la RFC 1155 (ver Cuadro 4.2). La sintaxis debe construirse usando los tipos universal y application-wide permitidos en la SMI.
- ACCESS: define la forma en la que puede accederse una instancia de un objeto, mediante SNMP u otro protocolo. La cláusula access especifica el mínimo nivel de protección requerido por este tipo de objeto. Se permiten adiciones o restricciones específicas de la implementación al acceso. Las opciones son *read-only*, *read-write*, *write-only* y *notaccessible*.
- STATUS: indica el soporte de implementación requerido por el objeto. Puede ser *mandatory* u *optional*. Alternativamente, un objeto puede especificarse como *deprecated*. Esto significa que debe ser soportado, pero que debería ser removido de la próxima versión de la MIB. Finalmente, el status puede ser *obsolete*, que significa que los sistemas gestionados no necesitan implementar más ese objeto.

En el siguiente cuadro se muestra una macro como ejemplo de un objeto.

- ***timeticks***: es un entero no negativo que cuenta el tiempo en centésimas de segundos desde el momento referenciado en la definición de un objeto que utilice este tipo.
- ***opaque***: este tipo soporta la capacidad de pasar datos arbitrarios. El dato es codificado como OCTET STRING para la transmisión. El dato en sí mismo puede estar en cualquier formato definido por ASN.1 u otra sintaxis

El counter es uno de los tipos más comúnmente utilizados en la definición de objetos. Las aplicaciones típicas son contar el número de paquetes u octetos que fueron enviados o recibidos. Como el counter sigue contando desde cero una vez que alcanzó su máximo, el sistema de gestión debe ser capaz de distinguir si un valor x significa x o (N * 232) + x. La única manera que la estación de gestión tiene para poder distinguir el valor correcto es encuestar periódicamente el objeto para mantener el valor N actual. Como se usan contadores de 32 bits, esto no tiene que hacerse muy frecuentemente.

El gauge se usa para medir el valor actual de alguna entidad, como ser el valor actual de paquetes almacenados en una cola. Puede también usarse para guardar la diferencia en el valor de alguna entidad desde el comienzo hasta el final de un intervalo de tiempo. Esto habilita al gauge para ser usado como monitor de la tasa de cambio del valor de una entidad.

El tipo timeticks es un timer relativo. El tiempo se mide en relación a algún evento (como ser un arranque o una reinicialización) dentro del sistema gestionado. Los valores de los timers en un sistema no pueden ser comparados con valores de timers en otro sistema. Un tipo de timer absoluto es impracticable en SNMP debido a que la mayoría de los sistemas que corren la suite de protocolos TCP/IP no soportan un protocolo de sincronización de tiempo.

4.4.3 Definición de Objetos.

Cada objeto está definido por un tipo y un valor. El *tipo del objeto* define una clase particular de objeto gestionado. La definición de un tipo de objeto es entonces una descripción sintáctica. Una *instancia de un objeto* es una instancia particular de un tipo de objeto que ha sido ligada a un *valor*.

SNMP usa una macro para definir un conjunto de tipos de objetos relacionados utilizados en la definición de objetos gestionados. Tenemos los siguientes niveles de definición:

- ***Definición de Macro***: especifica la sintaxis de un conjunto de tipos de objetos relacionados.

- ***Instancia de Macro***: una instancia generada a partir de una definición de macro específica suministrando los argumentos para los parámetros en la definición de macro; especifica un tipo particular.
- ***Valor de una Instancia de Macro***: representa una entidad específica con un valor específico.

La macro usada para las MIBs SNMP fue definida inicialmente en la RFC 1155 (Structure of Management Information) y luego extendida en la RFC 1212 (Concise MIB Definitions). La versión en la RFC 1155 se usa para definir objetos en la MIB-I. La versión en la RFC 1212, que incluye más información, se usa para definir objetos en la MIB-II y otras adiciones recientes a la MIB. La figura 4.2 muestra la definición de la macro OBJECT-TYPE en la RFC 1212.

Los principales componentes son los siguientes:

- SYNTAX: la sintaxis abstracta para el tipo de objeto. Ésta debe determinar una instancia del tipo ObjectSyntax definido en la RFC 1155 (ver Cuadro 4.2). La sintaxis debe construirse usando los tipos universal y application-wide permitidos en la SMI.
- ACCESS: define la forma en la que puede accederse una instancia de un objeto, mediante SNMP u otro protocolo. La cláusula access especifica el mínimo nivel de protección requerido por este tipo de objeto. Se permiten adiciones o restricciones específicas de la implementación al acceso. Las opciones son *read-only*, *read-write*, *write-only* y *notaccessible*.
- STATUS: indica el soporte de implementación requerido por el objeto. Puede ser *mandatory* u *optional.* Alternativamente, un objeto puede especificarse como *deprecated.* Esto significa que debe ser soportado, pero que debería ser removido de la próxima versión de la MIB. Finalmente, el status puede ser *obsolete*, que significa que los sistemas gestionados no necesitan implementar más ese objeto.

En el siguiente cuadro se muestra una macro como ejemplo de un objeto.

Cuadro 4.2 Macro para objetos gestionados (RFC 1212).

```
IMPORTE ObjectName,      ObjectSyntax  FROM RFC-1212-EMI

OJECT-TYPE MACRO ::"
BEGIN
        TYPE NOTATION ::"          "SYNTAX"          Type{TYPE ObectSyntax}
                                   "ACCESS"          Access
                                   "STATUS"          Status
                                   DescrPart
                                   ReferPart
                                   IndexPart
                                   DefValPart
        VALUES NOTATION ::= value {VALUE ObjectName}

        Access ::= "read-only"|"read-write"|"write-only"|"not-accssible"

        Status ::= "mandatory"|"optional"|"obsolete"|"deprecated"

        DescrPart ::= "DESCRIPTION" value {description DisplayString}|empty

        ReferPart ::= "REFERENCE" value {reference DisplayString}|empty

        IndexPart ::= "INDEX" "{" IndexTypes "}"

        IndexTypes ::= IndexType|IndexTypes "."

        IndexType ::= value {indexobkect ObjectName) --if indexobject, use the
                                          --SYNTAX value of the
                                          --correspondent  OBJECT-TYPE
                                          --invocation otherwise use
        |type {indextype}                 --name SMI type: must conform


                                          --to IndexSyntax below

        DefValPart ::= "DEFAL" "{" value ObjectSyntax "}" |empty
        DisplayString ::= OCTECT STRING SIZE {0..255}

END

IndexSyntax ::= CHOICE {   number INTEGER {0..MAX} ,
                           String OBJECT STRING,
                           Object OBJECT IDENTIFIER
                           Address NetworkAddress
                           IpAddress IpAddress }
```

- DescrPart: una descripción textual de la semántica de este tipo de objeto. Esta cláusula es opcional.
- ReferPart: una referencia textual hacia un objeto definido en algún otro módulo MIB.Esta cláusula es opcional.
- IndexPart: usado en la definición de tablas. Esta cláusula debe estar presente sólo si el tipo de objeto corresponde a una fila conceptual. Luego describiremos su uso.
- DefValPart: define un valor por defecto que puede usarse cuando se crea una instancia de un objeto, a juicio del agente. Esta cláusula es opcional

Cuadro 4.3. Estructura de la Información de Gestión (RFC 1155).

```
RFC-1155-SMI DEFINITIONS ::= BEGIN
EXPORTS –EVERYTHING
                    Internet, directory, mgmt experimental, private, enterprises, OBJECT-TYPE, ObjectName, ObjectSyntax, SimpleSyntax,
ApplicationSyntax, NetworkAddress, IpAddress, Counter, Gauge, TimeTicks, Opaque;

-- the path to the root
Internet              OBJECT IDENTIFIER : := {          IS<> ORG(3) dod(6) 1 }
Directory   OBJECT  IDENTIFIER : := { internet 1 }
mgmt                  OBJECT  IDENTIFIER : := { internet 2 }
experimental          OBJECT  IDENTIFIER : := { internet 3 }
private               OBJECT  IDENTIFIER : := { internet 4 }
enterprises OBJECT  IDENTIFIER : := { private 1 }

-- definition of the object types
OBJECT –TYPE MACRO ::=
BEGIN
          TYPE NOTATION       ::=       "Syntax"                type (Type ObjectSyntax)
                                        « ACCESS » Access
                                        « STATUS » Status
          VALUE NOTATION ::=value(VALUE
          Access ::= « read-only » | « read-write "| "write-only" |"not-accessible"
          Status ::= "nandatory"  |"optional"|"obsolete"
END

--names of the objects in the MIB
ObjectName ::- OBJETC IDENTIFIER
-- syntax of objects in the MIB
ObjectSyntax ::= CHOICE {simple SimpleSyntax,
          --note that simple SEQUENCES are not directly mentioned here to keep things
          --simple (i.e., prevent misuse). However, application-which are
          --IMPLICITY encoded simple SEQUENCEE may appear in the following CHICE

                                Application-wide ApplicationSyntax}
SimpleSyntax ::= CHOICE {number integer,
                                String OCTET STRING,
                                Object OBJECT IDENTIFIER
                                Empty NULL}
AplicationSyntax ::= CHOICE { address NetworkAddress,
                                    Counter Counter,
                                    gauge Gauge
                                    ticks TimeTicks,
                                    arbitrary Opaque
                          --other application-wide, as they are defined, will be addid here}
--application-wide types
NetworkAddress ::= Choice {internet IpAddress}

IpAddress ::= [APPLICATION 01                          --in network –byte order
                                IMPLICT OCTET STRING (SIZE(4))

Counter ::= [APPLICATION 1] IMPLICT INTEGER {0..4294967295}
Gauge ::= [APPLICATION 2] IMPLICT INTEGER {0..4294967295}
TimeTicks ::= [APPLICATION 3] IMPLICT INTEGER {0..4294967295}
Opaque ::= [APPLICATION 4] OCTET STRING   --arbitrary ASN.1 value, "double-wrapped"
END
```

El cuadro 4.4 que se muestra a siguiente muestra la definición de un tipo de objeto basado en la macro de definición de objetos

Cuadro 4.4 Ejemplo de una definición de objeto.

```
topMaxConn OBJECT-TYPE
        SYNTAX INTEGER
        ACCESS read-only
        STATUS mandatory
        DESCRIPTION
                "The limit on the number of TCP connections the entity can support. In entities where the
                maximum number of connections is dynamic, this object should contain the value -1."
::={top 4}
```

CAPITULO V
PROTOCOLOS DE GESTIÓN

5.1 Propósito de CMISE y CMIP.

El CMIP es un protocolo de gerencia definida según el modelo OSI. De la misma manera que el CMIP especifica como va a ser realizada el cambio de información entre el gestor y el agente en el Sistema de Gerencia o sea, como el primero visitando y cambiando informaciones que se encuentran en la MIB. Los tipos de información que serán intercambiadas son llevados en cuenta por el CMIS (Common management information service),que especifica el conjunto de servicios que los sistemas de administración y gestión podrán visitar para que sea realizado la gestión. Juntos CMIS y CMIP forman lo que se llama CMISE (Common Management information Service Element).

El CMISE utiliza dos aplicaciones de servicio comunes(Son aplicaciones de servicio común aquellas aplicaciones que ofrecen servicios no solo de aplicaciones de gestión, así como todas las otras.), ACSE y ROSE. La primera trata del establecimiento y liberación de conexiones entre un equipamiento y otro. La segunda ofrece servicios de pedido de operaciones remotas.

5.2 Common Management Information Service Element (CMISE/9595) Y Common Management Information Protocol (CMIP/9596).

El Common Management Information Service Element (CMISE) es especificado en dos documentos de ISO. La definición de servicio para el Common Management Information Service (CMIS) es dado en la ISO 9595 [11].

La especificación para el protocolo Common Management Information Protocol (CMIP) es encontrado en la ISO 9596 [12]. Además, soporta la operación para añadir/quitar de M-Set [32, 34] tambien deben soportar CMOT y CMIP, La estructura para M-Cancel-Get " [33, 35] puede soportar una implementación, pero esto es el empleo negociado como la parte de negociación de asociación.

[11] ISO 9595: "Information Processing Systems - Open Systems Interconnection, Management Information Service Definition - Part 2: Common Management Information Service", 22 December 1988.

[12] ISO 9596: "Information Processing Systems - Open Systems Interconnection, Management Information Protocol Specification - Part 2: Common Management Information Protocol", 22 December 1988.

[32] ISO IS 9595 1989: DAD1: "CMIS Add/Remove Addendum".

[33] ISO IS 9595 1989: DAD2: "CMIS Cancel-Get Addendum".

[34] ISO IS 9596 1989: DAD1: "CMIP Add/Remove Addendum".

[35] ISO IS 9596 1989: DAD2: "CMIP Cancel-Get Addendum"

CAPITULO VI
GESTION DE REDES DE TELECOMUNICACIONES
(TELECOMMUNICATONS MANAGEMENT NETWORK – TMN)

6.1 Introducción.

La gestión de redes y servicios se puede definir como el conjunto de procesos y actividades que realiza una operadora para ofrecer a sus clientes los servicios de telecomunicaciones, de tal forma que se cumplan tanto los criterios de calidad y coste establecidos en los objetivos de la empresa, como los reflejados en los correspondientes contratos con los clientes.

Las redes y servicios de telecomunicaciones surgen para cubrir la necesidad de transportar información entre varias localizaciones separadas físicamente. Por ello, la infraestructura necesaria para prestar estos servicios se encuentra distribuida en un espacio geográfico que puede abarcar miles de kilómetros.

La realización manual de cualquier operación sobre este tipo de infraestructura no es viable, por el tiempo y la cantidad de recursos que se necesitarían. Por ejemplo, ante la aparición de un fallo habría que ir comprobando cada uno de los equipos de la red hasta encontrar el que ha producido el fallo. Si no se dispone de los sistemas de gestión adecuados, debido al tamaño de las redes actuales y al número de equipos de telecomunicaciones que las forman, el tiempo de respuesta al problema sería muy elevado y pudiendo no satisfacer las exigencias del cliente, produciéndose, además, un gran coste de explotación. En un mercado de libre competencia, ambos factores pueden conducir al fracaso de una compañía, por lo que es necesario disponer de sistemas de soporte a la operación que ayuden a realizar todas las actividades de gestión de las redes y servicios.

Sin embargo, los sistemas de gestión por sí solos no son garantía de éxito: disponer de un sistema de gestión para supervisar las alarmas de los equipos de red permite determinar

de forma sencilla el equipo que ha fallado, pero esto no soluciona el problema. Es necesario definir los mecanismos y procedimientos adecuados con la finalidad de llevar a cabo las acciones necesarias para resolver el problema, es decir, hay que definir los procesos de negocio: ¿qué hacer ante una reclamación de usuario?, ¿cómo actuar ante la aparición de una alarma?, etc., y hacer que los sistemas presten el soporte adecuado a estos procesos.

La aparición de los primeros ordenadores dió paso a los primeros sistemas de gestión que automatizaban tareas como el procesamiento de solicitudes de suscripción a los servicios, la monitorización de alarmas, etc. Las compañías operadoras, para aumentar la productividad y reducir los costes, concentraron a su personal en torno a estos sistemas, llegando incluso a estructurar los departamentos en función de estos sistemas. En procesos donde se necesitaba la actuación de varios departamentos, la coordinación se realizaba a través de llamadas telefónicas entre los operadores y el paso de boletines por fax o por una red interna. La integración entre los sistemas era manual y cada operador introducía en su sistema los datos que había recibido por teléfono o por un boletín, lo que favorecía, de forma considerable, la aparición de errores.

A finales de los años 90, en la mayoría de los mercados de servicios de telecomunicaciones se produjo una evolución desde una situación de monopolio hasta un régimen de competencia. En este entorno, ya no es suficiente reducir los costes de explotación, sino que hay que aumentar los ingresos; para ello es fundamental que los clientes asocien la imagen de calidad de los servicios con el nombre de la operadora. Este hecho ha obligado a que las operadoras de telecomunicaciones modifiquen sus estrategias y revisen sus procesos de negocio.

Los procesos de negocio, ahora, deben girar en torno a la atención de los clientes de la compañía, y esta atención requiere la coordinación de todos los departamentos y sistemas involucrados en la prestación de los servicios. Esta coordinación se debe apoyar en la integración de los sistemas de gestión, de forma que se pueda aumentar el grado de automatización de los procesos de negocio, con el objetivo de reducir los errores y los tiempos de resolución de problemas y de provisión. De esta forma se consigue, en esencia, mejorar la calidad de los servicios y a la vez optimizar los costes. En esta línea se dirigen los trabajos del *TeleManagement Forum* (TMF), cuyos resultados más inmediatos se orientan al desarrollo del modelo *Telecommunication Management Network* (TMN) y que se pueden consultar en [1].

