

Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

G.808.3

(10/2012)

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

Redes digitales – Generalidades

**Conmutación de protección genérica –
Protección por malla compartida**

Recomendación UIT-T G.808.3

RECOMENDACIONES UIT-T DE LA SERIE G
SISTEMAS Y MEDIOS DE TRANSMISIÓN, SISTEMAS Y REDES DIGITALES

CONEXIONES Y CIRCUITOS TELEFÓNICOS INTERNACIONALES	G.100–G.199
CARACTERÍSTICAS GENERALES COMUNES A TODOS LOS SISTEMAS ANALÓGICOS DE PORTADORAS	G.200–G.299
CARACTERÍSTICAS INDIVIDUALES DE LOS SISTEMAS TELEFÓNICOS INTERNACIONALES DE PORTADORAS EN LÍNEAS METÁLICAS	G.300–G.399
CARACTERÍSTICAS GENERALES DE LOS SISTEMAS TELEFÓNICOS INTERNACIONALES EN RADIOENLACES O POR SATÉLITE E INTERCONEXIÓN CON LOS SISTEMAS EN LÍNEAS METÁLICAS	G.400–G.449
COORDINACIÓN DE LA RADIOTELEFONÍA Y LA TELEFONÍA EN LÍNEA	G.450–G.499
CARACTERÍSTICAS DE LOS MEDIOS DE TRANSMISIÓN Y DE LOS SISTEMAS ÓPTICOS	G.600–G.699
EQUIPOS TERMINALES DIGITALES	G.700–G.799
REDES DIGITALES	G.800–G.899
Generalidades	G.800–G.809
Objetivos de diseño para las redes digitales	G.810–G.819
Sincronización, objetivos de calidad y disponibilidad	G.820–G.829
Funciones y capacidades de la red	G.830–G.839
Características de las redes con jerarquía digital síncrona	G.840–G.849
Gestión de red de transporte	G.850–G.859
Integración de los sistemas de satélite y radioeléctricos con jerarquía digital síncrona	G.860–G.869
Redes ópticas de transporte	G.870–G.879
SECCIONES DIGITALES Y SISTEMAS DIGITALES DE LÍNEA	G.900–G.999
CALIDAD DE SERVICIO Y DE TRANSMISIÓN MULTIMEDIOS – ASPECTOS GENÉRICOS Y ASPECTOS RELACIONADOS AL USUARIO	G.1000–G.1999
CARACTERÍSTICAS DE LOS MEDIOS DE TRANSMISIÓN	G.6000–G.6999
DATOS SOBRE CAPA DE TRANSPORTE – ASPECTOS GENÉRICOS	G.7000–G.7999
ASPECTOS RELATIVOS A LOS PROTOCOLOS EN MODO PAQUETE SOBRE LA CAPA DE TRANSPORTE	G.8000–G.8999
REDES DE ACCESO	G.9000–G.9999

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

Recomendación UIT-T G.808.3

Conmutación de protección genérica – Protección por malla compartida

Resumen

En la Recomendación UIT-T G.808.3 se presenta una panorámica general de los aspectos genéricos de un mecanismo de protección por malla compartida para redes de capa con conexión que no depende de la presencia de un plano de control. La protección por malla compartida proporciona un método de intercambio de recursos en una red de malla para protegerse de uno o más fallos en la red.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T G.808.3	2012-10-29	15	11.1002/1000/11788

* Para acceder a la Recomendación, sírvase digitar el URL <http://handle.itu.int/> en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, <http://handle.itu.int/11.1002/1000/11830-en>.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) 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/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 en la dirección <http://www.itu.int/ITU-T/ipr/>.

© UIT 2017

Reservados todos los derechos. Ninguna parte de esta publicación puede reproducirse por ningún procedimiento sin previa autorización escrita por parte de la UIT.

ÍNDICE

	Página
1 Alcance	1
2 Referencias	1
3 Definiciones.....	1
3.1 Términos definidos en otros documentos.....	1
3.2 Términos definidos en esta Recomendación	2
4 Abreviaturas y acrónimos	3
5 Convenios	3
6 Aspectos generales.....	3
6.1 Topologías en malla	3
6.2 Consideraciones sobre la eficacia de capacidad.....	4
7 Tipos de arquitectura SMP	4
7.1 Generalidades de la arquitectura SMP	4
8 Tipos de conmutación.....	9
9 Tipos de funcionamiento	9
10 Tráfico no protegido y no prioritario (NUT) y tráfico extraordinario.....	9
11 Conmutación automática	9
12 Principio de prioridad	9
13 Supervisión del estado del trayecto	9
14 Protocolo de conmutación de protección automática (APS)	10
Anexo A – Objetivos.....	11
Apéndice I – Hipótesis de uso de la SMP.....	13
I.1 SMP simple	13
I.2 SMP en una red en malla.....	13
Apéndice II – Generalidades del funcionamiento del restablecimiento en malla compartida (SMR) y la protección en malla compartida (SMP).....	18
Bibliografía	19

Recomendación UIT-T G.808.3

Conmutación de protección genérica – Protección por malla compartida

1 Alcance

En esta Recomendación se presenta una panorámica general de los aspectos genéricos de un mecanismo de protección por malla compartida para redes de capa con conexión que no depende de la presencia de un plano de control. Este mecanismo está destinado a las arquitecturas de red en malla, que utilizan más eficazmente los recursos de protección. La característica primaria de este método de protección por trayectos es que conlleva la utilización previa de la computación y la atribución de recursos para maximizar la velocidad de recuperación. Los mecanismos de protección por malla compartida para cada tecnología concreta se definirán en Recomendaciones específicas a cada tecnología.

En esta versión de la Recomendación se facilita un marco arquitectónico para la protección por malla compartida.

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.

- [UIT-T G.780] Recomendación UIT-T G.780/Y.1351 (2010), *Términos y definiciones para las redes de jerarquía digital síncrona*.
- [UIT-T G.805] Recomendación UIT-T G.805 (2000), *Arquitectura funcional genérica de las redes de transporte*.
- [UIT-T G.806] Recomendación UIT-T G.806 (2006), *Características del equipo de transporte – Metodología de descripción y funcionalidad genérica*.
- [UIT-T G.808.1] Recomendación UIT-T G.808.1 (2010), *Conmutación de protección genérica – Protección lineal de camino y de subred*.
- [UIT-T G.870] Recomendación UIT-T G.870/Y.1352 (2010), *Términos y definiciones para redes ópticas de transporte*.

