

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.603.1

(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
de multidifusión con retransmisión –
Especificación de aplicaciones simplex
de grupo**

Recomendación UIT-T X.603.1

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.

**Tecnología de la información – Protocolo de multidifusión con retransmisión –
Especificación de aplicaciones simplex de grupo**

Resumen

La presente Recomendación | Norma Internacional describe un protocolo de la capa de aplicación que construye un árbol de multidifusión para distribuir datos de un remitente a varios destinatarios, utilizando Internet, que no soporta plenamente la multidifusión IP. El protocolo de multidifusión con retransmisión especificado está compuesto por un agente de multidifusión y un gestor de sesión. En la presente Recomendación | Norma Internacional se especifica un conjunto de funciones y procedimientos que utiliza el agente de multidifusión para construir un trayecto de datos retransmitidos de uno a varios y para retransmitir datos simplex. También se especifican las operaciones que realiza el gestor de sesión para administrar las sesiones de multidifusión. Puede emplearse este protocolo en aplicaciones que requieren servicios de distribución de datos de uno a varios, como el servicio multimedia de flujo continuo y el servicio de distribución de ficheros, entre otros.

Orígenes

La Recomendación UIT-T X.603.1 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 16512-2.

PREFACIO

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

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

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

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

NOTA

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

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

PROPIEDAD INTELECTUAL

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

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

© UIT 2009

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

ÍNDICE

	<i>Página</i>
1 Alcance	1
2 Referencias normativas	1
3 Definiciones	1
4 Abreviaturas	2
5 Generalidades	3
5.1 Entidades del RMCP-2	3
5.2 Bloque de protocolos RMCP-2	4
5.3 Modelo de entrega simplex del RMCP-2	5
5.4 Tipos de mensajes del RMCP-2	5
6 Funcionamiento del protocolo	6
6.1 Funcionamiento de los SM	6
6.2 Funcionamiento del MA	8
7 Formato de los mensajes del RMCP-2	18
7.1 Formato común de los mensajes del RMCP-2	18
7.2 Formato de los datos de control	19
7.3 Mensajes	20
8 Parámetros	43
8.1 Perfil de retransmisión de datos	44
8.2 Parámetros utilizados en el RMCP-2	44
8.3 Reglas de codificación para representar valores utilizados en el RMCP-2	45
Anexo A – Algoritmo para la configuración del árbol	48
A.1 Regla de iniciación	48
A.2 Regla para descubrir vecinos	49
A.3 Regla para seleccionar el HMA	49
A.4 Regla de aceptación de CMA	50
A.5 Regla para decidir el progenitor	50
A.6 Regla para perfeccionar el árbol	51
A.7 Regla de expulsión del PMA	51
Anexo B – Mecanismo de entrega de datos en tiempo real	52
B.1 Panorámica	52
B.2 Mecanismo túnel IP-IP para la entrega de datos en tiempo real de RMCP-2	52
Anexo C – Mecanismo para la entrega fiable de datos	54
C.1 Panorámica	54
C.2 Funcionamiento	54
C.3 Formato para la encapsulación de datos	56
C.4 Perfil de datos	56
Anexo D – API del RMCP-2	57
D.1 Panorámica	57
D.2 Funciones API del RMCP-2	59

Introducción

El protocolo de multidifusión con retransmisión parte 2 (RMCP-2, *relayed multicast protocol part 2*) es un protocolo de multidifusión con retransmisión de la capa de aplicación, destinado para las aplicaciones de grupo simplex. El protocolo RMCP-2 puede construir un trayecto óptimo y resistente para la distribución por multidifusión con retransmisión de uno a varios a través de una red de unidifusión, sirviéndose de las entidades RMCP definidas en la Rec. UIT-T X.603 | ISO/CEI 16512-1.

En cada sesión de RMCP-2 existe un gestor de sesión (SM, *session manager*) que se encarga de iniciar y finalizar la sesión y de gestionar la sesión de cada miembro. Cada uno de los agentes de multidifusión (MA, *multicast agent*) intercambia una serie de mensajes de control RMCP-2 para configurar por sí solo un árbol RMCP-2.

Se pueden construir varios tipos de canal para la distribución de datos a lo largo del trayecto de distribución por multidifusión con retransmisión, dependiendo de los requisitos de los servicios de aplicación.

**NORMA INTERNACIONAL
RECOMENDACIÓN UIT-T**

**Tecnología de la información – Protocolo de multidifusión con retransmisión –
Especificación de aplicaciones simplex de grupo**

1 Alcance

La presente Recomendación | Norma Internacional describe el protocolo de multidifusión con retransmisión (RMCP) parte 2, un protocolo de la capa de aplicación que construye un árbol de multidifusión para distribuir datos de un remitente a varios destinatarios, utilizando Internet, que no soporta plenamente la multidifusión IP. El protocolo de multidifusión con retransmisión especificado está compuesto por un agente de multidifusión y un gestor de sesión. En este texto se especifica un conjunto de funciones y procedimientos utilizado por el agente de multidifusión para construir un trayecto de datos retransmitidos de uno a varios y para retransmitir datos simplex. También se especifican las operaciones que utiliza el gestor de sesión para administrar las sesiones de multidifusión. Puede emplearse este protocolo en aplicaciones que requieren servicios de distribución de datos de uno a varios, como el servicio multimedia de flujo continuo y el servicio de distribución de ficheros, entre otros.

2 Referencias normativas

Las siguientes Recomendaciones del UIT-T y Normas Internacionales contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación | Norma Internacional. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y Normas son objeto de revisiones, por lo que se preconiza que los participantes en acuerdos basados en la presente Recomendación | Norma Internacional investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y Normas Internacionales. Los miembros de la CEI y de la ISO mantienen registros de las Normas Internacionales actualmente vigentes. La Oficina de Normalización de las Telecomunicaciones de la UIT mantiene una lista de las Recomendaciones del UIT-T actualmente vigentes.

- Recomendación UIT-T X.601 (2000), *Marco para comunicaciones entre múltiples pares*.
- Proyecto de Recomendación UIT-T X.603 (2004) | ISO/CEI 16512-1: 2005, *Tecnología de la información – Protocolo de multidifusión con retransmisión: Marco general*.
- 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 simplex*.
- Proyecto de 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 simplex*.

3 Definiciones

A los efectos de la presente Recomendación | Norma Internacional se aplican las siguientes definiciones:

- 3.1 multidifusión:** Mecanismo de entrega de datos en el que la misma unidad de datos se transmite desde un origen a múltiples destinos con una sola invocación del servicio.
- 3.2 multidifusión IP:** Mecanismo de *multidifusión* en la red IP en el que se utilizan varios encaminadores IP con capacidad de multidifusión.
- 3.3 multidifusión con retransmisión:** Mecanismo de entrega de datos multidifusión que puede emplearse en entornos unidifusión. El mecanismo se fundamenta en agentes de multidifusión intermedios que retransmiten datos desde un servidor de medios a reproductores de medios empleando una jerarquía arborescente.
- 3.4 protocolo de multidifusión con retransmisión (RMCP, *relayed multicast protocol*):** Protocolo empleado para el soporte y gestión del transporte de datos por multidifusión con retransmisión.
- 3.5 sesión RMCP-2:** Un conjunto de agentes de multidifusión (MA, *multicast agent*) que emplea el RMCP para configurar el trayecto de entrega de datos.

3.6 agente de multidifusión (MA, *multicast agent*): Entidad intermedia de transporte de datos utilizada para retransmitir los datos de aplicación por multidifusión. Dependiendo de la instalación, el MA podría residir en el mismo sistema que el cliente receptor.

3.7 agente de multidifusión de emisor (SMA, *sender multicast agent*): El MA acoplado al emisor en el mismo sistema o red local.

3.8 agente de multidifusión de receptor (RMA, *receiver multicast agent*): El MA acoplado al receptor en el mismo sistema o red local.

3.9 agente de multidifusión principal (HMA, *head multicast agent*): Un representante del MA al interior de una red local en la que se ha habilitado la multidifusión.

3.10 gestor de sesión (SM, *session manager*): Una entidad del RMCP que se encarga de las operaciones generales del RMCP. Puede ubicarse en el mismo sistema que el servidor de medios o puede ubicarse separado del servidor de medios.

3.11 agente de multidifusión progenitor (PMA, *parent multicast agent*): El siguiente MA en sentido ascendente del trayecto de entrega de datos del RMCP-2.

3.12 agente de multidifusión vástago (CMA, *child multicast agent*): El siguiente MA en el sentido descendente del trayecto de entrega de datos del RMCP-2.

4 Abreviaturas

En esta Recomendación | Norma Internacional, se aplican las siguientes abreviaturas.

AUTH	Autenticación (<i>authentication</i>)
CMA	Agente de multidifusión vástago (<i>child multicast agent</i>)
DMA	Agente de multidifusión especializado (<i>dedicated multicast agent</i>)
HANNOUNCE	Mensaje de anuncio del HMA (<i>HMA, announce message</i>)
HB	Mensaje de latido (<i>heartbeat message</i>)
HLEAVE	Mensaje de abandono del HMA (<i>HMA, leave message</i>)
HMA	Agente de multidifusión principal (<i>head multicast agent</i>)
HSOLICIT	Mensaje solicitar un HMA (<i>HMA, solicit message</i>)
IP-IP	IP en IP
LEAVANS	Respuesta de abandono (<i>leave answer message</i>)
LEAVREQ	Petición de abandono (<i>leave request message</i>)
MA	Agente de multidifusión (<i>multicast agent</i>)
MAID	Identificación del agente de multidifusión (<i>multicast agent identification</i>)
PMA	Agente de multidifusión progenitor (<i>parent multicast agent</i>)
PPROBANS	Mensaje de respuesta de búsqueda de progenitor (<i>parent probe answer message</i>)
PPROBREQ	Mensaje de petición de búsqueda de progenitor (<i>parent probe request message</i>)
RELANS	Mensaje de respuesta de retransmisión (<i>relay answer message</i>)
RELREQ	Mensaje de petición de retransmisión (<i>relay request message</i>)
RMA	Agente de multidifusión de receptor (<i>receiver multicast agent</i>)
RMCP	Protocolo de multidifusión con retransmisión (<i>relayed multicast protocol</i>)
SDP	Protocolo de descripción de la sesión (<i>session description protocol</i>)
SID	Identificador de la sesión RMCP2 (<i>RMCP2 session identification</i>)
SMA	Agente de multidifusión de emisor (<i>sender multicast agent</i>)
STANS	Mensaje de respuesta del informe de estado (<i>status report answer message</i>)
STCOLANS	Mensaje de respuesta de recopilación de informes de estado (<i>status report collect answer message</i>)

STCOLREQ	Mensaje de petición de recopilación de informes de estado (<i>status report collect request message</i>)
STREQ	Mensaje de petición de informe de estado (<i>status report request message</i>)
SUBSANS	Mensaje de respuesta de suscripción (<i>subscription answer message</i>)
SUBSREQ	Mensaje de petición de suscripción (<i>subscription request message</i>)
T/TCP	Ampliaciones TCP para transacciones (<i>TCP, extensions to transactions</i>)
TCP	Protocolo de control de transmisión (<i>transmission control protocol</i>)
TERMANS	Mensaje de respuesta de terminación (<i>termination answer message</i>)
TERMREQ	Mensaje de petición de terminación (<i>termination request message</i>)
UDP	Protocolo de datagrama de usuario (<i>user datagram protocol</i>)

5 Generalidades

RMCP-2 es un protocolo del nivel de aplicación que utiliza agentes de multidifusión (MA) y un gestor de sesión para soportar y gestionar el transporte de datos por multidifusión con retransmisión en una red Internet fundamentada en la unidifusión. Usando el SM, el RMCP-2 inicia la construcción de un árbol de control de multidifusión con retransmisión compuesto por MA. Posteriormente, una vez preconfigurado el árbol de control, cada MA se interconecta con los demás estableciendo los canales de datos adecuados.

En la cláusula 5.1 se describen las entidades del RMCP-2 de un modelo de entrega simplex.

5.1 Entidades del RMCP-2

Las entidades del RMCP-2 son las mismas que se describen para la parte 1 del RMCP. Como se indica en la figura 1, cada sesión del RMCP-2 construye un modelo para la entrega de datos por multidifusión con retransmisión que consta de las siguientes entidades:

- Un SM.
- Un agente de multidifusión de emisor (SMA) por cada aplicación de emisor.
- Uno o varios agentes de multidifusión de receptor (RMA).
- Una o varias aplicaciones de grupo emisoras y receptoras.

Se puede tener un SM, con capacidad para manejar una o varias sesiones, funcionando independientemente o formando parte de otras entidades de una sesión RMCP-2.

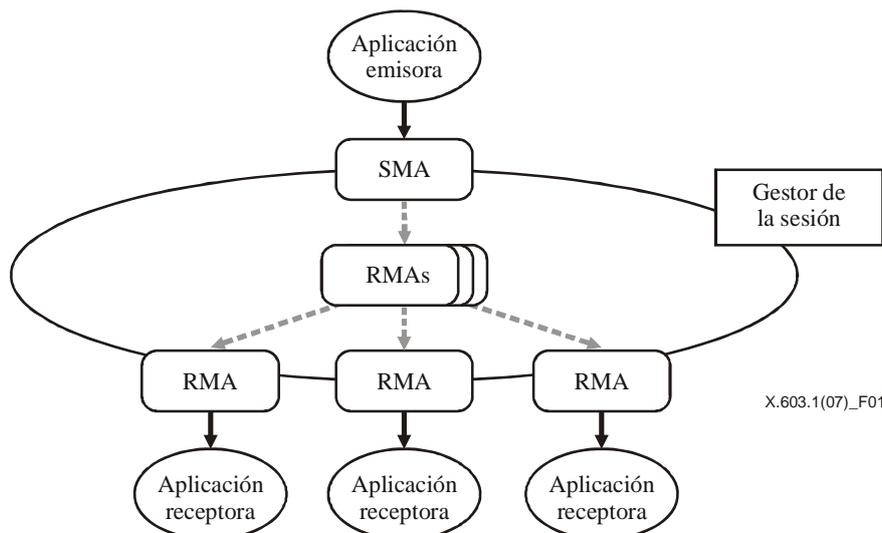


Figura 1 – Topología de servicio del RMCP-2

Un SM puede proporcionar las siguientes funciones:

- a) Inicio de la sesión.
- b) Liberación de la sesión.
- c) Gestión de los miembros de la sesión.
- d) Supervisión del estado de la sesión.

Un MA, que se refiere tanto al SMA como al RMA, construye un trayecto de entrega por multidifusión con retransmisión desde un emisor hasta varios receptores y luego retransmite los datos a lo largo del trayecto, puede proporcionar el siguiente conjunto de funciones:

- a) Inicio de la sesión.
- b) Adhesión a la sesión.
- c) Abandono de la sesión.
- d) Mantenimiento de la sesión.
- e) Informe del estado de la sesión.
- f) Retransmisión de datos de aplicación.

5.2 Bloque de protocolos RMCP-2

Los SM deben intercambiar mensajes de control con otros MA a fin de controlar y gestionar las sesiones RMCP-2. Los mensajes de control utilizados por los SM se deben entregar con fiabilidad, de lo contrario la sesión del RMCP-2 no se puede recuperar. En la figura 2, a continuación, se presenta la pila de protocolos de un SM.

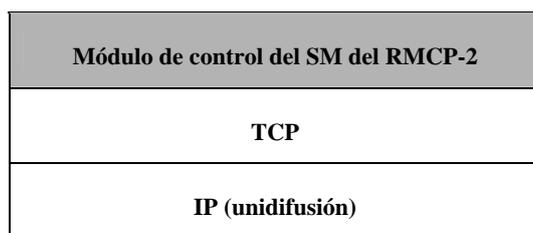


Figura 2 – Pila de protocolo de un SM

Un MA, que se refiere tanto al SMA como al RMA, construye un trayecto de entrega por multidifusión con retransmisión desde un emisor hasta varios receptores y luego retransmite los datos a lo largo del trayecto. Los MA están compuestos por un *módulo de control* y un *módulo de datos* del RMCP-2. El módulo de control establece el trayecto de entrega de datos retransmitidos. El módulo de transporte configura un canal de datos a lo largo del trayecto construido por el módulo de control y luego retransmite los datos a través del canal.

El módulo de control del MA configura el árbol de control desde el SMA a cada MA hoja mediante el intercambio de mensajes de control con otros MA. El SM también utiliza el módulo de control para el control y gestión de la sesión. En la figura 3 se presenta la pila de protocolo del módulo de control del MA.

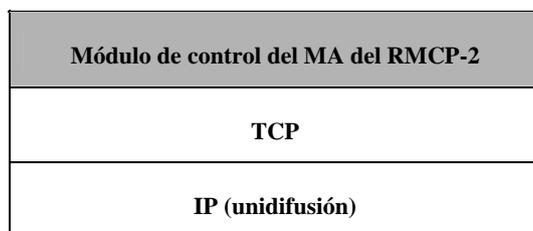


Figura 3 – Pila de protocolo de un módulo de control del MA

El módulo de datos del MA transmite datos de aplicación a través del árbol configurado por el módulo de control. En la figura 4 se presenta la pila de protocolo del módulo de datos del RMCP-2. De ser necesario, se puede incluir cualquier tipo de mecanismo de transporte, ya que el RMCP-2 no impone ninguna restricción respecto al tipo de datos de aplicación que se han de entregar.

A fin de garantizar que el RMCP-2 pueda adoptar cualquier tipo de mecanismo de transporte de datos, dos MA (concretamente, el agente de multidifusión progenitor (PMA) y el agente de multidifusión vástago (CMA)) construyen un trayecto para la entrega de datos a través del árbol, intercambiando los perfiles de datos que se describirán más adelante.



Figura 4 – Pila de protocolo del módulo de datos del RMCP-2

Las topologías de los dos trayectos destinados al control y la entrega de datos son normalmente la misma, ya que se construye un trayecto de entrega de datos a lo largo del árbol de control del RMCP-2. A lo largo del trayecto de entrega de datos, se pueden entregar los datos de aplicación del SMA a cada MA hoja. En el anexo B y en el anexo C se presentan, a modo de información, dos mecanismos posibles para la entrega fiable de datos en tiempo real.

5.3 Modelo de entrega simplex del RMCP-2

Los servicios previstos del RMCP-2 son *servicios de radiodifusión simplex*, como televisión en vivo por Internet y distribución de software. En esos modelos de servicio es importante construir un trayecto óptimo para la entrega de datos desde un emisor a varios receptores. El RMCP-2 puede soportar un modelo para la entrega de datos simplex, haciendo uso de los módulos de control y de datos del MA.

El trayecto de entrega de datos que el RMCP-2 emplea es un *árbol de multidifusión con retransmisión por cada fuente*. Puede construirse un *canal de datos unidireccional en tiempo real, o fiable* a lo largo del trayecto de multidifusión con retransmisión por cada fuente. En la figura 5 se presenta uno de los árboles de multidifusión con retransmisión que el RMCP-2 podría configurar para *aplicaciones simplex en tiempo real, o fiables*.

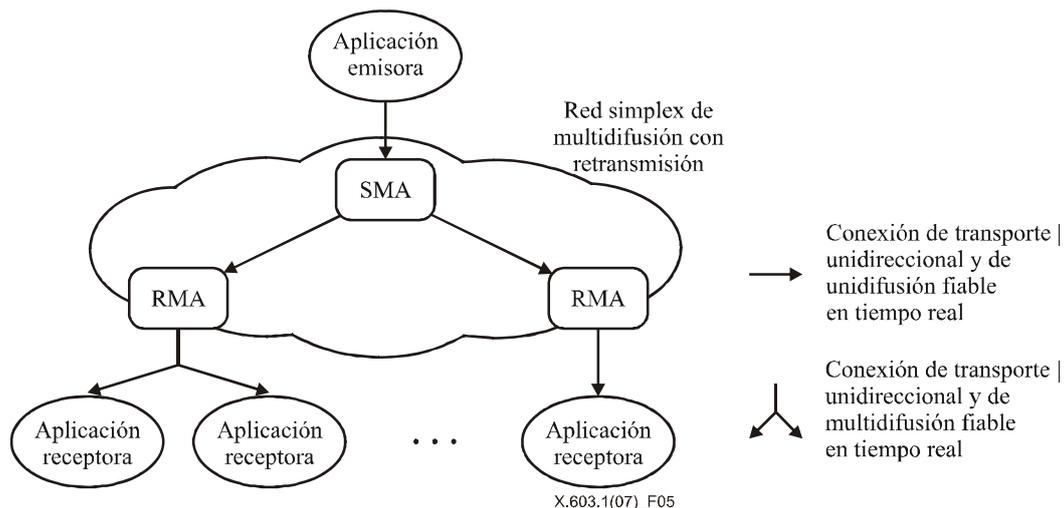


Figura 5 – Árbol de multidifusión con retransmisión configurado por el RMCP-2

5.4 Tipos de mensajes del RMCP-2

Para construir y mantener un árbol de multidifusión con retransmisión, los pares que emplean el protocolo RMCP-2 intercambian varios mensajes de control utilizando un esquema *petición y respuesta*. En el cuadro 1 se enumeran los mensajes de control del RMCP-2, agrupados según su función.

Cuadro 1 – Mensajes de RMCP-2

Mensajes	Descripciones	Operaciones del RMCP
SUBSREQ	Petición de suscripción	Inicio de la sesión
SUBSANS	Respuesta de suscripción	
PPROBREQ	Petición de búsqueda de progenitor	Descubrimiento del mapa
PPROBANS	Respuesta de búsqueda de progenitor	
HSOLICIT	Solicitar un HMA	Elección de HMA
HANNOUNCE	Anuncio del HMA	
HLEAVE	Abandono del HMA	
RELREQ	Petición de retransmisión	Entrega de datos
RELANS	Respuesta de retransmisión	
STREQ	Petición del informe de estado	Supervisión de la sesión
STANS	Informe de estado	
STCOLREQ	Petición de recopilación de informes de estado	
STCOLANS	Respuesta de recopilación de informes de estado	
LEAVREQ	Petición de abandono	Abandono de la sesión
LEAVANS	Respuesta de abandono	
HB	Latido	Latido de la sesión
TERMREQ	Petición de terminación	Terminación de la sesión
TERMANS	Respuesta de terminación	

6 Funcionamiento del protocolo

En esta cláusula se describen detalladamente las funciones del protocolo RMCP-2 y su funcionamiento. Todos los componentes descritos cumplen con las definiciones dadas en la Rec. UIT-T X.603 | ISO/CEI 16512-1.

6.1 Funcionamiento de los SM

6.1.1 Inicio de la sesión

Para que el SM pueda crear una nueva sesión, el proveedor de contenidos (CP, *content provider*) debe proporcionar un perfil de sesión, en el que se incluyan los detalles para crear la sesión, como el nombre de la sesión, las características de los medios y la dirección del grupo. Para distinguir las sesiones, el SM crea un identificador de la sesión (SID) globalmente singular. Una vez creada satisfactoriamente la sesión, el SM informa el SID al CP. Los CP pueden anunciar la creación de la sesión a través de un servidor de páginas web o del correo electrónico. En esta especificación no se trata la forma en que se anuncian las sesiones.

Una vez creada satisfactoriamente la sesión, el SM espera a que le lleguen peticiones de suscripción de los MA. Cuando el SM recibe una petición de suscripción de un MA, el SM decide si la acepta.

6.1.2 Control de admisión

Al recibir la petición de suscripción del MA, el SM primero revisa el SID del mensaje de petición y luego determina si es factible aceptar la petición conforme a las políticas de la sesión. La sesión RMCP-2 puede funcionar de forma privada o de forma pública utilizando información adicional, como información del sistema e información de autenticación.

Si el SID contenido en la SUBSREQ del MA es válido, el SM revisa la MAID propuesta y el perfil de datos propuesto. En la sesión se utilizará la MAID propuesta por el MA, pero si ésta tiene un valor nulo o duplicado, el SM propondrá un valor singular. Si no es factible soportar el perfil de datos propuesto, el SM deberá rechazar la petición, anunciando el motivo; en caso contrario, el SM podría negociar el perfil de datos que mejor convenga e informar el resultado de la negociación.

Una vez aceptada la SUBSREQ del MA, el SM responde con una MAID confirmada, la NL e información propia de la sesión.

Para expulsar un MA concreto, el SM inicia el procedimiento de expulsión mediante el envío de una petición de abandono (LEAVREQ) con el código de motivo "expulsado" (KO, *kicked-out*) y luego actualiza la lista de miembros de la sesión. El MA abandona rápidamente la sesión, tan pronto recibe el mensaje LEAVREQ del SM. En la figura 6 se ilustra el procedimiento en el que el SM envía un mensaje LEAVREQ con el código de motivo KO y luego el MA B abandona la sesión, notificando a su PMA y a sus CMA acerca de la expulsión.

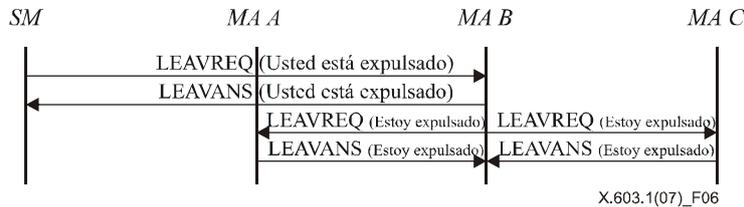


Figura 6 – El SM expulsando al MA

6.1.3 Supervisión de la sesión

El SM puede recuperar información sobre el estado de un MA en particular intercambiando mensajes de petición y respuesta de estado con cualquier MA concreto. Al recibir el mensaje de petición de estado, el MA responde con un mensaje de respuesta de estado que contiene la información solicitada. En la figura 7 se muestra al SM supervisando un MA en particular.

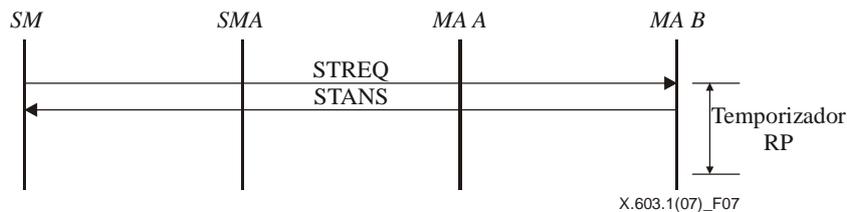


Figura 7 – Supervisión del árbol: informe del estado

El SM también puede recopilar información sobre el estado de la totalidad o de una parte de la sesión. En este caso, el SM envía un mensaje de petición de recopilación de estado al MA superior de la parte en cuestión. Cuando recibe el mensaje de petición de recopilación de estado, el MA debe enviar al SM la respuesta sobre el estado, con la información correspondiente al MA y sus vástagos. Si la sesión es grande, el empleo de este mecanismo para la sesión total podría sobrecargar la red y los recursos del sistema. A fin de limitar el campo de acción de la supervisión, los mensajes de recopilación de estado deben incluir un valor de la profundidad.