6.2 El Modelo de Gestión Tmn.

Las operadoras de servicios de telecomunicación han aceptado ampliamente el modelo de gestión TMN, como forma de estructurar lógicamente el soporte de las actividades necesarias para su negocio. El modelo TMN [3] fue definido por la UIT a mediados de los 80 y proporciona una arquitectura de referencia para el intercambio de información de gestión entre los sistemas de operación y / o los equipos.

El modelo TMN está basado en el modelo OSI para la interconexión de sistemas abiertos, que adopta el modelo gestor-agente para las relaciones entre sistemas o entre sistemas y equipos. El modelo considera la conexión de sistemas desde tres aspectos:

- *Funcional*. Define las actividades que hay que realizar y la organización de las mismas.
- *De información*. Modela la información de gestión que se intercambia entre el gestor y el agente. Este modelo depende de las funciones que se realicen y de los recursos que se quieran gestionar.
- *De comunicación*. Especifica los protocolos de comunicaciones utilizados para el intercambio de información entre sistemas. Su objetivo es permitir la transferencia e interpretación correcta de la información de gestión.

El modelo funcional representa el contexto de una comunicación, ya que un término puede tener diferentes significados según donde se utilice. El modelo de información es la parte semántica de la comunicación, se encarga del significado de cada frase. Por último, el modelo de comunicación define la sintaxis de la comunicación, describiendo su forma.

6.2.1 El modelo funcional

El modelo funcional utiliza las cinco áreas funcionales de OSI para agrupar las funciones de gestión. Estas áreas funcionales están recogidas en la Recomendación M.3400 [4] de la UIT, y son:

- *El área de configuración.* Comprende el conjunto de actividades y funciones cuyo objetivo es proporcionar los servicios solicitados por los clientes.

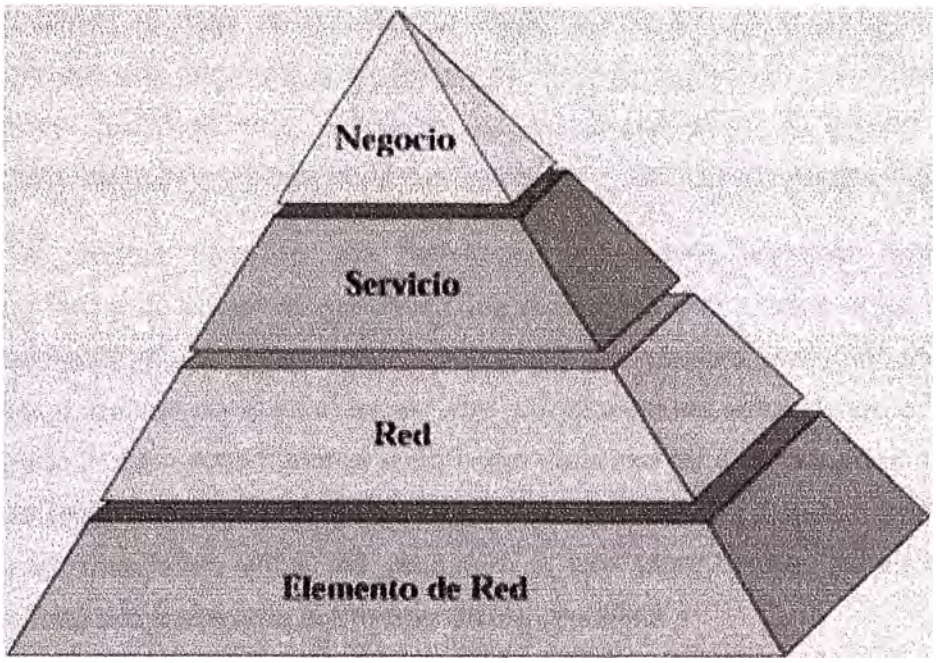

Figura 6.1. El modelo TMN

El nivel superior es el nivel de gestión de negocio que incluye los aspectos relacionados con las estrategias de negocio; en él se definen las acciones para conseguir el retorno de la inversión, aumentar la satisfacción de los accionistas de la compañía y de los empleados, etc. Las decisiones tomadas en este primer nivel definen los objetivos estratégicos de la compañía, y condicionan fuertemente las funciones y procesos de la capa de nivel de gestión de servicio.

En la capa de gestión del nivel de servicio se decide cómo gestionar los servicios que se van a prestar a los clientes. En este nivel se incluyen todos los aspectos relacionados con la atención a los clientes y los de desarrollo y operación de los servicios, y se realiza la gestión de las peticiones de servicio, la calidad del servicio –*Quality of Service* (QoS)–, la gestión de problemas, la facturación, etc.

Los servicios están soportados sobre redes de telecomunicaciones que pueden ser del proveedor de servicio o de otra compañía. El nivel de gestión de red es responsable del transporte de la información entre dos extremos y de asegurar que ésta se realiza de forma correcta. Cualquier error o problema que se detecte en este nivel y que afecte a los servicios que se prestan a los clientes debe ser notificado hacia el nivel de gestión de servicio.

Por último, el nivel de gestión de elemento de red se encarga de todos los aspectos relacionados con conmutadores, sistemas de transmisión, etc., considerados como elementos aislados. Cualquier error o evento que se produzca en un equipo que pueda afectar al transporte de la información debe ser notificado hacia el nivel de gestión de red.

Si bien el modelo TMN es una referencia, que puede seguirse más o menos fielmente, es una forma de poner de manifiesto las relaciones que existen entre las distintas tareas que debe realizar una operadora o proveedor de servicio. Así, por ejemplo, una decisión estratégica tomada en el nivel de servicio, condiciona las actuaciones en los niveles inferiores, pudiendo incluso determinar la instalación en la red de determinados equipos. Por otra parte, utilizar la misma referencia en las diferentes operadoras y proveedores de servicio permite establecer relaciones entre los procesos y, por tanto, entre los sistemas, para asegurar la automatización extremo a extremo de los procesos.

6.2.2 El modelo de información

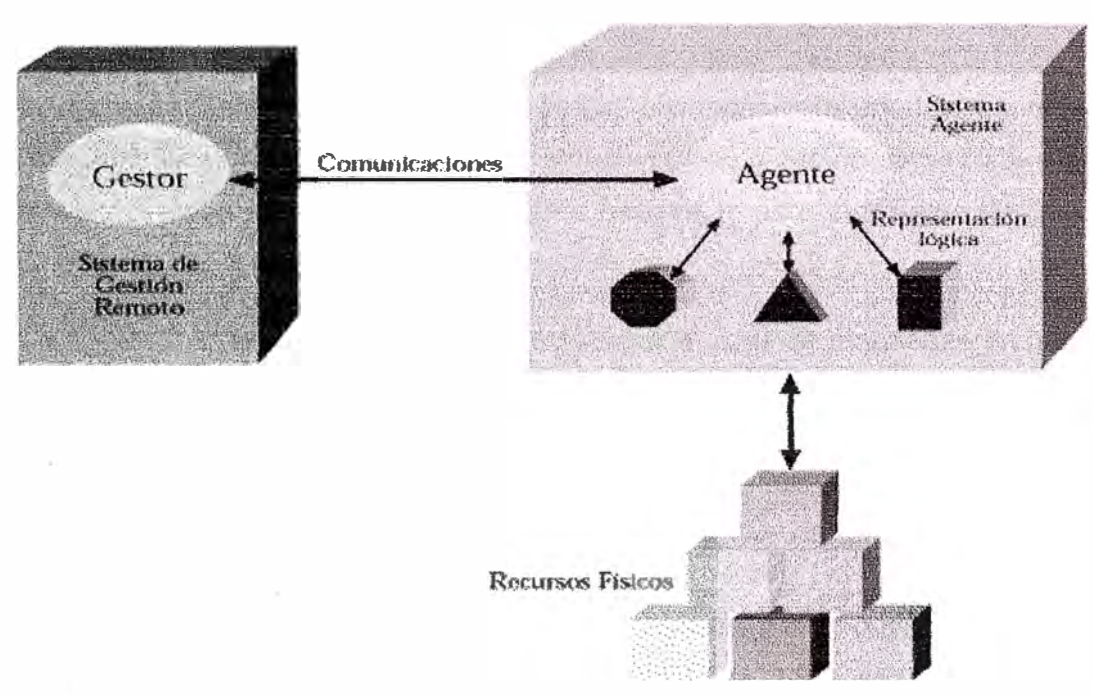

Figura 6.2. ***El modelo gestor-agente***

La comunicación entre el sistema de gestión y los recursos que se gestionan sigue el modelo gestor-agente de OSI, que se puede ver en la Figura 6.2. En este modelo, el sistema de gestión (gestor) no se comunica directamente con los recursos gestionados sino a través otra aplicación (agente) que es la que tiene la responsabilidad directa sobre ellos.

Para que este modelo funcione es necesario incluir el concepto de conocimiento de gestión compartido, de forma que el gestor y el agente tengan la misma visión de los recursos gestionados y de las operaciones que se pueden realizar sobre ellos. El objetivo del modelo de información es proporcionar esta visión común.

La visión de los recursos que hay que gestionar se consigue a través de los objetos gestionados, que son una abstracción de las capacidades de gestión de dichos recursos. Normalmente, los equipos de telecomunicaciones incluyen un gran número de funciones y propiedades, algunas de las cuales no son de interés para la gestión de determinada red o servicio. El objeto gestionado es una visión parcial del recurso, donde sólo se muestran los aspectos de interés para el sistema de gestión.

Desde el principio, el modelo TMN adoptó una tecnología orientada a objetos para definir y modelar la información de gestión. Los recursos se modelan como clases de objetos gestionados, que representan las características relevantes para el sistema de gestión; son, por tanto, una visión parcial de los recursos de red.

Las instancias de todas las clases de objetos definidas se mantienen en una base de datos de información de gestión o *Management Information Base* (MIB), que se organiza siguiendo el árbol de contención y de nombrado de las clases. La MIB forma la base común de conocimiento entre el sistema de gestión y los agentes de gestión.

El sistema de gestión realiza operaciones sobre los objetos gestionados, representados en la MIB, y el agente se encarga de traducir estas operaciones en acciones sobre los recursos físicos de la red. De igual forma, cualquier información que se produce en los elementos de red es enviada al sistema de gestión como una notificación emitida por el objeto gestionado que representa el recurso.

El desarrollo de los modelos se produjo en un momento en que no existían herramientas para diseño orientado a objetos, por lo que fue necesario el desarrollo de

herramientas adecuadas para ello. Se definió el lenguaje GDMO para la definición de las clases de objetos gestionados y sus relaciones, y para la definición de los tipos de los datos se utilizó la notación ASN.1.

Una de las actividades principales de la UIT es la definición de modelos de objetos gestionados, estándares para diferentes tecnologías, que sean utilizados por los fabricantes en sus equipos, de forma que todos presenten la misma visión hacía el sistema de gestión y como consecuencia se simplifique el desarrollo del mismo. La mayoría de los modelos estándares desarrollados hasta la actualidad son para el nivel de elemento de red.

6.2.3 El modelo de comunicaciones

El sistema de gestión y los agentes suelen estar situados en lugares diferentes, y, dado que para realizar su función necesitan intercambiar información entre ellos, es necesario definir los mecanismos de comunicación que se van a utilizar. El modelo de comunicaciones define los protocolos que se utilizan entre el gestor y los agentes, para los siete niveles del modelo OSI, siendo en el nivel de aplicación donde se definen los protocolos específicos para la gestión de redes y servicios. En este nivel se incluye el *Common Management Information Service Element (*CMISE), que se compone del *Common Management Information Service (CMIS*), que especifica los servicios, y el protocolo de comunicaciones *Common Management Information Protocol* (CMIP), que soporta estos servicios.

Las aplicaciones intercambian información utilizando las primitivas de CMIS, que permiten a un gestor conocer y modificar (si está autorizado) el valor de los atributos de un objeto gestionado y ejecutar sobre él las acciones que tenga definidas. De igual forma, los objetos gestionados pueden emitir notificaciones hacia el gestor cuando ocurra algún evento de importancia, pudiendo el gestor definir qué eventos le interesan.

Tanto CMIS como CMIP han demostrado ser bastante potentes y flexibles de usar, aunque algo complejos de implementar. Hay que destacar las posibilidades de ámbito (*scoping*) y de filtrado, que permiten seleccionar un conjunto de objetos gestionados, agrupados por diferentes condiciones, y realizar operaciones sobre el grupo completo.

Las funciones se agrupan para formar sistemas que intercambian información a través de interfaces. Estas interfaces ofrecen a las aplicaciones de gestión, a través del protocolo

las clases contenidas en la MIB. Cuando estas interfaces utilizan un modelo de información estándar se denominan interfaces Q3.

6.3 El Nuevo Entorno de Gestión.

El objetivo principal de TMN es la definición de interfaces estándares entre los diferentes niveles de gestión. Así, se definieron modelos de información para la gestión de elementos de red de varias tecnologías. La idea inicial era poder conectar equipos de varios fabricantes a un único sistema de gestión. La construcción de modelos de gestión en el nivel de red se ha realizado para permitir la gestión coherente de ciertas redes y servicios por un determinado operador, y, por tanto, suelen ser modelos propietarios.

Esta visión desde abajo hacia arriba produce estructuras de gestión verticales, orientadas a un servicio, a una red o a ciertas funciones, según se puede ver en la Figura 6.3. En estructuras de este tipo, la comunicación entre los sistemas de gestión de los distintos departamentos es escasa, siendo el paso de boletines por fax o las llamadas telefónicas entre los operadores el mecanismo común de comunicaciones.

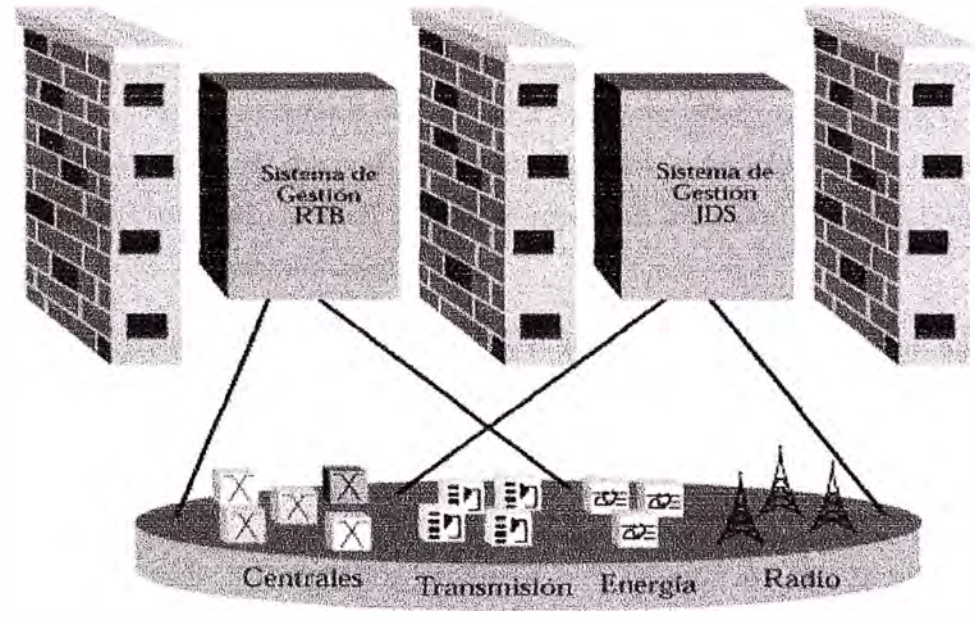

Figura 6.3. ***Arquitectura de gestión monolítica***

Esta estructura de gestión no es viable cuando se multiplican los servicios que se pueden prestar sobre las distintas redes, y cuando la necesidad de dar respuesta inmediata a las solicitudes de los clientes exige un intercambio ágil de información entre los distintos sistemas implicados.

En la actualidad, está aumentando rápidamente la demanda de nuevos servicios de telecomunicación que en muchos casos son integración de otros más sencillos. Este hecho, unido al proceso de desregularización de ámbito mundial de las telecomunicaciones, ha modificado drásticamente el entorno de las empresas de telecomunicaciones, que han pasado de realizar una gestión enfocada hacia la red a una gestión fundamentalmente orientada hacia los servicios y los clientes.

