UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T Y.1720

(04/2003)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE Y: INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN Y ASPECTOS DEL PROTOCOLO INTERNET

Aspectos del protocolo Internet – Operaciones, administración y mantenimiento

Conmutación de protección para redes con conmutación por etiquetas multiprotocolo

Recomendación UIT-T Y.1720

RECOMENDACIONES UIT-T DE LA SERIE Y

INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN Y ASPECTOS DEL PROTOCOLO INTERNET

INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN	
Generalidades	Y.100–Y.199
Servicios, aplicaciones y programas intermedios	Y.200–Y.299
Aspectos de red	Y.300–Y.399
Interfaces y protocolos	Y.400–Y.499
Numeración, direccionamiento y denominación	Y.500–Y.599
Operaciones, administración y mantenimiento	Y.600–Y.699
Seguridad	Y.700–Y.799
Características	Y.800–Y.899
ASPECTOS DEL PROTOCOLO INTERNET	
Generalidades	Y.1000–Y.1099
Servicios y aplicaciones	Y.1100–Y.1199
Arquitectura, acceso, capacidades de red y gestión de recursos	Y.1200–Y.1299
Transporte	Y.1300–Y.1399
Interfuncionamiento	Y.1400–Y.1499
Calidad de servicio y características de red	Y.1500–Y.1599
Señalización	Y.1600–Y.1699
Operaciones, administración y mantenimiento	**Y.1700–Y.1799**
Tasación	Y.1800–Y.1899

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

Recomendación UIT-T Y.1720

Conmutación de protección para redes con conmutación por etiquetas multiprotocolo

Resumen

Esta Recomendación describe los requisitos y mecanismos de la funcionalidad de conmutación de protección 1+1 y 1:1 en el plano usuario de las redes con conmutación por etiquetas multiprotocolo (MPLS). El mecanismo que se describe aquí está destinado a proteger trayectos conmutados por etiquetas (LSP) punto a punto y de extremo a extremo. La funcionalidad de conmutación de protección del LSP en los modos multipunto a punto y punto a multipunto queda en estudio. La conmutación de protección en el modo m:n también queda en estudio. La conmutación de protección sin errores se considera fuera del alcance de esta versión de la Recomendación.

Orígenes

La Recomendación UIT-T Y.1720 fue aprobada por la Comisión de Estudio 13 (2001-2004) del UIT-T por el procedimiento de la Recomendación UIT-T A.8 el 6 de abril de 2003.

Palabras clave

Conmutación de protección, defecto, fallo, LSP, MPLS, PML, PSL, reencaminamiento.

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 Y.1720

Conmutación de protección para redes con conmutación por etiquetas multiprotocolo

1 Alcance

Esta Recomendación describe los requisitos y mecanismos de la funcionalidad de conmutación de protección 1+1 y 1:1 en el plano usuario de las redes con conmutación por etiquetas multiprotocolo (MPLS, *multi-protocol label switching*). El mecanismo que se describe aquí está destinado a proteger trayectos conmutados por etiquetas (LSP, *label switched path*) punto a punto y de extremo a extremo. La funcionalidad de conmutación de protección del LSP en los modos multipunto a punto y punto a multipunto queda en estudio. La conmutación de protección en el modo m:n también queda en estudio. La conmutación de protección sin errores se considera fuera del alcance de esta versión de la Recomendación.

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.

[1] Recomendación UIT-T Y.1710 (2002), *Requisitos de la funcionalidad operación y mantenimiento para redes con conmutación por etiquetas multiprotocolo*.

[2] Recomendación UIT-T Y.1711 (2002), *Mecanismo de operación y administración para redes con conmutación por etiquetas multiprotocolo*.

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

NOTA – Hay algunas limitaciones para aplicar la arquitectura de la Rec. UIT-T G.805. No se puede utilizar en un LSP multipunto a punto basado en el protocolo de distribución de etiquetas (LDP, *label distribution protocol*) ni en el caso de que la salida del penúltimo salto que se utiliza (PHP, *penultimate hop popping*) no soporte el plano datos MPLS.

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

[5] Recomendación UIT-T I.630 (1999), *Conmutación de protección del modo de transferencia asíncrono*.

[6] Recomendación UIT-T M.20 (1992), *Filosofía de mantenimiento de las redes de telecomunicaciones*.

[7] IETF RFC 3031 (2001), *Multiprotocol Label Switching Architecture*.

[8] IETF RFC 3032 (2001), *MPLS Label Stack Encoding*.

3 Definiciones

En esta Recomendación se definen los términos siguientes.

3.1 protección 1+1: Mecanismo de protección en el cual se duplica el tráfico por el trayecto de protección (puenteo constante). El encaminador de conmutación de etiquetas (LSR, *label switch router*) de fusión de trayectos lleva a cabo la conmutación del tráfico entre los trayectos principal y de protección.

3.2 protección 1:1: Mecanismo de protección en el cual el tráfico se envía únicamente por el trayecto principal o por el trayecto de protección. El LSR de conmutación de trayectos efectúa la conmutación del tráfico entre los trayectos principal y de protección.

3.3 conmutación de protección bidireccional: Arquitectura de conmutación de protección en la cual, en el caso de un fallo unidireccional, ambos sentidos del LSP, incluidos el sentido afectado y el sentido no afectado, se conmutan al trayecto de protección.

3.4 puentear: Acción o función de transmitir el mismo tráfico por ambos LSP, el principal y el de protección.

3.5 defecto: (véase la nota 1) Interrupción de la capacidad de un LSP para transferir información de usuario o de operación, administración y mantenimiento (OAM, *operation, administration and maintenance*).

3.6 tráfico adicional: Tráfico que se añade deliberadamente al mismo recurso de capa de red como a un LSP de protección (aunque se emplea un LSP independiente que funciona en paralelo al LSP de protección) teniendo presente que en caso de fallo se interrumpirá este tráfico (adicional) para dar paso al tráfico de protección de la conexión principal que dejó de funcionar debido al fallo.

3.7 fallo: (véase la nota 1) Interrupción de la capacidad de un LSP para transferir información de usuario u OAM. La causa del fallo puede ser un defecto persistente.

3.8 conmutación forzada del trayecto conmutado por etiquetas principal: Acción de conmutación iniciada por la instrucción de un operador. Esta acción se ejecuta a menos de que esté en curso una petición de conmutación con mayor prioridad [es decir, la exclusión de protección (LoP, *lockout of protection*)].

3.9 tiempo de espera: Tiempo entre el aviso de señal degradada o de señal con fallo, y la activación del algoritmo de conmutación de protección.

3.10 conmutación manual: Acción de conmutación iniciada mediante la instrucción de un operador. Esta acción se ejecuta a menos de que esté en curso una petición de conmutación de igual o mayor prioridad [es decir, LoP, conmutación forzada (FS, *forced switch*), fallo de señal (SF, *signal fail*) o conmutación manual (MS, *manual switch*)].

3.11 dominio de protección de conmutación por etiquetas multiprotocolo: Conjunto de LSR por los que se encaminan el trayecto principal y su trayecto de protección correspondiente.

3.12 conmutación de protección sin reversión: Método de conmutación de protección en el cual no se lleva a cabo la acción de reversión (conmutación para regresar al LSP principal) después del restablecimiento del LSP principal.

3.13 sin petición: Estado en el que no existe petición de conmutación de protección.

3.14 encaminador de conmutación de etiquetas de conmutación de trayecto: LSR responsable de conmutar o reproducir el tráfico entre el LSP principal y el LSP de protección.

3.15 encaminador de conmutación de etiquetas de fusión de trayectos: LSR que es responsable de recibir tráfico del trayecto de protección y de fusionarlo nuevamente en el trayecto principal, o, si se trata del propio LSR de destino, de pasarlo a los protocolos de capa superior.

3.16 trayecto conmutado por etiquetas de protección: LSP dentro del dominio de protección que conduce tráfico principal que se recibe en el destino del dominio de protección cuando falla un LSP principal.

3.17 conmutación de protección: Mecanismo de recuperación con el que se prevé el LSP o los segmentos de trayecto de protección antes de que se detecte un fallo en el trayecto principal. En otras palabras, un mecanismo de protección con el que se puede precalcular, preasignar su capacidad y preestablecer el LSP de protección.

3.18 reencaminamiento: Mecanismo de recuperación con el que se crea dinámicamente el trayecto o segmentos de trayecto de recuperación tras la detección de un fallo en el trayecto principal. En otras palabras, un mecanismo de recuperación en el que el trayecto de recuperación no está preestablecido.

3.19 conmutación de protección reversiva: Método de conmutación de protección en el que se lleva a cabo una acción de reversión (conmutación para regresar al LSP principal) después del restablecimiento del LSP principal.

3.20 selector: Conmutador que permite seleccionar la recepción de tráfico del LSP principal o del LSP de protección en el sumidero del dominio de protección, o conmutador que permite seleccionar el envío de tráfico al LSP principal o al LSP de protección en la fuente del dominio de protección.

3.21 fuente del dominio de protección: Punto extremo de transmisión (ingreso) en un LSR de conmutación de trayectos del dominio de protección.

3.22 sumidero del dominio de protección: Punto extremo de recepción (egreso) en un LSR de fusión de trayectos del dominio de protección.

3.23 entidad de transporte: Componente de la arquitectura que transfiere información entre sus entradas y sus salidas dentro de una red de capa (véase la nota 2). En una red MPLS se usa un LSP como entidad de transporte.

3.24 conmutación de protección unidireccional: Arquitectura de conmutación de protección en la cual, en caso de un fallo unidireccional (es decir, que afecta solo a un sentido de la transmisión), únicamente se conmuta la protección en el sentido afectado del LSP.

3.25 en espera de restablecimiento: Instrucción iniciada automáticamente que se emite cuando el LSP principal se restablece de la condición de fallo de señal. Se utiliza para mantener ese estado hasta la expiración del temporizador "en espera de restablecimiento" a menos que se adelante una petición de puenteo con prioridad más alta.

3.26 temporizador de en espera de restablecimiento: Temporizador configurable que se utiliza para introducir un retardo antes de la acción de reversión.

3.27 trayecto conmutado por etiquetas principal: LSP dentro del dominio de protección cuyo tráfico principal se recibe en el sumidero del dominio de protección sin que haya averías en modo reversible.

NOTA 1 – Véase la Rec. UIT-T M.20 para una definición más detallada.

NOTA 2 – Véase la Rec. UIT-T G.805 para una definición más detallada.

4 Símbolos y abreviaturas

En esta Recomendación se utilizan las siguientes siglas:

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

BDI Indicación de defecto hacia atrás (*backward defect indication*)

CV Packet Paquete de verificación de la conectividad (*connectivity verification packet*)

FDI Indicación de defecto hacia adelante (*forward defect indication*)

FS Conmutación forzada (*forced switch*)

LDP Protocolo de distribución de etiquetas (*label distribution protocol*)

LOCV Verificación de pérdida de conectividad (*loss of connectivity verification*)

LoP Exclusión de protección (*lockout of protection*)

LSP Trayecto conmutado por etiquetas (*label switched path*)

LSR Encaminador de conmutación de etiquetas (*label switch router*)

MPLS Conmutación por etiquetas multiprotocolo (*multi-protocol label switching*)

MS Conmutador manual (*manual switch*)

OAM Operación, administración y mantenimiento (*operation, administration and maintenance*)

PHP Utilización del penúltimo salto (*penultimate hop popping*)

PML Encaminador de conmutación de etiquetas de fusión de trayectos (*path merge LSR*)

PS Conmutación de protección (*protection switching*)

PSL Encaminador de conmutación de etiquetas de conmutación de trayectos (*path switch LSR*)

SDH Jerarquía digital síncrona (*synchronous digital hierarchy*)

SF Fallo de señal (*signal fail*)

SLA Acuerdo de nivel de servicio (*service level agreement*)

TTSI Identificador de origen de terminación del camino (*trail termination source identifier*)

5 Requisitos

Las técnicas necesarias para mejorar la fiabilidad de funcionamiento de una red a través de mecanismos de recuperación en caso de interrupciones del servicio (por ejemplo, provocadas por defectos), se denominan técnicas de supervivencia. Éstas incluyen funciones de conmutación y reencaminamiento de protección. El objetivo de la presente Recomendación es describir técnicas de conmutación de protección. En esta Recomendación la diferencia entre conmutación de protección y reencaminamiento es la siguiente:

- Conmutación de protección: El cálculo y asignación del encaminamiento y de los recursos necesarios para un LSP de protección dedicado se realiza antes de que se produzca un fallo. Por consiguiente, la conmutación de protección constituye un mecanismo seguro para recuperar los recursos de red necesarios después de un fallo.
- Reencaminamiento: No se define un LSP de protección dedicado, ni se calculan/asignan el encaminamiento o los recursos necesarios antes de que se produzca una avería. Normalmente, el reencaminamiento se utiliza en aquellos casos en que hay funciones de encaminamiento y señalización en operación, que se ha de generar una "petición de reconexión" después de un fallo (ya sea la red o un cliente), y esta petición ha de competir con otros tipos de tráfico similares para obtener los recursos necesarios. Por consiguiente, el reencaminamiento no ofrece ninguna garantía de recuperación de los recursos de red necesarios después del fallo y por lo general es más lento que la conmutación de protección.

La conmutación de protección es necesaria para una rápida recuperación después de un fallo, y por lo tanto, mejora la fiabilidad y la disponibilidad de la calidad de funcionamiento de las redes MPLS. Para la conmutación de protección se requieren las siguientes características:

1) La conmutación de protección se debe aplicar a todo el LSP.
2) Protección con prioridad entre el SF (fallo de la señal) y la petición de conmutación del operador (véase el cuadro 1).
3) Se debe prever la posibilidad de efectuar la protección de la capa MPLS tan rápido como sea posible (en función del tiempo de activación del mecanismo de detección de defectos).
4) Relación de protección de 100%, es decir, se protege el 100% del tráfico principal afectado en el caso de un fallo en un solo LSP principal.
5) Cuando sea posible, se debe soportar la capacidad del tráfico adicional.

6 Principios

La conmutación de protección es un mecanismo de protección totalmente asignado y se puede utilizar en cualquier tipo de topología. Está totalmente asignado en el sentido de que se reservan la ruta y el ancho de banda de un LSP de protección para un LSP principal seleccionado. Sin embargo, para que esta protección pueda ser efectiva en cualquier tipo de fallo del LSP principal, el LSP de protección debe disponer de una diversidad física completa en todos los modos de fallo comunes, lo cual no siempre es posible. Además, esto podría requerir que el LSP principal no utilice el trayecto más corto.

La arquitectura de conmutación de protección (PS, *protection switching*) de MPLS puede ser del tipo 1+1 o bien 1:1. Otros tipos quedan en estudio.

En el tipo de arquitectura 1+1, se tiene un LSP de protección por cada LSP principal y este último se puentea hacia el LSP de protección en la fuente del dominio de protección. El tráfico de los LSP principal y de protección se transmite simultáneamente al sumidero del dominio de protección, donde se lleva a cabo la selección entre el LSP principal y el de protección basándose en criterios predeterminados, como la indicación del defecto.

En el tipo de arquitectura 1:1, se tiene un LSP de protección por cada LSP principal. El tráfico principal se transmite por el LSP principal o por el de protección. El método para la selección entre el LSP principal y el de protección depende del mecanismo. El LSP de protección se puede utilizar para transportar "tráfico adicional" cuando no se usa para transmitir tráfico principal.

En la siguiente lista se indican los principios de las arquitecturas de protección y el desarrollo de los mecanismos de MPLS.

1) Los defectos en las capas por encima de MPLS no deben provocar la conmutación de protección de la capa servidor. Por ejemplo, en caso de que se use el modo de transferencia asíncrono (ATM, *asynchronous transfer mode)* sobre MPLS, los defectos en la capa ATM no deben activar la conmutación de protección MPLS.
2) En general, si se utilizan mecanismos de protección de capa inferior (por ejemplo, SDH u óptica) junto con los mecanismos de protección de la capa MPLS, las capas inferiores deben tener la oportunidad de restablecer el tráfico principal antes de que se active la protección en la capa MPLS (por ejemplo, a través de un temporizador de espera). La finalidad es impedir la duplicación de la conmutación de protección en diferentes redes de capa.
3) Las acciones de conmutación de protección en un dominio de protección no deben afectar desfavorablemente a las operaciones, a la calidad de funcionamiento ni a la conmutación de protección de la red en otros dominios.

4) El mecanismo de conmutación de protección debe facilitar el restablecimiento rápido del tráfico principal para disminuir las interrupciones de red, e idealmente el restablecimiento se debería llevar a cabo antes de que se alcance el umbral de indisponibilidad.

7 Mecanismos

En esta cláusula se describen los mecanismos de la conmutación de protección unidireccional y bidireccional.

7.1 Conmutación de protección unidireccional

7.1.1 Arquitecturas de aplicación

7.1.1.1 Arquitectura de aplicación de la conmutación de protección unidireccional 1+1

En la figura 1 se ilustra la arquitectura de conmutación de protección lineal 1+1. En el caso del funcionamiento de la conmutación de protección unidireccional, ésta se realiza mediante el selector en el destino del dominio de protección basándose solo en información local (es decir, en el destino de protección). El tráfico principal se puentea permanentemente a los LSP principal y de protección en la fuente del dominio de protección. Si se utilizan paquetes de verificación de conectividad u otros paquetes de indagación de continuidad para detectar defectos en los LSP principales o de protección, los paquetes se insertan en la fuente del dominio de protección tanto en el lado principal como en el de protección y se detectan y extraen en el sumidero del dominio de protección. Obsérvese que los paquetes de verificación se deben enviar independientemente de que el LSP esté o no seleccionado.

Por ejemplo, si se presenta un defecto unidireccional [en el sentido de transmisión del PSL al encaminador de conmutación de etiquetas de fusión de trayectos (PML, *path merge LSR*)] en el LSP principal como se muestra en la figura 2, éste se detectará en el sumidero del dominio de protección en el PML y su selector conmutará al LSP de protección.

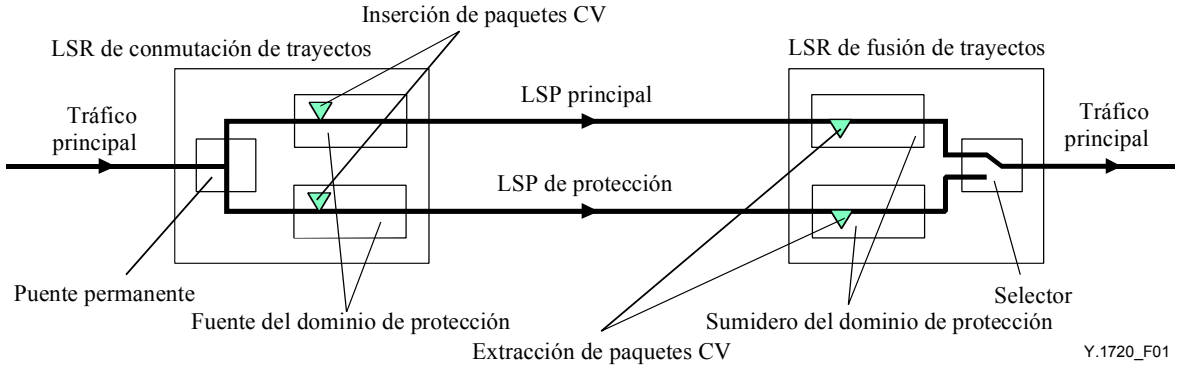

Figura 1/Y.1720 – Arquitectura de conmutación de protección unidireccional 1+1

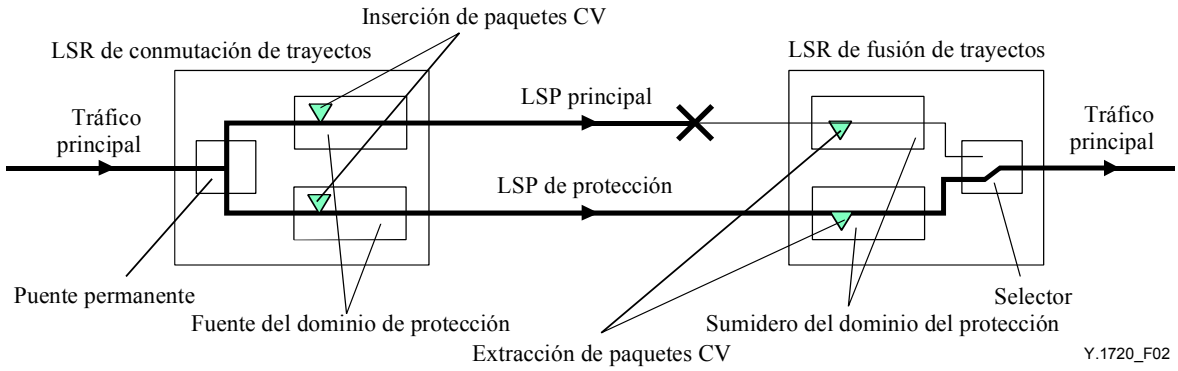

Figura 2/Y.1720 – Arquitectura de conmutación de protección unidireccional 1+1 – Fallo en el LSP principal

7.1.1.2 Arquitectura de aplicación de la conmutación de protección unidireccional 1:1

En la figura 3 se ilustra la arquitectura de conmutación de protección lineal 1:1. En el caso del funcionamiento de la conmutación de protección unidireccional, la conmutación de protección se realiza mediante el selector en el origen del dominio de protección basándose sólo en información local (es decir, en la fuente de protección). El tráfico principal y de protección se fusiona permanentemente en el sumidero del dominio de protección.

Si se utilizan paquetes de verificación de conectividad u otros paquetes de indagación de continuidad para detectar defectos en los LSP principales o de protección, los paquetes se insertan en la fuente del dominio de protección tanto en el lado principal como en el de protección y se detectan y extraen en el sumidero del dominio de protección. Obsérvese que los paquetes de verificación se deben enviar independientemente de que el LSP esté o no seleccionado.

Por ejemplo, si se presenta un defecto unidireccional (en el sentido de transmisión del PSL al PML) en el LSP principal como se muestra en la figura 4, éste se detectará en el destino del dominio de protección en el PML y con una indicación de defecto hacia atrás (BDI, *backward defect indication*) se informa la fuente del dominio de protección en el encaminador de conmutación de etiquetas de conmutación de trayectos (PSL, *path switch LSR*). Cuando se recibe el informe, el selector en el PSL se conmutará al LSP de protección.

NOTA – No se puede proteger dTTSI_Mismerge mediante la conmutación de protección 1:1.

Cuando se declara un SF en el LSP principal y el tráfico de usuario se transmite a través del LSP de protección, los paquetes de indicación de defecto hacia adelante (FDI, *forward defect indication*) y el tráfico de usuario se pueden fusionar en el destino del dominio de protección. Los nodos en el sentido descendente recibirían paquetes FDI, paquetes CV y tráfico de usuario al mismo tiempo. La misma situación se aplica cuando se declara un SF en el LSP de protección. El problema se puede resolver con la utilización de un selector de fusión. El funcionamiento de este último, cuando se detecta un defecto en el LSP principal, es:

1) Se reciben paquetes FDI o se detecta un defecto en la capa inferior a la salida del LSP principal.
2) Se conmuta el selector de fusión en la salida (es decir, se desconecta el interruptor del LSP principal y se conecta el interruptor del LSP de protección).
3) Se envían paquetes BDI por el LSP principal.
4) Se conmuta el selector en la entrada (es decir, se conmuta el LSP principal hacia el LSP de protección y se interrumpe el tráfico adicional).

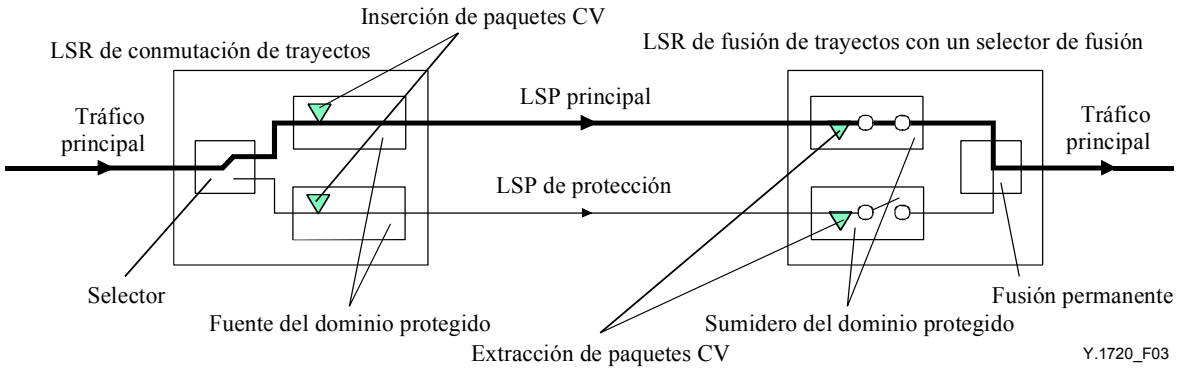

Figura 3/Y.1720 – Arquitectura de conmutación de protección unidireccional 1:1

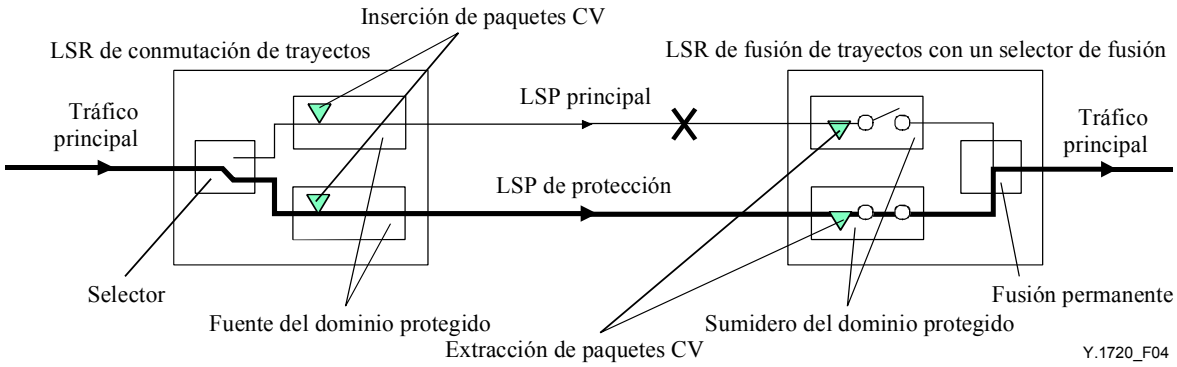

Figura 4/Y.1720 – Arquitectura de conmutación de protección unidireccional 1:1 – Fallo en el LSP principal

7.1.1.3 Tráfico adicional

La arquitectura 1:1 puede soportar tráfico adicional. Como el tráfico de los LSP principales y de protección se fusiona en el destino del dominio de protección, el tráfico adicional se transportará mediante un LSP independiente que tendrá una ruta física igual a la del LSP de protección (véase la figura 5) con objeto de impedir la fusión entre el tráfico adicional y el principal y para compartir el ancho de banda entre ellos. Cuando el tráfico principal conmuta al LSP de protección, el tráfico adicional se interrumpe para permitir la transmisión del tráfico principal que no puede pasar por conexión principal con fallo (véase la figura 6). Por lo general, esto requiere un protocolo de coordinación de la conmutación de protección. En esta Recomendación se utiliza BDI como el protocolo de la fase 1 (véase también la Rec. UIT-T I.630). La verificación de la conectividad de un LSP de tráfico adicional es facultativa. Si se requiere notificación de la desconexión del tráfico adicional, se debe utilizar la verificación de la conectividad.

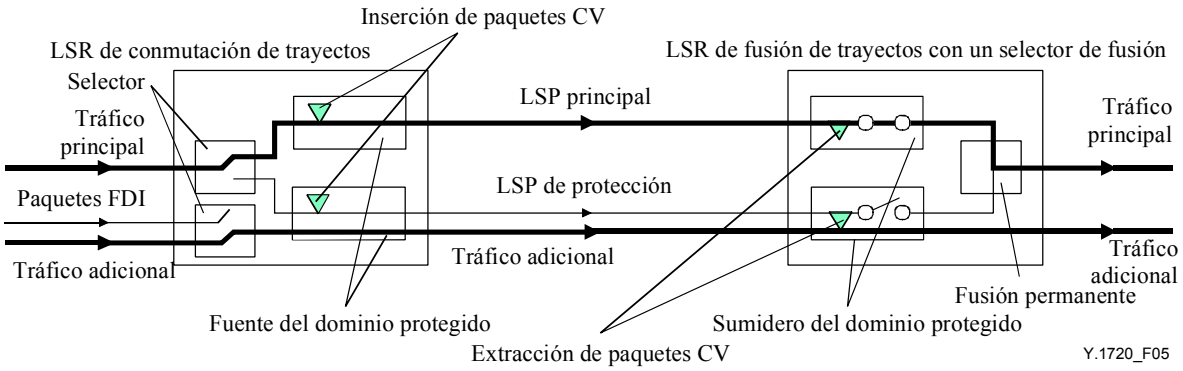

Figura 5/Y.1720 – Arquitectura 1:1 con tráfico adicional

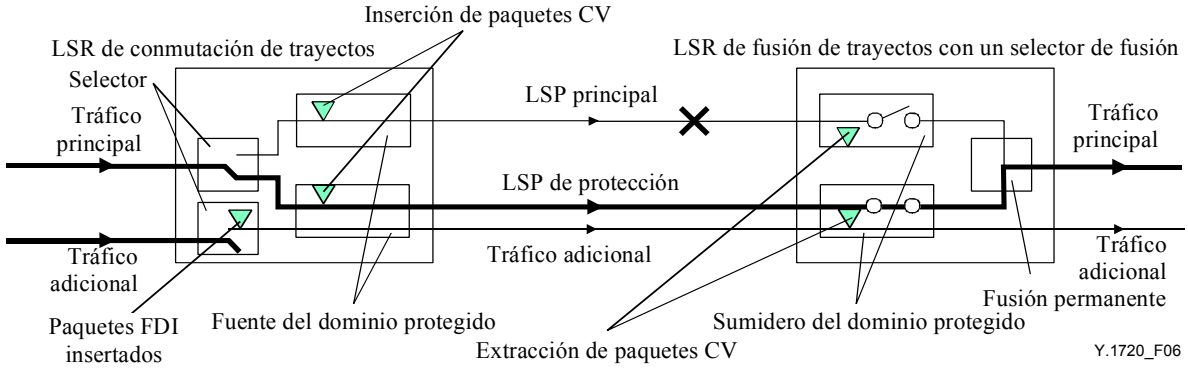

Figura 6/Y.1720 – Arquitectura 1:1 con tráfico adicional – Fallo en el LSP principal

7.1.2 Mecanismo de activación de la conmutación de protección

La conmutación de protección se debe realizar cuando:

1) se inicia por control del operador (por ejemplo, conmutación manual, conmutación forzada, y exclusión de protección) sin estar en curso una petición de conmutación con una prioridad más alta;
2) se declara SF en el LSP conectado (es decir, el LSP principal o el LSP de protección), no se declara en el otro LSP y ya ha expirado el temporizador de espera; o
3) expira el temporizador de espera de restablecimiento (modo reversible) y no se declara SF en el LSP principal.

7.1.2.1 Control manual

El control manual de la función de conmutación de protección se puede transferir del sistema de operaciones.

7.1.2.2 Condiciones de declaración de fallo de la señal

7.1.2.2.1 Arquitectura 1+1

En el caso de la arquitectura 1+1, se declara fallo de señal (SF) cuando el punto destino del dominio de protección pasa al estado de defecto de extremo próximo de destino del camino LSP pasando a la condición de dServer, dLOCV, dTTSI_Mismatch, dTTSI_Mismerge, dExcess, o dUnknown.

Para lograr una protección rápida (este requisito se encuentra en estudio) se puede declarar SF cuando el destino del dominio de protección recibe un paquete FDI, antes de pasar otras condiciones de defecto (por ejemplo, dLOCV). Permite una protección rápida contra los defectos

producidos en las capas por debajo de la capa MPLS (y requiere que la FDI entrante tenga el punto de código de tipo de defecto (DT) 0x0101).

NOTA – Su utilización es adecuada sólo cuando la capa inferior no está protegida. Si lo está, se puede provocar una conmutación de protección innecesaria al declarar SF cuando se reciben paquetes FDI.

En caso de que la función CV no esté activada, se declara SF cuando el sumidero del dominio de protección recibe un paquete FDI. Sólo se aplica a los defectos producidos en las capas por debajo de la capa MPLS (y requiere que la FDI entrante tenga el punto de código DT 0x0101)

7.1.2.2.2 Arquitectura 1:1

En el caso de la arquitectura 1:1, se declara fallo de señal (SF) cuando:

- la fuente del dominio de protección pasa al estado de defecto en el extremo próximo del sumidero del camino al recibir un paquete BDI (del LSP de retorno o fuera de banda).

NOTA – La protección contra defectos en el LSP bidireccional queda en estudio.

7.1.3 Conformidad con los objetivos de la red

Se aplican los siguientes objetivos de red:

1) *Modos de operación*

   Se ofrece conmutación reversible y no reversible.

2) *Control manual*

   Se soporta el control del operador a través de instrucciones de exclusión de protección, conmutación forzada y conmutación manual.

3) *Otros criterios de inicio de conmutación*

   Además de las instrucciones de control manual antes descritas, se soportan los criterios fallo de señal, en espera de restablecimiento, y sin petición de conmutación, para iniciar (o impedir) una conmutación de protección.

7.1.4 Criterios de inicio de conmutación

Se dispone de los siguientes criterios de inicio de conmutación:

1) instrucción iniciada externamente (despejar, exclusión de protección, conmutación forzada, conmutación manual);
2) instrucción iniciada automáticamente (fallo de señal) asociada con un dominio de protección; o
3) un estado (en espera de restablecimiento, sin petición de conmutación) de la función de conmutación de protección.

Todas las peticiones son locales (es decir, sumidero de protección en la arquitectura 1+1 y fuente de protección en la arquitectura 1:1). En el cuadro 1 se estipula la prioridad de las peticiones locales.

Cuadro 1/Y.1720 – Prioridad de las peticiones locales

Petición local (es decir, instrucción, estado iniciado automáticamente, o instrucción iniciada externamente)	Orden de prioridad
Despejar	La más alta
Exclusión de protección	|
Conmutación forzada	|
Fallo de la señal	|
Conmutación manual	|
Espera de restablecimiento	|
Sin petición	La más baja

NOTA 1 – Un fallo de señal en el LSP de protección no debe anular la conmutación forzada de un LSP principal. Como se está llevando a cabo una conmutación de protección unidireccional y el LSP de protección no soporta ningún protocolo de conmutación automática de protección (APS, *automatic protection switching*), el fallo en el LSP de protección no interfiere en la capacidad de realizar una conmutación forzada del LSP principal.

NOTA 2 – No se ha definido la conmutación forzada del LSP de protección ya que esta función puede llevarse a cabo a través de la instrucción de exclusión de protección.

7.1.4.1 Instrucciones iniciadas desde el exterior

A continuación se enumeran las instrucciones iniciadas desde el exterior en orden de prioridad descendente. Se describe la funcionalidad de cada instrucción.

despejar: Despeja todas las instrucciones de conmutación iniciadas externamente que se relacionan a continuación.

Exclusión de protección (LoP): Fija la posición del selector en el LSP principal. Impide que el selector se conmute hacia el LSP de protección cuando está en la posición del LSP principal. Conmuta el selector del LSP de protección al principal cuando está en la posición del LSP de protección.

Conmutación forzada (FS) del LSP principal: El selector conmuta del LSP principal al de protección [a menos que se encuentre en curso una petición de conmutación con una prioridad más alta (es decir, LoP)].

Conmutación manual (MS) del LSP principal: El selector conmuta del LSP principal al de protección [a menos que se encuentre en curso una petición de conmutación con una prioridad igual o más alta (es decir, LoP, FS, SF o MS)].

Conmutación manual (MS) del LSP de protección: El selector conmuta del LSP de protección al LSP principal [a menos de que se encuentre en curso una petición de conmutación con una prioridad igual o más alta (es decir, LoP, FS, SF o MS)].

7.1.4.2 Conmutación de protección activada por FDI

En este caso, si el LSP con SF no puede pasar al estado de defecto de extremo próximo, quizás sea necesario impedir las transiciones frecuentes. De ser así, se puede definir un tiempo antes de pasar a otra acción de conmutación de protección. Queda en estudio.

7.1.4.3 Estados

La instrucción en espera de restablecimiento solo se puede aplicar a un LSP principal en modo reversible. La función de conmutación de protección local pasa a este estado cuando el tráfico se recibe a través del LSP de protección mientras se restablece el LSP principal, si antes se había

activado la petición de conmutación de protección local y ahora se desactiva. Impide reseleccionar el LSP principal hasta que expira el temporizador en espera de restablecimiento. El operador puede configurar el tiempo de en espera de restablecimiento entre 1 y 30 minutos en pasos de 1 minuto; el valor por defecto es de 12 minutos.

La función de conmutación de protección local pasa al estado sin petición siempre que no haya peticiones en curso de conmutación de protección local (incluida en espera de restablecimiento).

7.1.5 Protocolo de conmutación de protección

La arquitectura de conmutación de protección unidireccional 1+1 y 1:1, no requiere protocolo APS.

7.1.6 Funcionamiento del algoritmo de conmutación de protección unidireccional

7.1.6.1 Control del selector

En la arquitectura de funcionamiento con conmutación de protección unidireccional 1+1 y 1:1, la petición local de la prioridad más alta controla el selector (es decir, sumidero del dominio de protección en la arquitectura 1+1; fuente del dominio de protección en la arquitectura 1:1) (instrucción iniciada automáticamente, estado o instrucción iniciada externamente). Por consiguiente, los extremos funcionan con independencia uno del otro. Si se presenta una condición de prioridad equivalente (por ejemplo, SF) en ambos LSP, no se realizará la conmutación.

7.1.6.2 Modo reversible

En el modo de funcionamiento reversible, se pasa al estado en espera de restablecimiento cuando el tráfico principal se transmite a través del LSP de protección mientras se restablece el LSP principal, si antes se había activado la petición de conmutación de protección local y ahora se desactiva.

Normalmente, cuando termina ese estado se pasa al estado sin petición después de la expiración del temporizador en espera de restablecimiento. A continuación se reselecciona el LSP principal. El temporizador en espera de restablecimiento se desactiva prematuramente si alguna petición local con una prioridad más alta se apropia de este estado.

7.1.6.3 Modo no revertido

Cuando el LSP con fallo ya ha superado la condición de SF, y no hay otras instrucciones en curso iniciadas externamente, se pasa al estado no petición. Durante este estado no hay conmutación.

7.2 Mecanismos de conmutación de protección bidireccional

Queda en estudio.

Apéndice I

Bibliografía

– IETF RFC 3469 (2003), *Framework for Multi-Protocol Label Switching (MPLS)-based Recovery*.

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	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	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 y aspectos del protocolo Internet**
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2003