Unión Internacional de Telecomunicaciones

UIT-T G.873.1

(03/2006)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

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

Redes digitales – Redes ópticas de transporte

Red óptica de transporte: Protección lineal

Recomendación UIT-T G.873.1

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
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
CARACTERÍSTICAS DE LOS MEDIOS DE TRANSMISIÓN	G.600–G.699
EQUIPOS TERMINALES DIGITALES	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
Gestión de red de transporte	G.850–G.859
Integración de los sistemas de satélite y radioeléctricos con jerarquía digital síncrona	G.860–G.869
Redes ópticas de transporte	**G.870–G.879**
SECCIONES DIGITALES Y SISTEMAS DIGITALES DE LÍNEA	G.900–G.999
CALIDAD DE SERVICIO Y DE TRANSMISIÓN – ASPECTOS GENÉRICOS Y ASPECTOS RELACIONADOS AL USUARIO	G.1000–G.1999
CARACTERÍSTICAS DE LOS MEDIOS DE TRANSMISIÓN	G.6000–G.6999
DATOS SOBRE CAPA DE TRANSPORTE – ASPECTOS GENÉRICOS	G.7000–G.7999
ASPECTOS RELATIVOS AL PROTOCOLO ETHERNET SOBRE LA CAPA DE TRANSPORTE	G.8000–G.8999
REDES DE ACCESO	G.9000–G.9999

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

Recomendación UIT-T G.873.1

Red óptica de transporte: Protección lineal

Resumen

En esta Recomendación se describe el protocolo de conmutación automática de protección (APS) y el funcionamiento de la conmutación de protección aplicable a los métodos de protección lineal de la red óptica de transporte en el nivel de la unidad k de datos de canal óptico (ODUk). Se examinan los siguientes métodos de protección:

– protección de conexión de subred ODUk con supervisión inherente (1+1, 1:n);

– protección de conexión de subred ODUk con supervisión no intrusiva (1+1);

– protección de conexión de subred ODUk con supervisión de subcapa (1+1, 1:n).

Orígenes

La Recomendación UIT-T G.873.1 fue aprobada el 29 de marzo de 2006 por la Comisión de Estudio 15 (2005-2008) del UIT-T por el procedimiento de la Recomendación UIT-T A.8.

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 Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), 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 1 de la AMNT.

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 "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

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 no 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

Recomendación UIT-T G.873.1

Red óptica de transporte: Protección lineal

1 Alcance

En esta Recomendación se describe el protocolo de conmutación automática de protección (APS, *automatic protection switch*) y el funcionamiento de la conmutación de protección aplicables a los métodos de protección lineal de la red óptica de transporte en el nivel de la unidad k de datos de canal óptico (ODUk, *optical channel data unit*). Se examinan los siguientes métodos de protección lineal:

– protección de conexión de subred ODUk con supervisión inherente (1+1, 1:n);

– protección de conexión de subred ODUk con supervisión no intrusiva (1+1);

– protección de conexión de subred ODUk con supervisión de subcapa (1+1, 1:n).

El protocolo APS y el funcionamiento de la conmutación de protección para la protección de anillo de la red óptica de transporte (OTN, *optical transport network*) se encuentran en estudio.

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. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

– Recomendación UIT-T G.709/Y.1331 (2003), *Interfaces para la red óptica de transporte*.

– Recomendación UIT-T G.798 (2004), *Características de los bloques funcionales del equipo de la jerarquía de la red óptica de transporte*.

– Recomendación UIT-T G.805 (2000), *Arquitectura funcional genérica de las redes de transporte*.

– Recomendación UIT-T G.806 (2006), *Características del equipo de transporte – Metodología de descripción y funcionalidad genérica*.

– Recomendación UIT-T G.808.1 (2006), *Conmutación de protección genérica – Protección lineal de camino y subred*.

– Recomendación UIT-T G.841 (1998), *Tipos y características de las arquitecturas de protección para redes de la jerarquía digital síncrona*.

– Recomendación UIT-T G.872 (2001), *Arquitectura de las redes ópticas de transporte*.

3 Términos y definiciones

En esta Recomendación se definen los términos siguientes.

3.1 canal de conmutación automática de protección: Véase la Rec. UIT-T G.870/Y.1352.

3.2 entidad: Véase la Rec. UIT-T G.870/Y.1352.

3.3 señal de tráfico adicional: Véase la Rec. UIT-T G.870/Y.1352.

3.4 **extremo de cabecera**: Véase la Rec. UIT-T G.870/Y.1352.

3.5 **señal de tráfico normal**: Véase la Rec. UIT-T G.870/Y.1352.

3.6 **señal nula**: Véase la Rec. UIT-T G.870/Y.1352.

3.7 **canal de comunicación de protección**: Véase la Rec. UIT-T G.870/Y.1352.

3.8 **grupo de protección**: Véase la Rec. UIT-T G.870/Y.1352.

3.9 **señal**: Véase la Rec. UIT-T G.870/Y.1352.

3.10 **extremo de cola**: Véase la Rec. UIT-T G.870/Y.1352.

4 Abreviaturas, siglas o acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas, siglas o acrónimos.

APS Conmutación automática de protección (*automatic protection switching*)

DNR No revertir (*do not revert*)

EXER Ejercicio (*exercise*)

FS Conmutación forzada (*forced switch*)

LO Exclusión de protección (*lockout for protection*)

MS Conmutación manual (*manual switch*)

NR Ninguna petición (*no request*)

ODUk Unidad k de datos de canal óptico (*optical channel data unit k*)

OTN Red óptica de transporte (*optical transport network*)

OTUk Unidad k de transporte de canal óptico (*optical channel transport unit k*)

PCC Canal de comunicación de protección (*protection communication channel*)

RR Petición de revertir (*reverse request*)

SD Degradación de señal (*signal degrade*)

SF Fallo de señal (*signal fail*)

WTR Espera al restablecimiento (*wait to restore*)

5 Características de la protección

5.1 Métodos y condiciones de supervisión

La conmutación de protección se produce al detectar ciertos defectos de las entidades de transporte (principal y protección) dentro del dominio protegido. En las Recomendaciones de equipos (por ejemplo, Recs. UIT-T G.806 y G.798) se describe cómo se detectan estos defectos. Desde el punto de vista del controlador de la conmutación de protección, una entidad del dominio protegido puede estar en tres estados: sin defecto = OK, degradado (degradación de señal = SD) o fallo (fallo de señal = SF).

Los métodos de supervisión habituales son:

Inherente – La conmutación de protección se activa por defectos detectados en la conexión de enlace ODUk (por ejemplo, función de adaptación de cola de capa servidora y de servidor/ODUk). La detección del estado sin defecto se lleva a cabo en la propia capa ODUk.

NOTA – En contraste con la protección de conexión de subred con supervisión intrínseca (SNC/I, *subnetwork connection protection with inherent monitoring*) de la jerarquía digital síncrona (SDH, *synchronous digital hierarchy*), la SNC/I de ODUk puede abarcar sólo una conexión de enlace, ya que la indicación de defecto hacia adelante (FDI) resultante de otros defectos en la capa servidora en sentido hacia el origen no se detecta en la función de adaptación servidor/ODUk.

