ESCUELA POLITECNICA NACIONAL

FACULTAD DE INGENIERIA ELECTRICA

"MECANISMOS DE PROTECCION EN REDES DIGITALES SINCRONICAS SDH"

TESIS PREVIA A LA OBTENCION DEL TITULO DE INGENIERO EN ELECTRONICA Y TELECOMUNICACIONES

Rodrigo Manuel Aguirre Vidal

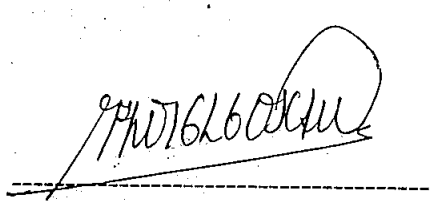
Quito, Julio de 1998

AGRADECIMIENTO

En especial al Ing. Pablo Hidalgo Lascano por su acertada dirección en el desarrollo de este trabajo, y al Ing. Fabio González González por su valiosa colaboración para la culminación del mismo.

A mis padres y hermanos

Certifico que la presente tesis ha sido elaborada en su totalidad por el Sr. Rodrigo Aguirre Vidal.



Ing. Pablo Hidalgo Lascano

Director de Tesis

TABLA DE CONTENIDOS

TABLA DE CONTENIDOS

Introducción

CAPITULO I

FUNDAMENTOS TEORICOS Y ESTRUCTURA DE LA JERARQUIA DIGITAL SINCRONICA (SDH)

1.1 Conceptos sobre Jerarquía Digital Sincrónica (SDH) 1

1.1.1 Estructura de la trama STM–1 1
1.1.2 Estructura del puntero de la AU-n 3
1.1.3 Justificación de trama en la AU-n 4
1.1.4 Unidades Tributarias 5
1.1.4.1 Unidad tributaria TU-3 6
1.1.4.2 Unidad Tributaria TU-12 7
1.1.5 Modalidades de transporte de los VC de orden inferior 9
1.1.6 Multiplexación 9
1.1.6.1 Formación de la TUG-2 9
1.1.6.2 Formación de la TUG-3 10
1.1.6.3 Formación del VC-4 a partir del TUG-3 12
1.1.6.4 Concatenación de Unidades Administrativas AU-4 12
1.1.7 Estructura del *overhead* de sección (SOH) y de recorrido (POH) 13
1.1.7.1 Secciones de regeneración, múltiplex y de recorrido 13
1.1.7.2 Descripción de los bytes de la SOH 14
1.1.7.3 Descripción del *overhead* de la sección de recorrido (POH) 17
1.1.8 Mapeo 19
1.1.8.1 Mapeo de 140 Mb/s en un VC-4 19
1.1.8.2 Mapeo de 34 Mb/s en un VC-3 21
1.1.8.3 Mapeo de 2 Mb/s en el VC-12 23

1.2 Equipos sincrónicos 24

1.2.1 Modelos de aparatos sincrónicos 26
1.2.1.1 Multiplexor terminal y de inserción/extracción 27
1.2.1.2 Aparatos de conmutación (*Digital Cross Connect* - DXC) 28
1.2.1.3 Aparatos SDH basados en sistemas de radio relés 29
1.2.2 Descripción funcional a nivel de bloques 30

CAPITULO II

ANILLOS SINCRONICOS EN REDES SDH

2.1 Clases de anillos **33**

2.1.1 Anillo unidireccional 33

2.1.2 Anillo bidireccional 33

2.2 Tipos de tráfico **34**

2.2.1 Tráfico entre nodos adyacentes 34

2.2.2 Tráfico uniforme 35

2.2.3 Tráfico con un nodo de concentración (*single hub*) 35

2.2.4 Tráfico con doble nodo de concentración (*double hub*) 35

2.3 Capacidad de tráfico **35**

2.3.1 Tráfico entre nodos adyacentes 36

2.3.2 Tráfico uniforme 37

2.3.3 Tráfico con un nodo de concentración 39

2.3.4 Tráfico con dos nodos de concentración 40

CAPITULO III

MECANISMOS DE PROTECCION EN REDES DIGITALES SINCRONICAS

3.1 Introducción **42**

3.2 Protección a nivel de sección múltiplex (MSP) **42**

3.2.1 Protección lineal 42

3.2.1.1 Proceso de conmutación automática 42

3.2.1.2 Protección 1:n bidireccional 45

3.2.1.3 Protección 1:n unidireccional 47

3.2.1.4 Protección 1+1 unidireccional 47

3.2.1.5 Protección 1+1 bidireccional compatible con 1:n bidireccional 49

3.2.1.6 Protección 1+1 bidireccional optimizada para una red con conmutación 50

predominantemente 1+1 bidireccional 50

3.2.2 Anillo de protección compartida (*SPRing*) 51

3.2.2.1 Anillo de protección compartida a dos fibras 51

3.2.2.2 Anillo de protección compartida a cuatro fibras 54

3.2.2.3 Protección por conmutación automática (APS) para anillos de protección 55

compartida 55

3.2.3 Anillo de protección dedicada (*DPRing*) 60
3.2.3.1 Anillo de protección dedicada a dos fibras 60
3.2.3.2 Anillo de protección decicada a cuatro fibras 62
3.2.3.3 Protección por conmutación automática (APS) para anillos de protección dedicada 63

3.3 Protección a nivel de recorrido 64

3.3.1 Protección a nivel de contenedor virtual (VC) 67
3.3.1.1 Protección por conmutación automática (APS) 70
3.3.2 Protección a nivel de conexión de sub-red (*Sub-network connection SNC*) 73
3.3.2.1 Protección por conmutación automática (APS) 74

CAPITULO IV

APLICACION DE LOS MECANISMOS DE PROTECCION EN REDES DIGITALES SINCRONICAS

4.1 Consideraciones generales 76

4.1.1 Evolución de PDH a SDH 76
4.1.2 Estructura de una red de transporte 77

4.2. Consideraciones generales sobre re-enrutamiento 78

4.2.1 Introducción 78
4.2.2 Algoritmo de *Floyd-Warshall* 80

4.3 Ejemplo de aplicación 83

4.3.1 Objetivos generales en el diseño de una red de transporte SDH 83
4.3.2 Funciones de la red de transporte SDH 83
4.3.3 Planificación general de una red de transporte SDH 83
4.3.4 Desarrollo del ejemplo de aplicación 84
4.3.4.1 Matriz de tráfico 84
4.3.4.2 Arquitectura 86
4.3.4.3 Enrutamiento de tráfico 86
4.3.4.4 Capacidad de la red 90
4.3.4.5 Mecanismos de protección 95
4.3.4.6 Agrupamiento de tráfico 130
4.3.4.7 Equipamiento 131
4.3.4.8 Disponibilidad y confiabilidad 133

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES 144

ANEXOS

1. Puntos de referencia Sn de la SEMF en los aparatos SDH.

2 a. Descripción funcional de los aparatos sincrónicos a nivel de bloques.

2 b. Diagrama general de procesamiento de alarmas y señales en los aparatos SDH.

3. "RUTAS.EXE" Programa para el enrutamiento inicial y cálculo de la carga de tráfico en la red.

4. Lista de abreviaturas utilizadas.

BIBLIOGRAFIA

INTRODUCCION

Actualmente se puede decir que estamos inmersos en un mar de redes de telecomunicaciones, los mismos que ofrecen una amplísima gama de servicios, ya sea en el ámbito bancario (cajeros automáticos, transferencias, control de fondos para tarjetas de crédito, etc.), de tipo comercial (reservación de asientos en las aerolíneas, hoteles), en el hogar (correo electrónico), etc. La demanda crece tan rápidamente que las redes actuales necesitan sistemas cada vez de mayor velocidad para satisfacerla.

Dentro de esta tendencia hacia la comunicación masiva de alta velocidad, surge la necesidad de actualización de las redes de transporte telecomunicaciones existentes, las cuales son las verdaderas portadoras de la información entre los usuarios. Inicialmente, los sistemas de transmisión de radio analógicos fueron reemplazados por radios de tipo digital basados en la Jerarquía Digital Plesiócrona (PDH); los sistemas PDH han tenido bastante éxito y han logrado incrementar enormemente la velocidad, llegando en algunas ocasiones a transmitir flujos de centenas de megabits por segundo. Sin embargo, los sistemas PDH han enfrentado algunas inconveniencias debido a la múltiple procedencia de los aparatos utilizados y las consecuentes incompatibilidades entre ellos al momento de integrar una red de telecomunicaciones.

Algunas de las características no provistas por los sistemas PDH son la utilización de interfaces estandarizados, la flexibilidad de configuración de los aparatos, la integración en un solo sistema de telesupervisión y telecontrol, etc. Estas son algunas de las mayores razones por las que surgieron los sistemas basados en la Jerarquía Digital Sincrónica (SDH), donde una estructura básica de transporte llamada STM-1, puede ser continuamente multiplexada hasta alcanzar velocidades de algunos gigabits por segundo en la actualidad. Tal cantidad de información puede ser transmitida principalmente a través de fibras ópticas y en algunas ocasiones vía radio.

Los sistemas SDH tuvieron su origen en los sistemas SONET (*Synchronous Optical Network*) que surgieron hace varios años en Norteamérica, y sobre la base de los cuales se conformaron los nuevos estándares de lo que hoy es la Jerarquía Digital Sincrónica SDH.

El presente trabajo pretende dar una visión general de la estructura de las redes de transporte de telecomunicaciones basadas en la Jerarquía Digital Sincrónica SDH,

poniendo especial énfasis en los "mecanismos de protección" disponibles actualmente, o en vías de definición de los organismos reguladores de telecomunicaciones (ITU y ETSI). Estos mecanismos de protección se basan en la sustitución de trayectorias cuya calidad de información presenta signos de degradación o han sido interrumpidas; de esta manera, se trata de conseguir que la disponibilidad de servicio sea la máxima posible. Adicionalmente, estos mecanismos son necesarios cuando existen requerimientos de los administradores de telecomunicaciones y se necesita re-enrutar la información por motivo de mantenimiento, pruebas de aparatos, reconfiguraciones de la red o actualizaciones de la misma.

Para cumplir con tales objetivos, en el Capítulo I se presenta una introducción a lo que constituye la filosofía SDH, su estructura y modos de acoplarse con las señales PDH existentes. Además, se da una breve revisión de la estructura de bloques de los aparatos sincrónicos existentes, y cuya descripción en detalle se adjunta en el Anexo # 2.

El Capítulo II trata sobre los tipos de configuraciones existentes para los anillos y los más comunes modelos de tráfico que se dan en una red de telecomunicaciones. Aquí se establecen las relaciones para evaluar la capacidad necesaria de la red para satisfacer la demanda de tráfico y la capacidad necesaria para la protección de la misma.

La parte medular de este trabajo, es decir los mecanismos de protección propiamente dichos se describen en detalle en el Capítulo III en sus diversas configuraciones. También se establecen los criterios de conmutación y se presentan algunas normas generales para su aplicación.

Todos los conocimientos anteriormente propuestos se afirman con un ejemplo de aplicación presentado en el Capítulo IV, donde se toma como base la información sobre la demanda de tráfico requerida por un operador de telecomunicaciones celulares. Para el desarrollo de este ejemplo se presenta inicialmente todos los pasos a seguirse para la planificación de una red de transporte de telecomunicaciones. A partir de la matriz ya proyectada hacia el futuro, se define la arquitectura de la red y se evalúa la capacidad de tráfico necesaria para la demanda y la protección. Otra de las etapas de planificación incluye una breve introducción al enrutamiento inicial de tráfico dentro de la red, para lo cual se creó un sencillo programa llamado "RUTAS.EXE"; la función de este programa es encontrar las rutas más cortas entre los nodos y la carga de tráfico que soportará la

red con dicha arquitectura o configuración. Los mecanismos de protección son entonces aplicados, describiendo el proceso de conmutación para cada uno de ellos. Se presenta algunas ideas sobre el agrupamiento de tráfico en la red y el tipo de aparatos que se debería utilizar para su puesta en marcha. Finalmente, sobre la base de la configuración de los aparatos propuesta, se procede con la evaluación de los parámetros de confiabilidad y disponibilidad para una de las rutas que atraviesa toda la red; se considera una trayectoria normal (sin protección) y la trayectoria protegida (una vez que los mecanismos de protección han sido activados) y se presentan los resultados.

El Capítulo V presenta una visión crítica de la red del ejemplo del capítulo IV, se señalan sus puntos débiles y se recomienda algunas ideas para mejorar su comportamiento. También se sugiere ideas sobre la utilización del programa para obtener mejores resultados.

El listado del programa "RUTAS. EXE", con su estructura e instrucciones de utilización se adjunta en el Anexo # 3. Para una mejor comprensión, en el Anexo # 4 se detalla una lista de abreviaturas utilizadas en el presente trabajo.

Se espera que el presente trabajo brinde realmente una clara introducción hacia este campo de las redes de transporte de telecomunicaciones, cuyo avance es realmente rápido, y que por tal razón obliga a realizar una continua búsqueda de fuentes de información, muchas veces fuera de alcance en nuestro país.

CAPITULO I

Fundamentos teóricos y estructura de la Jerarquía Digital Sincrónica (SDH)

FUNDAMENTOS TEORICOS Y ESTRUCTURA DE LA JERARQUIA DIGITAL SINCRONICA (SDH)

1.1 CONCEPTOS SOBRE JERARQUIA DIGITAL SINCRONICA (SDH)

1.1.1 Estructura de la trama STM–1

La estructura básica en la SDH se denomina STM-1, que significa Módulo de Transporte Sincrónico de Nivel 1. Es a partir de ésta que, mediante la acumulación ordenada de octetos, se construyen los módulos de transporte sincrónico de nivel superior STM-N (N = 1, 4, 16, 64,...).

Como se muestra en la figura 1.1, la trama STM-1 está compuesta de 9 hileras de 270 bytes cada una. Siendo la frecuencia de muestreo de 8 KHz, el ritmo de transmisión será:

$$R_{STM\text{-}1} = 8 \times (9 \times 270) \times (8 \times 10^3) = 155\,520 \text{ Mb/s.}$$

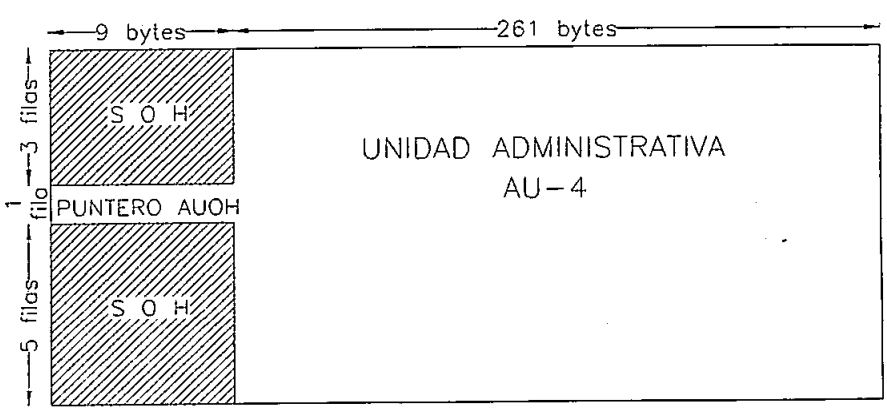


Fig. 1.1 Trama STM-1.

La trama STM-1 se compone de:

1. **SOH (*Section Overhead*)**: Sección dedicada a la transmisión de la información de servicio. Ocupa los 9 primeros bytes de todas las hileras, a excepción de la cuarta.
2. **Unidad administrativa (AU):** Se encarga del transporte e identificación de la carga útil a transmitirse, denominada contenedor virtual (VC) (Ver figura 1.2). La AU se compone de 261 bytes de todas las hileras (VC), más 9 bytes de la cuarta hilera que corresponde al puntero de trama, también denominado puntero de la AUOH (*Administrative Unit Overhead*). El puntero señala la dirección de inicio de la información útil (Byte **J1** de la figura 1.2). Un conjunto de N unidades administrativas forman una Unidad Administrativa de Grupo (AUG) que, junto a la SOH, forman la nueva trama STM-N.

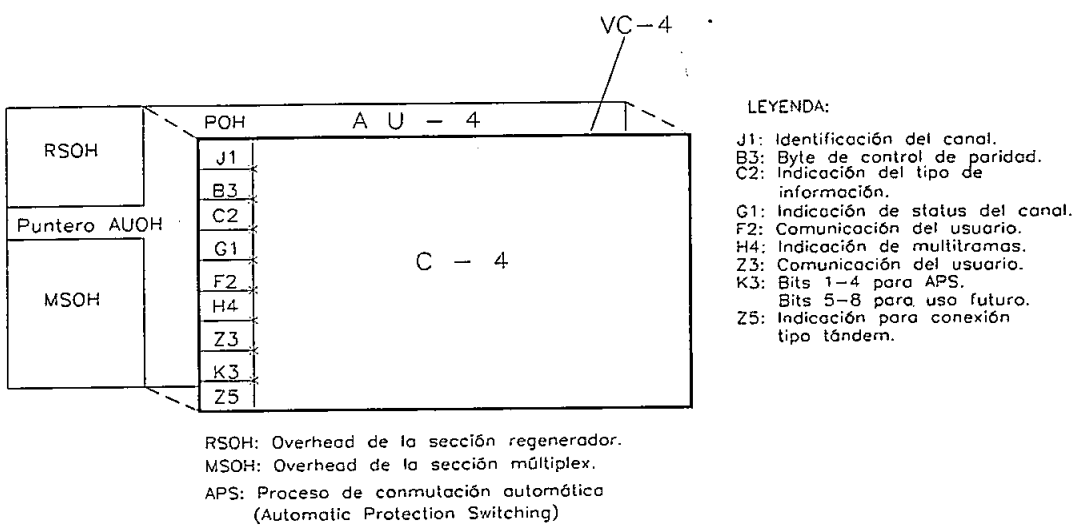


Fig.1.2 Unidad Administrativa AU-4 y Contenedor Virtual VC-4.

Contenedor Virtual (VC-4)

Existen dos posibilidades de formación de esta estructura:

1) Directamente formada por un contenedor de alto nivel, en este caso llamado C-4 (flujos a 140 Mb/s).
2) Indirectamente por contenedores de bajo nivel C-3, C-2, C-12, C-11 (45, 34, 6, 2 o 1.5 Mb/s) reagrupados. previamente en otra estructura transitoria llamada Unidad Tributaria de Grupo (TUG). La figura 1.3 muestra los flujos de multiplexación correspondientes.

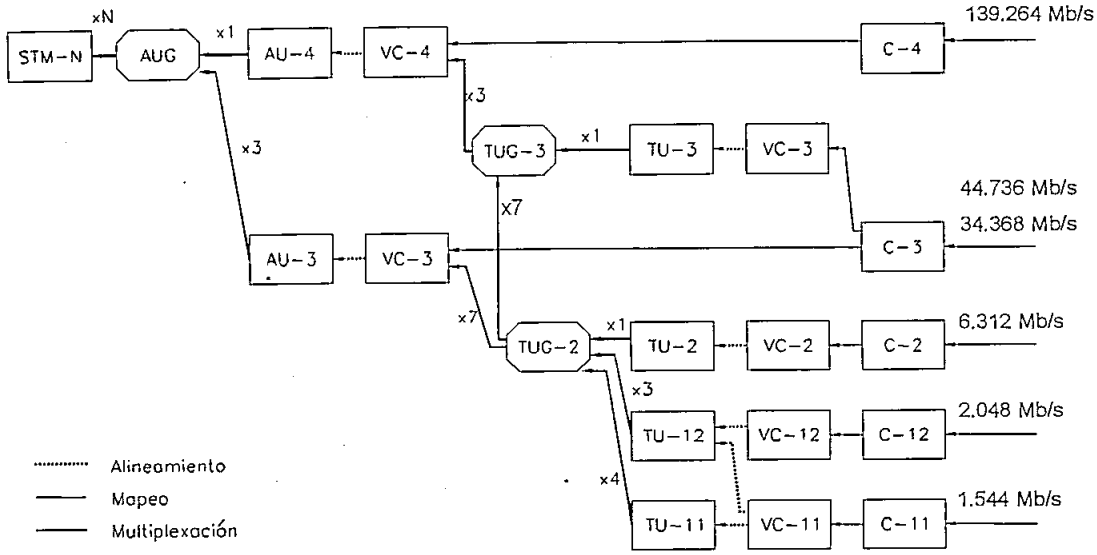


Fig.1.3 Estructura de la multiplexación en SDH[1].

Si bien la ITU-T presenta dos posibilidades de formar la AUG, la ETSI (*European Telecommunications Standardization Institute*) ha decidido adoptar aquella formada a partir del VC-4, que es la misma que se está aplicando en América Latina. Bajo el mismo criterio, el VC-11 es insertado directamente en la TU-12 en lugar de ir a la TU-11 como lo recomienda la ITU-T en su recomendación G.707.

La interconexión de redes basadas en la AU-3 con aquellas que se basan en AU-4, implica que la primera debe demultiplexar la AU-3 hasta el nivel de TUG-2 o de VC-3, de acuerdo al tipo de carga, y luego multiplexarla vía TU-3, TGU-3 y VC-4.

1.1.2 Estructura del puntero de la AU-n

El puntero tiene como función principal indicar la dirección de inicio de la información útil dentro del VC-n. Para cumplir con este objetivo, el puntero dispone de 3 bytes (**H1**, **H2**, **H3**) que están dentro de los 9 bytes de la AUOH (Ver figuras 1.2 y 1.4).

El seguimiento de la posición de inicio de la información implica que el puntero debe adaptar la diferencia en fase entre el VC-n y la SOH mediante la justificación (positiva o negativa) de la trama. En el caso de la estructura AU-4, los bytes **H1** y **H2** contienen el puntero en sí, mientras que los 3 bytes **H3** se utilizan para la justificación

[1] ITU-T, Rec. G.707 Network Node Interface For The Synchronous Digital Hierarchy (SDH), Geneve, March, 1996.

negativa. Para la justificación positiva se utilizan los 3 bytes de la VC-n ubicados a la derecha de los bytes **H3** (Ver figura 1.4).

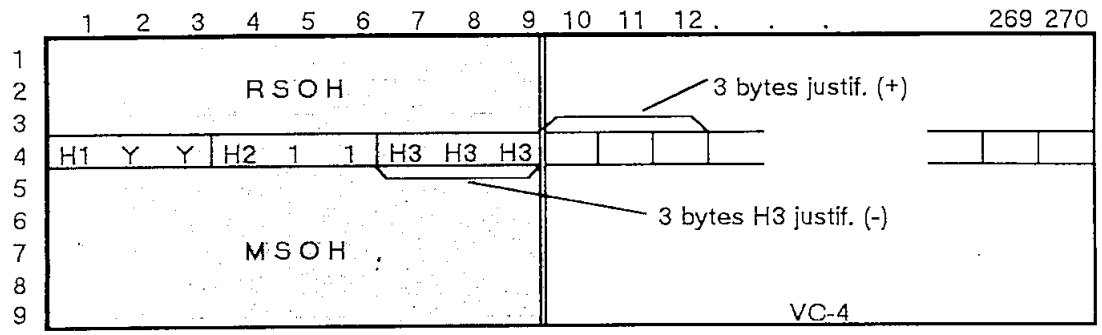
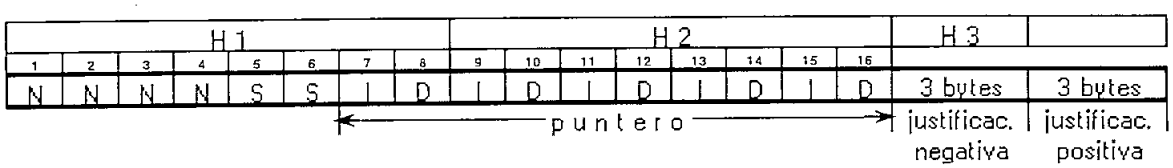


Fig. 1.4 Puntero de la AU-4.



N: Nueva señal **1001** Insertada
0110 No insertada.
SS: Valor de **10** para AU-4, AU-3, TU-3

I: Incremento.
D: Decremento.
Código de concatenación: 1001SS111111111

Fig. 1.5 Estructura del puntero de la AU-4 y TU-3.

1.1.3 Justificación de trama en la AU-n

Cuando la frecuencia de AUG es mayor que la frecuencia del VC, el puntero debe ser desplazado en el tiempo y su valor incrementado en una unidad para apuntar a la nueva dirección de inicio del VC. Para justificar este retardo del VC, los 3 bytes siguientes a **H3** (Figura 1.5) son utilizados como relleno de la trama, a la vez que los bytes **I** del puntero son invertidos indicando que se va a producir un incremento del puntero o lo que es igual, una **justificación positiva**. Si por el contrario, la frecuencia de la AUG es menor que la del VC, se produce la **justificación negativa** que implica la utilización de los 3 bytes **H3** y el decremento del puntero en una unidad; los bytes **D** son invertidos indicando que la justificación negativa está en proceso y que el valor del puntero será reducido en una unidad en la siguiente trama.

La justificación implica la adición o préstamo de 3 bytes, por lo tanto el puntero indicará la nueva dirección de inicio de información 3 bytes hacia adelante o hacia atrás.

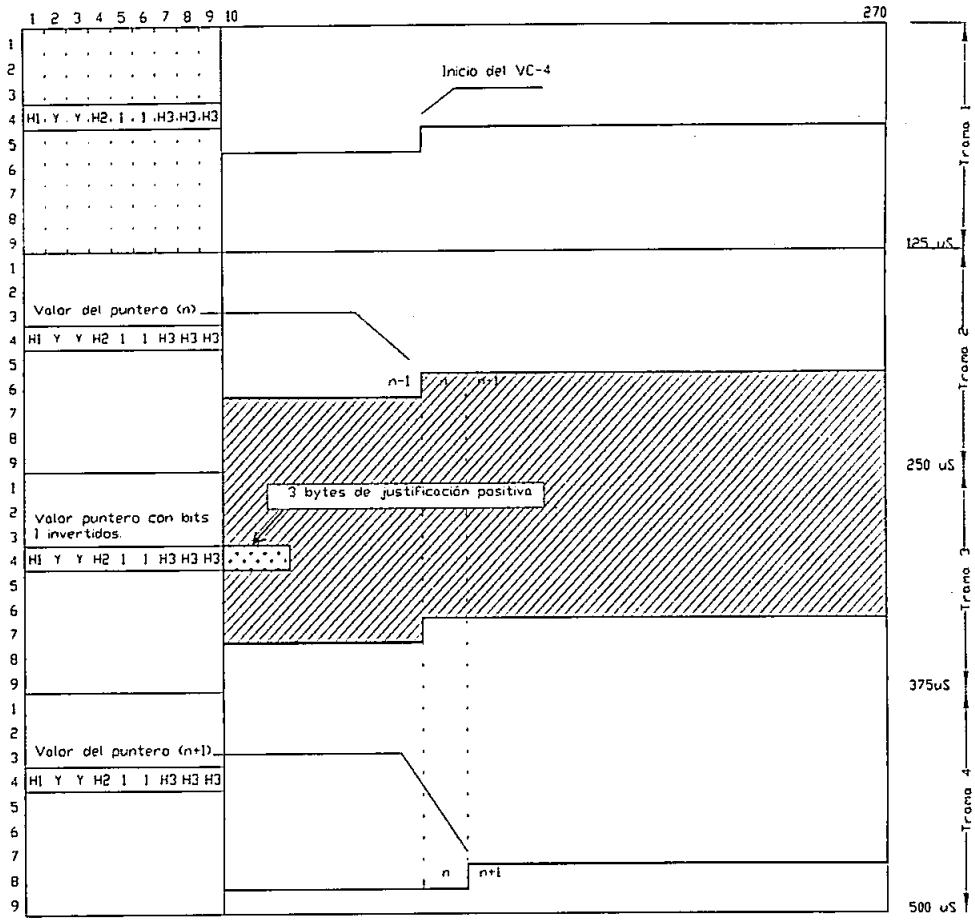


Fig. 1.6 Justificación Positiva[2].

1.1.4 Unidades Tributarias

Las unidades tributarias nacen con la necesidad de cargar el VC-4 no solo con una carga C-4 (140 Mb/s), si no con varias estructuras de transporte de menor capacidad como son los C-3, C-2, C-12 y C-11 (Ver la figura 1.3).

Obviamente, estas unidades pequeñas necesitan de punteros para indicar el inicio de la información, además de ciertas señales de sincronización que les permitan ser identificadas en cualquier momento de tal manera que puedan "flotar" libremente en estructuras de orden superior.

En el presente trabajo se analizará la estructura de las unidades tributarias TU-3

[2] La justificación negativa se diferencia solamente en el uso de los 3 bytes H3 del AUOH y decremento del puntero a n-1.

y TU-12 formadas por contenedores de 34 Mb/s y 2 Mb/s respectivamente de acuerdo con las recomendaciones ETSI.

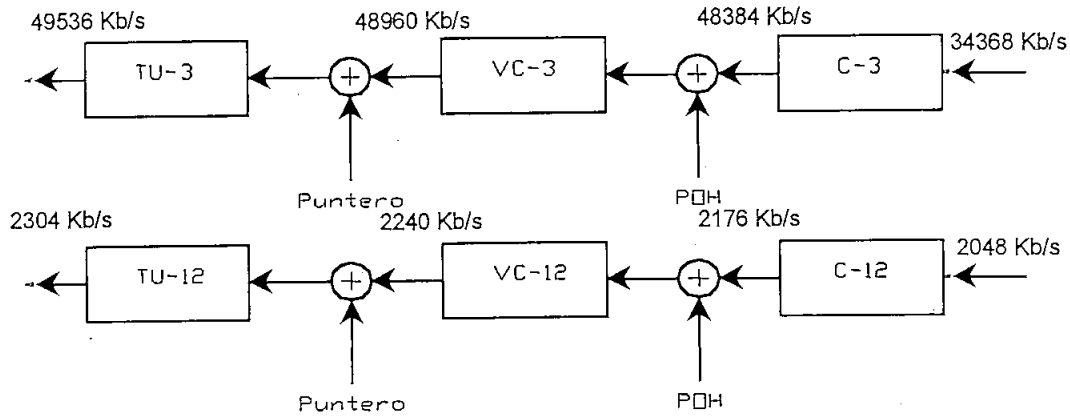


Fig. 1.7 Esquema de composición de las Unidades Tributarias.

1.1.4.1 Unidad tributaria TU-3

Se compone de 9 filas por 86 columnas distribuidas como se indica en la figura 1.8. La primera columna contiene los bytes **H1**, **H2**, **H3** que representan el puntero de la unidad TU-3. En la parte inferior existen seis bytes utilizados para justificación o relleno fijo de la trama. De la estructura de la TU-3 se determina que su capacidad de transporte es:

$$C_{TU\text{-}3} = 8\ [\text{bits/byte}] \times (3 + 6 + 85 \times 9)[\text{bytes}] \times 8.0\ [\text{KHz}] = 49\ 536\ \text{Kb/s}$$

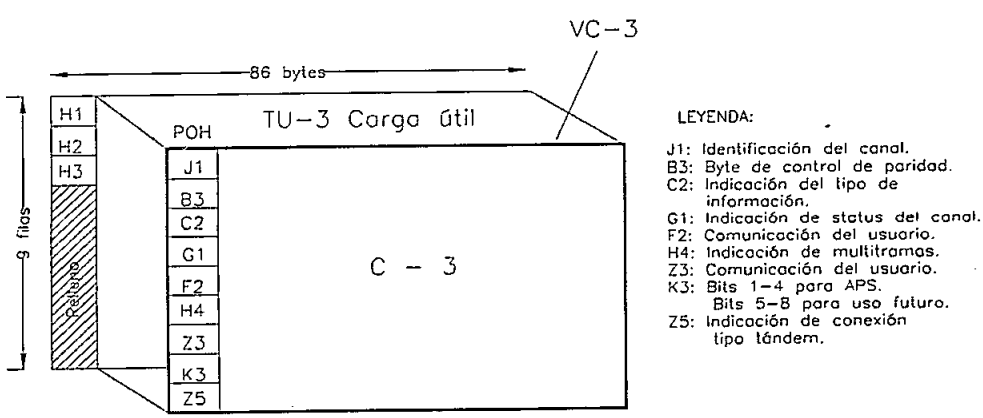


Fig.1.8 Estructura de la Unidad Tributaria TU-3.

1.1.4.2 Unidad Tributaria TU-12

La figura 1.9 a) muestra el proceso de formación de la unidad tributaria TU-12 a partir del contenedor C-12. Como paso inicial, el contenedor C-12 (34 bytes) se une al byte **V5** (POH) para formar el contenedor virtual VC-12 con un total de 35 bytes. Este contenedor virtual, junto con los bytes **V1**, **V2**, **V3**, y **V4** forman la unidad tributaria TU-12. Nótese que los bytes **V1** a **V4**, así como el contenedor virtual VC-12, son distribuidos en 4 diferentes tramas de 125 μs cada una.

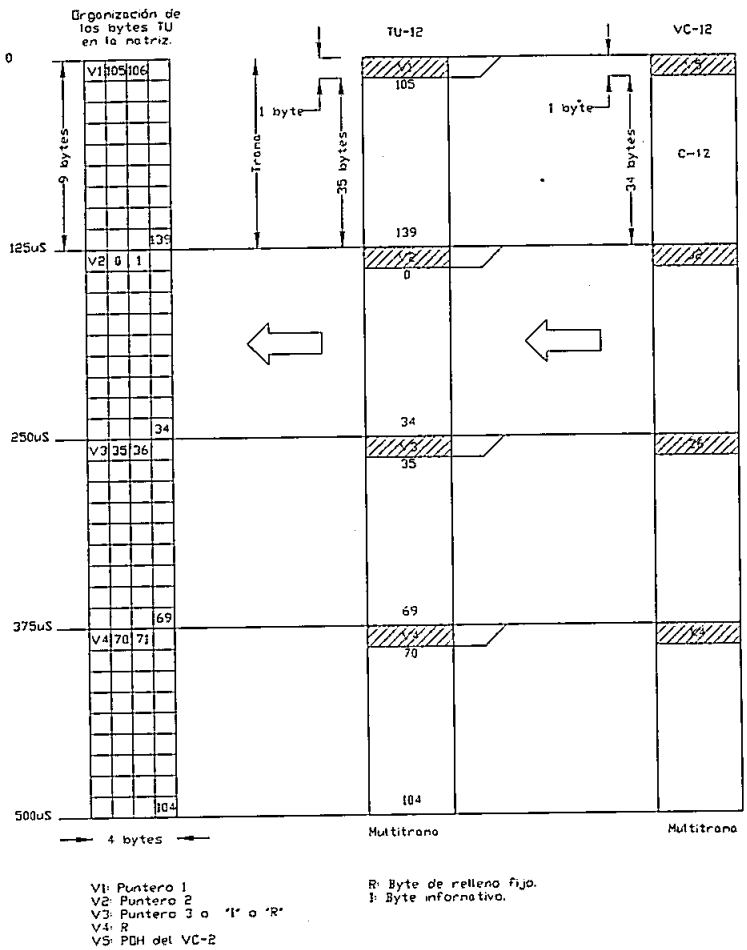


Fig. 1.9 a) Unidad tributaria TU-12

El contenedor C-12 está compuesto por 34 bytes, por lo que su capacidad está determinada por:

C_{C-12} = 8 [bits/byte] x 34 [bytes] x 8.0 [KHz] = 2 176 Kb/s.

La distribución de los bytes del VC-12 en 4 tramas implica que la frecuencia de inserción en la trama STM-1 será reducida 4 veces, es decir, a una velocidad de 2.0 KHz. Los cálculos de la velocidad de transmisión para el VC-12 se detallan a continuación:

- 34 bytes del VC-12 por cada trama (existe un total de 4 tramas).
- 4 bytes del POH (**V5**, **J2**, **Z6** y **K4**).

Por lo tanto, la velocidad de transmisión del VC-12 es:

$$C_{VC\text{-}12} = 8\ [\text{bits/byte}] \times (4\ [\text{bytes}] + 4\ [\text{tramas}] \times 34\ [\text{bytes/trama}]) \times 2.0\ [\text{KHz}]$$

$$C_{VC\text{-}12} = 2\ 240\ \text{Kb/s}.$$

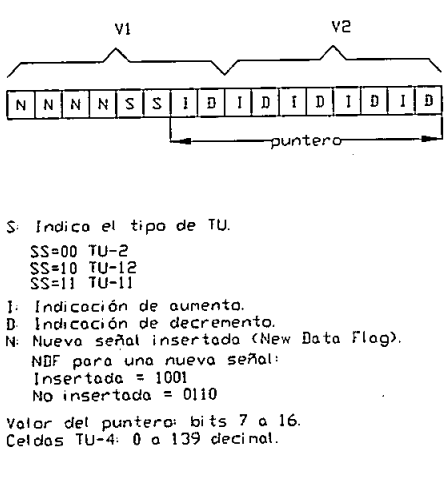
De manera análoga al caso del VC-12, y considerando la inclusión de los bytes **V1**, **V2**, **V3** y **V4**, se obtiene la siguiente situación para la TU-12:

- 35 bytes por cada trama (existe un total de 4 tramas).
- 4 bytes **V1**, **V2**, **V3** y **V4**.

Por lo tanto, la velocidad de transmisión de la TU-12 es:

$$C_{TU\text{-}12} = 8[\text{bits/byte}] \times (4\ [\text{bytes}] + 4[\text{tramas}] \times 35\ [\text{bytes/trama}]) \times 2.0\ [\text{KHz}]$$

$$C_{TU\text{-}12} = 2\ 304\ \text{Kb/s}.$$



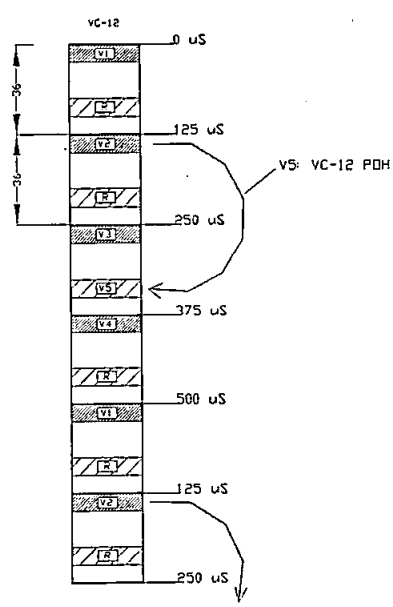


Fig. 1.9 b) Estructura del puntero de la TU-12.

La figura 1.9 b) muestra la configuración del puntero de la TU-12, cuyo contenido está distribuido en 4 tramas STM-1 consecutivas. El valor real del puntero está dado por los bytes **V1** y **V2** y contiene la dirección de ubicación del byte **V5**, el mismo que representa el primer byte del contenedor C-12. El puntero puede tomar valores de las celdas desde 0 a 139 dentro de las 4 tramas.

1.1.5 Modalidades de transporte de los VC de orden inferior

Existen dos modalidades de transporte de los contenedores virtuales VC-11, VC-12, VC-2 por medio de las unidades tributarias TU-12, TU-2 a través de la red SDH.

1. Modo flotante

Es análogo a lo visto anteriormente para el VC-4 y VC-3 con la técnica de los punteros. Estos permiten las fluctuaciones del VC dentro de la TU desvinculándolos de las diferencias en fase.

2. Modo enclavado

Obliga al VC a asumir una posición fija dentro de la TU. En este caso las celdas temporales asignadas a los punteros de la TU, así como las celdas temporales del VC asignadas para la transmisión del POH correspondiente, carecen de significado y se convierten en celdas de relleno fijo.

1.1.6 Multiplexación

Existen dos niveles de multiplexación: uno a nivel de unidades tributarias y otro a nivel de unidades administrativas. En ambos casos pueden distinguirse claramente dos entidades, una entidad de transporte (TUG o AUG) y otra entidad de carga a transportarse (VC). La multiplexación se basa en la adición intercalada de octetos, lo que permite insertar o extraer los tributarios de forma inmediata, hecho que constituye una de las principales ventajas de la filosofía SDH.

Los casos de multiplexación a considerarse en este trabajo son aquellos adoptados por la ETSI para la formación de unidades de transporte SDH.

1.1.6.1 Formación de la TUG-2

Puede formarse por la multiplexación de un TU-2 o 3 TU-12. Las figuras 1.10 a) y

b) muestran la formación de la TUG-2 a partir de tres TU-12 o una sola TU-2.

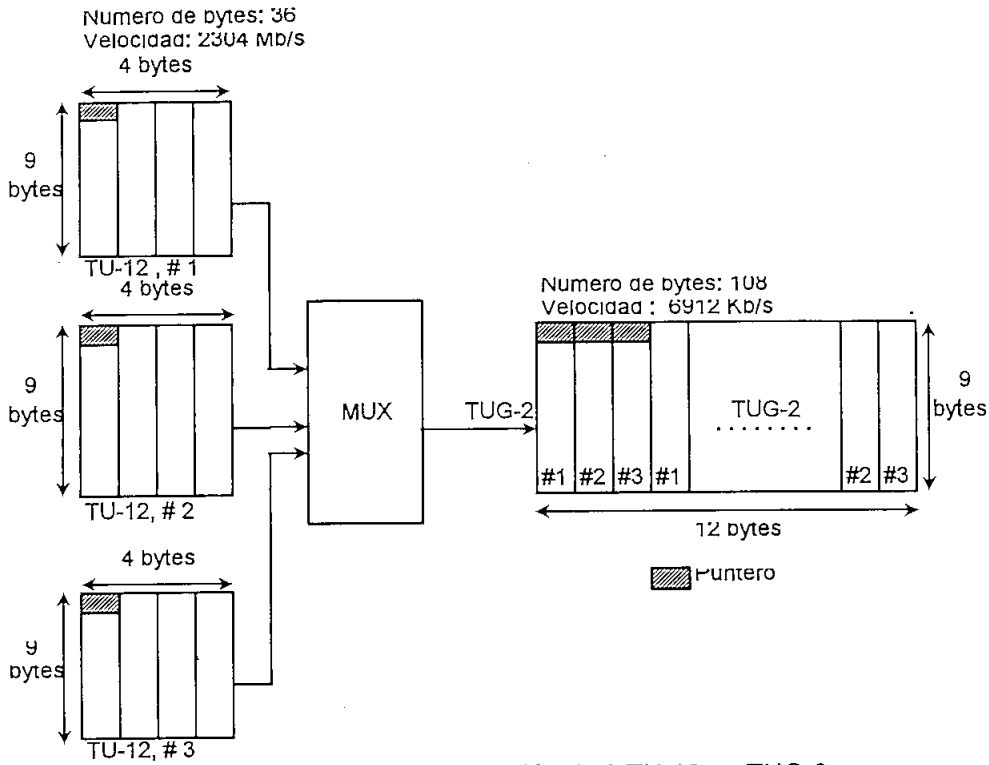


Fig. 1.10 a) Multiplexación de 3 TU-12 en TUG-2.

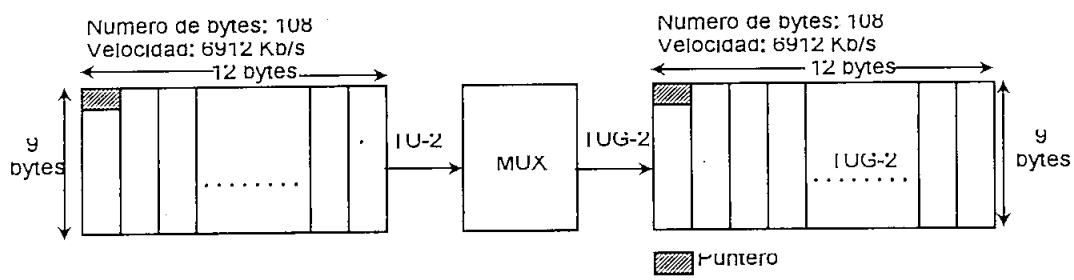


Fig. 1.10 b) Multiplexación de TU-2 en TUG-2

1.1.6.2 Formación de la TUG-3

La TUG-3 puede formarse ya sea por una TU-3 o siete TUG-2 (Ver figura 1.3). La multiplexación de estas entidades se puede observar en la figuras 1.11 a) y b).

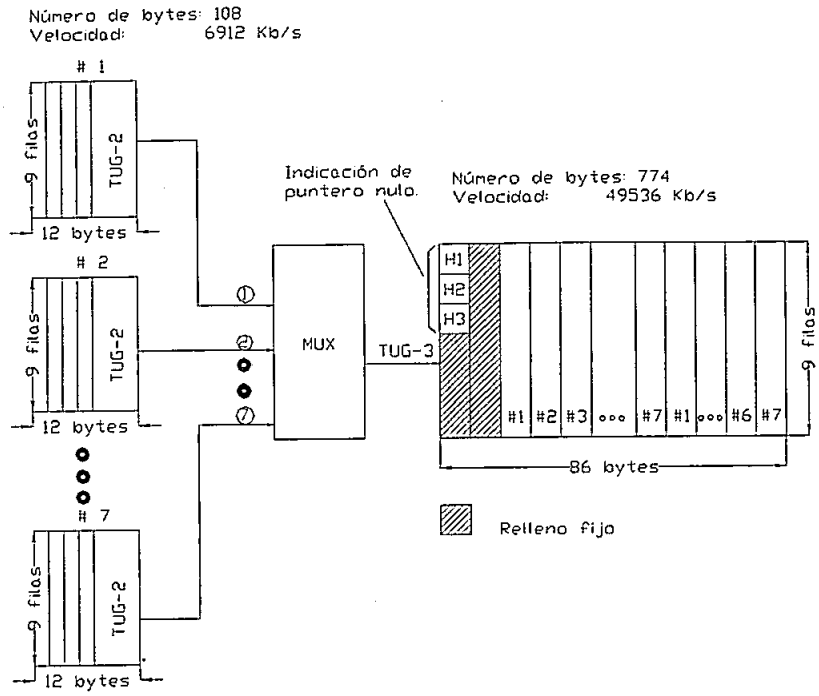


Fig. 1.11 a) Multiplexación de 7 TUG-2 en un TUG-3.

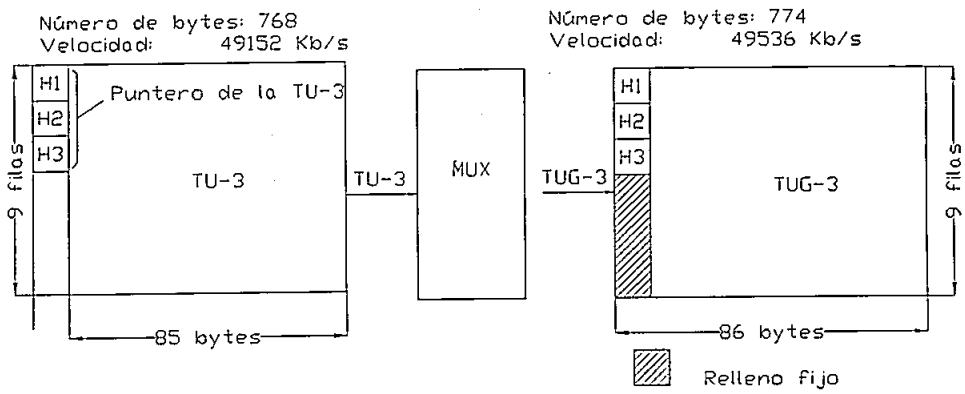
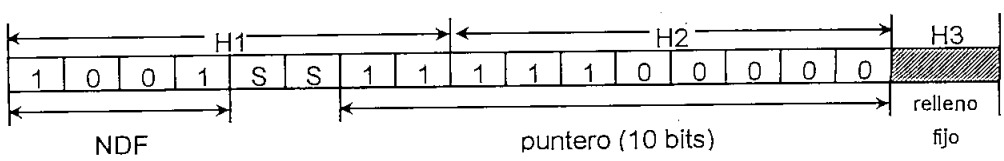


Fig. 1.11 b) Multiplexación de TU-3 en TUG-3.

En la figura 1.11 a) la TUG-3 formada muestra la combinación de tres bytes (**H1**, **H2**, **H3**) en la siguiente manera:



Esto indica que el puntero no es válido o se encuentra en estado inactivo. En este caso, el puntero debe ser ignorado debido a que cada una de las TUG-2 que forman la TUG-3, tiene ya su propio puntero de identificación. **H3** será siempre un byte de relleno fijo.

1.1.6.3 Formación del VC-4 a partir del TUG-3

En la figura 1.12 se muestran las tres TUG-3 formando un VC-4. Las columnas dos y tres son de relleno fijo para ajustar la longitud de la trama.

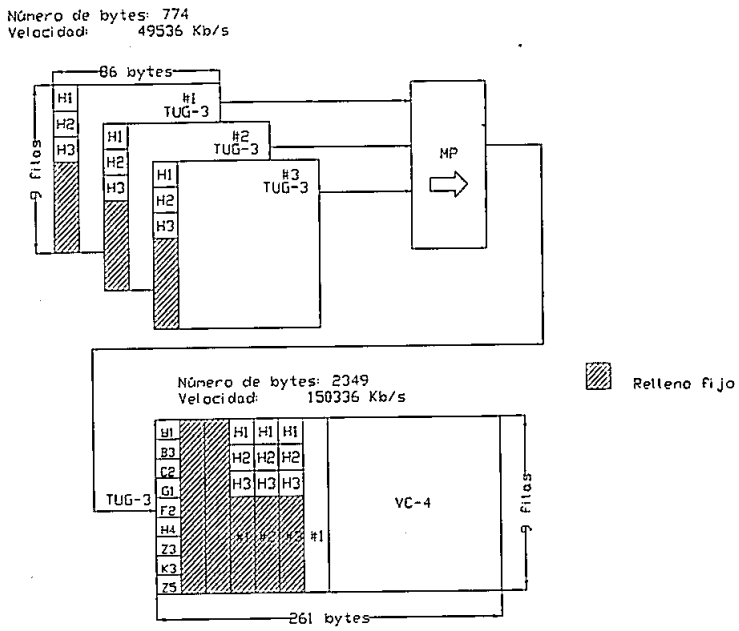


Fig. 1.12 Multiplexación de 3 TUG-3 en un VC-4.

1.1.6.4 Concatenación de Unidades Administrativas AU-4

La necesidad de sistemas con capacidades mayores a STM-1 puede satisfacerse mediante la concatenación de 4 o 16 unidades base STM-1, dando lugar a un multicontenedor cuya información de entramado reside en el puntero de la AU-4. El nuevo VC-4-X así formado contiene bytes de relleno fijo desde la columna 2 hasta la X (Ver figura 1.13).

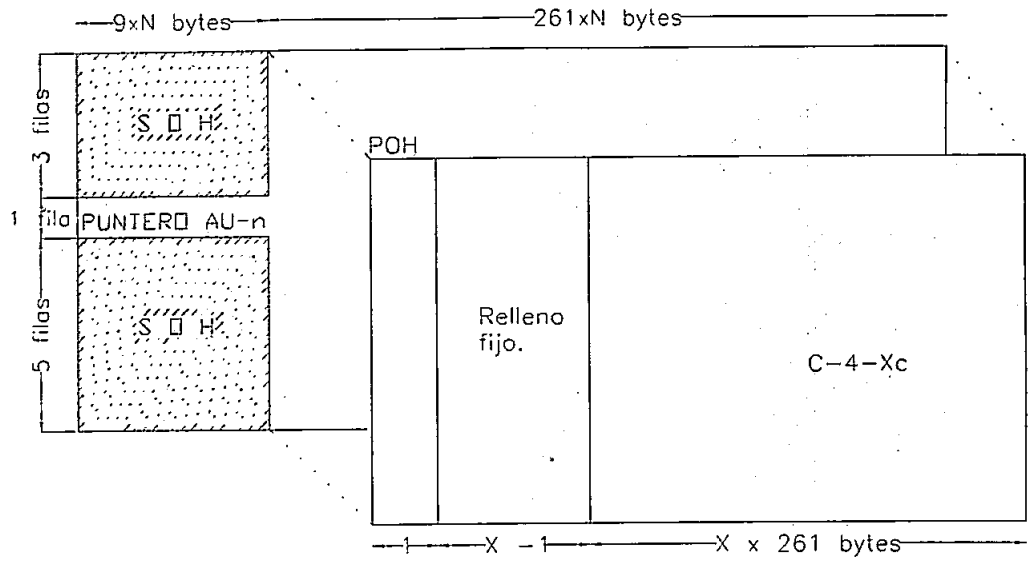


Fig. 1.13 Concatenación de Unidades Administrativas AU-4.

Los bytes **H1** y **H2** de la primera trama STM-1 son los únicos que contienen la información del puntero y de la inserción/no inserción de la nueva trama AU-4-X, mientras que los bytes **H1**y **H2** correspondientes a las tramas siguientes adoptan la "Indicación de concatenación" (1001SS1111111111, donde **SS** carecen de significado). La presencia de "Indicación de concatenación" obliga a los punteros de las siguientes tramas a realizar las mismas operaciones en cada una de las tramas AU-4 de la nueva AU-4-X. Esto significa además que las operaciones de justificación (positiva o negativa) que ocurren en la primera trama serán seguidas automáticamente por el resto.

1.1.7 Estructura del *overhead* de sección (SOH) y de recorrido (POH)

Esta parte de la estructura del STM-N se encarga de desarrollar operaciones de monitoreo de la calidad del sistema, información de la estructura de la trama, mantenimiento, etc.

1.1.7.1 Secciones de regeneración, múltiplex y de recorrido

Con referencia a la figura 1.14, la sección múltiplex comprende todo el trayecto entre terminales, incluyendo eventuales puntos de regeneración y el medio de transmisión utilizado. En general los equipos de conmutación automática están localizados a nivel de sección múltiplex.

La sección de regeneración representa cada tramo de interconexión entre dos puntos y comprende los equipos de transmisión y el medio de transporte. A su vez, la sección de recorrido comprende toda la trayectoria que sigue un canal desde que es insertado en la red SDH hasta que es detectado o recibido en su lugar de destino (el canal en este caso puede ser un flujo a 1.5, 2, 6, 34, 45, 140, 155, 622 Mb/s, etc.).

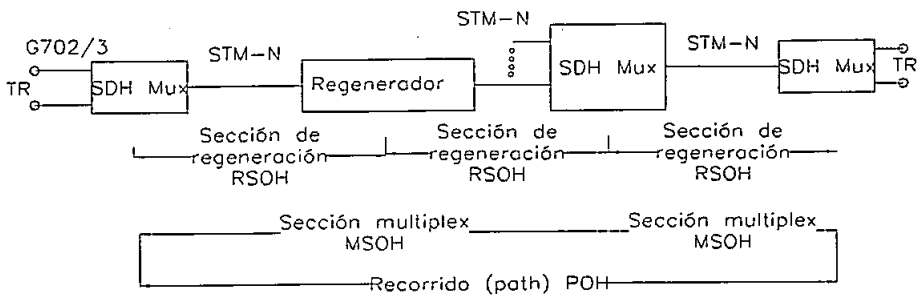


Fig. 1.14 Secciones de regeneración, múltiplex y de recorrido[3]

1.1.7.2 Descripción de los bytes de la SOH

La figura 1.15 muestra la estructura byte por byte del SOH incluyendo las dos secciones de múltiplex y regeneración.

9 Bytes

9 filas									
	A1	A1	A1	A2	A2	A2	J0	X*	X*
	B1	M	M	E1	M		F1	X	X
	D1	M	M	D2	M		D3		
	Puntero de la Unidad Administrativa AU.								
	B2	B2	B2	K1			K2		
	D4			D5			D6		
	D7			D8			D9		
	D10			D11			D12		
	S1	Z1	Z1	Z2	Z2	M1	E2	X	X

X: Bytes reservados para uso nacional.
*: Bytes no aleatorizados.
M: Bytes reservados para los medios de transmisión utilizados.

Fig. 1.15 Bytes de la SOH[4].

[3] SIP (Societa' Italiana delle Telecomunicazioni), La Gerarchia Numerica Sincrona di Multiplazione, Milan, Giugno, 1992.

[4] ITU-T, Rec. G.707 Network Node Interface For The Synchronous Digital Hierarchy (SDH), Geneve, March, 1996.

Los bytes de *overhead* de la sección de regeneración (RSOH) son:

A1, A2

- Palabra de alineación de trama: A1 = 11110110
  A2 = 00101000
- Se presenta al inicio de cualquier trama STM-1.

JO (C1)

- Identificación de la trama STM-1 dentro de una trama STM-N.

B1

- Byte de control de paridad par (BIP-8) para la trama STM-1 en una sección de regeneración.
- Se transmite, detecta y envía en cada punto de regeneración de la red SDH.
- En el caso de tramas STM-N, el byte **B1** de la primera trama STM-1 se encarga de controlar la paridad para todo el resto de tramas STM-1. El control se realiza en la trama STM-N aleatorizada.

E1

- Canal de fonía tipo ómnibus[5] para todos los puntos terminales o regeneradores de la red.

F1

- Canal reservado a los usuarios para voz, datos o mantenimiento de la red (64 Kb/s).

D1-D3

- Tres canales (192 Kb/s) de comunicación de datos utilizados para la administración y control de la red SDH. A este sistema de administración y control, la ITU-T lo ha denominado como TMN (*Telecommunications Management Network*).

Los bytes de *overhead* de la sección múltiplex (MSOH) se describen de la siguiente manera:

B2

- Tres bytes para el control de paridad par (BIP-24) de la trama STM-N, a excepción de los bytes de la RSOH.

---

[5] Canal común de voz que permite una comunicación simultánea entre todas las estaciones de la red. Es generalmente utilizado con fines de mantenimiento.

K1, K2 (bits 1 a 5)

- Sirven para el proceso de conmutación automática APS (ver sección 3.1.1) a nivel de sección múltiplex.

K2 (bits 6 a 8)

- Indicación de defectos en la sección múltiplex remota **MS-RDI** y señal de indicación de alarma **MS-AIS**.
- El valor indicado en el caso de **MS-RDI** es **110**, mientras que para **MS-AIS** toma el valor **111**.

D4-D12

- Nueve canales (576 Kb/s) de comunicación de datos para el sistema de administración y control de la red TMN.

S1

- Utilizado para indicar la calidad de la sincronización. Ver la tabla 1.1.

Z1, Z2

- Reservados para uso futuro.

M1

- Provisionalmente asignado para indicación de error de la sección múltiplex remota **MS-REI**.

E2

- Canal de fonía tipo expreso entre dos estaciones terminales. En el caso de una trama STM-N, solo el canal del primer STM-1 es utilizado.

Valor	Calidad de la sincronización
0000	Calidad desconocida
0001	Reservado
0010	G.811
0011	Reservado
0100	G.812 (tránsito)
0101	Reservado
0110	Reservado
0111	Reservado
1000	G.812 (local)
1001	Reservado
1010	Reservado
1011	Fuente de temporización para equipos síncrónicos (SETS)
1100	Reservado
1101	Reservado
1110	Reservado

Tabla 1.1 Byte de sincronización S1 (bits 5 a 8).

1.1.7.3 Descripción del *overhead* de la sección de recorrido (POH)

a) Bytes del POH del VC-4 y VC-3

La figura 1.2 muestra la ubicación de los bytes del POH para un VC-4 y VC-3. El POH ocupa las 9 filas de la primera columna del VC-4 o VC-3.

J1

- Es utilizado para la transmisión de una indicación de continuidad a lo largo de todo el recorrido de un canal. Normalmente se utiliza un formato de 16 bytes (un byte de inicio más 15 bytes de caracteres) que se transmiten a través de este byte[6].

B3

- Byte de control de paridad par (BIP-8) calculado en el último VC-3, VC-4 o VC-4-X antes de aleatorizarlo.

C2

- Indica la clase de información contenida en VC-3, VC-4, VC-4-X (Ver tabla 1.2).

G1

- Utilizado para la transmisión de alarmas locales hacia el terminal remoto.

Byte **G1**

REI				RDI	No utilizados		
1	2	3	4	5	6	7	8

REI indica el número de errores (máximo 8) detectados en **B3**.
RDI: vale **0** en ausencia de alarmas y **1** en caso de errores dentro del VC.

F2, Z3

- Bytes para comunicación del usuario.

H4

- Identificador del tipo de carga útil distribuida en una multitrama. Se aplica a los contenedores de orden inferior VC-11, VC-12, VC-2 que son distribuidos en 4 tramas consecutivas.

[6] Ver recomendación G.707 de la ITU-T, sección 9.3.1.1.

K3 (Bits 1 a 4)

- Protección por conmutación automática APS a nivel de recorrido (*Path protection* del VC-3,VC-4).

K3 (Bits 5 a 8)

- Reservados para uso futuro.

Z5 (Bits 1 a 4)

- Utilizados para indicación de conexión tipo tándem.

Z5 (Bits 5 a 8)

- Canal de datos a 32 Kb/s.

Bits 1234	Bits 5678	Hex	Significado
0000	0000	00	No equipado
0000	0001	01	Equipado-No reconocido
0000	0010	02	Estructura TUG
0000	0011	03	TU enclavado.
0000	0100	04	Mapeo asincrónico de 34 o 45 Mb/s en un contenedor C-3
0001	0010	12	Mapeo asincrónico de 140 Mb/s en un contenedor C-4
0001	0011	13	Mapeo de un flujo ATM
0001	0100	14	Mapeo de una MAN (Metropolitan Area Network)
0001	0101	15	Mapeo de FDDI (Fiber Distributed Data Interface)

Tabla 1.2 Codificación del byte C2

b) Bytes del POH del VC-2 y VC-1

La distribución de los bytes del POH para los contenedores de orden inferior se muestra en la figura 1.9.

V5

- Byte para el control de errores, indicación de fallas y modalidad de carga en el VC. La modalidad de carga es mostrada en la tabla 1.3.

Byte **V 5**

BIP-2		REI	RFI	Tipo de señal			RDI
1	2	3	4	5	6	7	8

- **BIP-2**: Controla la paridad del VC-1 y VC-2 pero excluye los bytes **V1**, **V2**, **V3** (excepto cuando existe justificación negativa) y **V4**.
- El bit 1 controla la paridad de todos los bits impares (1,3,5,7) de VC-1, VC-2.
- El bit 2 controla la paridad de todos los bits pares (2,4,6,8) del VC-1, VC-2.
- **REI**: Vale **1** si errores fueron detectados, **0** en caso contrario.

- **RFI**: Vale **1** si una falla ha sido declarada, **0** en caso contrario.
- **RDI**: Vale **1** para indicar presencia de AIS en TU-2, TU-1 o falla detectada.

J2

- Idéntico a **J1** del POH del VC-3, VC-4.

Z6

- Idéntico a **Z5** del VC-3, VC-4.

K4 (bits 1 a 4)

- Protección por conmutación automática APS para contenedores de orden inferior.

K4 (bits 5 a 8)

- Reservados para uso futuro.

Bits 5,6,7	Significado
000	No equipado
001	Equipado- No reconocido
010	Asincrónico
011	Sincrónica, bit por bit
100	Sincrónica byte por byte
101	Equipado-No utilizado
110	Equipado-No utilizado
111	Equipado-No utilizado

Tabla 1.3 Modalidad de carga indicada en el byte V5.

1.1.8 Mapeo

El mapeo es un proceso de carga de la información útil en una estructura compatible con la filosofía de la SDH. Este proceso de adaptación consiste en la reservación de todas las celdas de información necesarias, de tal manera que se pueda cumplir con el proceso de justificación, inclusión de los bytes de *overhead* (POH) y bytes de relleno fijo.

1.1.8.1 Mapeo de 140 Mb/s en un VC-4

El VC-4 es dividido en este proceso en 20 bloques de 13 bytes de ancho por 9 filas cada uno (Ver figura 1.16). De esta figura se obtiene el siguiente detalle en lo que respecta a los bytes y bits portadores de información (señalados con "I")[7]:

[7] ITU-T, Rec. G.707 Network Node Interface For The Synchronous Digital Hierarchy (SDH), Geneve, March, 1996.

- 20 x 12 bytes de la capacidad de carga del VC-4.
- 1 byte denominado **W**, que es parte de la capacidad de carga del VC-4.
- 6 bits del byte **Z**.

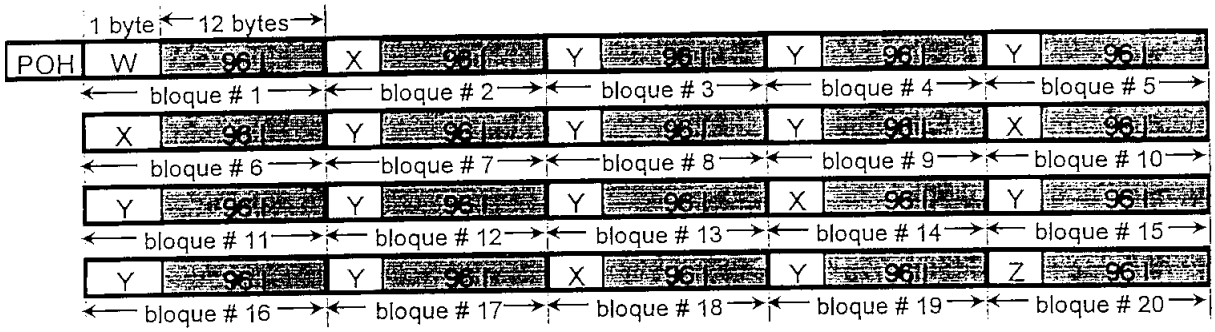
Los valores anteriores se distribuyen en las 9 filas de la trama STM-1.

Si se considera que el bit **S** representa un bit de relleno necesario para la justificación, la mínima velocidad de carga del VC-4 está determinada por:

$$C_{mín} = 9 \times ((20 \times 12 + 1) \times 8 \text{ [bits/byte]} + 6 \text{ [bits]}) \times (8 \times 10^3) = 139\,248 \text{ Kb/s}.$$

Por el contrario, si no existe justificación, el bit **S** está habilitado para transportar información, de tal manera que la capacidad de carga del VC-4 se incrementa en 9 bits (un bit por cada fila), y la máxima velocidad de carga se determina así:

$$C_{máx} = 9 \times ((20 \times 12 + 1) \times 8 \text{ [bits/byte]} + (6+1) \text{ [bits]}) \times (8 \times 10^3) = 139\,320 \text{ Kb/s}.$$



W: IIIIIIII
Y: RRRRRRRR
X: CRRRROO
Z: IIIIIISR
I: bit de información.
R: bit de relleno fijo.

S: bit disponible para justificación.
C: bit control de justificación.
CCCCC=00000: S es un bit información.
CCCCC=11111: S es un bit justificación.

Fig. 1.16 Carga de una señal a 140 Mb/s en un VC-4. Distribución de los bytes del VC-4.

Una señal plesiócrona a 140 Mb/s tiene una velocidad de carga nominal de 139264 Kb/s. Esto significa que si la velocidad del VC-4 es mayor que la señal plesiócrona, entre ellas existe una diferencia de:

$$139320 - 139264 = 56 \text{ Kb/s},$$

lo cual equivale a decir que 7 bits **S** son necesarios para relleno en cada trama de 125.μs.

En caso de que la velocidad de la señal plesiócrona sea mayor que la del VC-4 se obtiene lo siguiente:

139 264 – 139 248 = 16 Kb/s,

lo cual significa que 2 bits **S** son necesarios por cada trama para transportar la información.

1.1.8.2 Mapeo de 34 Mb/s en un VC-3

El VC-3 consiste de 9 filas x 84 bytes y se divide en tres subtramas de 3 filas x 84 bytes cada una (Ver figura 1.17). Los bits capaces de portar información se indican con una "I" en cada celda. El detalle de la capacidad de carga en este tipo de contenedor virtual se presenta a continuación[8]:

En las subtramas 1 y 2 se tiene lo siguiente:

- 20 [columnas] x 3 [bytes/fila] x 3 [filas] (total 180 bytes).

Mientras que para la subtrama 3 se tiene:

- 19 [columnas] x 3 [bytes/fila] x 3 [filas] (total 171 bytes).
- 1 [byte/fila] x 3 [filas] presente en la última columna (total 3 bytes).
- 7 [bits/fila] x 3 [filas] incluidos en los bytes **AB** (total 21 bits).

Los bits **S1** y **S2** -al igual que **S** en el caso del VC-4- pueden ser utilizados como bits de justificación o bits portadores de información. En caso de utilizarse como justificación, la capacidad total de transporte del VC-3 será la mínima y está determinada de la siguiente manera:

- Subtrama 1: C_1 = (20x3x3) [bytes] x 8 [bits/byte] = 1 440 [bits].
- Subtrama 2: C_2 = (20x3x3) [bytes] x 8 [bits/byte] = 1 440 [bits].
- Subtrama 3:C_3 = (19x3x3+3) [bytes] x 8 [bits/byte] + 21 = 1 413 [bits].

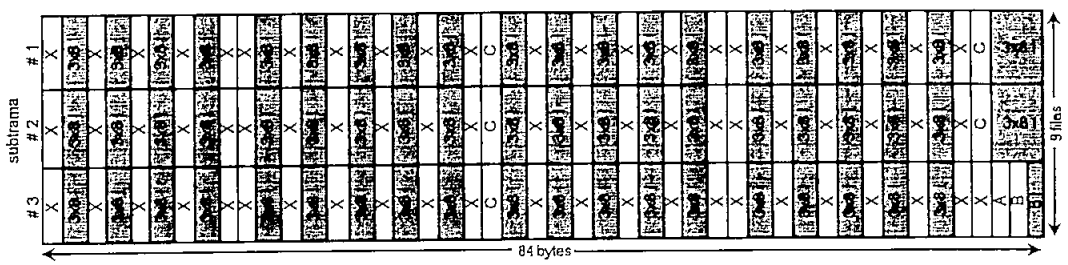
[8] MANCINI Cossimo, Concetti sulla multiplazione SDH, Siemens Telecomunicazioni S.p.A., Milan, Giugno, 1994.

De aquí se obtiene que la velocidad mínima de carga del VC-3 es:

$$C_{min} = (2x1440 + 1413)\ [bits] \times (8 \times 10^3)\ [Hz] = 34\ 344\ Kb/s.$$

En el caso de no existir ninguna justificación, **S1** y **S2** (total 6 bits) son habilitados para portar información, por lo que la velocidad de carga del VC-3 es máxima y se determina así:

$$C_{máx} = (2x1440 + 1413 + 6)\ [bits] \times (8 \times 10^3)\ [Hz] = 34\ 392\ Kb/s.$$



X: RRRRRRRR
R: bit de relleno fijo.
S: bit para justificación.
AB: RRRRRRR S_1 S_2IIIIIII
I: bit de información.

C: bit control de justificación.
$C_1C_1C_1C_1C_1$ = 11111 S_1 es bit de justificación.
$C_1C_1C_1C_1C_1$ = 00000 S_1 es bit de información.
C_2: idem que para C_1

Fig. 1.17 Carga de 34 Mb/s en un VC-3. Distribución de los bytes dentro del VC-3.

La señal plesiócrona a 34 Mb/s tiene una velocidad de carga de 34 368 Kb/s, por lo que la diferencia con la velocidad del VC-12 en el caso de máxima capacidad es:

$$34\ 392 - 34\ 368 = 24\ Kb/s,$$

lo cual significa que 3 bits (S_1 o S_2) por trama son necesarios como relleno.

Si la velocidad del VC-3 es menor a aquella de la señal plesiócrona se tiene que:

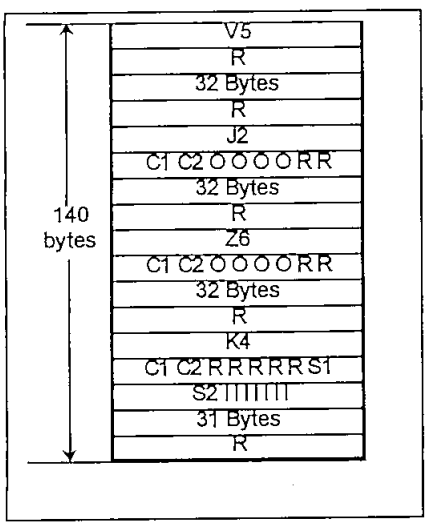
$$34\ 368 - 34\ 344 = 24\ Kb/s,$$

por lo que 3 bits (S_1 o S_2) por cada trama son necesarios para transportar información.

1.1.8.3 Mapeo de 2 Mb/s en el VC-12

a) Carga asincrónica de 2 Mb/s en un VC-12

La figura 1.18 muestra la estructura de los bytes para este tipo de carga.



I: bit de información.

R: bit de relleno fijo.

O: bit de *overhead* (para uso futuro).

S: bit disponible para justificación.

C: bit de control de justificación.

$C_1C_1C_1$ = **000** significa que S_1 es un bit de información.

$C_1C_1C_1$ = **111** significa que S_1 es un bit de justificación

$C_2C_2C_2$ = idem a C1.

Fig. 1.18 Carga asincrónica de 2 Mb/s en un VC-12[9].

Considerando la figura 1.18, la velocidad mínima de carga de un flujo a 2 Mb/s (es decir, cuando $S_1 = S_2 = R$) está determinada por lo siguiente:

- (32 x 3 + 31) [bytes] (total 127 bytes)
- 7 bits de información de la antepenúltima fila.

Por lo tanto, la velocidad mínima de carga es:

$$C_{mín} = (127\ [bytes] \times 8\ [bits/byte] + 7\ [bits]) \times 2.0\ [KHz] = 2\ 046\ Kb/s$$

Mientras que la velocidad máxima ($S_1 = S_2 = I$) está determinada por:

[9] ITU-T, Rec. G.707 Network Node Interface For The Synchronous Digital Hierarchy (SDH), Geneve, March, 1996

$C_{máx}$ = (127 [bytes]x8 [bits/byte] + (7+2) [bits]) x 2.0 [KHz] = 2 050 Kb/s

Una señal plesiócrona de 2 Mb/s tiene una velocidad nominal de 2048 Kb/s, por lo que la diferencia con la velocidad del V-12 en el caso de máxima capacidad es:

2 050 – 2 048 = 2 Kb/s

lo que equivale a insertar un bit de relleno (S_1 o S_2) por cada multitrama (500 μs).

En el otro caso, si la velocidad del VC-12 es menor a aquella de la señal plesiócrona, se tiene lo siguiente:

2 048 – 2 046 = 2 Kb/s

lo cual significa que 1 bit (S_1 o S_2) por cada multitrama (500 μs) es necesario para transportar la información.

b) Carga sincrónica byte a byte de 2 Mb/s en un VC-12 (Señalización asociada al canal o señalización por canal común)

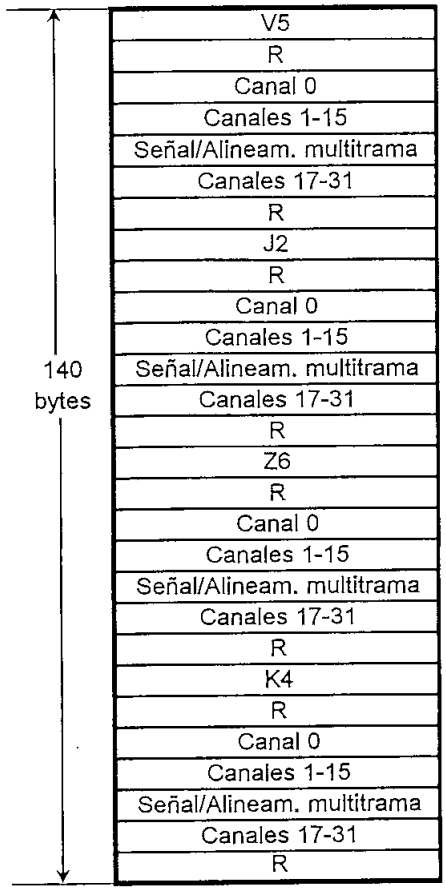
Se trata en este caso de cargar un flujo a 2048 Kb/s que contiene 30 canales de información utilizando el canal número 16 para la señalización (Ver figura 1.19).

c) Carga sincrónica byte a byte de 31 x 64 Kb/s en un VC-12

La distribución de los bytes en el VC-12 puede verse en la figura 1.20.

1.2 EQUIPOS SINCRONICOS

La Jerarquía Digital Sincrónica SDH permite integrar en un solo aparato las funciones de multiplexación, terminal de línea y conmutación de los flujos de información. Esto se logra gracias a que las características de control y administración no se refieren a la estructura física de los aparatos si no a las funciones por ellos desarrolladas.

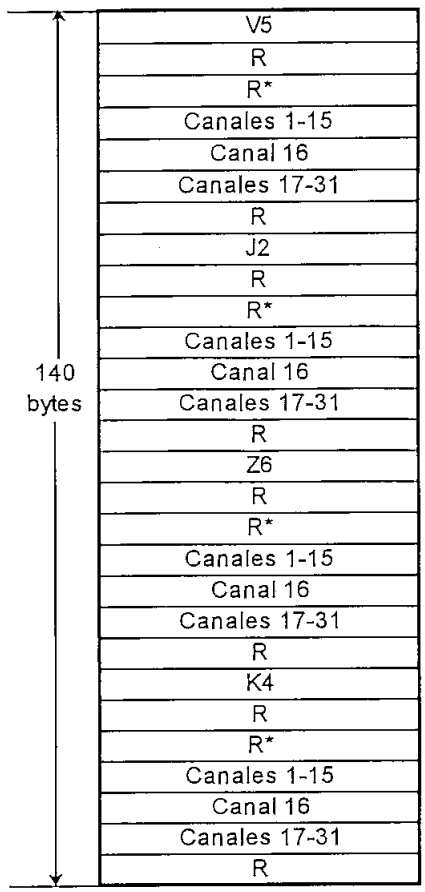


Longitud de trama: 500 μs.

Fig. 1.19 Carga sincrónica byte a byte de 2048 Kb/s en un VC-12[10].

La tendencia en SDH es hacia la estructuración de aparatos con capacidad de reconfiguración flexible y dinámica cuyas características de control y supervisión serán manejadas por un sistema conocido generalmente como *Telecommunication Management Network* (TMN). La estandarización de la SDH permite tener también la característica de "Compatibilidad Transversal", lo cual significa que los equipos de transmisión y recepción, aún siendo de distinta procedencia o fabricante, pueden comunicarse sin ningún problema gracias a las funciones compatibles por ellos desarrolladas.

[10] ITU-T, Rec. G.707 Network Node Interface For The Synchronous Digital Hierarchy (SDH), Geneve, March, 1996



Longitud de trama: 500 μs

R* puede ser utilizado para el intervalo 0 si es necesario.

Fig. 1.20 Carga sincrónica byte a byte de 31 x 64 Kb/s en un VC-12[11].

1.2.1 Modelos de aparatos sincrónicos

Los aparatos sincrónicos se dividen en dos grandes grupos:

Repetidores de Línea: Se encargan de la regeneración de la información y se comunican solo a nivel de RSOH.

Nodos Terminales: Son los responsables de la elaboración, conmutación y transmisión de los flujos de información. De acuerdo a la configuración de la red, ellos desarrollan

[11] Idem a ref. No. 10.

las funciones de administración y control a nivel de RSOH, MSOH y POH.

Los aparatos sincrónicos que se describirán son: Multiplexor Terminal y de Inserción/Extracción, *Digital Cross Connect* -a nivel de TU y AU- y algunas características de los aparatos SDH basados en sistemas de radio relés (SDH-SRR).

1.2.1.1 Multiplexor terminal y de inserción/extracción

La función principal de los aparatos multiplexores en configuración terminal es la

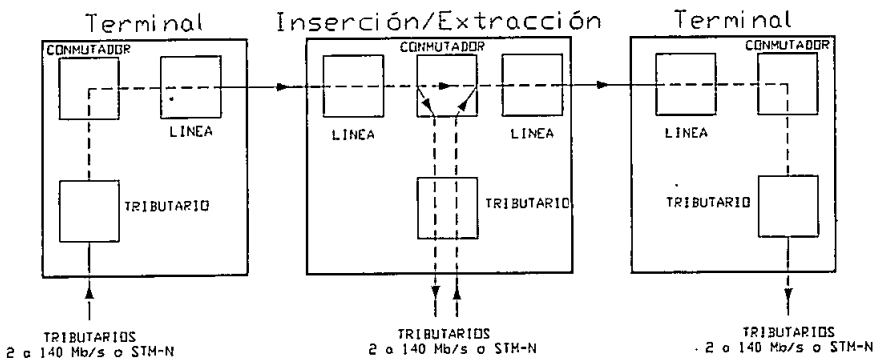


Fig.1.21 Multiplexores en configuración terminal y de inserción/extracción (solo se muestra una dirección de transmisión).

recolección de los flujos de tráfico provenientes de las áreas de distribución y su respectiva incorporación en un flujo STM-1. Los multiplexores de inserción/extracción en cambio realizan la función de tomar/distribuir flujos tributarios en el flujo de línea STM-1 (Ver figura 1.21).

Entre las características más importantes pueden incluirse las siguientes (Ver la figura 1.22):

- Capacidades de manejo de tráfico (a nivel de STM-1) en un máximo de:
  - 3 flujos a 34 o 45 Mb/s.
  - 63 flujos a 2 Mb/s.

  o una combinación de:
  - 21 flujos a 2 Mb/s más 2 flujos a 34 o 45 Mb/s.

- 42 flujos a 2Mb/s más un flujo a 34 o 45 Mb/s.

- Actualmente se están desarrollando aparatos con capacidad de multiplexación y conmutación a nivel de 64 Kb/s.
- Interfaces ópticas/eléctricas de línea a nivel STM-1/4/16.
- Interfaz Q para el sistema de supervisión y control TMN.
- Interfaz para la comunicación de servicio (*Engineering Order Wire*, bytes E1, E2 del SOH).
- Interfaz para canal de usuario (byte F1 de la SOH).
- Interfaz para sincronización externa (reloj externo).

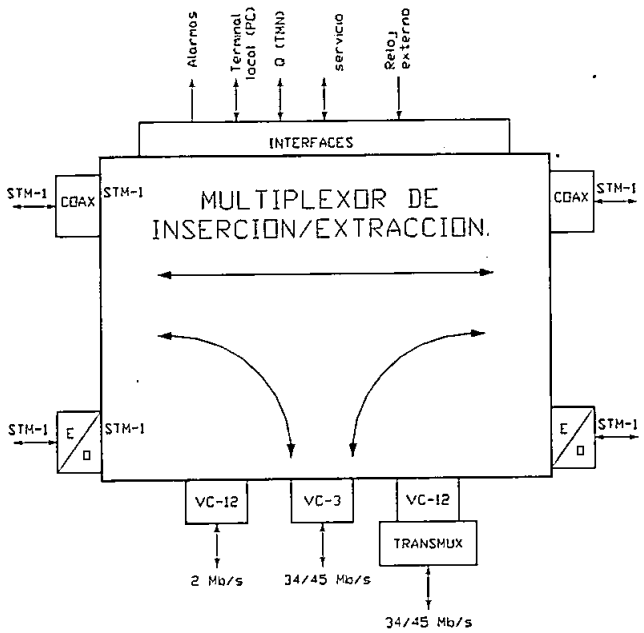


Fig.1.22 Diagrama del Multiplexor de Inserción/Extracción (ADM-1)

1.2.1.2 Aparatos de conmutación (*Digital Cross Connect* - DXC)

Estos aparatos permiten la conmutación de flujos entrantes y salientes de un nodo de tal manera de permitir un re-enrutamiento con el fin de proteger los flujos en caso de averías, o simplemente ejecutar funciones de mantenimiento. Esta conmutación se realiza a nivel de contenedores virtuales VC-12, VC-2, VC-3 y VC-4 en diversas modalidades (Ver figura 1.23):

- De línea a línea.
- De línea a tributario.
- De tributario a tributario.

A nivel de puertas STM-N (línea o tributario) cualquier combinación de contenedores virtuales VC es multiplexada y conmutada. Sin embargo, en el caso de interconexión de puertas con tributarios PDH (1.5, 2, 34, 45, 140 Mb/s) la conmutación se realiza de acuerdo a la tabla 1.4.

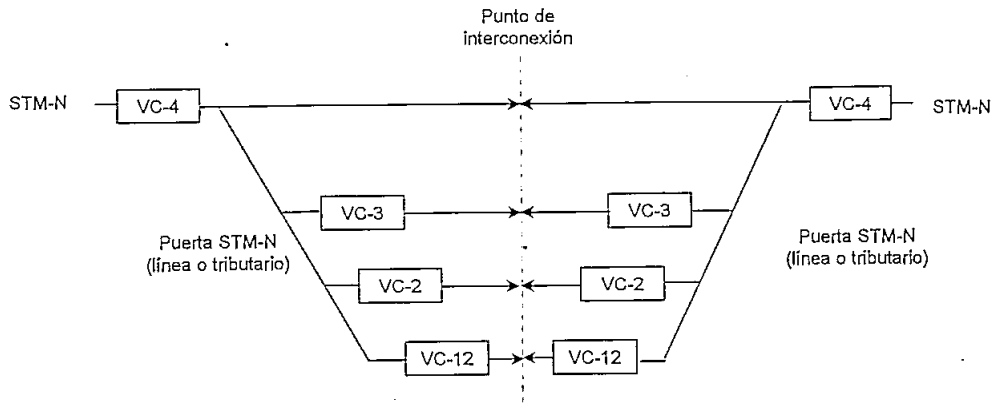


Fig.1.23 Diagrama de interconexión de flujos en un aparato de conmutación DXC.

Tipo de interconexión	Conmuta a nivel de:
Línea o tributario STM-N a tributario 1.5 o 2 Mb/s.	VC-12
Línea o tributario STM-N a tributario 34 o 45 Mb/s.	VC-3
Línea o tributario STM-N a tributario 140 Mb/s.	VC-4
Tributario 1.5 o 2 Mb/s a tributario 1.5 o 2 Mb/s.	VC-12
Tributario 34 0 45 Mb/s a tributario 34 o 45 Mb/s.	VC-3
Tributario 140 Mb/s a tributario140 Mb/s.	VC-4

Tabla 1.4 Interconexión y niveles de conmutación utilizados.

1.2.1.3 Aparatos SDH basados en sistemas de radio relés

La elaboración de recomendaciones para sistemas de radio SDH tiene como objetivo alcanzar la completa compatibilidad con los sistemas SDH basados en fibra óptica. Sin embargo, en un sistema de radio existen muchos parámetros como modulación, codificación, varios tipos de filtros, algoritmos de conmutación, etc., que son desarrollados por cada fabricante tratando de alcanzar un óptimo rendimiento del sistema. Esto implica obviamente que la "Compatibilidad transversal" está aún en vías de definición y estandarización a nivel de sistemas de radio SDH.

Las características principales de estos sistemas de radio son:

- Utilización como parte de un anillo sincrónico en fibra óptica.
- Protección de enlaces de fibra óptica en configuraciones 1+1.
- Enlaces punto-punto y punto-multipunto.

Las funciones de sección múltiplex y de regeneración son también ejecutadas sin ninguna variación respecto de los otros aparatos SDH. Si el enlace radio es utilizado como protección, éste puede representar una sección múltiplex, o su vez actuar como sección de regeneración a la cual se deben añadir aparatos multiplexores para formar la sección múltiplex.

Las capacidades de transmisión actualmente desarrolladas son de 155 Mb/s (STM-1) y 2x155 Mb/s (2xSTM-1) que se utilizan para sistemas troncales grandes. Estos aparatos pueden adoptar configuraciones N+1 (N canales con tráfico más uno de protección)[12]. Además, como enlaces de acceso a los sistemas troncales, se están desarrollando sistemas conocidos como Sub-STM-1, cuya capacidad de información es equivalente a un VC-3 (21x2Mb/s). Tres de ellos pueden ser multiplexados para formar una trama STM-1 de acuerdo con la recomendación G.707.

1.2.2 Descripción funcional a nivel de bloques

La recomendación G.783 del ITU-T[13] trata básicamente el funcionamiento de los aparatos multiplexores en configuración terminal y de inserción/extracción. Las recomendaciones para aparatos de conmutación (DXC) están en período de definición, pero su estructura funcional es la misma que aquella utilizada para los multiplexores en las recomendaciones G.782 y G.783. Actualmente, los aparatos multiplexores pueden configurarse también como conmutadores (DXC) simplemente vía software; esto es solamente para dar un ejemplo de la tendencia hacia la máxima flexibilidad a seguirse a futuro en las redes SDH.

La figura 1.24 muestra la estructura funcional de los aparatos sincrónicos SDH. Este diagrama permite visualizar varios grupos de funciones como se detallan a

---

[12] N+1 significa que se transmiten (N+1) canales STM-1 (N+1 tramas STM-1 son transmitidas), que no es lo mismo que transmitir un flujo STM-N (una sola trama STM-N es transmitida).

[13] ITU-T, Draft of new Recommendation G.783, Geneve, July, 1994.

continuación[14]:

- TTF (Función terminal de transporte): Está formada por varias funciones básicas como Interfaz física, terminación de sección de regeneración y múltiplex, protección de sección múltiplex y adaptación de sección múltiplex.
- HOI (Interfaz de orden superior): se encarga del ensamblaje de los contenedores de orden superior a partir de señales plesiócronas a 140 Mb/s.
- LOI (Interfaz de orden inferior): Agrupa un conjunto de funciones para ensamblar contenedores virtuales de orden inferior a partir de señales plesiócronas incluidas en los contenedores C-12 y C-2.
- HOA (Adaptación de orden superior): Permite la formación de contenedores virtuales de orden superior (VC-4) a partir de las estructuras formadas por la LOI y añade el POH correspondiente.
- Funciones de supervisión de orden inferior y superior (HSU y LSU): Realizan el monitoreo de flujos sincrónicos que podrían no ser portadores de tráfico, pero que requieren una generación y terminación apropiadas dentro de la red.
- HPC y LPC (Conexión de recorridos de orden superior e inferior): Su principal función es permitir la conmutación de flujos a nivel de contenedores virtuales de orden superior e inferior respectivamente. Están directamente relacionadas a la función cumplida por los aparatos de interconexión (DXC).
- Otras funciones como OHA (Acceso al *overhead*), SEMF (Función de administración), SETS (Temporización) y SETPI (Interfaz de temporización) se muestran en detalle en el Anexo # 2.

[14] Se recomienda revisar el Anexo # 2, donde se presenta una descripción de las funciones mostradas en la figura 1.24.

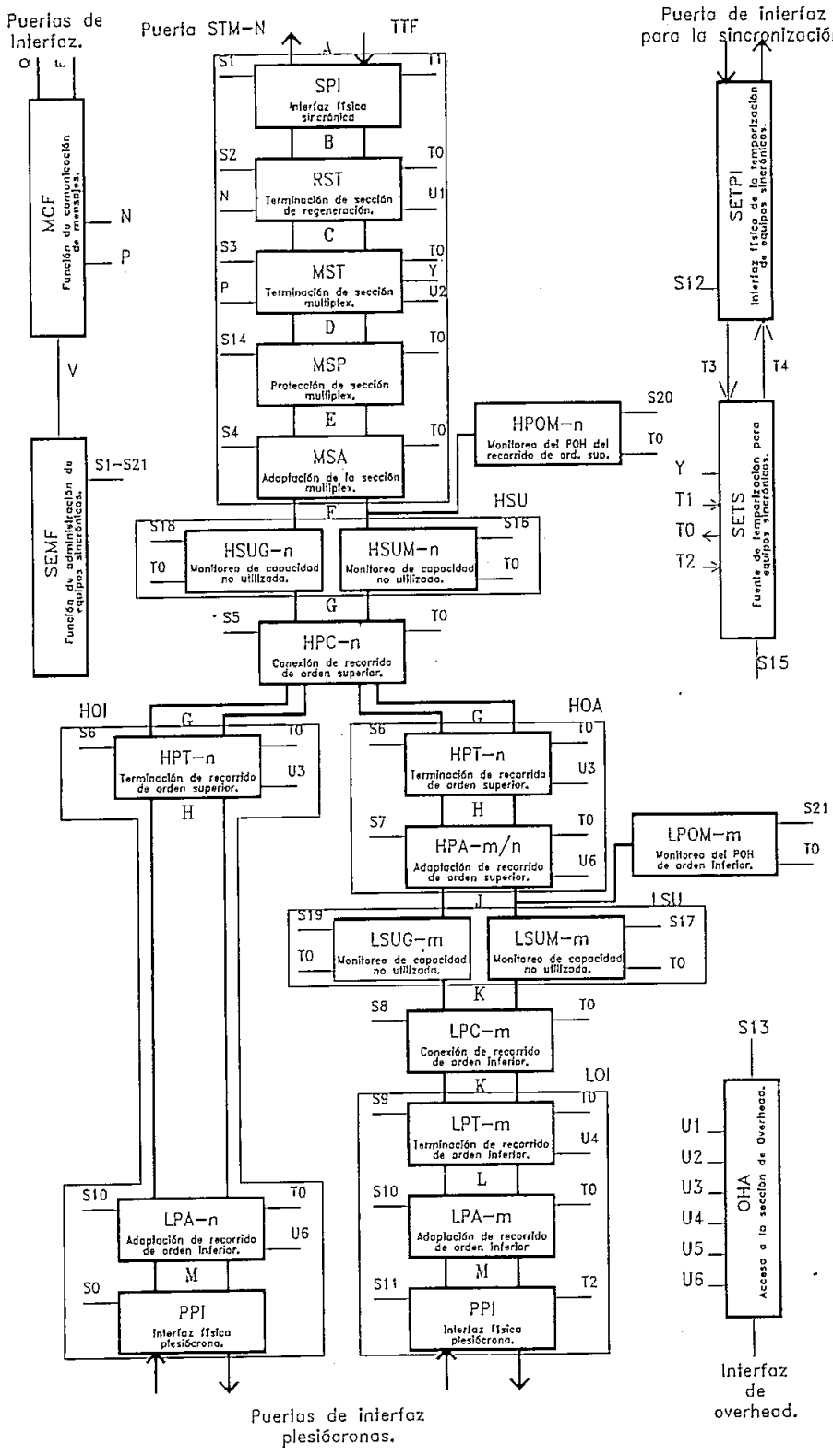


Fig. 1.24 Diagrama funcional a bloques de un aparato multiplexor SDH[15]

[15] ITU-T, Draft of new Recommendation G.783, Geneve, July, 1994.

CAPITULO II

Anillos sincrónicos en redes SDH

ANILLOS SINCRONICOS EN REDES SDH

2.1 CLASES DE ANILLOS

Un anillo se define en general como un conjunto de nodos que forman un lazo cerrado, donde cada nodo se comunica bilateralmente con sus nodos adyacentes.

Existen dos principales tipos de anillos en redes SDH:

2.1.1 Anillo unidireccional

Se caracteriza porque los flujos de tráfico de ida y vuelta entre dos nodos siguen un mismo sentido de rotación dentro del anillo, por ejemplo en el sentido contrario a las manecillas del reloj (Ver figura 2.1). Esto implica obviamente que los dos canales con tráfico son enrutados por trayectorias diferentes en el anillo.

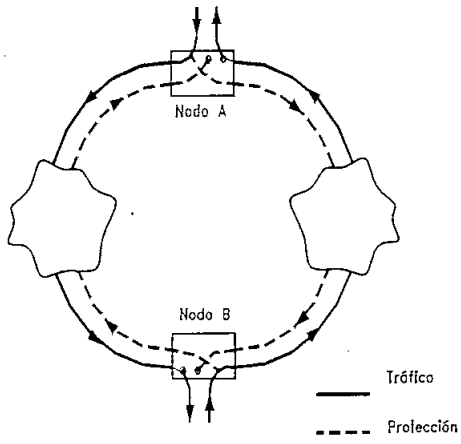


Fig. 2.1 Flujo de tráfico en un anillo unidireccional.

2.1.2 Anillo bidireccional

Los tráficos de ida y vuelta tienen diferentes sentidos de rotación. En este caso, la trayectoria seguida por ellos es la misma (Ver figura 2.2).

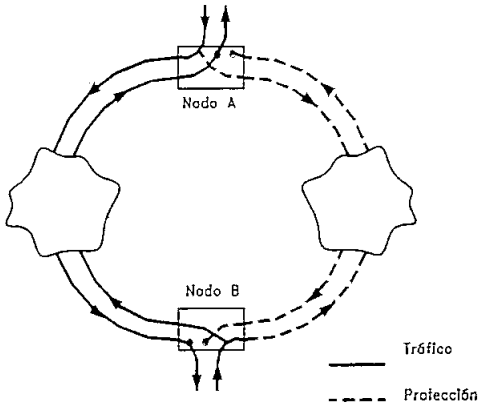


Fig. 2.2 Flujo de tráfico en un anillo bidireccional.

2.2 TIPOS DE TRÁFICO

En los anillos sincrónicos se distinguen 4 modelos de tráfico, los mismos que se muestran en la figura 2.3.

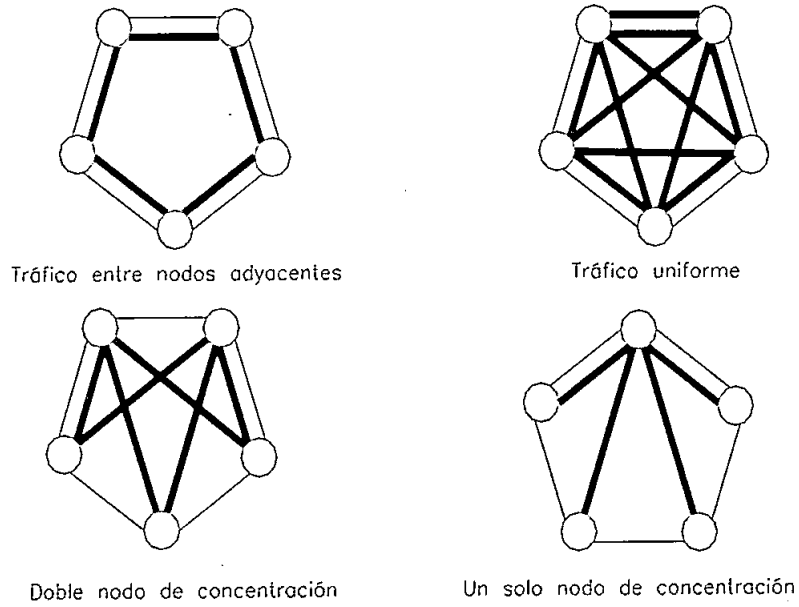


Fig. 2.3 Tipos de tráfico en anillos sincrónicos.

2.2.1 Tráfico entre nodos adyacentes

El tráfico fluye entre un nodo y sus vecinos más cercanos. Generalmente se caracteriza por tener una gran capacidad de tráfico entre nodos y se lo utiliza para la interconexión de grandes centros de información dentro una ciudad o un país.

2.2.2 Tráfico uniforme

Se caracteriza por la distribución equilibrada de tráfico entre todos los nodos. Se lo utiliza principalmente para el intercambio de flujos de tráfico a nivel urbano.

2.2.3 Tráfico con un nodo de concentración (*single hub*)

Un solo nodo es el eje o centro de recolección y distribución de tráfico en la red. Es utilizado para redes de acceso a redes principales, por ejemplo en la periferia de las ciudades. Los riesgos de pérdida de tráfico son evidentes debido a la presencia de un solo nodo de concentración que cumple las funciones de una compuerta principal hacia redes con mayor capacidad de tráfico.

2.2.4 Tráfico con doble nodo de concentración (*double hub*)

Existen dos nodos principales que comparten el tráfico hacia los otros nodos. Se utiliza con fines de protección, a través de los dos nodos de concentración en el caso de tener dos anillos sincrónicos conectados, o de conectar un anillo a otras redes con mayor capacidad de tráfico.

2.3 CAPACIDAD DE TRÁFICO

El análisis de la capacidad de tráfico se basa en el estudio de los dos tipos de anillos, unidireccional y bidireccional, los cuales son considerados de acuerdo a los cuatro modelos de tráfico a los que se hizo referencia en la sección 2.2.

Cuando se hace referencia a la capacidad de tráfico, se debe considerar que esta capacidad es la mínima que se necesita en un anillo para poder proteger el tráfico en caso de que se produzca una rotura de una de las secciones (enlaces) del anillo. Sin embargo, es conocido que el hecho de tener un sistema de mayor capacidad requiere una mayor inversión económica y mayores esfuerzos de operación y mantenimiento. Es decir, un sistema será más conveniente para el cliente si éste necesita menor capacidad de tráfico para la protección.

Las siguientes definiciones serán consideradas para fines de mayor claridad en la explicación:

d: demanda de tráfico entre dos nodos cualquiera del anillo (medida en número de contenedores virtuales VC).

n: número de nodos del anillo.

Cu: capacidad de tráfico de cada sección de un anillo unidireccional.

Cb: capacidad de tráfico de cada sección de un anillo bidireccional.

$R_{u/b}$: relación entre la capacidad requerida para un anillo unidireccional con respecto a un bidireccional. Es decir:

$$R_{u/b} = C_u / C_b \qquad (2.1)$$

Como regla general, para determinar la capacidad necesaria para protección se cumple que[1]:

a) Caso unidireccional: equivale a la suma de todas las demandas de tráfico en el anillo.
b) Caso bidireccional: equivale a suma de las dos mayores capacidades de tráfico en el anillo.

2.3.1 Tráfico entre nodos adyacentes

a) Caso unidireccional

La capacidad necesaria para la protección se obtiene claramente de la suma de todas las demandas de tráfico d entre los nodos, así:

$$C_u = n * d \qquad (2.2)$$

b) Caso bidireccional

En este caso la capacidad necesaria para protección se obtiene de la suma de las dos más grandes demandas en el anillo:

$$C_b = 2 * d \qquad (2.3)$$

Por lo tanto la relación unidireccional a bidireccional será:

$$R_{u/b} = n*d/(2*d) = n/2 \qquad (2.4)$$

---

[1] POH SOON CHERNG, Comparison of Bidirectional and Unidirectional SDH Rings, Northern Telecom, The Hague, 1991.

2.3.2 Tráfico uniforme

a) Caso unidireccional

La capacidad está definida por la suma total (combinación) de todos los pares de enlaces del anillo, donde el número total de combinaciones está dado por:

$$C_2^n = n * n\,(n-1)/2 \qquad (2.5)$$

De esta manera, la capacidad requerida por el anillo es:

$$C_u = [n*(n-1)/2]*d \qquad (2.6)$$

b) Caso bidireccional

Se deben considerar dos sub-casos:

1. Anillos con número impar de nodos

En este caso el cálculo de la capacidad requerida no implica que alguno de los nodos debe compartir sus demandas de tráfico. Considerando algunas propiedades geométricas de los polígonos se obtiene que la demanda de tráfico más alta en las secciones del anillo es[2]:

$$\sum_{i=1}^{(n-1)/2} i = \{[(n-1)/2]/2\} * [(n-1)/2+1] = (n^2-1)/8 \qquad (2.7)$$

La capacidad de tráfico requerida es dos veces la capacidad más alta en el anillo (determinada por la ecuación (2.7)):

$$C_b = [(n^2-1)/4]*d \qquad (2.8)$$

Reemplazando (2.6) y (2.8) en (2.1), fácilmente se obtiene que :

$$R_{u/b} = 2*n/(n+1) \qquad (2.9)$$

---

[2] Las fórmulas presentadas para la capacidad de protección, así como para el máximo número de nodos de los anillos, forman parte de la recomendación ETSI, DTR/M-3025 Transmission and Multiplexing (TM) SDH Network Protection Schemes: Types and Characteristics, Sophia Antipolis-France, September, 1995.

2. Anillos con número par de nodos

Las demandas de tráfico no compartidas entre nodos se calculan en base a propiedades geométricas de los polígonos[3]:

$$\sum_{i=1}^{(n-2)/2} i = \{[(n-2)/2]/2\} * [(n-2)/2 + 1] = n*(n-2)/8 \qquad (2.10)$$

Por otra parte, las demandas de tráfico compartidas corresponden a la mitad del número de nodos del anillo, es decir n/2. Además, es necesario considerar que el número de demandas de tráfico a compartirse puede ser par o impar, es decir pueden darse las siguientes situaciones:

(d-1)/2 o (d+1)/2, si d es impar o,
d/2 , si d es par.

El peor caso para la primera situación es cuando se requiere una mayor capacidad, es decir cuando se tiene (d+1)/2, de tal manera que la capacidad de tráfico requerida será[1]:

$$C_b = 2*\{[n*(n-2)/8]*d + (n/2)*(d+1)/2\}$$

$$C_b = (n^2/4)*d + n/2 \qquad (2.11)$$

En el caso de que d sea par se tiene que:

$$C_b = 2*\{[n*(n-2)/8]*d + (n/2)*(d/2)\}$$

$$C_b = (n^2/4)*d \qquad (2.12)$$

La relación de capacidades en este caso será:

$$R_{u/b} = 2*(n-1)*d/(n*d+2), \text{ si d es impar y,} \qquad (2.13)$$

---

[3] POH SOON CHERNG, Comparison of Bidirectional and Unidirectional SDH Rings, Northern Telecom, The Hague, 1991.

$R_{u/b} = 2*(n-1)/n$, si d es par (2.14)

2.3.3 Tráfico con un nodo de concentración

a) Caso unidireccional

En este caso todas las demandas de tráfico se dirigen hacia un solo nodo, de tal manera que la capacidad requerida es:

$C_u = (n-1)*d$ (2.15)

b) Caso bidireccional

Existen dos casos a considerarse:

1. Anillos con número impar de nodos

Ninguna partición de tráfico se produce y por lo tanto el número de demandas de tráfico que contribuyen a la capacidad de tráfico requerida es:

$(n-1)/2$

Las dos secciones más grandes del anillo son iguales, por lo tanto la capacidad de tráfico requerida es:

$C_b = [2*(n-1)/2]*d = (n-1)*d$ (2.16)

De aquí se obtiene que:

$R_{u/b} = 1$ (2.17)

2. Anillos con número par de nodos

La partición de demandas de tráfico es considerada para uno de los nodos conectados al nodo de concentración. Esto implica que el número total de demandas de tráfico que no sufren partición es:

$(n-2)/2$

La demanda de tráfico seccionada puede dividirse en dos partes d_1 y d_2, las cuales contribuyen a las dos más grandes secciones del anillo (se puede asumir que d_1

contribuye a la sección más grande y d_2 a la segunda sección más grande del anillo).

Para obtener la capacidad de tráfico requerida se suman las demandas de tráfico no seccionadas (d veces) más las demandas que han sufrido partición (d_1 o d_2 veces), así:

$$C_b = [(n-2)/2*d+d_1] + [(n-2)/2*d+d_2]$$

$$C_b = (n-1)*d. \qquad (2.18)$$

La relación $R_{u/b}$ entre las capacidades será, como en el caso anterior, igual a 1.

2.3.4 Tráfico con dos nodos de concentración

La deducción de las ecuaciones son similares al caso anterior. En este caso las dos secciones más grandes del anillo son aquellas adyacentes a los dos nodos de concentración (mas no la sección entre ellos). Todas las demandas de tráfico se dirigen desde un nodo hacia los dos nodos de concentración en dos partes d_1 y d_2, donde:

$$d_1+d_2=d.$$

a) Caso unidireccional

La totalidad de demandas de tráfico es (n-2), con lo que la capacidad de tráfico requerida es:

$$C_u = (n-2)*d \qquad (2.19)$$

b) Caso bidireccional

El número de demandas de tráfico es (n-2), con lo que la capacidad de tráfico requerida es:

$$C_b = (n-2)*(d1+d2) = (n-2)*d \qquad (2.20)$$

La relacion $R_{u/b}$ será también en este caso igual a 1.

Las capacidades requeridas y el máximo número de nodos pueden verse en la tabla 2.1.

	UNIDIRECCIONAL		BIDIRECCIONAL	
TIPO DE TRAFICO	Capacidad	Número nodos	Capacidad	Número nodos
Entre nodos Adyacentes	n*d	C/d	2*d	Ilimitado.
Uniforme (n impar)	n*(n-1)*d/2	$\sqrt{1 + 8 * C/d} / 2$	$(n^2-1)*d/4$	$\sqrt{1 + 4 * C/d}$
Uniforme (n par, d impar)	n*(n-1)*d/2	$\sqrt{1 + 8 * C/d} / 2$	$n^2*d/4 + n/2$	$(-1 + \sqrt{1 + 4 * C}) / d$
Uniforme (n par, d par)	n*(n-1)*d/2	$\sqrt{1 + 8 * C/d} / 2$	$n^2*d/4$	$2* \sqrt{C/d}$
Con un nodo concentración	(n-1)*d	C/d + 1	(n-1)*d	C/d + 1
Con dos nodos concentración	(n-2)*d	C/d + 2	(n-2)*d	C/d + 2

Tabla 2.1 Resumen de capacidades requeridas y número máximo de nodos para los diversos tipos de tráfico en los anillos unidireccional y bidireccional.

CAPITULO III

Mecanismos de protección en redes digitales sincrónicas

MECANISMOS DE PROTECCION EN REDES DIGITALES SINCRONICAS

3.1 INTRODUCCION

Los mecanismos de protección tienen como objetivo principal mantener la disponibilidad de la red de transporte de telecomunicaciones. Este objetivo es alcanzado mediante el remplazo de los enlaces con falla o degradados. La sustitución es realizada cuando se detecta un defecto, existe una degradación en la calidad del enlace o simplemente se tenga un requerimiento externo por motivo de mantenimiento, actualización de la red debido a cambios en la configuración, etc.

3.2 PROTECCION A NIVEL DE SECCION MULTIPLEX (MSP)

3.2.1 Protección lineal

Está definida como una protección punto a punto, donde la detección de fallas o degradaciones se realiza a nivel de sección múltiplex y la reconfiguración de la red utiliza las funciones de conmutación que están en la subcapa de protección de la sección múltiplex.

3.2.1.1 Proceso de conmutación automática

Es el proceso de conmutación entre dos secciones múltiplex, desde un canal con tráfico hacia el canal de protección. La decisión es tomada de acuerdo al estado del enlace indicado en los bytes **K1** y **K2** de la MSOH.

Byte K1

Los bits 1 a 4 indican el estado o condición del canal cuyo número está definido por los bits 5 a 8. Las tablas 3.1 y 3.2 muestran en detalle su contenido y función.

Bits 1234	Condición, estado o petición externa.	Prioridad
1111	Protección bloqueada en canal 0	Máxima
1110	Conmutación forzada (FS)	I
1101	Señal con falla (SF)- Alta prioridad	I
1100	Señal con falla (SF) - Baja prioridad	I
1011	Señal degradada (SD)- Alta prioridad	I
1010	Señal degradada (SD)- Baja prioridad	I
1001	No utilizada	I
1000	Conmutación manual (MS)	I
0111	No utilizada	I
0110	En espera antes de restablecer (WTR)	I
0101	No utilizada	I
0100	En ejercicio (EXER)	I
0010	Acuse de recibo de petición (RR)	I
0001	Acuse de recibo no requerido (DNR)	I
0000	Ninguna petición (NR)	Mínima.

Tabla 3.1 Tipos de petición en el byte K1.

Bits 5678	Significado
0000	Canal de protección (CERO)
0001	Canal 1. Sección 1 para conmutación predominantemente bidireccional 1+1.
0010	Canal 2. Sección 2 para conmutación predominantemente bidireccional 1+1.
0011/ 1110	Canales 3 a 14.
1111	Canal ocasional de tráfico. Ninguna de las condiciones descritas en la tabla 3.1 es aplicable. Existe solo en configuración 1:n.

Tabla 3.2 Número de canal en el byte K1.

Byte K2

El puente de conmutación mostrado en las figuras 3.1 y 3.2 está controlado por los bits 1 a 5 del byte **K2**. Los bits 6 a 8 indican una **MS-RDI** (valor = 110) y **AIS** (valor = 111)[1]. Los bits 1 a 4 indican el número de canal conectado hacia la protección a través del puente de conmutación (Ver tabla 3.3), mientras que el bit 5 muestra un **0** para una estructura 1+1 y **1** para una estructura 1:n.

[1] El Anexo # 4 presenta una lista completa de las abreviaturas utilizadas en el presente trabajo.

Bits 1234	Significado.
0000	Canal de protección (CERO)
0001	Canal 1 Sección 1 Para conmutación predominantemente bidireccional 1+1.
0010	Canal 2. Sección 2 para conmutación predominantemente bidireccional 1+1.
0000/ 1110	Canales 3 a 14.
1111	Canal ocasional de tráfico. Existe solo en configuración 1:n.

Tabla 3.3 Número de canal en el byte K2.

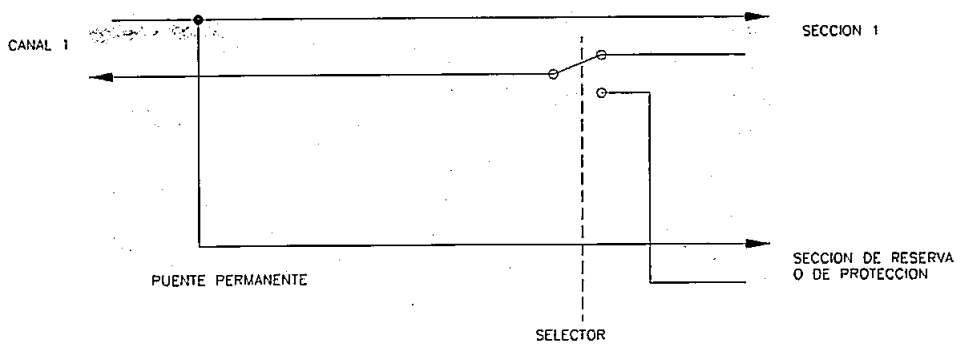


Fig. 3.1 Sistema de protección en configuración 1+1.

En la figura 3.1 existe un puente permanente hacia el canal de protección. Mientras tanto, el selector puede cambiar entre dos estados (**0** o **1**) a saber:

1. Estado **0** permanente para una operación a simple terminal[2] (conmutación solo en Tx).
2. Estados **0** y **1** para operación a doble terminal (conmutación en Tx y Rx), siempre que los bytes **K2** recibido y **K1** enviado contengan el mismo número de canal.

[2] La conmutación a simple terminal es también conocida como unidireccional (se conmuta solo un *sentido de transmisión* del canal). Aquella a doble terminal es conocida como bidireccional (conmutan los dos sentidos de transmisión del canal).

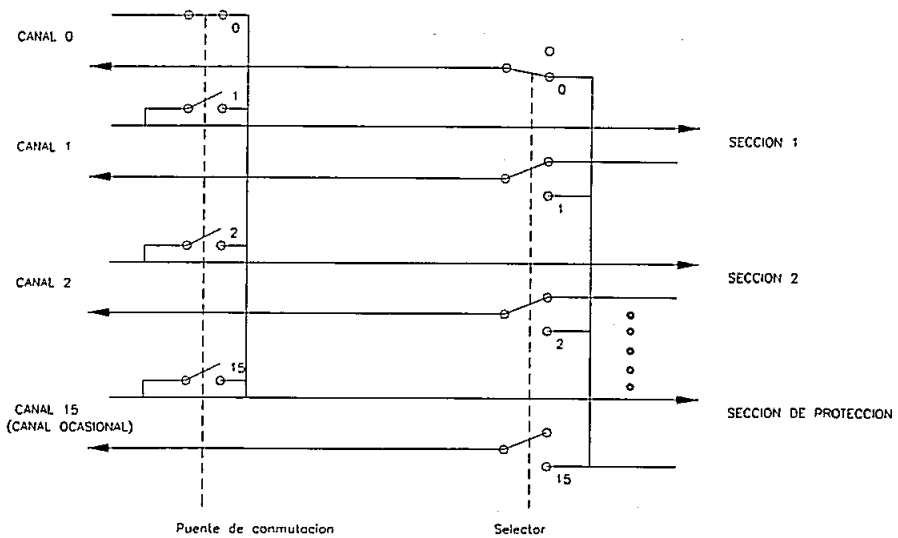


Fig. 3.2 Sistema de protección en configuración 1:n.

El puente de conmutación está asociado con el(los) canal(es) en transmisión, mientras que el selector tiene que ver con el(los) canal(es) en recepción. Por ejemplo, en el caso de una protección a doble terminal, se realiza la comparación de los canales de los bytes **K1** enviado y el **K2** recibido, si ellos coinciden el selector conmuta el canal hacia la protección.

La protección lineal está subdividida en las siguientes clases de acuerdo al tipo de conmutación, a simple o doble terminal:

3.2.1.2 Protección 1:n bidireccional

Se compone de n secciones múltiplex en paralelo más una sección dedicada a la protección. La figura 3.3 muestra un diagrama de bloques para una protección n+1 (n canales principales y un canal de protección).

La MSP evalúa la calidad del canal STM-N entrante y, dependiendo de los parámetros decide la conmutación hacia el canal de protección. Las dos MSP se comunican a través de los bytes **K1** y **K2** del MSOH.

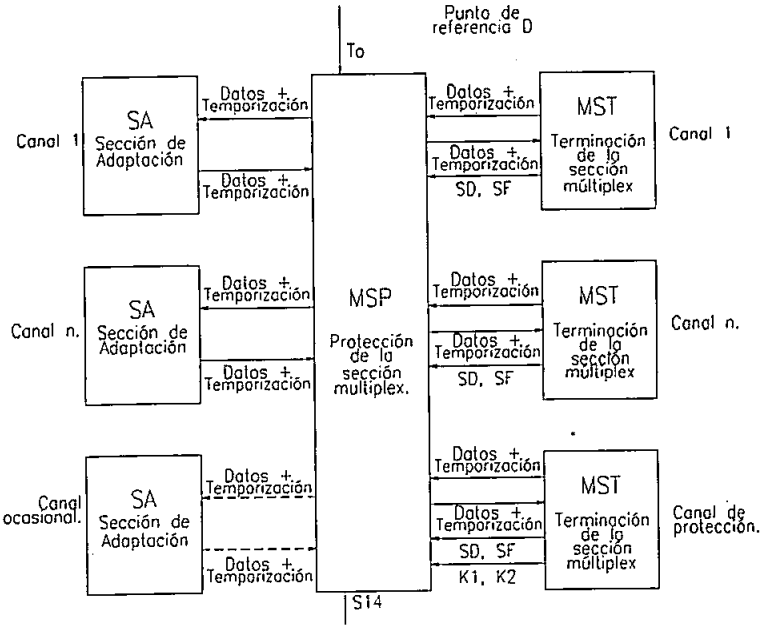


Fig. 3.3 Protección a nivel de sección múltiplex 1:n.

En la figura 3.3 se puede ver la presencia de un canal adicional de tráfico que utiliza la protección en condiciones normales de funcionamiento. Una vez que uno de los canales con tráfico ha conmutado hacia la protección, ese canal adicional se pierde pues no existe ningún tipo de protección para él.

En este tipo de protección 1:n, cada canal que parte de la sección de adaptación (SA) pasa a su correspondiente MST a menos que una falla o degradación sea detectada, entonces se conmuta hacia la protección perdiendo el canal adicional si éste estaba presente.

La conmutación automática (APS) -como se mencionó anteriormente- se realiza en base a las señales con falla (**SF**), señales degradadas (**SD**) recibidas en el punto D. Pero la conmutación puede efectuarse además por requerimientos del Sistema de Administración y Supervisión de Red (TMN). El tiempo de conmutación debe estar

dentro de los siguientes 50 ms luego de haberse detectado la **SF**, **SD** o haber recibido la orden del sistema de telesupervisión TMN. En caso contrario, un mensaje de "falla de protocolo" debería registrarse.

Podría darse el caso de que la calidad de la señal de un canal esté oscilando entre valores alrededor del umbral de decisión, lo que implicaría que la conmutación se produzca en forma intermitente es decir, conmutando hacia la protección y volviendo otra vez hacia el canal original durante muchas veces. Esta situación es controlada mediante la fijación de un valor umbral sobre el cual se debe mantener la calidad de la señal por un período de 5 a 12 minutos, antes de retornar al canal original. Sin embargo, cualquier indicación de **SD** o **SF** de otro canal eliminará esta condición de espera dando paso a la conmutación del mismo hacia la protección.

En la tabla 3.4 se muestra un ejemplo de este tipo de conmutación.

3.2.1.3 Protección 1:n unidireccional

Es idéntica a aquella bidireccional excepto que la conmutación se completa cuando el terminal remoto toma (recibe) de la protección el canal solicitado.

3.2.1.4 Protección 1+1 unidireccional

Cada terminal actúa independientemente del otro. No existe ningún diálogo entre los bytes **K1** y **K2** en ninguna dirección. **K1** se limita solamente a informar sobre la acción local al terminal remoto.

Paso No.	Estado	Terminal A	Terminal B
1	Normal – sin fallas.		
2	Canal 3 con **SD** en dirección A → B.		- Falla detectada. - Orden de conmutar puente del canal 3 hacia la protección.
3		-Puente del Canal 3 conmutado hacia la protección. -Orden hacia B de conmutar puente 3 a la protección.	
4			- Conmutación del selector y puente del canal 3 hacia la protección.
5		-Selector del canal 3 conmutado a la protección. -Conmutación completada.	
6	Canal 1 con **SF** en dirección B → A. (prioridad de **SF** mayor que **SD**).	-Falla (SF) detectada. -Orden de conmutar puente 1 a la protección. - Selector 3 liberado.	
7			-Puente 1 conmutado a la protección. -Orden hacia A de conmutar puente 1 a la protección. -Selector 3 liberado.
8		-Selector 1 y puente 1 conmutados hacia la protección.	
9			-Selector 1 conmutado a la protección. Final de la conmutación.
10	Canal 1 reparado pero canal 3 todavía con **SD**.	En espera antes de restablecer **WTR**.	
11			-Orden de conmutar puente 3 hacia la protección. -Selector 1 liberado.
12		-Puente 3 conmuta a la protección. -Selector 1 liberado. -Orden hacia B de conmutar puente 3 a la protección.	
13			-Selector 3 y puente 3 conmutan a la protección.
14		-Selector 3 conmuta a la protección. -Conmutación completada.	
15	Canal 3 reparado.		-En espera antes de restablecer.
16	Tiempo de **WTR** ha finalizado (Ninguna falla presente).		-Mensaje de ninguna petición (o lo que es igual, "pedido de restablecer el puente 3 a su estado normal"). -Selector 3 liberado.
17		-Puente 3 regresa a su estado normal. -Mensaje de ninguna petición hacia B (o "restablecer el puente 3 en B a su estado normal"). -Selector 3 liberado.	
18			-Puente 3 retorna al estado normal.

Tabla 3.4 Ejemplo de conmutación tipo 1: n bidireccional.

3.2.1.5 Protección 1+1 bidireccional compatible con 1:n bidireccional

En el caso de conmutación reversible el proceso es igual a lo explicado en la sección 3.2.1.2. El canal con tráfico está conectado directamente a la protección y se indica en el byte **K2**.

Para el caso no reversible el proceso puede ilustrarse con el siguiente ejemplo:

Paso No.	Estado	Terminal A	Terminal B
1	Normal		
2	Canal 1 con SF en dirección A → B		-SF detectada. -Orden de conmutar el puente 1 a la protección.
3		-Puente 1 conmutado. -Orden hacia B de conmutar puente 1 a la protección.	
4			-Puente 1 conmutado. -Selector 1 conmutado.
5		-Selector 1 conmutado. -Conmutación bidireccional completada.	
6	Canal 1 reparado pero todavía utilizando canal de protección [No reversible].		-Envío de "Acuse de recibo no requerido".
7	Canal de protección con SD de A → B		-SD detectada. -Orden de conmutar puente 0 hacia canal 1. -Selector 1 liberado.
8		-Orden hacia B de conmutar puente 0 hacia canal 1. -Puente 1 retorna sobre canal 1. -Selector 1 liberado.	
9			-Puente 1 retorna al canal 1.
10	Canal de protección reparado.		-Envía mensaje de "Ninguna petición".
11		-Envía mensaje de "Ninguna petición".	

Tabla 3.5 Ejemplo de protección 1+1 bidireccional compatible con 1:n bidireccional.

3.2.1.6 Protección 1+1 bidireccional optimizada para una red con conmutación predominantemente 1+1 bidireccional

Se basa en una conmutación no reversible (no utiliza el canal de protección o **0**) entre los canales **1** y **2**, teniendo como objetivo alcanzar una conmutación ágil y veloz para la configuración 1+1 bidireccional. El tráfico está siempre presente en los dos canales debido a la permanente conexión del puente de conmutación. El byte **K2** indicará el número de canal con tráfico y solamente cambiará una vez que la conmutación haya sido completada, es decir, cuando los selectores de ambos terminales hayan conmutado hacia el canal requerido (**1** o **2**) y además se recibe el mensaje de "Ninguna petición" en cada uno de ellos. El siguiente ejemplo tiene por objeto ilustrar el proceso de protección.

Paso No.	Estado	Terminal A	Terminal B
1	Normal		
2	SF en canal 1 en el terminal B		-Petición local de SF detectada. -Byte K1 actualizado con SF en canal 1.
3		-Petición remota detectada. -Canal 1 conmutado hacia canal 2 (*).	
4			-Detecta aviso de que el canal 1 ha sido conmutado. -Conmuta canal 1 hacia canal 2 (*).
5	Canal 1 reparado en terminal B. (En "Espera antes de restablecer").		
6	Tiempo de "Espera antes de restablecer" finalizado.		- Envía mensaje de "Ninguna petición". -Actualiza K1 y K2. -Canal 2 lleva ya tráfico.
7		-Detecta mensaje de "Ninguna petición". -Actualiza K1 y K2. -Canal 2 lleva ya tráfico.	

(*): K2 mantiene todavía 0001 en los bits 1-4.

Tabla 3.6 Ejemplo de protección 1+1 bidireccional optimizada para una red con conmutación predominantemente 1+1 bidireccional.

3.2.2 Anillo de protección compartida (*SPRing*)

Se basa en la configuración de los anillos bidireccionales introducidos en la sección 2.1 y se caracteriza por tener una capacidad de tráfico de protección accesible a cualquiera de los canales con tráfico dentro del anillo. Existen dos maneras de poner en práctica este tipo de protección: a dos y cuatro fibras.

Dentro de la arquitectura de anillos existen básicamente dos tipos de conmutación para la protección del tráfico:

Conmutación del enlace: Es la acción de conmutar desde los canales con tráfico hacia los canales de protección solamente en el enlace que ha sufrido fallas o defectos.

Conmutación del anillo: La conmutación hacia la protección se realiza a lo largo de toda la trayectoria del anillo, excepto en el enlace o nodo afectados.

3.2.2.1 Anillo de protección compartida a dos fibras

Está formado por una fibra que lleva la mitad de los canales con tráfico y su protección en una dirección, mientras que la otra fibra lleva la segunda mitad del tráfico y su respectiva protección en dirección opuesta (Ver figura 3.4 a). Es importante notar que en este caso la capacidad de cada fibra es dividida en dos partes iguales: una para canales con tráfico (numerados de 1 a N/2, donde N es el número total de canales con tráfico) y otra para los canales de protección (de N/2 +1 a N), ambas bajo una misma SOH. El canal m (m = 1,..., N/2) será protegido por el canal N/2 + m.

La conmutación se realiza en base al protocolo de Protección por Conmutación Automática (APS) mediante los bytes **K1** y **K2** de la SOH.

Las figuras 3.4 b) y c) muestran la acción de conmutación para la protección en caso de rotura de un enlace o un nodo del anillo. El tipo de conmutación utilizada en este caso es conmutación del anillo.

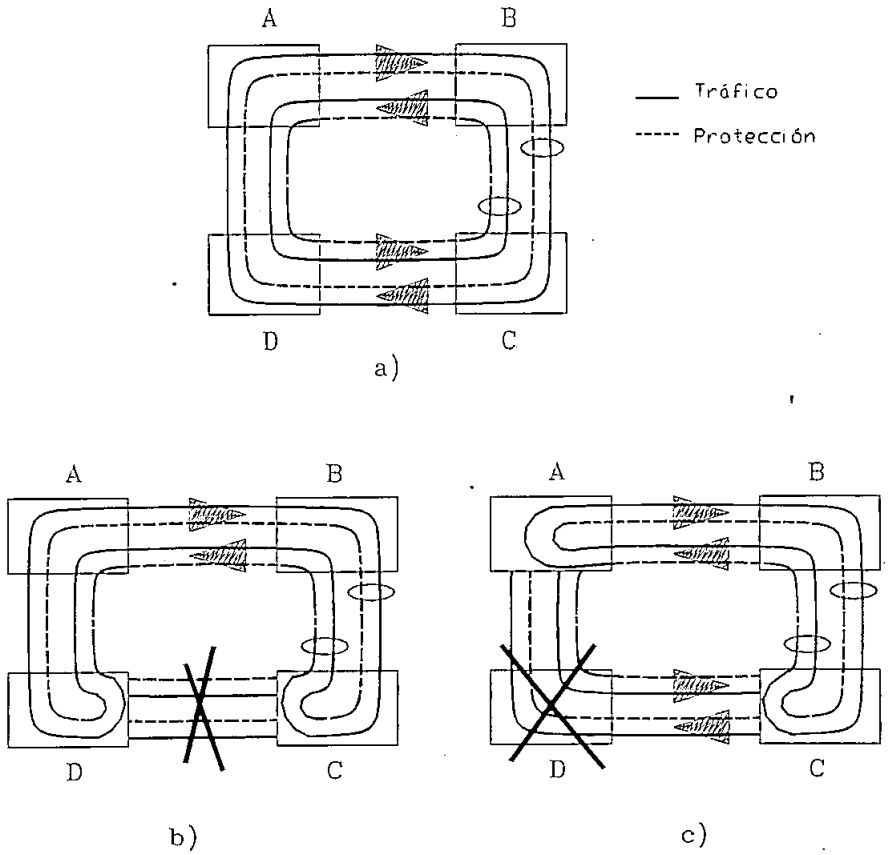


Fig. 3.4 a) Anillo de protección compartida a dos fibras. Condiciones normales.
b) Reconfiguración del anillo a 2 fibras ante rotura de un enlace.
c) Reconfiguración del anillo a 2 fibras ante falla de un nodo.

Como se puede apreciar en las figuras 3.5 a) y b), la protección se realiza mediante la conmutación automática de los canales afectados de una fibra, hacia los canales de protección de la otra fibra que va en dirección opuesta dentro del anillo[3]. Nótese que la conmutación, aun en el caso de la rotura del enlace en un solo sentido, se produce en los dos nodos adyacentes al enlace o nodo con falla, es decir es una conmutación a doble terminal.

Debido a que la protección se realiza a nivel de sección múltiplex (AU-n) y, considerando que en este tipo de protección la capacidad de tráfico (principal más protección) se divide en dos partes iguales, este tipo de protección no se aplica a anillos STM-1.

---

[3]ETSI, DTR/TM-03025 Transmission and Multiplexing, SDH Protection: Rings and Other Schemes, Sophia Antipolis Cedex - France, October, 1994.

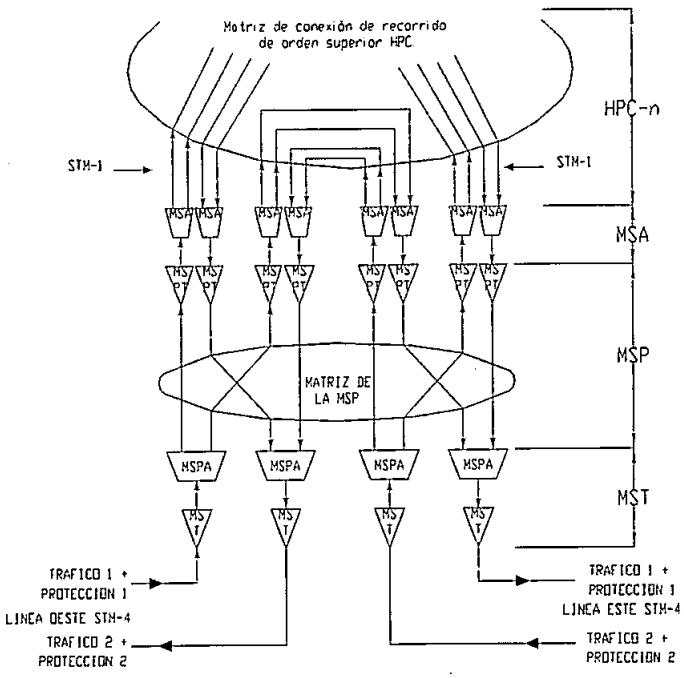


Fig. 3.5 a) Anillo de protección compartida. Modelo funcional de un nodo para un anillo a dos fibras en condiciones normales.

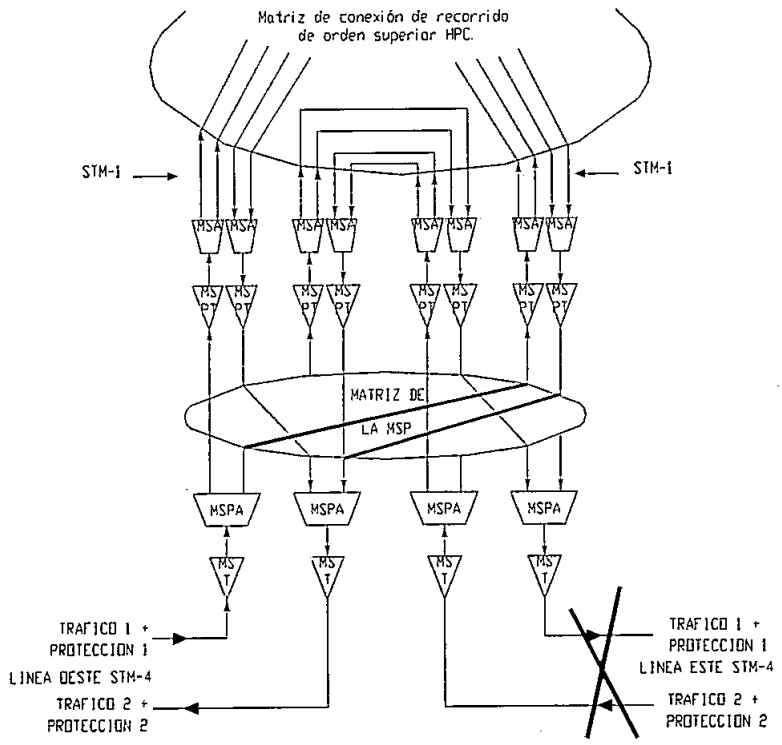


Fig. 3.5 b) Anillo de protección compartida. Modelo funcional para un anillo a dos fibras. Rotura de la línea Este.

De igual manera que en la Protección Lineal vista en la sección 3.2.1, existe la posibilidad de transportar una "capacidad extra de tráfico" (no importante) utilizando la capacidad asignada a la protección. También en este caso la capacidad extra de tráfico se pierde si es que se produce la conmutación de los canales principales canales hacia la protección en el anillo.

3.2.2.2 Anillo de protección compartida a cuatro fibras

Está formado por dos fibras que llevan los canales con tráfico en una dirección y dos fibras que representan la protección pero que viajan en dirección opuesta. Equivale a separar la protección del tráfico en un anillo a dos fibras, independizando cada uno de ellos y añadiendo su propia sección de *overhead* (SOH) (Ver figura 3.6).

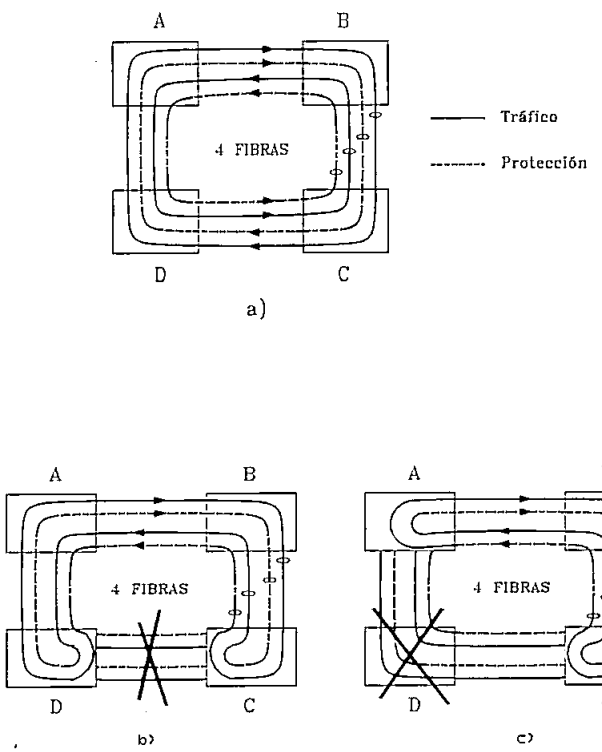


Fig. 3.6 a) Anillo de protección compartida a 4 fibras. Condiciones normales.
b) Reconfiguración del anillo a 4 fibras ante rotura del enlace.
c) Reconfiguración del anillo a 4 fibras ante falla de un nodo.

En el caso de anillos a 4 fibras, los dos tipos de conmutación (de enlace y de anillo) son aplicables y, de acuerdo a la prioridad de los requerimientos serán activados o anulados (Ver sección 3.2.2.3).

La conmutación se lleva a cabo mediante los bytes **K1** y **K2** (bits 1 a 5) de la SOH los cuales son activos solo en las fibras dedicadas a los canales de protección[4].

El proceso de conmutación es análogo al mostrado para el anillo de 2 fibras con la diferencia de que en este caso la conmutación es total desde una fibra con tráfico hacia la de protección en sentido opuesto.

3.2.2.3 Protección por conmutación automática (APS) para anillos de protección compartida

En el proceso de conmutación es necesario definir las prioridades de las peticiones de acuerdo al tipo de falla, el tipo de canal a ser protegido, etc. La tabla 3.7 muestra el tipo de petición y su respectiva prioridad contenida en los bits 1 a 4 de **K1**, mientras que el número de identificación del nodo de destino está contenido en los bits 5 a 8. El número de nodo de destino es el de aquel nodo hacia el cual se transmite el byte **K1**. Este número corresponde siempre al de un nodo adyacente.

Bits 1234	Tipo de petición
1111	Protección bloqueada (en el enlace) o Señal con falla (protección) LP-S
1110	Conmutación forzada (del enlace) FS-S
1101	Conmutación forzada (del anillo) FS-R
1100	Señal con falla (enlace) SF-S
1011	Señal con falla (anillo) SF-R
1010	Señal degradada (protección) SD-P
1001	Señal degradada (enlace) SD-S
1000	Señal degradada (anillo) SD-R
0111	Conmutación manual (enlace) MS-S
0110	Conmutación manual (anillo) MS-R
0101	En espera antes de restablecer WTR
0100	Ejercicio (enlace) EXER-S
0011	Ejercicio (anillo) EXER-R
0010	Acuse de recibo (enlace) RR-S
0001	Acuse de recibo (anillo) RR-R
0000	Ninguna petición NR

Tabla 3.7 Tipos de petición en el byte K1 y sus prioridades (mayor de arriba hacia abajo).

Como se puede ver en la tabla 3.7, las acciones relativas a un enlace tienen mayor prioridad que para un anillo en el caso de tener el mismo tipo de petición.

[4] ITU-T, Draft of New Rec. G.783, Geneve, July, 1994.

Obviamente, una petición de mayor prioridad de un anillo anulará la petición de un enlace.

Cuando se ha producido una conmutación del anillo y existe una falla que provoca una petición de igual o mayor prioridad que "señal con falla" (**SF-R**), una nueva conmutación del anillo se debe llevar a cabo provocando la segmentación del anillo en dos partes independientes. Si la nueva petición es de menor prioridad ésta será ignorada.

El estado o la recepción de una petición en un nodo son comunicados hacia el resto del anillo a través de los canales D1-D12 de la SOH (sección 1.1.7.2).

a) Criterios de conmutación

El inicio del proceso de conmutación puede darse por peticiones externas a la red (mantenimiento, ejercicio de pruebas, etc.) o automáticamente a través de la detección de parámetros de comportamiento de la red.

Dentro del primer grupo de peticiones (externas) se pueden tener las siguientes:

1. Comandos no considerados dentro de la protección por conmutación automática (APS) como:
   - Anulación de cualquier comando ya iniciado o "en espera antes de restablecer".
   - Bloqueo de la conmutación del anillo, negando al nodo la capacidad de acceso al canal de protección dentro del anillo sin importar el estado o condición del canal con tráfico. Si el tráfico está siendo transmitido a través de la protección, éste será conmutado hacia su respectivo canal principal y un mensaje de "ninguna petición" será transmitido.
   - Bloqueo a la conmutación del enlace, similar al anterior pero para un enlace solamente.
   - Bloqueo de protección, donde ninguna conmutación (sea de enlace o de anillo) hacia la protección es permitida en el anillo.
2. Comandos dentro de la APS
   - Referirse a la lista de la tabla 3.7 anteriormente mostrada.
   - Bloqueo de protección de enlace (**LP-S**), impide el acceso a la protección en aquel

enlace e incluso en el anillo si aquel enlace forma parte de la trayectoria de una conmutación del anillo.

- Conmutación forzada (de enlace y anillo) (**FS-S** y **FS-R**), conmuta hacia la protección de aquel enlace o anillo a menos que exista una petición de mayor prioridad.
- Conmutación manual (de enlace o anillo) (**MS-S** y **MS-R**), conmuta hacia la protección a menos que una petición de mayor prioridad esté presente.
- Pruebas de enlace y anillo (**EXER-S** y **EXER-R**), permite simular una conmutación de enlace o anillo sin afectar los canales con tráfico involucrados. Estas pruebas son esenciales para garantizar la verdadera conmutación cuando ésta sea requerida.

La iniciación automática en cambio se procesa a través del monitoreo de los canales de protección y portadores de tráfico a nivel de la sección múltiplex como:

- Señal con falla a nivel de enlace (**SF-S**), permite que el terminal remoto pida al terminal local la conmutación hacia la protección, iniciando una conmutación de enlace.
- Señal con falla a nivel de anillo (**SF-R**), inicia la conmutación del anillo si éste está formado por 2 fibras. En el caso de tener un anillo de 4 fibras, la conmutación del anillo se produce solamente si la conmutación del enlace (en el enlace afectado) no es suficientemente eficaz en la protección del tráfico (es decir si ambos, el tráfico y la protección han sido afectados).
- Señal con falla (canal de protección) (**SF-P**), indica la rotura del canal de protección, lo que equivale a tener una indicación de "Bloqueo de protección". Efectivamente, una indicación de **LP-S** es transmitida.
- Señal degradada en el enlace y anillo (**SD-S** y **SD-R**), inicia la conmutación cuando una señal entre dos secciones múltiplex presenta características pobres de calidad (**SD**) (Ver Anexo # 2, bloque MST). Para un anillo a 2 fibras, la protección contra este tipo de fallas se produce mediante la conmutación del anillo, mientras que para 4 fibras la conmutación del anillo es utilizada solo en caso de que la conmutación del enlace no sea suficiente.
- Señal degradada (canal de protección) (**SD-P**), indica la existencia de un canal de protección con baja calidad de la señal. Su presencia implica el retorno inmediato de los canales con tráfico a sus canales habituales, a menos que exista una

petición de mayor prioridad.

- En espera antes de restablecer (**WTR**), al igual que en la conmutación de la protección lineal (sección 3.2.1), su presencia indica que los canales con tráfico están bajo observación antes de volver a su estado habitual. Se aplica solamente después de una condición de **SD** o **SF**.
- Acuse de recibo en el enlace y anillo (**RR-S** y **RR-R**), es la confirmación (hacia el terminal remoto) de haber recibido el pedido de conmutar, sea el enlace o el anillo.

b) Definiciones para la conmutación automática

Los bytes **K1** y **K2** de la SOH son los responsables del proceso de control y conmutación a nivel de sección múltiplex. La tabla 3.8 muestra la estructura y significado de los bits de **K2**.

Identificación del nodo de origen (bits 1 a 4)	Trayectoria Larga/corta	Estatus (bits 6 a 8)	Significado
Es el número del nodo emisor del estatus	0 = corta 1 = larga	111	**MS-AIS**
		110	**MS-RDI**
		101	Uso futuro
		100	Uso futuro
		011	Uso futuro
		010	Puente y selector conmutados
		001	Puente conmutado
		000	Ninguna acción.

Tabla 3.8 Estructura y significado del byte **K2**.

1. La **trayectoria corta** se refiere al enlace sobre el cual se ha emitido o se está produciendo la conmutación.
2. **Trayectoria larga** en cambio es el camino dentro del anillo que excluye el enlace sobre el que se ha pedido o se está produciendo la conmutación[5].
3. **Selector**: Es el dispositivo de selección de los canales en recepción ya sea los canales con tráfico o los de protección
4. La relación entre los bits 1-4 de **K1** y el bit 5 de **K2** se muestra en la tabla 3.9.

[5] De esta manera, la trayectoria corta se relaciona con la conmutación de enlace y la trayectoria *larga con la* conmutación del anillo.

	Bits 1 a 4 de K1	
Bit 5 de K2	Conmutación del anillo	Conmutación del enlace
Trayectoria larga (=1)	Petición de conmutación del puente	Recepción de la petición de conmutación del puente
Trayectoria corta (=0)	Recepción de la petición de Conmutación del puente	Petición de conmutación del puente

Tabla 3.9 Relación entre bits 1-4 de K1 y bit 5 de K2[6].

5. **Petición de conmutación**: Es el mensaje del nodo remoto hacia el nodo local solicitando la conmutación del puente de transmisión hacia la protección.
6. **Recepción de la petición de conmutación**: Es el mensaje del nodo remoto hacia el resto de nodos del anillo informando que se ha emitido una petición de conmutación del puente en aquel nodo.
7. **Estado pasivo**: Estado de inactividad total de la conmutación automática APS en el nodo. Los bits de **K1** y **K2** se transmiten en ambas direcciones adoptando la siguiente configuración:

K1 Bits 1 a 4	K1 Bits 5 a 8	K2 bits 1 a 4	K2 bit 5	K2 bits 6 a 8
0000	No. de nodo de destino	No. de nodo de origen.	0 (trayectoria corta)	000 (ninguna acción)

Tabla 3.10 Configuración de K1 y K2 en estado pasivo.

En este estado, el número de nodo de origen es igual a aquel del nodo destino.

8. **Estado de conmutación**: Es el estado de generación, procesamiento y recepción de un pedido de conmutación. La configuración de los bytes **K1** y **K2** se muestra en la tabla 3.11.

K1 Bits 1 a 4	K1 bits 5 a 8	K2 bits 1 a 4	K2 bit 5	K2 bits 6 a 8
Petición de conmutación (Tabla 3.7)	No. de nodo de destino	No. de nodo de origen	0/1 (trayectoria corta o larga)	Estatus (Ver tabla 3.8)

Tabla 3.11 Configuración de K1 y K2 en estado de conmutación.

[6] K1 y K2 se refieren a un mismo nodo.

Nótese que en este estado, **K1** transmite la petición de conmutación hacia el nodo adyacente (nodo de destino) cuya sección presenta fallas o degradaciones, y **K2** transmite el estado del puente de conmutación en el nodo de origen.

9. **Estado de *By-Pass***: Los bytes **K1**, **K2** y los canales de protección recibidos desde una dirección se transmiten directamente hacia la otra dirección.

3.2.3 Anillo de protección dedicada (*DPRing*)

Es aplicable a anillos de tipo unidireccional como el de la figura 2.1. Su nombre de "dedicado" se debe a que cada canal con tráfico está provisto de su canal de protección, es decir existe una protección 1:1 o 1+1.

No está permitido ningún tráfico adicional. Es claro que la suma de todas las demandas de tráfico en el anillo no puede superar la capacidad máxima de protección de cualquiera de los enlaces del anillo.

Este tipo de protección puede ser puesto en práctica en anillos a dos o cuatro fibras.

3.2.3.1 Anillo de protección dedicada a dos fibras

La fibra perteneciente al anillo principal transporta el canal con tráfico en una dirección, mientras la otra fibra -del anillo de protección- adopta la dirección opuesta de transmisión. La figura 3.7 a) muestra la disposición de las fibras en el anillo.

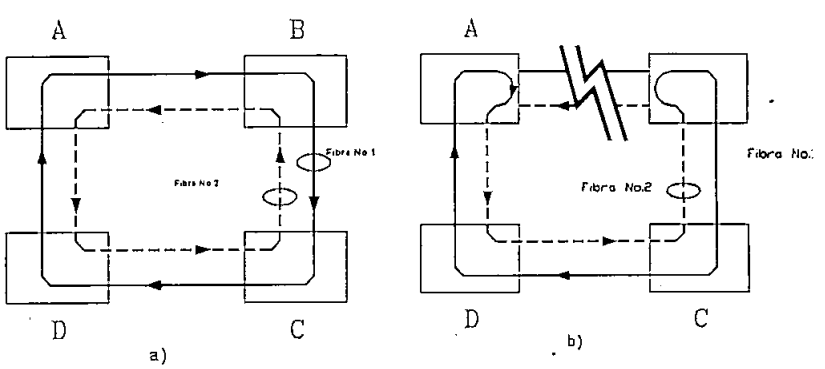


Fig. 3.7 a) Anillo de protección dedicado a dos fibras. Condiciones normales.
b) Reconfiguración ante rotura de un enlace.

Cuando existe la rotura de uno de los enlaces del anillo, la fibra portadora de tráfico conmuta hacia la de protección (dentro de los 50 ms siguientes a la detección de la rotura), enviando el tráfico en dirección contraria (Ver la figura 3.7 b). Obviamente la rotura de más de un enlace provocará la segmentación del anillo permitiendo solamente una comunicación parcial dentro del anillo. En el caso de falla de un nodo, la lógica de conmutación hacia la protección se produce de manera similar pero en los dos nodos adyacentes al nodo con falla.

La conmutación de tráfico se realiza a nivel de sección múltiplex, cuando se ha detectado la presencia de **LOS**, **LOF**, **MS-AIS** o debido a la presencia de errores una vez que se ha realizado el conteo mediante los bytes **B2** de la MSOH. Las figuras 3.8 a) y b) muestran el modelo funcional de un sistema a dos fibras con la correspondiente acción de protección realizada cuando existe la falla de uno de los enlaces del anillo[7]; solo uno de los nodos vecinos al enlace con falla es mostrado. Nótese que la matriz de la parte superior se encarga solamente de la interconexión de canales a nivel de recorridos de orden superior (*Cross-connection*), mientras la matriz de la sección múltiplex se encarga de la conmutación en sí de los canales a nivel STM-N.

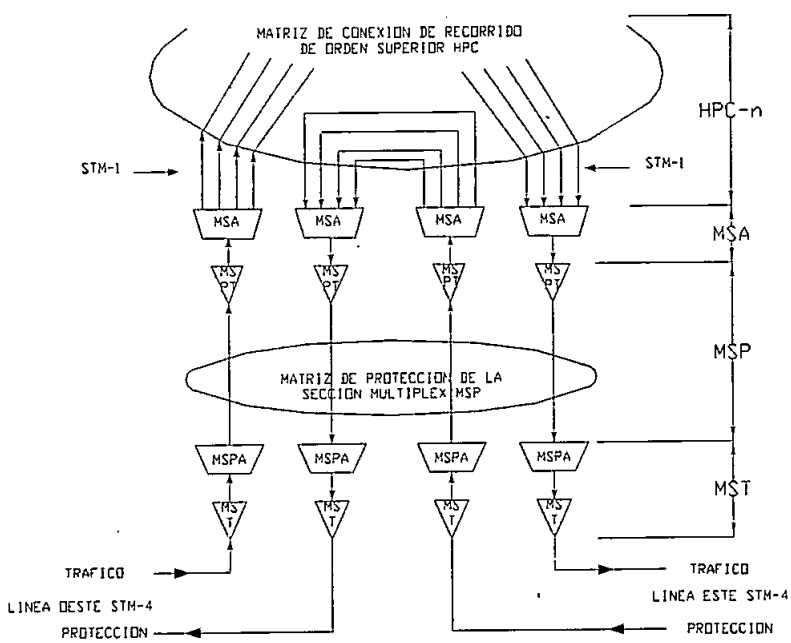


Fig. 3.8 a) Modelo funcional de un anillo de protección dedicado a dos fibras. Condiciones normales.

[7] ETSI, DTR/TM-03025 Transmission and Multiplexing, SDH Protection: Rings and Other Schemes, Sophia *Antipolis Cedex* - France, October, 1994.

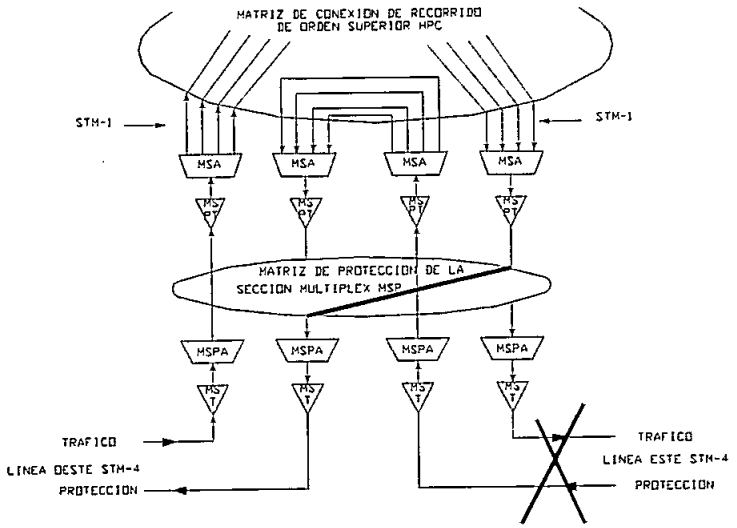


Fig. 3.8 b) Modelo funcional de un anillo de protección dedicado a dos fibras.
Reconfiguración ante la rotura de la línea Este.

3.2.3.2 Anillo de protección decicada a cuatro fibras

Es simplemente la duplicación del anillo a dos fibras: dos fibras llevan los canales con tráfico en una dirección y las otras dos fibras de protección viajan en dirección opuesta (Ver figura 3.9 a). La conmutación hacia la protección se realiza de manera similar al caso de dos fibras cuando se produce la rotura de un enlace o la falla de un nodo del anillo (Figura 3.9 b).

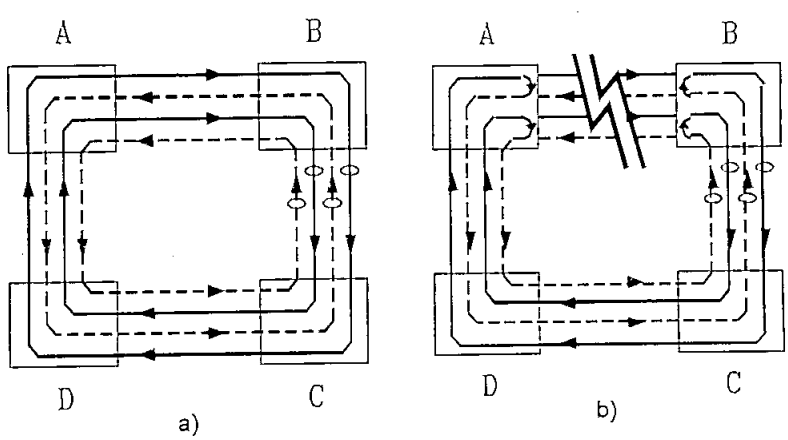


Fig. 3.9 a) Anillo de protección dedicado a cuatro fibras. Condiciones normales
b) Reconfiguración ante rotura de un enlace.

3.2.3.3 Protección por conmutación automática (APS) para anillos de protección dedicada

La protección por conmutación automática se aplica por ahora solamente a anillos con configuración 1+1. La APS para 1:1 se encuentra en fase de definición.

a) Criterios de conmutación

El protocolo aquí utilizado es compatible con aquel expuesto para la protección a nivel de sección múltiplex en configuración 1+1 bidireccional (sección 3.2.1.5).

Entre otros requerimientos de conmutación se mencionarán en primer lugar las peticiones externas tales como:

1. Peticiones no incluidas en el canal de la APS:
   - Borrado, cancela cualquier comando en curso.
2. Peticiones consideradas dentro del canal de la APS:
   - Bloqueo de la protección (**LP**), impide el acceso de los canales con tráfico a los canales de protección.
   - Conmutación forzada (**FS-W**), conmuta los canales con tráfico hacia la protección en aquel enlace incluyendo el nodo que originó el comando y su respectivo nodo de destino.
   - Conmutación manual (**MS-W**), conmuta los canales con tráfico hacia la protección cuando no exista una falla o degradación en el canal de protección. Incluye los nodos adyacentes al enlace.
   - Pruebas (**EXER**), permite simular el proceso de protección sin completar realmente la conmutación ni la selección. La orden es emitida y sus respuestas verificadas pero ningún canal con tráfico es realmente involucrado en la operación.

La iniciación automática de la conmutación en cambio implica el monitoreo de las condiciones del canal.

1. Señal con falla (**SF**).
2. Señal degradada (**SD**).

3. Acuse de recibo (**RR**), indicación hacia el terminal remoto de que se ha recibido la orden de conmutar.
4. En espera antes de restablecer (**WTR**), se ejecuta luego del restablecimiento de una **SD** o **SF** para garantizar que el canal con problemas está efectivamente apto para volver a operar en condiciones normales.

b) Definiciones para la conmutación automática

1. La generación de los bytes **K1** y **K2** del canal APS es idéntica a aquella mostrada en la sección 3.2.1.1, con la excepción de que el comando externo de bloqueo de la protección (**LP**) no es aplicable.
2. Dado que las peticiones en un anillo pueden darse en diferentes enlaces al mismo tiempo, las peticiones como: Conmutación forzada y manual, Señal con falla, Señal degradada tienen igual prioridad.

3.3 PROTECCIÓN A NIVEL DE RECORRIDO

Básicamente, un modelo de red de telecomunicaciones se compone de un grupo de funciones de transporte y de control. Dentro del primer grupo se encuentran las funciones desarrolladas para garantizar la transferencia de información entre dos o más nodos, mientras que dentro del grupo de las funciones de control están aquellas relacionadas con la operación, administración y mantenimiento de la red.

Las funciones de transporte se identifican en base a una estratificación por capas[8] (Ver figura 3.10).

1. **Capa de circuito**: Está relacionada con los servicios de telecomunicaciones como conmutación de paquetes, circuitos, etc.
2. **Capa de recorrido**: Está constituida por las estructuras de transporte de orden superior (VC-3/4/n) e inferior (VC-11/12/3).
3. **Capa de transmisión**: Se asocia al medio de transmisión utilizado, como fibra, radio, etc. Esta se subdivide a su vez en dos capas (Ver figura 3.11).

---

[8] ITU-T, Rec. G.803, Architecture of transport networks based on Synchronous Digital Hierarchy SDH, Geneve, March, 1993.

- **Capa de sección**: Está relacionada con la transferencia de información entre dos nodos en la capa de recorrido y se descompone en sección múltiplex y sección regenerador (Ver sección 1.1.7.1).
- **Capa del medio físico**: Es el medio de transporte en sí (radio, fibra, cable, etc.).

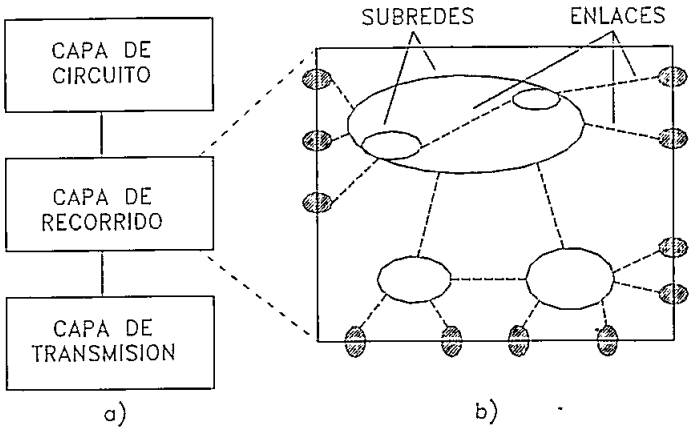


Fig. 3.10 Estructura de una red de transporte. a) Estratificación por capas. b) Partición topológica.

Cada una de estas capas se descompone internamente en subredes y enlaces que originan una expansión ortogonal de la red. Este concepto se conoce con el nombre de "Partición" y se muestra en la figura 3.10 b).

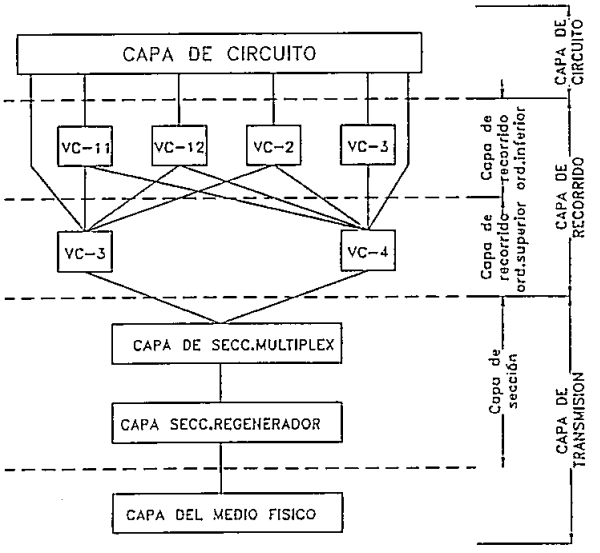


Fig. 3.11 Estratificación por capas.

Las diversas capas se asocian entre sí a través de una relación *cliente*/servidor que consiste en que las funciones de una capa superior (cliente), para transferir información entre dos puntos, utilizan los recursos de otra capa de menor nivel

(servidor), Esta capa de servidor es la que ejecuta las acciones necesarias para transportar la información en modo transparente. Por ejemplo, una conexión en la capa de recorrido (cliente) utiliza las funciones asociadas a la capa de sección múltiplex (servidor) (Ver figura 3.12).

Algunas definiciones importantes se presentan a continuación:

Conexión: Es una función de transporte encargada de transferir en modo transparente la información entre dos puntos.

Pista o trayectoria (*trail*): Función de transporte perteneciente a un nivel servidor que sirve como ruta de conexión para el cliente.

Terminación de pista: Función de transporte situada en los extremos de una pista. Se encarga principalmente de generar y recibir la información del SOH.

Adaptación cliente/servidor: Función de transporte encargada de adaptar la capa del servidor a las necesidades del cliente.

Punto de conexión (CP): Es la unión entre dos conexiones o entre una conexión y una adaptación cliente/servidor.

Punto de conexión terminal (TCP): Es la unión entre una conexión y una terminación de pista.

Punto de acceso (AP): Punto de unión entre una adaptación cliente/servidor y una terminación de pista. Este constituye el límite entre dos capas.

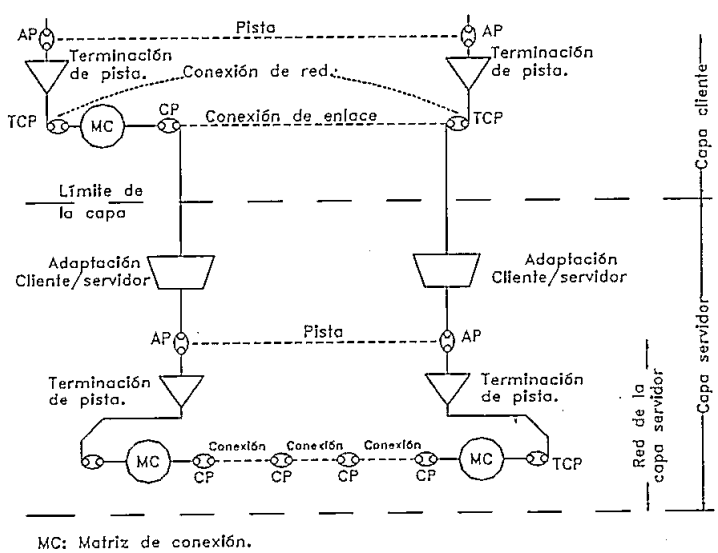


Fig. 3.12 Modelo de conexión asociada a la estratificación por capas[9].

[9] ITU-T, Recommendation G.803, Architecture of transport networks based on Synchronous Digital Hierarchy SDH, Geneve, March, 1993.

3.3.1 Protección a nivel de contenedor virtual (VC)

Este tipo de protección se aplica a nivel de contenedores virtuales, desde el punto en que ellos son insertados en la red sincrónica hasta su llegada al nodo destino. La red puede adoptar cualquier topología (siempre que permita al menos dos trayectorias distintas) y no existe limitación en cuanto al número de nodos dentro de ella.

Pueden existir protecciones de los VC de tipo 1+1 (protección dedicada) o 1:1 (protección compartida con capacidad de tráfico adicional), aunque esta última se encuentra en proceso de elaboración por parte del ITU-T.

Toda protección a este nivel inicia y termina con la generación y recuperación del POH para cada VC. La protección puede efectuarse indiferentemente para contenedores virtuales de orden superior (VC-3/4) o de orden inferior (VC-11/12/3) siendo el mismo protocolo de conmutación APS aplicable a ambos casos. El protocolo de conmutación se desarrolla a través de los bytes **K3** y **K4** del POH (*path overhead*).

Al igual que para las protecciones vistas anteriormente, un tiempo máximo de conmutación de 50 ms es recomendado, sin considerar el tiempo necesario para la detección de la falla y la puesta en marcha de la protección.

La estrategia general de protección utilizada en este caso es que, para cada dirección de transmisión, los canales de protección deben viajar a través de trayectorias diferentes respecto a los canales con tráfico. En la sección 2.1 se presentaron los dos tipos de anillo (unidireccional y bidireccional) cuyas formas de enrutamiento son utilizadas para la protección a nivel de VC a través de una red o anillo.

Las figuras 3.13 y 3.14 muestran los dos casos de protección (unidireccional y bidireccional) de los contenedores virtuales.

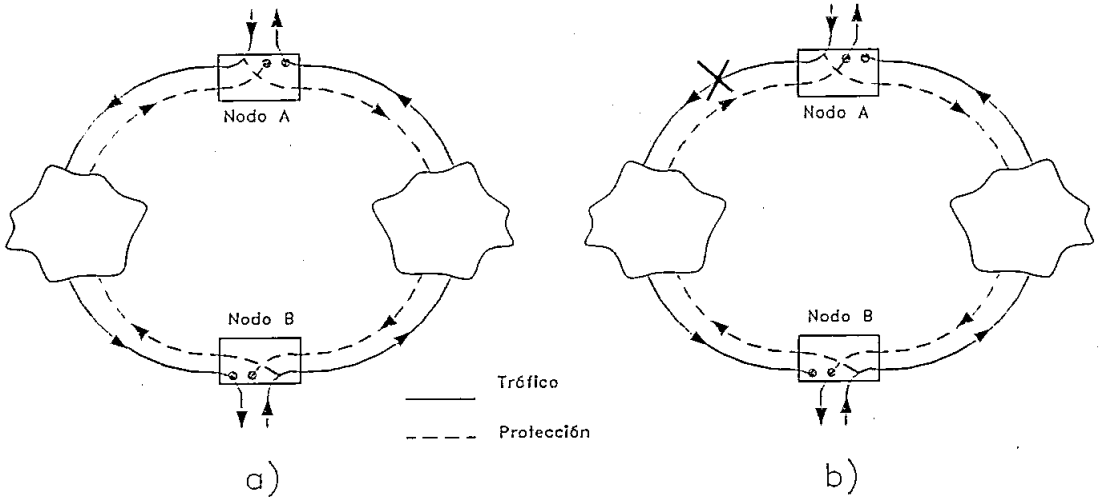


Fig. 3.13 Protección a nivel de contenedor virtual con enrutamiento unidireccional.
a) Condiciones normales b) Rotura de una de las fibras y acción de protección.

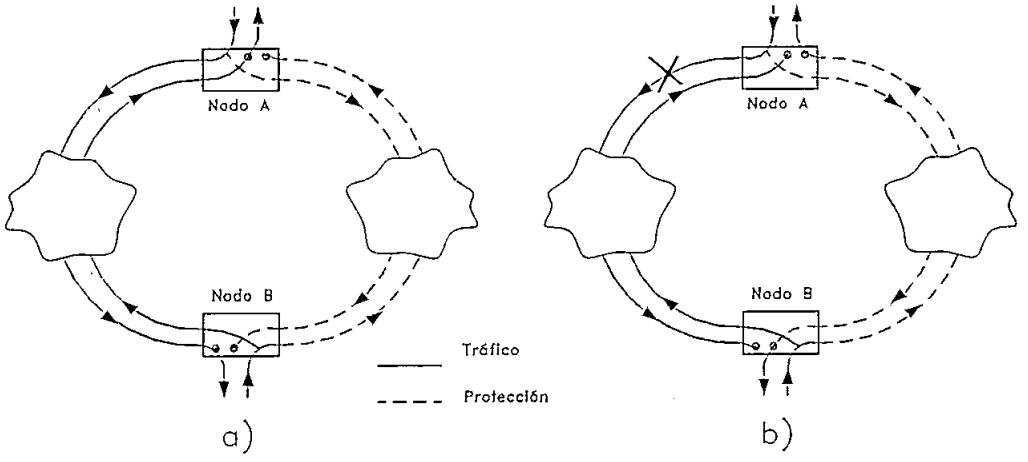


Fig. 3.14 Protección a nivel de contenedor virtual con enrutamiento bidireccional.
a) Condiciones normales b) Rotura de una de las fibras y acción de protección.

En el terminal de transmisión, el contenedor virtual es duplicado y enviado a través de dos trayectorias diferentes dentro de la red, mientras que en la recepción un selector escoge el canal cuya calidad está dentro de condiciones aceptables.

El modelo funcional de este tipo de protección[10] se muestra en la figura 3.15 a). La conmutación a través de los canales APS es necesaria solo cuando el sistema es provisto de una conmutación a doble terminal. En el caso de la figura 3.15 b) se muestra un sistema de protección 1:1 con capacidad de transportar tráfico adicional cuando el sistema se encuentra en condiciones normales de servicio.

En ambos casos, el bloque "Adaptación" A corresponde a la "Adaptación de recorrido" (superior o inferior), mientras que la "Terminación de pista" equivale a la "Terminación de recorrido" (superior o inferior).

Las conexiones de red (de protección y con tráfico) constituyen las dos trayectorias por las que se envía la información dentro de la red sincrónica con la finalidad de proteger el contenedor virtual en servicio.

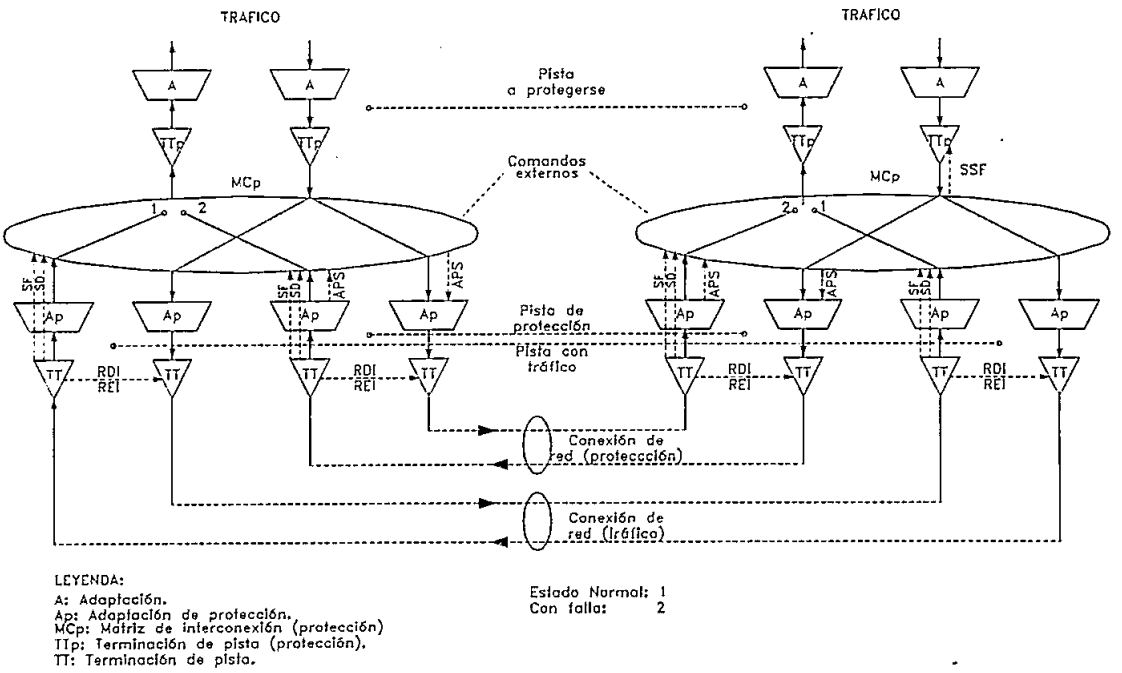


Fig. 3.15 a) Modelo funcional de un sistema de protección a nivel de VC para una configuración 1+1.

[10] ETSI, DTRM/TM -03025 Transmissión and Multiplex"TM' SDH Network Protection Schemes: Types and Characteristics, Sophia Antipolis Cedex-France, September, 1995.

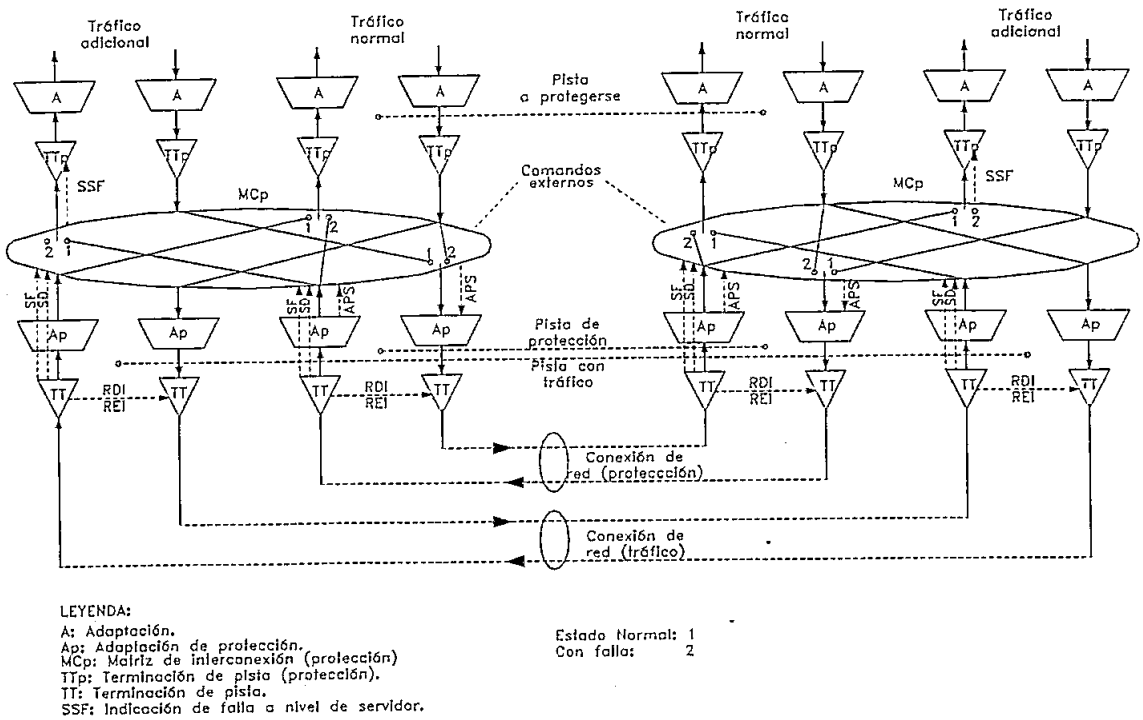


Fig. 3.15 b) Modelo funcional de un sistema de protección a nivel de VC con configuración 1:1 de tipo reversible y capacidad de tráfico adicional.

La matriz de conexión MC es configurada de acuerdo a los requerimientos del cliente a través del sistema de supervisión (TMN) y se encarga de la conmutación de los canales con falla o degradados cuyo procesamiento de información se realiza a través de los canales de la APS.

3.3.1.1 Protección por conmutación automática (APS)

La presencia de peticiones externas o la detección de una degradación de la señal (**SD**), falla (**SF**), etc., provocan el inicio de la conmutación automática del selector hacia el canal de protección disponible en el terminal de recepción. Las figuras 3.13 y 3.14 muestran solo el caso de conmutación a doble terminal, aunque los dos tipos de conmutación (a doble y simple terminal) pueden ser aplicadas independientemente del tipo de enrutamiento utilizado en la red. Es claro que si una rotura múltiple afecta simultáneamente a un canal con tráfico y a su protección en cualquier otro punto de la red, la interrupción de este canal será inevitable.

a) **Criterios de conmutación**

Para un sistema de protección en configuración 1+1 con conmutación a simple terminal, se presenta en la tabla 3.12, la lista de peticiones en orden de mayor prioridad de arriba hacia abajo.

Petición local	Prioridad
Anulación de órdenes, peticiones.	Máxima
Bloqueo de la protección LP.	
Conmutación forzada FS.	
Señal con falla SF.	
Señal degradada SD.	
Conmutación manual MS.	
En espera antes de restablecer WTR.	
Ninguna petición NR.	Mínima

Tabla 3.12 Peticiones locales con sus respectivas prioridades para un sistema 1+1 con conmutación unidireccional.

En este caso, la presencia de señal con falla en la protección (**SF-P**) no debería inhabilitar la conmutación forzada hacia la protección (**FS-P**), como sucede en los anillos de protección compartida (sección 3.2.2.3).

El inicio de la conmutación puede darse por peticiones externas a la red o producirse automáticamente. Dentro de las peticiones externas se incluyen las siguientes:

- Anulación de cualquier comando ya iniciado.
- Bloqueo de la protección (**LP**), la cual niega el acceso hacia el canal de protección.
- Conmutación forzada del tráfico desde la protección hacia el canal principal (**FS-P**).
- Conmutación forzada del tráfico desde el canal principal hacia la protección (**FS-W**). Se lleva a cabo independientemente de las condiciones (**SD**, **SF**) del canal de protección.
- Conmutación manual hacia la protección (**MS-P**).
- Conmutación manual desde el canal principal hacia el canal la protección (**MS-W**), se lleva a cabo solo si no existen las condiciones (**SD**, **SF**) del canal de protección.

Por otra parte, la conmutación puede iniciarse automáticamente cuando se ha detectado señal con falla (**SF**) o señal degradada (**SD**). Existen dos casos a considerarse:

1. Recorridos de orden superior (VC3-VC4)
   - La detección de señal con falla (**SF**) que inicia la protección automática, puede ser originada por las siguientes condiciones:
     i) Indicación "servidor del recorrido de orden superior con falla" (**HP-SSF**) la misma que es provocada por **AU-LOP** o **AU-AIS**.
     ii) Presencia de **HP-UNEQ**, **HP-TIM**, **HP-EXC**.
   - La detección de señal degradada se origina por **HP-DEG** (referirse al Anexo # 2, Terminación de recorrido de orden superior).

2. Recorridos de orden inferior (VC-3, VC-12, VC-11).
   - La detección de señal con falla (**SF**) que inicia la protección automática, puede ser originada por las siguientes condiciones:
     i) Indicación "servidor del recorrido de orden inferior con falla" (**LP-SSF**) la misma que es provocada por **TU-LOP** o **TU-AIS**.
     ii) Presencia de **LP-UNEQ**, **LP-TIM**, **LP-EXC**.
   - La detección de señal degradada se origina por **LP-DEG** (referirse al Anexo # 2, Terminación de recorrido de orden inferior).

b) Normas generales

1. En el caso de un sistema 1+1 con conmutación a simple terminal, el selector es controlado por la presencia de peticiones de acuerdo a la tabla de prioridades mostrada en la tabla 3.12. La presencia simultánea de peticiones de prioridad equivalente en ambos canales anula toda acción de conmutación debido a que la conmutación se basa en la verificación de la petición local de mayor prioridad solamente.
2. Un sistema 1+1 con conmutación a simple terminal puede trabajar en modo reversible con un tiempo de "espera antes de restablecer" (**WTR**) que puede ser definido desde 5 a 12 minutos luego de que el canal con tráfico ha recuperado un

nivel de calidad aceptable. Una indicación de "ninguna petición" (**NR**) será emitida al final del tiempo de espera.

3. El mismo sistema anterior pero en modo no reversible se limita a indicar una condición de " ninguna petición" (**NR**) cuando el canal con tráfico ha recuperado su nivel de calidad.
4. Un sistema 1+1 con conmutación a doble terminal, se hace uso del byte **K3** (bits 1 a 4) para VC de orden superior y **K4** (bits 1 a 4) para VC de orden inferior. Este protocolo se encuentra actualmente en vías de definición.

3.3.2 Protección a nivel de conexión de sub-red (*Sub-network connection SNC*)

Al igual que la protección a nivel de contenedor virtual, este tipo de protección puede aplicarse a todo tipo de red. Se utiliza generalmente para proteger una porción de recorrido o la totalidad de él. Este tipo de protección es normalmente utilizada en redes grandes manejadas por diferentes operadores, cuyas áreas de acción necesitan protegerse de tal manera que la información pueda fluir sin problemas cuando se trate de enviarla a través de las fronteras entre ellas.

De acuerdo al modo de activación de la conmutación puede dividirse en:

1. **Protección inherente**: Protege generalmente contra fallas en el servidor. La detección de la falla se realiza a nivel de servidor, el mismo que informa al cliente a través de una indicación SSF. La protección entonces se realiza a nivel de cliente.
2. **Protección *non-intrusive***: Protege contra fallas en el servidor y contra fallas y degradaciones en el cliente. Las condiciones de falla son detectadas por las funciones HPOM y LPOM (Ver Anexo # 2)

Los criterios de conmutación son idénticos a aquellos de la protección a nivel de contenedor virtual (sección 3.3.1) con la diferencia que la protección a nivel de conexión de sub-red no considera la POH como referencia de terminación en los extremos de la trayectoria. Es decir, la POH es transparente al proceso de protección.

Existen dos tipos de configuración 1+1 y 1:1 que emplean este tipo de protección, cuya filosofía de conmutación es similar a la protección a nivel de VC. La configuración 1:1 con capacidad de transporte adicional de tráfico se encuentra en fase

de estudio por parte del ITU-T. Ambos tipos de configuración utilizan conmutación a simple o doble terminal en sus extremos, y el tipo de enrutamiento puede ser también unidireccional y bidireccional.

El tiempo de conmutación recomendado es de 50 ms. Esto no incluye el tiempo necesario para la detección de la falla o degradación, ni tampoco la puesta en marcha de la protección. En lo que respecta a la estructura básica para la protección, el canal con tráfico es duplicado en el terminal de transmisión mientras que el selector escoge el canal que presenta una calidad aceptable (Ver las figuras 3.13 y 3.14).

El modelo funcional para este tipo de protecciones se muestra en la figura 3.16.

3.3.2.1 Protección por conmutación automática (APS)

a) Criterios de conmutación

La tabla de peticiones es la misma que para el caso de la protección a nivel de contenedor virtual de la sección 3.3.1 (Ver tabla 3.12). Igualmente sucede para los criterios de conmutación (Ver sección 3.3.1.1 a).

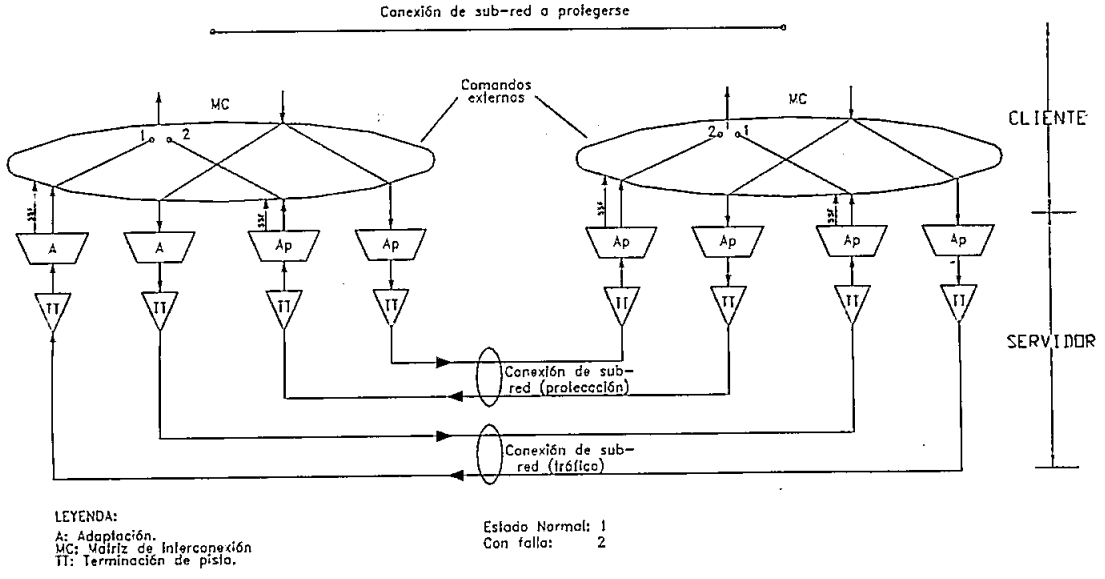


Fig. 3.16 a) Modelo funcional para la protección de una conexión de sub-red de tipo inherente.

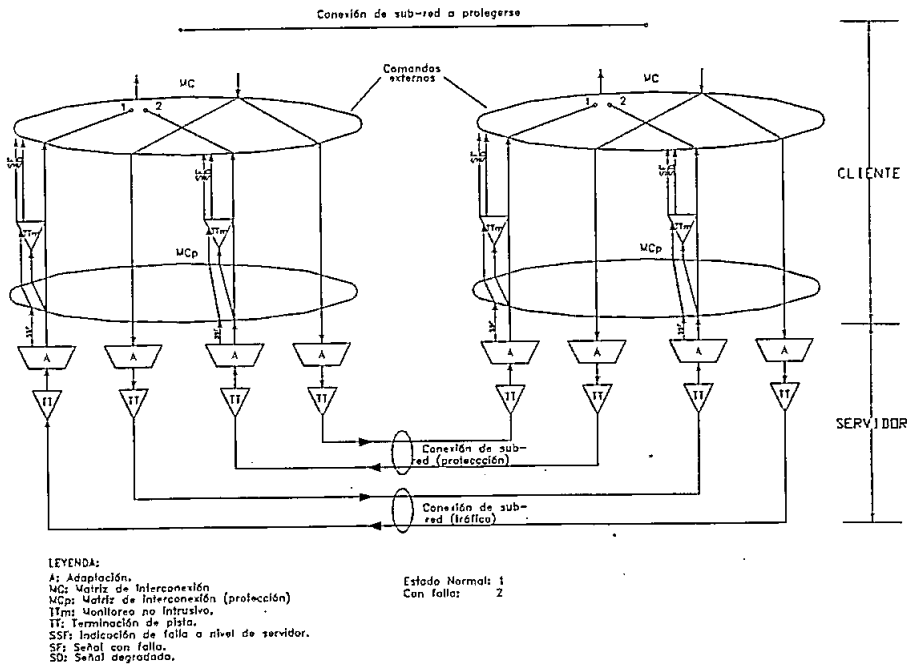


Fig. 3.16 b) Modelo funcional para la protección de una conexión de sub-red de tipo *non intrusive*.

b) Normas generales

1. En el caso de un sistema 1+1 con conmutación a simple terminal, el selector es controlado por la presencia de peticiones de acuerdo a la tabla de prioridades mostrada en la tabla 3.12. La presencia simultánea de peticiones de prioridad equivalente en ambos canales anula toda acción de conmutación debido a que la conmutación se basa en la verificación de la petición local de mayor prioridad solamente.
2. Un sistema 1+1 con conmutación a simple terminal puede trabajar en modo reversible con un tiempo de "espera antes de restablecer" (**WTR**) luego de que el canal con tráfico ha recuperado un nivel de calidad aceptable. Una indicación de "ninguna petición" (**NR**) será emitida al final del tiempo de espera.
3. El mismo sistema anterior pero en modo no reversible se limita a indicar una condición de " ninguna petición" (**NR**) cuando el canal con tráfico ha recuperado su nivel de calidad.

CAPITULO IV

Aplicación de los mecanismos de protección en redes digitales sincrónicas

APLICACION DE LOS MECANISMOS DE PROTECCION EN REDES DIGITALES SINCRONICAS

4.1 CONSIDERACIONES GENERALES

Actualmente, la mayoría de las redes de transporte de telecomunicaciones se caracterizan por su estructura rígida, compuesta básicamente por aparatos multiplexores estáticos (no reconfigurables), equipos de transmisión y bloques mecánicos de distribución de señales. Sin embargo, el crecimiento rápido de la demanda de voz, imagen, texto y datos exige ya la conversión a una red que permita:

- Continuo monitoreo de la señal a todo nivel.
- Rápida conmutación en caso de degradaciones o roturas.
- Elevada capacidad de tráfico.
- Re-enrutamiento adecuado de los canales de información.
- Compatibilidad con los sistemas plesiócronos existentes.

Estas características forman parte de los sistemas de transporte sincrónicos que están ganando presencia en todas las redes del mundo. A su gran capacidad de multiplexaje (de hasta n x 155 Mb/s, n=1, 4, 16, 64), se añade la ventaja de configurarse como anillos, los mismos que permiten una protección eficiente del tráfico en caso de fallas en nodos o enlaces.

4.1.1 Evolución de PDH a SDH

Consiste en la integración de las redes PDH existentes con el fin de crear una nueva red basada en la jerarquía digital sincrónica SDH. Existen varias estrategias, pero se destacan particularmente dos de ellas:

a) Islas SDH

Consiste en la creación de áreas SDH completamente funcionales en lo que respecta a manejo de tráfico, supervisión y control de red. Estas islas se conectan en

sus fronteras mediante interfaces SDH/PDH incluidos en los mismos aparatos SDH. Obviamente, en una red mixta SDH/PDH no todas las ventajas de la tecnología SDH están disponibles debido al desacoplamiento en las fronteras. Este tipo de islas podría ponerse en práctica en áreas de recolección de tráfico o distribución; su configuración adoptaría la forma de anillo o estrella (centro de concentración) con la suficiente flexibilidad como para expandirse paso a paso hasta conseguir la cobertura total de la red.

b) Redes SDH sobrepuestas

Es altamente recomendable cuando la mayor parte de la red existente utiliza fibra óptica como medio de transmisión. Consiste en la colocación de una nueva red (SDH) sobre la actual PDH ya sea a nivel nacional o regional. Esta nueva red puede considerarse como una protección de la actual, un interfaz SDH/PDH entre las dos redes o simplemente como una forma de incrementar la capacidad de la red en el futuro cuando la demanda de tráfico así lo requiera. Por ejemplo, una red a nivel de 140 o 565 Mb/s podría ser remplazada por una nueva con capacidad STM-4 o STM-16 utilizando terminales de línea ópticos que multiplexan 4x140 Mb/s o 16x140 Mb/s. El siguiente paso consiste en la introducción de aparatos de interconexión sincrónicos (DXC), los mismos que conducirían a la conversión total de la red.

4.1.2 Estructura de una red de transporte

Típicamente, una red de transporte se compone de red troncal, red regional y red de acceso (Ver figura 4.1).

La red troncal es la estructura encargada del transporte a nivel nacional y también internacional. Está formada por aparatos de conmutación (DXC) de alta capacidad en configuraciones lineales o de anillo.

La red regional se encarga del transporte de tráfico a nivel urbano. Generalmente está formada por aparatos de conmutación DXC que permiten un enrutamiento flexible, así como el agrupamiento de contenedores virtuales de bajo nivel.

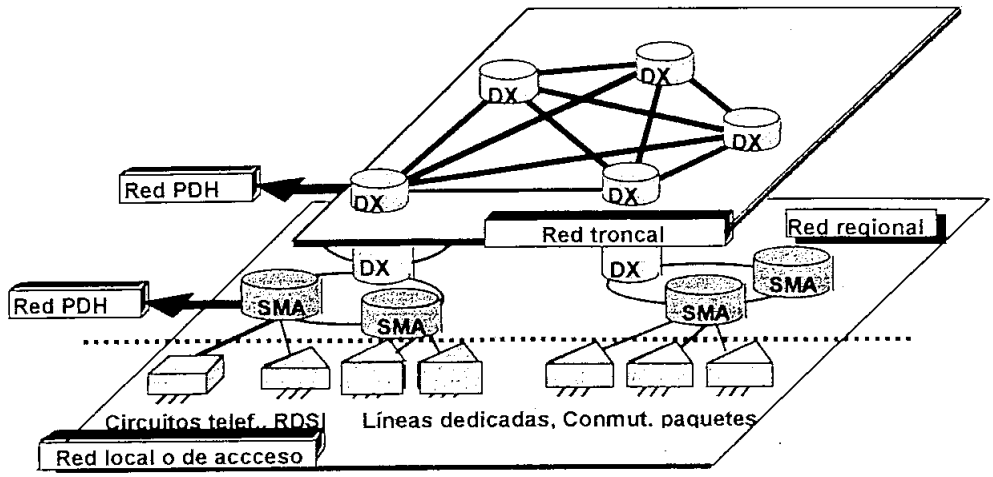


Fig. 4.1 Típica estructura de una red de transporte SDH.

La red local o de acceso transporta el tráfico de baja capacidad en pequeñas áreas geográficas. Puede configurarse incluso como anillos para dar protección y enrutamiento flexible del tráfico local.

4.2. CONSIDERACIONES GENERALES SOBRE RE-ENRUTAMIENTO

4.2.1 Introducción

El enrutamiento o re-enrutamiento de ciertos canales dentro de una red da como resultado una mejor distribución del tráfico en los enlaces. Sin embargo, también se podría provocar una congestión de tráfico si los algoritmos determinan que varios canales deben ser desviados hacia un mismo enlace. Como regla general un enlace tiene una carga normal de tráfico cuando ella no supera el 80% de la máxima capacidad del enlace.

Es oportuno hacer referencia a una red de computadoras que basa su estructura de interconexión mediante datagramas (mensajes) o circuitos. La interconexión mediante circuitos entre dos nodos cualquiera se realiza al inicio de la comunicación y se mantiene durante todo el tiempo que dura el proceso de intercambio de información entre los dos nodos. El recorrido en sí es lo que se conoce con el nombre de "Circuito Virtual", debido a su semejanza a un circuito de una red telefónica. Obviamente, el establecimiento de este recorrido es el resultado de un previo análisis que considera

muchas posibilidades y criterios que permiten decidir el camino a seguir para ir de un nodo a otro en la red. Todo este proceso está enmarcado dentro de los algoritmos de enrutamiento.

Los algoritmos de enrutamiento se clasifican en dos grandes grupos de acuerdo al lugar donde se toman las decisiones:

1. **Distribuidos:** Cada nodo decide las vías de enrutamiento.
2. **Centralizados:** Un nodo principal controla todo el proceso de enrutamiento en la red.

Criterio de enrutamiento

Un algoritmo puede decidir las trayectorias de enrutamiento de acuerdo a los siguientes criterios:

a) Número de enlaces
b) Costo
c) Retardo
d) Carga - Intensidad de tráfico en un nodo.

El criterio de enrutamiento por minimización de costo es uno de los más utilizados pues puede asociarse de varias maneras como se detalla a continuación:

1. Costo por cada enlace implica reducir el número de enlaces para ir de un nodo a otro.
2. Costo por cada enlace asociado al retardo implica reducir el retardo en la trayectoria a seguirse.
3. Si el costo es asociado a la longitud de un enlace, la distancia total entre dos nodos será minimizada.
4. Si el costo está asociado al costo real de operación del sistema, el costo de utilización del sistema de comunicación será optimizado.
5. Costo asociado a la confiabilidad del sistema. Para ir de un nodo ***a*** al nodo ***z*** la confiabilidad a ser maximizada será del tipo[1]:

[1] John D. Spragins, Telecommunications Protocols and Design, pp.362, Addison Wesley, New York, 1994.

$$R(a,z) = p_{ab} \cdot p_{bc} \cdots\cdots p_{mn} \cdot p_{nz}, \qquad (4.1)$$

donde P_{ij} es la probabilidad de que el enlace sea operacional. Se considera que la rotura de un enlace es independiente de cualquier otro enlace en la red.

Los algoritmos que usan el costo como criterio, son llamados "Algoritmos de mínima trayectoria". Este es el tipo de algoritmo que será considerado en este trabajo. El costo por enlace es indicado sobre cada enlace como en el ejemplo de red mostrado

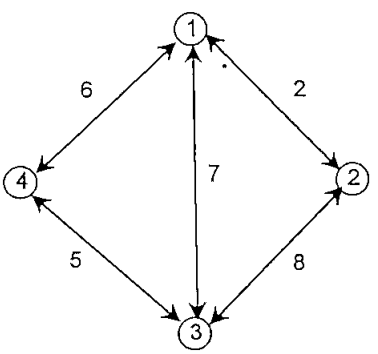


Fig. 4.2 Ejemplo de red.

en la figura 4.2. El costo es el mismo para las dos direcciones de transmisión de cada enlace (bidireccional).

4.2.2 Algoritmo de *Floyd-Warshall*

Este algoritmo tiene como objetivo calcular la distancia más corta entre todos los pares de nodos de la red. Inicialmente se asigna la distancia (longitud) entre cada par de nodos conectados directamente, en caso contrario (nodos no adyacentes), se debe asignar una longitud "infinita".

Para encontrar la trayectoria y distancia más corta entre dos nodos, el algoritmo toma como pivote un nodo intermedio entre los dos nodos considerados. La primera vez se toma el primer nodo como pivote y se realiza el barrido de todos los enlaces de la red. Se continúa con el segundo nodo como intermedio, se barren nuevamente los enlaces y así sucesivamente. Si el **k**-ésimo nodo es el intermedio, y se está analizando el enlace del nodo **i** al nodo **j**, se entiende como "barrer" el hecho de *verificar cuál* de las dos distancias -de **i** a **j** pasando por **k** o directamente de **i** a **j**- es la menor.

Inicialmente, a cada distancia entre dos nodos **i**, **j** se le asigna costo. En este caso, el costo está asociado a la distancia entre los dos nodos y por lo tanto a la longitud de los enlaces involucrados en aquella trayectoria[2]:

$$D_{ij}^{(0)} = c_{ij}, \forall\, i, j \quad i \neq j \qquad (4.2)$$

donde:

D_{ij} = trayectoria más corta entre los nodos **i** y **j**.

c_{ij} = costo inicial asociado a la longitud de la trayectoria entre dos nodos **i** y **j**.

Siendo N el número total de nodos de la red, los barridos se realizan para todo valor de k (k=0,1,2,....N-1), obteniéndose la mínima distancia entre ellos, de la siguiente manera:

$$D_{ij}^{(k+1)} = \text{mín}\,[D_{ij}^{(k)},\ D_{i(k+1)}^{(k)} + D_{(k+1)j}^{(k)}] \qquad (4.3)$$

siempre que **i** sea distinto de **j**.

Nótese que la mínima distancia se obtiene de la comparación entre la distancia directa (D_{ij}) entre los dos nodos y la trayectoria indirecta compuesta de dos partes: distancia del nodo de origen hasta el nodo pivote ($D_{i(k+1)}$), más la distancia del nodo pivote hasta el nodo de destino ($D_{(k+1)j}$).

El algoritmo da como resultado una matriz de distancias D entre todos los nodos de la red y una matriz de trayectorias P. De esta última se obtiene el recorrido a seguir dentro de la red para alcanzar la distancia más corta entre dos nodos. Por ejemplo, para la red de la figura 4.3, la condición inicial es:

Matriz inicial de distancias [Do]:

		Hasta					
		1	**2**	**3**	**4**	**5**	**6**
Desde	**1**	0	2	5	5	INF	INF
	2	2	0	3	2	INF	INF
	3	5	3	0	7	4	6
	4	5	2	7	0	2	INF
	5	INF	INF	4	2	0	1
	6	INF	INF	6	INF	1	0

Matriz inicial de trayectorias [Po]:

		Hasta					
		1	**2**	**3**	**4**	**5**	**6**
Desde	**1**	1	1	1	1	1	1
	2	2	2	2	2	2	2
	3	3	3	3	3	3	3
	4	4	4	4	4	4	4
	5	5	5	5	5	5	5
	6	6	6	6	6	6	6

[2] John D. Spragins, Telecommunications Protocols and Design, pp.374-376, Addison Wesley, New York, 1994.

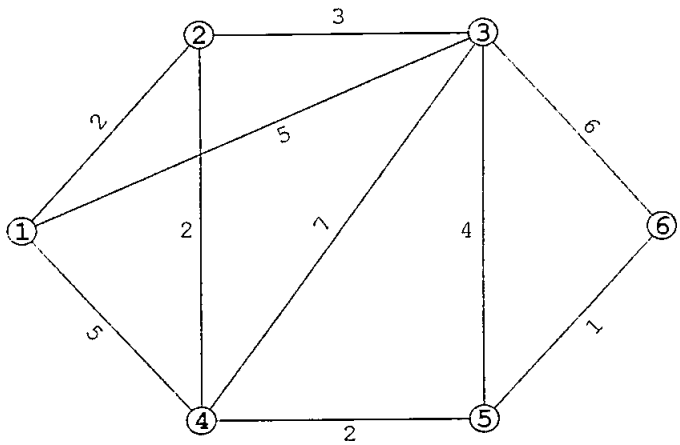


Fig. 4.3 Ejemplo de red para el Algoritmo de *Floyd-Warshall*.

Una vez aplicado el algoritmo, el resultado es:

Matriz final de distancias [Df]:

		H	a	s	t	a	
		1	**2**	**3**	**4**	**5**	**6**
D	**1**	0	2	5	4	6	7
e	**2**	2	0	3	2	4	5
s	**3**	5	3	0	5	4	5
d	**4**	4	2	5	0	2	3
e	**5**	6	4	4	2	0	1
	6	7	5	5	3	1	0

Matriz final de trayectorias [Pf]:

		H	a	s	t	a	
		1	**2**	**3**	**4**	**5**	**6**
D	**1**	0	1	1	2	4	5
e	**2**	2	0	2	2	4	5
s	**3**	3	3	0	2	3	5
d	**4**	2	4	2	0	4	5
e	**5**	2	4	5	5	0	5
	6	2	4	5	5	6	0

La matriz [Df] muestra la distancia total entre todos los nodos de la red. Esta distancia es la suma de todas las distancias parciales de cada enlace encontrado en el recorrido de un nodo a otro. La matriz [Pf] da el recorrido más corto a seguir para ir de un nodo a otro.

Por ejemplo, para encontrar la ruta más corta entre el nodo **1** y el nodo **6**, se parte desde el nodo final. El elemento de la matriz P[**1**,**6**] contiene el número **5**; el paso siguiente es ir al elemento P[**1**,**5**] cuyo contenido es **4**. P[**1**,**4**] contiene el número **2** y finalmente P[**1**,**2**] contiene el nodo número **1**, que indica el final del recorrido. En conclusión, para ir del nodo **1** al **6** el recorrido es: **1**, **2**, **4**, **5**, **6**. Obviamente, el recorrido entre **6** y **1** es el mismo puesto que todos los enlaces presentan flujos iguales en ambas direcciones. De hecho, la matriz [Df] es simétrica.

4.3 EJEMPLO DE APLICACION

4.3.1 Objetivos generales en el diseño de una red de transporte SDH

A continuación se describen brevemente los objetivos que se deben considerar para el diseño y puesta en marcha de una red de transporte de telecomunicaciones.

Costo: Incluye los costos de equipamiento más los costos de operación y mantenimiento de la red.

Capacidad: Es la cantidad de tráfico que puede soportar la red.

Confiabilidad: Está asociada al tiempo que la red se mantiene en operación sin sufrir ninguna interrupción o degradación del servicio.

Compatibilidad: Entre todos los componentes de la red, los cuales deben soportar diferentes tipos de tráfico, por ejemplo telefonía, datos, etc.

4.3.2 Funciones de la red de transporte SDH

Los objetivos antes mencionados se logran con la inclusión de ciertas características funcionales de la red, por ejemplo:

Conmutación: Es la facilidad de interconexión entre los canales de entrada a un nodo y los de salida del mismo.

Enrutamiento y re-enrutamiento: Consiste en la búsqueda de la trayectoria óptima para enviar la información entre dos nodos cualquiera dentro de la red.

Control del flujo: Administración del tráfico en los enlaces de la red, de tal manera que todos ellos tengan una carga aceptable de acuerdo a su capacidad.

Supervisión y manejo de la red: Es el sistema responsable de la detección de fallas y degradaciones en la red, de modo que la confiabilidad sea la máxima posible. Se encarga además de la seguridad, contabilidad y la interacción con otras redes. En el ámbito actual este sistema se conoce como TMN (*Telecommunications Management Network*).

4.3.3 Planificación general de una red de transporte SDH

El diseño y planificación general de una red de transporte puede resumirse en los siguientes pasos:

1. Elaboración de la **matriz de tráfico** de acuerdo a las necesidades actuales del cliente y su proyección a futuro.
2. Determinación de la **arquitectura** de la red (anillos, mallas, en estrella, etc.).
3. **Enrutamiento** y cálculo de la **capacidad** necesaria de la red, tanto para tráfico principal como para la protección.
4. Identificación de las estrategias de **protección** a utilizarse.
5. **Agrupamiento** de los canales de información de acuerdo a su trayectoria y eventualmente al tipo de información en ellos contenida.
6. Definición del tipo de **equipamiento** a utilizarse en la red.
7. Evaluación de la **disponibilidad** de la red.

El objetivo principal de este trabajo radica en el estudio del punto 4 de la lista antes mencionada, pero también se consideran brevemente los otros numerales para brindar una mejor concepción del proceso.

Se asume entonces que el(los) operador(es) de telecomunicaciones tiene(n) definido lo siguiente:

- La matriz actual de tráfico entre todos los nodos de la red y su proyección hacia el futuro.
- La prioridad (si existe) de los canales de tráfico.

4.3.4 Desarrollo del ejemplo de aplicación

4.3.4.1 Matriz de tráfico

Existen varios métodos para proyectar la matriz a futuro, pero entre los más utilizados se encuentran los siguientes[3]:

- Método de *Kruithof.*
- Método de los coeficientes de afinidad.
- Método gravitacional.

---

[3] VIDAL Arnoldo, Diseño de un sistema de fibra óptica de alta capacidad a 565 Mb/s entre las ciudades de Quito y Guayaquil, Tesis EPN, Quito, Abril, 1993.

A continuación se presenta la matriz de tráfico de un operador de telecomunicaciones[4] con previsiones para el año 2000 y 2005. Las unidades se expresan en número de canales a 2 Mb/s.

NODO	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1		54	38	0	21	41	10	15	4	4	0	4	4	2
2	54		57	0	18	12	13	27	0	4	8	4	4	2
3	38	57		11	19	9	13	27	7	4	6	4	5	0
4	0	0	11		22	0	0	0	0	0	0	0	0	2
5	21	18	19	22		10	7	12	8	4	8	8	4	3
6	41	12	9	0	10		5	2	2	8	4	9	0	2
7	10	13	13	0	7	5		15	10	4	2	0	0	3
8	15	27	27	0	12	2	15		4	2	2	0	4	4
9	4	0	7	0	8	2	10	4		32	8	14	4	4
10	4	4	4	0	4	8	4	2	32		4	7	2	9
11	0	8	6	0	8	4	2	2	8	4		12	2	4
12	4	4	4	0	8	9	0	0	14	7	12		3	7
13	4	4	5	0	4	0	0	4	4	2	2	3		2
14	2	2	0	2	3	2	3	4	4	9	4	7	2	
TOTAL/ NODO	197	203	200	35	144	104	82	114	97	84	60	72	34	44

Tabla 4.1 Matriz de tráfico para el año 2000.

NODO	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1		94	96	0	43	93	48	40	15	18	0	12	20	12
2	94		152	0	68	24	64	56	0	15	32	17	15	8
3	96	152		48	60	20	64	56	15	21	25	12	20	0
4	0	0	48		68	0	0	0	0	0	0	0	0	5
5	43	68	60	68		80	28	22	21	21	21	25	25	12
6	93	24	20	0	80		10	8	4	20	32	18	0	10
7	48	64	64	0	28	10		82	25	26	9	0	0	9
8	40	56	56	0	22	8	82		10	7	5	0	21	12
9	15	0	15	0	21	4	25	10		112	25	58	12	25
10	18	15	21	0	21	20	26	7	112		20	23	5	48
11	0	32	25	0	21	32	9	5	25	20		63	5	28
12	12	17	12	0	25	18	0	0	58	23	63		5	35
13	20	15	20	0	25	0	0	21	12	5	5	5		10
14	12	8	0	5	12	10	9	12	25	48	28	35	10	
TOTAL/ NODO	491	545	589	121	494	319	365	319	322	336	265	268	138	214

Tabla 4.2 Matriz de tráfico para el año 2005.

[4] Cellular Communications Networks, SDH Transportation Trunk, Kuala Lumpur, 1997.

4.3.4.2 Arquitectura

La infraestructura existente en lo que respecta a ductos y fibras ópticas, así como también la disponibilidad de las estaciones de comunicaciones es un factor importante a considerarse para la configuración de la red.

Existen muchas y muy conocidas configuraciones para definir la topología de una red como la de anillos, en estrella, en malla, o siguiendo una configuración jerárquica de la red. En el presente caso, la existencia de los ductos entre las estaciones y la alta demanda -y por tanto la importancia- de tráfico entre ellas, fueron determinantes para que la red sea configurada en forma de dos anillos principales como se puede ver en la figura 4.4.

Jerárquicamente, los anillos 1 y 2, así como su enlace de interconexión **2-9** pertenecerán a la red troncal; el área de los nodos **7** y **8**, así como los enlaces adicionales que convergen -actualmente y a futuro- hacia los anillos, se considerarán parte de la red regional.

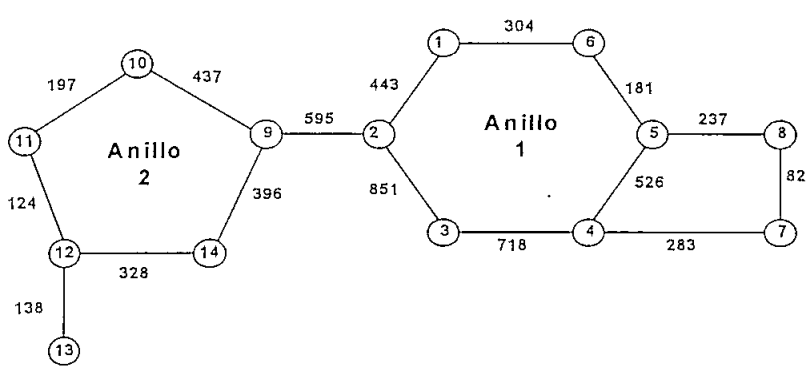


Fig. 4.4 Topología de la red y demanda inicial de tráfico entre nodos.

4.3.4.3 Enrutamiento de tráfico

Los valores de demanda de tráfico de la figura 4.4 se obtuvieron con la ejecución

del programa "RUTAS.EXE" [5], elaborado en lenguaje C. De esta manera se obtiene una mejor idea de la carga total de tráfico en la red. Para la ejecución del programa, se tomó como datos de entrada las conexiones entre nodos mostradas en la siguiente matriz:

		HASTA													
	NODO	1	2	3	4	5	6	7	8	9	10	11	12	13	14
DESDE	1		1	INF	INF	INF	1	INF	INF	INF	INF	INF	INF	INF	INF
	2			1	INF	INF	INF	INF	INF	1	INF	INF	INF	INF	INF
	3				1	INF	INF	INF	INF	INF	INF	INF	INF	INF	INF
	4					1	INF	1	INF	INF	INF	INF	INF	INF	INF
	5						1	INF	1	INF	INF	INF	INF	INF	INF
	6							INF	INF	INF	INF	INF	INF	INF	INF
	7								1	INF	INF	INF	INF	INF	INF
	8									INF	INF	INF	INF	INF	INF
	9										1	INF	INF	INF	1
	10											1	INF	INF	INF
	11												1	INF	INF
	12													1	1
	13														INF
	14														

Tabla 4.3 Matriz de conexiones entre nodos.

En la tabla anterior, "**1**" significa que existe conexión directa entre los nodos (es decir, son adyacentes), mientras que "**INF**" indica que los nodos no son adyacentes. Referirse a la figura 4.4 para una mejor ilustración de su proceso de elaboración.

		HASTA													
	NODO	1	2	3	4	5	6	7	8	9	10	11	12	13	14
DESDE	1	0	1	2	3	6	1	4	5	2	9	10	14	12	9
	2	2	0	2	3	4	1	4	5	2	9	10	14	12	9
	3	2	3	0	3	4	1	4	5	2	9	10	14	12	9
	4	2	3	4	0	4	5	4	5	2	9	10	14	12	9
	5	6	3	4	5	0	5	4	5	2	9	10	14	12	9
	6	6	1	2	5	6	0	4	5	2	9	10	14	12	9
	7	2	3	4	7	4	5	0	7	2	9	10	14	12	9
	8	6	3	4	5	8	5	8	0	2	9	10	14	12	9
	9	2	9	2	3	4	1	4	5	0	9	10	14	12	9
	10	2	9	2	3	4	1	4	5	10	0	10	11	12	9
	11	2	9	2	3	4	1	4	5	10	11	0	11	12	12
	12	2	9	2	3	4	1	4	5	14	11	12	0	12	12
	13	2	9	2	3	4	1	4	5	14	11	12	13	0	12
	14	2	9	2	3	4	1	4	5	14	9	12	14	12	0

Tabla 4.4 Matriz de trayectorias.

[5] El programa ejecutable RUTAS.EXE fue elaborado en base a la teoría del algoritmo de *Floyd-Warshall*, el cual fue descrito en la sección 4.2.2. El Anexo # 3 contiene más detalles sobre su utilización y estructura.

Luego de la ejecución del programa antes mencionado, se obtienen los resultados de la tabla 4.4, que muestra las rutas más cortas para ir de un nodo a otro en la red. En la sección 4.2.2 se presentó un ejemplo de cómo interpretar estos resultados. Sin embargo, considérese que se desea saber la ruta más corta entre los nodos **8** y **13**, en este caso se debe proceder de la siguiente manera:

1. Ubicar el elemento (8,13) de la matriz. Su contenido es **12**.
2. Manteniendo siempre la fila 8, identificar el elemento (8,12), cuyo contenido es **14**.
3. El siguiente elemento es (8,14). Su contenido es **9**.
4. Ubicar el elemento (8,9). Su contenido es **2**.
5. El siguiente elemento es (8,2). Su contenido es **3**.
6. El elemento (8,3) contiene el número **4**.
7. El elemento (8,4) contiene el número **5**.
8. Finalmente, el elemento (8,5) contiene el número **8**.
9. Por lo tanto, la ruta más corta para ir del nodo **8** al nodo **13** es: **8**, **5**, **4**, **3**, **2**, **9**, **14**, **12**, y **13**.

Nótese el desbalance de tráfico en los anillos de la figura 4.4; esto se debe principalmente a que el programa busca la ruta más corta entre dos nodos y, si la distancia entre dos nodos a través de dos rutas diferentes es igual, se mantiene siempre la primera ruta. El programa sirve inicialmente para dar la configuración inicial de tráfico (con el mínimo número de enlaces y nodos); sin embargo, será necesario balancear manualmente el tráfico para mejorar la distribución actual de carga y tener capacidad adicional de reserva para protección y probables expansiones de la red en el futuro.

a) Anillo 1

El balance manual de tráfico (sin cambiar el número de enlaces y nodos originalmente obtenidos) y su configuración final se muestra en la figura 4.5. Este reajuste de tráfico se detalla a continuación:

Flujo entre nodos	Tráfico (canales a 2 Mb/s)	Ruta original	Nueva ruta
5 → 2	68	5,4,3,2	5,6,1,2
5 → anillo 2	63	5,4,3,2	5,6,1,2
7 → 1	48	7,4,3,2,1	7,4,5,6,1
8 → 2	56	8,5,4,3,2	8,5,6,1,2
8 → anillo 2	55	8,5,4,3,2	8,5,6,1,2

Tabla 4.5 Balance manual del tráfico en el anillo 1.

Considerando que el tráfico entre los nodos **5** y **2** puede tomar dos rutas alternativas iguales, todo el tráfico entre el nodo **5** y cualquiera de los nodos del anillo **2** puede ser transferido como se indica en la tabla 4.5. El tráfico transferido es 63x2 Mb/s.

Adicionalmente, basándose en la configuración de la red, es posible mover todo el tráfico desde **8** hacia cualquier nodo del anillo **2** (pasando por **5**,**4**,**3**,**2**) y enrutarlo por los nodos **5**,**6**,**1**,**2**. Esta acción tampoco modifica el número de enlaces o nodos. El total de tráfico transferido es 55x2 Mb/s.

Con el mismo criterio, el tráfico entre los nodos **7** y **1** puede también ser transferido. Un total de 48x2 Mb/s es considerado en este caso.

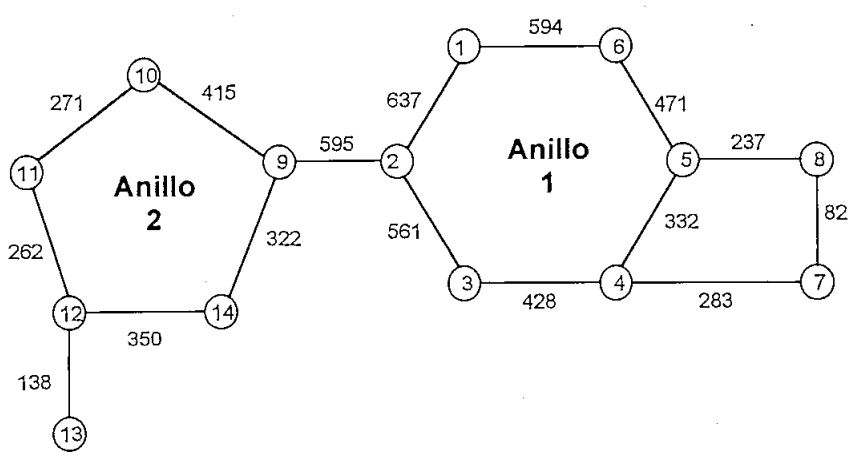


Fig. 4.5 Demanda de tráfico luego del balance manual en los anillos 1 y 2.

b) Anillo 2

La figura 4.5 muestra también la configuración final de tráfico para el anillo 2. En este caso, el tratar de balancear manualmente el anillo violaría el principio de tener la distancia más corta entre dos nodos cualquiera de la red. Sin embargo, las perspectivas a futuro involucrarán seguramente el incremento de tráfico hacia y desde los nodos **9**, **10**, **11**, **12**, **13** y **14**, por lo que el balance de tráfico será necesario aún si en este caso se sacrifica el principio de mínima distancia entre nodos. Obviamente, es más apropiado balancear el tráfico en fase de planificación que hacerlo en el futuro cuando la red se encuentre en servicio y se corra el riesgo de tener interrupciones de tráfico. Además, dicho balance permite aliviar la carga de tráfico en todos los enlaces del anillo de modo que ninguno de ellos trabaje con niveles de carga demasiado cercanos al máximo de la capacidad ofrecida. Los canales de tráfico involucrados en el balance de este anillo se detallan a continuación:

Flujo entre nodos	Tráfico (canales a 2 Mb/s)	Ruta original	Nueva ruta
2 → 11	32	2,9,10,11	2,9,14,12,11
9 → 12	58	9,14,12	9,10,11,12
10 → 14	48	10,9,14	10,11,12,14

Tabla 4.6 Balance manual de tráfico en el anillo 2.

4.3.4.4 Capacidad de la red

a) Anillo 1

La capacidad necesaria para manejar el tráfico en este anillo se puede calcular fácilmente de las fórmulas de la tabla 2.1. A continuación se muestran los cálculos necesarios considerando el tipo de tráfico tanto adyacente como uniforme:

Parámetros considerados

Número de nodos: 6

Capacidad (canales a 2 Mb/s o VC-12): C = 4x63 (caso STM-4)

C = 16x63 (caso STM-16)

Fórmulas

Tipo de anillo	Tráfico uniforme	Tráfico adyacente
Unidireccional	$d = 2*C/[n*(n-1)]$	$d = C/n$
Bidireccional	$d = 4*(C-n/2)/n^2$	$d = C/2$

Tipo De Anillo	Máxima demanda de tráfico permitida entre nodos (d)			
	Tráfico uniforme		Tráfico adyacente	
	STM-4	STM-16	STM-4	STM-16
Unidireccional	16	67	42	168
Bidireccional	27	111	126	504

Tabla 4.7 Cálculo de la máxima demanda en el anillo 1.

La tabla 4.7 muestra que los anillos bidireccionales son mucho más eficientes que los anillos unidireccionales desde el punto de vista de la demanda de tráfico permitida. Si se consideran los valores de la figura 4.5, el anillo con capacidad STM-4 no es suficiente para satisfacer aquellas demandas de tráfico.

Observando los valores de demanda de tráfico de la figura 4.5, existen demandas de tráfico entre nodos adyacentes del orden de 600x2 Mb/s; es decir, un anillo con capacidad STM-16, cuya máxima demanda entre nodos adyacentes es de 504x2 Mb/s, no es capaz de soportar tal cantidad de tráfico, por lo que en este caso no es aplicable. Una alternativa es utilizar anillos con capacidad STM-64. Sin embargo, la aplicación de este tipo de anillo está sujeta a dos consideraciones: la disponibilidad de los equipos de línea -que por ahora se encuentran en proceso de desarrollo- y el costo de inversión; este último implicaría tener un sistema cuya capacidad no sería completamente utilizada como se puede observar de las proyecciones de demanda de tráfico presentadas anteriormente.

En estas condiciones, es necesario tener otra alternativa que permita optimizar la capacidad a utilizarse, así como la disponibilidad de capacidad adicional para la aplicación de sistemas de protección y probables expansiones o reconfiguraciones de la red en el futuro. En este trabajo se propone la utilización de dos anillos a dos fibras con capacidad STM-16, sobrepuestos e independientes en lo que respecta a los

mecanismos de protección de cada uno de ellos. Esta solución se asemeja a un anillo a cuatro fibras como aquel presentado en la sección 3.2.2.2, pero que presenta mejores características como se detalla a continuación:

1. Mayores facilidades de interconexión con otros anillos de la red.
2. Mejor granularidad (mínima unidad de transporte de tráfico, por ejemplo VC-12, VC-11, etc., que puede ser manejada por el anillo).
3. Mayor flexibilidad en lo que respecta a la utilización de la capacidad de tráfico, lo que brinda más alternativas de enrutamiento en caso de congestión de tráfico.
4. Optimización de costos a mediano y largo plazo en razón de permitir un adecuado dimensionamiento de la red y su expansión a futuro.

Este doble anillo a 2 fibras tiene la misma capacidad de tráfico de un anillo a 4 fibras. Aunque con esta solución no se alcanza el elevado nivel de confiabilidad de un anillo a 4 fibras, se mantiene al menos aquel de un anillo a dos fibras. Además, ayuda a incrementar la confiabilidad total de la red debido a la diversificación de trayectorias que permite ejecutar. La figura 4.6 muestra la configuración de este doble anillo a dos fibras con su respectiva capacidad.

La idea de tener anillos sobrepuestos implica en la mayoría de casos una gran reducción de los costos de inversión del sistema, debido principalmente a la disminución de equipos terminales, interfaces ópticos y longitud de los medios de transmisión (fibra óptica).

En la figura 4.6, el anillo 1 se subdivide en dos anillos 1A y 1B, de acuerdo a la carga de tráfico a la que son sometidos. Originalmente, el anillo 1A transportaría solamente el tráfico interno entre nodos del anillo 1, mientras que el anillo 1B transportará el tráfico en tránsito hacia otros anillos y nodos externos al anillo 1. El objetivo es tener uno de los anillos trabajando con una carga relativamente grande, a la vez que el otro anillo lo haga con una carga ligera que permita expansiones a futuro sin tener que involucrar el tráfico existente en el otro anillo, es decir, logrando una independencia entre ellos.

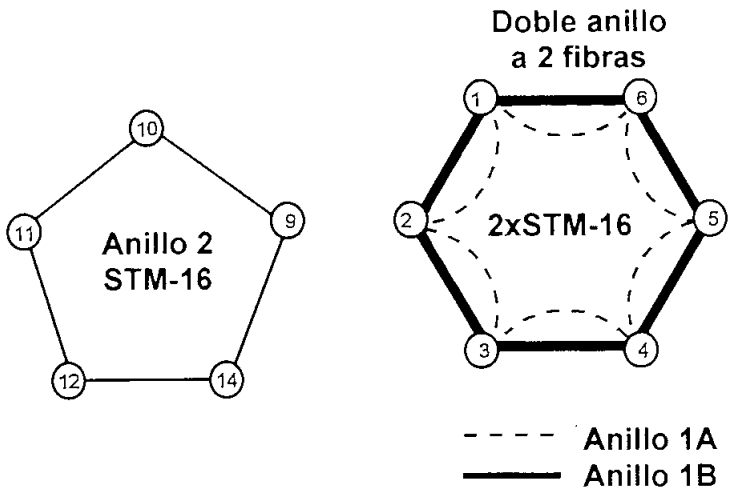


Fig. 4.6 Capacidad de los nuevos anillos.

Para definir la partición de tráfico entre los anillos 1A y 1B, se procede en primer lugar con la evaluación de la demanda interna de tráfico del anillo 1 solamente. Considérese la matriz de tráfico de la tabla 4.2, donde se observa que la demanda entre los nodos **1** a **6** es bastante uniforme, a excepción del nodo **4** que presenta solo dos canales de tráfico con los nodos **3** y **5**. Se podría pensar en excluir este nodo **4** con el fin de disminuir los costos de equipamiento y los interfaces ópticos en el anillo 1A; sin embargo, se verá más adelante que esto no es posible debido a los requerimientos adicionales de capacidad para protección en el área de los nodos **7** y **8**, los mismos que influyen en la demanda del enlace **4-5**.

A través de la ejecución del programa "RUTAS.EXE" se obtienen los valores de demanda de tráfico para cada enlace en el anillo 1A como se muestra en la figura 4.7.

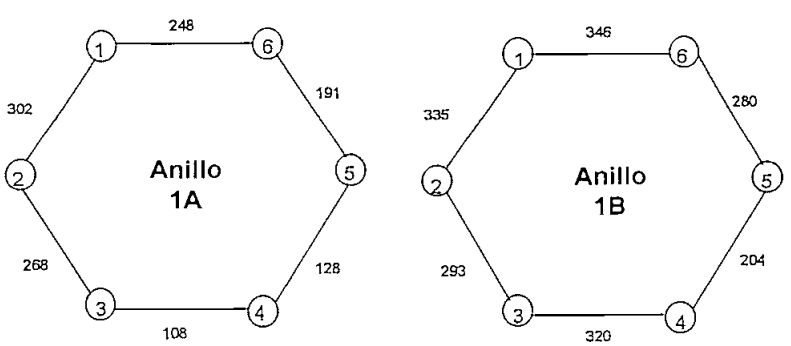


Fig. 4.7 Demanda de tráfico en los anillos 1A y 1B.

El único canal transferido para balancear el anillo es entre los nodos 2 y 5 (Ver tabla 4.5).

Para el anillo 1B, la distribución de la demanda de tráfico se obtiene mediante la diferencia entre la demanda en los enlaces de la figura 4.5 y los valores obtenidos anteriormente para el anillo 1A. La demanda final de tráfico en el anillo 1B en cada enlace, es generalmente mayor que la correspondiente al anillo 1A como se ve en la figura 4.7.

b) Anillo 2

Un cálculo similar a aquel realizado para el anillo 1 arroja los siguientes resultados:

Parámetros considerados

Número de nodos: 5

Capacidad (canales a 2 Mb/s o VC-12): C =.4x63 (caso STM-4)

C = 16x63 (caso STM-16)

Fórmulas

Tipo de anillo	**Tráfico uniforme**	**Tráfico adyacente**
Unidireccional	$d = 2*C/[n*(n-1)]$	$d = C/n$
Bidireccional	$d = 4*C/(n^2-1)$	$d = C/2$

Tipo De Anillo	**Máxima demanda de tráfico permitida entre nodos (d)**			
	Tráfico uniforme		**Tráfico adyacente**	
	STM-4	**STM-16**	**STM-4**	**STM-16**
Unidireccional	25	100	50	201
Bidireccional	42	168	126	504

Tabla 4.8 Cálculo de la máxima demanda en el anillo 2.

El resultado anterior conduce fácilmente a la utilización de un anillo con capacidad STM-16 para el anillo número 2, pues el máximo tráfico permitido para este

tipo de anillo (504x2 Mb/s) es mayor que la máxima demanda de tráfico requerida en el anillo 2 (415x2 Mb/s) de la figura 4.5.

c) Enlace 2 – 9

La capacidad necesaria se calcula de esta manera:

C = demanda tráfico/63 = 595/63 = 9.4 x STM-1,

por lo tanto, para transportar el tráfico principal se requiere al menos un sistema con capacidad STM-16.

d) Area de acceso (nodos 7 y 8)

La capacidad necesaria será determinada posteriormente, en virtud del tipo de mecanismos de protección a aplicarse en aquella parte de la red (referirse a la sección 4.3.4.5 c, sub-red 4).

e) Enlace 12 – 13

Se requiere de un enlace con capacidad suficiente para transportar los 138x2 Mb/s de tráfico.

C = 138/63 = 2.2xSTM-1,

es decir, la capacidad requerida es STM-4.

4.3.4.5 Mecanismos de protección

a) Combinación de mecanismos

Como se vio anteriormente en la sección 3.3, una red de transporte se descompone en varias capas, ("Estratificación") asociadas entre sí por una relación cliente/servidor. Además, cada uno de estos niveles se subdivide en sub-redes

("Partición") con fronteras claramente definidas entre ellas. Pues bien, el objetivo de esto es simplemente aislar el efecto de una falla ocurrida dentro de una sub-red perteneciente a cierta capa de modo que sea "internamente" controlada y no afecte el comportamiento total de la red. Por lo tanto, cada sistema de protección adoptado puede considerarse como una sub-capa de protección.

Sin embargo, podría ser que uno o más mecanismos de protección sean requeridos en una o más capas de la red. Por lo tanto, pueden existir sistemas de protección en varias modalidades como[6]:

1. **Protección intra-capa**
   a) Un solo mecanismo.
   b) Dos o más mecanismos en serie.
   c) Dos o más mecanismos anidados
2. **Protección inter-capa**
   a) Dos o más mecanismos anidados en capas diferentes.
   b) Dos o más mecanismos en serie pero en capas diferentes.
   c) Una combinación de los dos casos anteriores.

b) Objetivos

La aplicación de los mecanismos de protección en una red tiene como mayores objetivos los siguientes[7]:

1. **Disponibilidad de tráfico**: Se define como la capacidad de los mecanismos de protección para mantener la red en servicio ante eventuales fallas o degradaciones. Cuando varios mecanismos de protección se utilizan a la vez, existen tres niveles de disponibilidad de tráfico:

---

[6] ETSI, Rec. DTR/TM-03041, Transmission and multiplexing (T M) SDH Network Protection Interworking, Sophia Antipolis Cedex-Francia, pág.11, September, 1996.

[7] ETSI, Rec. DTR/TM-03041, Transmission and multiplexing (T M) SDH Network Protection Interworking, Sophia Antipolis Cedex-Francia, pág.16, September,1996.

a) **Nivel 1**: El sistema de protección (combinación de varios mecanismos) utilizado podría no ser capaz de restaurar el 100% del tráfico de la sub-red en el caso de un punto único de falla[8].

b) **Nivel 2**: El sistema de protección debe restaurar el 100% del tráfico entre sub-redes ante la presencia de cualquier punto único de falla.

c) **Nivel 3**: El sistema de protección debe ser capaz de restaurar el 100% del tráfico incluso ante la presencia simultánea de puntos únicos de falla en cada una de las sub-redes.

2. **Independencia**: Consiste en el aislamiento de los efectos colaterales en una sub-red cuando se ha producido la ejecución y por tanto la conmutación de un sistema o mecanismo de protección en otra sub-red.

3. **Variada cobertura de fallas**: La red debe proteger ante diversos tipos de fallas como por ejemplo:

a) Alarmas de servicio: Es el grupo de alarmas cuya presencia significa que se ha producido la pérdida total de la señal. Estas alarmas están relacionadas con la disponibilidad de la señal. Entre ellas se puede mencionar:

i) AIS - Señal de Indicación de Alarma (*Alarm Indication Signal*). AIS puede presentarse a nivel de AU, TU y MS
ii) LOS – Pérdida de señal (*Loss of Signal*).
iii) LOF – Pérdida de alineamiento de trama (*Loss of Frame*).
iv) LOP – Pérdida del puntero (*Loss of Pointer*). Puede presentarse a nivel de AU y TU.

b) Señales de monitoreo: Es el grupo de alarmas cuya presencia significa que la señal entrante presenta un cierto nivel de degradación. Estas alarmas están relacionadas a la calidad de la señal. Entre ellas se puede mencionar:

i) MS-SD - Degradación de la señal a nivel de sección múltiplex (*Multiplex Section Signal Degradation*).

---

[8] Se entiende por punto único de falla, la presencia de una sola falla física en la sub-red o anillo.

ii) SD para contenedores virtuales de orden superior (VC-3 y VC-4).

iii) SD para contenedores virtuales de orden inferior (VC-1, VC-2 y VC-3).

c) Otras señales de información

i) TIM – Identificación del canal (*Trace Identification Mismatch*)

ii) UNEQ – Canal no equipado.

4. **Interconexión de sub-redes protegidas en diferentes capas**: Debería ser posible por ejemplo interconectar sub-redes protegidas a nivel de contenedores virtuales de orden superior (HO-VC) y orden inferior (LO-VC).

5. **Interconexión de sub-redes con diferentes mecanismos de protección**: Debería ser posible interconectar sub-redes protegidas diversamente, sin la necesidad de tener señalización adicional entre las sub-redes.

6. **Minimización de la interrupción de tráfico**: Se refiere al período de tiempo que la red podría ser interrumpida mientras se desarrolla el proceso de conmutación. Depende principalmente del tipo de mecanismo utilizado y de la estrategia de conmutación a seguirse.

7. **Modos de operación**: Se proponen dos tipos:
   a) Modo reversible / no reversible.
   b) Conmutación a simple terminal / doble terminal.

8. **Capacidad utilizada**: Minimizar la capacidad (ancho de banda) utilizada. Depende del tipo de mecanismo utilizado y la forma en que éste ha sido puesto en práctica.

c) Partición de la red

La red se presenta nuevamente con el objetivo de mostrar el tipo de mecanismo de protección apropiado para cada parte de ella. Como primer paso se realiza la partición de la red en varias sub-redes. De esta manera se pueden definir las estrategias de protección y alcanzar la independencia entre ellas. Se definen a continuación cinco sub-redes como se muestra en la figura 4.8.

c1) Sub-redes 1 y 2

Las sub-redes 1 y 2 se determinaron en base a la configuración de la red y su relación con cada uno de los anillos existentes. Obviamente que la relación anillo/tipo de mecanismo fue ya determinada previamente durante la fase de estudio de la arquitectura y capacidad necesaria de la red. Se propone entonces que estas sub-redes sean protegidas por anillos de protección compartidos a dos fibras (o llamados también bidireccionales - *SPRings*) como se explicó en detalle en la sección 3.2.2. Es importante observar que la sub-red 1 se subdivide en dos sub-redes, correspondiendo un anillo a cada una de ellas (anillos 1A y 1B).

c2) Sub-red 3

Corresponde a un enlace que conecta los anillos 1 y 2 a través de los nodos **2** y **9**. Este enlace es uno de las partes más críticas de esta red debido a la gran cantidad de tráfico que por él atraviesa y además, no existen otras rutas alternativas que permitan el re-enrutamiento del tráfico en caso de falla de este enlace.

La capacidad necesaria fue determinada anteriormente como STM-16. Desde el punto de vista de protección, un sistema de protección lineal a nivel de sección múltiplex con conmutación a doble terminal y en configuración 1+1 será aplicado, de acuerdo con lo visto en la sección 3.2.1.5

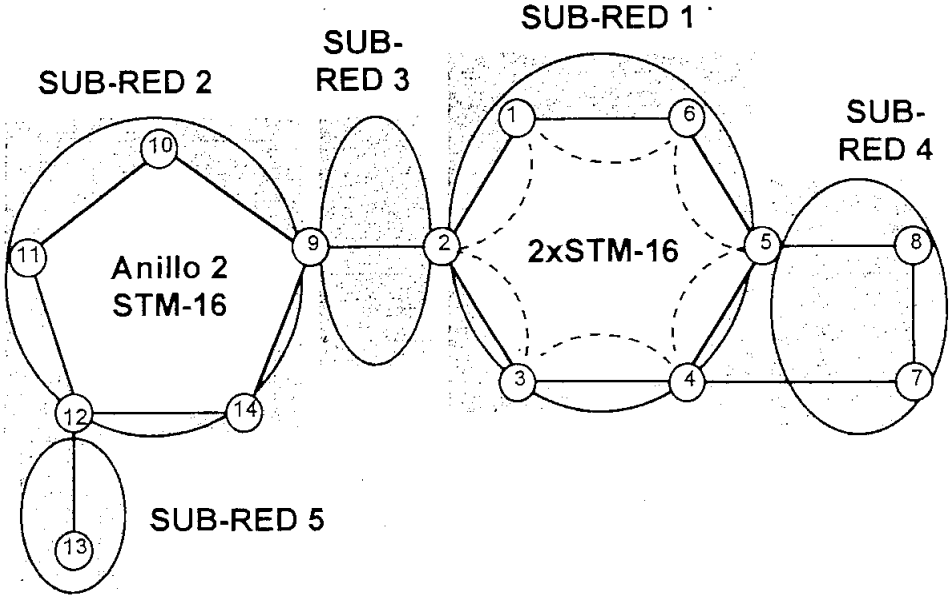


Fig. 4.8 Partición en sub-redes.

c3) Sub-red 4

La configuración de la red presenta dos nodos de interfaz entre esta sub-red y la sub-red 1; por lo tanto, las protecciones ya sean a nivel de contenedor virtual (VC) (Ver sección 3.3.1) o a nivel de conexión de sub-red (SNC) (Ver sección 3.3.2) podrían aplicarse. La utilización de una u otra depende de varios factores como el nivel de disponibilidad requerido por los clientes para cierto grupo de canales de tráfico, y las limitaciones de la capacidad de tráfico disponible en la red, factores que son parte de los objetivos de los sistemas de protección como se mencionó en la sección 4.3.4.5 b).

Si una elevada disponibilidad de tráfico se requiere para ciertos canales, se tendrá una mayor utilización de los recursos de la red, como por ejemplo la capacidad. Por lo tanto, la presencia de este tipo de canales debería reducirse al mínimo. En el presente caso, si se desea proteger el tráfico que va desde el nodo **8** al **13**, éste deberá estar doblemente protegido a nivel de los anillos **1** y **2**, ocupando un mayor ancho de banda en ellos. La protección a nivel de contenedor virtual (VC) es necesaria de modo que la diversificación de trayectorias se realice a lo largo de todo el recorrido del canal dentro de la red. Este tipo de protección sin embargo, no es aplicable en ciertas partes de la red actual por ejemplo los enlaces **2-9** y **12-13**, debido a la inexistencia de dos trayectorias totalmente independientes para enrutar el tráfico considerado.

En cambio, si la disponibilidad de los canales de tráfico no es demasiado exigente, bastaría con proteger la sub-red 4 a nivel de conexiones de sub-red (SNC) hasta su frontera con la sub-red 1, donde el tráfico es protegido a nivel de sección múltiplex por el anillo 1.

Reconsiderando la situación en lo que respecta a la capacidad necesaria para la protección de esta sub-red y habiéndose determinado que la protección a nivel de recorrido es apropiada para este caso, es importante volver a la figura 4.5, donde se muestra la demanda de tráfico en la red. Si se asume la presencia de una falla en el enlace **4-7** por ejemplo, todo este tráfico debe ser enrutado a través de los enlaces **7-8** y **8-5**; esto significa que en el enlace **8-5** se necesitan al menos:

$237 + 283 = 520x2$ Mb/s,

entonces,

$$C = 520/63 = 8.2 \times \text{STM-1},$$

lo que equivale a decir que un sistema con capacidad STM-16 es necesario para proteger el tráfico en esta sub-red.

c4) Sub-red 5

Consiste solamente de un enlace cuya capacidad es equivalente a STM-4. La protección será lineal a nivel de sección múltiplex en configuración 1+1 con conmutación a doble terminal, de acuerdo con lo expuesto en la sección 3.2.1.5

Un sistema en configuración 1+1 a nivel de sección múltiplex equivale a la duplicación del cable de fibra óptica -llamada también "Diversidad de cable"-, lo que se traduce en una considerable elevación de costos de inversión y posteriormente de instalación. Es importante por esto, proponer una solución alternativa a través de un enlace de protección vía radio paralelo a la fibra. Esta solución consistiría en un enlace de radio SDH en configuración inicial 3+1 con facilidades de expansión de hasta al menos 4+1, para proteger totalmente el enlace en fibra, incluso cuando la capacidad de tráfico en este último haya sido completamente utilizada. Un sistema de radio puede actualmente trabajar en configuración 11+1 (once STM-1 con tráfico más uno de protección) o 10+2 (diez con tráfico más dos de protección), de acuerdo con las necesidades de la red. Radio enlaces de alta capacidad son generalmente utilizados para las redes troncales nacionales, como un sistema adicional de protección para la fibra óptica, o donde las condiciones geográficas no permiten un fácil acceso para la instalación de fibras ópticas. Se caracterizan actualmente por su alto grado de confiabilidad, como lo demuestran las bajísimas tasas de error del orden de 1x10E-12, y su alta sensibilidad ante la presencia de bajas tasas de errores (1x10E-12 y 1x10E-09 son generalmente escogidos como umbrales para iniciar la conmutación).

d) Interacción entre sub-redes

En esta sección se mostrará en detalle la forma como se interconectan las sub-redes en las fronteras antes determinadas.

d1) Sub-redes 2 y 5

La figura 4.9 muestra la protección lineal a nivel de sección múltiplex para el enlace **12-13**, basada en una combinación de radio y fibra óptica.

Nótese que a través de la radio la capacidad transmitida es a nivel de canales STM-1 y no STM-4 como se la hace en la fibra. Esto se debe a la limitación del ancho de banda en las frecuencias de radio utilizadas. Generalmente, un sistema de radio utiliza un par de frecuencias para la transmisión y recepción de un canal STM-1; es decir que en este caso se utilizarán 5 pares de frecuencias para la configuración en 4+1 (cuatro canales con tráfico más uno para la protección). Sin embargo, la última generación de sistemas de radio (llamada co-canal) utiliza la técnica de transmisión en doble polarización que necesita un solo par de frecuencias para la transmisión y recepción de dos canales STM-1, cada uno de éstos en diferente polarización. Esto indudablemente ayuda a la mejor explotación de las bandas de radio frecuencia y por tanto al incremento de la capacidad total transmitida.

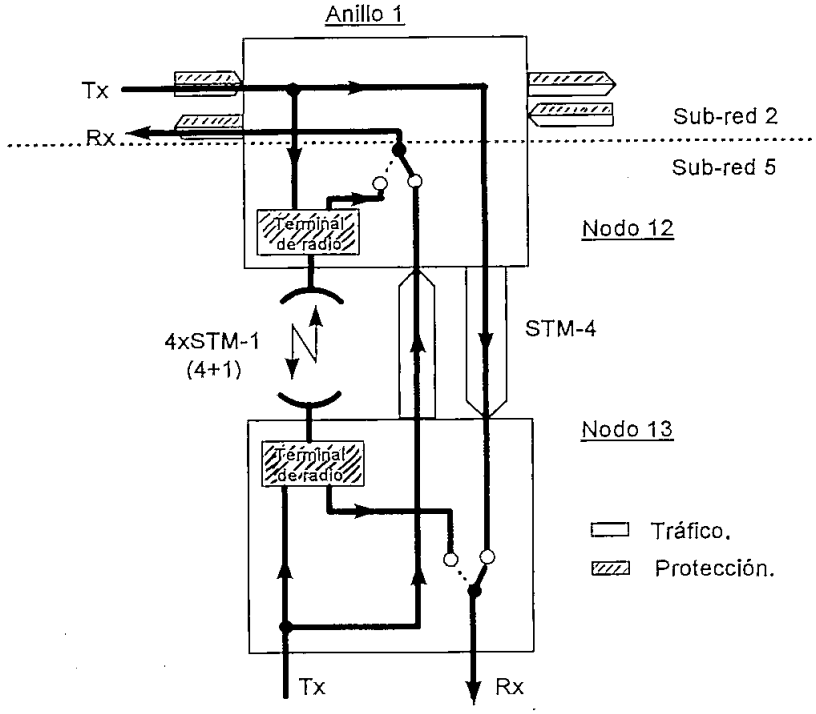


Fig. 4.9 Frontera entre las sub-redes 2 y 5. Protección lineal a nivel de sección múltiplex combinada entre fibra (canal principal) y radio (canal de protección).

d2) Sub-redes 1, 2 y 3

La figura 4.10 ilustra la configuración de la red constituida por el enlace **2-9**. La protección se hace mediante la duplicación de la señal en el lado de transmisión mientras que en la recepción, la detección de la calidad de las dos señales entrantes es el parámetro para decidir cuál es la señal a considerarse como válida.

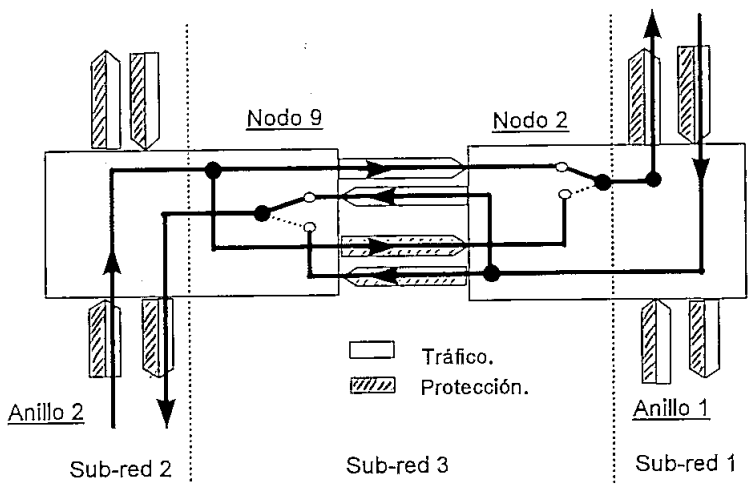


Fig. 4.10 Frontera entre las sub-redes 1, 2 y 3. Se utiliza protección a nivel de sección múltiplex en configuración 1+1 en el enlace 2 - 9 que interconecta los anillos 1 y 2.

La protección a nivel de sección múltiplex es puesta en marcha a través de la diversidad del cable (duplicación del cable de fibra óptica). Otras soluciones alternativas como un enlace vía radio no son aplicables en este caso debido a la elevada capacidad de tráfico involucrada (16xSTM-1).

d3) Sub-redes 1 y 4

En la figura 4.11 se muestra solamente el caso en que los canales entran o salen del nodo número **8** y que han sido enrutados a través de los nodos **5**, **6**, **1**, etc., para dirigirse hacia el nodo **2** y anillo 2. Nótese que la aplicación de protección a nivel de recorrido en la sub-red 4, implica la utilización de capacidad adicional en el anillo 1, entre los nodos **4** y **5**, en las dos direcciones de transmisión. Es muy importante el hecho de que existan dos nodos de interfaz entre estas dos sub-redes, gracias a esto es posible la aplicación de este tipo de protección; es decir, un doble nodo implica mayor confiabilidad de la red debido a la posibilidad de crear rutas diferentes para el tráfico que se desea proteger.

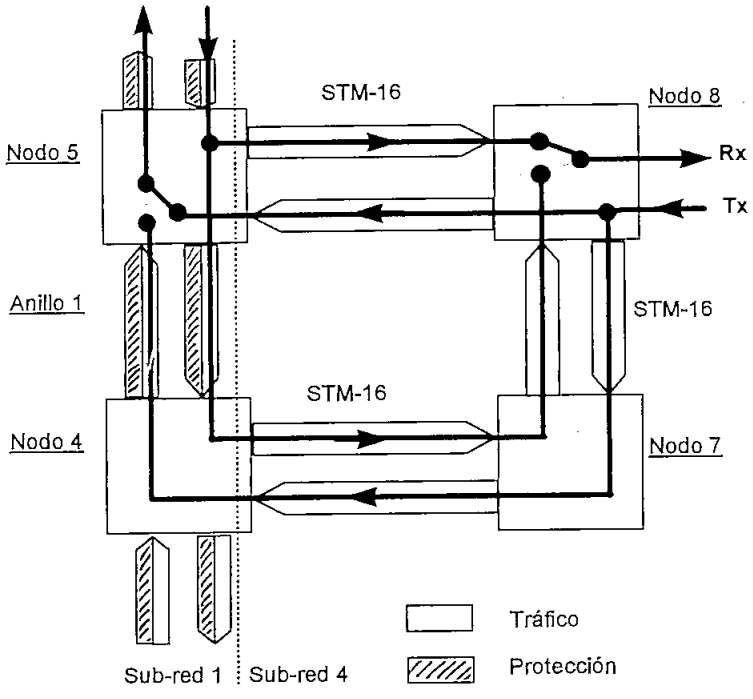


Fig. 4.11 Frontera entre las sub-redes 1 y 4. Se utiliza protección a nivel de recorrido para la sub-red 4 hasta su frontera con el anillo 1.

Aunque la capacidad de los anillos 1A y 1B fue determinada anteriormente, es importante conocer la real demanda de tráfico que existe en el enlace **4-5** como consecuencia de la protección aplicada a la sub-red 4. Existen básicamente dos tipos de mecanismos a ser aplicados: protección a nivel de conexión de sub-red y a nivel de contenedor virtual.

Capacidad requerida para la protección a nivel de conexión de sub-red 4

El tráfico entrante y saliente de la sub-red 4 necesita ser duplicado en cada uno de los nodos **7** y **8** como se muestra en al figura 4.12. Se muestra solamente uno de los sentidos de transmisión para mayor claridad.

Nótese que la protección a nivel de conexión de sub-red incrementa el tráfico entre los nodos **4** y **5** en 460x2 Mb/s. Estos canales están distribuidos así:

181x2 Mb/s adicionales para el anillo 1A y,
279x2 Mb/s adicionales para el anillo 1B.

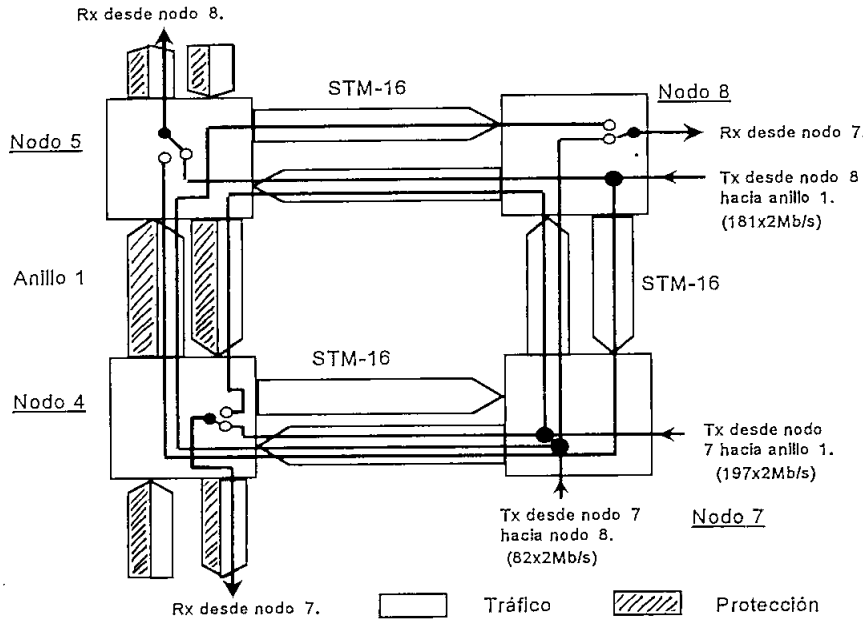


Fig. 4.12 Capacidad adicional de tráfico requerida en el nodo 4-5 para la protección a nivel de conexión de sub-red.

Sin embargo, no todo el tráfico debe ser duplicado. De acuerdo a la figura 4.13, un total de 142x2 Mb/s sigue una trayectoria apropiada de modo que la duplicación de capacidad no es necesaria y por tanto no se incrementa la demanda de tráfico en el enlace 4-5, pues ésta ya fue considerada como parte de la carga inicial en el anillo 1B (Figura 4.7).

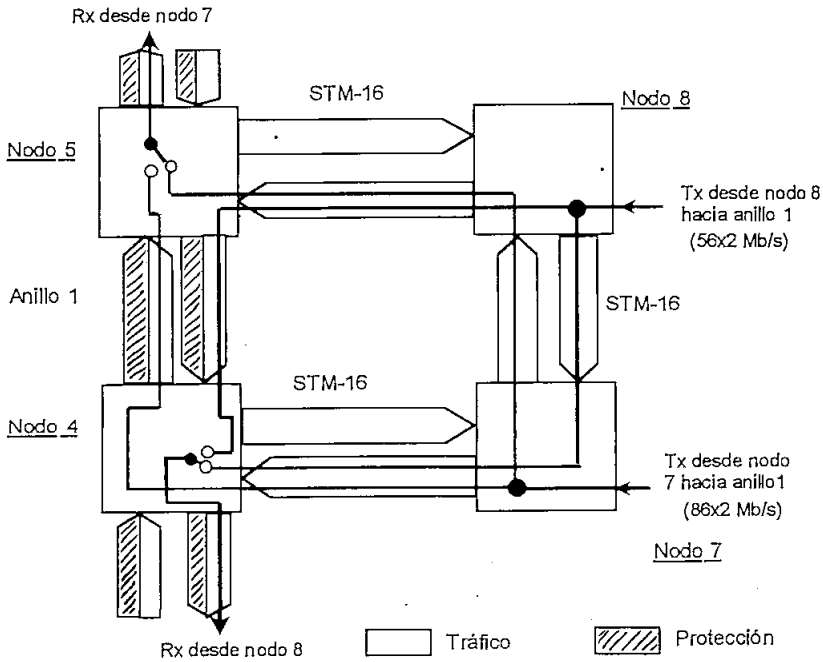


Fig. 4.13 Capacidad necesaria para la protección a nivel de sub-red pero que *no incrementa* la demanda de tráfico en el enlace 4-5.

Capacidad requerida para la protección a nivel contenedor virtual

Aunque no es recomendable aplicar este tipo de protección a nivel de toda la red debido a la ausencia de diversidad de trayectoria en los enlaces **2-9** y **12-13**, ésta se aplicará al tráfico entre los nodos **2** y **8**, como se ve en la figura 4.14. Un total de 56x2 Mb/s es considerado, lo que implica que la carga en el enlace **4-5** se reduce en 56x2 Mb/s, mientras que la demanda se incrementa en los enlaces **4-3-2** del anillo 1B.

La distribución de tráfico entre todos los nodos de la red, sin considerar la capacidad necesaria para la protección, se muestra en la figura 4.16. Además, la demanda final de tráfico (incluyendo la capacidad adicional para protección) se muestra en la figura 4.15. Nótese que los nodos **2**, **4** y **5** son comunes a los dos anillos con el fin de permitir el flujo de tráfico entre ellos y facilitar la interconexión con las sub-redes adyacentes 3 y 4.

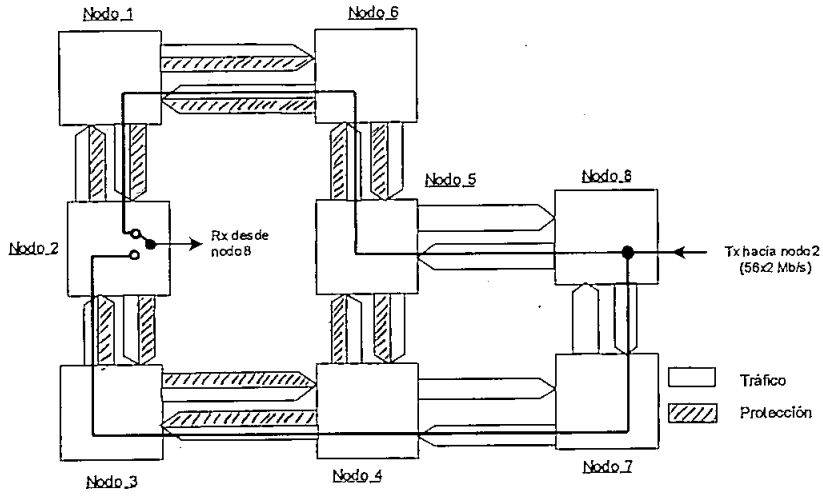


Fig. 4.14 Capacidad requerida para la protección a nivel de contenedor virtual. Solo una dirección de transmisión es mostrada.

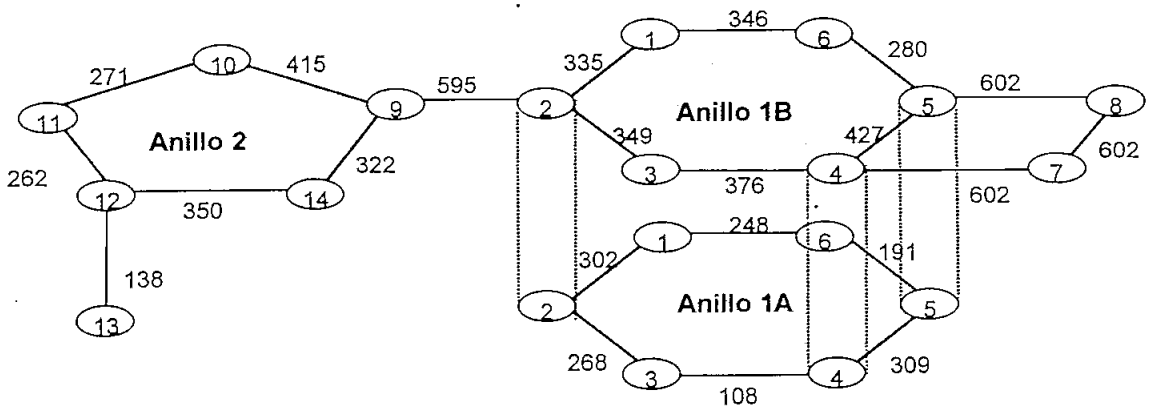


Fig. 4.15 Demanda final de tráfico en la red.

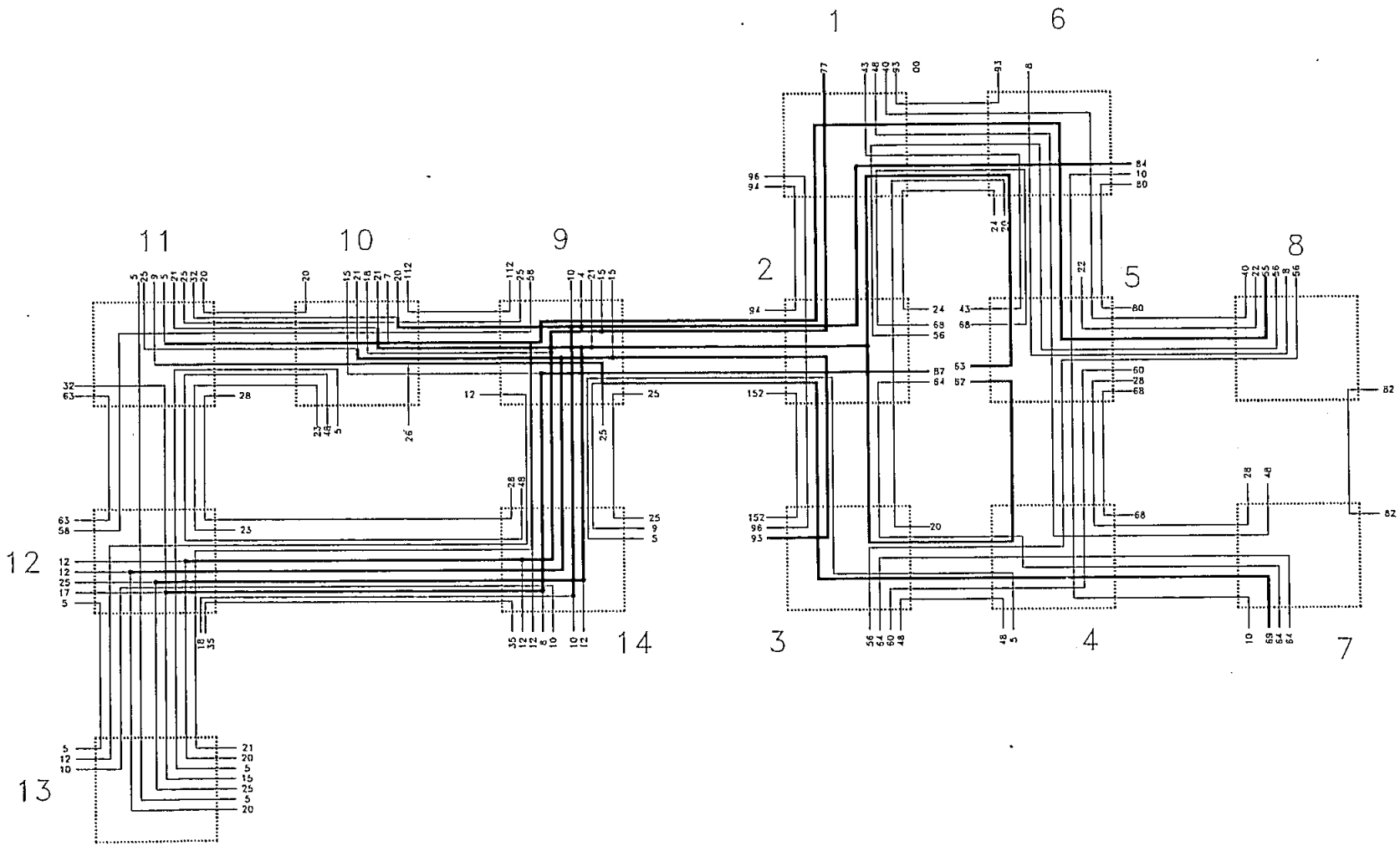


Fig. 4.16 Distribución de tráfico en la red. El tráfico adicional requerido para la protección a nivel de recorrido de la sub-red 4 no es mostrado.

e) Protección a través de la red

La figura 4.17 muestra la trayectoria completa de un canal que parte desde el nodo **8** hasta el nodo **13**, pasando por los anillos **1** y **2** y los enlaces **2-9** y **12-13**. Se ha escogido la trayectoria más corta entre los dos nodos. Las trayectorias de los canales principales se muestran en línea continua, mientras que las trayectorias alternativas de protección se muestran en líneas punteadas (protección a nivel de sección múltiplex) o líneas entrecortadas (protección a nivel de recorrido). En la sub-red 4, el canal es protegido a nivel de sub-red solo hasta su ingreso en el anillo 1.

Adicionalmente, el mismo canal se muestra en la figura 4.18, donde las trayectorias del canal muestran que la conmutación de protección ha sido ya ejecutada ante la presencia de múltiples fallas o degradaciones en la red. Los tipos de fallas consideradas son las siguientes:

1. Falla o degradación de la señal en el enlace **12-13**.
2. Falla del nodo **14**.
3. Falla o degradación de la señal en el enlace **2-9**.
4. Falla en el enlace **1- 6**.
5. Falla o degradación de la señal en el enlace **5-8**.

Nótese que los anillos **1** y **2** se reconfiguran automática e independientemente de los terminales de protección a nivel de sección múltiplex o a nivel de recorrido. La conmutación para la protección a nivel de sección múltiplex se realiza a doble terminal (ambos lados, transmisión y recepción conmutan simultáneamente). En lo que respecta a la capacidad utilizada, el canal con tráfico ha sido protegido a nivel de sub-red 4 con conmutación a simple terminal, sin que su trayectoria haya sido diversificada dentro del anillo 1; de esta manera se optimiza la utilización de la capacidad de la red.

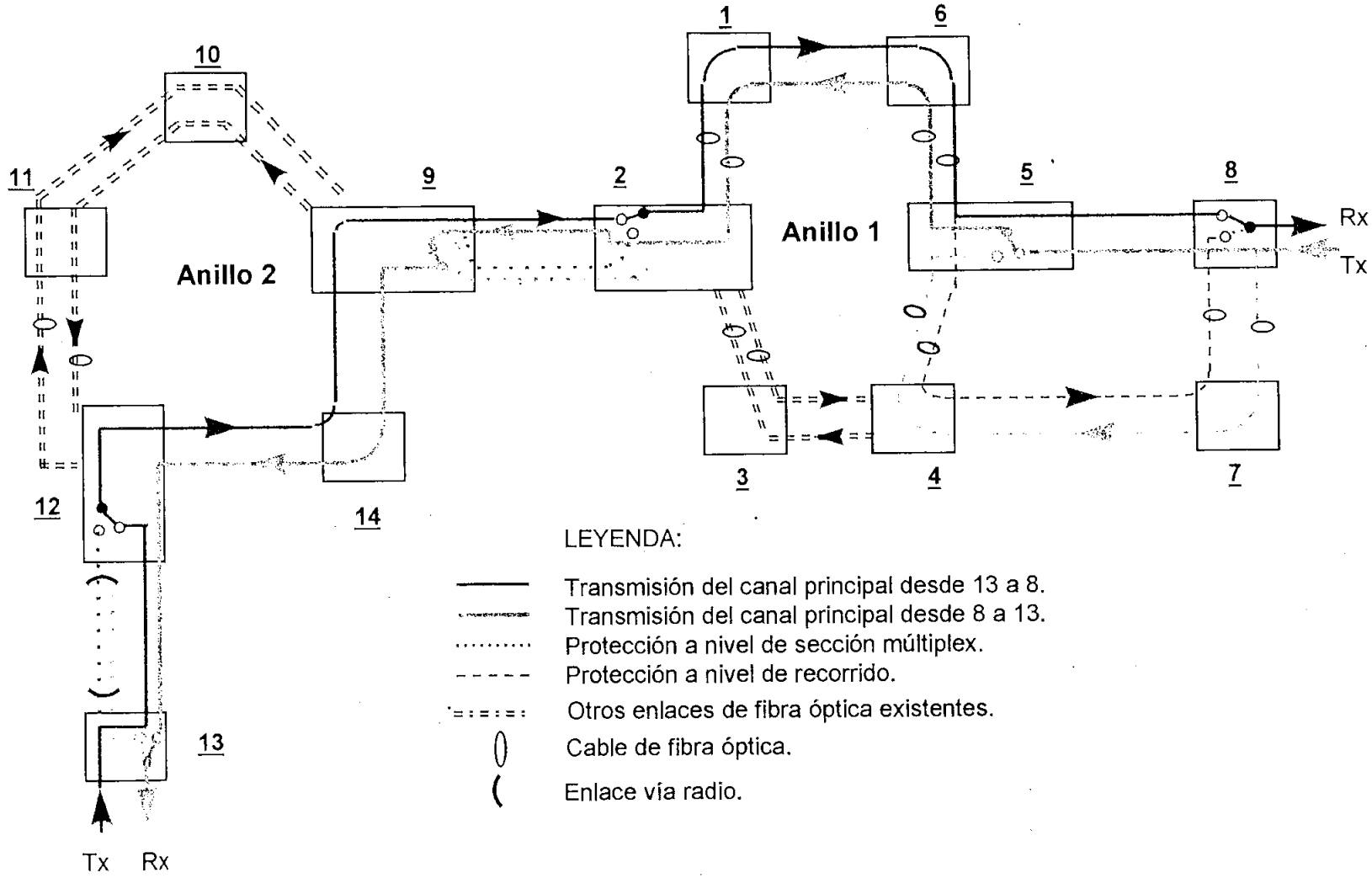


Fig. 4.17 Trayectoria completa a través de la red y mecanismos de protección asociados a un canal de 2 Mb/s entre los nodos 13 y 8.

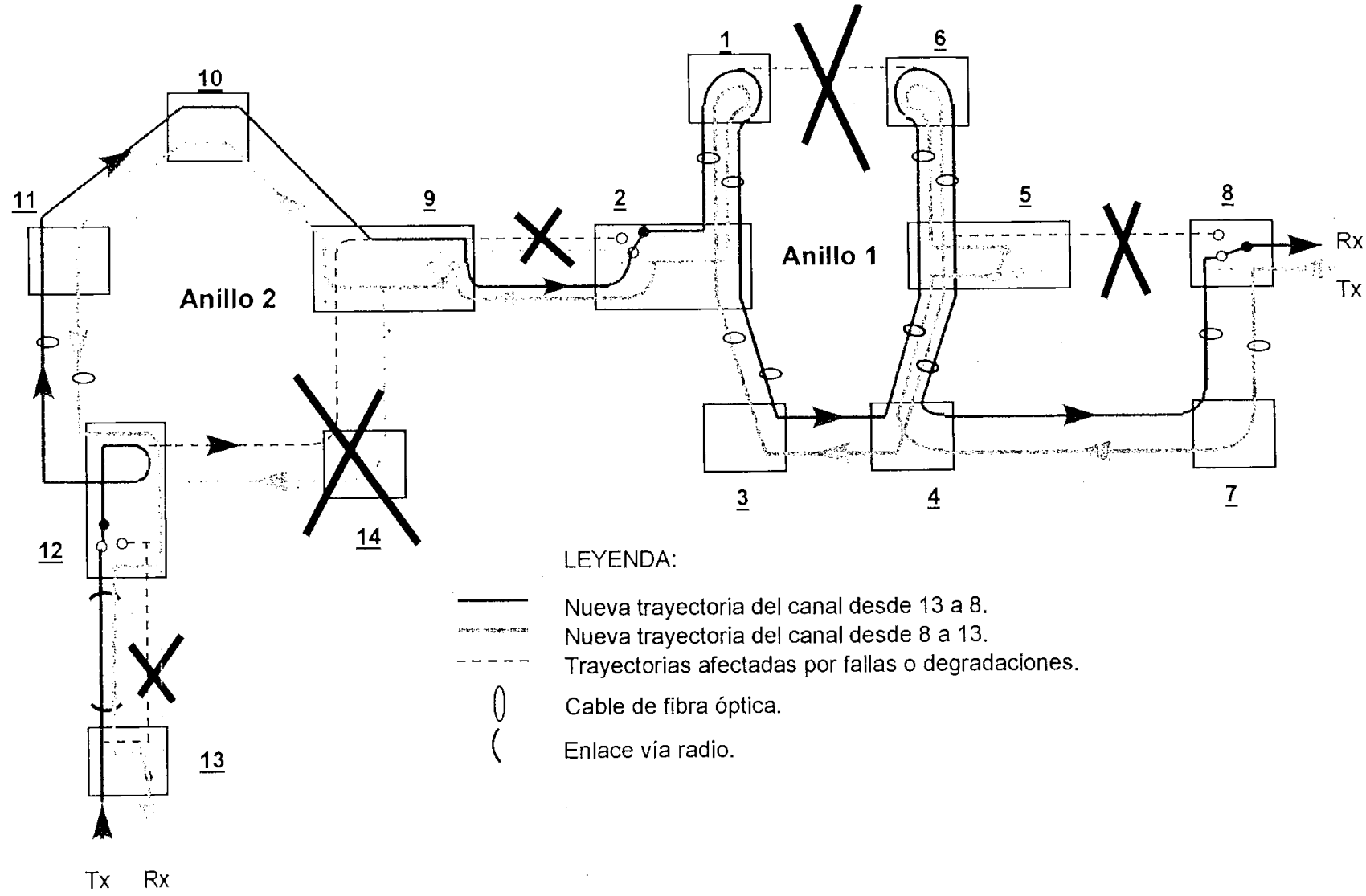


Fig. 4.18 Reconfiguración y re-enrutamiento del canal de la figura 4.17 ante la presencia de múltiples fallas en la red.

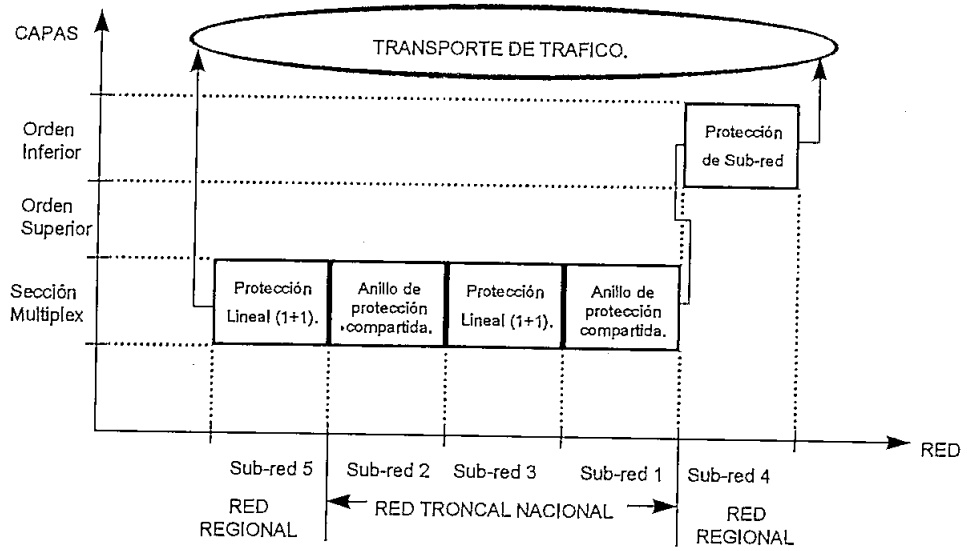


Fig. 4.19 Esquema de mecanismos de protección aplicados a un canal a 2 Mb/s entre los nodos 13 y 8.

En la figura 4.19 se muestran los mecanismos de protección adoptados para el canal a 2 Mb/s del ejemplo anterior. Cada sub-red muestra la capa a cuyo nivel la protección es aplicada. De acuerdo con lo expuesto en la sección 4.3.4.5 a), este esquema de protección se puede definir como un tipo de protección intra-capa en serie entre las sub-redes 5 y 1. Mientras tanto, entre la sub-red 1 y la sub-red 4 se aplica una protección inter-capa en serie.

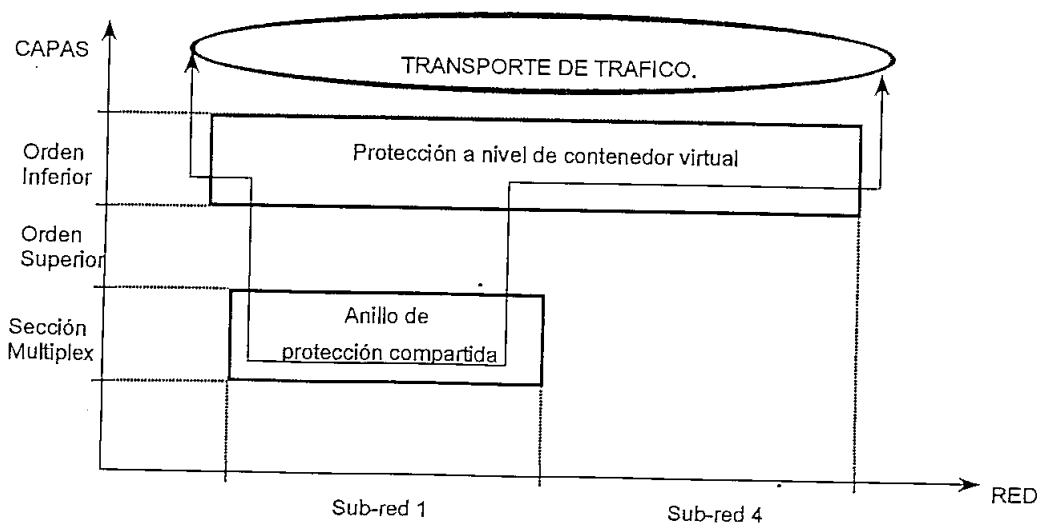


Fig. 4.20 Esquema de protección aplicado al tráfico entre los nodos 2 y 8. El anillo de protección 1A está anidado en la protección a nivel de contenedor virtual. Los dos esquemas se sobreponen en la sub-red 1, dando como resultado mayor confiabilidad al esquema de protección pero ocupando mayor capacidad en el anillo.

En el caso de la protección a nivel de contenedor virtual para las canales de tráfico entre los nodos **8** y **2** (referirse a la figura 4.14), el esquema de protección entre las sub-redes 1 y 4 se presenta como un solo bloque a nivel de la Capa de Orden Inferior, el mismo que atraviesa las sub-redes involucradas en la trayectoria, sobreponiéndose al anillo de protección 1B existente (Ver figura 4.20).

f) Proceso de conmutación

La conmutación es originada mediante la observación de las señales recibidas, lo cual implica la detección y/o generación de alarmas en los diversos niveles de la red[9].

Basándose en el ejemplo de las figuras 4.17 y 4.18, a continuación se describe el proceso de conmutación asociado a cada mecanismo de protección aplicado en las sub-redes del ejemplo.

f1) Protección lineal en la sub-red 5

La protección propuesta es lineal a nivel de sección múltiplex con conmutación a doble terminal (Tx y Rx conmutan en ambos terminales) y de tipo reversible. Se aplica conmutación de tipo reversible debido a que la comunicación vía fibra será considerada como principal, mientras que la radio trabajará como sistema de protección. Es decir, una vez que se ha producido la conmutación hacia la protección (radio), el tráfico debe volver a su canal habitual (fibra), si éste ha sido reparado y no presenta más fallas o degradaciones.

De acuerdo a lo expuesto en la sección 3.2.1.5, este caso de protección corresponde a la protección 1:n a doble terminal, cuyo modelo es expuesto en la figura 3.2. En el ejemplo del presente trabajo se tiene un solo canal STM-4 con tráfico más un canal STM-4 de protección (1+1).

Algunas características y definiciones adicionales se describen a continuación:

1) Los bytes **K** se transmiten a través del *overhead* de la sección múltiplex del canal de

---

[9] Ver la sección 4.3.4.5 b), donde se presentan las clases de alarmas en un sistema SDH. Adicionalmente, el Anexo # 2 contiene un diagrama general con el tipo de alarmas en cada uno de los bloques.

protección (Ver sección 3.2.1.1).

2) Estado Pasivo: Los bytes **Ki** presentan la configuración mostrada en la tabla 4.9[10].

	Valor	Significado
K1 bits 1234	0000	Ninguna petición
K1 bits 5678	0000	Canal de protección presente sobre la reserva.
K2 bits 1234	0000	Canal de protección conectado al puente de conmutación.
K2 bit 5	0	Tipo de conmutación es 1+1.

Tabla 4.9 Configuración de K1 y K2 en estado pasivo.

3) Estado de conmutación: Los bytes **Ki** corresponden a la configuración mostrada en la tabla 4.10.

	Valor	Significado
K1 bits 1234	Xxxx	Tipo de petición (ver tabla 3.1).
K1 bits 5678	Xxxx	Número de canal solicitante (tabla 3.2).
K2 bits 1234	000x	Canal x (0 o 1) viajando a través del canal de protección (tabla 3.3).
K2 bit 5	0	Tipo de conmutación es 1+1.

Tabla 4.10 Configuración de K1 y K2 en estado de conmutación.

4) Proceso de conmutación: En la tabla 4.11 se detalla el proceso de conmutación del presente ejemplo. Se considera que el origen del proceso es la presencia de una alarma de señal degradada (**SD**). Algunos comentarios importantes sobre el proceso se describen a continuación:

   a) El selector de recepción en un terminal conmuta hacia aquel canal, solamente si el número de canal en el byte **K1** enviado (bits 5 a 8) coincide con el número de canal del byte **K2** recibido (bits 1 a 4). En todos los otros casos el selector es liberado (vuelve a la posición normal). La presencia del canal **0** en aquellos bits también origina la liberación del selector.

---

[10] ETSI, Rec. DTR/TM-03041, Transmission and Multiplexing (TM) SDH Network Protection Interworking, Sophia Antipolis Cedex-Francia, September, 1996.

Paso No.	Estado	Dirección de Tx: 12 → 13		Dirección de Tx: 13 → 12		Terminal 12	Terminal 13
		Byte K1	Byte K2	Byte K1	Byte K2		
1	Normal.	0000 0000	0000 0000	0000 0000	0000 0000		
2	SD en canal 1, dirección 12 → 13.			1011 0001	0000 0000		- SD detectada. - Orden de conectar el tráfico a la protección.
3		0010 0001	0001 0000			- Acuse de recibo de petición RR. - Tráfico conmutado hacia la protección.	
4				1011 0001	0001 0000		- # de canal en K1 enviado y K2 recibido coinciden, entonces el selector recibe el tráfico a través de la protección. - Tráfico conmutado hacia la protección.
5		0010 0001	0001 0000			- # de canal en K1 enviado y K2 recibido coinciden, entonces el selector recibe el tráfico a través de la protección. - Conmutación a doble terminal ha concluido.	
6	Canal 1 reparado.			0110 0001	0001 0000		- Inicia el tiempo de espera antes de restablecer (WTR). - Nótese que siempre existe el "acuse de recibo" del terminal 12, y el tráfico se mantiene sobre la protección.
7	Tiempo de espera terminado.			0000 0000	0001 0000		- Ninguna petición (NR). - # de canal en K1 enviado y K2 recibido es diferente, entonces el selector es liberado y el tráfico se recibe a través del canal 1.
8		0000 0000	0000 0000			- Tráfico conmutado hacia el canal 1. - Ninguna Petición (NR). - # de canal en K1 enviado y K2 recibido es diferente, entonces el selector es liberado y el tráfico se recibe a través del canal 1.	
9		0000 0000	0000 0000	0000 0000	0000 0000		- Tráfico es conmutado hacia canal 1.

Tabla 4.11 Proceso de conmutación a nivel de sección múltiplex para el enlace 12-13.

b) Una indicación de "acuse de recibo de petición" (**RR**) es siempre emitida desde el terminal remoto, como respuesta a la presencia de indicaciones cuya prioridad es mayor a "pruebas" **EXER** en el terminal local.

c) Los bytes **K1** y **K2** son reconocidos como tales si se han presentado por al menos tres tramas consecutivas.

d) El proceso de conmutación a doble terminal se considera concluido, solamente si los canales con tráfico en los dos terminales han sido conmutados y una indicación de "ninguna petición" (**NR**) está presente.

f2) Protección en la sub-red 2

La sub-red 2 está constituida por un anillo de protección compartida a dos fibras (*SP-Ring*), cuyo proceso de conmutación se describe en esta sección.

Existen ciertas situaciones que se deben considerar durante la aplicación de los anillos de protección compartida a una red de transporte. Entre estos casos se pueden citar las "conexiones perdidas" y retardo en la transmisión dentro del anillo.

Conexiones perdidas

Esta situación acontece durante el proceso de conmutación en un anillo, cuando se ha producido una falla en uno de los nodos. Considérese el caso del anillo 2, donde el nodo **14** se ha reportado con falla (Ver figura 4.18). La rotura del nodo **14** implica que los nodos

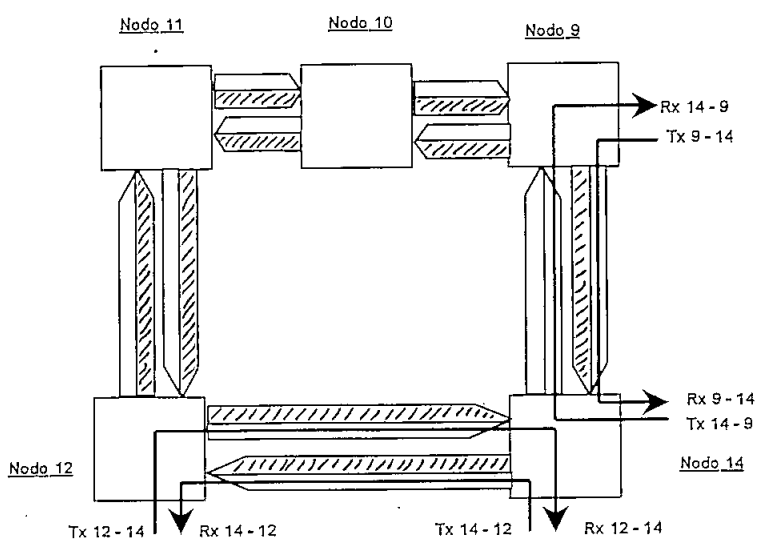


Fig. 4.22 Ejemplo de "conexiones perdidas" en un anillo. Condiciones normales.

9 y **12** ejecutarán el proceso de conmutación en el anillo. Se asume que los canales portadores de tráfico desde el nodo **14** hasta el nodo **12,** pertenecen a la misma sub-trama STM-1 número N (N=1, 2,..., 16) dentro de la trama STM-16 que comunica los nodos **14** y **12**; se asume también que el tráfico entre los nodos **14** y **9** pertenece a la sub-trama STM-1 número N dentro de la trama STM-16 que comunica directamente los nodos **14** y **9** en ambas direcciones (Ver figura 4.22).

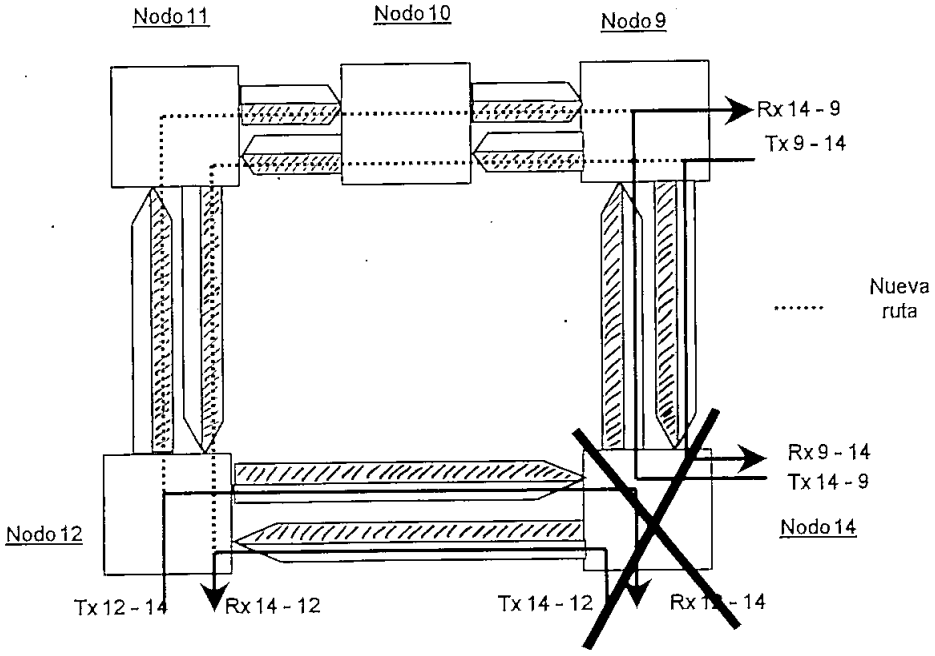


Fig. 4.23 Ejemplo de "conexiones perdidas" en un anillo. Rotura del nodo 14 y reconfiguración del tráfico entre los nodos 14 – 9 y 14 – 12.

La rotura del nodo **14** inicia el proceso de conmutación con la inmediata conmutación de los canales de recepción en ambos extremos de los nodos **12** y **9**, tomando como canal de recepción válido el canal de protección que proviene de los nodos **11** y **10** respectivamente (Ver figura 4.23). De igual manera, los terminales de transmisión en ambos lados ejecutarán la conmutación hacia los canales de protección en dirección contraria a la cual la rotura fue detectada; es decir, los nodos **12** y **9** transmitirán en dirección de los nodos **11** y **10** respectivamente. En estas condiciones, el nodo **9** recibe el tráfico del nodo **12** y no el del **14**; el nodo **12** recibe a su vez el tráfico del nodo **9**. Se ha producido una conexión errada originada por la conmutación del tráfico en el anillo. Este problema puede ser resuelto mediante la inserción de **AU-AIS** en los lados de transmisión de cada uno de los canales STM-1 que portaban tráfico hacia y desde el nodo **14**. Esta acción debe ser ejecutada antes de proceder con la conmutación, de modo que los nodos

cuyos canales estén conectados al nodo **14,** sean informados de que este nodo ha sufrido una rotura y simplemente ignoren la información recibida. El sistema de administración debería ser capaz de realizar un re-ensamblaje de los canales STM-1 con el fin de optimizar la utilización de la capacidad dentro del anillo.

Retardo en el anillo

Cuando se produce la conmutación en el anillo, la longitud de la trayectoria de los canales con tráfico cambia drásticamente, siguiendo un camino más largo y produciendo un incremento en el retardo creado por el medio de transmisión (fibra óptica).

Este fenómeno es particularmente importante en la evaluación del tiempo total empleado por la conmutación, el mismo que está estrechamente relacionado a la longitud del anillo. La ITU-T considera 50 ms. como tiempo de conmutación aceptable para anillos cuya longitud no sea mayor a 1200 Km.

En el caso de anillos con distancias mayores a 1200 Km., por ejemplo en el caso de comunicaciones intercontinentales, una pequeña variación en el proceso de conmutación es aplicada[11]. Esta acción consiste en que todos los canales afectados son conmutados – en cada uno de los nodos de origen- hacia los canales de protección. Con esto se evita el tener largas e incluso repetidas trayectorias en el anillo cuando se produce la conmutación hacia la protección.

Proceso de conmutación

Reglas generales

a) Los bytes **K** son reconocidos como tal, solamente si han sido recibidos durante tres tramas consecutivas.
b) Un anillo a 2 fibras conmuta solo a nivel de anillo, no de enlace.
c) La conmutación del anillo es iniciada, o se considera finalizada, solamente si el nodo ha recibido la confirmación desde el otro terminal a través de la trayectoria larga del anillo.

---

[11] ITU-T, Rec. G.841, Types and Characteristics of SDH Network Protection Architectures, Geneve, July, 1995.

d) Si un nodo recibe en ambas direcciones los bytes **K** emitidos por sí mismo, éste envía una indicación de estado pasivo. Es decir, **K1** (bits 1-4) indicará "ninguna petición" (**NR**) y **K2** (bits 6-8) "ninguna acción" en ambas direcciones.

e) La petición de conmutación emitida por un nodo se produce siempre en las dos direcciones del anillo (una en la trayectoria larga y otra en la trayectoria corta).

f) Un nodo que recibe una petición de conmutación emitirá inmediatamente una indicación de "acuse de recibo" (**RR**) de petición en la trayectoria corta, y la misma petición de conmutación en la trayectoria larga.

g) Si un nodo no está habilitado para ejecutar un proceso de conmutación automática APS, emitirá los bytes **K** con el número de nodo de origen igual al número de nodo de destino (el resto de bits no importa) en ambas direcciones. Esto se conoce como "código APS por omisión".

h) Siempre que un nodo recibe peticiones de conmutación de sus dos nodos adyacentes en las trayectorias cortas, indicando que existen fallas en las señales (**SF-R**), se emite una petición de conmutación en la trayectoria larga en ambas direcciones.

i) Si un nodo detecta señales con falla en ambas direcciones, éste emite una petición de conmutación sobre la trayectoria corta en ambas direcciones.

j) Si un nodo que detecta señal con falla en una dirección, recibe una petición de conmutación en la otra dirección, este nodo emite una petición de conmutación sobre la trayectoria corta en la primera dirección y otra petición de conmutación sobre la trayectoria larga en la segunda dirección.

k) Si un nodo recibe una petición de conmutación del anillo y su número de identificación no corresponde al número de nodo de destino indicado en los bytes **K**, éste debe adoptar la configuración de *by-pass* (recibe los bytes **K** y el canal de protección desde una dirección y los transmite en la otra dirección sin actuar sobre ellos).

l) Los siguientes casos simultáneos de conmutación son permitidos:

   i) **FS-R** con **FS-R**.
   ii) **SF-R** con **SF-R**.
   iii) **FS-R** con **SF-R**.

Esto trae como consecuencia la segmentación del anillo en dos o más partes

independientes.

m) La presencia simultánea de varias peticiones de igual prioridad como **SD-R**, **MS-R** y **EXE-R**, no origina ningún proceso de conmutación y más bien forza al anillo a volver a sus condiciones normales de funcionamiento si alguna conmutación está en curso.

Reglas de transición en un nodo[12]

a) Transición de estado pasivo a estado de *by-pass*. Inicia con cualquier cambio de estado en los bytes **K**, desde **NR** hacia cualquier otra petición de conmutación de acuerdo con la tabla 3.7, siempre que la petición no sea destinada a este nodo.

b) Transición de estado de *by-pass* a estado pasivo. La transición es iniciada con la presencia de ninguna petición (**NR**) en los bytes **K1** y "ninguna acción" es mostrada en **K2** en ambas direcciones del nodo.

c) Transición del estado pasivo al estado de conmutación. Se origina por las siguientes causas:
   i) Cambio en los bytes **K** desde **NR** hacia cualquier otro estado de acuerdo con la tabla 3.7, siempre que sea destinado a este nodo.
   ii) Comandos externos como se vieron en la sección 3.2.2.3.
   iii) Detección de una falla en este nodo.

d) Transición del estado de conmutación al estado pasivo. Se inicia con la detección de **NR** en **K1** y "ninguna acción" en byte **K2** en ambas direcciones. Este proceso se realiza en tres pasos como se explica a continuación:
   i) El terminal remoto que solicitó la conmutación libera el selector y envía indicaciones **NR** en **K1** y puente conmutado en **K2**.
   ii) Una vez que **NR** es recibido, el terminal local libera el puente y selector y envía la indicación de "ninguna acción" en **K2** en ambas direcciones.
   iii) Cuando el terminal remoto recibe la indicación de "ninguna acción", libera también el puente y selector y emite su indicación de "ninguna acción" en **K2** en ambas direcciones.

e) Transición entre estados de conmutación. Se consideran los siguientes casos:

---

[12] ETSI, Rec. DE/TM-03042, Transmission and Multiplexing (TM) SDH Network Protection Schemes, Sophia Antipolis Cedex-Francia, December, 1996.
ITU-T, Rec. G.841, Types and Characteristics of SDH Network Protection Architectures, Geneve, July, 1995.

i) Si un nodo que ha ejecutado la conmutación a nivel de anillo recibe otra petición de conmutación de mayor prioridad para el mismo enlace, éste debe cambiar su prioridad a aquella de la nueva petición de conmutación recibida.

ii) Si la nueva petición de conmutación recibida proviene de un enlace adyacente y es de mayor prioridad, se liberan puente y selector y se procede con la nueva petición.

f) Transición del estado de conmutación al estado de *by-pass*. Existen los siguientes casos como se detalla a continuación:

i) Cuando un nodo que ha ejecutado una conmutación del anillo para un cierto enlace, recibe una nueva petición de conmutación de mayor prioridad en la trayectoria larga para otro enlace no adyacente, éste debe liberar selector y puente, y adoptar la configuración de *by-pass*.

ii) Si un nodo que ha ejecutado una conmutación del anillo, recibe peticiones de conmutación de mayor prioridad en la trayectoria larga y en las dos direcciones, pero no dirigidas a este nodo, éste debe liberar puente y selector y adoptar la configuración de *by-pass*.

g) Transición del estado de *by-pass* al estado de conmutación. Esta transición es originada por la presencia de:

i) Comandos externos de igual o mayor prioridad.

ii) Detección de una falla de igual o mayor prioridad.

iii) Recepción de petición de conmutación de igual o mayor prioridad destinada a este nodo.

iv) Si un nodo que se encontraba en estado de *by-pass* debido a la presencia de **SF-R** o **FS-R**, se encuentra ahora emitiendo una petición de conmutación debida a **SF-R** o **FS-R**, éste debe determinar si la inserción de **AIS** (para evitar "conexiones perdidas") es necesaria y luego proceder con la nueva conmutación.

De acuerdo con las definiciones y reglas antes presentadas, el proceso de conmutación en el caso del anillo 2, cuya rotura ha sido detectada en el nodo **14**, se presenta en la tabla 4.12 y se detalla paso a paso a continuación[13]:

[13] Rotura del nodo significa que ningún canal, principal ni de protección, puede transmitirse ni recibirse en el nodo.

No	ESTADO	NODO									
		11	12		14		9		10		11
		→	←	→	←	→	←	→	←	→	←
1	Condiciones normales.	K1[NR/12] K2[11/S/I]	K1[NR/11] K2[12/S/I]	K1[NR/14] K2[12/S/I]	K1[NR/12] K2[14/S/I]	K1[NR/9] K2[14/S/I]	K1[NR/14] K2[9/S/I]	K1[NR/10] K2[9/S/I]	K1[NR/9] K2[10/S/I]	K1[NR/11] K2[10/S/I]	K1[NR/10] K2[11/S/I]
	Rotura del nodo 14.				X	X					
2,3	Nodos 9 12 detectan SF proveniente de 14.		K1[SF-R/14] K2[12/L/I]	K1[SF-R/14] K2[12/S/RDI]			K1[SF-R/14] K2[9/S/RDI]	K1[SF-R/14] K2[9/L/I]			
4	Nodos 10 y 11 entran en estado de *by-bass*.									K1[SF-R/14] K2[9/L/I]	K1[SF-R/14] K2[12/L/I]
5,6	Nodos 9 y 12 reciben peticiones a través de la trayectoria larga.	K1[SF-R/14] K2[9/L/I]							K1[SF-R/14] K2[12/L/I]		
	Nodos 9 y 12 insertan AIS, conmutan puente, selector y actualizan bytes K.		K1[SF-R/14] K2[12/L/S&B]					K1[SF-R/14] K2[9/L/S&B]			
										K1[SF-R/14] K2[9/L/S&B]	K1[SF-R/14] K2[12/L/S&B]
	Conmutación completada.	K1[SF-R/14] K2[9/L/S&B]							K1[SF-R/14] K2[12/L/S&B]		
7	Nodo 14 transmite código APS por omisión.				K1[XX/14] K2[14/X/X]	K1[XX/14] K2[14/X/X]					
8	Nodo 14 rehabilitado. Emite peticiones de conmutación en la trayectoria larga				K1[SF-R/9] K2[14/L/I]	K1[SF-R/12] K2[14/L/I]					
9	9 y 12 liberan puente, selector, suspenden AIS y entran en *by-pass*.		K1[SF-R/9] K2[14/L/I]					K1[SF-R/12] K2[14/L/I]			
										K1[SF-R/12] K2[14/L/I]	K1[SF-R/9] K2[14/L/I]

		K1[SF-R/12] K2[14/L/I]							K1[SF-R/9] K2[14/L/I]			
				K1[SF-R/12] K2[14/L/I]			K1[SF-R/9] K2[14/L/I]					
10	Nodo 14 emite indicación de estado pasivo (dos direcciones).				K1[NR/12] K2[14/S/I]	K1[NR/9] K2[14/S/I]						
			K1[NR/12] K2[14/S/I]		"	"		K1[NR/9] K2[14/S/I]				
11	Nodos 10 y 11 pasan a estado pasivo.		"		"	"		"		K1[NR/9] K2[14/S/I]	K1[NR/12] K2[14/S/I]	
	Nodo 9 y 12 pasan a estado pasivo.	K1[NR/9] K2[14/S/I]	"		"	"		"	K1[NR/12] K2[14/S/I]	"	"	
	Nodo 14 pasa a estado pasivo.	"	"	K1[NR/9] K2[14/S/I]	"	"	K1[NR/12] K2[14/S/I]	"	"	"	"	
	Condiciones normales.	K1[NR/12] K2[11/S/I]	K1[NR/11] K2[12/S/I]	K1[NR/14] K2[12/S/I]	K1[NR/12] K2[14/S/I]	K1[NR/9] K2[14/S/I]	K1[NR/14] K2[9/S/I]	K1[NR/10] K2[9/S/I]	K1[NR/9] K2[10/S/I]	K1[NR/11] K2[10/S/I]	K1[NR/10] K2[11/S/I]	

Leyenda:

S = trayectoria corta **RDI** = Indicación de defecto del terminal remoto. **NR** = ninguna petición. **S & B** = puente y selector conmutados.

L= trayectoria larga. **SF-R** = Señal con falla (anillo). **I** = ninguna acción (estado pasivo).

Tabla 4.12 Proceso de conmutación del anillo 2 cuando existe una rotura del nodo 14.

1. Inicialmente, todos los nodos se encuentran en estado pasivo (condiciones normales).
2. Los nodos **9** y **12** detectan la presencia de **SF** en los canales principales y de protección provenientes del nodo **14**.
3. Los nodos **9** y **12** emiten la petición de conmutación en las trayectorias larga y corta.
4. Los nodos **10** y **11** entran en estado de *by-pass*.
5. El nodo **9** recibe la petición de conmutación de **12** a través de la trayectoria larga, determina si la inserción de **AIS** es necesaria para evitar "conexiones perdidas" y conmuta el puente y selector. El byte **K2** es actualizado. En este caso, existen canales de tráfico entre los nodos **12** hacia **14** y desde **9** hacia **14**, por lo tanto se inserta **AIS** en la AU correspondiente[14].
6. El nodo **12** procede de igual manera que el **9** en el numeral anterior. La conmutación del anillo ha sido completada.
7. Cuando el nodo **14** ha sido reparado físicamente, pero todavía no es capaz de procesar información, éste transmite el código APS por omisión en ambas direcciones.
8. El nodo **14** ha sido rehabilitado. Este nodo recibe indicaciones de **SF-R** en ambas direcciones; por lo tanto, de acuerdo con la regla general (h), emite peticiones de conmutación en la trayectoria larga en ambas direcciones.
9. Los nodos **9** y **12** reciben la petición y, de acuerdo con la regla de transición (f, ii), liberan los puentes y selectores, suspenden la inserción de **AIS** (para conexiones perdidas) y entran en estado de *by-pass*.
10. La recepción en ambas direcciones de los mismos bytes transmitidos por el nodo **14**, sigue la regla general (d) y emite la indicación de estado pasivo en ambas direcciones.
11. El resto de nodos continúa paulatinamente su retorno al estado pasivo.

f3) Protección en la sub-red 3

La protección aquí utilizada es a nivel de sección múltiplex en configuración similar a aquella propuesta para la sub-red 5 (enlace **12-13**). La diferencia consiste en la capacidad del enlace, pues en este caso se tiene una capacidad STM-16. En este caso es más conveniente escoger una conmutación de tipo no reversible, debido a la gran cantidad de tráfico involucrada. De esta manera se reducen los efectos de la conmutación. El proceso

[14] De la tabla 4.2, el tráfico involucrado entre el nodo 14 y el resto de nodos del anillo es mayor a STM-1; es decir, toda AU que contenga estos canales será marcada como perdida. No existe todavía un pronunciamiento del *ITU-T respecto a la* inserción de AIS a nivel de TU.

de conmutación descrito en la tabla 4.11 se aplica hasta el paso número 5. Luego, una emisión de "Acuse de recibo no requerido" (**DNR**) se emite en el nodo detector de la falla. El proceso reinicia completamente cuando existe la presencia de una nueva falla, retornando al canal principal y se repite indefinidammente.

f4) Protección en la sub-red 1

Se propone la utilización de dos anillos sobrepuestos con capacidad STM-16 para cada uno. Siendo cada uno de estos anillos equivalentes a aquel del anillo 2, no existen diferencias en lo que respecta al proceso de protección desarrollado.

Se considerará en este caso que en el enlace **1-6**, existe la presencia de una falla en una de las direcciones de transmisión (Ver la figura 4.18). Una secuencia del proceso se describe a continuación y se complementa con la tabla 4.13, la misma que presenta el proceso a nivel de los bytes **K**.

Proceso de conmutación en la sub-red 1

1. Todos los nodos se encuentran estado pasivo.
2. Nodo **1** detecta la falla en la dirección proveniente del nodo **6**, y emite la petición de conmutación en ambas direcciones.
3. Nodo **6** recibe la petición del nodo **1** en la trayectoria corta y responde con acuse de recibo de petición.
4. Nodo **6** recibe petición del nodo **1** a través de la trayectoria larga, conmuta puente y selector, actualiza bytes **K** y los envía en las dos direcciones.
5. Nodo **1** recibe indicación sobre la conmutación de puente y selector en el nodo **6**, y conmuta su selector y puente correspondientes. Conmutación finalizada.
6. Cuando la falla ha sido reparada, el nodo **1** inicia el tiempo de espera (**WTR**) emitiendo la indicación en ambas direcciones.
7. Nodo **6** recibe indicación de tiempo de espera (**WTR**) del nodo **1** a través de la trayectoria larga, y responde con acuse de recibo en la trayectoria corta; esta situación se mantiene mientras dure el tiempo de espera.
8. Cuando el tiempo de espera termina, el nodo **1** libera el selector y emite indicación de "ninguna petición" (**NR**) a través de la trayectoria larga.

No	ESTADO	NODO												
		3	2		1		6		5		4		3	
		→	←	→	←	→	←	→	←	→	←	→	←	
1	Condiciones normales.	K1[NR/2] K2[3/S/I]	K1[NR/3] K2[2/S/I]	K1[NR/1] K2[2/S/I]	K1[NR/2] K2[1/S/I]	K1[NR/6] K2[1/S/I]	K1[NR/1] K2[6/S/I]	K1[NR/5] K2[6/S/I]	K1[NR/6] K2[5/S/I]	K1[NR/4] K2[5/S/I]	K1[NR/5] K2[4/S/I]	K1[NR/3] K2[4/S/I]	K1[NR/4] K2[3/S/I]	
	Falla en dirección de 6 a 1						X							
2	Nodo 1 detecta falla.				K1[SF-R/6] K2[1/L/I]	K1[SF-R/6] K2[1/S/RDI]								
3	Nodo 6 responde a nodo 1 con acuse de recibo.		K1[SF-R/6] K2[1/L/I]				K1[RR-R/1] K2[6/S/I]	K1[SF-R/1] K2[6/L/I]						
													K1[SF-R/6] K2[1/L/I]	
											K1[SF-R/6] K2[1/L/I]			
									K1[SF-R/6] K2[1/L/I]					
4	Nodo 6 recibe petición de 1 y conmuta puente y selector.						K1[RR-R/1] K2[6/S/B&S]	**K1[SF-R/1] K2[6/L/B&S]**						
										K1[SF-R/1] K2[6/L/B&S]				
												K1[SF-R/1] K2[6/L/B&S]		
		K1[SF-R/1] K2[6/L/B&S]												
				K1[SF-R/1] K2[6/L/B&S]										
5	Nodo 1 recibe petición de 6 y conmuta puente y selector.				K1[SF-R/6] K2[1/L/B&S]	K1[SF-R/6] K2[1/S/RDI]								
6	Falla reparada. Se inicia tiempo de espera.				K1[WTR/6] K2/L/B&S]	K1[WTR/6] K2[1/S/B&S]								

7	Nodo 6 recibe indicación de tiempo de espera y responde.						K1[RR-R/1] K2[6/S/B&S]	K1[WTR/1] K2[6/L/B&S]					
8	Tiempo de espera termina, nodo 1 libera el selector.				K1[NR/6] K2[1/L/B]	K1[NR/6] K2[1/S/B]							
			K1[NR/6] K2[1/L/B]										
												K1[NR/6] K2[1/L/B]	
										K1[NR/6] K2[1/L/B]			
									K1[NR/6] K2[1/L/B]				
9	Nodo 6 recibe "ninguna petición" de 1 y libera puente y selector.						K1[NR/1] K2[6/S/I]	K1[NR/1] K2[6/L/I]					
										K1[NR/1] K2[6/L/I]			
												K1[NR/1] K2[6/L/I]	
		K1[NR/1] K2[6/L/I]											
				K1[NR/1] K2[6/L/I]									
10	Nodo 1 recibe "ninguna petición" de 6 y libera el puente.				K1[NR/6] K2[1/L/I]	K1[NR/6] K2[1/S/I]							
11	El resto de nodos torna al estado pasivo cuando reciben NR en K1 y K2 muestra "ninguna acción" (I) en ambas direcciones.	K1[NR/2] K2[3/S/I]	K1[NR/3] K2[2/S/I]	K1[NR/1] K2[2/S/I]	K1[NR/2] K2[1/S/I]	K1[NR/6] K2[1/S/I]	K1[NR/1] K2[6/S/I]	K1[NR/5] K2[6/S/I]	K1[NR/6] K2[5/S/I]	K1[NR/4] K2[5/S/I]	K1[NR/5] K2[4/S/I]	K1[NR/3] K2[4/S/I]	K1[NR/4] K2[3/S/I]

Leyenda:

S = trayectoria corta **RDI** = Indicación de defecto **NR** = ninguna petición. **S & B** = puente y selector conmutados.

L= trayectoria larga. **SF-R** = Señal con falla (anillo). **I** = ninguna acción (estado pasivo). **WTR** = tiempo de espera antes de restablecer.

Tabla 4.13 Proceso de conmutación del anillo 1 cuando existe una degradación y falla en el enlace 1-6.

9. Nodo **6** recibe indicación de "ninguna petición" (**NR**) del nodo **1** y libera puente y selector. Emite como respuesta otra indicación de "ninguna petición" (**NR**).
10. Nodo **1** recibe indicación de "ninguna petición" del nodo **6**, y libera el puente. Emite "ninguna petición".
11. A medida que la emisión de "ninguna petición" del nodo **1** pasa a través de los otros nodos intermedios, éstos verifican el estado de los bytes K en las dos direcciones. La presencia de indicación de "ninguna petición" (**NR**) en **K1** y "ninguna acción" en **K2**, permite que los nodos vuelven al estado pasivo.

f5) Protección en la sub-red 4

En esta sub-red 4 se aplican dos tipos de mecanismos, como se describe a continuación:

- **Protección a nivel de conexión de sub-red**: Protege todo el tráfico hacia y desde los nodos **7** y **8**, a excepción de aquel entre los nodos **2** y **8**.
- **Protección a nivel de contenedor virtual**: Se aplica exclusivamente a los canales de tráfico entre los nodos **2** y **8**.

Protección a nivel de conexión de sub-red

El tráfico protegido a través de este mecanismo es mostrado en la figura 4.12. Existen dos puntos de interfaz entre esta sub-red 4 y el anillo 1. Estas interfaces corresponden a los nodos **4** y **5** que son los puntos donde se ubican los terminales para este tipo de protección. Las dos trayectorias (principal y de protección) son independientes, como se requiere para este mecanismo.

La teoría principal de este mecanismo fue presentada en la sección 3.3.2, donde se indicó que se puede aplicar con conmutación a simple o doble terminal. La conmutación a doble terminal carece aún de protocolos de conmutación oficiales por parte del ITU-T. Por el contrario, la conmutación a simple terminal no necesita de ningún protocolo y se basa solamente en la información proporcionada por el terminal local o por requerimientos externos también emitidos a nivel local.

La configuración adoptada es 1+1 dedicada, con conmutación a simple terminal

y de tipo no reversible. Se escoge el tipo no reversible debido a la gran cantidad de tráfico manejada, evitando de esta manera el doble efecto de la transición desde el canal principal hacia la protección y luego volver al canal principal como sucede en el caso reversible.

Un total de 546x2 Mb/s (=602-56) es protegido de esta manera[15] (Ver figuras 4.12 y 4.13). Estos canales serán multiplexados adecuadamente a nivel de STM-1, de modo que el monitoreo se la hará a nivel de recorrido de orden superior, lo cual permite realizar una tarea más simple y efectiva. El monitoreo de estos canales se realiza de acuerdo a la clase de conexión de sub-red utilizada, inherente o *non-intrusive*. Esto fue presentado en la sección 3.3.2.

Proceso de conmutación a nivel de conexión de sub-red

A manera de una breve introducción se podría decir que el terminal de transmisión duplica la información y se mantiene transmitiendo a través de las dos trayectorias disponibles. En el lado de recepción se decide la conmutación del selector de acuerdo al tipo de petición recibida y a su prioridad correspondiente.

Como parte de la demostración se asume la presencia de una señal defectuosa detectada en la dirección del nodo **5** hacia el nodo **8**. La indicación de **SF** es generada por la presencia de una de las alarmas indicadas en la sección 3.3.2.1. Entre estas alarmas se podría tener **HP-SSF**, provocada por **AU-LOP** o **AU-AIS**[16]. El proceso en sí se describe a continuación:

1. Nodo **8** detecta **SF** en el canal principal proveniente del nodo **5**.
2. El terminal local verifica la presencia de otras peticiones (tabla 3.12) y decide la conmutación del selector hacia el canal de protección proveniente del nodo **7**.
3. Tratándose de una conmutación total a nivel STM-16, todos los otros canales provenientes del nodo **5** serán simultáneamente conmutados hacia la protección.
4. Una vez que el canal con falla ha sido reparado, el nodo **8** emite una indicación de "ninguna petición" (**NR**).
5. Nodos en condiciones normales.

---

[15] En la fig. 4.15 existen 602x2 Mb/s en cada enlace. De éstos se excluyen 56x2 Mb/s que serán *protegidos a nivel de VC*.

[16] Referirse a la sección 3.3.2.1 y Anexo # 2 sobre las señales y alarmas.

Protección a nivel de contenedor virtual

Un total de 56 x 2 Mb/s es protegido a través de este mecanismo. Este grupo de canales es insertado en una misma trama STM-1 (63 x 2 Mb/s) de modo que sean considerados como una sola unidad de transporte y se faciliten las funciones de monitoreo y protección. En este caso sucede que 7 x 2 Mb/s no serán utilizados (se pueden considerar como capacidad de reserva), pero deberán ser identificados claramente como no equipados (**UNEQ**).

El tipo de configuración seleccionada es 1+1 con conmutación a simple terminal y de tipo reversible. Como en el caso anterior, la conmutación a simple terminal no necesita de ningún protocolo y se basa solamente en la información proporcionada por el terminal local o por requerimientos externos también emitidos a nivel local.

La evaluación de los canales recibidos se realiza mediante el monitoreo de los bytes **B3** (**HP-EXC**, **HP-DEG**), **J1** (**HP-TIM**), **C2** (**HP-UNEQ**) que pertenecen al POH del VC-4; además de la verificación del tipo de señalización recibida (**LOP**, **AIS**, etc.)[17].

La trayectoria principal de los canales incluye los nodos **8**, **5**, **6**, **1** y **2**, mientras que aquella de protección está formada por los nodos **8**, **7**, **4**, **3** y **2** (Ver figura 4.14). Nótese que ninguna de las dos trayectoria incluye nodos intermedios comunes a ellas. Es importante la independencia de trayectorias para mejorar la confiabilidad de estos canales.

Proceso de conmutación a nivel de contenedor virtual

El proceso de conmutación para la red del ejemplo con falla en el enlace **5** - **8** (Ver figura 4.14) es bastante simple y se detalla a continuación:

1. El nodo **2** detecta la presencia de **SF** en la trayectoria principal.
2. Si existen varios requerimientos a la vez, el nodo **2** verifica la prioridad de acuerdo con la tabla 3.12, y conmuta el selector hacia la protección.

---

[17] Referirse a la sección 3.3.1.1 sobre las señales y alarmas. El Anexo # 2 también muestra este tipo de información.

3. Se inicia el tiempo de espera **WTR**. Durante este tiempo de espera, cualquier indicación de mayor prioridad anulará esta condición y el selector se mantendrá conectado a la protección.
4. Cuando el tiempo de espera termina, se emite una indicación de "ninguna petición" (**NR**).
5. Selector del nodo **2** conmuta hacia el canal principal.
6. Nodo **2** en condiciones normales.

4.3.4.6 Agrupamiento de tráfico

Consiste en el ordenamiento o clasificación de los canales de tráfico de acuerdo a varios factores como: tipo de trayectoria, tipo de información transportada, prioridad previamente asignada por el cliente o tipo de mecanismo utilizado. En este último caso por ejemplo, la aplicación de protección lineal a nivel de sección múltiplex implica el agrupamiento previo de todos los canales involucrados entre los dos terminales en consideración. Una vez construida la trama a nivel STM-4 (caso del enlace **12-13**) o STM-16 (enlace **2-9**), el proceso de puesta en marcha y la ejecución del mecanismo puede ser iniciada. La protección a nivel de recorrido (ya sea a nivel de conexión de sub-red o de contenedor virtual) implica también un agrupamiento previo en el caso de que la protección sea dada a nivel de contenedores virtuales de orden superior.

Desde el punto de vista topológico de la red, el agrupamiento de tráfico se clasifica en:

1. **Agrupamiento de terminal a terminal**: Los canales agrupados se mantienen juntos desde el origen hasta su destino, pasando por todos los nodos intermedios sin ninguna inserción o extracción de ellos. Ejemplo: tráfico protegido a nivel de recorrido (conexión de sub-red o contenedor virtual).

2. **Agrupamiento por enlace**: Los canales son agrupados entre dos nodos adyacentes solamente. Ejemplo: protección a nivel de sección múltiplex.

3. **Agrupamiento seccional**: Está formado por un grupo de canales que son insertados y posteriormente extraídos de otro grupo principal. La trayectoria seguida

es solamente una parte de la trayectoria perteneciente al grupo principal. Ejemplo: inserción y extracción de canales en un anillo de protección.

4.3.4.7 Equipamiento

En base a las figuras 4.15 y 4.16, donde se muestra la demanda total de tráfico en la red y su respectiva distribución entre los nodos, en esta sección se plantea el tipo de aparatos a utilizarse para la puesta en marcha de la red. En la figura 4.24 se muestra el diagrama de bloques del equipamiento propuesto en base a los aparatos vistos en la sección 1.2, como son los multiplexores terminales, de inserción extracción y de conmutación. Los aparatos de radio también son propuestos como una vía adicional de protección, de acuerdo a lo explicado la sección 4.3.4.5 sobre los mecanismos de protección para la sub-red 5.

El enlace **12-13** está provisto de un terminal multiplexor TM 4 para la ruta principal, con capacidad de convertir flujos de 2 Mb/s en flujos STM-4. La ruta de protección utiliza terminales multiplexores TM 4/1 cuya función es la de convertir flujos STM-4 en flujos STM-1, puesto que los aparatos de radio generalmente transmiten flujos a nivel STM-1. De esta manera, los aparatos terminales TM 4/1 y la radio actúan solamente como regeneradores de información. Esto es importante para no interferir con la función principal de protección encargada a los terminales TM 4, los mismos que ejecutan la conmutación en caso de averías. Nótese además que para la ruta de protección que utiliza la radio, existe una protección de tipo n+1 en caso de tener otras averías en la sección de radio.

El anillo 2 está conformado por multiplexores de inserción/ extracción ADM 16 capaces de convertir señales tributarias de 2 Mb/s o STM-4, en señales STM-16, que son los niveles transmitidos en el lado de línea del anillo. Los multiplexorés ADM 16 son los encargados de la conmutación en caso de roturas. En el nodo **9** se utilizan terminales multiplexores TM 16 que son los encargados de insertar señales STM-4 provenientes del aparato ADM 16 o señales de 2 Mb/s, originadas en el mismo nodo, para la formación de una señal STM-16 que será transmitida hacia el nodo **2**. Los terminales TM 16 del nodo **9** y **2**, son los encargados de ejecutar la conmutación para la protección lineal a nivel de sección múltiplex.

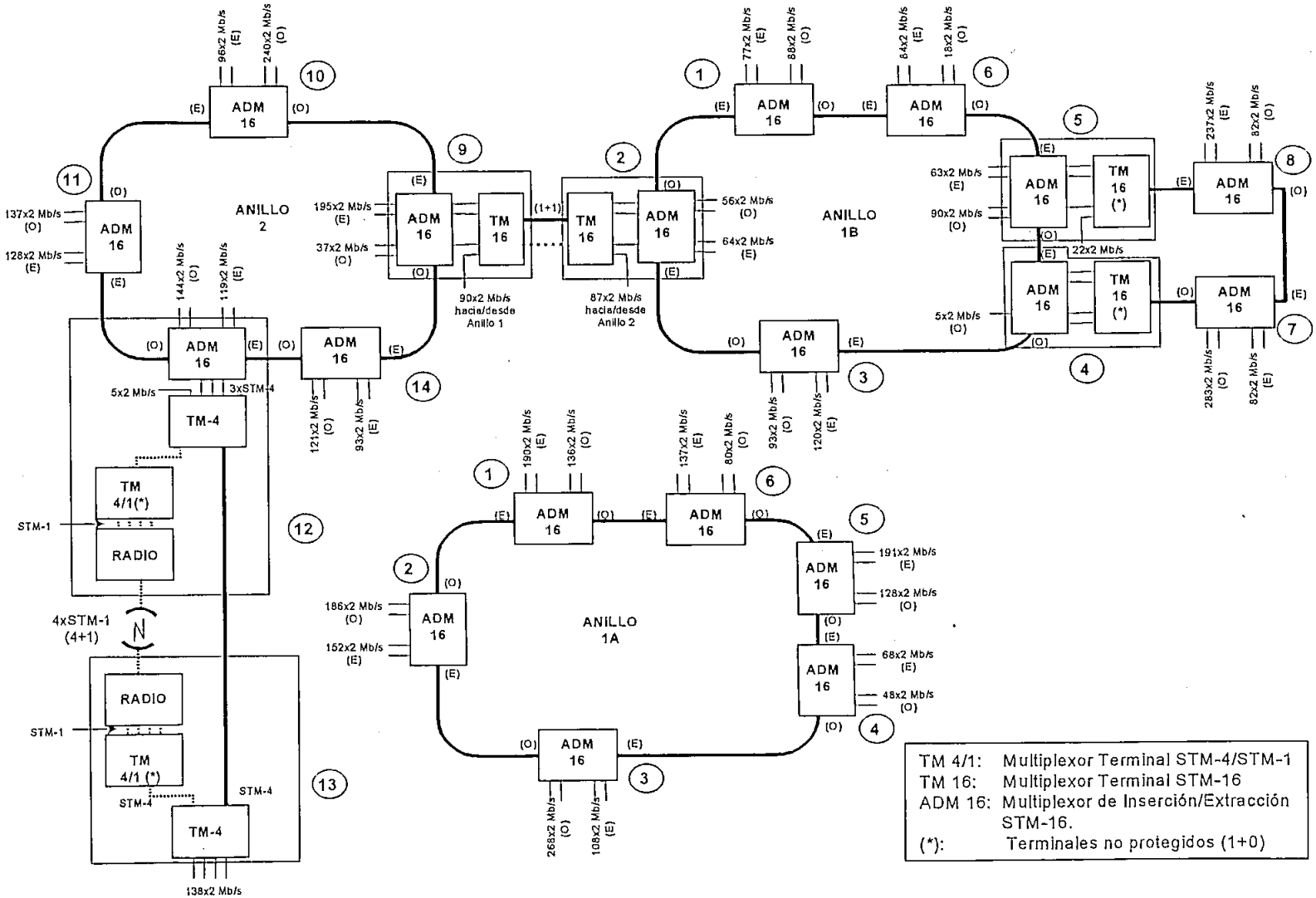


Fig. 4.24 Equipamiento de la red.

El anillo 1B utiliza multiplexores de inserción extracción ADM 16, que ejecutan el proceso de protección en configuración de anillo bidireccional a 2 fibras de acuerdo con lo expuesto en la sección 3.2.2. En el nodo **5** y **4** se utilizan terminales de multiplexación TM 16 cuya función se limita a multiplexar señales de 2 Mb/s y STM-4, formar una señal STM-16, y transmitirla hacia los nodos **8** y **7** respectivamente. La duplicación de los canales para la ejecución de la protección a nivel de conexión de sub-red es desarrollada por los aparatos ADM 16 del anillo 1B. De igual manera, los ADM 16 de los nodos **7** y **8** realizan la duplicación necesaria de los canales para la transmisión hacia los nodos **4** y **5**.

4.3.4.8 Disponibilidad y confiabilidad

Los términos disponibilidad y confiabilidad están estrechamente relacionados a la operación de la red. La confiabilidad representa la probabilidad de un componente, o de toda la red, de cumplir satisfactoriamente con una cierta función bajo determinadas condiciones de operación, y por un determinado período de tiempo para el que fueron diseñados. La disponibilidad se define entonces como la proporción de tiempo en que el componente o la red se encuentran en capacidad de brindar servicio. Así, la disponibilidad es una de las formas de representar la confiabilidad del componente o de la red.

Como se ha podido notar en el ejemplo de aplicación anteriormente mostrado, el nivel de confiabilidad alcanzado estaría determinado por la robustez de la red ante la presencia de fallas. La protección está basada en la disponibilidad de una determinada capacidad adicional que puede ser utilizada para permitir el re-enrutamiento o la diversificación de trayectorias necesarias, con el fin de mantener la comunicación entre un determinado par de nodos.

A continuación se definen algunos términos básicos utilizados en el estudio de la confiabilidad de la red.

MTBF: Tiempo promedio entre fallas de la unidad.
MTTR: Tiempo promedio empleado para reparar la unidad con falla (o sustituirla con una de repuesto).

MSRT: Tiempo promedio para restaurar el servicio (incluye el tiempo para detectar la falla).

MRT: Tiempo promedio empleado para la provisión de la unidad reparada (o de repuesto) en el sitio de ocurrencia de la falla.

De allí se concluye que,

$$MSRT = MTTR + MRT \qquad (4.4)$$

La estimación de la confiabilidad de la red se basa en la predicción de la tasa de roturas de cada uno de los componentes, y luego de toda la red. Así, la unidad básica de análisis está representada por el MTBF, cuyos valores son obtenidos de datos experimentales y sobre la base de los cuales se puede predecir la confiabilidad de una nueva y completa unidad que no ha sido todavía sometida a este tipo de pruebas[18]. Los MTBF se obtienen para cada uno de los componentes eléctricos, electrónicos, mecánicos, semiconductores, etc.

Para evaluar la disponibilidad de la red se utilizan los diagramas lógicos[19] y el llamado modelo de estructuras serie-paralelo[20]. Los diagramas lógicos consisten en la representación gráfica de ciertas combinaciones entre los componentes, cuya disposición muestra la secuencia funcional y lógica de la red. En el modelo de estructuras serie-paralelo, cada uno de los componentes es representado con sus respectivos parámetros de confiabilidad, y se realiza la reducción de componentes en paralelo a su equivalente en serie, hasta lograr la máxima simplificación de la red. En base a los últimos parámetros calculados se obtiene la probabilidad total de que el sistema esté trabajando, es decir la disponibilidad de la red.

Considérese un bloque de n componentes en paralelo o serie. La evaluación de su bloque equivalente utiliza los siguientes parámetros:

---

[18] La MIL-HDBK-217 es una base de datos de MTBF utilizada como un estándar para todas las industrias. Fue inicialmente elaborada con fines militares para la predicción de fallas de los componentes.

[19] ENDRENYI J., Reliability Modeling in Electrical Power System, John Wiley & Sons, New York, 1978.

[20] MODARRES M., A Method of Predicting Availability Characteristics of Series-Parallel Systems, IEEE Transactions On Reliability, Vol. R-33, No. 4, October 1984.

n: Número de componentes activos.

i: Número de componente en el bloque ($1 \leq i \leq n$)

λ: Tasa de roturas de cada componente.

$$\lambda = 1/MTBF \qquad (4.5)$$

μ: Tasa de reparación de cada componente.

$$\mu = 1/MTTR = 1/\tau \qquad (4.6)$$

Entonces, la tasa equivalente de roturas del bloque λ_{eq} y su correspondiente tasa de reparación μ_{eq} están dadas por[21]:

Configuración	Tasa de roturas λ_{eq}	Tasa de reparación μ_{eq}
Paralelo	$\prod_{i=1}^{n} \lambda_i \tau_i \sum_{i=1}^{n} 1/\tau_i$ (4.7)	$\sum_{i=1}^{n} 1/\tau_i$ (4.8)
Serie	$(1-\sum_{i=1}^{n} \lambda_i \tau_i) \sum_{i=1}^{n} \lambda_i$ (4.9)	$\frac{\left(1-\sum_{i=1}^{n} \lambda_i \tau_i\right)^2 \sum_{i=1}^{n} \lambda_i}{\sum_{i=1}^{n} \lambda_i \tau_i}$ (4.10)

En base a estos resultados se puede obtener la disponibilidad A_{eq} e indisponibilidad U_{eq} de cada bloque, como se define a continuación:

$$A_{eq} = MTBF_{eq} / (MTBF_{eq} + MTTR_{eq}) \qquad (4.11)$$

$$U_{eq} = MTTR_{eq} / (MTBF_{eq} + MTTR_{eq}) \qquad (4.12)$$

Reemplazando las ecuaciones (4.5) y (4.6) para el equivalente de cada bloque, en las ecuaciones (4.11) y (4.12), se obtiene lo siguiente:

---

[21] MODARRES M., A Method of Predicting Availability Characteristics of Series-Parallel Systems, IEEE Transactions On Reliability, Vol. R-33, No. 4, October 1984.

$$A_{eq} = \mu_{eq} / (\mu_{eq} + \lambda_{eq}) \quad (4.13)$$

$$U_{eq} = \lambda_{eq} / (\mu_{eq} + \lambda_{eq}) \quad (4.14)$$

Donde λ_{eq}, μ_{eq} se obtienen de las ecuaciones (4.7), (4.8), (4.9) y (4.10).

La disponibilidad antes mencionada se conoce como "disponibilidad intrínseca", o debida solo a problemas de roturas o degradaciones relacionadas estrictamente al sistema. Existe además la "disponibilidad operacional" que considera los tiempos de detección de falla, disponibilidad de repuestos en las estaciones de trabajo, tiempo de viaje hasta el sitio donde se produjo la falla, etc. En ese caso, el MSRT debería utilizarse en lugar de MTTR en la ecuación (4.11) para su respectiva evaluación.

Considerando como referencia el ejemplo de la sección 4.3.4, se procede a evaluar la confiabilidad y disponibilidad del canal a 2 Mb/s de las figuras 4.17 y 4.18. Para la elaboración del diagrama lógico de la red, se parte de la configuración de los aparatos propuestos en la figura 4.24. El diagrama lógico de las dos trayectorias (principal y de protección) se muestra en la figura 4.25.

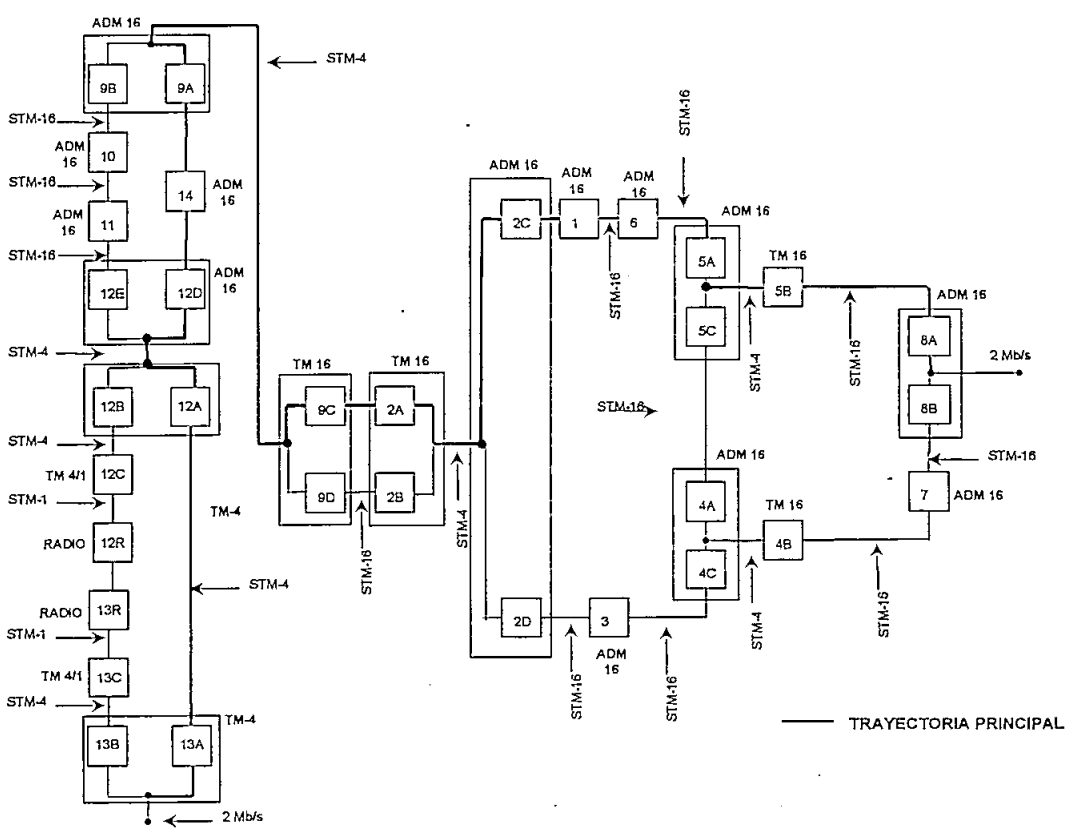


Fig. 4.25 Diagrama lógico de la red para un canal a 2 Mb/s entre los nodos 8 y 13.

Cada uno de los bloques del diagrama representa un aparato o parte de un aparato del sistema. El primer número indicado dentro de cada bloque representa el número de nodo dentro del sistema, mientras que las letras a continuación indican que más de un componente del aparato fue considerado. Los niveles de la señal considerada (2 Mb/s, STM-1, STM-4, etc.) son indicados en casi todos los puntos del diagrama. Esto es necesario para identificar el valor de MTBF a considerarse en la evaluación de los parámetros de confiabilidad.

La tabla 4.14 muestra los valores de MTBF para cada uno de los bloques del diagrama lógico de la red, además del tipo de aparato y señal involucrados. El tipo de interfaz indicado es igual para los dos sentidos de transmisión del canal.

NUMERO BLOQUE	FIGURA No.	TIPO DE APARATO	INTERFAZ	MTBF. [años]	MTBF [horas]	λ [fallas/hora]
1	4.27	ADM 16	STM-16 / STM-16	11.61	101703.60	9.83249E-06
2A	4.25	TM-16	STM-4 / STM-16	14.64	128246.40	7.79749E-06
2B	4.25	TM-16	STM-4 / STM-16	14.64	128246.40	7.79749E-06
2C	4.27	ADM 16	STM-4 / STM-16	14.64	128246.40	7.79749E-06
2D	4.25	ADM 16	STM-4 / STM-16	14.64	128246.40	7.79749E-06
2E	4.27	ADM 16	STM-16 / STM-16	11.61	101703.60	9.83249E-06
3	4.27	ADM 16	STM-16 / STM-16	11.61	101703.60	9.83249E-06
4A	4.25	ADM 16	STM-4 / STM-16	14.64	128246.40	7.79749E-06
4B	4.25	TM-16	STM-4 / STM-16	14.64	128246.40	7.79749E-06
4C	4.25	ADM 16	STM-4 / STM-16	14.64	128246.40	7.79749E-06
4D	4.27	ADM 16	STM-16 / STM-16	11.61	101703.60	9.83249E-06
5A	4.27	ADM 16	STM-4 / STM-16	14.64	128246.40	7.79749E-06
5B	4.25	TM-16	STM-4 / STM-16	14.64	128246.40	7.79749E-06
5C	4.25	ADM 16	STM-4 / STM-16	14.64	128246.40	7.79749E-06
5D	4.27	ADM 16	STM-16 / STM-16	11.61	101703.60	9.83249E-06
6	4.27	ADM 16	STM-16 / STM-16	11.61	101703.60	9.83249E-06
7	4.25	ADM 16	STM-16 / STM-16	11.61	101703.60	9.83249E-06
8A	4.25	ADM 16	2 Mbps / STM-16	18.04	158030.40	6.3279E-06
8B	4.25	ADM 16	2 Mbps / STM-16	18.04	158030.40	6.3279E-06
9A	4.25	ADM 16	STM-4 / STM-16	14.64	128246.40	7.79749E-06
9B	4.25	ADM 16	STM-4 / STM-16	14.64	128246.40	7.79749E-06
9C	4.25	TM-16	STM-4 / STM-16	14.64	128246.40	7.79749E-06
9D	4.25	TM-16	STM-4 / STM-16	14.64	128246.40	7.79749E-06
10	4.25	ADM 16	STM-16 / STM-16	11.61	101703.60	9.83249E-06
11	4.25	ADM 16	STM-16 / STM-16	11.61	101703.60	9.83249E-06
12A	4.26	TM-4	STM-4 / STM-4	19.83	173710.80	5.75669E-06
12B	4.26	TM-4	STM-4 / STM-4	19.83	173710.80	5.75669E-06
12C	4.26	TM 4/1	STM-1 / STM-4	27.75	243090.00	4.1137E-06
12D	4.25	ADM 16	STM-4 / STM-16	14.64	128246.40	7.79749E-06
12E	4.25	ADM 16	STM-4 / STM-16	14.64	128246.40	7.79749E-06
12R	4.26	RADIO	STM-1 / STM-1	30.70	268932.00	3.71841E-06
13A	4.26	TM-4	2 Mbps / STM-4	26.62	233191.20	4.28833E-06
13B	4.26	TM-4	2 Mbps / STM-4	26.62	233191.20	4.28833E-06
13C	4.26	TM 4/1	STM-1 / STM-4	27.75	243090.00	4.1137E-06
13R	4.26	RADIO	STM-1 / STM-1	30.70	268932.00	3.71841E-06
14	4.25	ADM 16	STM-16 / STM-16	11.61	101703.60	9.83249E-06

Tabla 4.14 Valores de MTBF utilizados para la evaluación de la confiabilidad de la red.

Para fines de demostración se asume que el tiempo medio de reparación MTTR de una unidad rota es constante e igual a 2 horas en todos los casos.

La figura 4.25 muestra las trayectorias disponibles para ir desde el nodo **8** al nodo **13**. Considerando nuevamente la figura 4.25, se procede con la evaluación de los parámetros de confiabilidad del enlace **12-13**. La figura 4.26 muestra la sub-red 5 y su proceso de reducción paralelo-serie, de acuerdo con las ecuaciones (4.7) a (4.10).

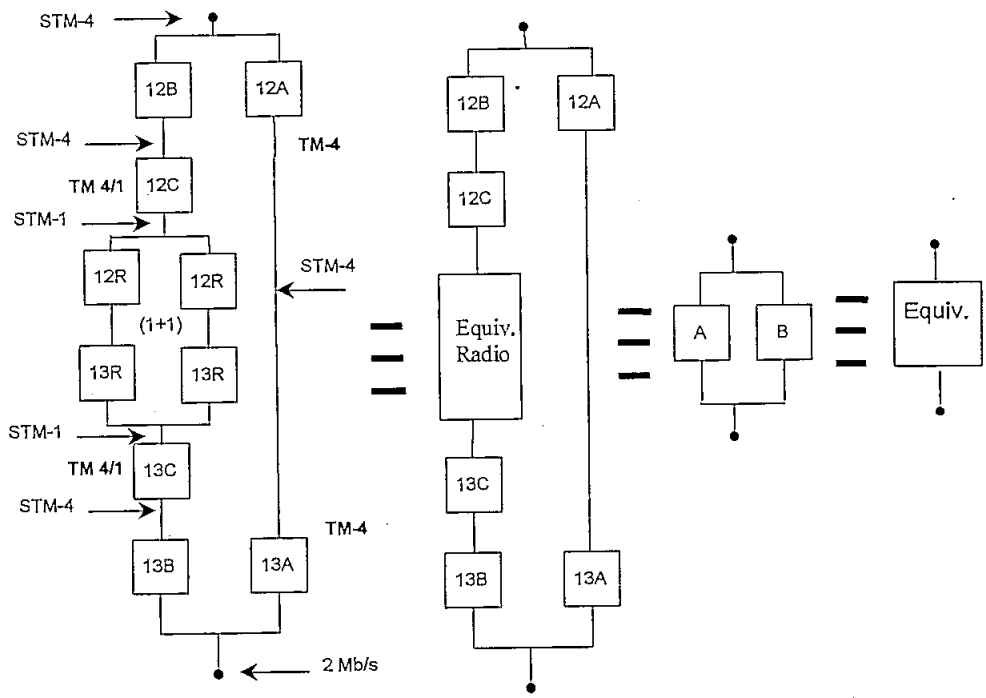


Fig. 4.26 Diagrama lógico de la sub-red 5 (enlace 12-13) y su reducción equivalente.

Para la sección de radio se tiene en realidad una configuración en n+1; sin embargo, el canal a 2 Mb/s considerado no puede ser conmutado entre los 4 flujos STM-1, sino solamente al flujo de protección. Es por esto que el bloque de radio se considera solamente como un sistema 1+1 (Ver figura 4.26).

Las tablas 4.15 a 4.19 muestran los cálculos de los parámetros de disponibilidad de las sub-redes que forman parte de la red, y la tabla 4.20 presenta los resultados de disponibilidad para la ruta entre los nodos **8** y **13** en condiciones normales de funcionamiento (es decir, si no se toma ninguna ruta de protección), así como también la disponibilidad de la ruta considerando las fallas o roturas mostradas en la figura 4.18.

SUB-RED 5 (Enlace- 12-13)							RESULTADOS	
UNIDAD	TIPO DE INTERFAZ	MTTR (τ) [horas]	μ [reparaciones/ hora]	MTBF [Años]	MTBF [horas]	λ [fallas/hora]	λ_{eq} [fallas/hora]	μ_{eq} [reparaciones hora]
Bloque radio:							2.2123E-10	0.99997025
13R	STM-1	2	0.5	30.70	268932.00	3.7184E-06		
12R	STM-1	2	0.5	30.70	268932.00	3.7184E-06		
Ruta de protección:							1.8272E-05	4.9997E-0
Radio		1.00002975	0.999970253			2.2123E-10		
13B	2Mbps / STM-4	2	0.5	26.62	233191.20	4.2883E-06		
13C	STM-4 / STM-1	2	0.5	27.75	243090.00	4.1137E-06		
12B	STM-4 / STM-4	2	0.5	19.83	173710.80	5.7567E-06		
12C	STM-4 / STM-1	2	0.5	27.75	243090.00	4.1137E-06		
Ruta principal:							1.0045E-05	4.9998E-0
13A	2Mbps / STM-4	2	0.5	26.62	233191.20	4.2883E-06		
12A	STM-4 / STM-4	2	0.5	19.83	173710.80	5.7567E-06		
Equivalente total del bloque:							7.3419E-10	0.99994639

Tabla 4.15 Cálculo de los parámetros de confiabilidad de la sub-red 5 (enlace 12-13)

Los parámetros λ y μ son calculados en base a la configuración mostrada en la figura 4.26. En primer lugar se evalúa el bloque radio, que está representado por dos ramas en paralelo. Mediante las fórmulas (4.7) a (4.10), se calcula el equivalente de este bloque. A continuación se obtiene otro diagrama serie-paralelo con dos ramas, una que constituye la ruta sin protección (representado por la ruta principal con fibra óptica) y otra ruta correspondiente a la radio. El siguiente diagrama para este bloque considera dos nuevas ramas paralelas (A y B en la figura 4.26), de las que se obtiene el equivalente de la sub-red 5 y se muestra en la última fila de la tabla 4.15.

SUB-RED 2 (Anillo 2)							RESULTADOS	
UNIDAD	TIPO DE INTERFAZ	MTTR (τ) [horas]	μ [reparaciones/ hora]	MTBF [Años]	MTBF [horas]	λ [fallas/hora]	λ_{eq} [fallas/hora]	μ_{eq} [reparaciones hora]
Ruta de protección:							3.5257E-05	4.9993E-0
12E	STM-4 / STM-16	2	0.5	14.64	128246.40	7.7975E-06		
11	STM-16 / STM-16	2	0.5	11.61	101703.60	9.8325E-06		
10	STM-16 / STM-16	2	0.5	11.61	101703.60	9.8325E-06		
9B	STM-4 / STM-16	2	0.5	14.64	128246.40	7.7975E-06		
Ruta principal:							2.5426E-05	4.9995E-0
12D	STM-4 / STM-16	2	0.5	14.64	128246.40	7.7975E-06		
14	STM-16 / STM-16	2		11.61	101703.60	9.8325E-06		
9A	STM-4 / STM-16	2	0.5	14.64	128246.40	7.7975E-06		
Equivalente total del bloque:							3.5863E-09	0.99987862

Tabla 4.16 Cálculo de los parámetros de confiabilidad de la sub-red 2 (Anillo 2).

Para la sub-red del diagrama de la figura 4.25 se obtienen dos ramas en paralelo. La rama principal se obtiene de la ruta a través de los nodos **12**, **14** y **9**,

mientras que la de protección está constituida por los nodos **12**, **11**, **10** y **9**. Finalmente, mediante el uso de las fórmulas (4.9) y (4.10) para el equivalente serie de cada rama, y con las fórmulas (4.7) y (4.8) para la combinación en paralelo, se obtiene su equivalente final.

SUB-RED 3 (Enlace 9 - 2)							RESULTADOS	
UNIDAD	TIPO DE INTERFAZ	MTTR (τ) [horas]	μ [reparaciones/ hora]	MTBF [Años]	MTBF [horas]	λ [fallas/hora]	λ_{eq} [fallas/hora]	μ_{eq} [reparacion hora]
Ruta de protección:								0.499968
9D	STM-4 / STM-16	2	0.5	14.64	128246.40	7.7975E-06	1.55945E-05	
2B	STM-4 / STM-16	2	0.5	14.64	128246.40	7.7975E-06		
Ruta principal:								0.499968
9C	STM-4 / STM-16	2	0.5	14.64	128246.40	7.7975E-06	1.55945E-05	
2A	STM-4 / STM-16	2	0.5	14.64	128246.40	7.7975E-06		
Equivalente total del bloque:							9.72814E-10	0.99993

Tabla 4.17 Cálculo de los parámetros de confiabilidad de la sub-red 3 (Enlace 9-2)

La sub-red 3 está representada por dos ramas en paralelo entre los nodos **9** y **2**. Una aplicación directa de las fórmulas (4.7) a (4.10) nos da el equivalente del bloque.

SUB-RED 1 (Anillo 1B)							RESULTADOS	
UNIDAD	TIPO DE INTERFAZ	MTTR (τ) [horas]	μ [reparaciones/ hora]	MTBF [Años]	MTBF [horas]	λ [fallas/hora]	λ_{eq} [fallas/hora]	μ_{eq} [reparacione s/hora]
Ruta de protección:							7.4579E-05	4.9985E-01
2C	STM-4 / STM-16	2	0.5	14.64	128246.40	7.7975E-06		
1	STM-16 / STM-16	2	0.5	11.61	101703.60	9.8325E-06		
2E	STM-16 / STM-16	2	0.5	11.61	101703.60	9.8325E-06		
3	STM-16 / STM-16	2	0.5	11.61	101703.60	9.8325E-06		
4D	STM-16 / STM-16	2	0.5	11.61	101703.60	9.8325E-06		
5D	STM-16 / STM-16	2	0.5	11.61	101703.60	9.8325E-06		
6	STM-16 / STM-16	2	0.5	11.61	101703.60	9.8325E-06		
5A	STM-4 / STM-16	2	0.5	14.64	128246.40	7.7975E-06		
Ruta principal:							3.5257E-05	4.9993E-01
2C	STM-4 / STM-16	2	0.5	14.64	128246.40	7.7975E-06		
1	STM-16 / STM-16	2	0.5	11.61	101703.60	9.8325E-06		
6	STM-16 / STM-16	2	0.5	11.61	101703.60	9.8325E-06		
5A	STM-4 / STM-16	2	0.5	14.64	128246.40	7.7975E-06		
Equivalente total del bloque:							1.0520E-08	0.999780314

Tabla 4.18 Cálculo de los parámetros de confiabilidad de la sub-red 1 (Anillo 1B)

En el caso de este anillo 1B, cuando ha existido una rotura en algunos de los enlaces o nodos intermedios, el verdadero recorrido de un canal entre dos nodos cualquiera es diferente a lo mostrado en la figura 4.25. Por ejemplo, la rotura del enlace **1-6** implica que el canal con tráfico debe ser re-enrutado hacia *atrás en el nodo* **1** y

atravesar (por segunda vez) el nodo **2**. Lo mismo sucede cuando el tráfico (ya re-enrutado a través de los nodos **2**, **3**, **4**, **5**) llega al nodo **6**; en este caso, el tráfico vuelve hacia atrás en el nodo **6** y atraviesa parcialmente el nodo **5** para luego ser extraído del anillo 1B. El diagrama lógico es presentado en la figura 4.27.

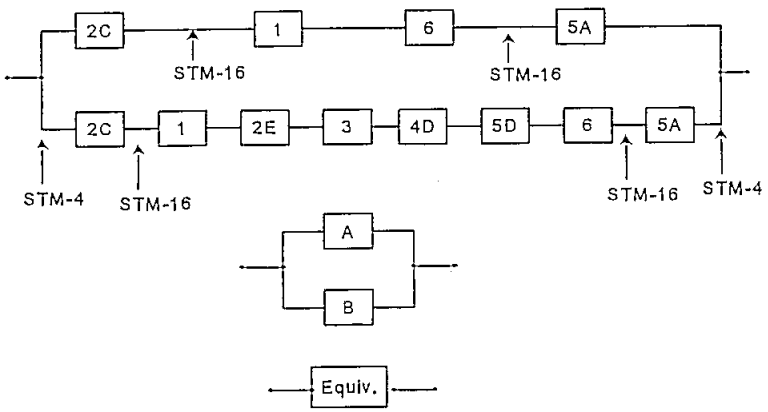


Fig. 4.27 Diagrama lógico para el recorrido dentro del anillo 1B.

Para la evaluación de los parámetros de confiabilidad λ_{eq} y μ_{eq}, se debe hacer referencia a la figura 4.27, donde se muestra el diagrama lógico en caso de la rotura del enlace **1-6.** La evaluación consiste en encontrar el equivalente serie para cada rama (A y B) mediante las ecuaciones (4.9) y (4.10), y luego proceder con el equivalente paralelo de aquellas dos ramas utilizando las ecuaciones (4.7) y (4.8). Esto nos da el equivalente total de la sub-red mostrado en la tabla 4.18 en la fila "equivalente total del bloque".

SUB-RED 4 (Area de los nodos 7 y 8)							RESULTADOS	
UNIDAD	TIPO DE INTERFAZ	MTTR (τ) [horas]	μ [reparaciones/ hora]	MTBF [Años]	MTBF [horas]	λ [fallas/hora]	λ_{eq} [fallas/hora]	μ_{eq} [reparaciones/hora]
Ruta de protección:							4.1019E-05	4.9992E-01
5C	STM-4 / STM-16	2	0.5	14.64	128246.40	7.7975E-06		
4A	STM-4 / STM-16	2	0.5	14.64	128246.40	7.7975E-06		
4B	STM-4 / STM-16	2	0.5	14.64	128246.40	7.7975E-06		
7	STM-16 / STM-16	2	0.5	11.61	101703.60	9.8325E-06		
8B	STM-4 / STM-16	2	0.5	14.64	128246.40	7.7975E-06		
Ruta principal:		2					1.7629E-05	4.9996E-01
5B	STM-4 / STM-16	2	0.5	14.64	128246.40	7.7975E-06		
8A	STM-16 / STM-16	2	0.5	11.61	101703.60	9.8325E-06		
Equivalente total del bloque:							2.8929E-09	0.999882699

Tabla 4.19 Cálculo de los parámetros de confiabilidad de la sub-red 4 (Area de los nodos 7 y 8)

Haciendo referencia a la figura 4.25, esta sub-red 4 está también constituida por dos ramas en paralelo. Una de ellas (la principal) incluye los nodos **5** y **8** directamente, mientras que la de protección está constituida por los nodos **5**, **4**, **7** y **8**. Nuevamente, las fórmulas (4.9) y (4.10) se utilizan para las ramas en serie, y su combinación en paralelo se obtiene a través de las ecuaciones (4.7) y (4.8), que da como resultado el equivalente de la sub-red.

TRAYECTORIA A TRAVES DE LA RED (Nodos 8 a 13)				RESULTADOS	
UNIDAD	MTTR (τ) [horas]	μ [reparaciones/ hora]	λ [fallas/hora]	λ_{eq} [fallas/hora]	μ_{eq} [reparaciones/ hora]
Ruta principal sin protección:					
Enlace 12-13	2.00008036	0.49997991	1.0045E-05	1.0393E-04	4.9974E-01
Anillo 2	2.00020344	0.499949146	2.5426E-05		
Enlace 9-2	2.00012477	0.499968811	1.5594E-05		
Anillo 1B	2.00028211	0.499929483	3.5257E-05		
Area 7-8	2.00014105	0.499964741	1.7629E-05		
Disponibilidad de la ruta sin protección [%]:					99.97920750
Ruta protegida:					
Enlace 12-13	1.00005361	0.999946392	7.3419E-10	1.8706E-08	9.9983E-01
Anillo 2	1.00012139	0.999878629	3.5863E-09		
Enlace 9-2	1.00006238	0.999937621	9.7281E-10		
Anillo 1B	1.00021973	0.999780314	1.0520E-08		
Area 7-8	1.00011731	0.999882699	2.8929E-09		
Disponibilidad de la ruta con protección [%]:					**99.99999813**

Tabla 4.20 Cálculo de la disponibilidad total de la trayectoria. Se considera un solo sentido de transmisión.

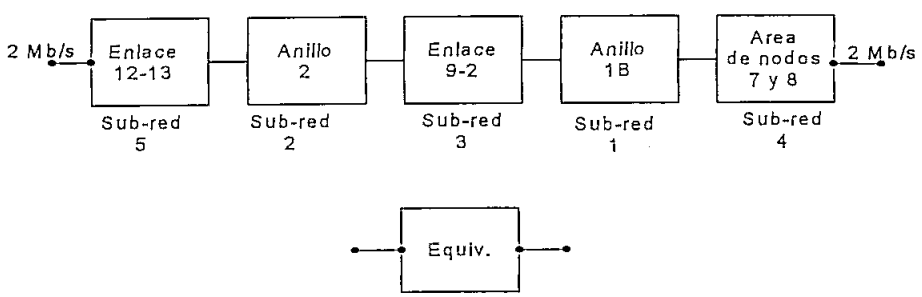


Fig. 4.28 Diagrama lógico para la trayectoria a través de toda la red.

En la tabla 4.20 se observan los resultados obtenidos para el equivalente total de la ruta entre los nodos 8 y 13. El diagrama lógico de la figura 4.28 muestra la configuración final obtenida para esta trayectoria. Los parámetros λ_{eq} y μ_{eq} de la ruta principal sin protección se obtienen de la combinación serial de todos los parámetros evaluados para cada una de las sub-redes anteriores (indicados como "ruta principal" en las tablas 4.15 a 4.19). En base a estos parámetros y mediante la ecuación (4.13) se calcula la disponibilidad para la ruta sin protección.

La ruta protegida se obtiene de la combinación serial de todos los parámetros λ_{eq} y μ_{eq} de las sub-redes (indicados como "equivalente total del bloque" en las tablas 4.15 a 4.19). Se considera el equivalente total de cada bloque porque éste ya incluye la combinación en paralelo de las dos rutas (principal y protección), bajo cuya configuración el canal de tráfico se encuentra normalmente en servicio. Con estos valores se calcula la disponibilidad de la ruta (ecuación 4.13) , que es mucho más alta que el valor obtenido para la ruta principal sin protección.

CAPITULO V

Conclusiones y recomendaciones

CONCLUSIONES Y RECOMENDACIONES

El presente trabajo ha sido elaborado con el objetivo de dar una visión global de la estructura y planificación de una red de transporte de telecomunicaciones, y está especialmente dedicado a la introducción de los diversos tipos de mecanismos de protección de redes SDH actualmente disponibles o en proceso de desarrollo, en base a normas internacionales, para su futura utilización.

La planificación de una red de transporte debe considerar en primer lugar un análisis de la red existente, con el fin de aprovechar la infraestructura y utilizarla para probables expansiones y actualización de red. Si ese no es el caso, se deberá ejecutar un nuevo y completo proceso de diseño de la red. En el presente caso, la información recopilada sobre la infraestructura de la red, consistió básicamente en la existencia de estaciones de telecomunicaciones, es decir, la disponibilidad de cabinas y salas de aparatos, torres, red de ductos en las cuales el cliente tenía algunas fibras instaladas, etc. En base a dicha información, y considerando la demanda de tráfico requerida y el tipo de mecanismo utilizado, se definió la capacidad necesaria de la red para soportar dicha demanda. Se debe notar que la red aquí propuesta corresponde a la configuración final de la red, cuando la demanda de tráfico haya alcanzado los niveles más altos como se especifica en la matriz de tráfico para el año 2005. Siendo este trabajo especialmente dedicado a la protección de la red, y no a la puesta en marcha de la misma, el proceso gradual año tras año no ha sido presentado. Sin embargo, se menciona cuales son los puntos críticos de la red y se recomienda la estrategia a seguirse a futuro para alcanzar un mejor rendimiento de la misma.

En lo que respecta a la protección, los mecanismos propuestos han sido de dos tipos: a nivel de sección múltiplex y a nivel de recorrido. Dentro del primer grupo se consideró la protección lineal para los enlaces **2-9** y **12-13** y, la protección a través de anillos de protección compartido (*SPRing*) (anillo 1 y 2). A nivel de recorrido, la protección a nivel de conexión sub-red es propuesta para los canales que llegan o provienen de la sub-red 4. Adicionalmente, con fines de demostración, se propone la protección a nivel de contenedor virtual para un grupo de canales entre los nodos **2** y **8**.

En el presente trabajo se trató de obtener los anillos 1 y 2 balanceados desde el inicio, modificando el programa "RUTAS.EXE", de modo que en caso de tener dos rutas de igual longitud entre dos nodos[1], se decida alternadamente por mantener la primera ruta o tomar la segunda. Sin embargo, debido a la poca uniformidad de las demandas de tráfico entre los nodos, los resultados no fueron satisfactorios y los anillos de todas maneras presentaron desbalances.

Los anillos de protección compartidos (*SPRing*) están limitados en lo que respecta al número de nodos que pueden ser incluidos (no más de 16 debido a las restricciones en el byte **K1**). Por otra parte, un incremento excesivo de nodos en el anillo involucra la formación de trayectorias más largas dentro del mismo, hecho que influirá en los retardos insertados por la misma fibra óptica o por los aparatos presentes en aquella trayectoria. Adicionalmente, una mayor cantidad de nodos incrementa la probabilidad de la presencia de roturas o fallas. Si existe solamente una falla en el anillo, el proceso de conmutación es ejecutado para evitar la interrupción de tráfico entre nodos, a menos que exista la rotura de uno de ellos bloqueando el acceso a aquel nodo. Si dos o más fallas ocurren simultáneamente, se produce necesariamente la segmentación del anillo en dos o más partes. Esto significa no solamente que algunos de los nodos del anillo quedan aislados, sino que éstos tampoco podrían comunicarse con otros nodos externos al anillo pero dentro de la misma red. De esto se concluye que no es conveniente tener anillos con elevado número de nodos (con el fin de tener menos riesgo de roturas o fallas) y que se debería estructurar la red en varios anillos independientes entre sí.

Como se describió al inicio de este capítulo, la configuración de red propuesta se basó principalmente en la infraestructura existente en la red del cliente. Esta red presenta un solo enlace (**2-9**) de unión entre los dos principales anillos, lo cual significa que en caso de rotura de uno de estos nodos, la red sería severamente afectada por esta segmentación. A continuación se propone una nueva configuración de red con una trayectoria adicional (un nuevo ducto por construir) entre los nodos **3** y **14** (Ver figura 5.1). Esto permite elevar el nivel de confiabilidad de la red mediante la diversidad de trayectorias disponibles entre los dos anillos principales (1 y 2).

---

[1] Ver numeral 4.3.4.3, Enrutamiento de tráfico.

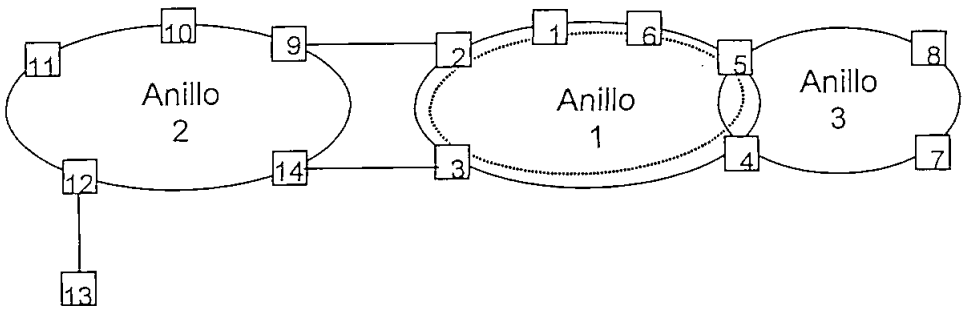


Fig. 5.1 Configuración de red con anillos adyacentes.

Adicionalmente, el anillo 3 es propuesto con el fin de proteger la sub-red 4, compartiendo dos nodos con el anillo 1 y manteniendo las dos vías de interconexión entre ellos. Este anillo permite un gran mejoramiento en la utilización de la capacidad de la red y en flexibilidad para expansiones en el futuro.

La figura 5.2 muestra la configuración del interfaz entre los anillos 1 y 2 antes mencionados. En el lado de transmisión se realiza la duplicación del canal y luego éste es enviado a través de las dos trayectorias disponibles hacia el otro anillo. Esto se realiza en cada uno de los cuatro nodos involucrados, siempre que se trate de canales cuyo tráfico deba ser enviado hacia el otro anillo. En el lado de recepción, el mejor de los dos canales recibidos es seleccionado. Esta adaptación del tráfico se realiza con el fin de garantizar la intercomunicación entre los dos anillos e incrementar la confiabilidad de la red.

Resumiendo lo anterior, la configuración propuesta en la figura 5.1 presenta las siguientes características:

Ventajas

1. Independencia entre los anillos 1 y 2 que constituyen el núcleo de la red.
2. Incremento de la confiabilidad a través de la duplicación de tráfico y la doble interconexión entre los anillos 1 y 2 (enlaces **2-9** y **3-14**).
3. Optimización de la carga en la sub-red 4 mediante el empleo de otro anillo de protección compartido (*SPRing*). Efectivamente, el anillo 3 presentaría *una carga* de

tráfico considerablemente menor que en el caso del ejemplo propuesto en el capítulo IV. Obviamente, en este caso la protección es a través del anillo y no a nivel de recorrido.

4. Uno de los sub-anillos del anillo 1 podría no considerar el tráfico hacia y desde el nodo **4**. En este caso, a diferencia del ejemplo propuesto en el capítulo IV, no se necesita de tráfico adicional entre los nodos[2] **4** y **5** (Ver figura 4.12), lo que permite la exclusión del nodo **4** en el sub-anillo. El hecho de no incluir el nodo **4**, implica una reducción en los interfaces ópticos y aparatos terminales de línea.
5. Gran flexibilidad para la inserción de nuevos nodos en cada uno de los anillos en caso de requerimientos adicionales de tráfico en el futuro.
6. Simplicidad en supervisión y manejo de la red, pues solo dos tipos de mecanismos de protección están presentes (anillos 1, 2 y 3 más la protección lineal en el enlace **12-13**).

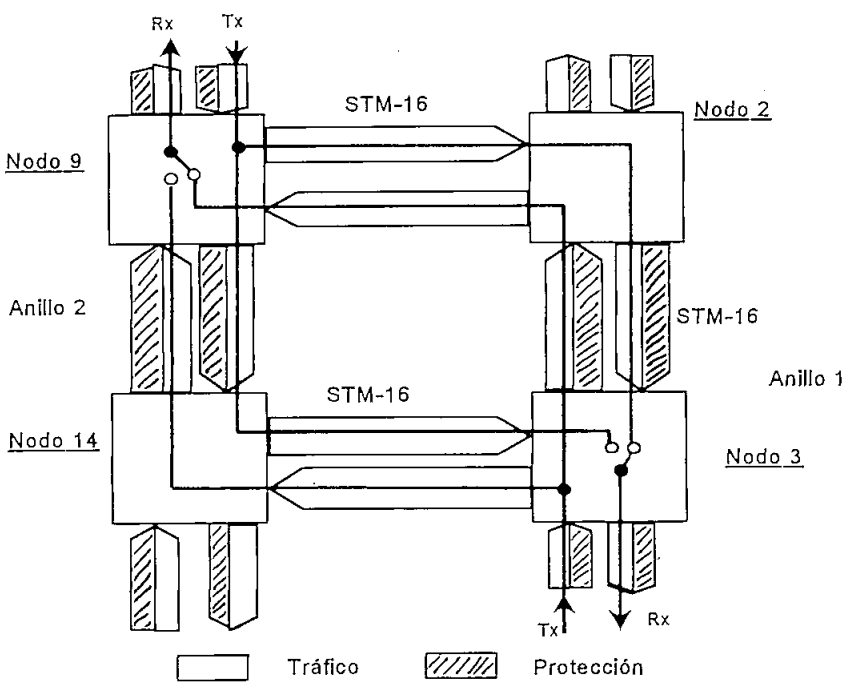


Fig. 5.2 Interfaz de conexión entre los anillos 1 y 2.

Desventajas

1. La independencia entre los anillos 1 y 3 se logra con la inclusión de 6 fibras entre los nodos **4** y **5**. Por lo tanto, el enlace **4-5** y sus respectivos nodos se convierten en puntos críticos de la red ante eventuales roturas o fallas en los mismos.
2. Mayor necesidad de aparatos de conmutación (DXC) en los nodos **2**, **3**, **9** y **14**

[2] Ver literal 4.3.4.4, Capacidad de la red, a) Anillo 1.

para la puesta en marcha de la interfaz de protección entre los anillos 1 y 2 (Ver figura 5.2).

Otra configuración alternativa de red, para el mismo caso del ejemplo, se propone en la siguiente figura:

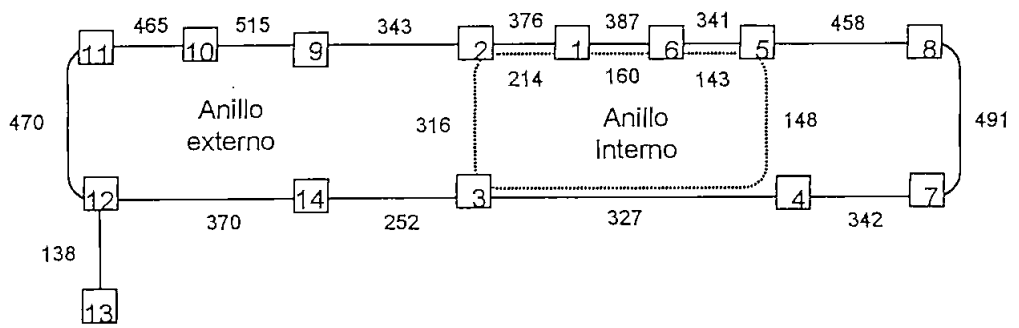


Fig. 5.3 Configuración de la red a través de anillos anidados y demanda inicial de tráfico en la red.

A través de la ejecución del programa "RUTAS.EXE" se obtiene la configuración inicial de la carga mostrada en la figura 5.3. Se consideró en primer lugar solo el tráfico entre los nodos del anillo interno y luego el tráfico del anillo externo. Nótese que el nodo **4** está excluido del anillo interno.

Adicionalmente, el anillo interno fue balanceado manualmente mediante la transferencia del tráfico entre los nodos **1** y **3** (96x2 Mb/s) desde la ruta **1, 2, 3** hacia la ruta **1, 6, 5, 3**. En el caso del anillo externo, se puede ver claramente que el enlace **9-10**

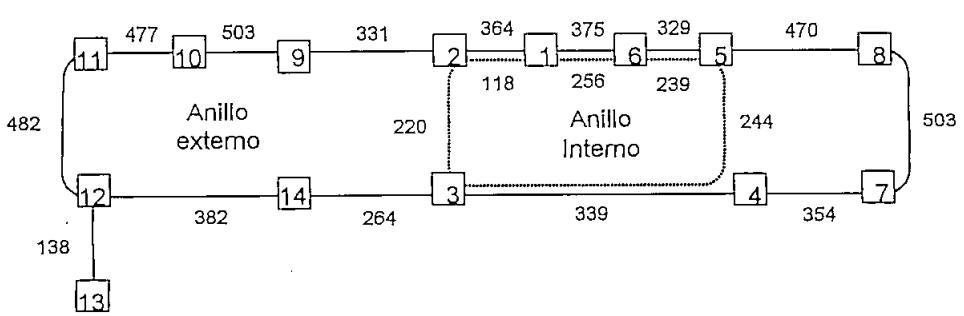


Fig. 5.4 Demanda final de tráfico en la red luego del balance de los anillos.

sobrepasa el máximo de 504x2 Mb/s para un anillo STM-16. Un total de 12x2 Mb/s entre los nodos **10** y **5** fueron transferido desde la ruta **10**, **9**, **2**, **1**, **6**, **5** hacia la ruta **10**, **11**, **12**, **14**, **3**, **4**, **7**, **8**. El resultado del balance se muestra en la figura 5.4. Los enlaces **9-10** y **7-8** tienen una carga elevada. Esta podría ser reducida mediante la desviación de algunos canales del anillo externo hacia el interno a través del enlace **2-3**.

Las características principales de esta configuración se detallan a continuación:

Ventajas

1. Utilización de casi todos los ductos existentes en la red actual, a excepción del ducto entre los nodos **3** y **14**. Esta utilización implica reducción de costos de inversión de la red.
2. Independencia entre tráfico de larga distancia (anillo externo) y tráfico regional (anillo interno). El anillo interno incluye los nodos del ex-anillo 1 (ejemplo del capítulo IV), cuya carga de tráfico es mayor al 50% de la carga total en aquel nodo.
3. El anillo interno excluye el nodo **4**; el resultado es la disminución de costos de inversión y operación de la red debido a la reducción de interfaces ópticos y aparatos terminales.
4. Simplicidad en la configuración de la red debido a la reducción del número de anillos (solamente dos) respecto a las dos configuraciones propuestas anteriormente.
5. Flexibilidad para la creación de otros anillos internos y el consecuente incremento de la capacidad de la red. Por ejemplo, utilizando ductos existentes se podría crear nuevos anillos internos con los nodos **9**, **10**, **11**, **12** y **14** o entre los nodos **2**, **9**, **10**, **11**, **12**, **14** y **3**. Adicionalmente, nuevos nodos y un anillo interno pueden ser creados en la sub-red 4 incluyendo los nodos **4**, **5**, **7** y **8**.
6. Una red con varios anillos internos como se recomienda en el numeral anterior, incrementa notablemente la robustez y por lo tanto la confiabilidad ante múltiples roturas o averías en los nodos o enlaces.
7. Optimización de la capacidad de la red requerida para la sub-red 4, si se compara con el ejemplo del capítulo IV.
8. Reducción del número de fibras utilizadas en el enlace **4-5**, si se compara con la configuración de 4 anillos anteriormente propuesta (Figura 5.1).
9. Mayor facilidad en el balance de la carga en cada anillo y en la red en general.

Desventajas

1. En la configuración mostrada en la figura 5.3 existe mayor probabilidad de roturas, y por lo tanto mayor sensibilidad ante la presencia de ellas, debido al incremento de nodos en el anillo externo.
2. Los retardos en el anillo externo deben ser cuidadosamente analizados, si la longitud total del anillo es demasiado grande.

Una atención especial merece el hecho de utilizar estrategias de enrutamiento en caso de rotura de nodos o enlaces. La estrategia aquí propuesta da como resultado una matriz con las trayectorias más cortas para ir de un nodo a otro de la red. En caso de roturas o fallas, otra ruta debe ser necesariamente elegida. En el ejemplo del capítulo IV, la nueva trayectoria es seleccionada simplemente con una conmutación hacia la otra fibra (protección lineal), conmutación del anillo o conmutación de los selectores en el lado de recepción (protección a nivel de recorrido). Podría presentarse el caso de tener una red topológicamente definida como una malla[3], donde varias trayectorias serían disponibles para la protección. El programa "RUTAS.EXE" se podría utilizar tantas veces como sea necesario, para encontrar una nueva ruta cuya distancia sea también la más corta, en caso de falla de nodos o enlaces involucrados en la ruta principal. A continuación, la trayectoria principal debe ser eliminada de la matriz original de tráfico y el programa debe ser ejecutado para encontrar una segunda ruta entre los dos nodos. Si es necesario, se elimina nuevamente esta segunda ruta de la matriz y se ejecuta el programa para obtener una tercera ruta y así sucesivamente. Al final, se tiene una tabla de rutas totalmente independientes para cada par de nodos. Cada par de nodos contará con una trayectoria principal y al menos dos rutas alternativas adicionales que serían escogidas -en orden de prioridad- cuando la trayectoria principal haya sido interrumpida o degradada. Esta información pasaría a formar parte de una base de datos del sistema de supervisión si el tipo de enrutamiento es **centralizado** o se mantendría en cada nodo si el enrutamiento es **distribuido**[4].

Otra idea factible de realizar sería la inclusión de la máxima capacidad disponible (o cierto porcentaje de ella) por enlace en la matriz de conexiones. El programa debería sumar el tráfico enrutado a través de cada enlace y comparar con el máximo valor permitido en aquel enlace. Cuando éste llega a ser superado, el valor correspondiente a

---

[3] Por ejemplo una red troncal nacional.

[4] Ver numeral 4.2.1, Introducción al re-enrutamiento.

la distancia en aquel enlace debería convertirse en "infinito" o enlace abierto. El tráfico adicional debería ser enrutado a través de otras trayectorias. El objetivo final es tener una asignación balanceada de carga en la red.

Los métodos de protección expuestos en este trabajo siguen un proceso de conmutación pre-definido (rígido) entre los terminales que lo ejecutan. Este proceso es bastante rápido (generalmente 50 ms), pues existe ya la capacidad asignada o dedicada a la protección que puede ser utilizada en caso de presencia de fallas o degradaciones. En los capítulos III y IV se vio que los mecanismos de protección necesitan el 100% de la capacidad (respecto al tráfico) para dedicarla a la protección. Actualmente, la tendencia es hacia la optimización de la utilización de esta capacidad dedicada de acuerdo con lo expuesto brevemente en el literal 4.2, sobre el enrutamiento distribuido. La protección/restablecimiento con control distribuido debería perseguir este objetivo, de tal manera que en el futuro se tendría redes con una combinación de los dos tipos de mecanismos, es decir, los mecanismos rígidos podrían compartir la capacidad de protección con los mecanismos distribuidos. Esto sería factible pues los mecanismos rígidos tienen ya la facilidad de portar tráfico adicional a través de la capacidad dedicada a la protección. Esta capacidad dedicada a la protección podría utilizarse entonces con el fin de alcanzar dos importantes objetivos en la protección a través de mecanismos de tipo distribuido: establecimiento de nuevas rutas de protección y la señalización entre los nodos para el proceso de protección/restablecimiento hacia condiciones normales de la red.

Redes con mucha más alta capacidad y elevada confiabilidad se esperan en un futuro cercano. Se anuncian redes con capacidad del orden de decenas de gigabits por segundo. Esta elevada capacidad puede ser transportada solamente a través de la fibra óptica y la multiplexación óptica que ello involucra. La tecnología ATM (*Asynchronous Transfer Mode*) está adentrándose cada vez más en las redes de comunicaciones y se debería buscar nuevos medios y protocolos de acoplamiento y protección global a nivel de estas capas de red: ATM, SDH y Capa Optica de multiplexación/transmisión. Existen algunos estudios que apuntan hacia la consecución de aquellos objetivos, como por ejemplo el proyecto PANEL (*Protection Across Network Layers*) que está siendo desarrollado por la EUROSCOM[5].

---

[5] European Institute for Research and Strategic Studies in Telecommunications.

ANEXOS

ANEXO # 1

Puntos de referencia Sn de la SEMF en los aparatos SDH

ANEXO # 1

Puntos de referencia Sn de la SEMF en los aparatos SDH[1]

Punto de referencia Sn	Status	Orden
S1 (SPI)	ALS disponible	
	ALS activo/inactivo	ALS activo/inactivo
	Salida del transmisor encendido/apagado	Salida del transmisor encendido/apagado
S2 (RST)		AIS del Tx en C
S3(MST)		AIS del Tx en D
		MS-RDI en C
S4 (SA)		AIS del Tx en F
		Tipo de multiplexor de ord. sup.
S5 (HPC)	Matriz de interconexión	Matriz de interconexión
S6 (HPT)		AIS del Tx en H
		RAI del Tx en G
	Identificador de recorrido-(J1) para Rx.	Identificador de recorrido-(J1) en G para Tx.
	Tipo señal-(C2) para Rx.	Tipo señal-(C2) en G para Tx.
		Identificador de recorrido-para Rx.
		Tipo de señal-para Rx.
		Tipo de recorrido (3,4)
S7 (HPA)		AIS de Tx en J
		Tipo de multiplex
S8 (LPC)	Matriz de interconexión	Matriz de interconexión
S9 (LPT)		AIS de Tx en L
		RAI de Tx en K
	Identificador de recorrido-(J1) para Rx.	Identificador de recorrido-(J1) en K para Tx.
	Tipo señal-(C2, V5 [b5-b7]) para Rx.	Tipo señal-(C2, V5 [b5-b7]) en K para Tx.
		Identificador de recorrido-para Rx.
		Tipo de señal-para Rx.
		Tipo de recorrido (11,12,2,3)
S10 (LPA)		AIS de Tx en M
		AIS de Tx en L
		Tipo de LPA (byte a byte, bit a bit, asinc., sinc. etc)
S11 (PI)		AIS de Tx en M.
S12 (SETPI)		AIS de Tx en T3.
S14 (MSP)		Tipo de operación.
		Comandos de conmutación.
	Estado de conmutación.	
S15 (SETS)	Estado de la entrada	
	Entrada seleccionada	Selección de la entrada
	Estado del MTG	
	MTG seleccionado	Selección de MTG
	Input fall-back order	Input fall-back order

[1] Se recomienda revisar también la recomendación G.783, Tabla 4-17, donde nuevos puntos de referencia han sido definidos.

ANEXO # 2

a) Descripción funcional de los aparatos sincrónicos a nivel de bloques.

b) Diagrama general de procesamiento de alarmas y señales en los aparatos SDH.

ANEXO # 2a

DESCRIPCION FUNCIONAL DE LOS APARATOS SINCRONICOS A NIVEL DE BLOQUES[1]

II-1 Interfaz física sincrónica (SPI)

Provee el acoplamiento entre el medio físico de transmisión y la función de RST en el punto **B**.

La señal en el punto **A** está estructurada de acuerdo con las recomendaciones G.707 y sus características físicas siguen las recomendaciones G.958 y G.703.

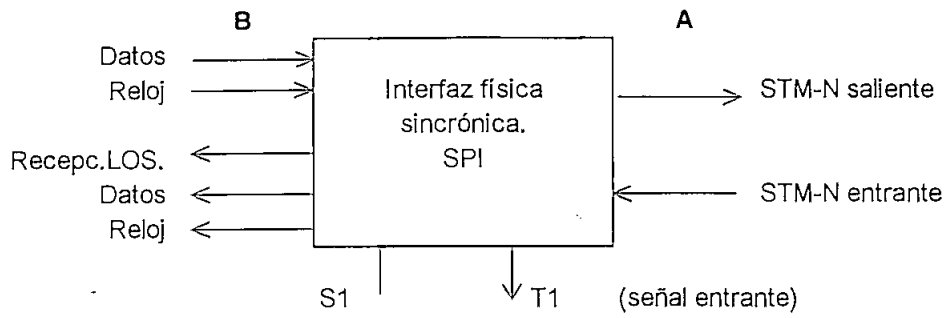


Fig. II-1 Interfaz física sincrónica.

En sentido de **B** hacia **A**, todos los parámetros de indicación de falla o degradación de la interfaz son reportados al punto **S1** (Ver figura II-1).

Desde **A** hacia **B**, la SPI regenera la señal entrante y extrae el reloj para presentarlos en **B**; la señal de reloj está disponible además en el punto **T1**. La ausencia de señal en **A** genera una indicación de **LOS** en la RST punto **B**.

II-2 Terminación de sección de regeneración (RST)

En dirección de **C** hacia **B** (Figura II-2), todos los bytes de la RSOH son generados e insertados en la trama STM-N por esta función RST. La trama STM-N es

---

[1] Este Anexo ha sido extraído del borrador de la Recomendación G.783, versión en Inglés (Draft of New Rec. G.783,

aleatorizada, a excepción de la primera fila de la RSOH (bytes **A1**, **A2**, **C1**(**J0**), y otros reservados para uso nacional) y, junto con el reloj es presentada en el punto **B**.

- El byte **B1** es calculado para todos los bytes de la última trama STM-N luego de aleatorizarla y su valor es asignado en la RSOH antes de aleatorizarla.
- El byte **C1** indicará la posición de la trama STM-1 dentro de una trama STM-N (N = 1, 4, 16,....).
- Los bytes no utilizados de la primera fila de la RSOH son asignados con el valor **10101010**.
- Si una señal todos UNOS es recibida en **C**, la indicación de **MS-AIS** se presentará en el punto **B**.

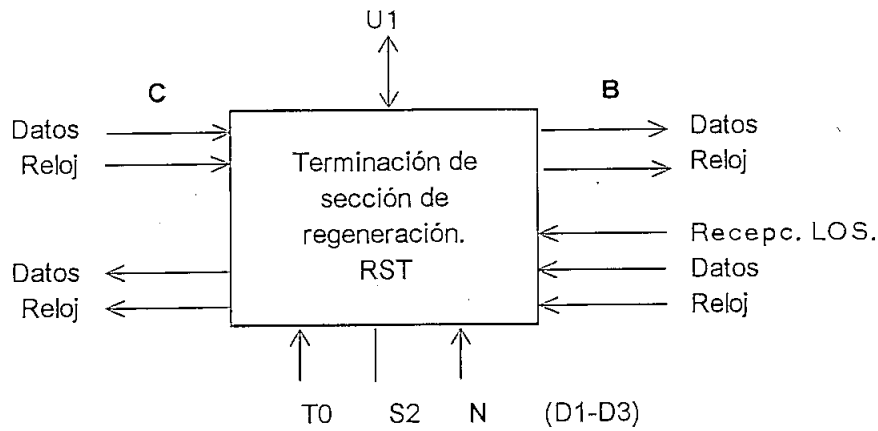


Fig. II-2 Terminación de sección de regeneración RST.

La trama STM-N entrante en **B** es desaleatorizada (a excepción de la primera fila de la RSOH) y es presentada junto con el reloj en el punto **C**.

- La alineación de trama es verificada mediante el control de los bytes **A1 y A2**. En el caso de que una condición de fuera de trama (**OOF**) sea detectada y se mantenga por un tiempo mayor a 3 ms. (no confirmado todavía), una indicación de pérdida de trama (**LOF**) será declarada. Tanto **OOF** como **LOF** serán reportadas en **S2** de la SEMF.
- El byte **B1** es extraído de la RSOH luego de la desaleatorización y comparado con el valor calculado (**BIP-8N**) para todos los bits de la anterior trama antes de desaleatorizarla. La presencia de errores es reportada en **S2**, así como también el valor del número de errores contenido en **B1**.

Geneve, July, 1994).

- Si **LOS** o **LOF** son detectadas en **B**, una señal de todos UNOS será enviada al punto **C** (MST).

II-3 Terminación de la sección múltiplex (MST)

En el sentido de **D** hacia **C** (Figura II-3) se encarga de la generación de los bytes de la MSOH y del monitoreo de los flujos STM-N.

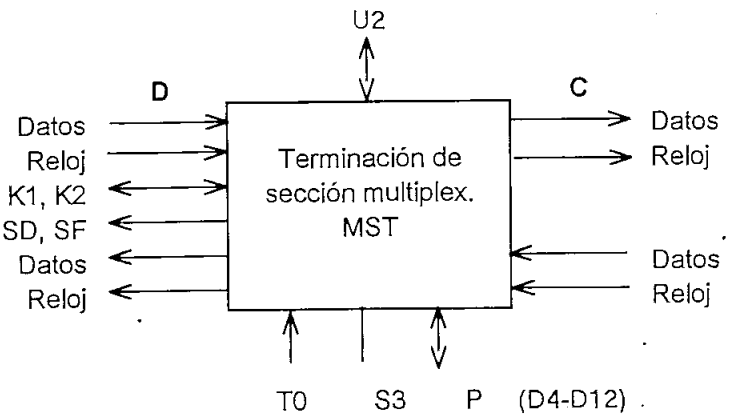


Fig. II-3 Terminación de la sección múltiplex MST.

- El monitoreo de errores se realiza mediante el control de paridad par (**BIP-24N** bits) de todos los bytes de la anterior trama STM-N, a excepción de los bytes de la RSOH y su resultado es almacenado en los Nx3x**B2** bytes de la actual trama STM-N.
- La protección mediante conmutación automática se realiza a través de los bytes **K1** y **K2** de la MSOH (Ver sección 3.1.1 para mayor detalles).
- Si una señal de todos UNOS está presente en **D**, una indicación de **AIS** de recorrido de la unidad administrativa (**AU *Path* AIS**) será enviada hacia la señal de salida en el punto **C**.
- De igual manera, una indicación de señal con falla (**SF**) en el punto **D**, generará una indicación de defecto en la sección múltiplex remota (**MS-RDI**) en la señal de salida en el punto **C** (bits 6 a 8 de **K2** contendrán el valor **110**).

En el sentido de **C** hacia **D**, los bytes **B2** son extraídos de la MSOH y comparados con el valor calculado mediante **BIP-24N** de la anterior trama recibida. Los errores son reportados en **S3** para ser procesadas por la SEMF.

- Los bytes **B2** sirven también para la detección de errores excesivos (**MS-EXC**) y señales degradadas (**MS-SD**), cuya definición se detalla a *continuación:*

1. Asumiendo que la red sigue una distribución de errores de *Poisson*, se considera que existe error excesivo (**MS-EXC**) si el BER es mayor a 10^{-3}.
2. Para una red con distribución de errores de *Poisson* de tipo ráfaga, existe una degradación de señal (**MS-DEG**) si el BER es mayor a un cierto valor predefinido de 10^{-x} donde x puede tomar valores entre 5 y 9.

- Los tiempos máximos de detección de niveles de errores para una sección múltiplex se indican en la tabla siguiente:

BER	Tiempo máximo de detección.
>= 10 E-03	10 ms
10 E-04	100 ms
10 E-05	1 s
10 E-06	10 s
10 E-07	100 s
10 E-08	1000 s
10 E-09	10000 s

Tabla II-1 Tiempos máximos de detección de la calidad de una sección múltiplex.

- La detección de **MS-AIS** o errores excesivos (**MS-EXC**) en **C** genera el envío de todos UNOS (**AIS**) en la señal de datos (punto **D**) y la indicación de señal con falla (**SF**) en el mismo punto (**D**). Esta generación e indicación se producirá en los siguientes 250 μs luego de haberse detectado la **MS-AIS** o **MS-EXC**.
- La detección de **MS-DEG** genera una indicación de **SD** en el punto **D** dentro de los siguientes 250 μs luego de haber sido detectada.

II-4 Protección de la sección múltiplex (MSP)

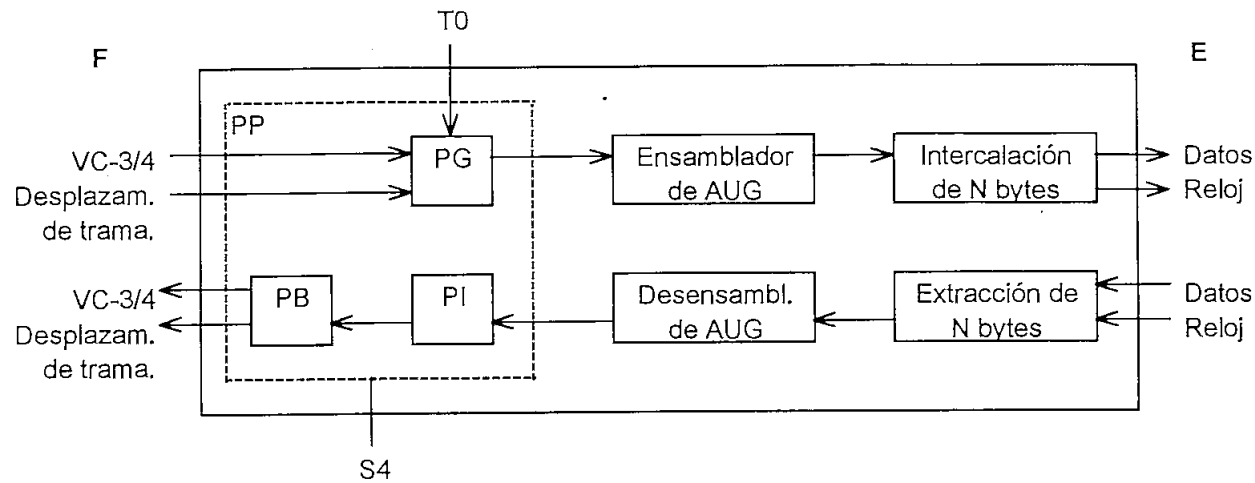
Es la parte encargada de la protección de la porción de red comprendida entre dos terminaciones de sección múltiplex. La sección 3.2 presenta en detalle el proceso de protección y las diferentes maneras de proteger una sección múltiplex. Esta función es una de las más importantes dentro del desarrollo y consecución de los objetivos del presente trabajo.

II-5 Adaptación de la sección múltiplex (MSA)

En el sentido de **F** hacia **E** (Ver figura II-4) tiene como función tomar los contenedores virtuales de orden superior (VC-3, VC-4) y componer las AU que forman

las AU de grupo. Estas a su vez formarán las tramas STM-N en el punto **E**.

- El desplazamiento de trama sirve para la generación del puntero de la AU por parte del módulo generador de puntero (PG).
- Las tramas STM-N en el punto **E** tienen como referencia de tiempo la señal del punto **T0**.
- La detección de una señal todos UNOS en **F** (pérdida de puntero), genera una indicación de **AIS** para el recorrido de la AU en el punto **E**.



PB: Buffer del puntero.
PG: Generador del puntero.
PI: Intérprete del puntero.
PP: Procesador de puntero.

Fig. II-4 Función de adaptación de sección.

Desde **E** hacia **F** los STM-N entrantes son descompuestos en contenedores virtuales VC-3 /4 de acuerdo con la información proporcionada por los punteros de la AU.

- El procesador de puntero es una especie de *buffer* de datos cuya información es escrita a la velocidad de reloj del VC recibido, y se lee con el reloj de referencia del punto T0. Es aquí donde, dependiendo de las velocidades de estos relojes de lectura/escritura, se produce la justificación positiva o negativa.
- Si **LOP** o **AIS** de recorrido de AU son detectados, una señal de todos UNOS es presentada en el punto **F**. Estas alarmas son reportadas al punto **S4**.

II-6 Función HSU (*High Order Supervisory-unequipped*)

Es muy frecuente tener en redes SDH que no toda la capacidad de los flujos

STM-N ha sido utilizada. Sin embargo, estos vacíos de información necesitan ser controlados, supervisados y principalmente dotados de una "terminación" apropiada dentro de la red. La recientemente incorporada función de supervisión de flujos no utilizados (HSU) trata de cumplir con este objetivo, para lo cual está dividida en dos partes:

1. **Función de generación (HSUG-n):** Genera un VC-n con carga indefinida pero con un POH válido en el punto F. Algunas características importantes son:
   - El byte **C2** es definido como no equipado.
   - Los bytes **J1** y **G1** son insertados en el POH.
   - Cálculo de errores mediante **BIP-8** cuyo resultado es insertado en la siguiente trama.
2. **Función de monitoreo (HSUM-n):** Encargada de la recolección de alarmas y detección de la calidad del POH de orden superior no utilizado. Esta función siempre espera recibir una señal de no equipado (**C2** = **00**H) en el POH recibido.

   - Los bytes **J1**, **G1** y **C2** son extraídos del POH y enviados al punto **S16**.
   - El byte **B3** es extraído del POH. El control de errores mediante **BIP-8** es realizado para la presente trama y su resultado será comparado con el contenido del byte **B3** de la siguiente trama. Los errores son reportados al punto **S16**.

II-7 Función de monitoreo del POH de orden superior (HPOM)

Es una función dependiente de los requerimientos de la SEMF ya sea como estado activo o inactivo.

- En estado activo permite el monitoreo del POH (con carga válida o indefinida) a través del punto **S20**, que la conecta hacia la SEMF, cumpliendo las mismas funciones que HSUM.
- En estado inactivo no se realiza ningún monitoreo del POH.

II-8 Conexión de recorridos de orden superior (HPC-n)

Permite la interconexión de flujos a nivel VC-3/4 desde **F** hacia **G** o viceversa. Puede ser interpretada como una matriz de conmutación configurable de acuerdo a varios requerimientos. El tipo de configuración depende del tipo de multiplexor utilizado (terminal, de inserción/extracción y de *cross-connection* como se vio en la sección

1.2.1). El punto **S5** sirve para la configuración de la matriz y reporte del estatus de la misma, cuando así lo requiera la SEMF.

II-9 Terminación de recorridos de orden superior (HPT-n)

Se encarga de la inserción y extracción del POH en los contenedores virtuales VC-3/4.

En el sentido de **H** hacia **G** (Ver figura II-5) se inserta toda la información relativa a la identificación (**J1**), tipo de información (**C2**) y calidad (**G1**).

- Se evalúan los errores mediante **BIP-8** y su valor es almacenado en **B3**.
- Un indicador de multitrama es insertado en **H4**.
- Byte **K3** es insertado para la protección del recorrido.
- La presencia de una señal todos UNOS, **HP-TIM** (pérdida del identificador de recorrido **J1**), **HP-EXC** (errores excesivos) o **HP-UNEQ** (no equipado) en la señal de datos recibida en el punto **G**, genera una indicación de **HP-RDI** que deberá ser insertada y enviada en **G1** dentro de las dos siguientes tramas.

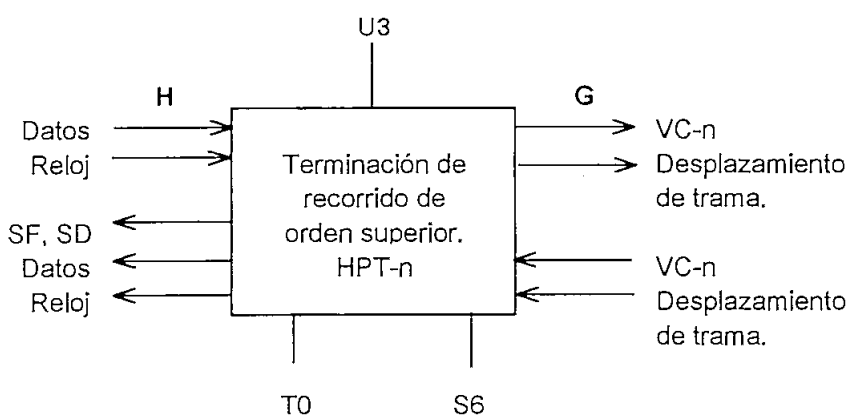


Fig. II-5 Terminación de recorrido de Orden superior HPT-n.

Desde **G** hacia **H** se realiza la extracción de los bytes del POH para ser procesados.

- **G1** (bits 1 a 5) es extraído del POH. Una indicación de **REI** o **RDI** es reportada al punto **S6** para conocimiento de la SEMF.
- **H4** da la indicación del número de trama STM-1 dentro de una multitrama. En caso de recibir una secuencia incorrecta varias veces (varía de 2 a 10), una indicación de pérdida de multitrama (**LOM**) será reportada al punto **S6**.
- **B3** es extraído del POH. Se realiza el cálculo de errores mediante **BIP-8** cuyo

resultado será comparado con el byte **B3** de la anterior trama. Los errores serán reportados en **S6** para ser procesados por la SEMF. El byte **B3** también es utilizado en el monitoreo de errores de la siguiente manera:

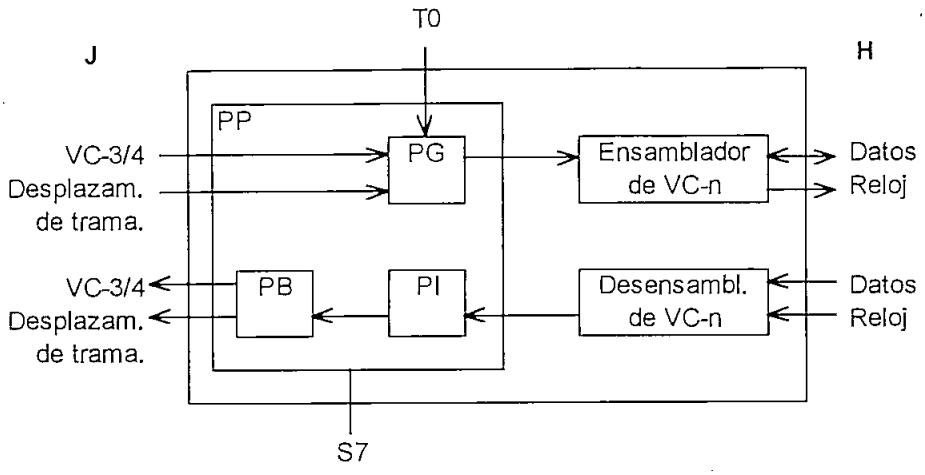
1. Asumiendo que la red sigue una distribución de errores de *Poisson*, se considera que existe error excesivo (**HP-EXC**) si el BER es mayor a 10^{-3}.
2. Para una red con distribución de errores de *Poisson* de tipo ráfaga, existe una degradación de señal (**HP-DEG**) si el BER es mayor a un cierto valor predefinido de 10^{-x} donde x puede tomar valores entre 5 y 9.
3. Los tiempos máximos de detección se muestran en la tabla II-1.

- La presencia de un VC no utilizado (**HP-UNEQ**), pérdida del identificador de recorrido (dado por **J1** y llamado **HP-TIM**) o de errores excesivos (**HP-EXC**) genera la presencia de todos UNOS en la señal de datos en el punto **H** (en dirección a HPA) dentro de los siguientes 250 μs.
- Una señal todos UNOS, **HP-UNEQ**, **HP-TIM**, **HP-EXC** en el punto **G** genera el envío de señal con falla (**SF**) en el punto **H** dentro de los 250 μs siguientes a la detección de las alarmas.
- La detección de **HP-DEG** genera la indicación de señal degradada (**SD**) en **H** dentro de las dos siguientes tramas (250 μs).

II-10 Adaptación de recorridos de orden superior (HPA-m/n)

Esta función se encarga de la generación e interpretación del puntero y del proceso de justificación de la Unidad Tributaria (TU).

En el sentido de **J** hacia **H** (Figura II-6), esta función ensambla los VC-m (m=1, 2 o 3) para formar la TU que será incorporada en los VC-n (n=3 o 4). El desplazamiento de la trama del VC-m respecto del VC-n está dado por el puntero de la Unidad Tributaria (TU).



PB: Buffer del puntero.
PG: Generador del puntero.
PI: Intérprete del puntero.
PP: Procesador de puntero.

Fig. II-6 Función de adaptación de recorrido de orden superior.

Desde **H** hacia **J**, el VC-n entrante se descompone en varios VC-m cuyos punteros de la TU contienen la dirección de inicio de cada VC de orden inferior respecto al VC de orden superior del cual provienen.

- Como en el caso de la adaptación de sección (SA), la HPA-m/n desarrolla el proceso de justificación de acuerdo a la diferencia en frecuencia de los VC de orden superior e inferior para lo cual hace uso de un *buffer* donde se escribe y lee la información de los VC desensamblados. Todos los eventos de justificación son reportados a **S7** para ser procesados por la SEMF.
- Cuando los contenedores son distribuidos en varias tramas (multitrama), la recepción incorrecta del byte H4 durante un cierto número de veces que varía de 2 a 10, genera la alarma de pérdida de multitrama (**LOM**), que será reportada en el punto **S7**.
- La detección de alarmas como pérdida del puntero (**LOP**) o de **AIS** de unidad tributaria, genera una señal de todos UNOS en el punto **J**, además de ser reportadas al punto **S7**.

II-11 Función LSU (*Low Order Supervisory-Unequipped*)

Cumple funciones análogas a la función HSU y está dividida en:

1. **Función de generación (LSUG-m):** Cumple funciones análogas a *HSUG-n* pero

para contenedores virtuales de orden inferior. Es oportuno notar que en este caso VC-3 puede ser considerado de orden inferior.

- Generación de **C2** para VC-3 y bits 5 a 7 del byte **V5** para VC-1/2.
- Se realiza la inserción de **J1**, **G1** para VC-3 y de **V5**, **J2** para VC-1/2.
- Cálculo de errores mediante **BIP-8** para VC-3 y **BIP-2** para VC-1/2. Su resultado es insertado en la siguiente trama.

2. **Función de monitoreo (LSUM-m):** En el caso de un contenedor virtual VC-3 (como VC de orden inferior), las funciones realizadas son idénticas a las desarrolladas por HSUM-n para contenedores VC-4 y VC-3:

- Los bytes **J1**, **G1** y **C2** son extraídos del POH y enviados al punto **S17**.
- El byte **B3** es extraído del POH. El control de errores mediante **BIP-8** es realizado para la presente trama y su resultado será comparado con el contenido del byte **B3** de la siguiente trama. Los errores son reportados al punto **S17**.

Para contenedores virtuales VC-1/2, el byte **V5** es recuperado del POH con la correspondiente información de estatus (bits 3 a 8) y calidad de la señal contenida (bits 1 y 2). Toda esta información pasa a la SEMF a través del punto **S17**.

II-12 Función de monitoreo del POH de orden inferior (LPOM)

En estado activo cumple las mismas funciones que HPOM para los VC de orden superior. En estado inactivo su función es transparente.

II-13 Conexión de recorrido de orden inferior (LPC-m)

Cumple una función análoga a HPC pero para VC1/2. El punto de referencia **S8** sirve para la configuración de la matriz de conmutación y reporte del estatus del aparato de multiplexación.

II-14 Función de terminación de recorridos de orden inferior (LPT-m)

La función LPT-m toma el contenedor y su respectivo desplazamiento respecto a la referencia **T0** para crear el contenedor virtual añadiendo el POH. En sentido contrario permite la extracción de los atributos del POH (bytes para detección de errores,

indicación de alarmas, tipo de carga por recibir, etc.).

Desde **L** hacia **K** (Ver figura II-7), la información contenida en **S9** es insertada en los bits 5, 6, 7 del byte **V5**. **BIP-2** es calculado en **L** para la trama anterior y el resultado insertado en bits 1 y 2 de **V5**. En caso de una indicación de **REI**, el bit 3 de **V5** presentará el valor de **1** en la siguiente trama. La presencia de una señal todos UNOS, **LP-TIM**, **LP-EXC** o **LP-UNEQ** en el punto **K** generará una indicación remota de defecto (**LP-RDI**) que será enviada en el bit 8 de **V5** dentro de las dos tramas siguientes.

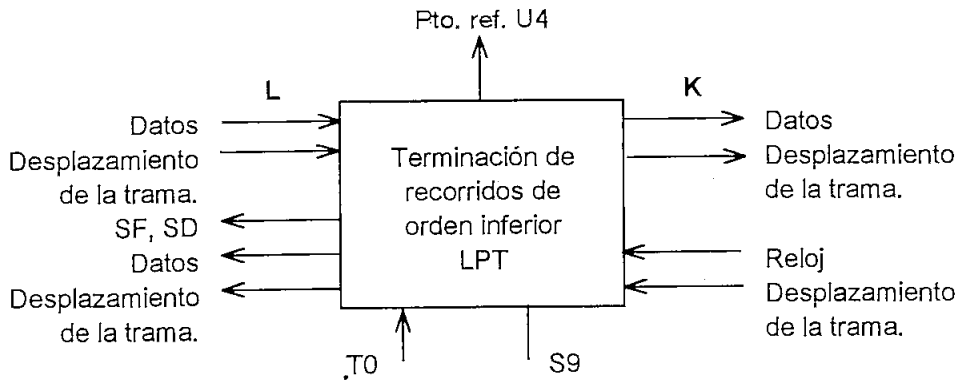


Fig. II-7 Función de terminación para recorridos de orden inferior LPT-m.

Cuando la señal recibida en el punto **K** contiene una indicación de **AIS**, ésta será presentada en el punto **S9** y una señal de todos UNOS se presentará en el punto **L**. Además, el bit 8 de **V5** tomará el valor de **1** para indicar una **LP-RDI** que será transmitida de regreso. Los bits 5 a 7 (tipo de señal, ver tabla 1.3), son reportados en el punto **S9**; mientras tanto, los bits 1 y 2 son extraídos en **K** y comparados con el valor de la trama anterior. El número de errores (máximo 2) será reportado en **S9**. Bit 3 (**REI**) es extraído y reportado en **S9**. Bit 4 pasa a la OHA (Acceso al *overhead*) y es también reportado en **S9**; esto solamente sucede si existe una aplicación que requiera su utilización, en caso contrario es ignorado.

De manera análoga a la función HPT-n, los bits 1 y 2 de **V5** se utilizan para la detección de calidad de la señal de la siguiente manera:

1. Asumiendo que la red sigue una distribución de errores de *Poisson*, se considera que existe error excesivo (**LP-EXC**) si el BER es mayor a 10^{-3}.
2. Para una red con distribución de errores de *Poisson* de tipo ráfaga, existe una

degradación de señal (**LP-DEG**) si el BER es mayor a un cierto valor predefinido de 10^{-x}, donde x puede tomar valores entre 5 y 9.

3. Los tiempos máximos de detección se muestran en la tabla II-2.

BER	Tiempo de detección
>= 10 E-03	40 ms
10 E-04	400 ms
10 E-05	4 s
10 E-06	40 s
10 E-07	400 s
10 E-08	4000 s

Tabla II-2 Tiempo máximo de detección para VC-1/2.

- La presencia de un VC no utilizado (**LP-UNEQ**), pérdida del identificador de recorrido (dado por **J2** y llamado **LP-TIM**) o de errores excesivos (**LP-EXC**) genera la presencia de todos UNOS en la señal de datos en el punto **L** (en dirección a LPA) dentro de 1 ms.
- Una señal todos UNOS, **LP-UNEQ**, **LP-TIM**, **LP-EXC** en el punto **K** genera el envío de señal con falla (**SF**) en el punto **L** dentro del primer milisegundo después de la detección de las alarmas.
- La detección de **LP-DEG** genera la indicación de señal degradada (**SD**) en **L** dentro de 1 ms.

II-15 Función de adaptación para recorridos de orden inferior (LPA-m)

Prepara las señales PDH (G.703) para su inserción en la red sincrónica. LPA-n realiza el mapeo de señales G.703 en contenedores de orden superior (C-3 y C-4) mientras que LPA-m mapea señales G.703 en contenedores de orden inferior (C-11, C-12, C-2 y C-3). En el caso del mapeo de señales asincrónicas, el proceso de justificación a nivel de bits está siempre involucrado.

La figura II-8 muestra la presencia, en los puntos **L** o **H**, del desplazamiento de la trama del contenedor respecto al punto de referencia T0.

En sentido contrario (de **L** o **H** hacia **M**) la trama del contenedor es recibida junto con su respectivo desplazamiento y a partir de éstos se extrae la señal plesiócrona y el

reloj presentados en el punto **M**. Cuando una **AIS** de recorrido es detectada en **S10**, se genera una **AIS** de acuerdo con las recomendaciones G.700.

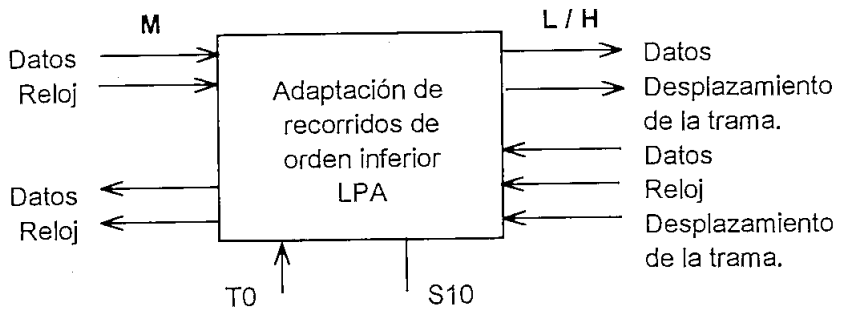


Fig. II-8 Función de adaptación para recorridos de orden inferior LPA-m.

II-16 Interfaz física plesiócrona (PPI)

Realiza el acoplamiento entre la señal física entrante o saliente (de acuerdo a las recomendaciones G.703 y G.704) y el aparato multiplexor SDH.

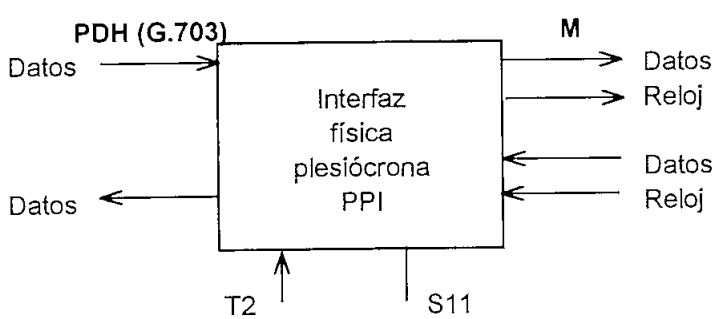


Fig. II-9 Interfaz física plesiócrona.

En el sentido que va desde el tributario de entrada hacia el punto de referencia **M** (Figura II-9), se encarga de la extracción del reloj, regeneración de los datos y decodificación de la señal de entrada. El punto **T2** puede ser utilizado también como reloj de referencia para la SETS. En caso de pérdida de señal en el tributario de entrada (**LOS**), una señal de **AIS** (todos unos) será presentada en el punto **M** y **LOS** reportada en el punto **S11**.

Desde **M** hacia el tributario saliente se encarga tomar la señal y el reloj recibidos

en el punto **M** y codificar la señal para enviarla al tributario saliente.

II-17 Función de administración de equipos sincrónicos (SEMF)

Esta función se encarga de la administración y control de los elementos de red (NE)[2] a través de los diversos puntos S existentes en cada uno de los bloques funcionales de los equipos sincrónicos. La estructura funcional se muestra en la figura II-10.

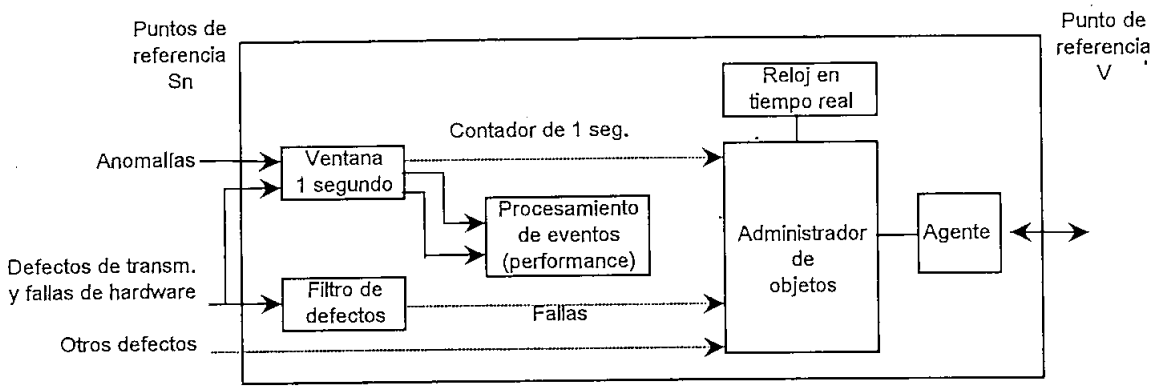


Fig. II-10 Función SEMF[3].

1. **Ventana de un segundo:** Reporta las anomalías hacia el bloque administrador de objetos en intervalos de 1 segundo. Las principales anomalías reportadas son:

   - Errores de la sección de regenerador (**B1**).
   - Fuera de trama de la sección de regenerador (**OOF**).
   - Errores de la sección múltiplex (**B2**).
   - Errores en el recorrido (**B3** y **V5**).
   - Errores (**REI**) en el recorrido de orden superior (**G1**).
   - Errores (**REI**) en el recorrido de orden inferior (**G1** y **V5**).
   - Eventos de justificación.

2. **Filtro de defectos:** Controla la situación de los defectos reportados a través de **Sn**. Las principales indicaciones disponibles en su salida son:

---

[2] Ver recomendación ITU-T M.3010 que trata sobre el sistema de administración y mantenimiento de la red (TMN).

[3] Una descripción detallada de los puntos de referencia Sn de la función SEMF se encuentra en el Anexo # 1.

- Pérdida de señal.
- Pérdida de trama.
- Pérdida del puntero de la AU.
- Pérdida del puntero de la TU.
- **AIS** de la sección múltiplex.
- **AIS** de la AU.
- **AIS** de la TU.
- Falla de recepción (**SF**) en la sección múltiplex.
- **RFI** para recorridos de orden superior e inferior, etc.

3. **Procesamiento de eventos:** Procesa toda la información disponible en la ventana de 1 segundo para el conteo de segundos con errores (**ES**), segundos con errores severos (**SES**) y errores de bloque de fondo (**BBE**).

II-18 Acceso a la sección de *overhead*

Permite acceder a todos aquellos bytes no involucrados en la SEMF. Su completa definición está aún siendo objeto de estudio.

Una de sus principales aplicaciones es el acceso a los bytes **Ei** (canales de voz) o llamados EOW que sirven para la comunicación entre estaciones terminales o de regeneración. Su punto de comunicación con SEMF está referido como **S13**.

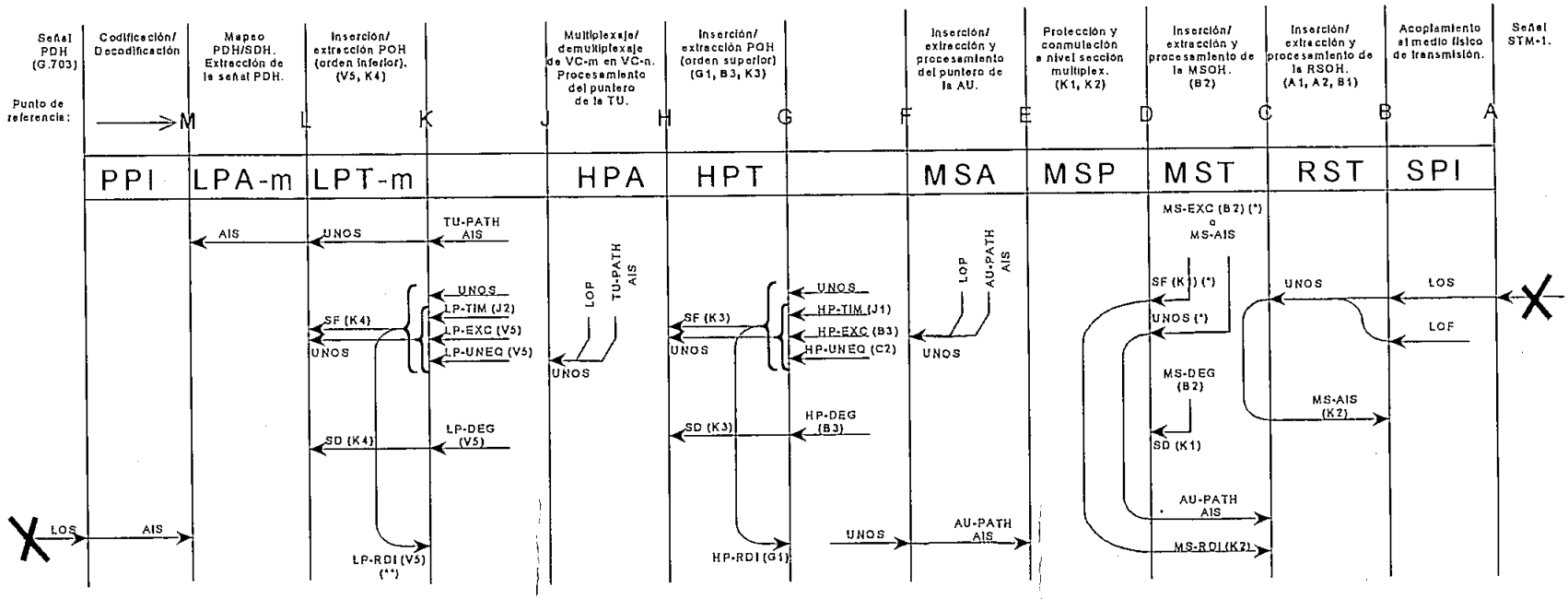
II-19 Fuente de temporización (SETS) e interfaz física (SETPI)

La figura 1.24 muestra el punto **T0** de SETS utilizado para la señal de temporización aplicada a los diversos bloques funcionales del aparato sincrónico. Básicamente la SETS está estructurada por un oscilador interno y una función de generación de temporización. Eventualmente, dos fuentes externas de temporización adicionales (**T1** y **T2**) pueden ser utilizadas como referencia.

Una salida adicional de temporización puede obtenerse del punto **Y** con el fin de sincronizar otros aparatos físicamente cercanos. Para esto, la SETPI realiza la tarea de codificación de la señal y su acoplamiento al medio físico externo. En sentido contrario, la SETPI decodifica la señal de sincronización externa a 2048 KHz definida en la recomendación G.703.

ANEXO # 2b

Diagrama general de procesamiento de alarmas y señales en los aparatos SDH



(*): Las alarmas resultantes de MS-EXC (en este caso SF y UNOS) pueden ser desactivadas.

(**): La generación de esta alarma (LP-RDI) puede ser desactivada.

ANEXO # 3

"RUTAS.EXE"

Programa para el enrutamiento inicial y cálculo de la carga de tráfico en la red

Anexo # 3

"RUTAS.EXE"

Programa para el enrutamiento inicial y cálculo de la carga de tráfico en la red

Introducción

Este programa ha sido elaborado en lenguaje C, considerando la teoría del algoritmo de Floyd-Warshall expuesta en el capítulo IV (sección 4.2.2). Se trata básicamente de un programa sencillo por su estructura y se limita a encontrar las rutas más cortas entre dos nodos cualquiera de la red. Adicionalmente, el programa se basa en las rutas más cortas encontradas, para evaluar la demanda total de tráfico que soporta cada uno de los enlaces de la red.

Estructura

En el texto del programa que se adjunta, se distinguen los siguientes bloques:

1. **Entrada de datos**: Lee los datos de entrada tanto para la distancia entre nodos de la red, como para la demanda de tráfico requerida entre todos los nodos.
2. **Lazo principal**: Se encarga de la búsqueda de las rutas más cortas entre todos los nodos de la red.
3. **Carga de tráfico**: Toma cada una de las rutas encontradas por el lazo principal y evalúa la demanda total de tráfico en cada uno de los enlaces.
4. **Presentación de resultados**: Muestra los resultados de la matriz de distancias obtenida, la demanda de tráfico en cada enlace y la matriz de las trayectorias más cortas entre dos nodos cualquiera de la red.

Definición de variables

Nombre	Tipo	Significado
i, j, k	entera	Contadores de lazo.
n	entera	Numero total de nodos de la red.
distaux	real	Distancia auxiliar (utilizada temporalmente para comparación).

entra	caracter	Entrada de datos para la distancia entre nodos. Toma valores caracter ("**I**" o "**i**" en caso de nodos no adyacentes) o valores reales luego de su conversión de caracter a real.
dist[ ][ ]	real	Matriz de distancias entre nodos.
cap[ ][ ]	entera	Matriz de tráfico entre nodos. Su contenido final será la carga total de tráfico en cada enlace de la red.
capx[ ][ ]	entera	Matriz auxiliar para evaluar la carga de tráfico en los enlaces.
preced[ ][ ]	entera	Matriz de trayectorias entre los nodos de la red. Su contenido final será la secuencia de todos los nodos intermedios involucrados en las trayectorias más cortas cuyas longitudes están dadas por **dist**[ ][ ].

Instrucciones para su utilización

1. Ingresar **n**, número de nodos de la red.
2. A partir de la configuración de la red, ingresar el valor de distancia[1]. Ingresar el valor real de distancia si los nodos son adyacentes, o la letra "**i**" (mayúscula o minúscula) para indicar una distancia "infinita" cuando los dos nodos no tienen conexión directa[2]. Solo se necesita ingresar los valores en una dirección. El programa asigna el mismo valor en sentido contrario para cada enlace.
3. Ingresar los valores de demanda de tráfico para cada par de nodos de la red. Solo se necesita ingresar los valores en un sentido, al igual que en el caso anterior.
4. El programa muestra un menú de aplicaciones que permite visualizar una de las siguientes opciones:
   a) Presione "**D**" para visualizar la Matriz de Distancias.
   b) Presione "**C**" para la Matrix de Carga de Tráfico.
   c) Presiones "**T**" para la Matriz de Trayectorias.
   d) Presione "**S**" para salir.

---

[1] Esta distancia puede ser asociada a la probabilidad (o prioridad) de utilización, al costo de operación o al retardo en cada enlace. Esto depende de los criterios de minimización a utilizarse para la planificación de la red.

[2] Estos datos forman parte de lo que se conoce también con el nombre de Matriz de Conexiones de la red (Ver ejemplo del capítulo IV).

Comentarios

1. Todas las matrices de datos consideran un máximo de 50 nodos en la red.
2. Se recomienda ingresar los datos cuidadosamente. No existe un control automático de entrada de datos. Es decir, variables numéricas o de tipo caracter pueden ser ingresadas erróneamente y sin advertencia alguna por parte del programa.

Listado del programa

```
#include <stdio.h>
#include <stdlib.h>
#include <math.h>
#include <string.h>

#define INF 99999.0

void main()

{


int n,q;
int i,j,k;
float distaux=INF;
char entra[13];
int respuesta;

double dist[50][50];
int cap[50][50];
int capx[50][50];
int preced[50][50];



printf("\n NUMERO DE NODOS DE LA RED: ");
scanf("%d",&n);

/* ************* INICIALIZACION DE MATRICES ***************/
for(i=0;i<n;i++) {
      for(j=0;j<n;j++) {
            dist[i][j]=0.0;
            cap[i][j]=0;
            capx[i][j]=0;
            preced[i][j]=0;
            }
      }
```

```
/* ENTRADA DE DATOS - DISTANCIA ENTRE NODOS ADYACENTES */
for(i=0;i<n;i++) {
      for(j=0;j<n;j++) {
            if(j > i) {
                  printf("\n distancia del nodo [%d] al
                  [%d]:",i+1,j+1);
                  scanf("%s",entra);
                  if(strcmp(entra,"i")==0 || strcmp(entra,"I")==0){
                        preced[i][j]=INF;
                        preced[j][i]=preced[i][j];
                        dist[i][j]=INF;
                        }
                  else {
                        dist[i][j]=atof(entra);
                        preced[i][j]=i+1;
                        preced[j][i]=j+1;
                        }
                  dist[j][i]=dist[i][j];
                  }
            }
      }

/* ENTRADA DE DATOS - TRAFICO ENTRE NODOS */
for(i=0;i<n;i++) {
      for(j=0;j<n;j++) {
            if(j > i) {
                  printf("\n tráfico del nodo [%d] al
                  [%d]:",i+1,j+1);
                  scanf("%d",&capx[i][j]);
                  capx[j][i]=capx[i][j];
                  }
            }
      }


/* ********************   LAZO PRINCIPAL   ********************* */
for(k=0;k<n;k++) {
      for(i=0;i<n;i++) {
            if((dist[i][k] != INF)) {
                  for(j=0;j<n;j++) {
                        distaux=dist[i][k]+dist[k][j];
                        if(distaux < dist[i][j]) {
                              dist[i][j]=distaux;
                              preced[i][j]=preced[k][j];
                              }
                        }
                  }
            }
      }

/* ********************    FIN LAZO PRINCIPAL   ***************** */
```

```
/* ************** CALCULO DE TRAFICO PARA CADA ENLACE ******** */
for(i=0;i<n;i++) {
      for(j=n-1;j>=0;j--) {
         if(j > i) {
         q=preced[i][j]-1;
         cap[q][j]=cap[q][j]+capx[i][j];
         while(q != i) {
         cap[preced[i][q]-1][q]=cap[preced[i][q]-1][q]+capx[i][j];
         q=preced[i][q]-1;
         }
         }
      }
}
/* ********* Suma total de capacidades por enlace ********** */
for(i=0;i<n;i++) {
      for(j=0;j<n;j++) {
            if(j > i) {
                  cap[i][j]=cap[i][j]+cap[j][i];
                  cap[j][i]=0;
                  }
            }
      }

/* **********************   RESULTADOS     ******************** */

system("cls");
do {
      if (respuesta == 'd'|| respuesta == 'D') {
      system("cls");
      printf("\n DISTANCIAS ENTRE NODOS DE LA RED:\n\n");
      printf("\t");
      for(i=0;i<n;i++)
      printf("N_%2d ",i+1);
      for(i=0;i<n;i++) {
      printf("\nN_ %2d ",i+1);
                  for(j=0;j<n;j++)
                  printf("%4d ",int(dist[i][j]));
                  }
      }
      if (respuesta == 'C'|| respuesta == 'c') {
      system("cls");
      printf("\n TRAFICO TOTAL EN LOS ENLACES DE LA RED:\n\n");
      printf("\t");
      for(i=0;i<n;i++)
      printf("N_%2d ",i+1);
      for(i=0;i<n;i++) {
      printf("\nN_ %2d ",i+1);
            for(j=0;j<n;j++)
            printf("%4d ",cap[i][j]);
            }
      }
      if(respuesta == 't'|| respuesta == 'T') {
      system("cls");
      printf("\n TRAYECTORIAS MINIMAS ENTRE NODOS DE LA
RED:\n\n");
      printf("\t");
      for(i=0;i<n;i++)
      printf("N_%2d ",i+1);
```

```
        for(i=0;i<n;i++) {
        printf("\nN_%2d ",i+1);
              for(j=0;j<n;j++)
              printf("%4d ",preced[i][j]);
              }
        }
        printf("\nMenú de resultados:\n");
        printf("[D]: Matriz de Distancias [C]: Carga de Tráfico [T]:
        Trayectorias:");
        printf(" [S]: Salir ");
        respuesta=getchar();
        system("cls");
        } while (respuesta != 's' && respuesta != 'S');

  exit(0);
  }
```

ANEXO # 4

Lista de abreviaturas utilizadas

Anexo # 4

Lista de abreviaturas utilizadas

Abrev.	Significado
ADM	Add Drop Multiplexer – Multiplexor de inserción y extracción.
AIS	Alarm Indication Signal – Señal de indicación de alarma.
AP	Acces Point - Punto de acceso.
APS	Automatic Protection Switching - Proceso de conmutación automatica.
ATM	Asyncronous Transfer Mode - Modo de transferencia asincrónica.
AU	Administrative Unit - Unidad administrativa.
AU-AIS	Administrative Unit Alarm Indication Signal - Señal de indicación de alarma para la unidad administrativa.
AUG	Administrative Unit Group - Grupo de unidades administrativas.
AU-LOP	Administrative Unit Loss of Pointer - Pérdida de puntero de la unidad administrativa.
AU-n	Unidad administrativa de nivel n.
AUOH	Administrative Unit Overhead - Overhead de la unidad administrativa.
BBE	Background Block Errores - Errores de bloque de fondo.
BIP-n	Bit Interleaved Parity for n bits - Paridad par en grupos de n bits.
CP	Connection Point – Punto de conexión.
DNR	Do Not Revert - Acuse de recibo no requerido.
DPRing	Dedicated Protection Ring - Anillo de protección dedicado.
DXC	Digital Cross Connect – Aparato de conmutación e interconexión.
EOW	Engineering Order Wire – Canal de comunicación de servicio de la red.
ES	Errored Seconds – Segundos con errores.
ETSI	European Teleacommunication Standardization Institute - Instituto europeo para la estandarización de las telecomunicaciónes.
EXER-R	Exercise for Ring – Condición de ejercicio (pruebas) en el anillo.
EXER-S	Exercise for Span – Condición de ejercicio (pruebas) en el enlace.
FDDI	Fiber Distribuited Data Interface - Interfaz de datos para fibra distribuida.
FS-P	Forced Switching from Protection to Working Channel - Conmutación forzada hacia el canal principal.
FS-R	Forced Switching for Ring - Conmutación de anillo forzada.
FS-S	Forced Switching for Span - Conmutación de enlace forzada.
FS-W	Forced Switching from Working to Protection Channel - Conmutación forzada hacia el canal de protección.
FS-W	Forced Switching of Working Channel to Protection - *Conmutación* manual

hacia el canal de protección.

HCS High Order Connection Supervisión – Supervisión de conexiones de orden superior.

HOA High Order Adaptation – Adaptación de orden superior.

HOI High Order Interface – Interfaz de orden superior.

HPA High Order Path Adaptation – Adaptación de recorrido de orden superior.

HPC High Order Path Connection – Conexión de recorridos de orden superior.

HP-DEG High Order Path Signal Degradation - Degradación de la señal a nivel de recorrido de orden superior.

HP-EXC High Order Path Excesive Errors - Indicación de errores excesivos en el recorrido de orden superior.

HPOM High Order Path Overhead Monitoring - Monitoreo del overhead de recorrido de orden superior.

HP-RDI Low Order Path Remote Defect Indication - Indicación de defecto remoto a nivel de recorrido de orden superior.

HP-SSF High Order Path Server Signal Failure - Señal con falla a nivel de servidor del recorrido de orden superior..

HPT High Order Path Termination - Terminación de recorrido de orden superior.

HP-TIM High Order Path Identification Mistmatch - Pérdida del identificador del recorrido de orden superior.

HP-UNEQ High Order Path Unequipped - Defecto en el recorrido de orden superior no equipado.

HSUG High Order Supervisory Unequipped Generator - Generador de la función de supervisión de VC de orden superior no equipado.

HSUM High Order Supervisory Unequipped Monitor - Monitoreo de la función de supervisión de VC de orden superior no equipado.

ITU International Telecommunications Union - Union internacional de telecomunicaciones.

LCS Low Order Connection supervisión - Supervisión de conexiones de orden inferior.

LOF Loss Of Frama - Pérdida de trama.

LOI Low Order Interface - Interfaz de orden inferior.

LOM Loss of Multiframe - Pérdida de la alineación de multitrama.

LOS Loss Of Signal - Pérdida de señal.

LPA Low Order Path Adaptation - Adaptación de recorrido de orden inferior.

LPC	Low Order Path Connection - Conexión de recorrido de orden inferior.
LPC	Low Order Path Connection - Conexión de recorridos de orden inferior.
LP-DEG	Low Order Path Signal Degradation - Degradación de la señal a nivel de recorrido de orden inferior.
LP-EXC	Low Order Path Excesive Errors - Indicación de errores excesivos en el recorrido de orden inferior.
LPOM	Low Order Path Overhead Monitoring - Monitoreo del overhead de recorrido de orden inferior.
LP-RDI	Low Order Path Remote Defect Indication – Indicación de defecto remoto a nivel de recorrido de orden inferior.
LP-S	Locked Protection for Span - Protección de enlace bloqueada.
LP-SSF	Low Order Path Server Signal Failure - Señal con falla a nivel de servidor del recorrido de orden inferior.
LPT	Low Order Path Termination - Terminación de recorrido de orden inferior.
LP-TIM	Low Order Path Identification Mistmatch – Pérdida del identificador del recorrido de orden inferior.
LP-UNEQ	Low Order Path Unequipped - Defecto en el recorrido de orden inferior no equipado.
LSUG	Low Order Supervisory Unequipped Generator – Generador de la función de supervisión de VC de orden inferior no equipado.
LSUM	Low Order Supervisory Unequipped Monitor – Monitoreo de la función de supervisión de VC de orden inferior no equipado.
MAN	Metropolitan Area Network - Red a nivel de area metropolitana.
MC	Matrix Connection - Conexión de matriz.
MCF	Management Communication Function - Función de comunicación del sistema de administración.
MRT	Mean Response Time - Tiempo medio requerido para proveer una unidad reparada (o de repuesto)
MS- REI	Multiplex Section Remote Error Indication – Indicación de error remoto a nivel de sección múltiplex.
MSA	Multiplex Section Adaptation - Adaptación a nivel de sección múltiplex.
MS-AIS	Multiplex Section Alarm Indication Signal - Señal de indicación de alarma a nivel de sección múltiplex.
MS-DEG	Multiplex Section Signal Degradation – Degradación de la señal a nivel de sección múltiplex.
MS-EXC	Multiplex Section Excesive Errors - Indicación de errores excesivos en la

sección múltiplex.

MSOH Multiplex Section Overhead - Overhead de sección múltiplex.

MSP Multiplex Section Protection - Protección a nivel de sección múltiplex.

MS-P Manual Switching from Protection to Working Channel - Conmutación manual hacia el canal principal.

MSPA Multiplex Section Protection Adaptation – Adaptación de la protección de la sección múltiplex.

MSPT Multiplex Section Protection Termination – Terminación de la protección de la sección múltiplex.

MS-R Manual Switch for Ring - Conmutación manual en el anillo.

MS-RDI Multiplex Section Remote Defect Indication – Indicación de defecto remoto a nivel de sección múltiplex.

MSRT Mean Restauration Time - tiempo medio para restaurar el servicio.

MS-S Manual Switch for Span - Conmutación manual en el enlace.

MS-SD Multiplex Section Signal Degradation – Degradación de la señal a nivel de sección múltiplex.

MS-SF Multiplex Section Signal Failure - Falla de la señal a nivel de sección múltiplex.

MST Multiplex Section Termination - Terminación de sección múltiplex.

MS-W Manual Switching from Working to Protection Channel - Conmutación manual hacia el canal de protección.

MS-W Manual Switching of Working Channel to Protection - Conmutación manual hacia el canal de protección.

MTBF Mean Time Between Failures - Tiempo medio entre ocurrencia de fallas

MTG Multiplexer Timing Generator – Generador de temporización del multiplexor.

MTTR Mean Time To restore - Tiempo medio para reparar una unidad.

NR No Request - Ninguna petición.

OHA Overhead Access Function - Función de acceso al overhead.

OOF Out Of Frame - Indicación de fuera de trama.

PDH Plesiochronous Digital Hierarchy - Jerarquía digital plesiócrona.

POH Path Overhead - Overhead de recorrido.

PPI Plesiochronous Physical Interface - Interfaz física plesiócrona.

RDI Remote Defect Indication - Indicación de defecto en el terminal remoto.

RDSI Red digital de servicios integrados.

REI Remote Error Indication - Indicación de error en el terminal remoto.

RFI	Remote Failure Indication - Indicación de falla remota.
RR-R	Revert Request for Ring - Acuse de recibo de petición para el anillo.
RR-S	Revert Request for Span - Acuse de recibo de petición para el enlace.
RSOH	Regeneration Section Overhead - Overhead de sección de regeneración.
RST	Regeneration Section Termination - Terminación de sección de regeneración.
SA	Section Adaptation - Adaptación de sección.
SD	Signal Degradation - Degradación de la señal.
SDH	Synchronous Digital Hierarchy - Jerarquía digital sincrónica.
SD-P	Signal Degradation on Protection - Señal degradada en la protección.
SD-R	Signal Degradation on the Ring - Señal degradada en el anillo.
SD-S	Signal Degradation on the Span - Señal degradada en el enlace.
SEMF	Synchronous Equipment Managenement Function - Función de administración de equipo sincrónico.
SES	Severely Errored Seconds - Segundos con errores severos.
SETPI	Synchronous Equipment Timing Physical Interface - Interfaz física de temporización de aparatos sincrónicos.
SETS	Synchronous Equipment Timing Source - Fuente de temporización de aparatos sincrónicos.
SF	Signal Failure - Falla de la señal.
SF-R	Signal Failure onthe Ring - Señal con falla en el anillo.
SF-S	Signal Failure onthe Span - Señal con falla en el enlace.
SMA	Synchronous Multiplexer Add/Drop - Equivale a ADM
SNC-P	Sub-Network Connection Protection - Protección a nivel de conexión de sub-red.
SOH	Section Overhead - Overhead de Sección.
SPI	Synchronous Physical Interface - Interfaz física sincrónica.
SPRing	Shared Protection Ring - Anillo de protección compartido
SSF	Server Signal Failure - Señal con falla a nivel de servidor.
STM	Synchronous Transport Module - Modulo de transporte sincrónico
STM-N	Synchronous Transport Module (level N) – Modulo de transporte sincrónico de nivel N.
TCP	Termination Connection Point - Punto de conexión terminal.
TMN	Telecommunications Management Network – Red de administración de telecomunicaciónes.
TT	Trail Termination – Terminación de pista (trayectoria).

TTF	Transport Terminal Function - Función terminal de transporte.
TU	Tributary Unit - Unidad tributaria.
TU-AIS	Tributary Unit Alarm Indication signal - Señal de indicación de alarma de la unidad tributaria.
TUG	Tributary Unit Group - Grupo de unidades tributarias.
TU-LOP	Tributary Unit Loss of Pointer - Pérdida de puntero de la unidad tributaria.
VC	Virtual Container - Contenedor virtual.
VC-n	Contenedor virtual de orden n.
WTR	Wait to Restore - En espera antes de restablecer.

BIBLIOGRAFIA

BIBLIOGRAFIA

1. ANGUS John, On computing MTBF for a k-out of-n: Repairable System, IEEE Transactions on Reliability, Vol.37, No.3, August, 1988.
2. BANDA Hugo, Programming in C, University of Dundee, 1991.
3. CELCOM (Cellular Communications Network), SDH Transportation Trunk, Kuala Lumpur, 1997.
4. ENDRENYI J., Reliability Modelling in Electrical Power Systems, John Wiley & Sons, New York, 1978.
5. ETSI, DTR/TM-3025 Transmission and Multiplexing (TM) SDH Network Protection Schemes: Types and Characteristics, Sophia Antipolis Cedex-France, September, 1995.
6. ETSI, DTR/TM-03041 Transmission and Multiplexing (TM) SDH Network Protection Interworking, Sophia Antipolis Cedex-France, September, 1995.
7. ETSI, DTR/TM-03042 Transmission and Multiplexing (TM) SDH Network Protection Schemes, Automatic Protection Switch Protocols and Operation, Sophia Antipolis Cedex-France, December, 1996.
8. FLOOD J. E., Telecommunications Switching, Traffic and Networks, Prentice Hall, First edition, Cambridge, 1995.
9. ITU-T, Rec. G.701 Vocabulary of Digital Transmission and Multiplexing, and Pulse Code Modulation (PCM) Terms, Geneve, March, 1993.
10. ITU-T, Rec. G.703 Physical/Electrical Characteristics of Hierarchical Digital Interfaces, Geneve, April, 1991.
11. ITU-T, Rec. G.707 Network Node Interface for the Synchronous Digital Hierarchy (SDH) (Includes the previous G.707, G.708 & G.709), Geneve, March, 1996.
12. ITU-T, Rec. G.780 Vocabulary of Terms for Synchronous Digital Hierarchy (SDH) Networks and Equipment, Geneve, November, 1994.
13. ITU-T, Rec. G.782 Types and General Characteristics of Synchronous Digital Hierarchy (SDH) Equipment, Geneve, January, 1994.
14. ITU-T, Rec. G.783 Characteristics of Synchronous Digital Hierarchy (SDH) Functional Blocks, Geneve, January, 1994.

15. ITU-T, Draft of New Rec. G.783 Characteristics of Synchronous Digital Hierarchy (SDH) Functional Blocks, Geneve, July, 1994.

16. ITU-T, Rec. G.803 Architecture of Transport Networks Based on the Synchronous Digital Hierarchy (SDH), Geneve, March, 1993.

17. ITU-T, Rec. G.831 Management Capability of Transport Networks Based On Synchronous Digital Hierarchy (SDH), Geneve, August, 1996.

18. ITU-T, Rec. G.841 Types and Characteristics of SDH Network Protection Architectures, Geneve, July, 1995.

19. ITU-T, Rec. G.957 Optical Interfaces for Equipment and Systems Relating to the Synchronous Digital Hierarchy, Geneve, July, 1995.

20. ITU-T, Rec. G.958 Digital Line System based on the Synchronous Digital Hierarchy for Use on Optical Fibre Cables, Geneve, November, 1994.

21. KERSHENBAUM Aaron, Telecommunications Network Design Algorithms, McGraw Hill, Singapore, 1993.

22. MANCINI Cossimo, SDH Multiplexing Concepts, Siemens Telecomunicazioni S.p.A., First edition, Milan, 1994.

23. MODARRES M., A Method of Predicting Availability Characteristics of Series–Parallel Systems, IEEE, Transactions On Reliability, Vol. R-33, No. 4, October, 1984.

24. POH Soon Cherng, Comparison of Bidirectional and Unidirectional SDH Rings, Northern Telecom, The Hague, 1991.

25. SIEMENS AG, Network Planning Basic Concepts, Munich, May, 1996.

26. SIEMENS AG, Computer Based Training: Introduction SDH, Siemens Training Center, Munich, 1997.

27. SIP (Societa' Italiana per l'Esercizio delle Telecomunicazioni S.p.a.), La Gerarchia Numerica Sincrona di Multiplazione, Milano, Giugno, 1992.

28. SPRAGINS John D., Telecommunications Protocols and Design, Addison-Wesley, New York, 1994.

29. TANENBAUM Andrew S., Computer Networks, Prentice Hall, Second edition, Singapore, 1988.

30. VIDAL Arnoldo, Diseño de un sistema de fibra óptica de alta capacidad a 565 Mb/s entre las ciudades de Quito y Guayaquil, Tesis de Grado E.P.N., Quito, Abril, 1994.