UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

# UIT-T G.841

(10/98)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE G: SISTEMAS Y MEDIOS DE TRANSMISIÓN, SISTEMAS Y REDES DIGITALES

Sistemas de transmisión digital – Redes digitales – Características de las redes con jerarquía digital síncrona

---

# Tipos y características de las arquitecturas de protección para redes de la jerarquía digital síncrona

Recomendación UIT-T G.841

(Anteriormente Recomendación del CCITT)

---

RECOMENDACIONES UIT-T DE LA SERIE G

**SISTEMAS Y MEDIOS DE TRANSMISIÓN, SISTEMAS Y REDES DIGITALES**

| | |
|---|---|
| CONEXIONES Y CIRCUITOS TELEFÓNICOS INTERNACIONALES | G.100–G.199 |
| ***SISTEMAS INTERNACIONALES ANALÓGICOS DE PORTADORAS*** | |
| CARACTERÍSTICAS GENERALES COMUNES A TODOS LOS SISTEMAS ANALÓGICOS DE PORTADORAS | G.200–G.299 |
| CARACTERÍSTICAS INDIVIDUALES DE LOS SISTEMAS TELEFÓNICOS INTERNACIONALES DE PORTADORAS EN LÍNEAS METÁLICAS | G.300–G.399 |
| CARACTERÍSTICAS GENERALES DE LOS SISTEMAS TELEFÓNICOS INTERNACIONALES EN RADIOENLACES O POR SATÉLITE E INTERCONEXIÓN CON LOS SISTEMAS EN LÍNEAS METÁLICAS | G.400–G.449 |
| COORDINACIÓN DE LA RADIOTELEFONÍA Y LA TELEFONÍA EN LÍNEA | G.450–G.499 |
| ***EQUIPOS DE PRUEBAS*** | |
| ***CARACTERÍSTICAS DE LOS MEDIOS DE TRANSMISIÓN*** | |
| ***SISTEMAS DE TRANSMISIÓN DIGITAL*** | |
| EQUIPOS TERMINALES | G.700–G.799 |
| REDES DIGITALES | G.800–G.899 |
| Generalidades | G.800–G.809 |
| Objetivos de diseño para las redes digitales | G.810–G.819 |
| Objetivos de calidad y disponibilidad | G.820–G.829 |
| Funciones y capacidades de la red | G.830–G.839 |
| **Características de las redes con jerarquía digital síncrona** | **G.840–G.849** |
| Red de gestión de las telecomunicaciones | G.850–G.859 |
| SECCIONES DIGITALES Y SISTEMAS DIGITALES DE LÍNEA | G.900–G.999 |

*Para más información, véase la Lista de Recomendaciones del UIT-T.*

**RECOMENDACIÓN UIT-T G.841**

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


## 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 de multiplexación (SDH) (por ejemplo, protección de sección de multiplexación 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 implementaciones 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.



## Orígenes

La Recomendación UIT-T G.841, ha sido revisada por la Comisión de Estudio 15 (1997-2000) del UIT-T y fue aprobada por el procedimiento de la Resolución N.° 1 de la CMNT el 13 de octubre de 1998.

## PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la 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.° 1 de la CMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

## NOTA

En esta Recomendación, la expresión *empresa de explotación reconocida (EER)* designa a toda persona, compañía, empresa u organización gubernamental que explote un servicio de correspondencia pública. Los términos *Administración, EER* y *correspondencia pública* están definidos en la *Constitución de la UIT (Ginebra, 1992).*

## PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB.

## ÍNDICE

**Página**

**Recomendación G.841**

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

*(revisada en 1998)*

## 1 Alcance

La presente Recomendación describe los distintos mecanismos de protección para las redes de la jerarquía digital síncrona (SDH, *synchronous digital hierarchy*), 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 siguientes Recomendaciones del UIT-T 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 otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes.

– Recomendación UIT-T G.707 (1996), *Interfaz de nodo de red para la jerarquía digital síncrona*.

– Recomendación CCITT G.774 (1992), *Modelo de información de gestión de la jerarquía digital síncrona desde el punto de vista de los elementos de red.*

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

– Recomendación UIT-T G.784 (1994), *Gestión de la jerarquía digital síncrona*.

– Recomendación UIT-T G.803 (1997), *Arquitecturas de redes de transporte basadas en la jerarquía digital síncrona*.

## 3 Términos y definiciones

En esta Recomendación se definen los términos siguientes.

**3.1 controlador de conmutación de protección automática (APS, *automatic protection switching*)**: 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-extracción (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 retiradas (extraídas) las señales constitutivas. Véase 3.5/G.782.

**3.3 tráfico añadido**: Tráfico normal o adicional insertado en los canales de servicio, de protección, o no protegidos y no desplazables con prioridad del anillo en un nodo de dicho anillo.

**3.4 unidad administrativa (AU, *administrative unit*)**: Véase la Recomendación G.707.

**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 petición de conmutación de protección automática**: Conjunto de señales entrantes en un controlador de APS que determina su comportamiento. Una petición de APS puede ser una instrucción iniciada externamente o bien una instrucción iniciada automáticamente.

**3.7 señal de indicación de alarma de unidad administrativa (AU-AIS, *administrative unit alarm indication signal*)**: Véase la Recomendación G.783.

**3.8 puntero de unidad administrativa**: Véase la Recomendación G.707.

**3.9 instrucción iniciada automáticamente**: Petición de APS iniciada por alguna de las siguientes motivaciones: 1) criterios de calidad de funcionamiento de recesión de multiplexación; 2) criterios de calidad de funcionamiento del equipo local, o 3) peticiones de puenteo recibidas.

**3.10 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.

**3.11 conexión bidireccional**: Véase la Recomendación G.803. Se ilustra en la figura 3-2.

**3.12 conmutación de protección bidireccional**: Arquitectura de conmutación de protección en la que, en caso de fallo unidireccional (es decir, un fallo que sólo afecta a un sentido de la transmisión), ambos sentidos (del "camino", de la "conexión de subred", etc.), el afectado y el no afectado, se conmutan a protección.

**3.13 anillo bidireccional**: En un anillo bidireccional el encaminamiento normal de las señales del tráfico normal es tal que los dos sentidos de una conexión bidireccional recorren el anillo a través de los mismos nodos, pero en sentidos opuestos.

**3.14 paridad N de entrelazado de bits (BIP-N, *bit interleaved parity N*)**: Véase la Recomendación G.707.

**3.15 puentear; puenteo**: Transmitir tráfico idéntico por los canales de servicio y de protección.

**3.16 petición de puenteo**: Mensaje enviado desde un nodo de extremo de cola hacia un nodo de extremo de cabecera en el que se solicita que el extremo de cabecera puentee el tráfico normal a los canales de protección.

**3.17 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.

**3.18 contenedor**: Véase la Recomendación G.707.

**3.19 fallo de controlador**: Condición durante la cual un nodo no puede tratar correctamente el protocolo de APS, pero sigue generando una trama SDH correctamente formatada.

**3.20 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 conmutación recibe una petición de puenteo de anillo desde el otro extremo.)

**3.21 canal de comunicación de datos (DCC, *data communications channel*)**: Véase la Recomendación G.784.

**3.22 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.

**3.23 código de conmutación de protección automática 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.

**3.24 encaminamiento diverso de ida y vuelta**: Se establece/encamina una entidad/señal de transporte bidireccional (es decir, de ida y vuelta) por diferentes facilidades físicas. Este encaminamiento puede aplicarse a caminos individuales, a conexiones de subred, o a señales. Se ilustra en la figura 3-2.

**3.25 encaminamiento diverso de par de protección [camino/conexión de subred (SNC, *subnetwork connection*)]**: Encaminamiento diverso de un camino/SNC, de servicio y su camino/SNC de protección asociado, en donde el camino/SNC de servicio (en ambos sentidos de la transmisión) toma una ruta (física), y el camino/SNC de protección (en ambos sentidos de la transmisión) toma otro.

**3.26 tráfico extraído; tráfico retirado**: Tráfico retirado normal o adicional de los canales de servicio de protección, o no protegidos y no desplazables con prioridad del anillo en un nodo de dicho anillo.

**3.27 instrucción iniciada externamente**: Petición de APS iniciada por un sistema operativo (OS, *operation system*) o por el operador.

**3.28 tráfico adicional**: Tráfico transportado por los canales de protección cuando esa capacidad no es utilizada para la protección del tráfico normal. El tráfico adicional no está protegido. Al necesitarse los canales de protección para proteger el tráfico normal, el tráfico adicional será desplazado.

**3.29 transferencia total**: Acción de transmitir los mismos K1, K2 y canales de protección que se reciben. La transferencia total es bidireccional. La transferencia total puede ser unidireccional o bidireccional, según se especifique en el texto. Cuando un nodo pase a transferencia total unidireccional, deberá continuar emitiendo los bytes K emitidos previamente en el sentido opuesto, con la salvedad de que los bits 6-8 del byte K2 deberán reflejar el código de situación apropiado.

**3.30 extremo de cabecera**: Nodo que ejecuta un puenteo. Se señala que un nodo funciona como un extremo de cabecera y un extremo de cola para una conmutación bidireccional del mismo tramo.

**3.31 contenedor virtual de orden superior**: Véase la Recomendación G.707.

**3.32 tiempo de abstención**: El tiempo comprendido entre la declaración de degradación de señal o fallo de señal y la iniciación del algoritmo de conmutación de protección.

**3.33 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.

**3.34 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.

**3.35 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.

**3.36 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.

**3.37 pérdida de trama (LOF, *loss of frame*)**: Véase la Recomendación G.783.

**3.38 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.

**3.39 contenedor virtual de orden inferior**: Véase la Recomendación G.707.

**3.40 acceso a contenedor virtual de orden inferior**: Terminación de un contenedor virtual de orden superior para añadir, retirar o interconectar un contenedor virtual o un grupo de contenedores virtuales de orden inferior.

**3.41 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.

**3.42 bit más significativo**: Posición de bit situado "más a la izquierda" o posición de bit que se transmite primero en un byte.

**3.43 sección de multiplexación (MS, *multiplex section*)**: Véase la Recomendación G.803.

**3.44 señal de indicación de alarma de sección de multiplexación (MS-AIS, *multiplex section alarm indication signal*)**: Véase la Recomendación G.783.

**3.45 indicación de defecto distante de sección de multiplexación (MS-RDI, *multiplex section remote defect indication*)**: Anteriormente conocida como fallo de extremo distante de sección de multiplexación. Véase la Recomendación G.707.

**3.46 protección de conexión de red**: Esquema que protege la conexión de subred más grande posible de un camino.

**3.47 interfaz de nodo de red (NNI, *network node interface*)**: Véase la Recomendación G.707.

**3.48 canal no protegido y no desplazable con prioridad**: Canal en un anillo de protección compartida de sección de multiplexación provisionado bidireccionalmente para proporcionar transporte sin conmutación de protección automática de anillo de protección compartida de sección de multiplexación. Los canales no protegidos y no desplazables con prioridad se provisionan desde pares de canales (correspondientes) de servicio y protección.

**3.49 tráfico no protegido y no desplazable con prioridad**: Tráfico no protegido transportado por un canal de protección excluida que no puede ser desplazado con prioridad (por ejemplo, por conmutadores de protección).

**3.50 tráfico normal**: Trafico transportado normalmente por los canales/secciones de servicio, salvo si se trata de un conmutador de protección, en cuyo caso se almacena en los canales/secciones de protección. El tráfico normal es protegido.

**3.51 señal nula**: La señal nula se indica en los canales de protección si no se utilizan para transportar tráfico normal o adicional. La señal nula puede ser una señal de cualquier clase que sea conforme a la estructura de señal de la capa específica y se ignora (no se selecciona) en el extremo de cola de la protección.

**3.52 transferencia**: Acción de transmitir la misma información que se recibe en cualquier sentido de transmisión.

**3.53 trayecto**: Véase la Recomendación G.803.

**3.54 tara de trayecto**: Véase la Recomendación G.707.

**3.55 canales de protección**: Canales asignados al transporte de tráfico normal durante un evento de conmutación. Los canales de protección se pueden utilizar para transportar tráfico adicional cuando no hay ningún evento de conmutación. Cuando hay un evento de conmutación, el tráfico normal en los canales de servicio afectados es puenteado a los canales de protección.

**3.56 sección de regeneración**: Véase la Recomendación G.803.

**3.57 indicación de error distante**: Anteriormente error de bloque en el extremo distante. Véase la Recomendación G.707.

**3.58 umbral de restablecimiento**: Para las instrucciones iniciadas automáticamente se utiliza un método de histéresis al conmutar tráfico normal de los canales de protección nuevamente a los canales de servicio. Este método especifica un umbral de la BER para la sección de multiplexación 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.

**3.59 restablecimiento**: Véase la Recomendación G.803.

**3.60 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.

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

**3.62 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 retire o inserte en el punto de fallo.

**3.63 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.

**3.64 tara de sección**: Véase la Recomendación G.707.

**3.65 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).

**3.66 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.

**3.67 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 cabecera 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.

**3.68 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.

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

**3.70 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 normal es transportado por los canales de protección del mismo tramo que el fallo.

**3.71 tráfico silenciado**: Señal de todos "1" que resulta del proceso de silenciamiento.

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

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

**3.74 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.

**3.75 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.

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

**3.77 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.

**3.78 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.

**3.79 síncrono**: 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.

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

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

**3.82 intercambio de intervalos de tiempo (TSI, *time slot 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 retirado del mismo).

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

**3.84 protección de camino**: El tráfico normal se transporta/selecciona de un camino de protección en vez de un camino de servicio si falla el primero o si su calidad de funcionamiento cae por debajo de un nivel requerido.

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

**3.86 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.

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

**3.88 conmutación de protección unidireccional**: Arquitectura de conmutación de protección en la que, en caso de fallo unidireccional (es decir, un fallo que sólo afecta un sentido de la transmisión), sólo el sentido afectado (del "camino", de la "conexión de subred", etc.) se conmuta a protección.

**3.89 anillo unidireccional**: En un anillo unidireccional (con conmutación de trayecto o con conmutación de sección de multiplexación), el encaminamiento normal del tráfico normal 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.

**3.90 encaminamiento uniforme de ida y vuelta**: La entidad/señal de transporte bidireccional (es decir, de ida y vuelta) es establecida/encaminada por las mismas facilidades físicas. Dicho encaminamiento puede aplicarse a caminos individuales, conexiones de subred, o señales. Esto se ilustra en la figura 3-2.

**3.91 contenedor virtual (VC, *virtual container*)**: Véase la Recomendación G.707.

**3.92 canales de servicio**: Canales por los que es transportado el tráfico normal cuando no hay eventos de conmutación.

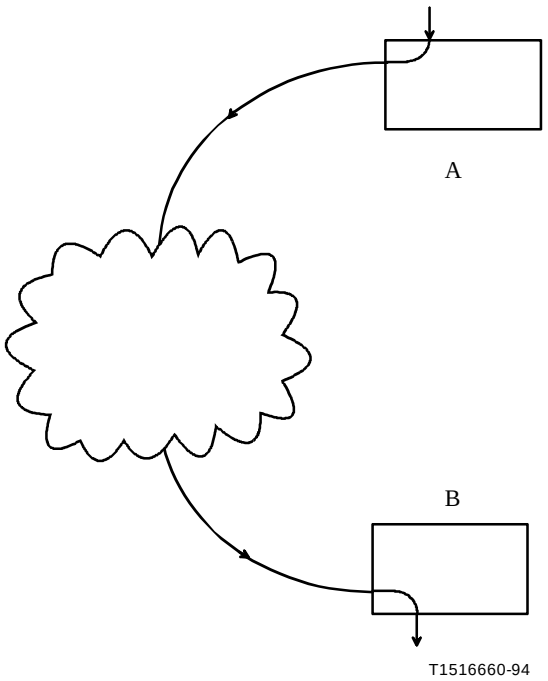
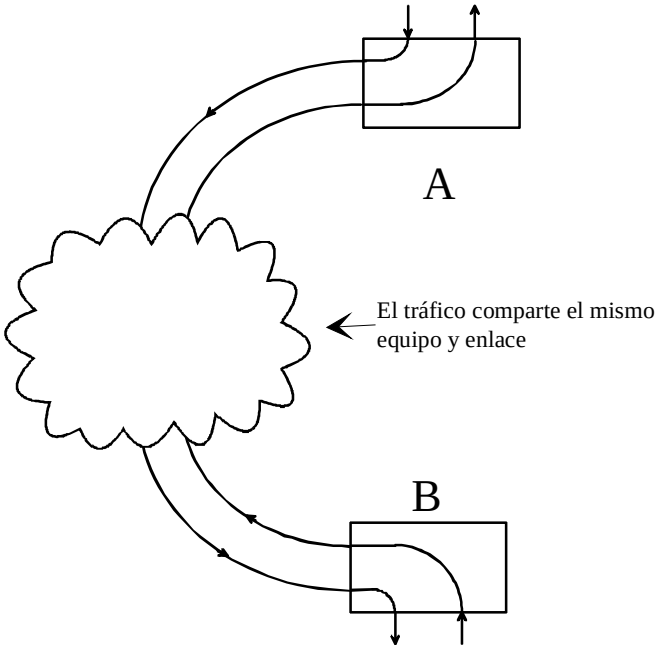
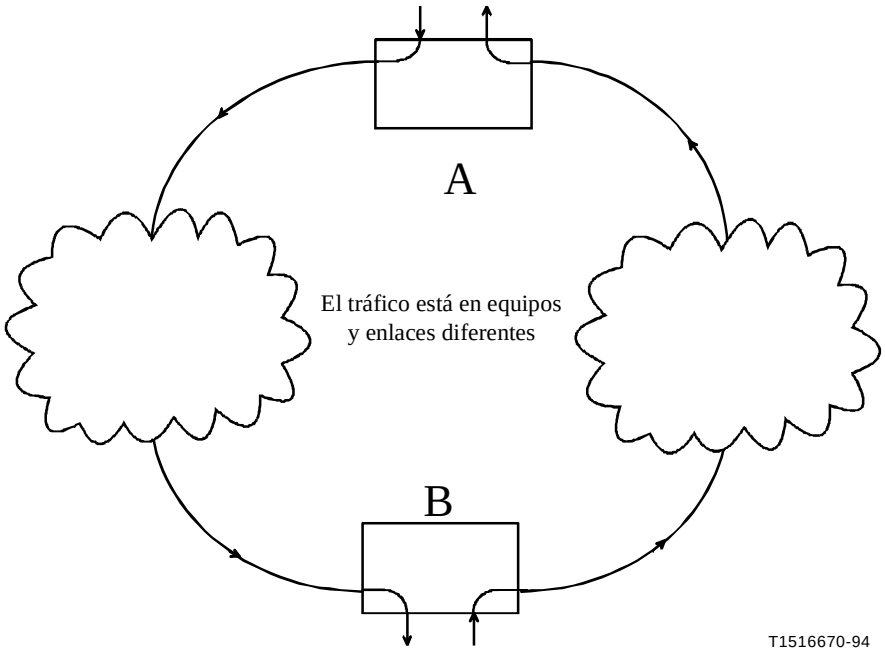



**Figura 3-1/G.841 – Conexión unidireccional**




**a) Encaminada uniformemente**




**b) Encaminada diversamente**

**Figura 3-2/G.841 – Conexión bidireccional encaminada uniformemente y encaminada diversamente**

## 4 Abreviaturas

En esta Recomendación se utilizan las siguientes siglas.

| | |
|---|---|
| ADM | Múltiplex de adición/retirada (extracción) (*add drop multiplex*) |
| AIS | Señal de indicación de alarma (*alarm indication signal*) |
| AP | Punto de acceso (*access point*) |
| APS | Conmutación de protección automática (*automatic protection switching*) |
| AU | Unidad administrativa (*administrative unit*) |
| AUG | Grupo de unidades administrativas (*administrative unit group*) |
| AU-AIS | Señal de indicación de alarma de unidad administrativa (*administrative unit alarm indication signal*) |
| AU-LOP | Pérdida de puntero de unidad administrativa (*administrative unit loss of pointer*) |
| BER | Tasa de errores en los bits (*bit error ratio*) |
| BIP-N | Paridad N de entrelazado de bits (*bit interleaved parity N*) |
| BLSR | Anillo conmutado de línea bidireccional (*bidirectional line switched rings*) |
| Br | Puenteo (puenteado) [*bridge (d)*] |
| CP | Punto de conexión (*connection point*) |
| DCC | Canal de comunicaciones de datos (*data communications channel*) |
| ET | Tráfico adicional (*extra traffic*) |
| EXER-R | Ejercicio-anillo (*exerciser-ring*) |
| EXER-S | Ejercicio-tramo (*exerciser-span*) |
| FS-P | Conmutación forzada a protección (*forced switch to protection*) |
| FS-R | Conmutación forzada de tráfico normal a protección-anillo (*forced switched working to protection-ring*) |
| FS-S | Conmutación forzada de tráfico normal a protección-tramo (*forced switched working to protection-span*) |
| FS-W | Conmutación forzada de tráfico normal a servicio (*forced switch to normal traffic to working*) |
| HO | Orden superior (*higher order*) |
| HO VC | Contenedor virtual de orden superior (*higher order virtual container*) |
| HP-DEG | Trayecto de orden superior degradado (*higher order path degraded*) |
| HP-EXC | Errores excesivos de trayecto de orden superior (*higher order path excessive errors*) |
| HP-SSF | Fallo de señal de servidor de trayecto de orden superior (*higher order path server signal fail*) |
| HP-TIM | Desadaptación de identificador de traza de trayecto de orden superior (*higher order path trace identifier mismatch*) |
| HP-UNEQ | Trayecto de orden superior no equipado (*higher order path unequipped*) |
| ID | Identificación |
| LO | Orden inferior (*lower order*) |
| LOF | Pérdida de trama (*loss of frame*) |
| LO VC | Contenedor virtual de orden inferior (*lower order virtual container*) |
| LP | Exclusión de protección (*lockout of protection*) |

LP-DEG Trayecto de orden inferior degradado (*lower order path degraded*)

LP-EXC Errores excesivos de trayecto de orden inferior (*lower order path excessive errors*)

LP-S Exclusión de protección – tramo (*lockout of protection – span*)

LP-SSF Fallo de señal de servidor de trayecto de orden inferior (*lower order path server signal fail*)

LP-TIM Desadaptación de identificador de traza de trayecto de orden inferior (*lower order path trace identifier mismatch*)

LP-UNEQ Trayecto de orden inferior no equipado (*lower order path unequipped*)

LOS Pérdida de señal (*loss of signal*)

MS Sección de multiplexación (*multiplex section*)

MSA Adaptación de sección de multiplexación (*multiplex section adaptation*)

MSP Protección de sección de multiplexación (*multiplex section protection*)

MSPA Adaptación de protección de sección de multiplexación (*multiplex section protection adaptation*)

MSPT Terminación de protección de sección de multiplexación (*multiplex section protection termination*)

MST Terminación de sección de multiplexación (*multiplex section termination*)

MS-P Conmutación manual a protección (*manual switch to protection*)

MS-R Conmutación manual de tráfico normal a protección – anillo (*manual switch normal traffic to protection – ring*)

MS-S Conmutación manual de tráfico normal a protección – tramo (*manual switch normal traffic to protection – span*)

MS-W Conmutación manual de tráfico normal a servicio (*manual switch normal traffic to protection to working*)

NE Elemento de red (*network element*)

NNI Interfaz de nodo de red (*network node interface*)

NR Ausencia de petición (*no request*)

NUT Tráfico no protegido y no desplazable con prioridad (*non-preemptable unprotected traffic)*

OAM&P Operación, administración, mantenimiento y suministro (*operations, administration, maintenance & provisioning*)

OS Sistema operativo (*operation system*)

POH Tara de trayecto (*path overhead*)

RCD Red de comunicaciones de datos

RGT Red de gestión de las telecomunicaciones

RR-R Invertir petición – anillo (*reverse request – ring*)

RR-S Invertir petición – tramo (*reverse request – span*)

RSOH Tara de sección de regeneración (*regenerator section overhead*)

SD Degradación de señal (*signal degrade*)

SDH Jerarquía digital síncrona (*synchronous digital hierarchy*)

SD-P Degradación de señal de los canales de protección (*signal degrade of the protection channels*)

SD-R Degradación de señal – anillo (*signal degrade – ring*)

SD-S Degradación de señal – tramo (*signal degrade – span*)

SF Fallo de señal (*signal fail*)

SF-R Fallo de señal – anillo (*signal fail – ring*)

SF-S Fallo de señal - tramo (*signal fail – span*)

SNC Conexión de subred (*subnetwork connection*)

SNC/I Protección de conexión de subred con supervisión intrínseca (*subnetwork connection protection with inherent monitoring*)

SNC/N Protección de conexión de subred con supervisión no intrusiva (*subnetwork connection protection with non-intrusive monitoring)*

SSF Fallo de señal de servidor (*server signal fail*)

STM-N Módulo de transporte síncrono de nivel N (*synchronous transport module level N*)

Sw Conmutación (conmutado) [*switch(ed)*]

TCP Punto de conexión de terminación (*termination connection point*)

TSI Intercambio de intervalos de tiempo (*time slot interchange*)

TU Unidad afluente (*tributary unit*)

VC Contenedor virtual (*virtual container*)

WTR En espera al restablecimiento (*wait to restore*)

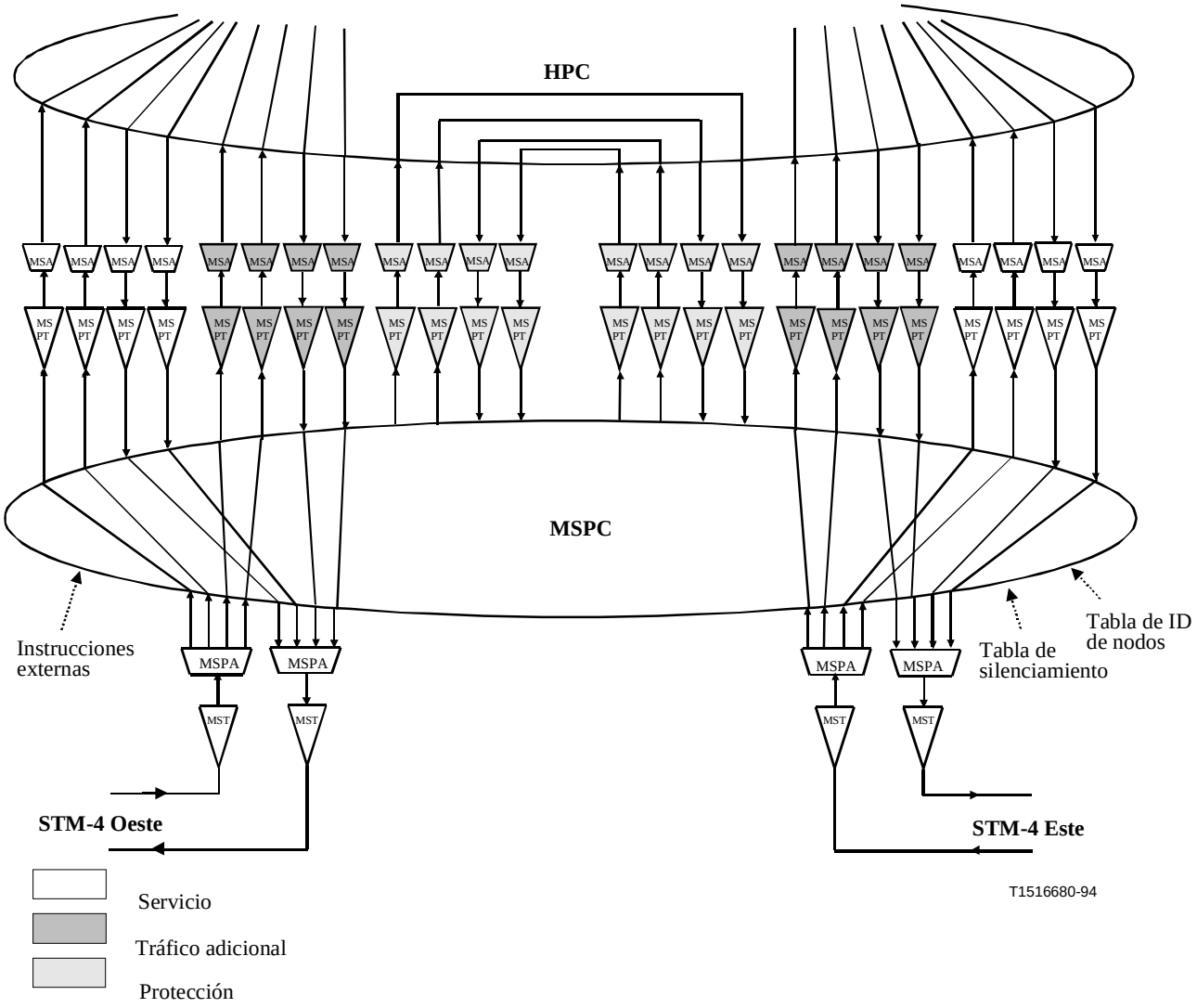
## 5 Clasificaciones de la protección

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

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.

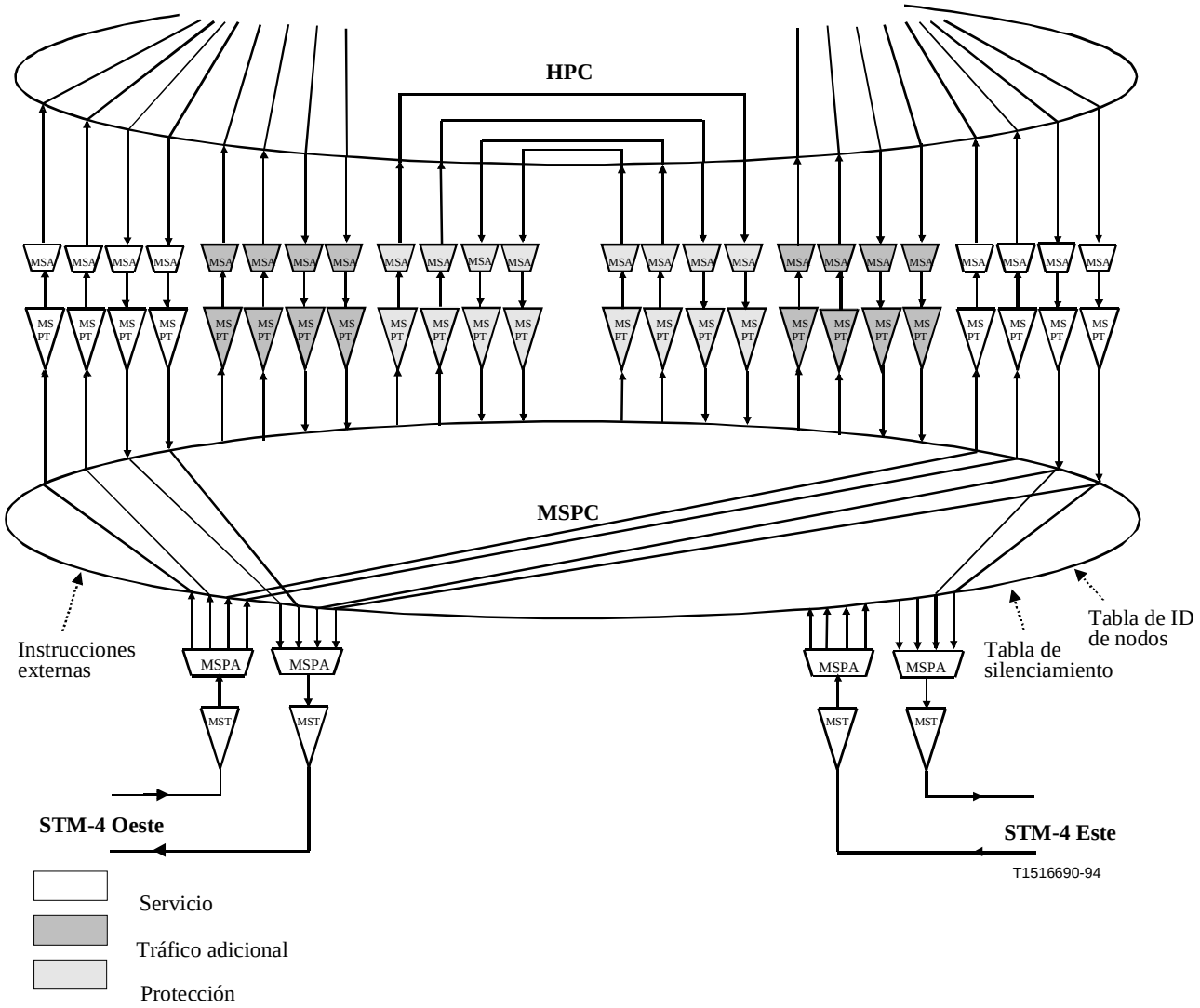
La figura 5-4 muestra el modelo funcional genérico para la protección de camino de VC 1 + 1. La figura 5-5 muestra el modelo funcional genérico para la protección de camino de VC reversivo 1:1 y la figura 5-6 muestra el modelo funcional genérico para la protección de camino de VC no reversivo 1:1.

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).



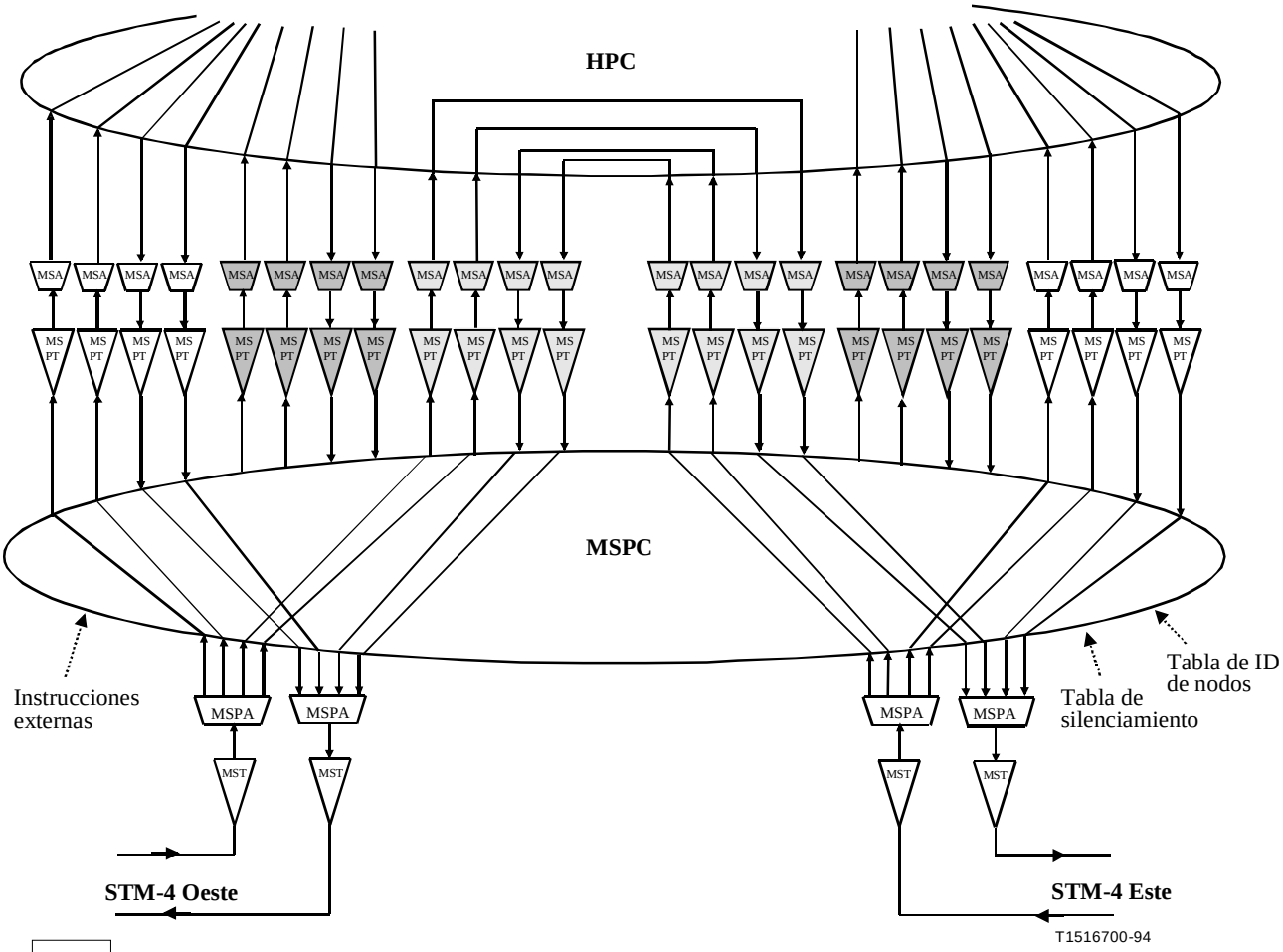

HPC Conexión de trayecto de orden superior
MSA Adaptación de sección de multiplexación
MSPA Adaptación de protección de sección de multiplexación
MSPC Conexión de protección de sección de multiplexación
MSPT Terminación de protección de sección de multiplexación
MST Terminación de sección de multiplexación

**Figura 5-1/G.841 – Modelo funcional para un anillo de protección compartida de MS de dos fibras – Estado normal con tráfico adicional**



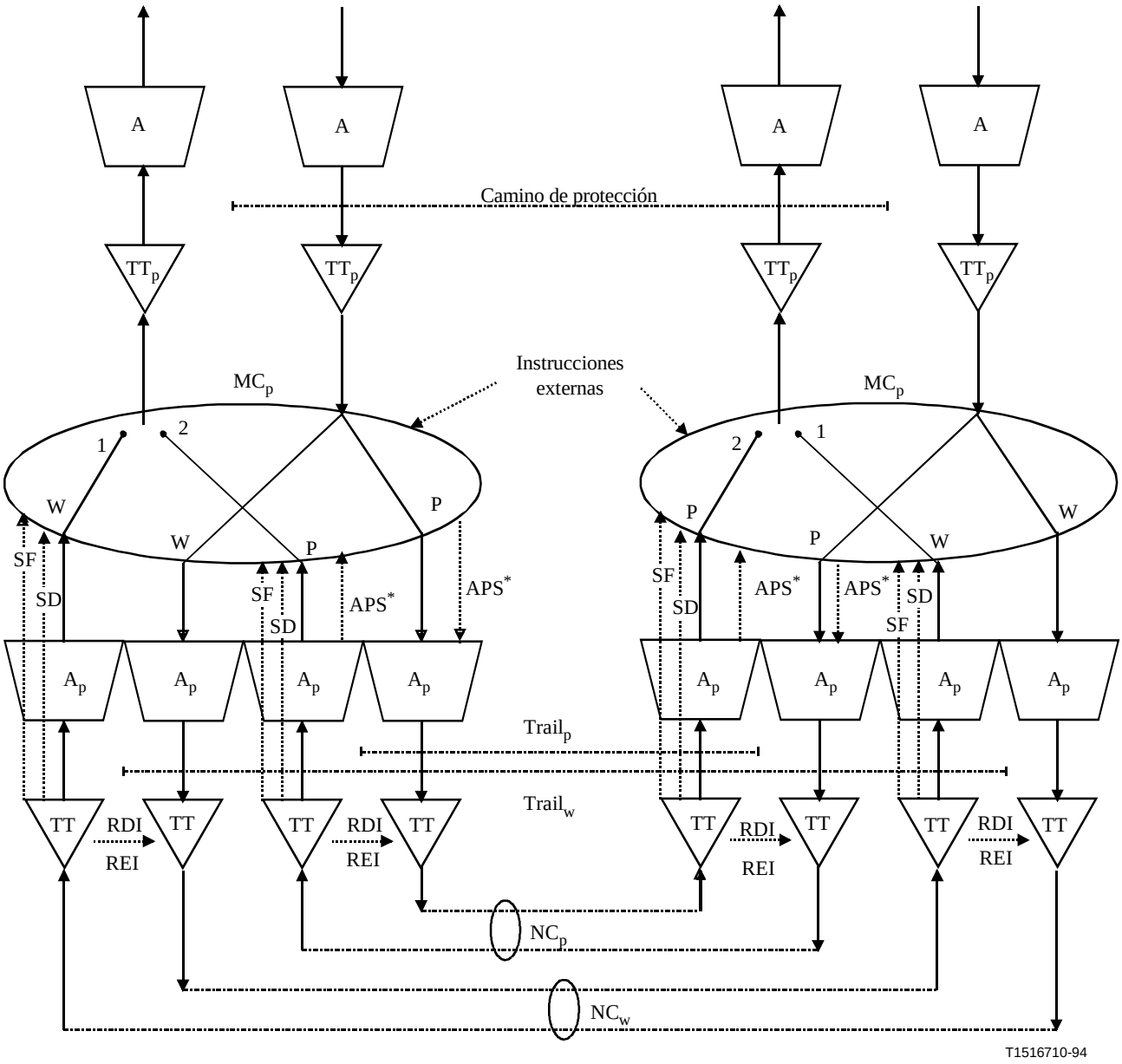

HPC Conexión de trayecto de orden superior
MSA Adaptación de sección de multiplexación
MSPA Adaptación de protección de sección de multiplexación
MSPC Conexión de protección de sección de multiplexación
MSPT Terminación de protección de sección de multiplexación
MST Terminación de sección de multiplexación

**Figura 5-2/G.841 – Modelo funcional para un anillo de protección compartida de MS de dos fibras – Fallo en el lado Este**




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**

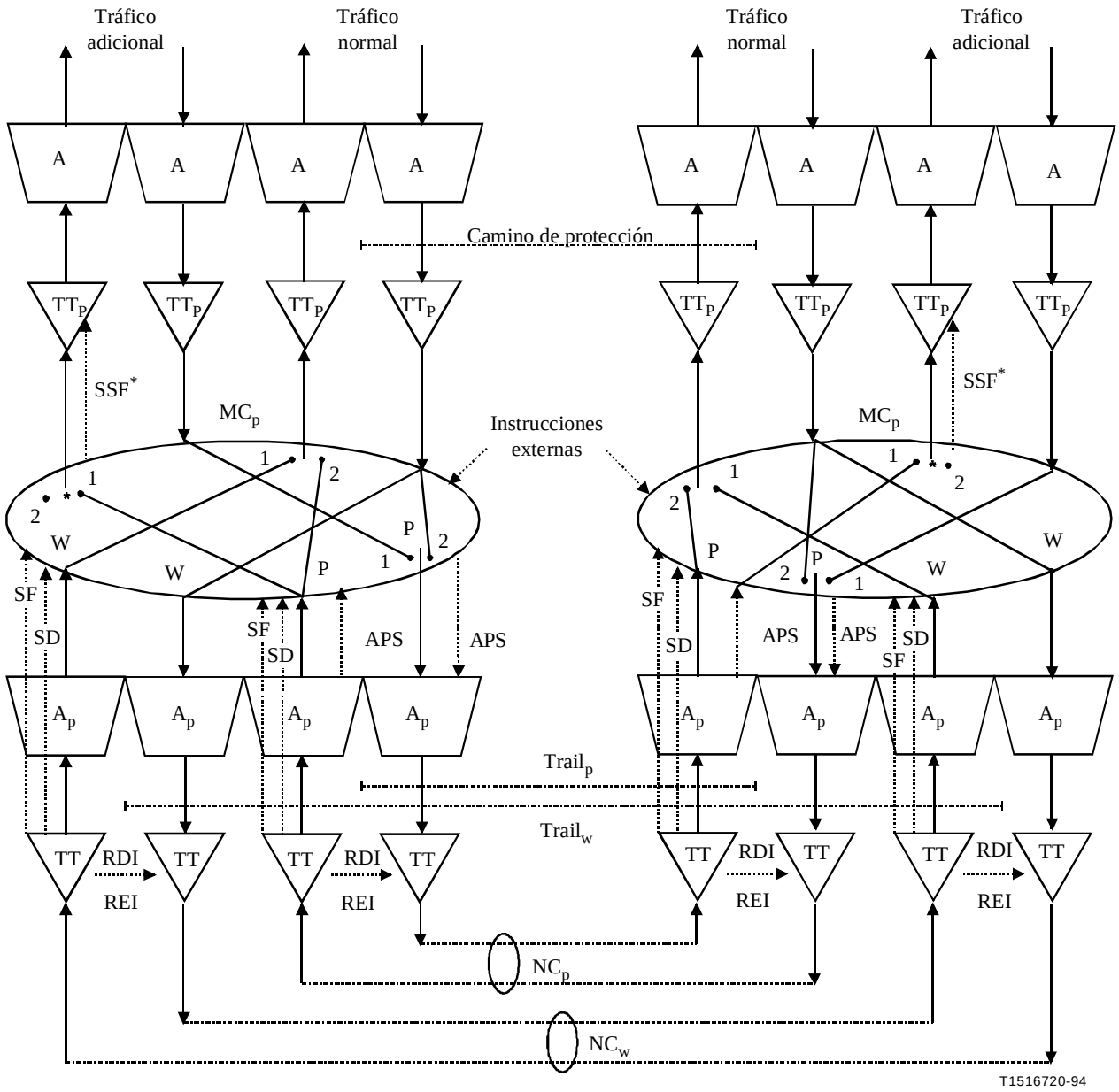



* Requerido para conmutación de extremo doble.
No requerido para conmutación de extremo único.

| | | | |
|---|---|---|---|
| A | Adaptación | SD | Degradación de señal |
| $A_p$ | Adaptación de protección | SF | Fallo de señal |
| $MC_p$ | Conexión de matriz de protección | SSF | Fallo de señal de servidor |
| $NC_p$ | Conexión de red de protección | $Trail_p$ | Camino de protección |
| $NC_w$ | Conexión de red de servicio | $Trail_w$ | Camino de servicio |
| RDI | Indicación de defecto a distancia | TT | Terminación de camino |
| REI | Indicación de error a distancia | $TT_p$ | 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**

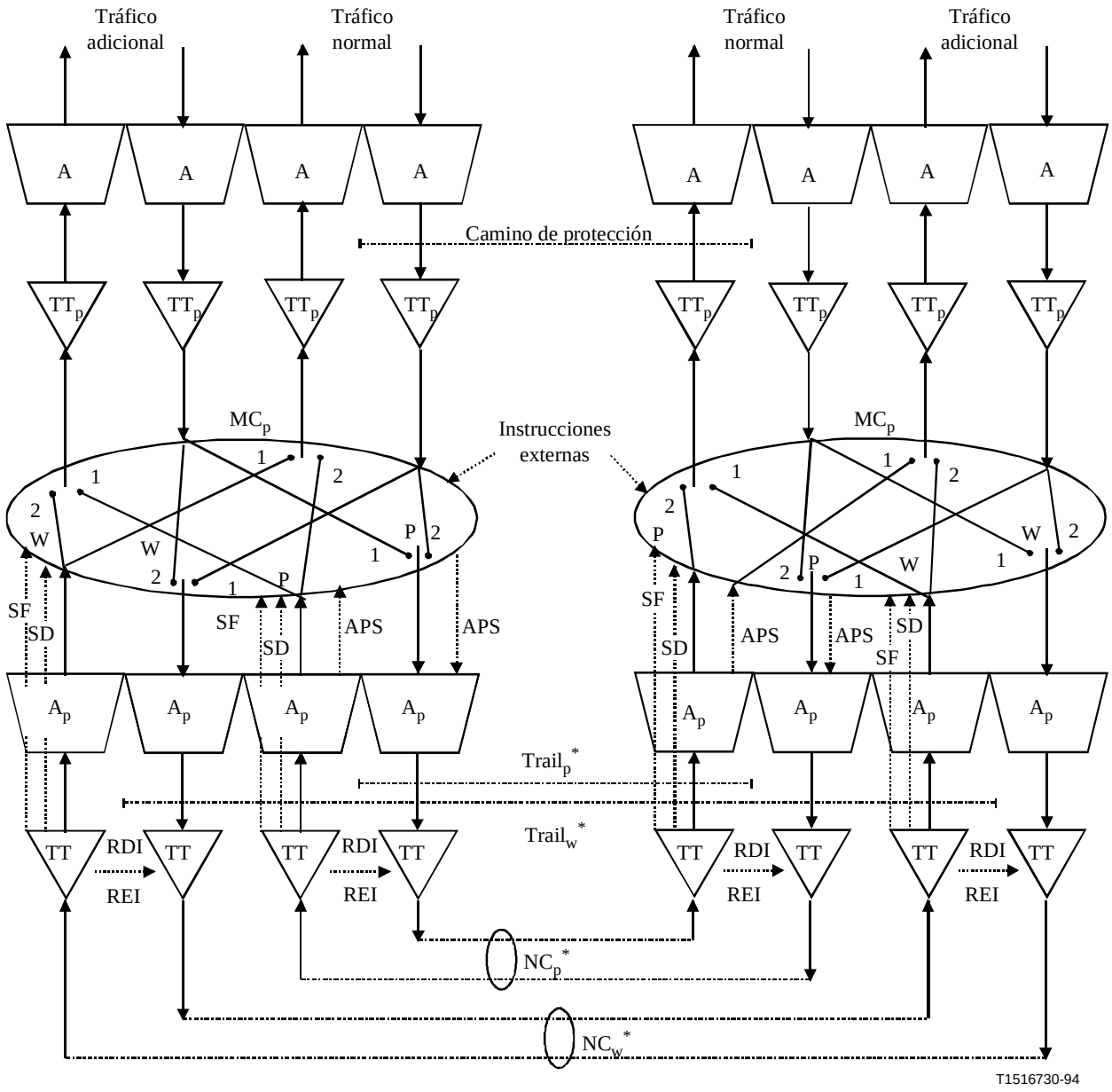



* SSF activo en conexión abierta [estado de fallo (2)]. Queda en estudio.

| | | | |
|---|---|---|---|
| A | Adaptación | SD | Degradación de señal |
| $A_p$ | Adaptación de protección | SF | Fallo de señal |
| $MC_p$ | Conexión de matriz de protección | SSF | Fallo de señal de servidor |
| $NC_p$ | Conexión de red de protección | $Trail_p$ | Camino de protección |
| $NC_w$ | Conexión de red de servicio | $Trail_w$ | Camino de servicio |
| RDI | Indicación de defecto a distancia | TT | Terminación de camino |
| REI | Indicación de error a distancia | $TT_p$ | 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**

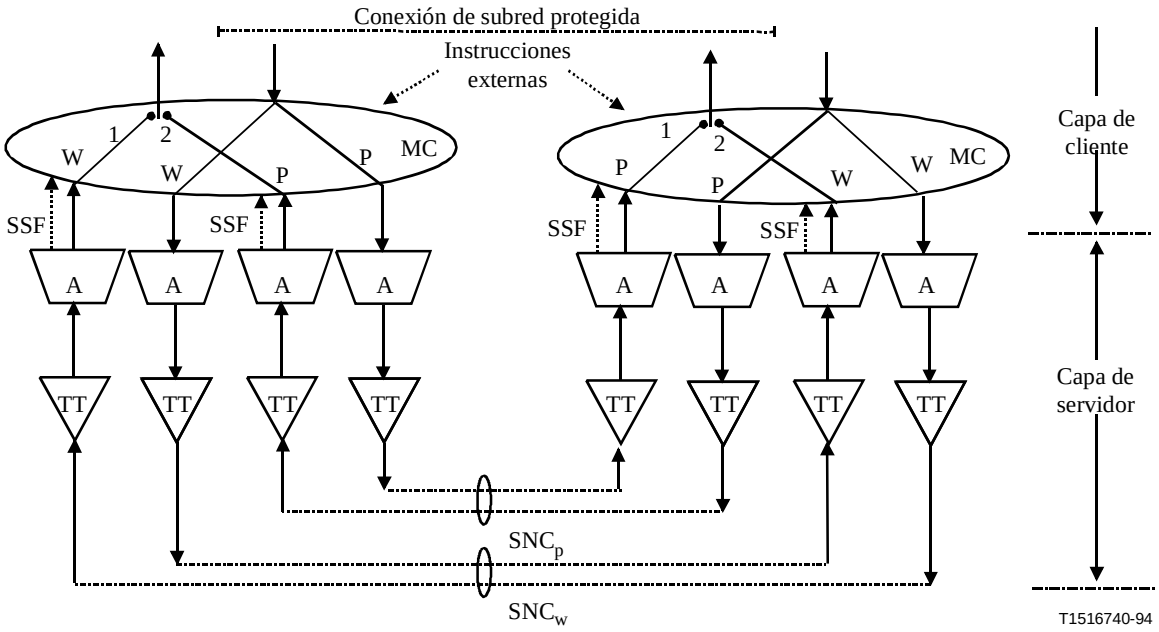



* En estado de fallo (2), $Trail_p$ pasa a ser $Trail_w$, $Trail_p$ pasa a ser $Trail_w$, $NC_p$ pasa a ser $NC_w$ y $NC_w$ pasa a ser $NC_p$.

| | |
|---|---|
| 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 |

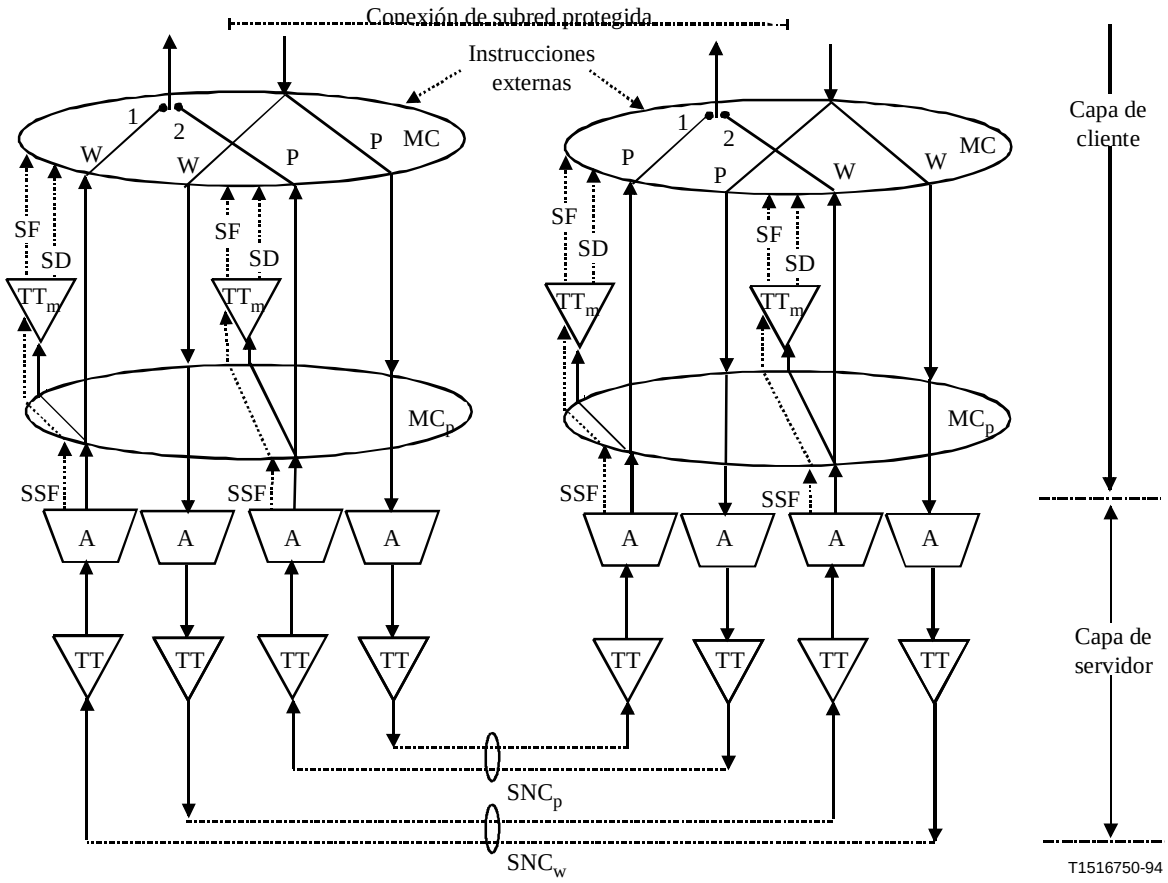
Estados: 1 Estado normal
2 Estado de fallo

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




A Adaptación
MC Conexión de matriz
$SNC_p$ Conexión de subred de protección
$SNC_w$ Conexión de subred de servicio
SSF Fallo 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 intrínsica (SNC/I) mediante un fallo de señal de servidor**




A Adaptación
MC Conexión de matriz
MC$_p$ Conexión de matriz de protección
SD Degradación de señal
SF Fallo de señal
SNC$_p$ Conexión de subred de protección
SNC$_w$ Conexión de subred de servicio
SSF Fallo de señal de servidor
TT Terminación de camino
TT$_m$ 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)**

## 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 señales de tráfico normal que han de protegerse, mientras que los canales de protección se reservan para la protección de este servicio. Los canales de protección se pueden utilizar para transportar tráfico adicional cuando no se utilizan para protección de tráfico normal. Las señales del tráfico normal son transportadas 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 retirado. 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 las señales de tráfico normal, pueden utilizarse para transportar señales de tráfico adicional. Al producirse una conmutación de protección, el tráfico normal 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 conmutación de anillo, el tráfico transmitido hacia el tramo que ha fallado es conmutado en un nodo de conmutación 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 conmutación en el que el tráfico normal de los canales de protección conmutado de nuevo a los canales de servicio. En el otro sentido, el tráfico normal es puenteado y conmutado de la misma manera. La figura 6-2 ilustra una conmutación de anillo en respuesta a un corte de cable.

Durante una conmutación de anillo, el tramo que ha fallado es "reemplazado" efectivamente mediante los canales de protección comprendidos entre los nodos de conmutación 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.

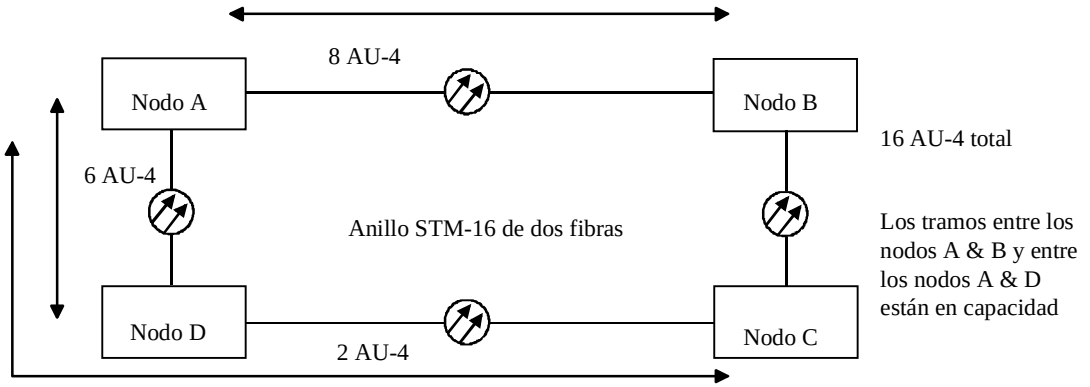
Los protocolos SPRING de sección de multiplexación (MS) permiten la división de la anchura de banda disponible en tres tipos de canales: canal de servicio para transportar tráfico normal, canal de protección que se puede utilizar para transportar tráfico adicional, y canal NUT para transportar tráfico no protegido y no desplazable con prioridad. El tráfico normal se protege contra eventos de fallo mediante el protocolo APS SPRING de sección de multiplexación (MS), mientras que el tráfico adicional es tráfico no protegido transportado por los canales de protección. Cualquier evento de fallo que hiciera necesario el empleo de los canales de protección a efectos de protección deberá desplazar con prioridad al tráfico adicional.

El tráfico no protegido y no desplazable con prioridad es un tráfico sin protección que se transporta por canales con el mecanismo de conmutación de protección APS SPRING de MS inhabilitado para determinados canales HO VC, (es decir, canales de servicio y sus correspondientes canales de protección). El tráfico transportado por estos canales es no protegido y no desplazable con prioridad. Así pues, el NUT transportado por canales no protegidos y no desplazables con prioridad permite un nivel mayor de supervivencia en comparación con el tráfico adicional, pero un nivel menor en comparación con el tráfico normal.

En las figuras 6-3 y 6-4 se dan ejemplos de utilización de los canales NUT:

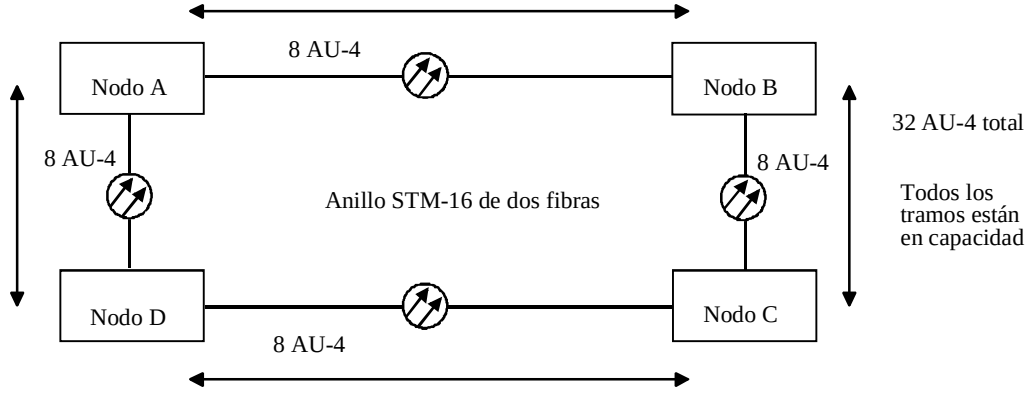
– La figura 6-3 muestra un anillo lógico en el que se utiliza SNCP como mecanismo de protección parcialmente incorporado en un MS SPRING que utiliza NUT. Esta disposición evita una innecesaria estratificación por capas de los mecanismos de protección y es mucho más eficaz desde el punto de vista del empleo de la anchura de banda que la misma aplicación sin NUT.

– La figura 6-4 muestra una aplicación similar, esta vez con los canales NUT soportando la conectividad HO VC entre conmutadores ATM. En el supuesto de que el tráfico ATM se protege por otros medios o no necesita ser protegido, esta aplicación de NUT tiene las mismas ventajas que las del ejemplo anterior.

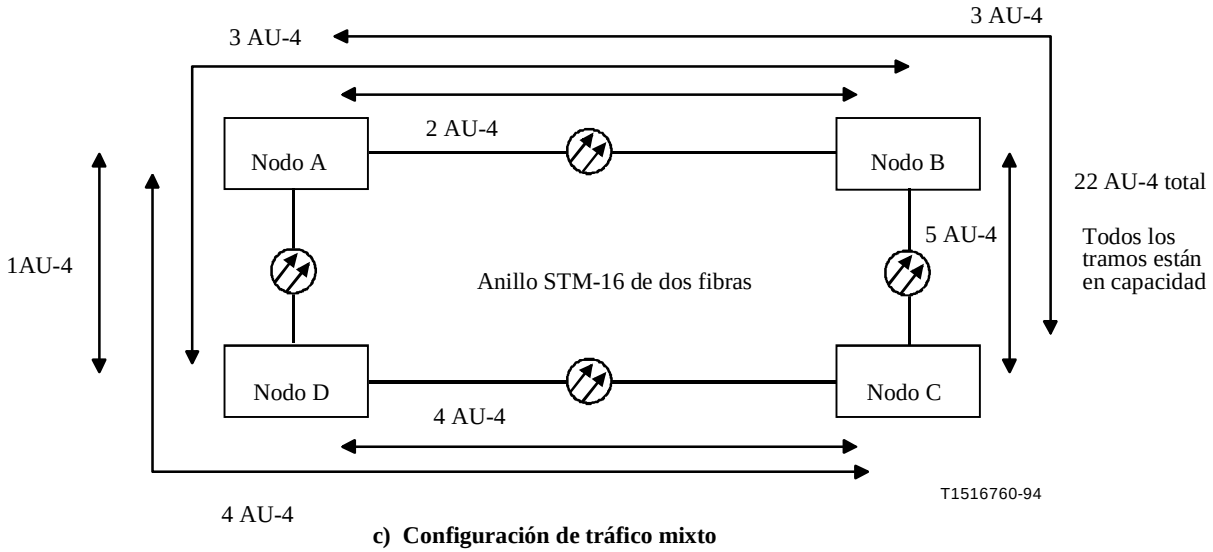



NOTA – Puesto que todo el tráfico está destinado al nodo A y el tramo entre el nodo A y el nodo B está lleno, el tráfico del nodo C se encamina a través del nodo B, dejando vacante el tramo entre el nodo B y el nodo C.

**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**

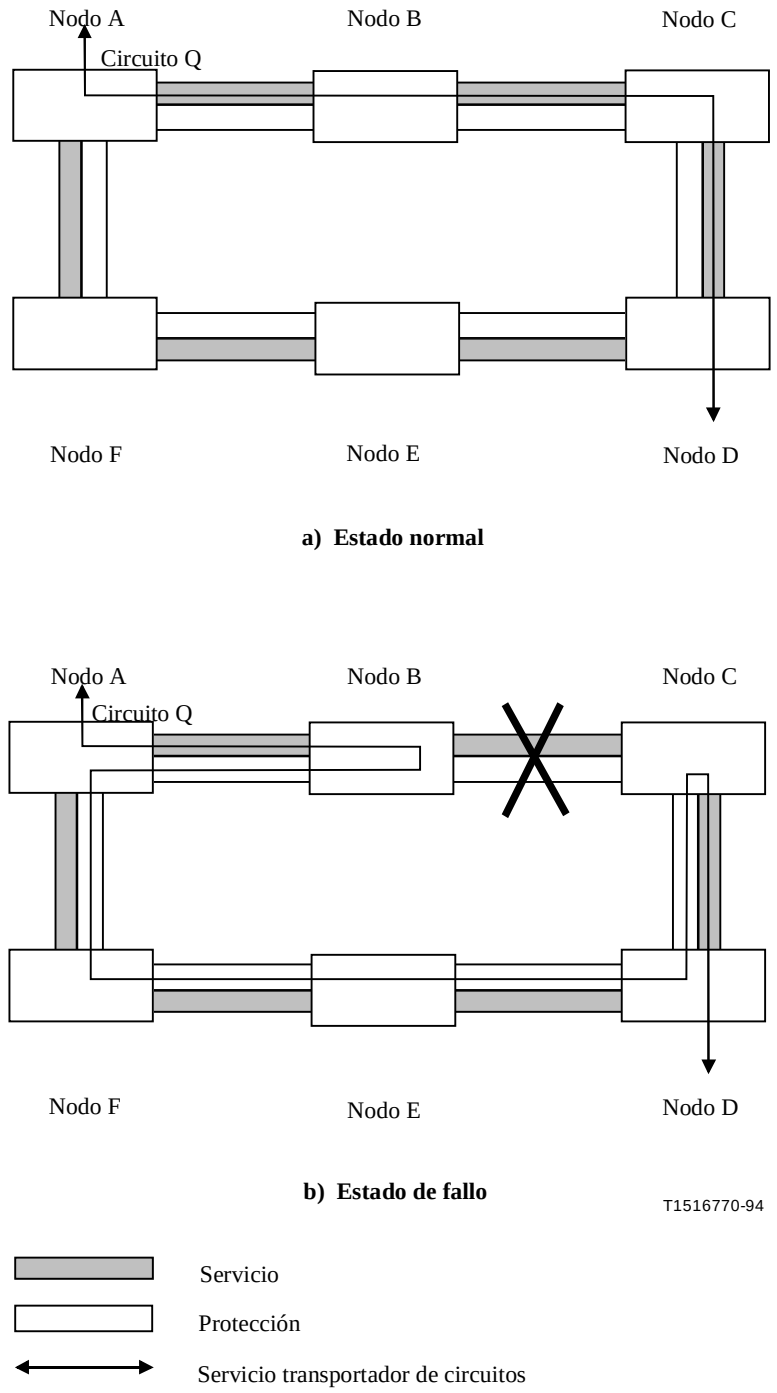



**Figura 6-2/G.841 – Ejemplo de encaminamiento de circuito en estado de fallo para una conmutación de anillo**

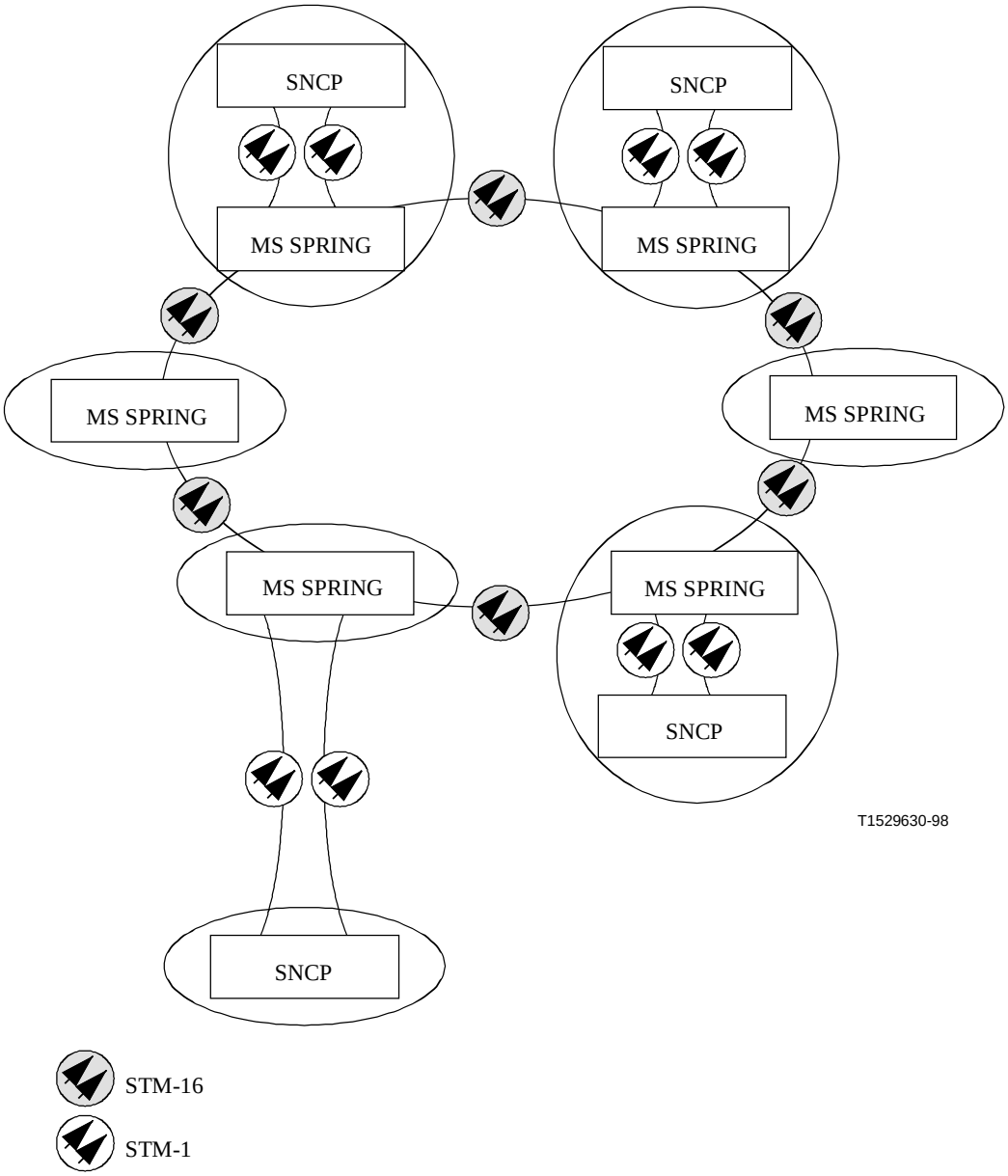



**Figura 6-3/G.841 – Anillo lógico en el que se utiliza SNCP como un mecanismo de protección incorporado parcialmente en un anillo de protección compartida de MS**

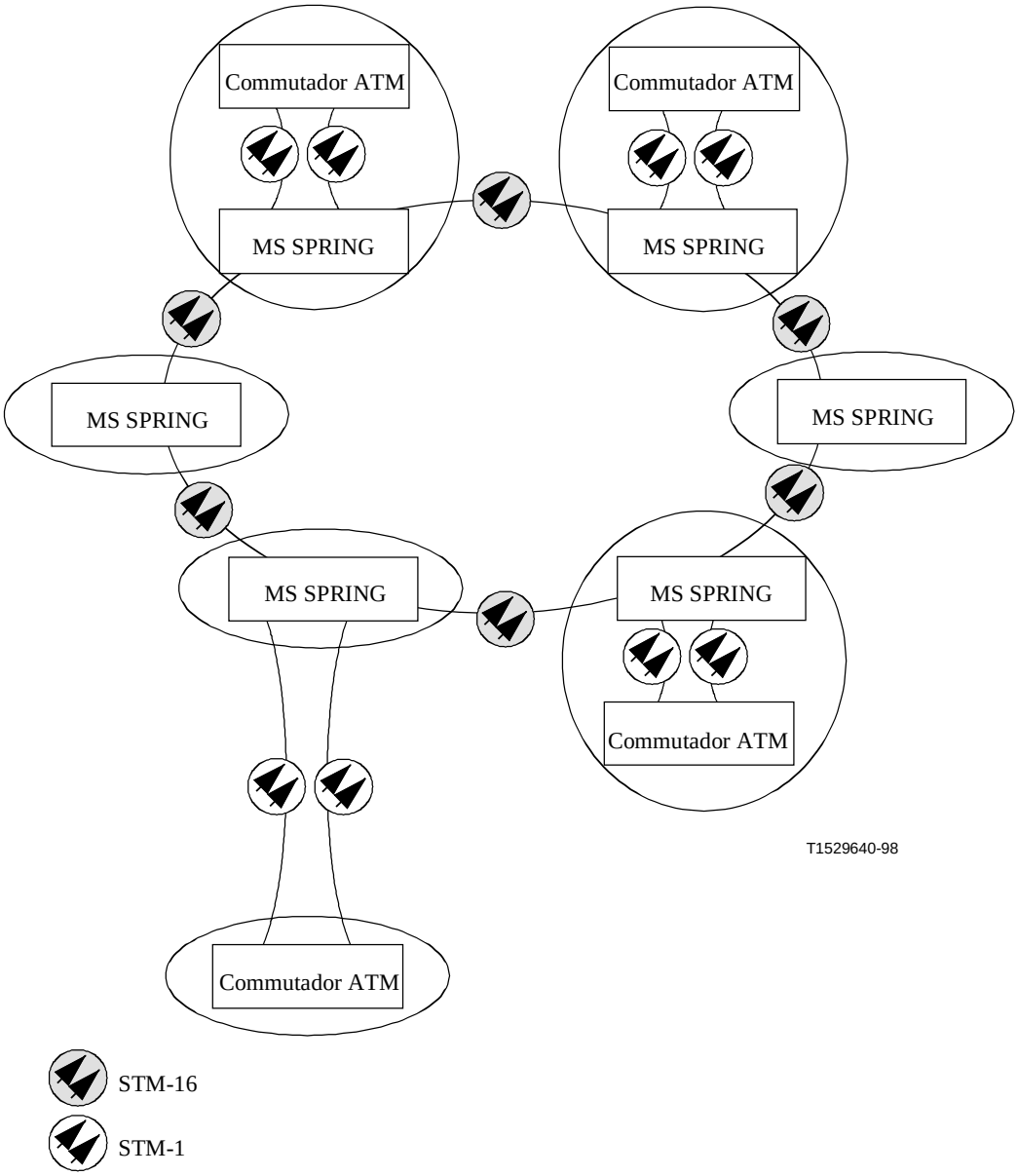



**Figura 6-4/G.841 – Canales NUT que soportan conectividad HO VC entre conmutadores ATM**

## 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 normal que ha de protegerse, mientras que el otro está reservado para la protección de este tráfico normal.

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 conmutación de protección.

### 6.4 Conmutación de protección unidireccional y bidireccional

Entre las posibles ventajas de la conmutación de protección unidireccional figuran las siguientes:

1) La conmutación de protección unidireccional es un esquema de implementación simple que no requiere protocolo.
2) La conmutación de protección unidireccional puede ser más rápida que la conmutación de protección bidireccional, 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 protección unidireccional que si se utiliza conmutación de protección bidireccional.

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

1) Con la conmutación de protección bidireccional 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 protección bidireccional, 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 protección bidireccional 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 protección bidireccional 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 protección bidireccional 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 conmutación de protección de camino de VC lineal puede funcionar en modo unidireccional o bidireccional. La conmutación de protección bidireccional 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) entre dos puntos de conexión (CP, *connection points*) o entre un CP y un punto de conexión de terminación (TCP, *termination connection point*), o la totalidad del trayecto de extremo a extremo entre dos TCP. Se conmuta al producirse fallos del servidor (utilizando supervisión intrínseca) o utilizando información de capa de cliente (utilizando supervisión no intrusiva).

La protección SNC es un esquema de protección lineal que se puede aplicar de manera individual a las señales del VC-n. No necesita utilizarse en todos los circuitos virtuales de una sección de multiplexación. No es necesario utilizarlo en todos los LO VC de un HO VC.

Los HO VC [LO VC] individuales transportados dentro de la red pueden ser no protegidos todos ellos, protegidos todos los HO VC [LO VC] 1 + 1 con SNC/I, protegidos todos los HO VC [LO VC] 1 + 1 con SNC/N, protegido todo el camino de HO VC [LO VC] (véase 6.5), o puede haber una combinación de no protegidos, HO VC [LO VC] 1 + 1 protegidos con SNC/I, HO VC [LO VC] 1 + 1 protegidos con SNC/I, HO VC [LO VC] 1 + 1 protegidos con SNC/N y protegido el camino de HO VC [LO VC].

Los HO VC [LO VC] que no están protegidos en su propia capa de trayecto HO [LO] se pueden proteger indirectamente en su capa de servidor; por ejemplo, una señal HO VC de un anillo protegido con SPRING de MS se protege frente a averías en el anillo con la protección de SPRING de MS.

Por otro lado, las señales de cliente transportadas dentro de un HO VC no protegido (por ejemplo, los LO VC, los trayectos virtuales (VP, *virtual path*) del ATM) se pueden proteger mediante sus esquemas de protección de capa de cliente (por ejemplo, LO VC con protección SNC, VP del ATM con protección SNC).

La decisión respecto a la protección de una señal y el tipo de protección utilizado finalmente quedan fuera del alcance de la presente Recomendación: vienen determinados por la arquitectura de red y las necesidades de calidad de servicio.

La protección SNC funciona en modo protección unidireccional. Queda en estudio la conmutación de protección bidireccional y el transporte de tráfico adicional.

### 6.7 Conmutación de protección de sección de multiplexación lineal

La conmutación de 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 el tráfico normal de un número (N) de secciones de multiplexación de servicio. No puede proteger contra los fallos de nodo. Puede funcionar como conmutación unidireccional o bidireccional, y puede transportar tráfico adicional por la sección de multiplexación de protección en funcionamiento bidireccional.

## 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

Esta subcláusula describe el protocolo de protección de sección de multiplexación (MSP) compatible con funcionamiento 1:n. En el anexo B se describe el protocolo de MSP optimizado para funcionamiento no reversivo 1 + 1.

### 7.1.1 Protocolo de protección de sección de multiplexación (MSP)

Las funciones MSP, en los extremos de una sección de multiplexación, solicitan y acusan recibo de las acciones de conmutación utilizando los bytes de APS [bytes K1 y K2 en la tara de sección de multiplexación (MSOH, *multiplex section overhead*)] de la sección de protección. Las asignaciones de bits para estos bytes y el protocolo de bits se definen a continuación.

#### 7.1.1.1 Byte K1

El byte K1 indica una petición de una señal de tráfico para acción de conmutación.

Los bits 1-4 indican el tipo de petición, según se enumera en el cuadro 7-1. Una petición puede ser:

1) una condición (SF y SD) asociada con una sección. Una condición tiene una prioridad alta o baja. Se fija la prioridad para cada sección correspondiente;

2) un estado (en espera al restablecimiento, no invertir, ausencia de petición, invertir petición) de la función MSP; o

3) una petición externa (exclusión de protección, conmutación forzada o manual y ejercicio).

Los bits 5-8 indican el número de la señal de tráfico o la sección para la cual se hace la petición, según se muestra en el cuadro 7-2.

**Cuadro 7-1/G.841 – Tipos de petición**

| Bits | Condición, estado o petición externa | Orden (Nota 1) |
|---|---|---|
| 1234 | | |
| 1111 | Exclusión de protección (nota 2) | Más alto |
| 1110 | Conmutación forzada | ↑ |
| 1101 | Prioridad de fallo de señal alta | . |
| 1100 | Prioridad de fallo de señal baja | . |
| 1011 | Prioridad de degradación de señal alta | . |
| 1010 | Prioridad de degradación de señal baja | . |
| 1001 | No utilizado (nota 3) | . |
| 1000 | Conmutación manual | . |
| 0111 | No utilizado (nota 3) | . |
| 0110 | En espera al restablecimiento | . |
| 0101 | No utilizado (nota 3) | . |
| 0100 | Ejercicio | . |
| 0011 | No utilizado (nota 3) | . |
| 0010 | Invertir petición | . |
| 0001 | No invertir | ↓ |
| 0000 | Ausencia de petición | Más bajo |

NOTA 1 – Una condición SF en la sección de protección tiene prioridad más alta que cualesquiera otras peticiones que seleccionarían una señal de tráfico normal de la sección de protección.

NOTA 2 – Sólo se permite la señal nulo (0) con una petición de exclusión de protección.

NOTA 3 – Algunas entidades operadoras de red pueden utilizar estos códigos para fines específicos de la red. El receptor debe ser capaz de omitir estos códigos.

NOTA 4 – Las peticiones se seleccionan de acuerdo con el cuadro, según las disposiciones de conmutación de protección; es decir, en cualquier caso particular, sólo se puede requerir un subconjunto de las peticiones.

**Cuadro 7-2/G.841 – Número de señal de tráfico K1**

| Número de señal | Petición de acción de conmutación |
|---|---|
| 0 | Señal nulo (ninguna señal de tráfico normal o adicional). Las condiciones y la prioridad asociada (prioridad alta) se aplican a la sección de protección. |
| 1-14 | Señal de tráfico normal (1-14).<br>Las condiciones y la prioridad asociada (alta o baja) se aplican a las secciones de servicio correspondientes.<br>Para 1 + 1 sólo es aplicable la señal de tráfico 1, con prioridad alta fija. Los sistemas 1 + 1 pueden tratar una petición de prioridad baja (incorrecta) recibida en los bits K como equivalente a la petición de prioridad alta correspondiente. |
| 15 | Señal de tráfico adicional.<br>Las condiciones no son aplicables.<br>Existe solamente cuando se suministra en una arquitectura 1:n. |

#### 7.1.1.2 Reglas de generación del byte K1

Las condiciones locales de SF y SD, los estados de espera al restablecimiento o no invertir y la petición externa son evaluadas por una lógica de prioridad, basada en el orden descendente de prioridades de las peticiones del cuadro 7-1. Si se detectan condiciones locales (SF o SD) del mismo nivel en diferentes secciones al mismo tiempo, tiene prioridad la condición con el número de sección más bajo. De estas peticiones evaluadas, la de más alta prioridad sólo sustituye a la petición local vigente si es de prioridad más alta.

Las condiciones SF y SD detectadas localmente y las peticiones iniciadas externamente de señales de tráfico normal que tienen aplicada la instrucción de control "exclusión de señal de tráfico normal de la protección" (véase 7.1.1.2.2) no son evaluadas durante la generación del byte K1.

##### 7.1.1.2.1 Funcionamiento en bidireccional

Las prioridades de la petición local y la petición distante en el byte K1 recibido se comparan de acuerdo con el orden descendente de prioridades del cuadro 7-1. Se señala que en la comparación no se considera una instrucción invertir petición o una petición distante para una señal de tráfico que tiene aplicada la instrucción "exclusión de señal de tráfico normal de la protección".

El byte K1 enviado indicará:

a) una instrucción invertir petición si la petición de puenteo distante es para una señal de tráfico que no está excluida y
   - i) la petición distante es de prioridad más alta, o si
   - ii) las peticiones son del mismo nivel (y son de prioridad más alta que la de ausencia de petición) y el byte K1 enviado no indica invertir petición, o si
   - iii) las peticiones son del mismo nivel (y son de prioridad más alta que ausencia de petición) y el byte K1 no indica invertir petición y la petición distante indica un número de señal de tráfico más bajo;

b) la petición local en todos los demás casos.

##### 7.1.1.2.2 Funcionamiento unidireccional

El byte K1 enviado indicará siempre la petición local. Por consiguiente, nunca se indica invertir petición.

### 7.1.1.3 Modos reversivo/no reversivo

En el modo de funcionamiento reversivo, cuando ya no se solicita la protección, es decir, la sección de servicio que ha fallado ya no está en condición SD o SF (y suponiendo que no hay otras secciones solicitantes), se activará un estado local de en espera al restablecimiento local. Puesto que este estado adquiere la prioridad más alta, se indica en el byte K1 enviado y se mantiene la señal de tráfico normal de la sección de servicio que falló previamente en la sección de protección. Este estado tiene normalmente una temporización y pasará a ser una señal nula (0) de ausencia de petición [o una señal de tráfico adicional (15) de ausencia de petición, si es aplicable]. El temporizador de en espera al restablecimiento se desactiva más pronto si el byte K1 enviado ya no indica en espera al restablecimiento, es decir, cuando cualquier petición de prioridad más alta desplace a este estado.

En el modo de funcionamiento no reversivo, aplicable solamente a la arquitectura 1 + 1, cuando la sección de servicio que ha fallado ya no está en la condición SD o SF, la selección de la señal de tráfico normal de protección se mantiene activando un estado de no invertir, en vez de un estado de ausencia de petición.

Normalmente se acusa recibo de las peticiones de en espera al restablecimiento y de no inversión en el byte K1 enviado mediante una instrucción de invertir petición en el byte K1 recibido. No obstante, el acuse de recibo de ausencia de petición se efectúa mediante otra ausencia de petición recibida.

### 7.1.1.4 Byte K2

Los bits 1-5 indican la situación del puenteo en el conmutador MSP (véase la figura 7-1). Los bits 6 a 8 se utilizan para indicación de MS-AIS y MS-RDI (véase la Recomendación G.707).

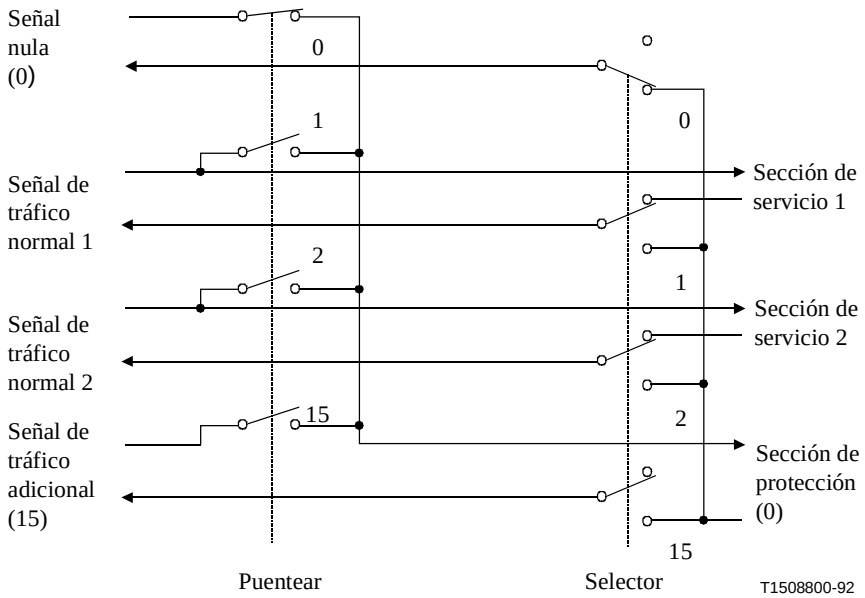



**Figura 7-1/G.841 – Conmutador MSP - Arquitectura 1:n (se muestra en posición de liberación)**

NOTA – En algunas aplicaciones regionales, cuando no se genera MS-RDSI, los bits 6 a 8 generados se utilizan para indicar el modo de conmutación (es decir, unidireccional utilizando el código 100, y bidireccional utilizando el código 101). Tales aplicaciones quedan fuera del alcance de la presente Recomendación.

Los bits 1-4 indican un número de señal, como se muestra en el cuadro 7-3. El bit 5 indica el tipo de la arquitectura MSP: puesto a 1 indica arquitectura 1:n y puesto a 0 indica arquitectura 1 + 1.

**Cuadro 7-3/G.841 – Número de señal de tráfico K2**

| Número de señal de tráfico | Indicación |
|---|---|
| 0 | Señal de tráfico nulo |
| 1-14 | Señal de tráfico normal (1-14)<br>Para 1 + 1, sólo es aplicable la señal de tráfico normal 1 |
| 15 | Señal de tráfico adicional.<br>Sólo existe cuando se suministra en una arquitectura 1:n |

#### 7.1.1.5 Reglas de generación del byte K2

El byte K2 enviado indicará en los bits 1 a 4, para todas las arquitecturas y modos de funcionamiento, señal nula (0) si el byte K1 recibido indica señal nula y el tráfico adicional no está puenteado. En todos los demás casos, el byte K2 deberá indicar el número de la señal que está puenteada.

El byte K2 enviado se indicará en el bit 5:

a) 0 si es la arquitectura 1 + 1;

b) 1 si es la arquitectura 1:n.

#### 7.1.1.6 Control del puenteo

##### 7.1.1.6.1 Arquitectura unidireccional/bidireccional 1 + 1

En la arquitectura 1 + 1, el canal de servicio 1 está conectado en puente permanentemente con la sección de servicio y protección, por lo que no se necesita control de puenteo.

##### 7.1.1.6.2 Arquitectura unidireccional 1:n

En la arquitectura unidireccional 1:n, el número de señal indicado en el byte K1 recibido se puentea con la sección de protección. Si se soporta tráfico adicional y el byte K1 recibido indica 0 ó 15 e indica ausencia de petición de exclusión de protección, la señal de tráfico adicional se puentea con la sección de protección.

Si, en el extremo del puente, la sección de protección está en condición SF, se congela el puente (puente vigente mantenido).

##### 7.1.1.6.3 Arquitectura bidireccional 1:n

En la arquitectura bidireccional 1:n, el control del puenteo se efectúa comparando los números de señal de los bytes K1 recibido y enviado:

a) Si el número de señal en el byte K1 recibido y enviado indica la misma señal de tráfico de servicio, la señal de tráfico de servicio correspondiente se puentea con la sección de protección.

b) Si se soporta tráfico adicional y el número de la señal en el byte K1 recibido indica 0 ó 15, el byte K1 enviado indica también 0 ó 15 (se permiten todas las combinaciones de 4), y ni el byte K1 recibido ni el byte K1 transmitido indican una petición de exclusión de protección, la señal de tráfico adicional se puentea con la sección de protección.

c) Si no se cumplen ni a) ni b) o la sección de protección está en condición SF, se deshace el puenteo (puenteada señal nula).

#### 7.1.1.7 Control del selector

##### 7.1.1.7.1 Arquitectura unidireccional 1 + 1

En la arquitectura 1 + 1, en funcionamiento unidireccional, el selector es controlado por la petición local de prioridad más alta. Si la sección de protección está en condición SF, se libera el selector.

##### 7.1.1.7.2 Arquitectura bidireccional 1 + 1

En la arquitectura 1 + 1, en funcionamiento bidireccional, el selector es controlado comparando los números de señal indicados en los bytes K2 recibido y K1 enviado. Si hay concordancia, se selecciona la señal indicada de la sección de protección. Si no hay concordancia, se libera el selector. Se señala que una concordancia en 0000 también libera el selector. Si la falta de concordancia persiste durante 50 ms, se indica en el punto de referencia MSP_MP. Si la sección de protección está en condición SF, se libera el selector y se inhabilita la indicación de falta de concordancia.

##### 7.1.1.7.3 Arquitectura unidireccional/bidireccional 1:n

En la arquitectura 1:n, el selector es controlado comparando los números de señal del byte K2 recibido y del byte K2 enviado:

a) Si el número de señal del byte K2 recibido y el byte K1 enviado indican la misma señal de tráfico de servicio, se selecciona la señal de tráfico de servicio correspondiente de la sección de protección.

b) Si el número de señal del byte K2 recibido indica 15 y el byte K1 enviado indica 0 ó 15, se selecciona la señal de tráfico adicional de la sección de protección.

c) Si no se cumplen ni a) ni b), se libera el selector (no se selecciona señal). Si esta condición está presente durante 50 ms, se notifica falta de concordancia K1/K2 en el punto de referencia MSP_MP.

d) Si la sección de protección está en condición SF, se libera el selector (no se selecciona señal) y se elimina una indicación activa de falta de concordancia K1/K2.

NOTA – En la definición del protocolo 1:n de la Recomendación G.783, se ha eliminado el tráfico adicional de la sección de protección en caso de SD para la sección de protección. En caso de interfuncionamiento entre un equipo en el que se haya diseñado el protocolo 1:n con tráfico adicional de acuerdo con la definición de la Recomendación G.783 y un equipo en el que el protocolo se haya diseñado de acuerdo con la definición nueva de la presente Recomendación, el equipo conforme a la definición de la Recomendación G.783 notificará un fallo de falta de concordancia K1/K2 en caso de SD para la sección de protección. La gestión hará caso omiso de tal fallo.

#### 7.1.1.8 Transmisión y aceptación de bytes de APS

El byte K1 y los bits 1 a 5 del byte K2 se transmitirán por la sección de protección. Aunque pueden ser transmitidos idénticamente por las secciones de servicio, los receptores no deben suponerlo así, y deben tener la capacidad de pasar por alto esta información en las secciones de servicio.

Los bytes APS serán aceptados como válidos solamente cuando se reciban bytes idénticos en tres tramas consecutivas.

Las condiciones que siguen se notifican como condiciones de defecto APS en el MSP_MP y dan como resultado la liberación del selector además de la condición definida en 7.1.1.7.

– Una falta de concordancia entre el bit 5 del byte K2 enviado y el byte K2 recibido durante 50 ms (opcional).

– En funcionamiento bidireccional, un código inapropiado que dura 50 ms en los bits 1-4 del byte K1 recibido. Los códigos apropiados son una petición de prioridad más alta que la

petición local, una petición idéntica a la petición local, o una petición de inversión de cualquier petición local, excepto la ausencia de petición. Cualquier otro valor que dure 50 ms se considera un código inapropiado.

– En funcionamiento bidireccional, un número de señal de tráfico inapropiado o no válido que dure 50 ms en los bits 5-8 del byte K1 recibido.

### 7.1.2 Instrucciones MSP

La función MSP recibe parámetros de control MSP y peticiones de conmutación de la función de gestión de equipo síncrono en el punto de referencia MSP_MP. Una instrucción de conmutación emite una petición externa apropiada en la función MSP. Sólo una petición de conmutación puede ser emitida en el MSP_MP. Una instrucción de control fija o modifica los parámetros MSP o pide la situación MSP.

Cualquier instrucción de conmutación externa de la cual el extremo lejano no haya acusado recibo dentro de 2,5 s, se debe notificar como fallo, y se debe retirar la instrucción y la petición del byte K. Si inicialmente se acusó recibo de una instrucción de conmutación que más tarde es invalidada, se retira en consecuencia la instrucción externa.

NOTA – Este comportamiento no se definió plenamente en las versiones anteriores de las Recomendaciones G.841 y G.783.

#### 7.1.2.1 Instrucciones de conmutación

Una instrucción de conmutación emitida en la interfaz del controlador MSP APS inicia una petición de puenteo externa para evaluación como se describe en 7.1.1.1.1. A continuación se indican las instrucciones de conmutación en orden de prioridad descendente y se describe la funcionalidad de cada una de ellas.

1) *Eliminación* – Esta instrucción elimina todas las instrucciones de conmutación iniciadas externamente enumeradas a continuación y WTR en el nodo al que se dirigió la instrucción.

   NOTA – En la definición de la Recomendación G.783 del MSP lineal la instrucción de eliminación no elimina WTR. El equipo diseñado de acuerdo con la definición de la Recomendación G.783 no eliminaría WTR cuando se envíe una instrucción de eliminación a ese equipo. No obstante, es posible conseguir un comportamiento similar mediante una secuencia de instrucciones externas seleccionadas cuidadosamente (por ejemplo, conmutación manual seguida de liberación).

2) *Exclusión de protección* – Niega a todas las señales de tráfico normal (y a la señal de tráfico adicional, si procede) el acceso a la sección de protección emitiendo una petición "exclusión de protección" a menos que esté en efecto una instrucción de conmutación de protección de prioridad igual.

3) *Conmutación forzada #* – Para las señales de tráfico normal #, conmuta la señal de tráfico normal # a la sección de protección, a menos que esté en efecto una instrucción de conmutación de prioridad igual o más alta o exista la condición SF en la sección de protección, emitiendo una petición de conmutación forzada para ese canal.

   Para sistemas 1 + 1 o sistemas 1:n sin tráfico adicional, la señal de tráfico nulo de conmutación forzada transfiere la señal de tráfico normal de la sección de protección a la sección de servicio, a menos que esté en efecto una petición de prioridad igual o más alta. Puesto que la conmutación forzada tiene una prioridad más alta que SF o SD en una sección de servicio, esta instrucción se aplicará con independencia de la condición de la sección o las secciones de servicio. La señal de tráfico nulo de conmutación forzada tiene una prioridad mayor que "la señal de tráfico normal de conmutación forzada #" cuando se detectan ambas instrucciones al mismo tiempo.

Para sistemas 1:n con tráfico adicional, la señal de tráfico adicional de conmutación forzada transferirá la señal de tráfico normal de la sección de protección a la sección de servicio y restablecerá la señal de tráfico adicional en la señal de protección, a menos que esté en efecto una petición de prioridad igual o más alta.

4) *Conmutación manual #* – Conmuta la señal de tráfico normal # a la sección de protección, a menos que exista una condición de fallo en otras secciones (incluida la sección de protección) o esté en efecto una instrucción de conmutación de prioridad más alta, emitiendo una petición de conmutación manual para esa señal de tráfico normal.

   Para sistemas 1 + 1 o sistemas 1:n sin tráfico adicional, la señal de tráfico nulo de conmutación manual transfiere la sección de servicio de la sección de protección a la sección de servicio, a menos que esté en efecto una petición de prioridad igual o más alta. Puesto que la conmutación manual tiene prioridad más baja que SF o SD en una sección de servicio, esta instrucción se aplicará solamente si la sección de servicio no está en condición SF o SD. "La señal de tráfico nulo" de conmutación manual tiene una prioridad mayor que "la señal de tráfico normal de conmutación manual 1" cuando se detectan ambas instrucciones al mismo tiempo.

5) *Ejercicio #* – Emite una petición de ejercicio para esa señal y comprueba las respuestas en los bytes APS, a menos que esté en uso el canal de protección. La conmutación no se completa realmente, es decir, el selector es liberado por una petición de ejercicio en el byte K1 enviado o recibido con acuse de recibo. La funcionalidad de ejercicio puede no existir en todas las funciones MSP.

Se señala que queda en estudio una funcionalidad y una instrucción adecuada para congelar la situación existente de las funciones MSP.

#### 7.1.2.2 Instrucciones de control

Las instrucciones de control fijan y modifican el funcionamiento del protocolo MSP. Las instrucciones de control definidas actualmente sólo se aplicarán a la conmutación 1:n (unidireccional o bidireccional).

Eliminar exclusión de señal de tráfico normal de la protección – Elimina la instrucción de excluir señal de tráfico normal de la protección para la señal (o las señales) de tráfico normal especificadas.

Excluir señal de tráfico normal de la protección – Impide la conmutación de la señal o las señales de tráfico normal especificadas a la sección de protección.

Estas instrucciones no se han de confundir con la petición de exclusión de la protección, que impide que todas las señales de tráfico normal o adicional utilicen la sección de protección. La petición de exclusión de una señal de tráfico normal individual de la protección o la eliminación de la exclusión de una señal de tráfico normal de la protección se recibirá en el punto de referencia MSP_MP. La exclusión de señal de tráfico normal de la protección puede ser activada o eliminada para cada señal de tráfico normal independientemente, y cualquier número de señales de tráfico normal pueden ser excluidas al mismo tiempo. La situación de excluida de una señal de tráfico normal no se refleja directamente en los bytes K.

La operación de exclusión de una señal de tráfico normal de la protección depende del modo de funcionamiento en la capa de protección MS en la cual se aplica. Si el funcionamiento es bidireccional, la exclusión de protección funciona también bidireccionalmente. Si una sección tiene aplicada una instrucción de exclusión de una señal de tráfico normal de la protección, las peticiones de puenteo local no se emiten para la señal de tráfico normal excluida (es decir, las condiciones locales para la sección de servicio asociada y las peticiones externas para la señal de tráfico normal no se consideran en el proceso de generación del byte K1), y no se acusa recibo de peticiones de

puenteo distantes para la señal (es decir, las peticiones distantes para la señal no se consideran en el proceso de generación del byte K1 y no se realiza el puenteo solicitado). Se señala que en el funcionamiento bidireccional, la instrucción de exclusión de señal de tráfico normal de la protección se debe aplicar en ambos extremos para que el funcionamiento sea el adecuado.

Si el funcionamiento es unidireccional, la exclusión funciona también unidireccionalmente. Si una señal de tráfico normal tiene aplicada una instrucción de exclusión de señal de tráfico normal de la protección, no se emiten peticiones de puenteo locales para la señal de tráfico normal excluida. Sin embargo, se acusa recibo de las peticiones de puenteo distantes para la señal de tráfico normal realizando el puenteo y señalizando dicho puenteo en el byte K2.

### 7.1.3 Condiciones MSP

Las siguientes condiciones MSP pueden provocar la conmutación de protección:

Condición fallo de señal (SF), definida como la presencia de la condición protección contra fallo de señal de camino (TSFprot, *trail signal fail protection*) generada por la función de terminación de camino de sección de multiplexación definida en la Recomendación G.783.

NOTA – La condición SF se amplía para la sección de protección. Véase 7.1.1.8.

Condición degradación de señal (SD), definida como la presencia de la condición degradación de la señal de camino (TSD, *trail signal degrade*) generada por la función de terminación de camino de sección de multiplexación (MS) definida en la Recomendación G.783.

### 7.1.4 Operación de conmutación

#### 7.1.4.1 Conmutación bidireccional 1:n sin tráfico adicional

El cuadro 7-4 ilustra la acción de conmutación de protección entre dos ubicaciones de multiplexor, indicadas por A y C, de un sistema de conmutación de protección bidireccional 1:n sin tráfico adicional.

Cuando no se utiliza la sección de protección, se indica señal nula en ambos bytes K1 y K2 enviados. La generación de la señal nula depende del equipo. La señal nula podría ser, por ejemplo, señal no equipada, señal AIS, o cualquier otra señal de tráfico normal conectada en puente a la sección de protección en el extremo de cabeza. El extremo de cola no debe suponer o requerir ninguna señal en la recesión de protección. En el ejemplo del cuadro 7-4, la ubicación C puede puentear la señal de trafico normal 3 como señal nula, mientras que la ubicación A puede puentear la señal de tráfico normal 4 como señal nula.

Cuando se detecta una condición de fallo o se recibe una instrucción de conmutación en el extremo de cola de una sección de multiplexación, la lógica de protección compara la prioridad de esta nueva condición con la prioridad de la petición de la señal de tráfico en la sección de protección. La comparación incluye la prioridad de cualquier orden de puenteo, es decir, de una petición en un byte K1 recibido. Si la nueva petición es de prioridad mayor, se carga el byte K1 con la petición y el número de la señal de tráfico que solicita la utilización de la sección de protección. En el ejemplo, se detecta SD en C en la sección de servicio 2, y esta condición es enviada en el byte K1 como una orden de puenteo en A.

En el extremo de cabecera, cuando este nuevo byte K1 entrante ha sido verificado (después de haberse recibido idénticamente en tres tramas sucesivas) y evaluado (por la lógica de prioridad), se puentea la señal de tráfico normal solicitada con la sección de protección, el byte K2 [1-4] saliente se envía para confirmar el puenteo solicitado, y el byte K1 saliente se fija con una instrucción de invertir petición para ordenar un puenteo en el extremo de cola de esa señal de tráfico normal, iniciando una conmutación bidireccional. Se señala que se devuelve una instrucción de invertir petición para el ejercicio y todas las demás peticiones de prioridad mayor. Esto identifica claramente

el extremo que originó la petición de conmutación. Si el extremo de cabecera hubiera originado también una petición idéntica (no confirmada aún por una instrucción de invertir petición) para la misma señal, ambos extremos continuarían transmitiendo el byte K1 idéntico y realizarían la acción de conmutación solicitada.

Asimismo, en el extremo de cabecera, la señal de tráfico indicada se conecta en puente con la protección. Cuando la señal está puenteada, se fija el byte K2 para indicar el número de la señal de tráfico en protección.

En el extremo de cola, cuando el número de la señal de tráfico en el byte K2 recibido concuerda con el número de la señal de tráfico que solicita la conmutación, se selecciona esa señal de la protección. Así se completa la conmutación de una señal de tráfico a protección para un sentido. El extremo de cola realiza también el puenteo ordenado por el byte K1 e indica la señal puenteada en el byte K2.

El extremo de cabecera completa la conmutación bidireccional seleccionando la señal de protección cuando recibe un byte K2 concordante.

Si la conmutación no se completa porque las señales solicitadas/puenteadas no concuerdan dentro de 50 ms, los selectores permanecerán liberados y se indicará fallo de protocolo. Esto puede suceder cuando un extremo es unidireccional y el otro es bidireccional. Se puede producir también una falta de concordancia cuando una señal de tráfico excluida en un extremo no lo está en el otro. Se señala que la falta de concordancia puede producirse también cuando una arquitectura 1 + 1 conecta con una arquitectura 1:1 (que no está prevista en el estado 1 + 1) debido a la falta de concordancia del bit 5 de los bytes K2. Lo que se puede utilizar para que la arquitectura 1:1 funcione como 1 + 1.

El ejemplo ilustra además una conmutación de prioridad, cuando una condición SF en la sección de servicio 1 desplaza con prioridad a la conmutación de la señal de tráfico normal 2. Se señala que los selectores son liberados temporalmente antes de seleccionar señal de tráfico normal 1 de protección, debido a la falta de concordancia temporal del número de la señal en los bytes K1 enviado y K2 recibido. En este ejemplo se muestra también la conmutación de la señal de tráfico normal 2 a protección después de que se ha reparado la sección 1 que había fallado.

Cuando ya no se requiere la conmutación, por ejemplo, porque la sección de servicio que había fallado se ha recuperado del fallo y ha expirado el tiempo de espera al restablecimiento, el extremo de cola indica "ausencia de petición" de señal nula en el byte K1 (0000 0000). Esto libera el selector debido a la falta de concordancia del número de sección.

El extremo de cabecera libera a continuación el puenteo y responde con la misma indicación en el byte K1 e indicación de señal nula en el byte K2. El selector del extremo de cabecera es liberado también debido a la falta de concordancia.

La recepción de la señal nula en el byte K1 hace que el extremo de cola libere el puenteo. Puesto que los bytes K2 indican ahora señal nula que concuerda con la señal nula de los bytes K1, los selectores permanecen liberados sin indicación alguna de falta de concordancia y se completa el restablecimiento.

## Cuadro 7-4/G.841 – Ejemplo de conmutación de protección bidireccional 1:n sin tráfico adicional

| Condición de fallo o estado de controlador | Bytes APS | | | | Acción | |
|---|---|---|---|---|---|---|
| | C → A | | A → C | | | |
| | Byte K1 | Byte K2 | Byte K1 | Byte K2 | En C | En A |
| Ningún fallo (la sección de protección no está en uso) | 0000 0000 | 0000 1000 | 0000 0000 | 0000 1000 | La señal nula está puenteada a protección. Se libera el selector. | La señal nula está puenteada a protección. Se libera el selector. |
| Sección de servicio 2 degradada en el sentido A → C | 1010 0010 | 0000 1000 | 0000 0000 | 0000 1000 | Fallo detectado. Petición de puenteo de señal de tráfico normal 2 – SD. | |
| | 1010 0010 | 0000 1000 | 0010 0010 | 0010 1000 | | Puenteo de señal de tráfico normal 2. Inversión de petición de puenteo de señal de tráfico normal 2. |
| | 1010 0010 | 0010 1000 | 0010 0010 | 0010 1000 | Conmutación de señal de tráfico normal 2 de la señal de protección. Puenteo de señal de tráfico normal 2 a protección. | |
| | 1010 0010 | 0010 1000 | 0010 0010 | 0010 1000 | | Conmutación de señal de tráfico normal 2 de protección. Conmutación bidirec-cional completada. |
| Fallo de la sección de servicio 1 en el sentido C → A | 1010 0010 | 0010 1000 | 1100 0001 | 0010 1000 | | Fallo detectado. Petición de puenteo de señal de tráfico normal 1 – SF. Liberación de conmuta-ción de señal de tráfico normal 2. |
| (Esto desplaza con prioridad la conmutación de la señal de tráfico normal 2) | 0010 0001 | 0001 1000 | 1100 0001 | 0010 1000 | Puenteo de señal de tráfico normal 1 a protección. Inversión de petición de puenteo de señal de tráfico normal 1. Liberación de conmuta-ción de señal de tráfico normal 2. | |
| | 0010 0001 | 0001 1000 | 1100 0001 | 0001 1000 | | Conmutación de señal de tráfico normal 1. Puenteo de señal de tráfico normal 1. |
| | 0010 0001 | 0001 1000 | 1100 0001 | 0001 1000 | Conmutación de señal de tráfico normal 1. Conmutación bidirec-cional completada. | |

**Cuadro 7-4/G.841 – Ejemplo de conmutación de protección bidireccional 1:n sin tráfico adicional *(fin)***

| Condición de fallo o estado de controlador | Bytes APS | | | | Acción | |
|---|---|---|---|---|---|---|
| | C → A | | A → C | | | |
| | Byte K1 | Byte K2 | Byte K1 | Byte K2 | En C | En A |
| Sección de servicio 1 | 0010 0001 | 0001 1000 | 0110 0001 | 0001 1000 | | Espera al restablecimiento. |
| Reparada (sección de servicio 2 todavía degradada) | 1010 0010 | 0001 1000 | 0110 0001 | 0001 1000 | Petición de puenteo de señal de tráfico normal 2. Liberación de conmutación de señal de tráfico normal 1. | |
| | 1010 0010 | 0001 1000 | 0010 0010 | 0010 1000 | | Puenteo de señal de tráfico normal 2. Inversión de petición de puenteo de señal de tráfico normal 2. Liberación de conmutación de señal de tráfico normal 1. |
| | 1010 0010 | 0010 1000 | 0010 0010 | 0010 1000 | Puenteo de señal de tráfico normal 2. Conmutación de señal de tráfico normal 2. | |
| | 1010 0010 | 0010 1000 | 0010 0010 | 0010 1000 | | Conmutación de señal de tráfico normal 2. Conmutación bidireccional completada. |
| Sección de servicio 2 reparada | 0110 0010 | 0010 1000 | 0010 0010 | 0010 1000 | Espera al restablecimiento de señal de tráfico normal 2. | |
| Espera al restablecimiento espirada (ausencia de fallos) | 0000 0000 | 0010 1000 | 0010 0010 | 0010 1000 | Supresión de orden de puenteo de señal de tráfico normal 2. Liberación de conmutación de señal de tráfico normal 2. | |
| | 0000 0000 | 0010 1000 | 0000 0000 | 0000 1000 | | Supresión de puenteo de señal de tráfico normal 2. Supresión de petición de puenteo de señal de tráfico normal 2. Liberación de conmutación de señal de tráfico normal 2. |
| | 0000 0000 | 0000 1000 | 0000 0000 | 0000 1000 | Supresión de puenteo de señal de tráfico normal 2. Señal nula puenteada a protección. | Señal nula puenteada a protección. |

#### 7.1.4.2 Conmutación bidireccional 1:1 con tráfico adicional

El cuadro 7-5 ilustra la acción de conmutación de protección entre dos ubicaciones de multiplexor, indicadas por A y C, de un sistema de conmutación de protección bidireccional 1:n con tráfico adicional.

Cuando ya no se utiliza la sección de protección, la señal de tráfico adicional se transfiere vía sección de protección.

Cuando falla una señal o se detecta una condición de degradación de señal o se recibe una instrucción de conmutación en el extremo de cola de una sección de multiplexación, la lógica de protección compara la prioridad de esta nueva condición con la prioridad de la petición de la señal de tráfico (si hay alguna) en la sección de protección. La comparación incluye la prioridad de cualquier orden de puenteo, es decir, de una petición en un byte K1 recibido. Si la nueva petición es de prioridad mayor, se carga el byte K1 con la petición y el número de la señal que solicita la utilización de la sección de protección. En el ejemplo, se detecta SD en C en la sección de servicio 2, y esta condición es enviada en el byte K1 como una orden de puenteo en A.

En el extremo de cabecera, cuando este nuevo byte K1 ha sido verificado y evaluado (por la lógica de prioridad), se fija con una instrucción de invertir petición como una confirmación de la señal para utilizar la protección y ordenar un puenteo en el extremo de cola de la señal. Así se inicia una conmutación bidireccional. Se señala que se devuelve una instrucción de invertir petición para el ejercicio y todas las demás peticiones de prioridad más alta. De esta manera se identifica claramente el extremo que originó la petición de conmutación. Si el extremo de cabecera hubiera originado también una petición idéntica (no confirmada aún con una instrucción de invertir petición) para el mismo canal, ambos extremos continuarían transmitiendo el byte K1 idéntico y realizarían la acción de conmutación solicitada.

Asimismo, en el extremo de cabecera, la señal de tráfico indicada se conecta en puente con la protección. Cuando la señal está puenteada, se fija el byte K2 para indicar el número de la señal de tráfico en protección.

En el extremo de cola, cuando el número de la señal en el byte K2 recibido concuerda con el número de la señal de tráfico que solicita la conmutación, se selecciona esa señal de protección. Así se completa la conmutación a protección para un sentido. El extremo de cola realiza también el puenteo ordenado por el byte K1 e indica la señal puenteada en el byte K2.

El extremo de cabecera completa la conmutación bidireccional seleccionando la señal de protección cuando recibe un byte K2 concordante.

Si la conmutación no se completa porque las señales solicitadas/puenteadas no concuerdan dentro de 50 ms, los selectores permanecerán liberados y se indicará fallo de protocolo. Esto puede suceder cuando un extremo es unidireccional y el otro es bidireccional. Se puede producir también una falta de concordancia cuando una señal excluida en un extremo no lo está en el otro. Se señala que esta falta de concordancia puede producirse también cuando una arquitectura 1 + 1 conecta con una arquitectura 1:1 (que no está prevista para el estado 1 + 1) debido a la falta de concordancia del bit 5 de los bytes K2. Lo que se puede utilizar para que la arquitectura 1:1 funcione como 1 + 1.

El ejemplo ilustra además una conmutación de prioridad, cuando una condición SF en la sección de servicio desplaza con prioridad a la conmutación de la sección de servicio 2. Se señala que los selectores son liberados temporalmente antes de seleccionar sección de servicio 1, debido a la falta de concordancia temporal del número de la señal en los bytes K1 enviado y K2 recibido. En el ejemplo se muestra también la conmutación de la sección de servicio 2 después de que se ha reparado la sección 1 que había fallado.

Cuando ya no se requiere la conmutación, por ejemplo, porque la sección de servicio que había fallado ha recuperado el fallo y ha expirado el tiempo de espera al restablecimiento, el extremo de cola indica ausencia de petición de señal de tráfico adicional en el byte K1 (señal nula si no se proporciona tráfico adicional). Esto libera el selector y el puenteo debido a la falta de concordancia del número de canal. El extremo de cabecera libera a continuación el selector, puentea la señal de tráfico adicional y responde con la misma indicación en el byte K1 e indicación de señal de tráfico adicional en el byte K2. El extremo de cola selecciona y puentea ahora la señal de tráfico adicional y responde con una indicación de señal de tráfico adicional en el byte K2. El extremo de cabecera selecciona el tráfico adicional en respuesta, lo que completa la conmutación bidireccional a la señal de tráfico adicional.

**Cuadro 7-5/G.841 – Ejemplo de conmutación de protección bidireccional 1:n con tráfico adicional**

| **Condición de fallo o estado de controlador** | **Bytes APS** | | | | **Acción** | |
|---|---|---|---|---|---|---|
| | **C → A** | | **A → C** | | | |
| | **Byte K1** | **Byte K2** | **Byte K1** | **Byte K2** | **En C** | **En A** |
| Ningún fallo (tráfico adicional en sección de protección) | 0000 1111 | 1111 1000 | 0000 1111 | 1111 1000 | Señal de tráfico adicional puenteada y seleccionada. | Señal de tráfico adicional puenteada y seleccionada. |
| Sección de servicio 2 degradada en el sentido A → C | 1010 0010 | 0000 1000 | 0000 1111 | 1111 1000 | Fallo detectado.<br>Orden de puenteo de sección de servicio 2 – SD.<br>Liberación de puenteo.<br>Liberación de selector. | |
| | 1010 0010 | 0000 1000 | 0010 0010 | 0010 1000 | | Liberación de selector.<br>Inversión de orden de puenteo de sección de servicio 2.<br>Puenteo de sección de servicio 2. |
| | 1010 0010 | 0010 1000 | 0010 0010 | 0010 1000 | Selección de sección de servicio 2.<br>Puenteo de sección de servicio 2. | |
| | 1010 0010 | 0010 1000 | 0010 0010 | 0010 1000 | | Selección de sección de servicio 2.<br>Conmutación bidireccional completada. |
| Sección de servicio 1 con fallo en el sentido C → A | 1010 0010 | 0010 1000 | 1100 0001 | 0000 1000 | | Fallo detectado.<br>Orden de puenteo de sección de servicio 1 – SF.<br>Liberación de selector.<br>Liberación de puenteo. |
| (Esto desplaza con prioridad a la conmutación de sección de servicio 2) | 0010 0001 | 0001 1000 | 1100 0001 | 0000 1000 | Liberación de selector de sección de servicio 2.<br>Inversión de orden de puenteo de sección de servicio 1.<br>Puenteo de sección de servicio 1. | |

**Cuadro 7-5/G.841 – Ejemplo de conmutación de protección bidireccional 1:n con tráfico adicional *(fin)***

| Condición de fallo o estado de controlador | Bytes APS | | | | Acción | |
|---|---|---|---|---|---|---|
| | C → A | | A → C | | | |
| | Byte K1 | Byte K2 | Byte K1 | Byte K2 | En C | En A |
| | 0010 0001 | 0001 1000 | 1100 0001 | 0001 1000 | | Selección de sección de servicio 1.<br>Puenteo de selección de servicio 1. |
| | 0010 0001 | 0001 1000 | 1100 0001 | 0001 1000 | Selección de sección de servicio 1.<br>Conmutación bidirec-cional completada. | |
| Sección de servicio 1 reparada | 0010 0001 | 0001 1000 | 0110 0001 | 0001 1000 | | Espera al restablecimiento. |
| (Sección de servicio 2 aún degradada) | 1010 0010 | 0000 1000 | 0110 0001 | 0001 1000 | Orden de puenteo de sección de servicio 2.<br>Liberación de selector.<br>Liberación de puenteo. | |
| | 1010 0010 | 0000 1000 | 0010 0010 | 0010 1000 | | Inversión de orden de puenteo de sección de servicio 2.<br>Puenteo de sección de servicio 2.<br>Liberación de selector. |
| | 1010 0010 | 0010 1000 | 0010 0010 | 0010 1000 | Puenteo de sección de servicio 2.<br>Selección de sección de servicio 2. | |
| | 1010 0010 | 0010 1000 | 0010 0010 | 0010 1000 | | Selección de sección de servicio 2.<br>Conmutación bidirec-cional completada. |
| Sección de servicio 2 reparada | 0110 0010 | 0010 1000 | 0010 0010 | 0010 1000 | Espera al restablecimiento de sección de servicio 2. | |
| Espera al restablecimiento expirada (ningún fallo, seleccionado tráfico adicional) | 0000 1111 | 0000 1000 | 0010 0010 | 0010 1000 | Orden de puenteo de tráfico adicional – NR.<br>Liberación de selector.<br>Liberación de puenteo. | |
| | 0000 1111 | 0000 1000 | 0000 1111 | 1111 1000 | | Orden de puenteo de tráfico adicional – NR.<br>Puenteo de tráfico adicional.<br>Liberación de selector. |
| | 0000 1111 | 1111 1000 | 0000 1111 | 1111 1000 | Puenteo de tráfico adicional.<br>Selección de tráfico adicional. | |
| | 0000 1111 | 1111 1000 | 0000 1111 | 1111 1000 | | Selección de tráfico adicional.<br>Conmutación bidirec-cional completada. |

#### 7.1.4.3 Conmutación unidireccional 1:n

Las acciones son las descritas en 7.1.4.1, salvo que la conmutación unidireccional se completa cuando el extremo de cola selecciona la protección de la sección para la que emitió una petición. Esta diferencia de funcionamiento se obtiene no considerando las peticiones distantes en la lógica de prioridad y, por consiguiente, no emitiendo peticiones inversas.

#### 7.1.4.4 Conmutación unidireccional 1 + 1

Para la conmutación unidireccional 1 + 1, la selección de señal se basa en las condiciones y peticiones locales. En consecuencia, cada extremo funciona independientemente del otro, y los bytes K1 y K2 no tienen que coordinar la acción de conmutación. Sin embargo, el byte K1 se utiliza aún para informar al otro extremo de la acción local y el bit 5 del byte K2 se pone a cero.

#### 7.1.4.5 Conmutación bidireccional 1 + 1

El funcionamiento de la conmutación bidireccional 1 + 1 se puede optimizar para una red en la que la conmutación de protección 1:n se utiliza ampliamente y que se basa por tanto en la compatibilidad con una disposición 1:n; como posibilidad alternativa, se puede optimizar para una red en la que se utiliza predominantemente la conmutación bidireccional 1 + 1. Esto conduce a dos operaciones de conmutación posibles que se describen a continuación y en el anexo B.

##### 7.1.4.5.1 Conmutación bidireccional 1 + 1 compatible con conmutación bidireccional 1:n

Los bytes K1 y K2 se intercambian como se describe en 7.1.4.1 para completar la conmutación. Puesto que el puenteo es permanente, es decir, la señal de tráfico normal está siempre puenteada a la sección de protección, la señal de tráfico normal 1 se indica en el byte K2, a menos que el byte K1 recibido indique señal nula (0). La conmutación se completa cuando ambos extremos seleccionan la señal de la protección, y puede tomar menos tiempo porque la indicación K2 no depende de una acción de puenteo.

Para la conmutación reversiva, el restablecimiento se efectúa como se describe en 7.1.4.1. Para la conmutación no reversiva, el cuadro 7-6 muestra el funcionamiento de un sistema de conmutación de protección bidireccional 1 + 1.

Para funcionamiento no reversivo, suponiendo que la señal de tráfico normal está en protección, cuando la sección de servicio es reparada, o se libera una instrucción de conmutación, el extremo de cola mantiene la selección e indica no inversión para la señal de tráfico normal. El extremo de cabeza mantiene también la selección y continúa indicando invertir petición. La instrucción de no invertir se suprime cuando sea desplazada con prioridad por una condición de fallo o una petición externa.

**Cuadro 7-6/G.841 – Ejemplo de conmutación bidireccional 1 + 1 compatible con conmutación bidireccional 1:n**

| Condición de fallo o estado de controlador | Bytes APS | | | | Acción | |
|---|---|---|---|---|---|---|
| | C → A | | A → C | | | |
| | Byte K1 | Byte K2 | Byte K1 | Byte K2 | En C | En A |
| Ningún fallo (se supone que la sección de protección no está en uso) | 0000 0000 | 0000 0000 | 0000 0000 | 0000 0000 | Se libera el selector. | Se libera el selector. |
| Sección de servicio 1 con fallo en el sentido A → C | 1101 0001 | 0000 0000 | 0000 0000 | 0000 0000 | Fallo detectado. Petición de puenteo de señal de tráfico normal 1 – SF. | |
| | 1101 0001 | 0000 0000 | 0010 0001 | 0001 0000 | | Indicación de señal de tráfico normal 1 puenteada. Inversión de petición de puenteo de señal de tráfico normal 1. |
| | 1101 0001 | 0001 0000 | 0010 0001 | 0001 0000 | Indicación de señal de tráfico normal 1 puenteada. Selección de señal de tráfico normal de sección de protección. | |
| | 1101 0001 | 0001 0000 | 0010 0001 | 0001 0000 | | Selección de señal de tráfico normal de sección de protección. Conmutación bidireccional completada. |
| Sección de servicio 1 reparada. Mantenimiento de conmutación (no reversivo) | 0001 0001 | 0001 0000 | 0010 0001 | 0001 0000 | Envío de no invertir. | |
| Sección de protección degradada en el sentido A → C | 1011 0000 | 0001 0000 | 0010 0001 | 0001 0000 | Fallo detectado. Petición de puenteo de señal nula – SD. Selección de señal de tráfico normal de sección de servicio. | |
| | 1011 0000 | 0001 0000 | 0010 0000 | 0000 0000 | | Inversión de petición de puenteo de señal nula. Supresión de indicación de puenteo de señal de tráfico normal. Selección de señal de tráfico normal de sección de servicio. |
| | 1011 0000 | 0000 0000 | 0010 0000 | 0000 0000 | Supresión de indicación de puenteo de señal de tráfico normal. | |
| Sección de protección reparada | 0000 0000 | 0000 0000 | 0010 0000 | 0000 0000 | Envío de no invertir. | |
| | 0000 0000 | 0000 0000 | 0000 0000 | 0000 0000 | | Envío de no invertir. |

## 7.2 Anillos de protección compartida de s ección de multiplexación

### 7.2.1 Anillos de protección compartida de sección de multiplexación de dos y de cuatro fibras

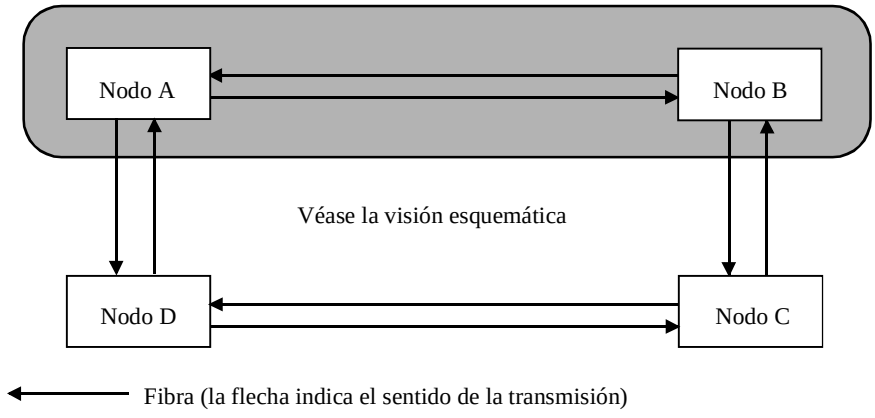
Todos los anillos de protección compartida de sección de multiplexación (MS) admiten la conmutación de anillo. Además, los anillos de protección compartida de sección de multiplexación de cuatro fibras admiten la conmutación de tramo.

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

Los anillos conmutados de sección de multiplexación 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. El tráfico normal transportado por los canales de servicio de una fibra está protegido por los canales de protección de sentido opuesto alrededor del anillo (véase la figura 7-2). Esto permite el transporte bidireccional del tráfico normal. En cada fibra se utiliza únicamente un conjunto de canales de tara.

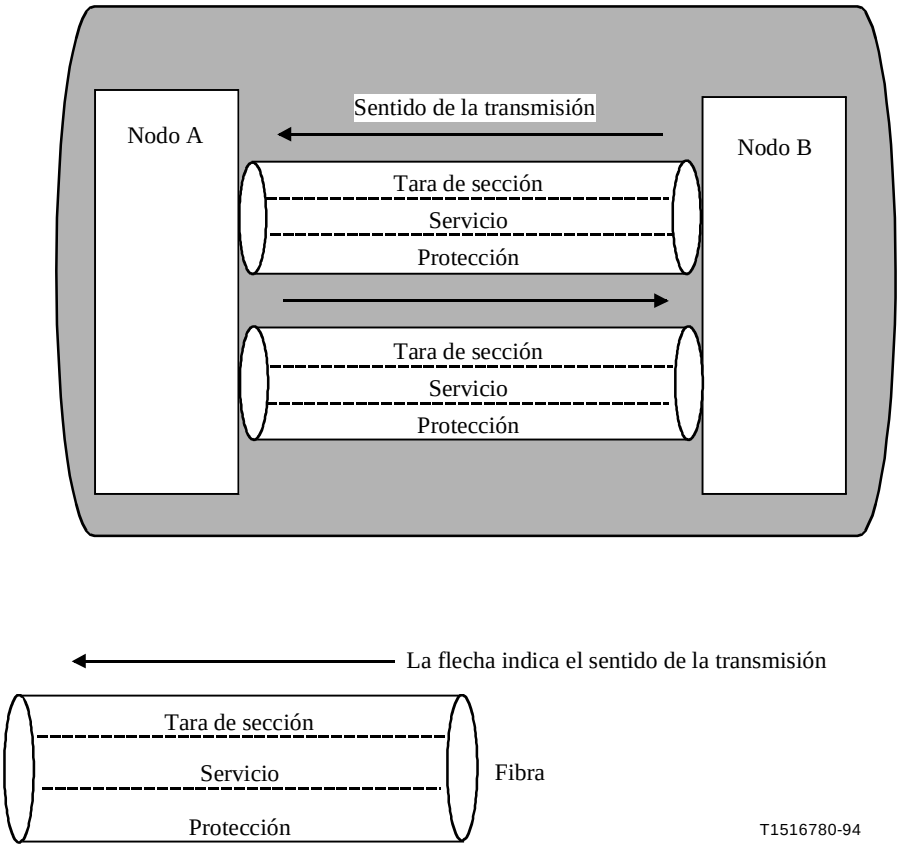
Los anillos de protección compartida de sección de multiplexación de dos fibras admiten únicamente la conmutación de anillo. Cuando se invoca una conmutación de anillo, el tráfico normal es conmutado de los canales de servicio a los canales de protección en el sentido opuesto.

Si se soporta tráfico no protegido y no desplazable con prioridad (NUT, *non-pre-emptable unprotected traffic*), se pueden provisionar canales seleccionados en la anchura de banda de servicio y sus correspondientes canales de protección como canales no protegidos y no desplazables con prioridad. Los canales de servicio restantes aún están protegidos por los correspondientes canales de protección. Los canales no protegidos y no desplazables con prioridad no tendrán protección APS de BLSR.




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 7-2/G.841 – Anillo de protección compartida de MS de dos fibras**

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

Los anillos de protección compartida de sección de multiplexación de cuatro fibras requieren cuatro fibras para cada tramo del anillo. Como se ilustra en la figura 7-3, 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 normal. 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 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.

Si se soporta el NUT, se pueden provisionar, en cada tramo, canales seleccionados en la anchura de banda de servicio y sus correspondientes canales de protección como canales no protegidos y no reemplazables con prioridad. Los canales de servicio restantes aún están protegidos, tanto a efectos de conmutación de tramo como de conmutación de anillo, por sus correspondientes canales de protección. El efecto en un canal seleccionado no protegido y no desplazable con prioridad es como sigue:

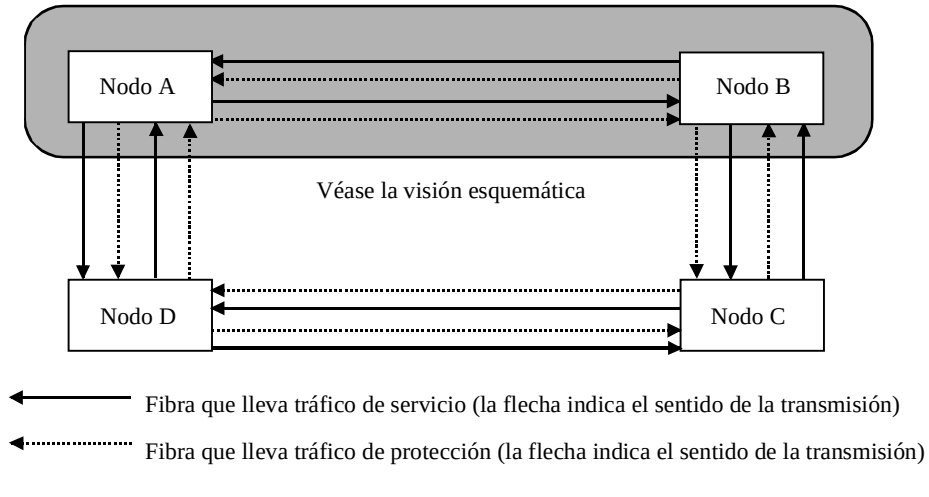
– la conmutación de anillo queda inhabilitada en ese canal en cualquier punto del anillo (como en el caso de dos fibras);

– la conmutación de tramo queda inhabilitada para ese canal en el tramo provisionado.

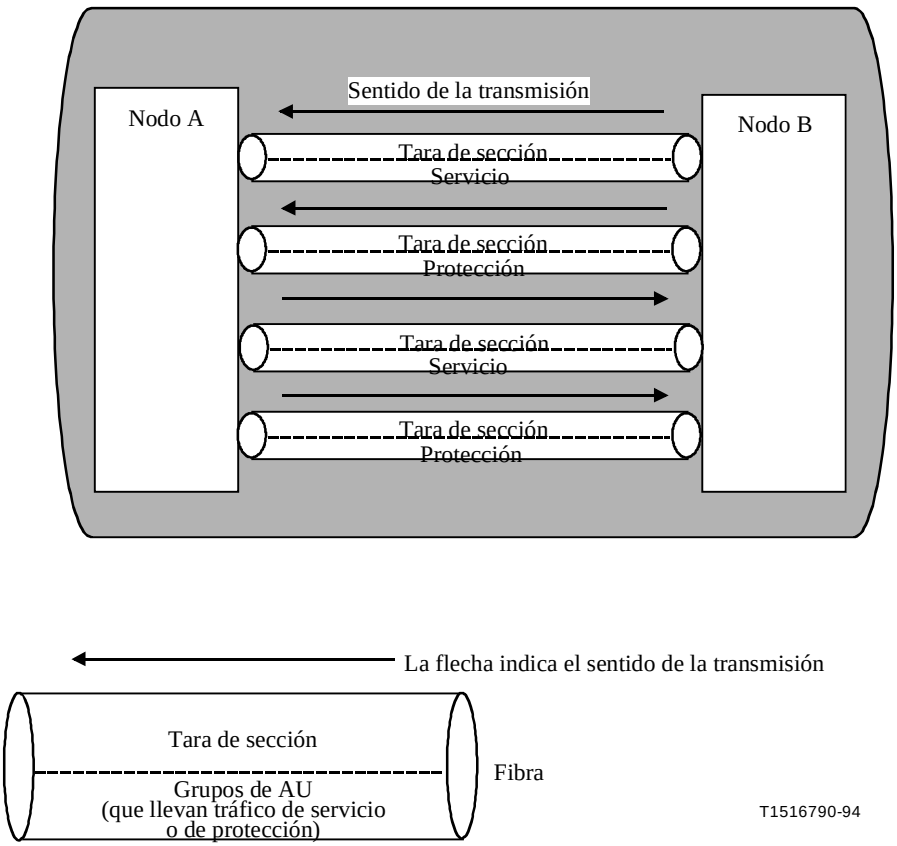
Por consiguiente, el canal NUT no tiene protección APS SPRING de MS en el tramo provisionado; en otros tramos, el mismo canal (si no se provisiona como NUT), sólo disponen de la conmutación de tramo. Se señala que, si estos canales se provisionan como canales de servicio en otros tramos, tendrán una capacidad de supervivencia inferior a la de otros canales de servicio porque no disponen de la conmutación de anillo.

El soporte de la provisión de canales no protegidos y no desplazables con prioridad requiere la presencia de una tabla de NUT en cada nodo en el protocolo MS SPRING. La figura 7-4 da la representación conceptual y un ejemplo de tabla de NUT. Dicha tabla contiene información para identificar los canales que han sido provisionados para NUT e identifica el tipo de conmutación (a saber, conmutación de tramo o de anillo) prohibida por el NUT. Puesto que la provisión de un canal de servicio no protegido y no desplazable con prioridad garantiza de manera automática que el canal de protección correspondiente también es no protegido y no desplazable con prioridad, basta con incluir en la tabla el identificador (ID) del canal de servicio. La tabla correspondiente para funcionamiento con dos fibras sólo necesita una columna para conmutación de anillo.

Los anillos de protección compartida de sección de multiplexación 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 podrá existir si se establece un segmento de anillo aislado antes de que todos los demás tramos sean totalmente operacionales.




**a) Visión del anillo en su totalidad**




**b) Visión esquemática de la porción sombreada del anillo**

**Figura 7-3/G.841 – Anillo de protección compartida de MS de cuatro fibras**


- Todos los tramos tienen NUT para AU-4 #1
- El tramo entre B y C tiene NUT en AU-4 #2

Nodo A

| AU-4 # | Conmutador de anillo | Conmutador de tramo | |
|---|---|---|---|
| | | Este | Oeste |
| 1 | – | – | – |
| 2 | – | | |
| 3 | | | |
| 4 | | | |
| 5 | | | |
| . . . | | | |

Nodo B

| AU-4 # | Conmutador de anillo | Conmutador de tramo | |
|---|---|---|---|
| | | Este | Oeste |
| 1 | – | – | – |
| 2 | – | – | |
| 3 | | | |
| 4 | | | |
| 5 | | | |
| . . . | | | |

Nodo C

| AU-4 # | Conmutador de anillo | Conmutador de tramo | |
|---|---|---|---|
| | | Este | Oeste |
| 1 | – | – | – |
| 2 | – | | – |
| 3 | | | |
| 4 | | | |
| 5 | | | |
| . . . | | | |

Nodo D

| AU-4 # | Conmutador de anillo | Conmutador de tramo | |
|---|---|---|---|
| | | Este | Oeste |
| 1 | – | – | – |
| 2 | – | | |
| 3 | | | |
| 4 | | | |
| 5 | | | |
| . . . | | | |

T1529650-98

– Indica que esta facilidad no está disponible para conmutación de protección.

NOTA – En este ejemplo, oeste se refiere al sentido contrario de las agujas del reloj.

**Figura 7-4/G.841 – Representación conceptual y ejemplo de tabla de NUT**

### 7.2.2 Objetivos de red

Son aplicables los siguientes objetivos de red:

1) *Tiempo de conmutación* – En un anillo en que no haya tráfico adicional, todos los nodos en estado de reposo (ningún fallo detectado, ninguna instrucción automática o externa activa y recibiendo solamente bytes K en reposo) y con menos de 1200 km de fibra, el tiempo de compleción de la conmutación (de anillo y de tramo) para un fallo en un solo tramo será inferior a 50 ms. En anillos bajo todas las demás condiciones, el tiempo de compleción de la conmutación puede exceder de 50 ms (el intervalo específico está siendo objeto de estudio) para dar tiempo para eliminar el tráfico adicional o para negociar y acomodar peticiones de APS coexistentes.

2) *Retardo de transmisión* – No hay objetivo de red relativo al retardo de transmisión.

3) *Tiempo de abstención* – No hay objetivo de red relativo a los tiempos de abstención.

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 protección bidireccional.

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 reversiva. 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 ausencia de 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, *time-slot interchange*), 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.

### 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 tráfico normal transportado por el canal de servicio *m* es protegido por el canal de protección (N/2) + *m*. Por ejemplo, un STM-4 puede considerarse como un múltiplex de cuatro 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 cuatro 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 conmutación 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 conmutación de protección que no son críticas con relación al tiempo (por ejemplo, las funciones que no necesitan ser completadas en un plazo de 50 ms).

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 tráfico normal o adicional en canales en cualquier sentido, retirar tráfico normal o adicional de canales de cualquier sentido o dejar pasar canales directamente para permitir la conexión de otros nodos. Puesto que anillos de protección compartida de sección de multiplexación soportan tráfico adicional, esta capacidad se puede aplicar no solamente al canal de servicio, sino también, opcionalmente, a los canales de protección. 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 la figura 7-5 se da un ejemplo de dicho mapa de anillo y en la figura 7-6 se da un ejemplo de tabla de silenciamiento.

| | 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 |

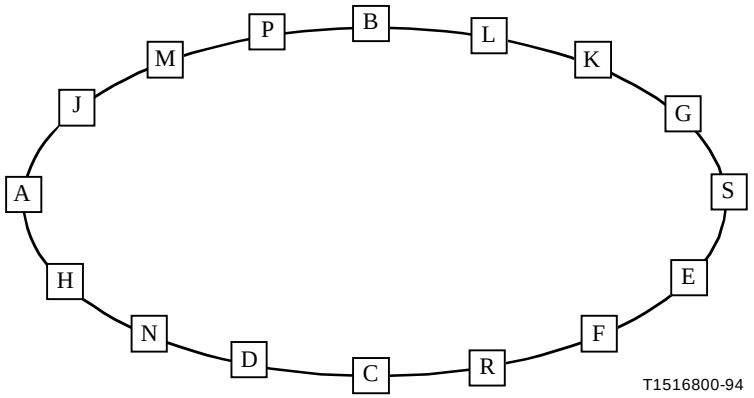
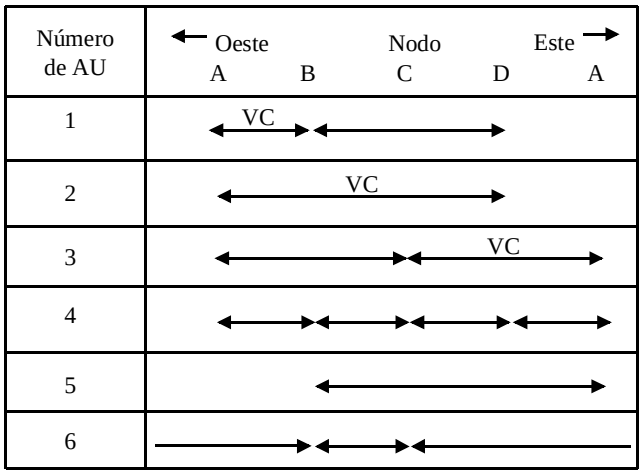



**Figura 7-5/G.841 – Representación conceptual de un mapa de topología en anillo**




Encaminamiento de tráfico de muestra para un anillo de 4 nodos

Nodo A

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

Nodo B

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

Nodo C

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

Nodo D

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

T1516810-94

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 7-6/G.841 – Representación conceptual de mapa de interconexión de nodos**

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.707. Este aspecto queda en estudio. La excepción es el tráfico adicional que puede añadirse, retirarse o transferirse de manera similar al tráfico normal.

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 situación de la petición de puenteo (o 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 7-7. En un anillo de dos fibras, B puenteará el tráfico normal de 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 el tráfico normal

de 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 el tráfico normal de 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 el tráfico normal de 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.

Cuando el fallo haya sido eliminado, los nodos que originan las peticiones de puenteo retirarán sus respectivas peticiones y conmutaciones. Los otros nodos del anillo detendrán la transferencia de los canales de protección y los bytes K. Por lo general, el tráfico normal sólo retorna de los canales de protección a los canales de servicio. Específicamente, en un anillo de cuatro fibras, si está activa una conmutación de anillo en los canales de protección del trayecto largo, y quedan disponibles los canales de protección del trayecto corto, el servicio no será conmutado 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 conmutaciones de anillo y de tramo pueden ser desplazadas por peticiones de puenteo de prioridad superior, como se determina mediante el cuadro 7-8. Considérese, por ejemplo, una conmutación de tramo que está activa debido a una degradación de señal en ese tramo, y que por otra parte, se requiere una conmutación 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 conmutación de trayecto y se establecerá la conmutación de anillo.

No se permite que las instrucciones iniciadas externamente, denegadas o desplazadas con prioridad debido a una petición de APS de prioridad mayor, queden pendientes.

Tan pronto como el nodo reciba una petición de prioridad mayor que la de ausencia de petición, y solamente si esa petición es una petición de anillo distinta de EXER-R, o requiere la utilización de canales que transportan el tráfico adicional, será desplazado con prioridad el tráfico adicional.

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 SF-R y FS-R), 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 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 conmutación.

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 puenteado 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.

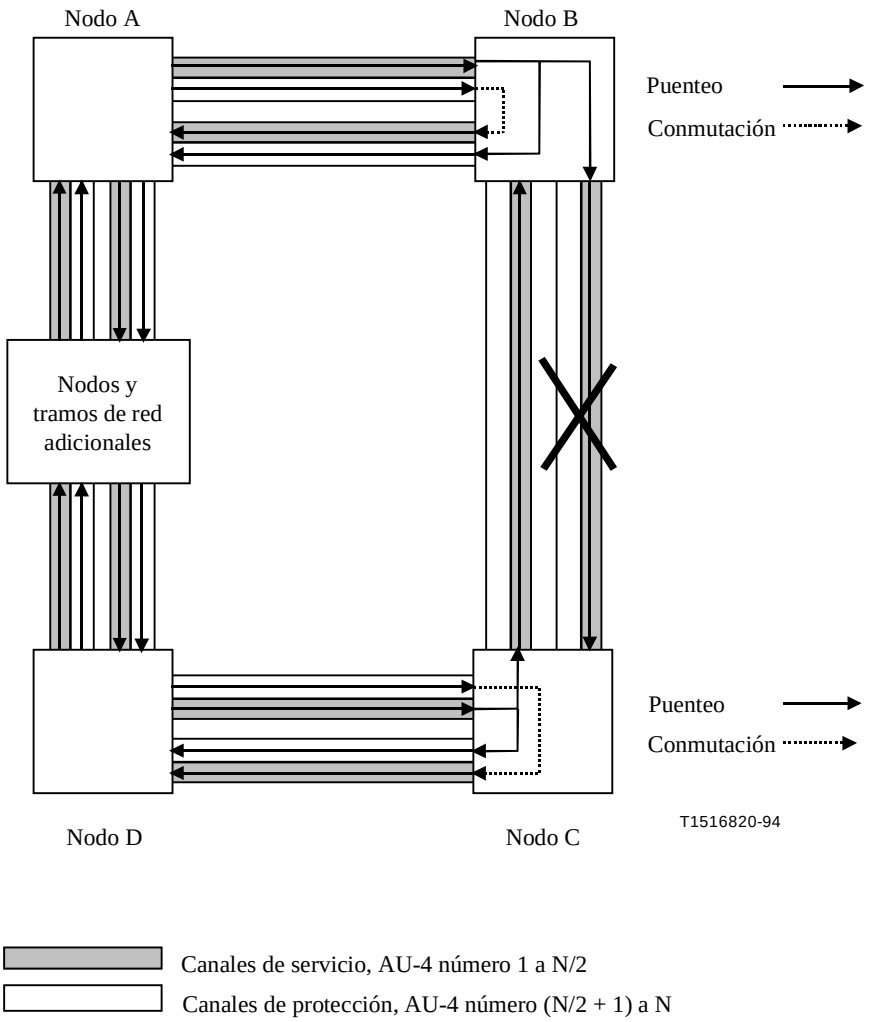
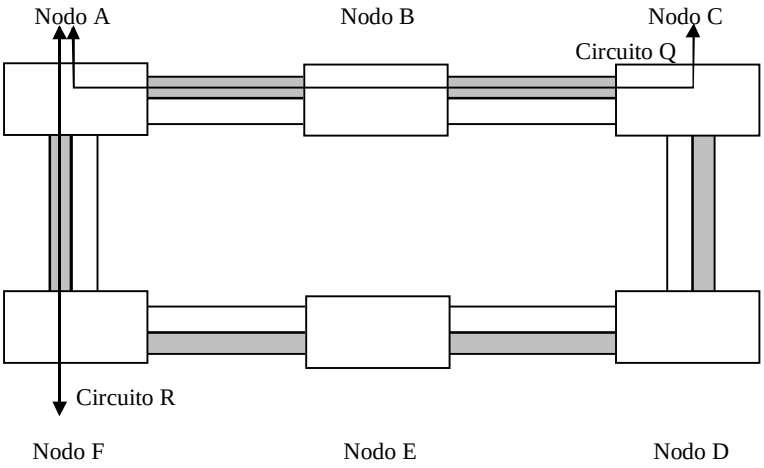
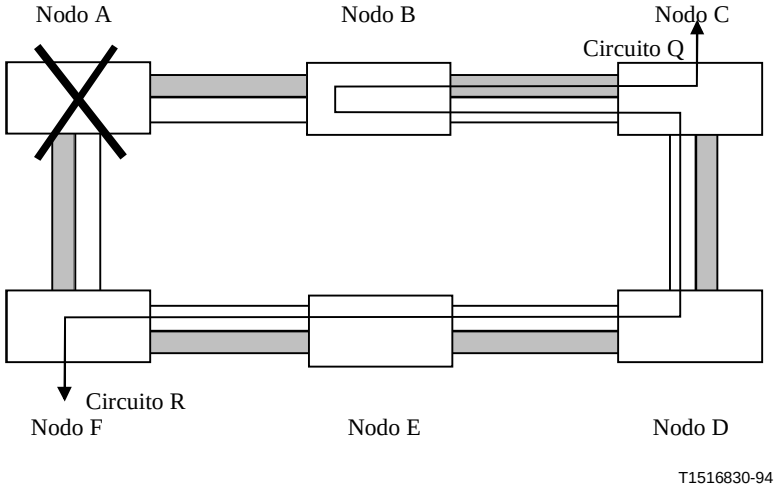



**Figura 7-7/G.841 – Puenteo y conmutación en un anillo de protección compartida de MS de dos fibras**




**a) Estado normal antes de fallo de nodo**




**b) Conexión incorrecta después de fallo de nodo**

| Circuito | Asignación de intervalos de tiempo | Canal |
|---|---|---|
| Q | 1W | Servicio |
| R | 1W | Servicio |

Servicio

Protección

Servicio transportador de circuitos

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 7-8/G.841 – Ejemplo de conexión incorrecta**

#### 7.2.3.1 Tráfico adicional

Durante las condiciones de ausencia de averías, es posible utilizar los canales de protección para transportar tráfico suplementario. Este tráfico suplementario, al que se hace referencia como tráfico adicional, tiene una prioridad menor que el tráfico normal por los canales de servicio y carece de medios de protección. El tráfico adicional se establece provisionando los nodos de adición y supresión de tráfico. Los nodos intermedios a lo largo del anillo se provisionan de tal manera que los canales de protección AU-3/4 que transportan tráfico adicional pasen por el nodo. (Los canales de protección que no transportan tráfico adicional se terminan en los nodos intermedios.) Los nodos que insertan, retiran o transfieren al tráfico adicional indican su presencia en esos tramos insertando el código de tráfico adicional en el byte K2. Se señala que el tráfico no protegido y no desplazable con prioridad no se considera tráfico adicional y, por tal motivo, no fijará el código ET (Extra Traffic, *tráfico adicional*).

Cuando sea necesario puentear el tráfico normal a los canales de protección (debido a un fallo o a una instrucción iniciada externamente), el tráfico adicional se desplaza con prioridad y se elimina en los tramos cuyos canales de protección se necesiten para la conmutación de protección. Los circuitos de tráfico adicional cuyo origen es eliminado por este desplazamiento con prioridad serán silenciados con AU-AIS. Cuando los nodos afectados vuelvan al estado de reposo, se restablece el tráfico adicional.

#### 7.2.3.2 Silenciamiento para evitar tráfico mal conectado

Para realizar una conmutación 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 normal 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 tráfico normal 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 7-8, un corte en ambos tramos entre los nodos A y F y entre los nodos A y B (que aisle 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 conmutación en caso de una petición de puenteo, y mediante el examen del tráfico que se verá afectado por la conmutación. Los nodos de conmutación pueden determinarse a partir de las direcciones de nodos en los bytes K1 y K2. Dichos nodos determinan el tráfico afectado por la conmutación de protección a partir de la información contenida en sus mapas de anillo y a partir de las identificaciones de los nodos de conmutación. Las posibles conexiones erróneas serán silenciadas insertando la AU-AIS apropiada en los intervalos de tiempo en que podría haber tráfico mal conectado. De manera específica, el tráfico originado o retirado en el nodo o los nodos aislados del anillo por el fallo deberá ser silenciado. Para los anillos que funcionan en un nivel AU-4, este silenciamiento se produce en los nodos de conmutación. El silenciamiento a nivel AU del tráfico normal o adicional se produce dentro o fuera de los canales de protección (es decir, el tráfico normal que entra o sale de los canales de servicio nunca se silencia). 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 conmutación 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) un mapa de anillo que contenga la información relativa al orden en que los nodos aparecen en el anillo;

2) un mapa de interconexión que contenga las asignaciones de intervalos de tiempo AU-4 para el tráfico que termina en ese nodo y lo atraviesa directamente;

3) una tabla de silenciamiento que contenga, 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.

Un MS SPRING (protocolo SPRING de MS) puede, facultativamente, soportar tráfico unidireccional. El tráfico unidireccional puede ser de uno de los siguientes tipos:

– una conexión dirigida simple originada en un nodo y terminada en otro nodo;

– un circuito retirado de manera múltiple (al modo de la función extracción y continuación utilizada en el interfuncionamiento de anillos [véase la Recomendación G.842]);

– un circuito originado de manera múltiple (al modo de la inversión de sentido del sentido de extracción y continuación de un circuito de interfuncionamiento de anillos).

En caso de fallo de un nodo, el silenciamiento efectuado para estos circuitos se basa solamente en lo siguiente:

– (para una conexión dirigida simple) el fallo del nodo de origen o el fallo del nodo de destino;

– (para un circuito retirado de manera múltiple) el fallo del nodo de origen o el fallo del nodo de la última extracción;

– (para un circuito originado de manera múltiple) el fallo del primer nodo de origen o el fallo del nodo de destino.

Para evitar una conexión errónea de tráfico adicional, las operaciones de puenteo o conmutación no se realizan sino hasta que los nodos de conmutación vean que se elimina el código de tráfico adicional de los tramos requeridos para la conmutación de protección.

Un nodo que desplaza con prioridad al tráfico adicional deberá silenciar los canales de tráfico adicional, que son desplazados de la siguiente manera:

– para un nodo que realiza una conmutación de tramo que desplaza con prioridad al tráfico adicional en ese tramo, el tráfico adicional es silenciado insertando AU-AIS en los canales de tráfico adicional de ese tramo que son retirados en ese nodo (es decir, en el lado de baja velocidad), e insertando AU-AIS en los canales de tráfico adicional de ese tramo que atraviesan el nodo (es decir, en el lado de alta velocidad), en tanto en cuanto no se requieran esos canales de protección para una conmutación de protección;

– para un nodo que realiza una conmutación de anillo, el tráfico adicional es silenciado insertando AU-AIS en los canales de tráfico adicional que son retirados en ese nodo (es decir, en el lado de baja velocidad);
– para un nodo que pasa a transferencia total, el tráfico adicional es silenciado insertando AU-AIS en los canales de tráfico adicional que se retiran en ese nodo (es decir, en el lado de baja velocidad).

#### 7.2.3.3 Acceso de contenedor virtual de orden inferior

Algunos nodos del anillo, a los que se hace referencia como nodos de acceso de contenedor virtual de orden inferior, pueden ser capaces de insertar, retirar o interconectar contenedores virtuales de orden inferior de las unidades administrativas (AU). Cuando múltiples nodos del anillo añaden VC de LO o interconectan VC de LO entre las AU, la cabida útil de una AU determinada puede tener nodos de origen múltiples o ser retirada entre nodos múltiples. A tales AU se hace referencia en esta Recomendación diciendo que son AU de VC accedidos de LO. El acceso de VC de LO queda en estudio.

### 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, *operations system*) 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, peticiones de puenteo recibidas e información sobre la situación de peticiones de puenteo recibidas. 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, *no request*) se transmite cuando no es necesario utilizar los canales de protección.

#### 7.2.4.1 Instrucciones iniciadas externamente

Las instrucciones iniciales externamente son iniciadas en un NE por el OS o el operador. La instrucción iniciada externamente puede ser transmitida al NE apropiado mediante los bytes de APS o la RGT 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.

**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.

**exclusión de los canales de servicio - conmutación de anillo**: Esta instrucción impide que el tráfico normal de los canales de servicio del tramo direccionado 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 normal 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.

**exclusión de los canales de servicio - conmutación de tramo**: Esta instrucción impide que el tráfico normal de los canales de servicio del tramo direccionado accedan a los canales de protección para una conmutación de tramo. Si ya hay tráfico normal 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.

**exclusión de protección - todos los tramos**: Esta instrucción impide la conmutación de protección en todo el anillo. Si hay tráfico normal por los canales de protección de cualquier tramo, esta instrucción hace que dicho tráfico se conmute de nuevo a los canales de servicio, independientemente de la condición de los canales de servicio. 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:

**Exclusión de protección - tramo (LP-S*, lockout of protection - span*)**: Esta instrucción impide la utilización del tramo para cualquier actividad de protección e impide la utilización de conmutaciones de anillo en cualquier punto del anillo. Si existen conmutaciones de anillo en el anillo, esta instrucción hace que se retiren las mismas. Si hay una conmutación de tramo para este tramo, es retirada. 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.

**Conmutación forzada a protección - anillo (FS-R*, forced switch to protection - ring*)**: Esta instrucción efectúa la conmutación de anillo de tráfico normal 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.

**Conmutación forzada a protección - tramo (FS-S*, forced switch to protection - span*)**: Esta instrucción conmuta el tráfico normal 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.

**Conmutación manual a protección - anillo (MS-R*, manual switch to protection - ring*)**: Esta instrucción efectúa la conmutación de anillo del tráfico normal 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).

**Conmutación manual a protección - tramo (MS-S, *manual switch to protection - span*)**: Esta instrucción conmuta el tráfico normal de los canales de servicio 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).

**Ejercicio - anillo (EXER-R, *exercise - ring*)**: 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 normal no es afectado.

**Ejercicio - tramo (EXER-S, *exercise - span*)**: 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 normal 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 de 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, *signal failure*), degradación de señal (SD, *signal degrade*), invertir petición (RR, *reverse request*) y espera al restablecimiento (WTR, *wait to restore*). 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 normal afectado por defectos, mientras que la petición de puenteo SD se utiliza para proteger contra degradaciones de la señal debidas a errores en los bits. 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 instrucciones iniciadas externamente.

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

**Fallo de señal - tramo (SF-S, *signal fail - span*)**: El SF se define como la presencia de la condición TSFprot generada por la función de terminación de camino de MS definida 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

conmutando a los canales de protección del mismo tramo. La petición de puenteo SF-S se utiliza para iniciar la conmutación de tramo para un SF en los canales de servicio de un anillo de cuatro fibras.

**Fallo de señal - anillo (SF-R, *signal fail - ring*)**: Para los anillos de dos fibras, todos los SF (definidos anteriormente para la conmutación de tramo) son protegidos utilizando la conmutación de anillo. Para los anillos de cuatro fibras, la conmutación de anillo se utiliza únicamente si el tráfico no puede restablecerse mediante la conmutación 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 conmutación de anillo para fallos de señal. Para un anillo de cuatro fibras, el SF-R resulta de la combinación de LOW-S y un fallo de línea de servicio detectado o recibido en el mismo tramo o la siguiente combinación de condiciones detectadas o recibidas en las líneas de servicio y protección:

– fallo de línea de servicio y fallo de línea de protección en el mismo tramo;

– fallo de línea de servicio y línea de protección degradada en el mismo tramo;

– línea de servicio degradada y fallo de línea de protección en el mismo tramo.

**Fallo de señal - protección (SF-P, *signal fail - protection*)**: Esta instrucción se utiliza para indicar a un nodo adyacente que los canales de protección están en un estado de fallo de señal (como se definió anteriormente para conmutación de tramo). 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.

**Degradación de señal - tramo (SD-S, *signal degrade - span*)**: La degradación de señal se define como la presencia de la condición TSD generada por la función de terminación de camino de MS definida 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 normal a los canales de protección en el mismo tramo en el que está situado el fallo.

**Degradación de señal - anillo (SD-R, *signal degrade – ring*)**: Para los anillos de dos fibras, cualquier sección de multiplexación degradada es protegida utilizando la conmutación de anillo. (La degradación se define más arriba: véase degradación de señal-tramo.) Para los anillos de cuatro fibras, la SD-R resulta de la combinación de LOW-S y una degradación de línea de servicio detectada o recibida en el mismo tramo o la combinación de condiciones de degradación de señal detectadas o recibidas en las líneas de servicio y protección en el mismo tramo.

**Degradación de señal - protección (SD-P, *signal degrade - protection*)**: Esta instrucción se utiliza cuando un NE detecta una degradación en sus canales de protección, y no existen peticiones de conmutación 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.

**Invertir petición - tramo (RR-S, *reverse request - span*)**: 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.

**Invertir petición - anillo (RR-R, *reverse request - ring*)**: 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.

**Espera al restablecimiento (WTR)**: Esta instrucción es emitida cuando los canales de servicio 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 conmutación de protección

Se utilizarán dos bytes de APS, a saber K1 y K2, para la conmutación 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.

Los bytes de APS sólo serán aceptados como válidos cuando se reciban bytes idénticos en tres tramas consecutivas.

#### 7.2.5.1 Byte K1

Estos bits serán asignados conforme al cuadro 7-7. Los bits 1-4 del byte K1 transportan códigos de petición de puenteo, enumerados por orden de prioridad descendente en el cuadro 7-7. 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 7-7/G.841 – Funciones del byte K1**

| **Código de petición de puenteo (Bits 1-4)** | | **Identificación de nodo de destino (Bits 5-8)** |
|---|---|---|
| Bits 1234 | | 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). |
| 1111 | Exclusión de protección (tramo) LP-S o fallo de señal (protección) SF-P | |
| 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 | Degradación de señal (protección) SD-P | |
| 1001 | Degradación de señal (tramo) SD-S | |
| 1000 | Degradación 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 | Ausencia de 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 7-8.

**Cuadro 7-8/G.841 – Funciones del byte K2**

| Identificación de nodo de origen (Bits 1-4) | Largo/corto (Bit 5) | Situación (Bits 6-8) |
|---|---|---|
| La ID del nodo de origen se fija a la ID del propio nodo | Bit<br>5<br>0 código de trayecto corto (S)<br>1 código de trayecto largo (L) | Bit<br>678<br>111 MS-AIS<br>110 MS-RDI<br>101 Reservado para uso futuro<br>100 Reservado para uso futuro<br>011 Tráfico adicional por canales de protección<br>010 Puenteado y conmutado (Br&Sw)<br>001 Puenteado (Br)<br>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 subcláusula 7.2.6.1 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 subcláusula 7.2.6.2 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 7-9 ilustra el funcionamiento conceptual de un controlador de APS de anillo de protección compartida de sección de multiplexación.

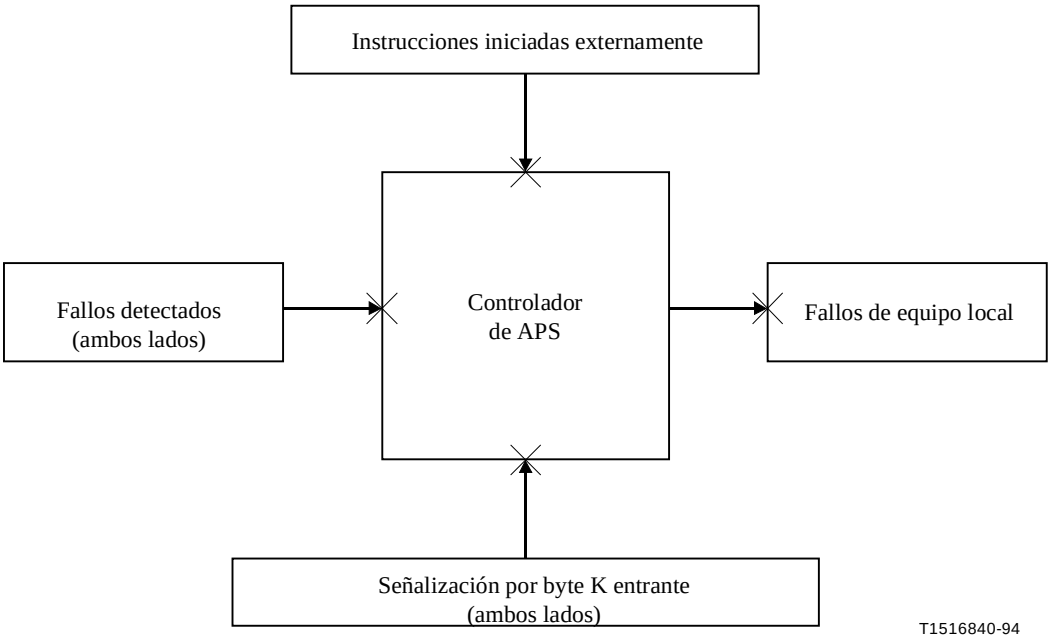



**Figura 7-9/G.841 – Controlador de APS de anillo de protección compartida de MS conceptual**

Se aplica el siguiente conjunto de reglas generales:

**Regla G #1** – VALIDACIÓN DE PETICIÓN DE PUENTEO (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.

**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.

**Regla G #1c**: Cuando un nodo de anillo de cuatro fibras está en una condición SF-R o SD-R, y no se puede señalizar la petición SF-R o SD-R porque no se permite que coexista con otras peticiones de APS de prioridad mayor en ese nodo, el nodo considerará la condición de la línea de protección detectada o recibida como una segunda entrada al controlador de APS.

En el cuadro 7-9 se indica la relación entre códigos de petición de puenteo, de situación de petición de puenteo e indicaciones de bytes K.

**Cuadro 7-9/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.

#### 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 o recibiendo ninguna petición de APS o situación de petición de puenteo y está recibiendo códigos de reposo o ET de ambos sentidos.

**Regla I #1** – BYTES K GENERADOS EN EL ESTADO DE REPOSO:

**Regla I #1a**: Los nodos que estén en el estado de reposo sin insertar, retirar o transferir tráfico adicional generarán los bytes K en ambos sentidos, tal como se indica en el cuadro 7-10.

**Cuadro 7-10/G.841 – Valores de los bytes K1 y K2 generados en el estado de reposo**

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

**Regla I #1b**: Los nodos que estén en el estado de reposo insertando, retirando o transfiriendo tráfico adicional generarán los bytes K que se muestran en el cuadro 7-10, con la salvedad de que los bits 6-8 del byte K2 transmitidos por cualquier tramo que contenga tráfico adicional deberán tener el valor 011 (código de tráfico adicional).

El nodo se comportará de conformidad con la regla I-S #3 hasta que tenga conocimiento del mapa del anillo. Queda en 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

Se entiende que un nodo que no está en el estado de reposo ni en el de transferencia se encuentra en el estado de conmutación. Se incluye aquí la situación de señalización por defecto, por ejemplo, arranque del nodo, cuando no haya un mapa de anillo disponible.

**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 7-11.

**Cuadro 7-11/G.841 – Valores de los bytes K1 y K2 originados por un nodo en el estado de conmutación**

| | | |
|---|---|---|
| K1 [1-4] | = | código (situación) 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 |

**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 (o situación de petición de puenteo) en el trayecto largo. Tanto la petición de puenteo como la situación de petición de puenteo tienen la misma prioridad (o una de ellas es invertir petición), y protegen el mismo tramo. Las excepciones se pueden producir cuando haya más de una petición de conmutación activa en el nodo. Las excepciones son como sigue:

– El caso de nodo aislado descrito en las reglas S #1c y S #1d.

– El caso de una petición de puenteo de tramo en cada lado del nodo, el nodo originará una petición de puenteo en cada trayecto corto, cuando los bits de situación indiquen el estado del puenteo y la conmutación para el tramo correspondiente.

– El caso de una petición de puenteo de anillo que desplaza con prioridad una petición de puenteo de tramo en un tramo adyacente como se describe en la regla S-S #2b.

– Los casos en que SF-P y SD-P coexisten con una conmutación de anillo en el mismo tramo. El cuadro 7-12 define la señalización para estos casos.

**Cuadro 7-12/G.841 – SD-P y SF-P coexistiendo con conmutaciones de anillo en el mismo tramo**

| Petición de anillo de prioridad mayor | Condiciones de trayecto corto | | Prioridad señalada en trayecto corto |
|---|---|---|---|
| | Servicio | Protección | |
| FS-R | eliminación, SD, o SF | SF | LP-S |
| FS-R | eliminación, SD, o SF | SD | SD-P |
| FS-R | eliminación, SD, o SF | LP-S o SD-P (byte K) | RR-S |
| SF-R(byte K) | eliminación | SF | LP-S |
| SF-R(byte K) | eliminación o SD | SD | SD-P |
| SD-R(byte K) | eliminación | SD | SD-P |
| MS-R o EXER-R | eliminación | SF | LP-S |
| MS-R o EXER-R | eliminación | SD | SD-P |
| MS-R o EXER-R | eliminación | LP-S o SD-P (byte K) | RR-S |

**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, se señalizará la petición de puenteo de trayecto corto en vez de las de invertir petición. 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 7-10 a)].

**Regla S #1d**: Cuando un nodo detecte una condición que requiera una conmutación de anillo o una instrucción iniciada externamente de conmutación de anillo aplicada a ese nodo, originará siempre, por el trayecto corto, una petición de puenteo de anillo de trayecto corto mientras la petición de anillo no sea desplazada por una petición de puenteo de anillo de prioridad mayor [véase la figura 7-10 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 en un lado y detecte una de las condiciones antes mencionadas en el otro, señalará la petición de puenteo asociada a esa condición [véase la figura 7-10 c)].

**Regla S #1e**: Un nodo en estado de conmutación insertará el código ET en los bits 6-8 del byte K2 en tramos que transporten tráfico adicional.

**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 PUENTEO 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:

– SD-P con cualquier conmutación de tramo;
– LP-S o SF-P con cualquier conmutación de tramo para otros tramos;
– SF-P o SD-P con cualquier conmutación de anillo en el mismo tramo;
– LP-S con SD-P;
– LP-S con LP-S;
– SD-P con SD-P;
– 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.

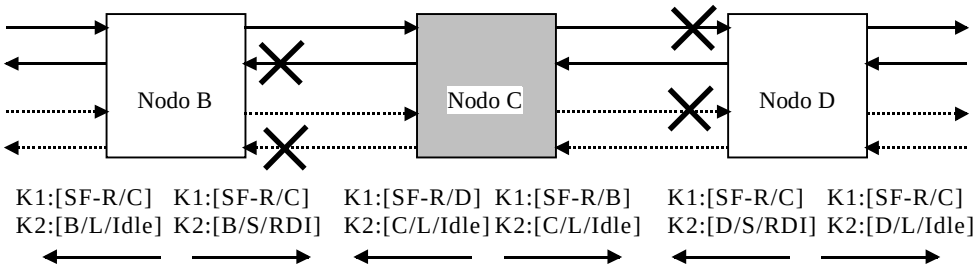
**Regla S #5** – PÉRDIDA DE PETICIÓN DE PUENTEO DE ANILLO: Si un nodo que efectúa un puenteo y conmutación de anillo ya no recibe una petición de puenteo de anillo válida en el trayecto largo, retirará su puenteo y conmutación de anillo y señalizará y actuará conforme a su entrada de máxima prioridad.

**Regla S #6** – PÉRDIDA DE PETICIÓN DE PUENTEO 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.

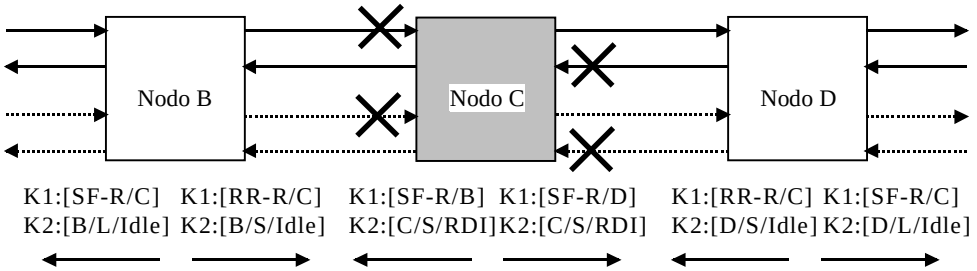
**Regla S #7** – TRÁFICO ADICIONAL: Cuando un nodo esté en el estado de conmutación no transferirá tráfico adicional, a menos de que esté en el estado de conmutación debido a un LP-S (fallo de señal-protección), o a una petición SD-P. Cuando un nodo esté en el estado de conmutación debido a una instrucción WTR para una conmutación de tramo, o a cualquier petición de tramo, salvo LP-S, SD-P o EXER-S, no originará ni terminará tráfico adicional por el trayecto corto de esa petición de puenteo. Cuando un nodo esté en el estado de conmutación debido a una instrucción WTR para una conmutación de anillo, o a cualquier petición de anillo, salvo EXER-R, no originará ni terminará tráfico adicional.

**Regla S #8** – TERMINACIÓN DE WTR: Cuando un nodo en el estado WTR retire su puenteo y conmutación antes de que expire la temporización de WTR, terminará inmediatamente la WTR y actuará en base a su entrada de prioridad mayor.

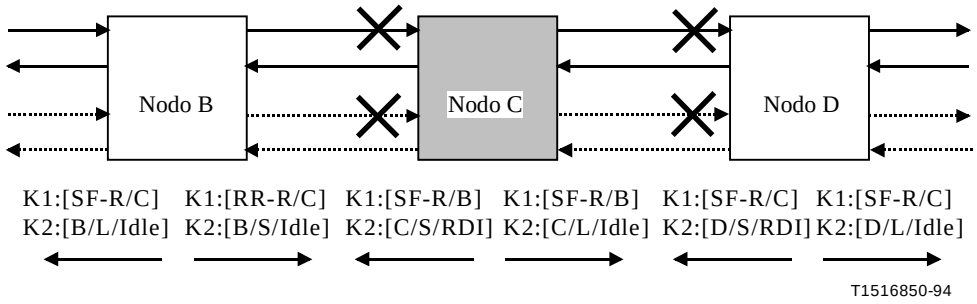
**Regla S #9** – Cuando un nodo en el estado conmutación reciba la instrucción externa LOW-R para el tramo afectado, retirará su puenteo y conmutación y señalizará ausencia de petición, SF-P o SD-P. Tras la recepción de ausencia de petición en combinación con el código de reposo o el código ET o situación de petición de puenteo procedente del tramo distante del tramo LOW-R, el nodo reinsertará el tráfico adicional que fue desplazado con prioridad en ese tramo.




**a) Se señalan cortes al nodo C**




**b) El nodo C detecta cortes**




**c) Se señala un corte en un lado al nodo C, que detecta un corte en el otro**

Canales de servicio

Canales de protección

Idle: Reposo

**Figura 7-10/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)**

### 7.2.6.1.3 Estado de transferencia

Un nodo está en el estado de transferencia cuando su petición de APS de prioridad mayor es una petición de puenteo o situación de petición de puenteo o no destinada a, ni originada por, él mismo. La transferencia puede ser unidireccional o bidireccional, dependiendo de su naturaleza. Hay tres tipos de transferencia: transferencia total unidireccional, transferencia total bidireccional, y de byte K (véase en la cláusula 3 la definición de las diferentes clases de transferencias).

**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. Un nodo en el estado de transferencia de bytes K emitirá el código ET en los bits 6-8 en tramos que transportan tráfico adicional. Un nodo de transferencia de bytes K que reciba el código tráfico adicional emitirá el código de reposo en el sentido opuesto si no existe tráfico adicional en el tramo opuesto. Un nodo en el estado de transferencia total unidireccional seguirá generando los bytes K generados previamente en el sentido opuesto, con la salvedad de que los bits 6-8 del byte K2 deberán reflejar el código de situación apropiado.

**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 de la condición de fallo de nodo. Véase la figura I.5.)

**Regla P #3** – TRÁFICO ADICIONAL: Un nodo en estado de transferencia total no deberá originar ni terminar tráfico adicional. Si un nodo está en el estado de transferencia de bytes K, puede originar, terminar y transferir tráfico adicional.

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

En la subcláusula 7.2.6.1 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 instrucción iniciada externamente o criterios de calidad de funcionamiento de equipo o sección de multiplexación detectados 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 o el tramo transporte tráfico adicional. 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. MS-RDI y MS-ASI terminan en los elementos de terminación de sección de multiplexación como se especifica en la Recomendación G.783. Un nodo deberá señalizar tráfico adicional en cualquier tramo que transporte tráfico adicional.

**Regla básica #4**: Las peticiones de APS en razón de un fallo detectado localmente, de una instrucción iniciada externamente o de bytes K recibidos desplazarán a las peticiones de APS en el orden de prioridades que se indica en el cuadro 7-7, a menos que las peticiones de puenteo estén autorizadas a coexistir. Las acciones resultantes de peticiones de puenteo entrantes tendrán prioridad con respecto a las acciones resultantes de 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 bytes K será provocada por un cambio de byte K válido, en cualquier sentido, del código de ausencia de 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 bytes K, de acuerdo con la regla I-P #1b.

**Regla I-P #1b**: Cualquiera que sea la situación de petición de puenteo de tramo o la petición de puenteo EXER-R, los nodos intermedios del trayecto largo irán hacia transferencia de bytes K. Las acciones efectuadas en un nodo intermedio tras recibir una petición de puenteo de anillo válida distinta de EXER-R son:

– para las NE sin tráfico adicional, cuando el nodo en estado de reposo reciba una petición de puenteo de anillo válida en cualquier sentido no destinada al propio nodo, pasará al estado de transferencia total bidireccional;

– para las NE con tráfico adicional, cuando el nodo en estado de reposo reciba una petición de puenteo de anillo válida en cualquier sentido no destinada al propio nodo, retirará el tráfico adicional bidireccionalmente, y pasará al estado de transferencia total unidireccional, en el sentido de la petición de puenteo solamente. Tras recibir los bytes K cruzados, el nodo pasará al estado de transferencia total bidireccional.

**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 de ausencia de petición en los bits 1-4 de K1 y códigos de indicación de reposo o ET 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. El tráfico adicional que hubiera sido desplazado con prioridad será reinsertado y se emitirá el código ET como se define en la regla I #1b.

#### 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 de ausencia de petición (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 conmutante 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 conmutado 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-S, EXER-R 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-S, EXER-R 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).

– El tráfico adicional se retirará inmediatamente de todos los tramos para una conmutación de anillo, o del tramo cuyos canales de protección se requieren para una conmutación de tramo.

– No se efectuará ningún puenteo o conmutación mientras se reciba el código ET en el tramo cuyos canales de protección son requeridos por ese puenteo y conmutación.

**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 o ET 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: Cuando expire el tiempo de una instrucción WTR o se elimine una instrucción iniciada externamente en un nodo, y el nodo reciba una instrucción de invertir petición procedente del tramo corto, el nodo retirará primero su conmutación y señalizará el código de ausencia de petición en los bits 1-4 del byte K1 y el código de puenteo en los bits 6-8 del byte K2. (Se señala que este paso puede ser ejecutado en transiciones del estado de conmutación al estado de transferencia.)

– Paso 2: Tras la recepción del código de ausencia de petición y de la indicación de que se ha retirado la conmutación, el nodo del extremo de cabecera retirará su puenteo y su conmutación y originará el código de 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 de reposo en ambos sentidos. El tráfico adicional que fue desplazado con prioridad será reinsertado y el código ET será emitido como se define en la regla I #1b. Se reinsertará un código LP-S debido a un fallo de señal-protección que fue desplazado con prioridad.

– Paso 4: Una vez que el extremo de cabecera detecte códigos de reposo o ET entrantes de ambos sentidos, volverá al estado de reposo. El tráfico adicional que fue desplazado con prioridad será reinsertado y el código ET será emitido como se define en la regla I #1b. Se reinsertará un código LP-S debido a un fallo de señal-protección que fue desplazado con prioridad.

– Se señala que hay casos en los que no hay que efectuar ninguna conmutación o puenteo 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 de ausencia de petición. Tras la recepción del código de ausencia de petición, el extremo de cabecera 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 de conmutación 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 de conmutación no conmutado ni puenteado 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** – Si un nodo de conmutación recibe de ambos sentidos los bytes de APS que él está originando, y no recibe ninguna otra petición de APS, pasará al estado de reposo. De no ser así, el nodo de conmutación señalizará de acuerdo con su entrada de prioridad mayor.

**Regla I-S #7** – Cuando un nodo reciba un código de 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 primero un conjunto de requisitos y objetivos con los que debe estar conforme cada nodo de anillo para poder efectuar una conmutación sin crear conexiones erróneas, y a continuación se indica el conjunto de reglas necesarias para coordinar una transición entre estados de conmutación.

##### 7.2.6.2.3.1 Mapa de anillo e información de tabla de silenciamiento

Cada nodo de un anillo mantendrá un mapa de anillo describiendo la conectividad del mismo, y una tabla de silenciamiento local indicando el origen y el destino de todas las AU-3/4 añadidas, retiradas y transferidas.

##### 7.2.6.2.3.2 Silenciamiento

El silenciamiento de una AU-3/4 se llevará a cabo en los nodos de conmutación insertando una AU-AIS.

El nodo de conmutación identificará, comparando las 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 de la tabla de silenciamiento, identificará las AU-3/4 que se añaden y se retiran en esos nodos y las silenciará bidireccionalmente.

##### 7.2.6.2.3.3 Reglas de transición

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 o 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 o 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 APS 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.

**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 APS 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 #1e**: Cuando un NE, que está ejecutando una petición EXER-R, reciba una petición de APS 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 destinada a él) para el mismo tramo, eliminará cualquier tráfico adicional. El nodo ejecutará a continuación la nueva petición de APS de anillo como se detalla en la regla I-S #1.

**Regla S-S #1f**: Cuando un NE, que está ejecutando una petición de EXER-S, reciba una petición de APS de tramo de prioridad mayor (en razón de un fallo detectado localmente, de una instrucción iniciada externamente, o de una petición de puenteo de anillo destinada a él) para el mismo tramo, con excepción de LP-S y SD-P, eliminará cualquier tráfico adicional del trayecto corto. A continuación señalizará la nueva petición de puenteo de tramo con el código de reposo en los bits 6-8 de K2 en el trayecto corto, y la nueva petición de puenteo de tramo en el trayecto largo. Si hay tráfico adicional en el trayecto largo, se señalizará el código ET en los bits 6-8 de K2. El nodo ejecutará a continuación la nueva petición de APS de tramo como se detalla en la regla I-S #1.

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

**Regla S-S #2a**: Cuando un NE que esté efectuando una conmutación de tramo reciba una petición de APS 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) destinada a él de prioridad mayor para el mismo tramo:

– retirará el puenteo de tramo y conmutará inmediatamente;

– efectuará la petición de APS 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 APS 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) destinada a él para su tramo adyacente de mayor prioridad que la conmutación de tramo que está efectuando, retirará la conmutación de tramo, señalará ausencia de petición en K1 y puenteado en K2 en el sentido de la petición de APS de tramo, y señalará la petición de anillo en K1 y reposo en K2 en el sentido de la petición de APS 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 ausencia de 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 ausencia de 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 ausencia de petición, el nodo originará ausencia de petición en K1 y reposo en K2 en ambos sentidos.

– Una petición de APS 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 APS 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 APS de anillo por trayecto largo destinada a otro nodo, el nodo señalizará de acuerdo con la regla S-P #1a o la regla S-P #1b, dependiendo de si se recibe o no la indicación de puenteado.

– Un estado de petición de APS de tramo destinado a otro nodo, el nodo señalizará de acuerdo con la regla S-P #1a o la regla S-P #1b, dependiendo de si se recibe o no la indicación de puenteado.

– Una petición de APS 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 ausencia de petición, el nodo originará ninguna petición en K1 y reposo en K2 en ambos sentidos.

– Una petición de APS 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 APS 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 esa petición.

– Una petición de puenteo de anillo por trayecto largo destinada a otro nodo, el nodo señalizará de acuerdo con la regla SP #1a o la regla SP #1b, dependiendo de si se recibe o no la indicación de puenteado.

– Un estado de petición de puenteo de tramo destinado a otro nodo, el nodo señalizará de acuerdo con la regla SP #1a o la regla SP #1b, dependiendo de si se recibe o no la indicación de puenteado.

– Una petición de APS 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 APS 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 APS 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 APS 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 APS de tramo.

**Regla S-S #2h**: Para un anillo de cuatro fibras: Si un nodo de conmutación de anillo recibe una petición de APS de prioridad mayor que la petición de APS de anillo que está efectuando, y no se permite que coexistan ambas peticiones, el nodo retirará la petición de prioridad menor y considerará la condición de su línea de protección detectada o recibida además de la petición de prioridad mayor. Si se permite que la petición detectada o recibida para la línea de protección coexista con la petición de APS de prioridad mayor, y si la petición de APS de prioridad mayor es para una conmutación de tramo en el tramo adyacente a la petición de canal de protección detectada o recibida, o si la petición de APS de prioridad mayor es para una conmutación de anillo para el mismo tramo que la petición de canal de protección detectada o recibida, el nodo responderá tanto a la petición de canal de protección como a la petición de APS de prioridad mayor en los tramos respectivos. Esta regla tiene precedencia con respecto a la regla S-S #1c y la regla S-S #2f.

**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, el nodo pasará a esperar 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**: Cuando un nodo que esté ejecutando una conmutación en respuesta a una petición de puenteo SD-S, SD-R, SF-S o SF-R entrante (no en razón de un fallo detectado localmente) reciba un código de espera al restablecimiento (caso de fallo unidireccional), enviará una instrucción de invertir petición por el trayecto corto y 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 SD-S o SF-S 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, incluyendo degradación o fallo de la línea de protección o LOW-S, se intentará la conmutación de anillo apropiada.

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

**Regla S-S #6** – Cuando un NE que esté recibiendo una petición de puenteo LP-S o que esté generando una petición de puenteo LP-S debido a un fallo de señal-protección, reciba una instrucción de puenteo de anillo iniciada externamente o detecte un fallo de la línea de servicio para el mismo tramo, asumirá la prioridad de la petición de puenteo de anillo.

#### 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 ausencia de petición en K1 y reposo en K2 en ambos sentidos.

**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:

– para los NE sin tráfico adicional, el nodo pasará al estado de transferencia total bidireccional;

– para los NE con tráfico adicional, el nodo retirará el tráfico adicional bidireccionalmente, y pasará al estado de transferencia total unidireccional en el sentido de la petición de puenteo solamente. Tras recibir los bytes K cruzados, el nodo pasará al estado de transferencia total bidireccional.

**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 ausencia de 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 bytes K. A continuación reinsertará cualquier tráfico adicional que hubiera sido desplazado con prioridad.

**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 bidireccional.

**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 bidireccional.

**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 bytes K. A continuación reinsertará cualquier tráfico adicional que hubiera sido reemplazado con prioridad.

**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;

4) la detección de un byte de APS asignado por ese NE.

**Regla S-P #2b**: La transición de un nodo de transferencia de bytes 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 un nodo que estaba en el estado de transferencia total está ahora generando una petición de puenteo de tramo debido a la regla S-P #2a, insertará una AU-AIS en los canales de protección en el tramo adyacente al tramo afectado, hasta que reciba una indicación de que se ha retirado la conmutación de anillo.

**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.

**Regla S-P #4**: Si un nodo en el estado de transferencia recibe de al menos un sentido un byte de APS que tiene él mismo ID de origen, emitirá reposo en ambos sentidos.

#### 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 bytes K a un estado de transferencia total, y viceversa.

Se aplican las siguientes reglas de transición:

**Regla P-P #1 –** TRANSICIÓN DE TRANSFERENCIA DE BYTES K A TRANSFERENCIA TOTAL:

– para los NE sin tráfico adicional, un nodo en el estado de transferencia de bytes K que reciba una petición de puenteo de anillo de trayecto distinta de EXER-R no destinada a él pasará al estado de transferencia total bidireccional;

– para los NE con tráfico adicional, el nodo eliminará el tráfico adicional bidireccionalmente, y pasará al estado de transferencia total unidireccional en el sentido de la petición de puenteo solamente. Tras recibir los bytes K cruzados, el nodo pasará al estado de transferencia total bidireccional.

**Regla P-P #2** – TRANSICIÓN DE TRANSFERENCIA TOTAL A TRANSFERENCIA DE BYTES K: Un nodo en el estado de transferencia total bidireccional que reciba un estado de petición de puenteo de tramo no destinado a él procedente de ambos sentidos pasará al estado de transferencia de bytes 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 unidireccional o bidireccional.

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 bidireccional 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 normal y tráfico adicional. En una aplicación de red, esto significa que los esquemas de tráfico normal 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 conmutación de protección bidireccional.

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. Un temporizador de tiempo de abstención arranca cuando se declara una condición de defecto y permanece en funcionamiento durante un periodo no reiniciable que puede fijarse de 0 a 10 s en pasos de 100 ms. Cuando expira el temporizador, se inicia la conmutación de protección si en ese punto está aún presente una condición de defecto. Se señala que no es necesario que una condición de defecto esté presente durante todo el periodo de tiempo de abstención, sólo importa el estado al expirar la temporización de abstención. Además, el defecto que da lugar a la puesta en marcha del temporizador de abstención no tiene porqué ser del mismo tipo que el existente al concluir el periodo de abstención.

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 protección unidireccional, conmutación de protección bidireccional 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 protección unidireccional 1 + 1 debe soportar conmutación reversiva, conmutación no reversiva o ambas. La conmutación de protección bidireccional reversiva 1:1 con tráfico adicional queda en estudio. (Se señala que una de las principales ventajas de la arquitectura 1:1 es su capacidad de llevar tráfico adicional.)

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.

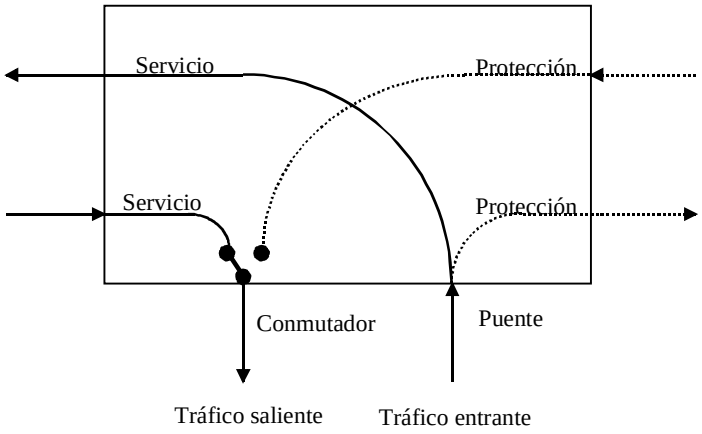
9) *Criterios para la iniciación de la conmutación* – Los criterios para la iniciación de la conmutación en caso de fallo de señal (SF) y/o degradación de señal (SD) deben estar en armonía con las definiciones utilizadas en la Recomendación G.783. Los criterios para la iniciación de la conmutación para la protección de camino de VC deben ser idénticos a los de protección de SNC/N correspondiente.

### 7.4.3 Arquitectura de aplicación

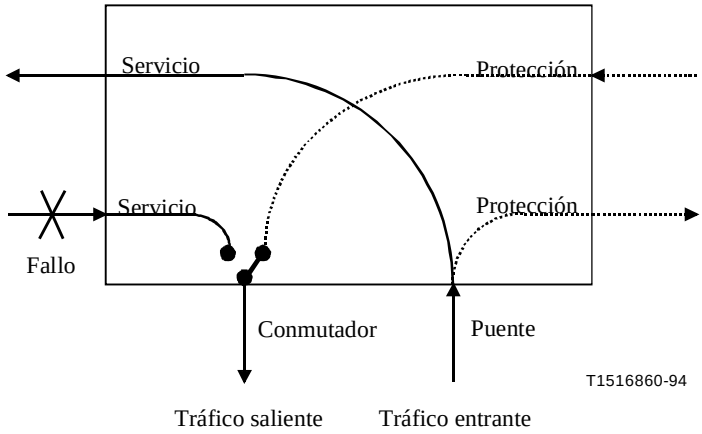
#### 7.4.3.1 Encaminamiento

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.

En la figura 7-11 a) se muestra un nodo en condiciones de funcionamiento normal. Se emplea un puente para transmitir simultáneamente señales de tráfico normal por los caminos de servicio y de protección. El receptor utiliza un conmutador para seleccionar la señal del camino de servicio en condiciones de funcionamiento normal. La figura 7-11 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.




**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 7-11/G.841 – Nodo que utiliza protección de camino o SNC 1 + 1**

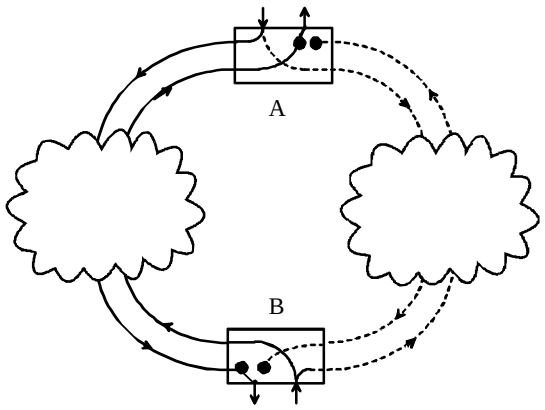
### 7.4.3.2 Conmutación de protección unidireccional 1 + 1

La figura 7-12 ilustra la conmutación de protección unidireccional para arquitectura 1 + 1. Es idéntica a la conmutación de protección bidireccional 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.

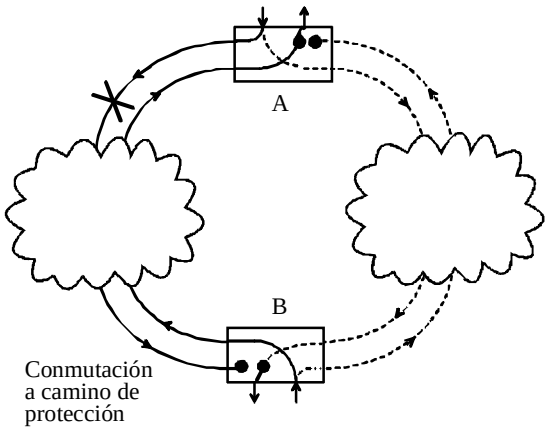
La figura 7-12 a) ilustra una red de protección de camino 1 + 1, con tráfico transmitido entre los nodos A y B. El tráfico insertado en el nodo A se transmite por diferentes caminos en dos direcciones al nodo B. En condiciones de funcionamiento normal en modos reversivos, el receptor del nodo B selecciona el tráfico del camino de servicio. El tráfico insertado en el nodo B 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 la señal del camino de protección. Si un fallo en un solo punto corta ambos sentidos de la transmisión, fallan ambos sentidos de la transmisión en el camino de servicio y ambos sentidos de la transmisión conmutan automáticamente al camino de protección.

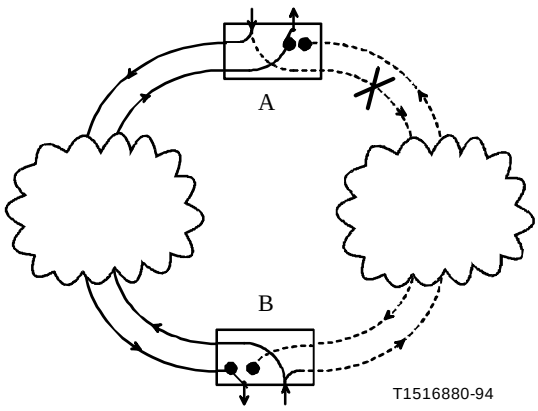
El tráfico puede ser restablecido cuando múltiples fallos afectan al tráfico solamente en uno de los caminos (el de servicio o el de protección). Si ambos caminos se ven afectados por determinados fallos, el tráfico no puede ser restablecido. El tráfico que termina en un nodo con fallos queda interrumpido,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




**a) Condiciones normales**




**b) Fallo unidireccional – Fibra 1**




**c) Fallo unidireccional – Fibra 2**

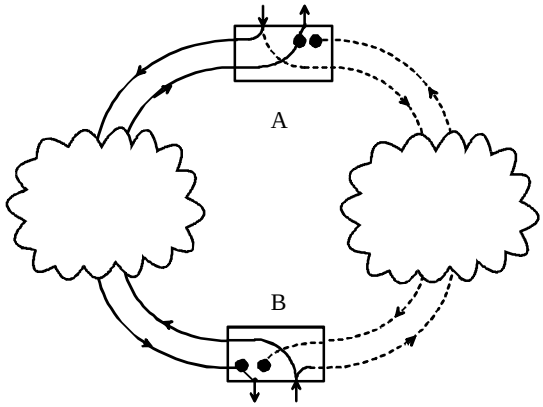
**Figura 7-12/G.841 – Red de protección de camino/SNC 1 + 1 de dos fibras con conmutación de extremo único**

#### 7.4.3.3 Conmutación de protección bidireccional 1 + 1

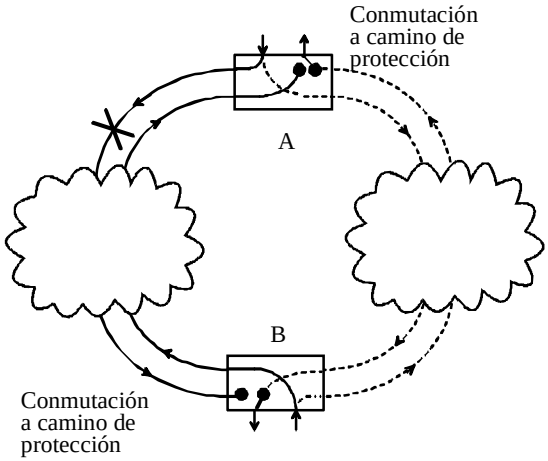
La figura 7-13 a) ilustra una red de protección de camino 1 + 1 con tráfico transmitido entre los nodos A y B. El tráfico insertado en el nodo A se transmite por diferentes caminos en dos direcciones al nodo B. En condiciones de funcionamiento normal en modo reversivo, el receptor del nodo B selecciona el tráfico del camino de servicio. El tráfico insertado en el nodo B 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 7-13 b), el conmutador del extremo de cola selecciona la señal del camino de protección. En caso de conmutación de protección bidireccional, se envía una indicación por medio del protocolo APS para forzar al sentido de la transmisión no afectada a que conmute también al camino de protección. Si un fallo en un solo punto corta ambos sentidos de la transmisión, fallan ambos sentidos de la transmisión en el camino de servicio y ambos sentidos de la transmisión conmutan automáticamente al camino de protección.

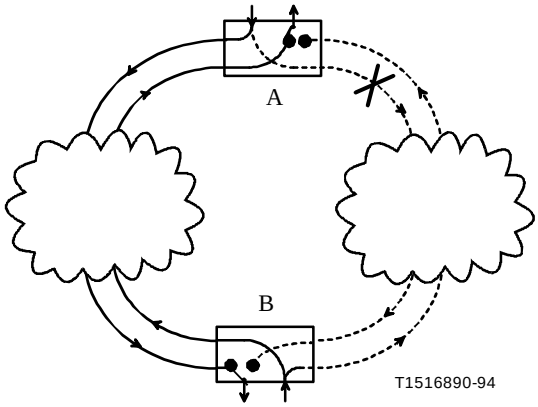
El tráfico puede ser restablecido cuando múltiples fallos afectan al tráfico solamente en uno de los caminos (el de servicio o el de protección). Si ambos caminos se ven afectados por determinados fallos, el tráfico no puede ser restablecido. El tráfico que termina en un nodo con fallos queda interrumpido,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




**a) Condiciones normales**




**b) Fallo unidireccional – Fibra 1**




**c) Fallo unidireccional – Fibra 2**

**Figura 7-13/G.841 – Red de protección de camino/SNC 1 + 1 de dos fibras con conmutación de extremo doble**

#### 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.

#### 7.4.4.1 Conmutación de protección unidireccional 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, ausencia de petición) del proceso de protección de camino de VC; o
3) una instrucción iniciada externamente (eliminación, exclusión, conmutación forzada, conmutación manual).

Para la arquitectura 1 + 1, todas las peticiones son locales. En el cuadro 7-13 se da la prioridad de las peticiones locales.

**Cuadro 7-13/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 | ↑ |
| Conmutación forzada | . |
| Fallo de señal | . |
| Degradación de señal | . |
| Conmutación manual | . |
| | . |
| | . |
| Espera al restablecimiento | ↓ |
| Ausencia de petición | Mínima |
| NOTA 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 protección unidireccional 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 conmutación forzada a protección.<br>NOTA 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 de servicio y un canal de protección. | |

#### 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.

**Eliminación**: Esta instrucción elimina todas las instrucciones de conmutación iniciadas externamente y enumerados a continuación y WTR en el nodo al que se dirigió la instrucción.

NOTA – En la definición de protección de camino de VC de la versión de 1995 de la Recomendación G.841, la instrucción de eliminación no eliminaba WTR. El equipo diseñado de acuerdo con esa definición de 1995 no eliminará WTR si se envía una instrucción de eliminación a ese equipo. No obstante, es posible conseguir un comportamiento similar mediante una secuencia seleccionada con cuidado de instrucciones externas (por ejemplo, conmutación manual seguida de eliminación).

**Exclusión de protección (LP, *lockout of protection*)**: Impide que el selector conmute al camino de VC de protección emitiendo una petición de exclusión de protección.

**Conmutación forzada a protección (FS-P, *forced switch to protection*)**: Conmuta el selector para tráfico normal 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).

**Conmutación forzada a servicio (FS-W, *forced switch to working*)**: Conmuta el selector para tráfico normal 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.

**Conmutación manual a protección (MS-P, *manual switch to protection*)**: Conmuta el selector para tráfico normal 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).

**Conmutación manual a servicio (MS-W, *manual switch to working*)**: Conmuta el selector para tráfico normal 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 de 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 la condición TSFprot generada por la función de terminación de camino de orden superior definida en la Recomendación G.783.

Para los HO VC, la instrucción iniciada automáticamente degradación de señal se define como la presencia de la condición TSD generada por la función de terminación de camino de orden inferior definida en la Recomendación G.783.

#### 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 la condición TSFprot generada por la función de terminación de camino de orden inferior definida en la Recomendación G.783.

Para los LO VC, la instrucción iniciada automáticamente degradación de señal se define como la presencia de la condición TSD generada por la función de terminación de camino de orden inferior definida en la Recomendación G.783.

### 7.4.4.2 Conmutación de protección bidireccional 1 + 1

Queda en estudio.

### 7.4.4.3 Conmutación de protección 1:1

Queda en estudio.

## 7.4.5 Protocolo de conmutación de protección

### 7.4.5.1 Conmutación de protección unidireccional 1 + 1

En esta arquitectura no se requiere canal de APS.

### 7.4.5.2 Conmutación de protección bidireccional 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.

El proceso de aceptación de APS queda en estudio.

### 7.4.5.3 Conmutación de protección 1:1

Queda en estudio.

## 7.4.6 Funcionamiento del algoritmo de protección

### 7.4.6.1 Conmutación de protección unidireccional 1 + 1

#### 7.4.6.1.1 Control del puenteo

En la arquitectura 1 + 1, el tráfico normal está permanentemente puenteado a los canales de servicio y protección.

#### 7.4.6.1.2 Control del selector

En la arquitectura 1 + 1 en funcionamiento de conmutación de protección unidireccional, 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 conmutación. (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 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 muchos caminos. 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.

#### 7.4.6.1.2.1 Modo reversivo

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

Para evitar el funcionamiento frecuente del selector debido a una avería intermitente, un camino de servicio que falle debe quedar libre de averías. Después de que el camino de servicio 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 para transportar la señal de tráfico normal. 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 condición SF o SD invalidará el WTR. Una vez completado el periodo de WTR se pasa a un estado de ausencia de petición. A continuación se produce la conmutación de la señal de tráfico normal 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 de ausencia de petición. Durante este estado no se produce conmutación.

### 7.4.6.2 Conmutación de protección bidireccional 1 + 1

Queda en estudio.

### 7.4.6.3 Conmutación de 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, *server signal fail*).

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 en el extremo transmisor de una conexión de subred se transmite de dos maneras diferentes por los trayectos de servicio y protección. 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 conmutación 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 unidireccional.

En el caso de conmutación de protección bidireccional, conmutación 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 conmutación y puenteo locales y distantes. Para ello quizás se requiera una técnica de subestratificación que queda en estudio.

## 8.2 Objetivos de red

Son aplicables los siguientes objetivos de red:

1) *Tiempo de conmutación* – 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 conmutación de protección excluye el tiempo de detección necesario para iniciar la conmutación de protección y el tiempo de abstención.

2) *Retardo de transmisión* – La conmutación protección unidireccional 1 + 1 no requiere transmisión de señalización APS, por lo que no están presentes retardos de transmisión de señalización.

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. Un temporizador de tiempo de abstención arranca cuando se declara una condición de defecto y permanece en funcionamiento durante un periodo no reiniciable que puede fijarse de 0 a 10 s en pasos de 100 ms. Cuando expira el temporizador, se inicia la conmutación de protección si en ese punto está aún presente una condición de defecto. Se señala que no es necesario que una condición de defecto esté presente durante todo el periodo de tiempo de abstención, sólo importa el estado al expirar la temporización de abstención. Además, el defecto que da lugar a la puesta en marcha del temporizador de abstención no tiene porqué ser del mismo tipo que el existente al concluir el periodo de abstención.

4) *Alcance de la protección* – La protección de LO/HO SNC restablecerá todo el tráfico LO/HO SNC protegido (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 protección unidireccional. Otras arquitecturas quedan en 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 protección unidireccional 1 + 1 debe soportar conmutación reversiva, conmutación no reversiva o ambas. La conmutación de protección bidireccional 1:1 con tráfico adicional queda en estudio. (Se señala que una de las principales ventajas de la arquitectura 1:1 es su capacidad de llevar tráfico adicional.)

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

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.

En la figura 7-11 a) se muestra un nodo 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 señal de la SNC de servicio en condiciones de funcionamiento normales en modo reversivo. La figura 7-11 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 automáticamente a la SNC de protección.

### 8.3.2 Conmutación de protección unidireccional 1 + 1

La figura 7-12 a) ilustra la protección de SNC con tráfico transmitido entre los nodos A y B. El tráfico insertado en el nodo A se transmite por diferentes SNC en direcciones separadas al nodo B (por ejemplo, una SNC de servicio y una SNC de protección). En condiciones normales de funcionamiento en modo reversivo, el receptor del nodo B selecciona la señal de tráfico en la SNC de servicio. Cuando hay un fallo en la SNC de servicio, como se muestra en la figura 7-12 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 7-12 c), el receptor no necesitará conmutar y continuará detectando el tráfico de la SNC de servicio.

### 8.3.3 Otras arquitecturas

La conmutación de protección bidireccional reversiva 1:1 con tráfico adicional queda en estudio.

## 8.4 Criterios para la iniciación de la conmutación

### 8.4.1 Conmutación de protección unidireccional 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, ausencia de petición) del proceso de protección de SNC; o
3) una instrucción iniciada externamente (eliminación, 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.

**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 | ↑ |
| Conmutación forzada | . |
| Fallo de señal | . |
| Degradación de señal | . |
| Conmutación manual | . |
| | . |
| | . |
| Espera al restablecimiento | ↓ |
| Ausencia de petición | Mínima |

NOTA 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 protección unidireccional 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.

NOTA 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.

#### 8.4.1.1 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.

**Eliminación**: Esta instrucción elimina todas las instrucciones de conmutación iniciadas externamente y enumeradas a continuación y WTR en el nodo al que se dirigió la instrucción.

NOTA – En la definición de protección de SNC de la versión de 1995 de la Recomendación G.841, la instrucción de eliminación no eliminaba WTR. El equipo diseñado de acuerdo con esa definición de 1995 no eliminará WTR si se envía una instrucción de eliminación a ese equipo. No obstante, es posible conseguir un comportamiento similar mediante una secuencia seleccionada con cuidado de instrucciones externas (por ejemplo, conmutación manual seguida de eliminación).

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

**Conmutación forzada a protección (FS-P)**: Conmuta 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 conmutación de prioridad igual o mayor).

**Conmutación forzada a servicio (FS-W)**: Conmuta 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 conmutación 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 conmutación 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.

**Conmutación manual para protección (MS-P)**: Conmuta 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 conmutación de prioridad igual o mayor).

**Conmutación manual a servicio (MS-W)**: Conmuta 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 conmutación de prioridad igual o mayor).

NOTA – La instrucción MS-W es unívoca solamente en sistemas no reversivos 1 + 1 ya que la instrucción de eliminación produciría el mismo resultado en un sistema reversivo. Puesto que la conmutación 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.

#### 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:

– para SNC/I, la condición SSF generada por el servidor en la función de adaptación de trayecto de orden superior (por ejemplo, adaptación MS/Sn definida en la Recomendación G.783);

– para SNC/N, la condición TSFprot generada por la función de terminación de trayecto de orden superior definida en la Recomendación G.783.

Para los HO VC que utilizan SNC/N, la instrucción iniciada automáticamente degradación de señal se define como la presencia de la condición TSD generada por la función de terminación de trayecto de orden superior definida en la Recomendación G.783.

##### 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:

– para SNC/I, la condición SSF generada por el servidor en la función de adaptación de trayecto de orden inferior (por ejemplo, adaptación Sn/Sm definida en la Recomendación G.783);

– para SNC/N, la condición TSFprot generada por la función de terminación de trayecto de orden inferior definida en la Recomendación G.783.

Para los LO VC que utilizan SNC/N, la instrucción iniciada automáticamente degradación de señal se define como la presencia de la condición TSD generada por la función de terminación de trayecto de orden inferior definida en la Recomendación G.783.

### 8.4.2 Otras arquitecturas

Queda en estudio.

## 8.5 Protocolo de conmutación de protección

### 8.5.1 Conmutación de protección unidireccional 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 conmutación de protección unidireccional 1 + 1

#### 8.6.1.1 Control del puente

En la arquitectura 1 + 1, la señal de tráfico normal está permanentemente puenteada a servicio y protección.

#### 8.6.1.2 Control del selector

En la arquitectura 1 + 1 en funcionamiento de conmutación de protección unidireccional, 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 la señal de tráfico normal, 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 de servicio que falla cumpla este criterio (y sin que estén presentes otras instrucciones iniciadas externamente), transcurrirá un periodo de tiempo fijo antes de que se restablezca la señal de tráfico normal a esa conexión de subred. 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 de ausencia de 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 de ausencia de petición. Durante este estado no se produce conmutación.

### 8.6.2 Otras arquitecturas

Queda en estudio.

ANEXO A

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

### 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 transoceánic" 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. Aunque este anexo se ha elaborado para satisfacer las necesidades de la aplicación transoceánica, las modificaciones de protocolo introducidas en él se pueden utilizar para atender las necesidades de otros tramos de alto retardo dentro de un anillo de protección compartida de MS, por ejemplo, los que se transmiten por sistemas de satélite.

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 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 ms, 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 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.

## 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:

**Conmutación forzada a protección-anillo (FS-R, *forced switch to protection - ring*)**: Esta instrucción efectúa la conmutación de anillo de señales de tráfico normal 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 normal 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.

**Conmutación manual a protección-anillo (MS-R, *manual switch to protection - ring*)**: Para aplicaciones transoceánicas, también es aplicable aquí lo descrito en relación con la FS-R.

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

**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 normal 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.

## 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 añadido/retirado se ve afectado por el fallo. La determinación de tráfico afectado se efectúa examinando las peticiones de puenteo de K1 (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/retirado dirigido hacia ese fallo). Sólo las AU-4 afluentes afectadas por el fallo son puenteadas y conmutadas, utilizando las mismas reglas descritas en esta Recomendación. 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.
2) Cuando un nodo conmutador de anillo reciba la nueva petición de puenteo de anillo con un código de situación "reposo", mantendrá:
   a) el puenteo y la conmutación (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 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", 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 conmutado" 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 conmutado", cambiará el código de situación a "puenteado y conmutado" para ambos lados, si el nodo estaba enviando "puenteado".

**Regla S #4a**: Para las conmutaciones coexistentes FS-R con FS-R y las conmutaciones 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 conmutación de anillo utilizada para sistemas transoceánicos no requiere la puesta en bucle del tráfico en nodos conmutantes. 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 conmutaciones 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 servicio 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 7-10, 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 servicio y de protección, señalizará el fallo detectado en ambos trayectos, corto y largo [véase la figura 7-10, 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 conmutación que origina la petición de puenteo SF-R continuará señalizando su petición de puenteo, retirará su puenteo y conmutación 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 conmutación de anillo reciba una petición de puenteo de anillo para un tramo no adyacente de mayor prioridad que la conmutación de anillo que está ejecutando, ya sea:

1) mantendrá los puenteos y conmutaciones 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 conmutaciones 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 conmutación 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 conmutaciones 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 conmutaciones 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.

**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;

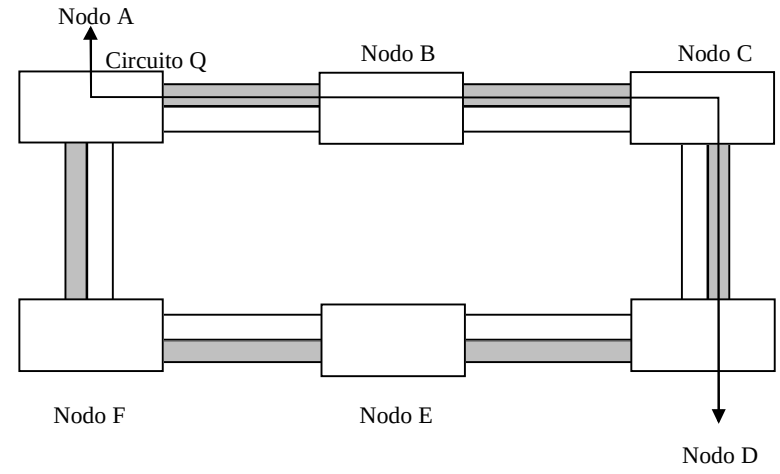
2) la detección de un fallo de prioridad igual o superior;

3) la recepción de una petición de puenteo de prioridad igual o superior destinada a ese NE;

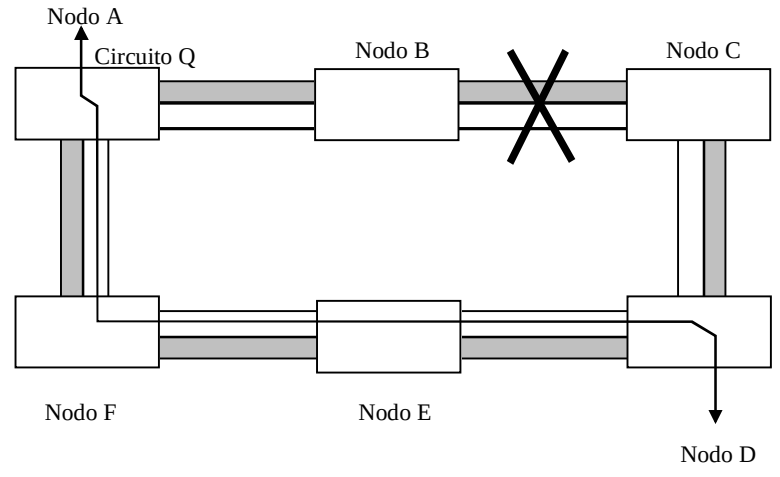
4) la detección de una condición SF-R (incluso de prioridad inferior); o

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.




**a) Estado normal**




**b) Estado de fallo**

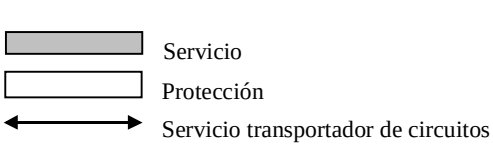



**Figura A.1/G.841 – Ejemplo de encaminamiento de circuitos en estado de fallo para una comunicación de circuito (aplicación transocenánica)**

ANEXO B

**Protocolo, instrucciones y funcionamiento de protección 1 + 1 optimizado de sección de multiplexación (MSP)**

## B.1 Conmutación optimizada bidireccional 1 + 1 para una red que utiliza predominantemente conmutación bidireccional 1 + 1

Este algoritmo utiliza las secciones de servicio 1 y 2 para realizar conmutación de protección no reversiva 1 + 1 de alta velocidad. En otras palabras, se impide la acción reversiva conmutando entre secciones de servicio.

Los bytes K1 y K2 (b1-b5) se intercambian para completar la conmutación. Como el puente es permanente (véase la figura B.1), el tráfico está siempre puenteado a la sección de servicio 1 y a la sección de servicio 2. El byte K2 indica el número de la sección que transporta tráfico cuando la conmutación no está activa. Ésta se denominará sección primaria. La otra sección de servicio, denominada sección secundaria, proporciona protección para la sección primaria. El intercambio de K1/K2 para controlar esta protección se produce en la sección secundaria. El número de sección en el byte K2 se cambiará después que se ha eliminado una conmutación. La eliminación de la conmutación se completa cuando los conmutadores de extremo recepción seleccionan la otra sección de servicio como primaria y no reciben ninguna petición.

En la conmutación optimizada bidireccional 1 + 1, las secciones 1 y 2 son iguales a secciones de servicio. Los bytes K1/K2 son recibidos por la sección secundaria. Estos bytes no siempre tienen que ser recibidos por la sección primaria, pero en general se debe enviar K1/K2 por ambas secciones para proporcionar operaciones de eliminación satisfactorias y permitir la recuperación de la condición de falta de concordancia del canal primario (véase B.1.5).

En el funcionamiento bidireccional 1 + 1 optimizado para una red que utiliza predominantemente la conmutación bidireccional 1 + 1, el selector está en la sección primaria cuando no hay una petición de conmutación. Todas las peticiones de conmutación son para conmutar de la sección primaria a la sección secundaria. Cuando una petición de conmutación se elimina normalmente, el tráfico se mantiene por la sección a la cual se conmutó convirtiéndose esa sección en sección primaria.

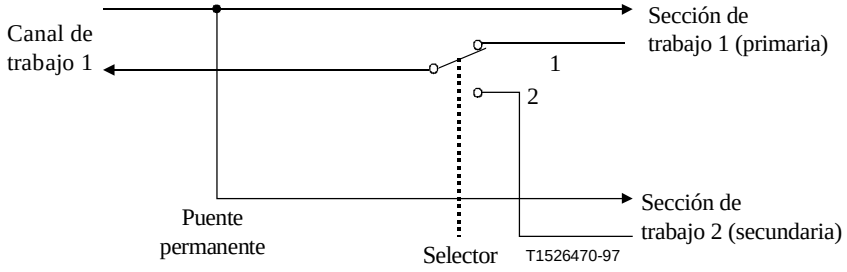



**Figura B.1/G.841 – Conmutación MSP – Conmutación bidireccional 1 + 1 optimizada (mostrada en posición liberada con la sección de servicio 1 como sección primaria)**

### B.1.1 Exclusión

En la conmutación optimizada bidireccional 1 + 1, la exclusión se considera como una petición local que no se señaliza a través de los bytes K. El efecto de la exclusión es congelar la posición del selector y los bytes K transmitidos hasta que se elimina la petición de exclusión. Cuando esta petición se libera, el selector y los bytes K transmitidos se fijarán aplicando cualquier condición de la sección que haya cambiado y los bytes entrantes al estado anterior.

### B.1.2 Fallo de sección secundaria

Se considera que hay un fallo en la sección secundaria siempre que esté en condición SF o SD. Como una opción, se puede considerar también que la sección secundaria ha fallado cuando se recibe MS-RDI para la sección secundaria.

No se emitirá ninguna petición de conmutación ni acuse de recibo cuando falle la sección secundaria. En este caso, el extremo cercano siempre indicará ausencia de petición en el byte K1 y el selector elegirá servicio de la sección primaria. Además, si la sección secundaria falla mientras una petición de conmutación está activa y no excluida, la petición de conmutación será abandonada: es decir, el selector volverá a la sección primaria y no se enviará ninguna petición en el byte K1.

### B.1.3 Codificación de los bytes K1/K2

El byte K1 indica una petición de conmutación.

Los bits 1-4 indican el tipo de petición, indicada en el cuadro B.1. Una petición puede ser:

1) Una condición (SF o SD) asociada con la condición primaria. No se indican condiciones para la sección secundaria.
2) Un estado (en espera al restablecimiento, ausencia de petición, invertir petición) de la función MSP. En espera al restablecimiento e invertir petición indican siempre la sección primaria. Ausencia de petición indica siempre la señal nula.
3) Una petición externa (conmutación forzada) para conmutar de la línea primaria a la secundaria.

**Cuadro B.1/G.841 – Tipos de petición**

| Bits | Condición, estado o petición externa | Orden |
|---|---|---|
| 1234 | | |
| 1111 | No utilizado (nota 1) | – |
| 1110 | Conmutación forzada | Más alto |
| 1101 | No utilizado (nota 1) | ↑ |
| 1100 | Fallo de señal | . |
| 1011 | No utilizado (nota 1) | . |
| 1010 | Degradación de señal | . |
| 1001 | No utilizado (nota 1) | . |
| 1000 | No utilizado (nota 1) | . |
| 0111 | No utilizado (nota 1) | . |
| 0110 | En espera al restablecimiento | . |
| 0101 | No utilizado (nota 1) | . |
| 0100 | No utilizado (nota 1) | . |
| 0011 | No utilizado (nota 1) | . |
| 0010 | Invertir petición | . |
| 0001 | No utilizado (nota 1) | ↓ |
| 0000 | Ausencia de petición | Más bajo |

NOTA 1 – Cuando se reciba un código no utilizado, el equipo actuará como si estuviese aún recibiendo el código utilizado recibido más recientemente.

NOTA 2 – En el caso de degradación de señal (SD) en ambas secciones de servicio, no se producirá ninguna conmutación de protección. Según el orden en el tiempo de SD, los selectores pueden ser conmutados a la sección 1 o a la sección 2. En todo caso, no se producirá conmutación.

Los bits 5-8 indican el número de la sección que se ha de proteger con la conmutación. Ésta será la sección nula para ausencia de petición y la sección primaria para todas las demás peticiones.

**Cuadro B.2/G.841 – Número de canal K1**

| Número de canal | Petición de acción de conmutación |
|---|---|
| 0 | Ninguna sección de servicio (sólo ausencia de petición) |
| 1 | Sección de servicio 1<br>Indica una petición para conmutar fuera de la sección número 1 |
| 2 | Sección de servicio 2<br>Indica una petición para conmutar fuera de la sección número 2 |

### B.1.4 Codificación del byte K2

Para la conmutación bidireccional 1 + 1 optimizada para una red que utiliza predominantemente la conmutación bidireccional 1 + 1, el byte K2 enviado indicará la posición del selector en los bits 1-4:

a) Canal número 1 (0001) si la sección 1 está funcionando.

b) Canal número 2 (0010) si la sección 2 está funcionando.

**Cuadro B.3/G.841 – Número de canal K2**

| Número de canal | Indicación |
|---|---|
| 1 | La sección 1 es primaria |
| 2 | La sección 2 es primaria |

### B.1.5 Falta de concordancia de la sección primaria

En el caso en que el extremo cercano y el extremo lejano no concuerdan sobre cuál es la sección primaria (es decir, un extremo indica la sección 1 en el byte K2 y el otro indica la sección 2), el extremo que considera que la sección 2 es la primaria cambiará, de modo que la sección 1 sea primaria y fije su estado conforme a las condiciones de línea locales y los bytes K entrantes.

## B.2 Instrucciones de conmutación

**Conmutación forzada**

Transfiere el servicio a la sección secundaria, a menos que esté en efecto una exclusión local, una petición de prioridad igual o más alta, o haya fallado la sección secundaria. Puesto que la conmutación forzada tiene prioridad más alta que SF o SD, se indicará conmutación forzada como el motivo para conmutar a la sección secundaria, incluso si la sección primaria está en una condición SF o SD.

**Eliminación de conmutación forzada**

Si no está en efecto una exclusión y está activa una conmutación forzada, ésta será eliminada cambiando la indicación de línea primaria a la línea actualmente activa y cambiando la petición a ausencia de petición. Si conmutación forzada no está activa, la instrucción de eliminación de conmutación forzada no es válida.

## B.3 Operación de conmutación

El cuadro B.4 ilustra el funcionamiento de un sistema de conmutación de protección bidireccional 1 + 1 en caso de fallo de señal en la sección primaria cuando la sección 1 es primaria. El cuadro B.5 ilustra el funcionamiento de un sistema de conmutación de protección optimizado bidireccional 1 + 1 en el caso de conmutación forzada de la sección primaria a la secundaria cuando la sección 2 es primaria. Obsérvese que, para una instrucción de conmutación forzada, el estado de en espera al restablecimiento no es necesario para la eliminación.

**Cuadro B.4/G.841 – Ejemplo de conmutación bidireccional 1 + 1 optimizada para una red que utiliza predominantemente conmutación bidireccional 1 + 1 – SF en la sección de servicio 1**

| Condición de fallo o estado de controlador | Bytes APS | | | | Acción | |
|---|---|---|---|---|---|---|
| | C → A | | A → C | | | |
| | Byte K1 | Byte K2 | Byte K1 | Byte K2 | En C | En A |
| Tráfico sin condición de avería por el canal 1 | 0000 0000 | 0001 0000 | 0000 0000 | 0001 0000 | | |
| Fallo de señal en la sección 1 en el lado C | 1100 0001 | 0001 0000 | 0000 0000 | 0001 0000 | Detección de petición local.<br>Actualización de K1. | |
| | 1100 0001 | 0001 0000 | 0010 0001 | 0001 0000 | | Detección de petición distante.<br>Conmutación a canal 2.<br>Emisión de invertir petición. |
| | 1100 0001 | 0001 0000 | 0010 0001 | 0001 0000 | Detección de invertir petición.<br>Conmutación a canal 2. | |
| Eliminación de fallo de señal en la sección 1 en el lado C y comprobación de persistencia | 0110 0001 | 0001 0000 | 0010 0001 | 0001 0000 | Emisión de petición de en espera al restablecimiento. | |
| Expiración de espera al restablecimiento | 0000 0000 | 0010 0000 | 0010 0001 | 0001 0000 | Ningún envío de petición.<br>Actualización de K1, K2. | |
| Ninguna condición de avería. Tráfico por la sección 2 | 0000 0000 | 0010 0000 | 0000 0000 | 0010 0000 | | Ningún envío de petición.<br>Actualización de K1, K2. |

**Cuadro B.5/G.841 – Ejemplo de conmutación bidireccional optimizada 1 + 1 para una red que utiliza predominantemente conmutación bidireccional 1 + 1 – Conmutación forzada desde la sección de servicio 2**

| Condición de fallo o estado de controlador | Bytes APS | | | | Acción | |
|---|---|---|---|---|---|---|
| | C → A | | A → C | | | |
| | Byte K1 | Byte K2 | Byte K1 | Byte K2 | En C | En A |
| Tráfico sin condición de avería por el canal 2 | 0000 0000 | 0010 0000 | 0000 0000 | 0010 0000 | | |
| Conmutación forzada desde la sección 2 en el lado C | 1110 0010 | 0010 0000 | 0000 0000 | 0010 0000 | Detección de petición local.<br>Actualización de K1. | |
| | 1110 0010 | 0010 0000 | 0010 0010 | 0010 0000 | | Detección de petición distante.<br>Conmutación a canal 2.<br>Emisión de invertir petición. |
| | 1110 0010 | 0010 0000 | 0010 0010 | 0010 0000 | Detección de invertir petición.<br>Conmutación a canal 2 . | |
| Eliminación de conmutación forzada en el lado C | 0000 0000 | 0001 0000 | 0010 0010 | 0010 0000 | Ningún envío de petición.<br>Actualización de K1, K2. | |
| Ninguna conmutación activa. Tráfico por la sección 1 | 0000 0000 | 0001 0000 | 0000 0000 | 0001 0000 | | Ningún envío de petición.<br>Actualización de K1, K2. |

## APÉNDICE I

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

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 de conmutación (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 bytes 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 puenteo 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 de ausencia de petición (regla I-S #2). El nodo E, tras la recepción del código de ausencia de 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 de reposo por el trayecto corto, retira su puenteo y origina también el código de reposo. Todos los nodos vuelven a continuación en cascada al estado de reposo.

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

Véase la figura I.2.

Este ejemplo se refiere al 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 de conmutación (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 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 puenteo 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 puenteo 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 tendrán 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 de ausencia de petición (regla I-S #2). El nodo E, tras la recepción del código de ausencia de petición procedente del nodo F por el trayecto largo, retira su puenteo y conmutación y origina el código de reposo (regla I-S #2). El nodo F, tras la recepción del código de reposo por el trayecto largo, retira su puenteo y origina también el código de 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 se refiere al 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 de conmutación (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 tendrán 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 dan lugar a una RR-R cruzante por el trayecto corto entre los nodos E y F. Ambos extremos de cabeza pasan al periodo de WTR (debido a la eliminación 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 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 cruzante, los nodos E y F retiran su conmutación de anillo y envían códigos de ausencia de 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 de 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 de 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 conmutación 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 de conmutación (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 conmutación 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 conmutación. La señalización alcanza el estado estacionario.

En las aplicaciones transoceánicas, las actividades conmutadoras tendrán 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 se refiere al 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 suministrada.

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 de conmutación (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 conmutación de anillo y actualiza los bits 6-8 del byte K2 (regla I-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 conmutación 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 conmutadoras tendrán 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 la información que se le había suministrado, 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.

En el momento $T_3$, el nodo F se ha recuperado plenamente y señaliza 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 conmutación, 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-anillo unidireccional 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 servicio. La señalización sigue su curso como se muestra en la figura I.1, salvo que:

1) los nodos de conmutación pasan a ser los nodos C y D, en lugar de los 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 momento $T_2$, el nodo F detecta una condición SF procedente del nodo G en sus canales de servicio y protección. El nodo F pasa a ser un nodo de conmutación (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, pasa a ser también un nodo de conmutación (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 conmutación de tramo, actualiza los bits 6-8 del byte K2, y origina ausencia de petición en ambos sentidos (regla S-S #2c). El nodo C, al ver ausencia de petición y la conmutación retirada del nodo D, retira su puenteo y conmutación, 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 ausencia de petición. El nodo C ve, en su momento, 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 conmutación 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 puenteo 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 conmutación (regla I-S #1b, segundo punto) y actualizan los bits 6-8 del byte K2. Las señalización alcanza el estado estacionario.

En el momento $T_3$, se elimina la condición SF del nodo E al nodo F en los canales de servicio y protección. El nodo F pasa a en espera al restablecimiento (regla S-S #3a). El nodo G, al ver la petición de puenteo WTR procedente del nodo F, también pasa a en espera al 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 pasa a ser un nodo de conmutación [regla S-P #2a, punto 2] y señaliza de manera apropiada. El nodo C, al ver una petición de puenteo de tramo de prioridad superior destinada a él, pasa a ser también un nodo de conmutación [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 a la situación de la petición de puenteo de tramo procedente del nodo D. El nodo F retira su puenteo y conmutación (regla S #5), termina su señalización WTR y pasa a transferencia de bytes K (regla S #8). En forma similar, cuando el nodo G pierde su petición de puenteo de anillo de trayecto largo, retira su puenteo y conmutación (regla S #5), termina su señalización WTR y pasa a transferencia de bytes K. El nodo D, al ver un código puenteado en el trayecto corto procedente del nodo C, efectúa un puenteo y conmutación de tramo y actualiza los bits 6-8 del byte K2 (regla I-S #1b). El nodo C, al ver un código puenteado y

conmutado procedente del nodo D, completa el proceso efectuando una conmutación de tramo y actualizando los bits 6-8 del byte K2 (regla I-S #1b). Los nodos A, E y B intermedios pasan entonces de transferencia total a transferencia de bytes K. La señalización alcanza el mismo estado estacionario que en el momento $T_1$.

En el momento $T_4$ (no mostrado), se elimina la condición SD de tramo en los canales de servicio del nodo C al nodo D. La señalización continúa su curso como se indica en el instante $T_2$ de la figura I.1, salvo que:

1) los nodos de conmutación pasan a ser los nodos C y D, en lugar de los nodos E y F; y

2) la petición de puenteo pasa a ser SD-S, en lugar de SF-S.

## I.7 SF-S unidireccional que desplaza con prioridad a un SF-R unidireccional en tramos adyacentes – Detectados SF-S y SF-R en nodos no adyacentes

Véase la figura I.7.

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

El estado inicial del anillo es el de reposo. En el momento $T_1$, el nodo C detecta una condición SF procedente del nodo D en sus canales de servicio y protección. La señalización continúa como en la figura I.2 (momento $T_1$), salvo que los nodos de conmutación pasan a ser los nodos C y D, en lugar de los nodos E y F. La señalización alcanza el estado estacionario.

En el momento $T_2$, el nodo E detecta una condición SF procedente del nodo D en sus canales de servicio. El nodo E pasa a ser 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 (reglas S #1, G #1). El nodo C, al ver esta situación de petición de puenteo de tramo, retira su puenteo y conmutación de anillo porque 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 ya que ésa 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 momento $T_3$, se elimina la condición SF del nodo D al nodo E en los canales de servicio. El nodo E debería pasar a en 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 ausencia de petición en el byte K1 y puenteado en el byte K2 (regla S-S #2c). El nodo D, al ver los códigos de ausencia de 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 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 también pasa 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 momento $T_1$.

En el momento $T_4$ (no mostrado), se elimina la condición SF en los canales de servicio y protección del nodo D al nodo C. La señalización continúa de manera similar a la indicada en la figura I.2 (momento $T_2$), salvo que los nodos de conmutación pasan a ser los nodos C y D, en lugar de los nodos E y F.

## 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-anillo unidireccional en un anillo de cuatro fibras que desplaza con prioridad a una condición de degradación de señal-tramo unidireccional que existía previamente en un tramo adyacente.

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

En el momento $T_2$, el nodo E detecta una condición SF procedente del nodo D en sus canales de servicio y protección. El nodo E retira su conmutación 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 ausencia de petición (en el byte K1) y puenteado (en el byte K2) hacia el nodo F (regla S-S #2b). El nodo D pasa a ser un nodo de conmutación [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 bytes K al estado de transferencia total (regla P-P #1). El nodo F, al ver una indicación de ausencia de petición y la conmutación retirada del nodo E, retira su puenteo y conmutación, 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 conmutación 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 bytes 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 conmutación (regla I-S #1b, segundo punto) y actualizan los bits 6-8 del byte K2. La señalización alcanza el estado estacionario.

En el momento $T_3$, se elimina la condición SF en los canales de servicio y protección del nodo D al nodo E. El nodo E inicia su periodo de en espera al 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 en espera al 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 pasa a ser nodo de conmutación 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. El nodo E, retira por tanto, su puenteo y conmutación 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 conmutación 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 conmutado procedente del nodo F, completa el proceso efectuando una conmutación 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. El nodo D, por tanto, retira su puenteo y conmutación de anillo (regla S #5) y actúa conforme a la situación de petición de puenteo de tramo destinada al nodo E pasando a transferencia de bytes 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 bytes K. La señalización alcanza el mismo estado estacionario que en el momento $T_1$.

En el momento $T_4$ (no mostrado), se elimina la condición SD del nodo E al nodo F en los canales de servicio. La señalización continúa como en la figura I.1 (momento $T_2$), salvo que la petición de puenteo pasa a ser SD-S, en lugar de SF-S.

## 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-anillo unidireccional en un anillo de cuatro fibras que coexiste con otra condición de fallo de señal-anillo unidireccional que existía previamente en un tramo no adyacente.

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. La señalización continúa como en la figura I.2 (momento $T_1$). La señalización alcanza el estado estacionario.

En el momento $T_2$, el nodo C detecta una condición SF en sus canales de servicio y protección. El nodo C pasa a ser nodo de conmutación [regla S-P #2a, punto 2)], 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). El nodo B, al ver la petición de puenteo procedente del nodo C, pasa a ser 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, ya que 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 momento $T_2$, el nodo C detecta una condición SF en sus canales de servicio y protección. El nodo C pasa a ser 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, pasa a ser 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 de 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 de 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 de 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), el anexo A]. La señal alcanza el mismo estado estacionario que el descrito para la figura I.9.

En el momento $T_3$, se elimina la condición SF del nodo B al nodo C en los canales de servicio y 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 a la de su condición local (WTR), por lo 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). 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 momento $T_1$.

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 momento $T_3$, se elimina la condición SF del nodo B al nodo C en los canales de servicio y protección. El nodo C ve una petición de puenteo de anillo para un tramo no adyacente procedente del nodo D y debida al primer SF-R entre los nodos E y F. Esta petición tiene una prioridad superior a la de su condición local (WTR), por lo 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). 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 momento $T_4$ (no mostrado), se elimina 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 (momento $T_3$).

## I.10 Fallo de nodo en un anillo con capacidad de tráfico adicional (véase la figura I.11)

La figura I.11 se refiere al caso de silenciamiento de tráfico adicional en un anillo después de un fallo de nodo en un anillo de dos o 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 suministrada.

El estado inicial del nodo es el de reposo. El tráfico adicional es soportado en los canales de protección en torno al anillo. En el momento $T_1$, los nodos E y G detectan una condición SF en sus canales de servicio y protección. Los nodos E y G suprimen el tráfico adicional bidireccionalmente, pasan a ser nodos de conmutación (regla I-S #1a, regla S #7) y originan peticiones de puenteo en los trayectos largo y corto. Todos los nodos intermedios suprimirán el tráfico adicional bidireccionalmente y pasarán a transferencia total unidireccional (regla I-P #1). Ningún nodo de acceso a LO VC pasa a transferencia total bidireccional tras recibir bytes K cruzados. El nodo E, tras la recepción de la petición de puenteo procedente de G por el trayecto largo, silencia todo tráfico potencialmente mal conectado, efectúa un puenteo y una conmutación de anillo y actualiza los bits 6-8 del byte K2 (regla I-S #1b). El nodo G, tras la recepción de la petición de puenteo procedente de E por el trayecto largo, silencia todo tráfico potencialmente mal conectado, efectúa un puenteo y una conmutación de anillo y actualiza los bits 6-8 del byte K2 (regla I-S #1b). La señalización alcanza el estado estacionario.

En el momento $T_2$, el nodo en fallo se ha recuperado y la secuencia de recuperación continúa como en una recuperación de nodo normal. El tráfico adicional no se silencia cuando el nodo recibe ausencia de petición o código de reposo o ET de ambos sentidos.

## I.11 SF-S unidireccional que desplaza con prioridad a un SF-R en tramos adyacentes – Detectados SF-S y SF-R en nodos adyacentes

Véase la figura I.11.

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

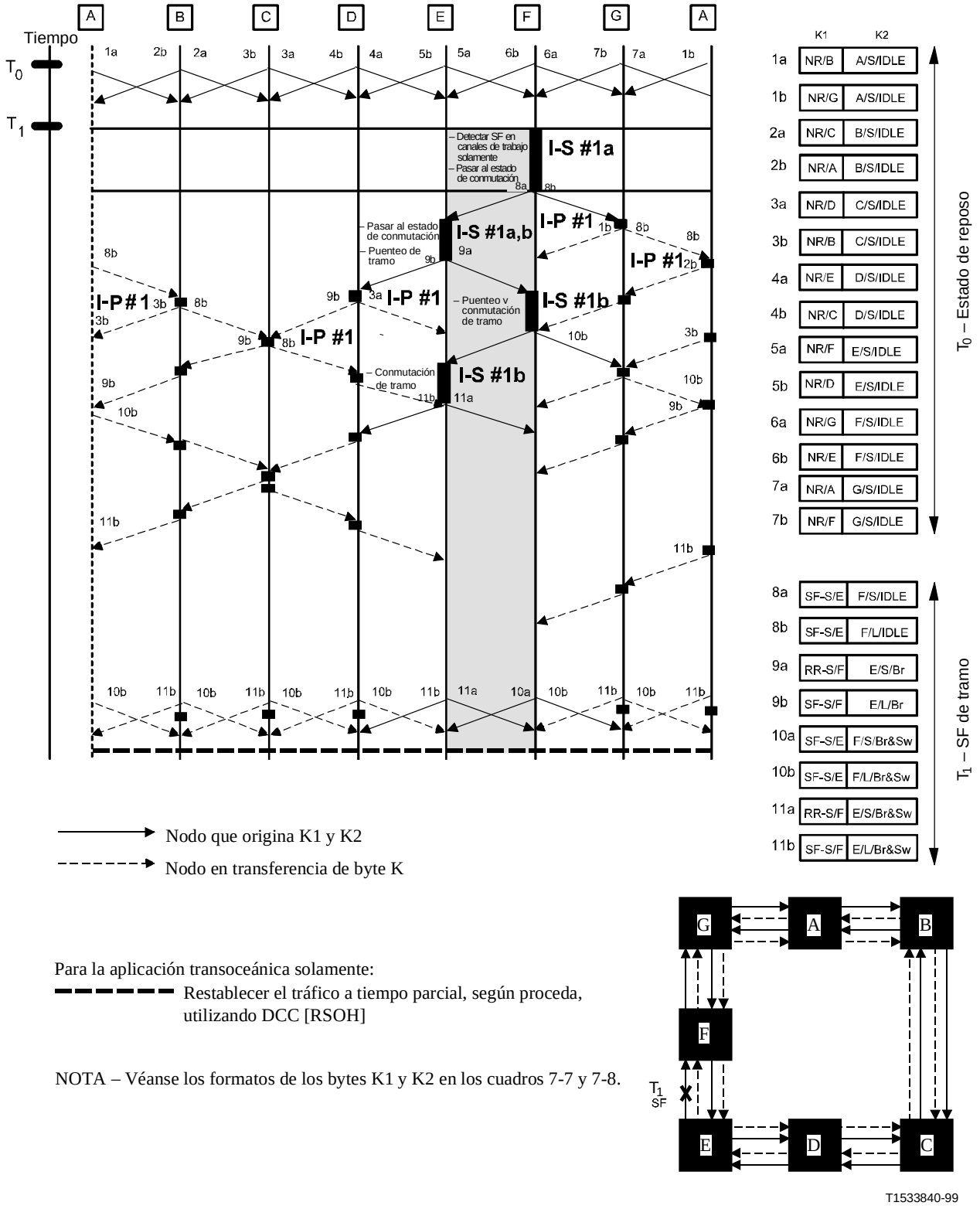
El estado inicial del anillo es el de reposo. En el momento $T_1$, el nodo D detecta una condición SF procedente del nodo C en sus canales de servicio y protección. La señalización sigue su curso como se muestra en la figura I.2 (en el momento $T_1$ en la figura), salvo que los nodos de conmutación pasan a ser los nodos C y D, en lugar de los E y F. La señalización alcanza el estado estacionario.

En el momento $T_2$, el nodo E detecta una condición SF procedente del nodo D en su canal de servicio. El nodo E pasa a ser un nodo de conmutación (regla S-P #2a) y origina una petición de puenteo de trama hacia el nodo D y una situación de petición de puenteo de tramo hacia el nodo F destinada al nodo D (regla S #1, regla G #1). El nodo D, al ver la petición de puenteo de tramo de prioridad superior procedente del nodo E, suprime su puenteo y su conmutación y señaliza en base a sus peticiones de APS coexistentes de prioridad máxima permitida (regla G #1c, regla S-S #2h). La entrada de prioridad máxima del nodo D a la que se permite coexistir es la petición SF-S procedente del nodo E, y la SF-P detectada procedente del nodo C (regla S-S #2h). Efectúa una petición de tramo hacia el nodo E (regla S-S #2f) y señaliza como corresponde (regla I-S #1b, regla S #3). El nodo D señaliza también SF-P y RDI hacia el nodo C, ya que se permite que coexistan SF-P y SF-S (regla S #4a, regla S-S #2h). El nodo C, tras perder la petición de puenteo de anillo y ver SF-P destinado a él por el trayecto corto, pasa a ser un nodo de conmutación de tramo y responde a la petición de tramo como corresponde (regla S-P #2b, regla S #1b). El nodo E, tras ver el código de puenteado procedente del nodo D, efectúa un puenteo y una conmutación de tramo y actualiza los bits 6-8 del byte K2 (regla I-S #1b). El nodo D, tras ver el código de puenteado procedente del nodo E, efectúa una conmutación y actualiza los bits 6-8 del byte K2 en consecuencia (regla I-S #1b). Los nodos intermedios pasan a transferencia de bytes K cuando se detectan bytes K cruzados (regla P-P #2). La señalización alcanza el estado estacionario.

En el momento $T_3$, se elimina la condición SF del nodo D al nodo E en los canales de servicio. El nodo E pasa a en espera al restablecimiento y señaliza como corresponda (regla S-S #3a). El nodo D, al ver el código WTR procedente del nodo E, retira su puenteo y conmutación de tramo y actúa en todas sus entradas, que son un SF-R detectado y una petición de WTR de prioridad menor procedente del nodo E. El nodo D señaliza una petición de puenteo de anillo hacia el nodo C tanto por el trayecto corto como por el trayecto largo (regla S-S #2d). El nodo E, al ver una petición de puenteo de anillo destinada a otro nodo, pasa a transferencia total bidireccional (regla S-P #1e). El nodo C, al perder la petición de puenteo de tramo y ver una petición de puenteo de anillo de trayecto largo procedente del nodo D, efectúa un puenteo y una conmutación de anillo y actualiza los bits 6-8 del byte K2 (regla S #6, regla I-S #1b). El nodo D, al ver una petición de puenteo de anillo de trayecto largo procedente del nodo C, efectúa también un puenteo y una 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 momento $T_1$.

En el momento $T_4$ (no mostrado), se elimina la condición SF en los canales de servicio y protección del nodo C al nodo D. La señalización continúa de manera similar a la indicada a la figura I.2 (en el

momento $T_2$ en la figura), salvo que los nodos de conmutación pasan a ser los nodos C y D, en lugar de los nodos E y F.




NOTA – Véanse los formatos de los bytes K1 y K2 en los cuadros 7-7 y 7-8.

**Figura I.1/G.841 – Anillo de protección compartida de MS de cuatro fibras – Fallo unidireccional (tramo) en servicio de E a F**

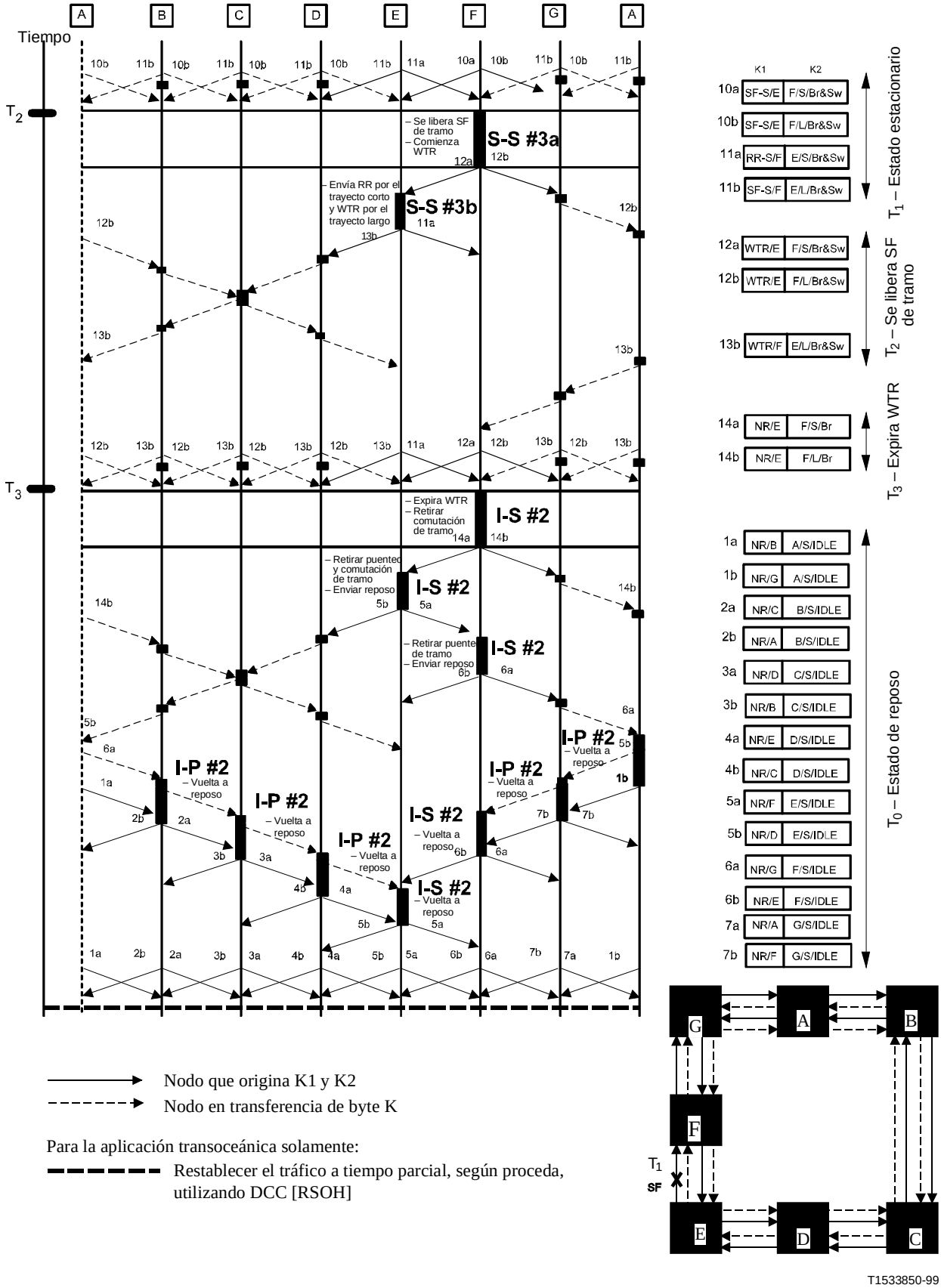



**Figura I.1/G.841 – Anillo de protección compartida de MS de cuatro fibras – Fallo unidireccional (tramo) en servicio de E a F *(fin)***

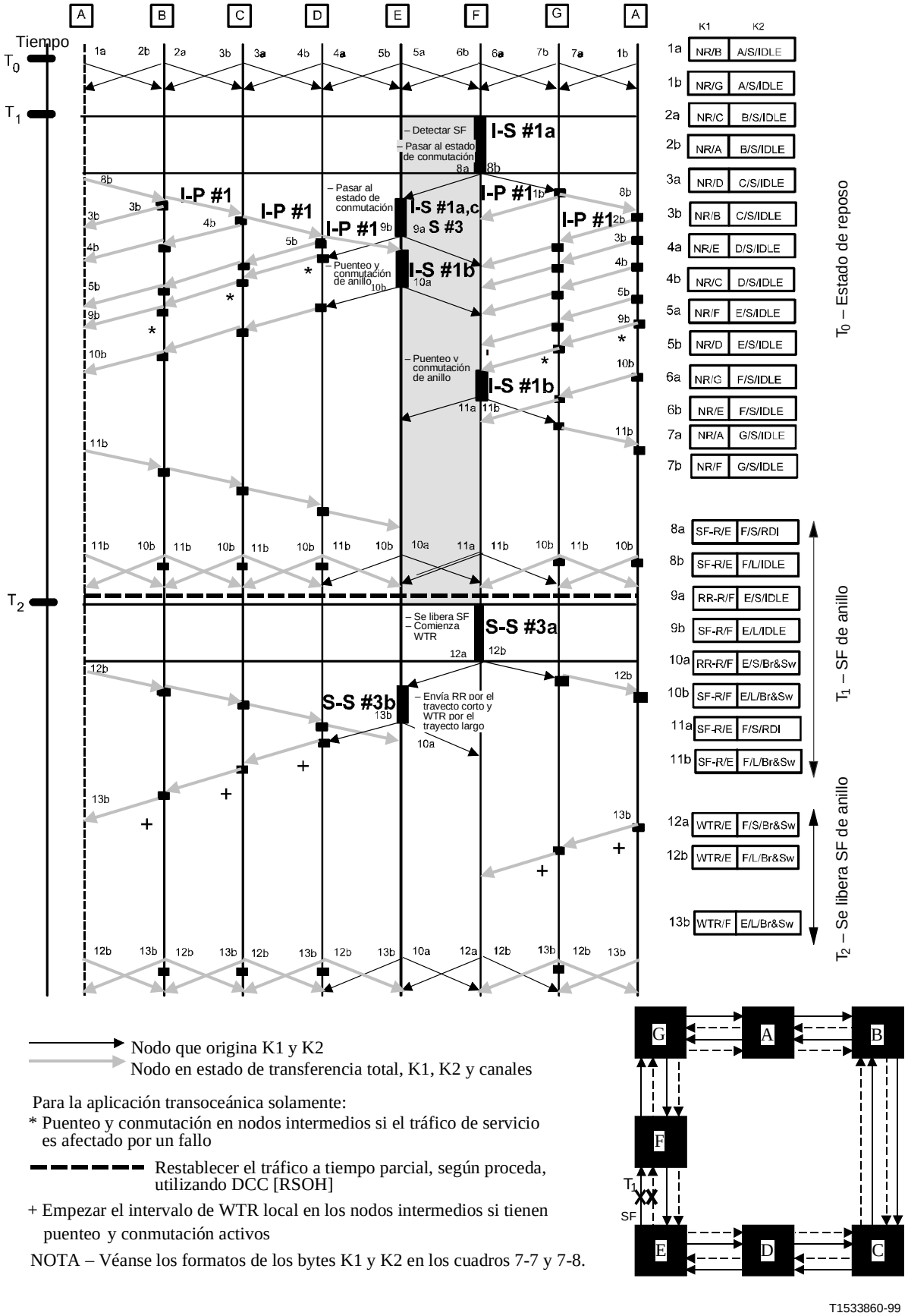



**Figura I.2/G.841 – Anillo de protección compartida de MS de dos o cuatro fibras – SF unidireccional (anillo)**

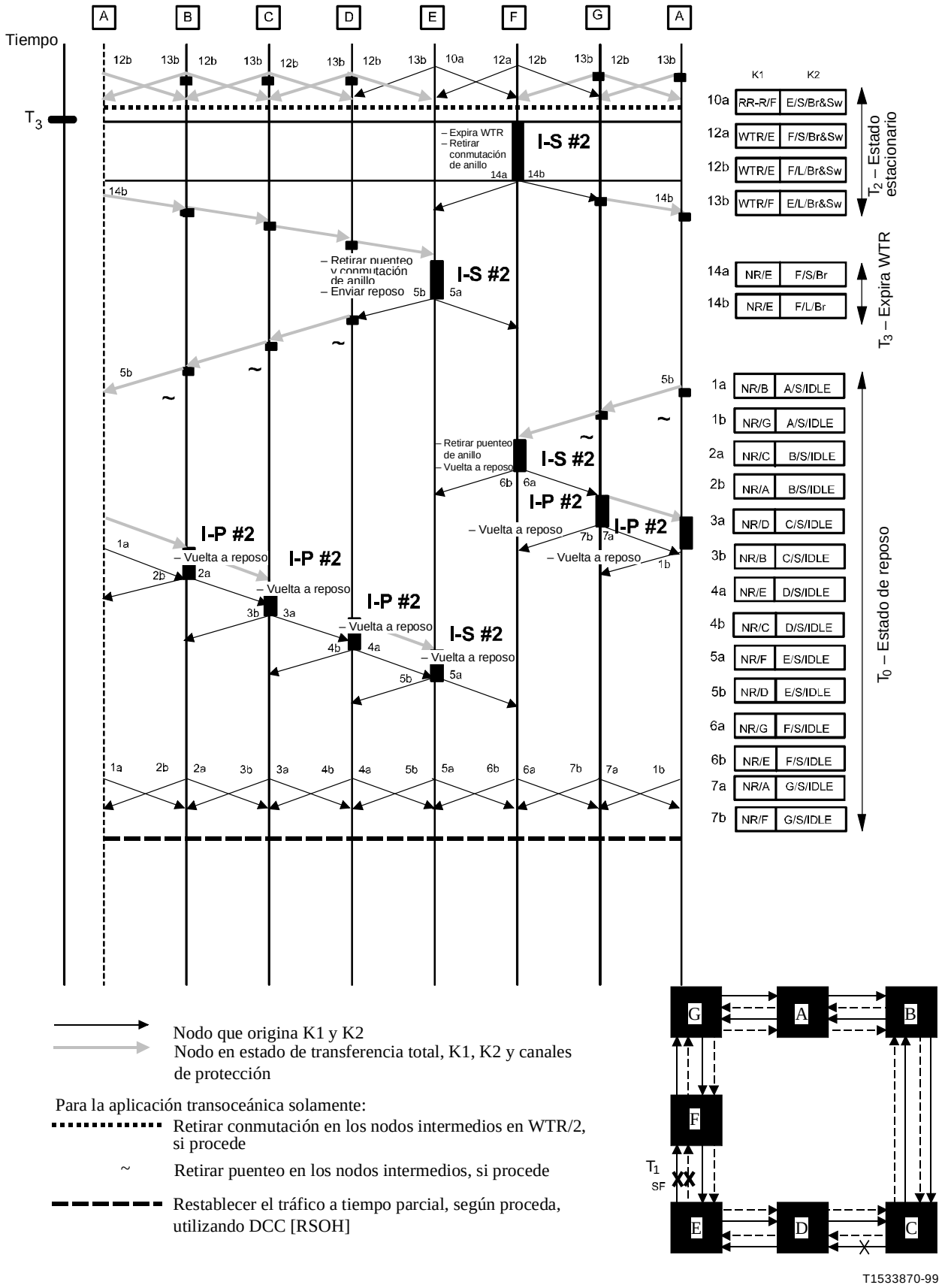



**Figura I.2/G.841 – Anillo de protección compartida de MS de dos o cuatro fibras – SF unidireccional (anillo) *(fin)***

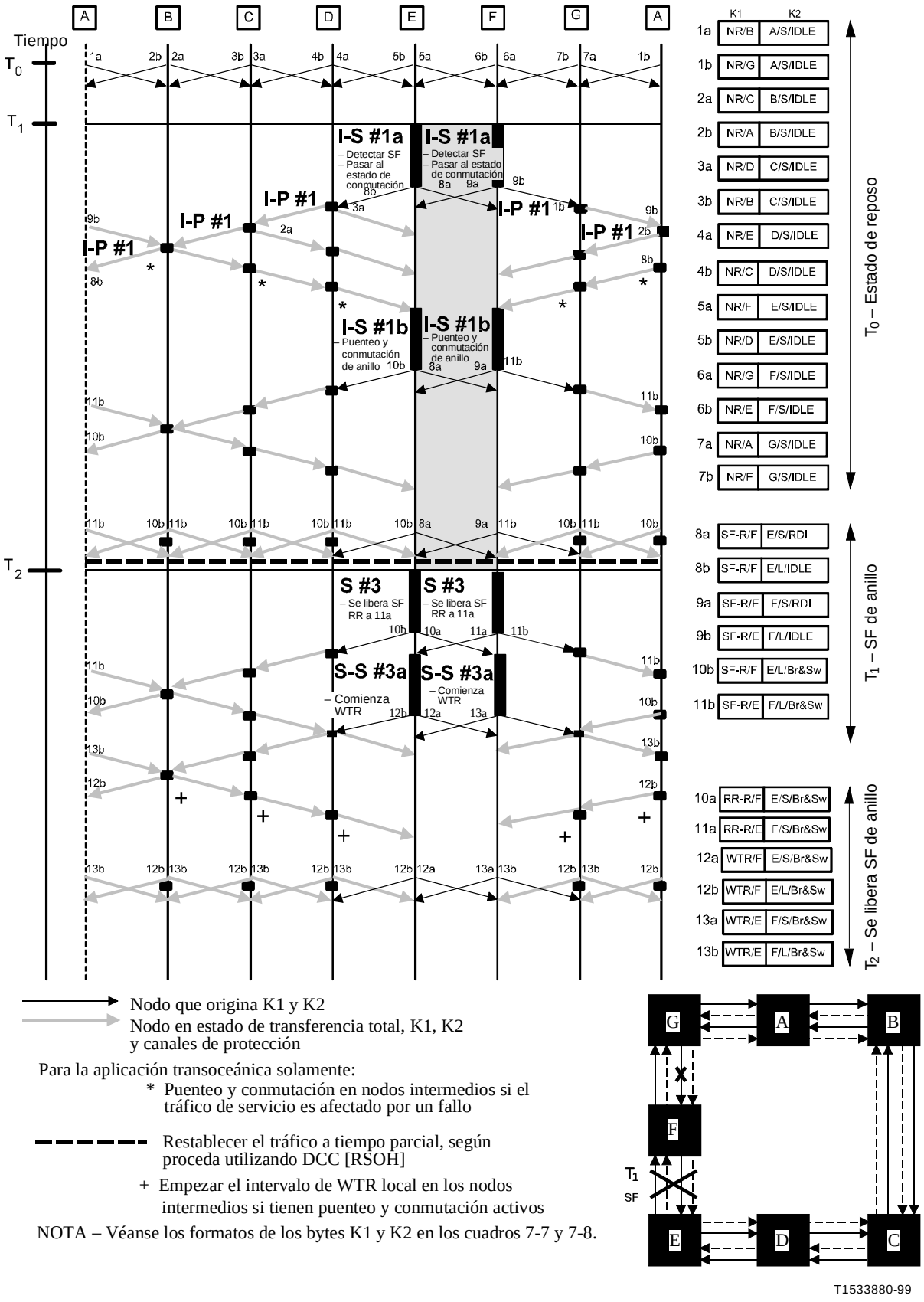



**Figura I.3/G.841 – Anillo de protección compartida de MS de dos o cuatro fibras – SF unidireccional (anillo)**

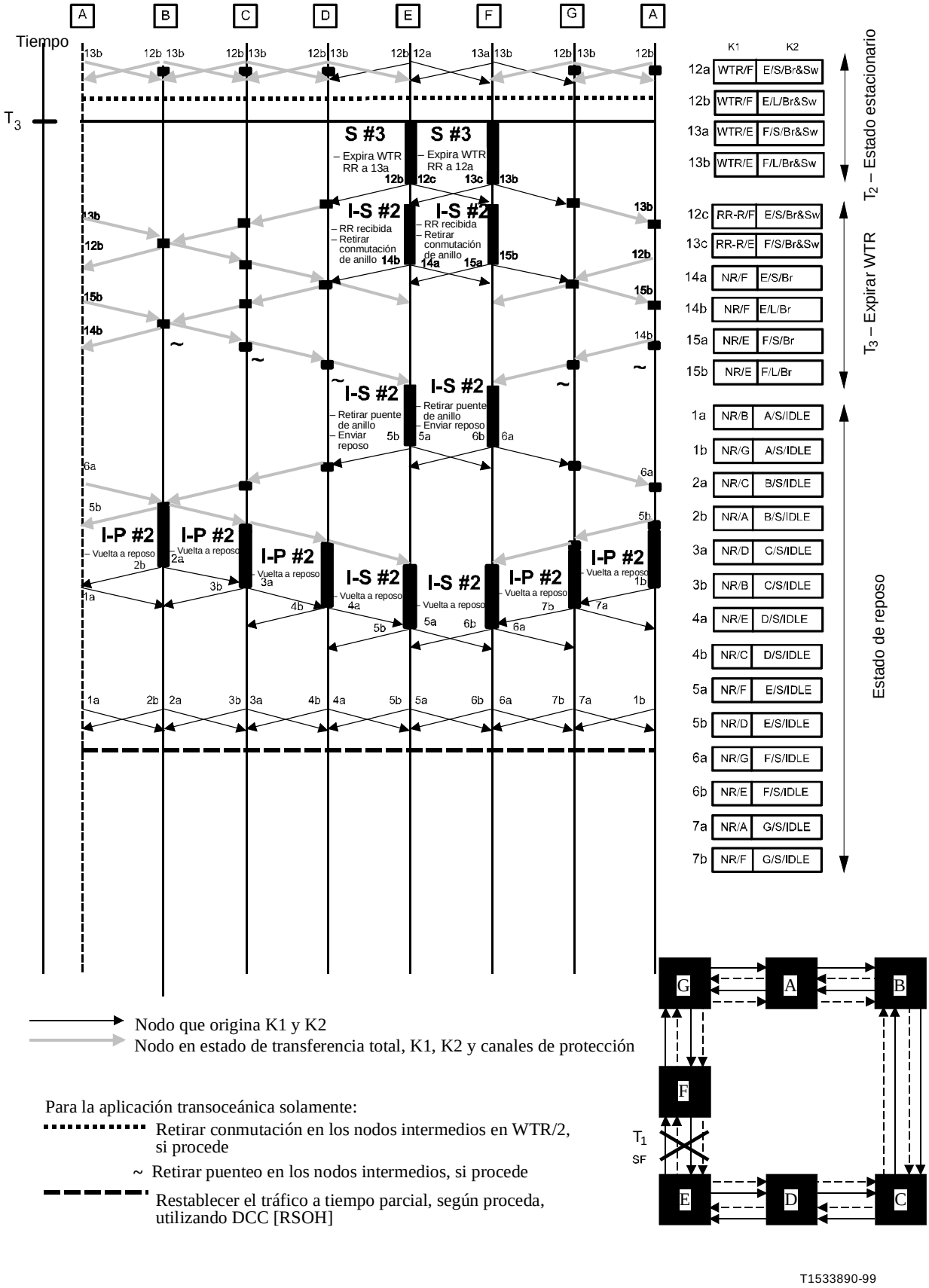



**Figura I.3/G.841 – Anillo de protección compartida de MS de dos o cuatro fibras – SF bidireccional (anillo) *(fin)***

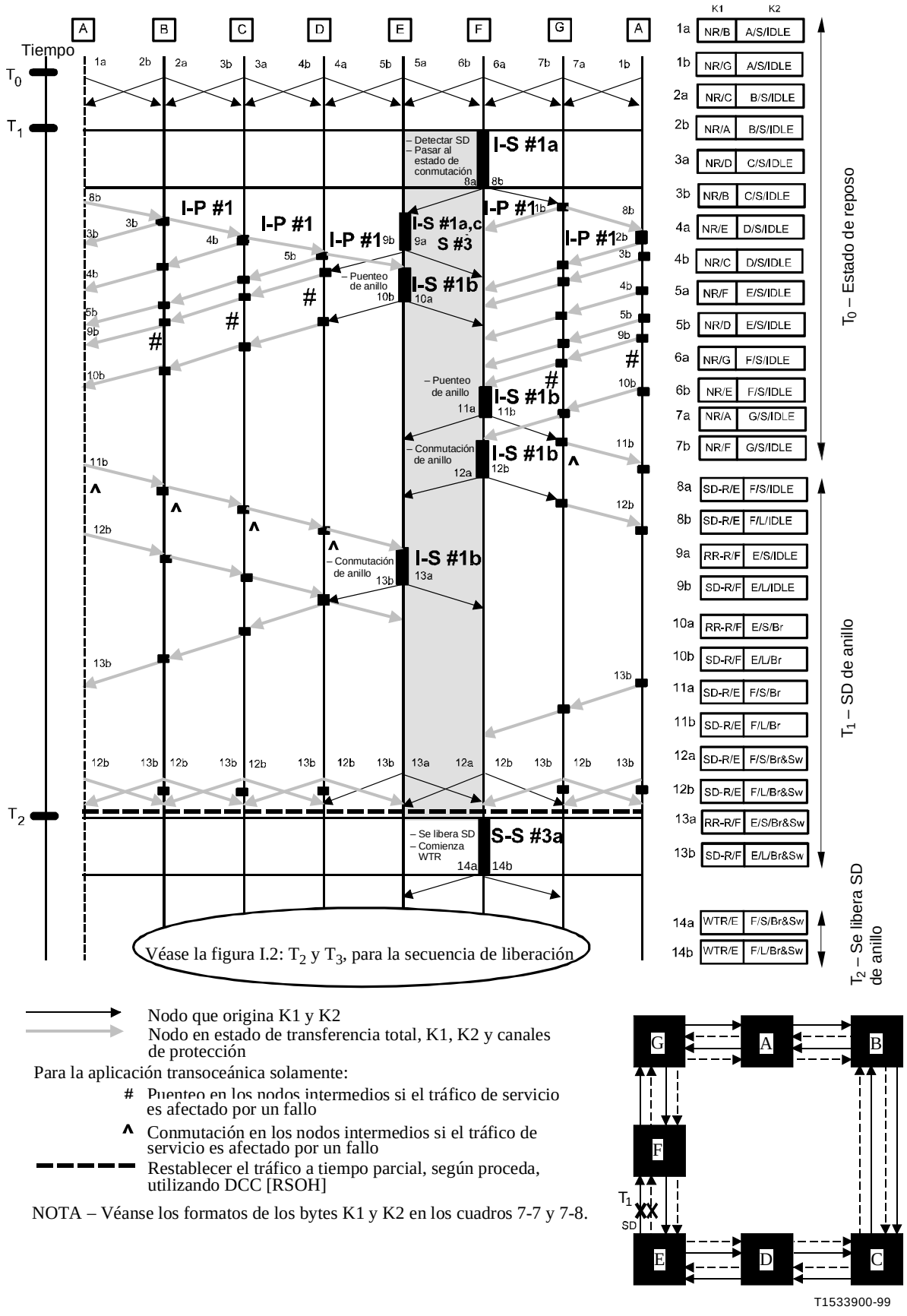



**Figura I.4/G.841 – Anillo de protección compartida de MS de dos o cuatro fibras – SD unidireccional (anillo)**

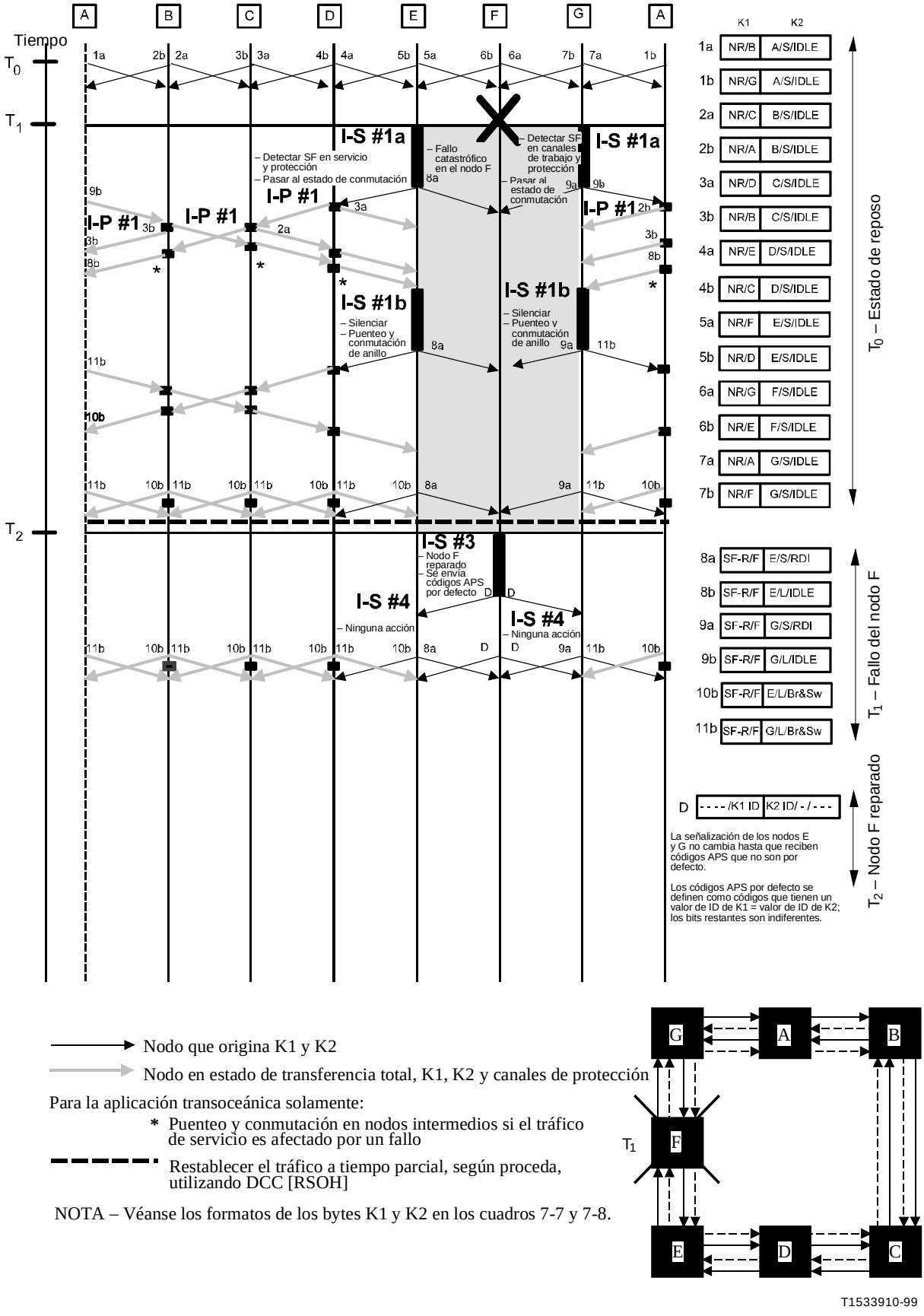



**Figura I.5/G.841 – Anillo de protección compartida de MS de cuatro fibras – Fallo de nodo**

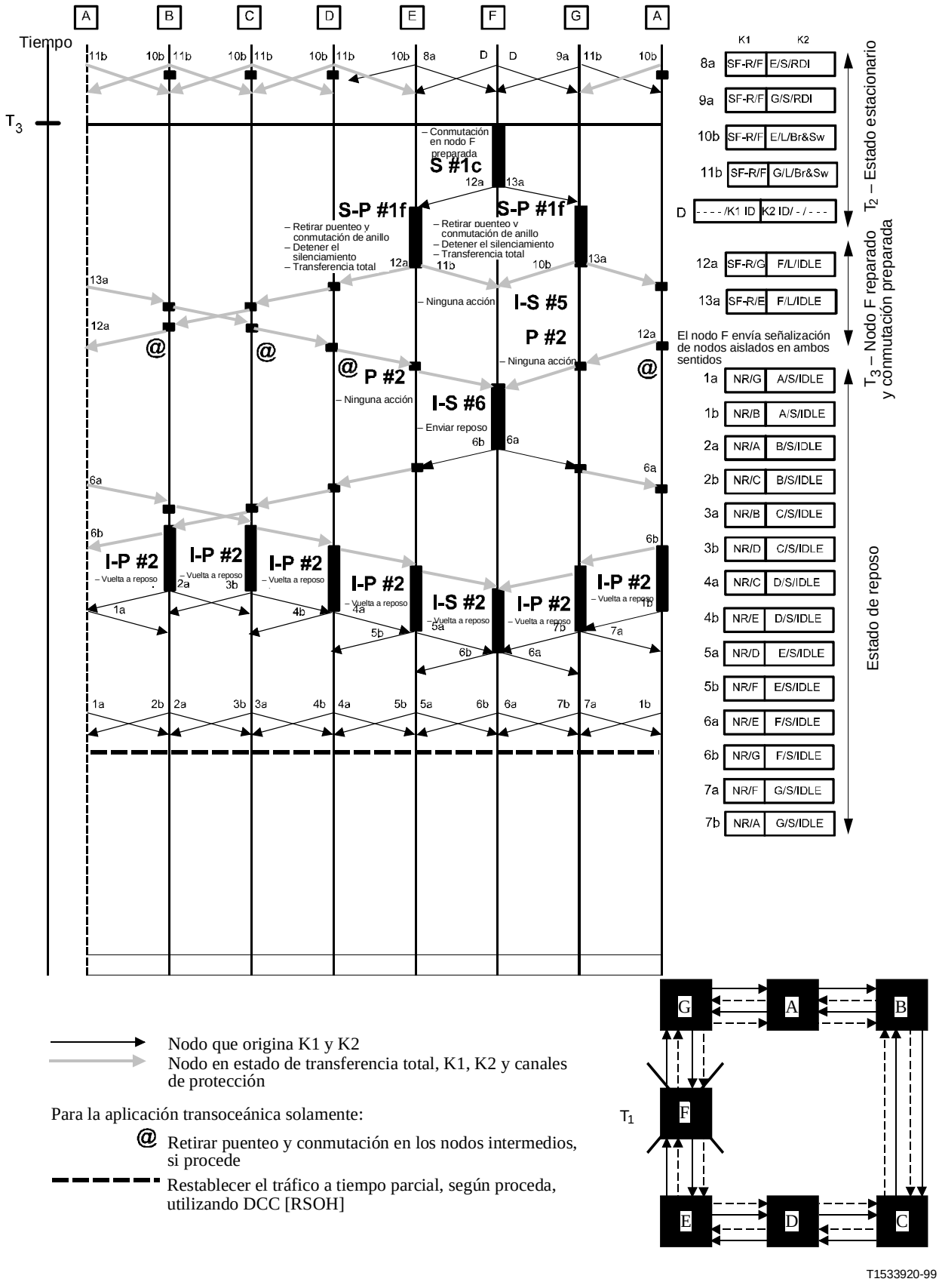



**Figura I.5/G.841 – Anillo de protección compartida de MS de cuatro fibras – Fallo de nodo *(fin)***

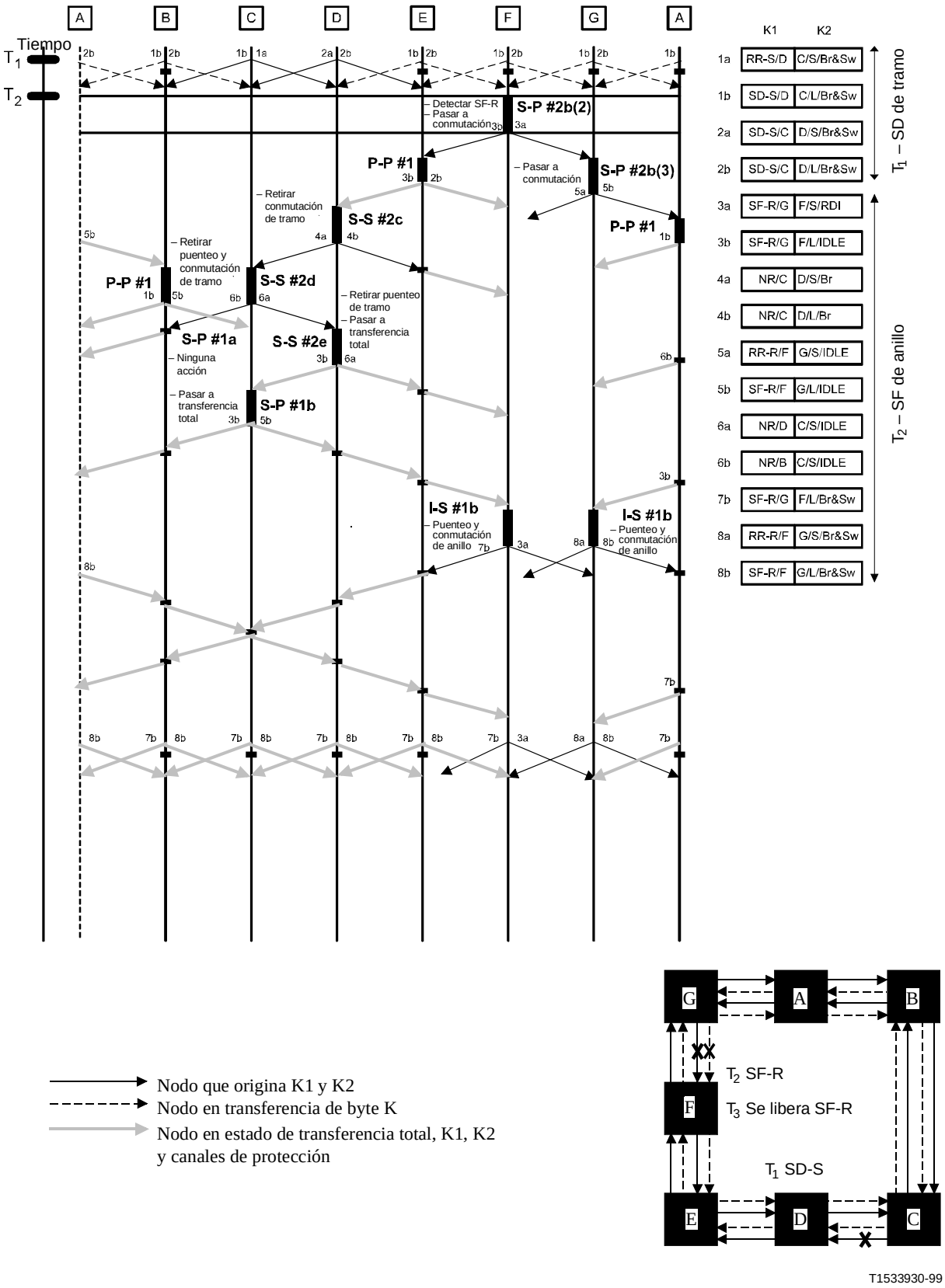



**Figura I.6/G.841 – Anillo de protección compartida de MS de cuatro fibras – SF-R unidireccional que desplaza con prioridad a un SD-S unidireccional en tramos no adyacentes**

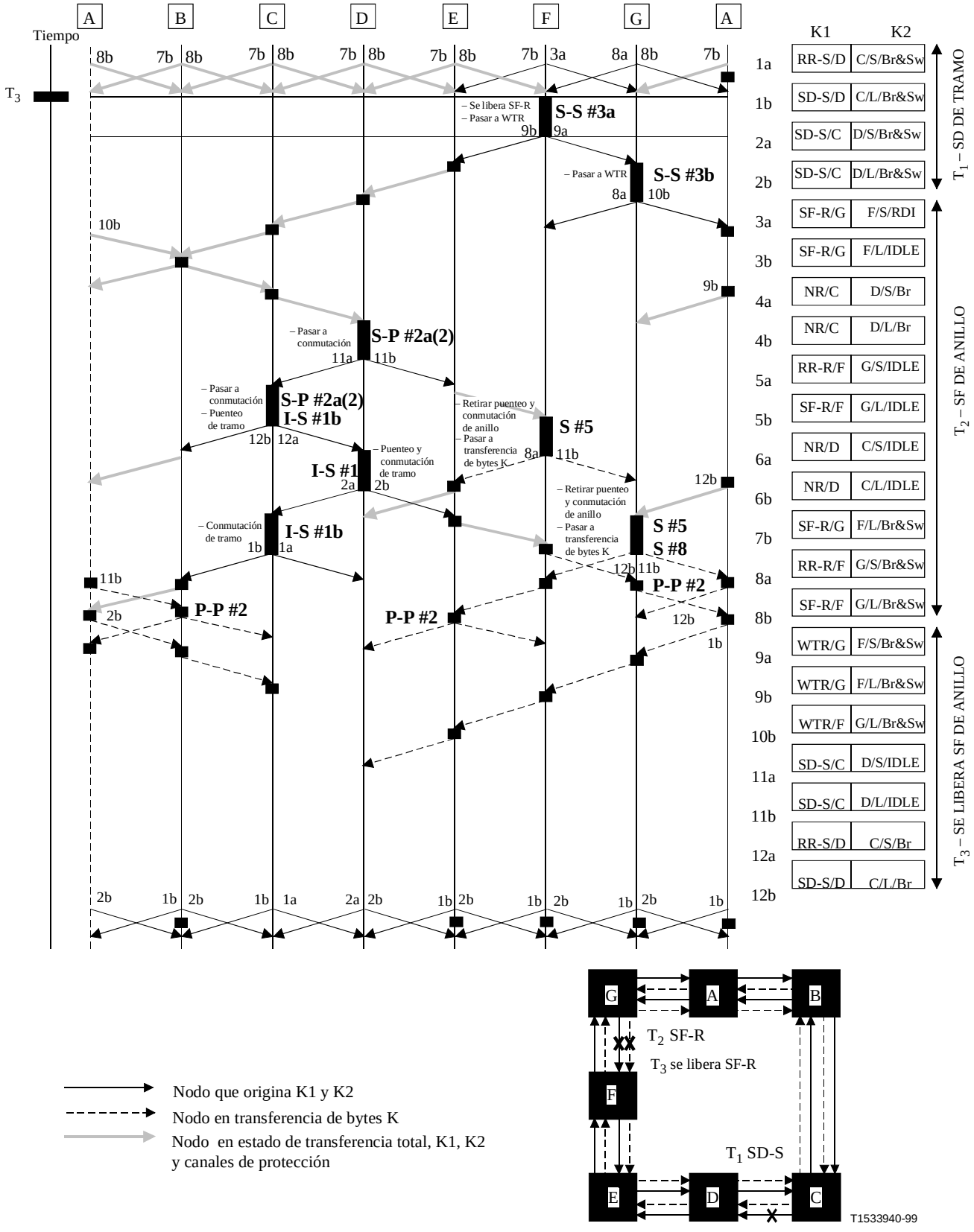



**Figura I.6/G.841 – Anillo de protección compartida de MS de cuatro fibras – SR-R unidireccional que desplaza con prioridad a un SD-S unidireccional en tramos no adyacentes *(fin)***

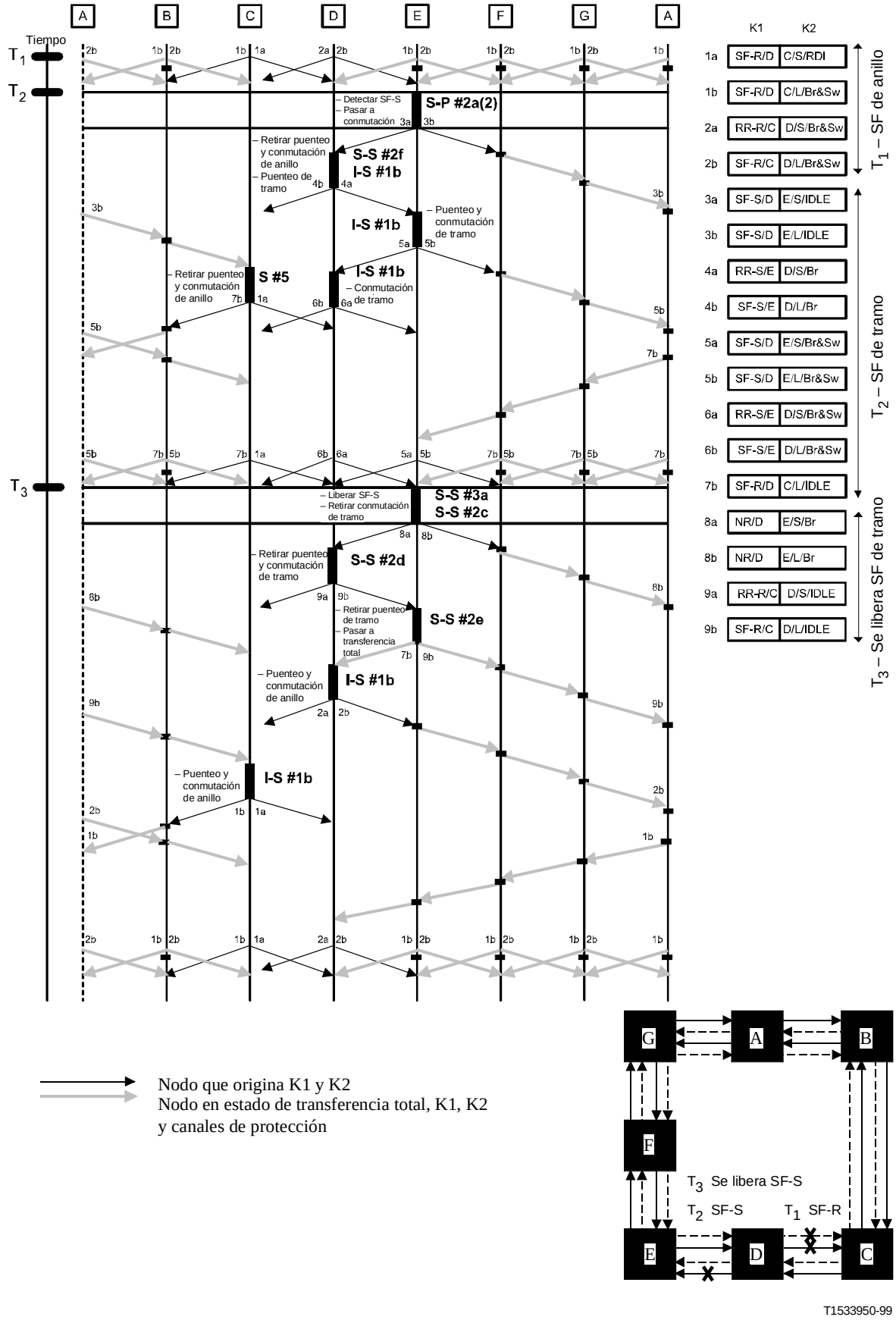



**Figura I.7/G.841 – Anillo de protección compartida de MS de cuatro fibras – SF-S unidireccional que desplaza con prioridad a un SF-R unidireccional en tramos adyacentes**

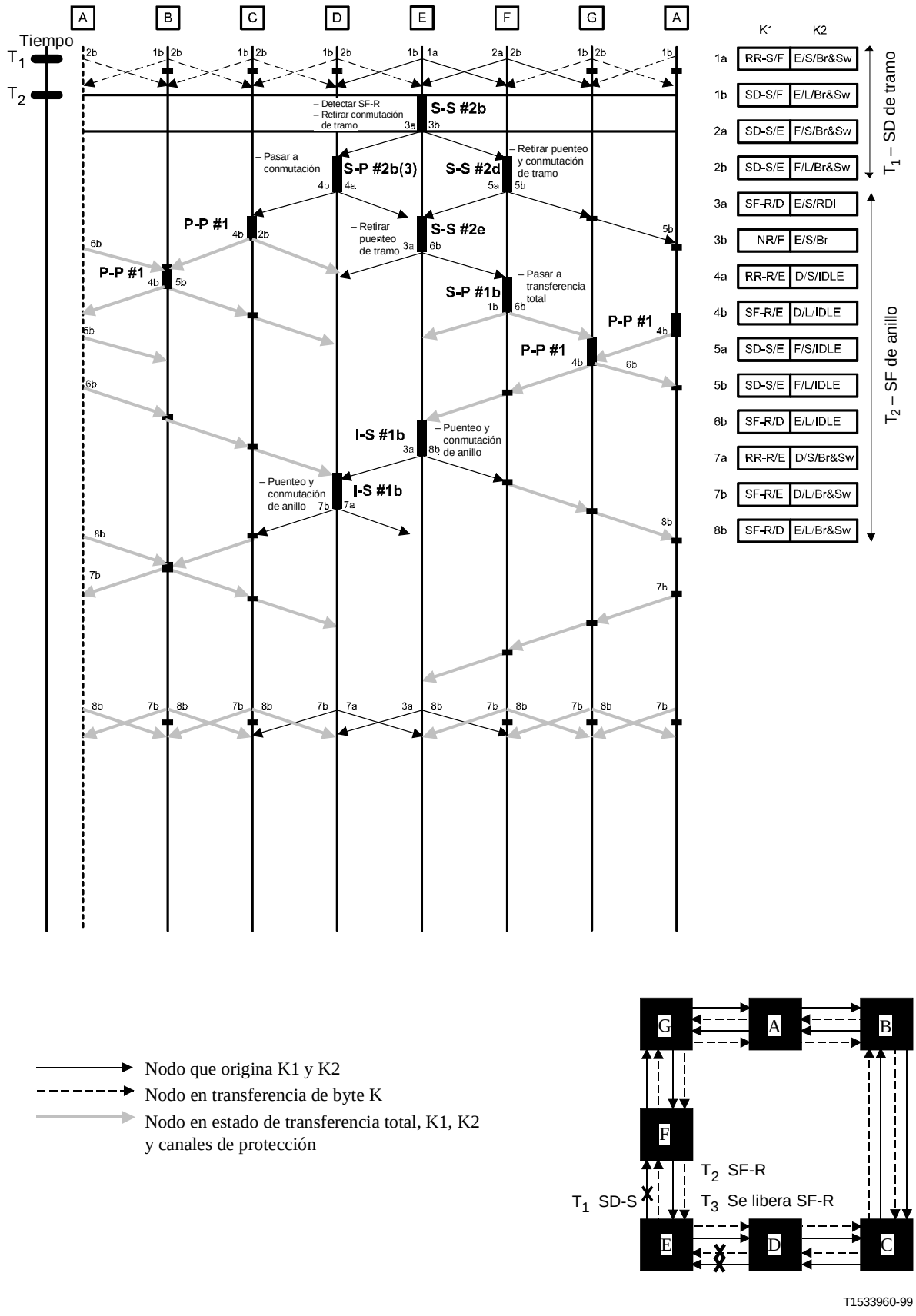



**Figura I.8/G.841 – Anillo de protección compartida de MS de cuatro fibras – SF-R unidireccional que desplaza con prioridad a un SD-S unidireccional en tramos adyacentes**

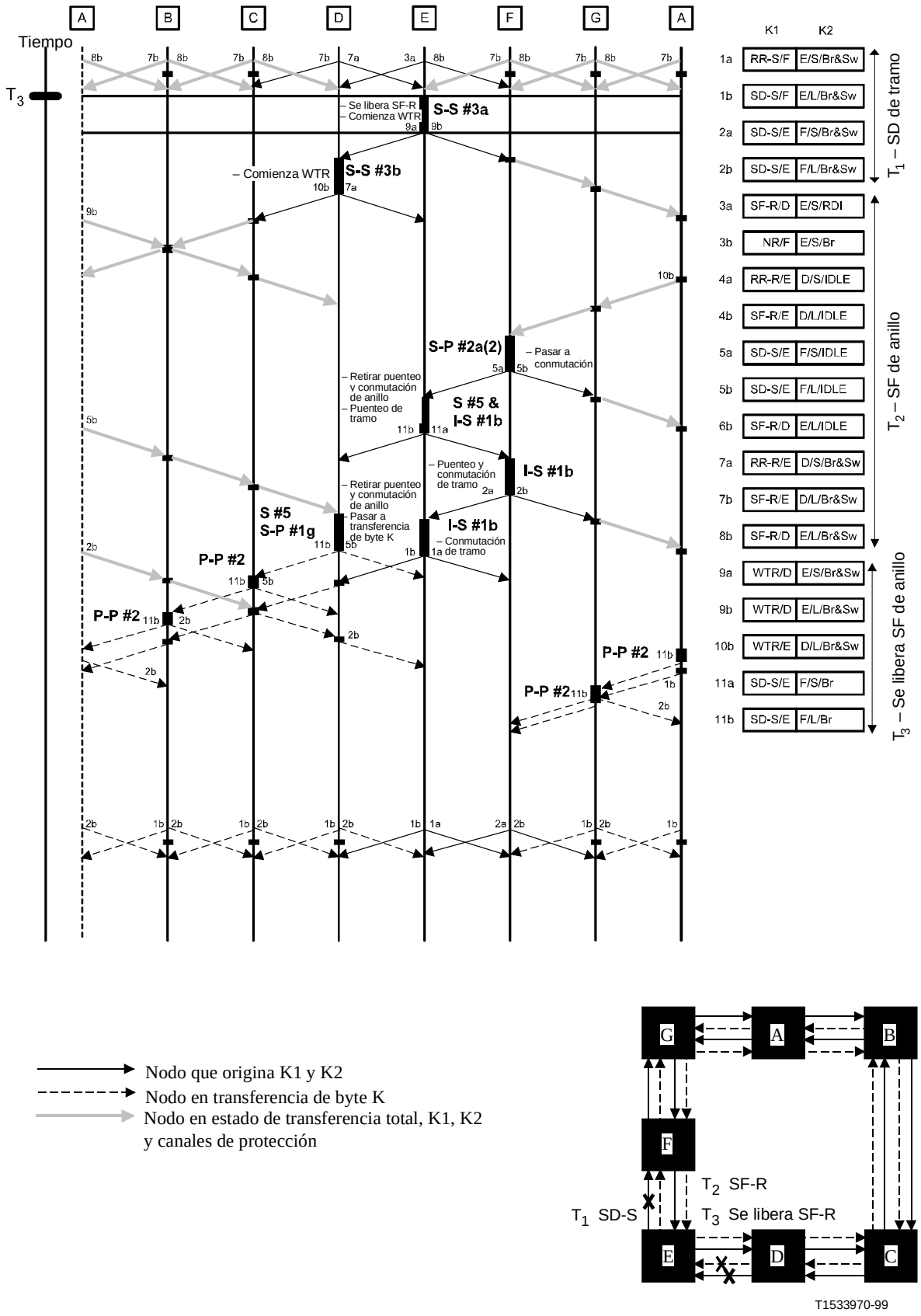



**Figura I.8/G.841 – Anillo de protección compartida de MS de cuatro fibras – SF-R unidireccional que desplaza con prioridad a un SD-S unidireccional en tramos adyacentes *(fin)***

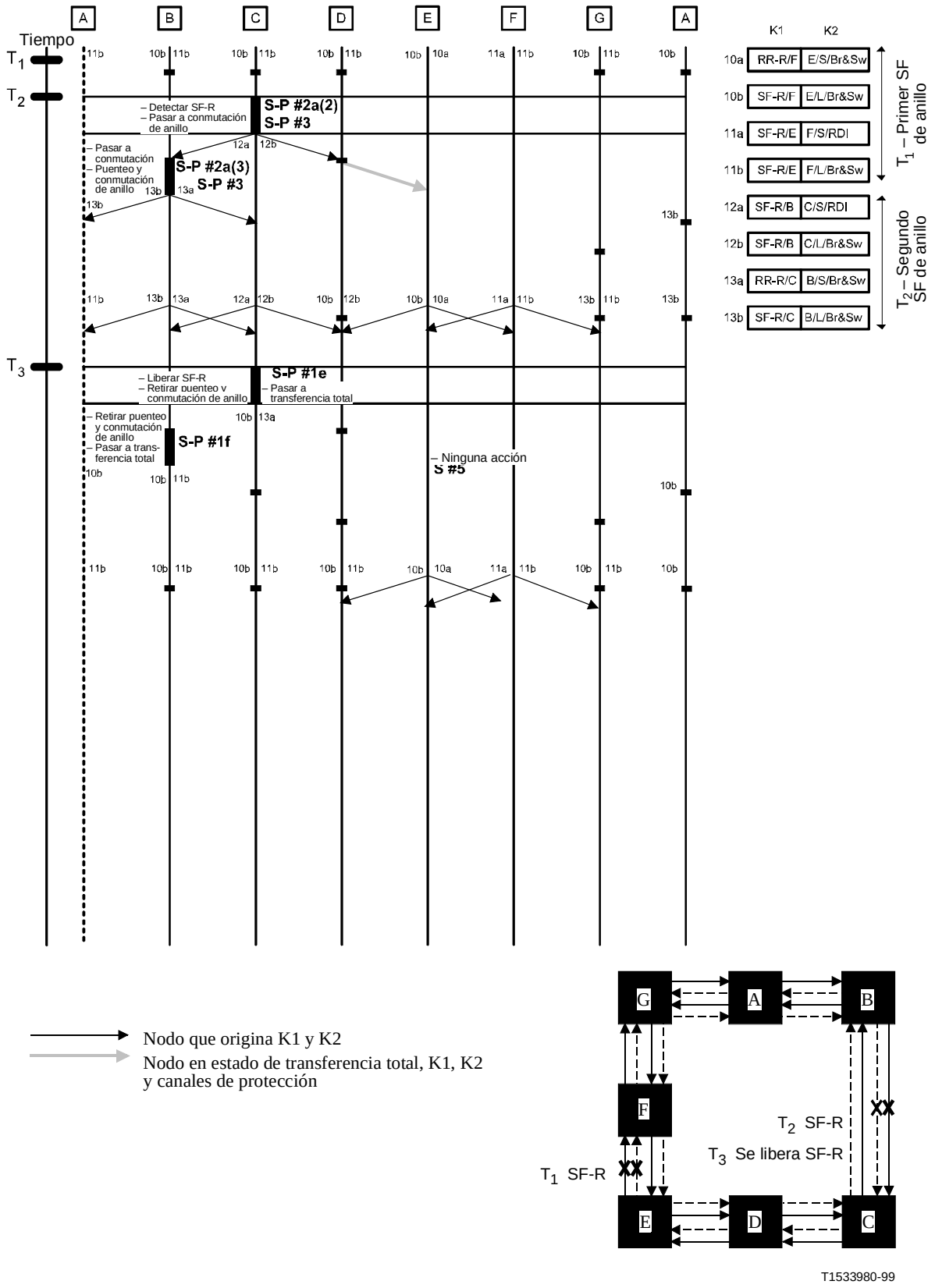



**Figura I.9/G.841 – Anillo de protección compartida de MS de cuatro fibras – SF-R unidireccional que desplaza con prioridad a un SF-R unidireccional en tramos no adyacentes**

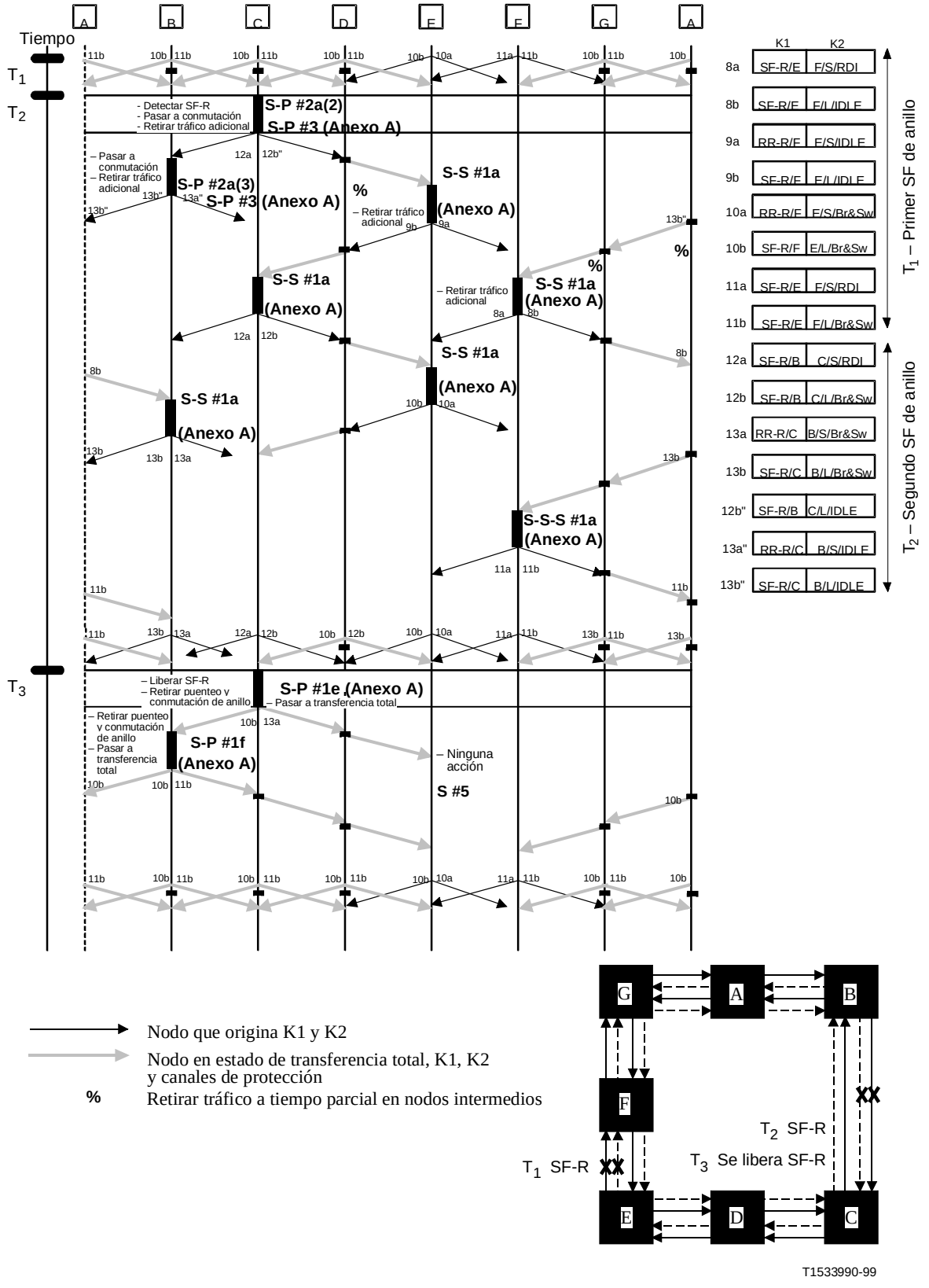
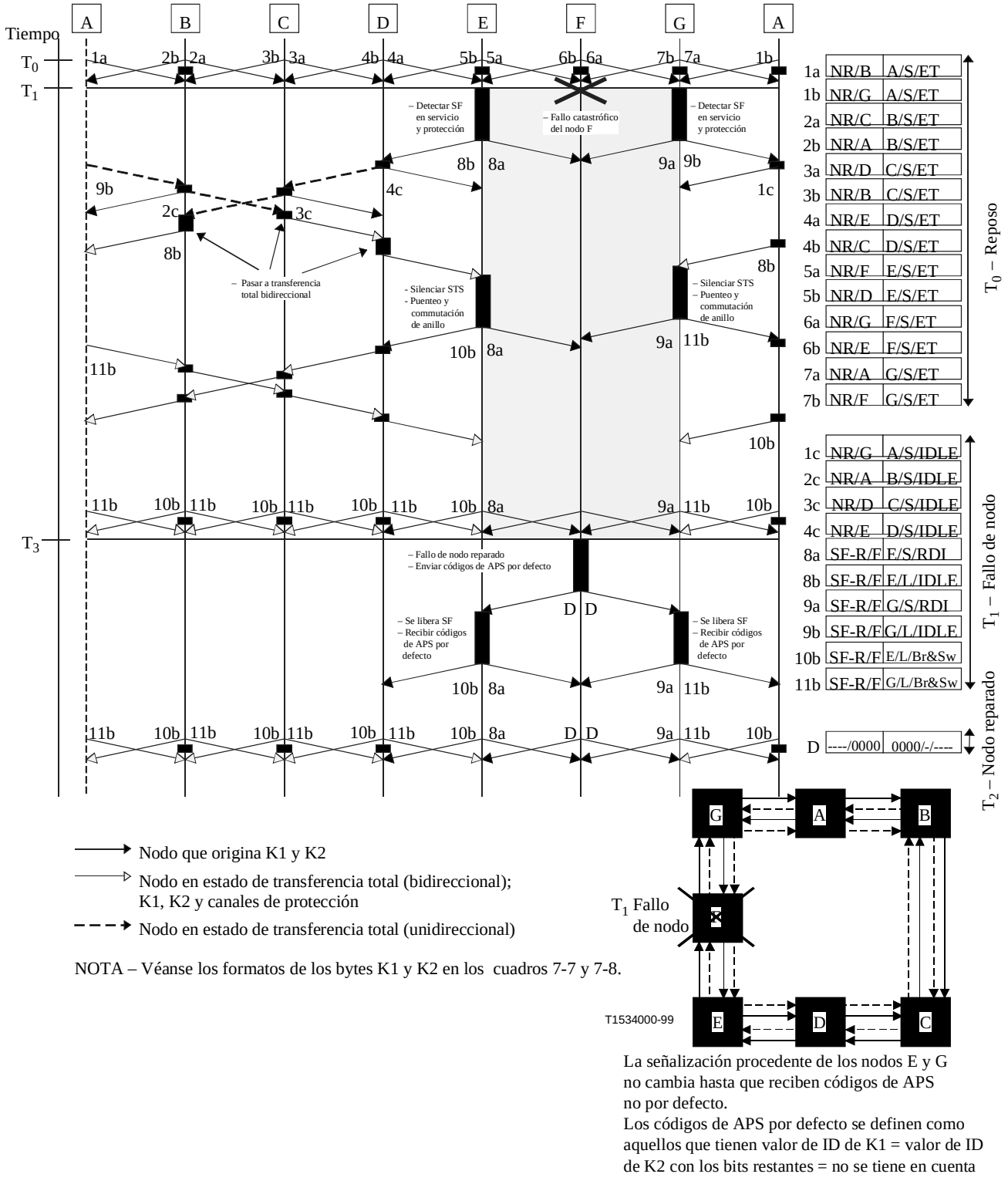



**Figura I.10/G.841 – Anillo de protección compartida de MS de cuatro fibras – SF-R unidireccional más SF-R unidireccional en tramos no adyacentes (aplicación transoceánica)**




NOTA – Véanse los formatos de los bytes K1 y K2 en los cuadros 7-7 y 7-8.

La señalización procedente de los nodos E y G no cambia hasta que reciben códigos de APS no por defecto.
Los códigos de APS por defecto se definen como aquellos que tienen valor de ID de K1 = valor de ID de K2 con los bits restantes = no se tiene en cuenta

**Figura I.11/G.841 – Anillo de protección compartida de MS de cuatro fibras – Fallo de nodo en un anillo con tráfico adicional**

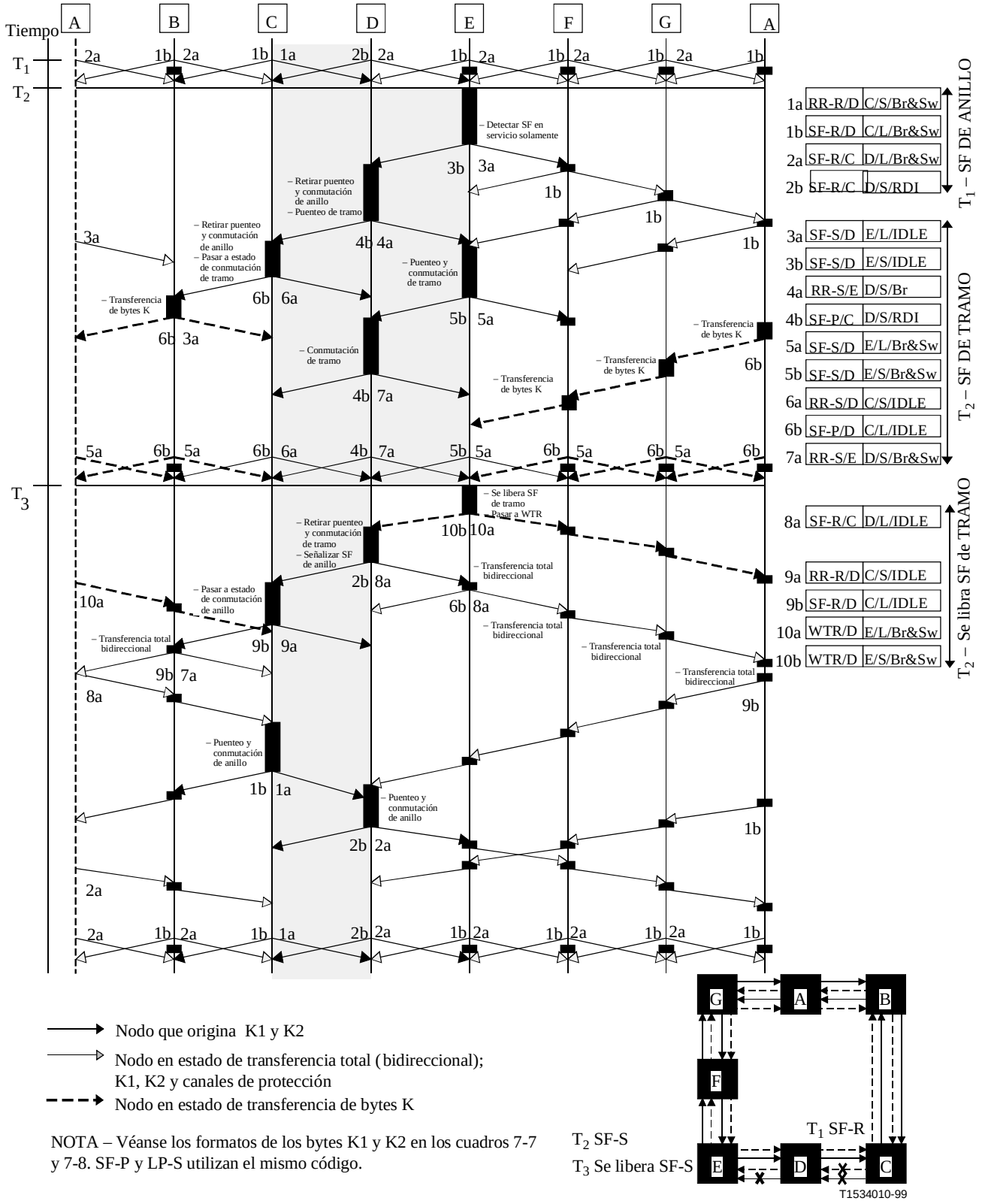



**Figura I.12/G.841 – Anillo de protección compartida de MS de cuatro fibras – SF-S unidireccional que desplaza con prioridad un SF-R unidireccional en tramos adyacentes – Detectados SF-S y SF-R en nodos adyacentes**

APÉNDICE II

## Lógica de silenciamiento generalizado

Este apéndice contiene la lógica de silenciamiento generalizado para circuitos que no son de naturaleza bidireccional simple. La lógica de silenciamiento generalizado se puede derivar de las nociones de silenciamiento para circuitos unidireccionales básicos, silenciamiento para circuitos unidireccionales retirados de manera múltiple y silenciamiento para circuitos unidireccionales originados de manera múltiple. La conmutación bidireccional y los protocolos de conmutación de anillo de protección compartida de sección de multiplexación descritos en otros puntos de la presente Recomendación no se ven influidos por esta generalización. La ampliación de la lógica de silenciamiento permite de manera formal la prestación de una variedad más amplia de servicios dentro del contexto de la presente Recomendación.

Para mayor claridad, los requisitos de silenciamiento de este apéndice se analizarán desde el punto de vista de un observador situado en un nodo de conmutación. Para simplificar, las figuras muestran sólo el nodo de conmutación en uno de los lados del fallo del nodo.

### II.1 Silenciamiento para circuitos unidireccional (y bidireccionales)

Para el silenciamiento de circuitos unidireccionales simples se aplican las dos reglas siguientes:

1) Suponer, con respecto al nodo de conmutación, que el fallo se ha producido en el sentido del circuito unidireccional. Silenciar el circuito (insertar AIS en el canal de protección correspondiente del circuito puesto que está puenteado en el sentido distinto al del fallo) si, y solamente si, el escenario del fallo del nodo incluye el nodo de salida para el circuito unidireccional. Véase la figura II.1.

2) Suponer, con respecto al nodo de conmutación, que el fallo se ha producido en el sentido opuesto al del circuito unidireccional. Silenciar el circuito (insertar AIS en el canal de servicio) si, y solamente si, el escenario del fallo del nodo incluye el nodo de entrada para el circuito unidireccional. Véase la figura II.2.

Se señala que la combinación de estas dos reglas constituye la regla actual para el silenciamiento bidireccional de un circuito bidireccional en un nodo de conmutación si el circuito termina en un nodo en fallo. Véase la figura II.3.

### II.2 Silenciamiento de circuitos unidireccionales retirados de manera múltiple y originados de manera múltiples

#### II.2.1 Circuitos unidireccionales retirados de manera múltiple

En la figura II.4 se muestra un circuito unidireccional retirado de manera múltiple. Por intuición, en presencia de fallos, la lógica del silenciamiento deberá permitir que se entregue un circuito a tantas extracciones como sea posible. Las reglas de silenciamiento correspondientes son similares a las de los circuitos unidireccionales simples:

1) Suponer, con respecto al nodo de conmutación, que el fallo se ha producido en el sentido del circuito unidireccional retirado de manera múltiple. Silenciar el circuito (insertar AIS en el canal de protección correspondiente del circuito puesto que está puenteado en el sentido distinto al del fallo) si, y solamente si, el escenario del fallo del nodo incluye el nodo de salida para el circuito unidireccional retirado de manera múltiple. Véase la figura II.5.

2) Suponer, con respecto al nodo de conmutación, que el fallo se ha producido en el sentido opuesto al del circuito unidireccional retirado de manera múltiple. Silenciar el circuito (insertar AIS en el canal de servicio) si, y solamente si, el escenario del fallo del nodo

incluye el nodo de entrada para el circuito unidireccional retirado de manera múltiple. Véase la figura II.6.

Una radiodifusión unidireccional se trata como dos circuitos unidireccionales independientes a efectos de silenciamiento.

### II.2.2 Circuitos unidireccionales originados de manera múltiple

En la figura II.7 se muestra un circuito unidireccional originado de manera múltiple. El análisis que sigue es independiente del origen que se transmite de hecho al nodo de extremo, o de cómo se toma o se aplica esa decisión. El objetivo de la lógica del silenciamiento es, en presencia de fallos, entregar el circuito al nodo de extracción mientras haya por lo menos un origen. Las reglas de silenciamiento correspondientes son similares a las de los circuitos unidireccionales simples:

1) Suponer, con respecto al nodo de conmutación, que el fallo se ha producido en el sentido del circuito unidireccional originado de manera múltiple. Silenciar el circuito (insertar AIS en el canal de protección correspondiente del circuito puesto que está puenteado en el sentido distinto al del fallo) si, y solamente si, el escenario del fallo del nodo incluye el nodo de salida para el circuito unidireccional originado de manera múltiple. Véase la figura II.8.

2) Suponer, con respecto al nodo de conmutación, que el fallo se ha producido en el sentido opuesto al del circuito unidireccional originado de manera múltiple. Silenciar el circuito (insertar AIS en el canal de servicio) si, y solamente si, el escenario de fallo del nodo incluye el nodo de entrada (es decir, el primer nodo de origen) para el circuito unidireccional originado de manera múltiple. Véase la figura II.9.

### II.2.3 Aplicación al interfuncionamiento de anillos

Para el interfuncionamiento de anillos descrito en la Recomendación G.842, el circuito de interfuncionamiento bidireccional es un circuito retirado de manera múltiple con dos supresiones (extracción y continuación), y es un circuito originado de manera múltiple con dos orígenes en el otro sentido. El silenciamiento para el interfuncionamiento de anillos es precisamente la combinación del silenciamiento para circuitos retirados de manera múltiple y circuitos originados de manera múltiple que se indica más arriba. De manera más general, las reglas de silenciamiento que aquí se examinan amplían los circuitos unidireccionales con combinaciones de supresiones múltiples, originaciones múltiples o radiodifusiones múltiples.

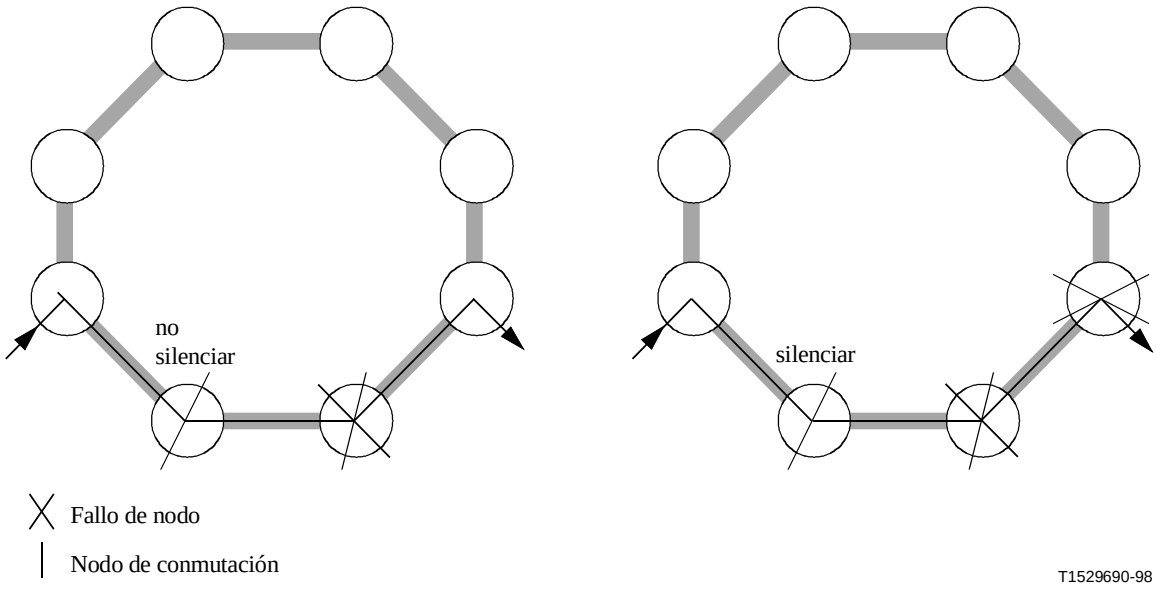



**Figura II.1/G.841 – Ejemplo de silenciamiento de circuito unidireccional en el que el fallo se produce en el sentido del circuito unidireccional**

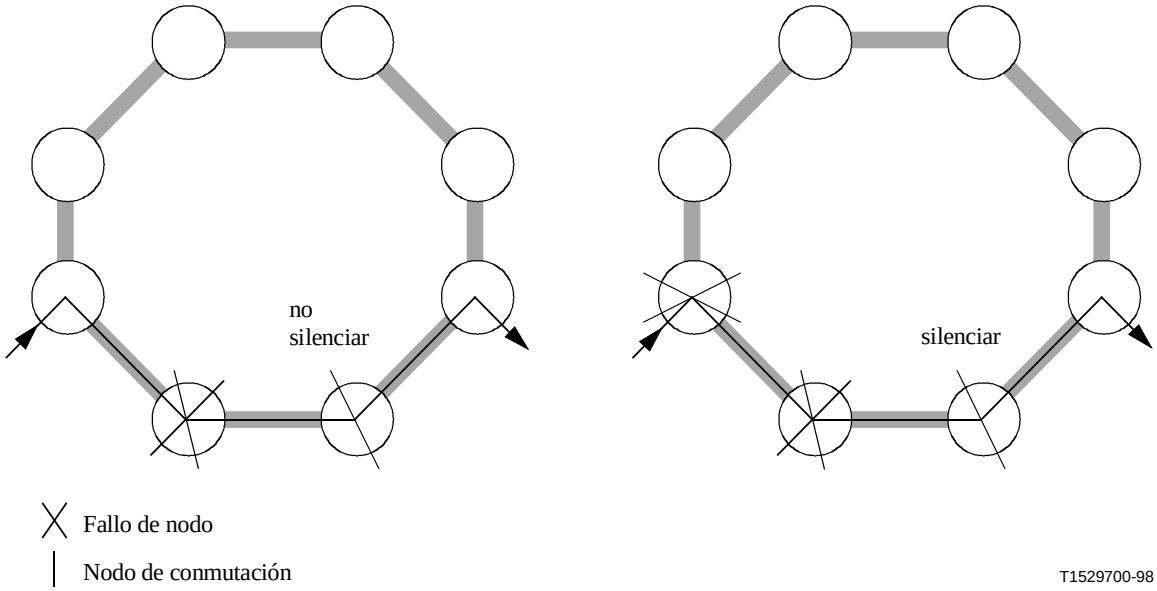



**Figura II.2/G.841 – Ejemplo de silenciamiento de circuito unidireccional en el que el fallo se produce en el sentido opuesto al del circuito unidireccional**

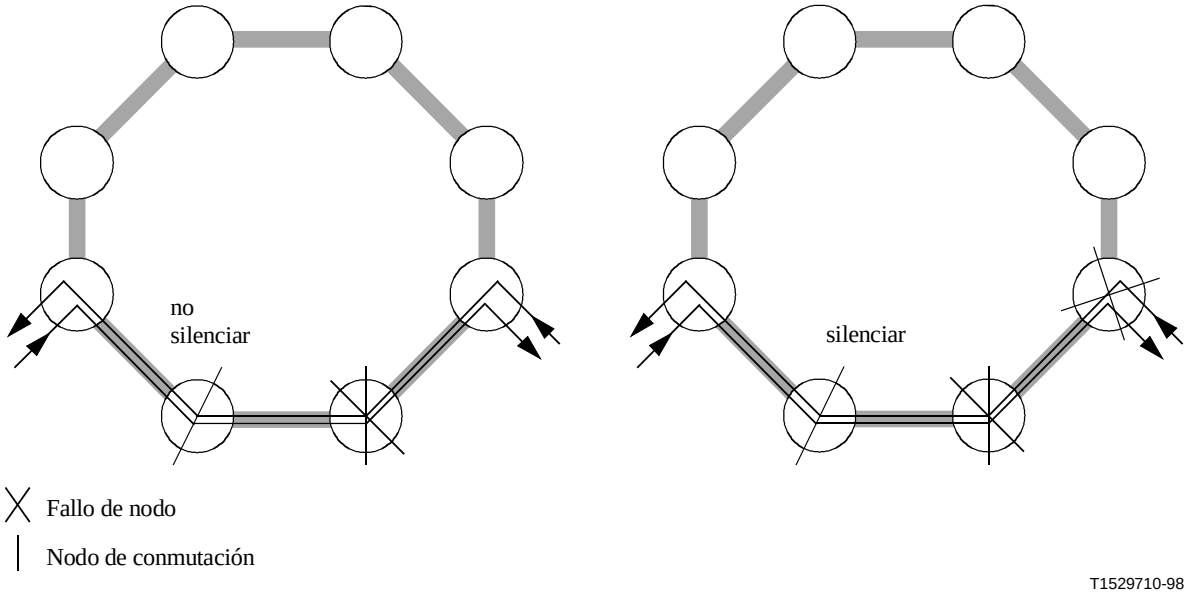



**Figura II.3/G.841 – Ejemplo de silenciamiento de circuito bidireccional**

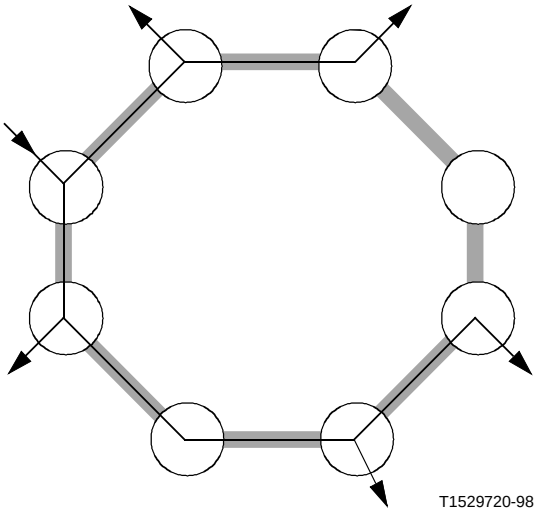



**Figura II.4/G.841 – Ejemplo de circuito unidireccional suprimido de manera múltiple**

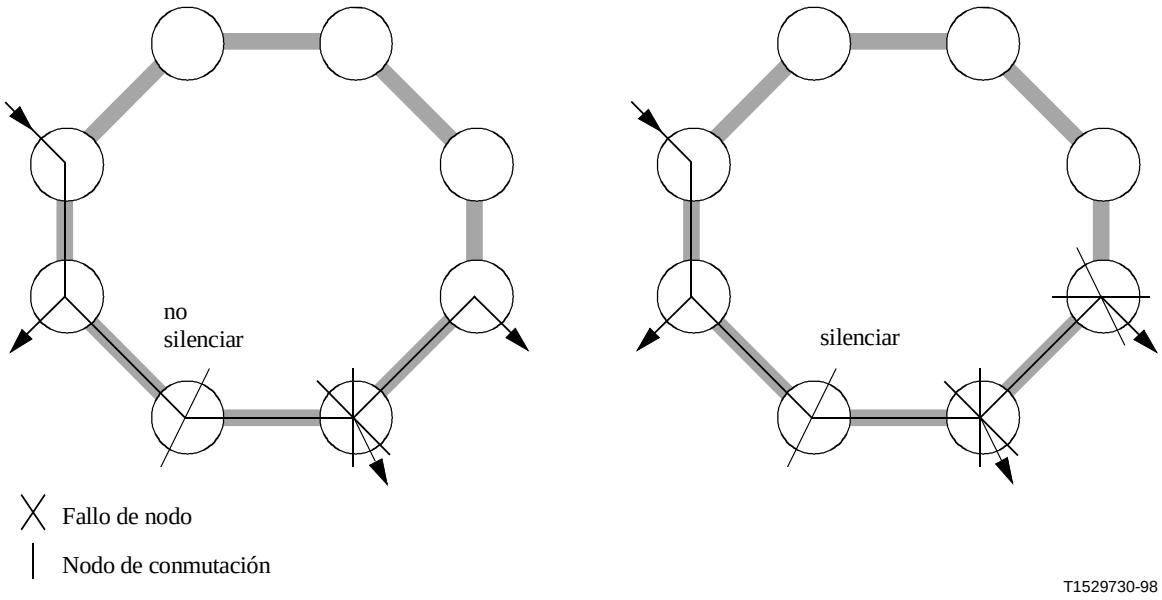



**Figura II.5/G.841 – Ejemplo de silencionamiento de circuito unidireccional suprimido de manera múltiple en el que el fallo se produce en el sentido del circuito unidireccional**

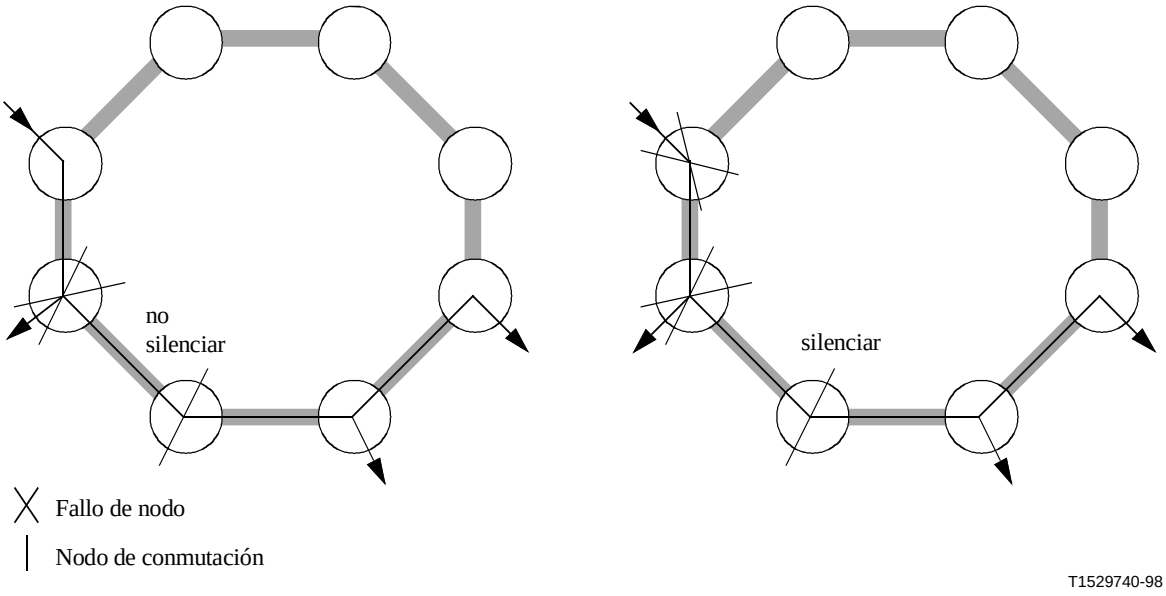



**Figura II.6/G.841 – Ejemplo de silencionamiento de circuito unidireccional suprimido de manera múltiple en el que el fallo se produce en el sentido opuesto al del circuito unidireccional**

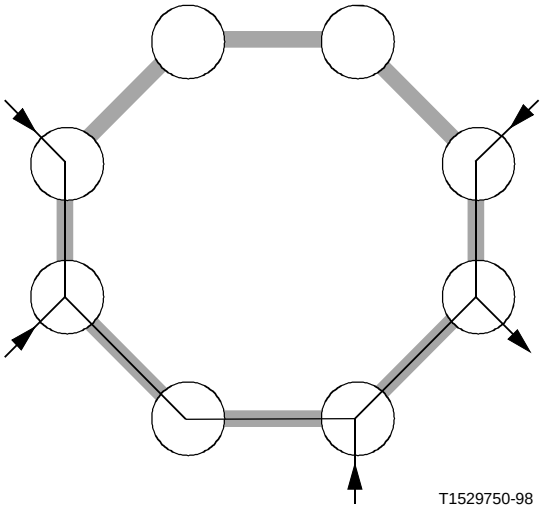



**Figura II.7/G.841 – Ejemplo de circuito unidireccional originado de manera múltiple**

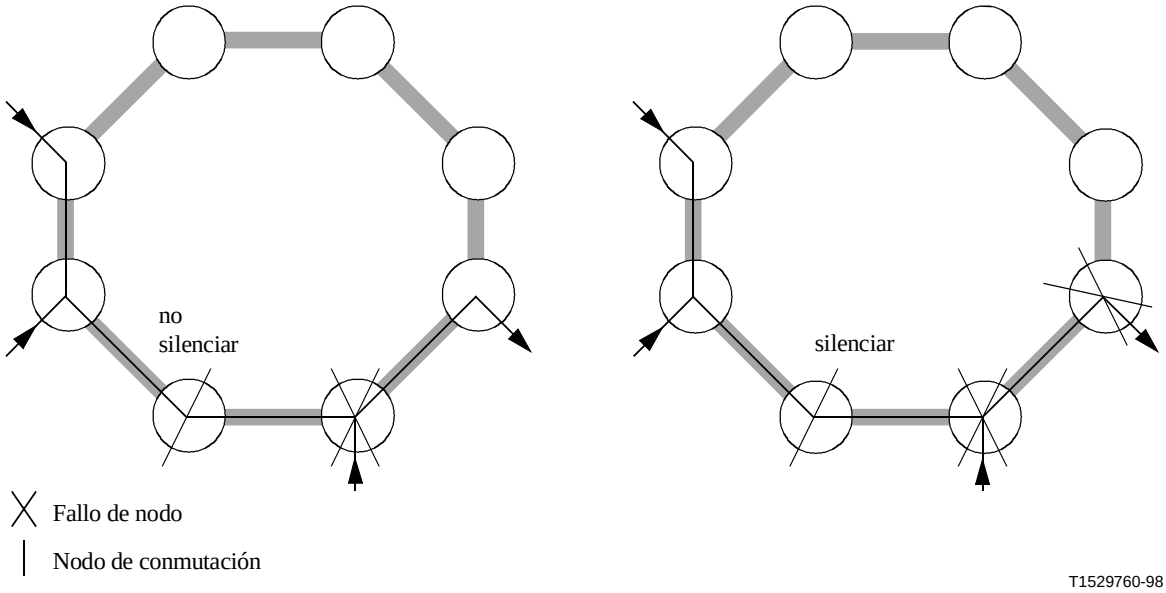



**Figura II.8/G.841 – Ejemplo de silencionamiento de circuito unidireccional originado de manera múltiple en el que el fallo se produce en el sentido del circuito unidireccional**

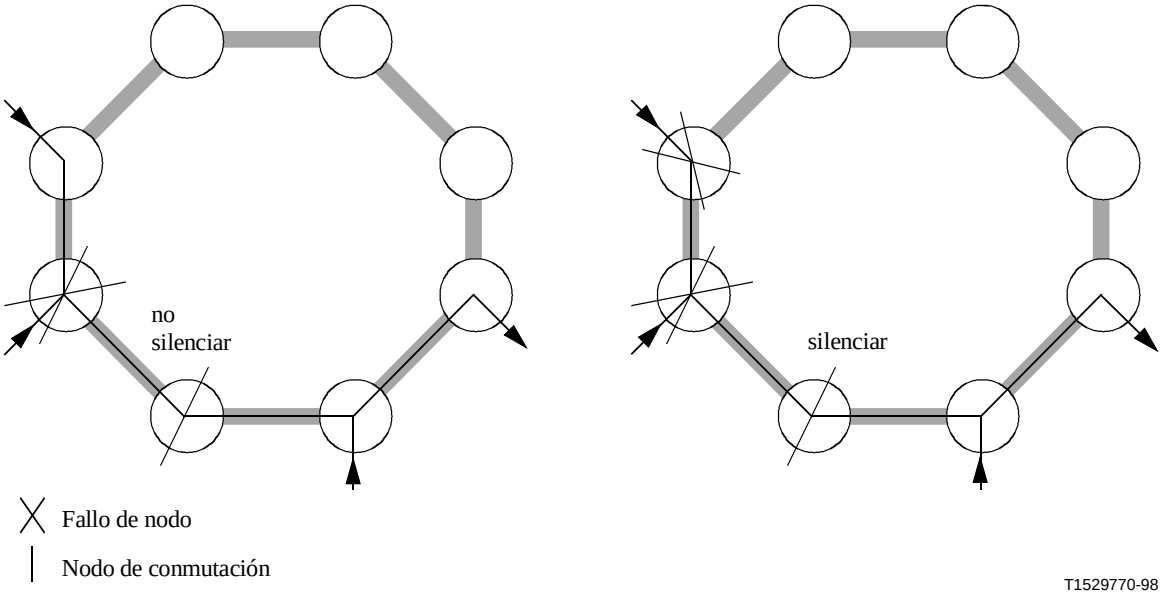



**Figura II.9/G.841 – Ejemplo de silencionamiento de circuito unidireccional originado de manera múltiple en el que el fallo se produce en el sentido opuesto al del circuito unidireccional**

## SERIES DE RECOMENDACIONES DEL UIT-T

| | |
|---|---|
| Serie A | Organización del trabajo del UIT-T |
| Serie B | Medios de expresión: definiciones, símbolos, clasificación |
| Serie C | Estadísticas generales de telecomunicaciones |
| Serie D | Principios generales de tarificación |
| Serie E | Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos |
| Serie F | Servicios de telecomunicación no telefónicos |
| **Serie G** | **Sistemas y medios de transmisión, sistemas y redes digitales** |
| Serie H | Sistemas audiovisuales y multimedios |
| Serie I | Red digital de servicios integrados |
| Serie J | Transmisiones de señales radiofónicas, de televisión y de otras señales multimedios |
| Serie K | Protección contra las interferencias |
| Serie L | Construcción, instalación y protección de los cables y otros elementos de planta exterior |
| Serie M | RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales |
| Serie N | Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión |
| Serie O | Especificaciones de los aparatos de medida |
| Serie P | Calidad de transmisión telefónica, instalaciones telefónicas y redes locales |
| Serie Q | Conmutación y señalización |
| Serie R | Transmisión telegráfica |
| Serie S | Equipos terminales para servicios de telegrafía |
| Serie T | Terminales para servicios de telemática |
| Serie U | Conmutación telegráfica |
| Serie V | Comunicación de datos por la red telefónica |
| Serie X | Redes de datos y comunicación entre sistemas abiertos |
| Serie Y | Infraestructura mundial de la información |
| Serie Z | Lenguajes de programación |