UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T G.808.1

(12/2003)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

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

Redes digitales – Generalidades

Conmutación de protección genérica – Protección lineal de camino y de subred

Recomendación UIT-T G.808.1

RECOMENDACIONES UIT-T DE LA SERIE G

SISTEMAS Y MEDIOS DE TRANSMISIÓN, SISTEMAS Y REDES DIGITALES

CONEXIONES Y CIRCUITOS TELEFÓNICOS INTERNACIONALES	G.100–G.199
CARACTERÍSTICAS GENERALES COMUNES A TODOS LOS SISTEMAS ANALÓGICOS DE PORTADORAS	G.200–G.299
CARACTERÍSTICAS INDIVIDUALES DE LOS SISTEMAS TELEFÓNICOS INTERNACIONALES DE PORTADORAS EN LÍNEAS METÁLICAS	G.300–G.399
CARACTERÍSTICAS GENERALES DE LOS SISTEMAS TELEFÓNICOS INTERNACIONALES EN RADIOENLACES O POR SATÉLITE E INTERCONEXIÓN CON LOS SISTEMAS EN LÍNEAS METÁLICAS	G.400–G.449
COORDINACIÓN DE LA RADIOTELEFONÍA Y LA TELEFONÍA EN LÍNEA	G.450–G.499
EQUIPOS DE PRUEBAS	G.500–G.599
CARACTERÍSTICAS DE LOS MEDIOS DE TRANSMISIÓN	G.600–G.699
EQUIPOS TERMINALES DIGITALES	G.700–G.799
REDES DIGITALES	G.800–G.899
Generalidades	**G.800–G.809**
Objetivos de diseño para las redes digitales	G.810–G.819
Objetivos de calidad y disponibilidad	G.820–G.829
Funciones y capacidades de la red	G.830–G.839
Características de las redes con jerarquía digital síncrona	G.840–G.849
Gestión de red de transporte	G.850–G.859
Integración de los sistemas de satélite y radioeléctricos con jerarquía digital síncrona	G.860–G.869
Redes ópticas de transporte	G.870–G.879
SECCIONES DIGITALES Y SISTEMAS DIGITALES DE LÍNEA	G.900–G.999
CALIDAD DE SERVICIO Y DE TRANSMISIÓN - ASPECTOS GENÉRICOS Y ASPECTOS RELACIONADOS AL USUARIO	G.1000–G.1999
CARACTERÍSTICAS DE LOS MEDIOS DE TRANSMISIÓN	G.6000–G.6999
EQUIPOS TERMINALES DIGITALES	G.7000–G.7999
REDES DIGITALES	G.8000–G.8999

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

Recomendación UIT-T G.808.1

Conmutación de protección genérica – Protección lineal de camino y de subred

Resumen

En esta Recomendación se describen los modelos funcionales genéricos, las características y los procesos asociados con diversos métodos de protección lineal para redes de capa orientadas a conexión; por ejemplo, redes ópticas de transporte (OTN), redes de jerarquía digital síncrona (SDH) y redes de modo de transferencia asíncrono (ATM).

Además, se describen los objetivos y las aplicaciones relativos a esos métodos. Los métodos de protección descritos en esta Recomendación son la protección de camino y la protección de conexión de subred con distintas opciones de supervisión de señales individuales o de grupos de éstas. Se describe también la capacidad de supervivencia ofrecida por el método de ajuste de capacidad de enlace (LCAS).

Los modelos funcionales genéricos, las características y los procesos de los métodos de protección de anillo y de la subred interconectada (por ejemplo, anillo) se definen en otras Recomendaciones.

Orígenes

La Recomendación UIT-T G.808.1 fue aprobada el 14 de diciembre de 2003 por la Comisión de Estudio 15 (2001-2004) del UIT-T por el procedimiento de la Recomendación UIT-T A.8.

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

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

NOTA

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

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

PROPIEDAD INTELECTUAL

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

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

ÍNDICE

Página

Recomendación UIT-T G.808.1

Conmutación de protección genérica – Protección lineal de camino y de subred

1 Alcance

En esta Recomendación se presenta una síntesis de los aspectos genéricos de la conmutación de protección lineal. Trata los métodos de protección basados en OTN, SDH y ATM. La visión general de los métodos de protección de anillo y de interconexión de subredes de nodo dual (por ejemplo, anillo) será tratada en otras Recomendaciones.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

– Recomendación UIT-T G.783 (2004), *Características de los bloques funcionales del equipo de la jerarquía digital síncrona*.

– Recomendación UIT-T G.798 (2002), *Características de los bloques funcionales del equipo de la jerarquía de la red óptica de transporte*.

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

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

– Recomendación UIT-T G.842 (1997), *Interfuncionamiento de las arquitecturas de protección para redes de la jerarquía digital síncrona*.

– Recomendación UIT-T G.873.1 (2003), *Red óptica de transporte: Protección lineal*.

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

– Recomendación UIT-T I.732 (2000), *Características funcionales del equipo de modo de transferencia asíncrono*.

– Recomendación UIT-T M.495 (1988), *Restablecimiento de la transmisión y diversidad de rutas de transmisión: terminología y principios generales*.

3 Términos y definiciones

3.1 En esta Recomendación se utilizan los siguientes términos:

A Designación de punto extremo que se utiliza para describir un dominio protegido; el extremo distante, Z, inicia la señalización de petición de conmutación para el extremo A que es el origen de las señales protegidas.

Z Designación de punto extremo que se utiliza para describir un domino protegido; Z es el extremo en el que se inicia la señalización de petición de conmutación.

3.2 En esta Recomendación se utilizan los siguientes términos definidos en la Rec. UIT-T G.805:

a) Información adaptada (AI, *adapted information*)

b) Información característica (CI, *characteristic information*)

c) Conexión de enlace

d) Red

e) Conexión de enlace combinado en serie

f) Subred

g) Camino

3.3 En esta Recomendación se definen los términos siguientes.

3.3.1 Acción

3.3.1.1 conmutación: En el caso del selector, se trata de la acción relativa a la selección del tráfico normal de la entidad de transporte de reserva (actual) en lugar de la entidad de transporte activa (actual). En el caso del puente (caso de conexión permanente a servicio) se trata de la acción de conexión o desconexión del tráfico normal a la entidad de transporte de protección. En el caso de conexión no permanente a servicio, se trata de la acción de conexión de la señal de tráfico normal a la entidad de transporte de reserva (actual).

3.3.2 Protocolo de conmutador de protección automática (APS)

3.3.2.1 1-fase: Medio para alinear los dos extremos del dominio protegido con el intercambio de un solo mensaje (Z → A). En el caso de arquitecturas $(1:1)^n$, el puente y el selector de Z funcionan antes de que se confirme si la condición de Z tiene prioridad con relación a la condición de A. Cuando A confirma la prioridad de la condición de Z, hace funcionar el puente y el selector. Cuando se trata de conmutación unidireccional la prioridad se determina sólo mediante Z y se hace funcionar el selector de Z y el puente de A. En el caso de arquitecturas 1+1 los puentes son permanentes y únicamente funcionarán los selectores.

3.3.2.2 2-fases: Medio para alinear los dos extremos del dominio protegido con el intercambio de dos mensajes (Z → A, A → Z). En el caso de arquitecturas $(1:1)^n$, Z señaliza la condición de conmutación al extremo A y hace funcionar el puente. Cuando A confirma la prioridad de la condición de Z, hace funcionar el puente y el selector. Cuando se recibe la confirmación, Z hace funcionar su selector. Cuando se trata de conmutación unidireccional la prioridad la determina sólo Z y se hace funcionar el selector de Z y el puente de A. En el caso de arquitecturas 1+1 los puentes son permanentes y sólo funcionarán los selectores.

3.3.2.3 3-fases: Medio para alinear los dos extremos del dominio protegido con el intercambio de tres mensajes (Z → A, A → Z, Z → A). En el caso de arquitecturas 1:n, m:n, Z no realiza ninguna acción de conmutación hasta que el extremo A confirma la prioridad de la condición de Z. Cuando A la confirma, hace funcionar el puente. Cuando se recibe la confirmación, Z hace funcionar su selector y su puente y señala al extremo A el accionamiento del puente. Finalmente, A hace funcionar el selector. Si se trata de arquitecturas 1+1 los puentes son permanentes y sólo funcionarán los selectores.

3.3.3 Clase de protección

3.3.3.1 protección de camino: Protección de la entidad de transporte en el caso de que ésta sea un camino. El camino se protege añadiendo puentes y selectores en ambos extremos del mismo, y un camino adicional entre esos puentes y selectores.

Para determinar una condición de fallo en un camino dentro del dominio protegido se realiza una supervisión del camino.

3.3.3.2 protección de conexión de subred: Protección de la entidad de transporte en el caso de que ésta sea una conexión de subred. La conexión de enlace combinado en serie en la conexión de subred se protege añadiendo puentes y selectores a las funciones de conexión en los bordes del dominio protegido, y una conexión de enlace combinado en serie adicional entre esas funciones de conexión.

Para determinar una condición de fallo en una conexión de enlace combinado en serie dentro del dominio protegido se efectúa lo siguiente:

3.3.3.2.1 supervisión de subcapa (/S): Cada conexión de enlace combinado en serie se amplía con supervisión de conexión en cascada o con funciones de terminación/adaptación de segmento para deducir el estado de condición de fallo independientemente de la señal de tráfico presente.

3.3.3.2.2 supervisión no intrusiva (/N): Cada conexión de enlace combinado en serie se amplía con una función de destino de terminación de supervisión no intrusiva para deducir el estado de condición del fallo a partir de la señal de tráfico que esté presente.

3.3.3.2.3 supervisión inherente (/I): El estado de condición de fallo de cada conexión de enlace se deduce del estado del camino de capa de servidor subyacente.

NOTA – La supervisión inherente también puede aplicarse a la conexión de enlace combinado en serie VC-n SDH.

3.3.3.2.4 supervisión de prueba (/T): Cada estado de condición de fallo de la conexión de enlace combinado en serie se deduce de una conexión adicional supervisada de enlace combinado en serie que se transporta por el mismo enlace combinado en serie.

3.3.3.3 protección de conexión de red: Caso especial de la protección de conexión de subred.

3.3.3.4 individual: La protección se realiza para una sola entidad de transporte.

3.3.3.5 grupo: La protección se realiza para un conjunto de entidades de transporte.

3.3.4 Subclase de protección

3.3.4.1 tara/OAM extremo a extremo (e): Tara/operaciones, administración y mantenimiento (OAM) asociados con el camino de red de capa. Ejemplos: tara PM ODUk OTN, OAM e-t-e VPC TM.

3.3.4.2 tara/OAM de subcapa (s): Tara/OAM asociados con un camino de subcapa (conexión en cascada, segmento). Ejemplos: tara TC VC-n SDH, OAM de segmento VCC ATM.

3.3.5 Componente

3.3.5.1 dominio protegido: El dominio protegido define una o más entidades de transporte (caminos, conexiones de subred), para los cuales está disponible un mecanismo de supervivencia en caso de que las degradaciones afecten a esa o esas entidades de transporte. Va desde el selector/puente de un punto extremo al selector/puente del otro punto extremo.

3.3.5.2 puente: Función que conecta las señales de tráfico normales y adicionales a las entidades de transporte de servicio y de protección.

3.3.5.2.1 puente permanente: En el caso de la arquitectura 1+1, el puente conecta la señal de tráfico normal a ambas entidades, de servicio y de protección.

3.3.5.2.2 puente de difusión: En el caso de arquitecturas 1:n, m:n, $(1:1)^n$, el puente conecta permanentemente la señal de tráfico normal a la entidad de transporte de servicio. De haber conmutación de protección, la señal de tráfico normal se conecta adicionalmente a la entidad de transporte de protección. La señal de tráfico adicional puede estar conectada o no a la entidad de transporte de protección.

3.3.5.2.3 puente selector: En el caso de arquitecturas 1:n, m:n, $(1:1)^n$, el puente conecta la señal de tráfico normal a la entidad de transporte de servicio o bien a la de protección. La señal de tráfico adicional puede estar conectada o no a la entidad de transporte de protección.

NOTA 1 – En el caso de SDH, se prefiere el puente de difusión ya que los elementos de transconexión utilizan cuadros de conexión que se organizan normalmente por salida. En un puente en el que hay dos salidas y una entrada el cuadro contendría "OUTx1:INy", "OUTx2:INy". La utilización del puente de difusión no exige la modificación de la conexión de la matriz de servicio, requiere únicamente la adición de una conexión de matriz de protección.

NOTA 2 – En el caso de ATM, se prefiere el puente selector ya que los cuadros de conexión se organizan normalmente por entrada. Un puente de difusión necesitaría por ejemplo, "INx:OUTy1" "INx:OUTy2", que es más complicado que un puente selector, que sólo tiene "INx:OUTy1" que cambia a "INx:OUTy2". Esto se aplica también a otras tecnologías de conmutación de paquetes.

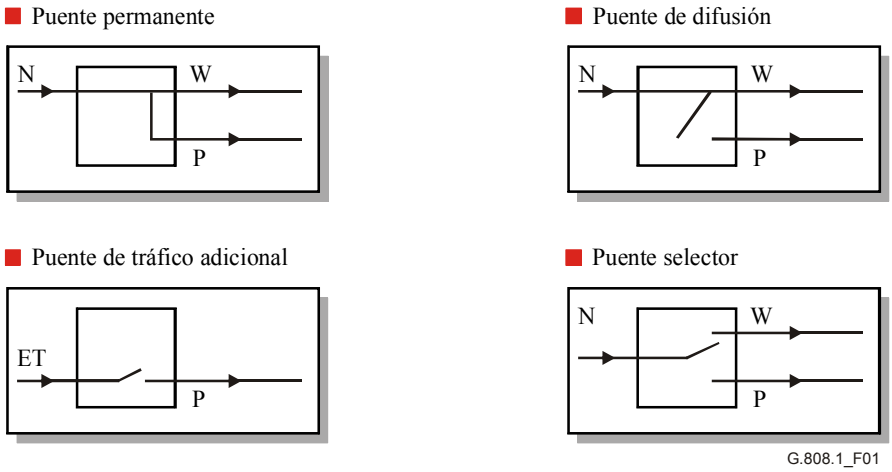


Figura 1/G.808.1 – Puentes de protección

3.3.5.3 selector: Función que extrae la señal de tráfico normal bien sea de la entidad de transporte de servicio o la de protección. La señal de tráfico adicional se extrae de la entidad de transporte de protección o no se extrae; en el último caso, se envía una señal de indicación de alarma (AIS).

3.3.5.3.1 selector selectivo: Selector que conecta la salida de señal de tráfico normal con las entradas de la entidad de transporte de servicio o la de protección.

3.3.5.3.2 selector de fusión: En el caso de las arquitecturas 1:1 y $(1:1)^n$, se trata de un selector que conecta permanentemente la salida de señal de tráfico normal con las entradas de ambas entidades de transporte, de servicio y de protección.

NOTA 1 – Esta opción funciona únicamente en combinación con un puente selector. Para evitar que la señal AIS/indicación de defecto hacia adelante (FDI) o el tráfico conectado/fusionado erróneamente en la entidad de transporte de reserva se fusione con la señal de tráfico normal seleccionada de la entidad de transporte activa, el selector de fusión incluye conmutadores en ambas entradas: de servicio y de protección. La entidad de transporte activa tendrá cerrado su conmutador, mientras que la entidad de transporte de reserva lo tendrá abierto. Por consiguiente, un selector de fusión es un tipo de selector selectivo distribuido.

NOTA 2 – En el caso de ATM, pueden asignarse conexiones pero las células no fluyen necesariamente por ellas. Un puente selector envía células únicamente por las conexiones de servicio o de protección y por consiguiente sólo llegará una copia al selector. Por lo tanto, el cuadro de conexiones puede tener dos conexiones de matriz permanentes "INx1:OUTy" e "INx2:OUTy". Esto se aplica también a otras tecnologías de conmutación de paquetes.

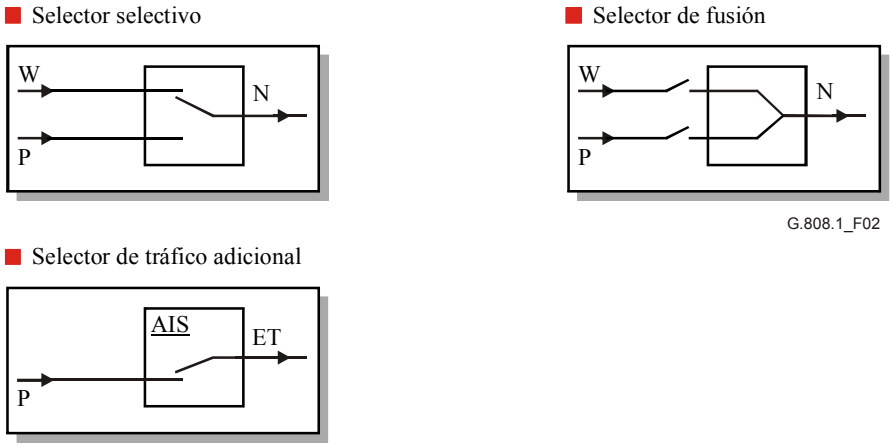


Figura 2/G.808.1 – Selectores de protección

3.3.5.4 extremo de cabecera: El extremo de cabecera del grupo de protección lineal es donde se localiza el proceso de puenteo. En el caso de que el tráfico esté protegido en ambos sentidos de transmisión, el proceso del extremo de cabecera estará presente en ambos extremos del grupo de protección.

3.3.5.5 extremo de cola: El extremo de cola del grupo de protección lineal es donde se localiza el proceso de selección. En el caso de que el tráfico esté protegido en ambos sentidos de transmisión, el proceso de extremo de cola estará presente en ambos extremos del grupo de protección.

3.3.5.6 nodo de destino: Nodo en la salida de un dominio protegido, donde es posible seleccionar la señal de tráfico normal bien sea de la entidad de transporte de servicio o de la entidad de transporte de protección.

3.3.5.7 nodo de origen: Nodo en la entrada de un dominio protegido, donde una señal de tráfico normal puede puentearse hacia la entidad de transporte de protección.

3.3.5.8 nodo intermedio: Nodo en la ruta física de la entidad de transporte de servicio o bien en la ruta física de la entidad de transporte de protección entre los nodos de origen y de destino del dominio protegido correspondiente.

3.3.6 Condición de fallo

3.3.6.1 degradación de señal (SD, *signal degrade*): Señal que indica que los datos asociados se han degradado, es decir que se ha activado una condición de defecto de degradación (por ejemplo, dDEG).

3.3.6.2 fallo de señal (SF, *signal fail*): Señal que indica un fallo de los datos asociados, es decir que se ha activado una condición de defecto de interrupción de señal de extremo cercano (no se trata del defecto de degradación).

3.3.6.3 grupo de señal degradada (SDG, *signal degrade group*): Señal que indica que los datos del grupo asociado se han degradado.

3.3.6.4 grupo de fallo de señal (SFG, *signal fail group*): Señal que indica que el grupo asociado ha fallado.

3.3.6.5 degradación de señal del servidor (SSD, *server signal degrade*): Salida de indicación de degradación de señal en el punto de conexión de una función de adaptación.

3.3.6.6 fallo de señal del servidor (SSF, *server signal fail*): Salida de indicación de fallo de señal en el punto de conexión de una función de adaptación.

3.3.6.7 degradación de señal de camino (TSD, *trail signal degrade*): Salida de indicación de degradación de señal en el punto de acceso de una función de terminación.

3.3.6.8 fallo de señal de camino (TSF, *trail signal fail*): Salida de indicación de fallo de señal en el punto de acceso de una función de terminación.

3.3.7 Arquitectura

3.3.7.1 arquitectura 1+1 (protección): La arquitectura de protección 1+1 tiene una señal de tráfico normal, una entidad de transporte de servicio, una entidad de transporte de protección y un puente permanente.

En el extremo de origen, la señal de tráfico normal se puentea permanentemente a ambas entidades de transporte, la de servicio y la de protección. En el extremo de destino, la señal de tráfico normal se selecciona de la mejor de las dos entidades de transporte.

Debido al puenteo permanente, la arquitectura 1+1 no permite que se proporcione una señal de tráfico adicional no protegido.

3.3.7.2 arquitectura 1:n (protección) (n ≥ 1): La arquitectura de protección 1:n tiene n señales de tráfico normal, n entidades de transporte de servicio y 1 entidad de transporte de protección. Puede tener 1 señal de tráfico adicional.

En el extremo de origen, una señal de tráfico normal está conectada permanentemente a su entidad de transporte de servicio y puede conectarse a la entidad de transporte de protección (caso de puente de difusión), o se conecta a la entidad de transporte de servicio o bien a la de protección (caso de puente selector). En el extremo de destino, la señal de tráfico normal se selecciona de su entidad de transporte de servicio o bien de la de protección.

Una señal de tráfico adicional no protegida puede transportarse por la entidad de transporte de protección siempre que esta última no esté siendo utilizada para transportar una señal de tráfico normal.

3.3.7.3 arquitectura m:n (protección): Una arquitectura de protección m:n tiene n señales de tráfico normal, n entidades de transporte de servicio y m entidades de transporte de protección. Puede tener hasta m señales de tráfico adicionales.

En el extremo de origen, una señal de tráfico normal se conecta permanentemente a su entidad de transporte de servicio y puede conectarse a una de las entidades de transporte de protección (caso de puente de difusión), o se conecta a su entidad de transporte de servicio o bien a una de las entidades de transporte de protección (caso de puente selector). En el extremo de destino, la señal de tráfico normal se selecciona de sus entidades de transporte de servicio o bien de una de las entidades de transporte de protección.

Hasta m señales de tráfico adicional no protegidas podrán transportarse por las m entidades de transporte de protección siempre que estas últimas no se estén utilizando para transportar una señal de tráfico normal.

3.3.7.4 arquitectura de protección $(1:1)^n$: Arquitecturas de n protecciones 1:1 paralelas, que tienen n entidades de transporte de protección y comparten (compiten por) la anchura de banda de protección. Tienen n señales de tráfico normal, n entidades de transporte de servicio y n entidades de transporte de protección. Pueden tener una señal de tráfico adicional en cuyo caso estará presente una entidad de transporte de protección adicional.

NOTA – Esta arquitectura puede aplicarse a redes de capa de células/paquetes (por ejemplo, ATM, MPLS).

3.3.8 Instrucciones externas

3.3.8.1 exclusión de la entidad de transporte de protección #i (LO #i, *lockout of protection transport entity* #i): Acción de configuración temporal iniciada por la instrucción de un operador. Provoca que la entidad de transporte de protección #i esté indisponible temporalmente para transportar una señal de tráfico (ya sea que se trate de tráfico normal o adicional).

3.3.8.2 exclusión de la señal de tráfico normal #i: Acción de configuración temporal iniciada por la instrucción de un operador. Provoca que la entidad de transporte de protección no pueda encaminar temporalmente la señal de tráfico normal #i. Las instrucciones de señal de tráfico normal #i serán rechazadas. Las señales de señal de fallo (SF) o de señal de degradación (SD) se ignorarán con relación a la señal de tráfico normal #i.

3.3.8.3 liberación de la exclusión de la señal de tráfico normal #i: Libera la instrucción de exlusión de la señal de tráfico normal #i.

NOTA – En el caso de la conmutación 1:n bidireccional, se seguirán aceptando las peticiones de puenteo distante para la señal de tráfico normal #i a fin de evitar fallos del protocolo APS. Como resultado, la señal de tráfico normal debe excluirse en ambos extremos para evitar que pueda ser seleccionada por la entidad de protección tras una instrucción o condición de fallo en cualquier extremo. Múltiples instrucciones de este tipo pueden coexistir para distintas señales de tráfico normal.

3.3.8.4 congelación: Acción de configuración temporal iniciada por la instrucción de un operador. Evita que se produzca cualquier acción de conmutación, y por consecuencia congela el estado actual. Hasta que se libera la congelación, se rechazan las instrucciones externas de extremo cercano adicionales. Se ignorarán los cambios de condición de fallo y la recepción de mensajes APS. Cuando se despeja la instrucción de congelación (**clear freeze**), se recalcula el estado del grupo de protección basándose en las condiciones de fallo y en los mensajes APS recibidos.

3.3.8.5 conmutación forzada de la señal de tráfico normal #i (FS #i, *forced switch for normal traffic signal* #i): Acción de conmutación iniciada por la instrucción de un operador. Conmuta la señal de tráfico normal #i a la entidad de transporte de protección, a menos que esté en curso una instrucción de conmutación con prioridad igual o superior.

En el caso de que se haya generado una señal APS, una señal SF en la entidad de transporte de protección (por la que se encaminó la señal APS) tendrá prioridad sobre la conmutación forzada.

3.3.8.6 conmutación forzada de la señal nula (FS #0, *forced switch for null signal*): Acción de conmutación iniciada mediante una instrucción de operador. En el caso de las arquitecturas 1:n, la acción conmuta la señal nula a la entidad de transporte de protección, a menos que esté en curso una instrucción de conmutación con prioridad igual o superior. Una señal de tráfico normal presente en la entidad de transporte de protección se transfiere a su entidad de transporte de servicio y se selecciona de la misma. En el caso de las arquitecturas 1+1, se selecciona la señal de tráfico normal de la entidad de transporte de servicio.

En el caso de que se haya generado una señal APS, una indicación SF en la entidad de transporte de protección (por la que se encaminó la señal APS) tendrá prioridad sobre la conmutación forzada.

3.3.8.7 conmutación forzada de la señal de tráfico adicional (FS #número de señal de tráfico adicional): Acción de conmutación iniciada mediante una instrucción de operador. Conmuta la señal de tráfico adicional a la entidad de transporte de protección, a menos que esté en curso una instrucción de conmutación con prioridad igual o superior. Una señal de tráfico normal presente en la entidad de transporte de protección se transfiere a la entidad de transporte de servicio y se selecciona de la misma.

En el caso de que se haya generado una señal APS, una indicación SF en la entidad de transporte de protección (por la que se encaminó la señal APS) tendrá prioridad sobre la conmutación forzada.

3.3.8.8 conmutación manual de la señal de tráfico normal #i (MS #i, *manual switch for normal traffic signal*): Acción de conmutación iniciada mediante una instrucción de operador. Conmuta la señal de tráfico normal #i a la entidad de transporte de protección, a menos que exista una condición de fallo en otras entidades de transporte (incluida la entidad de transporte de protección) o que esté en curso una instrucción de conmutación con prioridad igual o superior.

3.3.8.9 conmutación manual de la señal nula (MS #0, *manual switch for null signal*): Acción de conmutación iniciada mediante una instrucción de operador. En el caso de las arquitecturas 1:n, esta acción conmuta la señal nula a la entidad de transporte de protección, a menos que exista una condición de fallo en otras entidades de transporte o que esté en curso una instrucción de conmutación con prioridad igual o superior. Una señal de tráfico normal presente en la entidad de transporte de protección se transfiere a su entidad de transporte de servicio y se selecciona de la misma. Si se trata de las arquitecturas 1+1, se selecciona la señal de tráfico normal de la entidad de transporte de servicio.

3.3.8.10 conmutación manual de la señal de tráfico adicional (MS #número de señal de tráfico adicional): Acción de conmutación iniciada mediante la instrucción de un operador. Conmuta la señal de tráfico adicional a la entidad de transporte de protección, a menos que exista una condición de fallo en otras entidades de transporte o que esté en curso una instrucción de conmutación con prioridad igual o superior. Una señal de tráfico normal presente en la entidad de transporte de protección se transfiere a su entidad de transporte de servicio y se selecciona de la misma.

3.3.8.11 señal de ejercicio #i (EX, *exercise signal* #i): Emite una petición de ejercicio de esa señal (señal nula, señal de tráfico normal, señal de tráfico adicional) y verifica las respuestas en los mensajes APS, a menos que esté en uso la entidad de transporte de protección. En realidad no se completa la conmutación, es decir el selector se libera mediante una petición de ejercicio. La funcionalidad de ejercicio es facultativa.

3.3.8.12 despeje (CLR, *clear*): Despeja la exclusión de protección de extremo cercano activa, la conmutación forzada, la conmutación manual, el estado de espera de restablecimiento (WTR) o la instrucción de ejercicio.

3.3.9 Estados

3.3.9.1 sin reversión de la señal de tráfico normal #i (DNR #i, *do not revert normal traffic signal* #i): En el modo de funcionamiento no reversivo, se utiliza este estado para mantener la selección de una señal de tráfico normal desde la entidad de transporte de protección.

3.3.9.2 ninguna petición (NR, *no request*): Todas las señales de tráfico normal se seleccionan desde sus entidades de transporte de servicio correspondientes. La entidad de transporte de protección conduce la señal nula, el tráfico adicional o bien un puente de la señal de tráfico normal simple en un grupo de protección 1+1.

3.3.9.3 espera de restablecimiento de la señal de tráfico normal #i (WtR, *wait to restore normal traffic signal* #i): En el modo de funcionamiento reversivo, después del despeje de una indicación SF o SD en la entidad de transporte de servicio #i, este estado mantiene la señal de tráfico normal #i seleccionada de la entidad de transporte de protección hasta que expira el temporizador de retención de restablecimiento. Si el temporizador expira antes de cualquier otro evento o instrucción, el estado cambia a NR. Se utiliza para evitar el funcionamiento frecuente del selector en el caso de fallos intermitentes. El estado de espera de restablecimiento se activa únicamente si no hay una condición SF o SD para la entidad de transporte de protección.

3.3.10 Funcionamiento

3.3.10.1 funcionamiento reversivo (protección): Funcionamiento de conmutación de protección, en el que el transporte y la selección de la señal de tráfico normal (servicio) regresa siempre a (o permanece en) la entidad de transporte de servicio si terminan las peticiones de conmutación; es decir, cuando la entidad de transporte de servicio se ha recuperado del defecto o se despeja la petición externa.

3.3.10.2 funcionamiento no reversivo (protección): Funcionamiento de conmutación de protección, en el que el transporte y la selección de la señal de tráfico normal no regresan a la entidad de transporte de servicio cuando terminan las peticiones de conmutación.

3.3.11 Señal

3.3.11.1 señal de tráfico: Información característica o adaptada.

3.3.11.2 señal de tráfico normal: Señal de tráfico protegida por dos entidades de transporte opcionales, denominadas entidades de transporte de servicio y de protección.

3.3.11.3 señal de tráfico adicional: Señal de tráfico transportada por la entidad y/o ancho de banda de transporte de protección, cuando éstas no están siendo utilizadas para la protección de una señal de tráfico normal; es decir, cuando la entidad de transporte de protección se encuentra en reserva. Si se solicita la entidad/ancho de banda de transporte de protección para proteger o restablecer el tráfico normal de la entidad de transporte de servicio, se desplaza el tráfico adicional. El tráfico adicional no es tráfico protegido.