No intrusivo – La conmutación de protección se activa mediante una supervisión no intrusiva de la capa de unidad de nivel k de datos ópticos-trayecto (ODUkP, *optical data unit of level k, path*) o de las subcapas de la unidad de nivel k de datos ópticos-subcapa de conexión en cascada (ODUkT, *optical data unit of level k, tandem connection sub-layers*) en el extremo de cola del grupo de protección.

Subcapa – La conmutación de protección se activa por defectos detectados en el camino de subcapa de la ODUkT (supervisión de conexión en cascada (TCM, *tandem connection monitoring*)). Se establece un camino de subcapa ODUkT por cada entidad principal y de protección. Por consiguiente, la conmutación de protección se activa únicamente con defectos del dominio protegido.

El controlador de conmutación de protección no tiene que preocuparse del método de supervisión utilizado, siempre que se le proporcione información (OK, SD, SF) de las entidades de transporte en el dominio protegido. Es posible que algunos supervisores o capas de red no tengan un método para la detección de SD. Cuando éste sea el caso, no habrá necesidad de utilizar un protocolo APS distinto, ya que el equipo que no puede detectar la señal SD tampoco puede indicarla. Cuando se utilice el protocolo APS, la implementación no debe impedir que el extremo distante declare una SD por el canal APS, aunque el supervisor en el extremo cercano no pueda detectar SD.

6 Instrucciones en el grupo de protección

6.1 Instrucciones y estados extremo a extremo

En esta cláusula se describen las instrucciones que se aplican al grupo de protección en su totalidad. Cuando se utiliza el protocolo APS, las instrucciones se señalizan al extremo distante de la conexión. En el caso de la conmutación bidireccional, estas instrucciones se aplican al puente y al selector en ambos extremos.

Exclusión de protección – Esta instrucción impide que la entidad de protección transporte una señal principal. Esto inhabilita eficazmente el grupo de protección. Se interrumpe la transmisión de las señales de tráfico adicional que haya en la entidad de protección.

Conmutación forzada de la señal #n de tráfico normal a la protección – Obliga a la entidad de protección a seleccionar la señal #n de tráfico normal una vez activado el puente necesario.

Conmutación forzada de la señal nula – En el caso de las arquitecturas 1:n, conmuta la señal nula a la entidad de protección, a menos que esté en curso una instrucción de conmutación de protección de prioridad igual o superior. Si hubiera una señal de tráfico normal en la entidad de protección, se transfiere a su entidad principal para que se seleccione. En el caso de las arquitecturas 1+1, se elige la señal de tráfico normal de la entidad principal.

Conmutación forzada de la señal de tráfico adicional – Conmuta la señal de tráfico adicional a la entidad de protección, a menos que esté en curso una instrucción de conmutación de protección de prioridad igual o superior. Si hubiera una señal de tráfico normal en la entidad de protección se transfiere a su entidad principal para que se seleccione.

Conmutación manual de la señal #n de tráfico normal a la protección – Si no hay un fallo de una entidad principal o de protección, obliga a la entidad de protección a seleccionar la señal #n de tráfico normal una vez se dispone del puente.

Conmutación manual de la señal nula – En el caso de las arquitecturas 1:n, conmuta la señal nula a la entidad de protección, a menos que haya un fallo en otras entidades o que esté en curso una instrucción de conmutación de protección de prioridad igual o superior. Si hubiera una señal de tráfico normal en la entidad de protección se transfiere a su entidad principal para que se seleccione. En el caso de las arquitecturas 1+1, se selecciona la señal de tráfico normal de la entidad principal.

Conmutación manual de la señal de tráfico adicional – Conmuta la señal de tráfico adicional a la entidad de protección, a menos que haya una condición de fallo en otras entidades o que esté en curso una instrucción de conmutación de protección de prioridad igual o superior. Si hubiera una señal de tráfico normal en la entidad de protección se transfiere a su entidad principal para que se seleccione.

Espera al reestablecimiento de la señal #n de tráfico normal – En el modo funcionamiento reversible, después de borrar un SF o una SD de la entidad principal #n, mantiene la señal #n de tráfico normal seleccionada por la entidad de protección hasta que expira el temporizador "espera al restablecimiento". Si el temporizador expira antes de cualquier otro evento o instrucción, el estado cambiará a ausencia de petición (NR, *no request*). Esto se utiliza para evitar el funcionamiento frecuente del selector en el caso de fallos intermitentes.

Ejercicio de la señal #n – Ejercicio del protocolo APS. Se elige la señal de manera que no se modifique el selector.

No revertir señal #n de tráfico normal – En el modo de funcionamiento no reversible, se utiliza para mantener una señal de tráfico normal seleccionada por la entidad de protección.

Ninguna petición – Se eligen todas las señales de tráfico normales de sus correspondientes entidades de transporte principales. La entidad de protección transporta la señal nula, el tráfico adicional o un puente de la señal de tráfico normal simple en un grupo de protección 1+1.

Borrar – Borra la exclusión de protección de extremo cercano activa, la conmutación forzada, la conmutación manual, el estado WTR, o la instrucción ejercicio.

6.2 Instrucciones locales

Estas instrucciones se aplican únicamente al extremo cercano del grupo de protección. Cuando se utiliza el protocolo APS, no se señalizan las instrucciones al extremo distante a través del canal APS.

Congelar – Congela el estado del grupo de protección. Mientras no se borre la congelación, se rechazan las instrucciones de extremo cercano adicionales. Se ignoran los cambios de estado y los octetos APS recibidos. Cuando se borra la instrucción de congelación, el estado del grupo de protección se recalcula basándose en el estado y en los bytes APS recibidos.

Borrar congelación

Exclusión de la señal #n de tráfico normal de la protección – Impide que la entidad de protección seleccione la señal #n de tráfico normal. Las instrucciones para la señal #n de tráfico normal se rechazan. Se ignorarán las condiciones SF o SD para la señal #n de tráfico normal. En el caso de la conmutación 1:n bidireccional se seguirán aceptando las peticiones de puenteo distantes para la señal #n de tráfico normal a fin de evitar fallos de protocolo. Por esta razón, se debe excluir la protección de la señal de tráfico normal en ambos extremos para evitar que la entidad de protección la seleccione como consecuencia de una instrucción o fallo en cualquier extremo. Es posible la coexistencia de múltiples de estas instrucciones para distintas señales de tráfico normal.

Despejar la exclusión de la señal #n de tráfico normal de la protección.

7 Arquitecturas de protección

En una arquitectura de protección lineal, la conmutación de protección se produce en los dos puntos extremos de un camino protegido o conexión de subred protegida. Entre estos puntos extremo, habrá entidades "principales" y de "protección".

Para un determinado sentido de transmisión, el "extremo de cabecera" de la señal protegida tiene capacidad para llevar a cabo la función de puenteo, mediante la cual colocará una copia de la señal de tráfico normal en la entidad de protección cuando sea necesario. El "extremo de cola" se encargará de la función del selector, que consiste en seleccionar una señal de tráfico normal de su entidad principal o una entidad de protección. En el caso de transmisión bidireccional, con protección en ambos sentidos de transmisión, los dos extremos de la señal protegida llevarán a cabo normalmente funciones de puenteo y de selección.

