Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.608

(02/2007)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Gestión de redes de interconexión de sistemas abiertos y aspectos de sistemas – Gestión de redes

Tecnología de la información –Protocolo perfeccionado de transporte de comunicaciones: Especificación del transporte multidifusión N-plex

Recomendación UIT-T X.608

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	
Servicios y facilidades	X.1–X.19
Interfaces	X.20–X.49
Transmisión, señalización y conmutación	X.50–X.89
Aspectos de redes	X.90–X.149
Mantenimiento	X.150–X.179
Disposiciones administrativas	X.180–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Modelo y notación	X.200–X.209
Definiciones de los servicios	X.210–X.219
Especificaciones de los protocolos en modo conexión	X.220–X.229
Especificaciones de los protocolos en modo sin conexión	X.230–X.239
Formularios para declaraciones de conformidad de implementación de protocolo	X.240–X.259
Identificación de protocolos	X.260–X.269
Protocolos de seguridad	X.270–X.279
Objetos gestionados de capa	X.280–X.289
Pruebas de conformidad	X.290–X.299
INTERFUNCIONAMIENTO ENTRE REDES	
Generalidades	X.300–X.349
Sistemas de transmisión de datos por satélite	X.350–X.369
Redes basadas en el protocolo Internet	X.370–X.379
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	
Gestión de redes	**X.600–X.629**
Eficacia	X.630–X.639
Calidad de servicio	X.640–X.649
Denominación, direccionamiento y registro	X.650–X.679
Notación de sintaxis abstracta uno	X.680–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Marco y arquitectura de la gestión de sistemas	X.700–X.709
Servicio y protocolo de comunicación de gestión	X.710–X.719
Estructura de la información de gestión	X.720–X.729
Funciones de gestión y funciones de arquitectura de gestión distribuida abierta	X.730–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Compromiso, concurrencia y recuperación	X.850–X.859
Procesamiento de transacciones	X.860–X.879
Operaciones a distancia	X.880–X.889
Aplicaciones genéricas de la notación de sintaxis abstracta uno	X.890–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LAS TELECOMUNICACIONES	X.1000–

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

NORMA INTERNACIONAL ISO/CEI 14476-5
RECOMENDACIÓN UIT-T X.608

Tecnología de la información – Protocolo perfeccionado de transporte de comunicaciones: Especificación del transporte multidifusión N-plex

Resumen

En la presente Recomendación | Norma Internacional se describe un protocolo para el transporte multidifusión N-plex por Internet con soporte de la multidifusión IP. Se presentan los mecanismos de control de sesión y control de errores. Para el control de sesión, se designa a uno de los participantes como gestor de la creación/terminación de una conexión; el ingreso/egreso de un participante; y los testigos que permiten a los participantes enviar datos. Para el control de errores, se presentan los mecanismos de recuperación de pérdidas en árbol; de construcción de árboles de control con árboles de dos capas lógicas; y la adaptación de árbol lógico con estado de entrega de paquetes. En esta Especificación se describen los detalles del protocolo, tales como el formato de paquetes, los procedimientos y los valores de parámetro. Este protocolo puede utilizarse para las aplicaciones que requieren un servicio de entrega de datos de muchos a muchos fiable.

Orígenes

La Recomendación UIT-T X.608 fue aprobada el 13 de febrero de 2007 por la Comisión de Estudio 17 (2005-2008) del UIT-T por el procedimiento de la Recomendación UIT-T A.8. Se publica también un texto idéntico como Norma Internacional ISO/CEI 14476-5.

PREFACIO

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

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

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

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

NOTA

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

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

PROPIEDAD INTELECTUAL

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

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

ÍNDICE

Página

Introducción

El protocolo perfeccionado de transporte de comunicaciones (ECTP, *enhanced communications transport protocol*) está diseñado para soportar conexiones de multidifusión muy controladas en aplicaciones símplex, dúplex y N-plex. Esta parte del ECTP (Parte 5: Rec. UIT-T X.608 | ISO/CEI 14476-5) especifica los mecanismos del protocolo para el transporte de datos en multidifusión N-plex.

En las conexiones de multidifusión N-plex, los participantes comprenden un TC-Propietario y muchos TS-usuarios. Antes de empezar la conexión se designará al TC-Propietario de entre los TS-usuarios. El TC-Propietario se encuentra en el corazón de las comunicaciones del grupo de multidifusión. Es responsable de la gestión general de la conexión, ya que rige la creación de la conexión y su terminación, el transporte de datos en multidifusión y las operaciones de ingreso tardío y egreso.

En las conexiones de multidifusión N-plex, se permiten las transmisiones de datos en multidifusión de TS-usuarios y del TC-Propietario. Cada TS-usuario puede enviar datos en multidifusión al grupo únicamente si el TC-Propietario le concede un testigo, es decir, que el TC-Propietario controla las transmisiones de datos en multidifusión de los TS-usuarios.

La conexión de multidifusión N-plex que se especifica en esta Recomendación | Norma Internacional atañe a las aplicaciones de multidifusión de muchos a muchos en las que es posible que muchos participantes (TS-usuarios) quieran transmitir datos en multidifusión a todos los demás TS-usuarios. Como ejemplos típicos de estas aplicaciones pueden citarse la 'teleconferencia' y los 'juegos en línea con múltiples usuarios', etc. En la teleconferencia, el TC-Propietario puede hacer las veces de 'servidor de conferencia' y todos los demás participantes (TS-usuarios) pueden enviar datos en multidifusión, como voz, texto e imagen a los demás participantes.

NORMA INTERNACIONAL
RECOMENDACIÓN UIT-T

Tecnología de la información – Protocolo perfeccionado de transporte de comunicaciones: Especificación del transporte multidifusión N-plex

1 Alcance

Esta Recomendación | Norma Internacional especifica la conexión de transporte de multidifusión N-plex en la que todos los participantes son TS-usuarios y uno de ellos es el TC-Propietario. En la conexión de transporte de multidifusión N-plex se permite a todos los TS-usuarios enviar datos en multidifusión a todos los miembros del grupo. Hay que señalar que un TS-usuario puede enviar datos en multidifusión al grupo únicamente si obtiene un testigo del TC-Propietario.

En esta Especificación se describe el protocolo que soporta el transporte multidifusión N-plex, que incluye la gestión de la conexión (establecimiento, terminación, ingreso y egreso de usuarios) y los mecanismos de control de la fiabilidad del transporte de datos en multidifusión.

2 Referencias

2.1 Referencias normativas

Las siguientes Recomendaciones UIT-T y Normas Internacionales contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de esta Recomendación | Norma Internacional. A la fecha de esta publicación, las ediciones citadas están en vigor. Todas las Recomendaciones y Normas son objeto de revisión, por lo que se alienta a los usuarios de esta Recomendación | Norma Internacional a que utilicen la edición más reciente de las Recomendaciones | Normas Internacionales que se indican a continuación. Los miembros de la ISO y la CEI mantienen un registro de las Normas Internacionales en vigor. La Oficina de Normalización de las Telecomunicaciones del UIT-T publica periódicamente una lista de las Recomendaciones UIT-T vigentes.

- Recomendación UIT-T X.601 (2000), *Marco para comunicaciones entre múltiples pares*.
- Recomendación UIT-T X.602 (2004) | ISO/CEI 16513:2005, *Tecnología de la información – Protocolo de gestión de grupo*.
- Recomendación UIT-T X.605 (1998) | ISO/CEI 13252:1999, *Tecnología de la información – Definición del servicio perfeccionado de transporte de comunicaciones*.
- Recomendación UIT-T X.606 (2001) | ISO/CEI 14476-1:2002, *Tecnología de la información – Protocolo perfeccionado de transporte de comunicaciones: Especificación del transporte multidifusión símplex*.
- Recomendación UIT-T X.606.1 (2003) | ISO/CEI 14476-2:2003, *Tecnología de la información – Protocolo perfeccionado de transporte de comunicaciones: Especificación de la gestión de la calidad de servicio en el transporte multidifusión símplex*.
- Recomendación UIT-T X.607 (2007) | ISO/CEI 14476-3:2007, *Tecnología de la información – Especificación del protocolo perfeccionado de transporte de comunicaciones: transporte multidifusión dúplex*.

2.2 Referencia informativa

- Proyecto de Recomendación UIT-T X.607.1 | ISO/CEI 14476-4 , *Tecnología de la información – Especificación del protocolo perfeccionado de transporte de comunicaciones: Especificación de la gestión de la calidad de servicio en el transporte multidifusión dúplex.*

3 Definiciones

En esta Recomendación | Norma Internacional se utilizan las siguientes definiciones, ya especificadas en el servicio perfeccionado de transporte de comunicaciones (Rec. UIT-T X.605 | ISO/CEI 13252).

a) Conexión de transporte: símplex, dúplex y N-plex.

En esta Recomendación | Norma Internacional se redefinen los siguientes términos utilizados en el servicio perfeccionado de transporte de comunicaciones (Rec. UIT-T X.605 | ISO/CEI 13252).

a) **TC-propietario (TCN, *transport control network*)**: El TCN gestiona todas las operaciones de una conexión de multidifusión N-plex.

b) **usuario de servicio de transporte (TS-usuario)**: Los TS-usuarios pueden enviar y recibir datos en multidifusión a través de la conexión de multidifusión N-plex.

c) **TS-usuario emisor (SU, *sending TS-user*)**: TS-usuario que obtiene un testigo del TCN. El SU sólo puede enviar datos en multidifusión al grupo. En otros términos, antes de enviar datos en multidifusión, el TS-usuario debe solicitar un testigo al TCN.

En esta Recomendación | Norma Internacional se redefinen los siguientes términos utilizados en el protocolo perfeccionado de transporte de comunicaciones: parte 1 (Rec. UIT-T X.606 | ISO/CEI 14476-1) para adaptarlos a la conexión de multidifusión N-plex.

a) **Grupo local**: Conjunto de nodos vecinos que tienen un correlación red-capa en términos de pérdida y retardo de paquetes.

b) **Propietario local (LO, *local owner*)**: El LO es un nodo representativo de un grupo local y está estáticamente designado. Es responsable de mantener un árbol intragrupo del grupo y los árboles de control de todos los SU de su grupo local. Cada LO está también conectado a los demás LO en los árboles intergrupo. Asimismo, genera periódicamente tráfico de prueba para la adaptación del árbol lógico.

c) **Canal de datos multidifusión**: El TCN o el SU pueden enviar datos en multidifusión a todos los demás miembros del grupo a través de una dirección de multidifusión IP.

En esta Recomendación | Norma Internacional se definen los siguientes términos:

a) **árbol lógico**: Árbol que se divide en todos los TS-usuarios y en uno o más árboles de control que se derivan de él.

b) **árbol intergrupo**: Árbol lógico de los LO para cada origen.

c) **árbol intragrupo**: Árbol lógico compartido de cada grupo local.

d) **árbol de control**: Árbol que atraviesan los paquetes de control para el control de errores.

e) **testigo**: Representa el derecho de un TS-usuario a transmitir datos en multidifusión. El TS-usuario que tiene un testigo se denomina SU. El TCN gestiona los testigos.

4 Abreviaturas

En esta Recomendación | Norma Internacional se utilizan los siguientes acrónimos para los protocolos ECTP.

ECTP-1	ECTP parte 1 (Rec. UIT-T X.606 | ISO/CEI 14476-1)
ECTP-2	ECTP parte 2 (Rec. UIT-T X.606.1 | ISO/CEI 14476-2)
ECTP-3	ECTP parte 3 (Rec. UIT-T X.607 | ISO/CEI 14476-3)
ECTP-4	ECTP parte 4 (Rec. UIT-T X.607.1 | ISO/CEI 14476-4)
ECTP-5	ECTP parte 5 (Rec. UIT-T X.608 | ISO/CEI 14476-5)
ECTP-6	ECTP parte 6 (Rec. UIT-T X.608.1 | ISO/CEI 14476-6)

En esta Recomendación | Norma Internacional se utilizan los siguientes acrónimos para los paquetes ECTP-5.

ACK	Acuse de recibo (*acknowledgment)*
CC	Confirmar creación de conexión (*connection creation confirm*)
CCC	Confirmar cambio de árbol de control (*control tree change confirm)*
CCR	Petición de cambio de árbol de control (*control tree change request)*
CR	Petición de creación de conexión (*connection creation request*)
CT	Petición de terminación de conexión (*connection termination request)*
DT	Datos (*data*)
JC	Confirmar ingreso tardío (*late join confirm)*
JR	Petición de ingreso tardío (*late join request)*
LR	Petición de egreso de usuario (*user leave request)*

NACK	Acuse de recibo negativo (*negative acknowledgement)*
PB	Sonda (*probe)*
PBACK	Acuse de recibo de sonda (*probe acknowledgment)*
RD	Datos de retransmission (*retransmission data)*
TC	Confirmar ingreso en árbol (*tree join confirm*)
TCC	Confirmar cambio de árbol (*tree change confirm)*
TCR	Petición de cambio de árbol (*tree change request)*
TDC	Confirmar delegación de árbol (*tree delegation confirm)*
TDR	Petición de delegación de árbol (*tree delegation request)*
TGC	Confirmar obtención de testigo (*token get confirm)*
TGR	Petición de obtención de testigo (*token get request)*
TJ	Petición de ingreso en árbol (*tree join request)*
TLC	Confirmar egreso de árbol (*tree leave confirm)*
TLR	Petición de egreso de árbol (*tree leave request)*
TNC	Confirmar notificación de cambio de árbol (*tree change notification confirm)*
TNR	Petición de notificación de cambio de árbol (*tree change notification request)*
TRC	Confirmar devolución de testigo (*token return confirm)*
TRR	Petición de devolución de testigo (*token return request)*
TSR	Informe de estado de testigo (*token status report)*
TSRR	Petición de informe de estado de testigo (*token status report request)*

5 Convenios

En esta Recomendación | Norma Internacional, los paquetes de ECTP-5 se representan como palabras en mayúsculas (por ejemplo, CR para paquete de petición de creación de conexión), y los parámetros de sistema se representan como palabras en mayúsculas y cursiva (por ejemplo, *TD_PACKET_INT* para el intervalo de paquetes de datos de prueba).

6 Panorama general

El protocolo perfeccionado de transporte de comunicaciones (ECTP, *enhanced communications transport protocol*) es un protocolo de transporte diseñado para soportar aplicaciones multidifusión en Internet que se ejecutan sobre redes con capacidad de multidifusión. ECTP funciona sobre redes IPv4/IPv6 con capacidad de transmisión IP multidifusión mediante protocolos de encaminamiento multidifusión IGMP e IP, tal como se muestra en la figura 1. Posiblemente ECTP se podría implementar sobre UDP.

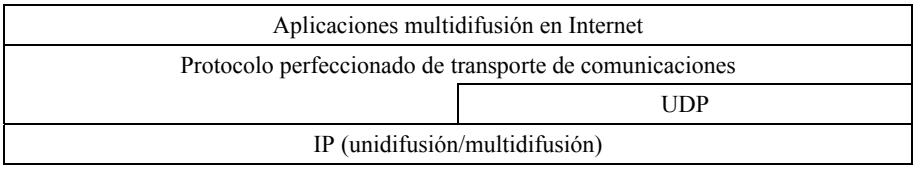

Figura 1 – Modelo ECTP

Esta Recomendación | Norma Internacional contiene la especificación de protocolo del ECTP parte 5 (ECTP-5) para la conexión de multidifusión N-plex. La conexión de multidifusión N-plex se utiliza para soportar el transporte de datos en multidifusión entre los participantes (TS-usuarios). En la conexión de multidifusión N-plex, los TS-usuarios pueden enviar paquetes de datos en multidifusión al grupo a través del canal de datos multidifusión. Un TS-usuario que envía datos en multidifusión a través de la conexión de multidifusión N-plex se denomina usuario emisor (SU, *sending TS-user*). Los SU deben tener un testigo para transmitir datos en multidifusión. En otras palabras, el TS-usuario que obtiene un testigo del TCN se denomina SU.

En la figura 2 se muestra el canal de transporte de datos multidifusión en la conexión de multidifusión N-plex. Como se ve, el TCN y el SU pueden transmitir datos en multidifusión a los demás miembros de la sesión a través de una dirección (de grupo) de multidifusión IP.

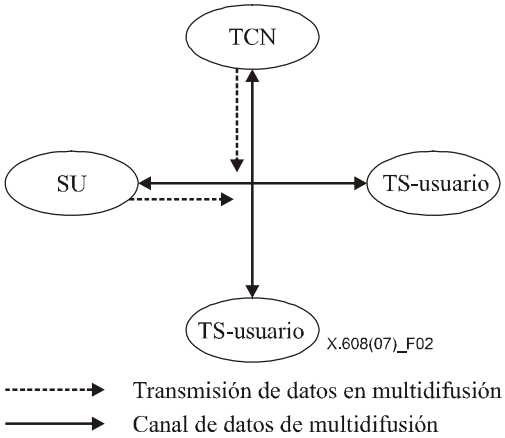

Figura 2 – Transporte de datos en multidifusión en la conexión de multidifusión N-plex

Para establecer una conexión de multidifusión N-plex, el TCN debe estar activado para gestionar la información de sesión y los testigos.

Si el TCN recibe una lista de participantes mediante señalización fuera de banda antes de empezar la conexión, debe iniciar la fase de creación de conexión transmitiendo un paquete CR al grupo. El paquete CR contiene la información de conexión, incluidas las características generales de la misma. Cada TS-usuario de la lista de participantes debe responder al TCN con un paquete CC. La operación de creación de conexión estará completada cuando el TCN reciba los paquetes CC de todos los TS-usuarios de la lista de participantes, y dará comienzo la fase de transmisión de datos. Si no hay participantes predeterminados antes de iniciarse la sesión, el TCN iniciará la fase de transmisión de datos sin realizar la operación de creación de conexión.

En medio de la fase de transmisión de datos, los TS-usuarios deben ingresar en la conexión indicando que lo hacen de manera tardía. Los TS-usuarios que ingresan tardíamente participan en la conexión enviando un mensaje petición de ingreso tardío (JR, *late join request*) al TCN. En respuesta al mensaje JR, el TCN envía un mensaje confirmar ingreso tardío (JC, *late join confirm*) al TS-usuario. Después de que se confirme el ingreso del TS-usuario en la sesión, deberá ingresar en un árbol lógico intercambiando los mensajes petición de ingreso en árbol (TJ, *tree join request*) y confirmar ingreso en árbol (TC, *tree join confirm*) con los LO correspondientes. El árbol lógico se utiliza para el control de errores.

Una conexión de multidifusión N-plex construye un árbol lógico de dos capas consistente en árboles intragrupo compartidos y árboles intergrupo por origen, como se muestra en la figura 3.

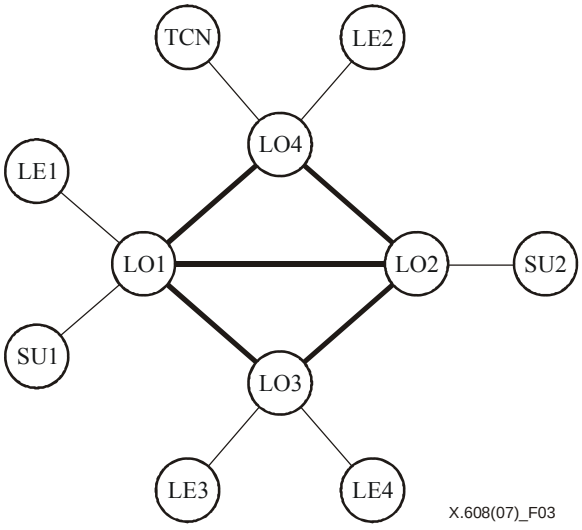

Figura 3 – Árbol de dos capas para la conexión de multidifusión N-plex

En la capa inferior, cada LE de un grupo local ingresa en un árbol lógico compartido cuya raíz es un LO (*árbol intragrupo*). En la capa superior, los LO constituyen árboles lógicos para cada SU (*árbol intergrupo*). Hay que señalar que el árbol de control de cada SU se deriva del cruce de los árboles intragrupo e intergrupo.

En la conexión de multidifusión N-plex, los árboles intragrupo pueden estar organizados de otra manera, dependiendo de las funciones de los LE, que están determinadas por la opción de configuración de árbol (TCO, *tree configuration option*). Una opción de la TCO es que todos los LE proceden directamente de los LO y no participan en el proceso de reparación y en las agregaciones ACK. Por tanto, de acuerdo con esta opción, los árboles intragrupo serán árboles de un solo nivel con raíz en un LO. La otra opción es que los LE procedan de otros LE. En este caso, los LE son responsables de soportar la fiabilidad de sus LE derivados y los árboles intragrupo pueden tener múltiples niveles. Por motivos de eficiencia del soporte de la fiabilidad, los árboles intragrupo multinivel deben estar lo más cerca posible del árbol de encaminamiento de multidifusión subyacente. La conexión de multidifusión N-plex adopta el mecanismo de adaptación de árbol lógico en este caso. Para ello se utilizan los mapas de bits con errores de los TS-usuarios. Un mapa de bits con errores representa el estado de entrega de paquetes, que indica el patrón de pérdidas de los paquetes de multidifusión. Cada TS-usuario envía su mapa de bits con errores a su progenitor con respecto a los datos en multidifusión del nodo raíz de su árbol intragrupo con mensajes ACK periódicos. Al comparar sus propios mapas de bits con errores y los de sus vástagos, un nodo decide si un vástago puede ser su vástago real en el árbol de encaminamiento de multidifusión subyacente o no. Si se determina que el nodo vástago no es su vástago real, el nodo cambia el árbol lógico delegando el vástago a su progenitor o a uno de sus otros vástagos. Tras múltiples modificaciones, el árbol intragrupo llegará a ser un árbol multinivel cercano al árbol de encaminamiento de multidifusión subyacente.

El control de errores se realizará de acuerdo con el árbol de control ECTP construido como se describe anteriormente. Si se detecta la pérdida de paquetes por un vacío en los números de secuencia de paquetes, un nodo vástago enviará un paquete NACK a su progenitor inmediatamente en unidifusión. El LO progenitor o el SU que reciba el paquete NACK retransmitirá un paquete de datos (RD, *retransmisión data*) al solicitante por unidifusión. Cada vástago genera un paquete ACK cada *ACK_GENERATION_NUM* (*AGN*) paquetes de datos.

En la transmisión de datos en multidifusión, el TCN y los SU pueden empezar la transmisión de datos al grupo utilizando la dirección de multidifusión IP y el número de puerto del grupo. Los TS-usuarios entregarán los paquetes DT recibidos a la aplicación de capa superior en el orden que los han transmitido los SU o el TCN.

Para el transporte de datos multidifusión, un TS-usuario de la conexión puede obtener un testigo del TCN enviándole un mensaje TGR. El TCN responderá al TS-usuario con un mensaje TGC que contenga un *ID de testigo*. Del mismo modo, el número total de testigos en la conexión está controlado por el TCN. El TS-usuario que tiene un testigo se denomina usuario emisor (SU). En algunos casos, puede ser el TCN quien pida al TS-usuario que se convierta en SU enviándole un mensaje TGR, lo que se denomina concesión de testigo.

Una vez terminada la transmisión de datos en multidifusión, el SU devolverá el testigo al TCN enviándole un mensaje TRR. El TCN responderá al SU con un mensaje TRC. En algunos casos, el TCN solicita al SU que devuelva el testigo, lo que se denomina retiro de testigo. El TCN anuncia el estado general de los ID de testigo válidos en la conexión al grupo enviando paquetes TSR.

El TCN gestiona el egreso de usuarios de la conexión. En la operación de egreso de usuarios, un TS-usuario participante puede dejar la conexión enviando un mensaje LR al progenitor. En algunos casos, el TCN puede obligar a un TS-usuario específico a abandonar la conexión enviándole un mensaje LR. Lo que se denomina expulsión de problemático.

El TCN puede terminar una conexión N-plex enviando un mensaje CT al grupo.

7 Consideraciones

7.1 Participantes

Todos los participantes en una conexión de multidifusión N-plex son TS-usuarios y uno de ellos es el TCN (TC-Propietario).

TCN (TC-Propietario):

Una conexión de multidifusión N-plex tiene un único TCN. El TCN es responsable de la gestión de la conexión, incluida la creación/terminación de la conexión, el ingreso tardío, el mantenimiento de la conexión y la gestión de los testigos.

Por ejemplo, en aplicaciones de teleconferencia, el TCN puede hacer las veces de 'servidor de conferencia', que puede utilizarse para el control de la conferencia sin enviar datos en multidifusión. En el ejemplo de las aplicaciones de 'juegos en línea multiusuario', el TCN puede ser el 'servidor de control de juego'.