3.3.11.4 señal nula: Puede tratarse de cualquier clase de señal conforme a la estructura de señal (información característica o adaptada) del punto de referencia en la capa específica. Por defecto es la señal insertada por una función de conexión en una salida, que no esté conectada a una de sus entradas.

En el extremo de destino de la protección se ignora (no se selecciona) la señal nula.

En el protocolo APS se indica la señal nula si la entidad de transporte de protección no se utiliza para transportar la señal de tráfico normal o adicional.

Ejemplos de señales nulas: VC-n no equipado (SDH), ODUk-OCI (OTN), sin señal (ATM, MPLS), una señal de prueba, una de las señales de tráfico normal, una señal AIS/FDI.

3.3.12 Conmutación

3.3.12.1 conmutación bidireccional (protección): Modo de conmutación de protección en el cual, para el caso de un fallo unidireccional, se conmuta a la protección la señal de tráfico normal en ambos sentidos (del "camino", "conexión de subred", etc.), incluidos los sentidos afectado y no afectado.

3.3.12.2 conmutación unidireccional (protección): Modo de conmutación de protección en el cual, en caso de fallo unidireccional (es decir, un fallo que afecta únicamente un sentido de transmisión), sólo se conmuta a la protección la señal de tráfico normal transportada en el sentido afectado (del "camino", "conexión de subred", etc.).

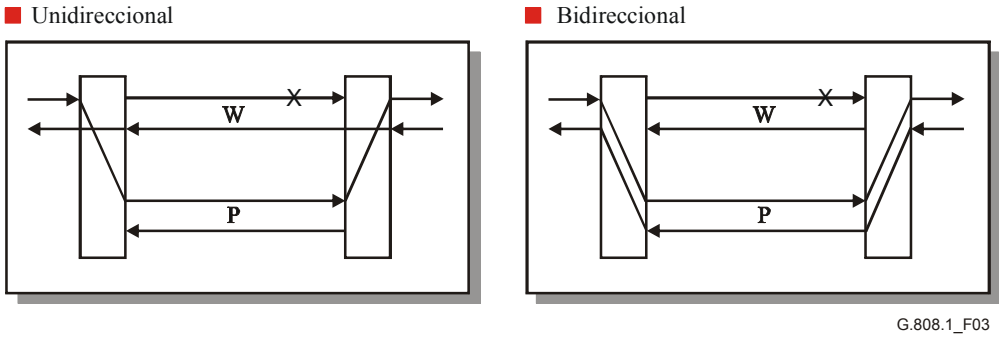


Figura 3/G.808.1 – Tipos de conmutación

3.3.13 Tiempo

3.3.13.1 periodo de tiempo de detección: El periodo de tiempo entre la aparición de la falla o degradación y su detección como una condición de defecto y la activación subsiguiente de la condición SF o SD.

3.3.13.2 periodo de tiempo de espera: El periodo de tiempo entre la declaración de una condición SF o SD y el inicio del algoritmo de conmutación de protección.

3.3.13.3 periodo de tiempo en espera de restablecimiento: Periodo de tiempo que debe transcurrir antes de que (a partir de la recuperación de una condición SF o SD) una entidad de transporte pueda reutilizarse para transportar la señal de tráfico normal y/o para seleccionarla de la misma.

3.3.13.4 periodo de tiempo de conmutación: Periodo de tiempo entre el inicio del algoritmo de conmutación de protección y el momento en que se selecciona el tráfico de la entidad de transporte en reserva.

3.3.14 Entidad de transporte

3.3.14.1 entidad de transporte: Componente de la arquitectura, que transfiere información entre sus entradas y salidas dentro de una red de capa. Ejemplos: camino, conexión de red, conexión de subred, conexión de enlace.

3.3.14.2 protección de entidad de transporte: Método que permite el transporte de una señal de tráfico por más de una entidad de transporte preasignada. El transporte de una señal de tráfico normal por una entidad de transporte de servicio se sustituye por el transporte de la misma señal a través de una entidad de transporte de protección si la primera sufre un fallo (condición SF), o si su calidad de funcionamiento cae por debajo de un nivel necesario (condición SD).

3.3.14.3 entidad de transporte de protección: Entidad de transporte asignada al transporte de la señal de tráfico normal durante un evento de conmutación. Puede utilizarse para conducir tráfico adicional en ausencia de un evento de conmutación. Cuando se presenta un evento de conmutación, el tráfico normal en la entidad de transporte de servicio afectada se puentea hacia la entidad de transporte de protección, desplazando el tráfico adicional (si existe).

3.3.14.4 entidad de transporte de servicio: Entidad de transporte por la que se conduce la señal de tráfico normal.

3.3.14.5 entidad de transporte activa: Entidad de transporte de la que el selector de protección elige la señal de tráfico normal.

3.3.14.6 entidad de transporte de reserva: Entidad de transporte no utilizada por el selector de protección para elegir la señal de tráfico normal.

3.3.14.7 grupo: Dos o más entidades de transporte, que se consideran como una sola entidad para la conmutación de protección. Por lo general, esas entidades de transporte se encaminan por los mismos enlaces dentro del dominio protegido.

3.3.15 protección: Utiliza capacidad preasignada entre nodos. La arquitectura más simple tiene una entidad de protección dedicada a cada entidad de servicio (1+1). La arquitectura más compleja tiene m entidades de protección que se comparten entre n entidades de servicio (m:n).

3.3.16 restablecimiento: Utiliza cualquier capacidad disponible entre nodos. En general, los algoritmos que se emplean para restablecimiento aplicarán reencaminamiento. Cuando se utiliza el restablecimiento se reserva un porcentaje de la capacidad de la red de transporte para el reencaminamiento del tráfico normal. En esta Recomendación no está prevista una descripción más detallada del restablecimiento.

3.3.17 acción de nivel superior: Acción de supervivencia de red provocada por la imposibilidad de la aplicación de la función de supervivencia en las capas inferiores.

3.3.18 conmutación de protección sin errores: Conmutación de protección, que no provoca pérdida de información característica o adaptada, duplicación, problemas o errores de bits durante la acción de conmutación de protección.

3.3.19 degradación: Fallo o degradación de la calidad de funcionamiento, que puede conducir a una condición de SF o SD.

3.3.20 supervivencia de red: Conjunto de capacidades que permiten que una red restablezca el tráfico afectado en el caso de una degradación. El grado de supervivencia lo determina la capacidad de la red para soportar degradaciones simples, degradaciones múltiples y degradaciones de equipo.

3.3.21 relación de protección: Cociente del ancho de banda realmente protegido dividido por el ancho de banda del tráfico, que se pretende proteger.

3.3.22 interfuncionamiento de subredes: Topología de red en la que se interconectan dos subredes (por ejemplo, anillo) en dos puntos y funcionan de tal manera que un fallo en cualquiera de estos dos puntos no provocará la pérdida de ningún tráfico, exceptuando la posibilidad de pérdida de tráfico derivada o insertada en el punto de fallo.

3.3.23 red con capacidad de supervivencia: Red capaz de restablecer el tráfico en el caso de una degradación. El grado de supervivencia lo determina la capacidad de la red para soportar degradaciones de enlaces simples, múltiples degradaciones de enlace y degradaciones de equipo.

3.3.24 evento de conmutación: Se produce un evento de conmutación si se presenta una condición de fallo en una entidad de transporte de servicio o mediante una instrucción externa, y el algoritmo de protección concluye que esta condición de fallo o instrucción externa es el evento de mayor prioridad.

4 Abreviaturas

En esta Recomendación se utilizan las siguientes siglas.

ABR Velocidad binaria disponible (*available bit rate*)

AI Información adaptada (*adapted information*)

AIS Señal de indicación de alarma (*alarm indication signal*)

AP Punto de acceso (*access point*)

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

ATM Modo de transferencia asíncrono (*asynchronous transfer mode*)

AU Unidad administrativa (*administrative unit*)

B Ancho de banda (*bandwidth*)

BER Tasa de errores en los bits (*bit error rate*)

BR Puente (*bridge*)

CC Comprobación de continuidad (*continuity check*)

CI Información característica (*characteristic information*)

CP Punto de conexión (*connection point*)

DEG Degradación (*degraded*)

ET Tráfico adicional (señal) [*extra traffic (signal)*]

F4 Flujo N.º 4 (ATM) [*flow #4* (ATM)]

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

HO Espera (*hold off*)

LCAS Esquema de ajuste de la capacidad del enlace (*link capacity adjustment scheme*)

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

MS Sección múltiplex (*multiplex section*)

N	Normal (señal) [*normal (signal)*]
NE	Elemento de red (*network element*)
NIM	Supervisión no intrusiva (*non-intrusive monitoring*)
NR	Ninguna petición (*no request*)
NUT	Tráfico no protegido ininterrumpible (*non-preemptible unprotected traffic*)
OAM	Operaciones, administración y mantenimiento (*operations, administration and maintenance*)
OCh	Canal óptico (*optical channel*)
OH	Tara (*overhead*)
OTN	Red óptica de transporte (*optical transport network*)
P	Protección (*protection*)
PDH	Jerarquía digital plesiócrona (*plesiochronous digital hierarchy*)
POH	Tara de trayecto (*path overhead*)
PP	Procesamiento de puntero (*pointer processing*)
PU	Unidad de puerto (*port unit*)
REI	Indicación de error distante (*remote error indication*)
RDI	Indicación de defecto distante (*remote defect indication*)
RI	Información distante (*remote information*)
RS	Sección regeneradora (*regenerator section*)
SD	Degradación de señal (*signal degrade*)
SDG	Grupo de degradación de señal (*signal degrade group*)
SDH	Jerarquía digital síncrona (*synchronous digital hierarchy*)
SEL	Selector (*selector*)
SES	Segundo con muchos errores (*severely errored second*)
SF	Fallo de señal (*signal fail*)
SFG	Grupo de fallos de señal (*signal fail group*)
Sm	Capa VC-m de orden inferior (m = 11, 12, 2) [*lower order VC-m layer (m = 11, 12, 2)*]
Sn	Capa VC-n de orden superior (n = 3, 4, 4-Xc) o capa VC-3 de orden inferior [*higher order VC-n layer (n = 3, 4, 4-Xc) or lower order VC-3 layer*]
SNC	Conexión de subred (*subnetwork connection*)
SNC/I	Protección de conexión de subred con supervisión inherente (*inherently monitored subnetwork connection protection*)
SNC/N	Protección de conexión de subred con supervisión no intrusiva (*non-intrusively monitored subnetwork connection protection*)
SNC/Ne	SNC/N, supervisión de OH extremo a extremo (*SNC/N, monitoring of end-to-end OH*)
SNC/Ns	SNC/N, supervisión de subcapa OH (*SNC/N, monitoring of sublayer OH*)
SNC/S	SNCP con supervisión de subcapa (*SNCP with sublayer monitoring*)
SNC/Ss	SNC/S, supervisión de subcapa OH (*SNC/S, monitoring of sublayer OH*)

SNC/T SNCP con supervisión de camino de prueba (*SNCP with test trail monitoring*)

SNC/Te SNC/T, supervisión de OH extremo a extremo (*SNC/T, monitoring of end-to-end OH*)

SNC/Ts SNC/T, supervisión de subcapa OH (*SNC/T, monitoring of sublayer OH*)

SNC/N Protección de conexión de subred con supervisión no intrusiva (*non-intrusively monitored subnetwork connection protection*)

SNCP Protección de conexión de subred (*subnetwork connection protection*)

Sn-Xv Capa VC-n-Xv (*layer VC-n-Xv*)

SOH Tara de sección (*section overhead*)

SSD Degradación de señal de servidor (*server signal degrade*)

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

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

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

TSD Degradación de señal de camino (*trail signal degrade*)

TSI Intercambio de intervalos de tiempo (*timeslot interchange*)

TT Terminación de camino (*trail termination*)

TSF Fallo de señal de camino (*trail signal fail*)

TU Unidad tributaria (*tributary unit*)

UBR Velocidad binaria no especificada (*unspecified bit rate*)

UPSR Anillo conmutado de trayecto unidireccional (*unidirectional path switch ring*)

VC Canal virtual (ATM) [*virtual channel (ATM)*]

VCG Grupo de concatenación virtual (*virtual concatenation group*)

VC-n Contenedor virtual n (*virtual container-n*)

VC-n-Xv Concatenación virtual de X contenedores virtuales (de nivel n) [*(virtual concatenation of X virtual containers (of level n))*]

VP Trayecto virtual (ATM) [*virtual path (ATM)*]

VPI Identificador de trayecto virtual (*virtual path identifier*)

W Servicio (*working*)

WTR En espera de restablecimiento (*wait-to-restore*)

X,Y,Z Capa (capas no especificadas) o designaciones de tamaño de grupo [*layer (for non-specified layers) or group size designations*)]

5 Convenios

Ninguno.

6 Concepto de protección individual y de grupo

El concepto de protección individual se aplica a situaciones en las que es necesario proteger sólo una parte de las señales de tráfico, que deben tener una fiabilidad elevada. El resto de las señales de tráfico en la capa de red quedan desprotegidas, permitiendo que se reduzca el ancho de banda necesario para la protección.

El concepto de protección de grupo se aplica a situaciones en las que:

i) resulta útil proteger un gran número de las señales de tráfico (pero no todas) que se transportan por los mismos caminos de capa servidora, con tiempos de protección del mismo orden de la protección individual (de un pequeño conjunto de señales de tráfico). Puede lograrse conmutación de protección rápida mediante el tratamiento de un agrupamiento lógico de entidades de transporte como una sola entidad después del comienzo de las acciones de protección;

ii) la protección de un grupo de señales de tráfico que se comportan como una sola señal de tráfico mediante por ejemplo, concatenación virtual, multiplexación inversa.

La complejidad del proceso de protección se reduce tratando el grupo de señales como una sola entidad, dentro de un solo proceso de protección. El estado de los grupos de servicio y protección se representa mediante indicaciones de grupo SF y de grupo SD.

La complejidad puede reducirse aún más introduciendo una señal de prueba adicional (que se transporta por los mismos caminos de capa servidora), de la cual se utilizan las indicaciones SF y SD para representar el estado del grupo. La *desventaja* de esta última técnica de reducción de complejidad es la imposibilidad de supervisar las señales individuales de cada grupo con relación a su conectividad, continuidad y calidad de funcionamiento. No podrá detectarse uno de esos fallos dentro de una de las señales en el grupo y por consiguiente no están protegidas.

7 Tipos de arquitectura

La arquitectura de protección puede ser del tipo 1+1, 1:n, m:n, o $(1:1)^n$.

Las posibles ventajas de la arquitectura 1+1 incluyen:

1) baja complejidad;

2) en el caso de la conmutación unidireccional, la posibilidad de soportar la interconexión de nodos duales de las subredes protegidas.

Las posibles desventajas de la arquitecturas 1+1 incluyen:

3) 100% de capacidad adicional.

Las posibles ventajas de la arquitectura 1:n, m:n, $(1:1)^n$ incluyen:

1) posibilidad de proporcionar acceso a la protección; la entidad/ancho de banda de transporte de protección puede transportar una señal de tráfico adicional durante periodos en los que no se requiere la entidad/ancho de banda de transporte de protección para transportar una señal de tráfico normal;

2) restricción de capacidad adicional a 100/n % o m × 100/n %;

3) en el caso de la protección m:n, es posible lograr la protección hasta de m fallos.

Las posibles desventajas de la arquitectura 1:n, m:n, $(1:1)^n$ incluyen:

4) complejidad;

5) en el caso de la clase de protección SNC, la necesidad de funciones de terminación de subcapa adicionales en los puntos de entrada y de salida del dominio protegido de cada entidad de transporte de servicio y de protección;

6) no soporta la interconexión de nodos duales de las subredes protegidas;

7) $n \geq 2$: cada una de las n entidades de transporte de servicio debe encaminarse por distintas facilidades y equipo para evitar la existencia de puntos comunes de fallo que no puedan protegerse mediante una sola entidad de transporte de protección en una arquitectura 1:n y $(1:1)^n$.

NOTA 1 – Por lo general, no se dispondrá de n+1 trayectos optativos entre dos nodos en la red. Por consiguiente, las arquitecturas 1:n y $(1:1)^n$, con n ≥ 2, *no proporcionarán una protección apropiada* para las n señales de tráfico normal que se transportan normalmente por las n entidades de transporte de servicio. n = 1 parece ser la única elección razonable.

NOTA 2 – En el caso de ATM, no se necesita explícitamente el acceso a la protección para poder emplear el ancho de banda de protección que no se utiliza normalmente; los tipos de tráfico ABR y UBR podrían utilizar este ancho de banda de protección mediante una gran demanda del ancho de banda de la señal del servidor que contiene la entidad de transporte de protección. Se supone que el mecanismo de control de la capa superior de ABR/UBR puede reducir el tráfico cuando se utiliza realmente la protección. Los nodos de entrada/salida del dominio de protección no tienen que alinearse con los nodos de entrada/salida del tráfico ABR/UBR. Esto añade flexibilidad a la red y reduce la complejidad.

7.1 Arquitectura de protección tipo 1+1

Cuando se trata del tipo de arquitectura 1+1, se designa una entidad de transporte de protección que actúe como facilidad de respaldo para la entidad de transporte de servicio y para la que la señal de tráfico normal se puentea hacia la entidad de transporte de protección en el punto extremo de origen del dominio protegido. El tráfico normal de las entidades de transporte de servicio y de protección se transmite simultáneamente al punto extremo de destino del dominio protegido, donde se efectúa una selección entre la entidad de transporte de servicio y la de protección basándose en algunos criterios predeterminados, como las indicaciones de fallo de señal y de degradación de señal.

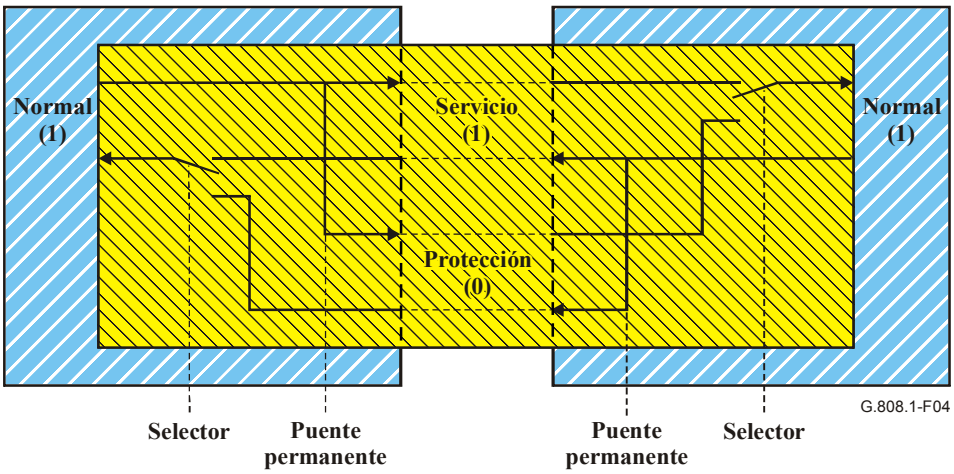


Figura 4/G.808.1 – Arquitectura de protección tipo 1+1

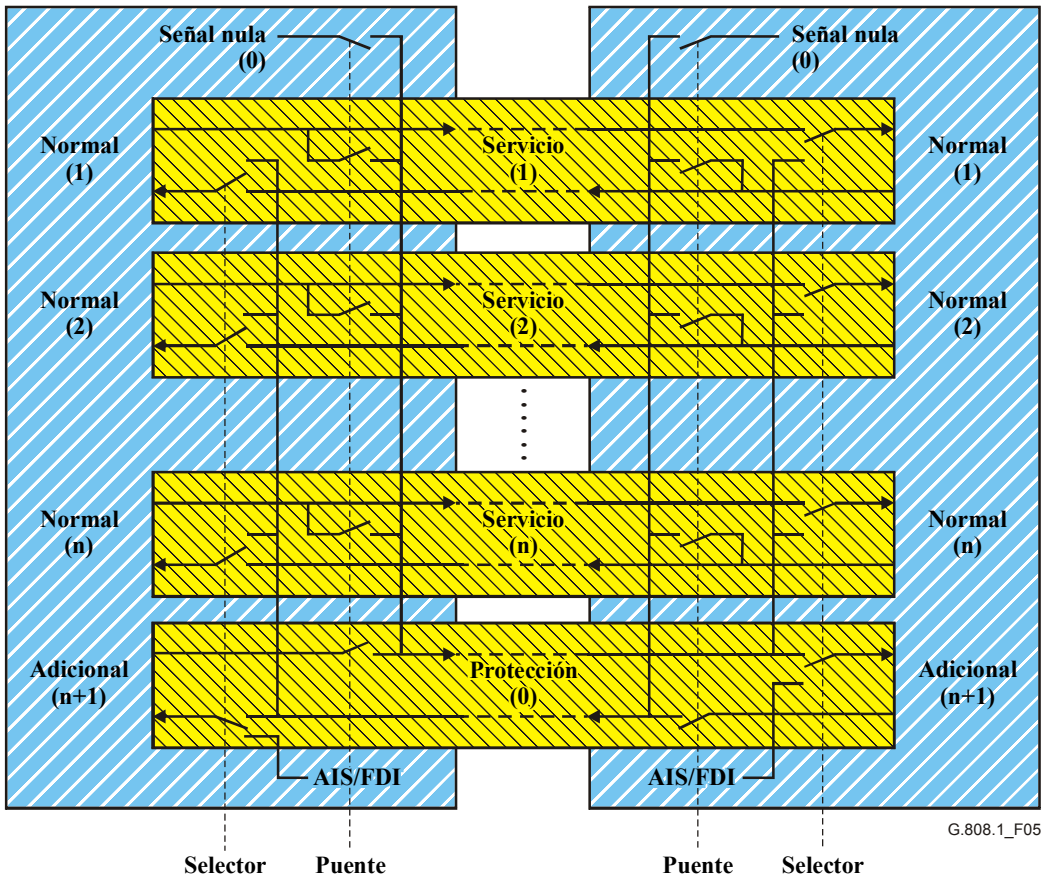
7.2 Arquitectura de protección tipo 1:n

Con el tipo de arquitectura 1:n, una entidad de transporte de protección dedicada se comporta como una facilidad de respaldo compartida entre n entidades de transporte de servicio. El ancho de banda de la entidad de transporte de protección debe asignarse de tal modo que pueda ser posible proteger cualquiera de las n entidades de transporte de servicio siempre que esté disponible la entidad de transporte de protección.

Cuando se determina que una entidad de transporte de servicio tiene degradaciones, su señal de tráfico normal debe transferirse de la entidad de transporte de servicio a la de protección, tanto en el punto extremo de origen como en el de destino del dominio protegido. Se observará que cuando más de una entidad de transporte de servicio tienen degradaciones, sólo puede protegerse una señal de tráfico normal.

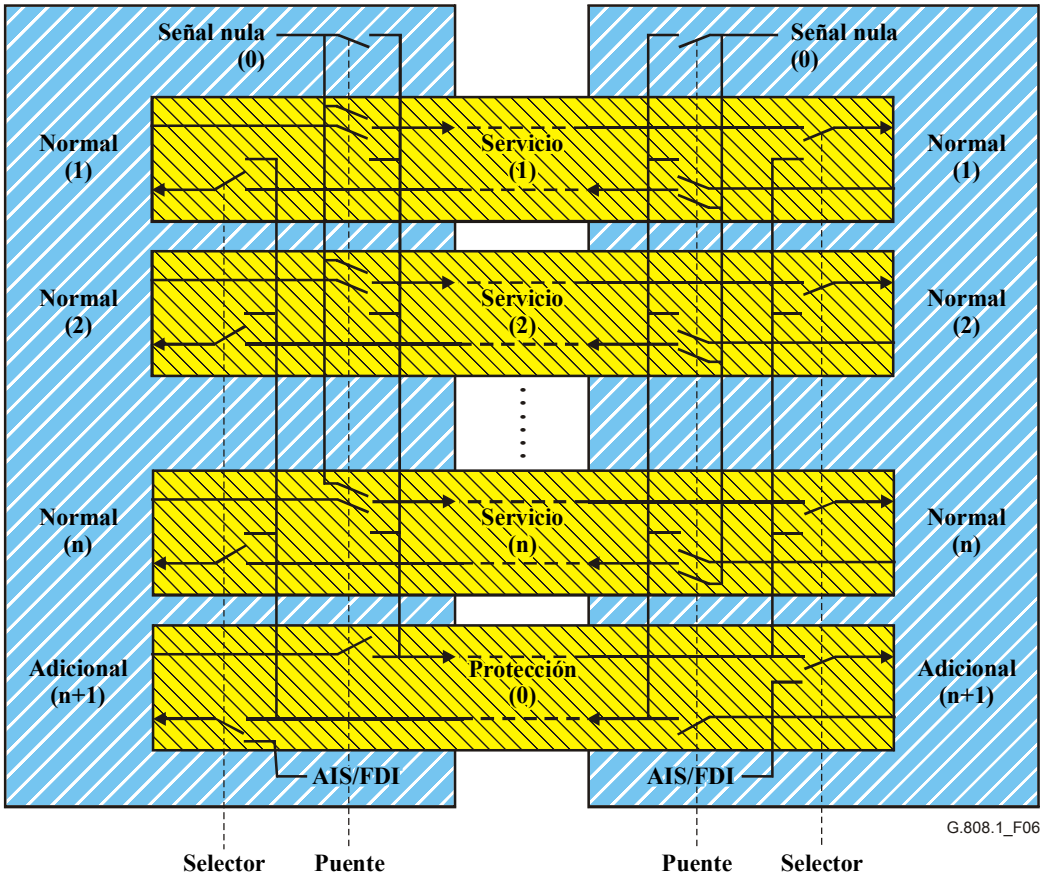
El puente puede realizarse de dos modos: puente selector o puente de difusión. Con la conectividad de puente selector (figura 6) la señal de tráfico normal se conecta a la entidad de transporte de servicio o bien a la entidad de transporte de protección. Con la conectividad de puente de difusión

(figura 5) la señal de tráfico normal se conecta permanentemente a la entidad de transporte de servicio y ocasionalmente también a la de protección. El interfuncionamiento entre las dos opciones está garantizado.



Opción de puente de difusión: conexión normal permanente a la entidad de servicio y ocasional a la de protección

Figura 5/G.808.1 – Arquitectura de protección tipo 1:n

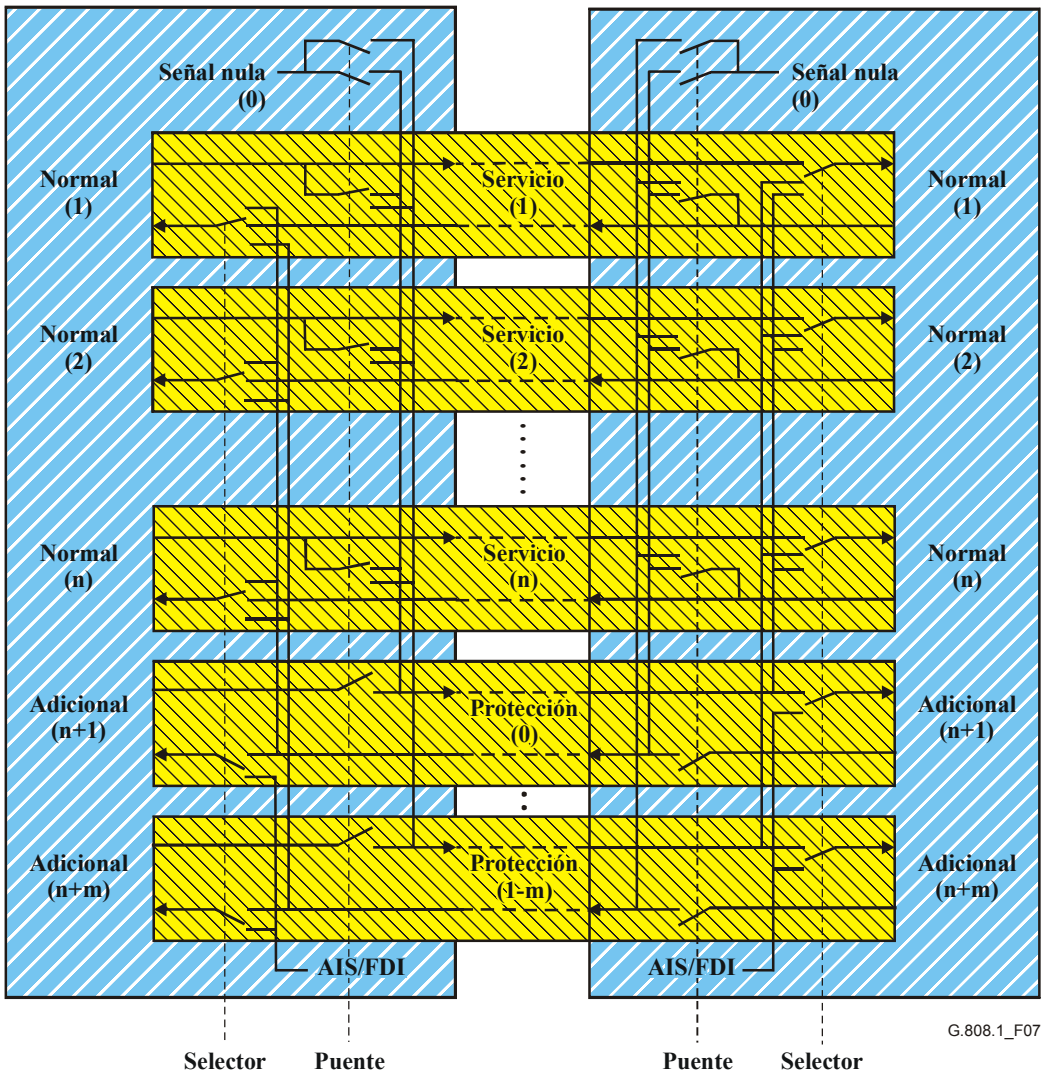


Opción de puente selector: conexión normal a la entidad de servicio o bien a la de protección

Figura 6/G.808.1 – Arquitectura de protección tipo 1:n

7.3 Arquitectura de protección tipo m:n

Con el tipo de arquitectura m:n, m entidades de transporte de protección dedicadas se asignan como facilidades de respaldo compartidas para n entidades de transporte de servicio, y en general se cumple que $m \leq n$. El ancho de banda de cada entidad de transporte de protección deberá asignarse de tal manera que pueda ser posible proteger cualquiera de las n entidades de transporte de servicio siempre que esté disponible al menos una de las m entidades de transporte de protección. Cuando se determina que una entidad de transporte de servicio tiene degradaciones, en primer lugar su señal de tráfico normal debe asignarse a una entidad de transporte de protección disponible y a continuación debe efectuarse la transición de la entidad de transporte de servicio a la de protección asignada en ambos puntos extremo de origen y de destino del dominio protegido. Debe observarse que cuando más de m entidades de transporte de servicio tienen degradaciones, sólo podrán protegerse m entidades de transporte de servicio.

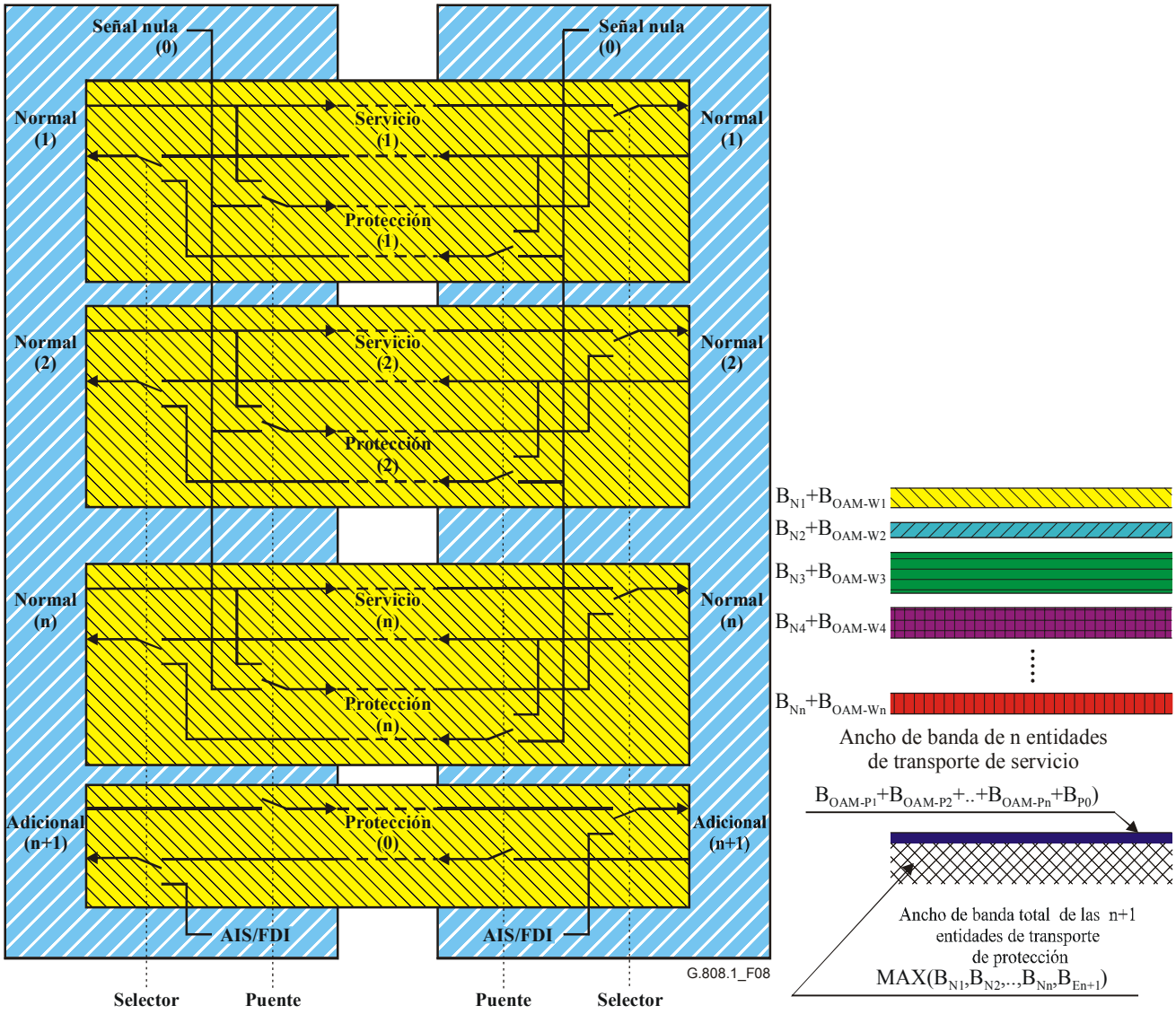


Opción de puente de difusión: conexión normal permanente a la entidad de servicio y ocasional a la de protección

Figura 7/G.808.1 – Arquitectura de protección tipo m:n

7.4 Arquitectura de protección tipo $(1:1)^n$

Con la arquitectura de protección tipo $(1:1)^n$, se asignan n entidades de transporte de protección dedicadas que comparten el mismo ancho de banda como facilidades de respaldo para n entidades de transporte de servicio. El ancho de banda de protección deberá asignarse de tal manera que sea posible proteger cualquiera de las n entidades de transporte de servicio siempre que estén disponibles el ancho de banda de transporte de protección y la entidad de transporte de protección específica asociada con la entidad de transporte de servicio que ha de conmutarse. Cuando se determina que una entidad de transporte de servicio tiene degradaciones, en primer lugar su señal de tráfico normal debe asignarse a la entidad de transporte de protección disponible asociada y a continuación se efectuará la transición de la entidad de transporte de servicio a la de protección asignada en ambos puntos extremo de origen y de destino del dominio protegido. Debe observarse que cuando más de una entidad de transporte de servicio tiene degradaciones, sólo podrá protegerse una de ellas.



Opción de puente de difusión: conexión normal permanente a la entidad de servicio y ocasional a la de protección

Figura 8/G.808.1 – Arquitectura de protección tipo $(1:1)^n$ con ancho de banda compartido

Todas la "n" entidades de transporte de servicio se encaminan por distintas facilidades y equipos (para evitar un punto común de fallo que no pueda protegerse). Todas las "n+1" entidades de transporte de protección se encaminan por las mismas facilidades y equipos, distintos de las facilidades y equipos de servicio. En el apéndice IV hay un ejemplo.

El ancho de banda ocupado por cada entidad de transporte de servicio es $B_{Wi} = B_{Ni}+B_{OAM-Wi}$; es decir, el ancho de banda de la señal de tráfico normal #i más el de las OAM de conexión/segmento en cascada que se utilizan para supervisar la entidad de transporte de servicio #i. El ancho de banda que ocupan las entidades de transporte de protección es $Bp = MAX(B_{N1},B_{N2},..,B_{Nn},B_{En+1}) + (B_{OAM-P1}+B_{OAM-P2}+..+B_{OAM-Pn}+B_{OAM-P0})$. Desde la perspectiva del ancho de banda esta arquitectura de protección $(1:1)^n$ se comporta como una arquitectura tipo 1:n.

No es posible que haya una conexión errónea entre una señal de tráfico normal #i en el ingreso al dominio protegido y la salida de una señal de tráfico normal #j ($j \neq i$) al egreso del dominio protegido. Por consiguiente no es necesario un protocolo APS de tres fases.

Obsérvese que esta arquitectura es útil para tráfico basado en paquetes/células, y no para tráfico de tipo de velocidad binaria constante.

8 Tipos de conmutación

Los tipos de conmutación de protección pueden ser: conmutación unidireccional o conmutación bidireccional.

En el caso de la conmutación **unidireccional**, se completa la conmutación cuando la señal de tráfico (servicio) se selecciona de la reserva en el extremo que detecta el fallo. Cuando se trata de la arquitectura 1+1, sólo se hace funcionar el selector en el extremo de destino (sin comunicación con el extremo de origen). En el caso de las arquitecturas 1:n, m:n, $(1:1)^n$, se hace funcionar el selector en el extremo de destino así como el puente en el extremo de origen.

En el caso de la conmutación **bidireccional**, se conmuta la señal de tráfico (servicio) de la entidad de transporte activa a la de reserva en ambos extremos del tramo de protección. Cuando se trata de la arquitectura 1+1, funcionan los selectores en los extremos de destino y de origen. En el caso de las arquitecturas 1:n, m:n, $(1:1)^n$, funcionan los selectores y los puentes en los extremos de destino y de origen.

NOTA 1 – Todos los tipos de conmutación excepto la conmutación unidireccional 1+1, necesitan un canal de comunicación entre los dos extremos del dominio protegido; éste se denomina canal de conmutación de protección automática (APS). Este canal termina en las funciones de conexión de cada extremo del dominio protegido.

Con los protocolos de conmutación bidireccional, no se permite la conmutación (funcionamiento de selector y puente) en un solo extremo. Los dos extremos se comunican para iniciar la transferencia de la señal de tráfico normal. Si la prioridad de la petición del extremo de origen es inferior que la del extremo de destino o no existe, el extremo de destino inicia la transferencia de la señal de tráfico normal y el extremo de origen da seguimiento a esa transferencia.

Con el tipo de conmutación unidireccional, las posibles ventajas incluyen:

1) La conmutación de protección unidireccional es un método de fácil implementación y no necesita un protocolo en una arquitectura 1+1.

   NOTA 2 – La conmutación unidireccional en una arquitectura 1:n (que se aplica normalmente en los enlaces de radiocomunicación/satélite) necesita un protocolo que funcione entre los dos puntos extremo del dominio protegido.

2) Cuando se trata de una arquitectura 1+1, la conmutación de protección unidireccional puede ser más rápida que la conmutación de protección bidireccional ya que no requiere de un protocolo.

3) Cuando se tienen múltiples condiciones de fallo hay una gran probabilidad de restablecer el tráfico mediante conmutación de protección si se utiliza la conmutación de protección unidireccional en lugar de emplear la conmutación de protección bidireccional.

4) La conmutación unidireccional permite una realización más simple de una red fiable por medio de subredes protegidas en cascada. Dos subredes se conectan mediante una arquitectura de interconexión de nodo dual/interfuncionamiento de subred dual.

Con el tipo de conmutación bidireccional, las posibles ventajas incluyen:

1) Con la conmutación de protección bidireccional, se utiliza el mismo equipo para ambos sentidos de transmisión después de un fallo. Esto significa que habrá menos interrupciones de servicio para la reparación y el retorno al trayecto de servicio original. Con la conmutación unidireccional, se activan las siguientes conmutaciones:

   i) Conmutación de protección.

   ii) Conmutación forzada para el sentido no afectado por el fallo.

   iii) Conmutación reversiva.

   Con la conmutación bidireccional, sólo se producen dos conmutaciones:

   i) Conmutación de protección.

   ii) Conmutación reversiva.

   Cada conmutación dará por resultado uno o dos segundos con muchos errores. Con la conmutación bidireccional resultan menos SES.

2) Con la conmutación de protección bidireccional, si hay un fallo en una entidad de transporte de la red, la transmisión de ambas entidades de transporte entre los nodos afectados se conmuta al sentido opcional alrededor de la red. Por consiguiente, no se transmite tráfico por la sección de la red fallida para que pueda repararse sin conmutación de protección adicional.

3) La conmutación de protección bidireccional es más fácil de gestionar ya que en ambos sentidos de transmisión se utiliza el mismo equipo a lo largo de toda la entidad de transporte.

4) La conmutación de protección bidireccional mantiene retardos iguales en ambos sentidos de transmisión. Esto puede ser importante cuando hay un desequilibrio significativo en la longitud de las entidades de transporte, por ejemplo, en los enlaces transoceánicos en los que una entidad de transporte se conduce a través de un enlace por satélite y la otra vía un enlace por cable.

5) Además, la conmutación de protección bidireccional tiene la capacidad para transportar tráfico adicional por la entidad de transporte de protección.

9 Tipos de funcionamiento

Los tipos de funcionamiento de protección pueden ser no reversivo o reversivo.

Con funcionamiento **reversivo**, la señal de tráfico (servicio) siempre regresa a (o permanece en) la entidad de transporte de servicio cuando se terminan las solicitudes de conmutación, es decir, cuando la entidad de transporte de servicio se restablece de la condición de defecto o se despeja la petición externa.

Con funcionamiento **no reversivo**, la señal de tráfico (servicio) no regresa a la entidad de transporte de servicio cuando se terminan las peticiones de conmutación.

Algunos métodos de protección son inherentemente reversivos. En otros casos es posible el funcionamiento reversivo o no reversivo. Una ventaja del funcionamiento no reversivo es que, por lo general, tendrá menos repercusión sobre la calidad de funcionamiento del tráfico. No obstante, hay situaciones en las que podrá tenerse preferencia por el funcionamiento reversivo. A continuación se presentan algunos ejemplos de casos en los que es apropiado el funcionamiento reversivo:

1) Cuando algunas partes de la entidad de transporte de protección pueden asignarse para proporcionar capacidad para satisfacer una necesidad más urgente. Por ejemplo, cuando la entidad de transporte de protección se ponga fuera de servicio para liberar capacidad que se utilizará para restablecer otro tráfico.

2) Cuando la entidad de transporte de protección pueda estar sujeta a reestructuraciones frecuentes. Por ejemplo, cuando una red tiene limitaciones de capacidad y las rutas de protección se reestructuran frecuentemente para maximizar la eficacia de la red cuando se producen cambios en la misma.

3) Cuando la entidad de transporte de protección tiene una calidad de funcionamiento significativamente inferior que la de la entidad de transporte de servicio. Por ejemplo, si la entidad de transporte de protección tiene una característica de error inferior o un retardo más prolongado que la entidad de transporte de servicio.

4) Cuando un operador necesita confirmar qué entidades de transporte conducen el tráfico normal, a fin de simplificar la gestión de la red.

10 Tipos de protocolos

Excepto en el caso de la conmutación unidireccional 1+1, todos los tipos de protección necesitan que los dos extremos, A y Z, del dominio protegido coordinen sus acciones de puenteo y selección. Se necesitan distintos protocolos conforme al tipo de protección y a los tipos de selector y puente utilizados. Por consiguiente, los nodos A y Z se comunican entre ellos a través del canal de conmutación de protección automática (APS).

Existen dos requisitos básicos para un protocolo de protección:

1) La prevención de conexiones erróneas.

2) La disminución del número de ciclos de comunicación entre los extremos A y Z del dominio protegido, para reducir el tiempo de conmutación de protección. La comunicación puede realizarse una vez (Z → A), dos veces (Z → A y A → Z), o tres veces (Z → A, A → Z y Z→ A). Estos protocolos se denominan de una fase, de dos fases y de tres fases.

En el cuadro 1 se muestran las condiciones en virtud de las cuales pueden utilizarse los distintos tipos de protocolos.

Cuadro 1/G.808.1 – Tipos de protocolos relacionados con las arquitecturas de protección y los tipos de selector/puente

Tipo de protocolo	Tipos de protección que utilizan protocolo	Tipo de puente	Tipo de selector
Sin protocolo	Sólo unidireccional 1+1	Permanente	Selectivo
Una fase	Sólo unidireccional $(1:1)^n$	Selector	Selectivo o de fusión
Dos fases	Sólo arquitecturas 1+1	Permanente	Selectivo
Tres fases	Todos los tipos de arquitecturas	Cualquiera	Selectivo
		Selector	De fusión (tecnologías basadas en células/paquetes)

Con el tipo de protocolo de tres fases las posibles ventajas incluyen:

1) funciona con todos los tipos de arquitecturas;
2) evita que se produzcan conexiones erróneas en cualquier circunstancia;
3) hace funcionar un selector o un puente únicamente después de la confirmación de la prioridad con el otro extremo del dominio protegido.

Con el tipo de protocolo de tres fases las posibles desventajas incluyen:

4) se necesita el intercambio de tres mensajes entre los dos extremos del dominio protegido, lo que aumenta el tiempo de conmutación.

Con el tipo de protocolo de dos fases las posibles ventajas incluyen:

1) tiempo de conmutación reducido en comparación con el protocolo de tres fases.

Con el tipo de protocolo de dos fases las posibles desventajas incluyen:

2) funciona sólo con las arquitecturas 1+1.

Con el tipo de protocolo de una fase las posibles ventajas incluyen:

1) tiempo de conmutación reducido ya que se necesita el intercambio de un solo mensaje entre los dos extremos del dominio protegido.

Con el tipo de protocolo de una fase las posibles desventajas incluyen:

2) funciona sólo con arquitecturas $(1:1)^n$;
3) necesita el establecimiento de "n" entidades de transporte adicionales (en comparación con la arquitectura 1:n) en el ancho de banda de protección, a fin de evitar que se produzcan conexiones erróneas;
4) hace funcionar un puente/selector antes de que el otro extremo del dominio protegido confirme la prioridad. Por consiguiente, es posible que tenga que revertirse una acción de conmutación y reemplazarse por otra acción de puente/selector iniciada por el otro extremo;
5) protocolo más complejo ya que hay "n" tipos de protección 1:1 paralelos.

11 Clases y subclases de protección

11.1 Protección de camino

La clase de protección de camino se utiliza para proteger un camino a través de toda la red del operador o de múltiples redes de operador. Se trata de una arquitectura de protección extremo a extremo dedicada, que puede utilizarse con distintas estructuras de red: redes en malla, anillos, y otras. Como la protección de camino es un mecanismo de protección dedicado, no hay límites fundamentales en el número de elementos de red (NE) a lo largo de los caminos.

La protección de camino funciona en todas las combinaciones de arquitecturas, conmutación y funcionamiento de protección.

Por lo general, la protección de camino protege contra fallos en la capa servidora, y fallos de conectividad y degradaciones de calidad de funcionamiento en la capa cliente.

En el caso de la protección de camino, se protege la información adaptada (AI) (es decir, la carga útil de la información característica (CI) de la capa de red). Véase la figura 9.

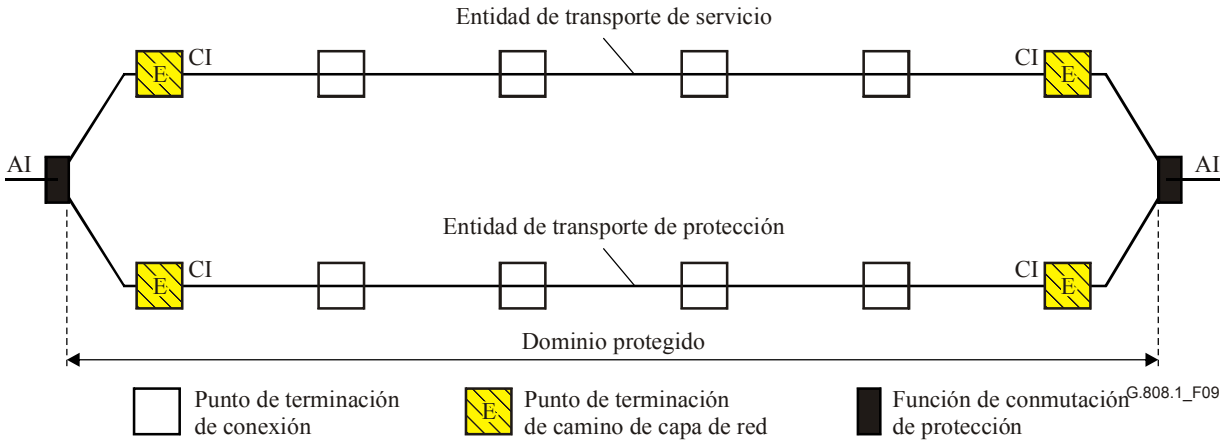


Figura 9/G.808.1 – Concepto genérico de la protección de camino

NOTA 1 – Ya que las protecciones de camino 1:1, 1:n, m:n son mecanismos de protección lineal, las funciones de terminación de camino normal y de tráfico adicional se ubican en el mismo NE. En una aplicación de red esto supone que deben coincidir los patrones de tráfico normal y adicional.

La protección de camino no soporta arquitecturas de red que utilicen subredes de protección en cascada en la misma capa. Por consiguiente, el tráfico puede restablecerse sólo en condiciones de fallo simple. Para restablecer el tráfico en condiciones de múltiples fallos tiene que utilizarse la protección SNC, o bien la protección de camino ha de complementarse con protección en las capas servidoras.

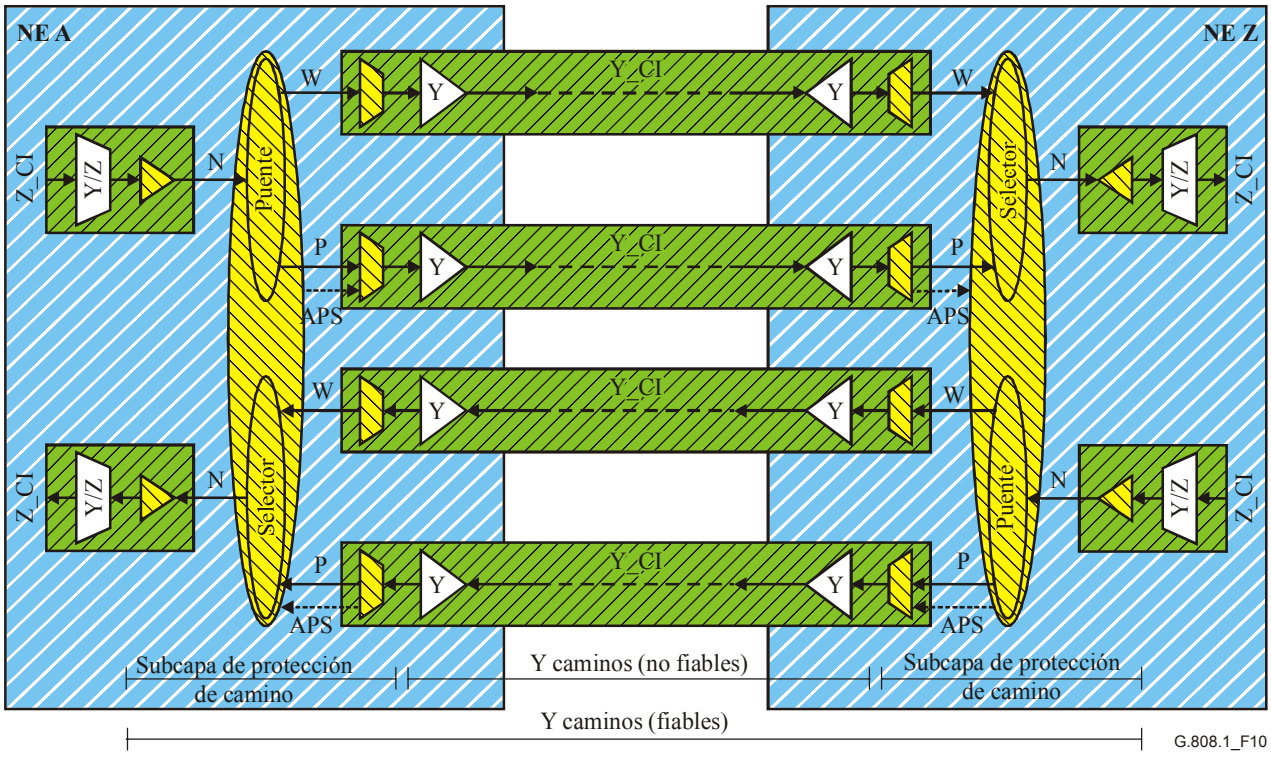
NOTA 2 – Cuando se trata de una arquitectura 1:1, m:n, o $(1:1)^n$ en ATM, el (los) camino(s) de protección deben incluir una señal que permita una supervisión precisa de su estado. En condiciones normales, cuando la señal de tráfico normal se transporta a través del camino de servicio, no hay señal que deba transportarse a través de la protección. Si la comprobación de continuidad (CC) va a estar inactiva, ese camino de protección no transportará ninguna información en condiciones normales sin fallo. Cuando se produce un fallo, se insertan células AIS. Cuando el fallo aparece sólo por un corto periodo (por ejemplo, provocado por una "acción de protección de capa física"), el detector de defectos AIS en el punto extremo del camino de protección detectará la condición de defecto AIS durante dos o tres segundos conforme a la definición de estado AIS definida en la Rec. UIT-T I.610. Cuando se activa CC, se despeja la condición de defecto AIS con la recepción de una célula CC, es decir, dentro de un periodo de un segundo después de que se despejó la interrupción del tráfico.

NOTA 3 – Si se utiliza protección de camino en el nivel de trayecto, puede dar por resultado la ocupación de un puerto adicional en el soporte físico en comparación con la protección SNC. Éste es el caso cuando el selector de protección se ubica en el puerto de salida del equipo.

11.1.1 Protección de camino individual

En la figura 10 se ilustra el caso de la protección de camino 1+1 y de la protección de camino 1:1 sin tráfico adicional entre la entrada y la salida del dominio protegido, es decir, entre los elementos de red A y Z. Hay dos caminos independientes (en la red de capa Y) que fungen como entidades de transporte de servicio y de protección para la señal de tráfico normal (cabida útil protegida). Las funciones de terminación de camino (TT) generan/insertan y supervisan/extraen la información de tara/OAM extremo a extremo para determinar el estado de las entidades de transporte de servicio y de protección. La información APS se transporta por el camino de protección, excepto en el caso de conmutación unidireccional 1+1.

Los casos de las arquitecturas 1:n, m:n y $(1:1)^n$ con/sin tráfico adicional son ampliaciones de la arquitectura 1+1/1:1, conforme a las descripciones del tipo de arquitectura en la cláusula 7.



NOTA – La señal APS no se aplica al caso de comuntación unidireccional 1+1.

Figura 10/G.808.1 – Modelo funcional de protección de camino tipo 1+1/1:1

11.1.2 Protección de camino de grupo

En la figura 11 se ilustra el caso de la protección de camino de grupo 1+1/1:1 entre los NE A y Z. En este ejemplo, hay dos veces tres caminos independientes paralelos (en la red de capa Y) que se comportan como grupos de entidades de transporte de servicio y de protección para las tres señales de tráfico normal (cabida útil protegida). Las tres señales de tráfico normal paralelas en el grupo están protegidas conjuntamente por la función de conexión de subcapa de protección de camino. Las funciones TT generan/insertan y supervisan/extraen información de tara/OAM extremo a extremo para determinar el estado de las entidades de transporte de servicio y de protección. La información APS se transporta por uno de los caminos de protección, excepto en el caso de la conmutación unidireccional 1+1.

Los casos de las arquitecturas 1:n, m:n y $(1:1)^n$ con/sin tráfico adicional son ampliaciones de la arquitectura 1+1/1:1, conforme a las descripciones del tipo de arquitectura en la cláusula 7.

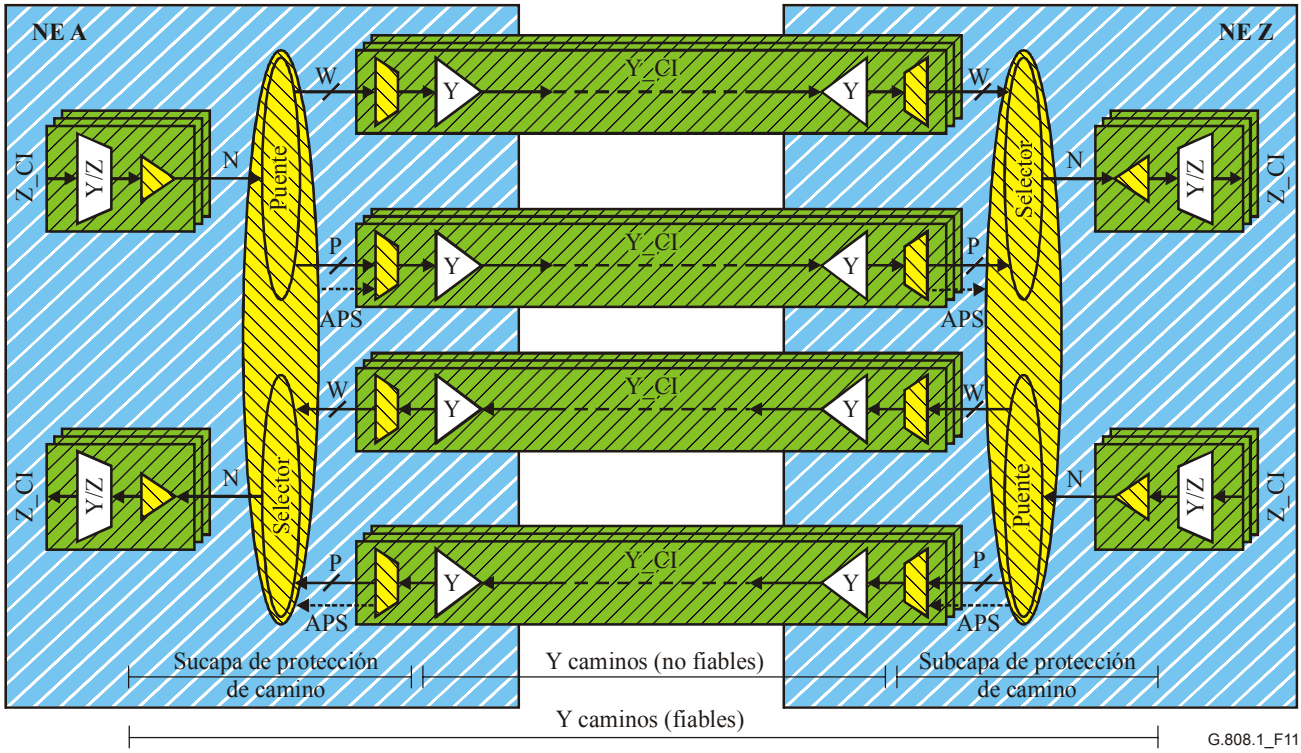


Figura 11/G.808.1 – Modelo funcional de protección de camino de grupo 1+1/1:1

En la figura 12 se presentan detalles adicionales relativos a estos procesos de la función de conexión de protección. El proceso lógico SFG/SDG es específico para la protección de grupo. Este proceso permite "fusionar" las tres señales de fallo de señal de camino (TSF) individual en un solo grupo SF (SFG) y las señales de degradación de señal de camino (TSD) individuales en un solo SDG.

La lógica SFG/SDG puede funcionar de distintas maneras:

- W-SFG = W1-TSF o W2-TSF o W3-TSF
  P-SFG = P1-TSF o P2-TSF o P3-TSF
- W-SFG = W1-TSF
  P-SFG = P1-TSF
- W-SFG = X% de las señales Wi-TSF están activas
  P-SFG = X% de las señales Pi-TSF están activas
- igual para SDG.

