UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T X.602

(04/2004)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE X: REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

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

Tecnología de la información – Protocolo de gestión de grupo

Recomendación UIT-T X.602

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

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.399
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.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LAS TELECOMUNICACIONES	X.1000–

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

NORMA INTERNACIONAL ISO/CEI 16513
RECOMENDACIÓN UIT-T X.602

Tecnología de la información – Protocolo de gestión de grupo

Resumen

El protocolo de gestión de grupo (GMP) es un protocolo de control de la capa aplicación para crear sesiones de grupo y gestionar los miembros que participan en los mismos. Por lo general, se supone que hay un servidor GMP, un cliente que crea la sesión (o creador de la sesión) y uno o varios clientes que participan en la sesión (o participantes en la sesión).

El GMP está formado por la gestión de sesión (SM), la gestión de miembros (MM) y la función de intercambio de información entre la SM y la MM.

Orígenes

La Recomendación UIT-T X.602 fue aprobada el 29 de abril de 2004 por la Comisión de Estudio 17 (2001-2004) del UIT-T por el procedimiento de la Recomendación UIT-T A.8. Se publica también un texto idéntico como Norma Internacional ISO/CEI 16513.

Palabras clave

Gestión de grupo, gestión de miembros, gestión de sesión, servidor QoS.

PREFACIO

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

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

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

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

NOTA

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

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

PROPIEDAD INTELECTUAL

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

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

ÍNDICE

Introducción

Los protocolos de transporte multidifusión convencionales no incluyen un mecanismo dinámico para la gestión de grupos en lo que respecta a la adhesión/abandono de miembros y a la modificación de información relativa a los miembros.

El GMP constituye el marco básico del mecanismo de gestión de sesiones (SM) multidifusión y gestión de miembros (MM), que permite gestionar de manera conveniente las sesiones y miembros multidifusión. Este protocolo puede constituir la base fundamental para la comunicación multidifusión fiable.

El GMP funciona sobre los protocolos de transporte convencionales y/o ECTP, como se muestra en la figura 1.

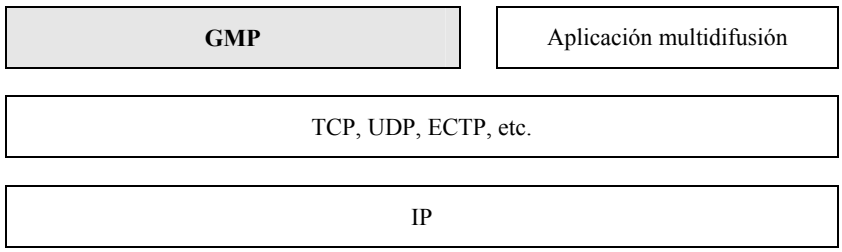

Figura 1 – Modelo GMP (pila de protocolos GMP)

NORMA INTERNACIONAL
RECOMENDACIÓN UIT-T

Tecnología de la información – Protocolo de gestión de grupo

1 Alcance

En esta Recomendación | Norma Internacional se especifica un protocolo de gestión de grupo (GMP, *group management protocol*), que es un protocolo de control de la capa de aplicación para la creación de sesiones de grupo y la gestión de los miembros que participan en los mismos.

El GMP está formado por la gestión de sesión (SM, *session management*), la gestión de miembros (MM, *membership management*) y la función de intercambio de información entre la SM y la MM. La SM se encarga de la creación y supresión de sesiones. La MM gestiona la lista de miembros utilizando para ello la información de sesiones que recupera de la SM.

De conformidad con la Rec. UIT-T X.601, "Marco para comunicaciones entre múltiples pares", el servicio de comunicación entre múltiples entidades pares se lleva a cabo en siete fases distintas: registro, inscripción (o enrolamiento), activación, transferencia de datos, desactivación, desinscripción (o desenrolamiento) y desregistro. Dado que una de estas operaciones, a saber, la transferencia de datos, puede realizarse utilizando ECTP o TCP, la SM puede ocuparse del resto de las operaciones: creación, anuncio, registro, inscripción, activación, en particular el anuncio de sesión. Además, la MM gestiona los miembros del grupo que pertenecen a grupos de inscritos o de activos.

La SM puede servir de interfaz adecuada para los usuarios dado que puede realizarse en la Web. La operación de la MM es transparente para los usuarios, al igual que el protocolo de transporte.

2 Referencias normativas

Las siguientes Recomendaciones 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 las Normas Internacionales citadas a continuación. Los miembros de la CEI y de la ISO mantienen registros de las Normas Internacionales actualmente vigentes. La Oficina de Normalización de las Telecomunicaciones del UIT-T mantiene una lista de las Recomendaciones UIT-T actualmente vigentes.

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

3 Definiciones

3.1 Términos definidos en la Rec. UIT-T X.601

Esta Recomendación | Norma Internacional se basa en los conceptos indicados en el marco para comunicaciones entre múltiples entidades pares (Rec. UIT-T X.601) y se utilizan los siguientes términos definidos en esa Recomendación:

a) múltiples pares;

b) comunicación entre múltiples entidades pares; y

c) transmisión multidifusión.

3.2 Términos definidos en la Rec. UIT-T X.605 | ISO/CEI 13252

Esta Recomendación | Norma Internacional se basa en los conceptos introducidos en la definición del servicio perfeccionado de transporte de comunicaciones (Rec. UIT-T X.605 | ISO/CEI 13252) y se utilizan los siguientes términos definidos en esa Recomendación:

a) grupo de inscritos;

b) grupo de registrados;

c) grupo de activos; y

d) propietario de la conexión de transporte (TC-owner).

3.3 Términos definidos en esta Recomendación | Norma Internacional

3.3.1 cliente GMP: Programa de aplicación que envía y recibe datos mediante el GMP. Los clientes almacenan y obtienen la información a través de un servidor. Todos los clientes deben acceder al servidor para obtener la información a través del mismo. Los clientes se dividen mayormente en el creador de la sesión y los participantes en la sesión.

3.3.2 servidor GMP: Programa de aplicación que se encarga de la gestión de la sesión y la gestión de miembros.

3.3.3 creador de la sesión: Cliente que crea y puede terminar una sesión. El creador accede al servidor mediante su identificador ID, introduce la información relativa a la creación de la sesión y envía la información al servidor. El servidor que recibe la petición del creador añade esa información a la lista de sesiones creadas. El creador de la sesión puede ser un propietario de la conexión de transporte definido en ECTS.

3.3.4 cliente de la sesión: Cliente que trata de ser un participante en la sesión.

3.3.5 participante en la sesión: Cliente que se ha registrado en una sesión y trata de participar en la misma. Después del registro, el participante en la sesión se suma a la sesión y se convierte en un miembro activo (es decir, se da de alta en la lista de sesiones y en la lista de miembros registrados). El participante en la sesión puede ser un participante en la conexión de transporte definido en ECTS.

4 Abreviaturas

A los efectos de esta Recomendación | Norma Internacional se utilizan las siguientes siglas.

4.1 Tipos de mensajes

4.1.1 Tipos de mensajes SM

SAREQ	Mensaje petición de activación de sesión (*session activation request message*)
SCACC	Mensaje aceptación de creación de la sesión (*session creation accept message*)
SCCON	Mensaje confirmación de creación de la sesión (*session creation confirm message*)
SCINF	Mensaje información de creación de la sesión (*session creation information message*)
SCREJ	Mensaje rechazo de creación de la sesión (*session creation reject message*)
SCREQ	Mensaje petición de creación de la sesión (*session creation request message*)
SDREQ	Mensaje petición de supresión de la sesión (*session deletion request message*)
SDREQ	Mensaje de respuesta a una supresión de la sesión (*session deletion response message*)
SJREQ	Mensaje petición de adhesión a la sesión (*session join request message*)
SJRES	Mensaje respuesta a la adhesión a la sesión (*session join response message*)
SRACC	Mensaje aceptación de registro en la sesión (*session registration accept message*)
SRREJ	Mensaje rechazo de registro en la sesión (*session registration reject message*)
SRREQ	Mensaje petición de registro en la sesión (*session registration request message*)
SRRES	Mensaje de respuesta al registro en la sesión (*session registration response message*)

4.1.2 Tipos de mensajes de gestión de miembros

KAREQ	Mensaje petición de actividad (*keepalive request message*)
KARES	Mensaje respuesta de actividad (*keepalive response message*)
KDUPT	Mensaje actualización de la distribución de claves (*key distribution update message*)
LVREQ	Mensaje petición de abandono (*leave request message*)
TRREQ	Mensaje petición de terminación (*termination request message*)
TRIND	Mensaje indicación de terminación (*termination indication message*)
UIREQ	Mensaje petición de información de usuario (*user information request message*)
UIRES	Mensaje respuesta a la información de usuario (*user information response message*)

4.2 Varios

ECTP	Protocolo perfeccionado de transporte de comunicaciones (*enhanced communications transport protocol*)
ECTS	Servicio de transporte de comunicaciones potenciadas (*enhanced communications transport service*)
IP	Protocolo Internet (*Internet protocol*)
LQA	Calidad más baja admisible (*lowest quality allowed*)
MM	Gestión de miembros (*membership management*)
MSS	Tamaño máximo de segmento (*maximum segment size*)
OT	Objetivo operativo (*operating target*)
QoS	Calidad de servicio (*quality of service*)
RMT	Transporte multidifusión seguro (*reliable multicast transport*)
RSVP	Protocolo de reserva de recursos (*resource reservation protocol*)
SAP	Protocolo de anuncio de sesión (*session announcement protocol*)
SDP	Protocolo de descripción de sesión (*session description protocol*)
SM	Gestión de sesión (*session management*)

5 Convenios

En esta Recomendación | Norma Internacional, los niveles de obligación se interpretarán de acuerdo con la RFC 2119 del IETF, en la que se indican los niveles de obligación de las implementaciones del ECTP conformes. Se hace distinción entre mayúsculas y minúsculas.

6 Consideraciones generales

El GMP es un protocolo de control de la capa de aplicación para la creación de sesiones de grupo y la gestión de los miembros que participan en los mismos.

Por lo general, se supone que hay un servidor GMP, un cliente que crea la sesión (o creador de sesión), y uno o varios clientes que participan en la sesión (o participantes en la sesión) como se muestra en la figura 2.