3 Definiciones

3.1 Términos definidos en otros documentos

En la presente Recomendación se emplean los siguientes términos definidos en otros documentos:

3.1.1 Términos relativos a las acciones

3.1.1.1 conmutador [UIT-T G.870]

3.1.2 Términos relativos a los componentes

3.1.2.1 puente [UIT-T G.870]

3.1.2.2 selector [UIT-T G.870]

- 3.1.2.3 **nodo intermedio** [UIT-T G.870]
- 3.1.3 **Términos relativos a las condiciones de fallo**
 - 3.1.3.1 **degradación de la señal (SD)** [UIT-T G.805]
 - 3.1.3.2 **fallo de la señal (SF)** [UIT-T G.805]
- 3.1.4 **Términos relativos a la arquitectura**
 - 3.1.4.1 **arquitectura (de protección) m:n** [UIT-T G.870]
- 3.1.5 **Términos relativos al funcionamiento**
 - 3.1.5.1 **funcionamiento (de protección) reversible** [UIT-T G.870]
- 3.1.6 **Términos relativos a las señales**
 - 3.1.6.1 **señal de tráfico** [UIT-T G.870]
 - 3.1.6.2 **señal de tráfico normal** [UIT-T G.870]
 - 3.1.6.3 **señal de tráfico extraordinario** [UIT-T G.870]
- 3.1.7 **Términos relativos a la conmutación**
 - 3.1.7.1 **conmutación (de protección) bidireccional** [UIT-T G.780]
 - 3.1.7.2 **conmutación (de protección) unidireccional** [UIT-T G.780]
- 3.1.8 **Términos relativos a las entidades de transporte**
 - 3.1.8.1 **enlace** [UIT-T G.805]
 - 3.1.8.2 **entidad de transporte** [UIT-T G.870]
 - 3.1.8.3 **entidad de transporte de protección** [UIT-T G.870]
 - 3.1.8.4 **entidad de transporte de trabajo** [UIT-T G.870]
- 3.1.9 **protección** [UIT-T G.870]
- 3.1.10 **restablecimiento** [UIT-T G.870]
- 3.1.11 **evento de conmutación** [UIT-T G.870]

3.2 **Términos definidos en esta Recomendación**

En la presente Recomendación se definen los términos siguientes:

- 3.2.1 **segmento de protección:** Enlace entre dos nodos de protección en malla compartida en una entidad de transporte de protección.
- 3.2.2 **protección en malla compartida:** Una arquitectura de protección en malla compartida conlleva múltiples señales de tráfico normal, cada una de las cuales tiene una entidad de transporte de trabajo correspondiente y una o más entidades de transporte de protección, en una red en malla. En la protección en malla compartida los recursos de protección están compartidos entre dos o más entidades de transporte de protección. Sólo una de esas entidades de transporte de protección puede utilizar los recursos de protección compartidos a la vez.
- 3.2.3 **segmento de protección compartida:** Enlace entre dos nodos de protección en malla compartida en que el ancho de banda del enlace está compartido entre múltiples entidades de transporte de protección.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas y acrónimos:

APS	Conmutación de protección automática (<i>automatic protection switching</i>)
NUT	Tráfico no protegido y no prioritario (<i>non-pre-emptible unprotected traffic</i>)
OTN	Red óptica de transporte (<i>optical transport network</i>)
P	Protección (<i>protection</i>)
SD	Degradación de la señal (<i>signal degrade</i>)
SDH	Jerarquía digital síncrona (<i>synchronous digital hierarchy</i>)
SF	Fallo de la señal (<i>signal fail</i>)
SMP	Protección en malla compartida (<i>shared mesh protection</i>)
W	Trabajo (<i>working</i>)

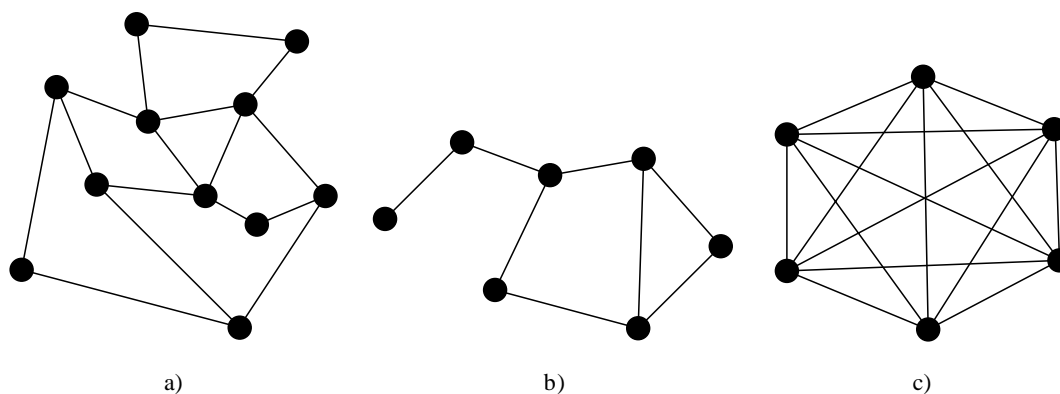
5 Convenios

Ninguno.

6 Aspectos generales

6.1 Topologías en malla

Una red de transporte en malla es aquella en que cada uno de los nodos de la red está interconectado por al menos dos enlaces cuyos extremos distantes se encuentran en nodos diferentes (véase el ejemplo a) de la Figura 1). Cabe señalar que, si bien la red de transporte general puede contener nodos que no satisfacen el criterio anterior (véanse los dos nodos a la izquierda en el ejemplo b) de la Figura 1), éstos no se considerarán parte de la porción de la red de transporte definida como una malla. Una topología en malla completa es aquella en la que cada nodo está directamente conectado a todos y cada uno de los nodos de la red (véase el ejemplo c) de la Figura 1).



G.808.3(12)_F01

- a): Ejemplo de red en malla
- b): Ejemplo de red donde sólo una parte es una malla
- c): Ejemplo de red en malla completa

Figura 1 – Ejemplos de red en malla

La mayoría de las redes de transporte en malla lo son sólo parcialmente (como en el ejemplo a) de la Figura 1), con algunos nodos en malla completa y otros conectados a uno o más nodos, pero no a todos (es decir, que su número máximo es inferior al total de número de nodos – 1). Aunque las

topologías en malla completa ofrecen un grado más elevado de supervivencia en caso de fallo, también tienen un mayor grado de redundancia de recursos de transporte. La mayoría de redes de transporte en malla lo son sólo parcialmente y por lo general necesitan nodos intermedios de paso para ir de un nodo a todos y cada uno de los demás nodos.

6.2 Consideraciones sobre la eficacia de capacidad

De la mayor compartición de los recursos de protección en las arquitecturas de red en malla se deriva naturalmente una reducción de los costos de red, al eliminarse los recursos de protección dedicados. Tales arquitecturas pueden diseñarse también en función del nivel de "protección garantizada" y de la eficiencia de las capacidades que desea el operador para cada nivel de los servicios que ofrece. La eficiencia de las capacidades en las arquitecturas de red en malla puede medirse de distintas maneras, incluidas las siguientes [b-BLTJ.1999]:

- i) la fracción de las demandas puede protegerse en función de las capacidades de red, de las demandas punto a punto y del trayecto de trabajo de cada demanda;
- ii) las capacidades de red necesarias para ofrecer una protección del 100% a las demandas punto a punto y el trayecto de trabajo de cada demanda; o
- iii) las capacidades de red totales para los trayectos de trabajo y protección de las demandas punto a punto y a los que se ofrece una protección del 100%.

El primer método conlleva la detección de los trayectos de protección para el mayor número de demandas posible dadas las limitaciones de capacidad de enlace en una red existente, lo que difiere de los dos últimos métodos, que asumen que la planificación de la capacidad se lleva a cabo para garantizar la protección al 100% de todas las demandas.