TS-usuario (Usuario del servicio de transporte):

Una conexión de multidifusión N-plex tiene uno o más TS-usuarios. Cada uno de ellos envía y recibe datos en multidifusión a través de esta conexión.

Un TS-usuario puede convertirse en LO o LE, dependiendo de su función.

LO (Propietario local):

El LO es un nodo representativo de un grupo local y está designado estáticamente. Es responsable del mantenimiento de un árbol intragrupo del grupo y de los árboles de control de todos los SU de su grupo local. Cada LO está también conectado a los otros LO mediante los árboles intergrupo. Asimismo, genera periódicamente tráfico de prueba para la adaptación de árbol lógico.

LE (Entidad hoja):

El LE es un miembro de un grupo local cuyo representante es un LO. Debe ingresar en un árbol intragrupo del grupo y es responsable de intercambiar paquetes de control con sus LE progenitor o vástago en el árbol de control.

Un TS-usuario puede convertirse en SU cuando obtiene un testigo del TCN.

SU (TS-usuario emisor):

Un SU es un TS-usuario que puede enviar datos en multidifusión al grupo. En una conexión de multidifusión N-plex, un TS-usuario se convierte en SU cuando tiene un testigo y, así, puede transmitir datos en multidifusión al grupo.

7.2 Canal de datos y direccionamiento

En una conexión de multidifusión N-plex, el SU o el TCN pueden enviar paquetes de datos en multidifusión a los miembros de la sesión, como se muestra en la figura 4.

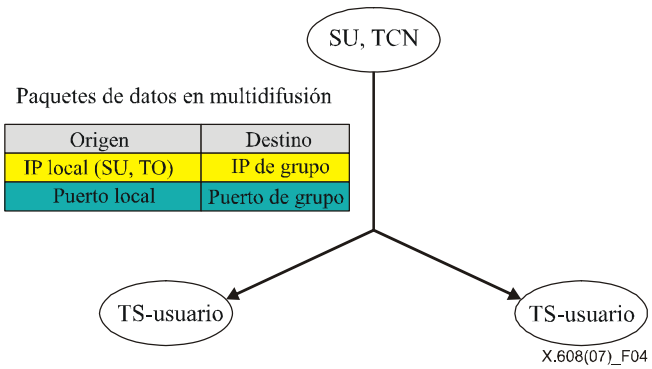

Figura 4 – Direccionamiento de datos en multidifusión en la conexión de multidifusión N-plex

En una conexión de multidifusión N-plex, los paquetes de datos en multidifusión (DT) utilizan la dirección de multidifusión IP y el número de puerto del grupo como dirección de destino. La dirección de origen de los paquetes IP de datos en multidifusión es la dirección IP del emisor de los paquetes. Por el contrario, los paquetes de datos de retransmisión (RD) en respuesta a las peticiones de reparación (NACK) son entregados por el LO o el SU a través del canal de control utilizando la unidifusión con la dirección IP del peticionario de reparación como destino.

7.3 Árbol y canal de control

En una conexión de multidifusión N-plex hay canales de control para la recuperación de errores. Todos los miembros participan en uno o más árboles de control. Estos árboles se utilizan como canales de control para el intercambio de mensajes de control entre los participantes. Un nodo progenitor actúa como agente que ayuda a los nodos vástagos a recuperar la pérdida de paquetes. También agrega la información de acuse de recibo de sus nodos descendientes. Todos los paquetes de control como RD, NACK y ACK se entregan por el canal de control utilizando la unidifusión.

Una conexión de multidifusión N-plex se divide en múltiples grupos locales de participantes para el control de errores. De acuerdo con éste método de grupo, los participantes construyen y mantienen los árboles de control a través de los cuales se intercambian los paquetes de control. Los árboles de control se construyen a partir de dos capas de árboles lógicos. En la capa inferior, los miembros de un grupo local ingresan en un árbol lógico compartido cuya raíz es un LO (*árbol intragrupo*). En la capa superior, los LO de los grupos forman los árboles lógicos por origen (*árbol intergrupo*).

Es decir, que todos los LE ingresan en un grupo local y se injertan en el árbol lógico del LO como vástagos (o descendientes) del LO. Todos los LO se injertan en el árbol lógico de los LO cuya raíz es el LO del grupo al que pertenece el SU. Se construye un árbol de control para cada origen conectando los árboles intergrupo y los árboles intragrupo.

Los árboles intergrupo se generan y mantienen sólo lo necesario. Los árboles intergrupo cuya raíz es un LO sin SU vástagos ha de eliminarse.

Los árboles intragrupo pueden evolucionar hacia árboles multinivel que reflejan los trayectos de encaminamiento de multidifusión reales mediante el mecanismo de adaptación de árbol lógico, que se detalla en 7.5.

Atravesando los árboles lógicos empezando por un SU, se puede obtener un árbol de SU, que es el árbol de control para ese SU.

Si un SU pertenece a otro grupo local, parte del árbol de control generado para el grupo local vigente es el árbol intragrupo del grupo. Los árboles de control para los SU pertenecientes al mismo grupo local son ligeramente diferentes de los árboles intragrupo, y a que los nodos intermedios entre el LO y el SU han invertido su relación progenitor-vástago.

Asumiendo que los árboles lógicos de los participantes se construyen como se muestra en la figura 5, el árbol de control del origen SU1 se construirá como se muestra en la figura 6.

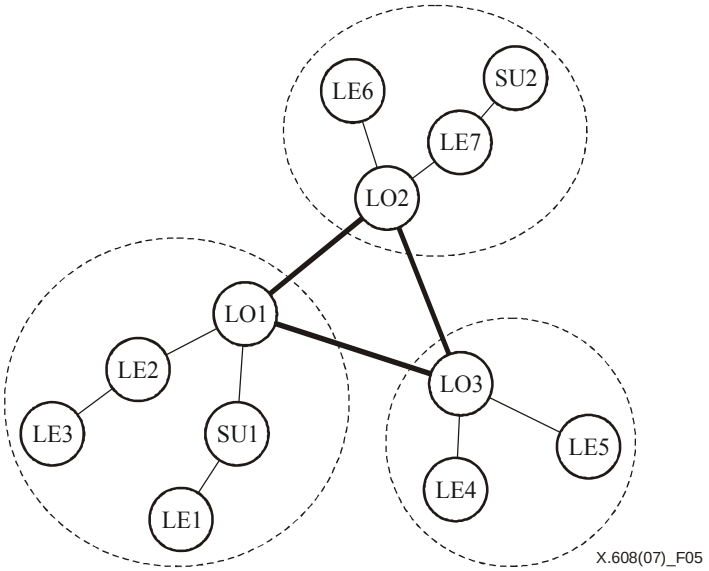

Figura 5 – Árboles lógicos de dos capas

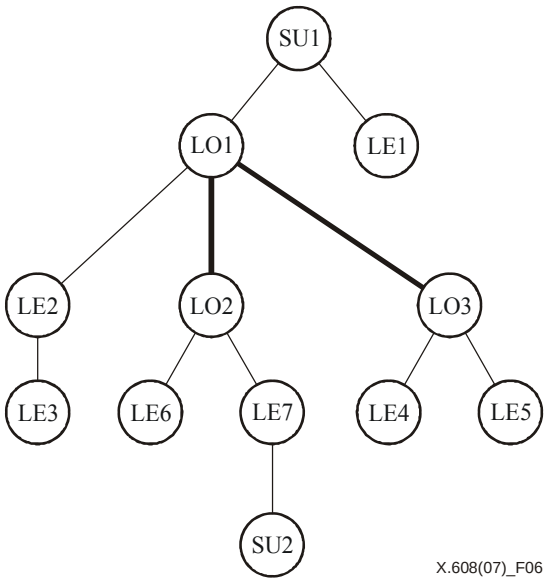

Figura 6 – Árbol de control cuando el emisor es SU1

Del mismo modo, en la figura 7 se muestra el árbol de control cuyo origen es SU2.

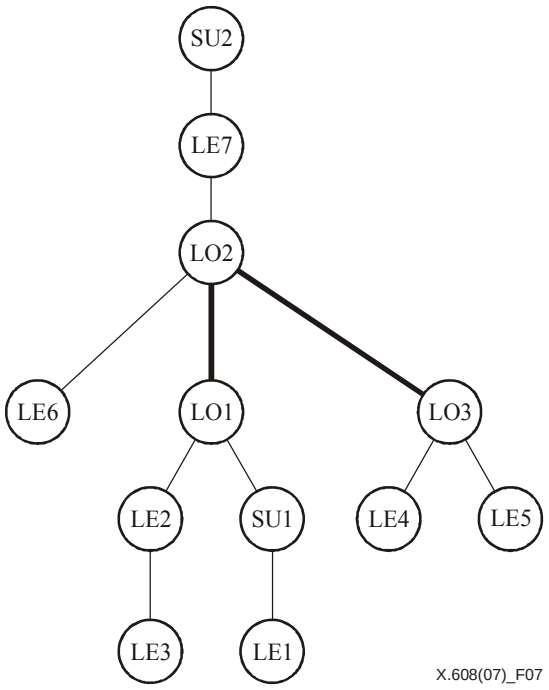

Figura 7 – Árbol de control cuando el emisor es SU2

Los árboles de control se mantienen gracias a la información obtenida mediante el intercambio de paquetes NACK y ACK. El progenitor puede detectar el fallo del vástago comparando su propio LSN y el LSN del vástago recibido. El vástago puede detectar el fallo de su progenitor si no obtiene respuestas de él a varias peticiones de reparación consecutivas. En ese caso, el vástago encuentra otro progenitor contactando con el LO.

7.4 Testigos

En una conexión de multidifusión N-plex, un testigo representa el derecho de un TS-usuario a enviar datos en multidifusión al TCN. Antes de transmitir los datos, cada TS-usuario ha de obtener un testigo del TCN, de acuerdo con los procedimientos de control de testigo de la conexión de multidifusión N-plex. Mediante este procedimiento, el TCN puede autorizar a un TS-usuario a convertirse en emisor de manera que los TS-usuarios puedan filtrar efectivamente los datos en multidifusión enviados por usuarios no autorizados. No obstante, hay que indicar que la utilización de testigos no supone una protección para la multidifusión IP.

Cada testigo está representado por un entero no negativo de un byte. Este número de testigo (o ID de testigo) será asignado por el TCN cuando un TS-usuario solicite un testigo en la conexión. El ID de testigo oscila entre 1 y 255. El ID de testigo '0' se reserva para utilización por el TCN. En el lado receptor, el ID de testigo puede utilizarse para autorizar quién puede enviar datos en multidifusión.

7.5 Adaptación de árbol lógico

En la conexión de multidifusión N-plex, los árboles intragrupo pueden evolucionar hacia árboles multinivel cercanos a los árboles de encaminamiento de multidifusión subyacentes cuando la TCO es '10'. Se utiliza la comparación del patrón de pérdida para estimar los árboles de encaminamiento de multidifusión subyacentes. La estimación es posible porque, si ocurre una pérdida en un nodo progenitor de un árbol de encaminamiento de multidifusión, todos sus vástagos sufrirán la misma pérdida. El proceso de adaptación de árbol lógico no modifica la raíz del árbol intragrupo.

Para ello, los receptores de una sesión de multidifusión mantendrán el estado de entrega de los paquetes denominado mapa de bits con errores, que indica el patrón de pérdida de paquetes de multidifusión. Un mapa de bits con errores está formado por dos partes: un número de secuencia (*Ns*) y el mapa de bits real (*B*). *Ns* es el número de secuencia del primer paquete de una secuencia de paquetes representada en el mapa de bits. Un bit de *B* indica el estado de recepción del paquete correspondiente; '1' significa que el paquete se ha entregado satisfactoriamente al receptor sin recuperación de errores y '0' cualquier otro caso. El mapa de bits incluye los patrones de pérdida de los paquetes de multidifusión. Por ejemplo, si $Ns = 5$ y $B = 11010$, el receptor ha recibido satisfactoriamente los paquetes 5, 6 y 8. Aunque los paquetes 7 y 9 se hayan recuperado gracias a retransmisiones, estos bits se ponen a '0'. Los receptores remiten periódicamente la

información del mapa de bits con errores a su progenitor en el árbol. Si el árbol lógico coincide con un árbol de encaminamiento de multidifusión y un bit del mapa de bits con errores está puesto a 1, con mucha probabilidad el bit correspondiente del mapa de bits con errores de su progenitor sea '1'. Cabe señalar que el mapa de bits con errores del origen siempre es todo '1'.

Todo nodo que tiene nodos vástagos compara su propio mapa de bits con errores y los de sus vástagos para verificar si la relación entre el nodo y sus vástagos refleja el árbol de encaminamiento de multidifusión subyacente. Un nodo progenitor puede inferir que algunos nodos vástagos han de modificar su ubicación en el árbol lógico. El nodo vástago sería vástago de otro nodo vástago, o no sería descendiente del nodo progenitor.

Por ejemplo, en la figura 8 se muestra un ejemplo de árbol de encaminamiento de multidifusión y los mapas de bits con errores de cada nodo.

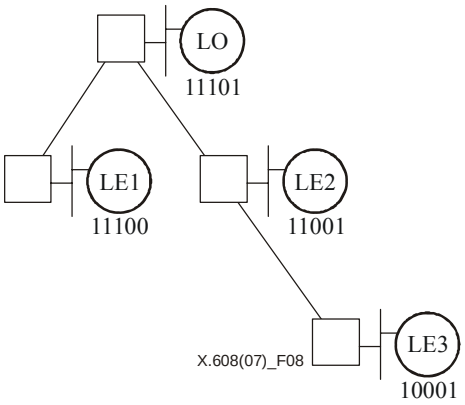

Figura 8 – Ejemplo de árbol de encaminamiento de multidifusión

En las figuras 9 y 10 se describe brevemente cómo se construye un árbol lógico cercano a un árbol de encaminamiento de multidifusión gracias a la información del mapa de bits con errores.

En primer lugar, se asume que un LO raíz es un servidor implantado estratégicamente que normalmente está ubicado cerca del punto de egreso del proveedor de servicios Internet. Los recuadro representan encaminadores y los números debajo de los nodos son los mapas de bits con errores de cada nodo.

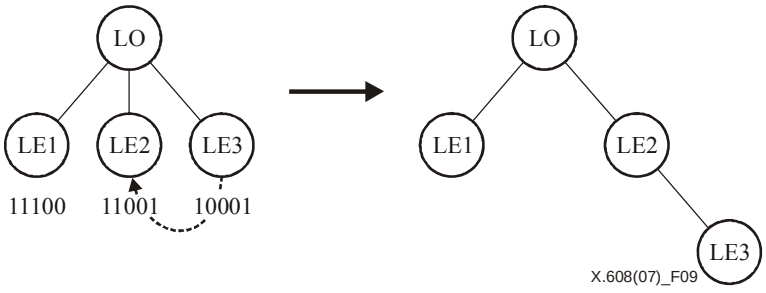

Figura 9 – Adaptación de árbol lógico (LE2 adopta LE3)

En la parte izquierda de la figura 9 se ve un árbol intragrupo de un nivel inicial de los nodos de la figura 8. Cuando el LO tiene conocimiento de los mapas de bits con errores de sus vástagos, ve que es probable que LE3 sea vástago o descendiente de LE2, ya que un conjunto de los paquetes recibidos de LE3 es un subconjunto de los de LE2. Por tanto, delega LE3 a LE2 enviando un mensaje TDR (petición de delegación de árbol). Al recibir el mensaje TCR, LE3 ingresa como vástago de LE2 enviándole el mensaje TJ y abandona a su anterior progenitor, LO, enviándole el mensaje TLR. Hay que indicar que un nodo que recibe un mensaje TCR está vinculado al nuevo progenitor antes de abandonar al anterior. El resultado es el árbol de la parte derecha de la figura 9.

En la figura 10 se ve otro ejemplo de adaptación de árbol lógico.

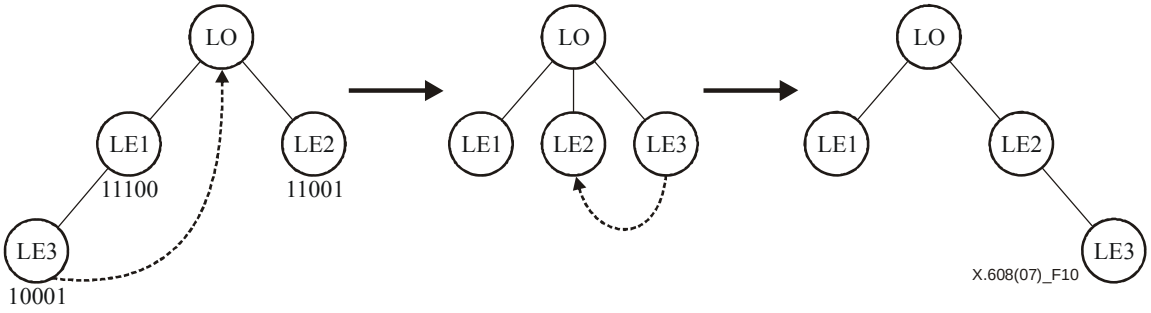

Figura 10 – Adaptación de árbol lógico (LO adopta LE3; LE2 adopta LE3)

En la parte izquierda de la figura 10, LE3 se ha convertido en vástago de LE1 por una adaptación de árbol lógico errónea. No obstante, el mapa de bits con errores actual de LE3 indica que LE3 no es vástago de LE1, ya que ha recibido un paquete que no ha recibido LE1. En este caso, LE1 delega LE3 a su progenitor, LO, para que encuentre la ubicación correcta de LE3 enviándole un mensaje TDR. LO recibe el mensaje TDR de LE1 acerca de LE3 y compara los mapas de bits con errores de LE3 con los de sus vástagos LE1 y LE2. El LO encuentra que es probable que LE3 sea vástago de LE2. Por ultimo, el árbol lógico se convierte en el árbol de la parte derecha de la figura 10.

De esta manera, los árboles intragrupo pueden evolucionar hacia árboles multinivel que se aproximan a los árboles de encaminamiento de multidifusión subyacentes. Los árboles de control construidos a partir de estos árboles intragrupo también serán muy parecidos a los árboles de encaminamiento de multidifusión.

Para ello, el LO envía paquetes DATA de prueba cuando detecta un cambio en el árbol intragrupo. Entonces, los LE de un grupo local construyen la información del mapa de bits con errores y la envían en un paquete ACK. Los paquetes DATA de prueba no están destinados a ninguna aplicación y deben enviarse cada *TD_PACKET_INT* y *TD_PACKET_NUM* veces.

8 Paquetes

Un paquete ECTP contiene un encabezamiento de 16 bytes y elementos de extensión o datos de usuario. Hay que señalar que los paquetes de datos (DT) no contienen elementos de extensión. En la figura 11 se muestra el formato genérico de los paquetes ECTP-5:

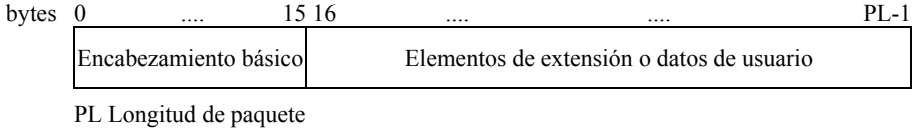

Figura 11 – Formato de los paquetes ECTP-5

8.1 Encabezamiento básico

El encabezamiento básico de 16 bytes contiene información común útil para todas las operaciones del protocolo, en concreto para los paquetes de datos. En la figura 12 se ve la estructura del encabezamiento básico cuando ECTP se utiliza con el IP.

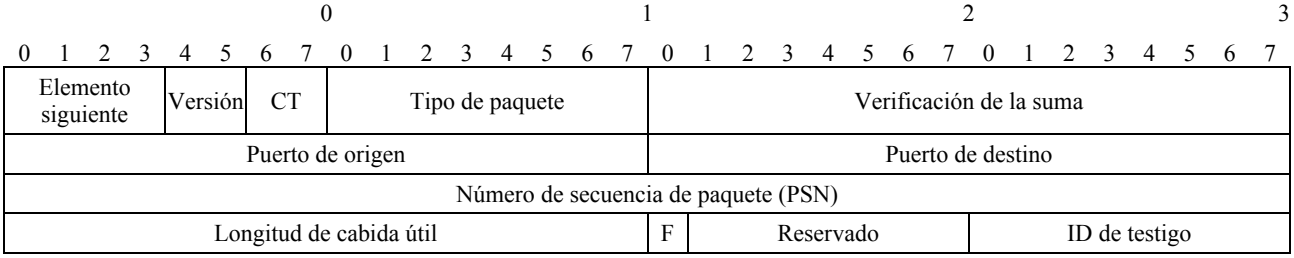

Figura 12 – Encabezamiento básico (ECTP sobre IP)

El encabezamiento básico contiene la siguiente información:

Elemento siguiente (4 bits)

Especifica el tipo de elemento de extensión que sigue inmediatamente al encabezamiento básico. Los valores de codificación de los elementos de extensión se describen a continuación. Un valor de elemento de extensión de '0000' significa que no hay más elementos de extensión después de este elemento.

Versión (2 bits)

Define la versión del protocolo para esta Recomendación | Norma Internacional. La versión actual se codifica como '00'.

CT (Tipo de conexión) (2 bits)

Especifica el tipo de conexión ECTP. Los valores de codificación son los siguientes:

01 – conexión de multidifusión símplex (para ECTP-1 y ECTP-2);

10 – conexión de multidifusión dúplex (para ECTP-3 y ECTP-4);

11 – conexión de multidifusión N-plex (para ECTP-5 y ECTP-6).

En esta Recomendación | Norma Internacional, *CT* debe ponerse a '11'.

Tipo de paquete (8 bits)

Indica el tipo del paquete.

Verificación de suma (16 bits)

Se utiliza para verificar la validez del paquete que incluye el encabezamiento básico, el encabezamiento de extensión y/o los datos de usuario. La verificación de suma se calcula utilizando la operación aritmética con complemento a uno convencional, igual que se hace en TCP y UDP.

Puerto de origen (16 bits) y *puerto de destino* (16 bits)

Estos números de puerto se utilizan para identificar las aplicaciones emisoras y receptoras cuando ECTP se utiliza sobre IP. Cuando ECTP se utiliza sobre UDP, estos campos se emplean para representar el identificador de conexión, como se describe más adelante.

PSN (32 bits)

Para los paquetes DT, esta campo es un número de 32 bits sin signo que comienza con el número de secuencia inicial y se incrementa en '1' por cada paquete y vuelve a '1' tras alcanzar el valor '$2^{32} – 1$'.

Para los paquetes ACK, este campo es el LSN de un SU con *ID de testigo*.

Para los paquetes RD, este campo es el PSN de los paquetes de datos, que se ha de retransmitir.

Para los paquetes TJ, TLR, JR, TGR, TRR, TCR, TDR, TNR y CCR, este campo es el número de secuencia de los paquetes de control de un nodo. Debe ser exclusivo dentro del mismo tipo de paquetes enviado por el nodo.

Para los paquetes TC, TLC, JC, TGC, TRC, TCC, TDC, TNC y CCC, este campo es una copia del campo *PSN* del correspondiente paquete petición.

Para los demás paquetes, este campo ha de ignorarse.

Longitud de cabida útil (16 bits)

Este valor indica la longitud total de los encabezamientos de extensión o los datos de usuario en bytes, después del encabezamiento básico.

F (1 bit)

Se trata de un bit de bandera. La utilización de esta bandera depende del tipo de paquete:

Para los paquetes JC, TC, TGC, TCC, TDC, TRC y TLC, el campo F = 1 indica que se aceptan cada una de las peticiones de ingreso correspondientes. En cualquier otro caso, F se pone a 0.

Para los paquetes TJ y TLR, el campo F se pone a '1' para el ingreso o egreso de un árbol intergrupo, o se pone a '0' para el ingreso o egreso de un árbol intragrupo, respectivamente.

Para el paquete LR, el campo F se pone a '1' para el egreso invocado por el usuario, o se pone a '0' para la expulsión de problemático.

Para el paquete CT, el campo F se pone a '1' para una terminación anormal, o se pone a '0' para la terminación normal después de que se hayan transmitido todos los datos.

Para las operaciones de control de testigo, los mensajes de petición TGR y TRR utilizan esta bandera para indicar si se trata del control de testigo iniciado por el TCN o por el TS-usuario.

Para el paquete TSR, el campo F = 1 indica que se ha modificado el estado general de testigo por la adición de un nuevo testigo o la supresión de un testigo existente. Por otra parte, el campo F = 0 significa que este paquete TSR es para información.

Para el paquete TNR, el campo F se pone a '1' para el ingreso en árbol, o se pone a '0' para el egreso de árbol.

Para el paquete DT, el campo F se pone a '1' para los DT de prueba del LO para la adaptación de árbol lógico, o se pone a '0' para los DT de aplicaciones normales.

Para el paquete RD, el campo F se pone a '1' so el emisor no tiene datos que reparar, y se pone a '0' en cualquier otro caso.

Para los demás paquetes, este campo se ignorará.

Reservado (7 bits)

ID de testigo (8 bits)

El ID de testigo es válido sólo para los paquetes DT y RD. Representa el origen de los paquetes de datos. El valor del ID de testigo oscila entre 0 y 255. Cada SU recibe un ID de testigo del TCN siguiendo el procedimiento de obtención y concesión de testigo y este campo se pone al número asignado por el TCN.

Por otra parte, cuando ECTP se utiliza sobre UDP, el encabezamiento del paquete no necesita especificar los puertos de origen y destino, a los que se hará referencia en el encabezamiento UDP. En este caso, el campo de 32 bits para los puertos de origen y destino se rellenará con el '*ID de conexión*'. Por defecto, puede configurarse para que sea la dirección de grupo IPv4.

El formato del encabezamiento básico para ECTP sobre UDP se muestra en la figura 13.

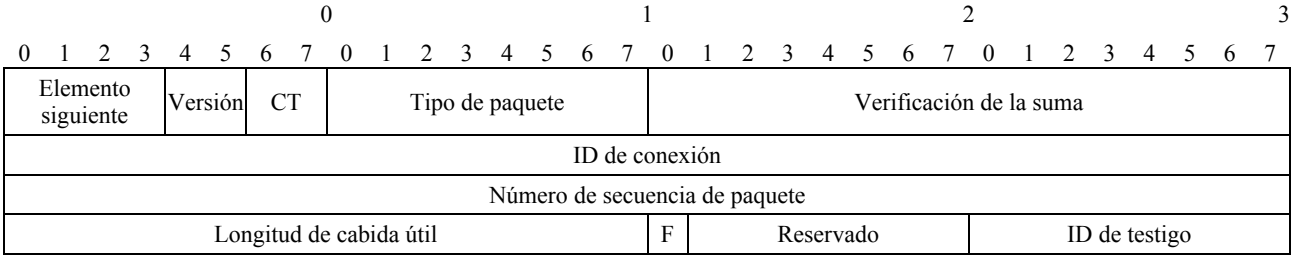

Figura 13– Encabezamiento básico (ECTP sobre UDP)

El *ID de conexión* se utiliza para que el anfitrión ECTP pueda identificar una conexión ECTP. También puede utilizarse para verificar la conexión. En la fase de establecimiento de la conexión, esta información debe ser transmitida en primer lugar por el TCN a los demás participantes mediante los paquetes CR o JC. Todos los demás paquetes de esta Recomendación | Norma Internacional deben poner este campo al valor anunciado por el TCN.

8.2 Elementos de extensión

Los paquetes de control ECTP pueden contener uno o más elementos de extensión además del encabezamiento básico. El campo 'elemento siguiente' del encabezamiento básico y de cualquier elemento de extensión habrá de señalar al elemento de extensión inmediatamente siguiente, de haberlo.

El campo elemento siguiente se codifica como se muestra en el cuadro 1. El ultimo elemento de extensión de un paquete debe poner su campo encabezamiento siguiente a '0000' (ningún elemento).

Cuadro 1 – Elementos de extensión

Elemento de extensión	Valor de codificación de elemento siguiente en el elemento precedente (4 bits)	Longitud del elemento de extensión (bytes)
Ningún elemento	0000	0
Conexión	0001	4
Mapa de bits con errores	0010	Variable
Indicación de tiempo	0100	12
Testigo	0110	Variable
Información de LO	0111	Variable
Acuse de recibo negativo	1000	8
Información de cambio de árbol	1001	8

8.2.1 Elemento Conexión

El elemento de extensión conexión contiene toda la información sobre la conexión de transporte. Se codifica como '0001' en el campo elemento siguiente del elemento precedente o el encabezamiento básico. El elemento de extensión ha de ir incluido en los paquetes CR, JC y TGR. El elemento tiene la estructura que se muestra en la figura 14 y tiene una longitud de '4' bytes:

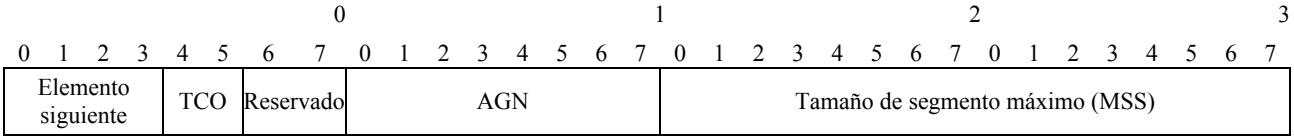

Figura 14 – Elemento de extensión Conexión

Los campos se especifican de la siguiente manera:

Elemento siguiente (4 bits)

Indica el tipo del elemento de extensión siguiente, como se indica en el cuadro 1.

TCO (Opción de configuración de árbol) (2 bits)

Especifica la opción de configuración de árbol que utiliza ECTP-5, de la siguiente manera:

00 – Reservado para utilización futura.

01 – Árbol intragrupo de un nivel sin adaptación de árbol lógico.

10 – Árbol intragrupo multinivel con adaptación de árbol.

11 – Reservado para utilización futura.

El valor por defecto de *TCO* es '10' en la conexión de multidifusión N-plex.

Reservado (2 bits)

AGN (Número de generación de ACK) (8 bits)

Se trata de un entero positivo entre 1 y 255 (*ACK_GENERATION_NUM*). El *AGN* es utilizado por un TS-usuario vástago para generar y transmitir un paquete ACK a su progenitor.

MSS (16 bits)

Especifica el tamaño máximo (en bytes) del segmento de datos de usuario (*MAX_SEGMENT_SIZE*) que puede contener un paquete DT. El valor por defecto es '1024'.

8.2.2 Elemento mapa de bits con errores

Este elemento de extensión proporciona información sobre el estado de la recepción de paquetes de un nodo vástago. Este encabezamiento de extensión va anexo a un paquete ACK en respuesta al tráfico de prueba del LO para la adaptación de árbol lógico que se describe en 7.5. Se codifica como '0010' en el campo elemento siguiente del elemento precedente o el encabezamiento básico.

Este elemento está formado por 4 bytes fijos y el *Mapa de bits con errores* de tamaño variable, como se muestra en la figura 15.

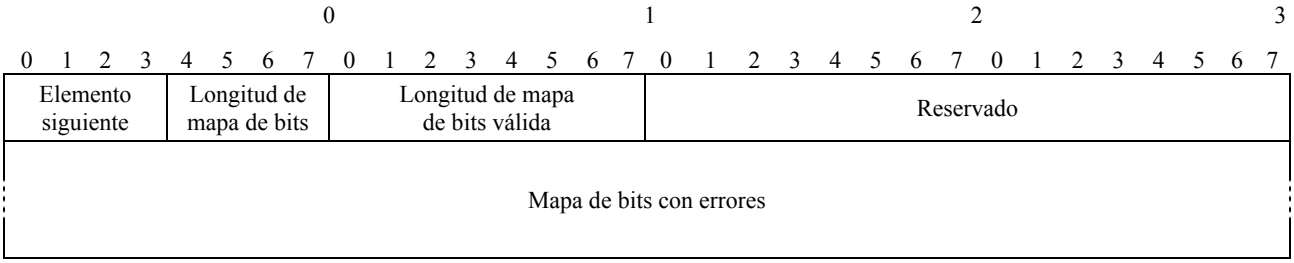

Figura 15 – Elemento de extensión mapa de bits con errores

Los campos se especifican de la siguiente manera:

Elemento siguiente (4 bits)

Indica el tipo del elemento de extensión siguiente, como se indica en el cuadro 1.

Longitud de mapa de bits (4 bits)

Especifica el tamaño total del *Mapa de bits ACK* en unidades de palabra (4 bytes).

Longitud de mapa de bits válida (8 bits)

Representa la longitud de la porción realmente válida en 'bits' para el *Mapa de bits ACK*.

Reservado (16 bits)

Mapa de bits con errores (variable)

Representa la información utilizando '0' o '1' para indicar los paquetes de datos que se han recibido (1) o perdido (0) en el lado receptor. En el *Mapa de bits con errores*, la información del mapa de bits comienza con el número de secuencia *LSN*, que representa el número de secuencia del paquete DT con un número más bajo que no se ha recibido aún en el lado receptor. El *LSN* se especificará en el campo PSN del encabezamiento básico. El *Mapa de bits con errores* contiene la información total del mapa de bits del tamaño de *Longitud de mapa de bits válida*.

8.2.3 Elemento Indicación de tiempo

El elemento Indicación de tiempo se codifica como '0100' en el campo elemento siguiente del elemento precedente o del encabezamiento básico. ECTP-5 utiliza la indicación de tiempo de 8 bytes para poder calcular el *Tiempo de ida y vuelta* (*RTT, round trip time*).

El formato del elemento de extensión Indicación de tiempo de 12 bytes se muestra en la figura 16.

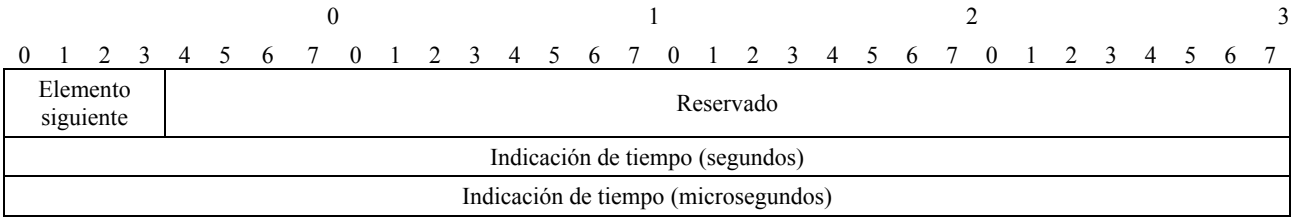

Figura 16 – Elemento de extensión Indicación de tiempo

Los campos se especifican de la siguiente manera:

Elemento siguiente (4 bits)

Indica el tipo del elemento de extensión siguiente, como se indica en el cuadro 1.

Reservado (28 bits)

Indicación de tiempo (64 bits)

Contiene un valor de indicación de tiempo de 8 bytes. Los primeros 4 bytes representan el valor de tiempo en segundos, y los últimos 4 bytes en microsegundos, como ocurre en el programa ping convencional.

8.2.4 Elemento Testigo

Este elemento de extensión proporciona información sobre el estado de los testigos que se están utilizando en la conexión. Este encabezamiento de extensión va anexo al paquete TSR. Se codifica como '0110' en el campo elemento siguiente del elemento precedente o el encabezamiento básico.

Este elemento está formado por 2 bytes fijos y los *ID de testigo válidos* de tamaño variable, como se muestra en la figura 17.

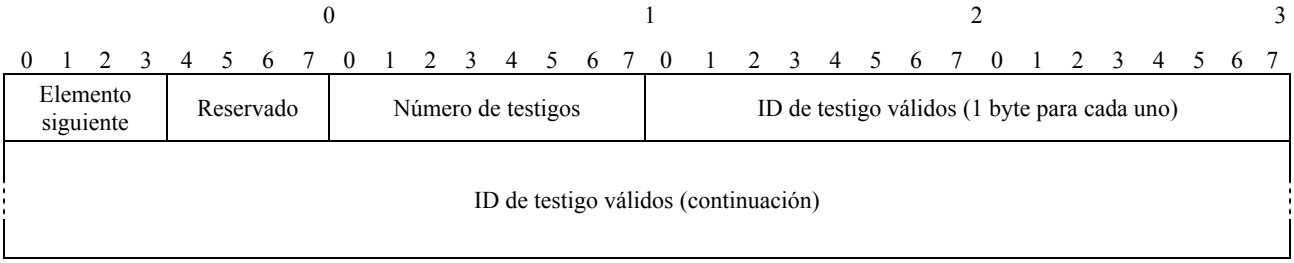

Figura 17 – Elemento de extensión Testigo

Los campos se especifican de la siguiente manera:

Elemento siguiente (4 bits)

Indica el tipo del elemento de extensión siguiente, como se indica en el cuadro 1.

Reservado (4 bits)

Número de testigos (8 bits)

Especifica el número total de *ID de testigo válidos* en la conexión.

ID de testigo válidos (variable)

Contiene la lista de ID de testigo válidos en la conexión. Cada *ID de testigo* tiene una longitud de 1 byte.

8.2.5 Elemento Información de LO

Este elemento de extensión proporciona información sobre un LO y sus correspondientes ID de testigo. Con esta información, un LO puede reconocer a su LO progenitor en el árbol intergrupo hacia un SU. Este encabezamiento de extensión va anexo a los paquetes TSR, TGR y TGC. Se codifica como '0111' en el campo elemento siguiente del elemento precedente o el encabezamiento básico. Este elemento está formado por 8 bytes fijos y los ID de testigo correspondientes de tamaño variable, como se muestra en la figura 18.

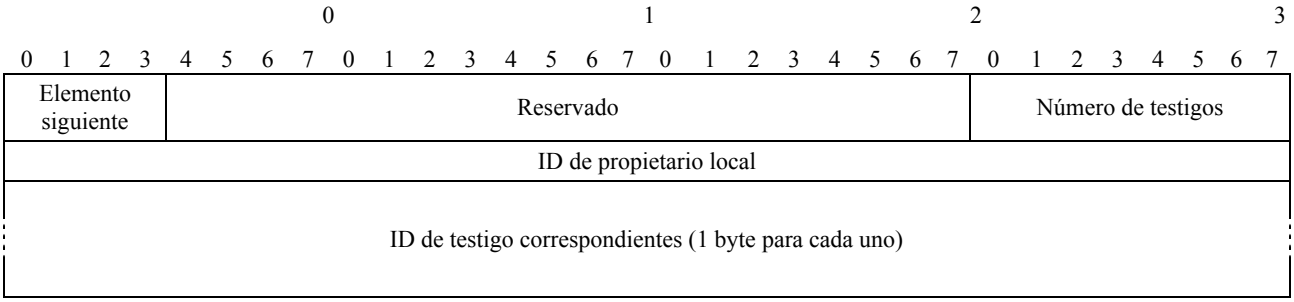

Figura 18 – Elemento de extensión Información de LO

Los campos se especifican de la siguiente manera:

Elemento siguiente (4 bits)

Indica el tipo del elemento de extensión siguiente, como se indica en el cuadro 1.

Reservado (20 bits)

Número de testigos (8 bits)

Especifica el número total de *ID de testigos correspondientes* para el LO cuyo ID es ID de propietario local.

ID de propietario local (32 bits)

Indica el ID del LO en el que ingresan los SU de los *ID de testigo correspondientes*. Este ID puede asignarse con un fin específico de la aplicación.

ID de testigo correspondientes (variable)

Contiene la lista de ID de testigo correspondientes al *ID de propietario local* en la conexión. Cada *ID de testigo* tiene una longitud de 1 byte.

8.2.6 Elemento Acuse de recibo negativo

Este elemento de extensión proporciona información sobre la petición de reparación de los paquetes DT perdidos por un nodo vástago. Si un LE o un LO detecta una o más pérdidas de DT, pide la reparación del/de los paquete(s) perdido(s) a su LE o LO progenitor en el árbol de control. En el caso de que se detecte la pérdida consecutiva de múltiples paquetes, el LE o el LO pueden pedir la reparación de un bloque de paquetes perdidos con un único paquete NACK que contiene el número de secuencia inicial y el número de paquetes perdidos consecutivamente.

Este encabezamiento de extensión va anexo al paquete NACK. Se codifica como '1000' en el campo elemento siguiente del elemento precedente o el encabezamiento básico. Este elemento está formado por 8 bytes fijos, como se muestra en la figura 19.

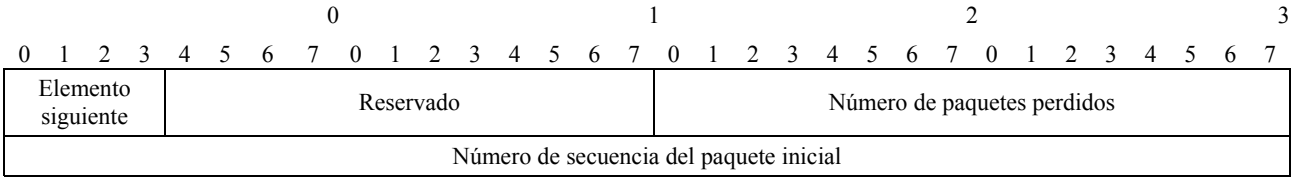

Figura 19 – Elemento de extensión Acuse de recibo negativo

Los campos se especifican de la siguiente manera:

Elemento siguiente (4 bits)

Indica el tipo del elemento de extensión siguiente, como se indica en el cuadro 1.

Reservado (12 bits)

Número de paquetes perdidos (16 bits)

Especifica el número de paquetes perdidos consecutivamente a partir del *Número de secuencia del paquete inicial*. Si se trata de una petición para un solo paquete perdido, este campo se pone a '1'.

Número de secuencia del paquete inicial (32 bits)

Especifica el número de secuencia del paquete inicial de un bloque de paquetes perdidos. Si se trata de una petición para un solo paquete perdido, este campo se pone al PSN del paquete perdido.

Se genera un paquete NACK para los paquetes de datos de un SU. El campo ID de testigo del encabezamiento básico del paquete NACK identifica el emisor asociado de los paquetes perdidos.

8.2.7 Elemento Información de cambio de árbol

Este elemento de extensión proporciona información sobre un cambio en el árbol intragrupo. Representa un cambio en un árbol intragrupo con respecto al emisor y al nodo con el *ID de nodo.* Este encabezamiento de extensión va anexo a los paquetes TCR, TDR, TNR y CCR. Se codifica como '1001' en el campo Elemento siguiente del elemento precedente o el encabezamiento básico. Este elemento está formado por 8 bytes fijos.

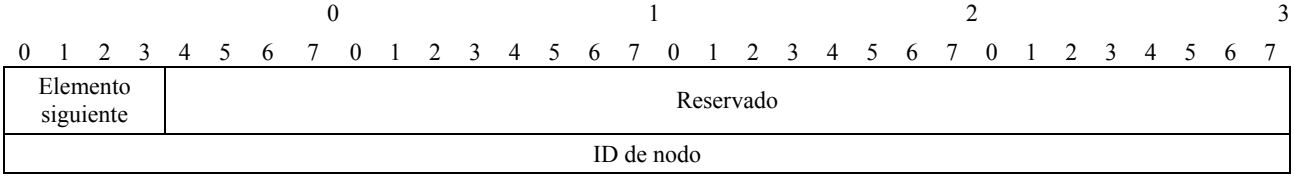

Figura 20 – Elemento de extensión Información de cambio de árbol

Los campos se especifican de la siguiente manera:

Elemento siguiente (4 bits)

Indica el tipo del elemento de extensión siguiente, como se indica en el cuadro 1.

Reservado (28 bits)

ID de nodo (32 bits)

Especifica el ID de un nodo para el que se ha de cambiar el árbol intragrupo. El contexto del cambio depende del tipo de paquete.

8.3 Formato de paquetes

En esta Recomendación | Norma Internacional, hay un total de 30 tipos de paquetes: 2 tipos de paquetes de datos y 28 tipos de paquetes de control. Los paquetes de datos son DT y RD.

Cuadro 2 – Paquetes ECTP-5

Nombre completo	Acrónimo	Transporte	Desde	Hacia
Petición de creación de conexión	CR	Multidifusión	TCN	TS-usuarios
Confirmar creación de conexión	CC	Unidifusión	TS-usuario	TCN
Petición de ingreso en árbol	TJ	Unidifusión	LELO	LE/LO
Confirmar ingreso en árbol	TC	Unidifusión	LE/LO	LE/ LO
Petición de egreso de árbol	TLR	Unidifusión	LE/LO	LE/LO
Confirmar egreso de árbol	TLC	Unidifusión	LE/LO	LE/LO
Datos	DT	Multidifusión	TCN/SU/LO	TS-usuarios
Datos de retransmisión	RD	Unidifusión	LE/LO	LE/LO
Acuse de recibo	ACK	Unidifusión	LE/LO	LE/LO
Acuse de recibo negativo	NACK	Unidifusión	LE/LO	LE/LO
Sonda	PB	Unidifusión	TCN	TS-usuario
Acuse de recibo de sonda	PBACK	Unidifusión	TS-usuario	TCN
Petición de ingreso tardío	JR	Unidifusión	TS-usuario	TCN
Confirmar ingreso tardío	JC	Unidifusión	TCN	TS-usuario
Petición de egreso de usuario	LR	Unidifusión	TCN TS-usuario	TS-usuario TCN
Petición de terminación de conexión	CT	Multidifusión	TCN	TS-usuario
Petición de obtención de testigo	TGR	Unidifusión	SU TCN	TCN SU
Confirmar obtención de testigo	TGC	Unidifusión	TCN SU	SU TCN
Petición de devolución de testigo	TRR	Unidifusión	TS-usuario TCN	TCN TS-usuario
Confirmar devolución de testigo	TRC	Unidifusión	TCN TS-usuario	TS-usuario TCN
Informe de estado de testigo	TSR	Multidifusión Unidifusión	TCN TCN	TS-usuarios TS-usuario
Petición de informe de estado de testigo	TSRR	Unidifusión	TS-usuario	TCN
Petición de cambio de árbol	TCR	Unidifusión	LO/LE	LE
Confirmar cambio de árbol	TCC	Unidifusión	LE	LO/LE
Petición de delegación de árbol	TDR	Unidifusión	LO/LE	LO/LE
Confirmar delegación de árbol	TDC	Unidifusión	LO/LE	LO/LE
Petición de notificación de cambio de árbol	TNR	Unidifusión	LE	LO
Confirmar notificación de cambio de árbol	TNC	Unidifusión	LO	LE
Petición de cambio de árbol de control	CCR	Unidifusión	LO	LE
Confirmar cambio de árbol de control	CCC	Unidifusión	LE	LO

En el cuadro 3 se muestran los valores de codificación y la estructura de los paquetes ECTP-5. Los elementos de extensión van anexos al encabezamiento básico en el orden especificado.

Cuadro 3 – Formato de los paquetes ECTP-5

Tipo de paquete	Valor de codificación	Elementos de extensión o datos de usuario (estructura de paquetes)	Longitud (bytes)	Fase operacional del protocolo
CR	0000 0001	Conexión	20	Creación de conexión
CC	0000 0010		16	
TJ	0000 0011	Indicación de tiempo	28	Gestión del árbol lógico
TC	0000 0100	Indicación de tiempo	28	
TLR	0010 0011		16	
TLC	0010 0100		16	
DT	0000 0101	Datos de usuario	16+	Transporte de datos
RD	0000 0111	Indicación de tiempo + *Datos de usuario*	28+	Control de errores
ACK	0000 1000	*Mapa de bits con errores*	16+	
NACK	0001 1000	Acuse de recibo negativo + Indicación de tiempo	36	
PB	0000 1001		16	Gestión de miembros
PBACK	0000 1110		16	
JR	0000 1010		16	Ingreso tardío
JC	0000 1011	Conexión	20	
LR	0000 1100		16	Egreso de usuario
CT	0000 1101		16	Terminación
TGR	0001 0001	Información de LO	16+	Obtención de testigo
TGC	0001 0010	Información de LO	16+	
TRR	0001 0011		16	Devolución de testigo
TRC	0001 0100		16	
TSR	0001 0101	*Testigo + Información de LO*	16+	Informe de testigo
TSRR	0010 0101		16	
TCR	0001 0110	Información de cambio de árbol	24	Adaptación de árbol lógico
TCC	0001 0111		16	
TDR	0001 1110	Información de cambio de árbol + Mapa de bits con errores	24+	
TDC	0001 1111		16	
TNR	0010 0001	Información de cambio de árbol	24	Gestión de árbol de control
TNC	0010 0010		16	
CCR	0010 1000	Información de cambio de árbol	24	
CCC	0010 1001		16	

La cursiva (en los elementos de extensión) indica que la utilización del correspondiente elemento de extensión es opcional, en vez de obligatoria. En la columna longitud de paquete, el símbolo '+' significa que el paquete puede tener mayor tamaño si se le añaden los elementos opcionales o datos de usuario especificados.

Por otra parte, los siguientes valores de codificación se reservan para utilización futura: '0000 0000', '0000 1111', '0001 0000', '0010 0000' y '0000 0110'.

8.3.1 Petición de creación de conexión (CR, *connection creation request*)

El TCN utiliza el paquete CR para crear una conexión de multidifusión N-plex. El TCN envía el paquete CR al grupo con las siguientes direcciones de origen y destino:

- IP de origen: dirección IP del TCN.
- Puerto de origen: número de puerto local del TCN.
- IP de destino: dirección IP de multidifusión del grupo.
- Puerto de destino: número de puerto del grupo.

La longitud del paquete CR es de 20 bytes (encabezamiento básico de 16 bytes + elemento Conexión de 4 bytes).

El formato del paquete CR se muestra en la figura 21.

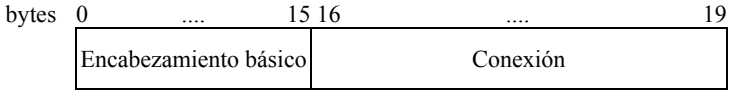

Figura 21 – Paquete CR

El encabezamiento básico de 16 bytes del paquete CR debe codificarse como sigue:

Elemento siguiente: '0001' (elemento Conexión).

Versión: '00' (versión actual de ECTP-5).

CT: '11' (conexión de multidifusión N-plex).

Tipo de paquete: '0000 0001' (CR).

Verificación de suma: por calcular.

Puerto de origen: número de puerto local del TCN (o ID de conexión).

Puerto de destino: número de puerto del grupo (o ID de conexión).

Longitud de cabida útil: '4'.

F: '0' (ignorar).

ID de testigo: '0' (el ID de testigo del TCN se pone a '0').

Todos los demás campos se pondrán a '0' y serán ignorados por el lado receptor.

El elemento Conexión de 4 bytes debe codificarse como sigue:

Elemento siguiente: '0000'.

TCO: configurada por el TCN.

AGN: configurado por el TCN.

MSS: configurado por el TCN (el valor por defecto es '1024').

8.3.2 Confirmar creación de conexión (CC, *connection creation confirm*)

El TS-usuario utiliza el paquete CC en respuesta al paquete CR del TCN. Un TS-usuario envía el paquete CC al TCN con las siguientes direcciones de origen y destino:

- IP de origen: dirección IP del TS-usuario.
- Puerto de origen: número de puerto local del TS-usuario.
- IP de destino: dirección IP del TCN.
- Puerto de destino: número de puerto del grupo.

El paquete contiene únicamente un encabezamiento básico de 16 bytes. El encabezamiento básico del paquete CC debe codificarse como sigue:

Elemento siguiente: '0000'.

CT: '11'.

Tipo de paquete: '0000 0010' (CC).

Verificación de suma: por calcular.

Puerto de origen: número de puerto local del TS-usuario (o ID de conexión).

Puerto de destino: número de puerto del grupo (o ID de conexión).

Todos los demás campos han de ponerse a '0' y serán ignorados por el lado receptor.

8.3.3 Petición de ingreso en árbol (TJ, *tree join request*)

El LE o el LO envían el paquete TJ al LO o el LE para ingresar en un árbol intragrupo o un árbol intergrupo. Este paquete tiene las siguientes direcciones:

- IP de origen: dirección IP del LE o el LO.
- Puerto de origen: número de puerto local del LE o el LO.

- IP de destino: dirección IP del LO o el LE.
- Puerto de destino: número de puerto del grupo.

El paquete TJ contiene el encabezamiento básico de 16 bytes y el elemento Indicación de tiempo de 12 bytes. El paquete TJ tiene el siguiente formato como se muestra en la figura 22.

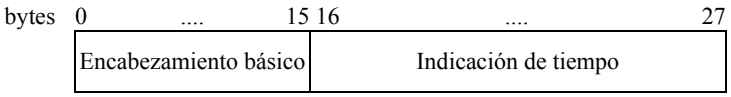

Figura 22 – Paquete TJ

El encabezamiento básico del paquete TJ debe codificarse como sigue:

Elemento siguiente: '0100' (elemento Indicación de tiempo).

CT: '11'.

Tipo de paquete: '0000 0011' (TJ).

Verificación de suma: por calcular.

Puerto de origen: número de puerto local del LE o el LO (o ID de la conexión).

Puerto de destino: número de puerto del grupo (o ID de la conexión).

PSN: número de secuencia de este paquete.

Longitud de cabida útil: '12'.

F: '1' (para ingreso en árbol intergrupo), '0' (para ingreso en árbol intragrupo).

Todos los demás campos se pondrán a '0' y serán ignorados por el lado receptor.

El elemento Indicación de tiempo de 12 bytes debe codificarse como sigue:

Elemento siguiente: '0000'.

Indicación de tiempo: tiempo actual del emisor del paquete.

8.3.4 Confirmar ingreso en árbol (TC, *tree join confirm*)

El nodo LO o LE envían el paquete TC en respuesta al paquete TJ. El LO o el LE envían el paquete TC al peticionario de ingreso en árbol (LE o LO) con las siguientes direcciones de origen y destino:

- IP de origen: dirección IP del LO o el LE.
- Puerto de origen: número de puerto del grupo.
- IP de destino: dirección IP del LE o el LO.
- Puerto de destino: puerto local del LE o el LO.

El paquete TC contiene el encabezamiento básico de 16 bytes y el elemento Indicación de tiempo de 12 bytes, como se muestra en la figura 23.

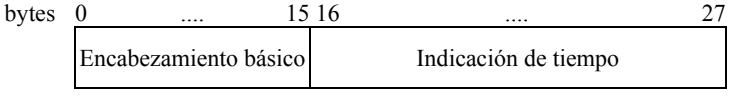

Figura 23 – Paquete TC

El encabezamiento de 16 bytes del paquete TC debe codificarse como sigue:

Elemento siguiente: '0100' (elemento Indicación de tiempo).

CT: '11'.

Tipo de paquete: '0000 0100' (TC).

Verificación de suma: por calcular.

Puerto de origen: puerto del grupo (o ID de conexión).

Puerto de destino: puerto local del LE o el LO (o ID de conexión).

PSN: El valor copiado del campo *PSN* del paquete de petición correspondiente.

Longitud de cabida útil: '12'.

F: '1' si se acepta la petición TJ, '0' en cualquier otro caso.

Todos los demás campos se pondrán a '0' y serán ignorados por el lado receptor.

El elemento Indicación de tiempo de 12 bytes debe codificarse como sigue:

Elemento siguiente: '0000'.

Indicación de tiempo: valor de tiempo de 8 bytes procedente del paquete TJ correspondiente.

8.3.5 Petición de egreso de árbol (TLR, *tree leave request*)

El LE o el LO envían el paquete TLR al LO o el LE progenitor para abandonar el árbol lógico. El paquete TLR se envía con las siguientes direcciones de origen y destino:

- IP de origen: dirección IP del LE o el LO.
- Puerto de origen: puerto local del LE o el LO.
- IP de destino: dirección IP del LO o el LE.
- Puesto de destino: número del puerto del grupo.

El paquete TLR contiene únicamente en encabezamiento básico de 16 bytes. El encabezamiento básico de 16 bytes del paquete TLR debe codificarse como sigue:

Elemento siguiente: '0000'.

CT: '11'.

Tipo de paquete: '0010 0011' (TLR).

Verificación de suma: por calcular.

Puerto de origen: puerto local del LE o el LO (o ID de conexión).

Puerto de destino: puerto del grupo (o ID de conexión).

PSN: número de secuencia de este paquete.

F: '1' (para el ingreso en un árbol intergrupo), '0' (para el ingreso en un árbol intragrupo).

Todos los demás campos se pondrán a '0' y deberán ser ignorados por el lado receptor.

8.3.6 Confirmar egreso de árbol (TLC, *tree leave confirm*)

El nodo LO o LE envían el paquete TLC en respuesta al paquete TLR. El LO o el LE envían el paquete TLC al LE o LO vástago con las siguientes direcciones de origen y destino:

- IP de origen: dirección IP del LO o el LE.
- Puerto de origen: número de puerto del grupo.
- IP de destino: dirección IP del LE o el LO.
- Puerto de destino: puerto local del LE o el LO.

El paquete TLC contiene únicamente el encabezamiento básico de 16 bytes. El encabezamiento básico del paquete TLC debe codificarse como sigue:

Elemento siguiente: '0000'.

CT: '11'.

Tipo de paquete: '0010 0100' (TLC).

Verificación de suma: por calcular.

Puerto de origen: número de puerto del grupo (o ID de conexión).

Puerto de destino: número de puerto local del LE o el LO (o ID de conexión).

PSN: el valor copiado del campo PSN del paquete de petición correspondiente.

F: '1' si se acepta la petición TLC, '0' en cualquier otro caso.

Todos los demás campos se pondrán a '0' y deben ser ignorados por el lado receptor.

8.3.7 Datos (DT)

El TCN o el SU utilizan el paquete DT para transmitir datos en multidifusión a los miembros del grupo. También el LO utiliza el paquete DT para transmitir tráfico de prueba para la adaptación del árbol lógico. Los paquetes DT en multidifusión se envían a los TS-usuarios con las siguientes direcciones de origen y destino:

- IP de origen: dirección IP del TCN o el SU o el LO.
- Puerto de origen: número de puerto local del TCN o el SU o el LO.
- IP de destino: dirección IP de multidifusión del grupo.
- Puerto de destino: número de puerto del grupo.

El paquete DT contiene el encabezamiento básico de 16 bytes y datos de usuario de longitud variable como se muestra en la figura 24.

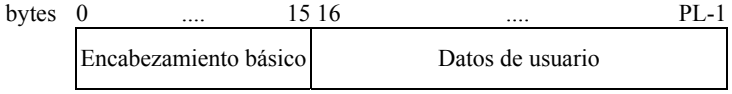

Figura 24 – Paquete DT

El encabezamiento básico de 16 bytes del paquete DT debe codificarse como sigue:

Elemento siguiente: '0000'.

CT: '11'.

Tipo de paquete: '0000 0101' (DT).

Verificación de suma: por calcular.

Puerto de origen: número de puerto local del TCN o el SU o el LO (o ID de conexión).

Puerto de destino: número de puerto del grupo (o ID de conexión).

PSN: el *PSN* de este paquete DT, que comienza con el número de secuencia inicial y se incrementa en '1', y vuelve a '1' tras alcanzar el valor '$2^{32} – 1$'.

Longitud de cabida útil: indica la longitud (en bytes) de los datos de usuario que contiene este paquete.

F: '1' (para el tráfico de prueba del LO), '0' en cualquier otro caso.

ID de testigo: ID de testigo del emisor de este paquete de datos ('0' para el TCN, o un número positivo de SU).

8.3.8 Datos de retransmisión (RD)

El LO o el LE envían el paquete RD para retransmitir datos en respuesta a las peticiones de reparación (NACK) de los nodos vástagos (LE o LO) del árbol de control. El formato del paquete es idéntico al del paquete DT. Sin embargo, el paquete DT se entrega en multidifusión, pero el RD se envía al peticionario en unidifusión con las siguientes direcciones de origen y destino:

- IP de origen: dirección IP del LO o el LE.
- Puerto de origen: número de puerto local del LO o el LE.
- IP de destino: dirección IP del peticionario de reparación (LE o LO).
- Puerto de destino: número de puerto del grupo.

El paquete RD contiene el encabezamiento básico de 16 bytes y datos de usuario de longitud variable como se muestra en la figura 25.

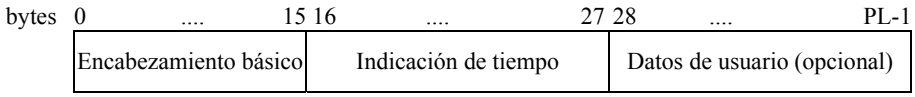

Figura 25 – Paquete RD

El encabezamiento básico de 16 bytes del paquete RD debe codificarse como sigue:

Elemento siguiente: '0100' (elemento Indicación de tiempo).

CT: '11'.

Tipo de paquete: '0000 0111' (RD).

Verificación de suma: por calcular.

Puerto de origen: número de puerto local del LO o el LE (o ID de conexión).

Puerto de destino: número de puerto del grupo (o ID de conexión).

PSN: el *PSN* del paquete de datos cuya retransmisión se solicita.

Longitud de cabida útil: indica la longitud (en bytes) de los datos de usuario que contiene este paquete.

F: '1' si el emisor de este paquete no tiene datos que reparar, '0' en cualquier otro caso.

ID de testigo: ID de testigo del emisor de este paquete de datos ('0' para el TCN, o un número positivo de SU).

El elemento Indicación de tiempo de 12 bytes debe codificarse como sigue:

Elemento siguiente: '0000'.

Indicación de tiempo: valor temporal de 8 bytes copiado del correspondiente paquete NACK.

8.3.9 Acuse de recibo (ACK)

El paquete ACK se envía al nodo progenitor en el árbol de control para acusar recibo de los paquetes DT recibidos de un SU. Los paquetes ACK se generan de acuerdo con la regla de generación ACK, que se describe más adelante. Si el paquete ACK responde al tráfico de prueba del LO, como se describe en 7.5, el paquete ACK debe contener un elemento Mapa de bits con errores para la adaptación de árbol lógico (LTA, *logical tree adaptation*).

Un LE o un LO envían el paquete ACK por el canal de control de unidifusión a su LE o LO progenitor en el árbol de control cuya raíz es el SU de los datos correspondientes. La transmisión se hace con las siguientes direcciones de origen y destino:

- IP de origen: dirección IP del LE o el LO.
- Puerto de origen: número de puerto local del LE o el LO.
- IP de destino: dirección IP del nodo progenitor (LO o LE).
- Puerto de destino: número de puerto del grupo.

El paquete ACK contiene el encabezamiento básico de 16 bytes y, opcionalmente, un Mapa de bits con errores de longitud variable, como se muestra en la figura 26.

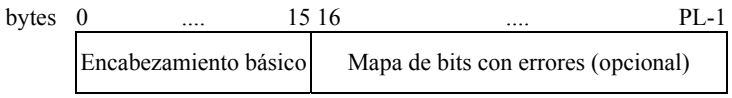

Figura 26 – Paquete ACK

El encabezamiento básico del paquete ACK debe codificarse como sigue:

Elemento siguiente: '0000' o '0010' (elemento Mapa de bits con errores) para el paquete ACK en respuesta al tráfico de prueba del LO.

CT: '11'.

Tipo de paquete: '0000 1000' (ACK).

Verificación de suma: por calcular.

Puerto de origen: número de puerto local del LE o el LO (o ID de conexión).

Puerto de destino: número de puerto del grupo (o ID de conexión).

PSN: *LSN*, el *PSN* del paquete DT con número más bajo que no se haya recibido todavía.

Longitud de cabida útil: longitud (en bytes) de los elementos de extensión anexos al encabezamiento básico.

F: '0' (ignorar).

ID de testigo: ID de testigo del correspondiente emisor ('0' para el TCN, o un número positivo de SU).

El elemento Mapa de bits con errores debe codificarse como sigue:

Elemento siguiente: '0000'.

Longitud del mapa de bits: representa la longitud total del *Mapa de bits con errores* en palabra (en 4 bytes).

Longitud del mapa de bits válida: longitud válida real del *Mapa de bits con errores* en bits.

Mapa de bits con errores: representa la información de mapa de bits acerca de los paquetes DT perdidos.

8.3.10 Acuse de recibo negativo (NACK)

El paquete NACK se utiliza para pedir al progenitor la retransmisión de los datos cuya pérdida se ha detectado. Cuando se detecta la pérdida de un paquete, se envía inmediatamente un paquete NACK. Con los campos *Número de paquetes perdidos* y *Número de secuencia de paquete inicial* del elemento Acuse de recibo negativo, un paquete NACK puede indicar que se pide la reparación de un bloque de dos o más paquetes perdidos consecutivamente.

El LE o el LO envían a través del canal de control de unidifusión un paquete NACK a su nodo progenitor en el árbol de control cuya raíz es el SU de los datos en cuestión. Este paquete se retransmite con las siguientes direcciones de origen y destino:

- IP de origen: dirección IP del LE o el LO.
- Puerto de origen: número de puerto local del LE o el LO.
- IP de destino: dirección IP del nodo progenitor (LO o LE).
- Puerto de destino: número de puerto del grupo.

El paquete NACK contiene el encabezamiento básico de 16 bytes, el elemento Acuse de recibo negativo de 8 bytes y el elemento Indicación de tiempo de 12 bytes, como se muestra en la figura 27.

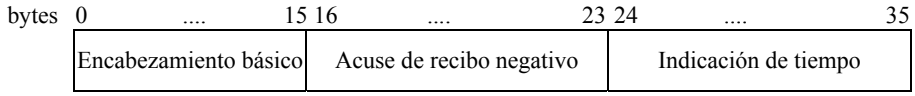

Figura 27 – Paquete NACK

El encabezamiento básico del paquete NACK debe codificarse como sigue:

Elemento siguiente: '1000' (Acuse de recibo negativo).

CT: '11'.

Tipo de paquete: '0001 1000' (NACK).

Verificación de suma: por calcular.

Puerto de origen: número de puerto local del LE o el LO (o ID de conexión).

Puerto de destino: número de puerto del grupo (o ID de conexión).

PSN: *LSN* que es el *PSN* del paquete DT con el número más bajo que aún no se ha recibido.

Longitud de cabida útil: '20'.

F: '0' (ignorar).

ID de testigo: ID de testigo del correspondiente emisor .

El elemento Acuse de recibo negativo debe codificarse como sigue:

Elemento siguiente: '0100' (elemento Indicación de tiempo).

Número de paquetes perdidos: representa el número de paquetes perdidos consecutivamente a partir del *Número de secuencia de paquete inicial*.

Número de secuencia de paquete inicial: número de secuencia del primer paquete de un bloque de paquetes perdidos.

El elemento Indicación de tiempo de 12 bytes debe codificarse como sigue:

Elemento siguiente: '0000'.

Indicación de tiempo: tiempo actual del emisor del paquete.

8.3.11 Sonda (PB)

El TCN utiliza el paquete PB para mantener la conexión. El TCN envía periódicamente paquetes PB a un TS-usuario de la sesión seleccionado con las siguientes direcciones de origen y destino:

- IP de origen: dirección IP del TCN.
- Puerto de origen: número de puerto local del TCN.
- IP de destino: dirección IP del TS-usuario seleccionado.
- Puerto de destino: número de puerto del grupo.

El paquete PB contiene únicamente el encabezamiento básico de 16 bytes. El encabezamiento básico del paquete PB tiene el siguiente formato:

Elemento siguiente: '0000'.

CT: '11'.

Tipo de paquete: '0000 1001' (PB).

Verificación de suma: por calcular.

Puerto de origen: número de puerto local del TCN (o ID de conexión).

Puerto de destino: número de puerto del grupo (o ID de conexión).

Todos los demás campos se pondrán a '0' y serán ignorados por el lado receptor.

8.3.12 Acuse de recibo de sonda (PBACK)

El TS-usuario envía el paquete PBACK en respuesta al paquete PB del TCN. Cuando un TS-usuario recibe el paquete PB del TCN, debe responder con el paquete PBACK. Este paquete se utiliza para indicar que sigue activo.

El TS-usuario envía el paquete PBACK al TCN con las siguientes direcciones de origen y destino:

- IP de origen: dirección IP del TS-usuario.
- Puerto de origen: número de puerto local del TS-usuario.
- IP de destino: dirección IP del TCN.
- Puerto de destino: número de puerto local del TCN.

El paquete PBACK contiene únicamente el encabezamiento básico de 16 bytes. El encabezamiento básico del paquete PBACK tiene el siguiente formato:

Elemento siguiente: '0000'.

CT: '11'.

Tipo de paquete: '0000 1110' (PBACK).

Verificación de suma: por calcular.

Puerto de origen: número de puerto local del TS-usuario (o ID de conexión).

Puerto de destino: número de puerto local del TCN (o ID de conexión).

Todos los demás campos se pondrán a '0' y serán ignorados por el lado receptor.

8.3.13 Petición de ingreso tardío (JR)

El paquete JR lo utiliza un nuevo TS-usuario para ingresar en la conexión ECTP. El nuevo TS-usuario envía el paquete JR al TCN con las siguientes direcciones de origen y destino:

- IP de origen: dirección IP del TS-usuario.
- Puerto de origen: número de puerto local del TS-usuario.
- IP de destino: dirección IP del TCN.
- Puerto de destino: número de puerto del grupo.

El paquete JR contiene únicamente el encabezamiento básico de 16 bytes. El encabezamiento básico del paquete JR debe codificarse como sigue:

Elemento siguiente: '0000' .

CT: '11'.

Tipo de paquete: '0000 1010' (JR).

Verificación de suma: por calcular.

Puerto de origen: número de puerto local del TS-usuario (o ID de conexión).

Puerto de destino: número de puerto del grupo (o ID de conexión).

PSN: número de secuencia de este paquete.

Todos los demás campos se pondrán a '0' y serán ignorados por el lado receptor.

8.3.14 Confirmar ingreso tardío (JC)

El TCN utiliza el paquete JC en respuesta al paquete JR. El TCN envía el paquete JC al nuevo TS-usuario con las siguientes direcciones de origen y destino:

- IP de origen: dirección IP del TCN.
- Puerto de origen: número de puerto local del TCN.
- IP de destino: dirección IP del TS-usuario.
- Puerto de destino: Puerto local del TS-usuario.

El paquete JC contiene el encabezamiento básico de 16 bytes y el elemento Conexión de 4 bytes.

El formato del paquete JC se muestra en la figura 28.

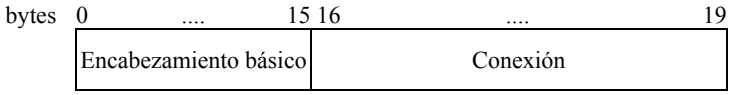

Figura 28 – Paquete JC

El encabezamiento básico de 16 bytes del paquete TC debe codificarse como sigue:

Elemento siguiente: '0001' (elemento Conexión).

CT: '11'.

Tipo de paquete: '0000 1011' (JC).

Verificación de suma: por calcular.

Puerto de origen: puerto local del TCN (o ID de conexión).

Puerto de destino: puerto local del TS-usuario (o ID de conexión).

PSN: el valor copiado del campo PSN del paquete de petición correspondiente.

Longitud de cabida útil: '4'.

F: '1' si se acepta la petición JR, '0' en cualquier otro caso.

Todos los demás campos se pondrán a '0' y serán ignorados por el lado receptor.

El elemento Conexión de 4 bytes debe codificarse como sigue:

Elemento siguiente: '0000'.

TCO: configurada por el TCN.

AGN: configurado por el TCN.

MSS: configurado por el TCN.

8.3.15 Petición de egreso de usuario (LR)

El TS-usuario utiliza el paquete LR para indicar que va a salir de la conexión; o lo utiliza el TCN para expulsar a un TS-usuario problemático. El paquete LR no necesita el correspondiente paquete de confirmación. Este paquete se envía con las siguientes direcciones de origen y destino:

- IP de origen: dirección IP del TS-usuario (egreso de usuario) o del TCN (expulsión de problemático).
- Puerto de origen: número de puerto local del TS-usuario o el TCN.
- IP de destino: dirección IP del TCN o el TS-usuario.
- Puerto de destino: número de puerto del grupo o número de puerto local del TS-usuario.

El paquete LR contiene únicamente el encabezamiento básico de 16 bytes. El encabezamiento básico tiene el siguiente formato:

Elemento siguiente: '0000'.

CT: '11'.

Tipo de paquete: '0000 1100' (LR).

Verificación de suma: por calcular.

Puerto de origen: puerto local del TS-usuario o el TCN (o ID de conexión).

Puerto de destino: puerto del grupo o puerto local del TS-usuario (o ID de conexión).

F: '1' para el egreso invocado por el usuario, o '0' para la expulsión de problemático.

Todos los demás campos se pondrán a '0' y serán ignorados por el lado receptor.

8.3.16 Petición de terminación de conexión (CT)

El TCN utiliza el paquete CT para terminar la conexión. El paquete CT no necesita el correspondiente paquete de confirmación. Este paquete lo envía el TCN con las siguientes direcciones de origen y destino:

- IP de origen: dirección IP del TCN.
- Puerto de origen: número de puerto local del TCN.
- IP de destino: dirección IP de multidifusión del grupo.
- Puerto de destino: número de puerto del grupo.

El paquete CT contiene únicamente el encabezamiento básico de 16 bytes. El encabezamiento básico tiene el siguiente formato:

Elemento siguiente: '0000'.

CT: '11'.

Tipo de paquete: '0000 1101' (CT).

Verificación de suma: por calcular.

Puerto de origen: puerto local del TCN (o ID de conexión).

Puerto de destino: puerto del grupo (o ID de conexión).

F: '1' para terminación anormal, o '0' para terminación normal (una vez completada la transmisión de datos en multidifusión).

Todos los demás campos se pondrán a '0' y serán ignorados por el lado receptor.

8.3.17 Petición de obtención de testigo (TGR)

El TS-usuario utiliza el paquete TGR para obtener un testigo para el transporte de datos en multidifusión (obtención de testigo iniciada por el TS-usuario). En este caso, el TS-usuario puede pedir un testigo al TCN enviando un paquete TGR. El TS-usuario que tiene un testigo se convierte en SU.

En la operación de concesión de testigo iniciada por el TCN, el TCN pide al TS-usuario que se convierta en SU. En este caso, el TCN enviará un paquete TGR a un determinado TS-usuario.

En el caso de la obtención de testigo, el elemento *Información de LO* debe ir anexo al paquete TGR del TS-usuario. Proporciona al TCN información acerca del LO al que se adjunta el TS-usuario. Esta información se utiliza al enviar paquetes TSR.

El paquete TGR se envía con las siguientes direcciones de origen y destino:

- IP de origen: dirección IP del TS-usuario (obtención de testigo) o dirección IP del TCN (concesión de testigo).
- Puerto de origen: número de puerto local del TS-usuario (obtención de testigo) o número de puerto local del TCN (concesión de testigo).
- IP de destino: dirección IP del TCN (obtención de testigo) o dirección IP del TS-usuario (concesión de testigo).
- Puerto de destino: número de puerto del grupo (obtención de testigo) o número de puerto local del TS-usuario (concesión de testigo).

El paquete TGR contiene el encabezamiento básico de 16 bytes y el elemento Información de LO de tamaño variable.

El paquete TGR tiene el siguiente formato como se muestra en la figura 29.

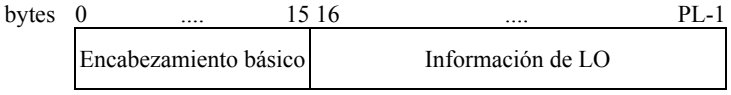

Figura 29 – Paquete TGR

El encabezamiento básico de 16 bytes del paquete TGR debe codificarse como sigue:

Elemento siguiente: '0000' o '0111' (elemento Información de LO, en el caso de obtención de testigo).

CT: '11'.

Tipo de paquete: '0001 0001' (TGR).

Verificación de suma: por calcular.

Puerto de origen: número de puerto local del TS-usuario o el TCN (o ID de conexión).

Puerto de destino: número de puerto del grupo o puerto local del TS-usuario (o ID de conexión).

PSN: número de secuencia de este paquete.

Longitud de cabida útil: longitud (en bytes) de los elementos de extensión anexos al encabezamiento básico.

F: ignorar.

ID de testigo: ID de testigo atribuido por el TCN (concesión de testigo); en el caso de obtención de testigo, este campo se ignora.

Si se añade el elemento Información de LO en elemento siguiente en el caso de obtención de testigo, debe codificarse como sigue:

Elemento siguiente: '0000'.

Número de testigos: '1'.

ID de propietario local: representa el ID del LO al que se une el LE.

Todos los demás campos se pondrán a '0' y serán ignorados por el lado receptor.

8.3.18 Confirmar obtención de testigo (TGC)

En respuesta al paquete TGR, el TCN envía un paquete TGC al TS-usuario que envió el paquete TGR (obtención de testigo iniciada por el TS-usuario). En la operación concesión de testigo iniciada por el TCN, el TS-usuario utiliza el paquete TGC para confirmar la petición.

En el caso de concesión de testigo, el elemento *Información de LO* debe ir anexo al paquete TGC del TS-usuario. Proporciona al TCN información acerca del LO al que se une el LE. Esta información se utiliza cuando se envían paquetes TSR.

El paquete TGC se envía con las siguientes direcciones de origen y destino:

- IP de origen: dirección IP del TCN (obtención de testigo) o dirección IP del LE (concesión de testigo).
- Puerto de origen: número de puerto del grupo (obtención de testigo) o número de puerto local del LE (concesión de testigo).
- IP de destino: dirección IP del LE (obtención de testigo) o dirección IP del TCN (concesión de testigo).
- Puerto de destino: puerto local del LE (obtención de testigo) o puerto local del TCN (concesión de testigo).

El paquete TGC contiene el encabezamiento básico de 16 bytes y el elemento Información de LO de tamaño variable.

El paquete TGC tiene el siguiente formato como se muestra en la figura 30.

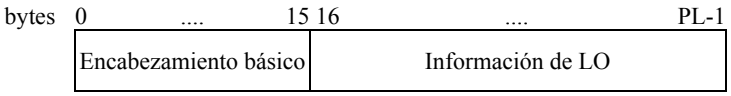

Figura 30 – Paquete TGC

El encabezamiento básico de 16 bytes del paquete TGC debe codificarse como sigue:

Elemento siguiente: '0000' o '0111' (elemento Información de LO, en el caso de concesión de testigo).

CT: '11'.

Tipo de paquete: '0001 0010' (TGC).

Verificación de suma: por calcular.

Puerto de origen: número de puerto del grupo o de puerto local del LE (o ID de conexión).

Puerto de destino: número de puerto del grupo o puerto local del LE (o ID de conexión).

PSN: el valor copiado del campo PSN del paquete de petición correspondiente.

Longitud de cabida útil: longitud (en bytes) de los elementos de extensión anexos al encabezamiento básico.

F: '0' (para aceptación) o '1' (para rechazo).

ID de testigo: ID de testigo atribuido por el TCN (obtención de testigo); en el caso de concesión de testigo, este campo se ignora.

Si se añade el elemento Información de LO como elemento siguiente en el caso de concesión de testigo, debe codificarse como sigue:

Elemento siguiente: '0000'.

Número de testigos: '1'.

ID de propietario local: representa el ID del LO al que se une el LE.

Todos los demás campos se pondrán a '0' y serán ignorados por el lado receptor.

8.3.19 Petición de devolución de testigo (TRR)

El TS-usuario utiliza el paquete TRR para devolver un testigo al TCN (devolución de testigo iniciada por el TS-usuario). En este caso, el TS-usuario envía un paquete TRR. En el caso de retiro de testigo iniciado por el TCN, el TCN pide al TS-usuario que devuelva el testigo. En este caso, el TCN enviará un paquete TRR al TS-usuario concernido.

El paquete TRR se envía con las siguientes direcciones de origen y destino:

- IP de origen: dirección IP del TS-usuario (devolución de testigo) o dirección IP del TCN (retiro de testigo).
- Puerto de origen: puerto local del TS-usuario (devolución de testigo) o puerto local del TCN (retiro del testigo).
- IP de destino: dirección IP del TCN (devolución de testigo) o dirección IP del TS-usuario (retiro de testigo).
- Puerto de destino: puerto del grupo (devolución de testigo) o puerto local del TS-usuario (retiro de testigo).

El paquete TRR contiene únicamente el encabezamiento básico de 16 bytes y debe codificarse como sigue:

Elemento siguiente: '0000' .

CT: '11'.

Tipo de paquete: '0001 0011' (TRR).

Verificación de suma: por calcular.

Puerto de origen: número de puerto local del TS-usuario o del TCN (o ID de conexión).

Puerto de destino: número de puerto del grupo o puerto local del TS-usuario (o ID de conexión).

PSN: número de secuencia de este paquete.

ID de testigo: ID de testigo del TS-usuario.

Todos los demás campos se pondrán a '0' y serán ignorados por el lado receptor.

8.3.20 Confirmar devolución de testigo (TRC)

El TCN o el TS-usuario utilizan el paquete TRC para confirmar la petición TRR asociada. El paquete TRC se envía con las siguientes direcciones de origen y destino:

- IP de origen: dirección IP del TCN (devolución de testigo) o dirección IP del TS-usuario (retiro de testigo).

- Puerto de origen: puerto del grupo (devolución de testigo) o puerto local del TS-usuario (retiro de testigo).
- IP de destino: dirección IP del TS-usuario (devolución de testigo) o dirección IP del TCN (retiro de testigo).
- Puerto de destino: puerto local del TS-usuario (devolución de testigo) o puerto local del TCN (retiro de testigo).

El paquete TRC contiene únicamente el encabezamiento básico de 16 bytes y debe codificarse como sigue:

Elemento siguiente: '0000'.

CT: '11'.

Tipo de paquete: '0001 0100' (TRC).

Verificación de suma: por calcular.

Puerto de origen: puerto del grupo o número de puerto local del TS-usuario (o ID de conexión).

Puerto de destino: número de puerto del grupo o puerto local del TS-usuario (o ID de conexión).

PSN: el valor copiado del campo PSN del correspondiente paquete de petición.

ID de testigo: ID de testigo del TS-usuario.

Todos los demás campos se pondrán a '0' y serán ignorados por el lado receptor.

8.3.21 Informe de estado de testigo (TSR)

El TCN utiliza el paquete TSR para anunciar los ID de testigo válidos en la conexión. También proporciona a los LO información sobre los ID de testigo correspondientes a cada LO anexando el elemento Información de LO. El paquete TSR se envía con las siguientes direcciones de origen y destino:

- IP de origen: dirección IP del TCN.
- Puerto de origen: puerto local del TCN o puerto del grupo (en respuesta al paquete TSRR).
- IP de destino: dirección IP de multidifusión del grupo o dirección IP del TS-usuario (en respuesta al paquete TSRR).
- Puerto de destino: puerto del grupo o puerto local del TS-usuario (en respuesta al paquete TSRR).

El paquete TSR tiene el siguiente formato como se muestra en la figura 31.

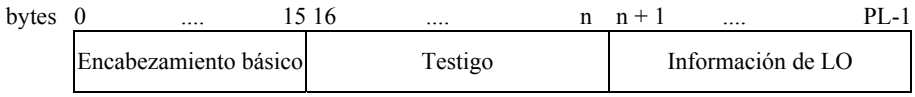

Figura 31 – Paquete TSR

El paquete TSR contiene el encabezamiento básico de 16 bytes, el elemento Testigo de tamaño variable y el elemento Información de LO de tamaño variable. El encabezamiento básico debe codificarse como sigue:

Elemento siguiente: '0110' (elemento Testigo).

CT: '11'.

Tipo de paquete: '0001 0101' (TSR).

Verificación de suma: por calcular.

Puerto de origen: número de puerto local del TCN (o ID de conexión) o puerto del grupo (en respuesta al paquete TSRR).

Puerto de destino: número de puerto del grupo (o ID de conexión) o puerto local del TS-usuario (en respuesta al paquete TSRR).

Longitud de cabida útil: longitud (en bytes) de los elementos de extensión anexos al encabezamiento básico.

Todos los demás campos se pondrán a '0' y serán ignorados por el lado receptor.

El elemento Testigo de tamaño variable se codificará como sigue:

Elemento siguiente: '0111' (elemento Información de LO).

Número de testigos: especifica el número total de *ID de testigo válidos* de la conexión.

ID de testigo válidos: contiene la lista de ID de testigo válidos de la conexión. Los *ID de testigo* tienen una longitud de 1 byte.

Todos los demás campos se pondrán a '0' y serán ignorados por el lado receptor.

El elemento Información de LO de tamaño variable debe codificarse como sigue:

Elemento siguiente: '0000' o '0111' (si sigue otro elemento Información de LO).

Número de testigos: número total de *ID de testigo correspondientes* para el LO cuyo ID es *ID de propietario local*.

ID de propietario local: representa el ID del LO al que se une el LE.

ID de testigo correspondientes: contiene la lista de ID de testigo correspondientes al *ID de propietario local* de la conexión. Los *ID de testigo* tienen una longitud de 1 byte.

Todos los demás campos se pondrán a '0' y deberán ser ignorados por el lado receptor.

8.3.22 Petición de informe de estado de testigo (TSRR)

El TS-usuario utiliza el paquete TSRR para pedir al TCN que actualice la lista de testigos. Un TS-usuario envía el paquete TSRR al TCN con las siguientes direcciones de origen y destino:

- IP de origen: dirección IP del TS-usuario.
- Puerto de origen: número de puerto local del TS-usuario.
- IP de destino: dirección IP del TCN.
- Puerto de destino: número de puerto del grupo.

El paquete TSRR contiene únicamente el encabezamiento básico de 16 bytes. El encabezamiento básico del paquete TSRR debe codificarse como sigue:

Elemento siguiente: '0000'.

CT: '11'.

Tipo de paquete: '0010 0101' (TSRR).

Verificación de suma: por calcular.

Puerto de origen: número de puerto local del TS-usuario (o ID de conexión).

Puerto de destino: número de puerto del grupo (o ID de conexión).

Todos los demás campos se pondrán a '0' y serán ignorados por el lado receptor.

8.3.23 Petición de cambio de árbol (TCR)

El paquete TCR se utiliza para modificar la relación progenitor-vástago de los nodos en los árboles intragrupo. Este paquete indica al nodo que lo recibe que se ha de convertir en vástago de otro nodo designado por un *ID de nodo*. El paquete TCR se envía por el canal de control unidifusión con las siguientes direcciones de origen y destino:

- IP de origen: dirección IP del LE o el LO.
- Puerto de origen: número de puerto local del LE o el LO.
- IP de destino: dirección IP del nodo objetivo (LE).
- Puerto de destino: número de puerto del grupo.

El paquete TCR contiene el encabezamiento básico de 16 bytes y el elemento Información de cambio de árbol de 8 bytes, como se muestra en la figura 32.

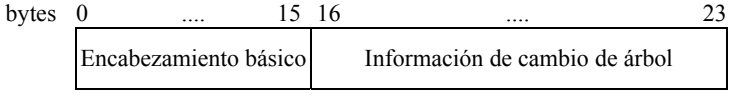

Figura 32 – Paquete TCR

El encabezamiento básico del paquete TCR debe codificarse como sigue:

Elemento siguiente: '1001' (elemento Información de cambio de árbol).

CT: '11'.

Tipo de paquete: '0001 0110' (TCR).

Verificación de suma: por calcular.

Puerto de origen: número de puerto local del LE o el LO (o ID de conexión).

Puerto de destino: número de puerto del grupo (o ID de conexión).

PSN: número de secuencia de este paquete.

Longitud de cabida útil: '8'.

Todos los demás paquetes se pondrán a '0' y serán ignorados por el lado receptor.

El elemento Información de cambio de árbol de 8 bytes debe codificarse como sigue:

Elemento siguiente: '0000'.

ID de nodo: representa un nuevo nodo progenitor para el nodo que recibe este paquete.

8.3.24 Confirmar cambio de árbol (TCC)

El LE envía el paquete TCC como respuesta al paquete TCR. El nodo envía el paquete TCC al nodo que envió el paquete TCR con las siguientes direcciones de origen y destino:

- IP de origen: dirección IP del LE.
- Puerto de origen: número de puerto del grupo.
- IP de destino: dirección IP del LE o el LO.
- Puerto de destino: puerto local del LE o el LO.

El paquete TCC contiene únicamente el encabezamiento básico de 16 bytes, que se codificará como sigue:

Elemento siguiente: '0000'.

CT: '11'.

Tipo de paquete: '0001 0111' (TCC).

Verificación de suma: por calcular.

Puerto de origen: número de puerto del grupo (o ID de conexión).

Puerto de destino: número de puerto local del LE o el LO (o ID de conexión).

PSN: el valor copiado del campo PSN del correspondiente paquete de petición.

F: se pone a '1' si se acepta la petición TCC, '0' en cualquier otro caso.

Todos los demás campos se pondrán a '0' y serán ignorados por el lado receptor.

8.3.25 Petición de delegación de árbol (TDR)

El paquete TDR se utiliza para delegar el proceso de determinación de posición adecuada de uno de los nodos vástago a otro nodo en los árboles intragrupo. El paquete incluye un *ID de nodo.* El nodo que recibe este paquete debe encontrar una mejor relación progenitor-vástago para el nodo con el *ID de nodo* utilizando sus mapas de bits con errores disponibles.

A través del canal de control unidifusión, cualquier nodo que tiene nodos vástagos envía el paquete TDR a sus nodos progenitor o vástagos en el mismo árbol intragrupo. Este paquete se transmite con las siguientes direcciones de origen y destino:

- IP de destino: dirección IP del LE o el LO.
- Puerto de origen: número de puerto local del LE o el LO.
- IP de destino: dirección IP del posible nodo progenitor (LO o LE).
- Puerto de destino: número de puerto del grupo.

El paquete TDR contiene el encabezamiento básico de 16 bytes, el elemento Información de cambio de árbol de 8 bytes y el elemento Mapa de bits con errores de longitud variable, como se muestra en la figura 33.

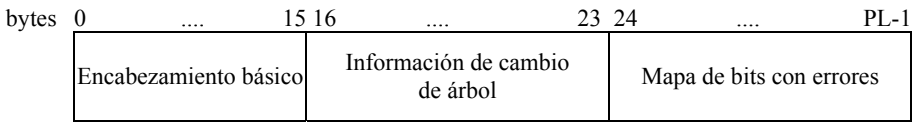

Figura 33 – Paquete TDR

El encabezamiento básico del paquete TDR se codificará como sigue:

Elemento siguiente: '1001' (elemento Información de cambio de árbol).

CT: '11'.

Tipo de paquete: '0001 1110' (TDR).

Verificación de suma: por calcular.

Puerto de origen: número de puerto local del LE o el LO (o ID de conexión).

Puerto de destino: número de puerto del grupo (o ID de conexión).

PSN: número de secuencia de este paquete.

Longitud de cabida útil: longitud (en bytes) de los elementos de extensión anexos al encabezamiento básico.

Todos los demás campos se pondrán a '0' y serán ignorados por el lado receptor.

El elemento Información de cambio de árbol de 8 bytes se codificará como sigue:

Elemento siguiente: '0010' (elemento Mapa de bits con errores).

ID de nodo: representa un posible vástago del nodo que recibe el paquete TDR.

El elemento Mapa de bits con errores debe codificarse como sigue:

Elemento siguiente: '0000'.

Longitud de mapa de bits: representa la longitud total del *Mapa de bits con errores* en palabra (en 4 bytes).

Longitud de mapa de bits válida: la longitud realmente válida del *Mapa de bits con errores* en bits.

Mapa de bits con errores: representa la información de mapa de bits acerca de los paquetes DT perdidos.

8.3.26 Confirmar delegación de árbol (TDC)

El paquete TDC se envía como respuesta al paquete TDR. El nodo envía el paquete TDC al nodo que envió el paquete TDR con las siguientes direcciones de origen y destino:

- IP de origen: dirección IP del LO o el LE.
- Puerto de origen: número de puerto del grupo.
- IP de destino: dirección IP del LE o el LO.
- Puerto de destino: puerto local del LE o el LO.

El paquete TDC contiene únicamente el encabezamiento básico de 16 bytes, que debe codificarse como sigue:

Elemento siguiente: '0000'.

CT: '11'.

Tipo de paquete: '0001 1111' (TDC).

Verificación de suma: por calcular.

Puerto de origen: número de puerto del grupo (o ID de conexión).

Puerto de destino: número de puerto local del LE o el LO (o ID de conexión).

PSN: el valor copiado del campo PSN del correspondiente paquete de petición.

F: '1' si se acepta la petición TDC, '0' en cualquier otro caso.

Todos los demás campos se pondrán a '0' y serán ignorados por el lado receptor.

8.3.27 Petición de notificación de cambio de árbol (TNR)

El paquete TNR se utiliza para notificar la modificación del árbol lógico (árbol intragrupo) al LO. Cuando reciba este paquete, el LO deberá reflejar la modificación en su árbol intragrupo con respecto al emisor y al nodo designado por el *ID de nodo*.

El LE envía por el canal de control unidifusión un paquete TNR que modifica su progenitor por cambio de árbol o ingreso en árbol. También se utiliza para que un nodo rechace a su vástago tras detectar un fallo en él. Se envía con las siguientes direcciones de origen y destino:

- IP de origen: dirección IP del LE.
- Puerto de origen: número de puerto local del LE.
- IP de destino: dirección IP del LO.
- Puerto de destino: número de puerto del grupo.

El paquete TNR contiene el encabezamiento básico de 16 bytes y el elemento Información de cambio de árbol de 8 bytes, como se muestra en la figura 34.

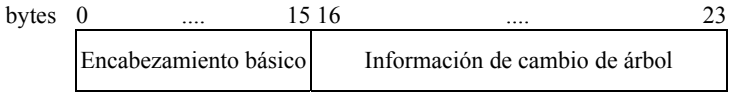

Figura 34 – Paquete TNR

El encabezamiento básico del paquete TNR debe codificarse como sigue:

Elemento siguiente: '1001' (elemento Información de cambio de árbol).

CT: '11'.

Tipo de paquete: '0010 0001' (TNR).

Verificación de suma: por calcular.

Puerto de origen: número de puerto local del LE (o ID de conexión).

Puerto de destino: número de puerto del grupo (o ID de conexión).

PSN: número de secuencia de este paquete.

Longitud de cabida útil: '8'.

F: F se pone a '0' si notifica un cambio de su nodo progenitor, o se pone a '1' si notifica el rechazo de su nodo vástago.

Todos los demás campos se pondrán a '0' y serán ignorados por el lado receptor.

El elemento Información de cambio de árbol de 16 bytes debe codificarse de la siguiente manera:

Elemento siguiente: '0000'.

ID de nodo: El ID del nuevo progenitor cuando *F* es '0', o el ID del nodo vástago que se rechaza cuando *F* es '1'.

8.3.28 Confirmar notificación de cambio de árbol (TNC)

El paquete TNC se envía en respuesta al paquete TNR. El LO envía el paquete TNC al nodo que envió el paquete TNR con las siguientes direcciones de origen y destino:

- IP de origen: dirección IP del LO.
- Puerto de origen: número de puerto del grupo.
- IP de destino: dirección IP del LE.
- Puerto de destino: puerto local del LE.

El paquete TNC contiene únicamente el encabezamiento básico de 16 bytes. El encabezamiento básico del paquete TNC debe codificarse como sigue:

Elemento siguiente: '0000'.

CT: '11'.

Tipo de paquete: '0010 0010' (TNC).

Verificación de suma: por calcular.

Puerto de origen: número de puerto del grupo (o ID de conexión).

Puerto de destino: número de puerto local del LE (o ID de conexión).

PSN: el valor copiado del campo PSN del correspondiente paquete de petición.

Todos los demás campos se pondrán a '0' y serán ignorados por el lado receptor.

8.3.29 Petición de cambio de árbol de control (CCR)

El LO envía el paquete CCR para modificar el árbol de control del LE. El LO envía a través del canal de control unidifusión un paquete CCR al LE que debe cambiar su información de árbol de control. La transmisión se hace con las siguientes direcciones de origen y destino:

- IP de origen: dirección IP del LO.
- Puerto de origen: número de puerto local del LO.
- IP de destino: dirección IP del nodo objetivo (LE).
- Puerto de destino: número de puerto del grupo.

El paquete CCR contiene el encabezamiento básico de 16 bytes y el elemento Información de cambio de árbol de 8 bytes, como se muestra en la figura 35.

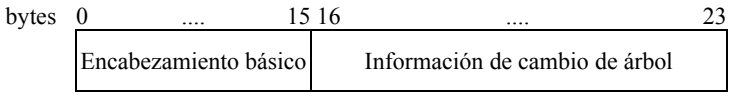

Figura 35 – Paquete CCR

El encabezamiento básico del paquete CCR debe codificarse como sigue:

Elemento siguiente: '1001' (elemento Información de cambio de árbol).

CT: '11'.

Tipo de paquete: '0010 1001' (CCR).

Verificación de suma: por calcular.

Puerto de origen: número de puerto local del LO (o ID de conexión).

Puerto de destino: número de puerto del grupo (o ID de conexión).

PSN: número de secuencia de este paquete.

Longitud de cabida útil: '8'.

ID de testigo: ID de testigo del correspondiente SU.

Todos los demás campos se pondrán a '0' y serán ignorados por el lado receptor.

El elemento Información de cambio de árbol de 8 bytes se codificará como sigue:

Elemento siguiente: '0000'.

ID de nodo: representa un nuevo nodo progenitor en el árbol de control para el SU especificado por el *ID de testigo* del encabezamiento básico.

8.3.30 Confirmar cambio de árbol de control (CCC)

El paquete CCC se envía en respuesta al paquete CCR. Un LE envía un paquete CCC al LO que envió el paquete CCR con las siguientes direcciones de origen y destino:

- IP de origen: dirección IP del LE.
- Puerto de origen: número de puerto local del LE.
- IP de destino: dirección IP del LO.
- Puerto de destino: número de puerto del grupo.

El paquete CCC contiene únicamente el encabezamiento básico de 16 bytes. El encabezamiento básico del paquete CCC debe codificarse de la siguiente manera:

Elemento siguiente: '0000'.

CT: '11'.

Tipo de paquete: '0010 1001' (CCC).

Verificación de suma: por calcular.

Puerto de origen: número de puerto del grupo (o ID de conexión).

Puerto de destino: número de puerto local del LO (o ID de conexión).

PSN: el valor copiado del campo PSN del correspondiente paquete de petición.

ID de testigo: ID de testigo del correspondiente SU.

Todos los demás campos se pondrán a '0' y serán ignorados por el lado receptor.

9 Procedimientos

En esta cláusula se describen los procedimientos de protocolo de ECTP-5. Antes de que se cree una conexión de multidifusión N-plex, habrá de anunciarse a los futuros participantes, los TS-usuarios, la siguiente información de dirección.

a) Dirección de multidifusión IP del grupo.

b) Número de puerto del grupo.

c) Dirección IP del TCN.

d) Dirección IP de un LO correspondiente (sólo para el LE).

Esta información puede anunciarse a los futuros participantes mediante un mecanismo de señalización fuera de banda, como un anuncio web. Del mismo modo, los futuros TS-usuario deben poder acceder a la dirección IP y el puerto del grupo para poder recibir el paquete CR del TCN. Un futuro TS-usuario que ingrese tardíamente también debe enviar un paquete JR al TCN.

9.1 Gestión de conexión

9.1.1 Creación de conexión

Una conexión de multidifusión N-plex comenzará cuando el TCN esté activado para gestionar la información de sesión y los testigos.

Si se comunica al TCN una lista de participantes antes del comienzo de la sesión, iniciará la fase de creación de conexión enviando un paquete CR al grupo a través del puerto y la dirección IP de multidifusión del grupo.

En la figura 36 se muestran las operaciones para la creación de conexión.

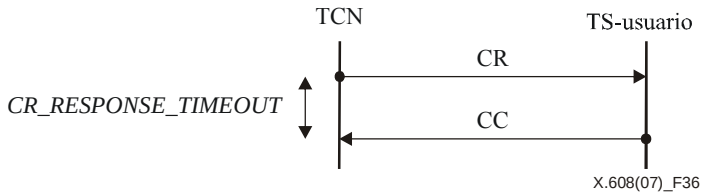

Figura 36 – Procedimientos de creación de conexión

El paquete CR contiene la información genérica del elemento Conexión, como la TCO (Opción de configuración de árbol) y el MSS (Tamaño de segmento máximo).

Si no todos los paquetes CC llegan dentro de *CR_RESPONSE_TIMEOUT*, el TCN envía de nuevo un paquete CR. Este proceso puede repetirse hasta *CR_MAX_RETRY* veces. Si el TCN no recibe paquetes CC de todos los TS-usuarios de la lista de participantes, abandona el procedimiento de creación de conexión y termina la conexión de multidifusión N-plex enviando un paquete CT (Terminación de conexión) al grupo. Si no hay participantes predeterminados antes de iniciar la sesión, el TCN comenzará la fase de transmisión de datos sin realizar la operación de creación de conexión.

9.1.2 Ingreso tardío

Algunos futuros participantes pueden ingresar en la conexión de multidifusión N-plex tardíamente. En la figura 37 se muestran las operaciones para el ingreso tardío.

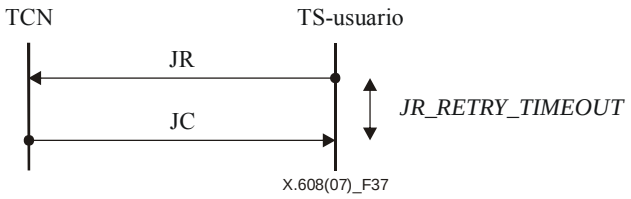

Figura 37 – Procedimientos de ingreso tardío

El TS-usuario que ingresa tardíamente envía un paquete JR al TCN. En respuesta al paquete JR, el TCN envía un paquete JC al TS-usuario. El paquete TJ debe indicar si se acepta o no la petición utilizando la bandera *F* del encabezamiento básico.

Si el paquete JC no llega dentro de *JR_RETRY_TIMEOUT*, el TS-usuario que ingresa tardíamente envía nuevamente el paquete JR. Este proceso puede repetirse hasta *JR_MAX_RETRY* veces. Si un nodo no recibe ningún paquete JC, abandonará el procedimiento de ingreso tardío y terminará la conexión de multidifusión N-plex.

9.1.3 Mantenimiento de conexión

Una conexión de multidifusión N-plex se mantiene utilizando los paquetes PB y PBACK. El TCN envía periódicamente paquetes PB cada *PB_PACKET_INT* a un TS-usuario seleccionado de la sesión. El correspondiente TS-usuario responde con el paquete PBACK. El método de selección del TS-usuario al que se mandan los paquetes PB estará diseñado para abarcar a todos los TS-usuarios de la sesión, por ejemplo, el método circular.

En la figura 38 se muestra la operación de gestión de miembros utilizando los paquetes PB y PBACK.

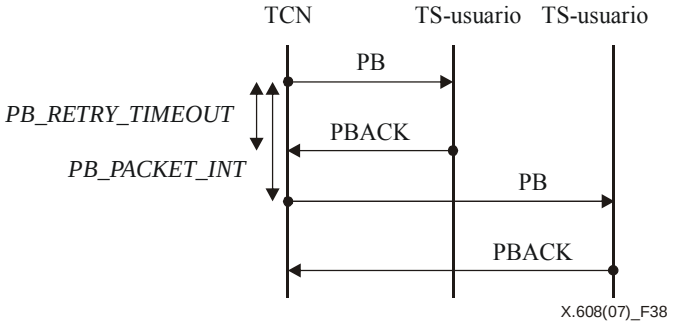

Figura 38 – Mantenimiento de conexión utilizando paquetes PB y PBACK

Si el paquete PBACK no llega dentro de *PB_RETRY_TIMEOUT*, el TCN envía de nuevo el paquete PB. Este proceso puede repetirse hasta *PB_MAX_RETRY* veces. Si el TCN no recibe ningún paquete PBACK, obliga al TS-usuario a abandonar la conexión enviándole el mensaje LR, que se denomina expulsión de problemático.

9.1.4 Egreso de usuario

En la figura 39 se muestran las operaciones de Egreso de usuario iniciado por el usuario y expulsión de problemático.

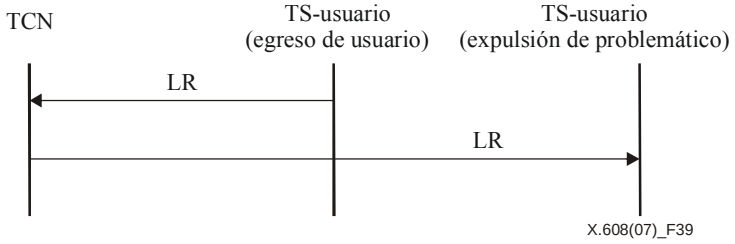

Figura 39 – Procedimientos de egreso de usuario y expulsión de problemático

En el caso de Egreso de usuario, el TS-usuario enviará un mensaje LR al TCN. En el caso de Expulsión de problemático, el TCN pedirá al TS-usuario concernido que abandone la conexión. En ambos casos, el mensaje LR no requiere el correspondiente mensaje de confirmación.

La expulsión de problemático se aplica al TS-usuario que no responde durante un determinado intervalo de tiempo en el marco de la operación PB y PBACK para el mantenimiento de conexión.

9.1.5 Terminación de conexión

En ECTP-5, el TCN también puede terminar la conexión cuando decide ponerle fin. El TCN termina la conexión enviando un mensaje CT al grupo. En la figura 40 se muestran las operaciones para la terminación de la conexión. Los paquetes CT no requieren un mensaje de confirmación.

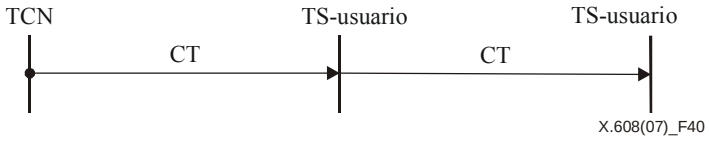

Figura 40 – Procedimientos de terminación de conexión

9.2 Gestión de árbol lógico

9.2.1 Ingreso en árbol intragrupo

Todos los LE deben ingresar en un árbol intragrupo para controlar los errores después de haber realizado el ingreso durante la creación de conexión inicial o de manera tardía.

Un LE inicia el procedimiento de ingreso en un árbol intragrupo enviando un paquete TJ al LO correspondiente. El LO responde con un paquete TC. El paquete TC debe indicar si se acepta o no la petición de ingreso en árbol utilizando la bandera F del encabezamiento básico. En la figura 41 se muestran las operaciones para el ingreso en árbol intragrupo.

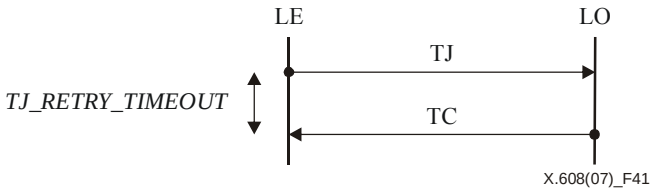

Figura 41 – Procedimientos de ingreso en árbol intragrupo

Si no se recibe un paquete TC del LO en respuesta al paquete TJ dentro de *TJ_RETRY_TIMEOUT*, el nodo envía de nuevo el paquete TJ. Este proceso puede repetirse hasta *TJ_MAX_RETRY* veces. Si el nodo no recibe un paquete TC, abandona el procedimiento de ingreso en árbol y devuelve un error con información de estado a la aplicación.

Este procedimiento también puede utilizarse entre LE durante el cambio de árbol por adaptación de árbol lógico, como se describe en 9.2.4.

9.2.2 Ingreso en árbol intergrupo

Al recibir los paquetes TSR, si un LO ve un nuevo LO que tiene uno o más SU, debe ingresar en un árbol intergrupo cuya raíz es el nuevo LO.

Para convertirse en SU, un LE debe notificar al TCN cuál es su LO durante los procedimientos de Obtención de testigo y Concesión de testigo. El TCN mantiene a los LO y les proporciona esta información enviando periódicamente paquetes TSR. Los paquetes TSR contienen el elemento Información de LO que consiste en una lista de ID de testigo de cada grupo local.

Con esta información, un LO ingresa en los árboles intergrupo cuya raíz es un LO enviando paquetes TJ a cada LO que tiene uno o más SU en su grupo local.

Entonces, los LO que son raíz de un árbol intergrupo responden con un paquete TC. El paquete TC debe indicar si se acepta o no la petición de ingreso en árbol utilizando la bandera F del encabezamiento básico. En la figura 42 se muestran las operaciones de ingreso en árbol intergrupo.

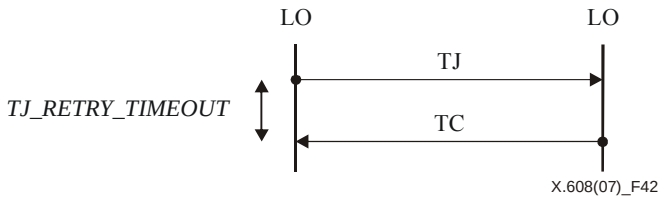

Figura 42 – Procedimientos de ingreso en árbol intergrupo

Si el paquete TC no llega dentro de *TJ_RETRY_TIMEOUT*, el emisor del paquete TJ puede intentar enviar nuevamente el paquete TC. Este proceso puede repetirse hasta *TJ_MAX_RETRY* veces. Si el nodo no recibe el paquete TC, abandona el procedimiento de ingreso en árbol y termina la conexión de multidifusión N-plex.

9.2.3 Egreso de árbol lógico

Antes de abandonar una sesión (Egreso de usuario) o de cambiar de nodo progenitor por el procedimiento de adaptación de árbol lógico, un LE sin nodos vástagos debe abandonar el árbol lógico (árbol intragrupo) enviando un paquete TLR a su nodo progenitor. El nodo progenitor eliminará el LE de su lista de vástagos y responderá con un paquete TLC.

En la figura 43 se muestran las operaciones para el egreso de árbol intragrupo.

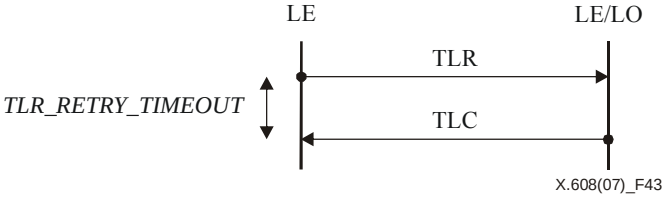

Figura 43 – Procedimientos de egreso de árbol intragrupo

Cuando un LE con uno o más vástagos abandona la sesión, debe anexar sus vástagos a su progenitor enviando un mensaje TCR a sus vástagos antes de salir. Un nodo vástago que recibe el mensaje TCR responde con un mensaje TCC. Además, el nodo vástago envía un mensaje TJ a su nuevo progenitor para ingresar como vástago. Una vez unido a su nuevo progenitor, el nodo vástago envía un mensaje TLR a su antiguo progenitor. Entonces, el LE saliente responde a cada mensaje TLR con mensajes TLC. Una vez que haya respondido a los mensajes TLR de todos sus vástagos, el LE puede egresar del árbol enviando un mensaje TLR a su progenitor. En la figura 44 se muestran las operaciones para el egreso de árbol intragrupo.

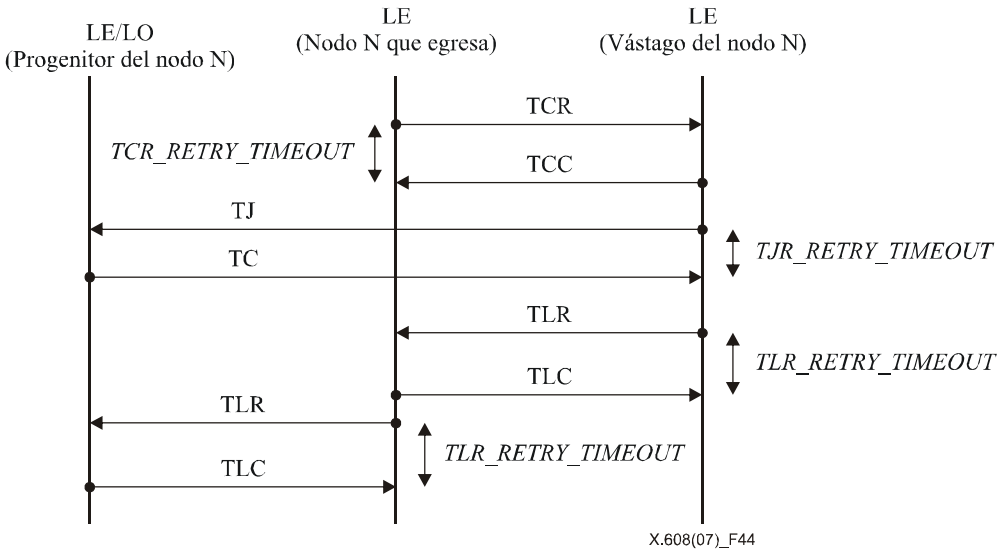

Figura 44 – Procedimientos para el egreso de árbol intragrupo del nodo *N* con vástagos

Un LO debe abandonar todos los árboles intergrupo si no tiene vástagos en su grupo local y no tiene aplicaciones para consumir los datos de sesión. Si un LO no tiene SU, todos los demás LO deberán retirarse del árbol intergrupo cuya raíz es el LO.

Un LO puede egresar de un árbol intergrupo enviando un paquete TLR a su LO progenitor. El LO progenitor que recibe el paquete TLR elimina al LO de su lista de vástagos y responde al LO con un paquete TLC. En la figura 45 se muestran las operaciones para el egreso de árbol intergrupo.

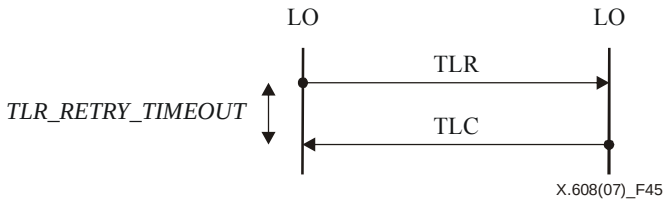

Figura 45 – Procedimientos para el egreso de árbol intergrupo

Si el mensaje TLC de respuesta no llega dentro de *TLR_RETRY_TIMEOUT*, el LE o el LO pueden enviar el mensaje TLR a su LE o LO progenitor de nuevo. Este proceso puede repetirse hasta *TLR_MAX_RETRY* veces. Si el nodo no recibe el paquete TLC, abandona el procedimiento de egreso de árbol y se extrae del progenitor.

9.2.4 Adaptación de árbol lógico

Cuando se utiliza la TCO '10', los árboles intragrupo pueden evolucionar en árboles multinivel cercanos a los árboles de encaminamiento de multidifusión subyacentes mediante la comparación de los patrones de pérdida de los nodos progenitores y vástagos del árbol. Un nodo puede determinar las relaciones entre él mismo y sus vástagos comparando sus mapas de bits con errores.

A fin de describir el mecanismo de adaptación de árbol lógico se definen a continuación tres operadores relacionales entre un par de nodos de un árbol intragrupo.

$B(N) = B(M)$

El nodo *N* y el nodo *M* tienen la relación $B(N) = B(M)$ (que se significa que el nodo *N* es potencialmente igual al nodo *M*) única y exclusivamente si $B_k(N) = B_k(M)$ para todos los $k = 1, 2, \ldots, n$. Aquí, $B_k(N)$ denota el *k*-ésimo bit (empezando por la izquierda) del mapa de bits del nodo *N* y $B(N)$ es una cadena de bits $B_1(N), B_2(N), \ldots, B_n(N)$, al tiempo que se asume que la longitud del mapa de bits es *n*.

$B(N) \supset B(M)$

El nodo *N* y el nodo *M* tienen la relación $B(N) \supset B(M)$ (que significa que el nodo *N* es potencialmente progenitor del nodo *M*) única y exclusivamente si $B_k(N) \geq B_k(M)$ para todos los $k = 1, 2, \ldots, n$, pero no $B(N) = B(M)$.

$B(N) \subset B(M)$

Del mismo modo, $B(N) \subset B(M)$ (que significa que el nodo *N* es potencialmente vástago del nodo *M*) única y exclusivamente si $B_k(N) \leq B_k(M)$ para todos los $k = 1, 2, \ldots, n$, pero no $B(N) = B(M)$.

En la figura 46, ERROR_BITMAP(*N*) representa un mensaje que contiene el mapa de bits con errores del nodo *N*. El mensaje TDR(*N*) es generado por un nodo que no puede determinar la posición del nodo *N*. Este mensaje contiene ERROR_BITMAP(*N*) para futuras delegaciones. TCR(*N*) representa que el nodo que recibe el mensaje debe unirse al nodo *N* como vástago. Progenitor (*N*) y vástago (*N*) representan el nodo progenitor y el nodo vástago del nodo *N*, respectivamente. El siguiente seudocódigo describe el algoritmo de adaptación de árbol lógico.

```
// nodo D recibe un mensaje m;
caso (m es ERROR BITMAP(N))
        si (B(D) ⊂ B(N))
                envía un mensaje TDR(N) a progenitor (D);
        si no
                si (∃ un vástago C tal que B(N) ⊃ B(C))
                        envía un mensaje TDR(C) a N;
                si no, si (∃ un vástago C tal que B(C) ⊃ B(N))
                        envía un mensaje TDR(N) a C;
                si no
                        nada;
caso (m es TDR(N))
        si (B(D) ⊂ B(N))
                envía un mensaje TDR(N) a progenitor (D)
        si no, si (B(D) = B(N))
                envía un mensaje TCR(D) a N;
        si no
                si (∃ un vástago C tal que B(N) ⊃ B(C))
                        envía un mensaje TDR(C) a N;
                        envía un mensaje TCR(D) a N;
                si no, si (∃ un vástago C tal que B(C) ⊃ B(N))
                        envía un mensaje TDR(N) a C;
                si no
                        envía un mensaje TCR(D) a N;
```

Figura 46 – Seudocódigo para adaptación de árbol lógico

El mensaje TDR(*N*) se entrega al progenitor potencial del nodo *N*. El mismo proceso se repite en sentido ascendente o descendente dentro del árbol intragrupo hasta que el nodo *N* encuentra su posición adecuada. En la figura 47 se muestra un procedimiento para la delegación de un nodo a un progenitor potencial.

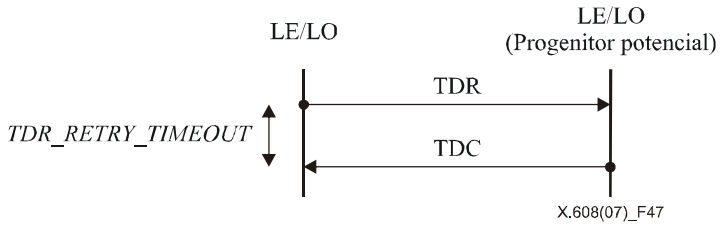

Figura 47 – Procedimiento de delegación de árbol

Si el paquete TDC no llega dentro de *TDR_RETRY_TIMEOUT*, el emisor del paquete TDR puede intentar enviar de nuevo el paquete TDR. Este proceso puede repetirse hasta *TDR_MAX_RETRY* veces. Si el nodo no recibe el paquete TDC, abandona el procedimiento de delegación de árbol.

Si un nodo puede determinar la posición adecuada del nodo *N*, envía un mensaje TCR al nodo *N*. Al recibir el mensaje TCR, el nodo *N* contesta con un mensaje TCC para confirmar el mensaje TCR de su nuevo progenitor. El nodo *N* se une al nuevo progenitor enviando el mensaje TJ. Entonces, el nodo *N* deja a su antiguo progenitor. Al hacerlo después de unirse a su nuevo progenitor, el nodo *N* puede seguir recuperando paquetes perdidos del antiguo progenitor durante los procesos de delegación y cambio de árbol.

Si el paquete TCC no llega dentro de *TCR_RETRY_TIMEOUT*, el emisor del paquete TCR puede intentar enviar de nuevo el paquete TCR. Este proceso puede repetirse hasta *TCR_MAX_RETRY* veces. Si el nodo no recibe el paquete TCC, abandona el procedimiento de cambio de árbol.

En la figura 48 se muestran las operaciones para el cambio de árbol.

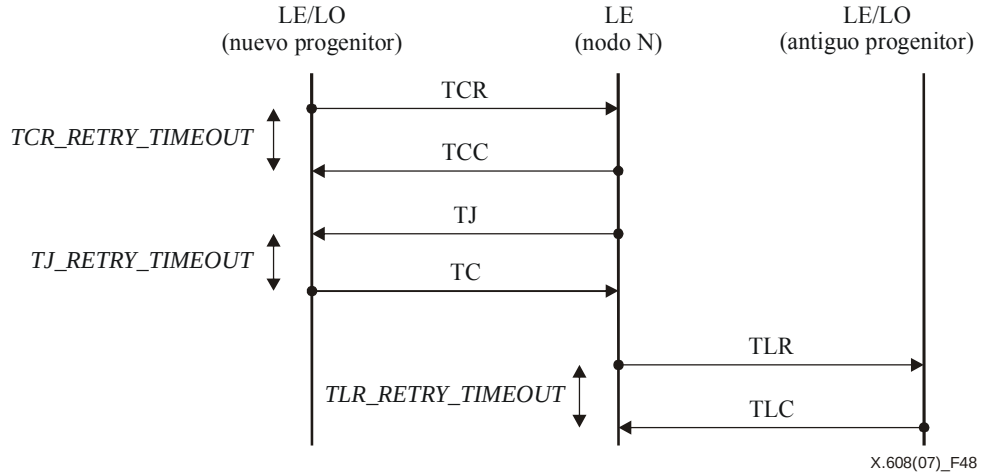

Figura 48 – Procedimiento de cambio de árbol

9.2.5 Notificación de cambio de árbol lógico

El LO debe gestionar su árbol intragrupo para generar árboles de control para los SU. Por tanto, se ha de informar al LO de los cambios del árbol intragrupo cuando se realicen mediante el procedimiento de ingreso en árbol lógico, el mecanismo de adaptación de árbol lógico o la adaptación del fallo del nodo.

Los LE envían el mensaje TNR al LO cuando reciben el paquete TJC o detecten el fallo de uno de sus vástagos. En la figura 49 se muestran las operaciones de cambio de árbol.

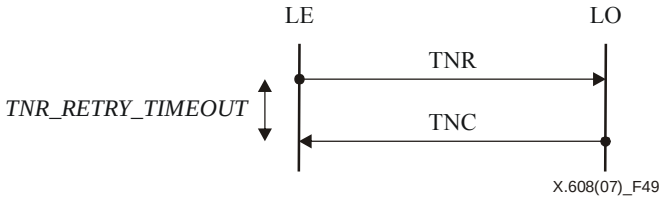

Figura 49 – Procedimiento de notificación de cambio de árbol

Si el paquete TNC no llega dentro de *TNR_RETRY_TIMEOUT*, el emisor del paquete TNR puede intentar enviar de nuevo el paquete TNR. Este proceso puede repetirse hasta *TNR_MAX_RETRY* veces. Si el nodo no recibe el paquete TNC, abandona el procedimiento de notificación de cambio de árbol, devuelve un error con información de estado a la aplicación y termina la conexión de multidifusión N-plex.

Al recibir el mensaje TNR del LO, el LO debe actualizar su información de árbol lógico. Una vez concluido el árbol lógico, examina los árboles de control para notificar a cada LE que debe cambiar su relación progenitor-vástago en el árbol de control con el paquete CCR.

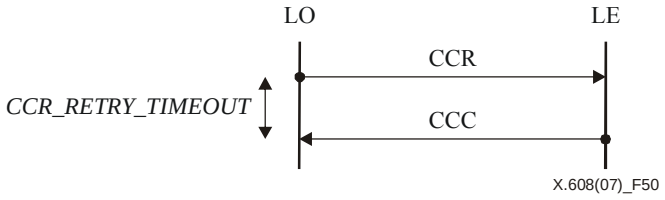

Figura 50 – Procedimiento de cambio de árbol de control

Si el paquete CCR no llega dentro de *CCR_RETRY_TIMEOUT*, el LO del paquete CCR puede intentar enviar de nuevo el paquete CCR. Este proceso puede repetirse hasta *CCR_MAX_RETRY* veces. Si el LO no recibe el paquete CCC, abandona el procedimiento de cambio de árbol de control y envía al correspondiente receptor el paquete LR.

9.2.6 Mantenimiento de árbol lógico

A fin de mantener el árbol lógico, los TS-usuarios utilizan la información obtenida de los paquetes NACK y ACK. Si un TS-usuario no recibe ningún paquete RD después de haber enviado paquetes NACK *NACK_MAX_RETRY* veces, abandona el procedimiento de recuperación de errores y supone que su progenitor está en fallo. A continuación, intenta encontrar otro progenitor adecuado poniéndose en contacto con el LO. El TS-usuario examina los LSN de sus vástagos y, si el LSN de un nodo vástago está por detrás de su propio LSN por *MAX_LSN_LAG*, supone que el vástago está en fallo. Entonces extrae al vástago de su árbol lógico e informa al LO.

9.3 Transporte de datos en multidifusión

En el canal de datos multidifusión de ECTP-5, el TCN o el SU pueden enviar paquetes DT en multidifusión al grupo. Cuando el TS-usuario receptor detecta la pérdida de un paquete de datos, el nodo progenitor en el árbol de control realizará la retransmisión para la recuperación de errores.

9.3.1 Transmisión de datos en multidifusión

El TCN o el SU generarán paquetes DT con el procedimiento de segmentación. Para ello, el emisor divide un tren de datos multidifusión de una aplicación en múltiples paquetes DT. Cada paquete DT tiene su propio *ID de testigo* y número de secuencia.

Los TS-usuarios entregan todos los paquetes recibidos a la aplicación en el orden que los envía el TCN. Cada receptor reensambla los paquetes recibidos. Los paquetes corrompidos y perdidos se detectan empleando la verificación de suma y el número de secuencia. Los paquetes corrompidos también se consideran perdidos. Los paquetes DT perdidos se recuperan en la función de control de errores.

Hay que señalar que los paquetes ACK son generados por cada SU, que se identifica por su ID de testigo.

ECTP-5 utiliza el flujo de control basado en una *ventana* de tamaño fijo. El *tamaño de ventana* representa el número de paquetes de datos de los que no se ha acusado recibo que están en la memoria tampón del emisor. El emisor puede transmitir como máximo el *tamaño de ventana* de paquetes de datos a la velocidad de transmisión de datos configurada. En ECTP-5, la velocidad de transmisión de datos en multidifusión está controlada por mecanismos de control de congestión de acuerdo a la velocidad.

El emisor de multidifusión numera secuencialmente los nuevos paquetes DT. El número de secuencia de un paquete DT comienza con el PSN inicial y se incrementa en '1'. El número de secuencia se utiliza para que los receptores detecten la pérdida de paquetes. El PSN se genera aleatoriamente y es distinto de '0'. El número de secuencia '0' está reservado. El número de secuencia de paquetes se incrementa para cada nuevo paquete DT. Se utiliza la aritmética de módulo 2^{32} y el número de secuencia vuelve a '1' tras haber alcanzado el valor "$2^{32} – 1$".

9.3.2 Control de fiabilidad para el transporte fiable

a) Los TS-usuario deben almacenar en la memoria tampón el tren de datos de cada SU para la recuperación de errores de los nodos vástagos en el árbol de control.

b) Cuando un TS-usuario detecta una o más pérdidas de paquetes, pide la retransmisión de los paquetes perdidos a su nodo progenitor en el árbol de control cuya raíz es el correspondiente SU a través de un mensaje de control NACK.

c) Un TS-usuario debe retransmitir los datos mediante unidifusión RD cuando recibe un paquete NACK de un nodo vástago en el árbol de control.

d) Un TS-usuario debe acusar recibo de los paquetes DT recibidos enviando un mensaje ACK al nodo progenitor en el árbol de control.

e) Los datos de la memoria tampón gestionada por el TS-usuario pueden liberarse cuando todos los vástagos en el árbol de control han acusado recibo de los mismos con mensajes ACK.

f) Todos los SU deben almacenar en la memoria tampón una parte de su tren de datos, incluso si todos los nodos vástagos han acusado recibo del mismo. Esto sirve para la recuperación de errores de un TS-usuario que no ha logrado recuperar las pérdidas de su nodo progenitor en el árbol de control. La parte del tren de datos está determinada por la semántica especificada por la aplicación en una capa superior.

9.3.2.1 Detección de errores

El campo verificación de suma del encabezamiento básico se utiliza para la detección de paquetes corrompidos, y el campo *PSN* para la detección de paquetes perdidos. Cuando se recibe un paquete de datos, cada receptor examina la verificación de suma. Si el campo verificación de suma no es válido, se considera que el paquete está corrompido y se descarta. La corrupción se considera como una pérdida. La pérdida puede detectarse por un vacío de dos números de

secuencia de paquetes DT consecutivos. Los paquetes NACK se utilizan para las peticiones de retransmisión cuando se detectan pérdidas.

9.3.2.2 Recuperación de errores por NACK y unidifusión RD

En la figura 51 se muestran las operaciones de recuperación de errores en el canal de control.

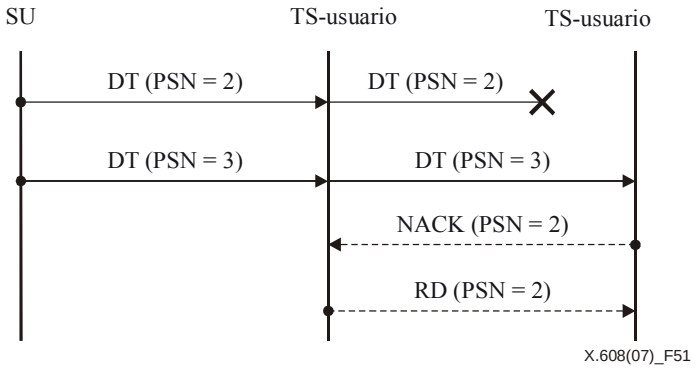

Figura 51 – Procedimientos de recuperación de errores

Si un participante detecta la pérdida de uno o más paquetes, inmediatamente transmite un paquete NACK al progenitor en el árbol de control. En respuesta al paquete NACK, el progenitor transmite uno o más paquetes RD al vástago en unidifusión.

Si un nodo progenitor recibe un paquete NACK pidiendo la reparación de paquetes de datos ya liberados, responde con un paquete RD con la bandera '1'. El nodo que recibe el paquete RD con bandera '1' envía otro paquete NACK al SU correspondiente. Por este motivo, el SU debe almacenar en la memoria tampón una cantidad suficiente de datos para poder reparar cualquier pérdida.

9.3.2.3 Retransmisión NACK con temporizador

Es posible que no se pueda entregar un paquete RD debido a la pérdida de paquetes NACK del peticionario de reparación o de paquetes RD de un progenitor. En este caso, puede retransmitirse un paquete NACK como se muestra en la figura 52.

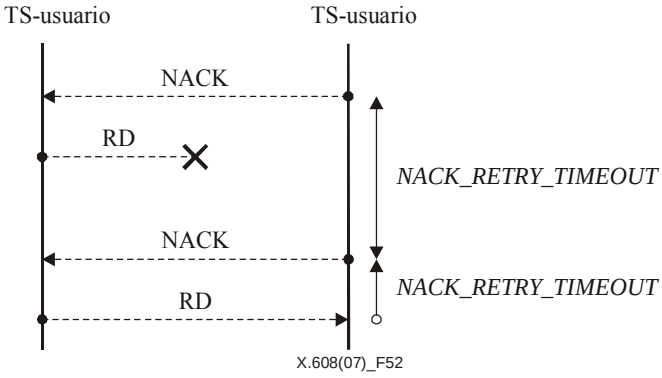

Figura 52 – Procedimiento de retransmisión NACK

Puede retransmitirse al progenitor un paquete NACK, si el peticionario de reparación no ha recibido el correspondiente paquete RD después de *NACK_RETRY_TIMEOUT*. El temporizador con *NACK_RETRY_TIMEOUT* se inicia con el envió de cada paquete NACK y se cancela cuando se recibe el correspondiente paquete RD. Este proceso puede repetirse hasta *NACK_MAX_RETRY* veces. Si el nodo no recibe ningún paquete RD, abandona el procedimiento de recuperación de errores y supone que su progenitor está en fallo. Entonces intenta encontrar otro progenitor adecuado poniéndose en contacto con el LO.

9.3.2.4 Generación de ACK

En la figura 53 se muestran las operaciones de acuse de recibo en el canal de control.

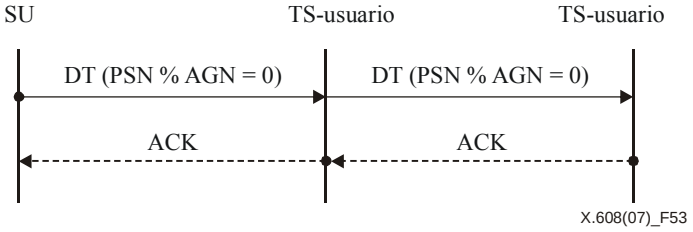

Figura 53 – Procedimientos de control ACK

Los vástagos generan un paquete ACK por cada *ACK_GENERATION_NUM (AGN)*. Cada *AGN* paquetes, examinan el estado de entrega de paquetes desde el anterior paquete acusado hasta el ultimo paquete recibido. Si se han recibido correctamente todos los paquetes de la fila, envía un paquete ACK a su progenitor.

Cada vástago envía un paquete ACK a su progenitor si el número *PSN* de un paquete DT módulo *AGN* es igual a cero, es decir, si:

$$PSN \% AGN = 0$$

Suponiendo que *AGN* = 8, el vástago genera un paquete ACK para los paquetes DT cuyos números de secuencia son 8, 16, 24, 32, etc. Esta regla de generación de ACK se aplica cuando el nodo recibe los correspondientes paquetes DT o RD.

9.3.2.5 Acuse de recepción de datos y agregación ACK

Los progenitores utilizan los paquetes ACK para obtener información relativa al estado de la recepción de datos por los TS-usuarios. Cada vez que un progenitor recibe un paquete ACK de uno de sus vástagos, registra y actualiza la información de estado de los paquetes que sus vástagos han recibido satisfactoriamente.

Un paquete DT se define como un paquete 'estable' si todos los vástagos lo han recibido. Los paquetes DT estables pueden liberarse de la memoria tampón del progenitor.

9.4 Control de testigo

En ECTP-5, un testigo representa el derecho de un TS-usuario a transmitir datos en multidifusión. Los TS-usuarios que desean transmitir datos deben obtener un testigo del TCN. El TS-usuario se convertirá en un SU después de obtener un testigo del TCN. De este modo, el TCN puede autorizar a un TS-usuario a que se convierta en emisor, de manera que los TS-usuarios pueden efectivamente filtrar los datos en multidifusión enviados por usuarios no autorizados. No obstante, hay que señalar que la utilización de testigos no proporciona protección a la multidifusión IP.

Los SU deben devolver el testigo una vez terminada la transmisión de datos.

9.4.1 Obtención de testigo

Un TS-usuario puede obtener un testigo de dos maneras distintas: obtención de testigo iniciada por el usuario y concesión de testigo iniciada por el TCN. En la operación Obtención de testigo, el TS-usuario pide un testigo al TCN, mientras que en la Concesión de testigo, es el TCN quien concede un testigo al TS-usuario.

En la figura 54 se muestran las operaciones de Obtención de testigo y Concesión de testigo.

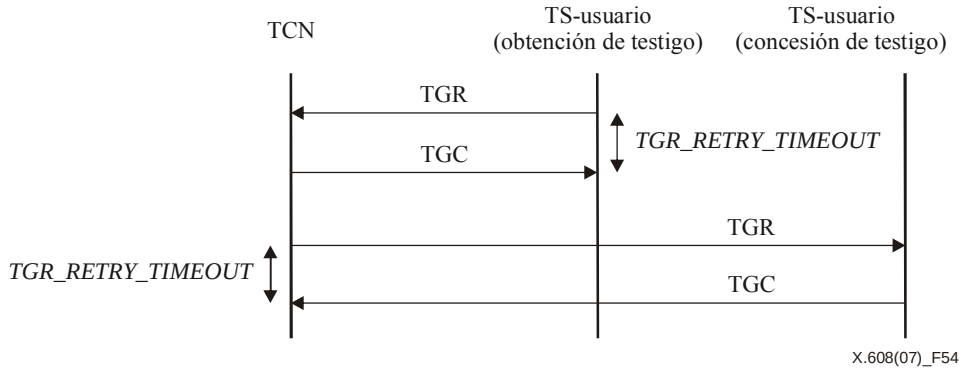

Figura 54 – Procedimientos de obtención y concesión de testigo

Para obtener un testigo en la Obtención de testigo, el TS-usuario envía un mensaje TGR al TCN, y espera el correspondiente mensaje TGC. En respuesta al paquete TGR, el TCN debe enviar un mensaje TGC al TS-usuario. El mensaje TGC debe indicar si se acepta o no la petición utilizando la bandera *F* del encabezamiento básico. En caso de que se acepte, el mensaje también contendrá un *ID de testigo* válido en el encabezamiento básico. Si el mensaje TGC de respuesta no llega dentro de *TGR_RETRY_TIMEOUT*, el TS-usuario puede enviar de nuevo el mensaje TGR al TCN. Este proceso puede repetirse hasta *TGR_MAX_RETRY* veces. Si el nodo no recibe el paquete TGC, abandona el procedimiento de obtención de testigo y devuelve un error con información de estado a la aplicación.

En la Concesión de testigo, el TCN enviará un mensaje TGR a un TS-usuario. El mensaje TGR debe contener el *ID de testigo* en el encabezamiento básico.

El TS-usuario (es decir, el SU) debe responder con el mensaje TGC con la bandera *F* puesta a '1' (aceptación). Si el mensaje TGC de respuesta no llega del SU dentro de *TGR_RETRY_TIMEOUT*, el TCN puede enviar de nuevo el mensaje TGR al SU. Este proceso puede repetirse hasta *TGR_MAX_RETRY* veces. Si el TCN no recibe el paquete TGC, abandona el procedimiento de concesión de testigo y excluye al TS-usuario de la lista de SU válidos, de manera que los siguientes paquetes TSR no incluyan al TS-usuario.

9.4.2 Devolución de testigo

Una vez completada la transmisión de datos, el SU puede devolver el testigo al TCN. El SU puede devolver su testigo al TCN de dos maneras distintas: Devolución de testigo iniciada por el TS-usuario y Retiro de testigo iniciado por el TCN. En la Devolución de testigo, el TS-usuario envía un paquete TRR al TCN, mientras que en el Retiro de testigo es el TCN quien envía en mensaje TRR al TS-usuario.

En la figura 55 se muestran las operaciones de Devolución de testigo y Retiro de testigo.

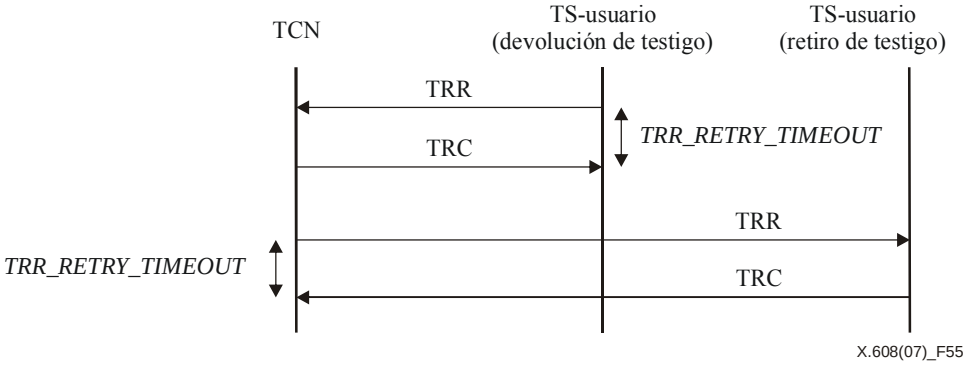

Figura 55 – Procedimientos de devolución y retiro de testigo

En el caso de la Devolución de testigo, el SU envía un mensaje TRR al TCN. El TCN responde con el mensaje TRC. Por otra parte, en el caso de Retiro de testigo, el TCN puede obligar al SU concernido a devolver el testigo enviándole un mensaje TRR. Si el mensaje TRC de respuesta no llega dentro de *TRR_RETRY_TIMEOUT*, puede volver a enviarse el mensaje TRR. Este proceso puede repetirse hasta *TRR_MAX_RETRY* veces.

En el caso de la Devolución de testigo, si el TS-usuario no recibe un paquete TRC, abandona el procedimiento. En el caso de Retiro de testigo, si el TCN no recibe un paquete TRC, abandona el procedimiento y elimina el testigo de la lista de testigos válidos y envía inmediatamente un paquete TSR actualizado para informar a los participantes.

9.4.3 Informe de estado de testigo

El TCN informa del estado de los ID de testigo válidos en la conexión enviando un paquete TSR. El TNC transmite el paquete TSR cuando un aparece un nuevo SU o cuando un SU existente deja de transmitir datos, o de manera periódica dentro del intervalo *TSR_PACKET_INT* para el mantenimiento de testigos.

En la figura 56 se muestran las operaciones de Informe de estado de testigo.

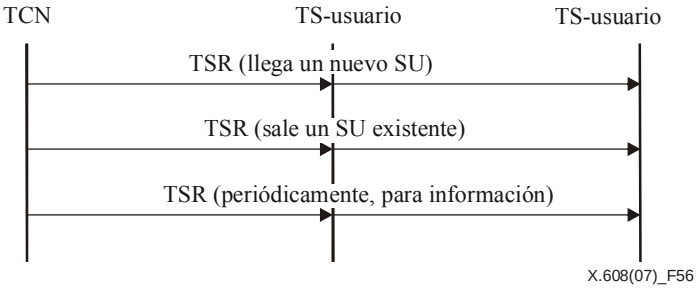

Figura 56 – Procedimientos de informe de estado de testigo

Si un TS-usuario recibe un paquete DT de un SU que no figura en la lista de testigos en vigor, solicita al TCN que actualice la lista de testigos enviando un paquete TSRR (Petición TSR) al TCN. Al recibir el paquete TSRR, el TCN contesta con un mensaje TSR que incluye la lista de testigos actualizada. Si un paquete TSR no llega dentro de *TSRR_RETRY_TIMEOUT*, el TS-usuario del paquete TSRR puede intentar enviar de nuevo el paquete TSRR. Este proceso puede repetirse *TSRR_MAX_RETRY* veces. Si el nodo no recibe el paquete TSR, abandona el procedimiento de petición de informe de estado de testigo e ignora los paquetes DT del SU.

Si un TS-usuario no recibe el siguiente TSR dentro de *TSR_ARRIVAL_TIMEOUT* después de haber recibido el último TSR, solicita al TCN que confirme que la conexión es válida enviando un paquete TSRR (Petición TSR) al TCN. Al recibir el paquete TSRR, el TCN responde con un paquete TSR que confirma la disponibilidad de la conexión. Si el paquete TSR no llega dentro de *TSRR_RETRY_TIMEOUT*, el TS-usuario del paquete TSRR puede intentar enviar de nuevo el paquete TSRR. Este proceso puede repetirse hasta *TSRR_MAX_RETRY* veces. Si el nodo no recibe el paquete TSR, abandona el procedimiento y devuelve un error con información de estado a la aplicación y termina la conexión de multidifusión N-plex.

En la figura 57 se muestran las operaciones para la Petición de informe de estado de testigo.

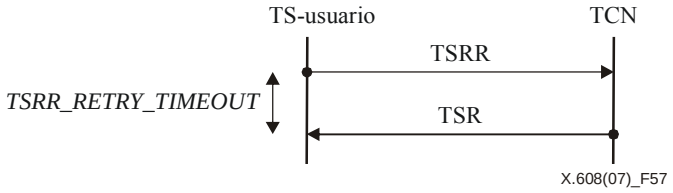

Figura 57 – Procedimiento de petición de informe de estado de testigo

9.5 Medición RTT

Puede utilizarse la RTT entre un nodo progenitor y un vástago para determinar el intervalo de reintento de paquetes de control que se intercambian entre ellos. A fin de estimar el valor RTT, se incluye en los paquetes TJ y NACK el tiempo actual de emisor. Entonces, el nodo receptor del paquete responde con los paquetes TC y RD, respectivamente, que contienen el valor de tiempo copiado del paquete recibido.

10 Parámetros de sistema

En el cuadro 4 se muestran los parámetros de sistema de ECTP-5.

Cuadro 4 – Parámetros de sistema ECTP-5

Nombre	Descripción
ACK_GENERATION_NUM	Intervalo mínimo de PSN para enviar el siguiente ACK
CCR_MAX_RETRY	Número máximo de reintentos para CCR
CCR_RETRY_TIMEOUT	Intervalo de reintentos para CCR
CR_MAX_RETRY	Número máximo de reintentos para CR
CR_RESPONSE_TIMEOUT	Tiempo de espera de las respuestas a CR de los TS-usuarios
JR_MAX_RETRY	Número máximo de reintentos para JR
JR_RETRY_TIMEOUT	Intervalo de reintentos para JR
MAX_LSN_LAG	Retardo máximo permitido para el LSN de un nodo vástago
MAX_SEGMENT_SIZE	Tamaño máximo del segmento de datos de usuario
NACK_MAX_RETRY	Número máximo de reintentos para NACK
NACK_RETRY_TIMEOUT	Intervalo de reintentos para NACK
PB_MAX_RETRY	Número máximo de reintentos para PB
PB_PACKET_INT	Intervalo de envío de PB
PB_RETRY_TIMEOUT	Intervalo de reintentos para PB
TCR_MAX_RETRY	Número máximo de reintentos para TCR
TCR_RETRY_TIMEOUT	Intervalo de reintentos para TCR
TD_PACKET_INT	Intervalo de envío de paquetes de datos de prueba
TD_PACKET_NUM	Número de paquetes de datos de prueba para un proceso de adaptación de árbol lógico
TD_PACKET_SIZE	Tamaño de cabida útil de paquete de datos de prueba
TDR_MAX_RETRY	Número máximo de reintentos para TDR
TDR_RETRY_TIMEOUT	Intervalo de reintentos para TDR
TGR_MAX_RETRY	Número máximo de reintentos para TGR
TGR_RETRY_TIMEOUT	Intervalo de reintentos para TGR
TJ_MAX_RETRY	Número máximo de reintentos para TJ
TJ_RETRY_TIMEOUT	Intervalo de reintentos para TJ
TLR_MAX_RETRY	Número máximo de reintentos para TLR
TLR_RETRY_TIMEOUT	Intervalo de reintentos para TLR
TNR_MAX_RETRY	Número máximo de reintentos para TNR
TNR_RETRY_TIMEOUT	Intervalo de reintentos para TNR
TRR_MAX_RETRY	Número máximo de reintentos para TRR
TRR_RETRY_TIMEOUT	Intervalo de reintentos para TRR
TSR_ARRIVAL_TIMEOUT	Latencia maxima hasta la llegada del siguiente TSR
TSR_PACKET_INT	Intervalo de envío de TSR
TSRR_MAX_RETRY	Número máximo de reintentos para TSRR
TSRR_RETRY_TIMEOUT	Intervalo de reintentos para TSRR

Anexo A

Interfaces de programación de aplicación

(Este anexo no es parte integrante de esta Recomendación | Norma Internacional)

En este anexo se especifican interfaces de programación de aplicación (API, *application programming interfaces*). Las API descritas en esta Recomendación | Norma Internacional pueden ser utilizadas por las aplicaciones que emplean capacidades de transporte de la parte 5 de ECTP (Rec. UIT-T X.608 | ISO/CEI 14476-5). Estas API se derivan del anexo B a la Rec. UIT -T X.606.1 | ISO/CEI 14476-2.

A.1 Generalidades

A.1.1 Funciones API

En el cuadro A.1 se resumen las funciones API.

Cuadro A.1 – Funciones API

Nombre de función	Descripción
`msocket()`	Crea un nuevo zócalo ECTP-5.
`mbind()`	Asocia un conjunto de direcciones/puertos locales y de grupo con el zócalo.
`mconnect()`	El TCN inicia la creación de una conexión a una dirección exterior específica. El TS-usuario tardío inicia el proceso de ingreso.
`maccept()`	Los posibles TS-usuarios ingresan en la conexión de multidifusión N-plex al aceptar la señal de creación de conexión del TCN.
`msend()`	Envía datos de aplicación a un grupo de destino.
`mrecv()`	Entrega los datos recibidos a la aplicación. Entrega algunos mensajes de indicación para el control de la aplicación durante la fase de transferencia de datos
`mclose()`	Termina la conexión y libera el zócalo.

A.1.2 Utilización de las funciones API

En la cláusula B.1.2 de la Rec. UIT-T X.606.1 | ISO/CEI 14476-2, puede verse la secuencia típica de utilización de las funciones API.

A.2 Funciones API ECTP-5

A.2.1 msocket()

Para utilizar el protocolo definido en esta Recomendación | Norma Internacional, una aplicación DEBE invocar la en primer lugar la función `msocket`, que especifica el tipo de protocolo de comunicación que se desea, como ECTP con IPv4 o ECTP con IPv6.

```
int msocket(int family, int type, int protocol);
```

Descripción de parámetros:

- *family*: especifica la familia de protocolos y es una de las constantes indicadas en el cuadro A.2;
- *type*: especifica el tipo de zócalo y es una de las constantes indicadas en el cuadro A.3;
- *protocol*: se pone a 0.

Cuadro A.2 – Constantes de familia de protocolos utilizadas para la función `msocket`

Familia	Descripción
AF_INET	Protocolos IPv4
AF_INET6	Protocolos IPv6

Cuadro A.3 – *Tipo* de zócalo utilizado para la función `msocket`

Tipo	Descripción
SOCK_ECTP5	Zócalo para la parte 5 de ECTP

La llamada `msocket` devuelve un descriptor no negativo de zócalo ECTP-5 si tiene éxito, o –1 en los siguientes casos relacionados en el cuadro A.4.

Cuadro A.4 – Códigos de error para la llamada `msocket`

Código de error	Descripción
EPROTONOSUPPORT	Dentro de este dominio no se soporta el tipo de protocolo o el protocolo especificado
EMFILE	El cuadro del descriptor por proceso está lleno
ENFILE	El cuadro de fichero de sistema está lleno
EACCES	Se niega el permiso para crear un zócalo del tipo y/o protocolo especificado
ENOBUFS	No hay suficiente espacio en la memoria tampón

A.2.2 mbind()

La función `mbind` asigna un conjunto de direcciones de control locales o de grupo, y el rol del nodo en la sesión hacia un zócalo.

En los protocolos Internet, la dirección de protocolo es la combinación de una dirección IPv4 de 32 bits o una dirección IPv6 de 128 bits, junto con un número de puerto de 16 bits.

`int mbind(int` *`msockfd`*`, const struct sockaddr *`*`laddr`*`, socklen_t` *`laddrlen`*`, const struct sockaddr *`*`gaddr`*`, socklen_t` *`gaddrlen`*`, int` *`role`*`, struct ectp5_option *`*`options`*` );`

Descripción de parámetros:

- *msockfd*: descriptor de zócalo devuelto por la función `msocket`;
- *laddr*: puntero a una dirección específica de protocolo para vincular una dirección local con el zócalo antes indicado;
- *laddrlen*: tamaño de la estructura de dirección indicada más arriba;
- *gaddr*: puntero a una dirección específica de protocolo para vincular una dirección de grupo objetivo con el zócalo;
- *gaddrlen*: tamaño de la estructura de dirección de grupo.
- *role*: especifica el rol de este iniciador de llamada, como TCN, Lo o LE.
- *options*: especifica las opciones de una conexión de multidifusión N-plex si *role* es TCN.

Cuadro A.5 – *role* del usuario del zócalo para la función `mbind`

role	Descripción
TCN	Creador de la conexión y emisor en tanto que propietario en las comunicaciones ECTP-5
LO	Receptor que asume la responsabilidad de las retransmisiones en la jerarquía basada en árbol
LE	Receptor no designado como LO

Cuadro A.6 – Campos del parámetro *options* en la función `mbind`

Campos Option	Descripción
TCO	Opción de configuración de árbol. '10' por defecto
AGN	Número de generación de ACK. '32' por defecto
MSS	Tamaño de segmento máximo. '1024' por defecto

Una aplicación puede aplicar una función `mbind` a una dirección IP específica y una dirección de red de grupo a su zócalo. Las direcciones de origen y de grupo deben pertenecer a una interfaz del anfitrión.

La llamada `mbind` devuelve cero si tiene éxito o –1 según los motivos enumerados en el cuadro A.7.

Cuadro A.7 – Códigos de error que puede causar `mbind`

Código de error	Descripción
EAGAIN	Los recursos de kernel para completar la petición están indisponibles temporalmente.
EBADF	*msockfd* no es un descriptor válido.
ENOTSOCK	*msockfd* no es un zócalo.
EADDRNOTAVAIL	La dirección especificada no está disponible en la máquina local.
EADDRINUSE	La dirección especificada ya está en uso.
EACCES	La dirección solicitada está protegida, y el usuario actual no tiene el permiso adecuado para el acceso.
EFAULT	El parámetro de dirección no está en una parte válida del espacio de dirección de usuario.
EROLE	El rol solicitado no es válido.

A.2.3 maccept()

Únicamente un LE o un LO pueden invocar esta función. Puede esperar que el TCN inicie un periodo especificado por el parámetro *timeout* e informe de si la conexión multidifusión se estableció o no.

```
int maccept(int msockfd, struct sockaddr *raddr, socklen_t *raddrlen, int timeout);
```

Descripción de parámetros:

- *msockfd*: descriptor de zócalo devuelto por la función msocket;
- *raddr*: devuelve la dirección de protocolo del iniciador de conexión distante (el emisor o TCN);
- *raddrlen*: puntero al tamaño de la estructura de dirección de zócalo señalada por *raddr*;
- *timeout*: es el valor de expiración del temporizador (en segundos) para el periodo de espera del CR del TCN.

Si `maccept` tiene éxito, devuelve el mismo valor que el primer argumento, ***msockfd.*** Por ello, al valor devuelto se le denomina descriptor de *zócalo conectado*.

La llamada `maccept` devuelve un descriptor no negativo si tiene éxito, o –1 por los motivos enumerados en el cuadro A.8.

Cuadro A.8 – Códigos de error utilizados para `maccept`

Código de error	Descripción
EBADF	El descriptor no es válido.
EINTR	Se interrumpió la operación `maccept`.
EMFILE	El cuadro de descriptor por proceso está lleno.
ENFILE	El cuadro de fichero de sistema está lleno.
ENOTSOCK	El descriptor hace referencia a un fichero, no a un zócalo.
EFAULT	El parámetro *addr* no está en la parte en la que se puede escribir del espacio de dirección de usuario.
EWOULDBLOCK	El zócalo está marcado sin bloqueo y no hay conexiones pendientes de aceptación.
ECONNABORTED	Llegó una conexión, pero se cerró mientras esperaba en la cola de escucha.
ECRTIMEOUT	Indica que expiró el tiempo de espera de CR.

A.2.4 mconnect()

El TCN o el LE que ingresa tardíamente utilizan la función `mconnect` para establecer una conexión.

```
int mconnect(int msockfd, const struct sockaddr *daddr, socklen_t daddrlen);
```

Descripción de parámetros:

- *msockfd*: descriptor de zócalo devuelto por la función `msocket`;
- *daddr*: puntero a una dirección de grupo;
- *daddrlen*: tamaño de *daddr*.

`mconnect` devuelve cero si tiene éxito o –1 en los casos anormales enumerados en el cuadro A.9.

Cuadro A.9 – Números de error de la función `mconnect`

Código de error	Descripción
EBADF	*msockfd* no es un descriptor válido.
ENOTSOCK	*msockfd* es un descriptor de fichero, no de zócalo.
EADDRNOTAVAIL	En esta máquina no está disponible la dirección especificada.
EAFNOSUPPORT	Las direcciones de la familia de direcciones especificada no se pueden utilizar con este zócalo.
EISCONN	El zócalo ya está conectado.
ECONNREFUSED	El intento de conectar fue rechazado por fuerza.
ENETUNREACH	No se puede llegar a la red desde este anfitrión.
EADDRINUSE	La dirección ya está en uso.
EFAULT	El parámetro de nombre especifica una zona fuera del espacio de dirección de proceso.
EALREADY	El zócalo es sin bloqueo y no se ha completado aún el intento de conexión previo.
EDENIED	Indica que el TCN no aceptó la petición incorporación de LE o LO.
ETIMEDOUT	Expiró el establecimiento de la conexión sin lograr establecerla. Indica que no hay respuesta del TCN.

A.2.5 msend()

Esta función msend escribe datos de una memoria tampón en un zócalo conectado.

```
ssize_t msend (int msockfd, const void *buf, size_t buflen, int *flags);
```

Descripción de parámetros:

- *msockfd*: descriptor de zócalo devuelto por la función `msocket`;
- *buf*: puntero a una memoria tampón para escribir;
- *buflen*: tamaño de *buf*; y
- *flags*: no se utiliza.

`msend` devuelve el número de bytes escritos si tuvo éxito o –1 en los casos anormales enumerados en el cuadro A.10.

Cuadro A.10 – códigos de error de msend

Código de error	Descripción
EBADF	Se especificó un descriptor no válido.
EACCES	La dirección de destino es una dirección de radiodifusión, y no se ha fijado SO_BROADCAST en el zócalo.
ENOTSOCK	El argumento *msockfd* no es un zócalo.
EFAULT	Se especificó una dirección de espacio de usuario no válida para un parámetro.
EMSGSIZE	El zócalo necesita que el mensaje se envíe atómicamente, y el tamaño del mensaje que hay que enviar no lo permite.
EAGAIN	El zócalo está marcado sin bloqueo y la operación solicitada se bloqueará.
ENOBUFS	El sistema no pudo asignar una memoria tampón interna. La operación se podrá realizar haya memorias tampón disponibles.
ENOBUFS	La cola de salida de una interfaz de red estaba llena. Esto indica normalmente que la interfaz ya no está transmitiendo, pero puede deberse a una congestión pasajera.
EPARTITIONED	Indica que la sesión se ha dividido.

A.2.6 mrecv()

La función mrecv se utiliza para recibir los datos multidifusión y las señales de indicación a efectos de control.

```
ssize_t mrecv (int msockfd, void *buf, size_t buflen, int *flags, struct sockaddr *fromaddr, socklen_t *fromaddrlen);
```

Descripción de parámetros:

- *msockfd*: descriptor de zócalo devuelto por la función `msocket`;
- *buf*: puntero a una memoria tampón para leer algo dentro;
- *buflen*: tamaño de *buf*;
- *flags*: aún no se ha definido;
- *fromaddr*: puntero a una dirección específica de protocolo que determina el SU;
- *fromaddrlen*: tamaño de *fromaddr*.

Cuando una aplicación recibe datos de la memoria tampón, puede identificar el emisor correspondiente (o SU) mediante *fromaddr.*

La función `mrecv` devuelve el número de bytes recibidos si tuvo éxito. De lo contrario devuelve –1 si se produce un error o si hay un mensaje de control que se entregará a la aplicación. Los códigos de error se enumeran en el cuadro A.11.

Cuadro A.11 – Códigos de error de la función `mrecv`

Código de error	Descripción
EBADF	El argumento *msockfd* es un descriptor no válido.
ENOTCONN	El zócalo está asociado con un protocolo orientado a conexión y no se ha conectado (véase `mconnect` y `maccept`).
ENOTSOCK	El argumento *msockfd* no se refiere a un zócalo.
EAGAIN	El zócalo está marcado sin bloqueo, y la operación de recepción se bloqueará, o se ha establecido un límite de temporización de recepción, que expiró antes de que los datos se hubieran recibido.
EINTR	La recepción se interrumpió con la llegada de una señal antes de que estuvieran disponibles los datos.
EFAULT	El puntero(s) a la memoria tampón de recepción apunta fuera del espacio de dirección del proceso.
ETOTERM	TCN dio por terminada la sesión.
ETOEXPEL	TCN expulsó a LE o LO.

A.2.7 mclose()

La función `mclose` se utiliza para abandonar o terminar una conexión de multidifusión N-plex mediante el cierre del zócalo. La acción por defecto de `mclose` con un zócalo ECTP-5 es marcar el zócalo como cerrado y regresar al proceso inmediatamente. El proceso no puede seguir usando el descriptor de zócalo.

```
int mclose (int msockfd);
```

Descripción de parámetros:

- *msockfd*: descriptor de zócalo devuelto por la función `msocket`.

`mclose` devuelve cero si tuvo éxito o –1 en el caso de los errores enumerados en el cuadro A.12.

Cuadro A.12 – Códigos de error de `mclose`

Código de error	Descripción
EBADF	*msockfd* no es un descriptor activo.
EINTR	Se recibió una interrupción.

Anexo B

Diagramas de transición de estado

(Este anexo no es parte integrante de esta Recomendación | Norma Internacional)

En este anexo se esbozan los diagramas de transición de estado de los nodos ECTP-5, TCN, LO y TS-usuario, a fin de facilitar la aplicación de esta Recomendación | Norma Internacional.

En la figura B.1 se muestra el diagrama de transición de estado del TCN ECTP-5, que se describe de acuerdo con la cláusula 8.

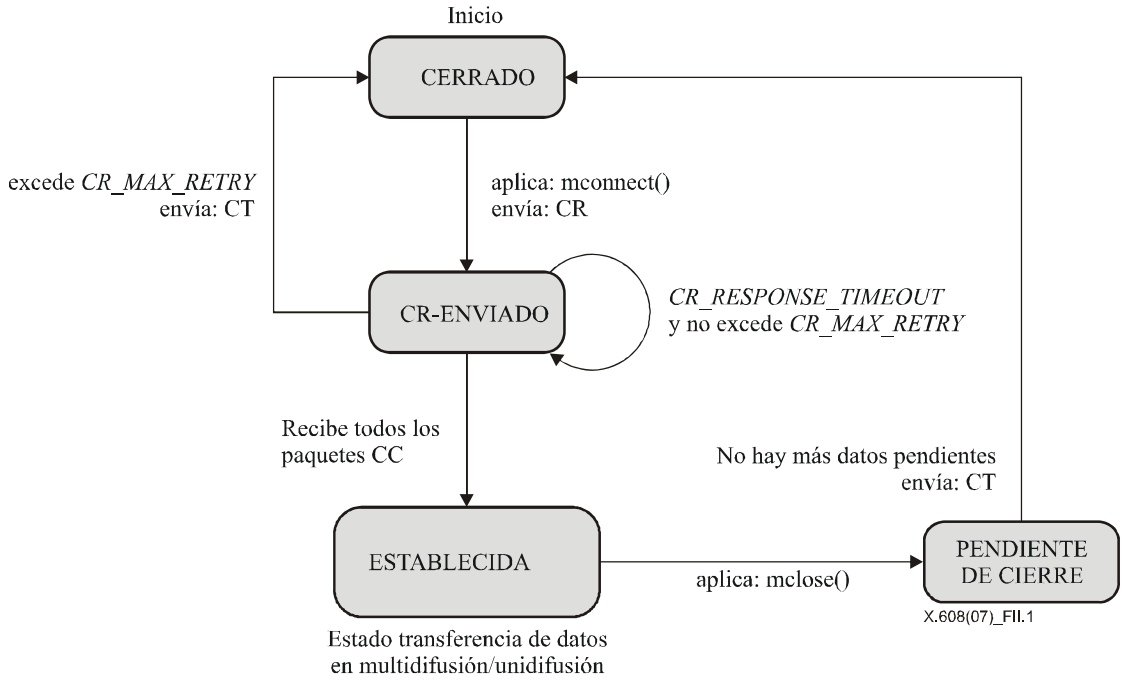

Figura B.1 – Diagrama de transición de estado de TCN

En la figura B.2 se muestra el diagrama de transición de estado de LO y TS-usuario ECTP-5, que se describen de acuerdo con la cláusula 8.

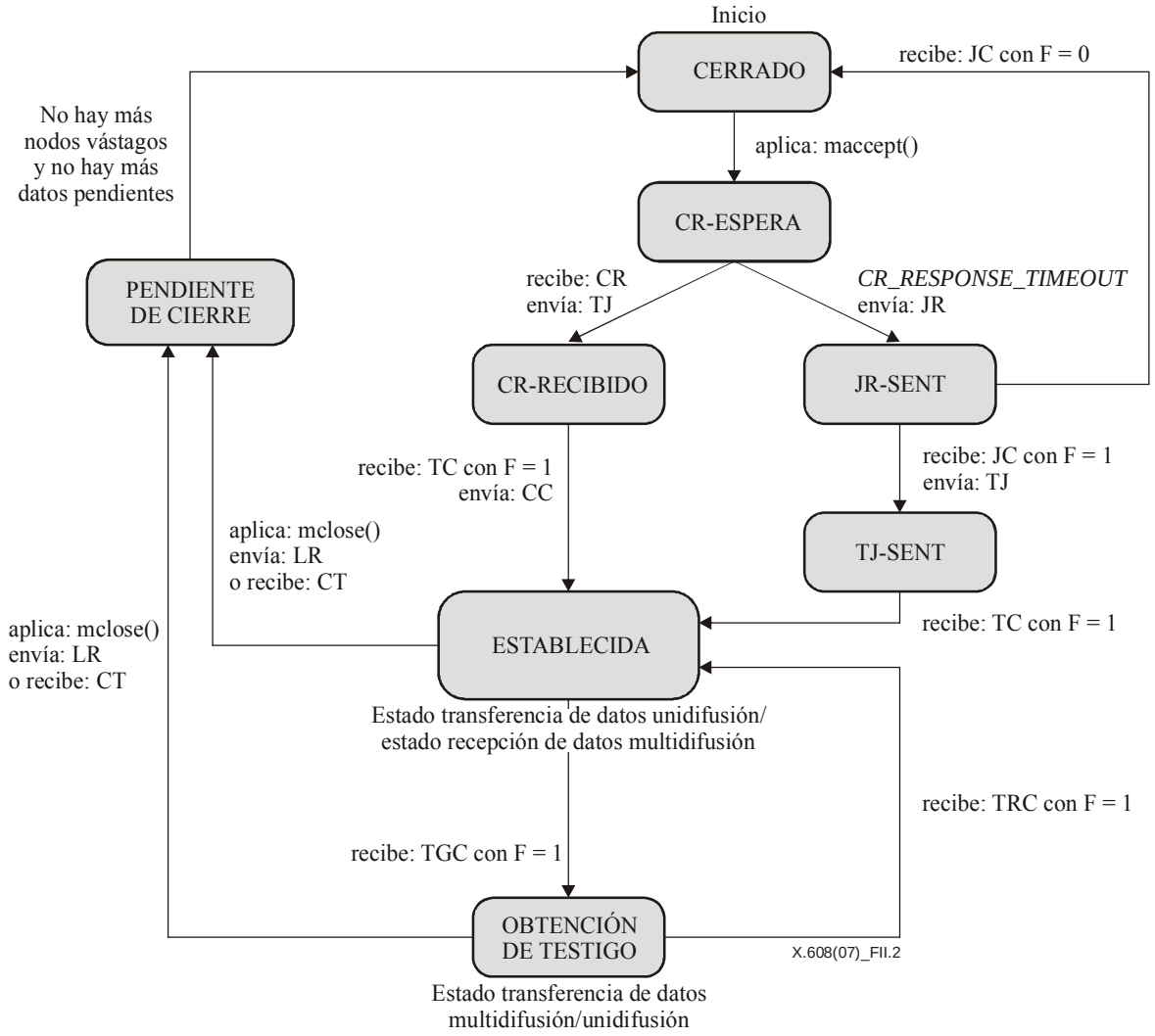

Figura B.2 – Diagrama de transición de estado de LO y TS-usuario ECTP-5

Anexo C

Ejemplo de valores de los parámetros de sistema de ECTP-5

(Este anexo no es parte integrante de esta Recomendación | Norma Internacional)

En este anexo se muestran ejemplos de los valores de los parámetros de sistema de ECTP-5 como referencia para los implementadores de ECTP-5. Véase el cuadro C.1.

Cuadro C.1 – Ejemplo de valores de parámetros de sistema de ECTP-5

Nombre	Valor por defecto
ACK_GENERATION_NUM	32
CCR_MAX_RETRY	5
CCR_RETRY_TIMEOUT	200 ms
CR_MAX_RETRY	5
CR_RESPONSE_TIMEOUT	5 s
JR_MAX_RETRY	5
JR_RETRY_TIMEOUT	200 ms
MAX_SEGMENT_SIZE	1024 bytes
NACK_MAX_RETRY	5
NACK_RETRY_TIMEOUT	200 ms
PB_MAX_RETRY	5
PB_PACKET_INT	3 s
PB_RETRY_TIMEOUT	500 ms
TCR_MAX_RETRY	5
TCR_RETRY_TIMEOUT	200 ms
TD_PACKET_INT	5 ms
TD_PACKET_NUM	1000
TD_PACKET_SIZE	512 bytes
TDR_MAX_RETRY	5
TDR_RETRY_TIMEOUT	200 ms
TGR_MAX_RETRY	5
TGR_RETRY_TIMEOUT	200 ms
TJ_MAX_RETRY	5
TJ_RETRY_TIMEOUT	200 ms
TLR_MAX_RETRY	5
TLR_RETRY_TIMEOUT	200 ms
TNR_MAX_RETRY	5
TNR_RETRY_TIMEOUT	200 ms
TRR_MAX_RETRY	5
TRR_RETRY_TIMEOUT	200 ms
TSR_ARRIVAL_TIMEOUT	15 s
TSR_PACKET_INT	5 s
TSRR_MAX_RETRY	5
TSRR_RETRY_TIMEOUT	500 ms

Estos valores se han seleccionado para el siguiente entorno:

- Tamaño de sesión: 30 TS-usuarios (30 SU).
- Número de grupos locales: 3 LO y 3 grupos locales.
- Velocidad de envío: 512 Kbit/s.
- Anchura de banda del enlace: 100 Mbit/s.
- Retardo del enlace: 40~50 ms entre grupos locales y 10~25 ms en un grupo local.
- Tasa de error de extremo a extremo: 0,05~0,25.

SERIES DE RECOMENDACIONES DEL UIT-T

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

Impreso en Suiza
Ginebra, 2008