Las siguientes arquitecturas son posibles:

1+1 – En una arquitectura 1+1, se protege una sola señal de tráfico normal mediante una sola entidad de protección. El puenteo en el extremo de cabecera es permanente. La conmutación se produce únicamente en el extremo de cola.

1:n – En una arquitectura 1:n, se protegen una o más señales de tráfico normal mediante una sola entidad de protección. El puenteo en el extremo de cabecera no se establece hasta que se solicita la conmutación de protección. En el caso $n > 1$, no se puede saber cuál de las señales de tráfico normales se debe puentear a la entidad de protección hasta que se detecta un defecto en una de las señales protegidas. Las arquitecturas 1:n tienen capacidad para transportar una señal de tráfico adicional (de baja prioridad, reemplazable) sobre la entidad de protección cuando no se utiliza para proteger alguna señal de tráfico normal. Se puede utilizar una arquitectura 1:n aun para $n = 1$(1:1). En este caso podría seleccionarse la arquitectura 1+1 que es más simple (la cual no requiere acciones del algoritmo de protección en el extremo de cabecera) ya que la arquitectura 1:1 puede transportar tráfico adicional, mientras que la arquitectura 1+1 no tiene esa capacidad.

m:n – En esta arquitectura, se utilizan m entidades de protección para proteger a n entidades principales. Esto queda en estudio.

Con la suposición de un canal APS más grande, la codificación de la entidad número "n" utilizará un byte completo en lugar de sólo unos pocos bits como en SDH. Se reservan dos de los 256 valores: se utiliza 0 para indicar una señal nula o la entidad de protección, y 0xFF (255) para indicar tráfico adicional.

La arquitectura en cada extremo de la conexión tiene que concordar.

7.1 Conmutación unidireccional y bidireccional

En el caso de transmisión bidireccional, es posible seleccionar conmutación unidireccional o bidireccional. En la conmutación unidireccional, los selectores en cada extremo son completamente independientes. En la conmutación bidireccional, se intenta coordinar los dos extremos de manera que ambos tengan la misma configuración de puenteo y de selección, aun en el caso de un fallo unidireccional. La conmutación bidireccional requiere siempre de un canal APS y/o un canal de comunicación de protección (PCC, *protection communication channel*) para coordinar los dos puntos extremo. La conmutación unidireccional puede proteger dos fallos unidireccionales en sentidos opuestos producidos en distintas entidades.

7.2 Necesidad de un canal APS/PCC

El único tipo de conmutación que NO requiere un canal APS y/o PCC es la conmutación unidireccional 1+1. Con un puente permanente en el extremo de cabecera y al no haber necesidad de coordinar las posiciones del selector en los dos extremos, el selector del extremo de cola puede controlarse completamente de acuerdo con los defectos y a las instrucciones que reciba.

La conmutación bidireccional siempre requiere un canal APS. La conmutación unidireccional 1:n necesita un canal APS para coordinar el puente del extremo de cabecera con el selector del extremo de cola.

7.3 Conmutación reversible y no reversible

En funcionamiento reversible, se restablece el tráfico a las entidades principales después de que haya pasado la causa de la conmutación. En el caso de borrado de una instrucción (por ejemplo conmutación forzada), el restablecimiento es inmediato. En el caso de borrado de un defecto, el restablecimiento sucede, por lo general, después de la expiración de un temporizador "espera al restablecimiento", que se utiliza para evitar el tableteo de los selectores en caso de defectos intermitentes.

En el modo de funcionamiento no reversible, se permite que el tráfico normal permanezca en la entidad de protección aun después de que haya pasado la causa de la conmutación. Por lo general, esto se lleva a cabo sustituyendo la petición de conmutación anterior con una petición de "no revertir (DNR, *do not revert*)", la cual tiene baja prioridad.

La protección 1+1 se configura a menudo en modo no reversible, ya que de todas las maneras no se utiliza para otra función, y se evita así un segundo "problema técnico" en el tráfico. Sin embargo, puede haber razones para configurar esta protección como reversible (por ejemplo, de manera que el tráfico utilice el sentido "corto" en un anillo salvo en situaciones de fallo. Las políticas de algunos operadores incluyen también el funcionamiento con inversión aun para la arquitectura 1+1).

Generalmente, la protección 1:n es reversible. Desde luego, en el caso de que se transporta una señal de tráfico adicional sobre la entidad de protección, el funcionamiento será siempre reversible para que se pueda restablecer la señal de tráfico adicional con prioridad. Es posible definir el protocolo de modo que permita el modo de funcionamiento no reversible en la protección 1:n, pero se considera mejor utilizar el modo reversible y restablecer el tráfico una vez reparada la entidad principal que esperar a que falle alguna otra entidad en el grupo y se necesite emplear la entidad de protección para transportar una señal de tráfico normal distinta.

En general, la elección de reversible o no reversible será la misma en ambos extremos del grupo de protección. No obstante, una discordancia de este parámetro no impide el interfuncionamiento, simplemente será peculiar que un lado pase a WTR para borrar las conmutaciones iniciadas en ese lado, mientras que el otro pase a DNR para las propias. Véase también 8.4.

7.4 Discordancias de configuración

Con todas las opciones de configuración en los grupos de protección, existe la posibilidad de que haya discordancias entre las configuraciones en los dos extremos. Estas discordancias pueden tomar algunas de las siguientes formas:

- Discordancias que impiden el buen funcionamiento.
- Discordancias en las que uno de los extremos puede adaptar su funcionamiento para proporcionar un grado de interfuncionamiento.
- Discordancias que no impiden el interfuncionamiento. Por ejemplo, la discordancia reversible/no reversible examinada en 8.4.

En la información que pasa por el canal APS no puede transportar y detectar todas las discordancias de configuración. Son posibles hasta 254 entidades principales en un grupo de protección 1:n, por lo que hay demasiadas combinaciones de números de entidad válidos para disponer fácilmente de una visión completa de todas las opciones de configuración. Sin embargo, conviene tener una visión de la categoría intermedia, cuando ambos extremos pueden adaptar su operación para interfuncionar a pesar de la discordancia. Por ejemplo, un equipo configurado para conmutación bidireccional podría pasar a conmutación unidireccional para facilitar el interfuncionamiento. Un equipo configurado

para conmutación 1+1 con un canal APS podría pasar al funcionamiento con conmutación unidireccional 1+1 sin canal APS. Si bien se podría seguir informando al usuario de la discordancia de configuración, el equipo podría continuar proporcionando cierto nivel de protección.

8 Protocolo APS

8.1 Formato del canal APS

El canal APS se transporta sobre los primeros tres bytes del campo APS/PCC de la tara ODUk. El cuarto byte del campo APS/PCC está reservado. Se dispone de ocho canales APS independientes para soportar la protección en la ODUkP, seis niveles ODUkT (TCM) y un nivel de SNC/I ODUk como se define en 15.8.2.4/G.709/Y.1331.

En la figura 1 se define el formato de los cuatro bytes APS de cada trama. En el cuadro 1 se definen los valores de campo de los canales APS.

1								2								3								4							
1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
Petición/ estado				Tipo de protección				Señal solicitada								Señal puenteada								Reservado							
				A	B	D	R																								

Figura 1/G.873.1 – Formato del canal APS

Cuadro 1/G.873.1 – Valores de los campos en el canal APS

Campo		Valor	Descripción
Petición/estado		1111	Exclusión de protección (LO)
		1110	Conmutación forzada (FS)
		1100	Fallo de señal (SF)
		1010	Degradación de señal (SD)
		1000	Conmutación manual (MS)
		0110	Espera al restablecimiento (WTR)
		0100	Ejercicio (EXER)
		0010	Petición de revertir (RR)
		0001	No revertir (DNR)
		0000	Ninguna petición (NR)
		Otros	Reservado para normalización internacional futura
Tipo de protección	A	0	Sin canal APS
		1	Canal APS
	B	0	1+1 (puente permanente)
		1	1:n (sin puente permanente)
	D	0	Conmutación unidireccional
		1	Conmutación bidireccional
	R	0	Funcionamiento reversible
		1	Funcionamiento no reversible
Señal solicitada		0	Señal nula
		1-254	Señal de tráfico normal 1-254
		255	Señal de tráfico adicional
Señal puenteada		0	Señal nula
		1-254	Señal de tráfico normal 1-254
		255	Señal de tráfico adicional

8.2 Transmisión y aceptación del protocolo APS

El protocolo APS/PCC se transmite por la entidad de protección. Aunque también se podría transmitir de la misma manera sobre las entidades principales, los receptores no lo suponen de esa manera, y deben ser capaces de hacer caso omiso de esta información cuando se transmite por las entidades principales.

Se realiza un proceso de aceptación independiente para cada uno de los ocho niveles. Como el protocolo APS se transporta en los primeros tres de los cuatro bytes de APS/PCC, sólo se tienen en cuenta estos tres bytes en el proceso de aceptación. Se aceptará un nuevo valor de protocolo APS si se recibe un valor idéntico en esos tres bytes tres veces en forma consecutiva de un nivel determinado.

NOTA – Como el cuarto byte del mensaje APS está 'reservado' no es necesario tenerlo en cuenta durante el proceso de aceptación de los bytes APS.

8.3 Tipo de petición

Los tipos de petición que pueden aparecer en los bytes APS son los tipos "normales" soportados tradicionalmente por la conmutación de protección de la red óptica síncrona (SONET, *synchronous optical network*) y de SDH. Estas peticiones indican la condición, instrucción o estado de la prioridad más alta (véanse los cuadros 2 y 3). En el caso de la conmutación unidireccional, éste es el valor de prioridad más alto determinado únicamente en el extremo cercano. En la conmutación bidireccional, se indicará petición local sólo en el caso de que la prioridad sea igual o más alta que cualquier petición recibida del extremo distante por el canal APS. En el caso de conmutación bidireccional, cuando la petición del extremo distante tiene la prioridad más alta, el extremo cercano indicará petición de revertir.

Cuadro 2/G.873.1 – Prioridades de petición/estado cuando se utiliza el protocolo APS

Petición/estado	Prioridad
Exclusión de protección (LO)	1 (la más alta)
Fallo de señal (SF) – protección	2 (véase 8.9)
Conmutación forzada (FS)	3
Fallo de señal (SF) – principal	4
Degradación de señal (SD)	5
Conmutación manual (MS)	6
Espera al restablecimiento (WTR)	7
Ejercicio (EXER)	8
Petición de revertir (RR)	9
No revertir (DNR)	10
Ninguna petición (NR)	11 (la más baja)

Cuadro 3/G.873.1 – Prioridades de petición/estado sin utilizar protocolo APS

Petición/estado	Prioridad
Exclusión de protección (LO)	1 (la más alta)
Conmutación forzada (FS)	2
Fallo de señal (SF)	3
Degradación de señal (SD)	4
Conmutación manual (MS)	5
Espera al restablecimiento (WTR)	6
No revertir (DNR)	7
Ninguna petición (NR)	8 (la más baja)

8.4 Tipos de protección

Los tipos de protección válidos son:

000x Unidireccional 1+1 sin APS

100x Unidireccional 1+1 con APS

101x Bidireccional 1+1 con APS

110x Unidireccional 1:n con APS

111x Bidireccional 1:n con APS

Los valores se eligen de tal manera que el valor por defecto (todos ceros) concuerde con el único tipo de protección que puede funcionar sin APS (unidireccional 1+1).

Obsérvese que no son válidos 010x, 001x y 011x ya que la protección 1:n y el funcionamiento bidireccional requieren APS.

Si no concuerda el bit "B", se libera el selector ya que 1:n y 1+1 son incompatibles. Esto generará una alarma.

En el caso de que concuerde el bit "B":

Si concuerda el bit "A", el extremo en espera de APS pasará a la conmutación unidireccional 1+1 sin APS.

NOTA 1 – Cuando un nodo no soporte el canal APS, el campo APS/PCC tendrá un patrón todos "0" como se especifica en la cláusula 15/G.709/Y.1331.

Si no concuerda el bit "D", el extremo bidireccional pasará a la conmutación unidireccional.

Si no concuerda el bit "R", un extremo despejará los conmutadores a "WTR" y el otro despejará a "DNR". Los dos lados interfuncionarán y el tráfico estará protegido.

NOTA 2 – Cada extremo señaliza siempre sus capacidades máximas en el campo tipo de protección aun en el caso de que pase a funcionar con menos capacidades (es decir, un extremo que soporta conmutación bidireccional pasa al modo de funcionamiento con conmutación unidireccional en el caso de interfuncionamiento con un extremo que soporta únicamente conmutación unidireccional, pero continúa señalizando "1" en el bit "D").

NOTA 3 – El informe de discordancias queda en estudio.

8.5 Señal solicitada

Indica la señal solicitada por el extremo cercano que debe transportarse por la entidad de protección. En el caso de NR, se trata de la señal nula (0) o del tráfico adicional (255). En el caso de LO, sólo puede tratarse de la señal nula (0). En el caso de ejercicio, puede tratarse de la señal nula (0) o de la señal de tráfico adicional (255) cuando ejercicio sustituye a NR, o el número de una señal de tráfico normal en el caso de que ejercicio sustituya a DNR. En el caso de SF o SD, será el número de una señal de tráfico normal o la señal nula (0) para indicar que la protección ha fallado o se ha degradado. Para el resto de las peticiones será el número de la señal de tráfico normal solicitada que se debe transportar por la entidad de protección.

8.6 Señal puenteada

Indica la señal que se ha puenteado en la entidad de protección. En el caso de la protección 1+1, esto debería indicar siempre la señal de tráfico normal 1, indicando así con precisión el puenteo permanente. Esto permite una conmutación de dos fases en lugar de tres en el caso de la arquitectura 1+1. Para la protección 1:n, esto indicará lo que realmente está puenteado a la entidad de protección (ya sea la señal nula (0), el tráfico adicional (255) o el número de una señal de tráfico normal). Por lo general, esto será el puenteo solicitado por el extremo distante.

8.7 Control del puenteo

En las arquitecturas 1+1, la señal de tráfico normal está permanentemente puenteada a la protección. La señal de tráfico normal número "1" se indicará siempre en el campo señal puenteada del canal APS.

En las arquitecturas 1:n, el puente se fijará conforme a lo indicado en el campo "señal solicitada" del canal APS entrante. Una vez establecido el puente, esto se indicará en el campo "señal puenteada" del canal APS saliente.

8.8 Control del selector

En la arquitectura unidireccional 1+1 (con o sin APS), el selector se configura de acuerdo a la petición local con la prioridad más alta. Se trata de una conmutación de una sola fase.

En la arquitectura bidireccional 1+1, la señal de tráfico normal se elige de la entidad de protección cuando la "señal solicitada" saliente y la "señal puenteada" entrante indican ambas señal de tráfico normal "1" (en esta arquitectura, la "señal puenteada" entrante siempre debería indicar "1"). Se trata de una conmutación de dos fases, ya que el extremo distante no conmuta hasta que recibe los bytes APS indicando que el extremo cercano inició una conmutación bidireccional.

En las arquitecturas unidireccional o bidireccional 1:n, se selecciona una señal de tráfico normal "n" o una señal de tráfico adicional 255 de la entidad de protección cuando aparece el mismo número "n" (o 255) en ambos campos "señal solicitada" saliente y "señal puenteada" entrante. Generalmente, esto da lugar a una conmutación de tres fases.

8.9 Fallo de señal de la entidad de protección

Un fallo de señal en la entidad de protección tiene una prioridad más alta que cualquier defecto que pudiese provocar la elección de una señal de transporte normal desde la entidad de protección. En el caso de que se esté utilizando una señal APS, una condición SF en la entidad de protección (sobre la que está encaminada la señal APS) tiene prioridad sobre la conmutación forzada. Una instrucción de exclusión tiene prioridad más alta que SF. Durante las condiciones de fallo se mantendrá activo el estado de exclusión.

8.10 Peticiones de prioridad equivalente

En general, una vez que se ha llevado a cabo una conmutación debido a una petición, no podrá anularse mediante otra petición con la misma prioridad (método por orden de petición). Cuando se reciben simultáneamente dos peticiones con la misma prioridad, el conflicto se resuelve en favor de la petición con el número de entidad más bajo. En el caso de conmutación bidireccional, una petición que se recibe por el canal APS con el número de entidad más bajo siempre anulará a una petición local con idéntica prioridad y con un número de entidad más alto. Las peticiones con prioridad equivalente para el mismo número de entidad desde ambos extremos de un grupo de protección bidireccional se consideran válidas, y desde el punto de vista de procesamiento de extremo cercano es equivalente a recibir "RR".

8.11 Aceptación y retención de instrucciones

Las instrucciones CLEAR (DESPEJAR), LO, FS, MS y EXER se aceptan o rechazan en función de instrucciones previas, del estado de las entidades principales y de protección del grupo de protección, y (únicamente en la conmutación bidireccional) de los bytes APS recibidos.

La instrucción CLEAR sólo es válida si está en curso una instrucción LO, FS, MS o EXER de extremo cercano o si existe un estado WTR en el extremo cercano o de lo contrario se rechaza. Esta instrucción suprimirá la instrucción de extremo cercano o el estado WTR, permitiendo que se imponga la siguiente condición de menor prioridad o (en la conmutación bidireccional) la petición APS.

El resto de las instrucciones se rechazan a menos que tengan una prioridad más alta que la instrucción, condición o (en la conmutación bidireccional) petición APS existente previamente. Si se acepta una nueva instrucción, se descarta cualquier instrucción previa con prioridad baja anulada. Si una instrucción con prioridad más alta anula una condición con prioridad baja o (en la conmutación bidireccional) una petición APS, esta otra petición se vuelva a imponer si aún existe en el momento de borrar la instrucción.

Si una condición o (en la conmutación bidireccional) una petición APS anula una instrucción, esta última se descarta.

8.12 Temporizador de espera

Es posible que se requiera un temporizador de espera para coordinar la temporización de los conmutadores de protección en múltiples capas o a través de los dominios de protección en cascada. La finalidad es permitir que un conmutador de protección de capa servidora tenga la oportunidad de resolver el problema antes de que se produzca la conmutación en una capa cliente, o para permitir la conmutación de un dominio de protección en sentido hacia el origen antes que la del dominio en sentido hacia el destino (por ejemplo, para permitir la conmutación de un anillo en sentido hacia el origen antes de la conmutación del anillo en sentido hacia el destino en una configuración de interconexión de nodos duales de modo que la conmutación se produzca en el mismo anillo en el que ocurrió el fallo).

Cada grupo de protección debe tener un temporizador de espera configurable. La gama y valores sugeridos son 0, 20 ms y 100 ms a 10 segundos en pasos de 100 ms (precisión de ±5 ms de acuerdo con la Rec. UIT-T G.808.1).

El funcionamiento del temporizador de espera utiliza el método "doble examen" especificado en las normas de SDH. Específicamente, cuando se presenta un nuevo defecto o un defecto más grave (nuevo SD o SF, o SD que se convierte en SF), el evento no será informado inmediatamente a la conmutación de protección si el valor del temporizador de espera configurado es diferente de cero. Por el contrario, se inicia el temporizador de espera. Cuando éste expira, se verifica si el defecto aún existe en el camino que activó el temporizador. Si aún existe, el defecto se informa a la conmutación de protección. El defecto no necesariamente es el mismo que inició el temporizador.

8.13 Modo ejercicio

Ejercicio es una instrucción que permite probar si el canal APS funciona correctamente. Tiene una prioridad más baja que cualquier petición de conmutación "real". Esta instrucción es válida únicamente en la conmutación bidireccional, ya que es la única situación en la que se puede llevar a cabo una prueba significativa si se espera una respuesta.

La instrucción ejercicio emitirá la instrucción con los mismos números de entidad solicitada y puenteada de la petición NR o DNR a la cual sustituye. La respuesta válida será una RR con los números de entidad solicitada y puenteada correspondientes. Para poder detectar la RR, la respuesta normal a DNR debería ser DNR en lugar de RR. Cuando se borra la instrucción ejercicio, se sustituirá con NR si el número de entidad solicitada es 0 ó 255, y con DNR para cualquier número de señal de tráfico normal 1 a 254.

NOTA – El funcionamiento de la instrucción ejercicio se ha definido de manera distinta para la red óptica de transporte (OTN, *optical transport network*) y para el sistema SDH.

8.14 Alarmas en el canal APS

Las situaciones de "fallo del protocolo" de los grupos que requieren APS son:

– Configuración totalmente incompatible (discordancia del bit "B"), descrita en 8.4.

– Ausencia de respuesta a una petición de puenteo (es decir, no hay concordancia entre la "entidad solicitada" enviada y la "entidad puenteada" recibida) durante > 50 ms.

Se ignorará la recepción de una petición desconocida o de una petición de un número de entidad que no es válido. Será responsabilidad del extremo distante generar una alarma cuando no hay respuesta del extremo cercano.

Apéndice I

Ejemplos de funcionamiento

I.1 Conmutación unidireccional 1+1

El protocolo APS puede o no utilizarse. Aun cuando no se utilice, se supone que el puenteo es permanente, de modo que las conmutaciones se pueden llevar a cabo inmediatamente de acuerdo con la petición local. Si hay bytes APS, son únicamente de tipo informativo y no controlan el funcionamiento del grupo de protección. Si los hay, el equipo puede permitir una consulta del estado del extremo distante.

En este ejemplo se ilustra la superposición de las peticiones SF y SD desde extremos opuestos. El ejemplo en la figura I.1 muestra con fines ilustrativos una configuración discordante donde el extremo A es no reversible mientras que el extremo B es reversible.

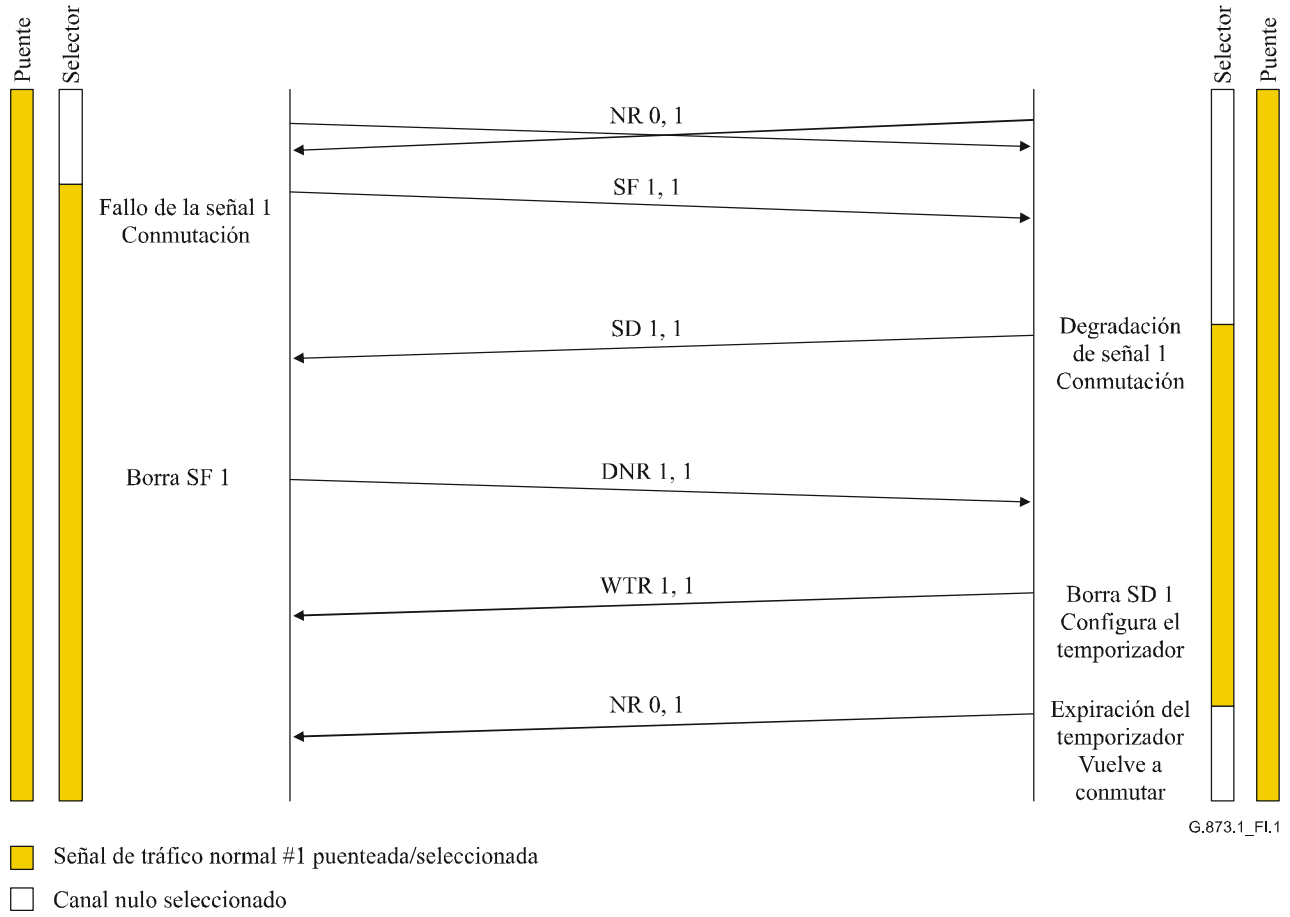

Figura I.1/G.873.1 – Ejemplo de flujo del mensaje APS en el caso de conmutación unidireccional 1+1

I.2 Conmutación bidireccional 1+1

El ejemplo en la figura I.2 ilustra una conmutación no reversiva, bidireccional 1+1. Dado que en los bytes APS se indica desde el principio la condición de puenteo permanente, la conmutación puede tener dos fases en lugar de tres.

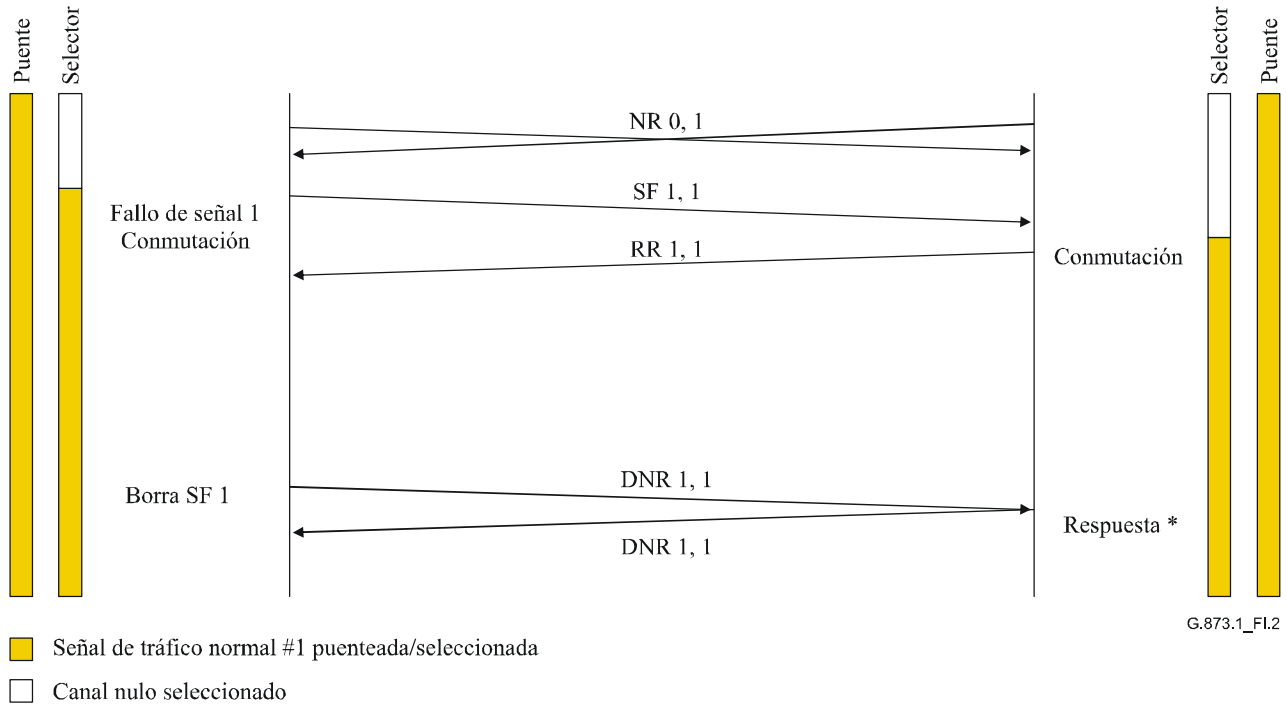

Figura I.2/G.873.1 – Ejemplo de flujo del mensaje APS en el caso de conmutación bidireccional 1+1

NOTA – Tradicionalmente se acusaba recibo de DNR con RR. Ahora, la respuesta a DNR con DNR no introduce ninguna diferencia fundamental en los estados de los dos extremos, y permite la implementación de un ejercicio significativo.

I.3 Conmutación bidireccional 1:n

En la figura I.3 se muestra un ejemplo de conmutación bidireccional 1:n con tráfico adicional (TA). Lo que realmente se ilustra es el caso en el que un SF en la entidad principal #3 sustituye a una SD en la entidad principal #2.

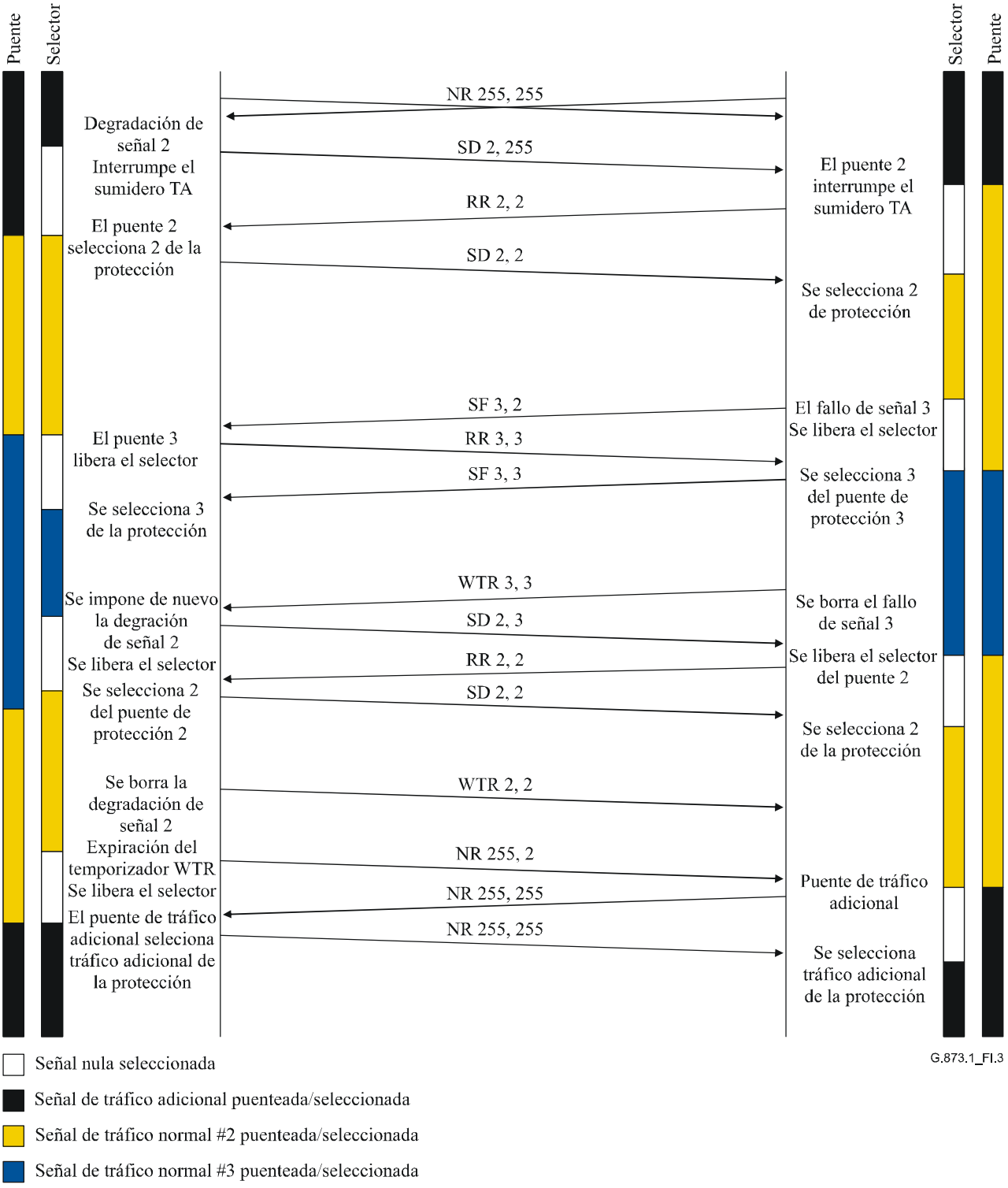

Figura I.3/G.873.1 – Ejemplo de flujo del mensaje APS en el caso de conmutación bidireccional 1:n

I.4 Funcionamiento de la instrucción ejercicio

La instrucción ejercicio es una prueba a la que responde el extremo distante al recibir una petición de canal APS, cuando se utiliza conmutación bidireccional, sin hacer funcionar el selector. Esta instrucción es de prioridad baja para que no interfiera con el funcionamiento del grupo de protección. Es válida únicamente cuando la petición actual es NR o DNR, ya que tiene prioridad más baja que el resto de las peticiones.

En las figuras I.4, I.5, I.6 y I.7 se dan ejemplos del funcionamiento de la instrucción ejercicio. En ningún caso se modifican los números de entidad solicitada y puenteada por la instrucción ejercicio. La recepción de "RR" con el mismo número de entidad es una respuesta positiva. Obsérvese que la recepción de DNR al enviar DNR es una manera de probar que la instrucción ejercicio recibe la respuesta RR apropiada.

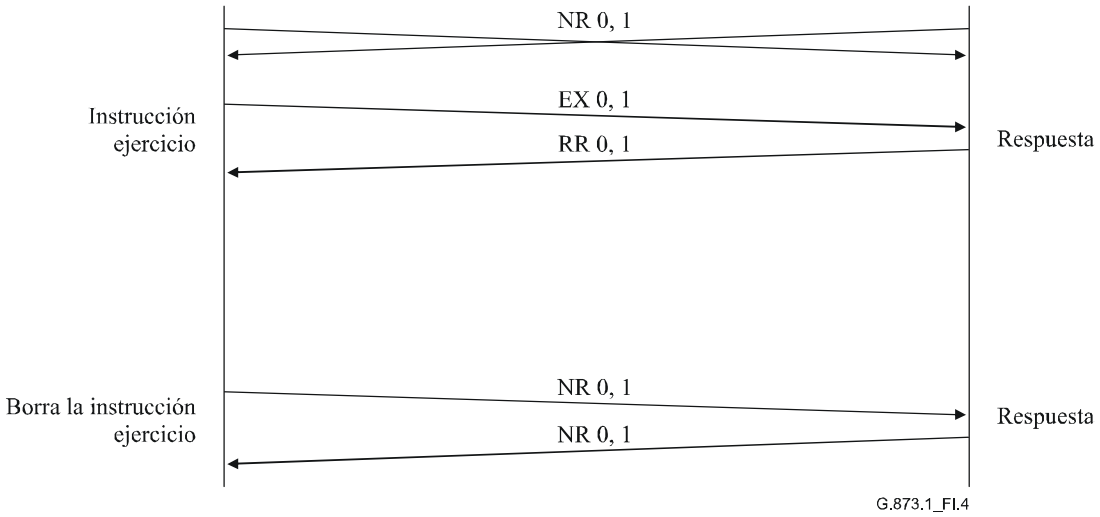

Figura I.4/G.873.1 – Ejemplo de la instrucción ejercicio partiendo del estado NR 1+1

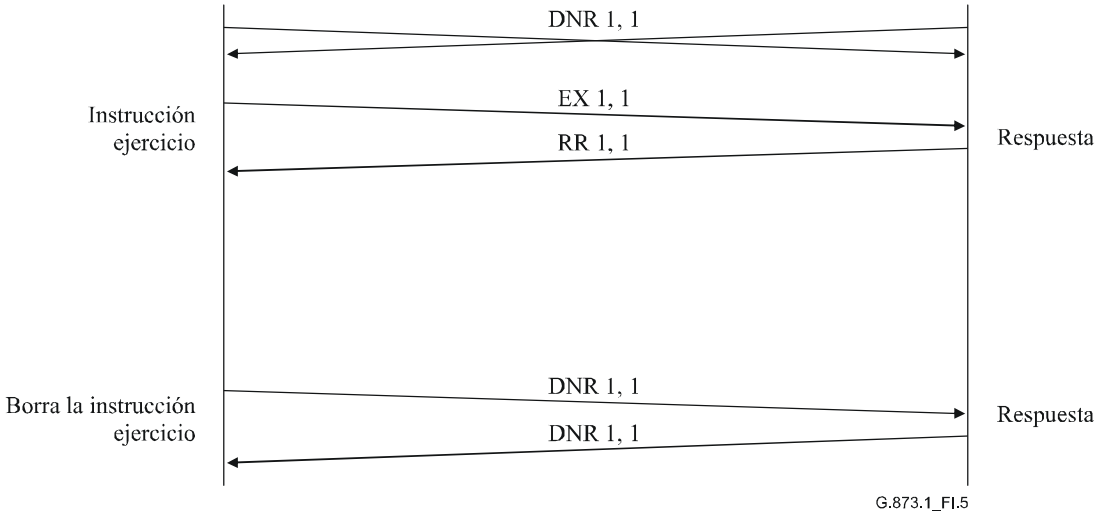

Figura I.5/G.873.1 – Ejemplo de la instrucción ejercicio partiendo del estado DNR 1+1

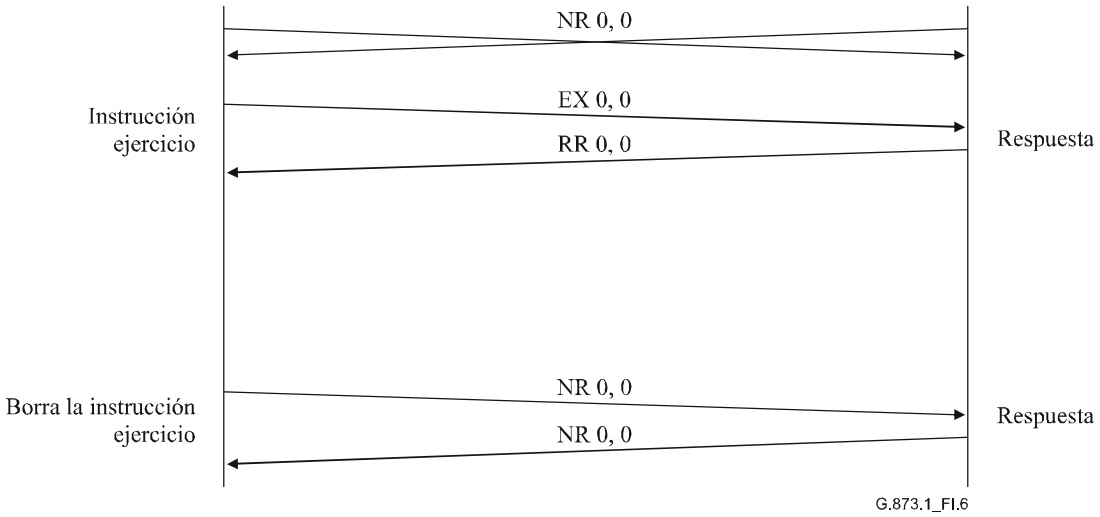

Figura I.6/G.873.1 – Ejemplo de la instrucción ejercicio partiendo del estado NR 1:n sin tráfico adicional

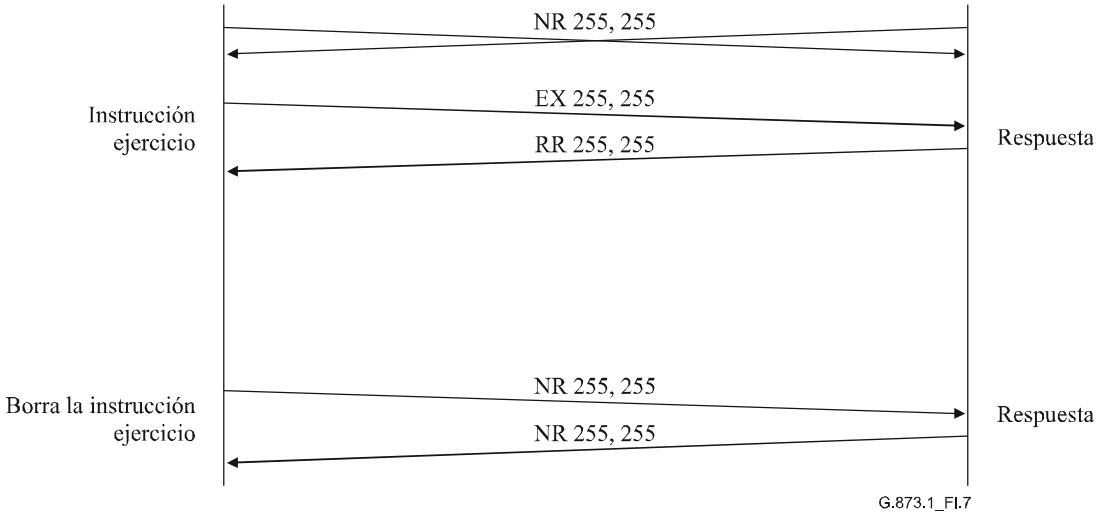

Figura I.7/G.873.1 – Ejemplo de la instrucción ejercicio partiendo del estado NR 1:n con tráfico adicional

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
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	Redes de cable y transmisión de programas radiofónicos y televisivos, 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	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
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, comunicaciones de sistemas abiertos y seguridad
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet y Redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2006