(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 381 175**

(51) Int. CI.:
H04L 12/18 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **10189098 .6**
(96) Fecha de presentación: **05.10.2007**
(97) Número de publicación de la solicitud: **2276198**
(97) Fecha de publicación de la solicitud: **19.01.2011**

(54) Título: **Dispositivo para gestionar grupos multidifusión**

(30) Prioridad:
26.06.2007 ES 200701775

(45) Fecha de publicación de la mención BOPI:
23.05.2012

(45) Fecha de la publicación del folleto de la patente:
23.05.2012

(73) Titular/es:
Media Patents, S. L.
Av. de Roma 159, 3º, 2ª
08011 Barcelona, ES

(72) Inventor/es:
Fernández Gutiérrez, Álvaro

(74) Agente/Representante:
Zea Checa, Bernabé

DESCRIPCIÓN

Dispositivos para gestionar grupos multidifusión

Campo de la invención

[0001] La invención se sitúa en el campo de la tecnología multidifusión (en inglés: *multicast*) en redes de datos. Más concretamente, la invención se refiere a un procedimiento para gestionar tráfico multidifusión en una red de datos, en la que unas fuentes envían datos dirigidos a por lo menos un grupo multidifusión y una pluralidad de hosts reciben de un enrutador (en inglés: *router*) los datos enviados por una o varias de dichas fuentes que envían a dicho grupo multidifusión, dichos hosts y dicho enrutador comunicándose entre ellos mediante un protocolo de comunicaciones, como por ejemplo el protocolo IGMP (*Internet Group Management Protocol*) o el protocolo MLD (*Multicast Listener Discovery*), que permite unas comunicaciones multidifusión host-enrutador a través de las cuales dicho host puede definir, para dicho grupo multidifusión, una lista de fuentes incluidas para indicar que desea recibir los datos enviados por las fuentes de dicha lista y una lista de fuentes excluidas para indicar que desea recibir el tráfico procedente de todas las fuentes de dicho grupo multidifusión excepto de las fuentes de dicha lista.

[002] La invención también se refiere a unos dispositivos que aplican dicho procedimiento.

Antecedentes de la técnica

[0003] La tecnología multidifusión hace posible enviar datos desde una única fuente a muchos destinatarios a través de una red de datos, sin que sea necesario establecer una comunicación unidifusión (en inglés: *unicast*), es decir una comunicación individual uno a uno entre la fuente y cada uno de los destinatarios. Para ello, la fuente envía datos, en forma de paquetes de datos, a una dirección única asociada a un grupo multidifusión al que pueden suscribirse los equipos interesados en ser destinatarios de dicha emisión de datos. Esta dirección, denominada dirección multidifusión o también dirección de grupo multidifusión, es una dirección IP (*Internet Protocol*) escogida dentro de un rango que está reservado para las aplicaciones multidifusión. Los paquetes de datos que han sido enviados por la fuente a la dirección multidifusión son entonces replicados en los diferentes enrutadores de la red para que lleguen a los destinatarios que se han unido al grupo multidifusión.

[0004] Normalmente, los destinatarios de las emisiones de datos en un grupo multidifusión son equipos conectados a la red de datos mediante un proxy o un enrutador. En adelante, se utilizará el término habitual "host" para referirse a dichos equipos. Un host puede ser, por ejemplo, un ordenador o un "set-top box" conectado a un televisor.

[0005] Cuando un host quiere recibir la información emitida por una o varias fuentes de un grupo multidifusión, envía al enrutador más cercano, o a un proxy intermedio, un mensaje de suscripción para suscribirse a dicho grupo de modo que el enrutador le transmita los datos que llegan a través de la red de datos y que han sido emitidos por las fuentes del grupo multidifusión. Asimismo, cuando un host desea dejar de recibir las emisiones de datos en el grupo multidifusión, envía al enrutador o al proxy un mensaje de baja de la suscripción para dejar de recibirlas.

[0006] Los mensajes intercambiados entre un host y el enrutador más cercano para gestionar la pertenencia a un grupo multidifusión utilizan el protocolo IGMP (*Internet Group Management Protocol*) o bien el protocolo MLD (*Multicast Listener Discovery*), según si el enrutador funciona con la versión 4 (*IPv4*) o con la versión 6 (*IPv6*) del protocolo IP (*Internet Protocol*) respectivamente.

[0007] Cuando hay un proxy entre el host y el enrutador, el proxy también utiliza los protocolos IGMP/MLD para intercambiar con el host, el enrutador más cercano u otro proxy intermedio los mensajes de pertenencia al grupo multidifusión. En estos casos, el proxy puede recibir de distintos hosts peticiones de suscripción o de baja de la suscripción a un grupo multidifusión, y las agrupa para reducir así el tráfico de mensajes IGMP/MLD que envía al enrutador.

[0008] Además, los enrutadores intercambian mensajes entre ellos con el fin de definir el enrutamiento que permita encaminar de forma eficiente los datos desde las fuentes hacia los hosts que se han suscrito a un grupo multidifusión. Para ello, los enrutadores utilizan unos protocolos específicos, incluyendo el muy conocido PIM-SM (*Protocol Independent Muticast - Sparse Mode*).

[0009] En resumen, los enrutadores reciben de los hosts, en forma de mensajes IGMP/MLD, una información que especifica de qué grupos multidifusión quieren recibir el tráfico, y se comunican con otros enrutadores, por ejemplo mediante el protocolo PIM-SM, con el fin de establecer un enrutamiento que haga llegar hasta los hosts el tráfico solicitado por éstos.

[0010] Todos los protocolos mencionados están definidos y documentados por la *Internet Engineering Task Force* (*IETF*).

[0011] La versión del protocolo IGMP que se utiliza actualmente es la IGMPv3, la cual está descrita en las especificaciones RFC 3376 publicadas en línea por la IETF (*B. Cain et al., Engineering Task Force, Network Working Group, Request for Comments 3376*, octubre de 2002; actualmente disponibles en la dirección Internet http://tools.ietf.org/html/rfc3376).

[0012] En lo que respecta al protocolo MDL, la versión que se utiliza actualmente es la MDLv2, que está descrita en las especificaciones RFC 3810 publicadas en línea por la IETF (*R. Vida et al., Engineering Task Force, Network Working Group, Request for Comments 3810*, junio de 2004; actualmente disponibles en la dirección Internet http://tools.ietf.org/html/rfc3810).

[0013] El funcionamiento de un proxy IGMP que utiliza los protocolos IGMP/MLD está descrito en las especificaciones RFC 4605 publicadas en línea por la IETF (*B. Fenner et al., Engineering Task Force, Network Working Group, Request for Comments 4605*, agosto de 2006; actualmente disponibles en la dirección Internet http://tools.ietf.org/html/rfc4605).

[0014] El protocolo PIM-SM utilizado para la comunicación entre enrutadores está descrito en las especificaciones RFC 4601 publicadas en línea por la IETF (*B. Fenner et al., Engineering Task Force, Network Working Group, Request for Comments 4601*, agosto de 2006; actualmente disponibles en la dirección Internet http://tools.ietf.org/html/rfc4601).

[0015] Inicialmente la tecnología multidifusión se implementó principalmente para aplicarla al modelo de comunicación varios-a-varios, conocido como ASM ("*Any Source Multicast*"), en el cual muchos usuarios se comunican entre sí y cualquiera de ellos puede emitir datos y también recibir datos de todos los demás. Una aplicación típica de ASM es la multiconferencia a través de Internet.

[0016] Posteriormente la tecnología multidifusión se implementó para aplicarla al modelo de comunicación uno-a-varios, conocido como SSM ("*Source Specific Multicast*"), en el cual una sola fuente envía datos para muchos destinatarios. La radio y la televisión a través de Internet son aplicaciones de SSM.

[0017] Por esta razón, el SSM presenta actualmente un gran interés.

[0018] En las primeras versiones del protocolo IGMP, un host no podía elegir las fuentes emisoras de datos a las que quería suscribirse dentro de un grupo multidifusión, sino que sólo podía suscribirse o darse de baja de la suscripción al grupo para todas las fuentes. Los mensajes que un host enviaba a un enrutador eran muy sencillos: Join(G) para recibir tráfico del grupo multidifusión G y Leave(G) para dejar de recibirlo. Por lo tanto, las primeras versiones del protocolo IGMP no permitían el SSM.

[0019] Para permitir el SSM, en la versión IGMPv3 del protocolo IGMP se introdujo la posibilidad de que los hosts pudieran escoger las fuentes dentro de un grupo multidifusión. Para ello, un host puede enviar dos tipos de menajes IGMP:

- Un mensaje INCLUDE, que consiste en indicar las direcciones IP de las fuentes de las cuales el host desea recibir la emisión de datos. Según la terminología de las especificaciones RFC 3376, a las direcciones IP de estas fuentes elegidas (o incluidas) se las denomina fuentes INCLUDE.

- Un mensaje EXCLUDE, que consiste en indicar las direcciones IP de las fuentes de las cuales el host no desea recibir la emisión de datos. En este caso, se interpreta que el host desea recibir datos emitidos por todas las fuentes excepto por las fuentes indicadas como excluidas en el mensaje. También según la terminología de las especificaciones RFC 3376, a las direcciones IP de estas fuentes excluidas se las denomina fuentes EXCLUDE.

[0020] Para ahorrar memoria, tráfico de datos o por otros motivos, en la versión IGMPv3 se decidió que cada interfaz de red y grupo multidifusión pudiera funcionar sólo en uno de los dos modos siguientes, pudiendo pasar de uno a otro: un modo INCLUDE en el cual la interfaz de red define una lista de fuentes INCLUDE o un modo EXCLUDE en el cual la interfaz de red define una lista de fuentes EXCLUDE.

[0021] Una interfaz de red puede recibir varias peticiones diferentes para cada grupo multidifusión G1. Cada petición contiene, para el mismo grupo multidifusión, una lista de fuentes INCLUDE o una lista de fuentes EXCLUDE. Para resolver esta situación y mantener la restricción de que cada interfaz de red pueda funcionar sólo en modo INCLUDE o sólo en modo EXCLUDE, el protocolo IGMPv3 establece que la interfaz de red debe aplicar las siguientes reglas:

Regla 1. Si alguna de las fuentes de datos de un grupo G1 es EXCLUDE, entonces la interfaz de red funciona en modo EXCLUDE para el grupo G1 y la lista de fuentes de la interfaz de red es la intersección de las listas de fuentes EXCLUDE menos las fuentes de la listas INCLUDE.

Regla 2. Si todas las fuentes son de tipo INCLUDE, entonces la interfaz de red funciona en modo INCLUDE para el grupo G1 y la lista de fuentes de la interfaz de red es la unión de todas las fuentes INCLUDE.

[0022] Como se entenderá más adelante con la descripción de varias realizaciones de la invención, estas reglas complican considerablemente las comunicaciones.

[0023] En la multidifusión ASM, cuando un host quiere recibir tráfico de un grupo multidifusión determinado G, hay que resolver el siguiente problema técnico: el host sólo conoce la dirección del grupo multidifusión G y desconoce las direcciones IP de las fuentes de ese grupo G que están emitiendo datos. Existen diferentes protocolos de comunicación multidifusión entre enrutadores que solucionan este problema de diferentes maneras. Actualmente, se aplica principalmente el protocolo PIM-SM y se resuelve el problema designando un enrutador denominado "*Rendez-vous Point*", en adelante enrutador RP, como responsable de conocer todas las fuentes de un mismo dominio multidifusión (conjunto de enrutadores que utilizan un mismo enrutador RP). Para averiguar las direcciones IP de las fuentes, cada enrutador establece una primera comunicación multidifusión con el enrutador RP para que éste le envíe el tráfico multidifusión solicitado. Cuando el enrutador recibe los primeros datos del tráfico multidifusión, éste descubre las direcciones IP de las fuentes. Entonces, el último enrutador, es decir el enrutador que recibe directamente los mensajes IGMP provenientes de los hosts, intenta recibir los datos directamente desde las fuentes utilizando el árbol SPT (*Shortest Path Tree*) que establece el camino más corto a través de la red, denominado camino SPT. Cuando el enrutador empieza a recibir los datos en forma duplicada, tanto a través del enrutador RP como directamente a través del camino SPT, corta la comunicación con el enrutador RP y conserva únicamente la comunicación directa a través del camino SPT.

[0024] En el SSM el problema de averiguar las direcciones IP de las fuentes de un grupo multidifusión no existe, ya que es el usuario quien elige las fuentes desde las cuales desea recibir el tráfico multidifusión. Por lo tanto, los hosts son capaces de indicar al enrutador o al proxy las direcciones IP de las fuentes. Como consecuencia de ello, en el SSM es posible eliminar numerosas complejidades técnicas que son propias del ASM. En particular, es posible eliminar las complejidades técnicas que están asociadas a la averiguación de las direcciones IP de las fuentes. Por ejemplo, en el SSM no es necesario utilizar un enrutador RP, puesto que los enrutadores pueden conocer las direcciones IP de las fuentes, las cuales son indicadas por los hosts cuando se suscriben al grupo multidifusión. Por lo tanto, en el SSM es posible aplicar algoritmos más eficientes que los que se utilizan actualmente.

[0025] Las reglas mencionadas anteriormente para el protocolo IGMPv3 impiden que se puedan explotar estas ventajas del sistema SSM. Cuando una interfaz de red trabaja en modo EXCLUDE desconoce las direcciones IP de las fuentes y por lo tanto se ve obligada a averiguar dichas direcciones IP a través del enrutador RP, tal como se ha explicado anteriormente para el ASM, con el inconveniente de que los procesos de enrutamiento para el ASM son más complicados.

[0026] Recientemente, la IETF ha publicado una nueva propuesta que modifica las especificaciones de las versiones IGMPv3 y MLDv2 de los protocolos IGMP y MDL para intentar resolver los inconvenientes citados, y que está descrita en las especificaciones RFC 4604 editadas en línea por la IETF (*H. Holbrook et al., Engineering Task Force, Network Working Group, Request for Comments 4604*, agosto de 2006; actualmente disponibles en la dirección Internet http://tools.ietf.org/html/rfc4604). La modificación propuesta consiste básicamente en reservar un rango para direcciones multidifusión SSM y en prohibir que en un sistema multidifusión SSM los hosts puedan enviar mensajes de tipo EXCLUDE. Esta restricción penaliza innecesariamente el pleno desarrollo del SSM, ya que impide que un host pueda mantenerse a la escucha de otras nuevas fuentes dentro del mismo grupo multidifusión.

[0027] Se conocen numerosas patentes o solicitudes de patentes que proponen diversas mejoras en comunicaciones multidifusión. Entre ellas, son de destacar las siguientes: US6434622B1, US6785294B1, US6977891B1, US2003/0067917A1, US2005/0207354A1, US2006/0120368, US2006/0182109A1 y WO2006/001803A1. Sin embargo, ninguna de ellas resuelve los problemas citados anteriormente.

