INTRODUCCIÓN A LA JERARQUÍA DIGITAL SÍNCRONA (SDH)

Luis Velasco

PRIMERA EDICIÓN: Enero 2005

ISBN 84-689-0673-5

Índice de Contenidos

PREFACIO

Este libro presenta los conceptos básicos de *Jerarquía Digital Síncrona*, SDH, desde el punto de vista de la propia tecnología, así como desde el punto de vista de red y de plano de gestión.

En la contraportada del libro puede observarse que la edición se ha realizado bajo licencia pública general (GPL, *General Public License*). Esto implica que se aplican los mismos derechos y obligaciones asociadas a la documentación del sistema operativo Linux, diseñadas por la GNU, esto es, el libro puede ser utilizado con total libertad sin pagar derechos de propiedad intelectual y puede ser extendido por otras personas para cubrir temas adicionales, mejorar el formato, introducir nuevas opciones, etc. En el sitio web de GNU (WWW.GNU.ORG) y en el apartado "Licencia de documentación libre de GNU", puede accederse a los detalles de licencia y posterior utilización del material para su extensión y enriquecimiento.

LICENCIA DE DOCUMENTACIÓN LIBRE DE GNU

Versión 1.2, Noviembre 2002

> This is an unofficial translation of the GNU Free Documentation License into Spanish. It was not published by the Free Software Foundation, and does not legally state the distribution terms for documentation that uses the GNU FDL -- only the original English text of the GNU FDL does that. However, we hope that this translation will help Spanish speakers understand the GNU FDL better.
>
> Ésta es una traducción no oficial de la GNU Free Document License a Español (Castellano). No ha sido publicada por la Free Software Foundation y no establece legalmente los términos de distribución para trabajos que usen la GFDL (sólo el texto de la versión original en Inglés de la GFDL lo hace). Sin embargo, esperamos que esta traducción ayude los hispanohablantes a entender mejor la GFDL. La versión original de la GFDL esta disponible en la Free Software Foundation.
>
> Esta traducción está basada en una de la versión 1.1 de Igor Támara y Pablo Reyes. Sin embargo la responsabilidad de su interpretación es de Joaquín Seoane.
>
>

A.1. PREÁMBULO

El propósito de esta Licencia es permitir que un manual, libro de texto, u otro documento escrito sea *libre* en el sentido de libertad: asegurar a todo el mundo la libertad efectiva de copiarlo y redistribuirlo, con o sin modificaciones, de manera comercial o no. En segundo término, esta Licencia proporciona al autor y al

editor[2] una manera de obtener reconocimiento por su trabajo, sin que se le considere responsable de las modificaciones realizadas por otros.

Esta Licencia es de tipo *copyleft*, lo que significa que los trabajos derivados del documento deben a su vez ser libres en el mismo sentido. Complementa la Licencia Pública General de GNU, que es una licencia tipo copyleft diseñada para el software libre.

Hemos diseñado esta Licencia para usarla en manuales de software libre, ya que el software libre necesita documentación libre: un programa libre debe venir con manuales que ofrezcan la mismas libertades que el software. Pero esta licencia no se limita a manuales de software; puede usarse para cualquier texto, sin tener en cuenta su temática o si se publica como libro impreso o no. Recomendamos esta licencia principalmente para trabajos cuyo fin sea instructivo o de referencia.

A.2. APLICABILIDAD Y DEFINICIONES

Esta Licencia se aplica a cualquier manual u otro trabajo, en cualquier soporte, que contenga una nota del propietario de los derechos de autor que indique que puede ser distribuido bajo los términos de esta Licencia. Tal nota garantiza en cualquier lugar del mundo, sin pago de derechos y sin límite de tiempo, el uso de dicho trabajo según las condiciones aquí estipuladas. En adelante la palabra *Documento* se referirá a cualquiera de dichos manuales o trabajos. Cualquier persona es un licenciatario y será referido como *Usted*. Usted acepta la licencia si copia. modifica o distribuye el trabajo de cualquier modo que requiera permiso según la ley de propiedad intelectual.

Una *Versión Modificada* del Documento significa cualquier trabajo que contenga el Documento o una porción del mismo, ya sea una copia literal o con modificaciones y/o traducciones a otro idioma.

Una *Sección Secundaria* es un apéndice con título o una sección preliminar del Documento que trata exclusivamente de la relación entre los autores o editores y el tema general del Documento (o temas relacionados) pero que no contiene nada que entre directamente en dicho tema general (por ejemplo, si el Documento es en parte un texto de matemáticas, una Sección Secundaria puede no explicar nada de matemáticas). La relación puede ser una conexión histórica con el tema o temas relacionados, o una opinión legal, comercial, filosófica, ética o política acerca de ellos.

Las *Secciones Invariantes* son ciertas Secciones Secundarias cuyos títulos son designados como Secciones Invariantes en la nota que indica que el documento es liberado bajo esta Licencia. Si una sección no entra en la definición de Secundaria, no puede designarse como Invariante. El documento puede no tener Secciones Invariantes. Si el Documento no identifica las Secciones Invariantes, es que no las tiene.

Los *Textos de Cubierta* son ciertos pasajes cortos de texto que se listan como Textos de Cubierta Delantera o Textos de Cubierta Trasera en la nota que indica que el documento es liberado bajo esta Licencia. Un Texto de Cubierta Delantera puede tener como mucho 5 palabras, y uno de Cubierta Trasera puede tener hasta 25 palabras.

Una copia *Transparente* del Documento, significa una copia para lectura en máquina, representada en un formato cuya especificación está disponible al público en general, apto para que los contenidos puedan ser vistos y editados directamente con editores de texto genéricos o (para imágenes compuestas por puntos) con programas genéricos de manipulación de imágenes o (para dibujos) con algún editor de dibujos ampliamente disponible, y que sea adecuado como entrada para formateadores de texto o para su traducción automática a formatos adecuados para formateadores de texto. Una copia hecha en un formato definido como Transparente, pero cuyo marcaje o ausencia de él haya sido diseñado para impedir o dificultar modificaciones posteriores por parte de los lectores no es Transparente. Un formato de imagen no es Transparente si se usa para una cantidad de texto sustancial. Una copia que no es *Transparente* se denomina *Opaca*.

Como ejemplos de formatos adecuados para copias Transparentes están ASCII puro sin marcaje, formato de entrada de Texinfo, formato de entrada de LaTeX, SGML o XML usando una DTD disponible públicamente, y HTML, PostScript o PDF simples, que sigan los estándares y diseñados para que los modifiquen personas. Ejemplos de formatos de imagen transparentes son PNG, XCF y JPG. Los formatos Opacos incluyen formatos propietarios que pueden ser leídos y editados únicamente en procesadores de palabras propietarios, SGML o XML para los cuáles las DTD y/o herramientas de procesamiento no estén ampliamente disponibles, y HTML, PostScript o PDF generados por algunos procesadores de palabras sólo como salida.

La *Portada* significa, en un libro impreso, la página de título, más las páginas siguientes que sean necesarias para mantener legiblemente el material que esta Licencia requiere en la portada. Para trabajos en formatos que no tienen página de portada como tal, *Portada* significa el texto cercano a la aparición más prominente del título del trabajo, precediendo el comienzo del cuerpo del texto.

Una sección *Titulada XYZ* significa una parte del Documento cuyo título es precisamente XYZ o contiene XYZ entre paréntesis, a continuación de texto que traduce XYZ a otro idioma (aquí XYZ se refiere a nombres de sección específicos mencionados más abajo, como *Agradecimientos*, *Dedicatorias* , *Aprobaciones* o *Historia*. *Conservar el Título* de tal sección cuando se modifica el Documento significa que permanece una sección *Titulada XYZ* según esta definición[3].

El Documento puede incluir Limitaciones de Garantía cercanas a la nota donde se declara que al Documento se le aplica esta Licencia. Se considera que estas Limitaciones de Garantía están incluidas, por referencia, en la Licencia, pero sólo en cuanto a limitaciones de garantía: cualquier otra implicación que estas Limitaciones de Garantía puedan tener es nula y no tiene efecto en el significado de esta Licencia.

A.3. COPIA LITERAL

Usted puede copiar y distribuir el Documento en cualquier soporte, sea en forma comercial o no, siempre y cuando esta Licencia, las notas de copyright y la nota que indica que esta Licencia se aplica al Documento se reproduzcan en todas las copias y que usted no añada ninguna otra condición a las expuestas en esta Licencia. Usted no puede usar medidas técnicas para obstruir o controlar la lectura o copia posterior de las copias que usted haga o distribuya. Sin embargo, usted puede

aceptar compensación a cambio de las copias. Si distribuye un número suficientemente grande de copias también deberá seguir las condiciones de la sección 3.

Usted también puede prestar copias, bajo las mismas condiciones establecidas anteriormente, y puede exhibir copias públicamente.

A.4. COPIADO EN CANTIDAD

Si publica copias impresas del Documento (o copias en soportes que tengan normalmente cubiertas impresas) que sobrepasen las 100, y la nota de licencia del Documento exige Textos de Cubierta, debe incluir las copias con cubiertas que lleven en forma clara y legible todos esos Textos de Cubierta: Textos de Cubierta Delantera en la cubierta delantera y Textos de Cubierta Trasera en la cubierta trasera. Ambas cubiertas deben identificarlo a Usted clara y legiblemente como editor de tales copias. La cubierta debe mostrar el título completo con todas las palabras igualmente prominentes y visibles. Además puede añadir otro material en las cubiertas. Las copias con cambios limitados a las cubiertas, siempre que conserven el título del Documento y satisfagan estas condiciones, pueden considerarse como copias literales.

Si los textos requeridos para la cubierta son muy voluminosos para que ajusten legiblemente, debe colocar los primeros (tantos como sea razonable colocar) en la verdadera cubierta y situar el resto en páginas adyacentes.

Si Usted publica o distribuye copias Opacas del Documento cuya cantidad exceda las 100, debe incluir una copia Transparente, que pueda ser leída por una máquina, con cada copia Opaca, o bien mostrar, en cada copia Opaca, una dirección de red donde cualquier usuario de la misma tenga acceso por medio de protocolos públicos y estandarizados a una copia Transparente del Documento completa, sin material adicional. Si usted hace uso de la última opción, deberá tomar las medidas necesarias, cuando comience la distribución de las copias Opacas en cantidad, para asegurar que esta copia Transparente permanecerá accesible en el sitio establecido por lo menos un año después de la última vez que distribuya una copia Opaca de esa edición al público (directamente o a través de sus agentes o distribuidores).

Se solicita, aunque no es requisito, que se ponga en contacto con los autores del Documento antes de redistribuir gran número de copias, para darles la oportunidad de que le proporcionen una versión actualizada del Documento.

A.5. MODIFICACIONES

Puede copiar y distribuir una Versión Modificada del Documento bajo las condiciones de las secciones 2 y 3 anteriores, siempre que usted libere la Versión Modificada bajo esta misma Licencia, con la Versión Modificada haciendo el rol del Documento, por lo tanto dando licencia de distribución y modificación de la Versión Modificada a quienquiera posea una copia de la misma. Además, debe hacer lo siguiente en la Versión Modificada:

- A. Usar en la Portada (y en las cubiertas, si hay alguna) un título distinto al del Documento y de sus versiones anteriores (que deberían, si hay alguna,

estar listadas en la sección de Historia del Documento). Puede usar el mismo título de versiones anteriores al original siempre y cuando quien las publicó originalmente otorgue permiso.

- B. Listar en la Portada, como autores, una o más personas o entidades responsables de la autoría de las modificaciones de la Versión Modificada, junto con por lo menos cinco de los autores principales del Documento (todos sus autores principales, si hay menos de cinco), a menos que le eximan de tal requisito.

- C. Mostrar en la Portada como editor el nombre del editor de la Versión Modificada.

- D. Conservar todas las notas de copyright del Documento.

- E. Añadir una nota de copyright apropiada a sus modificaciones, adyacente a las otras notas de copyright.

- F. Incluir, inmediatamente después de las notas de copyright, una nota de licencia dando el permiso para usar la Versión Modificada bajo los términos de esta Licencia, como se muestra en la Adenda al final de este documento.

- G. Conservar en esa nota de licencia el listado completo de las Secciones Invariantes y de los Textos de Cubierta que sean requeridos en la nota de Licencia del Documento original.

- H. Incluir una copia sin modificación de esta Licencia.

- I. Conservar la sección Titulada *Historia*, conservar su Título y añadirle un elemento que declare al menos el título, el año, los nuevos autores y el editor de la Versión Modificada, tal como figuran en la Portada. Si no hay una sección Titulada *Historia* en el Documento, crear una estableciendo el título, el año, los autores y el editor del Documento, tal como figuran en su Portada, añadiendo además un elemento describiendo la Versión Modificada, como se estableció en la oración anterior.

- J. Conservar la dirección en red, si la hay, dada en el Documento para el acceso público a una copia Transparente del mismo, así como las otras direcciones de red dadas en el Documento para versiones anteriores en las que estuviese basado. Pueden ubicarse en la sección *Historia*. Se puede omitir la ubicación en red de un trabajo que haya sido publicado por lo menos cuatro años antes que el Documento mismo, o si el editor original de dicha versión da permiso.

- K. En cualquier sección Titulada *Agradecimientos* o *Dedicatorias*, Conservar el Título de la sección y conservar en ella toda la sustancia y el tono de los agradecimientos y/o dedicatorias incluidas por cada contribuyente.

- L. Conservar todas las Secciones Invariantes del Documento, sin alterar su texto ni sus títulos. Números de sección o el equivalente no son considerados parte de los títulos de la sección.

- M. Borrar cualquier sección titulada *Aprobaciones*. Tales secciones no pueden estar incluidas en las Versiones Modificadas.

- N. No cambiar el título de ninguna sección existente a *Aprobaciones* ni a uno que entre en conflicto con el de alguna Sección Invariante.

- O. Conservar todas las Limitaciones de Garantía.

Si la Versión Modificada incluye secciones o apéndices nuevos que califiquen como Secciones Secundarias y contienen material no copiado del Documento, puede opcionalmente designar algunas o todas esas secciones como invariantes. Para hacerlo, añada sus títulos a la lista de Secciones Invariantes en la nota de licencia de la Versión Modificada. Tales títulos deben ser distintos de cualquier otro título de sección.

Puede añadir una sección titulada *Aprobaciones*, siempre que contenga únicamente aprobaciones de su Versión Modificada por otras fuentes --por ejemplo, observaciones de peritos o que el texto ha sido aprobado por una organización como la definición oficial de un estándar.

Puede añadir un pasaje de hasta cinco palabras como Texto de Cubierta Delantera y un pasaje de hasta 25 palabras como Texto de Cubierta Trasera en la Versión Modificada. Una entidad solo puede añadir (o hacer que se añada) un pasaje al Texto de Cubierta Delantera y uno al de Cubierta Trasera. Si el Documento ya incluye un textos de cubiertas añadidos previamente por usted o por la misma entidad que usted representa, usted no puede añadir otro; pero puede reemplazar el anterior, con permiso explícito del editor que agregó el texto anterior.

Con esta Licencia ni los autores ni los editores del Documento dan permiso para usar sus nombres para publicidad ni para asegurar o implicar aprobación de cualquier Versión Modificada.

A.6. COMBINACIÓN DE DOCUMENTOS

Usted puede combinar el Documento con otros documentos liberados bajo esta Licencia, bajo los términos definidos en la sección 4 anterior para versiones modificadas, siempre que incluya en la combinación todas las Secciones Invariantes de todos los documentos originales, sin modificar, listadas todas como Secciones Invariantes del trabajo combinado en su nota de licencia. Así mismo debe incluir la Limitación de Garantía.

El trabajo combinado necesita contener solamente una copia de esta Licencia, y puede reemplazar varias Secciones Invariantes idénticas por una sola copia. Si hay varias Secciones Invariantes con el mismo nombre pero con contenidos diferentes, haga el título de cada una de estas secciones único añadiéndole al final del mismo, entre paréntesis, el nombre del autor o editor original de esa sección, si es conocido, o si no, un número único. Haga el mismo ajuste a los títulos de sección en la lista de Secciones Invariantes de la nota de licencia del trabajo combinado.

En la combinación, debe combinar cualquier sección Titulada *Historia* de los documentos originales, formando una sección Titulada *Historia*; de la misma forma

combine cualquier sección Titulada *Agradecimientos*, y cualquier sección Titulada *Dedicatorias*. Debe borrar todas las secciones tituladas *Aprobaciones*.

A.7. COLECCIONES DE DOCUMENTOS

Puede hacer una colección que conste del Documento y de otros documentos liberados bajo esta Licencia, y reemplazar las copias individuales de esta Licencia en todos los documentos por una sola copia que esté incluida en la colección, siempre que siga las reglas de esta Licencia para cada copia literal de cada uno de los documentos en cualquiera de los demás aspectos.

Puede extraer un solo documento de una de tales colecciones y distribuirlo individualmente bajo esta Licencia, siempre que inserte una copia de esta Licencia en el documento extraído, y siga esta Licencia en todos los demás aspectos relativos a la copia literal de dicho documento.

A.8. AGREGACIÓN CON TRABAJOS INDEPENDIENTES

Una recopilación que conste del Documento o sus derivados y de otros documentos o trabajos separados e independientes, en cualquier soporte de almacenamiento o distribución, se denomina un *agregado* si el copyright resultante de la compilación no se usa para limitar los derechos de los usuarios de la misma más allá de lo que los de los trabajos individuales permiten. Cuando el Documento se incluye en un agregado, esta Licencia no se aplica a otros trabajos del agregado que no sean en sí mismos derivados del Documento.

Si el requisito de la sección 3 sobre el Texto de Cubierta es aplicable a estas copias del Documento y el Documento es menor que la mitad del agregado entero, los Textos de Cubierta del Documento pueden colocarse en cubiertas que enmarquen solamente el Documento dentro del agregado, o el equivalente electrónico de las cubiertas si el documento está en forma electrónica. En caso contrario deben aparecer en cubiertas impresas enmarcando todo el agregado.

A.9. TRADUCCIÓN

La Traducción es considerada como un tipo de modificación, por lo que usted puede distribuir traducciones del Documento bajo los términos de la sección 4. El reemplazo las Secciones Invariantes con traducciones requiere permiso especial de los dueños de derecho de autor, pero usted puede añadir traducciones de algunas o todas las Secciones Invariantes a las versiones originales de las mismas. Puede incluir una traducción de esta Licencia, de todas las notas de licencia del documento, así como de las Limitaciones de Garantía, siempre que incluya también la versión en Inglés de esta Licencia y las versiones originales de las notas de licencia y Limitaciones de Garantía. En caso de desacuerdo entre la traducción y la versión original en Inglés de esta Licencia, la nota de licencia o la limitación de garantía, la versión original en Inglés prevalecerá.

Si una sección del Documento está Titulada *Agradecimientos*, *Dedicatorias* o *Historia* el requisito (sección 4) de Conservar su Título (Sección 1) requerirá, típicamente, cambiar su título.

A.10. TERMINACIÓN

Usted no puede copiar, modificar, sublicenciar o distribuir el Documento salvo por lo permitido expresamente por esta Licencia. Cualquier otro intento de copia, modificación, sublicenciamiento o distribución del Documento es nulo, y dará por terminados automáticamente sus derechos bajo esa Licencia. Sin embargo, los terceros que hayan recibido copias, o derechos, de usted bajo esta Licencia no verán terminadas sus licencias, siempre que permanezcan en total conformidad con ella.

A.11. REVISIONES FUTURAS DE ESTA LICENCIA

De vez en cuando la Free Software Foundation puede publicar versiones nuevas y revisadas de la Licencia de Documentación Libre GNU. Tales versiones nuevas serán similares en espíritu a la presente versión, pero pueden diferir en detalles para solucionar nuevos problemas o intereses. Vea http://www.gnu.org/copyleft/.

Cada versión de la Licencia tiene un número de versión que la distingue. Si el Documento especifica que se aplica una versión numerada en particular de esta licencia o *cualquier versión posterior*, usted tiene la opción de seguir los términos y condiciones de la versión especificada o cualquiera posterior que haya sido publicada (no como borrador) por la Free Software Foundation. Si el Documento no especifica un número de versión de esta Licencia, puede escoger cualquier versión que haya sido publicada (no como borrador) por la Free Software Foundation.

A.12. ADENDA: Cómo usar esta Licencia en sus documentos

Para usar esta licencia en un documento que usted haya escrito, incluya una copia de la Licencia en el documento y ponga el siguiente copyright y nota de licencia justo después de la página de título:

> Copyright (c) AÑO SU NOMBRE. Se otorga permiso para copiar, distribuir y/o modificar este documento bajo los términos de la Licencia de Documentación Libre de GNU, Versión 1.2 o cualquier otra versión posterior publicada por la Free Software Foundation; sin Secciones Invariantes ni Textos de Cubierta Delantera ni Textos de Cubierta Trasera. Una copia de la licencia está incluida en la sección titulada GNU Free Documentation License.

Si tiene Secciones Invariantes, Textos de Cubierta Delantera y Textos de Cubierta Trasera, reemplace la frase *sin ... Trasera* por esto:

> siendo las Secciones Invariantes LISTE SUS TÍTULOS, siendo los Textos de Cubierta Delantera LISTAR, y siendo sus Textos de Cubierta Trasera LISTAR.

Si tiene Secciones Invariantes sin Textos de Cubierta o cualquier otra combinación de los tres, mezcle ambas alternativas para adaptarse a la situación.

Si su documento contiene ejemplos de código de programa no triviales, recomendamos liberar estos ejemplos en paralelo bajo la licencia de software libre que usted elija, como la Licencia Pública General de GNU (*GNU General Public License*), para permitir su uso en software libre.

Notas

[1] Ésta es la traducción del Copyright de la Licencia, no es el Copyright de esta traducción no autorizada.

[2] La licencia original dice *publisher*, que es, estrictamente, quien publica, diferente de *editor*, que es más bien quien prepara un texto para publicar. En castellano *editor* se usa para ambas cosas.

[3] En sentido estricto esta licencia parece exigir que los títulos sean exactamente *Acknowledgements*, *Dedications*, *Endorsements* e *History*, en inglés.

CAPÍTULO 1

Conceptos Básicos de la SDH

La demanda de servicios de telecomunicaciones más eficaces, y con capacidades de comunicación superiores, y una capacidad de gestión flexible y global, hacían necesario buscar una solución de red normalizada. Hoy en día, la solución más extendida es la Jerarquía Digital Síncrona (SDH).

El objetivo de esta unidad es presentar brevemente los conceptos de la SDH, y la definición de la terminología que se usará en posteriores capítulos.

También se pasará revista de forma somera a la función de sincronización de un equipo SDH, exponiendo los conceptos básicos sobre la sincronización.

Por último, trataremos las medidas de calidad que se pueden efectuar en una red gestionada. Al igual que en el resto de la capítulo, expondremos sólo ideas básicas que sirvan de partida a la hora de efectuar estudios más profundos en posteriores unidades.

ESQUEMA DE CONTENIDO

1.1 CONCEPTOS BÁSICOS

1.1.1 Orígenes de la SDH

La SDH es el producto de muchos años de trabajo, a escala mundial, por parte de los organismos de normalización, operadores de red, e industria de las telecomunicaciones. El objetivo era establecer, una base estándar de transmisión óptica de alta velocidad, válida internacionalmente y capaz de satisfacer la demanda actual y previsiones futuras.

Los trabajos en SDH comenzaron en el Grupo de Estudio XVIII del antiguo CCITT (ahora Unión Internacional de Telecomunicaciones - Transmisión, ITU-T) en Junio de 1986. El objetivo consistía en definir una norma mundial para sistemas de transmisión síncrona que aportase una red flexible y económica para las compañías de telecomunicaciones. En noviembre de 1988 se aprobó el primer estándar, definido en las Recomendaciones de la UIT-T G.707, G.708 y G.709, hoy refundidas en una única G.707. Esta Recomendación define las velocidades de transmisión, formatos de señal y estructura de multiplexación para la Interfaz de Nodo de Red (*Network Node Interface, NNI*).

Posteriormente se definieron los estándares relacionados con los modos de operación de los múltiplex síncronos (G.781, G.782 y G.783, hoy refundidas en una única G.783) y gestión de redes síncronas (G.784).

1.1.2 Estructura de multiplexación

La figura 1.1.2-1 muestra el esquema de multiplexación SDH aceptado a nivel europeo. A la derecha aparecen los flujos plesiócronos de 2, 34 y 140 Mbit/s. Cada una de las señales se adapta, para su transmisión por la red SDH, en contenedores síncronos (C-X). Estos contenedores se multiplexan para formar la señal STM-N resultante.

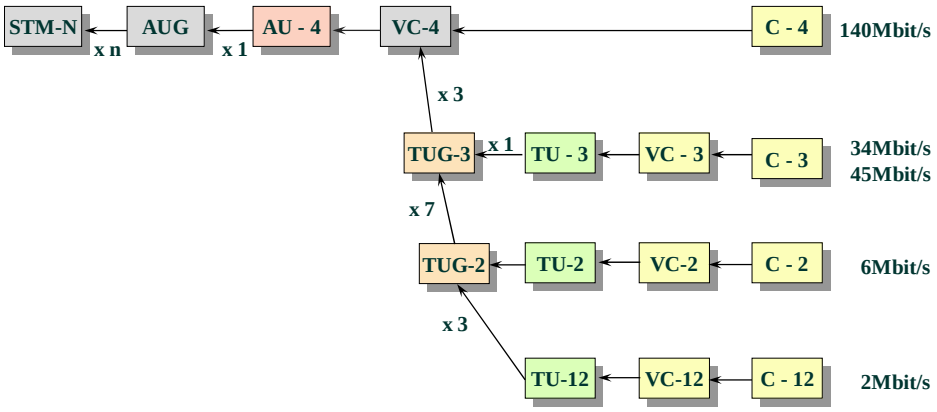

Figura 1.1.2-1 Estructura de multiplexación

1.2 BLOQUES FUNCIONALES

Una forma de describir la funcionalidad general de los equipos múltiplex SDH, es dividirla en bloques funcionales, según define la recomendación G.783 de la UIT-T. La división es genérica y no implica una partición física de funciones. Cada uno de estos bloques funcionales representa una función concreta, fácilmente definible. La concatenación de bloques funcionales discretos define la funcionalidad de un equipo múltiplex SDH. En próximas capítulos utilizaremos esta misma división.

La figura 1.1.2-1 nos muestra los bloques funcionales definidos. Si seguimos el flujo de señales de abajo hacia arriba, mapearemos una señal plesiócrona en un contenedor síncrono y obtendremos (arriba) una señal STM-N.

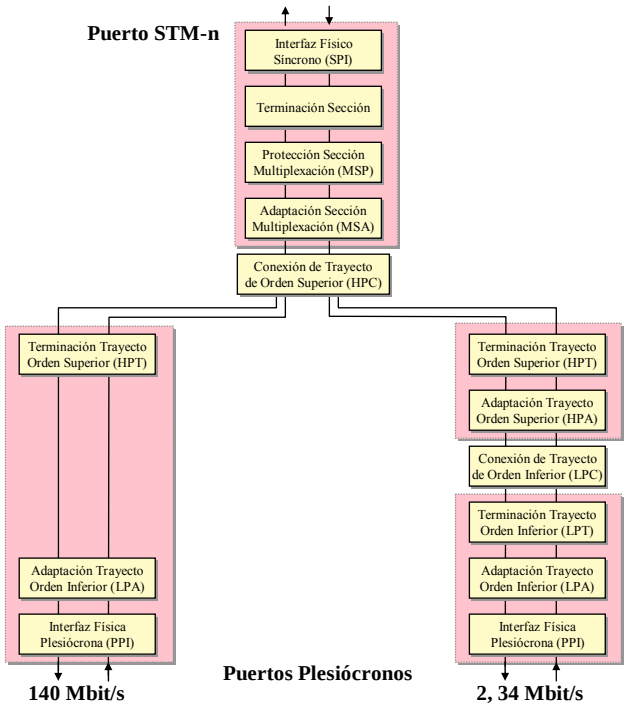

Figura 1.1.2-1 Bloques funcionales

Los bloques funcionales se pueden agrupar según la función que realizan, en:

- **Interfaces físicas**: hacen de interfaz con el medio físico de transmisión (fibra óptica, pares metálicos, frecuencias radioeléctricas),
- **Funciones de Terminación**: generan y analizan los bytes de cabecera,
- **Funciones de Adaptación**: adaptan señales, generalmente en velocidad, para su transmisión dentro de otras señales superiores. Son las funciones encargadas del tratamiento de punteros, justificaciones, etc.,
- **Funciones de Conexión**: conectan señales a la entrada con señales a la salida.

A continuación se describen cada uno de estos bloques funcionales.

1.2.1 Interfaz Física Síncrona (SPI)

Esta función proporciona la interfaz entre el medio físico de transmisión y la Terminación de Sección.

La función SPI proporciona información sobre los parámetros relacionados con el estado físico de la interfaz síncrona, tales como fallo de transmisión o transmisión degradada. Regenera la señal proveniente del medio físico y la separa en señal de reloj y datos.

La figura 1.2.1-1 muestra la estructura básica de una trama STM-N, representada como una matriz de 9xN filas y 270xN columnas, donde cada intersección es un byte (8 bits).

Los bits son transmitidos y recibidos en secuencia, comenzando por la primera fila y de izquierda a derecha. Tras la transmisión del último byte de la trama, se repite el proceso con la trama siguiente.

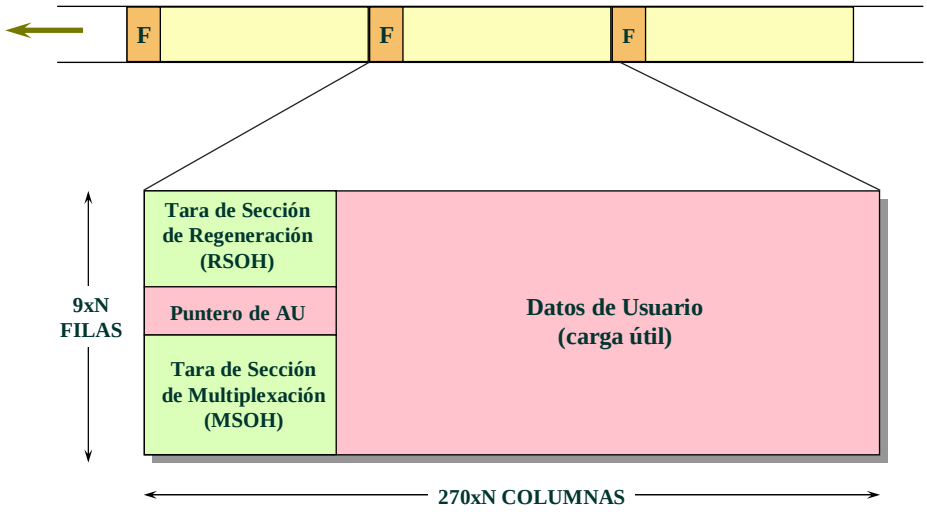

Figura 1.2.1-1 Estructura básica de una trama STM-N

1.2.2 Terminación de Sección

Bajo la denominación de Terminación de Sección agrupamos las funciones de Terminación de Sección de Regeneración (RST) y de Multiplexación (MST)

Estas funciones actúan como fuente y sumidero para la tara de Sección de Regeneración (RSOH) y Multiplexación (MSOH) respectivamente.

La figura 1.2.2-1 presenta la asignación de bytes de la tara de Sección, donde la parte por encima del puntero de AU corresponde a la Sección de Regeneración y la parte por debajo a la de Multiplexación.

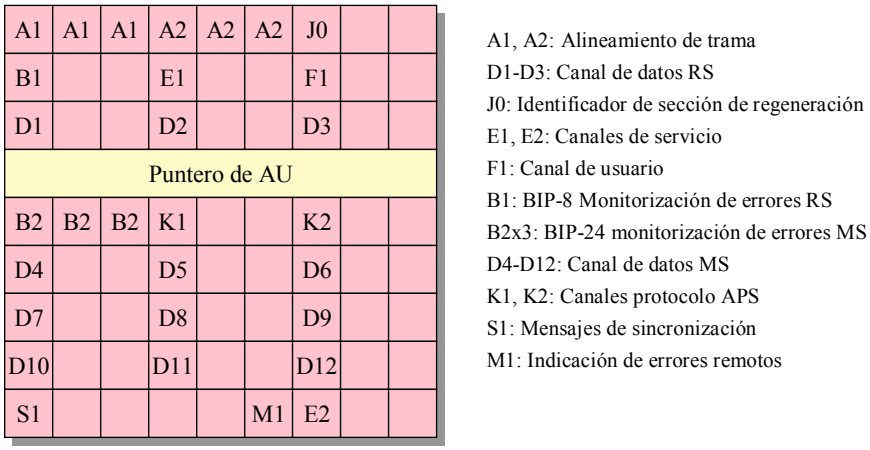

Figura 1.2.2-1 Asignación de bytes de la tara de Sección

1.2.3 Protección de Sección de Multiplexación (MSP)

La función MSP proporciona protección de la señal STM-N contra fallos en la sección de multiplexación. Las funciones, existen en ambos extremos de la sección de multiplexación, monitorizan las señales STM-N y conmutan al canal de reserva en caso de fallo.

Las dos funciones MSP se comunican entre sí por medio de los bytes K1 y K2 de la MSOH, utilizando un protocolo denominado APS (*Automatic Protection Switching*).

1.2.4 Adaptación de Sección (MSA)

Esta función permite la adaptación de trayectos de orden superior (VC-4) para su transmisión por secciones de Multiplexación. Se obtienen Capítulos Administrativas (AU-4) generando, interpretando y procesando punteros.

El puntero de AU-4 proporciona un método para permitir una alineación flexible y dinámica del VC-4 dentro de la trama STM-1. El puntero de AU-4 indica la ubicación del primer byte del VC-4 (J1), como se observa en la figura 1.2.4-1.

Si existe una diferencia de frecuencia entre la velocidad de la trama AU-4 (STM-N) y la del VC-4, el valor del puntero se incrementará o disminuirá según la necesidad.

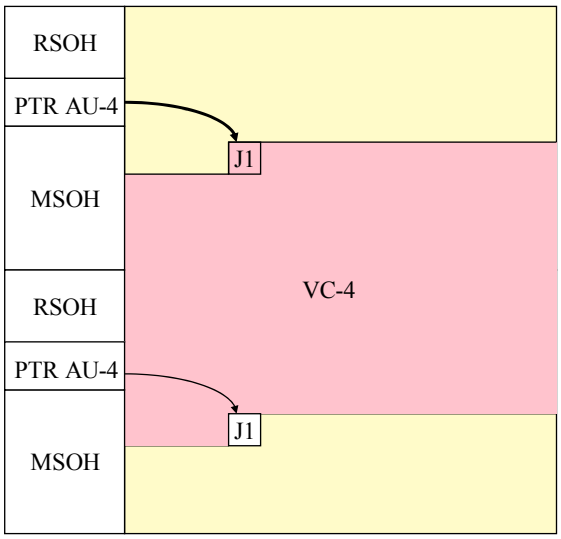

Figura 1.2.4-1 Puntero de AU-4

1.2.5 Conexión de Trayecto de Orden Superior (HOPC).

Esta función asigna VC-4 en sus puertos de entrada, a VC-4 en sus puertos de salida.

1.2.6 Terminación de Trayecto de Orden Superior (HOPT).

Esta función actúa como fuente y sumidero para la tara de trayecto de orden superior (POH).

En la figura 1.2.6-1 se muestra la asignación de bytes de la tara de trayecto de orden superior.

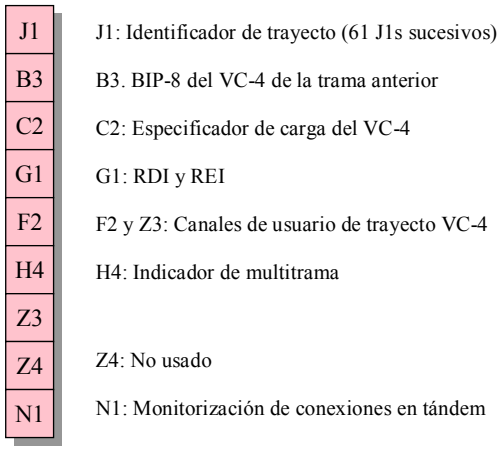

Figura 1.2.6-1 Asignación de bytes de la tara de trayecto VC-4

La figura 1.2.6-2 muestra cómo se obtiene la información de carga útil del VC-4, tras terminar cada una de las taras (Regeneración, Multiplexación y trayecto de orden superior) y procesar el puntero de AU-4

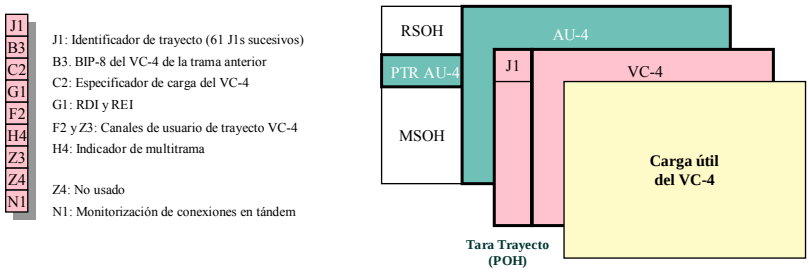

Figura 1.2.6-2 Obtención de la carga útil del VC-4

1.2.7 Adaptación de Trayecto de Orden Superior (HOPA).

Esta función permite la adaptación de trayectos de orden inferior (VC-12 y VC-3) para su transmisión por trayectos de orden superior (VC-4). Se obtienen Unidades de Tributario (TU) generando, interpretando y procesando punteros.

El puntero de TU proporciona un método para permitir una alineación flexible y dinámica del VC-12 o VC-3 dentro de la trama VC-4. El puntero de TU indica la ubicación del primer byte del VC-12 o VC-3.

Si existe una diferencia de frecuencia entre la velocidad del TU y la del VC-12 o VC-3, el valor del puntero se incrementará o disminuirá según la necesidad.

1.2.8 Conexión de Trayecto de Orden Inferior (LOPC).

Esta función asigna VC-12 o VC-3 en sus puertos de entrada, a VC-12 o VC-3 en sus puertos de salida.

1.2.9 Terminación de Trayecto de Orden Inferior (LOPT).

Esta función actúa como fuente y sumidero para la tara de trayecto de orden inferior.

1.2.10 Adaptación de Trayecto de Orden Inferior (LOPA).

Esta función opera en el puerto de acceso a una red síncrona o subred y adapta los datos para el transporte en el dominio síncrono. En el caso de datos plesiócronos, la adaptación de trayecto de orden inferior comprende la justificación de bits. La función hace corresponder las señales G.703 (2Mbit/s, 34Mbit/s, 140Mbit/s) con contenedores síncronos (C-12, C-3 y C-4).

Se han definido funciones para cada uno de los niveles existentes en la jerarquía plesiócrona. Cada una define la manera en que una señal de usuario puede

hacerse corresponder con uno de los contenedores síncronos. Existen funciones LOPA asíncronas y byte síncronas.

1.2.11 Interfaz Física Plesiócrona (PPI).

Esta función proporciona la interfaz entre la función LOPA y el medio físico que transporta una señal de tributaria.

1.3 SINCRONIZACIÓN

Los NEs de una red SDH necesitan un reloj para funcionar correctamente. Para generarlo reloj disponen de un oscilador interno. Este, por sí mismo, puede proporcionar un reloj aunque no de gran calidad, motivo por el que se utilizan referencias de sincronización externas al NE para generar una señal de reloj con mejor calidad.

Las referencias que se utilizan para sincronizar una red SDH, suelen originarse en relojes patrones de gran calidad (normalmente de cesio). Dichas referencias se irán transmitiendo a lo largo de la red, de forma que todos los NEs de la misma funcionen con el mismo reloj. La planificación de la distribución de la sincronización de una red es un aspecto importante que debe efectuarse con sumo cuidado.

1.3.1 Función de sincronización (SETS)

En la figura 1.3.1-1 se muestra la función de sincronización en un NE según se define en la recomendación G.783 de la UIT-T.

En ella se ve que la sincronización del NE o reloj del mismo, se obtiene de una de las referencias T1, T2, T3 o del oscilador interno. En realidad, el oscilador interno se va a enganchar a una de las citadas referencias o va a funcionar sin ninguna de ellas, en cuyo caso estará en oscilación libre o en modo de retención.

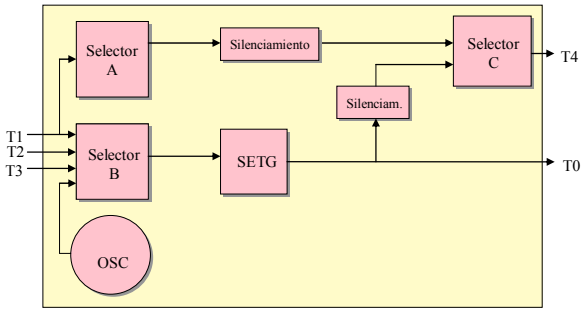

Figura 1.3.1-1 Función de sincronización

SETG (*Synchronization Equipment Timing Generator*): Es el generador de la temporización del equipo y de él se obtiene la referencia T0. Tiene tres modos de operación:

- **Enganchado** (*Locked*): El SETG está controlado por una de las referencias externas T1, T2 o T3. Es el modo normal de funcionamiento.
- **Retención** (*Hold-Over*): El SETG, durante su funcionamiento normal, es capaz de almacenar regularmente el valor de la referencia externa. Si pierde dicha referencia, será capaz de seguir funcionando algún tiempo con el valor memorizado.
- **Oscilación Libre** (*Free Running*): No es un modo de funcionamiento recomendable. Significa que las referencias externas se han perdido y el equipo no es capaz de seguir funcionando con el valor memorizado de la última referencia externa. En este caso, el SETG es controlado por el generador interno (2048 kbit/s) del equipo.

1.3.1.1 Referencias de sincronización T0,..., T4.

Según se puede ver en la figura 1.3.1-1, existen diversos tipos de referencias de sincronización. A continuación vamos a indicar brevemente su significado:

Referencias internas (entradas):

- **T1:** Representa una señal STM-N que entra al NE y que puede ser utilizada como referencia de sincronización.
- **T2:** Representa una señal de 2048 kbit/s que entra al NE y que puede ser utilizada como referencia de sincronización.
- **T3:** Representa una señal de 2048 kHz que entra al NE y que puede ser utilizada como referencia de sincronización.

Referencias externas (salidas):

- **T0:** Representa el reloj con que se está sincronizando el NE. Se origina en el oscilador interno del elemento, el cual puede estar utilizando una de las referencias T1, T2 o T3 para generar el citado reloj. Es la referencia con que se general la tramas salientes, y en ese sentido es considerada una referencia externa.
- **T4:** Representa una señal de sincronización (normalmente a 2048 kHz) que sale del NE mediante la cual pueden sincronizarse otros elementos.

En un NE podrá haber más de una señal de los tipos T1, T2 y T3.

1.3.1.2 Selectores A, B y C

Los selectores A, B y C realizan las siguientes funciones:

Selector A: Realiza la función de seleccionar entre las distintas señales de tipo T1. La señal seleccionada será la que se entregue en T4 si el selector C lo permite.

Selector B: Realiza la función de seleccionar entre las señales de tipo T1, T2 y T3 la que va a ser utilizada para generar la señal T0.

Selector C: Realiza la función de seleccionar qué señal queremos entregar en T4. Permite elegir entre las dos opciones T0=T4 y T1=T4.

1.3.1.3 Cómo se elige entre varias referencias de sincronismo

Los selectores A y B eligen entre las diferentes señales disponibles basándose en tres criterios: nivel de calidad, prioridad y comandos externos.

- **Nivel de calidad**: El NE tratará en todo momento de sincronizarse con la referencia que tenga el mejor nivel de calidad.

  Es posible que el algoritmo SSM esté deshabilitado, en cuyo caso el nivel de calidad no será tenido en cuenta.

- **Prioridad:** Si existiese más de una referencia con el mejor nivel de calidad, el NE tratará de sincronizarse con la referencia que tenga la mejor prioridad (La primera prioridad es mejor que la segunda).

  Los NE que no procesen el algoritmo SSM utilizarán el criterio de prioridad para seleccionar su referencia de sincronización.

- **Comandos externos:** Es posible, normalmente para mantenimiento, seleccionar o eliminar una determinada fuente de sincronismo.

1.3.1.4 Silenciamientos

Existen dos silenciamientos. Uno para la opción T1=T4 y otro para la T0=T4.

Cada silenciamiento funciona como un filtro en el cual se ha definido un umbral de calidad. Si la calidad de la señal que se pretende entregar en T4 no es igual o superior a la definida en el umbral, la señal T4 se cortará. Se prefiere no entregar la señal T4 a entregar una de una calidad no deseada.

1.3.2 Interfaces de sincronización

La sincronización se transporta a través de diferentes tipos de interfaces. Se pueden citar como las más frecuentes: 2048 kHz, 2048 kbit/s y STM-N.

Las interfaces STM-N y 2048 kbit/s pueden transportar una indicación del nivel de calidad de la señal de sincronización mediante los marcadores de sincronización SSM.

1.3.3 Nivel de calidad

Se han definido cuatro niveles de calidad para la sincronización de una red SDH.

- **PRC:** Transporta una señal de sincronización generada por un reloj de referencia primario PRC (*Primary Reference Clock*) según se define en la recomendación G.811.
- **SSU-T:** Transporta una señal de sincronización generada por una SSU de tránsito (*Transit Station Synchronization Unit*) según se define en la recomendación G.812.
- **SSU- L:** Transporta una señal de sincronización generada por una SSU local *(Local Station Synchronization Unit*) según se define en la recomendación G.812.
- **SEC:** Transporta una señal generada por el oscilador interno o reloj de sincronización de equipo SEC (*Synchronization Equipment Clock*) según define la recomendación G.813.

Además, se ha definido otro nivel de calidad para evitar bucles de sincronización en la red:

- **DNU:** Significa No Usar (*Do Not Use*) e indica que la señal no debe ser utilizada como referencia de sincronización. Es el nivel de calidad que envía en sentido contrario una interfaz que está siendo utilizada en ese mismo momento como fuente de sincronismo.

1.3.3.1 Orden de los niveles de calidad

El orden de los niveles de calidad se indica en la Tabla 1:

Nivel de Calidad	Orden
PRC (G.811)	Mejor
SSU-T (G.812)	
SSU-L (G.812)	
SEC (G.813 o	
DNU	Peor calidad

Tabla 1 Niveles de calidad

1.3.3.2 Los marcadores SSM. Dónde se encuentran y qué valores tienen.

Los marcadores SSM (*Synchronization Source Marker*) vienen incluidos:

- En el byte S1 (llamado SSMB) de la sección de multiplexación de las señales STM-N en sus bits 5 al 8.

- En los bits S_{ax1} a S_{ax4} (x= 4, 5, 6, 7 y 8) del intervalo de tiempo 0 (TS0) de las señales de 2048 kbit/s.

Actualmente, el algoritmo SSM es capaz de procesar cinco posibles códigos SSM:

- Código 0010. Indica que la fuente de sincronización es un PRC (G.811)
- Código 0100. Indica que la fuente de sincronización es una SSU de tránsito (G.812T)
- Código 1000. Indica que la fuente de sincronización es una SSU local (G.812L)
- Código 1011. Indica que la fuente de sincronización es un SEC (G.813 o G.81s)
- Código 1111. Indica que la fuente de sincronización que porta la señal no debe ser utilizada como referencia de sincronización al poderse producir un bucle de sincronización.

1.4 MEDIDAS DE CALIDAD

Las medidas de calidad tienen el propósito de evaluar la calidad de la transmisión, la detección de cualquier degradación en la misma y proporcionar datos relevantes al usuario.

Las medidas de la monitorización de calidad deberán poderse almacenar en forma de historia. Esa información podrá utilizarse para identificar fallos y localizar fuentes de errores intermitentes. Los datos históricos, se almacenarán en los NEs en forma de contadores de eventos. Todos los registros deberán llevar su fecha y hora.

Para cada evento y dirección de transmisión se deberán proporcionar registros de:

- 24 horas: Se acumularán los eventos de monitorización de prestaciones producidos en períodos prefijados de 24 horas.
- 15 minutos: Se acumularán los eventos de monitorización de prestaciones producidos en períodos prefijados de 15 minutos.

AL ACABAR UN PERÍODO, LOS VALORES DE LOS CONTADORES QUEDARÁN REGISTRADOS Y FECHADOS, Y POSTERIORMENTE, SERÁN PUESTOS DE NUEVO A CERO PARA COMENZAR LA CUENTA DEL SIGUIENTE PERÍODO.

Los NEs podrán almacenar un número de períodos de medida, por ejemplo 16 períodos en el caso de los registros de 15 minutos. Una vez que se exceda la máxima capacidad de almacenamiento, se descartará el registro más antiguo (*Wrapping*).

En la figura 1.4 se muestra la secuencia de recolección de un conjunto de contadores de calidad.

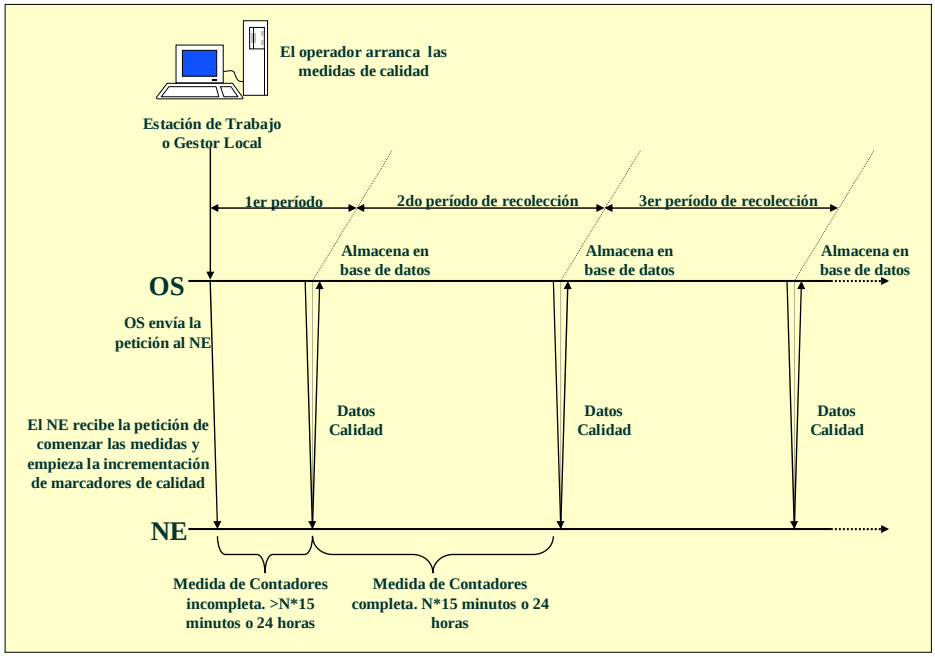

Figura 1.4 Secuencia de recolección de un conjunto de contadores de calidad

Comenzando con el proceso de arranque de las medidas de calidad o monitorización de prestaciones, y la recolección de los datos y posterior almacenado de estos en la base de datos. Esto se efectuará cada cierto tiempo (24 horas o 16*15 minutos), y después de la correspondiente petición hecha por el gestor.

1.4.1 Parámetros y eventos de monitorización de calidad

La recomendación G.826 de la UIT-T define los parámetros de monitorización de errores aplicables a redes de transporte a la velocidad primaria o superior.

Es posible, que un NE o sistema de gestión no soporte todos los eventos o parámetros.

Los **eventos** son:

- Bloque con error "*Errored Block*" (EB): Un bloque con uno o más errores de bit.
- Segundo con error "*Errored Second*" (ES): Se define como un período de un segundo con uno o más errores de bloque.
- Segundo con muchos errores "*Severely Errored Second*" (SES): Segundos con muchos errores. Es un período de un segundo que contiene al menos un 30% de bloques con error o un defecto (LOS, LOF, AIS).
- Error de bloque de fondo "*Background Block Error*" (BBE): Se define como un bloque con error que no forma parte de un SES.

Los **parámetros** son:

- Tasa de segundos con error "*Errored Second Ratio***"** (ESR): Es la relación entre los segundos con error (ER) y el número total de segundos de disponibilidad durante un intervalo fijo de medida.

- Tasa de segundos con muchos errores "*Severely Errored Second Ratio*" (SESR): Es la relación entre el número de segundos con muchos errores (SES) y el número total de segundos de disponibilidad durante un intervalo fijo de medida.

- Tasa de errores de bloque de fondo "*Background Block Error Ratio***"** (BBER): es la relación entre el número de bloques con error (EB) y el número total de bloques durante un intervalo fijo de medida, excluyendo todos los bloques durante SES y tiempo de indisponibilidad.

1.4.2 Eventos adicionales que pueden ser monitorizados

Aparte de los parámetros que deben medirse obligatoriamente, indicados en el apartado 1.4.1 de esta unidad, hay otra serie de eventos o parámetros que podrán ser medidos de forma opcional. Su implementación podrá efectuarse tanto en los períodos de 15 minutos como en los de 24 horas.

Los citados parámetros son:

- Segundo de pérdida de trama "*Out of Frame Second*" (OFS): Se define como un segundo en el cual ha habido uno o más eventos de pérdida de trama.

- Cuenta de conmutaciones de protección "*Protection Switch Count*" (PSC): Es el número de veces que se ha conmutado del canal activo al de protección.

- Duración de la conmutación de protección "*Protection Switch Duration*" (PSD): Es la duración de la protección.

- Segundo de indisponibilidad "*Unavailable Second*" (UAS): Un segundo que forma parte del período de indisponibilidad UAT.

- Cuenta de ajustes de puntero de AU4 "*AU4 Pointer Justification Count*" (PJC): Representa la cuenta de ajustes de puntero de AU4.

- Segundo consecutivo con muchos errores "*Consecutive Severely Errored Second*" (CSES): Indica una secuencia de X SES consecutivos, donde X puede ser configurado entre 2 y 9.

Si se proporcionan contadores de AU PJE, los ajustes positivos y negativos deberán poderse contar individualmente en un AU4 seleccionable de la señal STM-N.

1.4.3 La monitorización de prestaciones en el extremo remoto

La monitorización en el extremo remoto sólo está disponible en algunos tipos de NEs y en ciertas configuraciones de conexión.

El principal interés de este tipo de monitorización está en el caso de que las dos terminaciones de un trayecto estén en dominios de gestión de diferentes operadoras, pues se tendría acceso a los datos de prestaciones de ambos extremos sin necesidad de intercambiar información entre los gestores de ambas operadoras.

Los parámetros de la monitorización en el extremo remoto se basan en la medida de los bloques erróneos remotos (FEBE o REI) y en los fallos en el extremo remoto (FERF o RDI) que se transmiten en las taras de la trama SDH.

En el nodo A, la información del extremo cercano representará las prestaciones que está dando el trayecto o sección unidireccional de comienza en el nodo B y acaba en el nodo A, mientras que la información del extremo remoto representa las prestaciones que está dando la sección o trayecto que comienza en el nodo A y acaba en el nodo B. En el nodo B la situación será la misma pero desde el otro punto de vista.

Los parámetros de medida de calidad del extremo cercano obtenidos en el nodo A serán iguales a los parámetros de medida de calidad remotos obtenidos en el nodo B, y viceversa.

1.4.4 Los umbrales de calidad

Los umbrales de calidad son una serie de valores que se configuran para los diferentes contadores de calidad. Si los valores de esos contadores alcanzan o exceden los umbrales fijados, se generará una notificación de cruce de umbral.

Los umbrales pueden configurarse en el NE mediante el gestor. El gestor permitirá consultar y configurar los umbrales tanto para las medidas de 15 minutos como para las de 24 horas.

Para más detalles sobre los umbrales de calidad, se pueden consultar las recomendaciones M.20, M.2100 y M.2120 de la UIT-T.

1.4.5 La recolección de los datos de monitorización de prestaciones

Los valores de los contadores de calidad se irán almacenando en el NE. El gestor podrá recolectar esos datos para su posterior análisis.

La recolección se efectuará, normalmente de forma periódica, a partir de una petición del gestor y mediante la interfaz existente entre el gestor y el NE.

El procedimiento de recolección y el análisis que se haga de los datos dependerá del gestor de que se trate.

Resumen

Hemos recordado la **estructura de multiplexación** de la SDH a nivel europeo, viendo especialmente la estructura de los C-12, C-3 y C-4.

La funcionalidad de un equipo múltiplex SDH puede dividirse **en bloques funcionales**. Los bloques se pueden agrupar según la función que realizan en:

- Interfaces físicas: Hacen de interfaz con el medio físico de transmisión.
- Funciones de terminación: Generan y analizan los bytes de cabecera.
- Funciones de adaptación: Se encargan del tratamiento de los punteros.
- Funciones de conexión: Conectan señales de entrada con las de salida.

Se pasó revista al a **función de sincronización** de un equipo SDH. Se definieron las **referencias de sincronización** T0, T1, T2, T3 y T4. Con el reloj T0 se generan todas las señales salientes del equipo.

Hay tres **modos del generador de temporización** (SETG): enganchado, retención y oscilación libre.

Existen diferentes **criterios de selección de referencias de sincronización**. El primero será la calidad (si no está deshabilitado el algoritmo SSM) y el segundo es la prioridad.

La **calidad** de la sincronización viene codificada en el byte S1 de las señales STM-N. Las calidades, de mejor a peor son: G.811, G.812T, G.812L, G.813, No usar.

Las medidas de **monitorización de prestaciones** o de calidad evalúan la calidad de la transmisión, detectando degradaciones y proporcionando datos relevantes al usuario.

Se deben proporcionar **registros de 15 minutos y 24 horas**. En ellos se registran eventos y parámetros mediante conjuntos de contadores de calidad.

Los **eventos y parámetros más habituales** son: EB, ES, SES, BBE, ESR, SESR y BBER. Puede haber muchos más dependiendo de cada aplicación el que se midan o no.

Se podrán poner **umbrales de calidad** en el NE. Éste enviará notificaciones al gestor si sus valores se exceden sus valores.

El gestor realizará la **recolección de los valores de los contadores** de forma periódica. El NE almacenará los datos de calidad durante un cierto tiempo hasta que le sean pedidos por el gestor.

Ejercicios de Autoevaluación

Ejercicio 1

¿Qué es un AU4?

a. Una señal STM-1 a la que se le ha quitado la tara de sección de multiplexación.

b. Un contenedor virtual VC4 al que se le ha añadido la tara de trayecto.

c. Un contenedor C4 al que se le ha añadido la tara de trayecto y el puntero de AU.

d. Un contenedor virtual VC4 al que se le ha añadido el puntero de AU.

Ejercicio 2

¿Qué caracteriza a los bloques funcionales de terminación?

a. Son los bloques donde se pone o quita el puntero de AU.

b. Son los bloques donde pone o se quita la tara de la sección de multiplexación.

c. Son los bloques donde se termina la señal, accediendo a la señal demultiplexada.

d. Ninguna de las respuestas es totalmente correcta.

Ejercicio 3

¿Cómo se llama el reloj con que se generan las señales salientes de un NE?

a. T0

b. T1

c. T3

d. T4

Ejercicio 4

¿Qué se entiende por un error de bloque de fondo (BBE)?

a. Es un bloque con uno o más errores de bit, que no forma parte de un SES.

b. Es un bloque con uno o más errores de bit de fondo.

c. Es un bloque con uno o más errores de bit, que no forma parte de un período de indisponibilidad.

d. Ninguna respuesta es totalmente correcta.

SOLUCIONES A LOS EJERCICIOS

1.c y d, 2.d, 3.a, 4.a

CAPÍTULO 2

Arquitectura de la Red de Transporte SDH

Las diversas funciones que constituyen una red de telecomunicación pueden clasificarse en dos amplios grupos funcionales. Uno de ellos es el grupo funcional de transporte, que transfiere información de telecomunicación de uno a otro u otros puntos. El segundo es el grupo funcional de control, que ejecuta diversos servicios y operaciones auxiliares así como funciones de mantenimiento. Esta unidad se refiere al grupo funcional de transporte.

ESQUEMA DE CONTENIDO

2.1 COMPONENTES DE ARQUITECTURA

Se ha analizado la red de transporte para identificar una funcionalidad genérica que sea independiente de la tecnología de la implementación. Esto ha proporcionado un método para describir la funcionalidad de la red de manera abstracta, empleando un número reducido de componentes de arquitectura. Tales componentes se definen mediante la función que ejecutan en términos de tratamiento de la información o empleando las relaciones que describen entre otros componentes de arquitectura.

Los componentes de arquitectura están asociados conjuntamente de formas específicas, constituyendo los elementos de red a partir de los cuales se construyen las redes reales. Los puntos en los que se vinculan las entradas y salidas de las funciones de tratamiento y las entidades de transporte, son los puntos de referencia de la arquitectura de red de transporte.

2.1.1 Arquitectura de Red

Una red de transporte transfiere información de usuario desde un punto a otro u otros puntos de forma bidireccional o unidireccional. Una red de transporte puede también transferir diversas clases de información de control de red, tales como la señalización e información de operaciones y mantenimiento, tanto para el grupo funcional de control como para su propia utilización.

Como la red de transporte es una red extensa y compleja, con diversos componentes, es esencial para su diseño y gestión la elaboración de un modelo de red apropiado con entidades funcionales bien definidas. La red de transporte puede describirse definiendo las asociaciones existentes entre los puntos de la red. A fin de simplificar la descripción, se utiliza un modelo de red de transporte basado en los conceptos de estratificación y subdivisión dentro de cada capa, de una forma que permita un elevado grado de recurrencia.

2.1.2 Componentes topológicos

Los componentes topológicos proporcionan la descripción más abstracta de una red en términos de relaciones topológicas entre conjuntos de puntos de referencia similares.

Se distinguen tres componentes topológicos que son: la red de capa, la subred y el enlace. Utilizando únicamente estos componentes, es posible describir totalmente la topología lógica de una red.

a) Red de capa

Una red de capa es el conjunto completo de **puntos de acceso** similares, que pueden estar asociados a efectos de transferencia de información. La información transferida es característica de la capa y se denomina *información característica*.

En una red de capa pueden constituirse y deshacerse asociaciones de puntos de acceso, mediante un proceso de gestión de capa que modifica de esta forma su conectividad.

Una red de capa está constituida por subredes y enlaces entre ellas.

b) Subred

Una subred es el conjunto completo de **puntos de conexión** similares, que pueden asociarse a efectos de transferencia de información característica. En una subred, pueden constituirse y deshacerse asociaciones de puntos de conexión mediante un proceso de gestión de capa que modifica de esta forma su conectividad.

Generalmente, las subredes están constituidas por más pequeñas y enlaces entre ellas. El nivel mínimo de esta recurrencia, es la matriz de conexión contenida en un elemento de red individual.

c) Enlace

Un enlace es el sub-conjunto de **puntos de conexión** de una subred, que están asociados con un sub-conjunto de puntos de conexión de otra subred, a efectos de transferencia de información característica entre subredes.

El proceso de gestión de la red **no** puede constituir ni deshacer el conjunto de asociaciones de puntos de conexión que definen el enlace.

El enlace representa la relación topológica entre un par de subredes. Se utiliza, en general, para describir la asociación que existe entre los puntos de conexión contenidos en un determinado elemento de red y los de otro elemento de red. El nivel mínimo de recurrencia de un enlace (en el concepto de estratificación) representa los medios de transmisión.

La figura 2.1.2-1 representa la topología de una red de capa en términos de interconexión de puntos de acceso mediante subredes y enlaces.

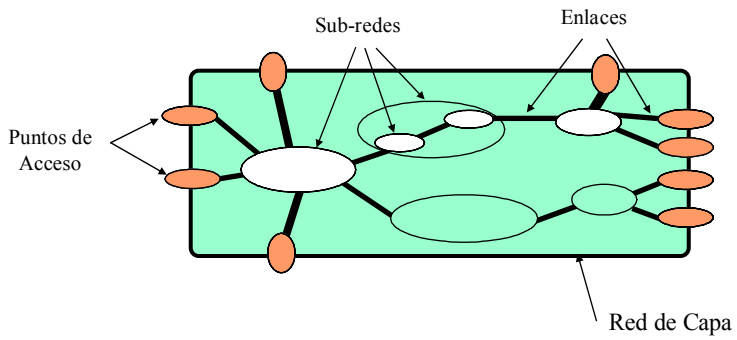

Figura 2.1.2-1 Red de capa

2.1.3 Entidades de transporte

Las entidades de transporte proporcionan la transferencia de información transparente entre puntos de referencia de una red de capa. Es decir, no existe modificación de la información entre la entrada y la salida salvo la resultante de las degradaciones del proceso de transferencia.

Se distinguen dos entidades básicas, según que se supervise o no la integridad de la información transferida, a los que se denomina entidades conexiones y caminos. Las conexiones se dividen en conexiones de red, conexiones de subred y conexiones de enlace, de acuerdo con el componente topológico al que pertenezcan.

Conexión de red

Una conexión de red es capaz de transferir información de forma transparente a través de una red de capa. Está delimitada por puntos de terminación de conexión (TCP). Constituye el nivel de abstracción más elevado dentro de una capa y puede subdividirse en una concatenación de conexiones de subred y conexiones de enlace.

No existe información acerca de la integridad de la información transferida, pero a menudo puede deducirse de otras fuentes información relativa a la integridad de la propia conexión.

d) Conexión de subred

Una conexión de subred es capaz de transferir información de forma transparente a través de una subred. Está delimitada por puntos de conexión en la frontera de la subred y representa la asociación entre puntos de conexión.

Las conexiones de subred están constituidas, en general, por una concatenación de conexiones de subred de nivel inferior y conexiones de enlace. El nivel más bajo de esta recurrencia, es decir, la conexión de matriz, representa una transconexión de una matriz individual en un elemento de red.

e) Conexión de enlace

Una conexión de enlace es capaz de transferir información de forma transparente a través de un enlace entre dos subredes. Está delimitada por puntos de conexión en la frontera del enlace y las subredes y representa la asociación entre tal pareja de puntos de conexión, como se observa en la figura 2.1.3-1. Las conexiones de enlace se establecen mediante caminos en la red de capa servidora.

Figura 2.1.3-1 Conexión de enlace

f) Camino

Se denomina camino a la transferencia de información característica entre puntos de acceso. Es decir, se trata, por tanto, de la asociación entre puntos de acceso junto con la información adicional relativa a la integridad de la transferencia de información. Un camino se forma a partir de una conexión de red, incluyendo funciones de terminación de camino entre los TCP y los puntos de acceso, como se observa en la figura 2.1.3-2.

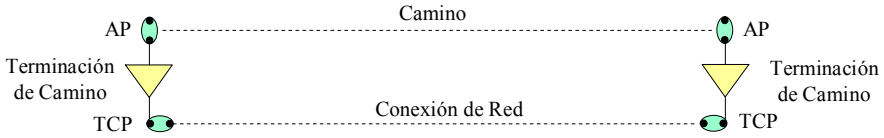

Figura 2.1.3-2 Camino

2.1.4 Funciones de tratamiento de transporte

En la descripción de la arquitectura de las redes de capa se distinguen dos funciones genéricas de tratamiento: la de adaptación y la de terminación. Intervienen conjuntamente en las fronteras de capa y se definen por el tratamiento de la información efectuado entre sus entradas y sus salidas.

Función de adaptación

La función de adaptación adapta la información característica de una red capa cliente, a una forma adecuada para su transporte por la red de capa servidora. La función de adaptación específica depende de la información característica de las dos capas.

Como ejemplos de funciones de adaptación intercapas pueden citarse la codificación, la modificación de la velocidad, la alineación, la justificación, y la multiplexación. Ejemplos de funciones de adaptación en la SDH, son los bloques funcionales de adaptación de trayecto de orden inferior (LOPA), de orden superior (HOPA) y de sección de multiplexación (MSA).

g) Función de terminación de camino

Las funciones de terminación de camino suministran información relacionada con la transferencia de información en un camino. Esto se consigue, por lo general, insertando información adicional en una función fuente de terminación de camino que se supervisa en la función sumidero correspondiente.

Ejemplos de funciones de terminación de camino en la SDH, son los bloques funcionales de terminación de trayecto de orden inferior (LOPT), de orden superior (HOPT) y de sección de multiplexación (MST).

h) Puntos de referencia

Se forman puntos de referencia en la red de capa vinculando la entrada de una función de tratamiento de transporte o entidad de transporte con la salida de otra. Existen tres tipos de puntos de referencia: puntos de acceso (AP), puntos de conexión (CP) y puntos de terminación de conexión (TCP).

En la figura 2.1.4-1 se muestra la representación gráfica de las funciones de adaptación, terminación y puntos de referencia.

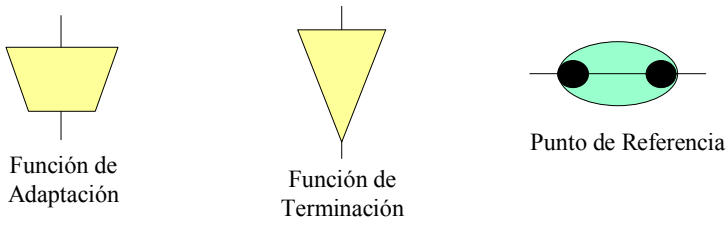

Figura 2.1.4-1 Representación gráfica

En la figura 2.1.4-2 se muestra un ejemplo de modelo funcional que ilustra la utilización de algunos componentes de arquitectura vistos anteriormente.

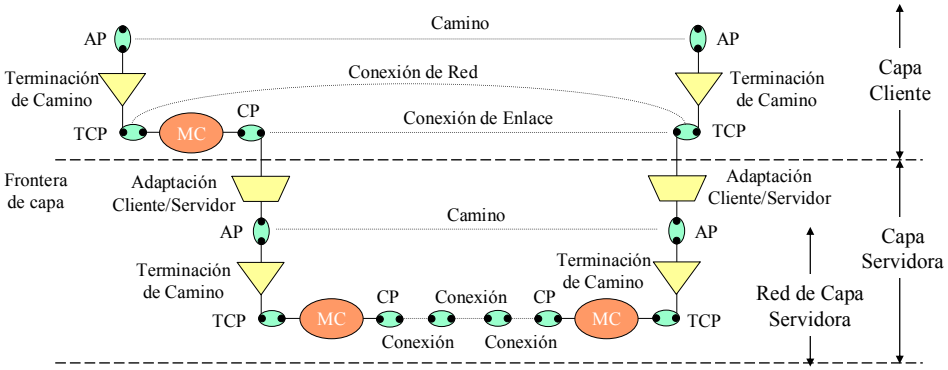

Figura 2.1.4-2 Ejemplo de modelo funcional

2.2 SUBDIVISIÓN Y ESTRATIFICACIÓN

Una red de transporte puede descomponerse en cierto número de capas de red de transporte independientes con una asociación cliente/servidor entre capas adyacentes. Cada red de capa puede subdividirse separadamente de manera que refleje la estructura interna de esa capa. Los conceptos de subdivisión y estratificación son, por tanto, ortogonales, como se indica en la figura 2.1.4-1.

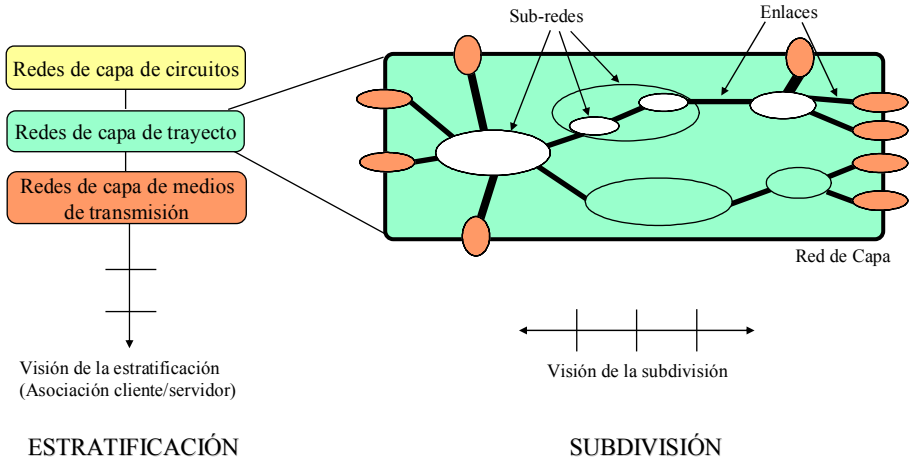

Figura 2.1.4-1 Subdivisión y estratificación

2.2.1 Importancia del concepto de subdivisión

El concepto de subdivisión es importante puesto que nos permite definir:

la estructura de la red dentro de una capa de red;

fronteras administrativas entre operadores de red que proporcionan conjuntamente trayectos de extremo a extremo dentro de una sola capa;

fronteras de dominio dentro de la red de capa de un mismo operador, para el establecimiento de objetivos de calidad de funcionamiento de los subsistemas que componen la red;

fronteras de dominio de encaminamiento independiente, relativas al funcionamiento del proceso de gestión del trayecto.

2.2.2 Importancia del concepto de estratificación

El concepto de estratificación de la red de transporte se basa en las siguientes hipótesis:

- cada red de capa puede clasificarse en base a funciones similares;

- es más sencillo diseñar y operar cada capa por separado que efectuar el diseño y la operación de la red de transporte completa como una sola entidad;
- puede ser útil un modelo de red estratificado para definir los objetos gestionados en la red de gestión de las telecomunicaciones (TMN), como se verá en próximas capítulos;
- cada red de capa puede poseer sus propias capacidades de operaciones y mantenimiento, tales como las funciones de conmutación de seguridad y restablecimiento automático en caso de fallo, protección frente a anomalías de funcionamiento, fallos o errores de utilización. Estas capacidades reducen al mínimo las intervenciones de operación y mantenimiento, sin repercusiones sobre las otras capas;
- es posible agregar o modificar una capa sin que esto afecte a otras capas desde el punto de vista de la arquitectura;
- cada red de capa puede definirse independientemente de las otras capas.

2.3 CONCEPTO DE SUBDIVISIÓN

El concepto de subdivisión puede dividirse en dos subconceptos conexos: la subdivisión de subredes, que describe la **topología**, y la subdivisión de conexiones de red, que describe la **conectividad**.

2.3.1 Subdivisión de subredes

Una subred describe simplemente la capacidad para asociar cierto número de puntos de conexión o de TCP. No describe directamente la topología de los componentes de arquitectura utilizados para constituir la subred. En general, cualquier subred puede subdividirse en un cierto número de subredes más pequeñas, interconectadas mediante enlaces. La forma según la cual se enlazan entre sí las subredes más pequeñas y los enlaces, describe la topología de la subred. Esto puede formularse como sigue:

Subred □ Subredes menores □ enlaces □ topología.

Así pues, utilizando el concepto de subdivisión, es posible descomponer de forma recurrente cualquier red de capa hasta revelar el nivel de detalle deseado. Es probable que este nivel de detalle corresponda a los equipos individuales que implementan matrices de conexión en los elementos de red individuales, lo que confiere a la red de capa, la capacidad de conexión flexible.

2.3.2 Subdivisión de las conexiones de red y conexiones de subred

Un camino es una entidad de transporte formada por la vinculación de terminaciones de camino con una conexión de red, como se indica en la figura

2.1.4-2 y constituye un caso particular de la capacidad de una red de capa. La conexión de red es un caso particular de la capacidad de la subred más amplia definible dentro de la red de capa. Del mismo modo que es posible subdividir una subred, también lo es efectuar la subdivisión de una conexión de red, como se observa en la figura 2.3.2-1.

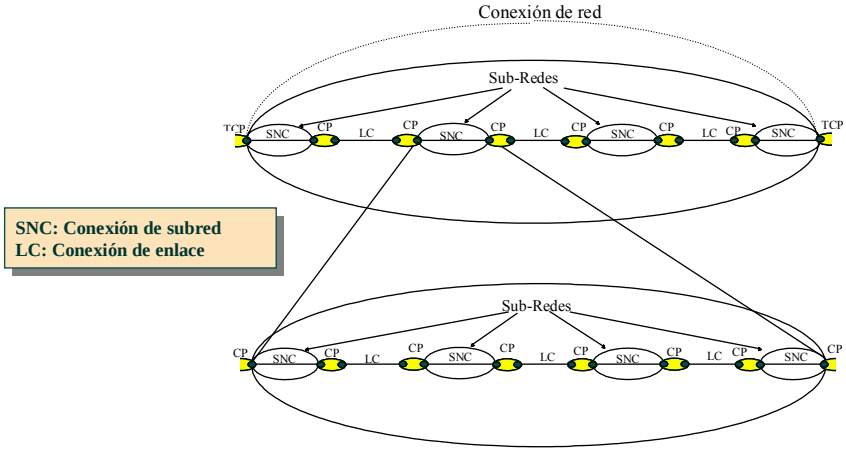

Figura 2.3.2-1 Subdivisión de una conexión de red en conexiones de subred

En general, una conexión de red puede subdividirse por combinación secuencial de conexiones de subred y conexiones de enlace, como sigue:

Conexión de red = TCP + conexiones de subred + conexiones de enlace TCP.

Cada una de las conexiones de subred pueden dividirse, en una combinación secuencial de conexiones de subred y conexiones de enlace, según el esquema siguiente:

Conexión de subred = punto de conexión + conexiones de subred más pequeñas + conexiones de enlace + punto de conexión.

2.4 CONCEPTO DE ESTRATIFICACIÓN

La asociación cliente/servidor entre redes de capa adyacentes es aquélla en la que un camino de la red de capa servidora proporciona una conexión de enlace de la red de capa cliente, como se observa en la figura 2.1.4-2.

Se introduce el concepto de adaptación para permitir, que redes de capa con una estructura de información característica diferente, se soporten entre sí por la relación cliente/servidor.

Desde el punto de vista funcional de la red de transporte, la función de adaptación está situada, por consiguiente, entre los planos de redes de capa, como se observa en la figura 2.3.2-1. Sin embargo, se considera que, desde el punto de vista administrativo, la función pertenece al camino de la capa servidora al que está vinculada.

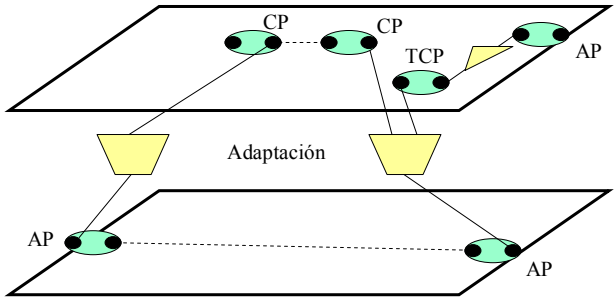

Figura 2.3.2-1 Asociación entre redes de capa

2.4.1 Capas de la red de transporte

En la figura 2.4.1-1 se representa el modelo estratificado de la red de transporte. Las características del modelo son las siguientes:

- se distinguen tres clases de redes de capa: redes de capa de circuito, redes de capa de trayecto y redes de capa de medios de transmisión;
- la asociación entre dos capas adyacentes cualesquiera es una asociación de tipo servidor/cliente;
- cada capa tiene su propia capacidad de operaciones y mantenimiento.

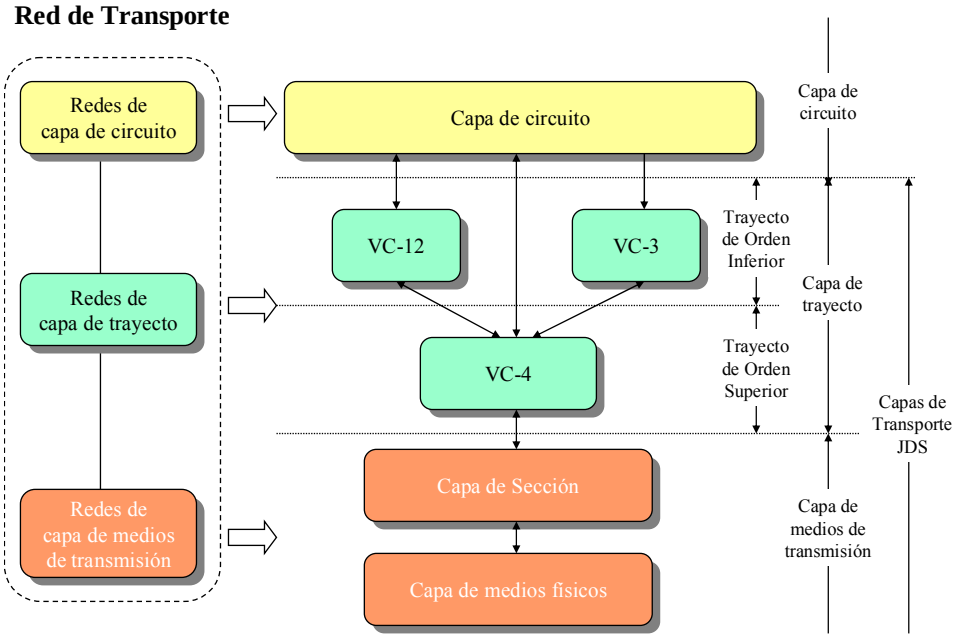

Figura 2.4.1-1 Capas de la red de transporte

Estas tres clases de redes de capa se describen como sigue:

- **Redes de capa de circuito**: Proporcionan a los usuarios servicios de telecomunicación tales como servicios con conmutación de circuitos, servicios con conmutación de paquetes y servicios por líneas arrendadas. Pueden identificarse redes de capa de circuito distintas, según los servicios proporcionados. Estas redes son independientes de las redes de capa de trayecto;

- **Redes de capa de trayecto.** Utilizadas para soportar diferentes tipos de redes de capa de circuito. En el caso de la SDH, hay dos redes de capa de trayecto: la red de capa de trayecto de orden inferior (LOP) y la red de capa de trayecto de orden superior (HOP).

  La red de capa de trayecto de orden inferior es la encargada de transportar flujos de usuario de 2Mbit/s, en contenedores virtuales VC-12, y de 34Mbit/s (y para alguna aplicación específica también de 45Mbit/s), en contenedores virtuales VC-3. Esta red de capa utiliza los servicios de transporte de los VC-4 de la red de capa de trayecto de orden superior.

  La red de capa de trayecto de orden superior proporciona servicios de transporte tanto a la capa de trayecto de orden inferior (transportando VC-12 y VC-3) como a la capa de circuitos (transportando flujos de usuario de 140Mbit/s).

  Un aspecto básico de las redes SDH es la posibilidad de controlar la gestión de la conectividad en las redes de capa de trayecto. Las redes de capa de trayecto son independientes de las redes de capa de medios de transmisión;

- **Redes de capa de medios de transmisión.** Dependen del medio de transmisión, que puede ser por ejemplo, la fibra óptica y los sistemas radioeléctricos. Las redes de capa de medios de transmisión se dividen en redes de capa de sección y redes de capa de medios físicos. Las redes de capa de sección abarcan todas las funciones que proporcionan la transferencia de información entre dos nodos, en tanto que las redes de capa de medios físicos se refieren a los medios reales de fibra, pares metálicos o canales de frecuencias radioeléctricas que soportan una red de capa de sección.

  En el caso de la SDH, hay dos redes de capa de sección:.

  - La red de capa de sección de multiplexación, que es responsable de la transferencia de la información de extremo a extremo, entre ubicaciones que encaminan o terminan trayectos,

  - La red de capa de sección de regeneración, que es responsable de la transferencia de información entre regeneradores individuales y entre regeneradores y ubicaciones que encaminan o terminan trayectos.

2.5 APLICACIÓN DE LOS CONCEPTOS A LA SDH

2.5.1 Circuitos plesiócronos soportados en capas de SDH

En la 2.5.1-1 se muestra el caso en que la SDH soporta señales plesiócronas. Se han representado cuatro capas de red:

capa de circuitos plesiócronos;

capa de trayecto de orden inferior (por ejemplo VC-12),

capa de trayecto de orden superior (VC-4),

capa de sección de STM-N.

En la figura 2.5.1-1 se muestra un circuito cliente que atraviesa cuatro elementos de red SDH. Los dos elementos extremos poseen tributarios a velocidades plesiócronas y son encargados de la adaptación del circuito para su transporte por la red SDH. Los elementos centrales realizan conexiones de trayecto de orden inferior (izquierda) y de trayecto de orden superior (derecha). Todas las interfaces (salvo los afluentes a las velocidades binarias plesiócronas), utilizan la capa de sección de STM-N.

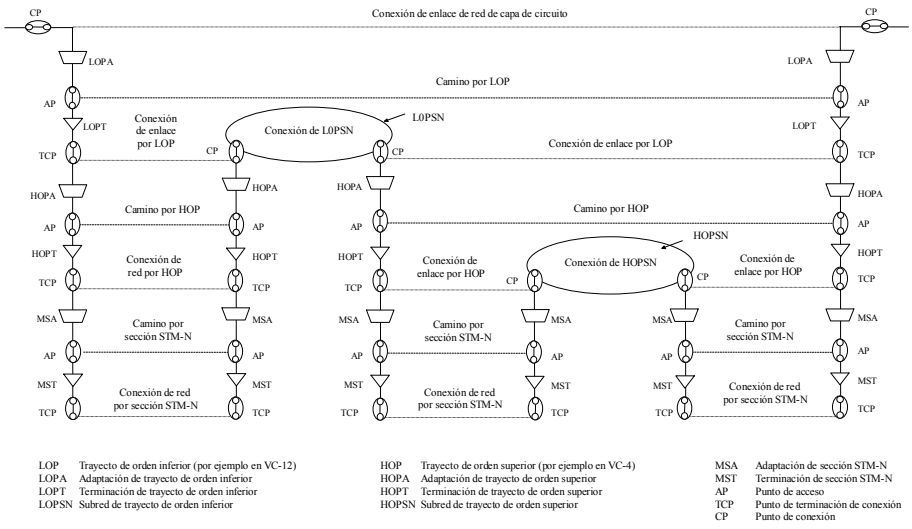

Figura 2.5.1-1 Aplicación a la SDH

Resumen

Una red de transporte puede descomponerse en cierto número de capas de red de transporte independientes con una asociación cliente/servidor entre capas adyacentes. Cada red de capa puede subdividirse separadamente de manera que refleje la estructura interna de esa capa.

La red de transporte SDH puede modelarse mediante tres redes de capa:

- ***Redes de capa de circuito****: Proporcionan a los usuarios servicios de telecomunicación tales como servicios con conmutación de circuitos, servicios con conmutación de paquetes y servicios por líneas arrendadas.*

- ***Redes de capa de trayecto.*** *Utilizadas para soportar diferentes tipos de redes de capa de circuito. En el caso de la SDH, hay dos redes de capa de trayecto: la red de capa de trayecto de orden inferior (LOP) y la red de capa de trayecto de orden superior (HOP).*

- ***Redes de capa de medios de transmisión.*** *Dependen del medio de transmisión, que puede ser por ejemplo, la fibra óptica y los sistemas radioeléctricos. Las redes de capa de medios de transmisión se dividen en redes de capa de sección y redes de capa de medios físicos. Las redes de capa de sección abarcan todas las funciones que proporcionan la transferencia de información entre dos nodos, en tanto que las redes de capa de medios físicos se refieren a los medios reales de fibra, pares metálicos o canales de frecuencias radioeléctricas que soportan una red de capa de sección.*

Ejercicios de Autoevaluación

Ejercicio 1

Una red de capa, es:

a. El conjunto completo de puntos de acceso similares.

b. El conjunto completo de puntos de conexión similares.

c. El subconjunto de puntos de acceso asociados con puntos de conexión.

Ejercicio 2

Una conexión de subred, es una entidad de transporte que proporciona la transferencia de información transparente entre:

a. Puntos de Terminación de Conexión.

b. Puntos de Conexión o entre Puntos de Terminación de Conexión y Puntos de Conexión.

c. Puntos de Acceso.

Ejercicio 3

La Red de Transporte SDH se puede representar mediante las redes de capa de:

a. Trayecto y de Medios de Transmisión.

b. Trayecto de Orden Superior y de Trayecto de Orden Superior.

c. Trayecto y de Sección.

SOLUCIONES A LOS EJERCICIOS

1.a, 2.b, 3.a

CAPÍTULO 3

Protecciones

En esta unidad repasaremos los principios generales de protección, que nos permitirán mejorar la disponibilidad de la Red de Transporte. Nos centraremos en los dos esquemas de protección más utilizados en la SDH, como son la protección de camino y la de subred.

ESQUEMA DE CONTENIDO

3.1 PRINCIPIOS GENERALES

La mejora de la disponibilidad de una Red de Transporte se puede alcanzar reemplazando las entidades de transporte degradadas o en fallo. El reemplazo se inicia, normalmente, por la detección de un defecto, una degradación de la calidad o un comando externo proveniente del Sistema de Gestión.

Se pueden utilizar dos estrategias diferentes: protección y restauración:

- La estrategia de protección utiliza capacidad preasignada para reemplazar entidades de transporte degradadas o en fallo.
- La estrategia de restauración utiliza cualquier capacidad disponible entre nodos para encontrar una entidad que se pueda utilizar para reemplazar a la que tiene el fallo. La restauración se basa en un algoritmo de reenrutamiento y requiere la intervención de un Sistema de Gestión.

La estrategia de restauración queda fuera del objetivo de la presente unidad.

3.1.1 Arquitectura de protección

La arquitectura de protección depende de la asignación de entidades de protección a entidades de trabajo.

- Arquitectura 1+1. Se utiliza una entidad de protección para proteger una entidad de transporte. El tráfico se transmite siempre sobre las entidades de trabajo y protección.
- Arquitectura 1:1. Se utiliza una entidad de protección para proteger una entidad de transporte. La entidad de protección puede utilizarse para transportar tráfico de baja prioridad cuando no se utiliza para protección.
- Arquitectura M:N. Se utilizan M entidades de protección para proteger N entidades de transporte. Las entidades de protección pueden utilizarse para transportar tráfico de baja prioridad cuando no se utilizan para protección.

Las arquitecturas de protección 1+1 y 1:1 se denominan de *protección dedicada*, puesto que a cada entidad de trabajo le corresponde una entidad de protección. Las arquitecturas de protección M:N se denominan de *protección compartida*, puesto que las entidades de trabajo comparten una o más entidades de protección.

3.1.2 Tipos de conmutación

El tipo de conmutación describe dónde se realiza la conmutación de protección en caso de fallo unidireccional como se observa en la figura 3.1.2-1.

- ***single-ended***. En caso de fallo unidireccional se conmuta a la entidad de protección, únicamente la dirección afectada.

- ***dual-ended***. Se conmuta a la entidad de protección ambas direcciones, incluso en caso de fallo unidireccional.

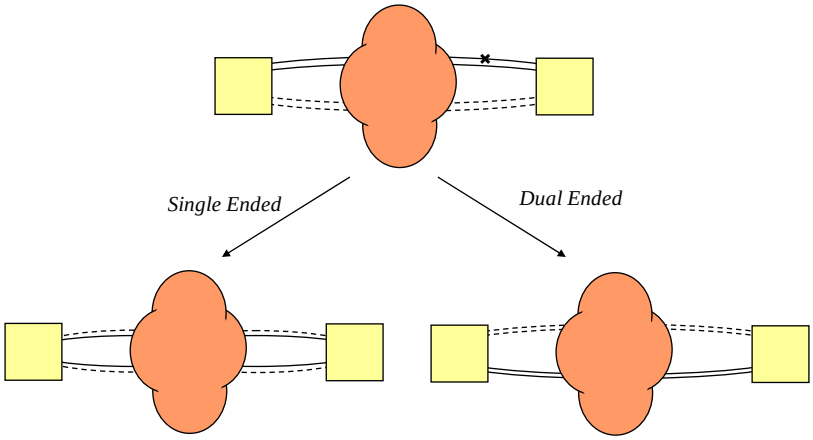

Figura 3.1.2-1 Tipos de conmutación

Las ventajas de la protección *single-ended*, son que es más simple de implementar y no requiere un protocolo, por lo que es más rápida.

Las ventajas de la protección *dual-ended*, son su facilidad de gestión, puesto que las dos direcciones utilizan los mismos recursos físicos, por lo que se mantiene un retardo parejo. Además, tiene la posibilidad de transportar tráfico de baja prioridad.

3.1.2.1 Modo de operación

El modo de operación describe el comportamiento del esquema de protección cuando desaparece el fallo.

- ***Modo reversible.*** Después de la desaparición del fallo, el tráfico se restaura a la entidad de trabajo original.

- ***Modo no reversible.*** Después de la desaparición del fallo, el tráfico no se restaura a la entidad de trabajo original, permaneciendo en la entidad de protección.

3.1.3 Criterio de iniciación de conmutación

La acción de conmutación puede iniciarse bien de forma automática, después de la detección de un fallo o una degradación, o bien por la recepción de un comando externo.

3.1.4 Tiempo de conmutación

El tiempo de conmutación es el intervalo desde la decisión de conmutación hasta la finalización de la operación de conmutación. No se incluye el tiempo necesario para detectar el fallo o la degradación, ni el *tiempo de espera*.

3.1.5 Tiempo de espera para proteger (hold-off)

El tiempo de espera para proteger, es el retardo entre la declaración de fallo o de degradación y el comienzo de la conmutación de protección. Es útil coordinar las acciones de protección en el caso de interfuncionamiento de esquemas de protección y/o restauración.

3.1.6 Tiempo de espera para revertir (WTR, Wait To Restore)

El tiempo de espera WTR, es el retardo desde el momento en que desaparece el defecto que provoca la conmutación de protección hasta que se revierte a la entidad de trabajo.

3.2 ESQUEMAS DE PROTECCIÓN DE CAMINO

En una protección de camino, un camino de trabajo se reemplaza por un camino de protección cuando se ve afectado por un fallo o degradación. El fallo o degradación se detecta por las funciones de terminación de camino, y la conmutación de protección la realiza una matriz de protección, localizada en la subcapa de protección de camino.

Se contemplan dos tipos, dependiendo de la capa donde se localiza la protección de camino:

- Protección de Camino de Sección de Multiplexación (Protección MS-Trail),
- Protección de Camino de Orden Superior (Protección HO-Trail).

La protección MS-Trail proporciona protección extremo a extremo de los MS-Trails, por medio de una subcapa de protección de MS-Trail. La función de terminación de camino, en la capa MS, se expande para formar la subcapa de protección.

En los esquemas de protección MS-Trail, la detección de eventos de fallo la realiza la FUNCIÓN de Terminación de Sección de Multiplexación (MST) y la reconfiguración resultante utiliza las funciones de Protección de Sección de Multiplexación (MSP), localizadas en la subcapa de protección de MS. Esta reconfiguración puede involucrar conmutación de protección en varios NEs. La coordinación de la conmutación en múltiples NEs se realiza por medio de un protocolo de conmutación de protección automática (APS).

Se contemplan dos esquemas de protección MS-Trail:

- Protección MS Lineal,
- Anillos de protección compartida MS.

La protección HO-Trail proporciona protección extremo a extremo de los trayectos de Orden Superior, por medio de una subcapa de protección de HO-Trail. La función de terminación de camino, en la capa HOP, se expande para formar la subcapa de protección.

En los esquemas de protección HO-Trail, la detección de eventos de fallo la realiza la función de Terminación de Trayecto de Orden Superior (HOPT) y la reconfiguración resultante utiliza la matriz de protección, localizadas en la subcapa de protección. Esta reconfiguración puede involucrar conmutación de protección en varios NEs. La coordinación de la conmutación en múltiples NEs se realiza por medio de un protocolo de conmutación de protección automática (APS).

3.2.1 Protección MS Lineal

Se contempla un esquema de protección lineal, tal y como se describe en [ITU-T G.803], MS-lineal 1+1. La arquitectura de protección de Sección de Multiplexación lineal 1+1 se caracteriza por tener dos secciones de Multiplexación con rutas físicas diferentes, como se observa en la figura 3.2.1-1.

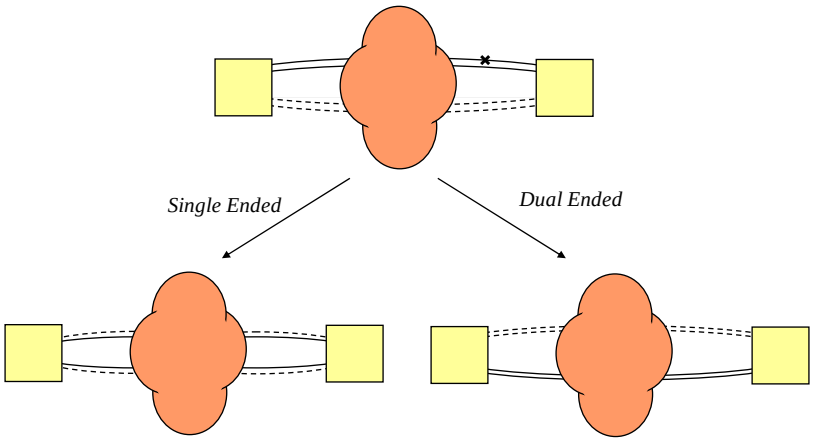

Figura 3.2.1-1 Protección MS Lineal

El tráfico se transmite permanentemente sobre la sección de principal y la de protección. El tipo de conmutación puede ser single-ended o dual-ended y el modo de operación puede ser reversible o no reversible.

Para realizar la conmutación de protección, los dos nodos se comunican mediante un canal APS transportado por los bytes K1 y K2 de la Tara de Sección de Multiplexación.

La conmutación de protección se realiza dentro de la capa de Sección de Multiplexación:

- La detección de fallos la realiza la función de terminación de Sección de Multiplexación,
- La conmutación de protección la realizan las funciones de protección de Sección de Multiplexación de los dos nodos.

Cualquier acción de protección viene dirigida por la detección o desaparición de un fallo o por un comando externo.

El tiempo de conmutación de protección debe ser menor que 50 ms.

3.2.2 Anillos de protección compartida (MS-SPRing)

En un anillo de protección compartida, la capacidad de transporte de una Sección de Multiplexación se divide en capacidad de trabajo y capacidad de protección. Los canales de trabajo transportan el servicio a ser protegido, mientras que los canales de protección se reservan para protección del servicio.

El mecanismo de protección de Sección de Multiplexación compartida se basa en:

- Detección de fallos por un nodo del enlace con fallo,
- Conmutación de protección automática realizada por los dos nodos del enlace con fallo.

La conmutación de protección se realiza dentro de la capa de Sección de Multiplexación:

- La detección de fallos la realiza la función de terminación de Sección de Multiplexación,
- La conmutación de protección la realizan las funciones de protección de Sección de Multiplexación de los dos nodos.

Únicamente se contemplan los anillos de protección compartida de dos fibras. En estos anillos el mecanismo de protección permite recuperar todo el tráfico en caso de un fallo simple en la capa de Sección de Multiplexación. La conmutación de protección viene dirigida por la detección de fallo de señal o señal degradada, detectada por la función de terminación de MS o por un comando externo.

Este tipo de esquema de protección tiene una arquitectura de protección 1:N. La conmutación de protección es *dual-ended*, con modo de operación reversible. Cuando los canales de protección no se utilizan para proteger los canales de trabajo, pueden utilizarse para transportar tráfico de baja prioridad. Si es necesario, se utilizan los canales de protección para proteger los canales de trabajo, cortando el tráfico de baja prioridad.

Para realizar la conmutación de protección, los dos nodos se comunican mediante un canal APS transportado por los bytes K1 y K2 de la Tara de Sección de Multiplexación. El tiempo de conmutación de protección debe ser menor que 50 ms.

Cuando sucede una conmutación de protección, los canales de trabajo que se transmitían hacia el enlace cortado, se conmutan a los canales de protección hacia la dirección opuesta. El tráfico puenteado viaja alrededor del anillo, por los canales de protección, hasta el nodo opuesto al enlace con fallo, donde los canales de protección son conmutados, de nuevo, al los canales de trabajo. Este funcionamiento se observa en la figura 3.2.2-1.

Dependiendo del patrón de tráfico que cursa el anillo con protección MS-SPRing, es posible transportar más o menos tráfico protegido. En la figura 3.2.2-2 se observa que, en el caso en que todo el tráfico sea entre nodos adyacentes, es posible transportar un máximo de 32 AU-4. En el extremo contrario, si todo el tráfico se dirige hacia un único nodo sumidero es posible transportar 16 AU-4 protegidas. Este último caso iguala a la máxima capacidad de tráfico protegido, que es capaz de transportar un anillo SNC.

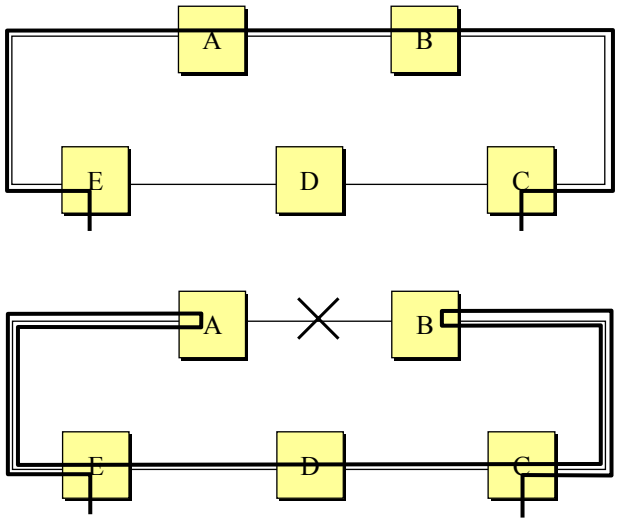

Figura 3.2.2-1 Funcionamiento de la protección MS-SPRing

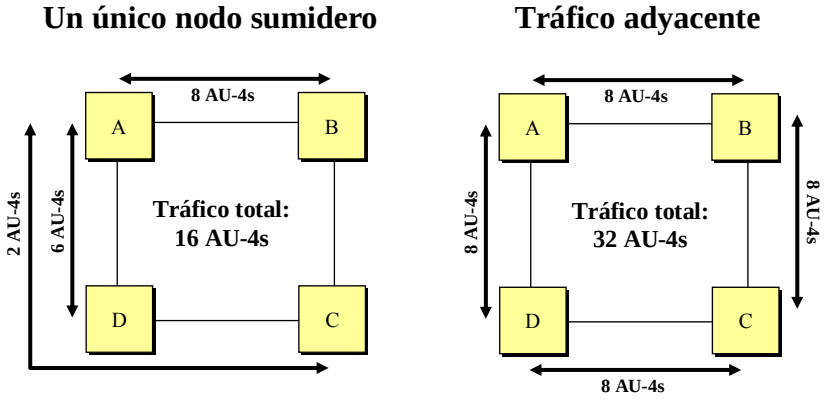

Figura 3.2.2-2 Efectos de los patrones de tráfico

3.2.3 Protección de HO-Trail

Este esquema de protección es un mecanismo de protección de la capa de trayecto basado en la monitorización de la información de tara de trayecto y puede utilizarse para proteger un camino a través de la red SDH. Se trata de un esquema de protección dedicada extremo-extremo que puede utilizarse sobre cualquier estructura física, por ejemplo mallas, anillos y redes mixtas.

La conmutación de protección se realiza dentro de la capa de trayecto de orden superior:

- La detección de fallos la realiza la función de terminación de Trayecto de Orden Superior,
- La conmutación de protección la realizan las funciones de protección de Trayecto de Orden Superior.

La arquitectura de protección es del tipo 1:1. El tipo de conmutación de protección contemplado single-ended, con modo de operación reversible y no reversible.

El tiempo de conmutación de protección debe ser menor que 50 ms.

El tiempo de espera, hold-off, debe poderse configurar entre 0 y 10s en pasos de 100ms.

La conmutación de protección viene dirigida por la detección de fallo de señal o señal degradada, detectada por la función de terminación de Trayecto de orden Superior o por un comando externo.

3.3 ESQUEMA DE PROTECCIÓN DE CONEXIÓN DE SUBRED

Como vimos en anteriores capítulos, se define una conexión de subred (SNC) como una entidad de transporte formada por una conexión a través de una subred entre puntos de conexión (CPs). Una conexión de red (NC) está formada por una serie de conexiones entre puntos de terminación de conexión (TCPs).

La protección de conexión de subred (SNCP) es un mecanismo de protección dedicado que consiste en reemplazar una conexión de subred de trabajo con una conexión de subred de protección cuando la primera falla o su calidad cae por debajo del nivel requerido.

La protección de conexión de subred puede utilizarse sobre cualquier estructura física, es decir, redes malladas, anillos o redes mixtas.

Los esquemas de protección SNCP pueden caracterizarse por el método de monitorización utilizado como criterio de conmutación:

- Monitorización inherente: Se utiliza la información derivada de la capa servidora,

- Monitorización no intrusiva: La conexión de subred se monitoriza empleando una función de terminación de camino.

3.3.1 Protección SNCP

La arquitectura de protección es del tipo 1:1. El tipo de conmutación de protección contemplado es *sigle-ended*, con modo de operación reversible y no reversible.

El tiempo de conmutación de protección debe ser menor que 50 ms. El tiempo de espera, hold-off, debe poderse configurar entre 0 y 10s en pasos de 100ms. La conmutación de protección viene dirigida por la detección de fallo o por un comando externo.

El criterio de conmutación automática es diferente dependiendo del tipo de monitorización:

- SNC inherente (SNCP/I):

  Defecto de Fallo de Señal Servidora. Este defecto aparece por defectos detectados en las capas servidoras, por ejemplo, LOP o SIA.

- SNC no intrusiva (SNCP/N):

  - Defecto de Fallo de Señal Servidora. Este defecto aparece por defectos detectados en las capas servidoras, por ejemplo, LOP o SIA.
  - Defecto de trayecto desequipado,
  - Defecto de discordancia de identificador de trayecto,
  - Defecto de error excesivo de trayecto,
  - Defecto de trayecto degradado.

La figura 3.3.1-1 muestra un nodo utilizando protección 1+1 uniforme. La parte superior ilustra el caso en que opera bajo condiciones normales. Se transmite simultáneamente por las conexiones de subred de trabajo y de protección. En recepción se utiliza un conmutador para seleccionar la conexión de subred de trabajo. La parte inferior ilustra el caso en que existe un fallo en la conexión de subred de trabajo. En este caso, el receptor detecta el fallo y conmuta a la conexión de subred de protección.

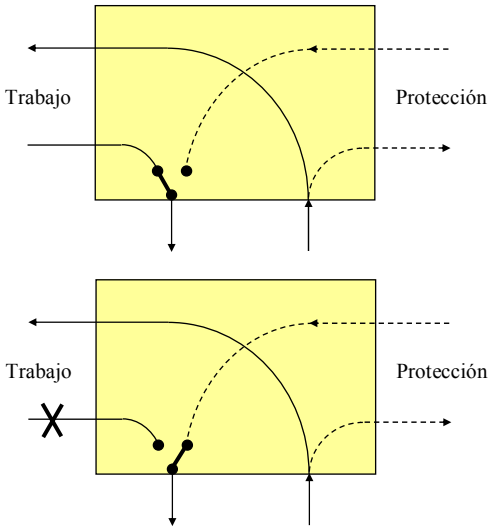

Figura 3.3.1-1 Protección SNC

3.3.2 Protección Drop&Continue

La protección Drop&Continue es un modo adicional de protección que mejora significativamente la disponibilidad de las conexiones de subred, en base a añadir conexiones de servicio en la unión entre anillos, como se observa en la figura 3.3.2-1.

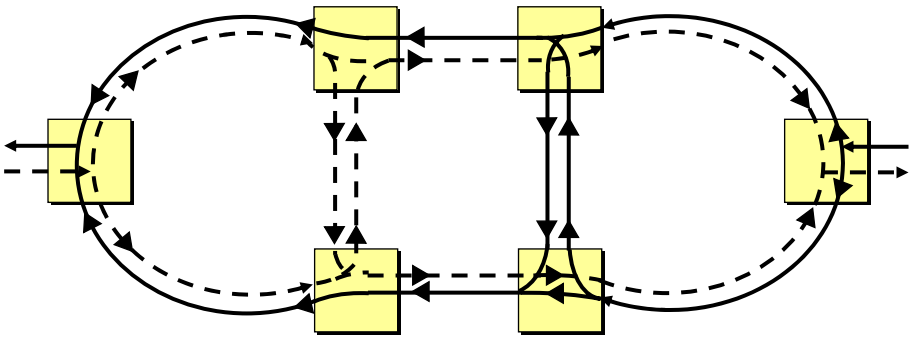

Figura 3.3.2-1 Protección Drop&Continue

En una conexión de subred protegida SNC, dos cortes en dos anillos diferentes puede causar la indisponibilidad de la misma. Sin embargo, utilizando la protección Drop&Continue, la conexión de subred no se ve afectada, como se indica en la figura 3.3.2-2.

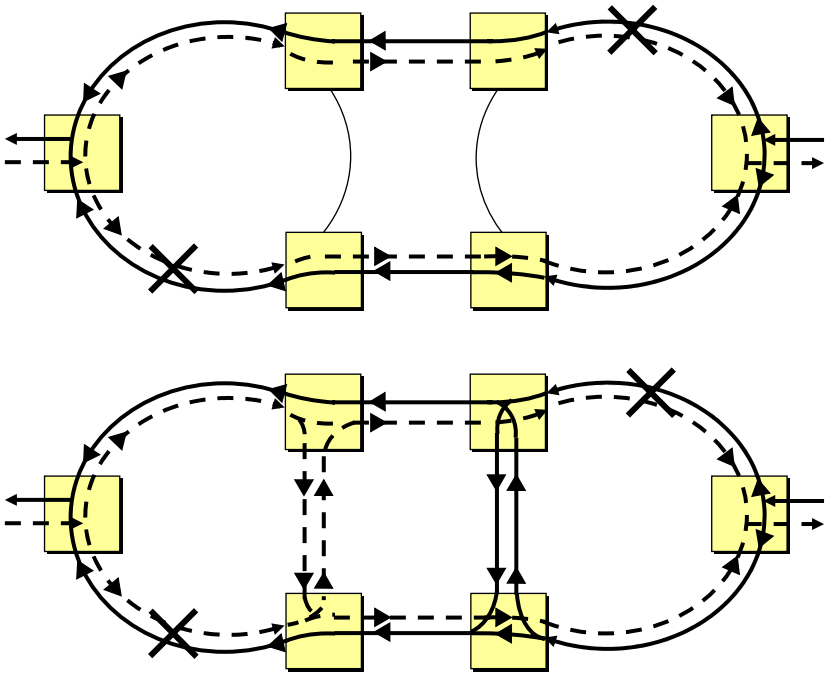

Figura 3.3.2-2 Protección SNC y Drop&Continue

La Figura *3.3.2-3* muestra una comparación de protecciones de conexión de subred.

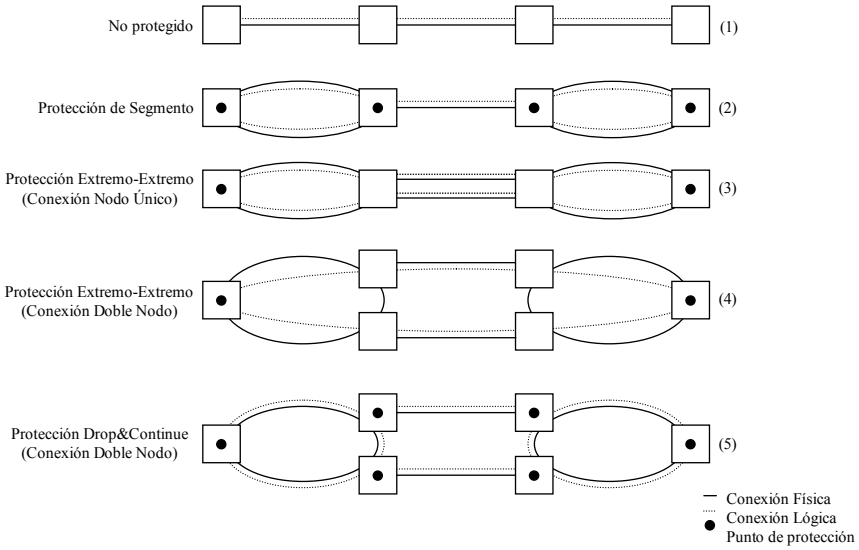

Figura 3.3.2-3 Tipos de Protección de conexión de subred

Resumen

En esta unidad hemos repasado los principios generales de protección que nos permitirán mejorar la disponibilidad de la red de transporte.

Los conceptos básicos, son:

- ***Arquitectura de protección***,
- ***Tipo de conmutación***,
- ***Modo de operación***,
- ***Tiempos de conmutación***.

Hemos visto los diferentes esquemas de protección de camino:

- ***Protección MS Lineal***,
- ***Protección MS-SPRing***.

Pro último, hemos visto los diferentes esquemas de subred:

- ***Protección SNC***,
- ***Protección Drop&Continue***.

Ejercicios de Autoevaluación

Ejercicio 4

El tiempo *Wait to Restore* (WTR), es:

a. Retardo desde el momento en que desaparece el defecto hasta que se revierte a la entidad de trabajo.

b. Retardo desde el momento en que desaparece el defecto hasta que se revierte a la entidad de protección.

c. Retardo entre la declaración de fallo y el comienzo de la conmutación de protección.

Ejercicio 5

En anillos de protección compartida, la conmutación es del tipo:

a. Dual-ended.

b. Single-ended.

c. Reversible.

Ejercicio 6

En una protección SNC/I, se conmuta por :

a. Fallo de Señal Servidora.

b. Pérdida de Señal.

c. SIA o Pérdida de señal.

SOLUCIONES A LOS EJERCICIOS

1.a, 2.a, 3.a

CAPÍTULO 4

Gestión de Redes de Telecomunicación

El objetivo de esta unidad es el de ofrecer una visión amplia y detallada de la evolución de las redes de telecomunicaciones y cómo esta evolución tiene una implicación inmediata sobre su gestión.

Se presentarán a continuación las soluciones más extendidas en la gestión de redes, así como sus principales campos de aplicación. La mayoría de los conceptos que se explican en esta unidad son adoptados por los organismos internacionales de estandarización, y son aplicados en su mayoría por los operadores de red y proveedores de servicio.

ESQUEMA DE CONTENIDO

4.1 EL ESTÁNDAR TMN DE GESTIÓN DE REDES DE TELECOMUNICACIÓN

En la presente unidad se introducirá un modelo de gestión de red, conocido por ***Red de Gestión de Telecomunicaciones***, a partir de ahora ***TMN (Telecomunication Management Network).*** Esta solución de gestión surge como la aplicación de la solución aportada por ISO[1] a las redes de telecomunicación. En su descripción, introduciremos la evolución del estándar, para posteriormente describir los conceptos genéricos definidos por las recomendaciones TMN.

4.1.1 Antecedentes

Los primeros trabajos que se desarrollaron en la estandarización de la gestión de redes se llevaron a cabo en el SG-IV (*Study Group IV)* del ITU-T, en el período de 1985 a 1988. Trataban de definir y desarrollar un sistema de interfaces de gestión para redes y equipos de telecomunicaciones públicos. El primer resultado importante de este trabajo fue la recomendación M.30 que fue publicada en el libro azul de 1989.

El concepto básico subyacente a una Red de Gestión de Telecomunicaciones, más conocida como red TMN, era proporcionar una arquitectura organizada a fin de conseguir la interconexión entre diversos tipos de Sistemas de Operación (SO) y/o equipos de telecomunicaciones para el intercambio de información de gestión. Esta arquitectura está basada en la definición de unos protocolos e interfaces estándares.

En el siguiente período de estudio (1989 a 1992) la Rec. M.30 identifica claramente la gestión de sistemas OSI como la base sobre la que construir el estándar TMN. Esta recomendación pasó a numerarse M.3010. De esta manera, los servicios y protocolos de gestión de sistemas OSI (Recs. de la serie X.700), representan actualmente un subconjunto de las capacidades de gestión que pueden ser proporcionadas por TMN.

4.1.2 TMN: Principios y Arquitectura.

Finalmente, la IUT-T en sus recomendaciones de gestión TMN (Recs. de la serie M.3000) establece todas las soluciones para la explotación del servicio de Telecomunicación, cubriendo su ciclo de vida completo, desde la planificación a la administración del mismo, pasando por las fases de provisión, instalación, mantenimiento y operación.

La Red de Gestión de Telecomunicaciones soporta una gran variedad de funciones de aplicación que cubren todas las tareas de gestión de una red de

[1] ISO *(International Organization for Standarizacion)* define un estándar de gestión para la arquitectura OSI *(Open System Interconection).* Estos conceptos de gestión ISO serán introducidos en el siguiente apartado.

telecomunicaciones. La red de gestión que se defina puede variar en tamaño, desde una simple conexión entre un sistema de gestión y un simple elemento de red, hasta grandes redes que interconecten muchos tipos diferentes de sistemas y elementos de red.

En la figura 4.1.2-1 se representa la relación general existente entre una red de gestión TMN y la red de telecomunicaciones que gestiona.

TMN es fundamentalmente una red propia que se comunica con la red de telecomunicaciones en diferentes puntos para recibir información de la misma y controlar su funcionamiento. Se puede implementar de muy diversas maneras y puede usar parte de la red que gestiona para sus comunicaciones. Es por ello necesario que la arquitectura de la red de gestión TMN ofrezca una alto grado de flexibilidad con el fin de poder adaptarse a cualquier topología de red e implementar tanto estándares abiertos como la adaptación a aplicaciones comerciales de gestión de red.

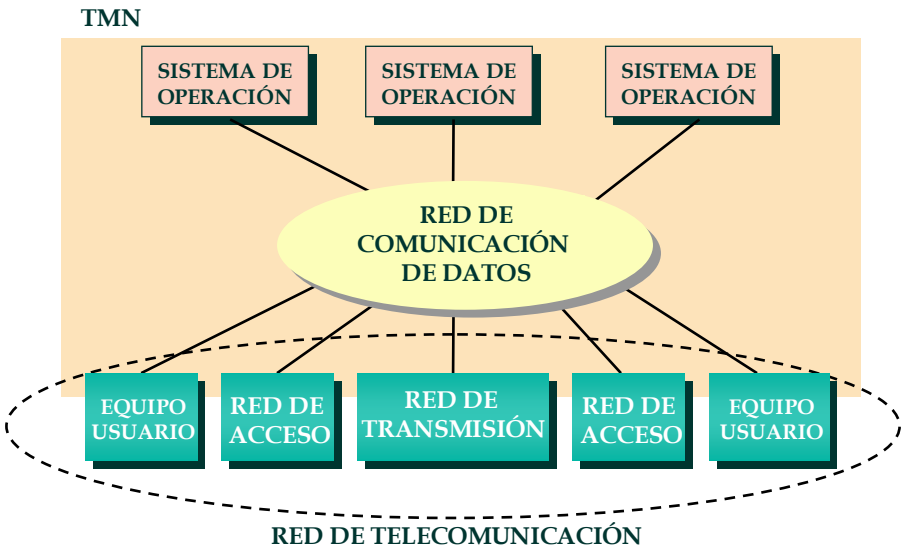

Figura 4.1.2-1 Relación TMN - Red de Telecomunicaciones

El objetivo que busca el estándar TMN es definir una arquitectura de gestión que sea válida para cualquier red. Para ello es imprescindible fijar un modelo genérico de red, de manera que su visión sea independiente de la tecnología concreta. Este concepto es posible gracias a modelos de información que representen los recursos de cualquier red, y de unas interfaces normalizadas que nos definan el intercambio de información de gestión entre los elementos de red y los sistemas de gestión.

De forma genérica, por lo tanto, la arquitectura TMN consiste en un cierto número de Sistemas de Operación que intercambian información de gestión entre ellos y los propios elementos que componen la red. Para dicho intercambio se definen las interfaces de gestión, incluyendo en esta definición el modelo de información que represente la red, como las funciones que soportarán dichas interfaces.

Se pueden gestionar, basándose en el estándar TMN, la gran mayoría de los servicios de telecomunicaciones y tipos de equipos que componen las redes de telecomunicaciones. Destacan los siguientes:

- Redes públicas y privadas, incluidas la RDSI (red digital de servicios integrados), redes móviles, redes privadas virtuales, redes privadas de voz y redes inteligentes.
- La propia Red de Gestión de Telecomunicaciones: permite la gestión de la propia red encargada de transferir los datos de gestión de la red de telecomunicaciones.
- Terminales de transmisión (multiplexores, equipos de modulación de canal, jerarquía digital síncrona, etc.).
- Sistemas de transmisión tanto digitales como analógicos.
- Redes de área amplia, metropolitana y local.
- Redes de conmutación de circuitos y paquetes, utilizando los protocolos de comunicación estándares, X.25.
- Terminales y sistemas de señalización.
- Servicios portadores y teleservicios.
- Centralitas privadas, accesos a centralitas privadas y terminales de usuario.
- Soporte lógico proporcionado por (o asociado a) servicios de telecomunicaciones, como por ejemplo de conmutación, directorio, bases de datos de mensajes, etc.

La red de gestión TMN ha sido concebida para soportar una gran diversidad de áreas de gestión, que abarcan la planificación, instalación, operaciones, administración, mantenimiento y la puesta en marcha y prestación de los servicio de redes de telecomunicación.

La especificación y el desarrollo de la funcionalidad de las aplicaciones requeridas para soportar las áreas de gestión anteriormente citadas no están recogidos en las Rec. M.3000 del estándar TMN, por lo que se deberán definir localmente. No obstante, el ITU-T proporciona algunas ideas al respecto, clasificando para ello la gestión en cinco áreas de funciones de gestión. Estas áreas proporcionan un marco que permite determinar las aplicaciones apropiadas de modo que sea posible atender a las necesidades comerciales de las entidades que explotan la red a gestionar. Hasta la fecha, han sido identificadas las cinco áreas funcionales de gestión siguientes:

- **Gestión de la calidad o funcionamiento**,
- **Gestión de fallos**,
- **Gestión de la configuración**,

- **Gestión de la contabilidad**,
- **Gestión de la seguridad**.

Parte de la información intercambiada en la red de gestión podrá ser usada como soporte de más de una área funcional de gestión.

Para la definición de una interfaz en el entorno TMN, se define una metodología [ITU-T M.3120, 92] que se basa en recoger los servicios de gestión y sus componentes (generalmente reutilizables para otras definiciones), [ITU-T M.3200, 92]. A partir de los servicios, se definen las funciones necesarias para su implementación [ITU-T M.3400, 92], que a su vez, harán uso de los recursos de la red, representados por clases de objetos gestionados [ITU-T M.3100 1, 92]. En la figura 4.1.2-2 se resumen las principales recomendaciones del estándar TMN.

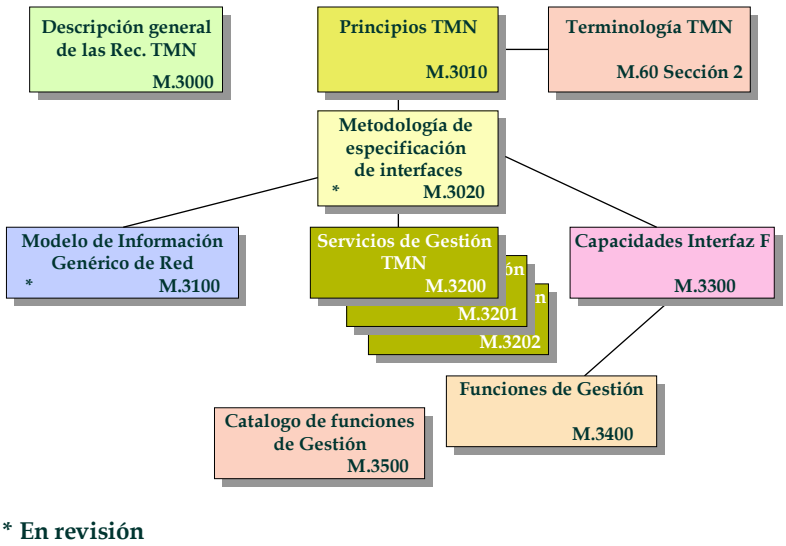

Figura 4.1.2-2 Recomendaciones de la ITU-T. Series M

Dentro de la arquitectura TMN general se pueden considerar por separado, al planificar y diseñar una interfaz en una red de gestión basada en TMN, tres aspectos básicos de la arquitectura:

i) Arquitectura Física

Describe interfaces realizables de componentes físicos que integran la red de gestión TMN. La arquitectura física representa los elementos reales de la red.

j) Arquitectura Funcional

Entre las interfaces definidas en la arquitectura física deberá intercambiarse información de gestión. La información que se intercambie entre unos y otros equipos de gestión depende del reparto apropiado de funcionalidad dentro de la red de gestión. Estas funciones se organizan en forma de bloques de gestión. La definición de bloques de función y puntos

de referencia entre bloques de función, da origen a los requisitos funcionales aplicables a la definición de una interfaz TMN.

k) Arquitectura de Información

La arquitectura de información, basada en un planteamiento orientado a objetos, proporciona el fundamento de aplicación de los principios de gestión de sistemas de interconexión de sistemas abiertos [OSI, 92] a los principios TMN. Este concepto lo veremos más extensamente en el siguiente apartado, *Gestión OSI*. De esta manera, se establece una correspondencia entre los principios de gestión de sistemas OSI y los principios TMN, y posteriormente se expandirán los primeros para adecuarlos al entorno TMN cuando sea necesario.

Una vez introducidos los conceptos que define TMN, definiremos los conceptos que permiten la representación lógica de los recursos físicos de la red a gestionar. A partir de esta arquitectura física, definiremos posteriormente los componentes funcionales y de información que complementan la arquitectura física.

4.1.3 Arquitectura Física

4.1.3.1 Bloques constitutivos de la arquitectura física

La arquitectura física se puede descomponer en bloques. Estos bloques agrupan recursos físicos y pueden identificarse según las funciones que realicen en la red. En la figura 4.1.3-1 aparecen representados tanto los bloques físicos como las interfaces entre ellos, caracterizados por la implementación de los puntos de referencia.

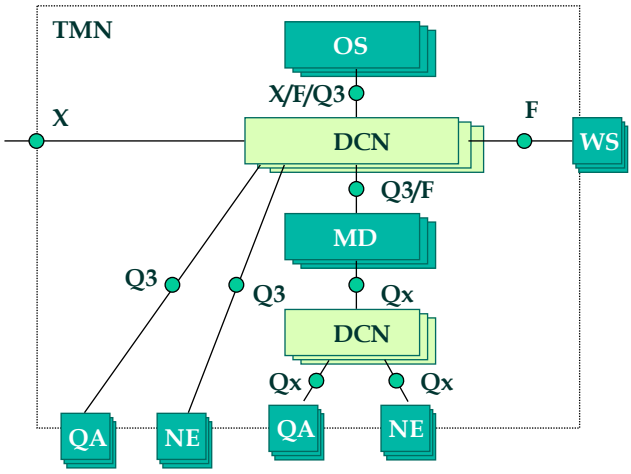

Figura 4.1.3-1 Arquitectura física

Las recomendaciones de la serie M de la ITU-T no indican la forma de implementar o distribuir la funcionalidad en distintos bloques físicos. En la

descripción de los bloques físicos incluiremos las posibles funciones que pueden ser implementadas para la gestión TMN. Los bloques son los siguientes:

Sistema de Operación (OS)

Representa los sistemas de gestión propiamente dichos, es decir, las aplicaciones que toman el rol de gestores y agentes. La principal función de este bloque es proporcionar la ***función de sistema de operación (OSF).*** Mediante esta función se supervisa, coordina y controla todas las funciones de telecomunicación, incluidas las funciones de gestión propiamente dichas. Opcionalmente, también puede proporcionar ***funciones de mediación (MF), adaptación Q (QAF) y de presentación (WSF).***

l) Dispositivo de Mediación (MD).

Sistema intermedio entre la red de comunicación de datos de la arquitectura de gestión y los gestores o agentes, cuya principal misión es proporcionar la función de **mediación (MF)**. La función de mediación actúa sobre la información que pasa entre un bloque de sistema de operación (gestor o agente), y los bloques que representan elementos de red. Mediante esta función se asegura que la información sea presentada de manera entendible por ambos sistemas. Los dispositivos de mediación podrán almacenar, filtrar, adaptar, establecer controles y condensar información de gestión. Opcionalmente pueden **proporcionar funciones de operación (*OSF*), de adaptación (*QAF*) y de presentación (WSF**). El bloque de mediación puede estar constituido por una cadena de sistemas.

m)Adaptador Q (QA)

Mediante este dispositivo seremos capaces de conectar elementos de red (NE) o sistemas de operación (OS) con interfaces que no sean compatibles con las definidas para la TMN (puntos de referencia M). Las funciones de adaptación se implementan físicamente en las interfaces Qx o Q_3, como se puede ver en la figura 4.1.3-1.

n) Red de Comunicación de Datos (DCN)

Es la red de comunicaciones que soporta el intercambio de información de gestión TMN. La red de comunicación de datos puede ser externa o hacer uso de la propia red de telecomunicaciones que es gestionada. Representa la implementación de los niveles 1 a 3 de OSI, y puede estar soportada por la capacidad portadora de diferentes tipos de subredes, como por ejemplo, redes de conmutación de paquetes, redes de área metropolitana, extensa o local.

o) Elemento de Red (NE)

Los recursos físicos a gestionar, es decir, los equipos o grupo de equipos de telecomunicación que forman parte de nuestra red se representan mediante este bloque físico. Su conexión con la red TMN es mediante una

interfaz de gestión Qx o Q3. Opcionalmente podrán proporcionar interfaces F o bien una interfaz X si soporta funciones OSF.

El elemento de red se comunica con la red de gestión con el fin de ser supervisado y/o controlado. Incluye todas las funciones de telecomunicación que serán gestionadas por el sistema de gestión.

p) Estaciones de Trabajo (WS)

Una vez que los sistemas de gestión tienen la información de gestión disponible, ésta se debe presentarse al usuario de una forma agradable e inteligible. El componente físico que contiene las funciones de presentación y de adaptación hombre-máquina es la Estación de Trabajo (WS). Este sistema soporta la función de traducción de la información de gestión ofrecida en el punto de referencia ***F*** a información presentable en el punto de referencia ***G***, y viceversa.

4.1.3.2 Puntos de Referencia (PRs)

La arquitectura de una red de gestión basada en TMN proporciona el medio de transportar y procesar la información relacionada con la gestión de redes de telecomunicaciones y los servicios que soporta. La arquitectura física como hemos visto está íntimamente ligada a los bloques funcionales que desempeñan. De esta manera, para esta trasferencia de información entre bloques funcionales se utiliza una ***Función de Comunicación de Datos (FCD)***. Las interfaces a través de las cuales los bloques funcionales intercambian información de gestión se denominan ***Puntos de Referencia (PRs).***

Los puntos de referencia definen fronteras de servicio entre dos bloques de función de gestión. Tienen por objeto identificar la información que pasa entre bloques funcionales, son puntos conceptuales de intercambio de información entre bloques de función de gestión no solapantes. Se definen las clases:

- **Q**: Entre sistemas de operación entre sí, es decir, gestores y agentes, entre sistemas de operaciones y los elementos de red, entre dispositivos de mediación y sistemas de operación, y entre dispositivos de mediación y elementos de red. Dentro de esta clase de punto de referencia se pueden definir dos subclases:
  - **Qx**: entre elementos de red y funciones de mediación, entre éstos últimos y dispositivos de adaptación, y por último, entre propias funciones de mediación.
  - **Q3**: entre elementos de red y sistemas de operación (gestores y agentes), entre dos sistemas de operación y entre éstos y dispositivos de adaptación.
- **F**: situado entre los sistemas de operación y las estaciones de trabajo.
- **X**: situados entre sistemas de operación pertenecientes a diferentes dominios TMN

- **G**: está situado fuera del ámbito de la TMN y representa la unión entre las estaciones de trabajo y el operador del sistema. Una descripción de éste se puede encontrar en las recomendaciones de la serie Z.300
- **M**: situados fuera del dominio TMN entre el dispositivo de adaptación y una entidad no TMN, o que no es conforme a las recomendaciones TMN.

En la figura 4.1.3-2 se pueden observar los puntos de referencia y los distintos bloques funcionales.

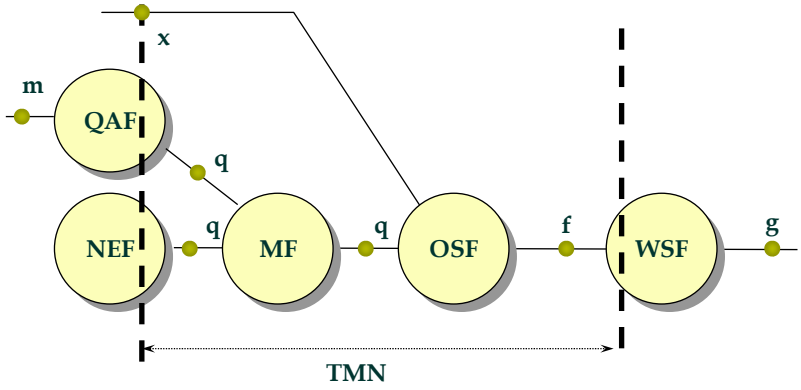

Figura 4.1.3-2 Puntos de referencia.

4.1.4 Arquitectura funcional para la jerarquía de la red de gestión TMN.

A efectos operacionales, podrá considerarse la funcionalidad de gestión particionada en capas. Aunque no está formalmente descrita en el estándar, si es comúnmente aceptada como un concepto muy útil a la hora de la definición de la arquitectura funcional recomendada por la M.3010.

Se realiza una división en cuatro niveles, como se muestra en la figura 4.1.4-1.

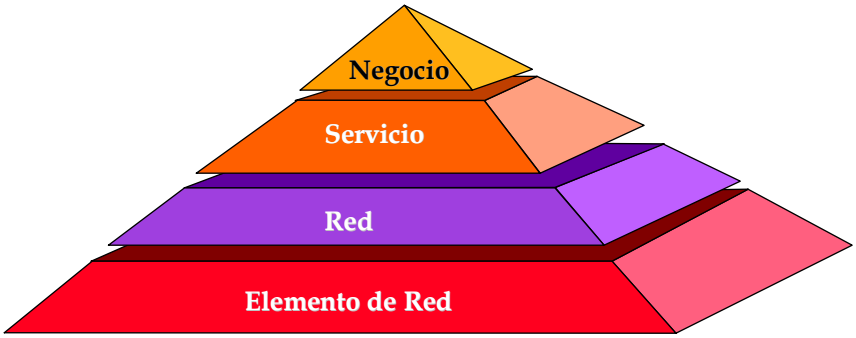

Figura 4.1.4-1 Estructura jerarquizada de gestión.

Nivel de Elemento de Red

Gestiona cada elemento o recurso de la red como un ente individual y aislado. Soporta una abstracción de las funciones de gestión proporcionadas por los distintos elementos de la red a gestionar.

q) Nivel de Red

Responsable de la gestión y coordinación de los recursos de red bajo su dominio, sin importar la diversidad de los equipos y tecnologías que los soportan.

Las funciones referentes a la gestión de un área geográfica extensa están ubicadas en esta capa.

r) Nivel de Servicio

Responsable de los aspectos contractuales de los servicios proporcionados a los clientes. Además tiene la labor de coordinación entre los distintos proveedores de servicios del mismo tipo, comportándose frente al cliente como un único proveedor de servicio.

s) Nivel de Negocio

Responsable de la empresa operadora como un todo y del cumplimiento de los acuerdos adoptados con otras compañías.

Aceptando la estructura jerarquizada de la gestión TMN, se podría considerar que en realidad la gestión se efectúa con la coordinación de cuatro sistemas o funciones de operación diferentes, cada uno especializado en las funciones de gestión de su nivel.

En la figura 4.1.4-1 se representa la jerarquización de las funciones que componen el sistema de operación TMN de una determinada red. A continuación se describe la funcionalidad de cada bloque representado:

Gestor de Elemento de Red

- Controlar y coordinar individualmente los distintos elementos de red involucrados.
- Proporcionar una función de mediación o adaptación que permita al nivel de red la interacción en términos de información de gestión con los elementos de red.
- Mantenimiento de estadísticas de utilización de los elementos de red.

t) Gestor de Red

- Control y coordinación de las redes bajo su dominio de gestión.
- Provisión, borrado o modificación de las capacidades de red necesarias para el soporte de los servicios ofrecidos a los clientes.

- Interacción con el nivel de servicio en términos de índices de prestaciones, disponibilidad, etc.

u) Gestor de Servicio

- Asegurar el lado del cliente y la interfaz con otros administraciones o empresas privadas.
- Interacción con usuarios, proveedores de servicios y otros servicios
- Interacciones con el nivel de red en términos de calidad de servicios.
- Interacción con el nivel de Negocio.

v) Gestor de Negocio

- Coordinación de acciones ejecutivas e interfaces con otros sistemas similares.

4.1.5 Conclusiones y futuro del estándar

Si nos preguntamos si el estándar TMN ha cumplido los objetivos que pretendían los organismos internacionales, y más concretamente el ITU-T, deberemos analizar si el estándar TMN para redes de telecomunicaciones es efectivamente una infraestructura de gestión apropiada para las futuras redes.

Como hemos visto, una red de gestión TMN se caracteriza por la estandarización de los protocolos, interfaces y arquitectura que la conforma y que constituyen la infraestructura o el marco adecuado para abordar la gestión de las cada vez más heterogéneas y complejas redes de telecomunicaciones.

En esta unidad se ha discutido con algo de detalle la arquitectura tanto física y funcional como de información del estándar TMN. Sin embargo, podemos afirmar que las labores de estandarización avanzan lentamente, tanto es así, que en muchas ocasiones van por detrás de la implementación que los laboratorios de I+D de importantes empresas del sector están desarrollando.

Si nos fijamos en la situación actual de los trabajos de estandarización, actualmente destacan los trabajos de los grupos XI y XV del ITU-T, que se encargan fundamentalmente de profundizar en el modelado y definición de objetos y mensajes. Más concretamente, el grupo XV trabaja en el modelado de equipos SDH, definiendo librerías de objetos y su funcionalidad [ETSI NA4, 95].

Uno de los mayores esfuerzos, anticipándose a los trabajos del ITU-T es el de reconsiderar y expandir los servicios de gestión. Esta línea de trabajo tiene su base en la recomendación M.3200 (Servicios de Gestión de la red de gestión TMN: Visión de Conjunto) [ITU-T M.3200, 92]. La rec. M.3200 incluye una descripción estándar de los servicios de gestión que ayuda a identificar la ubicación de las áreas funcionales de cada servicio en las distintas capas de gestión que presenta el modelo TMN.

Por último, mencionar el gran esfuerzo que las mayores empresas suministradoras de equipos síncronos están realizando para incorporar en sus sistemas de gestión propietarios modelos de información estándares y abiertos, de manera que puedan ofrecer soluciones de gestión globales con la posibilidad de entornos multivendores. De esta manera, un gran número de las grandes operadoras de redes de transmisión basadas en jerarquía digital síncrona, están optando por una arquitectura basada en varios suministradores, consiguiendo la integración de la gestión en alguna de las capas TMN. Sin duda, esta idea promete ser una interesante área de investigación y por supuesto, un gran avance para el desarrollo de las redes de telecomunicaciones.

4.2 GESTIÓN OSI

Los primeros trabajos en gestión de redes se realizaron sobre redes de datos[2], siendo muy importante la estandarización realizada por ISO (*International Organization for Standarization)* para la gestión de la arquitectura OSI *(Open System Interconection).* El resultado de este esfuerzo constituyó la fuente principal de muchas de recomendaciones de gestión de redes de telecomunicación del ITU-T.

Los esfuerzos de normalización en redes de telecomunicación comienzan con posterioridad a los de las redes de datos, por lo que se puede considerar como herederos de éstas. Sin embargo, la gestión de las redes de datos es más sencilla, por lo que actualmente los trabajos de estandarización no son suficientes para llevar a cabo una gestión global de una red de telecomunicaciones compleja. Como ejemplo de estas carencias, podemos citar la definición de la arquitectura de la red de gestión y los aspectos de modelado de la información de gestión.

Actualmente es en éste último aspecto donde se está trabajando más duramente desde los organismos internacionales de normalización, especialmente en la definición de modelos de información orientados a objetos, y válidos para implementar toda la funcionalidad necesaria en la gestión de una red de telecomunicaciones compleja.

4.2.1 Gestión de redes de datos

El desarrollo actual de la gestión de redes de telecomunicación es fruto de los esfuerzos llevados a cabo, a lo largo de muchos años, en el campo de las redes de datos. Es por ello necesario estudiar la evolución de la gestión de las redes de datos, para comprender mejor en qué situación se encuentra la gestión de dichas redes de telecomunicación, qué problemas se han solucionado, y cuales requieren una mayor investigación para alcanzar soluciones.

Los operadores de redes de datos fueron los primeros en plantearse la necesidad de desarrollar unos protocolos de gestión estándares, que permitieran acceder

[2] Por redes de datos se entiende aquellas formadas únicamente por equipos de comunicación de datos.

uniformemente a cualquier elemento de red, independientemente del fabricante. Pero no sólo interesaba que el acceso fuera uniforme, sino que fuera también uniforme la semántica de la información de gestión.

Como una solución rápida, la IAB *(Internet Activity Board)* recomendó la inmediata implementación del protocolo SNMP para gestionar los routers de Internet. Este protocolo de gestión estaba enfocado básicamente a las áreas de gestión de fallos y configuración. Actualmente el uso del protocolo SNMP está ampliamente extendido en todas las áreas de gestión.

Al mismo tiempo, la IAB recomendó a la comunidad de investigadores que explorara el protocolo CMIS/CMIP como la base para un protocolo de gestión que satisficiera las necesidades futuras. CMIS/CMIP fue desarrollado por ISO con objetivos muy diferentes a SNMP. Originariamente, SNMP se diseñó sólo para gestionar dispositivos IP, mientras que CMIS/CMIP se diseño para gestionar todo tipo de elementos de red, sin especificar el tipo de dispositivo en cuestión.

4.2.2 Modelo de gestión OSI

El modelo de referencia definido por ISO para establecer comunicaciones entre sistemas se denomina niveles o torre OSI *(Open System Interconnection)* . Este modelo contempla la separación de actividades, encaminadas a realizar la comunicación, por niveles. Cada uno de estos niveles realiza un conjunto de tareas para llevar a cabo la intercomunicación [ISO 7498/4, 7498/2].

El modelo de gestión propuesto por OSI permite crear, borrar, y acceder a información de gestión y modificarla. La base de datos de información interna a un sistema abierto y que puede ser transferida o utilizada para la gestión de dicho sistema se denomina MIB *(Management Information Base)*. La MIB está estructurada en forma de árbol, conteniendo instancias de objetos gestionados que se organizan en forma de árbol jerarquizado. En la figura 4.2.2-1 se representan las características de un objeto gestionado. Los nodos se modelan como objetos, y la información de gestión es almacenada en forma de atributos en las instancias de dichos objetos.

El modelo gestión OSI se basa en el esquema de ***gestor*** - ***agente***. Mediante esta estructuración será posible establecer responsabilidades de gestión sobre un cierto dominio y compartir el conocimiento almacenado en la MIB entre sistemas de gestión. El gestor recibirá notificaciones del agente y emitirá peticiones de ejecución de acciones sobre los objetos que modelan los recursos que gestiona. El agente será el proceso de aplicación que gestiona directamente los recursos, ejecuta las peticiones del gestor y suministra a éste una vista de estos recursos. Las funciones principales del agente, por lo tanto, serán mantener una visión de los recursos, ejecutar peticiones, y emitir notificaciones al gestor informando del comportamiento de los mismos.

El gestor y agente intercambian información en términos de objetos gestionados que modelan los recursos reales de la red a gestionar, y que forman la MIB.

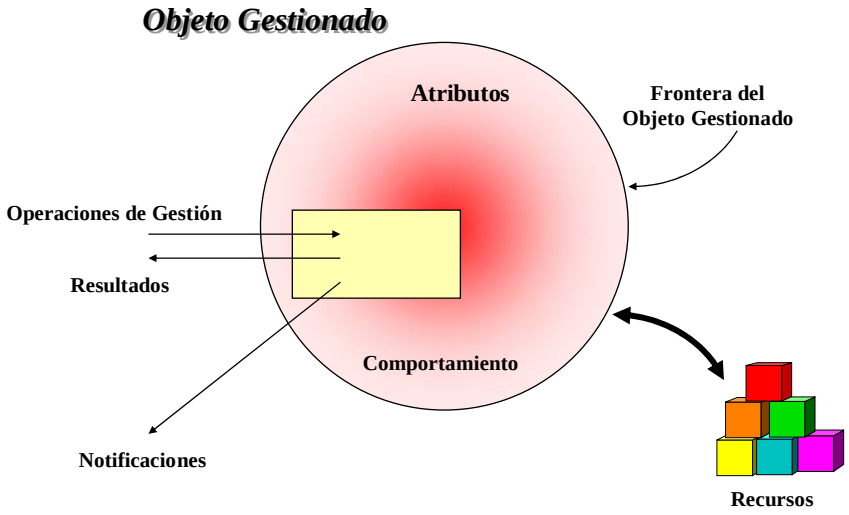

Figura 4.2.2-1 Objeto Gestionado

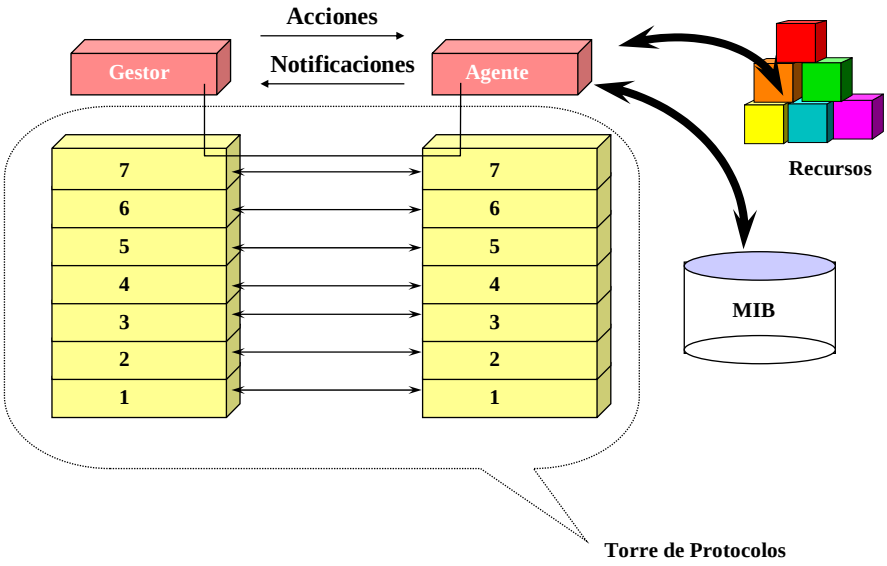

Figura 4.2.2-2 Relación Gestor-Agente

4.2.3 Modelo de comunicaciones

El modelo de comunicaciones define los protocolos y servicios de comunicaciones, que se utilizan para el intercambio de información de gestión entre el gestor y el agente. El modelo de comunicaciones de gestión basado en OSI, requiere transporte orientado a conexión y cuenta con el entorno de la capa de aplicación OSI [CMISE/ROSE 11, 92].

Los gestores y agentes son, por tanto, aplicaciones que usan los servicios de CMISE *(Common Management Information Service)* para intercambiar información de gestión. CMISE ofrece puntos de acceso al servicio (SAP´s) para controlar las asociaciones entre gestores y agentes. Estas asociaciones permiten el intercambio

de preguntas y respuestas, peticiones y confirmaciones, maneja notificaciones de eventos, y ofrece invocaciones remotas de operaciones sobre objetos. CMISE utiliza los servicios de ACSE y ROSE [CMISE/ROSE 11, 92]. La estructura típica del entorno de comunicaciones se muestra en la figura 4.2.3-1.

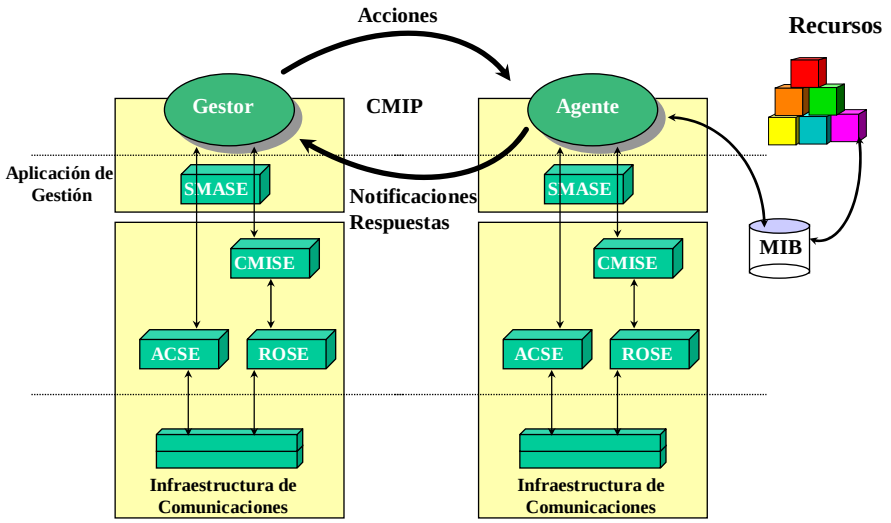

Figura 4.2.3-1 Modelo de Comunicaciones

El agente OSI ofrece funciones de selección de los objetos que son accedidos por SAPs a través de servicios de GET/SET/ACTION de CMISE. El agente también detecta los eventos y envía las notificaciones que le llegan a las entidades de gestión involucradas.

La entidad CMISE ofrece dos tipos básicos de servicio, los servicios de **operación** (el gestor envía una instrucción al agente para que éste envíe información o proceda a realizar cambios en los objetos bajo su dominio) y el servicio de **notificación** (el agente envía información relativa a objetos gestionados) como se refleja en la figura 4.2.3-2. Son los siguientes:

- **Servicios de Comunicación de Gestión**: M-INITIALIZATE (establece una asociación de gestión), M-TERMINATE (Finaliza una asociación de gestión) y M-ABORT (Terminación sin confirmar).
- **Servicios de Operación:**
  - M-CREATE: crea una instancia de un objeto en la MIB,
  - M-DELETE: borra una instancia de un objeto en la MIB,
  - M-SET: modifica algún atributo de un objeto en la MIB,
  - M-GET: obtiene información de la MIB,
  - M-CANCEL_GET: cancelación de peticiones, y

- M-ACTION: Invoca una operación en un objeto.

- **Servicios de notificación:** M-EVENT_REPORT, informa al gestor de un evento en un objeto.

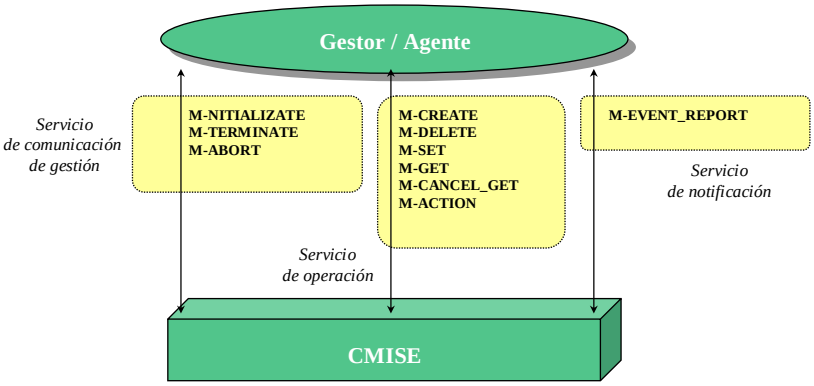

Figura 4.2.3-2 Servicios CMISE

El servicio quizás más importante de todos, debido a que a través de él el gestor y agente pueden mantener una información común, es el servicio M-GET. Este servicio permite acceder a la información de los valores de atributo de un objeto gestionado (o grupo de objetos gestionados). Este servicio es confirmado, ya que se utiliza para obtener información del agente. Es posible el acceso masivo a información de gestión mediante la indicación al agente del subárbol de la MIB donde se almacenan los datos a los que se quiere acceder a través de una única invocación al servicio M-GET. Para especificar un criterio de selección, M-GET define un filtro que el agente se encargará de emplear para llevar a cabo la búsqueda y selección. En este filtro se especifica:

- Identificación del objeto base sobre el que se realiza la búsqueda. Concepto de ***filtering*** o filtrado.

- Nivel de profundidad para realizar la búsqueda. Concepto de ***scope***.

4.2.4 Estructura del modelo de información de gestión.

La estructura del modelo de información de gestión que se ha seleccionado para ISO, está basado en las técnicas de orientación a objetos. Los objetos gestionados (*Managed Objects o MO*) son representaciones abstractas de los recursos, que representan propiedades y que son vistas por los gestores para la gestión de dichos recursos. El modelo de información es introducido y elaborado en los "***Principios para la Definición de los Objetos Gestionados (GDMO)***" [ITU-T X.722, 92]. Los objetos de gestión definidos como clases orientadas a objetos, ofrecen definiciones de propiedades comunes de un conjunto de recursos gestionados. Estas clases se definen mediante una plantilla o "template" [ITU-T X.722, 92], para encapsular datos y operaciones de gestión asociadas con

entidades de gestión. Los objetos gestionados que representen a un recurso concreto del mismo tipo pertenecerán a la misma clase, o en la "jerga" de objetos, serán todos ***instancias*** de la misma clase. La plantilla para la descripción de objetos en GDMO se representa en la figura 4.2.4-1.

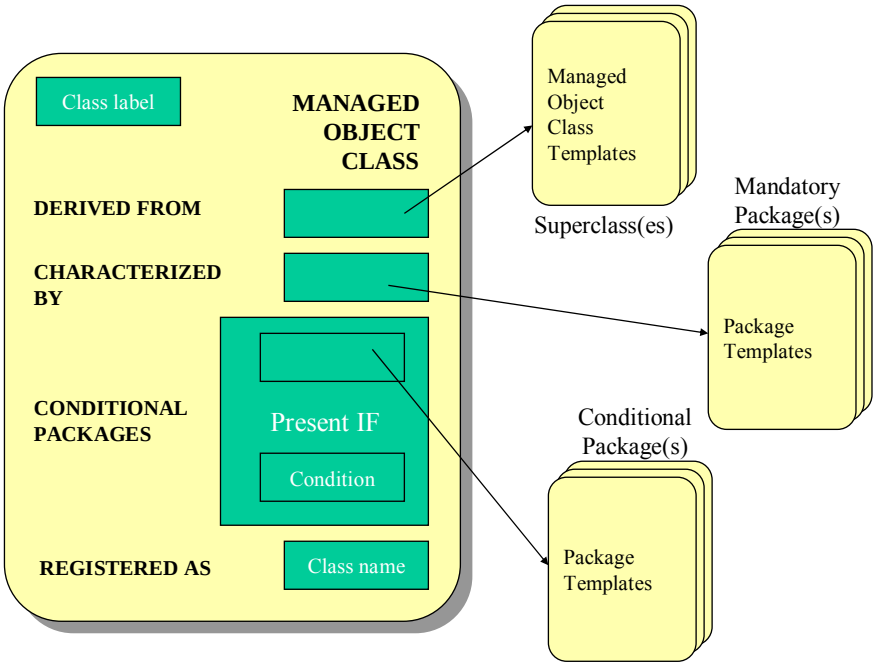

Figura 4.2.4-1 Plantilla GDMO

Los objetos así definidos son capaces de emitir notificaciones de eventos. De esta manera, las aplicaciones pueden invocar métodos de manera síncrona. Sin embargo, los eventos pueden ocurrir de forma asíncrona, es decir, independientemente a la actividad de los gestores, y seguir manteniéndose la estabilidad del sistema.

El concepto de ***herencia*** dota a este modelo de información orientado a objetos, de la posibilidad de definir una clase de objetos de manera que tenga todas las características de otra, y además, incorpore algo específico o una especialización de las primeras. Así, por ejemplo, de la clase ***casa***, con una serie de características, podríamos derivar la clase ***chalet,*** con características o atributos que sólo toman sentido cuando la casa es un chalet. En la relación de herencia se denomina superclase a la clase de la cual se hereda y subclase a la clase derivada.

La relación de herencia entre las clases de objetos permite definir una jerarquía entre estas clases llamada **"*arbol de herencia*".** En este árbol, las posiciones superiores las ocupan las superclases. La raíz del árbol lo ocupa la clase de objeto ***top***, de la que se derivan todas las demás. Cada clase nueva que se defina debe derivarse de alguna clase ya existente. Mediante el árbol de herencia, podemos dibujar el ***árbol de contención***, un grafo dirigido en el cual cada flecha apunta a un objeto gestionados contenido en el objeto origen de la flecha.

Otra relación importante entre las clases de objetos es la de nombrado. Mediante ésta, se identifica las instancias de objetos mediante un nombre único en todo el dominio de gestión. Así, el nombre de un objeto se obtiene en término de otro, que se llama objeto superior, mientras que el dependiente se llama objeto subordinado. Un objeto subordinado se nombra concatenando el nombre de su objeto superior y el nombre que identifica unívocamente el objeto dentro del contesto definido por el ámbito de su objeto superior. De esta manera se crea un ***árbol de nombrado*** mediante el que se explicita la relación entre objetos superiores y subordinados. Para localizar alguna característica de un objeto, deberemos recorrer el árbol de nombrado hasta alcanzar la instancia deseada. Los objetos subordinados sólo pueden existir si existe su objeto superior, dándose un atributo que le identifica unívocamente en el momento de la creación. En la figura 4.2.4-2 se puede apreciar un ejemplo de árbol de nombrado, en el que los nombres se forman por la concatenación de los nodos superiores.

El grupo de ISO responsable de los estándares de gestión de red ha definido el conjunto de objetos necesarios para soportar las actividades de gestión (filtros, históricos, etc), así como un conjunto de objetos básicos (equipos, alarmas, etc). Actualmente se está especificando las librerías de clases de objetos que se utilizan para cada nivel de comunicaciones.

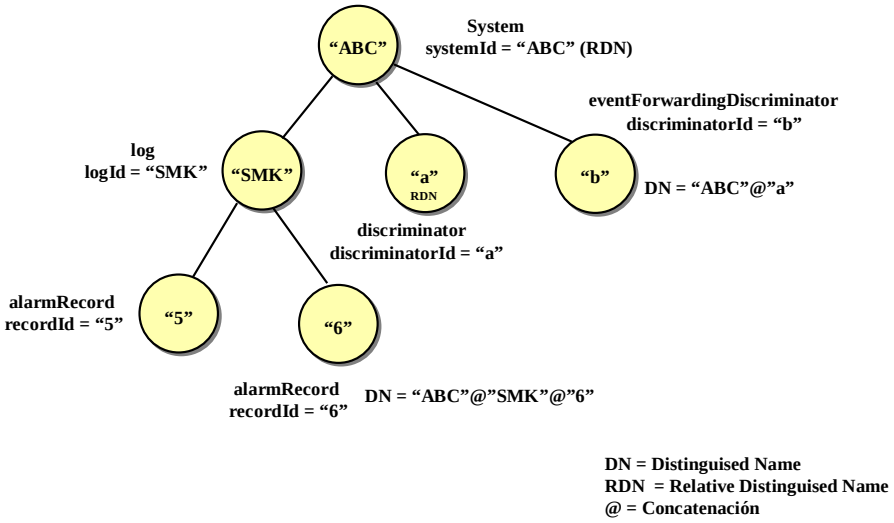

Figura 4.2.4-2 Arbol de nombrado

Entre las principales librerías se pueden citar:

- IS 10165-1 *Management Information Model*. Explica los conceptos generales del modelo de información de ISO, identificándose y describiéndose las operaciones que ofrecen los objetos gestionados.

- IS 10165-2. Librería de las clases de objetos más comunes utilizadas en la gestión OSI.

- IS 10165-3. Describe los atributos de carácter general utilizados en la gestión.
- IS 1065-4. *Guidelines for the Definition of Management Objects*. Describe la notación definida por ISO para especificar clases de objetos gestionados. Suministra, así mismo, reglas para utilizar esta notación
- Recomendación X.721 del ITU-T. Definición de Información de Gestión. Incluye definiciones genéricas en GDMO de clases, paquetes, atributos y notificaciones de uso general, así como sus sintaxis en ASN.1

Librerías definidas por los organismos de estandarización aplicadas a la gestión de redes de telecomunicaciones o servicios concretos:

- G.774. Modelo de Información de Gestión para la Jerarquía Digital Síncrona a Nivel de Elemento de Red.

4.2.5 Evaluación crítica del modelo OSI

El objetivo del modelo OSI es el de ofrecer un marco sobre el que poder llevar a cabo la gestión de sistemas arbitrariamente complejos. Vamos a evaluar ventajas e inconvenientes asociados a la generalidad de este modelo.

La principal ventaja que presenta la gestión OSI es el amplio respaldo por los principales organismos de estandarización (ISO e ITU-T). Esto facilita en gran medida la interoperabilidad de sistemas de distintos fabricantes. Si bien, la dificultad estriba en que no sólo se deben definir los protocolos de comunicación, sino también que el modelo funcional y de información definidos por estos organismos deben ser únicos.

Por otro lado, la gestión OSI suministra unos mecanismos muy potentes para realizar la gestión de equipos, redes y servicios de los que, hoy por hoy, ningún modelo de gestión se dispone. El precio que se paga a cambio, es la complejidad de las aplicaciones de cara a su desarrollo y un alto consumo de recursos. Tanto es así, que actualmente es la gestión y no los propios elementos de red, los que limitan los servicios que puede prestar una determinada red de telecomunicaciones.

Por lo tanto, la aplicación de la gestión OSI resulta adecuada en entornos para los cuales sea necesario disponer de las capacidades que ofrece OSI y que no suministran otros modelos y entornos multivendedor.

4.2.6 Aplicación de Gestión OSI

En la figura 4.2.6-1 se muestra un posible método de aplicación de la gestión OSI. Cuando tenemos un escenario o red que necesitamos gestionar, actuaremos según el esquema.

El primer paso consiste en determinar los requisitos del sistema. A partir de estos requisitos será posible obtener una especificación funcional del sistema, una definición de los recursos que es necesario gestionar y el modelo de organización

de la solución de gestión, es decir, dominios de gestión, gestores y agentes necesarios para nuestro problema.

Un análisis de la especificación funcional, junto con el modelo de organización, nos permitirá identificar las funciones de gestión con que es necesario dotar tanto a los gestores como a los agentes.

A partir de la identificación de las funciones a implementar, definiremos las librerías de clases de objetos gestionados que se utilizarán para representar el problema de gestión, junto con el modelado de los recursos que utilicen las funciones de gestión definidas, históricos, filtros, alarmas, etc. Una vez identificada la librería de clases será necesario definir esquemas de nombrado para cada una de las clases incluidas en la librería.

Las funciones de gestión, junto con los requisitos de prestaciones permitirán definir requisitos de comunicaciones, de los cuales se derivarán los perfiles de protocolos a utilizar en las comunicaciones gestor/agente. Por último, será necesario identificar el cumplimiento de los estándares que existen al objeto de proceder a su posterior verificación.

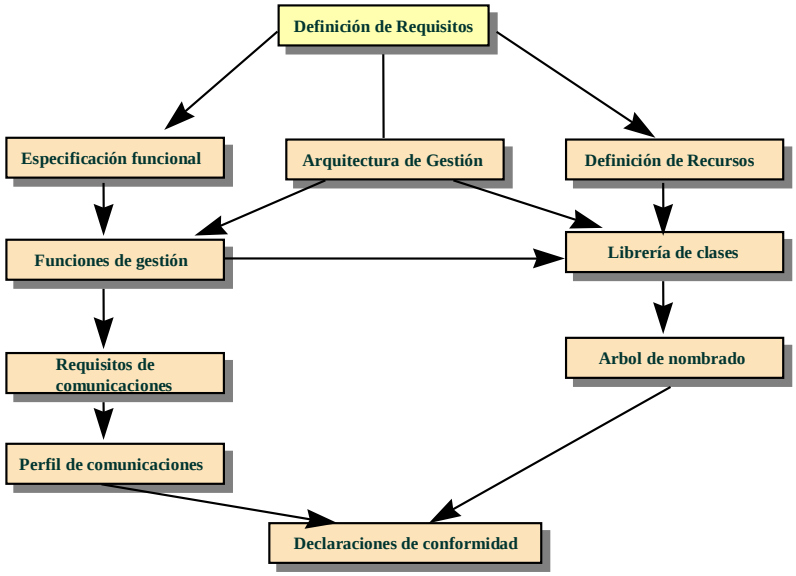

Figura 4.2.6-1 Aplicación de gestión OSI

Resumen

El estándar de gestión de redes de telecomunicaciones (TMN) define una arquitectura funcional y física con la que es posible modelar los sistemas de gestión de cualquier red de telecomunicaciones. Para ello se define un modelo genérico de red y un conjunto de interfaces normalizadas que modelan el intercambio de información de gestión entre dos sistemas de operación o elementos de red .Los bloques funcionales constituivos de la arquitectura TMN son: sistemas de operación, dispositivos de mediación, adaptadores Q, la propia red de comunicación de datos, los elementos de red y las estaciones de trabajo. Uniendo estos bloques funcionales se definen los puntos de referencia o interface Qx, Q3, F, X, G y M.

La arquitectura TMN se apoya en la distinción funcional de cuatro niveles: nivel de elemento de red, nivel de red, nivel de servicio y nivel de negocio. Así mismo, se apoya en la torre de protocolos OSI. A la aplicación de la arquitectura TMN para la gestión de redes complejas se denomina gestión OSI. La gestión OSI está basada en el paradigma gestor-agente, y define un modelo de información orientado a objetos, un modelo de comunicaciones basado en el protocolo CMIP de OSI, y funciones de gestión a través de las interfaces TMN definidas anteriormente.

Ejercicios de Autoevaluación

Ejercicio 7

La arquitectura de gestión TMN es capaz de gestionar:

a. Redes públicas y privadas.

b. Redes de transmisión tanto digitales como analógicos.

c. La propia red de gestión de telecomunicaciones.

d. Todas las anteriores.

Ejercicio 8

La interfaz Q3 de gestión se define entre los bloques funcionales:

a. Sistema de operación y elementos de red.

b. Sistema de operación y la función de presentación (WS).

c. La red de comunicaciones y los elementos de red..

d. Ninguna de las anteriores.

Ejercicio 9

El nivel de red de la arquitectura TMN comprende:

a. La gestión individual de los elementos de red.

b. Interconexión con otros proveedores de servicios.

c. Provisión de trayectos a nivel de red.

d. Mantenimiento de estadísticas de utilización de los elementos de red.

Ejercicio 10

El modelo de gestión OSI:

a. Es utilizado para la gestión de redes de datos simples.

b. Los gestores son inteligentes y los agentes sólo recogen datos.

c. Está basado en estándares de facto o de mercado.

d. Resulta adecuado a entornos complejos.

SOLUCIONES A LOS EJERCICIOS

1.d, 2.a, 3.c, 4.d

CAPÍTULO 5

El protocolo IS-IS

En este capítulo se describe el protocolo IS-IS y cómo está diseñada una red de gestión SDH basada en el protocolo de enrutamiento IS-IS de OSI. Además se describirá el formato de direcciones del protocolo.

La arquitectura jerárquica del protocolo IS-IS se desarrollará en esta unidad, describiendo los niveles 1 y 2 del protocolo y la distribución de la red en áreas.

La utilización de bridges y routers para prolongar redes IS-IS será descrita y las ventajas y desventajas de cada uno se explicarán.

ESQUEMA DE CONTENIDO

5.1 REDES IS-IS

El **protocolo IS-IS** (*Intermediate Systems - Intermediate Systems*) es un protocolo de nivel de red en sistemas intermedios[3]. El protocolo IS-IS es el encargado de crear, actualizar y mantener las tablas de enrutamiento usadas por los protocolos de red no orientados a conexión, cuando un paquete ha de ser enrutado a través de un nodo intermedio hacia su destino (nodo final).

IS-IS proporciona un mecanismo automático, fiable, eficiente y distribuido para mantener actualizada la red de comunicación de datos en términos de tablas de enrutamiento. De esta manera, el operador de la red no debe preocuparse de la topología de red cuando instala NEs y no es precisa la reconfiguración manual en caso de fallo de NEs o de algún enlace.

El **protocolo IS-IS** está definido en el estándar internacional **ISO/IEC 10589**.

5.1.1 El dominio de la red

El concepto de red aparece debido a la capacidad de interconectar subredes independientemente del enlace entre ellas y de sus protocolos de nivel 3. El entorno de red se construye usando **Sistemas Intermedios** (***IS****-Intermediate Systems*) y **Sistemas Finales** (***ES****-End Systems*) como componentes internos.

Los **ES** son máquinas con un único interfaz de red, por lo tanto conectadas sólo a una subred, que contienen las aplicaciones que soportan las actividades del usuario. Básicamente pueden ser desde un PC a un servidor, pero siempre conectados a un único punto de la red. Los ES pueden generar y recibir paquetes desde cualquier elemento de red que pertenezca al dominio de la red, pero no pueden enrutar paquetes. Cada ES debe implementar la pila completa de protocolos, incluyendo las capas superiores (Transporte, Sesión, Presentación y Aplicación). Obviamente las tres capas inferiores (Red, Enlace y Física) también deben estar implementadas para que pueda formar parte del dominio de la red.

El **IS** es un sistema que interconecta, y por lo tanto está conectado a dos o más subredes. El IS debe ser capaz de traspasar paquetes entre una redes. Básicamente, desde el punto de vista del IS, una subred es únicamente un conducto que permite a los paquetes alcanzar el siguiente IS o su destino final. Un IS puede generar, recibir y enrutar paquetes. Si un IS dispone sólo de una conexión a al red realiza las mismas funciones que un ES.

Un IS puede implementar las capas superiores de la pila de protocolos si las aplicaciones de usuario corren sobre él. Si es utilizado como enrutador puro para interconectar subredes, sería suficiente implementar las tres capas inferiores.

El **modelo OSI** sitúa las funciones de **interconexión de redes** como parte del nivel de red, además de ser usadas para generar y actualizar las tablas de enrutamiento.

---

[3] En la terminología OSI, *Sistema Intermedio* es equivalente a *Router*.

5.1.2 Tipos de subredes

Subredes son las unidades que forman los dominio de red. Las subredes se pueden clasificar según los tipos siguientes:

a) **Subredes Broadcast:** son subredes multiacceso que disponen de capacidad para direccionar un grupo de sistemas. Esto significa que cada sistema de este tipo de subredes puede enviar un mensaje a varios sistemas de la misma subred enviando sólo una trama, usando direcciones broadcast. Las **LAN Ethernet** (**ISO 8802-3**) y en general todas las **LAN** (**ISO 8802-2**) están incluidas en esta categoría.

b) **Subredes de topología general:** pueden modelarse como un conjunto de enlaces punto a punto, cada uno de los cuales interconecta exactamente dos sistemas. Esto no sólo significa que dos estaciones están físicamente conectadas al medio físico sino que lógicamente cada estación puede comunicarse con otra estación de la subred en un momento dado, no siendo posibles las direcciones broadcast.

   1) **Enlaces multipunto:** son enlaces entre más de dos sistemas donde un sistema de la subred es la estación primaria y los restantes sistemas son secundarios, o esclavos. La estación primaria es la que gestiona el enlace, dando a las estaciones secundarias el permiso para transmitir. La comunicación directa entre dos estaciones secundarias no es posible. El **HDLC punto-multipunto** (**ISO 4335**) es un ejemplo de este tipo de subred.

   2) **Enlaces permanentes punto a punto:** son enlaces entre dos sistemas que permanecen conectados todo el tiempo, como por ejemplo los enlaces punto a punto **LAPD** (**ITU-T Q.920** y **Q921**).

   3) **Enlaces establecidos dinámicamente:** son enlaces sobre redes. **X.25** o **RDSI** son ejemplos de este tipo de subredes. Dentro de este grupo se pueden distinguir entre:

      - **enlaces estáticos** punto a punto, como por ejemplo los circuitos virtuales conmutados en X.25,

      - **enlaces asignados dinámicamente**, donde el circuito se establece sólo cuando se recibe tráfico y se libera tras cierto tiempo sin transmitir ni recibir datos.

5.1.3 Direcciones

En el dominio de red cada estación se caracteriza por una única dirección de red llamada **Punto de Acceso a los Servicios de Red** (**NSAP -** *Network Service Access Point*). El **NSAP** identifica unívocamente cada estación dentro del dominio de red y no deben haber dos estaciones con la misma dirección en el mismo dominio de red.

Las **direcciones** deberán cumplir la recomendación **ISO 8348/Add.2** para lograr un sistema de numeración homogéneo.

En Telefónica se utiliza el formato de direcciones **ISO DCC NSAP**. La dirección **NSAP** consta de dos partes: el **IDP** (*Initial Domain Part*) y el **DSP** (*Domain Spacific Part*).

IDP		**DSP**						
AFI	**IDI**	**VER**	**AUTH**	**Rsvdo.**	**Dominio**	**Área**	**ID Sist.**	**Sel.**
1 byte	2 bytes	1 byte	3 bytes	2 bytes	2 bytes	2 bytes	6 bytes	1 byte
39	**724F**	**20**	**001A00**	**0000**	**00mm**	**nnnn**	**xxxx.xxxx.xxxx**	**tt**

Figura 6.1.3-1 ISO DCC NSAP

En la Figura 6.1.3-1 se muestra la dirección **NSAP** y el formato de direcciones de Telefónica como ejemplo, expresado en hexadecimal. Los campos que varían en la red de Telefónica son:

- **mm:** designa la subred del suministrador: 01 – Alcatel, 02 – Lucent y 03 – Ericsson.
- **nnnn:** identifica el área de gestión dentro de la subred de cada suministrador.
- **xxxx.xxxx.xxxx:** dirección del elemento de red.
- **tt:** dirección del puerto del protocolo de transporte al que va dirigido el mensaje.

La descripción de los campos del **NSAP** es la siguiente:

- **IDP**:
  - **AFI (***Authority and Format Identifier***):** especifica la autoridad responsable de asignar el campo IDI. El valor del AFI es 39 para el formato ISO-DCC
  - **IDI (***Initial Domain Identifier***):** para el formato ISO-DCC es el código de país. Para España es 724 (completado con unos 724F).
- **DSP**:
  - **VER (Version):** identifica el formato de DSP.
  - **AUTH (Authority):** identificador de la autoridad administrativa, es constante para toda la red.
  - **Reservado:** se fijará a 0000.
  - **Dominio:** identifica el dominio de enrutamiento al que pertenece un elemento de red. Este campo se usa por el propietario de la red para definir dominios de enrutamiento dentro de la red.

- **Área:** identifica el área a la que pertenece un elemento de red.
- **ID del sistema:** es el identificador del elemento de red dentro de su subdominio de enrutamiento, por ejemplo la dirección MAC 802.3 del elemento de red. Su longitud es de 6 bytes.
- **Sel.:** el selector identifica la aplicación sobre la capa de red a la que el mensaje va dirigido. Este campo no es utilizado para enrutar, sólo se usa en el elemento de red de destino para que el mensaje llegue a la capa de transporte correcta.

5.1.4 Proceso de entrega de paquetes en la red

El tráfico en la red comienza cuando uno de los nodos desea enviar un paquete a otro de los nodos. El nodo fuente construye el paquete apropiado insertando en la cabecera su propia dirección y la de destino y lo envía a través de la red. El paquete se direcciona (en el nivel 2) a la estación de destino si esta está en la misma subred o al IS que está en el camino hacia la estación de destino si ésta está en otra subred. En este último caso el IS tiene la responsabilidad de enviar el paquete hacia su destino.

Cada IS enruta paquetes, el problema es hacia donde se enrutan y quien escribe las tablas de enrutamiento. Los protocolos IS-IS y ES-IS son los responsables de definir estas tablas de enrutamiento.

5.2 PROTOCOLO IS-IS

El **protocolo IS-IS** es un protocolo definido por **OSI** (**ISO/IEC TR 9575**) para la creación y mantenimiento de las tablas de enrutamiento utilizadas por los IS para enrutar paquetes.

IS-IS define una **arquitectura jerárquica de dos capas**. Esta arquitectura define un enrutamiento intra-área, donde el área es la entidad más baja de la jerarquía, y un enrutamiento inter-área, para conectar áreas.

El protocolo IS-IS proporciona un mecanismo jerárquico para dividir los dominios de enrutamiento en áreas.

5.2.1 IS Nivel 1 (L1)

Cada área es un subdominio de enrutamiento restringido compuesto por elementos de red con características en común y que se desean ver como un conjunto. Cada uno de los NEs que pertenecen a la misma área comparten la misma dirección de área y cada uno de ellos tiene una visión completa de su propia área. Cada NE conoce cual es el mejor camino para llegar a cada uno de los otros NEs en su área y cualquier evento que ocurra en esta área (fallos, cambios topológicos, etc).

Todos los NEs que pertenecen a un área son IS de nivel 1 para esa área.

Dentro de cada área los **NEs se envían dos tipos de mensajes**:

- Mensajes para **conocer** cuales son los **elementos de red contiguos** y si están caídos o no.

- Mensajes enviados por cada elemento de red dentro del área a todos los demás **informando de cuales son sus vecinos y el coste relativo** de la comunicación con ellos. Estos mensajes se guardan en cada elemento de red y mediante el algoritmo de *Dijkstra* calculan el camino más corto para llegar a cualquier elemento de red del área y generan las tablas de enrutamiento de esa área. Por lo tanto, cuanto mayor sea un área, mayor será el tamaño de las tablas de enrutamiento.

Con estos mensajes cada elemento de red descubre a sus vecinos y distribuye esta información, además cada IS del área puede construir una tabla de enrutamiento que describe como llegar a cada uno de los elementos de red del área.

5.2.2 IS Nivel 2 (L2)

La cuestión ahora es como se realiza la interconexión entre áreas, es decir como un IS de nivel 1 puede enrutar un paquete a un IS que no pertenece a su misma área. La estructura jerárquica del IS-IS define elementos de red que actúan como frontera IS entre diferentes áreas, son los llamados IS de nivel 2. Estos IS actúan como IS de nivel 1 dentro de su propia área y como IS de nivel 2 respecto a las otras áreas.

Cuando un IS de nivel 1 tiene que enrutar un paquete que no va dirigido a su misma área, lo envía al IS de nivel 2 más cercano, delegando en éste la responsabilidad de enrutarlo hacia el área remota.

Cada IS de nivel 2 conoce cual es el mejor camino para alcanzar cualquier área dentro de su dominio de enrutamiento. Cada IS de nivel 2 contiene una entrada en su tabla de enrutamiento que define como llegar a cualquier otra área.

Los **mensajes IS-IS intercambiados** entre IS de nivel 2 son de dos tipos:

- Mensajes para **conocer** cuales son los **NEs que actúan como IS de nivel 2 contiguos** y si están caídos o no.

- Mensajes enviados por cada NE de nivel 2 del dominio a todos los IS de nivel 2 **informando de cuales son sus vecinos en términos de áreas y el coste relativo** de la comunicación con ellos. Estos mensajes se guardan en cada elemento de red de nivel 2 y mediante el algoritmo de *Dijkstra* calculan el camino más corto para llegar al resto de elementos de nivel 2 y generan las tablas de enrutamiento del dominio. Todos los elementos de red de un área se conocen globalmente como una única dirección que define el área en las tablas de enrutamiento de nivel 2. Por lo tanto, cuanto mayor sea el número de áreas, mayor será el tamaño de las tablas de enrutamiento en los IS de nivel 2

Con estos mensajes cada elemento de red de nivel 2 descubre a sus vecinos de nivel 2 y distribuye esta información, además cada IS de nivel 2 del dominio puede construir una tabla de enrutamiento que describe como llegar a cada área del dominio.

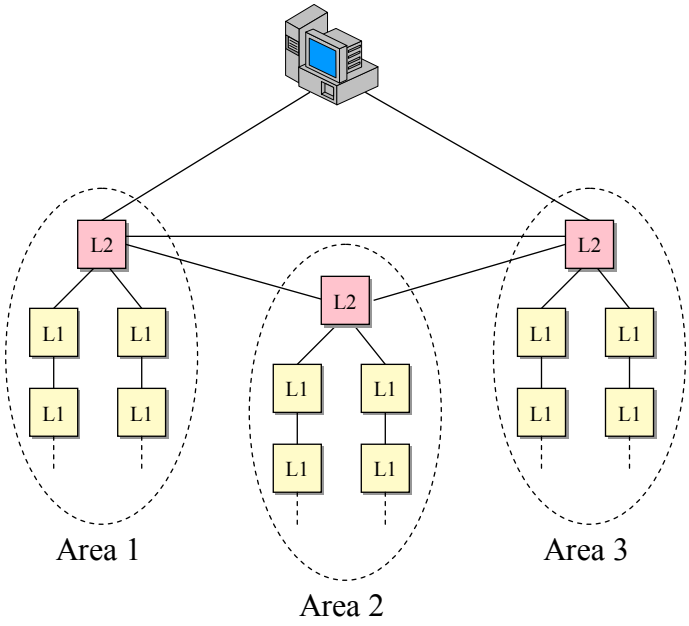

Figura 5.2.2 Niveles IS de los NEs

5.2.3 Conexión con otros sistemas

El **protocolo IS-IS** permite la **reconfiguración automática** de la red mediante la **construcción dinámica de las tablas de enrutamiento**. Este mecanismo funciona entre máquinas que implementan los protocolos IS-IS o ES-IS, aunque el protocolo IS-IS permite la interconexión con máquinas que no soporten los protocolos IS-IS o IS-ES.

Esto se consigue introduciendo manualmente la información de enrutamiento en el elemento de red que soporta IS-IS.

5.3 BRIDGES Y ROUTERS

Bridges y routers se utilizan cuando:

- Las interconexiones se realizan entre lugares remotos utilizando circuitos alquilados o una **WAN** (por ejemplo **X.25**) o una red **TCP/IP**.
- La topología de la red SDH no permita la creación de anillos que garanticen la fiabilidad de la red en caso de un fallo. Entonces se han de

añadir enlaces externos para forzar la presencia de anillos para proteger la red.

- La topología de la red SDH permite la creación de anillos pero el tamaño de éstos es demasiado grande para garantizar un rendimiento aceptable de la red. Entonces se han de añadir enlaces externos para dividir el anillo SDH en varios anillos DCN lógicos.

5.3.1 Bridges

Los **bridges interconectan dos o más partes de la misma LAN**, formado una LAN extendida. El bridge opera sólo a nivel de la capa física y de la de enlace (niveles 1 y 2 de ISO) gestionando tramas MAC. Los bridges son **independientes del protocolo** utilizado en el nivel de red y superiores y son completamente transparentes a ellos. En definitiva, los bridges **no realizan enrutamiento**, únicamente crean LANs extendidas.

Los bridges son capaces de realizar la segmentación del tráfico a nivel de la MAC identificando estaciones locales y remotas y evitando la transmisión de tramas dirigidas a estaciones locales.

La forma más simple de conectar bridges es uniéndolos mediante una conexión punto a punto. Los bridges disponen de dos o más salidas con lo que es posible conectar un bridge a otros dos a través de dos líneas dedicadas, o circuitos X.25.

Los bridges permiten pasar a través de ellos a las tramas broadcast, excepto si se les configura un filtro específico para que estas tramas no sean transmitidas. Como consecuencia, parte del ancho de banda de los enlaces de interconexión están ocupados por un tráfico que no es despreciable. El protocolo IS-IS utiliza frecuentemente las tramas broadcast para distribuir la información de enrutamiento a través de la red.

En algunos casos, dependiendo de la arquitectura de la red y su partición en áreas, la transmisión de tramas IS-IS a través de bridges puede ser completamente inútil desde el punto de vista de configuración de la red, además de perjudicial desde el punto de vista del tráfico, ancho de banda y utilización de la CPU. Para evitar estos problemas el planificador de la red deberá optimizar su diseño con soluciones particulares acordes con la topología de cada red.

A modo de resumen se presentan a continuación los principales puntos a favor y en contra de los bridges.

Ventajas de los bridges:

- Son flexibles e **independientes de los protocolos** de nivel de red.
- Cubren las necesidades de **filtrado de tráfico** y de seguridad en los accesos.
- Son **fáciles de configurar** e instalar.
- Son **baratos**.

Desventajas de los bridges:

- Los bridges operan sólo en una red, por lo tanto **no existe** un completo **aislamiento de tráfico**, y éste es “visto” por todos los nodos cabeceros de

gestión de la red. Esto puede saturar estos nodos con tráfico inútil, e incluso ser perjudicial y generar mensajes de error cuando pertenecen a áreas de enrutamiento diferentes.

- **Añaden** una **cabecera** en los paquetes, lo que afecta a la velocidad de los datos.
- **No protegen** la red **contra estaciones sin control** que llenan la *Ethernet* con mensajes erróneos.
- Algunos bridges no se pueden configurar con direcciones TCP/IP, y por tanto **no se pueden configurar y operar de forma remota**.

5.3.2 Routers

Un **router** es un equipo de red que **interconecta dos subredes LAN creando un entorno de red**. El router realmente **segmenta la red** en dos subredes independientes.

Los routers **operan a nivel de la capa de red**, proporcionando los protocolos de cada subred a la que está conectado. Los routers implementan el protocolo IP (*Internet network Protocol*) y procesan los paquetes de red leyendo la dirección de la red de destino de cada paquete y enrutándolos según sus tablas de enrutamiento.

Los routers no crean LAN extendidas, sino entornos de red compuestos por diferentes subredes. Sólo los paquetes cuya dirección de destino está almacenada en las tablas de enrutamiento son transmitidos por los routers. Los routers contienen protocolos de enrutamiento de red (como por ejemplo IS-IS) para poder crear y mantener las tablas de enrutamiento.

En un entorno **ISO/OSI**, cada router es un sistema intermedio IS (de nivel 1 ó 2) que implementa el protocolo IS-IS. Por lo tanto los routers deben tratarse exactamente igual que los elementos de red respecto al formato de direcciones.

Los routers realizan una segmentación completa del tráfico de las LAN conectadas, permitiendo pasar a través de ellos únicamente el tráfico que realmente va destinado a estaciones remotas. En particular, las tramas broadcast de IS-IS no son transmitidas por los routers pero son procesadas para actualizar las tablas de enrutamiento. Como consecuencia de esto, las líneas de conexión entre routers se deben dimensionar teniendo en cuenta sólo el tráfico entre LANs y no el tráfico total generado en las LANs por el protocolo IS-IS.

A continuación se presentan las **principales características** de los routers:

- **Necesitan menos ancho de banda** que los bridges en los enlaces de interconexión debido al aislamiento de subredes y filtrado de tráfico que realizan.
- Permiten **definir enlaces de reserva** hacia nodos cabecera de gestión de la red SDH que se usarán sólo cuando el enlace principal falle.
- Pueden **distribuir el tráfico entre dos líneas**, lo que produce un balanceado del tráfico.
- Permiten **definir una red segura y protegida** para arquitecturas con varios cabecera de gestión.

- Se pueden configurar con direcciones de red (direcciones **TCP/IP**) y por lo tanto **es posible configurarlos y gestionarlos remotamente**.
- Permiten **asignar prioridad** (coste) **a las diferentes líneas**, y por tanto definir criterios en la elección de los enrutamientos.
- Son mucho **más caros que los bridges** ya que el software que requieren es mucho más complejo. Además **necesitan memoria adicional**.
- Existen **pocos fabricantes de routers IS-IS** en el mercado. Entre ellos destacan CISCO y PROTEON.

Resumen

El **protocolo IS-IS** (*Intermediate System - Intermediate System*) es un protocolo de nivel 3 definido en en el standard **ISO/IEC 10589**.

El protocolo **IS-IS** se encarga de **crear y actualizar las tablas de enrutamiento**.

Las redes se componen de **sistemas intermedios** (IS) **y sistemas finales** (ES).

Los **ES** soportan las actividades de usuario y generan y reciben paquetes, pero no los enrutan.

Los **IS** interconectan subredes y transmiten paquetes entre ellas. Pueden generar, recibir y enrutar paquetes.

Tipos de subredes:

- Broadcast
- De topología general:
    - Enlaces multipunto
    - Enlaces permanentes punto a punto
    - Enlaces establecidos dinámicamente

Las direcciones de red **NSAP** identifican unívocamente cada estación dentro del dominio de red. El formato de direcciones utilizado en Telefónica es **ISO DCC NSAP**.

El protocolo IS-IS define una arquitectura jerárquica de dos niveles (nivel 1 y 2).

El **nivel 1** define las áreas y el enrutameiento dentro de éstas.

El **nivel 2** realiza la interconexión entre áreas

Los **bridges y routers** ofrecen soluciones para prolongar redes. En SDH se prolongan las redes de gestión, interconectando equipos entre lugares remotos mediante circuitos dedicados o WAN.

Ejercicios de Autoevaluación

Ejercicio 11

¿Cuál de las siguientes afirmaciones respecto al NSAP es cierta?

a. El selector es el mismo para todas las cabeceras.

b. La identificación del sistema no se puede repetir.

c. Debe ser único en todo el dominio de red.

Ejercicio 2

Los IS de nivel 2:

a. Solamente enrutan paquetes dentro su área.

b. Actúan como frontera IS entre diferentes áreas.

c. Sus tablas de enrutamiento se definen en el momento de crear la red.

Ejercicio 3

Se desea conectar dos conjuntos de equipos distantes con la única condición de que el ancho de banda del enlace entre ellos sea el mínimo posible y que el elemento que las interconecte sea configurable remotamente. ¿Qué tipo de equipo utilizaría?

a. Sólo routers.

b. Bridges o routers indistintamente.

c. Bridges en un extermo y routers en el otro.

SOLUCIONES A LOS EJERCICIOS

1.c, 2.b, 3.a

REFERENCIAS

UIT-T (Abr. 1991) G.703 – Características eléctricas y físicas de las interfaces digitales.

UIT-T (Mar. 1996) G.707 – Interfaz de nodo de red (NNI) para la jerarquía digital síncrona (SDH)

UIT-T (Nov. 1994) G.780 – Vocabulario de términos para redes y equipos de la jerarquía digital síncrona (SDH)

UIT-T (Abr. 1997) G.783 – Características de los bloques funcionales del equipo de la jerarquía digital síncrona (SDH)

UIT-T (Ene. 1994) G.784 – Gestión de la jerarquía digital síncrona (SDH)

UIT-T (Ago. 1996) G.810 – Definiciones y terminología para redes de sincronización

UIT-T (Mar. 1993) G.811 – Requisitos de sincronización en las salidas de relojes de referencia primaria adecuados para la operación plesiócrona en enlaces digitales internacionales

UIT-T (Mar. 1993) G.812 – Requisitos de sincronización en las salidas de relojes esclavos adecuados para la operación plesiócrona en enlaces digitales internacionales

UIT-T (Ago. 1996) G.813 – Requisitos de sincronización de los relojes esclavos de equipos SDH (SEC)

UIT-T (Mar. 1993) G.823 – El control de la fluctuación de fase y del wander en las redes digitales basadas en la jerarquía de 2048 Kb/s

UIT-T (Ago. 1996) G.826 – Parámetros y objetivos de característica de error para trayectos digitales internacionales de velocidad binaria constantes que funcionan a la velocidad primaria o a velocidades superiores

UIT-T (Jul. 1995) G.841 – Tipos y características de las arquitecturas de protección en redes SDH

UIT-T (May. 1995) G.957 – Interfaces ópticas para equipos y sistemas relacionados con la jerarquía digital síncrona (SDH)

UIT-T (Nov. 1994) G.958 – Sistemas de línea digitales basados en la jerarquía digital síncrona (SDH) para uso en fibras ópticas

SIGLAS Y ABREVIATURAS

ADM (*Add Drop Multiplexer*): Multiplexor con capacidad de extracción e inserción.

Agg (*Aggregate*): Agregado.

AIS (*Alarm Indication Signal*): Señal de indicación de alarma (SIA).

ALS (*Automatic LASER Shutdown*): Apagado automático del LASER.

AP (*Access Point*): Punto de Acceso.

APS (*Automatic Protección Switching*): Protección de sección de multiplexación.

ASAP (*Alarm Severity Assignment Profile*): Perfil de asignación de severidades de alarma.

AU (*Administrative Unit*): Unidad administrativa.

AU PJC (*Administrative Unit Pointer Justification Count*): Cuenta de ajustes de puntero en AU4.

BBE (*Background Block Error*): Error de bloque de fondo.

BBER (*Background Block Error Rate*): Tasa de errores de bloque de fondo.

BER (*Bit Error Rate*): Tasa de errores de bit.

BIP (*Bit Interleaving Parity*): Paridad de inserción de bits.

C (*Container*): Contenedor. C-4, C-3, C-12.

CAP (*Client Access Point*): Punto de acceso de cliente.

CCITT (*Comité Consultatif International Télégraphique et Téléphonique*): Comité Consultivo Internacional de Teléfonos y Telégrafos.

CMIP (*Common Management Information Protocol*): Protocolo común de información de gestión.

CMISE (*Common Management Information Service Element*): elemento común de servicio de información de gestión.

CP (*Conection Point*): Punto de conexión.

CPU (*Central Process Unit*): Unidad central de proceso.

CRU (*Clock Reference Unit*): Unidad de referencia de reloj.

CSES (*Consecutive Severely Errored Second*): Segundo consecutivo con muchos errores.

CT (*Craft Terminal*): Gestor local.

CTP (*Connection Termination Point*): Punto de terminación de conexión.

DCC (*Data Communication Channel*): Canal de comunicación de datos.

DCN (*Data Communications Network*): Red de comunicación de datos.

DMUX: Distribuidor multiplexor.

DNM (*Distributed Network Map*): Mapa distribuido de red.

DNU (*Do Not Use*): No usar.

DXC (*Digital Cross-Connect*): Distribuidor multiplexor.

EB (*Errored Block*): Bloque con error.

EBER (*Excesive Bit Error Rate*): tasa de error excesiva.

ECC (*Embedded Communication Channel*): Canal embebido de comunicaciones.

ECT (*Equipment Craft Terminal*): Gestor local del elemento de red.

EM (*Element Manager*): Gestor de elementos.

EML (*Element Management Layer*): Capa de gestión de elementos.

ENE (*Equivalent Network Element*): Elemento de red equivalente.

EPS (*Equipment Protection Switching*): Protección de equipo.

ES (*Errored Second*): Segundo con error.

ES (*End System*): Sistema final.

ESR (*Errored Second Ratio*): Tasa de segundos con error.

FAD (*Functional Access Domain*): Dominio de acceso a funciones.

FEBE (*Far-End Bit Error*): Error de bit remoto.

FERF (*Far-End Received Failure*): Fallo en el extremo remoto.

GNE (*Gateway Network Element*): Elemento cabecera de red.

GUI (*Graphical User Interfaz*): Interfaz gráfica de usuario.

HDLC (*High Data Link Control*): Control de alto nivel del enlace de datos.

HMI (*Human–Machine Inferface*): Interfaz hombre-máquina.

HO (*High Order*): Orden superior.

HOA (*High Order Assembler*): Ensamblador de orden superior. Función que está compuesta por las funciones de adaptación y de terminación de trayectos de orden superior.

HOPA (*High Order Path Adaptation*): Bloque funcional de adaptación de trayecto de orden superior.

HOPC (*High Order Path Conexión*): Bloque funcional de conexión de trayecto de orden superior.

HOPL (*High Order Path Layer*): Capa de trayectos de orden superior.

HOPT (*High Order Path Termination*): Bloque funcional de terminación de trayecto de orden superior.

HP: Hewlett Packard.

HP-VUE (*HP Visual User Environment*): Entorno visual de usuario de Hewlett Packard.

HP-OVw: HP Open View.

HW: Hardware.

IM (*Information Manager*): Gestor de información.

IP (*Internet Network Protocol*): Protocolo de red Internet.

IS-IS (*Intermediate Systems – Intermediate Systems*): Protocolo de red de sistemas intermedios.

ISO (*International Standards Organization*): Organización Internacional de Estándares.

ITU (*International Telecommunication Union*): Unión Internacional de las Telecomunicaciones.

JDP: Jerarquía Digital Plesiócrona.

SDH: Jerarquía Digital Síncrona.

LAN (*Local Area Net*work): Red de Área Local.

LAPD (*Link Access Procedure on D-Channel*): Procedimiento de acceso al enlace D.

LC (*Link Connection*): Conexión de enlace.

LO (*Low Order*): Orden inferior.

LOF (*Loss of Frame*): Pérdida de trama.

LOM (*Loss of Multiframe*): Pérdida de multitrama.

LOP (*Loss of Pointer*): Pérdida del puntero.

LOPA (*Low Order Path Adaptation*): Bloque funcional de adaptación de trayectos de orden inferior.

LOPC (*Low Order Path Connection*): Bloque funcional de conexión de trayectos de orden inferior.

LOPL (*Low Order Path Layer*): Capa de trayectos de orden inferior.

LOPT (*Low Order Path Termination*): Bloque funcional de terminación de trayectos de orden inferior.

LOS (*Loss of Signal*): Pérdida de señal.

MD (*Mediation Device*): Dispositivo de mediación.

MIB (*Management Information Base*): Base de información de gestión.

MM (*Maintenance Memory*): Memoria de mantenimiento.

MS (*Multiplex Section*): Sección de multiplexación.

MSOH (*Multiplex Section Overhead*): Tara o cabecera de la sección de multiplexación.

MSP (*Multiplex Section Protection*): Bloque funcional de protección de la sección de multiplexación o Protección de la sección de multiplexación.

MSL (*Multiplex Section Layer*): Capa de red de sección de multiplexación.

MS-SPRing (*Multiplex Section Self Protected Ring*): Protección compartida de sección de multiplexación.

MST (*Multiplex Section Termination*): Bloque funcional de terminación de la sección de multiplexación

MSTP (*Multiplex Section TP*): Punto de terminación de sección de multiplexación

NAD (*Network Access Domain*): Dominio de acceso a red.

NAP (*Network Access Point*): Punto de acceso a la red.

NE (*Network element*): Elemento de Red.

NM (*Network Manager*): Gestor de red.

NML (*Network Management Layer*): Capa de gestión de red.

NNI (*Network Node Interface*): Interfaz de nodo de Red.

NR (*Network Release*): Versión de Red, entrega de Red o Release de Red

NSAP (*Network Service Access Point*): Punto de acceso de a los servicios de la red.

OFS (*Out of Frame Second*): Segundo de pérdida de trama.

OH (*Overhead*): Tara, Cabecera.

OOS (*Out of Service, Disabled*): Fuera de servicio.

OPE (*Permanent Operator*): Operador permanente.

OS (*Operation System*): Sistema de operación. Gestor.

OSF (*Operation System Function*): Función del sistema de operación.

OSI (*Open System Interconnection*): Interconexión de sistemas abiertos.

PDH (*Plesiochronous Digital Hierarchy*): Jerarquía digital plesiócrona.

PJC (*Pointer Justification Counter*): Contador de movimientos de puntero.

PM (*Performance Monitoring*): Monitorización de prestaciones o medida de calidad.

PMTP (*Performance Monitoring Termination Point*): Punto de terminación de monitorización de prestaciones.

POH (*Path Overhead*): Tara o cabecera de trayecto.

PPI (*Plesiochronous Phisical Interface*): Interfaz física plesiócrona.

PPS (*Path Protection Switching*): Conmutación de protección de trayecto.

PRC (*Primary Reference Clock*): Reloj de referencia primario.

PSC (*Protection Switch Count*): Cuenta de conmutaciones de protección.

PSD (*Protection Switch Duration*): Duración de las conmutaciones de protección.

QA (*Q Adaptor*): Adaptador Q.

QAF (*Q Adapting Function*): Función de adaptación Q.

RAM (*Random Access Memory*): Memoria de acceso aleatorio.

RDI (*Remote Defect Indication*): Indicación de fallo remoto.

RDSI: Red Digital de Servicios Integrados.

REI (*Remote Error Indication*): Indicación de error remoto.

RS (*Regenerator Section*): Sección de regeneración.

RSOH (*Regenerator Section Overhead*): Tara o cabecera de la Sección de regeneración.

RST (*Regenerator Section Termination*): Bloque funcional de terminación de la sección de regeneración

RSTP (*Regenerator Section TP*): Punto de terminación de sección de regeneración.

SD (*Signal Degraded*): Señal degradada.

SDH (*Synchronous Digital Hierarchy*): Jerarquía Digital Síncrona

SEC (*Synchronization Equipment Clock*): Reloj de sincronización de equipo.

SES (*Severely Errored Seconds*): Segundos con muchos errores.

SESR (*Severely Errored Seconds Ratio*): Tasa de segundos con muchos errores.

SETG (*Synchronous Equipment Timing Generator*): Generador de temporización de un equipo síncrono.

SLM (*Signal Label Mismatch*): Etiqueta de señal incorrecta.

SNML (*SDH Network or Sub-Network Management Layer*): Capa de gestión de red SDH o capa de gestión de subred.

SNC (*Sub-Network Connection*): Conexión de subred.

SNC/I (*Intrusive SNCP*): Protección de subred intrusiva.

SNC/N (*Non Intrusive SNCP*): Protección de subred no intrusiva.

SNCP (*Sub-Network Connection Protection*): Protección de subred.

SPI (*Synchronous Phisical Interface*): Interfaz física síncrona.

SSM (*Synchronous Status Message or Marker*): Mensaje o marcador de estado de la sincronización.

SSU-L y SSU-T (*Local and Transit Station Synchronization Unit*): Unidad de sincronización de central, local y de tránsito.

STM (*Synchronous Transport Module*): Módulo de transporte síncrono.

SW: Software.

TCA (*Threshold Crossing Alarm*): alarma por cruce de umbral.

TCP (*Termination Connection Point*): Punto de terminación de conexión.

TCP-IP (*Transmission Control Protocol–Internet Protocol*): Protocolo de control de transmisión.

TIM (*Trace Identifier Mismatch*): Discordancia del identificador de trayecto.

TMN (*Telecommunication Network Management*): Red de gestión de las telecomunicaciones.

TP (*Termination Point*): Punto de terminación.

TSF(E/I): Terminal Síncrono Flexible con capacidad de extracción e inserción.

TTP (*Trail Termination Point*): Punto de terminación de trayecto.

TU (*Tributary Unit*): Unidad de tributario.

TUG (*Tributary Unit Group*): Grupo de unidades de tributario.

U (*Unequipped*): No equipado.

UAS (*Unavailable Second*): Segundo de indisponibilidad.

UAT (*Unavailable Time*): Tiempo de indisponibilidad.

UIT (*Union International de Telecomunications*): Unión internacional de las Telecomunicaciones.

UPA (*Unavailable Path Alarm*): Alarma de trayecto indisponible.

URU (*Underlying Resource Unavailable*): Recurso de respaldo indisponible.

USM (*User Service Manager*): Gestor de servios de usuario.

VC (*Virtual Container*): Contenedor virtual.

WAN (*Wide Area Network*): Red de área extensa

WS (*Workstation*): Estación de trabajo.

WTR (*Wait to Restore*): Tiempo de espera para revertir.

XC (Cross-Connection): Conexión.

Fin