6.3.1 Nuevos servicios y redes.

En un entorno de libre competencia, el lanzamiento de nuevos servicios es una forma de captar nuevos clientes y, como consecuencia, una forma de conseguir una posición mejor en el mercado. Los operadores que quieran sobrevivir en un mercado liberalizado deben tener el suficiente dinamismo y flexibilidad para ofertar a sus clientes nuevos servicios de telecomunicaciones, que le diferencien de otros operadores y poder dar una rápida réplica a los servicios que lancen éstos.

Por otro lado, la creación de nuevos servicios es una forma de aumentar el uso, por parte de los clientes, de los recursos de una operadora de telecomunicaciones. Una mayor utilización de estos recursos supone una amortización más rápida de las inversiones realizadas en infraestructuras, lo cual desde siempre ha sido uno de los objetivos de las compañías de servicios de telecomunicaciones.

En muchos casos, los nuevos servicios son únicamente mejoras sobre ciertos servicios básicos. Ejemplos de estas mejoras son la tarificación detallada o la tarificación por segundos del servicio telefónico básico, e incluso la emisión de la factura integrada o separada por servicios.

En algunos casos, los servicios suponen una integración de otros servicios más simples. Por ejemplo, en la Figura 7.4 podemos observar cómo un servicio de vídeo bajo petición se podría formar con un servicio de transmisión de vídeo a través de una red CATV,

integrado con una red de datos de baja velocidad a través de la RTB y con tarificación integrada en la factura telefónica.

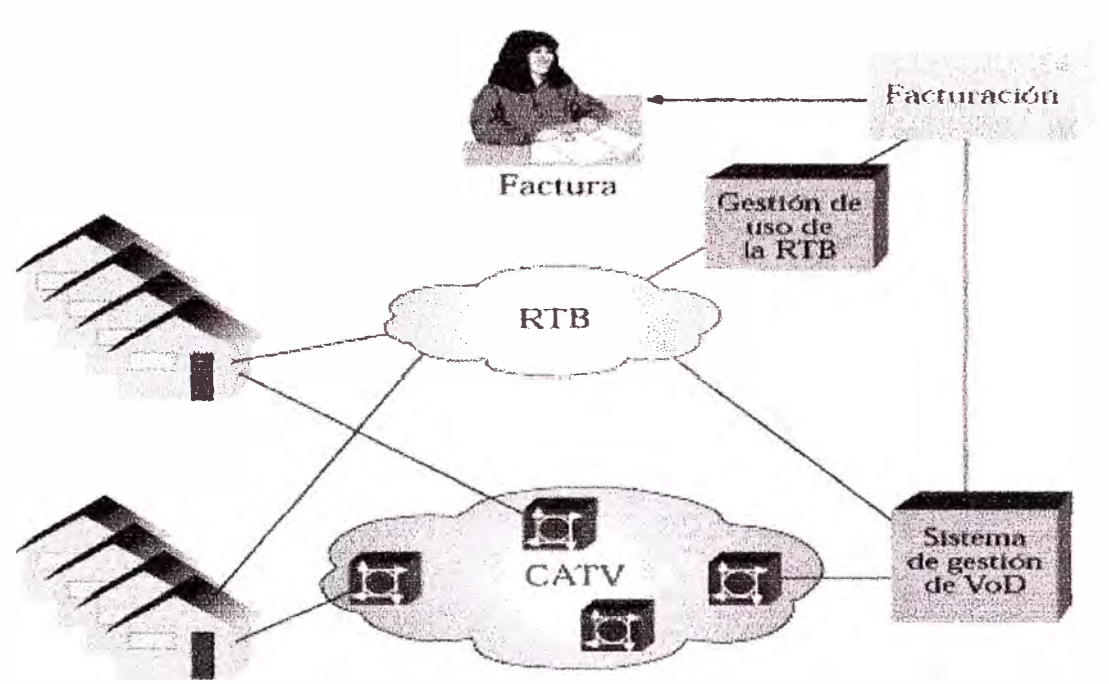

Figura 6.4. ***Creación de nuevos servicios utilizando servicios más básicos***

La gestión de un servicio de este tipo supone que tres sistemas de gestión tienen que interactuar y que, por tanto, existe una necesidad de integración, que en la mayor parte de los casos es compleja por las diferentes plataformas que sirven de base para cada sistema.

Otro aspecto importante es la introducción de redes de banda ancha. Este tipo de redes simplifican la arquitectura de red, puesto que pueden soportar un número considerable de servicios diferentes.

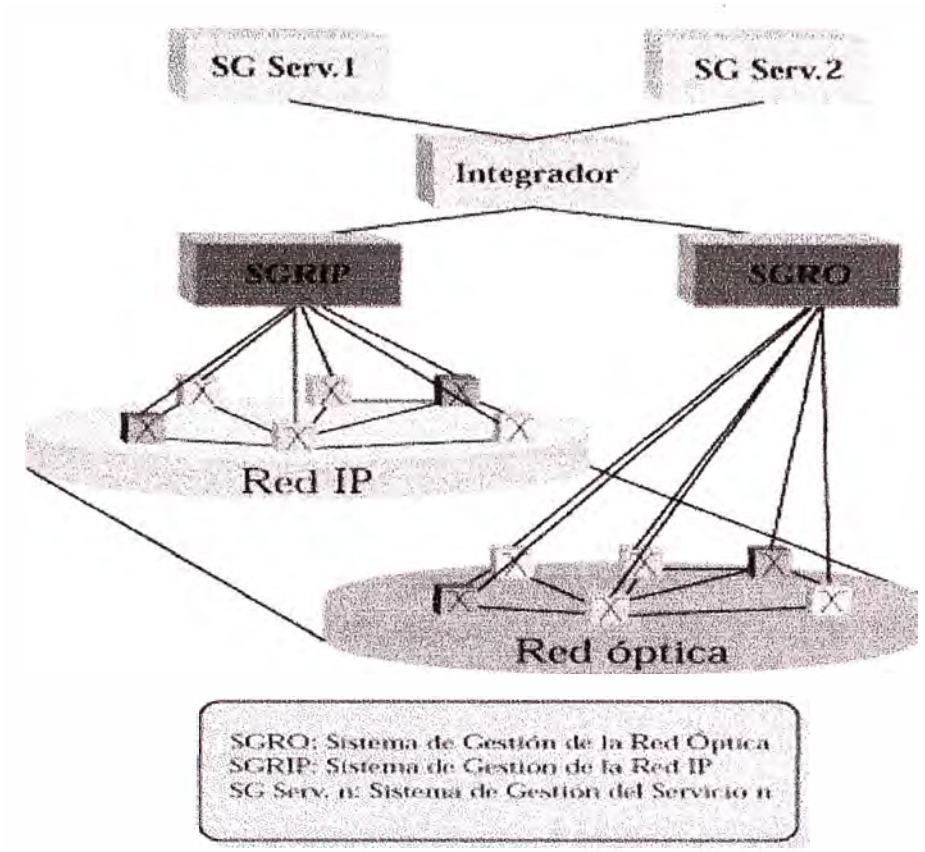

Figura 6.5 ***Arquitectura de red y de gestión para servicios soportados por IP / WDM***

La gestión de un servicio de este tipo supone que tres sistemas de gestión tienen que interactuar y que, por tanto, existe una necesidad de integración, que en la mayor parte de los casos es compleja por las diferentes plataformas que sirven de basa para cada sistema.

Otro aspecto importante es la introducción de redes de banda ancha. Este tipo de redes simplifican la arquitectura de red, puesto que pueden soportar un número considerable de servicios diferentes.

Al concentrar sobre una red varios servicios, la gestión de los servicios es mas compleja, puesto que puede haber varios sistemas de gestión del nivel de servicio enviando órdenes a los elementos de la red de transporte, órdenes que pueden ser contradictorias, conduciendo a errores y, por tanto, disminuyendo la calidad de los servicios que presta una operadora.

En la Figura 6.5 se presenta un modelo de arquitectura de gestión en la que un integrador coordinará las acciones de los gestores de red para evitar posibles conflictos. A la vez, este integrador evita que cada sistema de gestión de servicio tenga que comunicarse con todos los sistemas de gestión de las distintas tecnologías.

Este ejemplo se refiere a la prestación de servicios de transporte sobre redes IP soportadas directamente por redes ópticas, aprovechando la flexibilidad de una red de datos por transmisión de paquetes con la gran capacidad que ofrece la tecnología DWDM. Esto plantea el problema adicional de integrar aplicaciones de gestión de las redes IP que utilizan SNMP con las aplicaciones de gestión de las redes de transporte de las operadoras que utilizan TMN.

Gestionar este tipo de redes y servicios supone el manejo de un número considerable de entidades y controles que, además, evolucionan con la demanda. Esto implica que los sistemas deben ser flexibles y fácilmente escalables, para adaptarse a esta evolución.

6.3.2 Énfasis en los servicios y clientes.

En entornos competitivos, las empresas que llegan a transmitir una imagen de calidad a sus productos consiguen un mayor volumen de negocio que sus competidores y, por tanto, una mejor posición en el mercado. De esta forma, la gestión de la calidad se convierte en un requisito imprescindible para el éxito de un proveedor de servicio.

La calidad abarca cualquier aspecto de la relación entre el cliente y el proveedor de servicio, no siempre se puede medir de forma objetiva y no está restringido sólo a la prestación del servicio. Por ejemplo, en el caso de la aparición de un problema, disponer de los sistemas adecuados para atender rápida y adecuadamente al cliente es fundamental para mantener la imagen de calidad de una empresa. Estos sistemas deben proporcionar al personal técnico que atiende la reclamación información que le indique el fallo potencial y le permita realizar las acciones oportunas para solucionar el problema.

La gestión de la calidad implica el seguimiento de la forma en que los servicios se están prestando a los clientes, lo que requiere la recolección y análisis de los datos procedentes de la supervisión de los recursos que soportan dichos servicios, y su posterior tratamiento para elaborar los parámetros que determinan la calidad del servicio ofrecido.

Además, a medida que las comunicaciones adquieren protagonismo en la estructura productiva de las empresas, la calidad de los servicios de telecomunicaciones se hace más crítica. Un ejemplo de sector donde la calidad de los servicios es crítica puede ser el de la banca, o también el de los servicios financieros (Visa, Master Card, etc.), donde un fallo de la red puede suponer que no se puedan realizar un número considerable de operaciones, con la consiguiente pérdida económica y deterioro de la imagen de la empresa.

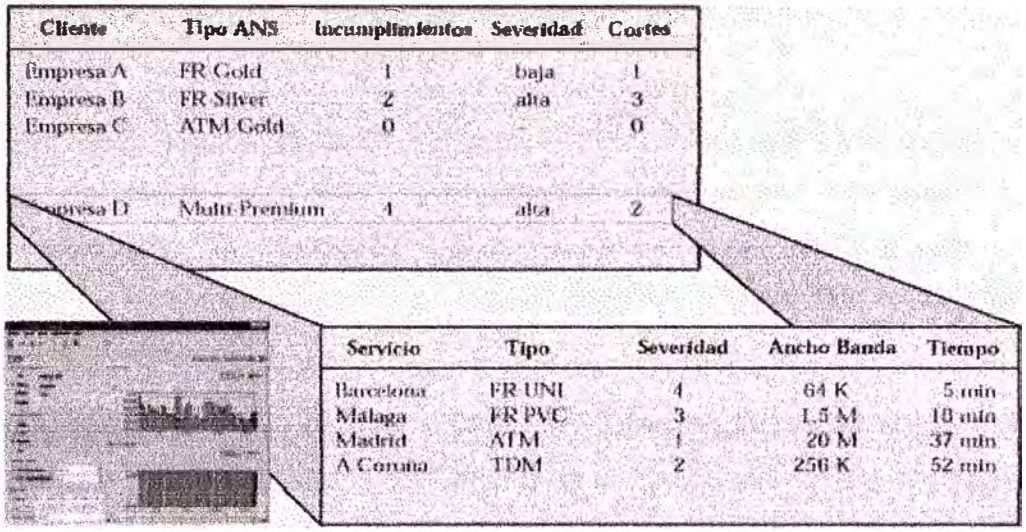

Figura 6.6. ***Ejemplo de interfaz para un sistema de supervisión del ANS***

Estos clientes exigen al proveedor de servicios de telecomunicaciones garantías sobre la calidad de los servicios utilizados. Las exigencias quedan plasmadas en un acuerdo entre ambas partes denominado Acuerdo del Nivel de Servicio (ANS), donde se reflejan todos los aspectos del servicio sobre los que se quieran garantías (mantenimiento, tasa de errores, etc.) y sus contraprestaciones económicas.

Es necesario controlar que se cumplen los acuerdos reflejados en el ANS para cada cliente y para ello hay que procesar la información técnica procedente de los sistemas de gestión de red. Esto crea la necesidad de disponer de sistemas que supervisen los servicios que se prestan a los clientes. En la Figura 7.6 se puede ver un ejemplo de la interfaz gráfica de un sistema que estaría supervisando la calidad de servicio que se presta a varios clientes, generando alarmas de diferente gravedad al producirse el incumplimiento de alguno de los compromisos reflejados en el ANS.

Conseguir elaborar este tipo de información implica un grado muy elevado de integración, tanto de las actividades que forman los procesos de negocio, como de los sistemas de información de la empresa que dan soporte a los procesos.

6.3.3 La importancia de la información.

La automatización de los procesos de gestión de redes y servicios tiene un resultado directo en la reducción de los costes de explotación y en la mejora de la calidad de estos procesos, y, por tanto, en la mejora de los servicios, lo que se traduce en un aumento de los ingresos al aumentar la cartera de clientes.

Se ha visto que la visión de abajo a arriba del modelo TMN puede conducir a arquitecturas monolíticas que no son muy apropiadas para afrontar los nuevos requisitos de gestión. En este caso, es interesante abordar el problema de arriba a abajo, viendo los procesos que es necesario realizar y cómo la información debe fluir entre los diferentes procesos y actividades.

Desde arriba se parte de una información relacionada con el cliente, que incluye aspectos técnicos muy básicos, y a medida que se va descendiendo en los niveles TMN se van incorporando los datos necesarios. De esta forma, se parte de un modelo independiente de la tecnología, al que se va añadiendo información en el nivel que sea necesario.

La definición de un modelo de datos común es una tarea necesaria e imprescindible para poder realizar la integración de los sistemas de forma eficiente, ya que este modelo permite articular un lenguaje común entre los sistemas. Este lenguaje común simplifica el desarrollo de las interfaces entre sistemas y, por tanto, su interconexión, lo que permite automatizar los procesos de negocio extremo a extremo.

En este sentido, el TMF está desarrollando un esfuerzo considerable para definir la información necesaria para las operadoras de telecomunicaciones. En el *Telecom Operation Map* (TOM) [2], el TMF identifica una serie de actividades que cubren los aspectos de atención al cliente, gestión de servicio y gestión de red, y ofrece una visión de alto nivel de los procesos de gestión. Este modelo puede verse en la Figura 6.7.

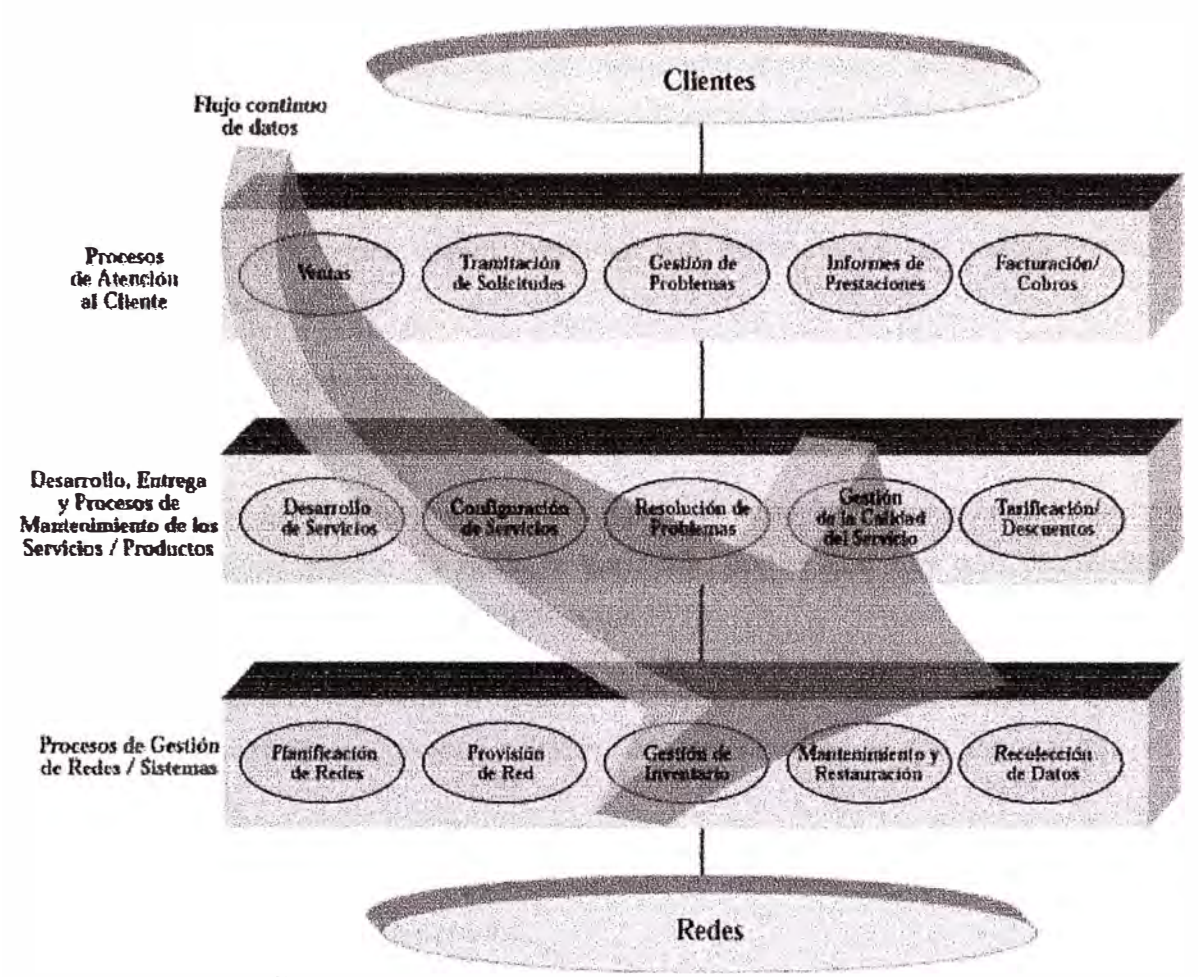

Figura 6.7. ***Modelo estático de procesos de negocios del TMF***

El modelo está basado en los niveles de gestión de TMN, pero divide la capa de gestión del servicio en dos sub capas: una de atención al cliente y otra para el desarrollo de servicios y procesos de operación. Este modelo permite definir los procesos de negocio y la información que es necesaria para realizar cada actividad.

6.4 Nuevos Sistemas De Gestión.

En los apartados anteriores se han descrito las necesidades que se están planteando a las operadoras de redes y servicios de telecomunicaciones para sus sistemas de gestión,

necesidades que, en general, aunque poniendo más énfasis en determinados aspectos, son comunes a cualquier aplicación distribuida. Las principales necesidades que se plantean son:

- *Distribución.* Las aplicaciones de telecomunicaciones están geográficamente distribuidas y, por tanto, las aplicaciones de gestión serán distribuidas.

- *Escalabilidad.* El creciente número de recursos, la cantidad de información y la variedad de redes que deben gestionar las aplicaciones de gestión, hacen esta cualidad imprescindible.

- *Diversidad.* La plataforma de gestión debe ser capaz de trabajar con la diversidad de recursos y sistemas operativos que existen en un dominio de gestión.

- *Consistencia.* La consistencia en los datos es muy importante cuando se trata de aplicaciones de gestión de redes y servicios, por lo que hay que proporcionar los mecanismos adecuados para mantenerla.

- *Prestaciones.* Los modelos de gestión incluyen, cada vez más, objetos gestionados que las aplicaciones deben manejar adecuadamente y sin menoscabo de sus prestaciones.

- *Fiabilidad.* Los sistemas de gestión deben ser capaces de trabajar las 24 horas del día y todos los días de la semana.

- *Integración de servicios.* La plataforma debe ofrecer funciones para permitir la introducción y gestión de nuevos servicios, así como la integración de los nuevos servicios con los existentes.

- *Interoperabilidad.* La interoperabilidad se consigue a través de estándares de gestión, de forma que sea posible realizar la automatización completa de los procesos, tanto internos a una operadora, como aquellos que exigen la colaboración entre diversas operadoras, con suministradores y con clientes.

- *Acceso a la información.* La información sobre las redes y servicios es muy importante, lo que implica que debe garantizarse que cada uno de los actores implicados en la gestión (operadores, clientes y suministradores) tienen acceso a la

información que necesitan. Permitir el acceso a los datos a cada actor hace que sea necesario considerar los aspectos de seguridad de los sistemas.

Estos requisitos han aumentado considerablemente la complejidad de las aplicaciones de gestión de redes y servicios y de las funciones que componen estas aplicaciones. Si bien el modelo TMN sigue siendo válido en la actualidad para la gestión de redes y servicios, la incorporación e integración en el modelo de las nuevas tecnologías que están apareciendo, tanto hardware como software, es necesaria para cumplir todos los requisitos impuestos a los nuevos sistemas de gestión de redes y servicios. En este sentido, el TMF estudia la aplicación de diferentes tecnologías en diferentes entornos específicos [2].

Por ejemplo, la naturaleza poco distribuida del modelo OSI hace difícil cumplir los requisitos de escalabilidad y prestaciones, a medida que aumenta el número de entidades (objetos gestionados) y las tareas que hay que realizar. En la Figura 6.8 se puede ver la arquitectura genérica de los nuevos sistemas de gestión, donde se pone de manifiesto el aumento de las relaciones entre sistemas para conseguir un mayor grado de automatización.

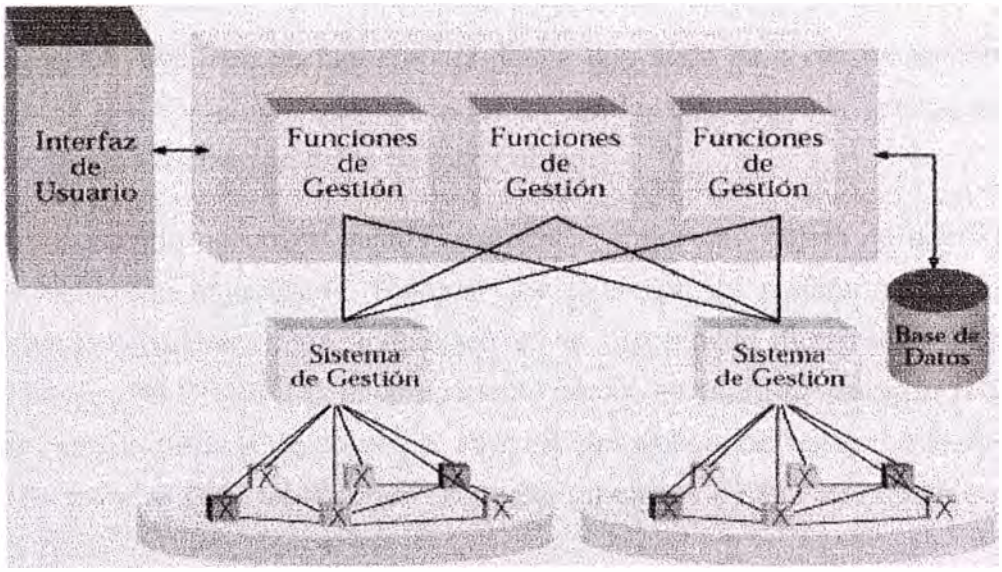

Figura 6.8. ***Arquitectura de las aplicaciones de gestión***

Los avances de las tecnologías de desarrollo software, especialmente en lo que a sistemas distribuidos se refiere, permiten al modelo TMN dar soporte a los nuevos requisitos de gestión. Entre estos avances se pueden mencionar:

- Las plataformas de desarrollo y ejecución de aplicaciones distribuidas, que permiten la integración de diferentes aplicaciones y sistemas con el objetivo de conseguir una automatización completa de los procesos.
- Las tecnologías de acceso a información remota.
- Las arquitecturas descentralizadas, como pueden ser los agentes inteligentes.

6.4.1 Plataformas de desarrollo y ejecución de aplicaciones distribuidas.

Las plataformas de desarrollo y ejecución de aplicaciones distribuidas pueden ayudar a resolver uno de los principales problemas que estaban apareciendo en la actualidad en el entorno de la gestión de las redes y servicios, como es la necesidad de integrar diferentes aplicaciones y plataformas.

De forma genérica, este tipo de plataformas define una serie de servicios comunes que los distintos objetos que componen una aplicación pueden utilizar y que le ocultan los aspectos relacionados con la localización física de estos objetos.

De esta forma, cuando un objeto invoca una acción sobre otro objeto no necesita conocer donde está localizado este último. Ejemplos de este tipo de plataformas son CORBA y DCOM, teniendo la primera más aceptación en el entorno de desarrollo de sistemas de gestión. En el caso de CORBA[5], el componente básico es el *Object Request Broker* (ORB), que es una especie de bus lógico por el cual se comunican los objetos que componen la aplicación. En torno al ORB se agrupan una serie de clases y servicios, como se puede ver en la Figura 7.9.

Existen una serie de clases genéricas, que serían utilizadas por casi todas las aplicaciones, denominadas *Facilidades Comunes*. Otro grupo son las entidades del dominio que reúne un conjunto de clases comunes en cierto ámbito de aplicación, como pueden ser las telecomunicaciones o la medicina. Por último, estarían las clases que son específicas de la aplicación que se ha desarrollado. El objeto de esta división es el desarrollo de bibliotecas de

clases para ciertos ámbitos de aplicación y la reutilización de estas clases. Junto a las clases, y asociado también al bus, aparecen una serie de servicios genéricos para el manejo y control de los objetos.

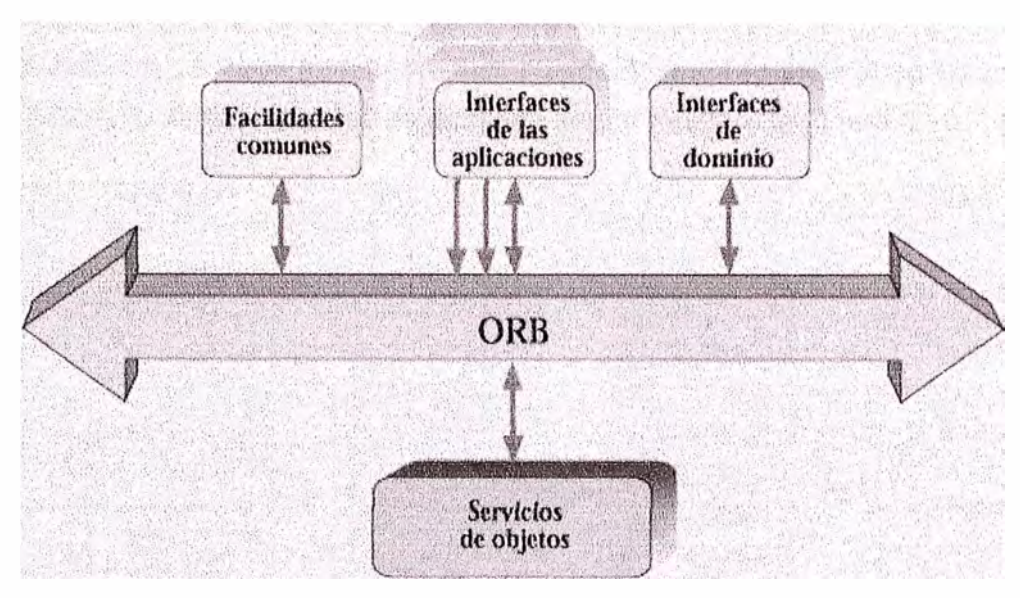

Figura 6.9. Arquitectura OMA

En CORBA no se especifican los objetos de la aplicación, sino sus interfaces. Para ello se utiliza el *Interface Definition Language* (IDL), un lenguaje definido por el *Object Management Group* (OMG). En IDL se especifican tanto los datos como los métodos que se pueden ver desde el exterior del objeto, de ahí el nombre de interfaz. La implementación de la clase se puede realizar en cualquier lenguaje de programación y es independiente de la declaración de la interfaz. Existen compiladores de IDL para muchos de los lenguajes de programación utilizados en la actualidad (IDL-C, IDL-C++, IDL-ADA, etc.)

CORBA está basado en el modelo cliente/servidor, aunque aplicado a cada transacción, con lo cual un cliente en una transacción puede ser el servidor de otra. El ORB se encarga de transportar las peticiones que hacen los clientes a los servidores y de devolver las respuestas que se generan. La principal característica del ORB es la transparencia con la que se realizan las operaciones frente a la localización de los objetos y el lenguaje de programación utilizado para la implementación.

La independencia del lenguaje de implementación ofrecido por CORBA permite la interoperabilidad entre clientes y servidores implementados en lenguajes de programación diferentes.

La incorporación progresiva de esta tecnología en el desarrollo de sistemas de gestión está permitiendo la evolución de sus arquitecturas desde los modelos monolíticos, típicos del mundo OSI, a otros totalmente distribuidos, lo que facilita la integración horizontal (áreas funcionales) y vertical (niveles de gestión), según muestra la Figura 6.10.

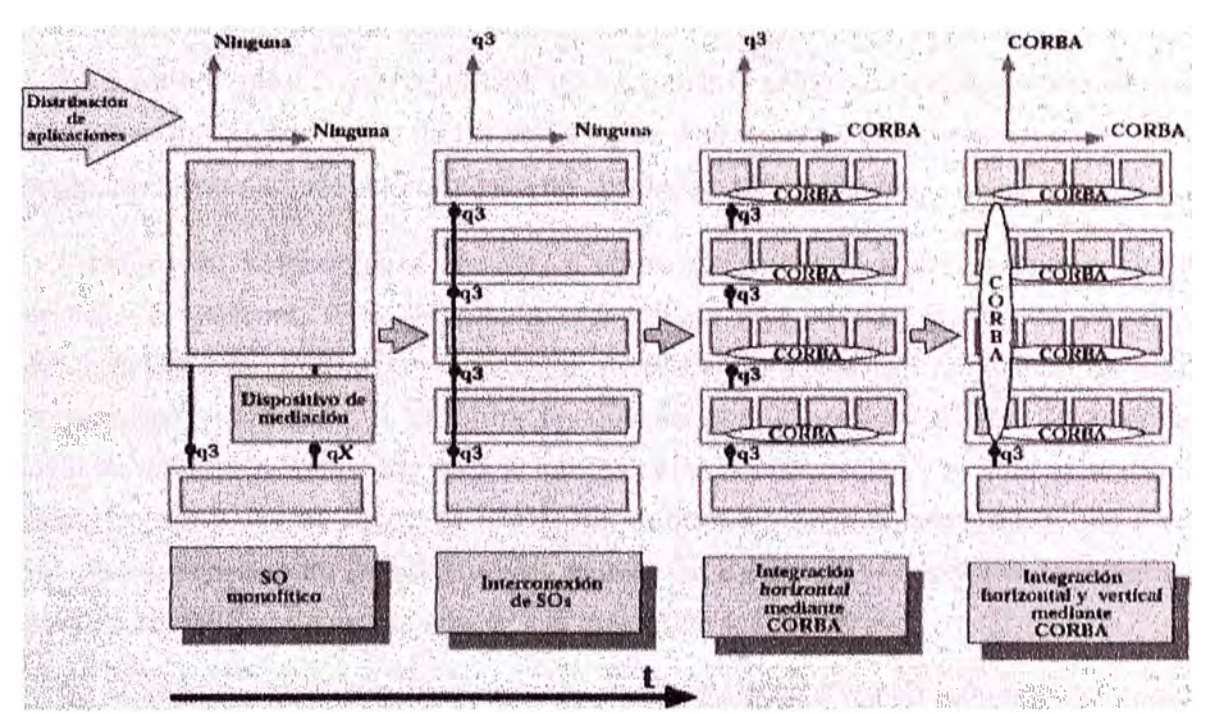

Figura 6.10. ***Evolución en la distribución de sistemas***

Hay que reseñar que CORBA sólo es una herramienta que ayuda a la integración de los sistemas y aplicaciones, pero que por sí sola no puede resolver nada. Aunque CORBA facilita la comunicación entre aplicaciones, para obtener todas las ventajas que ofrece la integración es necesario ordenar la información que se va a manejar, de forma que sea entendible por todas las aplicaciones.

El TMF, con el objetivo de conseguir la automatización total de los procesos de negocio de una operadora, ha definido una serie de modelos de información (propios o

basados en los estándares, cuando existen), para proporcionar una semántica común a las aplicaciones de gestión y de esta forma facilitar la integración.