6.1.4 Terminación de la sesión

La sesión en curso de un SM podría finalizar por dos motivos:

- 1) por solicitud administrativa; y
- 2) por abandono del SMA.

En la figura 8 se presenta el procedimiento de terminación de la sesión del SM.

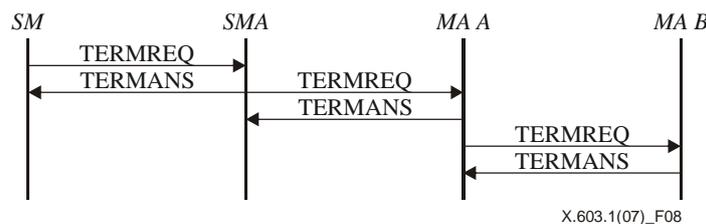


Figura 8 – Terminación de la sesión solicitada por el SM

Como la sesión RMCP-2 puede continuar sólo si el SMA está activo, el SMA debe notificar su abandono al SM. Al recibir la notificación, el SM debe terminar la sesión cuanto antes. En 6.2.4.4 se describe la finalización de la sesión por abandono del SMA.

6.2 Funcionamiento del MA

6.2.1 Suscripción a la sesión

La primera etapa que debe cumplir un MA para participar en una sesión de RMCP-2 es la suscripción. Cada MA debe suscribirse a la sesión enviando una petición de suscripción (SUBSREQ) al SM. Cabe señalar que el SMA debe finalizar su suscripción antes que cualquier otro y debe actuar como nodo raíz de la jerarquía arborescente. En este punto todos los MA deben conocer los detalles del perfil de la sesión, como la dirección del SM y las políticas.

En la figura 9 se muestra el procedimiento de suscripción a una sesión RMCP-2. La sesión RMCP-2 puede iniciar después de que el SMA se haya suscrito satisfactoriamente.



Figura 9 – Suscripción del SMA

En la figura 10 se presenta el procedimiento de suscripción de un MA (para los MA A y MA B). A fin de suscribirse a una sesión RMCP-2, cada MA envía un SUBSREQ al SM. Cuando recibe el SUBSREQ del MA, el SM decide si acepta la petición de suscripción. Si acepta la petición, el SM responde con un SUBSANS que contenga información de iniciación, como la NL. De no aceptarla, el SM responde con un SUBSANS que contenga el código apropiado de motivo de error.

Después de recibir del SM un SUBSANS afirmativo, el MA (MA A y MA B) puede finalizar la fase de suscripción.

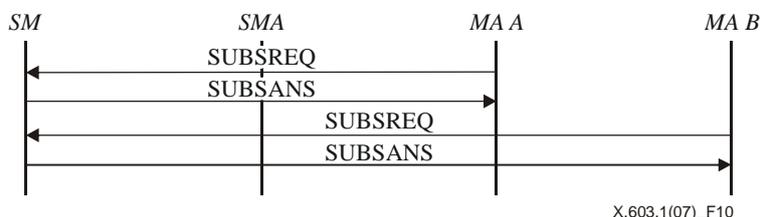


Figura 10 – Suscripción del MA

6.2.2 Descubrimiento del mapa

Por estar interconectados lógicamente, a los MA se les dificulta conocer la condición de la red entera. No obstante, cada MA puede explorar a los demás MA en la red RMCP-2 y medir su distancia hasta ellos, utilizando procedimientos de descubrimiento de mapas. El mecanismo para el descubrimiento del mapa consta de dos partes. Una de ellas se utiliza en zonas habilitadas para multidifusión, como la subred de una LAN, y la otra en zonas inhabilitadas para multidifusión, como una WAN.

6.2.2.1 Al interior de la zona habilitada para multidifusión

Es conveniente asignar como PMA al nodo más cercano. La distancia de red en RMCP-2 es una función de la fluctuación de fase del retardo, del número de saltos y del ancho de banda.

Normalmente, uno de los MA de la red está más cercano que los otros MA. Cada MA busca un candidato a PMA en su red local enviando por multidifusión una solicitud de agente de multidifusión principal (HSOLICIT), inicialmente a una dirección prefijada (también conocida como dirección de difusión). Si no hay respuesta, el MA se convierte en el HMA, que es uno de los MA de la red habilitada para multidifusión.

Una vez el MA se convierte en el HMA, el HMA anuncia su existencia a la red habilitada para multidifusión, enviando mensajes HANNOUNCE periódicos. El HMA envía rápidamente un HANNOUNCE si recibe un HSOLICIT de la zona habilitada para multidifusión.

El MA que recibe un HANNOUNCE del HMA supone que en su red ya existe un HMA y designa al HMA como candidato principal a PMA. En la figura 11 se muestra el procedimiento de elección del HMA.

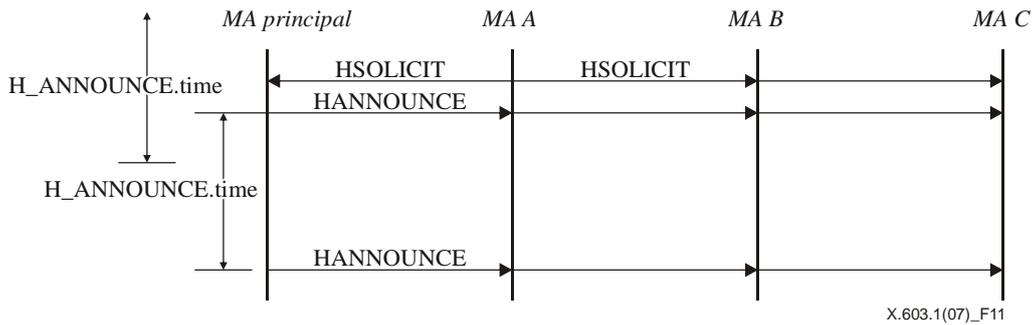


Figura 11 – Los mensajes de solicitud de HMA y de anuncio del HMA

En la figura 12 se muestra cómo un MA se convierte en HMA. Si un MA no recibe ningún HANNOUNCE durante un cierto tiempo ($H_SOLICIT.time \times N_SOLICIT$), se convierte en el nuevo HMA y difunde, hacia la zona habilitada para la multidifusión, un HANNOUNCE periódico cada H_ANNOUNCE.time.

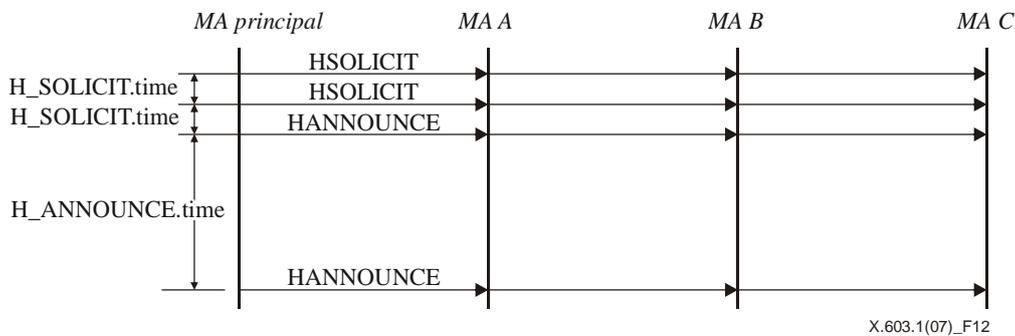


Figura 12 – Un MA se convierte en el nuevo HMA

En la figura 13 se muestra cómo se permanece como HMA. Una vez se convierte en HMA, el MA difunde cada H_ANNOUNCE.time un mensaje HANNOUNCE hacia la red habilitada para la multidifusión.

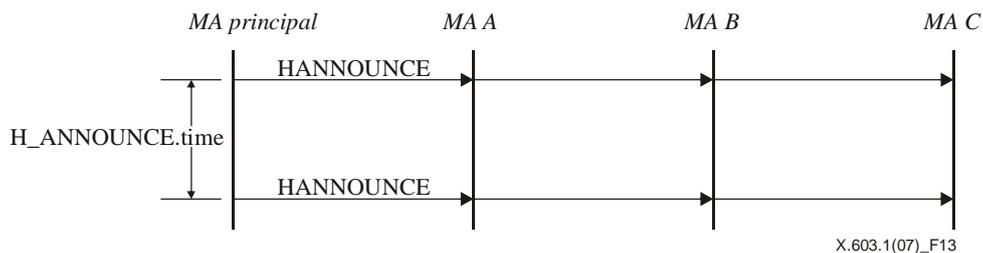


Figura 13 – Anuncio periódico del HMA principal

En la figura 14 se muestra cómo se selecciona un nuevo HMA. Si no se recibe ningún HANNOUNCE durante un tiempo dado ($H_ANNOUNCE.time \times N_ANNOUNCE$), el HMA espera durante un tiempo de guarda aleatorio. Si el HANNOUNCE no llega, el MA se convierte en el HMA de la red habilitada para multidifusión. Pero si llega el HANNOUNCE, el MA descarta el tiempo de guarda y selecciona al HMA como candidato principal a PMA. Si llegan más de dos mensajes HANNOUNCE, el emisor del primer mensaje HANNOUNCE se convierte en HMA. Si hay una colisión entre dos o más HANNOUNCE, el HMA deberá ejecutar el algoritmo para la supresión de duplicación.

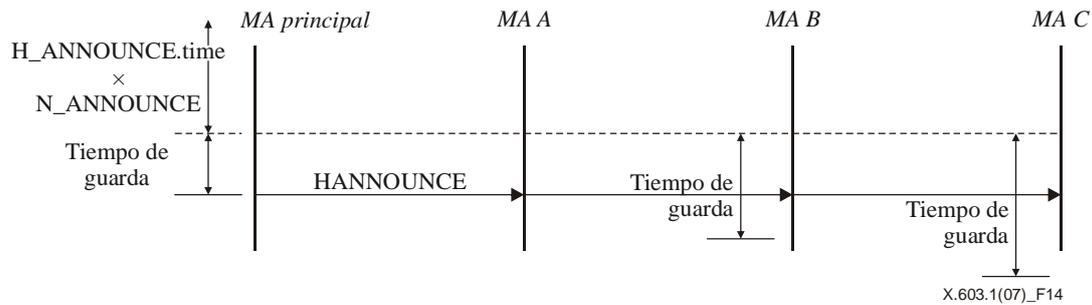


Figura 14 – Elección de un nuevo HMA

Como todos los MA de una red habilitada para la multidifusión pueden ser elegidos como HMA, todos los MA deberían llevar a cabo el mecanismo de descubrimiento de la red externa. El procedimiento detallado se analiza en la subcláusula a continuación.

6.2.2.2 Zona externa habilitada para la multidifusión

Cada MA debería iniciar el procedimiento de descubrimiento de vecinos, con base en la información de iniciación suministrada por el SM. Como se indica en la figura 15, los MA pueden conocer gradualmente la topología arborescente RMCP-2, intercambiando con cada MA la información que posee sobre el árbol.

El siguiente es el mecanismo básico para descubrir el árbol: Primero, utilizando los mensajes PPROBREQ y PPROBANS, cada MA puede intercambiar un cierto número de NL en cada intervalo de tiempo (PPROBE.time). Habida cuenta del número finito de recursos de cada MA, debería limitarse el número máximo de NL que se intercambien.

Para evitar que los MA se inunden de mensajes PPROBREQ, debería limitarse a N_MAX_PROBE el número máximo de mensajes PPROBREQ que pueden emitirse en un cierto periodo de tiempo.

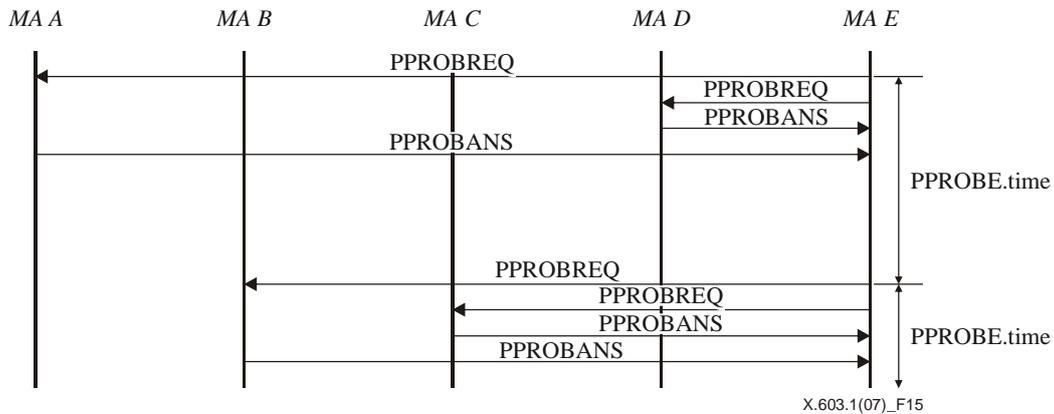


Figura 15 – Secuencia del protocolo de descubrimiento del mapa

6.2.3 Adhesión al árbol

El procedimiento de adhesión al árbol permite a cada MA elegir un PMA dentro de una sesión RMCP-2 suscrita. En la figura 16 se muestra cómo un MA elige su PMA con base en la NL suministrada por el SM. El MA que se adhiere (MA E) envía un mensaje PPROBREQ a uno o a varios de los nodos que figuran en la NL (MA A, C y D) y espera un mensaje PPROBANS de aceptación. Cuando reciba un mensaje PPROBANS, el MA E puede elegir el MA más cercano. En la figura 16, el MA que se adhiere (nodo E) estima que el MA D es el mejor y por tanto escoge al MA D como su PMA. Una vez elija el PMA, el MA adherente (nodo E) enviará al MA D un RELREQ con un perfil de datos propuesto.

Si puede aceptar el RELREQ, el MA D responde con un RELANS afirmativo, en el que incluye el perfil de datos que se haya acordado utilizar. De lo contrario, el MA D devuelve un código de motivo para el rechazo.

Si se recibe el RELANS afirmativo, se crea un canal de datos entre el MA D y el MA E, de conformidad con el perfil acordado; en caso contrario, el MA E debe intentar con el segundo mejor candidato a PMA.

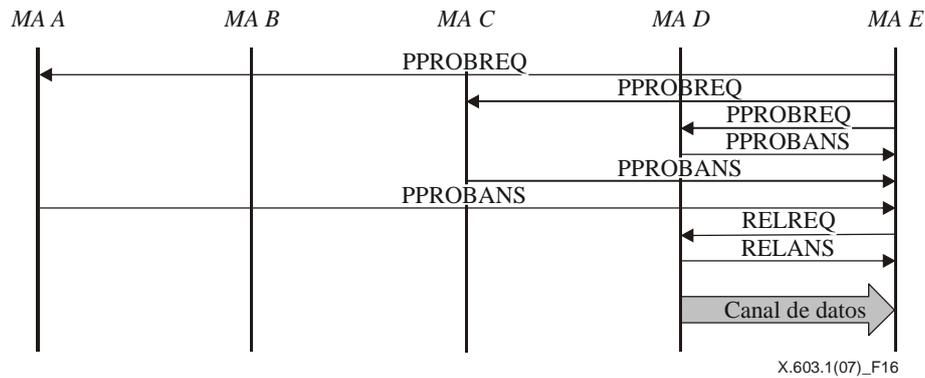


Figura 16 – Secuencia del protocolo de adhesión satisfactoria a un árbol

Si ningún MA desea retransmitir datos al MA adherente, el MA adherente puede volver a ejecutar el *procedimiento de adhesión al árbol*, después de un tiempo de espera. El usuario puede fijar el tiempo de espera, pero ese tema no se trata en la presente especificación. En la figura 17 se ilustra el caso en que todos los MA enumerados en la NL suministrada por el SM rechazan la petición de retransmisión del nodo E. No obstante, por los intercambios anteriores de PPROBREQ y PPROBANS, el MA E ya conoce de la existencia del MA B y podrá volver a iniciar el procedimiento de adhesión al MA B.

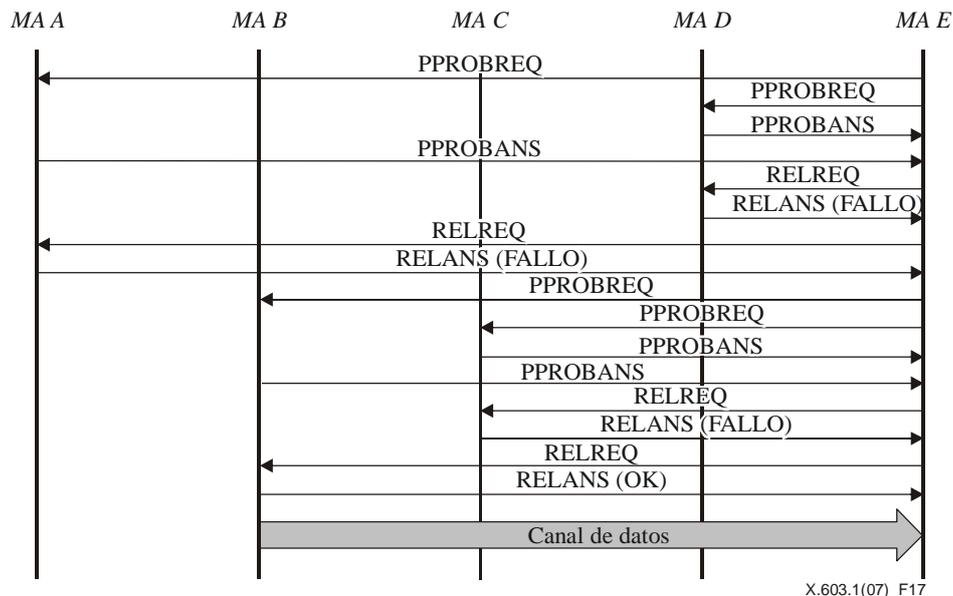


Figura 17 – Secuencia de un intento no satisfactorio de adhesión al árbol y de un nuevo intento

6.2.4 Abandono

Un MA RMCP-2 puede abandonar una sesión que esté en curso. Para que el árbol RMCP-2 sea resistente, los MA deben notificar el abandono a su PMA y a sus CMA. Tras recibir esta notificación, cada PMA y CMA deberá seguir el procedimiento adecuado.

El RMCP-2 contempla cuatro tipos de abandono. El primero es cuando un MA abandona la sesión por solicitud de un usuario del servicio. El segundo es cuando un MA abandona su PMA con el fin de cambiar de progenitor. El tercero es cuando un MA es expulsado por su PMA o por el SM. El último tipo es cuando el SMA abandona la sesión. En las siguientes subcláusulas se describen las operaciones detalladas de estos tipos de abandono.

6.2.4.1 Cuando un MA abandona la sesión

Los MA pueden abandonar en cualquier momento la sesión en curso. Antes de abandonarla, el MA debe notificar su abandono al PMA y a los CMA. El PMA suprime el nodo de su lista de CMA y reserva el espacio para un nuevo CMA.

a) *El MA abandona cuando está inhabilitado el mecanismo de entrega de datos por multidifusión*

Para abandonar la sesión, el MA envía un mensaje LEAVREQ a sus CMA. Cada CMA que recibe el mensaje LEAVREQ debe iniciar rápidamente el procedimiento de conexión a un PMA alternativo, enviando un mensaje RELREQ al PMA candidato. Si el resultado es satisfactorio, el CMA envía un mensaje LEAVANS al antiguo PMA.

En la figura 18 se muestra la forma en que actúa el MA C cuando el HMA abandona una sesión en la que no se emplea el mecanismo de entrega de datos por multidifusión. El MA C trata de abandonar la sesión enviando un mensaje LEAVREQ al MA D y al MA E, que son los CMA de MA C. Cuando reciben el mensaje LEAVREQ, tanto el MA D como el MA E envían un mensaje RELREQ a sus candidatos a PMA.

Una vez se haya vinculado con éxito a un nuevo PMA (MA A y MA B), cada MA (MA D y MA E) envía un mensaje LEAVANS al PMA actual (MA C). Después de recibir el mensaje LEAVANS de sus CMA, el MA C envía un mensaje LEAVREQ a su PMA (MA B). El PMA luego libera al MA de su lista de CMA. Si el MA que abandona no tiene CMA, éste sencillamente envía un LEAVREQ a su PMA.

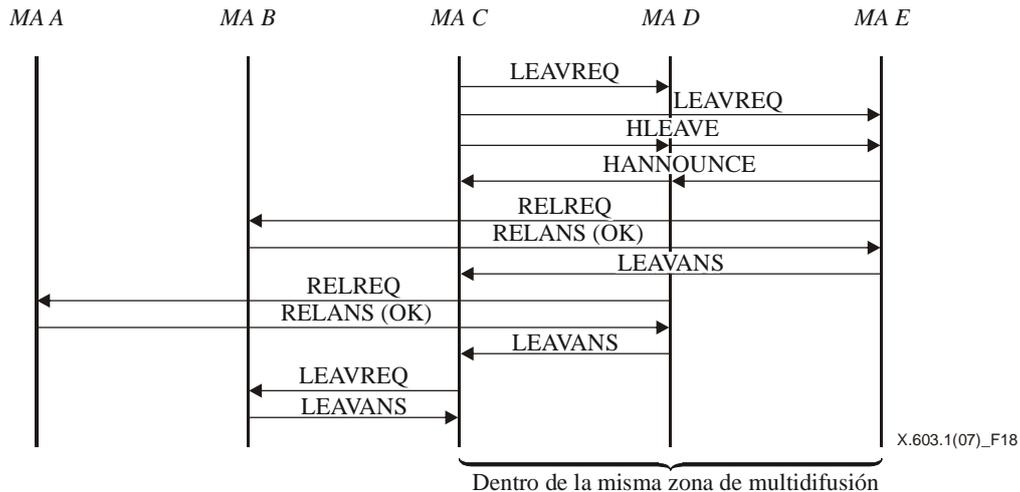


Figura 18 – El HMA abandona con el mecanismo de entrega de datos inhabilitado para la multidifusión

En la figura 19 se muestra la forma en que un MA, que no es el HMA, abandona la sesión cuando se emplea un mecanismo de entrega de datos inhabilitado para la multidifusión. En este caso hipotético, los procedimientos de abandono de un MA que es HMA y de un MA que no lo es son iguales, con la salvedad de que el HMA sigue la secuencia de intercambio de HLEAVE.

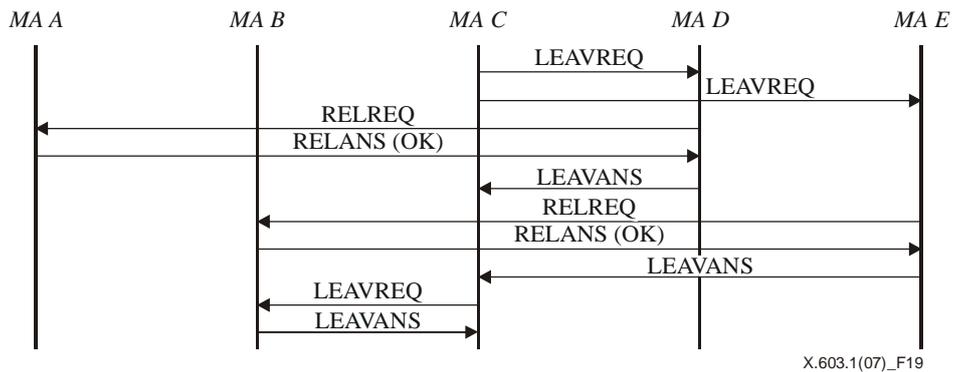


Figura 19 – El MA normal abandona con el mecanismo de entrega de datos inhabilitado para la multidifusión

b) *El MA abandona cuando está habilitado el mecanismo de entrega de datos por multidifusión*

Hay dos casos de MA que abandonan dentro de una zona habilitada para la multidifusión. El primero es cuando abandona el HMA y el segundo es cuando abandona un MA normal. Cuando el HMA de una zona habilitada para la multidifusión desea abandonar la sesión, éste debe notificar el abandono a los CMA dentro de la red local así como a los CMA y al PMA al exterior de la red.

En la figura 20 se muestra la forma en que el MA C, que actúa como HMA, abandona una sesión en que se emplea el mecanismo de entrega de datos por multidifusión. El HMA (MA C) envía un LEAVREQ a su CMA directo (MA F) al exterior de la red local. Tras recibir el mensaje LEAVREQ, el MA F inicia el cambio de progenitor y responde al MA C con un mensaje LEAVANS y envía por multidifusión hacia la red local un mensaje HLEAVE con una lista vacía de candidatos a HMA. El mensaje HLEAVE se utiliza para anunciar que el HMA abandona.

Después de recibir el mensaje HLEAVE del HMA, tanto el MA D como el MA E de la figura 20 esperan durante un cierto tiempo de guarda antes de enviar por multidifusión el mensaje HANNOUNCE. El MA D envía primero el mensaje HANNOUNCE y se convierte en el nuevo HMA. Esto ocurre porque el MA D utiliza un menor tiempo de guarda que cualquier otro MA. Como el MA C que abandona es un punto que se conecta a la red externa habilitada para la difusión, el MA D debería tomar el papel del MA C, conectándose al PMA al exterior de la red. En la figura 20 se ilustra cómo el MA D elige como progenitor al MA B, que es el PMA del MA C.

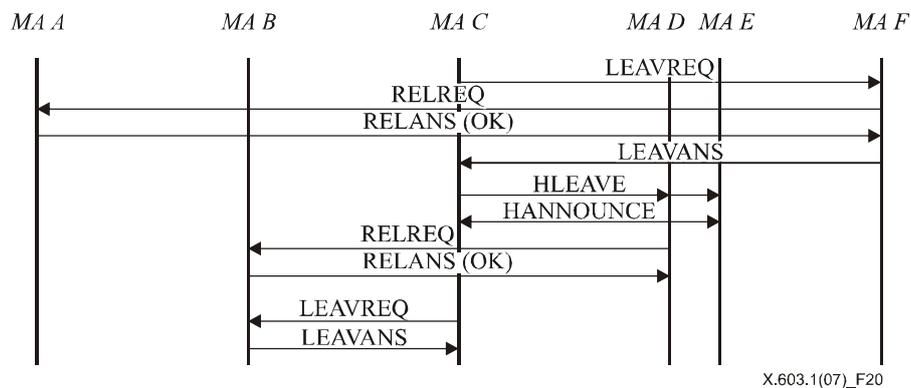


Figura 20 – Abandono del MA con entrega de datos por multidifusión

Cuando un MA diferente al HMA de una zona habilitada para la multidifusión abandona la sesión, lo hace silenciosamente. Ni el MA D ni el MA E de la figura 20 necesitan notificar su abandono a los otros MA.

6.2.4.2 Cuando un MA abandona su PMA para cambiar de progenitor

El MA que desee cambiar de PMA, puede abandonar su PMA actual. En ese caso, no es necesario que el MA envíe un mensaje LEAVREQ a sus CMA. Si reciben datos satisfactoriamente, los CMA no necesitan saber del abandono. Para cambiar de PMA, el MA envía un mensaje RELREQ al candidato a PMA. Cuando el PMA anterior recibe el mensaje LEAVREQ con el código de motivo fijado a PS (cambio de progenitor, *parent switching*), elimina de su lista de CMA al MA que le abandona, pero conserva la información en su NL, pues el MA que le abandona continúa activo en la sesión.

En la figura 21 se muestra la forma en que un MA cambia de progenitor. Cabe señalar que, a fin de no modificar el árbol, los MA pueden cambiar de progenitor sólo si reciben un HB. El mecanismo HB se describe en la subcláusula 6.2.5.1.

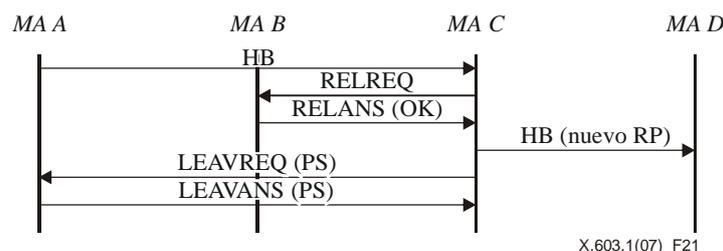


Figura 21 – Abandono del MA por cambio de progenitor

6.2.4.3 Cuando se expulsa al MA

El protocolo RMCP-2 posee un mecanismo para descartar ciertos MA. Por ejemplo, cuando un administrador de red desea que el SM descarte a un MA en particular o cuando un MA expulsa a un CMA después de que se da cuenta de que no puede soportar más CMA.

a) *Expulsión de un MA por su PMA*

Un PMA puede expulsar a uno de sus CMA cuando sus recursos escaseen y ya no pueda mantener al CMA o cuando el PMA advierta que uno de sus CMA ha agotado los recursos del sistema. El MA debería encontrar otro candidato a PMA que le permita ser el nuevo PMA.

En la figura 22 se presenta un ejemplo del flujo de mensajes. Inicialmente el PMA, concretamente el MA C, envía un mensaje LEAVREQ con el código de motivo KO, para expulsar al MA D. El MA D busca otros PMA y envía una petición de retransmisión. Tras cambiar de progenitor, el MA D transmite un mensaje LEAVANS a su antiguo PMA.

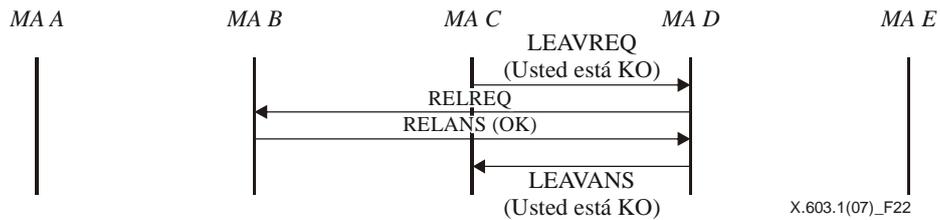


Figura 22 – El MA es expulsado por su PMA

b) *Expulsión de un MA por parte del SM*

El SM puede descartar cualquier MA, enviando un mensaje LEAVREQ con el código de motivo expulsado (KO). El MA debe abandonar rápidamente la sesión tras recibir el mensaje LEAVREQ del SM. Tras la expulsión, el SM debe actualizar su lista de miembros de la sesión.

En el flujo de mensajes que aparece en la figura 23, el SM le dice al MA B que abandone, enviándole un mensaje LEAVREQ con el código de motivo KO. El MA B debe abandonar la sesión, pero antes de irse debe notificar a su PMA y CMA acerca de la expulsión.

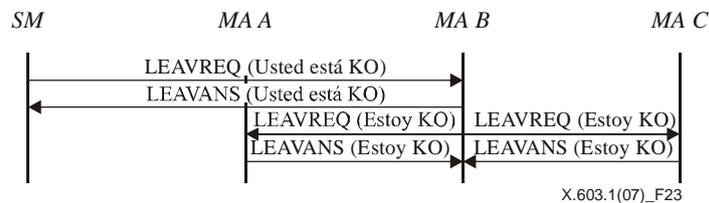


Figura 23 – El MA es expulsado por el SM

6.2.4.4 El SMA abandona la sesión

Como no es posible que la sesión RMCP-2 exista sin un SMA, el SMA nunca debería abandonar la sesión antes de que ésta haya terminado. Si el SMA abandona la sesión, ésta debe finalizar.

En la figura 24 se presenta el procedimiento que sigue el SMA para abandonar la sesión. El SMA envía un mensaje LEAVREQ al SM. Tras recibir el mensaje LEAVREQ del SMA, el SM suprime la información de la sesión y responde con un mensaje LEAVANS. Una vez reciba el mensaje LEAVANS del SM, el SMA envía a sus CMA directos un mensaje LEAVREQ con el código de motivo *abandono del SMA*. El LEAVREQ con código de motivo *abandono del SMA* debe retransmitirse rápidamente hacia abajo, para que finalice la sesión RMCP-2.

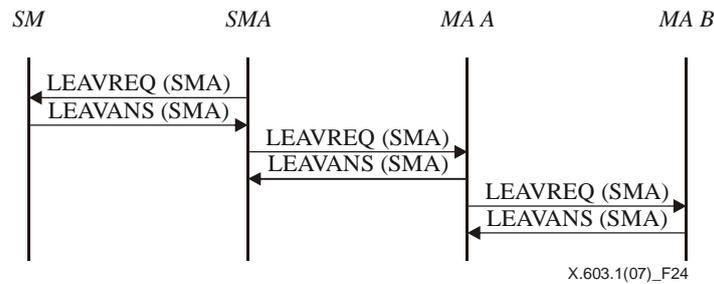


Figura 24 – El SMA abandona

6.2.5 Mantenimiento

6.2.5.1 Latido (HB, heartbeat)

El objetivo del latido es hacer que el árbol RMCP-2 construido sea resistente. El latido, que proporciona a la sesión información de sincronismo unificada, ayuda a que los MA detecten si la sesión está activa. También contiene información útil sobre el trayecto de entrega de datos, denominada ROOTPATH (trayecto desde la raíz). El ROOTPATH incluye un trayecto de datos retransmitidos que refleja la jerarquía arborescente.

En la figura 25 se ilustra el procedimiento de latido del RMCP-2. En este procedimiento el SMA envía a sus vástagos el HB, a lo largo del ROOTPATH. Cada vástago anexa al HB información sobre el salto, la que puede incluir la MAID, la distancia de red por salto e información sobre el sistema, como el ancho de banda de entrada y de salida, el número posible de CMA, etc., y retransmite el HB modificado a sus propios vástagos. Finalmente, el ROOTPATH contiene todos los MA recorridos en el árbol.

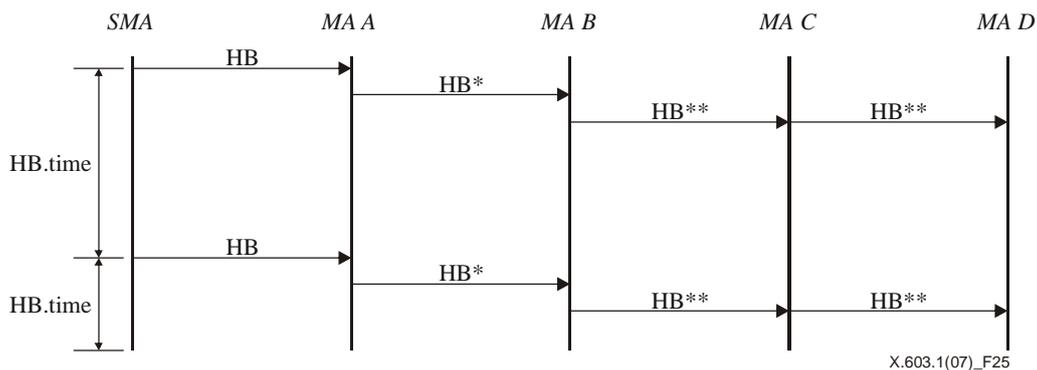


Figura 25 – Latido

6.2.5.2 Supervisión

El protocolo RMCP-2 posee dos tipos de mecanismos de supervisión. Mediante el primero, que se indica en la figura 26, se supervisa un MA en particular. El otro, que se muestra en la figura 27, se utiliza para supervisar una parte del árbol a través de un MA concreto.

En la figura 26 se ilustra la forma en que un SM supervisa un MA en particular. En este procedimiento el SM envía un mensaje STREQ al MA B para solicitar uno o varios tipos de información sobre el estado del MA B. Como respuesta, el MA B envía al SM un mensaje STANS con la información solicitada.

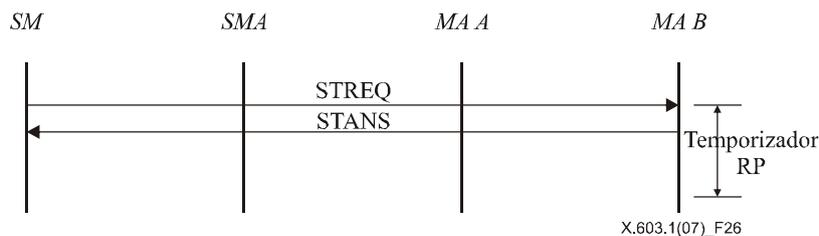


Figura 26 – Supervisión del árbol mediante solicitud de informe de estado

En la figura 27 se indica la forma en que el SM interroga la zona abarcada del árbol. Es decir, el SM pide información unificada sobre la zona abarcada del árbol, enviando un mensaje STREQ a un MA concreto (SMA y MA A) a fin de recopilar información sobre la zona específica.

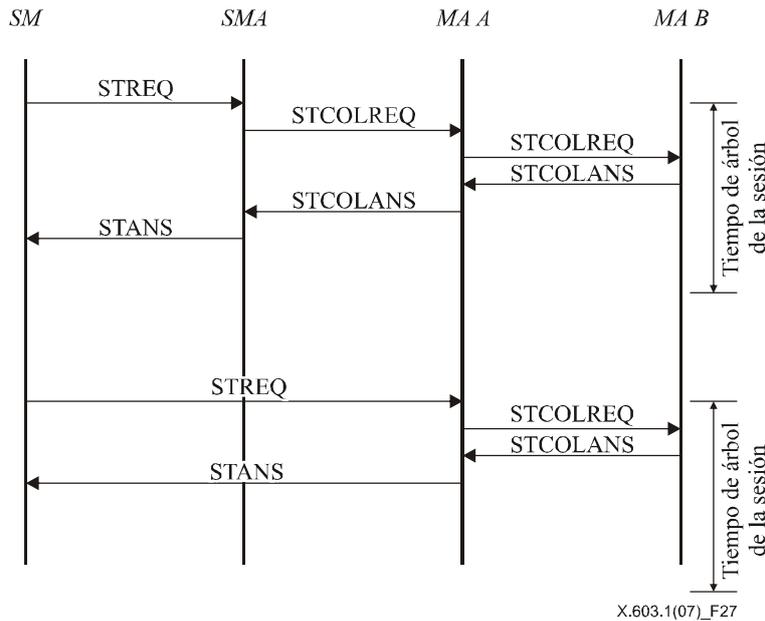


Figura 27 – Supervisión del árbol mediante recopilación de informes de estado

6.2.5.3 Detección de averías y recuperación

Cada MA realiza este procedimiento cuando detecta averías en la red y soluciona el problema para que el árbol RMCP-2 sea resistente. Las averías de la red, como los bucles y la subdivisión por general se originan en acciones frecuentes y descuidadas de los MA. El protocolo RMCP-2 proporciona los siguientes mecanismos que permiten detectar ese tipo de avería y realizar la recuperación.

a) Detección de bucles y recuperación

Pueden detectarse los bucles revisando el ROOTPATH incluido en el HB. Como el ROOTPATH contiene la trayectoria desde el SMA, un mismo salto registrado dos veces en el ROOTPATH indica que se formó un bucle. Cuando ocurre un bucle, cada MA utiliza el mecanismo de recuperación ante bucles que se indica a continuación: en el caso hipotético de la figura 28, el MA Y examina el HB. El MA Y detecta un bucle cuando recibe HB_{n+3} ya que MA Z, que es un CMA de MA Y, figura dos veces en el ROOTPATH. Para recuperarse ante el bucle, el MA Y envía al MA Z un mensaje LEAVREQ, para desconectarse.

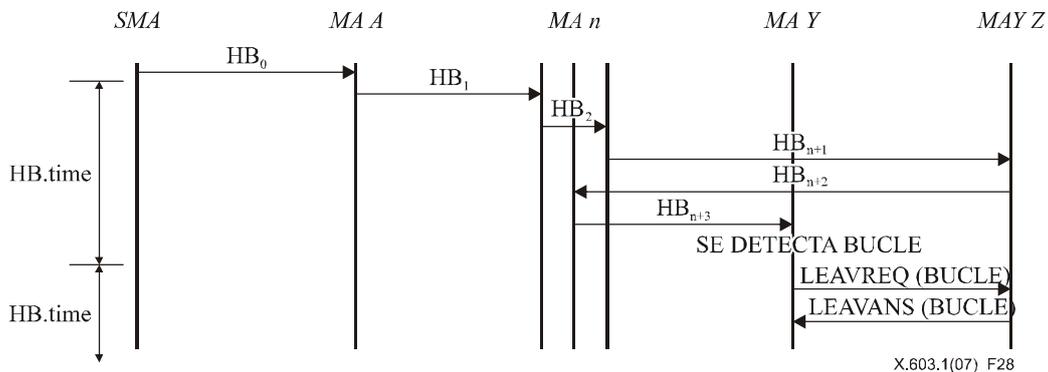


Figura 28 – Detección de bucles y recuperación

b) *Detección de subdivisiones de la red y recuperación*

Cuando un MA deja de recibir mensajes HB durante un tiempo dado, el MA supone que fue separado del árbol. Este tiempo debería fijarse lo suficientemente amplio como para permitir retardos de red. El protocolo RMCP-2 define este tiempo como $HB_TIME \times MAX_PARTITION_CNT$.

Las subdivisiones pueden ocurrir si se avería uno de los asociados de la subdivisión. El MA detecta el origen de la subdivisión contactando con sus asociados. Después el MA resuelve el problema.

En la figura 29 se ilustra la forma en que el MA Z detecta la subdivisión del árbol. Se detecta la subdivisión del árbol cuando el MA Z deja de recibir el mensaje HB durante un cierto periodo de tiempo ($HB_TIME \times MAX_PARTITION_CNT$). Cuando deja de recibirse el mensaje HB, se inicia la transmisión de una serie de mensajes PPROBREQ hacia los demás asociados. En la figura 29 se muestra que el MA Z recibe un mensaje PPROBANS de MA A y de MA B, pero no de MA C, el actual PMA de MA Z. El MA Z detecta que la subdivisión se debe al fallo del PMA directo de MA Z. Para recuperarse de la avería, el MA Z intenta cambiar de progenitor.

Durante el tiempo que tome al MA reparar la partición, los vástagos de MA podrían también detectar que la red se ha subdividido e intentar reparar la subdivisión. Esto significa que la avería de un MA en un solo punto podría ocasionar el desplome de todo el árbol. Para evitar este problema, el MA que esté reparando una avería de la red genera un pseudomensaje HB hacia sus vástagos, a fin de notificar que la sesión está temporalmente subdividida y se encuentra en reparación.

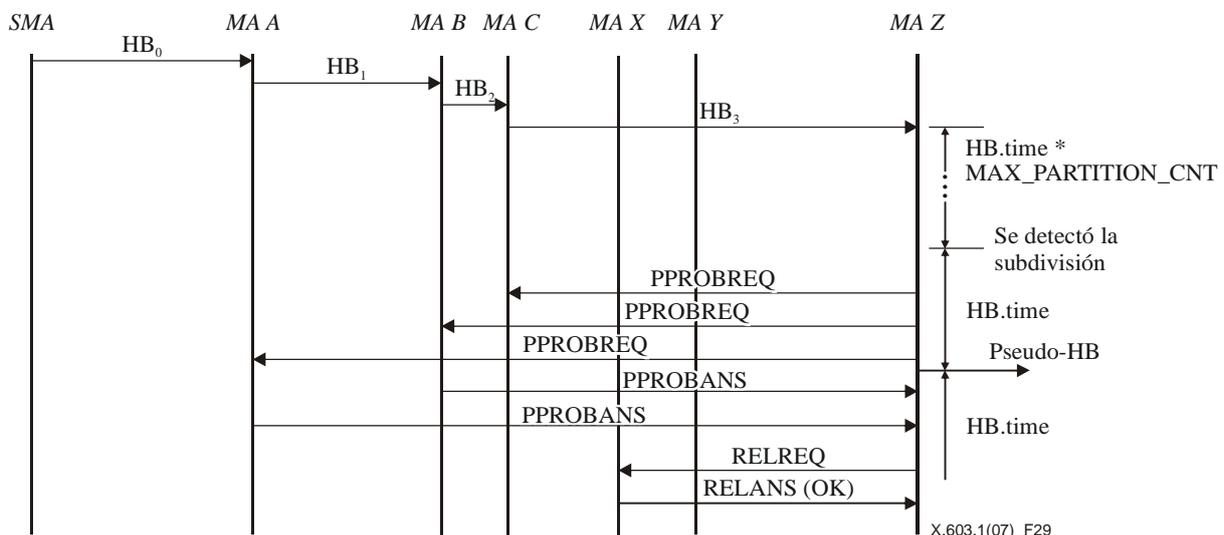


Figura 29 – Detección de una subdivisión de la red y su recuperación

6.2.5.4 Perfeccionamiento del árbol

El procedimiento de perfeccionamiento del árbol tiene lugar cuando un MA encuentra uno o varios candidatos a PMA más eficaces e intenta cambiar a uno de ellos. La aplicación del procedimiento de perfeccionamiento del árbol durante la sesión hace que el árbol RMCP-2 mejore gradualmente.

El procedimiento para hallar nodos mejores utiliza el mecanismo de descubrimiento del mapa descrito en la subcláusula 6.2.2. Con cada iteración del procedimiento de descubrimiento del mapa, cada MA compara los parámetros de QoS de su PMA actual con los del nodo recién descubierto. Cuando halla un MA mejor que su actual PMA, el MA puede cambiar su PMA actual por el MA descubierto, siguiendo el procedimiento para cambio de progenitor descrito en la subcláusula 6.2.4.2.

A medida que se perfecciona el árbol, pueden ocurrir averías de la red, como bucles y subdivisiones. Podrían suceder averías de la red en los siguientes casos particulares: cuando varios MA de una misma rama tratan de cambiar simultáneamente de PMA y cuando varios MA a lo largo de la rama tratan de cambiar consecutivamente de PMA.

Para proteger al árbol de estos peligros, el RMCP-2 garantiza la condición de atomicidad, que permite que los MA puedan cambiar de progenitor sólo si han recibido un mensaje HB en el que no se haya modificado el ROOTPATH.

6.2.6 Terminación

Para finalizar la sesión, el SM envía un mensaje TERMREQ al SMA, tal y como se indica en la figura 30. Un SMA (o MA) que reciba el mensaje TERMREQ del SM (o PMA) devuelve el mensaje TERMANS al SM (o PMA) y luego reenvía el mensaje TERMREQ a sus CMA hasta que éste llegue a los nodos finales del árbol. Finalmente se cierra la sesión.

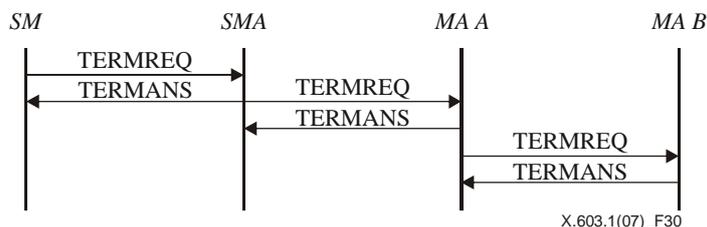


Figura 30 – Terminación de la sesión por parte del SM

7 Formato de los mensajes del RMCP-2

En esta cláusula se describen los formatos de los mensajes del RMCP-2 y la información que éstos requieren. En el capítulo 8 se describe el valor que puede tener la información transmitida en cada mensaje.

7.1 Formato común de los mensajes del RMCP-2

En la figura 31 se ilustra el formato común de los mensajes del RMCP-2. A continuación se indican el nombre y el significado de cada campo:

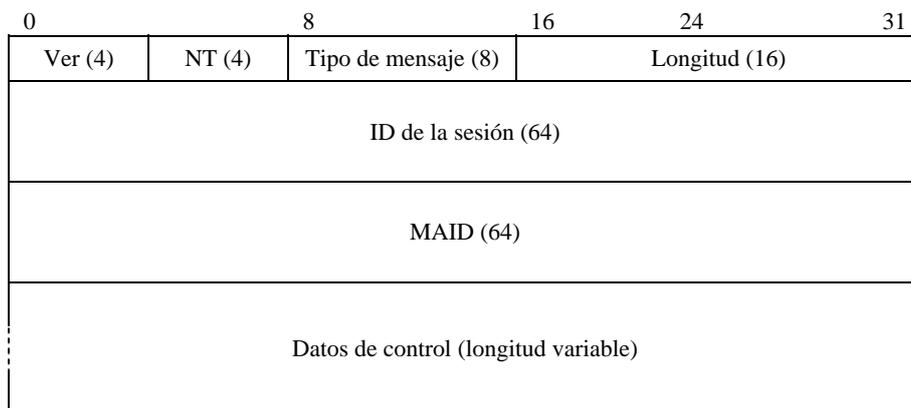


Figura 31 – Formato común de los mensajes del RMCP-2

La descripción de cada campo es la siguiente:

- a) *Versión*: Representa la versión del RMCP utilizada. El valor por defecto para RMCP-2 se fija a 0x2.
- b) *NT (tipo de nodo, node type)*: Representa el tipo de nodo. Debe identificarse a sí mismo como SM, SMA o MA.
- c) *Tipo de mensaje*: Representa el tipo de mensaje.
- d) *Longitud*: Representa la longitud total del mensaje en bytes, incluidos los datos de control.
- e) *ID de la sesión*: Es un entero de 64 bit que identifica la sesión.
- f) *MAID*: Es un valor único de 64 bits utilizado para identificar el MA ante una sesión.
- g) *Datos de control*: Contiene los datos de control utilizados por cada mensaje, según corresponda.

La ID de sesión y la MAID deben ser valores únicos utilizados para identificar la sesión y el MA, respectivamente. El protocolo RMCP-2 proporciona una regla para generar los valores de la ID de la sesión y del MA.

7.1.1 ID de la sesión

La ID de la sesión (SID) es una combinación de la dirección IP local del gestor de sesión (SM) y la dirección de grupo de la sesión. Si se le solicita crear una sesión, el SM puede atribuir la dirección de grupo de la nueva sesión. De esta forma se puede garantizar que la SID sea globalmente única. En la figura 32 se muestra el formato de la SID del RMCP-2.

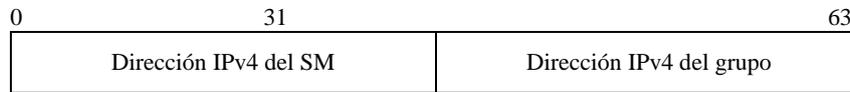


Figura 32 – Formato de la SID del RMCP-2

7.1.2 MAID

La MAID está compuesta por la dirección IP, el número de puerto y el número de serie locales, como se indica en la figura 33. La dirección IP local es la dirección IP del MA. Un MA de una sesión RMCP-2 podría tener que abrir varios puertos para la sesión. El número de puerto utilizado para generar el MAID es el de un puerto de escucha que se abrió, con el fin de recibir mensajes de control del SM o de otros MA, cuando el MA comenzó a ejecutar el RMCP-2.

Los MA se pueden identificar según su número de puerto en un sistema multiusuario. No obstante, es imposible identificar los MA al interior de una red que utilice NAT (traducción de direcciones de red, *network address translation*), ya que varios MA podrían utilizar una misma dirección IP para comunicarse con sus pares al exterior de la red. Para tratar este caso, el SM genera una MAID única, puesto que ésta asigna un valor único en el campo del número de serie cuando recibe una dirección NAT de un MA, y retorna la ID al MA.

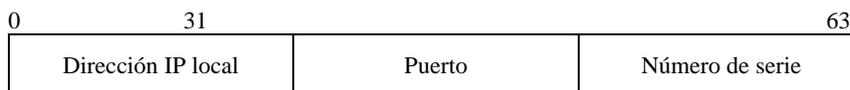


Figura 33 – Formato de la MAID del RMCP-2

En la figura 34 se presenta el algoritmo utilizado por la versión actual de RMCP-2 para generar una MAID única.

```

Si la dirección IP en la MAID recibida es una dirección NAT
  Busque su NAT_address_list (lista de direcciones NAT);
  si la dirección ya existe
    serial_number++;(incremente el número de serie)
  en caso contrario
    añada la lista a la NAT_address_list
    serial_number++;
  MAID = IP_address + port_number + serial_number;(dirección IP + número de puerto + número de serie)
return MAID; (devuelva la MAID)

```

Figura 34 – Un algoritmo sencillo para generar una MAID única

7.2 Formato de los datos de control

En la figura 35 se muestra el formato de los datos de control del protocolo RMCP-2.

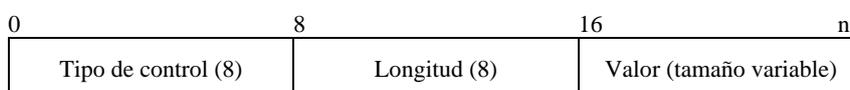


Figura 35 – Formato de control del RMCP-2

ISO/CEI 16512-2:2008 (S)

- a) *Tipo de control*: Representa el tipo de datos de control.
- b) *Longitud*: Representa la longitud, en bytes, del valor de los datos de control incluyendo los campos tipo y longitud, pero excluyendo el campo de datos de subcontrol.
- c) *Valor*: Contiene el valor de los datos de control.

Cuando los datos de control del RMCP-2 deseen especificar detalladamente el control, pueden emplear los datos de subopción. El formato de los datos de subopción es el mismo que el de los datos de control del RMCP-2, tal y como se muestra en la figura 36.

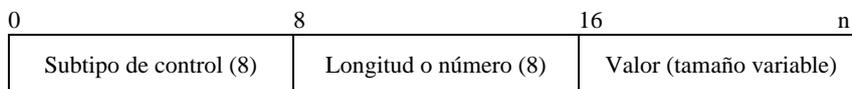


Figura 36 –Formato de subcontrol del RMCP-2

- a) *Subtipo de control*: Describe el tipo de dato de subcontrol.
- b) *Longitud o número*: Representa la longitud en bytes o el número de valores de datos de subcontrol. Depende del valor de los datos de subcontrol.
- c) *Valor*: Representa el valor del dato de subcontrol.