Cabe señalar que llega un punto en que el grado deseado de optimización de los recursos de red (lo que resulta en una insuficiencia de la capacidad del enlace) es inversamente proporcional al grado de "protección garantizada" que puede ofrecerse. En situaciones de capacidad limitada reales es necesario poder establecer la prioridad de las demandas y garantizar que a aquéllas con mayores requisitos de disponibilidad se les asignan siempre trayectos de protección.

En el marco de esta Recomendación el objetivo es lograr la mayor protección posible habida cuenta de las capacidades de una red dada, incluidos los mecanismos para determinar la prioridad de las demandas y permitir que a aquéllas con mayores requisitos de disponibilidad se les asignan trayectos de protección.

7 Tipos de arquitectura SMP

7.1 Generalidades de la arquitectura SMP

La SMP puede emplearse en redes de transporte en malla completa o parcial, que comprenden, aunque no únicamente, las redes de largo alcance y las redes metropolitanas. En función del grado de interconexión de los nodos de la red, la SMP puede mejorar notablemente la utilización de los recursos de la red, en comparación con los mecanismos de protección 1:1 alternativos.

Una arquitectura SMP conlleva múltiples señales de tráfico normal, cada una de ellas asociada a una entidad de transporte de trabajo y a una o más entidades de transporte de protección. La arquitectura SMP se basa en la protección m:1 (donde m puede ser igual o superior a uno).

En una arquitectura SMP m:1 cada entidad de transporte de trabajo está protegida por m entidades de transporte de protección. En esta arquitectura, la entidad de transporte de trabajo puede estar protegida cuando una de las m entidades de transporte de protección esté disponible.

Cada entidad de transporte de protección está formada por uno o varios segmentos de protección. El ancho de banda de cada segmento de protección puede estar compartido por múltiples entidades de transporte de protección. Para evitar que un fallo de red interrumpa la señal de tráfico normal

protegida, se recomienda que todas las entidades de transporte de trabajo compartan los recursos de protección estén separadas.

El ancho de banda compartido del segmento de protección debe poder soportar la mayor de las entidades de transporte de protección correspondientes.

NOTA – Los recursos de protección y la información de las entidades de transporte de protección están preconfiguradas mediante un plano de control o de gestión y queda fuera del alcance de esta Recomendación la descripción detallada de ese proceso de preconfiguración. Queda también fuera del alcance de esta Recomendación el mecanismo de restablecimiento en malla (compartida) basado en un plano de control.

En la Figura 2 se muestra un ejemplo de arquitectura SMP m:1 simple. Hay dos entidades de transporte de trabajo, W1 (A-B) y W2 (E-F). En este ejemplo las entidades de transporte de protección se han configurado de la siguiente manera:

- para W1 hay dos entidades de transporte de protección P1 (A-C-D-B) y P1' (A-G-H-B);
- para W2 hay una entidad de transporte de protección P2 (E-C-D-F).

Si se detecta un fallo en W2, la entidad de protección correspondiente, P2, se activará para transmitir el tráfico. Como el ancho de banda del segmento de protección PS3 está totalmente ocupado por P2, la entidad de transporte de protección P1 carece de capacidad para proteger la entidad de transporte de trabajo W1, para cuya protección puede utilizarse la otra entidad de transporte de protección P1'.

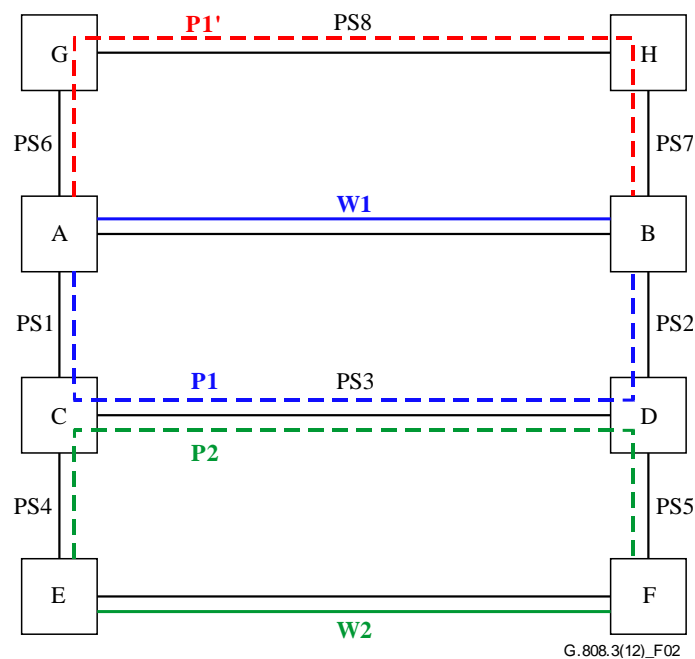


Figura 2 – Ejemplo de arquitectura SMP m:1

En la Figura 3 se muestra un ejemplo de arquitectura SMP m:1 simple, donde $m = 1$.

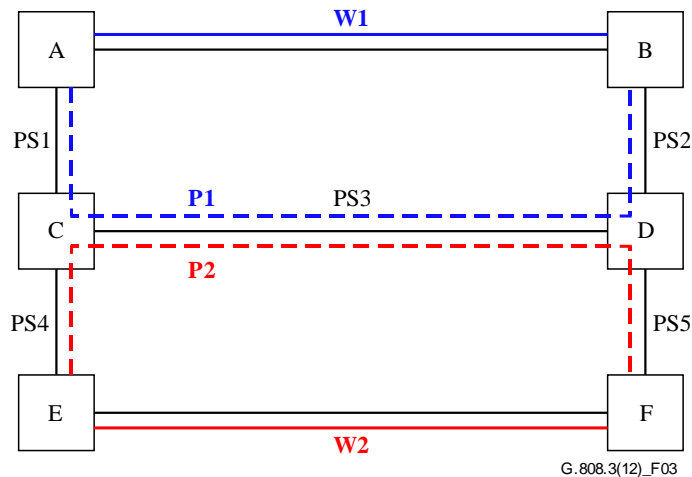


Figura 3 – Ejemplo de arquitectura SMP 1:1

7.1.1 SMP para redes de circuitos

En las redes con conmutación de circuitos (por ejemplo, SDH/OTN), no es posible establecer previamente la transconexión de los nodos intermedios de la entidad de transporte de protección cuando múltiples entidades de transporte de protección comparten el segmento de protección. En este caso, los nodos intermedios deben establecer la transconexión para la entidad de transporte de protección cuando se detecta que la entidad de transporte de trabajo entra en fallo.

