UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

I.630

(02/99)

SERIE I: RED DIGITAL DE SERVICIOS INTEGRADOS

Principios de mantenimiento

Conmutación de protección del modo de transferencia asíncrono

Recomendación UIT-T I.630

(Anteriormente Recomendación del CCITT)

RECOMENDACIONES UIT-T DE LA SERIE I

RED DIGITAL DE SERVICIOS INTEGRADOS

ESTRUCTURA GENERAL	
Terminología	I.110–I.119
Descripción de las RDSI	I.120–I.129
Métodos generales de modelado	I.130–I.139
Atributos de las redes de telecomunicaciones y los servicios de telecomunicación	I.140–I.149
Descripción general del modo de transferencia asíncrono	I.150–I.199
CAPACIDADES DE SERVICIO	
Alcance	I.200–I.209
Aspectos generales de los servicios en una RDSI	I.210–I.219
Aspectos comunes de los servicios en una RDSI	I.220–I.229
Servicios portadores soportados por una RDSI	I.230–I.239
Teleservicios soportados por una RDSI	I.240–I.249
Servicios suplementarios en RDSI	I.250–I.299
ASPECTOS Y FUNCIONES GLOBALES DE LA RED	
Principios funcionales de la red	I.310–I.319
Modelos de referencia	I.320–I.329
Numeración, direccionamiento y encaminamiento	I.330–I.339
Tipos de conexión	I.340–I.349
Objetivos de calidad de funcionamiento	I.350–I.359
Características de las capas de protocolo	I.360–I.369
Funciones y requisitos generales de la red	I.370–I.399
INTERFACES USUARIO-RED DE LA RDSI	
Aplicación de las Recomendaciones de la serie I a interfaces usuario-red de la RDSI	I.420–I.429
Recomendaciones relativas a la capa 1	I.430–I.439
Recomendaciones relativas a la capa 2	I.440–I.449
Recomendaciones relativas a la capa 3	I.450–I.459
Multiplexación, adaptación de velocidad y soporte de interfaces existentes	I.460–I.469
Aspectos de la RDSI que afectan a los requisitos de los terminales	I.470–I.499
INTERFACES ENTRE REDES	I.500–I.599
PRINCIPIOS DE MANTENIMIENTO	**I.600–I.699**
ASPECTOS DE LOS EQUIPOS DE RDSI-BA	
Equipos del modo de transferencia asíncrono	I.730–I.739
Funciones de transporte	I.740–I.749
Gestión de equipos del modo de transferencia asíncrono	I.750–I.799

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

RECOMENDACIÓN UIT-T I.630

CONMUTACIÓN DE PROTECCIÓN DEL MODO DE TRANSFERENCIA ASÍNCRONO

Resumen

La presente Recomendación "Conmutación de protección del modo de transferencia asíncrono" contiene la arquitectura y el mecanismo de conmutación de protección en la capa ATM. La arquitectura incluye el alcance del dominio protegido y la configuración del dominio protegido. Los recursos para las entidades de protección se atribuyen previamente. El mecanismo incluye el activador de la conmutación de protección, los sistemas de retención y el protocolo de control de la conmutación de protección.

En la presente Recomendación se describe la protección de VP/VC individual y la protección de grupo. La protección de VP/VC individual es una técnica en la que se utiliza una única conexión de red y/o subred para la entidad de trabajo y la entidad de protección. La protección de grupo es una técnica en la que se utiliza una agrupación lógica de una o más conexiones de red y/o subred para la entidad de trabajo y la entidad de protección.

Esta Recomendación describe, actualmente, la conmutación de protección bidireccional 1+1 y 1:1 así como la conmutación de protección unidireccional 1+1.

Orígenes

La Recomendación UIT-T I.630 ha sido preparada por la Comisión de Estudio 13 (1997-2000) del UIT-T y fue aprobada por el procedimiento de la Resolución N.° 1 de la CMNT el 26 de febrero de 1999.

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 Conferencia Mundial de Normalización de las Telecomunicaciones (CMNT), 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 N.° 1 de la CMNT.

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 *empresa de explotación reconocida (EER)* designa a toda persona, compañía, empresa u organización gubernamental que explote un servicio de correspondencia pública. Los términos *Administración, EER* y *correspondencia pública* están definidos en la *Constitución de la UIT (Ginebra, 1992).*

PROPIEDAD INTELECTUAL

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

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

ÍNDICE

Recomendación I.630

CONMUTACIÓN DE PROTECCIÓN DEL MODO DE TRANSFERENCIA ASÍNCRONO

(Ginebra, 1999)

1 Alcance

Esta Recomendación contiene la arquitectura y el mecanismo de conmutación de protección de VP/VC del ATM y la conmutación de protección de un grupo de VP del ATM. La arquitectura incluye el alcance del dominio protegido, la configuración del dominio protegido y las políticas de atribución de recursos. El mecanismo incluye el activador de la conmutación de protección, los sistemas de retención y el protocolo de control de la conmutación de protección. Se utiliza la metodología de modelado definida en las Recomendaciones G.805 [2] e I.326 [4] para describir la arquitectura de conmutación de protección de VP/VC del ATM y la arquitectura de conmutación de protección de grupo de VP/VC del ATM que se indican en la presente Recomendación.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes.

[1] Recomendación UIT-T G.707 (1996), *Interfaz de nodo de red para la jerarquía digital síncrona*.

[2] Recomendación UIT-T G.805 (1995), *Arquitectura funcional genérica de las redes de transporte*.

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

[4] Recomendación UIT-T I.326 (1995), *Arquitectura funcional de redes de transporte basadas en el modo de transferencia asíncrono.*

[5] Recomendación UIT-T I.610 (1999), *Principios y funciones de operaciones y mantenimiento de la red digital de servicios integrados de banda ancha*.

[6] Recomendación UIT-T I.732 (1996), *Características funcionales del equipo del modo de transferencia asíncrono*.

[7] Recomendación CCITT M.495 (1988), *Restablecimiento de la transmisión y diversidad de rutas de transmisión: terminología y principios generales.*

[8] Recomendación UIT-T M.3010 (1996), *Principios para una red de gestión de las telecomunicaciones.*

[9] Recomendación UIT-T M.3300 (1998), *Requisitos de la interfaz F de la red de gestión de las telecomunicaciones.*

3 Definiciones

En esta Recomendación se definen los términos siguientes.

3.1 conexión de canal virtual con conmutación de protección automática: Se trata de una VCC cuyo objetivo es el control, definida para todo el alcance del dominio protegido y contenida dentro de un VCG. Su finalidad es ayudar en la evaluación de la calidad del VCG asociado y servir a modo de conducto para los mensajes de protocolo de control de conmutación de protección. Hay una VCC con APS asociada con cada VCG_W y una VCC con APS asociada con cada VCG_P. La transmisión de los mensajes de protocolo de control de conmutación de protección se hace siempre por la VCC con APS del VCG_P.

3.2 conexión de trayecto virtual con conmutación de protección automática: Se trata de una VPC cuyo objetivo es el control, definida para todo el alcance del dominio protegido y contenida dentro de un VPG. Su finalidad es ayudar en la evaluación de la calidad del VPG asociado y servir a modo de conducto para los mensajes de protocolo de control de conmutación de protección. Hay una VPC con APS asociada con cada VPG_W y una VPC con APS asociada con cada VPG_P. La transmisión de los mensajes de protocolo de control de conmutación de protección se hace siempre por la VPC con APS del VPG_P.

3.3 conmutación de protección bidireccional: Arquitectura de conmutación de protección en la que, en caso de fallo unidireccional, ambos sentidos, es decir, el sentido afectado y el sentido no afectado (del "camino", de la "conexión de subred", etc.), se conmutan a protección.

3.4 puente: (Para configuración 1+1.) Acción o función de transmisión de tráfico idéntico por ambas entidades, la de trabajo y la de protección. (Para configuración 1:n.) Se definirá más adelante.

3.5 puntos de conexión (CP, *connection point*): (Véase la nota 2 en 3.38.) Puntos de referencia que se establecen a lo largo de una conexión de red definida en una capa de red determinada. Los CP establecidos en la capa ATM a lo largo de una conexión de VP (o VC) están situados en el ingreso y el egreso de un elemento de red (o equipo de cliente) ATM, en donde actúan las funciones de terminación de enlace de VP (o VC).

3.6 atribución de recursos de protección especializada: Política de atribución de recursos en la que tanto la ruta como la anchura de banda de la entidad de protección se atribuyen previamente.

3.7 egreso: En la figura 1 se ilustra el punto de egreso de un elemento de red ATM.

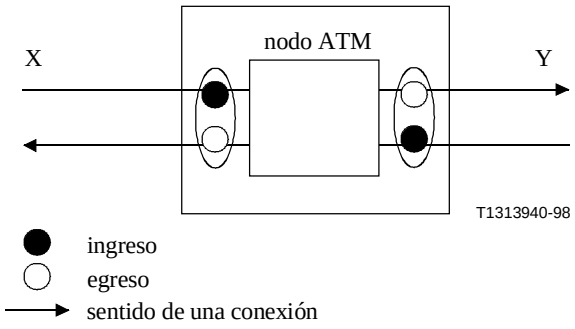


Figura 1/I.630 – Utilización de los términos ingreso y egreso en la Recomendación I.630

3.8 escalación: Acción de supervivencia de red que se produce cuando no se ha llevado a cabo la función supervivencia en capas inferiores.

3.9 tráfico adicional: Tráfico de prioridad inferior al que lleva la entidad de trabajo. Lo lleva la entidad de protección mientras la entidad de trabajo está activa. El tráfico adicional no está protegido, es decir que, cuando se pide a la entidad de protección que proteja el tráfico que está llevando la entidad de trabajo (debido a un fallo o a una operación de conmutación forzada/conmutación manual en esta última entidad), el tráfico adicional queda relegado.

3.10 conmutación forzada para la entidad de trabajo #n: Acción de conmutación iniciada por una instrucción de operador. La acción se lleva a cabo salvo cuando existe una condición de fallo de señal para que conmute la entidad de protección.

3.11 conmutación de protección sin errores: Conmutación de protección que no provoca pérdida de células, duplicación de células, desorden de células o errores en los bits tras la acción de conmutación de protección.

3.12 tiempo de retención: Intervalo de tiempo entre la detección de un SF o una SD y su confirmación como condición que requiere el procedimiento de conmutación de protección.

3.13 deficiencia: Defecto o degradación de la calidad de funcionamiento que puede llevar a una activación por SF o SD.

3.14 ingreso: En la figura 1 se ilustra el punto de ingreso de un elemento de red ATM.

3.15 nodo intermedio: Nodo en la ruta física de la entidad de trabajo o de la entidad de protección entre la fuente y el sumidero del dominio protegido correspondiente.

3.16 conexión de enlace: Su definición figura en la Recomendación G.805. A título de ejemplo, una conexión de enlace de VP está delimitada por los CP situados en dos elementos de red ATM consecutivos que funcionan a nivel de VP.

3.17 conmutación manual: Acción de conmutación iniciada por una instrucción de operador. La acción se lleva a cabo a menos que esté en efecto una petición de prioridad superior.

3.18 conexión de matriz: Conexión de subred delimitada, para la capa ATM, por los CP situados en el ingreso y el egreso de un elemento de red ATM (véase la nota 2 en 3.38).

3.19 conexión de red: Entidad de transporte utilizada para transferir información de usuario y OAM entre los puntos de extremo de la conexión (los TCP) (véase la nota 2 en 3.38).

3.20 supervivencia de red: Conjunto de capacidades que permiten a una red restablecer el tráfico afectado en caso de fallo. El grado de supervivencia viene determinado por la capacidad de la red de sobrevivir a fallos aislados, fallos múltiples y fallos de equipo.

3.21 conmutación de protección no reversiva: Método de conmutación de protección en el que no se lleva a cabo una acción reversiva (conmutación de retorno a la entidad de trabajo) después de que la entidad de trabajo ha sido reparada.

3.22 dominio protegido para la capa del modo de transferencia asíncrono: El dominio protegido define una o más VPC/VCC, o un tramo de estas conexiones, para las que se proporciona un mecanismo de supervivencia en el caso de que una degradación afecte a las mismas. Empieza tras el selector/puente de un punto de extremo y llega hasta el selector/puente del otro punto de extremo. Están excluidas del dominio tanto la función selector como la función puente.

3.23 entidad de protección: Tramo de la VPC/VCC o del VPG/VCG del ATM dentro del dominio protegido del que se recibe tráfico de trabajo en el sumidero del dominio protegido en donde ha fallado una entidad de trabajo.

3.24 conmutación de protección: Técnica de supervivencia de red con política de atribución de recursos de protección especializada.

3.25 conmutación de protección reversiva: Método de conmutación de protección en el que se lleva a cabo una acción reversiva (conmutación de retorno a la entidad de trabajo) después de que la entidad de trabajo ha sido reparada.

3.26 selector: Conmutador que selecciona el tráfico procedente de la entidad de trabajo o la entidad de protección.

3.27 conexión de subred: Entidad de transporte correspondiente a una parte de una conexión de red. Una conexión de subred se puede subdividir en una concatenación de enlaces y conexiones de matriz. Una conexión de matriz corresponde, como caso especial, a una conexión de subred única (indivisible) (véase la nota 2 en 3.38).

3.28 punto de conexión de terminación (TCP, *termination connection point*): Puntos de extremo de una conexión de red (véase la nota 2 en 3.38).

3.29 camino: "Entidad de transporte" que consta de un par asociado de "caminos unidireccionales" capaz de transferir información en sentidos opuestos simultáneamente entre sus respectivas entradas y salidas (véase la nota 2 en 3.38).

3.30 entidad de transporte: Componente arquitectural que transfiere información entre sus entradas y salidas dentro de una capa de red (véase la nota 2 en 3.38).

3.31 conmutación de protección unidireccional: Arquitectura de conmutación de protección en la que, en caso de fallo unidireccional (es decir, un fallo que afecta solamente a un sentido de la transmisión), sólo el sentido afectado (del "camino", de la "conexión de subred", etc.) se conmuta a protección.

3.32 grupo de canales virtuales de protección: VCG distinto físicamente alternativo formado por conexiones de red o conexiones de subred de VC de protección asignadas a un VCG_W o a un conjunto de VCG_W (como en funcionamiento 1:n).

3.33 grupo de canales virtuales de trabajo: VCG formado por conexiones de red o conexiones de subred de VC del ATM de trabajo que llevan tráfico protegido en condiciones de funcionamiento normales.

3.34 grupo de canales virtuales (VCG): Agrupación lógica de una o más conexiones de red y/o subred de VC del ATM que comparten el mismo o los mismos trayectos dentro del dominio protegido.

3.35 grupo de trayectos virtuales (VPG): Agrupación lógica de una o más conexiones de red y/o subred de VP del ATM que comparten el mismo o los mismos trayectos de transmisión dentro del dominio protegido.

3.36 grupo de trayectos virtuales de protección: VPG distinto físicamente alternativo formado por conexiones de red o conexiones de subred de VP de protección asignadas a un VPG_W o a un conjunto de VPG_W (como en funcionamiento 1:n).

3.37 grupo de trayectos virtuales de trabajo: VPG formado por conexiones de red o conexiones de subred de VP del ATM de trabajo que llevan tráfico protegido en condiciones de funcionamiento normales.

3.38 entidad de trabajo: Tramo de la VPC/VCC o del VPG/VCG del ATM dentro del dominio protegido del que se recibe tráfico de trabajo en el sumidero del dominio protegido en condición libre de fallos en modo reversivo.

NOTA 1 – Esta función es diferente de la de "puenteo" definida en la Recomendación G.841 [3].

NOTA 2 – La Recomendación G.805 da una definición más general y detallada.

4 Símbolos y abreviaturas

En esta Recomendación se utilizan las siguientes siglas.

AIS	Señal de indicación de alarma (*alarm indication signal*)
AN	Red de acceso (*access network*)
APS	Conmutación de protección automática (*automatic protection switching*)
ATM	Modo de transferencia asíncrono (*asynchronous transfer mode*)
CP	Punto de conexión (*connection point*)
CPN	Red en las instalaciones del cliente (*customer premises network*)
e-t-e_VC-XX	Célula OAM que proporciona la función OAM "XX" para una VCC de extremo a extremo (por ejemplo, e-t-e_VC-AIS ...)
e-t-e_VP-XX	Célula OAM que proporciona la función OAM "XX" para una VPC de extremo a extremo (por ejemplo, e-t-e_VP-AIS ...)
e-t-e_XX	Célula OAM que proporciona la función OAM "XX" para una VPC o una VCC de extremo a extremo (por ejemplo, e-t-e_AIS ...)
MS	Conmutación manual (*manual switch*)
NIM	Supervisión no intrusiva (*non intrusive monitoring*)
OAM	Operaciones y mantenimiento (*operations and maintenance*)
PS	Conmutación de protección (*protection switching*)
RGT	Red de gestión de las telecomunicaciones
SD	Degradación de señal (*signal degrade*)
SDH	Jerarquía digital síncrona (*synchronous digital hierarchy*)
seg_VC-XX	Célula OAM que proporciona la función OAM "XX" para un segmento de VCC (por ejemplo, seg_VC-AIS ...)
seg_VP-XX	Célula OAM que proporciona la función OAM "XX" para un segmento de VPC (por ejemplo, seg_VP-AIS ...)
seg_XX	Célula OAM que proporciona la función OAM "XX" para un segmento de VPC o VCC (por ejemplo, seg_AIS ...)
SF	Fallo de señal (*signal fail*)
SN	Subred (*subnetwork*)
SNC	Conexión de subred (*subnetwork connection*)
TCP	Punto de conexión de terminación (*termination connection point*)
TE	Equipo terminal (*terminal equipment*)
VC	Canal virtual (*virtual channel*)
VCC	Conexión de canal virtual (*virtual channel connection*)
VCG	Grupo de canales virtuales (*virtual channel group*)
VCI	Identificador de canal virtual (*virtual channel identifier*)
VP	Trayecto virtual (*virtual path*)

VPC Conexión de trayecto virtual (*virtual path connection*)

VPG Grupo de trayectos virtuales (*virtual path group*)

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

5 Principios de la conmutación de protección

El concepto de conmutación de protección de VP/VC individual se desarrolló para aplicarlo sobre todo en aquellas situaciones en que no está presente una conmutación de protección de capa de servidor. Conviene proteger solamente los VP/VC que necesitan un alto grado de fiabilidad. El resto de los VP/VC permanece sin protección. Así se ayuda a reducir la anchura de banda necesaria para protección. Aunque se puede emplear para protección frente a deficiencias de capa ATM y de capa física, no se excluye su aplicación para protección frente a defectos de capa física únicamente.

El concepto de protección de VPG/VCG se desarrolló en principio en la capa ATM para facilitar la conmutación de protección rápida de capa ATM (con unos tiempos de compleción del mismo orden que los de la conmutación de protección de capa SDH) principalmente en aquellas situaciones en que no está presente o no se puede desplegar ningún mecanismo de conmutación de protección de capa de servidor. La conmutación de protección rápida se obtiene tratando una agrupación lógica de conexiones de red y/o subred de VP/VC como una entidad única de VPG/VCG tras el comienzo de las acciones de protección. Aunque la protección de VPG/VCG se diseñó sobre todo con miras a la recuperación tras la ocurrencia de fallos de capa física, el concepto de protección de VPG/VCG no excluye su utilización en la protección frente a defectos de capa ATM. Además, la protección de VPG/VCG podría utilizarse junto con técnicas de conmutación de protección de VP/VC individual, que se pueden emplear para proteger conexiones de VP/VC individuales frente a defectos de capa ATM.

La conmutación de protección es un mecanismo de protección atribuido plenamente que se puede utilizar en cualquier topología física. Atribuido plenamente quiere decir que la ruta y la anchura de banda de la entidad de protección se reservan para una entidad de trabajo seleccionada.

La arquitectura de PS del ATM puede ser de tipo 1+1 o de tipo *m*:*n*.

En la arquitectura de tipo 1+1, se especializa una entidad de protección por cada entidad de trabajo estando la entidad de trabajo puenteada a la entidad de protección en la fuente del dominio protegido. El tráfico por las entidades de trabajo y protección se transmite simultáneamente al sumidero del dominio protegido, en donde se hace una selección entre la entidad de trabajo y la entidad de protección en base a algunos criterios predeterminados, por ejemplo, una indicación de defecto del servidor.

En la arquitectura de tipo *m*:*n*, *m* entidades de protección especializadas son compartidas por *n* entidades de trabajo, siendo normalmente $m \leq n$. La anchura de banda de cada entidad de protección deberá atribuirse de manera que sea posible proteger cualquiera de las *n* entidades de trabajo en el caso en que al menos una de las *m* entidades de protección esté disponible. Cuando se determine que una entidad de trabajo está degradada, deberá procederse primero a su asignación a una entidad de protección disponible, a lo que ha de seguir la transición de la entidad de trabajo a la entidad de protección tanto en la fuente como en el sumidero del dominio protegido. Se señala que cuando haya más de *m* entidades de trabajo degradadas, sólo se podrán proteger *m* de dichas entidades.

5.1 Principios, requisitos y objetivos generales

Los principios, requisitos y objetivos generales que se indican a continuación son comunes a la conmutación de protección de VC, VP, VCG y VPG.

5.1.1 Principios generales

Esta subcláusula contiene una lista de los principios generales utilizados como orientación para el desarrollo de arquitecturas y mecanismos de protección ATM.

1) Las técnicas de protección ATM deberán ser aplicables a VPG, VP, VCG y VC.
2) Deberán evitarse las infracciones de la estratificación por capas de la red (por ejemplo, un defecto a nivel de VP individual del ATM no deberá provocar alarmas de capa SDH).
3) Por lo general, si se utilizan mecanismos de protección de capa inferior (por ejemplo, SDH u óptica) junto con mecanismos de protección de capa ATM, deberá darse a las capas inferiores la oportunidad de restablecer el tráfico de trabajo antes de que la capa ATM inicie las acciones de protección. El objetivo aquí es evitar acciones de protección no necesarias y cualquier cuestión que plantee conflictos.
4) Las acciones de conmutación de protección en un dominio protegido no deberán afectar de manera adversa a las operaciones y a la calidad de funcionamiento de la red en otros dominios.
5) Los mecanismos de conmutación de protección deberán facilitar un rápido restablecimiento del tráfico de trabajo para que la indisponibilidad de la red sea mínima.

5.1.2 Requisitos y objetivos generales

1) Protección de caminos de VP/VC y conexiones de subred (SNC, *subnetwork connections*).
2) Protección de dominios protegidos de SNC que sean independientes o estén alineados con flujos OAM de segmento F4 o F5 (véase la Recomendación I.610 [5]).
3) Topología física lineal, de anillo o de malla.
4) Deberá utilizarse la detección de fallo de señal (SF, *signal fail*) y de degradación de señal (SD, *signal degrade*) para activar la conmutación de protección. La activación en caso de SD queda en estudio.
5) Tiempos de detección de SF tan breves como sea posible.
6) Protección prioritaria en caso de SF, SD, y peticiones de conmutación de operador.
7) Tiempo de compleción de la conmutación de protección: debe estar prevista la posibilidad de obtener protección en la capa ATM a la mayor brevedad. Algo que podría ser de sumo interés si, por ejemplo, la capa física no tuviera medios con los que protegerse en caso de fallo (por ejemplo, cuando una estructura en anillo recoge el tráfico procedente de nodos ATM). El valor o los valores exactos quedan en estudio.
8) Relación de protección del 100%, es decir, el 100% del tráfico de trabajo degradado está protegido frente a un fallo en una única entidad de trabajo.
9) Deberán soportarse modos de conmutación de protección unidireccional 1+1 y bidireccional 1+1 y 1:1 (el modo *m:n* generalizado requiere un estudio sobre la técnica de atribución de recursos de protección).
10) Capacidad de tráfico adicional, cuando sea posible.
11) Protocolo de control de conmutación de protección basado en los principios y las características de APS de la SDH, en la medida de lo posible.
12) Deberá soportarse la estrategia de escalación intercapa e intracapa.
13) Utilización de las herramientas OAM existentes definidas en la Recomendación I.610 y reducción al mínimo de la introducción de nuevas herramientas OAM, en la medida de lo posible.
14) Ausencia de interferencia no intencionada con la protección de la capa física.

15) Deberá ser posible la combinación de la conmutación de protección de VP/VC y VPG/VCG individual.

16) Deberá proporcionarse conmutación reversiva y no reversiva, como opción del operador de red.

17) Deberán soportarse instrucciones de control por el operador tales como la exclusión de protección, la conmutación forzada y la conmutación manual.

18) Deberá proporcionarse una "función de retención genérica" para retardar el comienzo de la acción de protección. El tiempo de retención conseguido con esta función deberá ser ajustable por el operador de red de modo que se funcione en base a una acción de protección "tan rápida como sea posible" o se retrase dicha acción durante algunos segundos.

19) La conectividad de la capa ATM de la entidad de protección deberá supervisarse regularmente para asegurar la disponibilidad cuando se precise efectuar una conmutación de protección. La frecuencia de inserción de las células APS y de una célula cada 5 segundos. La frecuencia de inserción ajustable queda en estudio. La necesidad de otras supervisiones (por ejemplo, de la anchura de banda, de la calidad de funcionamiento, etc.) de la entidad de protección queda en estudio.

    NOTA – La frecuencia de inserción se determinó efectuando una compensación entre anchura de banda requerida para las células APS y retardo adicional cuando se pierde una célula APS.

20) Si es posible, deberá proporcionarse protección jerarquizada.

21) En la primera versión de la presente Recomendación I.630 no se exige conmutación de protección sin errores.

5.2 Ejemplos de dominios protegidos de red

La figura 2 ilustra ejemplos de dominios protegidos. El dominio protegido se puede extender:

- a través de una conexión de red;
- a través de una conexión de subred;
- a través de una conexión de enlace único.

El dominio protegido para VPC/VCC puede coincidir con el alcance de los flujos OAM de extremo a extremo o de segmento. La Recomendación I.732 [6] define dos tipos de funcionalidad de terminación de segmento. En uno de ellos, la fuente está delante de la matriz y el sumidero asociado detrás de la matriz. En el otro, la fuente está detrás de la matriz y el sumidero asociado delante de la matriz. Si los puntos de extremo del dominio protegido coinciden con puntos de terminación de segmento del segundo tipo, los mecanismos de conmutación de protección ATM aplicados al dominio protegido pueden utilizar las herramientas OAM de segmento de VPC/VCC.

Cuando el dominio protegido no coincida con el alcance de los flujos OAM de extremo a extremo o de segmento, quizá sea necesario emplear capacidades tales como la de supervisión no intrusiva de las herramientas OAM existentes con mecanismos de conmutación de protección ATM aplicados al dominio protegido.

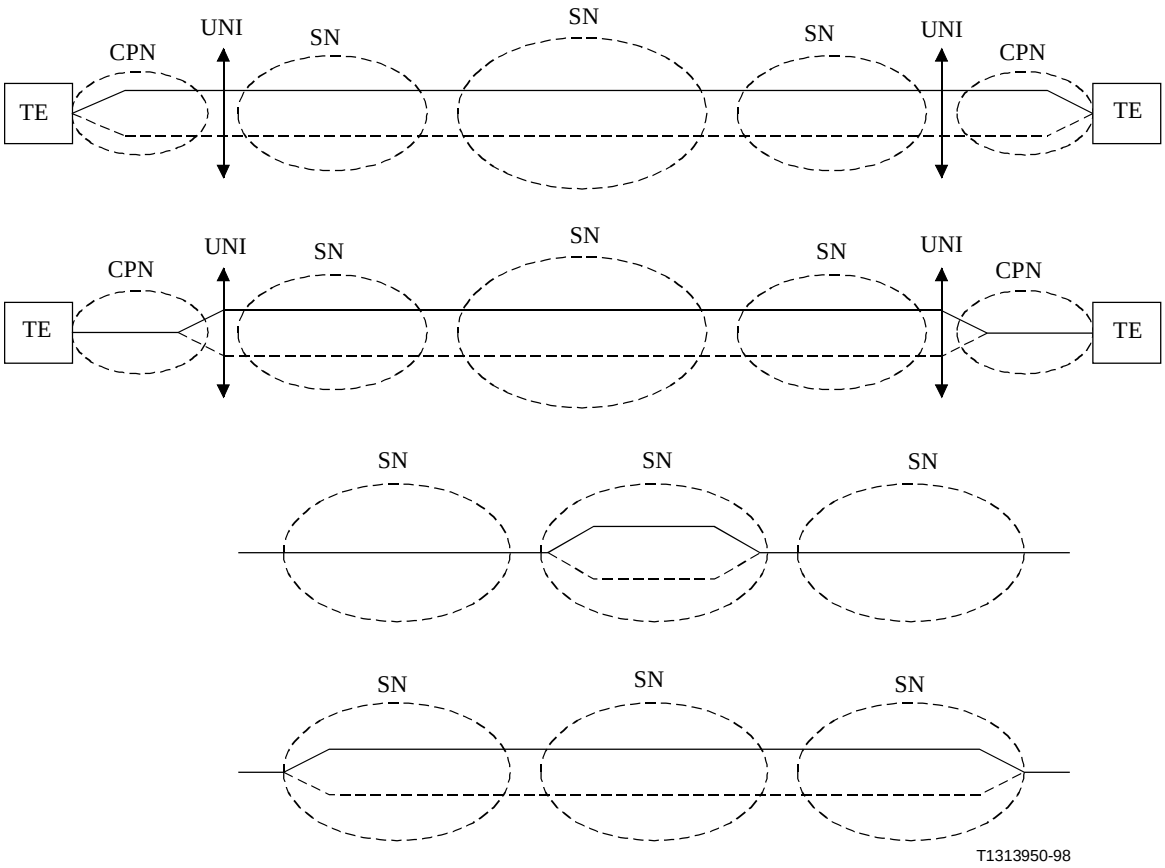


Figura 2/I.630 – Ejemplos de dominios protegidos

5.3 Alcance del dominio protegido

En las subcláusulas que siguen se utilizan los términos que se indican a continuación:

- Protección de camino 1+1/1:1 [conexión de extremo a extremo] – este esquema que utiliza el flujo OAM de conexión de extremo a extremo para supervisar el camino [de extremo a extremo] dentro del dominio protegido.
- Protección de conexión de subred con supervisión de subcapa 1+1/1:1 (SNC/S) – este esquema requiere que se añada un flujo OAM de dominio de protección adicional o de segmento de supervisión de conexión para supervisar la conexión de subred dentro del dominio protegido.
- Protección de conexión de subred con supervisión no intrusiva 1+1 (SNC/N) – este esquema no requiere la utilización de un flujo OAM adicional para supervisar la conexión de subred dentro del dominio protegido; se limita por tanto a unidireccional 1+1. El presente esquema es aplicable a protección de VP/VC individual solamente y no a la protección de grupo.
- Protección de conexión de subred con supervisión de camino de prueba 1+1/1:1 (SNC/T) – este esquema es aplicable a protección de grupo solamente; se establece un camino de prueba adicional (conexión de extremo a extremo) entre la fuente y el sumidero del dominio protegido. La situación de este camino de prueba se utiliza como una indicación de la condición SF y SD del grupo.

  NOTA 1 – En la cláusula 7 se hace referencia al camino de prueba para protección de grupo como una VPC/VCC con APS.

  NOTA 2 – En el caso general, se pueden asignar al mismo grupo conexiones de red y conexiones de subred que llevan tráfico de usuario.

- Protección de camino con supervisión de camino de prueba 1+1/1:1 (camino/T) – este esquema es aplicable a la protección de grupo solamente; se establece un camino de prueba adicional (conexión de extremo a extremo) entre la fuente y el sumidero del dominio protegido. La situación de este camino de prueba se utiliza como una indicación de la condición SF y SD del grupo.