Los datos de control pueden representarse utilizando únicamente un solo dato de control, como se indica en la figura 37.

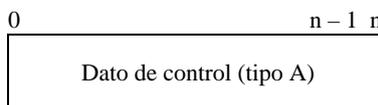


Figura 37 – Utilización de un solo dato de control

Los datos de subcontrol deben ir precedidos por los datos de control apropiados. En la figura 38 se muestra cómo un dato de control apropiado debe preceder al dato de subcontrol que se ha de utilizar.

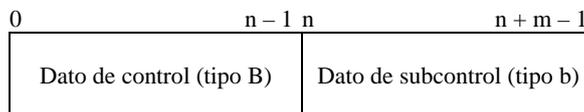


Figura 38 – Utilización de datos de control con datos de subcontrol

En un mismo campo de datos de control del RMCP-2 puede haber varios datos de control al mismo tiempo. Cuando un paquete del RMCP-2 desee incluir varios datos de control, deberá alinear los diversos datos de control de la forma indicada en la figura 39.

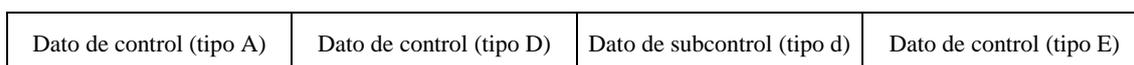


Figura 39 – Utilización de varios datos de control

7.3 Mensajes

En esta subcláusula se definen los mensajes utilizados por el protocolo RMCP-2. El protocolo RMCP-2 define siete conjuntos de mensajes que obedecen la forma *petición* y *respuesta* (a veces denominada forma *petición* y *confirmación*) y un mensaje de latido. En el cuadro 2 se enumeran los tipos de mensaje y sus correspondientes valores.

7.3.1 SUBSREQ

El mensaje SUBREQ se emplea para suscribirse a una sesión RMCP-2. Al emitir un mensaje SUBSREQ, los MA pueden obtener la información de iniciación del SM, si el mensaje es aceptable. En la figura 40 se indica el formato del mensaje.

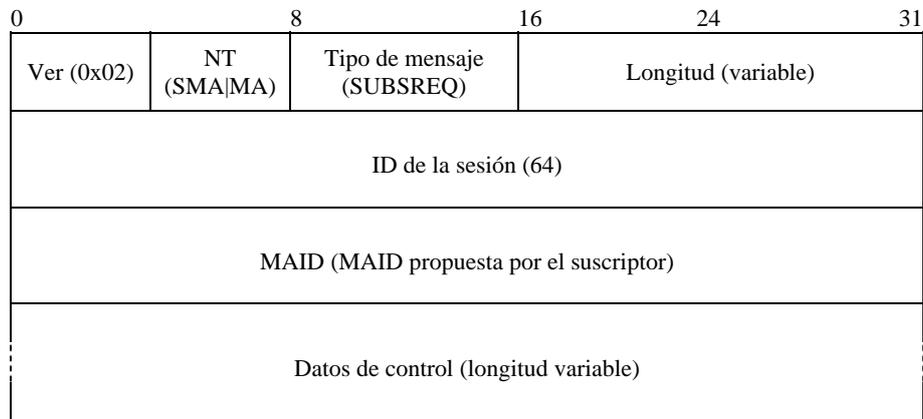


Figura 40 – Mensaje SUBSREQ

La descripción de cada campo es la siguiente:

- a) *Ver*: Representa la versión del RMCP (0x02).
- b) *NT*: El tipo de nodo de quien emitió el mensaje (SMA|MA).
- c) *Tipo de mensaje*: Representa el tipo de mensaje. El valor se fija a SUBSREQ en este mensaje.
- d) *Longitud*: Indica la longitud total en bytes del mensaje SUBSREQ.
- e) *ID de la sesión*: Valor de 64 bits con la ID de la sesión del RMCP.
- f) *MAID propuesta*: Valor único para identificar la entidad.
- g) *Datos de control*: Contiene el conjunto de información necesario para la suscripción a la sesión RMCP-2. Puede incluir la siguiente información:

- **SYSINFO**

Este mensaje de control indica al sistema la potencia del MA, como el ancho de banda de entrada/salida y el número de CMA que puede controlar.

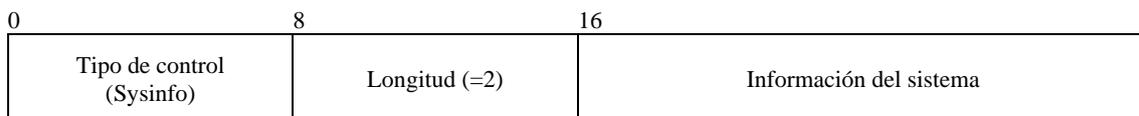


Figura 41 – Control SYSINFO

Los datos de subcontrol que se presentan en la figura 42 y en la figura 43 son datos de subcontrol que pueden ir a continuación de los datos de control de SYSINFO, indicados en la figura 41.

En la figura 42 se muestran datos de subcontrol seguidos por los datos de control de SYSINFO. La descripción de cada campo es la siguiente:

- a) *Tipo de subcontrol*: Available_CMA (capacidad disponible de CMA) (uno de los subtipos de SYS_INFO).
- b) *Longitud*: Representa la longitud del valor dato de control.
- c) *En reserva*: Se reserva para uso posterior.
- d) *Valor*: Contiene información pertinente del sistema.

0	8	16	24	31
Tipo de control (Sysinfo)	Longitud (=2)	Sysinfo_subtype (Available_CMA)	Longitud (= 6)	
En reserva		N.º de Available_CMA		

Figura 42 – Subcontrol AVAILABLE_CMA

En la figura 43 se muestran datos de subcontrol seguidos por los datos de control de SYSINFO. La descripción de cada campo es la siguiente:

- a) *Tipo de subcontrol*: possible bandwidth (ancho de banda posible) (uno de los subtipos de SYS_INFO).
- b) *Longitud*: Representa la longitud del valor del dato de control.
- c) *Valor*: Representa el ancho de banda de retransmisión del que puede disponer el MA.

0	8	16	24	31
Tipo de control (Sysinfo)	Longitud (= 2)	Sysinfo_subtype (ancho de banda posible)	Longitud (= 6)	
Ancho de banda de retransmission posible (en bit/s)				

Figura 43 – Subcontrol POSSIBLE_BW

Obsérvese que una trama de control de dos bytes precede cada dato de subcontrol.

- **DATAPROFILE**

El control DATAPROFILE entrega el perfil de datos que el MA puede controlar. El control DATAPROFILE tiene como objetivo permitir que el SM mantenga la lista clasificada de vecinos, si el SM tiene en cuenta la QoS.

Si el MA no incluye estos datos de control en el mensaje SUBSREQ, el SM no se preocupa por la gestión de la QoS del MA. La descripción de cada campo es la siguiente:

- a) *Tipo de control*: DATA_PROFILE.
- b) *Longitud*: Representa la longitud del perfil de datos.
- c) *Perfil de datos posible*: Representa el perfil de datos que el MA desea utilizar.

0	8	16	n - 1
Tipo de opción (perfil de datos)	Longitud (= n/8)	Perfil de datos posible	

Figura 44 – Control DATAPROFILE

El tamaño del mensaje es variable ya que el control DATAPROFILE está compuesto por un mensaje de texto de longitud variable. A fin de alinear longitudes de 4 bytes, cada perfil de datos utiliza un relleno de ceros de longitud de 0 ó 1 byte, como se indica en la figura 45. La descripción de cada campo es la siguiente:

- a) *Perfil de datos*: El perfil de datos describe las características del canal de datos y utiliza un método de codificación similar a SDL.
- b) *Relleno de cero o más ceros*: A fin de ajustar la longitud del perfil de datos, se anexa un relleno de cero o más ceros.

0	4n - 4	4n - 1	
Perfil de datos	00	00	00

Figura 45 – Control DATAPROFILE con relleno

- AUTH

La información de autenticación se puede entregar utilizando el control AUTH. A fin de soportar varios tipos de mecanismos de autenticación, se define el formato ampliable del subcontrol AUTH seguido por el control AUTH de dos bytes. La descripción de cada campo es la siguiente:

- Tipo de control:* AUTH.
- Longitud:* El tamaño del control AUTH, el cual debe valer dos.
- Información de la Auth:* Incluye la siguiente información detallada:

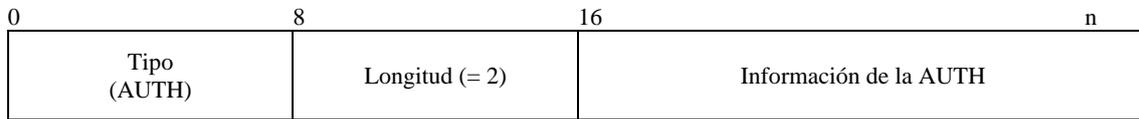


Figura 46 – Control AUTH

En la figura 47 se muestran los datos de subcontrol empleados para entregar la información de autenticación que ha de utilizarse. La descripción de cada campo es la siguiente:

- Tipo de Subcontrol:* Depende del mecanismo de AUTH empleado.
- Longitud:* Define el tamaño de los datos de subcontrol.
- Valor:* Representa los datos de control.

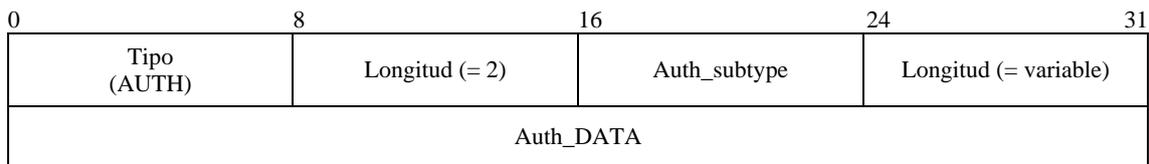


Figura 47 – Subcontrol AUTH

7.3.2 SUBSANS

El SM utiliza el mensaje SUBSANS para presentar los resultados de la petición de suscripción y la información de iniciación de la sesión. En la figura 48 se muestra el formato del mensaje.

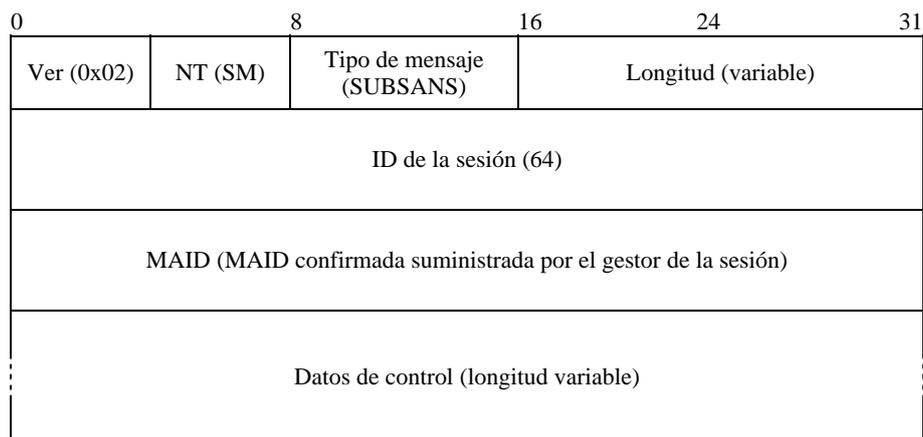


Figura 48 – Mensaje SUBSANS

La descripción de cada campo es la siguiente:

- Ver:* Representa la versión de RMCP (0x02).
- NT:* El tipo de nodo del emisor (SM).
- Tipo de mensaje:* Representa el tipo de mensaje. En este mensaje el valor se fija a SUBSANS.

ISO/CEI 16512-2:2008 (S)

- d) *Longitud*: Indica la longitud total del mensaje SUBSANS (en bytes).
- e) *ID de la sesión*: Valor de 64 bits que contiene la ID de la sesión RMCP.
- f) *MAID confirmada*: El número de identificación del MA. El SM proporciona una ID confirmada que depende de la MAID sugerida por el MA en el mensaje SUBSREQ.
- g) *Datos de control*: Contiene el conjunto de datos necesario para la adhesión a un árbol de multidifusión con retransmisión del RMCP. Puede incluir la siguiente información:

- **RESULT**

Este mensaje de control indica si la petición de suscripción del MA tuvo éxito o no. Si tuvo éxito, aparece el código OK dentro del código de resultado. Si no tuvo éxito, aparece el código de error correspondiente, como agotamiento de recursos o destino inalcanzable. En la figura 49 se muestra el formato del mensaje de control RESULT. Se utilizan los siguientes controles para entregar la información necesaria para adherirse al árbol RMCP-2. No se puede incluir el control siguiente cuando se rechaza una suscripción. La descripción de cada campo es la siguiente:

- a) *Tipo de control*: RESULT.
- b) *Longitud*: Representa la longitud del código de resultado.
- c) *Código de resultado*: Indica el resultado ocasionado por el solicitante. En el cuadro 3 figuran los códigos detallados.

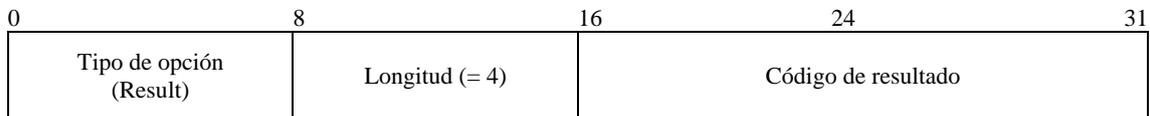


Figura 49 – Control RESULT

- **DATAPROFILE**

El SM utiliza el control DATAPROFILE para confirmarle al suscriptor el perfil de datos. El control DATAPROFILE cobra mayor importancia cuando el SM envía información de datos extrasesión a los suscriptores. En la figura 44 se muestra el formato del control DATAPROFILE y en la figura 84 se presenta el contenido.

- **NEIGHBORLIST**

Cuando una suscripción tiene lugar, el SM devuelve al suscriptor suficientes listas de suscriptores. Mediante el control NEIGHBORLIST los suscriptores obtienen la información de iniciación. En la figura 50 se presenta el formato de NEIGHBORLIST. Obsérvese que sólo entrega MAID. La descripción de cada campo es la siguiente:

- a) *Tipo de control*: NEIGHBOR_LIST.
- b) *Longitud*: Representa la longitud de los datos de control. Su tamaño debería ser dos.
- c) *Información de la lista de vecinos*: Incluye cierta información sobre las MAID. La forma de uso y el formato son los siguientes:

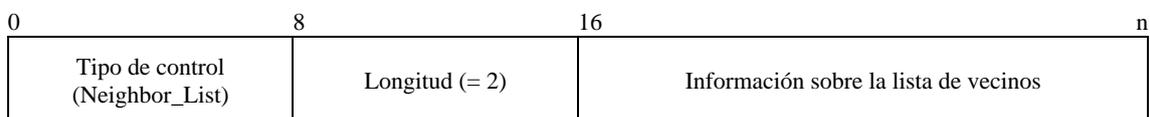


Figura 50 – Control NEIGHBORLIST

En la figura 51 se muestra el subcontrol que sigue al control NeighborList, con los siguientes campos:

- a) *Tipo de subcontrol*: Define el tipo de NL que se va a utilizar. En este ejemplo se utiliza la lista de MAID como NEIGHBOR_LIST.
- b) *Número de NL*: Representa el número de MAID que siguen.
- c) *MAID*: La lista de MAID proporcionada por el SM. El número de MA en la lista se registra en el campo NL.

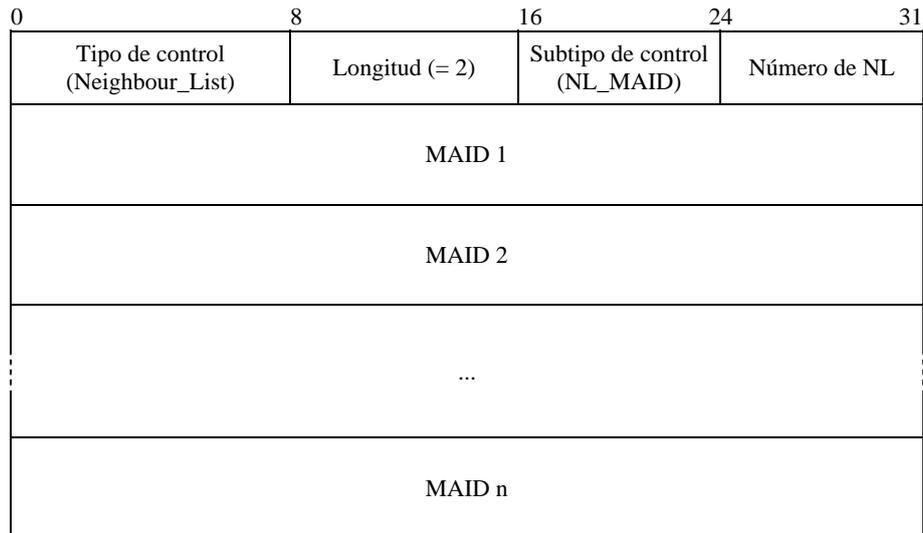


Figura 51 – Subcontrol NL_MAID

- AUTH

El control AUTH se usa para actualizar la información de autenticación de la sesión, de ser necesario. Si no se requiere actualizar la información de autenticación, el control sencillamente copia los datos de autenticación enviados del suscriptor. En las figuras 46 y 47 se muestra el formato del control AUTH.

7.3.3 PPROBREQ

Se utiliza durante el procedimiento de *descubrimiento del mapa* para averiguar la situación vigente de la red y para explorar los vecinos. También se emplea para verificar si la contraparte sigue activa. En la figura 52 se ilustra el formato del mensaje.

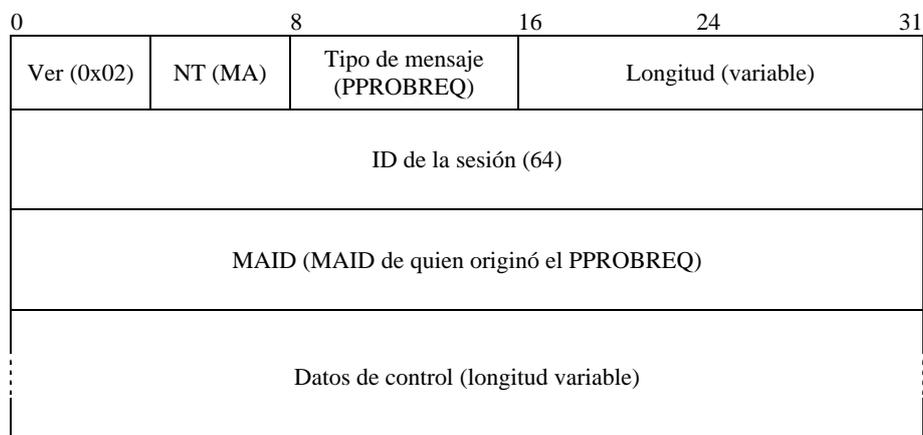


Figura 52 – Mensaje PPROBREQ

La descripción de cada campo es la siguiente:

- Ver*: Representa la versión del RMCP utilizada (0x02).
- NT*: El tipo de nodo del emisor del mensaje (MA).
- Tipo de mensaje*: Representa el tipo de mensaje. El valor se fija a PPROBREQ en este mensaje.
- Longitud*: Indica la longitud total del mensaje PPROBREQ, incluyendo los datos de control (en bytes).
- ID de la sesión*: Un valor de 64 bits que representa la ID de la sesión.
- MAID*: LA MAID del emisor del mensaje PPROBEREQ.
- Datos de control*: Puede incluir la siguiente información, utilizada para indagar sobre el mapa.

ISO/CEI 16512-2:2008 (S)

- **TIMESTAMP**

En la figura 53 se muestra el control **TIMESTAMP**, que se utiliza para medir la distancia entre dos MA. La descripción de cada campo es la siguiente:

- Tipo de control:* **TIMESTAMP**.
- Longitud:* Representa la longitud total de la opción **Timestamp**. El valor es 16 (bytes).
- En reserva:* Se reserva para fines posteriores.
- Time 1:* Marca horaria de cuando el emisor del **PPROBREQ** envía el paquete a su contraparte.
- Time 2:* Marca horaria de cuando el **PPROBREQ** llega a la contraparte.
- Time 3:* Marca horaria de cuando el receptor del **PPROBREQ** envía la opción **timestamp** como respuesta.

0	8	16	24	31
Tipo de control (Timestamp)	Longitud (16)	En reserva		
Marca horaria 1 (cuando el emisor empieza a enviar)				
Marca horaria 2 (cuando el paquete aparece en el receptor)				
Marca horaria 3 (cuando el receptor comienza a contestar)				

Figura 53 – Control **TIMESTAMP**

- **NEIGHBORLIST**

Para saber quiénes participan en el **RMCP-2**, cada MA puede utilizar el control **NEIGHBORLIST** para intercambiar información acerca de su vecino. En las figuras 50 y 51 se muestran el formato y la utilización del control.

- **ROOTPATH**

A fin de evitar bucles y para resolver el problema triangular, el MA que realiza la exploración puede incluir su *trayecto desde la raíz* utilizando el control **ROOTPATH** indicado en la figura 54. Los siguientes son los significados de los campos:

- Tipo de control:* **ROOTPATH**.
- Longitud:* Representa la longitud de la opción **ROOTPATH**. El tamaño es 2.
- Información de rootpath:* Este campo incluye la información del **rootpath**. Su formato y modo de uso son como sigue:

0	8	16	n
Tipo de control (ROOTPATH)	Longitud (2)	Información de rootpath	

Figura 54 – Control **ROOTPATH**

En la figura 55 se muestra el dato de subcontrol de **ROOTPATH**. El siguiente es el significado de los campos:

- Tipo de subcontrol:* Este campo del tipo subcontrol indica el tipo de información que se utilizará para el trayecto desde la raíz. En la actualidad existen siete tipos de información para el trayecto, los cuales se enumeran en el cuadro 4.
- Número de **ROOTPATH**:* Representa el número de trayectos seguidos.
- Uno o varios **ROOTPATH**:* Incluye la información sobre los saltos recopilada utilizando el tipo de subcontrol. El tamaño de cada **ROOTPATH** es fijo y se puede calcular combinando la longitud de cada tipo. Los tamaños por defecto para cada tipo de **ROOTPATH** se presentan en el cuadro 5.

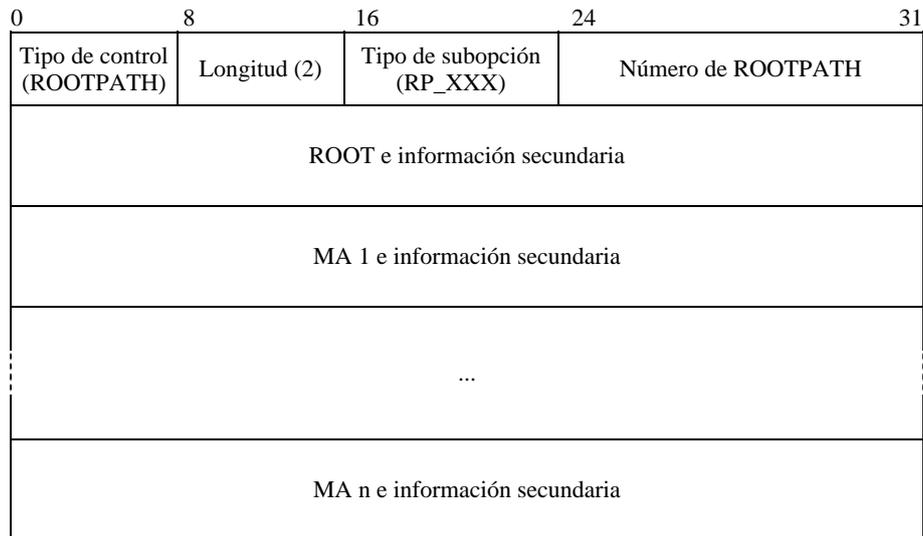


Figura 55 – Subcontrol RP_XXX

- **SYSTEMINFO**

Para evitar que en la parte alta de la jerarquía arborescente se ubiquen sólo nodos hoja o nodos lentos, en SYSTEMINFO se incluye información relativa al sistema, como el ancho de banda de entrada y de salida, el número posible de CMA, etc.

En la figura 41 se presenta el formato del control SYSTEMINFO.

- **DATAPROFILE**

El control DATAPROFILE se utiliza para verificar si el MA examinado está en capacidad de utilizar el método de entrega de datos que desea recibir el MA que realiza el examen. En la figura 44 se muestra el formato del control DATAPROFILE y en la figura 84 se muestran sus contenidos.

7.3.4 PPROBANS

Se emite como respuesta al mensaje PPROBREQ durante el procedimiento de *descubrimiento del mapa* y para confirmar que se encuentra activo. Puede incluir el estado real de la red y alguna información sobre los vecinos. En la figura 56 se ilustra el formato del mensaje PPROBANS.

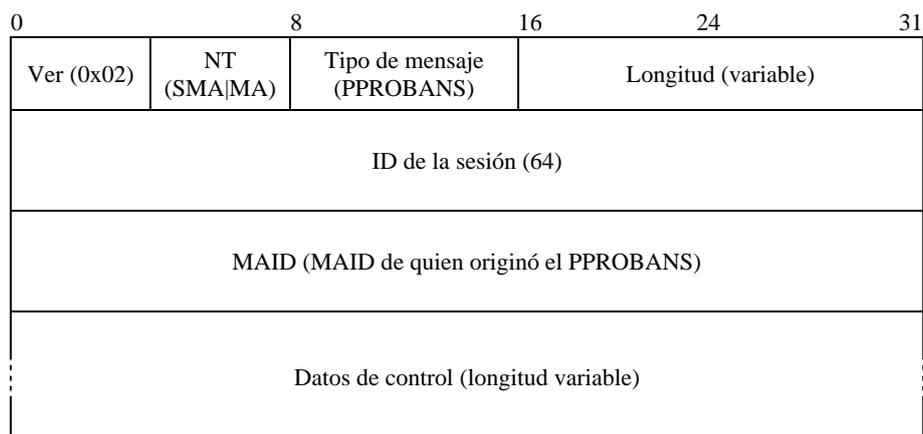


Figura 56 – Mensaje PPROBANS

La descripción de cada campo es la siguiente:

- Ver*: Representa la versión del RMCP utilizada (0x02).
- NT*: El tipo de nodo de quien emitió el mensaje (SMA o MA).

ISO/CEI 16512-2:2008 (S)

- c) *Tipo de mensaje*: Representa el tipo de mensaje. El valor se fija a PPROBANS en este mensaje.
- d) *Longitud*: Indica la longitud total del mensaje PPROBANS, incluidos los datos de control (en bytes).
- e) *ID de la sesión*: Valor de 64 bits con la ID de la sesión RMCP.
- f) *MAID*: La MAID de quien envió el mensaje PPROBANS.
- g) *Datos de control*: Debería incluir información acorde con el mensaje PPROBREQ. El campo datos de control de este mensaje podría incluir la siguiente información:

- **TIMESTAMP**

Este control se emplea para examinar la distancia entre dos MA durante la secuencia de exploración. En la figura 53 se muestra el formato de los datos de control **TIMESTAMP**.

- **NEIGHBORLIST**

El control **NEIGHBORLIST** se diseñó para explorar los participantes en el RMCP-2. Cada MA puede recopilar información sobre sus vecinos utilizando el control **NEIGHBORLIST**, como se indica en la figura 50 y en la figura 51.

- **ROOTPATH**

Los MA utilizan el control **ROOTPATH** para evitar bucles y solucionar el problema triangular. El MA que efectúa la exploración puede incluir su información acerca del trayecto a la raíz, utilizando el control **ROOTPATH**. En la figura 54 y en la figura 55 se muestra el formato de **ROOTPATH**, junto con el formato de subcontrol.

- **SYSTEMINFO**

Para evitar que en la parte alta de la jerarquía arborescente se ubiquen sólo nodos hoja o nodos lentos, en el mensaje **PPROBANS** se podría incluir información relativa al sistema, como ancho de banda de entrada y de salida, el número posible de CMA, etc., empleando el control **SYSTEMINFO**. En la figura 41 se presenta el formato del control **SYSTEMINFO**.

- **DATAPROFILE**

El control **DATAPROFILE** se utiliza para verificar si el MA examinado está en capacidad de utilizar datos que el MA que realiza el examen desea utilizar durante la entrega de datos. En la figura 44 se muestra el control **DATAPROFILE** y en la figura 84 se muestran sus contenidos.

7.3.5 HSOLICIT

HSOLICIT se utiliza para procesar la autoorganización de una red local. El objetivo es hallar el HMA dentro de la red local. En la figura 57 se ilustra el formato de mensaje de **HSOLICIT**.

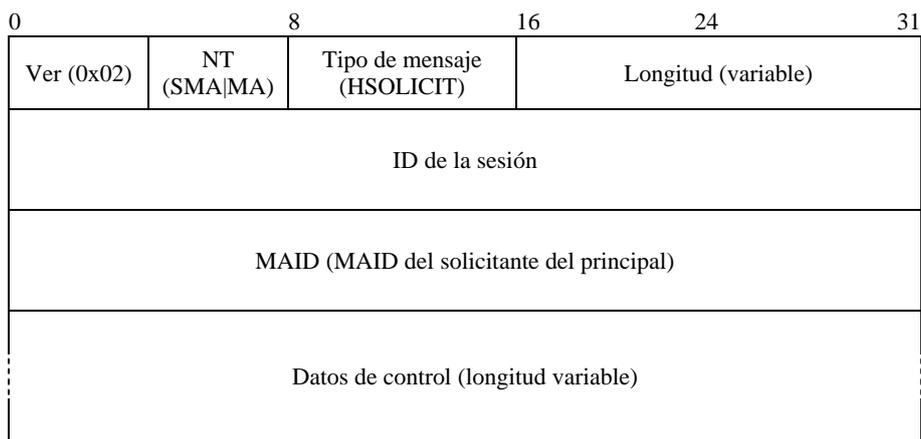


Figura 57 – Mensaje HSOLICIT

La descripción de cada campo es la siguiente:

- a) *Ver*: Representa la versión del RMCP utilizada (0x02).
- b) *NT*: El tipo de nodo de quien emitió el mensaje (SMA o MA).
- c) *Tipo de mensaje*: Representa el tipo de mensaje. El valor se fija a HSOLICIT en este mensaje.

- d) *Longitud*: Indica la longitud total del mensaje HSOLICIT, incluidos los datos de control (en bytes).
- e) *ID de la sesión*: Valor de 64 bits con la ID de la sesión RMCP.
- f) *MAID*: La MAID de quien envió el mensaje HSOLICIT a la red local.
- g) *Datos de control*: Podría incluir información sobre la lista de vecinos. El campo datos de control de este mensaje podría incluir la siguiente información:

- AUTH

El control AUTH se utiliza para verificar que el solicitante forma parte de la misma sesión RMCP-2. En las figuras 46 y 47 se indican el control y subcontrol de AUTH.

7.3.6 HANNOUNCE

Se utiliza como respuesta de HSOLICIT para anunciar la existencia del HMA en la red local. En la figura 58 se muestra el formato de este mensaje.

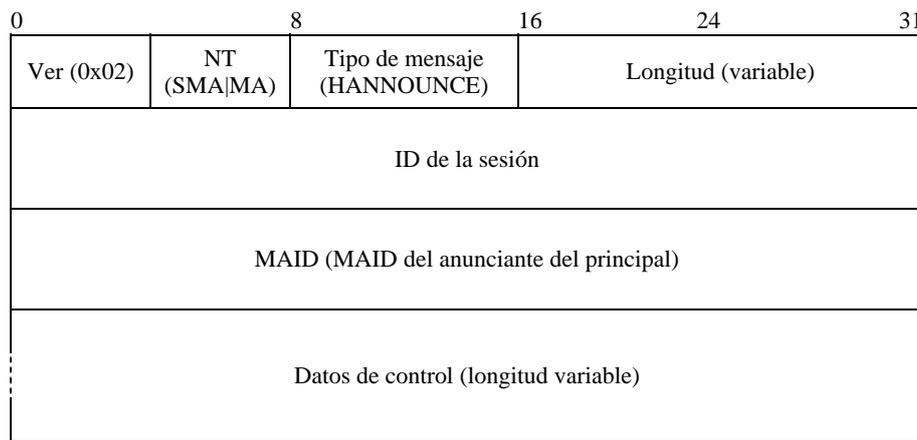


Figura 58 – Mensaje HANNOUNCE

La descripción de cada campo es la siguiente:

- a) *Ver*: Representa la versión del RMCP utilizada (0x02).
- b) *NT*: El tipo de nodo de quien emitió el mensaje (SMA o MA).
- c) *Tipo de mensaje*: Representa el tipo del mensaje. El valor se fija a HANNOUNCE en este mensaje.
- d) *Longitud*: Indica la longitud total del mensaje HANNOUNCE, incluidos los datos de control (en bytes).
- e) *ID de la sesión*: Valor de 64 bits con la ID de la sesión RMCP.
- f) *MAID*: La MAID del HMA de la red local.
- g) *Datos de control*: Podría incluir la siguiente información:

- AUTH

El control AUTH se utiliza para verificar que quien envía el HANNOUNCE forma parte de la misma sesión RMCP-2. En la figura 46 y en la figura 47 se indican el control y subcontrol de AUTH.

- SYSTEMINFO

A fin de indicar la potencia del HMA a los no-HMA de la misma zona de multidifusión, el HMA puede incluir la potencia de sistema del MA, como el ancho de banda de entrada y de salida y el número de CMA que puede controlar. El HMA también puede incluir información adicional como la IP local y el tiempo de vida que requiere el HAM para recuperarse de las colisiones de mensajes HANNOUNCE.

En la figura 59 se muestra un mensaje de subcontrol de la IP local, consecutivo al control SYSTEMINFO.

La descripción de cada campo es la siguiente:

- a) *Tipo de subcontrol*: Indica que los datos de subcontrol contendrán la dirección IP local.
- b) *Longitud*: Define el tamaño de los datos de subcontrol. Su valor es seis.
- c) *IP Local*: Representa la dirección IP del equipo local.

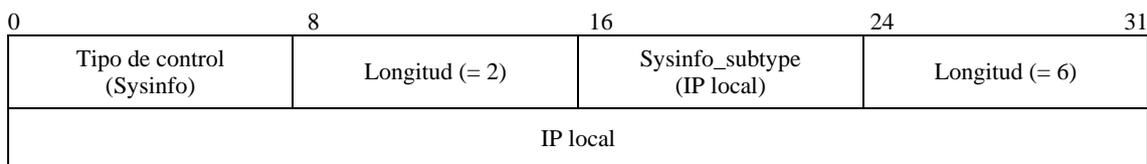


Figura 59 – Local IP sub-control

En la figura 60 se muestran los datos de control del tiempo de vida del HMA.

- a) *Tipo de subcontrol*: Indica el tipo de datos de subcontrol.
- b) *Longitud*: Define el tamaño de los datos de subcontrol y el valor que tendrá.
- c) *Uptime (tiempo activo)*: Representa, en segundos, el tiempo transcurrido desde que el nodo se adhirió a la sesión RMCP-2.

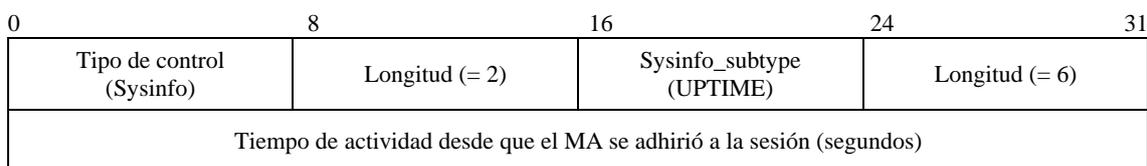


Figura 60 – Subcontrol UPTIME

- LISTA DE VECINOS (NEIGHBOR LIST)

El HMA puede incluir la lista de vecinos, de la forma indicada en las figuras 50 y 51 para compartir la información recopilada durante la exploración con los no-HMA de la misma zona habilitada para la multidifusión.

7.3.7 HLEAVE

HLEAVE se utiliza para anunciar que el HMA abandona la sesión RMCP-2 e ingresa a la red local. En la figura 61 se ilustra el formato de este mensaje.

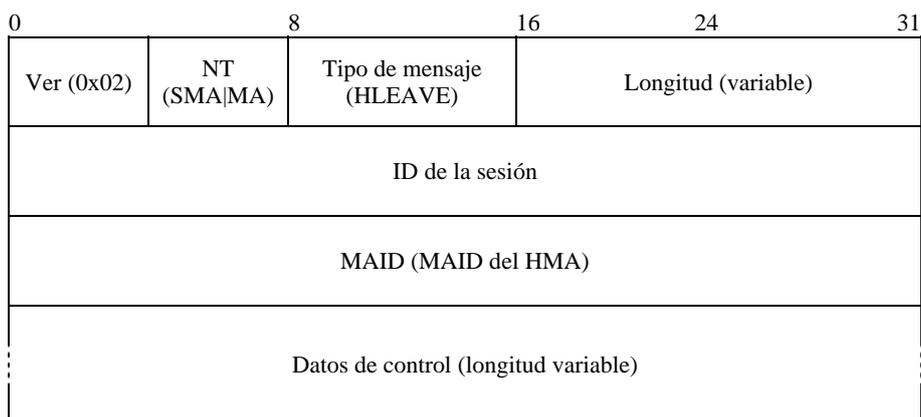


Figura 61 – Mensaje HLEAVE

La descripción de cada campo es la siguiente:

- a) *Ver*: Representa la versión del RMCP utilizada (0x02).
- b) *NT*: El tipo de nodo de quien emitió el mensaje (SMA o MA).
- c) *Tipo de mensaje*: Representa el tipo del mensaje. El valor se fija a HLEAVE en este mensaje.
- d) *Longitud*: Indica la longitud total del mensaje HLEAVE, incluidos los datos de control (en bytes).

- e) *ID de la sesión*: Valor de 64 bits con la ID de la sesión RMCP.
- f) *MAID*: La MAID del HMA de la red local.
- g) *Datos de control*: Podría incluir la siguiente información:

- CANDIDATEHMA

Cuando el HMA abandona la sesión, todos los demás MA en la zona habilitada para multidifusión pueden competir para convertirse en HMA. Esto puede hacer que la zona habilitada para multidifusión se inunde de mensajes HANNOUNCE. Para evitar colisiones en la elección del HMA, el HMA puede utilizar el control CANDIDATEHMA mostrado en la figura 62.

La descripción de cada campo es la siguiente:

- a) *Tipo de control*: Define el tipo a utilizarse.
- b) *Longitud*: Representa el tamaño de los datos de control. Su valor será dos.
- c) *Información de los HMA candidatos*: Lista de HMA candidatos. A continuación se presenta el formato detallado de la información:

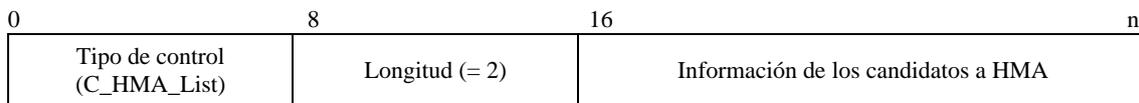


Figura 62 – Control CANDIDATE HMA LIST

En la figura 63 se muestra el subcontrol del control CANDIDATE HMA LIST. La descripción de cada campo es la siguiente:

- a) *Tipo de subcontrol*: Define el tipo de lista HMA que se empleará. En este ejemplo, se utiliza la lista de MAID como lista de candidatos a HMA.
- b) *Número de NL*: Representa el número de listas.
- c) *MAID*: Es una lista de MAID de candidatos a HMA, suministrada por el HMA que abandona.

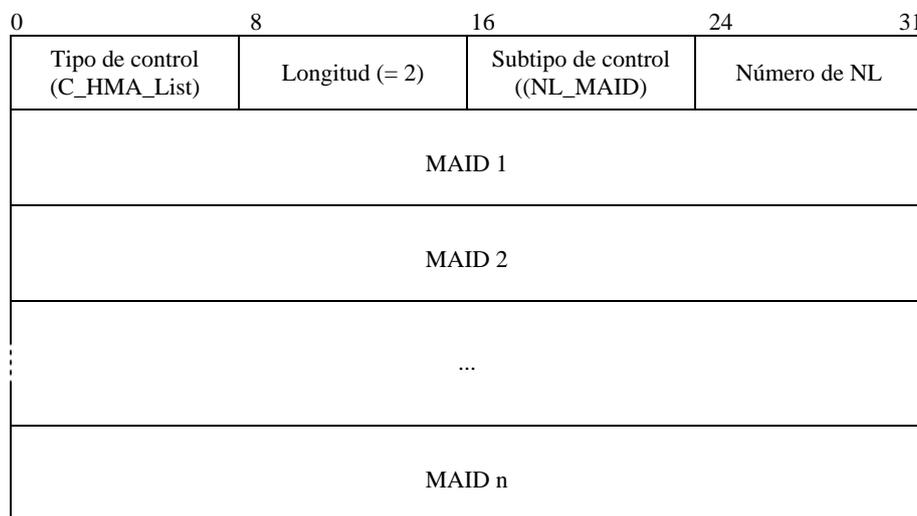


Figura 63 – Subcontrol CANDIDATE HMA LIST

- NEIGHBORLIST

Para compartir la información recopilada durante la exploración con los no HMA de la misma zona habilitada para la multidifusión, el HMA puede incluir la lista de vecinos, de la forma indicada en las figuras 50 y 51.

ISO/CEI 16512-2:2008 (S)

- ROOTPATH

El HMA que abandona puede incluir su trayectoria desde la raíz, utilizando el control ROOTPATH, de forma que el HMA recién elegido pueda seguir la misma trayectoria desde la raíz. En las figuras 54 y 55 se presenta el tipo de datos de control.

- AUTH

Se utiliza el control AUTH para verificar que quien hace la solicitud pertenezca a la misma sesión RMCP-2. En las figuras 46 y 47 se muestran el control AUTH y su subcontrol.

- REASON (Motivo)

El motivo por el que un HMA abandona difiere según la situación. Por ejemplo, los HMA pueden abandonar la sesión por voluntad propia. Pero podría suceder que el HMA abandone la sesión porque ésta finalizó. En ese caso, todo nodo no-HMA de la zona habilitada para la multidifusión debería abandonar la sesión cuanto antes.

Para informar el motivo por el que abandona la sesión, el mensaje HLEAVE debe incluir el control REASON, como se indica en la figura 64. La descripción de cada campo es la siguiente:

- Tipo de control:* Este campo representa el tipo de control.
- Longitud:* Representa la longitud de los datos de control. Su valor es 4.
- Código de motivo:* Este campo de dos bytes contiene un valor entero que indica el motivo concreto de abandono. En el cuadro 7 se enumeran los códigos con sus significados.

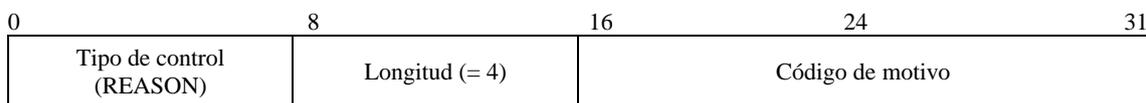


Figura 64 – Control REASON

7.3.8 RELREQ

EL CMA utiliza este mensaje para solicitarle al PMA la retransmisión de datos. Normalmente incluye un perfil de datos que puede negociarse mediante el intercambio de mensajes RELREQ y RELANS. En la figura 65 se representa el formato de este mensaje.

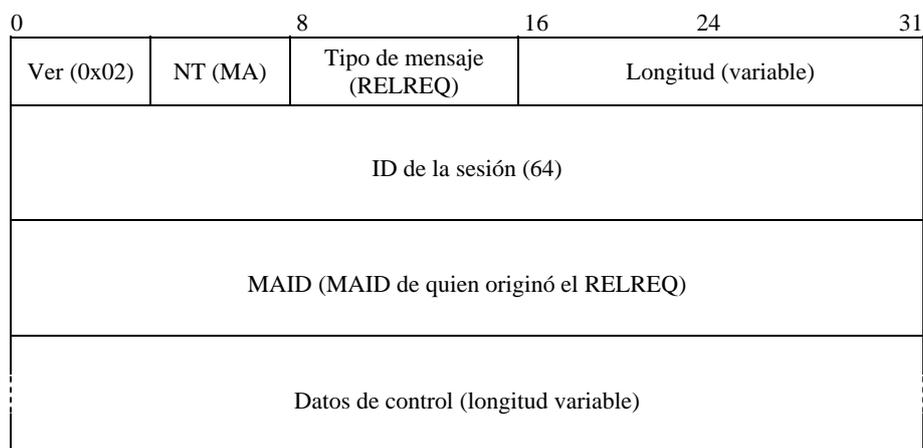


Figura 65 – Mensaje RELREQ

La descripción de cada campo es la siguiente:

- Ver:* Representa la versión del RMCP utilizada (0x02).
- NT:* El tipo de nodo de quien emitió el mensaje (MA).
- Tipo de mensaje:* Representa el tipo del mensaje. El valor se fija a RELREQ en este mensaje.
- Longitud:* Indica la longitud total del mensaje RELREQ, incluidos los datos de control (en bytes).

- e) *ID de la sesión*: Valor de 64 bits con la ID de la sesión RMCP.
- f) *MAID*: La MAID del nodo que envía el mensaje RELREQ.
- g) *Datos de control*: Podría incluir una o varias solicitudes relativas a la petición de retransmisión. Los siguientes son los controles que podrían utilizarse con este mensaje:

- **COMMAND (INSTRUCCIÓN)**

Cuando el CMA necesita que el DMA le suministre información, se la solicita utilizando el control COMMAND dentro del mensaje RELREQ.

Por ejemplo, cada vez que el MA vuelva a conectarse a su PMA durante el procedimiento de adhesión o de cambio de progenitor, el MA necesita conocer el trayecto desde la raíz del nuevo PMA para poder llevar a cabo el diagnóstico de red y la detección de bucles. En ese caso, el MA emplea el control COMMAND para averiguar el ROOTPATH del PMA al que se acaba de adherir.

En la figura 66 muestra el formato del control COMMAND. A continuación se presentan la descripción e información de cada campo:

- a) *Tipo de control*: Este campo representa el tipo de control.
- b) *Longitud*: Representa la longitud de los datos de control. Su valor es 4.
- c) *Código de instrucción*: Este campo de dos bytes contiene un valor entero que indica el motivo concreto de abandono. En 8.3, más adelante, se presentan los códigos junto con su significado.

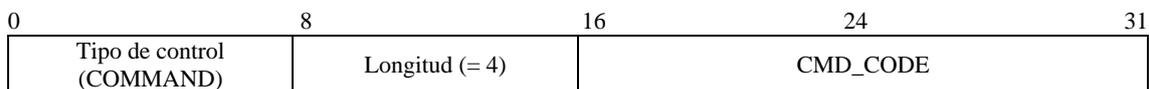


Figura 66 – Control COMMAND

- **DATAPROFILE**

Cuando el CMA se vuelve a conectar al PMA, los dos MA deben acordar un método de entrega de datos. Para que esto sea posible, cada CMA utiliza el control DATAPROFILE para negociar con su PMA. En las figuras 44 y 45 se presenta el formato del control DATAPROFILE y en la figura 84 sus contenidos.

- **TIMESTAMP**

Cada CMA debería medir el retardo salto a salto desde el PMA. Con este fin, el CMA incluye en el mensaje RELREQ el control TIMESTAMP, como se muestra en la figura 53.

7.3.9 RELANS

El PMA emite hacia el CMA el mensaje RELANS, como respuesta al mensaje RELREQ. El propósito de este mensaje es notificar si se permite la petición de retransmisión. Podría también contener información adicional necesaria para negociar el canal de datos con el PMA. En la figura 67 se presenta el formato de mensaje de RELANS.

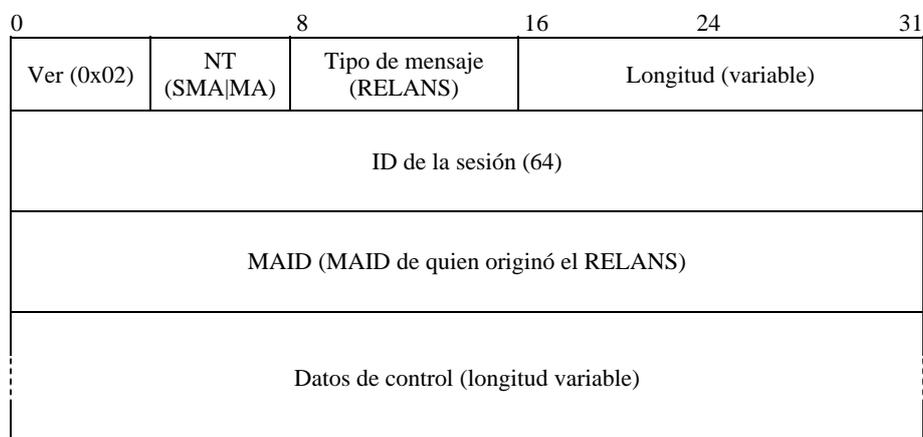


Figura 67 – Mensaje RELANS

ISO/CEI 16512-2:2008 (S)

La descripción de cada campo es la siguiente:

- a) *Ver*: Representa la versión del RMCP utilizada (0x02).
- b) *NT*: El tipo del nodo que emite el mensaje. Como tanto el SMA como los MA pueden emitir este mensaje, el tipo de nodo puede ser MA o SMA.
- c) *Tipo de mensaje*: Representa el tipo del mensaje. El valor se fija a RELANS en este mensaje.
- d) *Longitud*: Indica la longitud total del mensaje RELANS, incluidos los datos de control (en bytes).
- e) *ID de la sesión*: Valor de 64 bits con la ID de la sesión RMCP.
- f) *MAID*: La MAID del nodo que envía el mensaje RELANS.
- g) *Datos de control*: Podría incluir uno o varios de los siguientes controles:

- **RESULT**

El PMA utiliza el control RESULT dentro de cada mensaje RELANS para indicar si el resultado del RELREQ del CMA fue satisfactorio. Si la petición de retransmisión es satisfactoria, presenta OK como código del control RESULT. En caso contrario, presenta el código de error apropiado, como negación de retransmisión por cuestiones de las políticas o por agotamiento de recursos. En la figura 49 se presenta el formato del control RESULT.

- **DATAPROFILE**

Cuando el CMA se vuelve a conectar al PMA, envía un mensaje RELREQ con el control DATAPROFILE a fin de negociar el método de entrega de datos. En las figuras 44 y 45 se presenta el formato del control DATAPROFILE, y en la figura 84, sus contenidos.

- **TIMESTAMP**

En la figura 53 se presenta el control TIMESTAMP. El control TIMESTAMP se emplea para determinar la distancia entre dos MA.

- **ROOTPATH**

Cuando el CMA utiliza el control COMMAND para solicitar la trayectoria a la raíz, su PMA le responde con la información de ROOTPATH. En las figuras 54 y 55 se presenta el control ROOTPATH.

7.3.10 STREQ

Se utiliza STREQ para supervisar el estado de los MA de la sesión. En la figura 68 se muestra el formato de este mensaje.

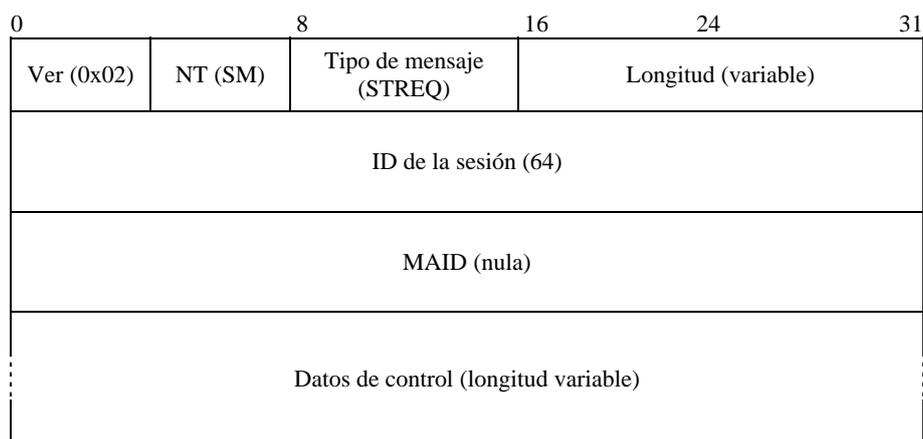


Figura 68 – Mensaje STREQ

La descripción de cada campo es la siguiente:

- a) *Ver*: Representa la versión del RMCP utilizada (0x02).
- b) *NT*: El tipo del nodo que emite el mensaje. Como sólo el SM puede emitir este mensaje, el tipo de nodo de este mensaje sólo puede ser SM.
- c) *Tipo de mensaje*: Representa el tipo del mensaje. El valor se fija a STREQ en este mensaje.

- d) *Longitud*: Indica la longitud total del mensaje RELREQ, incluidos los datos de control (en bytes).
- e) *ID de la sesión*: Valor de 64 bits con la ID de la sesión RMCP.
- f) *MAID*: Como el SM no posee una MAID, este campo se debería fijar a cero.
- g) *Datos de control*: Podría incluir una o varias peticiones sobre el informe de estado. Los siguientes controles son factibles:

- **COMMAND**

Para indicar el informe de estado que requiere, el mensaje STREQ debería incluir el control COMMAND que se muestra en la figura 66. El SM utiliza el control COMMAND dentro del mensaje STREQ para conocer el estado del SM. En el cuadro 6 se resumen muchas de las instrucciones empleadas para la supervisión del estado y se indican los informes esperados. En la figura 66 se ilustra el formato del control COMMAND.

- **TREEEXPLOR**

Podría no ser conveniente inspeccionar el estado de la totalidad del árbol, pues se puede desbordar el número de informes. Es por lo tanto muy importante limitar el ámbito de la inspección. En la figura 69 se presenta el control TREEEXPLOR, utilizado para especificar el ámbito. Los siguientes son los campos del control TREEEXPLOR:

- a) *Tipo de control*: Este campo representa el tipo de control, es decir, TreeExplor.
- b) *Longitud*: Representa la longitud de la opción TreeExplor. Su valor debería ser 4.
- c) *En reserva*: Este campo se reserva para uso futuro.
- d) *TREE_DEPTH (profundidad del árbol)*: Un valor entero de 8 bits, utilizado para especificar el ámbito.

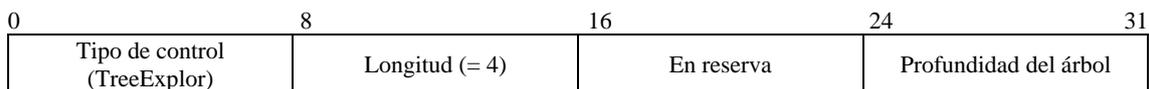


Figura 69 – Control TREEEXPLOR

7.3.11 STANS

Este mensaje se utiliza para supervisar el estado de los MA que forman parte de la sesión. En la figura 70 se muestra el formato del mensaje STANS.

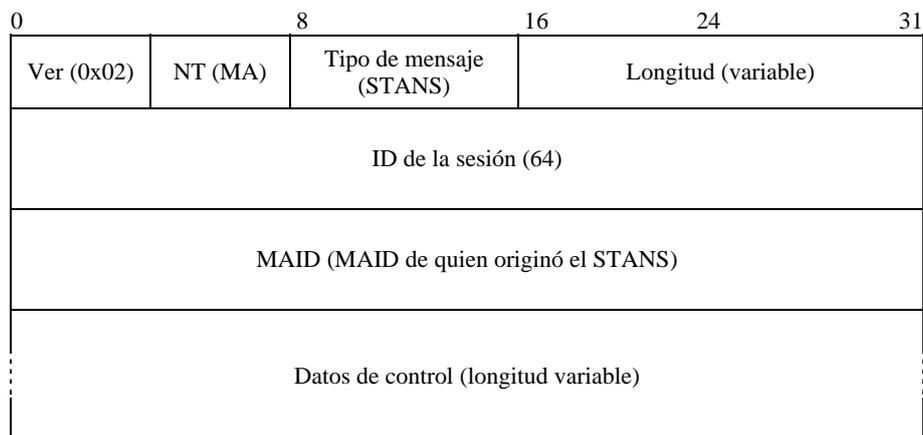


Figura 70 – Mensaje STANS

La descripción de cada campo es la siguiente:

- a) *Ver*: Representa la versión del RMCP utilizada (0x02).
- b) *NT*: *El tipo del nodo que emite el mensaje*. Como sólo los MA pueden emitir este mensaje, el tipo de nodo de este mensaje sólo puede ser MA.
- c) *Tipo de mensaje*: Representa el tipo del mensaje. El valor se fija a STANS en este mensaje.
- d) *Longitud*: Indica la longitud total del mensaje STANS, incluidos los datos de control (en bytes).

- e) *ID de la sesión*: Valor de 64 bits con la ID de la sesión RMCP.
- f) *MAID*: MAID de quien emitió el mensaje STANS.
- g) *Datos de control*: Debería incluir una o varias respuestas a la petición de informe de estado. El campo de datos de control del mensaje STANS puede incluir la siguiente información:

- REPORT (INFORME)

El MA debería responder con el informe apropiado, de conformidad con la petición del SM. El formato de mensaje de los informes tiene la forma {tipo de control, subtipo de control}.

Cada MA envía al SM el informe pertinente, de conformidad con la petición del SM. En el cuadro 6 se enumeran las peticiones de SM y en las figuras 71 a 76 se presentan algunos informes.

En la figura 71 se muestra el informe sobre la capacidad de poseer CMA. La descripción de cada campo es la siguiente:

- a) *Tipo de subcontrol*: Define el tipo de HMA que se utilizará. En este ejemplo, se utiliza la lista de MAID como lista de HMA candidatos.
- b) *Longitud*: Representa el número de listas.
- c) *Número de CMA asignados*: Indica la capacidad asignada para CMA.
- d) *Número de CMA reservados*: Indica la capacidad reservada para CMA. El número de CMA disponibles es, entonces, la diferencia entre el número de CMA asignados y el número de CMA reservados.

0	8	16	24	31
Tipo de opción (SYSINFO)	Longitud (= 2)	Sysinfo_subtype (SI_ROOM_CMA)	Longitud (= 6)	
N.º de CMA asignados		N.º de CMA reservados		

Figura 71 – Control SYSINFO_ROOM_CMA

En la figura 72 se presenta el informe sobre el valor de QoS, que puede ser proporcionado por el sistema. La descripción de cada campo es la siguiente:

- a) *Tipo de subcontrol*: Define el tipo de HMA que se utilizará.
- b) *Longitud*: Representa el tamaño del subcontrol.
- c) *Ancho de banda de entrada de la NIC*: Representa el máximo ancho de banda de entrada de la tarjeta de interfaz de red (NIC, *network interface card*) (en Mbps).
- d) *Ancho de banda de salida de la NIC*: Representa el máximo ancho de banda de salida de la tarjeta de interfaz de red (en Mbps).

0	8	16	24	31
Tipo de opción (SYSINFO)	Longitud (= 2)	Sysinfo_subtype (SI_PROV_QOS)	Longitud (= 6)	
Ancho de banda de entrada de la NIC (en Mbit/s)		Ancho de banda de salida de la NIC (en Mbit/s)		

Figura 72 – Control SYSINFO_PROVIDABLE_QOS

En la figura 73 se presenta el informe sobre el tiempo de actividad transcurrido desde que el MA se adhirió a la sesión. La descripción de cada campo es la siguiente:

- a) *Tipo de subcontrol*: Define el tipo de subcontrol que se utilizará.
- b) *Longitud*: Representa el tamaño del subcontrol.
- c) *Tiempo de actividad desde que el MA se adhirió a la sesión*: Indica, en segundos, el tiempo transcurrido desde que el MA se adhirió a la sesión.

0	8	16	24	31
Tipo de opción (SYSINFO)	Longitud (= 2)	Sysinfo_subtype (SI_PERSIST_TIME)	Longitud (= 6)	
Tiempo transcurrido desde que el MA se adhirió a la sesión (en segundos)				

Figura 73 – Control SYSINFO_PERSIST_TIME

En la figura 74 se presenta el informe sobre la QoS percibida por cada MA. La descripción de cada campo es la siguiente:

- a) *Tipo de subcontrol*: Define el tipo de subcontrol que se utilizará.
- b) *Longitud*: Representa el tamaño del subcontrol. El tamaño debería ser 22.
- c) *Número de PMA*: El número de PMA conectados directamente.
- d) *Número de CMA*: El número de CMA conectados directamente.
- e) *Bytes totales de entrada*: El número total de bytes de los datos entrantes.
- f) *Número de paquetes entrantes*: El número total de paquetes entrantes.
- g) *Bytes totales de salida*: El número total de bytes de los datos salientes.
- h) *Número de paquetes salientes*: El número total de paquetes salientes.

0	8	16	24	31
Tipo de opción (SYSINFO)	Longitud (= 2)	Sysinfo_subtype (ST_PERCV_QOS)	Longitud (= 22)	
N.º de PMA		N.º de CMA		
Bytes totales de entrada (bytes)				
Número de paquetes entrantes				
Bytes totales de salida (bytes)				
Número de paquetes salientes				

Figura 74 – Control STATE_PERCEIVED_QOS

En la figura 75 se presenta el informe sobre el estado de TREE (árbol). La descripción de cada campo es la siguiente:

- a) *Tipo de subcontrol*: Define el tipo de subcontrol que se utilizará.
- b) *Número de MAID*: La lista de MAID de los HMA candidatos y que es proporcionada por el HMA que abandona.
- c) *MAID del PMA*: La MAID del PMA directamente conectado.
- d) *MAID del CMA*: La lista de MAID de los CMA directamente conectados.

0	8	16	24	31
Tipo de opción (TREE)	Longitud (= 2)	Sysinfo_subtype (TREE_CONN)	N.º de MAID (= n + 1)	
MAID del PMA				
MAID del CMA 1				
MAID del CMA n				

Figura 75 – Control TREE_CONNECTION

En la figura 76 se presenta el informe sobre los miembros del TREE (árbol). La descripción de cada campo es la siguiente:

- a) *Tipo de subcontrol*: Define el tipo de subcontrol que se utilizará.
- b) *Número de MAID*: La lista de MAID enumeradas en el control.
- c) *MAID*: La lista de MAID para una rama específica, por ejemplo, el nodo superior de la rama específica se presentará en el campo MAID 1, el nodo inferior se presentará en el campo MAID n.

0	8	16	24	31
Tipo de opción (TREE)	Longitud (= 2)	Sysinfo_subtype (TREE_MEMBER)	N.º de MAID (= n)	
MAID 1				
MAID 2				
MAID n				

Figura 76 – Control TREE_MEMBERSHIP

NOTA – Obsérvese que a cada informe le precede el correspondiente control de 2 bytes.

7.3.12 STCOLREQ

Se utiliza STCOLREQ de una forma similar que STREQ para supervisar la sesión RMCP-2. La diferencia radica, primero, en que STREQ está limitado a un solo MA mientras que STCOLREQ puede abarcar una parte o toda la sesión y, segundo, en que a STREQ lo puede emitir sólo el SM mientras que a STCOLREQ lo puede emitir el PMA.

Cuando un MA recibe el mensaje STCOLREQ del PMA, inicia el *procedimiento de recopilación de estado* y reenvía el mensaje a los CMA en la zona limitada con la opción TreeExplor. En la figura 77 se presenta el formato del mensaje STCOLREQ.

0	8	16	24	31
Ver (0x02)	NT (MA)	Tipo de mensaje (STCOLREQ)	Longitud (variable)	
ID de la sesión (64)				
MAID (MAID de quien originó el STCOLREQ)				
Datos de control (longitud variable)				

Figura 77 – Mensaje STCOLREQ

La descripción de cada campo es la siguiente:

- a) *Ver*: Representa la versión del RMCP utilizada (0x02).
- b) *NT*: El tipo del nodo que emite el mensaje. Como sólo los PMA pueden emitir este mensaje, el tipo de nodo de este mensaje se fija a PMA.
- c) *Tipo de mensaje*: Representa el tipo del mensaje. El valor se fija a STCOLREQ en este mensaje.
- d) *Longitud*: Indica la longitud total del mensaje STCOLREQ, incluidos los datos de control (en bytes).
- e) *ID de la sesión*: Valor de 64 bits con la ID de la sesión RMCP.

- f) *MAID*: MAID de quien emitió el mensaje STCOLREQ. Para los CMA, normalmente es la MAID del PMA.
- g) *Datos de control*: Puede incluir una o varias peticiones de informes de estado. El campo datos de control de este mensaje puede incluir la siguiente información:

- **COMMAND**

Cuando el PMA pregunta el estado a los CMA, incluye el control COMMAND con el mensaje STCOLREQ. En el cuadro 6 se presenta un resumen de varias instrucciones utilizadas para la supervisión del estado.

- **TREEEXPLOR**

Podría no ser conveniente inspeccionar el estado de la totalidad del árbol, pues se puede desbordar el número de informes. Por tanto, es muy importante limitar el ámbito de la inspección.

En la figura 69 se presenta el control TREEEXPLOR, utilizado para limitar el ámbito del árbol.

7.3.13 STCOLANS

En la figura 78 se ilustra el formato del mensaje STCOLANS, utilizado para responder al mensaje STCOLREQ. Informa hacia arriba el estado recopilado hacia abajo. El mensaje STCOLANS sube por la jerarquía del árbol hasta llegar a quien lo emitió.

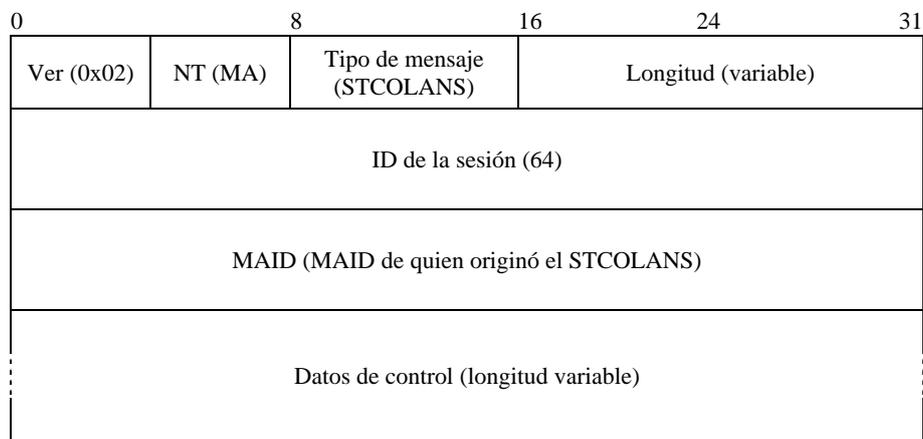


Figura 78 – Mensaje STCOLANS

La descripción de cada campo es la siguiente:

- Ver*: Representa la versión del RMCP utilizada (0x02).
- NT*: El tipo del nodo que emite el mensaje. Como sólo los CMA pueden emitir este mensaje, el tipo de nodo de este mensaje se fija a MA.
- Tipo de mensaje*: Representa el tipo del mensaje. El valor se fija a STCOLANS en este mensaje.
- Longitud*: Indica la longitud total del mensaje STCOLANS, incluidos los datos de control (en bytes).
- ID de la sesión*: Valor de 64 bits con la ID de la sesión RMCP.
- MAID*: MAID de quien emitió el mensaje STCOLANS. Para los PMA, normalmente es la MAID del CMA.
- Datos de control*: Puede incluir una o varias peticiones de informes de estado. El campo datos de control de este mensaje puede incluir la siguiente información:

- **REPORT**

El CMA debe responder con el informe apropiado, de conformidad con la petición del PMA. El formato de mensaje de los informes tiene la forma {tipo de control, subtipo de control}.

Cada CMA envía el informe correspondiente, de conformidad con la petición del PMA, enumerada en el cuadro 6. En las figuras 71 a 76 se presentan algunos informes.

7.3.14 LEAVREQ

Este mensaje se utiliza con tres propósitos diferentes. El primero es para abandonar. Cuando el MA abandona la sesión RMCP-2 o cuando el MA abandona su PMA con el fin de cambiar de progenitor, envía el mensaje LEAVREQ a los MA correspondientes, siguiendo el procedimiento de abandono.

Tanto el SM como el PMA pueden utilizar este mensaje, pero con agente objetivo diferente. El agente objetivo del SM es cualquier MA de la sesión y el del PMA son sólo sus CMA.

El último propósito es para finalizar la sesión. Cuando el SMA abandona la sesión, debería reenviarse este mensaje hasta el MA más lejano en la jerarquía arborescente. En la figura 79 se ilustra el formato del mensaje LEAVREQ.

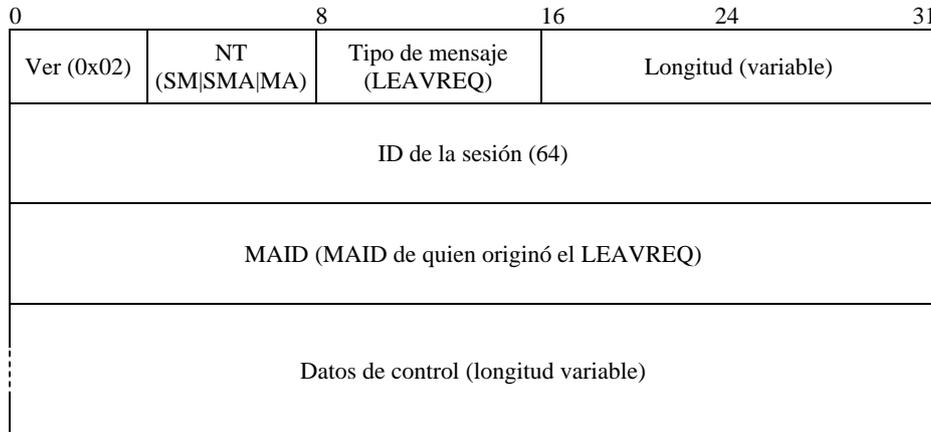


Figura 79 – Mensaje LEAVREQ

La descripción de cada campo es la siguiente:

- a) *Ver*: Representa la versión del RMCP utilizada (0x02).
- b) *NT*: El tipo del nodo que emite el mensaje. Como todas las entidades del RMCP-2 pueden emitir este mensaje, el tipo de nodo puede fijarse a SM, SMA o MA, en este mensaje.
- c) *Tipo de mensaje*: Representa el tipo del mensaje. El valor se fija a LEAVREQ en este mensaje.
- d) *Longitud*: Indica la longitud total del mensaje LEAVREQ, incluidos los datos de control (en bytes).
- e) *ID de la sesión*: Valor de 64 bits con la ID de la sesión RMCP.
- f) *MAID*: MAID de quien emitió el mensaje LEAVREQ. Cuando el SM genera el mensaje, este campo se debe fijar a cero.
- g) *Datos de control*: Este campo puede incluir la siguiente información:

- REASON (MOTIVO)

El mensaje LEAVREQ debe incluir el control REASON para informar el motivo por el que el MA intenta abandonar la sesión. En la figura 64 se muestra el formato del control REASON.

7.3.15 LEAVANS

Para confirmar el mensaje LEAVREQ, el MA que recibe el LEAVREQ responde con un mensaje LEAVANS. En la figura 80 se presenta el formato del mensaje LEAVANS.

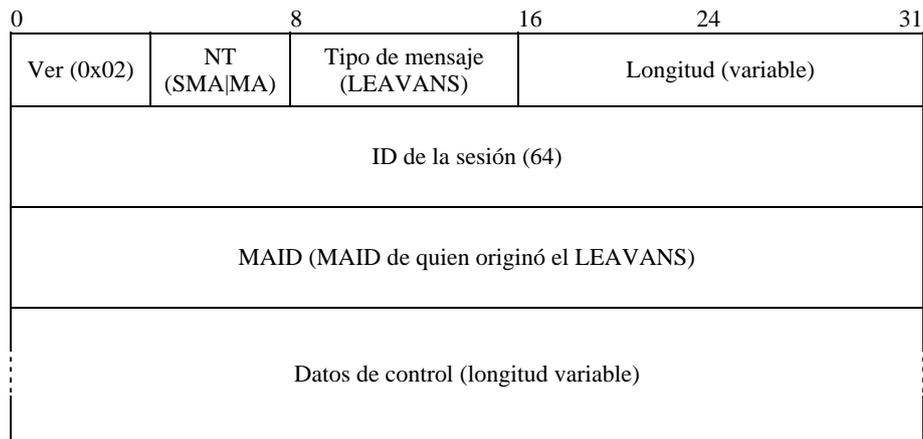


Figura 80 – Mensaje LEAVANS

La descripción de cada campo es la siguiente:

- a) *Ver*: Representa la versión del RMCP utilizada (0x02).
- b) *NT*: El tipo del nodo que emite el mensaje. En este mensaje, el tipo de nodo puede fijarse a SMA o a MA.
- c) *Tipo de mensaje*: Representa el tipo del mensaje. Se fija a LEAVANS.
- d) *Longitud*: Indica la longitud total del mensaje LEAVANS, incluidos los datos de control (en bytes).
- e) *ID de la sesión*: Valor de 64 bits con la ID de la sesión RMCP.
- f) *MAID*: MAID de quien emitió el mensaje LEAVANS.
- g) *Datos de control*: Puede incluir las opciones que convengan. El campo datos de control de este mensaje puede contener la siguiente información:

- **RESULT**

El mensaje LEAVANS se utiliza para indicar que el mensaje LEAVREQ del MA que abandona llega satisfactoriamente. Por tanto, el código de resultado en RESULT debería siempre tener el valor OK.

7.3.16 HB

El SMA emite periódicamente el mensaje HB para transmitir información del reloj durante la sesión RMCP-2. Los MA pueden diagnosticar el estado de la red utilizando el HB. En la figura 81 se presenta el formato del mensaje HB.

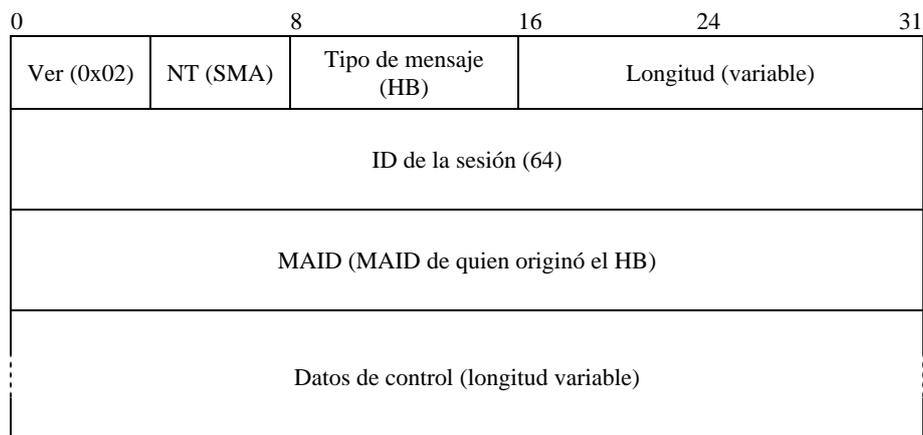


Figura 81 – Mensaje HB

ISO/CEI 16512-2:2008 (S)

La descripción de cada campo es la siguiente:

- a) *Ver*: Representa la versión del RMCP utilizada (0x02).
- b) *NT*: El tipo del nodo que emite el mensaje. En este mensaje, el tipo de nodo puede fijarse a SMA.
- c) *Tipo de mensaje*: Representa el tipo del mensaje. Se fija a HB.
- d) *Longitud*: Indica la longitud total del mensaje HB, incluidos los datos de control (en bytes).
- e) *ID de la sesión*: Valor de 64 bits con la ID de la sesión RMCP.
- f) *MAID*: MAID de quien emitió el mensaje HB. Aunque el PMA reenvía el HB al CMA, el campo no es modificado por los PMA intermedio que participan en la retransmisión.
- g) *Datos de control*: Debería incluir la opción ROOTPATH mostrada en la figura 54. El campo datos de control de este mensaje puede contener la siguiente información:

- **ROOTPATH**

Cada MA actualiza el control ROOTPATH. Desde la raíz, cada MA que retransmite el HB, anexa su MAID e información secundaria, como el retardo salto a salto y el ancho de banda salto a salto teniendo en cuenta la configuración de sesión precedente. En las figuras 54 y 55 se presentan el control ROOTPATH y sus datos secundarios.

- **AUTH**

Durante la sesión, puede actualizarse la información de autenticación utilizando el control AUTH. En las figuras 46 y 47 se presenta el control AUTH y su subcontrol.

- **COMMAND**

Cuando el PMA intenta recuperarse de una subdivisión de la red, sus vástagos podrían dar inicio al procedimiento de recuperación ante fallos debido a que expira el tiempo de espera del HB. Ése es sólo uno de los puntos en que se podría dar inicio en cadena al procedimiento de recuperación ante fallos.

Es, por tanto, necesario generar un seudomensaje HB, para retardar el inicio del procedimiento de recuperación ante fallos de los vástagos, y hallar los medios para notificar el seudomensaje HB a los vástagos.

Se utiliza la instrucción RP_PSEUDO del cuadro 4 para indicar que el ROOTPATH del mensaje HB que transporta esta instrucción (COMMAND) es un seudo ROOTPATH.

7.3.17 TERMREQ

El mensaje TERMREQ se utiliza para finalizar la sesión RMCP-2. El SM lo emite y luego el SMA lo reenvía a lo largo de la jerarquía arborescente hasta los MA más alejados. En la figura 82 se presenta el formato del mensaje TERMREQ.

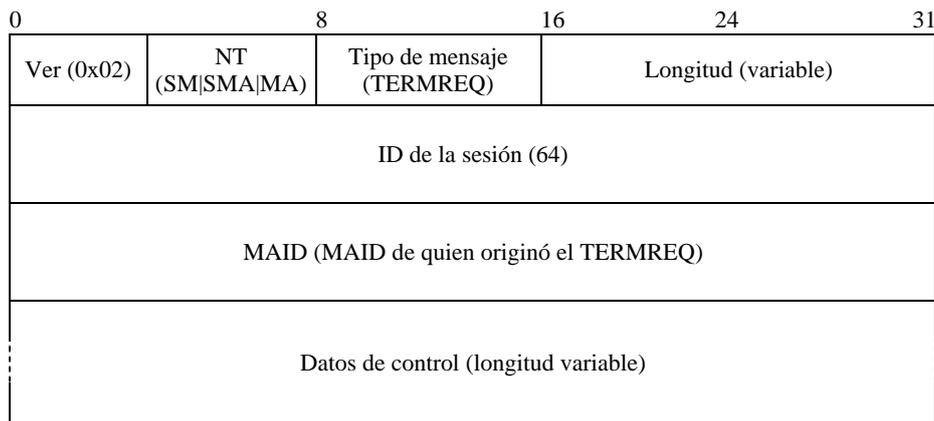


Figura 82 – Mensaje TERMREQ

La descripción de cada campo es la siguiente:

- a) *Ver*: Representa la versión del RMCP utilizada (0x02).
- b) *NT*: El tipo del nodo que emite el mensaje. Como este mensaje es emitido por el SM y debe ser retransmitido a lo largo del árbol RMCP-2 hasta los MA más alejados, el tipo de nodo del mensaje puede fijarse a SM, SMA o MA.
- c) *Tipo de mensaje*: Representa el tipo del mensaje. Se fija a TERMREQ.

- d) *Longitud*: Indica la longitud total del mensaje TERMREQ, incluidos los datos de control (en bytes).
- e) *ID de la sesión*: Valor de 64 bits con la ID de la sesión RMCP.
- f) *MAID*: MAID de quien emitió el mensaje TERMREQ. Cuando es el SM quien emite el mensaje, este campo debe fijarse a cero. Normalmente, la MAID del mensaje TERMREQ que llega a un MA corresponde al de su PMA.
- g) *Datos de control*: Puede contener el siguiente código de motivo para explicar la causa de terminación de la sesión:

- REASON

El mensaje TERMREQ debería incluir el control REASON presentado en la figura 64, para indicar el motivo de terminación de la sesión. La causa de la terminación puede ser que no exista el SMA o que el dueño de la sesión la finalice.

7.3.18 TERMANS

En la figura 83 se ilustra el formato del mensaje TERMANS.

