UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

GESTION DE REDES SDH

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

MIGUEL ANGEL TORRES SANCHEZ

PROMOCIÓN
1999 – II

LIMA – PERÚ
2006

GESTION DE REDES SDH

Dedico este trabajo a:

Mis Padres y Hermanos por el apoyo

que me han brindado.

SUMARIO

En el presente informe se verán los sistemas de gestión de red más importantes según los diferentes estándares actuales. Se estudia la estructura de la información de gestión y las comunicaciones entre sistemas abiertos, se describen las herramientas de gestión más utilizadas en diversos tipos de entornos de redes SDH, comparando las aproximaciones realizadas por los diversos estándares.

Se brinda una guía para los planificadores de redes y diseñadores de Redes, definiendo los requisitos de gestión exigibles a los gestores de los sistemas de transmisión SDH e ilustrando las características principales de una plataforma de gestión SDH. Además, veremos nuevas alternativas de gestión de redes y algunas pruebas de conformidad de los sistemas de gestión.

ÍNDICE

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

PRÓLOGO

La comunicación siempre ha sido una parte muy importante de la vida humana. A lo largo del tiempo, a medida que se ha desarrollado la tecnología, el hombre ha creado métodos de comunicación cada vez más sofisticados. Las invenciones del teléfono y del telégrafo en el siglo antepasado fueron avances importantes ya que estas nuevas tecnologías permitieron la comunicación directa entre personas que se encontraban muy alejadas, lo que hizo de las telecomunicaciones una realidad.

El explosivo desarrollo de las telecomunicaciones ha incrementado enormemente la complejidad de las redes y la gama de servicios disponibles, lo cual resalta la importancia de la gestión de redes como uno de los componentes esenciales para maximizar la relación costos / prestaciones, mediante la utilización de mejores recursos de configuración, supervisión y mantenimiento.

La eficiente gestión de los servicios que prestan las empresas de telecomunicaciones se ha convertido en una de las claves de la competitividad. Obtener la máxima satisfacción de sus clientes manteniendo márgenes de rentabilidad adecuados no es una tarea sencilla para estas, considerando que ello implica la gestión de una red de telecomunicaciones compuesta generalmente por equipos y sistemas de tecnologías y proveedores diversos, además el intercambio de información con otras empresas en un escenario de múltiples servicios y múltiples proveedores. Esta creciente complejidad y heterogeneidad de las modernas redes de telecomunicaciones ha generado la necesidad de buscar mecanismos simples y uniformes para gestionarlas.

El Capitulo I tiene por finalidad ofrecer una visión general de la tecnología de transmisión conocida como Jerarquía Digital Sincronía o comúnmente llamada SDH, empezando con un repaso del motivo del SDH y sus principales recomendaciones dadas por la UIT-T con

la finalidad de comprender con mayor profundidad la filosofía en que se basa dicha técnica.

En el Capitulo II se presenta una visión integrada sobre los principios, arquitecturas, plataformas, estándares y aplicaciones para la gestión de redes SDH. Se explica el modelo gestor / agente y se estudian a fondo los estándares existentes para redes SDH en el ámbito de TMN y OSI.

En el Capitulo III se describe la funcionalidad que deberá implementarse en el Gestor de Subred SDH, para realizar la gestión, tanto en el ámbito de Elementos de Red, como en el ámbito de Subred por una parte, y por otra las funciones a implementar en el propio sistema de Gestión.

En el Capitulo IV se explican las nuevas alternativas de gestión, los productos existentes en el mercado que están surgiendo y por la necesidad de realizar pruebas de conformidad una vez contratado un producto TMN se describen algunas aplicaciones.

CAPÍTULO I
JERARQUIA DIGITAL SINCRONA (SDH)

1.1 Visión General

Desde el siglo pasado, las tecnologías de telecomunicación han mejorado de forma continuada especialmente en el área de la transmisión de datos. Esta aplicación de la red de telecomunicaciones ha requerido un mayor ancho de banda a medida que las unidades de procesamiento de datos se han hecho cada vez más sofisticadas y potentes. Los sistemas de transmisión digital han proporcionado un aumento sostenido del ancho de banda a lo largo de las dos últimas décadas. Cuando la tecnología permitió la transmisión a velocidades más altas, pudo disponerse de mayor ancho de banda.

En el año 1985 la empresa Bell Core, le hace una propuesta al ANSI de estandarizar las velocidades mayores a 140Mb/s, que hasta el momento eran propietarias de cada empresa. En 1986, la Bell Core, y La AT&T, proponen al CCITT, posibles velocidades de transmisión para que las mismas sean estandarizadas, cada una de estas empresas propone diferentes velocidades transmisión posibles. Recién en el año 1988 se produce la primera regulación de la Jerarquía Digital Sincrónica (JDS), o más conocida por sus siglas en la lengua inglesa Synchronous Digital Hierarchy (SDH). La CCITT saca entonces, en su "Serie azul", las recomendaciones G707, G708 y G709 que constituyen la primera regulación de esta forma de transmisión.

Desde 1988 al día de hoy, ha habido 6 modificaciones de las recomendaciones, estando vigente hoy en día solamente la recomendación G707, que es la que se utiliza actualmente.
A partir de la introducción de la tecnología PCM hacia 1960, las redes de comunicaciones fueron pasando gradualmente a la tecnología digital en los años siguientes. Para poder soportar la demanda de mayores velocidades binarias surgió la jerarquía digital plesiocrona (PDH).

Pero como las velocidades de transmisión de esta jerarquía no son las mismas para EEUU y Japón que para Europa, las pasarelas entre redes de ambos tipos son complejas y costosas. Además si se tiene en cuenta que para poder llegar a un canal de 64Kb/s (canal de voz), habría que desarmar toda la señal PDH, hasta llegar al mismo, es decir abría que poner una cadena de multiplexores y demultiplexores, con el incremento de costo que esto significa.

1.2 Definición de SDH

SDH es un estándar para redes de telecomunicaciones de "alta velocidad, y alta capacidad"; más específicamente es una jerarquía digital sincrónica. Este es un sistema de transporte digital realizado para proveer una infraestructura de redes de telecomunicaciones más simple, económica y flexible.

Las viejas redes fueron desarrolladas en el tiempo en que las transmisiones punto a punto eran la principal aplicación de la red. Hoy en día los operadores de redes requieren una flexibilidad mucho mayor. El objetivo de la jerarquía SDH, nacida en los años 80, era subsanar estas desventajas inherentes a los sistemas PDH, como así también normalizar las velocidades superiores a 140Mb/s que hasta el momento eran propietarias de cada compañía (ver Tabla N° 1.1).

Tabla N° 1.1 Comparación entre PDH y SDH

PDH	SDH
No existen velocidades de transmisión normalizadas por encima de 565 Mbits/s.	Basada en Rec. UIT-T. Velocidades normalizadas de 155Mb/s, 622 Mb/s, y 2.5 Gb/s.
Solo tiene facilidades básicas de control y almacenamiento.	Gestión sofisticada basada en normas de TMN.
Presenta cadenas de multiplexación caras y rígidas necesarias para extraer o incorporar canales individuales.	Uso de Add/Drop para proveer, inserción y extracción de canales. Menos equipo requerido.
Los cambios en la provisión de servicio consumen tiempo, son manuales y costosos.	Respuesta mas rápida y mas flexible para la demanda de nuevos servicios y usuarios
La reconfiguración y protección es cara y difícil de lograr.	Restauración implementada a bajo costo, basada en la nueva arquitectura.

La tecnología SDH, ofrece a los proveedores de redes las siguientes ventajas:

1.2.1 Altas velocidades de transmisión

Los modernos sistemas SDH logran velocidades de 10 Gbit/s. SDH es la tecnología mas adecuada para los backbones, que son realmente las superautopistas de las redes de telecomunicaciones actuales.

1.2.2 Función simplificada de inserción / extracción

Comparado con los sistemas PDH tradicionales, ahora es mucho más fácil extraer o insertar canales de menor velocidad en las señales compuestas SDH de alta velocidad. Ya no hace falta demultiplexar y volver a multiplexar la estructura plesiócrona, procedimiento que en el mejor de los casos era complejo y costoso. Esto se debe a que en la jerarquía SDH todos los canales están perfectamente identificados por medio de una especie de "etiquetas" que hacen posible conocer exactamente la posición de los canales individuales.

1.2.3 Alta disponibilidad y grandes posibilidades de ampliación

La tecnología SDH permite a los proveedores de redes reaccionar rápida y fácilmente frente a las demandas de sus clientes. Por ejemplo, conmutar las líneas alquiladas es sólo cuestión de minutos. Empleando un sistema de gestión de redes de telecomunicaciones, el proveedor de la red puede usar elementos de redes estándar controlados y monitorizados desde un lugar centralizado.

1.2.4 Fiabilidad

Las modernas redes SDH incluyen varios mecanismos automáticos de protección y recuperación ante posibles fallos del sistema. Un problema en un enlace o en un elemento de la red no provoca el colapso de toda la red, lo que podría ser un desastre financiero para el proveedor. Estos circuitos de protección también se controlan mediante un sistema de gestión.

1.2.5 Plataforma a prueba de futuro

Hoy día, SDH es la plataforma ideal para multitud de servicios, desde la telefonía tradicional, las redes RDSI o la telefonía móvil hasta las comunicaciones de datos (LAN,

WAN, etc.) y es igualmente adecuada para los servicios más recientes, como el video bajo demanda (VOD) o la transmisión de video digital vía ATM.

1.2.6 Interconexión

Con SDH es mucho más fácil crear pasarelas entre los distintos proveedores de redes y hacia los sistemas SONET. Las interfaces SDH están normalizadas, lo que simplifica las combinaciones de elementos de redes de diferentes fabricantes. La consecuencia inmediata es que los gastos en equipamiento son menores en los sistemas SDH que en los sistemas PDH.

El motor que genera toda esta evolución es la creciente demanda de más ancho de banda, mejor calidad de servicio y mayor fiabilidad, junto a la necesidad de reducir costes manteniendo la competitividad. Para el futuro de las redes de transporte se tiende hacia velocidades mayores, tal como en el sistema STM-64 (multiplexado por división en el tiempo, TDM de 10 Gbps), pero los costes de los elementos de ese tipo son aún muy elevados, lo que está retrasando el proceso.

La alternativa es una técnica llamada DWDM (multiplexación densa por división de longitud de onda) que mejora el aprovechamiento de las fibras ópticas monomodo, utilizando varias longitudes de onda como portadoras de las señales digitales y transmitiéndolas simultáneamente por la fibra. Los sistemas actuales permiten transmitir 16 longitudes de onda, entre 1520 nm y 1580 nm, a través de una sola fibra. Se transmite un canal STM-16 por cada longitud de onda, lo que da una capacidad de unos 40 Gbit/s por fibra. Ya se ha anunciado la ampliación a 32, 64 e incluso 128 longitudes de onda.

Conectada al empleo del multiplexado DWDM se observa una tendencia hacia las redes en las que todos los elementos son ópticos. Ya existen en el mercado multiplexores add/drop (inserción / extracción) ópticos y se están realizando pruebas de dispositivos ópticos de transconexión (cross-connects). En términos del modelo de capas OSI, este desarrollo significa básicamente la aparición de una capa DWDN, adicional debajo de la capa SDH. Probablemente pronto veremos velocidades binarias aún más elevadas gracias a la tecnología DWDM.

1.3 Componentes de una Red Síncrona

La Figura 1.1 es un diagrama esquemático de una estructura SDH en anillo con varias señales tributarias. La mezcla de varias aplicaciones diferentes es típica de los datos transportados por la red SDH. Las redes síncronas deben ser capaces de transmitir las señales plesiócronas y, al mismo tiempo, ser capaces de soportar servicios futuros como ATM. Todo ello requiere el empleo de distintos tipos de elementos de red.

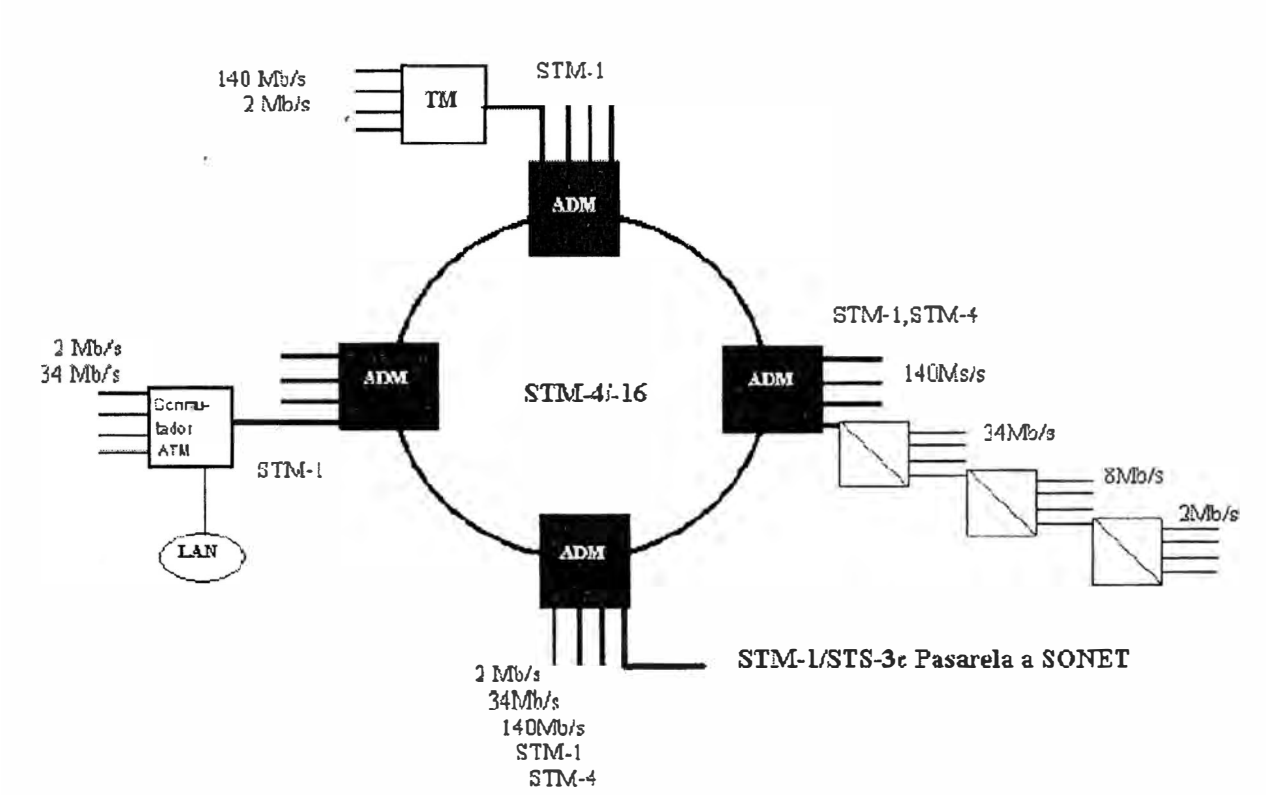

Figura 1.1 Diagrama esquemático de redes de comunicaciones híbridas

Las redes SDH actuales están formadas básicamente por 4 tipos de elementos. La topología (estructura de malla o de anillo) depende del proveedor de la red.

1.3.1 Regeneradores

Como su nombre implica, los regeneradores se encargan de regenerar el reloj y la amplitud de las señales de datos entrantes que han sido atenuadas y distorsionadas por la dispersión y otros factores. Obtienen sus señales de reloj del propio flujo de datos entrante. Los mensajes se reciben extrayendo varios canales de 64 kbit/s (por ejemplo, los canales de servicio El, F1 de la cabecera RSOH). También es posible enviar mensajes utilizando esos canales. Los regeneradores síncronos supervisarán también la calidad de transmisión de la línea a través del byte B1.

1.3.2 Multiplexores

Se emplean para combinar las señales de entrada plesiócronas y terminales: síncronas en señales STM-N de mayor velocidad. Los multiplexores síncronos pueden funcionar como interfaz entre señales PDH y señales SDH y entre señales SDH múltiplex de orden inferior y señales SDH de orden superior. Un MUX será una parte de las DXC y de los ADM.

1.3.3 Multiplexor de inserción y extracción (ADM)

Permiten insertar (o extraer) señales plesiócronas y síncronas de menor velocidad binaria en el flujo de datos SDH de alta velocidad. Gracias a esta característica es posible configurar estructuras en anillo, que ofrecen la posibilidad de conmutar automáticamente a un trayecto de reserva en caso de fallo de alguno de los elementos del trayecto.

1.3.4 Cross-Connection digital (DXC)

Este elemento de la red es el que más funciones tiene. Permite mapear las señales tributarias PDH en contenedores virtuales, así como conmutar múltiples contenedores, hasta VC-4 inclusive. Puede conectar y desconectar señales de orden inferior.

1.3.5 Gestión de los elementos de la red

La red de gestión de las telecomunicaciones (TMN) se considera un elemento mas de la red síncrona. Todos los elementos SDH mencionados hasta ahora se controlan por software, lo que significa que pueden monitorizarse y controlarse desde un lugar remoto, una de las ventajas más importantes de los sistemas SDH.

Todos los elementos de red (NE) anteriores son accesibles a través de la red de gestión de telecomunicaciones (TMN) para la operación y mantenimiento del propio NE y de la red completa.

1.4 Característica principales de SDH

- Velocidad básica 155Mb/s (STM-1).
- Técnica de multiplexado a través de punteros.

- Estructura modular: A partir de la velocidad básica se obtienen velocidades superiores multiplexando byte por byte varias señales STM-1. Las velocidades multiplexadas, a diferencia de PDH, son múltiplos enteros de la velocidad básica.
- A través del puntero, se puede acceder a cualquier canal de 2Mb/s.
- Posee gran cantidad de canales de overhead que son utilizados para supervisión, gestión, y control de la red.

1.5 Estructura de la trama básica SDH

La trama básica adoptada por CCITT es la llamada STM-1, está estructurada en bytes y tiene las siguientes características **[1]**:

- Largo: 2430 Bytes
- Duración: 125 uS.
- Velocidad: 155,520 Mb/s
- Carga útil (Payload): 2340 bytes (149,760 Mb/s)

Según la Figura 1.2 la trama STM-1 provee una matriz de 9 filas por 270 columnas (bytes). Esta matriz debe ser recorrida en izquierda a derecha, y en sentido descendente, para así ir siguiendo la secuencia en serie.

Se divide en tres zonas:

- SOH (Section Over Head), o encabezado de sección: el cual a su vez está subdividido en dos, un encabezado para secciones regeneradoras llamado RSOH, y otro para secciones multiplexoras llamado MSOH.
- Punteros de AU.
- Payload (C4)

La duración de transmisión de cada trama es de 125uS, la cual corresponde a una frecuencia de repetición de trama de 8000 Hz. La capacidad de transmisión de un byte individual es de 64Kb/s.

No hay que perder de vista que esta es solamente una representación, en realidad los bits van siguiendo una secuencia en serie, es decir cuando terminamos de recorrer una matriz, comenzaría la siguiente.

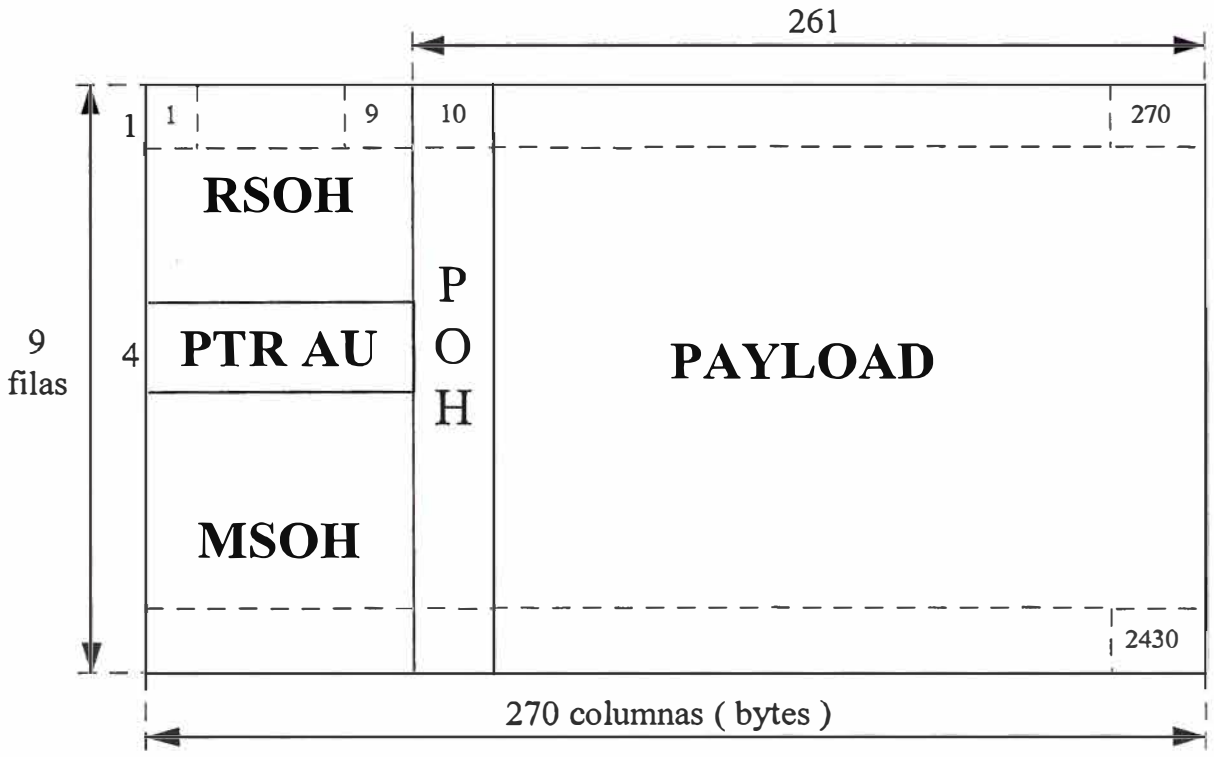

Figura 1.2 Trama básica STM-1

1.5.1 Utilización de los encabezados

Los encabezados tienen por función, entre otras, el monitoreo de calidad entre las diferentes secciones. En la Figura 1.3 se muestra el encabezado de sección de un STM-1.

También son los encargados de brindar canales de servicio, datos y gestión. A través de bytes de los encabezados viaja el protocolo de gestión con el cual se conectan los equipos SDH a la red de gestión TMN (Telecomunication Management Network).

a. Bytes del RSOH

- A1, A2: F.A.W. (Palabra de alineación de trama)
- C1 : identificador de AUG
- B1 : byte reservado para monitoreo de errores de bits en la sección regeneradora (entre dos regeneradores)
- E1 y F1: Estos dos bytes proveen canal de servicio y canal de usuario.
- D1 a D3: DCC (Data communication channel) de la sección regeneradora

b. Bytes del MSOH

- B2: tres bytes reservados para monitoreo de errores de bits en la sección multiplexora.
- K1, K2: Dos bytes reservados para APS (Automatic Protection Switching) 1+1 y 1:n, dentro de K2 tres bits son para AIS y FERF.
- D4-D12: DCC (Data communication channel) de la sección multiplexora.
- Z1, Z2: Uso futuro.
- E2: Canal de servicio 64 Kbit/s entre terminales.
- S1: Etiqueta de sincronismo.
- M1: MS-FEBE, numero de errores detectados en B2 del equipo remoto.

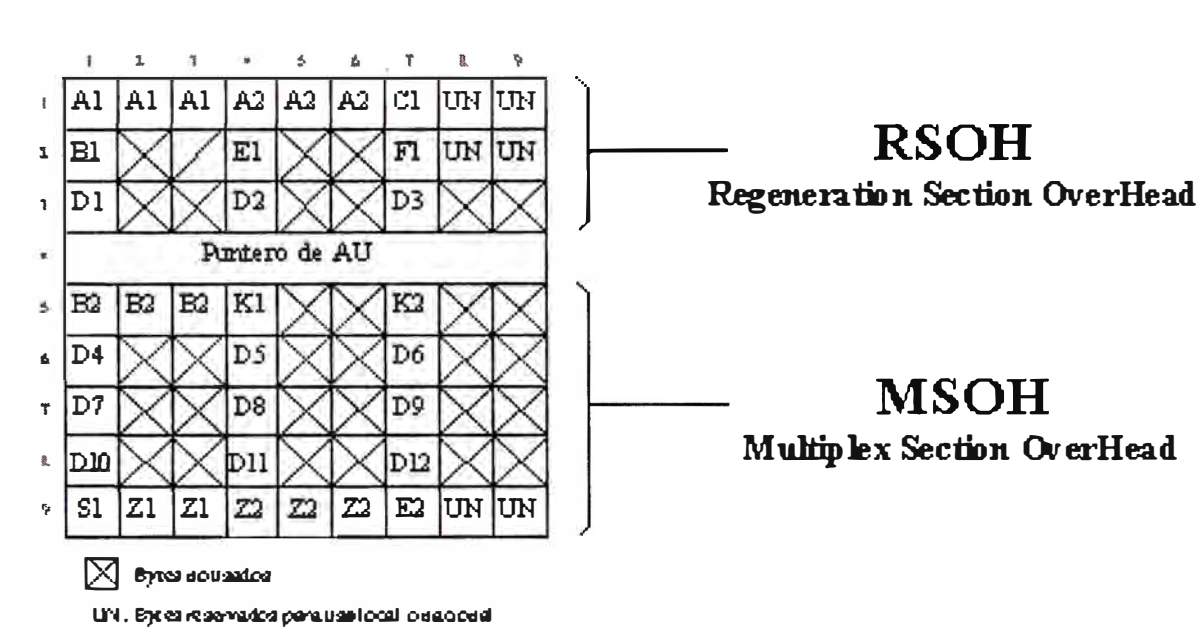

Figura 1.3 Descripción del encabezado de sección de STM-1 (SOH)

1.5.2 Función de los punteros

El AU4 está formado por un VC4 mas un puntero asociado dentro de la trama de un STM-1. El puntero hace posible el manejo de las pérdidas o defasajes de sincronismo debido a diferentes relojes usados en la sincronización de los equipos. El puntero asociado con un proceso de justificación (positiva, negativa o nula) provee a la trama SDH el manejo de señales desfasadas en frecuencia sin pérdida de información.

De hecho, el clock de una señal STM-1 puede ser independiente del VC4 transportado. En caso de haber un desfasaje entre las velocidades de trama y VC4, el valor del puntero se incrementará o decrementará según sea necesario. Pueden ocurrir dos casos:

a. La velocidad del VC4 es mayor que la velocidad del payload del STM-1

En este caso, para realizar el ajuste es necesario el uso de bytes adicionales para aumentar la capacidad del VC4. Estos bytes adicionales son usualmente bits de relleno, ubicados en el puntero dentro del SOH. La operación por la cual se usan estos bytes para transmitir información es llamada "justificación negativa".

b. La velocidad del VC4 es menor que la velocidad del payload del STM-1

Ahora, faltan bytes para completar el VC4. Los bytes de relleno se usan para ocupar ese lugar y así llenar el VC4. Esta operación se denomina "justificación positiva". Las justificaciones positivas y negativas, respectivamente, van acompañadas de un incremento o decremento en el valor del puntero.

1.6 Estructura de Multiplexación

A continuación se describe el proceso de formación de la trama STM-1 a partir de los diferentes tributarios incluidos en ella.

1.6.1 Contenedor (Cn)

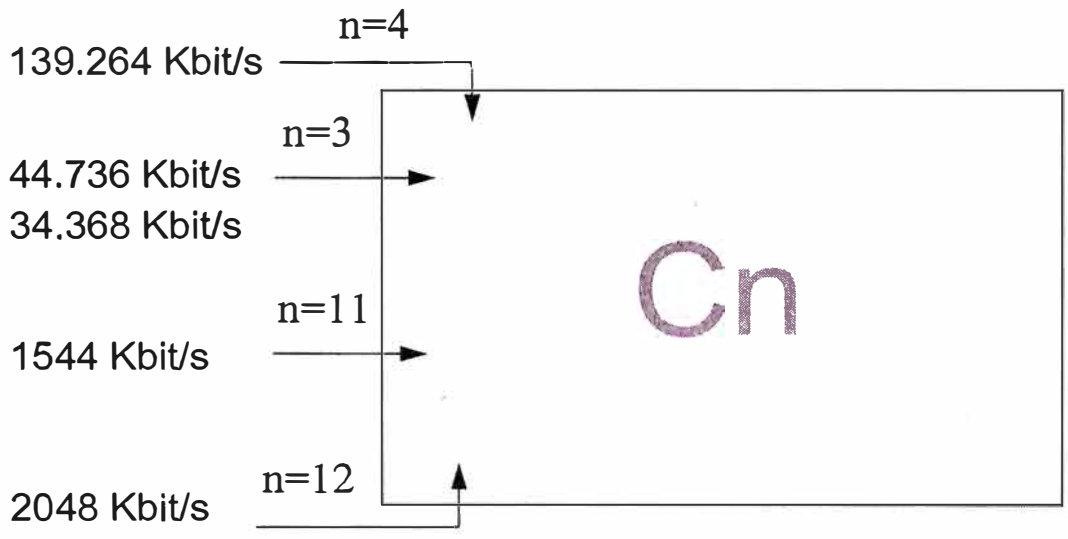

Figura 1.4 Contenedor Cn

n : índice de referencia del contenedor.

Una señal transmitida por la red sincrónica es previamente encapsulada dentro de un contenedor el cual está preparado para albergar esta señal y mantiene la estructura de trama

síncrona. El contenedor es una entidad cuya capacidad esta definida de manera que asegure la transmisión de señales tributarias definidas en la jerarquía plesiócrona (PDH) como se muestra en la Figura 1.4.

Los tributarios PDH son estructurados en bytes (8 bits). La operación de colocarlos en correlación es llamada mapeo. El mapeo organiza los bytes de información, de relleno y de servicio dentro del contenedor. Esta operación esta definida en la Rec. G709 de CCITT.

1.6.2 Contenedor Virtual (VC)

Al contenedor Cn se le asocia un encabezado de sección llamado POH (Path Over Head). Se denomina contenedor virtual VC al conjunto de contenedor mas el encabezado de sección. Donde VC-n = POH + Cn.

Se hace una distinción entre contenedores virtuales de bajo orden (VC11, VC12, VC2, y VC3) y los de alto orden (VC3 y VC4). Los VC de bajo orden están formados por un contenedor y su POH correspondiente. Los VC de alto orden pueden contener también a VCs de bajo orden.

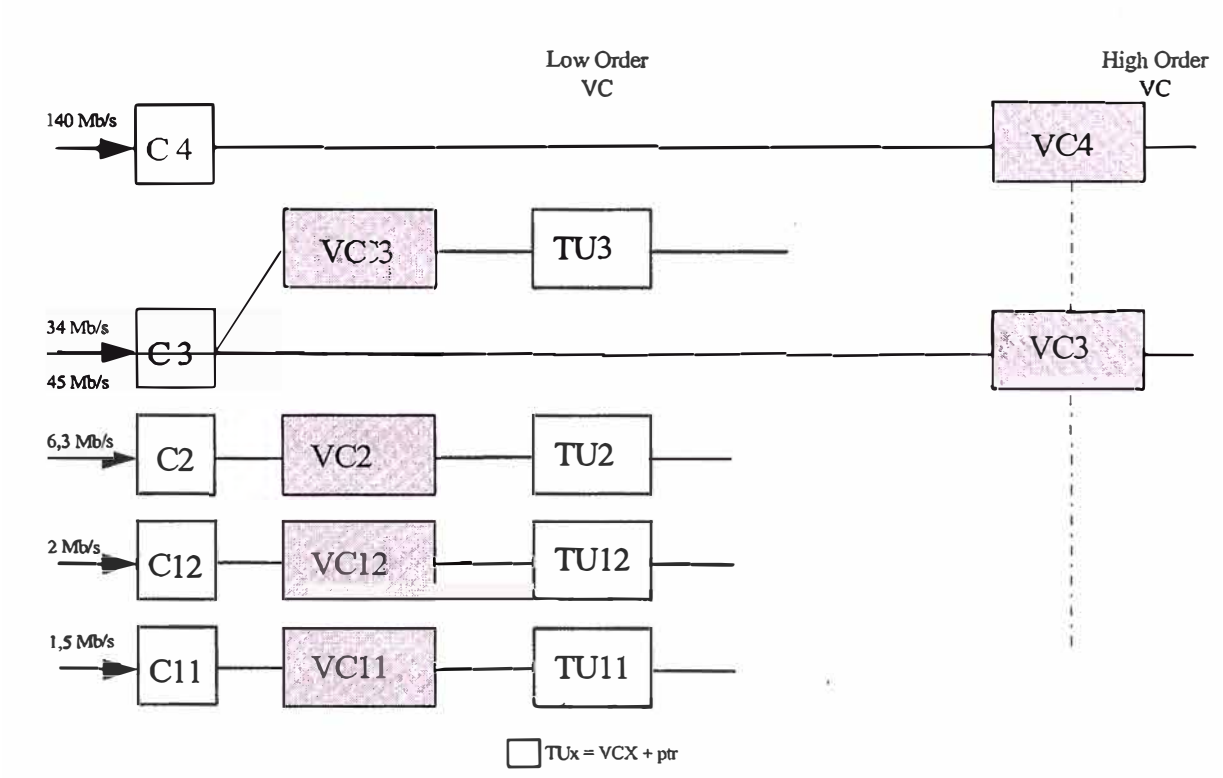

Figura 1.5 Formación de TU

1.6.3 Unidad Tributaria (TU)

Los TUs están compuestos por un contenedor virtual de bajo orden mas un puntero y se muestra en la Figura 1.5. El puntero indica el lugar en el cual comienza el VC en la trama.

1.6.4 Grupo de unidad tributaria (TUG)

El TUG está compuesto por un conjunto de TUs multiplexados y se muestra en la Figura 1.6. El TUG2 puede estar formado por 4xTU11, o 3xTU12, o 1xTU2. El TUG3 puede formarse con 7xTUG2 o 1xTU3.

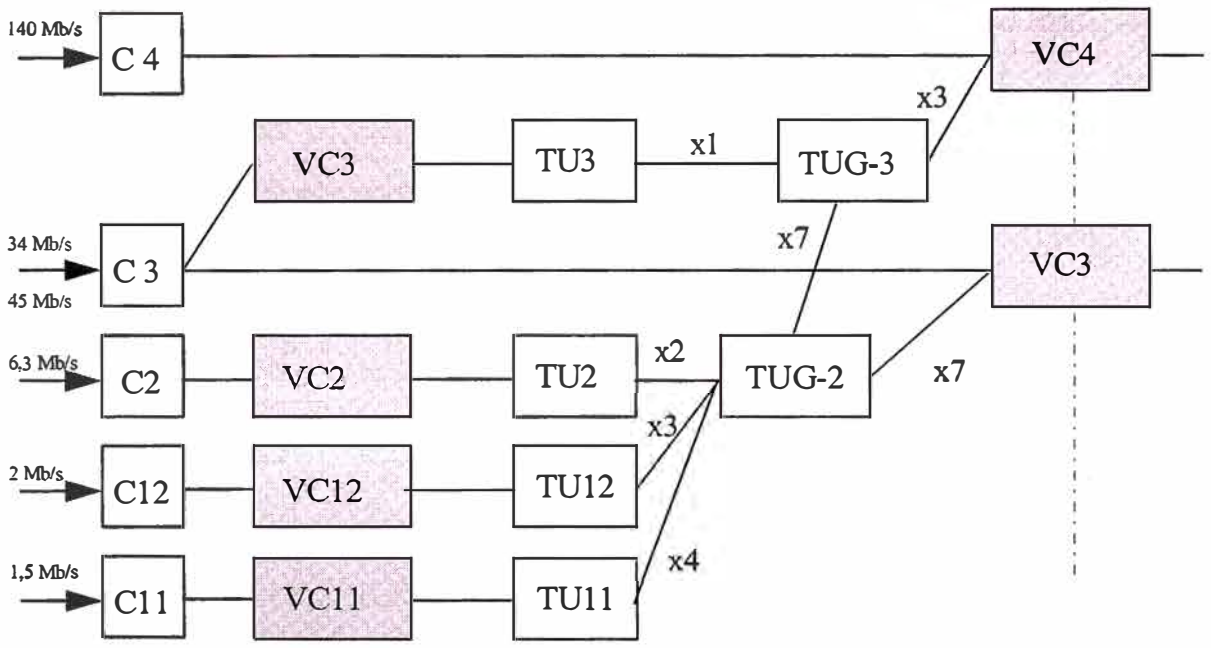

Figura 1.6 Formación de TUG

1.6.5 Unidad Administrativa (AU)

El AU lo compone un VC de alto orden mas un puntero de AU. El valor del puntero indica el punto de comienzo del VC en la trama usada. Un AU4 se compone de un VC4 más un puntero asociado. Un AU3 se compone de un VC3 más un puntero asociado.

1.6.6 Grupo de unidades administrativas (AUG)

El AUG no es una nueva estructura física. Es sólo una estructura virtual dentro de la trama SDH. EL AUG es el espacio que ocupa un AU4 con su trama de transmisión, o el que ocupan 3 AU3 multiplexados.

1.6.7 Trama de transmisión STM-N

En las Figuras 1.7 y 1.8 se muestra la estructura de multiplexado según ITU-T [2] y ETSI, respectivamente.

La trama STM-N (Synchronous Transport Module) se obtiene:

- Multiplexando N AUGs.
- Agregando un encabezado de sección, llamado SOH (Section Over Head).

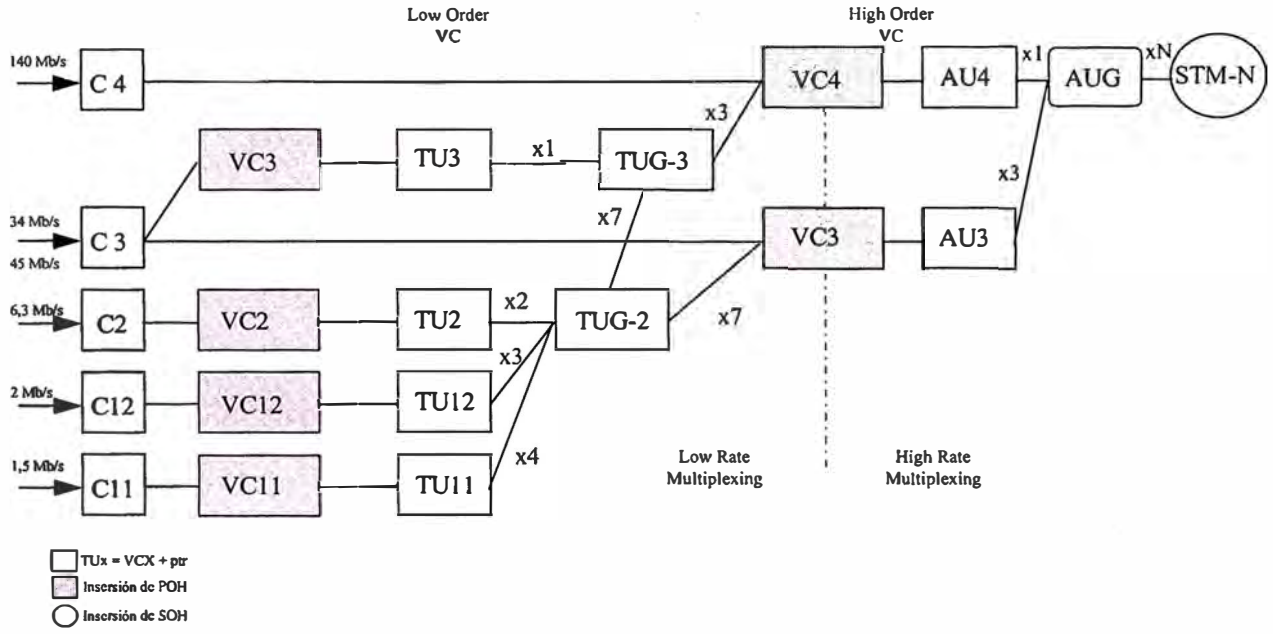

Figura 1.7 Estructura de multiplexado ITU-T

Ejemplos:

- STM-1 (155,520 Mb/s) es la trama básica, la cual contiene 1 AUG y su SOH.
- STM-4 (622,080 Mb/s), consta de 4 AUGs y su SOH.
- STM-16 (2488,320 Mb/s), contiene 16 AUGs y su SOH.

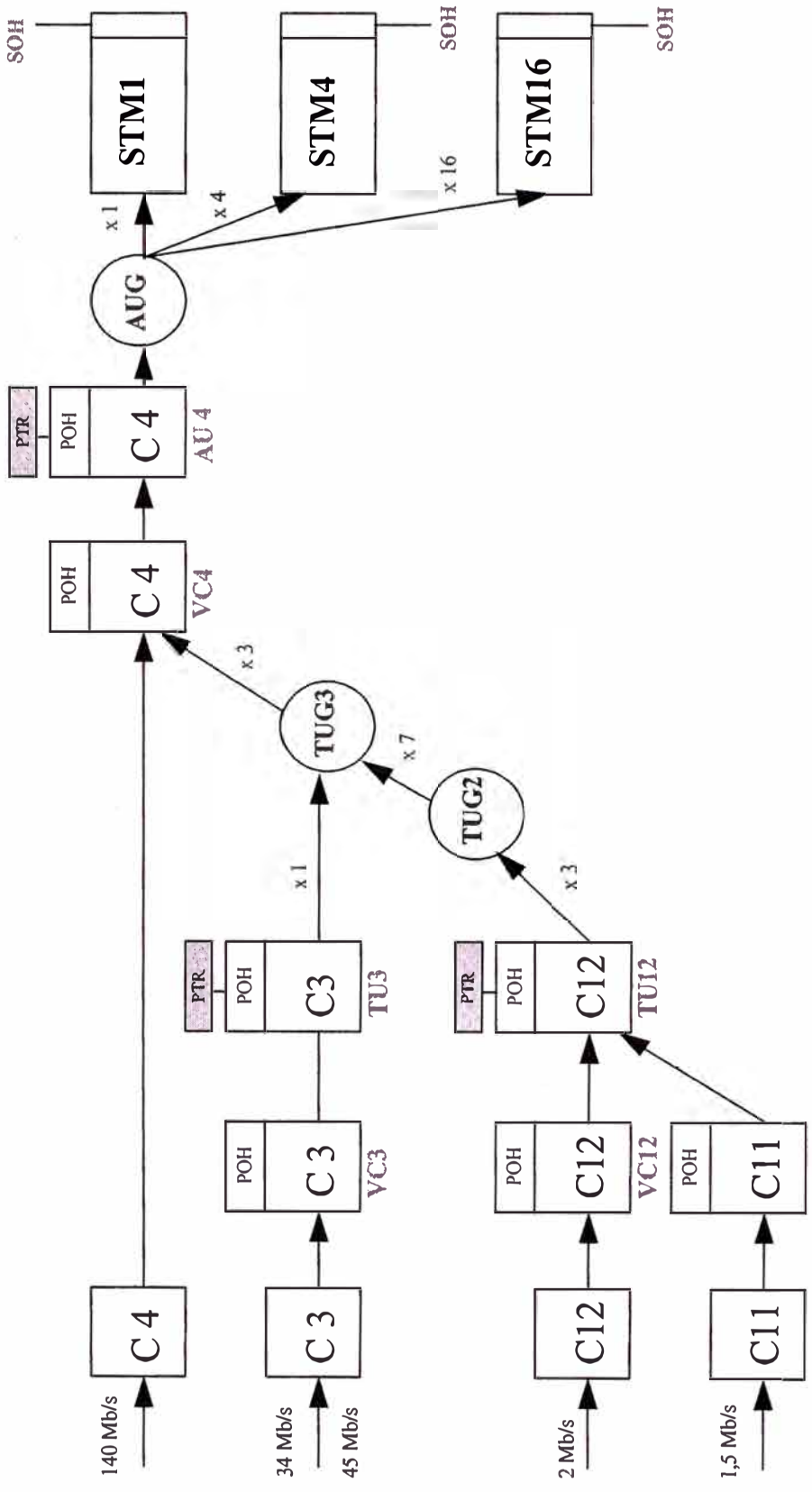

Figura 1.8 Estructura de multiplexado ETSI

1.7 Recomendaciones de la ITU-T relativas a los Sistemas SDH

Dado que el estándar abarca toda una serie de posibles variantes, que en función del área geográfica de utilización (USA, Japón ó resto del mundo) o de aplicaciones específicas el estándar se recoge en toda su extensión y alcance (al menos lo especificado hasta la actualidad) en las siguientes recomendaciones del ITU-T **[2]**:

G.652/653/654: Características de las fibras ópticas mono-modo.
G.703: Características físicas / eléctricas de las interfaces digitales jerárquicas.
G.707: Velocidades Binarias de la SDH. STM-1, STM-4, STM-16, STM-N.
G.708: Interfaz de Nodo de Red para SDH. Principio de multiplexación, elementos de multiplexación, estructura de trama, definiciones de encabezamiento o tara.
G.709: Estructura de Multiplexación Síncrona. Mapeo, contenedores y unidades tributarias, punteros, asignación de encabezamiento o tara.
G.772: Puntos de supervisión protegidos de los sistemas de transmisión digital.
G.774: Modelo de información de gestión de la jerarquía digital síncrona desde el punto de vista de los elementos de red.
G.774.01: Supervisión de la calidad de funcionamiento de la jerarquía digital síncrona desde el punto de vista de los elementos de red.
G.774.02: Configuración de la estructura de cabida útil de la jerarquía digital síncrona desde el punto de vista de los elementos de red.
G.774.03: Gestión de la protección de secciones de multiplexión de la jerarquía digital síncrona desde el punto de vista de los elementos de red.
G.774.04: Gestión de la protección de conexiones de subred de la jerarquía digital síncrona desde el punto de vista de los elementos de red.
G.774.05: Gestión en la jerarquía digital síncrona de la funcionalidad de supervisión de la conexión de orden superior e inferior desde el punto de vista de los elementos de red.
G.780: Vocabulario de términos para redes y equipos de la jerarquía digital síncrona.
G.783: Características de los bloques funcionales de los equipos de la jerarquía digital síncrona (sustituye a la versión 01/94 de G.781, G-782 y G.783).
G.784: Gestión de la jerarquía digital síncrona.
G.803: Arquitectura de redes de transporte basadas en la jerarquía digital síncrona.
G.810: Definiciones y terminología para las redes de sincronización.

G.811: Requisitos de temporización en las salidas de relojes de referencia primarios adecuados para la explotación plesiócrona de enlaces digitales internacionales.

G.813: Características de temporización de los relojes subordinados de los equipos de la jerarquía digital síncrona (SEC).

G.825: Control de la fluctuación de fase y de la fluctuación lenta de fase en las redes digitales basadas en la jerarquía digital síncrona.

G.826: Parámetros y objetivos de características de error para trayectos digitales internacionales de velocidad binaria constante que funcionen a la velocidad primaria o a velocidades superiores.

G.831: Capacidades de gestión de las redes de transporte basa das en la jerarquía digital síncrona.

G.832: Transporte de elementos SDH en redes PDH.

G.841: Tipos y características de las arquitecturas de protección de las redes SDH.

G.842: Interfuncionamiento de las arquitecturas de protección de las redes SDH.

G.957: Interfaces ópticas para equipos y sistemas relacionados con la jerarquía digital síncrona.

G.958: Sistemas de líneas digitales basados en la jerarquía digital síncrona para su uso en cables de fibra óptica.

M.2101: Límites de calidad de funcionamiento para la puesta en servicio y el mantenimiento de trayectos y secciones múltiplex de la jerarquía digital síncrona.

M.2110: Puesta en servicio de trayectos, secciones y sistemas internacionales de transmisión.

M.2120: Detección y localización de fallos en trayectos, secciones y sistemas de transmisión digital.

0.150: Requisitos generales para la instrumentación de mediciones de la calidad de funcionamiento de equipos de transmisión digital.

0.17s: Equipos de medida de la fluctuación de fase y de la fluctuación lenta de fase para sistemas digitales basados en la jerarquía digital síncrona.

0.181: Equipo de medición para determinar la característica de error en las interfaces de módulo de transporte síncrono de nivel N.

M.3xxx: Sobre Gestión.

CAPÍTULO II
GESTIÓN DE REDES SDH EN EL AMBITO DE TMN y OSI

2.1 Visión General de la Gestión de Red.

Teoría y práctica de la gestión de red han surgido en los primeros tiempos de las telecomunicaciones, mucho antes que se desarrollaran las tecnologías de comunicación de datos en banda ancha, tales como SONET/SDH, ATM, etc. Impulsadas por la demanda creciente sobre calidad de red y por la necesidad de reducir costos operacionales, se tornaron más utilizadas las herramientas de gestión de red que se interconectaban a través de redes LAN y WAN; adicionalmente, en una manera relativamente simple, también se aplicaron medios de gestión en redes analógicas de comunicación de voz (telefonía).

Con el incremento de volumen de computadoras y otros dispositivos inteligentes, los elementos de sistemas interdependientes tenían que ser interconectados por diferentes herramientas de comunicación (líneas de comunicación de datos, LANs, etc.). Redes de gran escala, con topologías complejas han evolucionado en este sentido. Sin embargo, si una red no opera de modo confiable, sino se pueden identificar posibles errores por métodos simples, y sino se pueden mantener bajo control a determinados parámetros operacionales de la red, y eventualmente ser modificados, los usuarios no obtendrán demasiados beneficios de la red implementada con gran costo y penuria.

El desarrollo de Sistemas de Gestión de Red estuvo motivado por la intención de eliminar todos estos problemas. Eventualmente, la gestión de red apunta a permitir al personal autorizado, a monitorear ó cambiar importantes parámetros operacionales de la red, utilizando uno ó más terminales de gestión. En la práctica, los Sistemas de Gestión de Red están implementados con software apropiado, el campo del cual básicamente se extiende a todos los elementos inteligentes de la red y a algunos elementos de hardware suplementarios ubicados en los nodos de la red.

La ventaja y resultado de la aplicación de un Sistema de Gestión de Red puede ser resumido como sigue:

- Incremento de confiabilidad (disminución de tiempo requerido para detección de error, diagnóstico y corrección de error, incremento de eficiencia de los esfuerzos apuntados a la corrección de errores, la posibilidad de enrutar tráfico de red automáticamente sí alguna parte de la red opera en déficit).
- Incremento de seguridad (acceso a la red controlado y regulado para cada usuario y de acuerdo a autorizaciones y autenticaciones predefinidas).
- Nuevos servicios provistos a los usuarios de red (adquisición de información de tarificación, de tráfico, etc.).
- Monitoreo computarizado efectivo de sistema (almacenando información de tarificación, estadística, seguimiento y evaluación de carga y performance de la red, así como estadísticas de errores, soporte de estrategias de desarrollo de red, etc.).

En conclusión, los objetivos de los Sistemas de Gestión de Red son:

- Costos operacionales decrecientes.
- Aumento en la calidad de los servicios.

El logro de estos objetivos es compartido por:

- Usuarios
- Operadores de red
- Proveedores de servicios
- Fabricantes de equipamiento de comunicaciones

La operación de un Sistema de Gestión de Red prácticamente significa ejecutar los siguientes pasos esenciales:

- Adquirir y recolectar datos característicos acerca de los elementos de la red, acerca de su operación e interrelación en la red (condiciones operacionales, performance, condiciones de falla y tipos de eventuales malos funcionamientos, relación entre elementos vecinos, parámetros de tráfico y carga, etc.).
- Almacenar y evaluar los datos recolectados a través de un centro de procesamiento de datos del sistema.

- Controlar la operación de la red (modificando la funcionalidad de algunos elementos en la red sí es necesario) como conclusión y resultado de la evaluación.

En la medida en que un Sistema de Gestión de Red debe ejecutar tareas de gestión de servicios y/o negocios, pueden ser necesario pasos adicionales como parte de la operación, tales como:

- Registro de contratos de servicio y gestión de servicios de cliente.
- Elaboración de planes de negocios y diseños técnicos.
- Modelado y simulación de procesos técnicos y/o financieros, etc.

Notar que la demanda de ejecución de los pasos operacionales listados requiere la habilidad de una arquitectura de red sofisticada, la presencia de elementos de red apropiadamente elaborados, así como un Sistema de Gestión de Red apropiado. Esto significa que las técnicas eficientes de gestión de red pueden ser consideradas como resultado de una asociación y desarrollo inseparables de las tecnologías de comunicación LAN/WAN y los métodos de gestión de red propiamente dichos. La gestión de red es enriquecida con mayor cantidad de herramientas efectivas por la evolución de las tecnologías de las comunicaciones. En lo que concierne a las soluciones de red actuales, no todos los pasos descriptos han sido comúnmente percibidos y elaborados hasta ahora.

En el primer escalón de desarrollo, la "gestión de red" estaba limitada a simplemente visualizar condiciones de falla (por ejemplo, por el destello de indicadores luminosos en el equipo) y supervisarlas por parte del personal operativo. De acuerdo al sentido presente de la terminología no puede ser considerada en absoluto como gestión de red. El primer paso significativo en el camino para lograr una supervisión de red eficiente, fue la asociación de las condiciones de falla y otros parámetros del sistema por computadoras, y su almacenamiento automático. La disponibilidad de los datos almacenados proveyeron una oportunidad conveniente para su evaluación programada. El incremento en el tamaño de la red y volumen de los datos resultaron en la mejora de los algoritmos de evaluación.

Los datos colectados y su evaluación permitieron luego que la operación apropiada de la red se restaure automáticamente en el caso de ciertas fallas del sistema (ejemplo: por medio de elementos de sistema stand-by/hot stand-by ó mediante una predeterminada

reconfiguración del sistema). El control de la operación de la red por parte de un Sistema de Gestión de Red fue aplicado únicamente en LANs sofisticadas por un considerable período de tiempo. Las redes WAN tradicionales, sin embargo, basadas en tecnología PDH ampliamente utilizada aún hoy, ofreció un número limitado de medios para un control de red apropiado.

Como efecto de la nuevas tecnologías de comunicación (tal como SONET/SDH y ATM) el contraste usual entre LANs y WANs, comunicación de voz y datos, tiende a desvanecerse ó desaparecer. Este es un momento importante en la promoción de la evolución de los métodos de gestión de red y probablemente resulte en una teoría homogénea de gestión de red. Productos reales de gestión de red apropiados para satisfacer gestión de servicios, planeamiento tanto de negocios como técnico, y tareas de modelado, están apareciendo en estos días.

TMN es un estándar de gestión actualizado que permite la construcción de Sistemas de Gestión de Red con el más comprensivo set de funciones de gestión de red explotando las facilidades de las más actualizadas tecnologías de comunicación.

La Gestión de Redes interviene en diferentes campos de aplicación:

- Redes públicas y privadas, incluidas las redes ISDN, ATM, redes Móviles, redes privadas virtuales y redes inteligentes.
- Terminales de Transmisión.
- Sistemas de transmisión digitales y analógicos.
- Centrales digitales y analógicas.
- Redes LAN, WAN, MAN.
- Redes de conmutación de circuitos y de paquetes.

A continuación se describen las tres principales arquitecturas de gestión de red: El Modelo OSI, El Modelo TMN y El Modelo Internet (SNMP).

2.2 Modelo OSI

La Organización Internacional de Normalización (ISO) ha definido una arquitectura de gestión OSI (Open Systems Interconnection) cuya función es permitir supervisar, controlar

y mantener una red de datos. Está dividida en cinco categorías de servicios de gestión [3] denominadas Áreas Funcionales Específicas de Gestión (Specific Management Functional Areas, SMFA). Estas categorías son las siguientes:

2.2.1 Gestión de configuración

La gestión de configuración comprende una serie de facilidades mediante las cuales se realizan las siguientes funciones:

- Iniciación y desactivación.
- Definición o cambio de parámetros de configuración.
- Recogida de información de estado.
- Denominación de los elementos de la red.

2.2.2 Gestión de fallos

Detección, diagnóstico y corrección de los fallos de la red y de las condiciones de error. Incluye:

- Notificación de fallos
- Sondeo periódico en busca de mensajes de error
- Establecimiento de alarmas

2.2.3 Gestión de prestaciones

Se define como la evaluación del comportamiento de los elementos de la red. Para poder efectuar este análisis es preciso mantener un histórico con datos estadísticos y de configuración.

2.2.4 Gestión de contabilidad

Determinación de los costes asociados a la utilización de los recursos y la asignación de sus correspondientes cargas.

2.2.5 Gestión de seguridad

Comprende el conjunto de facilidades mediante las cuales el administrador de la red modifica la funcionalidad que proporciona seguridad frente a intentos de acceso no autorizados. Incluye aspectos como la gestión de claves, cortafuegos e históricos de seguridad.

La arquitectura de gestión OSI define un objeto gestionable como la interfaz conceptual que han de presentar los dispositivos que ofrecen funciones de gestión. El proceso de supervisión y control de un objeto gestionable se realiza mediante una serie de interacciones. Estas interacciones son de dos tipos:

- **De operación:** el gestor solicita algún dato al objeto gestionable o desea realizar alguna acción sobre él.
- **De notificación:** cuando el objeto gestionable intenta enviar algún dato al gestor como consecuencia de algún evento ocurrido en el dispositivo.

Un objeto gestionable se caracteriza además por un conjunto de atributos que son las propiedades o características del objeto, y un comportamiento en respuesta a las operaciones solicitadas. La comunicación entre el gestor y el objeto gestionable no es directa, se realiza mediante un intermediario: el agente de gestión (esto se corresponde con un modelo centralizado gestor-agente). La función del agente es controlar el flujo de información de gestión entre el gestor y el objeto. Este control lo realiza comprobando una serie de reglas de gestión (por ejemplo que el gestor tenga la capacidad para solicitar una determinada operación), que han de cumplirse para poder realizar la operación. Estas reglas se incluyen en los datos como parte de la solicitud de una operación.

El flujo normal de información de gestión y control entre el gestor y el agente se realiza mediante el Protocolo de Información de Gestión Común (Common Management Information Protocol, CMIP), perteneciente al nivel de aplicación OSI. El protocolo permite que un sistema se pueda configurar para que opere como gestor o como agente. La mayoría de las realizaciones prácticas de sistemas gestionados se configuran con unos pocos sistemas operando en modo gestor, controlando las actividades de un gran número de sistemas operando en modo agente.

Cuando dos procesos se asocian para realizar una gestión de sistemas, deben establecer en qué modo va a operar cada uno de ellos (en modo agente o en modo gestor). Los procesos indican, mediante las denominadas unidades funcionales, qué funcionalidades de gestión y estándares utilizarán durante la asociación. Otros componentes de la arquitectura de gestión OSI son:

2.2.6 Estructura de la Información de Gestión (Structure of Management Information, SMI)

Define la estructura lógica de la información de gestión OSI. Establece las reglas para nombrar a los objetos gestionables y a sus atributos. Documento (RFC 1155 **[4]**) que define un conjunto de subclases y tipos de atributos que son en principio aplicables a todos los tipos de clases de objetos gestionables en la MIB.

2.2.7 Base de Información de Gestión (Management Information Base, MIB)

Representa la información que se está utilizando, modificando o transfiriendo en la arquitectura de los protocolos de gestión OSI. La MIB **[5]** conoce todos los objetos gestionables y sus atributos. No es necesario que esté centralizada físicamente en un lugar concreto, puede estar distribuida a través del sistema y en cada uno de sus niveles. Los objetos MIB se organizan en una estructura de árbol que incluye la rama pública (estándar) y privada (propietaria).

2.2.8 Servicios de Información de Gestión Común (Common Management Information Services, CMIS)

Es un conjunto de reglas que identifican las funciones de una interfaz OSI entre aplicaciones, utilizado por cada aplicación para intercambiar información y parámetros. CMIS define la estructura de la información que es necesaria para describir el entorno. Prácticamente todas las actividades de la gestión de red OSI están basadas en diez primitivas de servicio CMIS que son utilizadas por las SMFAs.

2.2.9 Notación de Sintaxis Abstracta Uno(ASN.1)

En el nivel de presentación es necesario un formato de datos común para todos los tipos de máquinas, para hacerlo se define unas estructuras de datos que son independientes del hardware, sistemas operativos y lenguajes de programación de las máquinas.

En los niveles más altos de OSI (Aplicación y presentación), las unidades de datos de protocolo (Protocol Data Unit, PDU) son más complejas de expresar que en los niveles inferiores, ya que vienen dados por estructuras de datos, esto quiere decir que las aplicaciones intercambian estructuras de datos. Esto hace necesario la aparición de una

notación sintaxis abstracta que permita expresar estas estructuras, cuyo formato depende de la aplicación.

Se podía haber utilizado el formato de representación de estructuras de datos de cualquier lenguaje de alto nivel (C, Pascal) ya que el formato es similar, pero para hacerlo independiente del lenguaje se ha preferido normalizar una notación particular. No obstante hay compiladores que convierten de ASN.1 a la notación particular del lenguaje que se esté utilizando para desarrollar la aplicación.

ISO ha estandarizado una notación de sintaxis abstracta denominada ASN.1 (Abstract Sintax Notation 1) y las reglas para traducirla a una sintaxis de transferencia BER (Basic Encoding Rules). La denominación de la Norma / Recomendación es:

- ASN.1: ISO 8824/UIT-T X.208.
- BER: ISO 8825/UIT-T X.209.

ASN.1 y BER son utilizadas también en la arquitectura Internet por el protocolo SNMP (Simple Network Management Protocol), este es un protocolo que permite enviar información de gestión de red. Este tipo de notación permite definir directamente APDUs (Application Protocol Data Unit) del nivel de aplicación.

2.2.10 Gestión basada en CMIP

La gestión basada en (OSI) CMIP define un verdadero Sistema de Gestión de Red orientado a objeto basado en la arquitectura de comunicaciones de OSI de siete capas. El modelo de referencia OSI se define en las series de recomendaciones X.200 de CCITT/ITU-T, y en estándar 7498 de ISO. La estandarización del modelo OSI comenzó en los últimos años de los 80s , y no ha sido totalmente terminado hasta ahora. Los primeros estándares de gestión de OSI fueron definidos por ISO; más tarde fueron adoptados y desarrollados por CCITT/ITU-T (recomendaciones de la serie X.700) y otros institutos de estandarización.

Los Sistemas de Gestión de Red basados en (OSI) CMIP pueden ser aplicados para gestionar:

- Redes de área local (LANs)

- Redes corporativas y redes privadas de área amplia (WANs)
- Redes nacionales e internacionales

El protocolo de séptima capa (aplicación) utilizado por la gestión OSI es el protocolo común de información de gestión (Common Management Information Protocol, CMIP).En un ambiente de gestión basado en (OSI) CMIP, el proceso de aplicación de usuario (cuya operación está basada en el principio de manager/agent) es provisto con el servicio común de información de gestión (Common Management Information Service, CMIS) en función de una interface de programa de aplicación (API) por la denominada entidad de aplicación de gestión de sistemas (Systems Management Application Entity, SMAE), la cual está implementada en la séptima capa (Aplicación) del modelo de siete capas ISO/OSI.

La operación de la gestión está basada en el principio de manager/agent. Las funciones de manager, agent, y MIB son básicamente similares a las de SNMP, o más característicamente a las de TMN.

Los siguientes son los elementos más importantes de la interface de programa de aplicación de gestión OSI **[6]**:

- elemento común de servicio de información de gestión (Common Management Information Service Element, CMISE)
- elemento de servicio de operación remota (Remote Operation Service Element, ROSE)
- elemento de servicio de aplicación de gestión de sistemas (Systems Management Application Service Element, SMASE)
- elemento de servicio de control de asociación (Association Control Service Element, ACSE)
- transferencia de archivo, acceso, y gestión (File Transfer, Access, and Management, FTAM)

El CMISE es responsable por la generación de requerimientos (requests) estándares básicos y el procesamiento de mensajes de respuesta según lo definido por el CMIS. El CMIS puede ser utilizado por un proceso de aplicación en un ambiente de gestión

centralizado ó descentralizado para intercambiar información y comandos para el propósito de sistemas de gestión. (Ver recomendación X.710 de ITU-T).

El ROSE controla y supervisa las interacciones entre entidades remotas de una aplicación distribuida, donde esas interacciones pueden ser modeladas y soportadas como operaciones remotas. Una operación remota es requerida por una entidad; la otra entidad intenta ejecutar la operación remota y luego reportar el resultado del intento (recomendaciones X.219 y X.229 de ITU-T).

El SMASE provee servicios (de gestión de sistemas) que dan soporte a funciones de gestión específicas (recomendación X.750 de ITU-T).

El ACSE es responsable de ejecutar la negociación inicial a efectos de decidir si se puede establecer una conexión de datos y ponerla a disposición de la comunicación. De acuerdo a la definición de la recomendación X.217: " ACSE provee facilidades básicas para el control de una asociación de aplicación entre dos entidades de aplicación. ACSE incluye dos unidades funcionales opcionales. Una unidad funcional soporta el intercambio de información soportando autenticación durante el establecimiento de la asociación. La segunda unidad funcional soporta la negociación del contexto de aplicación durante el establecimiento de la asociación" (recomendaciones X.217 y X.227 de la ITU-T).

FTAM organiza y gestiona acceso a archivos para propósitos de aplicación, de acuerdo a las especificaciones de ANS.1 (recomendación X.209 de ITU-T).

En términos del principio de manager/agent, el manager como un elemento de software del sistema puede generar operaciones de gestión en la forma de requests CMIS a cualquiera de los agentes software vía el protocolo de gestión CMIP. El agente retransmite esos requests a los objetos gestionados (managed objects, MOs) correspondientes, los cuales representan los recursos físicos y lógicos a ser gestionados, y los ejecuta sobre los MOs apropiados.

CMIP puede también proveer reportes manejados por eventos para el manager y puede identificar eventos substanciales que influenciaron el estado de los objetos gestionados.

Los requests CMIP/CMIS, generados por el manager al agente a efectos de iniciar una operación, son los siguientes:

- M-GET (obtiene un valor de atributo de uno ó más objetos gestionados)
- M-SET (establece / modifica el valor de atributo de uno ó más objetos gestionados)
- M-ACTION (ejecuta una acción específica sobre uno ó más objetos gestionados)
- M-CREATE (crea un nuevo objeto gestionado)
- M-DELETE (elimina uno ó más objetos gestionados)
- M-CANCEL-GET (cancela una operación M-GET requerida previamente y aún pendiente)

Adicionalmente, el agent puede enviar al manager:

- M-EVENT-REPORT (notifica al manager acerca de un evento que aconteció en el objeto gestionado)

La selección de los objetos gestionados que tienen que ser afectados por una operación CMIP/CMIS dada, es facilitada por la observación y el filtrado. La observación establece la identificación de los objetos gestionados a los cuales se les va a aplicar un filtro. El filtrado establece un conjunto de tests a cada miembro del grupo de los objetos gestionados, previamente observados, para extraer un subset de ellos.

El modelo de objeto de la gestión OSI está basado en las recomendaciones X.722 de CCITT/ITU-T, ampliamente conocida como GDMO(Guidelines for the Definition of Managed Objects). La estructura de información de gestión (SMI) está descripta en las recomendaciones X.720 de CCITT/ITU-T. SMI es similar a aquella de SNMP; sin embargo, los objetos estándar involucrados y sus atributos son diferentes. Los objetos estándar en la gestión OSI son también descriptos utilizando sintaxis ASN.1, definida en la recomendación X.208 de ITU-T.

CMIP es un protocolo real manejado por eventos; el modelo de objeto de GDMO es más comprensible que aquél de SNMP. Eso significa que la gestión OSI es más apropiada para gestionar redes grandes y complejas. La aplicación de Sistemas de Gestión de Red basados en (OSI) CMIP se está difundiendo gradualmente. Su significación crecerá en el futuro (particularmente para proveedores de servicios de telecomunicaciones). Sin embargo,

TMN, como sistema de gestión estandarizado, más comprensible, basado en OSI , parece ser un muy fuerte competidor de CMIP.

2.3 Modelo TMN

El término TMN (Telecommunications Management Network) fue introducido por la ITU-T, y está definido en la recomendación M.3010. Aunque en un principio no hubo mucha colaboración entre los grupos de gestión de red de la ISO y el CCITT (Comité Consultivo Internacional Telegráfico y Telefónico, actualmente la ITU-T), posteriormente fueron incorporados varios conceptos del modelo OSI al estándar TMN [7]. En concreto:

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

TMN es un conjunto de capacidades que permiten el intercambio y procesamiento de información de gestión de una Red de Telecomunicaciones. TMN debe proporcionar una arquitectura organizada a fin de conseguir la interconexión entre diversos sistemas de operaciones y/o equipos de telecomunicaciones. TMN ofrece funciones de Gestión y de Comunicación (Transporte) entre los diversos elementos que conforman la Red de Telecomunicaciones.

Un aspecto diferenciador con el modelo OSI consiste en la introducción del modelo TMN de una red separada de aquella que se gestiona, con el fin de transportar la información de gestión. A diferencia del modelo OSI, en el cual se definen cinco áreas funcionales, el estándar TMN no entra en consideraciones sobre las aplicaciones de la información gestionada. Por el contrario, se define la siguiente funcionalidad:

- El intercambio de información entre la red gestionada y la red TMN.
- El intercambio de información entre redes TMN.
- La conversión de formatos de información para un intercambio consistente de información.
- La transferencia de información entre puntos de una TMN.
- El análisis de la información de gestión y la capacidad de actuar en función de ella.
- La manipulación y presentación de la información de gestión en un formato útil para el usuario de la misma.

- El control del acceso a la información de gestión por los usuarios autorizados.

El modelo TMN define tres arquitecturas diferenciadas:

- Arquitectura funcional.
- Arquitectura física.
- Arquitectura de la información.

2.3.1 Arquitectura funcional

Las redes de telecomunicaciones son controladas y gestionadas a través de una TMN, cada nuevo sistema de telecomunicaciones soporta a una subred de gestión. Por ejemplo, los sistemas SDH poseerán, en su conjunto, una SMN (SDH management network). Cada subsistema SDH poseerá una SMS (SDH management subnetwork). La arquitectura funcional describe la distribución de la funcionalidad dentro de la TMN, con el objeto de definir los bloques funcionales a partir de los cuales se construye la TMN.

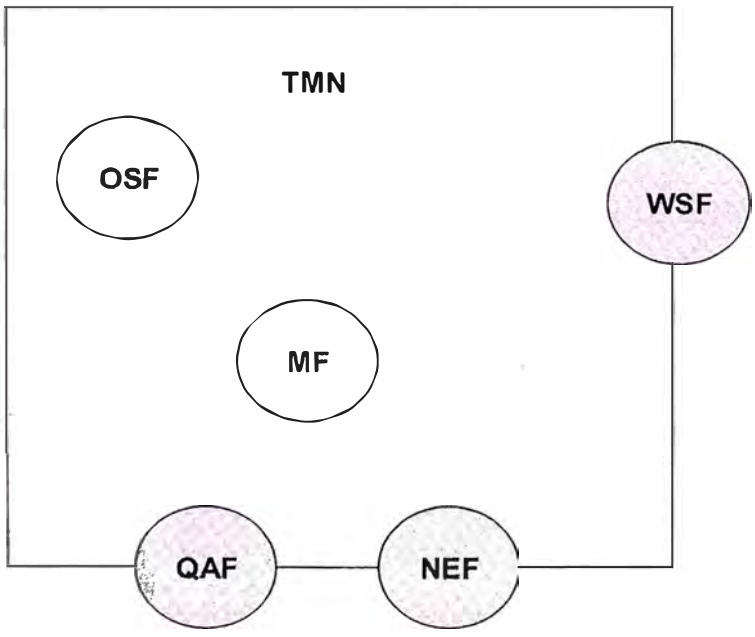

Figura 2.1 Bloques Funcionales TMN

Se definen cinco tipos de bloques funcionales, en la Figura 2.1 se ve si se encuentra en la frontera o no del bloque TMN. Estos bloques proporcionan la funcionalidad que permite a la TMN realizar sus funciones de gestión. Dos bloques funcionales que intercambian información están separados mediante puntos de referencia. La transferencia de información entre los bloques de función se realiza a través de una red de comunicación de

datos , utilizando la función de comunicación de datos (DCF). A continuación se describen los distintos tipos de bloques funcionales:

a. Función de operación de sistemas (Operation System Function, OSF)

Los OSF procesan la información relativa a la gestión de la red con el objeto de monitorizar y controlar las funciones de gestión. Cabe definir múltiples OSF dentro de una única TMN.

b. Función de estación de trabajo (Work-Station Function, WSF)

Este bloque funcional proporciona los mecanismos para que un usuario pueda interactuar con la información gestionada por la TMN.

c. Función de elemento de red (Network Element Function, NEF)

Es el bloque que actúa como agente, susceptible de ser monitorizado y controlado. Estos bloques proporcionan las funciones de intercambio de datos entre los usuarios de la red de telecomunicaciones gestionada.

d. Adaptadores Q (Q - Adapter Function, QAF)

Este tipo de bloque funcional se utiliza para conectar a la TMN aquellas entidades que no soportan los puntos de referencia estandarizados por TMN.

e. Función de mediación (Mediation Function, MF)

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

Puede realizar funciones de almacenamiento, adaptación, filtrado y condensación de la información. En la Figura 2.2 se especifican los puntos de referencia posibles entre los distintos bloques funcionales.

Cada bloque funcional se compone a su vez de un conjunto de componentes funcionales, considerados como los bloques elementales para su construcción. Estos componentes se identifican en la norma pero no están sujetos a estandarización.

	NEF	OSF	MF	QAF_{q3}	QAF_{qx}	WSF	Non-TMN
NEF		q_3	q_x				
OSF	q_3	x*, q_3	q_3	q_3		f	
MF	q_x	q_3	q_x		q_x	f	
QAF_{q3}		q_3					m
QAF_{qx}			q_x				m
WSF		f	f				g**
Non-TMN				m	m	g**	

m, g = no son puntos de referencia TMN
* El punto de referencia x solo aplica cuando cada OSF está en una TMN diferente.
** El punto de referencia g se sitúa entre el WSF y el usuario, quedando fuera del estándar.

Figura 2.2 Relación entre bloques funcionales

2.3.2 Arquitectura física

Describe las interfaces y el modo en que los bloques funcionales se implementan en equipos físicos, es decir se encarga de definir como se implementan los bloques funcionales mediante equipamiento físico y los puntos de referencia en interfaces. En la Figura 2.3 se ilustra la representación de la arquitectura física de una TMN.

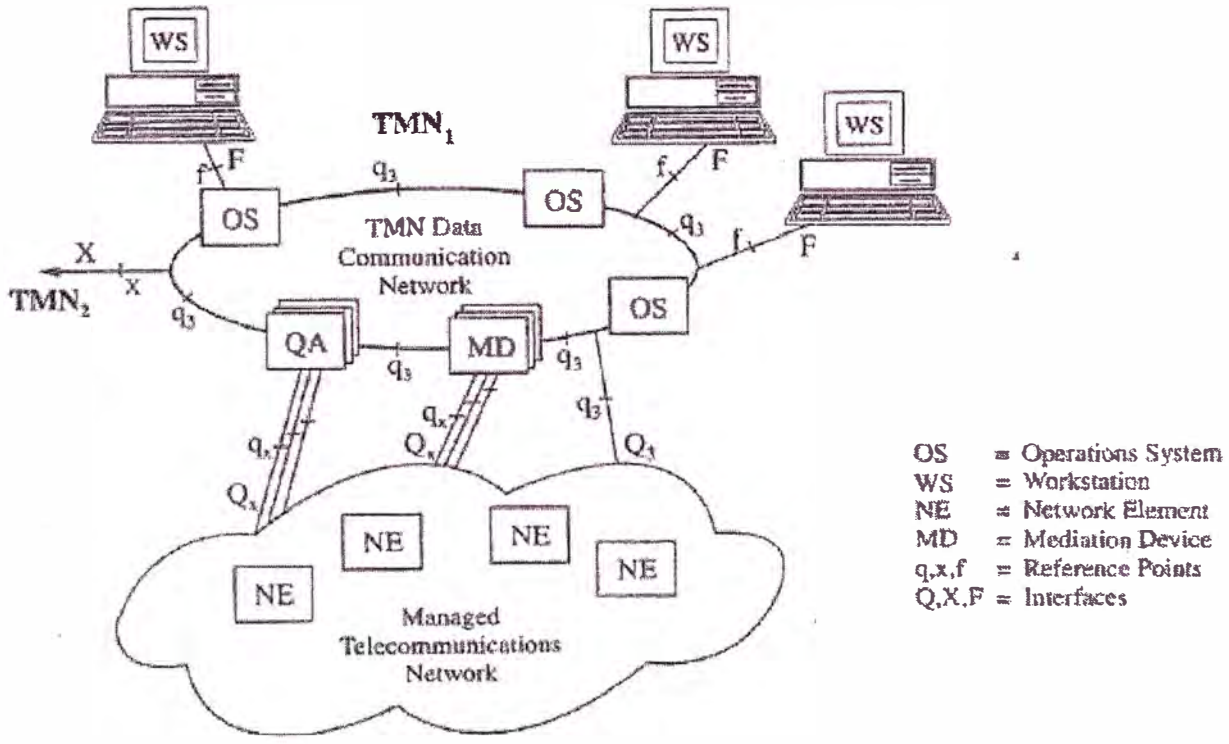

Figura 2.3 Arquitectura física de una TMN

a. Bloques constructivos

En la arquitectura física se definen los siguientes bloques constructivos:

- Elemento de red (NE)
- Dispositivo de mediación (MD)
- Adaptador Q (QA)
- Sistema de operaciones (OS)
- Red de comunicación de datos (DCN)
- Estación de Trabajo (WS)

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

b. Interfaces

Las interfaces son implementaciones de los puntos de referencia, y son comparables a las pilas de protocolos. Existe una correspondencia uno a uno entre los puntos de referencia y las interfaces, excepto para aquellos que están fuera de la TMN, es decir, los puntos de referencia g y m.

2.3.3 Arquitectura de la Información

Sigue los principios de los modelos OSI de gestión (CMIS y CMIP) y directorio (X.500, Recomendación de ITU-T para el mantenimiento distribuido de archivos y directorios).Las características generales del modelo de información de TMN son discutidas por las recomendaciones M.3010 y M.3100 de CCITT/ITU-T. Recomendaciones adicionales tratan los modelos de información para gestión de redes SDH y PDH (Ejemplo: recomendación G.774).

Esencialmente, la gestión de red involucra el intercambio de información entre procesos de gestión. El modelo de información de gestión de red TMN se soporta, en gran medida, sobre el modelo de gestión de red OSI/CMIP. La arquitectura de información de TMN está basada sobre un modelo orientado a objeto, aplica intercambio de información orientado a transacción, y utiliza el principio así llamado de agent/manager (agente / gestor).

Los conceptos básicos usados en la definición de la arquitectura de información de TMN son similares a aquellos aplicados en SNMP y OSI/CMIP. Ellos son:

- Objeto gestionado (Managed Object: MO)
- Agente (Agent)
- Gestor (Manager)
- Base de Información de Gestión (Management Information Base, MIB)

2.3.4 Arquitectura lógica de niveles

De acuerdo a la terminología TMN, las OSFs de la gestión de red están separadas en cuatro capas jerárquicas. Cada capa de la jerarquía dada define un grupo apropiado de operaciones de gestión. Estas capas son construidas una sobre otra; ellas (y sus operaciones apropiadas) están muy interrelacionadas.

El estándar TMN define las siguientes cuatro capas de la OSF:

- Capa de gestión de elemento de red (NE).
- Capa de gestión de red.
- Capa de gestión de servicio.
- Capa de gestión de negocio.

Las OSFs en estas capas interactúan con las OSFs en las mismas u otras capas dentro de la misma TMN a través de un punto de referencia "q3", y con aquellas de otra TMN a través de un punto de referencia "x".

Adicionalmente, la gestión de un elemento de red está basada en los datos colectados acerca de los respectivos elementos de la red , los elementos de red en si mismos pueden ser considerados como la capa más baja en la jerarquía.
En contraste con las cuatro capas de OSF, la capa de los elementos de red no involucra OSF, pero está relacionada con la NEF.

a. Capa de elemento de red (NEL)

Los elementos de red son componentes básicos de la red gestionada, instalados como dispositivos físicos , especificados por funciones e interfaces estándares, capaces de

distribuir datos en su operación, y proveer medios para ser controlados en una forma específica por el sistema de gestión.

b. Capa de gestión de elemento de red (EML)

La capa de gestión de elemento de red gestiona cada elemento de red sobre una base individual ó en grupo. La gestión de NE incluye la reunión de datos de cada uno de los elementos de red y el control individual de ellos. En esta capa, las decisiones sobre el cambio de estado de cualquiera de los NEs individualmente deben basarse en información acerca del mismo elemento, y no puede depender del estado de cualquier otro de los NEs ó del estado de la red entera.

La gestión básica de fallas, así como las operaciones de gestión de performance , tales como monitoreo y muestra de condiciones de faltas ó performance de tráfico de cualquiera de los elementos simples de red, así como la toma de acciones elementales para eliminar un error (ejemplo: conmutar a un canal auxiliar dentro del mismo elemento de red, etc.) son ejecutados por la capa de gestión de NE.

c. Capa de gestión de red (NML)

La capa de gestión de red tiene la responsabilidad por la gestión de la red completa como es soportada por la capa de gestión de elemento. Esta capa transgrede la competencia de la gestión de elemento de red y es responsable por la interconexión y cooperación de todos los elementos de red en el sistema gestionado.

Las tareas de esta capa incluyen gestión de configuración (ambas, estática y dinámica), gestión de eventos, faltas, y performance a nivel de red (todo esto empleando una aproximación de sistema, ejemplo: por aplicación de algoritmos de evaluación y correlación de error / performance), así como la gestión de seguridad (monitoreando los requests de usuario y tomando las acciones apropiadas a efectos de prevenir cualquier acceso no autorizado a la red).

d. Capa de gestión de servicio (SML)

Se relaciona con la gestión de red y es responsable de los aspectos contractuales de los servicios provistos a clientes ó disponibles para potenciales nuevos clientes. La gestión de

servicio apunta a establecer relaciones entre los servicios provistos por la red y los requerimientos de los usuarios ó clientes. Los clientes y los contratos de servicio son grabados, los clientes y los parámetros de servicio apropiados son relacionados, se traza la calidad de servicio, las quejas de los clientes son reportadas, y nuevas órdenes son aceptadas y procesadas, etc., en esta capa de gestión.

e. Capa de gestión de negocio(BML)

La gestión de negocio es responsable por la empresa total. Tiene que ver con aspectos técnicos y de negocios en función de un complejo orgánico de la actividad de los operadores de red, y tiene la responsabilidad por la empresa total. Las funciones incluidas en esta capa son tarificación y contabilidad (accounting), gestión de mantenimiento, control de costos, control de inventario de repuestos, diseño de nuevos elementos de red y/o nuevos servicios de red, modelado técnico y optimización, y planeamiento y evaluación de réditos de nuevas inversiones, etc.

La capa de gestión de negocio incluye funcionalidad propietaria. A efectos de prevenir acceso a su funcionalidad, las OSFs en la capa de gestión de negocios no tienen generalmente puntos de referencia "x" e interfaces "X". Esta capa se incluye en la arquitectura TMN para simplemente facilitar las especificaciones requeridas por las otras capas de gestión. Sin embargo, aún puede ser necesario que la capa de gestión de negocios interactúe con otros sistemas de gestión ó información. La tarea de estas interacciones deberían ser resueltas por soluciones especiales de software.

Las capas lógicas de la jerarquía de gestión no están definidas en total detalle por los estándares existentes. Las tareas y procesos de las diferentes capas y las reglas de intercambio de datos entre ellas no están exactamente determinados al presente. La estructura de capas está esquemáticamente cubierta por las recomendaciones M.30 y M.3010. En la literatura técnica, la discusión de funcionalidad de gestión de red es a menudo confinada a un simple listado de funciones de gestión sin detalle de sus jerarquías.

En la práctica, las soluciones estándar están mayormente restringidas a realizar las capas de gestión de elemento de red y gestión de red. Frecuentemente usadas, funciones de gestión estándar esencialmente corresponden a las tareas de estas dos capas de gestión. Aún,

relativamente pocas compañías ofrecen soluciones reales para la gestión de servicio. En algún grado, productos de gestión de red apropiados para ejecutar tareas de gestión de negocios están ahora mayormente bajo desarrollo.

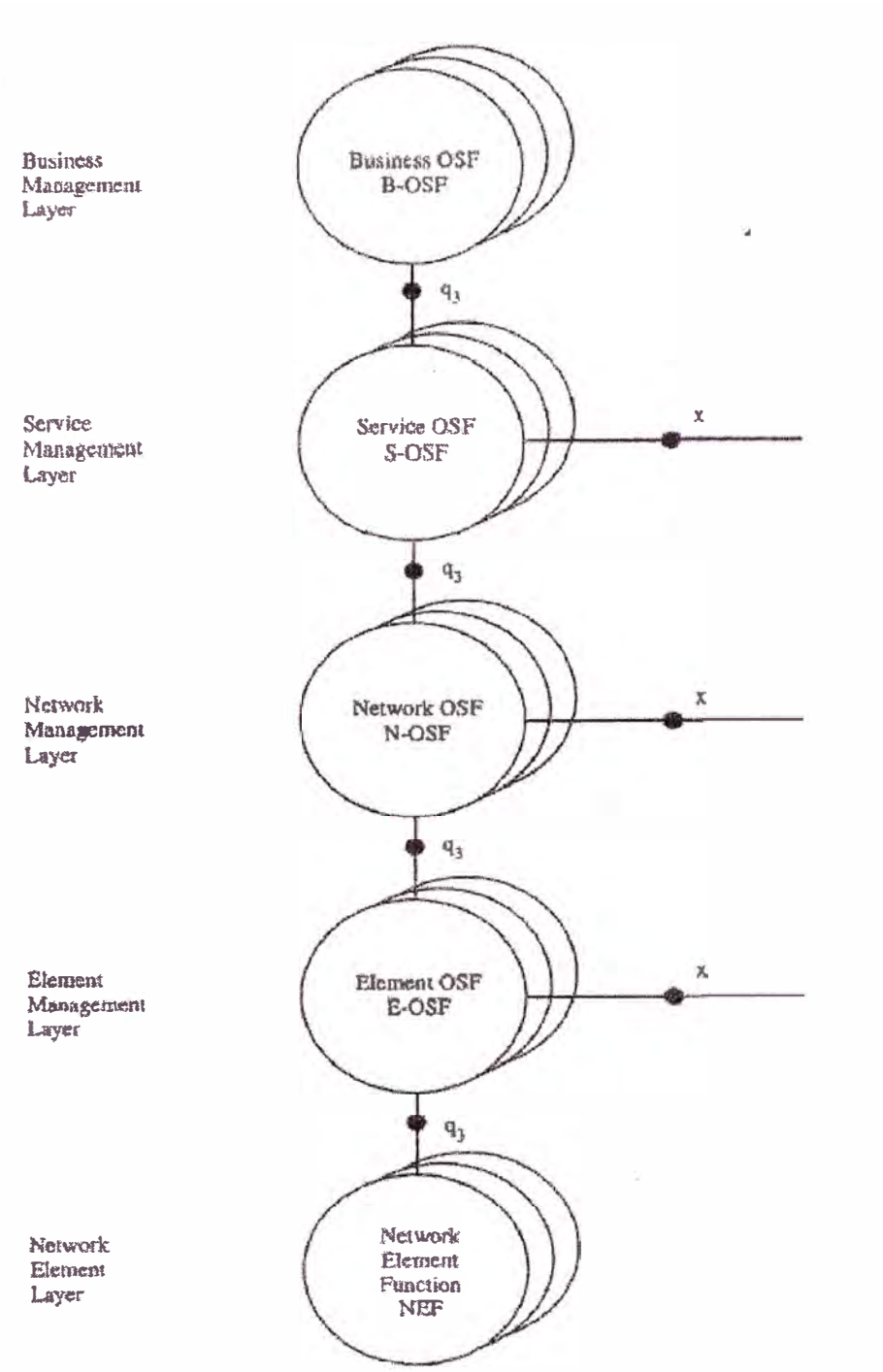

Figura 2.4 La arquitectura estratificada de las OSF

Como consecuencia, las herramientas existentes prometiendo resolver tareas de más alto nivel de la gestión de red pueden ser consideradas como productos de software propietario,

específico del fabricante. La arquitectura estratificada de las funciones del sistema de operaciones, tal como se define en la recomendación M.3010 se muestra en la Figura 2.4.

En referencias técnicas, las capas lógicas de las funciones de gestión son a menudo ilustradas por una pirámide (ver Figura 2.5), indicando que la mayor cantidad de datos elementales puede ser encontrada en la capa de base, pero el grado de su complejidad (en la medida en que los datos son procesados) se incrementa a través del ascenso en las capas.

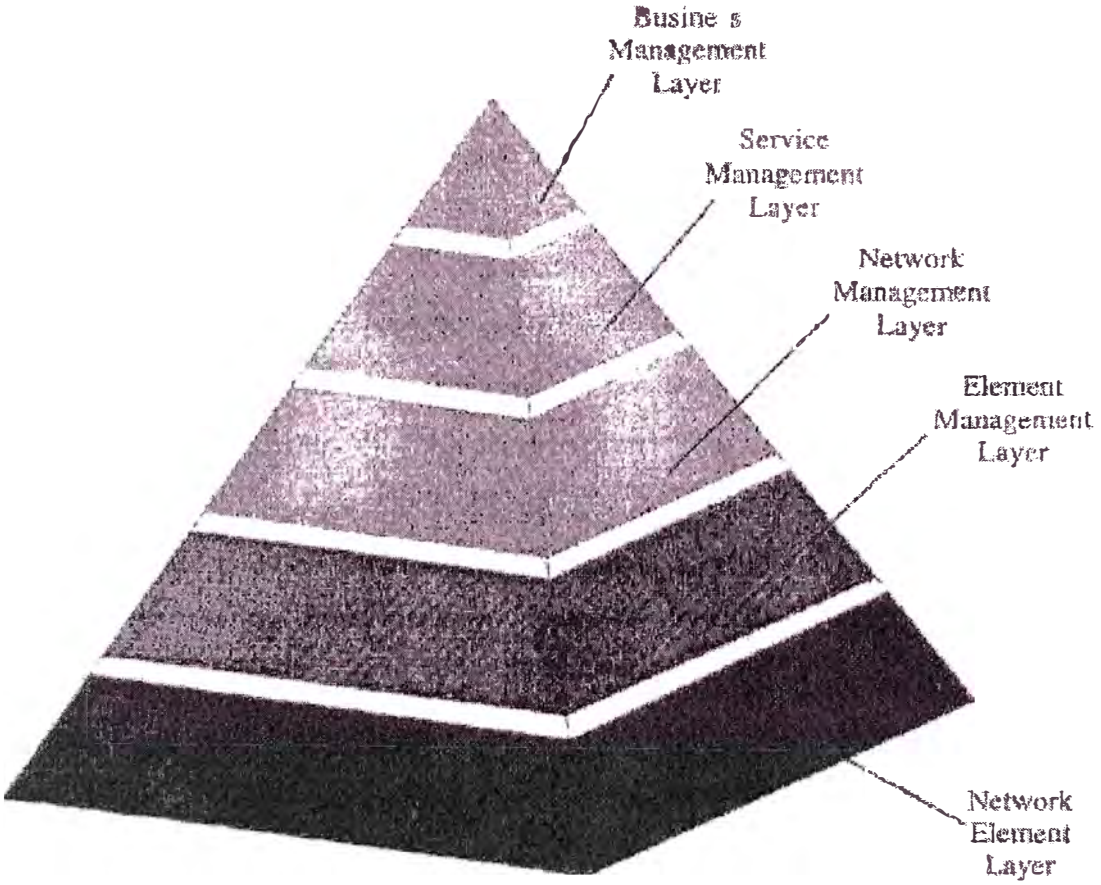

Figura 2.5 Ilustración Piramidal de la arquitectura lógica TMN

Una similitud puede ser establecida entre el modelo de gestión de red funcional con forma de pirámide y la estructura de una jerarquía de información de gestión de negocio típica. En general, esta puede también ser dividida en varias capas entre la capa operativa y la capa máxima de control de gestión. Es también obvio que puede requerirse una interrelación cercana entre la gestión de red a nivel de capa de negocio y la capa controlante superior del sistema de información relevante de gestión de negocio. (funciones interrelacionantes son: facturación, contabilidad (accounting), control de costo , y gestión de inventario, por ejemplo). El establecimiento de interconexión on-line entre los

Sistemas de Gestión de Red TMN y los sistemas de información de gestión de negocio puede representar uno de los más importantes esfuerzos de desarrollo futuros por el lado de los fabricantes de software de ambas familias de productos.

2.3.5 Normas TMN para Redes SDH

Los principios de TMN se especifican mediante ITU-T M.3010 con el propósito de normalizar su utilización para las redes SDH se tienen las siguientes recomendaciones:

- En M.3020 se disponen de las interfaces
- En M.3180 la información de gestión
- En M.3200 un resumen de los servicios
- En M.3300 las facilidades de la interfaz F

2.4 Modelo Internet

En 1988, el IAB (Internet Activities Board, Comité de Actividades Internet) determinó la estrategia de gestión para TCP/IP (Transfer Control Protocol/Internet Protocol, Protocolo de Control de Transmisión / protocolo de Internet). Esto significó el nacimiento de dos esfuerzos paralelos: la solución a corto plazo **[8]**, SNMP (Simple Network Management Protocol), y la solución eventual a largo plazo, CMOT (CMIP Over TCP/IP, CMIP sobre TCP/IP).

CMOT pretendía implantar los estándares del modelo de gestión OSI en el entorno Internet (TCP/IP). CMOT tuvo que afrontar los problemas derivados de la demora en la aparición de especificaciones y la ausencia de implementaciones prácticas. Como consecuencia de ello, la iniciativa CMOT fue paralizada en 1992.

2.4.1 Protocolo SNMP

SNMP es una extensión del protocolo de gestión de red para gateways SGMP (Simple Gateway Monitoring Protocol, Protocolo Simple de Supervisión de Pasarelas), que se convirtió en 1989 en el estándar recomendado por Internet. Está dirigido a proporcionar una gestión de red centralizada que permita la observación, el control y la gestión de las instalaciones. Utilizando SNMP, un administrador de red puede direccionar preguntas y comandos a los dispositivos de la red.

SNMP se ha convertido, debido al enorme éxito que ha tenido desde su publicación, en el estándar de facto de gestión de redes. Prácticamente todo el equipamiento de redes puede ser gestionado vía SNMP.

Algunas de las funciones que proporciona SNMP son:

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

El protocolo SNMP incorpora varios elementos presentes en otros estándares como el modelo gestor-agente, la existencia de una base de datos de información de gestión (MIB) o el uso de primitivas de tipo PUT y GET para manipular dicha información.

A continuación se describen dichos elementos:

- **Agente**: equipamiento lógico alojado en un dispositivo gestionable de la red. Almacena datos de gestión y responde a las peticiones sobre dichos datos.
- **Gestor**: equipamiento lógico alojado en la estación de gestión de red. Tiene la capacidad de preguntar a los agentes utilizando diferentes comandos SNMP.
- **MIB** (Management Information Base, Base de Información de Gestión): base de datos virtual de los objetos gestionables, accesible por un agente, que puede ser manipulada vía SNMP para realizar la gestión de red.

El protocolo SNMP es sólo un aspecto dentro de toda la estructura de gestión, la cual está compuesta de los siguientes elementos:

a. Estación de Gestión de Red (Network Management Station, NMS)

Es el elemento central que proporciona al administrador una visión del estado de la red y unas funciones de modificación de este estado (puede ser una estación de trabajo o un ordenador personal).

b. Estructura de la Información de Gestión (Structure of Management Information, SMI)

Es un conjunto de reglas que define las características de los objetos de la red y cómo obtienen los protocolos de gestión información de ellos. Aunque ha sido diseñado después del SMI de OSI, no es compatible con este.

c. Base de Información de Gestión (Management Information Base, MIB)

Es una colección de objetos, que representan de forma abstracta los dispositivos de la red y sus componentes internos. La MIB es conforme a la SMI para TCP/IP. Cada agente SNMP contiene instrumentación que, como mínimo, debe ser capaz de reunir objetos MIB estándar. Estos objetos incluyen direcciones de red, tipos de interfaz, contadores y datos similares. El estándar MIB de Internet define 126 objetos relacionados con los protocolos TCP/IP.

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

La carga de la gestión de todas las MIBs y de las extensiones privadas recae en el sistema de gestión. Las MIBs están escritas en una variante simple del lenguaje de definición OSI ASN.1.

En 1990 se introdujo una nueva versión de MIB, MIB II, donde la mayor aportación es la utilización de 185 nuevos objetos de extensiones privadas. Aparte de la MIB, existe la Base de Datos de Estadísticas de Red (Network Statistics Database, NSD) que está en la estación de trabajo de gestión. En esta base de datos se recoge información de los agentes para realizar funciones de correlación y planificación.

Las limitaciones de SNMP se deben a no haber sido diseñado para realizar funciones de gestión de alto nivel. Sus capacidades lo restringen a la supervisión de redes y a la detección de errores. Como todos los elementos TCP/IP, ha sido creado pensando más en su funcionalidad y dejando a un lado la seguridad.

2.4.2 Protocolo SNMPv2 y v3

En 1996 se publicó un nuevo estándar, el protocolo SNMPv2, resultado de una serie de propuestas para mejorar las características de SNMP. Los cambios se traducen fundamentalmente en una mejora de las prestaciones, un aumento de la seguridad y en la introducción de una jerarquía de gestión.

a. Prestaciones

SNMPv2 mejora el mecanismo de transferencia de información hacia los gestores, de forma que se necesitan realizar menos peticiones para obtener paquetes de información grandes.

b. Seguridad

A diferencia de SNMP, que no incorpora ningún mecanismo de seguridad, SNMPv2 define métodos para controlar las operaciones que están permitidas. Desafortunadamente surgieron dos planteamientos diferentes en cuanto al modelo de seguridad, que han dado lugar a dos especificaciones conocidas como SNMPv2* y SNMPv2u. Se están realizando esfuerzos para unificar ambos enfoques en un único estándar: SNMPv3.

c. Gestión jerárquica

Cuando el número de agentes a gestionar es elevado, la gestión mediante el protocolo SNMP se vuelve ineficaz debido a que el gestor debe sondear periódicamente todos los agentes que gestiona. SNMPv2 soluciona este inconveniente introduciendo los gestores de nivel intermedio. Son estos últimos los que se encargan de sondear a los agentes bajo su control. Los gestores intermedios son configurados desde un gestor principal de forma que solo se realiza un sondeo de aquellas variables demandadas por este último, y solo son notificados los eventos programados. SNMPv2 también introduce un vocabulario más extenso, permite comandos de agente a agente y técnicas de recuperación de mensajes.

2.4.3 Monitorización Remota (RMON)

La especificación RMON (Remote MONitor, monitorización remota) es una base de información de gestión (MIB) desarrollada por el organismo IETF (Internet Engineering Task Force) para proporcionar capacidades de monitorización y análisis de protocolos en redes de área local (segmentos de red). Esta información proporciona a los gestores una

mayor capacidad para poder planificar y ejecutar una política preventiva de mantenimiento de la red.

Las implementaciones de RMON **[9]** consisten en soluciones cliente / servidor. El cliente es la aplicación que se ejecuta en la estación de trabajo de gestión, presentando la información de gestión al usuario. El servidor es el agente que se encarga de analizar el tráfico de red y generar la información estadística. La comunicación entre aplicación y agente se realiza mediante el protocolo SNMP.

RMON es una herramienta muy útil para el gestor de red pues le permite conocer el estado de un segmento de red sin necesidad de desplazarse físicamente hasta el mismo y realizar medidas con analizadores de redes y protocolos.

Las iniciativas se dirigen en estos momentos hacia la obtención de una mayor y más precisa información. En concreto, se trabaja en la línea de analizar los protocolos de nivel superior, monitorizando aplicaciones concretas y comunicaciones extremo a extremo (niveles de red y superiores). Estas facilidades se incorporarán en versiones sucesivas de la especificación (RMON II).

2.4.4 Comparación entre SNMP y CMIP

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

- SNMP está basado en técnicas de sondeo, mientras que CMIP utiliza una técnica basada en eventos. Esto permite a CMIP ser más eficiente que SNMP en el control de grandes redes.
- CMIP es un protocolo orientado a conexión mientras que SNMP es un protocolo sin conexión. Esto significa que la carga de proceso de SNMP es reducida, pero cuando se envía un mensaje nunca se puede asegurar que el mensaje llega a su destino. La seguridad de los datos no es prioritaria para SNMP.
- CMIP permite la implementación de comandos condicionales sofisticados, mientras que SNMP necesita el nombre de cada objeto.
- CMIP permite, mediante una única petición, la recogida de gran cantidad de datos de los objetos gestionables, enviando información de retorno en múltiples respuestas. Esto no está permitido en SNMP.

- CMIP está especialmente preparado para gestionar grandes redes distribuidas, mientras que SNMP está recomendado para la gestión inter-red.
- CMIP realiza una distinción clara entre los objetos y sus atributos. SNMP no permite esto, lo cual hace imposible la reutilización de atributos y definiciones.

2.5 Gestión Integrada

Hasta hace poco, la gestión estaba orientada hacia soluciones en "islas". Los suministradores de sistemas (transmisión, conmutación, datos, etc.) ofrecían soluciones no estandarizadas; la arquitectura, interfase, protocolos y aplicaciones variaban según cada caso específico.

La gestión centralizada (integrada) de redes heterogéneas era impracticable por tener máquinas distintas, sistemas operativos distintos, aplicativos y protocolos distintos.
Hace unos años, la Telebrás (holding estatal dueña de las empresas regionales de telecomunicaciones de Brasil) definió las recomendaciones referentes a sistemas de gestión. Esas recomendaciones se basaron en los estándares ITU-T, todas las empresas regionales (28 en total) pasaron a exigir que los nuevos sistemas tengan una interfaz Q3. Si solo dispusieran de una interfaz propietaria, los suministradores debieron asumir el compromiso de desarrollar e implementar la nueva interfaz (sin costos adicionales).

Además de la interfaz Q3, los sistemas deberían implementar un modelo de información totalmente documentado. Ese modelo debería ser realizado en lenguaje ASN.1 (Abstract Syntax Notation One) preferiblemente, el formato debería ser GDMO (Guidelines Managed Object) Metalenguaje de plantillas simple (ISO 10165-4) basado en ASN.1.
Esa exigencia representa el primer paso hacia una futura integración de sistemas distintos en una plataforma de gestión de redes heterogéneas.

Dentro del ámbito de gestión de Redes se pueden dar tres escenarios posibles:

- El Modelo de información es suministrado por la contratante. Se debe verificar si las funcionalidades de gestión implementadas cumplen con el modelo de información suministrado.
- El Modelo es especificado por el suministrador, referenciado a estándares internacionales (ITU-T, ETSI, etc.) sin entrega del modelo. Se debe verificar si el

modelo de información cumple con los estándares especificados y si las funcionalidades de gestión implementadas cumplen con el modelo de información suministrado.

- El Modelo de información es suministrado por la contratada (modelo propietario). El contrato debe exigir el suministro del modelo en formato GDMO y lenguaje ASN.1 y se debe verificar si las funcionalidades de gestión, especificadas en el contrato, están de hecho implementadas.

2.5.1 Paradigma Gestor-Agente.

El ITU-T busca establecer un modelo universal de gestión, llamado Red de Gestión de Telecomunicaciones (TMN). Ese modelo describe una red con interfaces estandarizadas para comunicación entre los elementos de red y las plataformas de gestión. El modelo utiliza un paradigma gestor / agente, análogo al modelo cliente / servidor, en el que el sistema de gestión de red es un sistema de información concebido para el control y monitorización de la red; y cuyos componentes claves son: Gestores, Agentes, MIBs y Protocolos de Gestión.

Con los estándares OSI e ITU-T, se pasó a dar mayor atención al aspecto de integración de sistemas. El objetivo es garantizar la compatibilidad en un ambiente de múltiples suministradores (multi-vendor environment). Un sistema integrado de gestión tiene que atender a dos criterios fundamentales: interconectividad y interoperabilidad.

a. Interconectividad.

En una arquitectura de gestión centralizada (paradigma Gestor/ agente), debe haber estándares para garantizar la interconectividad entre distintos sistemas de soporte a la operación, entre esos sistemas y elementos de red, entre estaciones de trabajo y esos sistemas, entre dispositivos de mediación y los sistemas y los elementos de red.

b. Interoperabilidad.

No es suficiente que los sistemas posean la misma interfaz. Es necesario garantizar que cada modelo de información pueda ser comprendido por las aplicaciones conectadas a la red de gestión, todas las funciones de cada elemento de red son descritas en una base de datos (MIB, management information base) asociada a ese elemento. Esa base de datos

debe seguir criterios claros y universales en su estructuración (SMI, structure of management information).

2.5.2 Protocolos de gestión

Para cada interfaz, hay una familia de protocolos (Q3, Qx, X y F). La base para asegurar la interoperabilidad es la capa 7 (capa de aplicación), la cual es común a cada familia de protocolos ya que las capas inferiores soportan a las capas superiores. Los elementos de red que no poseen una interfaz interoperable requieren la conversión de los protocolos y mensajes, esta conversión es realizada por la función de comunicación de mensajes y por la función de adaptación Q.

Esas funciones pueden residir en el adaptador Q (QAs), en los propios elementos de re (NEs), en los dispositivos de mediación (MDs) o en los sistemas de soporte a la operación (OSs).

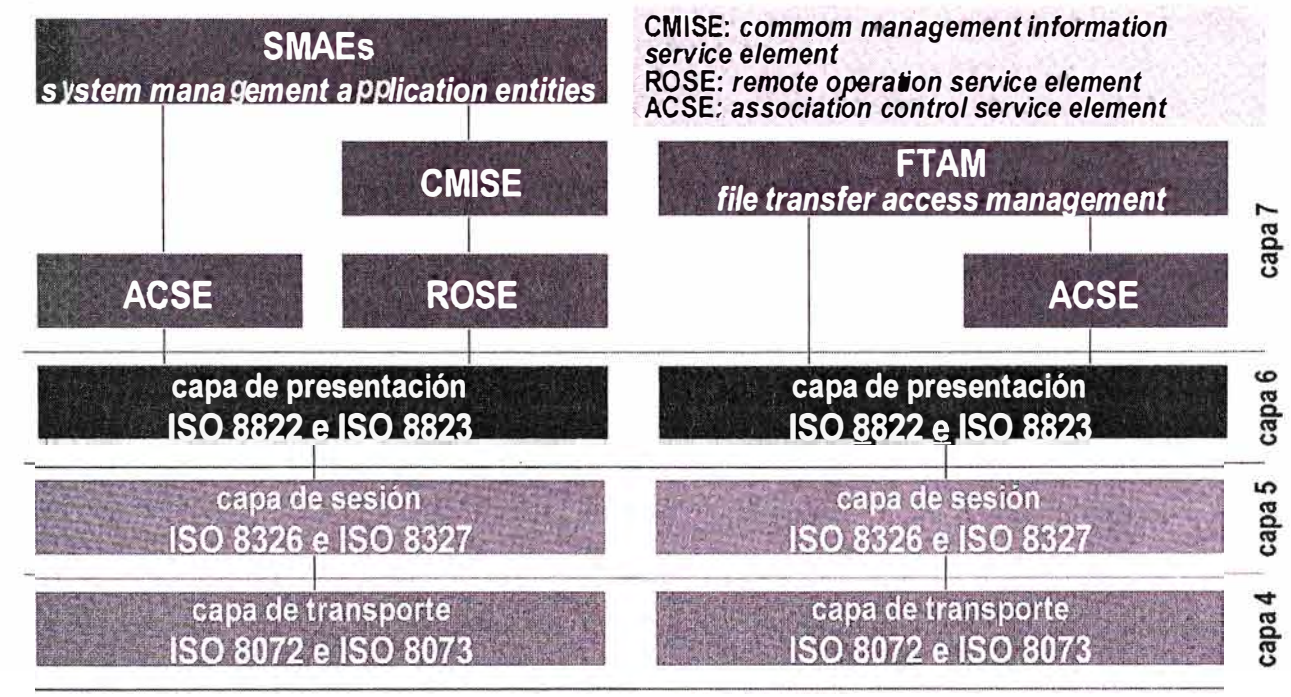

Figura 2.6 Interfaz Q3 – Capas superiores

a. Familia Q3

Se recomienda una única selección de protocolos para las capas 4 a 7 del modelo OSI como se ilustra en la Figura 2.6. Las capas 1 a 3 dependen de la disponibilidad de redes de

comunicación de datos, debiendo uno seleccionar el conjunto de protocolos más eficiente en cada caso y el que se muestra en la Figura 2.7.

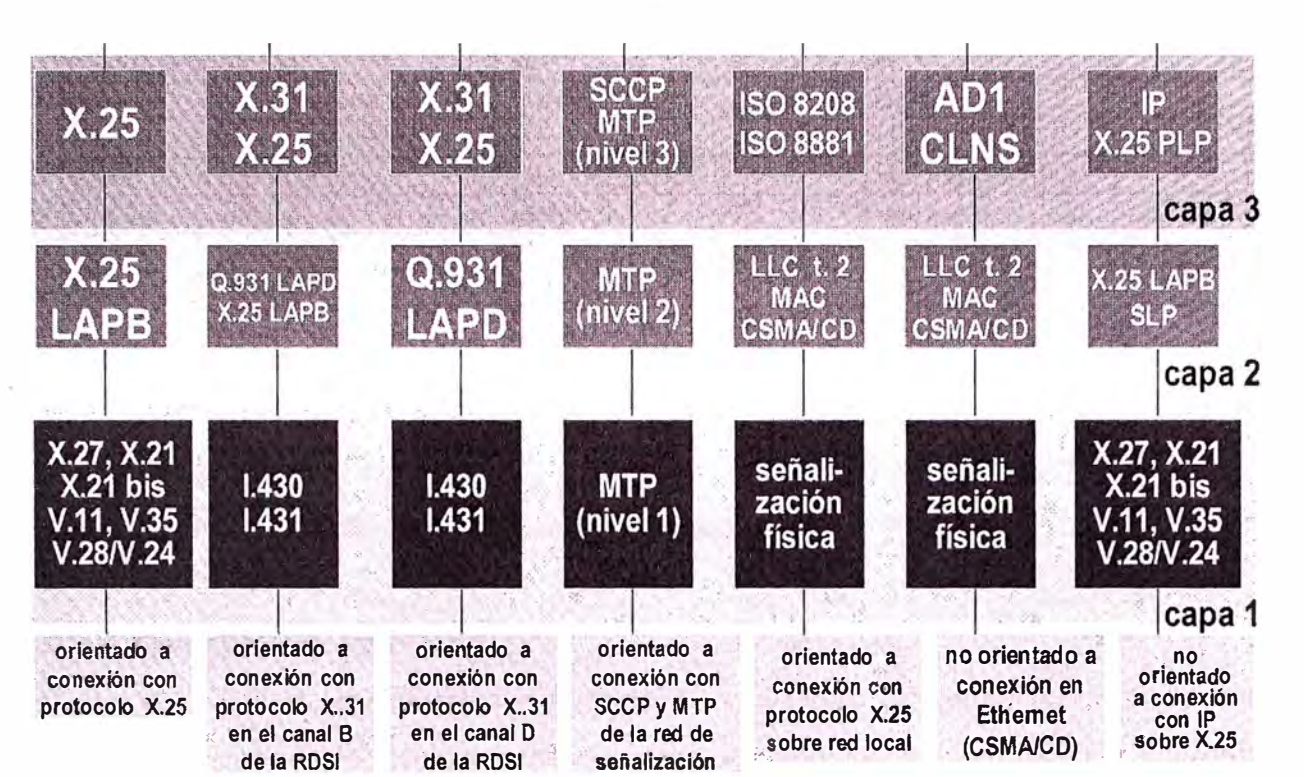

Figura 2.7 Interfaz Q3 – Capas inferiores

b. Familia Qx

La selección es hecha caso a caso, pues depende de las funciones de mediación requeridas. Las funciones de mediación, además, pueden estar repartidas entre varios dispositivos de mediación en cascada. La implementación exige la flexibilidad de adaptaciones a los casos necesarios en la red.

2.6 Comparación entre Sistemas de Gestión PDH y SDH

La tercera generación de sistemas de supervisión permite efectuar las operaciones de la segunda más otras adicionales (por ejemplo, reconfiguración dentro de una red en anillo).

Posee una velocidad de comunicación y una capacidad de memoria mayor. A continuación en la Tabla N° 2.1 se comparan ambos sistemas.

Tabla Nº 2.1 Comparación entre los sistemas de gestión PDH y SDH

Modelo del sistema de gestión	PDH	SDH
Funciones	Telesupervisión	Red TMN
Alarmas, Control, G.821	Si	Si
Configuración red	No	Si
Protocolo comunicación	Polling	HDLC
Velocidad comunicación	64 kb/s	192 y 576 kb/s
Canal de comunicación	Independiente	SOH en STM-1
Unidad de supervisión	Separada	Integrada
Periféricos previstos	RS-232 (VDU+Print+Host)	LAN-Ethernet (workstation)
Interfaz y software	Propietario	Normalizados

2.7 Arquitectura para Redes SDH

La arquitectura típica del sistema de gestión para las redes sincrónicas (su origen se remonta a 1988) contiene los siguientes componentes:

2.7.1 Elementos de Red (NE)

En una red SDH es el multiplexor terminal o Add-Drop, el equipo terminal de línea o repetidor, los circuitos Cross-Connect, el equipo de radió enlace y la fuente de sincronismo

Los elementos de red poseen hacia el exterior la interfaz F y Q que permiten la conexión con el sistema de operaciones. La interfaz F admite la conexión de una PC (Notebook o Laptop) como sistema de gestión local.

2.7.2 Adaptador de interfaz Q

Permite adaptar un elemento de la red NE ya existente a la TMN que se introduce. Los elementos de red SDH ya disponen de las interfaces Q y F. Téngase en cuenta que la interfaz Q3 es normalizada y la Qx es propietaria del fabricante.

2.7.3 Elemento de Mediación

Permite la conexión entre el elemento de red y el sistema de operaciones mediante un canal de comunicación de datos normalizado.

2.7.4 Sistema de operaciones

Se trata de componentes informáticos para el proceso y presentación de la información.

2.8 Modelo Funcional de Gestión en redes SDH

El ITU-T define las funciones de gestión de SDH en su recomendación G.784. La G.784 define el modelo funcional y de comunicaciones de la red y sub-redes de gestión de la SDH (SMN y SMS, respectivamente).

Una sub-red de gestión SDH (SMS) es un conjunto de NEs SDH en donde por lo menos un NE está conectado a un OS o MD. Una LCN es una red local para la comunicación entre los NEs (SDH o no) allí existentes:

2.8.1 Canal de comunicación de datos (DCC)

Los canales de comunicación son formados por los bytes D1 a D3 del encabezado de sección de regeneración (DCC_R). Los bytes D4 a D12 del encabezado de sección de multiplexación (DCC_M) pueden también ser utilizados.

2.8.2 Canal de control embebido (ECC)

Canal de comunicación con el modelo funcional asociado al mismo. Las funciones de gestión de ECC soportadas son:

- Recuperación de parámetros de la red (Ejemplo: tamaño de paquetes, timeout, calidad de servicio, tamaño de ventana).
- Enrutamiento de mensajes entre nodos de paso o junción de los CDS.
- Gestión de direcciones de red.
- Recuperación del estado de cada DCC en cada nodo.
- Capacidad de activar y desactivar un DCC.

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

- Gestión de sistema BML (Business Management Layer) para modelos de largo plazo, planes de servicios y tarifas.
- Gestión de servicio SML (Service ML) para la administración de órdenes de servicio.

- Gestión de red NML (Network ML) para gestión de alarmas, tráfico, performance y configuración de la red.
- Gestión de elemento de red EML (Element ML) gestión de alarmas, tráfico, performance y configuración del equipo.
- Gestión local del elemento de red NEL (Network Element Layer) para las funciones locales de gestión.

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

2.9 Componentes de la Gestión SDH

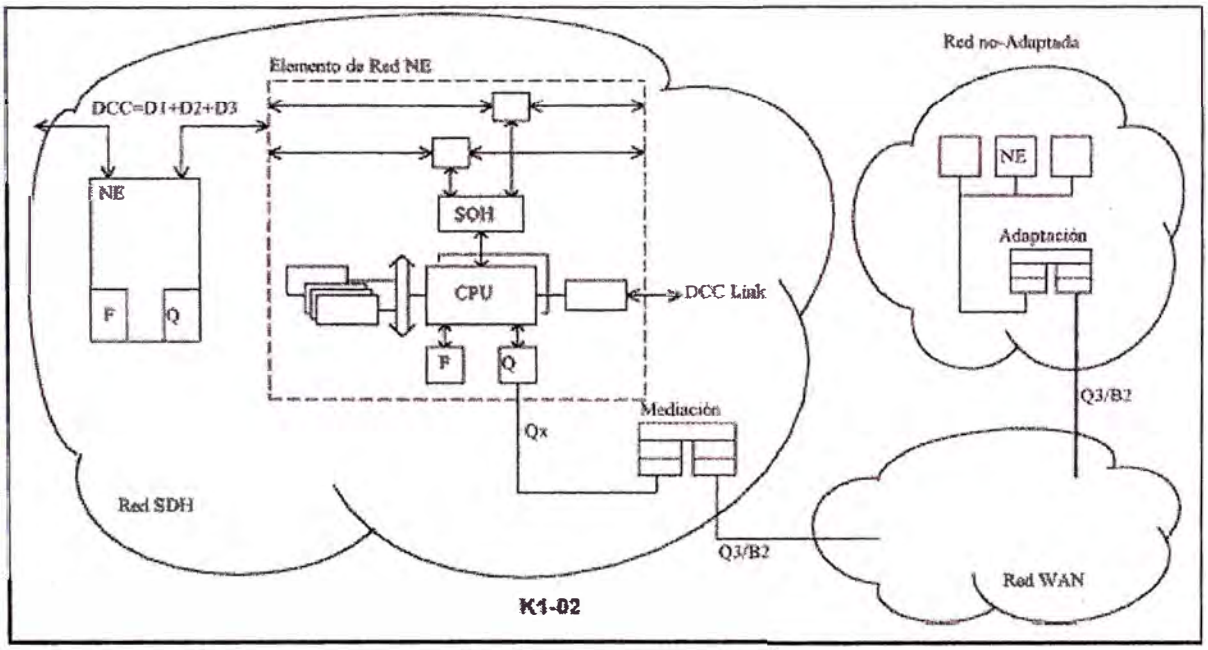

Figura 2.8 Estructura de enlace para gestión de equipos SDH

En el presente ítem se hace referencia al sistema de gestión EM-OS (Equipment Management Operation System) de Siemens, al 21SMX de Nec y al 1354RM / 1353SH de Alcatel; sin bien el tratamiento tiene un carácter general para otros diseños similares.
Siguiendo los lineamientos de la Figuras 2.8 y 2.9 los componentes que constituyen la red de gestión SDH son los siguientes:

- Unidad de Control y unidad de Gestión del equipo.
- Canal de comunicación hacia la PC que oficia de terminal local.
- Canal de comunicación entre equipos de la misma red.
- Red de comunicación entre distintos equipos en una misma estación.
- Red de comunicación en el Centro de Gestión Regional.
- Red de comunicación entre Centros Regionales con el Centro Nacional Unificado.

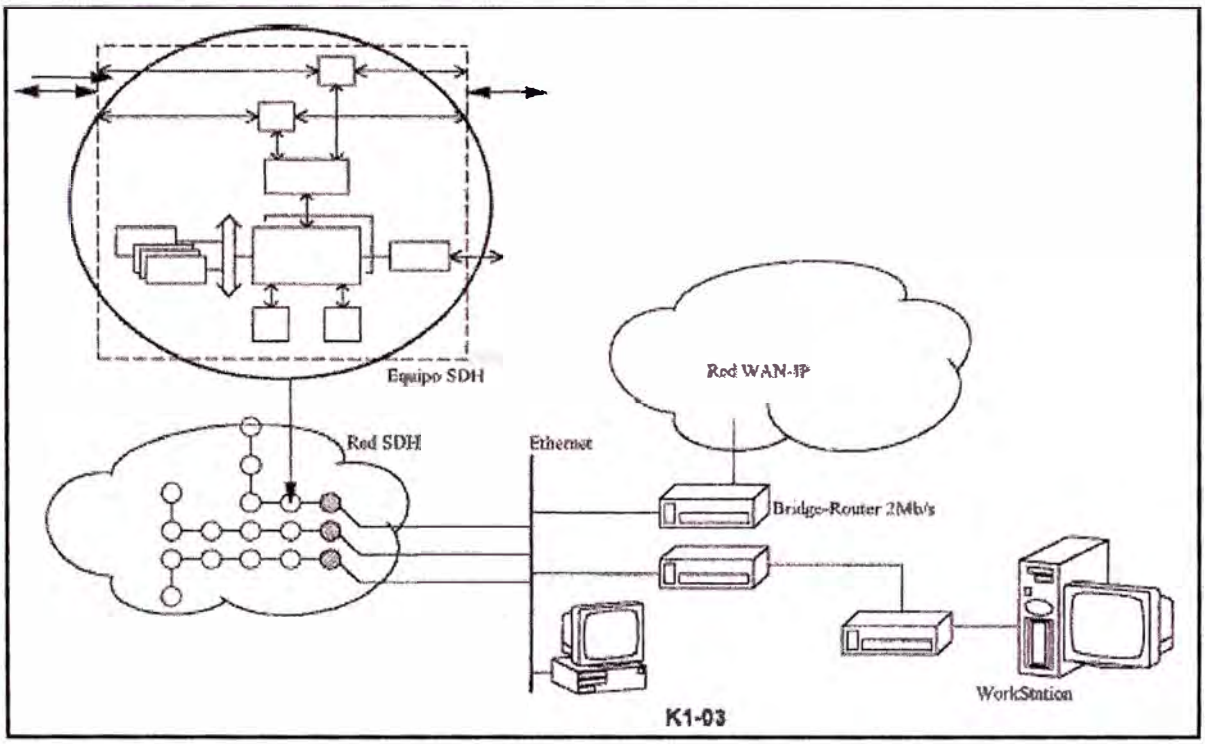

Figura 2.9 Componentes de una red de gestión SDH

2.9.1 Unidad de Control

Un equipo de la red SDH (multiplexor Add-Drop, terminal de línea óptica o radióenlace, Cross-connect, etc.) puede visualizarse como una serie de unidades con distintas misiones y funciones. La unidad de control mantiene actualizada la base de datos del equipo y permite la comunicación con el operador del Terminal Local.

Sus funciones en particular son:

- Comunicación con las distintas unidades del aparato. Se realiza mediante un canal de comunicaciones cuyo soporte físico (capa 1) es el backplane del bastidor. El protocolo de comunicación de capa 2 es el LAP-D (derivado de la red de acceso ISDN). Se trata de un proceso de comunicación del tipo Polling donde la unidad de

control interroga en forma periódica a las distintas unidades para actualizar la Base de Datos MIB.

- Actualización de la Base de Datos. En esta base de datos se sostiene la información de alarmas, configuración, reportes de performance, etc. El equipo dispone de una memoria EEPROM en cada unidad y otra en el backplane. En la EEPROM de cada unidad se mantiene el software de operación. En la EEPROM del backplane se mantiene la configuración del equipamiento. En caso de falla o corte de energía al reiniciarse el funcionamiento el equipo sé autoconfigura con los parámetros memorizados en esta memoria. No se requiere una intervención posterior al cambio de una unidad del equipo.
- Comunicación con el terminal local PC. Esto permite realizar las operaciones de gestión local desde una PC mediante la interfaz F.
- Comunicación con la Unidad de Gestión de red TMN. Entre ambas unidades (Control y Gestión) se puede enlazar al equipo con la TMN.

2.9.2 Terminal Local

La interfaz F permite comunicar al equipo con una PC (Notebook o Laptop) exterior de forma tal que pueden realizarse funciones de programación local. Esta función es necesaria en la configuración inicial del equipo cuando aún no se han ingresado los parámetros de comunicación de red (direcciones MAC, NSAP e IP) que permiten la conexión remota.

Las funciones son:

- Interfaz de conexión F que corresponde a una conexión hacia el terminal de operaciones (PC) mediante una salida ITU-T V.24 (similar a RS-232) a una velocidad de 9,6 ó 19,2 kb/s. Se trata de un conector tipo-D de 9 pines (DB-9). El diagrama de capas para una Interfaz F incluye el nivel de enlace de datos (capa 2 del tipo HDLC) y el protocolo de aplicación propietario del fabricante.
- Software de aplicación que permite realizar casi las mismas funciones que la gestión TMN. El terminal local permite leer y escribir en la base de datos del equipo, cuya memoria es reducida. Por ello, la capacidad de obtener estadísticas y resúmenes históricos es limitado. Sin embargo, permite las funciones básicas y es de utilidad en la puesta en marcha y reparación de emergencia.

- El software disponible mediante el terminal local es suficiente para operar una red de equipos pequeña. Cuando dicha red es más extensa se puede pensar en el sistema de gestión remoto TMN. Para ello se requiere la función de Unidad de Gestión.

2.9.3 Unidad de Gestión

Para efectuar las funciones de gestión remota TMN se requiere de una unidad de gestión que procesa los protocolos de comunicación apropiados (normas ISO para la TMN). Esta unidad puede ser la misma o distinta a la unidad de control.

Realiza las siguientes funciones:

- Proceso de comunicación entre estaciones mediante el canal DCC embebido en la trama STM-N.
- Interfaz Q de conexión al exterior. Normalmente se trata de una red Lan-Ethernet.
- Interfaz hacia otros equipos idénticos de la misma estación. Este último caso es disponible en algunos modelos de equipos para facilitar la extensión de la conexión de gestión a otros enlaces similares. Se trata de una extensión del canal DCC (DCC link) o una interfaz serie de interconexión.

2.9.4 Comunicación entre Estaciones

La comunicación entre los equipos que forman un enlace SDH ubicados en distintas estaciones se realiza mediante un canal de comunicaciones dedicado en la trama STM-N. Dicho canal se llama DCC (Data Communication Channel). Se disponen de dos canales de datos embebidos en el encabezamiento SOH de la trama STM-N. Las características de esta comunicación son las siguientes:

a. Canal de comunicación de datos de la sección de regeneración (DCC_R)

Que es accesible en los terminales y repetidores. La transmisión es serie del tipo full-duplex con protocolo HDLC a 192 kb/s (LAP-D). La interfaz al exterior para extensión es del tipo balanceada ITU-T V.11/RS-422 a 4-hilos, sobre línea de 150 ohmios.

b. Canal de comunicación de datos de la sección de multiplexación (DCC_M)

Que es accesible solo entre terminales multiplexores. La transmisión es contradireccional a 576 kb/s y la interfaz es ITU-T V.11. DCCR utiliza los Bytes D1-D3 de la RSOH y DCCM los Bytes D4-D12 de la MSOH (ver Figura 2.10).

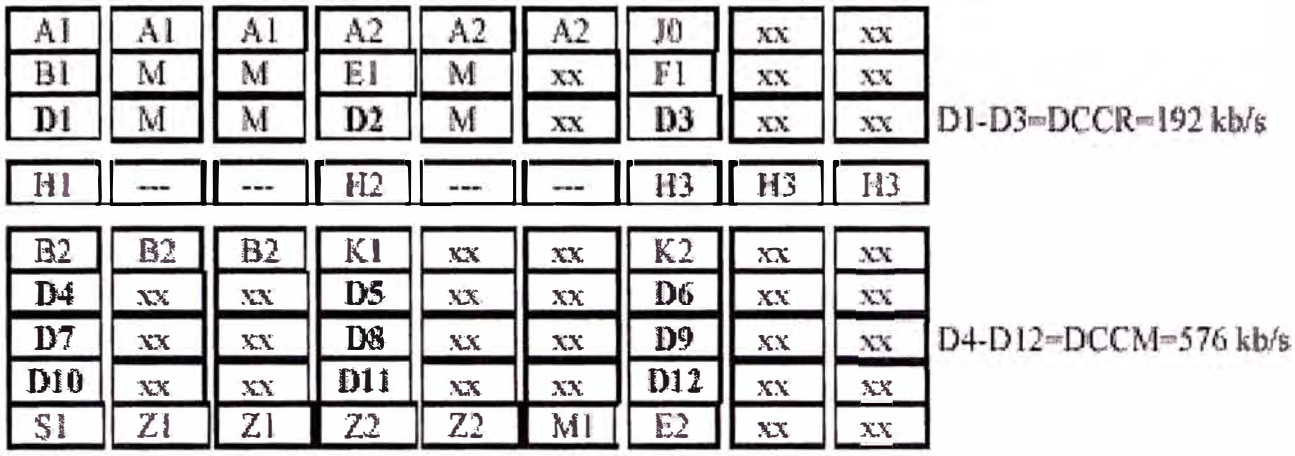

Figura 2.10 Canales DCC de la cabecera de un STM-1

El modelo de capas para el stack de protocolos (ver Figura 2.11) se encuentra determinado en ITU-T G.784 de la siguiente forma:

- En la Capa 2 se adopta la recomendación ITU-T Q.921. Se trata del protocolo HDLC LAP-D usado en el sistema de señalización DSS1 para usuarios de la ISDN. El mismo se utiliza también en la comunicación interna al aparato.
- En la Capa 3 se adopta el protocolo de la norma ISO 8473 (CLNP). Es un protocolo IP sin-conexión que permite el enrutamiento mediante la dirección NSAP. Este protocolo es equivalente al IP de UNIX-Internet.
- La capa 4 de Transporte es ISO 8073 (TP4) y realiza funciones de retransmisión de datos.
- La capa 5 de Sesión ITU-T X.215 (kernel dúplex) permite realizar las funciones de aceptación de conexión, rechazo y desconexión, aborto, transporte y segmentación.
- La capa 6 de Presentación ITU-T X.216/226 (kernel ASN.1) entrega las reglas de codificación para sintaxis de transferencia.
- La capa 7 de Aplicación utiliza las normas ITU-T X.217 (ACSE), X.219 (ROSE) y ISO 9595 (CMIS). Permite la acción del software de aplicación de cada elemento de red. Una misma plataforma permite visualizar diferentes equipos. El protocolo de comunicación entre CMIS es el CMIP.

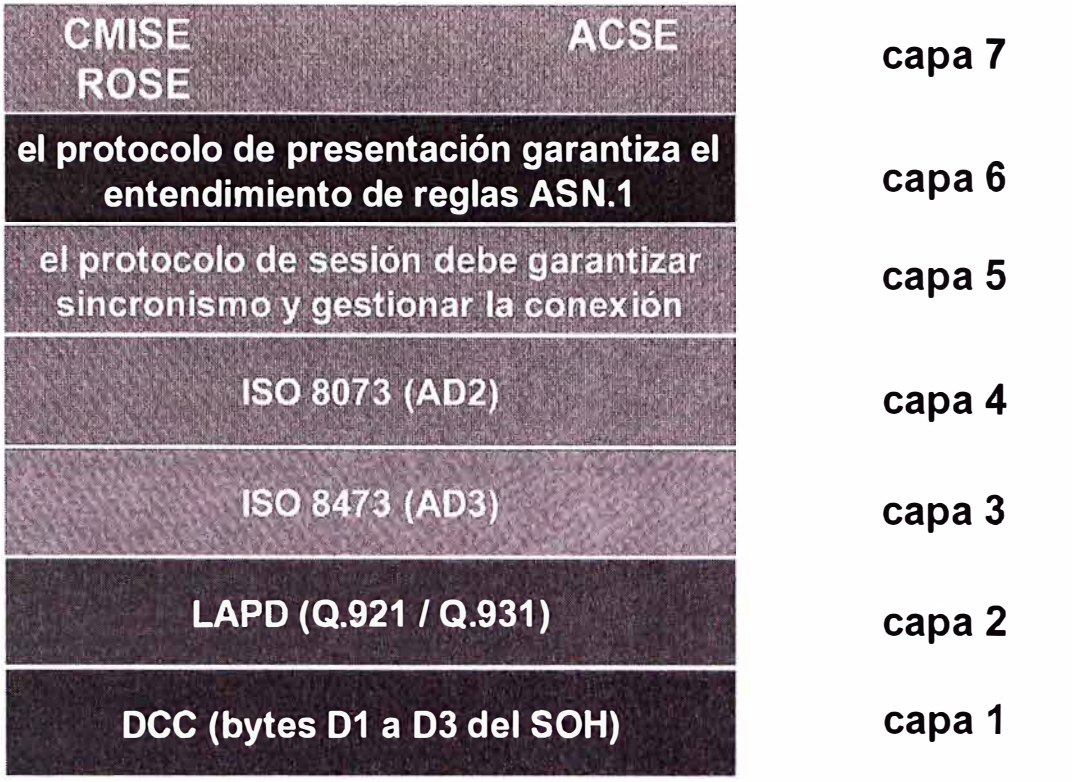

Figura 2.11 Stack de Protocolos de una SMS

2.9.5 Comunicación entre distintos Equipos

En una estación pueden coexistir distintos tipos de equipos SDH (multiplexores, terminales de Fibra Óptica, radió enlaces, etc.) y distintos enlaces que conforman la red. Para efectuar la interconexión de los mismos se requiere de la interfaz Q desde la Unidad de Gestión.

a. Interfaz Q1/Q2/Q3

Q1/Q2 se indican en la norma ITU-T G.771 y Q3 en Q.513. Q3 se encuentra en la norma ITU-T G.773 que identifica las capas del modelo ISO. Existen 5 variantes para Q3 propuestas y denominadas A1/A2/B1/B2/B3. La variante Q3/B2 se usa para comunicación con protocolo X.25 mientras que la variante Q3/B3 se usa para una salida LAN Ethernet (la LAN pertenece al sistema de operación).

La Interfaz Física es del tipo semidúplex con 2 pares balanceados uno en cada sentido de transmisión. La velocidad será de 19,2 o 64 kb/s con código NRZ Invertido. La capa 2 se determina en base a ITU-T X.25 (LAP-B) para la transferencia de datos por paquetes (interfaz y conector V.11/X.21) en Q3/B2. En el caso de Q3/B3 se trata de la IEEE 802.2

para la red de área local LAN tipo CSMA/CD (Ethernet). La capa 3 se encuentran conforme a X.25 en Q3/B2 y a ISO-8473 en el segundo. Se adopta, para X.25, el funcionamiento en módulo 8 y módulo 128 como opcional. La longitud máxima por trama es de 131 y 256 Byte.

b. LAN Ethernet

Normalmente los equipos SDH disponen de una interfaz física de conexión AUI que permite acceder al equipo mediante una LAN (10BaseT o 10Base2). En esta interfaz se conecta un transreceptor Ethernet con conexión coaxial BNC (10Base2) o RJ45 (10BaseT).

Todos los equipos a ser gestionados por la TMN deben ser interconectados mediante esta LAN. El protocolo de capa 2 es el definido en IEEE 802.3 (MAC y LLC). Para configurar correctamente la LAN se debe programar a cada equipo con una dirección MAC distinta.

2.9.6 Elemento de Adaptación

Permite la conexión entre un equipo no adaptado a la red TMN y que desea ser gestionado por el mismo sistema de operaciones mediante un canal de comunicación de datos normalizado. El proceso de adaptación involucra las siguientes funciones de comunicación entre el elemento de red y el sistema de operaciones:

a. Control de la comunicación

- Interrogación secuencial para recopilación de datos, direccionamiento y encaminamiento de mensajes, control de errores.
- Conversión de protocolos y tratamiento de datos: concentración de usuarios, compresión y recopilación de datos, formateo y traducción de información.
- Transferencia de funciones: secuenciación y eventual envío de alarmas, reporte de los resultados de las pruebas, carga de informes de estado.
- Proceso para toma de decisiones: fijación de umbrales de alarma, encaminamiento de datos, funciones de seguridad, y selección de circuitos.
- Almacenamiento de datos: configuración de redes, copia de memorias, identificación de equipos, etc.

b. Interfaz Q2

Conecta al elemento de red con el elemento de adaptación. La Capa 1 se trata de un bus o anillo, dúplex o semidúplex, mediante pares apantallados balanceados de 120 ohmios (interfaz V.11). La velocidad es de 19,2 a 64 kb/s en código NRZ Invertido. La Capa 2 determina el protocolo LAP-B de X.25 con un 1 byte de direcciones. El campo de información tiene una longitud máxima de 128 o 256 Byte.

2.9.7 Centro de Gestión Regional

En el Centro de Gestión Regional se concentra la gestión remota de los equipos en un sector de la red. Se trata de una red LAN del tipo Ethernet (10Base2 o 10BaseT) que interconecta los siguientes elementos:

- Equipos de red SDH. Se trata de los extremos de enlaces que confluyen en la estación central regional. Conexión mediante la interfaz AUI.
- Sistema de Operaciones. Está constituido por una o más (por razones de seguridad) estaciones de usuario WS (WorkStation). Esta WS puede funcionar con varios terminales X-Terminal para abastecer a diversos operadores simultáneamente.
- Bridge. Permiten interconectar distintas LAN del mismo tipo o generar varias desde una misma. Permite una mayor disponibilidad al generar LAN autosuficientes. Reduce el tráfico entre secciones de red LAN. Permiten solucionar problemas de congestión de paquetes mediante aislamiento de tráfico. Introduce retardo para medios de acceso de menor velocidad. Con dos bridge es posible abrir la red LAN del centro de gestión regional para disponer de acceso por ejemplo en el edificio de equipos de comunicaciones y el administrativo simultáneamente.
- Switch. Funciona en el ámbito de capa 2 (MAC), procesan direcciones y no modifican el contenido. Inspecciona la dirección de fuente y destino del paquete para determinar la ruta. La tabla de rutas es dinámica. Contiene suficiente memoria buffer para los momentos de demanda máxima (cola de espera). El overflow del buffer produce descarte de paquetes.
- Router. Funciona en el ámbito de capa 3 y por ello requiere un análisis del protocolo correspondiente IP (ISO o UNIX). Debe soportar distintos tipos de protocolos; por ejemplo ISO para la comunicación entre equipos SDH y TCP/IP de UNIX para la comunicación entre elementos informáticos. Interconectan LAN entre sí o una LAN con WAN (mediante protocolos punto-a-punto, X.25, Frame Relay o ATM). En una red de gestión el router dispone de salidas de 2 Mb/s hacia

la red de transmisión. Permiten mejorar la eficiencia de la red ya que tolera distintos caminos dentro de la red WAN (protección mediante múltiples posibles trayectos). El Router puede segmentar datagramas muy largos en caso de congestión.

2.9.8 Centro de Gestión Nacional

Este centro de gestión se comunica con todos los otros centros de gestión regionales mediante una red extensa WAN generada con routers. El protocolo de comunicación es el TCP/IP de UNIX. El canal de comunicación es una señal tributaria de 2 Mb/s (no estructurada) que se envía dentro de la misma red SDH.

La protección del tráfico se logra mediante una malla entre routers por distintas vías.

- Gateway. Se denomina así a la WorkStation que funciona en el ámbito de todo el modelo de capas para convertir los protocolos de ISO a UNIX. Interconectan redes de características diferentes con simulación de protocolos.
- Routing. Se entiende por routing el proceso que permite la interconexión de redes. Se efectúa mediante los Router por lo que se requiere la configuración para interpretar la dirección IP de capa 3. Bridge y Router son elementos que "aprenden de la red". Como analizan la dirección de cada paquete pueden formar una tabla de direcciones (MAC para el bridge e IP o NSAP para el router). Cuando se conecta un nuevo terminal a la red este envía un paquete indicando la activación con lo que puede integrarse a la tabla de direcciones. El Router debe poseer un set de direcciones IP. Tiene la capacidad de enrutamiento para optimizar el camino del paquete de datos (analiza el costo; retardo de tránsito; congestión de red y distancia en número de Router en el trayecto). La tabla de ruta (Routing Table) contiene solo el "próximo paso" en la red. Se han definido 2 tipos de protocolos para Router: en interior y exterior. Se denomina sistema autónomo (sistema interior o dominio) a un conjunto de sub-redes y Router que utilizan el mismo protocolo y el mismo control administrativo.
- Sistema Informático. Posee características similares a la del Centro Regional. Mediante sucesivos Password es factible administrar las funciones que pueden ser desarrollados por ambos tipos de Centros.

2.9.9 Direccionamiento

La configuración inicial de la red de Gestión involucra la programación de los parámetros de comunicación. Se trata de las capas 2,3 y 4. Se disponen de tres estructuras de suite de protocolos: LAN, ISO y UNIX. Las direcciones disponibles en UNIX (IP) e ISO (NSAP) son distintas:

a. Dirección IP

Disponible para direccionamiento entre componentes informáticos (Wokstation, X-Terminal, Routers, Impresoras, etc.). La dirección IP ocupa 32 bits (4 Bytes). Permite identificar la red y el host individual. Normalmente las direcciones IP de una red de gestión no están normalizadas. El formato de las direcciones puede ser de 5 tipos: Clase A, B, C, D y E.

b. Dirección NSAP (Netwotk Service Access Point)

Esta dirección está normalizada por ISO y permite el direccionamiento entre equipos de la red SDH. Trabaja sobre el protocolo de capa 3 de ISO/ITU-T CLNS (ConnectionLess Network Service, Servicio de Red no orientado a la conexión). Las funciones de router en este caso son desarrolladas por la Unidad de Gestión. La tabla de ruta (Routing Table) se actualizan en forma automática. El protocolo que permite actualizar esta Tabla es TCP/IP se denomina RIP y para el modelo ISO se denomina IS-IS.

La dirección NSAP (Netwotk Service Access Point, Punto de acceso de servicio de red) consiste en una secuencia jerárquica de bytes (generalmente entre 14 a 17 bytes, máximo 20 bytes).

El significado es el siguiente:

- Identificador de formato de dirección AFI: norma ISO 6523 (hexadecimal 47), ISO 3166 (39), X.121 (37 o 53).
- Identificador de dominio inicial IDI.
- Parte específica de dominio: Identificador de dominio DID y de sistema SID. Incluye la dirección MAC.
- Selector de NSAP (valor hexadecimal fijo 01).

c. Dirección MAC

El enrutamiento dentro de una LAN contiene 2 direcciones: una LLC y otra MAC. La dirección MAC identifica la estación sobre la red LAN (punto físico de la red, número de hardware que identifica al fabricante y serie del aparato) y la dirección LLC identifica al usuario. En LLC pueden estar conectados varios usuarios sobre la misma dirección MAC (MAC es una dirección en firmware mediante una memoria EPROM). La dirección puede ser individual, a un grupo multicast o broadcast. El formato de dirección MAC de 2 Bytes ocupa 1 bit para indicar una dirección individual o un grupo. La codificación FFFF (hexadecimal) señala la operación en broadcast para todas las estaciones activas en la LAN.

En el formato de 6 Bytes contiene: Un bit que indica una dirección individual o grupo. Un bit indica si se trata de direcciones administradas localmente o el formato universal (asignado por IEEE e ISO). El universal consiste en 22 bits asignados por IEEE al organismo que lo solicita (ejemplo: hexadecimal 08.00.20 para computadores Sun). Los 24 bits restantes son administrados localmente por el operador de la red LAN.

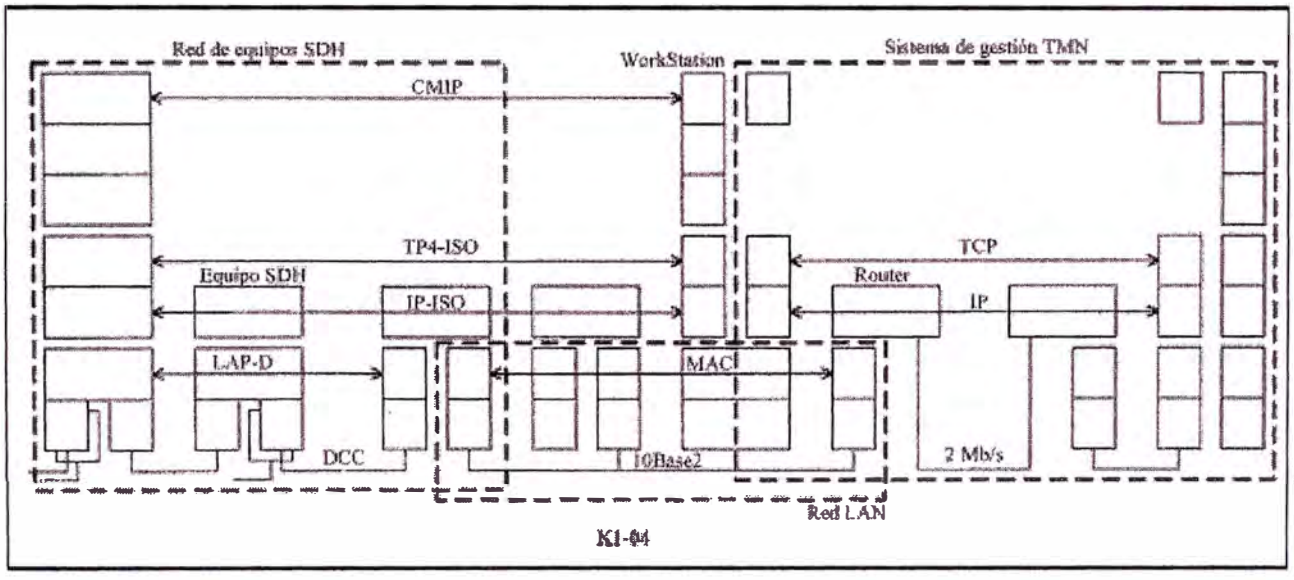

Figura 2.12 Diagrama de capas para la red de gestión SDH

Siguiendo a la Figura 2.12 se pueden observar las siguientes redes y protocolos de comunicación:

- Red entre equipos SDH. Consiste en la capa física DCC dentro de la trama STM-1. El protocolo de enlace de datos es el LAP-D. Los protocolos de capa superior son

los ISO (TP4/IP). Comunica a los distintos equipos NE con la estación WorkStation. El direccionamiento se efectúa mediante direcciones NSAP; la función de routing la realiza la Unidad de Gestión del equipo SDH.

- Red LAN. Consiste en la capa física 10Base2 o 10BaseT. El protocolo de enlace de datos es el MAC-LLC. En las capas superiores trabaja con los protocolos ISO o UNIX. Permite interconectar distintos equipos en una estación. En el Centro de Gestión interconecta los equipos SDH con los componentes del Sistema de Gestión (WorkStation, Printer, etc.). El direccionamiento se realiza mediante direcciones MAC.
- Sistema de Gestión. La capa física y de enlace de datos es la red LAN y WAN mediante routers. Utiliza los protocolos UNIX (TCP/IP) para las capas superiores. Permite la interconexión de varios Centros Regionales con el Centro Nacional. La interconexión se realiza mediante una red extensa conmutada por routers. El direccionamiento se efectúa mediante direcciones IP.

2.9.10 Software de Aplicación

El diseño e implementación del sistema de operaciones (OS) se basa en un software diseñado con la técnica orientada-al objeto. Consiste en definir Objetos abstractos cuyas características dinámicas se modelan y definen mediante el Comportamiento (behavior).

En una red real la función completa envuelve la interacción de todos los objetos asociados. La totalidad de los objetos se la conoce como base o modelo de datos-información de gestión.

CAPÍTULO III
FUNCIONES REQUERIDAS PARA UN SISTEMA DE GESTIÓN SDH

3.1 Gestión del Elemento de Red

Se describe a continuación la funcionalidad del gestor del elemento de red que debe trabajar como sistema gestor / agente (G/A) con el Elemento de Red. Nivel de Elemento de Red (EML) de acuerdo con Rec. M.3010.

3.1.1 Configuración

Se deben poder configurar desde el Gestor de Subred SDH, las siguientes características del Elemento de Red: Alta o baja de Elemento de Red.

Alta, baja y modificación de las características configurables desde el Control local, en las diferentes unidades u objetos lógicos que integran el Elemento de Red tales como:

- Modalidad de configuración, sencilla o duplicada de equipos.
- Tarjetas de tributario.
- Habilitación de canales.
- Velocidad de tributario que hay en cada puerto.
- Extracción e Inserción (ADM).
- Potencia óptica del agregado.

a. Presentación de la configuración

Se podrá pedir que el GSR presente la configuración actual del ER. Habrá mecanismos para comprobar coherencia entre las MIB de ambos.

b. Realización

Se podrá realizar la configuración de cada una de las partes del ER, sin que afecte al servicio de partes que no están implicadas directamente en dicha configuración.

Se podrán realizar los cambios en la configuración del ER, sin que afecte al servicio de partes que no están implicadas directamente en dicha configuración.

c. Notificación

El ER notificará al Gestor de Subred GSR, cualquier cambio que afecte a su configuración.

3.1.2 Gestión de Alarmas

En este apartado se describen las alarmas que deben presentarse, así como las funciones de gestión que podrán realizarse sobre dichas alarmas.

a. Presentación de alarmas

Las alarmas en los distintos elementos de red se presentarán de forma gráfica y con distintos colores dependiendo de su categoría. La actualización de las alarmas será espontánea, de manera inmediata, sin necesidad de refrescos.

Se deben presentar en la interfaz hombre / máquina del gestor del ER las siguientes alarmas:

- Nivel de potencia óptica recibida en cada tributario procedente del terminal remoto que provoca alarma de perdida de señal.
- Temperatura de láser que provoca alarma por temperatura excesiva.
- Pérdida de señal en cualquiera de los canales transportados, (detectados en los terminales), individualmente para cada canal.
- Pérdida de señal en cada una de las interfaces de tributarios y de agregado.
- Fallo de cada una de las tarjetas.
- Fallo de cada transpondedor.
- Fallo de cada láser, incluyendo el láser de bombeo de los amplificadores ópticos.
- Indicación de equipo o sección de fibra donde se ha producido el fallo o alarma.
- Fallo del canal de supervisión.
- Fallo de alimentación.
- Pérdida de conexión con el GSR.

b. Atención de Alarmas

Para cada alarma que se presente según el apartado anterior el operador del sistema podrá opcionalmente una vez que la visualice ponerla en la situación de atendida.

c. Inhibición de alarmas

Las alarmas descritas se podrán inhibir a voluntad del operador y cuando se ceda el control del ER desde el Centro de Gestión Centralizado al Control Local, pasando a tener la alarma el calificador, de "alarma inhibida".

d. Almacenamiento de alarmas

Cada una de las alarmas presentadas en la interfaz Hombre / Maquina se archivará en el correspondiente archivo histórico de alarmas que podrá ser consultado por el operador o bien secuencialmente, o bien por medio de una interrogación selectiva (empleo de filtros) según los campos que componen los registros de las alarmas.

Este archivo histórico podría ser vaciado o transferido a cinta luego que se supere un umbral o fecha, pudiendo ser estos modificables por el operador, a fin de no llenar espacio en disco.

e. Categoría de las alarmas

La categoría de las alarmas podrá ser configurable según quede afectado o no el servicio, a voluntad del operador. Las alarmas podrán tener dos categorías:

- Urgente
- No urgente

f. Envío de alarmas

El envío de alarmas se realizara con la fecha y hora en que se han producido. El envío de alarmas desde el ER al GSR se realizará de forma espontánea por parte del ER para las alarmas urgentes que puedan afectar al servicio. En caso de perdida de la conexión del GSR con el ER se realizará un nuevo envío de alarmas al GSR.

Se deberá garantizar en todo momento la coherencia entre las alarmas existentes en los elementos de red y las que aparecen en el Sistema de Explotación. Para ello, el Sistema de

Explotación dispondrá de la facilidad de solicitar al elemento de red el envío completo de la lista de alarmas activas.

El tiempo de presentación de alarmas deberá estar dentro de límites razonables. Con respecto a una indicación del tiempo de presentación de alarmas se considera que no sobrepasará los 30 segundos de retardo entre la ocurrencia de una alarma urgente y su presentación para el caso supuesto de estar procesando 1000 alarmas o mensajes por minuto.

3.1.3 Medidas de Calidad de Prestaciones

En este apartado se describen las medidas de calidad de prestaciones que se podrán realizar en el ER controladas y gestionadas desde el GSR.

a. Parámetros a medir

Se valorarán positivamente las medidas de Monitorización del byte B1 y J0 en tributarios SDH, así como la medida de relación Señal Ruido.

En las mediciones de calidad anteriores se podrán fijar umbrales de alarma. Se deberán realizar las siguientes medidas en el ER:

1. Potencia total recibida en el Agregado Óptico.
2. Potencia recibida en cada uno de los tributarios ópticos.
3. Corriente de polarización del láser.
4. Temperatura del láser.

b. Almacenamiento

Cada uno de los parámetros anteriores, se deberán almacenar en registros en el elemento de red. En todos los registros se efectuará una consignación de hora y día.

Por evento de funcionamiento y por sentido de la transmisión se proporcionarán los siguientes registros:

- Registros de medidas de 15 minutos que acumulen eventos de funcionamiento durante periodos fijos de 15 minutos.

- Registros de 24 horas que acumulen eventos de funcionamiento durante un periodo fijo de 24 horas.

En el ER se almacenarán al menos 16 registros de 15 minutos y un registro de 24 horas. Los registros de 15 minutos constituyen una pila de 16 registros recientes por lo menos. Cuando todos los registros de 15 minutos están llenos, se utiliza un mecanismo de "eliminación parcial" para descartar la información más antigua.

Se deberán enviar periódicamente al GSR de forma automática y sin intervención del operador las medidas almacenadas en el ER. En el GSR se almacenarán registros de 15 minutos durante 8 horas, y registros de 24 horas, durante 30 días.

Adicionalmente, el Sistema de Gestión deberá almacenar los datos recibidos durante un período mínimo de 3 meses debiendo además disponer de unidades de almacenamiento masivo para periodos superiores con objeto de poder analizar la evolución del tráfico, posibles degradaciones, etc.

c. Inhibición

Cualquiera de las medidas se podrá inhibir en un momento dado a voluntad del operador del GSR.

d. Visualización

El operador tendrá acceso para visualizar las medidas almacenadas en el GSR, o bien pedir un envío de las medidas que están almacenadas en el ER para su visualización.

e. Programación

Será posible realizar medidas de calidad programadas en fecha, hora y duración determinadas por el operador.

3.2 Gestión de Subred

En este apartado se definen las funciones de gestión relativas al TRAYECTO SDH extremo a extremo dentro de un sistema o dominio de un único suministrador.

3.2.1 General

El sistema de Gestión SDH permitirá supervisar y/o limitar el ancho de banda que se le ofrece a un cliente quien contrata como servicio un trayecto SDH.

3.2.2 Configuración

Se podrán constituir los trayectos SDH extremo a extremo:

- Alta / baja de Trayecto SDH.
- Modificación de las característica configurables en los objetos lógicos que integran el Trayecto SDH.
- Protección del Trayecto SDH.

a. Presentación de la configuración

Se podrá pedir que el GSR presente la configuración actual del Trayecto SDH.

b. Realización

Se podrán realizar los cambios en la configuración del Trayecto SDH, sin que afecte al servicio de partes que no están implicadas directamente en dicha configuración.

3.2.3 Gestión de Alarmas

En este apartado se describen las alarmas que deben presentarse, así como las funciones de gestión que podrán realizarse sobre dichas alarmas.

a. Presentación de alarmas de Trayecto SDH

Se deben presentar en la interfaz hombre / máquina del gestor del sistema las siguientes alarmas de Trayecto SDH:

- Corte de Trayecto SDH.
- Falta de nivel de potencia en el Trayecto SDH.
- Tasa de error excesiva en el Trayecto SDH.

b. Atención de Alarmas

Para cada alarma que se presente según el apartado anterior el operador del sistema podrá opcionalmente una vez que la visualice ponerla en la situación de atendida.

c. Almacenamiento de alarmas

Cada una de las alarmas presentadas en la interfaz Hombre / Maquina se archivará en el correspondiente archivo histórico de alarmas que podrá ser consultado por el operador, por medio de una interrogación selectiva según los campos que componen los registros de las alarmas.

Este archivo histórico podría ser vaciado o transferido a cinta luego que se supere un umbral o fecha, pudiendo ser estos modificables por el operador, a fin de no llenar espacio en disco.

d. Categoría de las alarmas

Las alarmas tendrán al menos dos categorías programables:

- Urgente
- No urgente

3.2.4 Medidas de Calidad de Prestaciones

En este apartado se describen las medidas de calidad de prestaciones que se podrán realizar extremo a extremo en los Trayecto SDH controladas desde el GSR.

a. Parámetros a medir

Se deberán realizar las siguientes medidas extremo a extremo sobre tramas SDH:

- Medidas de errores sobre el Byte B1.
- Monitorización del Byte J0.

b. Almacenamiento

Cada uno de los parámetros anteriores, se deberán almacenar en registros en el GSR. Por evento de funcionamiento y por sentido de la transmisión se proporcionarán los siguientes registros:

- Registros de medidas de 15 minutos que acumulen eventos de funcionamiento durante periodos fijos de 15 minutos.
- Registros de 24 horas que acumulen eventos de funcionamiento durante un periodo fijo de 24 horas.

Los registros de 15 minutos constituyen una pila de 16 registros recientes por lo menos. Cuando todos los registros de 15 minutos están llenos, se utiliza un mecanismo de "eliminación parcial" para descartar la información más antigua.

Se deberán enviar periódicamente al GSR de forma automática y sin intervención del operador las medidas almacenadas en el ER. En el GSR se almacenarán registros de 15 minutos durante 8 horas, y registros de 24 horas, durante 30 días.

c. Envío

Se deberán enviar periódicamente al GSR las medidas almacenadas en el ER, por medio de una petición de envío selectiva, de forma automática o a petición del operador.

d. Inhibición

Cualquiera de las medidas se podrá inhibir en un momento dado a voluntad del operador del GSR.

e. Visualización

El operador tendrá acceso para visualizar las medidas almacenadas en el GSR, o bien pedir un envío de las medidas que están almacenadas en el ER para su visualización.

f. Programación

Será posible realizar medidas de calidad programadas en fecha, hora y duración determinadas por el operador.

3.3 Seguridad

En este apartado se describen las funciones relativas al control del acceso al GSR y los privilegios que se pueden configurar para cada operador del sistema.

3.3.1 Control de Acceso

Se registrarán los intentos de acceso fallidos, así como los accesos y el operador que los ha realizado. Mas de un usuario, con idéntica categoría o privilegio, no podrá acceder a un nodo al mismo tiempo.

3.3.2 Cierre Automático de Sesiones

El sistema deberá cerrar automáticamente la sesión abierta por cualquier usuario tras un tiempo de inactividad definible (ejemplo: 30 minutos).

3.3.3 Privilegios de Operador

Se deberán establecer los siguientes niveles de privilegios:

- Administrador (Root) : Es el súper usuario del sistema. Puede acceder a todas las funcionalidades del sistema de gestión y de la plataforma de software básico usada para soportarlo(sistema operacional, privilegios de acceso, archivos de configuración, etc.);
- Supervisor: Es un usuario privilegiado, que tiene acceso a todas las funcionalidades de gestión, pero que no tiene acceso al software básico de la plataforma computacional. Además de eso el supervisor puede acceder a algunas de las funcionalidades de instalación, más no tiene acceso a otras;
- Operador: Es un usuario local común del sistema de Gestión. Puede acceder a un conjunto restringido de funcionalidades del sistema y no tiene acceso a funcionalidades de configuración;
- Instalador: Es un usuario (usualmente remoto) del Sistema de Gestión. Puede acceder a un conjunto restringido de funcionalidades de gestión y accede a todas las funcionalidades de configuración.
- Cliente, tiene acceso a un dominio restringido a nivel de circuitos, pudiendo ejecutar activar / desactivar pruebas, registro de conexiones, supervisión y monitorización de alarmas y configuraciones de los equipamientos del enlace, vía Web.

3.3.4 Palabra de Paso

El control de acceso al sistema se realizará por medio de palabra de paso de al menos 6 caracteres alfanuméricos. Se llevará control en el correspondiente histórico de operador de los intentos de acceso fallidos y la palabra de paso empleada.

3.3.5 Recuperación tras Intrusión

El Administrador del GSR podrá acceder a ficheros de respaldo para restaurar un servicio tras una violación de la seguridad o en caso de catástrofe.

3.4 Funciones de la Base de Datos del Gestor

Se describen en este apartado las funciones de gestión de la base de datos (MIB) del GSR.

3.4.1 Almacenamiento de Eventos

Se deberán registrar los siguientes tipos de eventos:

- Fallos en la red no achacables al equipo.
- Mal funcionamiento.
- Mala operación.

Se podrá realizar interrogación selectiva al histórico de eventos, según los diferentes campos que integran cada evento. En el histórico se almacenará en el campo correspondiente la fecha y hora del ER en que se ha producido el evento.

3.4.2 Visualización del Histórico de Eventos

La presentación del histórico de eventos se podrá realizar de forma selectiva de acuerdo con un "or" de los diferentes campos que integran la alarma.

3.4.3 Realización de Informes

Por medio de una Interrogación selectiva a la base de datos se podrán realizar informes de los elementos gestionados en la base de datos: ER, alarmas, mediciones, configuraciones, disponibilidad, etc. El suministrador proporcionará los archivos en formato exportable a programas de proceso de texto u hojas de calculo comerciales.

3.4.4 Consistencia de las Bases de Datos

Se podrá realizar interrogación selectiva a los elementos gestionados para comprobar consistencia entre MIB del gestor y del ER.

3.4.5 Copias de Respaldo (Backup)

La aplicación de gestión realizará las copias de respaldo de la MIB en el GSR. El administrador del sistema, tendrá privilegios para realizar funciones de mantenimiento de las copias de respaldo.

a. Realización

La realización de copias de respaldo podrá realizarse sin que quede afectado el servicio. Será posible desde la aplicación de gestión llevar un control semanal o mensual de las copias realizadas.

b. Acceso

El acceso tanto a las copias de respaldo como a las posibles restauraciones de dichas copias estará restringido al Administrador del Sistema en casos de emergencia.

3.5 Telecarga del Soporte Lógico (Software)

Esta función proporcionará la recarga software de los ER a distancia. Se entiende por recarga la transferencia de las tablas de configuración, funciones de aplicación residentes y funciones de comunicación de mensajes. Las funciones disponibles se describen a continuación.

3.5.1 Ejecución

Se realizará invocando la función "telecarga" por medio de la interfaz Hombre / Maquina del GSR, indicando unívocamente los datos identificativos del ER a recargar y todo tipo de información que permita identificar la operación a realizar. Se activará de forma simplificada por medio de una única operación.

3.5.2 Control

Se realizará el control de la Telecarga por medio de la presentación automática de informes que manifiesten cualquier incidencia acaecida durante su realización. Se presentará confirmación de fin de recarga realizada con éxito.

Se verificarán por medio de las auditorias pertinentes la integridad y coherencia de los datos. Se llevará un registro detallado de las actividades de telecarga, como son fecha y hora, usuario, versión de software y resultado de la operación.

3.5.3 Activación

Una vez completadas con éxito las anteriores operaciones de telecarga. Se podrá activar el nuevo software recargado.

Se habilitarán procedimientos de restauración a la versión original para el caso de fallo en la activación del nuevo software.

3.6 Sincronización de los ER

La sincronización de fecha y hora se realizará desde el GSR a todos los ER que dependan de él. La fecha y hora del GSR deberá sincronizarse con la fecha y hora de las demás plataformas de gestión existentes en la planta utilizando el protocolo Network Timing Protocolo (NTP) o Simple Network Timing Protocol (SNTP).

3.6.1 Envío

La Fecha y Hora se enviarán a todos los ER, de forma automática desde el GSR en los siguientes casos:

- Periódicamente al menos una vez al día.
- Cuando se pierda la conexión entre el ER y el GER, al recuperarse esta conexión.
- Cuando se produzca un rearranque del ER.

3.6.2 Programación

Se podrá programar y modificar la hora de envío de sincronización de fecha y hora desde el GSR a los ER que dependan de él.

3.7 Indicación Temporal

Los eventos, cuentas de eventos y alarmas del ER, llevarán indicación temporal, con una resolución de un segundo con relación al reloj local del ER.

El comienzo de los registros de 15 minutos y 24 horas, tendrá una aproximación de ±10 segundos con respecto al tiempo real del ER.

CAPÍTULO IV
PRUEBAS EN TMN Y NUEVAS ALTERNATIVAS DE GESTION

4.1 Introducción

Una vez contratado un producto TMN, es necesario comprobarlo para verificar el cumplimiento de las especificaciones. Es necesario comprobar la pila de protocolos completa, comprobar que la pila completa OSI está implementada, y que no se trata, por ejemplo, de un CMOT (CMIP over TCP/IP) en lugar de Q3. Después de aceptado el producto, modificaciones y cambios son demasiado costosos.

Era necesario contar con una entidad idónea que pudiera proveer la tecnología de pruebas. Como fabricante de soluciones de medición, Wandel & Goltermann no suministra plataformas de gestión, por esta razón, cuenta con la necesaria credibilidad para comprobar cualquier sistema.

4.2 Realización de las Pruebas

Las empresas contratantes deben contar con recursos propios para realizar las pruebas opcionalmente, pueden contar con servicios de empresas neutrales para ello. Para acompañar y/o realizar las pruebas, las empresas contratantes deben contar con personal especializado: ingenieros de telecomunicaciones, analistas de sistemas y técnicos en telecomunicaciones con buen conocimiento general de sistemas de telecomunicaciones, deben estar familiarizados con los conceptos de la TMN, estructuras de programación estándares OSI y ITU-T, conocimiento de protocolos y dominio del idioma inglés.

4.3 Ambiente de Pruebas

El ambiente de pruebas está compuesto por 3 sistemas básicos:

4.3.1 Plataforma de evaluación del modelo de información

Soporta la realización de pruebas estáticas en modelos de información, incluyendo:

- Análisis de modelos de información mediante un *browser*.
- Editor de clases de objetos.
- compiladores GDMO y ASN.1.
- Herramientas para crear módulos "gestores" y "agentes".

4.3.2 Plataforma de pruebas de interfaces TMN

Soporta pruebas dinámicas de implementaciones particulares de interfaces TMN, verificando el modelo de información y la pila de protocolos, incluyendo: Herramientas para la preparación de conjuntos de pruebas (*Abstract Test Suites*), su ejecución y emisión de diagnósticos de verificación de conformidad con un estándar pre-definido.

4.3.3 Dispositivo de monitorización de protocolos TMN

Permite, al ser conectado a una interfaz TMN entre gestor y agente, la monitorización de las PDUs de las 7 capas de la pila OSI, entre otros protocolos como: CMIP, ACSE (*Association Control Service Element*) y ROSE (*Remote Operation Service Element*).

4.4 Plataforma de Pruebas

Wandel & Goltermann actúa hace más de 60 años en el área de instrumentos de prueba. En el caso de pruebas de sistemas de gestión **[10]**, actúa en colaboración con una empresa de software especializado en Alemania, especializada en sistemas de pruebas para ambientes OSI (sistemas para X.400, X.500, FTAM). Uno de sus productos ofrecido es una plataforma de pruebas llamada NMA-100 (OSITEST-NM).

El NMA-100 / OSITEST FTAM ya es utilizado por muchas empresas que están desarrollando e implementando redes de gestión TMN a nivel mundial:

- CSELT S.p.A. -- Torino, Italia
- DeTeMobil -- Bonn, Alemania
- Ericsson -- Karlstaad, Suecia
- Nokia -- Espoo, Finlandia
- Joint International Test Center (JITC) -- Fort Huachuca, EUA
- PKI -- Nurimberga, Alemania
- SEL / Alcatel -- Stuttgart, Alemania
- Siemens Nixdorf -- Munich, Alemania

- TRT -- Lannion y Paris, Francia
- CPqD de Telebrás -- Campinas, Brasil
- Varias otras empresas con divulgación no autorizada, y otras muy brevemente en Brasil (Embratel, Telesp, etc.).

El costo de un sistema de pruebas es insignificante en comparación con los costos de los sistemas de gestión. Constituye una excelente inversión si se considera lo que se puede ahorrar en el futuro.

4.4.1 Características del NMA-100

El NMA-100 es un sistema de pruebas que se destina a la validación de aplicaciones de gestión de redes. Estas pueden ser estandarizadas o propietarias, también realiza la validación del stack OSI de comunicación incluyendo CMISE, ROSE, ACSE, además de las capas de presentación, sesión y transporte de la ISO. El NMA-100 constituye el soporte necesario para el desarrollo e integración de redes heterogéneas.

Se puede realizar una ejecución automática de pruebas que simulan condiciones de operación pré-definidas, también es posible realizar el envío interactivo de PDUs. Las siguientes pruebas son posibles:

- Aceptación y aprobación.
- Interoperabilidad.
- Pruebas de conformidad.
- Pruebas de esfuerzo (stress tests).
- Pruebas en desarrollo.

4.4.2 Aplicaciones del NMA-100

El NMA-100 puede simular el gestor, para ello, puede enviar PDUs a varios NEs simultáneamente y analizar su comportamiento. Puede simular diversos NEs simultáneamente, para ello, puede simular por lo menos 7 NEs y comprobar de esa forma el gestor.

El NMA-100 puede ejecutar pruebas de conformidad, cumple con el CTS-3 (comité europeo) y cumple también con los requerimientos de Bellcore. El NMA-100 fue

desarrollado según los estándares ISO 9646 e ITU-T X.290 (pruebas de sistemas abiertos); en la Figura 4.1 se ilustra algunas configuraciones para pruebas.

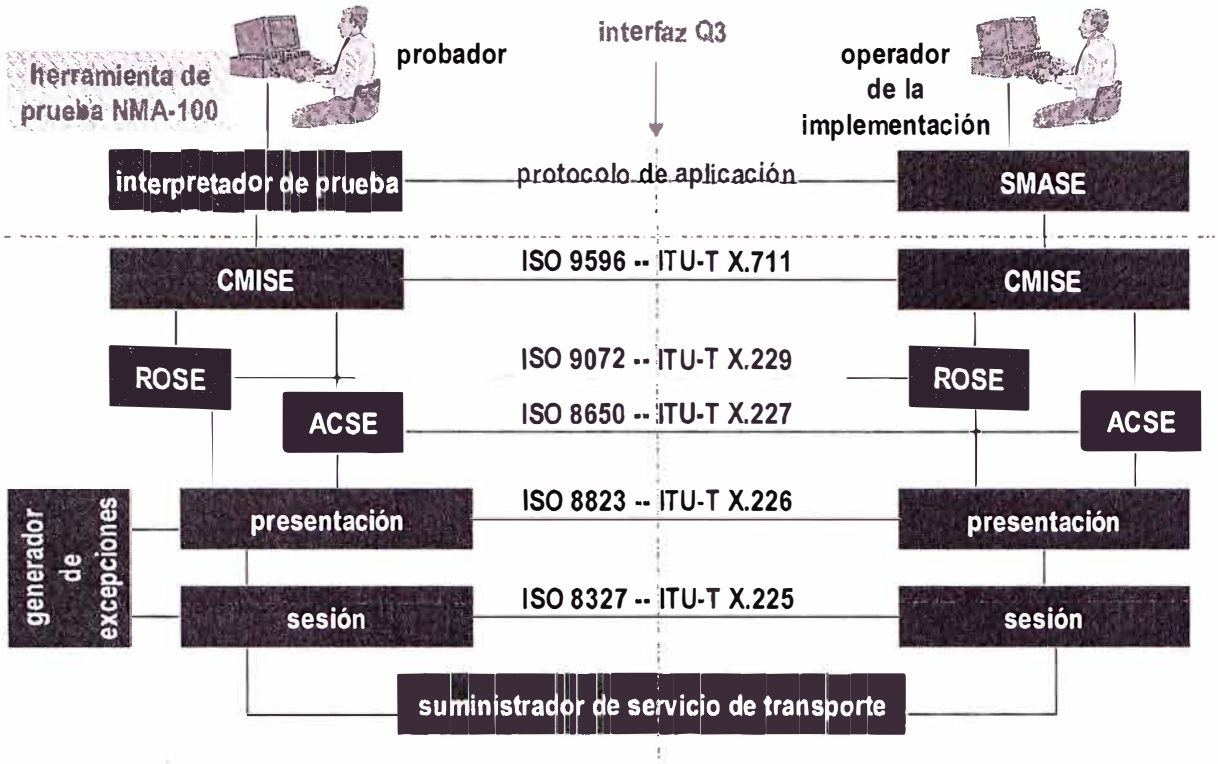

Figura 4.1 Configuraciones para Pruebas

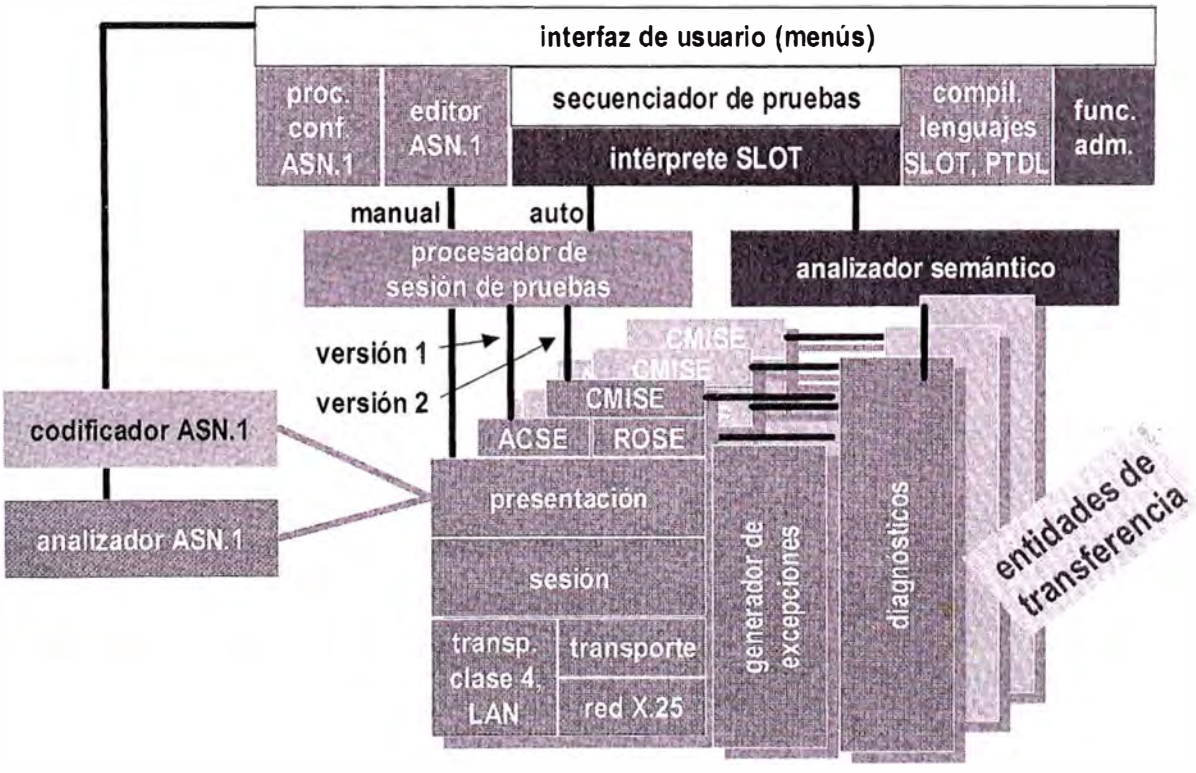

Figura 4.2 Componentes del Sistema NMA-100

4.4.3 Componentes del Sistema NMA-100

El sistema NMA-100 consta de lo siguientes componentes según la Figura 4.2:

a. Codificador ASN.1

Transforma valores de datos ASN.1 preparados por el editor en su representación de transferencia aplicando las reglas ISO 8825 / ITU-T X.209.

b. Procesador de configuraciones ASN.1

Compila descripciones modulares ASN.1 en una representación interna adecuada a los demás componentes del sistema.

c. Interfaz de usuario (sistema de menús)

Que permite acceder todos los demás componentes del sistema, soporta entrada de datos y validación de los parámetros a través de ventanas gráficas o interfaces de caracteres, según el caso.

d. Preprocesador de macros ASN.1

Parte stand-alone de la ASN.1, modifica descripciones textuales en ASN.1 para posterior entrada en el procesador de configuraciones. Soluciona macros ASN.1 y las sustituye por tipos básicos ASN.1.

e. Editor ASN.1

Constituye una facilidad para la manipulación de los módulos ASN.1 de forma amigable; esta preconfigurado para manejar las informaciones relevantes del protocolo en el contexto de gestión de redes.

f. Analizador ASN.1

Convierte la representación de transferencia de valores de datos ASN.1 (definida por la ISO 8825 / ITU-T X.209) en una representación interna legible por el editor ASN.1, además detecta y reporta errores de sintaxis.

g. Intérprete SLOT

Ejecuta secuencias de pruebas predefinidas escritas en el lenguaje SLOT (scenario language for OSI testing), derivado de TTCN. El interpretador de escenario es el único significativo en modo automático, siendo invocado por el procesador automático de prueba, no por el usuario.

h. Analizador semántico

Permite evaluar automáticamente cualquier dato recibido según las reglas semánticas de una especificación abstracta de prueba. Cuenta con un lenguaje dedicado (CSL, constraints specification language) suministrado con el sistema.

i. Procesador automático de prueba (ATP)

Dispara la ejecución de los escenarios de pruebas en un plan definido por el usuario, el plan es definido en una secuencia de pruebas utilizando un lenguaje dedicado (ATSL).

j. Procesador de sesión de pruebas

No es algo directamente visible desde la interfaz de usuario, sirve para la supervisión de todas las entidades de transferencia y para el suministro de las informaciones de estado de las conexiones.

k. Entidad de transferencia (TE)

Un caso particular de todos los protocolos de capas de comunicación, incluso las de presentación, sesión y transporte. Varios procesos TE pueden estar simultáneamente activos.

l. Administración

Maneja los resultados de las pruebas, escenarios de pruebas y PDUs.

m. Generador de excepciones

Dispara la ejecución de guiones de prueba PTDL para verificar el comportamiento de las capas de comunicación.

n. Compilador de lenguaje de prueba

Hay compiladores para cada uno de los lenguajes:

- SLOT (lenguaje de escenario de pruebas).
- PTDL (lenguaje de generación de excepciones).
- PDUDL (lenguaje para especificar PDUs excepcionales de sesión y transporte).

4.4.4 Monitor DA-3xQ

Existe un problema, interrupciones y fallas en la TMN pueden causar defectos fatales en redes de telecomunicaciones. Por ejemplo: Errores o alarmas graves detectados por la red de telecomunicaciones no llegan al sistema de gestión, ó, comandos del sistema de gestión para cambiar la capacidad de transmisión entre 2 sitios no llegan al equipo de telecomunicaciones.

Para solucionar esos problemas, es necesario monitorizar el tráfico de datos en la red de gestión de telecomunicaciones. El monitor DA-3xQ ayuda a mantener la TMN libre de errores. El DA-3xQ monitoriza todas las capas de la pila OSI en ambas direcciones y analiza las unidades de datos de protocolo.

La gran complejidad de la Interfaz Q3 puede causar problemas de interoperabilidad, el monitor DA-3xQ localiza esos problemas, muestra todas las unidades de datos de protocolo de todas las capas de forma inteligible. Con comandos de filtrado y búsqueda las PDUs erróneas pueden ser fácilmente identificadas.

Las capas propietarias de los protocolos aún están en uso y pueden ser mezcladas con protocolos de capas estandarizados. Muchos sistemas de gestión y elementos de red operan hoy con protocolos propietarios en las capas inferiores. Un monitor de protocolos debe poder adaptarse a esos protocolos de capas propietarios.

El DA-3xQ analiza capas de protocolo tanto estandarizadas como propietarias, además incluye un Paquete especial de "pegamento" de protocolos que permite definir capas propietarias de protocolos mediante un menú.

4.4.5 Aplicaciones del Analizador DA-3xQ

Para operadores de una TMN y suministradores de redes de gestión, sirve para una localización de fallas más eficaz aumenta la disponibilidad de la TMN y garantiza la continuidad de la gestión de las redes de telecomunicaciones.

Para los fabricantes de equipos sirve para *debugging* durante las pruebas de gestor / agente mejorando la calidad del producto y reduce los riesgos y los costos. Para los grupos de instalación e integración sirve en la puesta en servicio de la TMN, integración e instalación más rápida para una reducción de los costos.

4.4.6 Características del DA-3xQ

El analizador DA-3xQ presenta las siguientes características:

- Analizador para funciones de control y mensajes en la TMN. Las funciones de control se refieren a comandos del sistema de gestión a los elementos de red. Los mensajes se refieren a "alertas" y "notificaciones" generadas por los elementos de red hacia el sistema de gestión.
- Decodificación de toda la pila de protocolos hasta ACSE, ROSE y CMIP (capa de aplicación).
- La pila de protocolos puede ser configurada. En las capas para las cuales son estandarizadas varias opciones de protocolos de capas, el DA-3xQ presenta un menú a partir del cual se puede seleccionar la configuración de protocolo necesaria.
- Incluye herramientas que permiten una fácil adaptación a capas propietarias del protocolo. El paquete de "pegamento" (*Glue protocol package*) que acompaña al DA-3xQ permite definir capas que se adaptan exactamente al protocolo propietario.
- Despliegue de los protocolos de las capas de presentación y de aplicación en notación ASN.1. La ASN.1 es adecuada a estructuras de datos complejas como las utilizadas en CMIP.
- Comandos de búsqueda y filtros de pantalla para los datos capturados.
- Evaluaciones especiales programables. El DA-3xQ incluye el *PAL*, el lenguaje para análisis de protocolo del ITU-T compatible con SDL. La PAL permite definir procedimientos de análisis complejos, compuestos de varios procesos. La programación no ofrece dificultades ni consume mucho tiempo.

- Varias opciones de interfaces físicas. El estándar Q3/CMIP permite utilizar varios tipos de interfaces físicas, tales como Ethernet, X.21, V.11, etc. El DA-3xQ debe ser equipado con los mismos tipos de interfaz que el enlace Q3 a monitorizar, para ello, dispone de un amplio abanico de interfaces.

CONCLUSIONES

1) Actualmente todavía no existe una solución en el marco de la gestión de red que pueda proporcionar resultados satisfactorios a todo tipo de redes de telecomunicaciones. Es necesario entonces comprobar que las pilas (*stacks*) de protocolos fueran realmente Q3 y comprobar que todas las capas del protocolo fueran implementadas.

2) El modelo de información documentado también debería comprobarse para verificar que de hecho estuviera implementado. La finalidad de las pruebas sería evitar sorpresas en un futuro.

3) Tras la aceptación y el pago, es prácticamente imposible exigir la solución de esos problemas. Esto implicaría costos mucho más elevados en la interconexión (convertidores de protocolos) y en la interoperación (conversión de las MIBs).

4) La TNM, o red de gestión de telecomunicaciones es el camino más valido para enfocar la gestión en grandes redes. El protocolo CMIP permite utilizar las funcionalidades requeridas normalmente para gestionar redes con gran número de nodos obteniendo mejor rendimiento que entornos más simples y baratos como el basado en SNMP que genera a menudo un tráfico de señalización excesivo.

5) En cuanto al soporte por parte de fabricantes, el protocolo SNMP es el utilizado por la gran mayoría de fabricantes y clientes, y existe una multitud de productos comerciales. Los gastos de mantenimiento también suelen ser menores en SNMP al ser más simple y tener una mayor base comercial.

6) El sistema basado en SNMPv2 soluciona muchos de los problemas de su anterior versión, SNMP; sin embargo, su mayor complejidad e incompatibilidad con la versión SNMP esta desestimando su implementación.

ANEXO A

GLOSARIO

ASN.1	abstract syntax notation one
AOL	Amplificador óptico de línea
ER	Elemento de Red (Element Network)
GDMO	Guidelines Managed Object
GER	Gestor de Elementos de Red
GSR	Gestor de Subred
MO	Objeto gestionado (managed objects)
MIB	Base de información de gestión (management information base)
ADM	Equipo de Extracción / inserción.(Add Drop Multiplex)
OMG	Object Management Group
RCD	Red de comunicación de datos
RDSI	Red digital de servicios integrados
RO	Red Óptica
TMO	Terminal Multiplexor Óptico
UIT-T	Unión Internacional de Telecomunicaciones, sector de Transmisión

BIBLIOGRAFÍA

[1] ALCATEL HUAWEI y NEC, "Manuales de Equipos SDH".

[2] INTERNATIONAL TELECOMMUNICATIONS UNION (ITU) Telecommunication Standardization Sector (ITU-T). Recomendaciones de la Serie G, M y X. **http://www.itu.int/publications/.**

[3] OPEN SYSTEM INTERCONECTION (OSI) Management Standards. **http://www.iso.org.**

[4] INTERNET ENGINEERING TASK FORCE (IETF). RFCs, MIBs. **http://www.ietf.org.**

[5] Stephen B. Morris, "Network Management, MIBs and MPLS: Principles, Design and Implementation", Pearson Education, Inc., 2003.

[6] SunSoft, "SunLink OSI 8.1", Sun Microsystems, Inc., 1995. **http://docs.sun.com/.**

[7] Joan Serrat Fernández, "V Cátedra Fundación Telefónica: Gestión de Redes", Pontificia Universidad Católica del Perú - Lima, Agosto del 2003.

[8] Ángel López Gonzáles y Alejandro Novo López, "Protocolos de Internet: Diseño e Implementación en Sistemas UNIX", ALFAOMEGA S.A., 2000.

[9] Antoni Barba Marti, "Gestión de Red", Edicions UPC, 1999.

[10] Walden & Goltermanm, "Conceptos de Gestión de Redes y TMN, Pruebas de Conformidad, Análisis de protocolos", 1996.