(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 358 546**

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07818731 .7**
(96) Fecha de presentación : **05.10.2007**
(97) Número de publicación de la solicitud: **2078376**
(97) Fecha de publicación de la solicitud: **15.07.2009**

(54) Título: **Router para administrar grupos multicast.**

(30) Prioridad: **26.06.2007 ES 200701775**

(45) Fecha de publicación de la mención BOPI:
11.05.2011

(45) Fecha de la publicación del folleto de la patente:
11.05.2011

(73) Titular/es: **MEDIA PATENTS, S.L.**
Avda. de Roma, 159 - 3º 2ª
08011 Barcelona, ES

(72) Inventor/es: **Fernández Gutiérrez, Álvaro**

(74) Agente: **Zea Checa, Bernabé**

DESCRIPCIÓN

Campo de la invención

[001] La invención se sitúa en el campo de la tecnología multidifusión o "multicast" en redes de datos. Más concretamente, la invención se refiere a un procedimiento de gestión de tráfico multicast en una red de datos, donde unas fuentes emiten datos dirigidos a por lo menos un grupo multicast y una pluralidad de hosts reciben de un router los datos emitidos por una o varias de dichas fuentes que emiten en dicho grupo multicast, dichos hosts y dicho router comunicándose 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 multicast host-router a través de las cuales dicho host puede definir, para dicho grupo multicast, una lista de fuentes incluidas para indicar que desea recibir los datos emitidos por las fuentes de dicha lista y una lista de fuentes excluidas para indicar que desea recibir el tráfico de todas las fuentes de dicho grupo multicast excepto las fuentes de dicha lista.

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

Estado de la técnica

[003] La tecnología multicast 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 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 única dirección asociada a un grupo multicast al que pueden suscribirse los equipos interesados en ser destinatarios de dicha emisión de datos. Esta dirección, denominada dirección multicast o también dirección de grupo multicast, es una dirección IP (Internet Protocol) escogida dentro de un rango que está reservado para las aplicaciones multicast. Los paquetes de datos que han sido enviados por la fuente a la dirección multicast son entonces replicados en los diferentes routers de la red para que lleguen a los destinatarios que se han unido al grupo multicast.

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

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

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

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

[008] Por otra parte, los routers intercambian entre ellos unos mensajes con la finalidad de definir el ruteo que permita encaminar de forma eficiente los datos desde las fuentes hasta los hosts que se han suscrito a un grupo muilticast. Para ello, los routers utilizan unos protocolos específicos, entre los cuales el más extendido es el PIM-SM (Protocol Independent Muticast - Sparse Mode).

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

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

[011] La versión del protocolo IGMP que se utiliza actualmente es la IGMPv3, que está descrita en las especificaciones RFC 3376 editadas 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).

[012] En cuanto al protocolo MDL, la versión que se utiliza actualmente es la MDLv2, que está descrita en las especificaciones RFC 3810 editadas 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).

[013] El funcionamiento de un proxy IGMP que utiliza los protocolos IGMP/MLD está descrito en las especificaciones RFC 4605 editadas 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).

[014] El protocolo PIM-SM utilizado para la comunicación entre los routers está descrito en las especificaciones RFC 4601 editadas 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).

[015] Inicialmente, la tecnología multicast se implementó principalmente para aplicarla al modelo de comunicación muchos-a-muchos, 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.

[016] Posteriormente, la tecnología musticast se implementó para aplicarla al modelo de comunicación uno-a-muchos, conocido como SSM ("Source Specific Multicast"), en el cual una sola fuente emite datos para muchos destinatarios. La radio y la televisión a través de Internet son aplicaciones de SSM. Por esta razón, el SSM presenta actualmente un gran interés.

[017] 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 multicast, si no que sólo podía suscribirse o darse de baja al grupo para todas las fuentes. Los mensajes que enviaba un host a un router eran muy sencillos: Join(G) para recibir tráfico del grupo multicast G y Leave (G) para dejar de recibirlo. Por lo tanto, las primeras versiones del protocolo IGMP no permitían el SSM.

[018] 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 multicast. 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 sí desea recibir la emisión de datos. A las direcciones IP de las fuentes elegidas, siguiendo la terminología de las especificaciones RFC 3376, se las denomina fuentes INCLUDE.
- Un mensaje EXCLUDE, que consiste en indicar las direcciones IP de las fuentes de las cuales no desea recibir la emisión de datos. En este caso, se interpreta que el host desea recibir los datos emitidos por todas las fuentes menos las fuentes indicadas como excluidas en el mensaje. A las direcciones IP de las fuentes excluidas, siguiendo asimismo la terminología de las especificaciones RFC 3376, se las denomina fuentes EXCLUDE.

[019] Para ahorrar memoria, tráfico de datos o por otros motivos, en la versión IGMPv3 se decidió que cada interfaz de red y grupo multicast podría 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.

[020] Para cada grupo multicast G1, una interfaz de red puede recibir varias peticiones diferentes. Cada petición contiene, para el mismo grupo multicast, una lista de fuentes INCLUDE o bien una lista de fuentes EXCLUDE. Para resolver esta situación, y mantener la restricción de que cada interfaz de red sólo puede funcionar bien en modo INCLUDE bien en modo EXCLUDE, el

[021] protocolo IGMPv3 establece que la interfaz de red aplique las reglas siguientes :

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.

[022] Como se entenderá más adelante con la descripción de unas formas de realización de la invención, estas reglas complican considerablemente la comunicación.

[023] En el mutlicast ASM, cuando un host quiere recibir tráfico de un grupo multicast determinado G, hay que resolver el problema técnico siguiente: el host sólo conoce la dirección del grupo multicast G y desconoce las direcciones IP de las fuentes de ese grupo G que están emitiendo datos. Existen diferentes protocolos de comunicación multicast entre routers que solucionan este problema de diferentes maneras. Actualmente, se aplica principalmente el protocolo PIM-SM y se resuelve el problema designando un router denominado "Rendezvous Point", en adelante router RP, como responsable de conocer todas las fuentes de un mismo dominio multicast (conjunto de routers que utilizan un mismo router RP). Para averiguar las direcciones IP de las fuentes, cada router establece una primera comunicación multicast con el router RP para que éste le envíe el tráfico multicast solicitado. Cuando el router recibe los primeros datos del tráfico multicast, descubre las direcciones IP de las fuentes. Entonces, el último router, es decir el router 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 router empieza a recibir los datos en forma duplicada, tanto a través del router RP como directamente a través del camino SPT, corta la comunicación con el router RP y conserva únicamente la comunicación directa a través del camino SPT.

[024] En el SSM el problema de averiguar las direcciones IP de las fuentes de un grupo multicast no existe, ya que es el usuario quien elige las fuentes desde las cuales desea recibir el tráfico multicast. Por lo tanto, los hosts son capaces de indicar al router o al proxy las direcciones IP de la 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 router RP, puesto que los routers pueden conocer las direcciones IP de las fuentes, que son indicadas por los hosts cuando se suscriben al grupo multicast. Por lo tanto, en el SSM es posible aplicar algoritmos más eficientes que los que se utilizan actualmente.

[025] 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 router RP, tal como se ha expuesto anteriormente para el ASM, con el inconveniente de que los procedimientos de ruteo para el ASM son más complicados.

[026] 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 inconveniente 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 multicast SSM y en imponer que en un sistema multicast SSM los hosts no 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 de un mismo grupo multicast.

[027] Se conocen numerosas patentes o solicitudes de patentes que proponen diversas mejoras de las comunicaciones multicast. 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.

Sumario de la invención

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

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

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

[031] Para este propósito, la invención se refiere a un router de acuerdo a la reivindicación 1.

[032] Preferentemente, dicho router utiliza la información de las listas de fuentes incluidas comprendida en dichos mensajes recibidos por el router para solicitar a otros routers el tráfico de datos emitido por dichas fuentes incluidas.

[033] Preferentemente, para solicitar dicho tráfico de datos emitido por dichas fuentes incluidas, dicho router utiliza el protocolo PIM-SIM ("Protocol Independent Muticast - Sparse Mode").

[034] En una forma de realización preferente, al recibir un mensaje que le informa que algún host ya no desea recibir trafico de un determinado grupo multicast y una determinada fuente incluida, dicho router comprueba si existe un registro de fuentes excluidas de dicho grupo multicast y si dicho registro existe y no contiene una fuente excluida con la misma dirección IP que dicha fuente incluida, dicho router continúa transmitiendo dicho trafico, de dicho determinado grupo multicast y dicha determinada fuente incluida, sin enviar un mensaje de tipo "Group-And-Source Specific Query" en el protocolo IGMP para comprobar si hay otro host que todavía quiere recibir dicho tráfico.

[035] Asimismo, en una forma de realización preferente, al recibir un mensaje para actualizar la información del registro de fuentes excluidas, donde dicho mensaje solicita un bloqueo del tráfico de una determinada fuente y grupo multicast, dicho router comprueba si existe un registro de fuentes incluidas de dicho grupo multicast 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 router continúa transmitiendo dicho trafico, de dicho determinado grupo multicast y dicha determinada fuente, sin enviar un mensaje de tipo "Group-And-Source Specific Query" en el protocolo IGMP para comprobar si hay otro host que todavía quiere recibir dicho tráfico.

Breve descripción de los dibujos

[036] Otras ventajas y características de la invención se aprecian a partir de la siguiente descripción en la que, sin ningún carácter limitativo, se relatan unas formas preferentes de realización de la invención haciendo mención de los dibujos que se acompañan. Las figuras muestran:

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

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

Fig. 3, el formato de los mensajes “Membership Query” que envían los routers 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 “Membership Report” que envían los host a los routers, tanto en el protocolo IGMPv3 como en el protocolo IGMP modificado según la invención;

Fig. 5, el formato interno de los bloques de datos “Group Record” contenidos en cada mensaje “Membership Query” o “Membership Report”, en el protocolo IGMPv3;

Fig.6, formato de un mensaje “Membership Report” que corresponde al mensaje que envía el DSLAM 240 al router 260 en el sistema de la Fig. 2, cuando se aplica el protocolo IGMP modificado según la invención.

Descripción detallada de unas formas de realización de la invención

[037] La Fig. 1 muestra un ejemplo básico de un sistema multicast 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 del lado 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 router 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 router 110 que concentra los paquetes de datos emitidos por unas fuentes 111, 112 de un grupo multicast.

[038] Para simplificar, en la Fig. 1 se ha ilustrado un solo conjunto formado por varios hosts 101, 102, 103 conectados a un router 107, y un solo grupo de fuentes 111, 112 conectadas a un router 110. Por supuesto, en realidad un sistema multicast está compuesto por un gran número de estos conjuntos y grupos.

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

[040] En este ejemplo se ha supuesto que los routers 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).

[041] 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 router. Este funcionamiento está descrito en las especificaciones RFC 4605 de la IETF mencionadas al principio.

[042] El funcionamiento básico del sistema multicast ilustrado en la Fig. 1 es el siguiente.

[043] Los hosts 101, 102, 103 envían a los CPE 104, 105 unos mensajes IGMP en los que identifican la dirección multicast del grupo y las direcciones de las fuentes de las que quieren recibir una emisión 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 solo mensaje IGMP. 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 router 108, a través del switch 107, un mensaje IGMP en el que sólo se indican, para cada grupo multicast, las fuentes INCLUDE o EXCLUDE.

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

[045] Como se verá a continuación en un ejemplo más detallado, en el estado de la técnica anterior el router 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

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

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

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

[047] 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 el estado de la técnica anterior, que aplica el protocolo IGMPv3. Posteriormente se hará referencia a este mismo esquema de la Fig. 2 para explicar el funcionamiento según la invención.

[048] El host 200 es un ordenador personal PC en el cual se ejecutan dos aplicaciones 201, 202 que pueden pedir tráfico multicast. 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.

[049] Los hosts 220 y 225 son dos ordenadores personales PC que están equipados cada uno con una tarjeta de red 222, 223 conectada 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 pedir tráfico multicast.

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

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

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

[053] En el ejemplo de la Fig. 2 hay cinco fuentes emisoras 295, 296, 297, 298, 299 que pertenecen a un mismo grupo multicast G1. Para facilitar la explicación, en lo que sigue se 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.

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

[055] Las aplicaciones 201 y 202 que se ejecutan en el host 200 desean recibir las emisiones de datos en el grupo multicast 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).

[056] 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. Como 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).

[057] En principio, 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 ha perdido una información valiosa que estaba contenida en el mensaje IGMP enviado por la aplicación 201: las direcciones IP de las fuentes S1 y S2.

[058] 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.

[059] 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 al que está asociado la aplicación 221. 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).

[060] 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 al que está asociado la aplicación 226. Por lo tanto, la tarjeta de red 223 envía el CPE 228 un mensaje IGMP que contiene la misma información que la petición de la aplicación 226, es decir un mensaje INCLUDE({S3}, G1).

[061] 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).

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

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

EXCLUDE({S4}; G1), proveniente del CPE 208

INCLUDE ({S3, S5}; G1), proveniente del CPE 228

INCLUDE({S1}, G1), proveniente del CPE 229

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

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

[066] En la ejemplo de la Fig. 2, al utilizar inicialmente el árbol RPT el router 260 recibe las emisiones de las fuentes S1, S2 y S3 a través del camino 281 indicado en trazo discontinuo, y recibe la emisión de la fuente S5 a través del camino 282 indicado en trazo discontinuo. El router 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 en trazo continuo.

[067] El router 260 no conoce las direcciones IP de las fuentes incluidas, ya que sólo ha recibido del DSLAM 240 un mensaje EXCLUDE({S4}; G1). Por tanto, el router 260 no puede pedir el tráfico 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 router funciona únicamente en multicast SSM, no aceptará el mensaje EXCLUDE. Además, si el router es un router simplificado que sólo es capaz de conectar directamente con las fuentes no podrá hacerlo si no conoce las direcciones IP de las mismas.

[068] Las condiciones que establece 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 multicast 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
  }
}
```

[069] 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.

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

[071] 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)

[072] Esta condición no configurable establece que un router sólo cambia del árbol RPT al árbol SPT para un determinado canal (S,G) si hay alguna interfaz de red del router que ha recibido un mensaje IGMP INCLUDE (S,G) o si hay una interfaz de red del router 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). Como esta condición no configurable se refiere únicamente a los mensajes IGMP, el único router que puede iniciar un cambio al árbol SPT para establecer una conexión directa con el router de entrada del canal (S, G) es el router que recibe los mensajes IGMP, es decir el router 260 en el ejemplo de la Fig. 2. En los routers que no reciben mensajes IGMP directamente por una de sus interfaces de red, esta condición no se dará nunca, de manera que estos routers nunca iniciarán un cambio al árbol SPT.

[073] En el ejemplo de la Fig. 2, el único mensaje que recibe el router 260 es EXCLUDE({S4},G1), con lo cual no se cumple dicha condición no configurable. Consecuentemente, el router 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 router RP 264, en lugar de hacerlo por los caminos mas cortos 291, 292. Se distribuye pues el tráfico de una forma poco eficiente, y además se sobrecarga innecesariamente el router RP.

[074] 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 ruteo. El experto en la materia entenderá sin dificultad que esta situación se produce igualmente en otros sistemas multicast con combinaciones diferentes de las que se muestran en la Fig. 2.

Protocolo IGMP modificado según la invención

[075] 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.

[076] 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.

[077] 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 el principio, y sólo se exponen 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.

[078] 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 "Membership Query".

7) Descripción del protocolo para los routers.

8) Compatibilidad con un host IGMPv3

9) Proxy IGMP mejorado

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

[079] 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 multicast:

IPMulticastListen (socket, interface, multicast-address, filter-mode, {source-list})

donde:

"socket" es una 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.

"interface" es un identificador local de la tarjeta de red o interfaz de red en la cual se indican las fuentes de datos multicast que se quiere recibir.

"multicast-address" es la dirección del grupo multicast.

"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 "source-list" 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 "source-list" como EXCLUDE; esto quiere decir que debe enviarse el tráfico de todas las fuentes que emiten en el grupo multicast, excepto las fuentes de la lista.

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

[080] Las especificaciones RFC 3376 explicitan claramente que para una determinada combinación de socket, interfaz de red y grupo multicast, sólo puede haber un "filter mode", que puede ser INCLUDE o EXCLUDE.

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

(interface, multicast-address, filter-mode, {source-list})

[082] Para cada socket, el "filter-mode" del registro sólo puede ser INCLUDE o bien EXCLUDE.

[083] Asimismo, el sistema guarda un registro para cada interfaz de red. Este registro contiene la información siguiente:

(multicast-address, filter-mode, {source-list})

[084] Para cada interfaz de red y grupo multicast, el "filter-mode" del registro sólo puede ser INCLUDE o bien 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 “filter-mode” 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 “filter-mode” INCLUDE para el grupo G1 y la lista de fuentes es la unión de todas las fuentes INCLUDE.

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

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

IPMulticastListen (socket, interface, multicast-address, filter-mode, {source-list})

pero con la diferencia de que para cada socket y cada interfaz de red el sistema guarda dos registros: uno para el “filter-mode” EXCLUDE y otro para el “filter-mode” INCLUDE.

[087] El sistema guarda pues dos registros para cada socket :

Registro INCLUDE: (interface, multicast-address, INCLUDE, {source-list})

Registro EXCLUDE: (interface, multicast-address, EXCLUDE, {source-list})

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

Registro INCLUDE: (multicast-address, INCLUDE, {source-list})

Registro EXCLUDE: (multicast-address, EXCLUDE, {source-list})

[088] 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 multicast 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 el estado de la técnica anterior con el protocolo IGMPv3.

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

2) Forma de borrar un registro

[090] En el protocolo IGMPv3, para borrar un registro de un determinado grupo G1 se envía un mensaje de tipo INCLUDE con una lista de fuentes vacía: INCLUDE ({ }, G1). Por otra parte, 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 timer para cada grupo multicast que es distinto de cero si el estado del registro es EXCLUDE. Cuando el timer llega a cero el registro cambia del modo EXCLUDE al modo INCLUDE.

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

[092] Para borrar automáticamente un registro EXCLUDE de un determinado grupo G1, en el protocolo IGMP modificado los registros EXCLUDE también tienen un timer para cada grupo multicast, 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, cuando el timer llega a cero el registro EXCLUDE se borra.

[093] 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 routers, que se actualizan mediante mensajes IGMP.

[094] Para borrar registros EXCLUDE mediante la función IPMulticastListen, en el protocolo IGMP modificado se ha incorporado un nuevo parámetro de “filter-mode" denominado Filter_Delete_Exclude. Cuando la función IPMulticastListen recibe una llamada con este parámetro, sabe que debe borrar el registro EXCLUDE del grupo multicast que se indique en el “multicast-address”.

[095] Para borrar registros EXCLUDE de proxys y routers mediante mensajes IGMP, en el protocolo IGMP modificado se ha definido un nuevo valor para el campo “Group Record Type” de los mensajes “Membership Report” con la siguiente descripción abreviada:

7 DELEX - Type MODE_IS_DELETE_EXCLUDE

Este nuevo valor se añade a los valores 1 a 6 del campo “Group Record Type” que ya existen en el protocolo IGMPv3 con las siguientes descripciones abreviadas (apartado 4.2.12 de la especificaciones RFC 3376):

1 IS_IN (x) - Type MODE_IS_INCLUDE

2 IS_EX (x) - Type MODE_IS_EXCLUDE

3 TO_IN (x) - Type CHANGE_TO_INCLUDE_MODE

4 TO_EX (x) - Type CHANGE_TO_EXCLUDE_MODE

5 ALLOW (x) - Type ALLOW_NEW_SOURCES

6 BLOCK (x) - Type BLOCK_OLD_SOURCES

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

3) Reglas para derivar los registros de las interfaces de red

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

Registro INCLUDE: (multicast-address, INCLUDE, {source-list})

Registro EXCLUDE: (multicast-address, EXCLUDE, {source-list})

donde "multicast-address" es la dirección del grupo multicast y "source-list" es la lista de fuentes.

[097] 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 multicast.

[098] Para cada interfaz de red y grupo multicast el protocolo IGMP modificado aplica las reglas siguientes:

Regla1. Para cada grupo multicast, 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 multicast, 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

[099] Para simplificar la explicación, en el presente apartado se describen los mensajes IGMP entre el router 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.

[100] Para la comunicación entre un host y un router 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.

[101] La Fig. 3 muestra el formato de los mensajes que envían los routers a los hosts en el protocolo IGMPv3. Estos mensajes se denominan “Membership Query”. El formato mostrado en la Fig. 3 se aplica tanto al protocolo IGMPv3 como al protocolo IGMP modificado.

[102] La Fig. 4 muestra el formato de los mensajes que envían los hosts a los routers en el protocolo IGMPv3. Estos mensajes se denominan “Membership Report”. El formato mostrado en la Fig. 4 se aplica tanto al protocolo IGMPv3 como al protocolo IGMP modificado.

[103] La Fig. 5 muestra el formato interno de los bloques de datos denominados “Group Record” que están contenidos en cada mensaje “Membership Report”. El campo “Group Address” contiene la dirección de grupo multicast. Los campos “Source Address” contienen la información sobre las fuentes. El campo “Number of Sources” indica el número de campos “Source Address” que hay en cada “Group Record”. El formato mostrado en la Fig. 5 se aplica al protocolo IGMPv3.

[104] En el protocolo IGMP modificado, cuando se envía un mensaje del tipo “Membership Report”, 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 multicast se envían dos “Group Record”, 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 multicast, el sistema puede emitir un mensaje con dos “Group Record” diferentes para un mismo grupo o dirección multicast: uno de los "Group Record" transmite la información de las fuentes INCLUDE y el otro transmite la información de las fuentes EXCLUDE.

[105] En el protocolo IGMPv3 los routers envían un mensaje "Membership Query" de tipo "General Query" para interrogar a los hosts sobre su estado. En respuesta a este mensaje, los hosts envían un mensaje de estado "Membership Report" de tipo “Current-State Record”. En el protocolo IGMP modificado se mantiene este sistema, pero el mensaje “Current-State Record” que envía el host puede contener dos “Group Record” para un mismo grupo multicast: 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 "Record Type", respectivamente:

Record Type = 1 = MODE_IS_INCLUDE

Record Type = 2 = MODE_IS_EXCLUDE

[106] Se transmite así la información de los dos registros en un mismo mensaje “Current-State Record”.

[107] En el protocolo IGMPv3, los hosts envían unos mensajes “Source-List-Change Record” para informar de los cambios que ha habido en las fuentes INCLUDE y EXCLUDE. A diferencia de los mensajes "Current-State Record", los mensajes “Source-List-Change Record” no se envían en respuesta a un mensaje "Membership Query" enviado por el router, si no que los envía un host para indicar que se ha producido un cambio en su registro de fuentes.

[108] En el protocolo IGMP modificado, los hosts también envían mensajes “Source-List-Change Record”, como en el protocolo IGMPv3, pero con la diferencia siguiente: como puede haber dos registros distintos para un mismo grupo multicast (un registro INCLUDE y un registro EXCLUDE) el mensaje “Source-List-Change Record” debe indicar a cual de

los dos registros se refiere. Para ello, en el protocolo IGMP modificado se definen cuatro nuevos “Group Record Type”, con las siguientes expresiones abreviadas:

8 ALLOWIN (x) - Type ALLOW_NEW_SOURCES_INCLUDE

9 BLOCKIN (x) - Type BLOCK_OLD_SOURCES_INCLUDE

10 ALLOWEX (x) - Type ALLOW_NEW_SOURCES_EXCLUDE

11 BLOCKEX (x) - Type BLOCK_OLD_SOURCES_EXCLUDE

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

[109] Los nuevos "Group Record Type" 8 y 9, es decir las expresiones ALLOWIN (x) y BLOCKIN (x), se utilizan para enviar mensajes que añadan o quiten, respectivamente, elementos de las listas de fuentes en los registros INCLUDE.

[110] Los nuevos "Group Record Type" 10 y 11, es decir las expresiones ALLOWEX (x) y BLOCKEX (x), se utilizan para enviar mensajes para que se permita o se bloquee, respectivamente, el tráfico emitido por la fuente x.

[111] La Fig. 6 muestra un ejemplo de un mensaje “Membership Report” que corresponde al mensaje que envía el DSLAM 240 al router 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 router 260 y los hosts 200, 220, 225 y 231. Por tanto, en este caso la explicación que precede acerca de los mensajes IGMP entre un router y un host se aplica reemplazando dicho host por el DSLAM 240. Un Proxy IGMP se comporta como un host en sus comunicaciones con un Router IGMP y se comporta como un router IGMP en sus comunicaciones con un host.

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

[113] En el PC 200, si las aplicaciones 201 y 202 utilizan respectivamente el socket1 y el socket2, los registros de los estados 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 })

[114] El registro del 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 })

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

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

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

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

[117] El registro del 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 })

[118] En el STB 231, el registro del 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 })

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

[120] El registro del 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 })

[121] En respuesta a un mensaje “General Query” enviado por el router 260, el DSLAM 240 envía al router 260 el mensaje representado en la Fig. 6, que se analiza a continuación.

[122] Type = = 0x22 indica que es un “Membership Report” y Number of Group Records = 2 indica que se envían dos bloques de datos o “Group Record” para el mismo grupo multicast G1. Uno de los “Group Record” contiene la información de las fuentes INCLUDE y el otro la de las fuentes EXCLUDE. El primer “Group Record” tiene un “Record Type” igual a 1. Esto significa que es del tipo “MODE_IS_INCLUDE”, es decir que contiene la información de las fuentes INCLUDE. En este bloque de datos “Number of Sources” es igual a 4, lo que significa que se va a enviar información de cuatro fuentes INCLUDE. El grupo multicast G1 se indica en el campo “Multicast Address”. Los cuatro campos “Source Address [1]” a “Source Address [4]” contienen la información de las cuatro fuentes INCLUDE: S1, S2, S3 y S5. A continuación viene un segundo “Group Record” con un “Record Type” igual a 2. Esto significa que es del tipo MODE_IS_EXCLUDE, es decir que contiene la información de las fuentes EXCLUDE. “Number of Sources” es igual a 1, lo que significa que se va a enviar información de una fuente EXCLUDE. El grupo multicast G1 se indica en el campo “Multicast Address”. El campo “Source Address [1]” contiene la información de la fuente EXCLUDE: S4.

[123] El router 260 ha recibido la 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.

[124] Por defecto se configura la condición SwitchToSptDesired(S,G) del protocolo PIM-SM, que 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 desde 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 router 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 que le indica que quiere recibir el tráfico de todas la fuentes del grupo G y no habrá recibido un mensaje IGMP EXCLUDE (S,G).

[125] Por tanto, cuando se aplica el protocolo IGMP modificado todos los routers 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.

[126] Así, 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.

[127] Opcionalmente, el router 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 directamente utilizar el árbol SPT. Para ello basta con hacer que la función SwitchToSptDesired(S,G) sea cierta siempre.

[128] Además, opcionalmente, cada host puede indicar al router 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 multicast que queda fuera del rango de direcciones multicast y en el cual no se pone una dirección multicast, sino un mensaje. Por ejemplo, se ponen los dos primeros bytes de la dirección multicast a 0 y se usan los segundos dos bytes para enviar el mensaje al router, asociando a estos segundos dos bytes el siguiente significado:

100 = conectar directamente mediante el árbol SPT

200 = usar la configuración por defecto del router 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

[129] El router detecta que la dirección está fuera del rango de direcciones multicast 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 multicast que viene a continuación en el mismo “Group Record”.

5) Comportamiento cuando cambia la información de un registro

[130] En el protocolo IGMP modificado, cuando cambia el registro del estado de una interfaz de red para un determinado grupo multicast, el sistema simplemente debe transmitir los cambios enviando un mensaje “Source-List-Change Record” como se indica en el apartado anterior.

[131] En el protocolo IGMPv3 este proceso es más complejo porque el sistema debe tener en cuenta el "filter-mode" 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 se almacenan y transmiten por separado.

6) Comportamiento cuando un host recibe un mensaje "Membership Query"

[132] Tanto en el protocolo IGMPv3 como en el protocolo IGMP modificado los routers envían mensajes denominados “Membership Query” a los hosts para que éstos informen de los canales y grupos multicast que desean recibir. En el protocolo IGMP modificado, los hosts envían a los routers 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.

[133] Para evitar que todos los hosts respondan al mismo tiempo, se usan varios timers que retrasan las respuestas de los hosts para repartirlas durante un espacio de tiempo que está especificado en el mensaje “Membership Query”. Esto funciona igual en el protocolo IGMP modificado y en el protocolo IGMPv3.

[134] Existen tres tipo de mensajes “Membership Query”: "General Query", "Group-Specific Query" y "Group-and-Source-Specific Query".

[135] Los mensajes de tipo "General Query" son enviados por el router cada cierto tiempo (por defecto 125 segundos) para que todos los hosts informen de los grupos y canales multicast que quieren recibir enviando unos mensajes “Membership Report” que se denominan “Current-State Record”. Los mensajes con los que responde el host a una petición "General Query" incluyen bloques de datos denominados "Group Records", que pueden ser de dos tipos:

Record Type = 1 MODE_IS_INCLUDE

Record Type = 2 MODE_IS_EXCLUDE

[136] Como se ha visto anteriormente, en un solo mensaje o “Membership Report”, como el que se muestra en la Fig. 4, se envían varios bloques de datos denominados “Group Record” como el que se muestra en la Fig. 5. El primer campo de la Fig. 5, es decir del “Group Record”, es el campo “Record Type” que indica el significado de cada bloque de datos (en el ejemplo de la Fig. 5 el campo "Record Type" es el campo indicado como "Type").

[137] En el protocolo IGMPv3, como cada grupo multicast sólo puede estar en estado INCLUDE o en estado EXCLUDE, cada host sólo envía, para cada grupo multicast, un “Group Record”, con "Record Type" de valor 1 o de valor 2 según sea el estado del grupo INCLUDE o EXCLUDE, respectivamente.

[138] En el protocolo IGMP modificado, gracias a que la información de las fuentes INCLUDE y EXCLUDE se almacena y envía separadamente, es posible que un host necesite enviar dos “Group Record” para un mismo grupo multicast: un primer “Group Record” con Record Type = 1 para informar de las fuentes INCLUDE y un segundo “Group Record” con Record Type = 2 para informar de las fuentes EXCLUDE. Esto se puede ver en la Fig. 6, donde existen dos “Group Record” para el mismo grupo multicast G1.

[139] Para los mensajes de tipo "Group-Specific Query" y "Group-and-Source-Specific Query", 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 “Group Record”.

7) Descripción del protocolo para los routers

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

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

[142] El protocolo IGMP modificado permite a los routers usar mejor los algoritmos de ruteo, gracias a que los routers reciben desde los hosts una información detallada de las fuentes INCLUDE y EXCLUDE. Los routers ejecutan el protocolo IGMP en todas las redes a las que están directamente conectados. Si un router multicast 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 router ya no trabaja exclusivamente en un modo INCLUDE o EXCLUDE para cada grupo multicast 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.

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

Registro INCLUDE: (multicast-address, INCLUDE, {lista de fuentes y timers})

Registro EXCLUDE: (multicast-address, group-timer, EXCLUDE, {lista de fuentes y timers})

donde {lista de fuentes y timers} es una lista de elementos (source-address, source-timer), siendo "source-address" la dirección IP de una fuente y siendo "source-timer" un timer asociado a dicha fuente,

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

[145] Los dos registros, INCLUDE y EXCLUDE, almacenados en el router contienen pues un timer "source-timer" asociado a cada fuente "source-address".

[146] Como se ha expuesto anteriormente en el punto 2 referente a las formas de borrar un registro, cada registro EXCLUDE asociado a un grupo multicast contiene, además, un timer "group-timer" que sirve para eliminar el registro de estado EXCLUDE cuando pasa un determinado tiempo sin que el router reciba reports con peticiones de tráfico de tipo EXCLUDE.

[147] Como se ha explicado anteriormente, los routers envían periódicamente a los hosts unos mensajes denominados “Membership Query”, como el de la Fig. 3, para que los hosts contesten informando de los grupos y fuentes de las que desean recibir tráfico multicast. Los hosts también pueden enviar mensajes al router para solicitar tráfico multicast sin esperar a que el host envíe un mensaje “Membership Query”.

[148] El router utiliza los timers para asegurarse de que, tras haber enviado un mensaje “Group Specific Query” o un mensaje “Group and Source Specific Query”, todos los hosts han tenido tiempo suficiente para contestar a dicho mensaje. El valor de los timers va disminuyendo con el tiempo y si el router recibe de un host un mensaje “Membership Report” el router vuelve a reiniciar los timers correspondientes.

[149] En el registro INCLUDE los timers funcionan de la manera siguiente: para una determinada interfaz de red, un determinado grupo multicast y una determinada fuente incluida "source-address", mientras el "source-timer" sea mayor que cero el router continuará transmitiendo por dicha interfaz de red el tráfico multicast del canal (fuente, grupo multicast); cuando el “source-timer” llegue a cero, el router dejará de transmitir dicho tráfico y eliminará la fuente de la lista de fuentes INCLUDE de ese grupo multicast.

[150] En el registro EXCLUDE los timers funcionan de forma parecida, pero con la diferencia de que las fuentes EXCLUDE se clasifican en dos listas: una primera lista denominada “Requested List” que contiene las fuentes cuyo timer "source-timer" tiene un valor mayor que cero y una segunda lista denominada “Exclude List" que contiene las fuentes cuyo timer "source-timer" tiene valor cero.

[151] Para cada grupo Gi, el router transmite todo el tráfico solicitado por las fuentes INCLUDE. Si además hay un registro EXCLUDE para el grupo Gi, el router transmite además todo el tráfico restante del grupo Gi excepto las fuentes EXCLUDE de la lista "Exclude List".

[152] El motivo de que exista una lista “Requested List” es que en una red con varios hosts enviando mensajes a un Router 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 router un segundo mensaje EXCLUDE({S1,S2,S3},G1). Si el router, al recibir el segundo mensaje pusiera las fuentes del segundo mensaje{S1,S2,S3} en la lista "Exclude List", 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 router pone únicamente en la lista "Exclude List" la intersección del conjunto de fuentes del nuevo mensaje con el conjunto de fuentes que había en la lista "Exclude List" antes de recibir el mensaje. El resto de fuentes EXCLUDE pasan a la lista "Requested List" y, opcionalmente, el router envía un mensaje "Group-And-Source Specific Query" 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.

[153] El principio de clasificación de las fuentes EXCLUDE en dos listas “Requested List” y “Exclude List" según el valor del timer "source-timer" es análogo 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.

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

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

[156] 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 router tiene un registro INCLUDE con un conjunto de fuentes que denominamos A
- EXCLUDE (X,Y) indica que el router tiene un registro de estado EXCLUDE porque hay fuentes EXCLUDE
- X es la lista “Requested List”
- Y es la lista “Exclude List”
- GMI es un parámetro denominado “Group Membership Interval” que contiene un valor de tiempo. Por defecto, toma un valor de 250 segundos.
- LMQT es parámetro denominado "Last Member Query Time" que contiene un valor de tiempo. Es el tiempo que tiene un host para contestar a un mensaje del tipo "Group-And-Source Specific Query". Pasado este tiempo, si ningún host contesta que tiene interés en esos datos, el router deja de transmitirlos.
- T (S) es el timer "source timer" de la fuente S
- GT es el "Group Timer", es decir el timer del registro EXCLUDE para todo el grupo multicast
- SEND Q(G, S) significa que el router envía un mensaje "Group-And-Source specific Query" a los host para comprobar si todavía hay algún host interesado en las fuentes S del grupo multicast G. Cuando realiza esta acción, el router también disminuye los timers de las fuentes S al valor LMQT. Si el router recibe en respuesta un mensaje mostrando interés en alguna de las fuentes S, entonces inicializa el valor de los timers de dichas fuentes, para las que hay un host interesado, a un valor inicial igual a GMI.

[157] Una ventaja adicional del protocolo IGMP modificado es que permite al router consultar los dos registros INCLUDE y EXCLUDE antes de enviar un mensaje del tipo "Source-And-Group Specific Query" 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.

[158] Para ello, cuando el router 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 "Exclude List" porque significa que alguien las ha pedido mediante un mensaje EXCLUDE.

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

[160] Estas dos comprobaciones pueden eliminar un gran número de mensajes "Group-And-Source Specific Query", reduciendo el tráfico en la red y el número de mensajes que tienen que procesar los hosts y los routers.

8) Compatibilidad con un host IGMPv3

[161] Los routers que usan el protocolo IGMP modificado, denominados en lo que sigue routers mejorados, pueden comunicarse con los hosts que usan el protocolo IGMPv3. Por ejemplo, una red ethernet puede tener conectados unos hosts que funcionan con el protocolo IGMPv3 y unos hosts que funcionan con el protocolo IGMP modificado según la invención.

[162] Para ello, un router 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.

[163] Cuando el router mejorado recibe un mensaje del tipo ALLOW(B), el router se comporta con 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.

[164] Si las fuentes de B del mensaje ALLOW(B) están en ambos registros INCLUDE y EXCLUDE del router, el funcionamiento del router 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 router se permite elegir entre estas dos opciones.

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

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

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

9) Proxy IGMP mejorado

[168] 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 de las fuentes INCLUDE y EXCLUDE.

[169] Para cada interfaz de red y grupo multicast el Proxy IGMP mejorado puede guardar dos registros :

Registro INCLUDE: (multicast-address, INCLUDE, {lista de fuentes})

Registro EXCLUDE: (multicast-address, EXCLUDE, {lista de fuentes})

[170] 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 router IGMP o con otro Proxy IGMP. Dicho interfaz de red en la dirección del router IGMP se suele denominar interfaz “upstream”

[171] 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 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 se recoge en el registro de fuentes INCLUDE.

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

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

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

[173] Para transmitir por separado al router la información del los grupos multicast que contienen tanto orígenes INCLUDE como fuentes EXCLUDE, se usa el mismo sistema de mensajes con dos "Group Record" que se ha explicado en el punto 4.

[174] El Proxy IGMP mejorado puede trabajar de forma simultánea con unos hosts que usan el protocolo IGMPv3 y con unos 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(X-B) 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 router multicast (260) que tiene una o más interfaces de red “downstream” y situado en una red de datos entre fuentes (295,296,297,298,299) que transmiten paquetes multicast dirigidos a por lo menos una dirección de grupo multicast y uno o más hosts (200,220,225,230) que solicitan, de al menos una de las fuentes, los datos multicast enviados a por lo menos una dirección de grupo multicast,

el router multicast (260) caracterizado porque está adaptado para:

- almacenar para una interfaz de red “downstream” y dirección de grupo multicast un registro de fuentes INCLUDE que contiene información acerca de las listas de fuentes INCLUDE derivada de las solicitudes de datos realizadas por los uno o más hosts (200,220,225,230) y un registro de fuentes EXCLUDE que contiene información acerca de las listas de fuentes EXCLUDE derivadas de las solicitudes de datos realizadas por los uno o más hosts (200,220,225,230),

- usar un protocolo de enrutamiento multicast host-router basado en el protocolo IGMP, “Internet Group Management Protocol”, o el protocolo MLD, “Multicast Listener Discovery” para comunicarse con los uno o más hosts (200,220,225,230) y un protocolo de ruteo multicast router-router para comunicarse con por lo menos otro router multicast (261,262,263,264,265,266,267) situado entre él mismo y las fuentes (295,296,297,298,299), el router multicast (260) incluyendo un “source-timer” para cada una de las fuentes en la lista de fuentes INCLUDE y en la listas de fuentes EXCLUDE y EXCLUDE incluyendo una “Requested List” que contiene una lista de fuentes que tienen un “source-timer” con valor mayor que cero y una “Exclude List” que contiene una lista de fuentes que tienen un “source-timer” de valor cero,

- transmitir para la interfaz de red y para cada dirección de grupo multicast, paquetes multicast a los hosts (200,220,225,230) basados en la información del registro de fuentes INCLUDE y del registro de fuentes EXCLUDE,

- transmitir para cada fuente INCLUDE de una dirección de grupo multicast que tiene un “source-timer” con valor mayor que cero paquetes multicast a través de la interfaz de red, y

- cuando existe un registro de fuentes EXCLUDE transmitir también paquetes multicast de las fuentes restantes de las direcciones de grupo multicast a través de la interfaz de red excepto las fuentes EXCLUDE de la “Exclude List”.

2. Un router multicast según la reivindicación 1, donde el registro de fuentes INCLUDE almacenado en el router multicast (260) contiene la unión de todas las listas de fuentes INCLUDE solicitadas desde los hosts (200,220,225,230).

3. Un router multicast según la reivindicación 1, donde el registro de fuentes EXCLUDE almacenado en el router multicast (260) contiene la intersección de todas las listas de fuentes EXCLUDE solicitadas desde los hosts (200,220,225,230).

4. Un router multicast según la reivindicación 1, donde el router multicast (260) está adaptado para almacenar para la interfaz de red y dirección de grupo multicast sólo un registro de fuentes INCLUDE y solo un registro de fuentes EXCLUDE, el registro de fuentes INCLUDE contiene la unión de todas las listas de fuentes INCLUDE solicitadas desde los hosts (200,220,225,230) y el registro de fuentes EXCLUDE contiene la intersección de todas las listas de fuentes EXCLUDE solicitadas desde los hosts (200,220,225,230).

5. Un router multicast según la reivindicación 1, donde por lo menos un registro de fuentes INCLUDE para una interfaz de red y dirección de grupo multicast comprende (multicast-address, INCLUDE,{source list and timers}), y por lo menos un registro de fuentes EXCLUDE comprende (multicast-address,EXCLUDE,{source list and timers}), donde {source list and timers} comprende una lista de elementos {source-address y source-timer}, y donde source-address comprende la dirección IP de la fuente, y donde source-timer comprende un timer asociado a la fuente.

6. Un router multicast según la reivindicación 1, donde el router multicast (260) contiene instrucciones ejecutables para actualizar por lo menos un registro de fuentes INCLUDE y por lo menos un registro de fuentes EXCLUDE sobre la recepción desde los uno o más hosts (200,220,225,230) un mensaje de estado el cual contiene información acerca de una lista de fuentes INCLUDE y/o sobre una lista de fuentes EXCLUDE o un mensaje de cambio de estado que contiene información acerca de modificaciones de una lista de fuentes INCLUDE y/o información sobre modificaciones de una lista de fuentes EXCLUDE.

7. Un router multicast según la reivindicación 1, donde el router multicast (260) está adaptado para recibir un mensaje de estado originado desde uno o más hosts (200,220,225,230) que incluye instrucciones acerca del método que el router multicast (260) debe utilizar para establecer los árboles de ruteo desde las fuentes (295,296,297,298,299) hacia el router multicast (260).

8. Un router multicast según la reivindicación 1, donde el router multicast (260) almacena instrucciones ejecutables para (1) mantener, para cada interfaz de red “downstream” y dirección de grupo multicast el registro de fuentes INCLUDE y el registro de fuentes EXCLUDE, y (2) actualizar el registro de fuentes INCLUDE y el registro de fuentes EXCLUDE, para cada dirección de grupo multicast, cuando el router multicast recibe, a través de su propia interfaz de red “downstream”,

un mensaje que contiene información acerca de una lista de fuentes INCLUDE e información acerca de una lista de fuentes EXCLUDE originarias de uno o más de los hosts (200,220,225,230).

9. Un router multicast según la reivindicación 1, donde para una dirección de grupo multicast el router multicast (260) incluye una interfaz de red "upstream" la cual está adaptada para solicitar los datos provenientes de las fuentes (295,296,297,298,299) vía de al menos otro router multicast (261,262,263,264,265,266,267) situado dentro del árbol de ruteo entre las fuentes (295,296,297,298,299) y el router multicast (260), la interfaz de red "upstream" adaptada para comunicarse con por lo menos otro router multicast (261,262,263,264,265,266,267) vía el protocolo de ruteo multicast de router-router para solicitar los datos provenientes de las fuentes (295,296,297,298,299) usando la información en el registro de fuentes INCLUDE y la información en el registro de fuentes EXCLUDE para permitir una conexión directa con las fuentes (295,296,297,298,299) a través del árbol de ruteo de tipo "shortest path tree".

10. Un router multicast según la reivindicación 1, donde para una dirección de grupo multicast el router multicast (260) incluye una interfaz de red "upstream" la cual está adaptada para solicitar los datos provenientes de las fuentes (295,296,297,298,299) a través de una pluralidad de routers multicast (261,262,263,264,265,266,267) los cuales incluyen un "Rendezvous Point Router" (264), la pluralidad de routers multicast (261,262,263,264,265,266,267) situada dentro de un árbol de ruteo entre las fuentes (295,296,297,298,299) y el router multicast (260), el árbol de ruteo incluye el "rendezvous point tree", RPT (281,282), y "shortest path trees" SPT (291,292), para las fuentes (295,296,297,298,299), la interfaz de red "upstream" adaptada para comunicarse con la pluralidad de routers multicast (261,262,263,264,265,266,267) a través del protocolo de ruteo multicast de router-a-router para solicitar los datos desde las fuentes (295,296,297,298,299) utilizando la información en el registro de fuentes INCLUDE y la información en el registro de fuentes EXCLUDE para permitir una conexión directa con las fuentes (295,296,297,298,299) a través de los "shortest path trees" (291,292) sin necesidad de usar los "rendezvous point trees" (281,282).

11. Un router multicast según la reivindicación 1, que está adaptado en respuesta a la recepción de una interfaz de red "downstream" de un mensaje de tipo IS_IN (x) para una dirección de grupo multicast para no modificar ningún registro de fuentes EXCLUDE para el grupo multicast.

12. Un router multicast según la reivindicación 1, que está adaptado en respuesta a la recepción de una interfaz de red "downstream" de un mensaje de tipo IS_EX (x) para una dirección de grupo multicast no modifique ningún registro de fuentes INCLUDE.

13. Un router multicast según la reivindicación 1, donde para cada interfaz de red "downstream" y dirección de grupo multicast el router multicast (260) está adaptado para transmitir a los hosts (200,220,225,230) datos desde las fuentes (295,296,297,298,299) en la lista de fuentes INCLUDE y transmitir también a los hosts (200,220,225,230) datos provenientes de todas las fuentes restantes (295,296,297,298,299) excepto aquellas fuentes de la "Exclude List" cuando existe un registro de fuentes EXCLUDE para dicha dirección de grupo multicast.

14. Un router multicast según la reivindicación 1, donde el router multicast (260) está configurado para recibir mensajes originando desde los uno o más hosts (200,220,225,230) solicitando al router multicast (260) que detenga el envío de datos desde una fuente (295,296,297,298,299) en una dirección de grupo multicast, el router multicast (260) también configurado para enviar mensajes del tipo "Group-And-Source-Specific Query" a los uno o más hosts (200,220,225,230), el router multicast (260) almacena unas instrucciones ejecutables para determinar si uno o otros más hosts (200,220,225,230) están recibiendo datos desde la fuente (295,296,297,298,299) en la dirección de grupo multicast sobre la recepción de la petición de parada utilizando el registro de fuentes INCLUDE y el registro de fuentes EXCLUDE y de continuar enviando datos desde la fuente (295,296,297,298,299) en la dirección de grupo multicast en la dirección de grupo multicast a los otros uno o más hosts (200,220,225,230) sin enviar mensajes del tipo "Group-And-Source-Specific Query" a los otros uno o más hosts (200,220,225,230), recibiendo datos desde la fuente (295,296,297,298,299) en la dirección de grupo multicast.

15. Un router multicast según las reivindicaciones 9 o 10, donde el protocolo de ruteo multicast de router-a-router es una versión de un protocolo PIM-SM, Protocol Independent Multicast – Sparse Mode.

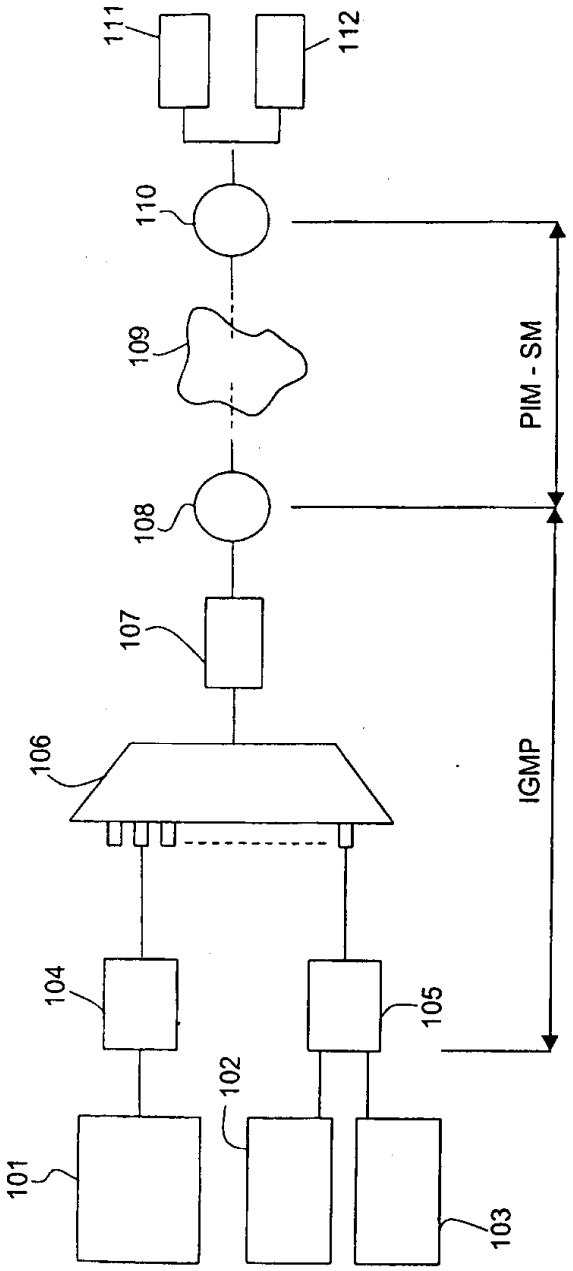

FIG. 1

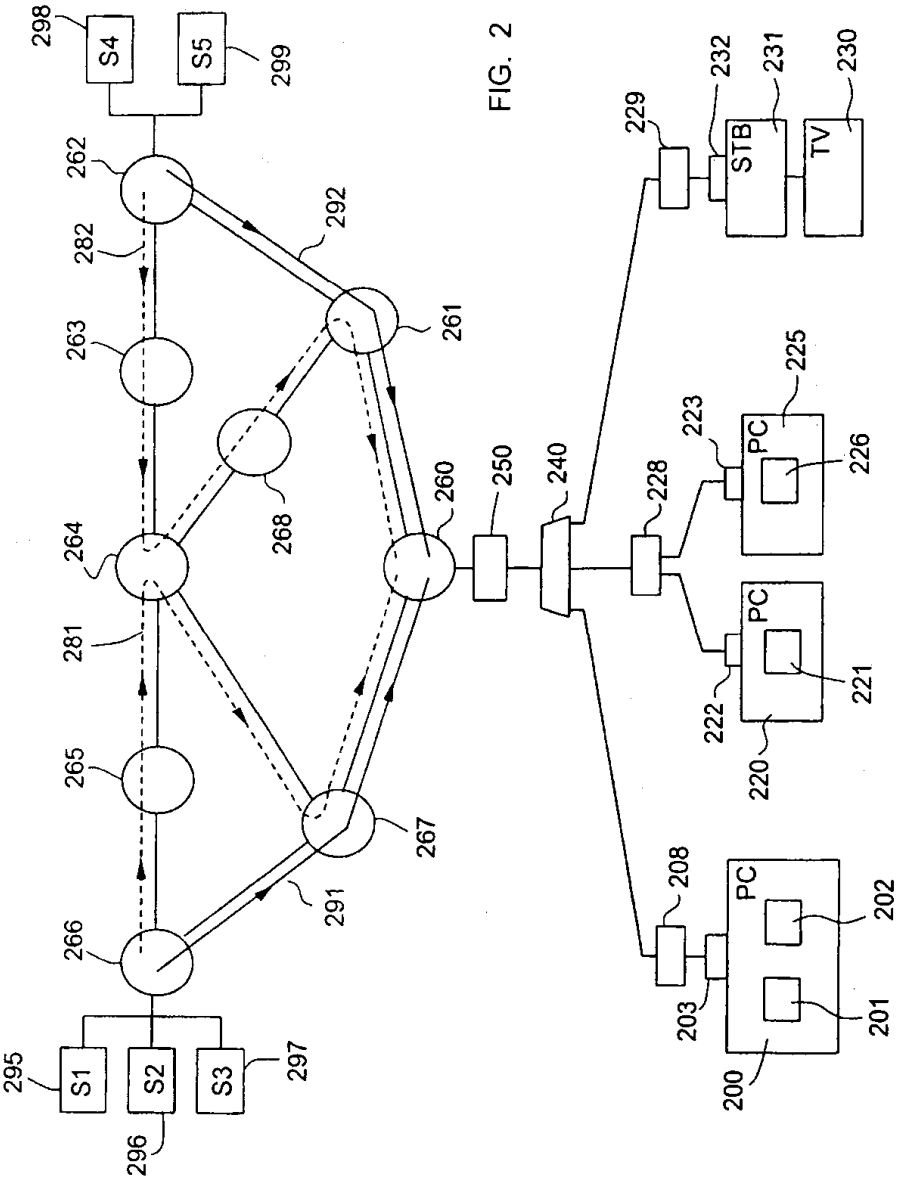
298
S4
S5
299
262
282
292
261
263
268
260
250
240
264
281
265
267
291
266
295
S1
S2
S3
297
296
229
232
231
230
STB
TV
228
223
225
PC
226
222
221
220
208
202
203
201
200

FIG. 2

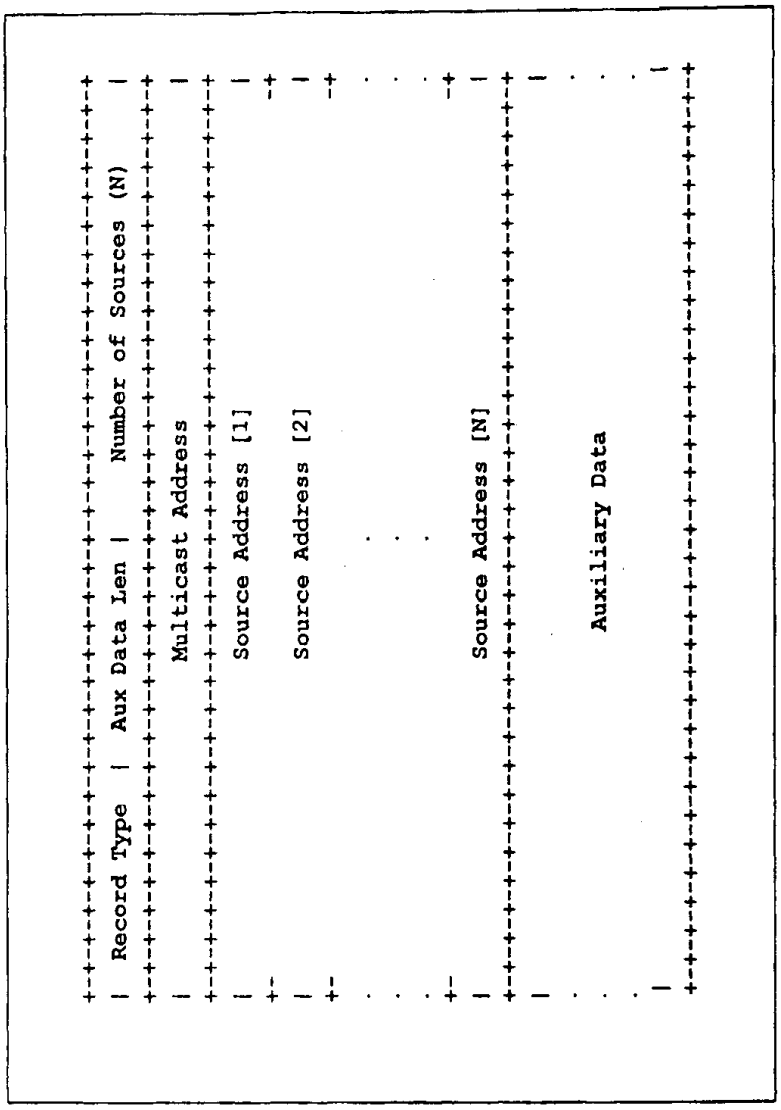
Record Type
Aux Data Len
Number of Sources (N)
Multicast Address
Source Address [1]
Source Address [2]
Source Address [N]
Auxiliary Data

FIG. 3

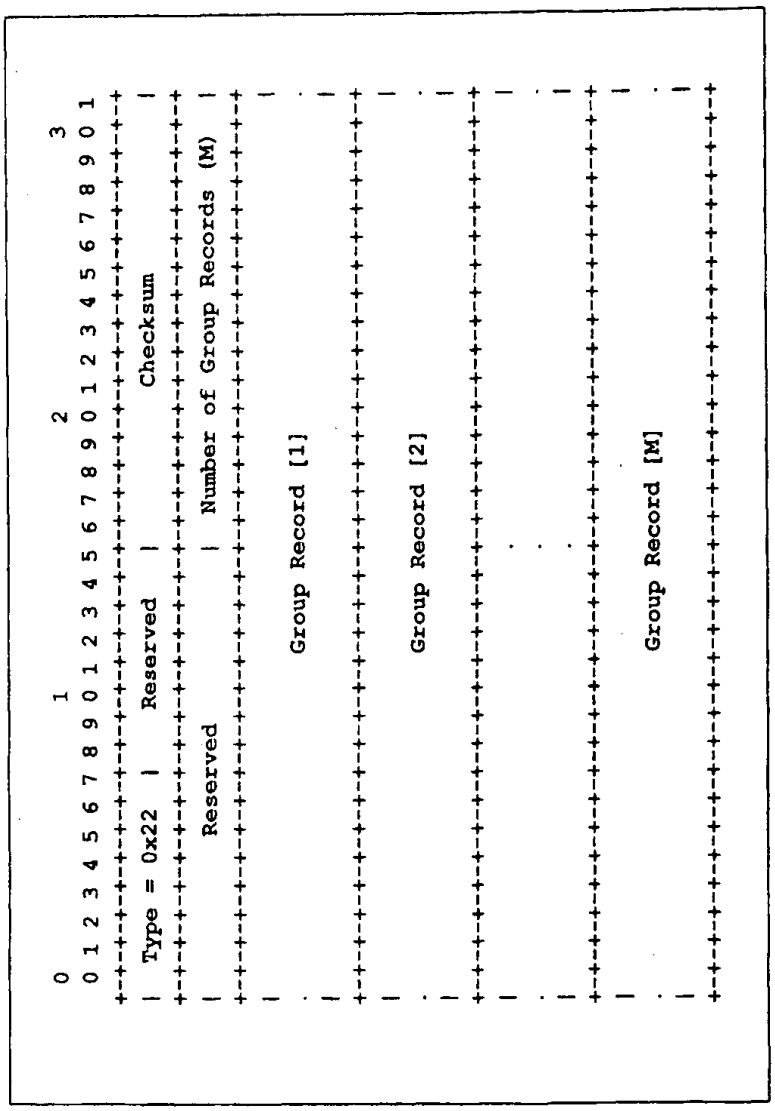
0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Type = 0x22
Reserved
Checksum
Reserved
Number of Group Records (M)
Group Record [1]
Group Record [2]
Group Record [M]

FIG. 4

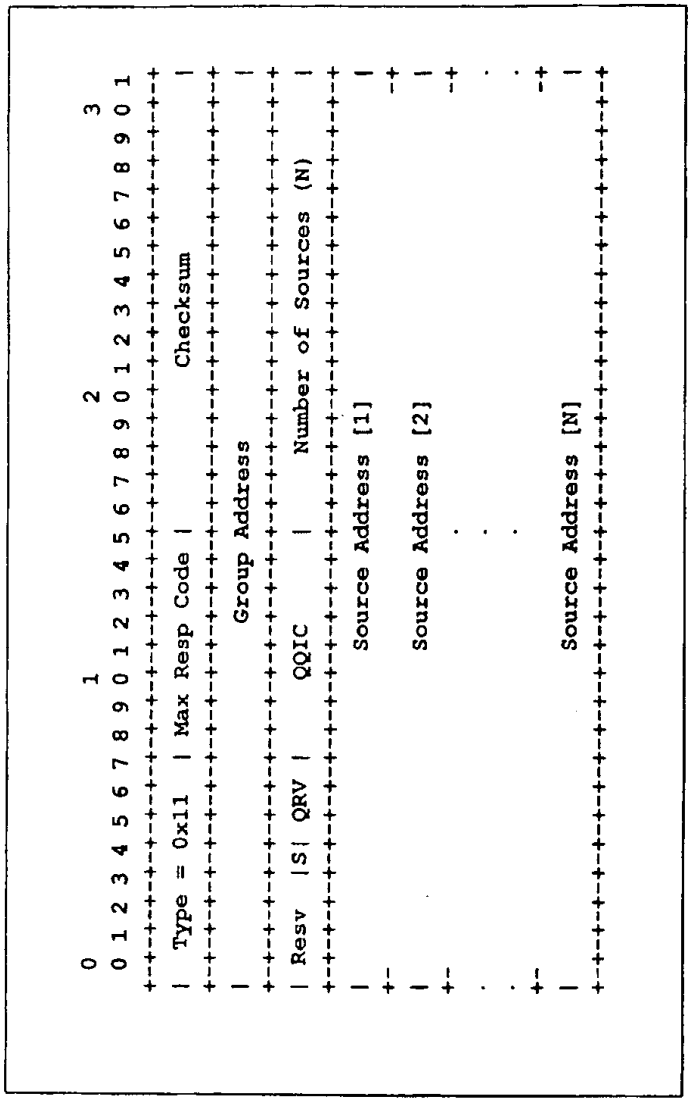
0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Type = 0x11
Max Resp Code
Checksum
Group Address
Resv
S
QRV
QQIC
Number of Sources (N)
Source Address [1]
Source Address [2]
Source Address [N]

FIG. 5

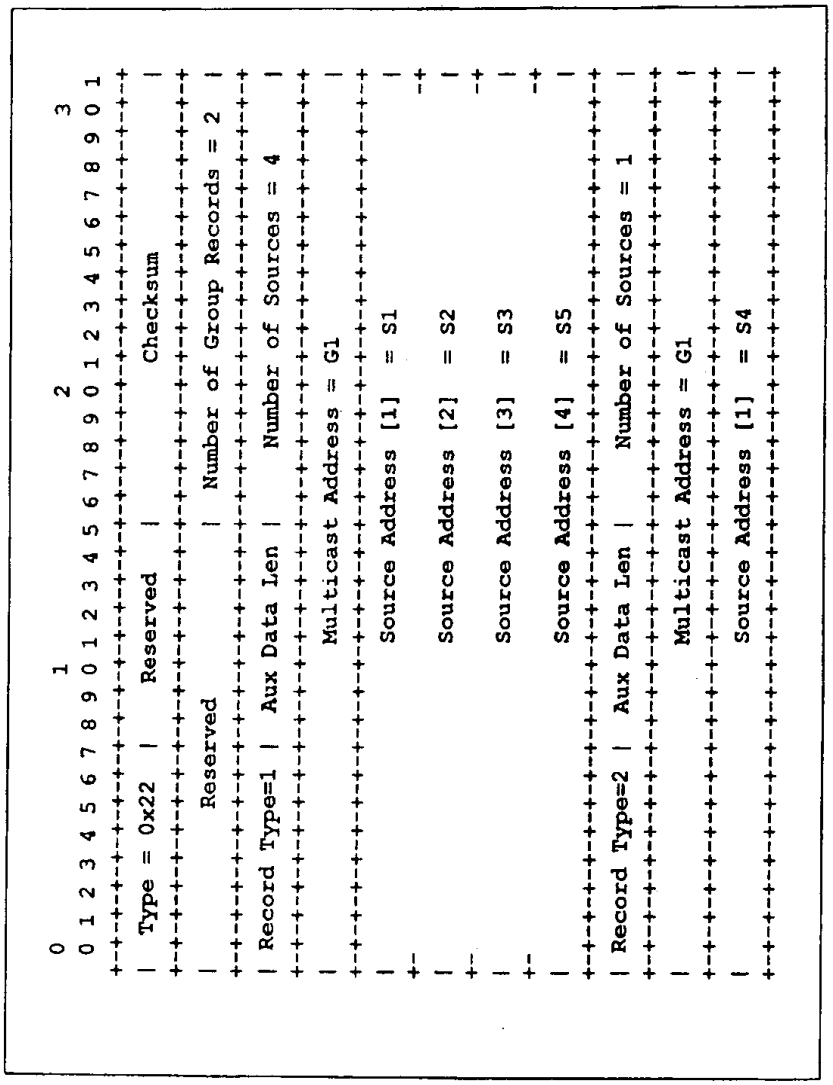
0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Type = 0x22 | Reserved | Checksum
Reserved | Number of Group Records = 2
Record Type=1 | Aux Data Len | Number of Sources = 4
Multicast Address = G1
Source Address [1] = S1
Source Address [2] = S2
Source Address [3] = S3
Source Address [4] = S5
Record Type=2 | Aux Data Len | Number of Sources = 1
Multicast Address = G1
Source Address [1] = S4

FIG. 6