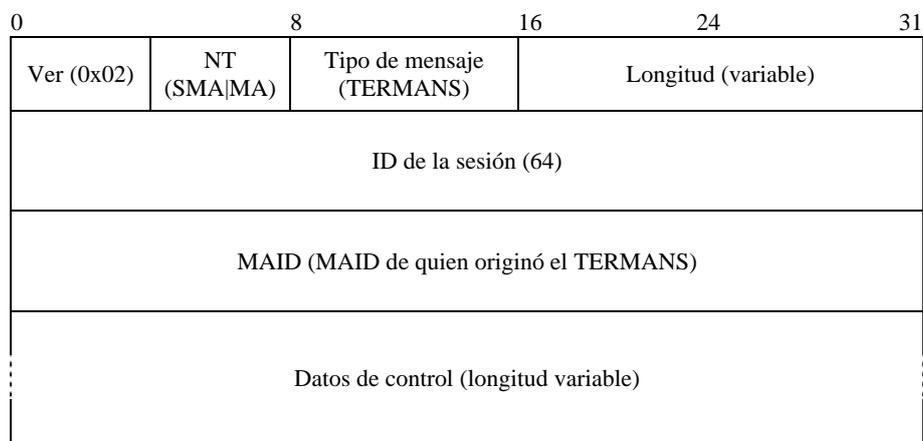


Figura 83 – Mensaje TERMANS

La descripción de cada campo es la siguiente:

- a) *Ver*: Representa la versión del RMCP utilizada (0x02).
- b) *NT*: El tipo del nodo que emite el mensaje. Como este mensaje se emite en sentido ascendente por la jerarquía del árbol RMCP-2 en respuesta al mensaje TERMREQ, el tipo de nodo del mensaje puede fijarse a SMA o a MA.
- c) *Tipo de mensaje*: Representa el tipo del mensaje. Se fija a TERMANS.
- d) *Longitud*: Indica la longitud total del mensaje TERMANS, incluidos los datos de control (en bytes).
- e) *ID de la sesión*: Valor de 64 bits con la ID de la sesión RMCP.
- f) *MAID*: MAID de quien emitió el mensaje TERMANS. Normalmente, la MAID del mensaje TERMANS corresponde al de uno de los CMA.
- g) *Datos de control*: El campo datos de control de este mensaje puede contener la siguiente información:

- RESULT

El mensaje TERMANS se utiliza para indicar que el mensaje TERMREQ llegó satisfactoriamente. Por tanto, el código de resultado de la figura 49 debería ser siempre OK.

8 Parámetros

En esta cláusula se explican los valores de los parámetros utilizados para la gestión del árbol RMCP-2. El protocolo RMCP-2 define el perfil de retransmisión de datos como un mecanismo para especificar la información del canal de datos en términos de tipos de datos. Adicionalmente, se utilizan algunos de los parámetros de control para la gestión eficaz y óptima del árbol de control.

8.1 Perfil de retransmisión de datos

El protocolo RMCP-2 define el perfil de retransmisión de datos como aquel que describe los requisitos para la retransmisión de datos entre un PMA y sus CMA conectados directamente. El perfil de retransmisión de datos se utiliza para negociar el canal de datos en términos del tipo de dato que se entrega durante la sesión. Cuando en una sesión se transmiten simultáneamente varios tipos de datos, la negociación toma en cuenta la descripción de la información de cada uno de los flujos de datos.

En la figura 84 se presenta un perfil de retransmisión en un formato de texto al estilo del SDP.

```
Stream1: Protocol = UDP, Listen address = a.b.c.d:9898, Encapsulation = IP-IP
Stream2: Protocol = UDP, Listen address = a.b.c.d:9899, Encapsulation = UDP
Stream3: Protocol = TCP, Listen address = a.b.c.d:9899, Encapsulation = TCP, CurrentSeq=xxxx,
        BufferedSeq = yyyy, CurrentRcvdSeq = xxxx-1
```

Figura 84 – Ejemplo del perfil de retransmisión de datos

8.2 Parámetros utilizados en el RMCP-2

El protocolo RMCP-2 define algunos parámetros para gestionar el árbol de control. Estos parámetros controlan la información horaria de la sesión RMCP-2, definen el número de mensajes o proporcionan otra información.

8.2.1 Parámetros para inicializar la sesión

Cada MA que desee adherirse a una sesión RMCP-2 debería contactar el SM para obtener la información de iniciación de la sesión. El SM somete una NL como información de iniciación. Debido a la limitación de recursos, la NL no puede contener todos los MA de la sesión. Por tanto, se utiliza el siguiente parámetro para limitar el tamaño de la NL:

- N_StartNL*: Define el número de MA enumerados en la lista de vecinos (*neighbor list*). El SM puede modificarlo antes de que inicie la sesión y también después de que esta haya iniciado. El valor por defecto de *N_StartNL* es 100.

8.2.2 Parámetros para el descubrimiento del mapa

En el RMCP-2, todos los MA llevan a cabo el procedimiento de descubrimiento del mapa, intercambiando periódicamente mensajes PPROBREQ y PPROBANS con los MA vecinos. Los siguientes parámetros se le relacionan con el procedimiento de descubrimiento del mapa:

- PPROB.time*: Define la frecuencia con que se emite el mensaje PPROBREQ. Cada MA envía mensajes PPROBREQ cada *PPROB.time*. El valor por defecto de *PPROB.time* es 45 segundos, pero se puede cambiar a un valor arbitrario.
- N_MAX_PROBE*: Este parámetro limita el número máximo de mensajes PPROBREQ simultáneos que cada MA puede enviar, para evitar que se desborde el número de mensajes PPROBREQ. El valor por defecto de *N_MAX_PROBE* es 1, pero se puede cambiar a un valor arbitrario.

8.2.3 Parámetros para el mantenimiento de la sesión

En la presente subcláusula se trata el mecanismo del latido así como el mantenimiento de la sesión.

El RMCP-2 utiliza el HB para mantener el árbol. El HB sincroniza la totalidad de la sesión a lo largo del trayecto de entrega de datos. En la sesión sincronizada, cada MA puede cambiar de progenitor a fin de mejorar la sesión RMCP-2. El HB también detecta fallos de la red, como bucles y subdivisiones. El RMCP-2 define los parámetros del latido como sigue:

- HB.time*: Frecuencia con que se emite el mensaje HB. El SMA de una sesión emite un mensaje HB cada *HB.time*. El valor por defecto de *HB.time* es 15 segundos.
- MAX_PARTITION_CNT*: Se utiliza para determinar si el árbol está subdividido. Si un MA no recibe el mensaje HB durante *MAX_PARTITION_CNT* * *HB.time*, puede determinar que el árbol está subdividido. El valor por defecto de *MAX_PARTITION_CNT* es 3.

8.2.4 Parámetros para la elección de HMA

El RMCP-2 permite una transmisión de datos IP por multidifusión en una zona habilitada para la multidifusión. Los siguientes parámetros soportan esa prestación:

- H_SOLICIT.time*: Define la frecuencia con que se envía el mensaje HSOLICIT. Los MA de la zona habilitada para la multidifusión envía el mensaje HSOLICIT cada *H_SOLICIT.time*. El valor por defecto de *H_SOLICIT.time* es 2 segundos.
- N_SOLICIT*: Es el número máximo de veces que un MA que no es HMA genera el mensaje HSOLICIT. Después de que emite el mensaje HSOLICIT *N_SOLICIT* veces, el MA intenta convertirse en el nuevo HMA de la zona habilitada para la multidifusión. El valor por defecto de *N_SOLICIT* es 3.
- H_ANNOUNCE.time*: Define la frecuencia con que se envía el mensaje HANNOUNCE. El HMA envía un mensaje HANNOUNCE cada *H_ANNOUNCE.time*. El valor por defecto de *H_ANNOUNCE.time* es 6 segundos.
- N_ANNOUNCE*: Es el número máximo de veces que un HMA genera un mensaje HANNOUNCE. Si no recibe ningún mensaje HSOLICIT, el HMA deja de enviar datos a la zona habilitada para la multidifusión. El valor por defecto de *N_ANNOUNCE* se fija a 3.

8.2.5 Parámetros utilizados para la entrega de datos

El CMA envía periódicamente un mensaje RELREQ a su PMA al conectarse y para continuar retransmitiendo datos,. Los siguientes parámetros se emplean para soportar el procedimiento de retransmisión de datos:

- RELREQ.time*: Es el tiempo entre dos mensajes RELREQ. El *RELREQ.time* es igual para el PMA como para el CMA. El valor inicial de *RELREQ.time* es 6 segundos.
- N_RELREQ*: Se utiliza para determinar si el CMA está activo. Si el PMA no recibe ningún mensaje RELREQ durante *RELREQ.time * N_RELREQ*, supone que el CMA abandonó intempestivamente la sesión. El valor por defecto de *N_RELREQ* es 3.

8.2.6 Parámetros utilizados al abandonar la sesión

El RMCP-2 permite que el MA abandone anticipadamente la sesión. Un MA que esté ubicado en el centro del árbol y deba abandonar la sesión, debe esperar cierto tiempo a que se reconfigure el árbol, antes de abandonar. Los siguientes parámetros se emplean para soportar el procedimiento de abandono de la sesión:

- LEAVE.time*: Es el tiempo que el PMA que abandona otorga a sus CMA para que encuentren un nuevo PMA y se le adhieran. El valor por defecto de *LEAVE.time* es 10 segundos.

8.3 Reglas de codificación para representar valores utilizados en el RMCP-2

8.3.1 Regla de codificación de mensajes RMCP-2

En el cuadro 2 se enumeran los tipos de mensaje y sus correspondientes valores codificados.

Cuadro 2 – Tipos de mensaje del RMCP-2 y su valor codificado

Tipo de mensaje	Valor (8 bits)
SUBSREQ	0000010 ₍₂₎
SUBSANS	0000011 ₍₂₎
PPROBREQ	00000100 ₍₂₎
PPROBANS	00000101 ₍₂₎
HSOLICIT	00000110 ₍₂₎
HANNOUNCE	00000111 ₍₂₎
HLEAVE	00001000 ₍₂₎
RELREQ	00001001 ₍₂₎
RELANS	00001100 ₍₂₎
STREQ	00010010 ₍₂₎
STANS	00010011 ₍₂₎
STCOLREQ	00010100 ₍₂₎

Cuadro 2 – Tipos de mensaje del RMCP-2 y su valor codificado

Tipo de mensaje	Valor (8 bits)
STCOLANS	00010101 ₍₂₎
LEAVREQ	00010110 ₍₂₎
LEAVANS	00010111 ₍₂₎
HB	00011000 ₍₂₎
TERMREQ	00011001 ₍₂₎
TERMANS	00011010 ₍₂₎

8.3.2 Valores que devuelve el RMCP-2

En el cuadro 3 se presentan los valores codificados y el significado de los códigos de resultado, que son los códigos que normalmente devuelven las peticiones del RMCP-2, como SUBSREQ y RELREQ.

Cuadro 3 – Códigos de resultado

Código de resultado	Significado
0x01 00	OK
0x02 00	Problema del sistema
0x03 00	Problema administrativo

8.3.3 Valores relativos al ROOTPATH de RMCP-2

En el cuadro 4 se enumeran los códigos que especifican los diversos tipos de ROOTPATH. El código de instrucción del ROOTPATH puede convertirse en un nuevo valor.

Cuadro 4 – Códigos de instrucción de ROOTPATH

Tipo	Código	Significado
RP_ID	0x01 01	El ROOTPATH seguido contiene sólo la MAID de cada salto
RP_BW	0x01 02	El ROOTPATH seguido contiene sólo el ancho de banda de cada salto
RP_DL	0x01 04	El ROOTPATH seguido contiene sólo el retardo percibido en cada salto
RP_ID_BW	0x01 03	El ROOTPATH seguido contiene la MAID y el ancho de banda de cada salto
RP_ID_DL	0x01 05	El ROOTPATH seguido contiene la MAID y el retardo de cada salto
RP_ID_BW_DL	0x01 07	El ROOTPATH seguido contiene la MAID, el ancho de banda y el retardo de cada salto
RP_PSEUDO	0x01 00	El ROOTPATH que sigue es un seudo ROOTPATH para la recuperación ante fallos

En el cuadro 5 se enumeran los tamaños de los elementos de ROOTPATH.

Cuadro 5 – Tamaño de cada tipo de ROOTPATH

Tipo	Longitud (Bytes)
RP_ID	16
RP_BW	4
RP_DL	4

8.3.4 Valores relativos a la recopilación de estados del RMCP-2

En el cuadro 6 se enumeran los valores codificados de STREQ y de STCOLREQ. Cada código posee dos bytes. En la lista se indica el tipo de petición, para garantizar que quien reciba la petición la pueda responder adecuadamente. Estos códigos de instrucción pueden combinarse para formar nuevos códigos.

Cuadro 6 – Código de instrucción para la indagación de estado

Tipo	Código	Significado
SI_UPTIME	0x02 01	El tiempo de actividad del MA
SI_DELAY	0x04 01	El estado del estado percibido por el MA desde la raíz (<i>ROOT</i>)
SI_RCV_PACKET	0x08 01	El número de paquetes recibidos por el MA desde que arrancó
SI_RCV_BYTES	0x08 02	El número de bytes recibidos por el MA desde que arrancó
SI_RCV_BW	0x08 04	El ancho de banda que el MA percibe con su PMA
SI_SND_PACKET	0x0F 01	El número total de paquetes enviados por el MA desde que arrancó
SI_SND_BYTES	0x11 02	El número total de bytes enviados por el MA desde que arrancó
SI_SND_BW	0x11 04	El ancho de banda total consumido por el MA destinado a servir los CMA
TI_DEPTH	0x12 01	La profundidad del MA dentro del árbol RMCP-2
TI_MA_LIST	0x14 01	Una lista de los MA del árbol RMCP-2, limitada por la opción TreeExplor
TI_AV_DELAY	0x14 02	El retardo medio limitado por la opción TreeExplor
TI_AV_BW	0x14 04	El ancho de banda medio abarcado por la opción TreeExplor

Los ocho bits más significativos del código especifican la categoría de la instrucción. Los ocho bits menos significativos especifican los elementos detallados, como el ancho de banda, los paquetes y los bytes.

8.3.5 Valores relativos al abandono

En el cuadro 7 se enumeran los códigos de motivo del abandono. Los ocho bits superiores de las reglas codificadas especifican la causa principal del abandono y los ocho bits menores especifican los motivos detallados para el abandono, como escasez de recursos o terminación por parte del usuario.

Cuadro 7 – Código de motivo del abandono

Categoría	Código LR Reason	Significado
Abandono	0x01 00	El MA decide abandonar
	0x02 00	Abandono del SMA
Expulsión	0x03 00	Expulsión del SM
	0x03 01	Expulsión del PMA
Cambio de progenitor	0x04 00	Cambio de progenitor del MA

8.3.6 Valores relativos a la terminación de la sesión

En el cuadro 8 se enumeran los códigos de la terminación de sesión. Los ocho bits más significativos de las reglas codificadas especifican el motivo principal de terminación de la sesión y los ocho bits menos significativos aclaran el motivo.

Cuadro 8 – Código de motivo de terminación

Categoría	TR_code	Significado
Terminación normal de la sesión	0xF1 00	La sesión termina normalmente
Terminación anormal de la sesión	0xF2 00	La sesión termina anormalmente sin motivo
	0xF2 01	La sesión termina anormalmente por solicitud del usuario

Anexo A

Algoritmo para la configuración del árbol

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

A.1 Regla de iniciación

El MA que se adhiera por primera vez a una sesión RMCP-2 debería recuperar la información de iniciación del SM, para unirse al árbol existente. Como ninguno de los MA posee información alguna sobre el árbol, cada MA deberá recopilar información acerca del árbol existente. Para construir independientemente el árbol RMCP-2, el SM entrega la información de iniciación a los MA que acaban de unirse. Por ende, la información de iniciación que maneja el SM debe ser tan fiable y óptima como sea posible. La información de iniciación consiste principalmente en un conjunto de listas de MA que gestiona el SM. Como la cantidad de información de iniciación es limitada, ésta no puede incluir una lista con todos los miembros, sino sólo la mínima necesaria para describir la sesión.

La información de iniciación óptima de cada MA está contenida en la lista que incluye los MA con la mayor capacidad de retransmisión, menores retardos y mayor posibilidad de unión satisfactoria al árbol. Por tanto, las únicas cosas que el SM puede determinar son la capacidad de hardware de los MA y la capacidad disponible en sentido descendente. En una sesión RMCP-2, el orden de preferencia de los MA es el siguiente:

- 1) MA especializado.
- 2) MA con la mayor profundidad en el árbol.
- 3) MA con el mayor ancho de banda.

Adicionalmente, cada MA debería saber cuántos nodos se permiten en sentido descendente.

- 1) Capacidad disponible para nuevos CMA.

Teniendo en cuenta todas estas consideraciones, el SM debería gestionar de la siguiente forma la información de iniciación, que contiene una lista de MA progenitores candidatos:

si se trata de un MA especializado

otorgue la mayor prioridad

en caso contrario

$$\begin{aligned} \text{priority} &= \text{Capacidad disponible de CMA} * \text{pw_cma} && + \\ &\text{possible_forwarding_bandwidth} * \text{pw_bandwidth} && + \\ &\text{diff_hop_rate} * \text{pw_hop} \end{aligned}$$

pw_cma = factor de ponderación dependiente de las políticas para el cma (%/cma)

pw_bandwidth = factor de ponderación dependiente de las políticas para el ancho de banda (%/bit/s)

pw_hop = factor de ponderación dependiente de las políticas para el salto (%/level)

Si todos los MA especializados de una sesión poseen suficiente capacidad para los MA en el sentido descendente, o si el administrador de la red desea conservar todos los MA hojas del MA, el SM sólo envía información sobre los DMA. Además, el SM debería garantizar que todos los MA que figuran en esta información estén activos.

Para asegurarse de que la lista de MA está actualizada, el SM verifica periódicamente el estado de los MA y emplea la siguiente regla para actualizar la información sobre el estado:

si expira el temporizador MA_LIST_PROB

explore y actualice el estado de los MA que figuran en MA_LIST

si ocurre una adhesión satisfactoria

explore y actualice el estado del MA que se adhirió

Si el tamaño de la sesión RMCP-2 es bastante pequeño o si el SM desea llevar un control estricto de la sesión, el SM entrega una lista completa de MA a cada MA nuevo.

si el SM lleva un control estricto de la sesión RMCP-2
en caso contrario, si el número de MA_LIST es menor al tamaño máximo de un mensaje SUBSANS
 envíe toda la lista MA_list de la base de datos del SM

A.2 Regla para descubrir vecinos

Como la información de iniciación del SM constituye tan sólo una parte de toda la sesión RMCP-2, la información es insuficiente para que los MA encuentren su mejor PMA. Además, los MA no pueden identificar sus vecinos más cercanos. Por tanto, los MA, independientemente de si ya se han adherido a la sesión, deberían explorar los vecinos intercambiando sus NL. Este mecanismo también ayuda a los MA a medir la distancia de la red y el estado de cada MA.

La NL utilizada para descubrir los vecinos se construye de la siguiente forma:

incluya el DMA en MA_LIST_FOR_ND
si el funcionamiento de la sesión se fundamenta en DMA
 break;
en caso contrario
 incluya su root_path en MA_LIST_FOR_ND
 incluya su lista de CMA directamente conectados en MA_LIST_FOR_ND
 incluya su lista de MA examinados y de MA sin examinar
 hasta que el tamaño del mensaje PPROB sea satisfactorio
 está completa la lista MA_LIST_FOR_ND

La condición de red de los dos MA que participan en el descubrimiento de vecinos puede calcularse así:

retardo = $RTT/2$
 ancho de banda = tamaño de paquete recibido/($RTT/2$)

A.3 Regla para seleccionar el HMA

Cuando en una misma zona habilitada para la multidifusión haya dos o más MA, puede ocurrir el problema de contienda por convertirse en HMA. En caso de contienda por convertirse en HMA, cada MA envía un mensaje HANNOUNCE para intentar convertirse en el nuevo HMA y por lo tanto, todos los MA de la zona habilitada para la multidifusión pueden recibir varios mensajes HANNOUNCE procedentes de diferentes MA. La siguiente regla se utiliza para detectar la contienda:

si llega un HANNOUNCE duplicado con Auth válida y la misma SID procedente de MAID diferentes
 decida hay colisión de HANNOUNCE

La siguiente regla resuelve el problema de contienda por convertirse en HMA:

si sus tiempos de adhesión a la sesión son diferentes
 elija como HMA a quien se adhirió primero
en caso contrario
 elija como HMA al de menor MAID

A.4 Regla de aceptación de CMA

Al recibir un nuevo RELREQ de un MA, el PMA debe decidir si acepta la petición de retransmisión. La siguiente es la regla para tomar la decisión:

llega una nueva petición de retransmisión (RELAY)

si tiene suficiente capacidad para aceptar el nuevo CMA

si se cumplen exigencia de QoS && políticas && perfil de datos && condiciones de los datos

acepte la petición de retransmisión del MA

en caso contrario

niegue la petición de retransmisión del MA

A.5 Regla para decidir el progenitor

Cada MA, incluidos los nuevos MA, debe seleccionar el MA de menor costo de entre los MA explorados. El MA seleccionado se convierte entonces en candidato a PMA. Cuando un MA se adhiere a la sesión RMCP-2 por primera vez, el MA considera que el candidato a PMA es su PMA o en su defecto se reserva el candidato a PMA para un cambio de progenitor. La regla para calcular el costo y seleccionar el mejor PMA se enuncia como sigue:

si hay un MA en la misma zona habilitada para la multidifusión

si el MA pertenece a la misma LAN local

seleccione al MA como candidato a PMA

en caso contrario

encuentre el MA de menor costo

costo = diff_delay_rate * wt_delay +

diff_bandwidth_rate * w_bandwidth +

diff_hop_rate * w_hop

si hay dos o más candidatos a PMA con el mismo costo

seleccione el nodo con la menor diferencia entre las dos MAID

*) $\text{sum}(\text{wt_delay}, \text{w_bandwidth}, \text{w_hop}) = 1$

w_delay = factor de ponderación para el retardo

w_bandwidth = factor de ponderación para el ancho de banda

w_hop = factor de ponderación para la profundidad en el árbol

El costo de seleccionar el PMA se puede calcular así: el RMCP-2 utiliza un factor de ponderación para configurar el árbol de entrega de datos óptimo. Este factor de ponderación lo fija el administrador de la red o el creador de la sesión. Se supone que el MA C obtuvo la siguiente información sobre el MA A y el MA B:

	MA A	MA B
retardo	10 mseg	11 mseg
ancho de banda	100 mbps	90 mbps
profundidad en el árbol	nivel 5	nivel 7

Utilizando estas medidas, el MA C puede identificar cuál de los MA se encuentra más cerca. Los siguientes ejemplos muestran la forma en que el MA C calcula el costo teniendo en cuenta el factor de ponderación:

	Caso 1	Caso 2	Caso 3
Comparación entre MA A y MA B	costo = $(10-11)/E(10,11)*0.5$ $+ (100-90)/E(100,90)*0.4$ $+ (5-7)/E(5,7) * 0.1$ = -0.039	costo = $(10-11)/E(10,11)* 0.4$ $+ (100-90)/E(100,90)*0.4$ $+ (5-7)/E(5,7) * 0.2$ = -0.063	costo = $(10-11)/E(10,11)*0.4$ $+ (100-90)/E(100,90)*0.6$ $+ (5-7)/E(5,7) * 0.0$ = 0.025
Decisión	Escoger MA A	Escoger MA A	Escoger MA B
Caso 1)	factor de ponderación (w_delay/w_bandwidth/w_hop) = (0.5/0.4/0.1)		
Caso 2)	factor de ponderación (w_delay/w_bandwidth/w_hop) = (0.4/0.4/0.2)		
Caso 3)	factor de ponderación (w_delay/w_bandwidth/w_hop) = (0.4/0.6/0.0)		

Si el costo de dos candidatos a PMA es igual, el MA utiliza la siguiente regla para elegir uno de los dos candidatos:

si dos o más candidatos a PMA tienen el mismo costo
 elija el nodo con la menor diferencia entre las dos MAID

A.6 Regla para perfeccionar el árbol

Como los MA no pueden conocer la información exacta de toda la topología de la red, podría no tomarse la mejor decisión al elegir el progenitor. Por tanto, cada MA debe mejorar gradualmente la decisión del RMCP-2 aplicando el mecanismo de cambio de progenitor. La siguiente regla determina cuándo iniciar el proceso de cambio de progenitor:

si $| (QoS\ percibida - nueva\ QoS) / QoS\ percibida | > Estabilidad$ (según las políticas)
 inicie el cambio de progenitor

*) El administrador fija el factor de estabilidad cuando crea la sesión.

Estabilidad = 0 ~ 100% (a mayor factor de estabilidad, menos cambios de progenitor)

A.7 Regla de expulsión del PMA

El PMA puede expulsar uno de sus CMA si disminuye el número de CMA permitidos a los MA o si el CMA causa problemas. El PMA utiliza la siguiente regla para decidir la expulsión:

si (número máximo de CMA < número actual de CMA)
 seleccione al peor CMA, envíe LEAVREQ al CMA

en caso contrario si (el CMA degrada la QoS de retransmisión CMA)
 envíe LEAVREQ al CMA

Anexo B

Mecanismo de entrega de datos en tiempo real

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

B.1 Panorámica

Cuando un MA necesita transferir datos en tiempo real a varios usuarios, adopta un mecanismo de tunelización IP-IP para obtener un alto caudal. En esta subcláusula se describe la utilización del método de tunelización en la entrega de datos en tiempo real. En la figura B.1 se presenta la arquitectura global de la tunelización IP.

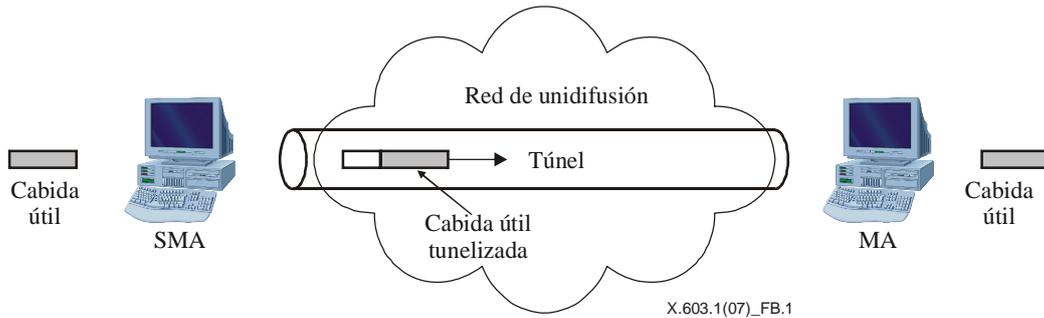


Figura B.1 – Método de tunelización IP

B.2 Mecanismo túnel IP-IP para la entrega de datos en tiempo real de RMCP-2

Se construye un trayecto para la entrega de datos por multidifusión en el trayecto de control, mediante el intercambio de una serie de mensajes de control RMCP-2. El MA construye el trayecto de entrega de datos hacia sus MA subordinados. El módulo de control proporciona un módulo de datos con la dirección IP de los MA subordinados y un mecanismo de encapsulación. Esta información se incluye en el perfil de datos del mensaje SUBSREQ a fin de construir el cuadro para la entrega de datos. El módulo de datos de cada MA almacena la dirección de los MA subordinados en el cuadro de entrega. Con éste método se construye un canal para la entrega de datos en tiempo real entre los PMA y sus CMA, que se utiliza para la entrega de datos en tiempo real desde el SMA a los MA hoja. Una vez establecido el canal de entrega, la aplicación de grupo lo opera como si perteneciera a la red IP con multidifusión, tal como se indica en la figura B.2.

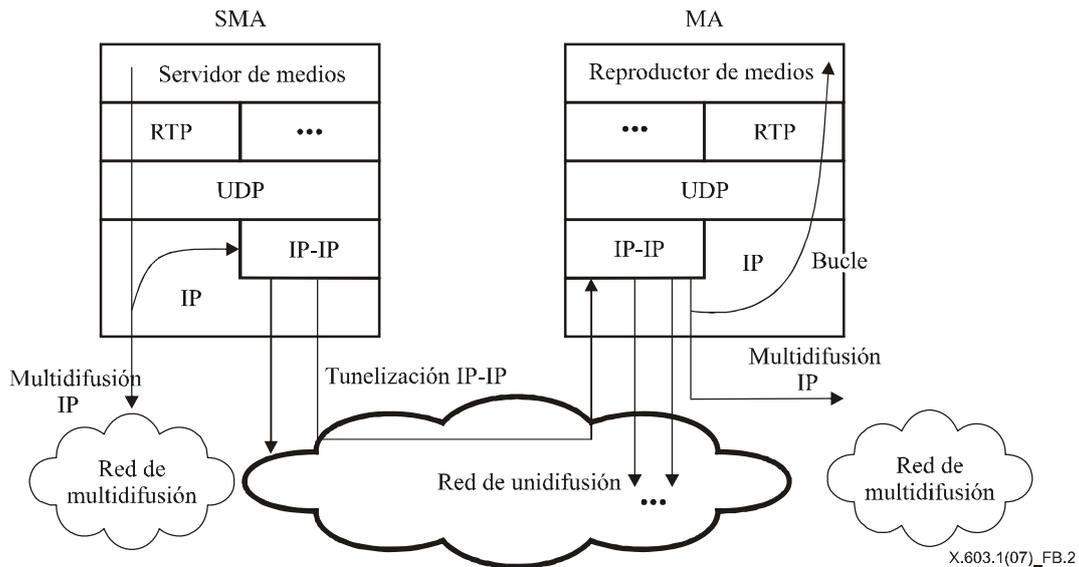


Figura B.2 – Canal de datos en tiempo real con encapsulación IP-IP

El SMA encapsula los paquetes de datos de multidifusión IP en los paquetes de datos de unidifusión y transmite los datos encapsulados hacia los MA en sentido descendente, utilizando unidifusión por la red de unidifusión. El SMA también envía por multidifusión los paquetes de datos de multidifusión IP hacia una zona habilitada para la multidifusión. Tras recibir los paquetes de datos tunelizados, cada CMA los desencapsula para extraer los paquetes de datos de multidifusión IP.

Si los CMA se encuentran en la misma región de multidifusión, el PMA sencillamente reenvía por multidifusión los datos hacia la región de multidifusión. Si uno o varios de los CMA se encuentran en la región de unidifusión, el PMA debe encapsular los paquetes de datos de multidifusión IP y transmitir los datos tunelizados hacia sus CMA.

Anexo C

Mecanismo para la entrega fiable de datos

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

C.1 Panorámica

El mecanismo presentado aquí es un mecanismo superpuesto para la entrega fiable de datos. Los nodos de la relación progenitor-vástago intercambian los perfiles de datos a fin de encontrar un conjunto de datos disponible. Para que sea factible, cada nodo abre una conexión TCP para la entrega fiable de datos. Una vez establecido el canal para la entrega de datos, cada nodo recibe los datos de su progenitor, si los hay, y los retransmite en sentido descendente. De esta forma, los datos de la raíz pueden llegar a los nodos hoja utilizando varios nodos intermedios.

Al utilizar perfiles de datos, los nodos pueden buscar otros nodos con los datos necesarios y, de ser necesario, los nodos que utilicen este mecanismo pueden cambiar de nodo en el sentido ascendente. En la siguiente cláusula se describe la secuencia del protocolo del método de multidifusión superpuesto en el caso de entrega fiable de datos simplex.

C.2 Funcionamiento

C.2.1 Conexión del canal

En la figura C.1 se presenta el procedimiento para la conexión del canal, que sigue los siguientes cuatro pasos:

- 1) El CMA envía al PMA un perfil de datos que contiene la dirección local y el número de secuencia que espera recibir del nodo que se adhiere. Si el nuevo nodo que se adhiere no posee información sobre el mecanismo de entrega, el número de secuencia que espera recibir se fijará a NEWEST (el más reciente).
- 2) Tras recibir el perfil de datos del CMA, el PMA responde con un perfil de datos que contiene la dirección de escucha y el número de secuencia actual.
- 3) Dos MA que intercambian información por el canal establecen conexiones TCP entre sí y luego atribuyen una ID de canal a la conexión establecida.
- 4) El PMA envía datos de usuario encapsulados empleando la ID de canal, atribuida por el propio PMA, y el número de secuencia.

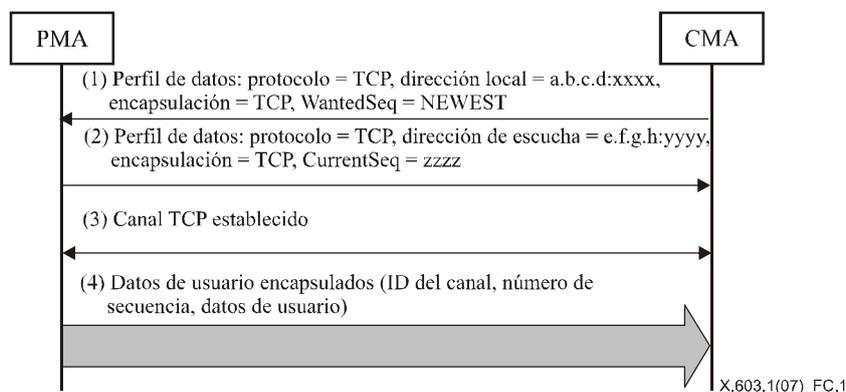


Figura C.1 – Procedimiento para la conexión del canal

C.2.2 Desconexión del canal

El proceso de desconexión del canal consta de los siguientes tres pasos, ilustrados en la figura C.2:

- 1) Se tiene una conexión TCP entre dos MA.
- 2) El PMA envía datos de usuario encapsulados con la ID de canal, atribuida por el PMA mismo, y el número de secuencia.
- 3) Cualquiera de los MA puede suprimir el canal TCP solicitando el cierre del TCP.

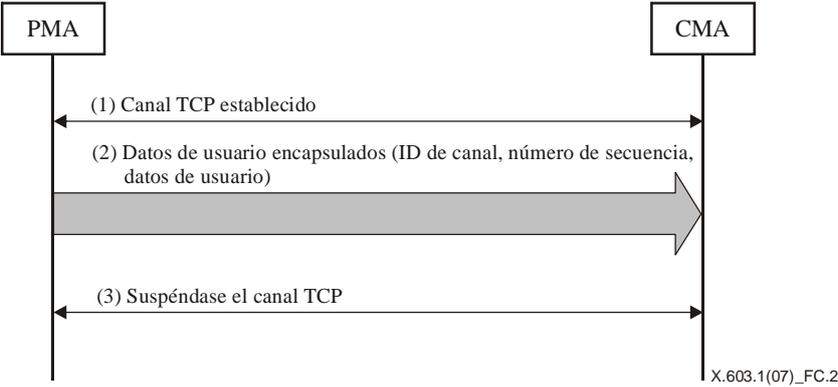


Figura C.2 – Procedimiento para la desconexión del canal

C.2.3 Cambio de canal

El procedimiento de cambio de canal consta de los siguientes siete pasos, ilustrados en la figura C.3:

- 1) Se tiene una conexión establecida entre dos MA.
- 2) El PMA envía datos de usuario encapsulados, con la ID de canal, atribuida por el PMA mismo, el número de secuencia y los datos de usuario.
- 3) El CMA envía al nuevo CMA el perfil de datos, que contiene su dirección local y el número de secuencia que espera recibir.
- 4) Al recibir de un nuevo CMA el perfil de datos, el nuevo PMA responde con el perfil de datos que contiene la dirección de escucha, el número de secuencia actual y el número de secuencia almacenado.
- 5) Si la secuencia deseada se encuentra entre el número de secuencia almacenado y el número de secuencia actual, el CMA desconecta el canal TCP con un PMA viejo.
- 6) Los nuevos PMA y CMA, que se conectan mediante TCP, atribuyen una nueva identificación de canal a la conexión.
- 7) El nuevo PMA envía datos encapsulados con la id de canal que él mismo atribuyó y el número de secuencia del número de secuencia deseado.

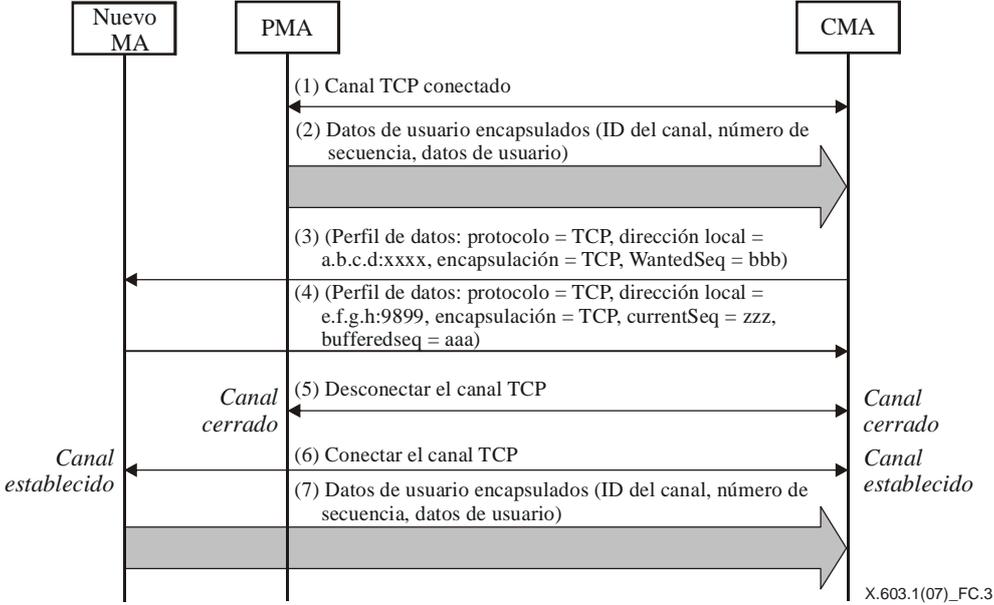


Figura C.3 – Procedimiento para el cambio de canal

C.3 Formato para la encapsulación de datos

En la figura C.4 se muestra el mensaje de datos de usuario de la entrega fiable de datos:

- a) En reserva: Se reserva para uso futuro y por ahora se fija a cero.
- b) Longitud: Longitud total del mensaje actual, en bytes.
- c) ID del canal: Identificación del canal de datos entre saltos de datos.
- d) Número de secuencia: El número de secuencia atribuido por un SMA de la actual unidad de datos de servicio. Este valor se puede atribuir circularmente de forma global.

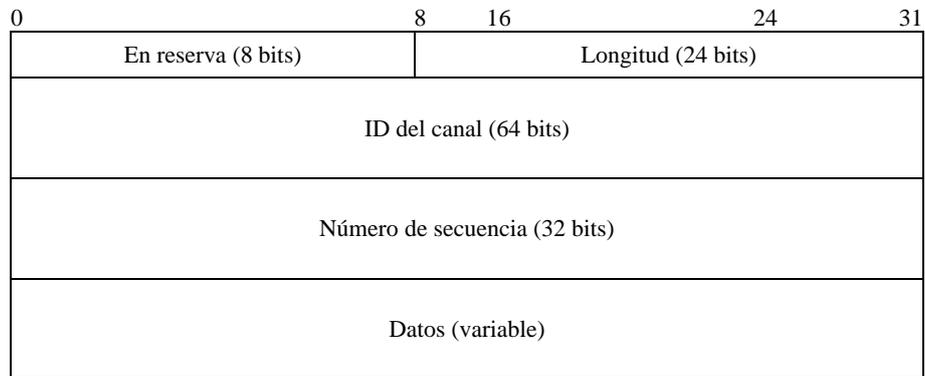


Figura C.4 – Formato para la encapsulación de datos

C.4 Perfil de datos

En RMCP-2, cuando se utiliza el método de tunelización, debe utilizarse el siguiente formato para el perfil de datos concreto:

```
"Protocolo = TCP, dirección de escucha = a.b.c.d:9899, Encapsulación= TCP, CurrentSeq=xxxx,  
BufferedSeq=yyyy, WantedSeq=zzz"
```

Anexo D

API del RMCP-2

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

En el presente apéndice se especifican las interfaces de programación de aplicaciones (API, *application programming interfaces*) del protocolo RMCP-2. Las API descritas en este anexo pueden utilizarse en aplicaciones que utilizan las capacidades del RMCP-2.

Las API del RMCP-2 obedecen las API de zócalo de Berkeley. No obstante, para distinguir las API del RMCP-2 de las funciones de zócalo de Berkeley, a las API del RMCP-2 se les coloca el prefijo "rmcp2_" (como por ejemplo, rmcp2_socket).

D.1 Panorámica

D.1.1 Las API

En el cuadro D.1 se resumen las funciones de las API del RMCP-2:

Cuadro D.1 – Resumen de las API del RMCP-2

Categoría	Nombre	Descripción
Control del MA	<i>rmcp2_socket()</i>	Crea un nuevo zócalo del RMCP-2.
	<i>rmcp2_bind()</i>	Vincula la información sobre una sesión, como la id de la sesión, la función, las direcciones local y de grupo, el perfil de datos, etc.
	<i>rmcp2_connect()</i>	Se adhiere a una sesión RMCP-2.
	<i>rmcp2_close()</i>	Finaliza la sesión y libera el zócalo.
	<i>rmcp2_setsockopt()</i>	Fija las opciones del zócalo y del protocolo al módulo de control del MA de RMCP-2.
	<i>rmcp2_getsockopt()</i>	Recupera las opciones del zócalo y del protocolo del módulo de control de RMCP-2.
	<i>rmcp2_recv()</i>	Entrega los datos recibidos a una aplicación.
	<i>rmcp2_send()</i>	Envía los datos de la aplicación a un grupo RMCP-2.
Entrega de datos	<i>rmcp2_recv()</i>	Entrega los datos recibidos a una aplicación.
	<i>rmcp2_send()</i>	Envía los datos de la aplicación a un grupo RMCP-2.
Gestión de la sesión	<i>rmcp2_session_open()</i>	Crea una nueva sesión RMCP-2.
	<i>rmcp2_session_close()</i>	Finaliza la sesión RMCP-2 y libera los recursos atribuidos.
	<i>rmcp2_member_out()</i>	Expulsa de la sesión al busca problemas.
	<i>rmcp2_status_report()</i>	Examina la situación de una sesión RMCP-2 concreta.
	<i>rmcp2_char_change()</i>	Fija o modifica las características de una sesión RMCP-2.

D.1.2 Utilización de la API del RMCP-2

En la figura D.1 se ilustra la utilización de la API del RMCP-2 y las secuencias de las API en términos del SM y de dos MA.

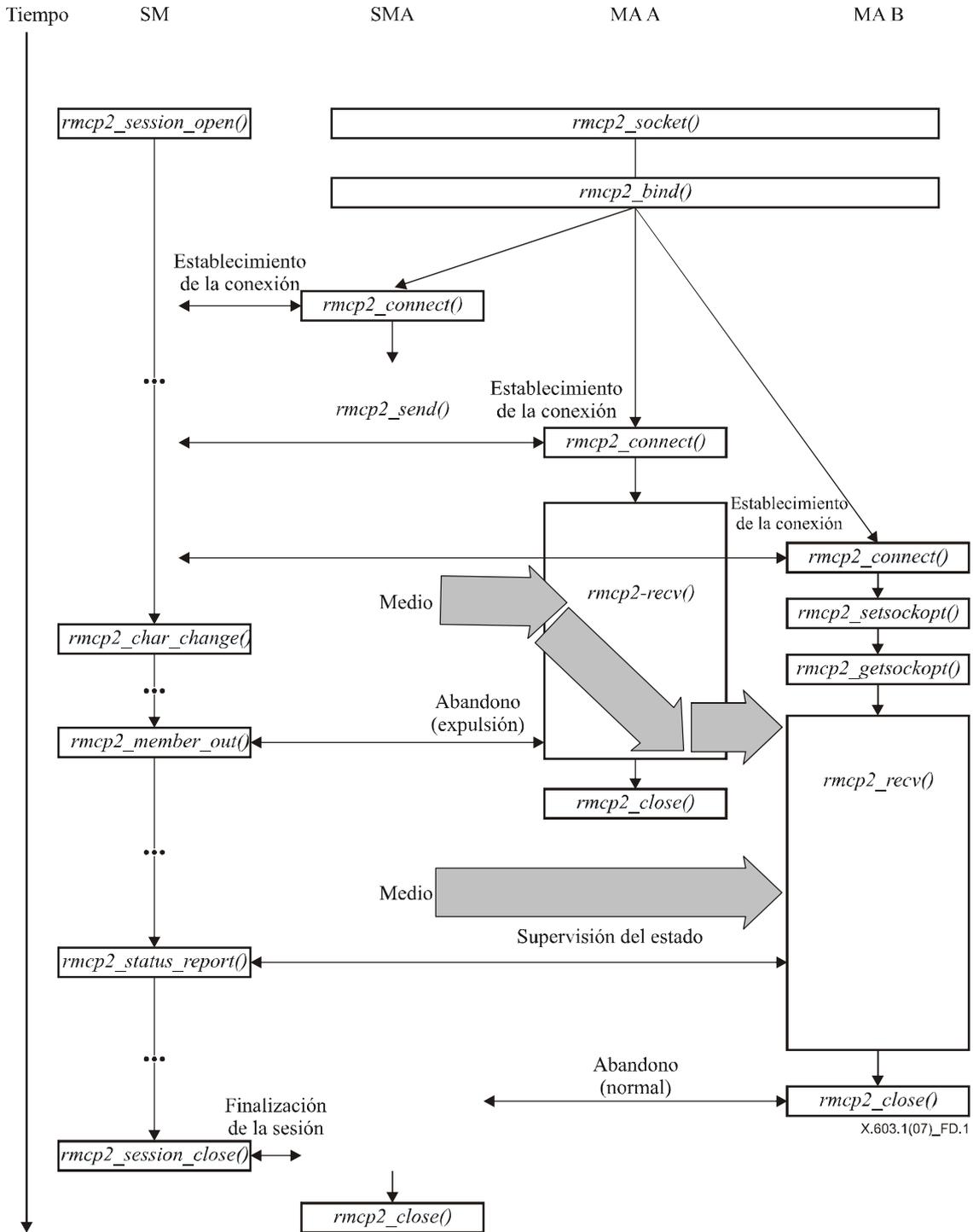


Figura D.1 – Utilización de las API del RMCP-2

D.2 Funciones API del RMCP-2

D.2.1 Funciones relativas al control del MA

En esta subcláusula se define un conjunto de API del RMCP-2 relacionadas con los MA. Las aplicaciones RMCP-2 utilizan las funciones definidas aquí para adherirse a las sesiones RMCP-2 y para abandonarlas. En la siguiente cláusula se definen las funciones de envío y recepción.

int rmcp2_socket(void)

Cuando se utiliza el protocolo RMCP-2, las aplicaciones invocan la función *rmcp2_socket()* para solicitar a un MA de RMCP-2 que inicie una sesión RMCP-2. Si el resultado es satisfactorio, la función devuelve un identificador de zócalo diferente a cero, y en caso contrario devuelve un valor negativo y los correspondientes códigos de error.

*int rmcp2_bind(int sd, session_profile *profile, int profile_len)*

Las aplicaciones RMCP-2 pueden invocar la función *rmcp2_bind()* cuando deseen fijar alguna información en una sesión. La función fija la información del MA necesaria para la adhesión de éste a una sesión RMCP-2. Los siguientes son algunos de los detalles más importantes de la sesión:

- a) ID de la sesión.
- b) Su función en la sesión RMCP-2, como por ejemplo MA del lado emisor o MA hoja.
- c) Una dirección de MA concreta para el funcionamiento.
- d) Una dirección de grupo.
- e) El perfil de datos que se desee utilizar.
- f) Otra información específica del fabricante, etc.

La función devuelve cero si el enlace se efectúa satisfactoriamente, o en caso contrario, devuelve un valor negativo con el correspondiente código de error.

*int rmcp2_connect(int sd, struct sockaddr *sm_addr, int addrlen)*

La aplicación RMCP-2 puede comenzar el proceso de adhesión a la sesión RMCP-2 sólo después de lograrse un enlace satisfactorio. Al hacer un llamado a la función *rmcp2_connect()*, las aplicaciones RMCP-2 pueden invocar el MA al que desean suscribirse y adherirse a la sesión RMCP-2. Los argumentos que la función emplea para adherirse a la sesión RMCP-2 son: la dirección del SM y la ID de la sesión. La función devuelve cero si la adhesión se efectúa satisfactoriamente, en caso contrario, devuelve un valor negativo con un código de error.

int rmcp2_close(int sd)

La aplicación RMCP-2 invoca la función *rmcp2_close()* para abandonar la sesión. Al hacer un llamado a la función *rmcp2_close()*, la aplicación hace que el MA de RMCP-2 inicie el procedimiento de abandono y libere el bloque de control del protocolo. La función devuelve cero si el abandono de la sesión es satisfactorio, en caso contrario, devuelve un entero negativo con el correspondiente código de error.

*int rmcp2_setsockopt(int sd, int opt_type, char *opt, int optlen)*

La función *rmcp2_setsockopt()* permite que una aplicación fije o modifique uno o varios de los parámetros del protocolo. Si es satisfactoria, la función devuelve cero, en caso contrario, devuelve un entero negativo con el correspondiente código de error.

*int rmcp2_getsockopt(int sd, int opt_type, char *opt, int *optlen)*

Si desea conocer el valor de uno o varios de los parámetros de protocolo del MA, la aplicación invoca la función *rmcp2_getsockopt()*, pasándole un *opt_type* y un **opt* vacío, lo suficientemente grande para contener la información que suministre el MA. Si el resultado es satisfactorio, la función devuelve cero, en caso contrario, devuelve un entero negativo con el correspondiente código de error.

D.2.2 Funciones relativas a la entrega de datos del MA

En esta cláusula se define un conjunto de API de RMCP-2 relacionadas con la entrega de datos del RMCP-2. Las aplicaciones utilizan estas API para la entrega y recepción de tráfico de datos del RMCP-2.

*int rmcp2_recv(int sd, char *buf, int len, int flags)*

La aplicación receptora que desee recibir datos de una sesión RMCP-2 invoca la función *rmcp2_recv()* y copia los datos recibidos de *len* del módulo de datos del MA. Si el resultado es satisfactorio, la función devuelve cero, en caso contrario devuelve un valor negativo con un código de error.

*int rmcp2_send(int sd, char *buf, int len, int flags)*

Las aplicaciones RMCP-2 invocan la función *rmcp2_send()* para enviar datos a una sesión RMCP-2. No obstante, como el protocolo RMCP-2 sólo admite el servicio de entrega de datos de uno a varios, el MA de la aplicación que hace el envío debe ser un SMA. Esta función copia los datos de *len* al módulo de datos del MA. Si el resultado es satisfactorio, la función devuelve el número de bytes que envió, en caso contrario, devuelve un valor negativo con un código de error.

D.2.3 Funciones relativas a la gestión de la sesión

La aplicación gestor de sesión (aplicación SM) puede iniciar, gestionar y finalizar las sesiones RMCP-2 invocando las API definidas en la presente cláusula. Se utiliza el término *aplicación SM* para hacer referencia al SM del RMCP-2, a fin de evitar la ambigüedad que pudiera suscitarse entre *aplicación que utiliza el SM de RMCP-2* y el *SM del RMCP-2*, propiamente dicho.

*SID rmcp2_session_open(session_profile *session_profile)*

La aplicación SM que desee que el SM inicie una sesión RMCP-2, invoca la función *session_open()* con un perfil de sesión. El argumento *session_profile* debe contener la suficiente información de sesión para crear y administrar una sesión RMCP-2. Una vez reciba un perfil de sesión, el SM atribuye la suficiente capacidad a la sesión RMCP-2 concreta. Si la sesión se crea satisfactoriamente, la función devuelve la ID de la nueva sesión, en caso contrario, devuelve cero y el correspondiente código de error.

int rmcp2_session_close(SID session_id)

La aplicación SM que desee que el SM finalice la sesión RMCP-2, invoca la API *session_close()*. Esta función solicita al SM que inicie el procedimiento de finalización de la sesión RMCP-2 y libera luego la suficiente capacidad para la sesión RMCP-2. Una vez la sesión haya finalizado satisfactoriamente, la función devuelve un valor no negativo, en caso contrario, devuelve un valor negativo con un código de error.

int rmcp2_member_out(SID session_id, MAID maid)

Cuando un miembro de la sesión o un MA ocasionan problemas graves o violan las normas de la sesión, la aplicación SM puede expulsar al miembro problemático de la sesión. Cuando la aplicación SM desea expulsar un miembro en particular de la sesión, invoca la API *member_out()* con la ID de sesión y la ID del miembro a ser expulsado.

*int rmcp2_status_report(SID session_id, int command, char *result, int *result_len)*

La función *status_report()* permite que la aplicación SM examine el estado de una sesión. Normalmente la función se invoca empleando argumentos como la ID de la sesión, las instrucciones de funcionamiento y una posición de memoria donde ubicar los resultados. Si el resultado es satisfactorio, la función devuelve cero, en caso contrario devuelve un valor negativo y un código de error.

*int rmcp2_char_change(SID session_id, int command, char *opt, int optlen)*

La función *rmcp2_char_change_setopt()* permite que la aplicación SM fije o modifique las características de la sesión RMCP-2, como la información de AUTH. Si el resultado es satisfactorio, la función devuelve cero, en caso contrario devuelve un entero negativo con el correspondiente código de error.

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