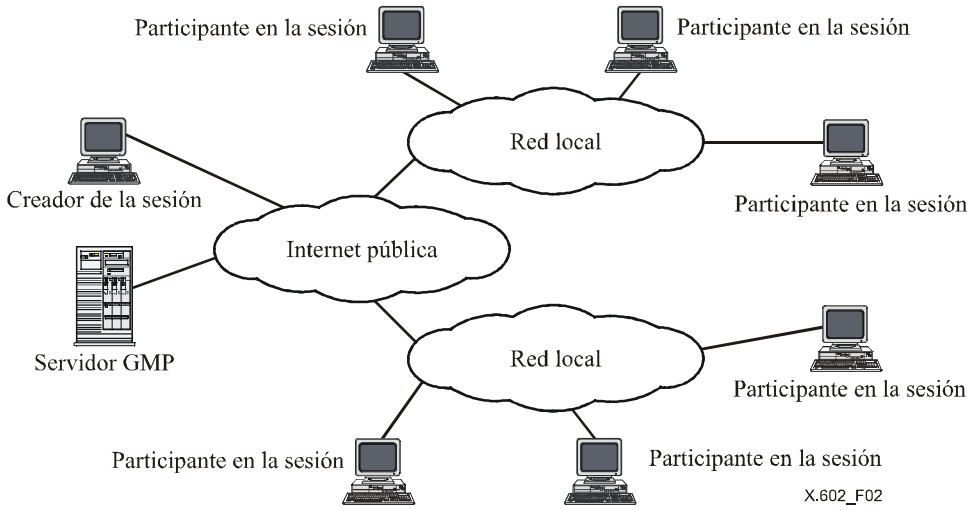

Figura 2 – Configuración de red para el GMP

El GMP está formado por la gestión de sesión (SM), la gestión de miembros (MM) y la función del intercambio de información entre SM y MM.

6.1 Gestión de sesión

La gestión de sesión (SM) se lleva a cabo en ocho fases distintas: creación, anuncio, registro, inscripción, activación, desregistro, desinscripción y desactivación.

Un determinado cliente, a saber, el creador de la sesión, crea la sesión en la SM, y ésta actualiza la lista de sesiones.

El creador de la sesión envía un mensaje de petición de creación de la sesión al servidor. Si la creación se acepta, el creador de la sesión recibe el mensaje de aceptación de creación de la sesión procedente del servidor. A continuación, el creador de la sesión envía la información detallada sobre la sesión hacia el servidor y recibe el mensaje de confirmación. Si la sesión no puede crearse o el creador de la sesión no tiene los derechos adecuados, se devuelve el mensaje petición de creación de sesión.

Una vez se ha creado con éxito la sesión, el servidor anuncia la nueva sesión a los clientes. El anuncio puede hacerse por correo electrónico, en una página web, etc. A partir de este momento esos clientes podrán ser miembros de un grupo multidifusión.

Los clientes pueden registrarse en una sesión. En el modo abierto, todos los clientes pueden registrarse en la sesión, pero en modo cerrado sólo algunos pueden registrarse en la sesión, a saber, aquellos a los que se haya autorizado previamente. Una vez completado con éxito el registro, el cliente pertenece al grupo registrado.

Cuando se inicia la sesión, los miembros registrados en la sesión inician una aplicación de grupo para enviar y recibir datos correspondientes a esa sesión. En ese momento se llevan a cabo todos los preparativos para la transferencia de datos y la gestión de grupo. El miembro de grupo registrado en la sesión pasa a formar parte del grupo de inscritos.

Cuando el creador de la sesión envía datos reales o los miembros inscritos en la sesión reciben datos reales, se dice que estos participantes están en el estado activo. Se habrá de activar la gestión de miembros.

6.2 Gestión de miembros

Cuando una sesión está activada, el servidor envía inmediatamente una petición de informe de estado a cada miembro activo de la sesión. El servidor actualiza la lista de miembros activos y demás información a partir de la información recibida de los participantes. Esta actualización se lleva a cabo periódicamente.

Para abandonar la sesión, el participante envía un mensaje abandono al servidor.

Para terminar la sesión en curso, el creador de la sesión envía un mensaje de terminación de la sesión al servidor, el cual se encarga de notificar la terminación de la sesión a cada participante y de terminarla.

En la figura 3 se muestra un ejemplo del funcionamiento del GMP y la relación entre el estado de la sesión y las fases de grupo multidifusión definidos en la Rec. UIT-T X.601.

Como se muestra en la figura, una vez creada y anunciada la sesión, los tres clientes A, B y C de la sesión tratan de registrarse en la misma. Sin embargo, el cliente C se rechaza por no estar autorizado o no tener los derechos adecuados. Cuando el creador de la sesión y los clientes envían al servidor la petición de adhesión a la sesión, pasan al estado inscritos. A partir de este momento ya pueden entablar la comunicación entre ellos. Cuando envían al servidor el mensaje de petición de activación, pasan al estado activo. La gestión de miembros (MM) clasifica a los miembros de acuerdo con ese mensaje, los cuales se encuentran en el estado activo o inscrito. El servidor actualiza la lista de miembros activos de acuerdo con las peticiones y respuestas de actualización periódicas. El participante en la sesión A abandona la sesión, para lo cual envía el mensaje abandono al servidor. A partir de ese momento para actualizar la lista de miembros activos el servidor envía la petición de actualización únicamente a los participantes activos. Cuando el creador de la sesión desea terminarla, envía una petición de terminación de sesión al servidor, el cual se encarga de notificarlo a los participantes en la sesión.

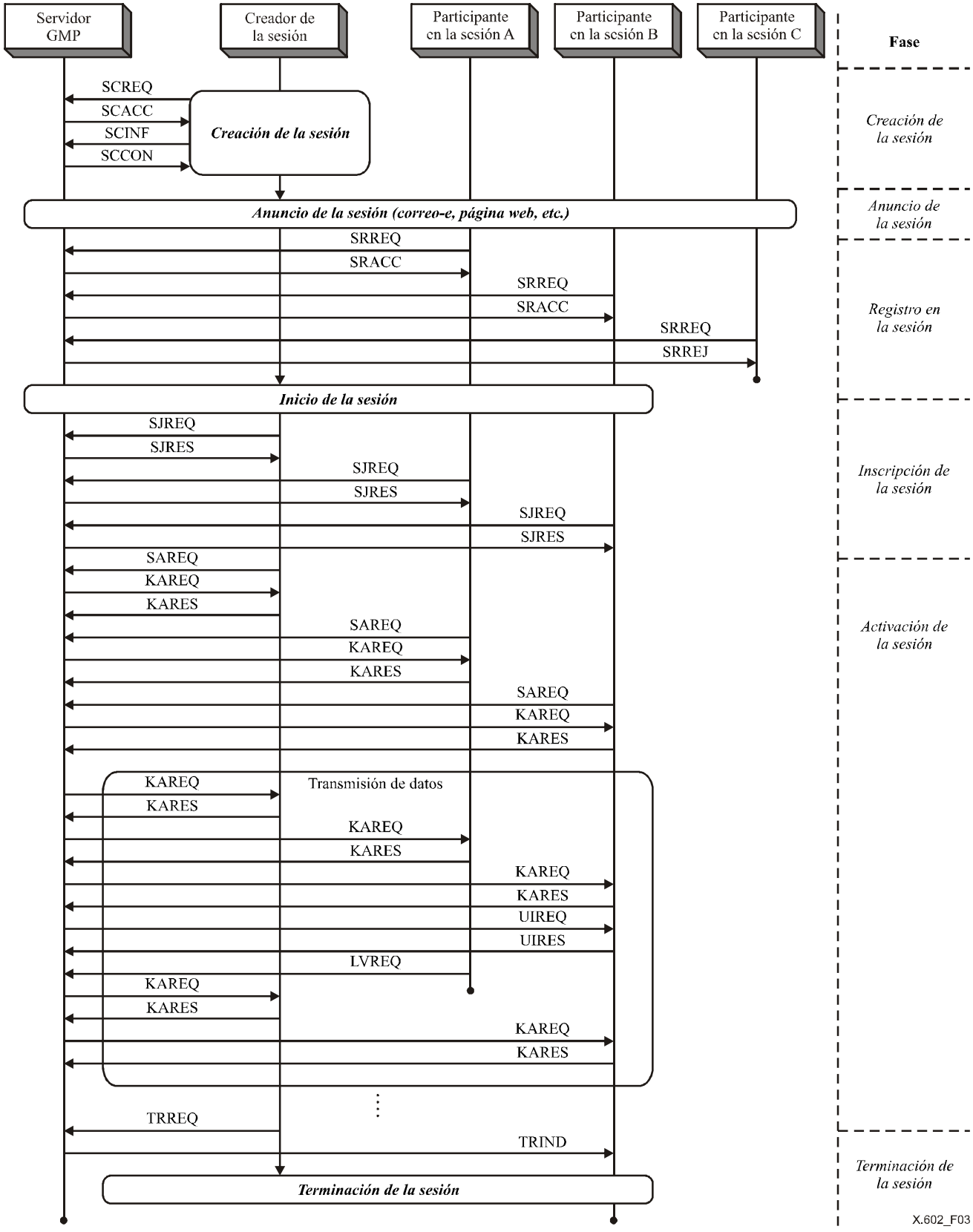

Figura 3 – Ejemplo de control GMP

7 Funcionamiento del protocolo

7.1 Gestión de sesión

La gestión de sesión (SM) se lleva a cabo en ocho fases distintas: creación, anuncio, registro, inscripción, activación, desregistro, desinscripción y desactivación.

La gestión de la sesión se encarga de lo siguiente:

a) Creación de la sesión: El creador de la sesión crea la sesión.

b) Anuncio de sesión: Normalmente, el servidor SM anuncia la sesión relativa a la sesión a los clientes de la misma.

c) Registro en la sesión: Los clientes se registran en una sesión a través del servidor SM.

d) Inscripción a la sesión: Una vez registrado, la función de inscripción lleva a cabo toda la "configuración" necesaria para la comunicación del grupo multidifusión.

e) Activación de la sesión: Tras la activación, los participantes en la sesión reciben los datos del creador de la sesión. Los participantes en la sesión pasan a formar parte del grupo activo.

La sesión puede ser de dos modos:

a) modo cerrado;

b) modo abierto.

En el modo cerrado, el creador de la sesión puede limitar la participación en la misma y distribuir los mensajes de control de acceso a los participantes destinatarios. Los participantes podrán registrarse en la sesión una vez concluido el proceso de autorización. En el modo abierto, cualquier cliente puede registrarse en la sesión.

7.1.1 Creación de la sesión

La sesión la crea el creador de la sesión, quien define y caracteriza la sesión en lo que respecta al tipo de medios, tipo de aplicación, información adicional, etc.

El creador de la sesión puede definir miembros principales, que deben estar registrados o inscritos. Si los miembros principales no se han inscrito o registrado, la sesión no podrá comenzar.

En la figura 4 se muestra el procedimiento de creación de sesión aceptada. El creador de la sesión define y caracteriza la sesión y envía al servidor de sesión un mensaje de petición de creación de sesión, SCREQ. El mensaje SCREQ sirve solamente para preguntar si la sesión puede crearse o no. En función del entorno multidifusión y su aplicación, el servidor podrá permitir la creación de una nueva sesión, para lo cual responderá con un mensaje aceptación de creación de la sesión, SCACC. A continuación, el creador de la sesión envía la información detallada de la misma en el mensaje información de creación de la sesión, SCINF, en el que puede incluir el tipo de medios, tipo de aplicación, etc. El servidor acusa recibo de la creación de sesión aceptada mediante el mensaje de confirmación de creación de sesión, SCCON, y actualiza la lista de sesiones.

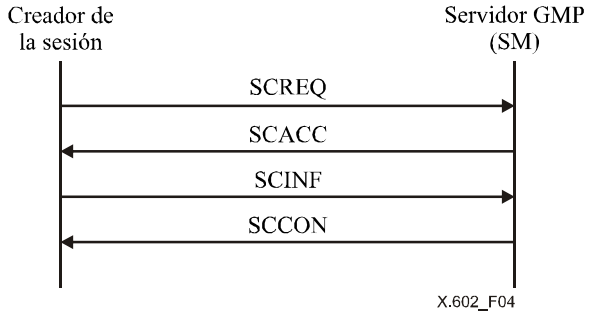

Figura 4 – Procedimiento de creación de la sesión aceptada

En la figura 5 se muestra el procedimiento de creación de la sesión rechazada. Cuando el creador de la sesión solicita la creación de una nueva sesión al servidor, y éste no dispone de recursos suficientes o el creador no tiene la autorización adecuada, el servidor la rechazará, para lo cual enviará el mensaje rechazo de creación de sesión, SCREJ.

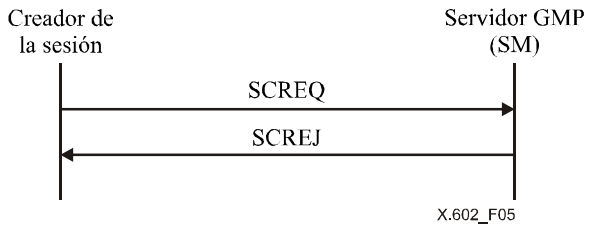

Figura 5 – Procedimiento de creación de sesión rechazada

7.1.2 Anuncio de la sesión

La sesión se anuncia por correo electrónico, en una página web o por otros medios no electrónicos. Los clientes se enterarán por ese anuncio de la existencia y de las características de todas las sesiones creadas. Los participantes en la sesión podrán saber si la sesión es de modo abierto o cerrado. En el modo cerrado se deben distribuir los mensajes de control de acceso a los clientes seleccionados por el creador de la sesión, los cuales utilizarán los clientes para acceder a la información de la sesión y registrarse a la sesión cerrada ulteriormente.

7.1.3 Registro en la sesión

El registro en la sesión consiste en seleccionar una sesión e informar al servidor y al creador que se desea participar en la misma.

En la sesión de modo abierto, el cliente selecciona una sesión y envía el mensaje de petición de registro en la sesión, SRREQ, al servidor. El servidor añade el cliente a la lista de miembros de grupos registrados, y responde al cliente con un mensaje aceptación de petición de sesión, SRACC, como se muestra en la figura 6.

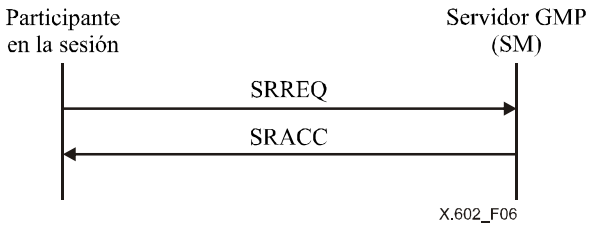

Figura 6 – Procedimiento de registro en la sesión aceptado (modo abierto)

En la sesión de modo cerrado el cliente selecciona una sesión y envía al servidor el mensaje petición de registro en la sesión, SRREQ. El servidor responde inmediatamente con el mensaje respuesta de registro en la sesión, SRRES, para indicar que procede a comprobar la autorización. Si el registro es válido, el servidor envía un mensaje de aceptación de registro de sesión, SRACC, como se muestra en la figura 7.

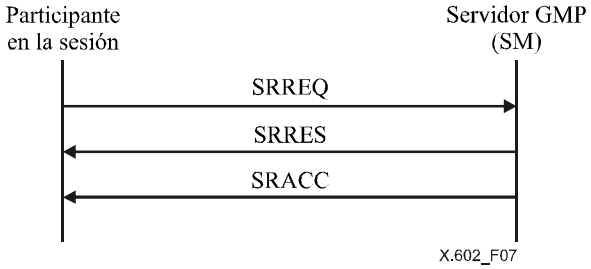

Figura 7 – Procedimiento de registro de sesión aceptado (modo cerrado)

Si el cliente que solicita el registro en la sesión no está autorizado en la sesión en modo cerrado, el servidor envía el mensaje rechazo de registro de sesión, SRREJ, como se muestra en la figura 8.

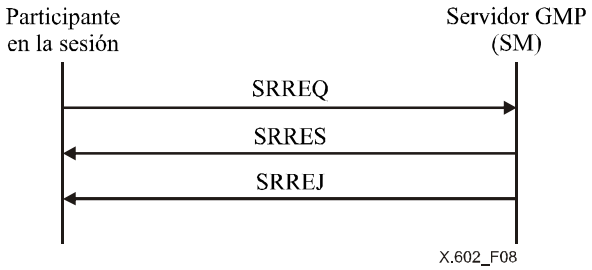

Figura 8 – Procedimiento de registro en la sesión rechazado (modo cerrado)

7.1.4 Inscripción en la sesión

La inscripción en la sesión es el estado en el que ya es posible la comunicación entre los participantes en la sesión y el creador de la misma. Los participantes en la sesión, incluido el creador de ésta, deben enviar el mensaje petición de adhesión a la sesión, SJREQ. El servidor añade a los participantes a la lista de miembros de grupo inscritos, y responde al solicitante con un mensaje respuesta de adhesión a la sesión, SJRES, como se muestra en la figura 9.

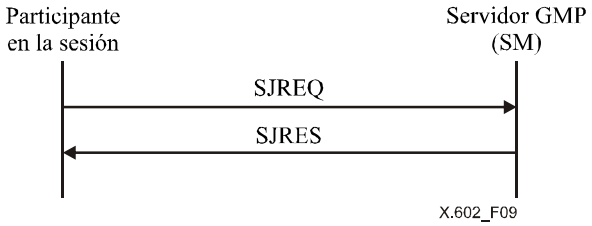

Figura 9 – Inscripción en la sesión aceptada

La MM mantiene por separado una lista de los miembros del grupo registrados y una lista de los miembros del grupo inscritos.

7.1.5 Activación de la sesión

La activación de la sesión es el estado en que los participantes en la sesión y el creador de ésta están transfiriendo datos. Los participantes en la sesión, incluido el creador de la misma, deben enviar el mensaje petición de activación de la sesión, SAREQ. El servidor responderá con el mensaje de petición de actividad, KAREQ. Si el servidor recibe el mensaje de respuesta de actividad, KARES, procedente de los participantes en la sesión, procederá a actualizar la lista de miembros del grupo activos, como se muestra en la figura 10.

El servidor mantiene una lista de miembros de grupos activos gracias al intercambio periódico de mensajes KAREQ y KARES.

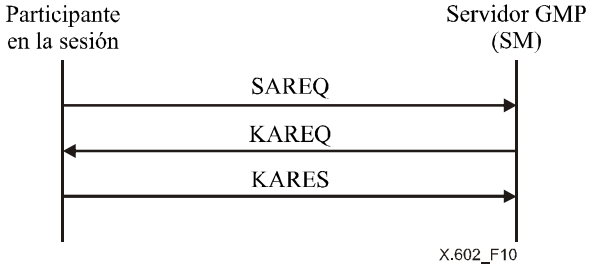

Figura 10 – Activación de la sesión aceptada

En el caso en el que un usuario desea sumarse a una sesión en curso, el participante que se encuentra en el estado inscrito envía el mensaje SAREQ para sumarse a una sesión en curso.

Si el participante en la sesión envía el mensaje KARES después de recibir KAREQ, el servidor añadirá este participante a la lista de miembros del grupo activos.

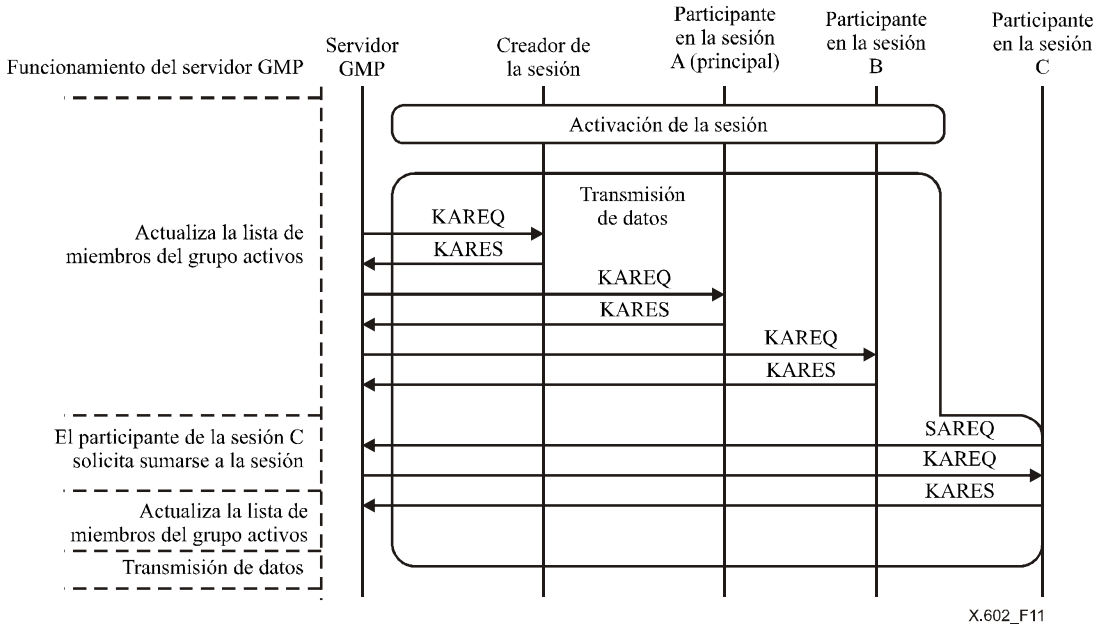

Figura 11 – Procedimiento para sumarse a una sesión en curso

7.2 Gestión de miembros

La gestión de miembros (MM) se encarga del mantenimiento y una gestión de los miembros de grupo activos.

En la figura 12 se ilustra el algoritmo de actualización de la lista de miembros que lleva a cabo la gestión de miembros en el servidor GMP. Tras recibir el mensaje KARES de los participantes en la sesión, el servidor de gestión de miembros GMP comprueba si el cliente forma parte de la lista del grupo de registrados. De ser así, el servidor comprueba si el cliente pertenece al grupo de inscritos, y si no forma parte del mismo lo añade. Si, por el contrario, ya forma parte del grupo de inscritos, el servidor GMP comprueba si el cliente forma parte del grupo de activos. Si no forma parte del mismo, lo añade al grupo de activos y reinicia el temporizador de actividad (o temporizador KA). Si, por el contrario, el cliente ya pertenece al grupo de activos, el servidor reinicia el temporizador de actividad o KA y espera la recepción del siguiente KARES.

Si el servidor GMP no recibe el mensaje KARES procedente del participante en la sesión y el temporizador KA correspondiente a ese participante expira, el servidor de gestión de miembros GMP comprueba a qué grupo pertenece el participante en la sesión. Si el participante en la sesión forma parte del grupo de activos, lo moverá al grupo de inscritos. Si, por el contrario, pertenece al grupo de inscritos, el participante se moverá al grupo de registrados. Seguidamente, el servidor GMP reiniciará el temporizador KA.

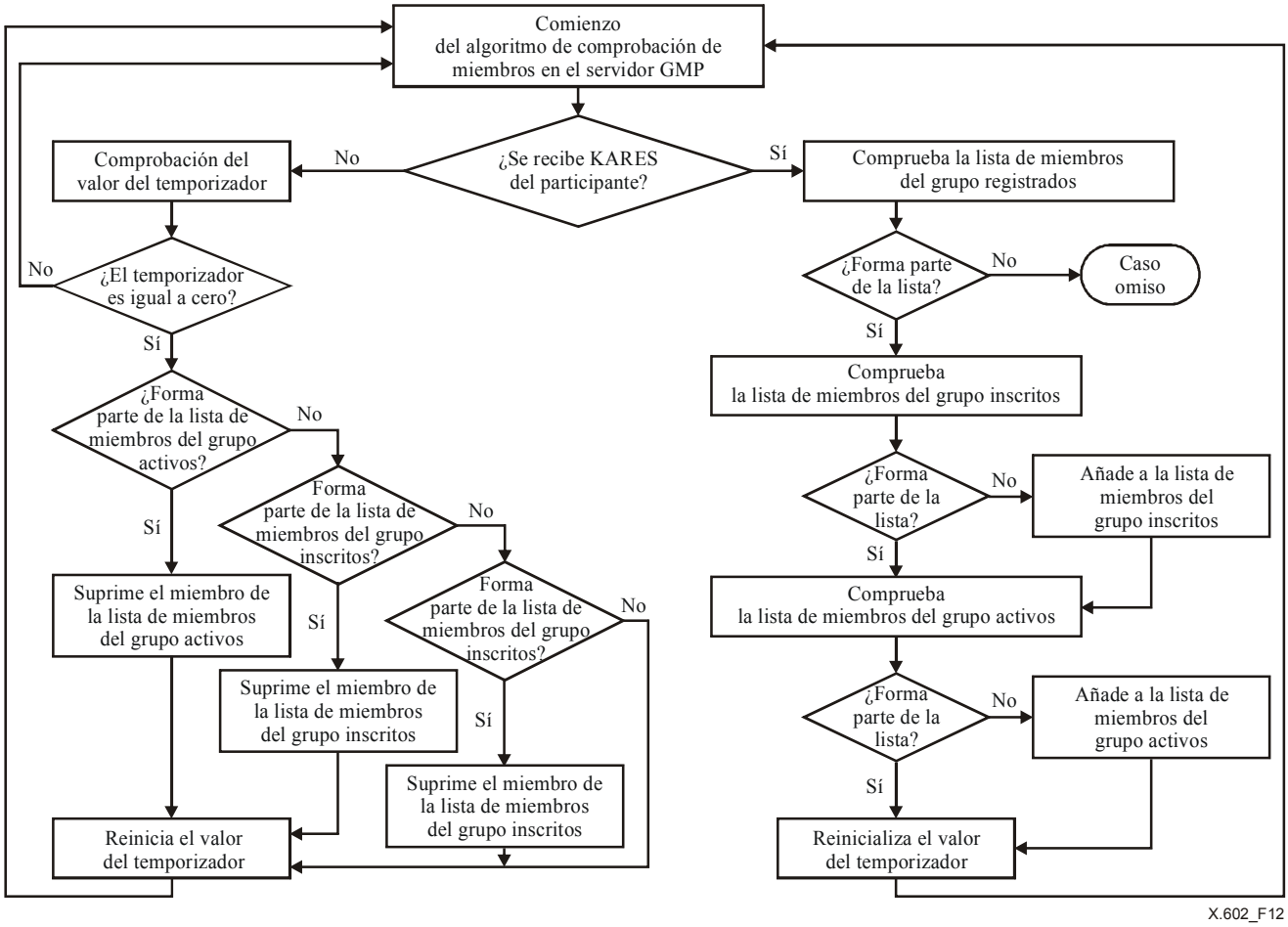

Figura 12 – Algoritmo de comprobación de miembros en el servidor

La figura 13 ilustra el proceso de recepción de mensajes de gestión de miembros en el servidor GMP.

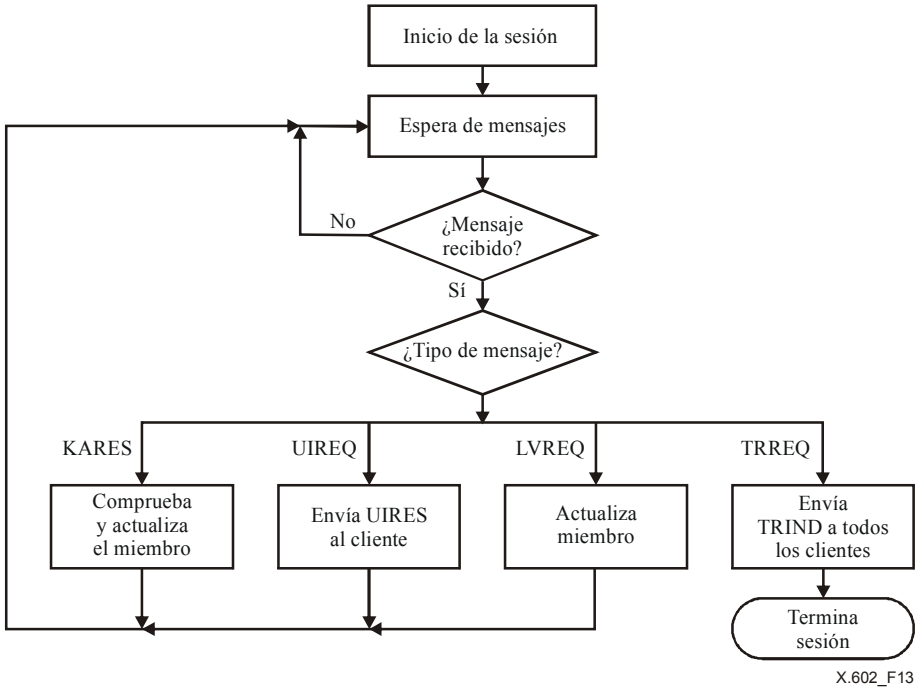

Figura 13 – Algoritmo de funcionamiento (MM) del servidor GMP

La figura 14 ilustra el proceso de envío de mensajes de gestión de miembros en el cliente.

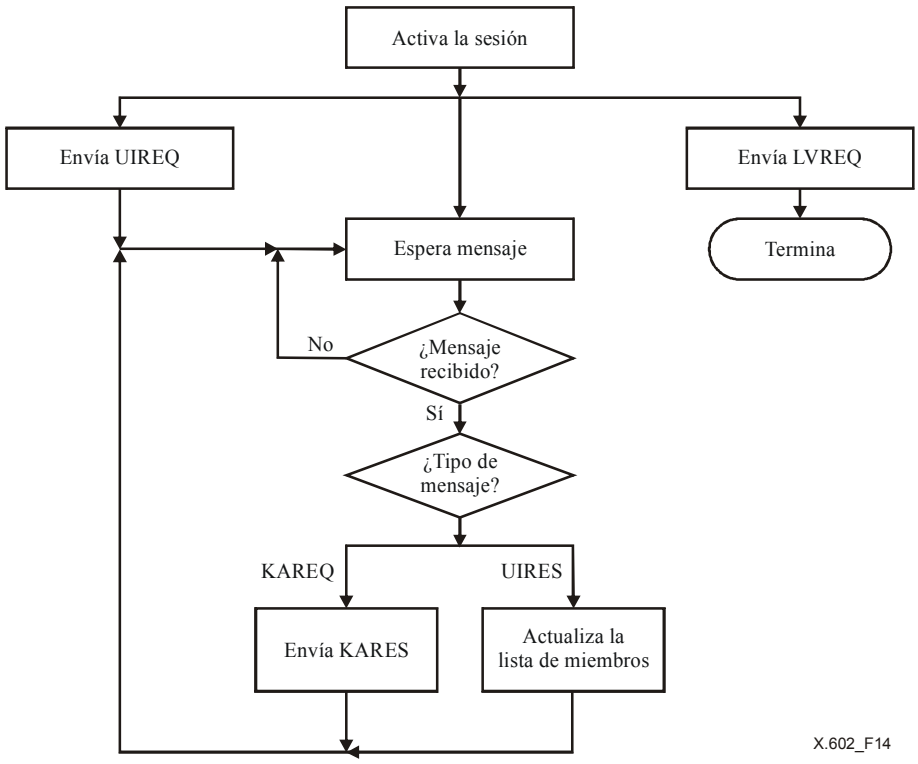

Figura 14 – Algoritmo de funcionamiento del cliente MM

7.2.1 Actualización de miembros

7.2.1.1 Modo abierto

El servidor envía periódicamente el mensaje KAREQ a todos los participantes en la sesión activa. Sin embargo, el servidor mantiene la información de estado de los miembros principales y del creador de la sesión de acuerdo con los KARES recibidos, mientras que los participantes distintos de los activos podrá contarlos basándose en los mensajes KARES recibidos o simplemente hace caso omiso de éstos, como se muestra en la figura 15.

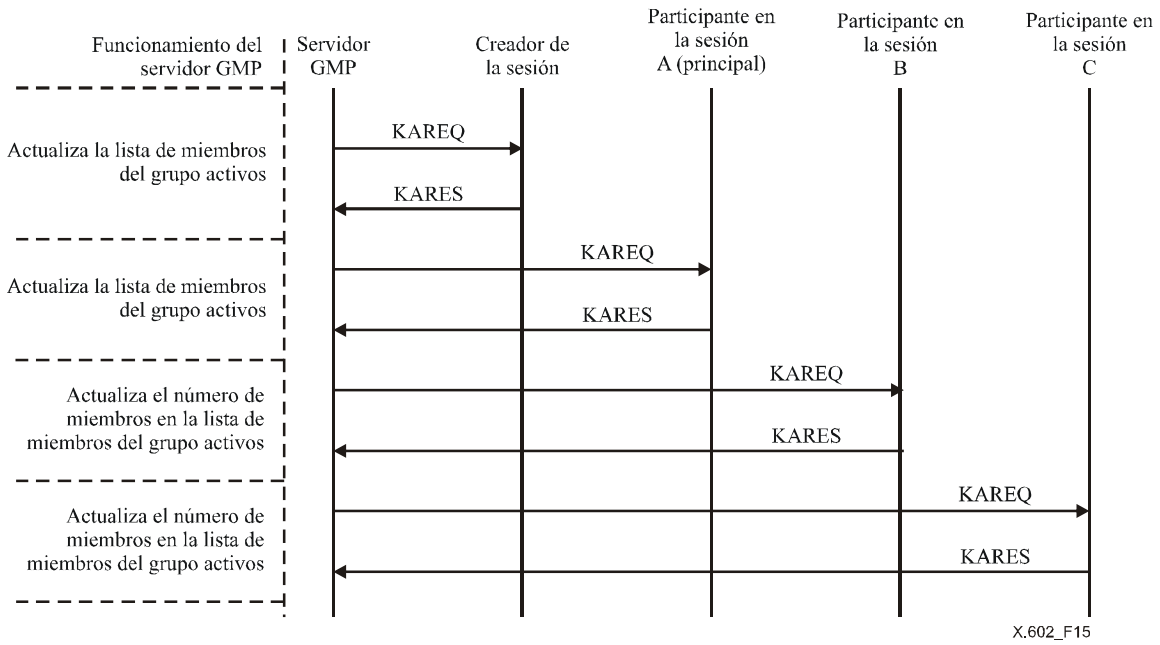

Figura 15 – Procedimiento de informe de estado (modo abierto)

Todo participante en la sesión puede solicitar la lista de miembros del grupo activos al servidor.

En la figura 16 se muestra el caso de la terminación de sesión: si el servidor GMP no recibe un mensaje KARES válido procedente del creador de la sesión y de los miembros principales de la sesión antes de que expire el temporizador KA predefinido, el servidor notificará que la sesión se está terminando mediante el mensaje indicación de terminación, TRIND, y a continuación terminará la sesión.

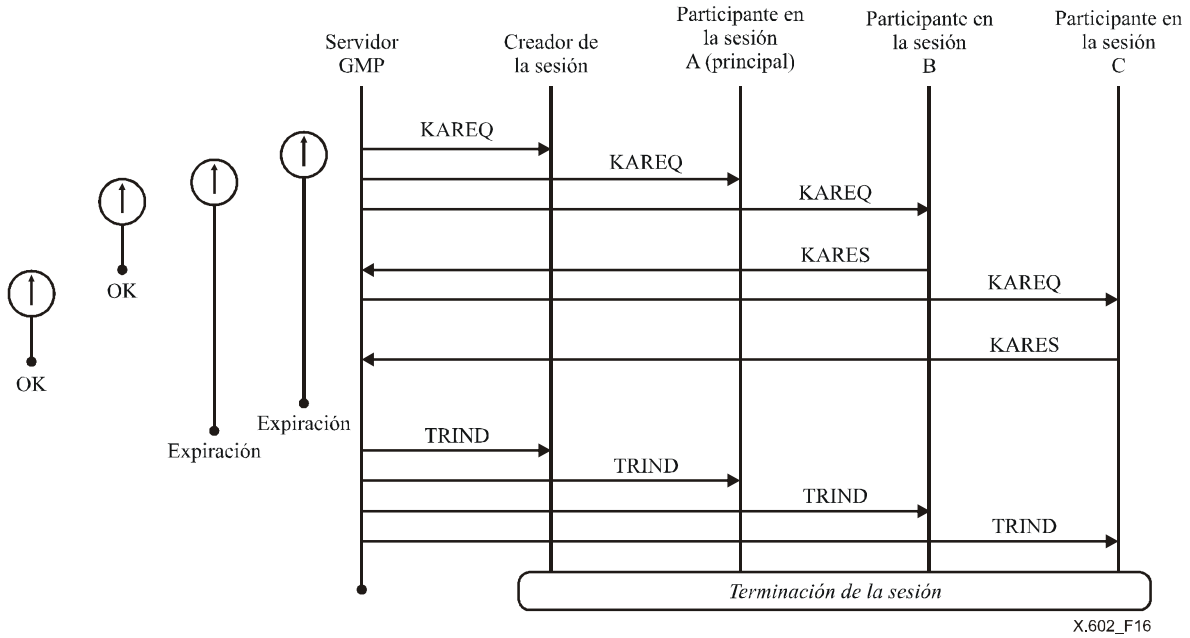

Figura 16 – Terminación de la sesión (modo abierto)

7.2.1.2 Modo cerrado

El servidor envía periódicamente el mensaje KAREQ a todos los participantes activos en la sesión. Mantiene la información de estado de todos los miembros activos incluidos los miembros principales y el creador de la sesión a partir de los mensajes KARES recibidos, como se muestra en la figura 17.

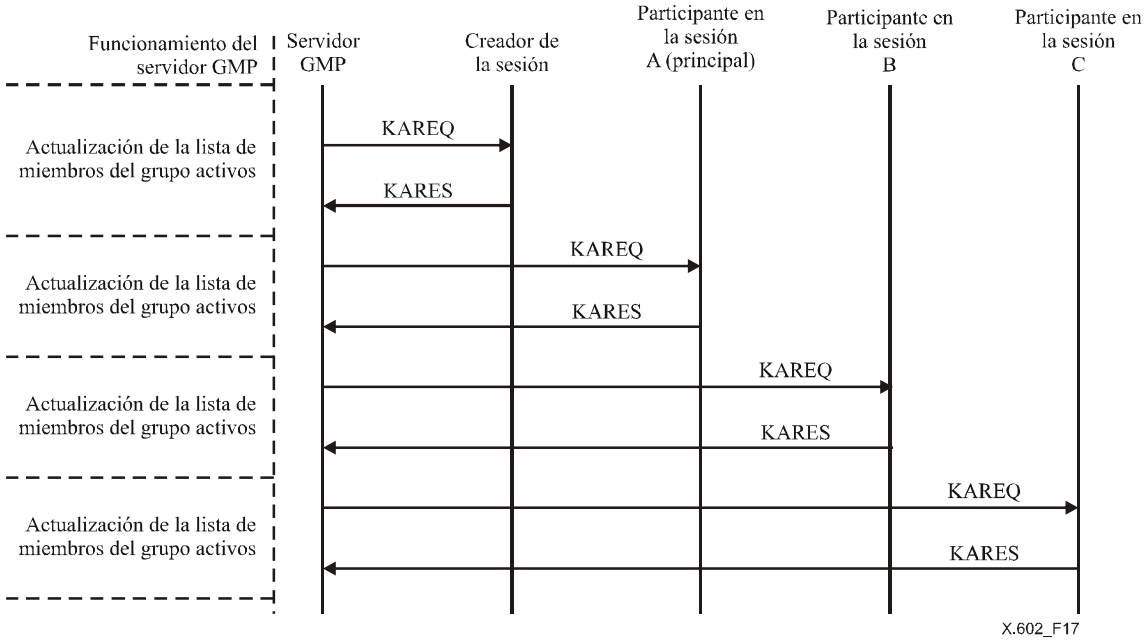

Figura 17 – Procedimiento para comunicar el estado (modo cerrado)

Todo participante en la sesión puede solicitar al servidor la lista de miembros de grupo activos.

7.2.2 Petición y respuesta de información de usuario

El miembro de grupo activo puede solicitar al servidor GMP la lista de miembros de grupo activos, para lo cual envía el mensaje UIREQ. El servidor GMP responde al UIREQ con el mensaje UIRES en el que incluye la lista de miembros del grupo activos, como se muestra en la figura 18.

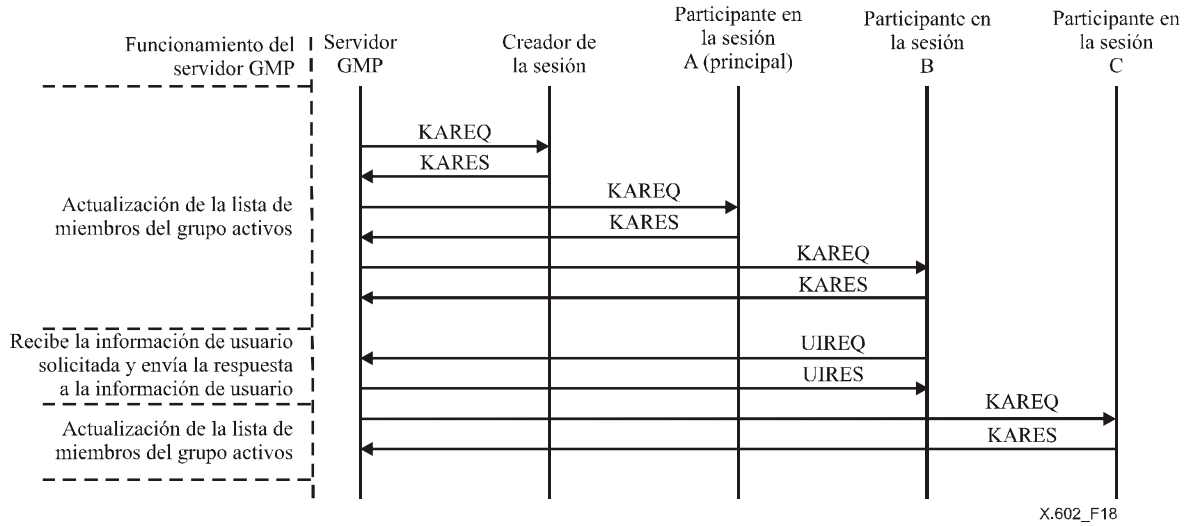

Figura 18 – Mensajes UIREQ y UIRES

7.2.3 Abandono de sesión

Normalmente, cuando un participante en la sesión activo desea abandonar la sesión envía LVREQ al servidor GMP, éste suprime al cliente de la lista de miembros del grupo activos y añade el cliente a la lista de miembros del grupo inscritos, como se muestra en la figura 19.

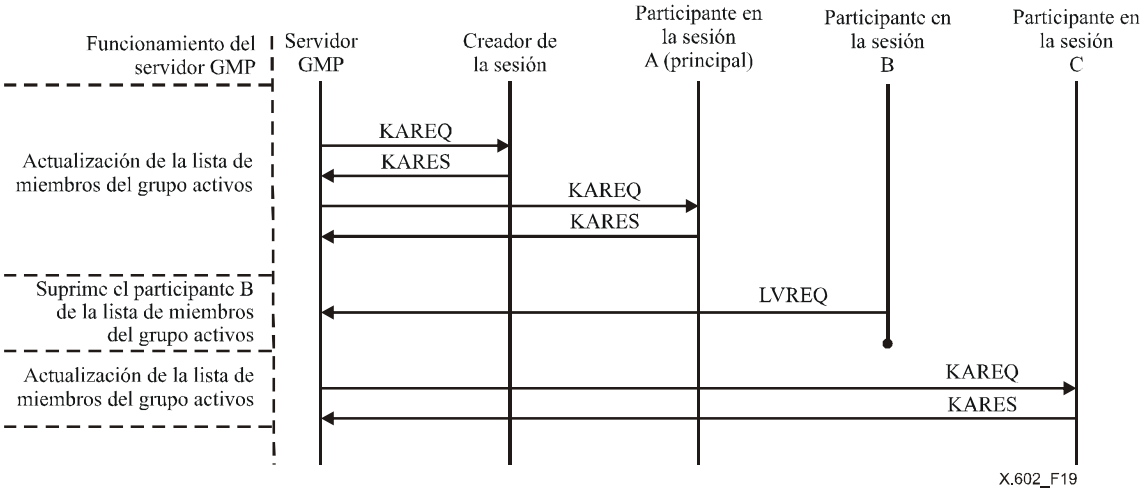

Figura 19 – Mensajes LVREQ

Ahora bien, cuando el participante en la sesión activo que abandona la sesión es el creador de la sesión o el miembro principal de la sesión, y envía el mensaje LVREQ, el servidor GMP que recibe este mensaje terminará la sesión, y enviará TRIND a cada uno de los participantes activos en la sesión, como se muestra en la figura 20.

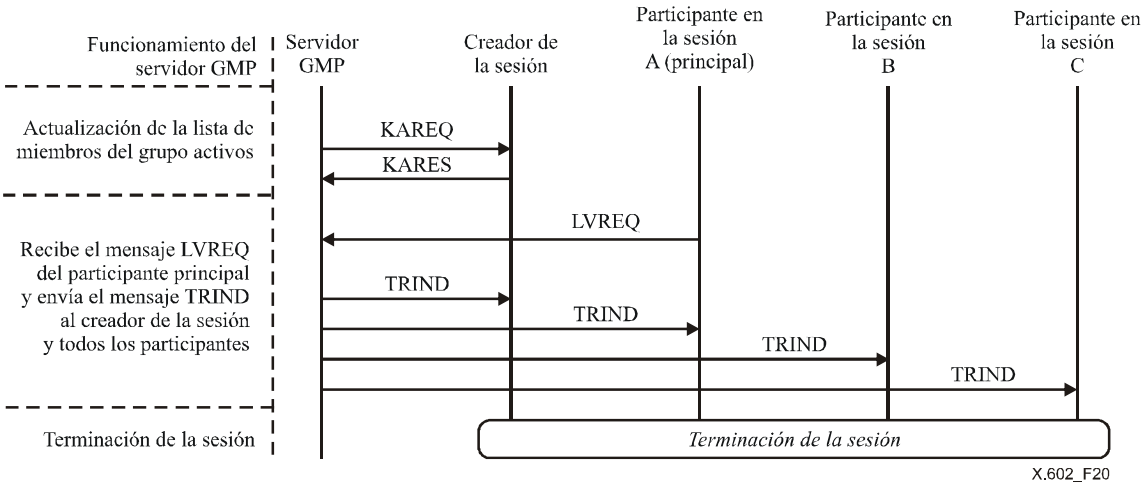

Figura 20 – Mensajes LVREQ que envía el participante principal

7.2.4 Terminación de la sesión

Para terminar una sesión, el creador de la sesión envía el mensaje TRREQ al servidor GMP. El servidor GMP que recibe el mensaje TRREQ termina la sesión, para lo cual envía el mensaje TRIND a cada participante en la sesión activo, como se muestra en la figura 21.

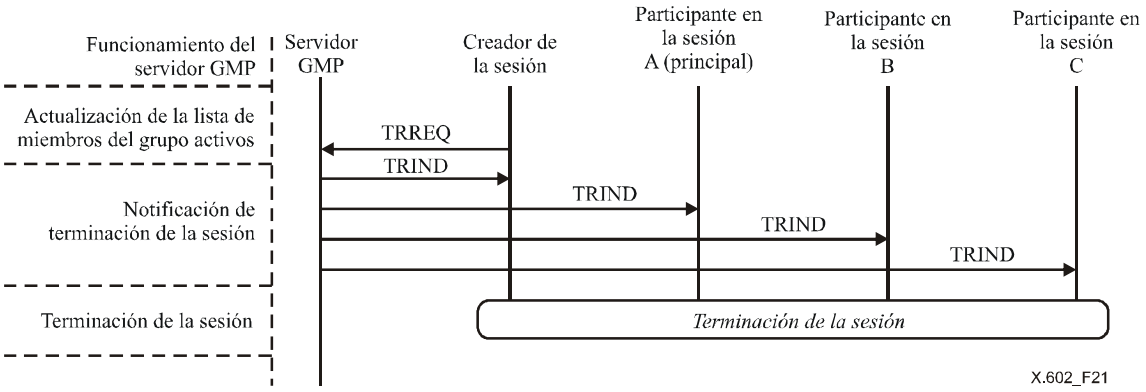

Figura 21 – Terminación de la sesión

Tras enviar KAREQ, el servidor GMP activa el temporizador de mantenimiento de la conexión, y si este temporizador expira antes de que se hayan recibido uno o varios KARES de respuesta procedentes de los miembros activos principales, el servidor GMP termina la sesión y envía el mensaje TRIND a cada participante en la sesión activo, como se muestra en la figura 22.

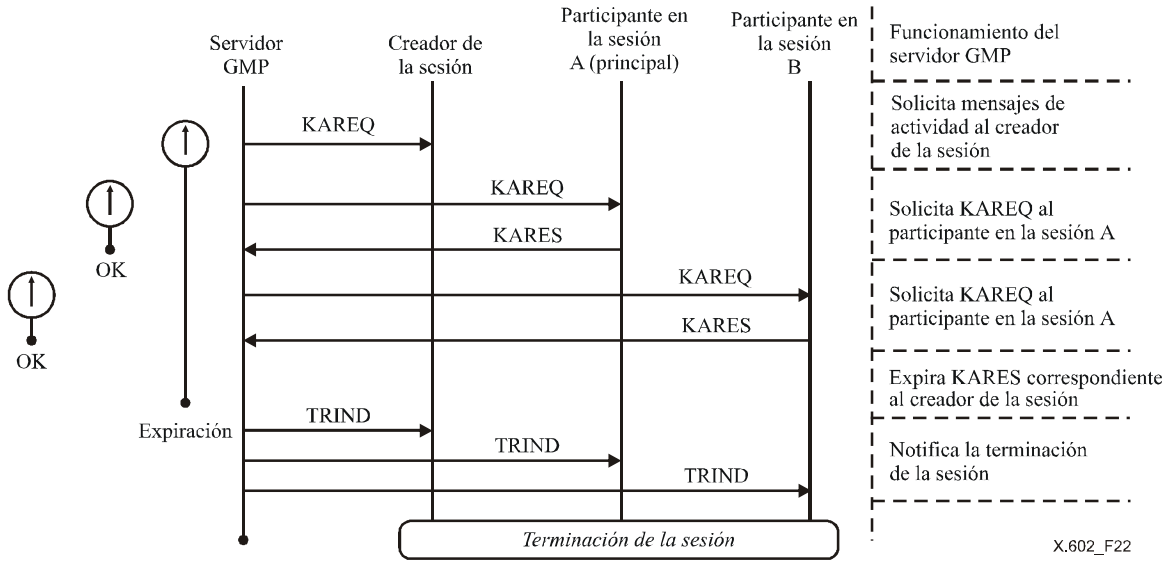

Figura 22 – Terminación de la sesión

7.3 Seguridad

El GMP utiliza la distribución de claves para aplicar la seguridad al protocolo de gestión de grupo. En la figura 23 se ilustra un ejemplo de control GMP para la seguridad del GMP.

Si el creador de la sesión desea crear una sesión tomando medidas de seguridad, el creador de la sesión envía SCREQ con el bit 'S' puesto a UNO al servidor GMP. Si el creador de la sesión solicita crear una sesión con medidas de seguridad, y el servidor GMP no soporta el modo seguro para una sesión, este servidor envía SCREJ con el bit "S" puesto a UNO al creador de la sesión.

Si el servidor GMP soporta el modo seguro para una sesión, el participante en la sesión recibe el mensaje SJRES con el bit 'S' puesto a UNO, que incluirá la clave en la fase de inscripción.

Si un participante en la sesión se inscribe o se suma más tarde a una sesión en curso, el servidor GMP envía el mensaje SJRES con el bit 'S' puesto a UNO en el que incluye la clave que se está utilizando en ese momento en la sesión.

Siempre que un participante en la sesión se desinscribe, el servidor GMP descarta la clave, genera una nueva clave y envía el mensaje KDUPT en el que incluye la clave a todos los miembros del grupo inscritos.

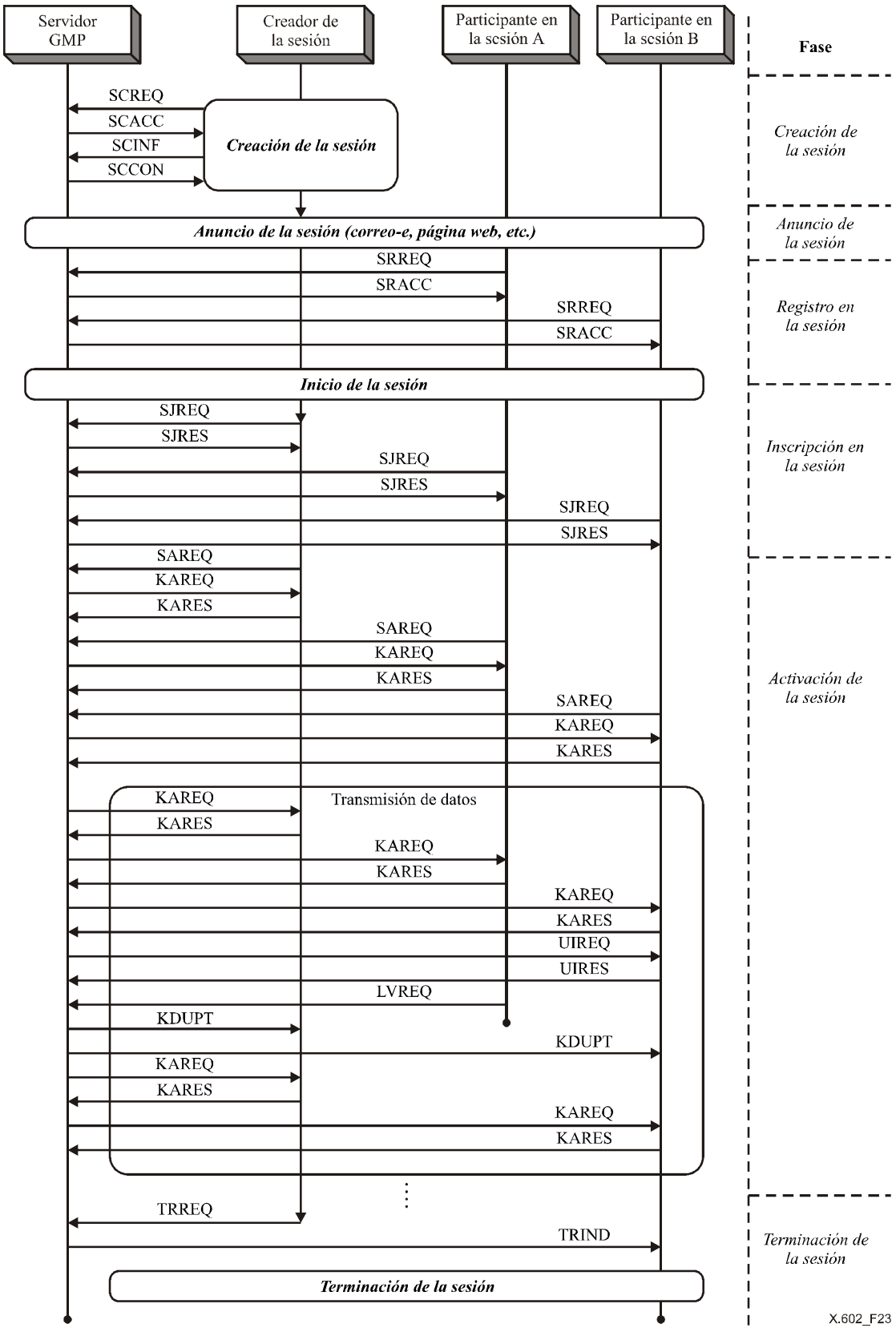

Figura 23 – Ejemplo de control del GMP (modo con seguridad)

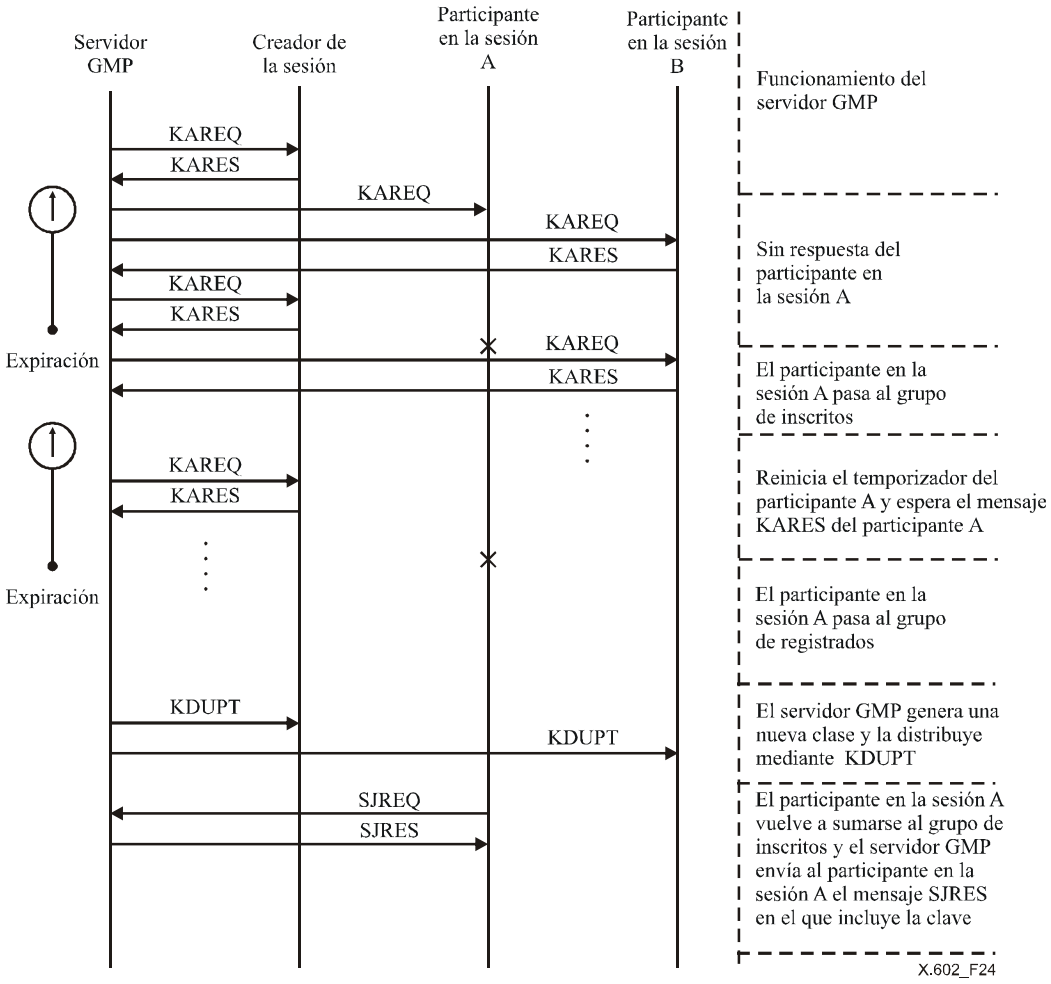

Figura 24 – Distribución de claves utilizando el mensaje KDUPT

8 Mensajes GMP

Los mensajes GMP se clasifican en mensajes de gestión de sesión y mensajes de gestión de miembros.

8.1 Tipos de mensaje de gestión de sesión

En el cuadro 1 se resumen los mensajes y su descripción que se utilizan para la gestión de sesiones GMP.

Cuadro 1 – Tipos de mensaje de gestión de sesión

Tipo de mensaje	Generado por	Descripción
SCREQ	Creador de la sesión	Mensaje de petición de creación de sesión
SCACC	Servidor GMP (SM)	Mensaje aceptación de creación de sesión
SCREJ	Servidor GMP (SM)	Mensaje de rechazo de la petición de creación de sesión
SDREQ	Creador de la sesión	Mensaje petición de supresión de sesión
SDRES	Servidor GMP (SM)	Mensaje de respuesta a la supresión de sesión
SCINF	Creador de la sesión	Mensaje de información de creación de sesión
SCCON	Servidor GMP (SM)	Mensaje de confirmación de la información de la creación de sesión
SRREQ	Creador de la sesión Participante en la sesión	Mensaje de petición de registro en la sesión
SRACC	Servidor GMP (SM)	Mensaje de aceptación de registro en la sesión
SRREJ	Servidor GMP (SM)	Mensaje de rechazo de registro en la sesión
SRRES	Servidor GMP (SM)	Mensaje de respuesta al registro en la sesión
SJREQ	Creador de la sesión Participante en la sesión	Mensaje de petición de adhesión a la sesión
SJRES	Servidor GMP (SM)	Mensaje de respuesta a la adhesión a la sesión
SAREQ	Creador de la sesión Participante en la sesión	Mensaje de petición de activación de la sesión

a) SCREQ: Mensaje que genera el creador de la sesión y envía al servidor GMP para que se le permita crear una nueva sesión.

b) SCACC: Mensaje que genera el servidor GMP y que envía al creador de la sesión para concederle el permiso de creación de la sesión.

c) SCREJ: Mensaje que genera el servidor GMP y que envía al creador de la sesión para indicarle que no le permite crear la sesión solicitada por las siguientes razones:

   – el servidor GMP no dispone de recursos suficientes;

   – el creador de la sesión no tiene la autorización necesaria para crear la sesión;

   – el creador de la sesión solicita al servidor GMP crear una sesión con medidas de seguridad, pero el servidor GMP no soporta el modo seguro para esa sesión.

d) SDREQ: Mensaje que genera el creador de la sesión para solicitar que se suprima una sesión existente de la lista de sesiones en el servidor GMP.

e) SDRES: Mensaje que genera el servidor GMP en respuesta al SDREQ.

f) SCINF: Mensaje que genera el creador de la sesión para informar al servidor GMP de las características de la sesión y sus criterios, por ejemplo el tipo de medios, aplicación, lista de medios principales, modo de sesión, etc.

g) SCCON: Mensaje que genera el servidor GMP en respuesta al SCINF y mediante el cual indica que la información sobre la sesión se ha almacenado correctamente en la lista de sesiones.

h) SRREQ: Mensaje que envían los clientes de sesión al servidor GMP para registrarse en una sesión.

i) SRACC: Mensaje que genera el servidor GMP y que envía a un cliente de la sesión para indicarle que se ha registrado correctamente en la sesión solicitada.

j) SRREJ: Mensaje que genera el servidor GMP y que envía al cliente de la sesión que solicitó registrarse. El registro podrá rechazar el registro si los clientes de la sesión no tienen las calificaciones adecuadas.

k) SRRES: En modo cerrado, mensaje que genera el servidor GMP y envía al cliente de la sesión que solicita registrarse, y mediante el cual indica que se está tramitando la petición de registro sobre la base de la autorización definida previamente.

l) SJREQ: Mensaje que generan y envían el creador de la sesión y los clientes en la sesión que se han registrado correctamente para indicar que se encuentran en el estado inscritos, y están preparados para entablar la comunicación.

m) SJRES: Mensaje que genera el servidor GMP en respuesta al SJREQ para indicar que se va a activar la sesión. Si la sesión soporta el modo seguro, el servidor GMP incluirá la clave en el mensaje SJRES.

n) SAREQ: Mensaje que generan y envían el creador de la sesión y los clientes en la sesión que se han inscrito satisfactoriamente para indicar que han pasado al estado activo y que están en línea. En este mensaje se incluye un número de puerto del cliente para iniciar la gestión de miembros en el campo opciones.

8.2 Formatos de los mensajes de gestión de la sesión

En la figura 25 se muestra la estructura de los mensajes de gestión de la sesión.

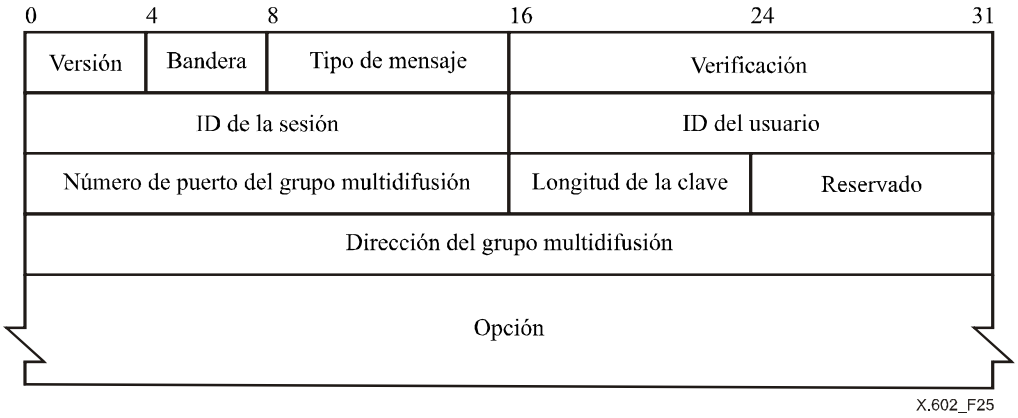

Figura 25 – Formato de mensaje de gestión de la sesión

La cabecera SM contiene la siguiente información:

a) Versión (4 bits) – Define la versión actual del protocolo GMP. Comienza en '1'.

b) Bandera (4 bits) – Bits de bandera. Dependiendo del tipo de mensaje, se utiliza para diferentes propósitos:

- I: Indica que el mensaje es SCINF cuando 'I = 1', el cual contiene el campo opción.
- M: Indica si el modo es abierto o cerrado.

  Modo cerrado: 'M = 1' Modo abierto: 'M = 0'
- S: Indica si el modo es seguro o no.

  Modo seguro: 'S = 1' Modo no seguro: 'S = 0'
- Q: Reservado para QoS.

3	2	1	0
Q	S	M	I

c) Tipo de mensaje (8 bits) – Indica el tipo de mensaje SM. En el cuadro 2 se resumen los tipos de mensaje y su codificación.

Cuadro 2 – Tipos de mensajes de gestión de sesión y su codificación

Tipo de mensaje	Codificación
SCREQ	0000 0001
SCACC	0000 0010
SCREJ	0000 0011
SDREQ	0000 0100
SDRES	0000 0101
SCINF	0000 0110
SCCON	0000 0111
SRREQ	0000 1000
SRRES	0000 1001
SRACC	0000 1010
SRREJ	0000 1011
SJREQ	0000 1100
SJRES	0000 1101
SAREQ	0000 1110
Reservado	0000 0000

d) Verificación (16 bits) – Verifica la validez del segmento del mensaje.

e) ID de la sesión (16 bits) – Identifica cada sesión.

f) ID del usuario (16 bits) – Identifica cada participante en la sesión. El ID del creador de la sesión y los demás participantes los asigna el servidor GMP en la fase de creación y registro, respectivamente.

g) Longitud de la clave (8 bits) – Valores de longitud de la clave en GMP en unidades de 8 bits.

h) Número de puerto del grupo multidifusión – Número de puerto para la comunicación del grupo multidifusión.

i) Dirección del grupo multidifusión – Dirección del grupo multidifusión.

j) Opción (32 bits × N).

- Este campo se adjunta al SCINF: Indica la información detallada de una nueva sesión.
- Este campo se adjunta al SJRES: Indica la clave del modo seguro.
- Este campo se adjunta al SAREQ: Indica el número de puerto del cliente para comenzar la gestión de miembros.

k) Reservado (8 bits) – Reservado.

8.3 Tipos de mensaje de gestión de miembros

En el cuadro 3 se resumen los mensajes y sus descripciones utilizados en la gestión de miembros GMP.

Cuadro 3 – Tipos de mensaje de gestión de miembros

Tipo de mensaje	Generado por:	Descripción
KAREQ	Servidor GMP (MM)	Mensaje petición de actividad
KARES	Creador de la sesión Participante en la sesión	Mensaje respuesta de actividad
UIREQ	Creador de la sesión Participante en la sesión	Mensaje de petición de información de usuario
UIRES	Servidor GMP (MM)	Mensaje respuesta a la información de usuario
LVREQ	Creador de la sesión Participante en la sesión	Mensaje de petición de abandono
TRREQ	Creador de la sesión	Mensaje de petición de terminación
TRIND	Servidor GMP (MM)	Mensaje indicación de terminación
KDUPT	Servidor GMP (MM)	Mensaje actualización de distribución de claves

a) KAREQ: Mensaje que genera el servidor GMP y que envía periódicamente a los participantes en la sesión activos para mantener la lista de miembros activos.

b) KARES: Mensaje que genera el participante en la sesión activo en respuesta al mensaje KAREQ para notificar el estado activo.

c) UIREQ: Mensaje que genera el cliente de la sesión activo y que envía al servidor GMP para solicitar la lista de miembros del grupo activos.

d) UIRES: Mensaje que genera el servidor GMP en respuesta al UIREQ en el que incluye la lista de miembros del grupo activos.

e) LVREQ: Mensaje generado por el participante en la sesión activo que envía al servidor GMP para notificar que abandona la sesión. El servidor GMP actualiza la lista de miembros del grupo activos y la lista de miembros del grupo inscritos.

f) TRREQ: Mensaje que genera el creador de la sesión y envía al servidor GMP para terminar la sesión que ha creado él mismo.

g) TRIND: Mensaje que genera el servidor GMP y envía a los participantes en la sesión activos para notificar que se va a dar fin a la sesión.

h) KDUPT: Mensaje que genera el servidor GMP y que envía a los participantes en la sesión activos y a los miembros del grupo inscritos para distribuir la clave.

8.4 Formatos de mensajes de gestión de miembros

En la figura 26 se muestra la estructura de los mensajes de gestión de miembros. El campo opción se emplea únicamente en el UIRES para enumerar los participantes en la sesión activos.

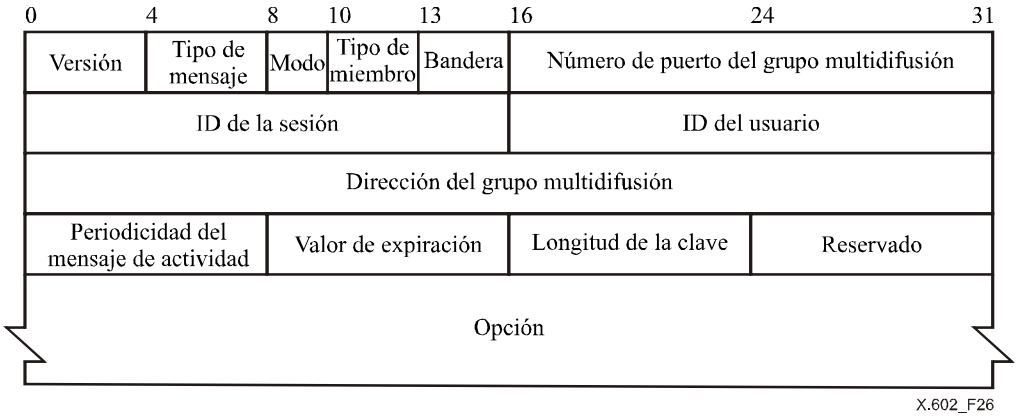

Figura 26 – Formato del mensaje de gestión de miembros que incluye el estado de la lista

La cabecera MM contiene la siguiente información:

a) Versión (4 bits): Define la versión actual del protocolo GMP. Comienza a partir de '1'.

b) Tipo de mensaje (4 bits): Indica el tipo de mensaje MM. En el cuadro 4 se resumen los tipos de mensaje y su codificación.

Cuadro 4 – Cuadro de codificación de los tipos de mensajes de gestión de miembros

Tipo de mensaje	Codificación
KAREQ	0001
KARES	0010
UIREQ	0011
UIRES	0100
LVREQ	0101
TRREQ	0110
TRIND	0111
Reservado	0000

c) Modo (2 bits): Indica si la sesión es abierta o cerrada.

Cuadro 5 – Cuadro de codificación del modo

Modo	Codificación
Modo abierto	01
Modo cerrado	10

d) Tipo de miembro (3 bits): Identifica el tipo de participantes en la sesión, como muestra el cuadro 6.

Cuadro 6 – Cuadro de codificación de los tipos de miembro

Tipo de miembro	Codificación
Creador de la sesión	100
Principal	010
Participante en la sesión	001

e) Bandera (3 bits): Bits de bandera. Dependiendo del tipo de mensaje, se utiliza para diferentes propósitos:
   - Información sobre el usuario (UI): Indica que el mensaje es UIRES cuando 'UI = 1'.
   - Estado de la sesión (SS): Indica el estado de la sesión. 'SS = 1' indica que se está dando fin a la sesión.
   - R: Reservado.

2	1	0
R	SS	UI

f) Número de puerto del grupo multidifusión (16 bits): Número de puerto para la comunicación del grupo multidifusión.

g) ID de la sesión (16 bits): Identifica cada sesión, asignado por el servidor GMP.

h) ID del usuario (16 bits): Identifica a los participantes en la sesión. El ID para el creador de la sesión y los demás participantes los asigna el servidor GMP en la fase de creación y en la fase de registro, respectivamente.

i) Dirección del grupo multidifusión (32 bits): Dirección del grupo multidifusión.

j) Periodicidad del mensaje de actividad (8 bits): Especifica un temporizador mediante el que se genera el mensaje KAREQ en unidades de 100 ms. Este valor lo define el creador de la sesión.

k) Valor de expiración (8 bits): Especifica el tiempo de espera para la señal KARES.

l) Longitud de la clave (8 bits): Los valores de longitud de la clave en GMP en unidades de 8 bits.

m) Reservado (8 bits): Reservado.

9 Variables GMP

9.1 Variables para toda la sesión

La gestión de sesión GMP mantiene y procesa los siguientes parámetros que se resumen en el cuadro 7.

Cuadro 7 – Parámetros de información de sesión

Parámetro	Descripción
Nombre y objeto de la sesión	Nombre y objeto de la sesión generados por el creador de la sesión
Contenido de la sesión	Asunto, introducción y contenido de la sesión
Información sobre el propietario	Información sobre el creador
Tiempo de inicio de la sesión	Tiempo de inicio de la sesión
Tiempo de fin de la sesión	Tiempo de terminación de la sesión
Información de medios	Tipos y características de los medios
Información relativa a la dirección	Dirección para las comunicaciones
Lista de miembros registrados	Lista de miembros registrados

9.2 Temporizadores

La periodicidad del mensaje de actividad, el tiempo de actividad o el temporizador de actividad (o temporizador KA) se definen en unidades de 100 milisegundos en el GMP.

a) Periodicidad del mensaje de actividad: El servidor envía el mensaje KAREQ a los participantes en la sesión activos con una periodicidad igual al valor de este parámetro.

b) Tiempo de actividad: Cuando el servidor GMP envía el mensaje KAREQ, activa el temporizador de actividad. El temporizador KA expira cuando haya pasado el tiempo de actividad. Si el KARES de respuesta no ha llegado antes de la expiración de este temporizador, el servidor GMP actualiza la lista de participantes en la sesión activos y decide si da fin a la sesión o no, en función de los criterios del creador de la sesión.

BIBLIOGRAFÍA

Las siguientes RFC del IETF son útiles para comprender esta Recomendación | Norma Internacional:

– IETF RFC 768 (1980), *User Datagram Protocol.*

– IETF RFC 791 (1981), *Internet Protocol.*

– IETF RFC 793 (1981), *Transmission Control Protocol.*

– IETF RFC 1112 (1989), *Host extensions for IP multicasting.*

– IETF RFC 1119 (1989), *Network Time Protocol (Version 2) Specification and Implementation.*

– IETF RFC 2119 (1997), *Key words for use in RFCs to indicate requirement levels.*

– IETF RFC 2236 (1997), *Internet Group Management Protocol, Version 2.*

– IETF RFC 2327 (1998), *SDP: Session Description Protocol.*

– IETF RFC 2362 (1998), *Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification.*

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

– IETF RFC 2543 (1998), *SIP: Session Initiation Protocol.*

– IETF RFC 2887 (2000), *The Reliable Multicast Design Space for Bulk Data Transfer.*

– IETF RFC 2974 (2000), *Session Announcement Protocol.*

– IETF RFC 3048 (2001), *Reliable Multicast Transport Building Blocks for One-to-Many Bulk-Data Transfer.*

SERIES DE RECOMENDACIONES DEL UIT-T

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

Impreso en Suiza
Ginebra, 2004