[0028] La publicación U.S. No. 2006/0262792 A1 divulga un sistema y un procedimiento para proporcionar direcciones IP multidifusión tanto estáticas como dinámicas, en las que se introduce el concepto de Rango-Estático de multidifusión (*multicast Static-Range*) que permite la coexistencia de direcciones IP multidifusión estáticas y dinámicas. El Rango-Estático de multidifusión es un conjunto de direcciones IP de clase D que está reservado para multidifusión estática, y que está configurado en todos los enrutadores. Cuando un enrutador recibe un mensaje PIM o un mensaje IGMP, el enrutador determina si el grupo especificado en el mensaje está dentro del Rango-Estático de multidifusión. Si el grupo pertenece a un grupo multidifusión estático, el enrutador no propaga el mensaje hacia enrutadores ascendentes (en inglés: *upstream routers*) usando los protocolos PIM-SM o PIM-SSM, y sólo conecta o desconecta interfaces internas del enrutador. Si la dirección del grupo multidifusión del mensaje no está dentro del Rango-Estático de multidifusión, el enrutador asume que el mensaje pertenece a un grupo multidifusión dinámico e implementa normalmente los protocolos PIM o IGMP.

Descripción resumida de la invención

[0029] La invención tiene como finalidad principal proporcionar un sistema mejorado de gestión de las comunicaciones multidifusión en una red de datos, aplicable especialmente a las comunicaciones SSM.

[0030] Un objetivo de la invención es aumentar la eficacia del enrutamiento entre las fuentes emisoras de datos y los hosts que han solicitado recibir dichas emisiones de datos.

[0031] Otro objetivo de la invención es que pueda implementarse en forma de un protocolo mejorado de comunicaciones multidifusión host-enrutador tomando como base los protocolos existentes y de forma compatible con las versiones anteriores de estos protocolos.

[0032] Para este propósito, se provee un host según la reivindicación 1 u 8. Se presentan realizaciones preferidas en las reivindicaciones dependientes.

[0033] También se describe un procedimiento para gestionar tráfico multidifusión en una red de datos del tipo indicado al principio, en el cual, de acuerdo con dicho protocolo de comunicaciones que permite comunicaciones multidifusión host- enrutador:

- los hosts almacenan, para cada grupo multidifusión e interfaz de red, dos registros diferentes: un registro de fuentes incluidas que contiene una lista de fuentes incluidas y un registro de fuentes excluidas que contiene una lista de fuentes excluidas;

- la interfaz de red de cada host envía a dicho enrutador un mensaje que contiene, para un único grupo multidifusión, información de la lista de fuentes del registro de fuentes incluidas y/o información de la lista de fuentes del registro de fuentes excluidas de dicho host;

- el enrutador almacena, para cada grupo multidifusión, dos registros diferentes: un registro de fuentes incluidas que contiene información de las listas de fuentes incluidas y un registro de fuentes excluidas que contiene información de las listas de fuentes excluidas;

- dicho enrutador actualiza su registro de fuentes incluidas y/o su registro de fuentes excluidas, para cada grupo multidifusión, cuando recibe a través de su interfaz de red un mensaje de los hosts que contiene información sobre una lista de fuentes incluidas y/o información sobre una lista de fuentes excluidas.

[0034] Se contempla que dicho mensaje que envía la interfaz de red de cada host a dicho enrutador es un mensaje de estado que contiene la lista de fuentes del registro de fuentes incluidas de dicho host y la lista de fuentes del registro de fuentes excluidas de dicho host.

[0035] También se contempla que dicho mensaje que envía la interfaz de red de cada host a dicho enrutador es un mensaje de cambio de estado que es enviado cuando dicho host detecta un cambio en su registro de fuentes incluidas o un cambio en su registro de fuentes excluidas, comprendiendo dicho mensaje de cambio de estado uno o más bloques de datos para cada grupo multidifusión, en el cual cada uno de dichos bloques de datos contiene información sobre modificaciones de la lista de fuentes del registro de fuentes incluidas o información sobre modificaciones de la lista de fuentes del registro de fuentes excluidas, y en el cual cada uno de dichos bloques de datos contiene un campo que indica si el bloque de datos se refiere a modificaciones de la lista de fuentes incluidas o a modificaciones de la lista de fuentes excluidas.

[0036] El enrutador usa de forma ventajosa la información de las listas de fuentes incluidas contenidas en dichos mensajes recibidos para solicitar el tráfico de datos emitido por dichas fuentes incluidas.

[0037] Cuando la interfaz de red es una interfaz de red de un host, se mantiene un registro de fuentes incluidas y un registro de fuentes excluidas para cada socket que usa dicha interfaz de red y cada grupo multidifusión, y se mantiene un registro de fuentes incluidas y un registro de fuentes excluidas para dicha interfaz de red, los cuales son actualizados, respectivamente, en base al contenido de dichos registros de fuentes incluidas para los sockets y en base a dichos registros de fuentes excluidas para los sockets.

[0038] En un ejemplo ventajoso, dichos mensajes de estado que llegan a la interfaz de red del enrutador contienen instrucciones sobre el procedimiento que el enrutador debe aplicar para establecer árboles de enrutamiento a partir de dichas fuentes incluidas para dicho enrutador. Preferiblemente, para incorporar dichas instrucciones a un mensaje de estado, dicho mensaje de estado indica una dirección multidifusión que se encuentra fuera del rango reservado para direcciones multidifusión; el enrutador detecta que la dirección multidifusión indicada se encuentra fuera de rango, interpreta que dicha dirección multidifusión contiene dichas instrucciones y lee dichas instrucciones en forma de un código numérico contenido en dicha dirección multidifusión.

[0039] El protocolo de comunicaciones entre el enrutador y los hosts es preferiblemente una versión del protocolo IGMP (*Internet Group Management Protocol*) o el protocolo MLD (*Multicast Listener Discovery*) en los que los mensajes de estado enviados por una interfaz de red o por una interfaz de equipo pueden contener, en el mismo mensaje, una lista de fuentes incluidas y una lista de fuentes excluidas.

[0040] También se describe un equipo de red compatible con el procedimiento, comprendiendo dicho equipo de red una interfaz de red y siendo dicho equipo de red adecuado para funcionar en la línea de intercambio entre dicho host y dicho enrutador, en el que se almacenan instrucciones ejecutables para:

- mantener, para cada grupo multidifusión, un registro de fuentes incluidas y un registro de fuentes excluidas;

- enviar, a una interfaz de red cercana en dirección a dicho enrutador, un mensaje que contiene, para un grupo multidifusión, información de la lista de fuentes de dicho registro de fuentes incluidas y/o información de la lista de fuentes de dicho registro de fuentes excluidas; y

- actualizar dicho registro de fuentes incluidas y/o dicho registro de fuentes excluidas, para cada grupo multidifusión, cuando la interfaz de red de dicho equipo de red recibe un mensaje de otra interfaz de red que contiene información sobre una lista de fuentes incluidas y/o información sobre una lista de fuentes excluidas.

[0041] También se describe un equipo compatible con el procedimiento, comprendiendo dicho equipo una interfaz de red y siendo dicho equipo adecuado para funcionar como un host que almacena instrucciones ejecutables para mantener, para cada socket que usa dicha interfaz de red y para cada grupo multidifusión, un registro de fuentes incluidas y un registro de fuentes excluidas, y mantener para dicha interfaz de red un registro de fuentes incluidas y un registro de fuentes excluidas los cuales son actualizados, respectivamente, en base al contenido de dichos registros de fuentes incluidas para los sockets y en base a dichos registros de fuentes excluidas para los sockets.

[0042] También se describe un enrutador compatible con el procedimiento que almacena instrucciones ejecutables para:

- mantener, para cada grupo multidifusión, dos registros diferentes: un registro de fuentes incluidas y un registro de fuentes excluidas; y

- actualizar dicho registro de fuentes incluidas y/o dicho registro de fuentes excluidas, para cada grupo multidifusión, cuando dicho enrutador recibe, a través de su interfaz de red, un mensaje que contiene información sobre una lista de fuentes incluidas y/o información sobre una lista de fuentes excluidas.

[0043] Dicho enrutador usa preferiblemente la información de las listas de fuentes incluidas que está comprendida en dichos mensajes recibidos por el enrutador para solicitar a otros enrutadores el tráfico de datos emitido por dichas fuentes incluidas.

[0044] Para solicitar dicho tráfico de datos emitido por dichas Fuentes incluidas, dicho enrutador usa preferiblemente el protocolo PIM-SM (*Protocol Independent Multicast - Sparse Mode*).

[0045] En un ejemplo preferido, al recibir un mensaje informando de que un host ya no desea recibir tráfico de un grupo multidifusión específico y una fuente incluida específica, dicho enrutador verifica si hay un registro de fuentes excluidas de dicho grupo multidifusión y si dicho registro existe y no contiene una fuente excluida con la misma dirección IP que dicha fuente incluida, dicho enrutador continua transmitiendo dicho tráfico de dicho grupo multidifusión específico y dicha fuente incluida específica, sin enviar un mensaje del tipo Consulta Específica de Grupo-Y-Fuente (en inglés: *Group-And-Source Specific Query*) en el protocolo IGMP para verificar si hay otro host que aún desea recibir dicho tráfico.

[0046] También en un ejemplo preferido, al recibir un mensaje para actualizar la información del registro de fuentes excluidas, en el cual dicho mensaje solicita el bloqueo del tráfico procedente de una fuente específica y grupo multidifusión específico, dicho enrutador verifica si hay un registro de fuentes incluidas de dicho grupo multidifusión y si dicho registro existe y contiene una fuente incluida con la misma dirección IP que la fuente para la cual dicho mensaje ha solicitado un bloqueo, dicho enrutador continua transmitiendo dicho tráfico de dicho grupo multidifusión específico y dicha fuente específica, sin enviar un mensaje del tipo Consulta Específica de Grupo-Y-Fuente (en inglés: *Group-And-Source Specific Query*) en el protocolo IGMP para verificar si hay otro host que aún desea recibir dicho tráfico.

Breve descripción de los dibujos

[0047] Pueden observarse otras ventajas y características de la invención a partir de la siguiente descripción en la que, sin carácter limitativo, se hace referencia a unas realizaciones preferidas de la invención haciendo referencia a los dibujos que se acompañan. Las figuras muestran:

Fig. 1, un ejemplo básico de un sistema multidifusión en una red de datos;

Fig. 2, un ejemplo más detallado de un sistema multidifusión en una red de datos;

Fig. 3, el formato de los mensajes "Consulta de Pertenencia" ("*Membership Query*") que envían los enrutadores a los host en el protocolo IGMPv3, tanto en el protocolo IGMPv3 como en el protocolo IGMP modificado según la invención;

Fig. 4, el formato de los mensajes "Informe de Pertenencia" ("*Membership Report*") que envían los host a los enrutadores, tanto en el protocolo IGMPv3 como en el protocolo IGMP modificado según la invención;

Fig. 5, el formato interno de los bloques de datos "Registro de Grupo" ("*Group Record*") contenidos en cada mensaje "Consulta de Pertenencia" o "Informe de Pertenencia", en el protocolo IGMPv3;

Fig.6, formato de un mensaje "Informe de Pertenencia" que corresponde al mensaje que envía el DSLAM 240 al enrutador 260 en el sistema de la Fig. 2, cuando se aplica el protocolo IGMP modificado según la invención.

Descripción detallada de realizaciones de la invención

[0048] La Fig. 1 muestra un ejemplo básico de un sistema multidifusión en una red de datos. En este ejemplo, tres hosts 101, 102, 103 están conectados a la red de datos a través de unos CPE 104, 105 (CPE: "Customer-Premises Equipment" o equipo local de cliente). Un CPE es un terminal de conexión a la red situado en el extremo del abonado a una línea de acceso, que se comunica por ejemplo mediante un modem DSL (DSL: "Digital Subscriber Line" o línea de abonado digital). El host 101 está conectado a un CPE 104 de una línea de un abonado, mientras que los host 102 y 103 están conectados ambos a otro CPE 105 de otra línea de abonado. Los CPE 104, 105 están conectados a un DSLAM 106 (DSLAM: "Digital Subscriber Line Access Multiplexer" o multiplexor digital de acceso a la línea de abonado) que dirige el tráfico de los diferentes CPE 104, 105 a través de un switch 107 hacia un enrutador 108 que, a su vez, está conectado a una red IP 109 (IP: "Internet Protocol"). En otro punto de la red IP 109 está conectado otro enrutador 110 que concentra los paquetes de datos emitidos por unas fuentes 111, 112 de un grupo multidifusión.

[0049] Por motivos de claridad, la Fig. 1 muestra un único grupo formado por varios hosts 101, 102, 103 conectados a un enrutador 107, y un único grupo de fuentes 111, 112 conectadas a un enrutador 110. Por supuesto, un sistema multidifusión está compuesto en realidad por un gran número de estos conjuntos y grupos.

[0050] La Fig. 1 también muestra el alcance de cada uno de los protocolos IGMP y PIM-SM : el protocolo IGMP se aplica a comunicaciones entre los hosts receptores y los enrutadores, a través de los CPE y los DSLAM, mientras que el protocolo PIM-SM se aplica a comunicaciones entre diferentes enrutadores a través de la red IP.

[0051] En este ejemplo se ha supuesto que los enrutadores funcionan con la versión IPv4 del protocolo IP y por lo tanto el sistema utiliza el protocolo IGMP. Sin embargo, los razonamientos expuestos también son aplicables a un sistema que utilice el protocolo MLD (versión IPv6 del protocolo IP).

[0052] Los CPE y los DSLAM son equipos que pueden realizar una función de proxy IGMP consistente en recibir varias peticiones IGMP y agruparlas para reducir el volumen de mensajes IGMP que son enviados al enrutador. Este funcionamiento está descrito en las especificaciones RFC 4605 de la IETF mencionadas al principio.

[0053] El funcionamiento básico del sistema multidifusión mostrado en la Fig. 1 es el siguiente.

[0054] Los hosts 101, 102, 103 envían a los CPE 104, 105 varios mensajes IGMP en los que identifican la dirección multidifusión del grupo y las direcciones de las fuentes de las que quieren recibir emisiones de datos. Los CPE que reciben varios mensajes IGMP de diferentes hosts, como es el caso del CPE 105 en el ejemplo de la Fig. 1, agrupan estos mensajes IGMP para enviar al DSLAM un mensaje IGMP único. Por su parte, el DSLAM 106 recibe mensajes IGMP de diferentes CPE, en este caso los CPE 104, 105, y los agrupa para enviar al enrutador 108, a través del switch 107, un mensaje IGMP en el que sólo se indican las fuentes INCLUDE o EXCLUDE para cada grupo multidifusión.

[0055] El enrutador 108 recibe el mensaje IGMP enviado por el DSLAM 106 a través del switch 107, y se comunica con otros enrutadores de la red IP utilizando el protocolo PIM-SM para establecer un enrutamiento a través de la red IP que haga llegar hasta el enrutador 108 los datos emitidos por las fuentes especificadas en el mensaje IGMP recibido por el enrutador 108.

[0056] Como se verá a continuación en un ejemplo más detallado, en la técnica anterior el enrutador 108 no siempre conoce las direcciones IP de las fuentes que habían sido especificadas por los hosts, ya que esta información se ha perdido cuando las interfaces de red han agrupado los mensajes IGPM enviados originalmente por los hosts. El

enrutador 108 tiene pues que averiguar las direcciones IP de las fuentes aplicando unos procedimientos complicados y poco eficaces.

Ejemplo de funcionamiento de un sistema multidifusión que aplica los procedimientos de la técnica anterior (protocolo IGMPv3)

[0057] En la Fig. 2 se muestra de forma más detallada un sistema multidifusión y las diferentes comunicaciones necesarias para su funcionamiento.

[0058] Con el fin de ilustrar los principios y ventajas de la invención a partir del esquema de la Fig. 2, se explica en primer lugar el funcionamiento según la técnica anterior, la cual aplica el protocolo IGMPv3. Posteriormente se hará referencia a este mismo esquema de la Fig. 2 para explicar el funcionamiento según la invención.

[0059] El host 200 es un ordenador personal PC en el que se ejecutan dos aplicaciones 201, 202 que pueden solicitar tráfico multidifusión. El ordenador 200 está equipado con una tarjeta de red 203 que está conectada a un CPE 208, que a su vez está conectado a un DSLAM 240.

[0060] Los hosts 220 y 225 son dos ordenadores personales PC que están equipados cada uno con una tarjeta de red 222, 223 conectadas a un mismo CPE 228, que a su vez está conectado al DSLAM 240. En cada ordenador 220, 225 se ejecuta una sola aplicación, respectivamente 221, 226, que puede solicitar tráfico multidifusión.

[0061] El host 231 es un decodificador STB (STB: "Set-Top-Box"), conectado a un televisor 230, que permite la recepción de canales de televisión por Internet. El decodificador 231 está equipado con una tarjeta de red 232 conectada a un CPE 229 que a su vez está conectado al DSLAM 240.

[0062] El DSLAM 240 está conectado al enrutador 260 a través del switch 250. El enrutador 260 está conectado a una red IP formada por otros enrutadores, que en este ejemplo son los enrutadores 261, 262, 263, 264, 265, 266, 267 y 268.

[0063] El enrutador 264 es un enrutador RP ("Rendezvous Point"), es decir un enrutador utilizado por el protocolo PIM-SM para establecer el enrutamiento entre las fuentes emisoras del grupo multidifusión y los hosts que desean recibir las emisiones de estas fuentes cuando no conocen las direcciones IP de estas últimas.

[0064] En el ejemplo de la Fig. 2 hay cinco fuentes emisoras 295, 296, 297, 298, 299 que pertenecen a un mismo grupo multidifusión G1. Para facilitar la explicación, la siguiente descripción hace referencia a estas fuentes a través de sus respectivas direcciones IP, que son respectivamente S1, S2, S3, S4 y S5 tal como se indica en la Fig. 2.

[0065] Las fuentes S1, S2 y S3 están conectadas a la red IP a través del enrutador 266, mientras que las fuentes S4 y S5 lo están a través del enrutador 262.

[0066] Las aplicaciones 201 y 202 que se ejecutan en el host 200 desean recibir las emisiones de datos en el grupo multidifusión G1, pero cada aplicación desea recibir unas emisiones de fuentes diferentes:

- la aplicación 201 desea recibir las emisiones de las fuentes S1 y S2, y para ello hará una petición del tipo INCLUDE({S1, S2}; G1);

- la aplicación 202 desea recibir las emisiones de todas las fuentes excepto la S4, y para ello hará una petición del tipo EXCLUDE({S4}; G1).

[0067] La tarjeta de red 203 es una interfaz de red que debe combinar el estado de los diferentes sockets asociados a las aplicaciones 201 y 202 aplicando las reglas del protocolo IGMPv3. Dado que uno de los sockets funciona en modo EXCLUDE, la interfaz de red 203 funcionará sólo en modo EXCLUDE y enviará al CPE 208 el mensaje siguiente: EXCLUDE({S4}; G1).

[0068] En teoría parece que enviar un mensaje EXCLUDE({S4}; G1) hace innecesario enviar un mensaje INCLUDE({S1, S2}; G1), puesto que el primero incluye implícitamente todas las fuentes excepto la S4 y por lo tanto incluye las fuentes S1 y S2. Sin embargo, al operar de esta forma se pierde una valiosa información contenida en el mensaje IGMP enviado por la aplicación 201: las direcciones IP de las fuentes S1 y S2.

[0069] El mensaje EXCLUDE({S4}; G1) enviado por la tarjeta de red 203 se transmite hasta el DSLAM 240, sin que sea modificada la información de las fuentes por el CPE 208 ya que éste sólo recibe mensajes IGMP de un origen.

[0070] La aplicación 221 que se ejecuta en el ordenador 220 hace una petición de tipo INCLUDE({S5}, G1), que indica que desea recibir la emisión de la fuente S5. La tarjeta de red 222 no tiene que combinar varias peticiones ya que sólo recibe peticiones del socket con el que la aplicación 221 está asociada. Por lo tanto, la tarjeta de red 222

envía el CPE 228 un mensaje IGMP que contiene la misma información que la petición de la aplicación 221, es decir un mensaje INCLUDE({S5}, G1).

[0071] La aplicación 226 que se ejecuta en el ordenador 225 hace una petición de tipo INCLUDE({S3}, G1), que indica que desea recibir la emisión de la fuente S3. La tarjeta de red 223 no tiene que combinar varias peticiones, ya que sólo recibe peticiones del socket con el que la aplicación 226 está asociada. Por lo tanto, la tarjeta de red 223 envía al CPE 228 un mensaje IGMP que contiene la misma información que la petición de la aplicación 226, es decir un mensaje INCLUDE({S3}, G1).

[0072] El CPE 228 actúa como un proxy IGMP, aplicando las reglas del protocolo IGMPv3 para combinar los mensajes enviados por las interfaces de red 222 y 223, respectivamente. Como todos los mensajes recibidos son de tipo INCLUDE, la interfaz de red 228 funcionará sólo en modo INCLUDE y transmitirá al DSLAM 240 el mensaje siguiente: INCLUDE ({S3, S5}; G1).

[0073] El STB 231 envía el mensaje INCLUDE({S1}, G1), que indica que desea recibir la emisión de la fuente S1. El CPE 229 transmite este mensaje intacto al DSLAM 240, ya que éste recibe mensajes IGMP de un único origen.

[0074] El DSLAM 240 recibe pues los tres mensajes IGMP siguientes:

EXCLUDE({S4}; G1), procedente del CPE 208
INCLUDE ({S3, S5}; G1), procedente del CPE 228
INCLUDE({S1}, G1), procedente del CPE 229

[0075] El DSLAM 240 es un proxy que debe combinar estos diferentes mensajes aplicando las reglas del protocolo IGMPv3. Dado que uno de los mensajes recibidos, referente al grupo multidifusión G1, es un mensaje de tipo EXCLUDE, la interfaz de red 240 funcionará sólo en modo EXCLUDE para dicho grupo multidifusión G1 y transmitirá al enrutador 260, a través del switch 250, el mensaje siguiente: EXCLUDE({S4}; G1), que indica que el enrutador 260 debe transmitir al DSLAM 240 las emisiones procedentes de todas las fuentes del grupo G1, excepto la S4.

[0076] El enrutador 260 se comunica entonces con los otros enrutadores de la red IP utilizando el protocolo PIM-SM para recibir los datos emitidos por las fuentes solicitadas en el mensaje IGMP, que son todas las fuentes del grupo multidifusión G1 excepto la fuente S4. El protocolo PIM-SM es un protocolo complejo que permite establecer dos tipos de árboles de enrutamiento: un árbol RTP ("Rendezvous Point Tree"), que tiene su centro en el enrutador RP (que en este caso es el enrutador 264) y un árbol SPT ("Shorter Path Tree"), que establece el camino más corto. El enrutador RP es un enrutador designado por el protocolo PIM-SM como el enrutador responsable de conocer las direcciones IP de todas las fuentes de un grupo multidifusión. Inicialmente el enrutador 260 siempre recibe el tráfico del grupo multidifusión a través del árbol RPT, ya que sólo el enrutador RP conoce las direcciones IP de las fuentes. Cuando se cumplen determinadas condiciones que se explicarán a continuación, el enrutador 260 pasa a utilizar el árbol SPT y abandona la transmisión a través del árbol RP.

[0077] En la ejemplo de la Fig. 2, al utilizar inicialmente el árbol RPT el enrutador 260 recibe las emisiones de las fuentes S1, S2 y S3 a través del camino 281 indicado con una línea discontinua, y recibe la emisión de la fuente S5 a través del camino 282 indicado con una línea discontinua. El enrutador 260 está pues recibiendo los datos por los caminos más largos, en lugar de por los caminos más cortos según los árboles STP, que son los caminos 291 y 292 indicados con una línea continua.

[0078] El enrutador 260 no conoce las direcciones IP de las fuentes incluidas porque sólo ha recibido un mensaje EXCLUDE({S4}; G1) del DSLAM 240. Por tanto, el enrutador 260 no puede solicitar el tráfico procedente de las fuentes incluidas utilizando directamente los árboles STP. Como ya se ha dicho al principio, éste es un serio inconveniente. Otro inconveniente consiste en que si el enrutador funciona únicamente en multidifusión SSM, no aceptará el mensaje EXCLUDE. Además, si el enrutador es un enrutador simplificado que sólo es capaz de conectar directamente con las fuentes, no podrá hacerlo si no conoce las direcciones IP de las mismas.

[0079] Las condiciones proporcionadas por el protocolo PIM-SM para cambiar del árbol RPT a un árbol SPT para un determinado canal (S, G), es decir el canal definido por la fuente S dentro del grupo multidifusión G, están detalladas en las especificaciones RFC 4601, en concreto en el apartado 4.2.1 denominado “Last Hop Switchover to the SPT” que define una función denominada "CheckSwitchToSpt(S,G)":

```
void
CheckSwitchToSpt(S,G) {
  if ( ( pim_include(*,G) (-) pim_exclude(S,G)
         (+) pim_include(S,G) != NULL )
       AND SwitchToSptDesired(S,G) ) {
         # Note: Restarting the KAT will result in
         # the SPT switch set KeepaliveTimer(S,G) to
        # Keepalive_Period
```

```
    }
  }
```

[0080] La función "CheckSwitchToSpt(S,G)" tiene una parte configurable, definida por la función configurable "SwitchToSptDesired(S,G)", y una parte no configurable. El cambio del árbol RPT al árbol SPT se realiza cuando se cumplen ambas partes de las condiciones.

[0081] Normalmente la función configurable "SwitchToSptDesired(S,G)" se utiliza para establecer un umbral de volumen de tráfico procedente de la fuente S, de manera que el cambio del árbol RPT al árbol SPT no se realiza si no se ha superado dicho umbral.

[0082] La parte no configurable, que forma parte del código de programación del protocolo PIM-SM, es la siguiente:

```
( pim_include(*,G) (-) pim_exclude(S,G)(+) pim_include(S,G) != NULL )
```

[0083] Esta condición no configurable establece que un enrutador sólo cambia del árbol RPT al árbol SPT para un determinado canal (S,G) si hay alguna interfaz de red del enrutador que ha recibido un mensaje IGMP INCLUDE (S,G) o si hay una interfaz de red del enrutador que ha recibido un mensaje de tipo IGMP que le indica que quiere recibir el tráfico de todas la fuentes del grupo G y dicha interfaz de red no ha recibido un mensaje IGMP EXCLUDE (S,G). Puesto que esta condición no configurable se refiere únicamente a los mensajes IGMP, el único enrutador que puede iniciar un cambio al árbol SPT para establecer una conexión directa con el enrutador de entrada del canal (S, G) es el enrutador que recibe los mensajes IGMP, es decir el enrutador 260 en el ejemplo de la Fig. 2. En los enrutadores que no reciben mensajes IGMP directamente a través de sus interfaces de red, esta condición no se dará nunca, de manera que estos enrutadores nunca iniciarán un cambio al árbol SPT.

[0084] En el ejemplo de la Fig. 2, el único mensaje que recibe el enrutador 260 es EXCLUDE({S4},G1), con lo cual no se cumple dicha condición no configurable. Consecuentemente, el enrutador 260 no podrá pasar del árbol RPT al árbol SPT y el tráfico continuará pasando indefinidamente por los caminos más largos 281, 282 a través del enrutador RP 264, en lugar de hacerlo por los caminos mas cortos 291, 292. Así pues el tráfico es distribuido de forma poco eficiente y además se sobrecarga innecesariamente el enrutador RP.

[0085] En resumen, este ejemplo muestra que la aplicación de las reglas del protocolo IGMPv3 para combinar los mensajes de tipo INCLUDE y los de tipo EXCLUDE afecta negativamente a la eficacia de los sistemas de enrutamiento. El experto en la materia entenderá sin dificultad que esta situación también se produce en otros sistemas multidifusión con combinaciones diferentes de las que se muestran en la Fig. 2.

Protocolo IGMP modificado según la invención

[0086] La invención resuelve estos problemas aplicando un protocolo IGMP modificado para que las interfaces de red puedan transmitir los mensajes enviados por los hosts sin perder la información contenida en dichos mensajes.

[0087] El protocolo IGMP modificado según la invención se diferencia del protocolo IGMPv3 en que las interfaces de red pueden funcionar en modo dual: almacenan y transmiten por separado la información contenida en los mensajes IGMP de tipo INCLUDE y la información contenida en los mensajes IGMP de tipo EXCLUDE.

[0088] A continuación se describe el protocolo IGMP modificado según la invención. Para facilitar la explicación, se hace referencia a la descripción del protocolo IGMPv3 según las especificaciones RFC 3376 de la IETF mencionadas al principio, y sólo se describen en detalle los cambios en el protocolo IGMP modificado con respecto a dicho protocolo IGMPv3. Las partes que no se detallan se ajustan al protocolo IGMPv3 y por tanto están al alcance de un experto en la materia.

[0089] La descripción se ha estructurado en los apartados siguientes:

1) Descripción de la Interfaz. Información de estado. Forma de agrupar las fuentes.
2) Forma de borrar un registro de estado.
3) Reglas para derivar los registros de las interfaces de red.
4) Descripción de los mensajes IGMP.
5) Comportamiento cuando cambia la información de un registro.
6) Comportamiento cuando un host recibe un mensaje "Consulta de Pertenencia".
7) Descripción del protocolo para los enrutadores.
8) Compatibilidad con un host IGMPv3
9) Proxy IGMP mejorado

1) Descripción de la Interfaz. Información de estado. Forma de agrupar las fuentes.

[0090] En las especificaciones RFC 3376 del protocolo IGMPv3 se explica que los sistemas deben soportar los mensajes IGMP de acuerdo con la siguiente función, que permite a un host elegir las fuentes de datos multidifusión:

IPMulticastListen (socket, interfaz, dirección-multidifusión, modo-de-filtro, {lista-de-fuentes}) donde:

"socket" es un parámetro que permite distinguir las diferentes aplicaciones que se ejecutan en el sistema y que llaman a la función "IPMulticastListen". Por ejemplo, pueden ser diferentes aplicaciones que se ejecutan en un mismo ordenador conectado a la red de datos.

"interfaz" ("*interface*") es un identificador local de la tarjeta de red o interfaz de red en la que se indican las fuentes de datos multidifusión que se quieren recibir.

"dirección-multidifusión" ("*multicast-address*") es la dirección del grupo multidifusión.

"modo-de-filtro" ("*filter-mode*") es el modo de la interfaz de red, que puede ser INCLUDE o EXCLUDE. En el modo INCLUDE, la interfaz de red define la lista de fuentes "lista-de-fuentes" como INCLUDE; esto quiere decir que debe enviarse el tráfico emitido por todas las fuentes de la lista. En el modo EXCLUDE, la interfaz de red define la lista de fuentes "lista-de-fuentes" como EXCLUDE; esto quiere decir que debe enviarse el tráfico procedente de todas las fuentes emisoras en el grupo multidifusión exceptuando las fuentes de la lista.

"lista-de-fuentes" ("*source-list*") es la lista de fuentes INCLUDE o EXCLUDE.

Las especificaciones RFC 3376 explicitan claramente que para una determinada combinación de socket, interfaz de red y grupo multidifusión, sólo puede haber un "modo de filtro", que puede ser INCLUDE o EXCLUDE.

[0091] El sistema guarda un registro de estado para cada socket activo. Este registro contiene la información siguiente:

(interfaz, dirección-multidifusión, modo-de-filtro, {lista-de-fuentes})

[0092] Para cada socket, el "modo-de-filtro" del registro sólo puede ser INCLUDE o bien EXCLUDE.

[0093] El sistema también guarda un registro para cada interfaz de red. Este registro contiene la información siguiente:

(dirección-multidifusión, modo-de-filtro, {lista-de-fuentes})

[0094] Para cada interfaz de red y grupo multidifusión, el "modo-de-filtro" del registro sólo puede ser INCLUDE o EXCLUDE. Los registros de cada interfaz de red se derivan de los registros de los sockets. Cuando el registro de una interfaz de red debe resultar de la combinación de diferentes registros, se aplican las reglas que ya se expusieron al principio y que se transcriben a continuación:

Regla 1. Si alguna de las fuentes de datos de un grupo G1 es EXCLUDE, entonces la interfaz de red tendrá un “modo-de-filtro” EXCLUDE para el grupo G1 y la lista de fuentes de la interfaz de red es la intersección de las listas de fuentes EXCLUDE menos las fuentes de la listas INCLUDE.

Regla 2. Si todas las fuentes son de tipo INCLUDE, entonces la interfaz de red tendrá un “modo-de-filtro” INCLUDE para el grupo G1 y la lista de fuentes es la unión de todas las fuentes INCLUDE.

[0095] Hasta aquí se han descrito las características del protocolo IGMPv3 según las especificaciones RFC 3376.

[0096] El protocolo IGMP modificado según la invención mantiene la misma estructura de la función IPMulticastListen del protocolo IGMPv3:

IPMulticastListen (socket, interfaz, dirección-multidifusión, modo-de-filtro, {lista-de-fuentes}) pero con la diferencia de que para cada socket y cada interfaz de red el sistema guarda dos registros: uno para el “modo-de-filtro” EXCLUDE y otro para el “modo-de-filtro” INCLUDE.

[0097] El sistema guarda por tanto dos registros para cada socket :

Registro INCLUDE: (interfaz, dirección-multidifusión, INCLUDE, {lista-de-fuentes})
Registro EXCLUDE: (interfaz, dirección-multidifusión, EXCLUDE, {lista-de-fuentes})

y dos registros para cada interfaz de red y grupo multidifusión :

Registro INCLUDE: (dirección-multidifusión, INCLUDE, {lista-de-fuentes})

Registro EXCLUDE: (dirección-multidifusión, EXCLUDE, {lista-de-fuentes})

[0098] Mientras sólo haya fuentes INCLUDE o sólo haya fuentes EXCLUDE, el sistema sólo necesita un registro. Pero si hay distintas llamadas a la función IPMulticastListen para el mismo grupo multidifusión con información de fuentes INCLUDE y fuentes EXCLUDE, entonces el sistema almacena la información en dos registros, en lugar de mezclar la información como ocurre en la técnica anterior con el protocolo IGMPv3.

[0099] Cada llamada a la función IPMulticastListen sustituye el contenido del registro para un determinado grupo multidifusión, y si no existe el registro, lo crea (esto ocurre, por ejemplo, cuando se llama por primera vez a la función para dicho grupo multidifusión).

2) Forma de borrar un registro

[0100] Para borrar un registro de un determinado grupo G1 en el protocolo IGMPv3, se envía un mensaje de tipo INCLUDE con una lista de fuentes vacía: INCLUDE ({ }, G1). Adicionalmente, un registro en modo EXCLUDE de un determinado grupo G1 cambia al modo INCLUDE automáticamente al cabo de cierto tiempo sin necesidad de enviar ningún mensaje. Para ello, en el protocolo IGMPv3 los registros tienen un temporizador (en inglés: *timer*) para cada grupo multidifusión que es distinto de cero si el estado del registro es EXCLUDE. Cuando el temporizador llega a cero el registro cambia del modo EXCLUDE al modo INCLUDE.

[0101] Para borrar un registro INCLUDE de un determinado grupo G1, en el protocolo IGMP modificado según la invención, se utiliza el mismo sistema que en el protocolo IGMPv3: se envía un mensaje de tipo INCLUDE con una lista de fuentes vacía: INCLUDE ({ }).

[0102] Para borrar automáticamente un registro EXCLUDE de un determinado grupo G1, en el protocolo IGMP modificado los registros EXCLUDE también tienen un temporizador para cada grupo multidifusión, como en el protocolo IGMPv3, pero el funcionamiento es más simple ya que no es necesario realizar un cambio del modo INCLUDE al modo EXCLUDE: simplemente se borra el registro EXCLUDE cuando el temporizador llega a cero.

[0103] Opcionalmente, el sistema IGMP modificado añade un nuevo sistema para borrar los registros de estado EXCLUDE de forma más rápida que se aplica a:

- los registros de los hosts, que se actualizan con la función IPMulticastListen;

- los registros de los proxys y enrutadores, que se actualizan mediante mensajes IGMP.

[0104] Para borrar registros EXCLUDE mediante la función IPMulticastListen en el protocolo IGMP modificado, se ha incorporado un nuevo parámetro de “modo-de-filtro" denominado Filtro_Borrar_Exclude (*Filter_Delete_Exclude*). Cuando la función IPMulticastListen recibe una llamada con este parámetro, sabe que debe borrar el registro EXCLUDE del grupo multidifusión que se indica en la “dirección-multidifusión”.

[0105] Para borrar registros EXCLUDE de proxys y enrutadores mediante mensajes IGMP, en el protocolo IGMP modificado se ha definido un nuevo valor para el campo "Tipo de Registro de Grupo" (“*Group Record Type*”) de los mensajes "Informe de Pertenencia" con la siguiente descripción abreviada:

```
7        DELEX  -  Tipo MODO_ES_BORRAR_EXCLUDE (MODE_IS_DELETE_EXCLUDE)
```

[0106] Este nuevo valor se añade a los valores 1 a 6 del campo "Tipo de Registro de Grupo" que ya existen en el protocolo IGMPv3 con las siguientes descripciones abreviadas (apartado 4.2.12 de las especificaciones RFC 3376):

```
1        IS_IN ( x )  -  Tipo MODO_ES_INCLUDE (MODE_IS_INCLUDE)
2        IS_EX ( x )  -  Tipo MODO_ES_EXCLUDE (MODE_IS_EXCLUDE)
3        TO_IN ( x )  -  Tipo CAMBIAR_A_MODO_INCLUDE (CHANGE_TO_INCLUDE_MODE)
4        TO_EX ( x )  -  Tipo CAMBIAR_A_MODO_EXCLUDE (CHANGE_TO_EXCLUDE_MODE)
5        ALLOW ( x )  -  Tipo PERMITIR_NUEVAS_FUENTES (ALLOW_NEW_SOURCES)
6        BLOCK ( x )  -  Tipo BLOQUEAR_VIEJAS_FUENTES (BLOCK_OLD_SOURCES)
```

donde x es la lista de direcciones IP de las fuentes.

3) Reglas para derivar los registros de interfaz de red

[0107] Como se ha indicado en el apartado 1), el protocolo IGMP modificado permite guardar dos registros para cada interfaz de red y grupo multidifusión:

Registro INCLUDE: (dirección-multidifusión, INCLUDE, {lista-de-fuentes})

Registro EXCLUDE: (dirección-multidifusión, EXCLUDE, {lista-de-fuentes})

donde "dirección-multidifusión" es la dirección del grupo multidifusión y "lista-de-fuentes" es la lista de fuentes.

[0108] Al igual que en el protocolo IGMPv3, los registros de las interfaces de red se derivan de los registros de los sockets. Sin embargo, al aplicar el protocolo IGMP modificado el proceso es mucho más sencillo ya que no es necesario mezclar las fuentes INCLUDE y las fuentes EXCLUDE de un mismo grupo multidifusión.

[0109] El protocolo IGMP modificado aplica las siguientes reglas para cada interfaz de red y grupo multidifusión:

Regla1. Para cada grupo multidifusión, cada registro INCLUDE de la interfaz de red contiene la unión de todas las fuentes de los registros INCLUDE de los sockets que usan dicha interfaz de red.

Regla 2. Para cada grupo multidifusión, cada registro EXCLUDE de la interfaz de red contiene la intersección de las fuentes de los registros EXCLUDE de los sockets que usan dicha interfaz de red.

4) Descripción de los mensajes IGMP

[0110] Para simplificar la explicación, en el presente apartado se describen los mensajes IGMP entre el enrutador y un host, suponiendo que no existe ningún Proxy IGMP entre ambos. Más adelante, en el apartado 9, se describirá el comportamiento de un Proxy IGMP.

[0111] Para la comunicación entre un host y un enrutador, el protocolo IGMP modificado utiliza los mismos mensajes que el protocolo IGMPv3, que se describen en el apartado 4 de las especificaciones RFC 3376, pero con las modificaciones que se explican más adelante.

[0112] La Fig. 3 muestra el formato de los mensajes que envían los enrutadores a los hosts en el protocolo IGMPv3. Estos mensajes se denominan "Consulta de Pertenencia". El formato mostrado en la Fig. 3 se aplica tanto al protocolo IGMPv3 como al protocolo IGMP modificado.

[0113] La Fig. 4 muestra el formato de los mensajes que envían los hosts a los enrutadores en el protocolo IGMPv3. Estos mensajes se denominan "Informe de Pertenencia". El formato mostrado en la Fig. 4 se aplica tanto al protocolo IGMPv3 como al protocolo IGMP modificado.

[0114] La Fig. 5 muestra el formato interno de los bloques de datos denominados Registro de Grupo ("*Group Record*") que están contenidos en cada mensaje "Informe de Pertenencia". El campo "Dirección de Grupo" contiene la dirección de grupo multidifusión. Los campos "Dirección de Fuente" contienen la información sobre las fuentes. El campo "Número de Fuentes" indica el número de campos "Dirección de Fuente" que hay en cada Registro de Grupo. El formato mostrado en la Fig. 5 se aplica al protocolo IGMPv3.

[0115] En el protocolo IGMP modificado, cuando se envía un mensaje del tipo "Informe de Pertenencia" se utiliza el mismo formato de mensajes que en el protocolo IGMPv3, pero cuando hay fuentes INCLUDE y también fuentes EXCLUDE para el mismo grupo multidifusión se envían dos Registros de Grupo, como puede verse en la Fig. 6 que se comenta más adelante. Como no se mezclan las fuentes y puede haber dos registros para cada interfaz de red y grupo multidifusión, el sistema puede emitir un mensaje con dos Registros de Grupo diferentes para un mismo grupo o dirección multidifusión: uno de los Registros de Grupo transmite la información sobre las fuentes INCLUDE y el otro transmite la información sobre las fuentes EXCLUDE.

[0116] En el protocolo IGMPv3 los enrutadores envían un mensaje "Consulta de Pertenencia" de tipo "Consulta General" ("*General Query*") para interrogar a los hosts sobre su estado. En respuesta a este mensaje, los hosts envían un mensaje de estado "Informe de Pertenencia" de tipo "Registro de Estado Actual" ("*Current-State Record*"). En el protocolo IGMP modificado se mantiene este sistema, pero el mensaje "Registro de Estado Actual" que envía el host puede contener dos Registros de Grupo para un mismo grupo multidifusión: uno en modo INCLUDE y otro en modo EXCLUDE. El modo INCLUDE o EXCLUDE se identifica, como en el protocolo IGMPv3, por el contenido del campo "Tipo de Registro" ("*Record Type*"), respectivamente:

Tipo de Registro = 1 = MODO_ES_INCLUDE (*MODE_IS_INCLUDE*)
Tipo de Registro = 2 = MODO_ES_EXCLUDE (*MODE_IS_EXCLUDE*)

[0117] Se transmite así la información sobre los dos registros en un mismo mensaje "Registro de Estado Actual".

[0118] En el protocolo IGMPv3, los hosts envían mensajes "Registro de Cambio en Lista de Fuentes" ("*Source-List-Change Record*") para informar de los cambios que ha habido en las fuentes INCLUDE y EXCLUDE. A diferencia de los mensajes "Registro de Estado Actual", los mensajes "Registro de Cambio en Lista de Fuentes" no son enviados en respuesta a un mensaje "Consulta de Pertenencia" enviado por el enrutador, sino que son enviados por un host para indicar que se ha producido un cambio en su registro de fuentes.

[0119] Al igual que en el protocolo IGMPv3, en el protocolo IGMP modificado los hosts también envían mensajes "Registro de Cambio en Lista de Fuentes", pero con la diferencia siguiente: como puede haber dos registros distintos para un mismo grupo multidifusión (un registro INCLUDE y un registro EXCLUDE), el mensaje "Registro de Cambio en Lista de Fuentes" debe indicar a cual de los dos registros se refiere. Para ello, en el protocolo IGMP modificado se definen cuatro nuevos “Tipos de Registro de Grupo”, con las siguientes expresiones abreviadas:

```
 8  ALLOWIN (x) - Tipo PERMITIR_NUEVAS_FUENTES_INCLUDE (ALLOW_NEW_SOURCES_INCLUDE)
 9  BLOCKIN (x) - Tipo BLOQUEAR_VIEJAS_FUENTES_INCLUDE (BLOCK_OLD_SOURCES_INCLUDE)
10  ALLOWEX (x) - Tipo PERMITIR_NUEVAS_FUENTES_EXCLUDE (ALLOW_NEW_SOURCES_EXCLUDE)
11  BLOCKEX (x) - Tipo BLOQUEAR_VIEJAS_FUENTES_EXCLUDE (BLOCK_OLD_SOURCES_EXCLUDE)
```

donde x es la lista de direcciones IP de las fuentes.

[0120] Los nuevos "Tipos de Registro de Grupo" 8 y 9, es decir las expresiones ALLOWIN (x) y BLOCKIN (x), se utilizan para enviar mensajes que añaden o quitan, respectivamente, elementos de las listas de fuentes en los registros INCLUDE.

[0121] Los nuevos "Tipos de Registro de Grupo" 10 y 11, es decir las expresiones ALLOWEX (x) y BLOCKEX (x), se utilizan para enviar mensajes para permitir o bloquear, respectivamente, el tráfico emitido por la fuente x.

[0122] La Fig. 6 muestra un ejemplo de un mensaje "Informe de Pertenencia" que corresponde al mensaje que envía el DSLAM 240 al enrutador 260 en el esquema de la Fig. 2 cuando se aplica el protocolo IGMP modificado según la invención. Más adelante se explicará en detalle el contenido de este mensaje. El DSLAM 240 actúa como un Proxy IGMP situado entre el enrutador 260 y los hosts 200, 220, 225 y 231. Por tanto, en este caso la explicación anterior sobre los mensajes IGMP entre un enrutador y un host es aplicable sustituyendo dicho host por el DSLAM 240. Un Proxy IGMP se comporta como un host en sus comunicaciones con un Enrutador IGMP y se comporta como un enrutador IGMP en sus comunicaciones con un host.

[0123] A continuación se indica el registro que almacena cada equipo de la Fig. 2 cuando se aplica el protocolo IGMP modificado según la invención.

[0124] En el PC 200, si las aplicaciones 201 y 202 utilizan respectivamente el socket1 y el socket2, los registros de estado de los socket1 y socket2, respectivamente, son los siguientes:

Registro INCLUDE: (Interfaz 203, Grupo G1, INCLUDE, { S1, S2 })
Registro EXCLUDE: (Interfaz 203, Grupo G1, EXCLUDE, { S4 })

[0125] El registro de estado de la interfaz de red 203 del PC 200, que coincide con el estado de la interfaz de red del CPE 208, es el siguiente:

Registro INCLUDE: (Grupo G1, INCLUDE, { S1, S2 })
Registro EXCLUDE: (Grupo G1, EXCLUDE, { S4 })

[0126] En el PC 220, si la aplicación 221 utiliza el socket1, el registro de estado del socket1 es el siguiente:

Registro INCLUDE: (Grupo G1, INCLUDE, { S5 })

[0127] En el PC 225, si la aplicación 226 utiliza el socket1, el registro de estado del socket1 es el siguiente:

Registro INCLUDE: (Grupo G1, INCLUDE, { S3 })

[0128] El registro de estado de la interfaz de red del CPE 228 que funciona como Proxy IGMP, después de agrupar las fuentes, es el siguiente:

Registro INCLUDE: (Grupo G1, INCLUDE, { S3, S5 })

[0129] En el STB 231, el registro de estado de la interfaz de red 232, que coincide con el estado de la interfaz de red del CPE 229, es la siguiente:

Registro INCLUDE: (Grupo G1, INCLUDE, { S1 })

[0130] Cada uno de los CPE 208, 228 y 229 envía sus mensajes IGMP al DSLAM 240, el cual los agrupa otra vez pero sin mezclar las fuentes INCLUDE y EXCLUDE.

[0131] El registro de estado de la interfaz de red del DSLAM 240 que funciona como Proxy IGMP, después de agrupar las fuentes, es el siguiente:

Registro INCLUDE: (Grupo G1, INCLUDE, { S1, S2, S3, S5 })
Registro EXCLUDE: (Grupo G1, EXCLUDE, { S4 })

[0132] En respuesta a un mensaje “Consulta General” enviado por el enrutador 260, el DSLAM 240 envía al enrutador 260 el mensaje representado en la Fig. 6, el cual es analizado a continuación.

[0133] Tipo = = 0x22 indica que es un "Informe de Pertenencia" y Número de Registros de Grupo = 2 indica que se envían dos bloques de datos o “Registros de Grupo” para el mismo grupo multidifusión G1. Uno de los “Registros de Grupo” contiene la información sobre las fuentes INCLUDE y el otro sobre las fuentes EXCLUDE. El primer “Registro de Grupo” tiene un “Tipo de Registro” igual a 1. Esto significa que es del tipo “MODO_ES_INCLUDE”, es decir que contiene información sobre las fuentes INCLUDE. En este bloque de datos, “Número de Fuentes” es igual a 4, lo que significa que se va a enviar información de cuatro fuentes INCLUDE. El grupo multidifusión G1 se indica en el campo “Dirección Multidifusión”. Los cuatro campos “Dirección de Fuente [1]” a “Dirección de Fuente [4]” contienen información sobre las cuatro fuentes INCLUDE: S1, S2, S3 y S5. A continuación hay un segundo “Registro de Grupo” con un “Tipo de Registro” igual a 2. Esto significa que es del tipo MODO_ES_EXCLUDE, es decir que contiene información sobre las fuentes EXCLUDE. “Número de Fuentes” es igual a 1, lo que significa que se va a enviar información sobre una fuente EXCLUDE. El grupo multidifusión G1 se indica en el campo “Dirección Multidifusión”. El campo “Dirección de Fuente [1]” contiene información sobre la fuente EXCLUDE: S4.

[0134] El enrutador 260 ha recibido información completa de todas las fuentes. Ahora sí que se cumplen los requisitos que establece el protocolo PIM-SM para cambiar del árbol RPT al árbol SPT, como se explica a continuación.

[0135] Se configura por defecto la condición SwitchToSptDesired(S,G) del protocolo PIM-SM, la cual es la parte configurable de las condiciones de cambio del árbol RPT al árbol SPT para el canal (S, G), de forma que esta condición se cumpla cuando llegue el primer paquete de datos procedente de la fuente S a través del árbol SPT. La condición no configurable de dichas condiciones de cambio se cumple siempre cuando se aplica el protocolo IGMP modificado, ya que el enrutador interesado en recibir el tráfico de la fuente S siempre habrá recibido un mensaje IGMP INCLUDE (S,G), o habrá recibido un mensaje de tipo IGMP indicando que quiere recibir el tráfico de todas la fuentes del grupo G y no habrá recibido un mensaje IGMP EXCLUDE (S,G).

[0136] Por tanto, cuando se aplica el protocolo IGMP modificado, todos los enrutadores que han recibido peticiones de tráfico para una fuente pueden pasar al árbol SPT y recibir el tráfico de dicha fuente por el camino más corto.

[0137] Por consiguiente, en el ejemplo de la Fig. 2 el tráfico emitido por las fuentes S1, S2 y S3 irá por el camino más corto 291, y el tráfico emitido por la fuente S5 irá por el camino más corto 292.

[0138] Opcionalmente, el enrutador 260 puede conectar directamente, desde el principio, con el árbol SPT de cada fuente S1, S2, S3 y S5, ya que conoce las direcciones IP de estas fuentes y por tanto puede utilizar directamente el árbol SPT. Para ello, basta con hacer que la función SwitchToSptDesired(S,G) sea cierta siempre.

[0139] Además, opcionalmente, cada host puede indicar al enrutador 260, en el propio mensaje IGMP, cuándo debe iniciar el cambio del árbol RPT al árbol SPT en función de cada fuente. Para ello, según la invención, se utiliza un campo de dirección multidifusión que queda fuera del rango de direcciones multidifusión y en el cual se pone un mensaje en lugar de poner una dirección multidifusión. Por ejemplo, se ponen los dos primeros bytes de la dirección multidifusión a 0 y se usan los segundos dos bytes para enviar el mensaje al enrutador, asociando a estos segundos dos bytes el siguiente significado:

100 = conectar directamente mediante el árbol SPT
200 = usar la configuración por defecto del enrutador y evaluar la función SwitchToSptDesired(S,G) para decidir el cambio al árbol SPT
300 = usar siempre el árbol RPT y no cambiar al árbol SPT

[0140] El enrutador detecta que la dirección está fuera del rango de direcciones multidifusión e interpreta esos 4 bytes como un mensaje que le indica la forma en que debe cambiar del árbol RPT al árbol SPT en la dirección multidifusión incluida después en el mismo Registro de Grupo.

5) Comportamiento cuando cambia la información de un registro

[0141] En el protocolo IGMP modificado, cuando cambia el registro de estado de una interfaz de red para un determinado grupo multidifusión, el sistema simplemente debe transmitir los cambios enviando un mensaje "Registro de Cambio en Lista de Fuentes" como se indica en el apartado anterior.

[0142] En el protocolo IGMPv3 este proceso es más complejo porque el sistema debe tener en cuenta el "modo-de-filtro" y los posibles cambios del mismo. Esta complejidad no existe en el protocolo IGMP modificado, puesto que la información de las fuentes INCLUDE y EXCLUDE es almacenada y transmitida por separado.

6) Comportamiento cuando un host recibe un mensaje "Consulta de Pertenencia"

[0143] Tanto en el protocolo IGMPv3 como en el protocolo IGMP modificado, los enrutadores envían mensajes denominados "Consulta de Pertenencia" a los hosts para que éstos informen de los canales y grupos multidifusión que desean recibir. En el protocolo IGMP modificado, los hosts envían a los enrutadores un mensaje de respuesta que es similar al que envían en el protocolo IGMPv3, pero con la diferencia de que se envía la información de las fuentes INCLUDE y EXCLUDE por separado.

[0144] Para evitar que todos los hosts respondan al mismo tiempo, se usan varios temporizadores que retrasan las respuestas de los hosts para repartirlas durante un espacio de tiempo que está especificado en el mensaje "Consulta de Pertenencia". Esto funciona de igual modo en el protocolo IGMP modificado y en el protocolo IGMPv3.

[0145] Existen tres tipos de mensajes "Consulta de Pertenencia": "Consulta General" ("*General Query*"), "Consulta de Grupo Específico" ("*Group-Specific Query*") y "Consulta de Grupo y Fuente Específicos" ("*Group-and-Source-Specific Query*").

[0146] Los mensajes de tipo "Consulta General" son enviados por el enrutador cada cierto tiempo (por defecto 125 segundos) para que todos los hosts informen de los grupos y canales multidifusión que quieren recibir enviando unos mensajes "Informe de Pertenencia" que se denominan "Registro de Estado Actual". Los mensajes con los que responde el host a una petición "Consulta General" incluyen bloques de datos denominados "Registros de Grupo", que pueden ser de dos tipos:

Tipo de Registro = 1 MODO_ES_INCLUDE (*MODE_IS_INCLUDE*)
Tipo de Registro = 2 MODO_ES_EXCLUDE (*MODE_IS_EXCLUDE*)

[0147] Como se ha visto anteriormente, en un mismo mensaje o "Informe de Pertenencia", como el que se muestra en la Fig. 4, se envían varios bloques de datos denominados "Registros de Grupo", como el que se muestra en la Fig. 5. El primer campo de la Fig. 5, es decir del "Registro de Grupo", es el campo “Tipo de Registro” que indica el significado de cada bloque de datos (en el ejemplo de la Fig. 5 el campo "Tipo de Registro" es el campo indicado como "Tipo").

[0148] En el protocolo IGMPv3, como cada grupo multidifusión sólo puede estar en estado INCLUDE o en estado EXCLUDE, cada host sólo envía, para cada grupo multidifusión, un "Registro de Grupo", con "Tipo de Registro" de valor 1 o de valor 2 según sea el estado del grupo INCLUDE o EXCLUDE, respectivamente.

[0149] En el protocolo IGMP modificado, dado que la información de las fuentes INCLUDE y EXCLUDE se almacena y envía separadamente, es posible que un host necesite enviar dos "Registros de Grupo" para un mismo grupo multidifusión: un primer "Registro de Grupo" con Tipo de Registro = 1 para informar sobre las fuentes INCLUDE y un segundo "Registro de Grupo" con Tipo de Registro = 2 para informar sobre las fuentes EXCLUDE. Esto se puede ver en la Fig. 6, donde existen dos "Registros de Grupo" para el mismo grupo multidifusión G1.

[0150] Para los mensajes de tipo "Consulta de Grupo Específico" y "Consulta de Grupo y Fuente Específicos" existe la misma diferencia que se acaba de explicar: cuando los hosts contestan a estos mensajes pueden enviar información por separado de las fuentes INCLUDE y EXCLUDE utilizando dos "Registros de Grupo".

7) Descripción del protocolo para los enrutadores

[0151] El funcionamiento según el protocolo IGMP modificado es muy similar al de los protocolos IGMPv3 y MLDv2. Por tanto, para facilitar la comprensión, en adelante se ha adoptado la misma nomenclatura que la usada en las especificaciones RFC 3376 (protocolo IGMPv3) y RFC 3810 (protocolo MLDv2) mencionadas al principio.

[0152] La principal diferencia con respecto a los protocolos IGMPv3 y MLDv2 de la técnica anterior es que en el protocolo IGMP modificado, el enrutador tiene dos registros de estado para cada grupo multidifusión: un registro INCLUDE y un registro EXCLUDE.

[0153] El protocolo IGMP modificado permite a los enrutadores usar mejor los algoritmos de enrutamiento gracias a que los enrutadores reciben de los hosts una información detallada de las fuentes INCLUDE y EXCLUDE. Los enrutadores ejecutan el protocolo IGMP en todas las redes a las que están directamente conectados. Si un enrutador multidifusión tiene más de una interfaz de red conectada a la misma red sólo necesita ejecutar el protocolo en una de las interfaces de red conectadas a esa red. A diferencia del protocolo IGMPv3, en el protocolo IGMP modificado el enrutador ya no trabaja exclusivamente en un modo INCLUDE o EXCLUDE para cada grupo

multidifusión e interfaz de red. Por lo tanto, ya no necesita todos los mecanismos que le permitían cambiar de modo INCLUDE a modo EXCLUDE y viceversa.

[0154] Para cada tarjeta de red o interfaz de red, y grupo multidifusión, los enrutadores que usan el protocolo IGMP modificado almacenan la información separada de las fuentes INCLUDE y EXCLUDE multidifusión en dos registros:

Registro INCLUDE: (dirección-multidifusión, INCLUDE, {lista de fuentes y temporizadores})

Registro EXCLUDE: (dirección-multidifusión, temporizador-de-grupo, EXCLUDE, {lista de fuentes y temporizadores}) donde {lista de fuentes y temporizadores} es una lista de elementos (dirección-de-fuente, temporizador-de-fuente), siendo "dirección-de-fuente" ("*source-address*") la dirección IP de una fuente y siendo "temporizador-de-fuente" ("*source-timer*") un temporizador asociado a dicha fuente,

[0155] Un temporizador es una variable en memoria que contiene un valor que va disminuyendo regularmente con el tiempo hasta llegar a cero.

[0156] Los dos registros, INCLUDE y EXCLUDE, almacenados en el enrutador contienen pues un "temporizador-de-fuente" asociado a cada "dirección-de-fuente".

[0157] Como se ha expuesto anteriormente en el punto 2 referente a las formas de borrar un registro, cada registro EXCLUDE asociado a un grupo multidifusión contiene además un "temporizador-de-grupo" que sirve para eliminar el registro de estado EXCLUDE cuando pasa un determinado tiempo sin que el enrutador haya recibido informes (*reports*) con peticiones de tráfico de tipo EXCLUDE.

[0158] Como se ha explicado anteriormente, los enrutadores envían periódicamente a los hosts unos mensajes denominados "Consulta de Pertenencia", como el de la Fig. 3, para que los hosts contesten informando de los grupos y fuentes de las que desean recibir tráfico multidifusión. Los hosts también pueden enviar mensajes al enrutador para solicitar tráfico multidifusión sin esperar a que el host envíe un mensaje "Consulta de Pertenencia".

[0159] El enrutador utiliza los temporizadores para asegurarse de que, tras haber enviado un mensaje "Consulta de Grupo Específico" o un mensaje "Consulta de Grupo y Fuente Específicos", todos los hosts han tenido tiempo suficiente para contestar a dicho mensaje. El valor de los temporizadores va disminuyendo con el tiempo y si el enrutador recibe un mensaje "Informe de Pertenencia" procedente de un host, el enrutador vuelve a reiniciar los temporizadores correspondientes.

[0160] En el registro INCLUDE los temporizadores funcionan de la manera siguiente: para una determinada interfaz de red, un determinado grupo multidifusión y una determinada "dirección-de-fuente" incluida, mientras el "temporizador-de-fuente" sea mayor que cero el enrutador continuará transmitiendo por dicha interfaz de red el tráfico multidifusión procedente del canal (fuente, grupo multidifusión); cuando el "temporizador-de-fuente" llegue a cero, el enrutador dejará de transmitir dicho tráfico y eliminará la fuente de la lista de fuentes INCLUDE de ese grupo multidifusión.

[0161] En el registro EXCLUDE los temporizadores funcionan de forma parecida, pero con la diferencia de que las fuentes EXCLUDE se clasifican en dos listas: una primera lista denominada "Lista de Solicitadas" ("*Requested List*") que contiene las fuentes cuyo "temporizador-de-fuente" tiene un valor mayor que cero y una segunda lista denominada "Lista de Exclusión" ("*Exclude List*") que contiene las fuentes cuyo "temporizador-de-fuente" tiene valor cero.

[0162] Para cada grupo Gi, el enrutador transmite todo el tráfico solicitado por las fuentes INCLUDE. Si además hay un registro EXCLUDE para el grupo Gi, el enrutador transmite además todo el tráfico restante del grupo Gi excepto las fuentes EXCLUDE de la lista "Lista de Exclusión".

[0163] El motivo de que exista una "Lista de Solicitadas" es que en una red con varios hosts enviando mensajes a un Enrutador, puede darse el caso de que haya un conflicto entre las peticiones de los diferentes host. Esto sucede, por ejemplo, cuando un host solicita tráfico de una determinada fuente y otro host solicita tráfico excluyendo dicha fuente. Por ejemplo, un host1 envía un primer mensaje EXCLUDE({S1},G1) y otro host2 en la misma red Ethernet envía después al mismo enrutador un segundo mensaje EXCLUDE({S1,S2,S3},G1). Si el enrutador, al recibir el segundo mensaje pusiera las fuentes del segundo mensaje {S1,S2,S3} en la "Lista de Exclusión", el host1 dejaría de recibir el tráfico de las fuentes S2 y S3 que sí quería recibir ya que quería recibir todo el tráfico menos el de la fuente S1. Para evitar este problema, el enrutador pone únicamente en la lista "Lista de Exclusión" la intersección del conjunto de fuentes del nuevo mensaje con el conjunto de fuentes que ya estaban en la "Lista de Exclusión" antes de recibir el mensaje. El resto de fuentes EXCLUDE pasan a la "Lista de Solicitadas" y, opcionalmente, el enrutador envía un mensaje "Consulta de Grupo y Fuente Específicos" a los host para preguntar si hay algún host que todavía está interesado en recibir el tráfico de las fuentes S2 y S3 del grupo G1.

[0164] El principio de clasificación de las fuentes EXCLUDE en dos listas, "Lista de Solicitadas" y "Lista de Exclusión", según el valor del "temporizador-de-fuente" es similar al que se aplica en los protocolos IGMPv3 y MLDv2. Las especificaciones RFC 3810 (protocolo MLDv2) citadas al principio contienen una explicación de este principio.

[0165] En la Tabla 1 (al final del documento) se ilustra el funcionamiento de un enrutador mejorado que aplica el protocolo IGMP modificado según la invención. En su estado inicial, el enrutador dispone, para un determinado grupo multidifusión G, de dos registros de estado para dicho grupo multidifusión G porque tiene tanto fuentes INCLUDE como fuentes EXCLUDE. En la Tabla 1, la primera columna "Estado 1" muestra el estado inicial de los registros INCLUDE y EXCLUDE del enrutador; la segunda columna "Mensaje" muestra el contenido de un mensaje "Informe de Pertenencia" recibido por el enrutador; la tercera columna "Estado 2" muestra el estado de dichos registros del enrutador tras haber recibido el mensaje "Informe de Pertenencia"; la cuarta y última columna "Acciones" muestra las acciones que el enrutador realiza tras haber recibido dicho mensaje "Informe de Pertenencia". La tabla contiene 6 filas separadas entre sí por una línea discontinua. Cada fila de la tabla es un ejemplo de funcionamiento del enrutador a partir de un estado inicial y dependiendo del mensaje que ha recibido.

[0166] La Tabla 1 se refiere a cada grupo multidifusión G de forma independiente. Cada grupo multidifusión G tendrá sus propios registros de estado INCLUDE y EXCLUDE que se verán afectados por los mensajes que reciba el enrutador referidos a dicho grupo G.

[0167] En la Tabla 1 se ha utilizado la nomenclatura siguiente:

- (A+B) significa la unión de los conjuntos de fuentes A y B

- (A*B) significa la intersección de los conjuntos de fuentes A y B

- (A-B) significa el conjunto de fuentes A menos las fuentes de A que también se encuentran en B.

- INCLUDE (A), indica que el enrutador tiene un registro INCLUDE con un conjunto de fuentes que denominamos A

- EXCLUDE (X,Y) indica que el enrutador tiene un registro de estado EXCLUDE porque hay fuentes EXCLUDE

- X es la lista "Lista de Solicitadas"

- Y es la lista "Lista de Exclusión"

- GMI es un parámetro denominado "Intervalo de Pertenencia al Grupo" ("*Group Membership Interval*") que contiene un valor de tiempo. Por defecto, toma un valor de 250 segundos.

- LMQT es parámetro denominado "Tiempo de la Última Consulta de Pertenencia" ("*Last Member Query Time*") que contiene un valor de tiempo. Es el tiempo que tiene un host para contestar a un mensaje del tipo "Consulta de Grupo y Fuente Específicos". Pasado este tiempo, si ningún host contesta que tiene interés en esos datos, el enrutador deja de transmitirlos.

- T (S) es el temporizador "temporizador-de-fuente" de la fuente S

- GT es el "temporizador-de-grupo", es decir el temporizador del registro EXCLUDE para todo el grupo multidifusión

- SEND Q(G, S) significa que el enrutador envía un mensaje Q de tipo "Consulta de Grupo y Fuente Específicos" a los host para comprobar si todavía hay algún host interesado en las fuentes S del grupo multidifusión G. Cuando realiza esta acción, el enrutador también disminuye los temporizadores de las fuentes S al valor LMQT. Si el enrutador recibe en respuesta un mensaje mostrando interés en alguna de las fuentes S, entonces inicializa el valor de los temporizadores de dichas fuentes, para las que hay un host interesado, a un valor inicial igual a GMI.

[0168] Una ventaja adicional del protocolo IGMP modificado es que permite al enrutador consultar los dos registros INCLUDE y EXCLUDE antes de enviar un mensaje del tipo "Consulta de Grupo y Fuente Específicos" y eliminar de la lista de fuentes del mensaje algunas fuentes, de modo que incluso puede llegar a suprimir el mensaje si todas las fuentes son eliminadas.

[0169] Para ello, cuando el enrutador recibe un mensaje del tipo BLOCKIN(B) como en el ejemplo mostrado en la fila 4 de la Tabla 1, antes de realizar la acción SEND Q(G, A*B) puede comprobar si existe un registro EXCLUDE para el mismo grupo G y eliminar del mensaje Q(G, A*B) todas las fuentes que no estén en la "Lista de Exclusión" porque significa que alguien las ha pedido mediante un mensaje EXCLUDE.

[0170] De la misma forma, cuando el enrutador recibe un mensaje del tipo BLOCKEX(B) como en el ejemplo mostrado en la fila 6 de la Tabla 1, el enrutador puede consultar la lista de fuentes del registro INCLUDE y usar esa información para suprimir del mensaje Q(G, B-Y) las fuentes existentes en el registro INCLUDE.

[0171] Estas dos comprobaciones pueden eliminar un gran número de mensajes "Consulta de Grupo y Fuente Específicos", reduciendo el tráfico en la red y el número de mensajes que tienen que procesar los hosts y los enrutadores.

8) Compatibilidad con un host IGMPv3

[0172] Los enrutadores que usan el protocolo IGMP modificado, en adelante denominados enrutadores mejorados, pueden comunicarse con los hosts que usan el protocolo IGMPv3. Por ejemplo, una red Ethernet puede tener conectados hosts que funcionan con el protocolo IGMPv3 y hosts que funcionan con el protocolo IGMP modificado según la invención.

[0173] Para ello, un enrutador mejorado capaz de atender los nuevos mensajes del protocolo IGMP modificado también atiende los mensajes utilizados por los protocolos IGMPv3 y MLDv2 que no se utilizan en el protocolo IGMP modificado.

[0174] Cuando el enrutador mejorado recibe un mensaje del tipo ALLOW(B), el enrutador se comporta como si hubiera recibido un mensaje ALLOWIN(B) para las fuentes de B que están en el registro INCLUDE, y se comporta como si hubiera recibido un mensaje ALLOWEX (B) para las fuentes de B que tienen un registro de estado EXCLUDE.

[0175] Si las fuentes de B del mensaje ALLOW(B) están en ambos registros INCLUDE y EXCLUDE del enrutador, el funcionamiento del enrutador puede configurarse para que se comporte como si hubiera recibido los dos mensajes ALLOWIN(B) y ALLOWEX(B) o como si sólo hubiera recibido uno de los dos mensajes. En la configuración del enrutador se permite elegir entre estas dos opciones.

[0176] De la misma forma se gestiona el caso en que el enrutador recibe un mensaje del tipo BLOCK(B): el funcionamiento del enrutador puede configurarse para que se comporte como si hubiera recibido los dos mensajes BLOCKIN(B) y/o BLOCKEX(B)

[0177] Cuando recibe un mensaje TO_IN(B), el enrutador lo trata como si fuera un mensaje IS_IN(B) ya que no necesita cambiar de modo INCLUDE a EXCLUDE y viceversa pues el enrutador puede funcionar en modo dual.

[0178] De la misma forma, cuando recibe un mensaje TO_EX(B), el enrutador lo trata como si fuera un mensaje IS_EX(B).

9) Proxy IGMP mejorado

[0179] El Proxy IGMP mejorado según la invención se diferencia del Proxy IGMP definido en las especificaciones RFC 4605 citadas el principio en que almacena y transmite por separado la información sobre las fuentes INCLUDE y EXCLUDE.

[0180] El Proxy IGMP mejorado puede guardar dos registros para cada interfaz de red y grupo multidifusión:

Registro INCLUDE: (dirección-multidifusión, INCLUDE, {lista de fuentes})
Registro EXCLUDE: (dirección-multidifusión, EXCLUDE, {lista de fuentes})

[0181] La función de un Proxy IGMP es agrupar los mensajes que recibe de sus interfaces de red conectados a los host para enviar un mensaje agrupado o resumido por la interfaz de red que conecta el Proxy IGMP con el enrutador IGMP o con otro Proxy IGMP. Dicha interfaz de red en la dirección del enrutador IGMP suele denominarse interfaz "ascendente" (“upstream”).

[0182] Para ello el Proxy IGMP aplica unas reglas que son similares a las que se han explicado anteriormente en el apartado 3 para deducir los registros procedentes de una interfaz de red de un host a partir de los registros de los sockets, pero con la diferencia de que, al haber dos registros separados, uno para las fuentes INCLUDE y otro para las fuentes EXCLUDE, para deducir la lista de fuentes del registro de fuentes EXCLUDE no es necesario tener en cuenta la información de las fuentes INCLUDE, ya que dicha información está incluida en el registro de fuentes INCLUDE.

[0183] Estas reglas, que el Proxy IGMP mejorado aplica para cada interfaz de red y grupo multidifusión, son las siguientes:

Regla1. Para cada grupo multidifusión, cada registro INCLUDE contiene la unión de todas de fuentes INCLUDE de los mensajes INCLUDE referidos a dicho grupo multidifusión recibidos en todas las interfaces de red del proxy.

Regla 2. Para cada grupo multidifusión, cada registro EXCLUDE contiene la intersección de todas las fuentes EXCLUDE de los mensajes EXCLUDE referidos a dicho grupo multidifusión recibidos en todas las interfaces de red del proxy.

[0184] Para transmitir por separado al enrutador la información sobre los grupos multidifusión que contienen tanto fuentes INCLUDE como fuentes EXCLUDE, se usa el mismo sistema de mensajes con dos "Registros de Grupo" según se ha explicado en el punto 4.

[0185] El Proxy IGMP mejorado puede trabajar de forma simultánea con hosts que usan el protocolo IGMPv3 y con hosts que usan el protocolo IGMP modificado según la invención.

Tabla 1

ESTADO 1	MENSAJE	ESTADO 2	ACCIONES
INCLUDE (A) EXCLUDE (X,Y)	IS_IN (B)	INCLUDE (A+B) EXCLUDE (X,Y)	T(B)=GMI
INCLUDE (A) EXCLUDE (X,Y)	IS_EX (B)	INCLUDE (A) EXCLUDE (B-Y,Y*B)	T(B-X-Y)=GMI DEL(Y-B) GT=GMI
INCLUDE (A) EXCLUDE (X,Y)	ALLOWIN (B)	INCLUDE (A+B) EXCLUDE (X,Y)	T(B)=GMI
INCLUDE (A) EXCLUDE (X,Y)	BLOCKIN (B)	INCLUDE (A) EXCLUDE (X,Y)	SEND Q(G,A*B) T(A*B)=LMQT
INCLUDE (A) EXCLUDE (X,Y)	ALLOWEX (B)	INCLUDE (A) EXCLUDE (X+B,Y-B)	T(B)=GMI
INCLUDE (A) EXCLUDE (X,Y)	BLOCKEX (B)	INCLUDE (A) EXCLUDE (X+(B-Y),Y)	T(B-X-Y)=GT SEND Q(G,B-Y) T(B-X-Y)=LMQT

REIVINDICACIONES

1. Un host (200, 220, 225, 230) que está situado en un sistema de red de datos y que usa un protocolo de enrutamiento multidifusión host-enrutador basado en el protocolo IGMP (*Internet Group Management Protocol*) o el protocolo MLD (*Multicast Listener Discovery*) para comunicarse con un enrutador o proxy multidifusión (260, 240) que está situado entre el host (200, 220, 225, 230) y unas fuentes (295, 296, 297, 298, 299) que envían paquetes multidifusión a al menos una dirección de grupo multidifusión, teniendo el host (200, 220, 225, 230) una interfaz de red (203, 222, 223, 232) y una o más aplicaciones implementadas en ordenador que solicitan datos procedentes de la al menos una dirección de grupo multidifusión y las fuentes (295, 296, 297, 298, 299), almacenando el host (200, 220, 225, 230) para la interfaz de red (203, 222, 223, 232) y para cada dirección de grupo multidifusión un primer registro de fuentes INCLUDE que contiene información sobre listas de fuentes include derivadas por solicitudes de datos realizadas por la una o más aplicaciones implementadas en ordenador y un primer registro de fuentes EXCLUDE que contiene información sobre listas de fuentes exclude derivadas por solicitudes de datos realizadas por la una o más aplicaciones implementadas en ordenador, en donde el host (200, 220, 225, 230) transmite para la interfaz de red (203, 222, 223, 232) y cada dirección de grupo multidifusión "mensajes de pertenencia a fuente específica" ("*source specific membership messages"*) al enrutador o proxy (260, 240) en base a la información del primer registro de fuentes INCLUDE y del primer registro de fuentes EXCLUDE.

2. Un host (200, 220, 225, 230) según la reivindicación 1, en el cual la información del primer registro de fuentes INCLUDE y la información del primer registro de fuentes EXCLUDE son transmitidas dentro de un único mensaje de pertenencia.

3. Un host (200, 220, 225, 230) según la reivindicación 1, en el cual el primer registro de fuentes INCLUDE contiene la unión de todas las listas de fuentes include solicitadas desde la una o más aplicaciones implementadas en ordenador.

4. Un host (200, 220, 225, 230) según la reivindicación 1, en el cual el primer registro de fuentes EXCLUDE contiene la intersección de todas las listas de fuentes exclude solicitadas desde la una o más aplicaciones implementadas en ordenador.

5. Un host (200, 220, 225, 230) según la reivindicación 1, en el cual el host (200, 220, 225, 230) almacena para la interfaz de red (203, 222, 223, 232) y dirección de grupo multidifusión sólo un primer registro de fuentes INCLUDE y sólo un primer registro de fuentes EXCLUDE, conteniendo el primer registro de fuentes INCLUDE la unión de todas las listas de fuentes solicitadas desde las aplicaciones implementadas en ordenador y conteniendo el primer registro de fuentes EXCLUDE la intersección de todas las listas de fuentes exclude solicitadas desde las aplicaciones implementadas en ordenador.

6. Un host (200, 220, 225, 230) según la reivindicación 1, en el cual el host (200, 220, 225, 230) almacena para un socket asociado con una de las aplicaciones implementadas en ordenador un segundo registro de fuentes INCLUDE que comprende (interfaz, dirección-multidifusión, INCLUDE, {lista-de-fuentes}) y un segundo registro de fuentes EXCLUDE que comprende (interfaz, dirección-multidifusión, EXCLUDE, {lista-de-fuentes}).

7. Un host (200, 220, 225, 230) según la reivindicación 1, en el cual el primer registro de fuentes INCLUDE para una interfaz de red (203, 222, 223, 232) y dirección de grupo multidifusión comprende (dirección-multidifusión, INCLUDE, {lista-de-fuentes}) y el primer registro de fuentes EXCLUDE comprende (dirección-multidifusión, EXCLUDE, {lista-de-fuentes}).

8. Un host (200, 220, 225, 230) para ser situado en un sistema de red de datos que comprende fuentes (295, 296, 297, 298, 299) que envían paquetes multidifusión a la menos una dirección de grupo multidifusión, teniendo el host (200, 220, 225, 230) una interfaz de red (203, 222, 223, 232) conectable a un enrutador o proxy multidifusión (260, 240) y siendo capaz de ejecutar una o más aplicaciones implementadas en ordenador que solicitan datos procedentes de la al menos dirección de grupo multidifusión y las fuentes (295, 296, 297, 298, 299), almacenando el host instrucciones ejecutables para 1) comunicarse con el enrutador o proxy multidifusión (260, 240) usando un protocolo de enrutamiento multidifusión host-enrutador basado en el protocolo IGMP (Internet Group Management Protocol) o el protocolo MLD (Multicast Listener Discovery); 2) almacenar para la interfaz de red (203, 222, 223, 232) y cada dirección de grupo multidifusión un primer registro de fuentes INCLUDE que contiene información sobre listas de fuentes include derivadas por solicitudes de datos realizadas por la una o más aplicaciones implementadas en ordenador y un primer registro de fuentes EXCLUDE que contiene información sobre listas de fuentes exclude derivadas por solicitudes de datos realizadas por la una o más aplicaciones implementadas en ordenador, y 3) transmitir para la interfaz de red (203, 222, 223,232) y cada dirección de grupo multidifusión "mensajes de pertenencia a fuente específica" ("source specific membership messages") al enrutador o proxy (260, 240) en base a la información del primer registro de fuentes INCLUDE y del primer registro de fuentes EXCLUDE.

9. Un host (200, 220, 225, 230) según la reivindicación 8, en el cual el host (200, 220, 225, 230) almacena instrucciones ejecutables para transmitir la información del primer registro de fuentes INCLUDE y la información del primer registro de fuentes EXCLUDE dentro de un único mensaje de pertenencia.

10. Un host (200, 220, 225, 230) según la reivindicación 8, en el cual el host (200, 220, 225, 230) almacena instrucciones ejecutables para causar que el primer registro de fuentes INCLUDE contenga la unión de todas las listas de fuentes include solicitadas desde la una o más aplicaciones implementadas en ordenador.

11. Un host (200, 220, 225, 230) según la reivindicación 8, en el cual el host (200, 220, 225, 230) almacena instrucciones ejecutables para causar que el primer registro de fuentes EXCLUDE contenga la intersección de todas las listas de fuentes exclude solicitadas desde la una o más aplicaciones implementadas en ordenador.

12. Un host (200, 220, 225, 230) según la reivindicación 8, en el cual el host (200, 220, 225, 230) almacena instrucciones ejecutables para almacenar para la interfaz de red (203, 222, 223, 232) y dirección de grupo multidifusión sólo un primer registro de fuentes INCLUDE y sólo un primer registro de fuentes EXCLUDE.

13. Un host (200, 220, 225, 230) según la reivindicación 12, en el cual el primer registro de fuentes INCLUDE contiene la unión de todas las listas solicitadas desde la una o más aplicaciones implementadas en ordenador y el primer registro de fuentes EXCLUDE contiene la intersección de todas las listas de fuentes exclude solicitadas desde la una o más aplicaciones implementadas en ordenador.

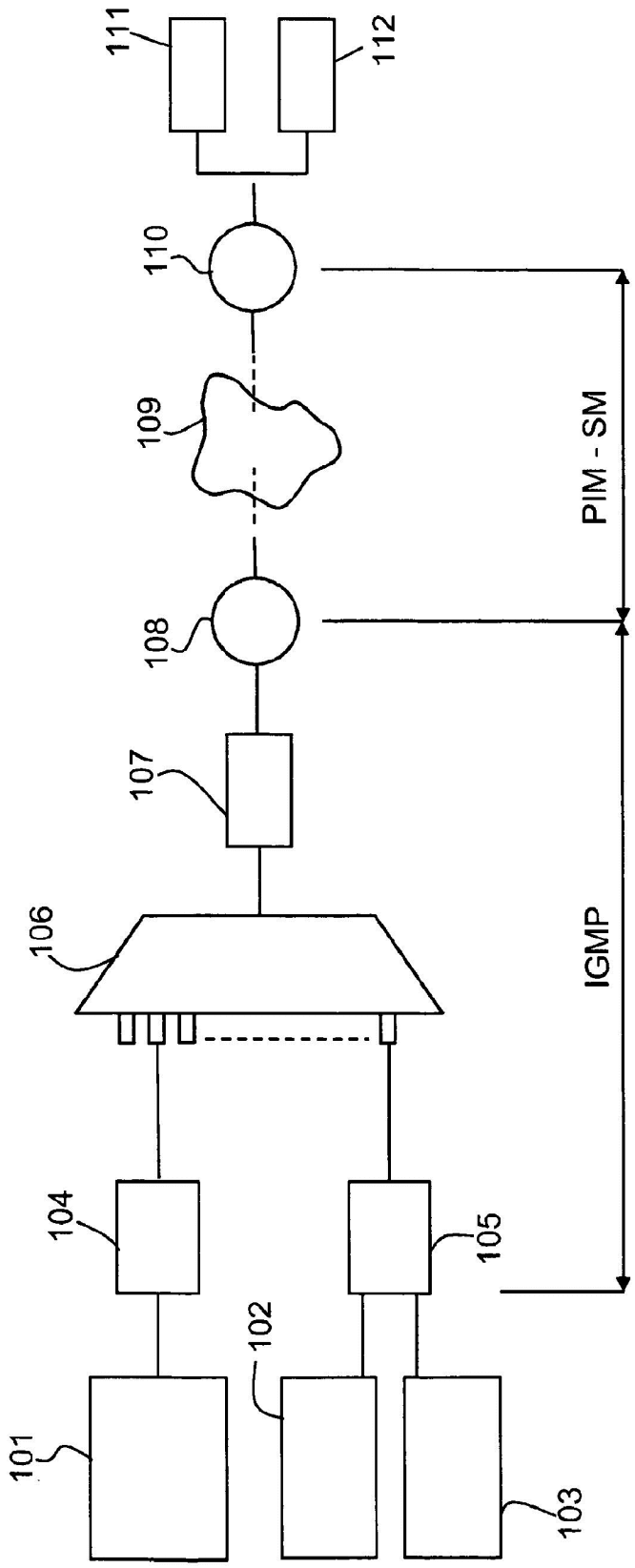

FIG. 1

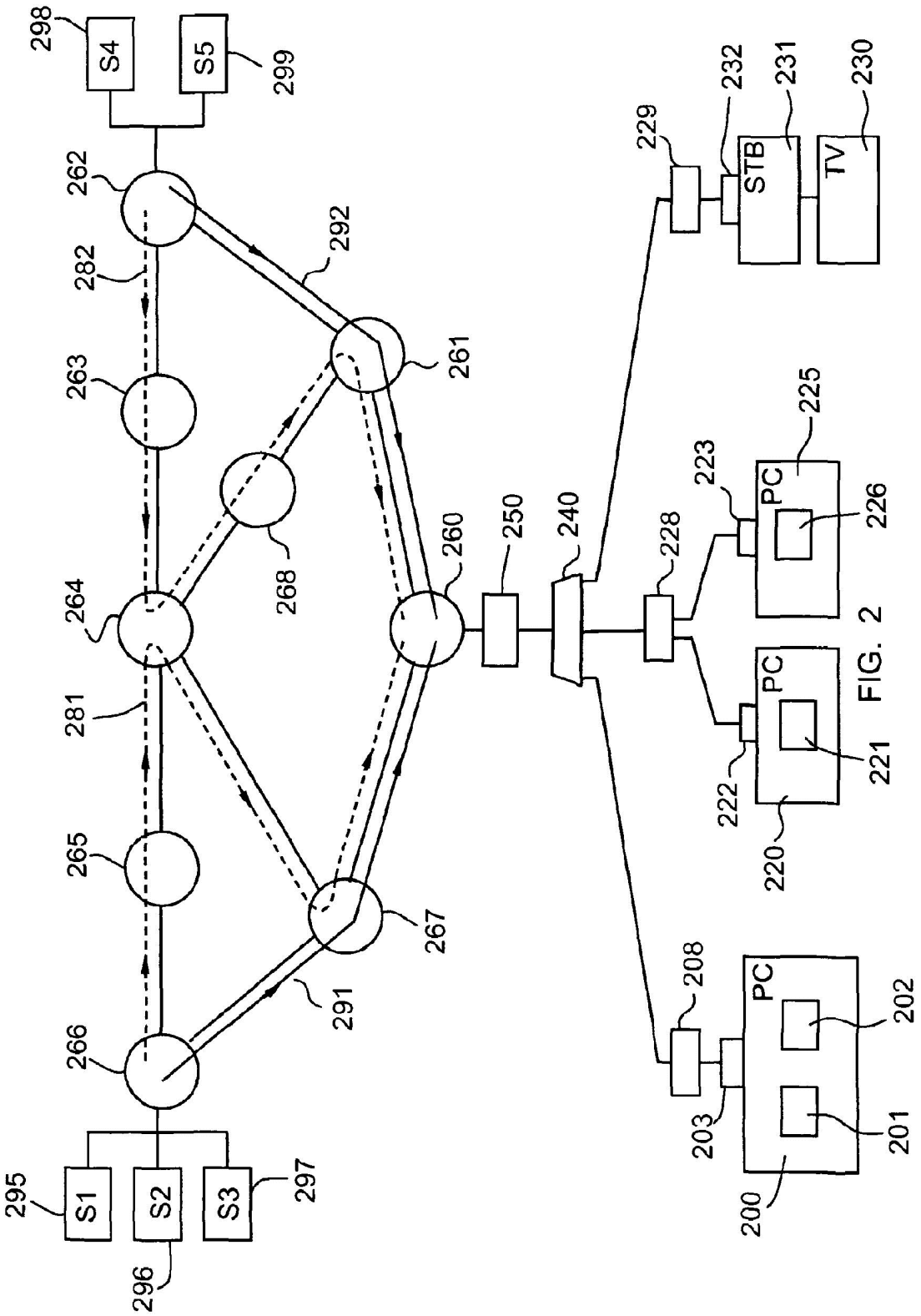
298
S4
S5
299
262
282
292
263
261
264
268
260
250
240
281
265
267
291
266
295
S1
S2
S3
297
296
229
232
231
230
STB
TV
228
223
225
PC
226
221
222
220
208
202
203
201
200

FIG. 2

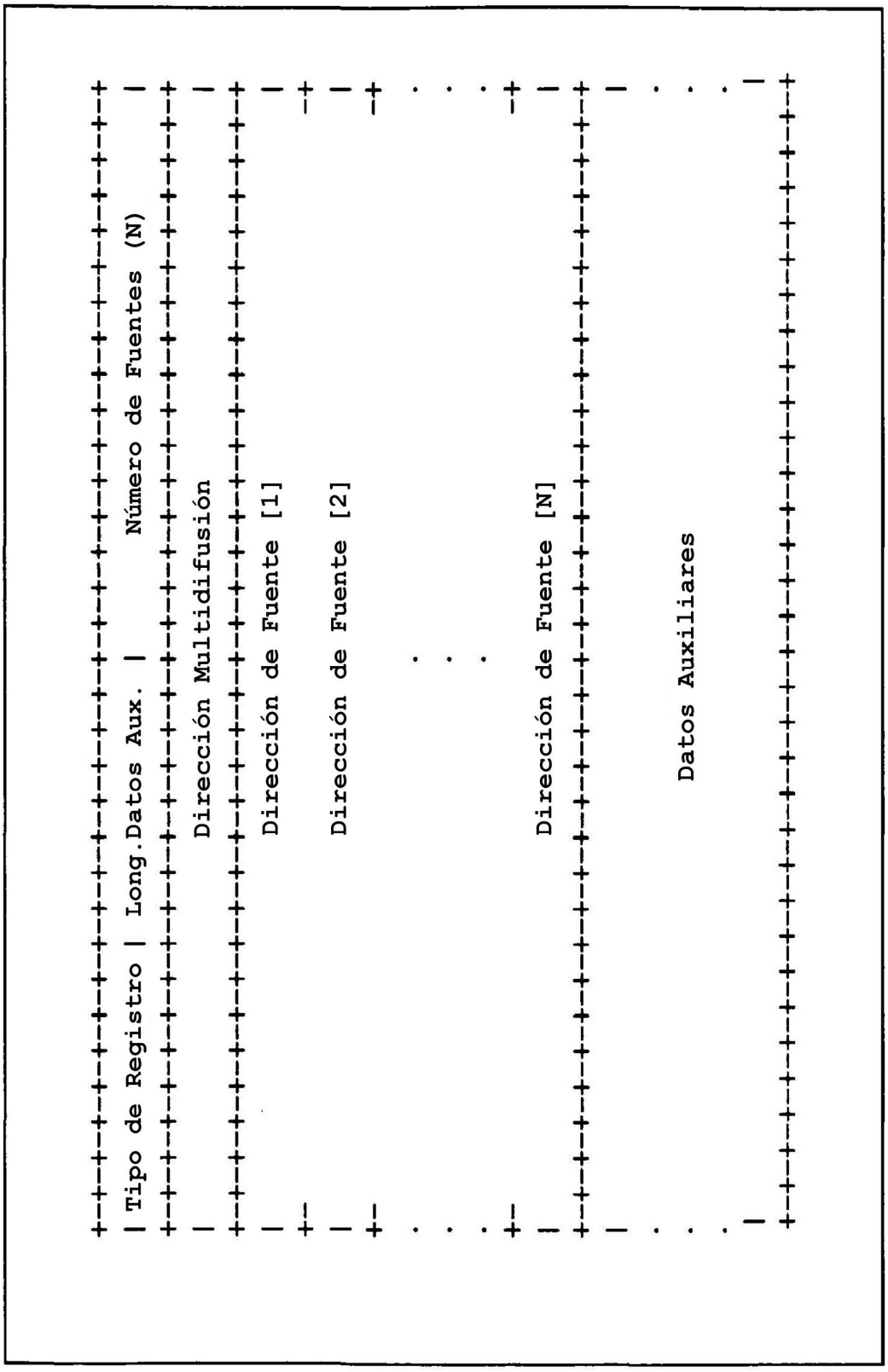
Tipo de Registro
Long.Datos Aux.
Número de Fuentes (N)
Dirección Multidifusión
Dirección de Fuente [1]
Dirección de Fuente [2]
Dirección de Fuente [N]
Datos Auxiliares

FIG. 3

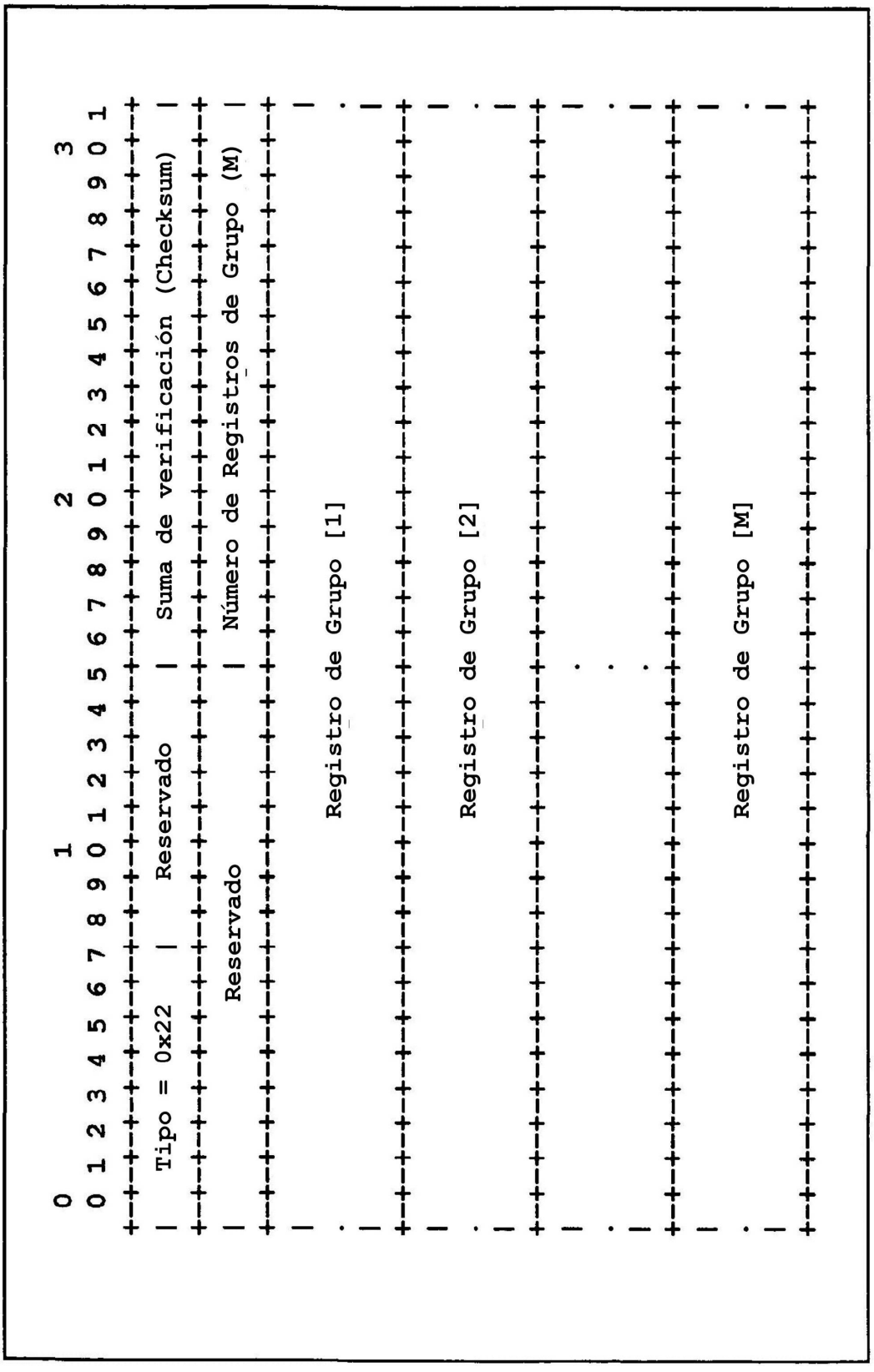
0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Tipo = 0x22
Reservado
Suma de verificación (Checksum)
Reservado
Número de Registros de Grupo (M)
Registro de Grupo [1]
Registro de Grupo [2]
Registro de Grupo [M]

FIG. 4

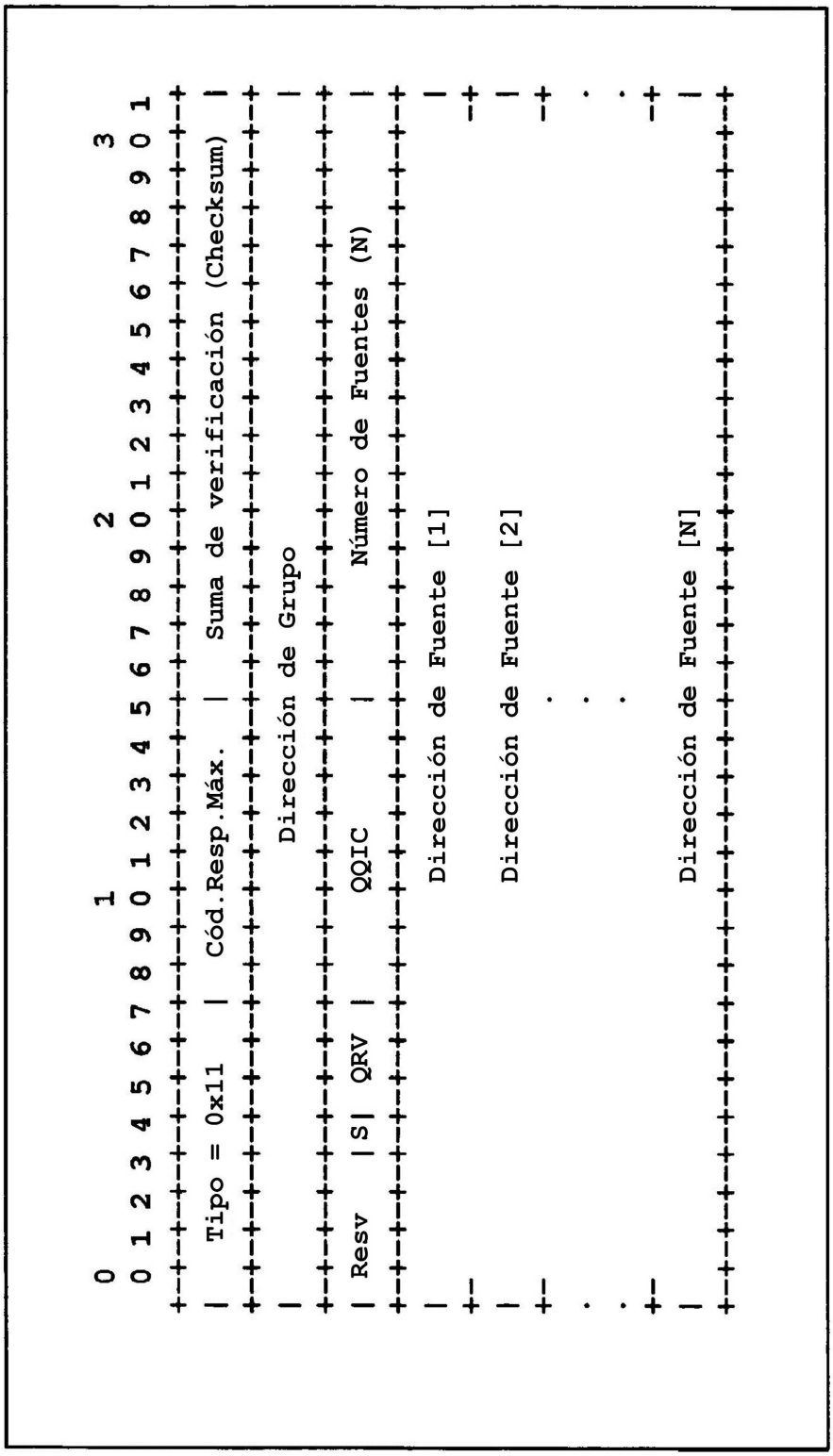
0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Tipo = 0x11
Cód.Resp.Máx.
Suma de verificación (Checksum)
Dirección de Grupo
Resv
S
QRV
QQIC
Número de Fuentes (N)
Dirección de Fuente [1]
Dirección de Fuente [2]
Dirección de Fuente [N]

FIG. 5

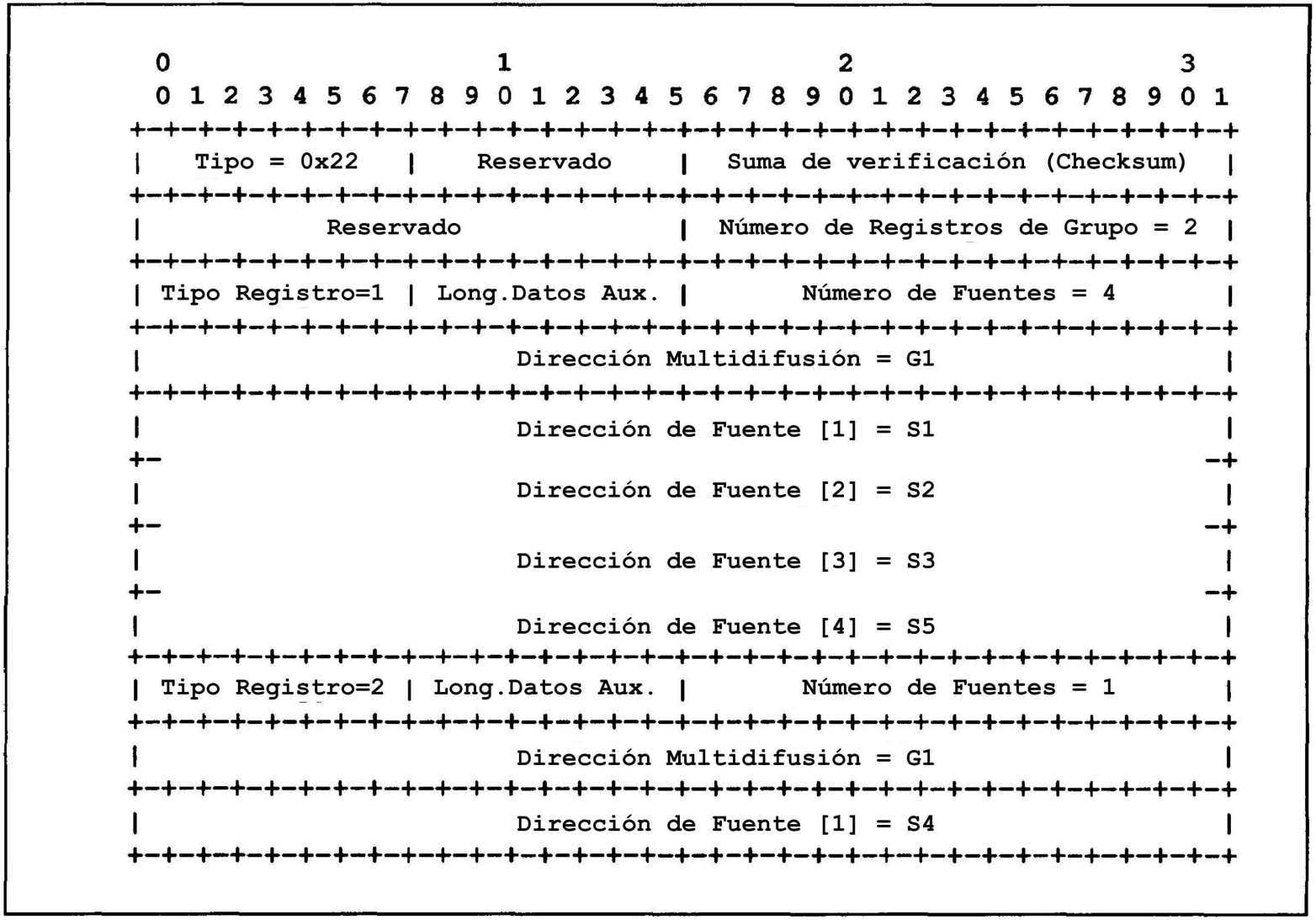
0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Tipo = 0x22
Reservado
Suma de verificación (Checksum)
Reservado
Número de Registros de Grupo = 2
Tipo Registro=1
Long.Datos Aux.
Número de Fuentes = 4
Dirección Multidifusión = G1
Dirección de Fuente [1] = S1
Dirección de Fuente [2] = S2
Dirección de Fuente [3] = S3
Dirección de Fuente [4] = S5
Tipo Registro=2
Long.Datos Aux.
Número de Fuentes = 1
Dirección Multidifusión = G1
Dirección de Fuente [1] = S4

FIG. 6

REFERENCIAS CITADAS EN LA DESCRIPCIÓN

Esta lista de referencias citadas por el solicitante es únicamente para la comodidad del lector. No forma parte del documento de la patente europea. A pesar del cuidado tenido en la recopilación de las referencias, no se pueden excluir errores u omisiones y la EPO niega toda responsabilidad en este sentido.

Documentos de patente citados en la descripción

- US 6434622 B1 **[0027]**
- US 6785294 B1 **[0027]**
- US 6977891 B1 **[0027]**
- US 20030067917 A1 **[0027]**
- US 20050207354 A1 **[0027]**
- US 20060120368 A **[0027]**
- US 20060182109 A1 **[0027]**
- WO 2006001803 A1 **[0027]**
- US 20060262792 A1 **[0028]**

Literatura diferente de patente citada en la descripción

- **B. Cain et al.** *Engineering Task Force, Network Working Group, Request for Comments*, October 2002, vol. 3376 **[0011]**
- **R. Vida et al.** *Engineering Task Force, Network Working Group, Request for Comments*, June 2004, vol. 3810, http://tools.ietf.org/html/rfc3810 **[0012]**
- **B. Fenner et al.** *Engineering Task Force, Network Working Group, Request for Comments*, August 2006, vol. 4605, http://tools.ieff.org/html/rfc4605 **[0013]**
- **B. Fenner et al.** *Engineering Task Force, Network Working Group, Request for Comments*, August 2006, vol. 4601, http://tools.ietf.org/html/rfc4601 **[0014]**
- **H. Holbrook et al.** *Engineering Task Force, Network Working Group, Request for Comments*, August 2006, vol. 4604, hftp://tools.ieff.org/html/rfc4604 **[0026]**