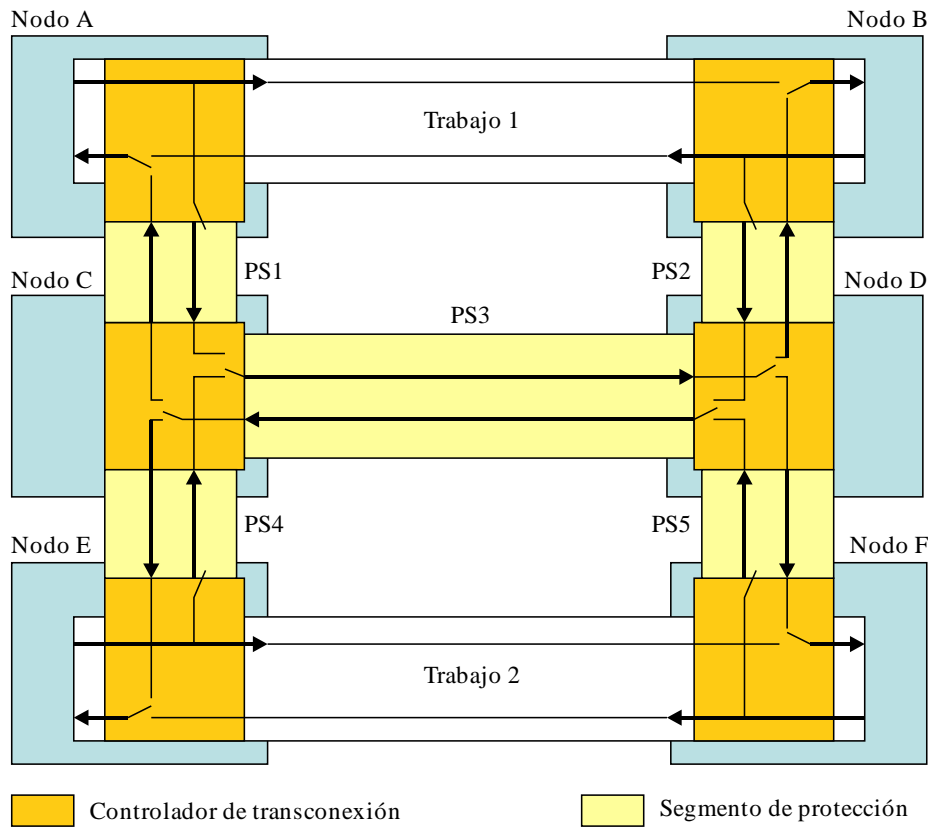
Los puntos extremos de cada entidad de transporte de trabajo deben tener las funciones necesarias para supervisar el estado de la entidad de transporte de trabajo. La detección de un estado de fallo de la señal/degradación de la señal (SF/SD) activará el procedimiento de conmutación de protección. Al mismo tiempo, los nodos a lo largo de la entidad de transporte de protección ejercerán también las funciones de supervisión del estado de los recursos de cada segmento de protección. El peor de entre todos los estados del segmento de protección a lo largo de la entidad de transporte de protección se notificará a los puntos extremos. Si el estado de la entidad de transporte de protección es peor que el de las entidades de transporte de trabajo, los puntos extremos impedirán que la señal de tráfico normal se conmute a la entidad de transporte de protección.

En la Figura 4 se muestra la SMP para una red de circuitos. La transconexión de los nodos intermedios de las entidades de transporte de protección no está preestablecida. Las conexiones de enlace pueden no atribuirse antes de detectar el fallo, como se muestra en el diagrama b) de la Figura 4.

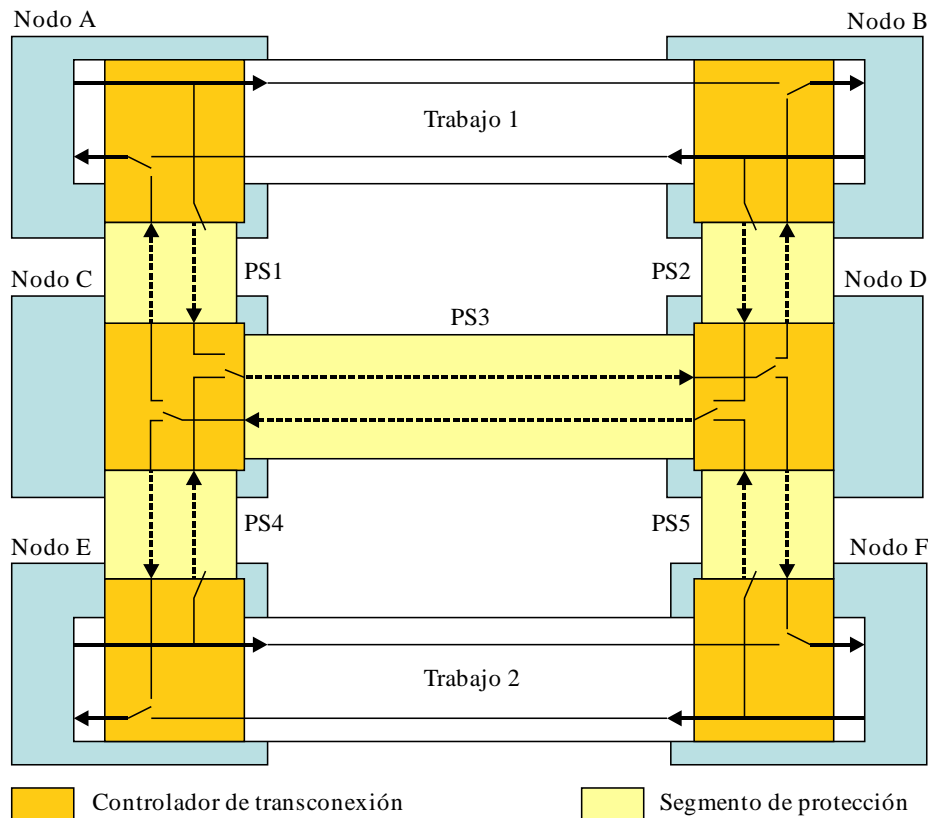
Los puntos extremos (por ejemplo, nodo A/B, nodo E/F) supervisarán el estado de Trabajo 1 (W1) y de Trabajo 2 (W2). Los nodos a lo largo de las dos entidades de transporte de protección (es decir, P1 y P2) supervisarán el estado de cada una de ellas.

Cuando se detecte una degradación o fallo de la entidad de transporte de trabajo W1, y si se dispone del estado de la entidad de transporte de protección, al recibir la señal APS, el nodo C debe establecer la transconexión entre PS1 y PS3 y el nodo D debe establecer la transconexión entre PS3 y PS2 para activar la entidad de transporte de protección P1. En el caso del diagrama b) de la Figura 4, se han de establecer las conexiones de enlace de PS1, PS3 y PS2.

NOTA – Por mor de sencillez, en la Figura 4 se muestra una arquitectura SMP 1:1 para las redes de circuitos. Este ejemplo puede ampliarse a una arquitectura SMP m:1, donde hay múltiples entidades de transporte de protección por cada entidad de transporte de trabajo.



a) SMP para red de circuitos con transconexión preestablecida



b) SMP para red de circuitos sin transconexión preestablecida

G.808.3(12)_F04

Figura 4 – Ejemplos de SMP para red de circuitos

7.1.2 SMP para redes de paquetes

En las redes con conmutación de paquetes se pueden preestablecer distintas entidades de transporte de protección que compartan el mismo ancho de banda del segmento de protección compartido. En condiciones normales, cuando las señales de tráfico normal se transportan a través de las entidades de transporte de trabajo, sólo los paquetes APS y OAM se transportarán a través de las entidades de transporte de protección. El ancho de banda de un segmento de protección compartido debe atribuirse de manera que se pueda proteger cualquiera de las entidades de transporte de trabajo cuyas entidades de transporte de protección comparten el segmento de protección.

Los puntos extremos de cada entidad de transporte de trabajo ejercerán las funciones necesarias para supervisar el estado de la entidad de transporte de trabajo. La detección de un estado SF/SD activará el procedimiento de conmutación de protección. Al haberse preestablecido la entidad de transporte de protección, también es posible supervisar en los puntos extremos el estado de la entidad de transporte de protección.

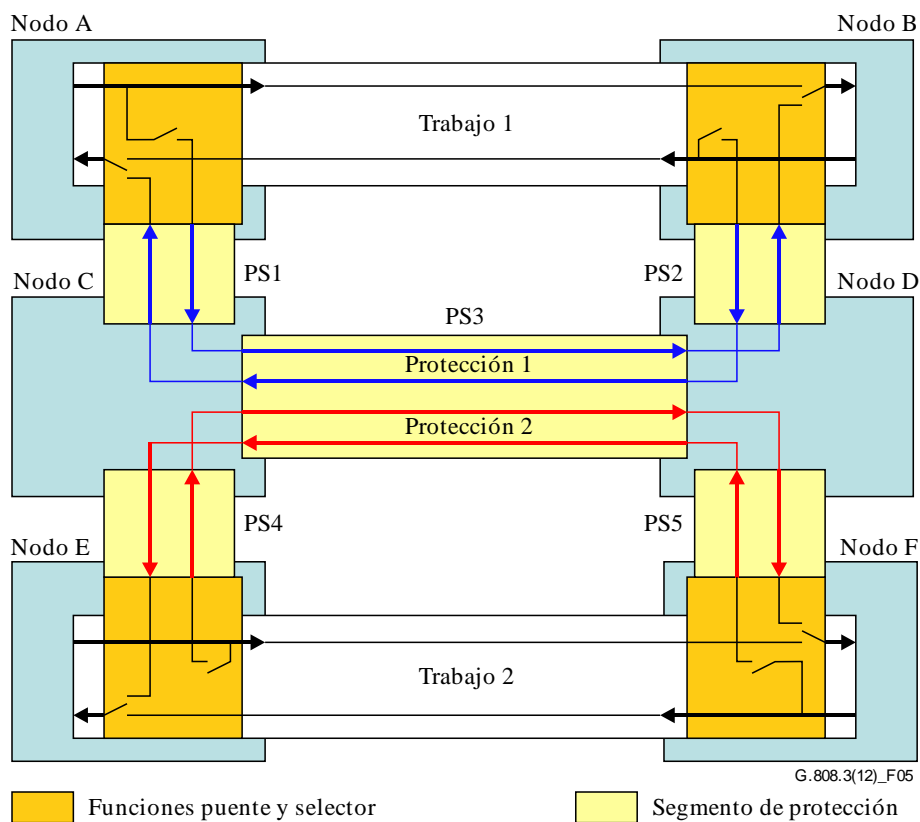


Figura 5 – Ejemplo de SMP para redes de paquetes

En la Figura 5 se muestra la arquitectura SMP 1:1 para redes de paquetes. PS3 está compartido entre las dos entidades de transporte de protección preestablecidas por A-C-D-B y E-C-D-F, respectivamente. Los dos pares de puntos extremos, el par de nodos A y B y el par de nodos E y F, supervisarán el estado de Trabajo 1 y Protección 1 y de Trabajo 1 y Protección 2, respectivamente. Cuando se detecta una degradación o fallo en una de las entidades de transporte de trabajo, y si se determina que la correspondiente entidad de transporte de protección está disponible, su señal de tráfico normal se conmutará de la entidad de transporte de trabajo a la de protección. En los nodos intermedios (C y D) no es necesario crear transconexiones, porque ya se han creado con antelación.

NOTA – Por mor de sencillez, en la Figura 5 se muestra una arquitectura SMP 1:1 para las redes de paquetes. Este ejemplo puede ampliarse a una arquitectura SMP m:1, donde hay múltiples entidades de transporte de protección por cada entidad de transporte de trabajo.

8 Tipos de conmutación

El mecanismo SMP soporta la conmutación bidireccional definida en [UIT-T G.808.1].

Para la SMP bidireccional, se utilizan los selectores y puentes a ambos extremos de la entidad de transporte de protección. Además, se activan las transconexiones bidireccionales en los nodos intermedios (si no están preestablecidos).

9 Tipos de funcionamiento

El mecanismo SMP soporta únicamente el funcionamiento reversible definido en [UIT-T G.808.1].

10 Tráfico no protegido y no prioritario (NUT) y tráfico extraordinario

La SMP soporta el tráfico no protegido y no prioritario (NUT).

Este NUT es genérico, lo que implica que es una clase de tráfico que no utiliza ningún recurso de protección y no se protege, ni siquiera en caso de fallo en su trayecto, pero que la red no puede abandonar para proteger otro tipo de tráfico.

Queda en estudio el tráfico extraordinario.

11 Conmutación automática

Queda en estudio.

12 Principio de prioridad

En la SMP se aplican los principios de prioridad cuando múltiples entidades de transporte de protección compiten por el mismo recurso compartido.

Para resolver esa competencia se han de tener en cuenta dos tipos de información:

- Prioridad de preferencia: se asigna a todas las entidades de transporte de protección una prioridad de preferencia configurada con antelación.
- Prioridad por solicitud: es la prioridad relativa de los eventos (condiciones de fallo e instrucciones externas) las que activan la protección. Queda en estudio la asignación de estas prioridades.

Todos los nodos de la entidad de transporte de protección han de tener en cuenta ambas prioridades.

- 1) En caso de competencia por un recurso entre múltiples entidades de transporte de protección con prioridades de preferencia distintas, ocupará el recurso la entidad de transporte de protección con la prioridad de preferencia más elevada.
- 2) En caso de competencia por un recurso entre múltiples entidades de transporte de protección con la misma prioridad de preferencia, ocupará el recurso la entidad de transporte de protección con la prioridad por solicitud más elevada.
- 3) En caso de competencia por un recurso entre múltiples entidades de transporte de protección con las mismas prioridades de preferencia y de solicitud, podrá utilizarse su ID de entidad de transporte para resolver la disputa.

13 Supervisión del estado del trayecto

El estado de la entidad de transporte de trabajo puede supervisarse utilizando métodos semejantes a los definidos para la protección lineal en [UIT-T G.808.1]. Los métodos de supervisión específicos dependerán de la tecnología utilizada.

En función de la tecnología de transporte de red subyacente, es posible que no se pueda establecer con antelación la entidad de transporte de protección. En tal caso, no habrá una supervisión directa del estado de extremo a extremo de la entidad de transporte de protección en los puntos extremos de protección, por lo que cada segmento de protección deberá notificar su estado a los puntos extremos de la entidad de transporte de protección.

Si es posible preestablecer la entidad de transporte de protección, podrá supervisarse su estado utilizando métodos semejantes a los definidos para la protección lineal en [UIT-T G.808.1]. Los métodos de supervisión específicos dependerán de la tecnología utilizada.