6.4.2 Accesibilidad a la información.

Otro de los requisitos que se imponen a los nuevos sistemas de gestión es la facilidad en el acceso a la información. La automatización extremo a extremo de los procesos implica la ampliación de los usuarios que acceden a los sistemas, que abarcarían, teniendo en cuenta los procesos de mejora de la calidad y atención al cliente, tanto al personal de la operadora como a los clientes.

Es evidente que en este escenario no es viable la utilización de terminales dedicados para cada sistema. El desarrollo de las tecnologías *web* y Java y su aplicación a los sistemas de gestión permiten cumplir este requisito de una forma fácil y flexible.

Inicialmente, la tecnología *web* surgió como una forma de acceso gráfico a una serie de servicios de Internet. Esta tecnología proporciona una interfaz gráfica de usuario que permite acceder a la información localizada en diferentes sitios, sin necesidad de conocer donde está esa información y la forma en que se puede acceder a ella. Se basa en el protocolo de comunicaciones *http* para el intercambio de información y en una aplicación que se ejecuta en PC y que es capaz de interpretar de forma gráfica la información que recibe e invocar ciertos servicios de la red. Cuando alguien se conecta a un servidor de información, los datos se descargan en su ordenador y la aplicación los interpreta.

Al principio, la tecnología *web* sólo permitía visualizar y volcar documentos desde un ordenador remoto; el siguiente paso fue hacer esta tecnología más interactiva. La utilización de la *Common Gateway Interface* (CGI) permitía al usuario lanzar procesos en el servidor de información, de forma que se podían ejecutar comandos en sistemas remotos. Una aplicación inmediata de este avance es la búsqueda de información en bases de datos. El usuario descarga en su ordenador una página *web,* que es un formulario donde rellena ciertos campos que va a utilizar para la búsqueda, estos campos serán los parámetros necesarios para ejecutar el programa. El servidor ejecuta la CGI y genera la respuesta, insertando la información en un fichero HTML que se descarga y visualiza en el navegador. Un ejemplo de arquitectura para este tipo de aplicaciones se puede ver en la Figura 6.11.

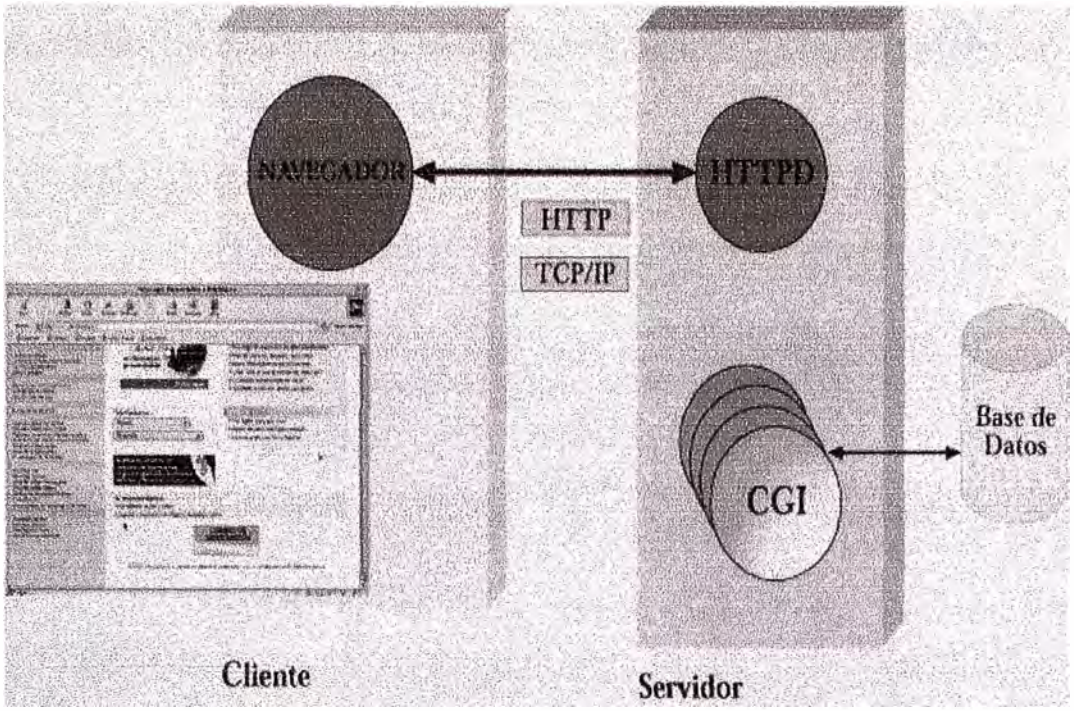

Figura 6.11. ***Aplicación de gestión basada en web y CG***

La facilidad para desarrollar los terminales de los operadores y los usuarios, así como la posibilidad de utilizar solamente un ordenador personal con un navegador *web,* ha hecho que esta tecnología sea muy atractiva para el desarrollo de ciertos sistemas. La forma de acceso también facilita la introducción de esta tecnología, pues en principio una simple conexión a Internet puede ser suficiente. Obviamente, este tipo de acceso plantea unos problemas de seguridad que es necesario tener muy en cuenta.

El siguiente paso fue dotar al cliente con la posibilidad de ejecutar en local alguno de los procesos. Utilizando el mismo protocolo de comunicaciones que para descargar páginas *web*, la tecnología Java permite que los clientes descarguen fragmentos de código (*applets*) que se ejecutan en el cliente.

Las tecnologías Java y CORBA se pueden integrar fácilmente en los sistemas de gestión. Java permite desarrollar interfaces de usuario que se descargan en la máquina cliente desde un servidor central utilizando *http*, a través de las cuales se utiliza CORBA para hacer llamadas a métodos remotos.

Los documentos *Hypertext Markup Language* (HTML) y los *applet* de Java se obtienen a través del servidor *web*, mientras que a través del ORB pueden ser invocadas operaciones sobre los objetos de la aplicación servidora, tal como se muestra en la Figura 6.12.

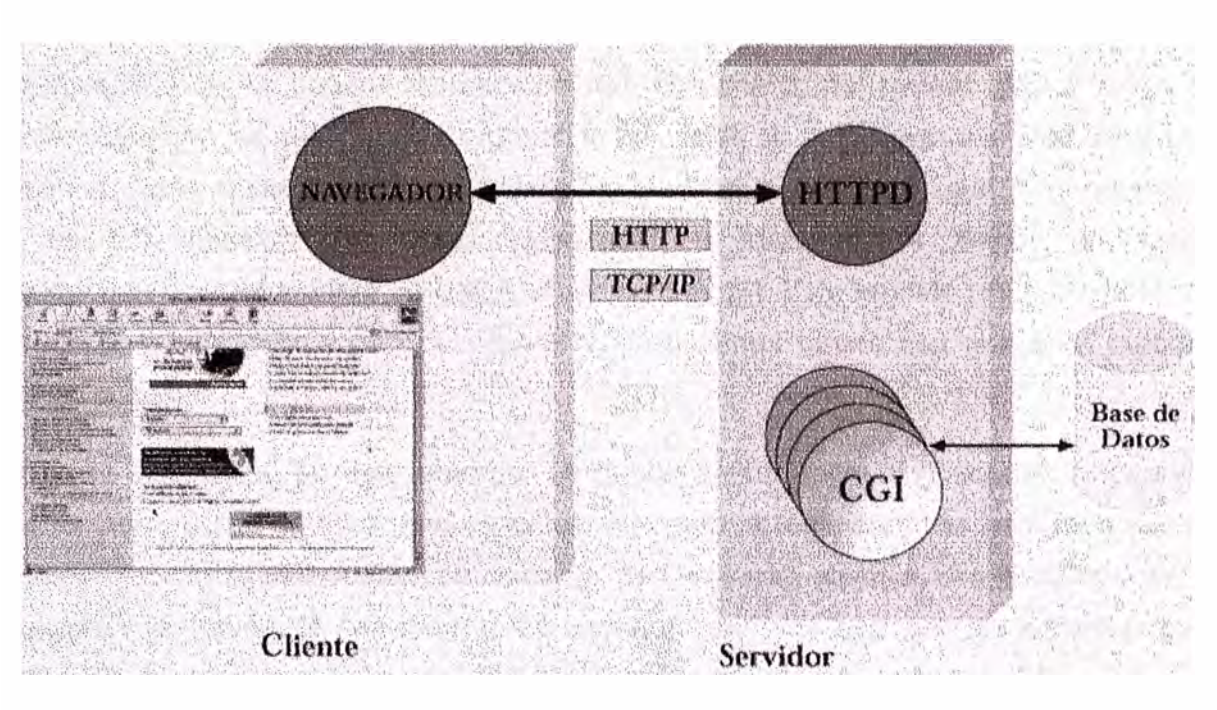

Figura 6.12. ***Aplicación de gestión que combina web y CORBA***

Esta arquitectura permite la realización de sistemas distribuidos utilizando Java como interfaz. Como ambas tecnologías son orientadas a objetos, un objeto Java puede tener una interfaz CORBA, de forma que un objeto remoto pueda invocar operaciones sobre él.

6.4.3 Agentes inteligentes.

Los modelos de gestión utilizados en la actualidad (TMN o SNMP) aplican el modelo gestor-agente. En este modelo, la aplicación de gestión se encuentra en el gestor y se comunica con los agentes (situados en los nodos o elementos de red) para obtener información sobre los recursos de red. La comunicación se hace, por lo general, mediante los protocolos CMIP o SNMP.

Este tipo de arquitectura centraliza en las aplicaciones de gestión las funciones de supervisión, análisis y control de los recursos de red. Incluso utilizando tecnologías como CORBA, que permiten distribuir las funciones de gestión entre varias máquinas, el hecho de tener una arquitectura cliente-servidor dificulta las posibilidades de escalabilidad de los sistemas, una vez llegados al límite del procesamiento de la máquina donde reside la aplicación de gestión.

La complejidad de los nuevos recursos de red, el aumento del tamaño de las redes y las nuevas exigencias de gestión, que suponen la ejecución de una mayor cantidad de procesos de gestión, están motivando que se investiguen modelos diferentes al gestor/agente clásicos. Uno de los modelos que están empezando a aplicarse, al menos en sistemas experimentales, es el modelo de agentes inteligentes [6]. Este modelo pretende dotar a los agentes de la inteligencia necesaria para realizar ciertas tareas con una gran autonomía respecto al gestor.

Un agente inteligente, en este entorno, se puede definir como una entidad software que presenta cierto grado de inteligencia y autonomía para la realización de las tareas que se le han impuesto. Un agente puede comunicarse, de una forma efectiva, con otros agentes, con los usuarios (a través de una interfaz de usuario) y con las aplicaciones software que los utilizan. En muchos casos, los agentes inteligentes presentan cierta movilidad, lo que les permite ejecutarse en máquinas diferentes.

Un ejemplo típico de agente inteligente, es el de un agente de búsqueda diferida en Internet. El usuario indica al agente lo que quiere buscar y éste realiza la búsqueda de forma independiente mientras el usuario está dedicado a otras tareas. Cuando el agente ha terminado su tarea avisa o envía los resultados al usuario. Durante la búsqueda el agente es guiado por eventos internos, procedentes de su conocimiento, en vez de eventos externos (botones de ratón, teclado del ordenador, etc.) como hasta ahora era habitual.

La aplicación de agentes inteligentes a la gestión de redes y servicios puede ser muy provechosa, puesto que permite adaptar las arquitecturas centralizadas de los sistemas actuales dotándolas de mejores prestaciones y mayor escalabilidad.

Un ejemplo puede ser un sistema de gestión de la calidad de servicio que se ofrece a un cliente determinado. Un operador podría encargar a un agente inteligente que supervise

ciertos parámetros del servicio y dedicarse a otras actividades. Este agente podría comunicarse con otros agentes instalados en determinados nodos para que le notifiquen cuando estos parámetros sobrepasan ciertos umbrales. En el caso que esto ocurra, el agente encargado de la supervisión podría ponerse en contacto con un agente proveedor de red, al objeto de localizar el ancho de banda necesario para seguir manteniendo la calidad del servicio. Si logra su objetivo, todas estas actividades se realizarían sin intervención del operador.

Normalmente, será necesario disponer de varios tipos de agentes, responsable cada uno de ellos de determinadas tareas, y aprovechar las posibilidades de comunicación entre ellos para coordinar las acciones que hay que realizar. Así, en la Figura 6.13 se presenta un agente supervisando la calidad de un nodo, otro supervisando la calidad de un cliente determinado y otro para proporcionar ancho de banda.

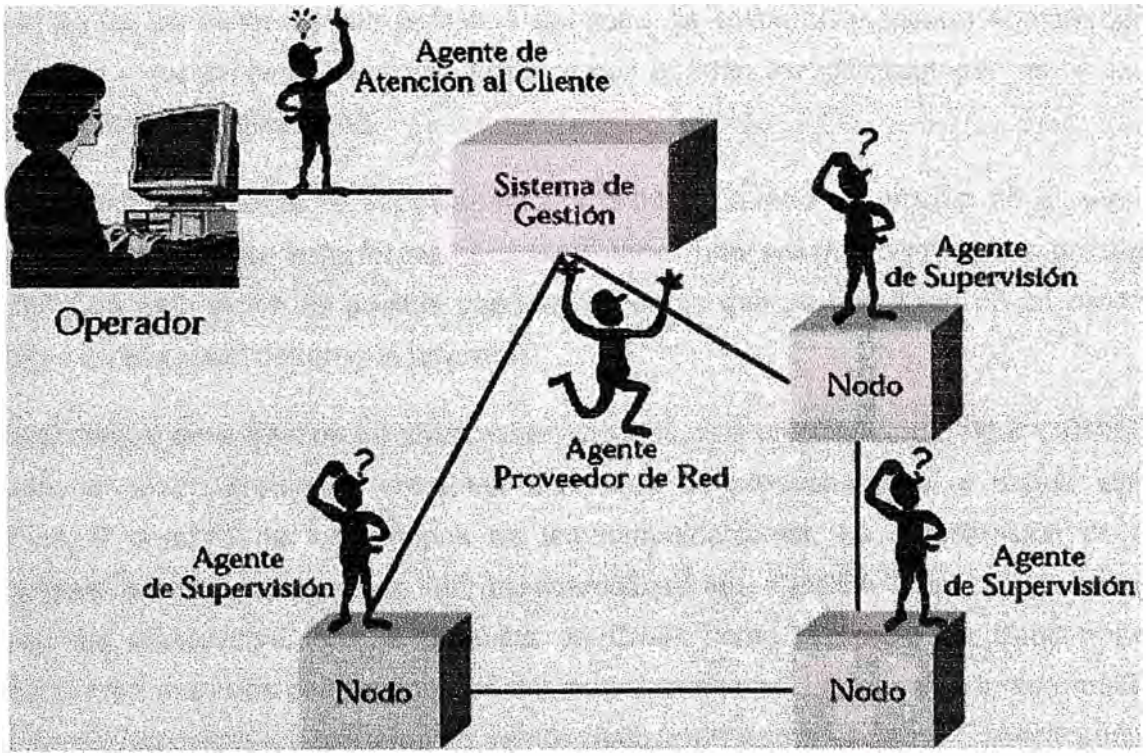

Figura 6.13. ***Ejemplo de cooperación entre agentes***

Otra característica de los agentes, que tiene particular interés en la gestión, es la posibilidad de movilidad de los agentes, lo que permite que se puedan mover de un nodo a otro. Esto puede permitir descargar el sistema y, en consecuencia, aumentar las prestaciones y acceder a recursos remotos.

6.5 Conclusiones.

Aunque el modelo de referencia TMN sigue siendo válido, los sistemas de gestión necesitan ir incorporando los nuevos avances tecnológicos para poder evolucionar de acuerdo con las necesidades de los operadores de red y los proveedores de servicio.

El único medio de conseguir una mejora en la calidad de los servicios y una reducción simultánea de los costes de explotación es la automatización extremo a extremo de los procesos de negocio. Para llevar a cabo la automatización de los procesos es necesario poder integrar los sistemas que realizan todas las actividades que forman el flujo de trabajo del proceso. Si cada sistema tiene un modelo de datos, automatizar un flujo en el que intervienen varios sistemas requiere una cantidad de esfuerzo y tiempo considerable. La planificación y desarrollo de modelos de datos que puedan ser utilizados por varios sistemas facilita enormemente esta tarea.

