

UIT-T

G.8131/Y.1382

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

(02/2007)

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

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

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

Aspectos del protocolo Internet – Transporte

**Conmutación lineal de protección para las redes
MPLS de transporte**

Recomendación UIT-T G.8131/Y.1382

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

CONEXIONES Y CIRCUITOS TELEFÓNICOS INTERNACIONALES	G.100–G.199
CARACTERÍSTICAS GENERALES COMUNES A TODOS LOS SISTEMAS ANALÓGICOS DE PORTADORAS	G.200–G.299
CARACTERÍSTICAS INDIVIDUALES DE LOS SISTEMAS TELEFÓNICOS INTERNACIONALES DE PORTADORAS EN LÍNEAS METÁLICAS	G.300–G.399
CARACTERÍSTICAS GENERALES DE LOS SISTEMAS TELEFÓNICOS INTERNACIONALES EN RADIOENLACES O POR SATÉLITE E INTERCONEXIÓN CON LOS SISTEMAS EN LÍNEAS METÁLICAS	G.400–G.449
COORDINACIÓN DE LA RADIOTELEFONÍA Y LA TELEFONÍA EN LÍNEA	G.450–G.499
CARACTERÍSTICAS DE LOS MEDIOS DE TRANSMISIÓN Y DE LOS SISTEMAS ÓPTICOS	G.600–G.699
EQUIPOS TERMINALES DIGITALES	G.700–G.799
REDES DIGITALES	G.800–G.899
SECCIONES DIGITALES Y SISTEMAS DIGITALES DE LÍNEA	G.900–G.999
CALIDAD DE SERVICIO Y DE TRANSMISIÓN – ASPECTOS GENÉRICOS Y ASPECTOS RELACIONADOS AL USUARIO	G.1000–G.1999
CARACTERÍSTICAS DE LOS MEDIOS DE TRANSMISIÓN	G.6000–G.6999
DATOS SOBRE CAPA DE TRANSPORTE – ASPECTOS GENÉRICOS	G.7000–G.7999
ASPECTOS RELATIVOS A LOS PROTOCOLOS EN MODO PAQUETE SOBRE LA CAPA DE TRANSPORTE	G.8000–G.8999
Aspectos relativos al protocolo Ethernet sobre la capa de transporte	G.8000–G.8099
Aspectos relativos al protocolo MPLS sobre la capa de transporte	G.8100–G.8199
Objetivos de calidad y disponibilidad	G.8200–G.8299
Gestión de servicios	G.8600–G.8699
REDES DE ACCESO	G.9000–G.9999

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

Recomendación UIT-T G.8131/Y.1382

Conmutación lineal de protección para las redes MPLS de transporte

Resumen

En la presente Recomendación se presentan los requisitos y mecanismos para la conmutación de protección de caminos extremo a extremo y conexiones de subred (SNC, *subnetwork connection*) en redes MPLS de transporte (T-MPLS, *transport multiprotocol label switching*). En ella se describen los tipos de arquitectura de protección de caminos y de protección de las SNC, los tipos de conmutación uni y bidireccionales y los tipos de operación reversibles y no reversibles. En la Recomendación se define el protocolo de conmutación de protección automática (APS, *automatic protection switching*) utilizado para coordinar los dos extremos del dominio protegido.

Orígenes

La Recomendación UIT-T G.8131/Y.1382 fue aprobada el 6 de febrero de 2007 por la Comisión de Estudio 15 (2005-2008) del UIT-T por el procedimiento de la Recomendación UIT-T A.8.

Palabras clave

APS, protección de camino, protección de SNC, puente, selector, T-MPLS.

PREFACIO

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

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

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

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

NOTA

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

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

PROPIEDAD INTELECTUAL

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

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

© UIT 2008

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

ÍNDICE

	Página
1 Alcance	1
2 Referencias	1
3 Definiciones.....	1
4 Abreviaturas, siglas o acrónimos	3
5 Convenciones.....	3
6 Objetivos de red.....	3
7 Tipos de arquitectura	4
7.1 Protección de camino de la T-MPLS.....	5
7.2 Protección de SNC de la T-MPLS.....	5
8 Tipos de conmutación.....	5
8.1 Tipo de conmutación unidireccional	5
8.2 Tipo de conmutación bidireccional	6
9 Tipos de funcionamiento	6
9.1 Funcionamiento no reversible	6
9.2 Funcionamiento reversible	6
10 Protocolo de conmutación de protección automática (APS).....	6
10.1 Estructura de la cabida útil del APS	6
10.2 Tipo de protocolo APS	7
11 Arquitecturas de aplicación	8
11.1 Conmutación de protección de camino unidireccional 1+1	8
11.2 Conmutación de protección de camino bidireccional 1:1	9
11.3 Conmutación de protección SNC/S 1+1 unidireccional.....	10
11.4 Conmutación de protección SNC/S 1:1 bidireccional.....	11
12 Mecanismo para iniciar la conmutación de protección	11
12.1 Control manual	12
12.2 Condiciones para declarar fallo de señal	12
13 Criterios de inicio de conmutación APS.....	12
13.1 Instrucciones iniciadas externamente	13
13.2 Estados.....	13
14 Aspectos relativos a la seguridad.....	13
Apéndice I – Tipos de selector.....	14
I.1 Selector selectivo.....	14
I.2 Selector de combinación selector	14
Bibliografía	15

Introducción

En la presente Recomendación se especifican los mecanismos de conmutación de protección lineal que se han de aplicar a las redes de capa T-MPLS, descritas en G.8110.1/Y.1370.1. La conmutación de protección es un mecanismo de capacidad de supervivencia (capacidad de recuperación ante fallos) totalmente asignado, en el sentido de que la ruta y el ancho de banda de la entidad de protección se reservan para una entidad activa seleccionada. Este tipo de conmutación se constituye en un mecanismo de capacidad de supervivencia rápido y simple. Para el operador de la red es más fácil detectar el estado de la red (por ejemplo, la topología de red activa) si utiliza el mecanismo de conmutación por protección que si usa otros mecanismos de capacidad de supervivencia.

En esta Recomendación se especifican la arquitectura 1+1 y la arquitectura 1:1. La arquitectura 1+1 emplea conmutación unidireccional. La arquitectura 1:1 emplea conmutación bidireccional.

En la arquitectura 1+1, se asigna una entidad de transporte de protección de forma exclusiva a cada entidad de transporte activa. El tráfico normal se copia y se entrega tanto a la entidad de transporte activa como a la entidad de transporte de protección mediante un puente permanente ubicado en la fuente del dominio protegido. El tráfico de las entidades de transporte activa y de protección se transmite simultáneamente hacia el sumidero del dominio protegido, donde se elige o la entidad de transporte activa o la de protección, dependiendo de criterios previamente determinados, como la indicación de defecto del servidor.

En la arquitectura 1:1, la entidad de transporte de protección se asigna de forma exclusiva a la entidad de transporte activa. No obstante, el tráfico normal se transporta bien sea por la entidad de transporte activa o por la de protección, haciendo uso de un puente selector ubicado en la fuente del dominio protegido. El selector ubicado en el sumidero del dominio protegido selecciona la entidad que transporta el tráfico normal. Es necesario emplear el protocolo APS para coordinar la fuente y el sumidero a fin de garantizar que el puente selector de la fuente y el selector del sumidero seleccionen la misma entidad.

Recomendación UIT-T G.8131/Y.1382

Conmutación lineal de protección para las redes MPLS de transporte

1 Alcance

En esta Recomendación se presentan la arquitectura y los mecanismos para la conmutación de protección del camino y de SNC/S para las redes MPLS de transporte (T-MPLS).

En la presente versión se definen el protocolo APS, las arquitecturas de protección del camino 1+1 y 1:1 y la arquitectura de protección SNC/S. Quedan en estudio otros tipos de arquitecturas de protección.

La Recomendación describe el conjunto de funciones de conmutación para protección de conexiones punto a punto.

En esta versión no se trata la conmutación de protección sin errores.

2 Referencias

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

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

[UIT-T G.808.1] Recomendación UIT-T G.808.1 (2006), *Conmutación de protección genérica – Protección lineal de camino y de subred*.

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

3 Definiciones

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

3.1 conmutación de protección bidireccional

3.2 conmutación de protección unidireccional

En esta Recomendación se utilizan los siguientes términos definidos en [UIT-T G.805]:

3.3 degradación de la señal (SD, *signal degrade*)

3.4 fallo de la señal (SF, *signal fail*)

3.5 trail

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

3.6 defecto

3.7 fallo

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

- 3.8 protocolo APS**
- 3.8.1 1 fase**
- 3.8.2 2 fases**
- 3.9 clase de protección**
- 3.9.1 individual**
- 3.9.2 protección de grupo**
- 3.9.3 protección de camino**
- 3.10 conmutación**
- 3.10.1 conmutación forzada**
- 3.10.2 conmutación manual**
- 3.11 componente**
- 3.11.1 dominio protegido**
- 3.11.2 puente**
- 3.11.2.1 puente permanente**
- 3.11.2.2 puente selector**
- 3.11.3 selector**
- 3.11.3.1 selector selectivo**
- 3.11.3.2 selector de combinación**
- 3.11.4 nodo sumidero**
- 3.11.5 nodo fuente**
- 3.12 arquitectura**
- 3.12.1 arquitectura de protección 1+1**
- 3.12.2 arquitectura de protección 1:n**
- 3.12.3 arquitectura de protección (1:1)ⁿ**
- 3.12.4 conmutación de protección no reversible**
- 3.12.5 conmutación de protección reversible**
- 3.13 señales**
- 3.13.1 señal de tráfico**
- 3.13.2 señal de tráfico normal**
- 3.13.3 señal de tráfico sin protección**
- 3.13.4 señal nula**
- 3.14 temporizadores**
- 3.14.1 tiempo de liberación**
- 3.14.2 tiempo de espera de restablecimiento**
- 3.15 entidades de transporte**

3.15.1 entidad de transporte de protección

3.15.2 entidad de transporte principal (de trabajo)

4 Abreviaturas, siglas o acrónimos

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

APS	Conmutación de protección automática (<i>automatic protection switching</i>)
DNR	No revertir (<i>do not revert</i>)
EXER	Ejercicio
FDI	Indicación de defecto hacia adelante (<i>forward defect indication</i>)
FS	Conmutación forzada (<i>forced switch</i>)
LP	Exclusión de protección (<i>lockout of protection</i>)
MPLS	Conmutación por etiquetas multiprotocolo (<i>multiprotocol label switching</i>)
MS	Conmutación manual (<i>manual switch</i>)
NR	Ninguna petición (<i>no request</i>)
OAM	Operaciones, administración y mantenimiento
PS	Conmutación de protección (<i>protection switching</i>)
RR	Petición de revertir (<i>reverse request</i>)
SD	Degradación de señal (<i>signal degrade</i>)
SDH	Jerarquía digital síncrona (<i>synchronous digital hierarchy</i>)
SF	Fallo de señal (<i>signal fail</i>)
SF-P	Fallo de señal en la protección (<i>signal fail for protection</i>)
SNC	Conexiones de subred (<i>subnetwork connection</i>)
T-MPLS	MPLS de transporte
TTSI	Identificador de origen de terminación del camino (<i>trail termination source identifier</i>)
WTR	Espera al restablecimiento (<i>wait to restore</i>)

5 Convenciones

Ninguna.

6 Objetivos de red

Son aplicables los siguientes objetivos de red:

- 1) *Tiempo de conmutación* – El algoritmo APS para la protección de camino y de SNC debería funcionar tan rápido como sea posible. Se ha propuesto un valor de 50 ms como tiempo objetivo. El tiempo de compleción de la conmutación de protección excluye el tiempo de detección necesario para iniciar la conmutación de protección y el tiempo de liberación.
- 2) *Retardo de transmisión* – El retardo de transmisión depende de la longitud física del camino y de las funciones de procesamiento dentro del mismo. El retardo de transmisión máximo de un esquema de camino con protección especializada queda en estudio. Pueden imponerse limitaciones al retardo de transmisión cuando haya que atenerse a un plazo de tiempo objetivo para la compleción de la conmutación en caso de operación de

conmutación de protección bidireccional. La conmutación de protección unidireccional 1+1 no requiere transmisión de señalización APS, por lo que no existen retardos de transmisión de señalización.

- 3) *Tiempos de liberación* – Los tiempos de abstención son útiles para el interfuncionamiento de los esquemas de protección. Lo que se pretende es que estos tiempos puedan fijarse de manera individual para cada uno de los caminos o SNC protegidos. Un temporizador de tiempo de liberación arranca cuando se declara una condición de defecto y permanece en funcionamiento durante un periodo no reinicializable que puede fijarse de 0 a 10 s en pasos de 100 ms. Cuando expira el temporizador, se inicia la conmutación de protección si en ese punto está aún presente una condición de defecto. Se señala que no es necesario que una condición de defecto esté presente durante todo el periodo de tiempo de liberación, sólo importa el estado al expirar la temporización de liberación. Además, el defecto que da lugar a la puesta en marcha del temporizador de liberación no tiene porqué ser del mismo tipo que el existente al concluir el periodo de liberación.
- 4) *Alcance de la protección* – La protección de camino y de SNC debería restablecer todo el tráfico que haya sido interrumpido a causa del fallo de una conexión de enlace que hubiera sido designada como integrante de un esquema de protección de camino o de SNC. El tráfico que termine en un nodo con fallos puede resultar perturbado, pero el tráfico transferido a otros nodos puede subsistir conmutando al camino o SNC de protección.
- 5) *Tipos de conmutación* – La protección de camino y de SNC 1+1 deberían soportar conmutación de protección unidireccional. La protección de camino y de SNC 1:1 debería soportar conmutación de protección bidireccional.
- 6) *Protocolo y algoritmo APS* – Tanto los protocolos APS de protección de camino como los de protección de SNC deberían ser idénticos para todas las aplicaciones de red. El APS se requiere únicamente para la conmutación bidireccional.
- 7) *Modos de funcionamiento* – La conmutación de protección unidireccional 1+1 debe soportar conmutación reversible, conmutación no reversible o ambas. La conmutación de protección bidireccional 1:1 debería ser reversible
- 8) *Control manual* – Pueden proporcionarse instrucciones iniciadas externamente para el control manual de la conmutación de protección por los sistemas de operaciones o los operadores. Deberían soportarse las siguientes instrucciones iniciadas externamente: Clear, Lockout of Protection, Forced Switch, Manual Switch, Exercise.
- 9) *Criterios para la iniciación de la conmutación* – Los criterios para iniciar la conmutación de protección del camino deberían ser idénticos a los de la protección SNC/S correspondiente. Se soportarán las siguientes instrucciones iniciadas automáticamente: Fallo de señal: principal, fallo de señal: protección, degradación de señal: principal, degradación de señal: protección, petición de revertir, espera al restablecimiento y ninguna petición. Los criterios de fallo de señal (SF) y/o degradación de señal (SD) deberían concordar con las definiciones usadas en la Rec. UIT-T G.8121/Y.1381.

7 Tipos de arquitectura

La conmutación de protección es un mecanismo de protección totalmente asignado, que puede emplearse en cualquier topología. Está totalmente asignado en el sentido de que la ruta y la anchura de banda de la conexión de protección se reservan para una conexión principal seleccionada. No obstante, para que sea eficaz frente a todos los posibles fallos de la conexión principal, se entiende que la conexión de protección posee diversidad física completa en todos los modos de fallo comunes, lo cual no siempre es posible. Además, esto podría requerir que la conexión principal no utilice el trayecto más corto.

La arquitectura de conmutación de protección de la T-MPLS puede estar compuesta por la protección de camino y por la protección SNC/S, definida en [UIT-T G.808.1]. Quedan en estudio otros tipos de protección.

7.1 Protección de camino de la T-MPLS

La protección de camino de la T-MPLS se utiliza para proteger las conexiones de la T-MPLS. Se trata de una arquitectura de protección especializada extremo a extremo que puede utilizarse con diversas estructuras de red, redes en malla, anillo, etc.

7.1.1 Protección de camino 1+1

En el tipo de arquitectura 1+1, se asigna una conexión de protección de forma exclusiva a cada conexión principal y se establece un puente entre la conexión principal y la conexión de protección, en la fuente del dominio de protección. El tráfico de las conexiones principal y de protección se transmite simultáneamente hacia el sumidero del dominio de protección, donde se elige o la conexión de transporte principal o la de protección, dependiendo de criterios previamente determinados, como la indicación de defecto.

NOTA – A fin de evitar puntos únicos de fallo, la conexión principal y la conexión de protección se encaminarán por caminos independientes.

7.1.2 Protección de camino 1:1

En el tipo de arquitectura 1:1, se asigna una conexión de protección de forma exclusiva a cada conexión principal. El tráfico protegido o de servicio se transporta bien sea por la conexión principal o por la de protección. El método para seleccionar la conexión principal o la de protección depende del mecanismo.

NOTA – A fin de evitar puntos únicos de fallo, la conexión principal y la conexión de protección se encaminarán por caminos independientes.

7.2 Protección de SNC de la T-MPLS

La protección de conexión de subred de la T-MPLS se emplea para proteger una sección de una conexión (por ejemplo, la sección a la que pertenezcan dos rutas independientes) al interior de la red de un operador o de las redes de varios operadores. Existen dos conexiones de subred independientes, que actúan como entidades de transporte principal y de protección, para la señal de tráfico normal (protegida).

7.2.1 Protección SNC/S

Las funciones de terminación de camino de subcapa de la T-MPLS (es decir, las funciones de terminación de conexiones en cascada) generan/insertan y supervisan/extraen la información de OAM de la T-MPLS a fin de determinar el estado de los caminos principales y de protección de subcapa de la T-MPLS. Véase también [b-UIT-T G.8110.1 Enm.1]. La información del APS se transporta por el SNC de protección, salvo en el caso de conmutación unidireccional 1+1, en el que no se sustenta el APS.

8 Tipos de conmutación

Los tipos de conmutación se clasifican en de conmutación unidireccional y de conmutación bidireccional.

8.1 Tipo de conmutación unidireccional

Cuando se tiene conmutación unidireccional, únicamente conmuta a protección la conexión en el sentido que se vio afectado. Los selectores de cada extremo son independientes. Este tipo de conmutación se puede aplicar para la protección SNC/S y de camino de la T-MPLS 1+1.

8.2 Tipo de conmutación bidireccional

Cuando se tiene conmutación bidireccional, conmutan a protección los dos sentidos de la conexión, tanto el sentido que se vio afectado como el que no. En la conmutación bidireccional es necesario el protocolo de conmutación de protección (APS) para coordinar los dos puntos extremos. Este tipo de conmutación se puede aplicar para la protección SNC/S y de camino de la T-MPLS 1:1.

9 Tipos de funcionamiento

Los tipos de funcionamiento se clasifican en no reversible y reversible.

9.1 Funcionamiento no reversible

Cuando se emplea el tipo de funcionamiento no reversible, el servicio no se revierte a la conexión principal cuando finalicen las peticiones de conmutación.

En el modo de funcionamiento no reversible, cuando la conexión con fallo deja de estar en SF o en SD y ya no existen otras instrucciones iniciadas externamente, se ingresa al estado Ninguna petición. En dicho estado no hay conmutación.

9.2 Funcionamiento reversible

Cuando se emplea el tipo de funcionamiento reversible, el servicio siempre regresa a la conexión principal (o permanece en ésta), una vez finalicen las peticiones de conmutación.

En el modo de funcionamiento reversible, si se está transmitiendo el tráfico de servicio por la conexión de protección y se ha restablecido la conexión principal, y las peticiones de conmutación de protección locales que estaban activas pasan a inactivas, se ingresa al estado Espera al restablecimiento local. Normalmente este estado expira y se convierte en el estado Ninguna petición una vez expire el temporizador de Espera al restablecimiento. Es entonces que tiene lugar la reversión a la conexión principal. El temporizador de Espera al restablecimiento se desactiva antes si alguna petición local de mayor prioridad hace que cambie el estado.

10 Protocolo de conmutación de protección automática (APS)

Salvo por el caso de conmutación unidireccional 1+1, se utiliza una señal APS para sincronizar las acciones en los extremos A y Z del dominio protegido. Se comunica lo siguiente: tipo de petición/estado, señal solicitada, señal puenteadada, configuración de protección.

10.1 Estructura de la cabida útil del APS

Queda en estudio la estructura de la cabida útil del APS (véase el cuadro 10-1) dentro de una trama OAM de la T-MPLS.

Cuadro 10-1 – Estructura de la cabida útil de los octetos del APS

1				2				3				4											
1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
Petición/ estado				Tipo de protección				Señal solicitada				Señal puenteadada				En reserva							
				A	B	D	R																

En el cuadro 10-2 se definen los valores de campo de los octetos del APS.

Cuadro 10-2 – Valores de los campos de los canales del APS

Campo		Valor	Descripción
Petición/estado		1111	Exclusión de protección (LP)
		1110	Fallo de señal en la protección (SF-P)
		1101	Conmutación forzada (FS)
		1100	Fallo de señal (SF)
		1010	Degradación de señal (SD)
		1000	Conmutación manual (MS)
		0110	Espera al restablecimiento (WTR)
		0100	Ejercicio (EXER)
		0010	Petición de revertir (RR)
		0001	No revertir (DNR)
		0000	Ninguna petición (NR)
		Otros	Se reserva para la normalización internacional futura
Tipo de protección	A	0	Sin canal APS
		1	Canal APS
	B	0	1+1 (Puente permanente)
		1	(1:1) ⁿ (Puente selector) ($n \geq 1$)
	D	0	Conmutación unidireccional
		1	Conmutación bidireccional
	R	0	Funcionamiento no reversible
		1	Funcionamiento reversible
Señal solicitada		0	Señal nula
		1-254	Señal de tráfico normal 1-254
		255	Señal de tráfico sin protección
Señal puenteada		0	Señal nula
		1-254	Señal de tráfico normal 1-254
		255	Señal de tráfico sin protección

10.2 Tipo de protocolo APS

Hay dos requisitos básicos para el protocolo APS:

- 1) Que evite conexiones erradas.
- 2) Que minimice el número de ciclos de comunicación entre los extremos A y Z del dominio protegido, a fin de reducir al mínimo el tiempo de la conmutación de protección. La comunicación puede darse una vez ($Z \rightarrow A$), dos veces ($Z \rightarrow A$ y $A \rightarrow Z$), o tres veces ($Z \rightarrow A$, $A \rightarrow Z$ y $Z \rightarrow A$). A estos protocolos se les califica como de 1 fase, de 2 fases o de 3 fases.

En el cuadro 10-3 se presentan los tipos de protocolo sugeridos para las diversas arquitecturas, con el propósito de preservar el equilibrio entre la disminución del tiempo para la operación, la reducción de la complejidad del protocolo y la simplificación de la aplicación.

Cuadro 10-3 – Tipo de protocolo respecto a la arquitectura de protección

Tipo de protocolo	Arquitectura de protección
Sin protocolo	Unidireccional 1+1
APS de 1 fase	Bidireccional (1:1) ⁿ (n ≥ 1)

Queda en estudio el funcionamiento del protocolo APS de 1 fase.

11 Arquitecturas de aplicación

11.1 Conmutación de protección de camino unidireccional 1+1

En la figura 11-1 se presenta la arquitectura de conmutación de protección de camino 1+1. En el caso del funcionamiento de conmutación de protección unidireccional descrito aquí, el selector ubicado en el lado sumidero del dominio de protección realiza la conmutación de protección basándose en información exclusivamente local (es decir, sumidero de protección). En el lado fuente del dominio de protección se puenta permanentemente el tráfico de servicio (protegido) hacia la conexión principal y la conexión de protección. Si se utilizan paquetes de verificación de conectividad para detectar los defectos de la conexión principal y de la de protección, éstos se insertan del lado fuente del dominio de protección tanto en la conexión principal como en la de protección y se detectan y extraen al lado sumidero del dominio de protección. Se señala que se deberían enviar estos paquetes independientemente de si el selector ha elegido o no la conexión.

La protección de camino unidireccional 1+1 puede ser reversible o no reversible.

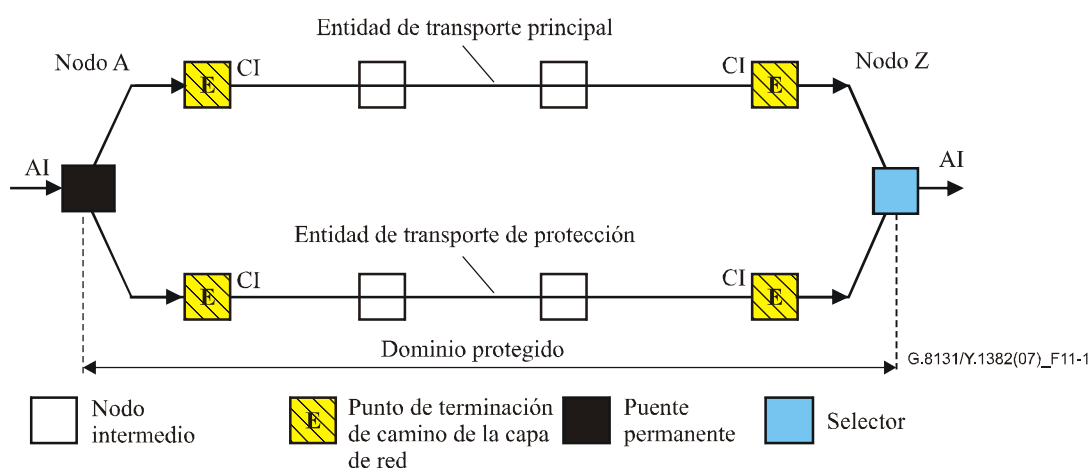


Figura 11-1 – Arquitectura de conmutación de protección de camino 1+1 unidireccional

Por ejemplo, si ocurre un defecto unidireccional (en el sentido de transmisión del nodo A al nodo Z) en la conexión principal, como se muestra en la figura 11-2, el defecto se detectará en el sumidero del dominio de protección en el nodo Z y el selector en el nodo Z conmutará a la conexión de protección.

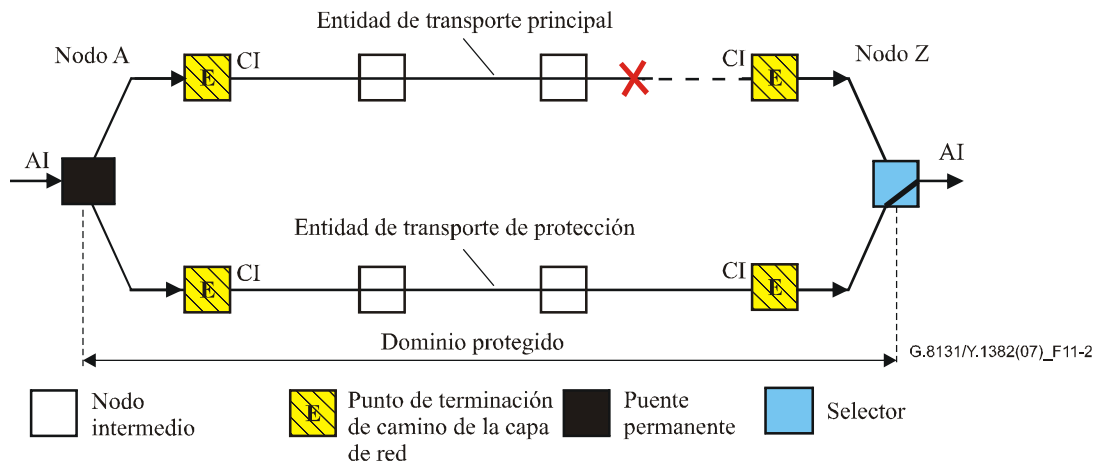


Figura 11-2 – Conmutación de protección de camino 1+1 unidireccional: fallo de la conexión principal

11.2 Conmutación de protección de camino bidireccional 1:1

En la figura 11-3 se presenta la arquitectura de conmutación de protección de camino 1:1. En el caso del funcionamiento de conmutación de protección bidireccional descrito aquí, tanto el puente selector al lado fuente como el selector al lado sumidero del dominio de protección realizan la conmutación de protección, basándose en información local, o del extremo cercano, y en la información del protocolo APS proveniente del otro lado, o extremo lejano.

Si se utilizan paquetes de verificación de conectividad para detectar los defectos de la conexión principal y de la de protección, éstos se insertan tanto en la conexión principal como en la de protección. Se señala que se deberían enviar estos paquetes independientemente de si el selector ha elegido o no la conexión.

La protección de camino bidireccional 1:1 debería ser reversible.

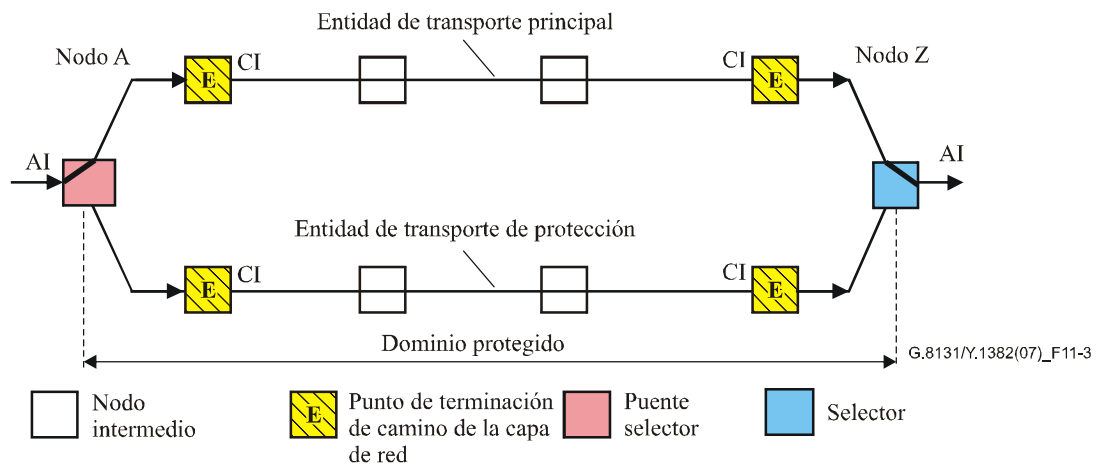
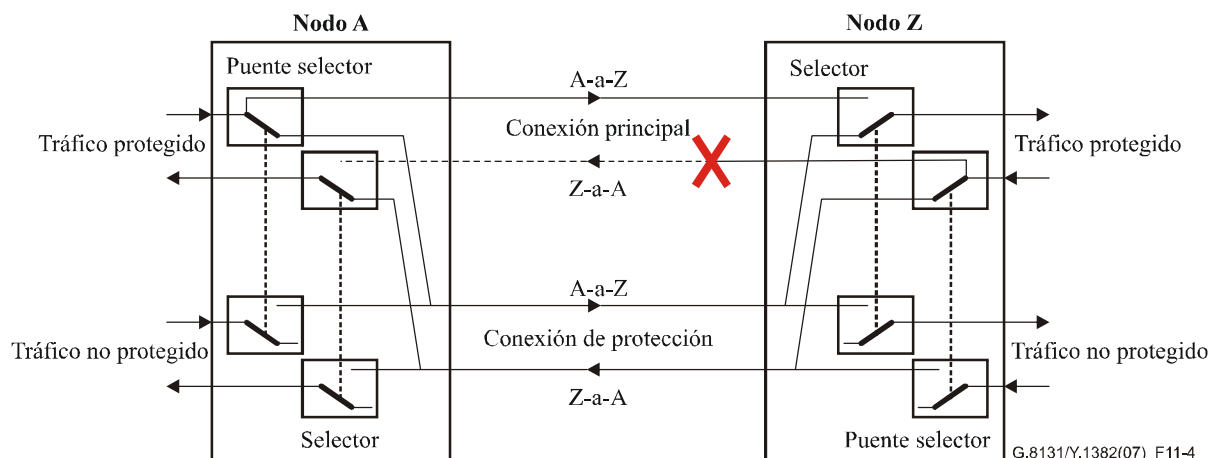


Figura 11-3 – Arquitectura de conmutación de protección de camino bidireccional 1:1 Representación unidireccional

Por ejemplo, si ocurre un defecto en la conexión principal de Z a A, en el sentido de transmisión del nodo Z al nodo A, como se muestra en la figura 11-4, el defecto se detectará en el nodo A. El protocolo APS inicia la conmutación de protección. Se utiliza un protocolo APS de 1 fase. El protocolo es así:

- el nodo A detecta el defecto;
- el puente selector en el nodo A conmuta a la conexión de protección de A a Z (es decir, en el sentido de A a Z, el tráfico de servicio se envía tanto por la conexión principal de A a Z como por la conexión de protección de A a Z) y el selector de combinación en el nodo A conmuta a la conexión de protección de Z a A;
- la instrucción APS enviada del nodo A al nodo Z solicita una conmutación de protección;
- después de que el nodo Z valida la prioridad de la solicitud de conmutación de protección, el selector de combinación en el nodo Z conmuta a la conexión de protección de A a Z y el puente selector en el nodo Z conmuta a la conexión de protección de Z a A (es decir, en el sentido de Z a A, el tráfico de servicio se envía tanto por la conexión principal de Z a A como por la conexión de protección de Z a A);
- se envía luego la instrucción APS desde el nodo Z al nodo A para informar al nodo A sobre la conmutación;
- el tráfico fluye ahora por la conexión de protección.



**Figura 11-4 – Conmutación de protección de camino bidireccional 1:1
Falla la conexión principal de Z a A**

11.3 Conmutación de protección SNC/S 1+1 unidireccional

En la figura 11-5 se presenta la arquitectura de conmutación de protección SNC/S 1+1 unidireccional. En el caso del funcionamiento de conmutación de protección unidireccional descrito aquí, el selector en el sumidero (nodo Z) del dominio de protección realiza la conmutación de protección basándose en información exclusivamente local. El tráfico de servicio se puentea permanentemente hacia las conexiones principal y de protección en la fuente (nodo A) del dominio de protección. Las funciones de terminación de camino y de adaptación del servidor o de la subcapa se emplean para supervisar y determinar el estado de la conexión de trabajo y de protección. En la sección 11.1 se trata con nivel de detalle el mecanismo de conmutación de protección de la protección de camino 1+1 unidireccional.

La protección SNC/S 1+1 unidireccional puede ser reversible o no reversible.

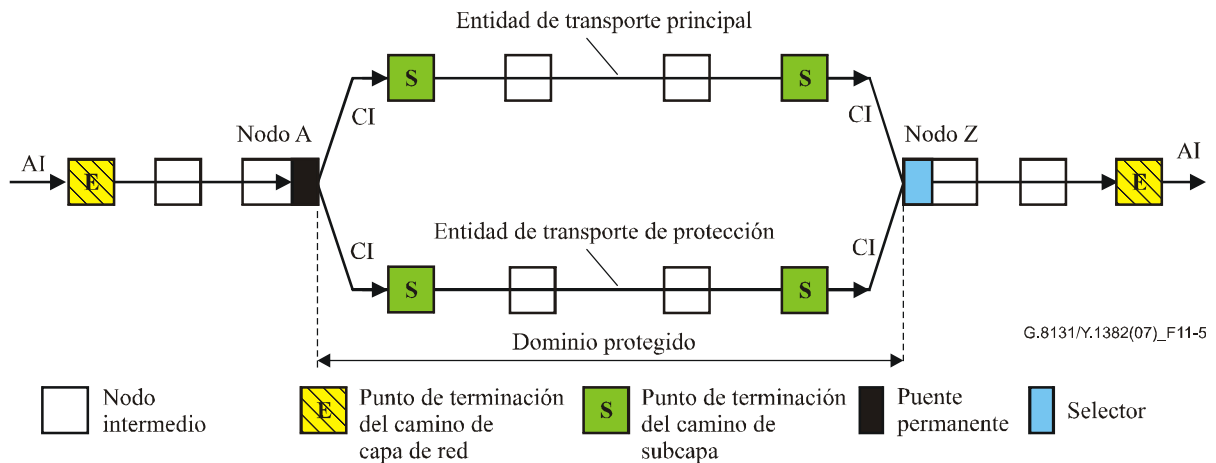
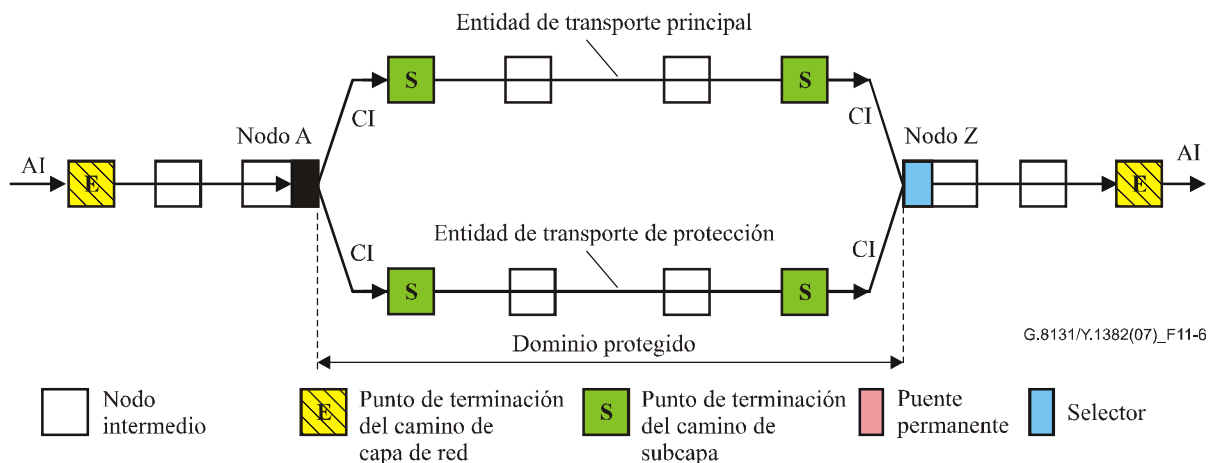


Figura 11-5 – Arquitectura de conmutación de protección SNC/S 1+1 unidireccional

11.4 Conmutación de protección SNC/S 1:1 bidireccional

En la figura 11-6 se presenta la arquitectura de conmutación de protección SNC/S 1:1 bidireccional. En el caso del funcionamiento de conmutación de protección bidireccional descrito aquí, tanto el puente selector al lado fuente como el selector al lado sumidero del dominio de protección realizan la conmutación de protección, basándose en información local, o del extremo cercano, y en la información del protocolo APS proveniente del otro lado, o extremo lejano. Las funciones de terminación de camino y de adaptación del servidor o de la subcapa se emplean para supervisar y determinar el estado de las conexiones de trabajo y de protección. En la cláusula 11.2 se trata con nivel de detalle el mecanismo de conmutación de protección de la protección de camino 1:1 bidireccional.

La protección SNC/S 1:1 bidireccional debería ser reversible.



**Figura 11-6 – Arquitectura de conmutación de protección SNC/S 1:1 bidireccional
Representación unidireccional**

12 Mecanismo para iniciar la conmutación de protección

La acción de conmutación de protección se realizará cuando:

- 1) la inicie el control del operador (por ejemplo, conmutación manual, conmutación forzada y exclusión de protección), si no está en efecto una petición de conmutación de mayor prioridad;

- 2) se declare un SF o una SD en la conexión en cuestión (es decir, en la conexión principal o en la de protección) sin que en la otra conexión se haya declarado alguna de éstas condiciones y haya expirado el temporizador de retención; o
- 3) el temporizador de espera al restablecimiento expira (en el modo reversible) y no se ha declarado SF ni SD en la conexión principal.

12.1 Control manual

Puede transferirse el control manual de la función de conmutación de protección del sistema de gestión del elemento o de la red.

12.2 Condiciones para declarar fallo de señal

Se declara un fallo de señal (SF) cuando la función TMT_TT_Sk detecta un fallo de señal de camino, conforme a lo descrito en [b-UIT-T G.8110.1 Enm.1].

Se declara una degradación de señal (SD) cuando la función TMT_TT_Sk detecta una degradación de señal de camino, conforme a lo descrito en [b-UIT-T G.8110.1 Enm.1].

13 Criterios de inicio de conmutación APS

Se dispone de los siguientes criterios de inicio de conmutación:

- 1) instrucción iniciada externamente (despejar, exclusión de protección, conmutación forzada, conmutación manual, ejercicio);
- 2) instrucción iniciada automáticamente (fallo de señal, degradación de señal) relacionada con un dominio de protección; o
- 3) un estado (espera al restablecimiento, petición de revertir, no revertido, ninguna petición) de la función de conmutación de protección.

En el cuadro 13-1 se presentan las prioridades de las peticiones/estados. En el caso de conmutación unidireccional, la prioridad se determina únicamente en el extremo cercano. En conmutación bidireccional, se indicará una petición local sólo si ésta tiene una prioridad igual o superior a la de toda petición recibida del extremo lejano a través del canal APS. En conmutación bidireccional, si la petición del extremo lejano es la que tiene mayor prioridad, el extremo cercano indicará petición de revertir.

Cuadro 13-1 – Prioridad de las peticiones/estados

Petición local	Orden de prioridad
Despejar	Mayor
Exclusión de protección (LP)	
Fallo de señal en la protección (SF-P)	
Conmutación forzada (FS)	
Fallo de señal (SF)	
Degradación de señal (SD)	
Conmutación manual (MS)	
Espera al restablecimiento (WTR)	
Ninguna petición (NR)	Menor

13.1 Instrucciones iniciadas externamente

A continuación se presentan las instrucciones iniciadas externamente, en orden descendente de prioridad, y se describen cada una de sus funciones:

Despejar: Esta instrucción despeja todas las instrucciones iniciadas externamente, y que figuran a continuación.

Exclusión de protección (LP): Mover la posición del selector a la conexión principal. Evita que el selector conmute a la conexión de protección cuando éste esté seleccionando la conexión principal. Hace que el selector conmute de la conexión de protección a la principal cuando éste esté seleccionando la conexión de protección.

Conmutación forzada (FS) de la conexión principal: Hace que el selector conmute de la conexión principal a la conexión de protección, a no ser que esté surtiendo efecto una petición de conmutación de prioridad mayor (es decir, LP).

Conmutación manual (MS) de la conexión principal: Hace que el selector conmute de la conexión de protección a la conexión principal, a no ser que esté surtiendo efecto una petición de conmutación de prioridad igual o superior (es decir, LP, FS, SF o MS).

Conmutación manual (MS) de la conexión de protección: Hace que el selector conmute de la conexión de protección a la conexión principal, a no ser que esté surtiendo efecto una petición de conmutación de prioridad igual o superior (es decir, LP, FS, SF o MS)

13.2 Estados

Espera al restablecimiento: Este estado sólo se puede aplicar en el modo reversible y se aplica sólo a la conexión principal. La función de conmutación de protección local ingresa a este estado, en circunstancias en que haya estado recibiendo tráfico local a través de la conexión de protección cuando se restablece la conexión principal, si las peticiones de conmutación de protección local que estaban activas pasan ahora a inactivas. Con esto se evita que se revierta a la conexión principal hasta que haya expirado el temporizador de espera al restablecimiento. El operador puede configurar el tiempo de espera al restablecimiento entre 5 y 12 minutos, en pasos de 1 minuto. El valor por defecto es de 5 minutos. Las condiciones de SF y SD tendrán prelación sobre el WTR.

Ninguna petición: La función de protección de conmutación ingresará a este estado siempre que no esté activa ninguna petición de conmutación de protección local (incluida espera al restablecimiento).

14 Aspectos relativos a la seguridad

Con la presente Recomendación no se suscita ningún problema de seguridad que no exista en la arquitectura de la T-MPLS o en la arquitectura de sus protocolos de capa de cliente.

Con la conmutación de protección podría mejorar la seguridad de las redes T-MPLS ya que ésta conmuta automáticamente, hacia conexiones con funcionamiento correcto, el tráfico de las conexiones defectuosas que podrían haberse afectado por conexiones o configuraciones indebidas. Esto evita que el tráfico de los clientes resulte expuesto a otros clientes.

Apéndice I

Tipos de selector

(Este apéndice no es parte integrante de la presente Recomendación)

Hay dos posibles tipos de selector: el selector selectivo y el selector de combinación. Los dos funcionan de la misma forma.

I.1 Selector selectivo

En estudio.

I.2 Selector de combinación selector

En estudio.

Bibliografía

- [b-UIT-T G.8113] Recomendación UIT-T G.8113/Y.1372 (2007), *Requisitos de la funcionalidad operación y mantenimiento para redes con conmutación por etiquetas multiprotocolo en la red de transporte (T-MPLS)*.
- [b-UIT-T G.8114] Recomendación UIT-T G.8114/Y.1373 (2007), *Mecanismo de operación y administración para redes con conmutación por etiquetas multiprotocolo, para las redes de capa T-MPLS*.
- [b-UIT-T G.8110.1 Enm.1] Recomendación UIT-T G.8110.1/Y.1370.1 (2006), *Arquitectura de red de capa de transporte con conmutación por etiquetas multiprotocolo en la red de transporte (T-MPLS) – Enmienda 1*.

RECOMENDACIONES UIT-T DE LA SERIE Y

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

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

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

SERIES DE RECOMENDACIONES DEL UIT-T

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