UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T G.7712/Y.1703

(03/2003)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

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

Equipos terminales digitales – Características de operación, administración y mantenimiento de los equipos de transmisión

SERIE Y: INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN Y ASPECTOS DEL PROTOCOLO INTERNET

Aspectos del protocolo Internet – Operaciones, administración y mantenimiento

Arquitectura y especificación de la red de comunicación de datos

Recomendación UIT-T G.7712/Y.1703

RECOMENDACIONES UIT-T DE LA SERIE G

SISTEMAS Y MEDIOS DE TRANSMISIÓN, SISTEMAS Y REDES DIGITALES

CONEXIONES Y CIRCUITOS TELEFÓNICOS INTERNACIONALES	G.100–G.199
CARACTERÍSTICAS GENERALES COMUNES A TODOS LOS SISTEMAS ANALÓGICOS DE PORTADORAS	G.200–G.299
CARACTERÍSTICAS INDIVIDUALES DE LOS SISTEMAS TELEFÓNICOS INTERNACIONALES DE PORTADORAS EN LÍNEAS METÁLICAS	G.300–G.399
CARACTERÍSTICAS GENERALES DE LOS SISTEMAS TELEFÓNICOS INTERNACIONALES EN RADIOENLACES O POR SATÉLITE E INTERCONEXIÓN CON LOS SISTEMAS EN LÍNEAS METÁLICAS	G.400–G.449
COORDINACIÓN DE LA RADIOTELEFONÍA Y LA TELEFONÍA EN LÍNEA	G.450–G.499
EQUIPOS DE PRUEBAS	G.500–G.599
CARACTERÍSTICAS DE LOS MEDIOS DE TRANSMISIÓN	G.600–G.699
EQUIPOS TERMINALES DIGITALES	G.700–G.799
REDES DIGITALES	G.800–G.899
SECCIONES DIGITALES Y SISTEMAS DIGITALES DE LÍNEA	G.900–G.999
CALIDAD DE SERVICIO Y DE TRANSMISIÓN - ASPECTOS GENÉRICOS Y ASPECTOS RELACIONADOS AL USUARIO	G.1000–G.1999
CARACTERÍSTICAS DE LOS MEDIOS DE TRANSMISIÓN	G.6000–G.6999
EQUIPOS TERMINALES DIGITALES	G.7000–G.7999
Generalidades	G.7000–G.7099
Codificación de señales analógicas mediante modulación por impulsos codificados (MIC)	G.7100–G.7199
Codificación de señales analógicas mediante métodos diferentes de la MIC	G.7200–G.7299
Características principales de los equipos múltiplex primarios	G.7300–G.7399
Características principales de los equipos múltiplex de segundo orden	G.7400–G.7499
Características principales de los equipos múltiplex de orden superior	G.7500–G.7599
Características principales de los transcodificadores y de los equipos de multiplicación de circuitos digitales	G.7600–G.7699
Características de operación, administración y mantenimiento de los equipos de transmisión	**G.7700–G.7799**
Características principales de los equipos múltiplex de la jerarquía digital síncrona	G.7800–G.7899
Otros equipos terminales	G.7900–G.7999
REDES DIGITALES	G.8000–G.8999

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

Recomendación UIT-T G.7712/Y.1703

Arquitectura y especificación de la red de comunicación de datos

Resumen

En esta Recomendación se definen los requisitos que debe satisfacer la arquitectura de una red de comunicación de datos (RCD) para soportar las comunicaciones distribuidas de gestión relacionadas con la red de gestión de las telecomunicaciones (RGT), las comunicaciones distribuidas de señalización relacionadas con la red de transporte con conmutación automática (ASTN, *automatic switched transport network*) y otras comunicaciones distribuidas (por ejemplo, las comunicaciones de línea de servicio o de voz y las descargas de soporte lógico). La arquitectura RCD contempla las redes exclusivamente IP, las redes exclusivamente OSI y las redes mixtas (es decir, aquellas que soportan tanto IP como OSI). También se especifica el interfuncionamiento entre las partes de la RCD que soportan exclusivamente IP, las partes que soportan exclusivamente OSI y las partes que soportan tanto IP como OSI.

Hay varias aplicaciones (RGT, ASTN, etc.) que necesitan una red de comunicaciones por paquetes para transportar información entre los distintos componentes. Por ejemplo, en la RGT es necesaria una red de comunicaciones, conocida como red de comunicaciones de gestión (RCG), para transportar los mensajes de gestión entre los componentes de la RGT (por ejemplo, el componente NEF (*network element function*) y el componente OSF (*operations system function*). En la ASTN es necesaria una red de comunicaciones, conocida como red de comunicaciones de señalización (RCS), para transportar los mensajes de señalización entre los componentes ASTN (por ejemplo, los componentes CC (*connection controller*)). En esta Recomendación se especifican funciones de comunicaciones de datos que se pueden utilizar para soportar una o más redes de comunicaciones de aplicación.

Las funciones de comunicaciones de datos previstas en la versión 11/2001 de esta Recomendación soportan servicios de red sin conexión. Esta revisión de la Recomendación incorpora el soporte de los servicios RCS de red con conexión, mediante la inclusión de un mecanismo específico basado en MPLS.

Esta Recomendación forma parte de una serie de Recomendaciones dedicadas a las redes de transporte.

Orígenes

La Recomendación UIT-T G.7712/Y.1703 fue aprobada por la Comisión de Estudio 15 (2001-2004) del UIT-T por el procedimiento de la Recomendación UIT-T A.8 el 16 de marzo de 2003.

Historia del documento	
Elemento	**Observaciones**
1.0	Resultado de la reunión Q14/15 de octubre de 2001
1.1	Resultado de la reunión Q14/15 de abril de 2002
1.2	Versión corregida de 1.1
1.3	Resultado de la reunión Q14/15 de octubre de 2002
1.4	Revisión de la versión 1.3: sustitución de las cabeceras de sección 7.1.a, etc. por 7.1.13, etc. Supresión de los comentarios editoriales.
1.5	Resultado de la reunión Q14/15 y sometimiento a aprobación

Palabras clave

Interfaz de sistema abierto (OSI), protocolo de Internet (IP), red de comunicación de datos.

PREFACIO

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

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

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

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

NOTA

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

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

PROPIEDAD INTELECTUAL

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

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

ÍNDICE

Página

Recomendación UIT-T G.7712/Y.1703

Arquitectura y especificación de la red de comunicación de datos

1 Alcance

En esta Recomendación se definen los requisitos que debe satisfacer la arquitectura de una red de comunicación de datos (RCD) para soportar las comunicaciones distribuidas de gestión relacionadas con la red de gestión de telecomunicaciones (RGT), las comunicaciones distribuidas de señalización relacionadas con la red de transporte conmutada automáticamente (ASTN) y otras comunicaciones distribuidas (por ejemplo, comunicaciones de línea de servicio o de voz y descargas de soporte lógico). La arquitectura RCD contempla las redes exclusivamente IP, las redes exclusivamente OSI y las redes mixtas (es decir, aquellas que soportan tanto IP como OSI). También se especifica el interfuncionamiento entre las partes de la RCD que soportan exclusivamente IP, las partes que soportan exclusivamente OSI, y las partes que soportan tanto IP como OSI.

La RCD proporciona funcionalidades de capa 1 (física), de capa 2 (enlace de datos) y de capa 3 (red), estando dotada de funcionalidades de encaminamiento/conmutación interconectadas a través de enlaces. Estos enlaces se pueden implementar en diversas interfaces, entre ellas las interfaces de red de área extensa (WAN, *wide area network*), las interfaces de red de área local (LAN, *local area network*) y los canales de control integrados (ECC, *embedded control channel*).

Hay varias aplicaciones (por ejemplo, RGT, ASTN, etc.) que necesitan una red de comunicaciones por paquetes para transportar información entre los diversos componentes. Por ejemplo, en la RGT es necesaria una red de comunicaciones, conocida como red de comunicación de gestión (RCG), para transportar los mensajes de gestión entre los componentes de la RGT (por ejemplo, el componente NEF (*network element function*) y el componente OSF (*operations system function*). En la ASTN es necesaria una red de comunicaciones, conocida como red de comunicaciones de señalización (RCS), para transportar los mensajes de señalización entre los componentes ASTN (por ejemplo, los componentes CC (*connection controller*)). En esta Recomendación se especifican funciones de comunicaciones de datos que se pueden utilizar para soportar una o más redes de comunicaciones de aplicación.

Las funciones de comunicaciones de datos presentadas en esta Recomendación soportan servicios de red sin conexión. En futuras versiones de esta Recomendación podrán añadirse otras funciones de soporte de los servicios de red con conexión.

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 acutalmente 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.707/Y.1322 (2000), *Interfaz de nodo de red para la jerarquía digital síncrona*.

– Recomendación UIT-T G.709/Y.1331 (2003), *Interfaz de nodo de red para la red de transporte óptica*.

- Recomendación UIT-T G.783 (2000), *Características de los bloques funcionales del equipo de la jerarquía digital síncrona*.
- Recomendación UIT-T G.784 (1999), *Gestión de la jerarquía digital síncrona*.
- Recomendación UIT-T G.798 (2000), *Características de los bloques funcionales de equipo de la jerarquía de la red de transporte óptica*.
- Recomendación UIT-T G.807/Y.1302 (2001), *Requisitos de la red de transporte con conmutación automática*.
- Recomendación UIT-T G.872 (2001), *Arquitectura de las redes de transporte ópticas*.
- Recomendación UIT-T G.874 (2001), *Aspectos de gestión del elemento de red de transporte óptica*.
- Recomendación UIT-T G.7710/Y.1701 (2001), *Requisitos de la función de gestión de equipo común*.
- Recomendación UIT-T G.8080/Y.1304 (2001), *Arquitectura para las redes ópticas conmutadas automáticas*.
- Recomendación UIT-T M.3010 (2000), *Principios para una red de gestión de las telecomunicaciones*.
- Recomendación UIT-T M.3013 (2000), *Consideraciones sobre una red de gestión de las telecomunicaciones*.
- Recomendación UIT-T M.3016 (1998), *Visión general de la seguridad en la red de gestión de las telecomunicaciones*.
- Recomendación UIT-T Q.811 (1997), *Perfiles de protocolo de capa inferior para las interfaces Q3 y X*.
- Recomendación UIT-T X.263 (1998) | ISO/CEI TR 9577:1999, *Tecnología de la información – Identificación de protocolos en la capa de red*.
- ISO/CEI 9542:1998, *Information processing systems – Telecommunications and information exchange between systems – End system to Intermediate system routeing exchange protocol for use in conjunction with the Protocol for providing the connectionless-mode network service (ISO 8473)*.
- ISO/CEI 10589:2002, *Information technology – Telecommunications and information exchange between systems – Intermediate System to Intermediate System intra-domain routeing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473)*.
- IETF RFC 791 (1981), *Internet Protocol DARPA Internet Program Protocol Specification*.
- IETF RFC 792 (1981), *Internet Control Message Protocol*.
- IETF RFC 826 (1982), *An Ethernet Address Resolution Protocol*.
- IETF RFC 894 (1984), *A Standard for the Transmission of IP Datagrams over Ethernet Networks*.
- IETF RFC 1122 (1989), *Requirements for Internet Hosts – Communication Layers*.
- IETF RFC 1172 (1990), *The Point-to-Point Protocol (PPP) Initial Configuration Options*.
- IETF RFC 1195 (1990), *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*.
- IETF RFC 1332 (1992), *The PPP Internet Protocol Control Protocol (IPCP)*.

– IETF RFC 1377 (1992), *The PPP OSI Network Layer Control Protocol (OSINLCP)*.

– IETF RFC 1661 (1994), *The Point-to-Point Protocol (PPP)*.

– IETF RFC 1662 (1994), *PPP in HDLC-like Framing*.

– IETF RFC 1812 (1995), *Requirements for IP Version 4 Routers*.

– IETF RFC 2328 (1998), *OSPF Version 2*.

– IETF RFC 2460 (1998), *Internet Protocol, Version 6 (IPv6) Specification*.

– IETF RFC 2463 (1998), *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*.

– IETF RFC 2472 (1998), *IP Version 6 over PPP*.

– IETF RFC 2740 (1999), *OSPF for IPv6*.

– IETF RFC 2784 (2000), *Generic Routing Encapsulation (GRE)*.

3 Términos y definiciones

3.1 Términos definidos en la Rec. UIT-T G.709/Y.1331:

a) Unidad de datos de canal óptico (ODUk)

b) Unidad de transporte de canal óptico (OTUk)

c) Señal de tara óptica (OOS)

3.2 Términos definidos en la Rec. UIT-T G.784:

a) Canal de comunicaciones de datos (DCC)

3.3 Términos definidos en la Rec. UIT-T G.807/Y.1302:

a) Red de transporte conmutada automáticamente (ASTN)

b) Interfaz red-red (NNI)

c) Interfaz usuario-red (UNI)

3.4 Términos definidos en la Rec. UIT-T G.8080:

a) Controlador de llamada (CallC)

b) Controlador de conexión (CC)

c) Interfaz de controlador de conexión (CCI)

d) Controlador de subred (SNCr)

3.5 Términos definidos en la Rec. UIT-T G.874:

a) Canal de comunicaciones generales (GCC)

b) Tara de comunicaciones de gestión generales (COMMS OH)

3.6 Términos definidos en la Rec. UIT-T G.7710/Y.1701:

a) Red de gestión X

b) Subred de gestión X

3.7 Términos definidos en la Rec. UIT-T G.872:

a) Elemento de transporte óptico (OTN)

3.8 Términos definidos en la Rec. UIT-T M.3010:

a) Dispositivo de adaptación (AD)

b) Función de comunicaciones de datos (DCF)

c) Dispositivo de mediación (MD)

d) Elemento de red (NE)

e) Función de elemento de red (NEF)

f) Sistema de operaciones (OS)

g) Función del sistema de operaciones (OSF)

h) Interfaz Q

i) Función de traducción

j) Función de estación de trabajo (WSF)

3.9 Términos definidos en la Rec. UIT-T M.3013:

a) Función de comunicaciones de mensajes (MCF)

3.10 En esta Recomendación se definen los siguientes términos.

3.10.1 red de comunicación de datos (RCD): La RCD es una red que soporta las funcionalidades de capa 1 (física), de capa 2 (enlace de datos) y de capa 3 (red). La RCD puede estar diseñada para soportar el transporte de comunicaciones distribuidas de gestión relacionadas con la RGT, comunicaciones distribuidas de señalización relacionadas con la ASTN y otras comunicaciones de operaciones (por ejemplo comunicaciones de línea de servicio/voz, o descarga de soporte lógico, etc.).

3.10.2 canal de control integrado (ECC, *embedded control channel*): Un ECC proporciona un canal lógico de operaciones entre elementos de red. El canal físico que soporta el ECC depende de la tecnología utilizada. Los siguientes son ejemplos de canales físicos que soportan el ECC: un canal DCC dentro de la jerarquía digital síncrona (SDH), un canal GCC dentro de una OTUk/ODUk de la OTN, o el canal de tara de comunicaciones de gestión generales (COMMS OH) dentro de una OOS de la OTN.

3.10.3 función de interfuncionamiento del encaminamiento IP: La función de interfuncionamiento del encaminamiento IP permite el paso de la topología IP o de las rutas IP desde un protocolo de encaminamiento IP a otro protocolo de encaminamiento IP incompatible. Por ejemplo, una función de interfuncionamiento de encaminamiento IP puede constituir una pasarela entre una RCD encaminada mediante un IS-IS integrado y una RCD encaminada mediante OSPF.

3.10.4 función de interfuncionamiento de la capa de red: La función de interfuncionamiento de la capa de red proporciona la interoperabilidad entre nodos que soportan protocolos de capa de red incompatibles. Un ejemplo de función de interfuncionamiento de capa de red son los túneles GRE estáticos y la AE-DCF.

3.10.5 función de comunicaciones de datos con encapsulación automática (AE-DCF, *automatic encapsulating data communications function*): La AE-DCF encapsula automáticamente los paquetes cuando es necesario de modo que puedan encaminarlos los NE que de lo contrario no podrían reenviarlos. La AE-DCF dispone asimismo de la correspondiente función de desencapsulación para restaurar el paquete a su forma original una vez a atravesados los NE incompatibles.

4 Abreviaturas

En esta Recomendación se utilizan las siguientes siglas.

AD Dispositivo de adaptación (*adaptation device*)

AE-DCF Función de comunicaciones de datos con encapsulación automática (*automatic encapsulating data communication function*)

ARP Protocolo de resolución de direcciones (*address resolution protocol*)

ASON Red óptica con conmutación automática (*automatic switched optical network*)

ASTN Red de transporte con conmutación automática (*automatic switched transport network*)

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

CallC Controlador de llamada (*call controller*)

CC Controlador de conexión (*connection controller*)

CCI Interfaz de controlador de conexión (*connection controller interface*)

CLNP Protocolo de capa de red sin conexión (*connectionless network layer protocol*)

CLNS Servicio de capa de red sin conexión (*connectionless network layer service*)

COMMS OH Tara de comunicaciones generales de gestión (*general management communications overhead*)

DCC Canal de comunicación de datos (*data communication channel*)

DCF Función de comunicación de datos (*data communication function*)

DF No fragmentar (*don't fragment*)

ECC Canal de control integrado (*embedded control channel*)

EMF Función de gestión de equipo (*equipment management function*)

ES Sistema de extremo (*end system*)

ESH Llamada del sistema de extremo (ISO 9542) (*end system hello*)

ES-IS Sistema de extremo a sistema intermedio (*end system-to-intermediate system*)

GCC Canal de comunicación general (*general communication channel*)

GNE Elemento de red de pasarela (*gateway network element*)

GRE Encapsulado de encaminamiento genérico (*generic routing encapsulation*)

HDLC Control de enlace de datos de alto nivel (*high level data link control*)

ICMP Protocolo de mensajes de control Internet (*Internet control message protocol*)

ID Identificador (*identifier*)

IIH Aviso inicial de IS-IS (*IS-IS hello*)

IntISIS Sistema intermedio integrado a sistema intermedio (*integrated intermediate system-to-intermediate system*)

IP Protocolo Internet (*Internet protocol*)

IPCP Protocolo de control de protocolo Internet (*Internet protocol control protocol*)

IPv4 Protocolo Internet versión 4 (*Internet protocol version 4*)

IPv6 Protocolo Internet versión 6 (*Internet protocol version 6*)

IS Sistema intermedio (*intermediate system*)

ISH Saludo del sistema intermedio (ISO 9542) (*intermediate system hello*)

IS-IS Sistema intermedio a sistema intermedio (*intermediate system-to-intermediate system*)

IWF Función de interfuncionamiento (*interworking function*)

LAN Red de área local (*local area network*)

LAPD Procedimiento de acceso al enlace por el canal D (*link-access procedure D-channel*)
LSP Unidad de datos de protocolo de estado del enlace (*link state protocol data unit*)
MAC Control de acceso a medios (*media access control*)
MCF Función de comunicación de mensajes (*message communication function*)
MD Dispositivo de mediación (*mediation device*)
MTU Unidad de transmisión máxima (*maximum transmission unit*)
NE Elemento de red (*network element*)
NEF Función de elemento de red (*network element function*)
NLPID Identificador de su protocolo de capa de red (*network-layer protocol identifier*)
NNI Interfaz red-red (*network-to-network interface*)
NSAP Punto de acceso al servicio de red (*network service access point*)
ODUk Unidad de datos de canal óptico (*optical channel data unit*)
OOS Señal de tara del OTM (*OTM overhead signal*)
OS Sistema de operaciones (*operations system*)
OSC Canal de supervisión óptico (*optical supervisory channel*)
OSF Función de sistema de operaciones (*operations system function*)
OSI Interfaz de sistema abierto (*open system interface*)
OSINLCP Protocolo de control de capa de red OSI (*OSI network layer control protocol*)
OSPF Primer trayecto más corto abierto (*open shortest path first*)
OTM Módulo de transporte óptico (*optical transport module*)
OTN Red óptica de transporte (*optical transport network*)
OTUk Unidad de transporte de canal óptico (*optical channel transport unit*)
PDU Unidad de datos de protocolo (*protocol data unit*)
PPP Protocolo punto a punto (*point-to-point protocol*)
RCD Red de comunicación de datos
RCG Red de comunicación de gestión
RCL Red de comunicación local
RCS Red de comunicación de señalización
RDSI Red digital de servicios integrados
RFC Petición de comentarios (*request for comment*)
RGT Red de gestión de las telecomunicaciones
SDH Jerarquía digital síncrona (*synchronous digital hierarchy*)
SID Identificador de su sistema (*system identifier*)
SNCr Controlador de subred (*subnetwork controller*)
SP Segmentación permitida (*segmentation permitted*)
SPF Primer trayecto más corto (*shortest path first*)
TCP Protocolo de control de transmisión (*transmission control protocol*)

TF	Función de traducción (*translation function*)
TLV	Valor de longitud de tipo (*type length value*)
TNE	Elemento de red de transporte (*transport network element*)
UNI	Interfaz usuario-red (*user to-network interface*)
WAN	Red de área extensa (*wide area network*)
WS	Estación de trabajo (*work station*)
WSF	Función de estación de trabajo (*work station function*)
xMS	Subred de gestión X (*X management subnetwork*)

5 Convenios

En esta Recomendación se utilizan los siguientes convenios.

RCD mixta: Una RCD mixta soporta múltiples protocolos de capa de red (por ejemplo OSI e IPv4). En una RCD mixta, el trayecto entre dos entidades comunicantes (por ejemplo un OS y un NE gestionado) pasa por algunas partes en las que sólo es posible un protocolo de capa de red (por ejemplo OSI) y por otras partes en las que sólo es posible otro protocolo de capa de red diferente (por ejemplo IPv4). Para que la comunicación entre estas entidades sea posible, uno de estos protocolos de capa de red debe encapsularse en el otro, en la frontera entre las partes que soportan protocolos de capa de red diferentes.

RCD exclusivamente OSI: Una RCD exclusivamente OSI sólo soporta el protocolo de capa de red sin conexión (CLNP). Por tanto, el trayecto de extremo a extremo entre dos entidades comunicantes (por ejemplo, un OS y un NE gestionado) soportará el protocolo CLNP, y no será necesaria la encapsulación de un protocolo de capa de red en el otro para soportar estas comunicaciones.

RCD exclusivamente IPv4: Una RCD exclusivamente IPv4 sólo soporta el protocolo de capa de red IPv4. Por tanto, el trayecto de extremo a extremo entre dos entidades comunicantes (por ejemplo, un OS y un NE gestionado) soportará el protocolo IPv4, y no será necesaria la encapsulación de un protocolo de capa de red en el otro para soportar estas comunicaciones.

RCD exclusivamente IPv6: Una RCD exclusivamente IPv6 sólo soporta el protocolo de capa de red IPv6. Por tanto, el trayecto de extremo a extremo entre dos entidades comunicantes (por ejemplo, un OS y un NE gestionado) soportará el protocolo IPv6, y no será necesaria la encapsulación de un protocolo de capa de red en el otro para soportar estas comunicaciones.

6 Características de la RCD

Hay varias aplicaciones (por ejemplo, RGT, ASTN, etc.) que necesitan una red de comunicaciones por paquetes para transportar información entre diversos componentes. Por ejemplo, la RGT necesita una red de comunicaciones conocida como red de comunicación de gestión (RCG) para transportar mensajes de gestión entre los componentes de la RGT (por ejemplo el componente NEF y el componente OSF). La red ASTN necesita una red de comunicaciones conocida como red de comunicaciones de señalización (RCS) para transportar mensajes de señalización entre componentes ASTN (por ejemplo componentes CC). En esta Recomendación se definen las funciones de comunicación de datos que pueden utilizarse para el soporte de redes de comunicaciones de una o varias aplicaciones.

En la figura 6-1 se representan ejemplos de aplicaciones que puede soportar una RCD. Cada aplicación puede estar soportada en una RCD distinta o en la misma RCD, lo que dependerá del diseño de la red.

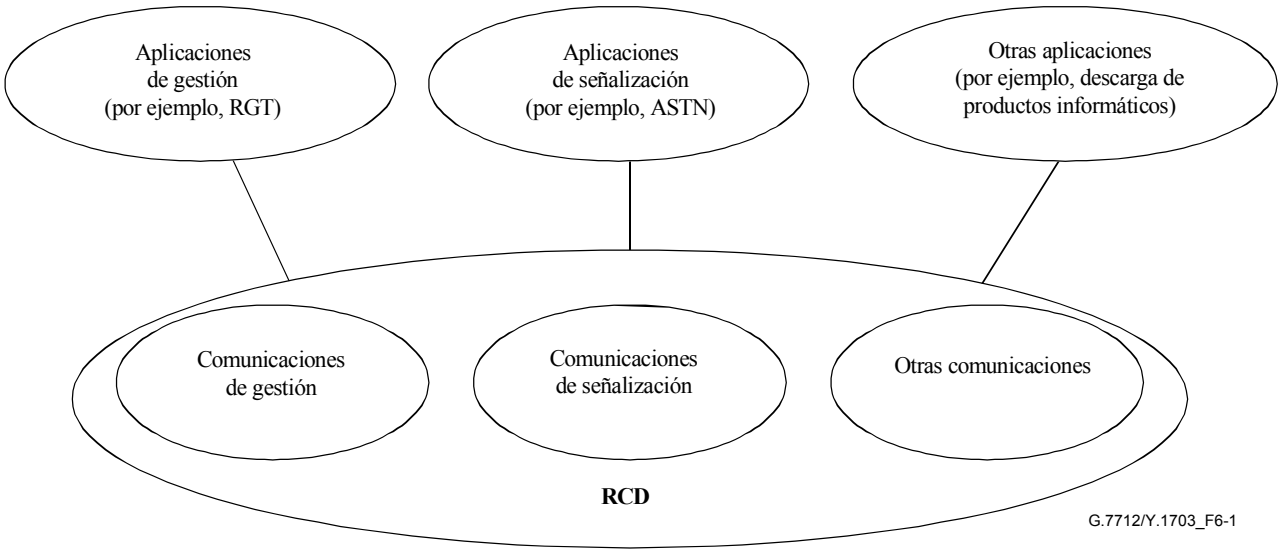


Figura 6-1/G.7712/Y.1703 – Ejemplos de aplicaciones soportadas por una RCD

La RCD conceptual es un conjunto de recursos para soportar la transferencia de información entre componentes distribuidos. Como se ha expresado anteriormente, la RCD puede soportar distintos tipos de comunicaciones distribuidas, por ejemplo comunicaciones distribuidas de gestión relacionadas con la RGT, y comunicaciones distribuidas de señalización relacionadas con la ASTN. En una RCD que soporte comunicaciones distribuidas de gestión, los componentes distribuidos son componentes de la RGT (NE, AD, OS, MD y WS que incorporan funciones RGT, tales como OSF, TF, NEF, WSF). En las Recomendaciones UIT-T M.3010 y M.3013 se especifican otros aspectos de las funciones RGT. En una RCD que soporte comunicaciones distribuidas de señalización, los componentes distribuidos son componentes ASTN (elementos de red que incorporan funciones SNCr de ASTN). Las Recomendaciones UIT-T G.807/Y.1302 y G.8080/Y.1304 contienen especificaciones adicionales de las funciones de la ASTN.

Hay varias tecnologías de telecomunicaciones que pueden soportar las funciones RCD, por ejemplo la conmutación de circuitos, la conmutación de paquetes, las LAN, el ATM, la SDH y la OTN. Es importante considerar en la RCD los aspectos de calidad de servicio, velocidad de transferencia de la información y diversidad de encaminamiento para satisfacer determinados requisitos de funcionamiento de las comunicaciones distribuidas soportadas a lo largo y ancho de la RCD (por ejemplo, las comunicaciones distribuidas de gestión y las comunicaciones distribuidas de señalización).

El objetivo de una especificación de interfaz es garantizar la validez del intercambio de datos entre los dispositivos interconectados a través de la RCD para realizar una determinada función (por ejemplo, la función de RGT o la función de ASTN). Una interfaz debe funcionar con independencia del tipo de dispositivo y del proveedor. Para ello es necesaria la compatibilidad de los protocolos de comunicación y de las representaciones de datos de los mensajes, y también la compatibilidad de las definiciones de los mensajes genéricos para las funciones de gestión de la RGT y las funciones de control de la ASTN.

La RCD es la encargada de proporcionar una comunicación compatible en la capa de red (capa 3), en la capa de enlace de datos (capa 2) y en la capa física (capa 1).

En cuanto a las interfaces, es importante considerar la compatibilidad con los dispositivos de transporte de datos más eficientes disponibles actualmente en cada elemento de red (por ejemplo, circuitos arrendados, conexiones con conmutación de circuitos, conexiones con conmutación de paquetes, sistema de señalización N.º 7, canales de comunicación integrados de la SDH, OTN y canales D y B de la red de acceso RDSI).

En esta Recomendación se especifican las tres capas inferiores para comunicación de datos y, por tanto, todo interfuncionamiento entre protocolos dentro de las tres capas inferiores. Este interfuncionamiento lo proporciona la función de comunicación de datos (DCF). En la figura 6-2 se representan ejemplos de interfuncionamiento. Obsérvese que este interfuncionamiento no termina los protocolos de la capa 3. En uno de los ejemplos se considera el interfuncionamiento entre diferentes capas físicas a través de un protocolo común de la capa 2 (por ejemplo, la transferencia de tramas MAC de una interfaz LAN a un canal ECC por medio de un puente). En otro ejemplo se representa el interfuncionamiento entre diferentes protocolos de la capa de enlace de datos a través de un protocolo común de la capa 3 (por ejemplo, el encaminamiento de paquetes IP de una interfaz LAN a un canal ECC). En el tercer ejemplo de la figura 6-2 se representa el interfuncionamiento entre diferentes protocolos de capa de red a través de una función de tunelización de la capa 3 (en este ejemplo, la interfaz OSI es encapsulada/tunelizada a través de IP, aunque también es posible encapsular/tunelizar IP a través de OSI).

El tipo de información transportada entre componentes distribuidos depende del tipo de interfaces soportadas entre los componentes. Una RCD que soporte comunicaciones distribuidas de gestión relacionadas con la RGT necesitará soportar el transporte de la información correspondiente a las interfaces RGT definidas en la Rec. UIT-T M.3010. Una RCD que soporte comunicaciones distribuidas de señalización relacionadas con la ASTN necesitará soportar el transporte de la información correspondiente a las interfaces ASTN definidas en la Rec. UIT-T G.807/Y.1302.

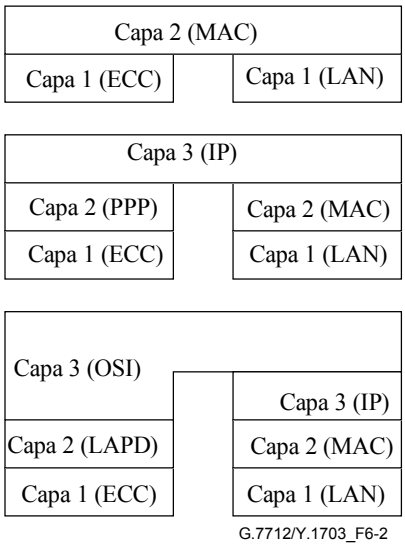


Figura 6-2/G.7712/Y.1703 – Ejemplos de interfuncionamiento de la RCD

6.1 Aplicación RGT

La RGT necesita una red de comunicaciones conocida como red de comunicación de gestión (RCG) para transportar mensajes de gestión entre componentes de la RGT (por ejemplo, el componente NEF y el componente OSF). En la figura 6-3 se representa un ejemplo de relación entre la RCG y la RGT. Las interfaces representadas en la figura 6-3 entre los diversos elementos (por ejemplo, OS, WS, NE) y la RCG, son interfaces lógicas que pueden ser soportadas a través de una sola interfaz RCG física o de varias interfaces RCG.

En la figura 6-4 se representa un ejemplo de implementación física de una RCG que soporta comunicaciones distribuidas de gestión. Según las opciones de implementación de la RCG, los elementos físicos pueden soportar cualquier combinación de interfaces ECC, interfaces LAN e interfaces WAN. En la figura 6-4 también se representan los tipos de bloques funcionales del plano de gestión que pueden soportarse en diversos elementos físicos. Las Recomendaciones UIT-T M.3010 y M.3013 contienen especificaciones detalladas relativas a estos bloques funcionales

de gestión. Cada elemento físico tiene una función de comunicación de datos (DCF) que proporciona funciones de comunicación de datos.

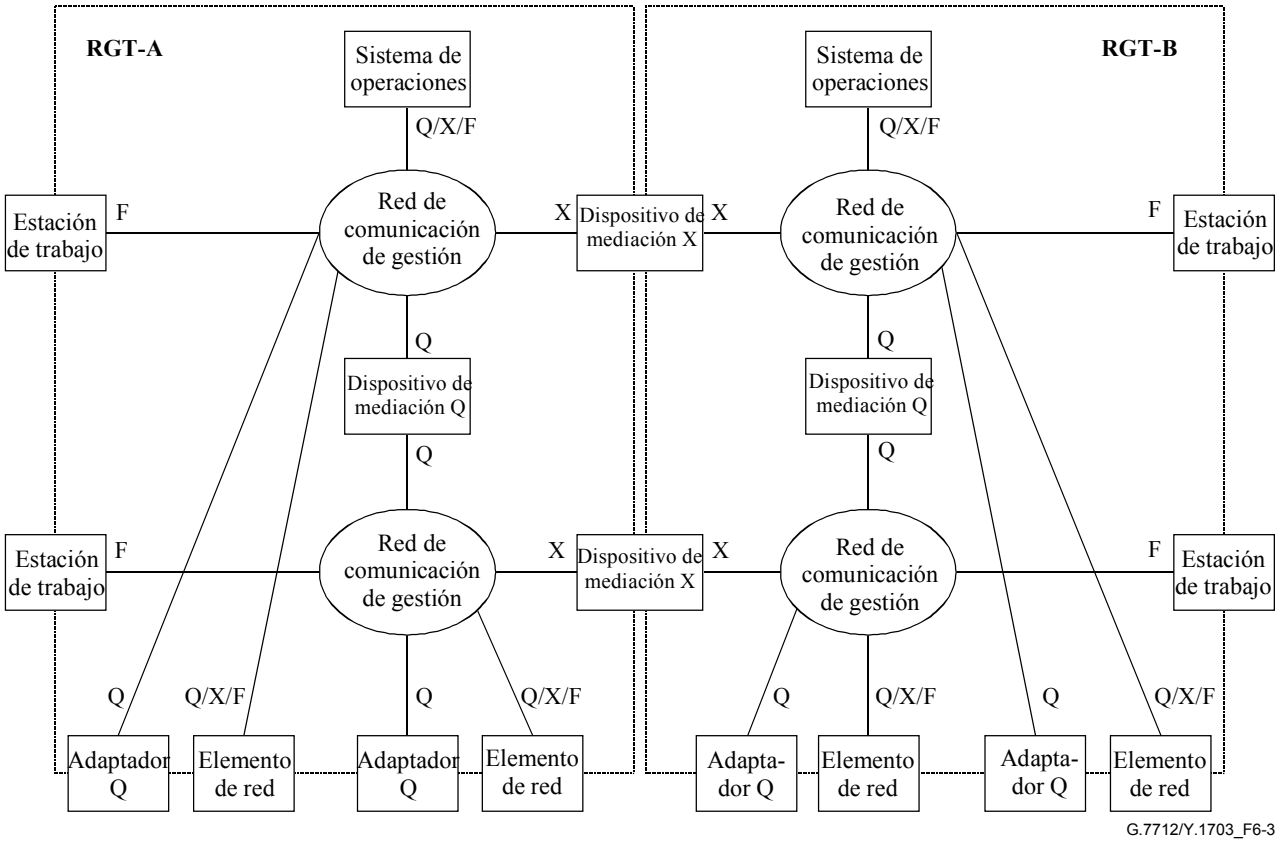


Figura 6-3/G.7712/Y.1703 – Ejemplo de relación entre las interfaces de la RGT y la RCG

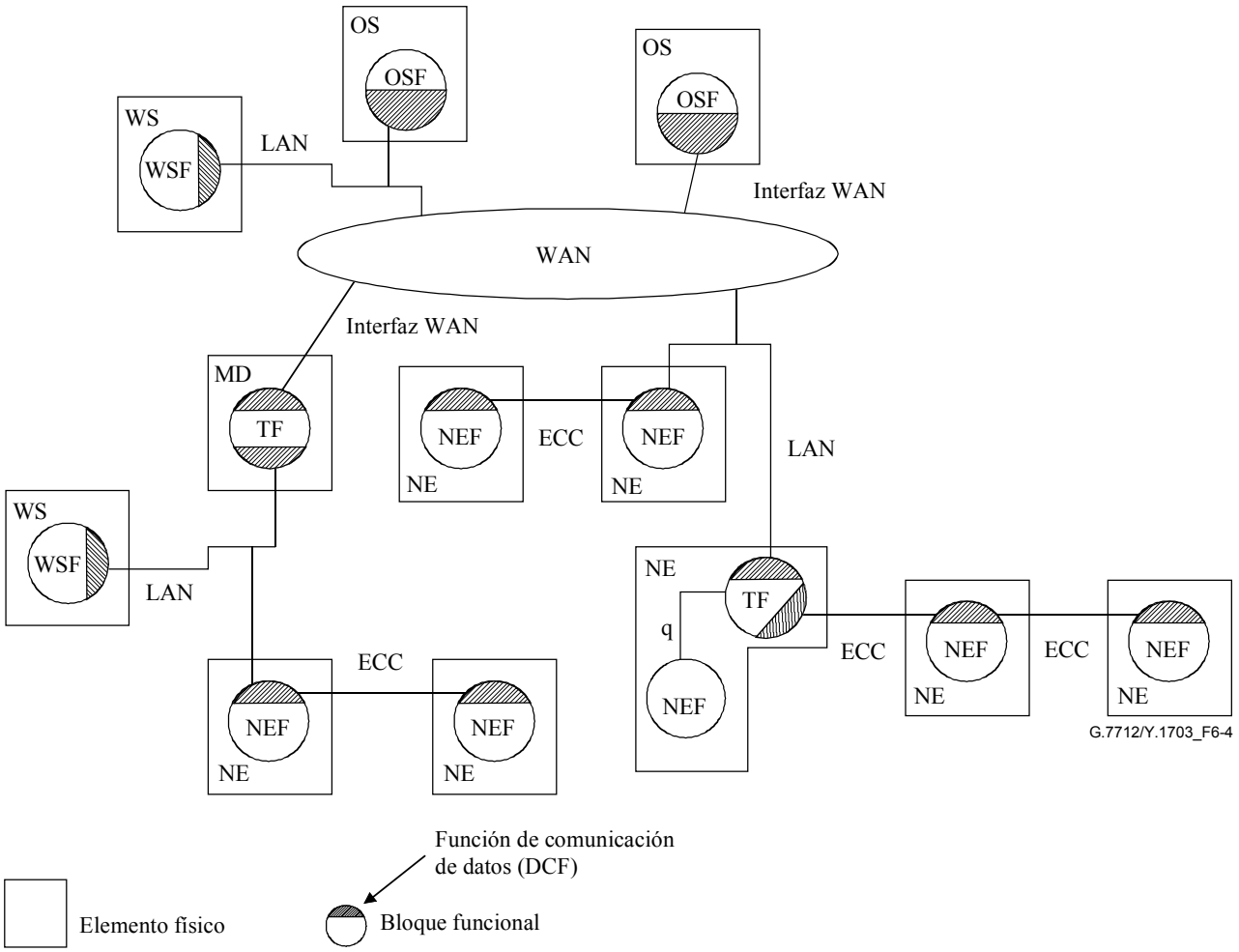


Figura 6-4/G.7712/Y.1703 – Ejemplo de implementación física de una RCG que soporta RGT

6.1.1 Arquitectura de la subred de gestión X

En la figura 6-5, deben señalarse algunos puntos relacionados con la arquitectura de la red de gestión X (xMS):

– *Varios NE en un solo emplazamiento*:

  En un mismo emplazamiento puede haber varios elementos de red (NE) SDH u OTN direccionables. Por ejemplo, los NE_E y NE_G de la figura 6-5 podrían estar situados en un único emplazamiento de equipos.

– *Elementos de red SDH/OTN y sus funciones de comunicación*:

  La función de comunicación de mensajes de un elemento de red SDH u OTN termina (en el sentido de las capas de protocolo inferiores), encamina o procesa de otra forma mensajes que se encuentren en el ECC o se transmitan a través de una interfaz externa.

  i) Es necesario que todos los elementos de red terminen el ECC. Esto significa que cada NE podrá realizar las funciones de un sistema de extremo OSI o de un anfitrión IP.

  ii) Es posible que los NE también tengan que encaminar mensajes ECC entre puertos, atendiendo a la información de control de encaminamiento retenida en el NE. Esto significa que es posible que un NE deba realizar también las funciones de un sistema intermedio OSI o de un encaminador IP.

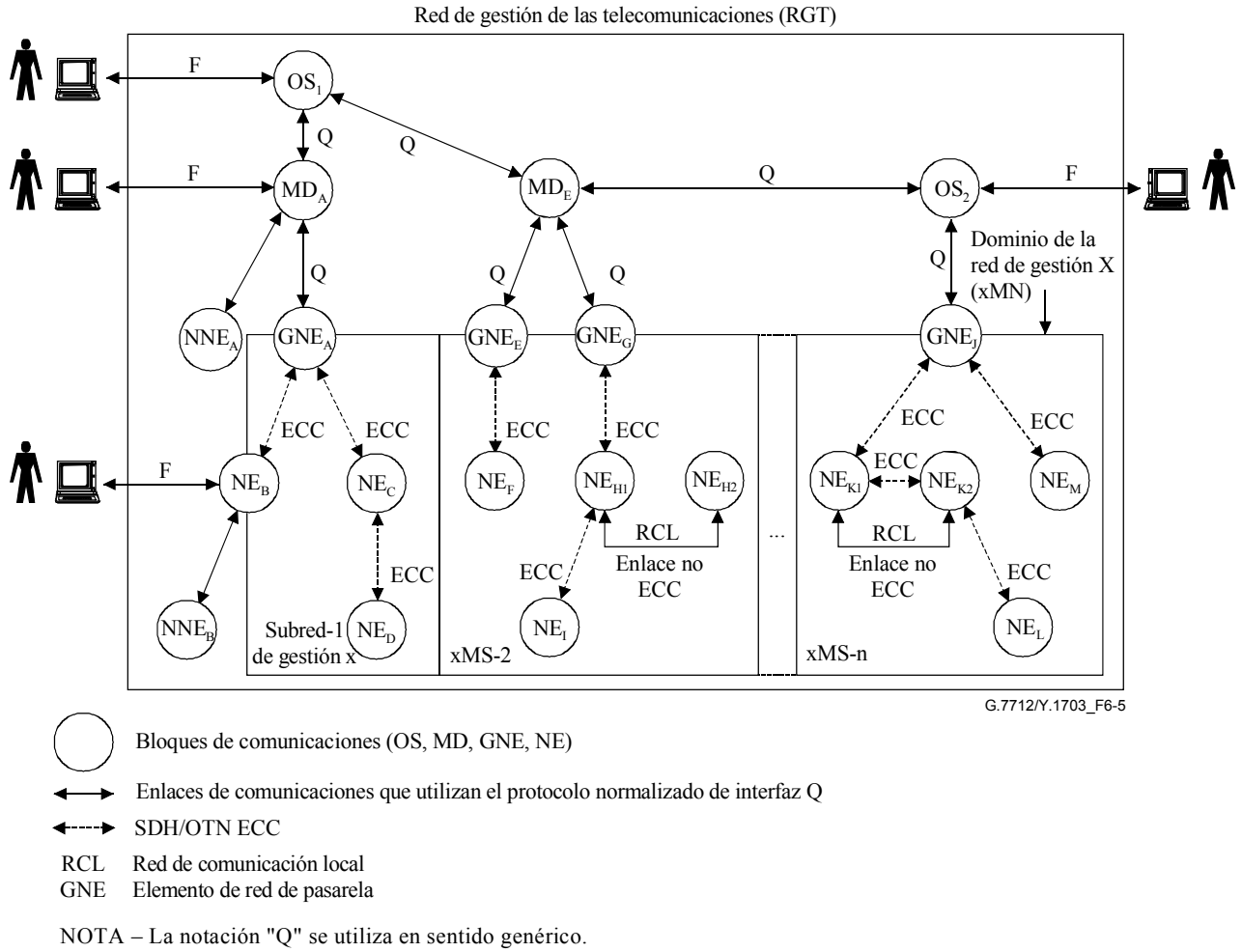
– *Comunicaciones entre emplazamientos SDH/OTN*:

  El enlace de comunicaciones entre emplazamientos o entre oficinas, entre elementos de red SDH/OTN se puede formar a partir de los ECC SDH/OTN.

– *Comunicaciones intraemplazamiento SDH/OTN*:

En un determinado emplazamiento, los elementos de red SDH/OTN pueden comunicarse a través de un ECC intraemplazamiento o a través de una red de comunicaciones local (RCL). En la figura 6-5 se representan los dos casos de esta interfaz.

NOTA – Como alternativa a la utilización de un ECC, se ha propuesto una RCL normalizada para las comunicaciones entre elementos de red situados en un mismo lugar. La RCL podría utilizarse como red general para comunicaciones de los emplazamientos, para dar servicio a elementos de red SDH, OTN y a elementos de red que no sean SDH/OTN (NNE).



NOTA – La notación "Q" se utiliza en sentido genérico.

Figura 6-5/G.7712/Y.1703 – Modelo de la red de gestión de las telecomunicaciones, de la red de gestión y de la subred de gestión

6.1.1.1 Topología de la subred de gestión

En la figura 6-6 se representan ejemplos de topologías de red de comunicaciones de gestión (RCG): lineal, en anillo, en malla y en estrella, que utilizan canales de control integrados (ECC) y/o redes de comunicaciones locales (RCL) (por ejemplo LAN Ethernet) como enlaces físicos para interconectar elementos de red. En la figura 6-7 se representa la forma de soportar una subred de gestión en cada topología. Todas las topologías tienen pasarelas dobles (GNE_1 y GNE_2) comunes que permiten el acceso fiable a los NE dentro de la subred de gestión. Otro aspecto común a todos los ejemplos de topologías es que cada una de ellas permite varios trayectos distintos entre cualquiera de los NE de la subred de gestión y el sistema de operaciones (OS).

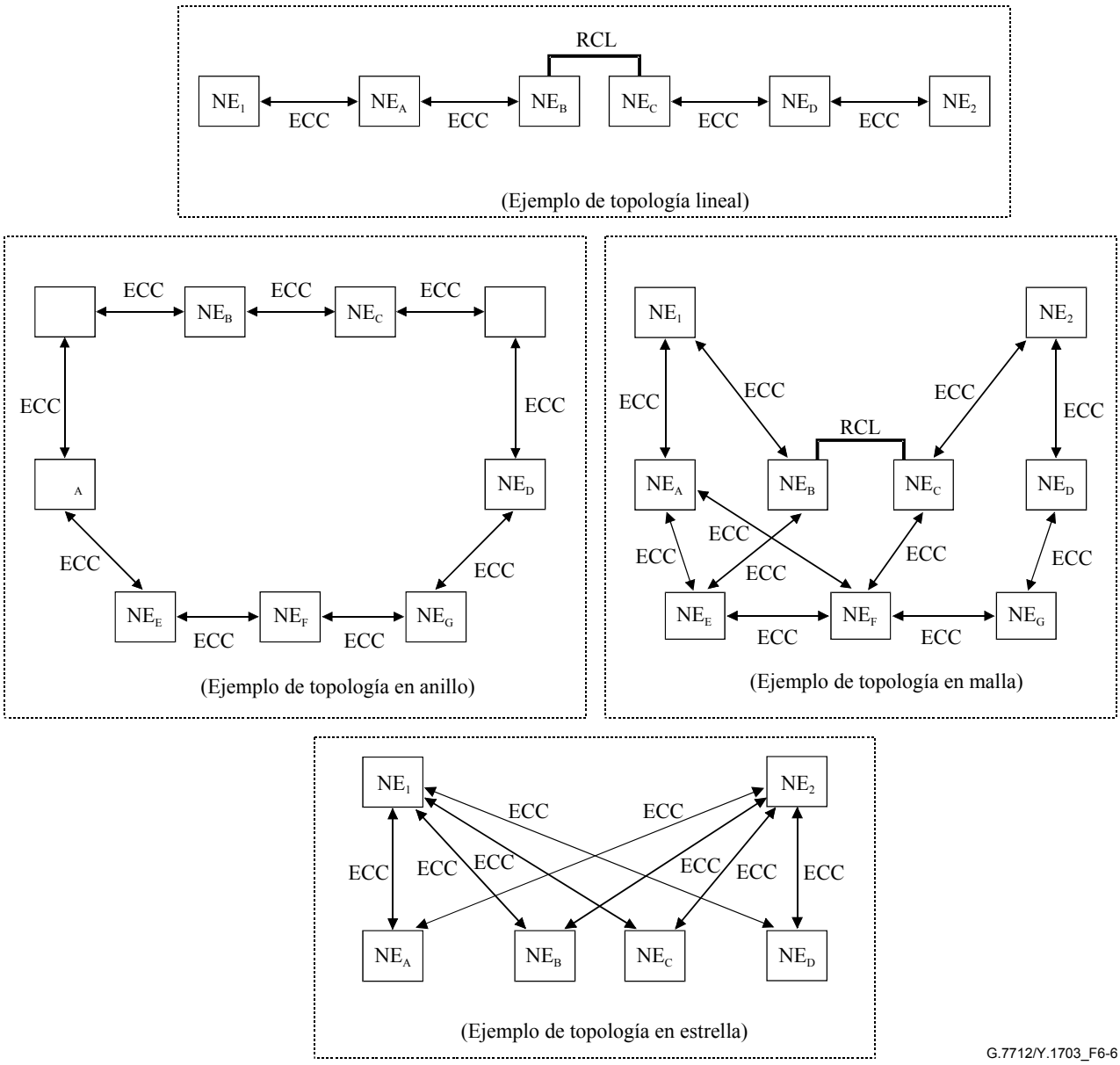


Figura 6-6/G.7712/Y.1703 – Ejemplo de topologías

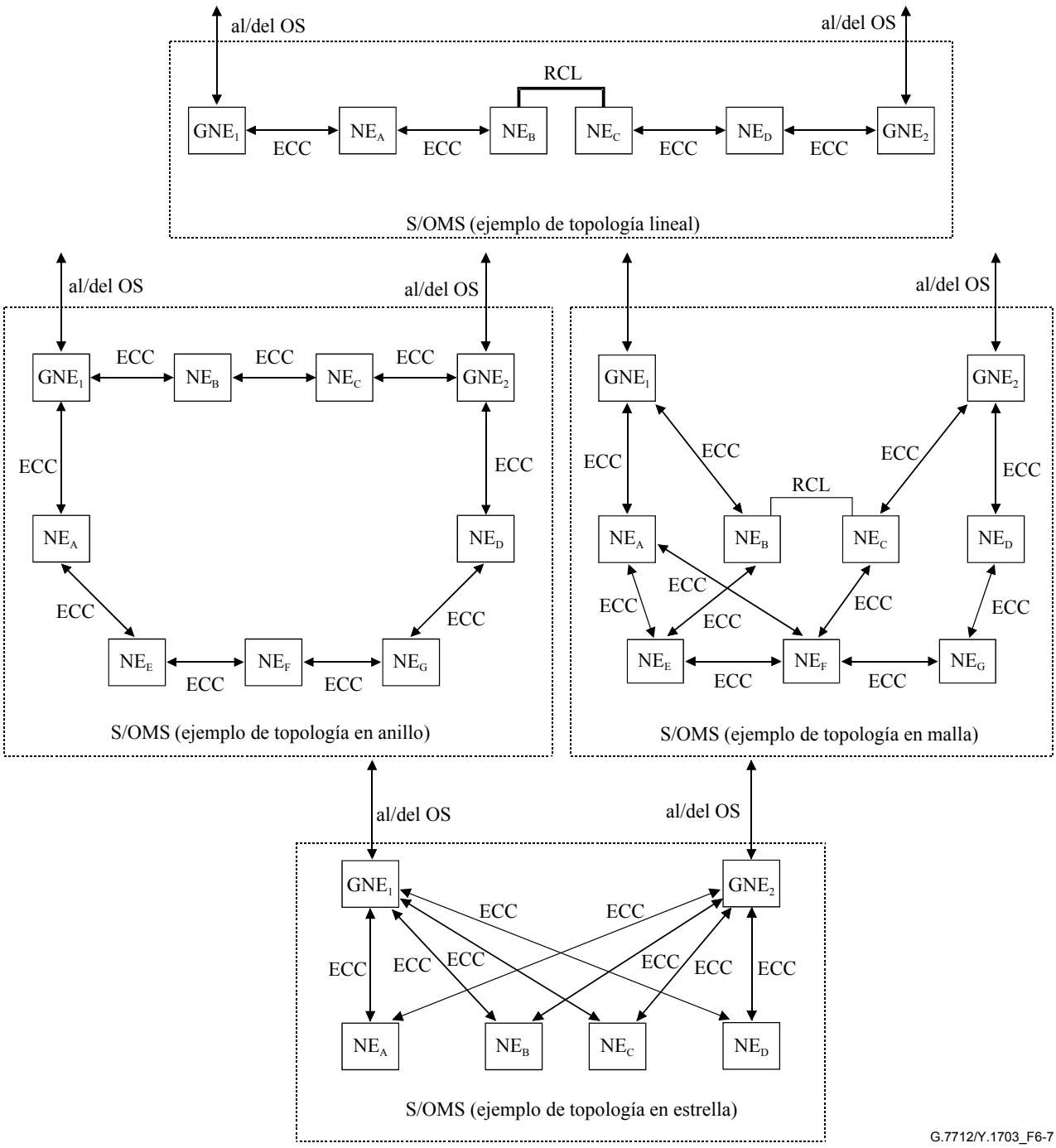


Figura 6-7/G.7712/Y.1703 – Soporte de una subred de gestión en diversas topologías

6.1.2 Fiabilidad de la RCG

Una RCG debe diseñarse de tal manera que un solo fallo no pueda impedir la transferencia de mensajes de gestión críticos.

En el diseño de la RCG también debe garantizarse que una congestión de la RCG no bloqueará ni retardará excesivamente los mensajes de gestión de red destinados a corregir un fallo o un fallo.

Los OS y NE que proporcionan una función de emergencia podrían necesitar un sistema redundante de canales de acceso a la RCG duplicados o alternativos.

6.1.3 Seguridad de la RCG

Para los requisitos de seguridad de la RCG, véase la Rec. UIT-T M.3016.

6.1.4 Funciones de comunicación de datos de la RCG

La función de comunicación de datos (DCF) en las entidades de la RGT debe soportar la funcionalidad de sistema de extremo (ES) (si se trata de OSI) o de anfitrión (si se trata de IP).

- Cuando la DCF en las entidades de la RGT soporte interfaces ECC, deberán soportarse las siguientes funciones:
  - Función de acceso a ECC (como se especifica en 7.1.1).
  - Función de terminación de enlace de datos del ECC (como se especifica en 7.1.2).
  - Función de encapsulación "PDU de capa de red en capa de enlace de datos del ECC" (como se especifica en 7.1.3).
- Cuando la DCF en las entidades de la RGT soporte interfaces LAN Ethernet, deberán soportarse las siguientes funciones:
  - Función de terminación de capa física LAN Ethernet (como se especifica en 7.1.4).
  - Función de encapsulación "PDU de capa de red en trama Ethernet" (como se especifica en 7.1.5).

La DCF en las entidades de la RGT puede funcionar como un sistema intermedio (IS) (si se trata de OSI) o como un encaminador (si se trata de IP). La DCF en las entidades de la RGT que funciona como IS/encaminador podrá efectuar encaminamiento dentro de su área de nivel 1 y por tanto deberá proporcionar la funcionalidad de un IS/encaminador de nivel 1. De otra parte, la DCF de una entidad de la RGT se puede proporcionar como un IS/encaminador de nivel 2, lo que ofrece la capacidad de encaminamiento de un área a otra. No es necesario ofrecer la funcionalidad de IS/encaminador de nivel 2 en la DCF de todas las entidades de la RGT. La DCF de un NE de pasarela es un ejemplo de DCF con funcionalidad de IS/encaminador de nivel 2.

- Cuando la DCF en las entidades de la RGT funcione como un IS/encaminador, deberán soportarse las siguientes funciones:
  - Función de reenvío de PDU de capa de red (como se especifica en 7.1.6).
  - Función de encaminamiento de capa de red (como se especifica en 7.1.10).

La DCF de una entidad RGT que soporte IP puede conectarse directamente a una DCF de una entidad RGT vecina que sólo soporte OSI.

- Cuando la DCF de una entidad RGT que soporte IP esté conectada directamente a la DCF de una entidad RGT vecina que sólo soporte OSI, la DCF que soporta IP deberá soportar la siguiente función:
  - Función de interfuncionamiento de PDU de capa de red (como se especifica en 7.1.7).

Es posible que la DCF de una entidad RGT tenga que reenviar una PDU de capa de red a través de una red que no soporte el mismo tipo de capa de red.

- Cuando la DCF de una entidad RGT deba reenviar una PDU de capa de red a través de una red que no soporte el mismo tipo de capa de red, deberán soportarse las siguientes funciones:
  - Función de encapsulación de PDU de capa de red (como se especifica en 7.1.8).
  - Función de tunelización de PDU de capa de red (como se especifica en 7.1.9).

La DCF de una entidad RGT que soporte IP mediante encaminamiento OSPF podrá conectarse directamente a una DCF de una entidad RGT vecina que soporte IP mediante el empleo de IntISIS.

- Cuando la DCF de una entidad RGT que soporte IP con encaminamiento OSPF esté conectada directamente a una DCF de una entidad RGT vecina, que soporte IP mediante el empleo de IntISIS, la DCF que soporta OSPF deberá soportar la siguiente función:
  - Función de interfuncionamiento de encaminamiento IP (como se especifica en 7.1.11).

6.2 Aplicación de la red de transporte conmutada automáticamente (ASTN)

La ASTN necesita una red de comunicaciones conocida como red de comunicaciones de señalización (RCS) para transportar mensajes de señalización entre componentes de la ASTN (por ejemplo, componentes CC).

En la figura 6-8 se representa un ejemplo de relación entre la RCS y la ASTN. Las interfaces entre los distintos elementos de red y la RCS representados en la figura 6-8 son interfaces lógicas y pueden ser soportadas a través de una sola interfaz física RCS, o de múltiples interfaces RCS.

En la figura 6-9 se representa un ejemplo de implementación física de una RCS que soporta comunicaciones distribuidas de señalización. Según las opciones de implementación de la RCS, los elementos físicos pueden soportar cualquier combinación de interfaces ECC, interfaces LAN o interfaces WAN. En la figura 6-9 también se representan los tipos de bloques funcionales del plano de control que pueden soportarse en diversos elementos físicos. Las Recomendaciones UIT-T G.807/Y.1302 y G.8080/Y.1304 describen en detalle estos bloques funcionales de control. Todos los elementos físicos tienen una función de comunicaciones de datos (DCF) que proporciona la funcionalidad de comunicación de datos.

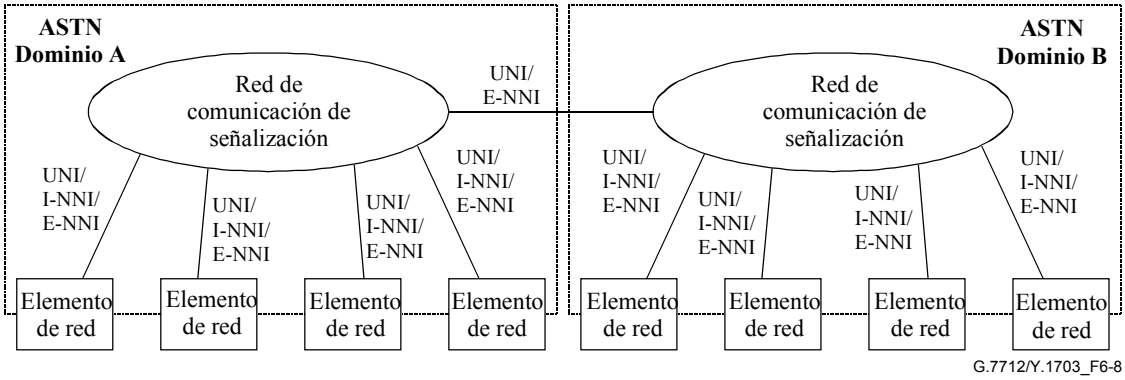


Figura 6-8/G.7712/Y.1703 – Ejemplo de relaciones de las interfaces de la ASTN con la RCS

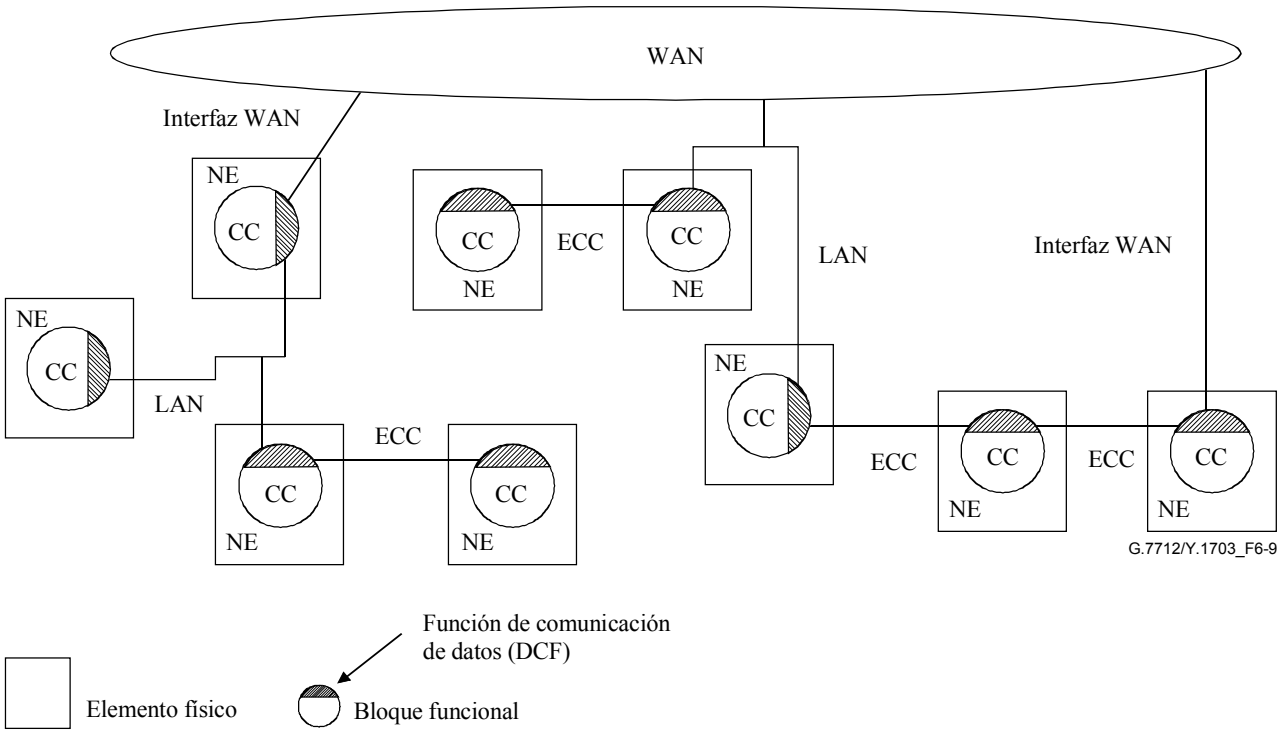


Figura 6-9/G.7712/Y.1703 – Ejemplo de implementación física de una RCS para ASTN

6.2.1 Topología de la RCS

En la figura 6-10 se representan ejemplos de topologías: lineal, en anillo, de malla y en estrella, que utilizan ECC y/o redes de comunicaciones locales (RCL) (por ejemplo, LAN Ethernet) como enlaces físicos para interconectar los elementos de red. En la figura 6-11 se representan soluciones para el soporte de la red de señalización ASTN en las distintas topologías. En todas las topologías existen distintos trayectos alternativos entre las entidades comunicantes (es decir, los elementos de red que soportan la ASTN). Obsérvese que para el soporte de los distintos trayectos alternativos entre los NE de ASTN comunicantes en una topología lineal podría preverse un enlace WAN externo entre los elementos de red ASTN periféricos.

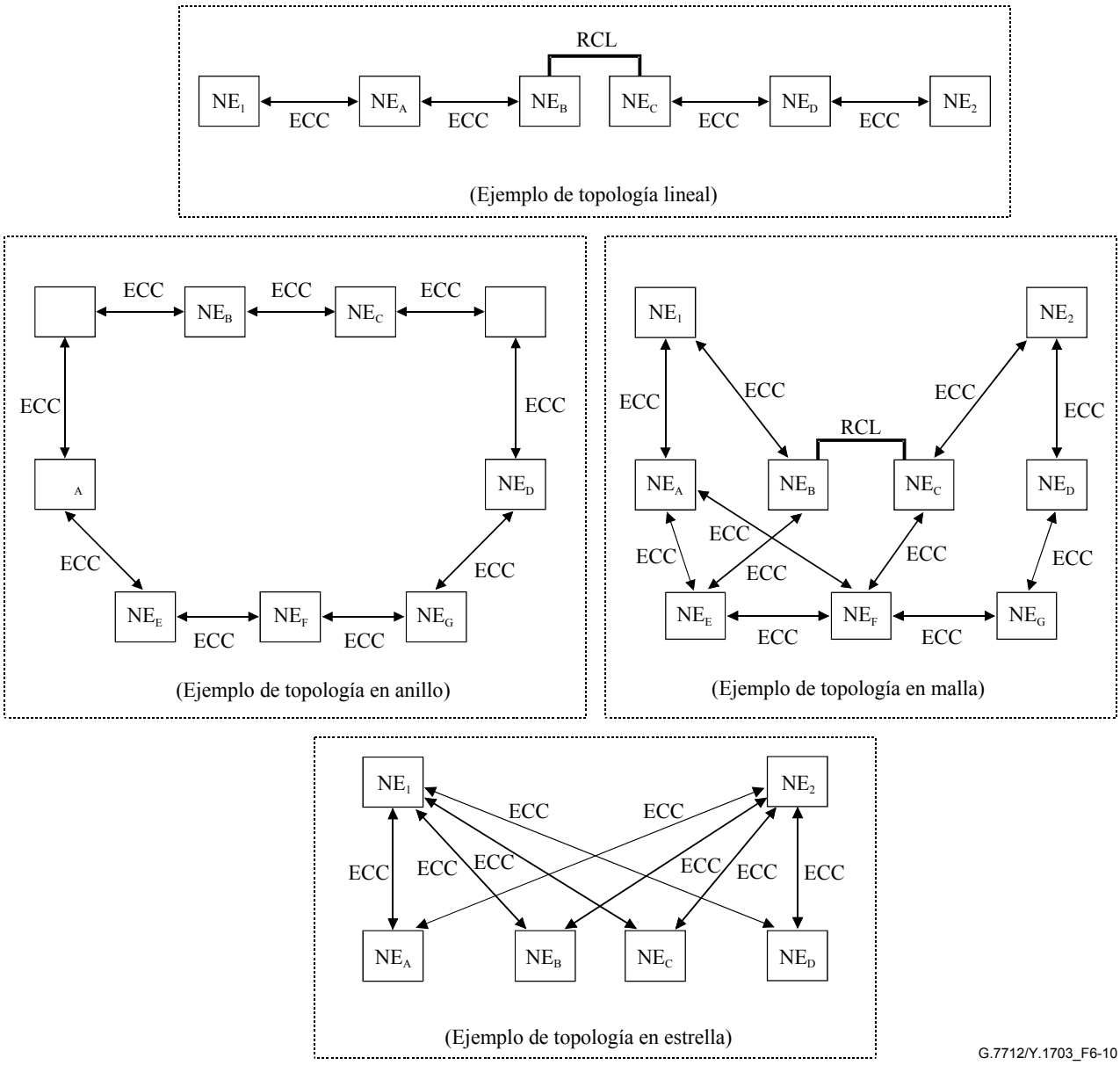


Figura 6-10/G.7712/Y.1703 – Ejemplos de topologías

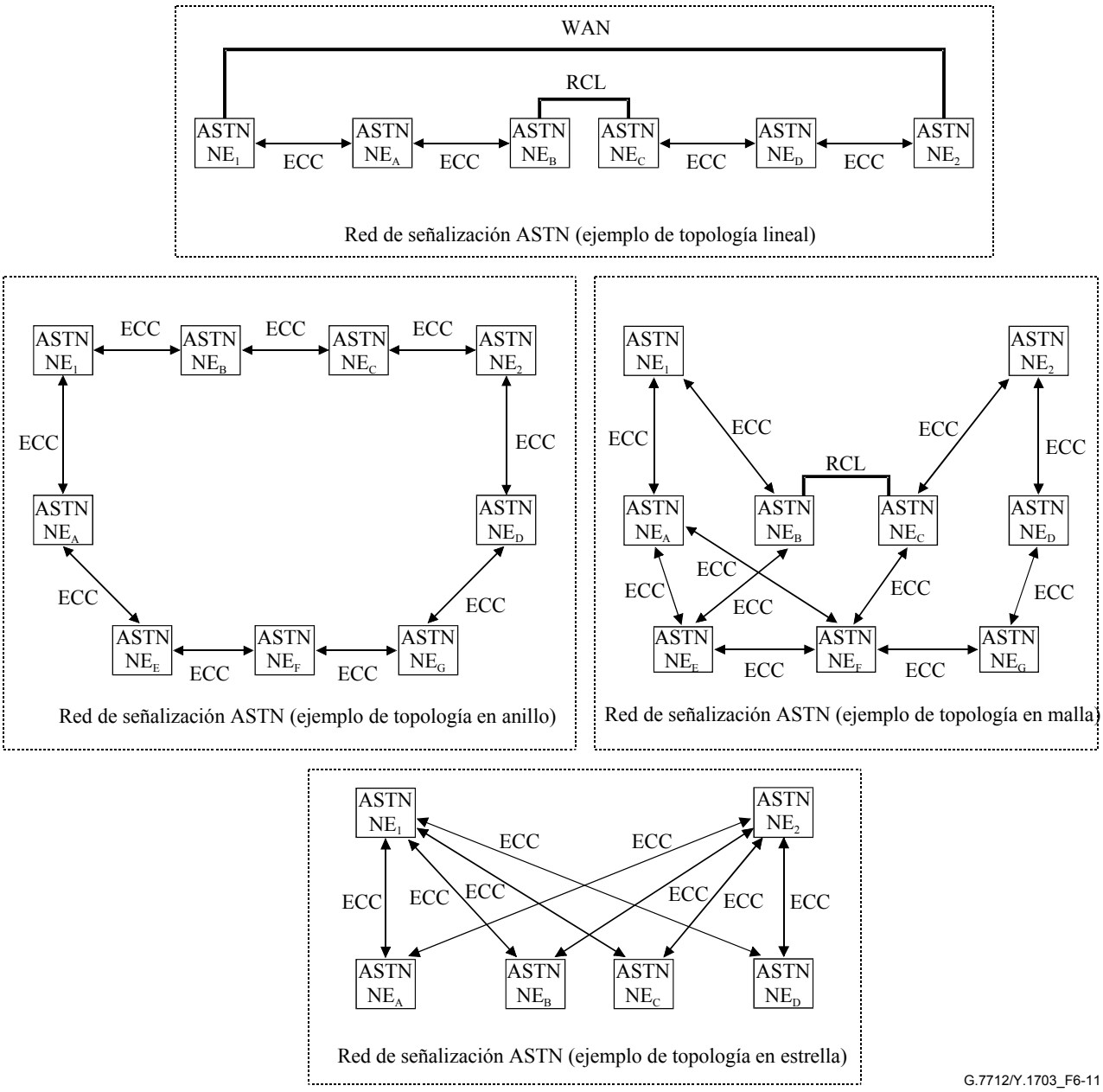


Figura 6-11/G.7712/Y.1703 – Soporte de una red de señalización ASTN en diversas topologías

En la figura 6-12 se representa una posible organización de la red de señalización ASTN en tres porciones diferentes: la porción cliente-red, la porción intradominio administrativo y la porción interdominios administrativos. Es un ejemplo de topología en malla en la que se utilizan ECC, redes de comunicaciones locales (por ejemplo, LAN Ethernet), y líneas arrendadas (por ejemplo, DS1/E1, VC-3/4) como los enlaces físicos que interconectan los elementos de red ASTN. La topología de la porción intradominio administrativo permite que la señalización se transmita por diversos trayectos alternativos entre dos elementos de red ASTN comunicantes. La topología de la porción interdominios administrativos depende de los acuerdos concluidos entre los dominios administrativos A y B. En este ejemplo hay dos puntos de acceso entre los dominios administrativos. La topología de la porción cliente-red depende de los acuerdos concluidos entre el cliente y el proveedor del servicio. En este ejemplo hay un solo punto de acceso entre el cliente y la red.

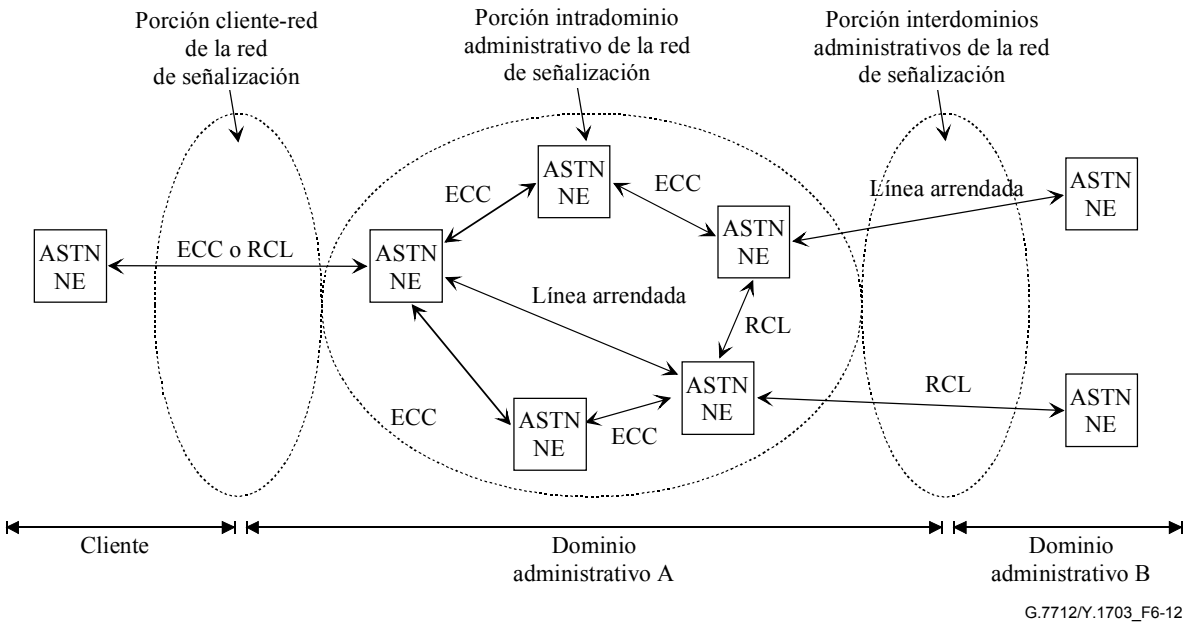


Figura 6-12/G.7712/Y.1703 – Ejemplo de red de comunicación de señalización (RCS)

6.2.2 Fiabilidad de la RCS

En la figura 6-13 se representan los mensajes de control ASTN transportados por una RCS. Se muestran las siguientes interfaces lógicas:

UNI Interfaz usuario-red (*user-to-network interface*).

NNI Interfaz red-red (*network-to-network interface*).

CCI Interfaz del controlador de conexión (*connection controller interface*).

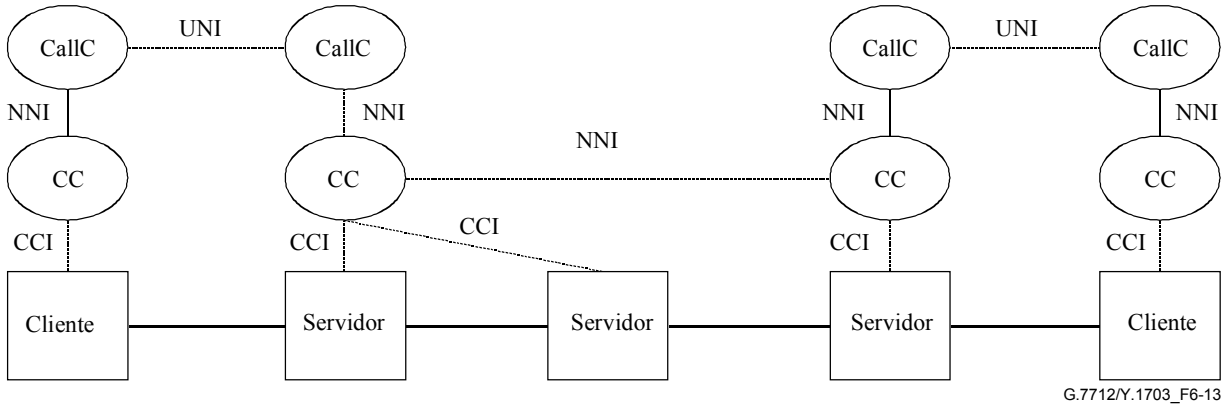


Figura 6-13/G.7712/Y.1703 – Interfaces ASTN soportadas en una RCS

En este ejemplo, las interfaces lógicas UNI, NNI y CCI pertenecen a la red RCS. La RCS puede estar formada por diversas subredes; los enlaces lógicos de algunas de estas subredes pueden, facultativamente, compartir rutas físicas comunes con la red de transporte.

Es posible que la RCS sufra un fallo que no haya sido causado por la red de transporte (fallo independiente de la red de transporte). En las figuras 6-14 y 6-15 se representa este caso. En este ejemplo de mensajes ASTN transportados por la RCS, un fallo independiente de la RCS afectaría a las nuevas peticiones de establecimiento de conexión y de supresión de conexión.

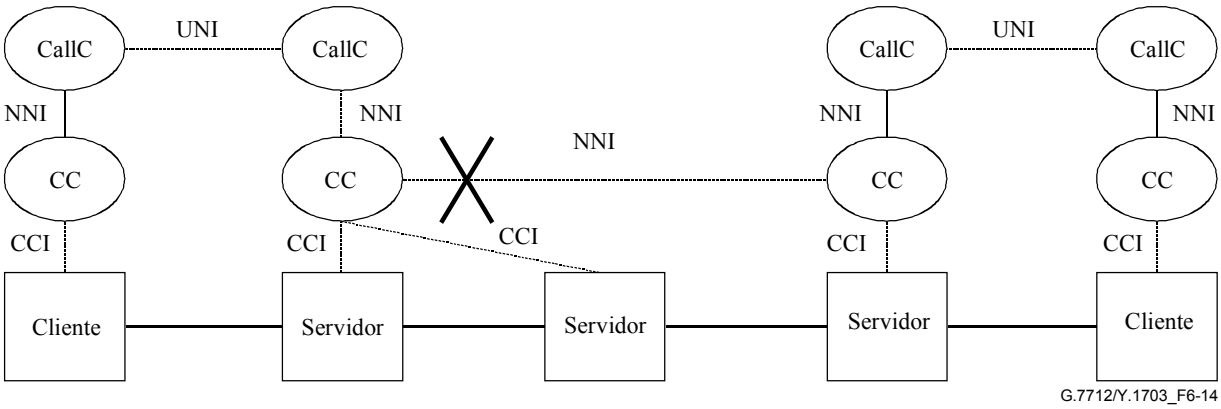


Figura 6-14/G.7712/Y.1703 – Fallo de la RCS que influye en la interfaz de señalización

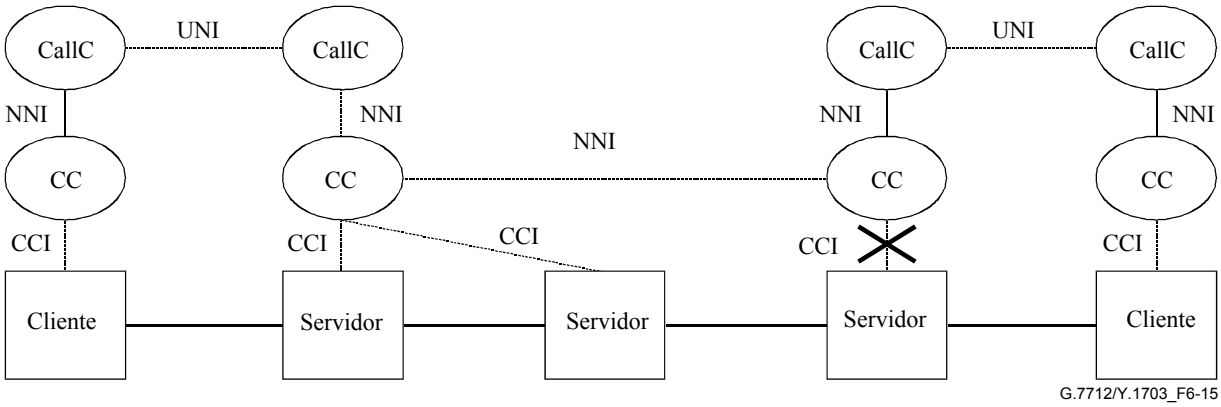


Figura 6-15/G.7712/Y.1703 – Fallo de la RCS que influye en la interfaz CCI

Como se ha indicado anteriormente, en la figura 6-15, algunos enlaces lógicos de la RCS pueden compartir rutas físicas con la red de transporte. En este caso, podría haber un fallo de la RCS que no fuera independiente de la red de transporte (es decir, el fallo interrumpe tanto el tráfico de la RCS como el tráfico de transporte), que es la situación representada en la figura 6-16. En este ejemplo de mensajes ASTN transportados por la RCS, este fallo podría afectar al restablecimiento si la ASTN se utiliza para restablecer conexiones existentes. Por eso, es indispensable que cuando la RCS transporta mensajes de restablecimiento proporcione la necesaria resiliencia.

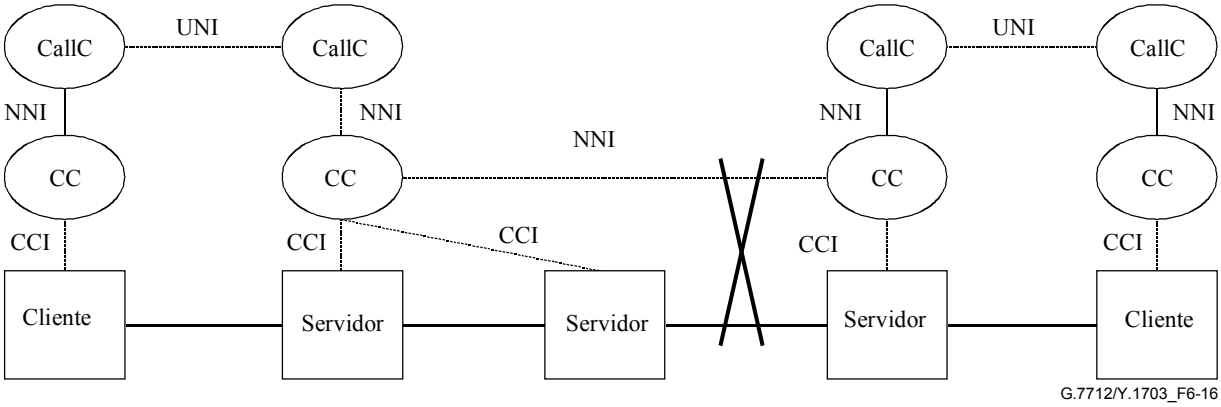


Figura 6-16/G.7712/Y.1703 – Fallo de la RCS que afecta a las interfaces de señalización y de datos

Si la aplicación ASTN sólo se utiliza para establecer y suprimir conexiones, puede bastar con una RCS sin conexión. Ahora bien, si la aplicación ASTN también se utiliza para restablecerlas, podría necesitarse una RCS con conexión. Una RCS con conexión requeriría la especificación de funciones adicionales para soportar servicios de red con conexión.

Los requisitos de fiabilidad de la RCS son los siguientes:

La RCS deberá soportar varios niveles de restablecimiento, según los requisitos de fiabilidad de los componentes comunicantes para los que proporcione transporte (es decir, puede soportarse el restablecimiento entre los componentes comunicantes que requieran comunicación muy fiable, aún no exigiendo el soporte del restablecimiento entre todos los componentes comunicantes).

Una manera de conseguir la fiabilidad de la RCS es mediante la protección de paquetes 1+1 en los protocolos con conexión tal como el MPLS descrito en 6.2.4.

La RCS puede transportar mensajes de restablecimiento. En tal caso, es indispensable que las velocidades de restablecimiento de la RCS permitan el correcto funcionamiento de las conexiones que son objeto de los mensajes de restablecimiento.

6.2.3 Seguridad de la RCS

Una RCS que soporta mensajes ASTN puede proporcionar conectividad entre dominios administrativos diferentes. Cuando una RCS proporciona conectividad entre dos dominios administrativos, es necesario tomar medidas para que sólo los mensajes autorizados a pasar entre los dos dominios administrativos puedan cruzar la interfaz, y se impida cruzar la interfaz a otros mensajes no autorizados a pasar entre los dominios administrativos. La RCS debe garantizar que los distintos mensajes autorizados por las partes administrativas a ambos lados de la interfaz son los únicos que pueden cruzar efectivamente la interfaz.

6.2.4 Funciones de comunicaciones de datos en la RCS

La función de comunicaciones de datos (DCF) en las entidades ASTN deberá soportar la funcionalidad de sistema de extremo (ES) (si se trata de OSI) o de anfitrión (si se trata de IP).

- Cuando la DCF de las entidades ASTN soporte interfaces ECC, deberán soportarse las siguientes funciones:
  - Función de acceso al ECC (como se especifica en 7.1.1).
  - Función de terminación de enlace de datos ECC (como se especifica en 7.1.2).
  - Función de encapsulación "PDU de capa de red en capa de enlace de datos ECC" (como se especifica en 7.1.3).
- Cuando la DCF de las entidades ASTN soporte interfaces LAN Ethernet, deberán soportarse las siguientes funciones:
  - Función de terminación de capa física LAN Ethernet (como se especifica en 7.1.4).
  - Función de encapsulación "PDU de capa de red en trama Ethernet" (como se especifica en 7.1.5).

La DCF de las entidades ASTN puede funcionar como un Sistema Intermedio (IS) (si se trata de OSI) o como un encaminador (si se trata de IP). La DCF de las entidades ASTN que funcione como IS/encaminador podrá encaminar dentro de su área de nivel 1, y por tanto proporcionará la funcionalidad de IS/encaminador de nivel 1. Además, la DCF de una entidad ASTN puede proporcionarse como un IS/encaminador de nivel 2, lo que supone la capacidad de encaminar de un área a otra. La funcionalidad de IS/encaminador de nivel 2 no es necesaria en la DCF de todas las entidades ASTN.

- Cuando la DCF de las entidades ASTN funcione como un IS/encaminador, deberán soportarse las siguientes funciones:
  - Función de reenvío de PDU de capa de red (como se especifica en 7.1.6).
  - Función de encaminamiento de capa de red (como se especifica en 7.1.10).

La DCF de una entidad ASTN que soporte IP podrá conectarse directamente a una DCF de una entidad ASTN vecina que sólo soporte OSI.

- Cuando la DCF de una entidad ASTN que soporte IP esté conectada directamente a una DCF de una entidad RGT vecina que sólo soporte OSI, deberá soportarse la siguiente función en la DCF que soporta IP:
  - Función de interfuncionamiento de PDU de capa de red (como se especifica en 7.1.7).

Es posible que la DCF de una entidad ASTN tenga que reenviar una PDU de capa de red a través de una red que no soporte el mismo tipo de capa de red.

- Cuando la DCF de una entidad ASTN tenga que reenviar una PDU de capa de red a través de una red que no soporte el mismo tipo de capa de red, deberán soportarse las siguientes funciones:
  - Función de encapsulación de PDU de capa de red (como se especifica en 7.1.8).
  - Función de tunelización de PDU de capa de red (como se especifica en 7.1.9).

La DCF de una entidad ASTN que soporte IP mediante encaminamiento OSPF podrá conectarse directamente a una DCF de una entidad ASTN vecina que soporte IP mediante IntISIS.

- Cuando la DCF de una entidad ASTN que soporte IP mediante encaminamiento OSPF esté conectada directamente a una DCF de una entidad ASTN vecina que soporte IP mediante IntISIS, la DCF que soporta OSPF deberá soportar la siguiente función:
  - Función de interfuncionamiento de encaminamiento IP (como se especifica en 7.1.11).

La DCF de las entidades ASTN puede funcionar como encaminador periférico de etiquetas (LER, *label edge router)*.

Cuando la DCF de las entidades ASTN funcione como LER, deberán soportarse las siguientes funciones:

- La función de encapsulación "PDU MPLS en capa de enlace de datos ECC" (especificada en 7.1.13), cuando la DCF soporte las interfaces ECC.
- La función de encapsulación "PDU MPLS en trama Ethernet" (especificada en 7.1.14) cuando la DCF soporte las interfaces LAN.
- La función de señalización MPLS LSP (especificada en 7.1.15).
- La función de reenvío MPLS LSP (especificada en 7.1.16).
- La función de cálculo del trayecto MPLS LSP (especificada en 7.1.17).
- La función de encapsulación "PDU de capa de red en MPLS" (especificada en 7.1.18).

La DCF de las entidades ASTN puede operar como un encaminador de conmutación de etiquetas (LSR, *label switch router*).

Cuando la DCF de las entidades ASTN opere como LSR, deberán soportarse las siguientes funciones:

- La función de encapsulación "PDU MPLS en la capa de enlace de datos ECC" (especificada en 7.1.13), cuando la DCF soporte las interfaces ECC.
- La función de encapsulación "PDU MPLS en la trama Ethernet" (especificada en 7.1.14) cuando la DCF soporte las interfaces LAN.
- La función de señalización MPLS LSP (especificada en 7.1.15).

- La función de reenvío MPLS LSP (especificada en 7.1.16).

La DCF de las entidades ASTN puede ofrecer capacidad de protección de paquetes 1+1.

Los requisitos mínimos para proporcionar el servicio de protección de paquetes 1+1 son los siguientes:

- Que no se requiera capacidad adicional en los nodos interiores de la red.
- Que la red soporte el establecimiento de conexiones con diversos encaminamientos.
- *Que el nodo de ingreso*
  - sea capaz de asociar las dos conexiones utilizadas para proporcionar la protección de paquetes de nivel 1+1 entre dos nodos extremos;
  - soporte el transporte de un identificador en el paquete destinado a identificar copias duplicadas de un paquete del nodo de egreso;
  - sea capaz de llevar a cabo la alimentación dual de cada paquete en las dos conexiones acopladas.
- *Que el nodo de egreso*
  - sea capaz de asociar las dos conexiones destinadas a proporcionar la protección de paquetes de nivel 1+1 entre los dos nodos extremos;
  - sea capaz de identificar copias duplicadas de un paquete de alimentación dual por medio del identificador;
  - sea capaz de seleccionar y reenviar una copia de un paquete y sólo una.

El mecanismo para asociar las dos conexiones distintas así como el formato y posición del identificador de secuencia deberán ajustarse a lo descrito en 7.1.19.

6.3 Otras aplicaciones que necesitan redes de comunicación

Además de las aplicaciones RGT y ASTN, otras aplicaciones como las comunicaciones de voz (por ejemplo, el circuito de servicio), descarga de soporte lógico y comunicaciones específicas del operador necesitan una red de comunicaciones para el transporte de información entre componentes.

6.4 Separación de las diferentes aplicaciones

Dependiendo del diseño de la red, de su tamaño, de la capacidad del enlace, de los requisitos de seguridad y de los de calidad de funcionamiento son posibles diversos niveles de separación entre las distintas aplicaciones (por ejemplo, RGT, ASTN). El nivel de separación proporcionado lo deciden los operadores y fabricantes cuando se diseña la red. A continuación se presentan ejemplos de diversos niveles de separación.

Opción A: Se puede diseñar la RCD de forma que la RCG, la RCS y otras aplicaciones (por ejemplo, las comunicaciones específicas del operador) estén soportadas en la misma red de capa 3 (por ejemplo, que compartan la misma red IP).

Opción B: La RCD se puede diseñar de forma que la RCG, la RCS y otras aplicaciones (por ejemplo, las comunicaciones específicas del operador) estén soportadas por distintas redes de capa 3, aunque puedan compartir algunos enlaces físicos.

Opción C: La RCD se puede diseñar de forma que la RCG, la RCS y otras aplicaciones (por ejemplo, las comunicaciones específicas del operador) estén soportadas por distintas redes físicas (es decir, distintas redes de capa 3 que no comparten ningún enlace físico).

7 Arquitectura y requisitos funcionales de la RCD

Los requisitos de la arquitectura de la RCD tratados en esta cláusula son aplicables a dominios exclusivamente IP, dominios exclusivamente OSI y dominios mixtos IP+OSI. Los requisitos de arquitectura de la RCD son independientes de la tecnología. Las Recomendaciones que sean específicas de cada tecnología, como la Rec. UIT-T G.784 para SDH y la Rec. UIT-T G.874 para OTN, especificarán los requisitos aplicables a cada tecnología.

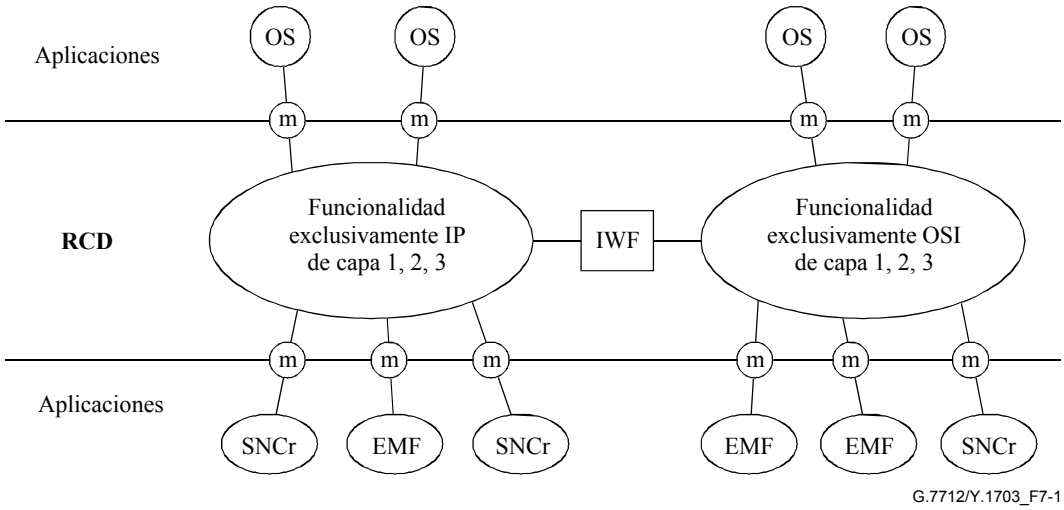
La RCD acepta los protocolos de capa 1, capa 2 y capa 3, y es transparente a los protocolos de capa superior utilizados por las aplicaciones que transporta.

Se puede diseñar una red RCD de manera que soporte únicamente IP. Una RCD que sólo soporta IP puede constar de varias subredes con distintos protocolos de capa física y de enlace de datos, aunque todas las subredes soportarán IP como protocolo de capa de red.

No obstante, como las redes RCD integradas soportan OSI, algunas RCD pueden tener partes que sólo soporten IP, partes que sólo soporten OSI y partes que soporten IP y OSI.

Las partes de la RCD que soportan IP (es decir, tanto las partes que sólo soportan IP como las partes que soportan IP y OSI) pueden tener DCF que soporten exclusivamente IP (es decir, DCF exclusivamente IP de una sola pila) y/o DCF que soporten IP y OSI (por ejemplo, una DCF de pila dual capaz de encaminar paquetes tanto IP como OSI). Las partes de la RCD que sólo soporten OSI tendrán DCF que soporten exclusivamente OSI (es decir, una DCF exclusivamente OSI de una sola pila).

En la figura 7-1 se representa la arquitectura funcional de la RCD. Como se ha indicado anteriormente, la RCD puede estar integrada por partes que sólo soportan IP, partes que sólo soportan OSI y partes que soportan tanto IP como OSI. También se especifica una función de interfuncionamiento (IWF) entre las partes de la RCD que soportan sólo IP, sólo OSI, o tanto IP como OSI, y funciones de correspondencia que hacen corresponder aplicaciones a la capa IP. Para proporcionar este transporte, la RCD soporta la funcionalidad de capa 1 (física), de capa 2 (enlace de datos), y de capa 3 (red). Se especifican los requisitos de arquitectura para las partes de la RCD que soportan sólo IP o sólo OSI, y los requisitos que debe satisfacer el interfuncionamiento entre las partes de la RCD que soportan sólo IP, sólo OSI, o tanto IP como OSI. El óvalo de la figura 7-1 que representa la parte de la RCD exclusivamente IP es una visión abstracta de la RCD y por tanto también se puede aplicar a un solo elemento de red IP interconectado a elementos de red OSI mediante una IWF.



IWF Función de interfuncionamiento
SNCr Controlador de conexión de subred
EMF Función de gestión de equipo
OS Sistema de operaciones
m Correspondencia entre aplicación y RCD

Figura 7-1/G.7712/Y.1703 – Arquitectura funcional de la RCD

7.1 Descripción de las funciones de comunicación de datos

En esta cláusula se especifican diversas funciones de comunicación de datos relacionados con interfaces ECC, interfaces LAN Ethernet y capacidades de capa de red.

7.1.1 Función de acceso a canal de control integrado (ECC)

Una función de acceso proporciona acceso al tren de bits del ECC. Esta función está definida en las Recomendaciones sobre equipos específicos de las distintas tecnologías (por ejemplo Recomendaciones UIT-T G.783 y G.798). Las velocidades binarias y las definiciones de los diversos ECC (por ejemplo, DCC, GCC y COMMS OH en OSC) figuran en las Recomendaciones sobre las distintas tecnologías (por ejemplo Recomendaciones UIT-T G.784 y G.874).

7.1.2 Función de terminación de la capa de enlace de datos ECC

Una función de terminación en la capa de enlace de datos ECC efectúa el procesamiento común de la capa de enlace de datos cualquiera que sea la PDU de capa de red encapsulada en la trama de la capa de enlace de datos. Esta función también se encarga de la correspondencia de la trama de la capa de enlace de datos en el ECC. Esta función se especifica en las Recomendaciones sobre las distintas tecnologías. No obstante, a continuación se proporciona la especificación de la función de terminación de la capa de enlace de datos ECC de la SDH.

7.1.2.1 Función de terminación de la capa de enlace de datos ECC de la SDH

7.1.2.1.1 Correspondencia de la trama de capa de enlace de datos SDH en ECC

La señal entramada según el control de enlace de datos de alto nivel (HDLC) es un tren de bits serie que contiene tramas rellenas, circundadas por una o más secuencias de banderas. En la Rec. UIT-T Q.921 se define el formato de la señal entramada según HDLC para LAPD, y en RFC 1662 para PPP en entramado HDLC. Una trama HDLC está formada por N octetos, como se representa en la figura 7-2. La trama HDLC se transmite de derecha a izquierda y de arriba a abajo. Se inserta un bit 0 después de todas las secuencias de cinco bits 1 consecutivos en el contenido de la trama HDLC (octetos 2 a N-1) para evitar que se simule una secuencia de banderas o de aborto dentro de una trama.

La correspondencia de la señal entramada según HDLC en el canal DCC es síncrona a nivel de bit (y no a nivel de octeto), dado que la trama HDLC rellena no contiene necesariamente un número entero de octetos, debido al proceso de inserción de 0. Por tanto, no hay una correspondencia directa de una trama HDLC rellena, a octetos, en un canal DCC. El generador de señales HDLC deriva su temporización de la función ServerLayer/DCC_A (es decir, la señal DCC_CI_CK) para SDH. Las siguientes funciones ServerLayer/DCC_A están definidas en la Rec. UIT-T G.783: función MSn/DCC_A, función MS256/DCC_A y función RSn/DCC_A.

La señal de trama HDLC es un tren de bits serie que se insertará en el canal DCC de forma que los bits serán transmitidos por el módulo STM-N en el mismo orden en que fueron recibidos del generador de señales de trama HDLC.

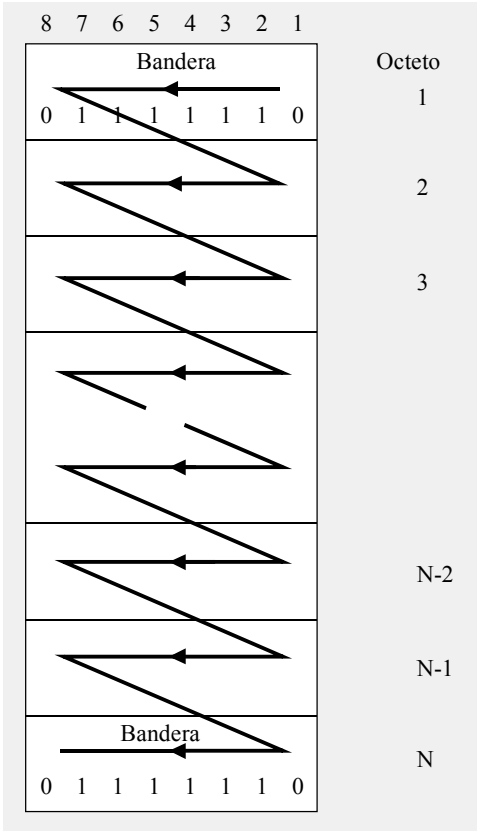


Figura 7-2/G.7712/Y.1703 – Formato de trama HDLC

7.1.2.1.2 Especificación del protocolo de capa de enlace de datos ECC SDH

Hay tres tipos de interfaces: interfaces exclusivamente IP, interfaces exclusivamente OSI, e interfaces duales (las interfaces duales pueden transportar tanto paquetes IP como OSI). Para transportar exclusivamente IP por el DCC, es necesario utilizar el entramado PPP en HDLC (conocido por PPPinHDLC) como protocolo de capa de enlace de datos. Dado que las interfaces duales pueden transportar tanto IP como OSI, una interfaz dual podrá conectarse sea a una interfaz exclusivamente IP, sea a una interfaz exclusivamente OSI, o a otra interfaz dual. En las redes actuales hay interfaces exclusivamente OSI, en las que se utiliza el protocolo LAPD definido en la Rec. UIT-T G.784 para el enlace de datos. Para que las interfaces duales puedan conectarse a una interfaz exclusivamente IP o a una interfaz exclusivamente OSI, es necesario que el protocolo de capa de enlace de datos soportado en la interfaz dual se pueda configurar para el soporte de PPPinHDLC o LAPD. Hay una excepción para los elementos de red SDH integrados que soportan LAPD en equipos potenciados para el soporte de interfaces duales. Para limitar la cantidad de

potenciaciones de equipos, se permite que los elementos de red SDH potenciados soporten únicamente LAPD.

7.1.2.1.2.1 Interfaz exclusivamente IP

En la figura 7-3 se representan las interfaces exclusivamente IP.

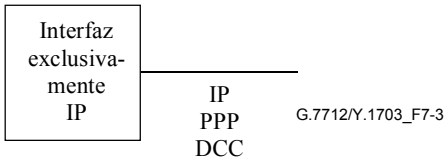


Figura 7-3/G.7712/Y.1703 – Interfaz exclusivamente IP

Las interfaces exclusivamente IP deben utilizar el protocolo PPP definido en RFC 1661.

7.1.2.1.2.2 Interfaz exclusivamente OSI

En la figura 7-4 se representan las interfaces exclusivamente OSI.

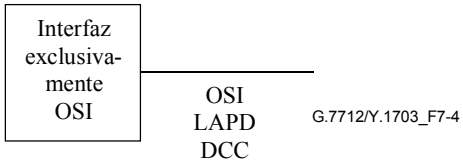


Figura 7-4/G.7712/Y.1703 – Interfaz exclusivamente OSI

Las interfaces exclusivamente OSI deben utilizar LAPD definido en la Rec. UIT-T G.784.

7.1.2.1.2.3 Interfaz dual (IP+OSI)

Las interfaces duales (interfaces que pueden transportar tanto paquetes OSI como IP) pueden conectarse a interfaces exclusivamente IP, interfaces exclusivamente OSI, o a otras interfaces duales. Para que las interfaces duales puedan conectarse a otras interfaces exclusivamente IP o interfaces exclusivamente OSI, es necesario que el protocolo de enlace de datos de la interfaz dual se pueda configurar para que conmute entre entramado PPP en HDLC (definido en RFC 1662) y LAPD (definido en la Rec. UIT-T G.784) como se ilustra en la figura 7-5. Se señala que los elementos de red SDH integrados que soportan LAPD en equipos potenciados para el soporte de IP no tienen que soportar también entramado PPP en HDLC en sus interfaces duales. Por tanto, estas interfaces duales sólo tienen que soportar LAPD.

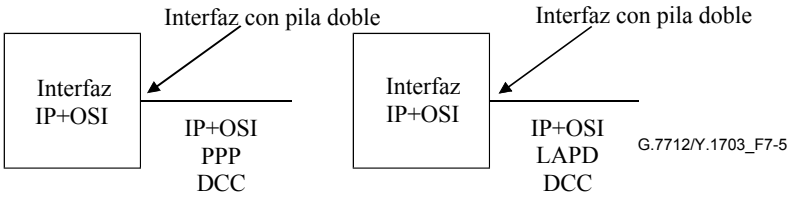


Figura 7-5/G.7712/Y.1703 – Interfaz dual

Las interfaces duales que soportan el protocolo PPP utilizarán el PPP definido en RFC 1661.

Las interfaces duales que soportan LAPD utilizarán el LAPD definido en la Rec. UIT-T G.784.

7.1.3 Función de encapsulación "PDU de capa de red en trama de enlace de datos ECC"

Una función de encapsulación "PDU de capa de red en trama de enlace de datos ECC" encapsula la PDU de capa de red en la trama de enlace de datos y la desencapsula de esta trama. Esta función también procesa el identificador de protocolo. Se define en las Recomendaciones para las distintas tecnologías. No obstante, a continuación se describe la función de encapsulación "PDU de capa de red en trama de enlace de datos ECC de SDH".

7.1.3.1 Función de encapsulación "PDU de capa de red en trama de enlace de datos ECC de SDH"

Se describe la función de encapsulación "PDU de capa de red en trama de enlace de datos ECC de SDH" para interfaces exclusivamente IP, interfaces exclusivamente OSI e interfaces duales.

7.1.3.1.1 Interfaz exclusivamente IP

Las interfaces exclusivamente IP utilizarán solamente IP/PPPinHDLCframing/DCC tal como está definido en RFC 1662.

A continuación se define la interfaz exclusivamente IP:

El extremo de transmisión

- Colocará paquetes IS-IS directamente en el campo Información PPP, de acuerdo con RFC 1661, con el valor de protocolo OSI, conforme a RFC 1377, en el campo Protocolo PPP.
- Colocará paquetes IPv4 directamente en el campo Información PPP, de acuerdo con RFC 1661, con el valor de protocolo IPv4, conforme a RFC 1332, en el campo Protocolo PPP.
- Colocará paquetes IPv6 directamente en el campo Información PPP, de acuerdo con RFC 1661, con el valor de protocolo IPv6, conforme a RFC 2472, en el campo Protocolo PPP.

En el extremo de recepción

- Se identificará un paquete IS-IS cuando el campo Protocolo PPP tenga el valor de protocolo OSI de acuerdo con RFC 1377 y el paquete tenga el NLPID correspondiente a IS-IS como se especifica en la Rec. UIT-T X.263 | ISO/CEI 9577.
- Se identificará un paquete IPv4 cuando el campo Protocolo PPP tenga el valor de protocolo IPv4 de acuerdo con RFC 1332.
- Se identificará un paquete IPv6 cuando el campo Protocolo PPP tenga el valor de protocolo IPv6 de acuerdo con RFC 2472.

7.1.3.1.2 Interfaz exclusivamente OSI

Las interfaces exclusivamente OSI utilizarán solamente LAPD/DCC, de acuerdo con la Rec. UIT-T G.784.

A continuación se define la interfaz exclusivamente OSI:

El extremo de transmisión

- Colocará paquetes CLNP, IS-IS y ES-IS directamente en la parte útil LAPD de acuerdo con la Rec. UIT-T G.784.

El extremo de recepción

– Examinará el identificador de protocolo situado en el primer octeto de la parte útil LAPD. El valor de este identificador corresponde a los valores asignados en la Rec. UIT-T X.263 | ISO/CEI 9577. Si la PDU recibida corresponde a un protocolo no soportado por el receptor, será descartada.

7.1.3.1.3 Interfaz dual (IP+OSI)

A continuación se define una interfaz dual que soporta PPP como protocolo de enlace de datos:

El extremo de transmisión

– Colocará paquetes CLNP, IS-IS y ES-IS directamente en el campo información PPP, de acuerdo con RFC 1661, con el valor de protocolo OSI, conforme a RFC 1377, en el campo protocolo PPP.

– Colocará paquetes IPv4 directamente en el campo información PPP, de acuerdo con RFC 1661, con el valor de protocolo IPv4, conforme a RFC 1332, en el campo protocolo PPP.

– Colocará paquetes IPv6 directamente en el campo información PPP, de acuerdo con RFC 1661, con el valor de protocolo IPv6, conforme a RFC 2472, en el campo protocolo PPP.

En el extremo de recepción

– Se identificará un paquete OSI cuando el campo Protocolo PPP tenga el valor de protocolo OSI conforme a RFC 1377.

– Se identificará un paquete IPv4 cuando el campo Protocolo PPP tenga el valor de protocolo IPv4 conforme a RFC 1332.

– Se identifica un paquete IPv6 cuando el campo Protocolo PPP tenga el valor de protocolo IPv6 conforme a RFC 2472.

A continuación se define una interfaz dual que soporta LAPD como protocolo de enlace de datos:

El extremo de transmisión

– Colocará paquetes CLNP, IS-IS y ES-IS directamente en la parte útil LAPD, de acuerdo con la Rec. UIT-T G.784.

– Colocará paquetes IP directamente en la parte útil LAPD, precedidos de un identificador de protocolo con una longitud de un octeto. Este identificador deberá corresponder a los valores asignados en la Rec. UIT-T X.263 | ISO/CEI 9577 para IPv4 e IPv6.

El extremo de recepción

– Examinará el identificador de protocolo situado en el primer octeto de la parte útil LAPD. El valor de este identificador corresponde a los valores asignados en la Rec. UIT-T X.263 | ISO/CEI 9577. Si la PDU recibida corresponde a un protocolo no soportado por el receptor, será descartada.

7.1.4 Función de terminación física LAN Ethernet

La función de terminación física LAN Ethernet termina la interfaz Ethernet física.

Se soportarán una o más de las siguientes velocidades: 1 Mbit/s, 10 Mbit/s, 100 Mbit/s.

Los elementos de red que soportan interfaces LAN Ethernet están autorizados a acceder a canales ECC terminados. No es necesario que todos los elementos de red que soportan canales ECC soporten puertos LAN Ethernet, siempre que exista un trayecto ECC desde el elemento de red que termina el canal ECC, y que otro elemento de red proporcione los puertos LAN Ethernet.

7.1.5 Función de encapsulación "PDU de capa de red en trama Ethernet"

Esta función encapsula PDU de la capa de red en tramas 802.3 o Ethernet (versión 2) y las desencapsula de éstas.

Encapsulará PDU de capa de red en tramas 802.3 o Ethernet (versión 2) de acuerdo con las siguientes reglas:

- Encapsulará PDU de CLNP, IS-IS, y ES-IS en tramas 802.3 de conformidad con la Rec. UIT-T Q.811, y las desencapsula de estas tramas.
- Encapsulará paquetes IP en tramas Ethernet (versión 2), de conformidad con RFC 894, y los desencapsula de estas tramas.
- Hará corresponder direcciones IP a direcciones MAC Ethernet, utilizando el protocolo de resolución de dirección definido en RFC 826.

Determina el tipo de trama recibida (802.3 o Ethernet versión 2) de acuerdo con 2.3.3 de RFC 1122.

7.1.6 Función de reenvío de PDU de capa de red

La función de reenvío de PDU de capa de red reenvía paquetes de capa de red.

Si esta función reenvía paquetes CLNP, los reenviará de acuerdo con la Rec. UIT-T Q.811.

Si esta función reenvía paquetes IPv4, los reenviará de acuerdo con RFC 791.

Si esta función reenvía paquetes IPv6, los reenviará de acuerdo con RFC 2460.

El formato de direccionamiento preferido es IPv6. El protocolo de encaminamiento IP debe admitir el direccionamiento IPv6 y el IPv4.

7.1.7 Función de interfuncionamiento de PDU de capa de red

La función de interfuncionamiento de PDU de capa de red sirve para que puedan comunicarse funciones DCF vecinas que utilizan protocolos de capa de red diferentes. La DCF que soporta IP también debe soportar OSI para permitir la comunicación con la DCF vecina que sólo soporta OSI.

7.1.8 Función de encapsulación de PDU de capa de red

La función de encapsulación de PDU de capa de red encapsula una PDU de capa de red en otra PDU de capa de red, y la desencapsula de ésta.

Los paquetes CLNP se encapsularán en IP mediante encapsulación de encaminamiento genérica (GRE, *generic routing encapsulation*), especificada en RFC 2784, como parte útil en un paquete IP utilizando un número de protocolo IP de 47 (decimal) y sin poner a "1" el bit DF (no fragmentar). Según RFC 2784, la GRE contendrá un ethertype para indicar el protocolo de capa de red que se está encapsulando. Debe utilizarse el ethertype 00FE (hex), que es la norma de la industria para OSI.

Los paquetes IP se encapsularán en CLNS utilizando la GRE, especificada en RFC 2784, como la parte útil de los datos de una PDU del tipo de datos CLNP, especificada en ISO/CEI 8473-1, con un valor de selector NSAP de 47 (decimal) y con la bandera SP (segmentación permitida) puesta a "1". Para mayor información véase RFC 3147.

Los paquetes IP se encapsularán en IP utilizando la GRE, especificada en RFC 2784, como parte útil en un paquete IP utilizando un número de protocolo IP de 47 (decimal) y sin poner a "1" el bit DF (no fragmentar).

Opcionalmente, la función de encapsulación de PDU de la capa red puede reenviar PDU a través de nodos incompatibles por medio del procedimiento de encapsulación automática descrito en el anexo B. Obsérvese que una DCF que soporte el procedimiento de encapsulación automática

descrito en el anexo B es compatible con una DCF que no soporte el procedimiento de encapsulación automática y puede instalarse en la misma área que ésta.

7.1.9 Función de tunelización de PDU de capa de red

La función de tunelización de PDU de capa de red proporciona un túnel estático entre dos DCF que soporten la misma PDU de capa de red. En el caso de un túnel en el que se haya configurado un tamaño de unidad de transmisión máxima (MTU), todo paquete IP que no pueda ser reenviado a través del túnel por ser más grande que el tamaño de la MTU, y cuyo bit DF está puesto a "1" deberá descartarse debiendo devolverse al originador del paquete un mensaje de error ICMP inalcanzable (en particular el código "se necesita fragmentación y DF puesto a 1").

7.1.10 Función de encaminamiento de capa de red

La función de encaminamiento de capa de red encamina paquetes de la capa de red.

Una DCF que soporte el encaminamiento OSI, también soportará IS-IS de conformidad con ISO/CEI 10589.

Una DCF que soporte el encaminamiento IP, también soportará IS-IS Integrado (véanse los requisitos para IS-IS integrado en 7.1.10.1) y también puede soportar OSPF y otros protocolos de encaminamiento IP.

7.1.10.1 Requisitos de IS-IS integrado

Una DCF que soporte IS-IS integrado, soportará RFC 1195.

Un DCF que soporte IS-IS integrado, soportará la toma de contacto triple en todos los enlaces punto a punto (véanse los requisitos de la toma de contacto triple en el anexo A). La toma de contacto triple modifica el comportamiento de la creación y mantenimiento de adyacencias especificada en ISO/CEI 10589.

7.1.10.1.1 Creación de adyacencias consciente del protocolo de capa de red

La DCF incluirá un TLV "protocolos soportados" en todas las PDU IIH e ISH de todas las interfaces, y en todos los LSP con número de LSP igual a cero, de acuerdo con RFC 1195.

Cuando reciba una PDU ISH o IIH IS-IS, la DCF inspeccionará la PDU para ver si contiene un TLV de "protocolos soportados". Esto tendrá lugar en todas las interfaces, ya sean de LAN, de DCC o de otros enlaces. Si una PDU ISH o IIH no contuviera un TLV "protocolos soportados", se trataría como si contuviese un TLV "protocolos soportados" que llevase únicamente el NLPID para CLNP.

La DCF comparará los NLPID relacionados en el TLV "protocolos soportados" (suponiendo solamente CLNP si no hay ninguno) con los protocolos de capa de red que la DCF es capaz de reenviar por sí misma.

De no existir ninguna adyacencia con el vecino que envió el ISH o IIH, y si la DCF no fuera capaz de reenviar ninguno de los protocolos de capa de red relacionados en el TLV "protocolos soportados" del ISH o IIH recibido del vecino, la DCF no deberá formar adyacencia alguna con dicho vecino.

De existir alguna adyacencia con el vecino que envió el ISH o IIH, y si la DCF no fuera capaz de reenviar ninguno de los protocolos de capa de red relacionados en el TLV "protocolos soportados" del ISH o IIH recibido del vecino, la DCF deberá suprimir la adyacencia con dicho vecino y generar un evento ProtocolsSupportedMismatch Event (*discordancia de los protocolos soportados*).

Si la DCF fuera capaz por sí misma de reenviar uno o más de los protocolos de capa de red relacionados en el TLV "protocolos soportados" de ISH o IIH recibido, la DCF deberá procesar el ISH o IIH con normalidad.

La DCF no considerará el valor del TLV "protocolos soportados" de los LSP durante este proceso.

Una DCF que no pueda enviar PDU CLNP deberá ignorar las PDU ESH, no debiendo por consiguiente anunciar su alcanzabilidad a los sistemas de extremo OSI.

7.1.10.1.2 Distribución de prefijo IP en todo el dominio IS-IS

Las DCF que soportan IS-IS integrado de nivel 1, nivel 2 soportarán el anuncio de prefijos de destino IP configurados, aprendidos mediante paquetes de estado de enlace (LSP) de nivel 2 pasados al nivel 1, así como prefijos de destino IP aprendidos mediante LSP de nivel 1 pasados al nivel 2. El comportamiento por defecto cuando no se haya configurado ningún prefijo de destino IP consistirá en no propagar ningún prefijo de nivel 2 en LSP de nivel 1, mientras que todos los prefijos aprendidos de nivel 1 se propagarán a LSP de nivel 2.

7.1.10.1.2.1 Prefijos de configuración

El operador deberá proporcionar dos cuadros para controlar la propagación de prefijos. Un cuadro controlará la propagación del nivel 1 al nivel 2, y el otro controlará la propagación del nivel 2 al nivel 1.

7.1.10.1.2.2 Etiquetado de los prefijos propagados

Puesto que la propagación de prefijos del nivel 2 al nivel 1, y el subsiguiente retorno del nivel 1 al nivel 2 puede producir bucles de encaminamiento, se necesita una etiqueta para identificar la fuente del prefijo. Esta etiqueta, conocido como bit activo/inactivo, se almacena en el bit de orden superior (bit 8), no utilizado anteriormente, del campo métrica por defecto, en los TLV de alcanzabilidad IP, y en los TLV de alcanzabilidad externa IP. Las implementaciones actuales de IS-IS que soporten RFC 1195 no resultarán afectadas por la redefinición de este bit, pues RFC 1195 establece que este bit debe ponerse a cero cuando se originen LSP y no debe tenerse en cuenta en recepción. Para más información, véase RFC 2966.

Los TLV de alcanzabilidad IP y los de alcanzabilidad externa IP deben ser procesados de la misma forma. El tipo de TLV recibido coincidirá con el utilizado para propagar el prefijo del nivel 2 a un área de nivel 1, y de un área de nivel 1 al nivel 2.

La diferencia con RFC 1195 radica en que aquí los TLV de alcanzabilidad externa IP sólo pueden aparecer en LSP de nivel 2.

7.1.10.1.2.2.1 Transmisión LSP con TLV de alcanzabilidad IP y TLV de alcanzabilidad externa IP

Al igual que en el caso normal de RFC 1195, el valor del bit activo/inactivo será cero para todos los TLV de IP en LSP de nivel 2. El valor del bit activo/inactivo deberá ser cero para los LSP de nivel 1 originados en un área de nivel 1.

El bit activo/inactivo se pondrá a "1" en los TLV de IP de un LSP de nivel 1 cuando los elementos de red de nivel 1, nivel 2 IS-IS integrados propaguen un prefijo configurado del nivel 2 al nivel 1.

7.1.10.1.2.2.2 Recepción de LSP con TLV de alcanzabilidad IP y TLV de alcanzabilidad externa IP

Una DCF que soporte IS-IS integrado deberá ignorar el valor del bit activo/inactivo cuando se desarrollen rutas para un área de nivel 1 o para el nivel 2.

Una DCF que soporte IS-IS integrado de nivel 1, nivel 2, y que reciba un LSP con un TLV de IP para un prefijo que concuerde con una entrada del cuadro de propagación de nivel 1 a nivel 2, anunciará el prefijo apropiado de nivel 1 a nivel 2.

Una DCF que soporte IS-IS integrado de nivel 1, nivel 2 y que reciba un LSP con un TLV de IP que tenga el bit activo/inactivo puesto a "1", no deberá utilizar nunca el prefijo para propagación de información de nivel 1 a nivel 2.

7.1.10.1.2.2.3 Utilización del bit activo/inactivo en LSP de nivel 2

La utilización del bit activo/inactivo en LSP de nivel 2 queda en estudio.

7.1.10.1.2.3 Preferencia de rutas

Dado que se puede propagar prefijos del nivel 2 al nivel 1, es necesario actualizar las preferencias de rutas especificadas en RFC 1195 para tener en cuenta este nuevo origen. El orden de preferencia de rutas resultante es el siguiente:

1) Rutas intraárea L1 con métrica interna.
   Rutas externas L1 con métrica interna.
2) Rutas intraárea L2 con métrica interna.
   Rutas externas L2 con métrica interna.
   Rutas interáreas propagadas de L1 a L2 con métrica interna.
   Rutas externas interáreas propagadas de L1 a L2 con métrica interna.
3) Rutas interáreas propagadas de L2 a un área L1 con métrica interna.
   Rutas externas propagadas de L2 a un área L1 con métrica interna.
4) Rutas externas L1 con métrica externa.
5) Rutas externas L2 con métrica externa.
   Rutas externas interáreas propagadas de L1 a L2 con métrica externa.
6) Rutas externas interáreas propagadas de L2 a un área L1 con métrica externa.

7.1.11 Función de interfuncionamiento del encaminamiento IP

Una DCF que soporte la función de interfuncionamiento de encaminamiento IP, deberá soportar los mecanismos de filtrado de ruta especificados en 7.5 y 7.6 de RFC 1812, para poder conectar redes con dos protocolos de encaminamiento a través de más de un punto de intercambio.

7.1.12 Función de correspondencia "aplicaciones a la capa de red"

Las aplicaciones OSI que funcionan sobre (una parte de) la RCD que sólo soporta IP se pueden hacer corresponder con IP como se especifica en 2.1.6/Q.811 que trata del perfil de protocolo RFC 1006/TCP/IP. Esta correspondencia es una solución de capa 4, por lo que está fuera del alcance de esta Recomendación. Otra opción para transportar aplicaciones OSI a través de (una parte de) la RCD que sólo soporta IP, es proporcionar una encapsulación de OSI en la capa 3 de IP, como se especifica en 7.1.8.

La correspondencia de aplicaciones IP a través de (una parte de) la RCD que soporta IP se ajustará a las especificaciones para la serie IP.

7.1.13 Función de encapsulación "PDU MPLS en capa de enlace datos ECC"

Esta función encapsula PDU MPLS en tramas de la capa de enlace de datos ECC y las desencapsula de éstas.

Cuando sea PPP el protocolo de enlace datos soportado en la interfaz ECC, se requerirá lo siguiente:

– *En el extremo de transmisión*

  Se colocarán los paquetes MPLS directamente en el campo Información PPP de acuerdo con RFC 1661 con el valor de protocolo MPLS 0281 hex en el campo Protocolo PPP de acuerdo con 4.3 de RFC 3032 sobre unidifusión MPLS.

– *En el extremo de recepción*

Se identificará un paquete MPLS cuando el campo Protocolo PPP tenga el valor de protocolo MPLS 0281 hex de acuerdo con 4.3 de RFC 3032 sobre unidifusión MPLS.

7.1.14 Función de encapsulación "PDU MPLS en trama Ethernet"

Esta función encapsula PDU MPLS en tramas Ethernet (versión 2) y las desencapsula de éstas.

Deberá encapsular PDU MPLS en tramas Ethernet (versión 2) de acuerdo con RFC 894 utilizando un valor ethertype de 8847 hex con arreglo a la sección 5 de RFC 3032 relativo a unidifusión MPLS.

7.1.15 Función de señalización MPLS LSP

La función de señalización MPLS LSP proporciona la señalización necesaria para establecer el MPLS LSP.

Una DCF que soporte la función de señalización MPLS LSP deberá soportar el siguiente modelo de reserva: trayecto explícito con una ruta estricta a través de nodos sencillos (dirección IP de 32 bits), para LSP unidifusión punto a punto, a través del estilo de reserva "FF" por IPv4.

El mensaje del trayecto se reenvía al destino en un trayecto especificado por una lista de direcciones IP en el objeto ruta explícita (ERO, *explicit route object*). Cada nodo (LSR) del trayecto registra el ERO. Mediante el objeto petición de etiqueta, los nodos (LSR) proporcionan la vinculación de etiquetas para la sesión. Véanse 2.2, 3.1, 4.2 y 4.3 de RFC 3209 – RSVP-TE.

El nodo de destino responde con un mensaje Resv, que se envía al remitente en el origen, en orden inverso de la lista de nodos del ERO. La etiqueta del objeto etiqueta del mensaje Resv se utiliza en cada LSR intermedio para asociar el tráfico saliente a dicho LSP. Si el nodo no fuera el del remitente, asignaría una nueva etiqueta y la colocaría en el objeto etiqueta del mensaje Resv, enviándolo hacia el origen al PHOP. Véanse los puntos 2.2, 3.2 y 4.1 de RFC 3209 – RSVP-TE.

Si el nodo no pudiera satisfacer la petición, enviaría un mensaje PathErr o ResvErr al nodo remitente. Véase 4.5 de RFC 3209 – RSVP TE.

El procedimiento de estado blando del RSVP supone el envío periódico de una representación completa del estado LSP en mensajes Resv y Path para mantener el LSP. Se utiliza el mensaje Srefresh en lugar del envío periódico de mensajes normales Path y Resv. Cada MessageID del mensaje Srefresh representa un mensaje Path o Resv completo, para el que no se modifica el estado. Véase 5.5 de RFC 2961 – RSVP-ORE.

El objeto MESSAGE_ID_NACK se utiliza para indicar la discordancia del MessageID recibido, necesitándose un mensaje Path o Resv completo para restaurar el LSP. Véase 5.4 de RFC 2961 – RSVP-ORE.

El objeto MESSAGE_ID_ACK se utiliza para el acuse de recibo de los mensajes que contienen un objeto MESSAGE_ID y para el que la bandera ACK_desired está activada. Forma parte del algoritmo de retransmisión de Srefresh descrito en 6.3 de RFC 2961 – RSVP-ORE.

7.1.16 Función de reenvío MPLS LSP

La función de reenvío MPLS LSP entrega el paquete MPLS de llegada a una interfaz de salida con arreglo a su etiqueta MPLS y a la entrada de reenvío de etiqueta del salto siguiente (NHLFE, *next hop label forwarding entry*) de acuerdo con RFC 3031.

La secuencia de los paquetes debe mantenerse dentro del LSP.

7.1.17 Función de cálculo del trayecto MPLS LSP

La función de cálculo del trayecto MPLS LSP calcula el trayecto para un LSP unidireccional. Esta función deberá poder calcular los trayectos para dos LSP unidireccionales con el mismo destino de modo que sus trayectos no atraviesen el mismo nodo o subred.

7.1.18 Función de encapsulación "Paquete de la capa de red en MPLS"

La función de encapsulación "Paquete de la capa de red en MPLS" añade la entrada de la pila de etiquetas MPLS al paquete de capa de red, o la suprime de éste, de acuerdo con RFC 3032.

7.1.19 Función de protección de paquetes MPLS 1+1

7.1.19.1 Asociación de dos LSP

Los nodos de ingreso y egreso deberán identificar y asociar los dos LSP que proporcionan el servicio de paquetes 1+1. Esta asociación entre dos LSP puede establecerse o bien mediante la interfaz de gestión de la red o mediante señalización.

Cuando se establezca mediante señalización, deberá transferirse un identificador en cada uno de los distintos LSP. El identificador deberá ser idéntico en cada uno de los distintos LSP y único entre los LSP iniciados por el nodo de ingreso y los LSP terminados por el nodo de egreso.

El mecanismo específico de asignación del identificador así como el medio de transporte del identificador en el protocolo de señalización queda en estudio. El mecanismo se asemejará al requerido para la asociación de LSP en otros mecanismos de protección basados en MPLS tales como 1+1 ó 1:1.

A fin de cumplir el requisito de que no sea necesario ampliar la señalización en los nodos intermedios, el identificador y el tipo de servicio LSP (o sea, el paquete 1+1) deberán transportarse en objetos opacos.

7.1.19.2 Formato del identificador de secuencia

El número de secuencia se utilizará como identificador para la protección de paquetes 1+1. El nodo de ingreso asigna el mismo número de secuencia único a cada copia del paquete de alimentación dual. El número de secuencia del paquete siguiente se genera sumando uno al número de secuencia actual.

El nodo de egreso utiliza el número de secuencia para garantizar que sólo se selecciona la primera copia recibida del paquete mientras que se descarta la segunda copia recibida. El nodo de egreso separa el número de secuencia del paquete tras su selección, antes de pasarlo a la capa superior de la pila. Obsérvese que el mecanismo de recuperación de paquetes 1+1 es independiente de las aplicaciones/protocolos soportados por encima de MPLS.

El número de secuencia de los paquetes se transportará en los cuatro primeros octetos del encabezamiento de cuña de cada uno de los LSP que proporcionan la protección de paquetes 1+1. El número inicial de secuencia asignado al primer paquete por el nodo de ingreso deberá acordarse entre los nodos de ingreso y egreso. El valor por defecto del número inicial de secuencia es cero.

El número de secuencia se sitúa tras el encabezamiento de encapsulación MPLS de 4 octetos como muestra la figura 7-6. Obsérvese que el paquete 1+1 puede suministrarse en cualquier nivel de la jerarquía de un LSP anidado.

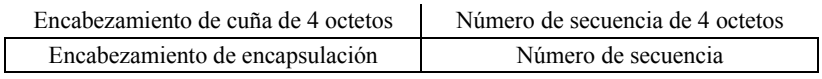


Figura 7-6/G.7712/Y.1703 – Formato identificador de secuencia

7.2 Requisitos relativos a la provisión

Todos los elementos de red deberán soportar la creación de una interfaz sin ninguna manifestación física. La interfaz deberá ser capaz de admitir una dirección IP.

El tamaño del LSP será configurable.

Así se podrá determinar el tamaño de la MTU dentro del dominio.

Para ajustarse al principio de prioridad del trayecto abierto más corto (OSPF, *open shortest path first*), es necesario proporcionar un identificador de área por interfaz, incluidos los canales ECC y la LAN.

7.3 Requisitos de seguridad

Deben tomarse precauciones para evitar interacciones (direcciones, etc.) no deseadas entre una red IP pública y una RCD que soporte IP.

Anexo A[1]

Requisitos de la toma de contacto triple

El procedimiento de toma de contacto triple se basa en la función de toma de contacto triple del Grupo de Trabajo IS-IS del IETF (RFC 3373) y se ha diseñado manteniendo la compatibilidad con la misma.

A.1 TLV de adyacencia triple punto a punto

Una DCF que soporte IS-IS integrado deberá incluir un TLV en todos las PDU IIH punto a punto. La estructura de dicho TLV será:

Tipo = 0xF0 (decimal 240)

Longitud = de 5 a 17 octetos

Valor:

Estado triple de la adyacencia (un octeto):

0 = Activo

1 = Inicialización

2 = Inactivo

ID del circuito local ampliado de cuatro octetos

ID del sistema vecino de 0 a ocho octetos si se conoce

ID del circuito local ampliado vecino de cuatro octetos si se conoce

El ID del circuito local ampliado lo designará la DCF cuando se cree el circuito; la DCF utilizará un valor distinto para cada uno de sus circuitos punto a punto.

El estado triple de adyacencia comunicado en el TLV se ajustará a lo especificado en la clásula A.2.

[1] NOTA – Este nuevo anexo A sustituye al de la versión 2001 de la Rec. UIT-T G.7712/Y.1703.

A.2 Estado triple de adyacencia

Una DCF que soporte IS-IS integrado deberá tener, para cada circuito punto a punto, un estado triple de adyacencia. Este estado es distinto del estado especificado en ISO/CEI 10589.

De no existir adyacencia alguna en un enlace, el estado triple de adyacencia deberá ponerse a "inactivo".

Si una DCF recibe un ISH en un enlace punto a punto y esto provoca la creación de una nueva adyacencia con el estado de adyacencia "inicialización", el estado triple de adyacencia deberá ponerse a "inactivo".

Si una DCF recibe un IIH punto a punto que no contenga TLV de adyacencia triple, la DCF deberá comportarse con arreglo a ISO/CEI 10589, aunque incluyendo el TLV en las PDU IIH de dicho enlace comunicando el estado triple de adyacencia "inactivo".

Si una DCF recibe una PDU IIH punto a punto que contenga un TLV de adyacencia triple, la DCF deberá comportarse de manera distinta al proceso de la PDU IIH de ISO/CEI 10589, en cuanto a lo siguiente:

- Si están presentes los campos ID del sistema vecino e ID del circuito local ampliado vecino del TLV y alguno de los ID de sistema vecino no concuerda con el ID de la DCF, o bien si el ID del circuito local ampliado vecino no concuerda con el ID ampliado de la DCF, se descartará la PDU IIH y no se procesará.
- Si la PDU IIH provoca que los cuadros de estados ISO/CEI 10589 produzcan un "activo" o "aceptar", y el estado triple de adyacencia recibido es "inactivo", la DCF deberá poner su estado triple de adyacencia a "inicialización".
- Si la PDU IIH provoca que los cuadros de estados ISO/CEI 10589 produzcan un "activo" o "aceptar", y el estado triple de adyacencia recibido es "inicialización", la DCF deberá modificar su estado triple de adyacencia de "inactivo" o "inicialización " a "activo" y generar un evento "AdjacencyChangeState(Up)".
- Si la PDU IIH provoca que los cuadros de estados de ISO/CEI 10589 produzcan un "activo" o "aceptar", y el estado triple de adyacencia recibido es "inicialización", cuando la DCF ya tenga el estado triple de adyacencia "activo" deberá mantener su estado triple de adyacencia en "activo".
- Si la PDU IIH provoca que los cuadros de estados de ISO/CEI 10589 produzcan un "activo" o "aceptar", y el estado triple de adyacencia recibido es "activo", cuando DCF ya tenga el estado triple de adyacencia de "inactivo", generará un evento "AdjacencyStateChange(Down)" con la razón "vecino rearrancado" y se suprimirá la adyacencia sin que tenga lugar procesamiento adicional de la PDU IIH.
- Si la PDU IIH provoca que los cuadros de estados de ISO/CEI 10589 produzcan un "activo" o "aceptar", y el estado triple de adyacencia es "activo", cuando la DCF ya tenga un estado triple de adyacencia "inicialización" modificará su estado triple de adyacencia a "activo" y generará un evento "AdjacencyChangeState(Up)".
- Si la PDU IIH provoca que los cuadros de estados de ISO/CEI 10589 produzcan un "activo" o "aceptar", y el estado triple de adyacencia recibido es "activo", cuando la DCF ya tenga un estado triple de adyacencia "activo", conservará su estado triple de adyacencia en "activo"
- No se ejecutarán la comparación subsiguiente del ID de origen de la PDU con el ID del sistema local ni la manipulación del ID del circuito.

Si la PDU IIH provoca que los cuadros de estados de ISO/CEI 10589 produzcan un "activo" o "aceptar", la DCF deberá efectuar lo siguiente:

1) copiar del campo Direcciones de área de la PDU, las entradas areaAddressOfNeighbour de la adyacencia,
2) fijar el valor holdingTimer del campo Tiempo de ocupación de la PDU, y
3) dar a neighbourSystemID el valor del campo ID de origen de la PDU de acuerdo con ISO/CEI 10589.

Anexo B

Requisitos de la encapsulación automática

B.1 Introducción

Este anexo presenta una especificación de la AE-DCF que hace posible que los nodos que soportan el encaminamiento de distintos protocolos incompatibles de la capa de red, tales como CLNS, IPv4 e IPv6, estén presentes en una única área de nivel 1 IS-IS o en un único subdominio de nivel 2, que encapsule automáticamente un protocolo de capa de red dentro del otro, cuando sea necesario, con tal de que todos los nodos soporten el encaminamiento IS-IS o el IS-IS integrado.

B.2 Alcance

La AE-DCF es una función opcional. De proporcionarse, deberá funcionar como se especifica en el presente anexo. Los requisitos del presente anexo se aplican únicamente a las DCF que contienen la funcionalidad adicional de una AE-DCF. La AE-DCF requiere asimismo ciertos comportamientos de las DCF que no incorporan la funcionalidad AE-DCF, a fin de poder interactuar con ellas. Los requisitos de las DCF que no incorporan la funcionalidad AE-DCF se presentan en 7.1.10.1 para los nodos IP y duales, y en ISO/CEI 10589 para los nodos OSI.

B.3 Descripción de la AE-DCF

B.3.1 Introducción

El IS-IS integrado especificado en RFC 1195 se diseñó inicialmente para encaminar IP y CLNS con un único protocolo de encaminamiento y un único algoritmo SPF. A tal efecto, las direcciones IPv4 y las máscaras de subred se representan como números de 64 bits a los que se aplica acto seguido el algoritmo SPF como si se tratase de una dirección de sistema de extremo OSI. Se exige que los nodos IS-IS integrados tengan una dirección de área IS-IS y un identificador de sistema, que se tratan del mismo modo que una dirección NSAP en un nodo exclusivamente OSI. Los nodos IS-IS integrados forman entonces adyacencias e identificadores del sistema de inundación y métricas en toda su área de nivel 1 (encaminadores de nivel 1) o en su subdominio de nivel 2 (encaminadores de nivel 2) del mismo modo que los nodos IS-IS exclusivamente OSI.

Los SID (identificadores de sistemas) y las métricas respecto a otros SID inundan toda un área de nivel 1 o un subdominio de nivel 2 mediante LSP (PDU de estado de enlace) comunes tanto a los nodos IS-IS como a los nodos IS-IS integrados. A continuación se añade a estos LSP la información específica de IP utilizando extensiones TLV que sólo pueden entender los nodos con capacidad IP. Los encaminadores exclusivamente OSI no pueden decodificar estos TLV aunque los dejen pasar inundando todas sus adyacencias. De este modo cualquier nodo IS-IS o IS-IS integrado puede construir un árbol SPF independientemente de si puede encaminar CLNS, IPv4 o IPv6. Los nodos con capacidad OSI calcularán los trayectos más cortos a los sistemas de extremo OSI, los nodos con

capacidad IPv4 calcularán los trayectos más cortos a las direcciones o prefijos IPv4, mientras que los nodos con capacidad IPv6 calcularán los trayectos más cortos a las direcciones o prefijos IPv6.

Una consecuencia de esto es que un nodo exclusivamente OSI calculará el trayecto más corto a un sistema de extremo OSI que atraviese un nodo exclusivamente IP aunque dicho nodo exclusivamente IP no pueda reenviar los paquetes CLNS. Análogamente un nodo exclusivamente IP calculará el trayecto más corto a un destino IP que atraviese un nodo exclusivamente OSI, aunque el nodo exclusivamente OSI no pueda reenviar paquetes IP. Por consiguiente un nodo exclusivamente capaz de OSI no debe situarse en un lugar de la red en el que exista la posibilidad de encontrarse en el trayecto más corto a destinos IP, y un nodo exclusivamente IP no debe situarse en un punto de la red en el que exista la posibilidad de encontrarse en el trayecto más corto a un sistema de extremo OSI.

El algoritmo IS-IS integrado sólo puede utilizar un único algoritmo SPF para dos o más protocolos de capa de red debido a la hipótesis de que todos los protocolos de capa de red tienen acceso a los mismos recursos, o dicho de otro modo, a la misma red con la misma topología. Por consiguiente el IS-IS integrado requiere que cualquier nodo de un área de nivel 1 o subdominio de nivel 2 sea capaz de encaminar cualquier protocolo de capa de red que esté presente en su área o dominio respectivamente.

Por esta razón, RFC 1195 impone restricciones topológicas a las redes que se encaminan mediante IS-IS integrado, requiriendo que todos los nodos soporten tanto IP como CLNS en las áreas en las que exista tanto tráfico CLNS como tráfico IP.

Por consiguiente, de acuerdo con RFC 1195, si se actualiza un nodo y reenvía paquetes IP, deberán actualizarse también todos los demás nodos del área de nivel 1 o subdominio de nivel 2.

La solución aquí planteada permite suprimir esta restricción topológica, al encapsular automáticamente los paquetes CLNS en paquetes IP para su reenvío a través de nodos exclusivamente IP y los paquetes IP en paquetes CLNS para su reenvío a través de nodos exclusivamente OSI. La solución aquí propuesta es totalmente compatible con los nodos exclusivamente OSI existentes, que no requieren actualización alguna. Sólo hay un requisito adicional a los de RFC 1195 para los nodos exclusivamente IPv4 o exclusivamente IPv6, a saber la función de creación de adyacencias consciente del protocolo de capa de red, especificada en 7.1.10.1.1.

B.3.2 El concepto de base

Esta característica se apoya en hecho de que todos los nodos IS-IS integrados e IS-IS comparten información topológica básica del mismo modo, y en el comportamiento de los nodos exclusivamente OSI en su intento de reenviar un paquete a través un nodo exclusivamente IP y viceversa, aunque dicho nodo sea incapaz de reenviar realmente dicho paquete. Normalmente esto provocaría la pérdida del paquete, pero una AE-DCF encapsula los paquetes antes de su reenvío a nodos incompatibles para que no se pierdan.

Cuando dos islas de nodos IS-IS integrados con capacidad IP se conecten por medio de una red central que soporte exclusivamente OSI, participando todos los nodos en la misma área (para nodos de nivel 1), los nodos con capacidad IP recibirán los LSP de los nodos con capacidad IP, incluso de los que se encuentran en otra isla, así como los LSP de todos los nodos exclusivamente OSI del centro. De este modo se calculan los trayectos más cortos a través de los nodos exclusivamente OSI para todos los destinos IP de la isla lejana. Sólo hay problemas cuando un nodo con capacidad IP reenvía realmente un paquete IP hacia un nodo exclusivamente OSI, perdiéndose el paquete. De aquí las restricciones topológicas de RFC 1195.

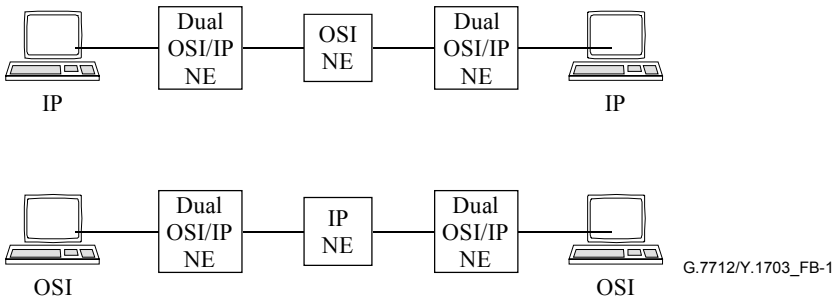


Figura B.1/G.7712/Y.1703 – Topologías prohibidas

La sencilla red anterior representada en la figura B.1 muestra topologías prohibidas por RFC 1195. En la red superior los paquetes IP se encaminan desde un lado de la red hacia el otro, pero cuando llegan al nodo exclusivamente OSI se descartan. Análogamente en la red inferior los paquetes CLNS se encaminan desde un lado de la red hacia el otro, pero al llegar al nodo exclusivamente IP se descartan. La especificación de una AE-DCF en este contexto corrige este comportamiento.

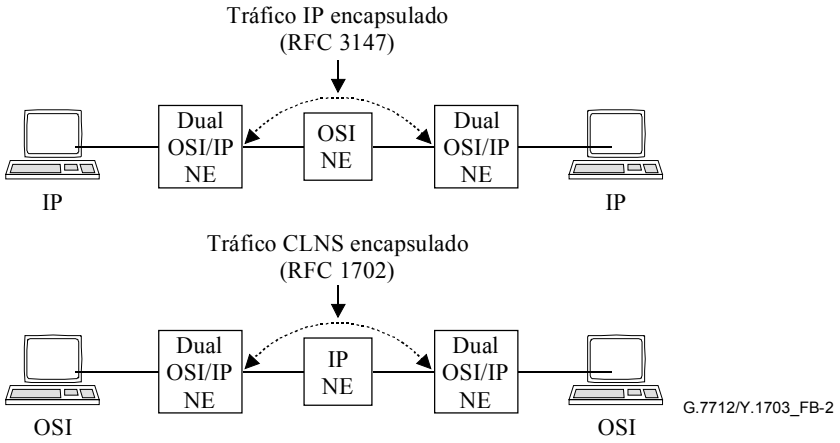


Figura B.2/G.7712/Y.1703 – Reparación por encapsulación

La AE-DCF reside en nodos duales permitiéndoles reconocer que un determinado vecino descartará cierto tráfico, a fin de encapsularlo de modo tal que no se descarte (véase la figura B.2). Esto 'repara' la red de modo que la parte de red comprendida entre los nodos duales se comporta como si estuviera constituida totalmente por nodos duales, cuando de hecho hay uno o más nodos no duales.

Una AE-DCF no altera el trayecto de los paquetes por la red; cualquier paquete individual seguirá atravesando la red por el trayecto más corto calculado mediante el algoritmo SPF IS-IS normal.

La función de creación de adyacencias consciente del protocolo de capa de red especificada en 7.1.10.1.1 forzará el tráfico a través de los nodos que soportan tanto IP como OSI cuando el trayecto más corto curse tráfico a través de una frontera entre las partes de un área con capacidad IP y las partes con capacidad OSI. Después, la AE-DCF hará que dichos nodos duales encapsulen los paquetes cuando sea necesario, para que los nodos que no soporten dicho protocolo de capa de red puedan reenviarlos. Esta encapsulación sólo tiene lugar cuando es necesario, de modo que estos túneles se crean automáticamente y son dinámicos. Los túneles resultantes no se conservan de ningún modo y existen únicamente como entradas en los cuadros de reenvío. Los túneles no aparecen como circuitos ni como interfaces en lo que al protocolo de encaminamiento respecta. Por consiguiente los paquetes suelen seguir cruzando la red por el trayecto más corto calculado por cada

nodo y, no habiendo necesidad de encapsular los paquetes IS-IS, sólo se encapsula el tráfico IP y CLNS.

B.4 Requisitos y límites

B.4.1 Requisitos de los nodos exclusivamente OSI

Para interfuncionar con la AE-DCF se requiere que los nodos exclusivamente OSI cumplan ISO/CEI 10589.

B.4.2 Requisitos de los nodos con capacidad IP

Para interfuncionar con la AE-DCF se requiere que los nodos exclusivamente IP cumplan RFC 1195.

En particular, se requiere que los nodos con capacidad IP ignoren los TLV "protocolos soportados" de los LSP de los nodos considerados como candidatos para trayectos más cortos al ejecutar el algoritmo SPF.

Un nodo con capacidad IP que sólo incluya nodos con capacidad IP en su cálculo SPF no se ajustará a RFC 1195, ya que éste especifica lo siguiente:

– De la página 26 de RFC 1195: "El cálculo de Dijkstra no tiene en cuenta si un encaminador es exclusivamente IP, exclusivamente OSI o dual. Las restricciones topológicas especificadas en 1.4 garantizan que los paquetes IP sólo se enviarán a través de encaminadores con capacidad IP, y que los paquetes OSI sólo se enviarán a través de encaminadores con capacidad OSI".

La AE-DCF es compatible con las implementaciones de RFC 1195 que se ajusten a la sentencia anterior. Una implementación que sólo incluya nodos con capacidad IP en su cálculo SPF no considerará los trayectos que atraviesen nodos exclusivamente OSI como rutas convenientes, no aprovechando de este modo la AE-DCF.

Para interfuncionar con la AE-DCF, se requiere que los nodos IP cumplan con 7.1.10.1.1. Esto se justifica por lo siguiente:

– Esta solución depende de que los paquetes IP lleguen a un nodo exclusivamente OSI sólo cuando hayan pasado previamente por una AE-DCF, y de que los paquetes CLNS lleguen a un nodo exclusivamente IP sólo cuando hayan pasado previamente por una AE-DCF. Por consiguiente la AE-DCF es la encargada de encapsular estos paquetes de modo que puedan reenviarse.
– Por consiguiente, un nodo exclusivamente IP no debe tener nunca una adyacencia con un nodo exclusivamente OSI.
– Si se utiliza esta solución para mezclar nodos IPv4 e IPv6 en la misma área de nivel 1 o subdominio de nivel 2, se concluye análogamente que un nodo exclusivamente IPv4 no debe tener nunca una adyacencia con un nodo exclusivamente IPv6.
– Este requisito se satisface si todos los nodos con capacidad IP se ajustan a 7.1.10.1.1. Obsérvese que este requisito no figura en RFC 1195.

Alternativamente, un operador puede controlar manualmente que los nodos que no soportan un protocolo común de capa de red no tengan adyacencias.

B.4.3 Requisitos para la encapsulación automática de nodos duales o plurilingües

Cuando haya que utilizar esta característica en un área de nivel 1 o subdominio de nivel 2, los nodos que soporten más de un protocolo de capa de red, pero que no soporten la AE-DCF, pueden utilizarse con reservas. Una alternativa más segura consiste en observar las restricciones topológicas de RFC 1195, o bien en utilizar exclusivamente nodos duales o plurilingües que contengan la AE-DCF.

B.4.3.1 TLV de capacidad de encapsulación

La AE-DCF incluirá un nuevo TLV en los LSP con un número de LSP igual a cero. El nuevo TLV tendrá la siguiente estructura:

Código: 16 (decimal)

Longitud: Longitud del valor

Valor: Parte de longitud variable con el siguiente contenido:

SubTLV tipo: 1

SubTLV longitud: tres veces el número de modos de encapsulación que haya en el subTLV

SubTLV valor:

47 indicando que los dos octetos siguientes son un encapsulación GRE;

El NLPID de un paquete que pueda encapsularse (interior);

El NLPID de un paquete que transporte el paquete encapsulado (exterior);

Octetos 4,5,6: Segundo modo de encapsulación (de ser necesario);

Octetos 7,8,9: Tercer modo de encapsulación (de ser necesario);

etc.

Los NLPID utilizados son los especificados en la Rec. UIT-T X.263/ISO/CEI 9577. Los nodos que transmitan este TLV deberán indicar los formatos que un nodo puede recibir y transmitir. Los nodos deben ser capaces de encapsular y desencapsular automáticamente los formatos descritos en el TLV, de modo que el tráfico pueda recibirse y pueda devolverse en sentido contrario.

Se recomienda que los nodos duales que soporten una AE-DCF sean capaces de encapsular/desencapsular A sobre B y B sobre A (siendo A y B los dos protocolos de capa de red soportados) lo que supone dos modos de encapsulación en un nodo dual típico.

Por ejemplo, el contenido del TLV para una AE-DCF OSI e IPv4 típica sería el siguiente:

16: código;

8: longitud del valor (en este ejemplo);

1: subTLV tipo 1;

6: subTLV longitud (en este ejemplo);

47: dos octetos siguientes soportados en modo GRE;

129: IPI para CLNP de la Rec. UIT-T X.263 | ISO/CEI 9577;

204: IPI para IPv4 de la Rec. UIT-T X.263 | ISO/CEI 9577;

47: dos octetos siguientes soportados en modo GRE;

204: IPI para IPv4 de la Rec. UIT-T X.263 | ISO/CEI 9577;

129: IPI para CLNP de la Rec. UIT-T X.263 | ISO/CEI 9577.

Por consiguiente una AE-DCF OSI, IPv4 e IPv6 utilizará típicamente seis modos de encapsulación para indicar CLNP por IPv4, CLNP por IPv6, IPv4 por CLNS, IPv4 por IPv6, IPv6 por CLNS, e IPv6 por IPv4, lo que supone una longitud de valor de 20.

Este TLV no se incluirá en los LSP de seudonodo.

Una AE-DCF que no tenga direcciones IPv4 no deberá colocar formatos de encapsulación en su TLV de tipo 16 que contenga IPv4 como NLPID de transporte (exterior) de encapsulación hasta el momento en que se proporcione y anuncie una dirección IPv4.

Una AE-DCF que no tenga direcciones IPv6 no deberá colocar formatos de encapsulación en su TLV de tipo 16 que incluya IPv6 como NLPID de transporte (exterior) de encapsulación hasta el momento en que se proporcione y anuncie una dirección IPv6.

B.4.3.2 Proceso de reenvío

Como la AE-DCF no modifica el trayecto de los paquetes, una AE-DCF puede calcular un trayecto más corto para un paquete IP de modo que el siguiente salto sea un nodo exclusivamente OSI.

Cuando esto ocurra la AE-DCF no deberá limitarse a reenviar el paquete a un nodo adyacente que no soporte dicho tipo de protocolo de capa de red. Por el contrario, la AE-DCF deberá encapsular el paquete en un nuevo paquete de un tipo soportado por el próximo salto. El criterio para determinar si un nodo adyacente soporta o no un determinado protocolo de capa de red consiste en averiguar si el protocolo de capa de red figura en el TLV "protocolos soportados" de las PDU de saludo IS-IS recibidas del nodo de la adyacencia que constituya el salto siguiente para dicho destino.

Este nuevo paquete necesita un protocolo de capa de red, una dirección de destino y una dirección de origen para encapsular el paquete original:

– El protocolo de capa de red del nuevo paquete debe ser uno de los soportados por el próximo salto y definido en el TLV "protocolos soportados" de las PDU de saludo recibidas del siguiente salto.
– La dirección de destino del nuevo paquete debe coincidir con la identidad del siguiente nodo del trayecto más corto al destino original que haya transmitido un modo de encapsulación que tenga tanto el tipo de protocolo de capa de red del paquete original como el NLPID encapsulado (interior), y un protocolo de capa de red soportado por el siguiente salto (definido por el TLV "protocolos soportados" de las PDU de saludo recibidas del siguiente salto) como NLPID de transporte (exterior) encapsulado.
– Esto debe conseguirse por inspección del nuevo TLV de tipo 16 en los LSP recibidos de cada nodo del trayecto al destino, hasta que se encuentre uno que satisfaga dicho requisito.
– Cuando una AE-DCF inspeccione TLV del tipo 16, deberá ignorar cualquier subTLV que no entienda y saltar al siguiente subTLV prosiguiendo la inspección hasta que encuentre todos los modos de encapsulación que busca o hasta alcanzar el final del TLV.
– La dirección de origen del nuevo paquete debe ser igual a la identidad de la AE-DCF que construya el nuevo paquete encapsulado.

Si una AE-DCF puede reenviar un paquete sin encapsular porque el siguiente salto soporta dicho tipo de paquete, la AE-DCF debe reenviar el paquete sin encapsularlo.

Una AE-DCF podría enviar LSP con alcanzabilidad IP de un nodo exclusivamente IP a un nodo de pila dividida o viceversa, y podría exigírsele por consiguiente que encapsulara paquetes dirigidos a un nodo de pila dividida, o que encapsulara paquetes procedentes de un nodo de pila dividida.

Por consiguiente, un nodo de pila dividida con encapsulación automática debe ejecutar también el proceso de inspeccionar los LSP de los nodos entre el propio y el de destino y buscar un nodo que tenga un formato de encapsulación conveniente.

Obsérvese que un nodo de pila dividida podría ser capaz de recibir un paquete IPv4 sólo si estuviese encapsulado en CLNS, por ejemplo. En tal caso, el nodo de pila dividida transmitiría solamente "CLNS" en el campo "protocolos soportados" de sus paquetes de saludo, y sólo incorporaría un modo de encapsulación en el TLV de tipo 16 de sus LSP. El modo de encapsulación sencillo especificará IPv4 como NLPID del paquete encapsulado (interior) y CLNS como NLPID del paquete de transporte (exterior) encapsulado.

B.4.3.3 Proceso de recepción

Cuando una AE-DCF reciba un paquete destinado a ella misma, deberá inspeccionar dicho paquete para ver si hay otro paquete encapsulado en su interior. El paquete desencapsulado CLNS, IPv4 o IPv6 se reenviará a continuación con toda normalidad. Si el paquete desencapsulado resultante contuviese otro paquete destinado a este nodo se repetiría el proceso; esto se debe a que puede haber varias capas de encapsulación que requieran la desencapsulación en una única AE-DCF.

Los paquetes IS-IS no son compatibles con los paquetes IP, no pudiendo por tanto reenviarse por la Internet pública o por otras redes exclusivamente IP. Esto supone una ventaja en materia de seguridad ya que sería difícil que una entidad malintencionada lanzase remotamente paquetes IS-IS a nodos IS-IS o IS-IS integrados a través de la Internet pública. Así pues, para conservar esta ventaja si un paquete IS-IS o ES-IS llegase encapsulado en el interior de otro paquete destinado a una AE-DCF debería descartarse salvo que proviniese de un nodo con el que la AE-DCF tuviese un túnel proporcionado manualmente con IS-IS proporcionado para atravesarlo. Opcionalmente puede generarse un informe de errores para comunicar al gestor de la red información tal como la recepción y rechazo de un paquete, su origen, o eventos potencialmente maliciosos.

Todos los paquetes deben encapsularse utilizando la encapsulación GRE especificada en 7.1.8.

B.4.3.4 Tamaño de la MTU y requisitos de fragmentación

La encapsulación de un paquete en el interior de otro puede resultar en un nuevo paquete de mayor longitud que el tamaño de la MTU del enlace por el que deba reenviarse este nuevo paquete. Este nuevo paquete GRE no debe descartarse, por lo que no deben tener activado el bit No fragmentar si se trata de paquetes IPv4 y deben tener la bandera Segmentación permitida activada si se trata de paquetes CLNS de acuerdo con 7.1.8.

Por lo tanto, los paquetes de encapsulación resultantes deben fragmentarse antes de su reenvío cuando su longitud supere el límite de la MTU del enlace.

No es necesario fragmentar los paquetes antes de encapsularlos, ya que los paquetes de encapsulación resultantes se fragmentarán cuando sea necesario.

B.4.3.5 Requisitos para la AE-DCF con interfaces (LAN) de difusión

B.4.3.5.1 Proceso de elección de seudonodos

De acuerdo con 7.1.10.1.1 no se permite a los nodos exclusivamente IP formar adyacencias con nodos exclusivamente OSI, ni a los nodos exclusivamente IPv4 formar adyacencias con los nodos exclusivamente IPv6.

Por consiguiente cuando se conecten nodos exclusivamente IP y nodos exclusivamente OSI a la misma LAN y en la misma área de nivel 1 o subdominio de nivel 2, los nodos exclusivamente IP formarán adyacencias entre sí y elegirán un seudonodo mientras que los nodos exclusivamente OSI formarán adyacencias independientes y elegirán un seudonodo diferente. Por consiguiente, habrá dos seudonodos independientes en la LAN, uno para los nodos exclusivamente OSI y otro para los exclusivamente IP.

Algo similar puede ocurrir cuando haya nodos exclusivamente IPv4 y nodos exclusivamente IPv6 conectados a la misma LAN.

Por lo tanto, una AE-DCF debe participar por separado en estos procesos de elección de seudonodos independientes, en cada red que soporte. Una AE-DCF de nivel 1/nivel 2 debe participar en dos procesos de elección de seudonodos para cada protocolo de capa de red que soporte (uno para el nivel 1 y otro para el nivel 2).

Cada seudonodo de la LAN que resida en un nodo de un protocolo de capa de red compatible con la AE-DCF tendrá una adyacencia con la AE-DCF. Por consiguiente, en una LAN IP y OSI, la AE-DCF será justamente la que tenga adyacencias válidas tanto con el seudonodo IP como con el

OSI (de haber varios seudonodos en la LAN). La AE-DCF tendrá entonces una adyacencia con el seudonodo IP y con el seudonodo OSI, pero el seudonodo IP no tendrá una adyacencia directa con el seudonodo OSI y viceversa, sino que alcanzará su conectividad sólo a través de la AE-DCF, garantizándose de este modo que los paquetes CLNS son encapsulados por la AE-DCF antes de su reenvío a los nodos exclusivamente IP y que los paquetes IP son encapsulados por la AE-DCF antes de su reenvío a los nodos exclusivamente OSI.

Una AE-DCF con capacidad IP y OSI puede ser elegida como encaminador designado por los nodos de la LAN con capacidad IP, pero no por los nodos con capacidad OSI; en este caso, la AE-DCF debe crear un seudonodo, pero el seudonodo debe declarar adyacencias en sus LSP sólo con los nodos de la LAN con capacidad IP.

Análogamente una AE-DCF con capacidad IP y OSI puede ser elegida como encaminador designado por los nodos de la LAN con capacidad OSI, pero no por los nodos con capacidad IP; en este caso, la AE-DCF debe crear un seudonodo, pero este seudonodo debe declarar adyacencias en sus LSP sólo con los nodos de la LAN con capacidad OSI.

Una AE-DCF con capacidad IP y OSI puede ser elegida como encaminador designado tanto por los nodos de la LAN con capacidad IP como con los de capacidad OSI; en este caso, la AE-DCF debe crear un seudonodo que declare adyacencias en sus LSP con todos los nodos de la LAN.

Lo esencial, es que una AE-DCF participa en un proceso de elección independiente para cada protocolo de capa de red que soporte y, si gana cualquiera de las elecciones, crea un seudonodo, pero el seudonodo declarará adyacencias en sus LSP sólo con el conjunto o conjuntos de nodos que lo hayan elegido.

Por consiguiente, los nodos exclusivamente OSI o exclusivamente IP pueden recibir LSP de un seudonodo que liste adyacencias con nodos de la LAN con los que no tengan adyacencias. Si un paquete necesitase reenviarse a través de uno de estos nodos, debería enviarse al IS designado de acuerdo con ISO/CEI 10589 sección C.2.5 apartado "h", y con RFC 1195 sección C.1.4 paso 0 cláusula 8 en la página 73. Obsérvese que estas cláusulas de ISO/CEI 10589 y RFC 1195 no son normativas. Es posible que haya implementaciones que no exhiban este comportamiento. Estas implementaciones rechazarán paquetes en vez de enviar tráfico a una AE-DCF con encapsulación automática, si la AE-DCF es el encaminador designado, y si los nodos no compatibles en la misma LAN se encuentran en el trayecto más corto.

Por consiguiente, los implementadores y los operadores se enfrentan a la siguiente elección:

1) Otorgar a la prioridad de la AE-DCF un valor alto. Esto provocaría la aparición de un único seudonodo en la LAN, soportado por una AE-DCF. El inconveniente de esta solución es que hay pocas probabilidades de que exista una implementación tradicional en la LAN que no reenvíe tráfico a una AE-DCF si un nodo no compatible de la LAN se encuentra en el trayecto más corto.

o bien

2) Otorgar a la prioridad de la AE-DCF un valor bajo. Esto provocaría la aparición de un seudonodo en la LAN para cada protocolo de capa de red soportado, enviando explícitamente tráfico para los nodos no compatibles a través de una AE-DCF. Esto mejoraría la interoperabilidad aunque duplicaría la cantidad de LSP transmitidos por la LAN, reduciendo probablemente la escalabilidad.

Se recomienda que la prioridad de una AE-DCF sea configurable por el operador.

B.4.3.5.2 Proceso de actualización de los LSP

En ISO/CEI 10589, sección 7.3.15.1, se afirma que un LSP recibido que no provenga de una adyacencia válida, debe descartarse. Una implementación exclusivamente OSI estricta rechazará, por consiguiente, los LSP transmitidos a una interfaz LAN por un nodo exclusivamente IP, ya que

el nodo exclusivamente IP habría rechazado la adyacencia en virtud de 7.1.10.1.1. Por consiguiente el nodo exclusivamente OSI puede recibir dicho LSP únicamente si procede de una AE-DCF. Un nodo dual cuyo comportamiento no se haya modificado, sólo reenviaría dicho LSP durante la sincronización periódica de la base de datos LSP.

Por consiguiente, se requiere que una AE-DCF tenga un comportamiento de inundación de LSP modificado de modo que los nodos exclusivamente OSI o exclusivamente IP no necesiten esperar el siguiente evento de sincronización de la base de datos LSP.

Una AE-DCF debe comprobar los LSP entrantes que llegan a las interfaces de la LAN para ver si proceden de un vecino que soporte todos los protocolos de capa de red soportados por la AE-DCF. Esto debe realizarse por inspección del TLV "protocolos soportados" en los paquetes de saludo recibidos de dicho vecino.

Si el LSP procede de un vecino que no soporta todos los protocolos de capa de red soportados por la AE-DCF, ésta deberá comportarse con arreglo a ISO/CEI 10589 y desactivar la bandera SRM para dicho LSP en dicha interfaz LAN si ya tiene el LSP, o inundarlo desde todas las demás interfaces si todavía no tiene el LSP.

Si el LSP procede de un vecino que no soporta todos los protocolos de capa de red que soporta la AE-DCF, y si todavía no tiene el LSP, la AE-DCF deberá activar la bandera SRM para dicho LSP en la interfaz LAN en la que se recibió el LSP y en todas las demás interfaces, lo que se traducirá en la retransmisión, por parte de la AE-DCF, del LSP por la LAN.

De este modo si un nodo exclusivamente IP transmite un LSP por la LAN, una AE-DCF retransmitirá el LSP de modo que pueda llegar a nodos de la LAN exclusivamente OSI de una adyacencia válida y viceversa.

B.4.3.5.3 Reencaminamientos

Si una AE-DCF origina una petición de reencaminamiento ICMP, la petición no debe reencaminar paquetes IPv4 desde un nodo con capacidad IPv4 a un nodo sin capacidad IPv4. Análogamente si una AE-DCF origina PDU de reencaminamiento ISO/CEI 9542 , el reencaminamiento no debe afectar a los paquetes CLNS de un nodo con capacidad OSI a un nodo sin capacidad OSI.

B.4.3.5.4 Coexistencia en una LAN de nodos exclusivamente duales RFC 1195 y de encapsulación automática

Un nodo dual que cumpla RFC 1195, pero que no soporte una AE-DCF, no debe residir en una LAN en la misma área de nivel 1 o subdominio de nivel 2 que nodos exclusivamente IP y nodos exclusivamente OSI, ya que puede reenviar tráfico IP a un nodo exclusivamente OSI, o tráfico CLNS a un nodo exclusivamente IP, incurriendo en pérdida de paquetes. Ésta es una restricción topológica de RFC 1195.

Un nodo dual que cumpla RFC 1195, pero que no soporte una AE-DCF, puede residir en una LAN en la misma área de nivel 1 o subdominio de nivel 2 que una AE-DCF.

Además, puede residir en una LAN con un nodo exclusivamente OSI si puede reenviar tráfico exclusivamente CLNS a dicho nodo, con un nodo exclusivamente IPv4 si puede reenviar tráfico exclusivamente IPv4 a dicho nodo, o con un nodo exclusivamente IPv6 si puede reenviar tráfico exclusivamente IPv6 a dicho nodo.

B.4.4 Requisitos de los nodos de pila dividida de encapsulación automática

Un nodo de pila dividida inicia y termina paquetes de un tipo de protocolo de capa de red que no pueda reenviar nativamente por sus canales DCC. Por consiguiente, la única posibilidad de que dicho nodo pueda iniciar o terminar dichos paquetes es que éstos estén encapsulados.

Esta solución es especialmente útil para añadir una tarjeta IP a un nodo predominantemente OSI, o a un nodo que se instale en una red OSI existente, por ejemplo. Asimismo puede ser más fácil

actualizar un elemento de red de pasarela OSI a un nodo de pila dividida que a una AE-DCF dual, de modo que el tráfico IP pueda entrar y salir de la red de la que el nodo es pasarela.

El nodo de pila dividida debe poder encaminar íntegramente los paquetes que reciba correspondientes a un protocolo de capa de red igual a alguno de los listados en los TLV "protocolos soportados" de sus LSP IS-IS.

Un nodo de pila dividida debe utilizar el TLV "protocolos soportados" en las PDU de saludo IS-IS para indicar únicamente los protocolos de capa de red que puede recibir y reenviar de forma nativa a cualquier interfaz individual (o no soportar este TLV cuando se trate de una interfaz exclusivamente OSI).

O sea, un nodo IP-sobre-OSI puede encaminar CLNS de forma nativa por sus canales DCC y puede encaminar tráfico IP con destino a sí mismo en paquetes encapsulados GRE IP-sobre-OSI, o posiblemente por una interfaz Ethernet.

Por consiguiente un nodo de pila dividida puede indicar un protocolo de capa de red en el TLV "protocolos soportados" de los paquetes de saludo de una interfaz, y un protocolo de capa de red distinto en el TLV "protocolos soportados" de los paquetes de saludo en otra interfaz. Un nodo como éste podría encaminar ambos protocolos de capa de red internamente, anunciando por consiguiente ambos en el TLV "protocolos soportados" de sus LSP.

Un nodo de pila dividida debe utilizar TLV de alcanzabilidad IP en los LSP IS-IS para indicar el intervalo de direcciones de paquetes encapsulados que es capaz de terminar.

Un nodo de pila dividida puede recibir ampliaciones de alcanzabilidad IP de un nodo exclusivamente IP, a través de una AE-DCF dual. Por consiguiente el nodo de pila dividida debe poder enviar tráfico a un destino a través de una AE-DCF, utilizándola para encapsular sus paquetes. Para llevar esto a cabo el nodo de pila dividida debe buscar el siguiente nodo del trayecto hacia cada destino capaz de desencapsulación, o un destino de pila dividida, del mismo modo que lo hace la AE-DCF.

Un nodo de pila dividida de encapsulación automática anunciará los modos de encapsulación que soporta por medio del TLV Capacidad de encapsulación de conformidad con B.4.3.1.

Cuando un nodo de pila dividida reciba un paquete destinado a sí mismo, deberá inspeccionar dicho paquete para ver si hay otro paquete encapsulado en su interior En tal caso, el paquete se procesará internamente, salvo que se trate de un paquete IS-IS o ES-IS en cuyo caso deberá descartarse (salvo que exista un túnel proporcionado manualmente con IS-IS proporcionado para atravesarlo) del mismo modo que ocurriría con un AE-DCF dual.

Al igual que la AE-DCF dual, un nodo de pila dividida debe soportar la encapsulación GRE como se especifica en 7.1.8.

B.4.5 Utilización de nodos IP que no se ajustan a 7.1.10.1.1, con AE-DCF

Los nodos exclusivamente IPv4 o IPv6 que no se ajusten a RFC 1195, pero que no soporten la función de creación de adyacencias consciente del protocolo especificada en 7.1.10.1.1, pueden utilizarse en la misma área de nivel 1 mixta o subdominio de nivel 2 mixto que una AE-DCF, pero el gestor de red debe controlar manualmente que dicho nodo no tenga adyacencias con otros nodos que pudieran reenviarle paquetes que no soporta.

B.4.6 Utilización de nodos duales sin AE-DCF y de nodos duales con AE-DCF en la misma área IS-IS

Los nodos duales que cumplan RFC 1195, pero que no soporten AE-DCF, pueden utilizarse en áreas de nivel 1 mixtas y en subdominios de nivel 2 mixtos con una AE-DCF, con las restricciones siguientes:

Los nodos IS-IS integrados (o agrupaciones de nodos) que soporten más de un protocolo de capa de red pero que no soporten una AE-DCF siguen estando sometidos a las restricciones topológicas de RFC 1195. Esto significa que el gestor de red debe verificar que dicho nodo no puede reenviar paquetes a un nodo vecino que no pueda reenviar dicho tipo de paquetes.

Por lo tanto se entiende por dual un nodo IS-IS integrado dual que cumpla RFC 1195 pero que no contenga una AE-DCF.

OSI-AEDCF-dual-AEDCF-IP es una combinación segura;

OSI-AEDCF-dual-dual-dual-AEDCF-IP es una combinación segura;

IPv4-AEDCF-dual IPv4&IPv6-AEDCF-IPv6 es una combinación segura;

dual-AEDCF-OSI-AEDCF-dual es una combinación segura;

OSI-IPv4&OSIAEDCF-dual IPv4&OSI-dual IPv4&IPv6-IPv4&IPv6 AEDCF-IPv6 no es una combinación segura;

OSI-IPv4&OSIAEDCF-dual IPv4&OSI-IPv4&IPv6&OSI-dual IPv4&IPv6-IPv4&IPv6 AEDCF-IPv6 no es una combinación segura.

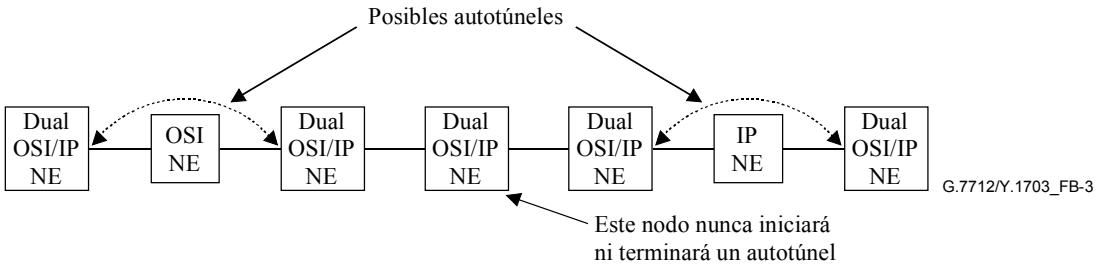


Figura B.3/G.7712/Y.1703 – Requisitos topológicos para nodos duales de área IS-IS

B.4.7 Requisitos de los nodos de nivel 1 y nivel 2

Se recomienda que los nodos que soporten tanto el encaminamiento de nivel 1 como el de nivel 2, y que se encuentren en un área en que se utilicen estas AE-DCF:

– Soporten todos los protocolos de capa de red presentes en el nivel 1 y en el subdominio de nivel 2 en los que participe el nodo y soporten una AE-DCF.

o

– Soporten todos los protocolos de capa de red presentes tanto en el nivel 1 como en el subdominio de nivel 2 en los que participe el nodo y estén o bien directamente conectados o conectados mediante cadenas continuas de otros nodos que soporten todos los protocolos de capa de red en el área, a nodos que soporten una AE-DCF y que soporten todos los protocolos de capa de red en el área.

Por tanto, se entiende por dual un nodo IS-IS integrado que cumpla RFC 1195 pero que no soporte una AE-DCF:

Subdominio L2-dual L1/L2-no dual es seguro (de acuerdo con RFC 1195);

Subdominio L2-dual L1/L2-dual-dual-no dual es seguro (de acuerdo con RFC 1195);

Subdominio L2-dual L1/L2-AE-DCF-red mixta es seguro;

Subdominio L2-dual L1/L2-dual-dual-AE-DCF-red mixta es seguro;

Subdominio L2-dual L1/L2-no dual-dual no es seguro (salvo que se apliquen las restricciones de RFC 1195);

Subdominio L2-dual L1/L2-no dual-AE-DCF no es seguro (salvo que se apliquen las restricciones de RFC 1195).

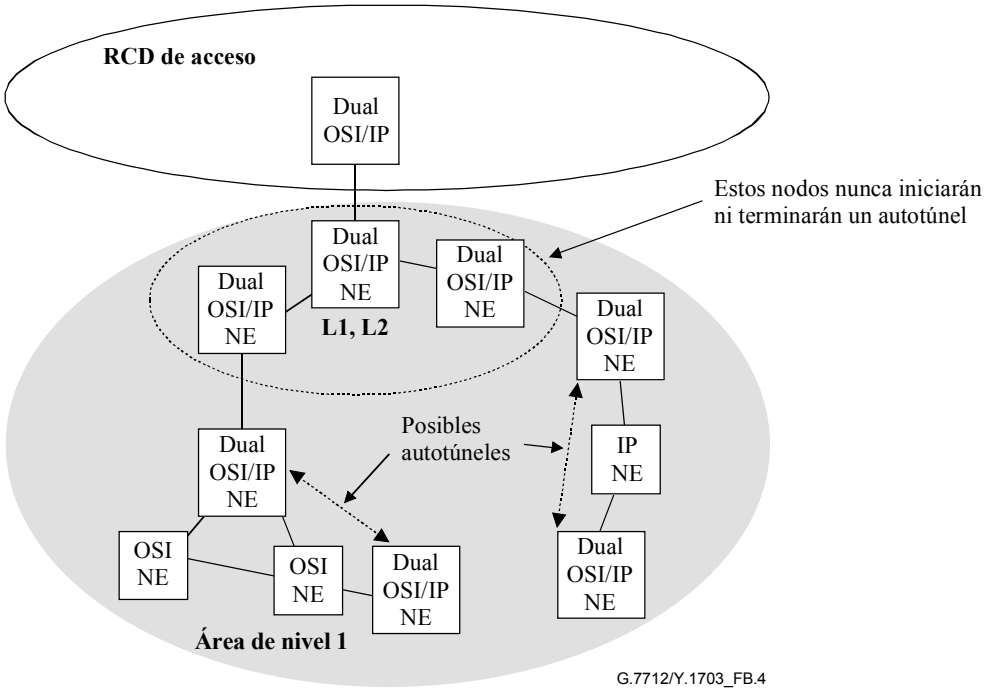


Figura B.4/G.7712/Y.1703 – Requisitos para los nodos de nivel 1 y nivel 2

No obstante, se entiende que un elemento de red pasarela, y por consiguiente un encaminador L1, L2, pueda ser un dispositivo existente exclusivamente OSI. En este caso es posible tener IP y encapsulación automática en el área utilizando el siguiente método, con precaución:

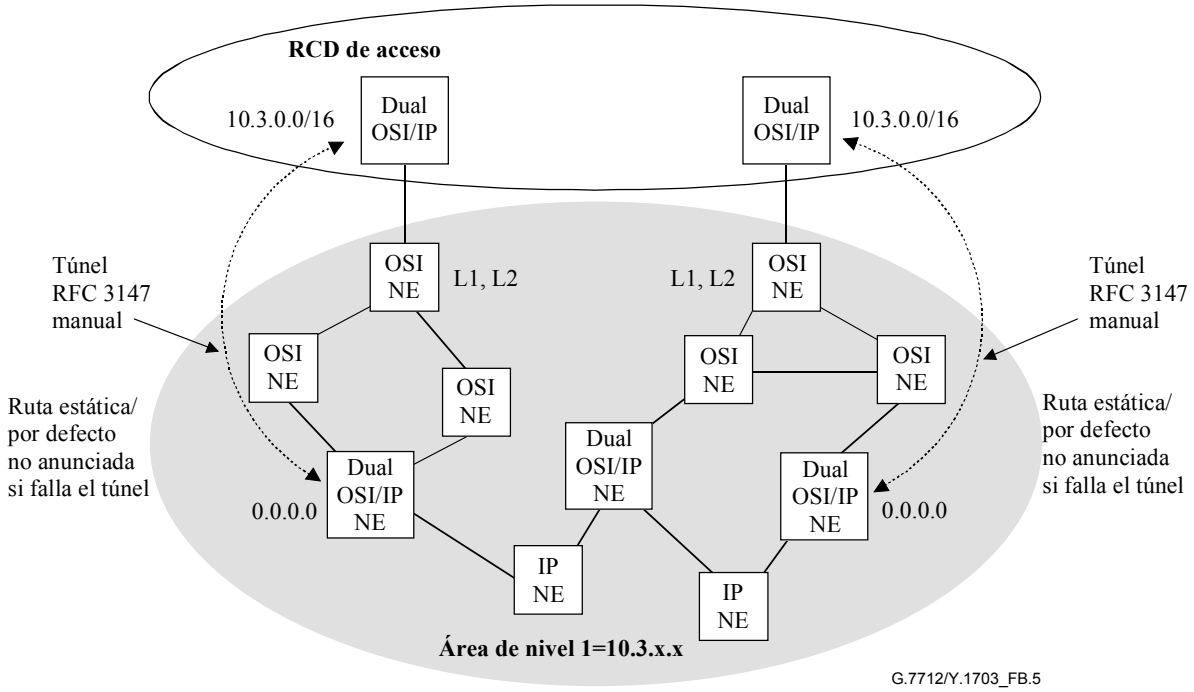


Figura B.5/G.7712/Y.1703 – Utilización de un dispositivo exclusivamente OSI como pasarela

Pueden escogerse uno o más nodos duales del área como pasarelas para los paquetes IP. Estos nodos se configurarán para anunciar una ruta por defecto (0.0.0.0) hacia el área, para atraer todo el tráfico IP de "fuera del área" hacia ellos. A continuación estos nodos reenviarán todo el tráfico de "fuera del área" a través de un túnel GRE proporcionado manualmente, que atraviese el nodo exclusivamente OSI de nivel 2, nivel 1 hacia otro nodo dual exterior al área.

El nodo dual exterior al área debe tener un prefijo proporcionado manualmente para atraer todo el tráfico IP destinado al área y enviarlo por el túnel hacia el área. Opcionalmente, puede proporcionarse un mecanismo, tal como un protocolo de encaminamiento IP, a través del túnel de modo que cada extremo pueda ver si el otro está vivo; no obstante, si se utiliza IS-IS integrado, debe ser un ejemplar de encaminamiento distinto al utilizado normalmente en el área, ya que se trata realmente de un dominio de encaminamiento diferente.

Si se utiliza tal mecanismo y desaparece el extremo lejano, el nodo dual interior al área debe dejar de anunciar la ruta por defecto, y el nodo dual exterior al área debe dejar de anunciar el prefijo que representa los nodos del área. De este modo, pueden proporcionarse pasarelas IP redundantes.

Obsérvese que RFC 1195 afirma que las rutas por defecto no deben anunciarse en LSP de nivel 1. Esta solución requiere el incumplimiento de esta regla. Normalmente un nodo RFC 1195 de nivel 1 consideraría a un nodo nivel 1, nivel 2 como su ruta por defecto. Esta solución requiere que este comportamiento se modifique por la recepción de un anuncio de ruta por defecto en un LSP de nivel 1. Si esto no fuera posible se debe configurar una alternativa para los nodos pasarela IP con una selección de rutas estáticas que cubran todos los destinos posibles de "fuera del área" que una pila IP del área pueda intentar alcanzar.

B.4.8 Requisitos del subdominio de nivel 2

Resulta admisible encaminar todos los protocolos presentes de forma nativa en el subdominio de nivel 2, con arreglo a RFC 1195, en cuyo caso ninguno de los nodos de nivel 2 necesita soportar una AE-DCF, aunque todos ellos deben soportar todos los protocolos de capa de red presentes.

Alternativamente resulta admisible utilizar nodos de nivel 2 que no soporten todos los protocolos de capa de red presentes en el dominio, en cuyo caso se requiere que los nodos de nivel 2 duales o plurilingües soporten una AE-DCF de modo que los paquetes puedan encapsularse automáticamente para poder atravesar dichos nodos.

Apéndice I[2]

Restricciones de las funciones de interfuncionamiento en la RCD

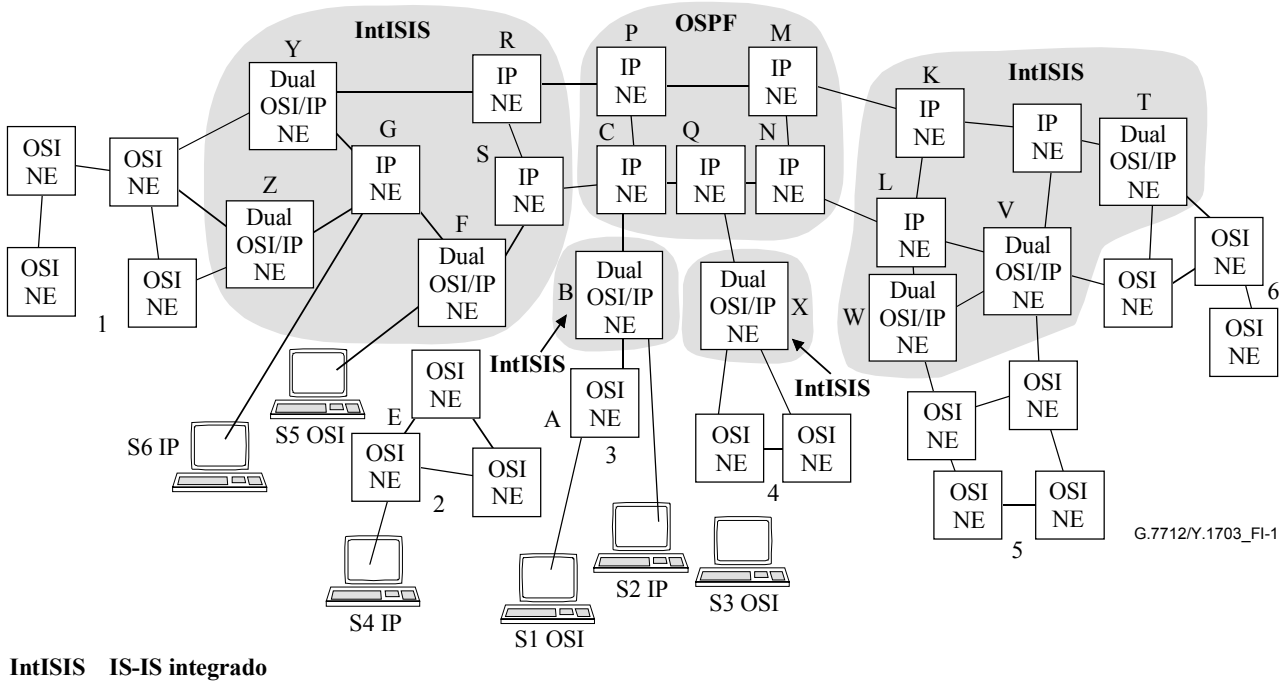


Figura I.1/G.7712/Y.1703 – Casos de interfuncionamiento

I.1 Hipótesis generales:

La RCD cubre la IWF para la capa 2-3 de las pilas IP-OSI. Los mecanismos de interfuncionamiento aplicables a otras capas (es decir la mediación) no son objeto de la presente Recomendación.

Véase en 7.1.7 la definición de interfuncionamiento.

Los túneles se basan en RFC.

Los elementos de red exclusivamente IP soportan el encaminamiento IP y pueden contener redistribución entre IS-IS integrado y OSPF.

I.2 Común para todos los casos

El encaminamiento dinámico se consigue gracias a la utilización de redistribución de rutas de información de direcciones IP entre los elementos de red OSPF e IS-IS. La redistribución de rutas tiene lugar en los nodos OSPF entre los pares (R,P), (S,C), (M,K) y (N,L).

I.2.1 Caso 1: Sistema de gestión basado en OSI conectado a un nodo A

Debe haber como mínimo un túnel configurado de B a uno o más de Y o Z.

Debe haber un túnel configurado de B a X.

Debe haber un túnel configurado de B a F.

Debe haber como mínimo un túnel configurado de B a uno o más de W, V o T.

---

[2] NOTA – Este nuevo apéndice I sustituye al de la Rec. UIT-T G.7712/Y.1703 de 2001.

Los anteriores túneles tendrán probablemente IS-IS atravesándolos (en el interior del túnel), no obstante, las técnicas de encaminamiento interdominios también constituyen una posibilidad. En ciertas condiciones algunos túneles podrían congestionarse como resultado de las opciones de encaminamiento.

Un sistema de gestión basado en OSI dispone ahora de conectividad CLNS con cualquier elemento de red exclusivamente OSI o de pila dual de la red, pero no tiene conectividad con elementos de red exclusivamente IP. Aunque un gestor basado en OSI pueda enviar paquetes CLNS a un elemento de red de pila dual, no podrá gestionarlo salvo que sea susceptible de gestión OSI.

I.2.2 Caso 2: Sistemas de gestión basado en IP conectados a un nodo B

En esta red específica, el tráfico IP puede reenviarse de B a todos los elementos de red IP sin requerir de túneles. Los elementos de red OSPF P, C, M, y N deben soportar la redistribución de rutas IP en IS-IS integrado. Será necesario configurar filtros en los nodos OSPF P, C, M, y N a fin de impedir la formación de bucles de encaminamiento.

Un sistema de gestión basado en IP tiene ahora conectividad IP con cualquier elemento de red exclusivamente IP o de pila dual que exista en la red, pero no tiene conectividad con los elementos de red exclusivamente OSI. Aunque un gestor basado en IP pueda enviar paquetes IP a un elemento de red de pila dual, no podrá gestionarlo salvo que sea susceptible de gestión IP.

I.2.3 Caso 3: Sistemas de gestión basados en OSI conectados a un nodo C

El elemento de red C no puede proporcionar conectividad OSI y por consiguiente los paquetes CLNS no pueden reenviarse, por lo tanto el sistema de gestión basado en OSI no puede funcionar en esta posición.

I.2.4 Caso 4: Sistemas de gestión basados en IP conectados a un nodo E

El elemento de red E no puede proporcionar conectividad IP y por consiguiente los paquetes IP no pueden reenviarse, por lo tanto un sistema de gestión basado en IP no puede funcionar en esta posición.

I.2.5 Caso 5: Sistemas de gestión basados en OSI conectados al nodo F

El tráfico CLNS puede pasar a través del elemento de red F a la red 2 OSI sin necesidad de túneles ya que el elemento de red F puede reenviar paquetes CLNS en modo nativo.

Debe haber un túnel configurado de F a B.

Debe haber como mínimo un túnel configurado de F a uno o más de Z o Y.

Debe haber un túnel configurado de F a X.

Debe haber como mínimo un túnel configurado de F a uno o más de W, V o T.

Los mencionados túneles tendrán probablemente IS-IS atravesándolos (dentro del túnel), no obstante, las técnicas de encaminamiento interdominio constituyen asimismo una posibilidad. En ciertas condiciones algunos túneles podrían congestionarse como resultado de las opciones de encaminamiento.

Un sistema de gestión basado en OSI tiene ahora conectividad CLNS con cualquier elemento de red exclusivamente OSI o de pila dual que exista en la red, pero no tiene conectividad con los elementos de red exclusivamente IP. Aunque un gestor basado en OSI pueda enviar paquetes CLNS a un elemento de red de pila dual, no podrá gestionarlo salvo que sea susceptible de gestión OSI.

I.2.6 Caso 6: Sistemas de gestión basados en IP conectados a un nodo G

En esta red específica, el tráfico IP puede reenviarse de G a todos los elementos de red IP sin necesidad de túneles. Los elementos de red OSPF P, C, M, y N deben soportar la redistribución de

rutas IP hacia IS-IS integrado. Habrá que configurar filtros en cada uno de los nodos OSPF P, C, M, y N a fin de impedir la formación de bucles de encaminamiento.

Un sistema de gestión basado en IP tiene ahora conectividad con cualquier elemento de red exclusivamente IP o de pila dual que exista en la red, pero no tiene conectividad con los elementos de red exclusivamente OSI. Aunque un gestor basado en IP pueda enviar paquetes IP a un elemento de red de pila dual no podrá gestionarlo salvo que sea susceptible de gestión IP.

Apéndice II

Ejemplo de implementación de la encapsulación automática

II.1 Introducción

Este apéndice no constituye un requisito sino un ejemplo que bosqueja cómo puede implementarse un nodo en relación con un aspecto de las características especificadas en esta Recomendación.

La manera más sencilla (aunque no la única) de que un nodo calcule el siguiente nodo a lo largo del trayecto más corto hacia el destino final de un paquete que pueda desencapsular es modificar el algoritmo SPF a tal efecto.

El algoritmo puede modificarse para encontrar el siguiente nodo del trayecto más corto hacia el destino que pueda aceptar tráfico IP encapsulado por OSI, y el siguiente nodo del trayecto más corto hacia el destino que pueda aceptar tráfico OSI encapsulado por IP. Obsérvese que éstos pueden ser el mismo nodo o bien dos nodos independientes. Más adelante se facilita un algoritmo Dijkstra modificado a este propósito.

Este proceso adicional sólo necesita ejecutarse cuando el siguiente salto no soporte el protocolo de capa de red del tipo que corresponda a la dirección de destino para dicho trayecto. Si el siguiente salto soporta dicho tipo de protocolo de capa de red (especificado en el TLV "protocolos soportados" presente en las PDU de saludo IS-IS procedentes de dicho nodo), puede bastar con reenviar los paquetes dirigidos hacia dicho destino de forma nativa sin más, de modo que la búsqueda de un nodo del trayecto que pueda desencapsular ya no es necesaria.

A continuación, el algoritmo debe identificar una dirección IP para el siguiente nodo de desencapsulación si el destino del trayecto es un sistema de extremo OSI, o una dirección OSI para el siguiente nodo de desencapsulación si el destino del trayecto es una dirección IP.

Si no se pudiera encontrar una dirección IP para este siguiente nodo de desencapsulación se señalaría un error de configuración en dicho nodo (sin dirección IP); esto podría provocar el envío opcional de un mensaje de error al administrador de la red. Si un paquete CLNS requiriese el envío por túnel a dicho nodo por IP se produciría pérdida de paquetes, ya que no es posible la encapsulación sin una dirección de destino IP, descartándose el paquete en este caso.

Si no se pudiera encontrar un nodo con capacidad de desencapsulación, se señalaría un error de diseño de la red, más específicamente la inobservancia de las restricciones topológicas declaradas en esta Recomendación. Esto generaría el informe de errores "destino inalcanzable".

Para cada destino IP que requiera de encapsulación para superar el siguiente salto, el nodo puede colocar un marcador en el cuadro de reenvíos IP indicando la dirección de destino OSI que debe utilizarse para encapsular todos los paquetes IP con destino a dicha dirección.

Para cada destino OSI que requiera de encapsulación para superar el siguiente salto, el nodo puede poner un marcador en el cuadro de reenvíos OSI indicando la dirección de destino IP que debe utilizarse para encapsular todos los paquetes OSI con destino a dicha dirección.

Un nodo que soporte IPv4, IPv6 y OSI puede encontrar dos direcciones (por ejemplo, una dirección IPv4 y otra IPv6) que podrían utilizarse para la encapsulación. En tal caso puede escoger cualquiera de ellas siempre que se genere un paquete que sea de un tipo de protocolo de capa de red soportado por el siguiente salto (el especificado en el TLV "protocolos soportados" de las PDU de saludo IS-IS procedentes de dicho nodo).

II.2 Actualizaciones del algoritmo de Dijkstra

Las siguientes cláusulas contienen el algoritmo de Dijkstra completo incluidas las ampliaciones para soportar la tunelización automática. Se basa en el algoritmo especificado en RFC 1195. El algoritmo presentado es adecuado para un nodo dual con encapsulación automática IPv4 y CLNS. Las modificaciones del algoritmo se muestran en ***cursiva y negrita***.

El algoritmo genera una base de datos PATHS (*trayectos*) que contiene, para cada uno de los destinos, la identidad del primer nodo de S a N capaz de desencapsular IP sobre OSI, y la identidad del primer nodo de S a N capaz de desencapsular OSI sobre IP.

Para cada uno de los destinos IP, el primer nodo de S a N capaz de desencapsular IP sobre OSI puede tener su dirección OSI cargada en el cuadro de reenvíos IP como dirección de destino a utilizar en cualquier paquete CLNP utilizado para encapsular IP sobre OSI, si el siguiente salto no soporta IP.

Para cada sistema de extremo OSI, el primer nodo de S a N capaz de desencapsular OSI sobre IP puede tener una de sus direcciones IP cargada en el cuadro de reenvíos OSI como dirección de destino a utilizar en cualquier paquete IP utilizado para encapsular OSI sobre IP, si el siguiente salto no soporta OSI.

II.2.1 Modificaciones de la base de datos

La base de datos PATHS y TENTS debe actualizarse para dar cabida a una ampliación del elemento {Adj(N)} de la tríada. El elemento N de la adyacencia contendrá dos entradas de Soporte de protocolo dual (IDP(N)-ODP(N)) que representarán el ID del sistema del primer encaminador dual del trayecto de S a N capaz de desencapsular paquetes IP tunelizados sobre OSI (IDP(N)) y el ID del sistema del primer encaminador dual del trayecto S a N capaz de desencapsular paquetes OSI tunelizados sobre IP (ODP(N). Si no existiera un encaminador *DP(N) en el PATH este valor se pondría a cero. Cuando existan varias entradas Adj(N) en la base de datos TENTS o en la PATHS, cada adyacencia tendrá sus correspondientes entradas *DP(N). Por consiguiente cada tríada tendrá el formato <N,d(N),{Adj(N)-IDP(N)-ODP(N)}>.

Si el valor de IDP(N) se pone a 0, significa que no existe ningún encaminador dual en el trayecto hacia el destino capaz de desencapsular y encapsular paquetes IP sobre OSI.

Si el valor de ODP(N) se pone a 0, significa que no existe ningún encaminador dual en el trayecto hacia el destino capaz de desencapsular y encapsular paquetes OSI sobre IP.

II.2.2 Modificaciones al algoritmo

El algoritmo SPF especificado en la sección C.1.4 de RFC 1195 se modifica quedando del siguiente modo:

```
Paso 0: Inicializar TENT y PATHS vaciándolos. Inicializar la longitud de la tríada
provisional (tentlength) a
[internalmetric=0, externalmetric=0].
...

    (tentlength es la longitud del trayecto (pathlength) de los elementos de TENT objeto
    de examen.)


    1) Añadir a PATHS <SELF,0,W-0-0>, siendo W un valor especial que indica que el
       tráfico hacia SELF se desvía a procesos internos (en vez de reenviarse).
```

2) Precargar ahora TENT con la base de datos de adyacencias locales (cada entrada de TENT debe marcarse como correspondiente o bien a un sistema de extremo o bien a un encaminador, para poder efectuar correctamente la comprobación al final del paso 2 – obsérvese que cada entrada de alcanzabilidad IP local se incluye como adyacencia, y se marca como correspondiente a un sistema de extremo. Para cada adyacencia Adj(N) (incluidas las adyacencias manuales OSI de nivel 1, o las direcciones alcanzables activadas por OSI de nivel 2, y las entradas de alcanzabilidad IP) en los circuitos activados, con el sistema N de SELF en estado "activo" calcular:

   d(N) = costo del circuito padre de la adyacencia (N), obtenido de metric.k , siendo k = uno de {métrica por defecto, métrica monetaria, métrica de error}

   Adj(N)***-IDP(N)- ODP(N)*** = número de adyacencia de la adyacencia con N***, el SID del encaminador del siguiente salto en el trayecto al vecino capaz de desencapsular paquetes IP sobre OSI y el SID del encaminador del siguiente salto en el trayecto al vecino capaz de desencapsular paquetes OSI sobre IP. En este caso, es decir durante la inicialización, ambos valores DP se pondrán a 0***

3) Si una tríada <N,x,{Adj(M)***-IDP(N)-ODP(N)***}> está en TENT, entonces:

   Si x = d(N), entonces {Adj(M)***-IDP(N)-ODP(N)***} <--- {Adj(M)***-IDP(M)-ODP(M)***}
   U {Adj(N)***-IDP(N)-ODP(N)***}.

4) Si N es una entrada de encaminador o de sistema de extremo OSI y hay en este momento más adyacencias en {Adj(M)} que maximumPathSplits, suprimir las adyacencias sobrantes como se explica en la cláusula 7.2.7 de ISO/CEI 10589. Si N es una entrada de alcanzabilidad IP, pueden suprimirse las adyacencias sobrantes sin problemas. Esto no afectará a la corrección del encaminamiento, aunque puede eliminar el determinismo de las rutas IP (es decir los paquetes IP seguirán utilizando las rutas óptimas de un área, pero cuando existen varias rutas de la misma calidad, no seguirán exactamente la ruta que un encaminador concreto hubiera previsto.

5) Si x < d(N), no hacer nada.

6) Si x > d(N), suprimir <N,x,{Adj(M)***-IDP(M)-ODP(M)***}> de TENT y añadir la tríada <N,d(N),{Adj(N) ***-IDP(N)-ODP(N)***}>.

7) Si no hay ninguna tríada <N,x,{Adj(M)***-IDP(M)-ODP(M)*** }> en TENT, añadir <N,d(N),{Adj(N)***-IDP(N)-ODP(N)***}> to TENT.

8) Añadir ahora los sistemas con los que el encaminador local no tenga adyacencias pero mencionados en los LSP del seudonodo vecino. Se otorga a la adyacencia para estos sistemas el valor del encaminador designado. Obsérvese que esto no incluye las entradas de alcanzabilidad IP de los LSP del seudonodo vecino. En particular, los LSP de seudonodo no incluyen entradas de alcanzabilidad IP.

9) Para todos los circuitos de difusión en estado "activo", averiguar el LSP del seudonodo para dicho circuito (específicamente el LSP número cero y con los 7 primeros octetos de LSPID igual a LnCircuitID para dicho circuito, siendo n igual a 1 (para el encaminamiento de nivel 1) ó 2 (encaminamiento de nivel 2). Si existe, para todos los vecinos N informados en todos los LSP de este seudonodo que no existan en TENT añadir una entrada <N,d(N),{Adj(N) ***-IDP(N)-ODP(N)***}> a TENT, siendo:

   d(N) = metric.k del circuito.
   Adj(N) = número de adyacencia de la adyacencia con el DR.

10) Ir al paso 2.

Paso 1: Examinar la PDU de estado de enlace número cero de P, el sistema recién colocado en PATHS (es decir, el LSP cuyos 7 primeros octetos coincidan con el LSPID de P, y número de LSP igual a cero).

1) Si existe este LSP y el bit "Costo infinito de encaminamiento por sistemas intermedios" está desactivado para cada par Adj(*) – IDP(*) – ODP(*) de la base de datos PATHS para P. Si este LSP no es de un seudonodo y si IDP(*) es igual a cero entoncescomprobar el campo de capacidad de desencapsulación del LSP, si soporta IPsobre OSI entonces fijar como valor IDP(P) para esta adyacencia el ID del

sistema de P. Si ODP(*) es igual a cero entonces comprobar el campo de capacidad dedesencapsulación del LSP, si soporta OSI sobre IP entonces hacer el valor IDP(P)para esta adyacencia igual al ID de sistema de P.

2) Si existe este LSP, y el bit "Costo infinito de encaminamiento por sistemas intermedios" está desactivado, entonces para cada LSP de P (es decir para todos los LSP con los mismos 7 primeros octetos de LSPID y P, independientemente del valor del número de LSP) calcular:

dist(P,N) = d(P) + metric.k(P,N)

para cada vecino N (tanto de sistema de extremo como de encaminador) del sistema P. Si el bit "Costo infinito de encaminamiento por sistemas intermedios" está activado, considerar únicamente los vecinos de sistema extremo del sistema P.

Obsérvese que entre los vecinos de sistema extremo del sistema P se encuentran las entradas de direcciones alcanzables IP incluidas en los LSP del sistema P. Aquí, d(P) es el segundo elemento de la tríada

<P,d(P),{Adj(P)***-IDP(P)-ODP(P)***}>

y metric.k(P,N) es el costo del enlace de P a N informado en la PDU de estado de enlace de P.

3) Si dist(P,N) > MaxPathMetric, no hacer nada.

4) Si <N,d(N),{Adj(N) ***– IDP(N)-ODP(N)***}> se encuentra en PATHS, no hacer nada.

NOTA – d(N) debe ser menor que dist(P,N), o de lo contrario N no habría sido colocado en PATHS. Puede efectuarse aquí una comprobación de seguridad adicional para garantizar que d(N) es realmente menor que dist(P,N)

5) Si una tríada <N,x,{Adj(N) ***-IDP(N)-ODP(N)***}> está en TENT, entonces:

a) Si x = dist(P,N), entonces {Adj(N)***, IDP(N)-ODP(N)***} <-- Adj(N) **-IDP(N)-ODP(N)**} U {Adj(P) ***-IDP(P)-ODP(N)***}.
Obsérvese que aunque el valor de Adj(N) sea igual al valor Adj(P), los valores correspondientes de IDP(P) o bien de ODP(P) y de IDP(N) o bien de ODP(N) son diferentes así pues, esto debería tratarse como una adyacencia distinta y representar un trayecto diferente hacia el destino.

b) Si N es un encaminador o un sistema de extremo OSI, y hay en este momento más adyacencias en {Adj(N)} que maximumPath Splits, suprimir las adyacencias sobrantes, como se explica en la cláusula 7.2.7 de ISO/CEI 10589. Para las entradas de alcanzabilidad IP, pueden suprimirse las adyacencias sobrantes sin problemas. Esto no afectará a la corrección del encaminamiento, aunque podría suprimir el determinismo de las rutas IP (es decir, los paquetes IP seguirán transportándose por las rutas óptimas de un área, pero cuando existan varias ç rutas de igual calidad, no seguirán forzosamente la misma ruta que cualquier encaminador particular habría previsto)

c) Si x < dist(P,N), no hacer nada.

d) Si x > dist(P,N), suprimir <N,x,{Adj(N)***- IDP(N)-ODP(N)***}> de TENT, y añadir <N,dist(P,N),{Adj(P)***- IDP(P)-ODP(P)***}>

6) Si no hay tríada <N,x,{Adj(N)}> en TENT, entonces añadir <N,dist(P,N),{Adj(P)}> to TENT.

Paso 2: Si TENT está vacía, parar. De lo contrario:

1) Encontrar el elemento <P,x,{Adj(P)***-IDP(P)-ODP(P)***}>, con la x mínima del siguiente modo:

a) Si un elemento <*,tentlength,*> permanece en TENT en la lista de tentlength, escoger dicho elemento. Si hay más de un elemento en la lista para tentlength, escoger uno de los elementos (de haberlos) para un sistema que sea un seudonodo con preferencia a uno que no lo sea. Si no hay más elementos en la lista para tentlength, incrementar tentlength y repetir el paso 2.

b) Suprimir <P,tentlength,{Adj(P)***-IDP(P)-ODP(P)***}> de TENT.

c) Añadir <P,d(P),{Adj(P) ***-IDP(P)-ODP(P)***}> a PATHS.

d) Si ésta es la ejecución del proceso de decisión de nivel 2 y el sistema recién añadido a PATHS figura como sistema intermedio de nivel 2 designado de la partición, añadir además <AREA.P,d(P),{Adj(P)}> a PATHS, siendo AREA.P el título de la entidad de red del otro extremo del enlace virtual, obtenido tomando la primera AREA listada en el LSP de P y añadiéndole el ID de P.

e) Si el sistema recién añadido a PATHS es un sistema de extremo, ir al paso 2. De lo contrario ir al paso 1.

NOTA – En el contexto de nivel 2, los "sistemas de extremo" son el conjunto de prefijos de direcciones alcanzables (para OSI), el conjunto de direcciones de área con costo cero (también para OSI), más el conjunto de entradas de alcanzabilidad IP (incluidas las externas y las internas).

Apéndice III

Guía de puesta en servicio de los elementos de red SDH en un entorno RFC 1195 dual y repercusión de la opción de encapsulación automática

III.1 Introducción

Este apéndice ofrece consejos sobre la instalación de nodos IS-IS integrados en una red dual IPv4 y OSI, y la utilización de la característica de encapsulación automática opcional descrita en el anexo B.

III.2 IS-IS integrado sin encapsulación automática

III.2.1 Introducción y reglas de RFC 1195

El IS-IS integrado, especificado en RFC 1195, se escribió originalmente como protocolo de encaminamiento dual. Específicamente, se escribió para poder encaminar tanto IPv4 como CLNP por medio de un sencillo cálculo SPF, un conjunto sencillo de métricas tanto para IP como CLNP, y un conjunto sencillo de saludos y LSP.

Más específicamente, los encaminadores IS-IS integrados que cumplen RFC 1195 calculan los trayectos más cortos a través de un área de nivel 1 o subdominio de nivel 2 sin considerar si algunos de los encaminadores candidatos puede reenviar realmente un tipo específico de paquete.

Esto se expresa con claridad en la sección 3.10 de RFC 1195:

– "El cálculo de Dijkstra no tiene en cuenta si el encaminador es exclusivamente IP, exclusivamente OSI o dual. Las restricciones topológicas especificadas en el punto 1.4 garantizan que los paquetes IP sólo se enviarán a través de encaminadores con capacidad IP, mientras que los paquetes OSI sólo se enviarán a través de encaminadores con capacidad OSI."

Con IS-IS integrado, un encaminador es simplemente un encaminador. La hipótesis consiste en que cualquier encaminador de la red puede manejar cualquier tipo de paquetes que se le envíe.

Por consiguiente los encaminadores IS-IS integrados calculan las rutas y reenvían paquetes con arreglo a esta hipótesis, siendo responsabilidad del operador verificar que la hipótesis es realmente cierta.

Así pues, hay restricciones topológicas en RFC 1195. Si no se respetan las restricciones topológicas de RFC 1195 se puede incurrir en pérdida de paquetes, ya que éstos desaparecerían en el agujero

negro de un encaminador que se limitase a descartar los paquetes que no pudiera reenviar por no soportarlos.

En una sencilla red de área única de nivel 1, las reglas son elementales. A saber:

1) Si hay que reenviar paquetes IPv4 en un área, todos los encaminadores del área deben ser capaces de reenviar paquetes IPv4.
2) Si hay que reenviar paquetes CLNP en un área, todos los encaminadores del área deben ser capaces de reenviar paquetes CLNP.
3) Si hay que reenviar paquetes tanto IPv4 como paquetes CLNP en un área, todos los encaminadores del área deben ser duales, es decir ser capaces de reenviar ambos.

Por consiguiente resulta bastante fácil clasificar las áreas de nivel 1 IS-IS en las clases "área exclusivamente OSI", "área exclusivamente IP", y "área dual". Esto se muestra en la figura III.1.

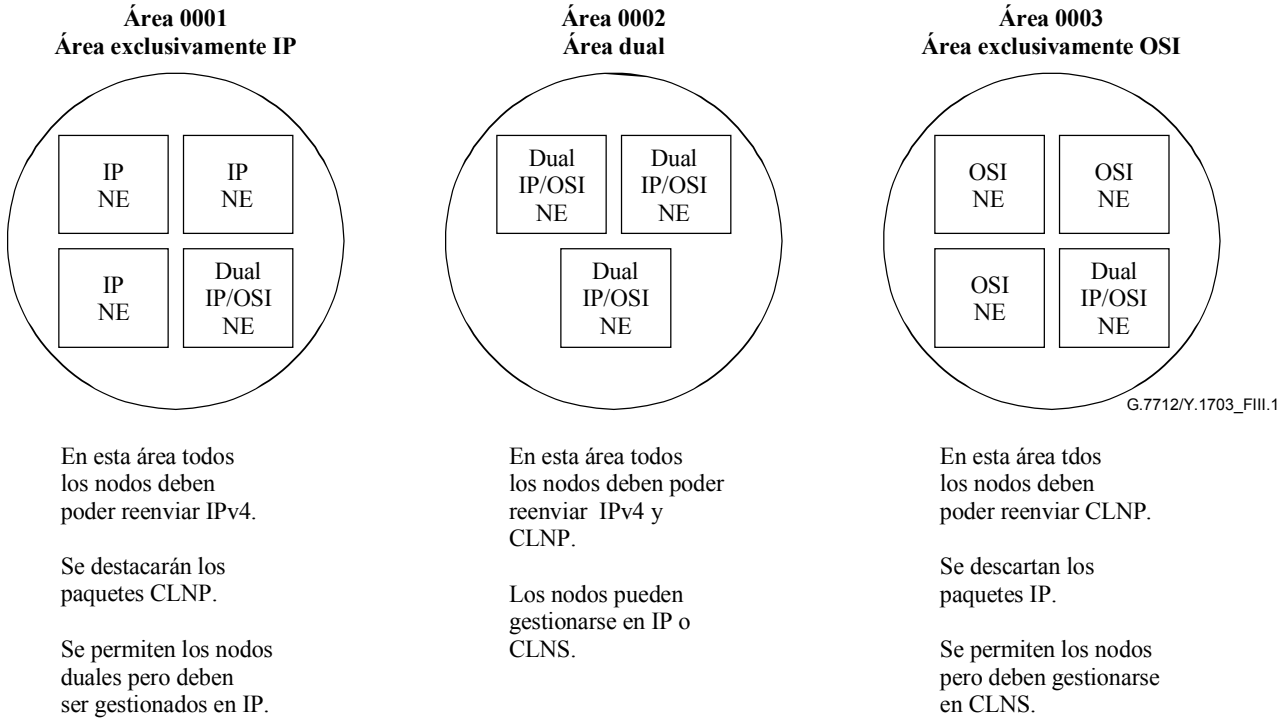


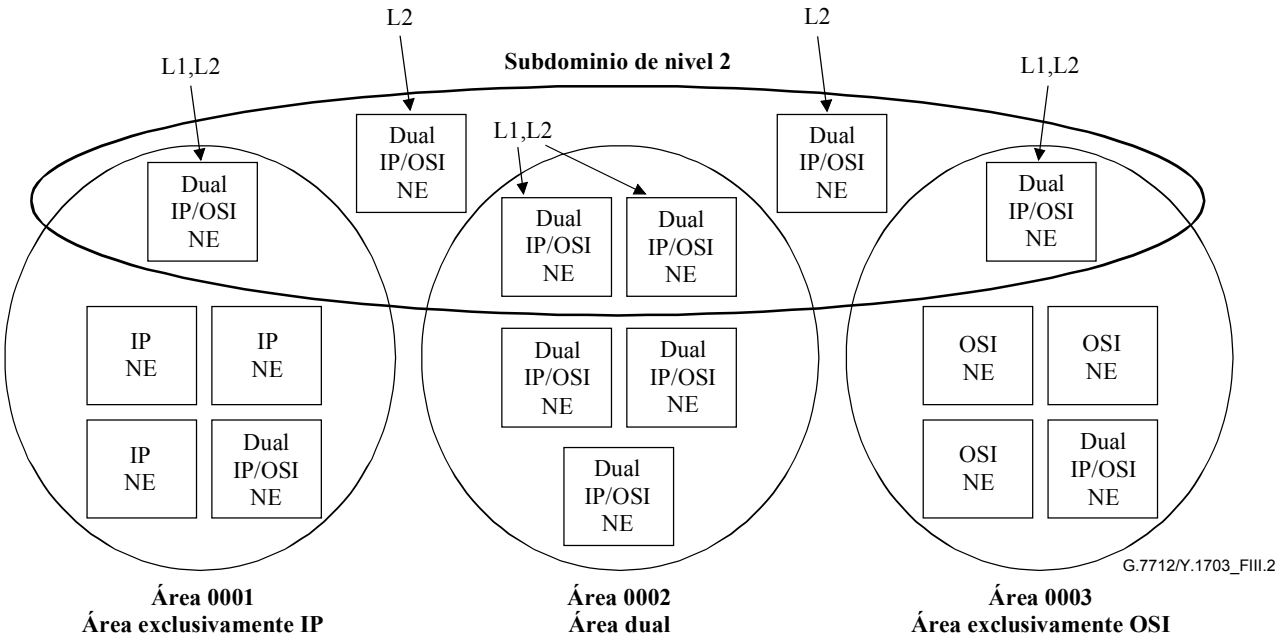
Figura III.1/G.7712/Y.1703 – Clasificación de IS-IS de área de nivel 1

III.2.2 Subdominio de nivel 2

Cuando se necesita una red más grande, que exija encaminamiento de nivel 2, el subdominio de nivel 2 reenvía paquetes entre las áreas de nivel 1 y por consiguiente debe soportar todos los tipos de paquetes existentes en todas las citadas áreas de nivel 1. Las reglas para el subdominio de nivel 2 son las siguientes:

1) Si se reenvían paquetes IPv4 en cualquiera de las áreas (ya sean áreas exclusivamente IP o duales), todos los encaminadores del subdominio de nivel 2 deben poder reenviar IPv4.
2) Si se reenvían paquetes CLNP en cualquiera de las áreas (ya sean áreas exclusivamente OSI o duales), todos los encaminadores del subdominio de nivel 2 deben poder reenviar CLNP.

Por consiguiente, si cualquiera de las áreas es dual, o si existen tanto áreas exclusivamente OSI como áreas exclusivamente IP, los encaminadores del subdominio de nivel 2 deberán ser duales. Esto se ilustra en la figura III.2.



Como en las áreas de nivel 1 se reenvían tanto IPv4 como CLNP, todos los nodos del subdominio de nivel 2 deben ser duales, incluso los existentes en las áreas exclusivamente IP o exclusivamente OSI.

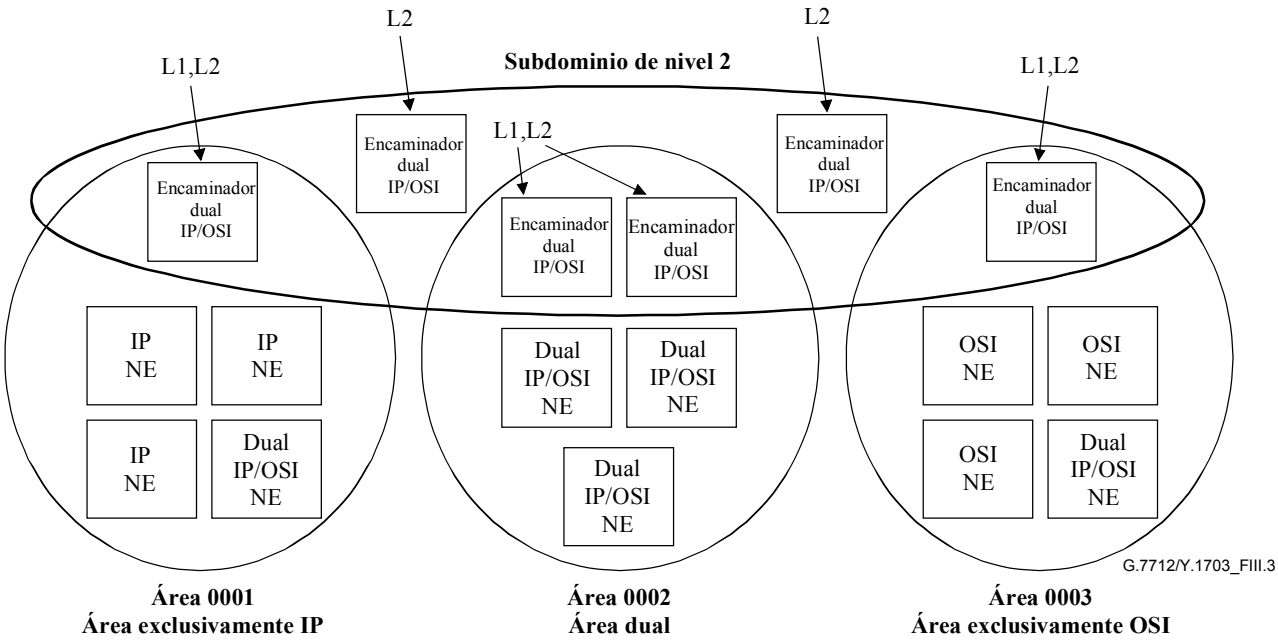
Un nodo se encuentra en el subdominio de nivel 2 si ejecuta el encaminamiento de nivel 2.

Figura III.2/G.7712/Y.1703 – Subdominio de nivel 2

III.2.3 Subdominio de nivel 2 con encaminadores externos ejecutando IS-IS integrado

En la actualidad muchos operadores ejecutan encaminamiento IS-IS de nivel 1 en sus elementos de red SDH exclusivamente OSI, enlazando a continuación varias áreas por medio de encaminamiento IS-IS de nivel 2 en una red de encaminadores exteriores.

Si un operador desea utilizar un modelo semejante para una red dual puede ejecutar IS-IS integrado de nivel 1 en cada área e IS-IS integrado de nivel 2 en una red de encaminadores externos. Esto genera una red muy semejante a la anterior, como se ve en la figura III.3



Como en las áreas de nivel 1 se reenvían tanto IPv4 como CLNP, todos los encaminadores del subdominio de nivel 2 deben ser duales, incluso los existentes en las áreas exclusivamente IP o exclusivamente OSI.

Figura III.3/G.7712/Y.1703 – Encaminadores IS-IS de nivel 2 en una red de encaminamiento externa

III.2.4 Encaminadores externos ejecutando OSPF u otros protocolos de encaminamiento IP

En la actualidad muchos operadores ejecutan IS-IS de nivel 2 en sus encaminadores externos, y OSPF u otros protocolos de encaminamiento para IP. En este caso el encaminador externo debe permanecer como encaminador de nivel 2 para los elementos de red SDH y por esto, para una área dual, debe haber un encaminador IS-IS integrado dual. No obstante puede configurarse el encaminador para encaminar todos los paquetes IP utilizando OSPF configurando la redistribución de rutas IP entre IS-IS y OSPF. De este modo todos los paquetes IP serán encaminados con OSPF, mientras que los paquetes CLNP continuarán siendo encaminados en IS-IS de nivel 2. Esto se representa en la figura III.4.

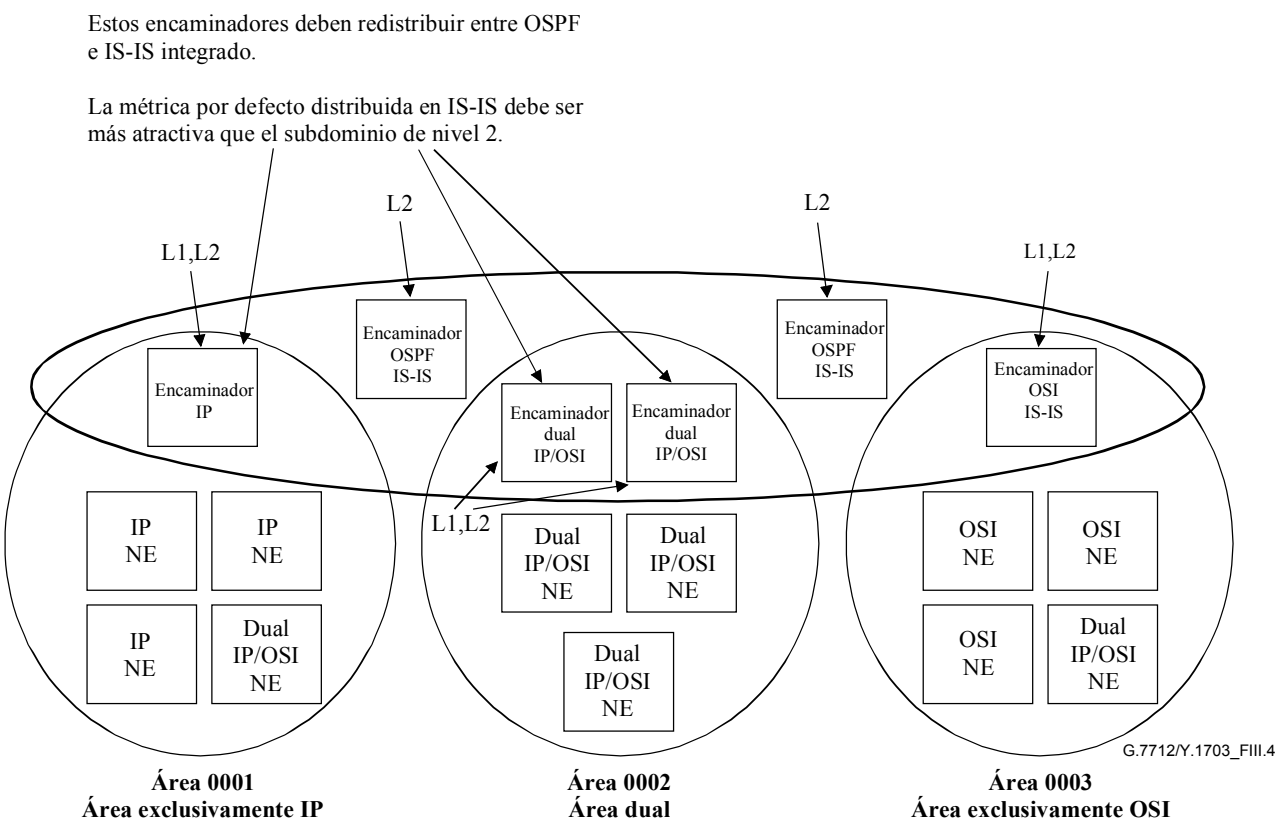


Figura III.4/G.7712/Y.1703 – Encaminadores externos ejecutando OSPF

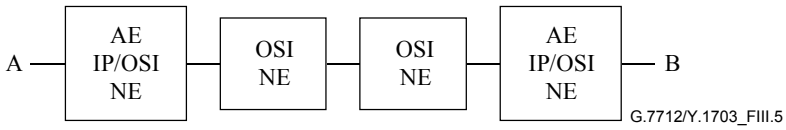
Obsérvese que la pila IS-IS integrada en los encaminadores externos no será consciente de que el subdominio de nivel 2 se reserva exclusivamente a los paquetes CLNP. Por consiguiente, las rutas aprendidas con OSPF deben ser redistribuidas a IS-IS integrados con una métrica por defecto baja, para hacerlas más atractivas a los paquetes IP que el subdominio de nivel 2.

III.3 IS-IS integrado con encapsulación automática

III.3.1 Introducción y repercusión sobre las restricciones topológicas

La opción de encapsulación automática permite incumplir las reglas topológicas de RFC 1195. La encapsulación automática hace que un nodo, o grupo de nodos, parezca efectivamente capaz de reenviar paquetes que en realidad no puede.

Esto se muestra en la figura III.5.



AE Encapsulación automática (*automatically encapsulating*)

Figura III.5/G.7712/Y.1703 – Grupo de nodos con encapsulación automática

Este grupo de nodos reenviará ahora paquetes tanto IPv4 como CLNP, siempre que los paquetes entren por los puntos A o B, a través de uno de los nodos de encapsulación automática.

El grupo de nodos puede ser colocado ahora sin problemas en un área dual o en un subdominio de nivel 2 dual, ya que el par de nodos de encapsulación automática reenviará paquetes IPv4

encapsulándolos en el interior de paquetes CLNP, de modo que se reenvíen por los elementos de red exclusivamente OSI en vez de ser descartados.

Un área dual válida puede tener ahora un aspecto similar al que se muestra en la figura III.6.

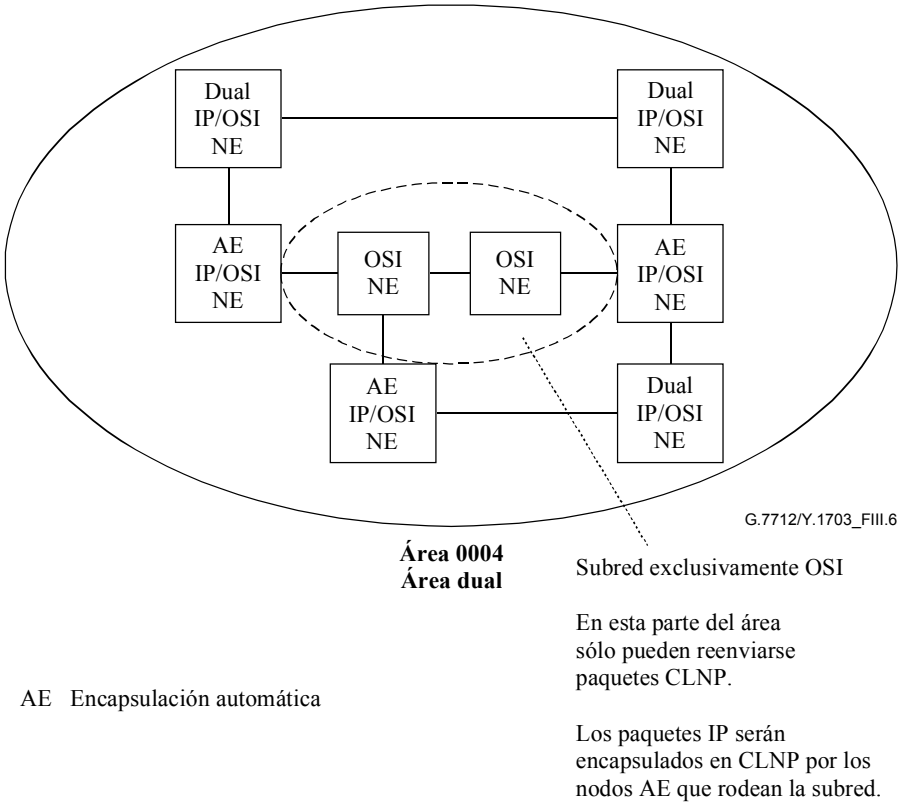


Figura III.6/G.7712/Y.1703 – Ejemplo de área dual válida

Obsérvese que los nodos exclusivamente OSI no deben conectarse directamente a ninguno de los nodos duales que no tengan la opción de encapsulación automática. Sólo la presencia de los nodos de encapsulación automática evita el envío de paquetes IPv4 a los nodos exclusivamente OSI.

Un nodo dual puede conectarse directamente a un nodo exclusivamente OSI si se trata también como un nodo exclusivamente OSI, como muestra la figura III.7.

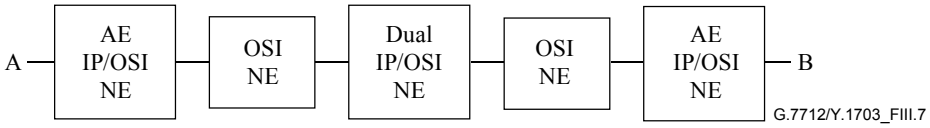


Figura III.7/G.7712/Y.1703 – Conexión de un nodo dual a un nodo exclusivamente OSI

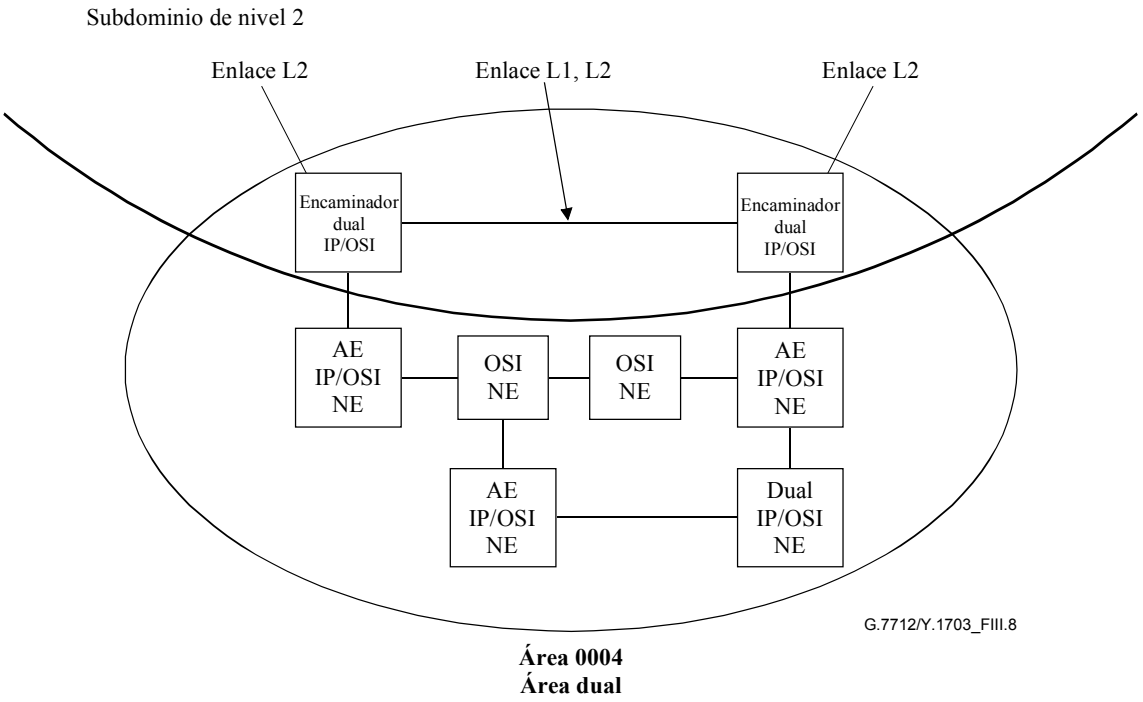
En este caso, la red se comporta como una red dual para los paquetes que vayan del punto A al B, pero los paquetes IPv4 no pueden alcanzar el nodo dual central. Este nodo dual se encuentra en el interior de una subred exclusivamente OSI. Este nodo dual sólo será capaz de reenviar paquetes CLNP y debe ser gestionado en CLNS. No debe haber otras conexiones con el nodo dual central, ya que si se introdujesen paquetes IPv4 en el nodo central, podrían reenviarse a un nodo exclusivamente OSI siendo descartados.

III.3.2 Introducción y extracción de tráfico IP en la red integrada SDH

III.3.2.1 Elemento de red pasarela con capacidad IP

Los paquetes IP y los CLNP deben poder entrar y salir de un área dual, se utilice o no la encapsulación automática. Normalmente el tráfico entra y sale de un área IS-IS a través de encaminadores de nivel 1, nivel 2. Estos encaminadores participan tanto en el área de nivel 1 como en el subdominio de nivel 2.

La manera más sencilla de construir esto es garantizar que todos los encaminadores de nivel 1, nivel 2 son duales, como se representa en la figura III.8.

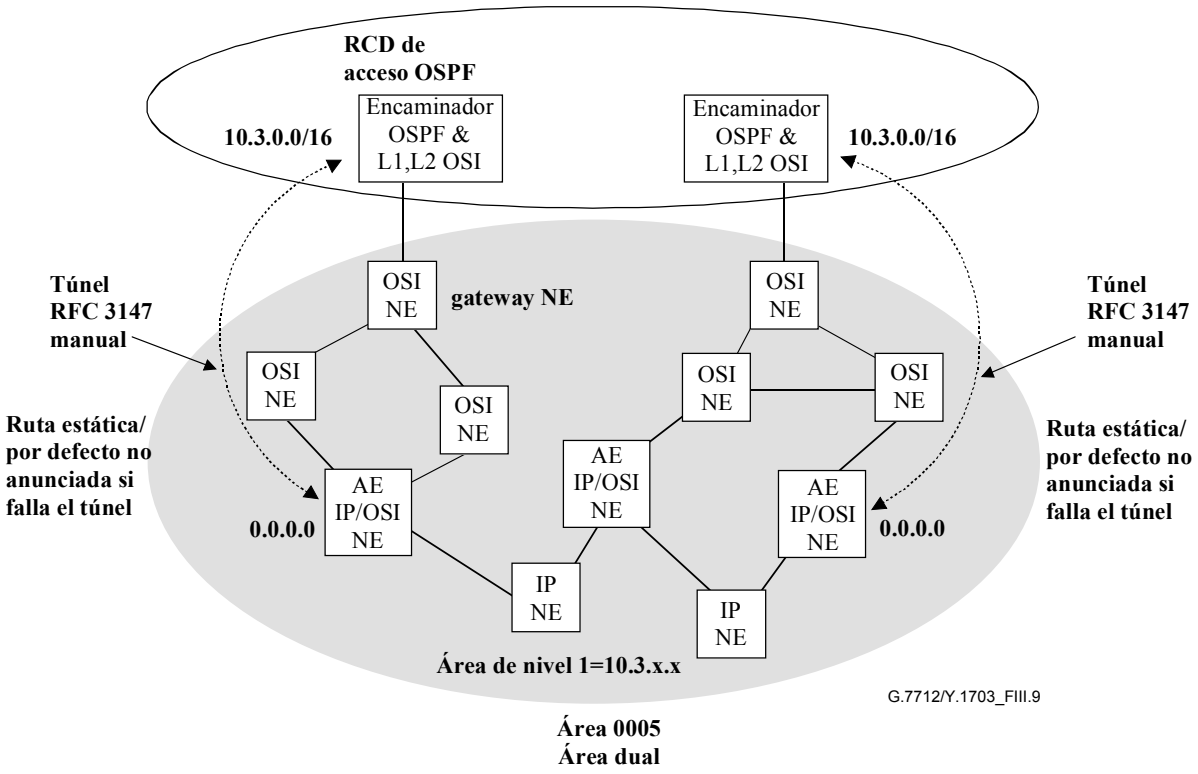


AE Encapsulación automática

Figura III.8/G.7712/Y.1703 – Pasarela dual

III.3.2.2 Elemento de red Pasarela exclusivamente OSI

Ocasionalmente, los nodos de encapsulación automática se utilizan para actualizar un área existente exclusivamente OSI y convertirla efectivamente en un área dual. En este caso, puede que los nodos de pasarela tengan que permanecer como nodos exclusivamente OSI. Si éste fuera el caso, la red podría construirse como se representa en la figura III.9.



AE Encapsulación automática

Figura III.9/G.7712/Y.1703 – Pasarela exclusivamente OSI

En esta red los paquetes CLNP que necesiten salir del área de nivel 1 continúan hasta el encaminador OSI de nivel 1, nivel 2. Los nodos con un túnel manual que conduzca al exterior del área de nivel 1 lo anuncian como ruta por defecto. Por consiguiente, los nodos con capacidad IP añadirán una entrada al final de su cuadro de encaminamiento para indicarles el envío de todos los paquetes IPv4 a uno de los nodos con túnel manual, salvo que haya una ruta más específica. De este modo, un paquete IPv4 nunca se envía a un nodo de nivel 1, nivel 2, sino que siempre se envía a través de uno de los túneles manuales.

El encaminador de la RCD de acceso que termina el túnel manual no necesita ejecutar IS-IS integrado. Puede ejecutar cualquier protocolo de encaminamiento IP que desee utilizar el operador. De este modo, una red existente que utilice OSPF e IS-IS de nivel 2 en la RCD de acceso, e IS-IS de nivel 1 en los elementos de red SDH, puede actualizar las áreas de nivel 1 a áreas duales con escasa repercusión sobre los elementos de red SDH exclusivamente OSI, o sobre la RCD de acceso.

Apéndice IV

Ejemplo ilustrativo de la protección de paquetes 1+1

IV.1 Resumen de la protección de paquetes 1+1

La protección de trayecto de paquetes 1+1 proporciona un servicio de protección a nivel de paquete semejante en ciertos aspectos al servicio de conexión de nivel 1+1 aunque con diferencias significativas. La protección de paquetes de nivel 1+1 permite la selección de paquetes de entrada desde cualquier conexión con independencia de la conexión de la que se seleccionó el último paquete. Es decir, la protección de paquetes 1+1 trata ambas conexiones como conexiones operativas en contraposición a la designación de una conexión como operativa y de la otra como

protección. En este último caso, los paquetes se seleccionan de la conexión operativa hasta que se detecte un fallo en la conexión operativa que provoque una conmutación a la conexión de protección. Por contra, la protección de paquetes 1+1 no requiere la detección explícita de fallos ni la conmutación de protección. Esto permite que el mecanismo de paquetes de nivel 1+1 subsane cualquier fallo instantáneamente y transparentemente. Al igual que la protección de conexión de nivel 1+1, sólo los nodos periféricos necesitan ser conscientes del servicio, lo que facilita la interoperabilidad.

Para proporcionar el servicio de protección de paquetes 1+1 entre dos nodos periféricos de red orientados a la conexión, se establece un par de conexiones en caminos disjuntos. Los paquetes de un flujo de aplicación abonados al servicio se introducen dualmente en las dos conexiones del nodo de entrada. En el caso más sencillo, los trayectos disjuntos pueden ser de enlaces disjuntos o de nodos disjuntos pero, en general, pueden implicar conceptos más complejos tales como grupos de riesgo compartido. En el nodo periférico de salida, cada una de las dos copias de los paquetes seleccionados y reenviados, de las dos copias posibles recibidas, recorre un trayecto disjunto. Teniendo esto en cuenta, cualquier fallo sencillo de la red, que no sea la del propio nodo de entrada o de salida, puede afectar como máximo a una copia de cada paquete. Esto permite que el servicio resista un único fallo transparentemente. En términos de tiempo de restauración esto puede caracterizarse como una recuperación instantánea de un fallo ya que no hay necesidad de detectar, notificar ni conmutar al trayecto de protección explícitamente. El mecanismo puede ampliarse con facilidad para protegerse de varios fallos utilizando más de dos trayectos disjuntos.

IV.2 Ilustración de la protección de paquetes 1+1

La figura IV.1 ilustra una realización del servicio que utilizan números de secuencia como identificadores. Tras pasar por el clasificador, el nodo periférico de origen consciente del servicio asigna a cada paquete que necesite reenviarse en los LSP acoplados un número de secuencia peculiar. El paquete con su identificación peculiar se duplica a continuación y se reenvía a los dos LSP disjuntos. El nodo de salida sólo seleccionará una copia del paquete duplicado. Para conseguir seleccionar el paquete sólo una vez, el destino debe poder identificar los paquetes duplicados, seleccionar a continuación sólo uno de ellos, y manejar todas las variaciones posibles. Este proceso de selección a nivel de paquete resulta complejo ya que los paquetes duplicados tal vez no lleguen al mismo tiempo (debido a los retardos de propagación y a las memorias intermedias) y además estos paquetes pueden perderse (debido a los errores de la transmisión y al desbordamiento de las memorias intermedias).

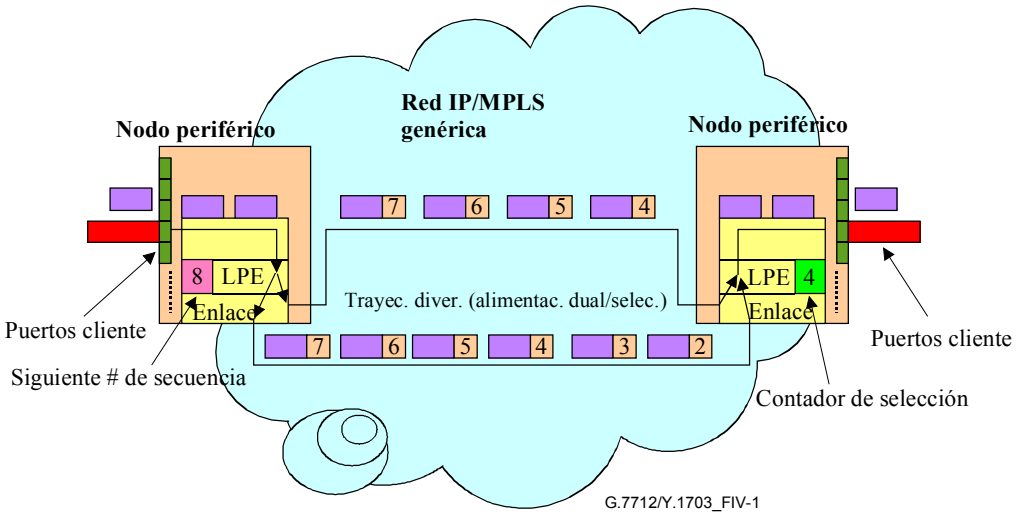


Figura IV.1/G.7712/Y.1703 – Protección 1 + 1

El nodo de ingreso inserta el número de secuencia como se define en 7.1.19.2. A continuación el paquete se duplica y se transporta por diversos LSP. Debido a la diversidad de los LSP, habrá un LSP de cabecera y un LSP de cola. El LSP de cabecera reenviará los paquetes al nodo de salida con más rapidez que el LSP de cola. Por consiguiente cuando no haya fallo, el nodo de salida seleccionará los paquetes del LSP de cabecera. Los paquetes recibidos en el LSP de cola serán paquetes duplicados siendo por consiguiente descartados.

La decisión de aceptar o rechazar un paquete recibido se basa en el número de secuencia del paquete recibido y en un contador más una ventana corrediza en el nodo de salida. El contador indica el número de secuencia del siguiente paquete esperado. El contador, más la ventana corrediza, proporciona una ventana de números de secuencia aceptables. La ventana corrediza es necesaria para la correcta aceptación y rechazo de paquetes. Si el paquete recibido encaja en la ventana, se considera legítimo y puede aceptarse, de lo contrario se rechaza. El tamaño de la ventana debe ser mayor que el máximo número de paquetes consecutivos que un LSP operativo (activo) puede perder.

La ventana corrediza se utiliza para solucionar el problema de la pérdida de paquetes en el LSP de cabecera cuando el número de secuencia del LSP de cabecera está muy próximo al punto en que da la vuelta el contador. La figura IV.2 ilustra un LSP de cabecera (LSP 1) que reenvía un paquete con un número de secuencia igual a 29. El paquete se acepta y el contador se incrementa hasta 30. Si se supone la pérdida de dos paquetes consecutivos (es decir los paquetes con números de secuencia 30 y 31), el siguiente paquete recibido en el LSP 1 será cero. Sin una ventana corrediza, el nodo de salida rechazaría el paquete ya que $0 < 30$. Implementando una ventana corrediza mayor que el número máximo de paquetes consecutivos que un LSP operativo (activo) puede perder, se soluciona este problema. Por ejemplo, supongamos que el número máximo de paquetes consecutivos que un LSP operativo puede perder es 5, en este caso puede definirse una ventana de 6. Tomando el mismo ejemplo anterior, aunque utilizando ahora la ventana corrediza, el nodo de salida aceptará paquetes en la gama de {30, 31, 0, 1, 2, 3, 4}. Por consiguiente, aunque se pierdan 5 paquetes (es decir el máximo número de paquetes consecutivos que puede perderse en un LSP operativo) el siguiente paquete recibido tendrá un número de secuencia de 3 y se aceptará el paquete.

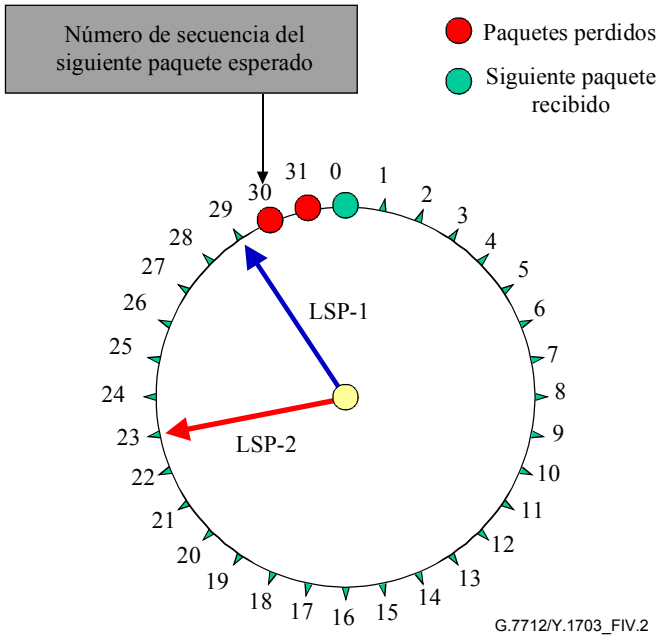


Figura IV.2/G.7712/Y.1703 – Funcionamiento de la ventana corrediza

Obsérvese que este concepto de ventana corrediza sólo funciona si el LSP retrasado no cae fuera del intervalo de la ventana corrediza. Si un paquete con un número de secuencia en el intervalo de la ventana corrediza se recibe del LSP con retraso, se aceptará indebidamente. Un LSP retrasado sólo puede recibir un paquete con un número de secuencia en el intervalo de la ventana corrediza si está retrasado en más de (2^N – tamaño de la ventana corrediza). Por consiguiente el número de bits "*N*" utilizados para el número de secuencia debe ajustarse a la siguiente ecuación:

$$2^N > \text{Ventana corrediza} + \text{Ventana de retardo}$$

siendo;

Ventana corrediza > máximo número de paquetes consecutivos que pueden perderse en un LPS

y

Ventana de retardo = máximo número de paquetes que el LSP de cola puede retrasarse con respecto al LSP de cabecera

Obsérvese que 7.1.19.2 define un campo de 4 octetos para transportar el número de secuencia. Este campo de 4 octetos proporciona una secuencia de más de cuatro mil millones de números que es suficientemente grande para acomodar las pérdidas de paquetes consecutivos en el caso más desfavorable y los diferenciales de retardo.

Una manera razonable de diseñar el tamaño de las ventanas corredizas y de retardo es hacer el tamaño de la ventana corrediza igual al tamaño de la ventana de retardo. (Obsérvese que se supone que el tamaño de la ventana de retardo suele ser mayor que el tamaño de la ventana corrediza.) Esto garantiza la selección de paquetes del LSP de cabecera en todos los casos una vez reparado un LSP fallido. Este punto se explica más detalladamente en la cláusula siguiente que trata de los diversos casos de fallo.

IV.3 Funcionamiento del algoritmo selector en diversos casos de fallo

Una manera de enfocar el funcionamiento del algoritmo selector es imaginar un reloj con 2^N intervalos. La figura IV.3 ilustra un ejemplo en el que N = 4 (es decir, un número de secuencia de 4 bits) oscilando por consiguiente el número de secuencia entre 0 y 15.

En este ejemplo, la ventana de desplazamiento se hace igual a la ventana de retardo, cuyo valor es 5.

La figura IV.3 muestra que el LSP de cabecera está 3 números de secuencia por delante del LSP de cola. El LSP de cabecera reenvía un paquete con el número de secuencia = 1 poniéndose en este momento el contador a 2.

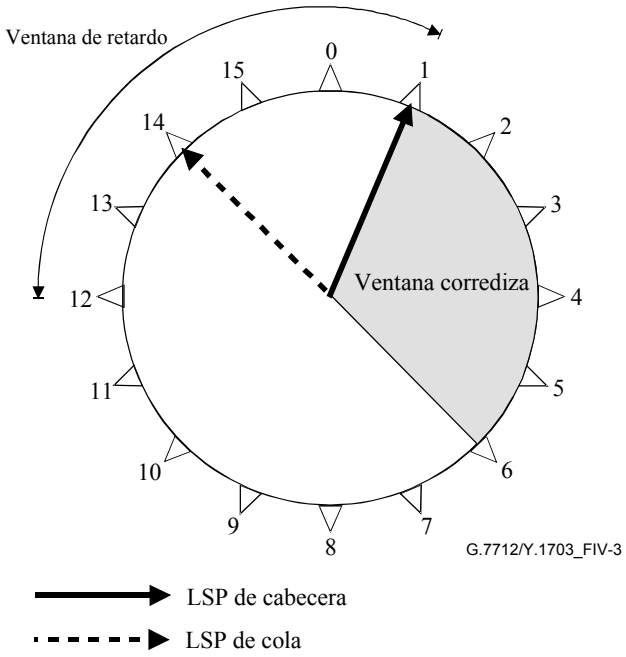


Figura IV.3/G.7712/Y.1703 – Funcionamiento del algoritmo selector

La figura IV.4 muestra que antes de recibir un paquete con un número de secuencia igual a 2 en el LSP de cabecera, el LSP de cabecera falla. Hasta que el LSP de cola no reenvíe el paquete cuyo número de secuencia es 2, el nodo de salida no seleccionará paquetes y el contador permanecerá igual a 2.

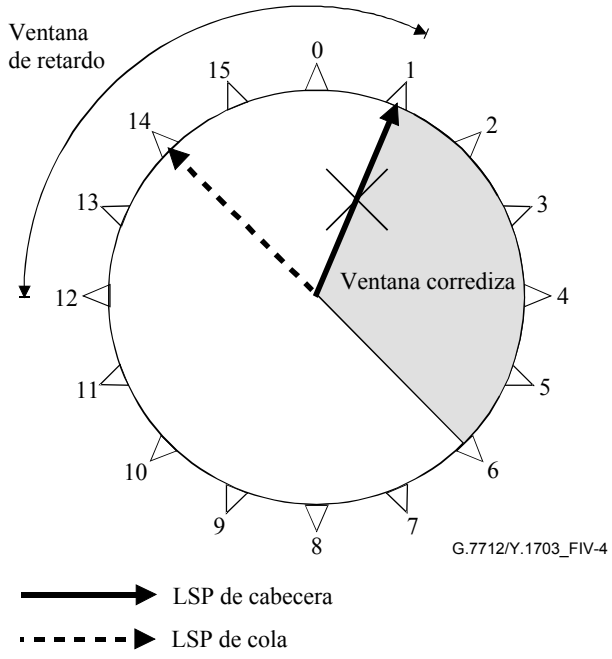


Figura IV.4/G.7712/Y.1703 – Fallo en el LSP de cabecera

La figura IV.5 muestra que cuando el paquete cuyo número de secuencia es 2 se recibe en el LSP de cola, el nodo de salida incrementa el contador hasta 3 y la ventana corrediza se desplaza de modo que un paquete cuyo número de secuencia se encuentre en el intervalo de 3 a 7 puede aceptarse.

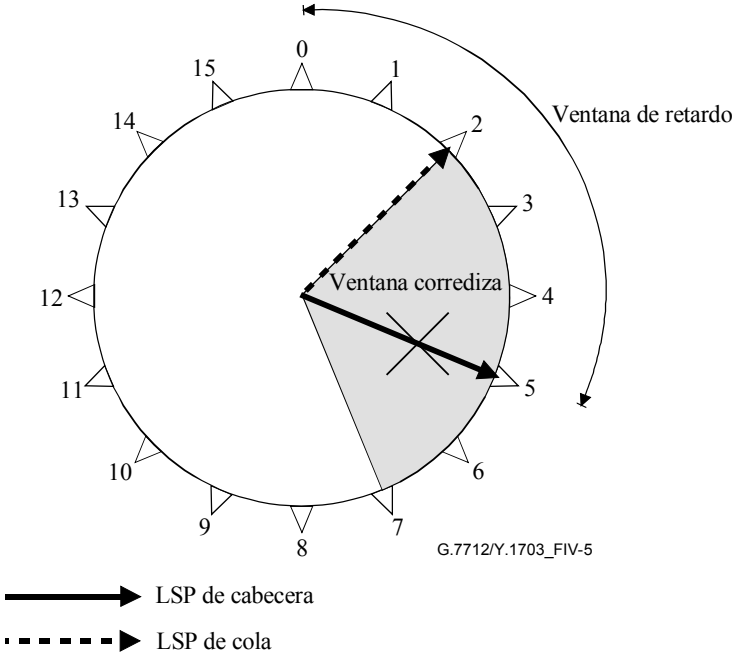


Figura IV.5/G.7712/Y.1703 – Recepción del paquete 2 por el LSP de cola

La figura IV.6 muestra que, antes de recibir un paquete cuyo número de secuencia sea 3 procedente del LSP de cola, se repara el LSP de cabeza y se recibe un paquete con número de secuencia 6 del LSP de cabecera. Como 6 pertenece al intervalo de la ventana corrediza, se acepta el paquete. Obsérvese que es importante que, mientras el LSP de cabecera funcione correctamente, se reciban los paquetes del mismo. Por consiguiente, para garantizar que, una vez reparado el LSP de cabecera, reenvía un paquete con un valor de número de secuencia perteneciente al intervalo de la ventana corrediza, ésta debe ser igual o mayor que la ventana de retardo, lo que corresponde al caso de este ejemplo.

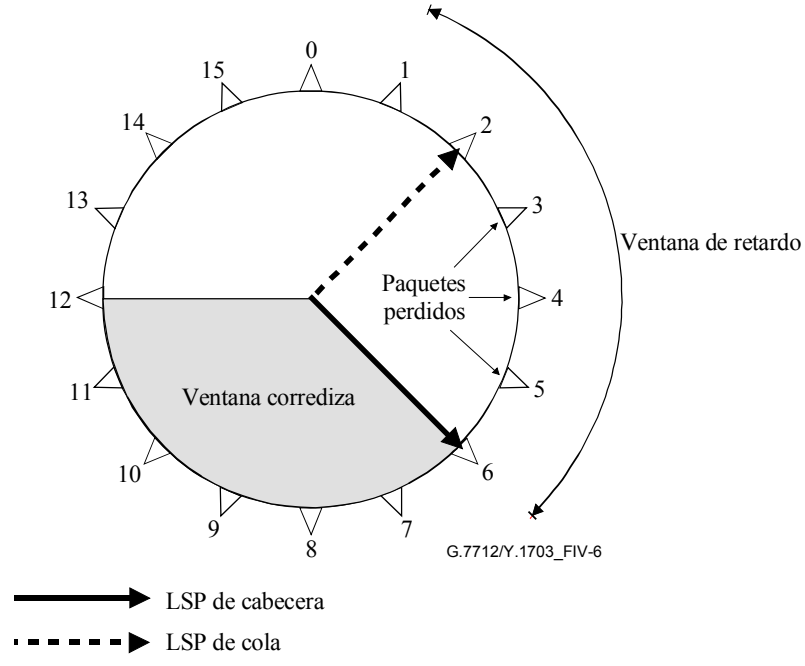


Figura IV.6/G.7712/Y.1703 – Reparación de LSP de cabecera

Las figuras IV.7, IV.8 y IV.9 ilustran el problema que se presenta cuando la ventana corrediza es menor que la ventana de retardo. En tal caso, es posible que, al reparar el LSP de cabecera, reenvíe paquetes con números de secuencia que no entren en la ventana corrediza y, por consiguiente, el nodo de salida continúe aceptando paquetes del LSP de cola. Si, en un instante posterior falla el LSP de cola, hay peligro de perder muchos paquetes (el caso más desfavorable sería 2^N– *tamaño de la ventana corrediza*, siendo N el número de bits utilizados para el número de secuencia).

La figura IV.7 muestra un ejemplo en el que la ventana corrediza se pone a 3, mientras que la ventana de retardo puede tener un valor de hasta 7. En este ejemplo, el LSP de cola está retrasado con respecto al LSP de cabecera en 4 números de secuencia. Como el LSP de cabecera tiene fallo, los paquetes se seleccionan del LSP de cola.

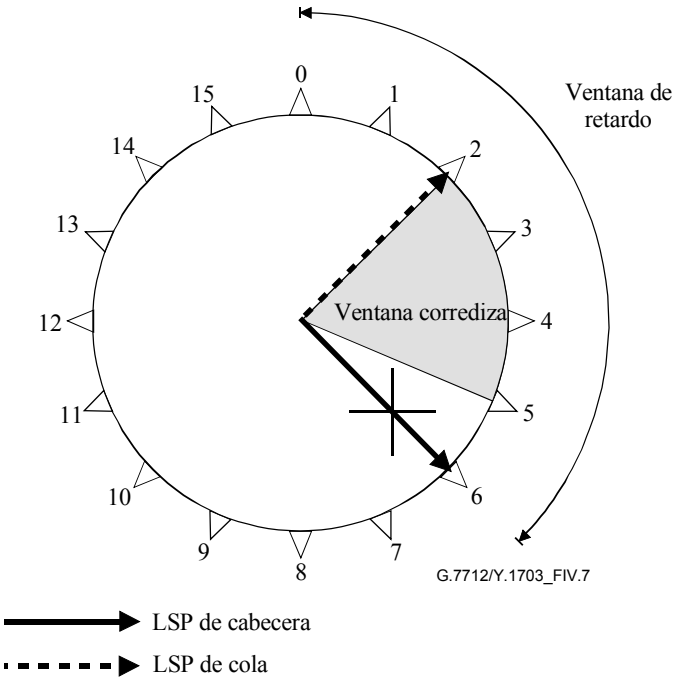


Figura IV.7/G.7712/Y.1703 – Ventana corrediza muy pequeña: paquetes seleccionados del LSP de cola

La figura IV.8 muestra que en el momento en que se repara el LSP de cabecera, reenvía un paquete con un número de secuencia igual a 7 que está fuera de la ventana corrediza, rechazándose por consiguiente. Los paquetes continúan seleccionándose del LSP de cola.

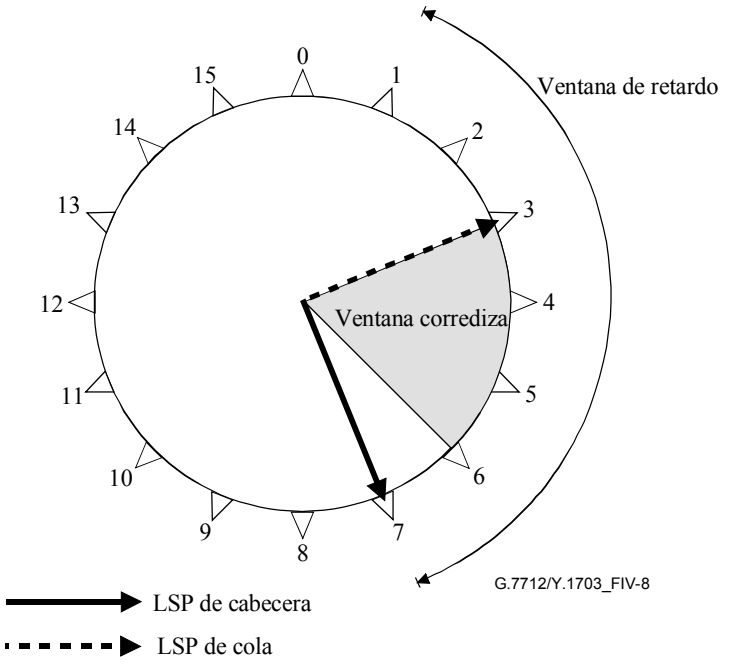


Figura IV.8/G.7712/Y.1703 – Ventana corrediza muy pequeña: rechazo de los paquetes enviados por el LSP de cabecera reparado

La figura IV.9 ilustra un fallo del LSP de cola. Dado que el LSP de cabecera reenvía paquetes fuera de la ventana corrediza y que, por consiguiente, dichos paquetes son rechazados, el nodo de salida no empezará a aceptar paquetes hasta que el LSP de cabecera dé la vuelta y comience a reenviar paquetes con un número de secuencia que entre en la ventana corrediza. Esto puede provocar una pérdida importante de paquetes. Por consiguiente, para evitar que ocurra esto, se recomienda que este tipo de algoritmos selector haga la ventana corrediza igual a la ventana de retardo.

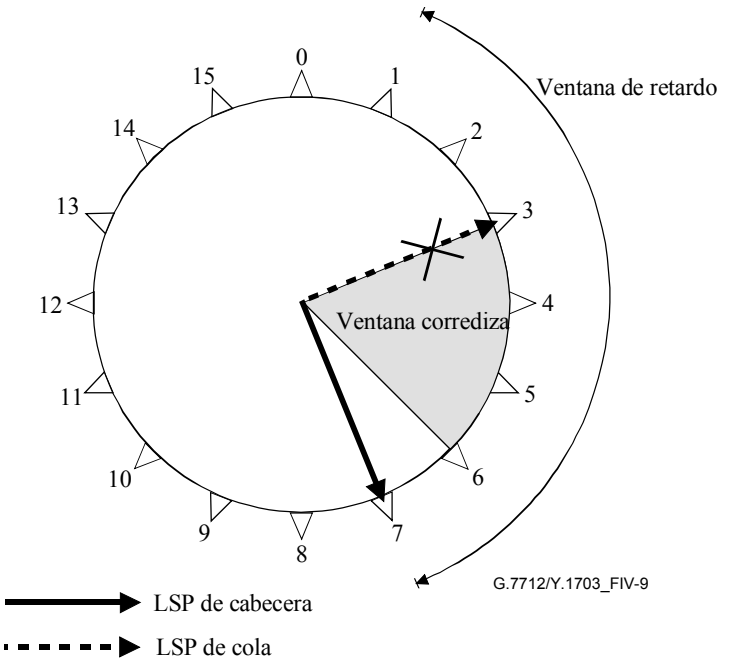


Figura IV.9/G.7712/Y.1703 – Ventana corrediza muy pequeña: efecto de un fallo del LSP de cola

Apéndice V

Bibliografía

– IETF RFC 1006 (1997), *ISO Transport Service on top of the TCP Version 3*.

– IETF RFC 2966 (2000), *Domain-wide Prefix Distribution with Two-Level IS-IS*

– IETF RFC 3147 (2001), *Generic Routing Encapsulation of CLNS Networks*.

– IETF RFC 3373 (2002), *Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies*.

RECOMENDACIONES UIT-T DE LA SERIE Y

INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN Y ASPECTOS DEL PROTOCOLO INTERNET

INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN	
Generalidades	Y.100–Y.199
Servicios, aplicaciones y programas intermedios	Y.200–Y.299
Aspectos de red	Y.300–Y.399
Interfaces y protocolos	Y.400–Y.499
Numeración, direccionamiento y denominación	Y.500–Y.599
Operaciones, administración y mantenimiento	Y.600–Y.699
Seguridad	Y.700–Y.799
Características	Y.800–Y.899
ASPECTOS DEL PROTOCOLO INTERNET	
Generalidades	Y.1000–Y.1099
Servicios y aplicaciones	Y.1100–Y.1199
Arquitectura, acceso, capacidades de red y gestión de recursos	Y.1200–Y.1299
Transporte	Y.1300–Y.1399
Interfuncionamiento	Y.1400–Y.1499
Calidad de servicio y características de red	Y.1500–Y.1599
Señalización	Y.1600–Y.1699
Operaciones, administración y mantenimiento	**Y.1700–Y.1799**
Tasación	Y.1800–Y.1899
REDES DE LA PRÓXIMA GENERACIÓN	
Marcos y modelos arquitecturales funcionales	Y.2000–Y.2099
Calidad de servicio y calidad de funcionamiento	Y.2100–Y.2199
Aspectos relativos a los servicios: capacidades y arquitectura de servicios	Y.2200–Y.2249
Aspectos relativos a los servicios: interoperabilidad de servicios y redes en las redes de 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 B	Medios de expresión: definiciones, símbolos, clasificación
Serie C	Estadísticas generales de telecomunicaciones
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	**Sistemas y medios de transmisión, sistemas y redes digitales**
Serie H	Sistemas audiovisuales y multimedios
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedios
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos y comunicación entre sistemas abiertos
Serie Y	**Infraestructura mundial de la información y aspectos del protocolo Internet**
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2003