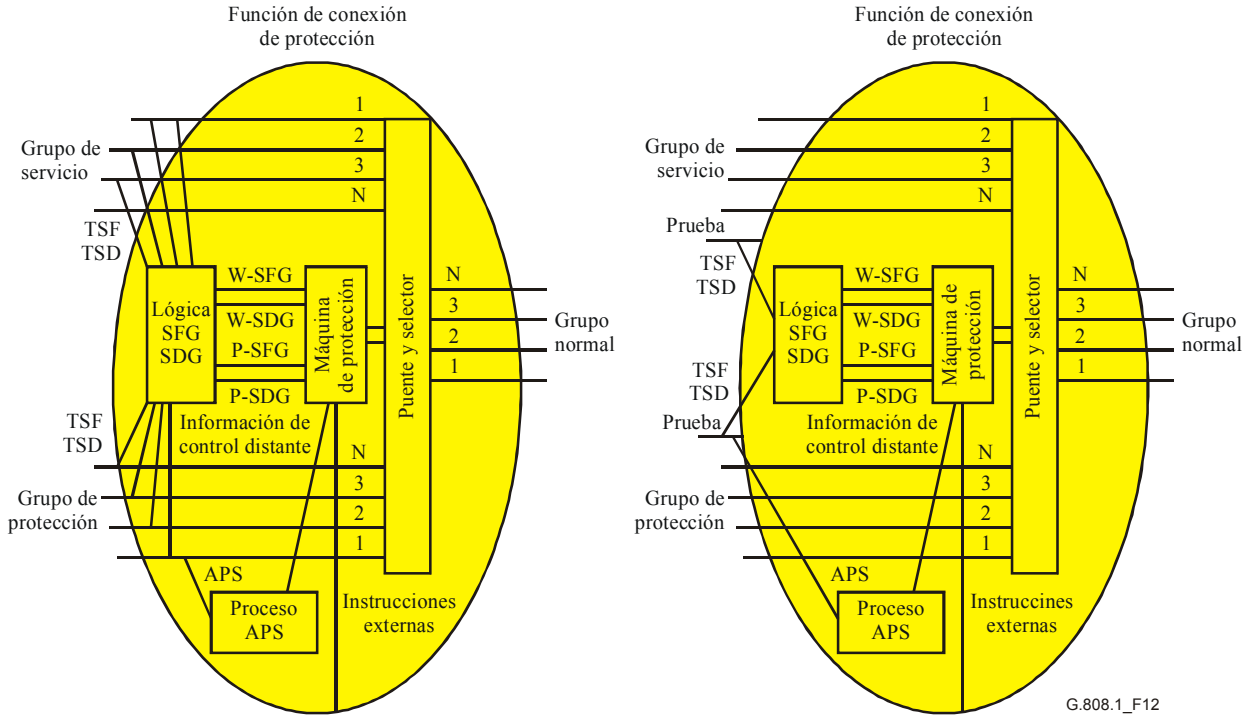


Figura 12/G.808.1 – Lógica SFG/SDG en el proceso de protección de grupo

Como resultado del gran número de intervalos tributarios de algunas tecnologías de transmisión (por ejemplo, ATM), se pueden asignar intervalos tributarios adicionales a las señales de la capa servidora de servicio y de protección para transportar señales de prueba por las entidades de transporte de prueba (figuras 13 y 14). Estas señales de prueba (una para servicio y otra para protección) pueden utilizarse en lugar de la información SFG, SDG como se describió anteriormente. La señal APS se transporta por la entidad de transporte de protección de prueba.

La lógica SFG/SDG funciona ahora de la siguiente manera:

- W-SFG = Wt-TSF
  P-SFG = Pt-TSF
- W-SDG = Wt-TSD
  P-SDG = Pt-TSD

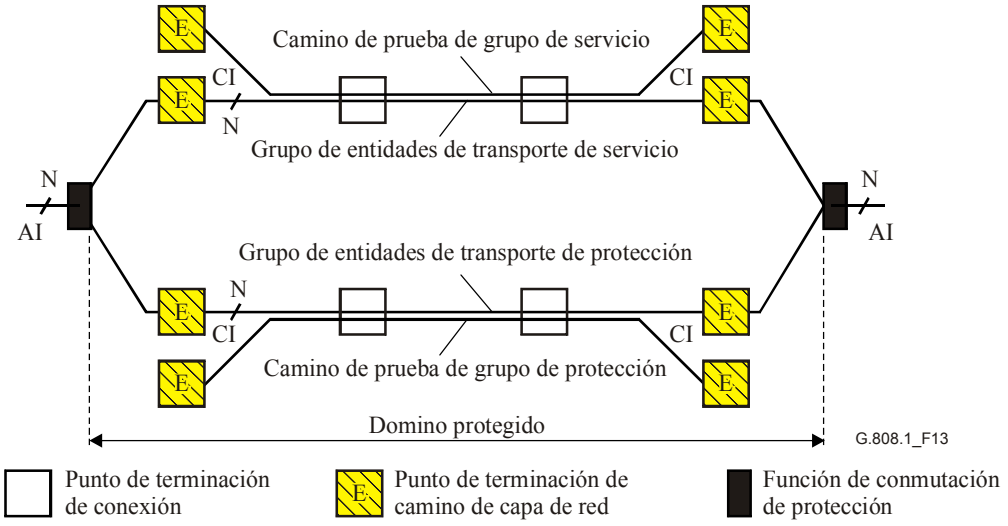


Figura 13/G.808.1 – Concepto genérico de la protección de camino/T de grupo

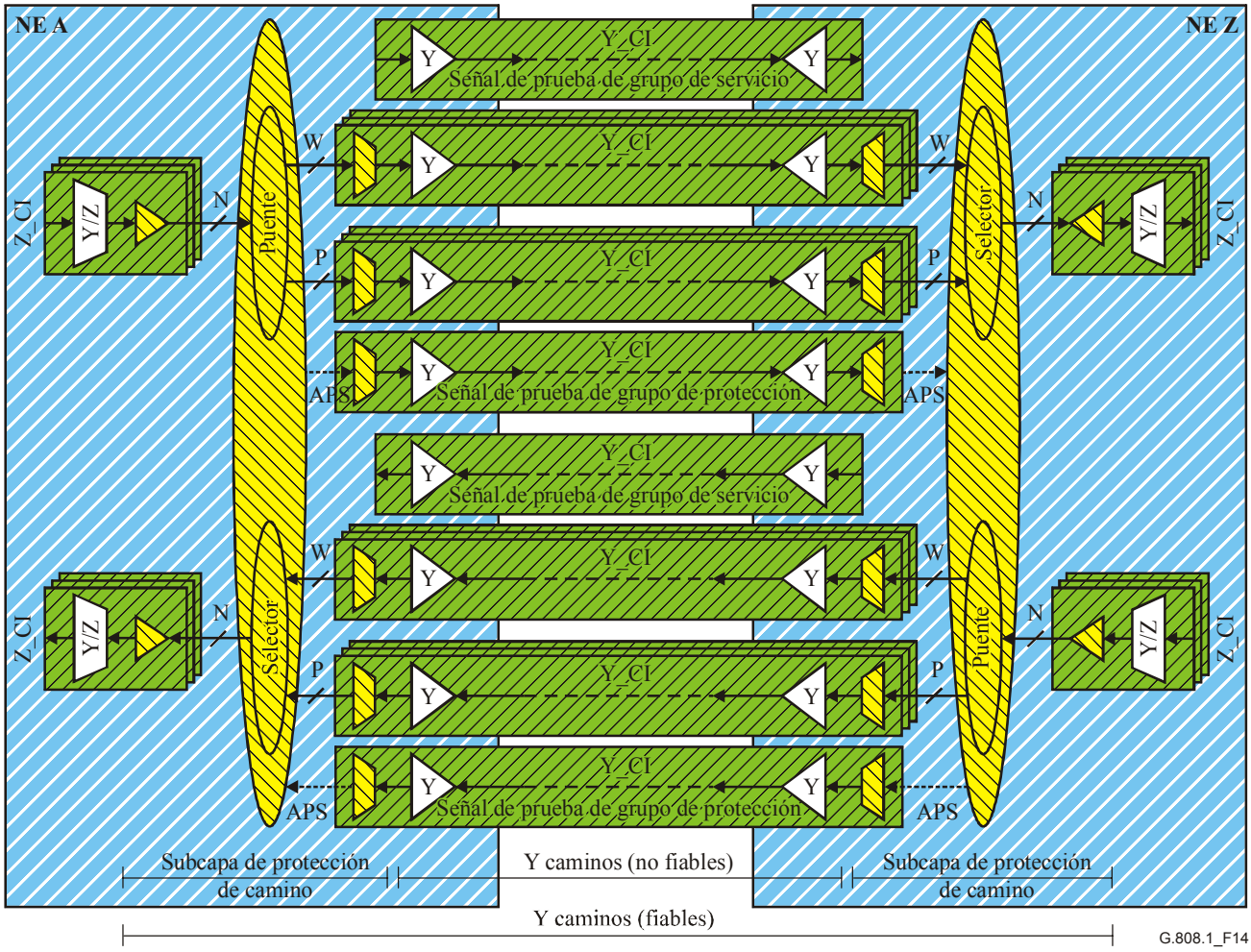


Figura 14/G.808.1 – Modelo funcional de protección de camino/T de grupo 1+1/1:1

11.2 Protección tipo SNC

La clase de protección de conexión de subred se utiliza para proteger un tramo de un camino (por ejemplo, el tramo en el que hay dos rutas independientes disponibles) dentro de una red de operador o de múltiples redes de operador.

La conexión de subred protegida puede ubicarse entre dos puntos de conexión (CP, *connection point*) (figura 15), entre un CP y un punto de conexión de terminación (TCP) (figura 16), o puede ser toda la conexión de red extremo a extremo entre los dos TCP (figura 17).

Ya que la protección de conexión de subred es un mecanismo de protección dedicado, puede utilizarse en cualquier estructura física (es decir, en malla, anillos, o mixta) y no hay límites fundamentales con relación al número de elementos de red dentro de la conexión de subred. Puede aplicarse a cualquier capa en una red de capas.

La protección SNC funciona en todas las combinaciones de arquitecturas, conmutación y funcionamiento de protección.

La SNCP puede dividirse incluso en subclases que representan las condiciones con defectos que contribuyen a las condiciones SF/SD, a saber:

1) Inherente – La terminación de camino de la capa servidora y las funciones de adaptación se utilizan para determinar la condición SF/SD. Soporta únicamente la detección de condiciones con defectos de capa servidora.

2) No intrusiva – Se despliegan funciones de supervisión no intrusiva para determinar la condición SF/SD.

   a) Extremo a extremo – Detección de condiciones con defectos de capa servidora, condiciones con defectos de continuidad/conectividad en la red de capa y condiciones de degradación de error en la red de capa. Se utiliza la tara OAM extremo a extremo.

   b) Subcapa – Detección de condiciones con defectos de capa servidora, condiciones con defectos de continuidad/conectividad en la red de capa y condiciones de degradación de error en la red de capa. Se utiliza la tara/OAM de subcapa.

3) Subcapa – Se despliegan funciones de subcapa de conexión/segmento en cascada para determinar la condición SF/SD. Soporta la detección de condiciones con defectos de capa servidora, condiciones de defectos de continuidad/conectividad en la red de capa y condiciones de degradación de error en la red de capa. Se utiliza la tara/OAM de subcapa.

Por lo general, la protección SNC exige la creación de caminos de subcapa (conexiones en cascada, segmentos) en las entidades de transporte de servicio y de protección para distinguir un fallo o una degradación que se produce "frente" al dominio protegido de aquéllos "dentro" del mismo dominio. Cuando el camino de subcapa tenga que incluir un solo camino de capa servidora, puede utilizarse este último camino en lugar del primero (proporcionando supervisión inherente). Si no puede crearse un camino de subcapa o no está disponible un camino de capa servidora simple entre los puntos de entrada y salida del dominio protegido, podrá realizarse la protección SNC mediante la doble realimentación de la señal de tráfico normal en ambas entidades de transporte de servicio y de protección, supervisando de modo no intrusivo ambas copias de la señal en el punto de salida y comparando el estado SF/SD obtenido de ambas supervisiones. Si el fallo o degradación se producen frente al dominio protegido, ambas supervisiones de servicio y de protección detectarán la degradación y no se llevará a cabo la acción de conmutación. De lo contrario, sólo una de las dos supervisiones detectará una condición SF/SD y podrá restablecerse el flujo de tráfico con una acción de conmutación.

NOTA 1 – En el caso de SDH, debido al tratamiento de los punteros AU/TU durante condiciones de TSF de capa servidora, podrá desplegarse protección SNC/I 1+1 en lugar de SNC/N 1+1 si sólo deben protegerse defectos de la capa servidora.

En el caso de protección SNC, se protege la información característica (CI) (es decir, la cabida útil y su tara de capa). Véanse las figuras 15 a 18.

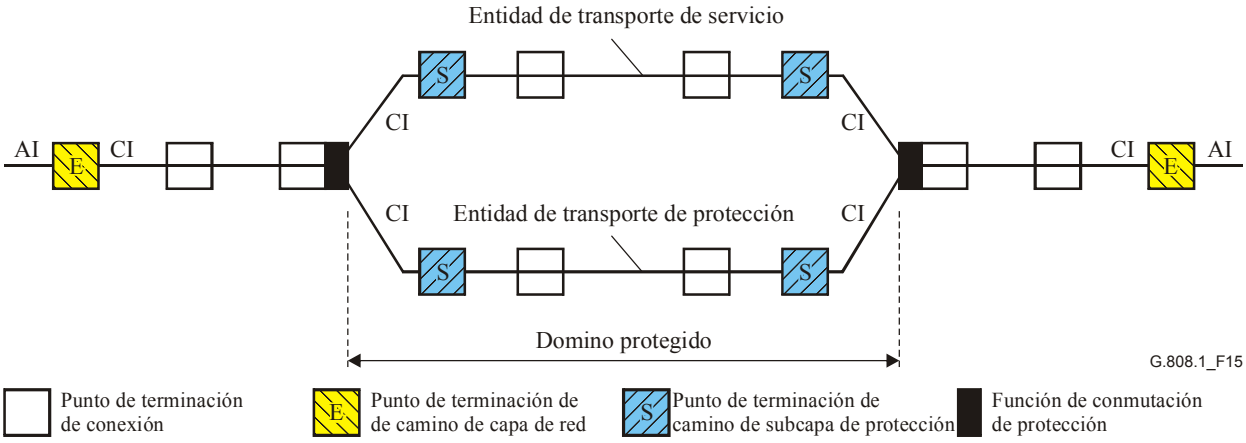


Figura 15/G.808.1 – Ejemplo 1 de protección SNC/S

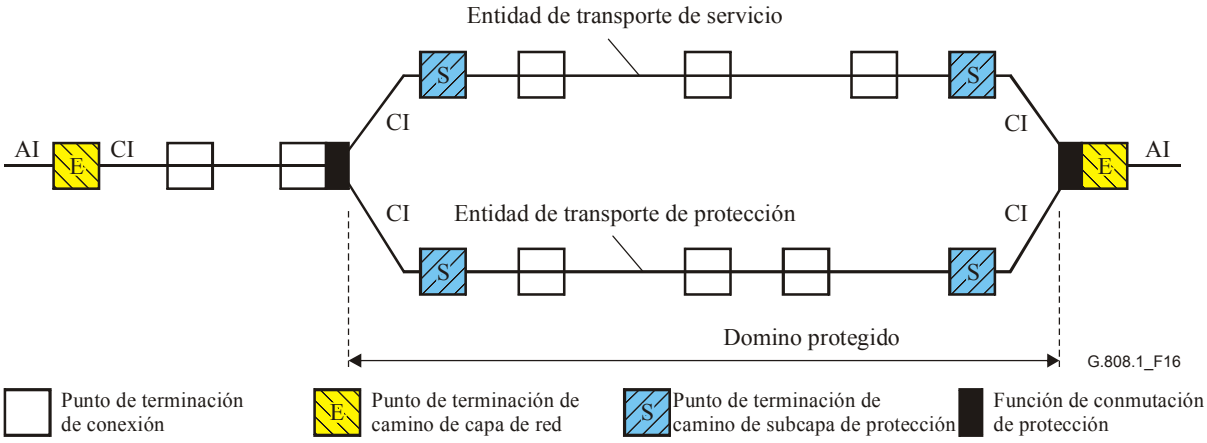


Figura 16/G.808.1 – Ejemplo 2 de protección SNC/S

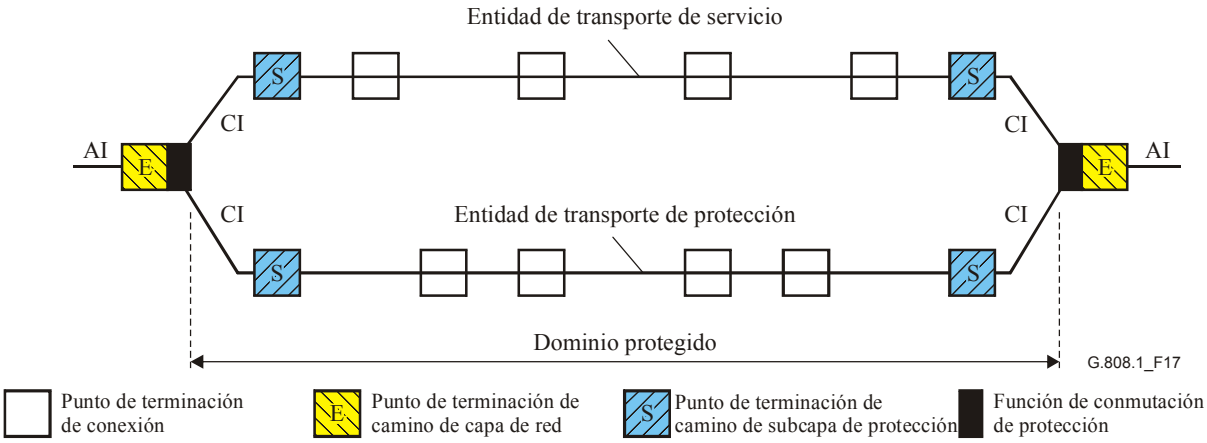


Figura 17/G.808.1 – Ejemplo 3 de protección SNC/S

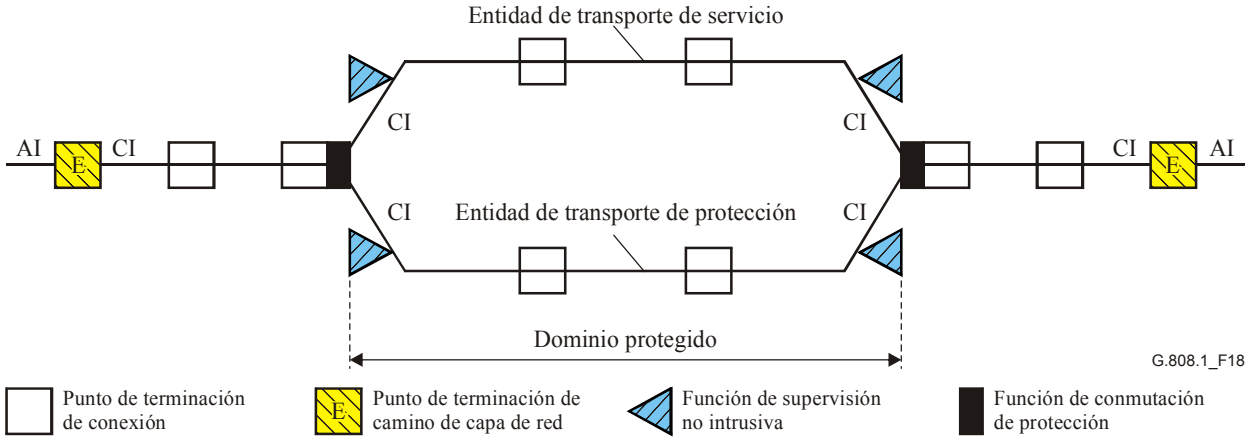


Figura 18/G.808.1 – Protección SNC/N 1+1

La protección SNC soporta arquitecturas de red que emplean subredes protegidas en cascada. Esas arquitecturas de red pueden restablecer el tráfico en el caso de múltiples fallos (un fallo por subred protegida); véase la figura 19.

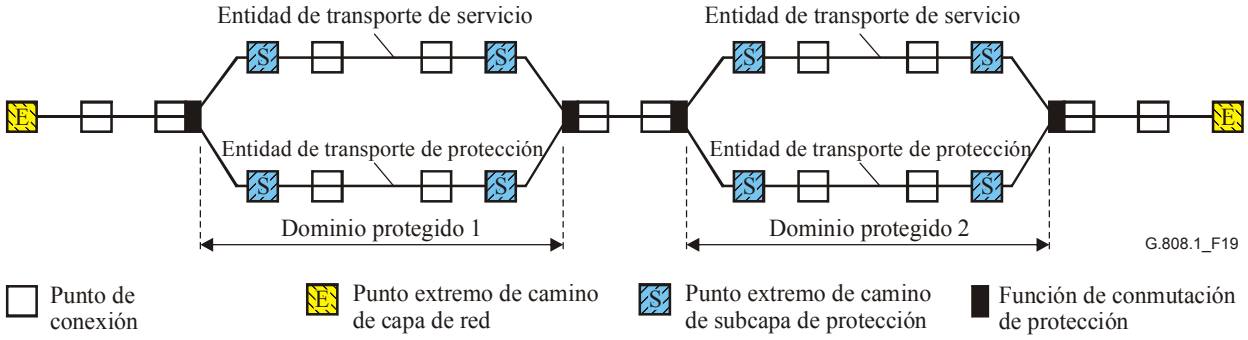


Figura 19/G.808.1 – Protección SNC/S en cascada

La tolerancia a los fallos (y la fiabilidad) de las subredes protegidas con SNC en cascada aumenta cuando se duplica la interconexión entre las subredes (figura 20), eliminando el punto simple de fallo. Esto necesita la utilización de tipos de protección SNC/N o SNC/I con conmutación unidireccional 1+1. Empleando protección 1:n, m:n, $(1:1)^n$ y/o conmutación bidireccional no es posible lo anterior.

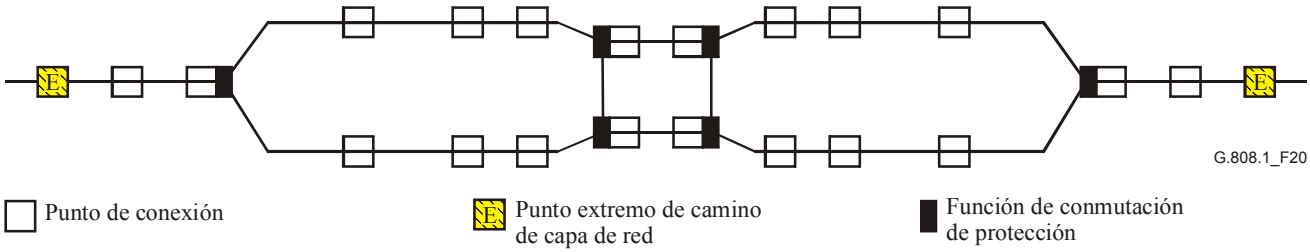


Figura 20/G.808.1 – Protección SNC 1+1 en cascada con interconexión a subred que tolera a fallos

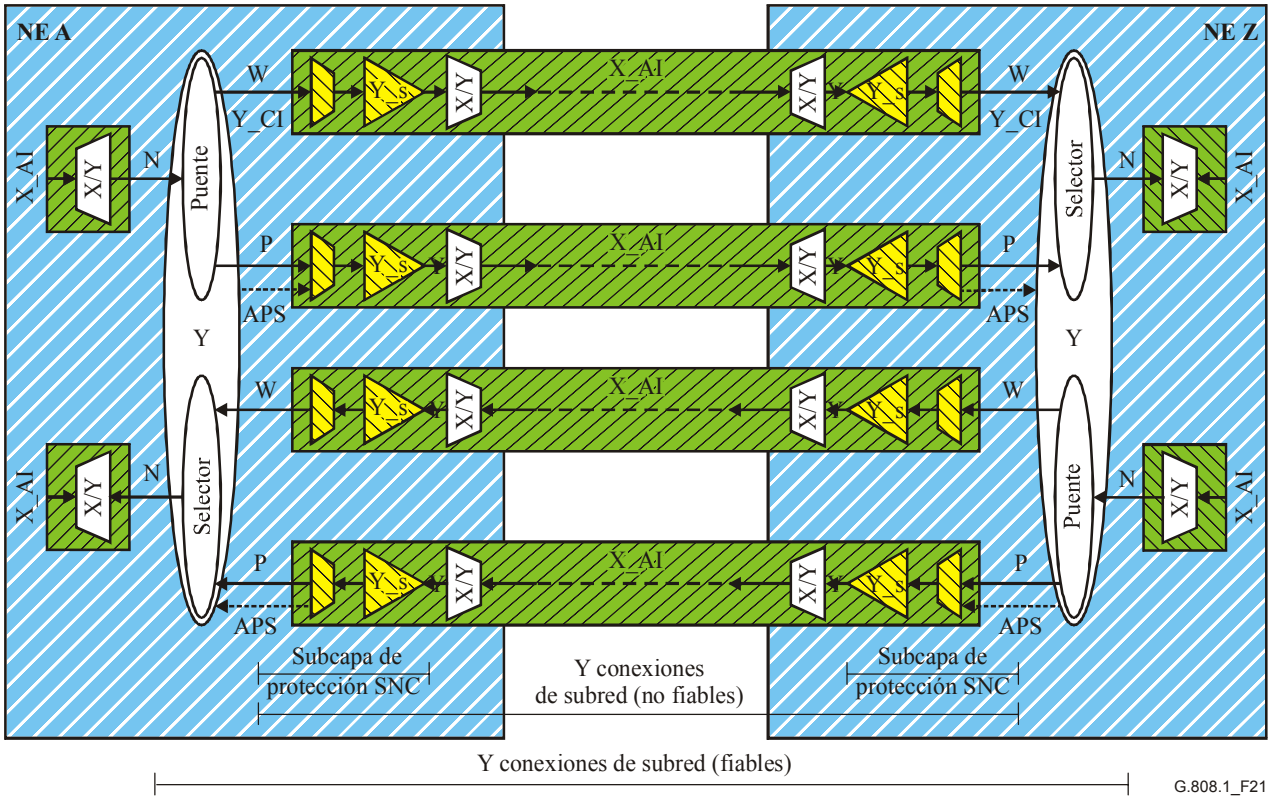
NOTA 2 – En el caso de una arquitectura 1:1, m:n, o $(1:1)^n$ en ATM, la(s) conexión(es) de subred de protección deben incluir una señal que permita una supervisión precisa de su estado. En condiciones normales, en las que se transporta la señal de tráfico normal por la SNC de servicio, no hay ninguna señal que deba transportarse por la protección. Si la comprobación de continuidad (CC) estuviese inactiva, la SNC de protección no transportaría ninguna información en condiciones normales sin fallos. Cuando se produce un fallo, se insertan células AIS. Cuando el fallo aparece sólo por un periodo corto (por ejemplo, debido a una "acción de protección de capa física"), el detector de defectos AIS en el punto extremo del segmento de protección detectará la condición de defecto AIS durante 2 ó 3 segundos conforme a la definición de estado AIS de la Recomendación I.610. Cuando está activada la CC, se despejará la condición de defecto AIS cuando se recibe una célula CC, es decir, dentro de un periodo de un segundo después de que se despejó la interrupción del tráfico.

11.2.1 Protección SNC individual

11.2.1.1 Protección SNC/S 1+1, 1:n, m:n, $(1:1)^n$

En la figura 21 se ilustra el caso de la protección SNC/S 1+1 y de la protección SNC/S 1:1 sin tráfico adicional entre la entrada y la salida del dominio protegido, es decir, entre los elementos de red A y Z. Hay dos caminos de subcapa independientes, que actúan como entidades de transporte de servicio y de protección para la señal de tráfico normal (protegida). Las funciones TT de subcapa generan/insertan y supervisan/extraen la información de tara/OAM de subcapa para determinar el estado de la entidad de transporte de servicio y de protección. La información APS se transporta por la SNC de protección, excepto en el caso de conmutación unidireccional 1+1.

Los casos de las arquitecturas 1:n, m:n y $(1:1)^n$ con/sin tráfico adicional son ampliaciones de la arquitectura 1+1/1:1, conforme a las descripciones del tipo de arquitectura en la cláusula 7.



NOTA – La señal APS no se aplica en el caso de conmutación unidireccional 1+1.

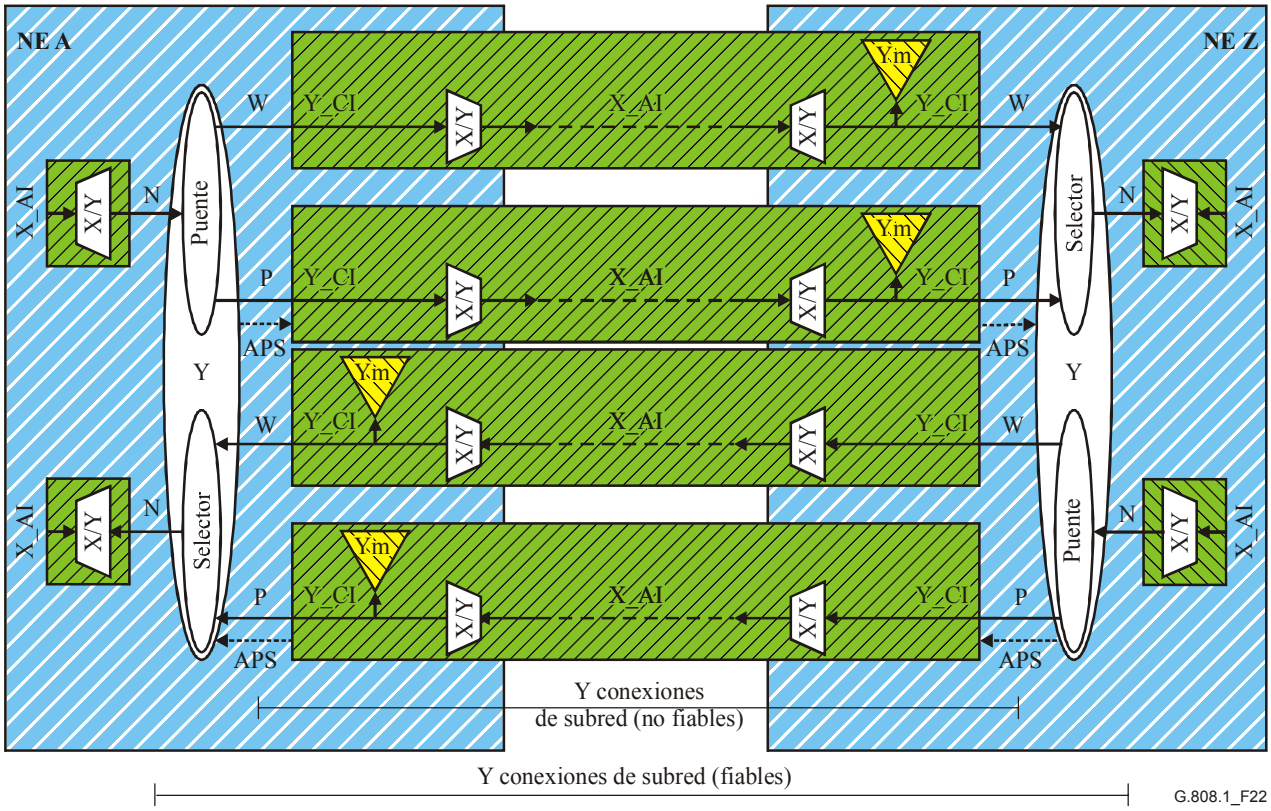
Figura 21/G.808.1 – Modelo funcional de protección SNC/S 1+1/1:1

NOTA – Las funciones de terminación de camino de subcapa (por ejemplo, funciones de conexión en cascada/terminación de segmento) se utilizan para fines administrativos (para supervisar la calidad de servicio del transporte a través del dominio de red administrativo) y para fines de protección. En este último caso, la ubicación de las terminaciones de camino de subcapa es la indicada en las figuras SNC/S. En el caso de fines administrativos, la ubicación óptima se encuentra en el otro lado de la función de conexión.

11.2.1.2 Protección SNC/N 1+1

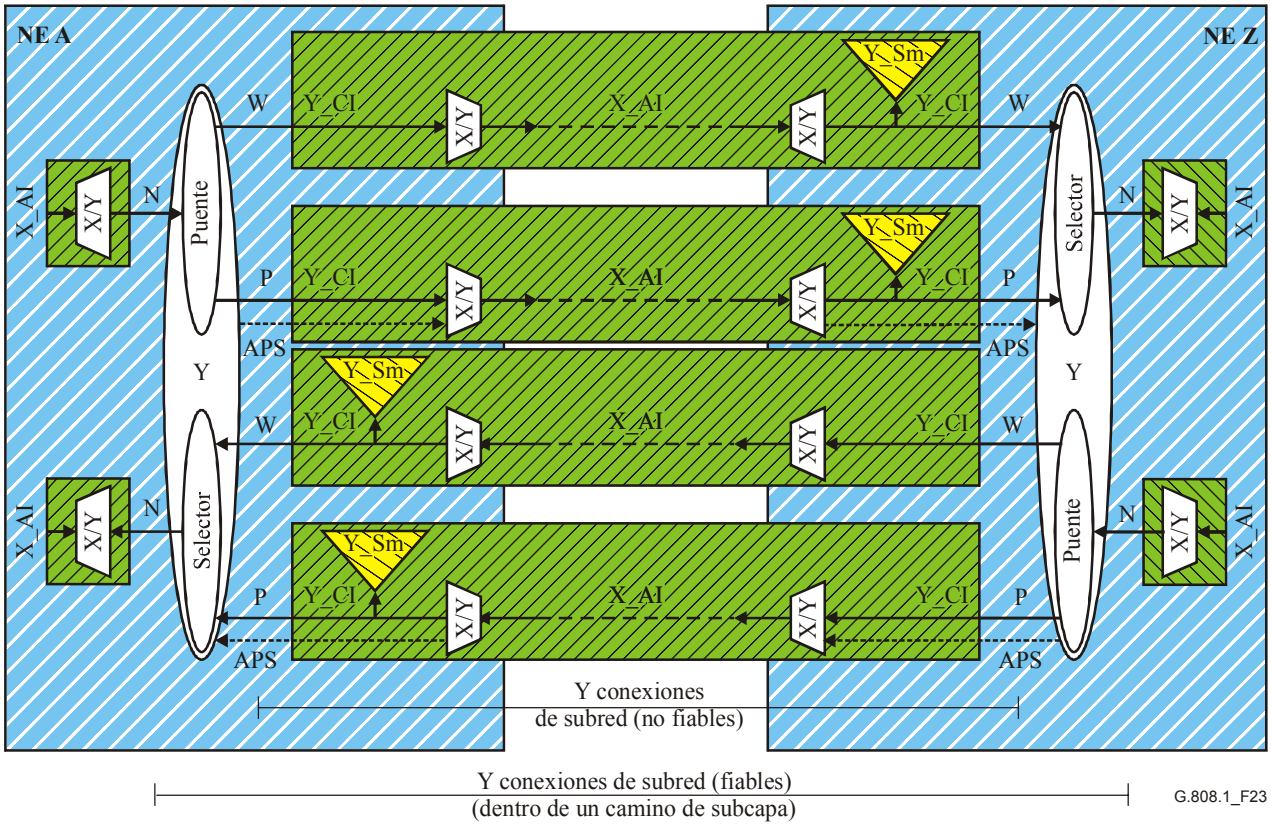
En el caso de la protección SNC 1+1, se define un método con *reducción de complejidad*: SNC/N.

En las figuras 22 y 23 se ilustra el caso de la protección SNC/N 1+1 entre la entrada y la salida del dominio protegido, es decir, entre los elementos de red A y Z. Hay dos conexiones de subred independientes, que actúan como entidades de transporte de servicio y de protección para la señal de tráfico normal (protegida). Las funciones de supervisión no intrusiva (NIM) (Ym_TT_Sk, Y_Sm_TT_Sk) supervisan la información de tara/OAM de extremo a extremo (SNC/Ne) o de subcapa (SNC/Ns) para determinar el estado de las entidades de transporte de servicio y de protección. La información APS se transporta por la SNC de protección, excepto en el caso de conmutación unidireccional 1+1.



NOTA – La señal APS no se aplica en el caso de conmutación unidireccinal 1+1.

Figura 22/G.808.1 – Modelo funcional de protección SNC/Ne 1+1



NOTA – La señal APS no se aplica en el caso de conmutación unidireccional 1+1.

Figura 23/G.808.1 – Modelo funcional de protección SNC/Ns 1+1

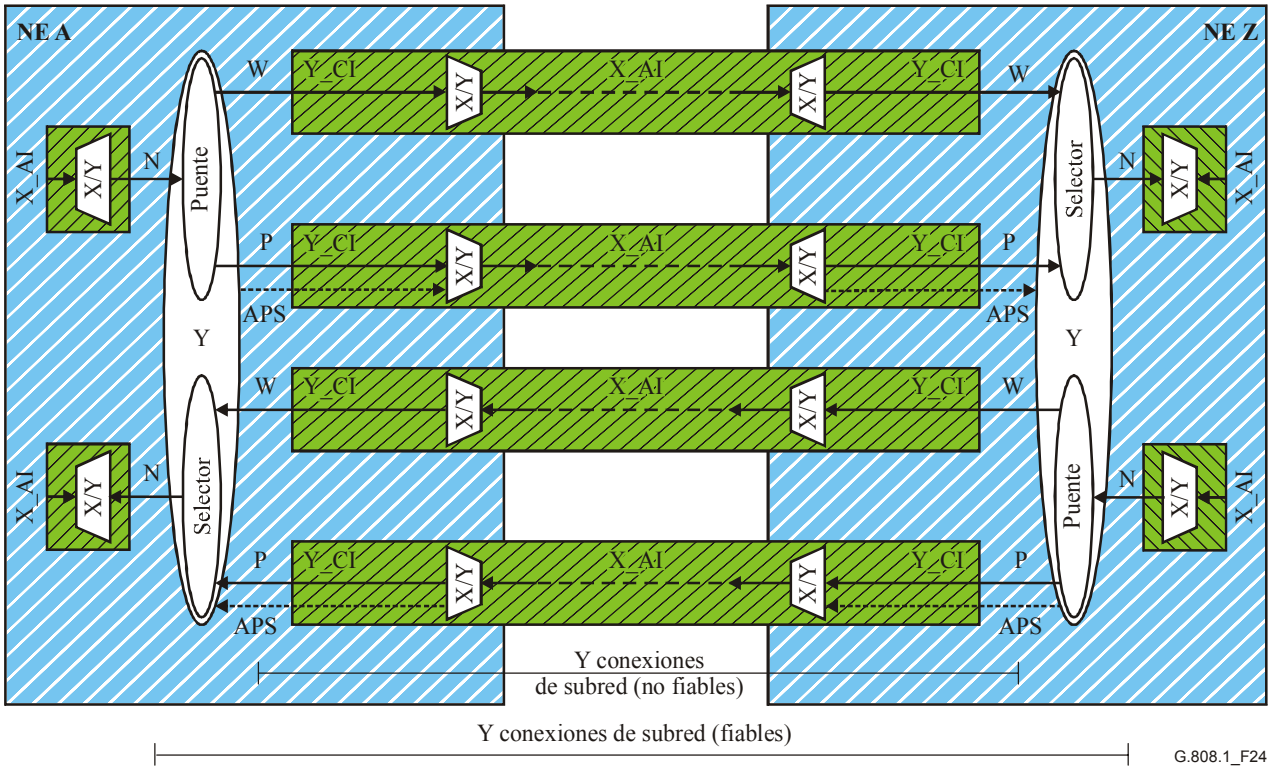
11.2.1.3 Protección tipo SNC/I 1+1/1:n

Cuando se trata de la protección tipo SNC 1+1/1:n, otro método con *complejidad reducida* es: SNC/I.

En la figura 24 se ilustra el caso de protección SNC/I 1+1/1:1 entre la entrada y la salida del dominio protegido, es decir, entre los elementos de red A y Z. Hay dos conexiones de subred independientes, que se comparten como las entidades de transporte de servicio y de protección de la señal de tráfico normal (protegida). Las funciones de adaptación X/Y supervisan la información adaptada de la capa servidora para detectar un fallo de señal, y para determinar el estado de las entidades de transporte de servicio y de protección. La información APS se transporta por la protección SNC, excepto en el caso de conmutación unidireccional 1+1.

Por lo general la protección SNC/I es un método para una sola conexión de enlace (que abarca sólo un camino de capa servidora) ya que las funciones de adaptación deducen sus condiciones SSF y SSD de las condiciones TSF/TSD de camino de la capa servidora. El estado TSF se retransmite como una señal de mantenimiento AIS/FDI de capa cliente y no es visible como tal en las funciones de adaptación en sentido descendente. La información TSD no se retransmite.

Hay una excepción para la protección SNC/I VC-n SDH; la protección SNC/I puede proteger una conexión de enlace combinado en serie ya que la señal de mantenimiento AIS se detecta en cada función de adaptación en sentido descendente del punto de inserción.



NOTA – La señal APS no se plica al caso con conmutación unidireccional 1+1.

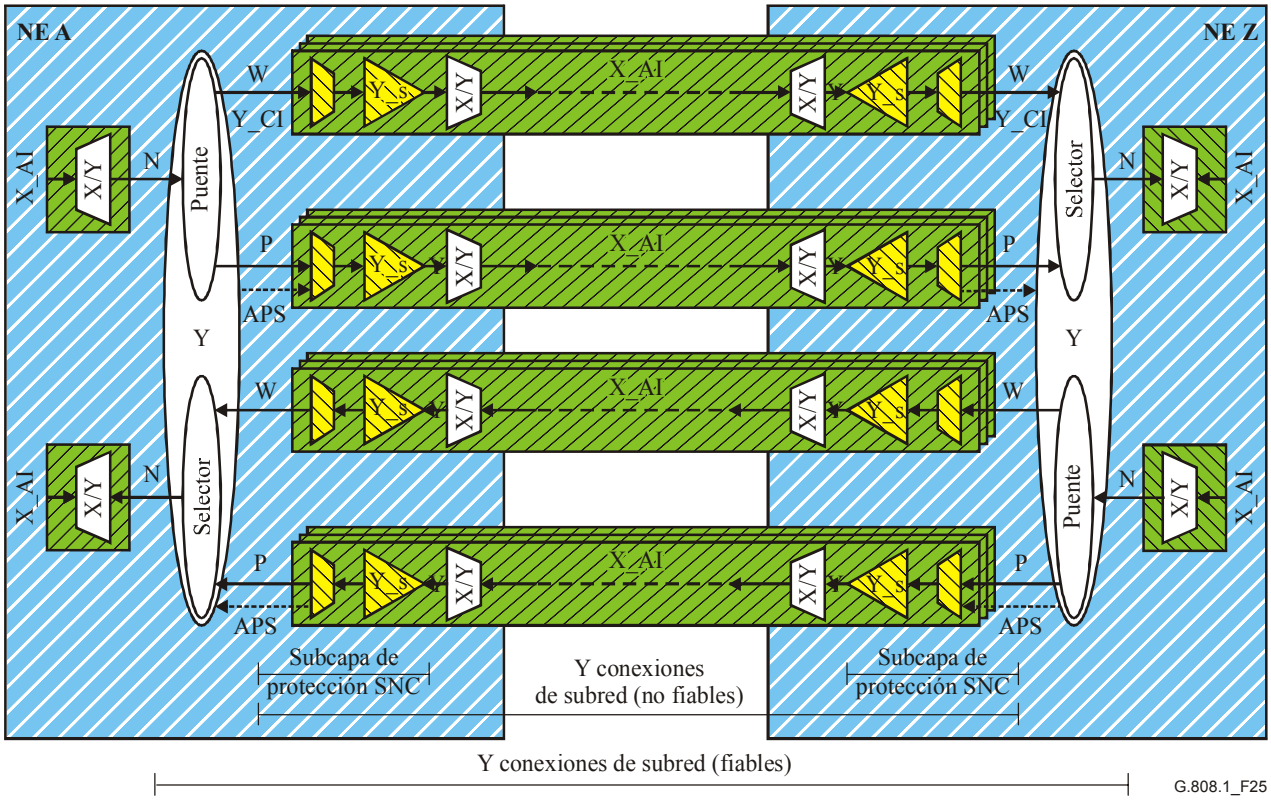
Figura 24/G.808.1 – Modelo funcional de protección SNC/I 1+1/1:1

11.2.2 Protección SNC de grupo

11.2.2.1 Protección SNC/S

En la figura 25 se ilustra el caso de protección SNC/S de grupo 1+1/1:1 entre los NE A y Z. En este ejemplo, hay dos veces tres conexiones de subred paralelas independientes con supervisión de camino de subcapa, que actúan como grupos de entidades de servicio y de protección de las tres señales de tráfico normal (protegidas). Las tres señales de tráfico normal paralelas en el grupo quedan protegidas conjuntamente por la función de conexión de capa. Las funciones TT de subcapa generan/insertan y supervisan/extraen información de tara/OAM de subcapa para determinar el estado de las entidades de transporte de servicio y de protección. La información APS se transporta por una de las SNC de protección, excepto en el caso de conmutación unidireccional 1+1.

Los casos de arquitecturas 1:n, m:n y $(1:1)^n$ con/sin tráfico adicional son ampliaciones de la arquitectura 1+1/1:1, conforme a las descripciones de tipo de arquitectura en la cláusula 7.



NOTA – La señal APS no se aplica en el caso de conmutación unidireccional 1+1

Figura 25/G.808.1 – Modelo funcional de protección SNC/S de grupo 1+1/1:1

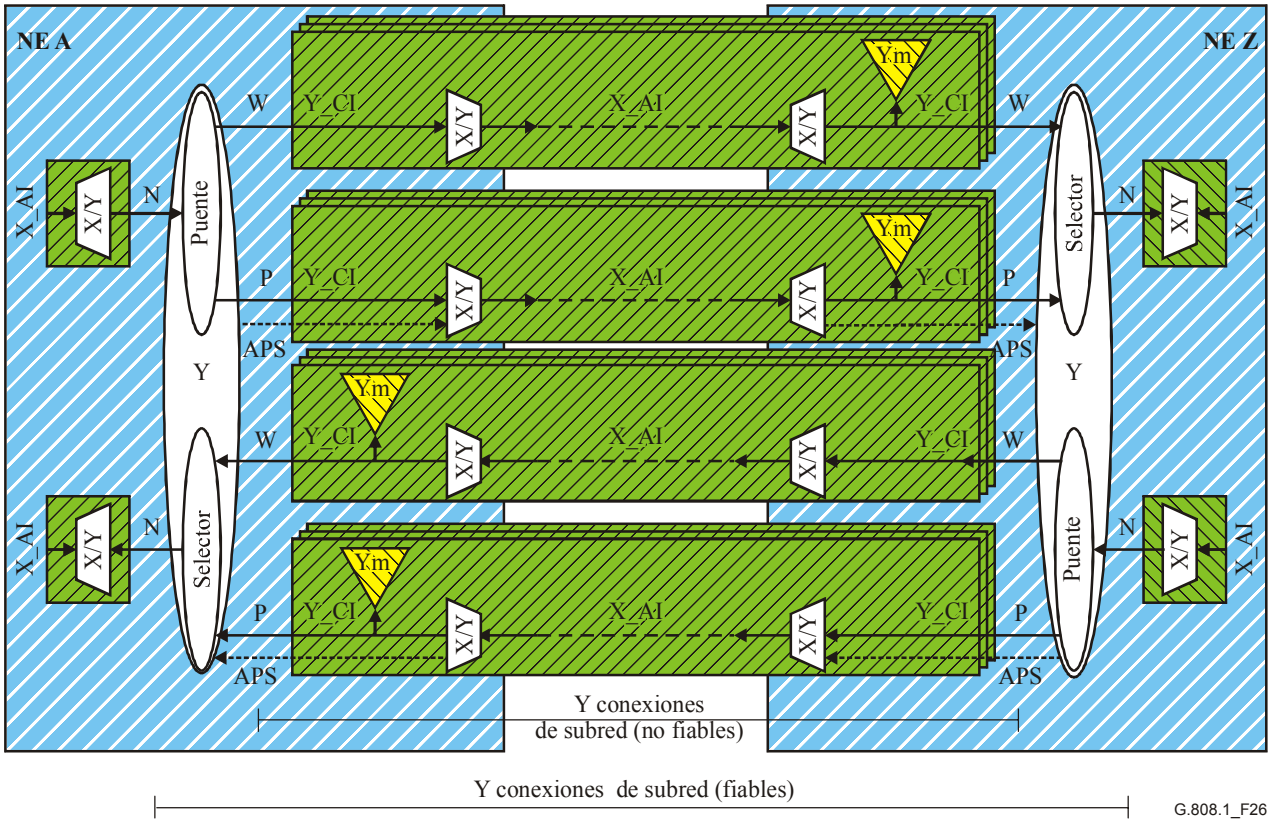
En la figura 12 se muestran detalles adicionales de estos procesos de función de conexión de protección. El proceso lógico SFG/SDG es específico de la protección de grupo. Este proceso "fusiona" las tres señales de fallo de señal de camino (TSF) individuales en un solo grupo SF (SFG) y las señales de degradación de señal de camino (TSD) individuales en un solo grupo SDG.

La lógica SFG/SDG SNC/S puede funcionar de distintos modos:

- W-SFG = W1-TSF o W2-TSF o W3-TSF
  P-SFG = P1-TSF o P2-TSF o P3-TSF
- W-SFG = W1-TSF
  P-SFG = P1-TSF
- W-SFG = X% de las señales Wi-TSF están activas
  P-SFG = X% de las señales Pi-TSF están activas
- igual a SDG.

11.2.2.2 Protección tipo SNC/N 1+1

En la figura 26 se ilustra el caso de protección SNC/N de grupo 1+1 entre los elementos de red A y Z. En este ejemplo, hay dos veces tres conexiones de subred paralelas independientes, que se comportan como grupos de entidades de transporte de servicio y de protección de las tres señales de tráfico normal (protegido). Las tres señales de tráfico normal paralelas en el grupo quedan protegidas conjuntamente por la función de conexión de capa. Las funciones NIM supervisan la información de tara/OAM extremo a extremo (SNC/Ne) o de subcapa (SNC/Ns) para determinar el estado de las entidades de transporte de servicio y de protección. La información APS se transporta por una de las SNC de protección, excepto en el caso de conmutación unidireccional 1+1.



NOTA – La señal APS no se aplica en el caso de conmutación unidireccional 1+1.

Figura 26/G.808.1 – Modelo funcional de protección SNC/Ne de grupo 1+1

En la figura 12 se muestran detalles adicionales de estos procesos de función de conexión de protección. El proceso lógico SFG/SDG es específico del grupo de protección SNC/N 1+1. Este proceso "fusiona" las tres señales de fallo de señal de camino (TSF) individuales en un solo grupo SF (SFG) y las tres señales de degradación de señal de camino (TSD) individuales en un solo SDG.

La lógica SFG/SDG SNC/N puede funcionar de distintos modos:

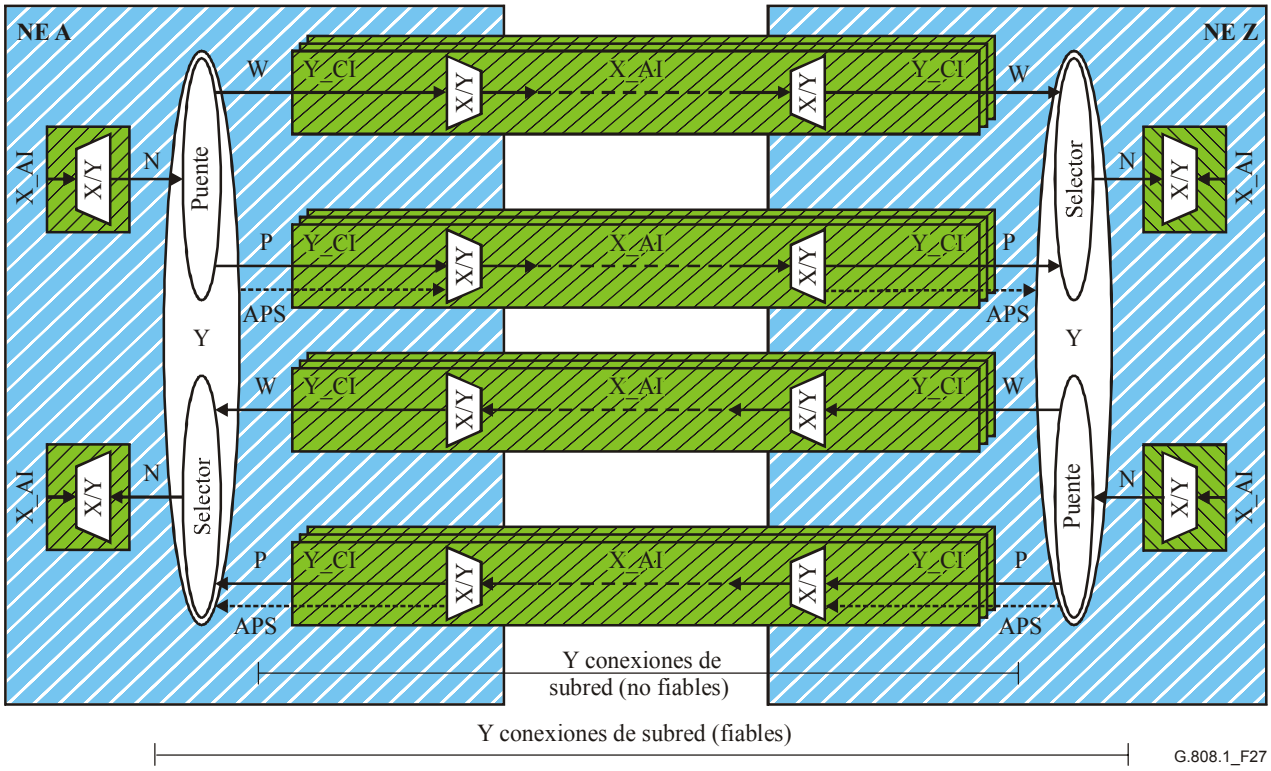
- W-SFG = (W1-TSF y no P1-TSF) o (W2-TSF y no P2-TSF) o (W3-TSF y no P3-TSF)
  P-SFG = (P1-TSF y no W1-TSF) o (P2-TSF y no W2-TSF) o (P3-TSF y no W3-TSF)
- W-SFG = (W1-TSF y no P1-TSF)
  P-SFG = (P1-TSF y no W1-TSF)
- W-SFG = X% de las señales (Wi-TSF y no Pi-TSF) están activas
  P-SFG = X% de las señales (Pi-TSF y no Wi-TSF) están activas
- igual a SDG.

En el caso de las señales VC-n SDH concatenadas virtuales (VC-n-Xv), las condiciones SF y SD de grupo deben declararse inmediatamente que sufre un fallo o degradación una de las X señales en el grupo.

- W-SFG = W1-TSF o W2-TSF o W3-TSF
  P-SFG = P1-TSF o P2-TSF o P3-TSF
- igual a SDG.

11.2.2.3 Protección SNC/I 1+1

En la figura 27 se ilustra el caso de protección SNC/I de grupo 1+1 entre los elementos de red A y Z. En este ejemplo, hay dos veces tres conexiones de subred paralelas independientes, que se comportan como grupos de entidades de transporte de servicio y de protección de las tres señales de tráfico normal (protegido). Las tres señales de tráfico normal paralelas en el grupo quedan protegidas conjuntamente por la función de conexión de capa. Las funciones de adaptación X/Y supervisan la información adaptada de capa servidora para detectar fallos de señal y determinar el estado de las entidades de transporte de servicio y de protección. La información APS se transporta por una de las SNC de protección, excepto en el caso de conmutación unidireccional 1+1.



NOTA – La señal APS no se aplica en el caso de conmutación unidireccional 1+1.

Figura 27/G.808.1 – Modelo funcional de protección SNC/I de grupo 1+1

En la figura 12 se muestran detalles adicionales de estos procesos de función de conexión de protección. El proceso lógico SFG es específico del grupo de protección SNC/I 1+1. Este proceso permite "fusionar" las tres señales de fallo de señal de servidor (SSF) individuales en un solo grupo SF (SFG).

La lógica SFG SNC/I puede funcionar de distintos modos:

- W-SFG = (W1-SSF y no P1-SSF) o (W2-SSF y no P2-SSF) o (W3-SSF y no P3-SSF)
  P-SFG = (P1-SSF y no W1-SSF) o (P2-SSF y no W2-SSF) o (P3-SSF y no W3-SSF)
- W-SFG = (W1-SSF y no P1-SSF)
  P-SFG = (P1-SSF y no W1-SSF)
- W-SFG = X% de las señales (Wi-SSF y no Pi-SSF) están activas
  P-SFG = X% de las señales (Pi-SSF y no Wi-SSF) están activas.

En el caso de las señales VC-n SDH concatenadas virtuales (VC-n-Xv), las condiciones SF y SD de grupo deben declararse inmediatamente que se detecte un fallo o degradación de una de las X señales en el grupo.

- W-SFG = W1-SSF o W2-SSF o W3-SSF
  P-SFG = P1-SSF o P2-SSF o P3-SSF
- igual a SDG.

11.2.2.4 Protección tipo SNC/T

Como resultado del gran número de intervalos de tiempo tributarios de algunas tecnologías de transmisión (por ejemplo, ATM) podrán asignarse intervalos de tiempo tributarios adicionales a las señales de capa servidora de servicio y de protección para transportar señales de prueba por las entidades de transporte de prueba (figuras 28, 30). Estas señales de prueba (una para servicio, una para protección) pueden emplearse en lugar de la información SFG, SDG como se describió anteriormente. La señal APS se transporta por la entidad de transporte de protección.

La lógica SFG/SDG funciona ahora de la siguiente manera:

- W-SFG = Wt-TSF
  P-SFG = Pt-TSF
- W-SDG = Wt-TSD
  P-SDG = Pt-TSD

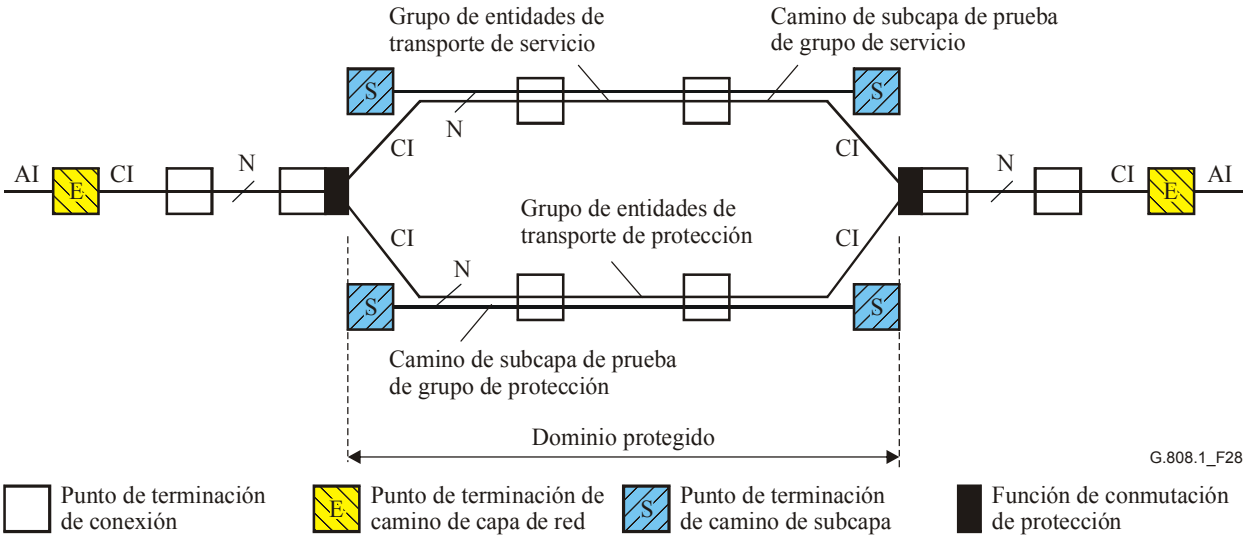


Figura 28/G.808.1 – Protección de grupo SNC/Ts 1:1 ó 1+1 utilizando terminaciones de camino de subcapa

La protección SNC/T de grupo también puede utilizar información de tara/OAM extremo a extremo para crear un camino de red de capa extremo a extremo como un camino de prueba (figura 29). Por lo general, los diseños de los equipos permiten ubicar esas funciones de terminación de capa en las unidades de puertos en el "otro lado" de la función de conexión; es decir, no están disponibles inmediatamente para fines de camino de prueba de protección de grupo.

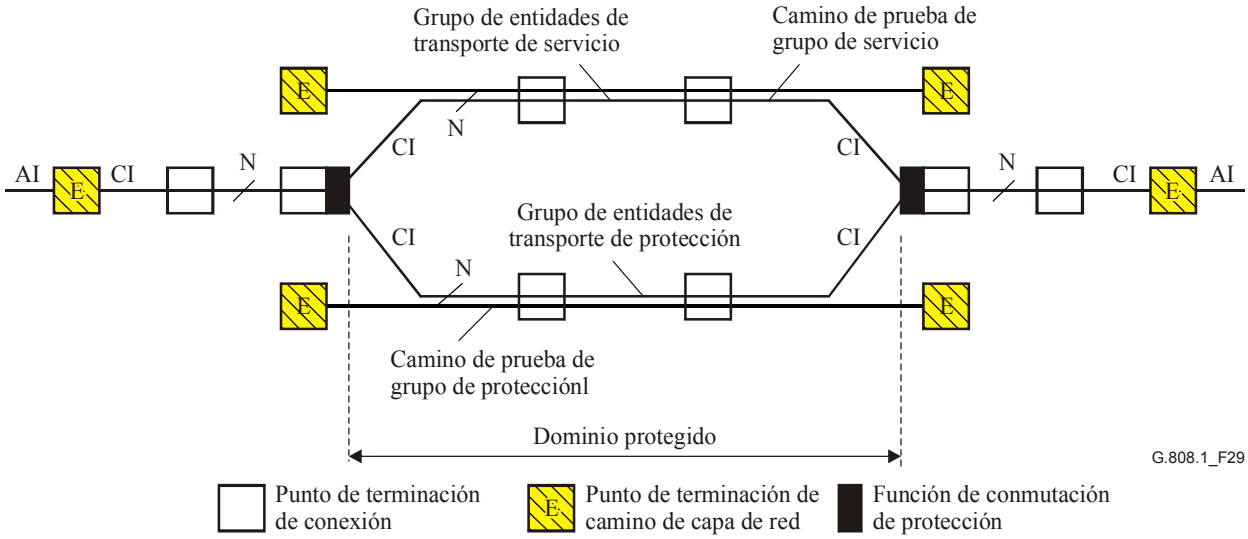
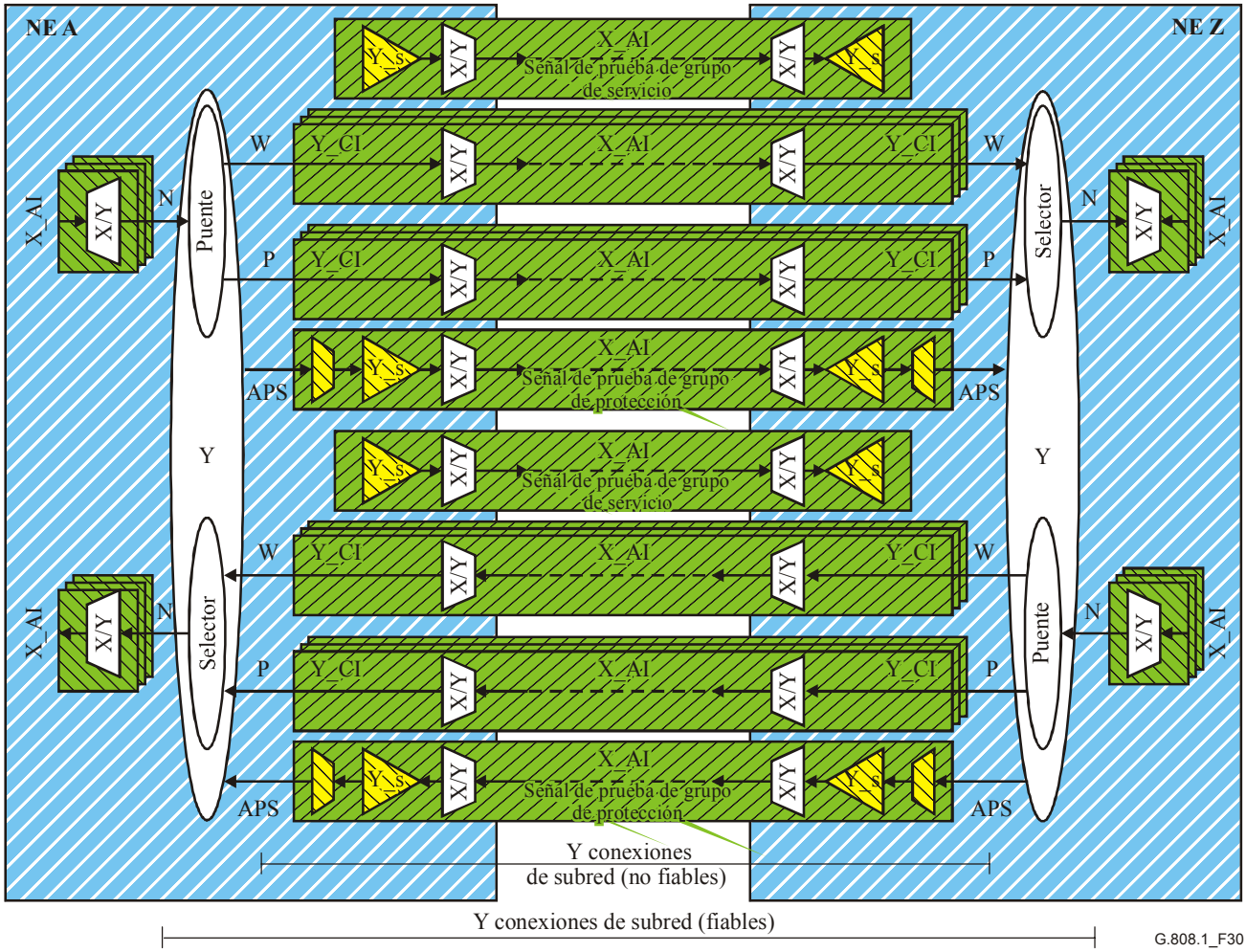


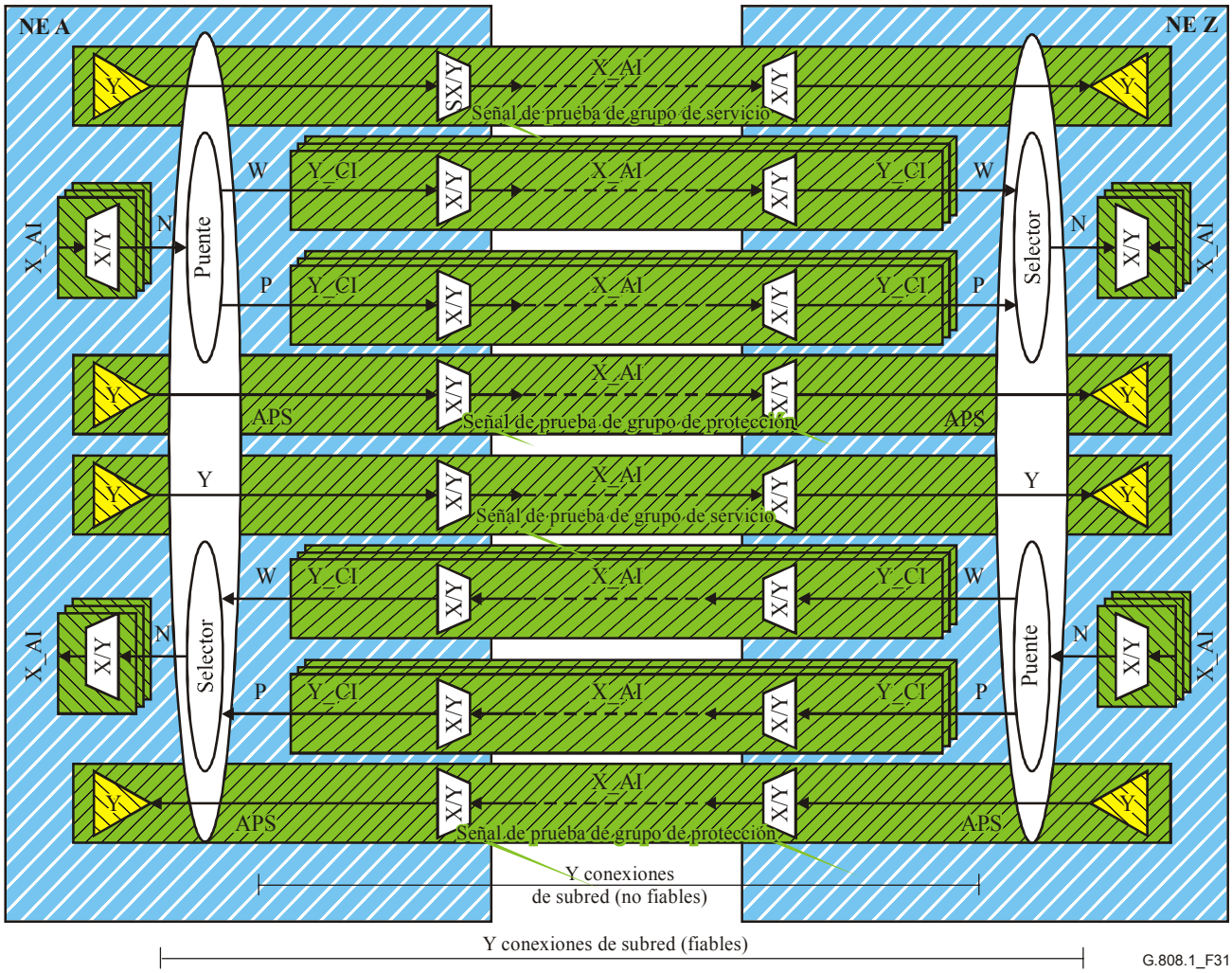
Figura 29/G.808.1 – Protección de grupo SNC/Te 1:1 ó 1+1 utilizando terminaciones de camino de red de capa



NOTA – La señal APS no se aplica al caso con conmutación unidireccional 1+1.

Figura 30/G.808.1 – Modelo funcional de protección SNC/Ts de grupo 1+1/1:1 que emplea terminaciones de camino de subcapa

NOTA – En el caso de ATM, el camino de prueba (subcapa) debe incluir una señal de prueba que tenga activada la comprobación de continuidad (CC). Si CC estuviese inactiva, ese camino de prueba (subcapa) no transportaría ninguna información en caso de condiciones normales sin fallos. Cuando se produce un fallo, se insertan células AIS. Cuando el fallo aparece solamente por un corto periodo de tiempo (por ejemplo, debido a una "medida de protección de capa física"), el detector de defectos AIS en el punto extremo del camino de prueba (subcapa) detectará la condición de defecto AIS durante 2 a 3 s conforme a la definición de estado AIS en la Rec. UIT-T I.610. Cuando CC está activada, la condición de defecto AIS se despejará con la recepción de una célula CC, es decir, dentro de un periodo de un segundo después de que se despejó la interrupción de tráfico.



NOTA – La señal APS no se aplica al caso con conmutación unidireccional 1+1.

Figura 31/G.808.1 – Modelo funcional de protección SNC/Te de grupo 1+1/1:1 utilizando terminaciones de camino de red de capa

12 Capacidad de supervivencia ofrecida por el método LCAS

El método de ajuste de capacidad de enlace (LCAS) permite adaptarse a los fallos de red. Se utiliza para ofrecer capacidad de supervivencia a un camino VC-n-Xv (a lo largo de toda una red de operador o de múltiples redes de operador). Se trata de una arquitectura de supervivencia extremo a extremo dedicada, que puede utilizarse en distintas estructuras de red; redes en malla, anillos, y otras. Como la capacidad de supervivencia LCAS es un mecanismo de supervivencia dedicado, no hay limitaciones fundamentales con relación al número de elementos de red dentro de los caminos.

El método LCAS funciona en todas las combinaciones de arquitecturas, conmutación y funcionamiento de protección.

Por lo general, el método LCAS protege contra fallos en la capa servidora y fallos de conectividad y degradaciones de calidad de funcionamiento en la capa cliente.

En el caso del método LCAS, se protege la información adaptada (AI) (es decir, la cabida útil total de la información característica (CI) individual de la capa de red). Véase la figura 32.

La adaptación consiste en suprimir la carga útil fraccional transportada por cualquier miembro del grupo de concatenación virtual (VCG) que se vea afectado por una condición de fallo en la entidad de transporte. El resultado es un tamaño de carga útil AI reducido.

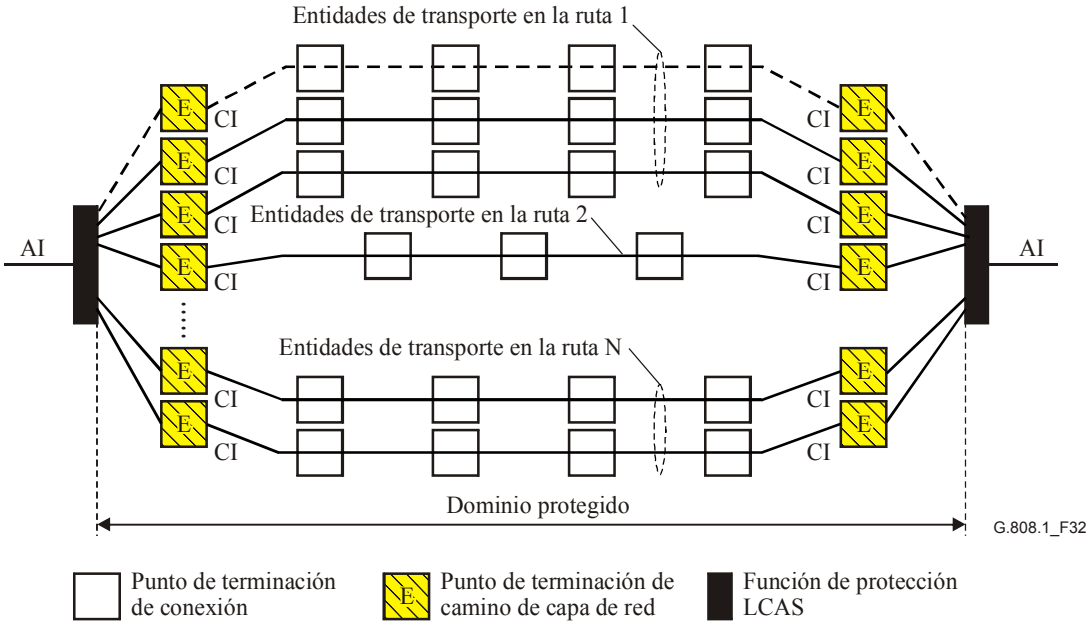


Figura 32/G.808.1 – Concepto genérico de la capacidad de supervivencia ofrecida por el método LCAS

La información AI se transporta utilizando un grupo concatenado virtual (VCG) con X miembros (VC_n_Xv, ODUk_Xv), distribuidos por N rutas, donde:

- N = número de rutas ($1 \leq N \leq X$) donde cada una incluye una o más conexiones de red dentro del VCG.
- X = número de miembros en el VCG necesarios para transportar la información AI de ancho de banda del cliente + capacidad adicional/protección Z ($X \geq 1$, $Z \geq 0$).
- X_{ACT} = cabida útil transportada real ($0 \leq X_{ACT} \leq X$); debido al fallo de uno o más de los caminos el ancho de banda de uno o más miembros en el VCG no se utilizará para transportar la información AI.

El método LCAS es independiente de la protección en las capas servidoras.

12.1 Modelo funcional LCAS

En la figura 33 se ilustra el caso de la utilización del método LCAS para el transporte entre los elementos de red A y Z. Se emplean múltiples caminos independientes (en la red de capa Y) como entidades de transporte para la señal de tráfico normal (cabida útil) Z_CI. Las X funciones Y_TT generan/insertan y supervisan/extraen la información de tara extremo a extremo para determinar el estado de las entidades de transporte individuales. Las funciones de concatenación virtual Y-Xv/Y-X-L_A generan/insertan y supervisan/extraen la concatenación virtual extremo a extremo y la información de tara LCAS para determinar y alinear el estado de los miembros en el VCG.

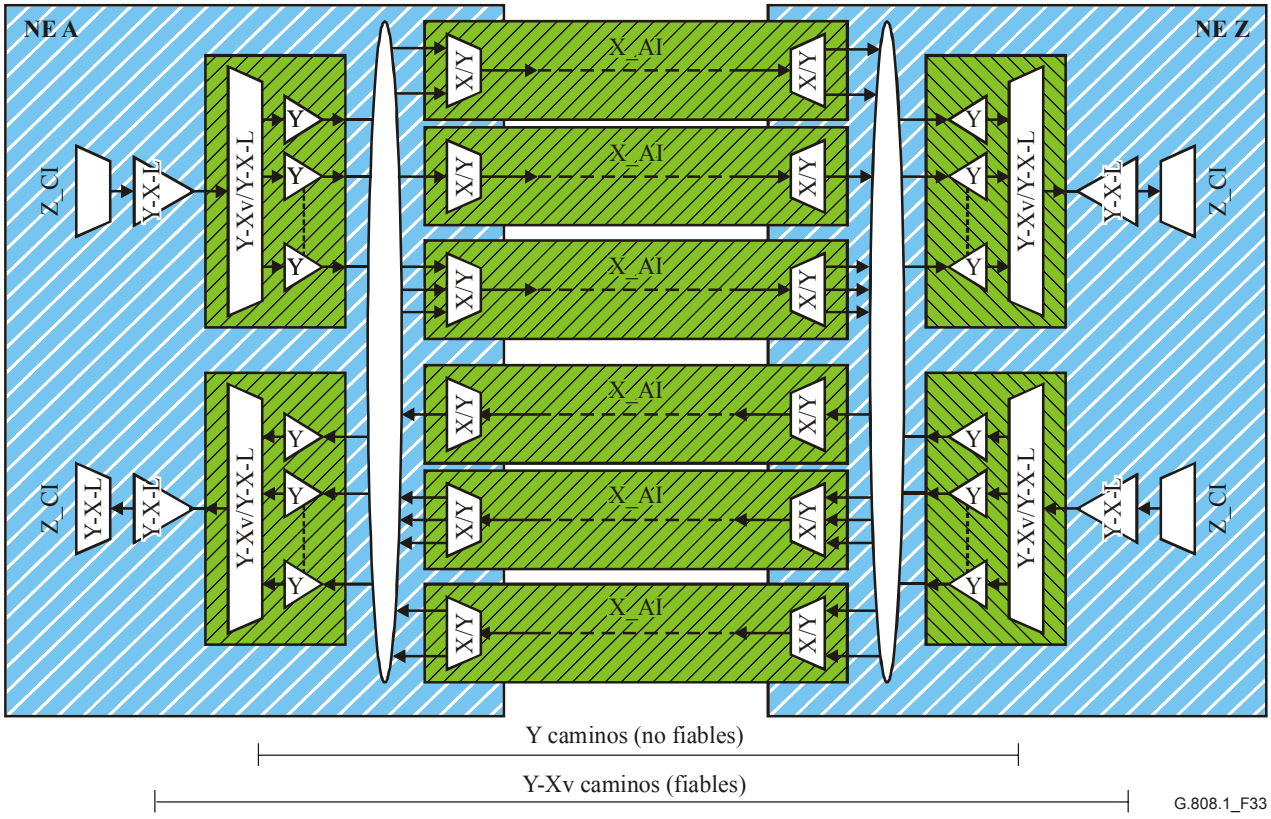


Figura 33/G.808.1 – Modelo funcional LCAS

Las funciones de concatenación virtual Y-Xv/Y-X-L_A distribuyen/recogen la cabida útil transportada utilizando los X_{ACT} caminos Y de red de capa disponibles de los X caminos Y de red de capa previstos.

Ejemplo – Para transportar una señal de 10 Mbit/s se necesita VC-12-5v. En este VCG se establecen cinco caminos VC-12, de los cuales dos se encaminan por la ruta uno y tres por la ruta dos (figura 34). En este caso el ancho de banda de supervivencia es 2 x VC-12 ó 40% y el ancho de banda sin supervivencia es 3 x VC-12 ó 60%. Si se hubiese previsto un camino VC-12 adicional (Z = 1) encaminado por la ruta uno, el ancho de banda de supervivencia habría sido 3 x VC-12 ó 60% y el ancho de banda sin protección de 2 x VC-12 ó 40%.

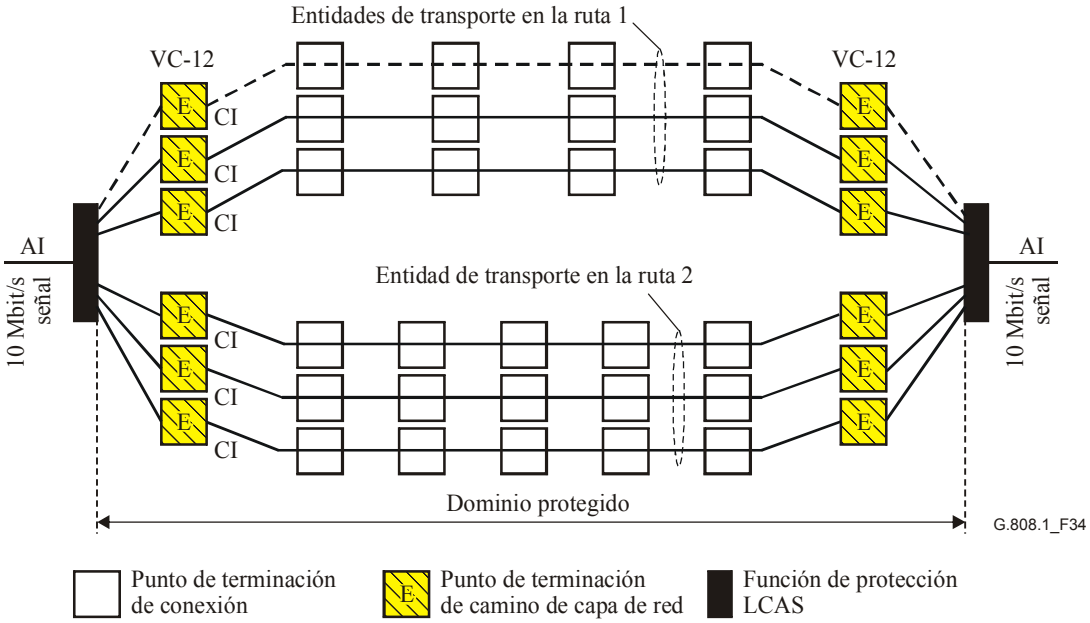


Figura 34/G.808.1 – Ejemplo de capacidad de supervivencia LCAS para una señal de 10 Mbit/s por VC-12-(X+Z)v (X=5, Z=0,1)

13 Calidad de funcionamiento de la conmutación de protección

En la figura 35 se ilustra el modelo temporal de conmutación de protección deducido de la Rec. UIT-T M.495. Los parámetros del modelo se definen de la siguiente manera.

13.1 tiempo de detección, T_1: Intervalo de tiempo comprendido entre la aparición de una degradación de red y la detección de una condición de fallo de señal (SF) o de degradación de señal (SD) activada por dicha degradación.

13.2 tiempo de retención, T_2: Intervalo de tiempo después de la detección de una condición SF o SD y su confirmación como una condición que necesita el procedimiento de conmutación de protección.

NOTA – En la Rec. UIT-T M.495 se describe el tiempo T_2 como "tiempo de espera".

13.3 tiempo de las operaciones de conmutación de protección, T_3: Intervalo de tiempo comprendido entre la confirmación de una condición SF o SD y la conclusión del procesamiento y la transmisión de las señales de control necesarias para efectuar la conmutación de protección.

13.4 tiempo de transferencia de la conmutación de protección, T_4: Intervalo de tiempo comprendido entre la conclusión del procesamiento y la transmisión de las señales de control necesarias para efectuar la conmutación de protección y la conclusión de las operaciones de conmutación de protección.

13.5 tiempo de recuperación, T_5: Intervalo de tiempo comprendido entre la conclusión de las operaciones de conmutación de protección y el restablecimiento total del tráfico protegido.

NOTA – Esto podrá incluir la verificación de las operaciones de conmutación, la resincronización de la transmisión digital, etc.

13.6 tiempo de confirmación, T_c: Tiempo comprendido entre la aparición de la degradación de red y el instante en el que se confirma la activación de la condición SF o SD para solicitar las operaciones de conmutación de protección:

$$T_c = T_1 + T_2.$$

13.7 tiempo de transferencia, T_t: Intervalo de tiempo después de la confirmación de que una condición SF o SD necesita las operaciones de conmutación de protección y la terminación de las mismas:

$$T_t = T_3 + T_4.$$

13.8 tiempo de restablecimiento del tráfico protegido, T_r: Tiempo comprendido entre la aparición de la degradación en la red y el restablecimiento del tráfico protegido:

$$T_r = T_1 + T_2 + T_3 + T_4 + T_5 = T_c + T_t + T_5.$$

NOTA – Un equipo podría detectar una degradación de red aparente que no se confirma después de las operaciones de confirmación. En este caso, sólo los tiempos T_1 y T_2 son pertinentes.

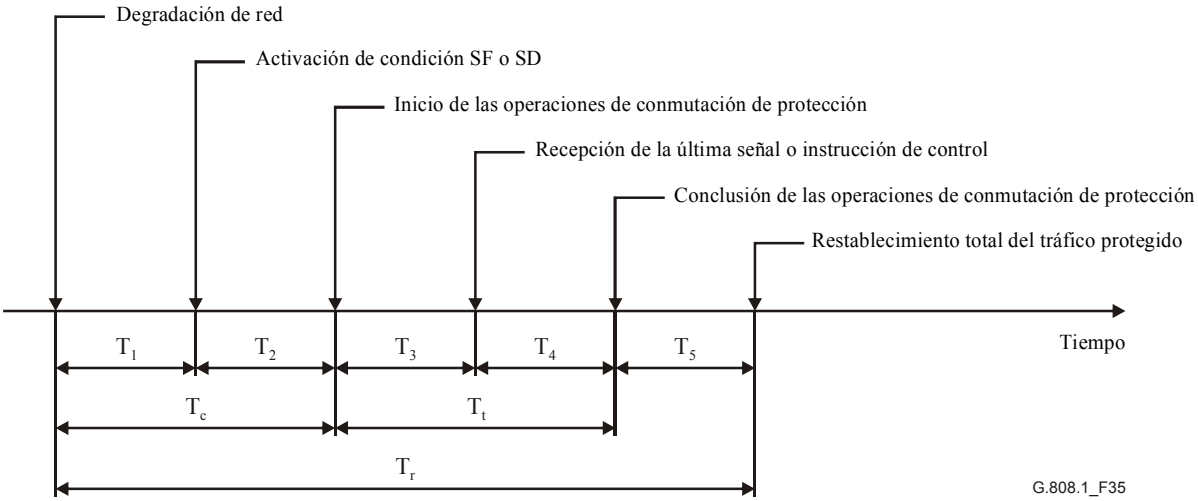


Figura 35/G.808.1 – Modelo temporal de conmutación de protección

14 Temporizador de retención

El objetivo de los temporizadores de retención es funcionar cuando una señal está protegida por medio de protección anidada. Estos temporizadores permiten que un grupo de protección interna restablezca el tráfico antes de que el grupo de protección externa intente hacerlo, a fin de limitar el número de acciones de conmutación.

Los temporizadores de retención se aplican también con los tipos de protección SNC/N 1+1 y SNC/I para evitar una conmutación demasiado prematura debido a la diferencia de retardo diferencial entre la ruta corta y la larga.

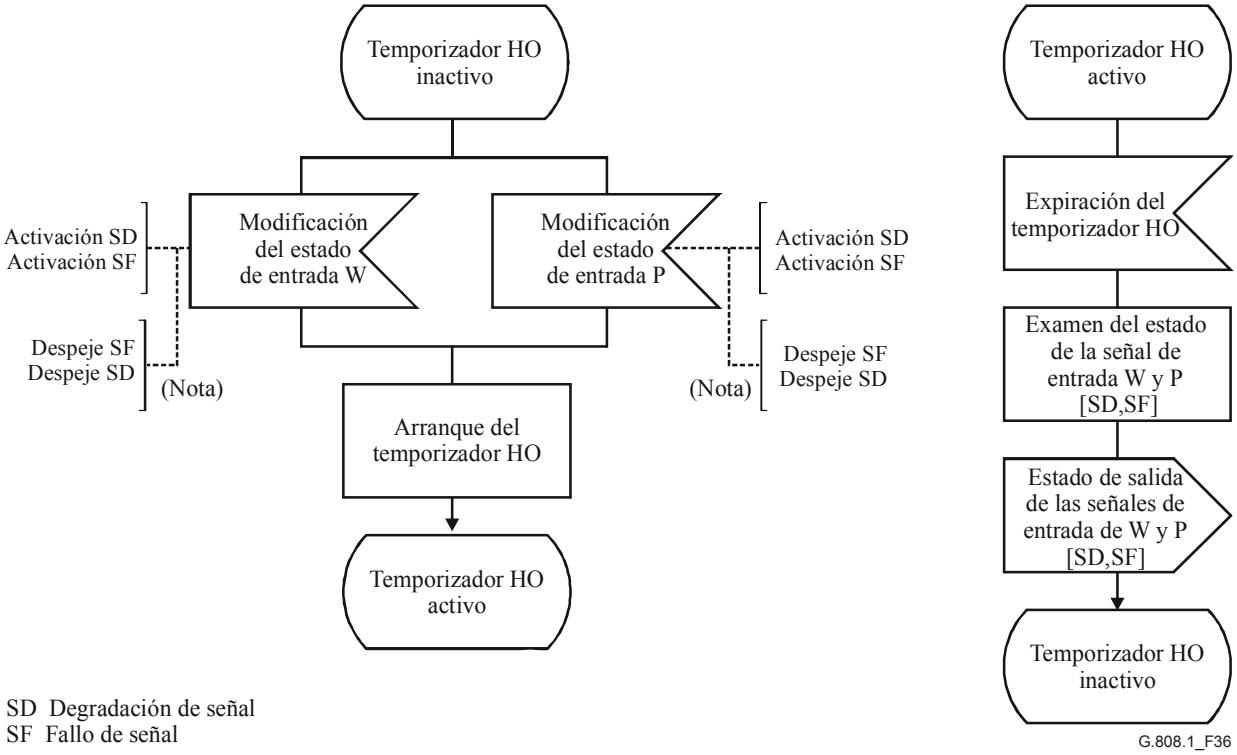
Cada selector de protección puede tener un temporizador de retención.

Se pone en funcionamiento un temporizador de retención cuando se activan una o más condiciones SF o SD en el grupo de protección y funciona durante un periodo de tiempo sin reiniciación que puede ajustarse de 0 a 10 s en pasos de X ms. X es 100 ms (SDH, OTN) y 500 ms (ATM).

Durante este periodo, los estados de condición SF/SD modificados no pasan al proceso de conmutación de protección.

Cuando el temporizador expira, el estado de la condición SF/SD de todas las señales se examina y se pasa al proceso de conmutación de protección. Este proceso reaccionará con el nuevo estado de condición SF/SD en este instante.

NOTA – No es necesario que esté presente una condición SF/SD durante todo el periodo de retención, sólo es importante el estado cuando expira el temporizador correspondiente. Además, tampoco es necesario que la condición SF/SD que activa el temporizador de retención sea la misma que la correspondiente cuando concluye el periodo de retención.



NOTA – No es obligatoria la utilización de eventos de despeje de la condición SF/SD como activadores del arranque del temporizador de retención, pero se recomienda para evitar conmutaciones de protección innecesarias que de lo contrario podrían producirse bajo ciertas circunstancias.

Figura 36/G.808.1 – Funcionamiento del temporizador de retención

15 Temporizador en espera de restablecimiento

En el modo de funcionamiento reversivo, para evitar la operación frecuente del conmutador de protección debido a un defecto intermitente (por ejemplo, fluctuación de BER con respecto al umbral de SD), una entidad de transporte de servicio fallida debe convertirse en una entidad libre de fallos (por ejemplo, proporción de bits erróneos (BER, *bit error ratio*) menor que un umbral de restablecimiento). Después de que una entidad de transporte de servicio fallida cumple con ese criterio, debe pasar un periodo de tiempo fijo antes de que una señal de tráfico normal la utilice nuevamente. Este periodo, denominado periodo de espera de restablecimiento (WTR), es del orden de 5 a 12 minutos y es necesario que se pueda ajustar. Una condición SF o SD anulará el periodo WTR.

En modo de funcionamiento reversivo, cuando ya no se solicita la protección, es decir, la entidad de transporte de servicio fallida ya no está en condición SD o SF (y suponiendo que no haya otras entidades de transporte solicitantes), se activará un estado de espera de restablecimiento local. Ya que este estado se vuelve el que tiene la prioridad más elevada, se indica en la señal APS (cuando proceda), y se mantiene la señal de tráfico normal de la entidad de transporte de servicio fallida anterior en la entidad de transporte de protección. Este estado llegará a un fin de temporización normal y se convertirá en una señal nula sin petición (o en una señal de tráfico adicional sin petición, cuando proceda). El temporizador de retención de restablecimiento se desactiva antes cuando cualquier petición con prioridad superior toma el lugar de este estado.

16 Señal de conmutación de protección automática (APS)

Se utiliza una señal APS para sincronizar las acciones de los extremos A y Z del dominio protegido. Se comunica lo siguiente:

– tipos de petición/estado;

– señal solicitada;

– señal puenteada;

– configuración de protección.

La información de tipo de petición/estado permite identificar la condición de fallo, instrucción externa o estado de proceso de protección con la prioridad más alta.

Cuando la información de señal deseada y puenteada se transporta en un campo de n bits permite identificar:

0 señal nula,

1.. 2^n–2 señal de tráfico normal 1 a 2^n–2,

2^n–1 señal de tráfico adicional.

La información de configuración de protección permite identificar:

– utilización de un canal APS;

– arquitectura de protección (1+1, 1:n);

– tipo de conmutación (unidireccional, bidireccional);

– tipo de funcionamiento (no reversivo, reversivo).

La señal APS se transporta por el canal APS. En principio, es posible asignar un canal APS a cada entidad de transporte. Si bien, la asignación de este tipo de canal a una entidad de transporte de servicio no proporcionará suficiente capacidad de supervivencia; es decir, si la entidad de transporte de servicio sufre un fallo, también fallará la comunicación entre los dos puntos extremos y no será posible aplicar la protección. Por consiguiente, el canal APS se atribuye a una o más entidades de transporte de protección.

17 Tráfico no protegido ininterrumpible (NUT)

El tráfico no protegido ininterrumpible es una de las tres clases de tráfico que hay en los métodos de protección (1:1) y $(1:1)^n$, mientras que las otras dos son el tráfico protegido y el adicional (3.18.3). El tráfico NUT no cuenta con protección asociada, pero no puede descartarse de la red para facilitar la protección de otro tipo de tráfico.

Con las arquitecturas (1:1) o $(1:1)^n$, el acceso de canal de tráfico adicional o de protección permite la utilización de las entidades de protección para el tráfico adicional durante el funcionamiento normal. Cuando se produce una conmutación de protección, este tráfico se descarta. El tráfico adicional permite un servicio más económico que el tráfico protegido o el tráfico no protegido ininterrumpible. No está relacionado con el tráfico protegido proveniente de un cliente distinto y puede utilizarse por ejemplo para proporcionar capacidad adicional en respuesta a un evento importante.

18 Entidad de tráfico adicional (protección) transporte información de tara/OAM

En el caso de protección SNC/S $(1:1)^n$ con tráfico adicional, la entidad de transporte (protección) de tráfico adicional no necesita la adición de una terminación de camino de subcapa. La entidad de transporte (protección) de tráfico adicional tiene un intervalo de tiempo tributario dedicado dentro de la señal agregada, independiente de los intervalos de tiempo tributarios de las entidades de transporte de protección que se utilizan para transportar una señal de tráfico normal.

El estado de la entidad de transporte (protección) de tráfico adicional no afecta al funcionamiento de la conmutación de protección, y por consiguiente no se necesita para supervisar esta entidad de transporte.

19 Instrucciones externas

El comportamiento autónomo del proceso de conmutación de protección en condiciones de fallo de sus entidades de transporte puede modificarse mediante instrucciones (de conmutación) externas, es decir, a través de una instrucción (conmutación) externa que emita una petición externa adecuada acerca del proceso de protección.

NOTA – Sólo puede emitirse una instrucción (conmutación) externa por grupo de protección. Se descartan las instrucciones externas que pueden ser desplazadas o anuladas por otras condiciones, estados o peticiones con prioridad más elevada.

Se definen instrucciones externas para facilitar los siguientes tipos de acciones (véanse en 3.3.8) las definiciones exactas de las instrucciones externas):

1) Modificaciones y mantenimiento de la configuración que se debe realizar en el grupo de protección o en sus entidades de transporte:
   - **la exclusión de protección** inhabilita temporalmente el acceso de todas las señales a la entidad de transporte de protección;
   - **la conmutación forzada de la señal #i** obliga temporalmente a encaminar la señal #i por la entidad de transporte de protección;
   - **la conmutación manual de la señal #i** encamina temporalmente la señal #i por la entidad de transporte de protección, a menos que una condición de fallo (SF, SD) solicite que otra señal se encamine por esta entidad de transporte.
2) Señales de exclusión del proceso de protección:
   - **la exclusión de la señal #i** inhabilita temporalmente el acceso de la señal específica a la entidad de transporte de protección;
   - **despeje de la exclusión de la señal #i**.
3) Congelación del proceso de protección:
   - **la congelación** temporal impide la realización de cualquier acción de conmutación, y por consecuencia congela el estado actual. Hasta que se despeje la congelación, se rechazan instrucciones externas de extremo cercano adicionales y se ignoran las modificaciones de condición de fallo y los mensajes APS que se reciben;
   - **despeje de congelación** cuando se despeja la instrucción de congelación, se recalcula el estado del grupo de protección basándose en las condiciones de fallo y en el mensaje APS recibido.
4) Prueba del proceso de protección y del canal APS entre los dos puntos extremos:
   - **ejercicio**, emula una petición de conmutación sin llevar a cabo la acción real correspondiente, a menos que se esté utilizando la entidad de transporte de protección.
5) Despeje de la instrucción (conmutación) externa anterior:
   - **despeje**, libera todas las instrucciones de conmutación.

20 Estados del proceso de conmutación de protección

Se dispone de los siguientes procesos de conmutación de protección:

Señal de tráfico normal #i sin reversión (DNR, *do not revert normal traffic signal* #i) – En el modo de funcionamiento no reversivo, se utiliza para mantener la selección de una señal de tráfico normal de la entidad de transporte de protección.

Ninguna petición (NR, *no request*) – Todas las señales de tráfico normal se seleccionan de sus entidades de transporte de servicio correspondientes. En un grupo de protección 1+1, la entidad de transporte de protección conduce la señal nula, el tráfico adicional o bien un puente de la señal de tráfico normal simple.

Espera de restablecimiento de la señal de tráfico normal #i (WtR, *wait to restore normal traffic signal* #i) – En el modo de funcionamiento reversivo, después de liberar una indicación SF o SD en la entidad de transporte de servicio #i, mantiene la señal de tráfico normal #i seleccionada de la entidad de transporte de protección hasta que expira el temporizador de retención de restablecimiento. Si el temporizador expira antes de cualquier otro evento o instrucción, el estado cambia a NR. Se utiliza para evitar el funcionamiento frecuente del selector en el caso de fallos intermitentes.

21 Prioridad

Se definen condiciones de fallo, instrucciones externas y estados de protección de tal manera que haya una prioridad relativa entre ellos. Se aplica prioridad a estas condiciones/instrucciones/estados localmente en cada punto extremo y entre los dos puntos extremos.

Véanse las Recomendaciones de conmutación de protección específicas para estas prioridades.

22 Condiciones de activación de SF y SD

Una condición SF es un TSF o un SSF, en función del tipo de protección.

En la figura 37 se ilustran las reglas de combinación de defectos. La condición SSF está dada por los defectos específicos de la función de adaptación y por AI_TSF. La condición TSF está dada por cualquier defecto del camino de red de capa y por CI_SSF.

Una condición de activación de SF se detecta directamente mediante la función de terminación de camino de la red de capa protegida o bien se pasa a través de una o más capas conforme a las reglas de combinación de los defectos específicos, CI_SSF y AI_TSF.

TSD es la única condición de activación de SD. Ésta se emite cuando se detecta dDEG. La condición TSD siempre es local para una función de terminación de camino, es decir, no pasa a través de fronteras de capa.

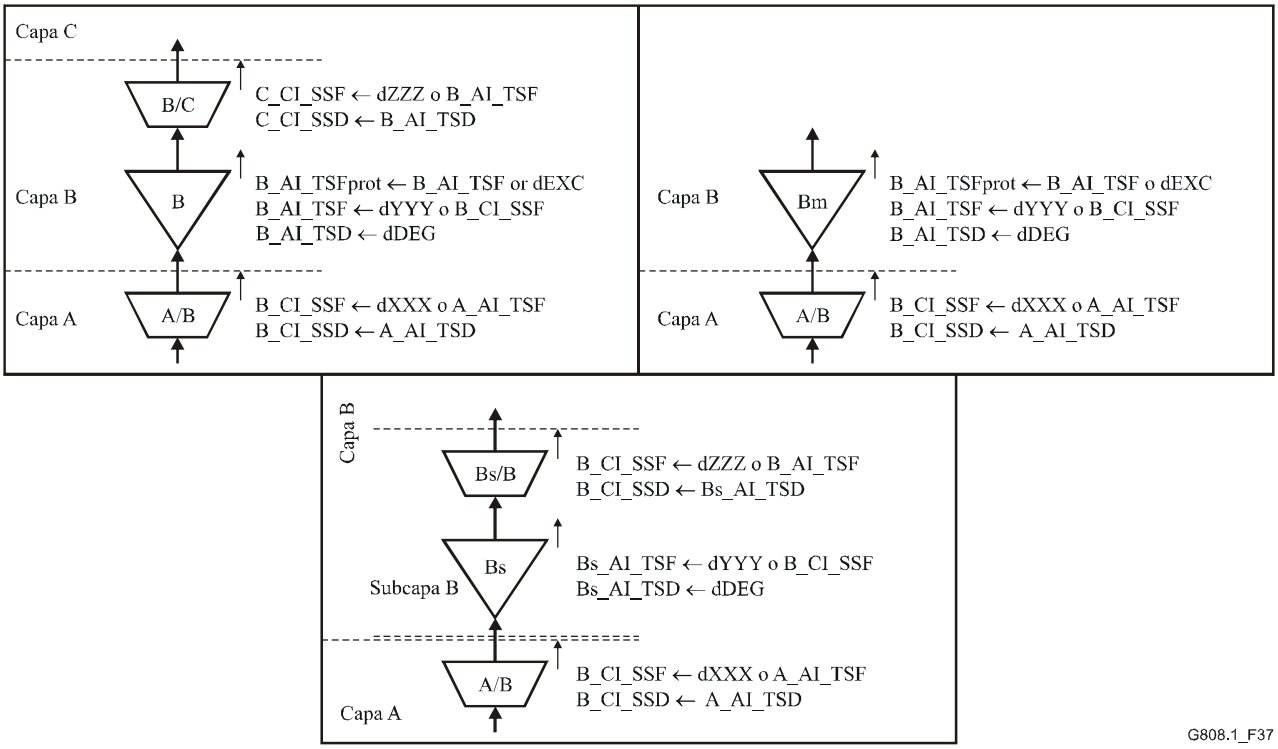


Figura 37/G.808.1 – Reglas de combinación de defectos

22.1 Visión general de las condiciones SF

En el cuadro 2 se presenta una síntesis de los defectos que contribuyen a las condiciones SF en diversas tecnologías de transmisión. Véanse las Recomendaciones de equipos (por ejemplo, Recomendaciones UIT-T G.783, G.798, I.732) por lo que se refiere a las especificaciones SF particulares.

Cuadro 2/G.808.1 – Síntesis de los defectos que contribuyen a la condición SF

	ATM	OTN	SDH
Defectos de continuidad	LOC	LOS, LOS-P, LCK, LTC	LOS, LTC
Defectos de conectividad	Ninguno	TIM, OCI	TIM, UNEQ
Defectos de adaptación	LCD	MSIM, LOM, PLM, LOFLOM	LOF, LOM, LOP, PLM
Defectos de capa servidora en sentido ascendente (nota 1)	AIS	FDI, FDI-P	AIS
Camino con muchos errores			EXC (nota 2)
Defectos de concatenación virtual (nota 3)		LOM, LOA	LOM, LOA
NOTA 1 – La detección de cualquier defecto provoca la generación de una señal de capa cliente AIS/FDI que se transporta en sentido descendente. En función de la capa específica, se puede detectar la señal AIS/FDI en una adaptación o en una función de destino de terminación de camino. NOTA 2 – EXC no contribuye a la condición TSF y, por consecuencia, se trata sólo de una condición de activación local de la red de capa protegida (a través de TSFprot) y no de alguna capa cliente. NOTA 3 – Los defectos de concatenación virtual se aplican únicamente en el caso del método LCAS.			

22.2 Visión general de las condiciones SD

En el cuadro 3 se presenta una síntesis de los defectos que contribuyen a las condiciones SD en diversas tecnologías de transmisión. Véanse las Recomendaciones de equipos (por ejemplo, Recomendaciones UIT-T G.783, G.798) por lo que se refiere a las especificaciones SD particulares.

Cuadro 3/G.808.1 – Síntesis de los defectos que contribuyen a la condición SD

	ATM	OTN	SDH
Degradaciones digitales	Ninguna	DEG	DEG
Degradaciones ópticas	No se aplica	En estudio (nota)	Ninguna
NOTA – Los umbrales para las degradaciones ópticas quedan en estudio. Además, queda en estudio determinar si los defectos de la señal de tara OTM (OOS, *OTM overhead signal*) contribuyen a la condición SD o no, ya que aún no se ha especificado OOS.			

23 Asignación de servicio y de protección

La conmutación de protección lineal 1+1 puede utilizarse como una aplicación de protección en un anillo físico. Como a menudo el anillo es parte de una red más grande y sólo una porción del camino atraviesa el anillo, por lo general, esa aplicación se utiliza para entidades de transporte de conexión de subred.

El tráfico bidireccional puede configurarse de dos maneras:

- Las entidades de transporte de servicio de ambos sentidos pueden seguir **distintos** trayectos físicos, y puede utilizarse todo el anillo. Eso se denomina anillo de conmutación de trayecto unidireccional (UPSR, *unidirectional path switch ring*) y se muestra en la figura 38. Se define en la red óptica síncrona (SONET, *synchronous optical network*) y por lo general, puede utilizarse en las arquitecturas SNC/I, SNC/N. No obstante, no debería utilizarse en las arquitecturas SNC/S y en las de protección de camino.

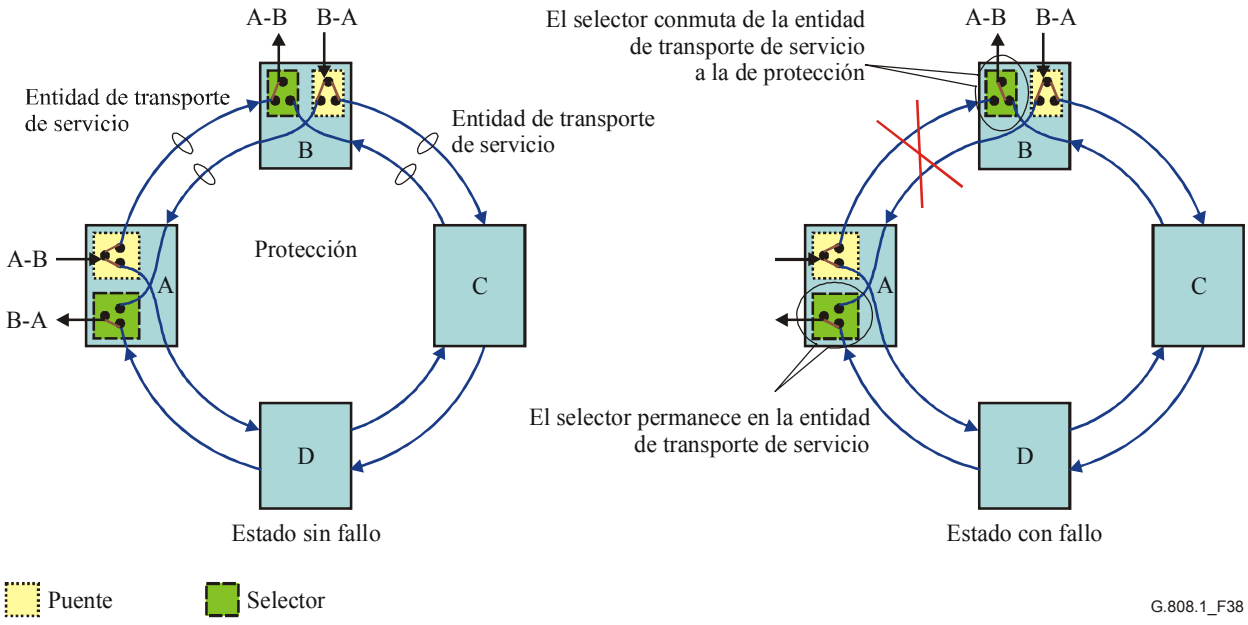


Figura 38/G.808.1 – Anillo de conmutación de trayecto unidireccional (UPSR)

- Las entidades de transporte de servicio en ambos sentidos siguen el **mismo** trayecto físico, que normalmente es el más corto. Las entidades de transporte de protección utilizarán el otro tramo del anillo. Esto se muestra en la figura 39 y se denomina protección de conexión de subred (SNCP). En una situación libre de fallos, esta aplicación permite reducir el tiempo de transferencia que es el mismo en ambos sentidos. Esta aplicación se define en SDH, OTN y ATM, y puede emplearse en todas las arquitecturas de protección. Los anillos con conmutación de trayecto unidireccional pueden funcionar también en este modo.

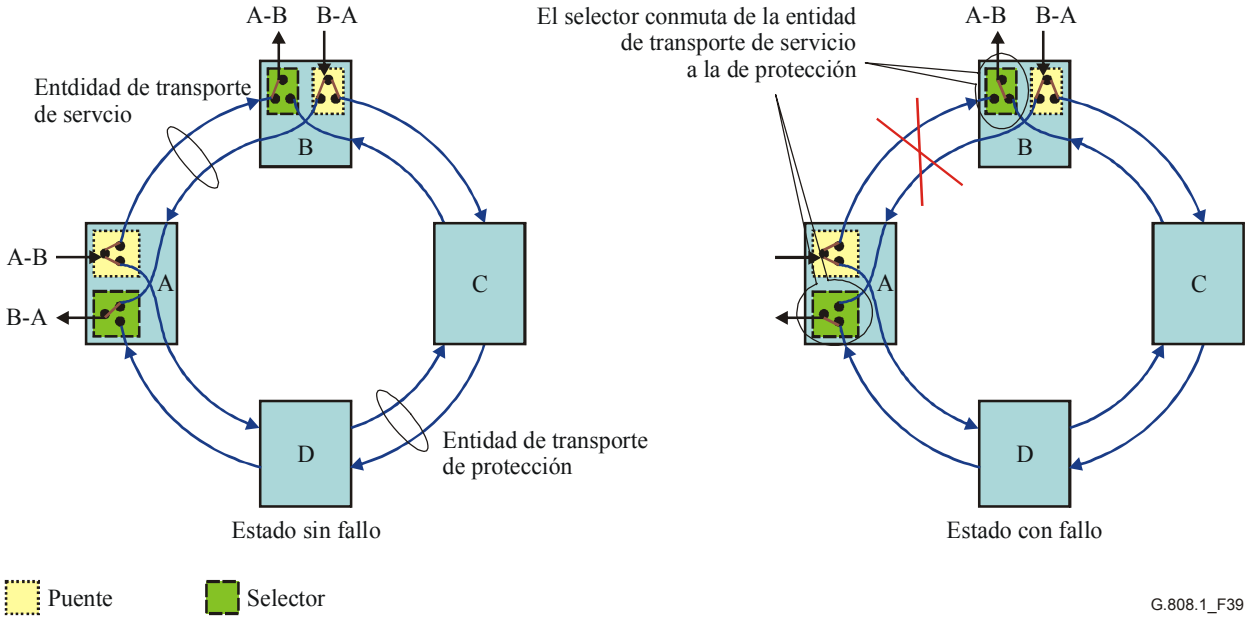


Figura 39/G.808.1 – Anillo de protección de conexión de subred (SNCP)

24 Protocolo APS

En la cláusula 3.3.2 se dan las definiciones genéricas de los tipos de protocolo APS. En esta cláusula se abordan las características de comportamiento de los protocolos y su posibilidad de aplicación a las distintas arquitecturas de protección que se definen en la presente Recomendación. Los detalles exactos de los métodos de codificación de protocolo, y la identificación de los canales de tara que se utilizan para el transporte del protocolo, se definen en las Recomendaciones de conmutación de protección correspondiente a cada tecnología (por ejemplo, Recomendaciones UIT-T G.841, G.873.1 e I.630).

Protocolo de 3 fases

– para todos los tipos de arquitectura;

– evita que se produzca una conexión errónea en cualquier circunstancia;

– hace funcionar un selector o un puente únicamente después de la confirmación de la prioridad.

Protocolo de 2 fases

– para las arquitecturas 1+1 y $(1:1)^n$;

– tiempo de conmutación de protección más corto.

Protocolo de 1 fase

– para la arquitectura $(1:1)^n$;

– tiempo de conmutación de protección más corto;

– hace funcionar un puente/selector antes de que se confirme la prioridad;

– protocolo más complejo.

24.1 Protocolo de 1 fase

Medio para alinear los dos extremos del dominio protegido a través del intercambio de un solo mensaje (Z → A).

Puede aplicarse a las arquitecturas $(1:1)^n$ y 1+1.

El puente/selector de Z funciona antes de que se sepa si la condición de Z tiene prioridad sobre la condición de A.

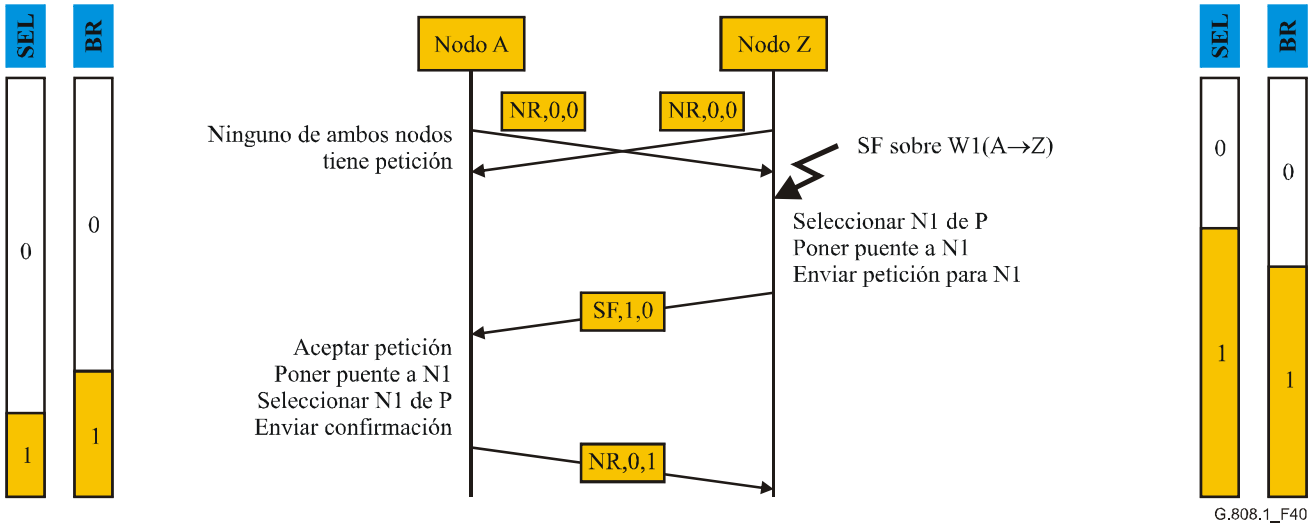


Figura 40/G.808.1 – Ejemplo de protocolo de 1 fase

24.2 Protocolo de 2 fases

Medio para alinear los dos extremos del dominio protegido mediante el intercambio de dos mensajes (Z → A, A → Z).

Puede aplicarse a las arquitecturas 1+1 con sus puentes permanentes.

Z no realiza ninguna acción de conmutación hasta que A confirma la prioridad de la condición en Z. Cuando A confirma la prioridad, hace funcionar el selector. Cuando se recibe la confirmación, Z hace funcionar su selector.

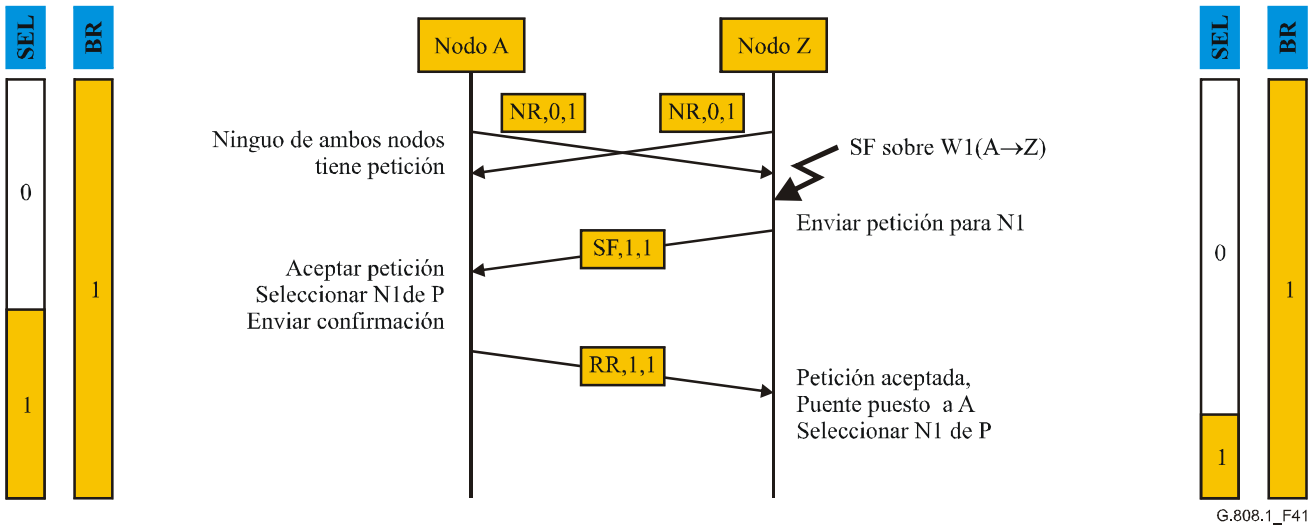


Figura 41/G.808.1 – Ejemplo de protocolo de 2 fases

24.3 Protocolo de 3 fases

Medio para alinear los dos extremos del dominio protegido mediante el intercambio de tres mensajes (Z → A, A → Z, Z → A).

Puede aplicarse a las arquitecturas 1:n y m:n y a las arquitecturas 1+1 con sus puentes permanentes.

En el caso de las arquitecturas 1:n, m:n, Z no realiza ninguna acción de conmutación hasta que A confirma la prioridad de la condición de Z. Cuando A confirma la prioridad hace funcionar el puente. Cuando se recibe la confirmación, Z hace funcionar su selector y puente y señala la acción de puenteo a A. Finalmente, A hace funcionar el selector.

En el caso de la arquitectura 1+1 con sus puentes permanentes, se hacen funcionar los selectores sólo como se describió en el caso 1:n.

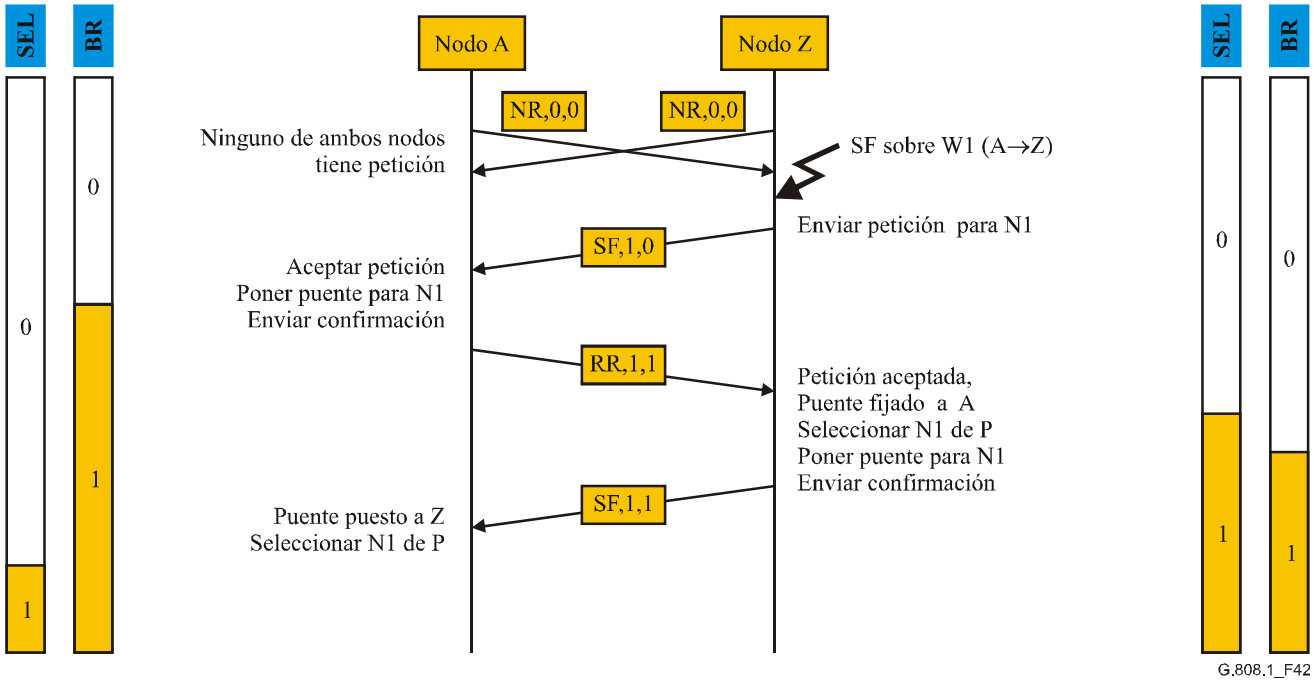


Figura 42/G.808.1 – Ejemplo de protocolo de 3 fases

Apéndice I

Implementación del temporizador de retención

Para la implementación de un temporizador de retención puede utilizarse un contador, el cual disminuye cada X milisegundos. Esta cuantificación introduce un límite de precisión para realizar el tiempo de retención. En la figura I.1 se presentan dos ejemplos: acciones de disminución cada 10 ms [25 ms]. En el caso de un tiempo de retención de 100 ms, el contador de retención puede cargarse con un valor de 10 [4] en el momento en que se presenta la condición SF/SD, para que disminuya al final de cada periodo de disminución de 10 ms [25 ms], y para que expire cuando llegue al valor 0. El tiempo de retención que se logra con esta implementación es de 95 ± 5 ms [82,5 ± 12,5 ms].

NOTA – En el caso de un periodo de disminución de 100 ms, el tiempo de retención de 100 ms es realmente de 50 ± 50 ms; es decir, entre 0 y 100 ms.

En lugar de cargar el contador con un valor de 10 [4], puede cargarse con un valor de 11 [5] para lograr tiempos de retención de 105 ± 5 ms [112,5 ± 12,5 ms].

La precisión de este tipo de temporizador de retención es 0,5 veces el periodo de disminución.

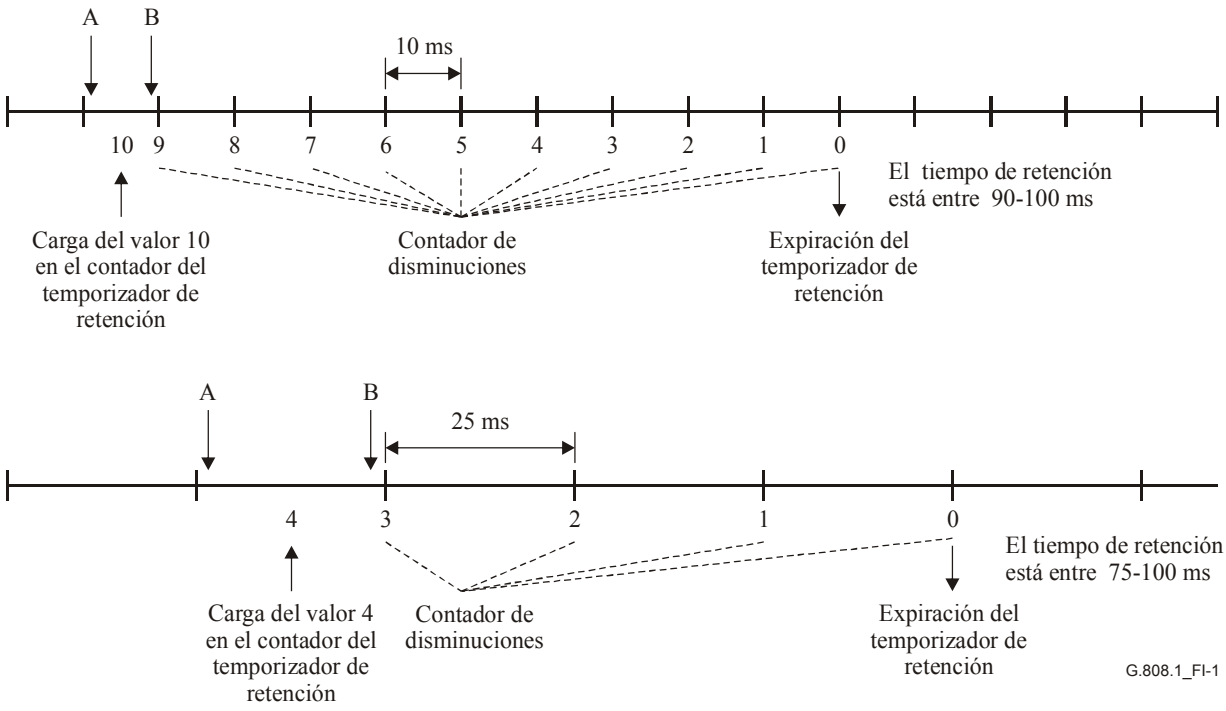


Figura I.1/G.808.1 – Precisión del temporizador de retención

Con un periodo de disminución de 10 ms, podrá compararse el efecto de las diferencias del tiempo de transferencia entre las entidades de transporte de servicio y de protección cuando se utiliza protección SNC/I 1+1 y SNC/N cuando se selecciona el valor "0" como tiempo de retención. Cuando se utiliza realmente el temporizador de retención (en lugar de desactivarlo) y el contador se carga con un valor de "2", pueden compensarse retardos diferenciales de 10 ms. Véase la Rec. UIT-T G.873.1.

Apéndice II

Condiciones automáticas (SF, SD) en la protección SNC de grupo

Con la protección SNC/N 1+1 [y SNC/I] las condiciones SF y SD para el grupo son SFG(roup) y SDG que son las entradas para el proceso de protección SNC. La lógica que permite calcular las condiciones SFG y SDG funcionan de la siguiente manera:

- SFG de servicio = (W-SF1 y no P-SF1) o (W-SF2 y no P-SF2) o ....
- SFG de protección = (P-SF1 y no W-SF1) o (P-SF2 y no W-SF2) o ....
- SDG de servicio = (W-SD1 y no P-SD1) o (W-SD2 y no P-SD2) o ....
- SDG de protección = (P-SD1 y no W-SD1) o (P-SD2 y no W-SD2) o ....

Esta definición de SFG y SDG permite diferenciar entre un fallo que se produce "frente al" o "dentro del" dominio protegido. Un fallo frente al dominio protegido en una señal simple no activará W-SFG [SDG] ni P-SFG [SDG], aunque en ambos estuviera activado el agrupamiento W y el agrupamiento P SF-i; no obstante, los términos "(W-SF-i y no P-SF-i)" y "(P-SF-i y no W-SF-i)" serán "falsos".

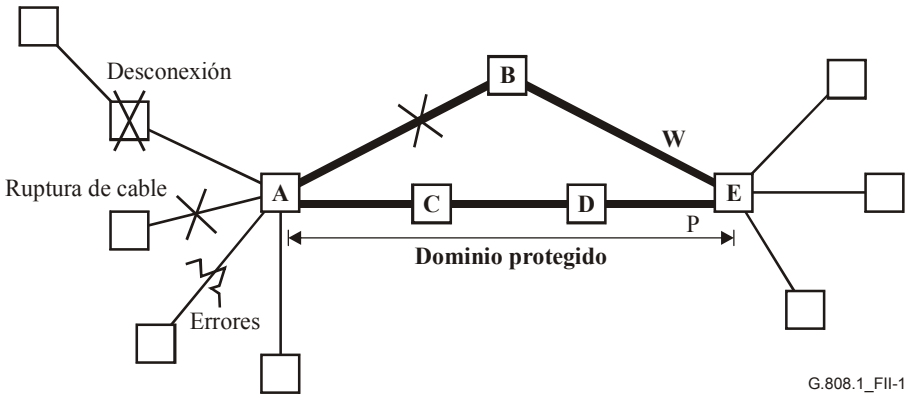


Figura II.1/G.808.1 – Ejemplo de fallo dentro del dominio protegido

Un fallo entre los elementos de red (NE) A y B (figura II.1) provocará la activación de W-SFG [o W-SDG]. Si se trata de un fallo de la señal de servidor, todas las señales dentro del agrupamiento pasarán a una condición SF. Si se trata de un fallo de conectividad, una sola señal pasará a una condición SF. Ambas situaciones provocarán la activación de W-SFG.

Si al mismo tiempo sucede por ejemplo, una desconexión o una ruptura de cable antes del elemento de red A (afectando a una de las señales del grupo) se activarán W-SF-i y P-SF-i. Cuando el fallo en el dominio de protección afecta al servidor, W-SFG aún estará activo, y P-SFG estará inactivo. En el otro caso (fallo de conectividad en el dominio de protección), el grupo se conmutará si las señales con fallo frente al dominio protegido y dentro del mismo son distintas.

NOTA – El caso especial en el que todas las señales hayan fallado antes del dominio de protección da por resultado W-SFG y P-SFG inactivos. Sin embargo, este caso especial no afecta el funcionamiento del proceso de protección; ya no hay nada que proteger.

Los errores/fallos dentro del dominio protegido que provocan defectos AIS y DEG harán esto en todos los miembros del grupo en el mismo momento (suponiendo que es necesario que se transporten todas las señales dentro del grupo *en la misma señal servidora)*. Por consiguiente, puede utilizarse como activador la aplicación del operador "OR" a las condiciones SF y SD particulares.

Con relación a una pérdida de señal (por ejemplo, pérdida de continuidad, sin equipo) o un defecto de conectividad (por ejemplo, desadaptación del identificador de traza), es posible que no esté presente este comportamiento de grupo. Las señales se transconectan (en principio) individualmente en cada elemento de red. Por consiguiente, la aplicación del operador OR a las señales particulares iniciará una conmutación de protección del grupo cuando sólo una (o un subconjunto) de las señales tiene una condición de defecto de pérdida de señal. Ésta es la *consecuencia de la reducción de complejidad*.

Apéndice III

Observaciones relativas a la implementación

Actualmente está disponible y se utiliza comúnmente la tecnología en la cual los elementos de red (NE) de SDH o de otras tecnologías (por ejemplo, ATM, OTN) constan de "unidades de puertos (PU)" y "unidades de conmutación". Estas últimas realizan la transconexión/conmutación, y las unidades de puertos llevan a cabo todo el procesamiento de tara (y OAM ATM) de SDH [PDH] necesario.

Para los elementos de red (NE) de transconexión VC-12 SDH, una unidad de puertos realizará el procesamiento de los punteros de SOH, AU4, VC-4 POH y TU12 (figura III.1). A continuación, las señales VC-12 SDH resultantes pasan a la unidad de conmutación para encaminarlas a sus unidades de puertos de salida correspondientes.

Es probable que se utilice la misma unidad de puertos cuando no se termina la señal VC-4 SDH, sino que pasa a través como una señal VC-4.

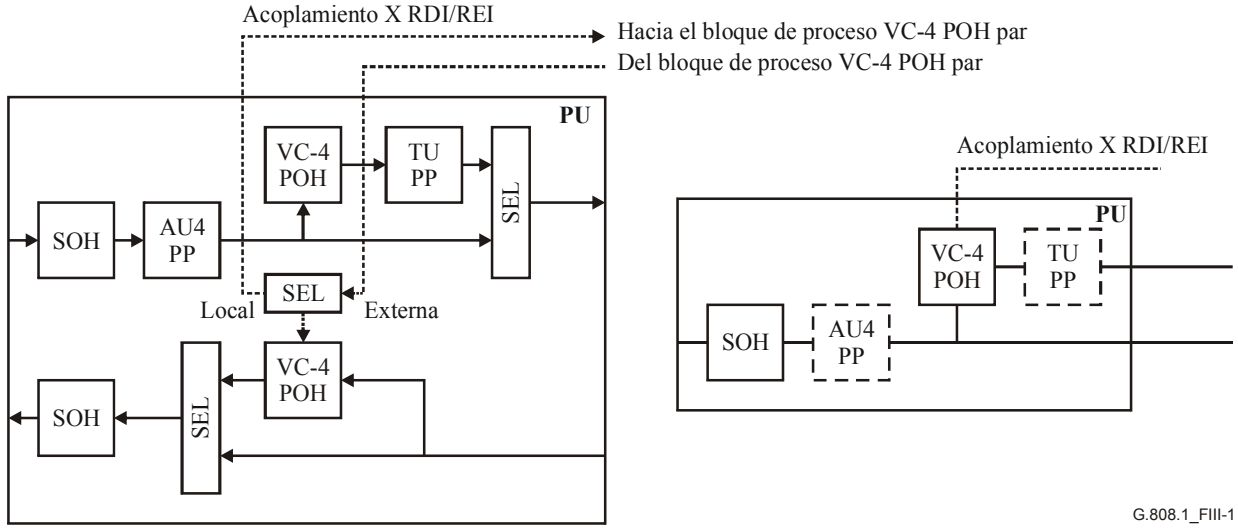


Figura III.1/G.808.1 – Vista (izquierda) detallada de la unidad de puertos y vista (derecha) comprimida (sólo la funcionalidad básica)

III.1 Análisis

Considere como un ejemplo el caso de la protección MS 1+1 (figura III.2); se utilizan dos unidades de puertos para este fin, ambos con soporte físico que realiza el procesamiento SOH, AU PP, VC-4 POH y TU PP, mientras que la conmutación de protección se realiza en la unidad de conmutación mediante la conmutación del grupo total de las señales de contenedor virtual de orden inferior (LOVC, *lower order virtual container*).

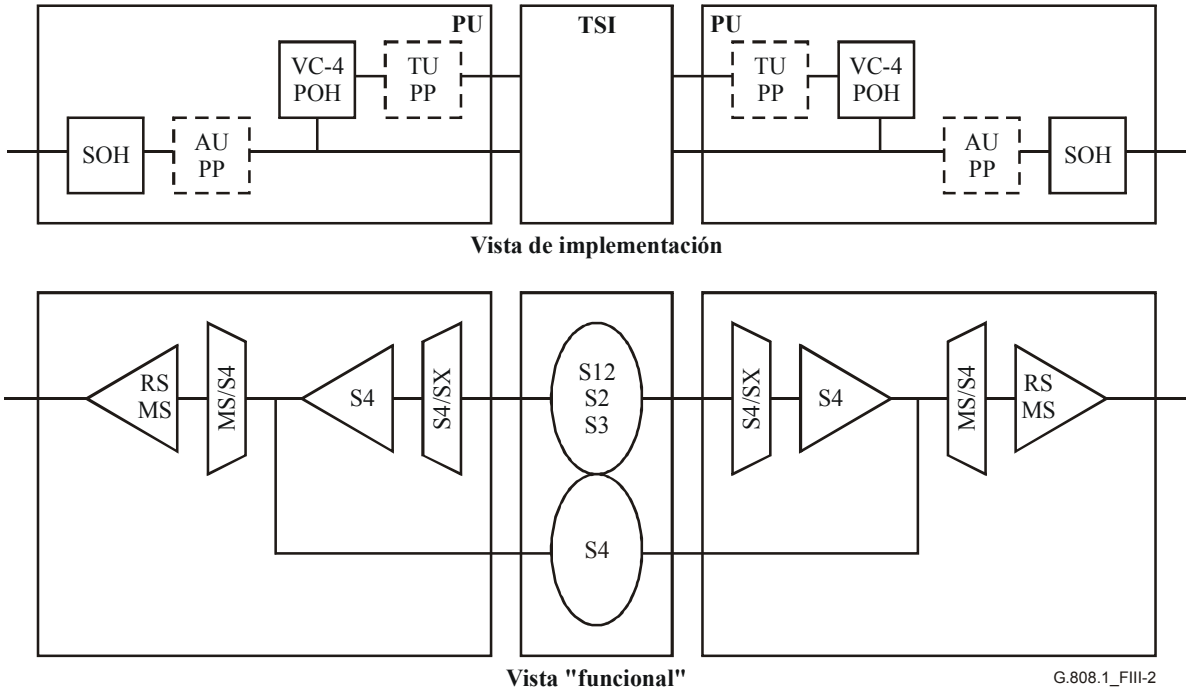


Figura III.2/G.808.1 – Correspondencia de la vista de la implementación con la vista funcional: funcionamiento básico

Conforme al modelo funcional hay demasiada funcionalidad (figura III.3); es decir, se prevé que habrá doble procesamiento SOH, mientras que sólo habrá un procesamiento AU PP, VC-4 POH y TU PP.

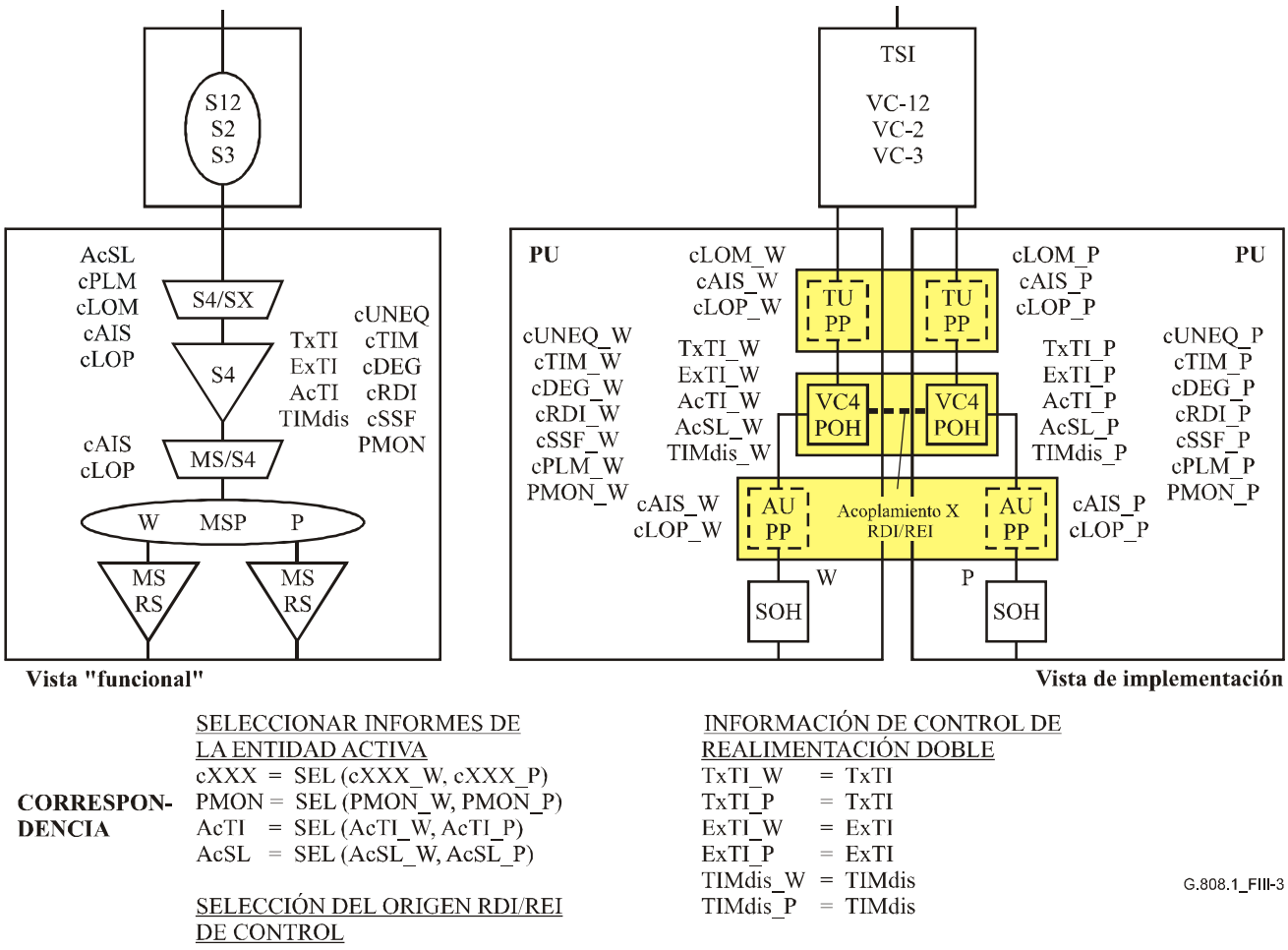


Figura III.3/G.808.1 – Correspondencia de la vista de la implementación con la vista funcional: protección MS

Con soporte lógico un elemento de red NE puede mostrar la funcionalidad esperada; éste oculta los procesos de reserva AU PP, VC-4 POH y TU PP al gestor.

Además, se necesita una máscara para las interfaces de transmisión; se prevé que las dos interfaces STM-N emitirán las mismas señales AU4(s), VC-4(s) y TU(s).

La implementación más sencilla emitirá "distintas" señales AU(s) y TU(s). La diferencia es el valor del puntero real; éstos no tienen que ser los mismos en las señales STM-N de servicio y de protección.

El hecho de que los valores de puntero AU/TU puedan ser distintos no tendrá ninguna repercusión en el funcionamiento de la red, es decir, en sentido estricto, esta "no conformidad" no tiene consecuencias. Lo anterior significa que no se necesita compensar esto.

No obstante, para el procesamiento VC-4 POH no es el mismo caso, ya que es necesario asegurarse de que las señales RDI y REI que se emiten a través de ambas interfaces STM-N son idénticas. Lo anterior significa que el proceso de supervisión de VC-4 POH en la unidad de puertos STM-N activa debe retransmitir sus señales RI_RDI/RI_REI a los procesos de generación VC-4 POH en ambas unidades de puertos (de servicio y de protección).

De modo similar, se requiere lo mismo cuando se selecciona la protección VC-4 SNC en lugar de la protección MS (figura III.4).

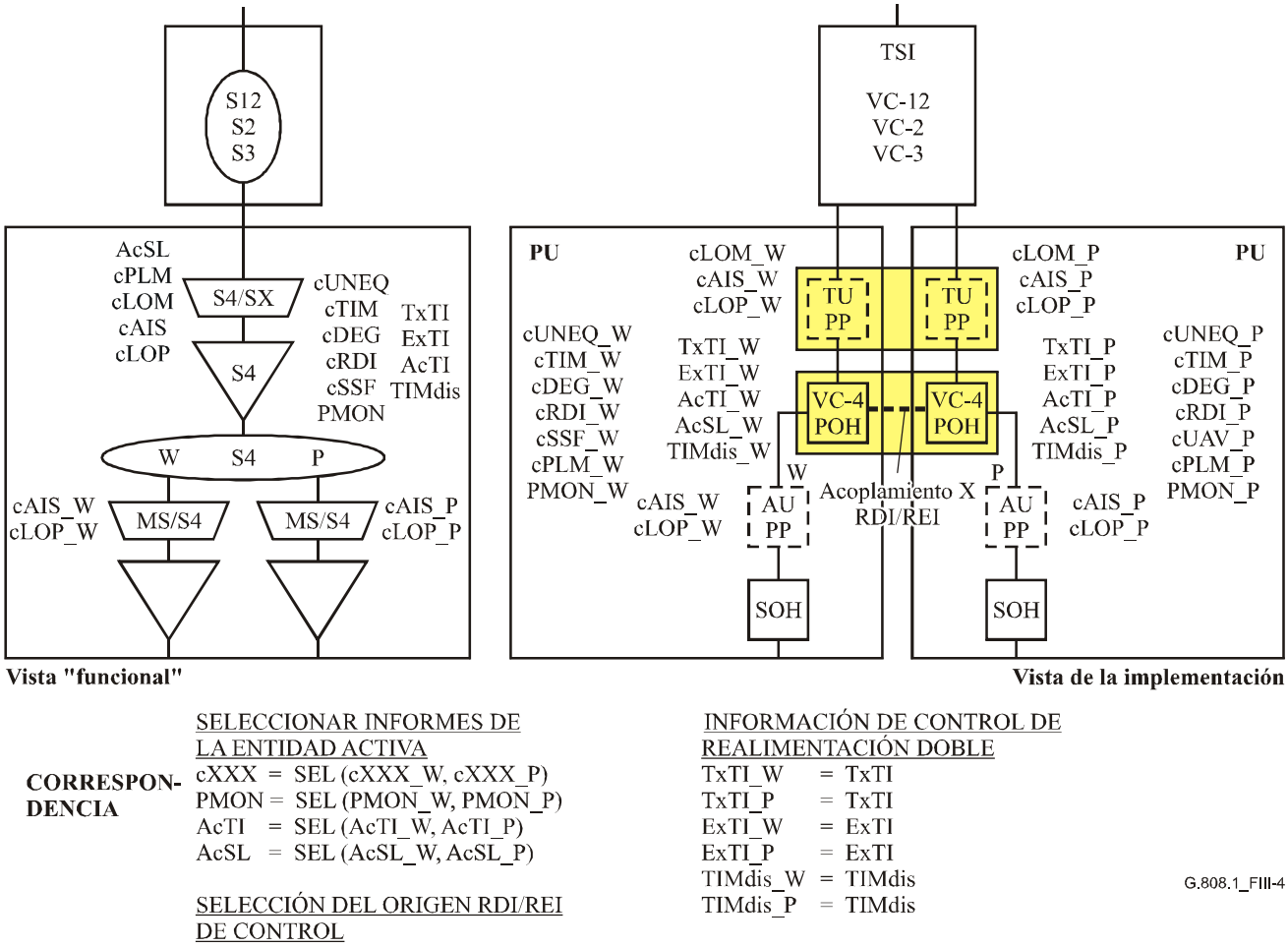


Figura III.4/G.808.1 – Correspondencia de la vista de la implementación con la vista funcional: protección VC-4 SNC/I

Si en algún caso no se implementa el acoplamiento X RDI/REI, no será posible añadir la supervisión de calidad de funcionamiento G.826 en las redes en las que están en funcionamiento las implementaciones de protección antes mencionadas. Conforme a la Rec. UIT-T G.826 se necesita el soporte de la supervisión de la calidad de funcionamiento bidireccional (basada en servicios). Esto exige que se utilice información del extremo distante. Esta información debe representar los errores/defectos detectados en el trayecto de señal que transporta realmente la información de cliente.

La conmutación unidireccional provoca que cada extremo del tramo de protección seleccione independientemente entre camino/SNC de servicio y de protección. Si, en la dirección A → Z se selecciona VC-4 SNC de servicio y en la dirección Z → A la protección VC-4 SNC, la información de extremo distante extraída de cada extremo se inserta en la unidad de puertos de reserva mediante el generador VC-4 POH, es decir, la unidad que no se seleccionó en este extremo. Si (ahora) utiliza sus señales RI_RDI/RI_REI locales (en lugar de sus señales RI_RDI/RI_REI compañeras), el extremo distante recibirá información de extremo distante no relacionada con la señal VC-4 seleccionada.

Los registros de supervisión de calidad de funcionamiento bidireccional representarán (en este caso) información errónea; es decir, información que no puede utilizarse.

Por supuesto, existe el mismo problema en el caso de los registros de extremo distante unidireccionales (basados en mantenimiento).

En el caso de encaminamiento NE de 64 kbit/s con interfaces STM-N, se presentará el mismo problema en el nivel VC-12.

NOTA – En las figuras III.3 y III.4 se representa la cuestión únicamente desde el punto de vista de RDI/REI. En estas figuras no se muestra la terminación de conexión/segmento en cascada o las funciones de supervisión no intrusivas que se necesitan para controlar el conmutador de protección.

Apéndice IV

Ejemplo de protección $(1:1)^n$

En este apéndice se da un ejemplo de conmutación de protección $(1:1)^n$ (para n = 3) en una red ATM. En este caso, hay tres entidades de servicio, que tienen encaminamiento diversificado. Éstas se protegen mediante una sola entidad de protección, que transporta tráfico adicional durante el funcionamiento normal. La entidad de protección debe tener suficiente anchura de banda para transportar la más grande de las tres señales de tráfico normal o la señal de tráfico adicional. Cada una de las entidades de servicio es un trayecto virtual ATM, cuyo tamaño e identificador de trayecto virtual (VPI) se muestran en la figura IV.1.

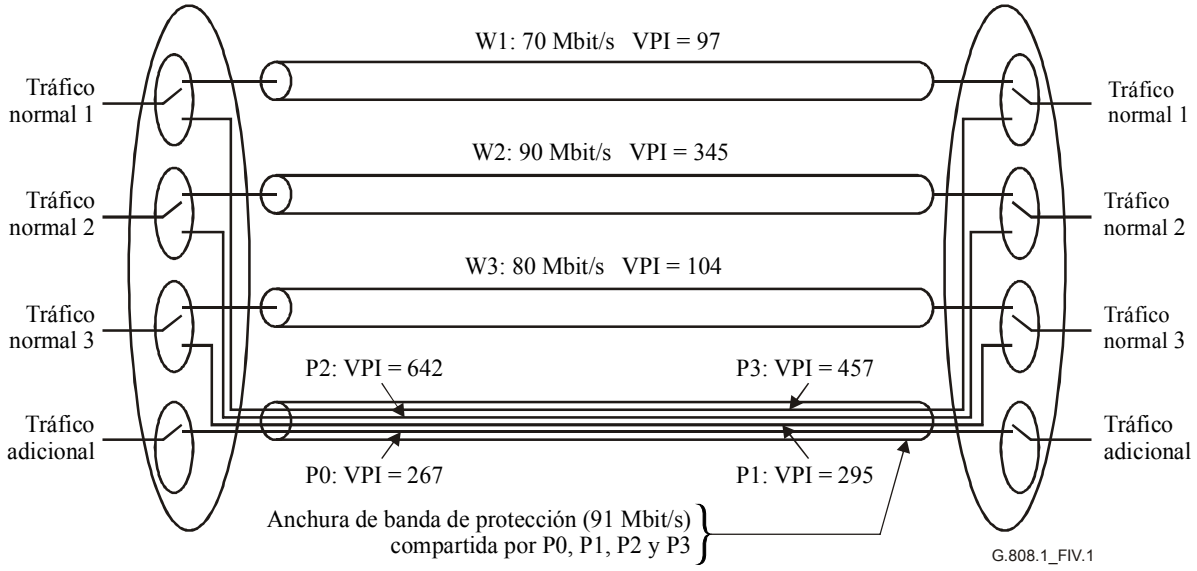


Figura IV.1/G.808.1 – Ejemplo de protección $(1:1)^n$

En este ejemplo, se necesitan 90 Mbit/s más las células OAM para P0 (incluye VP-APS OAM), P1, P2 y P3 para proporcionar la conmutación de protección. En el caso de la conmutación unidireccional, puede utilizarse un protocolo de una fase ya que cuando se detecta una condición de fallo, sólo se necesita que se envíe una señal del extremo Z al extremo A para iniciar la conmutación en el puente. No hay posibilidad de conexión errónea ya que la señal, que se encuentra en la entidad de protección, se identifica de manera singular mediante su VPI.

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

Impreso en Suiza
Ginebra, 2004