(12) SOLICITUD INTERNACIONAL PUBLICADA EN VIRTUD DEL TRATADO DE COOPERACIÓNEN MATERIA DE PATENTES (PCT)

(19) Organización Mundial de la Propiedad Intelectual
Oficina internacional

(43) Fecha de publicación internacional
11 de septiembre de 2009 (11.09.2009)

PCT

(10) Número de Publicación Internacional
WO 2009/109684 A1

(51) Clasificación Internacional de Patentes:
H04L 12/24 (2006.01) *H04L 12/26* (2006.01)

(21) Número de la solicitud internacional:
PCT/ES2009/070047

(22) Fecha de presentación internacional:
27 de febrero de 2009 (27.02.2009)

(25) Idioma de presentación: español

(26) Idioma de publicación: español

(30) Datos relativos a la prioridad:
200800646 5 de marzo de 2008 (05.03.2008) ES

(71) Solicitante *(para todos los Estados designados salvo US)*: **MEDIA PATENTS, S. L.** [ES/ES]; Av. de Roma, 159, 3º, 2ª, E-08011 Barcelona (ES).

(72) Inventor; e

(75) Inventor/Solicitante *(para US solamente)*: **FERNÁNDEZ GUTIÉRREZ, Álvaro** [ES/ES]; Ronda General Mitre, 104, E-08021 Barcelona (ES).

(74) Mandatario: **ZEA CHECA, Bernabé**; ZBM Patents, S. L., Balmes, 114 4rt, E-08008 Barcelona (ES).

(81) Estados designados *(a menos que se indique otra cosa, para toda clase de protección nacional admisible)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

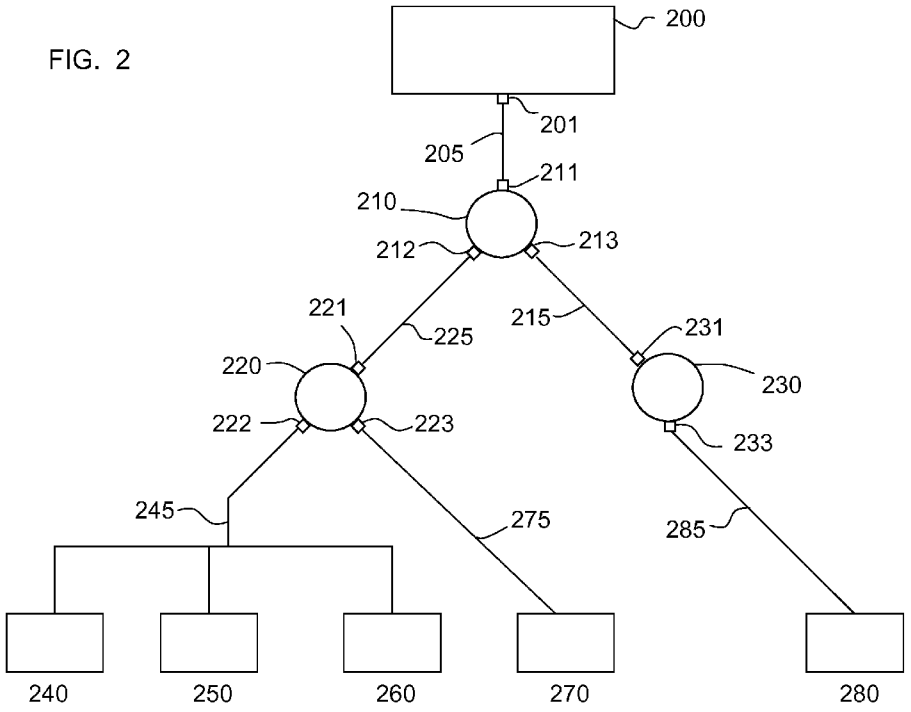
(84) Estados designados *(a menos que se indique otra cosa, para toda clase de protección regional admisible)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), euroasiática (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europea (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO,

[Continúa en la página siguiente]

(54) Title: METHOD FOR MONITORING OR MANAGING DEVICES CONNECTED TO A DATA NETWORK

(54) Título: PROCEDIMIENTO PARA MONITORIZAR O GESTIONAR EQUIPOS CONECTADOS A UNA RED DE DATOS

FIG. 2



[Continúa en la página siguiente]

WO 2009/109684 A1

SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaraciónes según la Regla 4.17:

— *sobre el derecho del solicitante a reivindicar la prioridad de la solicitud anterior (Regla 4.17(iii))*

Publicada:

— *con informe de búsqueda internacional (Art. 21(3))*

— *antes de la expiración del plazo para modificar las reivindicaciones y para ser republicada si se reciben modificaciones (Regla 48.2(h))*

(57) Abstract: The invention relates to a method for monitoring or managing devices (110, 120, 130) connected to a data network (150). The invention is characterised in that the data network (150) includes a control station (100) which monitors or manages the devices (110, 120, 130), each of which can be in one or more different states, and said devices (110, 120, 130) send messages in a multicast routing protocol in order to request receipt of multicast traffic, said requested multicast traffic consisting of multicast groups and multicast channels that correspond to the states of each device. The control station (100) ascertains the state(s) of each device from the multicast groups and multicast channels requested by each device.

(57) Resumen: Procedimiento para monitorizar o gestionar equipos (110, 120, 130) conectados a una red de datos (150) caracterizado porque dicha red de datos (150) dispone de una estación de control (100) que monitoriza o gestiona dichos equipos (110, 120,130), cada uno de los cuales puede estar en uno o en varios estados diferentes, y dichos equipos (110,120,130) envían mensajes en un protocolo de ruteo multicast para solicitar recibir tráfico multicast, donde dicho tráfico multicast solicitado consiste en grupos multicast y canales multicast que se corresponden con los estados de cada equipo, y dicha estación de control (100) conoce el estado o los estados de cada equipo a partir de los grupos multicast y canales multicast solicitados por cada equipo.

Procedimiento para monitorizar o gestionar equipos conectados a una red de datos.

DESCRIPCIÓN

Campo de la invención

La invención se sitúa en el campo de la tecnología de la monitorización, la gestión y la configuración de equipos conectados en redes de datos.

Más concretamente, la invención se refiere a un procedimiento de monitorización y gestión de equipos en red donde una pluralidad de equipos o dispositivos utilizan mensajes de protocolos de ruteo multicast para comunicarse con una estación de control de equipos.

La invención también se refiere a unos equipos de red que aplican dicho procedimiento.

Estado de la técnica

A medida que las redes de datos han ido creciendo en número de equipos, ha aumentado su complejidad y la heterogeneidad de los equipos conectados. Esto ha provocado un aumento en la dificultad y el coste de la monitorización, la gestión y la configuración de las redes de datos.

Para controlar este tipo de redes son necesarias herramientas estandarizadas que puedan ser utilizadas en equipos de diferentes fabricantes, incluyendo routers, switches y otros equipos de telecomunicaciones además de los ordenadores u otros equipos finales de la red como PDAs y teléfonos móviles. En adelante utilizaremos los términos host o dispositivo para referirnos a los equipos finales de la red de datos.

En respuesta a esta necesidad se desarrolló el protocolo “Simple Network Management Protocol” o SNMP, que es una herramienta que permite el mantenimiento y la configuración de equipos de red de diferentes fabricantes.

SNMP es un conjunto de estándares para la gestión de equipos de red. SNMP fue adoptado hace años como estándar para redes TCP/IP y se ha convertido en la herramienta más utilizada para la gestión de redes y dispositivos conectados a redes.

En 1991, se añadió un suplemento a SNMP, denominado Remote Network Monitoring (RMON). RMON extiende las capacidades de SNMP para incluir la gestión de redes de area local (LANs) además de la gestión de los dispositivos conectados a dichas redes.

Hay varias actualizaciones o nuevas versiones del protocolo SNMP. En 1995 se publicó una actualización denominada SNMPv2. En 1998 se publicó la última versión de este conjunto de estándares, denominada SNMPv3 que mejoró todos los aspectos relacionados con la seguridad.

Un sistema de gestión SNMP contiene los siguientes elementos:

- Al menos una estación de control o estación de gestión, tradicionalmente llamada “SNMP manager” o “management station”. En adelante utilizaremos el término estación de control para referirnos a este elemento.
- Varios nodos (potencialmente muchos), cada uno de los cuales utiliza una aplicación, tradicionalmente llamada agente SNMP, para comunicarse con la estación de control. Cada agente SNMP tiene acceso a la información de configuración de su nodo y puede enviar mensajes y recibirlos de la estación de control.
- Un protocolo de comunicaciones para la comunicación entre la estación de control y los agentes SNMP.

Los agentes SNMP gestionan los recursos de cada nodo utilizando unos objetos que representan a estos recursos. Cada objeto, es una variable con datos que representa un aspecto del nodo gestionado. El conjunto de estos objetos para un determinado nodo de la red se denomina “Management Information Base” o MIB.

Los MIB son estandarizados para cada clase de dispositivo de red. Por ejemplo un determinado MIB se utiliza para varios switches de diferentes fabricantes.

Una estación de control SNMP monitoriza el funcionamiento de un equipo recuperando el valor de los objetos contenidos en el MIB de dicho equipo. Para ello la estación de control SNMP se comunica con el agente SNMP y le solicita dicha información.

Una estación de control SNMP también puede modificar valores de los objetos contenidos en el MIB de un equipo enviando un mensaje al agente SNMP de dicho equipo para que modifique dichos valores.

Los MIB son especificaciones que contienen definiciones para la gestión y el mantenimiento de la información para una determinada clase de equipos de red de forma que dichos equipos de red, aunque sean de diferentes fabricantes, puedan ser monitorizados, configurados y controlados remotamente.

Las reglas que definen el lenguaje utilizado para escribir los MIB están definidas en las especificaciones RFC2578 (McCloghrie et al. , Internet Engineering Task Force, Request for Comments 2578, "The structure of Management Information Version 2, SMIv2", abril de 1999, actualmente disponible en la dirección de Internet http://www3.tools.ietf.org/html/rfc2578) y las especificaciones RFC2579 (McCloghrie et al. , Internet Engineering Task Force, Request for Comments 2579, "Textual Conventions for SMIv2", abril de 1999, actualmente disponible en la dirección de Internet http://www3.tools.ietf.org/html/rfc2579).

SMIv2 utiliza una pequeña parte de las instrucciones de un lenguaje denominado Abstract Syntax Notation One (ASN.1).

ASN.1 es un lenguaje formal estandarizado y es importante en el protocolo SNMP por varios motivos. En primer lugar, se utiliza para definir la sintaxis de los datos. También se utiliza para definir los mensajes del protocolo SNMP, también denominados "Protocol Data Units" (PDUs). Por último se utiliza para definir los MIB.

Aunque SNMP es el protocolo más extendido para la gestión de dispositivos de red y redes, presenta algunos inconvenientes.

Un primer inconveniente es la complejidad. Una visión conjunta del funcionamiento del protocolos SNMP y los equipos que lo implementan se describe en las especificaciones RFC3411 (D. Harrington et al., Internet Engineering Task Force, Request for Comments 3411, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", diciembre de 2002, actualmente disponible en la dirección de Internet http://www3.tools.ietf.org/html/rfc3411). En el apartado 10, referencias, de dichas especificaciones RFC3411 se enumeran otros 22 documentos de tipo RFC ("Request For Comments") que describen dicho funcionamiento del protocolo SNMP.

Una muestra de la complejidad del protocolo SNMP es el proyecto de software libre "Net-SNMP" disponible en la dirección de Internet http://net-snmp.sourceforge.net/ donde está disponible el código fuente de un agente SNMP. Dicho código fuente puede ser descargado libremente, y la versión disponible en enero de 2008 de dicho agente SNMP consta de un total de 878 archivos de código fuente en lenguaje C (archivos cuya terminación es "c" o "h") que incluyen un total de 316.435 líneas de código.

Esta complejidad es un problema por dos motivos. Un primer problema es económico por el tiempo, los conocimientos y los recursos humanos necesarios para implementar un agente SNMP. Un segundo problema es técnico por la capacidad de almacenamiento y de proceso necesaria en los dispositivos que deben incorporar agentes SNMP. Este último problema de recursos técnicos no es un problema en equipos como routers, switches u ordenadores que disponen de suficiente capacidad de procesamiento para implementar agentes SNMP. Sin embargo esta complejidad técnica sí es un problema en muchos otros equipos que disponen de una capacidad de procesamiento menor y donde además el consumo de energía puede ser un factor importante en el diseño de dichos equipos, como por ejemplo en teléfonos móviles o en sistemas controlados mediante microcontroladores con una capacidad limitada de memoria y procesamiento.

Otra limitación del protocolo SNMP es que la estación de control SNMP debe establecer una comunicación directa con cada agente SNMP. Esto supone varios problemas a medida que aumenta el número de agentes SNMP que debe controlar. El primer problema es que

la estación de control SNMP puede gestionar un número limitado de agentes SNMP y puede no tener suficiente capacidad de procesamiento si el número de agentes es de varios miles o cientos de miles. El segundo problema es el tráfico que se genera en la red por culpa de los mensajes SNMP entre la estación de control SNMP y los agentes SNMP a medida que crece el número de dispositivos gestionados.

Una tecnología que es posible utilizar para solucionar estas limitaciones de SNMP es la tecnología multicast. Hay algunos estudios científicos que estudian el uso de la tecnología multicast en el protocolo SNMP.

El siguiente documento describe el uso de envío de paquetes multicast entre agentes SNMP: Ehab Al-Hshaer, Yongning Tang. *"Toward Integrating IP Multicasting in Internet Network Management Protocols".* Computer Communications, Volumen 24, Numero 5, 15 Marzo 2001, pp. 473-485, Publisher: Elsevier, actualmente disponible en la dirección de internet http://citeseer.ist.psu.edu/447658.html.

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.

Los mensajes intercambiados entre un dispositivo 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.

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. En adelante, para designar a un proxy que utiliza los protocolos IGMP/MLD se utilizará el término genérico "proxy IGMP".

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 dispositivos que se han suscrito a un grupo multicast. Para ello, los routers utilizan unos protocolos específicos, entre los cuales el más extendido es el PIM-SM (Protocol Independent Muticast - Sparse Mode).

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

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).

En cuanto al protocolo MLD, la versión que se utiliza actualmente es la MLDv2, 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).

El funcionamiento de un proxy IGMP 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).

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).

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.

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.

En las primeras versiones del protocolo IGMP un dispositivo 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 dispositivo 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 ("Source Specific Multicast") en el cual los dispositivos eligen las fuentes emisoras de datos multicast.

Para permitir el SSM, en la versión IGMPv3 del protocolo IGMP se introdujo la posibilidad de que los dispositivos pudieran escoger las fuentes dentro de un grupo multicast. Para ello, un dispositivo puede enviar mensajes IGMP que contienen unos bloques de datos denominados "Group Record" en los cuales el dispositivo define las fuentes de las que desea recibir tráfico para cada grupo multicast. Estos bloques de datos "Goup Record" en un mensaje IGMP pueden ser de varios tipos:

- Un bloque de datos "Group Record" de tipo INCLUDE, que contiene información sobre direcciones IP de las fuentes de las cuales el dispositivo sí desea recibir la emisión de datos. Siguiendo la terminología de las especificaciones RFC 3376, a las fuentes

elegidas mediante un mensaje IGMP que contiene un "Group Record" de tipo INCLUDE se las denomina fuentes INCLUDE.

- Un bloque de datos "Group Record" de tipo EXCLUDE, que contiene información sobre direcciones IP de las fuentes de las cuales el dispositivo no desea recibir la emisión de datos. En este caso, se interpreta que el dispositivo desea recibir los datos emitidos por todas las fuentes de dicho grupo multicast menos las fuentes indicadas como excluidas en el mensaje. Siguiendo la terminología de las especificaciones RFC 3376, a las fuentes excluidas mediante un mensaje IGMP que contiene un "Group Record" de tipo EXCLUDE se las denomina fuentes EXCLUDE.

Para simplificar, en lo que sigue se utilizará el término "mensaje INCLUDE" para designar a un mensaje IGMP que contiene un "Group Record" de tipo INCLUDE, y el término "mensaje EXCLUDE" para designar a un mensaje IGMP que contiene un "Group Record" de tipo EXCLUDE.

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

Cada interfaz de red y grupo multicast tiene un registro de estado que almacena la información sobre dicha interfaz y grupo y dicho registro de estado contiene un campo denominado "filter-mode" que sólo puede ser de tipo INCLUDE, que contiene fuentes INCLUDE, o bien de tipo EXCLUDE, que contiene fuentes EXCLUDE. Cuando el registro de una interfaz de red debe resultar de la combinación de diferentes registros, se aplican las reglas 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.

Estas reglas se aplican en una interfaz de red de un equipo que funciona como proxy IGMP y que recibe mensajes INCLUDE o mensajes EXCLUDE provenientes de diferentes hosts o bien de diferentes proxys IGMP situados del lado "downstream" de dicha interfaz de red (es decir en la dirección que va desde el router hacia los hosts) . Estas mismas reglas también se aplican en una interfaz de red de un equipo, como por ejemplo un ordenador personal, provista de varios "sockets" que reciben diferentes peticiones de fuentes INCLUDE o de fuentes EXCLUDE provenientes de diferentes aplicaciones.

En lo que sigue, y siguiendo la nomenclatura común en la tecnología SSM, se denomina canal (S,G) a la emisión de la fuente S del grupo multicast G.

En el estado de la técnica actual, para ahorrar memoria los routers que utilizan el protocolo IGMPv3 almacenan sólo la información mínima del tráfico multicast que deben transmitir. Esta información mínima consiste en almacenar, para cada interfaz de red del router y grupo multicast, un estado que refleja si para un determinado canal (S,G) o grupo multicast (*,G) hay como mínimo un host interesado en recibir dicho tráfico multicast.

Sumario de la invención

La invención tiene como finalidad principal proporcionar un sistema mejorado de gestión de dispositivos en una red de datos.

Un objetivo de la invención es reducir significativamente la complejidad de los sistemas en los dispositivos que son controlados.

Otro objetivo de la invención es reducir la memoria y la capacidad de procesamiento necesarios en dichos dispositivos para utilizar el presente sistema de monitorización y gestión de dispositivos.

Otro objetivo de la invención es reducir el consumo de ancho de banda que se produce en las redes de datos como consecuencia de la utilización de sistemas de gestión de dispositivos.

Con este fin, se ha desarrollado un procedimiento para monitorizar o gestionar equipos conectados a una red de datos caracterizado porque:

- dicha red de datos (150) dispone de una estación de control (100) que monitoriza o gestiona dichos equipos (110, 120,130), y;
- cada uno de dichos equipos puede estar en uno o en varios estados diferentes, y;
- dichos equipos (110,120,130) envían mensajes en un protocolo de ruteo multicast para solicitar recibir tráfico multicast, y;
- dicho tráfico multicast solicitado consiste en grupos multicast y canales multicast que se corresponden con los estados de cada equipo, y;
- dicha estación de control (100) conoce el estado o los estados de cada equipo a partir de los grupos multicast y canales multicast solicitados por cada equipo.

La invención también contempla que:

- en dicha red de datos hay como mínimo un router multicast (220, 230) conectado a dichos equipos (240, 250, 260, 270, 280), y;
- dichos equipos envían dichos mensajes en un protocolo de ruteo multicast a un dicho router multicast (220, 230), y;
- un router multicast (210, 220, 230) transmite dicha información de grupos multicast y canales multicast solicitados por cada equipo a dicha estación de control (200)

Preferentemente dicha estación de control (100, 200) envía como mínimo a uno de dichos equipos una información para configurar o modificar el estado de dicho equipo.

En una realización ventajosa, el router conectado a dichos equipos es un router IGMP.

En otra realización ventajosa, dicho router que transmite la información a dicha estación de control es un router PIM-SM.

La invención también se refiere al procedimiento según cualquiera de los procedimientos antes mencionados cuando dicho router multicast que transmite dicha información a dicha

estación de control incluye un agente SNMP y dicha información se almacena en una base de datos MIB y se transmite a la estación de control mediante el protocolo SNMP.

Preferentemente, dicho router IGMP almacena en unos registros asociados con el protocolo IGMP la información de los grupos y canales multicast solicitados por cada equipo asociando dichos grupos y canales multicast solicitados por cada equipo con un identificador de cada equipo.

En una realización preferente, dicho router IGMP almacena dicha información de grupos y canales multicast solicitados por cada equipo en una base de datos MIB.

En una forma de realización ventajosa, dicho router IGMP transmite dicha información almacenada en dicha base de datos MIB a la estación de control.

Preferentemente, dicho router IGMP transmite dicha información almacenada en dicha base de datos MIB utilizado el protocolo SNMP.

La invención también contempla una forma de realización en la cual un router PIM-SM que transmite la información a dicha estación de control es un router PIM-SM mejorado que almacena en unos registros asociados con el protoclo PIM-SM la información de los grupos y canales multicast solicitados por cada router multicast asociando dichos grupos y canales multicast con un identificador de cada router que le solicita dichos grupos y canales multicast.

Preferentemente dicho router PIM-SM almacena dicha información de grupos y canales multicast solicitados por cada router multicast en una base de datos MIB.

En una forma de realización ventajosa dicho router PIM-SM transmite información almacenada en dicha base de datos MIB a la estación de control.

Preferentemente dicho router PIM-SM transmite dicha información utilizado el protocolo SNMP.

La invención se refiere asimismo a unos equipos de red aptos para aplicar el procedimiento según la invención.

Breve descripción de los dibujos

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.

La Fig. 1 muestra un ejemplo de una estación de control que monitoriza y gestiona dispositivos en el que la presente invención es aplicable.

La Fig. 2 muestra un ejemplo de la presente invención funcionando en una red de datos multicast donde hay routers IGMP y routers PIM-SM del estado de la técnica actual.

La Fig. 3 muestra un ejemplo de la presente invención funcionando en un sistema que utiliza también el protocolo SNMP.

La Fig 4 muestra un ejemplo simplificado de un sistema de comunicaciones multicast.

Descripción detallada de unas formas de realización de la invención

Primera forma de realización de la invención

La presente invención describe un nuevo procedimiento de gestión de dispositivos conectados en red desde una estación de control conectada a dicha red mediante un nuevo uso de los protocolos de ruteo multicast.

El nuevo procedimiento se caracteriza porque la estación de control conoce el estado de los dispositivos a partir de los grupos y canales multicast que ha solicitado recibir cada dispositivo. Es decir, la presente invención utiliza como medio de comunicación desde los dispositivos hacia la estación de control mensajes pertenecientes a protocolos de ruteo multicast.

En la presente invención unos dispositivos envían mensajes de protocolos de ruteo multicast que solicitan recibir un tráfico multicast a una estación de control que recibe la información de qué tráfico multicast ha solicitado cada dispositivo, pero dicha estación de control no necesita transmitir dicho tráfico multicast a los dispositivos porque la función de dichas solicitudes de tráfico multicast es transmitir a la estación de control una información del estado de cada dispositivo.

Los protocolos de ruteo multicast han sido pensados y diseñados para transmitir tráfico multicast y no para que unos dispositivos informen a una estación de control de cual es su estado y dicha estación de control conozca el estado de cada dispositivo a partir de los grupos y canales multicast que cada dispositivo solicita. Sin embargo, este nuevo uso de los protocolos multicast tiene algunas ventajas como reducir la complejidad en los sistemas de control que incorporan los dispositivos, reutilizar redes ya existentes y reducir el tráfico de gestión que circula por las redes.

En la presente descripción se utilizan los dos protocolos de ruteo multicast más extendidos en la actualidad: el protocolo IGMP para los mensajes de ruteo multicast host-router y el protocolo PIM-SM para los mensajes de ruteo multicast entre routers. Sin embargo, otros protocolos de ruteo multicast son igualmente aplicables.

En lo que sigue utilizaremos los términos “monitorizar” y “gestionar” de acuerdo con la siguiente explicación.

Diremos que la estación de control “monitoriza” un dispositivo cuando la estación de control recibe información de dicho dispositivo que le informa del estado del dispositivo pero la estación de control no envía información al dispositivo con la finalidad de configurarlo o modificar su estado. Durante un proceso de monitorización de un dispositivo, la estación de control también puede enviar información al dispositivo para que el dispositivo reciba una confirmación de que sus mensajes de solicitud de tráfico multicast han llegado a la estación de control. Sin embargo dicha información no se utiliza para configurar el dispositivo sino para informarle de que sus mensajes han llegado correctamente.

Diremos que la estación de control "gestiona" un dispositivo cuando la estación de control no sólo recibe información de dicho dispositivo sino que además la estación de control envía información al dispositivo con la finalidad de configurarlo o para que el dispositivo cambie de estado.

La figura 1 muestra un ejemplo de realización de la presente invención. En dicha figura hay tres dispositivos 110, 120 y 130 conectados a una red de datos multiacceso 150, por ejemplo ethernet.

Una estación de control 100 se haya conectada igualmente a dicha red 150. La dirección IP de dicho sistema de control 100 es IP100. El sistema de control 100 incluye un router IGMP 101 que se encarga de solicitar la información a los dispositivos de acuerdo con el procedimiento estándar del protocolo IGMPv3. El sistema de control 100 también dispone de varias interfaces de red 102, 103 y 104. La interfaz de red 102 está conectada a la red 150.

Dichos dispositivos incorporan un sistema que implementa la presente invención. Dicho sistema pueda ser implementado, por ejemplo, mediante un hardware especializado incluido en los dispositivos en comunicación con una tarjeta de red para permitir el acceso a la red multiacceso 150, que puede ser una red física que utilice cables o una red inalámbrica, como por ejemplo WIFI o WIMAX.

Los dispositivos de la figura 1 pueden ser cualquier tipo de dispositivos, pero en este ejemplo los dispositivos 110,120 y 130 son semáforos cuya utilidad es regular el tráfico de coches.

En dicho sistema se han definido varios estados con el objetivo de gestionar el correcto funcionamiento de los dispositivos. La siguiente tabla 1 explica los estados definidos, su significado, y el grupo multicast o canal multicast asociado a cada estado.

Estado	Significado	Grupo o Canal
0	El semáforo tiene todas sus luces apagadas	Gi
1	El semáforo tiene encendida una luz de color verde	(Si, G1)
2	El semáforo tiene encendida una luz de color naranja	(Si, G2)
3	El semáforo tiene encendida una luz de color roja	(Si, G3)

....

Los dispositivos 110, 120 y 130 de la figura 1 envían mensajes IGMPv3 a la estación de control 100. Dichos mensajes incluyen los grupos multicast y canales multicast correspondientes a los estados en los que se encuentra cada dispositivo. Gracias a estos mensajes, la estación de control 100 conoce el estado de cada dispositivo.

Un determinado dispositivo i (en la figura 1, i puede ser 120, 130 o 140) puede enviar seis tipos de mensajes IGMP distintos de acuerdo con la presente invención: mensajes IGMP solicitando cuatro tipos de canales multicast y mensajes IGMP solicitando dos tipos de grupos multicast:

- Mensajes del tipo (Si , Gi), donde la fuente de datos Si y el grupo multicast Gi sólo son utilizados por el dispositivo i.
- Mensajes del tipo (Si , G1) donde la fuente de datos Si sólo es utilizada por el dispositivo i pero el grupo multicast G1 se utiliza por varios dispositivos.
- Mensajes del tipo (S1,Gi) donde la fuente S1 es utilizada por varios dispositivos pero el grupo Gi sólo es utilizado por el dispositivo i.
- Mensajes del tipo (S1,G7) donde tanto la fuente de datos S1 como el grupo G7 son utilizados por todos los dispositivos.
- Mensajes del tipo Gi, donde el grupo multicast Gi sólo lo utiliza el dispositivo i.

- Mensajes del tipo G9, donde el grupo multicast G9 es utilizado por todos los dispositivos.

El tipo de mensajes que se utiliza para cada estado se puede elegir en función de los dispositivos y también en función de la red de datos multicast en la que están conectados los dispositivos. La correcta elección del tipo de mensaje permite que el sistema de control funcione de forma jerárquica en redes multicast que usan diferentes tipos de equipos multicast como routers PIM-SM, routers IGMP y Proxys IGMP.

En la tabla 1, el estado 0 utiliza un grupo multicat Gi que es único para el dispositivo. Los dispositivos 110, 120 y 130 tienen asignados los grupos multicast G110, G120 y G130 respectivamente.

El concepto de unicidad se debe entender en el sentido del dominio de ruteo multicast. Por ejemplo, redes de datos no conectadas entre sí que pueden utilizar el mismo Gi, ya que aunque sea el mismo grupo multicast, es único en cada red.

En los estados 1 a 6, la fuente Si del canal multicast es distinta para cada dispositivo. Los dispositivos 110, 120 y 130 tienen asignados las fuentes de datos multicast S110, S120 y S130 respectivamente.

En el estado 7 se utiliza el canal multicast (S1, G7), donde tanto la fuente S1 como el grupo multicast G7 son los mismos en todos los dispositivos.

En el estado 8 todos los dispositivos utilizan el mismo canal multicast (S1,G8), donde S1 es una dirección IP de la red de datos elegida de tal forma que las solicitudes de tráfico multicast lleguen siempre a la estación de control.

En el estado 9 cada dispositivo tiene asignado un grupo multicast G9 común para todos los dispositivos y un canal multicast (IP100,Gi) donde IP 100 es la dirección IP de la estación de control 100 y es por lo tanto común a todos los dispositivos y Gi es diferente en cada dispositivo. Los dispositivos 110, 120 y 130 tienen asignados los grupos multicast G110, G120 y G130 respectivamente.

En los estados 0 a 8 la explicación de la tabla 1 es suficiente para su comprensión. El estado 9 lo utilizan los dispositivos para indicar al sistema de gestión 100 que el dispositivo incorpora la presente invención y que está funcionando correctamente. Por lo tanto los dispositivos que ejecutan la presente invención siempre solicitan recibir el canal multicast (IP100,Gi) y el grupo multicast G9 cuando funcionan correctamente.

Esta propiedad puede ser utilizada por el sistema de control 100 para enviar datos a todos los dispositivos o a un único dispositivo concreto. El sistema de control 100 puede enviar datos individualizados a unos dispositivos 110, 120 o 130 enviando paquetes IP mediante los canales multicast (IP100,G110), (IP100, G120) y (IP100, G130) respectivamente.

Si el sistema de control desea enviar datos a todos los dispositivos de la red 150, por ejemplo una nueva tabla 1, puede enviar paquetes IP usando el grupo multicast G9 como dirección IP de destino de los paquetes IP. Esto es igualmente aplicable a una red con miles o millones de dispositivos y supone un ahorro de tráfico de datos en la red ya que el sistema de control sólo tiene que enviar los paquetes multicast una sola vez independientemente del número de dispositivos que estén conectados a la red 150.

Sin embargo, de acuerdo con las anteriores definiciones de monitorizar y gestionar, en un sistema de control que sólo monitorice los dispositivos no es necesario el envío de paquetes desde la estación de control hacia los dispositivos monitorizados. Dicho envío de información es necesario cuando la estación de control desea gestionar los dispositivos, por ejemplo para actualizar su configuración.

En la tabla de estados hay unos estados que son incompatibles entre sí y otros que son compatibles entre sí. Por ejemplo el estado 0, todas las luces apagadas, es incompatible con los estados 1, 2 y 3. Sin embargo los estados 1 y 5 son compatibles ya que un dispositivo puede tener al mismo tiempo ambos estados, es decir la luz verde encendida y la luz naranja estropeada.

Gracias a la asignación de grupos y canales multicast que se corresponden con los diferentes estados de un dispositivo, la presente invención permite monitorizar y gestionar dispositivos conectados en red de una forma mucho más sencilla que la utilizada en el protocolo SNMP.

También es posible que un dispositivo quiera recibir un tráfico multicast (Sx, Gy) por medio de la red de datos, por ejemplo para recibir una tabla de configuración necesaria para el funcionamiento dispositivo, o por cualquier otro motivo. En este caso la estación de control conoce que el dispositivo quiere recibir el canal multicast (Sx,Gy) que no se corresponde con ninguno de los estados definidos en la tabla 1 de dicho dispositivo y deja que los procedimientos de ruteo multicast de la red de datos hagan llegar el canal multicast (Sx,Gy) de la fuente Sx a dicho dispositivo. Aún así, la estación de control está monitorizando también este tráfico multicast que recibe el dispositivo. Si el router IGMP 101 implementado en la estación de control es el "Designated Router", en el sentido utilizado en las especificaciones IGMPv3, en la red 150, entonces el propio router 101 transmite el tráfico multicast (Sx,Gy).

El protocolo IGMPv3 es un protocolo sencillo y se puede implementar en un dispositivo la funcionalidad necesaria para enviar mensajes IGMPv3 con pocas líneas de código adicionales a las necesarias para implementar el protocolo IP. El protocolo IP es necesario porque los mensajes IGMPv3 se encapsulan en paquetes IP.

La figura 2 muestra un ejemplo de la presente invención funcionando en una red de datos multicast donde hay routers IGMP y routers PIM-SM del estado de la técnica actual.

En la figura 2 hay una serie de dispositivos de red que son monitorizados y gestionados desde una estación de control 200 que implementa la presente invención y que está conectada a la red 205 mediante una interfaz de red 201.

Un router multicast 210 utiliza el protocolo PIM-SM y se comunica con la estación de control 200 mediante su interfaz de red 211 conectada a la red 205. Dicho router multicast 210 dispone de otras dos interfaces de red 212 y 213 mediante las cuales se conecta con los routers 220 y 230 respectivamente.

Los routers 220 y 230 son routers multicast que utilizan el protocolo PIM-SM en sus comunicaciones con el router 210 y utilizan el protocolo IGMPv3 en sus comunicaciones con los dispositivos 240, 250, 260, 270 y 280.

Los dispositivos 240, 250 y 260 están conectados a una red multiacceso 245, por ejemplo una red ethernet, que a su vez está conectada a una interfaz de red del router 220. Dichos dispositivos envían solicitudes de tráfico multicast utilizando mensajes IGMPv3 a la interfaz de red 222 del router multicast 220 a través de la red 245. Otro dispositivo 270 está conectado a otra interfaz de red 223 del router 220 mediante la red 275.

El dispositivo 280 está conectado a la interfaz de red 233 del router 230 mediante la red 285.

Los dispositivos 240, 250, 260, 270 y 280 implementan la presente invención y transmiten su estado a la estación de control 200 enviando solicitudes de tráfico multicast en el protocolo IGMPv3.

Los routers 220 y 230 reciben dichas solicitudes de tráfico multicast en el protocolo IGMPv3 y las envían al router 210 utilizando el protocolo PIM-SM.

El router 210 transmite las peticiones de tráfico multicast a la estación de control 200 utilizando el protocolo PIM-SM y de esta forma la estación de control 200 conoce el estado de cada dispositivo a partir de los grupos y canales multicast que cada dispositivo ha solicitado recibir.

Segunda forma de realización de la invención

Aunque la presente invención puede funcionar sin necesidad del protocolo SNMP, dicho protocolo está ampliamente extendido y es el estándar que se utiliza actualmente para gestionar dispositivos de red.

Por ello es interesante que la presente invención se pueda integrar en una red de datos que utiliza el protocolo SNMP, especialmente en la parte de la red en contacto con dispositivos finales como ordenadores, teléfonos móviles, PDAs o cualquier otro dispositivo conectado a la red de datos.

La figura 3 muestra un ejemplo de la presente invención funcionando en una red que utiliza el protocolo SNMP.

Normalmente, para hacer compatible un nuevo protocolo de control con un sistema de control SNMP se suelen utilizar unos sistemas denominados "Proxys SNMP". La función de un Proxy SNMP es hacer de intermediario entre la estación de control que utiliza el sistema de gestión SNMP y el nuevo dispositivo que utiliza un protocolo de control distinto o propio. Para ello los diferentes mensajes y datos del nuevo protocolo de control deben convertirse a mensajes SNMP y viceversa, es decir, los mensajes y datos del protocolo SNMP deben también convertirse al sistema de control propio del dispositivo.

La presente invención también puede adaptar su funcionamiento a un sistema SNMP mediante un Proxy SNMP. Los Proxys SNMP son conocidos por un experto en la materia y no profundizaremos más en su explicación.

Sin embargo, hay otra forma de integrar la presente invención en un sistema de gestión de redes que utiliza el protocolo SNMP sin necesidad de crear un Proxy SNMP. Esto se consigue utilizando los agentes SNMP de los routers multicast. Tanto los routers multicast IGMPv3 como los routers multicast PIM-SM del estado de la técnica actual suelen disponer de agentes SNMP.

El funcionamiento de un agente SNMP para routers IGMP está descrito en el documento "Multicast Group Membership Discovery MIB" editado en línea por la IETF (J. Chesterfield et al., Internet Engineering Task Force, Magma Working Group, Request for Comments 4601, diciembre de 2007; actualmente disponible en la dirección Internet http://www.ietf.org/internet-drafts/draft-ietf-magma-mgmd-mib-11.txt).

El funcionamiento de un agente SNMP para routers PIM-SM está descrito en el documento "Protocol Independent Multicast MIB draft-ietf-pim-mib-v2-10.txt" editado en línea por la IETF (R. Sivaramu et al., Internet Engineering Task Force, PIM Working Group, septiembre de 2007, actualmente disponible en línea en la dirección de Internet ftp://ftp.rfc-editor.org/in-notes/internet-drafts/draft-ietf-pim-mib-v2-10.txt).

La presente invención utiliza agentes SNMP para almacenar la información del estado de los dispositivos, en forma de grupos y canales mutlicast solicitados por cada dispositivo, y

transmitir dicha información mediante el protocolo SNMP a la estación de control SNMP o "SNMP manager". La figura 3 ilustra dicho funcionamiento.

En la figura 3 hay una estación de control SNMP 300 que se comunica mediante el protocolo SNMP con un router PIM-SM 310 y dos routers IGMP 320 y 330. La comunicación entre la estación de control 300 y el router PIM-SM tiene lugar por medio de la red 315. La comunicación entre la estación de control 300 y los dos routers IGMP 320 y 330 tiene lugar mediante las redes 305 y 335 respectivamente.

El router PIM-SM se comunica con los dos routers IGMP 320 y 330 mediante una red multiacceso 345 utilizando el protocolo PIM-SM.

El router 310 dispone de un agente SNMP 316 que incluye una base de datos MIB 317 que almacena información relativa al protocolo PIM-SM. Una fuente de tráfico multicast 318 está conectada al router PIM-SM 310 por medio de su interfaz de red 312 y puede transmitir tráfico multicast a la red de datos.

Los dos routers 320 y 330 disponen de agentes SNMP 326 y 336 respectivamente. Cada uno de estos agentes SNMP almacena información relativa al protocolo IGMP en su base de datos MIB 327 y 337 respectivamente.

El router IGMP 330 se comunica con un Proxy IGMP 340, que a su vez dispone de un agente SNMP 346 que almacena información relativa al protocolo IGMP en una base de datos MIB 347. Dicho Proxy IGMP 340 está en comunicación con dos dispositivos 380 y 390 que le informan de su estado mediante mensajes IGMP que solicitan recibir grupos multicast y canales multicast tal como se ha explicado anteriormente. El Proxy IGMP 340 agrupa la información de los grupos y canales multicast solicitados por los dispositivos 380 y 390 y envía unos mensajes IGMP al router 330 con la información agrupada tal como establecen las especificaciones RFC 4605.

El router IGMP 320 se comunica con tres dispositivos 350, 360 y 370 mediante una red multiacceso 325. Dichos dispositivos informan de su estado enviando mensajes IGMP al router 320 en los cuales solicitan grupos multicast y canales multicast.

La información del estado de los dispositivos 350, 360 y 370 puede llegar a la estación de control SNMP 300 por medio del agente SNMP 326 del router 320 o por medio del agente 316 del router 310. Esto permite establecer un control de los dispositivos que solicitan grupos multicast y canales multicast de forma jerárquica, permitiendo un control distribuido de los dispositivos de la red. Esta es otra ventaja de la presente invención que utiliza el propio árbol de comunicaciones multicast para establecer este control jerárquico.

De forma similar, la información del estado de los dispositivos 380 y 390 puede llegar a la estación de control SNMP 300 por medio del agente SNMP 346 del Proxy IGMP 340, por medio del agente SNMP 336 del router IGMP 330 o por medio del agente SNMP 316 del router PIM-SM 310. Esto permite a la estación de control 300 controlar los dispositivos 380 y 390 desde cualquiera de estos tres niveles de la red.

La estación de control SNMP 300 incorpora una aplicación que permite mostrar el estado de cada dispositivo a partir de la información de los grupos multicast y canales multicast solicitados por cada dispositivo.

La figura 3 también muestra una fuente de datos multicast 318 conectada al router PIM-SM 310. Si alguno de los dispositivos 350, 360, 370, 380 o 390 envía mensajes IGMP para recibir tráfico multicast de la fuente 318, el sistema descrito también permite monitorizar dicho tráfico multicast solicitado por los dispositivos.