Cada segmento de protección tendrá que notificar la disponibilidad de sus recursos a los puntos extremos de la entidad de transporte de protección. Esta notificación tiene el objetivo de reducir la probabilidad de que se formulen solicitudes de conmutación de protección innecesarias, que resultarían en fallo al alcanzar un recurso de protección no disponible.

14 Protocolo de conmutación de protección automática (APS)

Queda en estudio.

Anexo A

Objetivos

(Este Anexo forma parte integrante de la presente Recomendación.)

- A.1 Se permitirá la compatibilidad con versiones anteriores de las estructuras/formatos núcleo de Recomendaciones sobre tecnologías específicas.
- A.2 No afectará a la utilización de los mecanismos de protección APS lineal y anular propios de cada tecnología existentes, ni de los canales de comunicación (es decir, la coexistencia con las especificaciones APS existentes).
- A.3 Se permitirá la implantación de aplicaciones internas de los operadores o entre ellos para la protección en cascada o anidada.
- A.4 Se permitirá la coexistencia de la protección/restablecimiento ASON y de la protección SMP en las fronteras entre dominios.
- A.5 Se podrá soportar la protección de una o más señales de tráfico normal bidireccional punto a punto desde el ingreso hasta el egreso del dominio SMP.
- A.6 No se exigirá que múltiples entidades de transporte de trabajo que compartan los mismos recursos de protección tengan los mismos puntos extremos.
- A.7 Se supervisará el estado de las entidades de transporte de trabajo para activar la conmutación de protección SMP (por ejemplo, SF, SD).
- A.8 Se supervisará la disponibilidad de los recursos de protección compartidos en las entidades de transporte de protección.
- A.9 Se incluirá el soporte de la comunicación de información sobre la disponibilidad de los recursos de protección compartidos en las entidades de transporte de protección a los puntos extremos de las entidades de transporte de trabajo que utilizan los recursos.
- A.10 Se incluirá el soporte de la comunicación de información entre nodos de red para efectuar la conmutación de protección. La codificación del mensaje y los canales de comunicación entre nodos dependerán de la tecnología utilizada.
- A.11 Se podrá recuperar la señal de tráfico normal tras uno o varios fallos de red de manera determinística. Por ejemplo, la conmutación de protección se completará dentro de un plazo finito (limitado), como se indica en las Recomendaciones sobre tecnologías específicas.
- A.12 Se soportará un mecanismo para detectar fallos de protocolo.
- A.13 Se soportará un mecanismo para detectar posibles incoherencias en la configuración entre los nodos de ingreso y egreso de un dominio SMP.
- A.14 Se podrá soportar el anidado de múltiples niveles de protección (sea SMP o protección de otro tipo, como SNC). Para ello, se incluirá el soporte de mecanismos que permitan la coordinación de la protección (por ejemplo, temporizador de espera).
- A.15 Se facilitará un mecanismo para evitar variación de la conmutación de protección (por ejemplo, temporizador de espera para restaurar).
- A.16 Se soportará la existencia de múltiples enlaces entre nodos, permitiendo así la diversidad de enlaces y nodos, y se preverá la adaptabilidad en cuanto al número de enlaces y nodos dentro del dominio de protección SMP.
- A.17 Se facilitará un mecanismo de solución de conflictos para que sólo una entidad de transporte de trabajo ocupe los recursos de protección en caso de que éstos estén compartidos entre más de una entidad de transporte de trabajo con la misma prioridad (debido a la topología de red y a la limitación de recursos).

- A.18 Se podrá soportar la capacidad de fijar un límite máximo de entidades de transporte de trabajo que pueden compartir recursos de protección (regido por cada tecnología específica).
- A.19 Se soportará la capacidad de fijar un límite máximo a la parte de recursos de enlace que puede atribuirse a la protección de entidades de transporte.
- A.20 Se permitirá la configuración (mediante el plano de gestión o el plano de control) de los identificadores de entidad de transporte de protección y el ancho de banda necesario, además de la SMP de circuitos y la asignación de TS para garantizar el adecuado funcionamiento del proceso de conmutación de protección.
- A.21 Se soportará la asignación de prioridades para soportar la solicitud de preferencia de una entidad de transporte con mayor prioridad sobre un recurso de protección compartido ocupado por una entidad de transporte con menor prioridad.
- A.22 Sólo se soportará el funcionamiento reversible.
- A.23 Sólo se soportará la conmutación bidireccional.
- A.24 Se podrán soportar las instrucciones externas de operadores de red.
- A.25 Se podrá soportar la protección para más de un fallo, incluidos los coincidentes y/o aquéllos que afecten a recursos compartidos.
- A.26 Se podrá activar la conmutación de protección desde uno o ambos extremos (incluso simultáneamente) del dominio SMP.

Apéndice I

Hipótesis de uso de la SMP

(Este apéndice no forma parte integrante de la presente Recomendación.)

En este apéndice se presentan algunos casos típicos de utilización de la SMP.

Téngase en cuenta que en este Apéndice no se muestran todas las hipótesis de uso.

I.1 SMP simple

En la Figura I.1 se muestra un caso simple. La conexión de trabajo W1 en el trayecto A-B está protegida por la conexión de protección P1 en el trayecto A-P-Q-B y la otra conexión de trabajo W2 en el trayecto C-D está protegida por la otra conexión de protección P2 en el trayecto C-P-Q-D. Las conexiones de protección P1 y P2 pueden compartir algunos recursos comunes (es decir, P1 y P2 pueden compartir el enlace de protección P-Q), porque W1 y W2 están separadas la una de la otra.

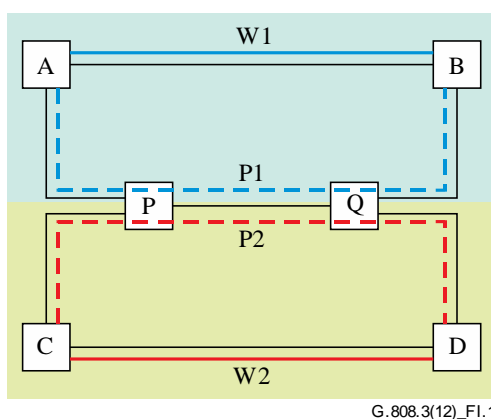


Figura I.1 – SMP simple

I.2 SMP en una red en malla

La red en malla general de la Figura I.2 se emplea para mostrar varias hipótesis de uso de la SMP.

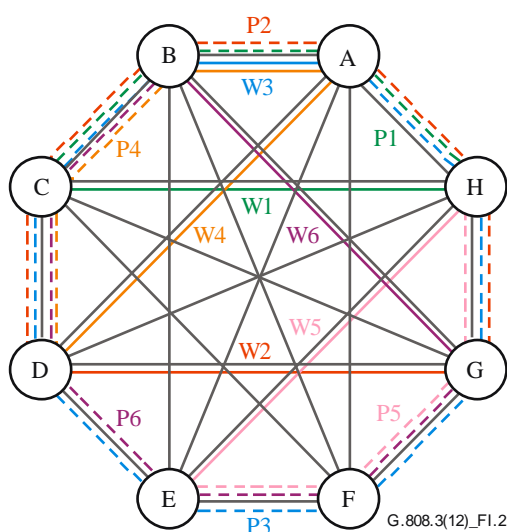


Figura I.2 – Ejemplo de SMP

En la red en malla de la Figura I.2 se muestran seis trayectos de trabajo (W1, W2, W3, W4, W5 y W6) y sus trayectos de protección (P1, P2, P3, P4, P5 y P6), como se resume en el Cuadro I.1.

Cuadro I.1 – Resumen

Color	Trayecto de trabajo	Trayecto de protección
Verde (W1, P1)	C-H	H-A-B-C
Rojo (W2, P2)	D-G	G-H-A- B-C-D
Azul (W3, P3)	A-B	B-C-D-E-F-G-H-A
Naranja (W4, P4)	B- A-D	B-C-D
Rosa (W5, P5)	H-E	H-G-F-E
Violeta (W6, P6)	B-G	B-C-D-E-F-G

W3, W4 y W6 tienen el mismo nodo extremo, B. W2 y W4 tienen el mismo nodo extremo, D. W2 y W6 tienen el mismo nodo extremo, G. W1 y W5 tienen el mismo nodo extremo, H. El nodo A es un nodo intermedio de W4, pero también el nodo extremo de W3.

NOTA – Cada hipótesis es independiente de las demás.

Hipótesis 1

Una hipótesis de SMP simple es que dos trayectos de protección comparten recursos comunes.

Color	Trayecto de trabajo	Trayecto de protección
Verde (W1, P1)	C-H	H-A-B-C
Rojo (W2, P2)	D-G	G-H-A- B-C-D

En la Figura I.2 el trayecto de trabajo W1 en el enlace C-H está protegido por el trayecto de protección P1 en el segmento H-A-B-C y el trayecto de trabajo W2 en el enlace D-G está protegido por el otro trayecto de protección, P2, en el segmento G-H-A- B-C-D. P1 y P2 pueden compartir algunos recursos comunes (es decir, el segmento de protección H-A-B-C).

Hipótesis 2

Un puerto o un enlace pueden tener algunos recursos utilizados para trayectos de trabajo y otros recursos utilizados para trayectos de protección.

Color	Trayecto de trabajo	Trayecto de protección
Verde (W1, P1)	C-H	H-A-B-C
Rojo (W2, P2)	D-G	G-H-A- B-C-D
Azul (W3, P3)	A-B	B-C-D-E-F-G-H-A
Naranja (W4, P4)	B- A-D	B-C-D

Como se ve en la Figura I.3, el enlace A-B contiene tanto el tráfico de trabajo de W3/W4 como un recurso de protección utilizado por P1/P2.

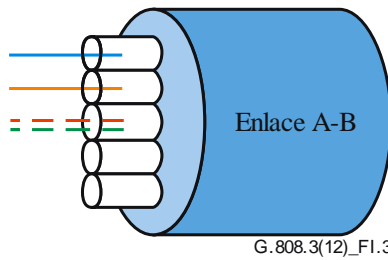


Figura I.3 – Detalle del enlace A-B

Hipótesis 3

Hay múltiples recursos de protección en un enlace. En este caso, los trayectos de trabajo que tienen enlaces en común aún pueden utilizar el mismo enlace de protección para ese fin, siempre y cuando se asigne un recurso diferente a sus trayectos de protección correspondientes.

Color	Trayecto de trabajo	Trayecto de protección
Azul (W3, P3)	A-B	B-C-D-E-F-G-H-A
Naranja (W4, P4)	B-A-D	B-C-D

Por ejemplo, como se ve en la Figura I.4, el segmento B-C-D soporta dos trayectos de protección en un único enlace, pero con distintos recursos. Por consiguiente, aunque W3 y W4 tienen el enlace A-B, aún pueden utilizar el segmento B-C-D como parte de sus trayectos de protección (P3 y P4).

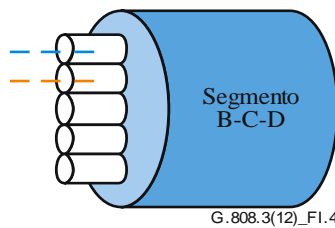


Figura I.4 – Detalle del segmento B-C-D

Hipótesis 4

Un recurso concreto utilizado para la protección puede ser un punto extremo para algunos trayectos de protección y un punto intermedio para otros trayectos de protección.

Color	Trayecto de trabajo	Trayecto de protección
Naranja (W4, P4)	B-A-D	B-C-D
Rosa (W5, P5)	H-E	H-G-F-E
Violeta (W6, P6)	B-G	B-C-D-E-F-G

Por ejemplo, en la Figura I.2, el nodo G, y más concretamente el puerto asociado al enlace G-F, muestra cómo el recurso de protección puede ser un punto intermedio para un trayecto (a saber, P5) y un punto extremo para otro trayecto (P6). Del mismo modo, el nodo D, y más concretamente el puerto asociado al enlace D-C, es un punto intermedio para P6 y un punto extremo para P4.

Hipótesis 5

Un trayecto de trabajo puede formar parte de múltiples grupos de riesgo compartido (SRG) distintos.

Color	Trayecto de trabajo	Trayecto de protección
Azul (W3, P3)	A-B	B-C-D-E-F-G-H-A
Naranja (W4, P4)	B-A-D	B-C-D
Rosa (W5, P5)	H-E	H-G-F-E
Violeta (W6, P6)	B-G	B-C-D-E-F-G

Como se ve en la Figura I.5, W6 (en violeta) forma parte de tres grupos de riesgo compartido: W6 y W4 forman un SRG a causa del segmento de protección B-C-D; W6 y W3 forman el segundo SRG a causa del segmento de protección D-E-F-G; y W6 y W5 forman el tercer SRG a causa del segmento de protección E-F-G.

En este caso, W3 y W5 también son un SRG a causa de los segmentos E-F-G, pero W4 y W5 no forman un SRG, pues no comparten ningún recurso de protección (es decir, que hay dos recursos de protección disponibles en el segmento B-C-D). Así, W4 puede compartir el riesgo con W3 y con W5.

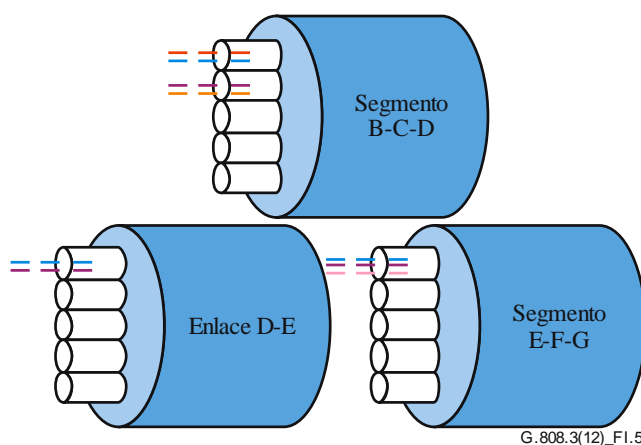


Figura I.5 – Detalle de los segmentos B-C-D y D-E-F-G

Hipótesis 6

Un recurso de protección asociado con un nodo puede soportar múltiples trayectos de protección. Sin bien cada uno de los trayectos de protección es una conexión punto a punto, si los trayectos comparten algunos recursos, hay algunos elementos de los circuitos punto a multipunto y multipunto a punto que se han de tener en cuenta al configurar la supervisión del trayecto de protección.

Color	Trayecto de trabajo	Trayecto de protección
Naranja (W4, P4)	B-A-D	B-C-D
Violeta (W6, P6)	B-G	B-C-D-E-F-G

Como se ve en la Figura I.6, el puerto asociado al nodo B que termina el segmento B-C-D ilustra el caso en que dos trayectos de protección (aquí, P4 y P6) comparten el segmento B-C-D, pero con distintos puntos extremos (es decir, que P4 termina en el nodo D y P6 termina en el nodo G). En un momento dado, en el puerto del nodo B habrá el trayecto P4, el trayecto P6 o no habrá trayecto alguno. Por este motivo, al configurar los valores del identificador de rastreo de camino (TTI) y los criterios de detección defecto de desadaptación del identificador de rastreo (dTIM), se habrá de tener cuidado de que, en caso de conexión en tándem, se supervise el trayecto de protección en su integridad.

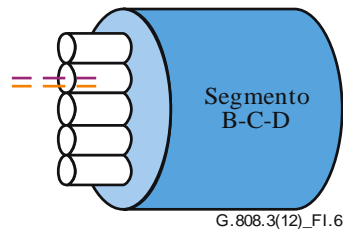


Figura I.6 – Detalle del segmento B-C-D

Estas hipótesis se deberán tener en cuenta al diseñar el protocolo APS y las arquitecturas de supervisión.

Apéndice II

Generalidades del funcionamiento del restablecimiento en malla compartida (SMR) y la protección en malla compartida (SMP)

(Este Apéndice no forma parte integrante de la presente Recomendación.)

En la Recomendación [UIT-T G.805] se describen las técnicas de mejora de disponibilidad de la red de transporte, donde "protección" significa la sustitución de un recurso en fallo por otro preasignado en espera y por "restablecimiento" se entiende la sustitución de un recurso en fallo mediante reencaminamiento utilizando la capacidad sobrante.

En [b-UIT-T G.8080] la protección es un mecanismo para mejorar la disponibilidad de una conexión a través del uso de capacidad asignada adicional. El restablecimiento de una llamada (servicio de conexión) en la red óptica con conmutación automática (ASON) es la sustitución de una conexión que ha fallado mediante el reencaminamiento de la llamada utilizando capacidad de reserva.

Se han definido distintos mecanismos para el restablecimiento en redes ASON. Se ha de tener en cuenta que el mecanismo de restablecimiento que más se parece a la SMP suele denominarse restablecimiento en malla compartida con trayectos de restablecimiento precalculados y preseñalizados. Esto implica que, cuando se crea satisfactoriamente una nueva conexión en el trayecto nominal/activo, se calcula un trayecto de seguridad (que debe estar completamente separado del trayecto nominal/activo). Posteriormente se establece una sesión de señalización en ese trayecto de seguridad y es durante el establecimiento de esa sesión de señalización que se verifica la disponibilidad de recursos libres. Una vez finalizado el proceso, el trayecto de seguridad se activa cuando el trayecto nominal/activo entra en fallo.

En la Figura II.1 se muestra la diferencia entre el restablecimiento en malla compartida ASON y la SMP.

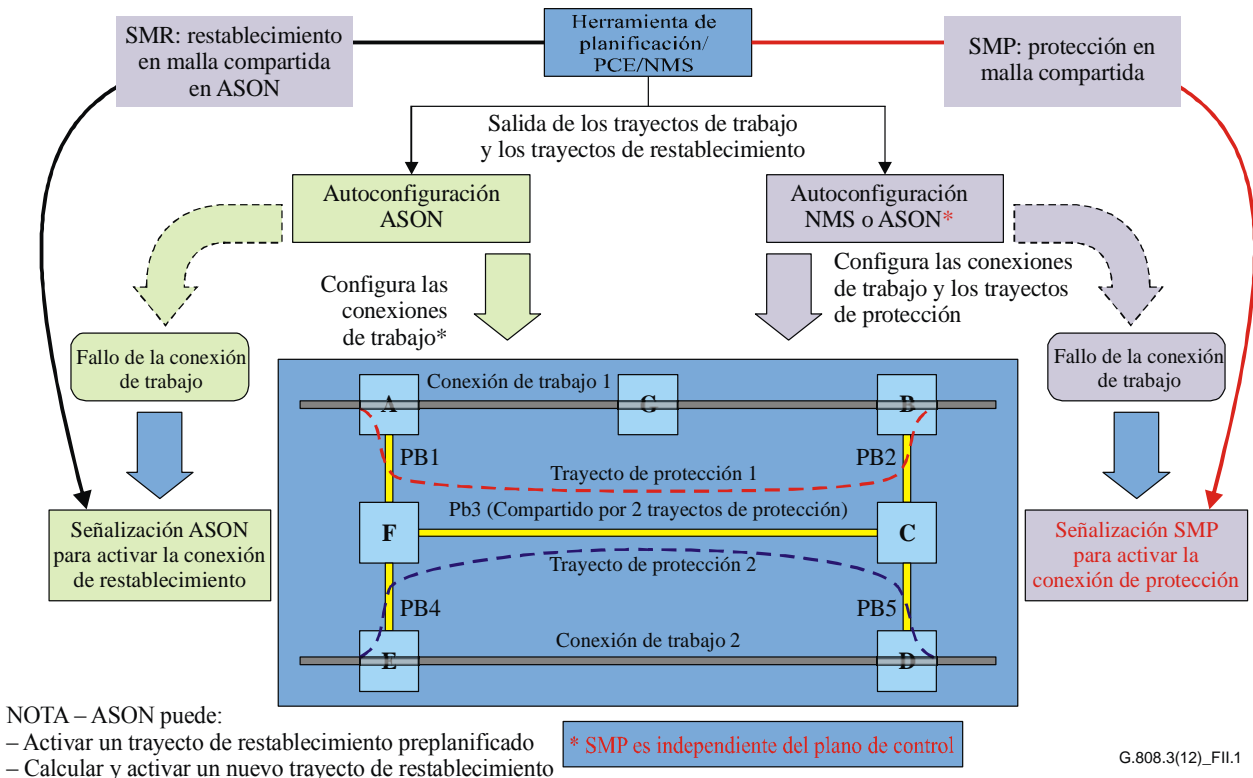


Figura II.1 – SMR y SMP

Bibliografía

- [b-UIT-T G.8080] Recomendación UIT-T G.8080/Y.1304 (2012), *Arquitectura de la red óptica con conmutación automática*.
- [b-BLTJ.1999] Doshi, B. T. et al. (1999), *Optical network design and restoration*, Bell Labs. Technical Journal, pp. 58-84, Jan.-Mar. 1999.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
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 multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos, comunicaciones de sistemas abiertos y seguridad
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación