

**UIT-T**

**G.8080/Y.1304**

SECTOR DE NORMALIZACIÓN  
DE LAS TELECOMUNICACIONES  
DE LA UIT

(06/2006)

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

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

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

Aspectos del protocolo Internet – Transporte

---

## **Arquitectura de la red óptica con conmutación automática**

Recomendación UIT-T G.8080/Y.1304

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
<b>Aspectos relativos al protocolo Ethernet sobre la capa de transporte</b>	<b>G.8000–G.8099</b>
Aspectos relativos al protocolo MPLS sobre la capa de transporte	G.8100–G.8199
Objetivos de calidad y disponibilidad (continuación de la serie G.82x)	G.8200–G.8299
Gestión de servicios	G.8600–G.8699
REDES DE ACCESO	G.9000–G.9999

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

## **Recomendación UIT-T G.8080/Y.1304**

### **Arquitectura de la red óptica con conmutación automática**

#### **Resumen**

La presente Recomendación describe la arquitectura de referencia para el plano de control de la red óptica con conmutación automática (ASON) aplicable a las redes de transporte de la jerarquía digital síncrona (SDH) definidas en la Rec. UIT-T G.803, y a las redes ópticas de transporte definidas en la Rec. UIT-T G.872. Esta arquitectura de referencia se describe en términos de los componentes funcionales clave y las interacciones entre éstos.

#### **Orígenes**

La Recomendación UIT-T G.8080/Y.1304 fue aprobada el 6 de junio de 2006 por la Comisión de Estudio 15 (2005-2008) del UIT-T por el procedimiento de la Recomendación UIT-T A.8.

## PREFACIO

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

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

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

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

## NOTA

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

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

## PROPIEDAD INTELECTUAL

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

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

© UIT 2007

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

## ÍNDICE

	<b>Página</b>
1 Alcance .....	1
2 Referencias .....	1
3 Definiciones.....	2
4 Abreviaturas, siglas o acrónimos .....	4
5 Visión de conjunto.....	5
5.1 Control de llamada y control de conexión.....	7
5.2 Interacción entre los planos de control, de transporte y de gestión.....	9
6 Recursos de transporte y su organización.....	11
6.1 Entidades de transporte.....	11
6.2 Áreas de encaminamiento.....	13
6.3 Topología y descubrimiento .....	18
6.4 Dominios .....	19
6.5 Aspectos de múltiples capas .....	21
6.6 Soporte de cliente entre capas .....	23
6.7 Llamadas que se soportan en llamadas de la misma capa.....	24
7 Arquitectura del plano de control .....	25
7.1 Notación .....	25
7.2 Política y federaciones.....	27
7.3 Componentes arquitecturales.....	30
7.4 Componente controlador de protocolo (PC, <i>protocol controller</i> ).....	49
8 Puntos de referencia.....	51
8.1 UNI.....	52
8.2 I-NNI .....	53
8.3 E-NNI .....	53
8.4 Arquitectura de usuario .....	53
8.5 Interacciones de NCC entre capas .....	54
9 Gestión de red de entidades del plano de control .....	56
10 Identificadores .....	57
10.1 Espacios de nombres .....	57
10.2 Nombres y direcciones .....	57
10.3 Relaciones entre los identificadores .....	59
11 Técnicas de mejoramiento de la disponibilidad de la conexión .....	59
11.1 Protección .....	60
11.2 Restablecimiento .....	60

	<b>Página</b>
12 Resiliencia .....	64
12.1 Principios de interacciones de los planos de control y de transporte .....	64
12.2 Principio de comunicación del controlador de protocolo.....	65
12.3 Interacciones de los planos de control y de gestión .....	65
Anexo A – Servicios de conexión.....	66
Apéndice I– Redes de capa ASON .....	69
Apéndice II– Ejemplo ilustrativo de implementaciones .....	70
Apéndice III– Relaciones de resiliencia.....	72
III.1 Relaciones de plano de control – RCD .....	72
III.2 Relaciones entre el plano de control y el plano de transporte .....	74
III.3 Relaciones del plano de control – Plano de gestión .....	75
III.4 Relaciones dentro del plano de control .....	75
Apéndice IV– Ejemplo de control de llamada estructurado por capas .....	77
Apéndice V– Interacción entre los componentes durante el establecimiento de la conexión.....	78
V.1 Encaminamiento jerárquico.....	78
V.2 Encaminamientos desde la fuente y paso a paso .....	80
V.3 Protección de la conexión.....	86
V.4 Restablecimiento – Reencaminamiento rígido – Intradominio – Método jerárquico .....	87
V.5 Restablecimiento – Reencaminamiento flexible dentro del dominio – Método desde la fuente.....	91
V.6 Restablecimiento – Reencaminamiento reversible – Intradominio – Método desde la fuente.....	95
V.7 Encaminamiento desde la fuente utilizando la interfaz interrogación de rutas.....	98
BIBLIOGRAFÍA .....	101

# Recomendación UIT-T G.8080/Y.1304

## Arquitectura de la red óptica con conmutación automática

### 1 Alcance

Esta Recomendación especifica la arquitectura y requisitos de las redes de transporte con conmutación automática, tal como se aplican a las redes de transporte de la jerarquía digital síncrona (SDH, *synchronous digital hierarchy*), definidas en la Rec. UIT-T G.803, y las redes ópticas de transporte, definidas en la Rec. UIT-T G.872.

La presente Recomendación describe el conjunto de componentes del plano de control que se utilizan para manipular los recursos de la red de transporte, a fin de proporcionar las funcionalidades de establecimiento, mantenimiento y liberación de las conexiones. El uso de componentes permite la separación del control de llamada del control de conexión y la separación del encaminamiento y la señalización.

A los efectos de esta Recomendación, los componentes se utilizan para representar entidades abstractas, más bien que aplicaciones de software implementable. Se utiliza una notación similar al lenguaje de modelado unificado (UML, *unified modelling language*) para describir los componentes de la arquitectura de la red óptica con conmutación automática.

### 2 Referencias

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

- Recomendación UIT-T G.705 (2000), *Características de los bloques funcionales de equipos de la jerarquía digital plesiócrona.*
- Recomendación UIT-T G.707/Y.1322 (2003), *Interfaz de nodo de red para la jerarquía digital síncrona.*
- Recomendación UIT-T G.709/Y.1331 (2003), *Interfaz para la red óptica de transporte.*
- Recomendación UIT-T G.783 (2006), *Características de los bloques funcionales del equipo de la jerarquía digital síncrona.*
- Recomendación UIT-T G.798 (2004), *Características de los bloques funcionales del equipo de la jerarquía de la red óptica de transporte.*
- Recomendación UIT-T G.803 (2000), *Arquitecturas de redes de transporte basadas en la jerarquía digital síncrona.*
- Recomendación UIT-T G.805 (2000), *Arquitectura funcional genérica de las redes de transporte.*
- Recomendación UIT-T G.872 (2001), *Arquitectura de las redes ópticas de transporte.*
- Recomendación UIT-T G.8081/Y.1354 (2004), *Términos y definiciones aplicables a las redes ópticas con conmutación automática.*

- Recomendación UIT-T M.3000 (2000), *Visión de conjunto de las Recomendaciones relativas a la RGT*.
- Recomendación UIT-T M.3010 (2000), *Principios para una red de gestión de las telecomunicaciones*.
- Recomendación UIT-T M.3100 (2005), *Modelo genérico de información de red*.
- Recomendación UIT-T X.25 (1996), *Interfaz entre el equipo terminal de datos y el equipo de terminación del circuito de datos para equipos terminales que funcionan en el modo paquete y están conectados a redes públicas de datos por circuitos especializados*.
- Recomendación UIT-T Y.1311 (2002), *Redes privadas virtuales basadas en red – Arquitectura y requisitos de servicio genéricos*.
- Recomendación UIT-T Y.1312 (2003), *Requisitos y elementos arquitecturales genéricos para redes privadas virtuales de capa 1*.
- Recomendación UIT-T Y.1313 (2004), *Arquitecturas de red y de servicio de la red privada virtual de capa 1*.

### 3 Definiciones

En esta Recomendación se utilizan los términos siguientes definidos en otras Recomendaciones UIT-T.

- 3.1 grupo de acceso (AG, *access group*):** Véase la Rec. UIT-T G.805.
- 3.2 adaptación:** Véase la Rec. UIT-T G.805.
- 3.3 dominio administrativo:** Véase la Rec. UIT-T G.805.
- 3.4 camino:** Véase la Rec. UIT-T G.805.
- 3.5 grupo cerrado de usuarios:** Véase la Rec. UIT-T X.25.
- 3.6 enlace:** Véase la Rec. UIT-T G.805.
- 3.7 conexión de enlace:** Véase la Rec. UIT-T G.805.
- 3.8 red privada virtual:** Véase la Rec. UIT-T Y.1311.
- 3.9 red de capa:** Véase la Rec. UIT-T G.805.
- 3.10 agente:** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.11 llamada:** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.12 segmento de llamada:** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.13 componente:** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.14 punto de conexión (CP, *connection point*):** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.15 punto de terminación de conexión (CTP, *connection termination point*):** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.16 plano de control:** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.17 plano de gestión:** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.18 multiaccesible:** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.19 política:** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.20 controlador de puerto:** Véase la Rec. UIT-T G.8081/Y.1353.



- 3.21 **ruta:** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.22 **área de encaminamiento:** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.23 **nivel de encaminamiento:** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.24 **subred:** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.25 **conexión de subred (SNC, *subnetwork connection*):** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.26 **punto de subred (SNP, *subnetwork point*):** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.27 **agrupación de puntos de subred (SNPP, *subnetwork point pool*):** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.28 **enlace de agrupación de puntos de subred:** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.29 **punto de conexión de terminación (TCP, *termination connection point*):** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.30 **punto de terminación de camino (TTP, *trail termination point*):** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.31 **plano de transporte:** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.32 **dominio de control:** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.33 **dominio de transporte:** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.34 **reencaminamiento rígido:** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.35 **protección configurada del plano de control:** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.36 **dominio de reencaminamiento:** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.37 **restablecimiento:** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.38 **dominio en control del restablecimiento:** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.39 **identificador de recurso de transporte:** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.40 **dirección:** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.41 **E-NNI:** Véase la Rec. UIT-T G.8081/Y.1353. (Véase también la cláusula 8.)
- 3.42 **interfaz:** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.43 **I-NNI:** Véase la Rec. UIT-T G.8081/Y.1353. (Véase también la cláusula 8.)
- 3.44 **nombre:** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.45 **conexión permanente:** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.46 **conexión conmutada (SC, *switched connection*):** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.47 **conexión lógica permanente (SPC, *soft permanent connection*):** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.48 **acuerdo del nivel de servicio:** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.49 **servicios suplementarios:** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.50 **señalización de tercero:** Véase la Rec. UIT-T G.8081/Y.1353.
- 3.51 **interfaz de la red de usuario para el plano de control (UNI, *user-network interface for the control plane*):** Véase la Rec. UIT-T G.8081/Y.1353. (Véase también la cláusula 8.)

En esta Recomendación se definen los términos siguientes.

**3.52 conexión:** Concatenación de conexiones de enlace y conexiones de subred (descritas en la Rec. UIT-T G.805) que permite el transporte de información de usuario entre los puntos de ingreso y egreso de una subred..

**3.53 Reencaminamiento flexible:** Función que sirve para reencaminar una conexión con fines administrativos. La conexión inicial no se saca de servicio mientras no se haya creado la conexión reencaminada.

#### 4 Abreviaturas, siglas o acrónimos

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

AG	Grupo de acceso ( <i>access group</i> )
AGC	Contenedor de grupo de acceso ( <i>access group container</i> )
CC	Controlador de conexión
CCC	Controlador de llamadas de la parte llamante ( <i>calling party call controller</i> )
CP	Punto de conexión ( <i>connection point</i> )
CPS	Estado de punto de conexión ( <i>connection point status</i> )
CTP	Punto de terminación de conexión ( <i>connection termination point</i> )
DA	Agente de descubrimiento ( <i>discovery agent</i> )
E-NNI	Interfaz lógica externa red-red (punto de referencia) ( <i>logical external network-network interface (reference point)</i> )
HOVC	Contenedor virtual de orden superior ( <i>higher order virtual container</i> )
id	Identificador
I-NNI	Interfaz lógica interna red-red (punto de referencia) ( <i>logical internal network-network interface (reference point)</i> )
LOVC	Contenedor virtual de orden inferior ( <i>lower order virtual container</i> )
LRM	Gestor de recursos de enlace ( <i>link resource manager</i> )
MI	Información de gestión ( <i>management information</i> )
MO	Objeto gestionado ( <i>managed object</i> )
NCC	Controlador de llamada de red ( <i>network call controller</i> )
PC	Controlador de protocolo ( <i>protocol controller</i> )
RC	Controlador de encaminamiento ( <i>routing controller</i> )
RCD	Red de comunicación de datos
RPV	Red privada virtual
SNC	Conexión de subred ( <i>subnetwork connection</i> )
SNP	Punto de subred ( <i>subnetwork point</i> )
SNPP	Agrupación de puntos de subred ( <i>subnetwork point pool</i> )
TAP	Ejecutante de terminación y adaptación ( <i>termination and adaptation performer</i> )
TCP	Punto de conexión de terminación ( <i>termination connection point</i> )

TTP	Punto de terminación de camino ( <i>trail termination point</i> )
UML	Lenguaje de modelado unificado ( <i>unified modelling language</i> )
UNI	Interfaz lógica usuario-red (punto de referencia) ( <i>logical user-network interface (reference point)</i> )

## 5 Visión de conjunto

El plano de control de la red óptica con conmutación automática (ASON, *automatic switched optical network*) tiene por finalidad:

- facilitar la configuración rápida y eficaz de las conexiones dentro de una red de capa de transporte, para el soporte de conexiones conmutadas y de conexiones permanentes programables;
- reconfigurar o modificar conexiones que soportan llamadas ya establecidas;
- realizar una función de restauración.

Una arquitectura de plano de control bien diseñada debe dar a los proveedores de servicio el control de sus redes, al mismo tiempo que proporciona una estructura de comunicaciones rápida y fiable. El plano de control en sí debe ser fiable, escalable, y eficaz. Debe ser lo suficientemente genérico para soportar tecnologías diferentes, satisfacer necesidades comerciales diferentes y a una distribución diferente de las funciones por los vendedores (es decir, un empaquetamiento diferente de los componentes del plano de control).

El plano de control ASON consta de diversos componentes que suministran funciones específicas, incluida la determinación de ruta y señalización. Los componentes del plano de control se describen en términos que no imponen restricciones a la forma en que estas funciones se combinan y se reúnen en lotes. Las interacciones entre estos componentes, y el flujo de información necesario para la comunicación entre ellos, se obtienen gracias a interfaces.

En esta Recomendación se tratan los componentes arquitecturales del plano de control y la interacción entre dicho plano, el plano de gestión y el plano de transporte. Los planos de gestión y transporte se especifican en otras Recomendaciones UIT-T y están fuera del alcance de la presente Recomendación.

En la figura 1 se presenta una visión de alto nivel de las interacciones de los planos de control, gestión y transporte para el soporte de conexiones conmutadas de una red de capa. Esta figura también incluye la red de comunicación de datos (RCD), que suministra los trayectos de comunicación para transportar información de señalización y gestión. Los detalles acerca de la RCD y de los planos de gestión y transporte están fuera del alcance de esta Recomendación. Las funciones pertinentes al plano de control se describen en esta Recomendación.

El despliegue del plano de control tendrá lugar dentro del contexto de las prácticas de negocios del operador comercial y de la heterogeneidad multidimensional de las redes de transporte. Esas consideraciones de funcionamiento y comerciales conducen a la necesidad de soporte arquitectural mediante, por ejemplo, barreras sólidas de abstracción a fin de proteger las prácticas de funcionamiento de la empresa comercial, la segmentación de las redes de transporte en dominios conforme a consideraciones de gestión y/o política y la heterogeneidad inherente de la red de transporte (incluyendo el control y la gestión). La noción de dominio incorporada en la definición de dominio administrativo G.805 y las regiones administrativas de Internet (por ejemplo, los sistemas autónomos) han sido generalizados en la arquitectura del plano de control a fin de expresar diferentes responsabilidades administrativas y/o de gestión, relaciones de confianza, esquemas de direccionamiento, capacidades de infraestructura, técnicas de supervivencia, distribuciones de la funcionalidad de control, etc. Los dominios son establecidos por políticas del operador y tienen una gama de criterios en cuanto a los miembros, de los que ya se han dado ejemplos.

El plano de control soporta los servicios de conexión (véase el anexo A) mediante el aprovisionamiento automático de conexiones de transporte extremo a extremo a través de uno o varios dominios. Esto exige una perspectiva tanto de servicio como de conexión:

- La perspectiva de servicio (llamada), para soportar el aprovisionamiento de servicios de extremo preservando la índole independiente de las distintas empresas involucradas.
- La perspectiva de conexión, para aprovisionar automáticamente conexiones de "capa de trayecto" (en soporte de un servicio) que se extienden a uno o más dominios.

La información relativa al estado de la conexión (por ejemplo, averías y calidad de la señal) es detectada por el plano de transporte y proporcionada al plano de control.

El plano de control transporta (distribuye) información relativa al estado del enlace (por ejemplo, adyacencia, capacidad disponible y fallos) necesaria para soportar el establecimiento/liberación y restablecimiento de la conexión.

La información pormenorizada de la gestión de averías o la correspondiente a la supervisión de la calidad de funcionamiento es transportada dentro del plano de transporte (a través de la tara/operación, administración y mantenimiento (OAM, *operation, administration and maintenance*) y a través del plano de gestión (incluida la red de comunicación de datos (RCD)).

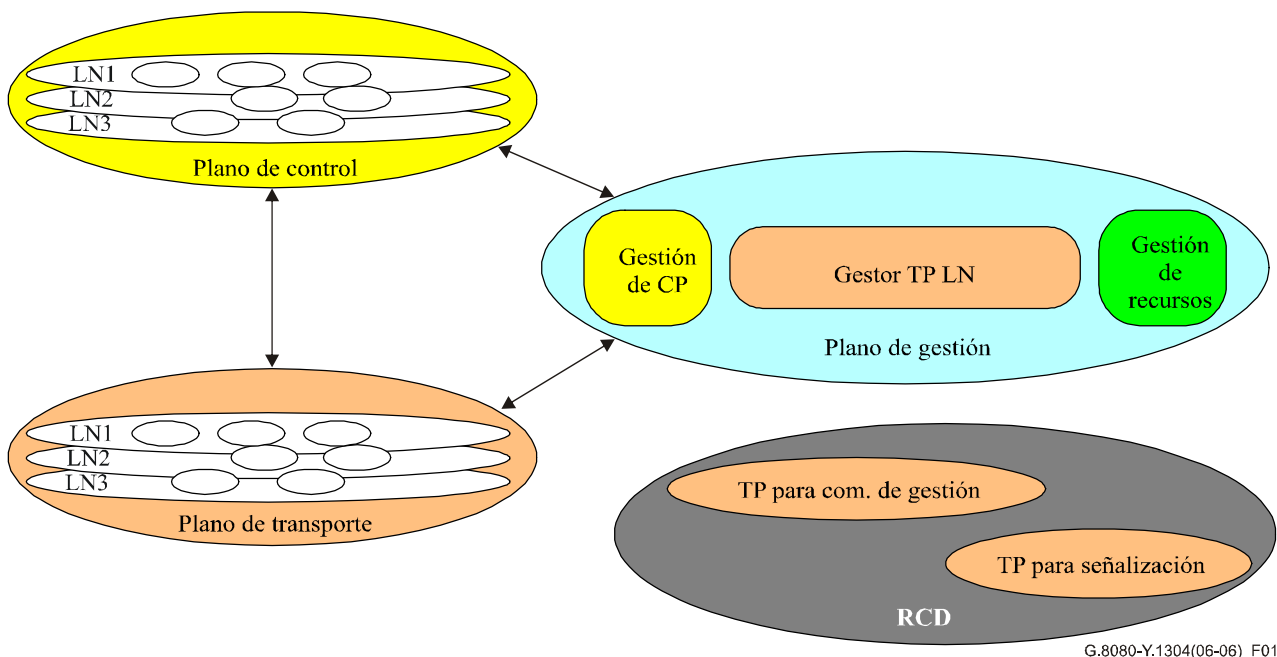
La interconexión entre y dentro de dominios se describe en términos de puntos de referencia. Como los dominios son establecidos por políticas de operador, los puntos de referencia entre dominios son puntos de demarcación de servicio para una sola capa de servicio (es decir, puntos donde se proporciona control de llamada). El intercambio de información a través de estos puntos de referencia es descrito por las múltiples interfaces abstractas entre componentes de control. Una interfaz física se provee haciendo corresponder una o más interfaces abstractas de componentes a un protocolo. Múltiples interfaces abstractas pueden ser multiplexadas por una sola interfaz física. El punto de referencia entre un usuario y un dominio de proveedor es la UNI, que representa un punto de demarcación de servicio entre el usuario y el proveedor. El punto de referencia entre dominios es la interfaz externa red-red (E-NNI, *external network-network interface*), que representa un punto de demarcación de servicio que soporta establecimiento de conexión multidominios. El punto de referencia dentro de un dominio es una interfaz interna red-red (I-NNI, *internal network-network interface*), que representa un punto de conexión que soporta establecimiento de conexión intradominio. Los flujos de información a través de estos puntos de referencia se describen con más detalle en la cláusula 8.

Se puede también subdividir el plano de control para permitir la segregación de recursos, por ejemplo entre redes privadas virtuales (RPV). Si los recursos están dedicados a dominios independientes, no se suministrarán puntos de referencia entre dichos dominios. El caso en que una parte de los recursos se comparte dinámicamente queda en estudio.

Se presentan descripciones independientes de las interacciones entre:

- el plano de control y las redes de capa del plano de transporte; y
- el plano de gestión y los planos de transporte que resulten de la adición del plano de control para la configuración de la supervisión y la gestión de conexiones.

La presente Recomendación abarca el control de las conexiones de red de capa de transporte, incluidas las interacciones que se producen dentro de la capa como resultado de peticiones de capacidad en las capas de servidores.



**Figura 1/G.8080/Y.1304 – Relaciones entre los componentes arquitecturales**

## 5.1 Control de llamada y control de conexión

En la presente Recomendación se separan los procedimientos de control de llamada de los de control de conexión, debido a que se requiere el control de conexión únicamente en las fronteras de los dominios (por ejemplo en las UNI y E-NNI). Por lo tanto, al interior de los dominios (es decir, en I-NNI) sólo es necesario soportar los procedimientos de control de conexión. Adicionalmente, se proporciona control de llamada en las fronteras de los NCC ubicados entre capas. Las funciones ejecutadas por los controladores de llamada en fronteras de dominio son definidas por las políticas asociadas por las interacciones permitidas entre los dominios. Las políticas son establecidas por el operador. De este modo, se considera que una llamada extremo a extremo está formada por múltiples segmentos de llamada, dependiendo de si la llamada atraviesa múltiples dominios. Esto permite flexibilidad en la elección de los paradigmas de señalización, encaminamiento y restablecimiento en diferentes dominios.

Debería señalarse que la llamada es la representación del servicio ofrecido al usuario de una capa de red, mientras que las conexiones son uno de los medios por los cuales las redes entregan dichos servicios. Puede haber otras entidades utilizadas para soportar llamadas, tales como las que contienen procesos específicos del servicio.

### 5.1.1 Control de llamada

El control de llamada es una asociación de señalización entre una o más aplicaciones de usuario y la red para controlar el establecimiento, liberación, modificación y mantenimiento de conjuntos de conexiones. Se utiliza el control de llamada para mantener la asociación entre partes, y una llamada puede incluir cualquier número de conexiones subyacentes, o ninguna, en cualquier momento.

Se puede realizar el control de llamada mediante uno de los métodos siguientes:

- Separación de la información de llamada en parámetros transportados por un solo protocolo de llamada/conexión.
- Separación de las máquinas de estados para el control de llamada y el control de conexión, mientras que se señala información en un sólo protocolo de llamada/conexión.
- Separación de información y máquinas de estados mediante protocolos de señalización distintos para el control de llamada y el control de conexión.

El control de llamada tiene que proporcionar coordinación de conexiones (en una llamada multiconexión) y coordinación de partes (en llamadas multipartitas). Para coordinar conexiones múltiples, deberán ejecutarse las siguientes acciones en la red:

- Todas las conexiones deben ser encaminadas para que puedan ser supervisadas por al menos una entidad (de control de llamada) coordinadora.
- Las asociaciones de control de llamada deben concluirse antes de establecer las conexiones. Una llamada puede existir sin conexiones (lo que facilita rearrreglos de conexión complejos).

Se puede considerar que una llamada tiene tres fases:

### **Fase de establecimiento**

Durante esta fase, se intercambian mensajes de señalización entre usuarios y la red para negociar las características de la llamada. El intercambio de mensajes de señalización entre la parte llamante y la red se conoce como llamada saliente. El intercambio de señalización entre la red y la parte llamada se designa por llamada entrante.

### **Fase de llamada activa**

Durante esta fase, se pueden intercambiar datos en las conexiones asociadas y se pueden también modificar parámetros de la llamada (por ejemplo, adición de nuevas partes en una llamada punto a multipunto, siempre que este tipo de llamada esté soportado).

### **Fase de liberación**

Durante esta fase se intercambian mensajes de señalización entre las partes llamante, llamada y la red para terminar la llamada. Una llamada puede ser liberada bien por el terminal llamante o por el terminal llamado, o por gestión de un apoderado o de la red.

## **5.1.2 Control de admisión de llamada**

El control de admisión de llamada es una función de política invocada por un rol de origen en una red y que puede implicar la cooperación con el rol de terminación en la red. Obsérvese que el hecho de permitir que una llamada prosiga sólo indica que ésta puede pedir una o más conexiones. Esto no implica que cualquiera de esas peticiones de conexión tendrá éxito. El control de admisión de llamada puede también ser invocado en otras fronteras de red.

La función admisión de llamada de origen se encarga de verificar que se ha suministrado un nombre de usuario llamado y parámetros válidos. Los parámetros de servicio se verifican de acuerdo con una especificación de nivel de servicio (un conjunto de parámetros y valores convenido entre el operador de red y el cliente para un determinado servicio, que indica el '*alcance*' de dicho servicio). Cuando sea necesario, estos parámetros podrían ser renegociados con el usuario de origen. El alcance de esta negociación se determina mediante políticas que se derivan de la especificación de nivel de servicio original, derivada a su vez del acuerdo de nivel de servicio (el contrato de servicio entre un operador de red y un cliente que define las responsabilidades globales de cada uno de ellos).

La función admisión de llamada de terminación se encarga de verificar que la parte llamada tiene derecho a aceptar la llamada, de acuerdo con los contratos de servicio entre la parte llamante y la parte llamada. Por ejemplo, una dirección llamante podría someterse a un proceso de cribado.

## **5.1.3 Control de conexión**

El control de conexión se encarga del control global de conexiones individuales. También puede considerarse que el control de conexión está asociado con el control de enlace. El control global de una conexión lo realiza el protocolo que emprende los procedimientos de establecimiento y liberación asociados con una conexión y el mantenimiento del estado de la conexión.

#### **5.1.4 Control de admisión de conexión**

El control de admisión de conexión es esencialmente un proceso que determina si existen suficientes recursos para admitir una conexión (o renegocia recursos durante una llamada). En general, esto se efectúa enlace por enlace, basándose en condiciones y políticas locales. En el caso de una red con conmutación de circuitos, esto se reducirá, sencillamente, a determinar si existen recursos disponibles libres. En cambio, en el caso de redes de conmutación de paquetes, como las que emplean ATM, en las que existen múltiples parámetros de calidad de servicio, el control de admisión de conexión debe asegurarse de que la admisión de nuevas conexiones es compatible con acuerdos de calidad de servicio existentes para conexiones existentes. El control de admisión de conexión puede rechazar la petición de conexión.

#### **5.1.5 Relaciones entre el estado de la llamada y el estado de la conexión**

El estado de la llamada depende del estado de las conexiones asociadas. Esta dependencia está relacionada con el tipo de llamada y la política aplicada. Por ejemplo, cuando exista una sola conexión y ésta falla, la llamada puede ser liberada inmediatamente, o como otra posibilidad, puede ser liberada después de transcurrido un periodo de tiempo, si no se puede obtener otra conexión mediante mecanismos tales como la protección o el restablecimiento. Cabe señalar que la llamada y la conexión coinciden en las fronteras de los dominios.

### **5.2 Interacción entre los planos de control, de transporte y de gestión**

La figura 1 ilustra las relaciones generales entre los planos de control, de gestión y de transporte. Cada plano es autónomo, pero se producen algunas interacciones. A continuación se proporcionan más detalles sobre las interacciones entre los distintos planos.

#### **5.2.1 Interacción gestión – transporte**

El plano de gestión interactúa con los recursos de transporte funcionando en un modelo de información adecuado, que presenta una visión de gestión del recurso subyacente. Los objetos del modelo de información están colocados físicamente con el recurso de transporte e interactúan con ese recurso a través de las interfaces de información de gestión (MI, *management information*) del modelo funcional específico de la capa. Estas interfaces deben estar colocadas con el objeto gestionado y el componente de control.

#### **5.2.2 Interacción control – transporte**

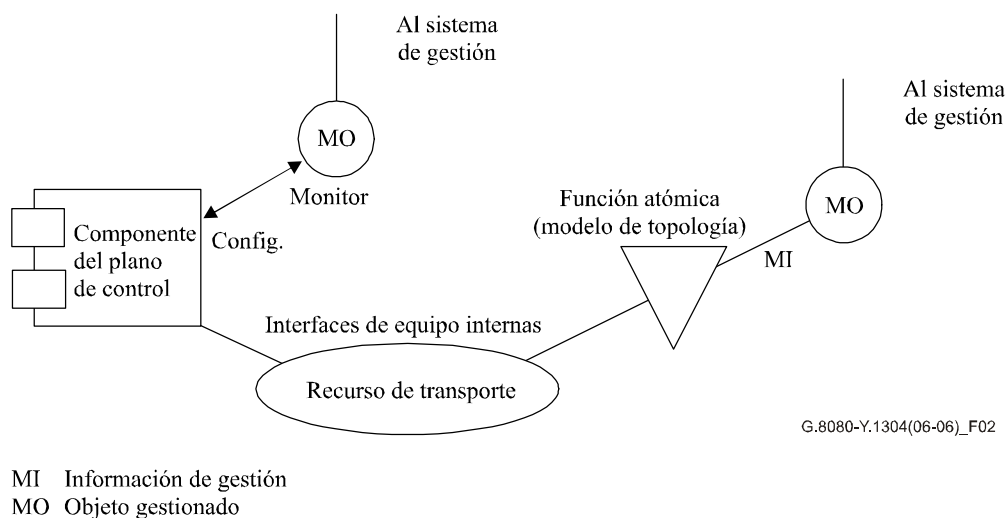
Sólo dos componentes arquitecturales tienen una estrecha relación con un recurso de transporte físico.

En el límite más bajo de recursión, el controlador de conexión (CC, *connection controller*) proporciona una interfaz de señalización para controlar una función de conexión. Este componente está colocado físicamente con la función de conexión y todos los demás detalles del soporte físico están ocultos. Sin embargo, dado el limitado flujo de información, un nuevo protocolo puede ser útil para optimizar esta comunicación. El ejecutante de terminación y adaptación (TAP, *termination and adaptation performer*) está colocado físicamente con el equipo que ejecuta funciones de adaptación y terminación, y proporciona una visión del plano de control de las conexiones de enlace. El TAP oculta la interacción con el soporte físico.

#### **5.2.3 Interacción gestión – control**

La cláusula 7.1 dice que cada componente tiene un conjunto de interfaces especiales que permiten supervisar el funcionamiento del componente, establecer dinámicamente las políticas e influir sobre el comportamiento interno. Estas interfaces son equivalentes a la interfaz MI del modelo funcional de transporte, y permiten que el componente presente una visión al sistema de gestión y ser configurado por un sistema de gestión. Esto se trata con más detalle en 7.1.

El plano de gestión interactúa con componentes de control ejecutando un modelo de información adecuado, que presenta una visión de gestión del componente subyacente. Los objetos del modelo de información están colocados físicamente con un componente de control e interactúan con ese componente a través de las interfaces de supervisión y configuración del mismo. Estas interfaces deben estar colocadas con el objeto gestionado y el componente de control.



**Figura 2/G.8080/Y.1304 – Interacciones del plano de gestión/transporte con recursos de transporte**

Los recursos de transporte físico, que representan la realidad física del equipo, se describen como las funciones atómicas G.805. Los objetos gestionados (MO, *managed objects*) que representan la visión de gestión externa del equipo, interactúan con el modelo funcional especificado en las recomendaciones del equipo a través de los puntos de referencia de MI, que también están contenidos completamente dentro del equipo. Obsérvese que el objeto gestionado representa la visión de gestión, con independencia del protocolo de gestión utilizado. Esta información es independiente del protocolo empleado.

A partir de la visión del plano de control, los componentes del plano de control actúan directamente sobre los recursos de transporte, de modo que el funcionamiento del plano de control aparece autónomo al plano de gestión. De la misma manera, las operaciones del plano de gestión aparecen autónomas al plano de control. Ésta es exactamente la misma situación que existe cuando múltiples gestores gestionan el equipo. Cada gestor desconoce la existencia de los otros y sólo ve el comportamiento del equipo autónomo. Aunque la información presentada al plano de control es similar a la presentada a la gestión, no es idéntica a la información de gestión (MI). La información del plano de control solapa los datos de MI porque el plano de control requiere alguna información de gestión, pero no toda. Por ejemplo, es probable que el restablecimiento sea activado por las mismas condiciones que normalmente activan acciones de protección.

Los objetos gestionados específicos del componente presentan una visión de gestión de los componentes del plano de control a través de las interfaces del monitor en el componente. Es crítico realizar que ésta es la visión de los aspectos gestionables del componente, y no una visión del recurso de transporte, que se obtiene a través de la visión de gestión.

#### 5.2.4 Gestión de recursos

Se pueden clasificar los recursos de red entre los que están bajo la autoridad del plano de gestión y los que están bajo la autoridad del plano de control. Para el plano de control no será posible modificar los recursos que estén bajo la autoridad del plano de gestión. Esta restricción tiene en cuenta los recursos de red que no estén en uso, pero que se hayan reservado para uso futuro



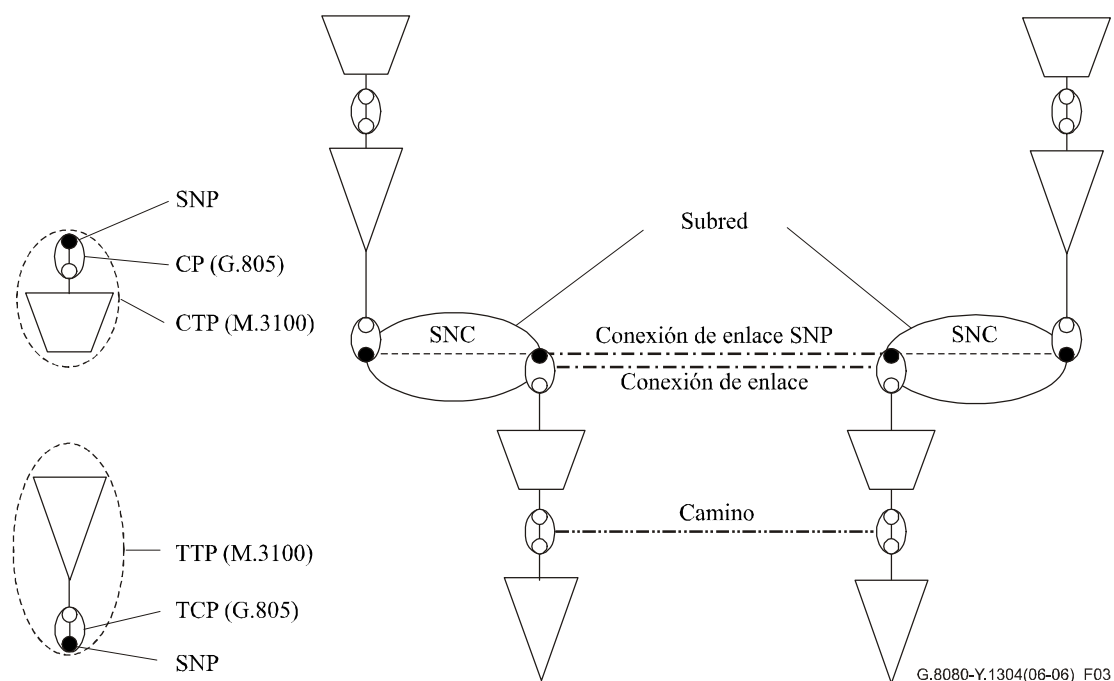
(por ejemplo, por los planificadores de red). Siendo esto así, la gestión de recursos es realizada por el plano de gestión y está fuera del ámbito de la presente Recomendación.

## 6 Recursos de transporte y su organización

La arquitectura funcional de la red de transporte describe la forma en que se utilizan los recursos de transporte para realizar las funciones básicas de transporte de una manera que no haga referencia al control ni a la gestión de dichas funciones. A los efectos del control y la gestión, cada recurso de transporte tiene un agente estrechamente acoplado que representa el rol que ha de desempeñar. Estos agentes interactúan con otras funciones que están participando en el control y la gestión a través de interfaces, y presentan información o ejecutan operaciones cuando sea necesario. Los recursos de transporte están organizados en áreas de encaminamiento y subredes para fines de control y gestión.

### 6.1 Entidades de transporte

A fin de gestionar conexiones dentro de una red de capa, los recursos del plano de transporte subyacente se representan por un número de entidades en el plano de control. En la figura 3 se muestran las relaciones entre los recursos de transporte descritos en la Rec. UIT-T G.805, las entidades que representan dichos recursos para fines de gestión de red (tal como se describe en la Rec. UIT-T M.3100) y los recursos de transporte desde el punto de vista del plano de control.



**Figura 3/G.8080/Y.1304 – Relaciones entre entidades arquitecturales en el plano de transporte, en el plano de gestión y en el plano de control**

Un SNP tiene cierto número de relaciones con otros SNP:

- Una relación estática entre dos SNP en subredes diferentes. Se designa por una conexión de enlace SNP.
- Una relación dinámica entre dos (o más, en el caso de conexiones de radiodifusión) puntos de subred en la frontera de la misma subred. Se designa por una conexión de subred.

Se puede también agrupar un punto de subred con otros SNP a efectos de encaminamiento. Ésta es una agrupación de puntos de subred (SNPP, *subnetwork point pool*), y está estrechamente relacionada con extremos de enlace (definidos en la Rec. UIT-T G.852.2); sin embargo, esta relación es más flexible que el extremo de enlace. Una SNPP puede ser subdividida en agrupaciones más pequeñas. Una utilización de esta subestructuración consiste en describir diferentes grados de diversidad de ruta. Por ejemplo, todos los SNP en una subred que tienen una relación con un grupo similar de otra subred se pueden agrupar en una sola SNPP. Esta SNPP puede ser entonces subdividida para representar diversas rutas y subdividida más aún para representar, por ejemplo, longitudes de onda individuales.

La asociación entre varias SNPP en diferentes subredes se conoce como enlace SNPP.

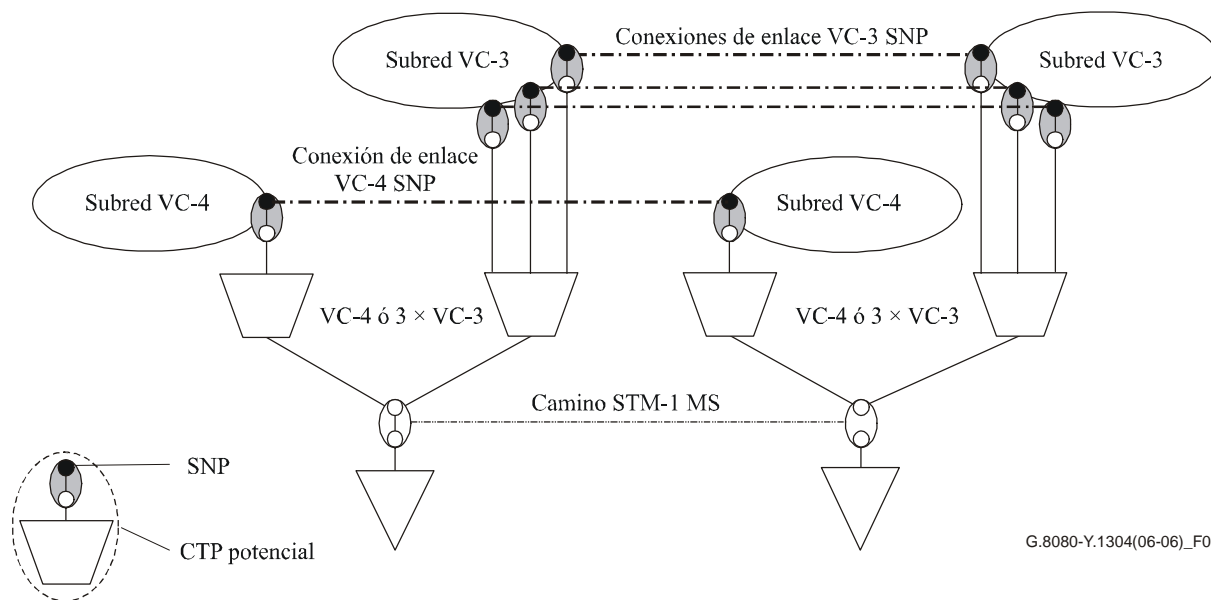
Los estados de SNP y de conexión de enlace SNP de interés para el plano de control se describen respectivamente en 7.3.7 (Ejecutantes de terminación y adaptación) y 7.3.3 (Componente gestor de recursos de enlace).

### Funciones de adaptación variable

Cierto número de sistemas de transporte soporta adaptación variable, según la cual un solo camino de capa servidora puede soportar dinámicamente diferentes estructuras de multiplexación.

Esta situación se puede modelar asignando SNP para cada CP en las diversas estructuras, y colocando esos SNP en sus respectivas subredes de capa. Cuando se atribuya un determinado ejemplar de SNP, se activará el proceso específico del cliente pertinente en la función de adaptación y creará el CTP asociado. Los SNP en otras redes de capa que utilicen los mismos recursos devienen ocupados.

En la figura 4 se muestra un ejemplo de un camino STM-1 que puede soportar bien un solo VC-4 o tres VC-3.

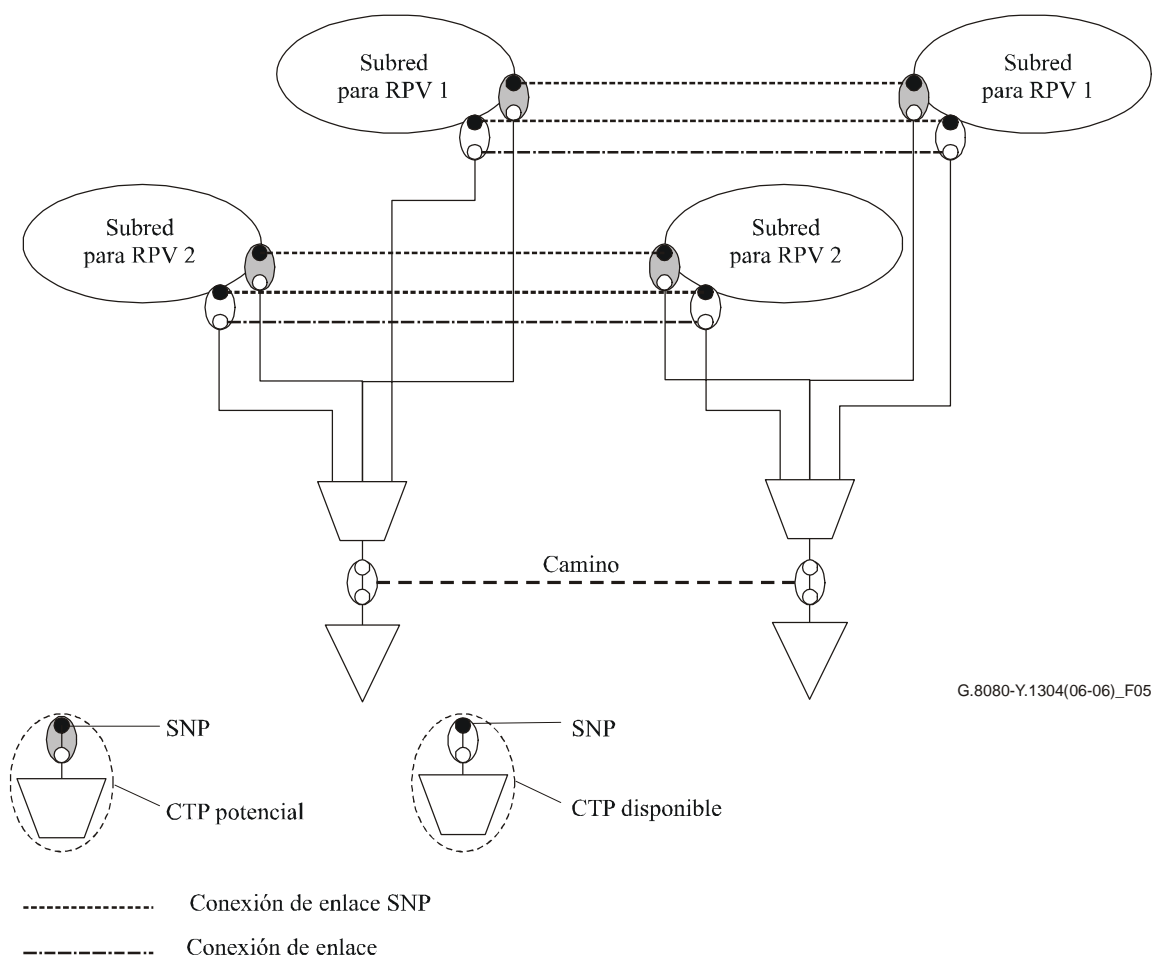


**Figura 4/G.8080/Y.1304 – Ejemplo de adaptación variable  
(camino STM-1 que soporta 3 × VC-3 ó 1 × VC-4)**

### Recursos de enlace compartidos entre RPV

La Rec. UIT-T Y.1313 define varios modelos básicos de servicio mediante los cuales pueden proporcionarse las RPV de capa 1 (L1RPV) a través de la arquitectura ASON.

Una RPV es un grupo cerrado de usuarios que puede utilizar un conjunto definido de recursos de red. En el plano de control, una SNPP puede ser pública, es decir, no asociada con ninguna RPV, o privada, es decir, asociada exactamente con una RPV. El encaminamiento de conexión en una RPV sólo puede emplear las SNPP asociadas con esa RPV. En el plano de transporte, un punto de conexión (CP, *connection point*) puede estar asignado a un SNP en múltiples SNPP, públicas o privadas. La conectividad en un enlace compartido entre las RPV puede ser modelizada creando un SNP por cada uno de los CP compartidos en cada RPV. Cuando un CP es adjudicado a un determinado SNP en una RPV, los SNP que representan los mismos recursos en otras RPV pasan al estado ocupado. La figura 5 muestra un ejemplo de dos RPV, cada una con dos SNP en el plano de control. En el plano de transporte, el primer CP está asignado y atribuido al segundo SNP en la RPV 2, el tercer CP está asignado y atribuido al segundo SNP en la RPV 1 y el segundo CP está asignado a ambos, el primer SNP en la RPV 1 y el primer SNP en la RPV 2. Si el segundo CP es adjudicado al primer SNP en la RPV 1, este SNP pasa al estado disponible mientras que el primer SNP en la RPV 2 pasa al estado ocupado.



**Figura 5/G.8080/Y.1304 – Atribución de recursos de enlace entre RPV**

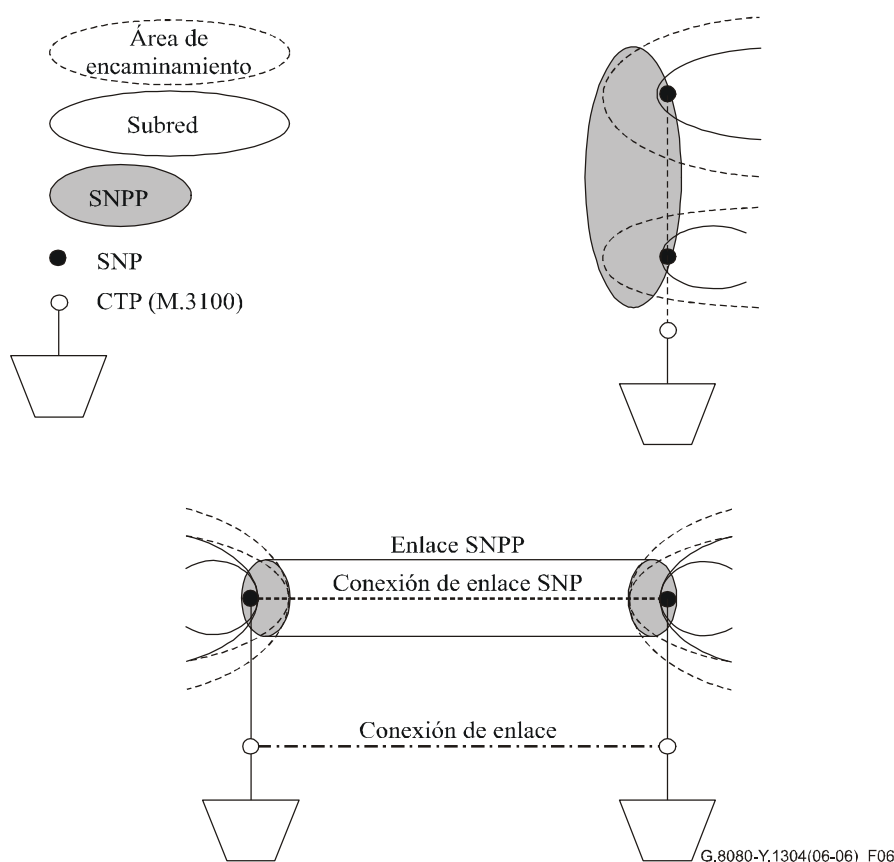
## 6.2 Áreas de encaminamiento

En el contexto de esta Recomendación un área de encaminamiento existe dentro de una red de capa simple. Un área de encaminamiento se define por un conjunto de subredes, los enlaces SNPP que las interconectan, y las SNPP que representan los extremos de los enlaces SNPP que salen de esa área de encaminamiento. Un área de encaminamiento puede incluir áreas de encaminamiento más

pequeñas interconectadas por enlaces SNPP. El límite de la subdivisión produce un área de encaminamiento que contiene una subred.

Las áreas de encaminamiento y las subredes están relacionadas muy estrechamente ya que ambas desempeñan una función idéntica en cuanto a la partición de una red. La distinción crítica es que en la frontera, los extremos del enlace son visibles desde *dentro* de un área de encaminamiento (RA, *routing area*), mientras que desde *dentro* de una subred sólo pueden verse los puntos de conexión. Vistas desde el *exterior* las subredes y las RA son idénticas, y ambos términos pueden utilizarse casi como sinónimos. La distinción entre los dos términos suele depender del contexto, aunque el término *nodo* se emplea a menudo para designar una subred o una RA. Obsérvese también que desde el exterior de las subredes y de las áreas de encaminamiento, no es posible apreciar los detalles internos, y que ambas aparecen como puntos en el gráfico de topología de la red.

Cuando un enlace SNPP cruza la frontera de un área de encaminamiento, todas las áreas de encaminamiento que comparten esa frontera común han contenido enlaces SNPP coincidentes. Esto se muestra en la figura 6.

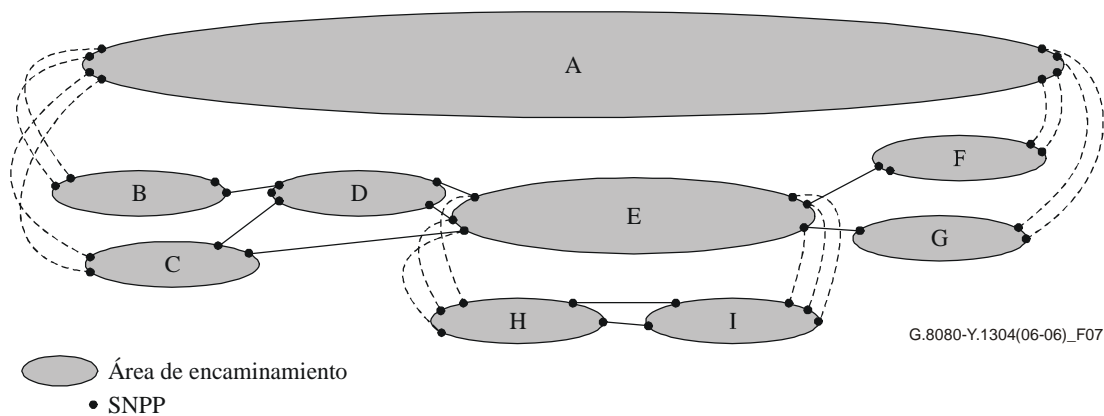


**Figura 6/G.8080/Y.1304 – Relación entre áreas de encaminamiento, subredes, SNP y SNPP**

### 6.2.1 Agregación de enlaces y áreas de encaminamiento

La figura 7 ilustra las relaciones entre las áreas de encaminamiento, las SNPP y los enlaces SNPP. Las áreas de encaminamiento y los enlaces SNPP pueden estar relacionados jerárquicamente. En el ejemplo, el área de encaminamiento A está dividida para crear un nivel más bajo de áreas de encaminamiento B, C, D, E, F, G y enlaces SNPP de interconexión. Esta recursión puede continuar tantas veces como sea necesario. Por ejemplo, el área de encaminamiento E se subdivide a su vez para mostrar las áreas de encaminamiento H e I. En el ejemplo indicado hay una sola área de encaminamiento de nivel superior. Al crear una estructura de áreas de encaminamiento jerárquico basadas en la contención (en la cual las áreas de encaminamiento de nivel más bajo están

contenidas completamente dentro de una sola área de encaminamiento de nivel más alto), sólo un subconjunto de las áreas de encaminamiento de nivel más bajo y un subconjunto de sus enlaces SNPP están en la frontera del área de encaminamiento de nivel más alto. La estructura interna del nivel más bajo es visible al nivel más alto cuando es visto desde dentro del área A, pero no desde fuera del área A. En consecuencia, sólo los enlaces SNPP en la frontera entre un nivel más alto y un nivel más bajo son visibles al nivel más alto cuando es visto desde fuera del área A. De este modo, los enlaces SNPP más externos de B y C y F y G son visibles desde fuera de A, pero no los enlaces SNPP internos asociados con D y E, o los que están entre B y D, C y D, C y E o entre E y F o E y G. La misma visibilidad se aplica entre E y sus áreas subordinadas H e I. Esta visibilidad de la frontera entre niveles es recursiva. Por consiguiente, las jerarquías de enlaces SNPP sólo pueden ser creadas en los puntos donde las áreas de encaminamiento de nivel más alto están limitadas por enlaces SNPP en áreas de encaminamiento de nivel más bajo.



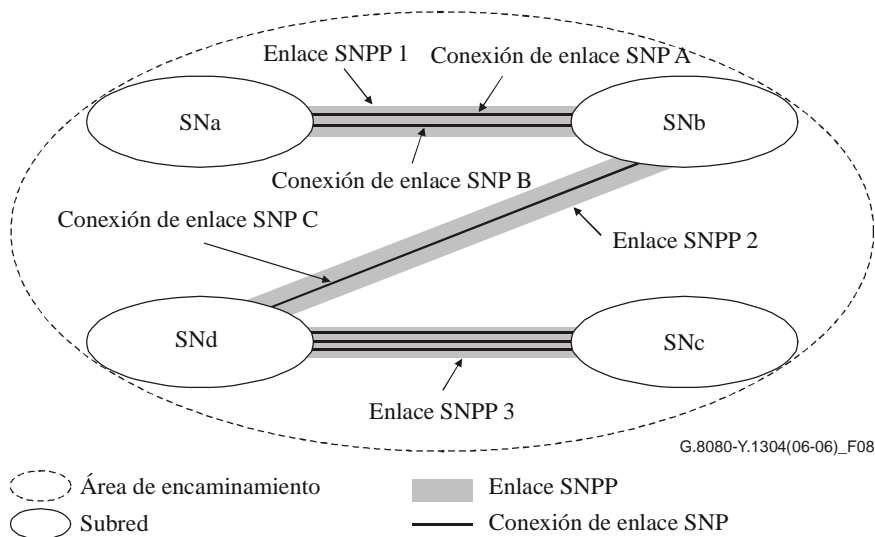
**Figura 7/G.8080/Y.1304 – Ejemplo de relaciones de una jerarquía de áreas de encaminamiento y de enlaces SNPP**

Los puntos de subred están atribuidos a un enlace SNPP en el nivel más bajo de la jerarquía de encaminamiento y pueden ser atribuidos solamente a una agrupación de puntos de subred en ese nivel. En las fronteras de la jerarquía de áreas de encaminamiento, la agrupación de enlaces SNPP en un nivel más bajo está totalmente contenida por un enlace SNPP en un nivel más alto. Una agrupación de enlaces SNPP de nivel más alto puede contener uno o más enlaces SNPP de nivel más bajo. En cualquier nivel de esta jerarquía, un enlace SNPP está asociado solamente con un área de encaminamiento. Como tal, las áreas de encaminamiento no se superponen en ningún nivel de la jerarquía. Los enlaces SNPP dentro de un nivel de la jerarquía de áreas de encaminamiento que no están en la frontera de un nivel más alto pueden estar en la frontera con un nivel más bajo creando así una jerarquía de enlaces SNPP desde ese punto (por ejemplo, área de encaminamiento E). Esto proporciona la creación de una jerarquía de contención para enlaces SNPP.

Un área de encaminamiento puede tener un espacio de nombre SNPP independiente de los utilizados en otras áreas de encaminamiento. Obsérvese que un nombre SNPP es encaminable en la RA a cuyo espacio de nombre SNPP pertenece.

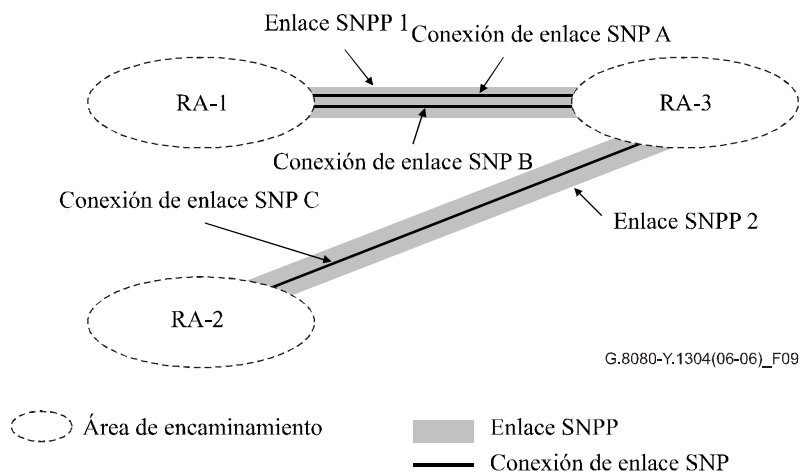
### 6.2.2 Relaciones con enlaces y agregación de enlaces

Varias conexiones de enlace SNP dentro de un área de encaminamiento pueden ser asignadas al mismo enlace SNPP solamente si van entre las dos mismas subredes. Esto se ilustra en la figura 8. Cuatro subredes, SNa, SNb, SNc y SNd y los enlaces SNPP 1, 2 y 3 están dentro de una sola área de encaminamiento. Las conexiones de enlace SNP A y B están en el enlace SNPP 1. Las conexiones de enlace SNP B y C no pueden estar en el mismo enlace SNPP porque no conectan con las dos mismas subredes. Se aplica un comportamiento similar a la agrupación de los SNP entre áreas de encaminamiento.



**Figura 8/G.8080/Y.1304 – Relación de enlaces SNPP con subredes**

La figura 9 muestra tres áreas de encaminamiento, RA-1, RA-2 y RA-3 y los enlaces SNPP 1 y 2. Las conexiones de enlace SNP A, B y C no pueden estar en el mismo enlace SNPP porque en sus puntos extremos se encuentran más de dos áreas de encaminamiento. Las conexiones de enlace SNP A y B no son equivalentes a la conexión de enlace SNP C para el encaminamiento desde el área de encaminamiento 3 (RA-3).



**Figura 9/G.8080/Y.1304 – Relaciones de enlaces SNPP con áreas de encaminamiento**

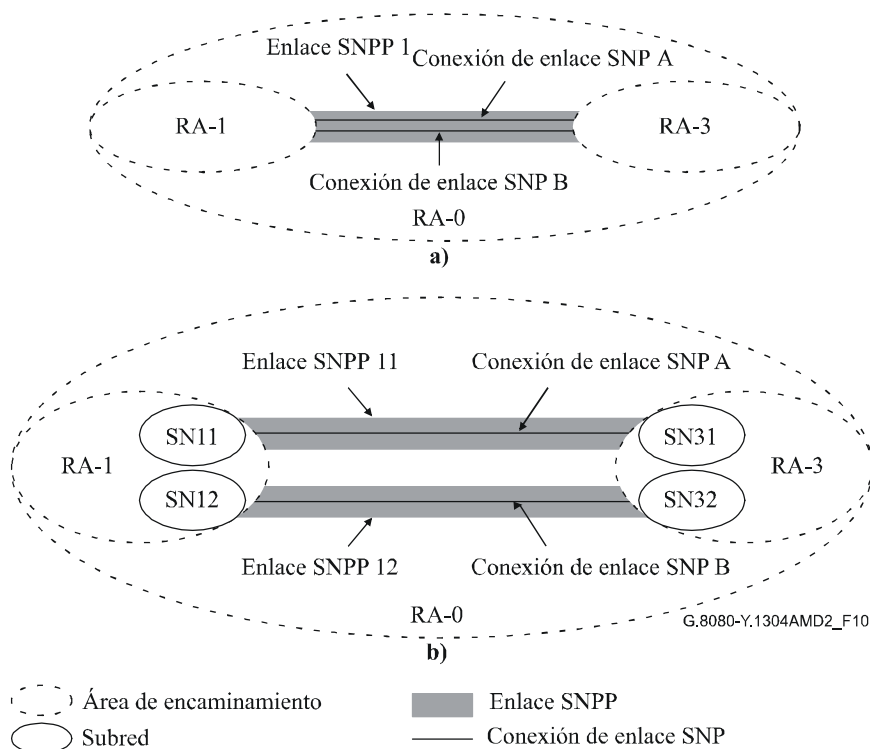
Las conexiones de enlace SNP entre dos áreas de encaminamiento, o subredes, pueden ser agrupadas en uno o más enlaces SNPP. Se puede requerir la agrupación en múltiples enlaces SNPP:

- si no son equivalentes a efectos de encaminamiento con respecto a las áreas de encaminamiento a las que están unidos, o al área de encaminamiento contenedora,
- si se requieren agrupaciones más pequeñas a efectos administrativos.

Puede haber más de un ámbito de encaminamiento para considerar cuándo organizar conexiones de enlace SNP en enlaces SNPP. En la figura 10 hay dos conexiones de enlace SNP entre las áreas de encaminamiento 1 y 3. Si estas dos áreas de encaminamiento están en la parte superior de la

jerarquía de encaminamiento (por consiguiente, no hay una sola área de encaminamiento de nivel máximo), el ámbito del encaminamiento de RA-1 y RA-3 se utiliza para determinar si las conexiones de enlace SNP son equivalentes a los efectos de encaminamiento.

Sin embargo, la situación puede ser la que se muestra en la figura 10. En este caso, RA-0 es un área de encaminamiento contenedora. Desde el punto de vista de RA-0, las conexiones de enlace SNP A y B podrían estar en uno (caso a) o dos (caso b) enlaces SNPP. Un ejemplo de cuándo basta un enlace SNPP, es cuando el paradigma de encaminamiento para RA-0 es paso por paso. El cálculo del trayecto no distingue entre la conexión de enlace SNP A y B como un siguiente paso a partir, digamos, de RA-1 a RA-2.



**Figura 10/G.8080/Y.1304 – Alcance del encaminamiento**

Desde el punto de vista de RA-1 y RA-3, las conexiones de enlace SNP pueden ser muy distintas desde el punto de vista del encaminamiento, pues la elección de la conexión de enlace SNP A puede ser más conveniente que la conexión de enlace SNP B por motivos de costo, protección u otros. En este caso, la colocación de cada conexión de enlace SNP en su propio enlace SNPP satisface el requisito de "equivalente a los efectos de encaminamiento". Obsérvese que en la figura 10, los enlaces SNPP 11, 12 y 1 pueden coexistir todos.

Otra razón para elegir el enlace SNPP 11 (figura 10-b) en lugar del enlace SNPP 12 podría deberse a que el costo de cruzar RA-3 es distinto desde el enlace SNPP 11 que desde el enlace SNPP 12, lo que sugiere que sería útil un mecanismo para determinar el costo relativo de cruzar RA-3 desde el enlace 11 y desde el enlace 12. Dicho mecanismo podría ser aplicado recurrentemente para determinar el costo relativo de atravesar RA-0. Obsérvese que esto no implica la necesidad de exponer la topología interna de ninguna área de encaminamiento fuera de su ámbito. Para obtener el costo de una determinada ruta elegida podría invocarse una función de interrogación. Los costos retornados de resultados de dicha interrogación serían determinados por la política aplicada a cada área de encaminamiento. En todas las áreas de encaminamiento debería aplicarse una política común, con lo que los costos serían comparables. Esa interrogación también podría generalizarse para poder aplicar constricciones de encaminamiento antes de calcular el costo.

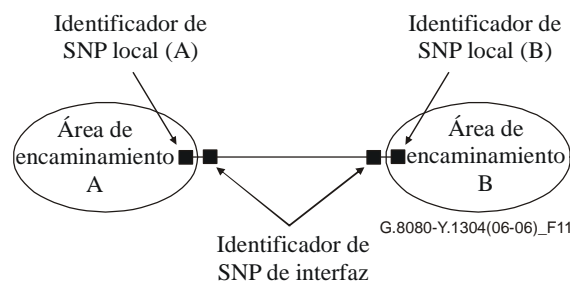
### 6.3 Topología y descubrimiento

La función encaminamiento entiende la topología en términos de enlaces SNPP. Antes de que se puedan crear enlaces SNPP, hay que establecer la topología de transporte subyacente, es decir, las relaciones conexión de enlace entre CP. Estas relaciones pueden ser descubiertas (o confirmadas de acuerdo con un plan de red) utilizando cierto número de técnicas diferentes; por ejemplo, se puede utilizar una señal de prueba o se pueden derivar de una traza de camino en la capa servidora. También pueden ser proporcionadas por un sistema de gestión basado en un plan de red. La capacidad del equipo de transporte para soportar funciones de adaptación flexible (y por tanto, conexiones de enlace para múltiples redes de capa de cliente) puede también ser descubierta o informada.

Las conexiones de enlace que son equivalentes para fines de encaminamiento serán entonces agrupadas en enlaces. Esta agrupación se basa en parámetros, tales como costo del enlace, retardo, calidad o diversidad. Algunos de esos parámetros pueden derivarse de la capa servidora, pero, en general, serán proporcionados por el plano de gestión.

Se pueden crear enlaces separados (es decir, conexiones de enlace que son equivalentes a efectos de encaminamiento pueden colocarse en diferentes enlaces) con el fin de permitir la división de recursos entre diferentes redes ASON (por ejemplo, diferentes RPV) o entre recursos controlados por una ASON y el plano de gestión.

La información de enlace (por ejemplo, las conexiones de enlace constituyente y los nombres de los pares CP) se utiliza entonces para configurar los ejemplares LRM (descritas en 7.3.3) asociadas con el enlace SNPP. También se pueden proporcionar características adicionales del enlace, basadas en parámetros de las conexiones de enlace. Los LRM en cada extremo del enlace tienen que establecer una adyacencia de plano de control que corresponda al enlace SNPP. Los identificadores de SNPP de interfaz se pueden negociar durante el descubrimiento de adyacencia o pueden ser proporcionados como parte de la configuración LRM. Las conexiones de enlace y los nombres de CP se hacen entonces corresponder a identificadores de SNP de interfaz (y a nombres de conexión de enlace SNP). Cuando ambos extremos del enlace están dentro de la misma área de encaminamiento, los identificadores de SNPP local y de interfaz, y los identificadores de SNP local y de interfaz pueden ser idénticos. De lo contrario, en cada extremo del enlace el identificador de SNP de interfaz se hace corresponder a un identificador de SNPP local, y los identificadores de SNP de interfaz se hacen corresponder a identificadores de SNP local. Esto se muestra en la figura 11.



**Figura 11/G.8080/Y.1304 – Relación entre identificador local e identificador de interfaz**

Seguidamente, las conexiones de enlace SNP resultantes pueden ser validadas mediante un proceso de descubrimiento. El grado de validación requerido en esta etapa depende de la integridad de las relaciones de conexión de enlace suministradas inicialmente por el plano de transporte o por el plano de gestión, y de la integridad del proceso utilizado para hacer corresponder los CP a SNP.



La validación se puede obtener a partir de una traza de camino en la capa servidora o utilizando una señal y conexiones de prueba. Si se utilizan conexiones de prueba, el proceso de descubrimiento puede establecer y liberar estas conexiones utilizando sea el plano de gestión, sea el plano de control. Si se utiliza el plano de control, el enlace se debe poner temporalmente a disposición del control de encaminamiento y conexión, sólo para conexiones de prueba.

Una vez concluida la validación de enlace SNPP, los LRM informan al componente RC (véase 7.3.2) de la adyacencia del enlace SNPP y las características del enlace, por ejemplo, costo, desempeño, calidad y diversidad.

## **6.4 Dominios**

Como ya se adelantó en la cláusula 5, hemos generalizado la noción de dominio incorporada en la definición G.805 de dominios administrativos y de gestión, así como la noción de regiones administrativas Internet, para expresar distintas responsabilidades administrativas y/o de gestión, relaciones de confianza, capacidades de infraestructura de esquemas de direccionamiento, técnicas de supervivencia, distribuciones de la funcionalidad de control, etc. Por consiguiente, un dominio representa un conjunto de entidades agrupadas para una determinada finalidad.

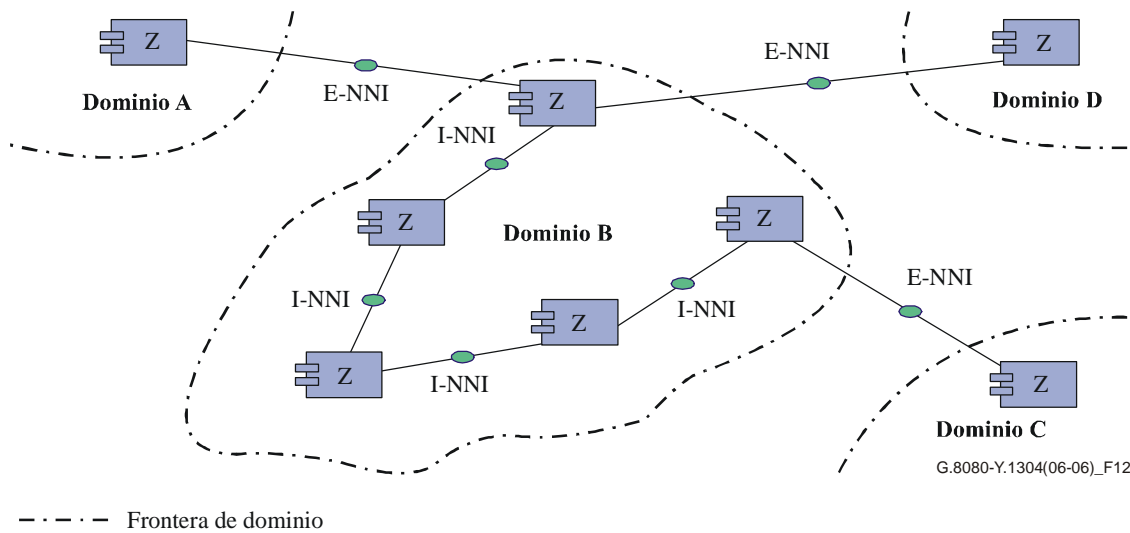
Un dominio de control consta de un conjunto de componentes del plano de control y proporciona una construcción arquitectural que encapsula y oculta el detalle de una implementación distribuida de un grupo determinado de componentes arquitecturales de uno o más tipos. Permite la descripción de un grupo de componentes distribuidos de manera que el grupo pueda ser representado por interfaces de distribución en una sola entidad, el dominio, que tiene características idénticas a las de las interfaces de distribución de componentes originales. La naturaleza de la información intercambiada entre dominios de control capta la semántica común de la información intercambiada entre interfaces de distribución de componentes, a la vez que permite diferentes representaciones dentro del dominio.

En general, un dominio de control se obtiene a partir de un tipo o tipos de componente determinados, que interactúan para una finalidad particular. Por ejemplo, los dominios (de control) de encaminamiento se derivan de los componentes de controlador de encaminamiento, mientras que un dominio de reencaminamiento se deriva de un conjunto de componentes de controlador de conexiones y de controlador de llamada de red que comparten la responsabilidad del reencaminamiento/restablecimiento de conexiones/llamadas que atraviesan ese dominio. En ambos ejemplos la operación que se efectúa, encaminamiento o reencaminamiento, está contenida enteramente dentro del dominio. En la presente Recomendación los dominios de control se describen en relación con componentes asociados con una red de capas.

Como un dominio se define desde el punto de vista de una finalidad, es evidente que los dominios definidos para una finalidad no tienen que coincidir con los dominios definidos para otra. Los dominios del mismo tipo están restringidos en cuanto a que pueden:

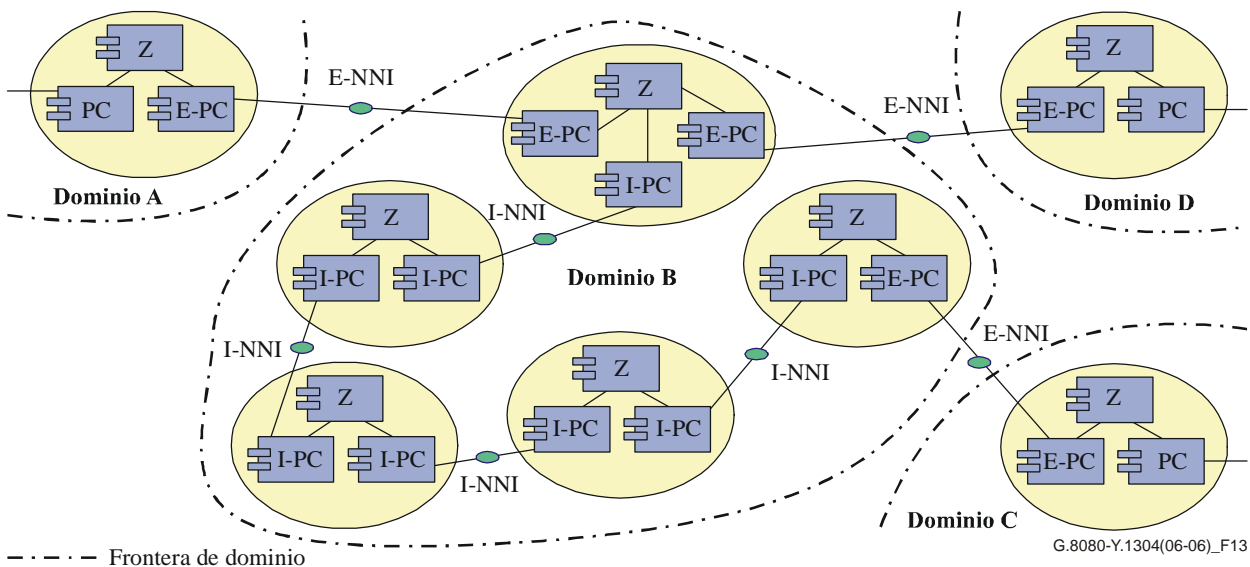
- contener totalmente otros dominios del mismo tipo, pero no superponerse;
- tener frontera entre sí;
- estar aislados entre sí.

Un ejemplo de las relaciones entre componentes, dominios y puntos de referencia se ilustra en la figura 12, que muestra un dominio B y su relación con los dominios A, C y D. Cada dominio se deriva de un tipo de componente Z. La estructura interna y las interacciones pueden ser diferentes en cada dominio, por ejemplo, pueden utilizar diferentes modelos de federación.



**Figura 12/G.8080/Y.1304 – Relación entre dominios, controladores de protocolo y puntos de referencia**

El mismo ejemplo se muestra en la figura 13 con las relaciones entre componentes, dominios e interfaces. Los componentes interactúan a través de sus controladores de protocolo, utilizando el protocolo I en I-PC y el protocolo E en E-PC. Es posible también que, por ejemplo, el protocolo utilizado interno de A sea diferente al usado en B y el protocolo utilizado entre B y C sea diferente al utilizado entre A y B. Las interfaces I-NNI están situadas entre controladores de protocolo dentro de dominios, mientras que las interfaces E-NNI están situadas en controladores de protocolo entre dominios.



**Figura 13/G.8080/Y.1304 – Relaciones entre dominios, controladores de protocolo e interfaces**

#### 6.4.1 Relación entre dominios de control y recursos del plano de control

Los componentes de un dominio pueden reflejar, dependiendo de su finalidad, los recursos de red de transporte subyacentes. Por ejemplo, un dominio de control de encaminamiento puede contener componentes que representan una o más áreas de encaminamiento en uno o más niveles de agregación, dependiendo del método/protocolo de encaminamiento utilizado a través del dominio.

#### **6.4.2 Relaciones entre dominios de control, interfaces y puntos de referencia**

Las interfaces I-NNI y E-NNI están siempre entre controladores de protocolo. Los protocolos que funcionan entre controladores de protocolo pueden utilizar o no enlaces SNPP en la red de transporte bajo control y, como tal, es incorrecto mostrar interfaces I-NNI y E-NNI en enlaces SNPP.

Los puntos de referencia I-NNI y E-NNI están entre componentes del mismo tipo, donde el tipo de componente no es un controlador de protocolo y representa flujos de mensajes de primitivas (véase la cláusula 7).

En un diagrama que muestra solamente dominios y las relaciones entre ellos (y que no muestra la estructura interna de los dominios) se supone que la transferencia de información se efectúa por un punto de referencia.

#### **6.5 Aspectos de múltiples capas**

La descripción del plano de control se puede dividir en los aspectos relacionados con una red de una sola capa, tales como encaminamiento, creación y supresión de conexiones, etc. y los relacionados con múltiples capas. La relación entre redes de las capas cliente y servidor es gestionada por medio de los ejecutores de terminación y adaptación (véase 7.3.7). La topología y conectividad de la capa de servidor subyacente no son explícitamente visibles a la capa de cliente, pues los aspectos de la capa de servidor son encapsulados y presentados a la red de capa de cliente. La capa de servidor se puede representar como un enlace SNPP de la capa de cliente, o como subredes de la capa de cliente interconectadas mediante enlaces SNPP. Esta abstracción de la topología de capa de servidor, hecha a efecto de calcular el trayecto en la capa de cliente, tiene propiedades similares a las de las relaciones de contención jerárquica descritas en 6.2.1. Por lo tanto, los resultados del cálculo de trayecto en la capa de cliente podrían no dar lugar al uso óptimo de los recursos de la capa de servidor. Si los recursos disponibles para la red de capa de cliente son insuficientes para soportar una petición de conexión, pueden proporcionarse recursos adicionales activando o creando nuevas conexiones en una o varias redes de capa de servidor. Las políticas del operador regirán la disponibilidad de los recursos subyacentes de la capa de servidor que pueden proporcionarse a la capa de cliente.

Cuando la capa de servidor se representa ante la capa de cliente como un enlace SNPP, esto se puede conseguir convirtiendo los SNP posibles en disponibles. Si la capa de servidor se representa como un conjunto de subredes y enlaces SNPP, el plano de control deberá solicitar directamente una nueva conexión de capa de servidor, dependiendo de las políticas del operador. En caso de que la capacidad de la conexión resultante de red de la capa de servidor sea mayor que la capacidad necesaria para soportar la conexión de capa de cliente, se creará un nuevo enlace SNPP como resultado indirecto de esta operación. En esta Recomendación no se trata el mecanismo para adicionar este nuevo enlace SNPP a la topología de la capa de cliente.

Por otra parte, la topología de capa de servidor podría no ser visible para la capa de cliente. En este caso, un proceso de planificación de la red podría tomar la decisión de adicionar nuevas conexiones de red de capa de servidor. La utilización de un sistema de planificación como mecanismo para recurrir a la configuración de la red de capa de servidor, a fin de suministrar recursos adicionales a la red de capa de cliente, podría dar como resultado una mejor utilización de los recursos de la capa de servidor. En la presente Recomendación no se trata detalladamente el proceso de planificación y su interacción con los planos de control del cliente y del servidor. La decisión de crear/suprimir las conexiones de la capa de servidor es una decisión de índole comercial que puede representarse en las políticas del operador.

Conforme se describió anteriormente, hay dos formas diferentes de representar los recursos de la capa de servidor en la capa de cliente. La representación que se use depende de si se han seleccionado previamente recursos de la capa de servidor para proporcionar conectividad a la capa

de cliente. El plano de control de una red de capa podría utilizar una sola o ambas formas en un momento dado. Quedan en estudio otras formas de representar los recursos de la capa de servidor.

### **6.5.1 Representación como conexiones de enlaces SNP**

Un proceso de planificación podría hacer que dos puntos de acceso de la capa de servidor se conecten, creando así un enlace SNPP de la capa de cliente que contenga varias conexiones de enlace SNP de la capa de cliente soportadas. Estas conexiones de enlace SNP podrían inicialmente ser activas o potenciales, ya que se podría o no adjudicar el recurso en cuestión para uso exclusivo de la capa de cliente (véase 6.1).

Este proceso podría aplicarse de forma iterativa en varias redes de capa de cliente/servidor. Por lo tanto, la conexión entre el par de puntos de acceso podría soportarse en conexiones de enlace potenciales. La conexión de los puntos de acceso en la capa de servidor sólo se activa cuando el plano de control recibe una petición de utilizar una de las conexiones potenciales de enlace de SNP de la capa de cliente. En ese momento se "suspende" la petición de la capa de cliente hasta que se establezcan las conexiones de la capa de servidor. Una vez se disponga de las conexiones de la capa de servidor, se activan las conexiones de enlace SNP de capa de cliente, lo que permite que se reanude la señalización de la capa de cliente. Si no puede establecerse una conexión en la capa de servidor, no se pueden activar las conexiones de enlace SNP de capa de cliente, lo que hace fallar el intento de conexión de la capa de cliente por falta de recursos.

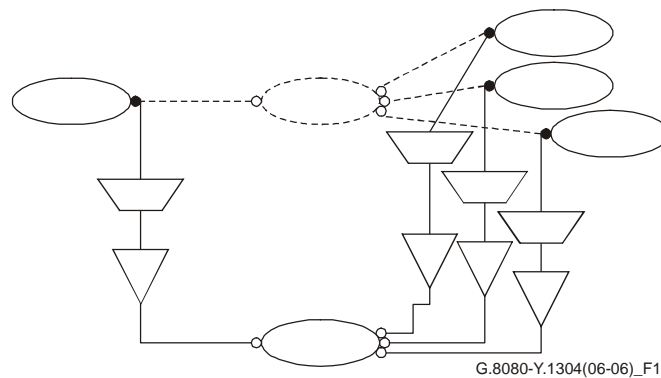
Cuando se suprime la conexión de enlace SNP, se liberan los recursos subyacentes que soportaban la conexión, y éstos pueden regresar al estado potencial, si así lo permiten las políticas. Cuando todas las conexiones de enlace SNP soportadas por un camino de servidor regresan al estado potencial, se puede cambiar el camino de servidor a potencial, si así lo permiten las políticas.

Cabe señalar que el enlace SNPP que contiene estas conexiones de enlace SNP puede representarse utilizando los componentes y estados existentes, conforme se describe en 6.1.

### **6.5.2 Representación como un conjunto de subredes y enlaces SNPP**

Dentro del proceso de planificación también se podría permitir al plano de control de la capa de cliente mayor flexibilidad para elegir los recursos de la capa de servidor necesarios para satisfacer una petición de conexión. Con este fin, algunos de los recursos de la capa de servidor se representan ante la capa de cliente en la forma de subredes y enlaces SNPP con los componentes apropiados del plano de control. Esta forma de representación es posible si la capa de servidor proporciona la flexibilidad que permita que las subredes de la capa de cliente se interconecten. En la figura 14 se ilustra la flexibilidad de la capa de servidor y la correspondiente flexibilidad de la capa de cliente. Con esto se permite que el controlador de encaminamiento sepa que se puede tener acceso a un conjunto de SNP de la capa de cliente a través de una capa de servidor común. Es decir que si en la figura 14 no existiera una representación de la capa de servidor, no se podrían calcular los caminos entre todos los SNP de la capa de cliente.

Las funciones de adaptación y terminación utilizadas para pasar de la capa de cliente a la capa de servidor se representan como enlaces SNPP en la capa de cliente. En esta figura se usan elementos punteados para distinguir esta forma de representar los recursos de la capa de servidor ante la capa de cliente de los demás recursos de la capa de cliente. Adicionalmente, los SNP de la capa de cliente y de la capa de servidor se representan como puntos rellenos y puntos vacíos, respectivamente. Sin embargo, desde el punto de vista del controlador de encaminamiento de la capa de cliente, no hay ninguna diferencia entre estos elementos representados y los otros elementos de la capa de cliente.



**Figura 14/G.8080/Y.1304 – Relación entre los elementos arquitectónicos del cliente y del servidor**

Tal como ocurre en la representación del enlace SNPP, las conexiones de enlace SNP que conectan la subred de la capa de cliente con la capa de servidor son potenciales, ya que los recursos de la capa de servidor no se adjudicaron para uso exclusivo de la capa de cliente. Cuando se recibe una petición de conexión que utiliza un recurso potencial, se calcula un camino a través de la capa de servidor a fin de identificar los recursos específicos que se han de usar. Como resultado de la identificación de estos recursos, se crean conexiones de enlace SNP de la capa de cliente, y continúa el procesamiento como anteriormente.

## 6.6 Soporte de cliente entre capas

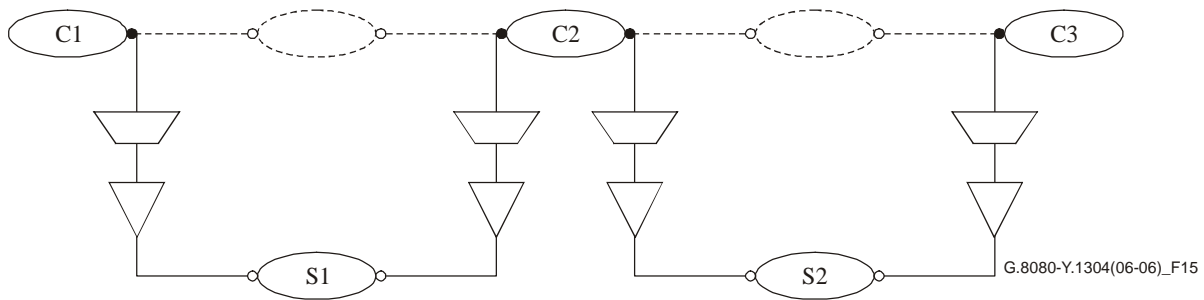
En las redes de transporte, los elementos de red pueden soportar más de una capa única. Por ejemplo, en el borde de una red de transporte con múltiples capas, los elementos de red pueden soportar redes de la capa de cliente que se soportan directamente en el núcleo de una red de transporte de múltiples capas. Por ejemplo, el elemento de red en la frontera podría soportar la adaptación de servicio a un VC de orden menor, mientras que los elementos de red del núcleo pueden proporcionar flexibilidad únicamente en la capa VC del orden superior. El elemento de red puede también adaptar un servicio Ethernet a VC de órdenes superiores. Un problema general es cómo transferir la información característica del cliente (CI, *characteristic information*) cuando no exista una red de capa de cliente continua/conectada entre dos contenedores de grupo de acceso (AGC) de cliente.

Para este problema hay dos soluciones. O bien, se puede crear la topología de la capa cliente a partir de las conexiones de la capa de servidor, conforme a lo descrito en 6.5, o puede adaptarse el CI de cliente, posiblemente varias veces, a las conexiones de la capa de servidor. Esto no sería visible para el controlador de encaminamiento de cliente.

Para poder aplicar las funciones de ASON a la segunda solución, se emplean interfaces entre los controladores de llamada de red (NCC, *network call controllers*) (véase 7.3.5.1) de distintas redes de capa. Esta interfaz entre capas posibilita una asociación entre llamadas en una relación de capas de cliente/servidor. Esta asociación puede recurrir a representar un conjunto de adaptaciones "apiladas". Es decir, los NCC recurren a las capas G.805. Los NCC de distintas capas pueden ejemplificarse de distinta manera entre sí. Por ejemplo, un NCC podría ser distribuido en una capa de cliente y centralizado en una capa de servidor. Un controlador de conexión (CC) de capa de servidor crea la(s) conexión(es). El CI de cliente se hace corresponder a la conexión de la capa de servidor y la relación NCC de cliente/servidor se encarga de mantener esta asociación. En esta situación, como resultado de la conexión de la capa de servidor y la correspondencia de la CI se crea una conexión de enlace de capa de cliente, aunque el CC de la capa de cliente no participa en esta actividad sino que vuelve a subir y crea una conexión de enlace en cada una de las capas de cliente afectadas.

El apéndice IV ilustra esta capacidad con un ejemplo.

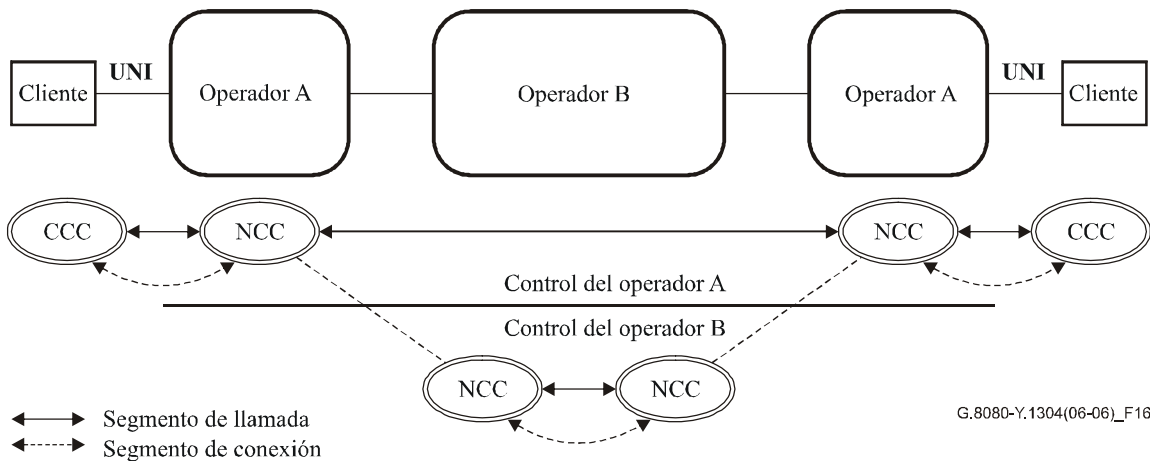
La relación NCC entre capas puede tener lugar en puntos diferentes a aquellos en que los contenedores de grupos de acceso se conectan con la red de capa de cliente. En la figura 14, las llamadas cruzan la subred de cliente antes de que las soporte una subred de capa de servidor. En la figura 15, las conexiones de una subred de la capa de cliente que no sea contigua a subredes de capa de cliente al ingreso o al egreso también pueden soportar las llamadas. En esta figura aparecen relaciones NCC entre la subred de cliente C2 y las subredes de servidor S1 y S2.



**Figura 15/G.8080/Y.1304 – Subredes de capa de cliente no contiguas**

### 6.7 Llamadas que se soportan en llamadas de la misma capa

Un segmento de llamada se puede soportar en una llamada diferente de la misma capa, aunque no a través de una E-NNI, de forma similar a aquella en que se disponen los NCC en una relación entre capas. En esta disposición, se soporta un segmento de llamada de NCC a NCC mediante una llamada completa con controladores de llamada de parte llamada/llamante. Esto se ilustra en la figura 16, en un escenario comercial de un operador de operadores. En este caso, las llamadas entre dos clientes relacionados con el operador A se soportan en dos subredes pertenecientes al operador A. Entre esas dos subredes, la llamada se soporta en una SPC interna del operador B. La conexión que devuelve el operador B se enlaza con las conexiones establecidas en las subredes del operador A.



**Figura 16/G.8080/Y.1304 – Llamadas que se soportan en llamadas de la misma capa**

## 7 Arquitectura del plano de control

Esta cláusula describe una arquitectura de referencia para el plano de control que satisface los requisitos de la presente Recomendación, identificando sus componentes funcionales esenciales y la forma en que interactúan. Esta arquitectura de referencia flexible tiene por objeto permitir a los operadores soportar sus prácticas internas de comercio y de gestión, así como facturar la utilización del servicio. La arquitectura del plano de control deberá tener las siguientes características:

- Soporte de diversas infraestructuras de transporte, tales como la red de transporte SONET/SDH, definida en la Rec. UIT-T G.803, y la red óptica de transporte (OTN, *optical transport network*), definida en la Rec. UIT-T G.872.
- Ser aplicable cualquiera que sea la opción de protocolo de control que se elija (es decir, emplear un enfoque neutro de protocolo que sea independiente de los protocolos de control de conexión utilizados).
- Ser aplicable cualquiera que sea la forma en que el plano de control se haya subdividido en dominios y áreas de encaminamiento, y la forma en que los recursos de transporte se hayan distribuido entre las subredes.
- Ser aplicable cualquiera que sea la implementación del control de conexión, que puede ir desde una arquitectura de control completamente distribuida hasta una arquitectura de control centralizada.

Esta arquitectura de referencia describe:

- los componentes funcionales del plano de control, incluidas las interfaces abstractas y las primitivas;
- las interacciones entre los componentes del controlador de llamada;
- las interacciones entre componentes durante el establecimiento de la conexión;
- el componente funcional que transforma las interfaces de componentes abstractos en protocolos para interfaces externas.

Los componentes especiales se definen en esta Recomendación y se proporcionan para permitir la flexibilidad de la implementación. Estos componentes son los controladores de protocolo y los controladores de puerto. Los detalles de las interfaces de éstos y otros componentes se describen en otras recomendaciones específicas de la tecnología.

Los controladores de protocolo se proporcionan para tomar la interfaz de primitivas suministrada por uno o más componentes arquitecturales y multiplexar estas interfaces en un solo caso de un protocolo. Esto se describe en 7.4 y se ilustra en la figura 37. De esta manera, un controlador de protocolo absorbe las variaciones entre distintas opciones de protocolo y la arquitectura permanece invariable. Uno o más controladores de protocolo son responsables de gestionar los flujos de información a través de un punto de referencia.

Los controladores de puerto se proporcionan para aplicar reglas a interfaces de sistemas. Su finalidad es proporcionar un entorno seguro para que los componentes arquitecturales puedan ser ejecutados en la misma, aislando así los componentes arquitecturales de las consideraciones relativas a la seguridad. En particular, aíslan la arquitectura con respecto a las decisiones de distribución adoptadas que entrañan aspectos de seguridad. Esto se describe en 7.2.1 y en la figura 18.

### 7.1 Notación

En esta cláusula se considera la notación arquitectural de componentes sobre la base de algunos bloques constructivos tomados del vocabulario del lenguaje de modelado unificado, (UML).

**Interfaz:** Una interfaz soporta una colección de operaciones que especifican un servicio de un componente, y es especificada independientemente de los componentes que utilicen o proporcionan dicho servicio. Las operaciones especifican la información que pasa hacia adentro o hacia afuera junto con toda restricción aplicable. Las definiciones de interfaz se presentan en forma de cuadro, por el estilo del cuadro 1. Cada interfaz tiene un nombre de interfaz que identifica el rol. Las interfaces de entrada representan servicios proporcionados por el componente; se requieren los parámetros de entrada básicos para el rol específico y los parámetros de retorno básicos son un resultado de la acción sobre los parámetros de entrada. Las interfaces de salida representan servicios utilizados por el componente; los parámetros de salida básicos definen la información suministrada; los parámetros de retorno básicos (si están identificados) son los que deben aparecer en respuesta a los parámetros de salida. Las interfaces de notificación representan acciones de salida no solicitadas por el componente y se representan por una interfaz de salida sin parámetros de retorno. Estos tres tipos de interfaz se describen separadamente en especificaciones de interfaz.

**Cuadro 1/G.8080/Y.1304 – Formato del cuadro de las descripciones de interfaz genéricas**

<b>Interfaz de entrada</b>	<b>Parámetros de entrada básicos</b>	<b>Parámetros de retorno básicos</b>
Nombre de la interfaz	Parámetros de entrada	Parámetros devueltos

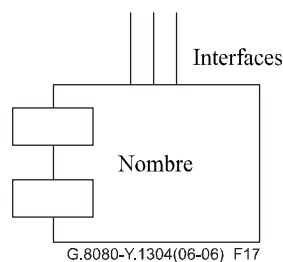
  

<b>Interfaz de salida</b>	<b>Parámetros de salida básicos</b>	<b>Parámetros de retorno básicos</b>
Nombre de la interfaz	Parámetros de salida	Parámetros devueltos

Se supone que las semánticas de transacción asociadas con una transacción dada son tratadas transparentemente, y que no es necesario mencionar explícitamente parámetros separados para este propósito en la descripción de interfaz.

**Rol:** Un rol es el comportamiento de una entidad cuando participa en un contexto particular. Los roles permiten que entidades diferentes participen en tiempos diferentes, y se designan anotando una relación con el nombre de una interfaz.

**Componente:** En esta Recomendación se utilizan componentes para representar entidades abstractas, más bien que ejemplares de código de implementación. Los componentes se utilizan para construir escenarios con el fin de explicar el funcionamiento de la arquitectura. Un componente se representa como un rectángulo con símbolos sobresalientes. Se muestra en la figura 17.



**Figura 17/G.8080/Y.1304 – Representación de un componente**

En general cada componente tiene un conjunto de interfaces especiales que permiten la supervisión del funcionamiento del componente, y dinámicamente establecer las políticas e influir sobre el comportamiento interno. Estas interfaces no son obligatorias, y se proporcionan en componentes específicos solamente cuando sea necesario. Cuando sea conveniente, la utilización de la interfaz de supervisión se explica en las descripciones de componentes individuales. No se supone que los componentes estén distribuidos estáticamente.



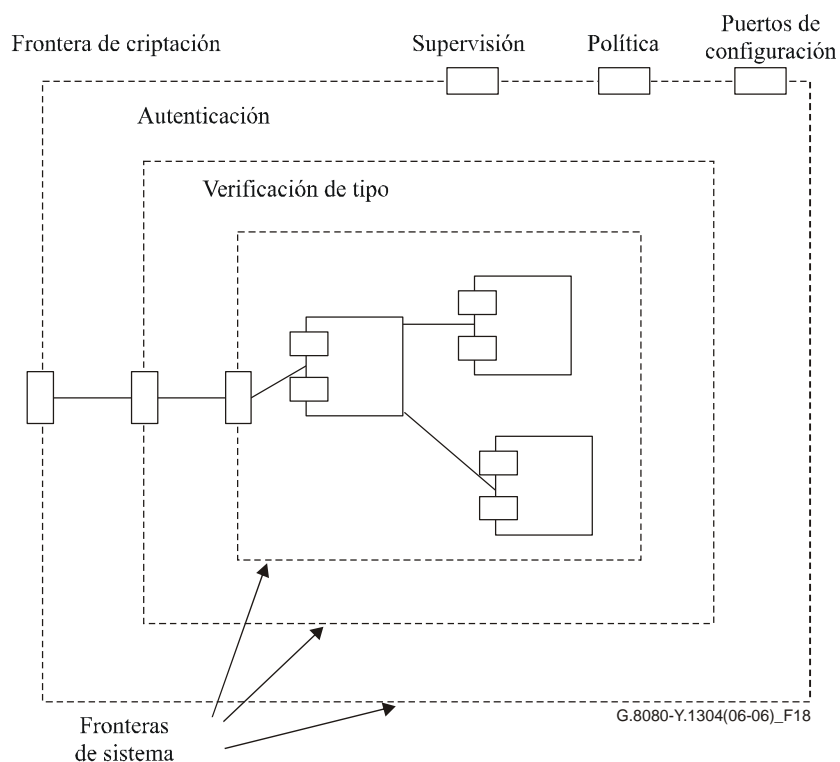
Cuando se describen interfaces en componentes, sólo se especifican los tipos de interfaz que son diferentes. Todos los componentes tienen la propiedad de soportar múltiples llamantes y múltiples proveedores, y la resolución de contiendas entre peticiones concurrentes no se menciona explícitamente.

Como los componentes se utilizan de una manera abstracta, esta especificación se puede ampliar mediante las técnicas de subclasificación y composición de componentes.

## 7.2 Política y federaciones

### 7.2.1 Modelo general de política

A efectos de este modelo de política, los sistemas representan colecciones de componentes, y una frontera de sistema proporciona un punto en que se puede aplicar una política. Una política se define como el conjunto de reglas aplicadas a interfaces en la frontera del sistema, e implementadas por los componentes controlador de puerto. Los puertos de política son empleados para simplificar la modelización de las políticas que son aplicadas en múltiples puertos. Las fronteras de sistema están anidadas para permitir un modelado correcto de políticas compartidas aplicadas con cualquier alcance (todo el sistema, cualquier conjunto de componentes, componentes individuales, etc.). Obsérvese que el orden de aplicación de las políticas es el especificado por el anidamiento.



**Figura 18/G.8080/Y.1304 – Ejemplo de fronteras de sistema relacionado con el control de política**

En la figura 18, las líneas de trazo discontinuo representan fronteras de sistema mientras que los rectángulos de trazo continuo en la frontera, llamados puertos, representan componentes controlador de puerto.

Los puertos de supervisión, política y configuración pueden estar disponibles en todos los sistemas (y en todos los componentes) sin que sea necesaria una especificación arquitectural adicional. El puerto de supervisión permite que la información de gestión relacionada con degradaciones de la calidad de funcionamiento, eventos perturbadores, fallos, etc., pase a través de la frontera, para

componentes, sometida a las constricciones impuestas por la política. El puerto de política permite el intercambio de información de política relacionada con los componentes. El puerto de configuración permite el intercambio de información de configuración, aprovisionamiento y administración, relacionada con los componentes (sometida a las constricciones impuestas por la política) que pueda ajustar dinámicamente el comportamiento interno del sistema.

En la figura 18 se muestra un ejemplo de la manera en que la criptación, autenticación y verificación de tipo se pueden implementar como un conjunto de tres controladores de puerto anidados, en el que el orden de aplicación de las políticas sigue el orden de anidamiento. Los componentes en el interior de una frontera de autenticación no especifican requisitos de criptación ni de autenticación, puesto que éstas son propiedades del entorno del componente. Se definen controladores de puerto para cada aspecto independiente de la política de puerto, y se obtiene una política combinada mediante una composición de controladores de puerto. Se permite así la creación de componentes reutilizables, que se distinguen por un prefijo descriptivo. Las violaciones de la política se informan a través del puerto de supervisión.

El puerto de política puede visualizarse como un filtro de mensajes entrantes, que rechaza los mensajes que hayan infringido la política. Las políticas se pueden cambiar dinámicamente a través del puerto de política del sistema, asegurando así que se puedan describir los cambios de comportamiento dinámicos.

Con frecuencia se discute cómo se puede aplicar una política a un punto de referencia; sin embargo, una política sólo puede aplicarse a interfaces individuales que cruzan el punto de referencia. Más adelante, en la cláusula 7.4, controladores de protocolo, se describe un método para combinar varias interfaces en una sola interfaz de implementación.

Otros aspectos de política se relacionan con el comportamiento variable de los componentes (tales como calendarios, derechos de acceso, etc.), y estos aspectos son especificados e implementados por los componentes. El comportamiento de un componente se puede también cambiar dinámicamente, y la habilidad de hacer esto puede ser controlada mediante una política. Esto permite determinar qué aspectos del comportamiento del sistema son especificados y en qué lugar.

La política, como otros aspectos del sistema, puede estar distribuida. Un ejemplo de un modelo adecuado de distribución podría ser el modelo de protocolo de servicio común de política abierta (COPS, *common open policy service*) de RFC 2753. El punto de imposición de la política (PEP, *policy enforcement point*) (el punto en que se hacen cumplir las decisiones de política) de dicho modelo corresponde al puerto en este modelo. El punto de decisión de la política (PDP, *policy decision point*) es el punto en que se toman decisiones de política. Esto puede realizarse dentro del puerto, aunque podría estar distribuido a un sistema diferente. Esta decisión de distribución depende de muchos factores que a su vez dependen de la política existente. Por ejemplo, el PDP podría verse obligado, por razones de desempeño, a estar dentro del puerto (criptación), mientras que por razones de seguridad podría verse obligado a estar en cualquier otro lugar (consulta de contraseña).

Se requiere cooperación cuando el PEP y el PDP no estén coubicados.

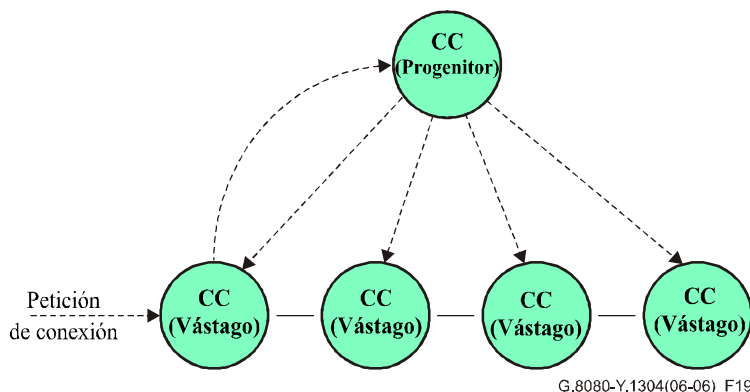
## **7.2.2 Modelo general de federación**

Se requiere la creación, mantenimiento y supresión de conexiones a través de múltiples dominios. Esto se alcanza mediante la cooperación entre controladores en diferentes dominios. A los efectos de esta Recomendación, se considera que una federación es una comunidad de dominios que cooperan para fines de gestión de conexión y se ilustra mediante la cooperación entre controladores de conexión (descritos en 7.3.1).

Existen dos tipos de federación, a saber:

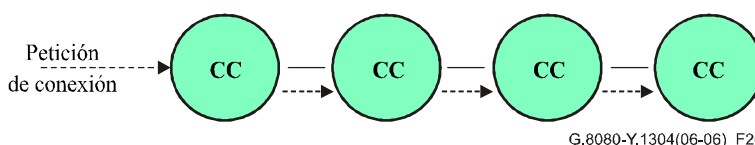
- Modelo de federación conjunta.
- Modelo cooperativo.

En el caso de la federación conjunta, un controlador de conexión, el controlador de conexión progenitor, tiene autoridad sobre los controladores de conexión que residen en diferentes dominios. Si se necesita que una conexión atraviese múltiples dominios, el controlador de conexión de más alto nivel (el progenitor) actúa como el coordinador. Este controlador de conexión conoce todos los controladores de conexión de más alto nivel en cada dominio. El controlador de conexión progenitor reparte la responsabilidad de la conexión de red entre los controladores de conexión del nivel siguiente, y cada uno de éstos es responsable de su parte de la conexión. Esto se ilustra en la figura 19. Este modelo es recursivo, siendo un controlador de conexión progenitor en un nivel un vástago de un progenitor en un nivel superior.



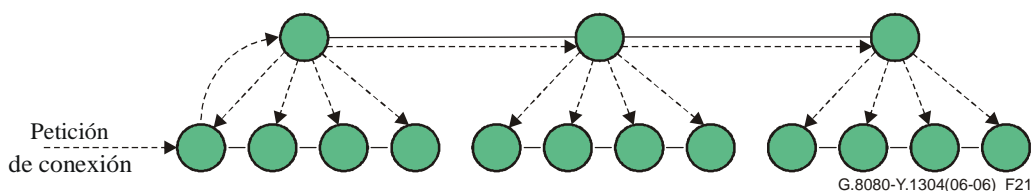
**Figura 19/G.8080/Y.1304 – Modelo de federación conjunta**

En el modelo cooperativo no existe el concepto de un controlador de conexión progenitor. En su lugar, cuando se hace una petición de conexión, el controlador de conexión de origen contactará voluntariamente cada uno de los controladores de conexión asociados con dominios y no existe coordinación global. El método más sencillo de obtener esto es disponiendo que el controlador de conexión de origen contacte el controlador de conexión siguiente en la cadena. Esto se ilustra en la figura 20, donde cada controlador de conexión calcula qué parte de la conexión puede proporcionar y cuál será el siguiente controlador de conexión. Este proceso se repite hasta que se obtiene la conexión.



**Figura 20/G.8080/Y.1304 – Modelo de federación cooperativa**

La federación entre dominios administrativos se obtiene mediante el modelo cooperativo. En este caso se espera que todos los dominios administrativos tengan la capacidad para federarse con otros dominios administrativos. Los controladores de conexión progenitores dentro de un dominio administrativo pueden federarse con otros controladores de conexión progenitores en otros dominios administrativos gracias al modelo cooperativo. Se puede también subdividir un dominio administrativo y la elección del modelo de federación empleado entre dominios, dentro del dominio administrativo puede ser independiente de lo que suceda en otro dominio administrativo. Por tanto, es posible combinar ambos modelos de federación para construir grandes redes, como se muestra en la figura 21. El principio descrito anteriormente puede también aplicarse a federaciones de controladores de llamada.



**Figura 21/G.8080/Y.1304 – Modelo de federación combinada**

### 7.3 Componentes arquitecturales

En esta cláusula se describen los componentes de la arquitectura del plano de control. Estos componentes se pueden combinar de diversas maneras, según la funcionalidad requerida. En el apéndice V se presentan algunos ejemplos de las interacciones de estos componentes, para su uso en el establecimiento de las conexiones. Se presenta cada componente mediante una breve descripción de su función primaria en esta arquitectura de referencia. A continuación, se presentan las interfaces de componente, y se da una descripción más detallada de funcionamiento.

El controlador de conexión, el controlador de encaminamiento, el controlador de llamada de la parte llamante/llamada y el controlador de llamada de red son componentes del plano de control. Estos componentes pueden ser públicos, en cuyo caso utilizan sólo SNPP públicos, o privados, en cuyo caso utilizan los SNPP asociados a una determinada RPV. El contexto RPV de un componente de plano de control es proporcionado por el controlador de protocolo asociado a ese componente.

#### 7.3.1 Componente controlador de conexión (CC)

El controlador de conexión se encarga de la coordinación entre el gestor de recursos de enlace, el controlador de encaminamiento, así como del controlador de conexión par y del controlador de conexión subordinado, a los efectos de gestión y supervisión de los establecimientos de conexión, liberaciones de conexión y la modificación de los parámetros de conexión en el caso de conexiones existentes. Este componente presta servicio a una subred individual, y proporciona las interfaces abstractas a otros componentes del plano de control indicados en el cuadro 2. El componente controlador de conexión se ilustra en la figura 22.

NOTA – El parámetro ruta no es aplicable a la interfaz CC en el punto de referencia UNI.

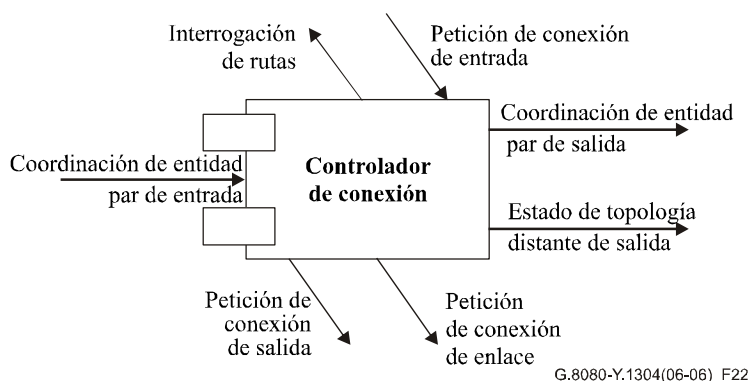
Además, el componente CC proporciona una interfaz de controlador de conexión (CCI, *connection controller interface*). Ésta es una interfaz entre una subred en el plano de transporte y el plano de control. Los componentes de control la utilizan para dirigir la creación, modificación, y supresión de SNC. No se aplican políticas a la CCI.

**Cuadro 2/G.8080/Y.1304 – Interfaces del componente controlador de conexión**

Interfaz de entrada	Parámetros de entrada básicos	Parámetros de retorno básicos
Petición de conexión de entrada	Un par de nombres de SNP local y opcionalmente una ruta	Una conexión de subred
Coordinación de entidad par de entrada	1) un par de nombres de SNP; o 2) SNP y SNPP; o 3) un par de SNPP; o 4) ruta.	Señal de confirmación

**Cuadro 2/G.8080/Y.1304 – Interfaces del componente controlador de conexión**

Interfaz de salida	Parámetros de salida básicos	Parámetros de retorno básicos
Interrogación de rutas	Fragmento de ruta no resuelto	Ruta
Petición de conexión de enlace	–	Una conexión de enlace (un par SNP)
Petición de conexión de salida	Un par de nombres de SNP local	Una conexión de subred
Coordinación de entidad par de salida	1) un par de nombres de SNP; o 2) SNP y SNPP; o 3) un par de SNPP	Señal de confirmación
Estado de topología distante de salida	Información de topología (enlace y/o subred) incluida la disponibilidad de recursos	–



**Figura 22/G.8080/Y.1304 – Componente controlador de conexión**

**Estado de la topología distante de salida:** Esta interfaz se utiliza para presentar la información del estado de la topología adquirida por el controlador de conexión. Esta indicación de estado incluirá la posibilidad de señalización a través de un enlace.

### Operación de establecimiento de conexión

Se realiza un establecimiento de conexión en respuesta sea a una petición de conexión, desde un controlador de conexión circundante, sea desde un controlador de conexión par. En el caso de encaminamiento jerárquico, donde el CC superior (es decir, progenitor) selecciona los SNP fuente y destino, se utiliza la interfaz de petición de conexión de entrada/salida. En todos los demás casos se utilizan las interfaces de coordinación de entidad par de entrada/salida. El funcionamiento del componente es igual en ambos casos.

La primera porción no resuelta de la ruta se resuelve a través de la interfaz de interrogación del cuadro de rutas, en un conjunto de enlaces que habrán de ser atravesados, y este nuevo conjunto de enlaces se añade al conjunto. El controlador de conexión examina el nuevo conjunto de enlaces para determinar cuáles de ellos están disponibles para asignación a la conexión de enlace. Se obtienen conexiones de enlace y sus enlaces se suprimen del conjunto de enlaces. Seguidamente, se solicitan correspondientes conexiones de subred de controladores de conexión subordinados (es decir, vástagos) a través de la interfaz de petición de conexión de salida. Todo componente de ruta no asignado se pasa al siguiente controlador de conexión par en sentido hacia el destino. La secuencia

real de operaciones depende de muchos factores, incluida la cantidad de información de encaminamiento disponible y el acceso a determinados gestores de recursos de enlace, pero el funcionamiento del controlador de conexión es invariante. La liberación de conexión es una operación análoga al establecimiento de conexión, excepto que las operaciones se invierten.

### 7.3.2 Componente controlador de encaminamiento (RC, *routing controller*)

El rol del controlador de encaminamiento es:

- responder a las peticiones, de información de trayecto (ruta) necesaria para establecer las conexiones. Esta información puede ir desde detalles del camino extremo a extremo hasta el siguiente salto. Dos o más RC cooperantes podrían calcular la ruta;
- responder a las peticiones de información de topología (SNP y sus abstracciones) a efectos de gestión de red.

Conforme se indicó en 7.1, el componente controlador de encaminamiento es una entidad abstracta que proporciona la función de encaminamiento. Puede estar compuesto por una unidad única o por un conjunto distribuido de unidades que conforman una federación cooperativa.

La información contenida en el controlador de ruta lo habilita para proporcionar rutas dentro del dominio de su responsabilidad. Esta información incluye tanto información de topología (SNPP, conexiones de enlace SNP), como direcciones de SNP (direcciones de red) que corresponden a las direcciones de sistema de extremo, todas en una capa determinada. Se puede mantener también información de direccionamiento acerca de otras subredes en la misma capa (subredes pares). Puede también mantener el conocimiento del estado de los SNP para permitir un encaminamiento basado en constricciones. De acuerdo con esto, se puede determinar una ruta posible entre dos o más (conjuntos de) SNP teniendo en cuenta algunas constricciones de encaminamiento. Existen niveles variantes de detalle de encaminamiento que abarcan lo siguiente:

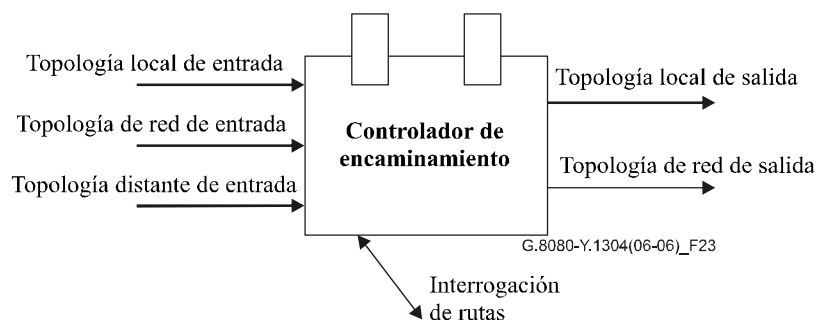
- Alcanzabilidad (por ejemplo, vista del vector distancia; se mantienen las direcciones y los saltos siguientes).
- Vista topológica (por ejemplo, estado del enlace; se mantienen las direcciones y la posición topológica).

El controlador de encaminamiento tiene las interfaces proporcionadas en el cuadro 3 e ilustradas en la figura 23.

**Cuadro 3/G.8080/Y.1304 – Interfaces de controlador de encaminamiento**

<b>Interfaz de entrada</b>	<b>Parámetros de entrada básicos</b>	<b>Parámetros de retorno básicos</b>
Interrogación de rutas	Elemento de ruta no resuelto	Ruta
Topología local de entrada	Actualización de topología local	–
Topología de red de entrada	Actualización de topología de red	–
Topología distante de entrada	Información de topología (enlace y/o subred) incluida la disponibilidad de recursos	

<b>Interfaz de salida</b>	<b>Parámetros de salida básicos</b>	<b>Parámetros de retorno básicos</b>
Interrogación de ruta	Elemento de ruta no resuelto	Ruta
Topología local de salida	Actualización de topología local	–
Topología de red de salida	Actualización de topología de red	–



**Figura 23/G.8080/Y.1304 – Componente controlador de encaminamiento**

**Interfaz de interrogación de rutas:** Esta interfaz acepta un elemento de ruta no resuelto y retorna una ruta. Un RC puede interrogar a otro RC (o a varios RC) en áreas de encaminamiento de progenitor o de vástago. Son ejemplos de consultas:

- 1) Retornar un SNPP de egreso en esta subred que se encuentra en un trayecto hacia un determinado SNPP de destino.
- 2) Retornar una secuencia de subredes que forman un trayecto entre un determinado par de SNPP de fuente/destino.
- 3) Retornar una secuencia de subredes que forman un trayecto entre dos conjuntos de SNPP.
- 4) Retornar una secuencia de SNPP que forman un trayecto entre un determinado par de SNPP de fuente/destino.
- 5) Retornar una secuencia de SNPP que forman un trayecto entre un determinado par de SNPP de fuente/destino e incluye uno o más SNPP específicos.
- 6) Retornar una secuencia de SNPP que forman un trayecto entre un determinado par de SNPP de fuente/destino que es diferente del trayecto dado.

Las SNPP retornadas deben ser todas públicas o todas asociadas con la misma RPV.

**Interfaz de topología local:** Se utiliza para configurar los cuadros de encaminamiento con información de topología local e información de actualización de topología local. Ésta es la información de topología que está dentro del dominio de responsabilidad del controlador de encaminamiento. La información de topología local se identifica como pública o asociada a una determinada RPV.

**Interfaz de topología de red:** Se utiliza para configurar los cuadros de encaminamiento con información de topología de red e información de actualización de topología de red. Ésta corresponde a la información de topología reducida (por ejemplo, topología resumida) que está fuera del dominio de responsabilidad del controlador de encaminamiento.

La información de topología de red se identifica como pública o asociada a una determinada RPV.

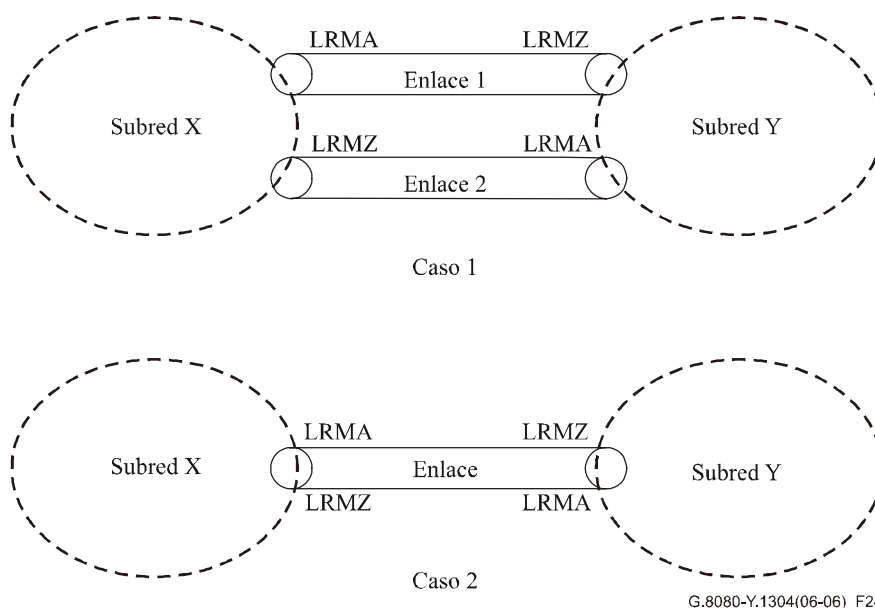
**Topología distante de entrada:** Esta interfaz se utiliza para aceptar información de topología de un controlador de conexión.

### 7.3.3 Componente gestor de recursos de enlace (LRMA y LRMZ)

Los componentes gestor de recursos de enlace (LRM, *link resource manager*) son responsables de la gestión de un enlace SNPP, incluidas la asignación y desasignación de conexiones de enlace SNP, que proporcionan información de topología y estado. Como un enlace SNPP puede ser público o privado, un LRM también puede ser público o asociado exactamente a una RPV.

Se utilizan dos componentes LRM – el LRMA y el LRMZ. Un enlace SNPP es gestionado por un par de componentes LRMA y LRMZ; cada uno de ellos gestiona un extremo del enlace. Las peticiones de asignación de conexiones de enlace SNP se dirigen solamente al LRMA.

En la figura 24 se muestran los dos casos para un enlace SNPP.



**Figura 24/G.8080/Y.1304 – Casos de enlace SNPP**

En el caso 1, el enlace 1 está dedicado al establecimiento de la conexión que se origina en la subred X. Las peticiones de conexiones de enlace SNP provenientes de la subred X se dirigen al LRMA adyacente para el enlace 1. Este LRMA puede asignar la conexión de enlace SNP sin negociación con el LRMZ para el enlace 1. De igual manera, el enlace 2 está dedicado a las peticiones de establecimiento de conexión que se originan en la subred Y. Las peticiones de conexiones de enlace SNP provenientes de la subred Y se dirigen al LRMA adyacente para el enlace 2. Este LRMA puede asignar la conexión de enlace SNP sin negociación con el LRMZ para el enlace 2.

En el caso 2, el enlace se comparte entre las subredes X e Y para establecimiento de conexión. Las peticiones de conexiones de enlace SNP provenientes de la subred X son dirigidas al LRMA adyacente; puesto que un componente LRMA en el extremo lejano del enlace puede también asignar conexiones de enlace SNP, el LRMA podría necesitar negociar una asignación con el LRMZ en el extremo lejano. Se requiere un proceso similar para las peticiones provenientes de la subred Y a su LRMA adyacente.

### 7.3.3.1 LRMA

El LRMA es responsable de la gestión del extremo A del enlace SNPP, incluidas la asignación y desasignación de conexiones de enlace, proporcionando información de topología y estado.

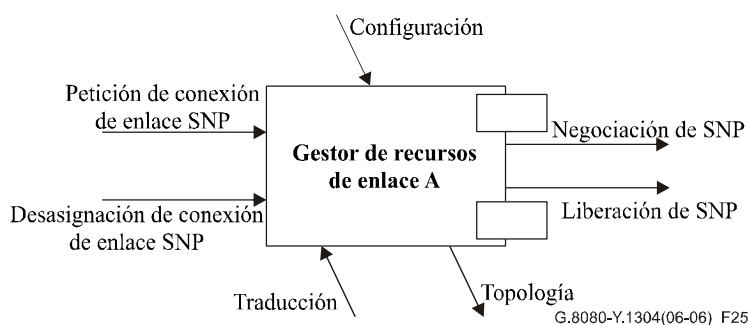
Las interfaces de componente LRMA se presentan en el cuadro 4 y se ilustran en la figura 25.



**Cuadro 4/G.8080/Y.1304 – Interfaces de componente LRMA**

<b>Interfaz de entrada</b>	<b>Parámetros de entrada básicos</b>	<b>Parámetros de retorno básicos</b>
Petición de conexión de enlace SNP	Id de petición Id de SNP (facultativo)	Id de petición Id de SNP par o negado
Desasignación de conexión de enlace SNP	Id de SNP	Confirmado o denegado
Configuración	Información de enlace	–
Traducción	Id local	Id de interfaz

<b>Interfaz de salida</b>	<b>Parámetros de salida básicos</b>	<b>Parámetros de retorno básicos</b>
Negociación de SNP (sólo en el caso 2)	Id de petición Lista de Id de SNP	Id de petición Id de SNP
Liberación de SNP (sólo en el caso 2)	Id de SNP	Confirmación
Topología	Información de enlace	–



**Figura 25/G.8080/Y.1304 – Componente gestor de recursos de enlace A**

- **Funciones**

- *Asignación de conexión de enlace*

Cuando se recibe una petición de asignación de conexión de enlace, se invoca la admisión de conexión para determinar si existen recursos libres suficientes para permitir una nueva conexión. Las decisiones sobre la admisión de conexión también pueden tomarse basándose en prioridades u otros aspectos de política. Las políticas de admisión de conexión están fuera del ámbito de la normalización.

Si los recursos son insuficientes se rechaza la petición.

Si hay recursos suficientes disponibles se permite proceder a la petición de conexión como se describe en los casos siguientes.

- Caso 1: Dado que las conexiones de enlace SNP se asignan sólo desde un extremo del enlace SNPP, el LRMA puede seleccionar la conexión de enlace SNP sin interacción con el LRMZ en el extremo lejano del enlace.
- Caso 2: Dado que las conexiones de enlace SNP pueden ser utilizadas por el LRMA en cualquier extremo del enlace SNPP, el LRMA pasa al LRMZ una lista de identificadores de SNP utilizables. El LRMZ (en cooperación con su LRMA local) selecciona uno de los SNP y retorna el identificador al LRMA de origen.

– *Desasignación de una conexión de enlace*

Cuando se recibe una petición de desasignación de una conexión de enlace SNP, se marca el SNP correspondiente como disponible. En el caso 2, se informa al LRMZ asociado.

– *Traducción de identificador de interfaz a identificador local*

Cuando sea necesario, el LRM proporciona la traducción de un identificador de interfaz a un identificador local. Esto se utiliza cuando, por ejemplo, los extremos del enlace SNPP están en diferentes áreas de encaminamiento.

• **Topología**

Esta función proporciona la topología de enlace utilizando los identificadores de SNPP de interfaz y los identificadores de SNP contenidos.

También proporciona características del enlace, por ejemplo, costo de enlace, diversidad y calidad. Algunas características, como el costo de enlace, pueden variar con la utilización del enlace. El proceso que se utiliza para modificar las características del enlace es controlado por una política local.

**7.3.3.2 LRMZ**

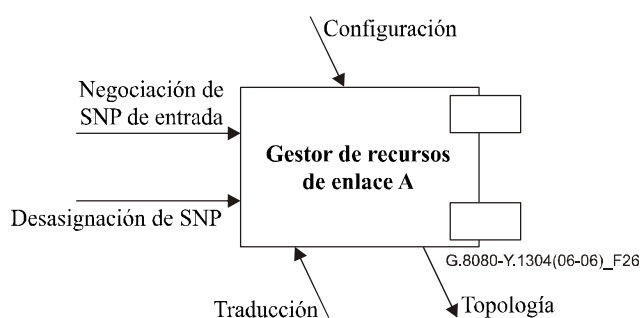
El LRMZ es responsable de la gestión del extremo Z del enlace SNPP, incluido el suministro de información de topología.

Las interfaces de componente LRMZ se presentan en el cuadro 5 y se ilustran en la figura 26.

**Cuadro 5/G.8080/Y.1304 – Interfaces de componente LRMZ**

Interfaz de entrada	Parámetros de entrada básicos	Parámetros de retorno básicos
Negociación de SNP de entrada (sólo en el caso 2)	Identificador de petición Lista de Id de SNP	Id de petición Id de SNP, o negado
Desasignación de SNP (sólo en el caso 2)	Id de SNP	Confirmación
Configuración	Información de enlace	–
Traducción	Id local	Id de interfaz

Interfaz de salida	Parámetros de salida básicos	Parámetros de retorno básicos
Topología	Información de enlace	–



**Figura 26/G.8080/Y.1304 – Componente gestor de recursos de enlace Z**

- **Funciones**

- *Asignación de SNP (utilizada solamente en el caso 2)*

Cuando se recibe una lista de identificadores de SNP utilizables se selecciona y retorna uno de ellos.

- *Desasignación de SNP (utilizada solamente en el caso 2)*

Cuando el LRMA asociado indica que se ha desasignado un SNP, dicho SNP se marca como disponible.

- *Traducción de identificador de interfaz a identificador local*

Cuando sea necesario, el LRM proporciona la traducción de un identificador de interfaz a un identificador local. Esto se utiliza cuando, por ejemplo, los extremos del enlace SNPP están en áreas de encaminamiento diferentes.

- **Topología**

Esta función proporciona la topología de enlace utilizando los identificadores de SNPP de interfaz.

### **7.3.4 Componente aplicación de políticas de tráfico (TP, *traffic policing*)**

Este componente es una subclase de puerto de política, cuyo cometido es verificar que la conexión de usuario entrante esté enviando tráfico de acuerdo con los parámetros convenidos. Cuando una conexión infringe los parámetros convenidos, el TP podrá inducir medidas para corregir la situación.

NOTA – Esto no es necesario en una red de capa de transporte de velocidad binaria continua, y no se trata con más detalle en la presente Recomendación. De la misma manera, la interfaz de política de TP no será tratada con detalle en esta Recomendación.

### **7.3.5 Componente controlador de llamada**

Las llamadas se controlan mediante controladores de llamada. Existen dos tipos de componentes controlador de llamada:

- Un controlador de llamada de parte llamante/llamada: Este controlador se asocia con un extremo de una llamada y puede estar ubicado con sistemas de extremo o ubicado a distancia y actuar como un apoderado en nombre de sistemas de extremo. Este controlador actúa en uno de los dos roles siguientes, o en ambos: soporte de la parte llamante y soporte de la parte llamada.
- Un controlador de llamada de red: Un controlador de llamada de red proporciona tres roles, uno para soporte de la parte llamante, otro para soporte de la parte llamada y un tercero para soporte de llamadas cuando éstas cruzan fronteras de dominio.

Un controlador de llamada de parte llamante interactúa con un controlador de llamada de parte llamada mediante uno o más controladores de llamada de red intermedia.

Cabe señalar que el control de llamada sólo es necesario en las asociaciones de señalización entre dominios. En una llamada, la señalización y el encaminamiento de conexión avanzan hasta completar la conexión efectuando la llamada. Por lo tanto, cuando se cruzan fronteras de dominio, se utilizan NCC. El estado de la llamada se registra en los NCC.

Además, los NCC no son jerárquicos. El NCC existente en la frontera de un conjunto de dominios anidados debe cumplir con las políticas de todos esos dominios. No existe un NCC diferente para cada dominio anidado.

### 7.3.5.1 Controlador de llamada de parte llamante/llamada

El rol de este componente comprende:

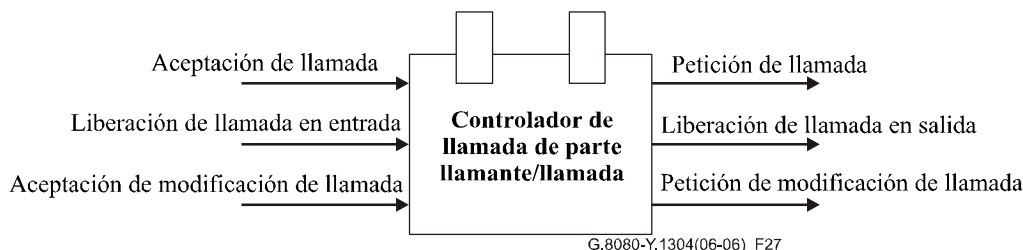
- la generación de peticiones de llamada saliente;
- la aceptación o rechazo de peticiones de llamada entrante;
- la generación de peticiones de terminación de llamada;
- el procesamiento de peticiones de terminación de llamada entrante;
- la gestión de estado de la llamada.

Este componente tiene las interfaces que se presentan en el cuadro 6. El componente controlador de llamada de parte llamante/llamada se ilustra en la figura 27.

**Cuadro 6/G.8080/Y.1304 – Interfaces de componente controlador de llamada de parte llamante/llamada**

Interfaz de entrada	Parámetros de entrada básicos	Parámetros de retorno básicos
Aceptación de llamada	Identificador de recurso de transporte o identificador de recurso de transporte de RPV	Confirmación o rechazo de petición de llamada
Liberación de llamada en entrada	Identificador de recurso de transporte o identificador de recurso de transporte de RPV	Confirmación de liberación de llamada
Aceptación de modificación de llamada	Nombre de llamada, parámetros que cambian	Confirmación o rechazo de modificación de llamada

Interfaz de salida	Parámetros de salida básicos	Parámetros de retorno básicos
Petición de llamada	Identificador de recurso de transporte o identificador de recurso de transporte de RPV; ruta (opcional, sólo para RPV)	Confirmación o rechazo de petición de llamada
Liberación de llamada en salida	Identificador de recurso de transporte o identificador de recurso de transporte de RPV	Confirmación de liberación de llamada
Petición de modificación de llamada	Nombre de llamada, parámetros que cambian	Confirmación o rechazo de modificación de llamada



**Figura 27/G.8080/Y.1304 – Componente controlador de llamada de parte llamante/llamada**

**Petición de llamada:** Esta interfaz se utiliza para presentar peticiones de establecimiento, mantenimiento y liberación de una llamada. También acepta la confirmación o rechazo de una petición de llamada.

**Aceptación de llamada:** Esta interfaz se utiliza para aceptar peticiones de llamada entrantes. También confirma o rechaza las peticiones de llamada entrantes.

**Liberación de llamada:** Esta interfaz se utiliza para enviar, recibir y confirmar peticiones de liberación.

**Petición de modificación de llamada:** Esta interfaz se utiliza para presentar peticiones de modificación de una llamada existente. También recibe la confirmación o rechazo de la petición.

**Aceptación de modificación de llamada:** Esta interfaz se utiliza para aceptar peticiones entrantes de modificación de una llamada existente. También confirma o rechaza la petición.

Obsérvese que el mismo controlador de llamada de parte llamante/llamada puede desempeñar el rol de originador o terminador en diferentes transacciones.

### 7.3.5.2 Controlador de llamada de red

Se tienen controladores de llamada de red en las fronteras de los dominios (es decir, en los puntos de referencia E-NNI, donde es necesario examinar los parámetros de llamada, por ejemplo, diferentes administraciones, diferentes dominios de recuperación, etc.).

Los controladores de llamada adyacentes (en el contexto de una llamada) forman un segmento de llamada.

El rol de este componente consiste en:

- el procesamiento de peticiones de llamada entrantes;
- la generación de peticiones de llamada salientes;
- la generación de peticiones de terminación de llamada;
- el procesamiento de peticiones de terminación de llamada;
- traducción de los identificadores de identificadores de fuente y destino de llamada RPV a identificadores de recursos de transporte;
- el control de admisión de llamada basado en la validación de parámetros de llamada, derechos de usuario y acceso a la política de recursos de red;
- la gestión del estado de la llamada.

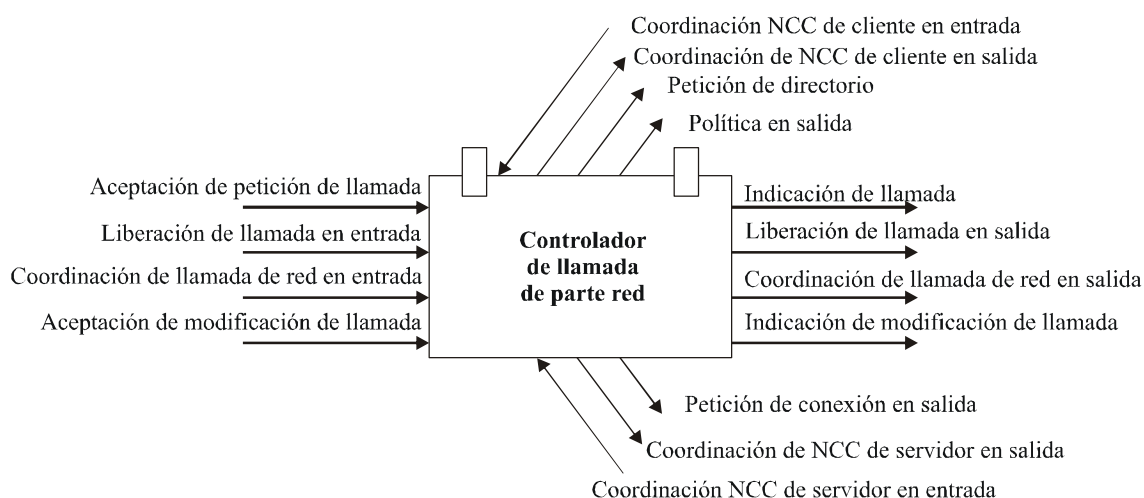
Este componente tiene las interfaces que se indican en el cuadro 7 y se ilustran en la figura 28.

**Cuadro 7/G.8080/Y.1304 – Interfaces de componente controlador de llamada de red**

Interfaz de entrada	Parámetros de entrada básicos	Parámetros de retorno básicos
Aceptación de petición de llamada	Identificador o alias de nombre de recurso de transporte UNI	Confirmación o rechazo de petición de llamada
Coordinación de llamada de red en entrada	Identificador o alias de nombre de recurso de transporte UNI	Confirmación o rechazo
Liberación de llamada entrante	Identificador o alias de nombre de recurso de transporte UNI	Confirmación de liberación de llamada
Coordinación de NCC de cliente en entrada	Parámetros de llamada de cliente opcionales, Identificación de capa cliente opcional, Identificadores de recursos de transporte	Un par de SNP en la capa cliente
Coordinación de NCC de servidor en entrada	Un par de SNP	Confirmación o rechazo de utilización
Aceptación de modificación de llamada	Nombre de llamada, parámetros que cambian	Confirmación o rechazo de modificación de llamada

**Cuadro 7/G.8080/Y.1304 – Interfaces de componente controlador de llamada de red**

Interfaz de salida	Parámetros de salida básicos	Parámetros de retorno básicos
Indicación de llamada	Identificador o alias de nombre de recurso de transporte UNI	Confirmación o rechazo de petición de llamada
Petición de conexión en salida	Identificador o alias de nombre de recurso de transporte UNI	Un par de SNP
Coordinación de llamada de red en salida	Identificador o alias de nombre de recurso de transporte UNI	Confirmación o rechazo de petición de llamada
Petición de directorio	Identificador o alias de nombre de recurso de transporte UNI	Nombre local
Política en salida	Parámetros de llamada	Aceptación o rechazo de llamada
Liberación de llamada en salida	Identificador o alias de nombre de recurso de transporte UNI	Confirmación de liberación de llamada
Coordinación de NCC cliente en salida	Un par de SNP en la capa de cliente	Confirmación o rechazo de utilización
Coordinación de NCC servidor en salida	Parámetros de llamada opcionales, Identificación de capa, Identificadores de recursos de transporte	Un par de SNP
Petición de modificación de llamada	Nombre de llamada, parámetros que cambian	Confirmación o rechazo de modificación de llamada



G.8080-Y.1304(06-06)\_F28

**Figura 28/G.8080/Y.1304 – Componente controlador de llamada de red**

**Aceptación de petición de llamada:** Esta interfaz se utiliza para aceptar un par de identificadores de fuente y de destino de llamada. También confirma o rechaza la petición de establecimiento de comunicación entrante.

**Petición de conexión en salida:** Esta interfaz se utiliza para enviar una petición de establecimiento de conexión a un controlador de conexión como un par de SNP.

**Petición de directorio:** Esta interfaz se utiliza para obtener un nombre de SNPP a partir de un identificador o un alias de recurso de transporte UNI. En el caso de los alias, es un asunto de política qué SNPP se retorna si hay varios representados .

**Coordinación de llamada de red:** Esta interfaz se utiliza para la coordinación de llamada a nivel de red.

**Liberación de llamada en entrada/salida:** Estas interfaces se utilizan para enviar, recibir y confirmar peticiones de liberación.

**Política en salida:** Esta interfaz proporciona verificación de política.

**Coordinación de NCC de cliente en entrada:** Esta interfaz se utiliza para aceptar una petición de un NCC de capa de cliente de un par de SNP. El NCC recibe los identificadores de origen y destino en su capa a fin de que proporcione una conexión de red destinada a la capa de cliente. Se retornan los SNP de la capa de cliente que son soportados por una adaptación a la conexión de red. Esta interfaz es también utilizada por el cliente para liberar o modificar el uso del par de SNP. El NCC retorna el resultado de la acción.

**Coordinación del NCC de cliente en salida:** Esta interfaz se utiliza para presentar a una capa de cliente un par de SNP que son soportados por una adaptación a una conexión de red. El NCC de cliente indica si acepta o no este recurso. Esta interfaz es también utilizada por el servidor para liberar o presentar un par de SNP modificados. El cliente NCC retorna el resultado de la acción.

**Coordinación de NCC de servidor en salida:** Esta interfaz se utiliza para solicitar un par de SNP (entrada y salida) que pueden ser usados por la llamada para transferir información característica. Es idéntica a los parámetros de retorno correspondientes a la interfaz de petición de conexión en salida excepto que no está prevista la creación de una conexión de red en esta capa. Esta interfaz también se utiliza para liberar o solicitar la modificación del uso del par de SNP proporcionados por la capa de servidor. El NCC de servidor retorna el resultado de la acción.

**Coordinación de NCC de servidor en entrada:** Esta interfaz se utiliza para aceptar un par de SNP (entrada y salida) presentados desde un NCC de capa de servidor. El par puede ser aceptado o rechazado. Esta interfaz es también utilizada por el servidor para liberar o presentar un par de SNP modificados. El NCC retorna el resultado de la acción.

**Aceptación de modificación de llamada:** Esta interfaz se utiliza para aceptar una petición de modificación de llamada. Esta interfaz también confirma o rechaza la petición de modificación de llamada entrante.

**Indicación de modificación de llamada:** Esta interfaz se utiliza para continuar una petición de modificación de llamada a otro NCC. También recibe la confirmación o rechazo de la petición.

El rol del control de admisión de llamada en el controlador de llamada de red de parte llamante es verificar que se ha proporcionado un nombre y unos parámetros de servicio de usuario llamante válidos. Los parámetros de servicio se verifican cotejándolos con una especificación de nivel de servicio. Cuando sea necesario, se podrán renegociar estos parámetros con el controlador de llamada de parte llamante. El alcance de esta negociación está determinado por políticas derivadas de la especificación de nivel de servicio original, que a su vez se deriva del convenio del nivel de servicio.

El rol del control de admisión de llamada en el controlador de llamada de red de parte llamada, cuando lo haya, es verificar que la parte llamada tiene derecho a aceptar la llamada, basándose en los contratos de servicio de parte llamada y parte llamante. Por ejemplo, una dirección de llamante se puede someter a un proceso de cribado y la llamada puede ser rechazada.

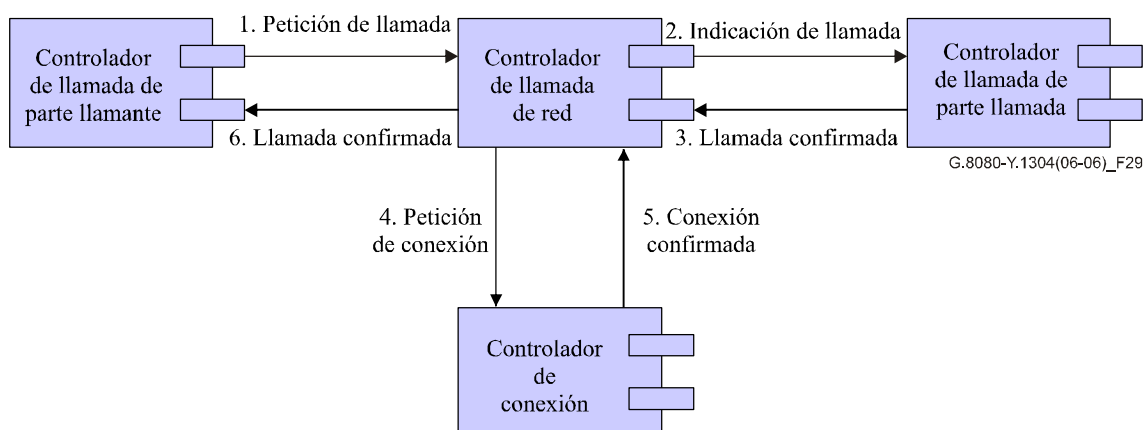
La interfaz de petición de directorio del controlador de llamadas de la red se utiliza para acceder a una función de directorio usada para transformar identificadores entre espacios de nombres o al interior de los mismos. Se proporciona un identificador a la función de directorio, la cual retorna uno o varios identificadores. En esta Recomendación no se trata la forma de mantener ni de configurar el directorio, pero esto será tema de otras Recomendaciones. Algunos ejemplos de correspondencia que podría proporcionar la función de directorio son:

- Identificador de recurso de transporte UNI a identificador SNPP. Un controlador de red requiere de una SNPP para formular una petición a un controlador de conexión.
- Alias de identificador de recurso de transporte UNI a identificador de recurso de transporte UNI. Una aplicación de esto consiste en identificar recursos asociados con un AGC multiaccesible con un identificador que es un alias de identificador de recurso de transporte UNI.
- Identificador SNPP a identificador de recurso de transporte UNI. Para poder utilizar las interfaces coordinación de NCC de servidor en salida y coordinación de NCC de cliente en entrada se necesitan algunos identificadores de recursos de transporte UNI que se encuentran en la capa de servidor. Esto se utiliza para realizar la llamada de capa de servidor. Antes de que se efectúe la llamada, la capa de cliente no conoce los identificadores de recursos de transporte UNI de la capa de servidor; sólo posee los SNPP de la capa de cliente en la frontera de la subred de capa de servidor. Una correspondencia entre los SNPP de la capa de cliente y los identificadores de recursos de transporte UNI de la capa de servidor proporciona los medios para realizar la llamada de capa de servidor.
- Alias SNPP a SNPP. Se utiliza en la coordinación de los niveles de encaminamiento.

### 7.3.5.3 Interacciones de controlador de llamada

La interacción entre los componentes controlador de llamada depende del tipo de llamada y del tipo de conexión, como se describe a continuación.

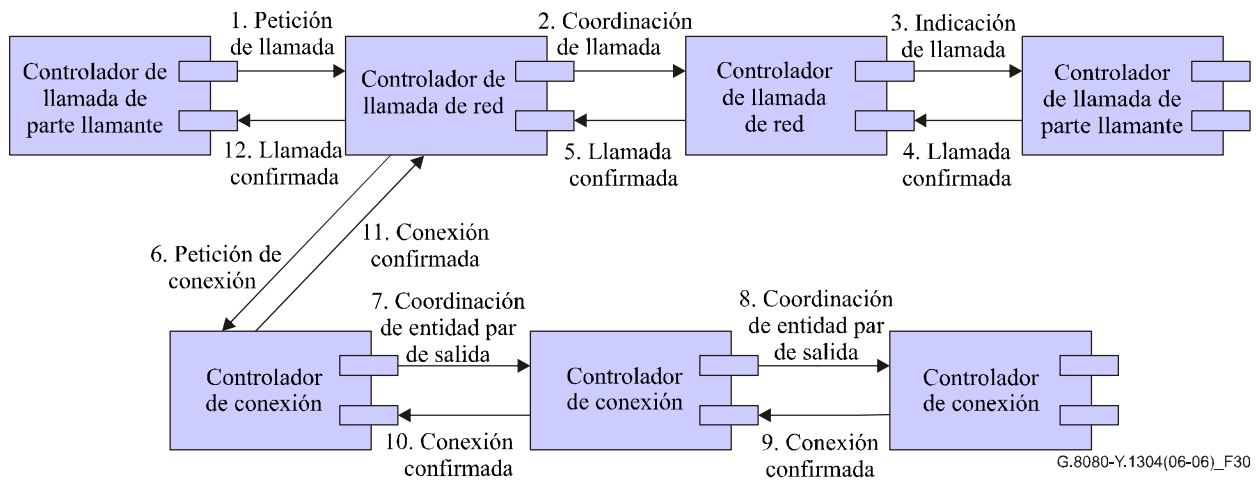
**Conexiones conmutadas:** El controlador de llamada de parte llamante (asociado con un terminal de extremo) interactúa con el controlador de llamada de red para formar una llamada entrante, y el controlador de llamada de red interactúa con el controlador de llamada de parte llamada (asociado con un terminal de extremo) para formar una llamada saliente. El controlador de llamada de red interactúa con los controladores de conexión para proporcionar la llamada. Un ejemplo de dicha interacción se muestra en la figura 29. Obsérvese que los controladores de llamada de parte llamante/llamada no interactúan directamente con el controlador de conexión asociado con el controlador de llamada de red correspondiente.



**Figura 29/G.8080/Y.1304 – Interacción de controlador de llamada de parte llamada/llamante para conexiones conmutadas: Ejemplo 1**

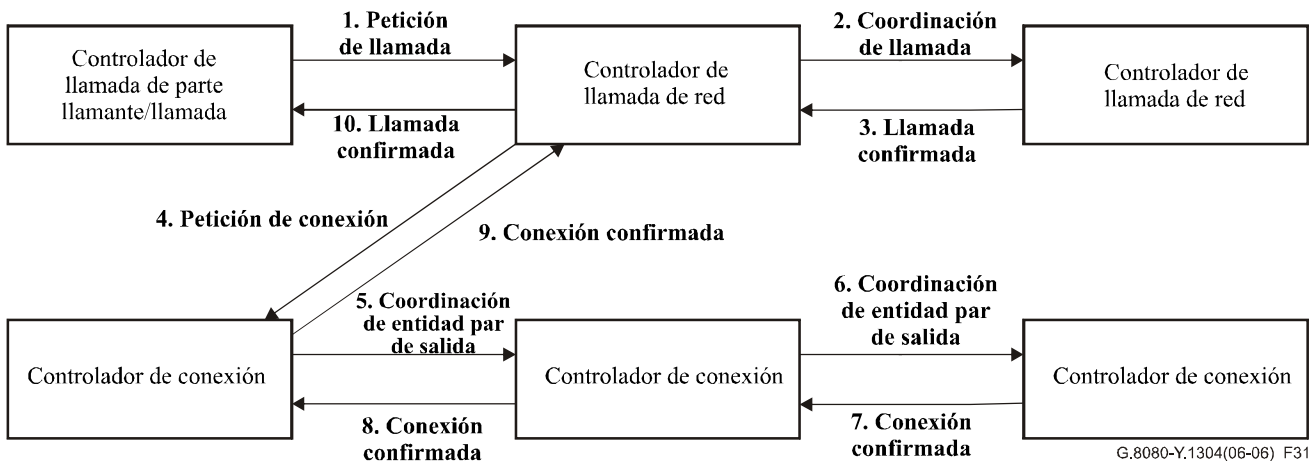
En la figura 29 se muestra la situación en la cual el controlador de llamada de parte llamada acepta la llamada, antes de que el controlador de llamada de la red de ingreso solicite la conexión. También es válido definir la interacción de tal manera que el establecimiento de conexión siga a la llamada, como se ilustra en la figura 30.





**Figura 30/G.8080/Y.1304 – Interacción de controlador de llamada de parte llamada/llamante para conexiones conmutadas: Ejemplo 2**

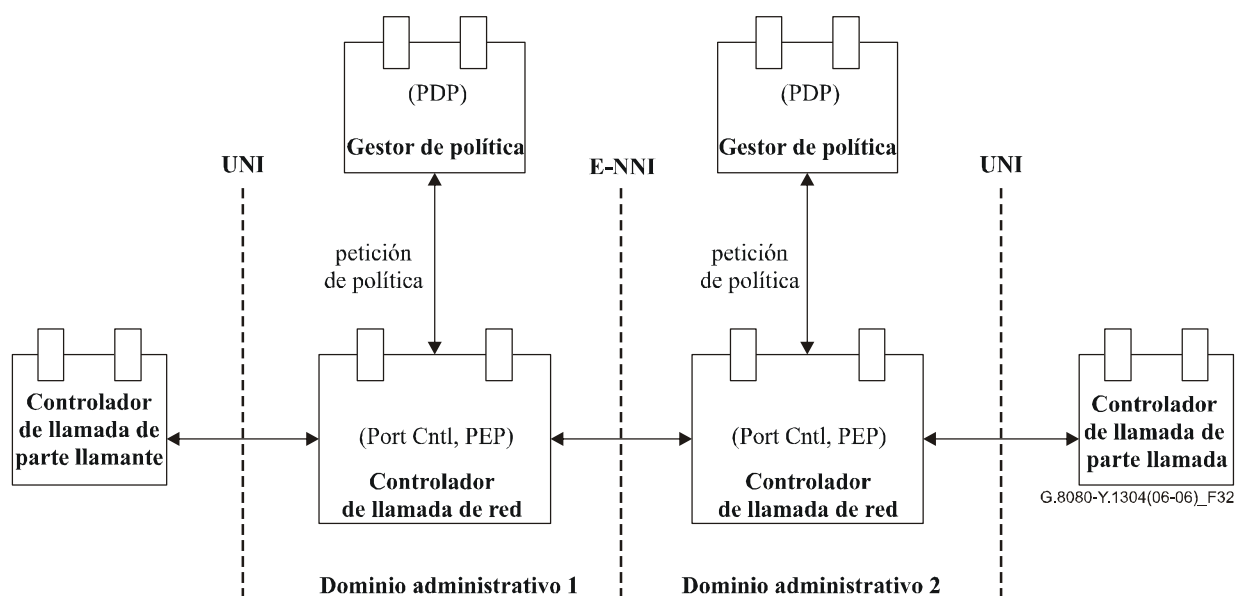
**Conexiones permanentes programables:** Se considera que el sistema de gestión de red contiene los controladores de parte llamante/llamada. El sistema de gestión envía una instrucción para configurar el controlador de llamada de parte llamante que inicia los controladores de llamada de red en un plano de control cuando las instrucciones de configuración de llamadas son enviadas a un plano de control. La respuesta a una instrucción de configuración de llamada recibida desde el plano de control es considerada por un plano de gestión como una confirmación de establecimiento de comunicación. Esto representa una llamada nula sin servicio. Los protocolos entre el plano de gestión de red y el plano de control son una instrucción y una interfaz de respuesta de instrucción. La figura 31 ilustra las interacciones del controlador de llamada para el caso de conexiones permanentes programables.



**Figura 31/G.8080/Y.1304 – Interacciones del controlador de llamada para las conexiones permanentes programables**

**Llamada de apoderado:** El controlador de llamada de parte llamante/llamada interactúa con el controlador de llamada de red mediante un protocolo de llamada, pero no es coincidente con el usuario.

En la figura 32 se muestra un ejemplo de las interacciones necesarias para el soporte de la política de control de admisión de llamada entre controladores de llamada de red.



Port Cntl Controlador de puerto (*port controller*)  
PDP Punto de decisión de la política (*policy decision point*)  
PEP Punto de imposición de la política (*policy enforcement point*)

**Figura 32/G.8080/Y.1304 – Ejemplo de interacciones de política de control de admisión de llamada**

**Llamadas por capas:** Dos NCC de distintas capas pueden cooperar para permitir el soporte de CI de cliente en una capa de servidor. Las políticas de operador rigen la utilización de estas interfaces entre capas. Esto puede ser iniciado hacia una capa de servidor, o desde la misma, dependiendo en qué capa se inició el funcionamiento. Desde un NCC, la petición a un NCC de capa de servidor retorna el mismo resultado que la interfaz de "Petición de conexión en salida". La diferencia estriba en que se ha efectuado una asociación con un NCC de servidor. Esta acción da lugar a la utilización o la creación de un segmento de llamada de capa de servidor que soportará el NCC de cliente. Si la capa de servidor necesita crear una llamada como resultado de la utilización de la interfaz de "coordinación de NCC de servidor en salida" o la interfaz de "coordinación de NCC de cliente en entrada", los identificadores de fuente y de destino son utilizados como parámetros de llamada. Se ejecuta entonces una acción idéntica al comportamiento de la interfaz de "aceptación de petición de llamada" si se determina que el establecimiento de la conexión en esa capa de servidor es la acción correcta. El NCC de capa de servidor podría alternativamente utilizar su interfaz de "coordinación de NCC de servidor en salida" para efectuar una petición (reiterativa en la capa) de un par de SNP de otro NCC de capa que sea servidor del primero.

Un NCC podría también iniciar una acción hacia una capa de cliente por medio de la cual presenta un par de SNP que pueden ser utilizados por la capa de cliente para transferir CI de cliente. Para esta finalidad son útiles las interfaces de "coordinación de NCC de cliente en salida" o de "coordinación de NCC de servidor en entrada". Cuando se utiliza esta interfaz, el par de SNP presentado podrá transferir CI de cliente sin iniciar ninguna acción de llamada en la capa de servidor. Esto se utiliza para una operación cuando una capa de servidor ya ha establecido una comunicación y ésta es presentada a la capa de cliente en un punto de tiempo ulterior. La capa de cliente puede aceptar o rechazar la utilización del par de SNP ofrecido.

#### 7.3.5.4 Modificación de llamada

El servicio proporcionado por una llamada puede ser modificado por acciones iniciadas por un controlador de llamada de parte llamante/llamada (CCC, *calling/called party call controller*) o una aplicación de gestión de red que actúa sobre un NCC en la UNI. El grado de modificación es establecido por la política del operador, la cual puede o no ser compartida con el usuario de extremo (por ejemplo, para informar al usuario de que se permiten incrementos de anchura de banda). El grado al que podrá modificarse una llamada está sujeto a las siguientes reglas:

- La CI asociada con la llamada en la UNI no es modificable.
- Los puntos extremos de la conexión de enlace asociada con la llamada en la UNI-N no son modificables. Sin embargo, se pueden añadir o suprimir cuando se añadan o supriman conexiones de una llamada.

Las acciones pueden ser la modificación de un segmento de llamada cuando los NCC permanecen fijos o la creación/supresión de segmentos de llamada dentro de una llamada completa cuando los NCC son creados/suprimidos.

Ejemplos de lo que puede ser modificado en la UNI son la anchura de banda (por ejemplo, velocidad de llamada Ethernet) y el número de CCC participantes (por ejemplo, llamada multipartita).

Ejemplos de lo que puede ocurrir dentro de la red de resultados de peticiones de modificación de llamada UNI son:

- Cambiar el número de conexiones de capa de servidor asociado con una llamada VCAT que soporta una llamada Ethernet.
- En respuesta a una petición de aumentar la disponibilidad de una llamada, añadir una conexión adicional para crear una configuración 1+1.

#### 7.3.5.5 Tratamiento de fallo de la llamada

En el caso de una nueva petición de llamada, si la red no puede establecer todas las conexiones necesarias para satisfacer la petición de llamada, se liberarán (suprimirán) todas las conexiones y conexiones parciales que se hayan establecido y se rechazará la petición de conexión.

En el caso de modificaciones de llamada, si la red no puede añadir las conexiones solicitadas, se considerará que ha fallado la modificación de la llamada. Se suprimirán todas las conexiones y conexiones parciales y no se harán cambios a la llamada existente.

#### 7.3.6 Agente de descubrimiento (DA, *discovery agent*)

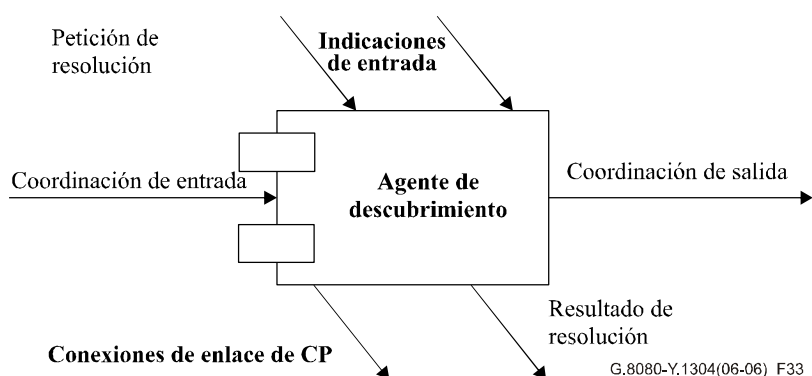
La federación de agentes de descubrimiento funciona en el espacio de nombre del plano de transporte y proporciona la separación entre ese espacio y los nombres del plano de control. La federación tiene conocimiento de los puntos de conexión (CP) y de los puntos de conexión de terminación (TCP, *termination connection point*) en la red, mientras que un DA local sólo tiene conocimiento de los puntos que le han sido asignados. La coordinación de DA conlleva la aceptación de posibles indicaciones sobre CP y conexiones de enlace preexistentes. El DA mantiene las conexiones de enlace CP-CP para poder confinar las conexiones de enlace SNP-SNP a estas últimas ulteriormente. Las interfaces de resolución ayudan al descubrimiento proporcionando traducción de nombres de TCP globales a la dirección del DA responsable de ese punto, junto con el nombre local del TCP. Obsérvese que las indicaciones resultan de la cooperación con otros componentes o de sistemas de aprovisionamiento externos.

Los DA no tienen interfaces de equipos privadas y pueden estar situados en cualquier plataforma adecuada.

**Cuadro 8/G.8080/Y.1304 – Interfaz del componente agente de descubrimiento (DA)**

Interfaz de entrada	Parámetros de entrada básicos	Parámetros de retorno básicos
Coordinación de entrada		
Indicaciones de entrada	Par de CP	
Petición de resolución	Nombre de TCP	

Interfaz de salida	Parámetros de salida básicos	Parámetros de retorno básicos
Coordinación de salida		
Conexión de enlace CP	Par de CP	
Resultado de resolución		Dirección RCD de DA, índice de TCP



**Figura 33/G.8080/Y.1304 – Componente agente de descubrimiento**

### 7.3.7 Ejecutantes de terminación y adaptación

El ejecutante de terminación y adaptación (TAP) está coubicado con la función de adaptación y terminación. Proporciona al plano de control (el LRM) una visión del recurso de conexión de enlace que soporta un SNP y oculta los detalles específicos del soporte físico y la tecnología del control de adaptación y terminación.

El TAP funciona en dos instantes de tiempo diferentes y proporciona dos funciones diferentes.

Cuando se asigna un recurso a un plano de control, el TAP se configura con una vinculación permitida a un SNP, lo que provoca la creación de un SNP (en un extremo de un enlace) dentro del ámbito de un LRM. Si el recurso es compartido entre múltiples planos de control (por ejemplo, distintas redes de capa o distintas RPV de capa 1), el TAP mantiene una lista de las vinculaciones permitidas. El TAP controla la vinculación entre un CTP y cada SNP que hace referencia a cualquiera de los recursos dentro del ámbito de ese TAP. Los estados del SNP que reflejan la relación de vinculación se describen en el cuadro 9.

**Cuadro 9/G.8080/Y.1304 – Estados de vinculación del SNP**

<b>Estado</b>	<b>Descripción</b>
Ocupado	Vinculación permitida, el recurso al que se hace referencia está atribuido actualmente a otro plano de control o al plano de gestión.
Potencial	Vinculación permitida, en este momento el recurso al que se hace referencia no está atribuido a ningún plano de control o al plano de gestión.
Atribuido	La vinculación está permitida y el recurso se configura y se atribuye a este LRM.
Cierre	Notificación del TAP de que el recurso debe ser retornado dentro de un marco de tiempo explícito, por ejemplo: inmediatamente (interrupción de la llamada en curso); rápidamente (reencaminamiento de la llamada antes de su eliminación); próxima ventana de mantenimiento; cuando se elimina la llamada.
Liberado	El LRM ya no está utilizando el recurso.

Cuando un SNP se encuentra en el estado atribuido, el TAP debe configurar correctamente los recursos (por ejemplo, adaptación variable) y fijar el estado de cualquier otro SNP referenciando el mismo recurso a ocupado.

Cuando las conexiones de enlace SNP están vinculadas a su conexión de enlace CP correspondiente, el TAP se encarga de mantener la vinculación entre el SNP-CP. Un TAP local coopera con un TAP distante para coordinar cualquier adaptación variable o para cualquier otra coordinación necesaria cuando se forman las conexiones de enlace CP.

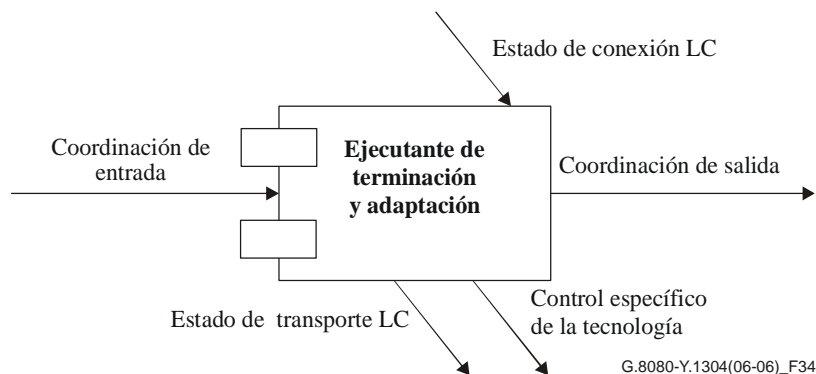
Si un LRM desea utilizar un SNP en el estado potencial para satisfacer una petición de conexión, durante el establecimiento de la conexión, un par de TAP coopera entonces a través del LRM para coordinar cualquier establecimiento de adaptación requerido por la conexión de enlace.

El TAP proporciona información sobre la situación de transmisión de la conexión de enlace y acepta información de estado de conexión del enlace para garantizar que las indicaciones del plano de gestión son congruentes. Esta congruencia incluye garantizar que el estado de alarma de la conexión de enlace es coherente, de manera que no se generan ni se notifican alarmas no deseadas.

**Cuadro 10/G.8080/Y.1304 – Interfaz del componente ejecutante de terminación y adaptación (TAP)**

<b>Interfaz de entrada</b>	<b>Parámetros de entrada básicos</b>	<b>Parámetros de retorno básicos</b>
Estado de la conexión LC (SNP-SNP)	Enum: en servicio, fuera de servicio	
Coordinación de entrada	Dependiente de la tecnología	

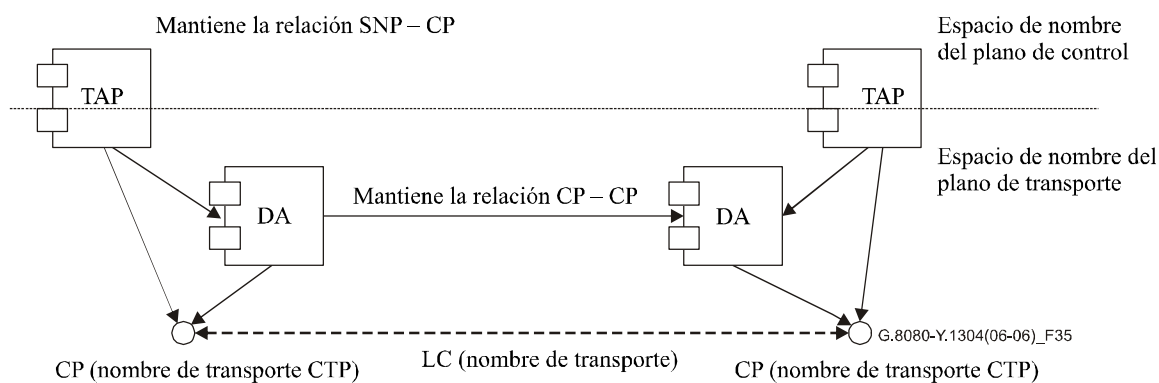
<b>Interfaz de salida</b>	<b>Parámetros de salida básicos</b>	<b>Parámetros de retorno básicos</b>
Estado de transporte LC (SNP-SNP)	Enum: ascendente, descendente	
Coordinación de salida	Dependiente de la tecnología	Dependiente de la tecnología
Control	Específico del soporte físico	Específico del soporte físico



**Figura 34/G.8080/Y.1304 – Componente ejecutante de terminación y adaptación**

### 7.3.8 Proceso de descubrimiento de enlace

El proceso genérico de descubrimiento se divide en dos instantes de tiempo y nombres de espacio separados y distintos. La primera parte ocurre enteramente en el espacio de nombre del plano de transporte (CP y CTP).

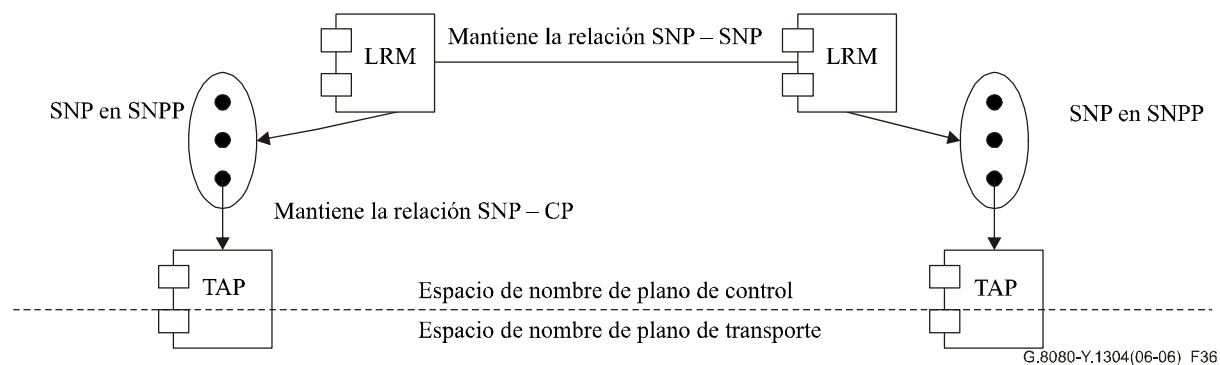


**Figura 35/G.8080/Y.1304 – Descubrimiento de las conexiones del enlace de transporte (LC)**

El DA funciona enteramente dentro del espacio de nombre de transporte y es responsable de mantener el nombre de transporte de la conexión de enlace (asociada con cada CP). Esta información se puede obtener utilizando mecanismos de transporte invisibles al espacio de nombre del plano de control, manteniendo información de relaciones previamente obtenida o por aprovisionamiento. El DA asiste en un proceso de descubrimiento automático subyacente resolviendo cooperativamente nombres CP de transporte entre todos los DA en la red, permitiendo así que los DA (u otros componentes) responsables de cada extremo de la conexión del enlace de transporte comuniquen sobre esa conexión de enlace.

Un CP puede ser asignado a un conjunto de RPV, incluido el conjunto vacío y el conjunto de un elemento único (*singleton*). Este conjunto de RPV puede ser representado mediante una etiqueta de propiedad. El DA verifica que la etiqueta de propiedad agregada a cada CP de una conexión de enlace sea la misma.

La segunda parte ocurre enteramente dentro del espacio de nombre de plano de control (SNP).



**Figura 36/G.8080/Y.1304 – Población de conexiones de enlace del plano de control**

El gestor de recursos de enlace (LRM) mantiene la información de vinculación SNP-SNP necesaria para el nombre del plano de control de la conexión de enlace, mientras que el TAP mantiene la relación entre el nombre del plano de control (SNP) y el nombre del plano de transporte (CP) del recurso. Esta separación permite que los nombres del plano de control estén totalmente separados de los nombres del plano de transporte y sean completamente independientes del método utilizado para poblar los DA con estos nombres de transporte.

Para asignar una conexión de enlace SNP-SNP a un enlace SNPP, sólo es necesario que exista el nombre de transporte para la conexión de enlace. Por consiguiente, es posible asignar conexiones de enlace al plano de control sin que la conexión de enlace esté físicamente conectada. Este procedimiento de asignación puede ser verificado por los LRM que intercambian el nombre de enlace de transporte que corresponde al SNP.

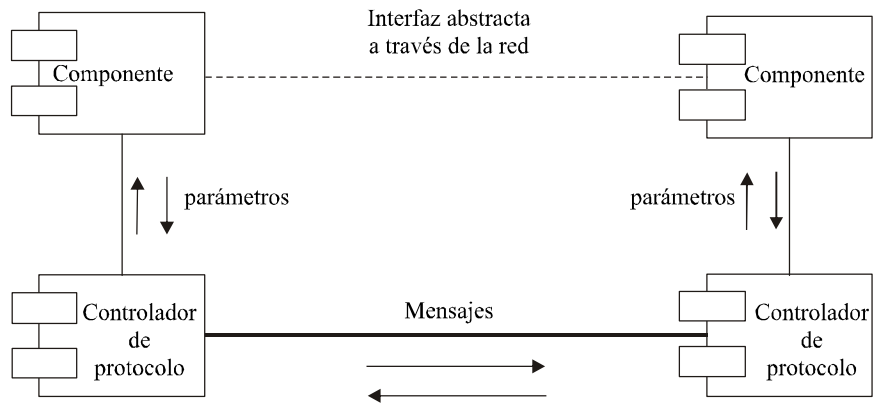
Obsérvese que el nombre de enlace SNPP plenamente calificado es un nombre de plano de control que refleja la estructura de los recursos del plano de transporte.

#### 7.4 Componente controlador de protocolo (PC, *protocol controller*)

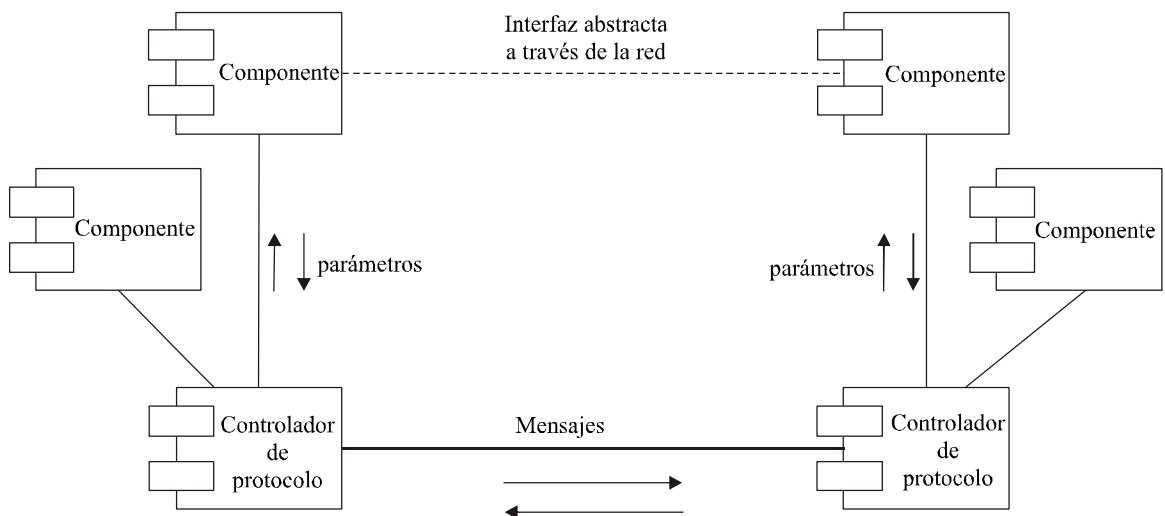
El controlador de protocolo proporciona la función para hacer corresponder los parámetros de las interfaces abstractas de los componentes de control con mensajes que son transportados por un protocolo para el soporte de la interconexión a través de una interfaz. Los controladores de protocolo son una subclase de controlador de puerto, y proporcionan todas las funciones asociadas con esos componentes. En particular, los controladores de protocolo informan violaciones de protocolo a sus puertos de supervisión. Pueden también desempeñar el rol de multiplexar varias interfaces abstractas en ejemplares de protocolo simples, como se muestra en la figura 37. Los detalles de un controlador de protocolo en particular atañen al diseño de protocolo, aunque en esta Recomendación se den algunos ejemplos.

El rol de un controlador de protocolo de transporte es proporcionar transferencia autenticada, segura, y fiable de primitivas de control a través de la red mediante una interfaz definida. De esta manera, se puede seguir el rastro de las transacciones y asegurarse de que se reciben las respuestas esperadas, o se informa una excepción al originador. Cuando existen funciones de seguridad, el controlador de protocolo informará violaciones a la seguridad a través de su puerto de supervisión.

Se transmiten primitivas de señalización entre el controlador de conexión y el controlador de protocolo, que es semánticamente transparente a las primitivas de mensajería, puesto que esto tiene por consecuencia mensajes de protocolo externos y viceversa. Se transmiten mensajes de señalización entre los dos controladores de protocolo. Esto se muestra en la figura 38.



a) Utilización genérica de un controlador de protocolo

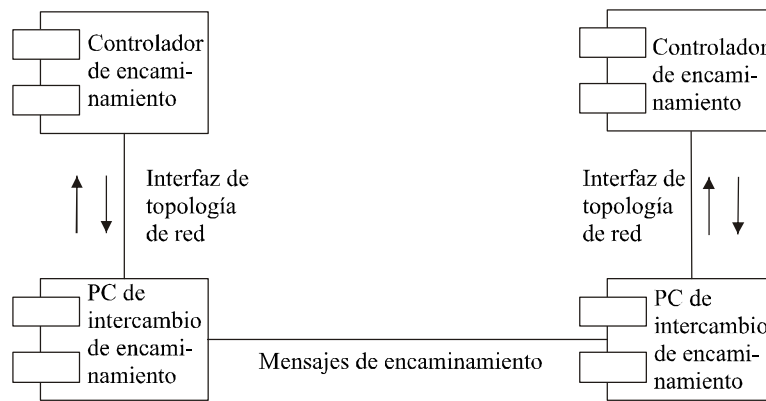


G.8080-Y.1304(06-06)\_F37

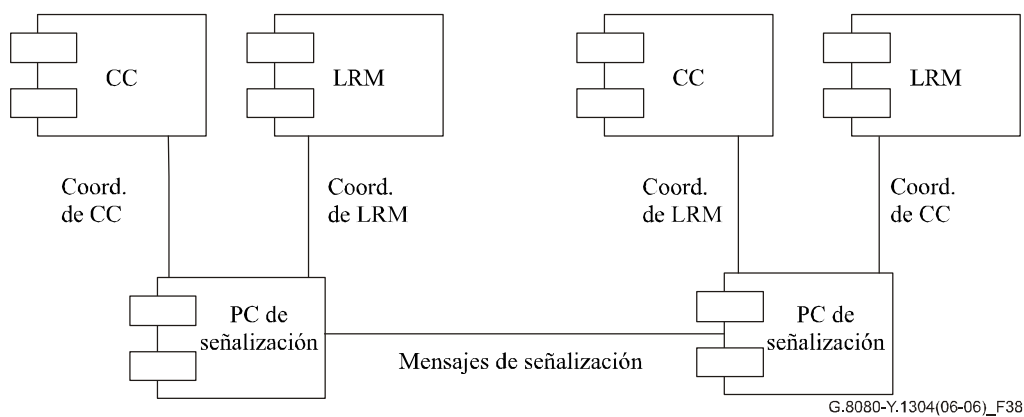
b) Multiplexación genérica de diversos trenes de primitivas en un solo protocolo

**Figura 37/G.8080/Y.1304 – Controlador de protocolo**





a) Intercambio de cuadro de encaminamiento mediante el PC de intercambio de encaminamiento



b) Multiplexación de LRM y coordinación de CC mediante el PC de señalización

**Figura 38/G.8080/Y.1304 – Ejemplos de uso de controlador de protocolo**

Son ejemplos de uso de controlador de protocolo la transferencia de la siguiente información:

- Mensajes de actualización de cuadros de rutas transmitidos a través de un controlador de protocolo de intercambio de encaminamiento (como se muestra en la figura 38-a).
- Mensajes de coordinación de gestor de recursos de enlace (donde sea adecuado, como en las conexiones de velocidad binaria disponibles) transmitidos a través de un controlador de protocolo de gestor de recurso de red.
- Mensajes de coordinación de control de conexión transmitidos a través de un controlador de protocolo de controlador de conexión, (como se muestra en la figura 38-b). Obsérvese que las interfaces de coordinación de LRM y de CC pueden ser multiplexadas en el mismo controlador de protocolo.

## 8 Puntos de referencia

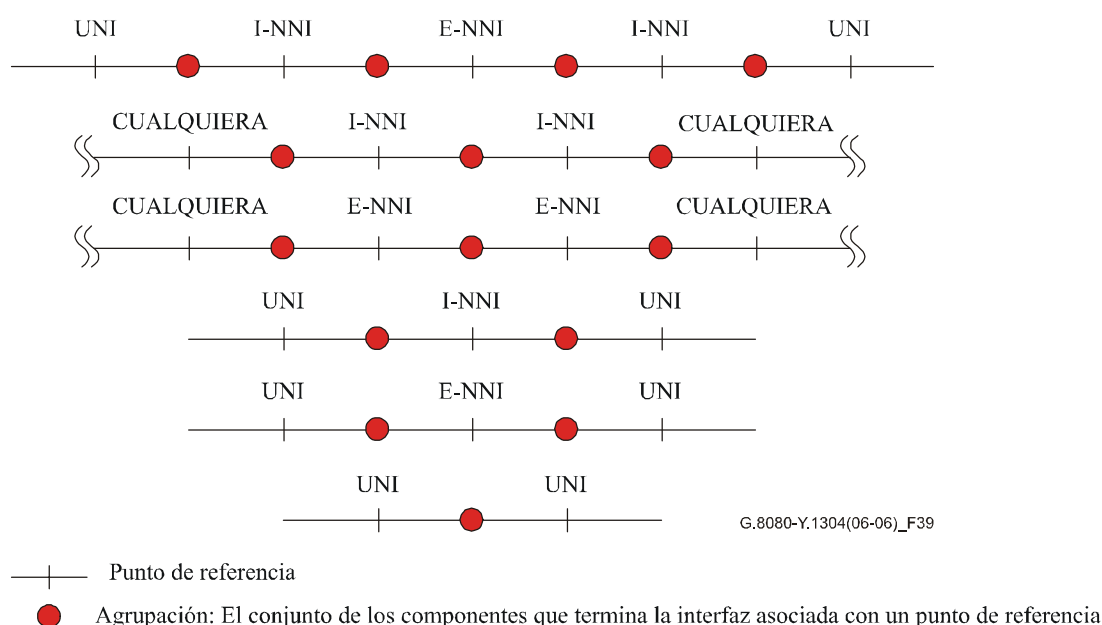
La presente Recomendación define diversas interfaces lógicas (es decir, puntos de referencia) dentro de una red de transporte típica en que se intercambia información de señalización/encaminamiento. Los puntos de referencia pueden ser soportados por interfaces múltiples. Estos puntos de referencia son la UNI, la I-NNI y la E-NNI. Es importante reconocer que habrá múltiples dominios dentro de la ASON y que las UNI y E-NNI se utilizarán, en particular, para la señalización de control entre dominios. En las siguientes cláusulas se describen las

funcionalidades específicas que deben ser transportadas a través de los diversos puntos de referencia (UNI, I-NNI y E-NNI) y la forma en que difieren.

Una política se puede aplicar en las interfaces que soportan un punto de referencia. Las políticas aplicadas dependen del punto de referencia y de las funciones soportadas. Por ejemplo, en los puntos de referencia UNI, I-NNI y E-NNI, se puede aplicar una política al control de llamada y conexión. Además, para los puntos de referencia I-NNI y E-NNI se puede aplicar una política al encaminamiento.

Un punto de referencia representa un conjunto de servicios, proporcionado por interfaces en uno o más pares de componentes. La interfaz de componente es independiente del punto de referencia, por lo que la misma interfaz puede participar en más de un punto de referencia. Desde la perspectiva del punto de referencia, los componentes que soportan la interfaz no son visibles, por lo que la especificación de la interfaz puede ser tratada independientemente del componente.

Los flujos de información que transportan servicios a través del punto de referencia son terminados (u originados) por componentes, y múltiples flujos no tienen que ser terminados en el mismo lugar físico. Pueden atravesar diferentes secuencias de puntos de referencia, como se ilustra en la figura 39.



**Figura 39/G.8080/Y.1304 – Puntos de referencia**

## 8.1 UNI

Los flujos de información esperados a través del punto de referencia UNI soportan las siguientes funciones:

- Control de llamada.
- Descubrimiento de recursos.
- Control de conexión.
- Selección de conexión.

Obsérvese que no existe función de encaminamiento asociada con el punto de referencia UNI.

A este conjunto básico de funciones se pueden añadir funciones adicionales, tales como seguridad y autenticación de llamadas, o servicios de directorio mejorados.

La utilización del punto de referencia en la capa 1 de la RPV queda en estudio.

## 8.2 I-NNI

Los flujos de información esperados a través del punto de referencia I-NNI soportan las siguientes funciones:

- Descubrimiento de recursos.
- Control de conexión.
- Selección de conexión.
- Encaminamiento de conexión.

## 8.3 E-NNI

Los flujos de información esperados a través del punto de referencia E-NNI soportan las siguientes funciones:

- Control de llamada.
- Descubrimiento de recursos.
- Control de conexión.
- Selección de conexión.
- Encaminamiento de conexión.

A este conjunto básico de funciones se pueden añadir funciones adicionales, tales como seguridad y autenticación de llamadas, o servicios de directorio mejorados.

Cuando existe el punto de referencia E-NNI entre un dominio de cliente RPV y una RPV en un dominio de proveedor de servicio, pueden soportarse servicios suplementarios (véase la Rec. UIT-T Y.1312). Ejemplos son:

- autenticación y autorización de usuario RPV;
- gestión de política de usuario RPV, incluidas restricciones de conectividad;
- transferencia transparente de información de control entre usuarios RPV;
- participación de la RPV en el dominio de encaminamiento de cliente;

El soporte de tales servicios queda fuera del alcance de esta Recomendación.

## 8.4 Arquitectura de usuario

El lado usuario se denominará UNI-C (para "cliente") y el lado red se denominará UNI-N (para "red").

El identificador de recurso de transporte UNI G.8080/Y.1304 (véase la cláusula 10) define uno o más nombres globalmente únicos para cada enlace SNPP que forma parte de una UNI. Estos nombres se utilizan para identificar destinos de llamada. Dado que una UNI puede contener múltiples enlaces SNPP, como en el caso de multiaccesibilidad (*multi-homing*), una UNI puede, por lo tanto, tener múltiples nombres globalmente únicos para sus recursos portadores. Obsérvese que estos nombres no son nombres de usuario.

Cuando hay múltiples enlaces SNPP que forman parte de la misma UNI, las direcciones pueden servir para discriminar entre los enlaces SNPP que se han de utilizar. Factores tales como la diversidad o el costo podrían ser invocados por los llamantes para seleccionar el enlace SNPP apropiado. Los enlaces SNPP entre un AGC común y una red pueden estar en la misma UNI, si se encuentran en el lado red y están en el ámbito de un componente controlador de llamada de red común.

Los identificadores de recursos de transporte UNI pueden ser usados para diferenciar entre las UNI a un usuario. Cuando hay múltiples UNI, cada una tiene identificadores de recursos de transporte UNI distintos y no comparten una dirección común.

Se describe a continuación la arquitectura UNI-C:

- 1) Existe una entidad de transporte denominada contenedor de grupo de acceso (AGC, *access group container*) que puede terminar múltiples enlaces SNPP. Esta entidad puede contener un conjunto de grupos de acceso G.805.
- 2) Un AGC es una entidad de capa que contiene grupos de acceso, LRM y TAP. Es similar a las subredes G.805, salvo que no se define recursivamente, puede ser o no una matriz (no tiene que estar especificada) y no tiene conexiones de subred definidas. Múltiples AGC de diferentes capas pueden coincidir en el mismo equipo.
- 3) Las funciones del plano de control asociadas con una UNI-C en un AGC son: control de llamada (controlador de llamada de la parte llamante/llamada) y descubrimiento de recursos (LRM). El control de conexión limitado y la selección de conexión están presentes para interactuar con el controlador de conexión en el lado UNI-N. Esto se debe a que el control de conexión en el lado UNI-N tiene una interfaz de encaminamiento, mientras que el control de conexión en el lado UNI-C sigue la aceptación/interrupción de la conexión desde el lado UNI-N.
- 4) Las aplicaciones que utilizan uno o más caminos en un AGC se conocen como "usuarios de conexión de <nombre de aplicación>". Interactúan directamente con los puntos de acceso G.805 presentando y recibiendo información adaptada. Para cada usuario de conexión puede haber un "solicitante de conexión de <nombre de aplicación>". Estas entidades interactúan con las UNI-C para pedir/liberar conexiones. Un solo solicitante de conexión podrá obtener conexiones de una o más UNI-C para un usuario de conexión conexas.
- 5) Un usuario se considera multiaccesible cuando existen dos o más enlaces SNPP que conectan el AGC a la red. Hay también un acuerdo de servicio entre el usuario y la red de manera que ésta ofrece fiabilidad, diversidad y otra característica de servicio entre las conexiones por distintos enlaces SNPP multiaccesibles.

## **8.5 Interacciones de NCC entre capas**

### **8.5.1 Llamadas de NCC a NCC**

Puede haber una llamada entre un par de NCC, aunque no haya CCC. Dicha llamada está en una misma capa. A fin de que puedan solicitarse estas llamadas, se asigna un identificador de recurso de transporte a un conjunto de SNP que hacen referencia a los recursos que se pueden usar para soportar la llamada. Esto es similar al identificador de recurso de transporte UNI asociado a recursos de transporte en la UNI.

Se puede utilizar la llamada de NCC a NCC en al menos dos casos. Primero, como una llamada que se causa en una llamada entre capas, y segundo, como otro tipo de frontera entre dominios de la misma capa.

Cuando se usa en una llamada entre capas, se utiliza un NCC de cliente para iniciar la llamada entre otro par de NCC en una capa de servidor. Cuando el NCC de la capa de cliente efectúa la llamada de la capa de servidor, se cruza una frontera de dominio. Esa frontera de dominio tiene por objeto proporcionar un punto de control de políticas, así como una separación del SNPP, además de suministrar los identificadores de recursos de transporte utilizados en las capas de servidor y de cliente. Los identificadores de recursos de transporte empleados para la petición de llamada se encuentran en la capa de servidor. Esto se ilustra en la figura 40.

La conexión de capa de servidor de las llamadas de NCC a NCC usada para soportar la correspondencia de la CI del cliente está asociada a una adaptación. Dicha llamada/conexión puede existir antes de que llegue realmente a utilizarse la adaptación.

### 8.5.2 Interacciones de espacios de nombre

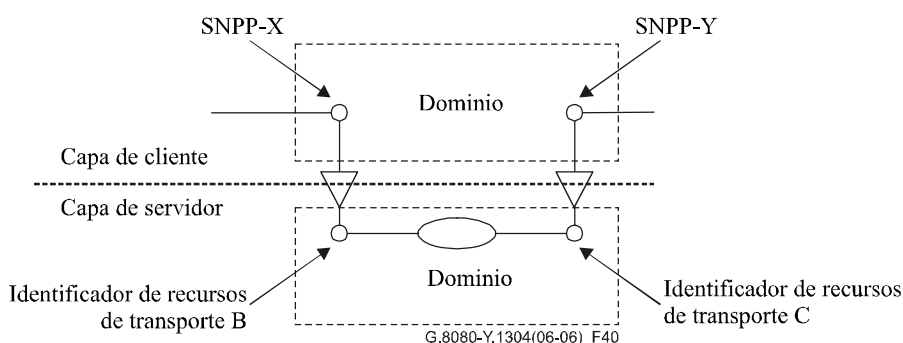
Por definición, los identificadores de recursos de transporte son globalmente únicos. No se requiere que los identificadores de recursos adicionales formen parte del espacio de identificadores de recursos de transporte de la UNI. Los identificadores de recursos de transporte asociados a las llamadas de NCC a NCC pueden provenir de espacios de identificadores diferentes.

En una misma red de capa puede haber espacios de identificadores de SNPP independientes. Se pueden crear conexiones que utilicen estos diversos espacios de identificadores de SNPP debido a que los RC entienden la correspondencia entre los identificadores de SNPP efectuada entre niveles de encaminamiento.

Si no se ha hecho una correspondencia entre dos espacios de identificadores de SNPP mediante encaminamiento, se puede hacer corresponder un espacio de identificadores de SNPP con los identificadores de recursos de transporte asociados al segundo espacio de identificadores de SNPP. Esto se podría emplear en una frontera comercial sin intercambio de encaminamiento. Un caso de esto es una frontera entre capas.

Se accede a esta correspondencia mediante una función de resolución de direcciones que recibe un identificador de SNPP como entrada y devuelve un identificador de recursos de transporte asociado a un SNPP en otro espacio de identificadores. Se tiene acceso a la resolución de direcciones existente en esta Recomendación mediante la interfaz de salida petición de directorio, del componente NCC. Se tendría acceso a la función de resolución de direcciones adicional mediante la misma interfaz de salida. En una llamada entre capas, un NCC en la frontera de la subred que representa la flexibilidad de la capa de servidor posee dos SNPP en la capa de cliente, para las que requiere una conexión. Ésta se obtiene a partir de una interrogación de ruta. El NCC de la capa de cliente utiliza la función de resolución de direcciones entre capas para obtener el recurso de transporte de capa de servidor correspondiente a esos dos SNPP de capa de cliente. Se utilizan los dos identificadores de recurso de transporte para hacer una llamada a la capa de servidor.

En la figura 40 se hace corresponder SNPP-X en la capa de servidor al identificador de recursos de transporte B, y se hace corresponder SNPP-Y al identificador de recursos de transporte C. Se puede efectuar una llamada entre capas utilizando el identificador de recursos de transporte devuelto.



**Figura 40/G.8080/Y.1304 – Interacciones de espacios de nombres**

## 9 Gestión de red de entidades del plano de control

Hay interacción entre el plano de control y el plano de gestión, como se describe en la cláusula 5. En esta cláusula se identifican algunas capacidades de gestión que puedan influir en las interacciones entre los planos de gestión y control. En particular, estas capacidades de gestión pueden incluir:

- 1) Creación y supresión de una conexión.
- 2) División de los recursos de red entre aquellos que son visibles para el plano de control y aquellos que son visibles para el plano de gestión.
- 3) Asignación de recursos de transporte a un determinado cliente para crear una RPV.
- 4) Asignación de identificadores únicos a los CTP y asignación de vinculaciones permitidas entre el CTP y sus SNP asociados.
- 5) Suministro de información de configuración y de política a la función de cribado de dirección y a la RPV, si está presente la una o la otra en el plano de control.
- 6) Establecimiento y modificación de los valores de los parámetros del sistema de señalización, tales como periodos de temporización (por ejemplo, temporización para establecimiento de la comunicación), umbrales, mecanismos de control de congestión, número máximo de conexiones permitidas, máxima carga de señalización (por encima de la cual el procesador de señalización rechaza las peticiones de establecimiento de la comunicación, etc.).
- 7) Cuando se produzca encaminamiento en el plano de gestión (centralizado):
  - cálculo de la ruta para conexiones permanentes y utilización de protocolos de gestión para gestión de conexión;
  - cálculo de la ruta para conexiones permanentes programables y suministro de una ruta explícita al plano de control.
- 8) Medición del desempeño (calidad de funcionamiento) de la llamada. Los parámetros pueden incluir:
  - tasas de petición de llamada (tasas de llegada);
  - utilización de circuito;
  - tiempo de retención de llamada;
  - tiempos de retención (el tiempo medio de retención de conexiones multiplicado por la tasa de petición de llamada indica la carga ofrecida en Erlangs);
  - promedios estadísticos calculados para el número total de peticiones de conexión en un periodo de tiempo dado;
  - una identificación de la RPV a la que pertenecen los parámetros de calidad de funcionamiento de la llamada.
- 9) Gestión del control de admisión de llamadas.
- 10) Determinación de la cantidad máxima de conexiones que pueden ser soportadas por un elemento de red y fijación, cuando sea adecuado, de la cantidad máxima que ha de ser soportada.
- 11) Distinción entre los cambios del estado de las conexiones debidos a acciones de los planos de gestión o de control y los cambios debidos a fallos de red, y supresión o generación de alarmas, cuando proceda.
- 12) Fijación o modificación de los niveles de prioridad de supervivencia o de los niveles estipulados en el contrato de calidad de servicio (QoS, *quality of service*) para todas las conexiones asociadas con una "clase de calidad de funcionamiento" dada.

- 13) Asignación del valor máximo de un identificador de conexión en un enlace donde sea apropiado, fijación de controles de gestión de tráfico, sea manualmente como resultado, de una entrada específica, sea automáticamente en respuesta a estímulos internos o externos. (En el caso de control automático, el sistema de gestión fija las condiciones en las que se aplica el control y la magnitud de la respuesta.)
- 14) Activación o desactivación de "encaminamiento directo y encaminamiento alterno".
- 15) Soporte de esquemas de reencaminamiento temporal.
- 16) Gestión de la red de señalización para asegurar una configuración coherente de los recursos de señalización.
- 17) Determinación de los atributos de los enlaces de señalización, incluidos su estado funcional, indicaciones de error, datos de tráfico o ancho de banda máximo.
- 18) Migración de una conexión permanente (PC) a una conexión permanente programable (SPC), donde los recursos de transporte relacionados con la PC son asignados al plano de control sin interrupción del servicio.

## **10 Identificadores**

### **10.1 Espacios de nombres**

Hay tres espacios de nombre de transporte separados en la sintaxis de denominación de ASON:

- 1) Espacio de nombre de área de encaminamiento.
- 2) Espacio de nombre de subred.
- 3) Espacio de nombre de contexto de enlace.

Los dos primeros espacios siguen a la estructura de subred de transporte y no tienen que estar relacionados. Tomados en conjunto, definen el punto topológico donde está situado un SNPP. El espacio de nombre de contexto especifica dentro del SNPP dónde está el SNP. Se puede usar para reflejar la estructura de subagrupaciones de SNPP y diferentes tipos de nombres de enlace.

Un nombre SNPP es una concatenación de:

- uno o más nombres de área de encaminamiento anidados;
- un nombre de subred opcional dentro del nivel de área de encaminamiento más bajo. Éste sólo puede existir si están presentes los nombres de RA contenedores;
- uno o más nombres de contexto de recursos anidados.

Al utilizar este diseño, el nombre SNPP puede recurrir con áreas de encaminamiento hacia la subred más baja y subdivisiones de enlace (subagrupaciones de SNPP). Este esquema permite que los SNP sean identificados en cualquier nivel de interfuncionamiento.

**Nombre SNP:** A un SNP se da una dirección utilizada para asignación de conexión de enlace y, en algunos casos, encaminamiento. El nombre SNP se deriva del nombre SNPP concatenado con un índice SNP significativo localmente.

Un alias SNPP representa un nombre SNPP alternativo para el mismo enlace SNPP, que puede generarse a partir de otro espacio de nombres SNPP.

NOTA – El alias SNPP puede ser generado a partir del mismo espacio de nombre SNPP o de otro diferente. Si está presente en un área de encaminamiento, está disponible para el RC asociado con la RA.

### **10.2 Nombres y direcciones**

Los nombres y direcciones proporcionan a los componentes del plano de control los medios necesarios de identificación que les permiten controlar cooperativamente los recursos de una red de transporte. Conforme a lo definido en la Rec. UIT-T G.8081/Y.1353, las direcciones dependen de la

ubicación, mientras que los recursos no. Es importante señalar que un identificador dado puede utilizarse como nombre en un contexto y como dirección en otro. Por ejemplo, considérese el área de encaminamiento A que se muestra en la figura 11 de 6.3. Al interior del área de encaminamiento A, el identificador de SNP local es una dirección, mientras que el identificador de SNP de interfaz es un nombre. Sin embargo, al exterior del área de encaminamiento, el identificador SNP de interfaz puede ser una dirección en el contexto de otra área de encaminamiento (que no se muestra en la figura).

Diversas entidades en el plano de control ASON necesitan nombres y direcciones, como se describe a continuación:

### **Recurso de transporte E-NNI**

Al enlace SNPP E-NNI se le puede asignar un nombre para que los controladores de llamada de red especifiquen los E-NNI. Estos nombres deben ser globalmente únicos y son asignados por la red ASON. Se pueden asignar múltiples nombres al enlace SNPP. Puede existir un alias para un conjunto de identificadores de recursos de transporte E-NNI, por ejemplo cuando la llamada debe atravesar varios dominios y el usuario puede especificar el dominio de tránsito, pero no una E-NNI en particular.

Cuando existe el punto de referencia E-NNI entre un dominio de cliente RPV y una RPV en un dominio de proveedor de servicio, el identificador del recurso de transporte puede ser único entre todos los demás enlaces SNPP E-NNI asignados a la RPV y no necesariamente ser globalmente único. Puede ser asignado por el cliente RPV o por la red ASON.

**Recurso de transporte UNI:** El enlace SNPP UNI requiere una dirección para el controlador de llamada de parte llamante y el controlador de llamada de red, para especificar destinos. Estas direcciones deben ser globalmente únicas y son asignadas por la red ASON. Se pueden asignar múltiples nombres al enlace SNPP. Los identificadores de recursos de transporte pueden guardar una relación 1:N o N:1 con los enlaces SNPP. Esto permite a una parte llamante/llamada asociar diferentes aplicaciones con direcciones específicas a través de un enlace común. Puede existir un alias para un conjunto de identificadores de recursos de transporte UNI.

**Controlador de protocolo del controlador de encaminamiento:** El controlador de protocolo del controlador de encaminamiento (RCPC, *routing controller protocol controller*) necesita una dirección RCD para intercambiar mensajes del protocolo de encaminamiento con RCPC pares. El controlador de protocolo del controlador de encaminamiento debe también tener un nombre que lo identifique ante los pares, a efectos de mantener las relaciones del protocolo de encaminamiento.

**Controlador de encaminamiento:** El controlador de encaminamiento necesita un nombre que lo identifique como la fuente de la información de topología que suministra y comparte con otros RC.

**Controlador de protocolo del controlador de llamadas de red:** El controlador de llamadas de red necesita una dirección RCD para intercambiar mensajes de señalización de llamada. El controlador de protocolo del controlador de llamadas de red también debe tener un nombre que lo identifique ante los pares a efectos de mantener las relaciones de señalización de llamadas.

**Controlador de protocolo del controlador de conexión:** El Controlador de protocolo del controlador de conexión necesita una dirección RCD para intercambiar mensajes de señalización de conexión. Estas direcciones son únicas en el ámbito de un dominio administrativo. El controlador de protocolo del controlador de conexión puede tener un nombre que lo identifique ante los pares a efectos de mantener las relaciones de señalización de la conexión.

**Controlador de protocolo del controlador de llamada de parte llamante/llamada:** El controlador de llamada de parte llamante/llamada necesita una dirección RCD para intercambiar mensajes de señalización de las llamadas. El controlador de llamada de parte llamante/llamada también debe tener un nombre que lo identifique ante los pares a efectos de mantener las relaciones de señalización de llamadas.



**Subred:** Se da a una subred una dirección que representa la colección de todos los SNP en esa red, y que se utiliza para encaminamiento de conexión. La dirección es única dentro del alcance de un dominio administrativo.

**Área de encaminamiento:** Se da a un área de encaminamiento una dirección que representa la colección de todos los SNPP en esa área de encaminamiento que se utiliza para encaminamiento de conexión.

### 10.3 Relaciones entre los identificadores

Los recursos de transporte pueden verse afectados tanto por los componentes del plano de control como por los componentes del plano de gestión (véase 5.2). Como resultado de ello, se hará referencia a los recursos de transporte mediante identificadores dependientes del contexto. Para que las aplicaciones de estos contextos diferentes puedan intercambiar información acerca del recurso común, se necesita una correspondencia entre los identificadores de recursos de transporte usados en el contexto del plano de gestión y aquéllos utilizados en el contexto del plano de control.

También se requiere una correspondencia del conjunto de identificadores de los recursos del plano de transporte utilizados por el plano de control. Por ejemplo, para hacer corresponder un identificador de recursos de transporte con uno o varios SNPP.

En la presente Recomendación no se tratan en detalle las correspondencias entre identificadores, las cuales se describen en las Recomendaciones UIT-T pertinentes de la serie G.771x.x.

## 11 Técnicas de mejoramiento de la disponibilidad de la conexión

En esta cláusula se describen las estrategias que pueden utilizarse para mantener la integridad de una llamada existente en caso de fallos en la red de transporte.

La Rec. UIT-T G.805 describe técnicas de mejoramiento de la disponibilidad de red de transporte. Los términos "protección" (sustitución de un recurso que ha fallado, por un recurso de reserva activa (preasignado) y "restauración" (sustitución de un recurso que ha fallado, por reencaminamiento mediante el uso de capacidad de reserva) se utilizan para clasificar estas técnicas. En general, las acciones de protección se ejecutan en lapsos de tiempo en la gama de decenas de milisegundos, mientras que las acciones de restauración normalmente se ejecutan en lapsos de tiempo comprendidos entre centenas de milisegundos y algunos segundos.

El plano de control de la ASON proporciona a un operador de red la aptitud para ofrecer al usuario llamadas con una clase de servicio (CoS, *class of service*) (por ejemplo, disponibilidad, duración de las interrupciones, segundos con error, etc.) seleccionable. La protección y la restauración son mecanismos (utilizados por la red) para soportar la CoS solicitada por el usuario. La selección del mecanismo de supervivencia (protección, restauración o ninguna de las dos) para una determinada conexión que soporta una llamada se basará en la política del operador de red, la topología de la red y la capacidad del equipo desplegado. Se pueden utilizar diversos mecanismos de supervivencia en las conexiones que están concatenadas a fin de suministrar una llamada. Si una llamada se transmite por la red de más de un operador, cada red debe ser responsable de la supervivencia de las conexiones de tránsito. Las peticiones de conexión en la UNI o E-NNI contendrán solamente la CoS solicitada, y no un tipo de protección o restauración explícito.

La protección o restauración de una conexión se puede invocar o inhabilitar temporalmente mediante un comando proveniente del plano de gestión. Estos comandos se pueden utilizar para permitir que se efectúen actividades de gestión calendarizadas. También pueden utilizarse para dejar sin efecto operaciones automáticas en algunas condiciones de fallo excepcionales.

El mecanismo de protección o restauración debe:

- ser independiente del tipo de cliente y debe soportar cualquier tipo de cliente (por ejemplo, IP, ATM, SDH, Ethernet);
- proporcionar escalabilidad para acomodar un fallo catastrófico en una capa servidora, como en el caso de rotura de un cable de fibra, que repercute en un gran número de conexiones de capa de cliente que deberán ser restauradas simultánea y rápidamente;
- utilizar un mecanismo de señalización robusto y eficiente, que continúe funcionando incluso después de un fallo en la red de transporte o de señalización;
- no confiar en funciones que no sean críticas respecto al tiempo para iniciar acciones de protección o restauración. Por lo tanto, se deben considerar esquemas de protección o restauración que no dependan de la localización de avería.

La descripción de la forma en que habrán de utilizarse las capacidades de protección y restauración por los planos de transporte, control y gestión de una red habilitada ASON queda en estudio.

### **11.1 Protección**

La protección es un mecanismo para mejorar la disponibilidad de una conexión a través del uso de capacidad asignada adicional. Una vez que se ha asignado capacidad para fines de protección, no hay reencaminamiento y los SNP asignados en puntos intermedios para soportar la capacidad de protección no cambian como resultado de un evento de protección. El plano de control, específicamente el componente de control de conexión, es responsable de la creación de una conexión. Esto incluye crear una conexión de trabajo y una conexión de protección, o proporcionar información de configuración específica de la conexión para un esquema de protección. Para la protección del plano de transporte, la configuración de protección se hace bajo la dirección del plano de gestión. Para la protección del plano de control, la configuración de protección está bajo la dirección del plano de control y no del plano de gestión.

La protección del plano de control se produce entre el controlador de conexión de origen y el controlador de conexión de destino de un dominio de protección del plano de control, donde el origen y el destino se definen en relación con la conexión. El funcionamiento del mecanismo de protección es coordinado entre el origen y el destino. En caso de un fallo, la protección no supone reencaminamiento ni establecimiento de conexión adicional en controladores de conexión intermedios, sólo intervienen los controladores de conexión de origen y de destino. Ésta es la principal diferencia entre protección y restablecimiento.

### **11.2 Restablecimiento**

El restablecimiento de una llamada es la sustitución de una conexión que ha fallado mediante el reencaminamiento de la llamada utilizando capacidad de reserva. En contraste con la protección, algunos o todos los SNP utilizados para soportar la conexión pueden ser modificados durante un evento de restablecimiento. El restablecimiento del plano de control se produce en relación con dominios de reencaminamiento. Un dominio de reencaminamiento es un grupo de controladores de llamada y de conexión que comparten el control del reencaminamiento basado en el dominio. Los componentes en los bordes de los dominios de reencaminamiento coordinan operaciones de reencaminamiento basadas en el dominio para todas las llamadas/conexiones que atraviesan el dominio de reencaminamiento. Un dominio de reencaminamiento debe estar contenido enteramente dentro de un dominio o área de control de encaminamiento. Un dominio de control de encaminamiento puede contener totalmente varios dominios de reencaminamiento. Por tanto, los recursos de red asociados con un dominio de reencaminamiento deben estar contenidos totalmente dentro de un área de encaminamiento. Cuando una llamada/conexión es reencaminada dentro de un dominio de reencaminamiento, la operación de reencaminamiento basada en el dominio se produce entre los bordes del dominio de reencaminamiento y está totalmente contenida dentro de éste.

La activación de un servicio de reencaminamiento es negociada como parte de la fase inicial de establecimiento de la comunicación. Para un solo dominio, se negocia un servicio de reencaminamiento dentro del dominio entre los componentes de origen (controladores de conexión y llamada) y de destino (controladores de conexión y llamada) dentro del dominio de reencaminamiento. Las peticiones de un servicio de reencaminamiento dentro del dominio no atraviesan la frontera de dominio.

Cuando hay múltiples dominios de reencaminamiento que participan, los componentes de borde de cada dominio de reencaminamiento negocian la activación de los servicios de reencaminamiento a través del dominio de reencaminamiento para cada llamada. Una vez que la comunicación ha sido establecida, cada uno de los dominios de reencaminamiento en el trayecto de la llamada tienen conocimiento de los servicios de reencaminamiento que están activados para la llamada. Como para el caso de un solo dominio de reencaminamiento, una vez que la comunicación ha sido establecida, los servicios de reencaminamiento no pueden ser renegociados. Esta negociación también permite que los componentes asociados con las partes llamante y llamada pidan un servicio de reencaminamiento. En este caso, el servicio se denomina servicio entre dominios, porque las peticiones son pasadas a través de fronteras de dominios de reencaminamiento. Aunque se puede solicitar un servicio de reencaminamiento para cada llamada de extremo a extremo, el servicio se proporciona dominio por dominio de encaminamiento (es decir, entre los componentes de origen y de destino dentro de cada dominio de reencaminamiento atravesado por la llamada).

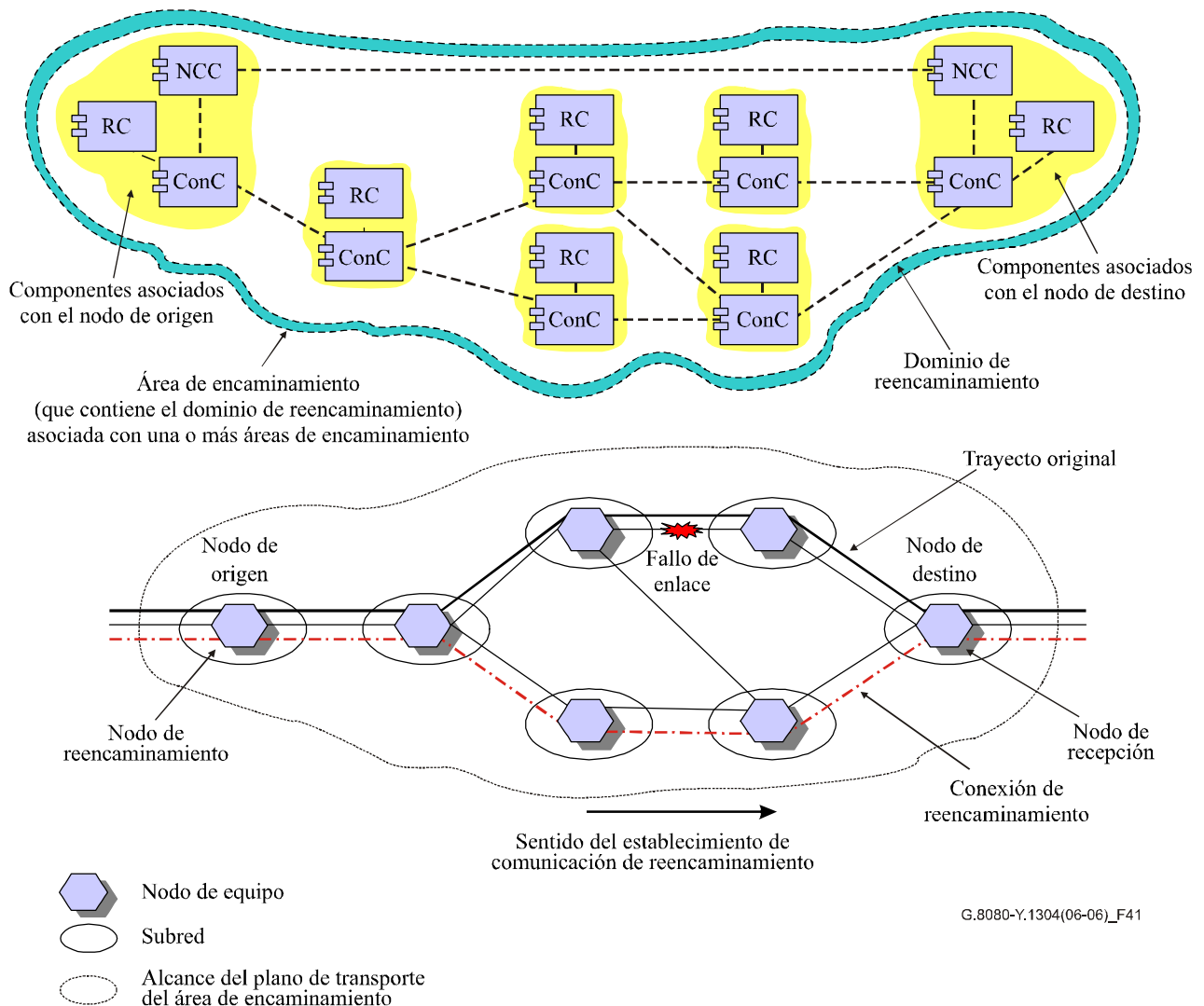
Durante la negociación de los servicios de reencaminamiento, los componentes de borde de un dominio de reencaminamiento intercambian sus capacidades de reencaminamiento y la petición de un servicio de reencaminamiento sólo puede ser soportada si el servicio está disponible en el origen y en el destino en el borde del dominio de reencaminamiento.

Un servicio de reencaminamiento rígido ofrece un mecanismo de restablecimiento de las llamadas, siempre en respuesta a un evento de fallo. Cuando falla un enlace o un elemento de red en un dominio de reencaminamiento, la llamada es liberada hasta los bordes del dominio de reencaminamiento. Para un servicio de reencaminamiento rígido que ha sido activado para esa llamada, el origen bloquea la liberación de llamada e intenta crear un segmento de conexión alternativa al destino en el borde del dominio de reencaminamiento. Esta conexión alternativa es la conexión de reencaminamiento. El destino en el borde del dominio de reencaminamiento bloquea también la liberación de la llamada y espera que el origen en el borde del dominio de reencaminamiento cree la conexión de reencaminamiento. En el reencaminamiento rígido, el segmento de conexión original es liberado antes de la creación de un segmento de conexión alternativa. Esto se denomina "romper antes de construir". Un ejemplo de reencaminamiento rígido se muestra en la figura 41. En este ejemplo el dominio de control de encaminamiento está asociado con un área de encaminamiento y un solo dominio de reencaminamiento. La llamada es reencaminada entre los nodos de origen y de destino y los componentes asociados con ellos.

El servicio de reencaminamiento flexible es un mecanismo para reencaminar una conexión con fines administrativos (por ejemplo, optimización del trayecto, mantenimiento de red y trabajos de ingeniería planificados). Cuando se activa una operación de reencaminamiento (generalmente mediante una petición del plano de gestión) y se envía al lugar de los componentes de reencaminamiento, éstos establecen una conexión de reencaminamiento al lugar de los componentes prefijados. Una vez creada la conexión de reencaminamiento, los componentes de reencaminamiento utilizan la conexión de reencaminamiento y suprimen la conexión inicial. Esto se denomina "construir antes de romper".

En un procedimiento de reencaminamiento flexible, puede producirse un fallo en la conexión inicial. En este caso, la operación de reencaminamiento rígido se apropia de la operación de reencaminamiento flexible y los componentes de origen y de destino dentro del dominio de reencaminamiento aplican el proceso de reencaminamiento rígido.

Si se requiere un comportamiento reversivo (es decir, la llamada debe ser restablecida a las conexiones originales cuando el fallo ha sido reparado), los controladores de llamada de red no deben liberar las conexiones originales (que han fallado). Los controladores de llamada de red deben continuar supervisando las conexiones originales y, cuando el fallo es reparado, la llamada es restablecida a las conexiones originales.



G.8080-Y.1304(06-06)\_F41

**Figura 41/G.8080/Y.1304 – Ejemplo de reencaminamiento rígido**

## 11.2.1 Reencaminamiento en respuesta a un fallo

### 11.2.1.1 Fallos dentro del dominio

Todos los fallos dentro de un dominio de reencaminamiento deben resultar en una acción de reencaminamiento (restablecimiento) dentro de ese dominio, de modo que cualesquiera dominios hacia el destino sólo observen un fallo de señal entrante momentáneo (o fallo de la sección anterior). Las conexiones que soportan la llamada deben continuar utilizando los mismos nodos de pasarela de origen (ingreso) y de destino (egreso) en el dominio de reencaminamiento.

### 11.2.1.2 Fallos entre dominios

Se han de considerar dos casos de fallo: el fallo de un enlace entre dos elementos de red de pasarela en diferentes dominios de reencaminamiento y el fallo de elementos de red de pasarela entre dominios.

### 11.2.1.3 Fallo de enlace entre elementos de red de pasarela adyacentes

Cuando se produce un fallo fuera de los dominios de reencaminamiento (por ejemplo, el enlace entre elementos de red de pasarela en diferentes dominios de reencaminamiento A y B en la figura 42-a), no se puede ejecutar ninguna operación de reencaminamiento. En este caso, es posible emplear los mecanismos de protección alternativos entre los dominios.

La figura 42-b muestra el ejemplo con dos enlaces entre los dominios A y B. La función de selección de trayecto en el extremo A (de origen) de la llamada debe seleccionar un enlace entre dominios con el nivel de protección apropiado. En este caso, el método más sencillo para proporcionar protección es a través de un mecanismo de protección preestablecido (por ejemplo, en una red de capa de servidor; este esquema es transparente a las conexiones que pasan por encima de ésta). Si el enlace protegido falla, el esquema de protección de enlace iniciará la operación de protección. En este caso, la llamada es encaminada aún por los mismos elementos de red de pasarela de ingreso y de egreso de los dominios adyacentes y la recuperación tras el fallo está confinada al enlace entre dominios.

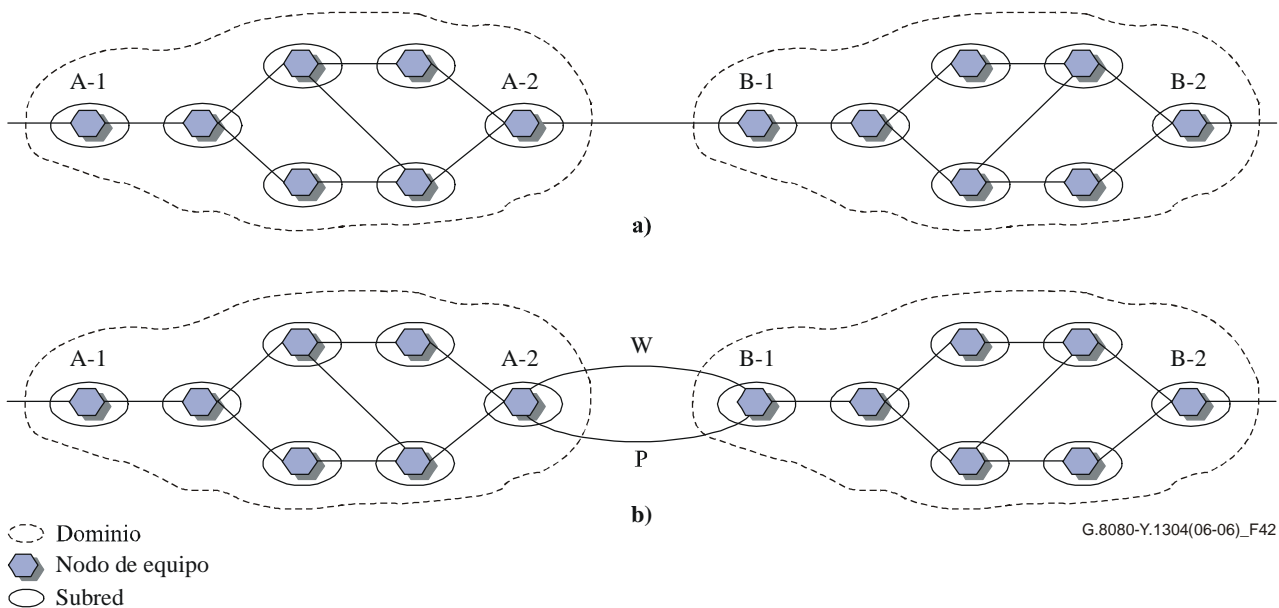
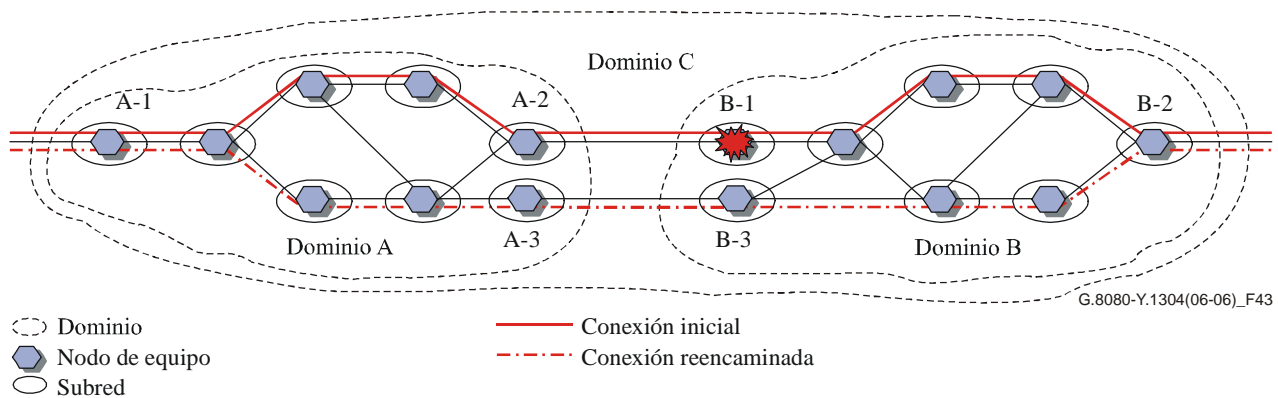


Figura 42/G.8080/Y.1304 – Escenarios de fallos de enlaces

### 11.2.1.4 Fallo de elementos de red de pasarela

Este caso se muestra en la figura 43. Para restablecer una llamada cuando B-1 falla, se debe utilizar un nodo de pasarela diferente, B-3, para el dominio B. En general, esto requerirá el uso de una pasarela diferente en el dominio A, en este caso A-3. En respuesta al fallo del elemento de red de pasarela B-1 (detectado por el elemento de red de la pasarela A-2), el nodo de origen en el dominio A, A-1, debe emitir una petición de una nueva conexión para soportar la llamada. La indicación a este nodo debe señalar que se ha de evitar el reencaminamiento dentro del dominio A entre A-1 y A-2, y que se requiere una nueva ruta y trayecto a B-2. Esto se puede considerar como reencaminamiento en un dominio mayor, C, que se produce solamente si el reencaminamiento en A o en B no puede restablecer la conexión.



**Figura 43/G.8080/Y.1304 – Reencaminamiento en caso de fallo de un elemento de red de pasarela**

## 12 Resiliencia

La resiliencia es la capacidad de que el plano de control continúe funcionando en condiciones de fallo. El funcionamiento del plano de control depende de elementos de la red de comunicaciones de datos (RCD), del plano de transporte, del plano de gestión y de los componentes internos del propio plano de control (véase la figura 1). En el apéndice II figura información adicional.

### 12.1 Principios de interacciones de los planos de control y de transporte

Se aplican los siguientes principios para las interacciones de los planos de control y de transporte cuando las comunicaciones están disponibles entre los dos planos:

- 1) El plano de control se basa en el plano de transporte para la información sobre los recursos del plano de transporte.
- 2) La compatibilidad entre la visión del plano de control y el correspondiente elemento de red de transporte se establece primero (compatibilidad vertical).
- 3) Una vez establecida la compatibilidad, se intenta la compatibilidad horizontal. En este caso, los componentes del plano de control se sincronizan con sus componentes adyacentes. Esto se utiliza para restablecer una visión compatible del estado del encaminamiento, de la llamada y de la conexión.

Otro principio de interacción de los planos de control y de transporte es que:

- 4) Las conexiones existentes en el plano de transporte no son alteradas si el plano de control falla y/o se restablece. Los componentes del plano de control son por consiguiente dependientes del estado de la SNC.

Para la resiliencia, la información de los recursos del plano de transporte y del estado de la SNC debe ser mantenida en un almacenamiento no volátil. Se debe almacenar alguna información ulterior sobre el uso del plano de control de la SNC. Esto incluye si la SNC fue creada por la gestión de conexión y cómo fue utilizada. Por ejemplo, cuál es el extremo de la SNC hacia el extremo de cabecera de toda la conexión. En un nodo dado, el plano de control debe asegurar que tiene información sobre recursos del estado de la SNC que concuerda con la información del estado de los recursos de la SNC mantenida por el NE de transporte. De no ser así, los componentes de control responsables de ese nodo deben:

- advertir que no hay anchura de banda disponible a los nodos adyacentes para asegurar que no habrá peticiones de la red de encaminar una nueva conexión a través de ese nodo;
- no realizar ningún cambio de conexión (por ejemplo, liberación).

El estado de la SNC es la información más importante para el restablecimiento, en primer lugar porque es la base de conexiones que proporcionan servicio a usuarios de extremo. Esto sigue el principio anterior. Durante el restablecimiento, el plano de control reconstruye el estado de la llamada y de la conexión correspondiente a las conexiones existentes. Por ejemplo, el encaminamiento tendrá que difundir información de SNP correcta después de que es sincronizado por los componentes del plano de control local (LRM).

La concordancia del restablecimiento de información del plano de control con el NE del plano de transporte debe producirse en la siguiente secuencia:

- el gestor de recursos de enlace se sincroniza con la información de estado del NE de transporte;
- el controlador de conexión se sincroniza después con el gestor de recursos de enlace;
- el controlador de llamada de red se sincroniza después con el controlador de conexión.

Tras el restablecimiento de la concordancia de estado local, el plano de control debe asegurar entonces la concordancia de la información del estado de la SNC con nodos adyacentes, como se expone en el principio 3 anterior, antes de participar en las peticiones de establecimiento o liberación de conexiones del plano de control.

## **12.2 Principio de comunicación del controlador de protocolo**

Cuando se interrumpe la comunicación entre controladores de protocolo, las llamadas existentes y sus conexiones no son alteradas. Se puede notificar al plano de gestión si el fallo persiste y requiere intervención del operador (por ejemplo, para liberar una llamada).

Un fallo de la RCD puede afectar a una o más sesiones de comunicación de controlador de protocolo a controlador de protocolo. El controlador de protocolo asociado con cada canal de señalización debe detectar y notificar una alarma de un fallo del canal de señalización.

Cuando se restablece la sesión de comunicación de controlador de protocolo a controlador de protocolo, se debe efectuar la resincronización de estados entre controladores de protocolo.

El fallo de un controlador de protocolo se trata de manera similar al fallo de una sesión de controlador de protocolo a controlador de protocolo.

## **12.3 Interacciones de los planos de control y de gestión**

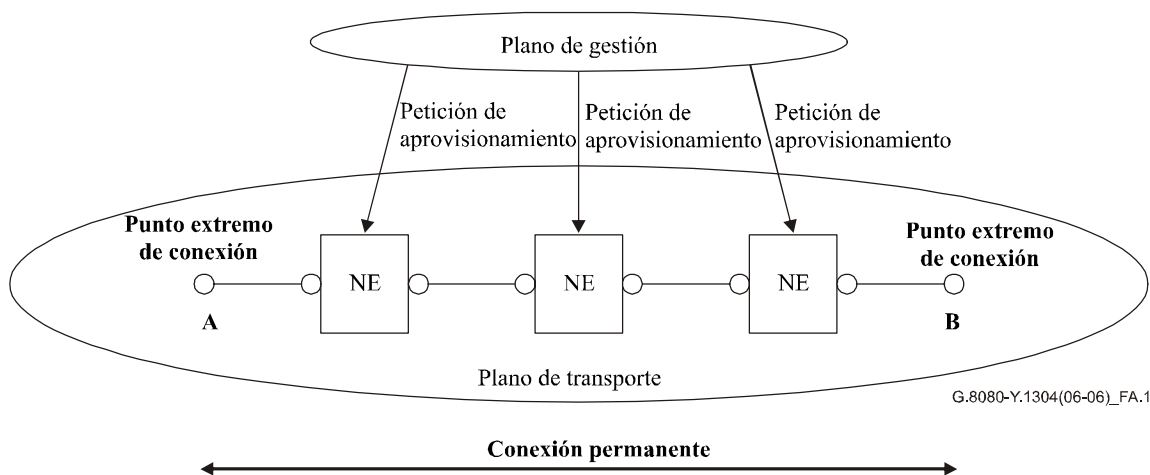
Cuando las funciones del plano de gestión no están disponibles, se pueden degradar varias funciones de control. Cuando las funciones del plano de control están disponibles de nuevo, los componentes del plano de control pueden tener que informar al plano de gestión las acciones que ejecutaron mientras el plano de gestión no estaba disponible (por ejemplo, registros de llamadas).

## Anexo A

### Servicios de conexión

El control de conectividad es fundamental para el funcionamiento de las redes de transporte. Puede describirse la red de transporte como un conjunto de redes de capas, cada una de las cuales actúa como una función de conexión mediante la cual se crean y suprimen asociaciones entre las entradas y las salidas de las funciones. Estas asociaciones se denominan conexiones. Se definen tres tipos de establecimiento de conexión:

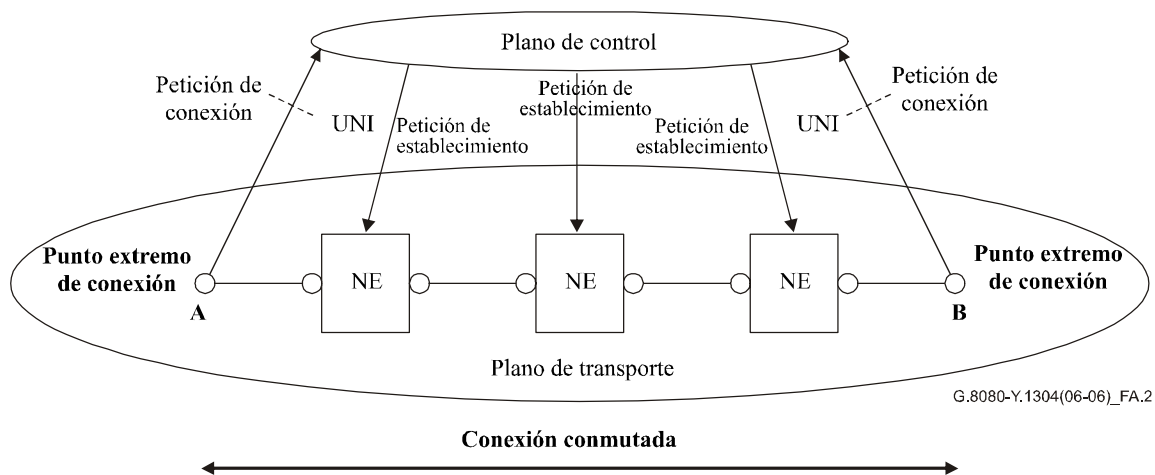
- 1) **Conexión permanente:** Este tipo de conexión se establece suministrando a cada elemento de red a lo largo del trayecto la información necesaria para establecer la conexión extremo a extremo. El aprovisionamiento de información se logra bien a través de los sistemas de gestión o por intervención manual. Si se utiliza un sistema de gestión de red, suele ser necesario emplear un modelo de bases de datos de la red para establecer, en primer lugar, la ruta más adecuada y luego enviar instrucciones a los elementos de red que soportan la conexión. Este tipo de conexión se denomina conexión física permanente. Véase la figura A.1. Nota: En la arquitectura de G.8080/Y.1304 no se describen las conexiones permanentes.



**Figura A.1/G.8080/Y.1304 – Ejemplo de establecimiento de una conexión de transporte extremo a extremo utilizando aprovisionamiento a través del plano de gestión**

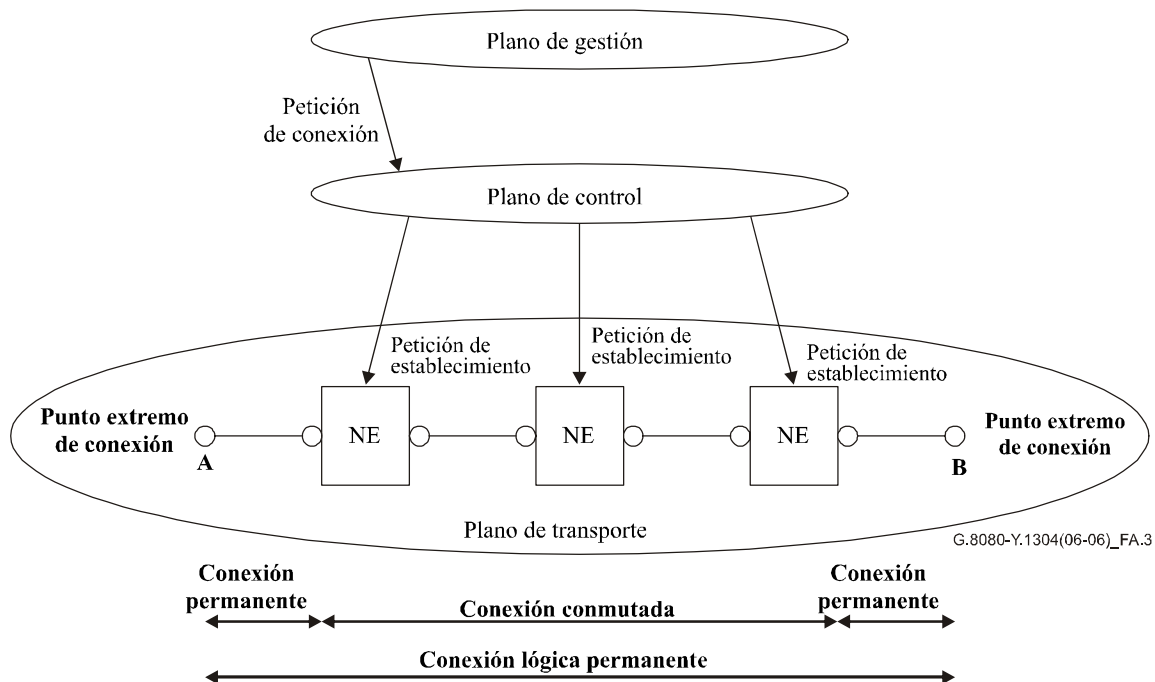
- 2) **Conexión conmutada (SC, *switched connection*):** Este tipo de conexión se establece, intercambiando mensajes de señalización de protocolo dinámico, a petición de los puntos extremos del plano de control de comunicación que se están comunicando. Estos mensajes atraviesan la I-NNI o la E-NNI del plano de control. Este tipo de conexión se denomina conexión conmutada. Estas conexiones requieren sistemas de asignación de nombres y direcciones de red y protocolos del plano de control. Véase la figura A.2.





**Figura A.2/G.8080/Y.1304 – Ejemplo de establecimiento de una conexión de transporte extremo a extremo utilizando señalización del plano de control (conexión conmutada de A a B)**

- 3) **Conexión lógica permanente (SPC, *soft permanent connection*):** Este tipo de establecimiento de la conexión consiste en que la red proporciona una conexión permanente en la frontera de la red al tiempo que utiliza una conexión conmutada dentro de la red para proporcionar conexiones extremo a extremo entre las conexiones permanentes en las fronteras de la red. Las conexiones se establecen mediante señalización generada por la red y usando protocolos de encaminamiento. El establecimiento de estas conexiones depende de la definición de la NNI. Por consiguiente, sólo es necesario proporcionar las conexiones en la frontera. No se define la UNI. Este tipo de conexión de red se conoce como conexión lógica permanente (SPC). Desde la perspectiva de los puntos extremos, la conexión lógica permanente no se diferencia de la conexión permanente, provista y controlada mediante gestión. Véase la figura A.3.



**Figura A.3/G.8080/Y.1304 – Ejemplo de establecimiento de una conexión de transporte de extremo a extremo como conexión lógica permanente (SPC)**

Lo que más diferencia los tres métodos anteriores es la parte que establece la conexión. En el caso de la conexión aprovisionada, el establecimiento de la conexión es responsabilidad del operador de la red, mientras que en la señalizada el establecimiento de la conexión puede también ser responsabilidad del usuario. Adicionalmente, debería admitirse la señalización de terceros a través de la UNI.

NOTA 1 – El tipo de conexión puede repercutir en los futuros sistemas de facturación.

El plano de control soportará una conexión conmutada (SC) o una conexión lógica permanente (SPC) de las contempladas en la capacidad de conexión básica de la red de transporte. A continuación se definen estos tipos de capacidad de conexión.

- Conexión unidireccional punto a punto.
- Conexión bidireccional punto a punto.
- Conexión unidireccional punto a multipunto.

NOTA 2 – Podría contemplarse otro tipo de conexión, la conexión asimétrica. Ésta se podría constituir bien como dos conexiones unidireccionales punto a punto, con propiedades diferentes en cada sentido, o como un caso especial de la conexión bidireccional.

La función de una UNI consiste en pasar mensajes de señalización directamente a la entidad del plano de control de la red. De forma alternativa, si el operador de la red ya cuenta con grandes sistemas de gestión para planificar las asignaciones y efectuar la autoconfiguración, los mensajes de señalización podrían pasarse directamente a los agentes de los sistemas de gestión del servicio y de gestión de la red para que establezcan la conexión. Esta aplicación permitirá prestar el servicio de forma automática, prácticamente en tiempo real, con las plataformas de gestión actuales.

## Apéndice I

### Redes de capa ASON

La red óptica conmutada automática (ASON, *automatic switched optical network*) se puede aplicar a redes de capa. En el cuadro I.1 se presentan ejemplos de redes de capa definidas en otras Recomendaciones UIT-T. La ASON también se puede aplicar a otras redes de capa, incluido el soporte de las cabidas útiles virtualmente concatenadas.

**Cuadro I.1/G.8080/Y.1304 – Redes de capa: SDH, OTN y PDH**

SDH	Trayecto LOVC	VC-11
		VC-12
		VC-2
		VC-3
Trayecto HOVC	VC-4	
	VC-4-4c	
	VC-4-16c	
	VC-4-64c	
	VC-4-256c	
Sección	M <sub>n</sub> , n = 1, 4, 16, 64, 256	
	R <sub>n</sub> , n = 1, 4, 16, 64, 256	
	ES1	
	O <sub>n</sub> , n = 1, 4, 16, 64, 256	
	sSTM-1k, k = 1, 2, 4, 8, 16	
	sSTM-2n, n = 1, 2, 4	
	E31/P31s	
E4/P4s		

OTN	Trayecto digital	ODU1
		ODU2
		ODU3
	Sección digital	OTU <sub>k</sub> , k = 1, 2, 3
	Trayecto óptico	OCh
	Sección	OMS <sub>n</sub>
		OTS <sub>n</sub>
		OPS <sub>n</sub>

PDH	Trayecto	P11 <sub>x</sub> , P11 <sub>s</sub>
		P12 <sub>x</sub> , P12 <sub>s</sub>
		P21 <sub>x</sub>
		P22 <sub>x</sub> , P22 <sub>e</sub>
		P31 <sub>x</sub> , P31 <sub>e</sub>
		P32 <sub>x</sub> , P32
		P4 <sub>x</sub> , P4 <sub>e</sub>
	Sección	Eq, q = 11, 12, 21, 22, 31, 32, 4

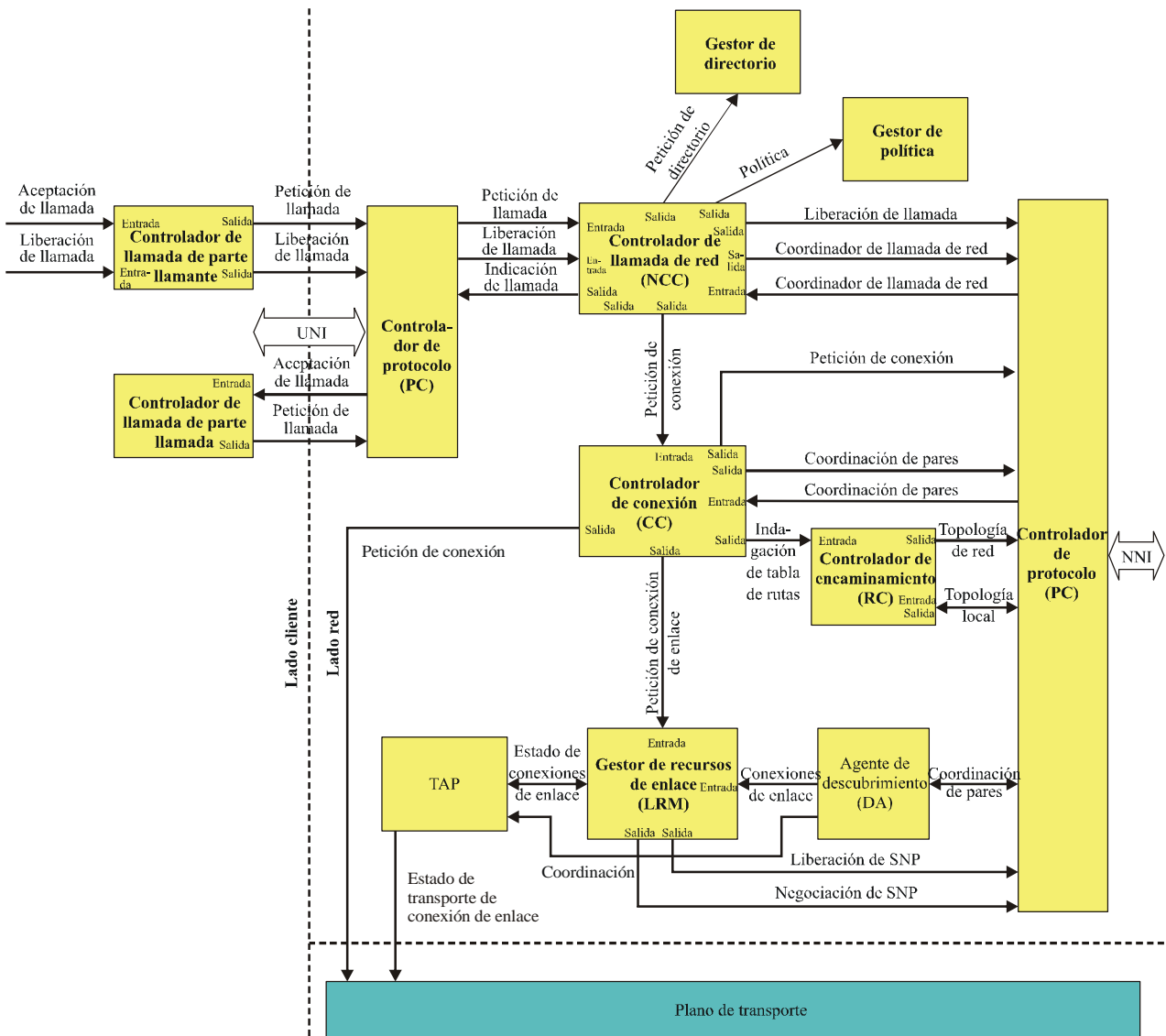
## Apéndice II

### Ejemplo ilustrativo de implementaciones

La arquitectura de la red óptica con conmutación automática se define desde el punto de vista de diversas.

La arquitectura, especificada en esta Recomendación, permite la flexibilidad en la implementación y reconoce que los operadores de redes pueden tener prácticas diferentes. La arquitectura reconoce también que las funciones pueden ser implementadas de varias maneras. Además, dependiendo de la funcionalidad requerida, no todos los componentes pueden ser necesarios. Por ejemplo, la arquitectura descrita en esta Recomendación proporciona flexibilidad de encaminamiento y permite encaminamiento centralizado y distribuido. En el caso de encaminamiento distribuido, hay interacciones entre varias funciones de controlador de encaminamiento, mientras que en un esquema centralizado, el encaminamiento puede ser mantenido como una alternativa por el plano de gestión, suprimiendo la necesidad de un componente de controlador de encaminamiento. Las peticiones de circuitos, incluidas sus rutas, son transferidas del plano de gestión al plano del control.

Aunque se proporciona flexibilidad dentro de la arquitectura, las interfaces y los flujos de información definidos permiten la interconexión de los distintos componentes. Un ejemplo de esto se ilustra en la figura II.1. Otro ejemplo se ilustra en la figura III.1.



G.8080-Y.1304(06-06)\_FII.1

Figura II.1/G.8080/Y.1304 – Ejemplo ilustrativo de interconexión de componentes

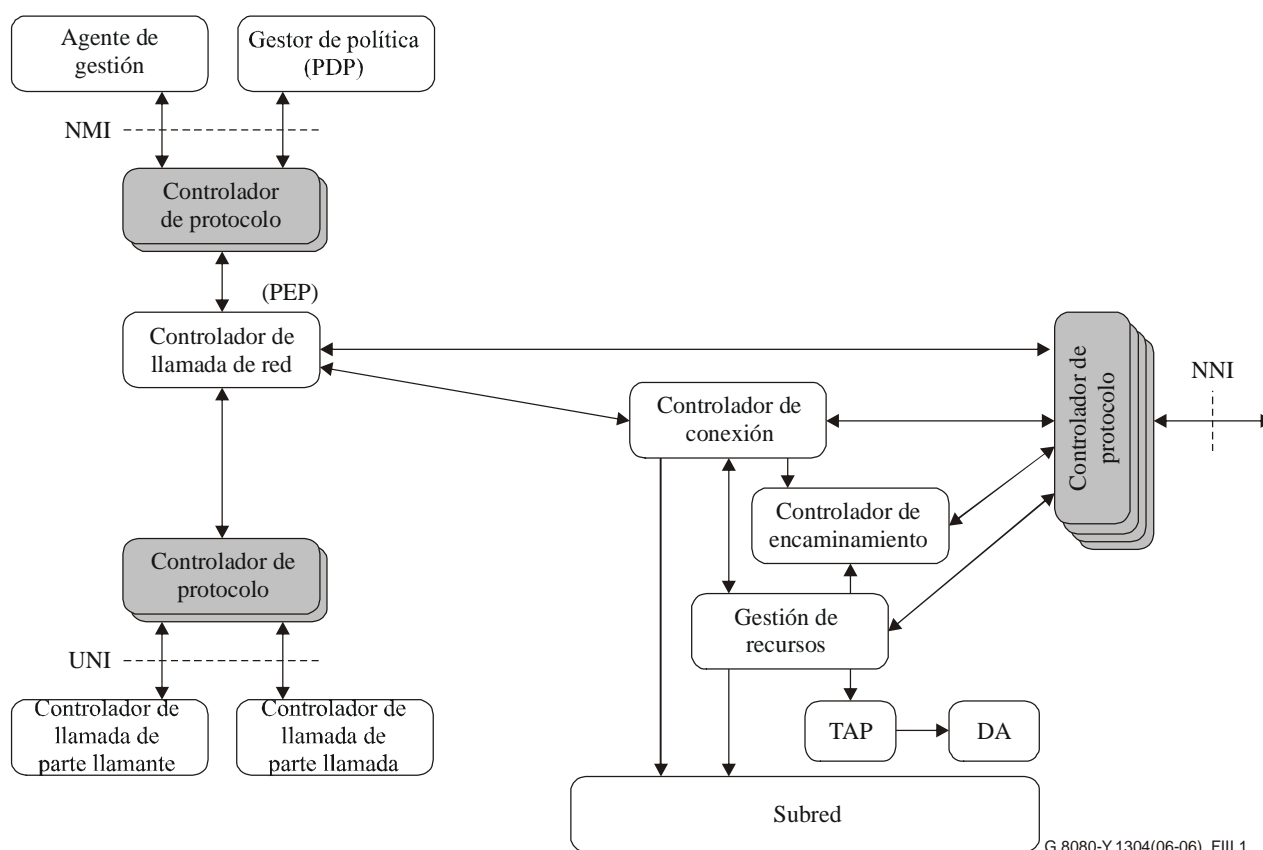
## Apéndice III

### Relaciones de resiliencia

La resiliencia es la capacidad del plano de control de continuar funcionando en condiciones de fallo. El funcionamiento del plano de control depende de los elementos de la red de comunicaciones de datos (RCD), del plano de transporte, del plano de gestión y de los componentes internos del propio plano de control (véase la figura 1). Las siguientes cláusulas identifican las dependencias del plano de control en estas áreas. El grado deseado de resiliencia del plano de control puede ser diseñado proporcionando redundancia apropiada para las funciones dependientes.

#### III.1 Relaciones de plano de control – RCD

El plano de control depende de la RCD para la transferencia de mensajes de señalización por algunas o todas las interfaces siguientes (véase la figura III.1): UNI, NNI, NMI. Se examinará la repercusión del fallo de un canal de señalización en el funcionamiento del plano de control para cada uno de los controladores de protocolo asociados con cada interfaz.



**Figura III.1/G.8080/Y.1304 – Componentes del plano de control  
(una interpretación)**

#### III.1.1 UNI

Hay dos controladores de protocolo potencialmente distintos que tratan las sesiones de señalización por la UNI: uno para el enlace de controlador de llamada de parte llamante y otro para el enlace de controlador de llamada de parte llamada.

### **III.1.1.1 Caso de fallo**

Un fallo de la sesión de señalización que soporta la UNI para el enlace de controlador de llamada de parte llamante resultará en la pérdida de los flujos de control de petición de llamada/liberación de llamada.

Un fallo de la sesión de señalización que soporta la UNI para el enlace de controlador de llamada de parte llamada resultará en la pérdida de los flujos de control de petición de llamada/indicación de llamada.

Un fallo de cualquiera de las sesiones de señalización relacionadas con la UNI repercute en la función de controlador de llamada de red.

En todos los casos anteriores, las llamadas existentes y sus conexiones no son alteradas. Se puede notificar al plano de gestión si el fallo persiste y requiere intervención de operador (por ejemplo, para liberar una llamada).

### **III.1.1.2 Caso de restablecimiento**

Cuando se restablece el canal de señalización, se debe efectuar la resincronización de estados entre los controladores de llamada de cliente y el controlador de llamada de red, y los controladores de conexión por la UNI.

## **III.1.2 NNI**

Hay posiblemente cuatro controladores de protocolo distintos que tratan las sesiones de señalización por la NNI: uno para el enlace de controlador de llamada de red, uno para el enlace de controlador de conexión, uno para el enlace de controlador de encaminamiento y uno para el enlace de gestor de recursos de enlace.

### **III.1.2.1 Caso de fallo**

Un fallo de la sesión de señalización que soporta la NNI para el enlace de controlador de llamada de red resultará en la pérdida de los flujos de control de coordinación de controlador de llamada de red. El establecimiento o la liberación de la llamada no será posible, pero no hay repercusión sobre el establecimiento o supresión de la conexión.

Un fallo de la sesión de señalización que soporta la NNI para el enlace de controlador de conexión resultará en la pérdida de los flujos de control de petición de coordinación y conexión del controlador de conexión/liberación de llamada. No será posible establecer o liberar la conexión. Además, si el control de llamada es llevado en el control de conexión, no será posible tampoco el establecimiento ni la liberación de la llamada.

Un fallo de la sesión de señalización que soporta la NNI para el enlace de controlador de encaminamiento resultará en la pérdida de los flujos de control de topología de red/local.

Un fallo de la sesión de señalización que soporta la NNI para el enlace de gestor de recursos de enlace resultará en la pérdida de los flujos de control de negociación/liberación de SNP.

Un fallo de la sesión de señalización del gestor de recursos de enlace repercute en la función de controlador de encaminamiento y en la función de controlador de conexión. Un fallo de la sesión de señalización del controlador de encaminamiento repercute en la función de controlador de conexión. Un fallo de la sesión de señalización del controlador de conexión repercute en la función de controlador de llamada de red.

En todos los casos anteriores, las llamadas existentes y sus conexiones no son alteradas. Se puede notificar al plano de gestión si el fallo persiste y requiere intervención de operador (por ejemplo, para liberar una llamada).

Obsérvese que un fallo de la RCD puede afectar simultáneamente a una o a varias o a todas las sesiones de señalización anteriores. El controlador de protocolo asociado con cada canal de señalización debe detectar y enviar una alarma en caso de fallo de un canal de señalización.

### **III.1.2.2 Caso de restablecimiento**

Después del restablecimiento de un canal de señalización que ha fallado previamente, el correspondiente controlador de protocolo debe asegurar que toda la mensajería se reanuda en secuencia. Los componentes son responsables de restablecer la información de estado después de la recuperación del controlador de protocolo.

## **III.2 Relaciones entre el plano de control y el plano de transporte**

Esta cláusula sólo considera los fallos del plano de transporte que afectan a la capacidad del plano de control para ejecutar sus funciones, por ejemplo, cuando un LRM no puede ser informado. Los fallos del plano de transporte, tales como fallos de puertos, no están dentro del alcance de esta Recomendación, pues se prevé que el plano de control sea informado de esta situación. La compatibilidad de información entre los dos planos se trata en 12.1.

### **III.2.1 Información del plano de transporte – Indagación**

El plano de control interrogará al plano de transporte en los siguientes casos:

- cuando se activa, o reactiva, una sesión de señalización de controlador de conexión (por ejemplo, después del restablecimiento de un enlace de datos o NE de transporte);
- el plano de control interroga sobre los recursos de transporte;
- como parte de la sincronización de información de recursos de transporte (por ejemplo, cuando el plano de control se recupera tras un fallo).

### **III.2.2 Información del plano de transporte – Evento activado**

El plano de transporte informará al plano de control sobre un evento en los siguientes casos:

- fallo de un recurso de transporte;
- adición/supresión de un recurso de transporte.

#### **III.2.2.1 Protección del plano de transporte**

Las acciones de protección del plano de transporte que tienen éxito son totalmente transparentes al plano de control. El plano de transporte sólo tiene que notificar al plano de control los cambios de disponibilidad de los recursos de transporte.

Los intentos de protección del plano de transporte que no tienen éxito aparecen ante el plano de control como fallos de conexión y pueden activar acciones de restablecimiento del plano de control, si esta funcionalidad está proporcionada. Dado que el plano de control soporta la funcionalidad de restablecimiento, existen las siguiente relaciones.

El controlador de encaminamiento debe ser informado del fallo de un enlace o nodo del plano de transporte y actualizará la base de datos de topología de red/local en consecuencia. El controlador de encaminamiento puede informar las averías al controlador de conexión local.

### **III.2.3 Dependencia del plano de transporte del plano de control**

Si el plano de control falla, no es posible procesar las nuevas peticiones de conexión que requieren el uso de los componentes del plano de control que ha fallado. Obsérvese, no obstante, que el plano de gestión podrá ser utilizado como un repliegue para responder a nuevas peticiones de conexión. La conexión establecida no debe ser afectada por un fallo del plano de control.



### **III.3 Relaciones del plano de control – Plano de gestión**

El plano de control puede obtener información de directorio y de política del plano de gestión durante el proceso de validación de control de admisión de llamada. El fallo de los servidores de directorio o de política podrá resultar en el fallo de las peticiones de establecimiento de conexión.

Como ejemplos cabe citar:

- En el controlador de llamada de red (en el extremo de la parte llamante o llamada), las peticiones de llamada pueden tener que ser validadas comprobando la política.
- Cuando el controlador de conexión solicita un trayecto del controlador de encaminamiento, puede ser necesario consultar a un servidor de política.

Las acciones de liberación de llamada pueden efectuarse en el plano de control si el plano de gestión no está disponible. El plano de control debe mantener un registro de estas acciones, de modo que cuando el plano de gestión esté disponible, se pueda enviar un registro cronológico al plano de gestión o el plano de control pueda ser interrogado sobre esta información.

#### **III.3.1 NMI**

Todos los componentes de control tienen puertos de monitor, política y configuración que proporcionan la visión de gestión de los componentes del plano de control (véase 7.2.1).

Hay dos sesiones potencialmente separadas de controladores de protocolo/señalización que comprenden flujos de información de gestión: una para la sesión del gestor de política y otra para la sesión de gestión de transporte. Otros controladores de protocolo pueden ser introducidos en el futuro para otras funciones de gestión.

##### **III.3.1.1 Caso de fallo**

Un fallo de la sesión de señalización que soporta el enlace de gestor de política resultará en la pérdida de los flujos de control de política en salida.

Un fallo de la sesión de señalización de gestión de transporte resultará en la pérdida del intercambio de información de averías, configuración, contabilidad, calidad de funcionamiento, seguridad (FCAPS, *fault, configuration, accounting, performance, security*).

Un fallo de la sesión de política repercute en la función de controlador de llamada de red. Por ejemplo, el posible fallo de nuevas peticiones de establecimiento de conexión cuando el proceso de validación de control de admisión de llamada requiere acceso al gestor de política.

##### **III.3.1.2 Caso de restablecimiento**

Cuando la comunicación de señalización de gestión es restablecida, se envía la información almacenada en el plano de control que debe ser enviada al plano de gestión (por ejemplo, registros de llamada). La información pendiente del plano de gestión al plano de control debe ser enviada (por ejemplo, política o configuración revisadas).

### **III.4 Relaciones dentro del plano de control**

La repercusión de los fallos de componentes del plano de control en el funcionamiento de todo el plano de control será examinada según la relación de componentes ilustrada en la figura III.1. Para lograr el funcionamiento continuo del plano de control en caso de fallo de un componente, se requiere la capacidad de detectar el fallo de un componente y conmutar a un componente redundante, sin pérdida de mensajes e información de estado.

Si los componentes del plano de control no son redundantes, cuando un componente que ha fallado es restablecido, debe restablecer una visión suficiente de los recursos del plano de transporte para ser operacional.

Se supone que las comunicaciones entre componentes distintos de los controladores de protocolo (es decir, comunicaciones distintas de PC) son altamente fiables. Estas comunicaciones probablemente son internas de un nodo del plano de control y son específicas de la implementación, por lo que están fuera del ámbito de la presente recomendación.

#### **III.4.1 Controlador de llamada de red**

El fallo de un controlador de llamada de red resultará en la pérdida de nuevas peticiones de establecimiento de comunicación y de las peticiones existentes de liberación de llamada.

#### **III.4.2 Controlador de conexión**

El fallo de un controlador de conexión resultará en la pérdida de nuevas peticiones de establecimiento de conexión y peticiones existentes de liberación de conexión. Como la señalización de control de llamada se implementa a menudo mediante el controlador de conexión y su controlador de protocolo, un fallo del controlador de conexión puede repercutir en la función de controlador de llamada de red (por ejemplo, puede no ser capaz de liberar las llamadas existentes).

#### **III.4.3 Controlador de encaminamiento**

El fallo de un controlador de encaminamiento resultará en la pérdida de nuevas peticiones de establecimiento de conexión y pérdida de la sincronización de la base de datos de topología. Como el controlador de conexión depende del controlador de encaminamiento para la selección del trayecto, un fallo del controlador de encaminamiento repercute en el controlador de conexión. Las indagaciones del plano de gestión de información de encaminamiento serán también afectadas por un fallo del controlador de encaminamiento.

#### **III.4.4 Gestor de recursos de enlace**

El fallo de un gestor de recursos de enlace resultará en la pérdida de nuevas peticiones de establecimiento de conexión y de peticiones existentes de liberación de conexión, así como en la pérdida de sincronización de la base de datos de SNP. Como el controlador de encaminamiento depende del gestor de recursos de enlace para la información de recursos de transporte, la función de controlador de encaminamiento es afectada por un fallo del gestor de recursos de enlace.

#### **III.4.5 Controladores de protocolo**

El fallo de cualquiera de los controladores de protocolo tiene el mismo efecto que el fallo de las correspondientes sesiones de señalización de RCD, identificadas anteriormente. El fallo de un nodo completo del plano de control debe ser detectado por los controladores de protocolo de la NNI de nodos vecinos.

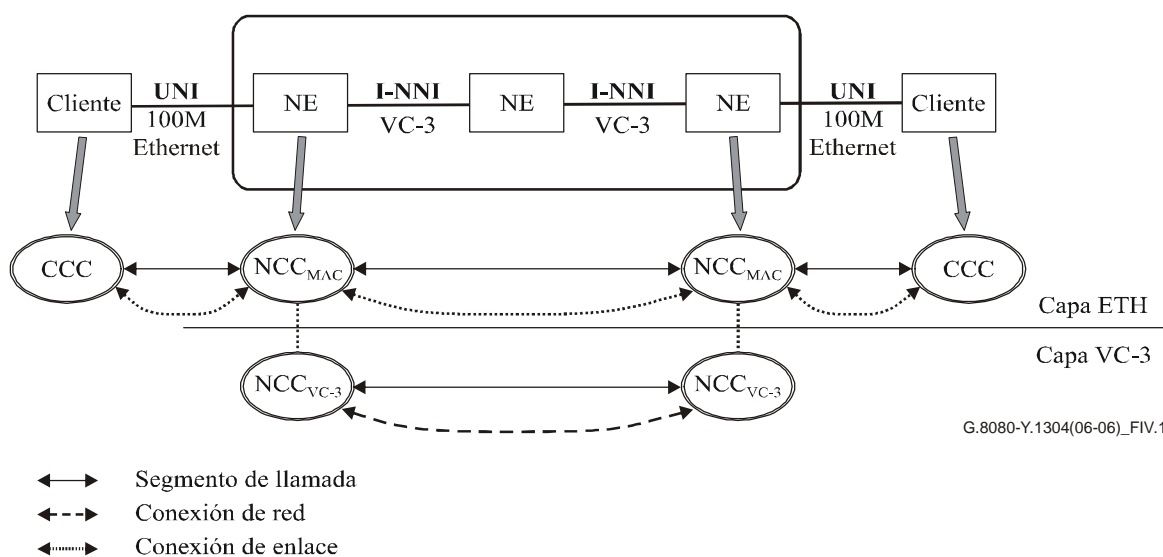
#### **III.4.6 Compatibilidad de información dentro del plano de control**

Como se examina en 12.1, en un nodo dado, se debe establecer primero la compatibilidad de la información de recursos de componentes y del plano de control y del estado de la SNC con la información local de recursos y estados de NE de transporte. A continuación, los componentes del plano de control deben asegurar la compatibilidad de la información del estado de SNC con sus componentes de plano de control adyacentes. Cualquier diferencia de conexión debe ser resuelta de modo que no quede ningún fragmento de conexión o se produzcan conexiones erróneas. Después de la comprobación de la compatibilidad de información del plano de control, los componentes del plano de control pueden participar en las peticiones de establecimiento o liberación de conexiones del plano de control.

## Apéndice IV

### Ejemplo de control de llamada estructurado por capas

La figura IV.1 ilustra el caso de correspondencia de servidor empleando el modelo de llamada entre capas de dos clientes Ethernet que están conectados a una red VC-3 común que no soporta la conmutación Ethernet. Supongamos que se recibe una solicitud de llamada de 40 Mbit/s por una UNI Ethernet de Gigabits. Para transportar la CI Ethernet, es necesario crear una conexión VC-3. La decisión de la  $NCC_{MAC}$  de efectuar una llamada al correspondiente  $NCC_{VC-3}$  se rige por las políticas del operador. Ambas capas se muestran indicando que sólo la capa VC-3 tiene una conexión de red. Una vez establecida la conexión VC-3, aparece la conexión de enlace FPP ETH entre los dos  $NCC_{MAC}$ .



G.8080-Y.1304(06-06)\_FIV.1

**Figura IV.1/G.8080/Y.1304 – Ejemplo de Ethernet por VC-3**

En la secuencia de los eventos, el establecimiento de comunicaciones en capas de servidor diferentes puede ser independiente en el tiempo. Por ejemplo, la llamada Ethernet de entrada podría activar la conexión VC-3. Alternativamente, la conexión VC-3 puede ya existir y asociarse entonces a una llamada MAC de entrada. Las políticas del operador también rigen la asociación de la conexión VC-3 con la llamada Ethernet solicitada.

Hay muchos otros ejemplos de llamadas entre capas tales como el canal de fibra por la jerarquía digital síncrona (SDH, *synchronous digital hierarchy*)/red óptica de transporte (OTN, *optical transport network*).

## Apéndice V

### Interacción entre los componentes durante el establecimiento de la conexión

En la cláusula 7.1 se estipula que los componentes controladores son entidades abstractas que pueden estar compuestas por una sola entidad o por un conjunto distribuido de entidades que conforman una federación cooperativa. Sin embargo, en aras de una mayor claridad, los ejemplos presentados en el presente apéndice muestran posibles estrategias de puesta en práctica en las que los componentes que se muestran no son entidades abstractas sino casos particulares de código de implementación. Concretamente:

- Los controladores de llamada de red se muestran como una federación cooperativa distribuida.
- Los controladores de encaminamiento se muestran en una federación cooperativa distribuida.
- Los controladores de conexión se muestran como una entidad única para una matriz.
- Los LRM se muestran como una entidad única que gestiona todos los extremos de enlace de una matriz.

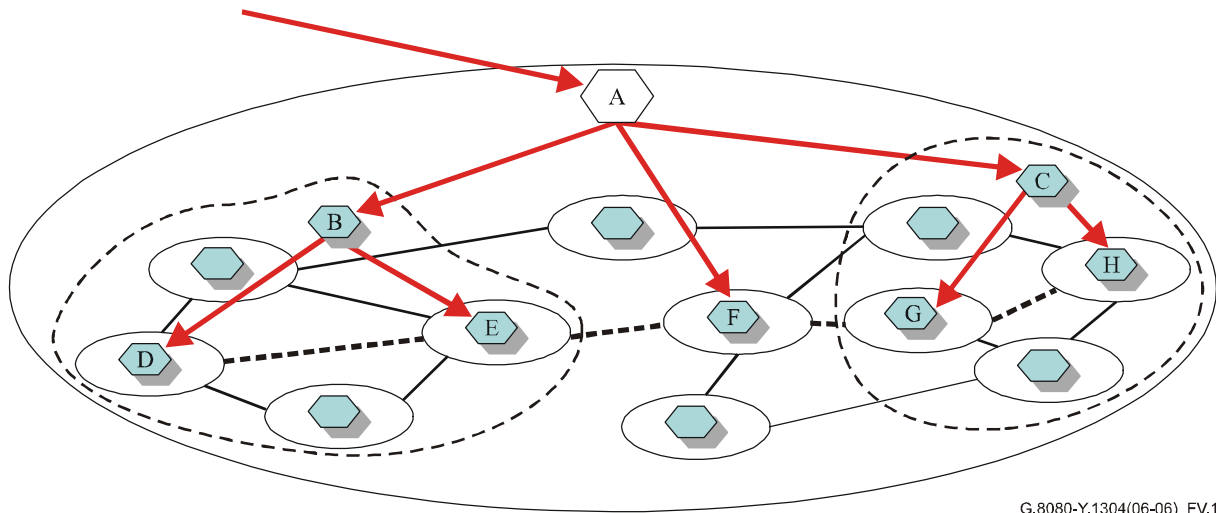
En algunos ejemplos se utiliza una caja sombreada para indicar las fronteras de la federación cooperativa distribuida que conforma una entidad abstracta.

Para controlar una conexión es necesario que cierto número de componentes interactúen.

Se pueden distinguir tres formas básicas de algoritmo para el control dinámico del trayecto: el encaminamiento jerárquico, el encaminamiento desde la fuente y el encaminamiento paso a paso, como se muestra en las figuras siguientes. Las diversas formas de control del trayecto producen diversas distribuciones de componentes entre los nodos y relaciones entre estos controladores de conexión. Si un RC no tiene información suficiente para proporcionar una ruta para una petición de conexión, éste se puede comunicar con otros RC para encontrar la ruta, empleando la interfaz de interrogación de rutas descrita en 7.3.2.

#### V.1 Encaminamiento jerárquico

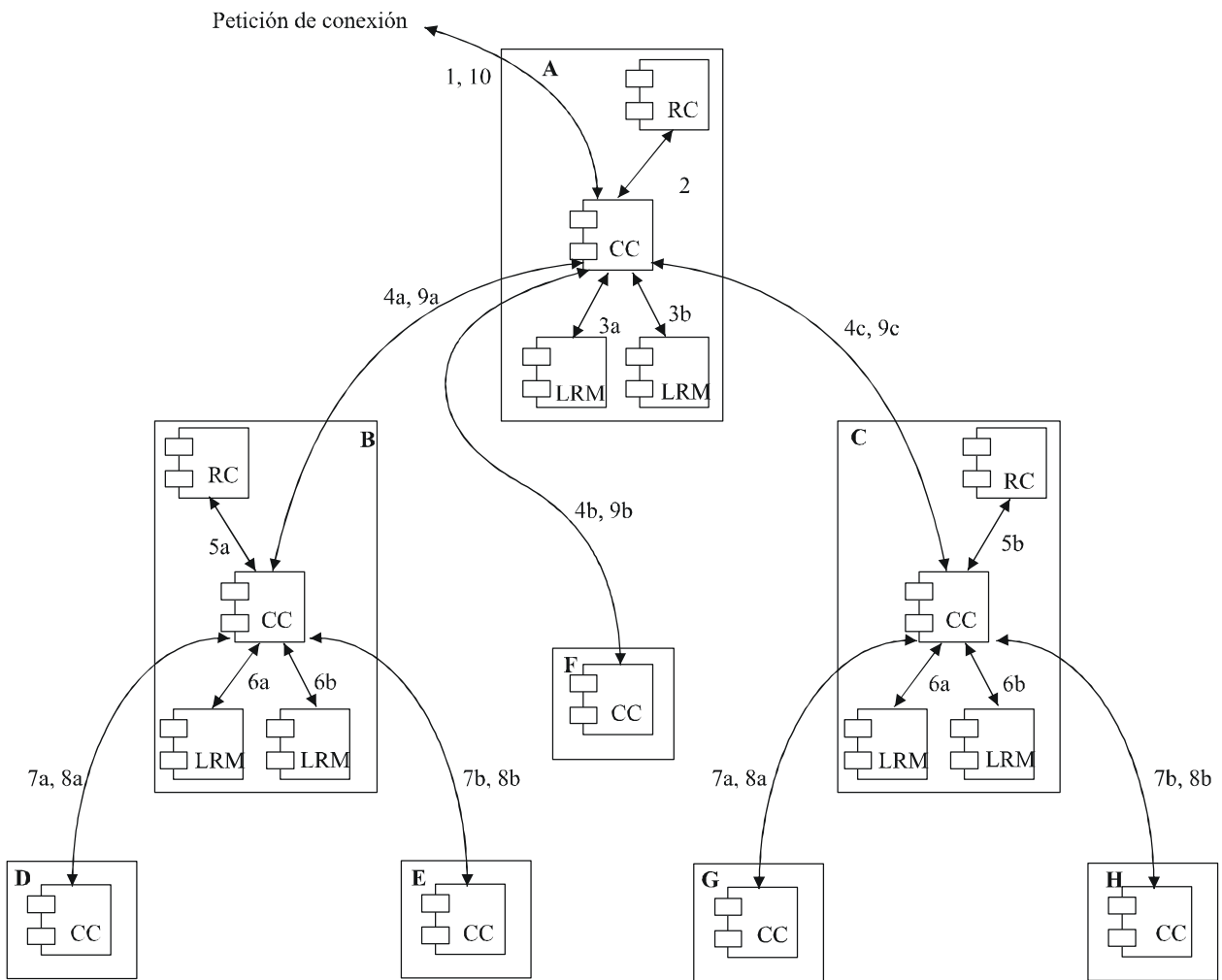
En el caso de encaminamiento jerárquico, que se ilustra en la figura V.1, un nodo posee un controlador de encaminamiento, controladores de conexión y gestores de recursos de enlace para un solo nivel en una jerarquía de área de encaminamiento. La red de capa y, a su turno, el área de encaminamiento se descomponen en una jerarquía de subredes (en armonía con los conceptos descritos en la Rec. UIT-T G.805). Los controladores de conexión se relacionan unos con otros de una manera jerárquica. Cada área de encaminamiento tiene su propio control de conexión dinámico, que tiene conocimiento de la topología de su área de encaminamiento pero no de la topología de las áreas de encaminamiento de nivel superior o inferior en la jerarquía, ni de otras áreas de encaminamiento en el mismo nivel de la jerarquía.



G.8080-Y.1304(06-06)\_FV.1

- ➔ Mensaje de petición de conexión
- Nodo de equipo
- Área de encaminamiento
- Conexión establecida
- Subred

**Figura V.1/G.8080/Y.1304 – Flujo de señalización jerárquica**



G.8080-Y.1304(06-06)\_FV.2

**Figura V.2/G.8080/Y.1304 – Interacciones de encaminamiento jerárquico**

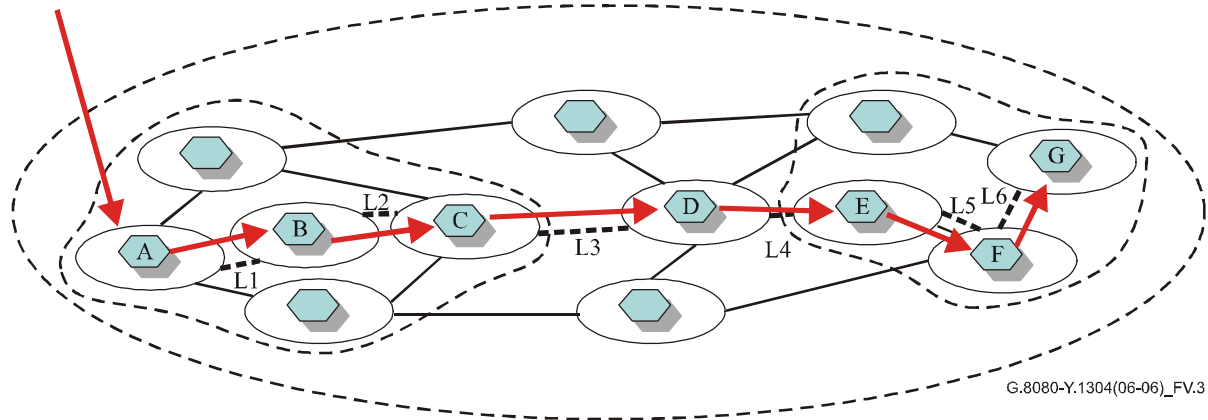
En la figura V.2 se describe la secuencia detallada de operaciones que intervienen en el establecimiento de una conexión mediante encaminamiento jerárquico. A continuación se enumeran los pasos de esta secuencia:

- 1) Llega al controlador de conexión (CC) una petición de conexión procedente de la interfaz petición de conexión de entrada, especificada como un par de SNP en el borde del área de encaminamiento del nivel superior.
- 2) El componente encaminamiento (RC, *routing controller*) es interrogado (utilizando el SNP del extremo Z mediante la interfaz de interrogación del cuadro de rutas) y retorna el conjunto de enlaces y subredes que intervienen.
- 3) Se obtienen conexiones de enlace (en cualquier orden, por ejemplo 3a, o 3b en la figura V.2) procedentes de los gestores de recursos de enlace (LRM) a través de la interfaz petición de conexión de enlace.
- 4) Una vez obtenidas conexiones de enlace (especificadas como pares de SNP), se pueden solicitar conexiones de subred de las áreas de encaminamiento vástago, pasando un par de SNP a través de la interfaz petición de conexión y confirmando conexiones de subred al CC por medio de la interfaz petición de conexión de salida. También en este caso, el orden de estas operaciones no es fijo, siendo el único requisito que las conexiones de enlace se obtengan antes de que se puedan crear conexiones de subred. El proceso inicial se repite ahora recursivamente.
- 5) Los controladores de encaminamiento vástago determinan ahora una ruta entre los SNP especificados.
- 6) Se obtienen conexiones de enlace (en cualquier orden) de los gestores de recursos de enlace (LRM) a través de la interfaz petición de conexión de enlace.
- 7) Como paso final, los conmutadores de nivel inferior, que no contienen componentes de asignación de enlace o encaminamiento, proporcionan las necesarias conexiones de subred.
- 8) Los pasos restantes indican el flujo de confirmaciones de que se ha establecido la conexión; el proceso culmina en el paso 10), donde se retorna la confirmación al usuario original.

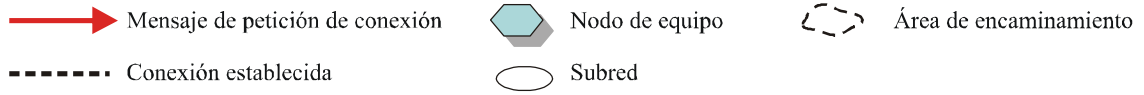
## **V.2 Encaminamientos desde la fuente y paso a paso**

Aunque similar al encaminamiento jerárquico, en lo tocante al encaminamiento desde la fuente el proceso de control de conexión se implementa mediante una federación de controladores de conexión y encaminamiento distribuidos. La diferencia más importante es que los controladores de conexión utilizan secuencias de funciones de cálculo de trayecto entre niveles de encaminamiento que son diferentes entre el encaminamiento jerárquico y el encaminamiento desde la fuente. El flujo de señal para el encaminamiento desde la fuente (y el encaminamiento paso a paso) se muestra en la figura V.3.

A fin de reducir la cantidad de topología de red que cada controlador debe tener disponible, sólo se pone a disposición la porción de la topología que se aplica a su propia área de encaminamiento.

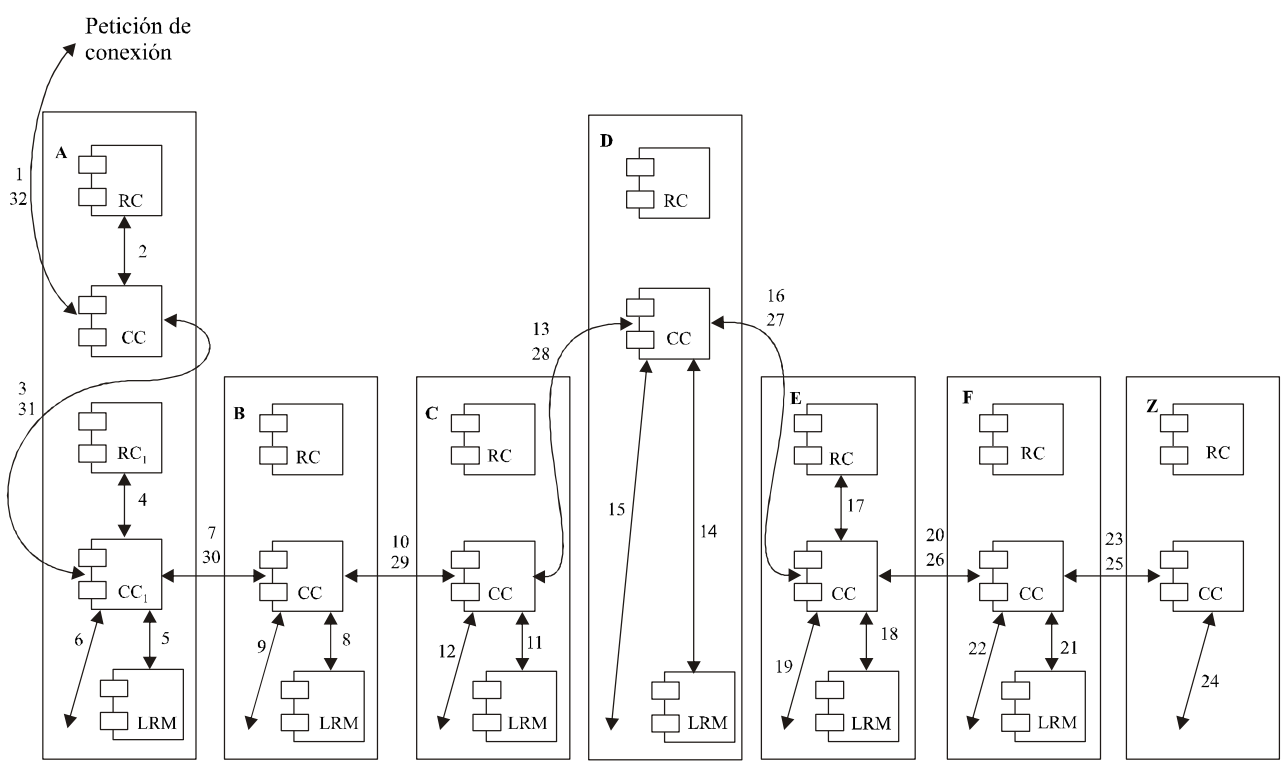


G.8080-Y.1304(06-06)\_FV.3



**Figura V.3/G.8080/Y.1304 – Flujo de señalización en los casos de encaminamiento desde la fuente y paso a paso**

**V.2.1 Encaminamiento desde la fuente**



G.8080-Y.1304(06-06)\_FV.4

**Figura V.4/G.8080/Y.1304 – Interacciones en el caso de encaminamiento desde la fuente**

En los siguientes pasos se describe la secuencia de interacciones mostrada en la figura V.4. Se utiliza la siguiente notación:  $X_A$  representa el componente en el nivel superior del nodo A;  $X_{An}$  representa el componente en el siguiente  $n$ -ésimo nivel superior del nodo A.

- 1) Llega al controlador de conexión ( $CC_A$ ) una petición de conexión procedente de la interfaz petición de conexión de entrada, especificada como un par de nombres (A y Z) en el borde de la subred.
- 2) El controlador encaminamiento ( $RC_A$ ) es interrogado (utilizando el SNP del extremo Z a través de la interfaz de interrogación del cuadro de rutas), y retorna la ruta, A, L3, L4, Z.
- 3) Como  $CC_A$  no tiene acceso al necesario gestor de recursos de enlace ( $LRM_C$ ), la petición (A, L3, L4, Z) se hace pasar a un  $CC_{A1}$  por (a través de la interfaz petición de conexión de entrada/salida), que controla el encaminamiento a través de esta área de encaminamiento.
- 4)  $CC_{A1}$  interroga a  $RC_{A1}$  (a través de la interfaz interrogación de rutas) para L3 y obtiene una lista de enlaces adicionales, L1 y L2.
- 5) El enlace L1 es local a este nodo, y se obtiene una conexión de enlace para L1 desde  $LRM_A$  a través de la interfaz petición de conexión de enlace.
- 6) Se establece una SNC a través del conmutador local (no se muestra el controlador).
- 7) La petición, que ahora contiene el resto de la ruta (L2, L3, L4 y Z), es reenviada al  $CC_B$  por siguiente (a través de la interfaz coordinación de entidad par de entrada/salida).
- 8)  $LRM_B$  controla L2, de tal manera que se obtiene una conexión de enlace desde este enlace a través de la interfaz petición de conexión de enlace.
- 9) La SNC se establece a través del conmutador local (no se muestra el controlador).
- 10) La petición, que ahora contiene el resto de la ruta (L3, L4 y Z), es reenviada al  $CC_C$  por siguiente (a través de la interfaz coordinación de entidad par de entrada/salida).
- 11)  $LRM_C$  controla L3, de tal manera que se obtiene una conexión de enlace desde este enlace a través de la interfaz petición de conexión de enlace.
- 12) La SNC se establece a través del conmutador local (no se muestra el controlador).
- 13) La petición, que ahora contiene el resto de la ruta (L4, Z), es reenviada al  $CC_D$  por siguiente (a través de la interfaz coordinación de entidad par de entrada/salida).
- 14)  $LRM_D$  controla L4, de tal manera que se obtiene una conexión de enlace desde este enlace a través de la interfaz petición de conexión de enlace.
- 15) La SNC se establece a través del conmutador local (no se muestra el controlador).
- 16) La petición, que ahora contiene el resto de la ruta (Z), es reenviada al  $CC_E$  por siguiente (a través de la interfaz coordinación de entidad par de entrada/salida).
- 17)  $CC_E$  interroga a  $RC_E$  para Z (a través de la interfaz de interrogación del cuadro de rutas) y obtiene los enlaces L5 y L6.

El proceso de conexión a través de la siguiente área de encaminamiento (por ejemplo, pasos 18 a 24 en la figura V.4) es idéntico al que ya se ha descrito. Los eventos 25 a 32 describen el flujo de señales de confirmación hacia el originador de la conexión.

### V.2.2 Encaminamiento paso a paso

En esta forma de encaminamiento se produce una ulterior reducción de la información de encaminamiento en los nodos, lo que impone restricciones a la manera de determinar el encaminamiento a través de la subred. La figura V.5 es aplicable al diagrama de red de la figura V.3.

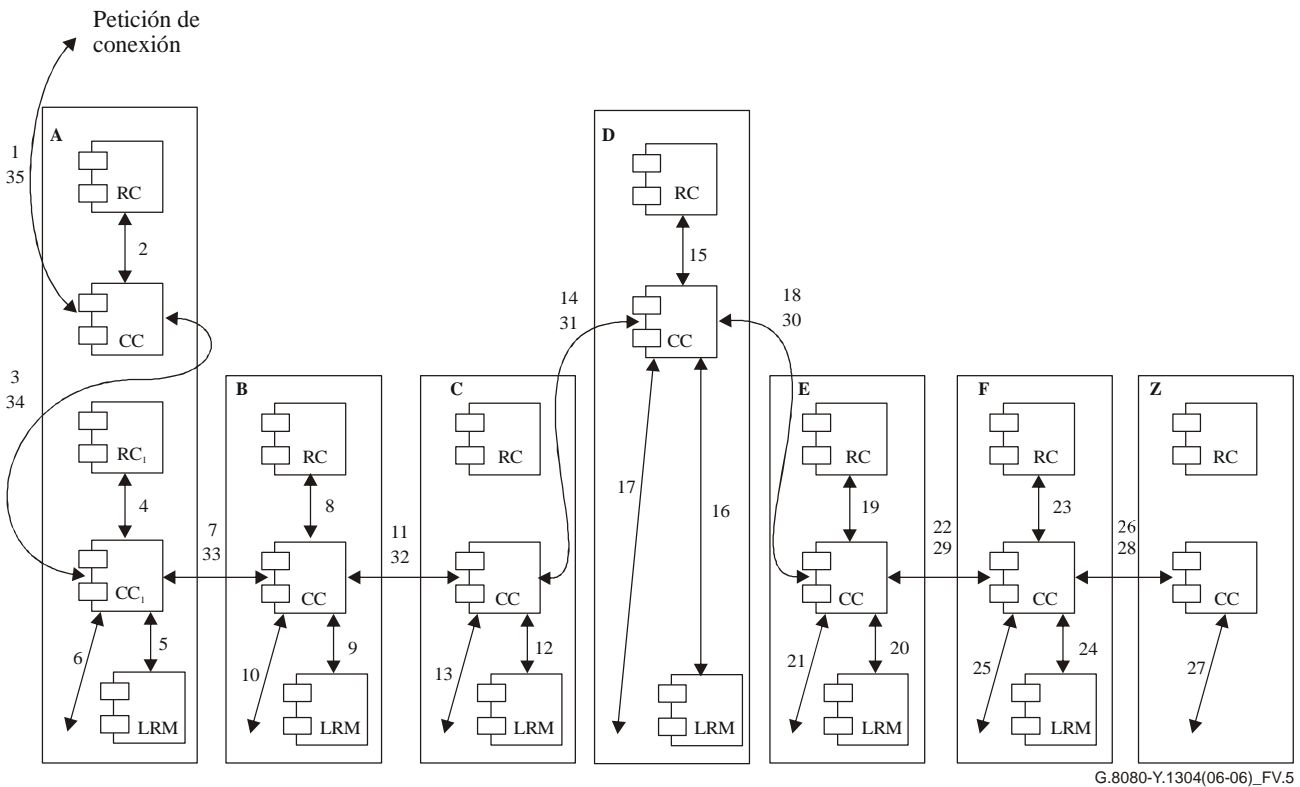
El proceso de encaminamiento paso a paso es idéntico al descrito para el encaminamiento desde la fuente, con la siguiente diferencia: el controlador de encaminamiento  $RC_{A1}$  sólo puede proporcionar



el enlace L1, y no proporciona también el enlace L2.  $CC_B$  debe entonces interrogar a  $RC_B$  (a través de la interfaz interrogación del cuadro de rutas) para L2 con el fin de obtener L2. Se sigue un proceso similar de obtención de un enlace cada vez cuando se conecta a través de la segunda área de encaminamiento.

- 1) Llega al controlador de conexión ( $CC_A$ ) una petición de conexión procedente de la interfaz petición de conexión de entrada, especificada como un par de nombres (A y Z) en el borde de la subred.
- 2) El controlador de encaminamiento ( $RC_A$ ) es interrogado (utilizando el SNP del extremo Z a través de la interfaz de interrogación del cuadro de rutas), y retorna el enlace de salida, L3.
- 3) Como  $CC_A$  no tiene acceso al necesario gestor de recursos de enlace ( $LRM_C$ ), la petición (A, L3, Z) se hace pasar a un  $CC_{A1}$  par (a través de la interfaz petición de conexión de entrada/salida), que controla el encaminamiento a través de esta área de encaminamiento.
- 4)  $CC_{A1}$  interroga a  $RC_{A1}$  (a través de la interfaz interrogación de rutas) para L3 y obtiene L1.
- 5) El enlace L1 es local a este nodo, y se obtiene una conexión de enlace para L1 desde  $LRM_A$  a través de la interfaz petición de conexión de enlace.
- 6) Se establece una SNC a través del conmutador local (no se muestra el controlador).
- 7) La petición, que ahora contiene el resto de la ruta (L3 y Z), es reenviada al  $CC_B$  par siguiente (a través de la interfaz coordinación de entidad par de entrada/salida).
- 8)  $CC_{B1}$  interroga a  $RC_{B1}$  (a través de la interfaz interrogación de rutas) para L3 y obtiene L2.
- 9)  $LRM_B$  controla L2, de tal manera que se obtiene una conexión de enlace desde este enlace a través de la interfaz petición de conexión de enlace.
- 10) La SNC se establece a través del conmutador local (no se muestra el controlador).
- 11) La petición, que ahora contiene el resto de la ruta (L3 y Z), es reenviada al CCC par siguiente (a través de la interfaz coordinación de entidad par de entrada/salida).
- 12)  $LRM_C$  controla L3, de tal manera que se obtiene una conexión de enlace desde este enlace a través de la interfaz petición de conexión de enlace.
- 13) La SNC se establece a través del conmutador local (no se muestra el controlador).
- 14) La petición, que ahora contiene el resto de la ruta (Z), es reenviada al  $CC_D$  par siguiente (a través de la interfaz coordinación de entidad par de entrada/salida).
- 15)  $CC_D$  interroga a  $RC_D$  (a través de la interfaz interrogación de rutas) para Z y obtiene el enlace L4.
- 16)  $LRM_D$  controla L4, de tal manera que se obtiene una conexión de enlace desde este enlace a través de la interfaz petición de conexión de enlace.
- 17) La SNC se establece a través del conmutador local (no se muestra el controlador).
- 18) La petición, que ahora contiene el resto de la ruta (Z), es reenviada al  $CC_E$  par siguiente (a través de la interfaz coordinación de entidad par de entrada/salida).
- 19)  $CC_E$  interroga a  $RC_E$  (a través de la interfaz de interrogación del cuadro de rutas) para Z y obtiene el enlace L5.
- 20)  $LRM_E$  controla L5, de tal manera que se obtiene una conexión de enlace desde este enlace a través de la interfaz petición de conexión de enlace.
- 21) La SNC se establece a través del conmutador local (no se muestra el controlador).
- 22) La petición, que ahora contiene el resto de la ruta (Z), es reenviada al  $CC_F$  par siguiente (a través de la interfaz coordinación de entidad par de entrada/salida).
- 23)  $CC_F$  interroga a  $RC_F$  (a través de la interfaz interrogación de rutas) para Z y obtiene el enlace L6.

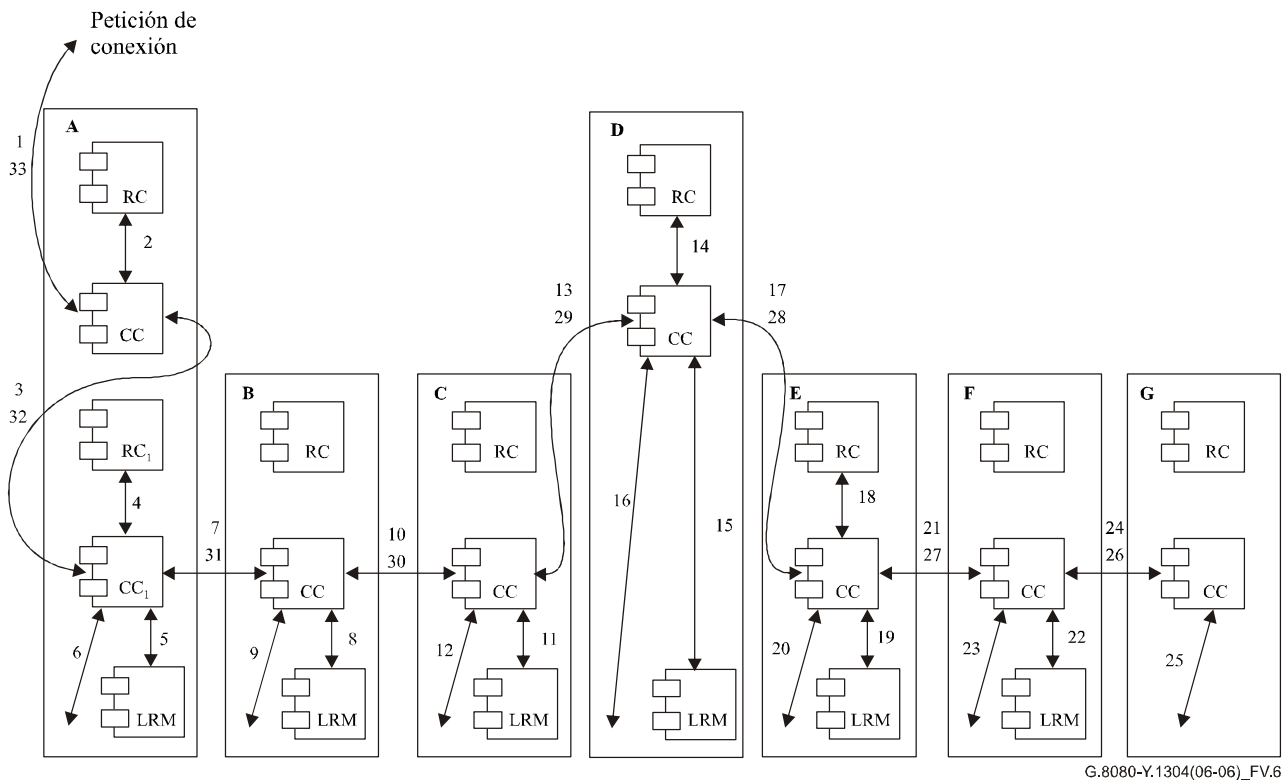
- 24) LRM<sub>F</sub> controla L6, de tal manera que se obtiene una conexión de enlace desde este enlace a través de la interfaz petición de conexión de enlace.
- 25) La SNC se establece a través del conmutador local (no se muestra el controlador).



**Figura V.5/G.8080/Y.1304 – Encaminamiento paso a paso**

### V.2.3 Combinación de los encaminamientos desde la fuente y paso a paso

En la figura V.6 se presenta un ejemplo en el que se puede utilizar encaminamiento desde la fuente y paso a paso, pero en diferentes niveles de encaminamiento. En el ejemplo, el encaminamiento de bajo nivel es el encaminamiento desde la fuente, mientras que el encaminamiento de alto nivel es el encaminamiento paso a paso.



G.8080-Y.1304(06-06)\_FV.6

**Figura V.6/G.8080/Y.1304 – Encaminamiento combinado desde la fuente y paso a paso**

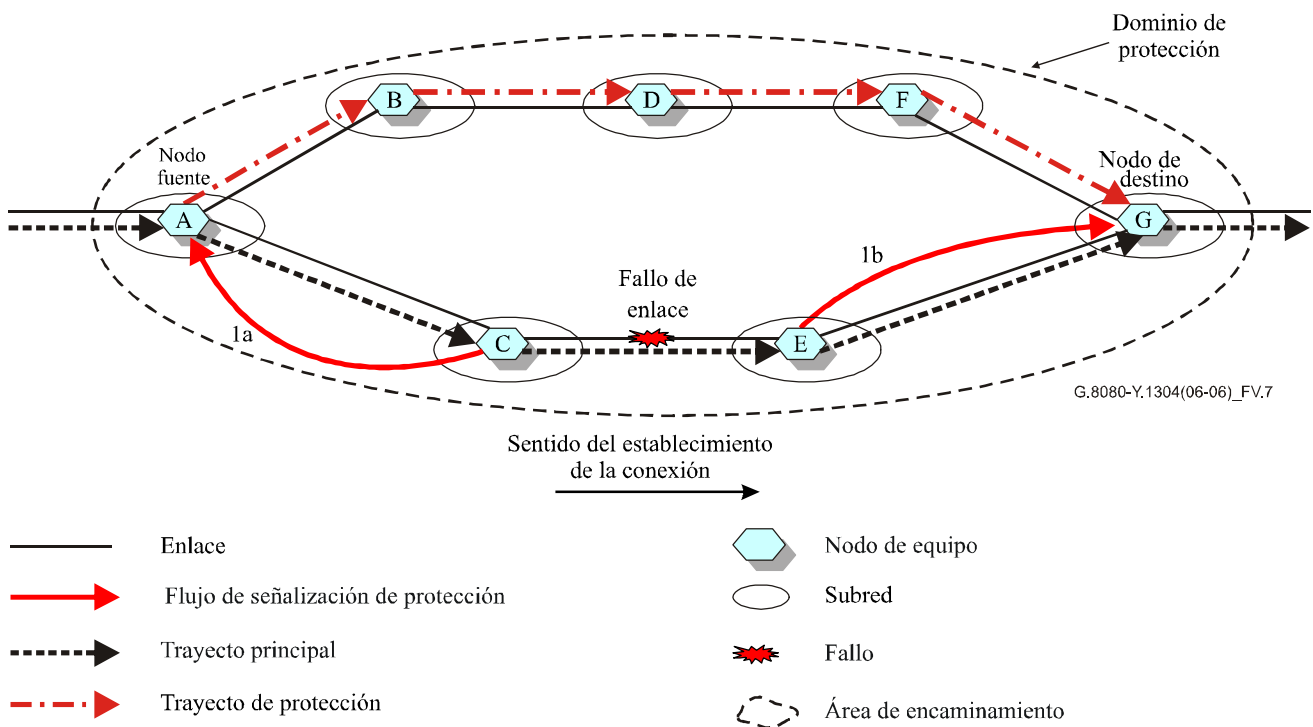
- 1) Llega al controlador de conexión ( $CC_A$ ) una petición de conexión procedente de la interfaz petición de conexión de entrada, especificada como un par de nombres (A y Z) en el borde de la subred.
- 2) El controlador encaminamiento ( $RC_A$ ) es interrogado (utilizando el SNP del extremo Z a través de la interfaz de interrogación del cuadro de rutas), y retorna el enlace de salida, L3.
- 3) Como  $CC_A$  no tiene acceso al necesario gestor de recursos de enlace ( $LRM_C$ ), la petición (A, L3, Z) se hace pasar a un  $CC_{A1}$  par (a través de la interfaz petición de conexión de entrada/salida), que controla el encaminamiento a través de esta área de encaminamiento.
- 4)  $CC_{A1}$  interroga a  $RC_{A1}$  (a través de la interfaz interrogación del cuadro de rutas) para L3 y obtiene una lista de enlaces adicionales, L1 y L2.
- 5) El enlace L1 es local a este nodo, y se obtiene una conexión de enlace para L1 desde  $LRM_A$  a través de la interfaz petición de conexión de enlace.
- 6) Se establece una SNC a través del conmutador local (no se muestra el controlador).
- 7) La petición, que ahora contiene el resto de la ruta (L2, L3 y Z), es reenviada al  $CC_B$  par siguiente (a través de la interfaz coordinación de entidad par de entrada/salida).
- 8)  $LRM_B$  controla L2, de tal manera que se obtiene una conexión de enlace desde este enlace a través de la interfaz petición de conexión de enlace.
- 9) La SNC se establece a través del conmutador local (no se muestra el controlador).
- 10) La petición, que ahora contiene el resto de la ruta (L3 y Z), es reenviada al  $CC_C$  par siguiente (a través de la interfaz coordinación de entidad par de entrada/salida).
- 11)  $LRM_C$  controla L3, de tal manera que se obtiene una conexión de enlace desde este enlace a través de la interfaz petición de conexión de enlace.
- 12) La SNC se establece a través del conmutador local (no se muestra el controlador).
- 13) La petición, que ahora contiene el resto de la ruta (Z), es reenviada al  $CC_D$  par siguiente (a través de la interfaz coordinación de entidad par de entrada/salida).

- 14)  $CC_D$  interroga a  $RC_D$  (a través de la interfaz interrogación del cuadro de rutas) para Z y obtiene el enlace L4.
- 15)  $LRM_D$  controla L4, de tal manera que se obtiene una conexión de enlace desde este enlace a través de la interfaz petición de conexión de enlace.
- 16) La SNC se establece a través del conmutador local (no se muestra el controlador).
- 17) La petición, que ahora contiene el resto de la ruta (Z), es reenviada al  $CC_E$  por siguiente (a través de la interfaz coordinación de entidad par de entrada/salida).
- 18)  $CC_E$  interroga a  $RC_E$  (a través de la interfaz interrogación del cuadro de rutas) para Z y obtiene los enlaces L5 y L6.

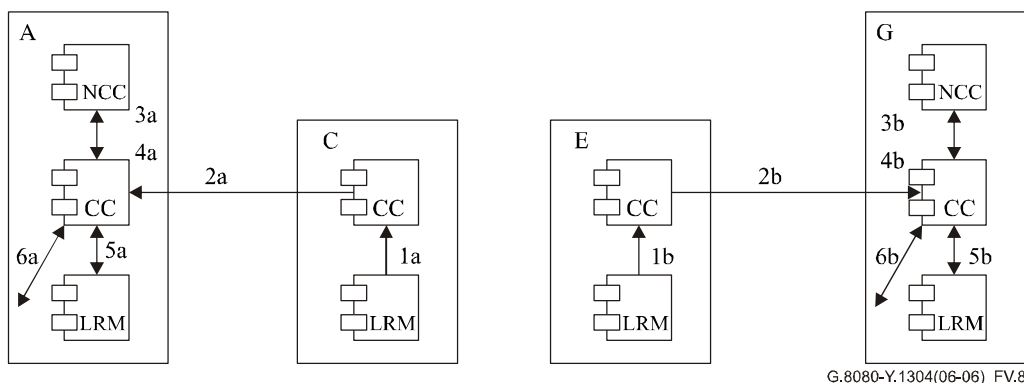
### V.3 Protección de la conexión

Cuando se utiliza el plano de control para la protección, se establece una conexión de protección a fin de proteger la conexión de trabajo antes de que ocurra un fallo. Una vez detectado un fallo de la conexión principal, únicamente los controladores de conexión de la fuente y del destino participan en el resto de la operación de conmutación de protección desde la conexión inicial a la conexión de protección.

En la figura V.7 se presenta un ejemplo de protección de conexión que utiliza encaminamiento basado en la fuente y señalización distribuida. En la figura se indica el flujo de señalización de protección después de detectado un fallo del enlace. Se supone que la relación entre el enlace principal y el de protección es 1:1. Es decir, la CI no se transfiere simultáneamente al enlace principal y al de protección, sino que cuando un fallo interrumpe el trayecto principal, se utiliza el plano de control para conmutar la CI del usuario al trayecto de protección.



**Figura V.7/G.8080/Y.1304 – Flujo de señalización de protección**



**Figura V.8/G.8080/Y.1304 – Interacciones de protección**

En la figura V.8 se describe la secuencia detallada de las operaciones que suceden durante la protección. La siguiente es la lista de pasos que tienen lugar:

- 1) Al controlador de conexión (CC) llega una notificación de fallo de enlace bidireccional, generada por los gestores de recursos de enlace (LRM) y que contiene la información relativa al fallo de enlace. Esto sucede en el nodo E y en el nodo C.
- 2) La notificación de fallo de enlace se retransmite a  $CC_A$  desde  $CC_C$ , y a  $CC_G$  desde  $CC_E$ .
- 3) Se advierte a los NCC tanto de  $CC_A$  como de  $CC_G$  sobre el fallo del trayecto principal.
- 4) Los NCC dan inicio a la petición de conmutación de protección a sus CC, lo que hace que se establezca una SNC a través del conmutador local de la conexión principal a la conexión de protección.

#### V.4 Restablecimiento – Reencaminamiento rígido – Intradominio – Método jerárquico

En el reencaminamiento rígido, conocido como romper antes de construir, se libera el segmento inicial antes de crearse un segmento de conexión alternativo.

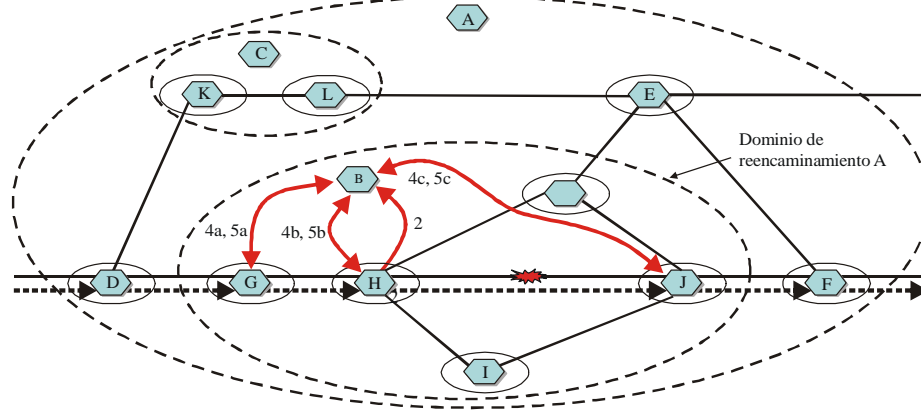
En la figura V.9 se muestra el flujo de señalización de un caso de reencaminamiento rígido con control de conexión jerárquico, después de que se ha detectado el fallo de un enlace dentro del dominio. En el paso de reencaminamiento se emplea el algoritmo jerárquico de creación de conexión.

En la figura V.10 se describe la secuencia detallada de las operaciones que suceden durante la protección en la figura 9. La siguiente es la lista de pasos que tienen lugar:

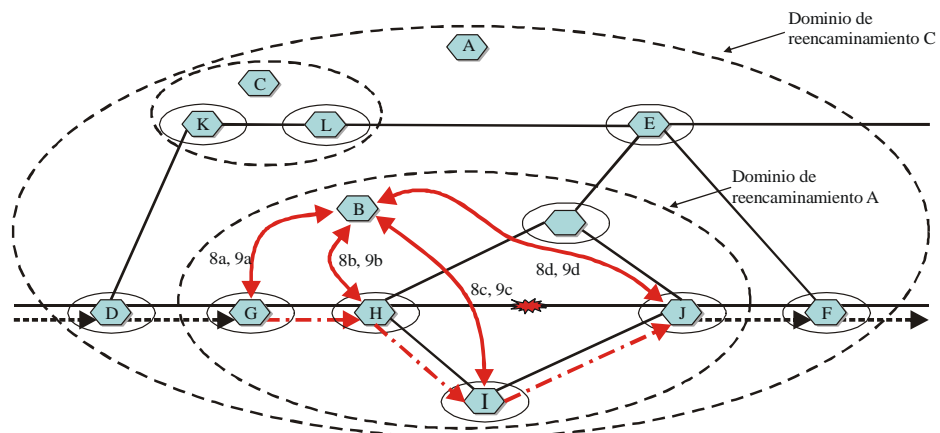
- 1) Al controlador de conexión (CC) llega una notificación de fallo de enlace dentro del dominio, generada por los gestores de recursos de enlace (LRM) y que contiene la información relativa al reencaminamiento automático hacia atrás. Esto puede ocurrir en el nodo J, en el nodo H, o en los dos, dependiendo del nodo que detecte el fallo de enlace.
- 2) Se retransmite a  $CC_B$  la notificación de fallo de enlace dentro del dominio.
- 3) El LRM libera las conexiones de enlace (en cualquier orden, es decir, 3a o 3b en la figura V.10).
- 4) Los conmutadores del nivel inferior liberan las SNC.
- 5) Las confirmaciones de liberación de conexión retornan al  $CC_B$ .
- 6) Se interroga al controlador de encaminamiento ( $RC_B$ ) respecto a la información de reencaminamiento automático hacia atrás, el cual devuelve el conjunto de enlaces del que se excluyen el enlace de fallo y las subredes afectadas.
- 7)-9) En los pasos 7 a 9 se describe el flujo de establecimiento de la conexión utilizando un algoritmo jerárquico idéntico al descrito en V.1, Encaminamiento jerárquico.

- 10) Si falla el establecimiento de la conexión en el dominio de reencaminamiento A, la información de reencaminamiento automático hacia atrás se retransmite al dominio de reencaminamiento C de nivel superior.
- 11) El LRM libera las conexiones de enlace restantes.
- 12) Los conmutadores del nivel inferior liberan las SNC. Esto requiere liberación en los nodos G y J a través de  $CC_B$ , luego a través de  $CC_G$  y de  $CC_J$ .
- 13) Las confirmaciones de liberación de conexión retornan al  $CC_A$ . Éstas incluyen la liberación de  $CC_B$ .
- 14) Se interroga  $RC_A$  respecto a la información de reencaminamiento automático hacia atrás, el cual devuelve el conjunto de enlaces del que se excluyen el enlace de fallo y las subredes afectadas.
- 15)-21) En los pasos 15 a 21 se describe el flujo de establecimiento de la conexión utilizando un algoritmo jerárquico idéntico al descrito en V.1, Encaminamiento jerárquico.
- 22) Si falla el establecimiento de la conexión en el dominio de reencaminamiento C, la información de reencaminamiento automático hacia atrás se retransmite al dominio de reencaminamiento de nivel superior.

**Paso 1: Liberar el segmento inicial de conexión en el dominio de reencaminamiento A**

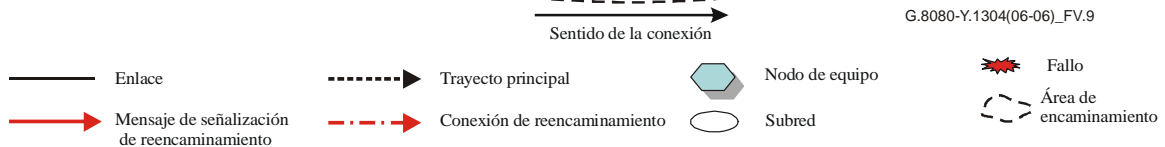
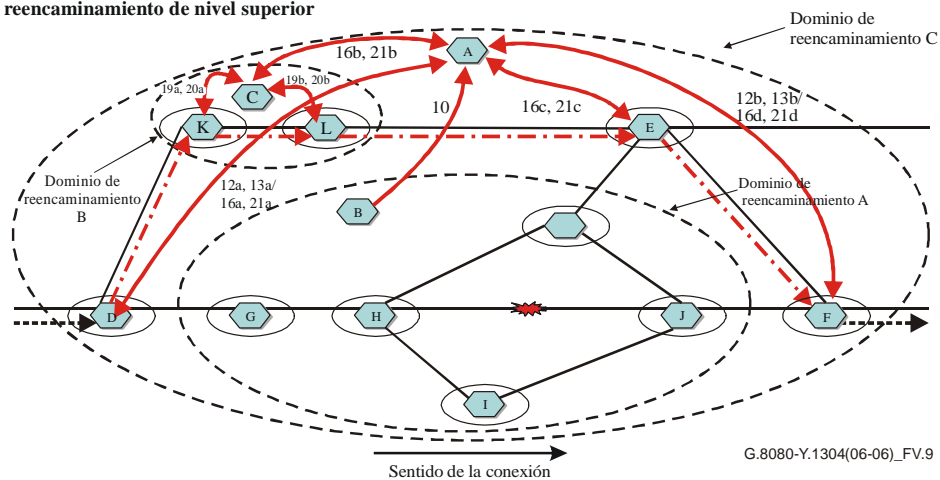


**Paso 2: Crear la conexión de reencaminamiento en el dominio de reencaminamiento A**

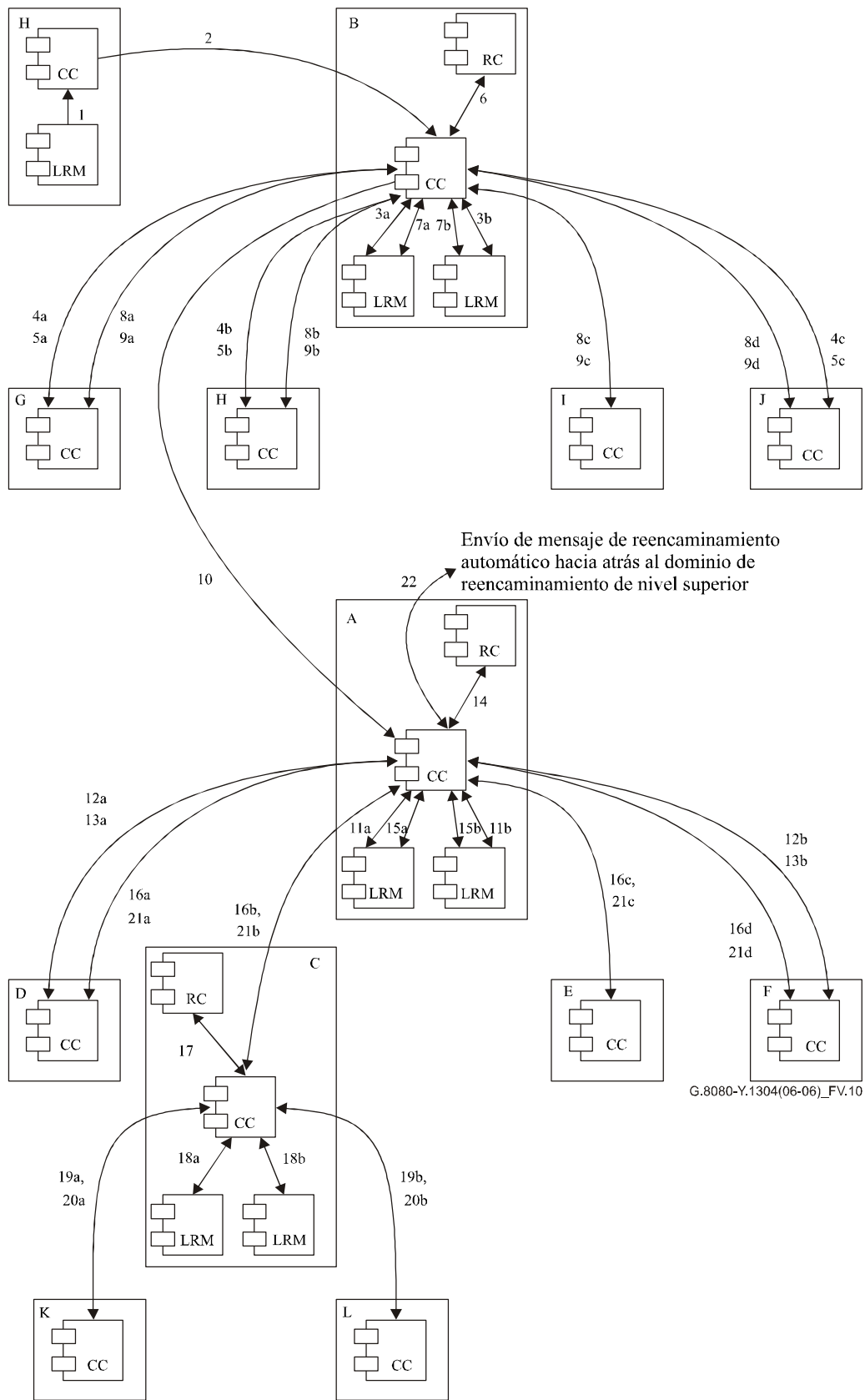


**Paso 3: Si falla el paso 2, efectuar reencaminamiento automático hacia atrás del mensaje de encaminamiento, hacia el dominio de reencaminamiento C, de nivel superior**

Si falla el establecimiento de la conexión de reencaminamiento en el dominio de reencaminamiento C, transmitir por reencaminamiento automático hacia atrás el mensaje de encaminamiento, hacia el dominio de reencaminamiento de nivel superior



**Figura V.9/G.8080/Y.1304 – Flujo de señalización para el reencaminamiento rígido, utilizando un algoritmo de reencaminamiento jerárquico, tras el fallo de un enlace dentro del dominio**



**Figura V.10/G.8080/Y.1304 – Interacción de los componentes para el reencaminamiento rígido, utilizando un algoritmo jerárquico, tras el fallo de un enlace dentro del dominio**



## V.5 Restablecimiento – Reencaminamiento flexible dentro del dominio – Método desde la fuente

El servicio de reencaminamiento flexible es un mecanismo para reencaminar las llamadas con fines administrativos. Cuando se activa una operación de reencaminamiento (generalmente mediante una petición del plano de gestión) y se envía al lugar de los componentes de reencaminamiento, éstos establecen una conexión de reencaminamiento que cruza (o podría no hacerlo) el conjunto de componentes elegidos, dependiendo de los fines administrativos. En reencaminamiento flexible, conocido como "construir antes de romper", se suprime la conexión inicial después de creada la conexión de reencaminamiento.

En la figura V.11 se muestra el flujo de señalización de un caso de reencaminamiento flexible con control de conexión de encaminamiento desde la fuente (o paso a paso), tras recibirse del plano de gestión una petición de reencaminar una conexión excluyendo un cierto enlace al interior del dominio.

En la figura V.12 se describe la secuencia detallada de las operaciones que se suceden en la figura V.11, usando encaminamiento desde la fuente. La siguiente es la lista de pasos que tienen lugar:

- 1) Al controlador de conexión ( $CC_G$ ) llega una petición del plano de gestión en la que se indican restricciones que debe cumplir la conexión de reencaminamiento. Por ejemplo, una ruta en particular de la conexión de reencaminamiento. En este ejemplo existe una restricción de exclusión que especifica que no debe utilizarse el enlace L1 en la conexión de reencaminamiento.
- 2a) El controlador de conexión ( $RC_G$ ) recibe una solicitud de establecimiento de conexión de reencaminamiento iniciada por  $CC_G$  que incluye el par de SNP en el borde del dominio de reencaminamiento A y la restricción de exclusión.
- 2b)  $RC_G$  retorna el conjunto de enlaces, excluyendo el enlace L1.
- 3-15) En los pasos 3 a 15 se describe el flujo del establecimiento de la conexión utilizando un algoritmo de encaminamiento desde la fuente idéntico al descrito en V.2.3 Combinación de los encaminamientos desde la fuente y paso a paso. La nueva conexión se empalma con la inicial, que ingresa al dominio A en G y en J.

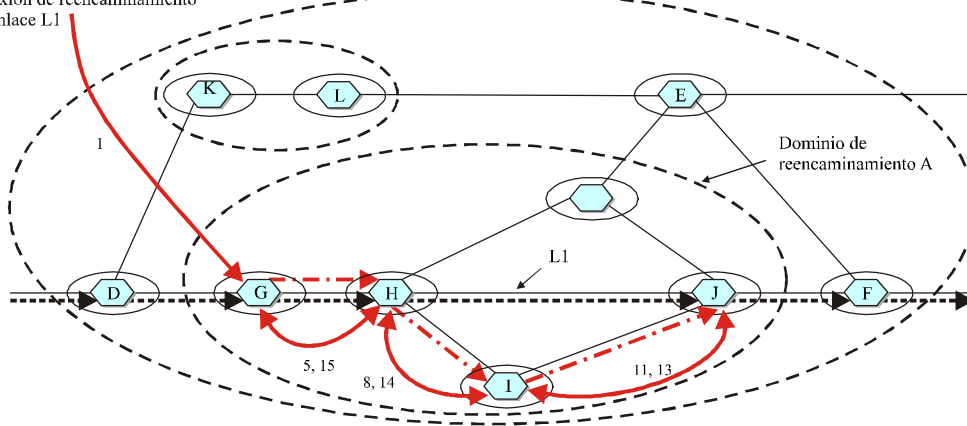
Si la conexión se establece exitosamente en el dominio de reencaminamiento A, se llevan a cabo los pasos 16a, en caso contrario, se llevan a cabo los pasos 16b.

- 16a) En el paso 16a, que consta de los pasos 16a1 y 16a2, el  $LRM_G$  libera la conexión de enlace del trayecto inicial.
- 17) Se libera la SNC que atraviesa el conmutador local.
- 18) Se retransmite a  $CC_H$  la petición de liberación de conexión, que contiene la información de la conexión inicial.
- 19) El  $LRM_H$  libera la conexión de enlace del trayecto inicial.
- 20) Se libera la SNC que atraviesa el conmutador local.
- 21) Se retransmite a  $CC_J$  la petición de liberación de conexión, que contiene la información de la conexión inicial.
- 22) Se libera la SNC que atraviesa el conmutador local.
- 23) Se devuelve la confirmación de liberación de conexión a la fuente  $CC_G$  y finaliza el proceso de reencaminamiento.
- 16b) La información de reencaminamiento automático hacia atrás se retransmite a  $CC_D$  en el dominio de reencaminamiento C del nivel superior.

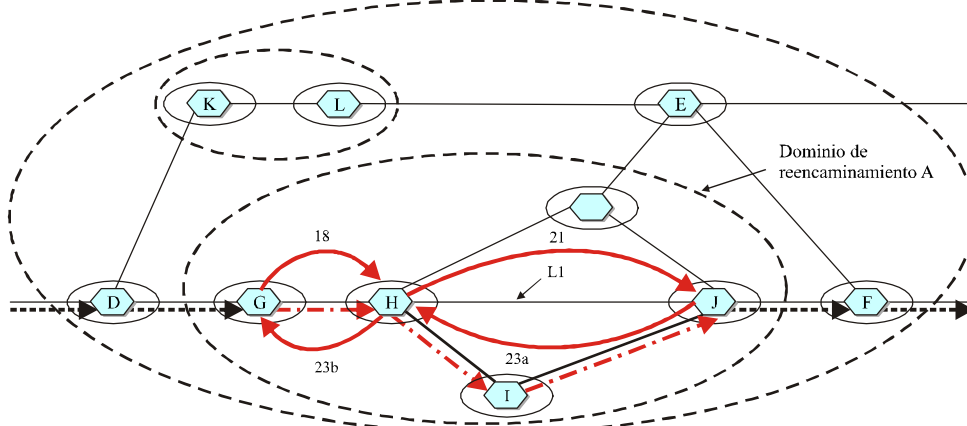
- 17a)  $RC_D$  recibe una petición de establecimiento de conexión de reencaminamiento iniciada por  $CC_D$  que incluye el par de SNP en el borde del dominio de reencaminamiento C y la restricción de exclusión de evitar el dominio A.
- 17b)  $RC_D$  devuelve el conjunto de enlaces, excluyendo el dominio A.
- 18)-39) En los pasos 18 a 39 se describe el flujo del establecimiento de conexión utilizando el algoritmo de enrutamiento desde la fuente idéntico al descrito en V.2.3 Combinación de los encaminamientos desde la fuente y paso a paso.
- 40) En el paso 40, que consta de los pasos 40a y 40b, el  $LRM_D$  libera la conexión de enlace del trayecto inicial.
- 41) Se libera la SNC que atraviesa el conmutador local.
- 42) Se retransmite a  $CC_G$  la petición de liberación de conexión, que contiene la información de la conexión inicial.
- 43) El  $LRM_G$  libera la conexión de enlace del trayecto inicial.
- 44) Se libera la SNC que atraviesa el conmutador local.
- 45) Se retransmite a  $CC_H$  la petición de liberación de conexión, que contiene la información de la conexión inicial.
- 46) El  $LRM_H$  libera la conexión de enlace del trayecto inicial.
- 47) Se libera la SNC que atraviesa el conmutador local.
- 48) Se retransmite a  $CC_J$  la petición de liberación de conexión, que contiene la información de la conexión inicial.
- 49) El  $LRM_J$  libera la conexión de enlace del trayecto inicial.
- 50) Se libera la SNC que atraviesa el conmutador local.
- 51) Se retransmite a  $CC_F$  la petición de liberación de conexión, que contiene la información de la conexión inicial.
- 52) Se libera la SNC que atraviesa el conmutador local.
- 53) Se devuelve la confirmación de liberación de conexión a la fuente  $CC_D$ .

**Paso 1: Crear la conexión de reencaminamiento en el dominio de reencaminamiento A**

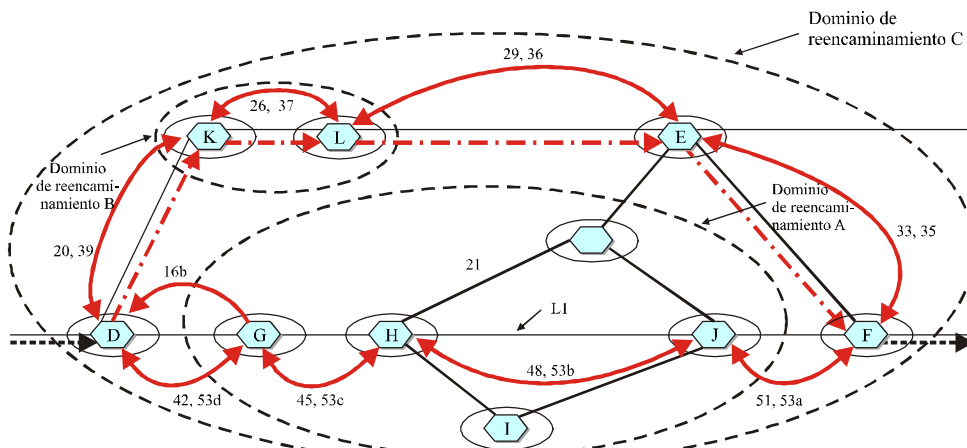
Petición de reencaminamiento del plano de gestión solicitando que se cree una conexión de reencaminamiento que no atraviese el enlace L1



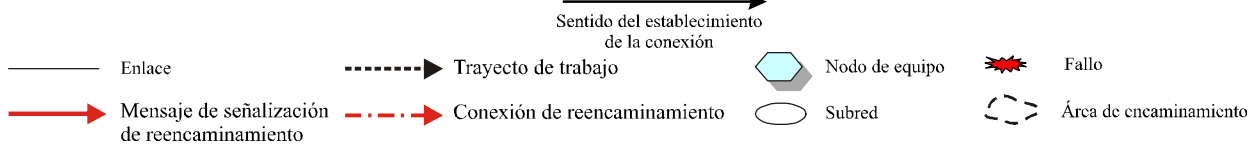
**Paso 2: Liberar el segmento de conexión inicial en el dominio de reencaminamiento A**



**Paso 3: Si falla el paso 1, efectuar reencaminamiento automático hacia atrás del mensaje de encaminamiento, hacia el dominio de reencaminamiento C, de nivel superior**

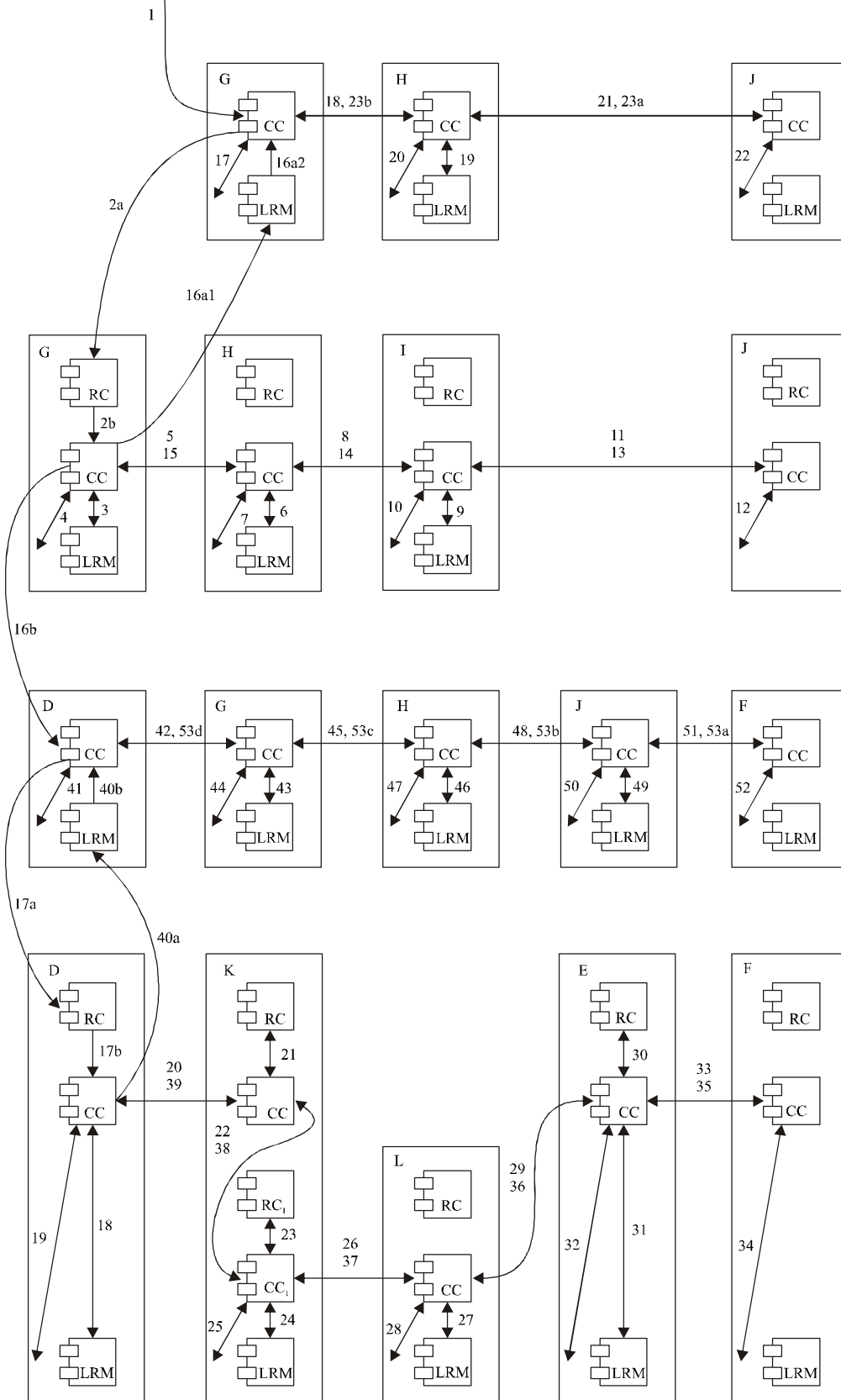


G.8080-Y.1304(06-06)\_FV.11



**Figura V.11/G.8080/Y.1304 – Flujo de señalización para el reencaminamiento flexible utilizando el algoritmo de encaminamiento desde la fuente (o paso a paso) y excluyendo un enlace dentro del dominio**

Petición de reencaminamiento del plano de gestión solicitando que se cree una conexión de reencaminamiento que no atraviese el enlace L1



G.8080-Y.1304(06-06)\_FV.12

**Figura V.12/G.8080/Y.1304 – Interacciones de los componentes para el reencaminamiento flexible utilizando el algoritmo desde la fuente y excluyendo un enlace dentro del dominio**

## **V.6 Restablecimiento – Reencaminamiento reversible – Intradominio – Método desde la fuente**

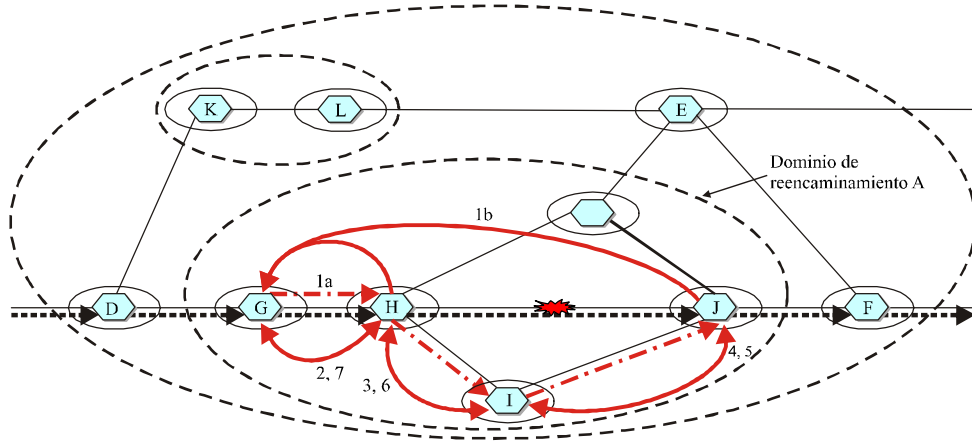
En el reencaminamiento con comportamiento reversible no es permitido liberar la conexión inicial y ésta es supervisada por los controladores de llamada de red. Una vez reparado el fallo, se restablece la llamada utilizando la conexión inicial.

En la figura V.13 se muestra un caso de reencaminamiento con comportamiento reversible y con control de conexión de reencaminamiento desde la fuente (o paso a paso), después de que se ha detectado un fallo dentro del dominio.

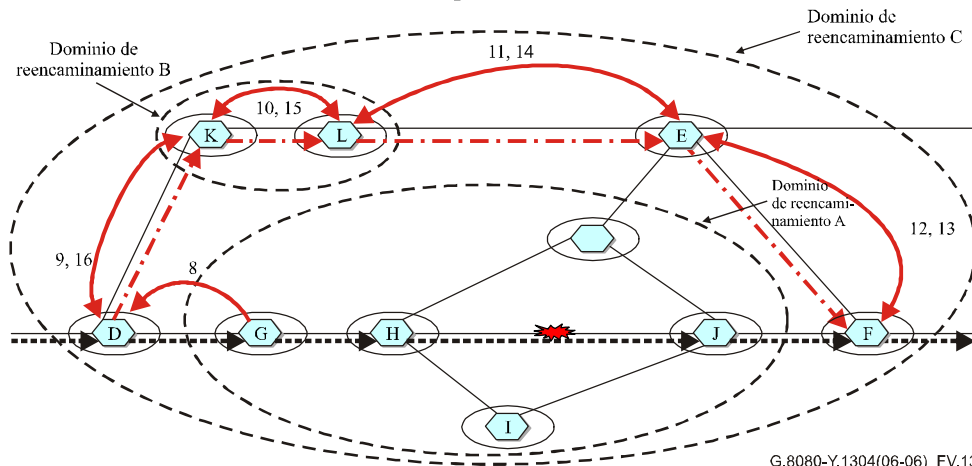
En la figura V.14, se describe la secuencia detallada de las operaciones que se suceden usando encaminamiento desde la fuente en la figura V.13. La siguiente es la lista de pasos que tienen lugar:

- 1) Al controlador de conexión (CC) llega una notificación de fallo de enlace dentro del dominio, generada por los gestores de recursos de enlace (LRM) y que contiene la información relativa al reencaminamiento automático hacia atrás que especifica el enlace de fallo. Esto puede ocurrir en el nodo J, en el nodo H, o en los dos, dependiendo del nodo que detecte el fallo de enlace.
- 2) Se retransmite a  $CC_G$  la notificación de fallo de enlace dentro del dominio. No se modifican SCN.
- 3) Se interroga al controlador de encaminamiento ( $RC_G$ ) respecto a información de reencaminamiento automático hacia atrás, el cual devuelve el conjunto de enlaces, excluyendo el enlace de fallo y las subredes afectadas.
- 4)-16) En los pasos 4 a 16 se describe el flujo de establecimiento de conexión utilizando un algoritmo de encaminamiento desde la fuente idéntico al descrito en V.2.3 Combinación de los encaminamientos desde la fuente y paso a paso.
- 17) Si falla el establecimiento de la conexión en el dominio de reencaminamiento A, la información de reencaminamiento automático hacia atrás se retransmite al dominio de reencaminamiento C de nivel superior.
- 18) Se interroga  $RC_D$  respecto a información de reencaminamiento automático hacia atrás, el cual devuelve el conjunto de enlaces excluyendo el dominio A.
- 19)-40) Los pasos 19 a 40 describen el establecimiento de la conexión utilizando un algoritmo de encaminamiento desde la fuente idéntico al descrito en V.2.3 Combinación de los encaminamientos desde la fuente y paso a paso.

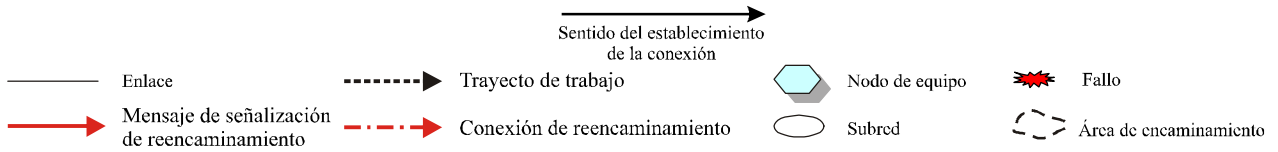
**Paso 1: Crear la conexión de reencaminamiento en el dominio de reencaminamiento A**



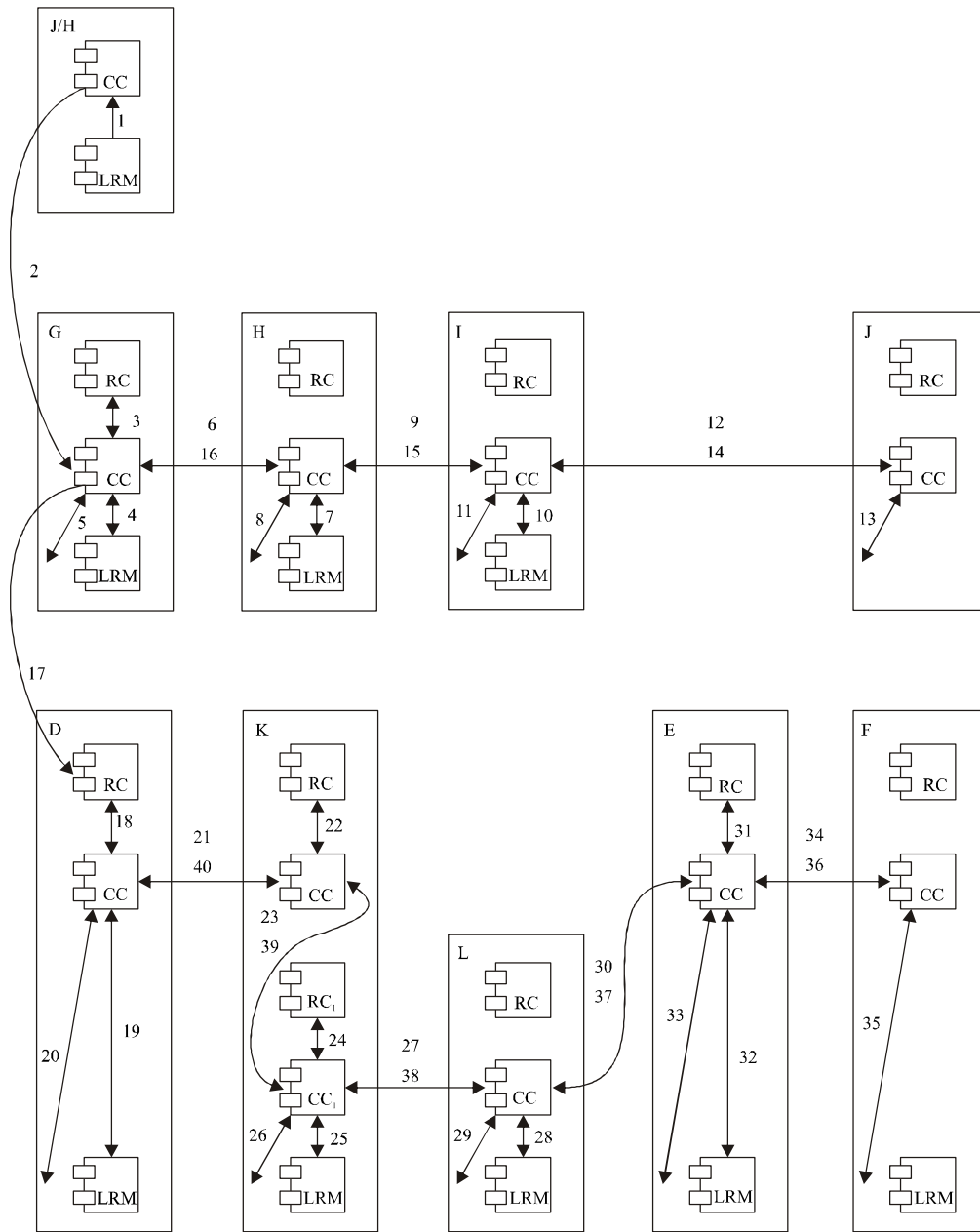
**Paso 2: Si falla el paso 1, efectuar reencaminamiento automático hacia atrás del mensaje de encaminamiento, hacia el dominio de reencaminamiento C, de nivel superior**



G.8080-Y.1304(06-06)\_FV.13



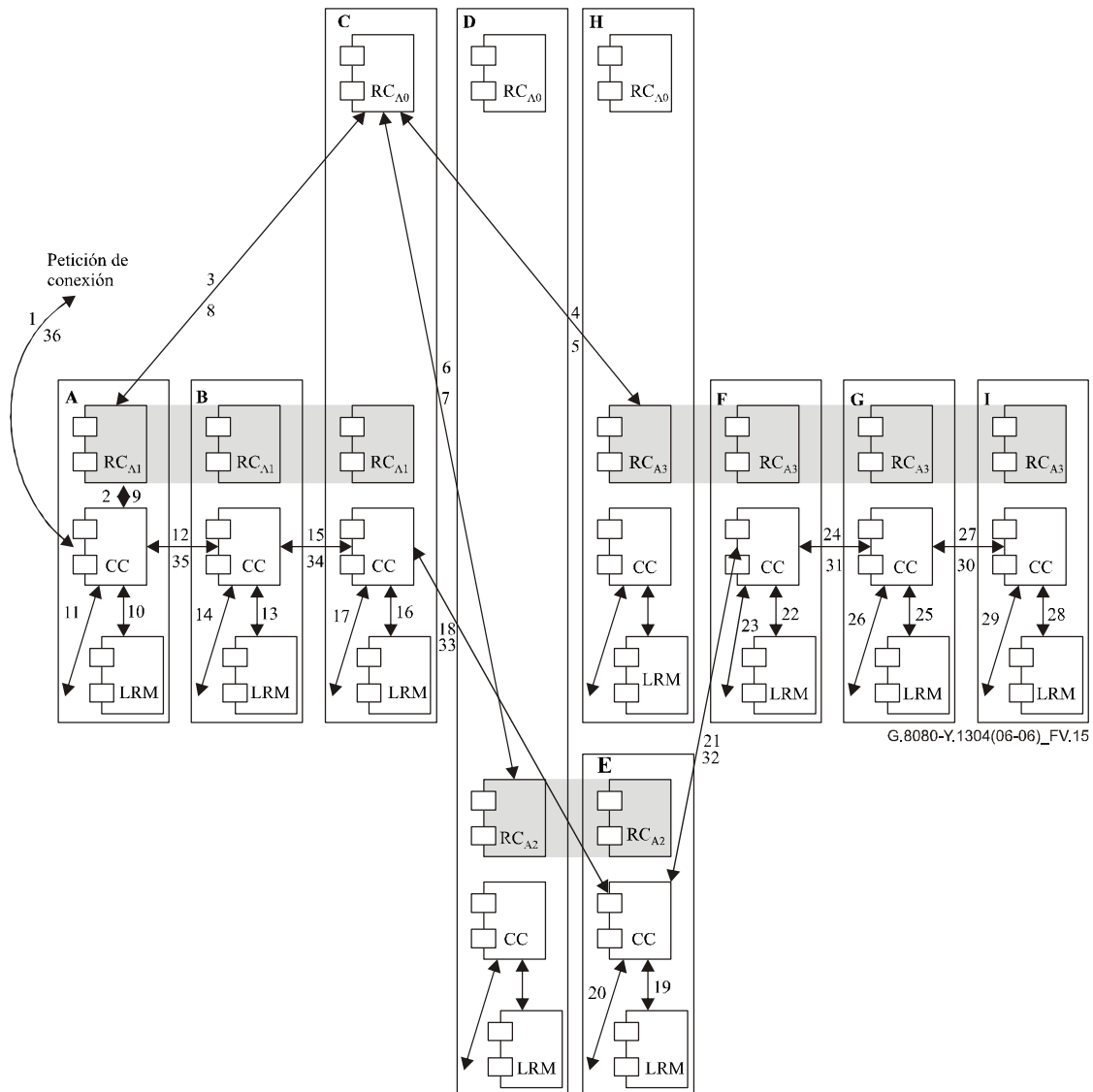
**Figura V.13/G.8080/Y.1304 – Flujo de señalización para el reencaminamiento con comportamiento reversible utilizando el algoritmo de encaminamiento desde la fuente (o paso a paso), tras el fallo de un enlace dentro del dominio**



G.8080-Y.1304(06-06)\_FV.14

**Figura V.14/G.8080/Y.1304 – Interacciones de los componentes para reencaminamiento con comportamiento reversible, utilizando el algoritmo de reencaminamiento desde la fuente tras el fallo de un enlace dentro del dominio**

## V.7 Encaminamiento desde la fuente utilizando la interfaz interrogación de rutas



**Figura V.15/G.8080/Y.1304 – Interacción de los componentes para el encaminamiento desde la fuente utilizando la interfaz interrogación de rutas**

En la figura V.15 se ilustra la secuencia detallada de operaciones que tiene lugar al establecerse una conexión utilizando encaminamiento con ayuda de interrogación entre RC. La notación  $RC_{A1}$ ,  $RC_{A2}$ , etc., representa al controlador de encaminamiento en el área A1, A2, etc. Los componentes de comunicación podrían en realidad ser suministrados por otros componentes intermedios. Por ejemplo, la comunicación del  $RC_{A0}$  en el nodo C al  $RC_{A2}$  del nodo D podría realizarse transfiriendo el mensaje a través del  $RC_{A0}$  del nodo D.

A continuación se presentan los pasos que se llevan a cabo:

- 1) Llega al controlador de conexión ( $CC_A$ ) una petición de conexión procedente de la interfaz petición de conexión de entrada, especificada como un par de nombres (A y Z) en el borde de la subred.
- 2) El controlador encaminamiento  $RC_{A1}$  del nodo A es interrogado (utilizando el SNP del extremo Z a través de la interfaz de interrogación de rutas).



- 3) El controlador de encaminamiento  $RC_{A1}$  del nodo A se da cuenta de que no le es posible ver la dirección de destino desde el área A1, por lo que envía, a través de la interfaz interrogación de rutas, una petición de ruta a  $RC_{A0}$  del nodo C, solicitando ayuda. Mientras que  $RC_{A1}$  del nodo C posee la misma información de encaminamiento que  $RC_{A1}$  del nodo A, ya que los dos están en un área de encaminamiento común,  $RC_{A0}$  del nodo C puede ver el destino, haciendo que sea posible el cálculo de un trayecto.
- 4) Durante el cálculo de un trayecto al destino,  $RC_{A0}$  del nodo C se da cuenta de que para llegar al destino necesita alcanzar el área A3. Sin embargo, como hay varios trayectos entre el área A1 y el área A3, requiere de la ayuda de  $RC_{A2}$  y  $RC_{A3}$  para determinar el mejor trayecto. Por lo tanto,  $RC_{A0}$  del nodo C envía una petición a  $RC_{A3}$  del nodo H para determinar el enlace de A2 a A3 que debería usar.
- 5)  $RC_{A3}$  del nodo H calcula los posibles trayectos al destino en el área A3, a partir de los enlaces que ingresan al área A3 desde el área A2. A partir de esto, puede calcular el costo de utilizar cualquiera de los caminos, y retorna esa información al  $RC_{A0}$  del nodo C.
- 6) Así como ocurrió con  $RC_{A3}$  del nodo H,  $RC_{A0}$  del nodo C envía una petición a  $RC_{A2}$  del nodo D a fin de determinar los trayectos entre los nodos de egreso que salen del área A2 e ingresan al área A3 y los enlaces de ingreso que entran al área A2 del área A1.
- 7)  $RC_{A2}$  del nodo D calcula los posibles trayectos a través del área A2 y retorna esa información a  $RC_{A0}$  del nodo C.
- 8)  $C_{A0}$  del nodo C proporciona a  $RC_{A1}$  del nodo A la lista de trayectos calculados desde el borde del área A1 al área de destino A3 e incluye el costo total de cada uno de los trayectos calculados.
- 9) El  $RC_{A1}$  del nodo A posee ahora la información necesaria para calcular un trayecto a través del área A1, empleando la información de costos proporcionada por  $RC_{A0}$  del nodo C para determinar el trayecto extremo a extremo de menor costo. En el resto de este ejemplo se supone que el trayecto elegido se inicia en A, sigue por L1 hasta B, por L2 hasta C, por L3 hasta E, por L4 hasta F, por L5 hasta G y por L6 hasta I. El  $RC_{A1}$  del nodo A envía luego la respuesta al CC del nodo A, que inicia el proceso de formación de la petición de conexión extremo a extremo utilizando la ruta (A, L1, L2, L3, L4, L5, L6 y Z).
- 10) L1 es local respecto al nodo A, y se obtiene de  $LRM_A$  un enlace de conexión para L1, a través de la interfaz de petición de conexión de enlace.
- 11) Se establece la SNC apropiada en el conmutador local (no se muestra el controlador).
- 12) Luego se retransmite la petición de conexión (L2, L3, L4, L5, L6 y Z) al siguiente CC, en el nodo B (por la interfaz de coordinación de entidad par de entrada/salida).
- 13)  $LRM_B$  controla el enlace L2, por lo que se obtiene una conexión de enlace de este enlace a través de la interfaz de petición de conexión.
- 14) Se establece la SNC apropiada en el conmutador local (no se muestra el controlador).
- 15) Luego se retransmite la petición de conexión (L3, L4, L5, L6 y Z) al siguiente CC, en el nodo C (por la interfaz de coordinación de entidad par de entrada/salida).
- 16)  $LRM_C$  controla el enlace L3, por lo que se obtiene una conexión de enlace de este enlace a través de la interfaz de petición de conexión.
- 17) Se establece la SNC apropiada en el conmutador local (no se muestra el controlador).
- 18) Luego se retransmite la petición de conexión (L4, L5, L6 y Z) al siguiente CC, en el nodo E (por la interfaz de coordinación de entidad par de entrada/salida).
- 19)  $LRM_E$  controla el enlace L4, por lo que se obtiene una conexión de enlace de este enlace a través de la interfaz de petición de conexión.
- 20) Se establece la SNC apropiada en el conmutador local (no se muestra el controlador).

- 21) Luego se retransmite la petición de conexión (L5, L6 y Z) al siguiente CC, en el nodo F (por la interfaz de coordinación de entidad par de entrada/salida).
- 22)  $LRM_F$  controla el enlace L5, por lo que se obtiene una conexión de enlace de este enlace a través de la interfaz de petición de conexión.
- 23) Se establece la SNC apropiada en el conmutador local (no se muestra el controlador).
- 24) Luego se retransmite la petición de conexión (L6 y Z) al siguiente CC, en el nodo G (por la interfaz de coordinación de entidad par de entrada/salida).
- 25)  $LRM_G$  controla el enlace L6, por lo que se obtiene una conexión de enlace de este enlace a través de la interfaz de petición de conexión.
- 26) Se establece la SNC apropiada en el conmutador local (no se muestra el controlador).
- 27) Luego se retransmite la petición de conexión (Z) al siguiente CC, en el nodo I (por la interfaz de coordinación de entidad par de entrada/salida).
- 28)  $LRM_I$  controla el enlace de salida, por lo que se obtiene una conexión de enlace para este enlace a través de la interfaz de petición de conexión.
- 29) Se establece la SNC apropiada en el conmutador local (no se muestra el controlador).
- 30) Luego el CC del nodo I envía una confirmación al CC del nodo G. Luego se repite el intercambio de respuestas entre los pares de CC hasta devolverse al CC que inició la conexión en el nodo A.

## BIBLIOGRAFÍA

- IETF RFC 2753 (2000), *A Framework for Policy-based Admission Control*.
- Unified Modelling Language (UML) (OMG UML Specification v. 1.3:OMG document ad/99-06-08).



RECOMENDACIONES UIT-T DE LA SERIE Y

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

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

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

## SERIES DE RECOMENDACIONES DEL UIT-T

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