El modelo TMN adquiere especial valor y utilidad cuando se analiza en el sentido de arriba abajo, ya que de esta forma es posible tener una visión global de los procesos de negocio. Con esta visión es posible conocer los datos que se necesitan en un proceso de negocio y en que nivel tienen que aparecer.

En el campo de la gestión de redes y servicios, se está proponiendo utilizar CORBA, para proporcionar interoperabilidad entre las entidades de procesamiento, y seguir utilizando CMIP en el dominio de los equipos de telecomunicaciones. La combinación de ambas tecnologías permite aprovechar las características de CORBA para el desarrollo de aplicaciones distribuidas, con la potencia de CMIP como protocolo de transferencia de información en entornos con equipos de diversos fabricantes. El acceso a la información por parte de los operadores y usuarios se puede realizar de forma eficiente y sencilla utilizando la tecnología *web*.

La consecuencia de una estructura de gestión adecuada es de vital importancia para un operador que presta servicios en un mercado de libre competencia. Una estructura de gestión adecuada acorta de forma considerable el tiempo de lanzamiento de los nuevos servicios que se crean y facilita su mantenimiento, lo que permite dar una respuesta óptima a las necesidades de los clientes.

6.6 Referencias del Capitulo.

[1] *Telecom Operations Map (TOM).* TeleManagement Forum, GB910, issue 2.0. November 1999.

[2] *Technology Integration Map (TIM).* TeleManagement Forum, GB909, issue 1. April 1998.

[3] *Principles for a Telecommunication Management Network.* ITU-T Recommendation M.3010, 1992.

[4] *TMN Management Functions.* ITU-T Recommendation M.3400. Octuber 1992.

[5] *The Common Object Request Broker: Architecture and Specification.* Issue 2.0, Object Management Group (OMG). May 1996.

[6] *Intelligent and Mobile Agents and their Applicability to Service and Network Management.* Eurescom P712, deliverable 1. June 1999.

CAPITULO VII
PROTOCOLOS DE GESTIÓN DE INTERNET.

7.1 Modelo de Gestión de Internet.

A continuación, se muestra la figura 7.1 en la cual se ve la distribución de los bloques de la gestión de red en Internet

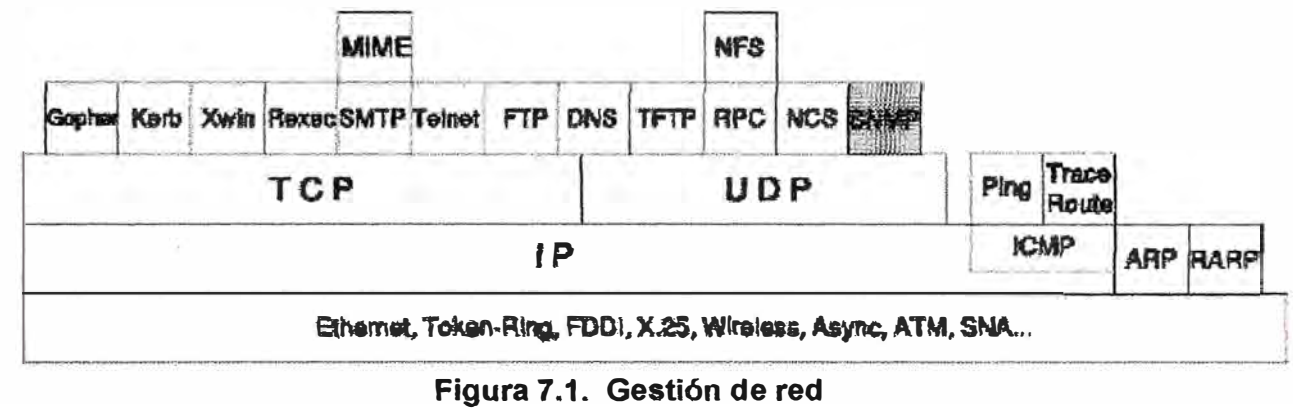

Figura 7.1. Gestión de red

Con el crecimiento en tamaño y complejidad de las redes basadas en TCP/IP, la necesidad de mecanismos de gestión de red se ha vuelto muy importante. En la actualidad, los protocolos que forman el soporte de la gestión de red son:

- SMI (RFC 1155) - describe cómo se definen los objetos gestionados contenidos en el MIB (se verá en SMI("Structure and Identification of Management Information").)
- MIB-II (RFC 1213) - describe los objetos gestionados contenidos en el MIB(se verá en MIB("Management Information Base").)
- SNMP (RFC 1098) - define el protocolo usado para gestionar estos objetos(se verá en SNMP("Simple Network Management Protocol").)

El IAB("Internet Architecture Board") emitió un RFC al respecto, en el que adoptaba dos actitudes diferentes:

A corto plazo, se recomienda el uso de SNMP.

A corto plazo, se recomienda el uso de SNMP.

El IAB recomienda que todas las implementaciones de IP y TCP sean gestionables. Actualmente, esto implica la implementación de MIB-II (RFC 1213), y de al menos el protocolo recomendado de gestión SNMP (RFC 1157).

Notar que los protocolos históricos SGMP (Simple Gateway Monitoring Protocol, RFC 1028) y MIB-I (RFC-1156) no están recomendados.

A largo plazo, se debería investigar el uso del incipiente protocolo de gestión de red de OSI(CMIP). Es lo que se conoce como CMIP sobre TCP/IP (CMOT).(Se discutirá en CMOT ("Common Management Information Protocol over TCP/IP")).)

Tanto SNMP y CMOT utilizan los mismos conceptos básicos en la descripción y definición de la información de gestión denominada SMI("Structure and Identification of Management Information") descrita en el RFC 1155 y MIB("Management Information Base"), descrita en el RFC 1156.

7.2 El Protocolo Simple de Gestion de Redes (Snmp – Simple Network Management Protocol)

SNMP añadió las mejoras de muchos años de experiencia con SGMP y le permitió trabajar con los objetos definidos en el MIB con la representación del SIM.

El RFC 1157 define NMS("Network Management Station") como una estación que ejecuta aplicaciones de gestión de red(NMA) que monitorizan y controlan elementos de red(NE) como hosts, pasarelas y servidores de terminales. Estos elementos usan un agente de gestión(MA) para realizar estas funciones. En la Figura 7.2 ilustra algunos componentes de SNMP.

Todos las funciones de los MA son sólo alteraciones(set) o consultas(get) de variables, limitando así el número de funciones esenciales a dos y simplificando el protocolo. En la comunicación NE-NMS, se utilizan un número limitado de mensajes no solicitados(traps) para informar de eventos asíncronos. Del mismo modo, en un intento de mantener la sencillez, el intercambio de información requiere sólo un servicio de datagramas y cada mensaje se envía en un único datagrama. Esto significa que SNMP es adecuado para una gran variedad de protocolos de transporte. El RFC 1157 especifica el intercambio de mensajes vía UDP, aunque es posible emplear otros.

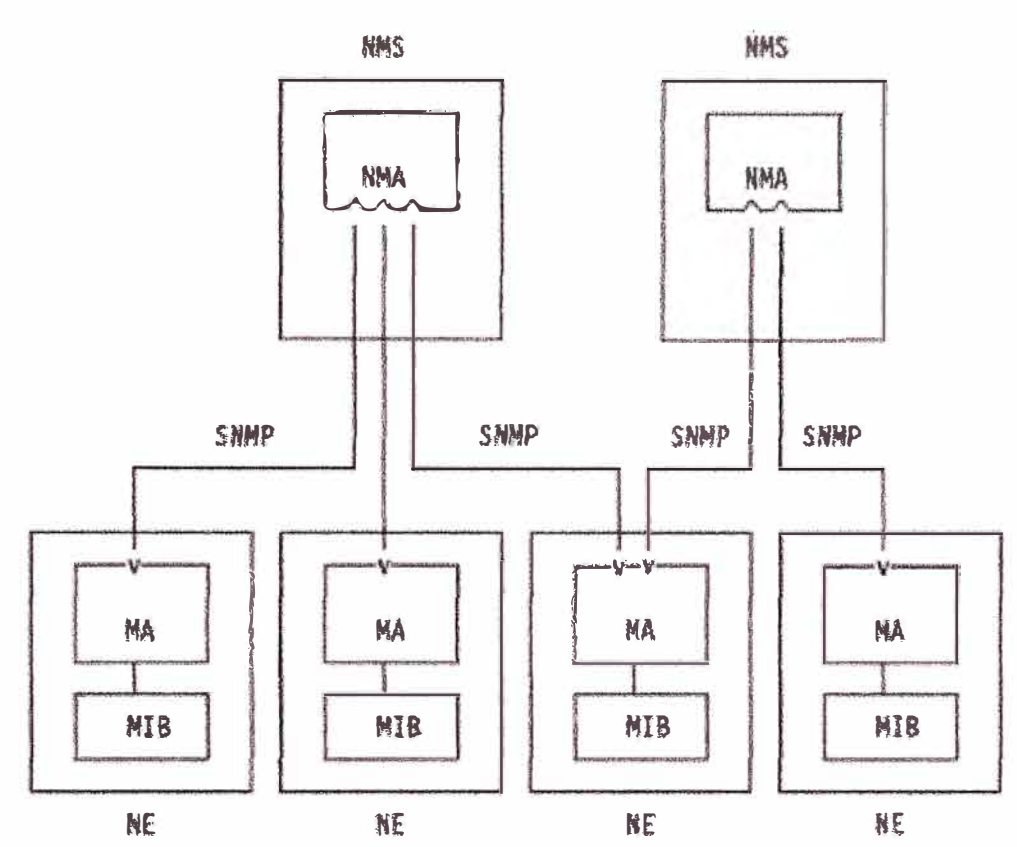

Figura 7.2. ***SNMP - Componentes de SNMP.***

Las entidades que residen en las NMS y los elementos de red que se comunican con otros a través de SNMP se denominan entidades de aplicación de SNMP. Los procesos que las implementan son las entidades de protocolo. Un agente SNMP con un conjunto arbitrario de entidades es una comunidad SNMP, en la que cada entidad se nombra con una ristra de bytes que debe ser unívoca para esa comunidad.

Un mensaje de SNMP consiste en un identificador de la versión, un nombre de la comunidad SNMP y un PDU("protocol data unit"). Toda implementación de SNMP debe soportar las cinco PDUs siguientes:

- **GetRequest**: Recuperar los valores de un objeto del MIB
- **GetNextRequest**: Recorrer parte del MIB

- **SetRequest**: Alterar los valores de un objeto del MIB

- **GetResponse**: Respuesta de GetRequest, GetNextRequest y SetRequest

- **Trap**: Capacidad de los elementos de red para generar eventos como la inicialización., reinicio o fallo en el enlace del MA. Hay siete tipos de traps definidos en el RFC 1157: coldStart, warmStart, linkDown, linkUp, authenticationFailure, egpNeighborLoss y enterpriseSpecific.

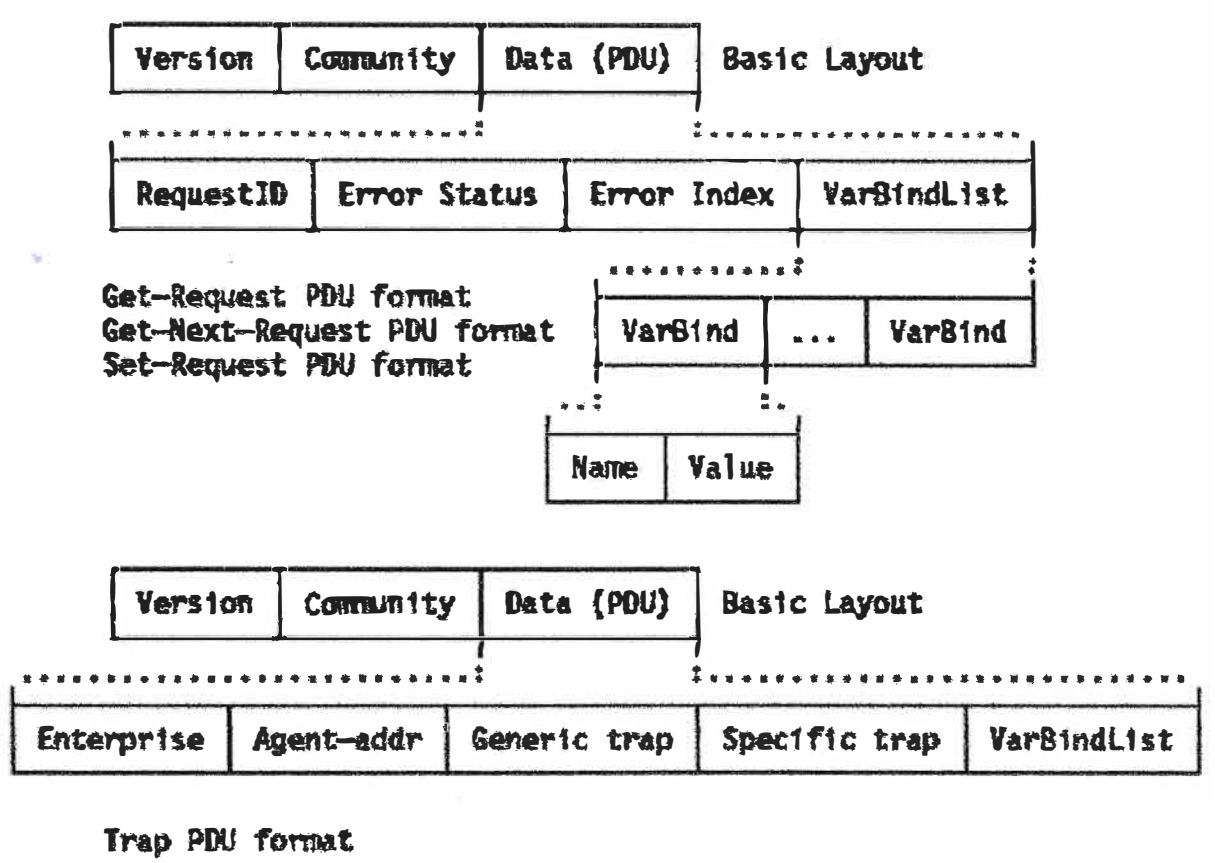

Figura 7.3. ***Formato de mensaje SNMP - Formato de las PDU Request, Set y Trap***

En la figura 7.3 se muestran los bloques del formato de mensaje SNMP, donde se puede observar el formato de las PDU en sus partes.

Los formatos de estos mensajes son los siguientes:

7.1.1 Protocolo Común de Información de Gestión sobre TCP/IP (CMOT – Common Management Information Protocol).

CMOT es la arquitectura de gestión de red desarrollada con vistas a mantener una relación más estrecha con el CMIP("Common Management Information Protocol") de OSI("Open System Interconnection"). Con esta premisa, CMOT se divide, como en OSI, en un modelo organizacional, funcional e informacional.

En los dos primeros, el mismo concepto de OSI se usa en CMOT y SNMP. La identificación de objetos se efectúa empleando el subárbol relacionado con DoD con subdivisiones en lo que respecta a gestión, directorio, experimental y privado. Todos los objetos de gestión se definen en el MIB("Management Information Base"), y se representan con el SMI("Structure and Identification of Management Information"), un subconjunto de ASN.1("Abstract Syntax Notation 1" de OSI).

En el modelo funcional, CMOT (Figura 7.4) adopta el modelo OSI que divide los componentes de gestión en managers y agentes. El agente recoge información, realiza comandos y ejecuta tests, y el manager recibe datos, genera comandos y envía instrucciones a los agentes. El manager y el agente están constituidos por un conjunto específico de entidades de información de gestión por cada capa de comunicación, denominadasLME ("Layer Management Entities").

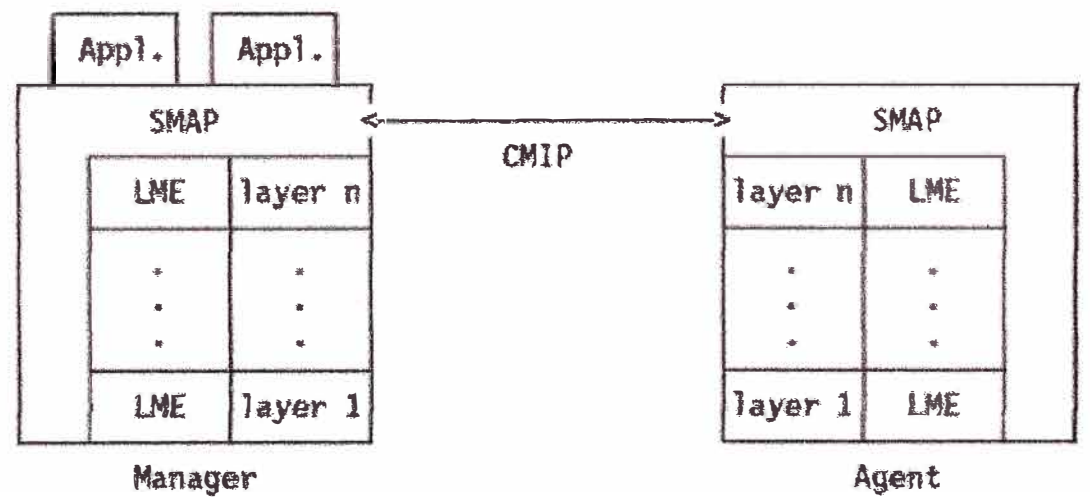

Figura 7.4. *CMOT - Componentes de CMIP sobre TCP/IP.*

Todos los LME los coordina el SMAP("System Management Application Process") que es capaz de comunicarse entre diferentes sistemas a través de CMIP ("Common Management Information Protocol").

En el mundo OSI, la gestión sólo se puede producir sobre conexiones establecidas por completo entre managers y agentes. CMOT permite el intercambio de información de

gestión usando servicios no orientados a conexión(datagramas). Pero para mantener la misma interfaz del servicio que requiere CMIP, llamada CMIS("Common Management Information Services"), la arquitectura de CMOT define una nueva capa, el LPP("Lightweight Presentation Protocol") (Figura 7.5). Esta capa se ha definido para proporcionar los servicios de presentación que necesita CMIP de tal forma que la totalidad de los estándares OSI para la gestión de red se adapten a la arquitectura TCP/IP de CMOT.

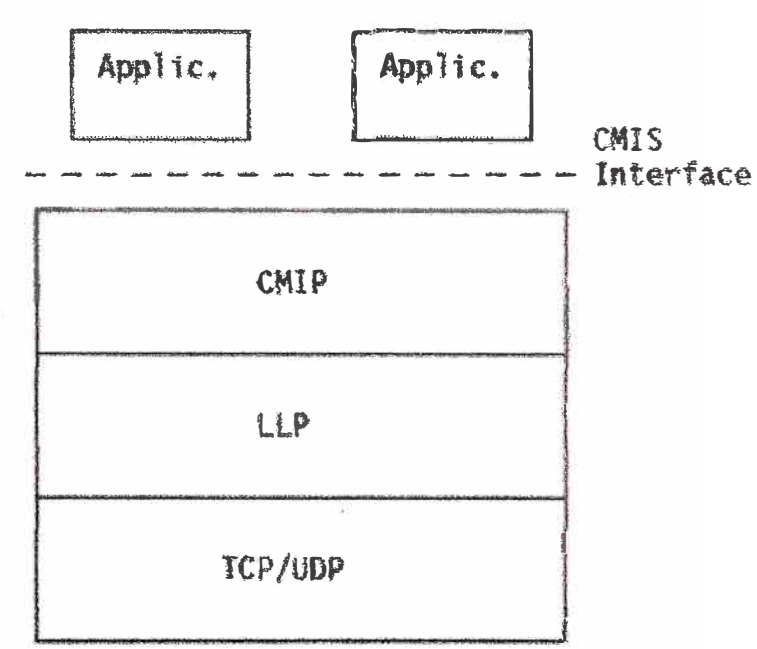

Figura 7.5. ***LPP("Lightweight Presentation Protocol")***

7.2.2 La Interfaz de Programa Distribuido de SNMP(Distributed Programming Interface – DPI – SNMP).

SNMP define un protocolo que permite efectuar operaciones en una serie de variables. Este conjunto de variables(el MIB) y un conjunto básico o núcleo está predefinidas. Sin embargo, el diseño del MIB cuenta con la posibilidad de expandir este núcleo. Desafortunadamente, las implementaciones convencionales de agentes SNMP no suministran mecanismos para que el usuario creé nuevas variables. El DPI enfoca esta cuestión proporcionando mecanismos que permiten al usuario añadir, borrar o reemplazar dinámicamente variables en el MIB local sin tener que recompilar el agente SNMP. Esto es

posible gracias a un subagente que se comunica con el agente a través del DPI. El RFC 1228 lo describe.

El DPI de SNMP habilita a un proceso para registrar la existencia de una variable MIB en el agente SNMP, quien pasará la solicitud al subagente. El subagente devuelve a su vez la respuesta apropiada al agente. Este, finalmente, empaqueta una respuesta SNMP y envía la respuesta a la NMS que inició la solicitud. El subagente es completamente invisible (transparente) para la NMS.

La comunicación, entre el agente SNMP y sus clientes(subagentes) tiene lugar sobre un canal. Típicamente se trata de una conexión TCP, pero se pueden emplear otros protocolo de transporte orientados a conexión. El agente en el DPI puede:

- Crear y borrar subárboles del MIB
- Crear un paquete de solicitud de registro para que el subagente informe al agente SNMP
- Crear un paquete de respuesta para que el subagente responda a la solicitud del agente SNMP
- Crear un paquete de solicitud TRAP

La Figura 7.6 muestra el flujo entre el agente SNMP y el subagente.

- El agente SNMP se comunica con el manager por medio de SNMP.
- La comunicación del agente con las capas TCP/IP y con el núcleo del sistema operativo depende de la implementación.
- Un subagente SNMP, ejecutando un proceso aparte(que potencialmente puede estar en otra máquina), puede registrar objetos con el agente SNMP(Register).
- El agente SNMP decodificará los paquetes. Si un paquete contiene una solicitud Get/GetNext o Set para un objeto registrado en el subagente, se la enviará en el correspondiente paquete(MIB query).
- El subagente SNMP responde con un paquete RESPONSE(Reply).
- El agente codifica la respuesta en un paquete SNMP y lo envía al manager.
- Si el subagente desea informar de un cambio de estado importante, envía un Trap al agente que a su vez lo codificará y enviará al manager.

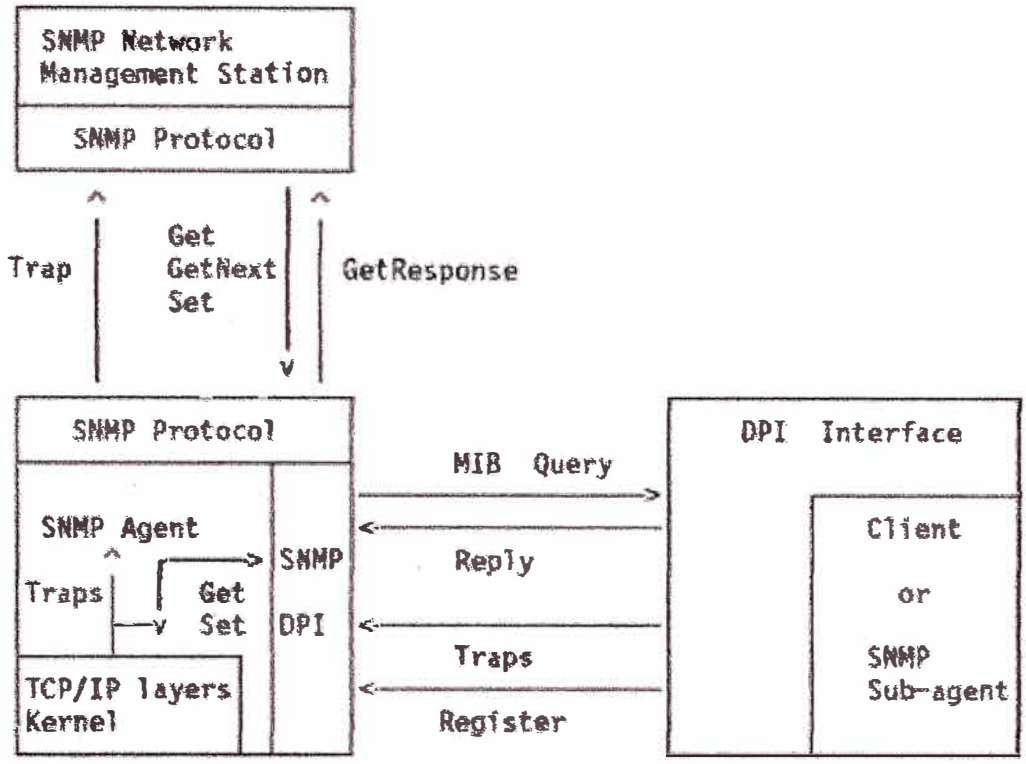

Figura 7.6. ***Descripción del DPI de SNMP***

7.3 El Protocolo de Gestion Snmpv2(Simple Network Management Protocol, Versión 2).

La infraestructura de la versión 2 de SNMP se publicó en abril de 1993 y consiste en 12 RFCs, incluyendo el primero, el 1441, que es una introducción. En agosto de 1993 los 12 RFCs se convirtieron en un estándar con status electivo.

Esta infraestructura consta de las siguientes disciplinas:

- SMI("Structure of Management Information")

  Definición del subconjunto de ASNN.1 para la creación de módulos MIB. Descripción en el RFC 1442.

- Convenios textuales

Definición del conjunto inicial de convenios textuales disponible para todos los módulos MIB. Descripción en el RFC 1443.

- Operaciones del protocolo

Definición de las operaciones del protocolo con respecto a las PDUs enviadas y recibidas en el RFC 1448.

- Mapeados de transporte

Definición del mapeado de SNMPv2 sobre un conjunto inicial de dominios de transporte, ya que se puede utilizar en diferentes pilas de protocolo. El mapeado en UDP es el preferido. El RFC, también define OSI, AppleTalk, IPX, etc. Descripción en el RFC 1449.

- Instrumentación del protocolo

Definición del MIB y del MIB Manager-Manager. Descripción en los RFCs 1450 y 1451.

- Infraestructura administrativa

Definición de SNMPv2 Party, SP("Security Protocols") y Party MIB. Descripción en los RFCs 1445, 1446 y 1447.

- Compatibilidades

Definición de la *compatibilidad* o *capacidad* de notación de los agentes. Descripción en el RFC 1444.

Las siguientes secciones describen las principales diferencias y mejoras desde SNMPv1 a SNMPv2.

7.3.1 Entidad SNMPv2.

Una entidad SNMPv2 es un proceso real que realiza operaciones de gestión de red mediante la generación y/o respuesta a/de mensajes SNMPv2. Todas las posibles operaciones de una entidad se pueden restringir a un subconjunto de las operaciones que puede efectuar el entorno de gestión("SNMPv2 Party" o EG). Remitirse a SNMPv2 Party más abajo. Una entidad SNMPv2 podría pertenecer a múltiples entidades gestoras, y mantiene las siguientes bases de datos locales:

Una base de datos, para todos los EG que conoce la entidad, que podrían ser:

- Operación local
- Operación local realizada por interacciones con EG o dispositivos remotos
- Operación realizada por otras entidades SNMPv2.
- Otra base de datos que representa todos los recursos de los objetos gestionados que conoce la entidad.

- Como mínimo, una base de datos que representa una política de control de acceso que define los privilegios de acceso de acuerdo con los EG conocidos

Una entidad SNMPv2 puede actuar como agente o como manager SNMPv2.

7.3.2 Entorno de gestión("SNMPv2 Party" o EG).

Un entorno de gestión es un entorno de ejecución virtual cuyas operaciones se restringen, por razones de seguridad o de otra índole, a un subconjunto definido administrativamente de todas las operaciones que puede realizar una entidad SNMPv2 particular. Remitirse a Entidad SNMPv2 más arriba. Arquitectónicamente, cada EG comprende:

- Una identidad unívoca del entorno.
- Una localización lógica de red en la que se ejecuta el EG, caracterizada por un dominio del protocolo de transporte y por información de direccionamiento del nivel de transporte.
- Un sólo protocolo de autentificación y parámetros asociados con los que se autentifican el origen y la integridad de los mensajes del protocolo generados por el entorno .
- Un sólo protocolo de privacidad y parámetros asociados con los que los mensajes de protocolo que recibe el entorno se protegen de cualquier intrusión

7.3.3 Mensaje de Solicitud de Transferencia (GetBulkRequest.)

El GetBulkRequest, está definido en el RFC 1448 y forma por tanto, parte de las operaciones del protocolo. Un mensaje GetBulkRequest se genera y se transmite como una petición de una aplicación SNMPv2. Su fin es solicitar la transferencia de una cantidad de datos potencialmente elevada, incluyendo, sin que ello le condicione, la rapidez y eficiencia en la recuperación de grandes tablas. GetBulkRequest es más eficiente que GetNextRequest en la recuperación de grandes tablas MIB de objetos. Su sintaxis se ve en el Cuadro 7.1:

Cuadro 7.1. Sintaxis GetBulkRequest.

```
GetBulkRequest [ non-repeaters = N, max-repetitions = M ]
            ( RequestedObjectName1,
              RequestedObjectName2,
              RequestedObjectName3 )
Where:
RequestedObjectName1, 2, 3
```

Identificador MIB del objeto, como sysUpTime, etc. Los objetos están en una lista ordenada léxicamente. Cada identificador de objeto está ligado como mínimo a una variable. Por ejemplo, el identificador *ipNetToMediaPhysAddress* está ligado a una variable para cada dirección IP de la tabla ARP y su contenido es la dirección MAC asociada.

N: Especifica el valor de non-repeaters, lo que significa que se solicita sólo el contenido de la variable inmediata al objeto indicado en la solicitud, para los primeros N objetos nombrados entre paréntesis. Se trata de la misma función que desempeña GetNextRequest.

M : Especifica el valor max-repetitions, lo que significa que se solicita del resto de los objetos(habiéndose solicitado N) el contenido de las M variables inmediatas al objeto indicado en la solicitud. Es similar a un GetNextRequest iterado pero transmitido en una sola solicitud.

Con GetBulkRequest se pueden conseguir los valores de sólo la siguiente variable o de las siguientes M variables con una sola solicitud.

Asumiendo que el siguiente cuadro ARP en un host que ejecuta un agente NMPv2 (Cuadro 7.2):

Cuadro 7.2. *ARP*

Interface-Number	Network-Address	Physical-Address	Type
1	10.0.0.51	00:00:10:01:23:45	static
1	9.2.3.4	00:00:10:54:32:10	dynamic
2	10.0.0.15	00:00:10:98:76:54	dynamic

Un manager SNMPv2 envía la siguiente respuesta para conseguir sysUpTime y el cuadro ARP completo (Cuadro 7.3):

Cuadro 7.3. ***Manager SNMPv2.***

```
GetBulkRequest [ non-repeaters = 1, max-repetitions = 2 ]
        ( sysUpTime,
          ipNetToMediaPhysAddress,
          ipNetToMediaType )
```

La entidad SNMPv2 que actúa como agente responde con la PDU Response (Cuadro 7.4.):

Cuadro 7.4. ***Respuesta PDU (Response).***

```
Response (( sysUpTime.0 =  "123456" ),
        ( ipNetToMediaPhysAddress.1.9.2.3.4 =
                "000010543210" ),
        ( ipNetToMediaType.1.9.2.3.4 =  "dynamic" ),
        ( ipNetToMediaPhysAddress.1.10.0.0.51 =
                "000010012345" ),
        ( ipNetToMediaType.1.10.0.0.51 =  "static" ))
```

La entidad SNMPv2 que hace de manager continúa con (Cuadro 7.5.) :

Cuadro 7.5. ***Entidad SNMP - Manager***

```
GetBulkRequest [ non-repeaters = 1, max-repetitions = 2 ]
        ( sysUpTime,
          ipNetToMediaPhysAddress.1.10.0.0.51,
          ipNetToMediaType.1.10.0.0.51 )
```

El agente responde con (cuadro 7.6):

Cuadro 7.6. *Agent – Response.*

```
Response (( sysUpTime.0 =  "123466" ),
                ( ipNetToMediaPhysAddress.2.10.0.0.15 =
                                "000010987654" ),
                ( ipNetToMediaType.2.10.0.0.15 =
                                "dynamic" ),
                ( ipNetToMediaNetAddress.1.9.2.3.4 =
                                "9.2.3.4" ),
                ( ipRoutingDiscards.0 =  "2" ))
```

Esta respuesta señala el final de la tabla al manager. Con GetNextRequest se hubieran necesitado cuatro solicitudes para conseguir la misma información. Si se hubiera fijado el valor *max-repetition* de GetBulkRequest a tres, en este ejemplo sólo se hubiera necesitado una solicitud.

7.3.4 Mensaje de Solicitud de Informacion (InformRequest.)

Un mensaje InformRequest se genera y se transmite como una solicitud de una aplicación de una entidad manager SNMPv2 que desea notificar a otra aplicación, que se ejecuta también en un manager SNMPv2, información en el ámbito del MIB para un entorno local a la aplicación que envía el mensaje. El paquete se utiliza para indicar al manager del otro entorno de la información accesible en el emisor. (comunicación manager-manager a través de los límites del entorno). Las dos primeras variables en la lista de asociaciones de variables de un mensaje InformRequest son sysUpTime.0 y snmpEventID.i respectivamente. Les pueden seguir otras variables.

7.3.5 El MIB para SNMPv2.

Este MIB, define los objetos gestionados, que determinan el comportamiento de la entidadSNMPv2.

Nota: No es una sustitución del MIB-II. Las siguientes son algunas definiciones de objetos para hacerse una idea de sus contenidos. Esto lo podemos ver en el cuadro 7.7:

Cuadro 7.7. Algunas definiciones de objetos MIB

```
snmpORLastChange OBJECT-TYPE
    SYNTAX     TimeStamp
    MAX-ACCESS read-only
            STATUS     current
            DESCRIPTION
                    "El valor de sysUpTime en el momento
                            del cambio más reciente en el valor
                            o estado de cualquier instancia de
                            snmpORID."
        warmStart NOTIFICATION-TYPE
            STATUS  current
            DESCRIPTION
                    "Un trap warmStart significa que la entidad
                    SNMPv2, actuando como agente, se está
                    reinicializando a sí misma de tal modo que la
                    configuración no se altere."
```

a) Entorno de Gestión del MIB("Party MIB").

El EG del MIB define los objetos gestionados que se corresponden con las propiedades asociadas a un EG SNMPv2. En el cuadro 7.8 se muestra un ejemplo de algunos objetos del MIB:

Cuadro 7.8. *Objetos MIB*

```
partyIdentity OBJECT-TYPE
   SYNTAX      Party
   MAX-ACCESS  not-accessible
   STATUS      current
   DESCRIPTION
         "Un identificador de EG unívoco
        para un EG de SNMPv2 particular."
partyAuthProtocol OBJECT-TYPE
   SYNTAX      OBJECT IDENTIFIER
   MAX-ACCESS  read-create
   STATUS      current
   DESCRIPTION
                        "El protocolo de autentificación
                        por el que se autentifican el
                        origen y la integridad de todos
                        los mensajes que genera el EG. El
                        valor noAuth significa que los
                        mensajes no están autentificados.
                        Una vez que se crea una instancia
                        de este objeto, su valor no puede
                        ser alterado."
```

b) MIB Manager-Manager.

La finalidad de este MIB, es proporcionar los medios para la coordinación entre múltiples estaciones de gestión. Es decir, los medios por los que las funciones de control y monitorización de la gestión de red se pueden distribuir entre múltiples NMS en una gran red. Específicamente, este MIB suministra mecanismos para que una NMS solicite servicios de gestión de otra. Por tanto, una entidad SNMPv2 puede tener un doble papel; cuando proporciona información de gestión a otro manager, actúa como agente, y cuando pide información, actúa como manager. El MIB manager-manager consta de las tres tablas siguientes:

- Alarmas.
    - Eventos.
    - Notificaciones.

Cada alarma es una condición específica detectada mediante la monitorización periódica, en un intervalo de muestreo configurable, de los valores de una determinada variable con información de gestión. Un ejemplo de condición de alarma es cuando la variable monitorizada toma un valor fuera de rango. Cada condición de alarma dispara un evento, que puede a su vez desencadenar una o más notificaciones para otras NMS usando el InformRequest.

7.3.6 Protocolo Único de Autentificación y Seguridad Sapp(Single Authentication and Privacy Protocol).

El protocolo de autentificación proporciona un mecanismo para que la gestión de SNMPv2 permita identificar que las comunicaciones que genera un entorno se originan efectivamente en ese entorno.

El protocolo de autentificación proporciona un mecanismo para que la gestión de SNMPv2 permita proteger las comunicaciones que genera un entorno de cualquier intrusión.

Las principales amenazas contra las que el protocolo de seguridad de SNMPv2 aporta protección son:

- Modificación de información.
- Enmascaramiento.
- Modificación del flujo de mensajes.
- Intrusión en la información.

Los siguientes servicios de seguridad proporcionan medidas contra las anteriores amenazas:

- **Integridad de los datos.**

La proporciona el algoritmo de condensación de mensajes MD5. Se calcula un resumen o extracto de 128 bits de la porción indicada del mensaje SNMPv2 y se incluye como parte del mensaje enviado al receptor.

- **Autentificación del origen de los datos.**

A cada mensaje se le añade un prefijo con un valor secreto que comparten el emisor del mensaje y el receptor, antes de calcular el extracto.

- **Delay o retardo del mensaje.**

En cada mensaje se incluye un sello de tiempo.

- **Confidencialidad de los datos.**

La proporciona el protocolo simétrico de privacidad que encripta una porción adecuada del mensaje de acuerdo con una llave secreta conocida sólo por el emisor y el receptor. Este protocolo se usa conjuntamente con el algoritmo simétrico de encriptación, en el modo de encadenamiento de cifrado de bloques, que forma parte del DES("Data Encryption Standard"). La parte designada del mensaje se encripta y se incluye como parte el mensaje enviado el receptor.

7.4 El Nuevo Modelo Administrativo.

Uno de los propósitos del modelo administrativo para SNMPv2 es definir como la infraestructura administrativa se aplica para llevar a cabo una administración de red efectiva en diversas configuraciones y entornos.

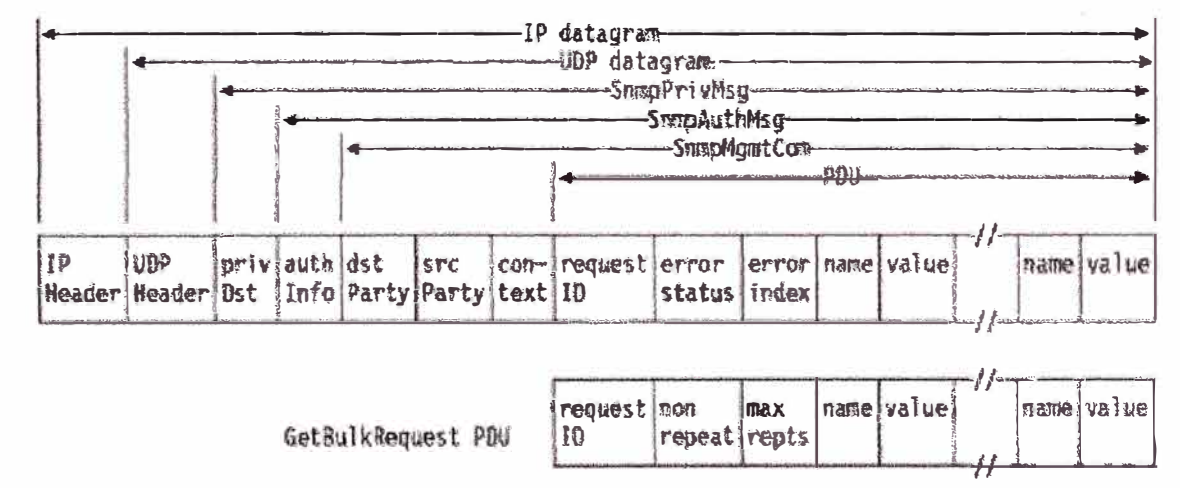

Figura 7.7. ***Formato de mensaje de SNMPv2***

El modelo implica el uso de diferentes identidades en el intercambio de mensajes. De esta forma, representa abandonar el basado en comunidades del SNMPv1 original. Al identificar sin ambigüedad al emisor y al receptor de cada mensaje, esta nueva estrategia mejora el esquema histórico de comunidades ya que permite un diseño del control de acceso a los datos más conveniente así como el empleo de protocolos de seguridad asimétricos(con llave pública) en el futuro. Ver la Figura 7.7 para observar el Formato de mensaje de SNMPv2 para conocer el nuevo formato de mensaje.

PDU

Incluye una de las siguientes PDUs

- GetRequest
- GetNextRequest
- Response
- SetRequest
- InformRequest
- SNMPv2-Trap

El GetBulkRequest tiene un formato de PDU distinto al mostrado más arriba.

Nota: El SNMP-Trap tiene ahora el mismo formato que las demás solicitudes.

SnmpMgmtCom ("SNMP Management Communication")

Añade el identificador del entorno emisor(srcParty), del receptor(dstParty) y el contexto a la PDU. El contexto especifica el ámbito de SNMPv2 que contiene la información de gestión a la que referencia la comunicación.

SnmpAuthMsg

Este campo se utiliza como información de autentificación para el protocolo de información usado por el entorno en cuestión. El SnmpAuthMsg está serializado de acuerdo con ASN.1 BER por lo que puede ser encriptado.

SnmpPrivMsg SNMP Private Message

El SNMPv2 Private Message es un mensaje SNMPv2 autentificado que posiblemente está protegido de intrusiones en la información que contiene. Un destino privado(privDst) se añade al entorno de destino.

El mensaje pasa a ser encapsulado en un datagrama UDP/IP normal y se envía a su destino a través de la red.

CAPITULO VIII
ANÁLISIS DE PROTOCOLOS DE GESTIÓN

8.1 Protocolo SNMP

Ventajas:

- Utilizan un protocolo estándar que permite integrar varios Agents de distintas marcas al Manager, compatibilizando el manejo centralizado de las redes.
- La plataforma de trabajo para el Administrador de la Red puede ser una estación UNIX o un simple PC con Windows 95.
- Constituye una plataforma de trabajo muy simple para la administración, donde entrega parámetros globales y específicos según la necesidad del administrador.

Desventajas:

- Es claramente un monitor de estados, por lo que sólo puede medir variables globales de tráfico según la información entregada por el Agent respectivo, el cual no está destinado a medir en tiempo real ninguna clase de tráfico.
- La mayor cantidad de reportes que entrega son históricos, por lo que no sirve para monitorear transiciones y/o fluctuaciones del tráfico mientras ocurren. Sólo es posible enterarse después.
- Dado que los Agents y los MIBS vienen del fabricante y el Manager sólo agrupa y despliega la información entregada, el SNMP no es una plataforma para poder medir variables de Protocolos y estándares en desarrollo o experimentación. El investigador debe programar su propio Agent y su propio MIB.

8.2 Protocolo CMIP/CMIS

Ventajas

- Alto nivel de seguridad
- Es posible distribuir los procesos de gestión a los dispositivos
- La estructura de la información de gestión es dinámica orientada a objetos (MIT Management Information Tree)
- Proporciona un protocolo de gestión de red completo para cualquier dispositivo de red
- El protocolo de gestión es orientado a conexión (gestor – dispositivo gestionado).
- El modelo OO proporciona una mejora en el manejo de notificación de eventos
- La información de gestión (MIT) colectada por el agente, se encuentra tanto en las hojas del árbol como en los nodos.

Desventajas.

- Demasiado difícil de programar.
- Sus variables son demasiado complejas.
- Su implementación es demasiado costosa, tanto a nivel de Hardware como de Software
- Los dispositivos necesitan más capacidad de procesamiento y memoria.
- La creación y borrado de objetos gestionados en los agentes, puede crear inconsistencias.
- El dispositivo gestionado necesita el stack de protocolo OSI completo (se necesitan recursos de memoria y procesamiento en el dispositivo).
- En situaciones cuando la red transporta mucho tráfico, ésta conexión de gestión se puede saturar cuando más se necesita, en situaciones difíciles.
- Utiliza mucho overhead y es difícil de implementar

CONCLUSIONES

1 Después de los tratado podemos ver que la variedad de fundamentos de los protocolos de gestión de red, se puede ver que estos se aplican en todos los campos en donde se transmite un dato o una señal, siendo estos tratados desde su "principio básico" los cuales son lo modelos de capas de red en su variedades de estándar como lo son OSI, IEEE e Internet (TCP/IP), hasta ver algunos ejemplos y aplicaciones como se ven en el Capitulo 5, el cual ha sido ampliamente desarrollado en este informe.

2 También el saber de algunos conceptos de los componentes de los estándares, así como su forma de representarlos a través de un código de programación, resulta una manera practica de demostrar como son ordenadas a través de los RFC's , la aplicación y desarrollo de estos a lo largo de los años junto con el intercambio y evolución de la tecnología.

3 Se muestra también algunas conclusiones como por ejemplo para el Protocolo Simple de Gestión de Red. SNMP es un conjunto de especificaciones de comunicación de red muy simple que cubre los mínimos necesarios de gestión de red exigiendo muy poco esfuerzo a la red sobre el que SNMP está implementado.

4 Así mismo podemos decir que CMIP es un sistema de gestión de red muy bien diseñado que mejora muchas de las deficiencias del SNMP. El precio de esto es que se ha convertido en un sistema tan grande y completo sólo las redes mejor equipadas pueden soportarlo.

GLOSARIO DE ACRÓNIMOS

Muchos de estos acrónimos se mencionan en sus respectivos capítulos pero en algunos casos hay pequeñas variaciones las cuales se muestran seguidamente:

- ANS Acuerdo de Nivel de Servicio.
- ASN.1 Abstract Syntax Notation number 1.
- CATV Cable TeleVision.
- CGI Common Gateway Interface.
- CMIP Common Management Information Protocol.
- CMIS Common Management Information Service.
- CORBA Common Object Request Broker Architecture.
- DCOM Distributed Common Object Model.
- DWDM Dense Wavelength Division Multiplexing.
- GDMO Guidelines for Definition of Management Objects.
- HTML Hypertext Markup Language.
- HTTP Hypertext Transfer Protocol.
- IDL Interface Definition Language.
- IP Internet Protocol.
- MIB Management Information Base.
- OMA Object Management Architecture.

- OMG Object Management Group.
    - ORB Object Request Broker.
- OSI Open System Interconnection.
- QoS Quality of Service.
- SNMP Simple Network Management Protocol.
- TIM Technology Integration Map.
- TMF Tele-management Forum.
- TMN Telecommunication Management Network.
- TOM Telecom Operation Map.
- UIT Unión Internacional de las Telecomunicaciones.

BIBLIOGRAFIA

[1] Rafael T. de Sousa Jr. "Administración y Gestión de Redes "
Universidad de Brasilia – 1999

[2] Greg JONES Counsellor "ITU – T of SG4 and SG15"
Study Group 4: Telecommunication management.

[3] TMN: José Antonio Lozano López, Carmen de Hita Álvarez "Telefónica Investigación y Desarrollo."

[4] SNMP BTW Sociedad Anónima.
http://www.btwsa.com.ar/siteDocs/_snmp.asp.

[5] Leschenne, Sebastián - Salazar, Martín ."Modelo de Gestión Internet SNMP RMON / Redes de datos" .Universidad Nacional de Rosario - 2002

[6] Warrier, Besaw, LaBarre & Handspicker. "CMOT y CMIP"

[7]"Network Working Working Group Request for Comments"
1189 U. Warrier (Netlabs) , Obsoletes: RFC 1095: L. Besaw (Hewlett-Packard)

[8]RFC: http://csrc.nist.gov/secpubs/rainbow/

[9]Fernando Lacunza Prieto, Eduardo Magaña Lizarrondo, Alfonso Martínez de Lizarrondo Artola. "SNMP y CMIP"
http://www.arrakis.es/~gepetto/redes/rog08p1.htm

[9]GTA / URFJ: Grupo de teleinformática y Automatización, http://www.gta.ufrj.br/grad/, 27/06/2003.

[10] Márcia Zechlinski Gusmão, "Documentos Técnicos do Grupo de Redes" - UFRGS – Universidad de Federal do Rio Grande do Sul.-2000

[11] "Arquitectura de Redes de Computadores "
Área de Ingeniería Telemática - Universidad de Oviedo .

[12] Gestión de Redes, http://www.vozip.net/.

[13] Gestión de Redes. Ministerio de Administraciones Publicas MAP, Consejo Superior de Informática. España.
http://www.csi.map.es/csi/silice/Gesred.html.

[11] Márcia Zechlinski Gusmão, "Documentos Técnicos do Grupo de Redes" - UFRGS – Universidad de Federal do Rio Grande do Sul.-2000.

[12] "Arquitectura de Redes de Computadores "
Área de Ingeniería Telemática - Universidad de Oviedo .

[13] Gestión de Redes, http://www.vozip.net/.

[14] Gestión de Redes. Ministerio de Administraciones Publicas MAP, Consejo Superior de Informática. España. http://www.csi.map.es/csi/silice/Gesred.html.