5.3.1 Protección de camino

La figura 3 muestra un ejemplo de protección de camino de VP/VC individual 1+1 ó 1:1.

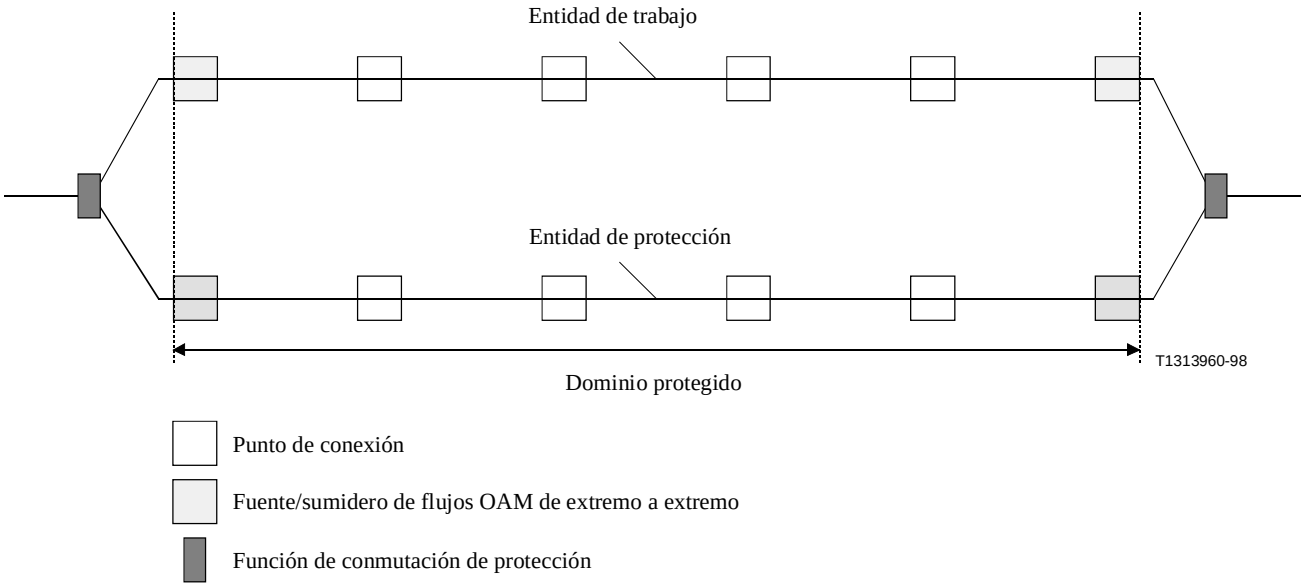


Figura 3/I.630 – Protección de camino de VP/VC individual 1:1 ó 1+1

La figura 4 muestra un ejemplo de protección de grupo de camino/T 1+1 ó 1:1.

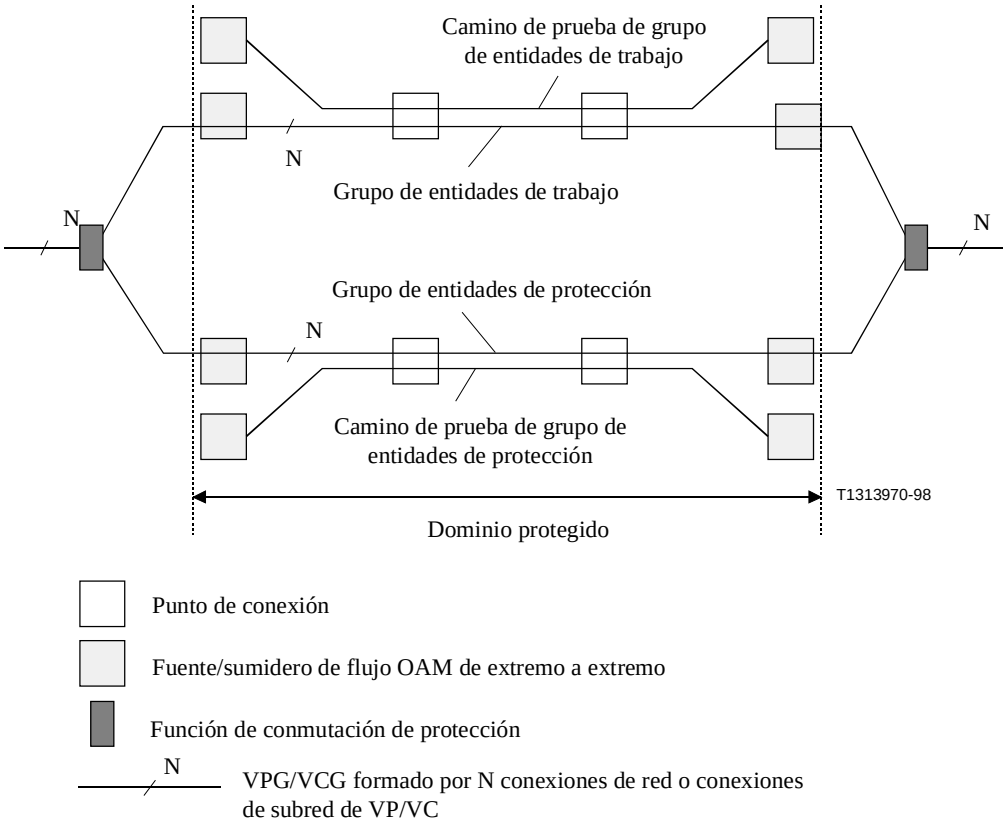


Figura 4/I.630 – Protección de grupo de camino/T 1+1 ó 1:1

5.3.2 Protección de conexión de subred

La figura 5 muestra un ejemplo de protección de VP/VC individual de SNC/S 1+1 ó 1:1.

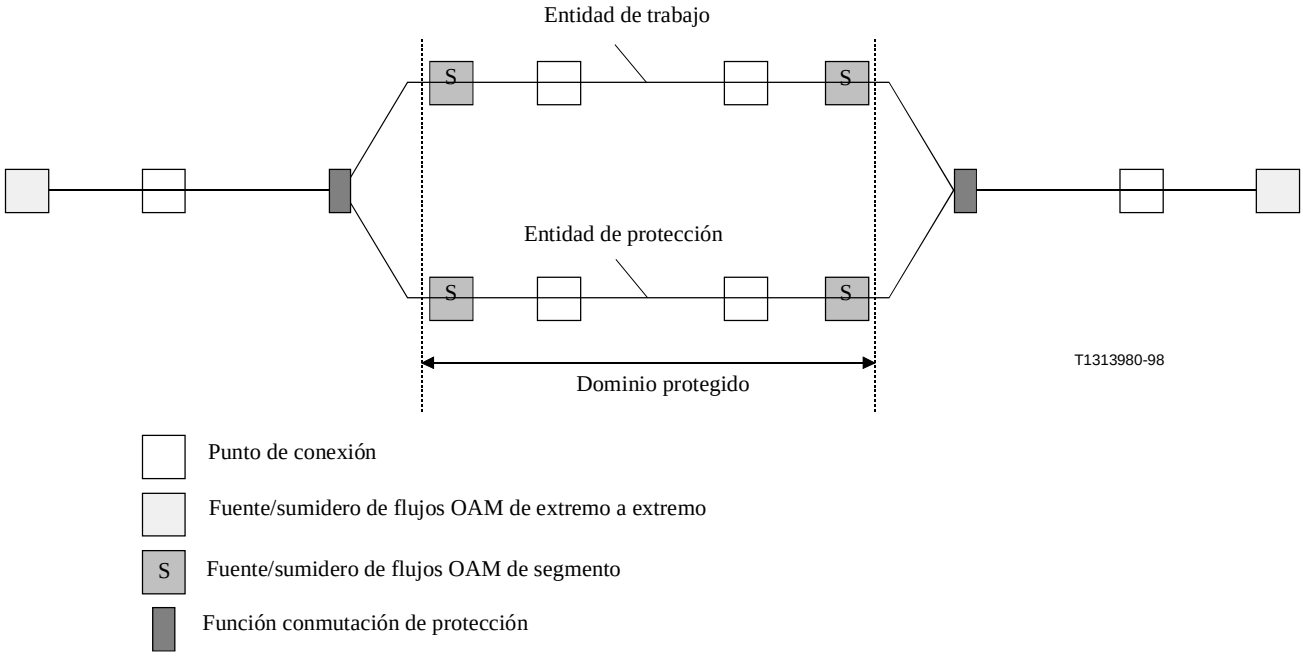


Figura 5/I.630 – Protección de VP/VC individual de SNC/S 1+1 ó 1:1

La figura 6 muestra un ejemplo de protección de grupo de SNC/T 1:1 ó 1+1.

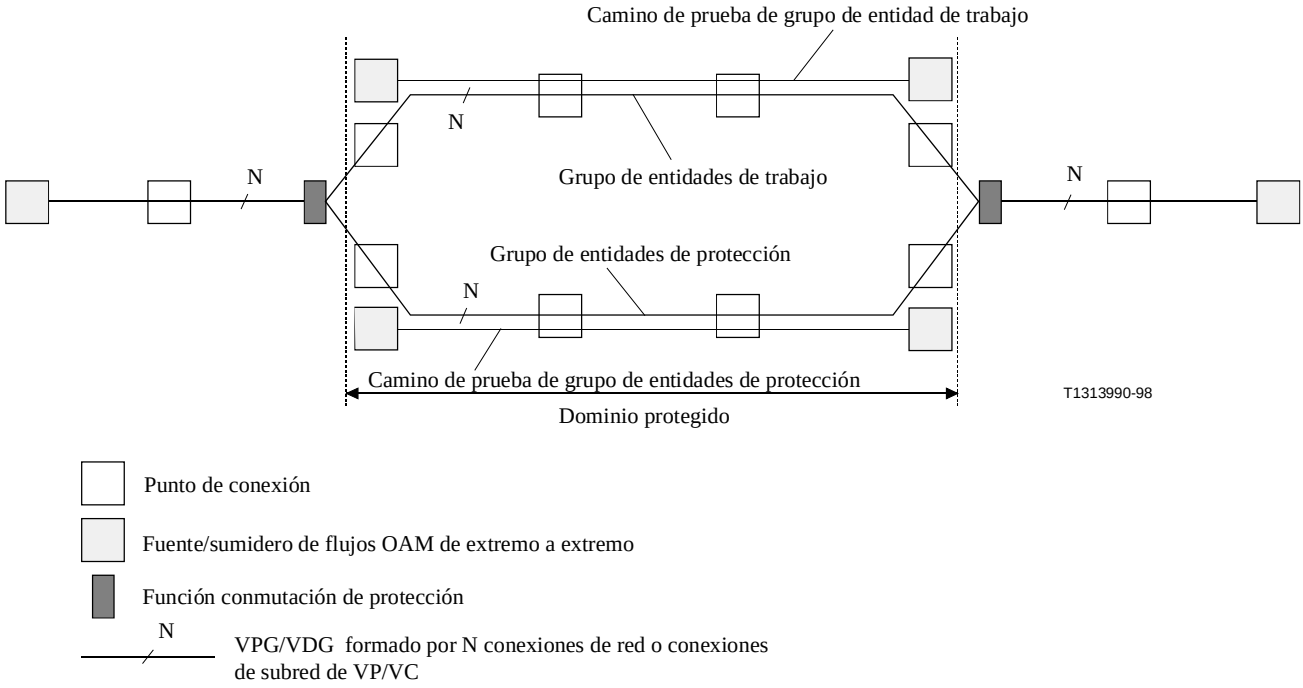


Figura 6/I.630 – Protección de grupo de SNC/T 1:1 ó 1+1

5.3.3 Protección de conexión de subred con supervisión no intrusiva 1+1 (SNC/N)

La figura 7 muestra un ejemplo de protección de conexión de subred de VP/VC individual con supervisión no intrusiva 1+1 (SNC/N).

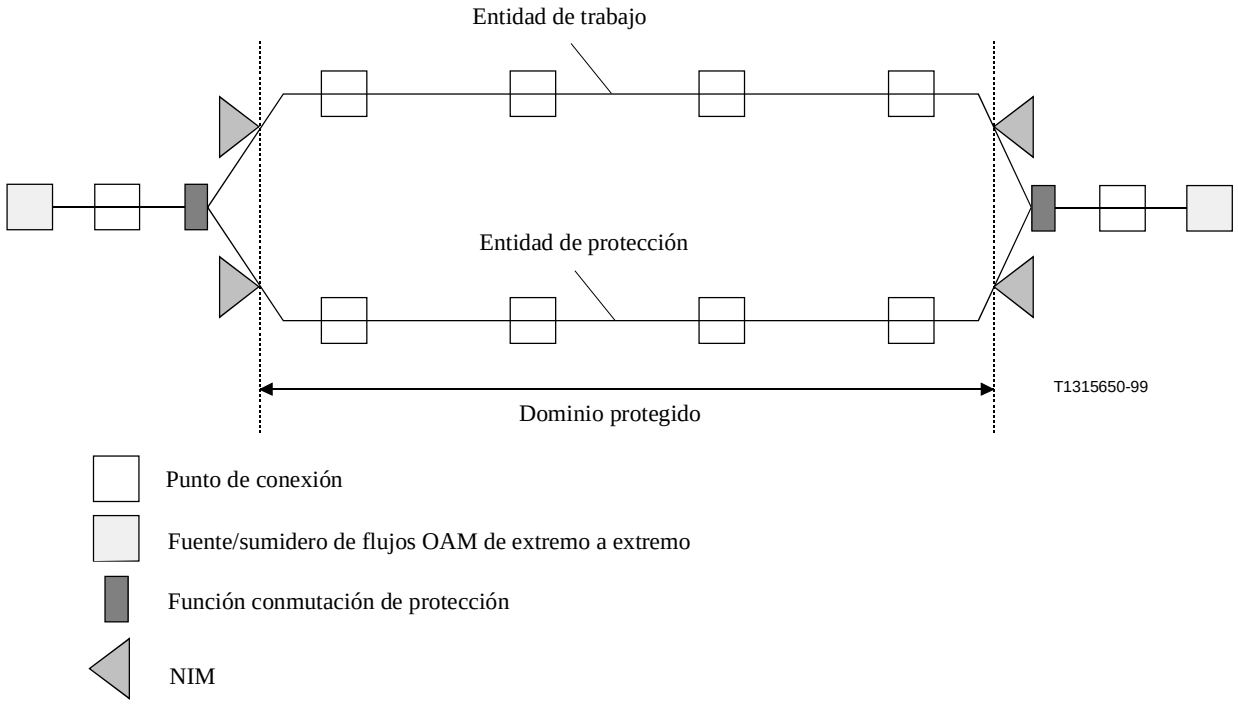


Figura 7/I.630 – Protección SNC/N de VP/VC individual con supervisión no intrusiva 1+1

5.3.4 Relación entre el dominio protegido y el alcance de los flujos OAM

No puede soportarse una configuración en la que se superponen un dominio protegido y un segmento OAM. No puede soportarse para conmutación de protección bidireccional una configuración en la que se superponen dos dominios protegidos. Se señala no obstante que sí pueden soportarse dominios protegidos superpuestos en el caso de conmutación de protección unidireccional 1+1.

5.4 Dependencia de la configuración de la red de capa física

Normalmente, las entidades de protección y trabajo deberán ser encaminadas por entidades de transporte de características físicas distintas.

5.5 Configuraciones de conmutación de protección

5.5.1 Configuración (1:1)

Se asigna una entidad de protección especializada a cada entidad de trabajo. La entidad de protección solamente lleva tráfico si la entidad de trabajo ha fallado o se ha efectuado una conmutación forzada/conmutación manual para el funcionamiento de la entidad de trabajo. De no ser así, no lleva tráfico y puede llevar tráfico adicional.

5.5.2 Configuración (1+1)

Se asigna una entidad de protección especializada a cada entidad de trabajo. Las entidades de trabajo y protección llevan el tráfico simultáneamente.

5.5.3 Configuración (1:n)

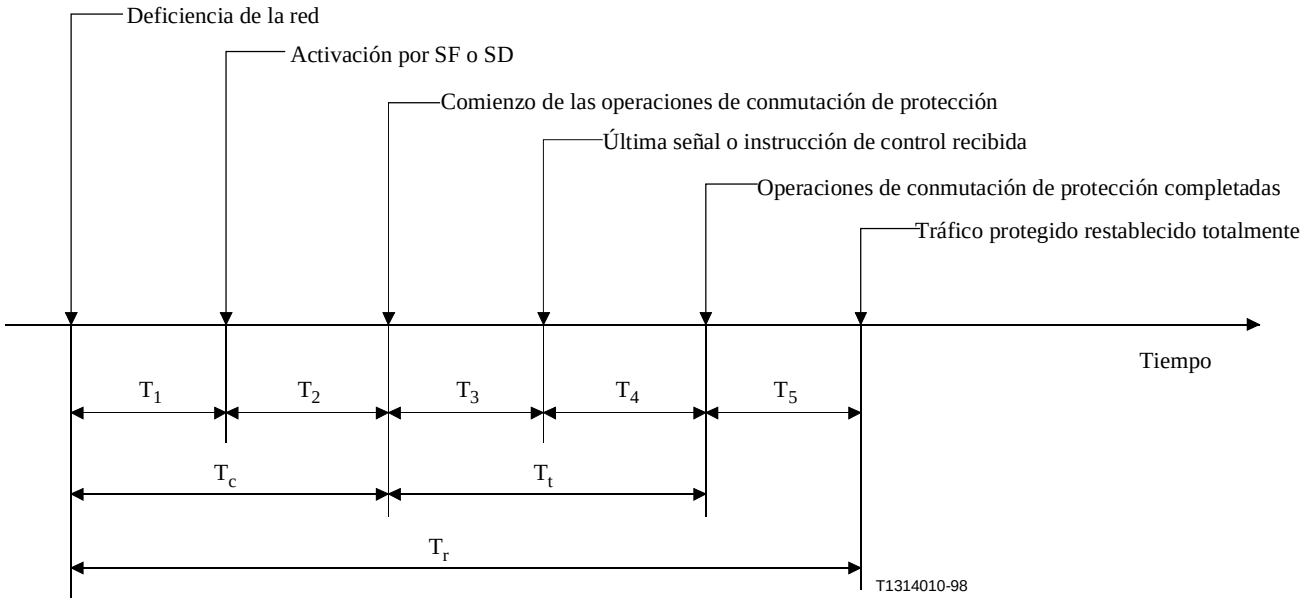
Queda en estudio.

5.5.4 Configuración (m:n)

Queda en estudio.

5.6 Calidad de funcionamiento de la conmutación de protección

En la figura 8 se ilustran el modelo temporal de conmutación de protección ATM basado en la Recomendación M.495 [7] y sus parámetros.



tiempo de detección, T_1

tiempo de espera, T_2 **:** [Este tiempo corresponde al tiempo de retención (véase 5.7).]

tiempo de las operaciones de conmutación de protección, T_3

tiempo de transferencia de la conmutación de protección, T_4

tiempo de recuperación, T_5

tiempo de confirmación, T_c

tiempo de transferencia, T_t

tiempo de restablecimiento del tráfico protegido, T_r

Figura 8/I.630 – Modelo temporal de conmutación de protección

5.7 Función tiempo de retención en la escalación de supervivencia del ATM

Para dar a las funciones de conmutación de protección de capa inferior la oportunidad de proteger el tráfico de trabajo antes de que se produzca la conmutación de protección de capa ATM, o para confirmar la persistencia del defecto contra el que hay que protegerse, o para retardar la conmutación de protección por otros motivos operacionales, deberá proporcionarse un tiempo de retención.

Puesto que las células VP/VC-AIS se transmiten tan pronto como se puede tras la detección de un defecto, el tiempo de retención se fija en el sumidero del dominio protegido. La operación de conmutación de protección comienza una vez que han transcurrido *x* segundos de un estado de extremo a extremo o seg_AIS observado en el sumidero del dominio protegido.

El valor de *x* se puede seleccionar dentro de la gama de 0 a 10 segundos con una granularidad de 500 ms.

5.8 Protocolo de control de la conmutación de protección

La conmutación de protección bidireccional se realiza intercambiando información de coordinación entre la fuente y el sumidero del dominio protegido. La información de coordinación se transmite utilizando la célula VP/VC-APS especializada. El formato de la célula VP/VC-APS se da en la figura 9. Los puntos de código conexos se dan en el cuadro 1. La descripción detallada de los mecanismos de coordinación de conmutación de protección para las configuraciones (1:1) y (1+1) se hace en el anexo A.

La conmutación de protección unidireccional (1+1) se realiza sin un protocolo de coordinación. Los detalles se indican en el anexo B.

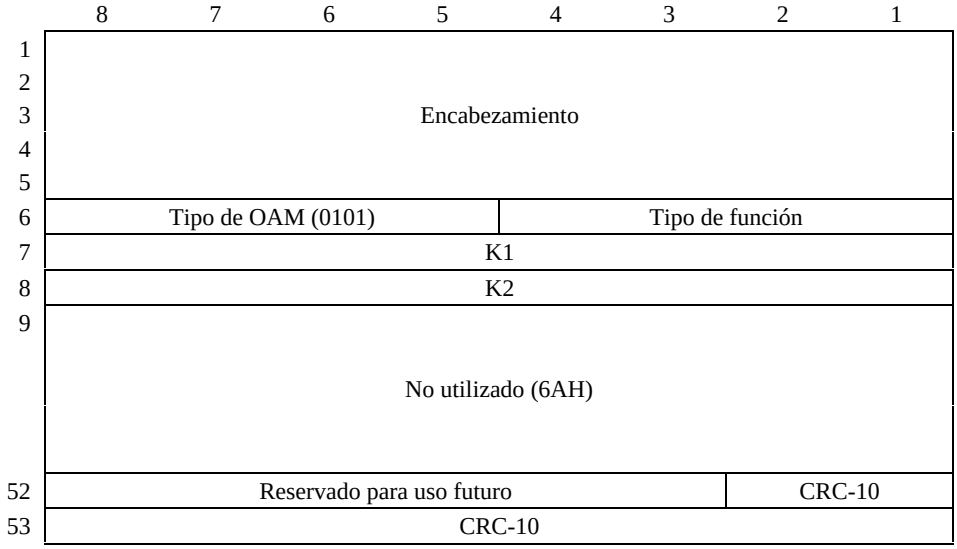


Figura 9/I.630 – Formato de células APS

Cuadro 1/I.630 – Puntos de código para la célula APS

Tipo de OAM	Codificación	Tipo de función	Codificación
Protocolo de coordinación	0101	Protección de grupo	0000
		Protección individual	0001

6 Conmutación de protección de VP/VC del ATM

6.1 Requisitos y objetivos específicos

Los requisitos y objetivos generales de 5.1.2 son aplicables a la conmutación de protección de VP/VC del ATM.

6.2 Mecanismo activador de la conmutación de protección

Deberá llevarse la conmutación de protección a cabo cuando:

1) la inicie el control de operador (por ejemplo, conmutación manual, conmutación forzada, exclusión de protección),
2) se detecte SF,
3) se detecte SD, o
4) expire el temporizador de "espera al restablecimiento".

6.2.1 Control de operador

El control por parte del operador de la función de conmutación de protección puede ser transferido vía interfaces de la RGT (interfaces F o Q3 [8] y [9]).

6.2.2 Activación por fallo de señal

La conmutación de protección de VP/VC individual (unidireccional o bidireccional), en los casos en que el dominio protegido va acompañado de un segmento OAM, se inicia cuando el estado seg_AIS continúa más allá del tiempo de retención establecido en el sumidero del dominio protegido para las entidades de trabajo y protección respectivamente.

La conmutación de protección de VP/VC individual (unidireccional o bidireccional), en los casos en que el dominio protegido va acompañado de una conexión de extremo a extremo, se inicia cuando el estado e-t-e_AIS continúa más allá del tiempo de retención establecido en el sumidero del dominio protegido para las entidades de trabajo y protección respectivamente.

La conmutación de protección unidireccional de VP/VC individual 1+1, en el caso de protección de conexión de subred con supervisión no intrusiva, se inicia cuando el estado e-t-e_AIS (determinado localmente utilizando supervisión no intrusiva) continúa más allá del tiempo de retención establecido en el sumidero del dominio protegido para las entidades de trabajo y protección respectivamente.

Los formatos de la célula e-t-e_/seg_VP-AIS y la célula e-t-e_/VC-AIS así como las condiciones de declaración y liberación del estado AIS se especifican en la Recomendación I.610 [5].

6.2.3 Activación por degradación de señal

La degradación de la calidad de funcionamiento de las entidades de trabajo y protección se puede detectar con los flujos OAM de calidad de funcionamiento de extremo a extremo o de segmento.

Los detalles quedan en estudio.

7 Conmutación de protección de grupo de VP/VC del ATM

7.1 Requisitos y objetivos específicos

Los requisitos y objetivos generales de 5.1.2 son aplicables a la conmutación de protección de VPG/VCG del ATM.

7.2 Arquitectura

7.2.1 Introducción

La entidad lógica de la agrupación de protección en la capa ATM es el grupo de trayectos virtuales (VPG, *virtual path group*) y el grupo de canales virtuales (VCG, *virtual channel group*).

Un VPG/VCG (VPG/VCG de trabajo [VPG_W/VCG_W] o VPG/VCG de protección [VPG_P/VCG_P]) es una agrupación lógica de una o más conexiones de red y/o subred de VP/VC del ATM que comparten el mismo o los mismos trayectos de transmisión dentro del dominio protegido. El VPG/VCG es configurado por el operador en la fuente y también en el sumidero del dominio protegido. En caso de conmutación de protección, todos los VP/VC contenidos en el VPG/VCG, salvo por lo que se refiera al VPC/VCC con APS, se conmutan simultáneamente. Véase en la figura 10 un ejemplo de los VPG.

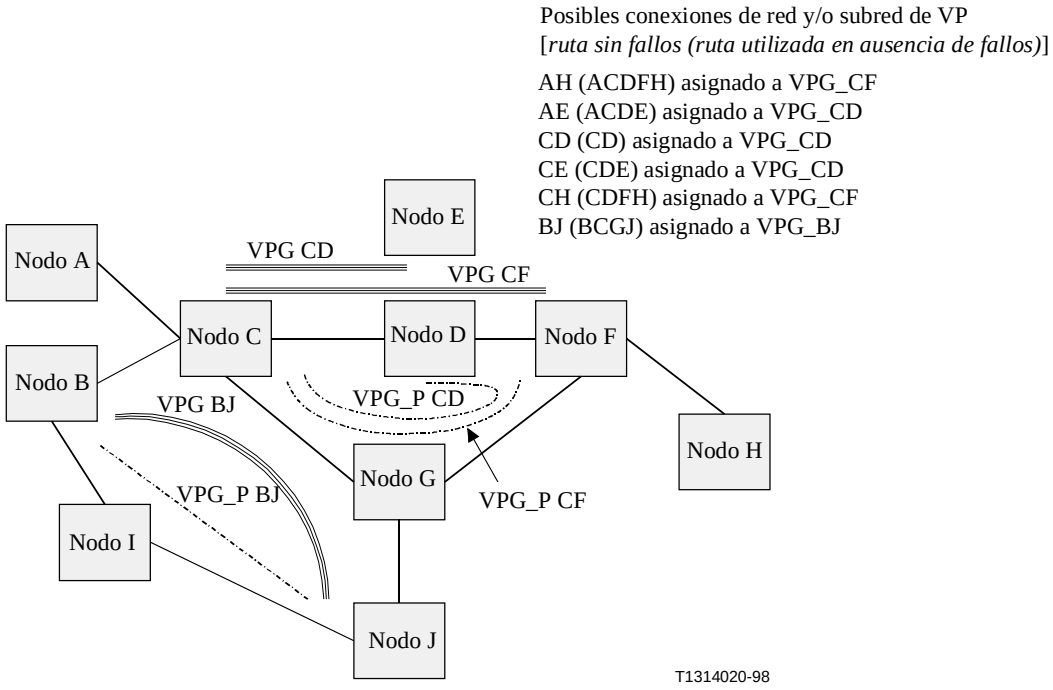


Figura 10/I.630 – Ejemplo de VPG

7.2.2 Generalidades

El esquema de conmutación de protección de VPG/VCG aquí definido tiene las siguientes características arquitecturales:

- utiliza un algoritmo de control distribuido;
- utiliza recursos de ruta especializada y anchura de banda especializada para la entidad de protección;
- la fuente y el sumidero del dominio protegido pueden estar asociados con, o disociados de, los puntos de extremo de la conexión/el segmento OAM;
- actualmente se define sólo para configuraciones lineales y es independiente de la topología de la capa de servidor (es decir, de la capa física);

- la iniciación de la acción de protección se puede retardar durante un periodo ajustable (tiempo de retención), para permitir que la acción de la capa o de las capas de servidor se ejecute primero.

7.2.3 Arquitectura de protección 1+1 de VPG/VCG

La figura 11 ilustra la arquitectura de la configuración 1+1 de VPG/VCG (sólo se muestra uno de los sentidos de la transmisión).

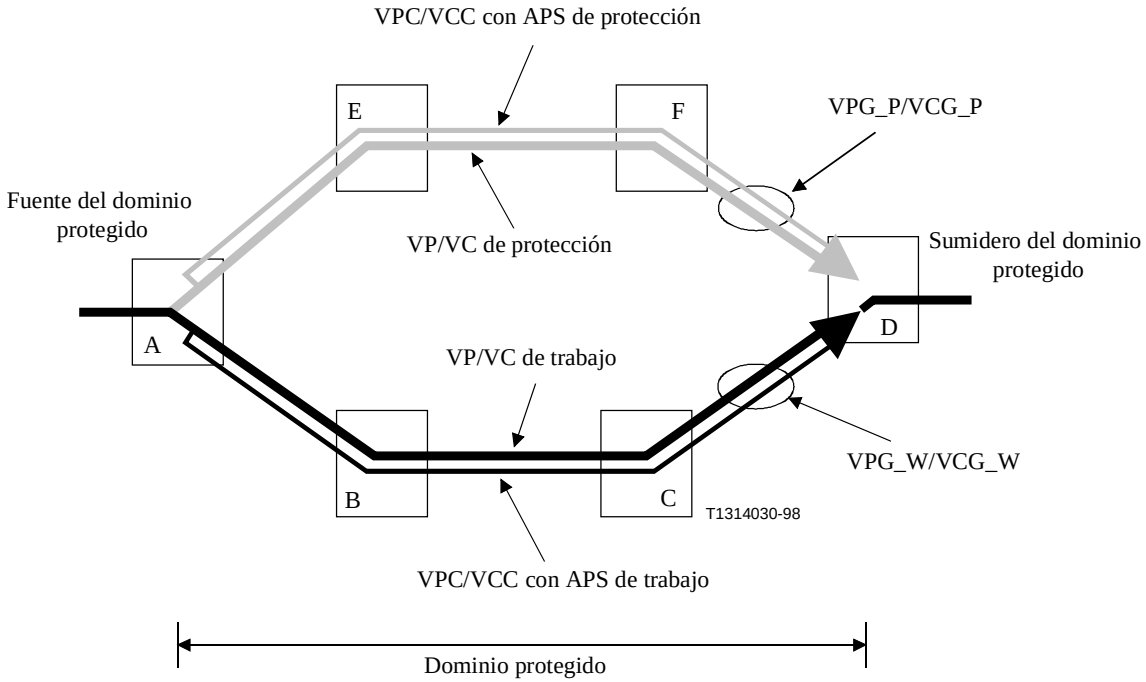


Figura 11/I.630 – Configuración 1+1 de VPG/VCG

Se señala que en la fuente del dominio protegido, el tráfico de trabajo está puenteado permanentemente a la entidad de protección.

7.2.4 Arquitectura de protección 1:1 de VPG/VCG

La figura 12 ilustra la arquitectura de la configuración 1:1 de VPG/VCG (sólo se muestra uno de los sentidos de la transmisión).

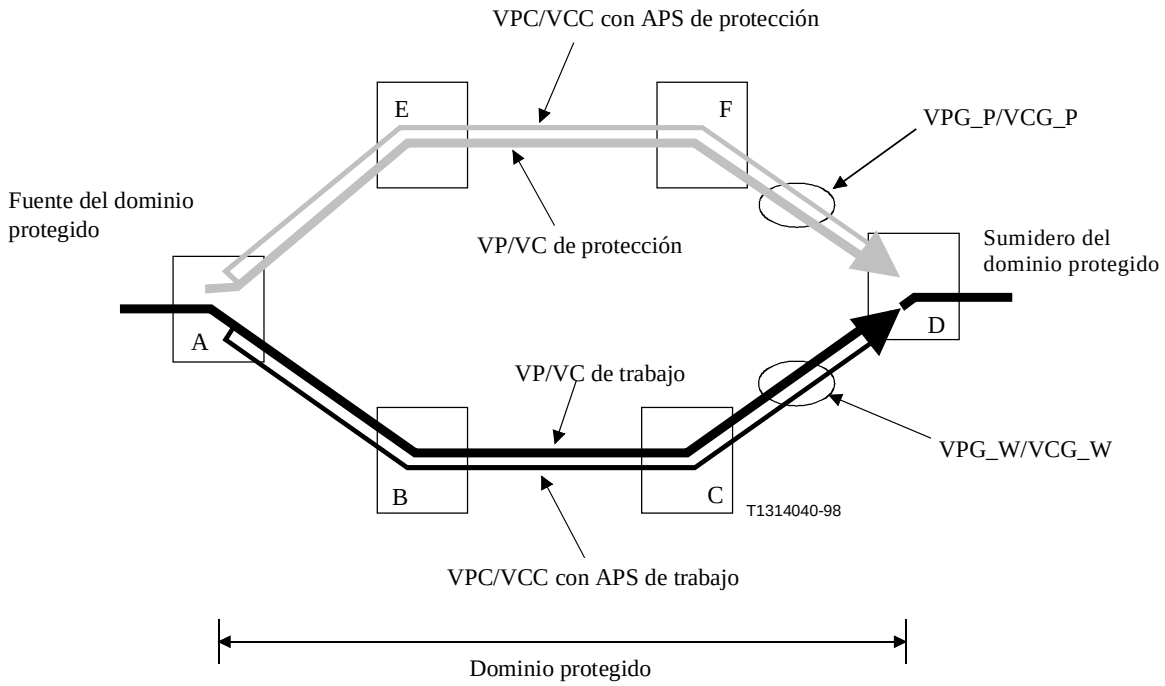


Figura 12/I.630 – Configuración 1:1 de VPG/VCG

Se señala que este puente es considerado funcionalmente como un conmutador simple (que transmite tráfico alternativamente a las entidades de trabajo o a las entidades de protección), y no como un puente de difusión como en la figura 11, en donde el tráfico se puentea tanto a las entidades de trabajo como a las entidades de protección.

7.2.5 Arquitectura de protección 1:N (N>1) de VPG/VCG

Queda en estudio.

7.2.6 Arquitectura de protección M:N de VPG/VCG

Queda en estudio.

7.3 Mecanismo de activación de la conmutación de protección

Deberá llevarse a cabo la conmutación de protección cuando:

1) la inicie el control de operador (por ejemplo, conmutación manual, conmutación forzada, exclusión de protección);

2 se detecte SF;

3) se detecte SD; o

4) expire el temporizador de "espera al restablecimiento".

7.3.1 Control de operador

El control por parte del operador de la función de conmutación de protección puede ser transferido vía interfaces de la RGT (interfaces F o Q3 [8] y [9]).

7.3.2 Activación por fallo de señal

Para la protección de grupo (unidireccional o bidireccional) que utiliza VPC/VCC con APS, la conmutación de protección es iniciada cuando el estado AIS de extremo a extremo continúa más allá

del tiempo de retención establecido en el sumidero del dominio protegido para la VPC/VCC con APS asociada.

7.3.3 Activación por degradación de señal

Queda en estudio.

ANEXO A

Protocolo de coordinación de la conmutación de protección para las configuraciones 1+1/1:1

A.1 Introducción general

El protocolo de coordinación de la conmutación de protección descrito en este anexo se puede aplicar a las configuraciones lineales 1+1 y 1:1.

A.1.1 Arquitectura de aplicación

El protocolo de conmutación de protección ATM lineal 1+1/1:1 descrito en la subcláusula siguiente se puede aplicar a arquitecturas de protección ATM lineales (punto a punto) de la clase conmutación de protección (PS, *protection switching*), con recurso de protección especializada (ruta y anchura de banda atribuidas previamente) y control distribuido (el algoritmo de protección actúa en elementos de red ATM en ambos extremos del dominio de protección).

El dominio protegido puede ser una conexión de VP (o VC) de extremo a extremo, o un segmento de una conexión de VP (o VC) para la protección individual. La aplicación al caso en que el dominio protegido no va acompañado de una conexión de extremo a extremo ni de un segmento OAM queda en estudio.

Este protocolo se aplica también a la protección de grupo además de a la protección individual. La información de coordinación APS se lleva a través de una conexión especializada (canal APS) para la protección del grupo. El dominio protegido puede estar alineado con, o ser independiente de, una conexión de extremo a extremo o un segmento OAM.

El protocolo soporta arquitecturas 1+1. Soporta también la arquitectura 1:1 con o sin tráfico adicional. El tráfico adicional es un tráfico de prioridad baja, que se puede transmitir vía la entidad de protección mientras ésta no esté siendo utilizada para transmitir tráfico de trabajo.

Un esquema de protección 1:1 es, por su propia naturaleza, más lento que un esquema 1+1 en la conmutación, exigiendo comunicación entre ambos extremos del dominio de protección para efectuar incluso una operación de conmutación unidireccional, pero tiene la ventaja del soporte facultativo de tráfico adicional. Además, en las configuraciones 1:1 sin tráfico adicional, la anchura de banda de la entidad de protección se atribuye previamente pero no se utiliza en la práctica en condiciones de ausencia de fallos.

A.1.1.1 Arquitectura 1+1

La figura A.1 ilustra la arquitectura de conmutación de protección lineal 1+1. El tráfico está puenteado permanentemente tanto a la entidad de trabajo (#1) como a la entidad de protección (#0). En la figura, se muestra el tráfico recibido vía el selector y procedente de la entidad de trabajo (#1). Se señala que la función selector utiliza la funcionalidad de encaminamiento VPI/VCI y se puede implementar de dos maneras:

– como un cambio de las tablas de encaminamiento VPI/VCI que se hace en el caso de una conmutación de protección; o

– inhibiendo simplemente el tráfico procedente de la entidad de trabajo o la entidad de protección, con las tablas de encaminamiento VPI/VCI configuradas para una función lógica "OR" de todo el tráfico procedente de la entidad de trabajo y la entidad de protección.

La figura A.2 ilustra una situación en la que se ha producido una conmutación de protección (bidireccional), debido a una condición de fallo de señal en la entidad de trabajo (#1).

A.1.1.2 Arquitectura 1:1

La figura A.3 ilustra la arquitectura de conmutación de protección lineal 1:1, con el tráfico de trabajo transmitido vía la entidad de trabajo (#1). El tráfico adicional que se transmite por la entidad de protección es facultativo. La función selector del tráfico de trabajo es la misma que para la arquitectura 1+1. El selector de tráfico adicional utiliza también la funcionalidad de encaminamiento VPI/VCI con lo que el tráfico se encamina de acuerdo con el valor de VPI/VCI a la salida del tráfico adicional.

La figura A.4 ilustra una situación en la que se ha producido una conmutación de protección (bidireccional), debido a una condición de fallo de señal en la entidad de trabajo (#1). En el lado transmisión, el tráfico de trabajo es puenteado a la entidad de protección y el tráfico adicional es eliminado. Se señala que el puente se considera funcionalmente como una simple conmutación (transmitiendo tráfico alternativamente a las entidades de trabajo o a las entidades de protección), y no como un puente de difusión como en la figura A.1, en donde el tráfico se puentea tanto a las entidades de trabajo como a las entidades de protección. En el lado recepción se activa el selector, de manera que el tráfico de trabajo se recibe de la entidad de protección. Al mismo tiempo, se inhibe la recepción de tráfico adicional y se inserta AIS en sentido descendente en la salida del tráfico adicional. Durante la operación de conmutación de protección, se puede producir una desadaptación transitoria entre las posiciones del puente selector en las ubicaciones OESTE y ESTE. Sin embargo, no es posible que se produzcan conexiones erróneas entre tráfico de trabajo y tráfico adicional, porque el tráfico se encamina siempre correctamente a través de la función selector, en base al valor de VPI/VCI, ya sea a la salida del tráfico de trabajo o a la del tráfico adicional. Se señala que, para conseguir este encaminamiento VPI/VCI, se deben configurar diferentes valores de VPI/VCI en la entidad de protección para tráfico de trabajo y tráfico adicional. Esto se puede lograr automáticamente configurando una ruta VPI/VCI individual para el tráfico de trabajo vía la entidad de protección; el tráfico sólo se puentea entonces a esta ruta en caso de conmutación de protección. Se señala que en el caso de protección individual de VP/VC, si en la entidad de protección están configuradas diferentes valores de VPI/VCI para tráfico de trabajo y tráfico adicional, la supervisión de SF/SD y la comunicación del protocolo de protección sólo se aplican el valor de VPI/VCI configuración para el tráfico de trabajo.

El encaminamiento del tráfico de acuerdo con el valor de VPI/VCI en la función selector significa que, para arquitecturas 1:1 no es posible que se produzcan jamás conexiones erróneas de tráfico. De esta manera se simplifica en gran medida la funcionalidad del protocolo de conmutación de protección, lo que permite la utilización de un protocolo de una fase, requiriéndose un sólo intercambio de información entre ambos extremos para completar una conmutación bidireccional. Por el contrario, no es posible el encaminamiento VPI/VCI para proteger secciones múltiplex de redes SDH. Se necesita por tanto un protocolo de dos o tres fases, en el caso de arquitecturas de 1:n, para evitar aquellas situaciones en las que se podría activar un selector antes que un puente, creando conexiones erróneas temporales entre tráfico de trabajo y tráfico adicional.

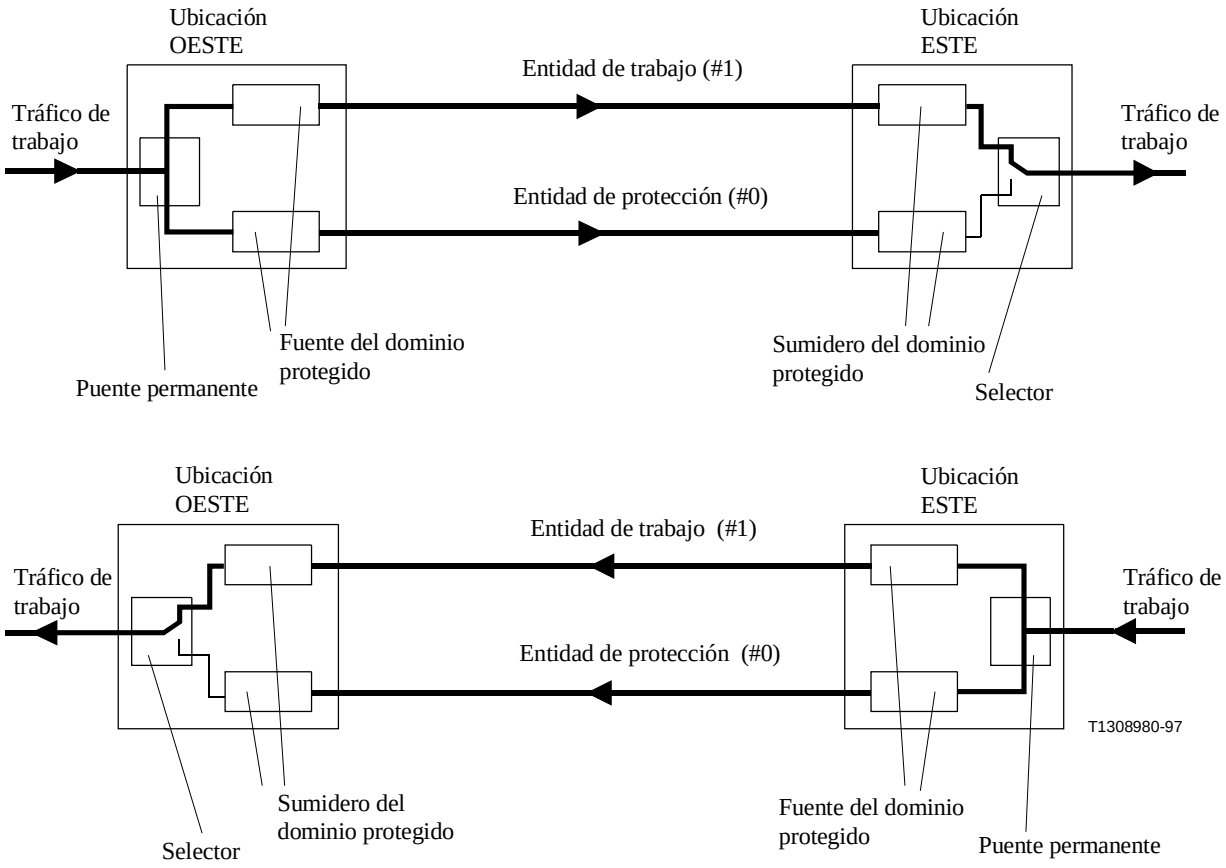


Figura A.1/I.630 – Arquitectura de conmutación de protección lineal 1+1 – El selector está posicionado para recibir tráfico de la entidad de trabajo (#1)

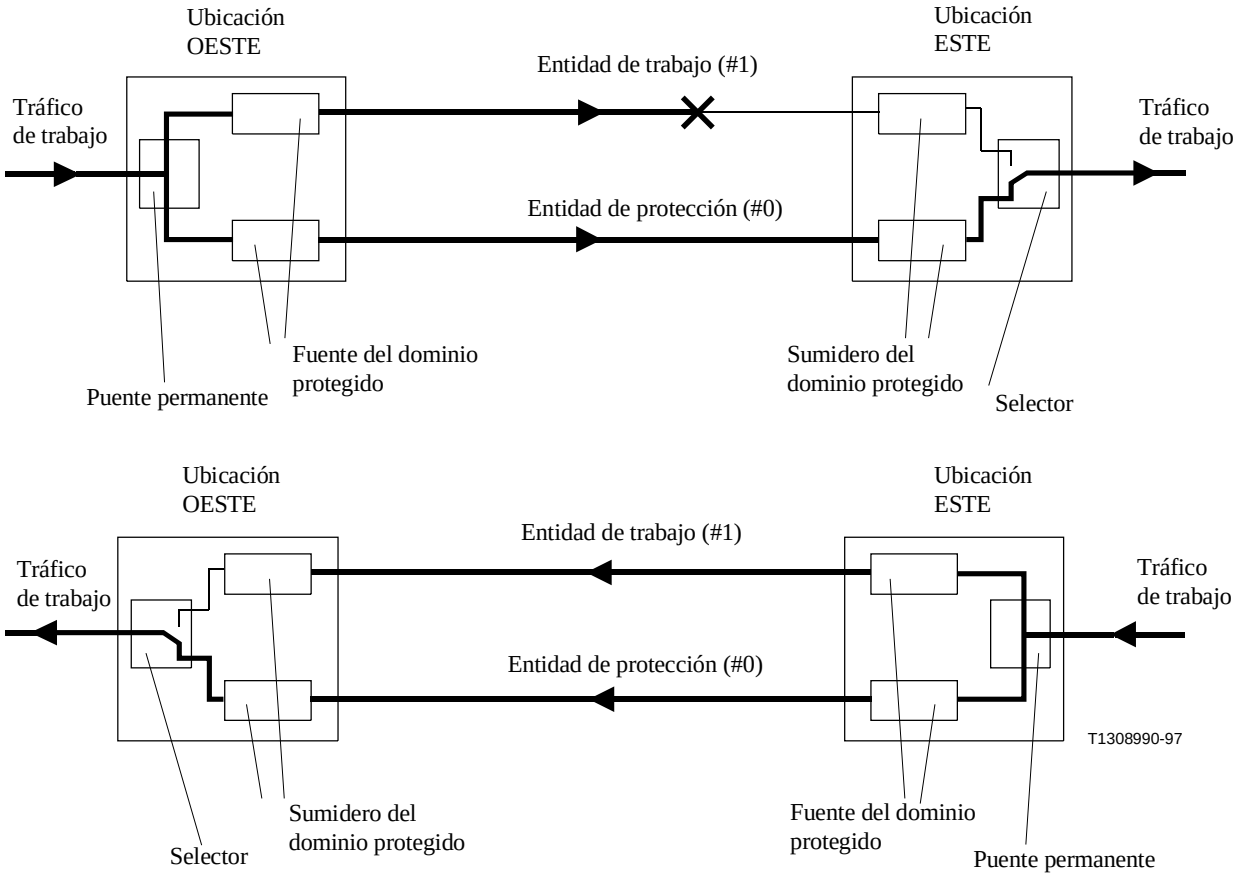


Figura A.2/I.630 – Arquitectura de conmutación de protección lineal 1+1 – El selector está posicionado para recibir tráfico procedente de la entidad de protección (#0) debido a condición de fallo de señal unidireccional para entidad de trabajo (#1)

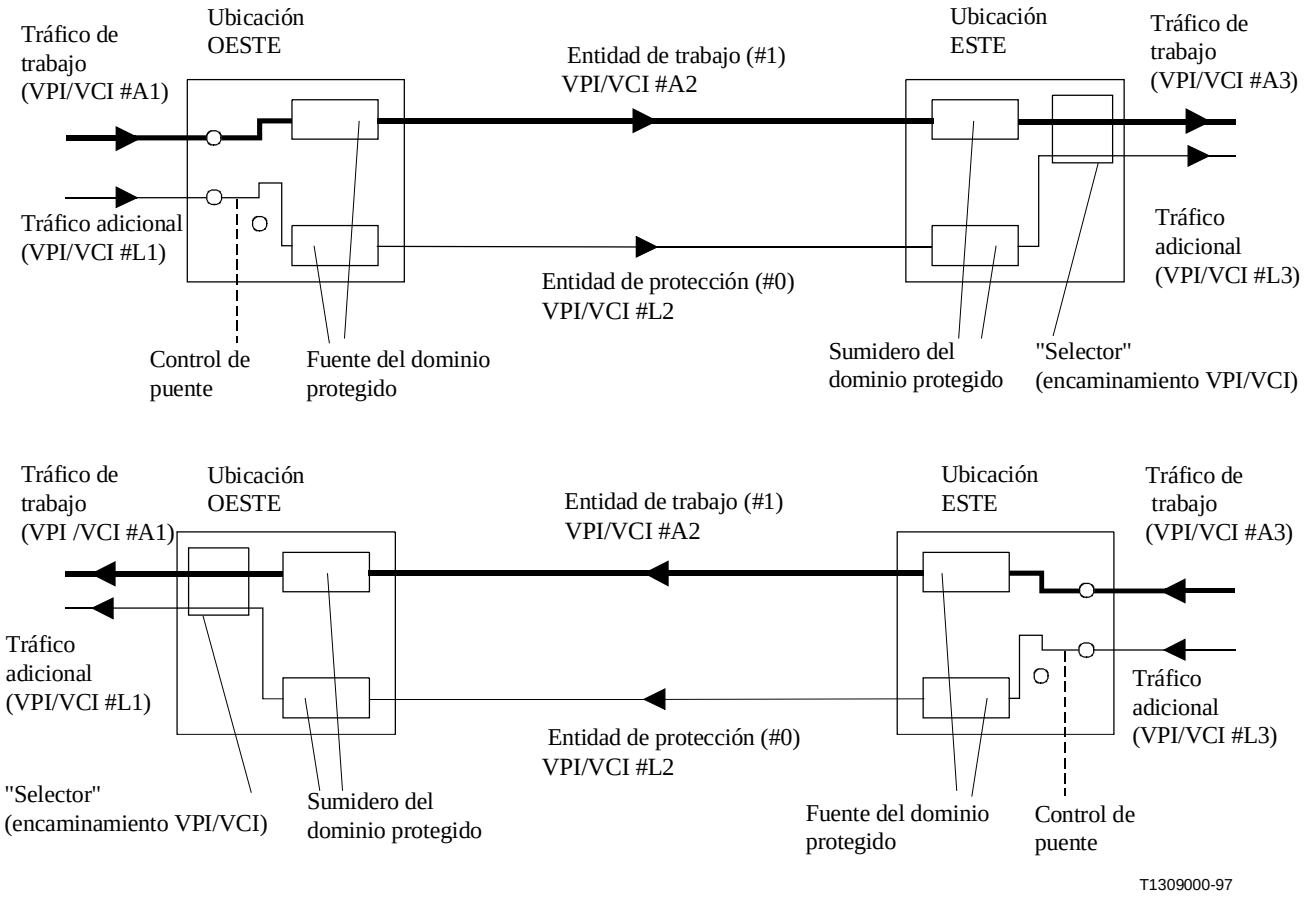


Figura A.3/I.630 – Arquitectura de conmutación de protección lineal 1:1 – Transmisión de tráfico de trabajo vía entidad de trabajo (#1)

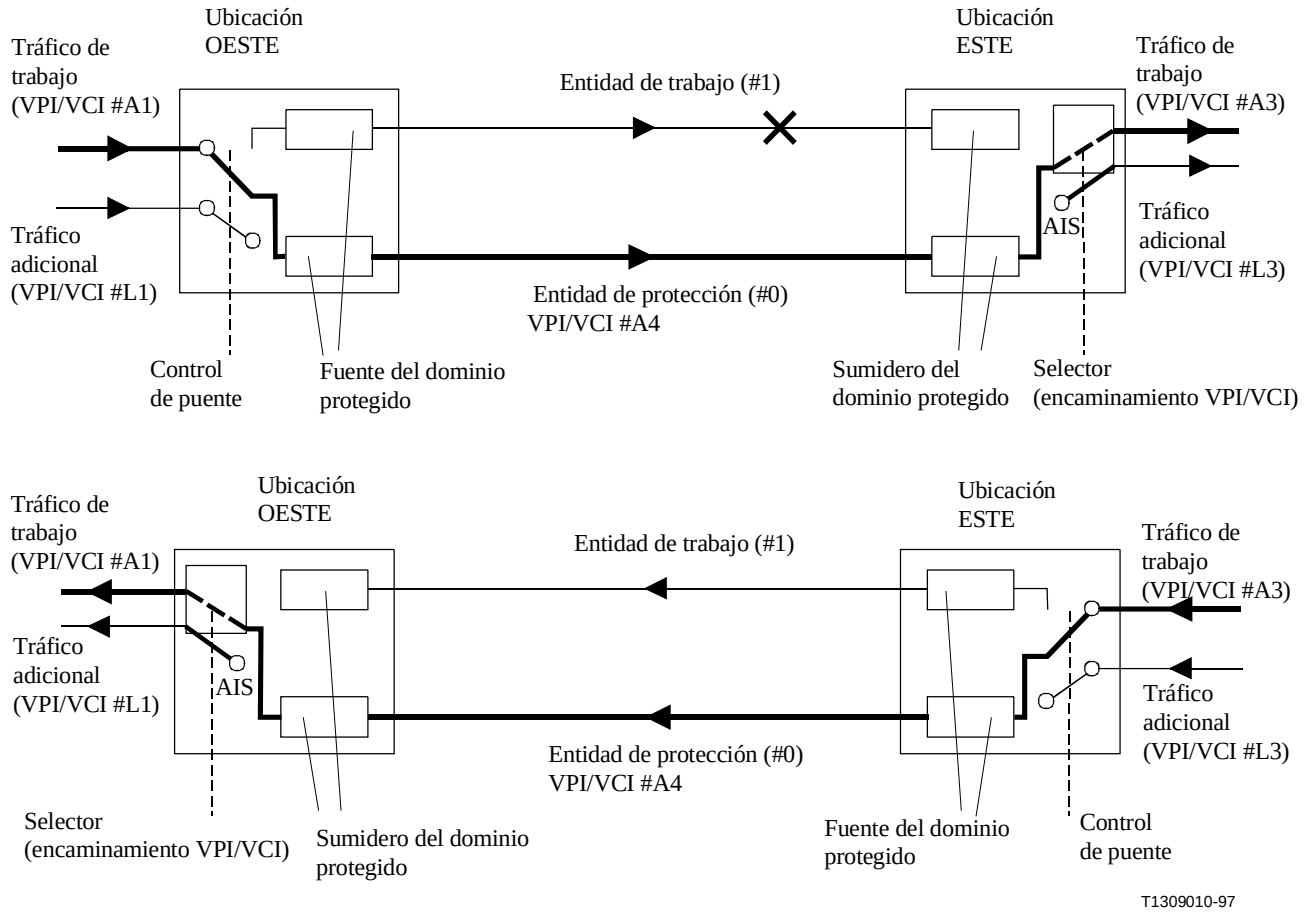


Figura A.4/I.630 – Arquitectura de conmutación de protección lineal 1:1 – Transmisión de tráfico de trabajo vía entidad de protección (#0) debido a condición de fallo de señal unidireccional para entidad de trabajo (#1)

A.1.2 Conformidad con los objetivos de red

Los objetivos de red importantes se examinan desde la perspectiva de su cumplimiento por parte del protocolo de conmutación de protección de ATM que se describe en A.2.

1) *Alcance de la protección*

En el caso de un solo fallo en un punto, se restablece todo el tráfico que hubiera pasado a través de la ubicación en fallo, si éste no se hubiera producido. En el caso de fallos múltiples, el fallo con prioridad más alta adquiere precedencia. Por ejemplo, un fallo de tipo SF tiene precedencia con respecto a un fallo de tipo SD.

2) *Tipos de conmutación*

El presente anexo se refiere a la conmutación bidireccional.

3) *Protocolo de conmutación de protección*

El protocolo PS es sencillo, rápido y resistente. Su sencillez ayuda a la implementación y transparencia de la operación. Un protocolo rápido (o de "toma de contacto optimizada") facilita el cumplimiento del tiempo de compleción de la conmutación requerido. El protocolo es resistente por su propia sencillez, haciendo así poco probable un funcionamiento defectuoso (por errores de implementación residuales).

4) *Modos de funcionamiento*

Se proporciona conmutación reversiva. Con arquitecturas 1:1 sin tráfico adicional y arquitecturas 1+1, también es posible la conmutación no reversiva.

5) *Control manual*

Se soporta el control por parte del operador mediante las instrucciones congelación de la función, conmutación de protección local, exclusión de protección, conmutación forzada y conmutación manual. No son necesarias instrucciones de ejercicio, por la sencillez del protocolo.

6) *Otros criterios para la iniciación de la conmutación*

Además de las instrucciones de control manual indicadas más arriba, se soportan como criterios para la iniciación (o prevención) de una conmutación de protección un fallo de señal, una degradación de señal, un estado de espera al restablecimiento, de no revertir y de ninguna petición.

A.2 Protocolo de conmutación de protección lineal 1+1/1:1

A.2.1 Criterios para la iniciación de la conmutación

Existen los siguientes criterios para la iniciación de la conmutación:

1) una instrucción iniciada externamente (eliminación, congelación de la función conmutación de protección local, exclusión de protección, conmutación forzada, conmutación manual);

2) una instrucción iniciada automáticamente (fallo de señal o degradación de señal) asociada con un dominio de protección; o

3) un estado (espera al restablecimiento, no revertir, ninguna petición) de la función conmutación de protección.

A.2.1.1 Instrucciones iniciadas externamente

La relación de instrucciones iniciadas externamente se indica más abajo, en orden descendente de prioridad. Cada instrucción puede aplicarse al elemento de red OESTE o ESTE de un esquema APS lineal (véase, por ejemplo, la figura A.1).

Eliminación: esta instrucción elimina todas las instrucciones de conmutación enumeradas a continuación para el elemento de red asociado. Se señala que la instrucción eliminación sólo se utiliza para reponer la instrucción congelación de la función conmutación de protección local, exclusión de protección, conmutación forzada o conmutación manual. Esta instrucción no se señala con el protocolo de conmutación de protección.

Congelación de la función conmutación de protección local: congela (mantiene) la posición vigente del puente/selector y los valores de los bytes K1/K2 transmitidos en esos momentos para la función conmutación de protección local. Tiene la máxima prioridad de todas las instrucciones iniciadas externamente, salvo la de eliminación. Así pues, cuando la presente instrucción está en efecto se hace caso omiso de cualquier petición local que no sea la de eliminar. Se señala que los bytes K1/K2 recibidos del extremo distante siguen siendo evaluados, por lo que sigue siendo posible la detección local de una desadaptación de puente/selector. Esta instrucción no se señala con el protocolo de conmutación de protección.

NOTA – El objetivo principal de esta instrucción es el mantenimiento. Cuando en la entidad de trabajo se efectúan tareas de mantenimiento, se puede pedir la no utilización de dicha entidad incluso si falla la de protección. No se puede utilizar, a tal efecto, la instrucción conmutación forzada (FS) porque sería invalidada

por un fallo de señal (SF) para entidad de protección. Un ejemplo de posible escenario de mantenimiento a este respecto es como sigue:

1) Confirmación de que la entidad de protección no ha fallado.

2) Emisión de una instrucción FS para conmutar a la entidad de protección.

3) Emisión de una instrucción "congelación de la función conmutación de protección local".

4) Realización de las tareas de mantenimiento en la entidad de trabajo.

5) Eliminación de la instrucción "congelación de la función conmutación de protección local".

Exclusión de protección (LoP): deniega el acceso de todo el tráfico de trabajo (pero no del tráfico adicional) a la entidad de protección.

Conmutación forzada (FS) para entidad de trabajo (#1): puentea/conmuta el tráfico de trabajo (#1) a la entidad de protección, a menos que exista una condición de fallo de señal para la entidad de protección. Se señala que no se define la conmutación forzada para la entidad de protección (#0), porque esta función se lleva a cabo mediante una instrucción exclusión de protección.

Conmutación manual (MS) para entidad de protección (#0): deniega el acceso del tráfico de trabajo a la entidad de protección, a menos que esté en efecto una petición de prioridad superior (por ejemplo, SF o SD para una entidad de trabajo).

Conmutación manual (MS) para entidad de trabajo (#1): puentea/conmuta el tráfico de trabajo (#1) a la entidad de protección, a menos que esté en efecto una petición de prioridad superior.

Se señala que no se requieren las instrucciones de ejercicio, definidas para algunos protocolos de protección más complejos, y por tanto no se definen.

A.2.1.2 Instrucciones iniciadas automáticamente

Para evitar frecuentes transiciones, la transición de fallo de señal de la condición activa a la condición inactiva sólo deberá producirse si el estado AIS permanece eliminado de manera contínua durante un periodo de persistencia de 5 segundos.

A.2.1.3 Estados

El estado de espera al restablecimiento (WTR, w*ait to restore*) sólo es aplicable al modo reversivo y se aplica a una entidad de trabajo (#1). A este estado pasa la función conmutación de protección local cuando se está recibiendo tráfico de trabajo (#1) vía la entidad de protección, si las peticiones de conmutación de protección local (véase la figura A.5) que estaban previamente activas han pasado ahora a estar inactivas. Impide el retorno a la posición liberado del puente/selector hasta que haya expirado el tiempo de espera al restablecimiento. Dicho tiempo puede ser configurado por el operador en pasos de 1 minuto entre 1 y 30 minutos; el valor por defecto es de 12 minutos.

El estado no revertir (DNR, *do not revert*) sólo es aplicable al modo no reversivo (que es posible en arquitecturas 1:1 sin tráfico adicional o arquitecturas 1+1) y sólo se define para la entidad de trabajo (#1). A este estado pasa la función conmutación de protección local cuando se está transmitiendo tráfico de trabajo (#1) vía la entidad de protección, si las peticiones conmutación de petición local (véase la figura A.5) que estaban previamente activas han pasado ahora a estar inactivas. Impide el retorno a la posición liberado del puente/selector en modo no reversivo en condiciones de ninguna petición.

El estado ninguna petición [(NR, *no request*); que sólo se define para la entidad de protección (#0)] es el estado al que pasa la función conmutación de protección local (véase la figura A.5) en todas las condiciones en que no hay peticiones de conmutación de protección local activas (en concreto las de

espera para el establecimiento y de no revertir); se señala que esto puede ocurrir cuando el puente/selector es activado o cuando es liberado.

A.2.2 Reglas de generación de los bytes K1/K2

NOTA – En este anexo, el bit 1 es el bit más significativo (MSB, *most significant bit*) y el bit 8 es el bit menos significativo (LSB, *least significant bit*).

Para el funcionamiento del protocolo 1+1/1:1 lineal, la información del protocolo se lleva entre los elementos de red situados en las ubicaciones OESTE y ESTE mediante 2 bytes de información llamados K1 y K2. Estos 2 bytes son transportados por células APS vía la entidad de protección (véase, por ejemplo, la figura A.1), siendo insertados por la función fuente del dominio de protección y extraídos por la función sumidero del mismo dominio. Los 8 bits del byte K1 están definidos; sólo los 4 primeros bits del byte K2 lo están.

Las asignaciones de bits para el funcionamiento del protocolo 1+1/1:1 lineal es como sigue:

Los bits 1-8 del byte K1 indican una petición de acción conmutadora de la lógica de prioridad local de la conmutación de protección (véase la figura A.5).

Los bits 1-4 indican el tipo de petición, de los listados en el cuadro A.1.

Los bits 5-8 del byte K1 indican el número de entidad asociada, es decir, si la petición se aplica a la entidad de trabajo (#1 a #n, siendo n inferior o igual a 15) o a la entidad de protección (#0), como sigue:

Bits	
5678	
0000	si la petición se aplica a la entidad de protección.
0001	si la petición se aplica a la entidad de trabajo (#1).

Los bits 1-4 del semibyte K2 indican la situación del puente/selector local de la lógica de prioridad global de la conmutación de protección (véase la figura A.5), de la siguiente manera:

Para el modo de funcionamiento 1+1, la posición del selector de elemento de red local se indica como sigue:

Bits	
1234	
0000	si el selector es activado para recibir tráfico procedente de la entidad de protección (véase le figura A.2).
0001	si el selector es liberado para recibir tráfico procedente de la entidad de trabajo (#1) (véase la figura A.1).

Para el modo de funcionamiento 1:1, la posición del puente/selector del elemento de red local se indica como sigue:

Bits	
1234	
0000	si el puente/selector es liberado de modo que todo el tráfico de trabajo se transmita vía las entidades de trabajo asociadas y el tráfico adicional (si está configurado) se transmita vía la entidad de protección.
0001	si el puente/selector es activado para transmitir tráfico de trabajo (#1) vía la entidad de protección.

Se señala que empleando una estrategia de codificación del byte K2 diferente para funcionamiento 1+1 y para funcionamiento 1:1 se tiene la seguridad de que se generará automáticamente una alarma de desadaptación si el elemento de red en un extremo del dominio de protección está configurado para funcionamiento 1+1 y en el otro extremo está configurado (de manera no intencionada) para funcionamiento 1:1.

Los bits 5-8 del byte K2 no se utilizan para funcionamiento del protocolo 1+1/1:1 lineal.

Cuadro A.1/I.630 – Codificación de las peticiones del byte K1

Codificación del byte K1: bits 1234	**Petición (es decir, instrucción iniciada automáticamente, estado o instrucción iniciada externamente)**	**Orden de prioridad**
1111	Exclusión de protección (nota 1)	Máxima
1110	Fallo de señal para entidad de protección (nota 1)	|
1101	Conmutación forzada para entidad de trabajo (#1) (nota 5)	|
1100	Reservado para uso futuro (nota 2)	|
1011	Fallo de señal para entidad de trabajo (#1)	|
1010	Reservado para uso futuro (nota 2)	|
1001	Degradación de señal para entidad de protección	|
1000	Degradación de señal para entidad de trabajo (#1)	|
0111	Reservado para uso futuro (nota 2)	|
0110	Conmutación manual para entidad de protección	|
0101	Conmutación manual para entidad de trabajo (#1)	|
0100	Reservado para uso futuro (nota 2)	|
0011	Espera al restablecimiento para entidad de trabajo (#1) (nota 3)	|
0010	Reservado para uso futuro (nota 2)	|
0001	No revertir para entidad de trabajo (#1) (nota 4)	|
0000	Ninguna petición (nota 1)	Mínima

Se señala que en el caso en que estén activas simultáneamente más de una petición de la misma prioridad de las indicadas en este cuadro, tiene precedencia la petición con el número de entidad más bajo. Por consiguiente, una petición (por ejemplo, degradación de señal) para la entidad de protección (#0) invalida la misma petición para la entidad de trabajo (#1).

NOTA 1 – Sólo se permite la codificación "0000" de los bits 5-8 del byte K1 con ninguna petición, exclusión de protección, fallo de señal para entidad de protección, degradación de señal para entidad de protocolo, y conmutación manual para entidad de protección.

NOTA 2 – Estos códigos son ignorados por el receptor.

NOTA 3 – Espera al restablecimiento para la entidad de trabajo (#1) sólo es aplicable en caso de funcionamiento reversivo.

NOTA 4 – No revertir para la entidad de trabajo (#1) sólo es aplicable en caso de funcionamiento no reversivo; sólo se permite la codificación "0001" de los bits 5-8 del byte K1.

NOTA 5 – No se define conmutación forzada para entidad de protección (#0) porque a esta función se puede llegar vía una instrucción exclusión de protección.

A.2.3 Algoritmo de conmutación de protección lineal 1+1/1:1

A.2.3.1 Principio de funcionamiento

La figura A.5 ilustra el principio del algoritmo de conmutación de protección lineal 1+1/1:1. Se trata de un algoritmo aplicado en elementos de red a ambos extremos del dominio de protección (ubicaciones OESTE y ESTE). La conmutación bidireccional se consigue transmitiendo peticiones de conmutación local al extremo distante vía el byte K1. El byte K2 transmitido contiene información sobre la situación del puente/selector local; de esta manera, una desadaptación persistente entre ambos extremos puede ser detectada y provocar una alarma.

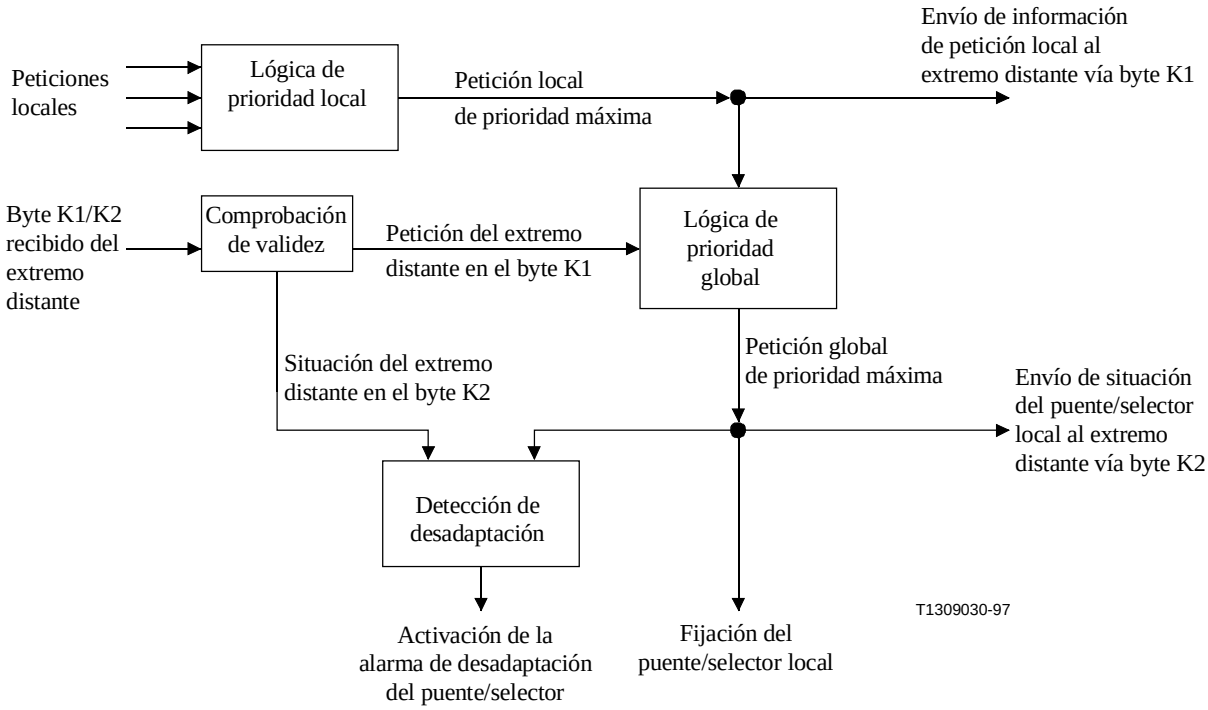


Figura A.5/I.630 – Principio del algoritmo de conmutación de protección lineal 1+1/1:1

La funcionalidad, de manera detallada, es como sigue (véase la figura A.5):

En el elemento de red local, pueden estar activas una o más peticiones de conmutación de protección local (de las indicadas en A.2.1). La "lógica de prioridad local" determina cuál de estas peticiones es la de prioridad máxima, utilizando el orden de prioridad que se da en el cuadro A.1. Esta información de petición local de prioridad máxima se transmite al extremo distante vía el byte K1 (con la codificación que se describe en A.2.2). La información se pasa también a la "lógica de prioridad local".

El elemento de red local recibe información procedente del elemento de red del extremo distante vía los bytes K1 y K2. Los bytes K1/K2 recibidos son sometidos a una comprobación de validez (véase A.2.3.4). La información del byte K1 recibido (que indica la petición local de prioridad máxima del extremo distante) se pasa a continuación a la "lógica de prioridad global". La "lógica de prioridad global" compara la petición local de prioridad máxima con la petición del byte K1 recibido (de acuerdo con el orden de prioridad del cuadro A.1) para determinar cuál es la petición global de prioridad máxima. Esta petición determina entonces la posición (o situación) del puente/selector del elemento de red local como sigue:

– para arquitecturas 1+1 (véanse las figuras A.1 y A.2) sólo se controla la posición del selector. Para arquitecturas 1:1 (véanse las figuras A.3 a A.5) se controlan simultáneamente las posiciones del puente y del selector, es decir, cuando quiera que el puente de un elemento de red es activado (o liberado), el selector del mismo elemento de red es activado (o liberado) al mismo tiempo;
– si la petición global de prioridad máxima es una petición para una entidad de trabajo (véase el cuadro A.1), el tráfico de trabajo asociado es puenteado/conmutado a/de la entidad de protección, es decir, el puente/selector asociado del elemento de red local es activado;
– si la petición global de prioridad máxima es una petición para la entidad de protección (véase el cuadro A.1), el tráfico de trabajo no es puenteado/conmutado a/de la entidad de protección, es decir, el puente/selector asociado del elemento de red local es liberado.

La situación del puente/selector se transmite al extremo distante vía el byte K2 (con la codificación que se describe en A.2.2). Además se compara con la situación del puente/selector del extremo distante indicada por el byte K2 recibido: si una desadaptación entre las posiciones del extremo cercano y el extremo distante persiste durante más de *m* segundos, se activa la alarma de desadaptación del puente/selector para el elemento de red local. El tiempo de persistencia de *m* segundos deberá ser lo suficientemente largo como para permitir la pérdida de 3 células de protocolo APS antes de que se genere la alarma.

Se señala que el algoritmo de conmutación de protección lineal comienza inmediatamente cada vez que una de las señales de entrada (véase la figura A.5) cambia, es decir, cuando cambia la situación de cualquier petición local, o cuando se recibe un byte K1/K2 diferente procedente del extremo distante. Las acciones consiguientes del algoritmo se inician también inmediatamente, es decir, el cambio de posición del puente/selector local (si es necesario), la transmisión de la nueva situación del byte K1/K2 (si es necesario), o la activación de la alarma de desadaptación del puente/selector (si ha terminado el tiempo de persistencia).

A.2.3.2 Modo reversivo

En el modo de funcionamiento reversivo, cuando se está recibiendo tráfico de trabajo (#1) vía la entidad de protección, si las peticiones de conmutación de protección local (véase la figura A.5) que estaban previamente activas han pasado ahora a estar inactivas, se pasa a un estado de espera al restablecimiento local. Puesto que este estado representa ahora la petición local de prioridad máxima, es indicado en el byte K1 transmitido y mantiene el conmutador.

Este estado concluye normalmente y pasa a ser un estado de ninguna petición después de que haya expirado el temporizador de espera al restablecimiento (véase A.2.1.3). El temporizador de espera al restablecimiento se desactiva antes si cualquier petición local de prioridad superior relega este estado.

Se señala que para la decisión de pasar o no al estado espera al restablecimiento, sólo se consideran las peticiones locales. Una conmutación a la entidad de protección puede ser mantenida por un estado de espera al restablecimiento local o por una petición distante (espera al restablecimiento u otra) recibida vía el byte K1. Por consiguiente, si se produce un fallo bidireccional para una entidad de trabajo y se lleva a cabo la reparación subsiguiente, la reversión bidireccional de retorno a la entidad de trabajo no se produce hasta que hayan expirado ambos temporizadores de espera al restablecimiento en ambos extremos.

A.2.3.3 Modo no reversivo

El modo no reversivo sólo es aplicable (como una alternativa al modo reversivo) para arquitecturas 1+1 o arquitecturas 1:1 en configuraciones sin tráfico adicional.

En el modo de funcionamiento no reversivo, cuando se está transmitiendo tráfico de trabajo (#1) vía la entidad de protección, si las peticiones de conmutación de protección local (véase la figura A.5) que estaban previamente activas pasan ahora a estar inactivas, se pasa a un estado de no revertir local. Puesto que este estado representa ahora la petición local de prioridad máxima, es indicado en el byte K1 transmitido y mantiene el conmutador, evitando así la reversión de vuelta a la posición de puente/selector liberado en modo no reversivo en condiciones de ninguna respuesta.

A.2.3.4 Transmisión y aceptación de bytes de protocolo de protección

Los bytes K1/K2 del protocolo de protección son transportados por células APS vía la entidad de protección (véase, por ejemplo, la figura A.1), siendo insertados por la función fuente del dominio de protección y extraídos por la función sumidero del mismo dominio.

Se debe transmitir inmediatamente una célula APS nueva cada vez que se produce un cambio en la situación del byte K1 o K2 transmitido (véase la figura A.5).

Para evitar la inundación de células APS en los casos en que el sensor de fallo de señal oscile rápidamente, la transición de fallo de señal de la condición activa a la condición inactiva durante el procesamiento de las peticiones locales (véase la figura A.5) sólo deberá ocurrir si el estado AIS permanece eliminado de manera continua durante un periodo de persistencia de 5 segundos.

Para asegurar el funcionamiento del protocolo en las situaciones en que las células APS se hayan perdido o no sean válidas, el elemento de red transmitirá una célula APS con la situación de transmisión del byte K1/K2 vigente de manera permanente cada 5 segundos (mecanismo de "mantenimiento en activo"). Así se elimina la necesidad de complejos escenarios de protocolo de retransmisión en el caso en que se pierdan células APS, o no sean válidas. Con arquitecturas 1:1, esto da lugar a un retardo de 5 segundos en la compleción de la conmutación de protección si se pierde una célula APS, o no es válida.

Si se reciben bytes K1/K2 no válidos, siguen siendo aplicables los últimos bytes recibidos válidos. Durante las condiciones de fallo de señal de la entidad de protección (prorrogadas 5 segundos como se describe más arriba), no se evalúan los bytes K1/K2.

A.2.3.5 Ejemplo de protocolo para arquitectura 1+1 en modo no reversivo

El cuadro A.2 ilustra la acción de conmutación de protección (en modo no reversivo) para este esquema.

Cuando se está recibiendo tráfico procedente de la entidad de trabajo (#1) en condiciones de ausencia de fallos, se indica ninguna petición con número de entidad "0" para los bytes K1 transmitidos en ambos extremos. Los bits 1-4 de los bytes K2 transmitidos en ambos extremos se fijan en "0001" para indicar que el selector se ha liberado y que recibe tráfico de la entidad de trabajo (#1). Véase una ilustración en la figura A.1.

La lógica de prioridad global de cada extremo determina la petición global de prioridad máxima que está activa. Puede ser una petición de extremo distante (recibida vía el byte K1) o una petición local. La lógica de prioridad global fijará el selector local de acuerdo con la petición global de prioridad máxima. La posición resultante del selector se indicará en los bits 1-4 del byte K2. Para la generación del byte K1 transmitido, sólo se considera la petición local de prioridad máxima; las peticiones del extremo distante no se consideran nunca.

En el ejemplo, se detecta SF en la ubicación ESTE de la entidad de trabajo (#1). En consecuencia, la lógica de prioridad global en ESTE activará el selector para recibir tráfico procedente de la entidad de protección (#0). La lógica de prioridad global en OESTE detecta el fallo vía el byte K1 recibido y activa también su selector, manteniendo "ninguna petición" para el byte K1 transmitido, puesto que no hay ninguna petición local activa. Véase una ilustración en la figura A.2.

Después de reparar la entidad de trabajo (#1), se indica "no revertir" en ESTE y los selectores de ESTE y OESTE permanecen activados. El sistema no revierte de vuelta a una entidad preferida como en el caso del funcionamiento reversivo. Se señala que el estado "no revertir" se elimina si es relegado por una petición local. Si, por consiguiente, se detecta a continuación un fallo del tipo SD de la entidad de protección (#0) en ESTE, se indicará en el byte K1 transmitido en ESTE y el selector de ESTE será liberado. La lógica de prioridad global en OESTE detecta el fallo vía el byte K1 recibido y libera también su selector.

Una vez reparada la entidad de protección (#0), se indica de nuevo "ninguna petición" en ambos extremos.

Se señala que, para el mismo ejemplo, con funcionamiento en modo no reversivo nunca se indicará "no revertir". Después de reparar la entidad de trabajo (#1), se indica "espera al restablecimiento" en ESTE en vez de "no revertir". Se señala que el estado "espera al restablecimiento" es eliminado, y el temporizador reiniciado, si ese estado es relegado por una petición local. Cuando expira el temporizador de espera al restablecimiento, ambos selectores son liberados para recibir tráfico procedente de la entidad de trabajo (#1) y se indica "ninguna petición" en ambos extremos.

Cuadro A.2/I.630 – Ejemplo de protocolo para arquitectura 1+1 en modo de funcionamiento no reversivo

Condición de fallo	**Codificación de los bytes del protocolo**				**Acción**	
	ESTE → OESTE		**OESTE → ESTE**			
Bits	**Byte K1 12345678**	**Byte K2 1234**	**Byte K1 12345678**	**Byte K2 1234**	**En la ubicación ESTE**	**En la ubicación OESTE**
Ausencia de fallos. Se recibe tráfico de la entidad de trabajo (#1)	00000000	0001	00000000	0001	Liberación del selector	Liberación del selector
Entidad de trabajo (#1) en fallo en el sentido OESTE → ESTE	10110001	0000	00000000	0001	Detección de petición local. Activación del selector; actualización de K1/K2.	
	10110001	0000	00000000	0000		Detección de petición de extremo distante. Activación del selector; actualización de K1/K2.

Cuadro A.2/I.630 – Ejemplo de protocolo para arquitectura 1+1 en modo de funcionamiento no reversivo *(fin)*

Condición de fallo	Codificación de los bytes del protocolo				Acción	
	ESTE → OESTE		OESTE → ESTE			
Bits	Byte K1 12345678	Byte K2 1234	Byte K1 12345678	Byte K2 1234	En la ubicación ESTE	En la ubicación OESTE
Entidad de trabajo (#1) reparada	00010001	0000	00000000	0000	Detección de eliminación de petición local; paso al estado no revertir; actualización de K1.	
entidad de protección (#0) degradada en el sentido OESTE → ESTE	10010000	0001	00000000	0000	Detección de petición local. Liberación del selector; actualización de K1/K2.	
	10010000	0001	00000000	0001		Detección de petición de extremo distante. Liberación del selector; actualización de K1/K2.
Entidad de protección (#0) reparada	00000000	0001	00000000	0001	Estado ninguna petición. Actualización de K1.	

A.2.3.6 Ejemplo de protocolo para arquitectura 1:1 en modo reversivo

El cuadro A.3 ilustra la acción de conmutación de protección (en modo reversivo) para este esquema.

Durante las condiciones de trabajo normales, todo el tráfico de trabajo se transmite vía las entidades de trabajo asociadas y el tráfico adicional (si está configurado) se transmite vía la entidad de protección (#0). Los puentes/conmutadores en OESTE y ESTE están liberados. Se indica "ninguna petición" con el número de entidad "0" para los bytes K1 transmitidos en ambos extremos, y "0000" para los bytes K2 transmitidos en ambos extremos.

La lógica de prioridad global de cada extremo determina la petición global de prioridad máxima que está activa. Puede ser una petición de extremo distante (recibida vía el byte K1) o una petición local. La lógica de prioridad global fijará el puente/selector local de acuerdo con la petición global de prioridad máxima. La posición resultante del puente/selector se indicará en los bits 1-4 del byte K2. Para la generación del byte K1 transmitido, sólo se considera la petición local de prioridad máxima; las peticiones de extremo distante no se consideran nunca.

En el ejemplo, se detecta SF en la ubicación ESTE de la entidad de trabajo (#1). En consecuencia, la lógica de prioridad global en ESTE activará el puente/selector para transmitir tráfico de trabajo (#1) a la entidad de protección (#0). La lógica de prioridad global en OESTE detecta el fallo vía el byte K1 recibido y activa también su puente/selector, manteniendo "ninguna petición" para el byte K1 transmitido, puesto que no hay ninguna petición local activa. Véase una ilustración en la figura A.5.

Después de reparar la entidad de trabajo (#1), se indica "espera al restablecimiento" en ESTE y los puentes/conmutadores en ESTE y OESTE permanecen activados. Se señala que el estado "espera al restablecimiento" sería eliminado, y el temporizador reiniciado, si ese estado fuera relegado por una petición local. Cuando expira el temporizador de espera al restablecimiento en ESTE, se pasa al estado ninguna petición en ESTE, el puente/selector es liberado y los bytes K1/K2 transmitidos son actualizados. Así pues, se reanuda una vez más el trabajo en el estado de libre de fallos.

Cuadro A.3/I.630 – Ejemplo de protocolo para arquitectura 1:1 en modo de funcionamiento reversivo

Condición de fallo	**Codificación de los bytes del protocolo**				**Acción**	
	ESTE → OESTE		**OESTE → ESTE**			
Bits	**Byte K1 12345678**	**Byte K2 1234**	**Byte K1 12345678**	**Byte K2 1234**	**En la ubicación ESTE**	**En la ubicación OESTE**
Ausencia de fallos. Todo el tráfico de trabajo es transmitido vía entidades de trabajo asociadas	00000000	0000	00000000	0000	Liberación del puente/selector	Liberación del puente/selector
Entidad de trabajo (#1) en fallo en el sentido OESTE → ESTE	10110001	0001	00000000	0000	Detección de petición local. Activación del puente/selector para tráfico de trabajo (#1); actualización de K1/K2.	
	10110001	0001	00000000	0001		Detección de petición de extremo distante. Activación del puente/selector para tráfico de trabajo (#1); actualización de K2.

Cuadro A.3/I.630 – Ejemplo de protocolo para arquitectura 1:1 en modo de funcionamiento reversivo *(fin)*

Condición de fallo	Codificación de los bytes del protocolo				Acción	
	ESTE → OESTE		OESTE → ESTE			
Bits	Byte K1 12345678	Byte K2 1234	Byte K1 12345678	Byte K2 1234	En la ubicación ESTE	En la ubicación OESTE
Entidad de trabajo (#1) reparada	00110001	0001	00000000	0001	Detección de eliminación de petición local. Paso al estado espera al restablecimiento para el tráfico de trabajo (#1); actualización de K1.	
Espera al restablecimiento expirado en ESTE	00000000	0000	00000000	0001	Estado ninguna petición. Liberación del puente/selector; actualización de K1/K2.	
	00000000	0000	00000000	0000		Ninguna petición (ni local ni del extremo distante). Liberación del puente/selector; actualización de K2.

ANEXO B

Funcionamiento de la conmutación de protección de SNC y de camino unidireccional 1+1

B.1 Arquitectura de aplicación

En la figura A.1 se muestra la arquitectura de protección lineal 1+1. En el caso del funcionamiento de conmutación de protección unidireccional que se describe en el presente anexo B, el selector efectúa una conmutación de protección en el sumidero del dominio de protección en base a información puramente local.

Por ejemplo, si se produce un fallo unidireccional (en el sentido de la transmisión OESTE a ESTE) para la entidad de trabajo de la figura A.1, dicho fallo será detectado en el sumidero del dominio de protección de la ubicación ESTE y el selector de la ubicación ESTE conmutará a la entidad de protección. Se señala que el selector de la ubicación OESTE permanece inalterado.

B.2 Conformidad con los objetivos de red

Son aplicables los siguientes objetivos de red:

1) *Tipos de conmutación*

   El presente anexo se refiere a la conmutación de protección unidireccional 1+1.

2) *Protocolo de conmutación de protección*

   No hay protocolo APS para protección de SNC y de camino unidireccional 1+1.

3) *Modos de funcionamiento*

   Se proporciona conmutación reversiva y no reversiva.

4) *Control manual*

   Se soporta el control por parte del operador mediante las instrucciones exclusión de protección, conmutación forzada y conmutación manual.

5) *Otros criterios para la iniciación de la conmutación*

   Además de las instrucciones de control manual indicadas más arriba, se soportan como criterios para la iniciación (o prevención) de una conmutación de protección un fallo de señal, una degradación de señal, un estado de espera al restablecimiento y de ninguna petición.

B.3 Criterios para la iniciación de la conmutación

Existen los siguientes criterios para la iniciación de la conmutación:

1) una instrucción iniciada externamente (eliminación, exclusión de protección, conmutación forzada, conmutación manual);
2) una instrucción iniciada automáticamente (fallo de señal o degradación de señal) asociada con un dominio protegido; o
3) un estado (espera al restablecimiento, ninguna petición) de la función conmutación de protección.

Para la arquitectura 1+1, todas las peticiones son locales. En el cuadro B.1 se da la prioridad de las peticiones locales.

Cuadro B.1/I.630 – Prioridad de las peticiones locales

Petición local (es decir, instrucción iniciada automáticamente, estado o instrucción iniciado externamente)	**Orden de prioridad**
Eliminación	Máxima
Exclusión de protección	|
Conmutación forzada	|
Fallo de señal	|
Degradación de señal	|
Conmutación manual	|
Espera al restablecimiento	|
Ninguna petición	Mínima

NOTA 1 – Una conmutación forzada para entidad de trabajo no deberá ser invalidada por un fallo de señal en la entidad de protección. Puesto que se está efectuando una conmutación de protección unidireccional y no se soporta ningún protocolo APS en la entidad de protección, el fallo de la señal en dicha entidad no interfiere con la capacidad de efectuar una conmutación forzada para una entidad de trabajo.

NOTA 2 – No se define una conmutación forzada para entidad de protección porque esta función se puede llevar a cabo mediante una instrucción exclusión de protección.

B.3.1 Instrucciones iniciadas externamente

La relación de instrucciones iniciadas externamente se indica más abajo, en orden descendente de prioridad. A continuación se describe la funcionabilidad de cada una de ellas.

Eliminación: esta instrucción elimina todas las instrucciones de conmutación iniciadas externamente y enumeradas a continuación.

Exclusión de protección (LoP*, lockout of protection*): impide que el selector conmute a la entidad de protección, o conmuta el selector de la entidad de protección a la entidad de trabajo.

Conmutación forzada (FS*, forced switch*): **para entidad de trabajo**: conmuta el selector de la entidad de trabajo a la entidad de protección (a menos que esté en efecto una petición de conmutación de prioridad igual o superior).

Conmutación manual (MS*, manual switch*): **para entidad de trabajo**: conmuta el selector de la entidad de trabajo a la entidad de protección (a menos que esté en efecto una petición de conmutación de prioridad igual o superior).

Conmutación manual (MS) para entidad de protección: conmuta el selector de la entidad de protección a la entidad de trabajo (a menos que esté en efecto una petición de conmutación de prioridad igual o superior).

B.3.2 Instrucciones iniciadas automáticamente

Para evitar frecuentes transiciones, la transición de fallo de señal de la condición activa a la condición inactiva sólo deberá producirse si el estado AIS permanece eliminado de manera continua durante un periodo de persistencia de 5 segundos.

B.3.3 Estados

El estado espera al restablecimiento sólo es aplicable al modo reversivo y se aplica a una entidad de trabajo. A este estado pasa la función conmutación de protección local cuando se está recibiendo tráfico de trabajo vía la entidad de protección, si las peticiones de conmutación de protección local que previamente estaban activas han pasado ahora a estar inactivas. Impide el retorno a la posición liberado del selector hasta que haya expirado el tiempo de espera al restablecimiento. Dicho tiempo puede ser configurado por el operador en pasos de 1 minuto entre 1 y 30 minutos; el valor por defecto es de 12 minutos.

El estado ninguna petición es el estado al que pasa la función de conmutación de protección local en todas las condiciones en que no hay peticiones de conmutación de protección local activas (en concreto, la de espera al restablecimiento); se señala que esto puede ocurrir cuando el selector es activado o cuando es liberado.

B.4 Protocolo de conmutación de protección

En la arquitectura 1+1 unidireccional no hay protocolo APS.

B.5 Funcionamiento del algoritmo de conmutación de protección unidireccional 1+1

B.5.1 Control del puente

En la arquitectura 1+1, el tráfico de trabajo está puenteado permanentemente a las entidades de trabajo y protección.

B.5.2 Control del selector

En la arquitectura 1+1 en funcionamiento de conmutación de protección unidireccional, el selector es controlado por la petición local de prioridad máxima (instrucción iniciada automáticamente, estado, o instrucción iniciada externamente). Por consiguiente, cada extremo funciona independientemente del otro. Si existe una condición de prioridad igual (por ejemplo, SF, SD) en ambas entidades, no se llevará a cabo la conmutación.

B.5.3 Modo reversivo

En el modo de funcionamiento reversivo, cuando se está recibiendo tráfico de trabajo vía la entidad de protección, si las peticiones de conmutación de protección local que estaban previamente activas han pasado ahora a estar inactivas, se pasa a un estado de espera al restablecimiento local.

Este estado concluye normalmente y pasa a ser un estado de ninguna petición después de que haya expirado el temporizador de espera al restablecimiento. El temporizador de espera al restablecimiento se desactiva antes si cualquier petición local de prioridad superior relega este estado.

B.5.4 Modo no reversivo

Cuando la entidad en fallo ya no está en una condición de SD o SF, y no está presente ninguna otra instrucción iniciada externamente, se pasa a un estado de ninguna petición. Durante este estado, no se producen conmutaciones.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie B	Medios de expresión: definiciones, símbolos, clasificación
Serie C	Estadísticas generales de telecomunicaciones
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedios
Serie I	**Red digital de servicios integrados**
Serie J	Transmisiones de señales radiofónicas, de televisión y de otras señales multimedios
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos y comunicación entre sistemas abiertos
Serie Y	Infraestructura mundial de la información y aspectos protocolo Internet
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación