

**UIT-T**

**G.8031/Y.1342**

SECTOR DE NORMALIZACIÓN  
DE LAS TELECOMUNICACIONES  
DE LA UIT

(06/2006)

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

Aspectos relativos a los protocolos en modo paquete  
sobre la capa de transporte – Aspectos relativos al  
protocolo Ethernet sobre la capa de transporte

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

Aspectos del protocolo Internet – Transporte

---

## **Conmutación de protección Ethernet**

Recomendación UIT-T G.8031/Y.1342

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 SATELITE E INTERCONEXIÓN CON LOS SISTEMAS EN LÍNEAS METÁLICAS	G.400–G.449
COORDINACIÓN DE LA RADIOTELEFONÍA Y LA TELEFONÍA EN LÍNEA	G.450–G.499
CARACTERÍSTICAS DE LOS MEDIOS DE TRANSMISIÓN Y DE LOS SISTEMAS ÓPTICOS	G.600–G.699
EQUIPOS TERMINALES DIGITALES	G.700–G.799
REDES DIGITALES	G.800–G.899
SECCIONES DIGITALES Y SISTEMAS DIGITALES DE LÍNEA	G.900–G.999
CALIDAD DE SERVICIO Y DE TRANSMISIÓN – ASPECTOS GENÉRICOS Y ASPECTOS RELACIONADOS AL USUARIO	G.1000–G.1999
CARACTERÍSTICAS DE LOS MEDIOS DE TRANSMISIÓN	G.6000–G.6999
DATOS SOBRE CAPA DE TRANSPORTE – ASPECTOS GENÉRICOS	G.7000–G.7999
ASPECTOS RELATIVOS A LOS PROTOCOLOS EN MODO PAQUETE SOBRE LA CAPA DE TRANSPORTE	G.8000–G.8999
<b>Aspectos relativos al protocolo Ethernet sobre la capa de transporte</b>	<b>G.8000–G.8099</b>
Aspectos relativos al protocolo MPLS sobre la capa de transporte	G.8100–G.8199
Objetivos de calidad y disponibilidad (continuación de la serie G.82x)	G.8200–G.8299
Gestión de servicios	G.8600–G.8699
REDES DE ACCESO	G.9000–G.9999

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

## **Recomendación UIT-T G.8031/Y.1342**

### **Conmutación de protección Ethernet**

#### **Resumen**

En la presente Recomendación se describen las particularidades de la conmutación de protección de señales VLAN Ethernet. Se incluye información relativa a las características, arquitecturas y protocolo APS para la protección ETH. La estrategia de protección empleada en esta Recomendación es:

- Protección de conexión de subred Ethernet basada en VLAN, con supervisión de subcapa.

#### **Orígenes**

La Recomendación UIT-T G.8031/Y.1342 fue aprobada el 6 de junio de 2006 por la Comisión de Estudio 15 (2005-2008) del UIT-T por el procedimiento de la Recomendación UIT-T A.8.

## PREFACIO

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

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

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

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

## NOTA

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

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

## PROPIEDAD INTELECTUAL

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

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección <http://www.itu.int/ITU-T/ipr/>.

© UIT 2007

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

## ÍNDICE

	<b>Página</b>
1 Alcance .....	1
2 Referencias .....	1
3 Definiciones.....	2
4 Abreviaturas, siglas o acrónimos .....	5
5 Convenios .....	6
5.1 Representación de octetos .....	6
6 Introducción.....	6
7 Requisitos .....	7
8 Características de la protección .....	8
8.1 Métodos y condiciones de supervisión.....	8
9 Instrucciones relativas al grupo de protección.....	9
9.1 Instrucciones y estados extremo a extremo .....	9
9.2 Instrucciones locales.....	9
10 Arquitecturas de protección.....	10
10.1 Conmutación unidireccional y bidireccional.....	10
10.2 Necesidad de comunicación APS.....	10
10.3 Conmutación reversible y no reversible .....	11
10.4 Discordancias de configuración .....	11
10.5 Activación de la conmutación de protección.....	12
10.6 Modelos de conmutación de protección.....	12
11 Protocolo APS .....	18
11.1 Formato del APS .....	18
11.2 Protocolo APS de una fase .....	20
11.3 Tipo de petición.....	23
11.4 Tipos de protección .....	23
11.5 Señal solicitada.....	23
11.6 Señal puenteada .....	24
11.7 Control del puente .....	24
11.8 Control del selector.....	24
11.9 Fallo de señal de la entidad de transporte de protección.....	24
11.10 Peticiones con la misma prioridad.....	24
11.11 Aceptación y acogida de instrucciones.....	25
11.12 Temporizador de espera .....	25
11.13 Temporizador de espera para el restablecimiento .....	25
11.14 Instrucción ejercicio .....	26
11.15 Defectos de fallo del protocolo.....	26

	<b>Página</b>
Anexo A – Cuadros de transición de estado para la conmutación de protección .....	27
A.1    Transición de estado de la conmutación bidireccional 1:1 con modo reversible .....	27
A.2    Transición de estado para conmutación bidireccional 1:1 en modo no reversible .....	30
A.3    Transición de estado para conmutación bidireccional 1+1 con modo reversible .....	32
A.4    Transición de estado para conmutación bidireccional 1+1 con modo no reversible .....	34
A.5    Transición de estado para 1+1 conmutación unidireccional con modo reversible .....	36
A.6    Transición de estado para la conmutación unidireccional 1+1 con modo no reversible .....	37
Apéndice I – Ejemplo del funcionamiento del protocolo APS de una fase .....	38
I.1    Introducción.....	38
I.2    Caso hipotético .....	38
I.3    Ejemplos del protocolo APS .....	38
Apéndice II – Interacción entre conmutación de protección Ethernet y STP .....	41
Apéndice III – MIP para el entorno de conmutación de protección .....	43
III.1    Introducción.....	43
III.2    Consideraciones.....	43
III.3    Ejemplos de configuración .....	45

# Recomendación UIT-T G.8031/Y.1342

## Conmutación de protección Ethernet

### 1 Alcance

En la presente Recomendación se definen los mecanismos del protocolo APS y conmutación de protección lineal para conexiones de subred (SNC) Ethernet (ETH) basadas en redes de área local virtual (VLAN) punto a punto en redes de transporte Ethernet. Quedan en estudio todas las demás estrategias de protección incluidas las punto a multipunto y multipunto a multipunto.

En esta versión de la Recomendación se definen las arquitecturas de conmutación de protección lineal 1+1 y 1:1 con conmutación unidireccional y bidireccional.

Queda en estudio el funcionamiento del protocolo APS y conmutación de protección para todas las demás arquitecturas de red Ethernet (por ejemplo en anillo, malla, etc.).

### 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.780/Y.1351 (2004), *Términos y definiciones para las redes de jerarquía digital síncrona*.
- Recomendación UIT-T G.805 (2000), *Arquitectura funcional genérica de las redes de transporte*.
- Recomendación UIT-T G.806 (2006), *Características del equipo de transporte – Metodología de descripción y funcionalidad genérica*.
- Recomendación UIT-T G.808.1 (2006), *Conmutación de protección genérica – Protección lineal de camino y de subred*.
- Recomendación UIT-T G.841 (1998), *Tipos y características de las arquitecturas de protección para redes de la jerarquía digital síncrona*.
- Recomendación UIT-T G.870/Y.1352 (2004), *Términos y definiciones para redes ópticas de transporte*.
- Recomendación UIT-T G.8010/Y.1306 (2004), *Arquitectura de redes de capa Ethernet*.
- Recomendación UIT-T G.8021/Y.1341 (2004), *Características de los bloques funcionales de equipos de red de transporte Ethernet*.
- Recomendación UIT-T M.495 (1988), *Restablecimiento de la transmisión y diversidad de rutas de transmisión: terminología y principios generales*.
- Recomendación UIT-T Y.1731 (2006), *Funciones y mecanismos de operación, administración y mantenimiento para redes basadas en Ethernet*.

- IEEE Standard 802-2001, *IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture*.
- IEEE Standard 802.1D-2004, *IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges*.
- IEEE Standard 802.1Q-2005, *IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks*.

### **3 Definiciones**

En esta Recomendación se utilizan los siguientes términos definidos en la Rec. UIT-T G.780/Y.1351.

#### **3.1 conmutación de protección bidireccional**

#### **3.2 conmutación de protección unidireccional**

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

#### **3.3 información adaptada**

#### **3.4 información característica**

#### **3.5 enlace**

#### **3.6 conexión de enlace**

#### **3.7 degradación de señal (SD, *signal degrade*)**

#### **3.8 fallo de señal (SF, *signal fail*)**

#### **3.9 conexión en cascada**

#### **3.10 camino**

#### **3.11 terminación de camino**

En esta Recomendación se utilizan los siguientes términos definidos en la Rec. UIT-T G.806.

#### **3.12 función atómica**

#### **3.13 defecto**

#### **3.14 fallo**

#### **3.15 fallo de señal de servidor (SSF, *server signal fail*)**

#### **3.16 fallo de la señal de camino (TSF, *trail signal fail*)**

En esta Recomendación se utilizan los siguientes términos definidos en la Rec. UIT-T G.870/Y.1352.

#### **3.17 protocolo APS**

##### **3.17.1 fase 1**

#### **3.18 clase de protección**

##### **3.18.1 individual**

##### **3.18.2 grupo**

##### **3.18.3 protección de conexión de red**

##### **3.18.4 protección de conexión de subred**

- 3.18.4.1 supervisión de subcapa (/S)
- 3.18.4.2 supervisión no intrusiva
- 3.18.4.3 supervisión inherente
- 3.18.4.4 supervisado de prueba (/T)
- 3.18.5 protección de camino
- 3.19 conmutación
- 3.20 componente
  - 3.20.1 dominio protegido
  - 3.20.2 puente
    - 3.20.2.1 puente permanente
    - 3.20.2.2 puente selector
  - 3.20.3 selector
    - 3.20.3.1 selector selectivo
    - 3.20.3.2 selector de combinación
  - 3.20.4 extremo cabecera
  - 3.20.5 extremo cola
  - 3.20.6 nodo sumidero
  - 3.20.7 nodo fuente
  - 3.20.8 nodo intermedio
- 3.21 arquitectura
  - 3.21.1 arquitectura de protección 1+1
  - 3.21.2 arquitectura de protección 1:n
  - 3.21.3 arquitectura de protección (1:1)<sup>n</sup>
- 3.22 señales
  - 3.22.1 señal de tráfico
    - 3.22.2 señal de tráfico normal
    - 3.22.3 señal de tráfico adicional
    - 3.22.4 señal nula
- 3.23 tiempo
  - 3.23.1 tiempo de detección
  - 3.23.2 tiempo de liberación
  - 3.23.3 tiempo de espera para el restablecimiento
  - 3.23.4 tiempo de conmutación
- 3.24 entidad de transporte
  - 3.24.1 entidad de transporte de protección

- 3.24.2 entidad de transporte de trabajo**
- 3.24.3 entidad de transporte activa**
- 3.24.4 entidad de transporte de reserva**
- 3.25 protección**
- 3.26 deficiencia**
- 3.27 relación de protección**

En esta Recomendación se utilizan los siguientes términos definidos en la Rec. UIT-T G.809.

- 3.28 adaptación**
- 3.29 flujo**
- 3.30 dominio de flujo**
- 3.31 punto de flujo**
- 3.32 terminación de flujo**
- 3.33 red de capa**
- 3.34 flujo de enlace**
- 3.35 red**
- 3.36 puerto**
- 3.37 transporte**
- 3.38 entidad de transporte**
- 3.39 punto de flujo de terminación**

En esta Recomendación se utilizan los siguientes términos definidos la Rec. UIT-T G.8010/Y.1306.

- 3.40 información característica Ethernet (ETH\_CI, *Ethernet characteristic information*)**
- 3.41 punto de flujo Ethernet (ETH\_FP, *Ethernet flow point*)**
- 3.42 entidad de mantenimiento**
- 3.43 grupo de entidades de mantenimiento**
- 3.44 nivel de grupo de entidades de mantenimiento**

En esta Recomendación se utiliza el siguiente término definido en la Rec. UIT-T G.8021/Y.1341.

- 3.45 función de reenvío del flujo Ethernet (ETH\_FF, *Ethernet flow forwarding function*)**

En esta Recomendación se utiliza el siguiente término definido en la Rec. UIT-T M.495.

- 3.46 tiempo de transferencia (Tt, *transfer time*)**

En esta Recomendación se utiliza el siguiente término definido y descrito en las Recs. UIT-T G.8010/Y.1306 y en Y.1731.

- 3.47 punto extremo de grupo de entidades de mantenimiento**

#### 4 Abreviaturas, siglas o acrónimos

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

AI	Información adaptada ( <i>adapted information</i> )
APS	Conmutación automática de protección ( <i>automatic protection switching</i> )
CCM	Mensaje de verificación de continuidad ( <i>continuity check message</i> )
CI	Información característica ( <i>characteristic information</i> )
DNR	No revertir ( <i>do not revert</i> )
EC	Conexión Ethernet ( <i>Ethernet connection</i> )
ETH	Red de capa Ethernet ( <i>Ethernet layer network</i> )
ETH-AIS	Función de señal de indicación de alarma Ethernet ( <i>Ethernet alarm indication signal function</i> )
ETH-APS	Función de conmutación de protección automática Ethernet ( <i>Ethernet automatic protection switching function</i> )
ETH-CC	Función de verificación de continuidad Ethernet ( <i>Ethernet continuity check function</i> )
EXER	Ejercicio ( <i>exercise</i> )
FS	Conmutación forzada ( <i>forced switch</i> )
FT	Terminación de flujo ( <i>flow termination</i> )
LCK	Bloqueado ( <i>locked</i> )
LO	Exclusión para protección ( <i>lockout for protection</i> )
LOC	Pérdida de continuidad ( <i>loss of continuity</i> )
LSB	Bit menos significativo ( <i>least significant bit</i> )
MEP	Punto extremo de grupo de entidad de mantenimiento ( <i>maintenance entity group end point</i> )
MIP	Punto intermedio de grupo de entidad de mantenimiento ( <i>maintenance entity group intermediate point</i> )
MS	Conmutación manual ( <i>manual switch</i> )
MSB	Bit más significativo ( <i>most significant bit</i> )
NR	Ninguna petición ( <i>no request</i> )
OAM	Operación, administración y mantenimiento ( <i>operation, administration and maintenance</i> )
PDU	Unidad de datos de protocolo ( <i>protocol data unit</i> )
PS	Conmutación de protección ( <i>protection switching</i> )
RR	Petición de revertir ( <i>reverse request</i> )
RSTP	Protocolo de árbol abarcante rápido ( <i>rapid spanning tree protocol</i> )
SD	Degradación de señal ( <i>signal degrade</i> )
SF	Fallo de señal ( <i>signal fail</i> )
SF-P	Fallo de señal en la protección ( <i>signal fail on protection</i> )

SNC	Conexión de subred ( <i>subnetwork connection</i> )
SNC/I	Conexión de subred con supervisión inherente ( <i>inherently monitored subnetwork connection</i> )
SNC/N	Conexión de subred con supervisión no intrusiva ( <i>non-intrusively monitored subnetwork connection</i> )
SNC/S	Conexión de subred con supervisión de subcapa ( <i>sub-layer monitored subnetwork connection</i> )
SNC/T	Conexión de subred con supervisión de prueba ( <i>test-trail monitored subnetwork connection</i> )
VID	Identificador de VLAN ( <i>VLAN identifier</i> )
VLAN	LAN virtual ( <i>virtual LAN</i> )
WTR	Espera para restauración ( <i>wait to restore</i> )

## 5 Convenios

### 5.1 Representación de octetos

Los octetos se representan de la forma definida en IEEE 802.1D.

Cuando se utilizan varios octetos consecutivos para representar un número binario, el número de octeto más bajo posee el valor más significativo.

Los bits de un octeto se enumeran de 1 a 8, siendo 1 el bit menos significativo (LSB) y 8 el bit más significativo (MSB).

## 6 Introducción

En esta Recomendación se especifican los mecanismos de conmutación de protección lineal que deben aplicarse a las redes Ethernet basadas en VLAN descritas en la Rec. UIT-T G.8010/Y.1306. La conmutación de protección es un mecanismo de supervivencia de adjudicación completa, en el sentido de que la ruta y el ancho de banda de la entidad de protección se reserva para la entidad de trabajo seleccionada. Consiste en un mecanismo de supervivencia rápido y sencillo. Con conmutación de protección es más fácil para el operador de la red percibir el estado de la red (por ejemplo, la topología de red activa) que con otros mecanismos de supervivencia como RSTP.

En esta Recomendación se especifican la arquitectura de conmutación de protección 1+1 lineal y la arquitectura de conmutación de protección 1:1 lineal. La arquitectura de conmutación de protección 1+1 lineal funciona con conmutación que puede ser unidireccional o bidireccional. La arquitectura de conmutación de protección 1:1 lineal funciona con conmutación bidireccional.

En la arquitectura de conmutación de protección 1+1 lineal se asigna exclusivamente una entidad de transporte de protección a cada entidad de transporte de trabajo. El tráfico normal se copia y se entrega tanto a la entidad de transporte de trabajo como a la entidad de transporte de protección mediante un puente permanente ubicado al inicio del dominio protegido. Los tráficos de las entidades de transporte de trabajo y de protección se transmiten simultáneamente al sumidero del dominio protegido, donde se elige la entidad de transporte de protección o la entidad de transporte de trabajo con base en algún criterio predeterminado, como la indicación de defecto del servidor.

Aunque en la arquitectura de conmutación de protección 1+1 lineal la elección se lleva a cabo únicamente en el sumidero del dominio protegido, la conmutación de protección 1+1 bidireccional necesita del protocolo de coordinación APS para que los selectores de ambas direcciones elijan la misma entidad. Por otro lado, la conmutación de protección 1+1 unidireccional no requiere del protocolo de coordinación APS.

En la arquitectura de conmutación de protección 1:1 lineal, la entidad de transporte de protección es exclusiva de la entidad de transporte de trabajo. Sin embargo, el tráfico normal se transporta bien sea por la entidad de transporte de trabajo o por la entidad de transporte de protección mediante un puente selector ubicado en la fuente del dominio protegido. El selector ubicado en el sumidero del dominio protegido elige la entidad que transporta el tráfico normal. Es necesario el protocolo de coordinación APS ya que se requiere coordinar la fuente y el sumidero a fin de garantizar que el puente selector en la fuente y el selector en el sumidero elijan la misma entidad.

## **7 Requisitos**

- 1) La conmutación de protección Ethernet debe aplicarse a las SNC ETH basadas en VLAN punto a punto que proporcionen conectividad entre dos puntos de flujo ETH en un dominio de flujo ETH. Se pueden utilizar los VID para identificar las SNC ETH basadas en VLAN punto a punto en enlaces ETH. En la Rec. UIT-T G.8010/Y.1306 se trata detalladamente ETH y las funciones atómicas relacionadas. Aún no se ha determinado qué otras entidades deben ser protegidas.
- 2) Debe configurarse el dominio protegido de forma que se proteja el 100% del tráfico de trabajo degradado contra fallos en una entidad de trabajo única.
- 3) El tiempo de transferencia (Tt) debe ser menor de 50 ms.
- 4) Deben supervisarse periódicamente la conectividad de la capa ETH de la entidad de transporte de trabajo y la entidad de transporte de protección.
- 5) Una vez efectuada una conmutación de protección las tramas de evento deben entregarse ordenadamente.  
NOTA – Posterior al evento de conmutación de protección, algunas tramas podrían perderse temporalmente o resultar duplicadas debido a un retraso de trayecto diferencial.
- 6) Deben soportarse la conmutación de protección individual y en grupo.
- 7) La conmutación reversible y la conmutación no reversible deben proporcionarse como opciones del operador de la red.
- 8) Debe poderse detectar cualquier discordancia de funcionamiento entre puente/selector del extremo cercano y el puente/selector del extremo lejano.
  - Debe detectarse e informarse la discordancia del puente/selector del elemento de red local.
  - El operador de red debe eliminar la discordancia del puente/selector.
- 9) Deben soportarse las solicitudes del operador, como las instrucciones de protección contra el bloqueo, de conmutación forzada y de conmutación manual.
- 10) Debe soportarse protección con prioridad del fallo de la señal (SF, *signal fail*) y las peticiones del operador.
- 11) Debe proporcionarse la posibilidad de una "función de retención genérica" para retardar el comienzo de la acción de conmutación de protección.

## 8 Características de la protección

### 8.1 Métodos y condiciones de supervisión

La conmutación de protección ocurre cuando se detectan ciertos defectos en las entidades de transporte (de trabajo o de protección) en el dominio protegido. En las Recomendaciones que tratan de los equipos (por ejemplo, la Rec. UIT-T G.8021/Y.1341) se describe cómo se detectan estos defectos. Desde el punto de vista del funcionamiento del controlador de conmutación de protección, las entidades del dominio protegido pueden estar en el estado OK, de fallo (fallo de señal = SF) o degradada (degradación de señal = SD), de ser procedente.

Los siguientes son los métodos de supervisión habituales:

**Inherente** – La supervisión inherente se basa en los defectos detectados por una función de terminación del camino o por una función de adaptación al final del camino. La protección de subred Ethernet con supervisión inherente (SNC/I) depende de la supervisión inherente.

**No intrusiva** – La conmutación de protección se activa mediante una supervisión no intrusiva en el extremo de cola del grupo de protección. Esto permite proteger un camino que no esté limitado por el inicio o el fin del camino. La protección de subred Ethernet con supervisión no intrusiva (SNC/N) es una protección lineal que depende de la supervisión no intrusiva. La supervisión no intrusiva podría basarse en la supervisión de capa o de subcapa (un ejemplo de supervisión no intrusiva, es la supervisión de conexión en cascada (TCM)).

**Subcapa** – La protección de subred Ethernet con supervisión de subcapa (SNC/S) es una arquitectura de protección lineal que emplea supervisión de subcapa. Todas las conexiones de enlace compuesto en serie se amplían añadiéndoles supervisión de conexión en cascada (TCM, *tandem connection monitoring*) o funciones de terminación/adaptación, para así determinar el estado de la situación de fallo independientemente de la señal de tráfico presente. En las capas de red que soportan TCM, es conveniente crear segmentos de conmutación de protección que cubran con precisión los segmentos protegidos para que de esta forma, la conmutación de protección dependa únicamente de los defectos que ocurran en el segmento protegido. Esto tiene una ventaja adicional sobre SNC/N en el sentido de que los defectos que ocurran hacia el origen con respecto al segmento protegido, no afectarán la conmutación de protección.

**Camino de prueba** – Los defectos se detectan haciendo uso de un camino de prueba adicional. Se establece un camino de prueba adicional entre la fuente y el sumidero del dominio protegido, que incluya un grupo de protección de conexiones de subred. La protección de subred Ethernet con supervisión de camino de prueba (SNC/T) emplea la supervisión de un camino de prueba que se puede usar únicamente para la protección de grupos.

Para el controlador de conmutación de protección es irrelevante el método de supervisión utilizado, siempre y cuando pueda recibir información (OK, SF, SD si es procedente) destinada a las entidades de transporte al interior del dominio protegido. Algunos mecanismos de supervisión y capas de subred pueden no poseer un método para detectar SD, en cuyo caso no es necesario utilizar un protocolo APS diferente. Sencillamente no se emitiría una señal de SD del equipo que no la pueda detectar. Si se utiliza un protocolo APS, la implementación no debería impedir que el extremo lejano anuncie una SD utilizando el protocolo APS, aun si el supervisor del extremo cercano no puede detectar una SD.

En la presente versión de la Recomendación, se soporta la arquitectura de supervisión SNC/S para SNC de ETH punto a punto basadas en VLAN. Quedan en estudio otros métodos de supervisión como SNC/I, SNC/N y SNC/T.

## 9 Instrucciones relativas al grupo de protección

### 9.1 Instrucciones y estados extremo a extremo

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

**Exclusión de protección** – Con esta instrucción se impide que se elija cualquier señal de trabajo de la entidad de transporte de protección. Con esto, en efecto se inhabilita el grupo de protección.

**Conmutación forzada de la señal de tráfico normal a protección** – Obliga a que se elija una señal de tráfico normal de la entidad de transporte de protección.

**Conmutación manual de la señal de tráfico normal a protección** – Si no existe ningún fallo en ninguna de las entidades de transporte de trabajo o de protección, la instrucción obliga a que se elija una señal de tráfico normal de la entidad de transporte de protección.

**Espera para el restablecimiento de la señal de tráfico** – Durante el funcionamiento reversible, una vez se haya eliminado una SF (o SD, si es procedente) en la entidad de transporte de trabajo, la instrucción hace que se mantenga seleccionada la señal de tráfico normal de la entidad de transporte de protección, hasta que finalice un temporizador de espera para el restablecimiento. El estado cambiará a sin petición (NR) si el temporizador finaliza antes que cualquier otro evento o instrucción. Esta instrucción se utiliza para evitar la activación reiterativa del selector en caso de fallos intermitentes.

**Señal de ejercicio** – Ejercicio del protocolo APS. Se elige la señal de forma que no se modifique el selector.

**No revierta la señal de tráfico normal** – Se utiliza durante el funcionamiento no reversible para mantener seleccionada una señal de tráfico normal de la entidad de transporte de protección.

**Sin petición** – Sin petición es el estado al que ingresa la prioridad local en toda circunstancia en que no esté activa ninguna solicitud de conmutación de protección local (incluidas espera para el restablecimiento y no revertir). Se elige la señal de tráfico normal de la entidad de transporte correspondiente.

**Eliminar** – Elimina la instrucción activa de bloqueo de protección del extremo cercano activo, conmutación forzada, conmutación manual, estado de espera para el restablecimiento o ejercicio.

### 9.2 Instrucciones locales

Estas instrucciones se aplican únicamente al extremo cercano del grupo de protección. Aún si se utiliza el protocolo APS, las instrucciones no se señalan al extremo distante.

**Inmovilizar** – Bloquea el estado del grupo de protección. Mientras no se elimine la instrucción inmovilizar, se rechazan las instrucciones de extremo cercano adicionales, se hace caso omiso de los cambios de estado y de la información APS recibida. Cuando se elimina la instrucción inmovilizar, el estado del grupo de protección se recalcula basándose en el estado y en la información APS recibidos.

#### **Eliminar inmovilizar**

**Excluir la señal de tráfico normal de la protección** – Impide que la entidad de protección seleccione la señal de tráfico normal. Se rechazan las instrucciones relativas a la señal de tráfico normal. Si se trata de tráfico normal, se hará caso omiso de cualquier indicación de SF (o SD, si es

procedente). En el caso de conmutación bidireccional, se aceptarán todas las peticiones de tráfico normal del puente distante a fin de evitar fallos del protocolo. En consecuencia, se debe excluir la señal de tráfico normal de la entidad de transporte de protección en ambos extremos, para evitar que la entidad de transporte la seleccione como resultado de una instrucción o de un fallo en cualquiera de los extremos.

## **Eliminar excluir de la señal de tráfico normal de la protección**

### **10 Arquitecturas de protección**

En la arquitectura de protección lineal definida en la presente versión de esta Recomendación, la conmutación de protección se produce en los dos puntos extremos de una SNC ETH punto a punto basada en VLAN. Entre estos puntos extremo, habrá entidades "de trabajo" y de "protección".

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

Las siguientes arquitecturas son posibles:

**1+1** – En las arquitecturas 1+1, se emplea una entidad de transporte de protección para proteger la señal de tráfico normal. En el extremo cabecera, el puente es permanente. La conmutación se produce únicamente en el extremo de cola.

**1:1** – En las arquitecturas 1:1, se emplea una entidad de transporte de protección para proteger la señal de tráfico normal. En el extremo de cabecera no se crea el puente sino hasta que sea necesario un puente de protección.

Las arquitecturas de los dos extremos debe ser la misma.

#### **10.1 Conmutación unidireccional y bidireccional**

En el caso de transmisión bidireccional, es posible elegir conmutación unidireccional o bidireccional. En la conmutación unidireccional, los selectores de cada extremo son totalmente independientes. En conmutación bidireccional, se trata de coordinar los dos extremos de manera que ambos tengan la misma configuración de puenteo y de selección, aun si ocurre un fallo unidireccional. Para efectuar la conmutación bidireccional se requiere siempre de información APS para coordinar los dos puntos extremo. La conmutación unidireccional puede proteger contra dos fallos unidireccionales en sentidos opuestos, producidos en entidades distintas.

#### **10.2 Necesidad de comunicación APS**

El único tipo de conmutación que NO requiere comunicación APS es la conmutación unidireccional 1+1. Al tenerse un puente permanente en el extremo de cabecera, y al no haber necesidad de coordinar las posiciones del selector en los dos extremos, el selector del extremo de cola puede controlarse completamente conforme a los defectos e instrucciones recibidos en el extremo de cola.

La conmutación bidireccional siempre requiere de comunicaciones APS.

### 10.3 Conmutación reversible y no reversible

En funcionamiento reversible, se restablece la señal de tráfico normal a la entidades de trabajo después de que se hayan eliminado las causas de la conmutación. Si se elimina una instrucción (por ejemplo, conmutación forzada), el restablecimiento es inmediato. Si se elimina un defecto, el restablecimiento sucede, por lo general, después de que expire un temporizador "espera para el restablecimiento", que se utiliza para evitar el tableteo de los selectores en caso de defectos intermitentes.

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

La protección 1+1 se configura a menudo en modo no reversible, ya que de todas maneras la protección es exclusiva, y se evita así una segunda "alteración" de la señal de tráfico normal. Sin embargo, pueden existir motivos para configurar esta protección como reversible (por ejemplo, para que la señal de tráfico normal utilice el camino "corto", salvo en situaciones de fallo. Las políticas de algunos operadores incluyen también el funcionamiento reversible aun para la arquitectura 1+1).

Generalmente, la protección 1:1 es reversible. Aunque es posible definir el protocolo de forma que se permita el funcionamiento no reversible en la protección 1:1, es preferible efectuar la reversión y afectar la señal de tráfico normal una vez reparada la entidad de transporte de trabajo, ya que normalmente ésta última se ha optimizado mejor (desde el punto de vista de retraso y de recursos) que la entidad de transporte de protección.

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

### 10.4 Discordancias de configuración

Con todas las opciones de configuración en los grupos de protección, existe la posibilidad de que haya discordancias entre las configuraciones en los dos extremos. Estas discordancias se clasifican así:

- Discordancias que impiden el buen funcionamiento.
- Discordancias en las que uno o los dos los extremos puede adaptar su funcionamiento para proporcionar un grado de interfuncionamiento a pesar de la discordancia.
- Discordancias que no impiden el interfuncionamiento. Por ejemplo, la discordancia reversible/no reversible examinada en las cláusulas 10.3 y 11.4.

Con la información que se cursa en una comunicación APS no se puede transportar y detectar todas las discordancias de configuración. Sencillamente, hay demasiadas combinaciones de números válidos de entidad como para percibir fácilmente una panorámica de todas las opciones de configuración. Sin embargo, conviene tener una visión de la categoría intermedia, en la que ambos extremos pueden adaptar su operación para interfuncionar a pesar de la discordancia. Por ejemplo, un equipo configurado para conmutación bidireccional podría pasar a conmutación unidireccional para facilitar el interfuncionamiento. Un equipo configurado para conmutación 1+1 con comunicación APS podría pasar al funcionamiento con conmutación unidireccional 1+1 sin comunicación APS. Si bien se podría informar al usuario de la discordancia de configuración, el equipo podría continuar proporcionando cierto nivel de protección.

## 10.5 Activación de la conmutación de protección

Por ejemplo, podría efectuarse conmutación de protección si:

- la inicia el control del operador (por ejemplo, conmutación forzada, conmutación manual) y tiene una prioridad mayor que la de cualquier otra petición local o la petición del extremo distante; o
- se indica SF en la entidad de transporte activa, pero ésta no se indica en la entidad de transporte de reserva y la circunstancia de SF detectada tiene una prioridad mayor que la de cualquier otra petición local o que la de la petición del extremo distante; o
- en las arquitecturas bidireccionales 1+1 y 1:1, el protocolo APS recibido solicita la conmutación y tiene una prioridad mayor que la de cualquier otra petición local.

En el anexo A se describen otros casos como transición de estado.

### 10.5.1 Condiciones para la indicación de declaraciones de fallo

Se indica SF si se detecta la situación de fallo de la señal de camino ETH. En la Rec. UIT-T G.8021/Y.1341 se trata el fallo de la señal de camino ETH.

## 10.6 Modelos de conmutación de protección

En la figura 10-1 se ilustra un ejemplo de los modelos de conmutación de protección de SNC/C ETH basada en VLAN definidos en esta Recomendación. Se admiten otros casos de red.

Dentro de la función de reenvío de flujo ETH (ETH\_FF, *Ethernet flow forwarding function*), se crea un proceso de conmutación de protección de la SNC ETH a fin de proteger la conexión ETH (EC, *ETH connection*). Cuando se configura la conmutación de protección de una EC, es decir de la SNC ETH protegida, ésta se define entre dos puntos de flujo ETH (ETH\_FP, *ETH flow points*), tal como se indica en la figura 10-1. Cada proceso de conmutación de protección de SNC creado determina el ETH\_FP particular de salida utilizado para transferir la ETH\_CI protegida.

Por ejemplo, en el caso de configuración de conmutación de protección 1:1, el proceso que se crea en la ETH\_FF para la conmutación de protección de la SNC ETH puede reenviar la ETH\_CI de la conexión ETH protegida bien a la entidad de transporte trabajo o a la de protección.



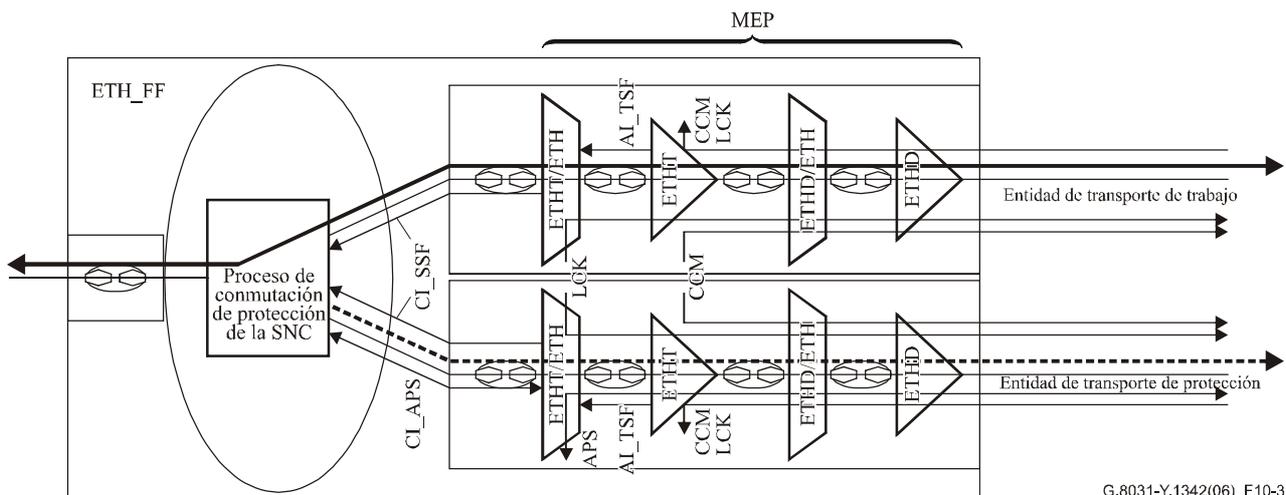
La información de APS y la indicación de defecto terminadas/detectadas por la función de sumidero del MEP pueden ingresarse al proceso de conmutación de protección de la forma mostrada en la figura 10-3.

Si un MEP detecta una anomalía que contribuya a una condición de defecto SF, éste informará al proceso de conmutación de protección que ha detectado una condición de fallo. La terminación del CCM y del LCK (que se definen en la Rec. UIT-T Y.1731) se lleva a cabo mediante la función atómica ETH\_FT. Si el ETH\_FT detecta una condición de fallo, se indica un AI\_TSF a la función ETH(x) a sumidero de adaptación ETH (ETH(x)/ETH\_A\_Sk) que en lo subsiguiente genera un CI\_SSF. La función de adaptación ETH(x)/ETH utiliza este CI\_SSF para notificar la situación de fallo de la señal al proceso de conmutación de protección de la SNC ETH dentro de la ETH\_FF.

La función ETH(x)/ETH\_A\_Sk dentro del MEP termina la PDU de la APS. La función ETH(x)/ETH\_A\_Sk extrae luego la información particular de la APS, de la PDU de la APS recibida, y la transfiere luego al proceso de conmutación de protección de la SNC ETH como información característica de APS (CI\_APS).

Tras recibir CI\_SSF o CI\_APS, el proceso de conmutación de protección determina el nuevo estado de conmutación, y posteriormente determina los ETH\_FP de salida particulares por los que se ha de transferir la ETH\_CI según sea necesario.

Cabe señalar que el estado administrativo de la función de adaptación de ETH(x)/ETH tanto para la entidad de transporte de trabajo como de protección no será "bloqueado".



G.8031-Y.1342(06)\_F10-3

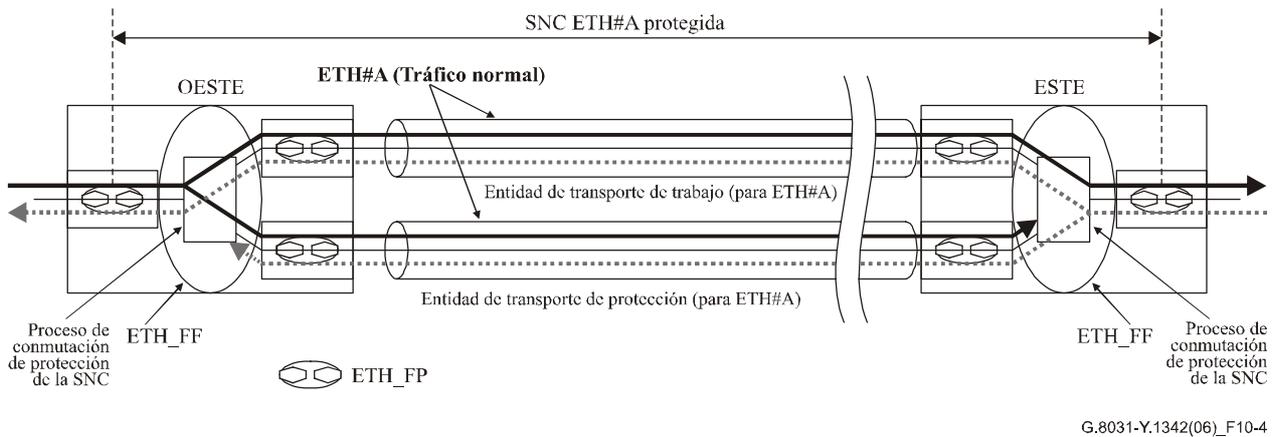
**Figura 10-3/G.8031/Y.1342 – Comportamientos de MEP y del proceso de conmutación de protección de la SNC en la arquitectura de conmutación de protección SNC/S ETH**

La protección SNC/S no se limita únicamente a las conexiones de subred, sino que también es posible extender este mecanismo de protección a conexiones de enlace único y a conexiones de red.

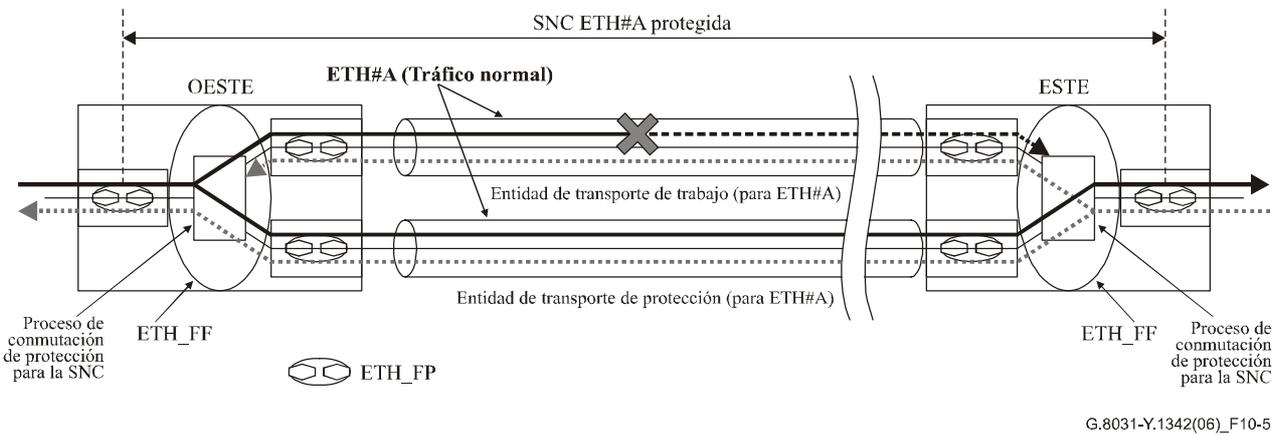
### 10.6.1 Conmutación de protección bidireccional 1+1

En la figura 10-4 se ilustra la arquitectura de conmutación de protección lineal bidireccional 1+1. El tráfico ETH\_CI protegido se puentea permanentemente tanto hacia la entidad de transporte de trabajo como hacia la entidad de transporte de protección. En esta figura, el tráfico se muestra como proveniente únicamente de la entidad de trabajo a través de la ETH\_FF. En la figura 10-5 se ilustra el caso en que se ha producido una conmutación de protección debido a un fallo de señal en la

entidad de transporte de trabajo. Cabe señalar que aunque suceda un defecto unidireccional, se conmutan ambas direcciones. Para lograr esto es necesario el protocolo de coordinación APS.



**Figura 10-4/G.8031/Y.1342 – Arquitectura de conmutación de protección bidireccional 1+1**

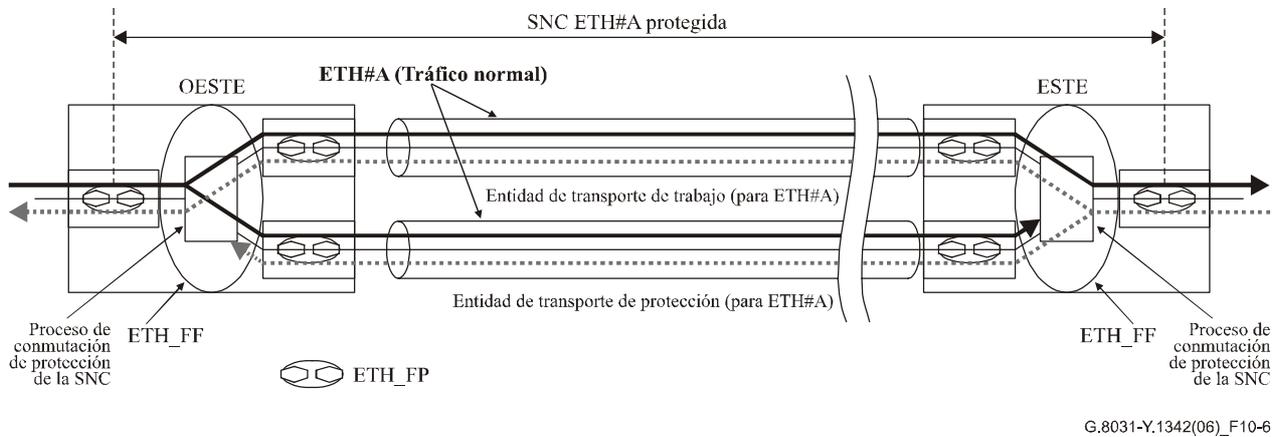


**Figura 10-5/G.8031/Y.1342 – Arquitectura de conmutación de protección bidireccional 1+1 – Situación de fallo de señal para la entidad de trabajo**

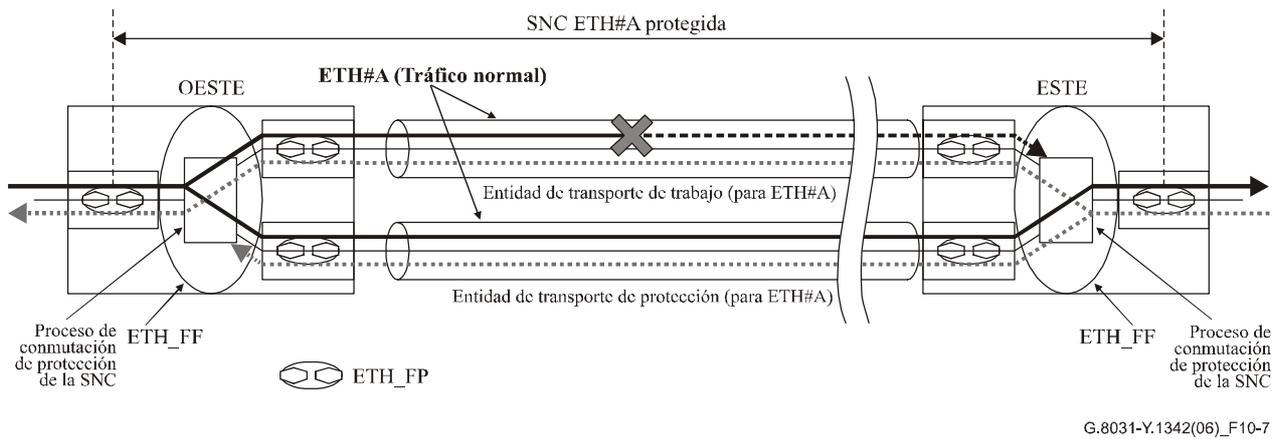
### 10.6.2 Conmutación de protección unidireccional 1+1

En la figura 10-6 se ilustra la arquitectura de conmutación de protección lineal unidireccional 1+1. El tráfico ETH\_CI protegido se puentea permanentemente tanto hacia la entidad de transporte de trabajo como hacia la entidad de transporte de protección. En esta figura se muestra el tráfico en ambas direcciones como recibido únicamente de la entidad de trabajo a través de la ETH\_FF. En la figura 10-7 se ilustra el caso en que se produce una conmutación de protección debido a una situación de fallo de señal de la entidad de transporte de trabajo en la dirección oeste a este. Se continúa recibiendo el tráfico normal de la dirección este a oeste a través de la entidad de transporte de trabajo. En la conmutación de protección unidireccional, cada dirección se conmuta de forma independiente. Los selectores en el sumidero del dominio protegido funcionan utilizando únicamente la información local. No es necesario el protocolo de coordinación APS para lograr este propósito.

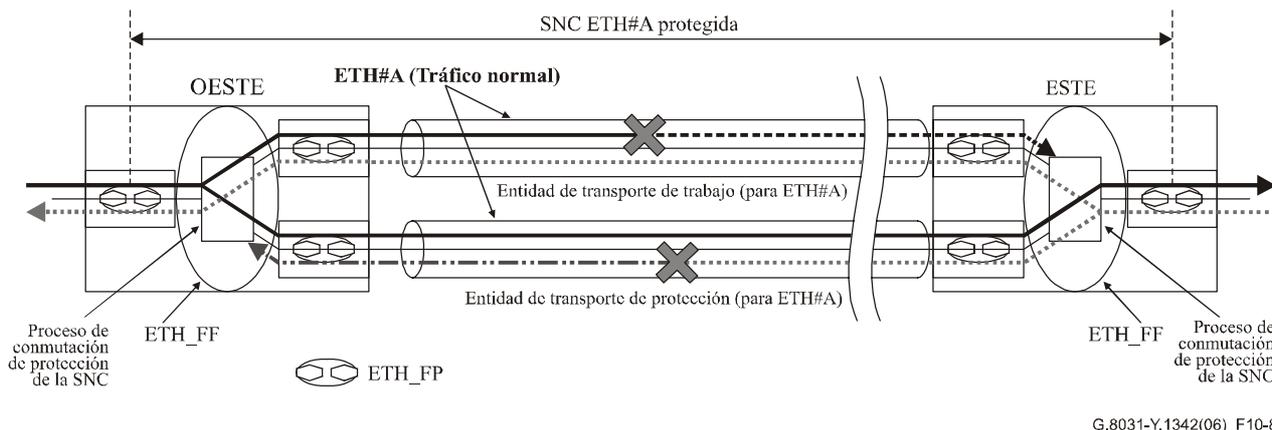
En la figura 10-8 se ilustra el caso en que existe una condición de fallo de señal en la entidad de transporte en la dirección oeste a este y en la entidad de transporte de protección en la dirección este a oeste. La conmutación de protección unidireccional puede brindar protección en este tipo de casos de doble defecto mientras que la conmutación de protección bidireccional no la ofrece.



**Figura 10-6/G.8031/Y.1342 – Arquitectura de conmutación de protección unidireccional 1+1**



**Figura 10-7/G.8031/Y.1342 – Arquitectura de conmutación de protección unidireccional 1+1 – Situación de fallo de señal en la entidad de transporte de trabajo en la dirección oeste a este**



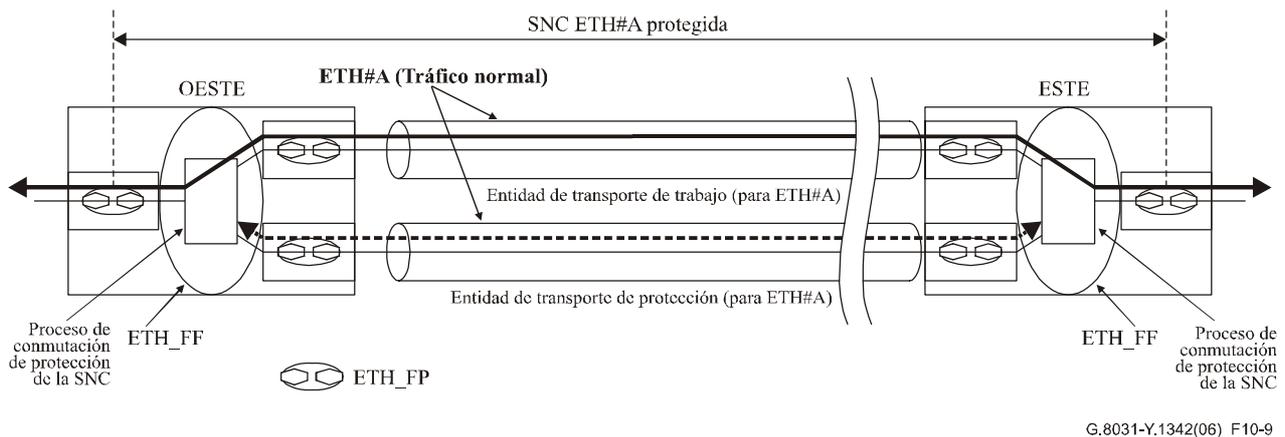
**Figura 10-8/G.8031/Y.1342 – Arquitectura de conmutación de protección unidireccional 1+1 – Situación de fallo de señal en ambas direcciones**

### 10.6.3 Conmutación de protección 1:1

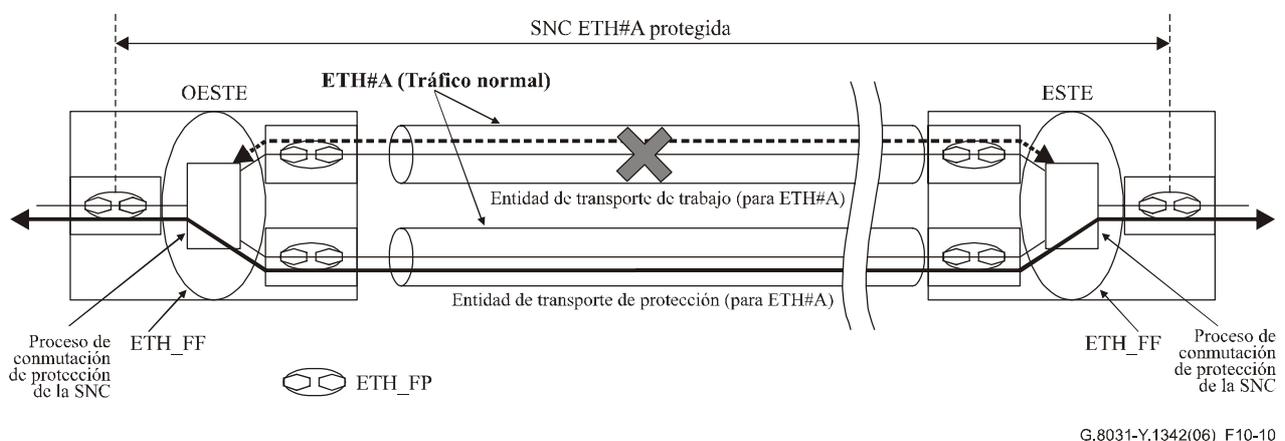
En la figura 10-9 se ilustra la arquitectura de conmutación de protección lineal 1:1, en la que el tráfico normal (ETH#A) se está transmitiendo a través de la entidad de transporte de trabajo. Aunque pueden utilizarse tanto la entidad de transporte de trabajo como de protección de ETH#A para cualquier otro tráfico de ETH, el proceso de conmutación de protección de la SNC ETH determina únicamente el ETH\_FF de salida a través del cual se transfiere la ETH\_CI protegida de la ETH#A, si se ha establecido conmutación de protección sólo para ETH#A.

En la figura 10-10 se ilustra el caso en que se ha producido una conmutación de protección debido a una situación de fallo de señal en la entidad de transporte de trabajo. En el nodo fuente, se retransmite el tráfico normal (ETH#A) a la entidad de transporte de protección. En el nodo sumidero, se recibe el tráfico normal (ETH#A) de la entidad de transporte de protección. Durante la operación de conmutación de protección es posible que ocurra una discordancia transitoria entre las posiciones del puente/selectores en los dos extremos del dominio protegido. Sin embargo, no es posible una conexión errónea entre la ETH\_CI y la ETH#A y otras ETH\_CI, debido a que el tráfico siempre se retransmite correctamente a través de la ETH\_FF utilizando la VID. Obsérvese que para lograr este comportamiento de reenvío, en la entidad de transporte de protección para la ETH#A protegida se deben configurar VID diferentes para el tráfico protegido de ETH#A y para el tráfico ETH no protegido.

El reenvío de tráfico utilizando la VID en la función ETH\_FF significa que para las arquitecturas 1:1 nunca son posibles conexiones erróneas de tráfico. Eso simplifica enormemente la funcionalidad del protocolo de conmutación de protección, lo que permite emplear un protocolo de una fase, en el que para completar la conmutación bidireccional es necesario un solo intercambio de información entre los dos extremos.



**Figura 10-9/G.8031/Y.1342 – Arquitectura de conmutación de protección 1:1**

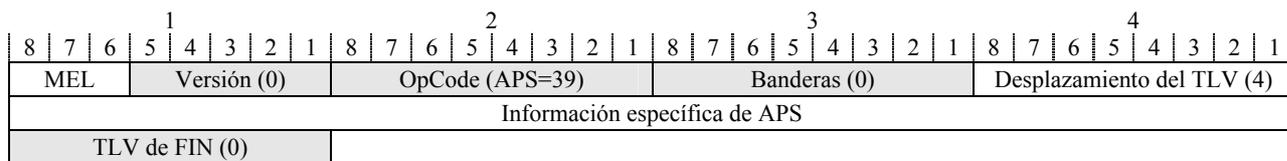


**Figura 10-10/G.8031/Y.1342 – Arquitectura de conmutación de protección 1:1 – Situación de fallo de señal en la entidad de transporte de trabajo**

## 11 Protocolo APS

### 11.1 Formato del APS

La información APS se transporta en una PDU de la APS, que es un elemento del conjunto de PDU de OAM Ethernet. Los formatos de PDU de OAM para cada tipo de operación de OAM Ethernet se definen en la Rec. UIT-T Y.1731. Se transmite información particular de la APS en campos específicos de la PDU de la APS. La PDU de la APS se identifica mediante un OpCode particular de OAM Ethernet. En esta versión de la Recomendación se utilizan 4 octetos de la PDU de la APS para transportar información específica de la APS. Esto se muestra en la figura 11-1 a continuación. Debe además observarse que para la versión actual de esta Recomendación, se requiere que el campo de desplazamiento TLV se haya fijado a 0x04.



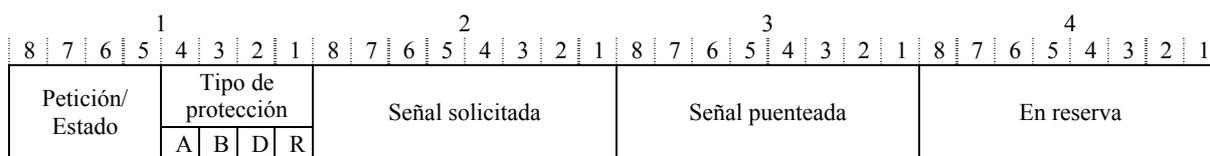
**Figura 11-1/G.8031/Y.1342 – Formato de la PDU del APS**

Se deben utilizar los siguientes valores para los campos Versión, OpCode, Banderas y TLV de FIN, conforme se define en la Rec. UIT-T Y.1731.

- **Versión:** 0x00
- **OpCode:** 0x39
- **Banderas:** 0x00
- **TLV de FIN:** 0x00

En el campo MEL se incluye el nivel de MEG de la PDU del APS.

El formato de la información específica de la APS en cada PDU de la APS se define conforme a la siguiente figura 11-2:



**Figura 11-2/G.8031/Y.1342 – Formato de información específica de la APS**

En el cuadro 11-1 se describen los puntos de código y los valores de la información específica de la APS.

**Cuadro 11-1/G.8031/Y.1342 – Puntos de código y valores de campo para la información específica de la APS**

Petición/Estado	1111	Exclusión de protección (LO)	Prioridad
	1110	Protección para fallo de señal (SF-P)	más alta
	1101	Conmutación forzada (FS)	
	1011	Fallo de señal para entidad de trabajo (SF)	
	1001	Degradación de señal (SD) (nota 1)	
	0111	Conmutación manual (MS)	
	0101	Espera para la restauración (WTR)	
	0100	Ejercicio (EXER)	
	0010	Petición de revertir (RR) (nota 2)	
	0001	No revertir (DNR)	
	0000	Ninguna petición (NR)	más baja
	Otros	Reservado para normalización internacional futura	
Tipo de protección	A	0	Sin canal de APS
		1	Canal de la APS
	B	0	1+1 (puente permanente)
		1	1:1 (sin puente permanente)
	D	0	Conmutación unidireccional
		1	Conmutación bidireccional
	R	0	Operación no reversible
		1	Operación reversible
Señal solicitada	0	Señal nula	
	1	Señal de tráfico normal	
	2-255	(Reservado para uso futuro)	
Señal puenteadada	0	Señal nula	
	1	Señal de tráfico normal	
	2-255	(Reservado para uso futuro)	
NOTA 1 – SD queda en estudio.			
NOTA 2 – RR se reserva para normalización futura del UIT-T.			

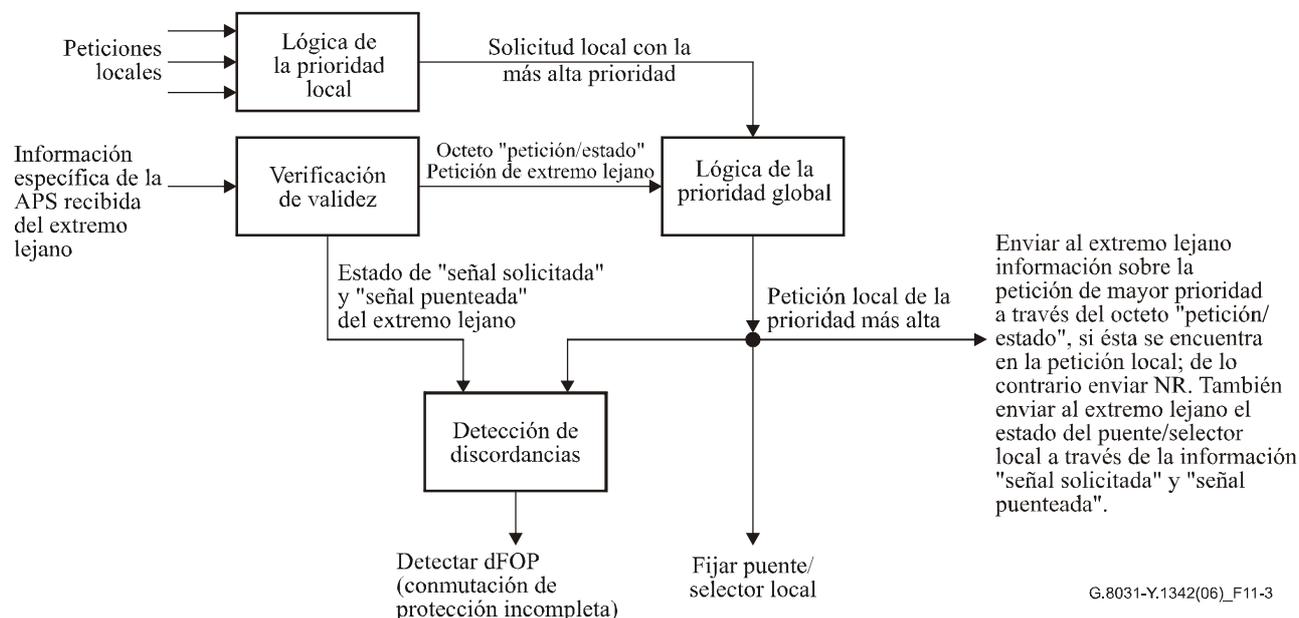
En las arquitecturas de protección soportadas que se describen en la cláusula 10, se ha de utilizar el protocolo APS de una fase.

## 11.2 Protocolo APS de una fase

### 11.2.1 Fundamentos del funcionamiento

En la figura 11-3 se ilustran los fundamentos del algoritmo de conmutación de protección lineal 1+1/1:1. Este algoritmo se ejecuta en los elementos de red en los dos extremos del dominio protegido (las ubicaciones OESTE y ESTE). La conmutación bidireccional se logra mediante la transmisión de peticiones de conmutación locales al extremo lejano utilizando el campo "petición/estado" del primer octeto de la información específica del APS (véase la figura 11-2). La "señal solicitada" y "señal puenteadada" transmitidas en el segundo y tercer octeto de la información

específica del APS contienen la información de estado del puente/selector local; por lo tanto se puede detectar y emitir una alarma en caso de existir una discordancia persistente entre los dos extremos.



**Figura 11-3/G.8031/Y.1342 – Fundamentos del algoritmo de conmutación de protección lineal 1+1/1:1**

A continuación se describe el funcionamiento detallado (véase la figura 11-3):

Puede haber una o varias peticiones de conmutación de protección locales activas (conforme se indica en 9.1 y en 9.2) en el elemento de red local. La "lógica de prioridad local" determina cuál de estas peticiones es la de mayor prioridad, utilizando el orden de prioridad que se presenta en el cuadro 11-1. Esta información de petición local de mayor prioridad se entrega a la "lógica de prioridad global".

El elemento de red local recibe información del elemento de red del extremo lejano mediante la información específica del protocolo APS. La información específica del APS recibida se somete a una verificación de validez (véase 11.2.4). La información de la "petición/estado" recibida (que indica la petición local de la más alta prioridad del extremo lejano) se entrega luego a la "lógica de de la prioridad local". La "lógica de prioridad global" compara la petición local de mayor prioridad con la de la petición de la información de "petición/estado" recibida (de conformidad con el orden de prioridades del cuadro 11-1) a fin de determinar la petición global de mayor prioridad. Si la petición global de mayor prioridad es la petición local, esto se indicará en el campo "petición/estado", de lo contrario se indicará "NR". Esta petición determina luego la posición del puente/selector (o el estado) del elemento de red local, de la siguiente forma:

- en arquitecturas 1+1, solamente se controla la posición del selector. En arquitecturas 1:1, se operan tanto la posición del puente como la del selector a fin de seleccionar una misma posición;
- si la petición global de mayor prioridad es una petición para una entidad de trabajo, se puentea/conmuta el tráfico de trabajo correspondiente hacia/desde la entidad de protección. Es decir, el correspondiente puente/selector del elemento de red local selecciona la entidad

de protección. Una petición de conmutación para una entidad de trabajo significa que se trata de una petición de conmutar de una entidad de trabajo a la entidad de protección.

El estado del puente/selector se transmite al extremo lejano mediante las señales "señal de petición" y "señal puenteada" (con la codificación que se describe en el cuadro 11-1). Este estado también se compara con el estado del puente/selector del extremo lejano indicado por la "señal de petición" y "señal puenteada" recibidas. Obsérvese que el algoritmo de conmutación de protección lineal comienza inmediatamente cada vez que cambia una de las señales de entrada (véase la figura 11-3), es decir, cuando cambia el estado de cualquier petición local, o cuando se recibe del extremo lejano información diferente específica del APS. También se inician inmediatamente las acciones subsiguientes del algoritmo, es decir, cambiar la posición del puente/selector local (de ser necesario), transmitir nueva información específica del APS o detectar dFOP si la conmutación de protección no finaliza en el periodo especificado en la cláusula 11.15.

### **11.2.2 Modo reversible**

En el modo de funcionamiento reversible se ingresa a un estado de espera para el restablecimiento cuando se está recibiendo tráfico de trabajo a través de la entidad de protección, si algunas peticiones de conmutación de protección locales (véase la figura 11-3) que habían estado activas pasan a inactivas. Como este estado representa ahora la petición local de mayor prioridad, se indica en la información "petición/estado" transmitida y se mantiene la conmutación.

Normalmente este estado finaliza y pasa a un estado sin petición una vez expira el temporizador de espera para el restablecimiento. El temporizador de espera para el restablecimiento se desactiva antes si aparece alguna petición local de mayor prioridad con precedencia sobre este estado.

Cabe señalar que para la decisión de si se ingresa o no al estado de espera para el restablecimiento, únicamente se tienen en cuenta las peticiones locales. Un estado local de espera para el restablecimiento o una petición distante (espera para el restablecimiento u otra) recibida a través de la información "petición/estado" pueden hacer que se mantenga la conmutación hacia la entidad de protección. Por lo tanto, si se ha producido un fallo bidireccional de la entidad de trabajo y se ha llevado a cabo la reparación subsiguiente, no tiene lugar la reversión bidireccional hacia la entidad de trabajo sino hasta que hayan expirado los dos temporizadores de espera para el restablecimiento ubicados en los dos extremos.

### **11.2.3 Modo no reversible**

En el modo de operación no reversible, se ingresa a un estado local de no reversión cuando se está transmitiendo tráfico de trabajo a través de la entidad de protección, si algunas peticiones locales de conmutación de protección (véase la figura 11-3) que habían estado activas pasan ahora a inactivas. Como este estado representa ahora la petición local de mayor prioridad, se indica en la información "petición/estado" transmitida y se mantiene la conmutación, evitando así que en el modo no reversible se regrese a la posición del puente/selector abandonada, si no existen peticiones.

### **11.2.4 Transmisión y aceptación del APS**

Las unidades de tráfico que transportan PDU del APS se denominan tramas APS. Las tramas APS se transportan únicamente mediante la entidad de transporte de protección, puesto que son introducidas por el extremo de cabecera del dominio protegido y extraídas por el extremo de cola del dominio protegido.

Se debe transmitir una nueva trama de APS inmediatamente se produzca un cambio en el estado transmitido (véase la figura 11-3).

Deben transmitirse las primeras tres tramas del APS tan rápido como sea posible tras el cambio de estado del punto extremo de protección, de forma que pueda realizarse la conmutación de

protección rápida aun si se pierden o se dañan una o dos tramas del APS. Para realizar esta conmutación de protección rápida en 50 ms, el intervalo de tiempo en que se transmiten las primeras tres tramas del APS es preferiblemente de 3,3 ms, que es el mismo intervalo de tiempo de las tramas del CCM utilizado para la detección rápida de defectos. Una vez transmitidas las primeras tres tramas, se deben transmitir tramas APS en un intervalo de tiempo de 5 segundos.

Si no se recibe información válida específica del APS, permanece vigente la última información válida recibida. Si se detecta una condición de fallo de señal en la entidad de transporte de protección, se debe evaluar la información específica del APS recibida.

Si un punto extremo de protección recibe de la entidad de trabajo información específica del APS, debe hacer caso omiso a esta información y detectar el defecto de fallo de protocolo en el elemento de red local (véase 11.15).

### **11.3 Tipo de petición**

Los tipos de petición que pueden indicarse en la información específica del APS son los tipos "normales" soportados habitualmente por la conmutación de protección de SONET y SDH. Estas peticiones indican la circunstancia, instrucción o estado de mayor prioridad. En el caso de conmutación unidireccional, se trata del valor de mayor prioridad determinado únicamente por el extremo cercano. En conmutación bidireccional, se indicará la petición local únicamente si tiene una prioridad al menos igual que la de cualquier petición recibida del extremo cercano mediante la comunicación APS, en caso contrario se indicará NR. En el protocolo APS de una fase, el extremo cercano nunca indicará petición de revertir ni siquiera si la petición del extremo lejano tiene la prioridad más alta.

### **11.4 Tipos de protección**

Los tipos válidos de protección son:

000x	1+1 Unidireccional, sin comunicación APS
100x	1+1 Unidireccional con comunicación APS
101x	1+1 Bidireccional con comunicación APS
111x	1:1 Bidireccional con comunicación APS

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

Obsérvese que 010x, 001x y 011x no son válidos ya que 1:1 y bidireccional requieren de comunicación APS.

Si el bit "B" no concuerda, se libera el selector ya que 1:1 y 1+1 son incompatibles. Esto dará como resultado un defecto.

Siempre y cuando el bit "B" concuerde:

Si el bit "A" no concuerda, el lado que espera recibir APS regresará a conmutación unidireccional 1+1 sin comunicación APS.

Si el bit "D" no concuerda, el lado bidireccional regresará a conmutación unidireccional.

Si el bit "R" no concuerda, uno de los lados fijará los conmutadores a "WTR" y el otro lado los fijará a "DNR". Los dos lados interfundionarán y el tráfico estará protegido.

### **11.5 Señal solicitada**

La señal solicitada indica la señal que el extremo cercano solicita se transporte por el camino de protección. Para NR se trata de la señal nula si el extremo lejano no está puenteando la señal normal

hacia la entidad de protección. Si el extremo lejano está puenteando la señal de tráfico normal hacia la entidad de protección, la señal solicitada es la señal de tráfico normal para NR; para LO, ésta puede únicamente ser la señal nula. Para Ejercicio, ésta puede ser la señal nula si Ejercicio sustituye a NR, o la señal de tráfico normal si Ejercicio sustituye a DNR. Para SF (o SD si es procedente), ésta será la señal de tráfico normal, o la señal nula para indicar que la protección falló o se degradó. Para las demás peticiones, ésta será la señal de tráfico normal que se solicitó se transporte a través de la entidad de transporte de protección.

### **11.6 Señal puenteada**

Ésta indica la señal puenteada hacia el camino de protección. En protección 1+1, ésta debería siempre indicar la señal de tráfico normal evidenciando con precisión la posición del puente permanente. Para la protección 1:1, ésta indicará lo que en realidad se está puenteando hacia la entidad de protección (bien sea la señal nula o la señal de tráfico normal). Por lo general ésta será el puente solicitado por el extremo lejano.

### **11.7 Control del puente**

En las arquitecturas 1+1 la señal de tráfico normal siempre se puentea hacia la protección. El campo de señal puenteada de la información APS siempre indicará la señal de tráfico normal.

En las arquitecturas 1:1, el puente se fijará a lo señalado por el campo "Señal solicitada" de la información APS entrante. Una vez establecido el puente, esto se indicará en el campo "Señal puenteada" de la información APS saliente.

### **11.8 Control del selector**

En las arquitecturas unidireccionales 1+1 (con o sin comunicación APS), el selector se fija por completo conforme a la petición local de mayor prioridad. Se trata de un conmutador de una sola fase.

En las arquitecturas bidireccionales 1+1, se seleccionará la señal de tráfico normal de la entidad de protección cuando la "Señal solicitada" indique la señal de tráfico normal.

En las arquitecturas bidireccionales 1:1, se seleccionará la señal de tráfico normal de la entidad de protección cuando el número aparezca en la "Señal solicitada" de salida.

### **11.9 Fallo de señal de la entidad de transporte de protección**

El fallo de señal en la entidad de transporte de protección tiene una prioridad más alta que cualquier defecto que podría ocasionar que se seleccione una señal de tráfico normal de la protección. En caso que se esté utilizando una señal del APS, una SF-P en la entidad de transporte de protección (sobre la cual se encamina la señal del APS) tiene prelación sobre la conmutación forzada. La instrucción de exclusión tiene una prioridad mayor que SF-P: se ha de mantener activo el estado de exclusión durante el fallo.

### **11.10 Peticiones con la misma prioridad**

Por lo general, una vez se ha finalizado una conmutación como consecuencia de una petición, ninguna otra petición con la misma prioridad (comportamiento primero en llegar, primero en ser atendido) anulará la conmutación. Se consideran válidas las peticiones con una misma prioridad provenientes de ambos lados del grupo de protección bidireccional.

### **11.11 Aceptación y acogida de instrucciones**

Las instrucciones CLEAR, LO, FS, MS y EXER se aceptan o se rechazan dependiendo de las instrucciones precedentes, el estado de las entidades de trabajo y de protección en el grupo de trabajo y (únicamente para la conmutación bidireccional) de la información APS recibida.

La instrucción CLEAR es válida únicamente si tiene una instrucción LO, FS, MS o EXER del extremo cercano o si en el extremo cercano existe el estado WTR, y se rechaza en caso contrario. Esta instrucción suprimirá la instrucción del extremo cercano o el estado WTR, permitiendo así que tenga efecto la siguiente situación de prioridad más baja o (en conmutación bidireccional) la petición APS.

Se rechazan las demás instrucciones salvo que sean de una prioridad mayor que la instrucción, condición o (en conmutación bidireccional) petición APS anterior vigente. Si se acepta una nueva instrucción, se olvida cualquier instrucción anterior de menor prioridad que resulte anulada. Si una instrucción de mayor prioridad anula una situación de prioridad menor o (en conmutación bidireccional) una petición APS, se hará valer dicha otra petición si ésta aún existe en el momento en que se elimina la instrucción.

Si una instrucción resulta anulada por una situación o (en conmutación bidireccional) petición APS, se olvida dicha instrucción.

### **11.12 Temporizador de espera**

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

Cada grupo de protección debe tener un temporizador de espera configurable. La gama sugerida es de 0 a 10 segundos en pasos de 100 ms (precisión de  $\pm 5$  ms).

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

### **11.13 Temporizador de espera para el restablecimiento**

En el modo de funcionamiento reversible, para evitar la operación frecuente del conmutador de protección debido a un defecto intermitente, una entidad de transporte de servicio fallida debe convertirse en una entidad libre de fallos. 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. El operador puede configurar este periodo, denominado periodo de espera para el restablecimiento (WTR), entre 5 y 12 minutos, en pasos de 1 minuto. Su valor por defecto es de 5 minutos. Una condición SF (o SD, si es precedente) anulará la WTR.

En modo de funcionamiento reversible, cuando ya no se solicita la protección, es decir, la entidad de transporte de servicio fallida ya no está en condición SD (o SF, si es procedente) (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. El temporizador de espera para el restablecimiento se desactiva antes cuando cualquier petición con prioridad superior toma el lugar de este estado.

#### 11.14 Instrucción ejercicio

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

La instrucción ejercicio emitirá la instrucción con los mismos números de entidad solicitada y puenteada de la petición NR o DNR que sustituye. En el protocolo APS de 1 fase, la respuesta válida será una NR con los números de entidad solicitada y puenteada correspondientes. La respuesta normal a DNR debería ser DNR en lugar de NR. Cuando se elimina la instrucción ejercicio, se sustituirá por NR si el número de entidad solicitada es 0, y por DNR para cualquier número de señal de tráfico normal 1.

#### 11.15 Defectos de fallo del protocolo

En el cuadro 11-2 a continuación se presentan los criterios de entrada y de salida del fallo por defectos del protocolo (dFOP, *failure of protocol defect*) APS definido en esta Recomendación.

**Cuadro 11-2/G.8031/Y.1342 – Criterios de entrada y salida del dFOP**

<b>Aprovisionamiento completamente incompatible (la discordancia del bit "B")</b>	
Criterio de entrada	Recepción de tres tramas APS con valores incompatibles del bit "B", en el periodo de 22,5 segundos.
Criterio de salida	Recepción de la primera trama APS con un valor compatible del bit "B".
<b>Conmutación de protección incompleta</b>	
Criterio de entrada	Si las señales "señal solicitada" transmitida y "señal puenteada" recibida no concuerdan durante un periodo de al menos 50 ms.
Criterio de salida	Recepción de la primera trama APS que indica una "señal puenteada" con el mismo valor que el de la "señal solicitada" transmitida.
<b>Discordancia entre las configuraciones de trabajo y de protección</b>	
Criterio de entrada	Recepción de tres tramas APS de la entidad de transporte de trabajo en el periodo de 22,5 segundos.
Criterio de salida	Si no se recibe ninguna trama APS de la entidad de transporte de trabajo en el periodo de 22,5 segundos.
NOTA – En 22,5 segundos se pueden recibir tres tramas APS aún si se pierden dos tramas APS.	

Se hará caso omiso de peticiones desconocidas y de peticiones de número de señal no válidos.

## **Anexo A**

### **Cuadros de transición de estado para la conmutación de protección**

En este anexo se describen los cuadros de transición de estado de las siguientes configuraciones de conmutación de protección.

- Bidireccional 1:1 (modo reversible, modo no reversible).
- Bidireccional 1+1 (modo reversible, modo no reversible).
- Unidireccional 1+1 (modo reversible, modo no reversible.)

#### **A.1 Transición de estado de la conmutación bidireccional 1:1 con modo reversible**

##### **A.1.1 Peticiones locales**

En el cuadro A.1 se presenta la transición de estado causada por una petición local en la conmutación de protección 1:1 en modo reversible.

**Cuadro A.1/G.8031/Y.1342 – Transición de estado causada por peticiones locales (1:1, bidireccional, modo reversible)**

Estado	APS señalado	Petición local										
		a	b	c	d	e	f	g	h	i	j	
		Exclusión	Commutación forzada	Fallo de señal en entidad de trabajo	Entidad de trabajo se recupera de SF	Fallo de señal en entidad de protección	Entidad de protección se recupera de SF	Commutación manual	Eliminar	Ejercicio	Expira el temporizador WTR	
A	Sin petición De trabajo/Activa Protección/Reserva	NR [r/b=nula]	→C	→D	→E <sup>a)</sup>	N/A	→F	N/A	→G	O	→I	N/A
B	Ninguna petición De trabajo/Reserva Protección/Activa	NR [r/b=normal]	→C	→D	(→B) <sup>b)</sup> o →E	O	→F	N/A	→G	O	O	N/A
C	Exclusión De trabajo/Activa Protección/Reserva	LO [r/b=nula]	O	O	O	O	O	O	O	→A <sup>o)</sup> →E <sup>c)</sup> →F <sup>d)</sup>	O	N/A
D	Commutación forzada De trabajo/Reserva Protección/Activa	FS [r/b=normal]	→C	O	O	O	→F	N/A	O	→A <sup>o)</sup> →E <sup>c)</sup>	O	N/A
E	Fallo de señal (Trab) De trabajo/Reserva Protección/Activa	SF [r/b=normal]	→C	→D	N/A	→H	→F	N/A	O	O	O	N/A
F	Fallo de señal (P) De trabajo/Activa Protección/Reserva	SF-P [r/b=nula]	→C	O	O	O	N/A	→A	O	O	O	N/A
G	Commutación manual De trabajo/Reserva Protección/Activa	MS [r/b=normal]	→C	→D	→E	N/A	→F	N/A	O	→A	O	N/A
H	Espera para restablecimiento De trabajo/Reserva Protección/Activa	WTR [r/b=normal]	→C	→D	→E	N/A	→F	N/A	→G	→A	O	→A
I	Ejercicio De trabajo/Activa Protección/Reserva	EXER [r/b=nula]	→C	→D	→E	N/A	→F	N/A	→G	→A	O	N/A

NOTA 1 – "N/A" significa que el evento no puede ocurrir en el estado.  
 NOTA 2 – "O" significa que la condición actual anulará la petición, porque la petición tiene una prioridad menor.  
 NOTA 3 – "(→X)" indica que el estado no cambia y sigue siendo el mismo.

<sup>a)</sup> Cambia al estado E si el fallo de señal persiste después de que expire temporizador de espera.  
<sup>b)</sup> Si en el APS recibido del extremo lejano está indicado FS.  
<sup>c)</sup> Si se ratifica SF.  
<sup>d)</sup> Si se ratifica SF-P.

## A.1.2 Peticiones del extremo lejano

En el cuadro A.2 se presenta la transición de estado causada por una petición del extremo lejano recibida por el APS en conmutación de protección bidireccional 1:1 en modo reversible.

**Cuadro A.2/G.8031/Y.1342 – Transición de estado causada por peticiones del extremo lejano (1:1, bidireccional, modo reversible)**

Estado	APS señalado	Petición del extremo lejano recibida									
		k	l	m	n	o	p	q	r	s	
		LO [r/b=nula]	SF-P [r/b=nula]	FS [r/b=normal]	SF [r/b=normal]	MS [r/b=normal]	WTR [r/b=normal]	EXER [r/b=nula]	NR [r/b=nula]	NR [r/b=normal]	
A	Ninguna petición De trabajo/Activa Protección/Reserva	NR [r/b=nula]	(→A)	(→A)	→B	→B	→B	N/A	(→A)	(→A) o →E <sup>a)</sup> o →F <sup>b)</sup>	(→A)
B	Ninguna petición De trabajo/Reserva Protección/Activa	NR [r/b=normal]	→A	→A	(→B)	(→B)	(→B)	(→B)	N/A	→A o →E <sup>a)</sup>	N/A
C	Exclusión De trabajo/Activa Protección/Reserva	LO [r/b=nula]	(→C)	O	O	O	O	O	O	O	O
D	Conmutación forzada De trabajo/Reserva Protección/Activa	FS [r/b=normal]	→A	→A	(→D)	O	O	O	O	O	O
E	Fallo de señal (Trab) De trabajo/Reserva Protección/Activa	SF [r/b=normal]	→A	→A	→B	(→E)	O	O	O	O	O
F	Fallo de señal (P) De trabajo/Activa Protección/Reserva	SF-P [r/b=nula]	→A	(→F)	O	O	O	O	O	O	O
G	Conmutación manual De trabajo/Reserva Protección/Activa	MS [r/b=normal]	→A	→A	→B	→B	(→G)	O	O	O	O
H	Espera para restablecimiento De trabajo/Reserva Protección/Activa	WTR [r/b=normal]	→A	→A	→B	→B	→B	(→H)	O	N/A	O
I	Ejercicio De trabajo/Activa Protección/Reserva	EXER [r/b=nula]	→A	→A	→B	→B	→B	N/A	(→I)	O	N/A

NOTA 1 – "N/A" significa que el evento no puede ocurrir en el estado.  
 NOTA 2 – "O" significa que la condición actual anulará la petición, porque la petición tiene una prioridad menor.  
 NOTA 3 – "(→X)" indica que el estado no cambia y sigue siendo el mismo.  
<sup>a)</sup> Si se ratifica SF.  
<sup>b)</sup> Si se ratifica SF-P.

## A.2 Transición de estado para conmutación bidireccional 1:1 en modo no reversible

### A.2.1 Peticiones locales

En el cuadro A.3 se presenta la transición de estado causada por una petición local en la conmutación de protección bidireccional 1:1 en modo no reversible.

**Cuadro A.3/G.8031/Y.1342 – Transición de estado causada por peticiones locales  
(1:1, bidireccional, modo no reversible)**

Estado	APS señalado	Petición local									
		a	b	c	d	e	f	g	h	i	
		Exclusión	Conmutación forzada	Fallo de señal en entidad de trabajo	Entidad de trabajo se recupera de SF	Fallo de señal en entidad de protección	Entidad de protección se recupera de SF	Conmutación manual	Eliminar	Ejercicio	
A	Ninguna petición De trabajo/Activa Protección/Reserva	NR [r/b=nula]	→C	→D	→E <sup>a)</sup>	N/A	→F	N/A	→G	O	→I
B	Ninguna petición De trabajo/Reserva Protección/Activa	NR [r/b=normal]	→C	→D	(→B) <sup>b)</sup> o →E	N/A	→F	N/A	→G	O	O
C	Exclusión De trabajo/Activa Protección/Reserva	LO [r/b=nula]	O	O	O	O	O	O	O	→A o →E <sup>c)</sup> →F <sup>d)</sup>	O
D	Conmutación forzada De trabajo/Reserva Protección/Activa	FS [r/b=normal]	→C	O	O	O	→F	N/A	O	→H o →E <sup>c)</sup>	O
E	Fallo de señal (Trab) De trabajo/Reserva Protección/Activa	SF [r/b=normal]	→C	→D	N/A	→H	→F	N/A	O	O	O
F	Fallo de señal (P) De trabajo/Activa Protección/Reserva	SF-P [r/b=nula]	→C	O	O	O	N/A	→A	O	O	O
G	Conmutación manual De trabajo/Reserva Protección/Activa	MS [r/b=normal]	→C	→D	→E	N/A	→F	N/A	O	→H	O
H	No revertir De trabajo/Reserva Protección/Activa	DNR [r/b=normal]	→C	→D	→E	N/A	→F	N/A	→G	O	→J
I	Ejercicio De trabajo/Activa Protección/Reserva	EXER [r/b=nula]	→C	→D	→E	N/A	→F	N/A	→G	→A	O
J	Ejercicio De trabajo/Reserva Protección/Activa	EXER [r/b=normal]	→C	→D	→E	N/A	→F	N/A	→G	→H	O

NOTA 1 – "N/A" significa que el evento no puede ocurrir en el estado.  
 NOTA 2 – "O" significa que la condición actual anulará la petición, porque la petición tiene una prioridad menor.  
 NOTA 3 – "(→X)" indica que el estado no cambia y sigue siendo el mismo.  
<sup>a)</sup> Cambia al estado E si el fallo de señal persiste después de que expire temporizador de espera.  
<sup>b)</sup> Si en el APS recibido del extremo lejano está indicado FS.  
<sup>c)</sup> Si se ratifica SF.  
<sup>d)</sup> Si se ratifica SF-P.

## A.2.2 Peticiones de extremo lejano

En el cuadro A.4 se presenta la transición de estado causada por una petición de extremo lejano recibida por el APS en la conmutación de protección bidireccional 1:1 en modo no reversible.

**Cuadro A.4/G.8031/Y.1342 – Transición de estado causada por peticiones de extremo lejano (1:1, bidireccional, modo no reversible)**

Estado	APS señalado	Petición de extremo lejano recibida										
		k	l	m	n	o	q	r	s	t	u	
		LO [r/b=nula]	SF-P [r/b=nula]	FS [r/b=normal]	SF [r/b=normal]	MS [r/b=normal]	EXER [r/b=nula]	EXER [r/b=normal]	NR [r/b=nula]	NR [r/b=normal]	DNR [r/b=normal]	
A	Ninguna petición De trabajo/Activa Protección/Reserva	NR [r/b=nula]	(→A)	(→A)	→B	→B	→B	(→A)	N/A	(→A) o →E <sup>a)</sup> o →F <sup>b)</sup>	(→A)	N/A
B	Ninguna petición De trabajo/Reserva Protección/Activa	NR [r/b=normal]	→A	→A	(→B)	(→B)	(→B)	N/A	(→B)	→A o →E <sup>a)</sup>	N/A	(→B)
C	Exclusión De trabajo/Activa Protección/Reserva	LO [r/b=nula]	(→C)	O	O	O	O	O	O	O	O	O
D	Conmutación forzada De trabajo/Reserva Protección/Activa	FS [r/b=normal]	→A	→A	(→D)	O	O	O	O	O	O	O
E	Fallo de señal (Trab) De trabajo/Reserva Protección/Activa	SF [r/b=normal]	→A	→A	→B	(→E)	O	O	O	O	O	O
F	Fallo de señal (P) De trabajo/Activa Protección/Reserva	SF-P [r/b=nula]	→A	(→F)	O	O	O	O	O	O	O	O
G	Conmutación manual De trabajo/Reserva Protección/Activa	MS [r/b=normal]	→A	→A	→B	→B	(→G)	O	O	O	O	O
H	No revertir De trabajo/Reserva Protección/Activa	DNR [r/b=normal]	→A	→A	→B	→B	→B	N/A	(→H)	O	O	(→H)
I	Ejercicio De trabajo/Activa Protección/Reserva	EXER [r/b=nula]	→A	→A	→B	→B	→B	(→I)	N/A	O	O	N/A
J	Ejercicio De trabajo/Reserva Protección/Activa	EXER [r/b=normal]	→A	→A	→B	→B	→B	N/A	(→J)	O	O	O

NOTA 1 – "N/A" significa que el evento no puede ocurrir en el estado.  
NOTA 2 – "O" significa que la condición actual anulará la petición, porque la petición tiene una prioridad menor.  
NOTA 3 – "(→X)" indica que el estado no cambia y sigue siendo el mismo.  
<sup>a)</sup> Si se ratifica SF.  
<sup>b)</sup> Si se ratifica SF-P.

### A.3 Transición de estado para conmutación bidireccional 1+1 con modo reversible

#### A.3.1 Peticiones locales

En el cuadro A.5 se presenta la transición de estado causada por una petición local en la conmutación de protección bidireccional 1+1 en modo reversible.

**Cuadro A.5/G.8031/Y.1342 – Transición de estado causada por peticiones locales (1+1, bidireccional, modo reversible)**

Estado	APS señalado	Petición local										
		a	b	c	d	e	f	g	h	i	j	
		Exclusión	Conmutación forzada	Fallo de señal en entidad de trabajo	Entidad de trabajo se recupera de SF	Fallo de señal en entidad de protección	Entidad de protección se recupera de SF	Conmutación manual	Eliminar	Ejercicio	Expira el temporizador WTR	
A	Ninguna petición De trabajo/Activa Protección/Reserva	NR [r/b=nula/normal]	→C	→D	→E <sup>a)</sup>	N/A	→F	N/A	→G	O	→I	N/A
B	Ninguna petición De trabajo/Reserva Protección/Activa	NR [r/b=normal]	→C	→D	(→B) <sup>b)</sup> o →E	O	→F	N/A	→G	O	O	N/A
C	Exclusión De trabajo/Activa Protección/Reserva	LO [r/b=nula/normal]	O	O	O	O	O	O	O	→A <sup>c)</sup> o →E <sup>c)</sup> →F <sup>d)</sup>	O	N/A
D	Conmutación forzada De trabajo/Reserva Protección/Activa	FS [r/b=normal]	→C	O	O	O	→F	N/A	O	→A <sup>c)</sup> o →E <sup>c)</sup>	O	N/A
E	Fallo de señal (Trab) De trabajo/Reserva Protección/Activa	SF [r/b=normal]	→C	→D	N/A	→H	→F	N/A	O	O	O	N/A
F	Fallo de señal (P) De trabajo/Activa Protección/Reserva	SF-P [r/b=nula/normal]	→C	O	O	O	N/A	→A	O	O	O	N/A
G	Conmutación manual De trabajo/Reserva Protección/Activa	MS [r/b=normal]	→C	→D	→E	N/A	→F	N/A	O	→A	O	N/A
H	Espera para restablecimiento De trabajo/Reserva Protección/Activa	WTR [r/b=normal]	→C	→D	→E	N/A	→F	N/A	→G	→A	O	→A
I	Ejercicio De trabajo/Activa Protección/Reserva	EXER [r/b=nula/normal]	→C	→D	→E	N/A	→F	N/A	→G	→A	O	N/A

NOTA 1 – "N/A" significa que el evento no puede ocurrir en el estado.  
 NOTA 2 – "O" significa que la condición actual anulará la petición, porque la petición tiene una prioridad menor.  
 NOTA 3 – "(→X)" indica que el estado no cambia y sigue siendo el mismo.  
<sup>a)</sup> Cambia al estado E si el fallo de señal persiste después de que expire temporizador de espera.  
<sup>b)</sup> Si en el APS recibido del extremo lejano está indicado FS.  
<sup>c)</sup> Si se ratifica SF.  
<sup>d)</sup> Si se ratifica SF-P.

### A.3.2 Peticiones de extremo lejano

En el cuadro A.6 se presenta la transición de estado causada por una petición de extremo lejano recibida por el APS en la conmutación de protección bidireccional 1+1 en modo reversible.

**Cuadro A.6/G.8031/Y.1342 – Transición de estado causada por peticiones de extremo lejano (1+1, bidireccional, modo reversible)**

Estado	Petición	Petición de extremo lejano recibida									
		k	l	m	n	o	p	q	r	s	
		LO [r/b= nula/normal]	SF-P [r/b= nula/normal]	FS [r/b=normal]	SF [r/b=normal]	MS [r/b=normal]	WTR [r/b=normal]	EXER [r/b=nula/normal]	NR [r/b=nula/normal]	NR [r/b=normal]	
A	Ninguna petición De trabajo/Activa Protección/Reserva	NR [r/b=nula/normal]	(→A)	(→A)	→B	→B	→B	N/A	(→A)	(→A) o →E <sup>a)</sup> o →F <sup>b)</sup>	(→A)
B	Ninguna petición De trabajo/Reserva Protección/Activa	NR [r/b=normal]	→A	(→A)	(→B)	(→B)	(→B)	(→B)	N/A	→A o →E <sup>a)</sup>	N/A
C	Exclusión De trabajo/Activa Protección/Reserva	LO [r/b=nula/normal]	(→C)	O	O	O	O	O	O	O	O
D	Conmutación forzada De trabajo/Reserva Protección/Activa	FS [r/b=normal]	→A	→A	(→D)	O	O	O	O	O	O
E	Fallo de señal (Trab) De trabajo/Reserva Protección/Activa	SF [r/b=normal]	→A	→A	→B	(→E)	O	O	O	O	O
F	Fallo de señal (P) De trabajo/Activa Protección/Reserva	SF-P [r/b=nula/normal]	→A	(→F)	O	O	O	O	O	O	O
G	Conmutación manual De trabajo/Reserva Protección/Activa	MS [r/b=normal]	→A	→A	→B	→B	(→G)	O	O	O	O
H	Espera para restablecimiento De trabajo/Reserva Protección/Activa	WTR [r/b=normal]	→A	→A	→B	→B	→B	(→H)	O	N/A	O
I	Ejercicio De trabajo/Activa Protección/Reserva	EXER [r/b =nula/normal]	→A	→A	→B	→B	→B	N/A	(→I)	O	N/A

NOTA 1 – "N/A" significa que el evento no puede ocurrir en el estado.  
NOTA 2 – "O" significa que la condición actual anulará la petición, porque la petición tiene una prioridad menor.  
NOTA 3 – "(→X)" indica que el estado no cambia y sigue siendo el mismo.  
<sup>a)</sup> Si se ratifica SF.  
<sup>b)</sup> Si se ratifica SF-P.

## A.4 Transición de estado para conmutación bidireccional 1+1 con modo no reversible

### A.4.1 Peticiones locales

En el cuadro A.7 se presenta la transición de estado causada por una petición local en la conmutación de protección bidireccional 1+1 en modo no reversible.

**Cuadro A.7/G.8031/Y.1342 – Transición de estado causada por peticiones locales  
(1+1, bidireccional, modo no reversible)**

Estado	APS señalado	Petición local									
		a	b	c	d	e	f	g	h	i	
		Exclusión	Conmutación forzada	Fallo de señal en entidad de trabajo	Entidad de trabajo se recupera de SF	Fallo de señal en entidad de protección	Entidad de protección se recupera de SF	Conmutación manual	Eliminar	Ejercicio	
A	Ninguna petición De trabajo/Activa Protección/Reserva	NR [r/b=nula/normal]	→C	→D	→E <sup>a)</sup>	N/A	→F	N/A	→G	O	→I
B	Ninguna petición De trabajo/Reserva Protección/Activa	NR [r/b=normal]	→C	→D	(→B) <sup>b)</sup> o →E	N/A	→F	N/A	→G	O	O
C	Exclusión De trabajo/Activa Protección/Reserva	LO [r/b=nula/normal]	O	O	O	O	O	O	O	→A <sup>o</sup> →E <sup>c)</sup> →F <sup>d)</sup>	O
D	Conmutación forzada De trabajo/Reserva Protección/Activa	FS [r/b=normal]	→C	O	O	O	→F	N/A	O	→H <sup>o</sup> →E <sup>c)</sup>	O
E	Fallo de señal (Trab) De trabajo/Reserva Protección/Activa	SF [r/b=normal]	→C	→D	N/A	→H	→F	N/A	O	O	O
F	Fallo de señal (P) De trabajo/Activa Protección/Reserva	SF-P [r/b=nula/normal]	→C	O	O	O	N/A	→A	O	O	O
G	Conmutación manual De trabajo/Reserva Protección/Activa	MS [r/b=normal]	→C	→D	→E	N/A	→F	N/A	O	→H	O
H	No revertir De trabajo/Reserva Protección/Activa	DNR [r/b=normal]	→C	→D	→E	N/A	→F	N/A	→G	N/A	→J
I	Ejercicio De trabajo/Activa Protección/Reserva	EXER [r/b=nula/normal]	→C	→D	→E	N/A	→F	N/A	→G	→A	O
J	Ejercicio De trabajo/Reserva Protección/Activa	EXER [r/b=normal]	→C	→D	→E	N/A	→F	N/A	→G	→H	O

NOTA 1 – "N/A" significa que el evento no puede ocurrir en el estado.  
 NOTA 2 – "O" significa que la condición actual anulará la petición, porque la petición tiene una prioridad menor.  
 NOTA 3 – "(→X)" indica que el estado no cambia y sigue siendo el mismo.  
<sup>a)</sup> Cambia al estado E si el fallo de señal persiste después de que expire temporizador de espera.  
<sup>b)</sup> Si en el APS recibido del extremo lejano está indicado FS.  
<sup>c)</sup> Si se ratifica SF.  
<sup>d)</sup> Si se ratifica SF-P.

## A.4.2 Peticiones de extremo lejano

En el cuadro A.8 se presenta la transición de estado causada por una petición de extremo lejano recibida por el APS en la conmutación de protección bidireccional en modo no reversible.

**Cuadro A.8/G.8031/Y.1342 – Transición de estado causada por peticiones de extremo lejano  
(1+1 bidireccional, modo no reversible)**

Estado	APS señalado	Petición de extremo lejano recibida										
		k	l	m	n	o	q	r	s	t	u	
		LO [r/b=nula/normal]	SF-P [r/b= nula/normal]	FS [r/b=normal]	SF [r/b=normal]	MS [r/b=normal]	EXER [r/b=nula/normal]	EXER [r/b=normal]	NR [r/b=nula/normal]	NR [r/b=normal]	DNR [r/b=normal]	
A	Ninguna petición De trabajo/Activa Protección/Reserva	NR [r/b=nula/normal]	(→A)	(→A)	→B	→B	→B	(→A)	N/A	(→A) o →E <sup>a)</sup> o →F <sup>b)</sup>	(→A)	N/A
B	Ninguna petición De trabajo/Reserva Protección/Activa	NR [r/b=normal]	→A	→A	(→B)	(→B)	(→B)	N/A	(→B)	→A o →E <sup>a)</sup>	N/A	(→B)
C	Exclusión De trabajo/Activa Protección/Reserva	LO [r/b= nula/normal]	(→C)	O	O	O	O	O	O	O	O	O
D	Conmutación forzada De trabajo/Reserva Protección/Activa	FS [r/b=normal]	→A	→A	(→D)	O	O	O	O	O	O	O
E	Fallo de señal (Trab) De trabajo/Reserva Protección/Activa	SF [r/b=normal]	→A	→A	→B	(→E)	O	O	O	O	O	O
F	Fallo de señal (P) De trabajo/Activa Protección/Reserva	SF-P [r/b= nula/normal]	→A	(→F)	O	O	O	O	O	O	O	O
G	Conmutación manual De trabajo/Reserva Protección/Activa	MS [r/b=normal]	→A	→A	→B	→B	(→G)	O	O	O	O	O
H	No revertir De trabajo/Reserva Protección/Activa	DNR [r/b=normal]	→A	→A	→B	→B	→B	N/A	(→H)	O	O	(→H)
I	Ejercicio De trabajo/Activa Protección/Reserva	EXER [r/b=nula/normal]	→A	→A	→B	→B	→B	(→I)	N/A	O	O	N/A
J	Ejercicio De trabajo/Reserva Protección/Activa	EXER [r/b=normal]	→A	→A	→B	→B	→B	N/A	(→J)	O	O	O

NOTA 1 – "N/A" significa que el evento no puede ocurrir en el estado.  
NOTA 2 – "O" significa que la condición actual anulará la petición, porque la petición tiene una prioridad menor.  
NOTA 3 – "(→X)" indica que el estado no cambia y sigue siendo el mismo.  
<sup>a)</sup> Si se ratifica SF.  
<sup>b)</sup> Si se ratifica SF-P.

## A.5 Transición de estado para 1+1 conmutación unidireccional con modo reversible

### A.5.1 Peticiones locales

En el cuadro A.9 se presenta la transición de estado causada por una petición local en la conmutación de protección unidireccional 1+1 en modo reversible.

**Cuadro A.9/G.8031/Y.1342 – Transición de estado causada por peticiones locales (1+1, unidireccional, modo reversible)**

Estado		Petición local									
		a	b	c	d	e	f	g	h	i	j
		Exclusión	Conmutación forzada	Fallo de señal en entidad de trabajo	Entidad de trabajo se recupera de SF	Fallo de señal en entidad de protección	Entidad de protección se recupera de SF	Conmutación manual	Eliminar	Ejercicio	Expira el temporizador WTR
A	Ninguna petición De trabajo/Activa Protección/Reserva	→B	→C	→D <sup>a)</sup>	N/A	→E	N/A	→F	O	N/A	N/A
B	Exclusión De trabajo/Activa Protección/Reserva	O	O	O	O	O	O	O	→A <sup>o</sup> →D <sup>b)</sup> →E <sup>c)</sup>	N/A	N/A
C	Conmutación forzada De trabajo/Reserva Protección/Activa	→B	O	O	O	→E	N/A	O	→A <sup>o</sup> →D <sup>c)</sup>	N/A	N/A
D	Fallo de señal (Trab) De trabajo/Reserva Protección/Activa	→B	→C	N/A	→G	→E	N/A	O	O	N/A	N/A
E	Fallo de señal (P) De trabajo/Activa Protección/Reserva	→B	O	O	O	N/A	→A	O	O	N/A	N/A
F	Conmutación manual De trabajo/Reserva Protección/Activa	→B	→C	→D	N/A	→E	N/A	O	→A	N/A	N/A
G	Espera para restablecimiento De trabajo/Reserva Protección/Activa	→B	→C	→D	N/A	→E	N/A	→F	→A	N/A	→A

NOTA 1 – "N/A" significa que el evento no puede ocurrir en el estado.  
 NOTA 2 – "O" significa que la condición actual anulará la petición, porque la petición tiene una prioridad menor.

<sup>a)</sup> Cambia al estado D si el fallo de señal persiste después de que expire temporizador de espera.  
<sup>b)</sup> Si se ratifica SF.  
<sup>c)</sup> Si se ratifica SF-P.

## A.6 Transición de estado para la conmutación unidireccional 1+1 con modo no reversible

### A.6.1 Peticiones locales

En el cuadro A.10 se presenta la transición de estado causada por una petición local en la protección de conmutación unidireccional 1+1 en modo no reversible.

**Cuadro A.10/G.8031/Y.1342 – Transición de estado causada por peticiones locales (1+1, unidireccional, modo no reversible)**

Estado		Petición local								
		a	b	c	d	e	f	G	i	j
		Exclusión	Conmutación forzada	Fallo de señal en entidad de trabajo	Entidad de trabajo se recupera de SF	Fallo de señal en entidad de protección	Entidad de protección se recupera de SF	Conmutación manual	Eliminar	Ejercicio
A	Ninguna petición De trabajo/Activa Protección/Reserva	→B	→C	→D <sup>a)</sup>	N/A	→E	N/A	→F	O	N/A
B	Exclusión De trabajo/Activa Protección/Reserva	O	O	O	O	O	O	O	→A o →D <sup>b)</sup> →E <sup>c)</sup>	N/A
C	Conmutación forzada De trabajo/Reserva Protección/Activa	→B	O	O	O	→E	N/A	O	→G o →D <sup>b)</sup>	N/A
D	Fallo de señal (Trab) De trabajo/Reserva Protección/Activa	→B	→C	N/A	→G	→E	N/A	O	O	N/A
E	Fallo de señal (P) De trabajo/Activa Protección/Reserva	→B	O	O	O	N/A	→A	O	O	N/A
F	Conmutación manual De trabajo/Reserva Protección/Activa	→B	→C	→D	N/A	→E	N/A	O	→G	N/A
G	No revertir De trabajo/Reserva Protección/Activa	→B	→C	→D	N/A	→E	N/A	→F	O	N/A

NOTA 1 – "N/A" significa que el evento no puede ocurrir en el estado.  
 NOTA 2 – "O" significa que la condición actual anulará la petición, porque la petición tiene una prioridad menor.

<sup>a)</sup> Cambia al estado D si el fallo de señal persiste después de que expire temporizador de espera.  
<sup>b)</sup> Si se ratifica SF.  
<sup>c)</sup> Si se ratifica SF-P.

## Apéndice I

### Ejemplo del funcionamiento del protocolo APS de una fase

#### I.1 Introducción

En este apéndice se muestran algunos ejemplos del funcionamiento del protocolo APS de una fase (1:1, modos reversible y no reversible).

#### I.2 Caso hipotético

##### I.2.1 Modo reversible

Para este ejemplo se supone el siguiente caso hipotético:

- 1) El dominio protegido funciona sin defectos (la entidad de trabajo se encuentra seleccionada).
- 2) Luego ocurre un SF (fallo de señal) en el sentido oeste a este (se conmuta a la entidad de protección).
- 3) A continuación se repara este defecto (se ingresa al estado WTR, sigue seleccionada la entidad de protección).
- 4) Luego expira el WTR (se conmuta a la entidad de trabajo).

##### I.2.2 Modo no reversible

Para este ejemplo se supone el siguiente caso hipotético:

- 1) El dominio protegido funciona sin defectos (la entidad de trabajo se encuentra seleccionada).
- 2) Luego ocurre un SF (fallo de señal) en el sentido oeste a este (se conmuta a la entidad de protección).
- 3) A continuación se repara este defecto (se ingresa al estado DNR, sigue seleccionada la entidad de protección).

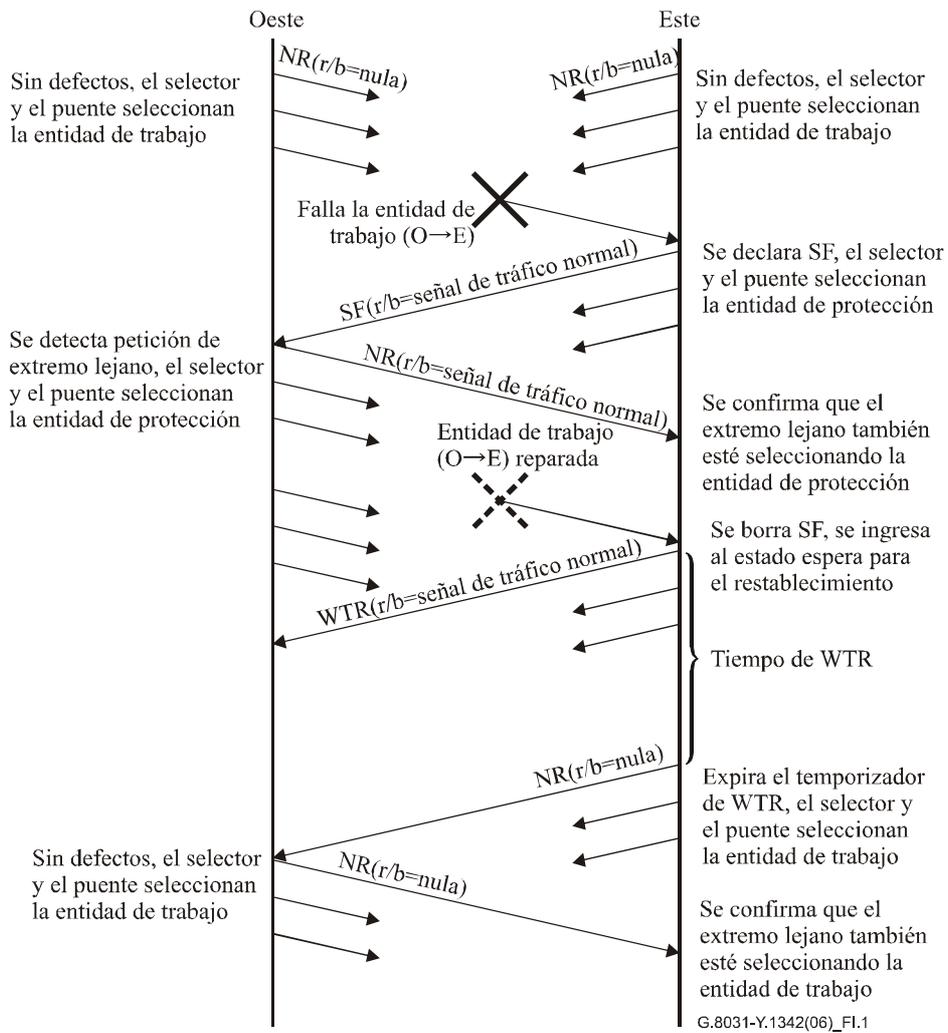
##### I.2.3 Fallo de señal y conmutación forzada

Para este ejemplo se supone el siguiente caso hipotético:

- 1) Ocurre un SF (fallo de señal) en el sentido oeste a este (se conmuta a la entidad de protección).
- 2) Luego, en el este se acepta la instrucción FS (conmutación forzada) (se ingresa al estado FS).
- 3) A continuación, se elimina la FS en el este y se ratifica el SF en el este.

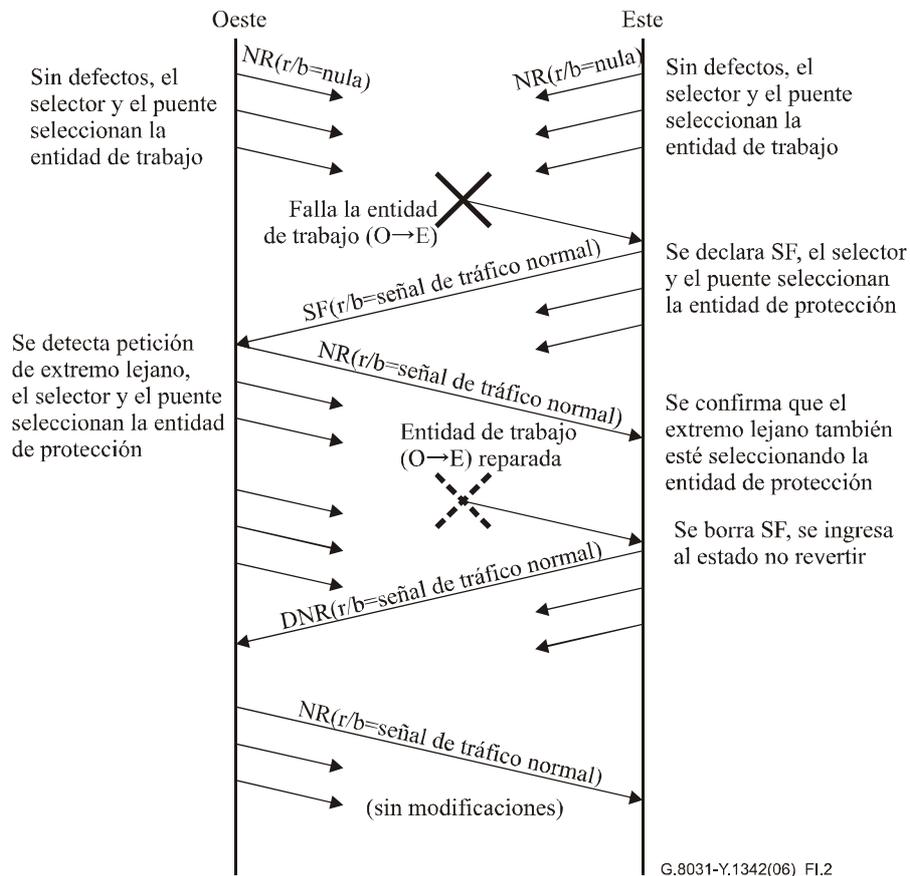
#### I.3 Ejemplos del protocolo APS

En las figuras I.1 (modo reversible), I.2 (modo no reversible) e I.3 (SF y FS), se presentan ejemplos del protocolo APS.



DNR: No revertir  
 NR: Ninguna petición  
 r/b: Señal solicitada/señal puenteadada  
 SF: Fallo de señal  
 WTR: Espera para el restablecimiento  
 O→E: Sentido de oeste a este

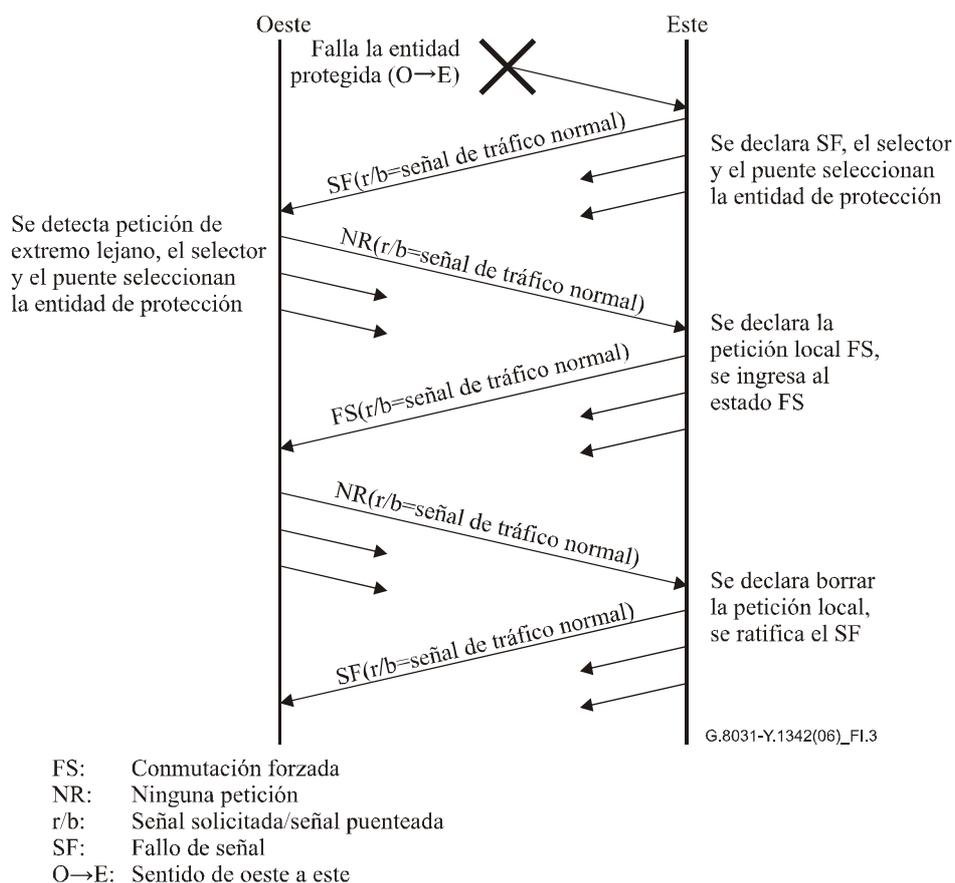
**Figura I.1/G.8031/Y.1342 – Ejemplo del protocolo (modo reversible)**



G.8031-Y.1342(06)\_FI.2

- DNR: No revertir
- NR: Ninguna petición
- r/b: Señal solicitada/señal puenteadada
- SF: Fallo de señal
- WTR: Espera para el restablecimiento
- O→E: Sentido de oeste a este

**Figura I.2/G.8031/Y.1342 – Ejemplo del protocolo (modo no reversible)**



**Figura I.3/G.8031/Y.1342 – Ejemplo del protocolo (SF y FS)**

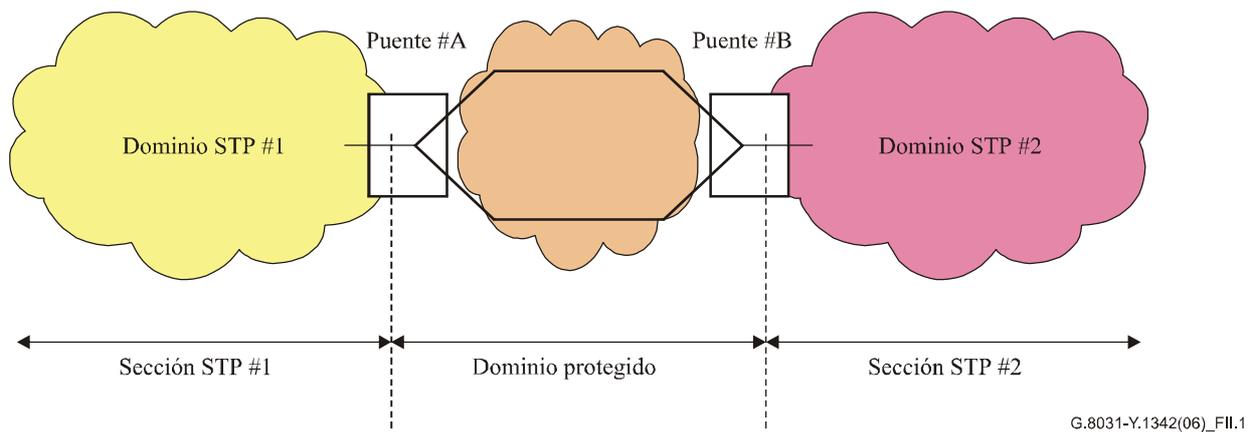
## Apéndice II

### Interacción entre conmutación de protección Ethernet y STP

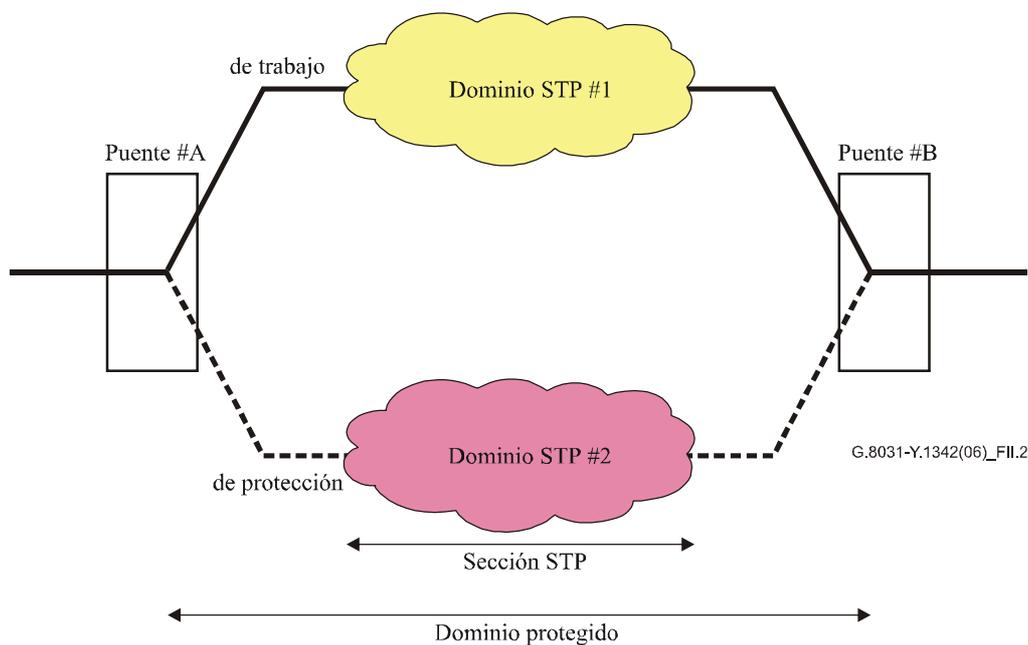
En este apéndice se plantea que los puertos de puente del dominio protegido no deben formar parte de los dominios del protocolo de árbol abarcante (STP, *spanning tree protocol*) a fin de evitar una interacción inconveniente entre STP y la conmutación de protección Ethernet. Una forma de lograr esto consiste en inhabilitar STP en el dominio protegido; admitiendo que los dominios externos al dominio protegido puedan funcionar con el protocolo STP habilitado. Esto también se logra si las entidades de transporte de trabajo y de protección pertenecen a dos dominios STP diferentes. Estos dos casos se describen en la presente sección.

En la figura II.1 se ilustra la primera de las situaciones expuestas: el dominio protegido y los dominios STP (#1 y #2) están segmentados verticalmente y no se superponen. Los puentes #A y #B, ubicados en las fronteras entre el dominio protegido y los dominios STP, interconectan los dominios STP sin que se presenten problemas de bucles.

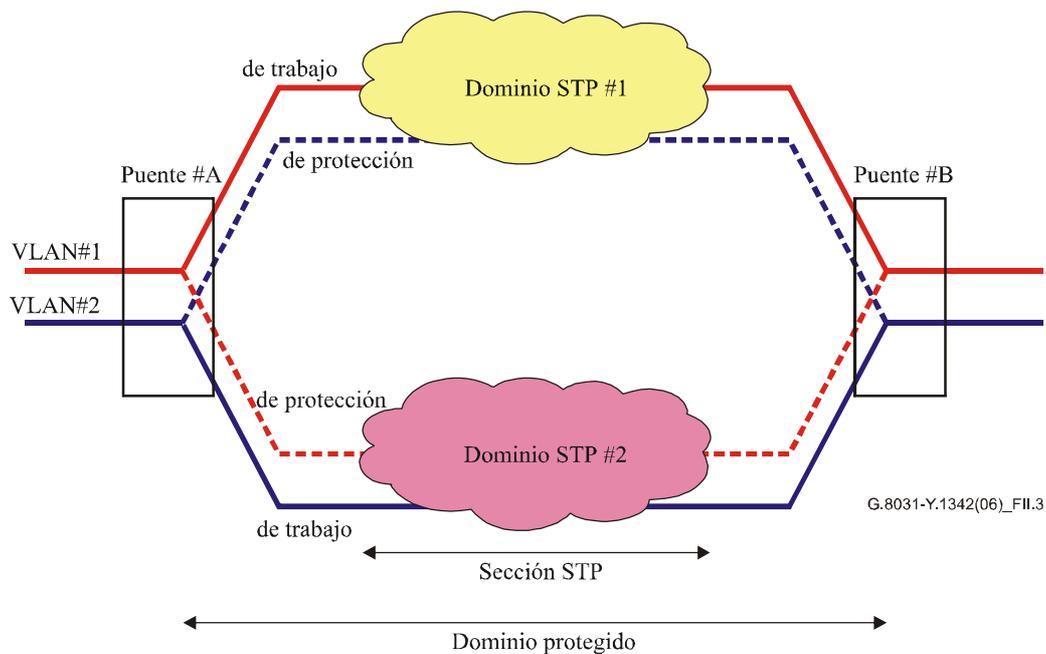
En la figura II.2 se muestra la segunda de las situaciones expuestas: Se segmentan horizontalmente los dominios STP (#1 y #2), proporcionando dos entidades de transporte para la conmutación de protección Ethernet. En la figura II.3 se muestra que las entidades de transporte de trabajo y de protección se configuran separadamente en dominios STP diferentes. En este ejemplo, todas las VLAN y todos los recursos de red se estarían utilizando eficazmente.



**Figura II.1/G.8031/Y.1342 – Sin superposición entre el dominio protegido y STP**



**Figura II.2/G.8031/Y.1342 – Superposición entre el dominio protegido y STP**



**Figura II.3/G.8031/Y.1342 – Superposición entre el dominio protegido y STP por cada VLAN**

## Apéndice III

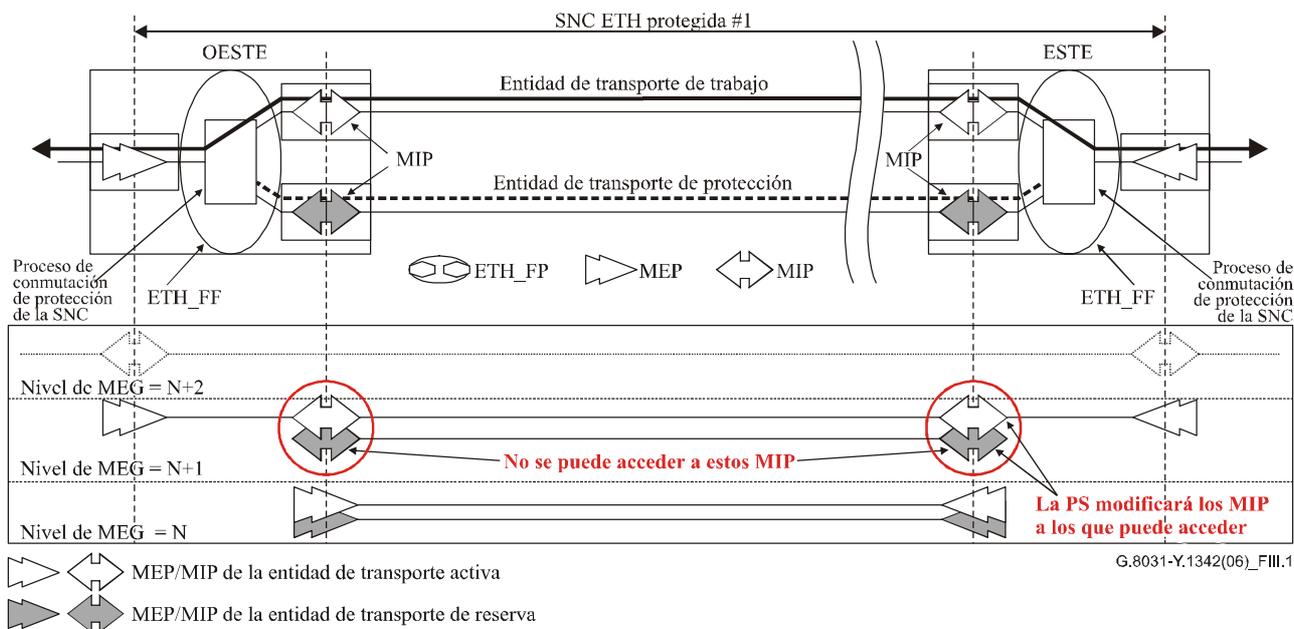
### MIP para el entorno de conmutación de protección

#### III.1 Introducción

En este apéndice se presentan algunas consideraciones y algunos ejemplos de MIP para el entorno de conmutación de protección.

#### III.2 Consideraciones

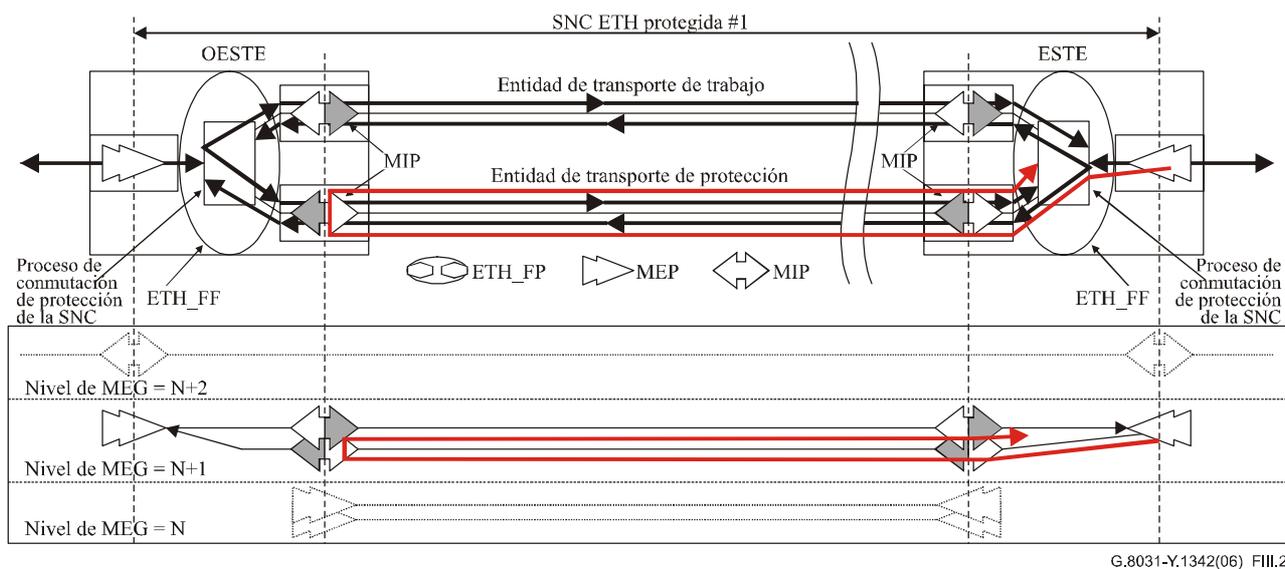
En la figura III.1 se muestra un ejemplo de configuración de MEP y MIP para la conmutación de protección. En la figura III.1 se presentan dos pares de MEP y MIP configurados para supervisar tanto las entidades de transporte de trabajo como de protección en el nivel de MEG N. Tal y como se indica en la figura, también se configuran MEP y MIP en cada puerto del nivel de MEG N+1.



**Figura III.1/G.8031/Y.1342 – MEP y MIP para la conmutación de protección bidireccional 1:1**

Si se ha configurado conmutación de protección 1:1, los MEP no podrán acceder a los MIP del nivel de MEG N+1 en la entidad de transporte de reserva del mismo MEG; y la conmutación de protección modificará los MIP a los que se puede acceder. Por lo tanto, parecen innecesarios los MIP del nivel de MEG N+1, que se muestran en la figura III.1.

En la figura III.2 se muestra una configuración de MEP y MIP en un entorno de conmutación de protección unidireccional 1+1. En este caso no se pueden llevar a cabo correctamente las comunicaciones de petición y respuesta entre los MEP y los MIP. Por lo tanto, también parecen innecesarios los MIP del nivel de MEG N+1 que se muestran en la figura III.2.



**Figura III.2/G.8031/Y.1342 – MEP y MIP para la conmutación de protección unidireccional 1+1**

De acuerdo con lo anterior, parece innecesario configurar MIP en cualquier parte del dominio protegido, en niveles de MEG superiores al de los MEP que supervisan tanto las entidades de transporte de protección como de trabajo.

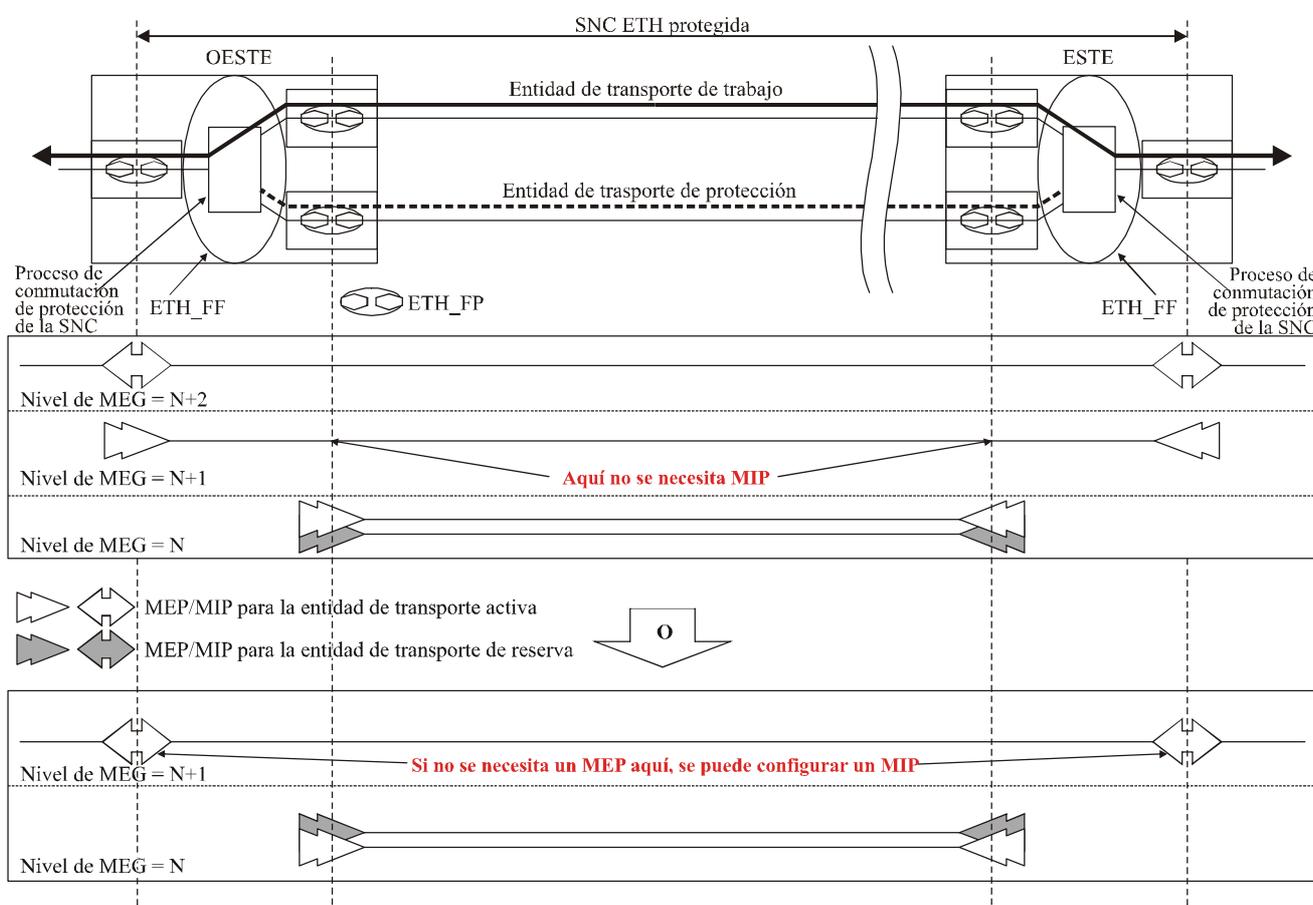
### III.3 Ejemplos de configuración

En la figura III.3 se muestran dos ejemplos de configuración de MEP y MIP.

En el primero de los ejemplos, que se muestra en el centro de la figura III.3, no se han configurado MIP en el nivel de MEG N+1 pero a cambio se configuraron MEP. En este caso, el MEG del nivel de MEG N+1 representa el dominio protegido.

El segundo ejemplo está en la parte baja de la figura III.3. En este caso se configuraron MIP en el nivel de MEG N+1, en la frontera del dominio protegido.

Se puede tener acceso pleno a los MEG y MIP que se aparecen en ambos ejemplos ya que éstos no se configuraron al interior del dominio protegido.



G.8031-Y.1342(06)\_FIII.3

**Figura III.3/G.8031/Y.1342 – Ejemplos de configuración de MEP y MIP en el entorno de conmutación de protección**



RECOMENDACIONES UIT-T DE LA SERIE Y

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

<b>INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN</b>	
Generalidades	Y.100–Y.199
Servicios, aplicaciones y programas intermedios	Y.200–Y.299
Aspectos de red	Y.300–Y.399
Interfaces y protocolos	Y.400–Y.499
Numeración, direccionamiento y denominación	Y.500–Y.599
Operaciones, administración y mantenimiento	Y.600–Y.699
Seguridad	Y.700–Y.799
Características	Y.800–Y.899
<b>ASPECTOS DEL PROTOCOLO INTERNET</b>	
Generalidades	Y.1000–Y.1099
Servicios y aplicaciones	Y.1100–Y.1199
Arquitectura, acceso, capacidades de red y gestión de recursos	Y.1200–Y.1299
<b>Transporte</b>	<b>Y.1300–Y.1399</b>
Interfuncionamiento	Y.1400–Y.1499
Calidad de servicio y características de red	Y.1500–Y.1599
Señalización	Y.1600–Y.1699
Operaciones, administración y mantenimiento	Y.1700–Y.1799
Tasación	Y.1800–Y.1899
<b>REDES DE LA PRÓXIMA GENERACIÓN</b>	
Marcos y modelos arquitecturales funcionales	Y.2000–Y.2099
Calidad de servicio y calidad de funcionamiento	Y.2100–Y.2199
Aspectos relativos a los servicios: capacidades y arquitectura de servicios	Y.2200–Y.2249
Aspectos relativos a los servicios: interoperabilidad de servicios y redes en las redes de próxima generación	Y.2250–Y.2299
Numeración, denominación y direccionamiento	Y.2300–Y.2399
Gestión de red	Y.2400–Y.2499
Arquitecturas y protocolos de control de red	Y.2500–Y.2599
Seguridad	Y.2700–Y.2799
Movilidad generalizada	Y.2800–Y.2899

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

## SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
<b>Serie G</b>	<b>Sistemas y medios de transmisión, sistemas y redes digitales</b>
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos, comunicaciones de sistemas abiertos y seguridad
<b>Serie Y</b>	<b>Infraestructura mundial de la información, aspectos del protocolo Internet y Redes de la próxima generación</b>
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación