UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T Y.1720

(09/2003)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE Y: INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN, ASPECTOS DEL PROTOCOLO INTERNET Y REDES DE LA PRÓXIMA GENERACIÓN

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, ASPECTOS DEL PROTOCOLO INTERNET Y REDES DE LA PRÓXIMA GENERACIÓN

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
REDES DE LA PRÓXIMA GENERACIÓN	
Marcos y modelos arquitecturales funcionales	Y.2000–Y.2099
Calidad de servicio y calidad de funcionamiento	Y.2100–Y.2199
Aspectos relativos a los servicios: capacidades y arquitectura de servicios	Y.2200–Y.2249
Aspectos relativos a los servicios: interoperabilidad de servicios y redes en las redes de próxima generación	Y.2250–Y.2299
Numeración, denominación y direccionamiento	Y.2300–Y.2399
Gestión de red	Y.2400–Y.2499
Arquitecturas y protocolos de control de red	Y.2500–Y.2599
Seguridad	Y.2700–Y.2799
Movilidad generalizada	Y.2800–Y.2899

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, 1:1, de malla compartida y de paquete 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 el 13 de septiembre de 2003 por la Comisión de Estudio 13 (2001-2004) del UIT-T por el procedimiento de la Recomendación UIT-T A.8.

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 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

1 Alcance 1

2 Referencias 1

3 Definiciones 2

4 Símbolos y abreviaturas 4

5 Requisitos 5

6 Principios 5

7 Mecanismos 6

7.1 Conmutación de protección unidireccional 6

7.2 Mecanismos de conmutación de protección bidireccional 17

8 Aspectos de seguridad 17

Apéndice I – Ejemplo de compartición de la capacidad de protección para la conmutación de protección de malla compartida 17

Apéndice II – Ejemplo de aplicación de la protección 1+1 de paquete 19

II.1 Mecanismo de doble alimentación y de selección 20

II.2 Análisis del método de protección 1+1 de paquete 21

Apéndice III – Bibliografía 28

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, 1:1, de malla compartida y de paquete 1+1 en el plano usuario de las redes con conmutación por etiquetas multiprotocolo (MPLS, *multiprotocol 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.495 (1988), *Restablecimiento de la transmisión y diversidad de rutas de transmisión: Terminología y principios generales.*

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

[8] IETF RFC 3031 (2001), *Multiprotocol Label Switching Architecture*, *Category: Standards Track.*

[9] IETF RFC 3032 (2001), *MPLS Label Stack Encoding, Category: Standards Track.*

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 protección de malla compartida: Puede considerarse como una ampliación de la protección 1:1. Prevé el uso compartido del ancho de banda entre los LSP de protección correspondientes a los LSP principales que pertenecen a enlaces, nodos, o grupos de riesgo compartido (SRG) disjuntos.

3.4 grupo de riesgo compartido (SRG, *shared risk group*): Grupo de enlaces o nodos susceptibles de fallo simultáneo debido a un solo fallo. Un ejemplo son las fibras dentro de un conducto que pertenece a un SRG, ya que una sola ruptura del conducto puede cortar todas las fibras que pasan por él.

3.5 protección 1+1 de paquete: Como en el caso de la protección 1+1 el tráfico se alimenta en ambos SLP. El nivel 1+1 de paquete permite la selección del paquete entrante de cualquiera de los dos LSP independientemente del LSP por el que se haya seleccionado el último paquete. Es decir, la protección 1+1 de paquete trata ambos LSP como principales a diferencia de la designación de un LSP como principal mientras el otro se considera como LSP de protección.

3.6 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.

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

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

3.9 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.

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

3.11 conmutación forzada del LSP 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*)].

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

3.13 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*)].

3.14 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.

3.15 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.

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

3.17 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.

3.18 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.

3.19 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.

3.20 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.

3.21 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.

3.22 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.

3.23 selector: Conmutador que permite seleccionar la recepción de tráfico del LSP principal o del LSP de protección en el destino 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.

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

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

3.26 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.

3.27 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.

3.28 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.

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

3.30 trayecto conmutado por etiquetas principal: LSP dentro del dominio de protección cuyo tráfico principal se recibe en el destino 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)*
FFD Packet	Paquete de detección rápida de fallo (*fast failure detection packet*)
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 *(multiprotocol 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, 1:1, de malla compartida o 1+1 de paquete. 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 el tipo de arquitectura de malla compartida, es posible compartir la capacidad de protección en caso de fallos de enlaces, nodos o SRG disjuntos y, a su vez, garantiza la recuperación al producirse un fallo simple. Para cada enlace en la red, se hace un seguimiento de todos los trayectos principales cuyo tráfico se conmutará hacia la malla compartida en caso de producirse un determinado fallo. De esta manera, sólo es necesario reservar el máximo de la capacidad de protección necesaria para proteger un fallo simple de red.

En el tipo de arquitectura 1+1 de paquete, el tráfico se transmite simultáneamente por dos posibles LSP disjuntos hacia el sumidero del dominio de protección. A cada par de paquetes transmitidos por duplicado se les asigna el mismo identificador (número de secuencia) que es distinto del de los otros pares de paquetes duplicados. En el destino del dominio de protección se emplea el mecanismo de selección de nivel de paquete para seleccionar una de las dos posibles copias recibidas de cada paquete. 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 debe 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 sumidero del dominio de protección basándose solo en información local (es decir, en el sumidero 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 (CV), paquetes FFD 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.

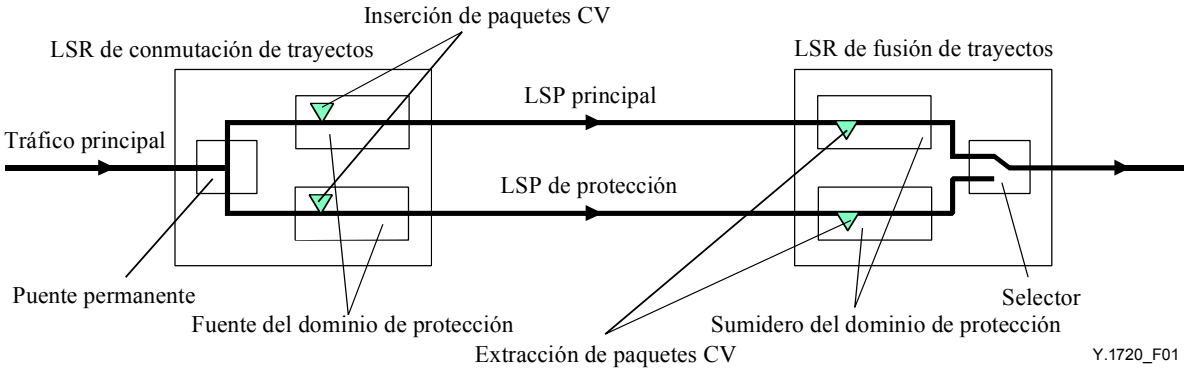

Figura 1/Y.1720 – Arquitectura de conmutación de protección unidireccional 1+1

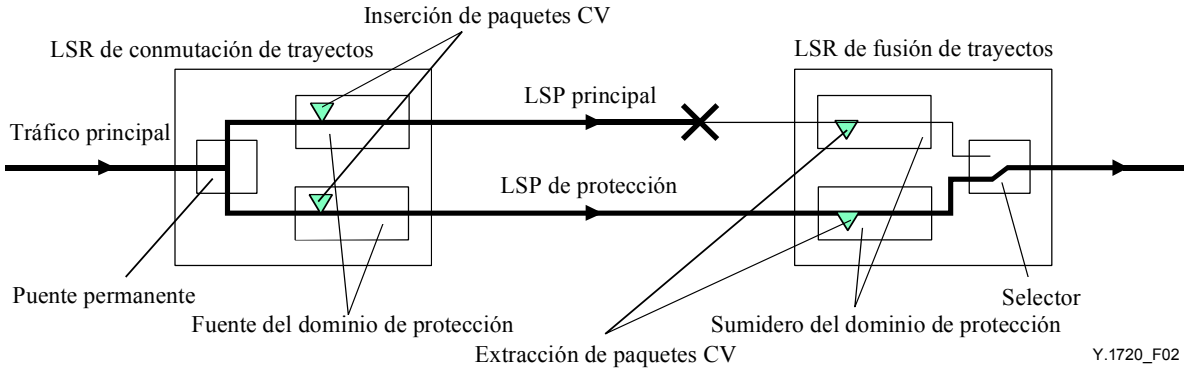

Figura 2/Y.1720 – Arquitectura de conmutación de protección unidireccional 1+1 – Fallo en el LSP principal

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 la fuente 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 (CV), paquetes FFD 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 sumidero 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 sumidero del dominio de protección. Los nodos en el sentido descendente recibirían paquetes FDI, paquetes CV o paquetes FFD 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).

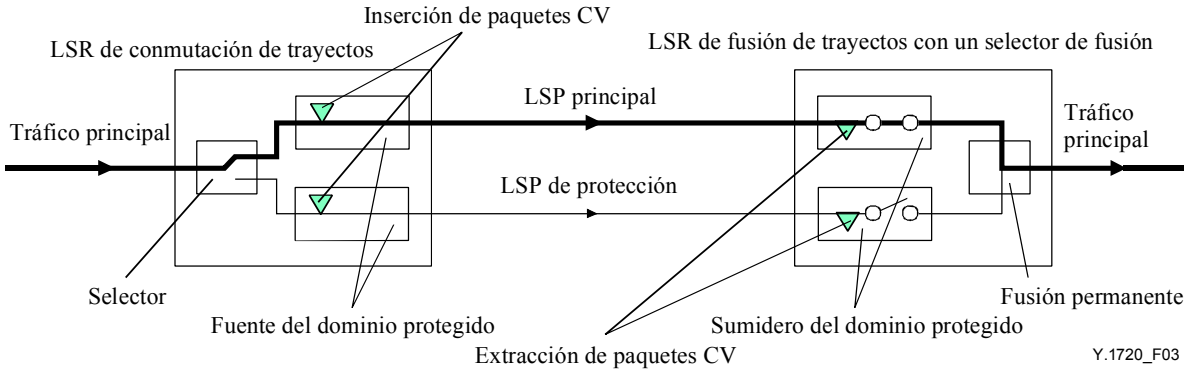

Figura 3/Y.1720 – Arquitectura de conmutación de protección unidireccional 1:1

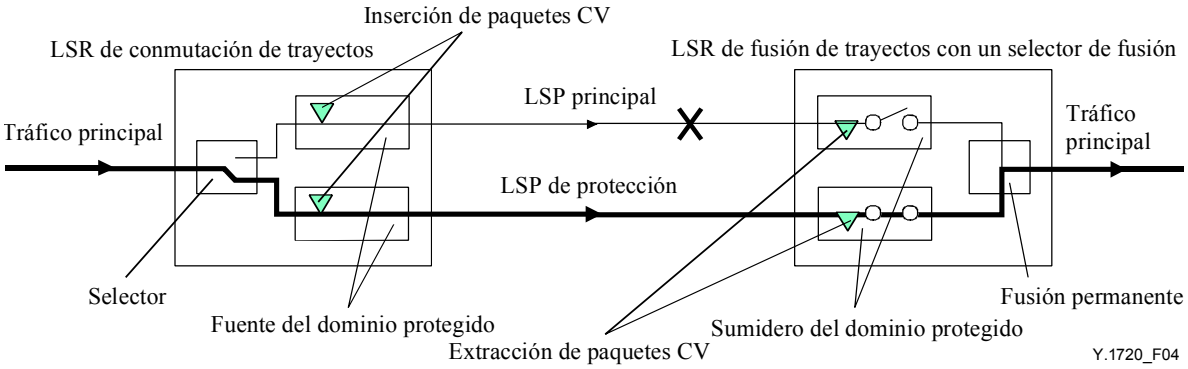

Figura 4/Y.1720 – Arquitectura de conmutación de protección unidireccional 1:1 – Fallo en el LSP principal

Tráfico adicional

La arquitectura 1:1 puede soportar tráfico adicional. Como el tráfico de los LSP principales y de protección se fusiona en el sumidero 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.

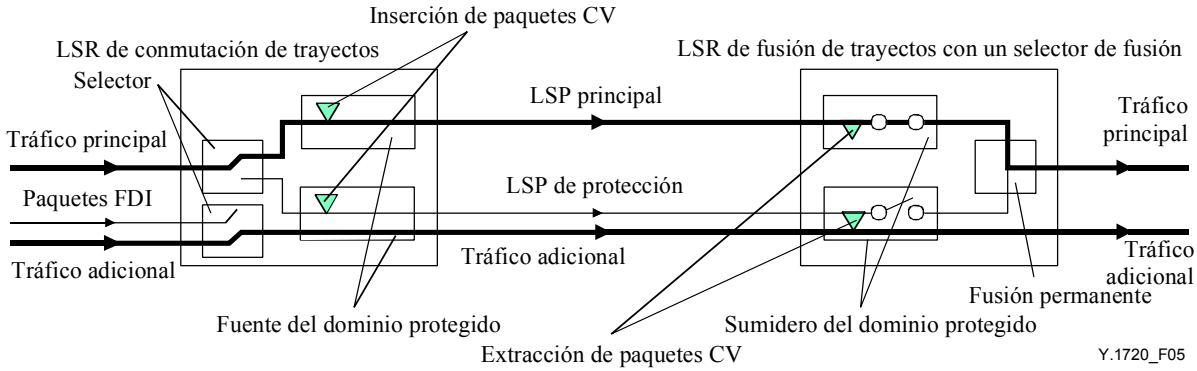

Figura 5/Y.1720 – Arquitectura 1:1 con tráfico adicional

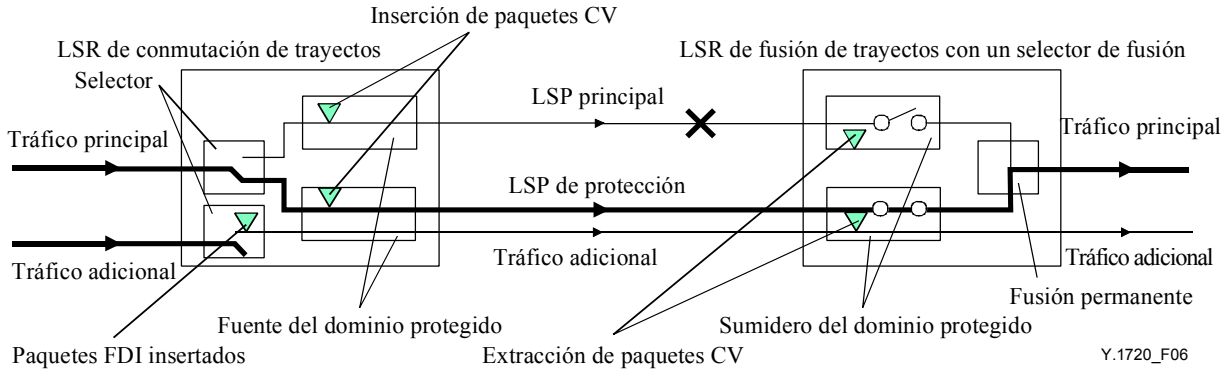

Figura 6/Y.1720 – Arquitectura 1:1 con tráfico adicional – Fallo en el LSP principal

7.1.1.3 Arquitectura de aplicación de la conmutación de protección de malla compartida unidireccional

La conmutación de protección de malla compartida puede considerarse como una ampliación de la protección 1:1. Requiere de toda la funcionalidad para realizar la protección 1:1 y funcionalidad adicional para compartir la capacidad de protección en caso de fallos de enlaces, nodos o grupos de riesgo compartido (SRG) disjuntos.

Requisitos funcionales

Los requisitos funcionales necesarios para realizar un método de protección de malla compartida en tiempo real son los siguientes:

1) La conmutación de protección de malla compartida debe poder compartir la capacidad de protección en caso de fallos de enlaces, nodos o SRG disjuntos en la red y, a su vez, garantizar la recuperación al producirse un fallo simple.

2) La conmutación de protección de malla compartida debe ser capaz de reservar (dejar de lado) la capacidad necesaria para la protección de cada enlace sin atribuirla a ningún LSP.

3) La conmutación de protección de malla compartida debe ser capaz de detectar (notificar) el fallo en (hacia) los nodos extremos (de entrada y salida).

4) La conmutación de protección de malla compartida debe tener la posibilidad de asignar capacidad de protección a los LSP de protección en el momento del fallo.

5) La conmutación de protección de malla compartida debe tener la capacidad de conmutar la alimentación del tráfico en la entrada y seleccionar el tráfico en la salida del LSP principal (protección) al LSP de protección (principal).

6) La conmutación de protección de malla compartida debe soportar la recuperación dentro de ciertos límites de tiempo y podrá ser conforme a los tiempos de recuperación que se utilizan normalmente.

7) La conmutación de protección de malla compartida debe permitir la utilización eficaz del ancho de banda del LSP principal mediante medidas como la optimización de rutas, y teniendo en cuenta las dependencias de la ruta entre un trayecto principal y su trayecto de protección.

Arquitectura de aplicación

El esquema de protección de malla compartida está pensado para garantizar la recuperación utilizando el mínimo ancho de banda de protección en una topología de malla genérica. Se reserva un conjunto de capacidad de protección dedicada, suficiente para recuperar todo el tráfico protegido en caso de producirse un fallo simple en la red. La capacidad de protección de cada conexión principal protegida, se asigna en el momento de su activación. Cuando se recibe una petición para establecer el servicio de protección de malla compartida entre dos nodos se activa el cálculo de un par de trayectos disjuntos entre ambos con dos limitaciones necesarias. La primera indica que debe disponerse de suficiente ancho de banda en la ruta de la conexión principal para dar cabida al tráfico solicitado. La segunda indica que el ancho de banda de protección que se ha reservado para el trayecto de protección ha de ser suficiente para garantizar la recuperación al producirse un fallo simple en la ruta primaria, o bien que el ancho de banda disponible en el trayecto de protección tiene que ser suficiente todo el ancho de banda adicional necesario para proteger la nueva conexión principal. Obsérvese que para lograr la compartición en primer lugar siempre se trata de dar cabida a una nueva petición con la capacidad de protección ya asignada. Esto se puede lograr mediante el seguimiento, para cada enlace en la red, de la cantidad de capacidad necesaria para la recuperación al producirse un fallo en cada nodo o enlace en la red. Obsérvese que, según lo comúnmente aceptado y verificado, en el sentido de que es muy poco probable que se produzcan múltiples fallos simultáneos en la mayoría de las redes, el método se describe para la protección contra fallos simples en la red.

La conmutación de protección y el mecanismo de activación de cada LSP principal afectado son similares a los del método de protección 1:1. En la figura 7 se ilustra un ejemplo de protección de malla compartida. En la figura 8 se presenta la protección del tráfico después de producirse un fallo específico.

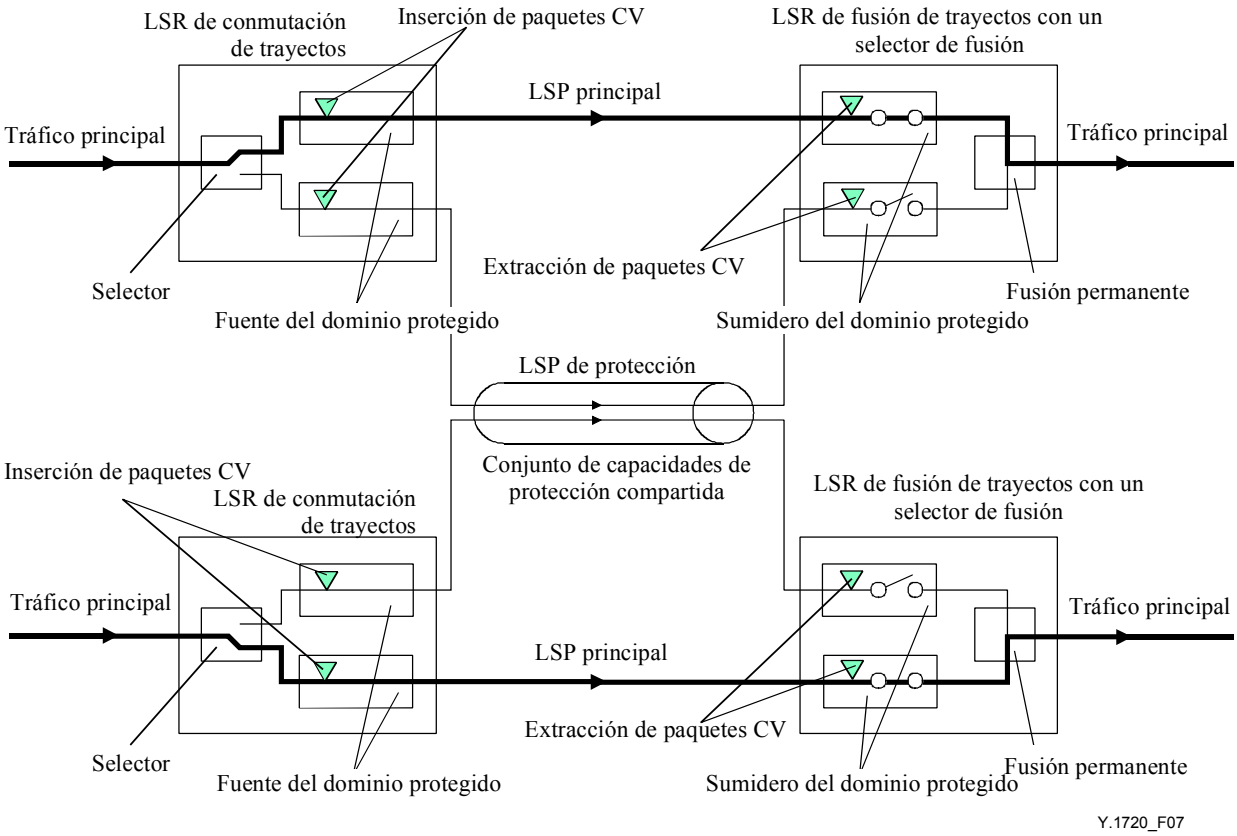

Figura 7/Y.1720 – Arquitectura de conmutación de protección de malla compartida unidireccional

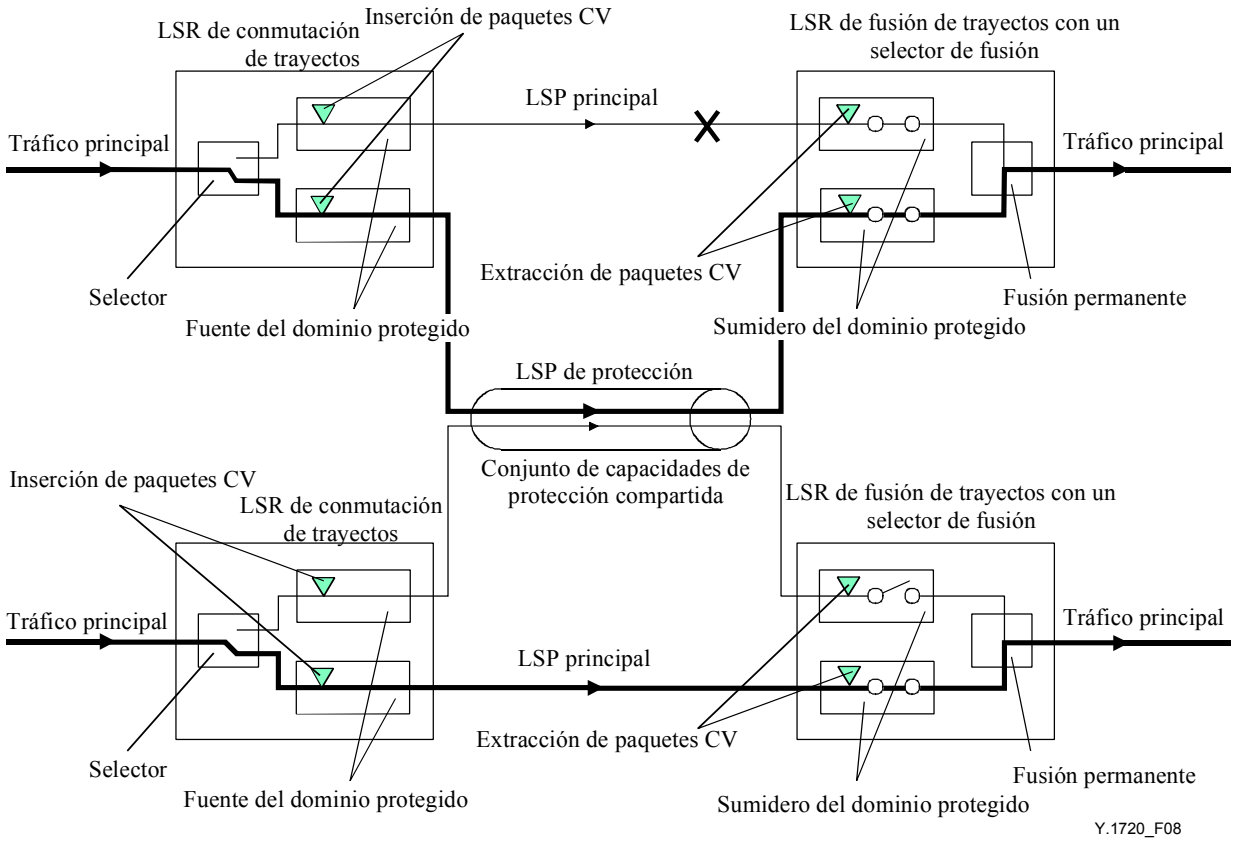

Figura 8/Y.1720 – Arquitectura de conmutación de protección de malla compartida unidireccional – Fallo simple

7.1.1.4 Arquitectura de aplicación de la conmutación de protección 1+1 de paquetes unidireccional

La protección de trayecto 1+1 de paquetes ofrece un servicio de protección a nivel de paquetes similar en algunos aspectos al servicio 1+1 de nivel de conexión convencional con varias diferencias importantes. La protección 1+1 a nivel de paquete permite seleccionar el paquete entrante de cualquier conexión independientemente de la conexión por la que se seleccionó el último paquete. Es decir, la protección 1+1 de paquetes trata ambas conexiones como principales en lugar de distinguir a una como conexión principal y a la otra como de protección. En este último caso, los paquetes se seleccionan de la conexión principal hasta que la detección de un fallo en la conexión principal causa la conmutación a la conexión de protección. Por el contrario, la protección 1+1 de paquete no requiere la detección del fallo y la conmutación de protección explícitas. Esto permite que con el método de protección 1+1 a nivel de paquete la recuperación al producirse un fallo sea instantánea y transparente. De manera similar al método de protección 1+1 a nivel de conexión, sólo los nodos limítrofes tienen necesidad de estar al corriente del servicio.

Para proporcionar servicio de protección 1+1 de paquete entre dos nodos en una red MPLS, se establece un par de LSP entre ellos a través de trayectos disjuntos. Los paquetes del flujo de un cliente abonado al servicio se alimentan por duplicado en los dos LSP en el nodo de entrada. En el caso más simple, los trayectos disjuntos pueden ser enlaces o nodos disjuntos pero en general pueden incluir una configuración más complicada como es el caso de los grupos de enlace de riesgo compartido. En el nodo limítrofe de salida se selecciona una de las dos copias recibidas de los paquetes y se reenvía atravesando un trayecto disjunto. Por consiguiente, cualquier fallo simple en la red, en algún lugar diferente de los propios nodos de entrada o salida, puede afectar como máximo una copia de cada paquete. Esto permite que el servicio sea resistente a los fallos simples de manera transparente. En términos de tiempo de restablecimiento, la recuperación tras producirse

un fallo puede considerarse instantánea dado que no hay necesidad de detectar, notificar y conmutar al trayecto de protección explícitamente.

Requisitos funcionales

Los requisitos mínimos para ofrecer el servicio de protección 1+1 de paquetes son:

a) No hay requisitos adicionales para los nodos internos de la red.

b) La red debe soportar el establecimiento de LSP con diversidad de encaminamiento.

c) *Nodo de entrada*

1) Debe ser capaz de asociar los dos LSP que se utilizan para proporcionar la protección 1+1 a nivel de paquete entre dos nodos extremos.

2) Debe soportar el transporte de un identificador en el paquete que se utilizará para determinar copias duplicadas de un paquete en el nodo de salida.

3) Debe ser capaz de alimentar cada paquete por duplicado en los dos LSP apareados.

d) *Nodo de salida*

1) Debe ser capaz de asociar los dos LSP que se utilizan para ofrecer protección 1+1 a nivel de paquete entre dos nodos extremos.

2) Debe ser capaz de identificar las copias duplicadas de un paquete alimentado por duplicado utilizando para ello el identificador.

3) Debe ser capaz de seleccionar y reenviar solamente una de las copias de cada paquete.

Los requisitos establecidos anteriormente describen la funcionalidad mínima necesaria para implementar un método de protección 1+1 a nivel de paquete.

Modelo de referencia

En la figura 9 se ilustra una aplicación del método de protección 1+1 de paquete utilizando como identificadores números de secuencia. Después de pasar a través del clasificador a cada paquete que necesita reenviarse por los LSP acoplados, se le asigna un número de secuencia distinto en el nodo de entrada. A continuación, este paquete se reenvía por los dos LSP disjuntos. En el nodo de salida se utiliza un contador para controlar el número de secuencia esperado del siguiente paquete. En el apéndice se describen los detalles de un ejemplo de implementación.

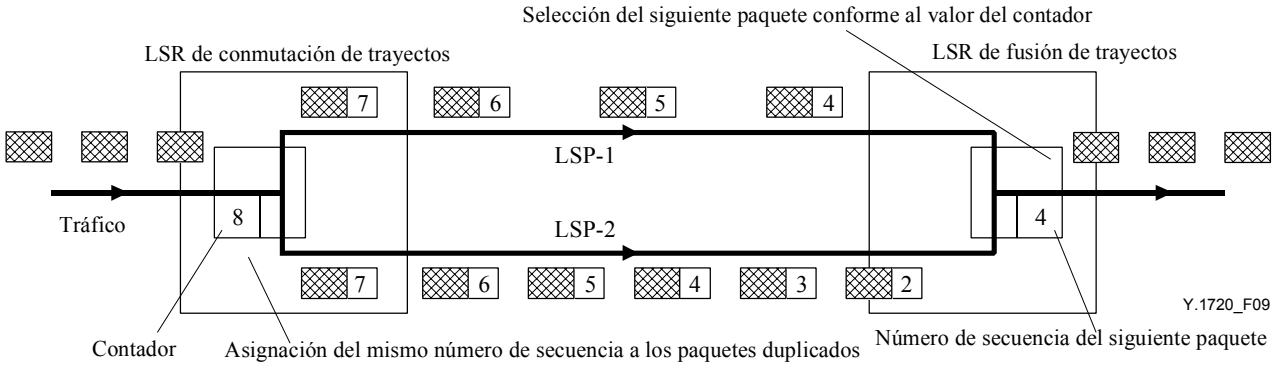

Figura 9/Y.1720 – Arquitectura de conmutación de protección 1+1 de paquete unidireccional

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, *signal fail*) cuando el punto sumidero 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 sumidero 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).

Además, se puede utilizar la función FDD para lograr una notificación más rápida de la condición de fallo de la señal.

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 o FDD no esté activada, se declara SF cuando el destino 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 destino" del camino al recibir un paquete BDI (del LSP de retorno o fuera de banda).

7.1.2.2.3 Arquitectura de malla compartida

La arquitectura de malla compartida es una ampliación de la arquitectura 1:1. El fallo de la señal (SF) se manifiesta de la misma manera que en la arquitectura 1:1.

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, destino 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, *lockout of protection*): 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, *forced switch*) 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, *manual switch*) 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 de conmutación de protección activada por FDI, 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, 1:1 y de malla compartida 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, 1:1 y de malla compartida 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.

En el método de protección 1+1 de paquete, los paquetes se eligen mediante un selector de nivel de paquetes que detecta los identificadores (números de secuencia) transportados en los paquetes transmitidos.

7.1.6.2 Modo revertido

En el modo de funcionamiento revertido, 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 sin petición. Durante este estado no hay conmutación.

7.2 Mecanismos de conmutación de protección bidireccional

Queda en estudio.

8 Aspectos de seguridad

En esta Recomendación no se propone ninguna cuestión de seguridad que no esté ya incluida en la arquitectura MPLS o en la arquitectura de sus protocolos de capa cliente.

La conmutación de protección puede mejorar la seguridad de las redes MPLS ya que podrá conmutar automáticamente el tráfico de los LSP con defectos, que se haya bifurcado o configurado erróneamente hacia otros LSP, a LSP que funciona correctamente. Esto evitará que el tráfico de los clientes se exponga a otros clientes.

Apéndice I

Ejemplo de compartición de la capacidad de protección para la conmutación de protección de malla compartida

Para garantizar la recuperación con un grado similar de servicio es necesario reservar el suficiente ancho de banda en la red para fines de restablecimiento. Un método de malla compartida requiere que el ancho de banda de protección sea suficiente para transportar todo el tráfico afectado al producirse un fallo simple en la red. Esto puede lograrse calculando y reservando capacidad de protección en el momento de activar el LSP principal. Una petición para establecer el servicio de malla compartida entre dos nodos activa el cálculo de un par de trayectos disjuntos entre ellos con dos premisas obligatorias. En primer lugar, en la ruta primaria del LSP debe haber ancho de banda suficiente para el ancho de banda solicitado. En segundo lugar, o el ancho de banda de protección reservado en el trayecto de protección es suficiente para garantizar la recuperación del LSP al producirse un fallo simple en la ruta primaria, o bien el ancho de banda disponible en el trayecto de protección tendrá que ser suficiente para todo el ancho de banda adicional necesario para protegerlo.

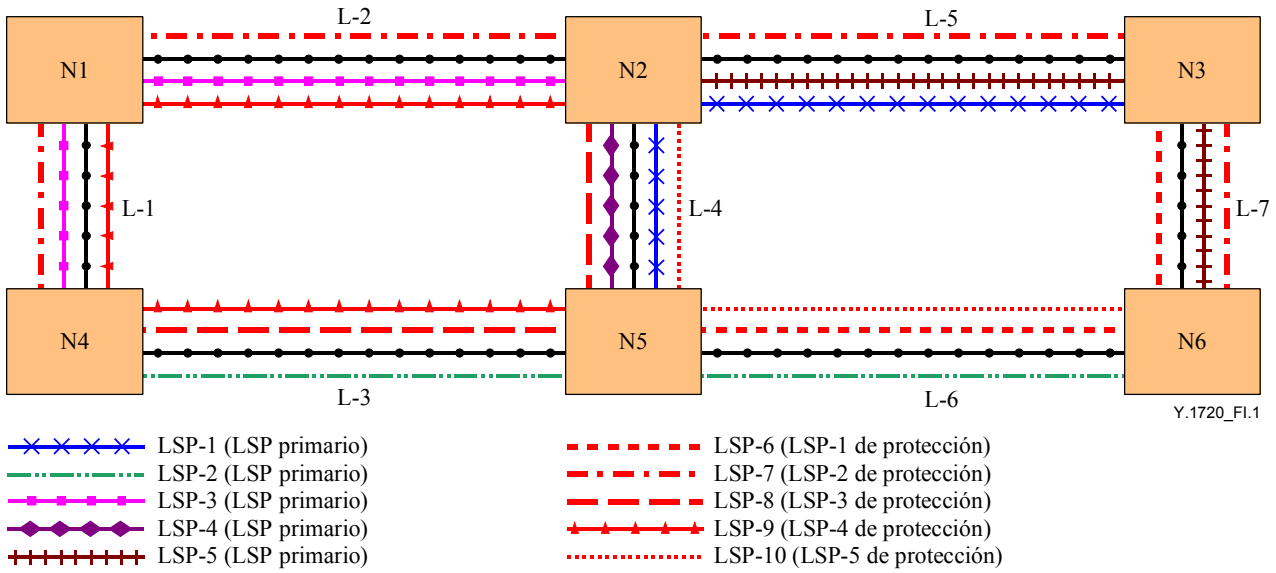

Figura I.1 – Ejemplo de trayectos de conexión principal y de protección

La compartición de la capacidad de protección entre distintos fallos puede lograrse haciendo un seguimiento a la cantidad de capacidad necesaria para que cada enlace se recupere de cada uno de esos fallos en la red. Esto se puede ilustrar mediante un ejemplo de red MPLS. En la figura I.1 se presenta un ejemplo de red con cinco conexiones principales bidireccionales junto con sus cinco conexiones de protección bidireccionales y disjuntas. (Obsérvese que cada conexión consiste de un par de LSP unidireccionales.) En este ejemplo se supondrá que para cada conexión principal se necesita una unidad de ancho de banda.

En el cuadro I.1 se muestra la capacidad de protección necesaria en cada enlace por cada posible fallo de enlace o de nodo en la red. Para comprender el cuadro I.1, considérese la primera fila correspondiente al enlace L-1. La casilla en la columna L-3 de esa fila indica que hay una unidad de tráfico, debida a LSP-2, en el enlace L-3, que podría emplear el enlace L-1 en su ruta de restablecimiento si se produjera un fallo en el enlace L-3. De manera similar, el asiento en la columna N5 contempla el caso de un fallo del nodo N5 y su repercusión en el enlace L-1. La última columna titulada Máx es el valor máximo de todas las casillas en esa fila y representa la cantidad de ancho de banda de protección que se necesita reservar en ese enlace para el caso más desfavorable de un fallo simple en la red. Por ejemplo, para el enlace L-6 este valor es de 2 unidades para tener en cuenta el caso de que fallara el enlace L-5.

Cuadro I.1 – Cuadro para seguir el curso de los fallos y el ancho de banda de protección necesario

Enlace	L-1	L-2	L-3	L-4	L-5	L-6	L-7	N1	N2	N3	N4	N5	N6	Máx
L-1			1	1		1						1		1
L-2			1	1		1						1		1
L-3	1	1		1				1						1
L-4	1	1			1		1	1		1				1
L-5			1			1						1		1
L-6				1	2		1		1	1				2
L-7			1	1	1	1			1			1		1

La información del cuadro I.1 permite saber, dada la ruta y el ancho de banda de un LSP principal, cuánta capacidad de protección adicional se necesita reservar por cada enlace a lo largo de su ruta para garantizar su protección al producirse un fallo.

En el caso de una nueva conexión protegida, el contenido del cuadro I.1 puede actualizarse modificando las filas correspondientes a los enlaces en su trayecto de protección. Esta actualización consiste en aumentar, por una cantidad igual al ancho de banda de la conexión solicitado, el valor de cada columna correspondiente a los nodos y enlaces en la ruta principal. Seguidamente, se calcula el valor máximo de cada fila actualizada como se indica en la última columna del cuadro I.1.

Cuadro I.2 – Cuadro actualizado para dar cabida a la petición de servicio "oro" adicional

Enlace	L-1	L-2	L-3	L-4	L-5	L-6	L-7	N1	N2	N3	N4	N5	N6	Máx
L-1			2	2		1						2		2
L-2			2	2		1						2		2
L-3	1	1		1				1						1
L-4	1	1			1		1	1		1				1
L-5			1			1						1		1
L-6				1	2		1		1	1				2
L-7			1	1	1	1			1			1		1

Como ejemplo, considérese la recepción de una petición de servicio de protección de malla compartida entre los nodos N4 y N2 de la red de la figura I.1. Supóngase que cuando llega la petición, la red estaba en el estado que se muestra en la figura I.1 y en el cuadro I.1. Además, supóngase que (N4-L3-N5-L4-N2) y (N4-L1-N1-L2-N2) son respectivamente, las rutas principal y de protección calculadas, para atender esta petición. Dadas estas rutas de conexión disjuntas, se actualizan los enlaces L-1 y L-2 del cuadro I.1. El cuadro actualizado se muestra en el cuadro I.2. Obsérvese que ahora se necesita una unidad de ancho de banda adicional en ambos enlaces L-1 y L-2 para garantizar la recuperación de esta nueva petición de conexión en caso de fallo a lo largo de su ruta principal.

Apéndice II

Ejemplo de aplicación de la protección 1+1 de paquete

El método de protección 1+1 de paquete puede implementarse utilizando como identificador una secuencia. El número de secuencia puede transportarse en los primeros cuatro bytes dentro de la cabecera suplementaria del LSP que proporciona la protección 1+1 de paquete. Dado que los nodos de entrada y salida deben tener conocimiento de cada LSP que participa en la protección 1+1 de paquete, el nodo de salida reconocerá que hay un número de secuencia dentro de la etiqueta. El número de secuencia lo utilizará para realizar la selección y después lo descartará antes de reenviar el paquete aceptado. Obsérvese que se puede ofrecer la protección 1+1 de paquete en cualquier nivel de la jerarquía de un LSP anidado. En la figura II.1 se ilustra la posición del número de secuencia detrás de la cabecera de encapsulado MPLS de 4 bytes.

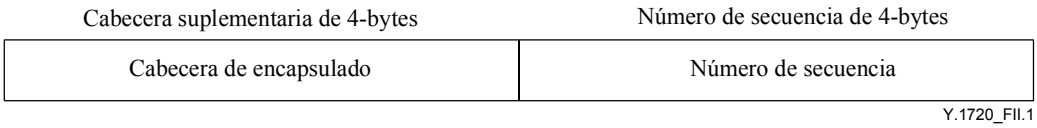

Figura II.1 – Ilustración del transporte del número de secuencia

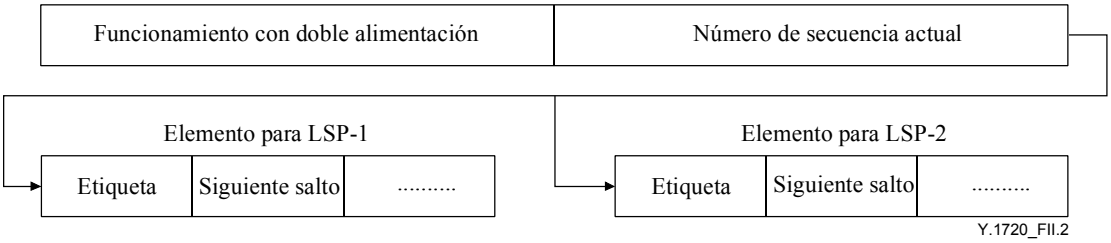

Figura II.2 – Funcionalidad NHLFE mejorada para soportar doble alimentación

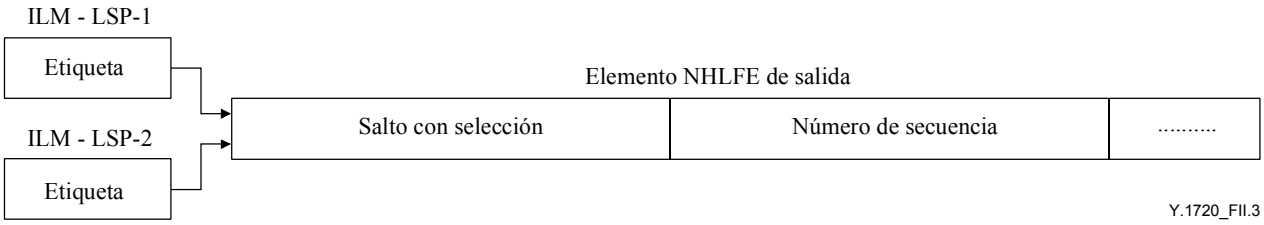

Figura II.3 – Funcionalidad NHLFE mejorada para soportar la selección

Las capacidades de doble alimentación y selección se pueden implementar en la capa suplementaria de MPLS mejorando los elementos de reenvío de etiqueta al siguiente salto (NHLFE, *next-hop-label-forward-entry*). Para proporcionar la funcionalidad de doble alimentación en el nodo de entrada, es necesario que el NHLFE soporte dos LSP de salida en lugar de uno. Esto se logra fácilmente utilizando dos elementos siguiente salto/etiqueta en lugar de uno, donde cada uno corresponde a uno de los LSP acoplados por diversidad. En la figura II.2 se ilustra este caso. Dada esta situación, cuando se reenvía el paquete de capa cliente al NHLFE que soporta doble alimentación, primero se duplica el paquete y a continuación se envía a los siguientes saltos con las etiquetas apropiadas conforme a sus dos elementos de siguiente salto/etiqueta. En la parte media de la red cada copia del paquete atraviesa el LSP de la manera convencional, como lo haría cualquier otro paquete, es decir de manera transparente a los LSR. En el nodo de salida, el mapa de etiquetas de entrada (ILM, *incoming label map*) tiene que hacer corresponder las etiquetas de los dos LSP apareados por diversidad a un solo elemento NHLFE para permitir que el lado de recepción seleccione una de las dos copias recibidas posibles. En la figura II.3 se ilustra este caso.

II.1 Mecanismo de doble alimentación y de selección

Se necesitan dos componentes para cualquier mecanismo de doble alimentación y de selección, que son:

1) la capacidad para la doble alimentación en un extremo, y

2) la capacidad para seleccionar adecuadamente una de las dos señales en el otro extremo. Por lo general, la realización de la doble alimentación es simple, mientras que la realización de la selección requiere un tratamiento cuidadoso que a menudo no es trivial. En el origen, la alimentación doble de paquetes puede hacerse copiándolos en dos trenes de paquetes. En los destinos, cada paquete se puede recibir dos veces en instantes distintos (o bien una sola vez o ninguna), en cada uno de los dos LSP. Para seleccionar adecuadamente el paquete

una sola vez, el destino debe ser capaz de identificar los paquetes duplicados y seleccionar uno, y poder manejar todas las variantes posibles. Este proceso de selección en el nivel de paquete no es trivial, dado que es posible que los paquetes duplicados no lleguen al mismo tiempo (debido al retardo de propagación y al almacenamiento intermedio) y también es posible que se pierdan algunos paquetes (debido a errores de transmisión y a la saturación de las memorias).

En el ejemplo del algoritmo siguiente se muestra un método que aborda todas estas cuestiones.

Algoritmo

Variables

```
N              /* número de bits que se utilizan para el número de secuencia */
rec_seq_no     /* número de secuencia del paquete recibido */
select_counter /* contador de N bits en el receptor que da seguimiento al número de secuencia del
                  siguiente paquete esperado */
window_sz      /* tamaño de la ventana; debe ser menor que 2^N */
```

Inicialización:

```
Rec_seq_no = 0;
select_counter = 0;
```

Algoritmo

Emisor

```
inserta rec_seq_no en la "etiqueta" interior del paquete;
transmite una copia del paquete en cada LSP apareado;
rec_seq_no ++;
```

Selector

```
Si (rec_seq_no está fuera de la ventana corrediza definida por
  [select_counter, select_counter+window_sz])
  se debe rechazar el paquete;
de lo contrario /* rec_seq_no está en la ventana */
{
    aceptar el paquete;
    select_counter = rec_seq_no +1;
}
```

II.2 Análisis del método de protección 1+1 de paquete

El nodo de entrada introduce el número de secuencia. A continuación el paquete se duplica y transporta por distintos LSP. Debido a la diversidad de los LSP, habrá un LSP destacado y un LSP de cola. El LSP destacado hará llegar los paquetes al nodo de salida más rápido que el LSP de cola. Por consiguiente, si no se producen fallos, el nodo de salida seleccionará los paquetes del LSP destacado. Los paquetes que se reciben del LSP de cola serán paquetes duplicados y por lo tanto se descartarán.

La decisión de aceptar o descartar un paquete recibido se establece a partir del número de secuencia del paquete recibido y de un contador + una ventana corrediza en el nodo de salida. El contador indica el número de secuencia previsto del siguiente paquete. El contador y la ventana corrediza proporcionan una ventana de números de secuencia aceptables. La ventana corrediza es necesaria

para aceptar y rechazar paquetes adecuadamente. Si el paquete recibido entra dentro de la ventana, se considera legítimo y puede aceptarse. De lo contrario, se rechaza. El tamaño de la ventana debe ser más grande que el número máximo de paquetes consecutivos que puede perder un LSP principal (activo).

La ventana corrediza se utiliza para resolver el problema de paquetes perdidos en el LSP destacado cuando el número de secuencia del LSP destacado es muy cercano al punto de retorno a cero. En la figura II.4 se ilustra un LSP destacado (LSP 1) que transporta un paquete con el número de secuencia 29. El paquete se acepta y el contador se incrementa a 30. Si suponemos que se pierden dos paquetes consecutivos (es decir, los paquetes con los números de secuencia 30 y 31), el siguiente paquete que se recibe en el LSP 1 será el número 0. Sin una ventana corrediza, el nodo de salida rechazará el paquete ya que 0 < 30. Al implementar una ventana de este tipo que sea más grande que el número máximo de paquetes consecutivos que puede perder un LSP principal (activo), se puede resolver este problema. Por ejemplo, supóngase que el número máximo de paquetes consecutivos que puede perder un LSP principal sea 5, por consiguiente se puede definir una ventana corrediza para 6 paquetes. Utilizando el mismo ejemplo, pero ahora con la ventana corrediza, el nodo de salida aceptará paquetes en la gama de {30, 31, 0, 1, 2, 3}. Por consiguiente, aun si se hubieran perdido 5 paquetes (es decir, el número máximo de paquetes consecutivos que se pueden perder en un LSP principal) el siguiente paquete recibido tendrá un número de secuencia 3 y será aceptado.

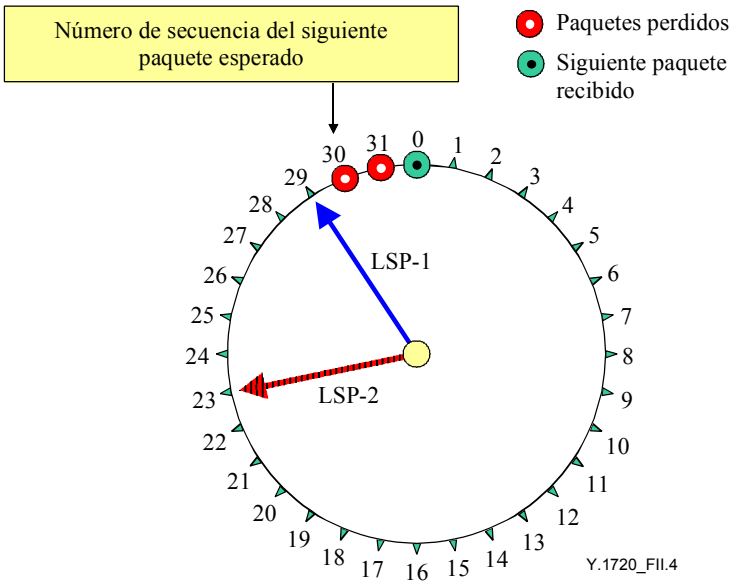

Figura II.4/Y.1720 – Pérdida de paquetes y retorno a cero

Obsérvese que la idea de la ventana corrediza funciona únicamente si el LSP que se queda retrasado (el de cola) no puede caer en la gama de valores de la ventana corrediza. Si se recibe un paquete del LSP de cola con un número de secuencia en la gama de valores de la ventana corrediza, en ese caso se aceptará indebidamente. Un LSP sólo puede recibir un paquete con un número de secuencia en la gama de valores de la ventana corrediza si se rezaga por más que (2^N – tamaño de la ventana corrediza). Por lo tanto, el número de bits *N* utilizado para el número de secuencia debe soportar la siguiente ecuación:

$$2^N > \text{Ventana corrediza} + \text{Ventana de retardo}$$

donde:

Ventana corrediza > número máximo de paquetes consecutivos que se pueden perder en un LSP

y

Ventana de retardo = número máximo de paquetes del LSP de cola que pueden llegar retrasados con respecto al LSP destacado.

Obsérvese que el campo de 4 bytes permite una secuencia de más de 4 billones de números que es lo suficientemente grande para dar cabida a las pérdidas de paquetes y diferencias de retardo consecutivas en el caso más desfavorable.

Una forma razonable de diseñar el tamaño de las ventanas corredizas y de retardo es que el tamaño de la ventana corrediza sea igual al tamaño de la ventana de retardo. (Obsérvese que se supone que el tamaño de la ventana de retardo es generalmente más grande que el de la ventana corrediza.) Esto garantiza la selección de los paquetes del LSP destacado en todos los casos después de la reparación de un LSP que ha fallado. Este punto se desarrolla más detalladamente en la siguiente cláusula en la que se discuten distintos casos de fallo.

II.2.1 Funcionamiento del mecanismo de selección en varios casos de fallo

Una manera de considerar el funcionamiento del mecanismo de selección es imaginarse un reloj con 2^N intervalos. En la figura II.5 se ilustra un ejemplo donde N = 4 (es decir, número de secuencia de 4 bits) y por consiguiente el número de secuencia va de 0 a 15. En este ejemplo, la ventana corrediza se pone igual a la ventana de retardo, es decir a 5.

En la figura II.5 se representa el LSP destacado adelante del LSP de cola por 3 números de secuencia. El LSP destacado entrega un paquete con número de secuencia = 1 y el contador se pone ahora a 2.

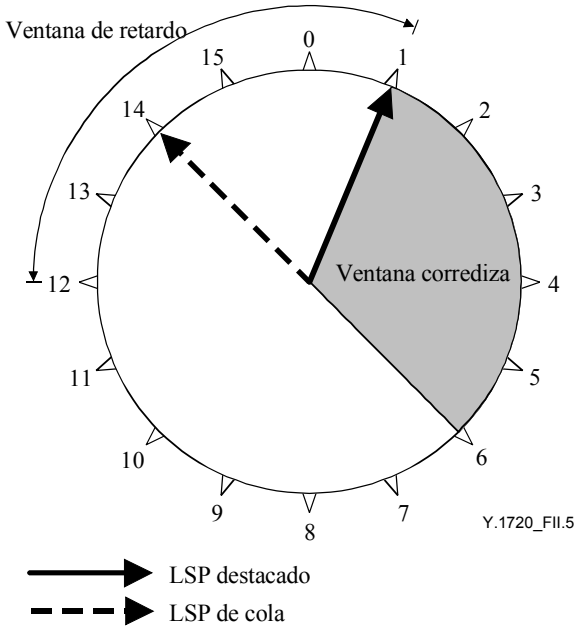

Figura II.5/Y.1720 – Concepto de ventana corrediza y ventana de retardo

En la figura II.6 se muestra que antes de recibir un paquete con el número de secuencia igual a 2 en el LSP destacado, se produce un fallo en este último. Hasta que el LSP de cola entrega el paquete con el número de secuencia igual a 2, el nodo de salida no seleccionará ningún paquete y el contador permanecerá igual a 2.

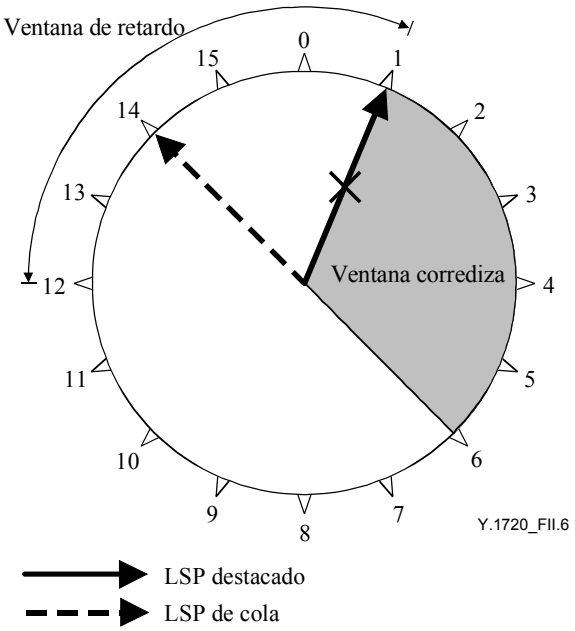

Figura II.6/Y.1720 – Escenario de fallo en el LSP de cabecera

En la figura II.7 se ilustra que cuando se recibe el paquete con el número de secuencia igual a 2 en el LSP de cola, el nodo de salida aumenta el contador a 3 y la ventana corrediza se mueve de manera que se pueda aceptar un paquete con números de secuencia en la gama de valores de 3 a 7.

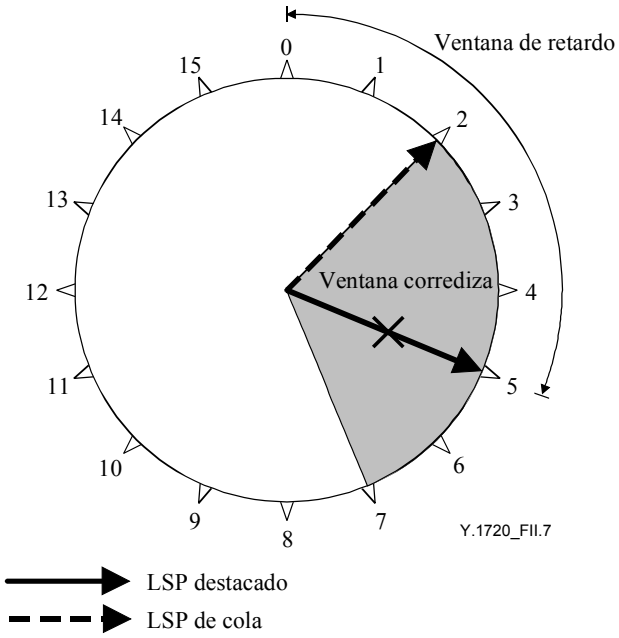

Figura II.7/Y.1720 – Recuperación del tráfico tras el fallo en el LSP de cabecera

En la figura II.8 se muestra que antes de recibirse un paquete con número de secuencia igual a 3 del LSP de cola, se repara el LSP destacado y se recibe un paquete con número de secuencia igual a 6 del LSP destacado. Ya que el número 6 está dentro de la gama de valores de la ventana corrediza, se acepta el paquete. Obsérvese que es importante que mientras esté funcionando el LSP destacado, los paquetes deben recibirse de este último. Por lo tanto, para garantizar que cuando se repara el LSP destacado hará llegar un paquete con un valor de número de secuencia que esté dentro de la gama de valores de la ventana corrediza, esta última debe ser igual a la ventana de retardo, o mayor que ella, que es el caso para este ejemplo.

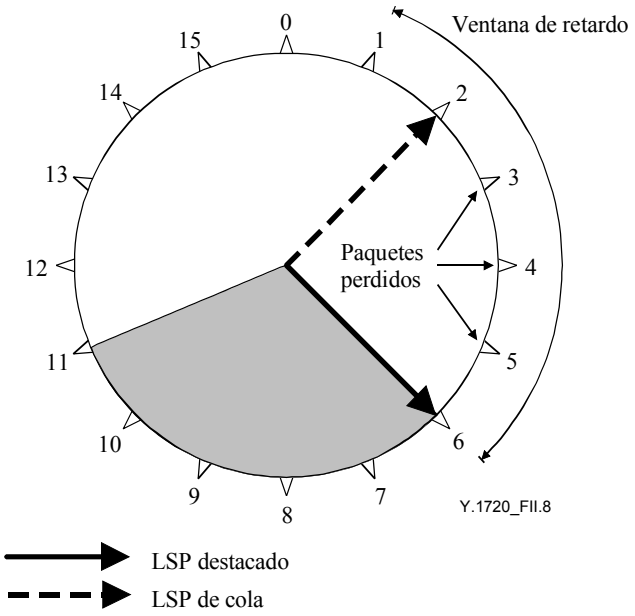

Figura II.8/Y.1720 – Escenario de reparación del LSP de cabecera

En las figuras II.9, II.10 y II.11 se presenta un problema en el que la ventana corrediza se configura más pequeña que la ventana de retardo. En este caso, es posible que cuando se repara el LSP destacado, entregará paquetes con números de secuencia que caen fuera de la ventana corrediza y por consiguiente el nodo de salida continúa aceptando paquetes del LSP de cola. Si posteriormente falla el LSP de cola, existe la posibilidad de perder muchos paquetes (el caso más desfavorable sería 2^N–*tamaño de la ventana corrediza*, donde N es el número de bits que se utiliza para el número de secuencia).

En la figura II.9 se ilustra un ejemplo en el que la ventana corrediza se configura a 3 y la ventana de retardo puede ser de hasta 6. En este ejemplo, el LSP de cola se retrasa con respecto a LSP destacado por 4 números de secuencia. Como el LSP destacado tiene fallo, los paquetes se seleccionan del LSP de cola.

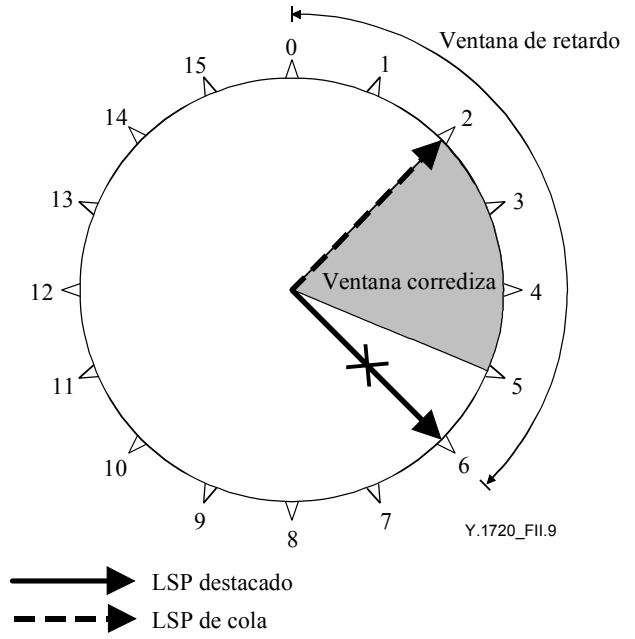

Figura II.9/Y.1720 – Escenario en que la ventana deslizante es inferior a la ventana de retardo

En la figura II.10 se ilustra que en el momento en que se repara el LSP destacado, entrega un paquete con un número de secuencia igual a 7 que cae fuera de la ventana corrediza y por consecuencia se rechaza. Los paquetes continúan seleccionándose del LSP de cola.

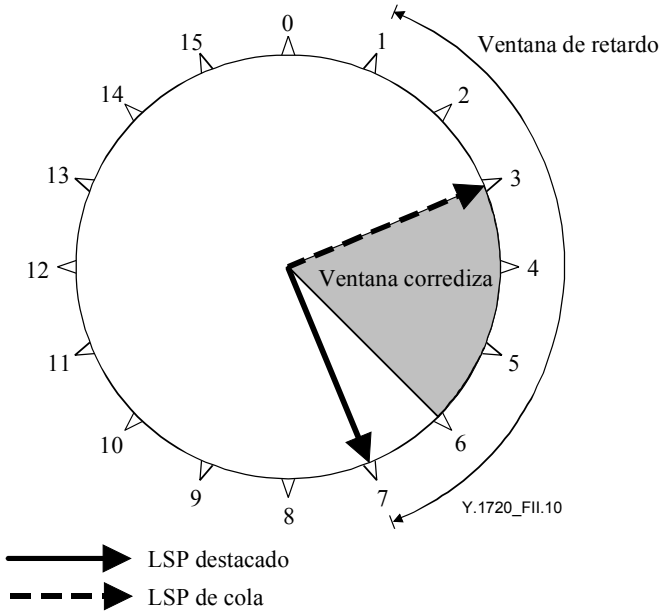

Figura II.10/Y.1720 – Reparación del LSP: ventana deslizante inferior a la ventana de retardo

En la figura II.11 se muestra que se produce un fallo en el LSP de cola. Como el LSP destacado está entregando paquetes que caen fuera de la ventana corrediza y por consiguiente se rechazan, el nodo de salida no comenzará a aceptar paquetes hasta que el LSP destacado da toda la vuelta y comienza a entregar paquetes con un número de secuencia que cae dentro de la ventana corrediza. Esto puede dar por resultado una pérdida significativa de paquetes. Por lo tanto, para evitar esa posibilidad, se recomienda que con este tipo de algoritmo de selección se configure la ventana corrediza igual a la ventana de retardo.

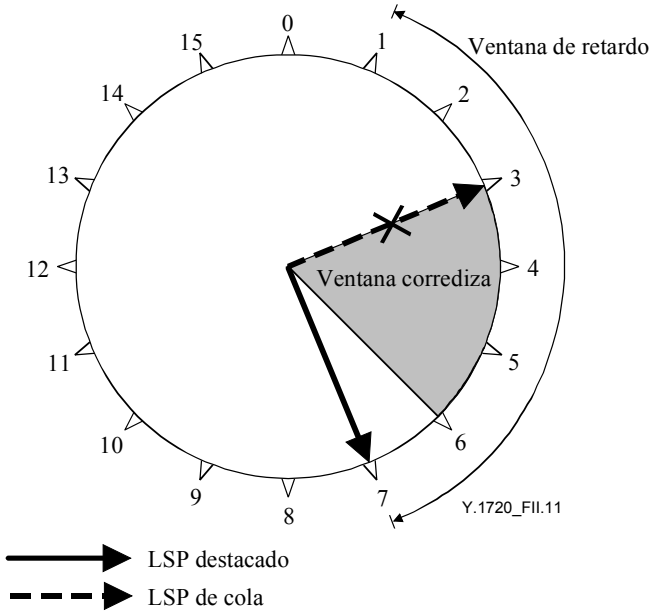

Figura II.11/Y.1720 – Posible problema cuando la ventana deslizante es inferior a la ventana de retardo

II.2.2 Comentarios adicionales

a) El método requiere inteligencia únicamente en los nodos en el borde. Además, el método no requiere ninguna detección o notificación explícita de los fallos. Esto se deduce del método de selección de paquetes en la salida, que se realiza basándose en el número de secuencia y en los contadores que se mantienen localmente.

b) El procedimiento de doble alimentación requiere la duplicación de los paquetes en la entrada. Esto introduce un tratamiento mínimo adicional en la entrada. El método de selección exige la comparación del número de secuencia transportado en el paquete con el valor del contador conservado en el receptor conduciendo a una condición de aceptación o rechazo del paquete. En el caso de implementación de equipos o programas informáticos, el costo de tratamiento es mínimo. Otra repercusión en la calidad de funcionamiento es el costo del ancho de banda debido al número de secuencia transportado en los paquetes. Esto introduce alguna tara de paquetes adicionales en función de la longitud del número de secuencia. Con un número de secuencia de 32 bits utilizando toda la etiqueta de 4 bytes, la tara de ancho de banda es simplemente de 4% para paquetes cortos de 100 bytes.

c) La pérdida de calidad de funcionamiento del servicio propuesto se puede considerar de la siguiente manera. Como el mecanismo de selección en el nodo de salida recibe los paquetes de cualquier LSP, de hecho el servicio puede compensar, aunque no es necesario, las pérdidas de paquetes en la red. En el mejor caso, esto podría dar por resultado una pérdida nula aunque cada LSP puede sufrir pérdidas. Por otro lado, en el caso más desfavorable, la pérdida de paquetes global sería la suma de las pérdidas de ambos LSP. En otras palabras, la pérdida de calidad de funcionamiento del servicio no será peor que el mismo orden de magnitud del LSP con la peor calidad de funcionamiento y algunas veces podría ser incluso mucho mejor.

d) La característica de retardo del servicio propuesto se puede considerar de la siguiente manera. Como el algoritmo siempre selecciona, sin almacenamiento intermedio, el primer paquete elegible que se recibe del par, la característica de retardo siempre es mejor que cualquiera de la de los LSP.

e) El tamaño de la ventana debe configurarse de manera que sea más grande que el número máximo de paquetes consecutivos que puede perder un LSP destacado. Como resultado, se garantiza que el número de secuencia del siguiente paquete del mismo LSP siempre caerá dentro de la ventana y se aceptará.

f) El tamaño de la ventana debe configurarse de manera que la diferencia de retardo de los pares de paquetes que pasan por los LSP apareados, si no se pierden, nunca sea más de (2^N – tamaño de la ventana) paquetes. Como resultado, se garantiza que un paquete antiguo no se confundirá con un paquete nuevo que pueda provocar entregas erróneas.

g) En el caso de un fallo simple en la red, en un lugar distinto de los nodos de entrada o salida, sólo se verá afectado uno de los LSP apareado por diversidad. El LSP superviviente continuará entregando los paquetes. Si el LSP superviviente es el LSP destacado, es decir, el último paquete recibido y seleccionado provenía de este LSP, en ese caso la función de selección en el nodo de salida continuará aceptando paquetes del mismo LSP mientras que si el LSP superviviente es el LSP de cola, en ese caso la función de selección rechaza los paquetes hasta que encuentra un paquete cuyo número de secuencia cae dentro de la ventana corrediza. Cuando el LSP con fallo se repara satisfactoriamente, convendría ponerlo de nuevo en servicio. En este "modo de restablecimiento reversivo", el método más simple sería permitir que el primer paquete alimentado por duplicado obtenga el siguiente número de secuencia usual, a continuación del asignado al último paquete alimentado solamente al LSP superviviente. Se pueden realizar varias mejoras para gestionar la característica de pérdida del servicio durante esta operación, si se desea.

h) En caso de que ambos LSP fallen, será necesario definir mecanismos adicionales para mantener el servicio y los estados asociados de los LSP para garantizar operaciones robustas.

Apéndice III

Bibliografía

IETF, RFC3469 (2003), *Framework for MPLS-based Recovery, Category: Informational*.

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, aspectos del protocolo Internet y Redes de la próxima generación**
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Ginebra, 2004