

**Reemplazada por una versión más reciente**



UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

**UIT-T**

**G.841**

SECTOR DE NORMALIZACIÓN  
DE LAS TELECOMUNICACIONES  
DE LA UIT

(07/95)

## **REDES DIGITALES**

---

# **TIPOS Y CARACTERÍSTICAS DE LAS ARQUITECTURAS DE PROTECCIÓN PARA REDES DE LA JERARQUÍA DIGITAL SÍNCRONA**

**Recomendación UIT-T G.841**

Reemplazada por una versión más reciente

(Anteriormente «Recomendación del CCITT»)

---

# **Reemplazada por una versión más reciente**

## **PREFACIO**

El UIT-T (Sector de Normalización de las Telecomunicaciones) es un órgano permanente de la Unión Internacional de Telecomunicaciones (UIT). Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Conferencia Mundial de Normalización de las Telecomunicaciones (CMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución N.º 1 de la CMNT (Helsinki, 1 al 12 de marzo de 1993).

La Recomendación UIT-T G.841 ha sido preparada por la Comisión de Estudio 15 del UIT-T y fue aprobada por el procedimiento de la Resolución N.º 1 de la CMNT el 10 de julio de 1995.

---

## **NOTA**

En esta Recomendación, la expresión «Administración» se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

# Reemplazada por una versión más reciente

## ÍNDICE

	<i>Página</i>
1 Alcance .....	1
2 Referencias .....	1
3 Términos y definiciones .....	1
4 Abreviaturas .....	7
5 Clasificaciones de la protección .....	8
6 Consideraciones relativas a las aplicaciones .....	17
6.1 Anillos de protección compartida de sección de multiplexación .....	17
6.2 Anillos de protección compartida de sección de multiplexación (aplicación transoceánica).....	17
6.3 Anillos de protección especializada de sección de multiplexación.....	17
6.4 Comutación de extremo único y de extremo doble .....	20
6.5 Protección de camino de contenedor virtual lineal .....	20
6.6 Protección de conexión de subred.....	20
6.7 Protección de sección de multiplexación lineal .....	20
7 Protección de camino SDH.....	21
7.1 Protección de sección de multiplexación lineal .....	21
7.2 Anillos de protección compartida de sección de multiplexación .....	21
7.2.1 Arquitectura de la aplicación.....	21
7.2.2 Objetivos de red .....	21
7.2.3 Arquitectura de la aplicación.....	25
7.2.4 Criterios para la iniciación de la comutación .....	31
7.2.5 Protocolo de comutación de protección .....	33
7.2.6 Funcionamiento del algoritmo de protección.....	35
7.2.7 Ejemplos.....	46
7.3 Anillos de protección especializada de MS.....	46
7.4 Protección de camino de VC lineal .....	46
7.4.1 Arquitectura de red.....	46
7.4.2 Objetivos de red .....	46
7.4.3 Arquitectura de aplicación.....	47
7.4.4 Criterios de iniciación de la comutación .....	50
7.4.5 Protocolo de comutación de protección .....	55
7.4.6 Funcionamiento del algoritmo de protección.....	55
8 Protección de conexión de subred de SDH .....	56
8.1 Arquitectura de red.....	56
8.2 Objetivos de red .....	56
8.3 Arquitectura de aplicación .....	57
8.3.1 Encaminamiento .....	57
8.3.2 Protección de extremo único 1 + 1 .....	58
8.3.3 Otras arquitecturas.....	58
8.4 Criterios para la iniciación de la comutación .....	58
8.4.1 Protección de extremo único 1 + 1 .....	58
8.4.2 Otras arquitecturas.....	62
8.5 Protocolo de comutación de protección .....	63
8.5.1 Protección de extremo único 1 + 1 .....	63
8.5.2 Otras arquitecturas.....	63
8.6 Funcionamiento del algoritmo de protección.....	63
8.6.1 Algoritmo de protección de extremo único 1 + 1 .....	63
8.6.2 Otras arquitecturas.....	63

# Reemplazada por una versión más reciente

	<i>Página</i>
Anexo A – Anillos de protección compartida de MS (aplicación transoceánica) .....	64
A.1    Aplicación .....	64
A.2    Objetivos de red .....	64
A.3    Arquitectura de aplicación .....	66
A.4    Criterios de conmutación .....	66
A.5    Protocolo de conmutación de protección .....	67
A.6    Funcionamiento del algoritmo de protección.....	67
Apéndice I – Ejemplos de conmutación de protección en un anillo de protección compartida de MS .....	69
I.1    Fallo de señal unidireccional (tramo) en un anillo de cuatro fibras .....	69
I.2    Fallo de señal unidireccional (anillo) .....	72
I.3    Fallo de señal bidireccional (anillo).....	72
I.4    Degrado de señal unidireccional (anillo).....	73
I.5    Fallo de nodo.....	73
I.6    SF-R unidireccional que desplaza con prioridad a una SD-S unidireccional en tramos no adyacentes .....	81
I.7    SF-S unidireccional que desplaza con prioridad a un SF-R unidireccional en tramos adyacentes ...	84
I.8    SF-R unidireccional que desplaza con prioridad a una SD-S unidireccional en tramos adyacentes.	86
I.9    SF-R unidireccional que coexiste con un SF-R unidireccional en tramos no adyacentes.....	89

# **Reemplazada por una versión más reciente**

## **RESUMEN**

Esta Recomendación proporciona las especificaciones necesarias en materia de equipos para implementar diferentes tipos de arquitecturas de protección para redes de la jerarquía digital síncrona (SDH, *synchronous digital hierarchy*). Las entidades protegidas pueden ir desde una sola sección múltiplex (SDH) (por ejemplo, protección de sección múltiplex lineal) hasta una parte de un trayecto de extremo a extremo SDH (por ejemplo, protección de conexión de subred) o hasta un trayecto entero de extremo a extremo SDH (por ejemplo, protección de camino de contenedor virtual lineal de orden superior/inferior). Las realizaciones físicas de estas arquitecturas de protección pueden incluir anillos o cadenas lineales de nodos. Cada clasificación de la protección incluye directrices sobre objetivos de red, arquitectura, funcionalidad de las aplicaciones, criterios de conmutación, protocolos y algoritmos.



# Reemplazada por una versión más reciente

Recomendación G.841

## TIPOS Y CARACTERÍSTICAS DE LAS ARQUITECTURAS DE PROTECCIÓN PARA REDES DE LA JERARQUÍA DIGITAL SÍNCRONA

(Ginebra, 1995)

### 1 Alcance

La Recomendación G.841 describe los distintos mecanismos de protección para las redes de la jerarquía digital síncrona (SDH), sus objetivos y sus aplicaciones.

Los esquemas de protección se clasifican como sigue:

- protección de camino SDH (en la capa de sección o de trayecto);
- protección de conexión de subredes SDH (con supervisión intrínseca, supervisión no intrusiva y supervisión de subcapa).

Los casos de interfuncionamiento de protección (incluida la jerarquía de conmutación) y de interconexión están estudiándose en el marco de otra Recomendación.

Quedan en estudio los aspectos de satélite/radio, operación, administración, mantenimiento y suministro, OAM&P y calidad de funcionamiento. No se describen aquí la arquitectura de sincronización ni la protección de la sincronización. No es necesario que se describan en esta Recomendación todos los mecanismos de protección disponibles en el mismo equipo SDH.

### 2 Referencias

Las Recomendaciones UIT-T siguientes y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones, por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y de otras referencias citadas a continuación. Regularmente se publica una lista de las Recomendaciones UIT-T actualmente vigentes.

- Recomendación UIT-T G.707 (1993), *Velocidades binarias de la jerarquía digital síncrona*.
- Recomendación UIT-T G.708 (1993), *Interfaz de nodo de red para la jerarquía digital síncrona*.
- Recomendación UIT-T G.709 (1993), *Estructura de multiplexación síncrona*.
- Recomendación G.774 del CCITT (1992), *Modelo de información de gestión de la jerarquía digital síncrona desde el punto de vista de los elementos de red*.
- Recomendación G.782 del CCITT (1990), *Tipos y características generales de multiplexación de la jerarquía digital síncrona*.
- Recomendación G.783 del CCITT (1990), *Características de los bloques funcionales del equipo de multiplexación para la jerarquía digital síncrona*.
- Recomendación UIT-T G.784 (1994), *Gestión de la jerarquía digital síncrona*.
- Recomendación UIT-T G.803 (1993), *Arquitecturas de redes de transporte basadas en la jerarquía digital síncrona*.

### 3 Términos y definiciones

A los efectos de esta Recomendación se aplican las siguientes definiciones:

**3.1 controlador de APS:** Parte de un nodo que es responsable de generar y terminar la información transportada en el protocolo APS e implementar el algoritmo APS.

**3.2 múltiplex de adición-sustracción** (ADM, *add-drop multiplex*): Elementos de red que proporcionan acceso a todas las señales constitutivas contenidas en una señal STM-N o a un subconjunto de las mismas. Cuando la señal STM-N pasa por el ADM, le son añadidas (insertadas) y/o sustraídas (extraídas) las señales constitutivas. Véase 3.5/G.782.

## Reemplazada por una versión más reciente

- 3.3 **tráfico añadido:** Tráfico insertado en los canales de trabajo del anillo en un nodo de dicho anillo.
- 3.4 **unidad administrativa (AU, administrative unit):** Véase la Recomendación G.708.
- 3.5 **señal de indicación de alarma (AIS, alarm indication signal):** Código enviado hacia adelante en una red digital como indicación de que atrás ha sido detectado un fallo y se ha dado aviso de él. Está asociada con múltiples capas de transporte.
- 3.6 **AU-AIS:** Véase la Recomendación G.783.
- 3.7 **puntero de AU:** Véase la Recomendación G.709.
- 3.8 **autoaprovisionamiento:** Asignación de valores a parámetros en un elemento de red, sin que dichos valores sean introducidos de manera específica desde el exterior por un usuario.
- 3.9 **conexión bidireccional:** Véase la Recomendación G.803. Se ilustra en la Figura 3-2.
- 3.10 **anillo bidireccional:** En un anillo bidireccional el encaminamiento normal del tráfico del trabajo es tal que los dos sentidos de una conexión bidireccional recorren el anillo a través de los mismos nodos, pero en sentidos opuestos.
- 3.11 **paridad N de entrelazado de bits (BIP-N, bit interleaved parity N):** Véase la Recomendación G.708.
- 3.12 **puentear:** Transmitir tráfico idéntico por los canales de servicio y de protección.
- 3.13 **petición de puenteo:** Mensaje enviado desde un nodo de extremo de cola hacia un nodo de extremo de cabeza en el que se solicita que el extremo de cabeza puentee los canales de servicio a los canales de protección.
- 3.14 **situación de petición de puenteo:** Mensaje enviado desde un nodo de extremo de cola a todos los demás nodos en el sistema de protección, indicando que el extremo de cola ha solicitado un puenteo.
- 3.15 **contenedor:** Véase la Recomendación G.708.
- 3.16 **fallo de controlador:** Condición durante la cual un nodo no puede tratar correctamente el protocolo de APS, pero sigue generando una trama SDH correctamente formada.
- 3.17 **bytes-K cruzados:** Cuando un nodo ve peticiones de puenteo de anillo de igual prioridad en ambos «lados». (Esto incluye el caso en que un nodo de commutación recibe una petición de puenteo de anillo desde el otro extremo.)
- 3.18 **canal de comunicación de datos (DCC, data communications channel):** Véase la Recomendación G.784.
- 3.19 **protección especializada:** Arquitectura de protección que proporciona capacidad reservada para la protección de las capacidades de transporte de tráfico (1 + 1). Véase la Recomendación G.803.
- 3.20 **código de APS por defecto:** Este término se refiere a los bytes de APS transmitidos con la ID de nodo de origen igual a la ID de nodo de destino.
- 3.21 **encaminamiento diverso:** Se transporta tráfico de servicio bidireccional (es decir, de ida y vuelta) por las diferentes facilidades físicas en condiciones de ausencia de fallo. Este encaminamiento puede aplicarse a caminos individuales o a conexiones de subred. Se ilustra en la Figura 3-2.
- 3.22 **tráfico sustraído:** Tráfico extraído de los canales de trabajo del anillo en un nodo de dicho anillo.
- 3.23 **comutación de extremo doble:** Método de commutación de protección que realiza la acción de commutación en ambos extremos de la entidad protegida (por ejemplo, «conexión», «trayecto»), incluso en caso de fallo unidireccional. Véase la Recomendación G.803.
- 3.24 **tráfico adicional:** Tráfico transportado por los canales de protección cuando esa capacidad no es utilizada para la protección del tráfico de servicio. El tráfico adicional no está protegido. Al necesitarse los canales de protección para proteger el tráfico de servicio, el tráfico adicional será desplazado.
- 3.25 **transferencia total:** Acción de transmitir los mismos K1, K2 y canales de protección que se reciben. La transferencia total es bidireccional.
- 3.26 **extremo de cabeza:** Nodo que ejecuta un puenteo. Se señala que un nodo funciona como un extremo de cabeza y un extremo de cola para una commutación bidireccional del mismo tramo.

## Reemplazada por una versión más reciente

- 3.27 **contenedor virtual de orden superior:** Véase la Recomendación G.708.
- 3.28 **tiempo de espera:** El tiempo comprendido entre la declaración de degradación de señal o fallo de señal y la iniciación del algoritmo de conmutación de protección.
- 3.29 **reposo:** Estado de un nodo que no está generando, detectando ni viendo pasar por él peticiones de puenteo o información de situación de petición de puenteo.
- 3.30 **nodo aislado:** Nodo que está aislado de la perspectiva de tráfico por conmutaciones de anillo en cada uno de sus dos tramos por sus nodos adyacentes.
- 3.31 **transferencia de bytes K:** Acción de transmitir los mismos bytes K1 y K2 que se reciben. Los canales de protección no son transferidos. La transferencia de bytes K es bidireccional.
- 3.32 **trayecto largo:** Segmento de trayecto fuera del tramo para el que se inicia la petición de puenteo. Por lo general hay otros nodos intermedios a lo largo de este segmento de trayecto.
- 3.33 **pérdida de trama (LOF, loss of frame):** Véase la Recomendación G.783.
- 3.34 **pérdida de señal (LOS, loss of signal):** Véase la Recomendación G.783 para los sistemas SDH y la Recomendación G.775 para los sistemas PDH.
- 3.35 **contenedor virtual de orden inferior:** Véase la Recomendación G.708.
- 3.36 **acceso a contenedor virtual de orden inferior:** Terminación de un contenedor virtual de orden superior para añadir, sustraer o interconectar un contenedor virtual o un grupo de contenedores virtuales de orden inferior.
- 3.37 **conexión errónea:** Condición en la que el tráfico destinado a determinado nodo es encaminado incorrectamente hacia otro nodo y no se ha emprendido ninguna acción correctiva.
- 3.38 **bit más significativo:** Posición de bit «más a la izquierda» o posición de bit que se transmite primero en un byte.
- 3.39 **sección de multiplexación (MS, multiplex section):** Véase la Recomendación G.803.
- 3.40 **señal de indicación de alarma de sección de multiplexación (MS-AIS, multiplex section alarm indication signal):** Véase la Recomendación G.783.
- 3.41 **indicación de defecto distante de sección de multiplexación (MS-RDI, multiplex section remote defect indication):** Anteriormente conocida como fallo de extremo distante de sección múltiple. Véase la Recomendación G.709.
- 3.42 **protección de conexión de red:** Esquema que protege la conexión de subred más grande posible de un camino.
- 3.43 **interfaz de nodo de red (NNI, network node interface):** Véase la Recomendación G.708.
- 3.44 **transferencia:** Acción de transmitir la misma información que se recibe en cualquier sentido de transmisión.
- 3.45 **trayecto:** Véase la Recomendación G.803.
- 3.46 **tara de trayecto:** Véase la Recomendación G.708.
- 3.47 **canales de protección:** Canales asignados al transporte de tráfico de servicio durante un evento de conmutación. Cuando hay un evento de conmutación, el tráfico en los canales de servicio afectados es puenteado a los canales de protección.
- 3.48 **sección de regeneración:** Véase la Recomendación G.803.
- 3.49 **indicación de error distante:** Anteriormente error de bloque en el extremo distante. Véase la Recomendación G.709.
- 3.50 **umbral de restablecimiento:** Para las instrucciones iniciadas automáticamente se utiliza un método de histéresis al conmutar de los canales de protección nuevamente a los canales de servicio. Este método especifica un umbral de la BER para la sección múltiple que transporta los canales de servicio. Este umbral se denomina comúnmente «umbral de restablecimiento». El umbral de restablecimiento se fija a una BER más baja que el umbral de degradación de señal.
- 3.51 **restablecimiento:** Véase la Recomendación G.803.

## **Reemplazada por una versión más reciente**

**3.52 anillo:** Conjunto de nodos que forman un bucle cerrado en el que cada nodo está conectado a dos nodos adyacentes a través de una facilidad de comunicaciones dúplex. Un anillo proporciona anchura de banda redundante o equipos de red redundantes, o ambos, de manera que los servicios distribuidos pueden ser restablecidos automáticamente después de un fallo o después de una degradación en la red. Así, un anillo puede autorrepararse.

**3.53 fallo de anillo:** Fallo para el que el restablecimiento puede realizarse únicamente mediante una conmutación de anillo.

**3.54 interfuncionamiento de anillos:** Topología de red en la que dos anillos están conectados en dos puntos y funcionan de manera que el fallo de cualquiera de estos dos puntos no cause pérdida de tráfico, salvo el que posiblemente se sustraiga o inserte en el punto de fallo.

**3.55 conmutación de anillo:** Mecanismo de protección que se aplica, tanto a los anillos de dos fibras como a los de cuatro fibras. Durante una conmutación de anillo, el tráfico del tramo afectado es transportado a través de los canales de protección por el trayecto largo.

**3.56 tara de sección:** Véase la Recomendación G.708.

**3.57 anillo segmentado:** Anillo que está separado en dos o más segmentos, ya sea externamente mediante conmutaciones forzadas (FS-R) o automáticamente como resultado de conmutaciones fallo de señal – anillo (SF-R).

**3.58 protección compartida:** Arquitectura de protección que utiliza  $m$  entidades de protección compartidas por  $n$  entidades de servicio ( $m : n$ ). Las entidades de protección pueden utilizarse también para transportar tráfico adicional cuando no se utilizan para la protección. Véase la Recomendación G.803.

**3.59 trayecto corto:** Segmento del trayecto por el tramo para el que se inicia la petición de puenteo. Este tramo es siempre el tramo al que se conectan el extremo de cabeza y el extremo de cola. La petición de puenteo de trayecto corto es la petición de puenteo enviada por el tramo para el que es iniciada la petición de puenteo.

**3.60 conmutación de extremo único:** Método de conmutación de protección que efectúa la acción de conmutación únicamente en el extremo afectado de la entidad protegida (por ejemplo, «camino», «conexión de subred») en el caso de un fallo unidireccional. Véase la Recomendación G.803.

**3.61 fallo en un solo punto:** Fallo localizado en un solo punto físico de un anillo. El fallo puede afectar a una o más fibras. Un fallo en un solo punto puede ser detectado por un número cualquiera de NE.

**3.62 tramo:** Conjunto de secciones de multiplexión entre dos nodos adyacentes de un anillo.

**3.63 conmutación de tramo:** Mecanismo de protección similar a la APS lineal 1 : 1 que se aplica únicamente a anillos de cuatro fibras en los que los canales de servicio y de protección están contenidos en fibras separadas y el fallo sólo afecta a los canales de servicio. Durante una conmutación de tramo, el tráfico de servicio es transportado por los canales de protección del mismo tramo que el fallo.

**3.64 tráfico silenciado:** Señal de sólo «1» que resulta del proceso de silenciamiento.

**3.65 silenciamiento:** Proceso consistente en insertar AU-AIS para evitar conexiones erróneas.

**3.66 conexión de subred:** Véase la Recomendación G.803.

**3.67 protección de conexión de subred:** Una conexión de subred de servicio es sustituida por una conexión de subred de protección si falla la conexión de subred de servicio o si su calidad de funcionamiento cae por debajo de un nivel requerido.

**3.68 red con capacidad de supervivencia:** Red capaz de restablecer el tráfico en caso de fallo. El grado de supervivencia viene determinado por la capacidad de la red para sobrevivir a fallos individuales de sistema de línea, fallos múltiples de sistema de línea y fallos de equipo.

**3.69 conmutar:** Acción consistente en seleccionar tráfico de los canales de protección en vez de hacerlo de los canales de servicio.

**3.70 tiempo de compleción de conmutación:** Intervalo entre la decisión de conmutar hasta la compleción de la operación de puenteo y conmutación en un nodo de conmutación que inicia la petición de puenteo.

**3.71 nodo de conmutación:** Nodo que realiza la función de puenteo o conmutación para un evento de protección. En el caso de una arquitectura de red en anillo con conmutación de sección de multiplexión, este nodo lleva a cabo también cualquier silenciamiento necesario del tráfico mal conectado para trayectos de VC-3/4 o de velocidad superior.

## Reemplazada por una versión más reciente

**3.72 sincrónico:** Característica esencial de las escalas o señales de tiempo, en virtud de la cual sus instantes significativos correspondientes ocurren precisamente a la misma velocidad en promedio.

**3.73 módulo de transporte sincrónico de nivel N** (STM-N, *synchronous transport module level N*): Véase la Recomendación G.707.

**3.74 extremo de cola:** Nodo que solicita el puenteo. Se señala que un nodo funciona como un extremo de cabeza y un extremo de cola para una conmutación bidireccional del mismo tramo.

**3.75 intercambio de intervalos de tiempo** (TSI, *timeslot interchange*): A los efectos de la presente Recomendación, el TSI es la capacidad de cambiar la posición de los intervalos de tiempo del tráfico transconectado (es decir, el tráfico que no es añadido al nodo o sustraído del mismo).

**3.76 camino:** Véase la Recomendación G.803.

**3.77 protección de camino:** Un camino de servicio es reemplazado por un camino de protección si falla el primero o si su calidad de funcionamiento cae por debajo de un nivel requerido.

**3.78 transporte:** Facilidades asociadas con el transporte de señales STM-1 o de nivel más alto.

**3.79 fallo no detectado:** Cualquier defecto de equipo que no es detectado por las funciones de mantenimiento de equipo, y que, por consiguiente, no inicia una conmutación de protección ni proporciona la notificación OA&M apropiada. Estos tipos de fallo no se manifiestan por sí mismos antes de que se intente efectuar una conmutación de protección.

**3.80 conexión unidireccional:** Véase la Recomendación G.803. En la Figura 3-1 se da una ilustración.

**3.81 anillo unidireccional:** En un anillo unidireccional (con conmutación de trayecto o con conmutación de sección de multiplexación), el encaminamiento normal del tráfico de servicio es tal que ambos sentidos de una conexión bidireccional se desplazan alrededor del anillo en el mismo sentido (por ejemplo, en el sentido de las agujas de un reloj). Específicamente, cada conexión bidireccional utiliza las capacidades situadas a lo largo de toda la circunferencia del anillo.

**3.82 encaminamiento uniforme:** El tráfico de servicio bidireccional (es decir, de ida y vuelta) es transportado por las mismas facilidades físicas en condiciones de ausencia de fallos. Dicho encaminamiento puede aplicarse a caminos individuales o conexiones de subred. Esto se ilustra en la Figura 3-2.

**3.83 contenedor virtual** (VC, *virtual container*): Véase la Recomendación G.708.

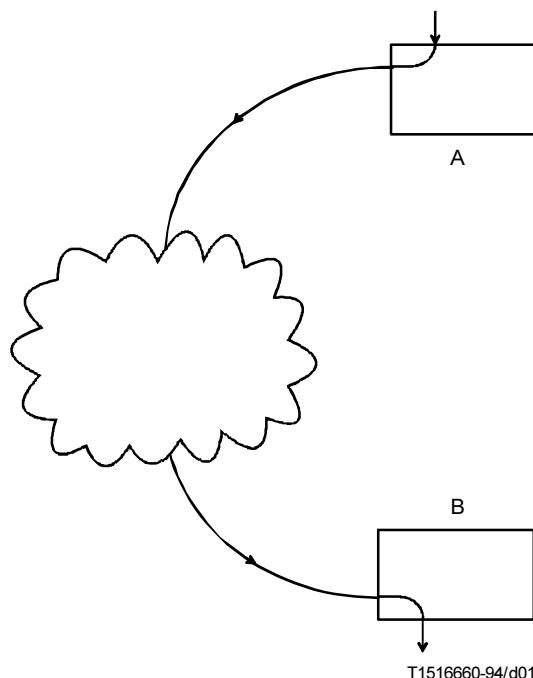


FIGURA 3-1/G.841  
Conexión unidireccional

## Reemplazada por una versión más reciente

**3.84 canales de servicio:** Canales por los que es transportado el tráfico de servicio cuando no hay eventos de conmutación. Un sistema de APS lleva a cabo el restablecimiento únicamente para los canales de servicio.

**3.85 tráfico de servicio:** El tráfico que atraviesa un anillo es transportado normalmente por los canales de servicio, salvo en caso de conmutación de protección de tramo o anillo, caso en el cual es restablecido por los canales de protección.

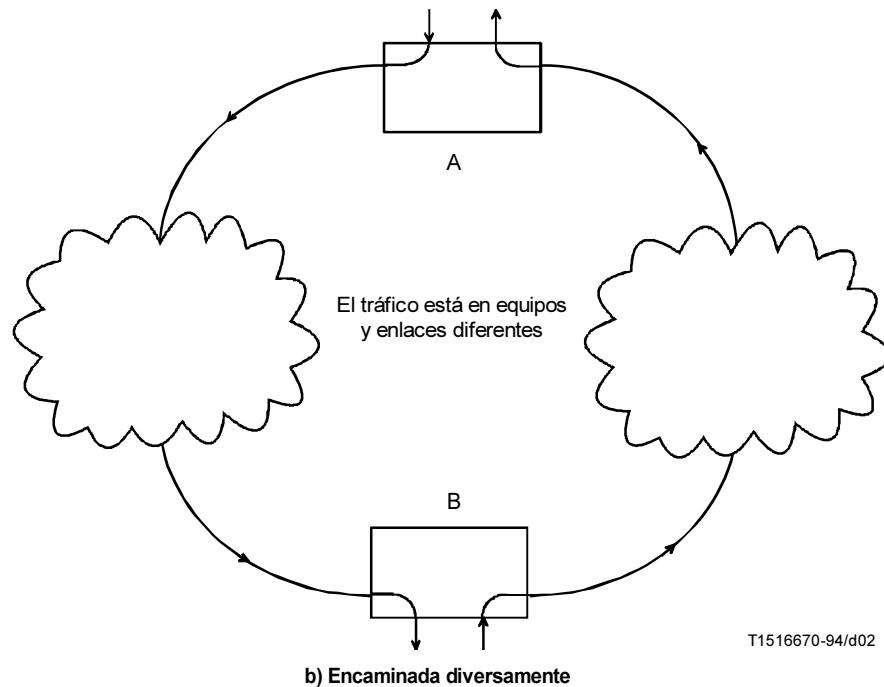
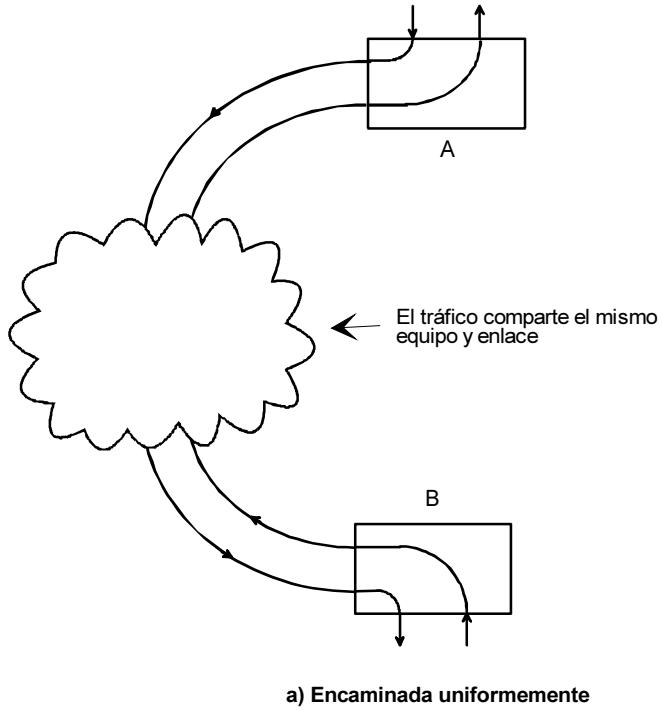


FIGURA 3-2/G.841

**Conexión bidireccional encaminada uniformemente  
y encaminada diversamente**

# Reemplazada por una versión más reciente

## 4 Abreviaturas

A los efectos de esta Recomendación se utilizan las abreviaturas siguientes:

ADM	Múltiplex de adición/sustracción ( <i>add drop multiplex</i> )
AIS	Señal de indicación de alarma ( <i>alarm indication signal</i> )
AP	Punto de acceso ( <i>access point</i> )
APS	Conmutación de protección automática ( <i>automatic protection switching</i> )
AU	Unidad administrativa ( <i>administrative unit</i> )
AUG	Grupo de unidades administrativas ( <i>administrative unit group</i> )
AU-AIS	Señal de indicación de alarma de unidad administrativa ( <i>administrative unit alarm indication signal</i> )
AU-LOP	Pérdida de puntero de unidad administrativa ( <i>administrative unit loss of pointer</i> )
BER	Tasa de errores en los bits ( <i>bit error ratio</i> )
BIP-N	Paridad N de entrelazado de bits ( <i>bit interleaved parity N</i> )
Br	Puenteo (puenteado) [ <i>bridge (d)</i> ]
CP	Punto de conexión ( <i>connection point</i> )
DCC	Canal de comunicaciones de datos ( <i>data communications channel</i> )
EXER-R	Ejercicio – anillo ( <i>exerciser – ring</i> )
EXER-S	Ejercicio – tramo ( <i>exerciser – span</i> )
FS-P	Conmutación forzada a protección ( <i>forced switch to protection</i> )
FS-R	Conmutación forzada de trabajo a protección – anillo ( <i>forced switched working to protection – ring</i> )
FS-S	Conmutación forzada de servicio a protección – tramo ( <i>forced switched working to protection – span</i> )
FS-W	Conmutación forzada a servicio ( <i>forced switch to working</i> )
HO	Orden superior ( <i>higher order</i> )
HOVC	Contenedor virtual de orden superior ( <i>higher order virtual container</i> )
HP-DEG	Trayecto de orden superior degradado ( <i>higher order path degraded</i> )
HP-EXC	Trayecto de orden superior – errores excesivos ( <i>higher order path excessive errors</i> )
HP-SSF	Trayecto de orden superior – fallo de señal de servidor ( <i>higher order path –server signal fail</i> )
HP-TIM	Trayecto de orden superior – desadaptación de identificador de traza ( <i>higher order path trace identifier mismatch</i> )
HP-UNEQ	Trayecto de orden superior no equipado ( <i>higher order path unequipped</i> )
ID	Identificación ( <i>identification</i> )
LO	Orden inferior ( <i>lower order</i> )
LOF	Pérdida de trama ( <i>loss of frame</i> )
LOVC	Contenedor virtual de orden inferior ( <i>lower order virtual container</i> )
LP	Exclusión de protección ( <i>lockout of protection</i> )
LP-DEG	Trayecto de orden inferior degradado ( <i>lower order path degraded</i> )
LP-EXC	Trayecto de orden inferior – errores excesivos ( <i>lower order path excessive errors</i> )
LP-S	Exclusión de protección – tramo ( <i>lockout of protection – span</i> )
LP-SSF	Trayecto de orden inferior – fallo de señal de servidor ( <i>lower order path server signal fail</i> )
LP-TIM	Trayecto de orden inferior – desadaptación de identificador de traza ( <i>lower order path trace identifier mismatch</i> )
LP-UNEQ	Trayecto de orden inferior no equipado ( <i>lower order path unequipped</i> )
LOS	Pérdida de señal ( <i>loss of signal</i> )
MS	Sección de multiplexación ( <i>multiplex section</i> )
MSA	Adaptación de sección de multiplexación ( <i>multiplex section adaptation</i> )

## Reemplazada por una versión más reciente

MSP	Protección de sección de multiplexación ( <i>multiplex section protection</i> )
MSPA	Adaptación de protección de sección de multiplexación ( <i>multiplex section protection adaptation</i> )
MSPT	Terminación de protección de sección de multiplexación ( <i>multiplex section protection termination</i> )
MST	Terminación de sección de multiplexación ( <i>multiplex section termination</i> )
MS-P	Comutación manual a protección ( <i>manual switch to protection</i> )
MS-R	Comutación manual – anillo ( <i>manual switch – ring</i> )
MS-S	Comutación manual – tramo ( <i>manual switch – span</i> )
MS-W	Comutación manual a servicio ( <i>manual switch to working</i> )
NE	Elemento de red ( <i>network element</i> )
NNI	Interfaz de nodo de red ( <i>network node interface</i> )
NR	Ausencia de petición ( <i>no request</i> )
OAM&P	Operación, administración, mantenimiento y suministro ( <i>operations, administration, maintenance &amp; provisioning</i> )
OS	Sistema (operativo) ( <i>operation system</i> )
POH	Tara de trayecto ( <i>path overhead</i> )
RCD	Red de comunicaciones de datos
RGT	Red de gestión de las telecomunicaciones
RR-R	Invertir petición – anillo ( <i>reverse request – ring</i> )
RR-S	Invertir petición – tramo ( <i>reverse request – span</i> )
RSOH	Tara de sección de regeneración ( <i>regenerator section overhead</i> )
SD	Degradación de señal ( <i>signal degrade</i> )
SDH	Jerarquía digital síncrona ( <i>synchronous digital hierarchy</i> )
SD-P	Degradación de señal de los canales de protección ( <i>signal degrade of the protection channels</i> )
SD-R	Degradación de señal – anillo ( <i>signal degrade – ring</i> )
SD-S	Degradación de señal – tramo ( <i>signal degrade – span</i> )
SF	Fallo de señal ( <i>signal fail</i> )
SF-R	Fallo de señal – anillo ( <i>signal fail – ring</i> )
SF-S	Fallo de señal - tramo ( <i>signal fail – span</i> )
SNC	Conexión de subred ( <i>subnetwork connection</i> )
SNC/I	Protección de conexión de subred con supervisión intrínseca ( <i>subnetwork connection protection with inherent monitoring</i> )
SNC/N	Protección de conexión de subred con supervisión no intrusiva ( <i>subnetwork connection protection with non-intrusive monitoring</i> )
SSF	Fallo de señal de servidor ( <i>server signal fail</i> )
STM-N	Módulo de transporte síncrono de nivel N ( <i>synchronous transport module level N</i> )
Sw	Comutación (conmutado) [ <i>switch(ed)</i> ]
TCP	Punto de conexión de terminación ( <i>termination connection point</i> )
TSI	Intercambio de intervalos de tiempo ( <i>timeslot interchange</i> )
TU	Unidad afluente ( <i>tributary unit</i> )
VC	Contenedor virtual ( <i>virtual container</i> )
WTR	En espera al restablecimiento ( <i>wait to restore</i> )

## 5 Clasificaciones de la protección

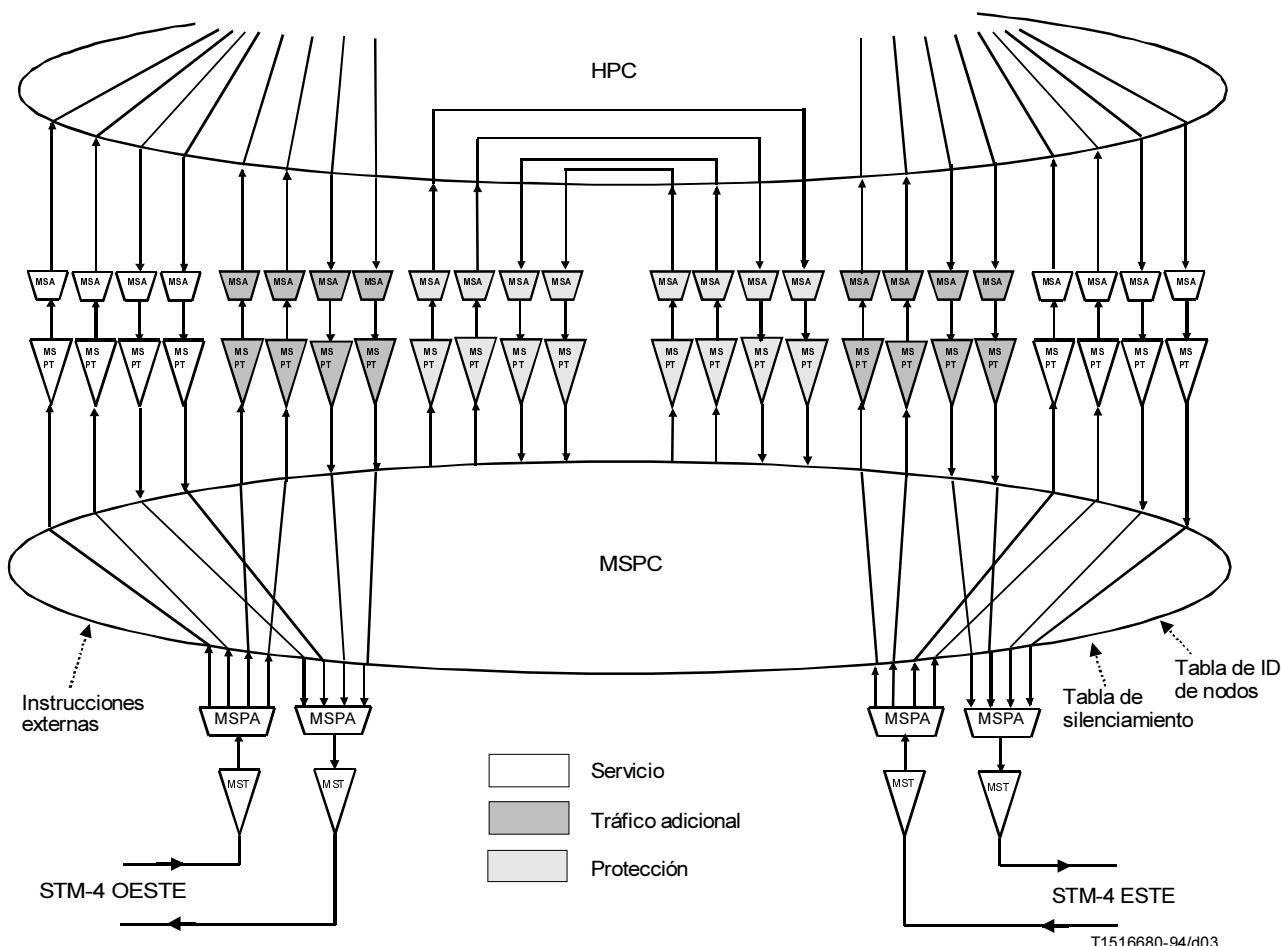
Esta cláusula describe en términos generales los tipos de arquitectura de protección descritos en la presente Recomendación. Basicamente, hay dos tipos de conmutación de protección: protección de camino SDH y protección de conexión de subred SDH.

## Reemplazada por una versión más reciente

Los anillos de protección compartida de MS son una protección de camino SDH. La Figura 5-1 ilustra el modelo de un anillo de protección compartida de MS de dos fibras con una capacidad de 4 AUG, incluyendo las conexiones de subred de transmisión y recepción. La Figura 5-2 muestra la reacción del mismo modelo al corte completo de cable en un lado. La Figura 5-3 muestra la reacción del mismo modelo como nodo de transferencia.

La Figura 5-4 muestra el modelo funcional genérico para la protección de camino de VC 1 + 1. La Figura 5-5 muestra el modelo funcional genérico para la protección de camino de VC reversivo 1:1 y la Figura 5-6 muestra el modelo funcional genérico para la protección de camino de VC no reversivo 1:1.

La Figura 5-7 muestra el modelo funcional para la protección de conexión de subred con supervisión intrínseca (SNC/I). La Figura 5-8 muestra el modelo funcional para la conexión de subred con supervisión no intrusiva (SNC/N).

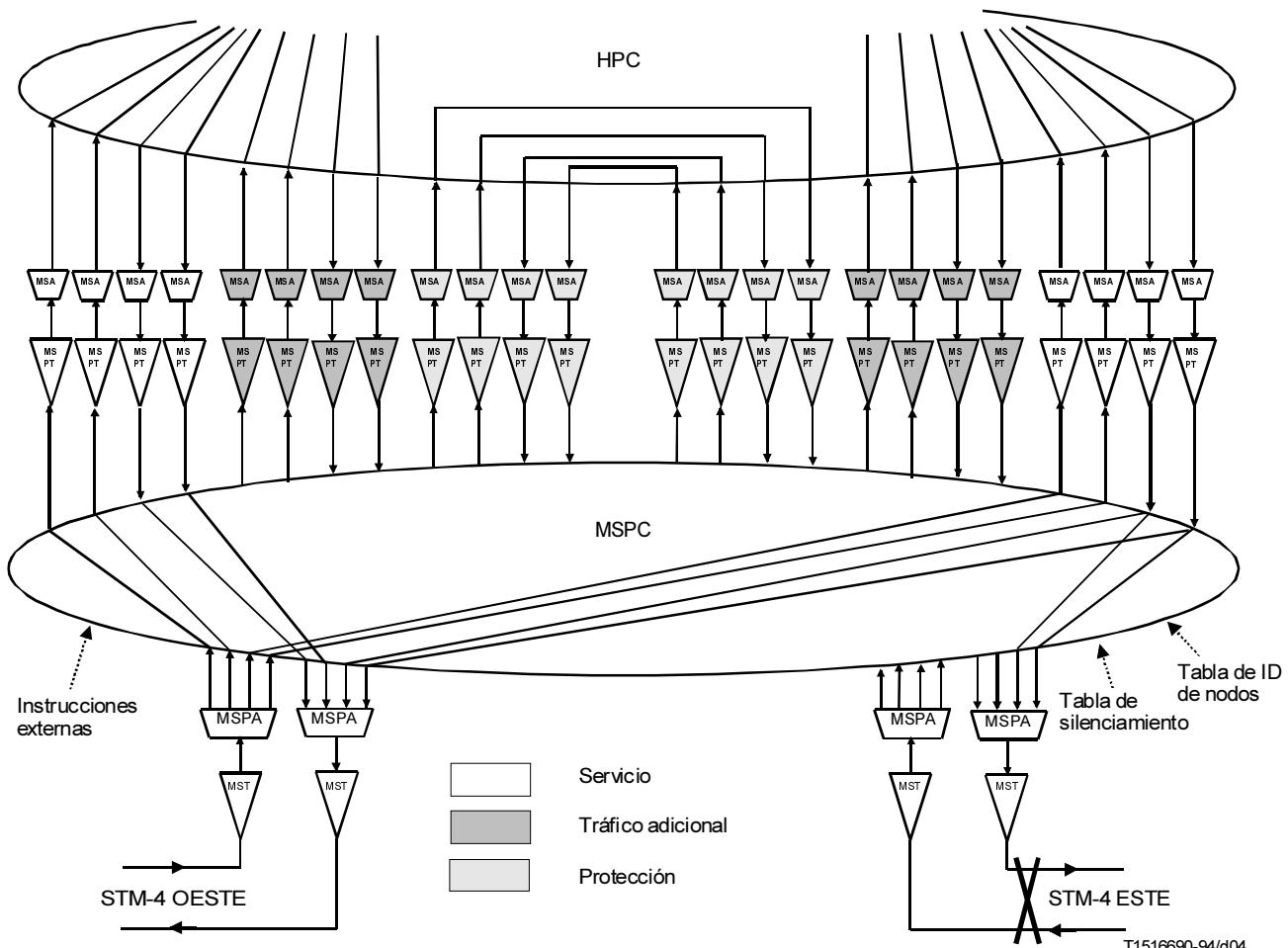


HPC	Conexión de trayecto de orden superior
MSA	Adaptación de sección de multiplexación
MSPC	Conexión de protección de sección de multiplexación
MSPT	Terminación de protección de sección de multiplexación
MST	Terminación de sección de multiplexación

FIGURA 5-1/G.841

Modelo funcional para un anillo de protección compartida de MS de dos fibras –  
Estado normal con tráfico adicional

## Reemplazada por una versión más reciente

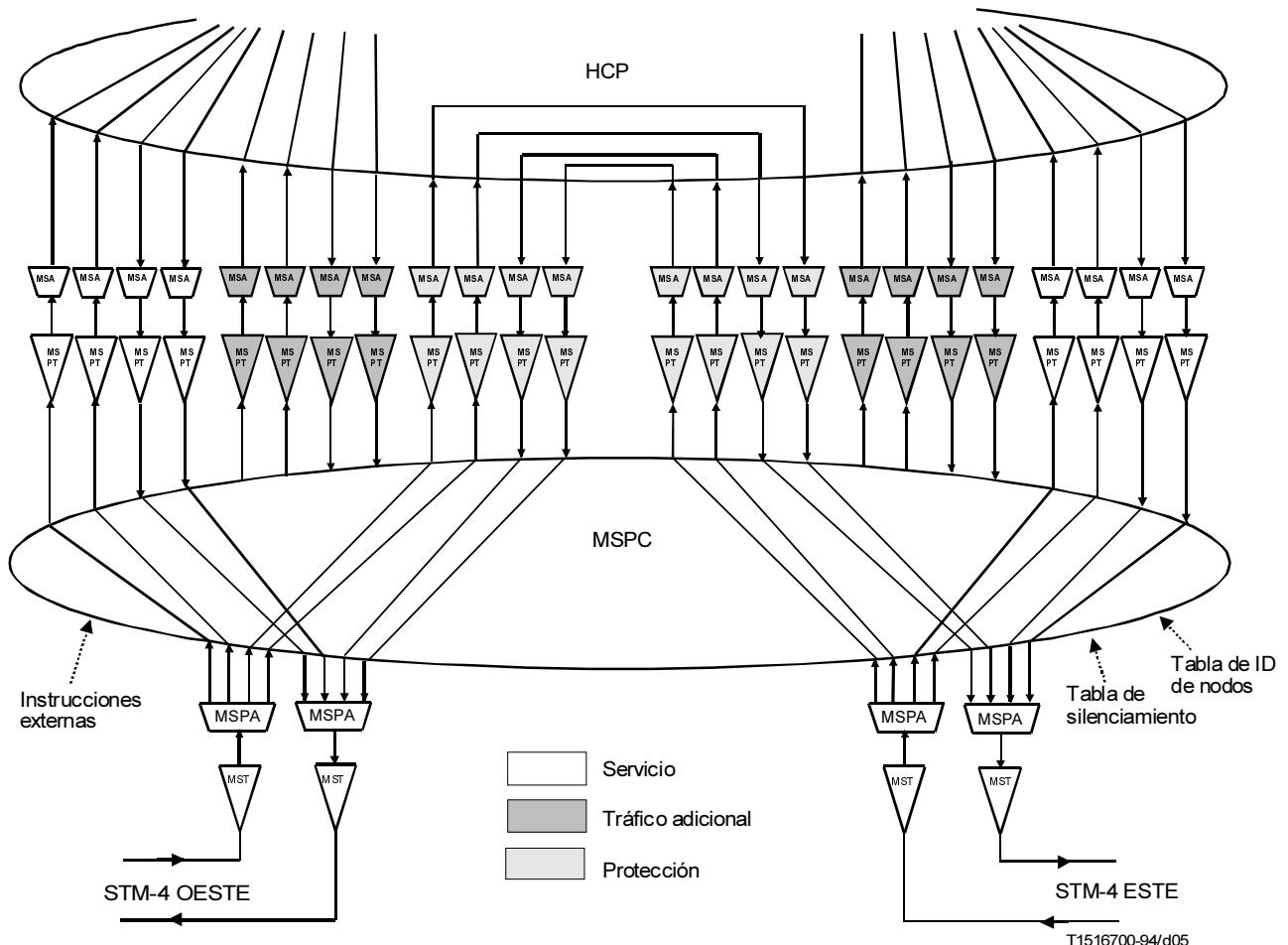


HPC	Conexión de trayecto de orden superior
MSA	Adaptación de sección de multiplexación
MSPA	Adaptación de protección de sección de multiplexación
MSPC	Conexión de protección de sección de multiplexación
MSPT	Terminación de protección de sección de multiplexación
MST	Terminación de sección de multiplexación

FIGURA 5-2/G.841

**Modelo funcional para un anillo de protección compartida de MS de dos fibras – Fallo en el lado Este**

# Reemplazada por una versión más reciente

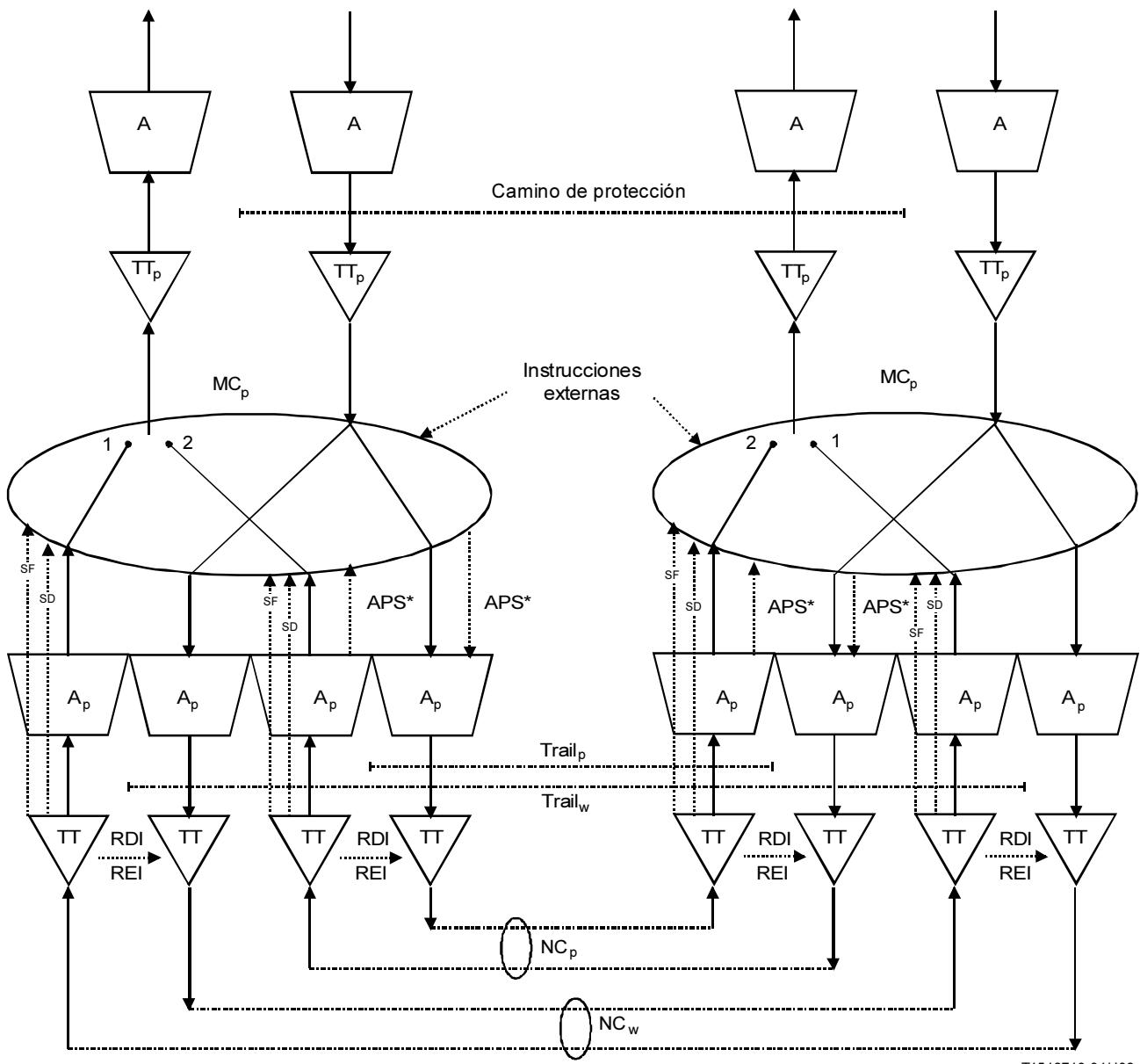


HPC Conexión de trayecto de orden superior  
 MSA Adaptación de sección de multiplexación  
 MSPA Adaptación de protección de sección de multiplexación  
 MSPC Conexión de protección de sección de multiplexación  
 MSPT Terminación de protección de sección de multiplexación  
 MST Terminación de sección de multiplexación

FIGURA 5-3/G.841

Modelo funcional para un anillo de protección compartida de MS de dos fibras – Estado de transferencia

## Reemplazada por una versión más reciente



\* Requerido para conmutación de extremo doble.  
No requerido para conmutación de extremo único.

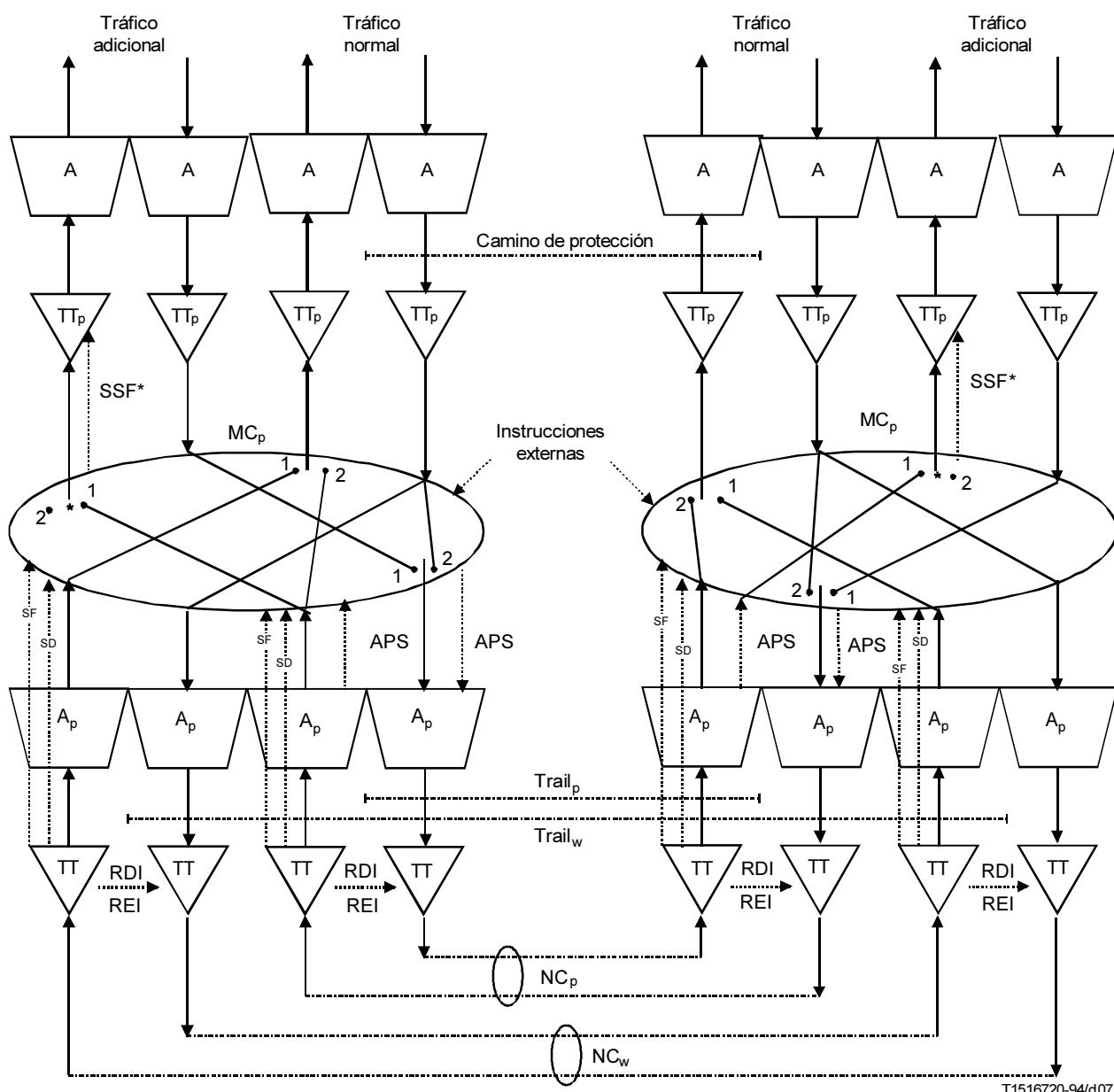
**A** Adaptación  
 **$A_p$**  Adaptación de protección  
 **$MC_p$**  Conexión de matriz de protección  
 **$NC_p$**  Conexión de red de protección  
 **$NC_w$**  Conexión de red de servicio  
**RDI** Indicación de defecto a distancia  
**REI** Indicación de error a distancia

**SD** Degradación de señal  
**SF** Fallo de señal  
**SSF** Fallo de señal de servidor  
 **$Trail_p$**  Camino de protección  
 **$Trail_w$**  Camino de servicio  
**TT** Terminación de camino  
 **$TT_p$**  Terminación de camino de protección

Estados: 1 Estado normal  
2 Estado de fallo

FIGURA 5-4/G.841  
Modelo funcional para protección de camino lineal 1 + 1 genérica

# Reemplazada por una versión más reciente



\* SSF activo en conexión abierta [estado de fallo (2)]. Queda en estudio.

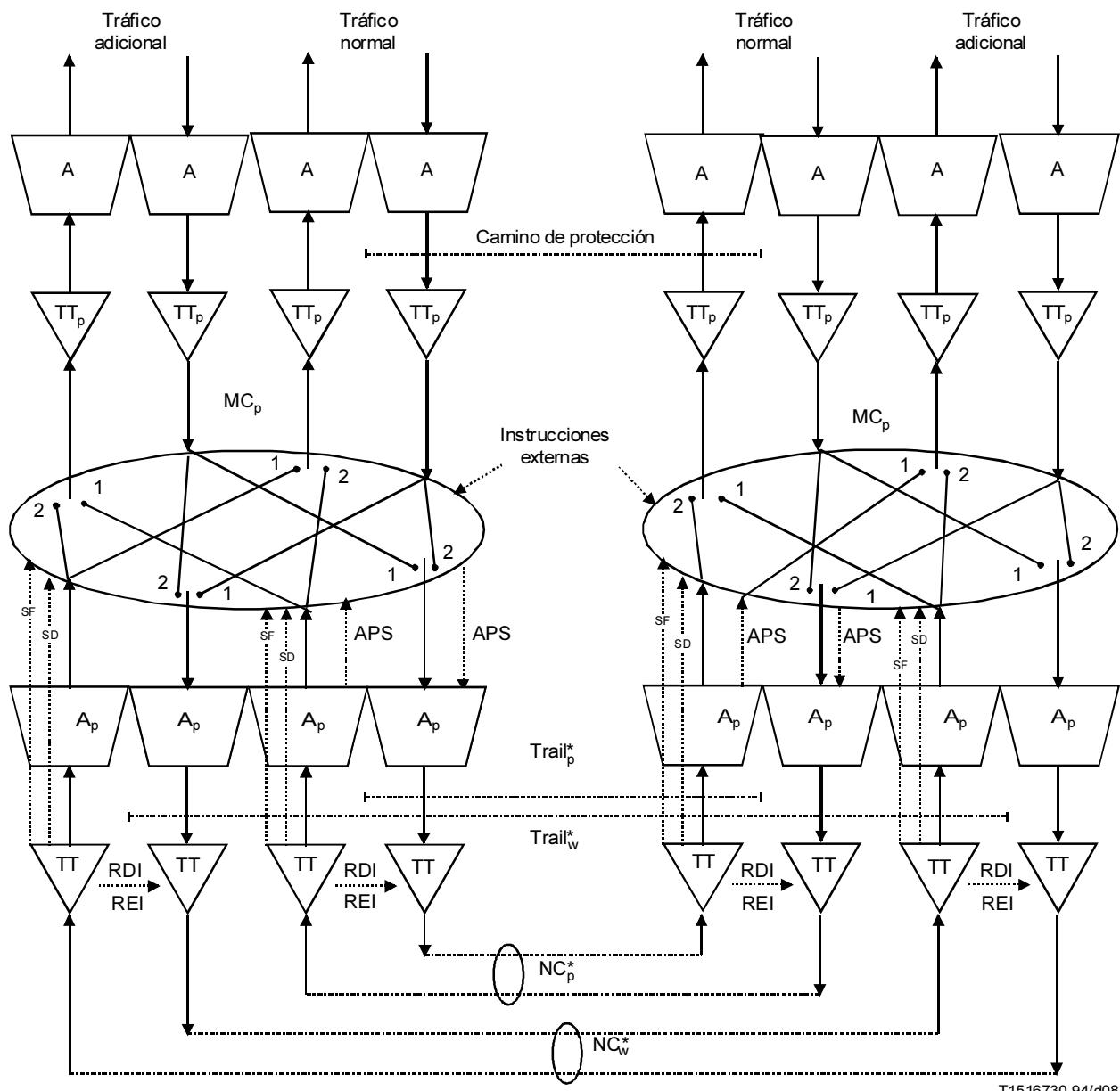
A	Adaptación
$A_p$	Adaptación de protección
$MC_p$	Conexión de matriz de protección
$NC_p$	Conexión de red de protección
$NC_w$	Conexión de red de servicio
RDI	Indicación de defecto a distancia
REI	Indicación de error a distancia

SD	Degradación de señal
SF	Fallo de señal
SSF	Fallo de señal de servidor
$Trail_p$	Camino de protección
$Trail_w$	Camino de servicio
TT	Terminación de camino
$TT_p$	Terminación de camino de protección

Estados: 1 Estado normal  
2 Estado de fallo

FIGURA 5-5/G.841  
Modelo funcional para protección de camino lineal 1 : 1 genérica –  
Funcionamiento reversivo

# Reemplazada por una versión más reciente



\* En estado de fallo (2), Trail<sub>p</sub> pasa a ser Trail<sub>w</sub>, Trail<sub>p</sub> pasa a ser Trail<sub>w</sub>, NC<sub>p</sub> pasa a ser NC<sub>w</sub> y NC<sub>w</sub> pasa a ser NC<sub>p</sub>.

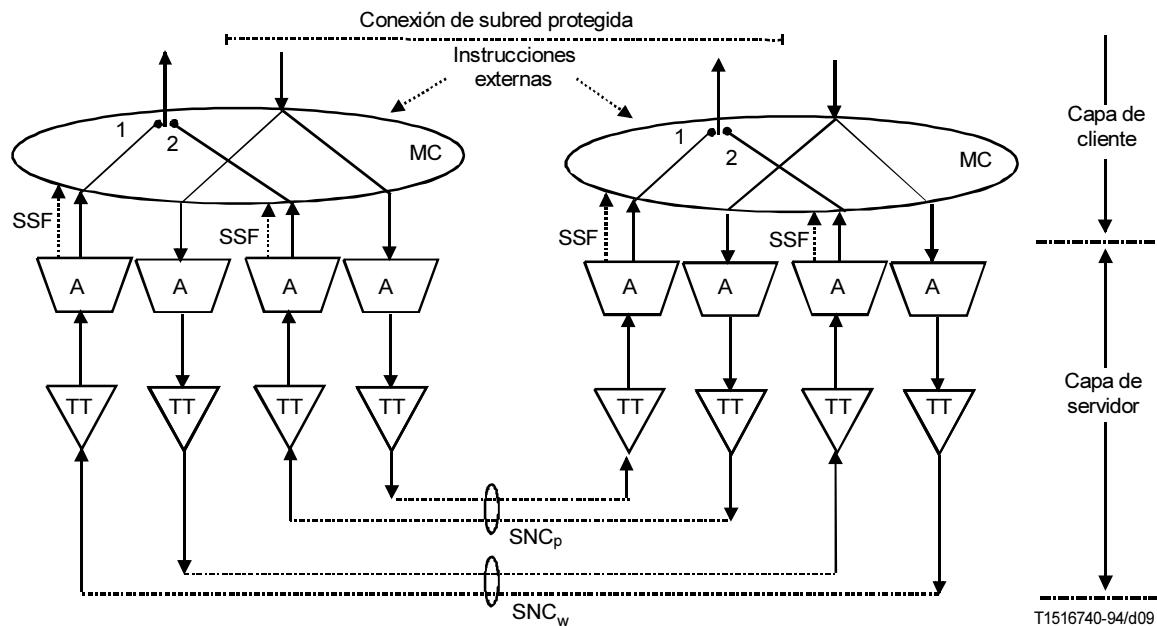
A	Adaptación
A <sub>p</sub>	Adaptación de protección
MC <sub>p</sub>	Conexión de matriz de protección
NC <sub>p</sub>	Conexión de red de protección
NC <sub>w</sub>	Conexión de red de servicio
RDI	Indicación de defecto a distancia
REI	Indicación de error a distancia

SD	Degradación de señal
SF	Fallo de señal
SSF	Fallo de señal de servidor
Trail <sub>p</sub>	Camino de protección
Trail <sub>w</sub>	Camino de servicio
TT	Terminación de camino
TT <sub>p</sub>	Terminación de camino de protección

Estados:  
 1 Estado normal  
 2 Estado de fallo

FIGURA 5-6/G.841  
Modelo funcional para protección de camino lineal 1 : 1 genérica – Funcionamiento no reversivo

## Reemplazada por una versión más reciente



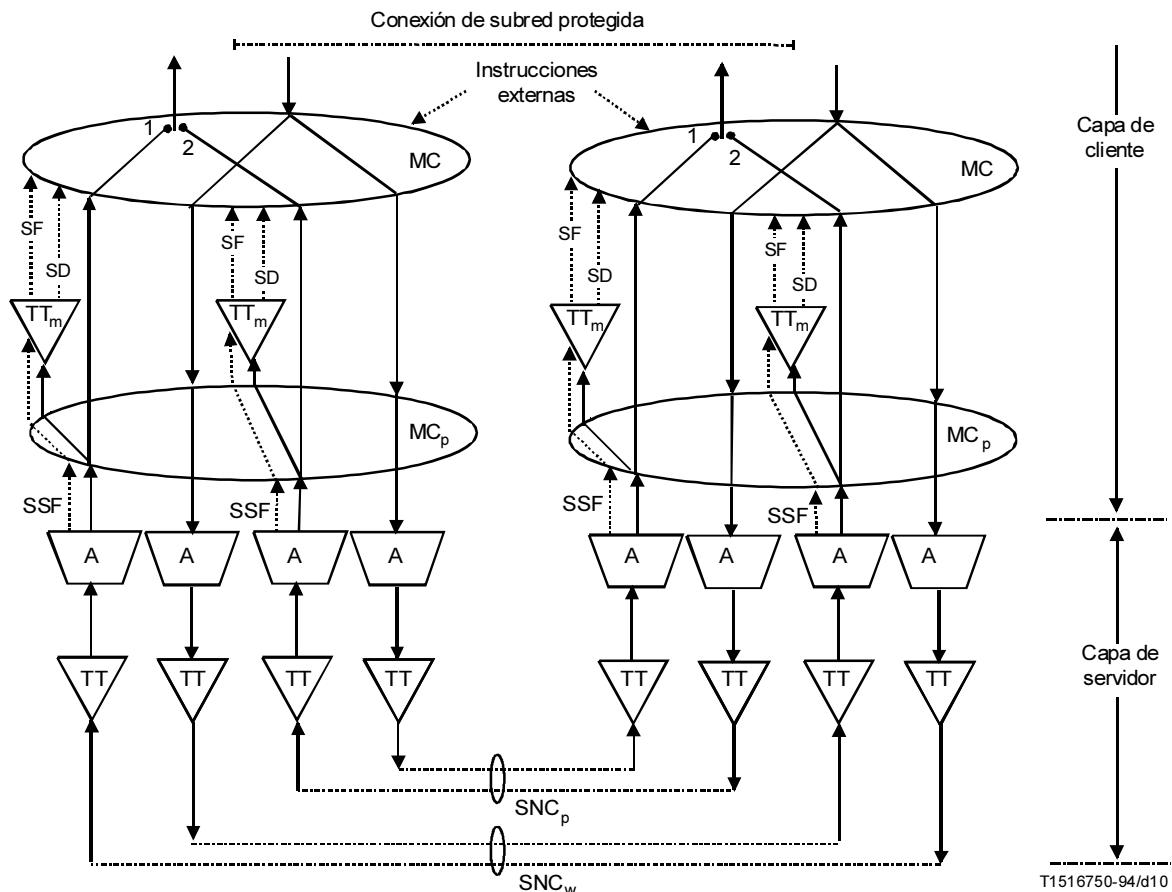
A Adaptación  
MC Conexión de matriz  
SNC<sub>p</sub> Conexión de subred de protección  
SNC<sub>w</sub> Conexión de subred de servicio  
SSF Fallido de señal de servidor  
TT Terminación de camino

Estados: 1 Estado normal  
2 Estado de fallo

FIGURA 5-7/G.841

Modelo funcional para protección de conexión de subred con supervisión intrínseca (SNC/I) mediante un fallo de señal de servidor

## Reemplazada por una versión más reciente



A	Adaptación
MC	Conexión de matriz
MC <sub>p</sub>	Conexión de matriz de protección
SD	Degrado de señal
SF	Fallo de señal
SNC <sub>p</sub>	Conexión de subred de protección
SNC <sub>w</sub>	Conexión de subred de servicio
SSF	Fallo de señal de servidor
TT	Terminación de camino
TT <sub>m</sub>	Supervisor no intrusivo

Estados: 1 Estado normal  
2 Estado de fallo

FIGURA 5-8/G.841

**Modelo funcional para protección de conexión de subred con supervisión no intrusiva (SNC/N)**

# **Reemplazada por una versión más reciente**

## **6 Consideraciones relativas a las aplicaciones**

Esta cláusula describe en términos generales algunas de las ventajas posibles que pueden obtenerse gracias a las distintas arquitecturas de protección.

### **6.1 Anillos de protección compartida de sección de multiplexación**

Los anillos de protección compartida de sección de multiplexación puede clasificarse en dos tipos: de dos fibras y de cuatro fibras. El protocolo de APS de anillo contempla ambos tipos.

Para los anillos de protección compartida de sección de multiplexación, los canales de servicio transportan servicio que ha de protegerse, mientras que los canales de protección se reservan para la protección de este servicio. El tráfico de servicio es transportado bidireccionalmente por los tramos: un afluente entrante se desplaza en uno de los sentidos de los canales de servicio, mientras que el afluente saliente asociado se desplaza en el sentido opuesto, pero por los mismos tramos.

El par de afluentes (entrante y saliente) utiliza únicamente capacidades a lo largo de los tramos comprendidos entre los nodos en que el par es añadido y sustraído. Así, como se ilustra en la Figura 6-1, la manera en que estos pares de afluentes están colocados en el anillo repercute en la carga máxima que pueden soportar los anillos de protección compartida de sección de multiplexación. La suma de los afluentes que atraviesan un tramo no puede exceder de la capacidad máxima de dicho tramo.

Según el diagrama de los afluentes, la carga máxima que puede admitir un anillo de protección compartida de sección de multiplexación (bidireccional) puede exceder de la carga máxima que puede admitir el tipo equivalente de anillo unidireccional (por ejemplo, protección especializada de sección de multiplexación o protección SNC) con la misma velocidad óptica y el mismo número de fibras. Esto da al anillo bidireccional una ventaja de capacidad con relación a los anillos unidireccionales, salvo cuando todos los afluentes están destinados a un solo nodo del anillo, caso en el cual son equivalentes.

Una de las ventajas de los anillos de protección compartida de sección de multiplexación es que el servicio puede ser encaminado por el anillo en cualquiera de los dos sentidos, por el camino largo o por el camino corto alrededor del anillo. Si bien se preferirá por lo general el camino corto, ocasionalmente el encaminamiento del servicio por el camino largo dará algunas posibilidades en materia de equilibrio de carga.

Cuando los canales de protección no están utilizándose para restablecer los canales de servicio, pueden utilizarse para transportar tráfico adicional. Al producirse una comutación de protección, el tráfico de servicio cursado por los canales de servicio pasará a los canales de protección, lo que tendrá como consecuencia que el tráfico adicional sea retirado de los canales de protección.

Durante una comutación de anillo, los canales de servicio transmitidos hacia el tramo que ha fallado son comutados en un nodo de comutación a los canales de protección transmitidos en el sentido opuesto (en el sentido opuesto al del fallo). Este tráfico puenteado recorre el camino largo alrededor del anillo por los canales de protección hacia el otro nodo de comutación en el que los canales de protección son comutados de nuevo a los canales de servicio. En el otro sentido, los canales de servicio son puenteados y comutados de la misma manera. La Figura 6-2 ilustra una comutación de anillo en respuesta a un corte de cable.

Durante una comutación de anillo, el tramo que ha fallado es «reemplazado» efectivamente mediante los canales de protección comprendidos entre los nodos de comutación por el camino largo alrededor del anillo. Habida cuenta de que los canales de protección situados a lo largo de cada tramo (salvo el tramo que ha fallado) son utilizados para el restablecimiento, la capacidad de protección es efectivamente compartida por todos los tramos.

### **6.2 Anillos de protección compartida de sección de multiplexación (aplicación transoceánica)**

Esta aplicación, incluidos los requisitos adicionales y las características de explotación, se describe en el Anexo A.

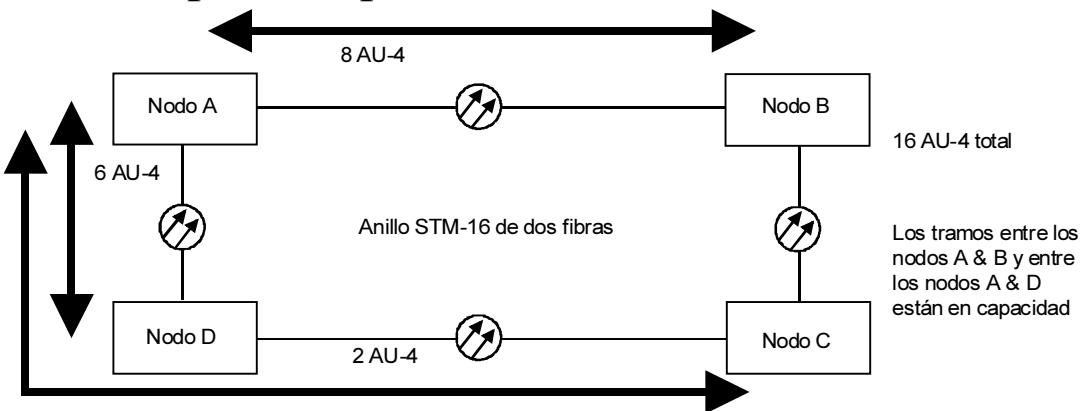
### **6.3 Anillos de protección especializada de sección de multiplexación**

Un anillo de protección especializada de sección de multiplexación consta de dos anillos de sentido opuesto. En este caso, sólo un anillo transporta el tráfico de servicio que ha de protegerse, mientras que el otro está reservado para la protección de este tráfico de servicio.

La demanda máxima que puede admitir el anillo está limitada a la capacidad de un tramo. La forma de la demanda no tiene repercusiones sobre la capacidad de los anillos unidireccionales. En otras palabras, la suma de la demanda de todos los nodos no puede exceder de la capacidad de un solo tramo.

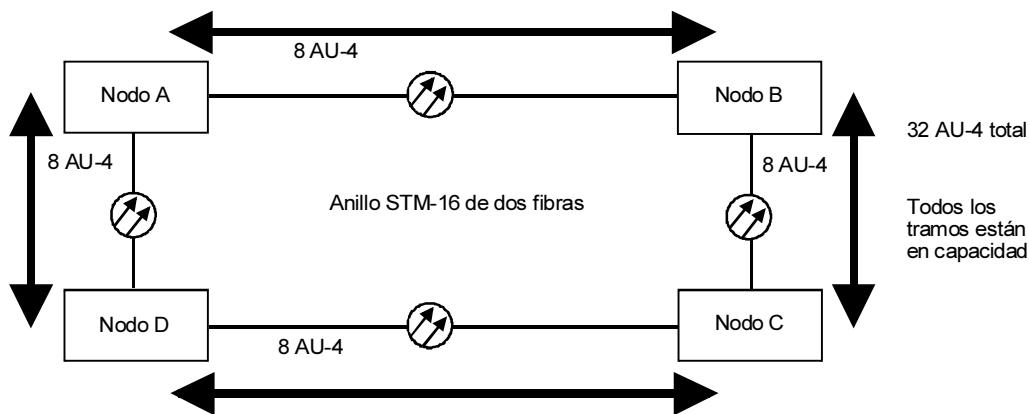
Los anillos de protección especializada de sección de multiplexación requerirán también el uso de los bytes de APS, K1 y K2, para la comutación de protección.

## Reemplazada por una versión más reciente

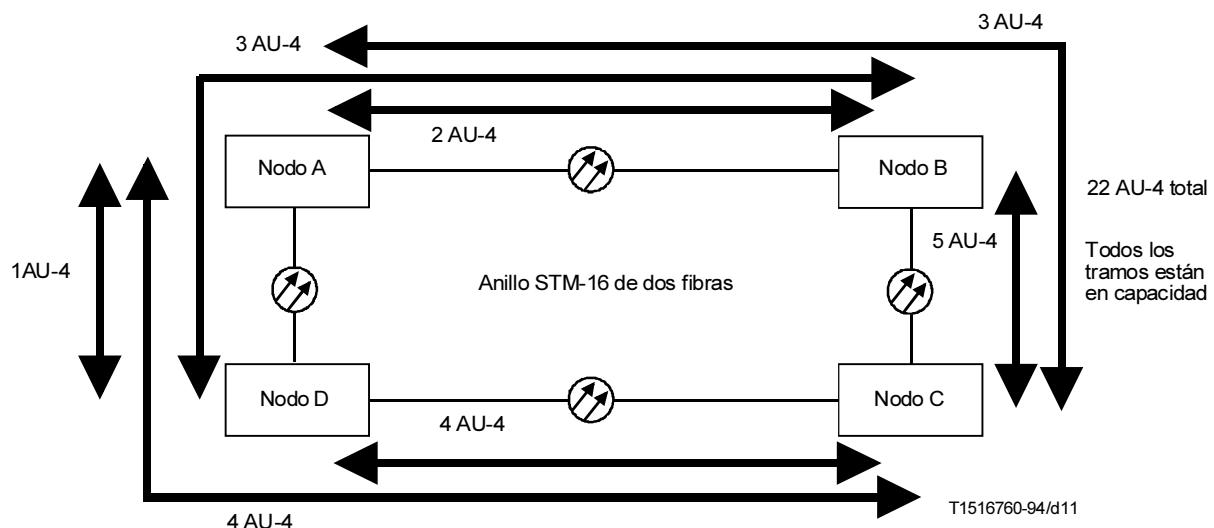


NOTA – Puesto que todo el tráfico está destinado al nodo A y el tramo entre el A y el nodo B está lleno, el tráfico del nodo C se encamina a través del nodo B, dejando vacante el tramo entre el nodo B y el nodo C.

a) Todo el tráfico destinado a un nodo, el nodo A



b) Todo el tráfico destinado a nodos adyacentes solamente

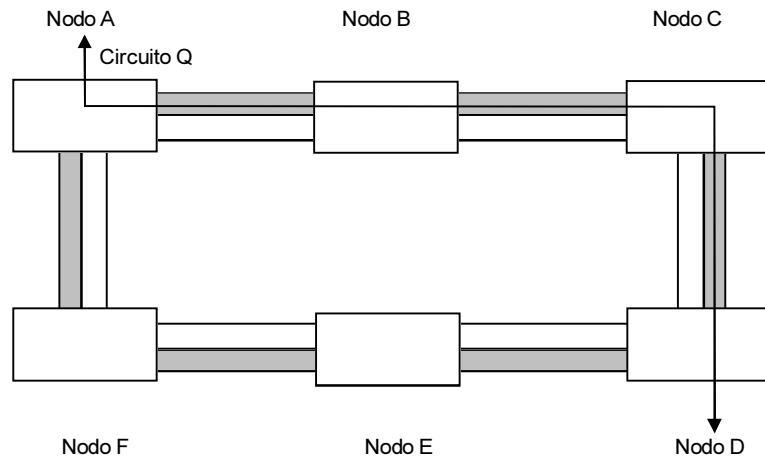


c) Configuración de tráfico mixto

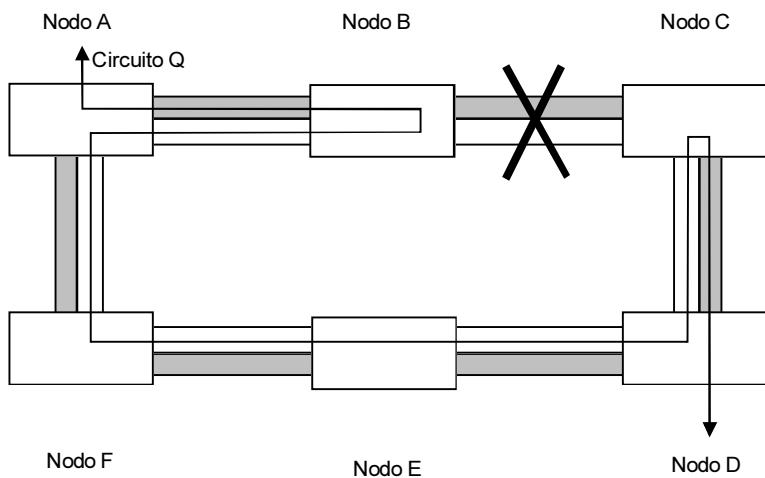
FIGURA 6-1/G.841

Efectos de la configuración de la demanda en la capacidad de los anillos de protección compartida de MS bidireccional

## Reemplazada por una versión más reciente



a) Estado normal



b) Estado de fallo

T1516770-94/d12

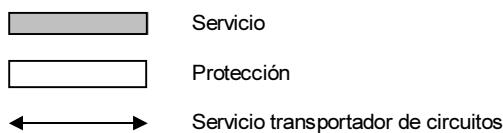


FIGURA 6-2/G.841

Ejemplo de encaminamiento de circuito en estado de fallo  
para una commutación de anillo

## **Reemplazada por una versión más reciente**

### **6.4 Comutación de extremo único y de extremo doble**

Entre las posibles ventajas de la conmutación de extremo único figuran las siguientes:

- 1) La conmutación de extremo único es un esquema de realización simple que no requiere protocolo.
- 2) La conmutación de extremo único puede ser más rápida que la conmutación de extremo doble, ya que no requiere protocolo.
- 3) En condiciones de fallos múltiples existen mayores probabilidades de restablecer el tráfico mediante la conmutación de protección si se utiliza la conmutación de extremo único que si se utiliza conmutación de extremo doble.

Las posibles ventajas de la conmutación de extremo doble cuando se utiliza encaminamiento uniforme incluyen, entre otras, las siguientes:

- 1) Con la conmutación de extremo doble se utiliza el mismo equipo para ambos sentidos de transmisión después de un fallo. El número de interrupciones debido a fallos individuales será inferior al número correspondiente si el trayecto incluye equipos diferentes.
- 2) Con la conmutación de extremo doble, si hay una avería en un trayecto de la red, la transmisión de ambos trayectos entre los nodos afectados es conmutada al sentido alternativo alrededor de la red. No se transmite tráfico por la sección averiada de la red y, de esta manera, dicha sección puede ser reparada sin conmutación de protección adicional.
- 3) La conmutación de extremo doble es más fácil de gestionar, ya que ambos sentidos de transmisión utilizan los mismos equipos a lo largo de todo el camino.
- 4) La conmutación de extremo doble mantiene retardos iguales para ambos sentidos de transmisión. Esto puede ser importante cuando hay un desequilibrio significativo en la longitud de los caminos, por ejemplo, en los enlaces transoceánicos en que un camino se hace a través de un enlace por satélite y el otro a través de un enlace por cable.
- 5) La conmutación de extremo doble permite también transportar tráfico adicional por el trayecto de protección.

### **6.5 Protección de camino de contenedor virtual lineal**

La protección de camino de contenedor virtual (VC) lineal es un mecanismo de protección especializada que puede utilizarse en cualquier estructura física (a saber, en malla, en anillo o mixta). Puede aplicarse en cualquier capa de trayecto en una red estratificada.

Se trata de un mecanismo de protección de extremo a extremo, y se conmuta en caso de fallos de servidor o utilizando información a nivel de cliente, incluyendo información de calidad de trayecto. No necesita ser utilizado en todos los VC de una sección de multiplexación.

La protección de camino de VC lineal puede funcionar en modo conmutación de extremo único o de extremo doble. La conmutación de extremo doble permite transportar tráfico adicional por el trayecto de protección.

### **6.6 Protección de conexión de subred**

La protección de conexión de subred es un mecanismo de protección especializada que puede utilizarse en cualquier estructura física (a saber, en malla, en anillos o mixta). Puede aplicarse en cualquier capa de trayecto en una red estratificada.

Puede utilizarse para proteger una parte de un trayecto (por ejemplo, aquella en la que hay dos segmentos de trayecto separados) o la totalidad del trayecto de extremo a extremo. Se conmuta al producirse fallos del servidor (utilizando supervisión intrínseca) o utilizando información de capa de cliente (utilizando supervisión no intrusiva).

No necesita utilizarse en todos los circuitos virtuales de una sección de multiplexación. La protección SNC funciona en modo conmutación de extremo único. Queda en estudio la conmutación de extremo doble y el transporte de tráfico adicional.

### **6.7 Protección de sección de multiplexación lineal**

La protección de sección de multiplexación lineal puede ser un mecanismo de protección especializada o compartida. Protege la capa de sección de multiplexación y se aplica a redes físicas punto a punto. Una sección de multiplexación de protección puede utilizarse para proteger un número (N) de secciones de multiplexación de servicio. No puede proteger contra los fallos de nodo. Puede funcionar como conmutación de extremo único o de extremo doble, y puede transportar tráfico adicional por la sección de multiplexación de protección.

# **Reemplazada por una versión más reciente**

## **7 Protección de camino SDH**

Esta cláusula describe las características detalladas de los equipos que se requieren para admitir las aplicaciones de protección de camino SDH.

### **7.1 Protección de sección de multiplexación lineal**

Para mayor información sobre esta arquitectura, refiérase al Anexo A/G.783.

### **7.2 Anillos de protección compartida de sección de multiplexación**

#### **7.2.1 Arquitectura de la aplicación**

Todos los anillos de protección compartida de sección de multiplexación (MS) admiten la conmutación de anillo. Además, los anillos de protección compartida de sección de multiplexación de cuatro fibras admiten la conmutación de tramo.

##### **7.2.1.1 Anillos de protección compartida de sección de multiplexación de dos fibras**

Los anillos conmutados de sección de multiplexación (MS) de dos fibras requieren sólo dos fibras para cada tramo del anillo. Cada fibra transporta tanto los canales de servicio como los canales de protección. En cada fibra, la mitad de los canales están definidos como canales de servicio y la otra mitad como canales de protección. Los canales de servicio de una fibra están protegidos por los canales de sentido opuesto alrededor del anillo (véase la Figura 7-1). Esto permite el transporte bidireccional del tráfico de servicio. En cada fibra se utiliza únicamente un conjunto de canales de tara.

Los anillos de protección compartida de sección de multiplexación de dos fibras admiten únicamente la conmutación de anillo. Cuando se invoca una conmutación de anillo, los intervalos de tiempo que transportan los canales de servicio son conmutados a los intervalos de tiempo que transportan los canales de protección en el sentido opuesto.

##### **7.2.1.2 Anillos de protección compartida de sección de multiplexación de cuatro fibras**

Los anillos de protección compartida de sección de multiplexación (MS) de cuatro fibras requieren cuatro fibras para cada tramo del anillo. Como se ilustra en la Figura 7-2, los canales de servicio y los de protección son transportados por fibras diferentes: dos secciones de multiplexación que transmiten en sentidos opuestos transportan los canales de servicio mientras que dos secciones de multiplexación, que transmiten también en sentidos opuestos, transportan los canales de protección. Esto permite el transporte bidireccional del tráfico de servicio. La tara de sección de multiplexación está dedicada a, ya sea los canales de servicio o los de protección, dado que los canales de servicio y los de protección no son transportados por las mismas fibras.

Los anillos de protección compartida de sección de multiplexación (MS) de cuatro fibras admiten la conmutación de anillo como conmutación de protección, así como la conmutación de tramo, si bien no admiten las dos al mismo tiempo. Pueden coexistir varias conmutaciones de tramo en el anillo, dado que, para cada conmutación de tramo, sólo se utilizan los canales de protección de ese tramo. Algunos fallos múltiples (aquellos que afectan únicamente a los canales de servicio de un tramo, tales como los fallos electrónicos y los cortes de cable que afectan únicamente a los canales de servicio) pueden ser totalmente protegidos mediante la conmutación de tramo.

Los anillos de protección compartida de sección de multiplexación (MS) de cuatro fibras pueden tener la capacidad de funcionar de manera similar a una cadena ADM lineal cuando no están totalmente conectados como un anillo continuo (es decir, pueden excluir las conmutaciones de anillo y utilizar únicamente las conmutaciones de tramo para proteger el tráfico existente). Esta configuración puede existir si se establece un segmento de anillo aislado antes de que todos los demás tramos sean totalmente operacionales.

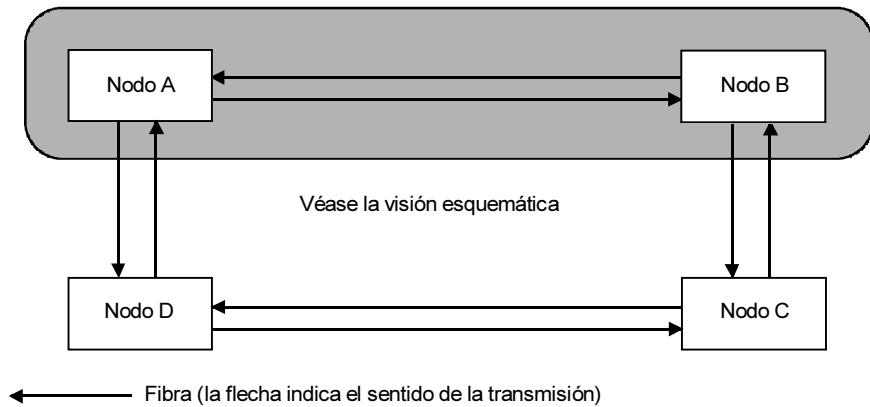
#### **7.2.2 Objetivos de red**

- 1) *Tiempo de conmutación* – En los anillos en que no haya tráfico adicional, no haya peticiones de puenteo anteriores y haya menos de 1200 km de fibra, el tiempo de compleción de la conmutación será inferior a 50 milisegundos.
- 2) *Retardo de transmisión* – No hay objetivo de red relativo al retardo de transmisión.
- 3) *Tiempos de espera* – No hay objetivo de red relativo a los tiempos de espera.

# Reemplazada por una versión más reciente

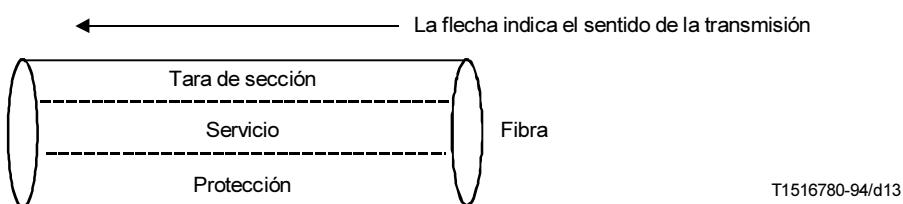
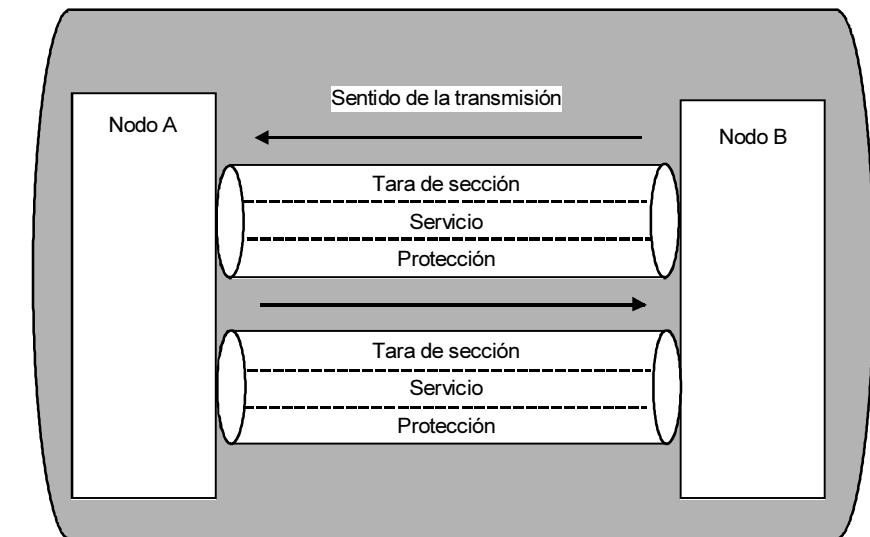
- 4) *Alcance de la protección*
  - a) Para un fallo en un solo punto, el anillo restablecerá todo el tráfico que atravesaría de manera transparente el sitio que ha fallado si no hubiera ocurrido ningún fallo.
  - b) El anillo restablecerá todo el tráfico posible, incluso en condiciones de múltiples peticiones de puenteo de igual prioridad (incluida la combinación de anillo de conmutación forzada-anillo y fallo de señal-anillo).
- 5) *Tipos de conmutación* – Se proporcionará la conmutación de extremo doble.
- 6) *Protocolo y algoritmo de APS*
  - a) El protocolo de conmutación podrá contemplar hasta 16 nodos en un anillo.
  - b) Para proporcionar un grado de protección adicional para el anillo de 4 fibras, se proporcionará en el protocolo de APS un mecanismo destinado a realizar la conmutación de tramo.
  - c) El protocolo de APS será óptimo para el nivel de funcionamiento AU-3/4.
  - d) El protocolo de APS y las funciones de OAM&P asociadas incluirán la posibilidad de modificar y mejorar el anillo. En particular, se incluirá la adición y supresión de nodos del anillo.
  - e) Se utilizará un proceso determinista para evitar el tráfico con conexiones erróneas.
  - f) Todos los tramos de un anillo tendrán igual prioridad. Por lo tanto, no existirán tramos de prioridad mayor cuyas peticiones de puenteo de anillo invaliden (automáticamente) otras conmutaciones de tramo del mismo tipo (por ejemplo, fallo de señal, degradación de señal o conmutación forzada).
  - g) El estado del anillo (es decir, normal o protegido) será conocido en cada nodo.
  - h) Una petición de puenteo de tramo tendrá una prioridad superior que una petición de puenteo de anillo del mismo tipo.
  - i) Si existe una conmutación de anillo y se produce un fallo de igual prioridad en otro tramo que requiere una conmutación de anillo (incluida la combinación de conmutación forzada – anillo y fallo de señal – anillo), entonces, si la prioridad de la petición de puenteo es la de fallo de señal (anillo) o superior, se establecerán ambas conmutaciones de anillo, lo que resultará en la segmentación del anillo en dos segmentos separados.
  - j) El silenciamiento de AUG se hará en los nodos de conmutación.
- 7) *Modos de funcionamiento*
  - a) Se proporcionará conmutación reversible. Una conmutación volverá únicamente a los canales de servicio, y no a un conjunto diferente de canales de protección.
  - b) La señalización APS de anillo proporcionará conmutación de protección, tanto para los anillos de protección compartida de MS bidireccional de cuatro fibras como de dos fibras.
- 8) *Control manual* – Se admitirán las siguientes instrucciones iniciadas externamente: exclusión de protección – tramo, conmutación forzada – tramo, conmutación forzada – anillo, conmutación manual – tramo, conmutación manual – anillo, ejercitador – tramo y ejercitador – anillo.
- 9) *Criterios de iniciación de la conmutación* – Se admitirán las siguientes instrucciones iniciadas automáticamente: fallo de señal – protección, fallo de señal – tramo, fallo de señal – anillo, degradación de señal – tramo, degradación de señal – anillo, degradación de señal – protección, invertir petición – tramo, invertir petición – anillo, espera al restablecimiento y ninguna petición.
- 10) *Criterios de utilización del anillo*.– El intercambio de intervalos de tiempo permitirá utilizar mejor la anchura de banda del anillo. Si se admite el intercambio de intervalos de tiempo (TSI), puede restablecerse o no restablecerse el tráfico que tiene un intercambio de intervalo de tiempo a través del sitio que ha fallado. Queda en estudio el saber si se admitirá el TSI y, en caso de que se admita, si será restablecido el tráfico que tiene intercambio de intervalos de tiempo a través del sitio que ha fallado.

# Reemplazada por una versión más reciente



NOTA – Cada fibra lleva tráfico de servicio y de protección, como se muestra en la visión esquemática.

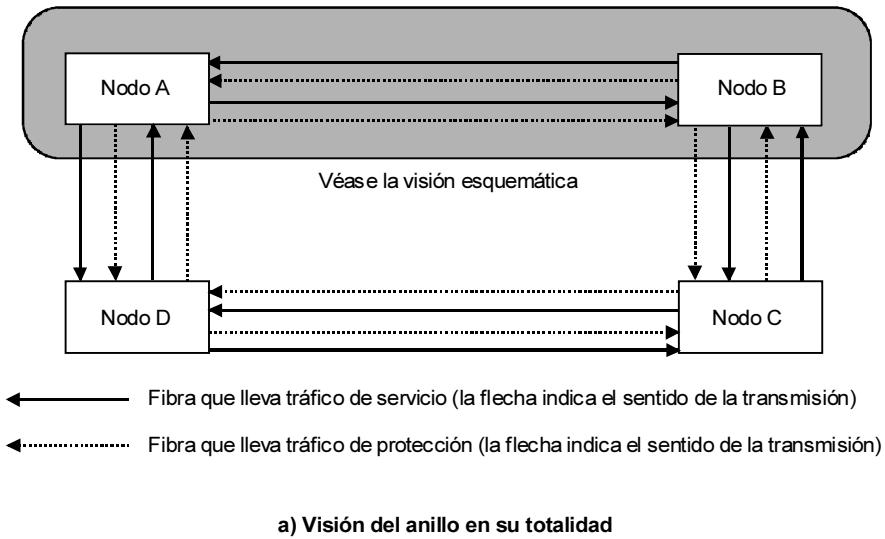
a) Visión del anillo en su totalidad



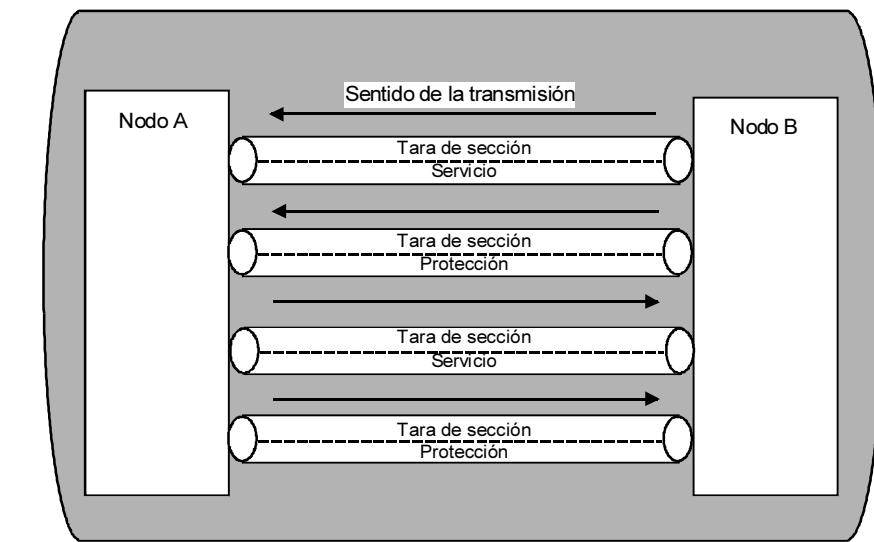
b) Visión esquemática de la porción sombreada del anillo

FIGURA 7-1/G.841  
Anillo de protección compartida de MS de dos fibras

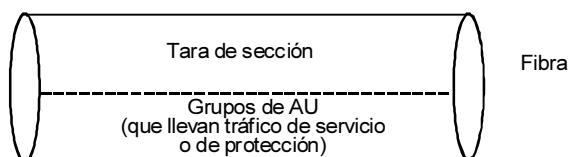
## Reemplazada por una versión más reciente



a) Visión del anillo en su totalidad



← La flecha indica el sentido de la transmisión



T1516790-94/d14

b) Visión esquemática de la porción sombreada del anillo

FIGURA 7-2/G.841

Anillo de protección compartida de MS de cuatro fibras

# Reemplazada por una versión más reciente

## 7.2.3 Arquitectura de la aplicación

Los grupos de AU que atraviesan el tramo entre dos nodos adyacentes se dividen en canales de servicio y canales de protección. En el caso de un anillo de dos fibras, el STM-N puede ser considerado como un múltiplex de N AU-4, en el que las AU-4 están numeradas de 1 a N de conformidad con el orden en que aparecen en el múltiplex. Las AU-4 numeradas de 1 a N/2 serán asignadas como canales de servicio y las AU-4 numeradas de (N/2) + 1 a N serán asignadas como canales de protección. Además, el canal de trabajo m es protegido por el canal de protección (N/2) + m. Por ejemplo, un STM-4 puede considerarse como un múltiplex de 4 AU-4 numeradas de 1 a 4. Las AU-4 número 1 y 2 serían asignadas como canales de servicio y las AU-4 números 3 y 4 serían asignadas como canales de protección. Esta asignación se aplica a ambos sentidos de la transmisión y a todos los tramos.

En el caso del anillo de cuatro fibras, cada STM-N de servicio y protección es transportado por una fibra separada.

El protocolo de APS de anillo será transportado en los bytes K1 y K2 en la tara de sección de multiplexación. En el caso del anillo de 4 fibras, el protocolo de APS es activo únicamente en las fibras que transportan canales de protección. Las funciones que se requieren en tiempo real y las que se requieren para hacer una comutación de protección se definen en el protocolo de APS de anillo utilizando los bytes K1 y K2. Otros canales de operaciones, incluidos los canales de comunicaciones de datos de la sección de multiplexación y la sección de regeneración, pueden también proporcionar funciones de comutación de protección que no son críticas con relación al tiempo (por ejemplo, las funciones que no necesitan ser completadas en un plazo de 50 milisegundos).

Se asignará una ID a cada nodo del anillo; dicha ID es un número de 0 a 15, lo que permite tener un máximo de 16 nodos en el anillo. La ID es independiente del orden en que aparecen los nodos en el anillo.

Un nodo del anillo puede insertar canales en cualquier sentido, retirar canales de cualquier sentido o dejar pasar canales directamente para permitir la conexión de otros nodos. Esta versión del documento sustenta únicamente el acceso de AU. Cada nodo tiene un mapa del anillo que es mantenido por personal local o por un OS y contiene información acerca de la asignación de canales que trata el nodo. En las Figuras 7-3 y 7-4 se da un ejemplo de dicho mapa de anillo.

Nodo
1 A
2 J
3 M
4 P
5 B
6 L
7 K
8 G
9 S
10 E
11 F
12 R
13 C
14 D
15 N
16 H

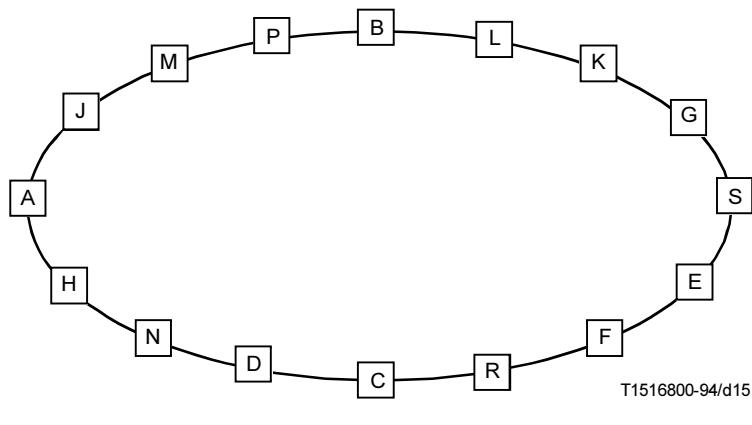
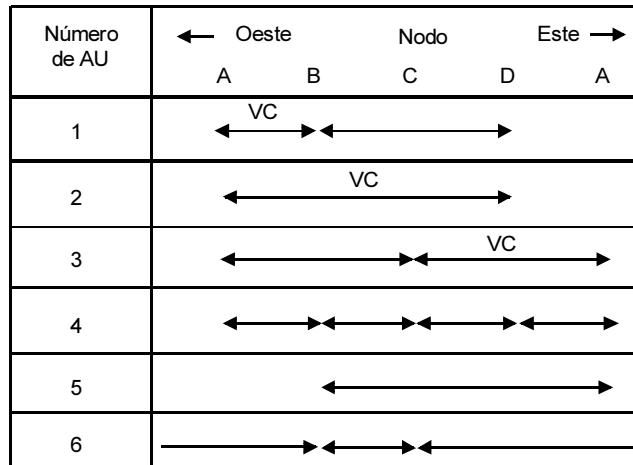


FIGURA 7-3/G.841  
Representación conceptual de un mapa de topología en anillo

## Reemplazada por una versión más reciente



Encaminamiento de tráfico de muestra para un anillo de 4 nodos

Nodo A

	Oeste		Este	
	Org/Trm	VC	Org/Trm	VC
1			A	✓
2			A	✓
3	A	✓	A	
4	A		C	
5	A		B	
6	B		B	

Nodo B

	Oeste		Este	
	Org/Trm	VC	Org/Trm	VC
1	B	✓	B	
2	A	✓	A	
3	A		C	
4	A		B	
5	B		B	
6	C		B	

Nodo C

	Oeste		Este	
	Org/Trm	VC	Org/Trm	VC
1	B	✓	B	✓
2	A		A	
3	C		C	
4	C		D	
5	B		B	
6	C		C	

Nodo D

	Oeste		Este	
	Org/Trm	VC	Org/Trm	VC
1	D		B	
2	D		A	
3	C		A	✓
4	D		C	
5	B		A	
6	C		B	

T1516810-94/d16

Org Nodo en el que un HO VC entra en el anillo o es originado

Trm Nodo en el que un HO VC sale del anillo o es terminado

✓ Indica una AU organizada en LO VC

NOTA – La marcación de las AU para acceso de LO VC es facultativa. Todas las conexiones de este ejemplo son bidireccionales.

FIGURA 7-4/G.841

Representación conceptual de mapa de interconexión de nodos

## **Reemplazada por una versión más reciente**

Cuando no hay conmutaciones de protección activas en el anillo, cada nodo emite los bytes-K en cada sentido indicando que no hay petición de puenteo. Por lo general, los canales de protección que son originados en cada nodo contienen trayecto sin equipos, tal como se especifica en la Recomendación G.709. Este aspecto queda en estudio. La excepción es el tráfico adicional que puede añadirse, retirarse o transferirse de manera similar al tráfico de servicio. La identificación del tráfico adicional en el protocolo de APS de anillo queda en estudio.

Una conmutación puede ser iniciada mediante uno de los criterios especificados en 7.2. Un fallo del protocolo o controlador de APS no desencadenará una conmutación de protección. Sin embargo, se supone que se generarán las alarmas apropiadas.

Un anillo de dos fibras únicamente utiliza conmutaciones de anillo para restablecer el tráfico. Un anillo de cuatro fibras tiene la opción adicional de la conmutación de tramo. Específicamente, desde el punto de vista de un nodo en un anillo de cuatro fibras, existen dos canales de protección: un trayecto corto por el tramo utilizado en la conmutación de tramo y un trayecto largo por el camino largo alrededor del anillo utilizado en una conmutación de anillo. Con la conmutación de tramo, cada tramo de un anillo de cuatro fibras puede comportarse de manera similar a un sistema lineal protegido 1:1. Por consiguiente, los fallos que sólo afectan a los canales de servicio y no a los canales de protección pueden ser restablecidos utilizando una conmutación de tramo. En los anillos de cuatro fibras debe utilizarse, cuando sea posible, la conmutación de tramo, a fin de que puedan coexistir múltiples conmutaciones de tramo. Por lo tanto, la conmutación de tramo tiene prioridad con relación a la conmutación de anillo para las peticiones de puenteo del mismo tipo (por ejemplo, fallo de señal, degradación de señal, conmutación forzada). Las conmutaciones de tramo de prioridad inferior no se mantendrán en el caso de una petición de puenteo de anillo de prioridad superior.

Cuando un nodo determina que se requiere una conmutación, emite la petición de puenteo apropiada en los bytes-K en ambos sentidos, a saber, el trayecto corto y el trayecto largo.

En el caso de fallos unidireccionales, la señalización por el trayecto corto puede permitir que la conmutación sea completada más rápidamente. Habida cuenta de que el nodo a través del tramo que ha fallado verá por lo general mucho más pronto la petición de puenteo por el trayecto corto que la petición de puenteo por el trayecto largo, podrá iniciar sus propias peticiones de puenteo más rápidamente. En el caso de peticiones de puenteo de tramo en anillos de cuatro fibras, la señalización por el trayecto largo informa a los otros nodos del anillo que existe una conmutación de tramo en otro sitio del anillo. Este mecanismo niega las conmutaciones de anillo de prioridad inferior.

El nodo de destino es el nodo adyacente al nodo de origen a través del tramo que ha fallado. Cuando un nodo que no es el de destino recibe una petición de puenteo de prioridad superior, pasa al estado de transferencia apropiado. De esta manera, los nodos de conmutación pueden mantener una conmutación directa de los bytes-K por el trayecto largo. Se señala que en el caso de fallo bidireccional, tal como un corte de cable, el nodo de destino detectaría el fallo él mismo y emitiría una petición de puenteo en el sentido opuesto alrededor del anillo.

Cuando el nodo de destino recibe la petición de puenteo, realiza el puenteo. Si la petición de puenteo es del tipo anillo, el nodo puentea los canales que estaban entrando en el tramo que ha fallado, conectándolos a través de los canales de protección en el sentido opuesto. Además, para conmutaciones de anillo de fallo de señal, el nodo realiza también la conmutación a los canales de protección.

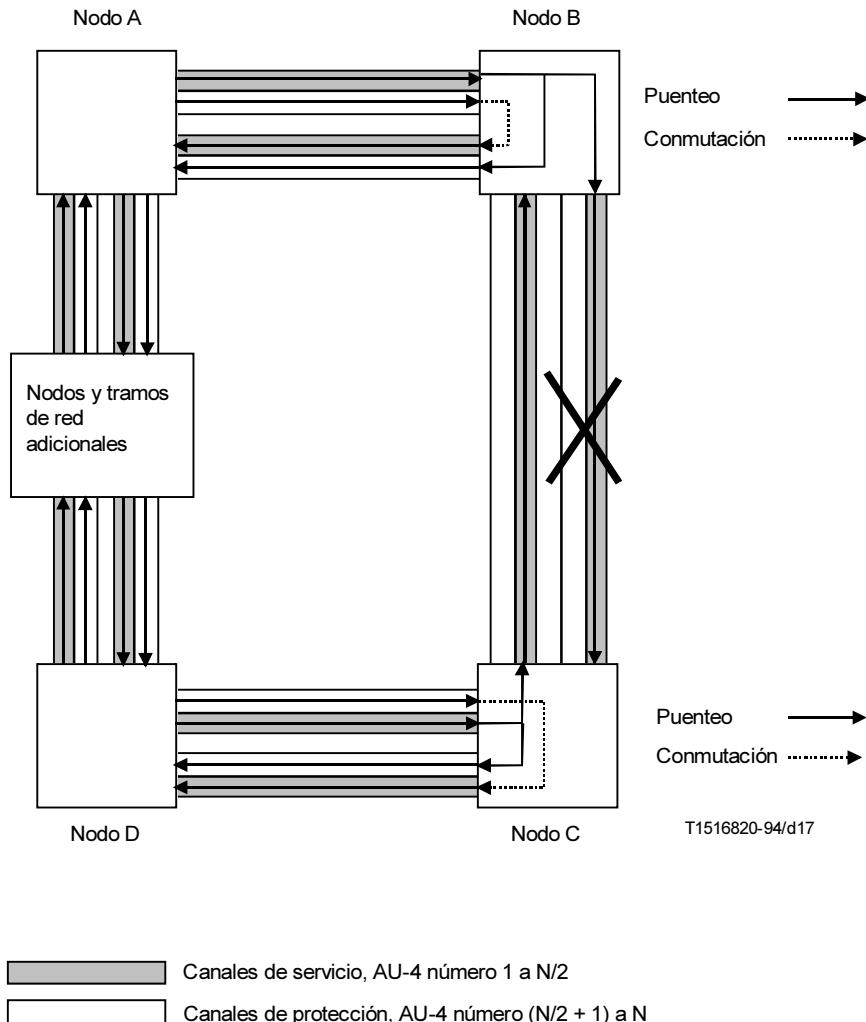
Considérese, por ejemplo, una sección de anillo que conste de cuatro nodos, A, B, C, D, en la que el tramo entre B y C haya fallado. Esta situación se ilustra en la Figura 7-5. En un anillo de dos fibras, B puenteará los canales AU-4 numerados de 1 a N/2 (servicio) que estaban siendo transmitidos de B a C por los canales AU-4 (N/2) + 1 a N (protección), transmitidos de B a A, y, alrededor del anillo, de regreso a C. Esta acción se denomina puenteo. C conmutará los canales de protección recibidos de B por conducto de A a los canales de servicio hacia D. Esta acción es la conmutación.

Si la conmutación de anillo de este ejemplo se lleva a cabo en un anillo de cuatro fibras, B puenteará los canales que estaban siendo transmitidos por la fibra de servicio de B a C hacia los canales transmitidos por la fibra de protección de B a A. De manera similar, C conmutará los canales de la fibra de protección recibidos de D a los canales transmitidos por la fibra de servicio a D.

El resultado final de este ejemplo es que todos los canales que estaban siendo enviados de B a C a través del tramo que ha fallado son ahora enviados de B a C por el camino largo alrededor del anillo a través de los nodos A y D. Se llevarán a cabo acciones simétricas para restablecer los canales que estaban siendo enviados de C a B.

## Reemplazada por una versión más reciente

Cuando el fallo haya sido eliminado, los nodos que originan las peticiones de puenteo suspenderán sus respectivas peticiones y commutaciones. Los otros nodos del anillo detendrán la transferencia de los canales de protección y los bytes-K. Por lo general, el tráfico sólo retorna de los canales de protección a los canales de servicio. Específicamente, en un anillo de cuatro fibras, si está activa una commutación de anillo en los canales de protección del trayecto largo, y quedan disponibles los canales de protección del trayecto corto, el servicio no será commutado a los canales de protección del trayecto corto a menos que una nueva petición de puenteo desplace con prioridad a los canales de protección del trayecto largo.



Las commutaciones de anillo y de tramo pueden ser desplazadas por peticiones de puenteo de prioridad superior, como se determina mediante el Cuadro 7-1. Considérese, por ejemplo, una commutación de tramo que está activa debido a una degradación de señal en ese tramo, y que por otra parte, se requiere una commutación de anillo debido a un fallo ocurrido en otro tramo que afecta tanto a los canales de servicio como a los canales de protección. Se generará una petición de puenteo de anillo, se suprimirá la commutación de tramo y se establecerá la commutación de anillo.

## **Reemplazada por una versión más reciente**

Si existe una commutación de anillo y se produce un fallo de igual prioridad en otro tramo que requiere una commutación de anillo, entonces, si la prioridad de la petición de puenteo es la de fallo de señal (anillo) o superior, se establecerán ambas commutaciones de anillo, lo que dará como resultado la segmentación del anillo en dos segmentos separados. De no ser así, si la prioridad de la petición de puenteo es inferior a la de fallo de señal (anillo), la nueva petición de puenteo no se establecerá y se suprimirá la primera commutación.

Por lo general, el funcionamiento adecuado del anillo se basa en el hecho de que todos los nodos tengan conocimiento del estado del anillo, de manera que no desplacen a una petición de puenteo, a menos que tengan una petición de puenteo de prioridad superior. Para hacer posible este conocimiento del estado del anillo, se utilizará la señalización por el trayecto largo durante una petición de puenteo, además de la señalización por el trayecto corto. Por ejemplo, si bien pueden establecerse puenteos de tramo con sólo señalización de trayecto corto, se envía una indicación de puenteo por el trayecto largo a fin de informar a los otros nodos acerca del estado del anillo. Además, los mensajes OAM&P transportados por el DCC pueden utilizarse para determinar los detalles relativos a la condición del anillo.

Para realizar una commutación de anillo, los canales de protección están compartidos esencialmente entre cada tramo del anillo. Asimismo, puede haber tráfico adicional en los canales de protección cuando éstos no se están utilizando para restablecer el tráfico de servicio transportado por los canales de servicio. Así, cada intervalo de tiempo de canal de protección es utilizado por múltiples servicios (servicios del mismo intervalo de tiempo pero en diferentes tramos, y servicio de tráfico adicional). Si no hay tráfico adicional en el anillo, en caso de fallos de múltiples puntos, tales como los que causan el aislamiento del o de los nodos, los servicios (del mismo intervalo de tiempo pero en diferentes tramos) pueden competir por el acceso al mismo intervalo de tiempo de canal de protección. Esto puede generar tráfico mal conectado. Si hay tráfico adicional en el anillo, incluso en caso de fallos de un solo punto, un servicio en los canales de servicio puede competir por el acceso al mismo intervalo de tiempo de canal de protección que transporta el tráfico adicional. Esto también puede dar lugar a tráfico mal conectado.

Sin un mecanismo que impida la conexión errónea, la situación siguiente podría dar lugar a conexiones erróneas. Refiriéndose a la Figura 7-6, un corte en ambos tramos entre los nodos A y F y entre los nodos A y B (que aísle el nodo A) hace que los circuitos Q y R intenten acceder al intervalo de tiempo #1P en los canales de protección.

Una posible conexión errónea se determina identificando los nodos que actuarán como nodos de commutación en caso de una petición de puenteo, y mediante el examen del tráfico que se verá afectado por la commutación. Los nodos de commutación pueden determinarse a partir de las direcciones de nodos en los bytes K1 y K2. Dichos nodos determinan el tráfico afectado por la commutación de protección a partir de la información contenida en sus mapas de anillo y a partir de las identificaciones de los nodos de commutación. Las posibles conexiones erróneas serán silenciadas insertando la AU-AIS apropiada en los intervalos de tiempo en que podría haber tráfico mal conectado. Para los anillos que funcionan en un nivel AU-4, este silenciamiento se produce en los nodos de commutación. Para los anillos que utilizan acceso de VC de orden inferior, están estudiándose los sitios de silenciamiento.

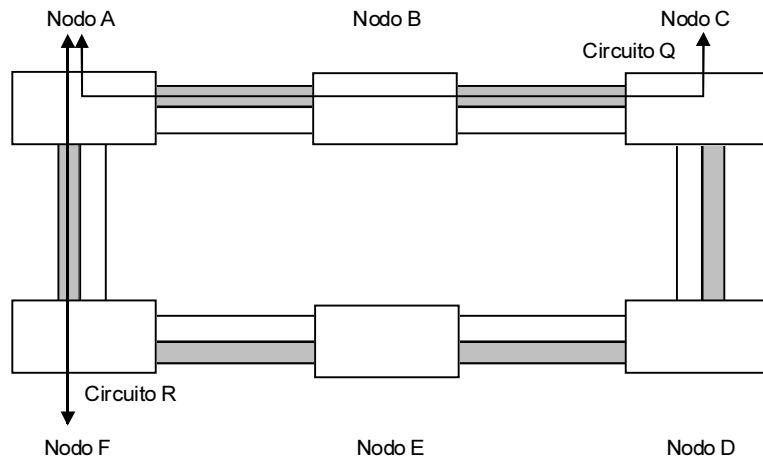
Considérese, por ejemplo, un segmento de anillo que consta de tres nodos, a saber, A, B y C, en el que B ha fallado. En una situación típica, tanto A como C enviarán peticiones de puenteo destinadas a B. Cuando A ve la petición de puenteo procedente de C, y observa que B está entre A y C (a partir del mapa de nodos), puede deducir que B está aislado del anillo. A y C utilizarán sus mapas respectivos para determinar qué canales son añadidos o retirados por B. A y C silenciarán estos canales antes de que se produzca la commutación de anillo insertando AU-AIS. Así, cualquier nodo del anillo que antes estaba conectado a B recibirá ahora AIS por esos canales.

Cada uno de los mapas de anillo, contendrá por lo menos:

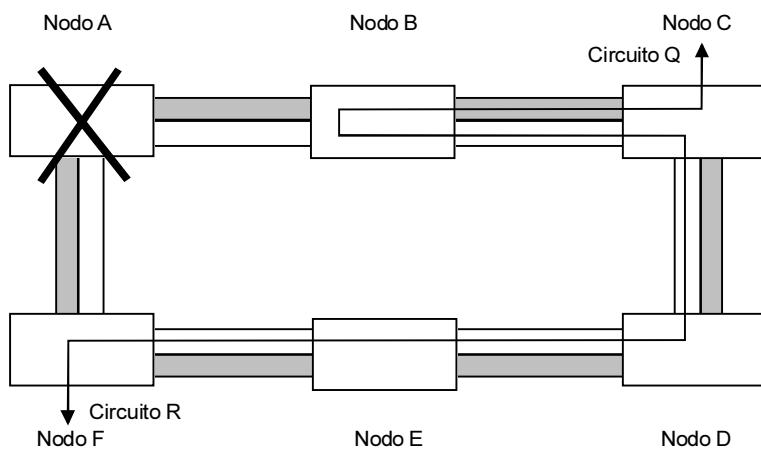
- 1) información relativa al orden en que los nodos aparecen en el anillo,
- 2) las asignaciones de intervalos de tiempo AU-4 para el tráfico que termina en ese nodo y lo atraviesa directamente,
- 3) para cada uno de estos intervalos de tiempo AU-4, las direcciones de nodo en las que el tráfico entra y sale del anillo; y
- 4) una indicación facultativa de si se está accediendo a la AU al nivel de VC de orden inferior en algún punto del anillo.

En las Figuras 7-3 y 7-4 se da un ejemplo de esos mapas de anillo. Están estudiándose los requisitos de los mapas para el acceso de VC de orden inferior y el tráfico adicional.

## Reemplazada por una versión más reciente



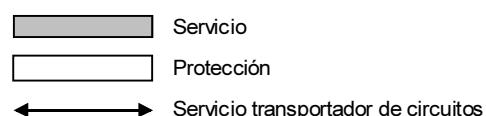
a) Estado normal antes de fallo de nodo



T15 16830-94/d 18

b) Conexión incorrecta después de fallo de nodo

Círculo	Asignación de intervalos de tiempo	Canal
Q	1W	Servicio
R	1W	Servicio



NOTA – En la columna «asignación de intervalos de tiempo», la designación «1W» indica que es el primer intervalo de tiempo de la capacidad reservada para tráfico de servicio.

FIGURA 7-6/G.841

Ejemplo de conexión incorrecta

# Reemplazada por una versión más reciente

## 7.2.4 Criterios para la iniciación de la conmutación

Las peticiones de realización de conmutación de protección pueden ser iniciadas externamente o automáticamente. Las instrucciones iniciadas externamente son introducidas mediante el sistema operativo (OS) o la interfaz humana. En 7.2.4.1 se describen estas instrucciones iniciadas externamente y de las cuales dispone el OS, la interfaz humana o ambas interfaces. Las instrucciones iniciadas automáticamente pueden ser iniciadas también en base a criterios de calidad de funcionamiento de sección de multiplexación y equipos. En 7.2.4.2 se indican los criterios de las instrucciones iniciadas automáticamente.

Las peticiones de puenteo relativas a la conmutación de tramo (salvo para la exclusión de la protección) se utilizan sólo para anillos de protección compartida de sección de multiplexación de cuatro fibras.

El código ausencia de petición (NR) se transmite cuando no es necesario utilizar los canales de protección.

### 7.2.4.1 Instrucciones iniciadas externamente

Las peticiones de puenteo externas son iniciadas en un NE por el OS o el operador. La petición de puenteo externa puede ser transmitida al NE apropiado mediante los bytes de APS o la TMN o por la interfaz manual local. Las peticiones de puenteo son evaluadas por el algoritmo de prioridad en el controlador de conmutación de protección.

#### 7.2.4.1.1 Instrucciones no señaladas por el canal de APS

A continuación se describen las instrucciones iniciadas externamente.

**7.2.4.1.1.1 eliminación:** Esta instrucción elimina la instrucción y el WTR iniciados externamente en el nodo al que estaba dirigida la instrucción. La señalización de NE a NE que sigue a la eliminación de las instrucciones iniciadas externamente se realiza mediante el código NR.

Las dos instrucciones siguientes son útiles si un tramo tiene excesiva conmutación a protección. Otra utilización de estas instrucciones incluye la exclusión del acceso a protección para algunos tramos que cursan sólo tráfico que no necesita protección. Las instrucciones no son críticas con relación al tiempo (es decir, no necesitan ser completadas en decenas de milisegundos). Así, pueden ser transmitidas por el DCC.

**7.2.4.1.1.2 exclusión de los canales de servicio – conmutación de anillo:** Esta instrucción impide que los canales de servicio del tramo direccional accedan a los canales de protección para una conmutación de anillo, inhabilitando la capacidad del nodo para solicitar una conmutación de protección de anillo de cualquier clase que sea. Si ya hay tráfico de servicio en los canales de protección, el puenteo del anillo es eliminado, independientemente de la condición de los canales de servicio. Si ninguna otra petición de puenteo está activa en el anillo, se transmite el código NR. Esta instrucción no tiene repercusiones sobre la utilización de los canales de protección para cualquier otro tramo. Por ejemplo, el nodo puede pasar a cualquiera de los modos de transferencia.

**7.2.4.1.1.3 exclusión de los canales de servicio – conmutación de tramo:** Esta instrucción impide que los canales de servicio del tramo direccional accedan a los canales de protección para una conmutación de tramo. Si ya hay tráfico de servicio en los canales de protección, se elimina la conmutación de tramo independientemente de la condición de los canales de servicio. Si no está activa ninguna otra petición de puenteo en el anillo, se transmite el código NR. Esta instrucción no tiene repercusiones sobre la utilización de los canales de protección para cualquier otro tramo.

**7.2.4.1.1.4 exclusión de protección – todos los tramos:** Esta instrucción impide la conmutación de protección en todo el anillo. Si hay tráfico de servicio por los canales de protección de cualquier tramo, esta instrucción hace que dicho tráfico se commute de nuevo a los canales de servicio, independientemente de la condición de los canales de trabajo. Se señala que los bytes K1 y K2 no soportan esta instrucción. Así pues, la instrucción ha de ser enviada a cada uno de los NE y la petición de exclusión de protección – tramo es utilizada por cada NE para coordinar las actividades con el extremo distante.

#### 7.2.4.1.2 Instrucciones que utilizan los bytes de APS

Las instrucciones siguientes son transmitidas por los bytes de APS:

**7.2.4.1.2.1 exclusión de protección – tramo (LP-S):** Esta instrucción impide la utilización del tramo para cualquier actividad de protección. Si ya hay tráfico de servicio por los canales de protección de este tramo, esta instrucción hace que dicho tráfico pase de nuevo a los canales de servicio. Así, pues, toda conmutación de anillo que utiliza la capacidad de protección del tramo excluido es impedida (y desplazada con prioridad), y la conmutación de tramo es impedida únicamente en el tramo excluido.

## **Reemplazada por una versión más reciente**

**7.2.4.1.2.2 conmutación forzada de servicio a protección – anillo (FS-R):** Esta instrucción efectúa la conmutación de anillo desde los canales de servicio a los canales de protección para el tramo incluido entre el nodo en el que es iniciada la instrucción y el nodo adyacente al que va destinada. Esta conmutación ocurre independientemente del estado de los canales de protección, a menos que estén cumplimentando una petición de puenteo de prioridad superior.

**7.2.4.1.2.3 conmutación forzada de servicio a protección – tramo (FS-S):** Esta instrucción conmuta el tráfico de los canales de servicio a los canales de protección de ese tramo. Esta conmutación ocurre independientemente del estado de los canales de protección, a menos que estén cumplimentando una petición de puenteo de prioridad superior, o que exista un fallo de señal (o un fallo de byte K) en los canales de protección del tramo.

**7.2.4.1.2.4 conmutación manual – anillo (MS-R):** Esta instrucción efectúa la conmutación de anillo de los canales de servicio a los canales de protección para el tramo incluido entre el nodo en el que es iniciada la instrucción y el nodo adyacente al que va destinada. Esta conmutación ocurre si los canales de protección no están en una condición SD y no están cumplimentando una petición de puenteo de prioridad igual o superior (incluido el fallo de los canales de protección).

**7.2.4.1.2.5 conmutación manual – tramo (MS-S):** Esta instrucción conmuta el tráfico de los canales de trabajo a los canales de protección para el mismo tramo por el que es iniciada la instrucción. Esta conmutación ocurre si los canales de protección no están en una condición SD y no están cumplimentando una petición de puenteo de prioridad igual o superior (incluido el fallo de los canales de protección).

**7.2.4.1.2.6 ejercicio – anillo (EXER-R):** Esta instrucción ensaya la conmutación de protección de anillo del canal solicitado sin completar el puenteo y la conmutación reales. Se emite la instrucción y se comprueban las respuestas, pero el tráfico de trabajo no es afectado.

**7.2.4.1.2.7 ejercicio – tramo (EXER-S):** Esta instrucción ensaya la protección de tramo del canal solicitado sin completar el puenteo y la conmutación reales. Se emite la instrucción y se comprueban las respuestas, pero el tráfico de trabajo no es afectado.

NOTA – Los fallos no detectados constituyen un problema, dado que no se manifiestan por sí mismos hasta el momento en que se hace una conmutación, por lo cual la facilidad de protección estará indisponible cuando más se necesite. En un anillo de protección compartida de MS la función de ejercicio es aún más esencial, ya que la facilidad de protección está compartida entre todos los nodos del anillo. Un fallo no detectado en un tramo hace imposible la conmutación de anillo para todos los tramos del anillo. Así pues, la probabilidad de que haya fallos no detectados se reduce al ensayar el controlador de conmutación de protección. Si se detecta un fallo del controlador durante un ejercicio o diagnóstico de rutina, no se inicia ninguna petición de conmutación de protección, a menos que el fallo afecte al servicio. Se genera una alarma para facilitar la pronta reparación.

### **7.2.4.2 Instrucciones iniciadas automáticamente**

Las peticiones de APS son iniciadas también en base a criterios de calidad de funcionamiento de equipo y de sección multiplexación detectados por el NE. Todos los canales de servicio y de protección son supervisados independientemente de las condiciones de fallo o degradación (es decir, toda la supervisión de calidad de funcionamiento apropiada continúa después de la compleción de una conmutación). El NE inicia automáticamente las siguientes peticiones de puenteo: fallo de señal (SF), degradación de señal (SD), invertir petición (RR) y espera al restablecimiento (WTR). Las peticiones de puenteo son transmitidas de NE a NE (y no de OS a NE).

La petición de puenteo SF se utiliza para proteger el tráfico de servicio afectado por un fallo grave, mientras que la petición de puenteo SD se utiliza para proteger contra un fallo de poca gravedad. Las peticiones de puenteo son transmitidas, tanto por el trayecto corto como el trayecto largo. Cada nodo intermedio verifica la ID del nodo de destino de la petición de puenteo de trayecto largo y retransmite la petición de puenteo. El nodo de destino recibe la petición de puenteo, realiza la actividad de conformidad con el nivel de prioridad, y envía la indicación de puenteo.

La petición de puenteo WTR se utiliza para evitar la oscilación frecuente entre los canales de protección y los canales de servicio. Tiene como objetivo minimizar el número de oscilaciones, dado que se producen perturbaciones momentáneas durante la conmutación. La petición de puenteo WTR es emitida tras la eliminación de la condición de defecto en los canales de servicio. La WTR es emitida únicamente después de una condición SF o SD y, de esta manera, no se aplica a las peticiones de puenteo iniciadas externamente.

A continuación se definen las peticiones de puenteo iniciadas automáticamente y sus condiciones de ocurrencia.

## **Reemplazada por una versión más reciente**

**7.2.4.2.1 fallo de señal – tramo (SF-S):** El SF se define en la Recomendación G.783. El extremo de cola detecta el fallo y genera la petición de puenteo. Para los anillos de cuatro fibras, si el fallo afecta únicamente a los canales de servicio, el tráfico puede restablecerse comutando a los canales de protección del mismo tramo. La petición de puenteo SF-S se utiliza para iniciar la comutación de tramo para un SF en los canales de servicio de un anillo de cuatro fibras.

**7.2.4.2.2 fallo de señal – anillo (SF-R):** Para los anillos de dos fibras, todos los SF (definidos anteriormente para la comutación de tramo) son protegidos utilizando la comutación de anillo. Para los anillos de cuatro fibras, la comutación de anillo se utiliza únicamente si el tráfico no puede restablecerse mediante la comutación de tramo. Si existen fallos, tanto en los canales de servicio como de protección en un tramo, es necesario iniciar una petición de puenteo de anillo. Por consiguiente, esta instrucción se utiliza para solicitar la comutación de anillo para fallos de señal.

**7.2.4.2.3 fallo de señal – protección (SF-P):** Esta instrucción se utiliza para indicar a un nodo adyacente que los canales de protección están en un estado de fallo de señal. Un fallo de señal de los canales de protección es equivalente a una exclusión de la protección para el tramo que es afectado por el fallo. Por lo tanto, el byte K1 que es transmitido al nodo adyacente tiene el mismo código que el de un bloqueo de la protección – tramo. SF-P se utiliza únicamente para anillos de cuatro fibras.

**7.2.4.2.4 degradación de señal – tramo (SD-S):** La degradación de señal se define en la Recomendación G.783. En los anillos de cuatro fibras, los canales de servicio del tramo degradado pueden ser protegidos utilizando los canales de protección del mismo tramo. Esta petición de puenteo se utiliza para conmutar el tráfico de servicio a los canales de protección en el mismo tramo en el que está situado el fallo.

**7.2.4.2.5 degradación de señal – anillo (SD-R):** Para los anillos de dos fibras, cualquier sección de multiplexación degradada es protegida utilizando la comutación de anillo. (La degradación se define más arriba: véase degradación de señal-tramo.) Para los anillos de cuatro fibras, esta petición de puenteo se utiliza cuando los canales de servicio están degradados y los canales de protección del mismo tramo están degradados o no están disponibles.

**7.2.4.2.6 degradación de señal – protección (SD-P):** Esta instrucción se utiliza cuando un NE detecta una degradación en sus canales de protección, y no existen peticiones de comutación de prioridad mayor en los canales de servicio. (La degradación se define más arriba: véase degradación de señal - tramo.) Esta petición de puenteo se utiliza únicamente para anillos de cuatro fibras.

**7.2.4.2.7 invertir petición – tramo (RR-S):** Esta instrucción es transmitida al NE del extremo de cola como un acuse de recibo de la petición de puenteo de tramo por el trayecto corto. Sólo se transmite por el trayecto corto.

**7.2.4.2.8 invertir petición – anillo (RR-R):** Esta instrucción es transmitida al NE del extremo de cola por el camino corto como acuse de recibo de la petición de puenteo de anillo por el trayecto corto.

**7.2.4.2.9 espera al restablecimiento (WTR):** Esta instrucción es emitida cuando los canales de trabajo encuentran el umbral de restablecimiento después de una condición SD o SF. Se utiliza para mantener el estado durante el periodo de WTR, a menos que sea desplazada por una petición de puenteo de prioridad mayor.

### **7.2.5 Protocolo de comutación de protección**

Se utilizarán dos bytes de APS, a saber K1 y K2, para la comutación de protección. Véase 7.2.6 para mayores detalles sobre la utilización operacional de estos bytes.

Los bytes K1 y K2 serán transmitidos en la tara de la sección de multiplexación del STM-N que transporta los canales de protección. Se señala, no obstante, que los bits 6-8 del byte K2 se utilizan en todas las señales de línea STM-N para señalar MS-RDI y MS-AIS.

## Reemplazada por una versión más reciente

### 7.2.5.1 Byte K1

Estos bits serán asignados conforme al Cuadro 7-1. Los bits 1-4 del byte K1 transportan códigos de petición de puenteo, enumerados por orden de prioridad descendente en el Cuadro 7-1. Los bits 5-8 del byte K1 transportan la ID del nodo de destino para el código de petición de puenteo que se indica en los bits 1-4 del byte K1.

CUADRO 7-1/G.841

#### Funciones del byte K1

Código de petición de puenteo (bits 1-4)				Identificación de nodo de destino (bits 5-8)			
Bit 1	Bit 2	Bit 3	Bit 4	Bit 5	Bit 6	Bit 7	Bit 8
1111	Exclusión de protección (tramo) LP-S o fallo de señal (protección) SF-P				La ID de nodo de destino se fija al valor de la ID del nodo para el que está destinado ese byte K1. La ID de nodo de destino es siempre la de un nodo adyacente (salvo para bytes APS por defecto).		
1110	Conmutación forzada (tramo) FS-S						
1101	Conmutación forzada (anillo) FS-R						
1100	Fallo de señal (tramo) SF-S						
1011	Fallo de señal (anillo) SF-R						
1010	Degradoación de señal (protección) SD-P						
1001	Degradoación de señal (tramo) SD-S						
1000	Degradoación de señal (anillo) SD-R						
0111	Conmutación manual (tramo) MS-S						
0110	Conmutación manual (anillo) MS-R						
0101	Espera de restablecimiento WTR						
0100	Ejercicio (tramo) EXER-S						
0011	Ejercicio (anillo) EXER-R						
0010	Invertir petición (tramo) RR-S						
0001	Invertir petición (anillo) RR-R						
0000	Ninguna petición NR						

NOTA – La instrucción invertir petición supone la prioridad de la petición de puenteo a la que responde.

### 7.2.5.2 Byte K2

El byte K2 se codificará de conformidad con el Cuadro 7-2.

# Reemplazada por una versión más reciente

CUADRO 7-2/G.841

## Funciones del byte K2

Identificación de nodo de origen (bits 1-4)				Largo/corto	Situación (bits 6-8)			
Bit 1	Bit 2	Bit 3	Bit 4		Bit 5	Bit 6	Bit 7	Bit 8
La ID del nodo de origen se fija a la ID del propio nodo				Situación:				
				111 MS-AIS				
				110 MS-RDI				
				101 Reservado para uso futuro				
				100 Reservado para uso futuro				
				011 Reservado para uso futuro				
Largo/corto (bit 5):				010 Puenteado y conmutado (Br&Sw)				
0 = Código de trayecto corto (S)				001 Puenteado (Br)				
1 = Código de trayecto largo (L)				000 Reposo				

### 7.2.6 Funcionamiento del algoritmo de protección

Esta subcláusula está estructurada de la manera siguiente:

Primero se dan algunas reglas generales relativas al algoritmo de APS, después de lo cual se dan las reglas detalladas. La primera subsección abarca las tres clases de estados de APS de nodo de anillo, así como el comportamiento en régimen permanente del nodo en estos estados. La segunda subsección describe las reglas de transición entre los diferentes estados de APS de nodo de anillo.

Estas reglas se aplican conceptualmente a un controlador de APS de anillo de protección compartida de MS que funciona en un nodo. Se trata de escoger las acciones de conmutación y señalización para ambos lados del nodo, en base a toda la señalización de bytes K entrante en ambos sentidos, los fallos detectados en ambos lados, los fallos de equipos locales y las instrucciones iniciadas externamente. Por lo general, este controlador conceptual examina toda la información entrante, escoge la entrada de prioridad mayor y realiza una acción en base a dicha elección.

La Figura 7-7 ilustra el funcionamiento conceptual de un controlador de APS de anillo de protección compartida de sección múltiple.

Se aplica el siguiente conjunto de reglas generales:

**Regla G #1 – VALIDACIÓN DE PETICIÓN DE PUENTE** (definiciones de petición de puenteo y situación de petición de puenteo):

**Regla G #1a – (petición de puenteo)**

La información contenida en los bits 1-4 del byte K1 se considerará como una petición de puenteo si:

- estos bits indican uno de los códigos de petición de puenteo de anillo y el bit 5 del byte K2 indica un código de trayecto largo, o
- estos bits indican uno de los códigos de petición de puenteo de anillo y el bit 5 del byte K2 indica un código de trayecto corto, o
- estos bits indican uno de los códigos de petición de puenteo de tramo y el bit 5 del byte K2 indica un código de trayecto corto.

## Reemplazada por una versión más reciente

**Regla G #1b** – (situación de petición de puenteo).

La información contenida en los bits 1-4 del byte K1 se considerará como una situación de petición de puenteo si:

- estos bits indican uno de los códigos de petición de puenteo de tramo y el bit 5 del byte K2 indica un código de trayecto largo.

En el Cuadro 7-3 se indica la relación entre códigos de petición de puenteo, códigos de situación de petición de puenteo e indicaciones de bytes K.

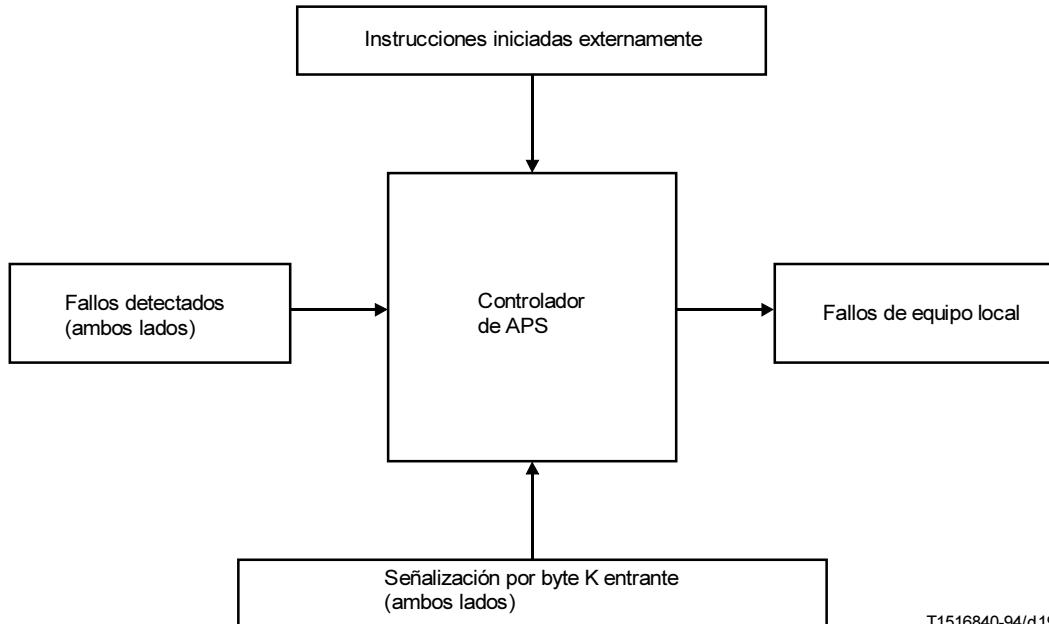


FIGURA 7-7/G.841  
Controlador de APS de anillo de protección compartida de MS conceptual

CUADRO 7-3/G.841

### Relaciones entre el bit 5 del byte K2 y los bits 1-4 del byte K1

Bits 1-4 del byte K1		
Código del bit 5 del K2	Código de puenteo de anillo	Código de puenteo de tramo
Trayecto largo	Petición de puenteo	Situación de petición de puenteo
Trayecto corto	Petición de puenteo	Petición de puenteo

Se señala que las señales MS-RDI y MS-AIS terminan en los elementos de terminación de sección de multiplexación, tal como se especifica en la Recomendación G.783.

## Reemplazada por una versión más reciente

### 7.2.6.1 Estado de APS de nodo de anillo

Hay tres clases de estado de nodo de anillo: reposo, conmutación y transferencia.

#### 7.2.6.1.1 Estado de reposo

Un nodo se encuentra en el estado de reposo cuando no está generando, detectando ni transfiriendo peticiones de puenteo o códigos de estado de petición de puenteo.

**Regla I #1 – BYTES K GENERADOS EN EL ESTADO DE REPOSO:** Los nodos que estén en el estado de reposo generarán los bytes K en ambos sentidos, tal como se indica en el Cuadro 7-4.

CUADRO 7-4/G.841

#### Valores de los bytes K1 y K2 generados en el estado de reposo

K1 [1-4]	=	0000 (código ninguna petición)
K1 [5-8]	=	ID de NODO de destino
K2 [1-4]	=	ID de NODO de origen
K2 [5]	=	0 (código trayecto corto)
K2 [6-8]	=	000 (código reposo)

El nodo se comportará de conformidad con la regla I-S #3 hasta que tenga conocimiento del mapa del anillo. Queda para ulterior estudio la señalización en el estado de arranque.

**Regla I #2 – BYTES K RECIBIDOS EN EL ESTADO DE REPOSO:** Los nodos que estén en el estado de reposo terminarán los bytes K1 y K2 en ambos sentidos.

#### 7.2.6.1.2 Estado de conmutación

Un nodo está en un estado de conmutación cuando origina una petición de puenteo (automáticamente o externamente) o termina una petición de puenteo.

**Regla S #1 – BYTES K ORIGINADOS EN EL ESTADO DE CONMUTACIÓN:**

**Regla S #1a –** Cualquier nodo en el estado de conmutación originará bytes K tal como se muestra en el Cuadro 7-5:

CUADRO 7-5/G.841

#### Valores de los bytes K1 y K2 originados por un nodo en el estado de conmutación

K1 [1-4]	=	código PETICIÓN DE PUENTEO
K1 [5-8]	=	ID de NODO de destino
K2 [1-4]	=	ID de NODO de origen
K2 [5]	=	0/1 (código de trayecto corto/largo)
K2 [6-8]	=	código SITUACIÓN

## Reemplazada por una versión más reciente

**Regla S #1b** – Cualquier nodo en el estado de conmutación (para peticiones de puenteo de tramo o de anillo) originará una petición de puenteo en el trayecto corto y una petición de puenteo en el trayecto largo. Ambas peticiones de puenteo tienen la misma prioridad (o una de ellas es invertir petición), y protegen el mismo tramo. Las excepciones son el caso de nodo aislado, el caso de una petición de puenteo de tramo en cada lado del nodo, el caso de una petición de puenteo de anillo que desplaza con prioridad a una petición de puenteo de tramo en un tramo adyacente y el caso en que existe un puenteo de anillo en un tramo excluido. Véanse en la Figura 7-8 los casos de señalización de nodo aislado.

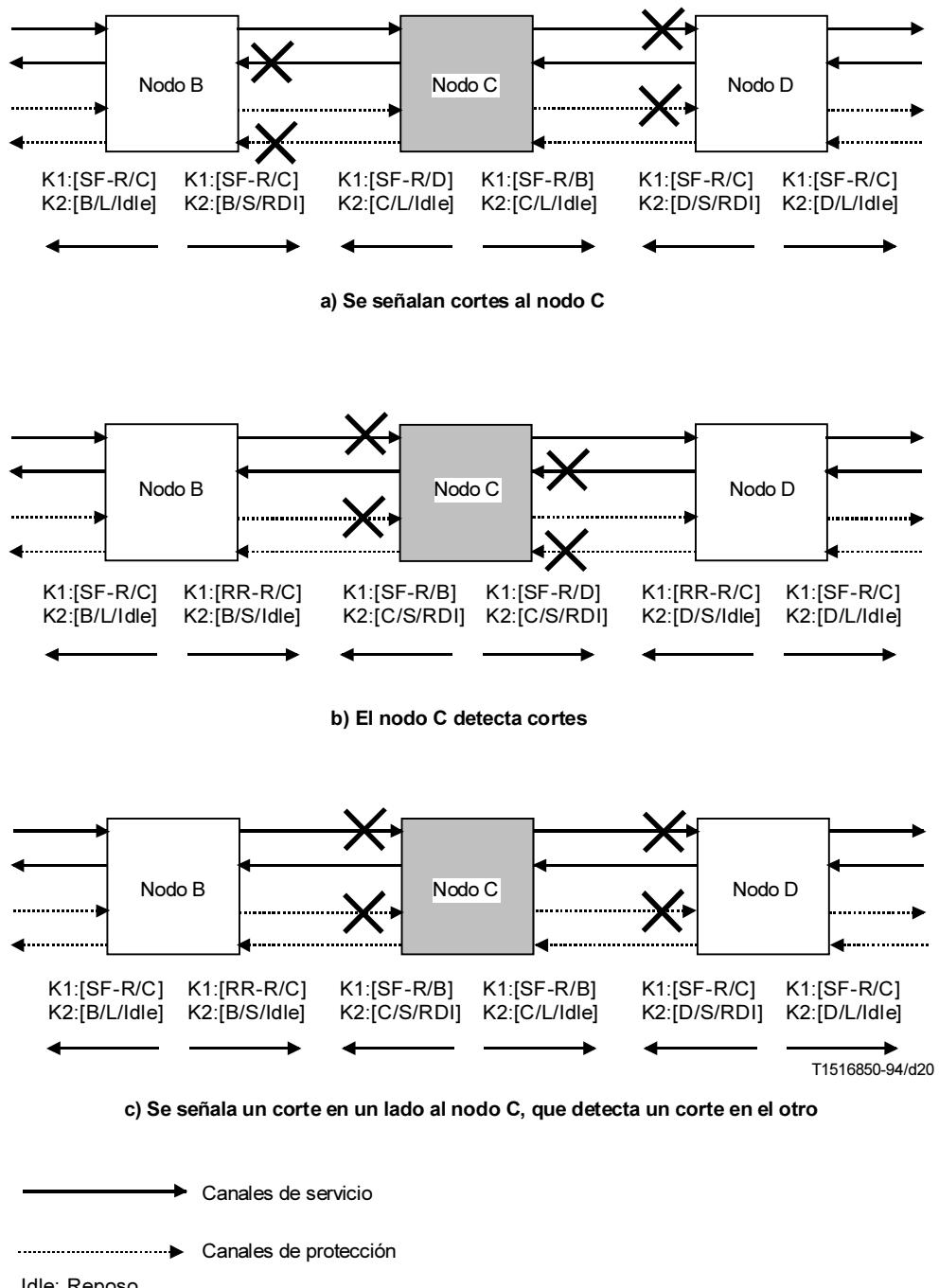


FIGURA 7-8/G.841

Señalización de nodo aislado (estados de señalización antes de que los nodos B y D establezcan un puenteo y una conmutación de anillo)

## Reemplazada por una versión más reciente

**Regla S #1c** – Cuando un nodo en el estado de conmutación termine una nueva petición de puenteo de byte K por trayecto corto procedente de un nodo adyacente, de prioridad igual o mayor que la petición de puenteo a la que está dando cumplimiento en esos momentos, en el mismo tramo, originará una petición de puenteo de la misma prioridad por el trayecto largo correspondiente. Cuando un nodo reciba peticiones de puenteo de anillo por ambos trayectos cortos procedentes de sus nodos adyacentes, indicando que las dos señales que está enviando han fallado (SF), la petición de puenteo de trayecto largo pasará a tener precedencia con respecto a las de invertir petición de trayecto corto. Esta regla adquiere precedencia con respecto a la Regla S #1b en caso de peticiones de puenteo múltiples en el mismo nodo [véase la Figura 7-8 parte a)].

**Regla S #1d** – Cuando un nodo detecte un fallo entrante en los canales de servicio y de protección, originará siempre, por el trayecto corto, una petición de puenteo de anillo de trayecto corto, incluso en el caso de fallos múltiples, mientras la petición de anillo no sea desplazada por una petición de puenteo de anillo de prioridad mayor [véase la Figura 7-8 parte b)]. Esta regla tiene precedencia con respecto a la regla S #1c. Se señala que siempre que un nodo reciba en un sentido una petición de puenteo de anillo por el trayecto corto (indicando que la señal que está enviando ha fallado) y detecte en el otro un fallo entrante en los canales de servicio y de protección, señalará el fallo detectado por ambos trayectos, el corto y el largo [véase la Figura 7-8 parte c)].

**Regla S #2** – BYTES K RECIBIDOS EN EL ESTADO DE CONMUTACIÓN: Cualquier nodo en el estado de conmutación terminará K1 y K2 en ambos sentidos.

**Regla S #3** – ACUSE DE RECIBO DE PETICIÓN DE PUENTE UNIDIRECCIONAL: Tan pronto como reciba una petición de puenteo o una situación de petición de puenteo, el nodo al que va dirigida acusará recibo de la petición de puenteo cambiando los bytes 1-4 de K1 al código invertir petición en el trayecto corto y a la prioridad de la petición de puenteo recibida en el trayecto largo.

**Regla S #4** – CONMUTACIONES DE PROTECCIÓN COMPLETADAS COEXISTENTES PERMITIDAS:

**Regla S #4a** – Está permitido que coexistan las siguientes conmutaciones:

- LP-S o SD-P con cualquier conmutación de tramo;
- LP-S o SD-P con cualquier conmutación de anillo en el mismo tramo;
- LP-S con SD-P;
- LP-S con LP-S;
- FS-R con FS-R (división del anillo en múltiples subanillos);
- SF-R con SF-R (división del anillo en múltiples subanillos);
- FS-R con SF-R (división del anillo en múltiples subanillos);
- Cualquier conmutación de tramo con cualquier otra conmutación de tramo.

**Regla S #4b** – Cuando existan al mismo tiempo múltiples peticiones de puenteo de igual prioridad en tramos diferentes de SD-R, MS-R o EXER-R, no se efectuará ningún puenteo o conmutación y se suprimirán las conmutaciones y los puenteos existentes. (Se señala que en caso de fallos SD-R múltiples, todos ellos serán notificados o señalados con alarma. No obstante, este comportamiento puede ser considerado como previsto por el usuario.) Los nodos señalarán la petición de puenteo de anillo en el byte K1 y los bits 6-8 del byte K2 se fijarán a reposo.

**Regla S #5** – PÉRDIDA DE PETICIÓN DE PUENTE DE ANILLO: Si un nodo que efectúa un puenteo y conmutación de anillo ya no recibe una petición de puenteo de anillo válida en el trayecto largo, retirará su puenteo y conmutación de anillo y señalizará y actuará conforme a su entrada de máxima prioridad. Se señala que invertir petición y otras peticiones de puenteo de anillo coexistentes permitidas con un código de trayecto corto se consideran peticiones de puenteo de anillo válidas.

**Regla S #6** – PÉRDIDA DE PETICIÓN DE PUENTE DE TRAMO: Si un nodo que efectúa un puenteo y conmutación de tramo ya no recibe una petición de puenteo de tramo válida (en el trayecto corto), retirará su puenteo y conmutación de tramo y señalizará y actuará conforme a su entrada de prioridad máxima.

### 7.2.6.1.3 Estado de transferencia

Un nodo está en el estado de transferencia cuando transmite por un lado la totalidad o parte de los bytes K1 y K2, y posiblemente los canales de protección, que recibe por el otro lado. Hay dos tipos de transferencia: total y de byte K (véase en la cláusula 3 la definición de las diferentes clases de transferencia).

## Reemplazada por una versión más reciente

**Regla P #1 – BYTES K ORIGINADOS Y RECIBIDOS EN EL ESTADO DE TRANSFERENCIA:** Cuando un nodo está en el estado de transferencia, transmite por un lado la totalidad o parte de los bytes K1 y K2 que recibe por el otro lado. La parte de K1 y K2 que se transfiere depende de las reglas de transición de estado.

**Regla P #2 – PERMANENCIA EN EL ESTADO DE TRANSFERENCIA DURANTE LAS TRANSICIONES DE SEÑALIZACIÓN:** Cuando un nodo que esté en un estado de transferencia reciba una petición de puenteo de anillo de trayecto largo destinado a él mismo y otra petición de puenteo de anillo de trayecto largo de la misma prioridad destinada a otro nodo, no pasará a otro estado. (Esta regla es necesaria para la secuencia de eliminación (liberación) de la condición de fallo de nodo. Véase la Figura I.5.) Una mayor aclaración de esta regla queda para un estudio ulterior.

### 7.2.6.2 Reglas de transición de estado de APS de nodo de anillo

En la subcláusula anterior se han descrito los tres estados de nodo de anillo. En la presente se describen las reglas de transición entre estos estados diferentes. Se señala que, al igual que en la APS lineal, se aplican las siguientes reglas básicas:

**Regla básica #1 – PROVOCACIÓN DE TRANSICIÓN DE ESTADO:** Toda transición de estado es provocada por un cambio de byte K entrante, una expiración de WTR, una petición de puenteo iniciada externamente o un fallo detectado localmente.

**Regla básica #2 – VALIDACIÓN DE BYTES K:** Antes de aceptar los bytes K como válidos, el valor deberá ser recibido idénticamente en tres tramas sucesivas.

**Regla básica #3 – ACTUALIZACIÓN DE LOS BITS 6-8 DE K2:** Todas las acciones de puenteo y conmutación deberán quedar reflejadas por la actualización de los bits 6-8 del byte K2, a menos que exista una condición MS-RDI. La condición MS-RDI hará que el código MS-RDI invalide todos los demás códigos de los bits 6-8 del byte K2 del tramo en fallo (excepto MS-AIS), con independencia del estado del puenteo y la conmutación.

**Tipos de mapa de anillo** – Cada nodo de un anillo mantendrá un mapa de anillo describiendo la conectividad del anillo y un mapa de interconexión local indicando el origen y el destino de todas las AU-3/4 añadidas, extraídas y transferidas. Además, los nodos de un anillo que soporten accesos de VC de orden inferior en el futuro deberán incluir una indicación en el mapa del anillo de cuáles AU-3/4 de transferencia tienen acceso de VC de orden inferior.

**Silenciamiento de AU-3/4** – El silenciamiento de las AU-3/4 se efectuará en los nodos conmutantes insertando AU-AIS. El nodo conmutante identificará, comparando direcciones de bytes K (bytes K cruzados) con la información contenida en el mapa de anillo, los nodos que faltan. A partir de esta información y del mapa de interconexión deberá identificar qué AU-3/4 han sido añadidas en estos nodos y cuáles se han retirado de los mismos y las silenciará bidireccionalmente.

Además, los nodos de los anillos que soporten acceso de VC de orden inferior en el futuro deberán silenciar bidireccionalmente todas las AU-3/4 con acceso de VC de orden inferior (como se indica en el mapa del anillo). Tras recibir el código de puenteado y conmutado procedente del nodo conmutante del extremo distante los nodos de anillos que soporten acceso de VC de orden inferior en el futuro deberán detener el silenciamiento de las AU-3/4 que tengan acceso de VC de orden inferior. El acceso de LO VC queda en estudio.

**Regla básica S #4:** Las peticiones de puenteo (en razón de un fallo detectado localmente, de una instrucción iniciada externamente o de bytes K recibidos) desplazarán a las peticiones de puenteo en el orden de prioridades que se indica en el Cuadro 7-1, a menos que las peticiones de puenteo estén autorizadas a coexistir. Las peticiones de puenteo desplazarán a la señalización de situación de peticiones de puenteo con independencia de la prioridad de cada una de ellas. Una señalización de situación de petición de puenteo nunca desplazará con prioridad a una petición de puenteo.

### 7.2.6.2.1 Transiciones entre estados de reposo y de transferencia

**Regla I-P #1 – TRANSICIÓN DEL ESTADO DE REPOSO AL ESTADO DE TRANSFERENCIA:**

**Regla I-P #1a** – La transición del estado de reposo a los estados de transferencia total o de transferencia de byte K será provocada por un cambio de byte K válido, en cualquier sentido, del código ninguna petición a cualquier otro código de petición de puenteo, en tanto en cuanto la nueva petición de puenteo no esté destinada al propio nodo. Ambos sentidos irán a continuación hacia transferencia total o transferencia de byte K, de acuerdo con la regla I-P #1b.

## Reemplazada por una versión más reciente

**Regla I-P #1b** – Para cualquier petición de puenteo de anillo, los nodos intermedios del trayecto largo irán hacia transferencia total. Cualquiera que sea la situación de petición de puenteo de tramo, el nodo intermedio del trayecto largo irá hacia transferencia de byte K.

**Regla I-P #2** – TRANSICIÓN DEL ESTADO DE TRANSFERENCIA AL ESTADO DE REPOSO: Un nodo volverá desde cualquier estado de transferencia al estado de reposo cuando detecte códigos ninguna petición en los bits 1-4 de K1 y códigos de indicación de reposo en los bits 6-8 de K2, procedentes de ambos sentidos. Los dos sentidos vuelven simultáneamente al estado de reposo desde el estado de transferencia.

### 7.2.6.2.2 Transiciones entre estados de reposo y de conmutación

**Regla I-S #1** – TRANSICIÓN DEL ESTADO DE REPOSO AL ESTADO DE CONMUTACIÓN:

**Regla I-S #1a** – La transición de un NE del estado de reposo al estado de conmutación será provocada por una de las condiciones siguientes:

- un cambio de byte K válido del código ninguna respuesta (NR) a cualquier código de petición de puenteo de anillo recibido por el trayecto largo o por el trayecto corto y destinado a ese NE;
- un cambio de byte K válido del código NR a cualquier código de petición de puenteo de tramo recibido por el trayecto corto y destinado a ese NE;
- una instrucción iniciada externamente para ese NE;
- la detección de un fallo en ese NE.

**Regla I-S #1b** – Las acciones realizadas en un NE comutante tras recibirse una petición de puenteo válida son las siguientes (se señala que para efectuar un puenteo y conmutación de anillo, la petición de puenteo ha de ser recibida en el trayecto largo; véase la regla I-S #1c):

- Para peticiones de puenteo FS-R, el nodo comprobará si hay alguna necesidad de silenciamiento y silenciará como corresponda, efectuará un puenteo e insertará el código de puenteado en los bits 6-8 de K2 en ambos sentidos (con las excepciones de MS-RDI y MS-AIS). Tras recibirse un código de puenteo en los bits 6-8 del byte K2 por el trayecto de petición de puenteo, el NE efectuará una conmutación y actualizará los bits 6-8 de K2 en consecuencia en ambos trayectos.
- Para peticiones de puenteo de SF-R, el nodo comprobará si hay necesidad de silenciamiento y silenciará como corresponda, efectuará un puenteo y una conmutación e insertará en los bits 6-8 del byte K2 el código puenteado y comutado tanto en el trayecto largo como en el trayecto corto (con las excepciones de MS-RDI y MS-AIS).
- Para todas las demás peticiones de puenteo, excepto SD-P, EXER y LP-S, el nodo efectuará un puenteo e insertará el código de puenteado en los bits 6-8 del byte K2 en ambos sentidos (con las excepciones de MS-RDI y MS-AIS). Tras recibir un código de puenteo en los bits 6-8 del byte K2 por el trayecto de petición de puenteo, el NE efectuará una conmutación y actualizará los bits 6-8 de K2 en consecuencia en ambos trayectos.
- Para SD-P, EXER y LP-S, el nodo señalizará como para cualquier otra petición de puenteo, pero no efectuará el puenteo o la conmutación (véase 7.2.1.2).

**Regla I-S #1c** – Una conmutación de tramo sólo se establecerá o se deshará con peticiones de puenteo de trayecto corto. Una conmutación de anillo sólo se establecerá o se deshará con peticiones de puenteo de trayecto largo.

**Regla I-S #2** – TRANSICIÓN DEL ESTADO DE CONMUTACIÓN AL ESTADO DE REPOSO: Un nodo volverá del estado de conmutación al estado de reposo cuando detecte códigos NR en los bits 1-4 del byte K1 y códigos de reposo en los bits 6-8 del byte K2 procedentes de ambos sentidos. La transición del estado de conmutación al estado de reposo se hará en tres pasos.

- *Paso 1* – El nodo (extremo de cola) que origina la petición de puenteo retira primero su conmutación y señaliza el código ninguna petición en los bits 1-4 del byte K1 y el código de puenteo en los bits 6-8 del byte K2.

## **Reemplazada por una versión más reciente**

- *Paso 2* – Tras la recepción del código ninguna petición y de la indicación de que se ha retirado la conmutación, el nodo del extremo de cabeza retirará su puenteo y su conmutación y originará el código reposo en ambos sentidos. La indicación de que ha sido retirada la conmutación se recibe por el trayecto corto para peticiones de puenteo de tramo y por el trayecto largo para peticiones de puenteo de anillo.
- *Paso 3* – Una vez que el extremo de cola detecte códigos de reposo entrantes, retirará también su puenteo y conmutación y originará el código reposo en ambos sentidos.

Se señala que hay casos en los que no hay que retirar ninguna conmutación o puenteo (por ejemplo para SD-P, LP-S, EXER, o conmutaciones que no podrían ser ejecutadas debido a otras condiciones en el anillo). En estos casos, el NE que inició la petición (es decir, el extremo de cola) señalará el código ninguna petición. Tras la recepción del código ninguna petición, el extremo de cabeza originará también el código reposo.

**Regla I-S #3** – Un nodo transmitirá el código APS por defecto hasta que sea capaz de efectuar la señalización de APS adecuada, de conformidad con el estado en que se halla el anillo. Los códigos APS por defecto se utilizarán para indicar que el nodo no puede señalar adecuadamente bytes de APS, por lo que no puede efectuar la conmutación de protección de manera apropiada.

**Regla I-S #4** – Un nodo conmutante de anillo (tramo) que reciba el código APS por defecto por el trayecto corto (largo) no cambiará su señalización ni tomará ninguna medida asociada a ese trayecto hasta que se reciban códigos APS adecuados. Un nodo conmutante de anillo (tramo) que reciba un código APS por defecto por el trayecto largo (corto) retirará su puenteo y conmutación.

**Regla I-S #5** – Un nodo que reciba peticiones de puenteo de anillo de trayecto largo destinadas a él mismo procedentes de sus dos vecinos no tomará ninguna medida basada en esas peticiones de puenteo.

**Regla I-S #6** – Un nodo que reciba los bytes APS que él está originando en ambos sentidos pasará al estado de reposo.

**Regla I-S #7** – Cuando un nodo reciba un código invertir petición por el tramo que está protegiendo y cuando el mismo nodo esté enviando un código de invertir petición, retirará su puenteo y conmutación como se describe en la regla I-S #2, excepto por lo que se refiere a las peticiones de situación de petición de puenteo o puenteo de prioridad de fallo de señal y degradación de señal. En el caso de fallo de señal y degradación de señal, el nodo retirará la conmutación y el puenteo después de que expire el tiempo de WTR, de acuerdo con la regla S-S #3.

### **7.2.6.2.3 Transiciones entre estados de conmutación**

En esta subcláusula se indica el conjunto de reglas necesarias para coordinar una transición entre estados de conmutación.

Son aplicables las siguientes reglas de transición:

**Regla S-S #1 – TRANSICIÓN DEL ESTADO DE CONMUTACIÓN AL ESTADO DE CONMUTACIÓN:**

**Regla S-S #1a** – Cuando un NE que esté efectuando una conmutación SF-R reciba otra petición de puenteo SF-R por el trayecto largo o una petición de puenteo FS-R por el trayecto largo, no destinada a ese NE, comprobará si hay alguna necesidad de silenciamiento y silenciará como corresponda. El NE detendrá el silenciamiento cuando se retiren el puenteo y la conmutación.

**Regla S-S #1b** – Cuando un NE que esté efectuando una conmutación FS-R reciba otra petición de puenteo FS-R por el trayecto largo o una petición SF-R por el trayecto largo, no destinada a ese NE, comprobará si hay alguna necesidad de silenciamiento y silenciará como corresponda. El NE detendrá el silenciamiento cuando se retiren el puenteo y la conmutación.

**Regla S-S #1c** – Cuando un NE que esté efectuando cualquier conmutación de anillo reciba una petición de puenteo de anillo de prioridad mayor (en razón de un fallo detectado localmente, de una instrucción iniciada externamente, o de una petición de puenteo de anillo destinado a él) para el mismo tramo, elevará la prioridad de la conmutación de anillo que está efectuando a la prioridad de la petición de puenteo de anillo recibida.

## **Reemplazada por una versión más reciente**

**Regla S-S #1d** – Cuando un NE que esté efectuando cualquier conmutación de tramo reciba una petición de puenteo de tramo de prioridad mayor (en razón de un fallo detectado localmente, de una instrucción iniciada externamente, o de una petición de puenteo de tramo destinada a él) para el mismo tramo, elevará la prioridad de la conmutación de tramo que está efectuando a la prioridad de la petición de puenteo de tramo recibida.

### **Regla S-S #2 – DESPLAZAMIENTO CON PRIORIDAD DE COMUTACIÓN:**

**Regla S-S #2a** – Cuando un NE que esté efectuando una conmutación de tramo reciba una petición de puenteo de anillo (en razón de un fallo detectado localmente, de una instrucción iniciada externamente, o de una petición de puenteo de anillo destinada a él) de prioridad mayor para el mismo tramo:

- retirará el puenteo de tramo y conmutará inmediatamente;
- efectuará la petición de puenteo de anillo (como se detalla en la regla I-S #1).

**Regla S-S #2b** – Cuando un nodo que esté efectuando una conmutación de tramo reciba una petición de puenteo de anillo (en razón de un fallo detectado localmente, de una instrucción iniciada externamente, o de una petición de puenteo de anillo destinada a él) para su tramo adyacente de mayor prioridad que la conmutación de tramo que está efectuando, retirará la conmutación de tramo, señalará ninguna petición en K1 y puenteado en K2 en el sentido de la petición de puenteo de tramo, y señalará la petición de anillo en K1 y reposo en K2 en el sentido de la petición de anillo.

**Regla S-S #2c** – Cuando un nodo que esté efectuando una conmutación de tramo reciba una petición de puenteo de anillo por el trayecto largo para un tramo no adyacente de prioridad mayor que la conmutación de tramo que se está efectuando, retirará la conmutación de tramo y señalará ninguna petición en K1 y puenteado en K2 en ambos sentidos.

**Regla S-S #2d** – Si un nodo de conmutación de tramo que está puenteado y conmutado recibe ninguna petición y una indicación de que la conmutación para ese tramo ha sido retirada, el nodo retirará su puenteo y conmutación y, si la entrada de máxima prioridad del nodo es:

- Un estado de petición de puenteo de tramo destinado al propio nodo, o ninguna petición, el nodo originará ninguna petición en K1 y reposo en K2 en ambos sentidos.
- Una petición de puenteo de tramo (en razón de un fallo detectado localmente, de una instrucción iniciada externamente, o de una petición de puenteo de tramo destinada a él) para un tramo adyacente, el nodo señalizará de conformidad con esa petición.
- Una petición de puenteo de anillo (en razón de un fallo detectado localmente, de una instrucción iniciada externamente, o de una petición de puenteo de anillo destinada a él) para un tramo adyacente, el nodo efectuará la petición de puenteo de anillo.
- Una petición de puenteo de anillo por trayecto largo destinada a otro nodo, el nodo pasará al estado de transferencia total (como se detalla en la regla S-P #1b).
- Un estado de petición de puenteo de tramo destinado a otro nodo, el nodo pasará al estado de transferencia de byte K (como se detalla en la regla S-P #1d).
- Una petición de puenteo de tramo (en razón de un fallo detectado localmente o de una instrucción iniciada externamente) para el mismo tramo, el nodo señalizará la petición de puenteo de tramo en K1 y reposo en K2.

**Regla S-S #2e** – Si un nodo de conmutación de tramo que está puenteado recibe una indicación de que se ha retirado la conmutación para ese tramo, el nodo retirará su puenteo y, si la entrada de máxima prioridad del nodo es:

- Un estado de petición de puenteo de tramo destinado al propio nodo, o ninguna petición, el nodo originará ninguna petición en K1 y reposo en K2 en ambos sentidos.
- Una petición de puenteo de tramo (en razón de un fallo detectado localmente, de una instrucción iniciada externamente, o de una petición de puenteo de tramo destinada a él) para un tramo adyacente, el nodo señalizará de conformidad con esa petición.
- Una petición de puenteo de anillo (en razón de un fallo detectado localmente, de una instrucción iniciada externamente, o de una petición de puenteo de anillo destinada a él) para un tramo adyacente, el nodo efectuará la petición de puenteo de anillo.

## **Reemplazada por una versión más reciente**

- Una petición de puenteo de anillo por trayecto largo destinada a otro nodo, el nodo pasará al estado de transferencia total (como se detalla en la regla S-P #1b).
- Un estado de petición de puenteo de tramo destinado a otro nodo, el nodo pasará al estado de transferencia de byte K (como se detalla en la regla S-P #1d).
- Una petición de puenteo de tramo (en razón de un fallo detectado localmente o de una instrucción iniciada externamente) para el mismo tramo, el nodo señalizará la petición de puenteo de tramo en K1 y reposo en K2.

**Regla S-S #2f** – Cuando un NE que esté efectuando una conmutación de anillo reciba una petición de puenteo de tramo o de anillo (en razón de un fallo detectado localmente, de una instrucción iniciada externamente, o de una petición de puenteo de tramo o anillo destinada a él) de prioridad mayor para un tramo adyacente que la de conmutación de anillo que está efectuando:

- retirará el puenteo de anillo y conmutación inmediatamente;
- efectuará la petición de puenteo de prioridad mayor (como se detalla en la regla I-S #1).

**Regla S-S #2g** – Cuando un NE que esté efectuando una conmutación de anillo reciba una petición de puenteo de tramo (en razón de un fallo detectado localmente, de una instrucción iniciada externamente, o de una petición de puenteo de tramo destinada a él) de mayor prioridad para el mismo tramo:

- retirará el puenteo de anillo y conmutación inmediatamente;
- efectuará la petición de puenteo de tramo.

**Regla S-S #3 – ELIMINACIÓN DE CONMUTACIÓN DE ANILLO Y TRAMO (SIN DESPLAZAMIENTO CON PRIORIDAD):**

**Regla S-S #3a** – Cuando en un nodo desaparezca una condición de fallo que afecte solamente a un tramo, el nodo pasará a espera al restablecimiento y permanecerá en ese estado durante el intervalo de temporización adecuado, a menos que:

- 1) se reciba una petición de puenteo diferente de prioridad mayor que la de WTR; o
- 2) se detecte otro fallo; o
- 3) se active una instrucción iniciada externamente.

El nodo enviará un código WTR por los trayectos largo y corto.

**Regla S-S #3b** – Tan pronto como un nodo al que se haya pedido que efectúe un puenteo, pero que de hecho no detectó el fallo, reciba un código espera al restablecimiento (caso de fallo unidireccional), continuará enviando una instrucción invertir petición por el trayecto corto y enviará WTR por el trayecto largo.

**Regla S-S #4 – TEMPORIZACIÓN DE CONMUTACIÓN DE TRAMO:** En el caso de un anillo de cuatro fibras, cuando no sea posible cumplimentar una petición de puenteo de tramo (en razón de un fallo detectado localmente, de una instrucción iniciada externamente, o de una petición de puenteo de tramo destinada a él) porque no se haya recibido acuse de recibo por el trayecto corto (temporización, cuya duración depende del equipo) o porque no se disponga ya de canales de protección, se intentará la conmutación de anillo equivalente.

**Regla S-S #5** – Un nodo que reciba peticiones de puenteo de anillo de trayecto largo destinadas a él mismo procedentes de sus dos vecinos retirará su puenteo y su conmutación.

**Regla S-S #6** – Si un tramo queda excluido, la petición de puenteo LP-S será señalizada por el trayecto corto. Si la condición de prioridad máxima detectada requiere una conmutación de anillo para el mismo tramo (el tramo excluido), la petición de puenteo de anillo será señalada por el trayecto largo. En cualquier otro caso, la situación de la petición de puenteo LP-S será señalizada por el trayecto largo.

### **7.2.6.2.4 Transiciones entre los estados de conmutación y transferencia**

**Regla S-P #1 – REGLAS DE DESPLAZAMIENTO CON PRIORIDAD DE CONMUTACIÓN (estado de conmutación a estado de transferencia):**

**Regla S-P #1a** – Si un nodo de conmutación de tramo que no está puenteado ni conmutado está recibiendo un código puenteado para ese tramo y su entrada de máxima prioridad es una petición de puenteo de anillo por trayecto largo destinado a otro nodo, el nodo señalizará ninguna petición en K1 y reposo en K2 en ambos sentidos.

## **Reemplazada por una versión más reciente**

**Regla S-P #1b** – Si un nodo de conmutación de tramo que no está puenteado ni conmutado recibe una indicación de que el puenteo para ese tramo se ha retirado y su entrada de máxima prioridad es una petición de puenteo de anillo por trayecto largo destinada a otro nodo, el nodo pasará al estado de transferencia total.

**Regla S-P #1c** – Si un nodo de conmutación de tramo que no está puenteado ni conmutado está recibiendo un código puenteado para ese tramo y su entrada de máxima prioridad es un estado de petición de puenteado de tramo destinado a otro nodo, el nodo señalizará ninguna petición en K1 y reposo en K2 en ambos sentidos.

**Regla S-P #1d** – Si un nodo de conmutación de tramo que no está puenteado ni conmutado recibe una indicación de que se ha retirado el puenteo para ese tramo y la entrada de máxima prioridad es un estado de petición de puenteo de tramo destinada a otro nodo, el nodo pasará al estado de transferencia de byte K.

**Regla S-P #1e** – Cuando un nodo que esté efectuando una conmutación de anillo reciba una petición de puenteo de anillo por trayecto largo para un tramo no adyacente de mayor prioridad que la que está efectuando la conmutación de anillo, retirará su puenteo y conmutación inmediatamente y pasará al estado de transferencia total.

**Regla S-P #1f** – Cuando un nodo que esté efectuando una conmutación de anillo tenga como entrada de máxima prioridad peticiones de puenteo de anillo por trayecto largo no destinadas a él procedentes de ambos sentidos, retirará inmediatamente su puenteo y conmutación y pasará al estado de transferencia total.

**Regla S-P #1g** – Si un nodo de conmutación de anillo que no está puenteado ni conmutado tiene como entrada de máxima prioridad un estado de petición de puenteo de tramo destinado a otro nodo, el nodo pasará al estado de transferencia de byte K.

### **Regla S-P #2 – TRANSICIONES DE TRANSFERENCIA A CONMUTACIÓN:**

**Regla S-P #2a** – La transición de un nodo de transferencia total a conmutación se producirá por:

- 1) una instrucción iniciada externamente igual, de prioridad superior o de coexistencia permitida;
- 2) la detección de un fallo igual, de prioridad superior o de coexistencia permitida;
- 3) la recepción de una petición de puenteo igual, de prioridad superior o de coexistencia permitida destinada a ese NE.

**Regla S-P #2b** – La transición de un nodo de transferencia de byte K a conmutación se producirá por:

- 1) cualquier instrucción iniciada externamente;
- 2) la detección de cualquier fallo;
- 3) la recepción de cualquier petición de puenteo destinada a ese NE.

**Regla S-P #2c** – Si una petición de puenteo de tramo desplaza con prioridad a una petición de puenteo de anillo (en razón de un fallo detectado localmente, de una instrucción iniciada externamente, o de una petición de puenteo de tramo destinada a él), el nodo que desplaza la conmutación de anillo insertará AU-AIS en todos los canales de protección distintos de los del tramo pedido, a menos que sean utilizados por otra conmutación de tramo.

**Regla S-P #3** – Si un nodo que estaba en el estado de transferencia debido a una petición SF-R o FS-R en el anillo está originando ahora una petición de puenteo SF-R o FS-R (debido a la regla S-P #2a), el nodo:

- 1) determinará si hay alguna necesidad de silenciamiento y silenciará como corresponda; y
- 2) efectuará el puenteo y la conmutación de anillo.

#### **7.2.6.2.5 Transiciones entre estados de transferencia**

Esta subcláusula indica el conjunto de reglas necesarias para pasar de un estado de transferencia de byte K a un estado de transferencia total, y viceversa.

Se aplican las siguientes reglas de transición:

## **Reemplazada por una versión más reciente**

**Regla P-P #1 – Transición de transferencia de byte K a transferencia total:** Un nodo en el estado de transferencia de byte K que reciba una petición de puenteo de anillo de trayecto largo no destinada a él pasará al estado de transferencia total.

**Regla P-P #2 – Transición de transferencia total a transferencia de byte K:** Un nodo en el estado de transferencia total que reciba un estado de petición de puenteo de tramo no destinado a él procedente de ambos sentidos pasará al estado de transferencia de byte K.

### **7.2.7 Ejemplos**

En el Apéndice I se describe la aplicación de las reglas anteriores en un conjunto de ejemplos básicos.

## **7.3 Anillos de protección especializada de MS**

Queda en estudio.

## **7.4 Protección de camino de VC lineal**

### **7.4.1 Arquitectura de red**

La protección de camino de LO/HO VC es un mecanismo de protección de capa de trayecto y puede utilizarse para proteger un camino a través de la totalidad de una red de operador o de redes de operadores múltiples. Se trata de un esquema de protección especializada de extremo a extremo que puede emplearse en diferentes estructuras de red: redes en malla, redes en anillo, etc. La conmutación de protección puede ser de extremo único o de extremo doble.

La protección del camino protege genéricamente contra fallos en la capa de servidor y fallos y degradaciones en la capa de cliente.

El esquema de protección puede ser 1 + 1, cuando el camino de protección especializada se utilice únicamente a efectos de protección, o 1:1 cuando el camino de protección especializada pueda utilizarse para soportar tráfico adicional. La conmutación de protección de extremo doble y la conmutación de protección 1:1 requieren un protocolo de APS para la coordinación entre las operaciones de conmutación y puenteo locales y distantes.

Puesto que la protección especializada 1:1 de camino de VC es un mecanismo de protección lineal, se produce un solapamiento de las funciones de terminación de camino de tráfico de servicio y tráfico adicional. En una aplicación de red, esto significa que los esquemas de tráfico de servicio y tráfico adicional deben coincidir. La protección de camino de VC es un mecanismo de protección de camino especializada, por lo que no existe una limitación fundamental al número de NE dentro de la conexión de red.

### **7.4.2 Objetivos de red**

Son aplicables los siguientes objetivos de red:

- 1) *Tiempo de conmutación* – El algoritmo APS para la protección de camino de LO/HO VC deberá funcionar tan rápido como sea posible. Se ha propuesto un valor de 50 ms como tiempo objetivo. Se han formulado algunos reparos a esta propuesta de tiempo objetivo para el caso en que participen muchos VC. Esto queda en estudio. El tiempo de compleción de la conmutación de protección excluye el tiempo de detección necesario para iniciar la conmutación de protección y el tiempo de abstención.
- 2) *Retardo de transmisión* – El retardo de transmisión depende de la longitud física del camino y de las funciones de procesamiento dentro del mismo. El retardo de transmisión máximo de un esquema de camino de VC con protección especializada queda en estudio. Pueden imponerse limitaciones al retardo de transmisión cuando haya que atenerse a un plazo de tiempo objetivo para la compleción de la conmutación en caso de operación de extremo doble.
- 3) *Tiempos de espera* – Los tiempos de espera son útiles para el interfuncionamiento de los esquemas de protección. Lo que se pretende es que estos tiempos puedan fijarse de manera individual para cada uno de los VC. La condición de defecto debe ser supervisada continuamente durante todo el tiempo de espera antes de que se produzca la conmutación. El tiempo de espera debe ser ajustable, por tanto, entre 0 y 10 segundos con pasos de unos 100 ms.

## Reemplazada por una versión más reciente

- 4) *Alcance de la protección* – La protección de camino de LO/HO VC restablecerá todo el tráfico que haya sido interrumpido a causa del fallo de una conexión de enlace que hubiera sido designada como integrante de un esquema de protección de camino de VC. El tráfico que termine en un nodo con fallos puede resultar perturbado, pero el tráfico transferido a otros nodos puede subsistir conmutando al camino de protección.
- 5) *Tipos de conmutación* – Tanto la protección de camino 1 + 1 como la 1:1 deben soportar conmutación de extremo único, conmutación de extremo doble o ambas.
- 6) *Protocolo y algoritmo APS* – Los protocolos APS de protección de camino de VC de orden inferior y de orden superior deben ser idénticos para todas las aplicaciones de red. El requisito mínimo del protocolo es que pueda soportar protección especializada 1 + 1. Es conveniente una opción 1:1 para acomodar tráfico adicional. Esto queda en estudio.
- 7) *Modos de funcionamiento* – La conmutación de extremo único 1 + 1 debe soportar conmutación reversiva, conmutación no reversiva o ambas. La conmutación de extremo doble reversiva: 1:1 con tráfico adicional queda para un ulterior estudio. (Se señala que una de las principales ventajas de la arquitectura 1:1 es su capacidad de llevar tráfico adicional.) El encaminamiento del tráfico de servicio (a saber, uniforme o diverso) no debe estar limitado por el esquema de protección de SNC. El operador de red puede elegir entre encaminamiento uniforme o diverso para cada SNC.
- 8) *Control manual* – Pueden proporcionarse instrucciones iniciadas externamente para el control manual de la conmutación de protección por los sistemas de operaciones o los operadores. Las instrucciones iniciadas externamente son las mismas (o un conjunto de las) que se utilizan para la protección de secciones de multiplexación lineal.
- 9) *Criterios para la iniciación de la conmutación* – Los criterios para la iniciación de la conmutación en caso de fallo de señal (SF) y/o degradación de señal (SD) deben estar en armonía con las definiciones utilizadas en la Recomendación G.783. Los criterios para la iniciación de la conmutación para la protección de camino de VC deben ser idénticos a los de protección de SNC/N correspondiente.

### 7.4.3 Arquitectura de aplicación

#### 7.4.3.1 Encaminamiento

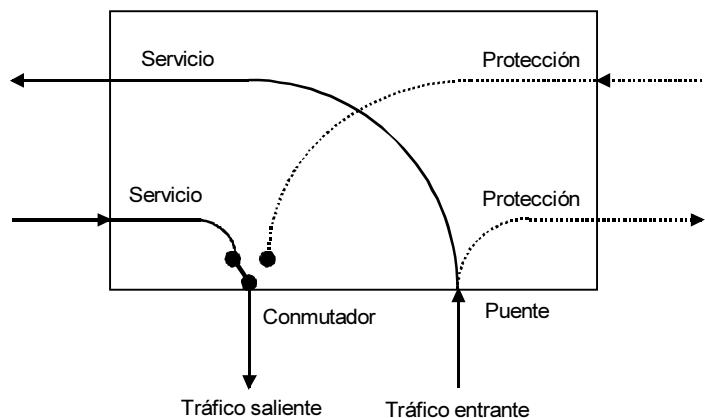
Los encaminamientos siguientes se aplican a los canales de servicio en condiciones de ausencia de fallos. Como regla general y para cada sentido de la transmisión, los canales de protección deben seguir un encaminamiento distinto del de los canales de servicio.

Como se indica en los objetivos de red, el operador de la red puede elegir entre encaminamiento uniforme o encaminamiento diverso camino por camino. En las Figuras 7-9 y 7-10 se ilustra la diferencia entre la provisión de un nodo para encaminamiento uniforme y la provisión de un nodo para encaminamiento diverso para protección 1 + 1, en el caso más sencillo en que los caminos de servicio y los caminos de protección están situados en rutas separadas. Para la protección de camino de VC lineal, los nodos representados contienen la terminación de los caminos implicados.

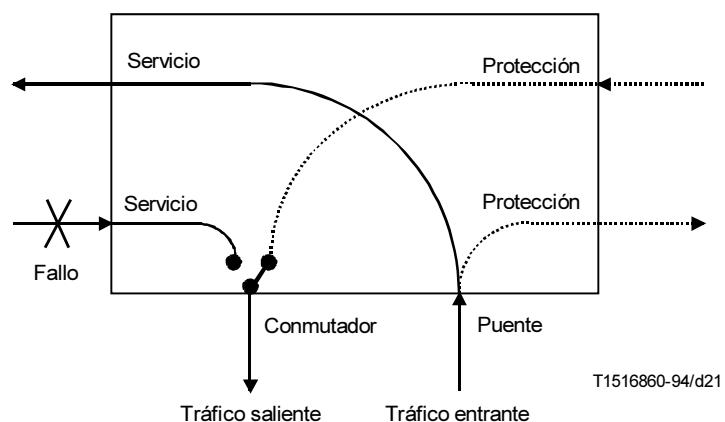
En la Figura 7-9 a) se muestra un nodo que utiliza encaminamiento uniforme 1 + 1 en condiciones de funcionamiento normal. Se emplea un puente para transmitir simultáneamente señales por los caminos de servicio y de protección. El receptor utiliza un conmutador para seleccionar el camino de servicio en condiciones de funcionamiento normal. Se señala que los caminos de servicio están situados en las mismas facilidades (es decir, en el lado izquierdo del nodo). La Figura 7-9 b) muestra el nodo cuando hay un fallo en el camino de servicio. En este caso, el receptor detectará la pérdida de señal y conmutará al camino de protección.

En la Figura 7-10 a) se muestra un nodo que utiliza encaminamiento diverso 1 + 1 en condiciones de funcionamiento normal. Se emplea un puente para transmitir simultáneamente señales por los caminos de servicio y de protección. El receptor utiliza un conmutador para seleccionar el camino de servicio en condiciones de funcionamiento normal. Se señala que los caminos de servicio están situados en facilidades diferentes (es decir, uno en el lado izquierdo del nodo y el otro en el lado derecho). La Figura 7-10 b) muestra el nodo cuando hay un fallo en el camino de servicio. En este caso, el receptor detectará la pérdida de señal y conmutará al camino de protección.

## Reemplazada por una versión más reciente



a) Condición normal. El tráfico transmitido es puenteado a trayectos de servicio y protección. El conmutador de tráfico recibido selecciona canal de servicio

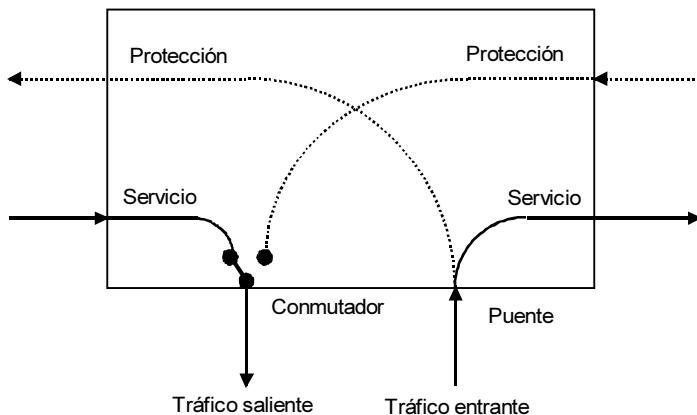


b) Fallo en el canal de servicio del tráfico entrante. El conmutador receptor selecciona trayecto de protección

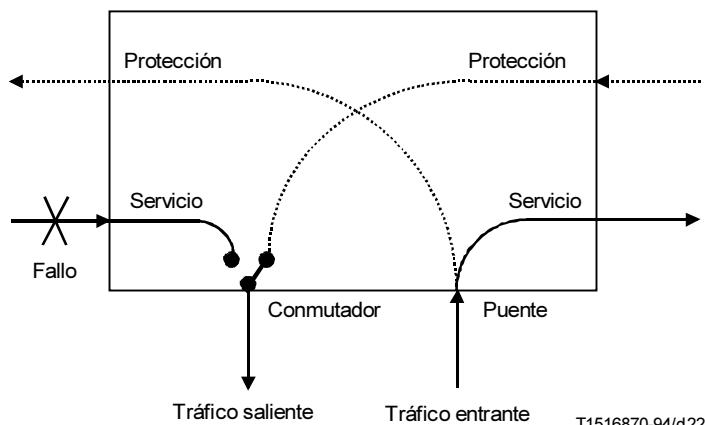
FIGURA 7-9/G.841

Nodo que utiliza encaminamiento uniforme para protección de camino o SNC 1 + 1

## Reemplazada por una versión más reciente



a) Condición normal – El tráfico transmitido es puenteado a trayectos de servicio y protección – El comutador de tráfico recibido selecciona canal de servicio



b) Fallo en el canal de servicio del tráfico entrante – El comutador receptor selecciona trayecto de protección

FIGURA 7-10/G.841

Nodo que utiliza encaminamiento diverso para protección de camino o SNC 1 + 1

## **Reemplazada por una versión más reciente**

### **7.4.3.2 Protección de extremo único 1 + 1**

La Figura 7-11 ilustra la protección de extremo único para arquitectura 1 + 1 con encaminamiento uniforme. Es idéntica a la protección de extremo doble con la salvedad de que en el caso de fallos unidireccionales no se conmuta el sentido no afectado de la transmisión. En consecuencia, no se requiere un canal APS para coordinar la conmutación del sentido no afectado de la transmisión.

La Figura 7-11 a) ilustra una red de protección de camino con encaminamiento uniforme 1 + 1, con tráfico transmitido entre los nodos A y C. El tráfico insertado en el nodo A se transmite por diferentes caminos en dos direcciones al nodo C. En condiciones de funcionamiento normal, el receptor del nodo C selecciona el tráfico de servicio. El tráfico insertado en el nodo C también se transmite en dos direcciones al nodo A.

Cuando se produce un fallo unidireccional en el camino de servicio, como se muestra en la Figura 7-11 b) o en la Figura 7-11 c), el conmutador del extremo de cola selecciona el camino de protección. Si un fallo en un solo punto corta ambos sentidos de la transmisión, fallan ambos sentidos de la transmisión en el trayecto de servicio y ambos sentidos de la transmisión comutan automáticamente al camino de protección.

El tráfico puede ser restablecido cuando múltiples fallos afectan al tráfico solamente en uno de los caminos (el de servicio o el de protección). Si ambos caminos se ven afectados por determinados fallos, el tráfico no puede ser restablecido. El tráfico que termina en un nodo con fallos queda interrumpido, pero el transferido a otros nodos puede subsistir conmutando al camino de protección.

La protección de camino de VC 1 + 1 también puede utilizar encaminamientos diversos.

### **7.4.3.3 Protección de extremo doble 1 + 1**

La Figura 7-12 a) ilustra una red de protección de camino con encaminamiento diverso 1 + 1 con tráfico transmitido entre los nodos A y C. El tráfico insertado en el nodo A se transmite por diferentes caminos en dos direcciones al nodo C. En condiciones de funcionamiento normal, el receptor del nodo C selecciona el tráfico de servicio. El tráfico insertado en el nodo C también se transmite en dos direcciones al nodo A.

Cuando se produce un fallo unidireccional en el camino de servicio, como se muestra en la Figura 7-12 b), el conmutador del extremo de cola selecciona el camino de protección. En caso de conmutación de extremo doble, se envía una indicación por medio del protocolo APS para forzar al sentido de la transmisión no afectada a que commute también al camino de protección. De esta manera se mantiene un encaminamiento uniforme (es decir, ambos sentidos de la transmisión utilizan las mismas rutas) incluso en condiciones de fallo unidireccional. Si un fallo en un solo punto corta ambos sentidos de la transmisión, fallan ambos sentidos de la transmisión en el trayecto de trabajo y ambos sentidos de la transmisión comutan automáticamente al camino de protección.

El tráfico puede ser restablecido cuando múltiples fallos afectan al tráfico solamente en uno de los caminos (el de servicio o el de protección). Si ambos caminos se ven afectados por determinados fallos, el tráfico no puede ser restablecido. El tráfico que termina en un nodo con fallos queda interrumpido, pero el transferido a otros nodos puede subsistir conmutando al camino de protección.

La protección de camino de VC 1 + 1 también puede utilizar encaminamientos diversos.

### **7.4.3.4 Protección 1:1**

Este esquema de protección queda en estudio.

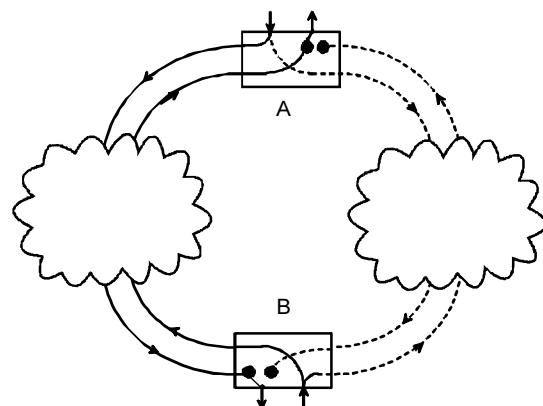
### **7.4.3.5 Conexión de tráfico errónea**

Queda en estudio.

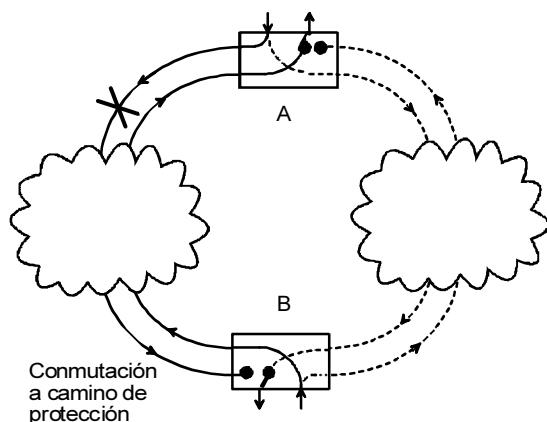
### **7.4.4 Criterios de iniciación de la conmutación**

Las peticiones de conmutación de protección de camino de LO/HO VC se inician automáticamente en base a las instrucciones de fallo de señal de camino y degradación de señal de camino (tales como AU-AIS y característica de error) e instrucciones APS.

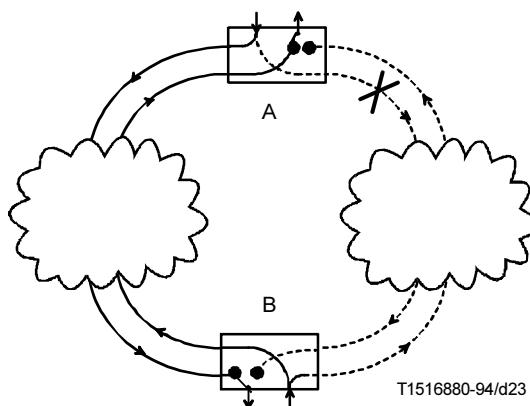
## Reemplazada por una versión más reciente



a) Condiciones normales



b) Fallo unidireccional – Fibra 1

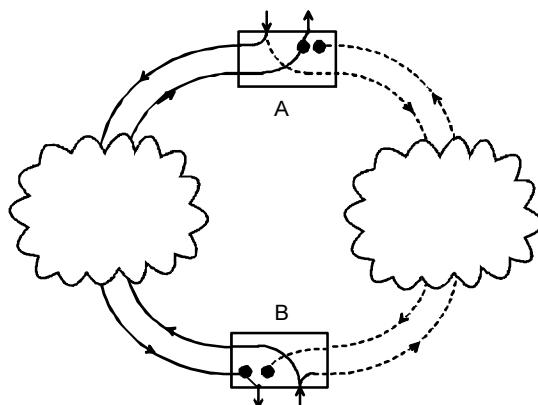


c) Fallo unidireccional – Fibra 2

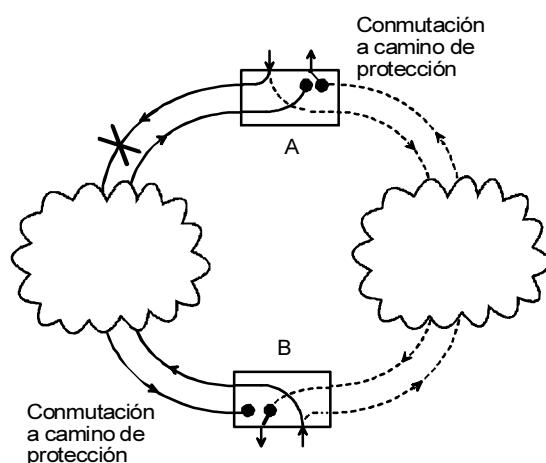
FIGURA 7-11/G.841

Red de protección de camino 1 + 1 encaminada uniformemente de dos fibras con conmutación de extremo único

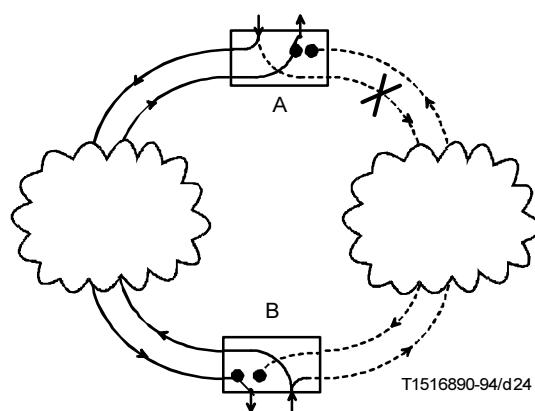
## Reemplazada por una versión más reciente



a) Condiciones normales



b) Fallo unidireccional – Fibra 1



c) Fallo unidireccional – Fibra 2

FIGURA 7-12/G.841

**Red de protección de camino 1 + 1 encaminada uniformemente de dos fibras con conmutación de extremo doble**

# Reemplazada por una versión más reciente

## 7.4.4.1 Protección de extremo único 1 + 1

Una petición puede ser:

- 1) una instrucción iniciada automáticamente (SF o SD) asociada con un camino de VC;
- 2) un estado (espera al restablecimiento, ninguna petición) del proceso de protección de camino de VC; o
- 3) una instrucción iniciada externamente (liberación, exclusión, commutación forzada, commutación manual).

Para la arquitectura 1 + 1, todas las peticiones son locales. En el Cuadro 7-6 se da la prioridad de las peticiones locales.

### NOTAS

1 Una commutación forzada a protección no debe ser invalidada por un fallo de señal en el canal de protección. Puesto que se está efectuando una commutación de extremo único y en el canal de protección no se soporta protocolo APS, el fallo de señal en el canal de protección no interfiere con la capacidad de efectuar una commutación forzada a protección.

2 No es necesario que el número del canal de servicio forme parte de las instrucciones de commutación, ya que un sistema 1 + 1 tiene solamente un canal de servicio y un canal de protección.

CUADRO 7-6/G.841

### Prioridad de las peticiones locales

Petición local (es decir, instrucción iniciada automáticamente, estado o instrucción iniciado externamente)	Orden de prioridad
Eliminación	Máxima
Exclusión de protección	
Commutación forzada	
Fallo de señal	
Degradoación de señal	
Commutación manual	
Espera al restablecimiento	
Ninguna petición	Mínima

#### 7.4.4.1.1 Instrucciones iniciadas externamente

La relación de instrucciones iniciadas externamente se indica más abajo, en el orden descendente de la prioridad. Estas instrucciones son aplicables tanto con funcionamiento reversivo como con funcionamiento no reversivo. Sin embargo, dependiendo del modo de funcionamiento, algunas de las instrucciones pueden dar como resultado la aplicación de las mismas medidas. La funcionalidad de cada instrucción se describe seguidamente.

**7.4.4.1.1.1 liberación:** Libera todas las instrucciones de commutación enunciadas a continuación.

**7.4.4.1.1.2 exclusión de protección (LP):** Impide que el selector commute al camino de VC de protección emitiendo una petición de exclusión de protección.

**7.4.4.1.1.3 commutación forzada a protección (FS-P):** Conmuta el selector del camino de VC de servicio al camino de VC de protección (a menos que esté en efecto una petición de commutación de prioridad igual o mayor).

## **Reemplazada por una versión más reciente**

**7.4.4.1.1.4 conmutación forzada a servicio (FS-W):** Conmuta el selector del camino de VC de protección al camino de VC de servicio (a menos que esté en efecto una petición de conmutación de prioridad igual o mayor).

NOTA – La instrucción FS-W es exclusiva solamente en sistemas no reversivos 1 + 1, ya que la instrucción LP produciría el mismo resultado en un sistema reversivo. Puesto que conmutación forzada tiene mayor prioridad que las instrucciones fallo de señal o degradación de señal en el camino de VC de servicio, esta instrucción se llevará a cabo con independencia de la condición del camino de VC de servicio.

**7.4.4.1.1.5 conmutación manual a protección (MS-P):** Conmuta el selector del camino de VC de servicio al camino de VC de protección (a menos que esté en efecto una petición de conmutación de prioridad igual o mayor).

**7.4.4.1.1.6 conmutación manual a servicio (MS-W):** Conmuta el selector del camino de VC de protección al camino de VC de servicio (a menos que esté en efecto una petición de conmutación de prioridad igual o mayor).

NOTA – La instrucción MS-W es unívoca solamente en sistemas no reversivos 1 + 1, ya que la instrucción eliminación produciría el mismo resultado en un sistema reversivo. Puesto que conmutación manual tiene menor prioridad que las instrucciones fallo de señal o degradación de señal en un camino de VC de servicio, esta instrucción se llevará a cabo solamente si el camino de VC de servicio no está en la condición fallo de señal o degradación de señal.

### **7.4.4.1.2 Instrucciones iniciadas automáticamente**

Las dos instrucciones iniciadas automáticamente son fallo de señal y degradación de señal.

#### **7.4.4.1.2.1 Instrucciones iniciadas automáticamente de orden superior**

Para los HO VC, la instrucción iniciada automáticamente fallo de señal se define como la presencia de una o más de las siguientes condiciones de defecto detectadas en la función de terminación de trayecto de orden superior (descrita en la Recomendación G.783):

- defecto fallo de señal de servidor de trayecto de orden superior (HP-SSF) – El HP-SSF se produce como consecuencia de defectos de capa de servidor tales como pérdida de puntero de unidad administrativa (AU-LOP) o señal de indicación de alarma de unidad administrativa (AU-AIS);
- defecto trayecto de orden superior no equipado (HP-UNEQ);
- defecto desadaptación de identificador de camino de trayecto de orden superior (HP-TIM) (si el proveedor de la red permite la utilización de esta condición);
- defecto errores excesivos en trayecto de orden superior (HP-EXC) (si el proveedor de la red permite la utilización de esta condición).

Las contribuciones de HP-EXC y HP-TIM a la condición SF son facultativas y sus definiciones quedan en estudio.

Para los HO VC, la instrucción iniciada automáticamente degradación de señal se define como la presencia de la siguiente condición de defecto detectada en la función de terminación de trayecto de orden superior (descrita en la Recomendación G.783):

- defecto trayecto de orden superior degradado (HP-DEG).

#### **7.4.4.1.2.2 Instrucciones iniciadas automáticamente de orden inferior**

Para los LO VC, la instrucción iniciada automáticamente fallo de señal se define como la presencia de una o más de las siguientes condiciones de defecto detectadas en la función de terminación de trayecto de orden inferior (descrita en la Recomendación G.783):

- defecto fallo de señal de servidor de trayecto de orden inferior (LP-SSF) – El LP-SSF se produce como consecuencia de defectos de capa de servidor tales como pérdida de puntero de unidad afluente (TU-LOP) o señal de indicación de alarma de unidad afluente (TU-AIS);
- defecto trayecto de orden inferior no equipado (LP-UNEQ);
- defecto desadaptación de identificador de camino de trayecto de orden inferior (LP-TIM) (si el proveedor de la red permite la utilización de esta condición);

## **Reemplazada por una versión más reciente**

- defecto errores excesivos en trayecto de orden inferior (LP-EXC) (si el proveedor de la red permite la utilización de esta condición).  
Las contribuciones de LP-EXC y LP-TIM a la instrucción iniciada automáticamente SF son facultativas y sus definiciones quedan para ulterior estudio.

Para los LO VC, la instrucción iniciada automáticamente degradación de señal se define como la presencia de la siguiente condición de defecto detectada en la función de terminación de trayecto de orden inferior (descrita en la Recomendación G.783):

- defecto trayecto de orden inferior degradado (LP-DEG).

### **7.4.4.2 Protección de extremo doble 1 + 1**

Queda en estudio.

### **7.4.4.3 Protección 1:1**

Queda en estudio.

## **7.4.5 Protocolo de commutación de protección**

### **7.4.5.1 Protección de extremo único 1 + 1**

En esta arquitectura no se requiere canal de APS.

### **7.4.5.2 Protección de extremo doble 1 + 1**

Al nivel HO VC, el canal de APS puede hacer uso de los bits 1-4 del byte K3 (anteriormente byte Z4). Al nivel LO VC, el canal de APS puede hacer uso de los bits 1-4 del byte K4 (anteriormente byte Z7). El protocolo específico queda en estudio.

### **7.4.5.3 Protección 1:1**

Queda en estudio.

## **7.4.6 Funcionamiento del algoritmo de protección**

### **7.4.6.1 Protección de extremo único 1 + 1**

#### **7.4.6.1.1 Control del puenteo**

En la arquitectura 1 + 1, el canal de servicio está permanentemente puenteado a protección.

#### **7.4.6.1.2 Control del selector**

En la arquitectura 1 + 1 en funcionamiento de extremo único, el selector es controlado por la condición local, el estado o la instrucción iniciada externamente de prioridad mayor. Por consiguiente, cada uno de los extremos funciona con independencia del otro. Si existe una condición de prioridad igual (por ejemplo, SF, SD) en ambos canales, no se llevará a cabo la commutación. (Se señala que este algoritmo no hace distinción entre las «severidades» de una degradación de señal, sólo constata que existe una condición degradación de señal.)

En el caso de instrucciones iniciadas automáticamente, la compleción de la commutación de protección deberá producirse tan rápido como sea posible. Se ha propuesto un valor de 50 ms como tiempo objetivo. Se han formulado algunos reparos a esta propuesta de tiempo objetivo para el caso en que participen muchos caminos. Esto queda en estudio. El tiempo de compleción de la commutación de protección excluye el tiempo de detección necesario para iniciar la commutación de protección y el tiempo de abstención.

#### **7.4.6.1.2.1 Modo reversivo**

En el modo de funcionamiento reversivo se restablecerá el canal de servicio, es decir, la señal del camino de protección se comutará de vuelta al camino de servicio cuando el canal de servicio se haya recuperado de la avería.

Para evitar el funcionamiento frecuente del selector debido a una avería intermitente, un camino que falle debe quedar libre de averías. Después de que el camino que falla cumpla este criterio (y sin que estén presentes otras instrucciones iniciadas externamente), transcurrirá un periodo de tiempo fijo antes de que se utilice de nuevo como canal de servicio. Este periodo, llamado espera al restablecimiento, debe ser del orden de 5 a 12 minutos y la fijación del mismo deberá

## **Reemplazada por una versión más reciente**

poderse hacer con pasos de un segundo. Durante este estado no se produce comutación. Una condición SF o SD invalidará el WTR. Una vez completado el periodo de WTR se pasa a un estado ninguna petición. A continuación se produce la comutación de canal de protección a canal de servicio.

NOTA – El modo reversivo podría utilizarse para soportar ciertos servicios en donde la ruta física más corta se mantiene en condiciones de ausencia de fallos para una conexión bidireccional.

### **7.4.6.1.2.2 Modo no reversivo**

Cuando el camino que falla deja de estar en una condición SD o SF, y no está presente ninguna otra instrucción iniciada externamente, se pasa a un estado ninguna petición. Durante este estado no se produce comutación.

### **7.4.6.2 Protección de extremo doble 1 + 1**

Queda en estudio.

### **7.4.6.3 Protección 1:1**

Queda en estudio.

## **8 Protección de conexión de subred de SDH**

### **8.1 Arquitectura de red**

La protección SNC/I protege, genéricamente, contra fallos en la capa de servidor. El proceso de protección y el proceso de detección de defectos los llevan a cabo dos capas adyacentes. La capa de servidor efectúa el proceso de detección de defectos y envía la situación a la capa de cliente mediante la señal fallo de señal de servidor (SSF).

La protección SNC/N protege, genéricamente, contra fallos en la capa de servidor y fallos y degradaciones en la capa de cliente.

La protección de LO/HO SNC es otra protección de capa de trayecto. Es un esquema de protección especializada que puede utilizarse con diferentes estructuras de red: redes en malla, redes en anillo, etc.

Se trata de protección 1 + 1 ó 1:1 especializada en la que el tráfico de servicio y el tráfico de protección en el extremo transmisor de una conexión de subred se transmiten de dos maneras diferentes. La protección especializada 1:1 podría soportar tráfico adicional.

En el caso de protección especializada 1 + 1, el extremo transmisor está puenteado permanentemente y el tráfico se transmite por ambas conexiones de subred, la de servicio y la de protección. En el extremo receptor de la SNC se efectúa una comutación de protección seleccionando una de las señales en base a información puramente local. No se requiere protocolo APS para este esquema de protección si es de extremo único.

En el caso de comutación de protección de extremo doble, comutación de protección 1:1 o transporte de tráfico adicional por el camino de protección, se requiere un protocolo APS para la coordinación entre la operaciones de comutación y puenteo locales y distantes. Para ello quizás se requiera una técnica de subestratificación que queda para ulterior estudio.

### **8.2 Objetivos de red**

Son aplicables los siguientes objetivos de red:

- 1) *Tiempo de comutación* – El algoritmo de protección de LO/HO SNC deberá funcionar tan rápido como sea posible. Se ha propuesto un valor de 50 ms como tiempo objetivo. Se han formulado algunos reparos a esta propuesta de tiempo objetivo para el caso en que participan muchas conexiones de subred. Esto queda en estudio. El tiempo de compleción de la comutación de protección excluye el tiempo de detección necesario para iniciar la comutación de protección y el tiempo de abstención.
- 2) *Retardo de transmisión* – La comutación de extremo único 1 + 1 no requiere transmisión de señalización APS, por lo que no están presentes retardos de transmisión de señalización.

## Reemplazada por una versión más reciente

- 3) *Tiempos de abstención* – Los tiempos de abstención son útiles para el interfuncionamiento de los esquemas de protección. Lo que se pretende es que estos tiempos puedan fijarse de manera individual para cada uno de los VC. La condición de defecto debe ser supervisada continuamente durante todo el tiempo de abstención antes de que se produzca la conmutación. El tiempo de abstención debe ser ajustable, por tanto, entre 0 y 10 segundos con pasos de unos 100 ms.
- 4) *Alcance de la protección* – La protección de LO/HO SNC restablecerá todo el tráfico (excepto el tráfico adicional) que haya sido interrumpido a causa del fallo de una conexión de enlace que hubiera sido designado como integrante de un esquema de protección de SNC.
- 5) *Tipos de conmutación* – La protección de SNC 1 + 1 debe soportar conmutación de extremo único. Otras arquitecturas quedan para ulterior estudio.
- 6) *Protocolo y algoritmo de APS* – El proceso de protección de SNC debe actuar de manera similar tanto en las capas de HO como en las de LO.
- 7) *Modos de funcionamiento* – La conmutación de extremo único 1 + 1 debe soportar conmutación reversiva, conmutación no reversiva o ambas. La conmutación de extremo doble reversiva 1:1 con tráfico adicional queda para ulterior estudio. (Se señala que una de las principales ventajas de la arquitectura 1:1 es su capacidad de llevar tráfico adicional.) El encaminamiento del tráfico de servicio (a saber, uniforme o diverso) no debe estar limitado por el esquema de protección de SNC. El operador de red puede elegir entre encaminamiento uniforme o diverso para cada SNC.
- 8) *Control manual* – Pueden proporcionarse instrucciones iniciadas externamente para el control manual de la conmutación de protección por los sistemas de operaciones o los operadores. Las instrucciones iniciadas externamente son las mismas (o un subconjunto de las) que se utilizan para la protección de la sección de multiplexación lineal.
- 9) *Criterios para la iniciación de la conmutación* – Los criterios para la iniciación de la conmutación en caso de fallo de señal (SF) y/o degradación de señal (SD), basados en la BER o en la característica de error de bloque, deben estar en armonía con las definiciones utilizadas en la Recomendación G.783. Los criterios para la iniciación de la conmutación para la protección de SNC/N deben ser idénticos a los de la protección del camino VC correspondiente.

### 8.3 Arquitectura de aplicación

#### 8.3.1 Encaminamiento

Los encaminamientos siguientes se aplican a los canales de servicio en condiciones de ausencia de fallos. Como regla general y para cada sentido de la transmisión, los canales de protección deben seguir un encaminamiento distinto del de los canales de servicio.

Como se indica en los objetivos de red, el operador de la red puede elegir entre encaminamiento uniforme o encaminamiento diverso para cada una de las SNC. En las Figuras 7-9 y 7-10 se ilustra la diferencia entre la provisión de un nodo de encaminamiento uniforme y la provisión de un nodo para encaminamiento diverso para protección 1 + 1, en el caso más sencillo en el que las conexiones de subred de servicio y las conexiones de subred de protección están situadas en rutas separadas. Para la protección de SNC (en contraste con la protección de camino de VC lineal), los nodos representados no necesariamente tienen que contener la terminación de los caminos implicados.

En la Figura 7-9 a) se muestra un nodo que utiliza encaminamiento uniforme 1 + 1 en condiciones normales de funcionamiento. Se emplea un puente para transmitir simultáneamente señales por las SNC de servicio y de protección. El receptor utiliza un conmutador para seleccionar la SNC de servicio en condiciones de funcionamiento normales. Se señala que las SNC de servicio están situadas en las mismas facilidades (es decir, en el lado izquierdo del nodo). La Figura 7-9 b) muestra el nodo cuando hay un fallo en la SNC de servicio. En este caso, el receptor detectará la pérdida de señal y conmutará a la SNC de protección.

## **Reemplazada por una versión más reciente**

En la Figura 7-10 a) se muestra un nodo que utiliza encaminamiento 1 + 1 diverso en condiciones normales de funcionamiento. Se emplea un puente para transmitir simultáneamente señales por las rutas de servicio y de protección. El receptor utiliza un conmutador para seleccionar la SNC de servicio en condiciones de funcionamiento normales. Se señala que las SNC de servicio están situadas en facilidades diferentes (es decir, una en el lado izquierdo del nodo y la otra en el lado derecho). La Figura 7-10 b) muestra el nodo cuando hay un fallo en la SNC de servicio. En este caso, el receptor detectará la pérdida de señal y conmutará a la SNC de protección.

### **8.3.2 Protección de extremo único 1 + 1**

La Figura 8-1 a) ilustra la protección de SNC encaminadas diversamente con tráfico transmitido entre los nodos A y C. El tráfico insertado en el nodo A se transmite por diferentes SNC en direcciones separadas al nodo C (por ejemplo, una SNC de servicio y una SNC de protección). En condiciones normales de funcionamiento, el receptor del nodo C selecciona el tráfico de SNC de servicio. Cuando hay un fallo en la SNC de servicio, como se muestra en la Figura 8-1 b), el conmutador del extremo de cola selecciona la SNC de protección. Si hay un fallo en la SNC de protección, como se muestra en la Figura 8-1 c), el receptor no necesitará conmutar y continuará detectando el tráfico de la SNC de servicio.

Las SNC encaminadas diversamente son capaces de sobrevivir a determinados fallos múltiples, incluyendo los cortes de cables, si provocan la interrupción de la misma SNC, como se muestra en la Figura 8-2 a). La conectividad se romperá si se producen fallos que afectan a ambas SNC, como se indica en la Figura 8-2 b). La Figura 8-2 c) da un ejemplo de conmutación de protección provocada por un fallo nodal. El tráfico que termina en el nodo con fallos se interrumpe, pero el tráfico transferido a otros nodos puede subsistir conmutando a la SNC de protección.

### **8.3.3 Otras arquitecturas**

La conmutación de extremo doble reversiva 1:1 con tráfico adicional queda para ulterior estudio.

## **8.4 Criterios para la iniciación de la conmutación**

### **8.4.1 Protección de extremo único 1 + 1**

Una petición puede ser:

- 1) una instrucción iniciada automáticamente (SF o SD) asociada con una conexión de subred de VC;
- 2) un estado (espera al restablecimiento, ninguna petición) del proceso de protección de SNC; o
- 3) una instrucción iniciada externamente (liberación, exclusión, conmutación forzada, conmutación manual).

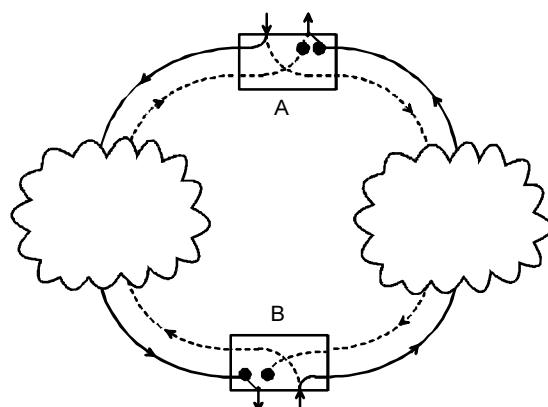
Para la arquitectura 1 + 1, todas las peticiones son locales. En el Cuadro 8-1 se da la prioridad de las peticiones locales.

#### **NOTAS**

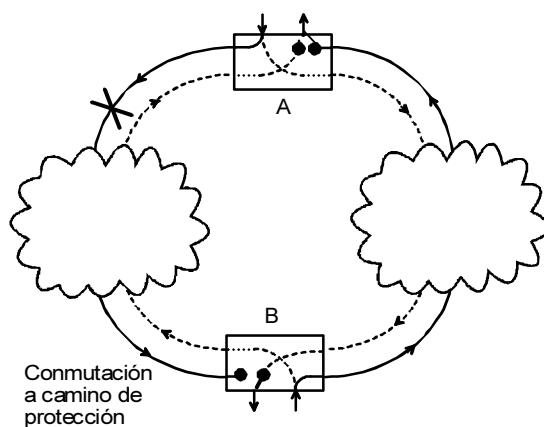
1 Una conmutación forzada a protección no debe ser invalidada por un fallo de señal en el canal de protección. Puesto que se está efectuando una conmutación de extremo único y en el canal de protección no se soporta protocolo de APS, el fallo de señal en el canal de protección no interfiere con la capacidad de efectuar una conmutación forzada a protección.

2 No es necesario que el número del canal de servicio forme parte de las instrucciones de conmutación, ya que un sistema 1 + 1 tiene solamente un canal en servicio y un canal de protección.

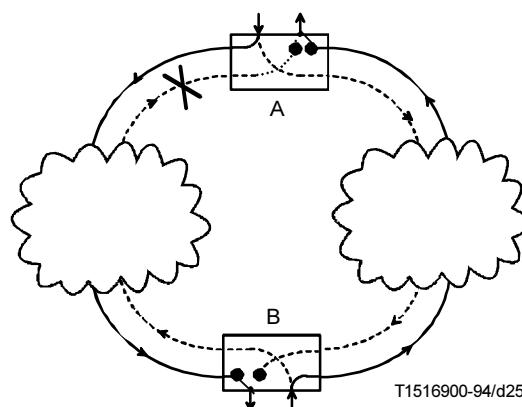
## Reemplazada por una versión más reciente



a) Condiciones normales



b) Fallo unidireccional – Fibra 1

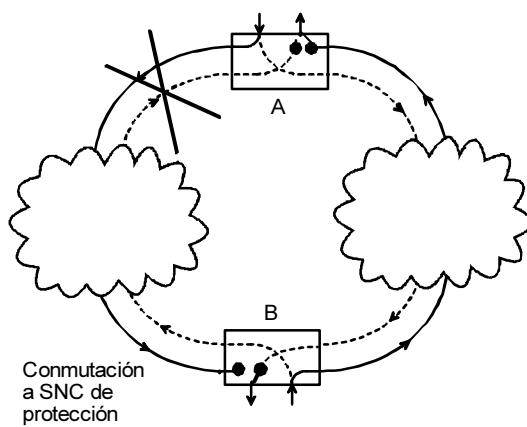


c) Fallo unidireccional – Fibra 2

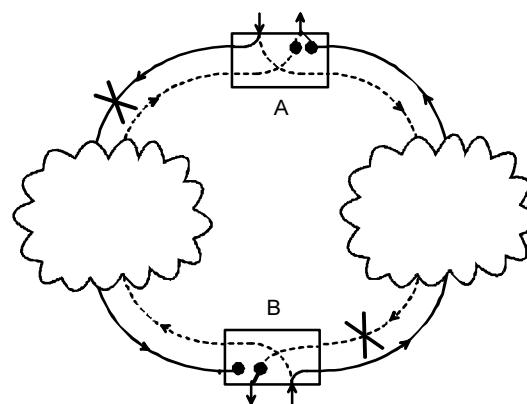
FIGURA 8-1/G.841

Red de protección de SNC 1 + 1 encaminada diversamente  
de dos fibras con un solo fallo

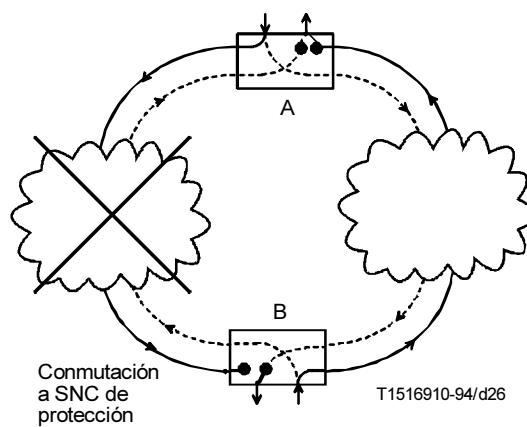
## Reemplazada por una versión más reciente



a) Múltiples fallos – Corte de cable



b) Múltiples fallos – Fallos independientes en las fibras 1 y 2  
Transmisión interrumpida



c) Fallo de nodo dentro de SNC

FIGURA 8-2/G.841

Red de protección de SNC 1 + 1 encaminada diversamente  
de dos fibras con múltiples fallos

# Reemplazada por una versión más reciente

CUADRO 8-1/G.841

## Prioridad de las peticiones locales

Petición local (es decir, instrucción iniciada automáticamente, estado o instrucción iniciado externamente)	Orden de prioridad
Eliminación	Máxima
Exclusión de protección	
Commutación forzada	
Fallo de señal	
Degradoación de señal	
Commutación manual	
Espesa al restablecimiento	
Ninguna petición	Mínima

### 8.4.1.1 Instrucciones iniciadas externamente

La relación de instrucciones iniciadas externamente se indica más abajo, en orden descendente de prioridad. Estas instrucciones son aplicables tanto con funcionamiento reversivo como con funcionamiento no reversivo. Sin embargo, dependiendo del modo de funcionamiento, algunas de las instrucciones pueden dar como resultado la aplicación de las mismas medidas. La funcionalidad de cada instrucción se describe seguidamente.

**8.4.1.1.1 eliminación:** Elimina todas las instrucciones de commutación enumeradas a continuación.

**8.4.1.1.2 exclusión de protección (LP):** Impide que el selector commute a la conexión de subred de VC de protección emitiendo una petición exclusión de protección.

**8.4.1.1.3 commutación forzada a protección (FS-P):** Commute el selector de la conexión de subred de VC de servicio a la conexión de subred de VC de protección (a menos que esté en efecto una petición de commutación de prioridad igual o mayor).

**8.4.1.1.4 commutación forzada a servicio (FS-W):** Commute el selector de la conexión de subred de VC de protección a la conexión de subred de VC de servicio (a menos que esté en efecto una petición de commutación de prioridad igual o mayor).

NOTA – La instrucción FS-W es unívoca solamente en sistemas no reversivos 1 + 1, ya que la instrucción LP produciría el mismo resultado en un sistema reversivo. Puesto que commutación forzada tiene mayor prioridad que las instrucciones fallo de señal o degradación de señal en la conexión de subred de VC de servicio, esta instrucción se llevará a cabo con independencia de la condición de la conexión de subred de VC de servicio.

**8.4.1.1.5 commutación manual para protección (MS-P):** Commute el selector de la conexión de subred de VC de servicio a la conexión de subred de VC de protección (a menos que esté en efecto una petición de commutación de prioridad igual o mayor).

**8.4.1.1.6 commutación manual a servicio (MS-W):** Commute el selector de la conexión de subred de VC de protección a la conexión de subred de VC de servicio (a menos que esté en efecto una petición de commutación de prioridad igual o mayor).

NOTA – La instrucción MS-W es unívoca solamente en sistemas no reversivos 1 + 1 ya que la instrucción liberación produciría el mismo resultado en un sistema reversivo. Puesto que la commutación manual tiene menor prioridad que las instrucciones fallo de señal o degradación de señal en una conexión de subred de VC de servicio, esta instrucción se llevará a cabo solamente si la conexión de subred de VC de servicio no está en la instrucción iniciada automáticamente fallo de señal o degradación de señal.

## **Reemplazada por una versión más reciente**

### **8.4.1.2 Instrucciones iniciadas automáticamente**

Las dos instrucciones iniciadas automáticamente son fallo de señal y degradación de señal.

#### **8.4.1.2.1 Instrucciones iniciadas automáticamente de orden superior**

Para los HO VC, la instrucción iniciada automáticamente fallo de señal se define como la presencia de una o más de las siguientes condiciones de defecto detectadas en la función de supervisión de tara de trayecto de orden superior (descrita en la Recomendación G.783):

Para SNC/N y SNC/I:

- defecto fallo de señal de servidor de trayectos de orden superior (HP-SSF). El HP-SSF se produce como consecuencia de defectos de capa de servidor tales como pérdida de puntero de unidad administrativa (AU-LOP) o señal de indicación de alarma de unidad administrativa (AU-AIS).

Para SNC/N solamente:

- defecto trayecto de orden superior no equipado (HP-UNEQ);
- defecto desadaptación de identificador de rastreo de trayecto de orden superior (HP-TIM) (si el proveedor de la red permite la utilización de esta condición);
- defecto errores excesivos en trayecto de orden superior (HP-EXC) (si el proveedor de la red permite la utilización de esta condición).

Las contribuciones de HP-EXC y HP-TIM a la condición SF son facultativas y sus definiciones quedan en estudio.

Para los HO VC que utilizan SNC/N, la instrucción iniciada automáticamente degradación de señal se define como la presencia de la siguiente condición de defecto detectada en la función de supervisión de tara de trayecto de orden superior (descrita en la Recomendación G.783):

- defecto trayecto de orden superior degradado (HP-DEG).

#### **8.4.1.2.2 Instrucciones iniciadas automáticamente de orden inferior**

Para los LO VC, la instrucción iniciada automáticamente fallo de señal se define como la presencia de una o más de las siguientes condiciones de defecto detectadas en la función de supervisión de tara de trayecto de orden inferior (descrita en la Recomendación G.783):

Para SNC/N y SNC/I:

- defecto fallo de señal de servidor de trayecto de orden inferior (LP-SSF). El LP-SSF se produce como consecuencia de defectos de capa de servidor tales como pérdida de puntero de unidad afluente (TU-LOP) o señal de indicación de alarma de unidad afluente (TU-AIS).

Para SNC/N solamente:

- defecto trayecto de orden inferior no equipado (LP-UNEQ);
- defecto desadaptación de identificador de rastreo de trayecto de orden inferior (LP-TIM) (si el proveedor de la red permite la utilización de esta condición);
- defecto errores excesivos en trayecto de orden inferior (LP-EXC) (si el proveedor de la red permite la utilización de esta condición).

Las contribuciones de LP-EXC y LP-TIM a la instrucción iniciada automáticamente SF son facultativas y sus definiciones quedan en estudio.

Para los LO VC que utilizan SNC/N, la instrucción iniciada automáticamente degradación de señal se define como la presencia de la siguiente condición de defecto detectada en la función de supervisión de tara de trayecto de orden inferior (descrita en la Recomendación G.783):

- defecto trayecto de orden inferior degradado (LP-DEG).

### **8.4.2 Otras arquitecturas**

Queda en estudio.

## **Reemplazada por una versión más reciente**

### **8.5 Protocolo de conmutación de protección**

#### **8.5.1 Protección de extremo único 1 + 1**

En esta arquitectura no se requiere canal de APS.

#### **8.5.2 Otras arquitecturas**

Queda en estudio.

### **8.6 Funcionamiento del algoritmo de protección**

#### **8.6.1 Algoritmo de protección de extremo único 1 + 1**

##### **8.6.1.1 Control del puente**

En la arquitectura 1 + 1, el canal de servicio está permanentemente puenteado a protección.

##### **8.6.1.2 Control del selector**

En la arquitectura 1 + 1 en funcionamiento de extremo único, el selector es controlado por la condición local, el estado o la instrucción iniciada externamente de prioridad más alta. Por consiguiente, cada uno de los extremos funciona con independencia del otro. Si existe una condición de igual prioridad (por ejemplo, SF, SD) en ambos canales, no se llevará a cabo la conmutación. (Se señala que este algoritmo no hace distinción entre las «severidades» de una degradación de señal, solamente constata que existe una condición de degradación de señal.)

En el caso de instrucciones iniciadas automáticamente, la compleción de la conmutación de protección deberá producirse tan rápido como sea posible. Se ha propuesto un valor de 50 ms como tiempo objetivo. Se han formulado algunos reparos a esta propuesta de tiempo objetivo para el caso en que participen muchas conexiones de subred. Esto queda en estudio. El tiempo de compleción de la conmutación de protección excluye el tiempo de detección necesario para iniciar la conmutación de protección y el tiempo de abstención.

##### **8.6.1.2.1 Modo reversivo**

En el modo de funcionamiento reversivo se restablecerá el canal de servicio, es decir, la señal de la conexión de subred de protección se conmutará de vuelta a la conexión de subred de servicio cuando esta conexión de subred en servicios se haya recuperado de la avería.

Para evitar el funcionamiento frecuente del selector debido a una avería intermitente, una conexión de subred que falle debe quedar libre de averías. Después de que la conexión de subred que falla cumpla este criterio (y sin que estén presentes otras instrucciones iniciadas externamente), transcurrirá un periodo de tiempo fijo antes de que se utilice de nuevo como canal de servicio. Este periodo, llamado espera al restablecimiento, debe ser del orden de 5 a 12 minutos, y la fijación del mismo deberá poderse hacer con pasos de un segundo. Durante este estado no se produce conmutación. Una instrucción iniciada automáticamente SF o SD invalidará el WTR. Una vez completado el periodo WTR se pasa a un estado ninguna petición. A continuación se produce la conmutación de canal de protección a canal de servicio.

NOTA – El modo reversivo podría utilizarse para soportar ciertos servicios en donde la ruta física más corta se mantiene en condiciones de ausencia de fallos para una conexión bidireccional.

##### **8.6.1.2.2 Modo no reversivo**

Cuando la SNC que falla deja de estar en condición SD o SF, y no está presente ninguna otra instrucción iniciada externamente, se pasa a un estado ninguna petición. Durante este estado no se produce conmutación.

#### **8.6.2 Otras arquitecturas**

Queda en estudio.

# Reemplazada por una versión más reciente

## Anexo A

### Anillos de protección compartida de MS (aplicación transoceánica)

(Este anexo es parte integrante de la presente Recomendación)

#### A.1 Aplicación

Dado el carácter particular de los sistemas transoceánicos, esto es, trayectos de transmisión muy largos, el procedimiento descrito para anillos de protección compartida de MS de uso general resulta insuficiente. Para algunos tipos de fallos, la adaptación total del anillo de protección compartida de MS de uso general llevaría a trayectos de transmisión de restablecimiento que cruzarían el océano tres veces. Los retardos inherentes a tal procedimiento no harían sino degradar la calidad de funcionamiento.

El texto adicional para la implementación de la opción «aplicación transoceánica» demuestra, en consecuencia, cómo utilizando el protocolo existente y aumentando la acción de conmutación en los nodos del anillo se consigue eliminar el problema mencionado más arriba. Se señala que estos problemas sólo se pondrán de manifiesto en redes de gran longitud, en las que las distancias entre los nodos del anillo son superiores a 1500 km.

Cuando se produce una conmutación de anillo en la red en anillo transoceánico, todas las AU-4 afluentes afectadas por el fallo son puenteadas en sus nodos de origen a los canales de protección que se alejan del fallo. Cuando las afluentes afectadas alcanzan sus nodos de destino final, son conmutadas a sus puntos de extracción originales, como se ilustra en la Figura A.1. Esto se consigue utilizando los mapas de anillos de nodos locales y el protocolo de byte K. Las diferencias entre las Figuras 6-2 y A.1 ilustran las diferencias de longitud del canal de protección.

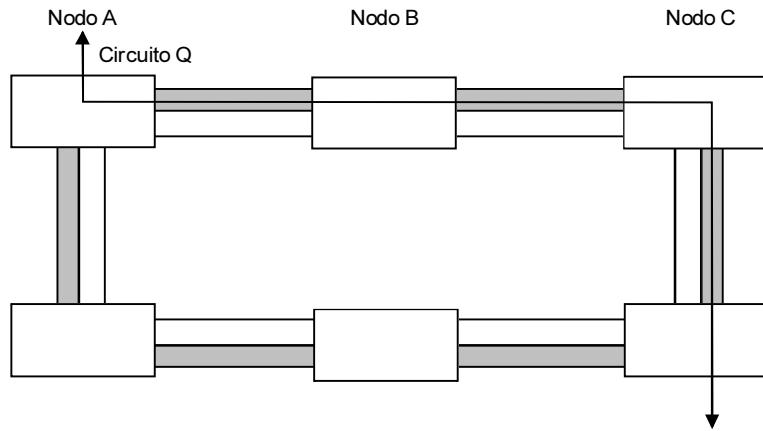
En el caso de red en anillo no transoceánico, el tráfico adicional permanece fuera de la red en anillo hasta que se elimina el fallo. Puesto que sólo las AU-4 afluentes afectadas son conmutadas para red en anillo transoceánico, el tráfico adicional desplazado con prioridad puede ser restablecido en los canales de protección no utilizados para restaurar el tráfico de servicio normal. El canal de señalización utilizado para restablecer el tráfico adicional es el DCC.

#### A.2 Objetivos de red

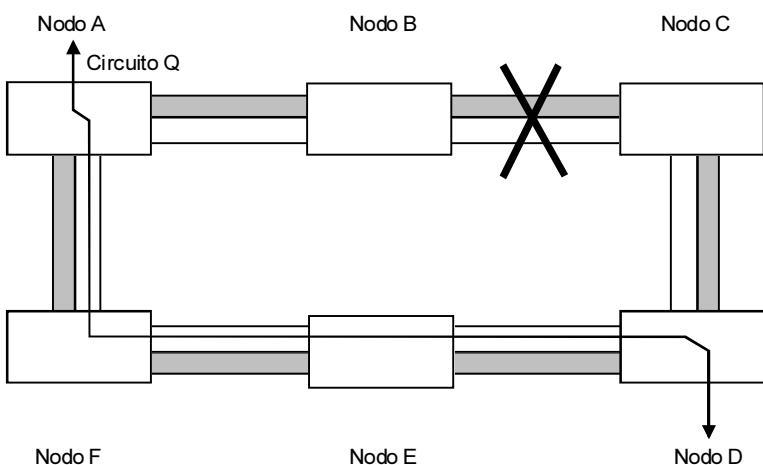
Para aplicaciones transoceánicas de anillos de protección compartida de MS son aplicables algunos objetivos de red adicionales:

- 1) *Tiempo de conmutación* – El tiempo de compleción de la conmutación deberá ser inferior a 300 milisegundos, con independencia de si el anillo lleva o no tráfico adicional. Este objetivo reemplaza al objetivo 1 de 7.2.2.
- 2) *Alcance de la protección* – El objetivo 4 b) de 7.2.2 es reemplazado por el siguiente: b) El anillo restablecerá todo el tráfico posible, incluso en condiciones de peticiones de puenteo múltiples de la misma prioridad.
- 3) *Protocolo y algoritmo de APS*
  - a) No se requiere silenciamiento de AUG. Esto reemplaza al objetivo 6 j) de 7.2.2.
  - b) Durante un fallo, el tráfico adicional desplazado con prioridad puede ser restablecido en los canales de protección no utilizados para restaurar el tráfico de servicio normal.
  - c) En las aplicaciones transoceánicas, se utilizan mapas de anillo para conmutar el tráfico afectado por un fallo en los nodos intermedios. Debe acomodarse un mecanismo que proporcione de manera autónoma los datos que requieren estos mapas y mantenga su coherencia. El mecanismo cuya utilización se propone es el DCC.
  - d) El objetivo 6 i) de 7.2.2 queda reemplazado por el siguiente: i) Cuando exista una conmutación de anillo y se produzca un fallo de igual prioridad en otro tramo que requiera una conmutación de anillo, si la prioridad de la petición de puenteo es fallo de señal (anillo) o superior, se establecerán ambas conmutaciones de anillo dando lugar a la división del anillo en dos segmentos separados.

## Reemplazada por una versión más reciente



a) Estado normal



b) Estado de fallo

T1516920-94/d27

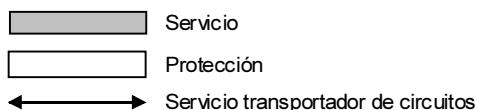


FIGURA A.1/G.841

Ejemplo de encaminamiento de circuitos en estado de fallo para una conmutación de circuito (aplicación transoceánica)

# Reemplazada por una versión más reciente

## A.3 Arquitectura de aplicación

Un anillo de protección compartida de MS de una aplicación transoceánica utiliza indicaciones de capa de sección de multiplexación SDH para provocar la conmutación de protección. La acción conmutadora se lleva a cabo solamente en AU-4 afluentes afectadas por el fallo. Los indicadores de sección de multiplexación incluyen condiciones de fallo de MS y mensajes de señalización que se envían entre nodos para influir en una conmutación de protección de MS coordinada.

En caso de fallo, se establecen conmutaciones de anillo en cualquier nodo cuyo tráfico resulte afectado por el fallo. A pesar de los procedimientos de uso general descritos anteriormente, no se establecen bucles. Los bucles y las conmutaciones sólo en los nodos adyacentes a un fallo son la causa del triple cruce oceánico existente en el trayecto de restablecimiento del tráfico mencionado más arriba. Por ello, en el procedimiento transoceánico se permite a todos los nodos conmutar y utilizar el protocolo existente junto con los mapas de anillos. Como en los casos de uso general descritos en 7.2.1.1 y 7.2.1.2, el tráfico afectado se reencamina alejándolo del fallo por los canales de protección.

El problema de la conexión incorrecta se elimina en el caso de aplicación de anillo transoceánico, ya que no hay bucles en los nodos que conmutan. Es la formación de bucles en los nodos conmutantes lo que crea la posibilidad de conexiones incorrectas. En consecuencia, no es necesario el silenciamiento descrito para anillos de protección compartida de MS de uso general. Además, los fallos simples y múltiples en la conmutación de anillos se solucionan de la misma manera, puenteando y conmutando simplemente y aprovechando la información de mapa de anillo recién descrita.

## A.4 Criterios de conmutación

Son aplicables los criterios de 7.2.4 con las siguientes interpretaciones adicionales:

**A.4.1 conmutación forzada de servicio a protección-anillo (FS-R):** Esta instrucción efectúa la conmutación de anillo de canales de servicio a canales de protección para el tramo entre el nodo en el que la instrucción se inicia y el nodo adyacente al que la instrucción está destinada. La conmutación tiene lugar con independencia del estado de los canales de protección, a menos que dichos canales estén dando cumplimiento a una petición de puenteo de prioridad mayor o exista un fallo de señal (o un fallo de byte K) en los canales de protección de trayecto largo. Para las aplicaciones transoceánicas, la FS-R ha de provocar la misma respuesta de conmutación que para un corte de cable en el tramo entre el nodo en el que la instrucción se inicia y el nodo adyacente al que está destinada la instrucción. No obstante, al igual que en el comportamiento para cortes de cables, no se establecen bucles. El tráfico de servicio entre dos nodos cualesquiera que hayan estado utilizando el tramo afectado se reencamina ahora a partir de ese tramo por conducto de los canales de protección.

**A.4.2 conmutación manual de servicio a protección-anillo (MS-R):** Para aplicaciones transoceánicas, también es aplicable aquí lo descrito en relación con la FS-R.

**A.4.3 ejercicio-anillo (EXER-R):** Para aplicaciones transoceánicas, el tráfico adicional tampoco se ve afectado.

**A.4.4 ejercicio-tramo (EXER-S):** Para aplicaciones transoceánicas, el tráfico adicional tampoco se ve afectado.

Como se describe en 7.4.2, la petición de puenteo de SF se utiliza para proteger el tráfico de servicio afectado por un fallo grave mientras que la petición de puenteo de SD se utiliza como protección frente a un fallo de poca gravedad. Las peticiones de puenteo se transmiten tanto por el trayecto corto como por el trayecto largo. Cada nodo intermedio verifica la ID del nodo de destino de la petición de puenteo de trayecto largo y retransmite la petición de puenteo. El nodo de destino recibe la petición de puenteo, lleva a cabo la actividad de acuerdo con el nivel de prioridad y envía la indicación de puenteado. Para aplicaciones transoceánicas, esta actividad se produce en los nodos conmutantes y en los nodos intermedios.

Como se describe también en 7.4.2, la petición de puenteo de WTR se utiliza para evitar la oscilación frecuente entre los canales de protección y los canales de servicio. Lo que se pretende es minimizar las oscilaciones, ya que durante la conmutación se producen perturbaciones momentáneas. La petición de puenteo de WTR se emite una vez que la BER de los canales de servicio satisface el umbral de restablecimiento. La WTR se emite solamente después de una condición SF o SD y, por ello, no se aplica en caso de peticiones de puenteo iniciadas externamente. Para conmutaciones de anillo de una aplicación transoceánica, una petición de puenteo de WTR recibida bidireccionalmente por un nodo intermedio con tráfico puenteado y conmutado da lugar a lo siguiente. El nodo intermedio inicia una WTR cuyo intervalo de tiempo es la mitad del intervalo de WTR del nodo conmutante. Para aplicaciones transoceánicas, el intervalo de WTR se fija en el mismo valor para todos los nodos.

## **Reemplazada por una versión más reciente**

### **A.5 Protocolo de conmutación de protección**

Este protocolo es el mismo que se describe en 7.2.5.

### **A.6 Funcionamiento del algoritmo de protección**

En el caso de aplicaciones transoceánicas, el estado de transferencia en los nodos intermedios puede entrañar también actividad conmutadora cuando se requieran conmutaciones de anillo, como se describe a continuación.

En aplicaciones transoceánicas, los nodos intermedios pueden tener cierta actividad conmutadora. Según se indica en 6.2, todos los nodos están autorizados a conmutar si su tráfico insertado/retirado se ve afectado por un fallo, y esto incluye a los nodos intermedios. Cuando se requiera una conmutación de anillo, cualquier nodo intermedio efectuará puenteos y conmutaciones si su tráfico insertado/retirado se ve afectado por el fallo. La determinación de tráfico afectado se efectúa examinando las peticiones de puenteo de K 1 (que indican los nodos adyacentes al fallo o fallos) y los mapas de anillo almacenados (que indican la posición relativa del fallo y del tráfico añadido/extráido dirigido hacia ese fallo). Sólo las AU-4 afluentes afectadas por el fallo son puenteadas y conmutadas, utilizando las mismas reglas descritas en este documento. Los detalles específicos respecto al puenteo y a la conmutación en nodos intermedios se dan en las figuras de los ejemplos del Apéndice I.

Las reglas siguientes modifican o amplían las de 7.2.6 para satisfacer las necesidades de la aplicación transoceánica:

**Regla básica #3 – ACTUALIZACIÓN DE LOS BITS 6-8 DE K2:** Dado que «Todas las acciones de puenteo y conmutación serán reflejadas mediante la actualización de los bits 6-8 del byte K2, a menos que exista una condición MS-RDI», para las aplicaciones transoceánicas esto sólo ocurre en los nodos conmutantes. El resto de esta regla se aplica tal como se indica en 7.2.6.2.

**Regla básica #4 –** En las aplicaciones transoceánicas, lo que sigue reemplaza a la regla básica #4: Las peticiones de puenteo (en razón de un fallo detectado localmente, de una instrucción iniciada externamente o de bytes K recibidos) desplazarán con prioridad a las peticiones de puenteo en el orden de prioridades que figuran en el Cuadro 7-1. Las peticiones de puenteo desplazarán a la señalización de situación de petición de puenteo con independencia de la prioridad de cada una de ellas. La señalización de situación de puenteo nunca desplazará a una petición de puenteo.

**Regla I-S #1b –** Puesto que las aplicaciones transoceánicas no requieren silenciamiento, las actividades silenciadoras descritas en esta regla no se realizan.

**Regla S-S #1a –** Puesto que las aplicaciones transoceánicas no requieren silenciamiento, las actividades silenciadoras descritas en esta regla no se realizan. Lo siguiente reemplaza a la regla S-S #1a en las aplicaciones transoceánicas solamente:

- 1) La coexistencia de FS-R con SF-R no se utiliza en aplicaciones transoceánicas.
- 2) Cuando un nodo conmutador de anillo reciba la nueva petición de puenteo de anillo con un código de situación de «reposo», mantendrá:
  - a) el puenteo y la conmutación (y retirará el tráfico adicional, que se restablecerá si procede), y cambiará el código de estado a «reposo» para ambos lados, si el nodo estaba enviando «puenteado y conmutado»; o bien
  - b) cambiará el código de situación a «puenteado y conmutado» para ambos lados, si el nodo estaba enviando «reposo».
- 3) Cuando el nodo que ejecuta 2) reciba la petición de puenteo de anillo con un código de situación «puenteado y conmutado», cambiará el código de situación a «puenteado y conmutado» para ambos lados, si el nodo estaba enviando «reposo».

**Regla S-S #1b –** Puesto que las aplicaciones transoceánicas no requieren silenciamiento, las actividades silenciadoras descritas en esta regla no se realizan. Lo siguiente reemplaza a la regla S-S #1b en las aplicaciones transoceánicas solamente:

- 1) La coexistencia de FS-R con SF-R no se utiliza en aplicaciones transoceánicas.

## Reemplazada por una versión más reciente

- 2) Cuando un nodo comutador de anillo reciba la nueva petición de puenteo de anillo con un código de situación «reposo», mantendrá:
  - a) el puenteo y la comutación (y retirará el tráfico adicional que se restablecerá, si procede), y cambiará el código de situación a «reposo» para ambos lados, si el nodo estaba enviando «puenteado y comutado»; o bien
  - b) cambiará el código de situación a «puenteado y comutado» para ambos lados, si el nodo estaba enviando «reposo».
- 3) Cuando el nodo que ejecuta 2) reciba la petición de puenteo de anillo con un código de situación «puenteado», cambiará:
  - a) el código de situación a «puenteado» para el lado de trayecto largo, si el nodo estaba enviando «reposo»; o bien
  - b) el código de situación a «puenteado y comutado» para ambos lados, si el nodo estaba enviando «puenteado».
- 4) Cuando el nodo que ejecuta 3) reciba la petición de puenteo de anillo con un código de situación «puenteado y comutado», cambiará el código de situación a «puenteado y comutado» para ambos lados, si el nodo estaba enviando «puenteado».

**Regla S #4a** – Para las comutaciones coexistentes FS-R con FS-R y las comutaciones coexistentes de SF-R y SF-R, el anillo no se subdivide en múltiple subanillos. En el caso de la aplicación transoceánica de anillos de protección compartida de MS, la comutación de anillo utilizada para sistemas transoceánicos no requiere la puesta en bucle del tráfico en nodos comutantes. En consecuencia, el anillo es segmentado, pero no en anillos más pequeños. La segmentación es en cadenas de adición/extracción lineales separadas por fallos de cable y/o el número de comutaciones forzadas (anillo) existentes en el anillo. La coexistencia de FS-R con SF-R no se aplica a aplicaciones transoceánicas.

**Regla S-P #2c** – Esta regla no se requiere en las aplicaciones transoceánicas.

**Regla S #1d** – En las aplicaciones transoceánicas, lo siguiente reemplaza a la regla S #1d: Cuando un nodo detecte un fallo entrante en los canales de trabajo y de protección, originará siempre sobre el trayecto corto una petición de puenteo de anillo de trayecto corto, aun en el caso de múltiples fallos, a condición de que la petición de puenteo de anillo no esté desplazada por una petición de puenteo de mayor prioridad ubicada en el mismo tramo [véase la Figura 7-8, b)]. Esta regla tiene precedencia sobre la regla S #1c. Se señala que, cuando un nodo reciba en un sentido una petición de puenteo de anillo por el trayecto corto (lo que indica que la señal que se envía tiene fallos) y detecte en el otro lado un fallo entrante en los canales de trabajo y de protección, señalizará el fallo detectado en ambos trayectos, corto y largo [véase la Figura 7-8, c)].

**Regla S-S #2d** – En las aplicaciones transoceánicas, lo siguiente reemplaza a la regla S-S #2d: Si una petición de puenteo (en razón de un fallo detectado localmente, de una instrucción indicada externamente o de bytes K recibidos) a través de un tramo diferente desplaza con prioridad a una petición de puenteo SF-R, el nodo de comutación que origina la petición de puenteo SF-R continuará señalizando su petición de puenteo, retirará su puenteo y comutación e insertará AU-AIS en los afluentes con fallos.

**Regla S-P #1e** – En las aplicaciones transoceánicas, lo que sigue reemplaza a la regla S-P #1e: Cuando un nodo que esté efectuando una comutación de anillo reciba una petición de puenteo de anillo para un tramo no adyacente de mayor prioridad que la comutación de anillo que está ejecutando, ya sea:

- 1) mantendrá los puenteos y comutaciones en los afluentes afectados por el primer fallo, si la petición de puenteo de anillo de trayecto largo está aún señalizando ese fallo; o bien
- 2) retirará los puenteos y comutaciones de anillo en los afluentes afectados por el primer fallo, si la petición de puenteo de anillo de trayecto largo ya no está señalizando ese fallo. Pasará entonces al estado de transferencia total.

**Regla S-P #1f** – En las aplicaciones transoceánicas, lo que sigue reemplaza a la regla S-P #1f: Cuando un nodo que esté efectuando una comutación de anillo tenga como entrada de máxima prioridad peticiones de puenteo de anillo de trayecto largo no destinadas a él procedentes de ambos sentidos, ya sea:

- 1) mantendrá los puenteos y comutaciones de anillo en los afluentes afectados por el primer fallo, si las peticiones de puenteo de anillo de trayecto largo aún están señalizando ese fallo; o bien
- 2) retirará los puenteos y comutaciones de anillo en los afluentes afectados por el primer fallo, si las peticiones de puenteo de anillo de trayecto largo ya no están señalizando ese fallo. Pasará entonces al estado de transferencia total.

## **Reemplazada por una versión más reciente**

**Regla S-P #1g** – En las aplicaciones transoceánicas no se aplica esta regla.

**Regla S-P #2a** – En las aplicaciones transoceánicas, lo que sigue reemplaza a la regla S-P #2a: La transición de un nodo de transferencia total a conmutación se producirá por:

- 1) una instrucción iniciada externamente de prioridad igual o superior;
- 2) la detección de un fallo de prioridad igual o superior;
- 3) la recepción de una petición de puenteo de prioridad igual o superior destinada a ese NE;
- 4) la detección de una condición SF-R (incluso de prioridad inferior); o
- 5) la recepción de una petición de puenteo SF-R destinada a ese NE.

**Regla S-P #3** – En las aplicaciones transoceánicas, lo que sigue reemplaza a la regla S-P #3: Si un nodo que se encontraba en el estado de transferencia debido a una petición de puenteo SF-R o FS-R origina ahora una petición SF-R o FS-R (conforme a la regla S-P #2a), el nodo retirará el tráfico adicional y mantendrá el puenteo y conmutación de anillo del primer fallo.

## **Apéndice I**

### **Ejemplos de conmutación de protección en un anillo de protección compartida de MS**

(Este apéndice no es parte integrante de la presente Recomendación)

En este apéndice se dan ejemplos que muestran cómo se utilizan las reglas de transición de estados para efectuar una conmutación de anillo.

#### **I.1 Fallo de señal unidireccional (tramo) en un anillo de cuatro fibras**

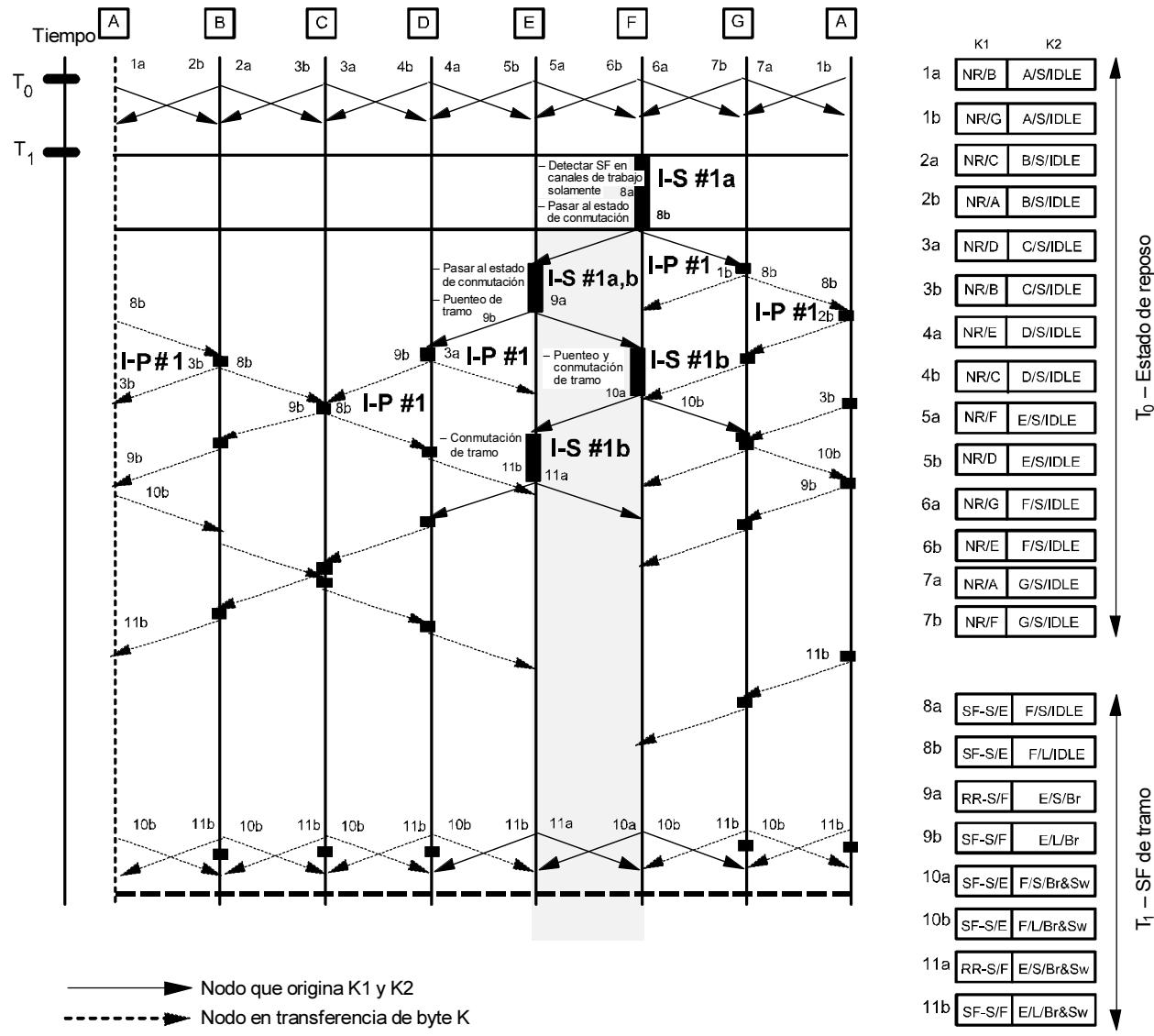
Véase la Figura I.1.

En este ejemplo, se efectúa y se elimina una conmutación de tramo para una condición SF en los canales de servicio de un anillo de cuatro hilos. El estado inicial del anillo es el estado de reposo. En el momento  $T_1$ , el nodo F detecta una condición SF en sus canales de servicio. El nodo pasa a ser un nodo conmutante (regla I-S #1) y envía peticiones de puenteo en ambos sentidos (regla S #1). El nodo G y todos los nodos intermedios sucesivos del trayecto largo pasan al estado de transferencia de byte K (regla I-P #1). El nodo E, tras la recepción de la petición de puenteo procedente del nodo F por el trayecto corto, efectúa un puenteo de tramo y transmite una petición de puenteo de tramo de SF por el trayecto largo y una invertir petición por el trayecto corto (reglas S #3, S #1 e I-S #1b). El nodo F, tras la recepción del acuse de recibo de puenteo procedente del nodo B por el trayecto corto, efectúa un puenteo y conmutación de tramo y actualiza la señalización de byte K (regla I-S #1b). El nodo E, tras la recepción del acuse de recibo de puenteo y conmutación procedente del nodo F por el trayecto corto, completa la conmutación. La señalización alcanza el estado estacionario.

En las aplicaciones transoceánicas, las actividades conmutadoras tendrían lugar en los nodos intermedios. En todos los canales de protección de AU-4 que no se utilizan para proteger canales de servicio se restablece el tráfico adicional utilizando el DCC.

En el momento  $T_2$ , se elimina la condición SF de tramo y el nodo F pasa al estado de espera al restablecimiento y señala su nuevo estado en ambos sentidos (regla S-S #3a). El nodo E, tras la recepción de la petición de puente WTR procedente del nodo F por el trayecto corto, envía invertir petición por el trayecto corto y WTR por el trayecto largo (regla S-S #3b). En el momento  $T_3$ , expira el intervalo de WTR. El nodo F retira la conmutación de tramo y envía códigos ninguna petición (regla I-S #2). El nodo E, tras la recepción del código ninguna petición procedente del nodo F por el trayecto corto, retira su puenteo y conmutación y origina el código reposo (regla I-S #2). El nodo F, tras la recepción del código reposo por el trayecto corto, retira su puenteo y origina también el código reposo. Todos los nodos vuelven a continuación en cascada al estado de reposo.

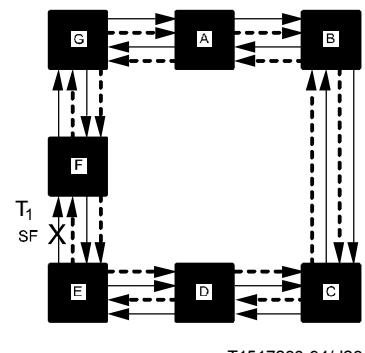
# Reemplazada por una versión más reciente



Para la aplicación transoceánica solamente:

Restablecer el tráfico a tiempo parcial, según proceda,  
utilizando DCC [RSOH]

NOTA – Véanse los formatos de los bytes K1 y K2 en los Cuadros 1 y 2.



T1517280-94/d28

FIGURA I.1/G.841

Anillo de protección compartida de MS de cuatro fibras –  
Fallo unidireccional (tramo) en servicio de E a F

# Reemplazada por una versión más reciente

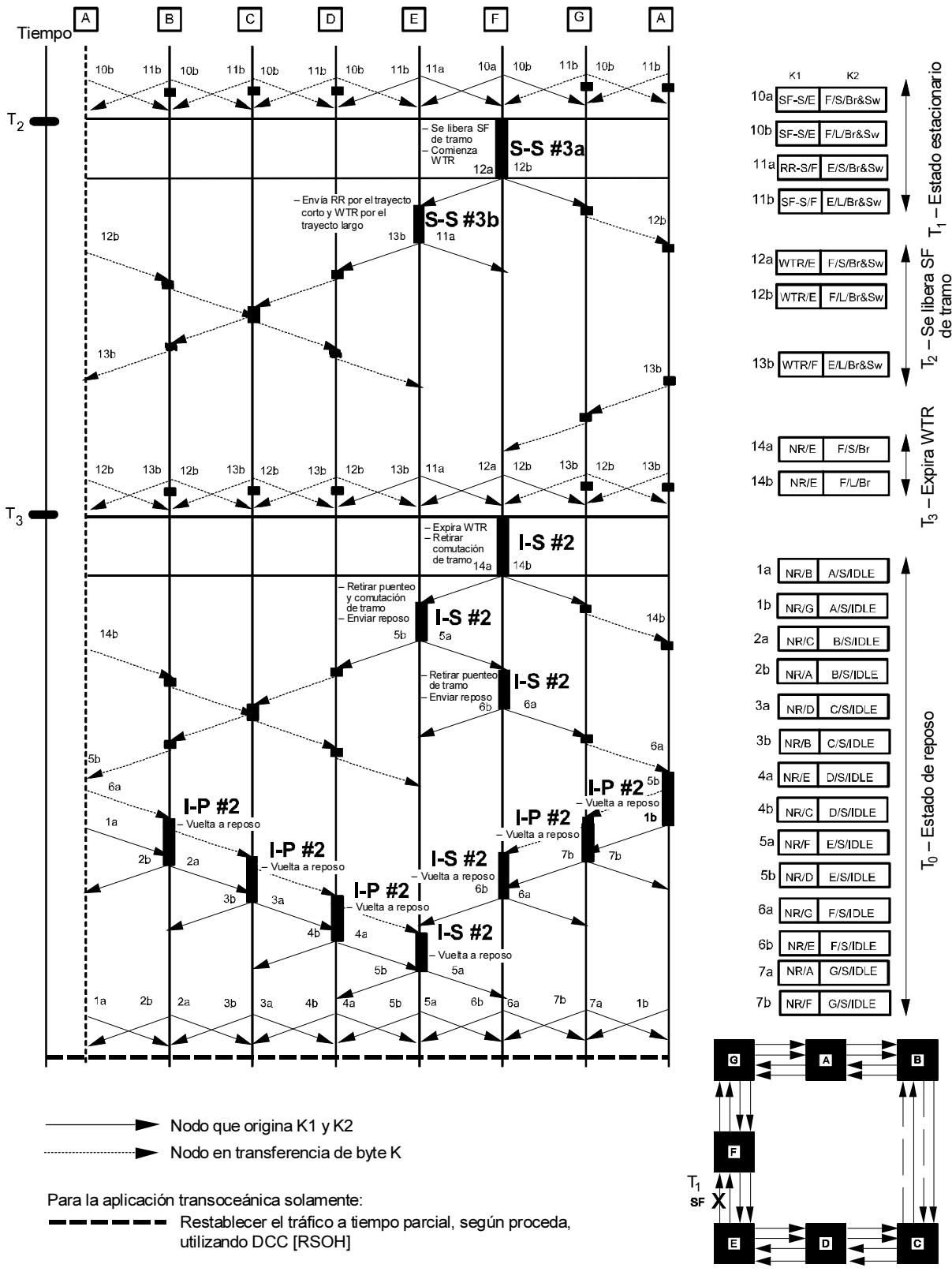


FIGURA I.1/G.841 (*fin*)

Anillo de protección compartida de MS de cuatro fibras – Fallo unidireccional (tramo) en servicio de E a F

## **Reemplazada por una versión más reciente**

### **I.2 Fallo de señal unidireccional (anillo)**

Véase la Figura I.2.

Este ejemplo abarca el caso de una condición SF unidireccional en un anillo de dos fibras y el de una condición SF unidireccional tanto en canales de servicio como en canales de protección en un anillo de cuatro fibras.

El estado inicial del anillo es el de reposo. En el momento  $T_1$ , el nodo F detecta una condición SF en sus canales de servicio y protección. El nodo pasa a ser un nodo conmutante (regla I-S #1) y envía peticiones de puente en ambos sentidos (regla S #1). El nodo G y todos los nodos intermedios sucesivos del trayecto largo, pasan al estado de transferencia total (regla I-P #1). El nodo E, tras la recepción de la petición de puenteo procedente del nodo F por el trayecto corto, transmite una petición de puenteo de anillo de SF por el trayecto largo y una instrucción invertir petición por el trayecto corto (reglas S #3 e I-S #1a). El nodo E, tras la recepción de la petición de puenteo procedente del nodo F por el trayecto largo, efectúa un puente y conmutación de anillo y actualiza los bits 6-8 del byte K2 (regla I-S #1b). El nodo F, tras la recepción del acuse de recibo procedente del nodo E por el trayecto largo, efectúa un puente y conmutación de anillo y actualiza su señalización de byte K (regla I-S #1b). La señalización alcanza el estado estacionario.

En las aplicaciones transoceánicas, las actividades conmutadoras tendrían lugar en los nodos intermedios. En todos los canales de protección de AU-4 que no se utilizan para proteger los canales de servicio se restablece el tráfico adicional utilizando el DCC.

En el momento  $T_2$ , se elimina la condición SF de anillo y el nodo F pasa al estado de espera al restablecimiento y señala su nuevo estado en ambos sentidos (regla S-S #3a). El nodo E, tras la recepción de la petición de puenteo de WTR procedente del nodo F por el trayecto corto, envía invertir petición por el trayecto corto y WTR por el trayecto largo (regla S-S #3b). En el momento  $T_3$ , expira el intervalo de WTR. El nodo F retira la conmutación de anillo y envía códigos ninguna petición (regla I-S #2). El nodo E, tras la recepción del código ninguna petición procedente del nodo F por el trayecto largo, retira su puenteo y conmutación y origina el código reposo (regla I-S #2). El nodo F, tras la recepción del código reposo por el trayecto largo, extrae su puenteo y origina también el código reposo. Todos los nodos vuelven a continuación en cascada al estado de reposo.

### **I.3 Fallo de señal bidireccional (anillo)**

Véase la Figura I.3.

Este ejemplo abarca el caso de una condición SF bidireccional en un anillo de dos fibras y el de una condición SF bidireccional tanto en canales de servicio como en canales de protección en un anillo de cuatro fibras.

El estado inicial del anillo es el de reposo. En el momento  $T_1$ , los nodos E y F detectan una condición SF en sus canales de servicio y protección. Los nodos pasan a ser nodos conmutantes (regla I-S #1) y envían peticiones puenteo en ambos sentidos (regla S #1). Los nodos D y G, y todos los nodos intermedios sucesivos del trayecto largo, pasan al estado de transferencia total (regla I-P #1). El nodo E, tras la recepción de la petición de puenteo procedente del nodo F por el trayecto largo, efectúa un puenteo y conmutación de anillo y actualiza los bits 6-8 del byte K2 (regla I-S #1b). El nodo F, tras la recepción de la petición de puenteo procedente del nodo E por el trayecto largo, efectúa un puenteo y conmutación de anillo y actualiza los bits 6-8 del byte K2 (regla I-S #1b). La conmutación alcanza el estado estacionario.

En las aplicaciones transoceánicas, las actividades conmutadoras tendrían lugar en los nodos intermedios. En todos los canales de protección AU-4 que no se utilizan para proteger canales de servicio, se restablece el tráfico adicional utilizando el DCC.

En el momento  $T_2$ , cuando se elimina la condición SF-R, los valores del byte K que reciben los nodos E y F indican, tanto a E como a F, que son extremos de cabeza de una condición SF unidireccional en el tramo que desplaza con prioridad a WTR. Para esta condición debe señalarse la prioridad de SF-R por el trayecto largo y RR-R por el trayecto corto (regla S #3). Estas acciones provocan el cruce de RR-R por el trayecto corto entre los nodos E y F. Ambos extremos de cabeza pasan al periodo de WTR (debido a la liberación simultánea), una vez que han recibido una RR-R cruzante procedente del nodo que era su extremo de cola. En el momento  $T_3$ , expiran los intervalos de WTR. Ambos

## **Reemplazada por una versión más reciente**

nodos reaccionan como extremos de cabeza a la WTR originando la prioridad de WTR en el trayecto largo y RR-R en el trayecto corto. Tras recibir la RR-R que cruza, los nodos E y F retiran su comutación de anillo y envían códigos ninguna petición (regla I-S #2). El nodo E, tras la recepción del código NR procedente del nodo F por el trayecto largo, retira su puenteo y origina el código reposo (regla I-S #2). El nodo F, tras la recepción del código NR procedente del código E por el trayecto largo, retira su puenteo y origina el código reposo (regla I-S #2). Todos los nodos vuelven a continuación en cascada al estado de reposo.

### **I.4 Degradación de señal unidireccional (anillo)**

Véase la Figura I.4.

En este ejemplo, se efectúa y se elimina una comutación de anillo para una condición SD de anillo en un anillo de dos fibras y para una condición SD de anillo en los canales de servicio y protección de un anillo de cuatro fibras.

El estado inicial del anillo es el de reposo. En el momento  $T_1$ , el nodo F detecta una condición SD de anillo. El nodo pasa a ser un nodo comutante (regla I-S #1) y envía peticiones de puenteo en ambos sentidos (regla S #1). El nodo G y todos los nodos intermedios sucesivos del trayecto largo pasan al estado de transferencia total (regla I-P #1). El nodo E, tras la recepción de la petición de puenteo procedente del nodo F por el trayecto corto, transmite una petición de puenteo de anillo de SD por el trayecto largo y una invertir petición por el trayecto corto (regla S #3). El nodo E, tras la recepción de la petición de puenteo procedente del nodo F por el trayecto largo, efectúa un puenteo de anillo y actualiza los bits 6-8 del byte K2 (regla I-S #1b). El nodo F, tras la recepción del acuse de recibo de puenteo procedente del nodo E por el trayecto largo, efectúa una comutación de anillo y actualiza su señalización de byte K (regla I-S #1b). El nodo E, tras la recepción por el trayecto largo del acuse de recibo de puenteo procedente del nodo F, completa la comutación. La señalización alcanza el estado estacionario.

En las aplicaciones transoceánicas, las actividades comutadoras tendrían lugar en los nodos intermedios. En todos los canales de protección de AU-4 que no se utilizan para proteger canales de servicio se restablece el tráfico adicional utilizando el DCC.

La eliminación es idéntica a la de una condición SF-R unidireccional.

### **I.5 Fallo de nodo**

Véase la Figura I.5.

Este ejemplo abarca el caso de un fallo de nodo tanto en un anillo de dos fibras como en uno de cuatro fibras. Fallo de nodo significa aquí que ha fallado toda transmisión, entrante o saliente, hacia y desde el nodo, afectando a los canales de servicio y a los canales de protección, y que el propio nodo ha perdido toda la información provisionada.

El estado inicial del nodo es el de reposo. En el momento  $T_1$ , los nodos E y G detectan una condición SF en sus canales de servicio y protección. Los nodos pasan a ser nodos comutantes (regla I-S #1) y originan peticiones de puenteo por los trayectos cortos y largos (regla S #1). Los nodos A y D, y todos los nodos intermedios sucesivos del trayecto largo, pasan al estado de transferencia total (regla I-P #1). El nodo E, tras la recepción de la petición de puenteo procedente del nodo G por el trayecto largo, silencia todo el tráfico posiblemente conectado de manera incorrecta, efectúa un puenteo y comutación de anillo y actualiza los bits 6-8 del byte K2 (regla S-S #1b). El nodo G, tras la recepción de la petición de puenteo procedente del nodo E por el trayecto largo, silencia todo el tráfico posiblemente conectado de manera incorrecta, efectúa un puenteo y comutación de anillo y actualiza los bits 6-8 del byte K2 (regla I-S #1b). La señalización alcanza el estado estacionario.

En las aplicaciones transoceánicas, las actividades comutadoras tendrían lugar en los nodos intermedios. En todos los canales de protección AU-4 que no se utilizan para proteger canales de servicio se restablece el tráfico adicional utilizando el DCC.

En el momento  $T_2$ , el nodo en fallo se ha recuperado físicamente pero no ha recuperado por completo su información de provisionamiento, lo que impide al nodo que se recupera efectuar una señalización de byte K adecuada. Hasta que el nodo que se recupera sea capaz de efectuar una señalización de byte K adecuada de acuerdo con el estado vigente del anillo, se transmiten códigos APS por defecto (regla I-S #3). Los nodos E y G detectan la eliminación física de la señal procedente del nodo F pero reciben también códigos APS por defecto. Mientras los nodos E y G reciben los códigos APS por defecto, no declaran el defecto eliminado (regla I-S #4). La señalización alcanza el estado estacionario.

# Reemplazada por una versión más reciente

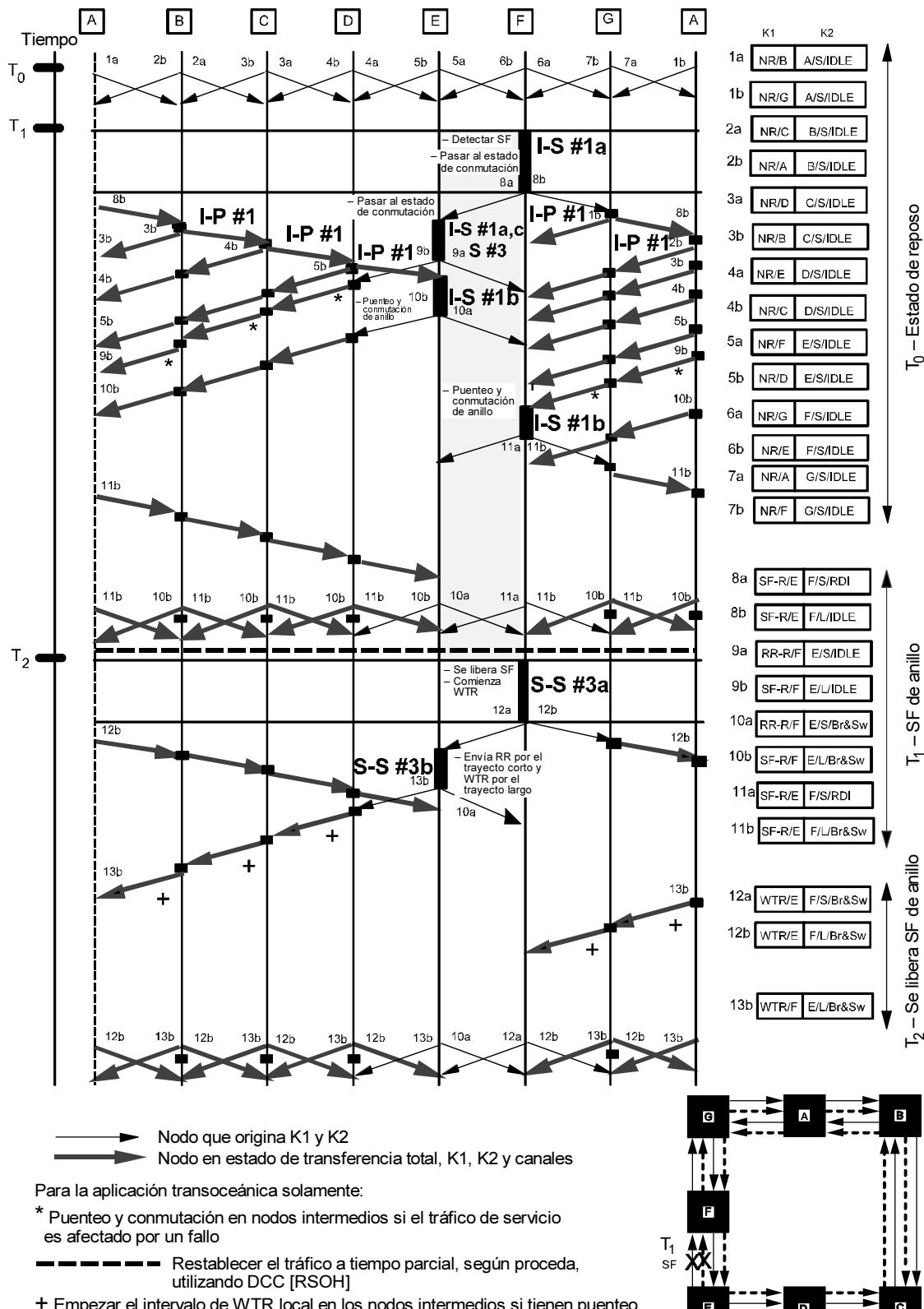


FIGURA I.2/G.841  
Anillo de protección compartida de MS de dos o cuatro fibras –  
SF unidireccional (anillo)

# Reemplazada por una versión más reciente

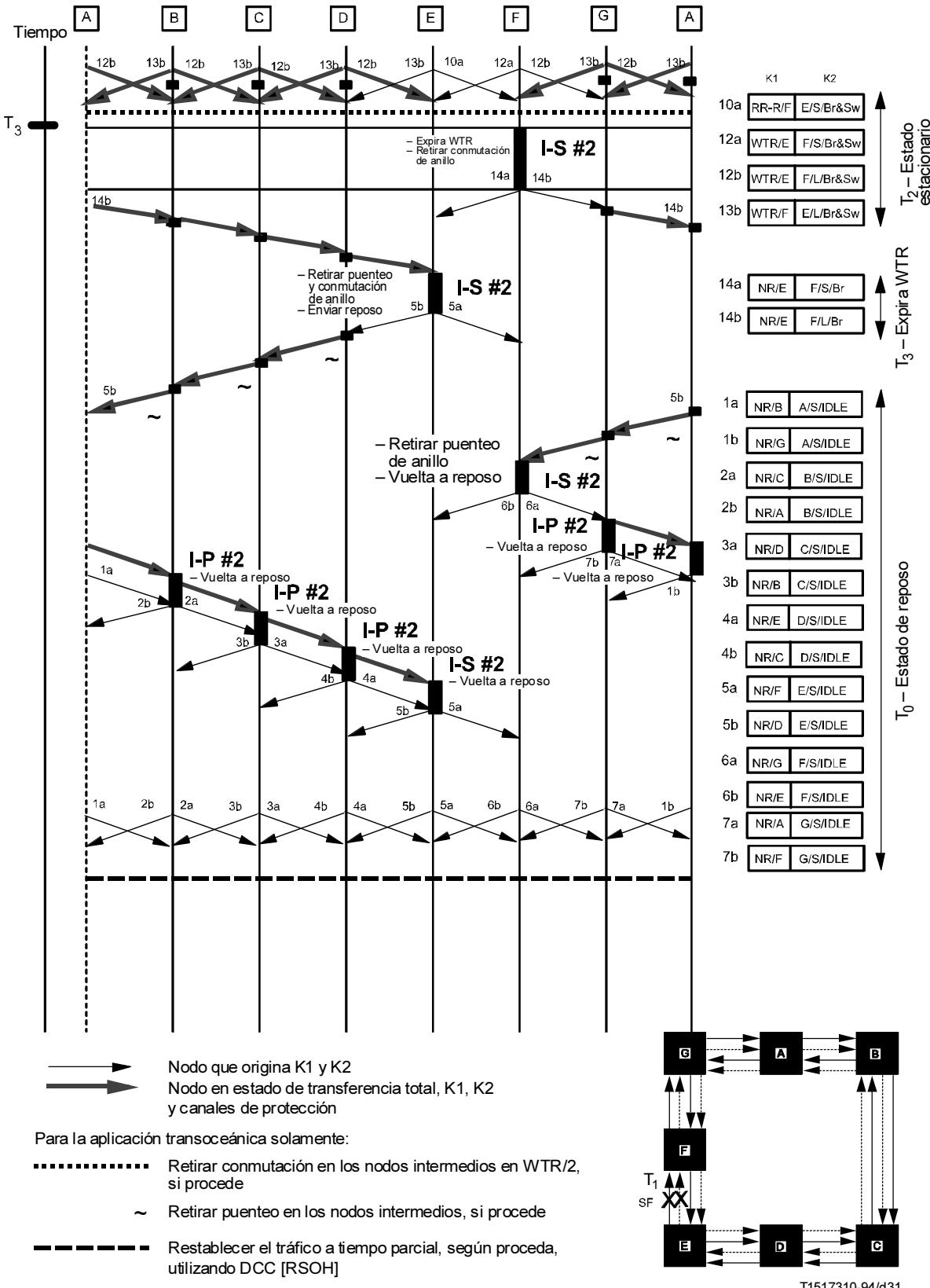


FIGURA I.2/G.841 (fin)

Anillo de protección compartida de MS de dos o cuatro fibras – SF unidireccional (anillo)

# Reemplazada por una versión más reciente

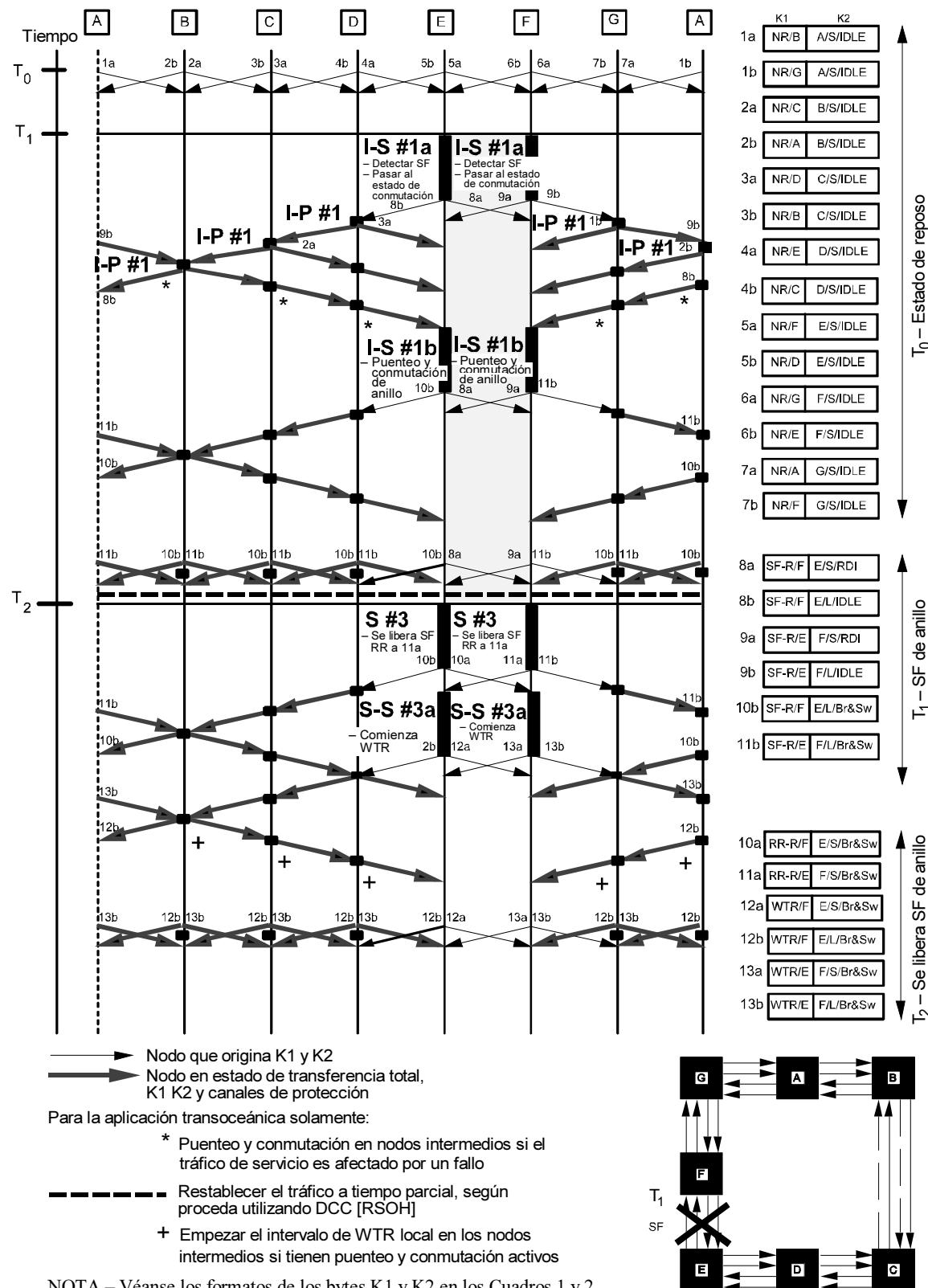


FIGURA I.3/G.841

Anillo de protección compartida de MS de dos o cuatro fibras –  
SF bidireccional (anillo)

# Reemplazada por una versión más reciente

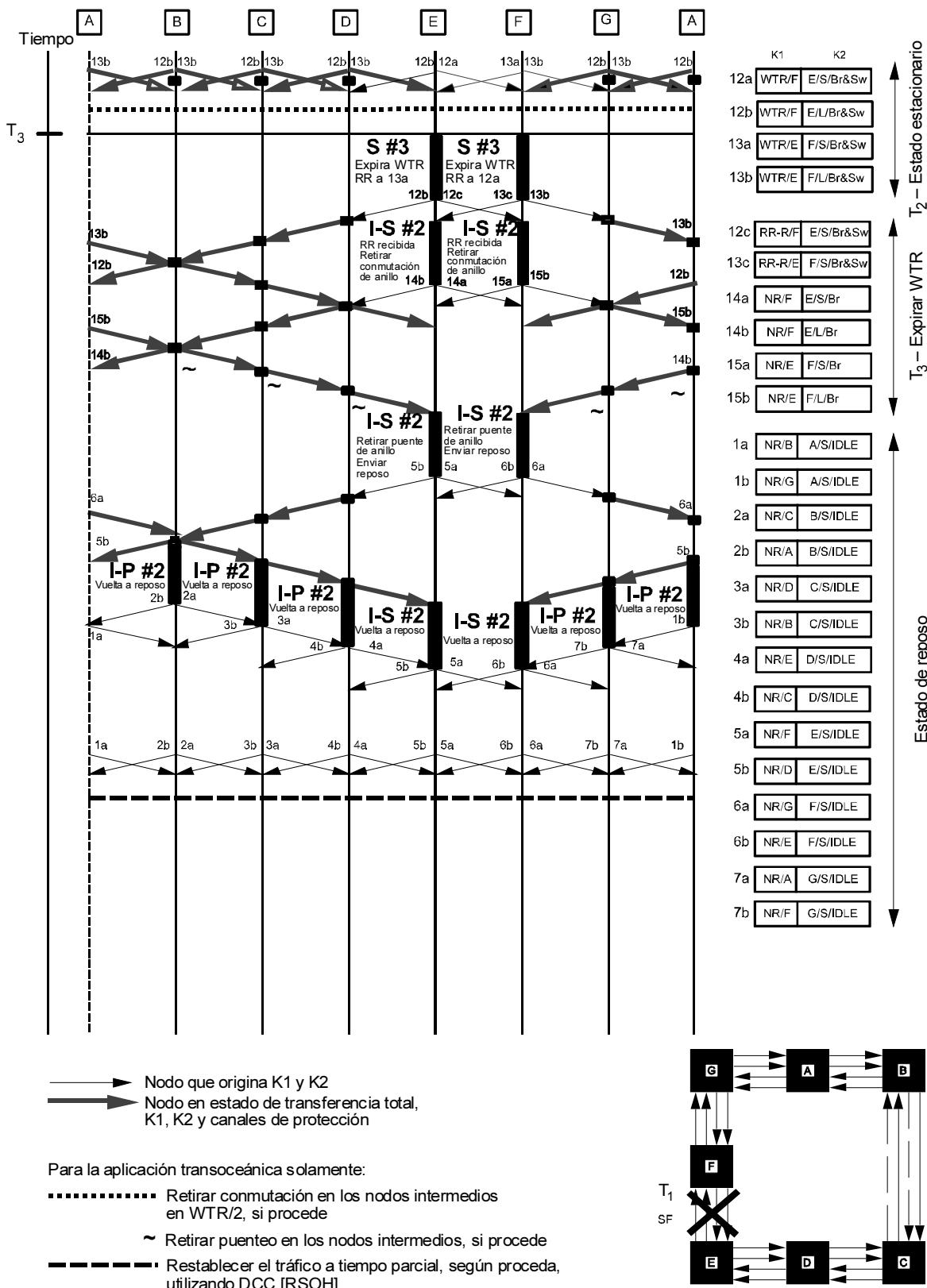


FIGURA I.3/G.841 (fin)

Anillo de protección compartida de MS de dos o cuatro fibras – SF bidireccional (anillo)

# Reemplazada por una versión más reciente

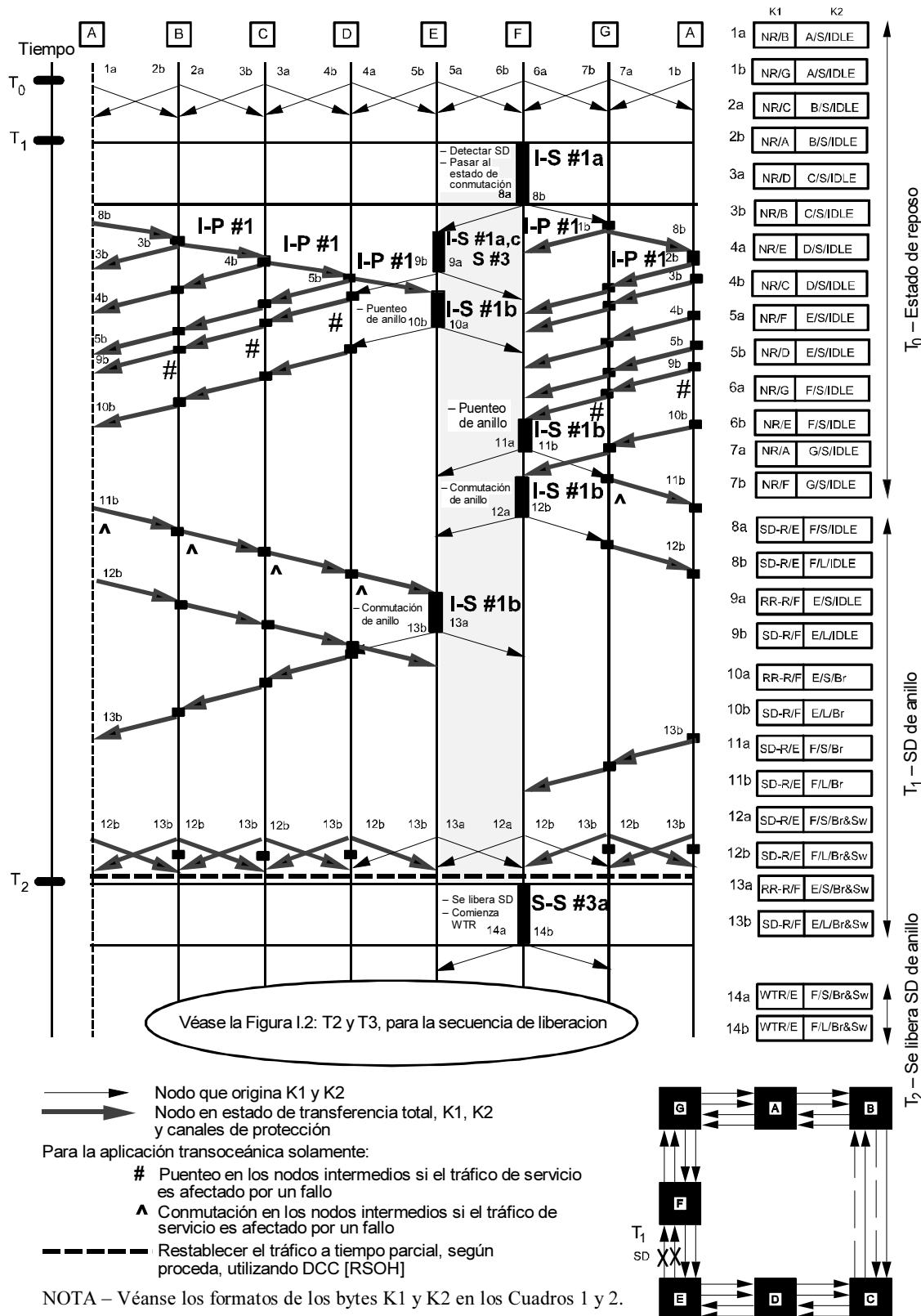


FIGURA I.4/G.841

Anillo de protección compartida de MS de dos o cuatro fibras – SD unidireccional (anillo)

# Reemplazada por una versión más reciente

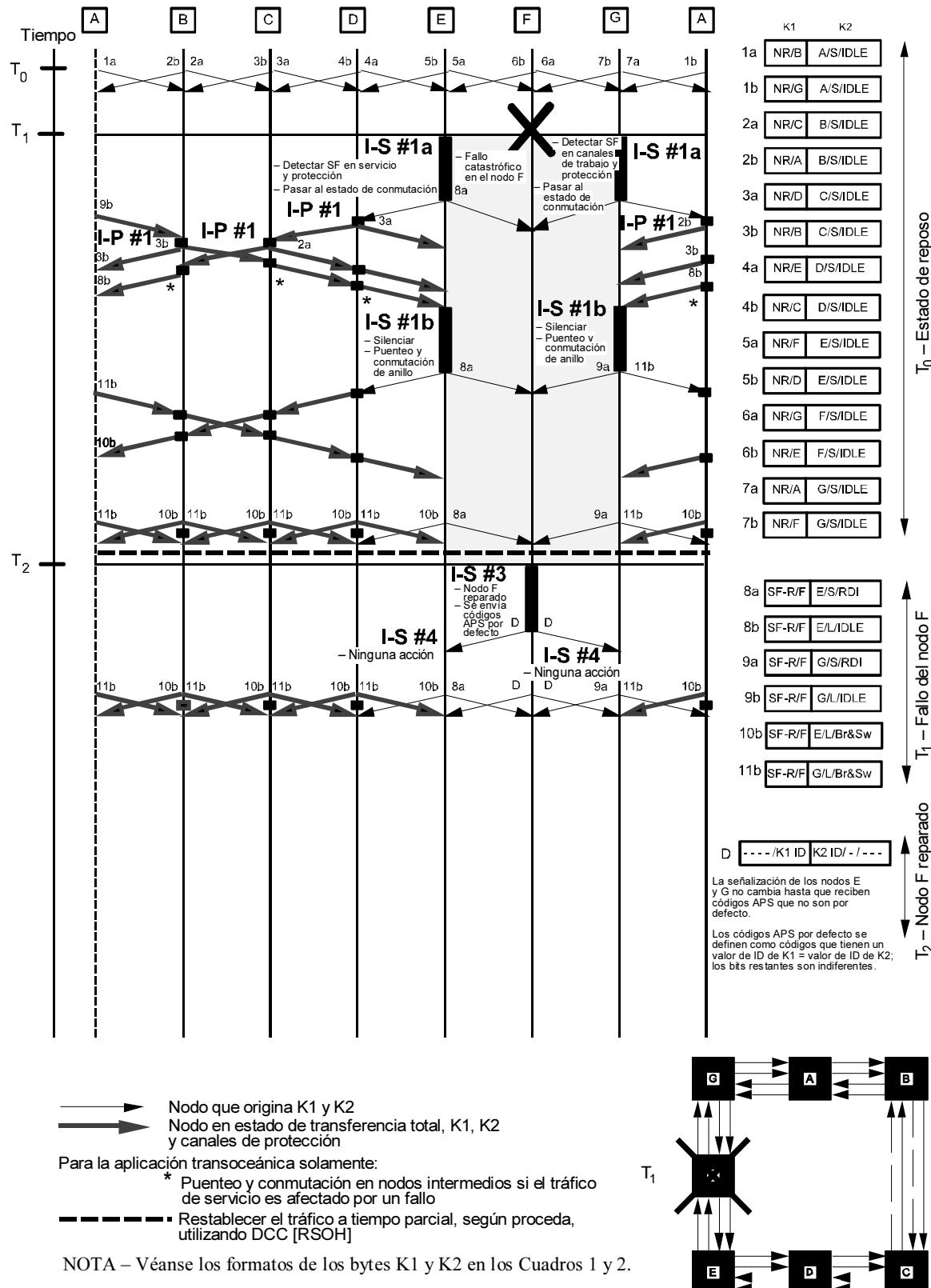


FIGURA I.5/G.841

Anillo de protección compartida de MS  
de cuatro fibras – Fallo de nodo

T1517350-94/d35

# Reemplazada por una versión más reciente

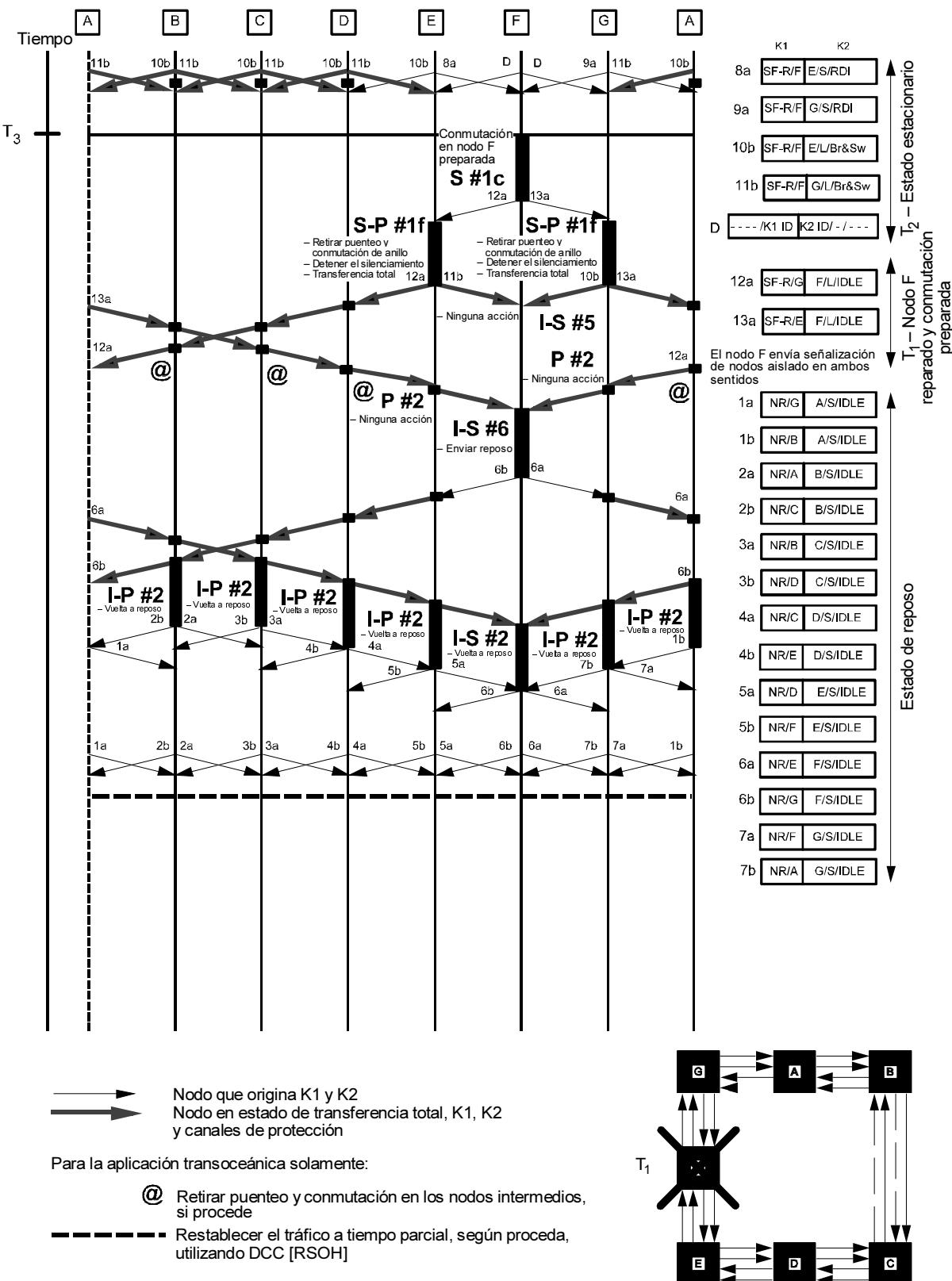


FIGURA I.5/G.841 (fin)

Anillo de protección compartida de MS  
de cuatro fibras – Fallo de nodo

T1517360-94/d36

## **Reemplazada por una versión más reciente**

En el momento  $T_3$ , el nodo F se ha recuperado plenamente y señala de manera apropiada. Los nodos E y G reciben códigos APS que no son por defecto y declaran el defecto eliminado. Los intervalos de WTR de los nodos E y G son desplazados con prioridad por las peticiones de puenteo de trayecto largo de prioridad mayor, haciendo que los nodos E y G retiren su puenteo y comutación, detengan el silenciamiento y pasen al estado de transferencia total (regla S-P #1f). Después de que los nodos E y G han pasado al estado de transferencia total, el nodo F recibe peticiones de puenteo de trayecto largo destinadas a él mismo, procedentes tanto de E como de G, y no realiza ninguna acción (regla I-S #5). Cuando el nodo F recibe las mismas señales que él está enviando, señala el código reposo en ambos sentidos (regla I-S #6). Todos los nodos pasan a continuación en cascada al estado de reposo.

### **I.6 SF-R unidireccional que desplaza con prioridad a una SD-S unidireccional en tramos no adyacentes**

Véase la Figura I.6

Este ejemplo se refiere al caso de una condición de fallo de señal unidireccional (anillo) en un anillo de cuatro fibras que desplaza con prioridad a una condición de degradación de señal unidireccional (tramo) que existía previamente en un tramo no adyacente.

El estado inicial del anillo es el de reposo. En el instante  $T_1$ , el nodo D detecta una condición SD-S procedente del nodo C en sus canales de trabajo. La señalización sigue su curso como se muestra en la Figura I.1, salvo que:

- 1) los nodos de comutación pasan a ser los nodos C y D, en lugar de E y F; y
- 2) la petición de puenteo pasa a ser SD-S, en lugar de SF-S.

La señalización alcanza el estado estacionario.

En el instante  $T_2$ , el nodo F detecta una condición SF procedente del nodo G en sus canales de trabajo y de protección. El nodo F se convierte en un nodo de comutación (regla S-P #2b) y origina peticiones de puenteo en ambos sentidos (regla S #1). El nodo G, al ver la petición de puenteo de trayecto corto procedente del nodo F, también se convierte en nodo de comutación (regla S-P #2b). El nodo G origina invertir petición hacia atrás en el trayecto corto, y SF-R en el trayecto largo (regla S #3). Los nodos A, B y E intermedios cambian de transferencia de bytes K a transferencia total (regla P-P #1). El nodo D, al ver una petición de puenteo de anillo de prioridad superior, retira su comutación de tramo, actualiza los bits 6-8 del byte K2, y origina ninguna petición en ambos sentidos (regla S-S #2c). El nodo C, al ver ninguna petición y la comutación retirada del nodo D, retira su puenteo y comutación, actualiza los bits 6-8 del byte K2, y actúa conforme a su entrada de máxima prioridad (regla S-S #2d, primer punto) para originar ninguna petición. El nodo C ve finalmente una petición de puenteo de anillo destinada al nodo F, pero esto no cambia la señalización del nodo C (regla S-P #1a). El nodo D, al ver una comutación retirada en el nodo C, retira su puenteo y actúa conforme a su entrada de máxima prioridad (regla S-S #2e) para pasar al estado de transferencia total. El nodo C, al ver el puente retirado del nodo D, actúa conforme a su entrada de máxima prioridad (regla S-P #1b) para pasar al estado de transferencia total. Con todos los nodos intermedios en transferencia total, los nodos F y G reciben finalmente peticiones de puenteo de anillo de trayecto largo. Los nodos F y G efectúan cada uno un puenteo y comutación (regla I-S #1b, segundo punto) y actualiza los bits 6-8 del byte K2. Las señalización alcanza el estado estacionario.

En el instante  $T_3$  se libera la condición SF del nodo E al nodo F en los canales de trabajo y de protección. El nodo F pasa a espera de restablecimiento (regla S-S #3a). El nodo G, al ver la petición de puenteo WTR procedente del nodo F, también pasa a espera de restablecimiento (regla S-S #3b). El nodo D, al ver dos peticiones de puenteo WTR que tienen menor prioridad que su condición SD detectada localmente, se convierte en un nodo de comutación (regla S-P #2a, punto 2) y señala de manera apropiada. El nodo C, al ver una petición de puenteo de tramo de prioridad superior destinada a él, se convierte también en un nodo de comutación (regla S-P #2a, punto 2), efectúa un puenteo de tramo y actualiza los bits 6-8 del byte K2 (regla I-S #1b). El nodo F pierde su petición de puenteo de anillo de trayecto largo debido al estado de petición de puenteo de tramo procedente del nodo D. El nodo F retira su puenteo y comutación y señala su entrada (WTR) de máxima prioridad (regla S #5). En forma similar, cuando el nodo G pierde su petición de puenteo de anillo de trayecto largo, retira su puenteo y comutación y señala su entrada de máxima prioridad (regla S #5). El nodo D, al ver un código puenteado en el trayecto corto procedente del nodo C, efectúa un puenteo y comutación de tramo y actualiza los bits 6-8 del byte K2 (regla I-S #1b). El nodo C, al ver un código puenteado y comutado procedente del nodo D, completa el proceso efectuando una comutación de tramo y actualizando los bits 6-8 del byte K2 (regla I-S #1b).

# Reemplazada por una versión más reciente

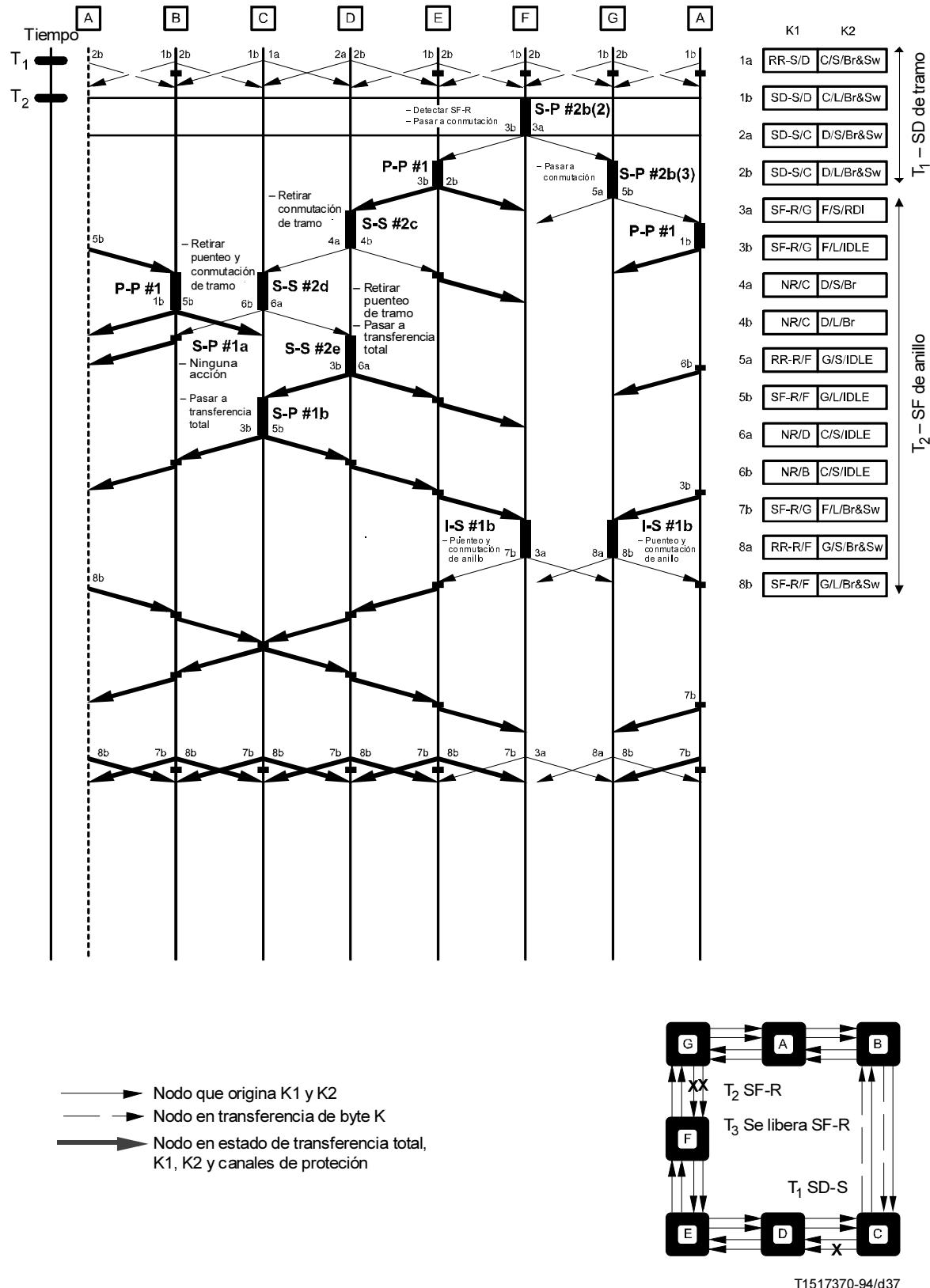
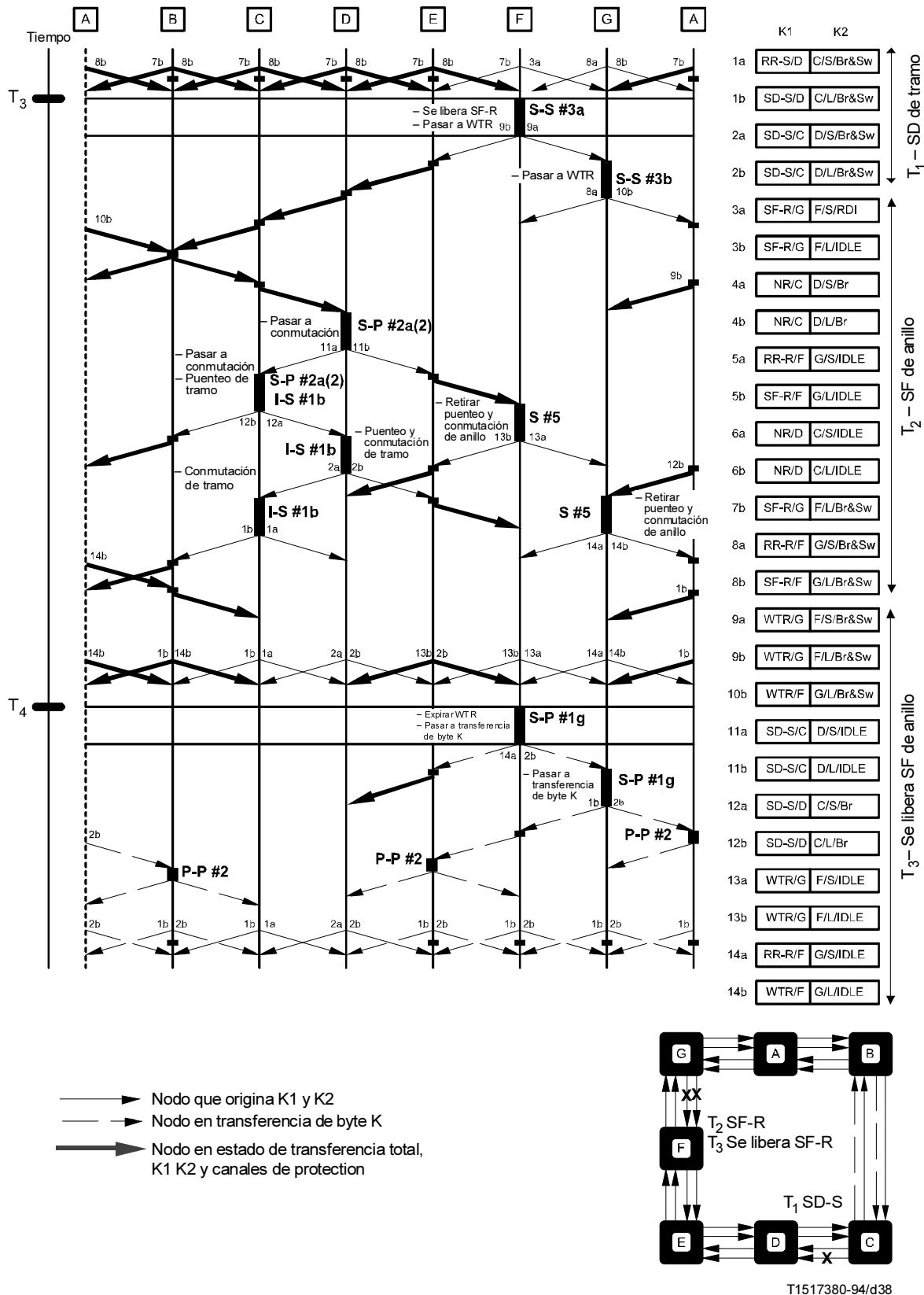


FIGURA I.6/G.841

Anillo de protección compartida de MS de cuatro fibras – SF-R unidireccional que desplaza con prioridad a un SD-S unidireccional en tramos no adyacentes

# Reemplazada por una versión más reciente



## **Reemplazada por una versión más reciente**

En el instante T<sub>4</sub>, expira WTR en el nodo F. La entrada de máxima prioridad del nodo F es ahora un estado de petición de puenteo de tramo destinado al nodo C, de modo tal que el nodo F pasa a transferencia de byte K (regla S-P #1g). El nodo G, al ver un estado de petición de puenteo de tramo no destinado a él procedente de ambos sentidos, también pasa a transferencia de byte K. Los nodos A, E y B intermedios pasan entonces de transferencia total a transferencia de byte K. La señalización alcanza el mismo estado estacionario que en el instante T<sub>1</sub>.

En el instante T<sub>5</sub> (no mostrado) se libera la condición SD de tramo en los canales de trabajo del nodo C al nodo D. La señalización continúa su curso como se indica en el instante T<sub>2</sub> de la Figura I.1, salvo que:

- 1) los nodos de conmutación se convierten en nodos C y D, en lugar de nodos E y F; y
- 2) la petición de puenteo se convierte en SD-S, en lugar de SF-S.

### **I.7 SF-S unidireccional que desplaza con prioridad a un SF-R unidireccional en tramos adyacentes**

Véase la Figura I.7.

Este ejemplo se refiere al caso de una condición de fallo de señal unidireccional (tramo) en un anillo de cuatro fibras que desplaza con prioridad a una condición de fallo de señal unidireccional (anillo) que existía previamente en un tramo adyacente.

El estado inicial del anillo es el de reposo. En el instante T<sub>1</sub>, el nodo C detecta una condición SF procedente del nodo D en sus canales de trabajo y de protección. La señalización continúa como en la Figura I.2 (instante T<sub>1</sub>), salvo que los nodos de conmutación se convierten en nodos C y D, en lugar de E y F. La señalización alcanza el estado estacionario.

En el instante T<sub>2</sub> el nodo E detecta una condición SF procedente del nodo D en sus canales de trabajo. El nodo E se convierte en nodo de conmutación (regla S-P #2a, punto 2) y origina una petición de puenteo de tramo hacia el nodo D y una situación de petición de puenteo de tramo hacia el nodo F (regla S #1, G #1). El nodo C, al ver esta situación de petición de puenteo de tramo, retira su puenteo y conmutación de anillo pues ya no recibe una petición de puenteo de anillo de trayecto largo (regla S #5). El nodo C actualiza sus bits 6-8 del byte K2 y origina SF-R en el byte K1 pues esa es su entrada de máxima prioridad (regla S #5). El nodo D, al ver la petición de puenteo de tramo de máxima prioridad procedente del nodo E, retira su puenteo y conmutación de anillo, efectúa un puenteo de tramo hacia el nodo E (regla S-S #2f) y señaliza de manera apropiada (regla I-S #1b, tercer punto, y regla S #3). El nodo E, al ver el código puenteado procedente del nodo D, efectúa un puenteo y conmutación de tramo y actualiza los bits 6-8 del byte K2 (regla I-S #1b, tercer punto). El nodo D, al ver el código puenteado procedente del nodo E, efectúa una conmutación y actualiza los bits 6-8 del byte K2 como corresponde (regla I-S #1b, tercer punto). La señalización alcanza el estado estacionario.

En el instante T<sub>3</sub> se libera la condición SF del nodo D al nodo E en los canales de trabajo. El nodo E debería pasar a espera al restablecimiento, pero detecta otro fallo (regla S-S #3a). El nodo E, al ver la petición de puenteo SF-R destinada al nodo D (para un tramo que no es adyacente), retira su conmutación de tramo, señaliza ninguna petición en el byte K1 y puenteado en el byte K2 (regla S-S #2c). El nodo D, al ver los códigos ninguna petición y puenteado procedentes del nodo E, retira su puenteado y conmutación de tramo y actúa conforme a la entrada del nodo C para señalizar hacia atrás al nodo C una petición de puenteo de anillo (regla S-S #2d). El nodo E, al ver que el nodo D ha retirado su conmutación, retira su puenteo (regla S-S #2e). El nodo E ve también una petición de puenteo de anillo de trayecto largo destinada al nodo D, por lo que pasa también a transferencia total (regla S-S #2e, cuarto punto). El nodo E, al ver una petición de puenteo de anillo de trayecto largo procedente del nodo C, efectúa un puenteo y conmutación de anillo y actualiza los bits 6-8 del byte K2 (regla I-S #1b). El nodo C, al ver una petición de puenteo de anillo de trayecto largo procedente del nodo D, también efectúa un puenteo y conmutación de anillo y actualiza los bits 6-8 del byte K2 (regla I-S #1b). La señalización alcanza el mismo estado estacionario que en el instante T<sub>1</sub>.

En el instante T<sub>4</sub> (no mostrado) se libera la condición SF en los canales de trabajo y de protección del nodo D al nodo C. La señalización continúa de manera similar a la indicada en la Figura I.2 (instante T<sub>2</sub>), salvo que los nodos de conmutación se convierten en nodos C y D, en lugar de E y F.

# Reemplazada por una versión más reciente

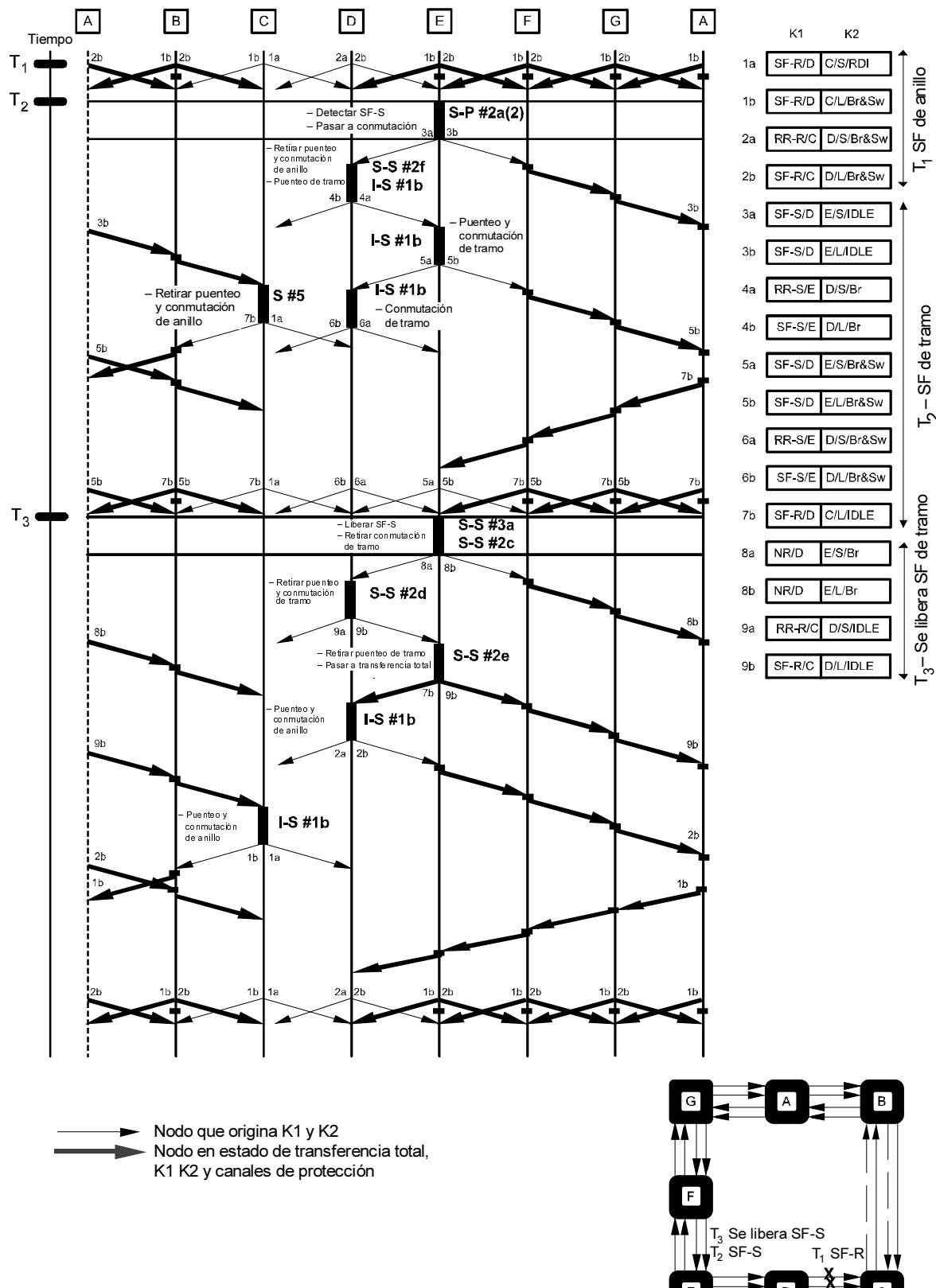


FIGURA I.7/G.841

T1517390-94/d39

Anillo de protección compartida de MS de cuatro fibras – SF-S unidireccional que desplaza con prioridad a un SF-R unidireccional en tramos adyacentes

## **Reemplazada por una versión más reciente**

### **I.8 SF-R unidireccional que desplaza con prioridad a una SD-S unidireccional en tramos adyacentes**

Véase la Figura I.8.

Este ejemplo se refiere al caso de una condición de fallo de señal unidireccional (anillo) en un anillo de cuatro fibras que desplaza con prioridad a una condición de degradación de señal unidireccional (tramo) que existía previamente en un tramo adyacente.

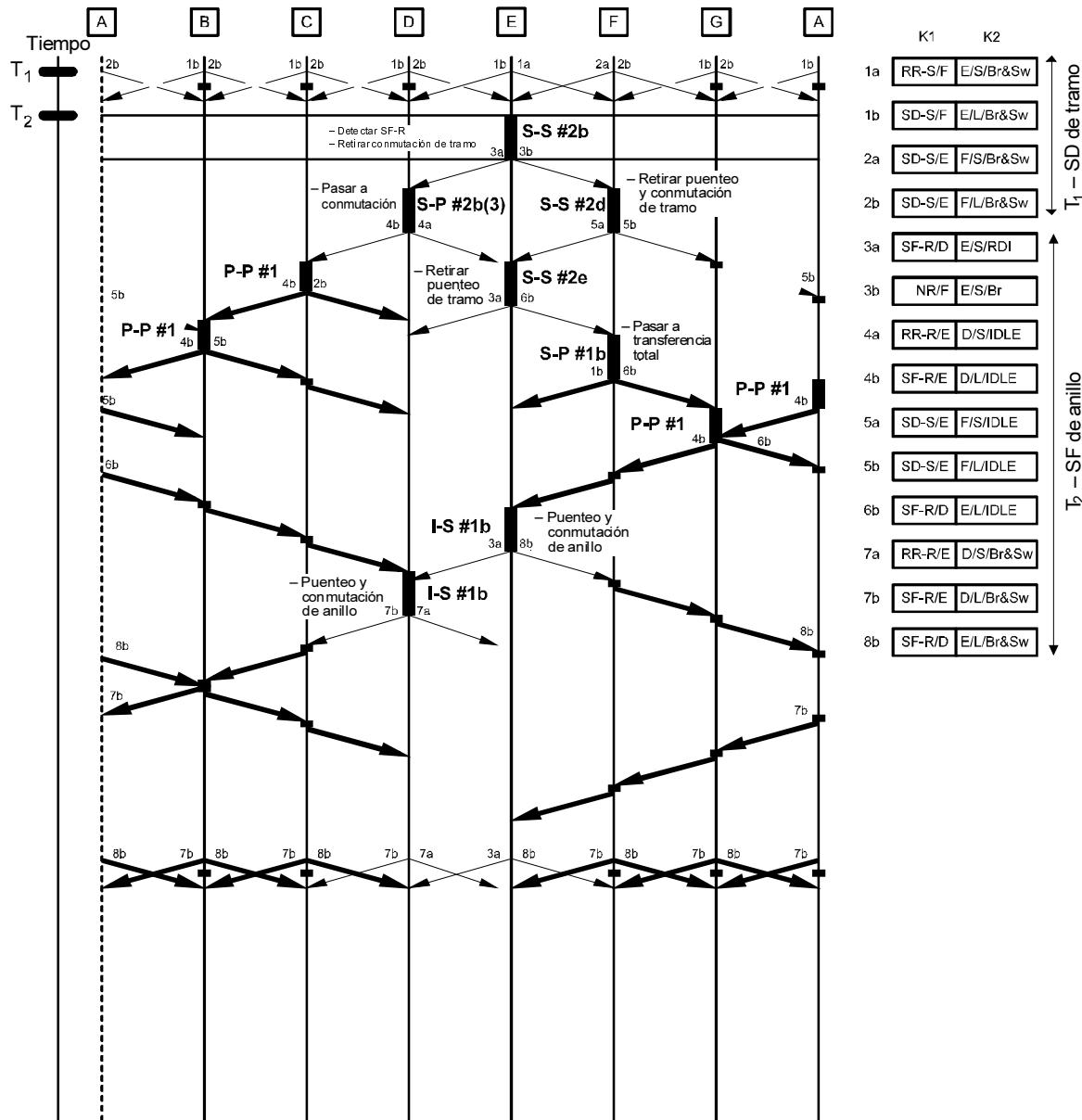
El estado inicial del anillo es el de reposo. En el instante  $T_1$  el nodo F detecta una condición SD procedente del nodo E en sus canales de trabajo. La señalización continúa como se indica en la Figura I.1 (instante  $T_1$ ), salvo que la petición de puenteo se convierte en SD-S, en lugar de SF-S. La señalización alcanza el estado estacionario.

En el instante  $T_2$  el nodo E detecta una condición SF procedente del nodo D en sus canales de trabajo y de protección. El nodo E retira su comutación de tramo, origina una petición de puenteo de anillo de fallo de señal (en el byte K1) y una indicación de defecto distante de sección de multiplexación (MS-RDI) (en el byte K2) hacia el nodo D, y origina ninguna petición (en el byte K1) y puenteado (en el byte K2) hacia el nodo F (regla S-S #2b). El nodo D se convierte en un nodo de comutación (regla S-P #2b, punto 3). El nodo D origina invertir petición en el trayecto corto y una petición de puenteo de anillo fallo de señal en el trayecto largo (regla S #3). Esta petición de puenteo de anillo de trayecto largo hace pasar los nodos C, B, y A del estado de transferencia de byte K al estado de transferencia total (regla P-P #1). El nodo F, al ver una indicación ninguna petición y la comutación retirada del nodo E, retira su puenteo y comutación, actualiza los bits 6-8 del byte K2 y actúa conforme a su entrada de máxima prioridad (regla S-S #2d, último punto) para originar una petición de puenteo de tramo de degradación de señal hacia el nodo E. El nodo E, al ver una comutación retirada en el nodo F, retira su puenteo, actualiza los bits 6-8 del byte K2 y actúa conforme a su entrada de máxima prioridad (regla S-S #2e, tercer punto) para originar peticiones de puenteo de anillo en ambos sentidos. El nodo F, al ver el puenteo retirado del nodo E, actúa conforme a su entrada de máxima prioridad (regla S-P #1b) para pasar a transferencia total. Esto permite que una petición de puenteo de anillo de trayecto largo llegue al nodo G, y el nodo G pasa de transferencia de byte K a transferencia total (regla P-P #1). Con todos los nodos intermedios en transferencia total, los nodos E y D reciben finalmente peticiones de puenteo de anillo de trayecto largo. Los nodos E y D efectúan cada uno un puenteo y comutación (regla I-S #1b, segundo punto) y actualizan los bits 6-8 del byte K2. La señalización alcanza el estado estacionario.

En el instante  $T_3$  se libera la condición SF en los canales de trabajo y de protección del nodo D al nodo E. El nodo E inicia su periodo de espera de restablecimiento y señaliza en consecuencia (regla S-S #3a). El nodo D, al ver la petición de puenteo WTR procedente del nodo E, inicia también su periodo de espera de restablecimiento y señaliza en consecuencia (regla S-S #3b). El nodo F, al ver las peticiones de puenteo WTR de ambos sentidos, actúa conforme al hecho de que su condición SD-S local es de prioridad superior, y se convierte en nodo de comutación de tramo (regla S-P #2a, punto 2). El nodo E, al ver la petición de puenteo de tramo procedente del nodo F, pierde su petición de puenteo de anillo de trayecto largo procedente del nodo D. Por tanto, el nodo E retira su puenteo y comutación de anillo (regla S #5) y actúa conforme a la petición de puenteo de tramo procedente del nodo F efectuando un puenteo de tramo (regla I-S #1b, tercer punto). El nodo F, al ver el código puenteado procedente del nodo F, efectúa un puenteo y comutación de tramo y actualiza los bits 6-8 del byte K2 (regla I-S #1b, tercer punto). El nodo E, al ver el código puenteado y comutado procedente del nodo F, completa el proceso efectuando una comutación de tramo y adaptando los bits 6-8 del byte K2 (regla I-S #1b, tercer punto). Entre tanto, el nodo D, al ver la petición de puenteo de tramo procedente del nodo F, pierde su petición de puenteo de anillo de trayecto largo procedente del nodo E. Por tanto, el nodo D retira su puenteo y comutación de anillo (regla S #5) y actúa conforme a la situación de petición de puenteo de tramo destinada al nodo E pasando a la transferencia de byte K (regla S-P #1g). Los nodos A, B, C y G intermedios en transferencia total reciben finalmente una situación de petición de puenteo de tramo no destinada a ellos proveniente de ambos sentidos, por lo que pasan a transferencia de byte K. La señalización alcanza el mismo estado estacionario que en el instante  $T_1$ .

En el instante  $T_4$  (no mostrado) se libera la condición SD del nodo E al nodo F en los canales de trabajo. La señalización continúa como en la Figura I.1 (instante  $T_2$ ), salvo que la petición de puenteo se convierte en SD-S, en lugar de SF-S.

# Reemplazada por una versión más reciente



- Nodo que origina K1 y K2
- Nodo en transferencia de byte K
- Nodo en estado de transferencia total, K1, K2 y canales de protección

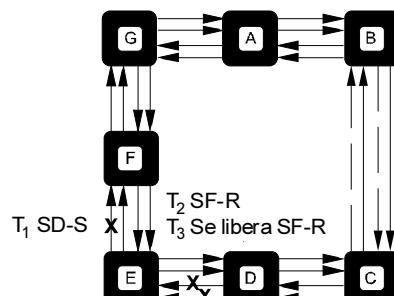


FIGURA I.8/G.841

Anillo de protección compartida de MS de cuatro fibras – SF-R unidireccional que desplaza con prioridad a un SD-S unidireccional en tramos adyacentes

# Reemplazada por una versión más reciente

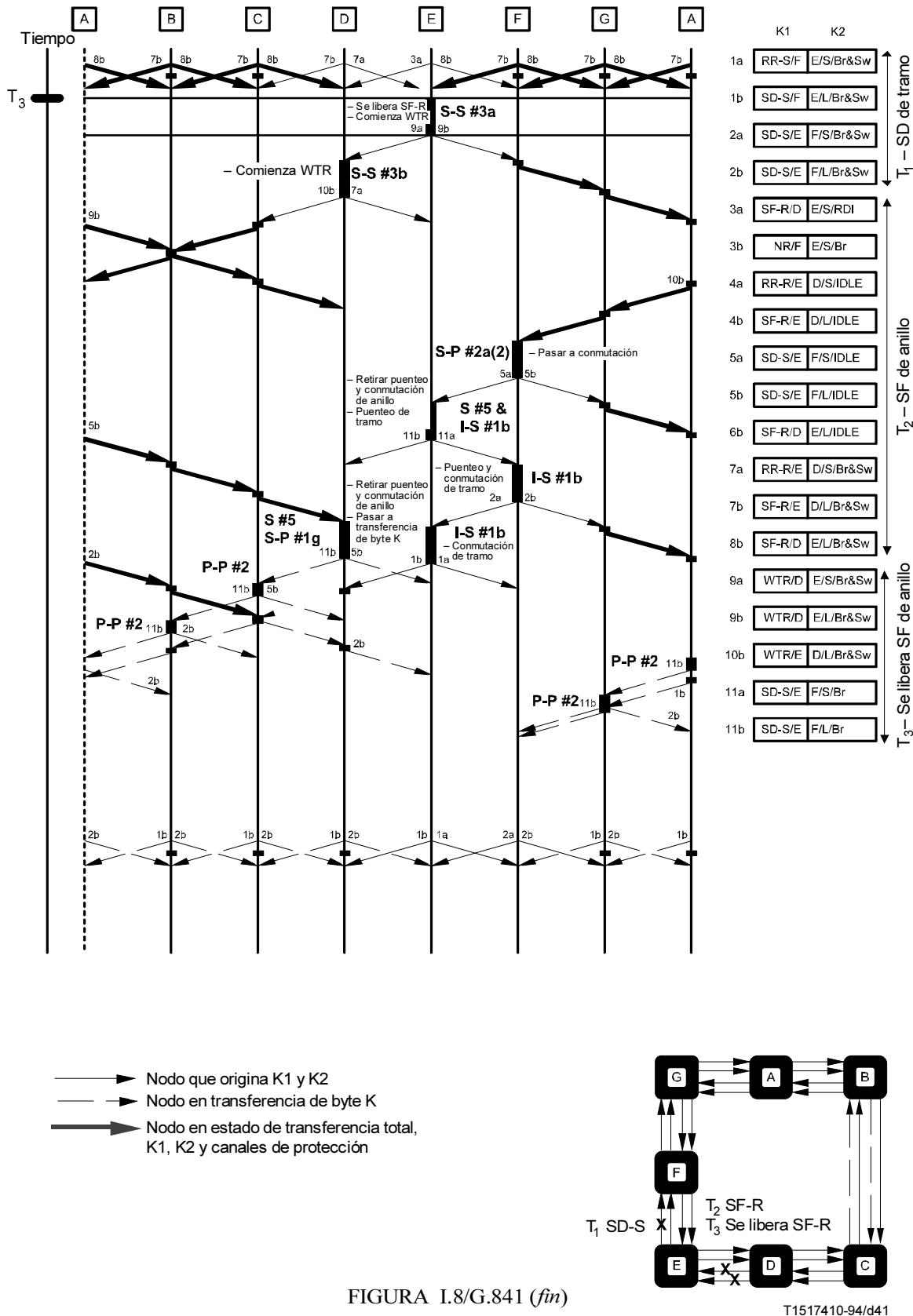


FIGURA I.8/G.841 (*fin*)

Anillo de protección compartida de MS de cuatro fibras – SF-R unidireccional que desplaza con prioridad a un SD-S unidireccional en tramos adyacentes

## Reemplazada por una versión más reciente

### I.9 SF-R unidireccional que coexiste con un SF-R unidireccional en tramos no adyacentes

Véase la Figura I.9.

Este ejemplo se refiere al caso de una condición de fallo de señal unidireccional (anillo) en un anillo de cuatro fibras que coexiste con otra condición de fallo de señal unidireccional (anillo) que existía previamente en un tramo no adyacente.

El estado inicial del anillo es el de reposo. En el instante  $T_1$  el nodo F detecta una condición SF en sus canales de trabajo y de protección. La señalización continúa como en la Figura I.2 (instante  $T_1$ ). La señalización alcanza el estado estacionario.

En el instante  $T_2$  el nodo C detecta una condición SF en sus canales de trabajo y de protección. El nodo C se convierte en nodo de conmutación (regla S-P #2a, punto 2), silencia el tráfico de ser necesario, efectúa un puenteo y conmutación de anillo y origina peticiones de puenteo de anillo en ambos sentidos (regla S-P #3). El nodo B, al ver la petición de puenteo procedente del nodo C, se convierte en nodo de conmutación (regla S-P #2a, punto 3). El nodo B también silencia el tráfico si es necesario, efectúa un puenteo y conmutación de anillo y origina peticiones de puenteo de anillo en ambos sentidos (regla S-P #3). Las peticiones de puenteo de anillo de trayecto largo procedentes de los nodos B y C no afectan a los puenteos y conmutaciones en los nodos E y F, pues pueden coexistir conmutaciones SF-R múltiples (regla S #4a, regla S #5). La señalización alcanza el estado estacionario.

En aplicaciones transoceánicas se produce una señalización adicional. Como se muestra en la Figura I.10, en el instante  $T_2$  el nodo C detecta una condición SF en sus canales de trabajo y de protección. El nodo C se convierte en nodo de conmutación (regla S-P #2a, punto 2), retira el tráfico adicional si lo hubiera, mantiene los puenteos y conmutaciones de anillo en los afluentes afectados por el primer fallo y origina peticiones de puenteo de anillo en ambos sentidos (regla S-P #3 en el Anexo A). El nodo B, al ver la petición de puenteo procedente del nodo C, se convierte en nodo de conmutación (regla S-P #2a, punto 3). El nodo B también retira el tráfico adicional si lo hubiera, mantiene los puenteos y conmutaciones de anillo en los afluentes afectados por el primer fallo y origina peticiones de puenteo de anillo en ambos sentidos (regla S-P #3 en el Anexo A). El nodo E (F), al ver la petición de puenteo de anillo procedente del nodo C (B), retira el tráfico adicional si lo hubiera, mantiene los puenteos y conmutaciones de anillo en los afluentes afectados por el primer fallo y actualiza los bits 6-8 del byte K2 para el código reposo (regla S-S #1a, punto 2, en el Anexo A). El nodo C (B) al ver la petición de puenteo de anillo y un código reposo procedente del nodo E (F), actualiza los bits 6-8 del byte K2 a puenteado y conmutado (regla S-S #1a, punto 2, en el Anexo A). El nodo E (F), al ver la petición de puenteo de anillo y el código puenteado y conmutado procedente del nodo C (B), actualiza los bits 6-8 del byte K2 a puenteado y conmutado (regla S-S #1a, punto 3, en el Anexo A). La señal alcanza el mismo estado estacionario que el descrito para la Figura I.9.

En el instante  $T_3$  se libera la condición SF del nodo B al nodo C en los canales de trabajo y de protección. El nodo C ve del nodo D una petición de puenteo de anillo para un tramo no adyacente. Esta petición tiene una prioridad superior que su condición local (WTR), de modo que el nodo C retira su puenteo y conmutación y pasa a transferencia total (regla S-P #1e). Esto permite que la señal invertir petición de anillo de tramo corto procedente del nodo B llegue al nodo E. El nodo E considera aún que ésta es una petición de puenteo de anillo válida, por lo que retiene su puenteo y conmutación de anillo (regla S #5, nota). El nodo B, al recibir ambas peticiones de puenteo de anillo que no están destinados a él, retira su puenteo y conmutación y pasa a transferencia total (regla S-P #1f). La señalización alcanza el mismo estado estacionario que en el instante  $T_1$ .

En aplicaciones transoceánicas la señalización es idéntica, pero los nodos tienen que efectuar acciones adicionales. Como se muestra en la Figura I.10, en el instante  $T_3$  se libera la condición SF del nodo B al nodo C en los canales de trabajo y de protección. El nodo C ve del nodo D una petición de puenteo de anillo para un tramo no adyacente, debida al primer SF-R entre los nodos E y F. Esta tiene una prioridad superior a la de su condición local (WTR), de modo que el nodo C mantiene los puenteos y conmutaciones de anillo en los afluentes afectados por el primer fallo y pasa a transferencia total (regla S-P #1e, punto 1, en el Anexo A). Esto permite que la señal invertir petición de anillo de trayecto corto procedente del nodo B llegue al nodo E. El nodo E aún considera que esta es una petición de puenteo de anillo válida, por lo que retiene su puenteo y conmutación de anillo (regla S #5, nota). El nodo B ve peticiones de puenteo de anillo que no están destinada a él, debido al primer SF-R entre los nodos E y F. El nodo B mantiene los puenteos y conmutaciones de anillo en los afluentes afectados por el primer fallo y pasa a transferencia total (regla S-P #1f, punto 1, en el Anexo A). La señalización alcanza el mismo estado estacionario que el descrito para la Figura I.9.

En el instante  $T_4$  (no mostrado) se libera la condición SF del nodo E al nodo F en los canales de trabajo y de protección. La señalización continúa como en la Figura I.2 (instante  $T_3$ ).

# Reemplazada por una versión más reciente

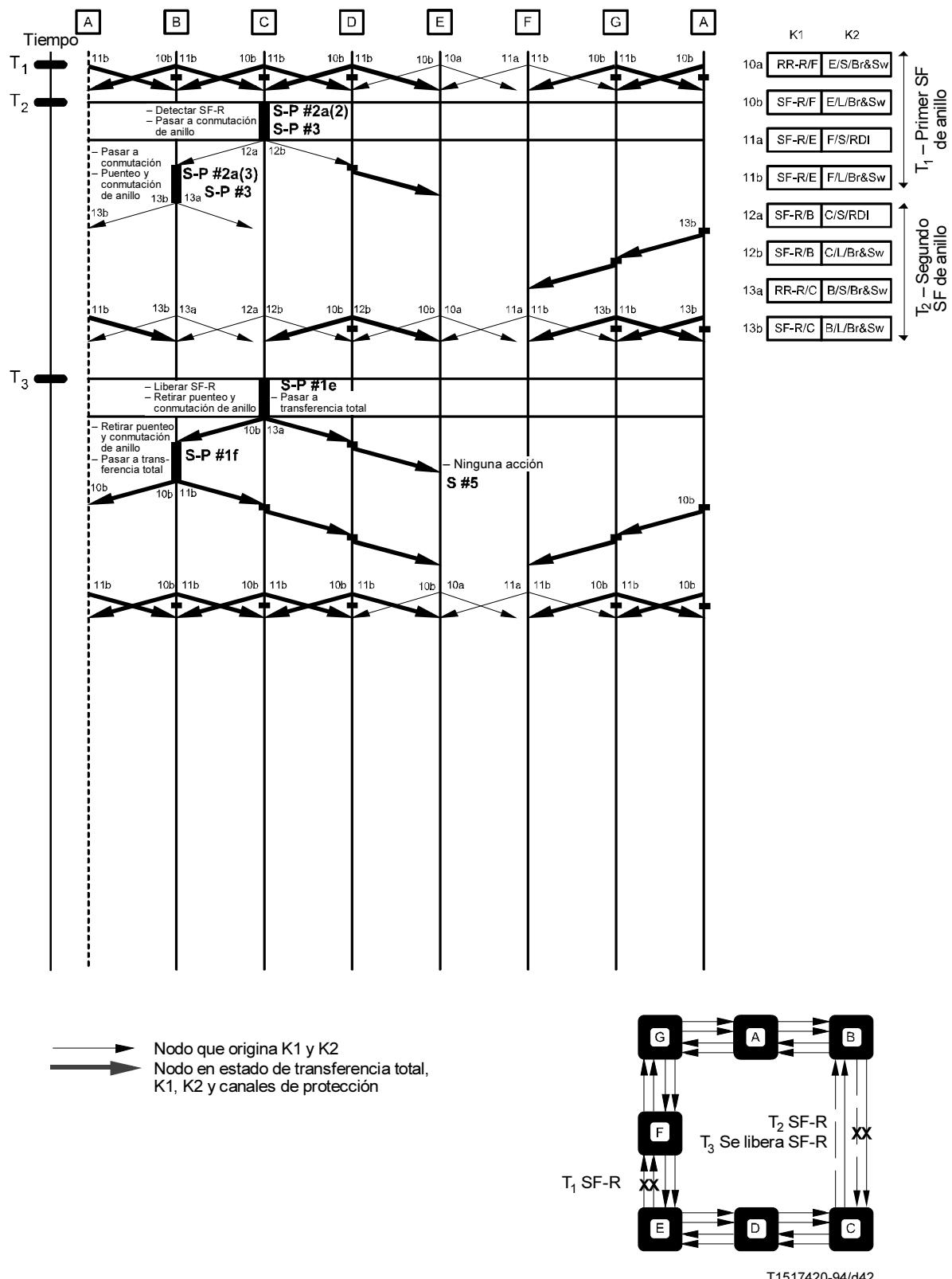


FIGURA I.9/G.841

Anillo de protección compartida de MS de cuatro fibras –  
SF-R unidireccional más SF-R unidireccional en tramos no adyacentes

# Reemplazada por una versión más reciente

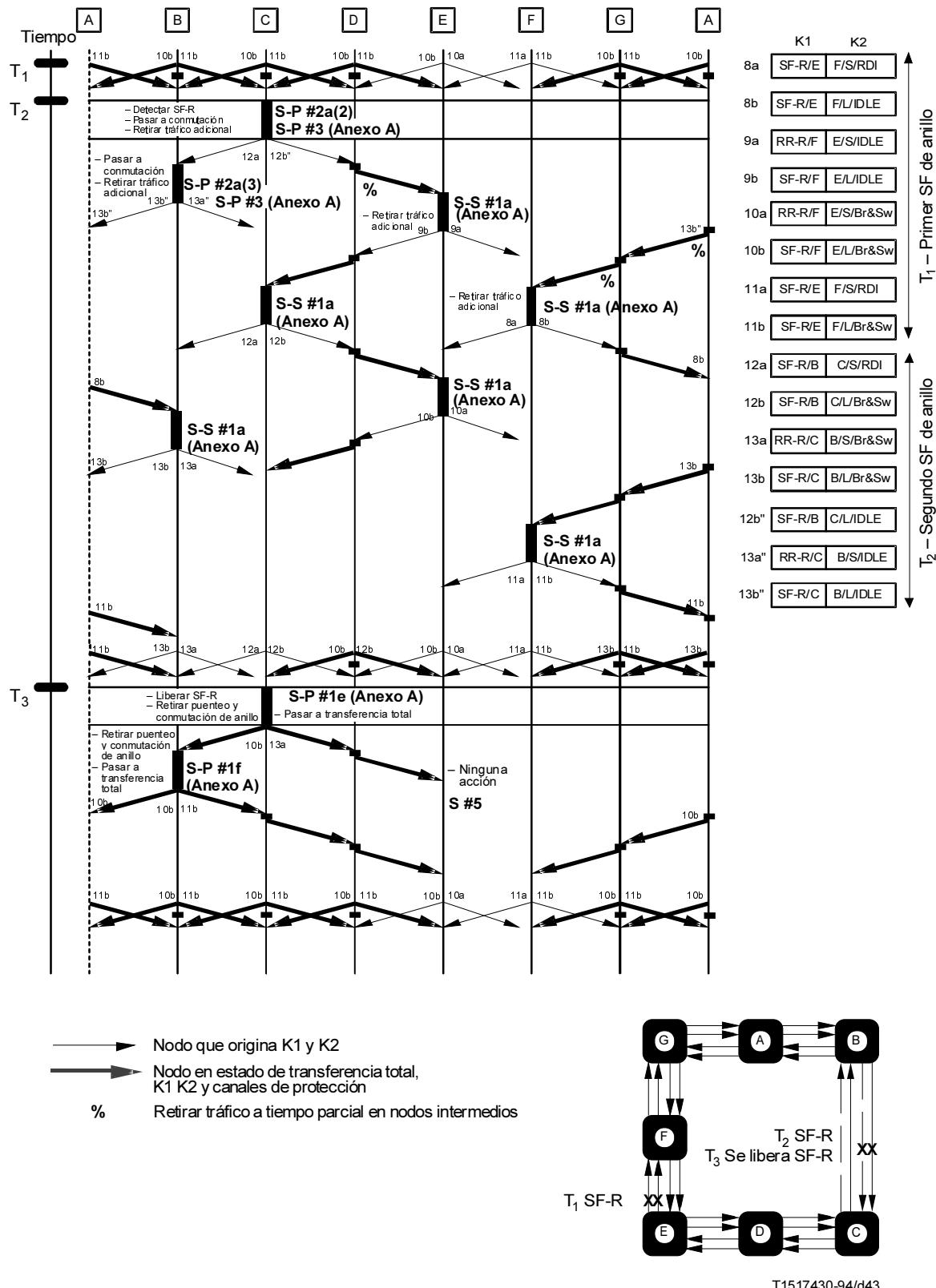


FIGURA I.10/G.841

Anillo de protección compartida de MS de cuatro fibras – SF-R unidireccional más SF-R unidireccional en tramos no adyacentes (aplicación transoceánica)