De forma similar a lo explicado en la primera forma de realización, la estación de control puede enviar paquetes IP de datos multicast a un único dispositivo, utilizando un canal multicast que sólo ha solicitado dicho dispositivo, o a todos los dispositivos, utilizando un grupo multicast que han solicitado todos los dispositivos. Estos paquetes IP de datos pueden contener, por ejemplo, información para configurar los dispositivos, información para que los dispositivos sepan a qué router deben enviar los mensajes IGMP o cualquier otra información que sea útil a los dispositivos.

Tercera forma de realización de la invención

El funcionamiento del sistema de la figura 3 puede presentar sin embargo varios problemas debido a la forma en que están definidos los protoclos IGMPv3 y PIM-SM en el estado de la

técnica actual. Esta puede ser una causa por la que no se esté utilizando la tecnología multicast para el control de dispositivos en red.

Un primer problema en la figura 3 es que exista en la red 325 algún dispositivo que solicite tráfico multicast de alguno de los grupos multicast utilizados en los dispositivos mediante mensajes IGMP de tipo EXCLUDE para un determinado grupo multicast. En este caso, de acuerdo con el protocolo IGMPv3, se pierde en el router 320 la información de todos los canales multicast asociados a dicho grupo multicast solicitados por los dispositivos y la información del estado de los dispositivos no llega a la estación de control.

Por ejemplo, si el dispositivo 350 envía un mensaje IGMPv3· de tipo EXCLUDE ({},G5), de acuerdo con el protocolo IGMPv3, el router IGMP sólo almacena la petición del grupo multicast G5 y no almacena ninguna petición de canales multicast correspondiente al grupo G5 y por lo tanto se pierde la información de los canales multicast del grupo G5 solicitados por los dispositivos 360 y 370 y dicha información no llega a la estación de control.

El dispositivo 350 que envía el mensaje IGMP de tipo EXCLUDE puede ser un dispositivo que no implementa la presente invención. También puede suceder que el dispositivo 350 tenga algún virus u otro tipo de software que pretende interferir en el correcto funcionamiento de los dispositivos 360 y 370

Para evitar este problema es conveniente separar en los routers 320 y 330 las peticiones IGMPv3 de tipo INCLUDE y las peticiones IGMPv3 de tipo EXCLUDE. La solicitud de patente española número 2007011775 presentada por el solicitante el 26 de junio de 2007 y titulada “Procedimiento de gestión de tráfico multicast en una red de datos y dispositivos que utilizan dicho procedimiento” describe un router IGMPv3 que separa los mensajes INCLUDE y los mensajes EXCLUDE y puede aplicarse para resolver este problema.

Aplicando dicho procedimiento a los routers 320 y 330 de esta tercera forma de realización, se elimina dicho problema.

Un segundo problema relativo al protocolo IGMPv3 es que los routers IGMP no almacenan la información del tráfico multicast solicitado por cada equipo. Si hay varios dispositivos que solicitan el mismo grupo multicast, por ejemplo el grupo G9 para transmitir el estado 9 en la

tabla 1 del semáforo del ejemplo anterior, o varios dispositivos que solicitan el mismo canal multicast, por ejemplo el canal multicast (S1,G8) para transmitir la información del estado 8 de dicha tabla1, el router IGMP sólo almacena en cada interfaz de red si debe transmitir o no dicho tráfico, pero no almacena qué dispositivos han solicitado dicho tráfico. Esto puede suceder, por ejemplo, en los dispositivos 350, 360 y 370 de la figura 3 que están conectados a la misma interfaz de red 323 del router IGMP 320 mediante una red multiacceso, como por ejemplo una red ethernet.

Un problema similar al explicado en las redes multiacceso que conectan hosts con routers o routers con routers sucede cuando dichos equipos se comunican mediante un switch, ya que el switch es un equipo de nivel 2 que no sabe a qué puertos debe enviar los paquetes IP multicast y, por defecto, envía los paquetes multicast a todos los puertos.

Para evitar este problema, los routers IGMP 320 y 330 de la presente invención almacenan de forma separada la información del tráfico multicast solicitada por cada dispositivo.

Una primera forma de almacenar dicho tráfico multicast solicitado por cada dispositivo es hacerlo directamente en la base de datos MIB del agente SNMP del router IGMP y no tener en cuenta dicha información en el funcionamiento del router IGMP y en sus comunicaciones con los dispositivos que le envían mensajes IGMP solicitando tráfico multicast. Esta implementación es posible pero no es óptima.

Una segunda forma especialmente ventajosa de que los routers IGMP almacenen la información del tráfico multicast que solicita cada dispositivo es que lo hagan en los propios registros que utilizan para el ruteo IGMPv3. Esto tiene la ventaja de optimizar el funcionamiento del router IGMP, reduciendo la latencia y eliminando mensajes IGMP innecesarios.

La solicitud de patente española número 200702687 presentada por el solicitante el 15 de octubre de 2007 que tiene por título “Procedimiento de gestión de tráfico multicast en una red de datos y equipos de red que utilizan dicho procedimiento” resumida más adelante, describe un router IGMP mejorado que almacena la información del tráfico multicast solicitado por cada dispositivo y dicho funcionamiento de un router IGMP mejorado puede aplicarse a la presente invención para almacenar la información del tráfico multicast que

solicita cada dispositivo. Para que el agente SNMP puede enviar dicha información, sólo es necesario que además de guardar dicha información en los registros de ruteo, el router IGMP la almacene también en la base de datos MIB mejorada del agente SNMP del router mejorado.

La descripción de la base de datos MIB del router IGMP mejorado que almacena la información del tráfico multicast solicitado por cada dispositivo está al alcance de un experto en la materia que conozca el lenguaje SMIv2 ("Structure for Management Information") y no profundizaremos más en su explicación.

De esta forma, los routers IGMP 320 y 330 de la figura 3 son routers mejorados que almacenan el tráfico multicast solicitado por cada dispositivo y dicha información se almacena en la base de datos MIB del agente SNMP de cada router. Lo mismo sucede con el Proxy IGMP 340.

Un problema similar ocurre con el protocolo PIM-SM. En la figura 3 el router 310 se comunica con los routers 320 y 330 utilizando el protocolo PIM-SM en una red multiacceso 345. El protocolo PIM-SM del estado de la técnica tampoco almacena la información del tráfico solicitado por cada router PIM-SM y sólo almacena si debe transmitir o no un determinado tráfico por una deteminad interfaz de red del router. En la figura 3 este problema se presenta en la red multiacceso 345.

De la misma forma que con el protocolo IGMP, un router PIM-SM puede almacenar la información del tráfico solicitado por cada router de dos formas distintas: una primera forma poco óptima es hacerlo directamente en la base de datos MIB del agente SNMP y una segunda forma es almacenar dicha información en los registros de ruteo PIM-SM para optimizar el funcionamiento del router PIM-SM. En este segundo caso sólo es necesario que también se incluya dicha información en las base de datos MIB del agente SNMP del router PIM-SM.

La solicitud de patente española número 200702849 presentada por el solicitante el 30 de octubre de 2007, titulada "Procedimiento de gestión de tráfico multicast entre routers que se comunican mediante un protocolo que integra el protocolo PIM; y router y switch que intervienen en dicho procedimiento" y resumida más adelante, describe el funcionamiento

de un router PIM-SM mejorado que almacena la información del tráfico multicast que le solicita cada router PIM-SM y puede aplicarse a la presente invención.

De esta forma, el router PIM-SM 310 de la figura 3 es un router PIM-SM mejorado que almacena el tráfico multicast solicitado por cada router 320 y 330 en la red multiacceso 345 y dicha información se almacena también en la base de datos MIB del agente SNMP de cada router.

La descripción de la base de datos MIB del router PIM-SM mejorado que almacena la información del tráfico multicast solicitado por cada dispositivo está al alcance de un experto en la materia que conozca el lenguaje SMIv2 ("Structure for Management Information") y no profundizaremos más en su explicación.

También, de forma similar a lo explicado en la segunda forma de realización, si alguno de los dispositivos 350, 360, 370, 380 o 390 envía mensajes IGMP para recibir tráfico multicast de la fuente 318, la presente invención permite monitorizar dicho tráfico multicast solicitado por los dispositivos.

A continuación se muestra de forma resumida la información más relevante para la presente invención de las solicitudes de patentes españolas 2007011775, 200702687 y 200702849 que son incorporadas aquí por referencia.

Resumen de la patente española 200702687.

En el siguiente resumen, la palabra invención se refiere a la invención descrita en la solicitud de patente 200702687.

La segunda forma de realización de la solicitud de patente española 200702687 describe las principales características de la solicitud de patente española 200701775 por lo que se considera que la presente explicación es suficiente para entender la separación de registros INCLUDE y EXCLUDE.

1. Funcionamiento de un equipo de red perteneciente al estado de la técnica anterior que utiliza el protocolo IGMPv3 .

Para poner de relieve las características y ventajas de la invención, se expone en primer lugar el funcionamiento de un equipo de red que aplica el protocolo IGMPv3 de acuerdo con el estado de la técnica.

Para explicar la forma de agrupar los mensajes en un proxy que utiliza el protocolo IGMPv3, las especificaciones RFC 4605 que definen el funcionamiento del proxy IGMP se remiten al apartado 3.2 de las RFC 3376 que definen el protocolo IGMPv3. Las reglas son las mismas para deducir el estado de una interfaz de red de un host a partir de varios registros. A continuación se reproducen estas reglas adaptadas al funcionamiento en un proxy IGMP :

Regla 1. Para una determinada interfaz de red y grupo multicast, si alguna de las fuentes de datos de los mensajes recibidos del grupo es EXCLUDE, entonces se envía un mensaje de tipo EXCLUDE para el grupo y la lista de fuentes del mensaje es la intersección de las listas de fuentes EXCLUDE menos las fuentes de los mensajes INCLUDE.

Regla 2. Para una determinada interfaz de red y grupo multicast, si todas las fuentes de datos de los mensajes recibidos del grupo son de tipo INCLUDE, entonces se envía un mensaje de tipo INCLUDE para el grupo y la lista de fuentes de la interfaz de red es la unión de todas las fuentes INCLUDE.

Por lo tanto, el método que aplica un proxy IGMP consiste en agrupar las fuentes de los diferentes mensajes de cada grupo multicast recibidos en cada interfaz de red del proxy sin tener en cuenta cual es el host que envía el mensaje: el proxy almacena en qué interfaz de red ha recibido el mensaje IGMP, pero no almacena la identificación del host que ha solicitado cada fuente.

Lo mismo sucede en un router IGMP, cuyo funcionamiento se explica en el apartado 6 de las RFC 3376. Para cada interfaz de red del router IGMP y para cada grupo multicast, el router IGMP almacena la información de los canales y grupos multicast solicitados pero no almacena la identificación del host que solicita cada canal o cada grupo multicast.

Los routers IGMP envían periódicamente a los hosts unos mensajes denominados “Membership Query", para que los hosts contesten informando de los grupos y fuentes de los que desean recibir tráfico multicast. Los hosts también pueden enviar mensajes al router para solicitar tráfico multicast sin esperar a que el router IGMP envíe un mensaje “Membership Query”.

Los routers IGMP ejecutan el protocolo IGMP en todas las redes a las que están directamente conectados. Si un router IGMP tiene más de una interfaz de red conectada a la misma red sólo necesita ejecutar el protocolo en una de dichas interfaces de red.

Para cada tarjeta de red o interfaz de red, y para cada grupo multicast los routers IGMP almacenan la información de las fuentes INCLUDE y EXCLUDE multicast en un registro:

Registro : (multicast-address, group-timer, filter-mode, {(source-address, source-timer)})

donde

“multicast-address” es el grupo multicast.

{(source-address, source-timer)} 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.

"filter-mode" puede ser INCLUDE o EXCLUDE y tiene el mismo funcionamiento que el que se describe en las RFC 3376: indicar si las fuentes de la lista de fuentes y timers son fuentes INCLUDE o fuentes EXCLUDE.

“group-timer” es un timer que se utiliza como mecanismo para la transición del “filter-mode” de un registro de estado del router del modo EXCLUDE al modo INCLUDE. Cuando el “group-timer” de un determinado grupo multicast e interfaz de red llega a cero, el router asume que ya no quedan hosts con “filter-mode” EXCLUDE conectados a dicha interfaz de red y cambia al modo INCLUDE.

El valor de los timers va disminuyendo con el tiempo y cuando el router recibe de un host un mensaje “Membership Report” reinicializa los timers que correspondan.

Si el registro tiene un filter-mode 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.

Si el registro tiene un filter-mode 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.

Si un registro tiene un filter-mode EXCLUDE para un determinado grupo multicast, el router transmite todo el tráfico de todas las fuentes de dicho grupo multicast excepto las fuentes EXCLUDE de la lista "Exclude List".

El router utiliza también 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.

Hay varios motivos para que exista una lista “Requested List” en IGMPv3. Uno de ellos es que en una red con varios hosts enviando mensajes a un router IGMP, puede darse el caso de que haya un conflicto entre las peticiones de los diferentes hosts. Esto sucede, por ejemplo, cuando un host solicita tráfico de una determinada fuente y otro host solicita tráfico excluyendo dicha fuente. Por ejemplo, un host H1 envía un primer mensaje EXCLUDE({S1},G1) y otro host H2 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 host H1 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 IGMP 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 dicho 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 hosts para preguntar si hay algún host que todavía esté interesado en recibir el tráfico de las fuentes S2 y S3 del grupo G1

La Tabla 2 (al final del presente documento), extraída de las RFC 3376, resume el funcionamiento de un router según el protocolo IGMPv3.

En la Tabla 2, la primera columna "Estado 1" muestra el estado inicial del registro del router IGMP; la segunda columna "Mensaje" muestra el contenido de un mensaje "Membership Report" recibido por el router IGMP; la tercera columna "Estado 2" muestra el estado de dicho registro del router IGMP tras haber recibido el mensaje "Membership Report"; la cuarta y última columna "Acciones" muestra las acciones que el router IGMP realiza tras haber recibido dicho mensaje "Membership Report". La Tabla 2 contiene 12 filas que corresponden respectivamente a 12 ejemplos que ilustran cada uno el funcionamiento del router según su estado inicial (columna 1) y según los mensajes que ha recibido (columna 2). Cada fila de la Tabla 2 está separada de otra fila por una línea punteada.

La Tabla 2 se refiere a una determinada interfaz de red del router IGMP que ejecuta el protocolo IGMPv3 y un determinado grupo multicast G. Cada interfaz de red y grupo multicast G tendrá sus propios registros de estado que se verán afectados por los mensajes que reciba el router IGMP por dicha interfaz de red referidos a dicho grupo G.

En la Tabla 2 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 IGMP tiene un registro con "filter-mode" INCLUDE con un conjunto de fuentes A.

EXCLUDE (X,Y) indica que el router IGMP tiene un registro con "filter-mode" EXCLUDE porque hay fuentes EXCLUDE, siendo:

X la lista “Requested List” de fuentes EXCLUDE

Y la lista “Exclude List” de fuentes EXCLUDE

GMI es un parámetro denominado “Group Membership Interval” que contiene un valor de tiempo. Por defecto, toma un valor de 260 segundos.

T (S) es el timer "source timer" de la fuente S.

GT es el "Group Timer", es decir el timer del registro para cambiar de modo EXCLUDE a modo INCLUDE.

SEND Q(G, S) significa que el router IGMP envía un mensaje "Group-And-Source specific Query" a los host para comprobar si todavía hay algún host interesado en recibir las emisiones de las fuentes S del grupo multicast G. Cuando realiza esta acción, el router IGMP también reduce los timers de las fuentes S al valor LMQT. Si el router IGMP 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.

DEL(A) significa que el router IGMP suprime del registro las fuentes de la lista A.

LMQT es un 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" enviado por el router IGMP. Pasado este tiempo, si ningún host contesta que tiene interés en recibir los canales especificados en dicho mensaje, el router IGMP deja de transmitirlos. El valor por defecto de LMQT en el protocolo IGMPv3 es 20 segundos.

Los mensajes que aparecen en la columna 2 de la Tabla 2 son los seis tipos de mensajes IGMP definidos en el protocolo IGMPv3 para indicar al router las fuentes de las que se desea obtener tráfico multicast. El significado de estos seis mensajes IGMP está descrito en las RFC 3376 (capítulo 4.2.12) y es el siguiente:

IS_IN (Z), IS_EX (Z) indican que la interfaz de red del host que ha enviado el mensaje tiene un "filter-mode" INCLUDE o bien EXCLUDE, respectivamente, para las fuentes de la lista Z.

TO_IN (Z), TO_EX (Z) indican que la interfaz de red del host que ha enviado el mensaje ha pasado el "filter-mode" de modo EXCLUDE a modo INCLUDE, o bien de modo INCLUDE a modo EXCLUDE, respectivamente, para las fuentes de la lista Z.

ALLOW (Z) indica que la interfaz de red del host que ha enviado el mensaje desea recibir el tráfico de las nuevas fuentes de la lista Z. Estas fuentes son las que dicha interfaz de red añadirá a su lista de fuentes INCLUDE o bien las que suprimirá de su lista de fuentes EXCLUDE.

BLOCK (Z) indica que la interfaz de red del host que ha enviado el mensaje ya no desea recibir el tráfico de las fuentes de la lista Z. Estas fuentes son las que dicha interfaz de red suprimirá de su lista de fuentes INCLUDE o bien las que añadirá a su lista de fuentes EXCLUDE.

Se observará que las 12 filas de la Tabla 2 corresponden a las 12 posibles combinaciones de un registro de estado inicial del router (columna 1) y de un tipo de mensaje IGMP recibido (columna 2).

El router siempre consulta a los hosts mediante un mensaje “Group-And-Source-Specific-Query” (mensajes SEND en la columna 4 de la Tabla 2) para comprobar si hay algún host interesado en recibir aquellas fuentes cuyo tráfico se estaba transmitiendo inicialmente (columna 1 de la Tabla 2) y ya no se desea recibir según las fuentes indicadas en el último mensaje IGMPv3 recibido (columna 2 de la Tabla 2). Este funcionamiento es ineficiente, porque se envían mensajes de tipo “Group-And-Source-Specific-Query” innecesarios y, además, se transmite tráfico de fuentes que ningún host desea ya recibir. Además,

gestionar estas situaciones en los doce casos de la Tabla 2 supone una gran complejidad técnica.

Por otra parte, es usual que los usuarios de un sistema multicast, que actúan a través de los hosts, tengan un comportamiento conocido como "zapping", que consiste en cambiar de canal rápida y sucesivamente. Cuando un host solicita un nuevo canal, el router IGMP inicia la transmisión de dicho canal pero no la detiene cuando el host cambia otra vez de canal, si no que el router envía un mensaje “Group-And-Source-Specific-Query” y mantiene la transmisión durante el tiempo LMQT. Si esto sucede repetidas veces en un corto espacio de tiempo, el router IGMP tiene que gestionar todos estos mensajes y, además, estará emitiendo inútilmente toda la serie de canales por los que el usuario ha pasado haciendo "zapping".

La Tabla 3 (al final del presente documento) muestra un ejemplo concreto que ilustra estas ineficiencias. El ejemplo de la Tabla 3 se refiere al caso de un host que va cambiando de canal dentro de un grupo multicast G. La columna 1 de la tabla muestra los sucesivos mensajes IGMP enviados por el host, la columna 2 muestra la lista de fuentes cuyo tráfico envía el router tras haber recibido dicho mensaje IGMP, y la columna 3 muestra las acciones realizadas por el router tras haber recibido dicho mensaje IGMP. Los dos mensajes SEND Q(G, S1) y SEND Q(G, S2) (mensajes “Group-And-Source-Specific-Query” enviados por el router) que aparecen en la columna 3 de la Tabla 3 son innecesarios porque el host ya no desea recibir el tráfico emitido por las fuentes S1 y S2 que se indican respectivamente en dichos mensajes. También es innecesario que el router transmita los canales (S1, G) y (S2, G) durante el tiempo LMQT.

La gestión de mensajes innecesarios por parte el router implica un consumo considerable de capacidad de cálculo que podría evitarse. Además, la transmisión de tráfico no deseado consume innecesariamente ancho de banda. Cuando hay miles de hosts realizando cambios de canal estas ineficiencias se multiplican en el router.

2. Primera forma de realización de la invención de la patente 200702687.

El funcionamiento de los equipos de red que aplican el protocolo IGMP según la invención es similar al de los equipos de red del estado de la técnica que aplican 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.

Por otra parte, como el funcionamiento del protocolo IGMP según la invención es similar al del protocolo IGMPv3, no se explican todas las características que son comunes al IGMPv3.

La característica principal de la invención consiste en que los equipos de red que reciben mensajes IGMPv3 mediante los cuales los hosts solicitan tráfico multicast, como son un router IGMPv3, un switch y un proxy IGMPv3, almacenan en una tabla la información separada de las fuentes que solicita cada host que envía mensajes IGMPv3 solicitando tráfico multicast junto con un identificador único del host que ha enviado cada mensaje.

Para ello, estos equipos de red mantienen un registro de estado para cada interfaz de red, grupo multicast y host que envía el mensaje, con lo cual conocen con exactitud cuales son las fuentes de tráfico multicast solicitadas por cada host de forma independiente.

Al almacenar la información por separado identificando las peticiones de cada host, ya no hay conflictos entre las fuentes solicitadas en los mensajes de diferentes hosts, ya que cuando un host envía un mensaje para dejar de recibir un determinado canal (S,G) a una interfaz de red de un router IGMP, dicho router conoce con exactitud si hay otro host conectado a esa misma interfaz de red e interesado en recibir ese mismo canal (S,G). Si hay otro host interesado, el router IGMP continúa transmitiendo el canal (S,G), pero si no hay ningún otro host interesado deja de emitir el canal (S,G) en el mismo momento en que recibe el mensaje que le pide que deje de transmitirlo, sin necesidad de enviar un mensaje “Group-And-Source-Specific Query” y esperar la respuesta.

Tal como indican las RFC 3376, al inicio del apartado 4, los mensajes IGMP se encapsulan en datagramas IPv4, con número de protocolo 2. Un datagrama IPv4 contiene un campo que indica la dirección IP del equipo que envía dicho datagrama.

Una forma particularmente eficaz para implementar la presente invención consiste en utilizar, como identificador del equipo que envía cada mensaje IGMP, la dirección IP de

dicho equipo. Es posible que algunos equipos que envían mensajes IGMP no dispongan de una IP propia. Esto sucede, por ejemplo, en algunos tipos de DSLAM que envían los mensajes IGMP usando la IP 0.0.0.0. En estos casos es posible asignar una dirección IP al DSLAM y que éste la utilice en sus mensajes IGMP.

También puede utilizarse como identificador de dicho host la dirección MAC Address ("Media Access Control Address") de la trama de datos que encapsula el paquete de datos IP que transporta el mensaje IGMP enviado por el host. El uso de este identificador es particularmente útil en los switches que implementan la presente invención pues los switches son equipos de nivel 2 que conocen en qué puerto se halla conectado cada equipo identificándolo por su MAC Address y no por su dirección IP.

A continuación se describe en detalle el funcionamiento del protocolo IGMP según la invención en cada uno de los equipos de red: el router IGMP mejorado, el proxy IGMP mejorado y un switch mejorado que realiza la función IGMP "snooping".

2.1) Funcionamiento de un router IGMP mejorado.

La principal diferencia con respecto a los routers IGMP del estado de la técnica que aplican los protocolos IGMPv3 y MLDv2 es que el router IGMP mejorado según la invención tiene un registro de estado para cada interfaz de red, grupo multicast y host de origen, donde almacena las fuentes solicitadas por cada host:

Registro : (interface, multicast-address, hostID, group-timer, filter-mode {(source-address, source-timer)})

donde

“interface” indica la interfaz de red del router por la cual el router IGMP ha recibido el mensaje IGMP.

“multicast-address” es el grupo multicast.

“hostID” es un identificador del host que ha enviado el mensaje IGMP.

{(source-address, source-timer)} 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.

"filter-mode" puede ser INCLUDE o EXCLUDE y tiene el mismo funcionamiento que el que se describe en las RFC 3376: indicar si las fuentes de la lista de fuentes y timers son fuentes INCLUDE o fuentes EXCLUDE.

En los registros de estado que tienen un "filter-mode" EXCLUDE 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.

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.

Cada mensaje que recibe el router IGMP por una determinada interfaz de red, de un determinado host y referido a un determinado grupo multicast, sólo afecta al registro de estado de dichos interfaz de red, host y grupo multicast.

Gracias a que el router IGMP mejorado identifica el origen de cada mensaje IGMP, puede comportarse de una forma determinista para cada host, es decir que los mensajes de cada host determinan el estado de los registros del router asociados a dicho host y no es necesario realizar consultas a otros hosts ni tener en cuenta otros hosts.

Este comportamiento determinista del router IGMP queda claramente reflejado en la Tabla 4 (al final del presente documento), que es análoga a la Tabla 2 pero para un router IGMP mejorado según la invención.

La Tabla 2 se refiere a una determinada interfaz de red del router, mientras que la Tabla 4 se refiere a una determinada interfaz de red del router y un determinado host que envía mensajes IGMP.

Ambas tablas muestran las mismas combinaciones de estados iniciales (columna 1) y mensajes IGMP recibidos (columna 2), pero como puede verse, los estados finales (columna 3) y las acciones del router IGMP (columna 4) son diferentes. En particular, puede apreciarse que en la Tabla 4, la columna 4 (acciones realizadas por el router IGMP) no contiene ningún mensaje SEND Q(G,S), ya que el router IGMP mejorado según la invención no necesita enviar mensajes "Group-And-Source-Specific Querys" para comprobar si queda algún host interesado en recibir el canal (S,G).

Cuando el router IGMP mejorado tiene que decidir si debe transmitir un determinado canal por una determinada interfaz de red, el algoritmo de dicho router tiene en cuenta los diferentes registros de estado de los hosts que hacen referencia a dicho grupo multicast y dicha interfaz de red.

Para una determinada interfaz de red, un determinado grupo multicast G, y una determinada fuente S INCLUDE, mientras exista un registro de estado de algún host referido a dicha interfaz de red y dicho grupo multicast G cuyo "filter-mode" sea INCLUDE y cuyo "source-timer" asociado a dicha fuente S INCLUDE sea mayor que cero, el router IGMP mejorado transmitirá por dicha interfaz de red el tráfico multicast del canal (S,G). Además, si para dichos interfaz de red y grupo multicast G, existen registros de estado cuyo "filter-mode" sea EXCLUDE, el router IGMP mejorado transmitirá además por dicha interfaz de red el tráfico multicast de todas las fuentes excepto las del conjunto que resulta de la intersección de todas las listas "Exclude List" de dichos registros de estado con "filter-mode" EXCLUDE para dicha interfaz de red y grupo multicast G.

Cuando el timer asociado a una determinada fuente S INCLUDE de un registro de estado con "filter-mode" INCLUDE llega a cero, dicha fuente S se elimina de la lista de fuentes INCLUDE de dicho registro de estado.

Cuando un registro de estado con "filter-mode" INCLUDE no contiene ninguna fuente en su lista INCLUDE, dicho registro de estado es eliminado.

La lista “Requested List” sigue siendo necesaria en el router IGMP mejorado para cambiar un registro de estado de "filter-mode" EXCLUDE a "filter-mode" INCLUDE, tal como se explica en el apartado 3 del apéndice A de las RFC 3376.

Otra ventaja de mantener la lista “Requested List” es que permite gestionar de forma eficaz la situación que se produce cuando el router IGMP mejorado tiene un registro con un "filter-mode" EXCLUDE para una determinada interfaz de red de dicho router, un determinado grupo multicast y un determinado host, y dicho router recibe de ese mismo host un segundo mensaje que le indica que desea recibir tráfico de una determinada fuente S1, por ejemplo un mensaje ALLOW (S1). En este caso si el router elimina la fuente S1 de la “Exclude List”, y no existiera la lista "Requested List", dicho router perdería la información de la dirección IP de la fuente S1 y tendría que utilizar algoritmos de ruteo de tipo ASM para recibir el tráfico de la fuente S1. Al mantener en la “Requested List” la información de S1, dichas información no se pierde y puede ser utilizada por el router para acceder directamente a la fuente S1.

3) Segunda forma de realización de la invención de la patente 200702687

La forma de realización de la invención que se describe a continuación implementa una modificación del protocolo IGMP que permite que un router o un proxy IGMP no esté obligado a combinar las peticiones de tráfico que recibe referidas a un mismo grupo multicast en un solo mensaje IGMP de tipo INCLUDE o de tipo EXCLUDE, como exige actualmente el protocolo IGMPv3, si no que pueda combinarlas en un mensaje de tipo INCLUDE y en un mensaje de tipo EXCLUDE y enviar ambos mensajes.

Para que los routers IGMP y los proxys IGMP puedan funcionar de esta forma, es decir agrupando separadamente los mensajes INCLUDE y los mensajes EXCLUDE y enviando mensajes PIM-SM independientes para cada grupo multicast y filter-mode del protocolo IGMP, se han desarrollado unas modificaciones adicionales al protocolo IGMP, además de las explicadas en el primer ejemplo de realización.

El protocolo IGMP modificado según la invención se diferencia del protocolo explicado anteriormente en que las interfaces de red, además de hacer un seguimiento individual de

las fuentes que solicita cada host de origen que envía cada mensaje, pueden funcionar en modo dual: pueden almacenar y transmitir por separado la información de las fuentes contenidas en los mensajes IGMP de tipo INCLUDE y la información de las fuentes contenidas en los mensajes IGMP de tipo EXCLUDE.

Para ello, el protocolo IGMP modificado guarda dos registros: uno para el “filter-mode” EXCLUDE y otro para el “filter-mode” INCLUDE para cada interfaz de red y grupo multicast. Así, un proxy o router IGMP que utiliza el protocolo IGMP modificado puede guardar, para cada interfaz de red y grupo multicast, dos registros separados:

Registro INCLUDE: (interface, multicast-address, hostID, group-timer, filter-mode =INCLUDE, {(source-address, source-timer)})

Registro EXCLUDE: (interfaz, multicast-address, hostID, group-timer, filter-mode =EXCLUDE, {(source-address, source-timer)})

donde

“interface” indica la interfaz de red del router por la cual el router IGMP ha recibido el mensaje IGMP.

“multicast-address” es el grupo multicast.

“hostID” es un identificador del host que ha enviado el mensaje IGMP.

{(source-address, source-timer)} 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.

"filter-mode" puede se INCLUDE o EXCLUDE y tiene el mismo funcionamiento que el que se describe en las RFC 3376: indicar si las fuentes de la lista de fuentes y timers son fuentes INCLUDE o fuentes EXCLUDE.

Cuando el router o el Proxy IGMP mejorado tiene que decidir si debe transmitir un determinado canal por una determinada interfaz de red, el algoritmo de dicho router o proxy tiene en cuenta los diferentes registros de estado de los hosts que hacen referencia a dicho grupo multicast y dicha interfaz de red, pero con la diferencia de que ahora los hosts pueden tener dos registros de estado con diferentes filter-mode INCLUDE y EXCLUDE, para un mismo grupo multicast. El algoritmo aplica las reglas siguientes:

- Para una determinada interfaz de red, un determinado grupo multicast G, y una determinada fuente S INCLUDE, mientras exista un registro de estado de algún host referido a dicha interfaz de red y dicho grupo multicast G cuyo filter-mode sea INCLUDE y cuyo source-timer asociado a dicha fuente S INCLUDE sea mayor que cero, el router IGMP mejorado transmitirá por dicha interfaz de red el tráfico multicast del canal (S,G).

- Además, si para dichos interfaz de red y grupo multicast G, existen registros de estado cuyo filter-mode sea EXCLUDE, el router IGMP mejorado transmitirá además por dicha interfaz de red el tráfico multicast de todas las fuentes excepto las del conjunto que resulta de la intersección de todas las listas “Exclude List” de dichos registros de estado con filter-mode EXCLUDE para dicha interfaz de red y grupo multicast G.

En la Tabla 5 (al final del presente 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 una determinada interfaz de red, un determinado grupo multicast G y un determinado host, de dos registros de estado para dicho grupo multicast G porque tiene tanto fuentes INCLUDE como fuentes EXCLUDE.

Al igual que la Tabla 4, la Tabla 5 se refiere a una determinada interfaz de red del router y un determinado host que envía mensajes IGMP.

Como se puede observar en la Tabla 5, el uso de dos registros separados para almacenar las fuentes INCLUDE y EXCLUDE junto con el seguimiento individual de las peticiones de tráfico de cada host, permite eliminar la lista “Requested-List” que ya no es necesaria. Las listas EXCLUDE(Y), representan las Exclude-List y las fuentes EXCLUDE ya no necesitan timers, lo que simplifica su funcionamiento.

El Group-Timer o GT se sigue utilizando para eliminar el registro EXCLUDE cuando dicho timer llega a cero.

También se puede observar en la Tabla 5 que se han definido cuatro nuevos mensajes IGMP. Los dos primeros ALLOWIN (B) y BLOCKIN (B) modifican las fuentes del registro INCLUDE y los dos últimos ALLOWEX (B) y BLOCKEX (B) modifican las fuentes del registro EXCLUDE.

De la misma forma, el mensaje IS_IN(B) sólo afecta al registro INCLUDE y el mensaje IS_EX(B) sólo afecta al registro EXCLUDE. Esta separación de los mensajes que afectan a los registros INCLUDE y EXCLUDE aporta una gran simplicidad. Comparando la Tabla 5 con la Tabla 2, resulta evidente que la Tabla 5 es mucho más sencilla que la Tabla 2. Además de haber simplificado la gestión de los timers y eliminado el envío de mensajes "Group-And-Source-Specific-Query", se ha conseguido que el router IGMP sólo tenga que gestionar los seis casos que corresponden a las seis filas de la Tabla 5, en lugar de los doce casos que aparecen en la Tabla 2. La comparación entre las Tablas 2 y 5 pone pues de manifiesto que el protocolo IGMP mejorado facilita considerablemente la implementación y programación de los algoritmos en los routers, además de solucionar los problemas de ineficiencia antes mencionados.

Para las comunicaciones entre un host y un router IGMP, el protocolo IGMP modificado utiliza los mismos mensajes que el protocolo IGMPv3, que se describen en el apartado 4 de las RFC 3376. La única diferencia está en el formato interno de los bloques de datos denominados "Group Record" que están contenidos en cada mensaje "Membership Report": en el protocolo IGMP modificado, cuando hay fuentes INCLUDE y también fuentes EXCLUDE para el mismo grupo multicast se incluyen en el mensaje "Membership Report" dos "Group Record": uno para las fuentes INCLUDE y otro para las fuentes EXCLUDE.

<u>Resumen de la solicitud de patente española número 200702849</u>

En el siguiente resumen, la palabra invención se refiere a la invención de la solicitud de patente española 200702849.

En lo que sigue, y siguiendo la nomenclatura común en la tecnología SSM, se denomina canal (S,G) a la emisión de la fuente S del grupo multicast G, donde S es una dirección IP que identifica la fuente que emite los datos y G es una dirección IP, dentro del rango reservado para grupos multicast, que identifica el grupo multicast.

Asimismo, en lo que sigue se utilizarán las expresiones “upstream” y “dowstream” para indicar unas ubicaciones relativas desde un equipo de red: la expresión “upstream” se refiere a una ubicación en dirección a la fuente multicast y la expresión “downstream” se refiere a una ubicación en la dirección contraria.

En los primeros protocolos de ruteo multicast, como por ejemplo el protocolo DVMRP (“Distance Vector Multicast Routing Protocol”), los routers intercambiaban entre sí unos mensajes denominados “DVMRP Route Reports” con información para construir la base de datos de topología multicast. La base de datos de topología multicast es donde los routers almacenan la información de todos los routers multicast que hay en la red y cómo están conectados entre sí. En el protocolo DVMRP, cada router enviaba cada 60 segundos estos mensajes.

El protocolo PIM-SM funciona de una forma diferente. Los routers PIM-SM no envían mensajes para crear la base de datos de topología multicast, sino que utilizan la base de datos unicast del router para deducir a partir de ella la base de datos de topología multicast y lo hacen independientemente del protocolo unicast que utilice el router. De aquí viene el nombre de “Protocol Independent Multicast”. De esta forma, PIM-SM no depende de ningún protocolo unicast concreto y puede crear la base de datos de topología multicast en los routers independientemente del protocolo unicast que utilice cada router.

En el protocolo PIM-SM la base de datos de topología multicast es almacenada en una tabla denominada MRIB (“Multicast Routing Information Base”) que se usa, entre otras cosas, para decidir a qué router deben ser enviados los mensajes JOIN/PRUNE. Estos mensajes JOIN/PRUNE del protocolo PIM-SM, que son de sobra conocidos por el experto en la materia, son los mensajes que envía un router PIM-SM a otro router PIM-SM para indicar que desea recibir tráfico multicast (mensajes JOIN) o que desea dejar de recibir tráfico multicast (mensajes PRUNE). Los datos multicast se transmiten hacia el router que

ha solicitado el tráfico multicast siguiendo la misma dirección que los mensajes JOIN, pero en el sentido contrario.

Un primer problema que afecta al protocolo PIM-SM es el retraso en transmitir los mensajes de tipo "PRUNE" que envía un router PIM-SM a otro router PIM-SM para indicarle que no desea seguir recibiendo un determinado tráfico multicast. Cuando un router PIM-SM recibe un mensaje de tipo PRUNE, por ejemplo PRUNE (S,G), no deja de transmitir inmediatamente el tráfico del canal multicast (S,G), sino que espera un tiempo determinado antes de dejar de transmitir el canal multicast (S,G) por su interfaz de red donde ha recibido el mensaje de tipo PRUNE. En la configuración por defecto del protocolo PIM-SM este tiempo de espera es de 3 segundos. El motivo de este tiempo de espera es que puede haber otros routers PIM-SM compartiendo una red multiacceso y es posible que haya otro router PIM-SM que desee seguir recibiendo el canal multicast (S,G), para lo cual dicho router debe enviar un mensaje JOIN(S,G) de forma inmediata para cancelar el efecto del anterior mensaje PRUNE(S,G).

Si el número de routers es alto y hay miles de usuarios realizando cambios de canales multicast, la consecuencia es que hay una enorme cantidad de ancho de banda ocupado en la red por la latencia o retraso en suprimir la transmisión de canales multicast no deseados. Si además los canales multicast (S,G) transmiten video o canales IPTV que requieren un ancho de banda de entre 4 Mbits/s en resolución normal y 20 Mbits/s en alta resolución, el problema se agrava considerablemente.

Las RFC 4601, en el apartado 4.3.3 "Reducing PRUNE Propagation Delay on LANs", proponen una solución al problema de latencia que consiste en utilizar los mensajes "Hello" que utilizan los routers PIM-SM para intercambiar información entre ellos y negociar varios parámetros. Los mensajes "Hello" se utilizan, por ejemplo, para negociar si hay o no supresión de mensajes PIM-SM, el tiempo de retardo en los mensajes PRUNE y otros parámetros. Los routers PIM-SM envían estos mensajes "Hello" de forma periódica, por cada interfaz de red del router donde esté ejecutándose el protocolo PIM-SM, a una dirección multicast denominada "ALL-PIM-ROUTERS". Gracias a estos mensajes "Hello", cada router PIM-SM conoce la existencia de otros routers PIM-SM conectados en cada una de sus interfaces de red. Todos los routers almacenan además la información de configuración de los demás routers que se ha intercambiado mediante mensajes "Hello".

Sin embargo, los mensajes “Hello” utilizados en el protocolo PIM-SM no transmiten información sobre la topología de routers multicast. Esta información la deduce el router PIM-SM a partir de las tablas de ruteo unicast.

Como se ha dicho anteriormente, cuando un router PIM-SM recibe un mensaje de tipo PRUNE(S,G) espera un tiempo para ver si hay otro router que envía un mensaje JOIN(S,G) que cancele el primer mensaje PRUNE. El tiempo de espera es la suma de dos variables denominadas “Effective_Propagation_Delay” y “Effective_Override_Interval”, que por defecto toman los valores de 0,5 segundos y 2,5 segundos, respectivamente. El motivo de utilizar como retardo esta suma de dos variables es el siguiente: si hay un router R1 que está recibiendo el tráfico del canal multicast (S,G) de un router R2, y el router R1 ve que otro router R3 envía un mensaje PRUNE(S,G), el router R1 debe enviar un mensaje de tipo JOIN(S,G) al router R2 para cancelar el efecto del mensaje PRUNE (S,G) antes del tiempo “Effective_Override_Interval”. Como “Effective_Override_Interval” siempre es menor que la suma de “Effective_Override_Interval” y “Effective_propagation_Delay”, el mensaje JOIN(S;G) del router R1 llegará al router R2 antes de que el router R2 deje de enviar el tráfico del canal multicast (S,G).

La solución que proponen las RFC 4601 para reducir el tiempo de latencia consiste en que los routers PIM-SM utilicen los mensajes “Hello” para reducir los valores de las variables “Effective_Propagation_Delay” y “Effective_Override_Interval”. Para ello, todos los routers PIM-SM anuncian sus propios parámetros “Propagation_Delay” y “Override_Interval” en los mensajes “Hello”. Estos parámetros están contenidos en los mensajes “Hello” en un bloque de datos denominado “LAN_PRUNE_Delay”. Cuando todos los routers que ejecutan el protocolo PIM-SM en una red han enviado mensajes “Hello” incluyendo el bloque de datos “LAN_PRUNE_Delay”, todos los routers conectados a una misma red multiacceso utilizan como valores de “Effective_Propagation_Delay” y “Effective_Override_Interval” los valores máximos de los parámetros “Propagation_Delay” y “Override_Interval”, respectivamente, que han sido anunciados por dichos routers en los mensajes “Hello”.

Sin embargo, este mecanismo tiene varias limitaciones.

En primer lugar, las propias RFC 4601 indican que si las variables "Effective_Propagation_Delay" y "Effective_Override_Interval", toman valores muy bajos es posible que, siguiendo con el ejemplo anterior, el router R2 suprima el tráfico del canal (S,G) antes de que el router R1 tenga tiempo de enviar su mensaje JOIN o antes de que el router R2 tenga tiempo de procesar dicho mensaje. Para evita este problema, las RFC 4601 recomiendan no bajar demasiado los valores de estas variables. Esta es una grave limitación de este mecanismo de reducción de latencia.

Además, otra limitación o problema que tiene este mecanismo de reducción de latencia es que es necesario que todos los routers que ejecutan el protocolo PIM-SM en una red envíen mensajes incluyendo el bloque de datos "LAN_PRUNE_Delay". Si hay un router que no incluye este bloque de datos en sus mensajes "Hello", ya no se puede utilizar este mecanismo de reducción de latencia y las variables "Effective_Propagation_Delay" y "Effective_Override_Interval" toman sus valores por defecto, que son de 2,5 segundos y 0,5 segundos respectivamente, en todos los routers de la red multiacceso, causando por lo tanto una latencia de 3 segundos en cada router.

Por otra parte, al final del mencionado apartado 4.3.3 de las RFC 4601 dedicado a la reducción de la latencia, se explica que es posible que un router PIM-SM upstream lleve un control o seguimiento individual de las peticiones de tráfico multicast de varios routers downstream. Aunque no explica cómo implementar dicho seguimiento individual ni qué utilidad tiene, sí indica que para hacerlo es imprescindible que todos los routers de la misma red multiacceso se pongan primero de acuerdo en cancelar la supresión de mensajes. El apartado mencionado 4.3.3 de las RFC 4601 incluye incluso el código que se puede utilizar para comprobar que todos los routers se han puesto de acuerdo en cancelar la supresión de mensajes.

Un segundo problema que afecta al protocolo PIM-SM es la complejidad del mecanismo de supresión de mensajes JOIN. Básicamente, la supresión de mensajes JOIN consiste en que si un router downstream R1 ve que otro router downstream R2 envía un mensaje JOIN solicitando el mismo tráfico multicast que el que iba a pedir, dicho router R1 puede suprimir su propio mensaje JOIN, pues basta con que el router upstream reciba una única solicitud para que transmita el tráfico multicast solicitado.

En la última versión del protocolo multicast IGMP (versión IGMPv3), mediante el cual los hosts solicitan tráfico multicast a un router, se ha cancelado la supresión de mensajes, que existía en las versiones anteriores de IGMP. En cambio, en el protocolo PIM-SM, mediante el cual un router solicita tráfico multicast a otro router, todavía existe la supresión de mensajes. De hecho, la supresión de mensajes es la configuración por defecto que debe aplicarse según las RFC 4601. Existe una opción de configuración para que no se realice la supresión de mensajes, pero sólo se aplica en determinadas circunstancias y requiere una implementación compleja.

El mecanismo de supresión de mensajes que se aplica en el protocolo PIM-SM, según las RFC 4601, es muy complicado. También es muy complicado el mecanismo para cancelar la supresión de mensajes, según las RFC 4601. Por ello, cualquier modificación del protocolo PIM-SM relacionada con la supresión de mensajes es muy complicada. Probablemente esto explica la falta de investigación de mejoras en el protocolo PIM-SM relacionadas con la supresión de mensajes. Por otra parte, al final del mencionado apartado 4.3.3 de las RFC 4601 se indica que para hacer un seguimiento individual del tráfico multicast que solicita cada router dowsntream, es necesario cancelar la supresión de mensajes. Según las RFC 4601, si hay routers que suprimen mensajes no es posible hacer el seguimiento individual del tráfico multicast que solicita cada router.

La descripción siguiente ilustra lo complejos que son el mecanismo de supresión de mensajes y las condiciones para cancelar dicha supresión de mensajes, según las RFC 4601.

Para explicar el mecanismo de supresión de mensajes un experto en la materia tiene que analizar y entender en detalle la máquina de estados denominada “upstream” (S,G), mediante la cual las RFC 4601 especifican el funcionamiento del envío “upstream” de mensajes de tipo JOIN (S,G). Esta máquina de estados se encuentra ilustrada en forma de una tabla en el apartado "4.5.7 Sending (S,G) Join/Prune messages" de las RFC 4601.

Cada máquina de estados “upstream“ (S,G) es independiente para cada interfaz de red del router y para cada canal multicast (S,G) y tiene sólo dos estados: el estado “Not_Joined”, que significa que el router no necesita recibir el canal multicast (S,G) por dicha interfaz de red, y el estado “Joined”, que significa que el router necesita recibir el canal multicast (S,G)

por dicha interfaz de red.

Si la máquina de estados está en el estado “Not_Joined”, y por tanto el router no está recibiendo el canal multicast (S,G), y se produce un evento “JoinDesired(S,G)->true”, que indica que el router ha recibido una petición de tráfico del canal (S,G) por parte de otro router “downstream”, la máquina de estados del router ejecuta las acciones siguientes: cambiar el estado a “Joined”, enviar un mensaje JOIN (S,G) a otro router “upstream” que figura en su tabla MRIB como apto para enviarle el tráfico del canal (S,G), e inicializar un timer denominado “Join_Timer” a un valor inicial denominado “t_periodic”.

En el estado “Joined”, cuando sucede el evento “Timer_Expires”, que indica que el timer “Join_Timer” ha llegado a cero, el router envía (“Send Join(S,G)”) un nuevo mensaje JOIN (S,G) y vuelve a inicializar el timer “Join_Timer” al valor “t_periodic”.

Por lo tanto, en el estado “Joined” el router vuelve a enviar de forma periódica los mensajes JOIN (S,G) para seguir recibiendo el tráfico del canal multicast (S,G).

Cuando sucede el evento “See Join(S,G) to RPF’(S,G)”, que indica que el router ha visto en la red multiacceso a la que está conectado que otro router ha enviado un mensaje similar al mensaje JOIN (S,G) que tiene que enviar cuando el timer “Join_Timer” llegue a cero, el router incrementa el valor del timer “Join_Timer” para retrasar el envío de su propio mensaje JOIN (S,G). Esto se explica con mayor detalle en la página 74 de las RFC 4601, que indica que si el timer “Join_Timer” tiene un valor menor que una variable denominada “t_joinsuppress” entonces se inicializa dicho timer “Join_Timer” con el valor de esta variable “t_joinsuppress”. Si en cambio el timer “Join_Timer” tiene un valor mayor que la variable “t_joinsuppress”, entonces el timer “Join_Timer” no se modifica.

Por lo tanto, el mecanismo de supresión de mensajes del protocolo PIM-SM consiste en aumentar el valor del timer “Join_Timer” que controla el envío periódico de mensajes JOIN (S,G). Como el aumento del timer “Join_Timer” al valor “t_joinsuppress” se realiza cada vez que el router ve en la red multiacceso un mensaje JOIN (S,G) de otro router, el timer “Join_Timer” se vuelve a inicializar al valor “t_joinsuppress” de forma periódica y nunca llega a cero. Esto es lo que hace que el router no envíe su propio mensaje JOIN (S,G), es decir que suprima su propio mensaje JOIN (S,G) periódico mientras haya otro router en la

misma red multiacceso que esté enviando un mensaje JOIN (S,G) equivalente.

Hasta aquí se ha explicado cómo funciona la supresión de mensajes en el protocolo PIM-SM. Ahora se va explicar cómo funciona el mecanismo que cancela dicha supresión de mensajes.

El mecanismo para cancelar la supresión de mensajes en el protocolo PIM-SM, según se deduce de las RFC 4601, consiste en hacer que el valor de la variable "t_joinsuppress" sea cero. Cuando el router ve un mensaje JOIN (S,G) comprueba si el timer "Join_Timer" es menor que la variable "t_joinsuppress", que es igual a cero, lo cual obviamente nunca sucede, y deja dicho timer "Join_Timer" sin modificar. De esta forma, el router envía su propio mensaje JOIN (S,G) cuando su timer "Join_Timer", que no se ve modificado por los mensajes de los demás routers, llega a cero.

La variable "t_joinsuppress" toma el valor menor entre el valor de otra variable denominada "t_suppressed" y un parámetro denominado "holdtime" que es transmitido en los mensajes JOIN (S,G) y que indica durante cuánto tiempo el router que ha envía el mensaje JOIN (S,G) desea estar recibiendo el canal (S,G). La variable "t_suppressed" toma un valor diferente en función de si está o no habilitada la supresión de mensajes. Hay una función denominada "Suppression_Enabled(I)" que es específica para cada interfaz de red I y que devuelve el valor TRUE si la supresión de mensajes está permitida, y el valor FALSE si la supresión de mensajes está cancelada:

Si la función "Supression_Enabled(I)" devuelve un valor TRUE entonces la variable "t_suppressed" toma un valor aleatorio dentro del rango [1,1 * "t_periodic"; 1,4 * "t_periodic"], donde "t_periodic" es una variable que por defecto toma el valor de 60 segundos.

Si la función "Supression_Enabled(I)" devuelve el valor FALSE, la variable "t_suppresed" es cero, y también es cero la variable "t_joinsuppress", que toma el valor menor entre "t_suppressed" y el parámetro "holdtime". De esta forma se evita modificar el timer "Join_Timer" cuando la función "Supression_Enabled(I)" devuelve un valor FALSE y así cada router envía sus mensajes periódicos JOIN (S,G) sin tener en cuenta los mensajes JOIN (S,G) que envían los demás routers, con lo cual se ha cancelado la supresión de

mensajes.

Este mecanismo de cancelación de la supresión de mensajes definido en las RFC 4601 es innecesariamente complicado. Además, es ineficiente porque si la función "Supression_Enabled(I)" devuelve un valor FALSE, el router, antes de tomar la decisión de modificar o no el timer "Join_Timer", habrá comprobado dos veces si una cantidad positiva es menor que cero, algo que no puede suceder.

Como el protocolo PIM-SM es un protocolo complejo, los programadores de aplicaciones que implementan dicho protocolo siguen las especificaciones RFC 4601 de la forma más exacta posible para evitar enfrentarse a nuevos problemas de diseño que no estén previstos en dichas especificaciones. Como consecuencia de ello, las aplicaciones que implementan el protocolo PIM-SM presentan las limitaciones expuestas anteriormente. Estas limitaciones, junto a la complejidad que supone la supresión de mensajes en el protocolo PIM-SM, son los motivos por los cuales hasta ahora no se ha desarrollado ninguna solución satisfactoria al problema de la latencia en el protocolo PIM-SM.

Descripción detallada de unas formas de realización de la patente española número 200702849

1) Router mejorado

La Fig. 4 muestra un ejemplo simplificado de un sistema de comunicaciones multicast en el cual operan seis routers PIM-SM 410, 420, 430, 440, 450 y 470. Una fuente 400 que emite un canal multicast (S,G) está conectada al router 410, que transmite dicho canal multicast por medio de los routers PIM-SM 410, 420, 430 y 440, hasta llegar al router 450 que está conectado a un host 460 que desea recibir dicho canal (S,G). El host 460 indica al router 450 el tráfico multicast que desea recibir. Para ello, el host 460 y el router 450 se comunican mediante el protocolo IGMPv3 o el protocolo MLDv2.

El router 440 y el router 450 están conectados entre sí mediante una red local multiacceso 445, por ejemplo una red Ethernet, a la que pueden estar conectados otros routers PIM-

SM. En la figura se muestra sólo otro router PIM-SM 470 conectado a la red multiacceso 445, pero evidentemente pueden haber más routers PIM-SM conectados a dicha red 445. De la misma forma, hay otra red local multiacceso 435 entre los routers 440 y 430, otra red multiacceso 425 entre los routers 430 y 420 y otra red multiacceso 415 entre los routers 420 y 410. En cada una de estas redes multiacceso 415, 425 y 435 pueden haber otros routers PIM-SM conectados, que no se muestran en la figura para simplificarla.

En el ejemplo, cada router 410, 420, 430, 440 y 450 tiene una interfaz de red "upstream", respectivamente 411, 421, 431, 441 y 451, y una interfaz de red "downstream", respectivamente 412, 422, 432, 442 y 452.

El canal multicast (S,G) se transmite desde la fuente 400 hacia el host 460 siguiendo el camino 480 indicado con una línea discontinua que atraviesa los routers 410, 420, 430, 440 y 450 de la figura hasta llegar al host 460.

Los mensajes PIM-SM siguen el mismo camino 480, pero en sentido contrario de los datos que van desde la fuente 400 al host 460 que recibe dicho tráfico, y se transmiten desde el router 450 hacia el router 410 pasando por los routers intermedios 440, 430 y 420. En el caso del canal multicast (S,G) emitido por la fuente 400 de la figura 4, los mensajes PIM-SM pueden ser mensajes de tipo JOIN(S,G) para solicitar recibir el tráfico de la fuente 400 o mensajes de tipo PRUNE (S,G) para solicitar dejar de recibir el tráfico de la fuente 400.

Suponiendo que inicialmente el host 460 está recibiendo el canal multicast (S,G) transmitido por la fuente 400, a continuación se analizara el proceso que tiene lugar cuando el host 460 envía un mensaje IGMPv3 o MLDv2 al router 450 para indicar que desea dejar de recibir el tráfico de dicho canal (S,G). Cuando esto sucede, el router 450 envía un mensaje PRUNE(S,G) al router 440 para indicarle que ya no desea recibir el canal (S,G). Dicho mensaje PRUNE(S,G) se transmite por la interfaz de red 451 del router 450 por medio de la red multiacceso 445 y es recibido por la interfaz de red 442 del router 440.

En el estado de la técnica anterior, el router 440 espera 3 segundos para ver si hay algún router que todavía esté interesado en recibir el (S,G), en cuyo caso dicho router interesado deberá enviar inmediatamente al router 440 un mensaje JOIN (S,G) antes de que transcurran los tres segundos, para que así el router 440 continúe transmitiendo el tráfico

(S,G). Si transcurren los tres segundos sin que ningún router conectado a la red 445 envíe un mensaje JOIN(S,G), el router 440 dejará de transmitir el canal multicast (S,G) por su interfaz de red 442 y transmitirá otro mensaje PRUNE (S,G) hacia el router 430 por medio de la red multiacceso 435. El mismo proceso se repite en los siguientes routers 430 y 420, que envían sucesivos mensajes PRUNE (S,G). En cada router se añaden tres segundos de espera para comprobar si en cada red multiacceso 435, 425 hay algún otro router interesado en recibir el canal (S,G). El resultado final es que, en el estado de la técnica anterior, desde que el router 450 envía el primer mensaje PRUNE(S,G) hasta que el router 410 deja de transmitir el canal (S,G), hay un retardo total de 12 segundos (3 segundos sucesivamente en cada uno de los routers) durante los cuales el router 410 ha continuado transmitiendo el tráfico del canal (S,G) de forma innecesaria.

La solución adoptada por la presente invención para eliminar completamente este problema de latencia consiste en que el router PIM-SM que recibe por una interfaz de red un mensaje PIM-SM de otro router solicitando tráfico multicast, identifica y almacena la dirección IP del router de origen de dicho mensaje PIM-SM. La dirección IP de origen de los mensajes PIM-SM se obtiene del campo “Source Address” de los paquetes IP que transportan dichos mensajes PIM-SM. De esta forma, el router de la presente invención conoce con exactitud, para cada una de sus interfaces de red, qué equipos están interesados en recibir cada tipo de tráfico multicast en cada momento. Al llevar un control individual del tráfico solicitado por cada router, cuando el router PIM-SM según la invención recibe un mensaje de tipo PRUNE para dejar de transmitir un determinado trafico multicast, dicho router ya no necesita esperar un tiempo para ver si otro router envía un mensaje de tipo “JOIN” referido al mismo tráfico multicast, pues conoce con exactitud el tráfico multicast solicitado por cada router. Si el router sabe que no hay ningún otro router que desea recibir dicho tráfico multicast, puede cancelar de inmediato la transmisión del mismo, con lo cual se elimina completamente la latencia.

Un router mejorado según la invención realiza una función que las especificaciones RFC 4601, al final de su apartado 4.5.7, afirman que es imposible, esto es, hacer un seguimiento individual de las peticiones de tráfico multicast de los routers “downstream” sin eliminar primero la supresión de mensajes en todos los routers de la red multiacceso. De esta forma la presente invención cambia la importancia que tiene la supresión de mensajes en el control individual de las peticiones de tráfico de los routers “downstream”: pasa de ser

algo imprescindible para un experto en la materia, que sigue las especificaciones RFC 4601 debido a la complejidad del protocolo PIM-SM, a ser algo relativamente poco importante para un experto en la materia que aplica la presente invención.

De acuerdo con lo que establecen las RFC 4601, si se realiza una supresión de mensajes un router PIM-SM no puede hacer un seguimiento individual del tráfico multicast que le ha solicitado cada router "dowsntream". Siguiendo esta idea establecida, un experto en la materia pensará que si se realiza una supresión de mensajes, un router PIM-SM según la invención no podrá mantener actualizada la información del tráfico multicast que le ha solicitado cada router "downstream".

El router PIM-SM mejorado según la invención, que almacena la dirección IP de todos los equipos que le solicitan tráfico multicast y lleva un seguimiento exacto del tráfico multicast que le ha solicitado cada equipo, tiene que solucionar el problema que supone la supresión de mensajes para mantener actualizada dicha información. La presente invención soluciona este problema gracias a que explota unas características del protocolo PIM-SM que no se explican en las especificaciones RFC 4601 pero que el solicitante ha deducido a partir de una observación detallada de la máquina de estados "upstream" (S,G) que figura en el apartado 4.5.7 de dichas especificaciones. A continuación se explica brevemente en qué consisten estas características.

Un router PIM-SM tiene una máquina de estados "upstream" (S,G) independiente para cada interfaz de red del router y para cada canal multicast (S,G). Esta máquina de estados "upstream" (S,G) tiene sólo dos estados: un estado Not_Joined (NJ) que significa que el router no necesita recibir el canal multicast (S,G) por dicha interfaz de red, y un estado Joined (J) que significa que el router necesita recibir el canal multicast (S,G) por dicha interfaz de red. No se considera necesario explicar en detalle el funcionamiento de la máquina de estados "upstream" (S,G) que se utiliza para enviar mensajes Join(S;G) en el protocolo PIM-SM, pues ya está explicado en el mencionado apartado 4.5.7 de las RFC 4601. Las características del protocolo PIM-SM que el solicitante ha deducido a partir de un análisis detallado de dicha máquina de estados "upstream" (S,G), y que son explotadas por la presente invención, son las siguientes:

- Al pasar de un estado “Not Joined” (NJ) a un estado “Joined” (J), un router PIM-SM siempre envía un mensaje JOIN(S,G).

- Al pasar de un estado “Joined” (J) a un estado “Not Joined” (NJ) un router PIM-SM siempre envía un mensaje PRUNE (S,G).

Como consecuencia de estas dos características resulta la característica siguiente:

- A cada mensaje inicial de tipo JOIN que envía un determinado router PIM-SM para solicitar un determinado tráfico multicast, le corresponde siempre un mensaje final de tipo PRUNE procedente del mismo router cuando éste quiere dejar de recibir dicho tráfico multicast.

Por lo tanto, un router que ejecuta el protocolo PIM-SM siempre envía un mensaje inicial JOIN (S,G) cuando el router desea empezar a recibir el tráfico del canal multicast (S,G) y siempre envía un mensaje final PRUNE (S,G) cuando dicho router desea dejar de recibir dicho canal multicast. Los mensajes de tipo JOIN (S,G) que puede suprimir el router PIM-SM son únicamente los mensajes de tipo JOIN (S,G) periódicos que se vuelven a enviar cuando expira el timer denominado "Join_Timer", pero nunca se suprime el mensaje inicial JOIN (S,G).

Además, esto es así independientemente de que esté activada o no la supresión de mensajes. Gracias a estas características de la máquina de estados “upstream” de PIM-SM, el router según la presente invención puede hacer el seguimiento exacto del tráfico multicast que quiere cada router PIM-SM tanto si está activada la supresión de mensajes como si no, y no hace falta que todos los routers se pongan de acuerdo en eliminar la supresión de mensajes tal como requieren las RFC 4601.

El router según la invención explota estas características de la manera siguiente: realiza el seguimiento individual del tráfico multicast que solicita cada router “downstream”, por ejemplo el tráfico (S,G), usando el mensaje inicial JOIN(S,G) que recibe de cada router y el mensaje final PRUNE(S,G) que recibe de cada router. Gracias a ello, un router según la invención que aplica el protocolo PIM-SM es capaz de realizar dicho seguimiento individual

del tráfico multicast aunque se supriman los mensajes JOIN(S,G) periódicos que los otros routers envían entre un mensaje inicial JOIN (S,G) y un mensaje final PRUNE (S,G).

Por lo tanto, un router según la invención que aplica el protocolo PIM-SM puede hacer un seguimiento del tráfico multicast solicitado por cada router "downstream" tanto si está activada la supresión de mensajes como si no, contrariamente a lo que establecen las RFC 4601. Además, asimismo contrariamente a lo que establecen las RFC 4601, para ello no hace falta que todos los routers se pongan de acuerdo en cancelar la supresión de mensajes.

En resumen, un router según la invención es apto para funcionar en una red de comunicaciones según el protocolo PIM-SM en la cual los otros routers pueden ser tanto routers según la invención como routers según el estado de la técnica anterior, y dicho router según la invención puede realizar un seguimiento individualizado del tráfico multicast solicitado por los otros routers independientemente de si los routers según el estado de la técnica anterior han cancelado o no la supresión de mensajes.

En el estado de la técnica anterior, los routers que aplican el protocolo PIM-SM envían los mensajes JOIN (S,G) periódicos para evitar que, si se pierde un mensaje final PRUNE (S,G), el router "usptream" que no ha recibido dicho mensaje PRUNE (S,G) perdido continúe transmitiendo el canal (S,G) de forma indefinida hacia una red aunque no haya ningún router interesado en recibir dicho canal. El router "upstream" actualiza un timer denominado "Expiry_Timer" cada vez que recibe un mensaje JOIN (S,G), ya sea el inicial o uno de los periódicos. Cuando el timer "Expiry_Timer" llega a cero, el router deja de transmitir el canal (S, G).

En el router de la presente invención que realiza un seguimiento individual del tráfico multicast que solicita cada router, por ejemplo el tráfico (S,G), usando el primer mensaje JOIN (S,G) que recibe de cada router y el mensaje PRUNE (S,G) que recibe de cada router, también es conveniente utilizar un timer que evite que un determinado tráfico multicast se siga transmitiendo de forma indefinida si se pierde un paquete IP que transporta un mensaje PRUNE. El funcionamiento en detalle de este timer que implementa la presente invención se explica más adelante.

Aunque las explicaciones que preceden se refieren al tipo de tráfico multicast (S,G) y a los mensajes PIM-SM correspondientes, de tipo JOIN/PRUNE (S,G), lo explicado es aplicable a los otros tres tipos de tráfico multicast y a sus mensajes PIM-SM correspondientes que, como es conocido por el experto en la materia, son los siguientes:

- Tráfico (*,*,RP) ; mensajes de tipo JOIN / PRUNE (*,*,RP)
- Tráfico (*,G) ; mensajes JOIN / PRUNE (*,G)
- Tráfico (S,G,rpt) ; mensajes JOIN / PRUNE (S,G,rpt)

En la Tabla 6 se muestra el funcionamiento de la máquina de estados “downstream” (S,G) de un router según la invención, es decir la máquina de estados que gestiona el control del estado del tráfico multicast (S,G) en función de los mensajes JOIN / PRUNE (S,G) recibidos por cada interfaz de red de dicho router. El experto en la materia comprenderá sin dificultad que los conceptos que se explican a continuación para la máquina de estados (S,G) y los mensajes de tipo JOIN / PRUNE (S,G) también son aplicables a los otros tres tipos de tráfico multicast y a sus mensajes PIM-SM correspondientes.

La máquina de estados de la Tabla 6 almacena la información de estado de cada tipo de tráfico multicast solicitado en unos registros que tienen la forma siguiente:

REGISTRO (Interface, Trafic_Type=(S,G) , Expiry_Timer, {(IP_Router, IP_Timer)})

donde:

- Interface es la interfaz de red del router en la que se reciben los mensajes PIM-SM.

- Trafic_Type es un parámetro que indica el tipo de tráfico multicast. La máquina de estados de la Tabla 6 se refiere al tipo de tráfico (S,G), donde S es la dirección IP de origen de la fuente y G la dirección IP del grupo multicast. Por eso se ha indicado Trafic_Type = (S,G). Sin embargo, podría ser igualmente cualquier otro entre los cuatro tipos de tráfico multicast mencionados anteriormente.

- Expiry_Timer o ET es un timer que se reinicia cada vez que llega a la interfaz de red indicada en el campo Interface un mensaje de tipo JOIN referido al tipo de tráfico

indicado en el campo Trafic_Type. Si el timer Expiry_Timer llega a cero, el router deja de transmitir el tráfico indicado en el campo Trafic_Type (en este caso el tráfico (S, G)) por la interfaz de red indicada en el campo Interface.

- {(IP_Router, IP_Timer)} es una lista de elementos (IP_Router, IP_Timer), siendo "IP_Router" la dirección IP del router que ha enviado el mensaje PIM-SM y siendo IP_Timer un timer asociado a cada IP_Router que se reinicia cada vez que la interfaz de red indicada en el campo Interface recibe un mensaje de tipo JOIN proveniente del router cuya IP es IP_Router. El valor que se utiliza para reiniciar el timer IP_Timer es el valor del parámetro "Holdtime" contenido en el mensaje JOIN(S,G). El parámetro "holdtime" es un parámetro que se transmite en los mensajes JOIN(S,G) del protocolo PIM-SM, de forma conocida por un experto en la materia, y que indica el tiempo que el router que envía el mensaje Join(S,G) desea estar recibiendo el canal (S,G). La dirección IP del router que ha enviado el mensaje PIM-SM se extrae de la dirección de origen del datagrama IP que encapsula dicho mensaje PIM-SM.

En la máquina de estados de la Tabla 6, que como se ha dicho se refiere a una determinada interfaz de red del router y un determinado tipo de tráfico multicast (en este caso el tráfico de tipo (S,G)), la primera columna contiene un estado inicial del router, la segunda columna contiene un mensaje o evento, la tercera columna contiene el estado final del router como resultado de dicho mensaje o evento de la segunda columna y la cuarta columna contiene las acciones que realiza el router en cada caso.

Los estados en los que puede estar una interfaz de red "downstream" del router para un determinado canal multicast (S, G) son los dos siguientes:

- NI ("No_Info"). Este estado indica que la interfaz de red del router no tiene ninguna información que indique al router que debe transmitir el canal (S,G) por dicha interfaz de red. Por lo tanto, en el estado NI el router no transmite el canal (S,G).

- JOIN ({IP}), donde {IP} es una lista de direcciones IP de routers PIM-SM que han enviado al router mensajes de tipo JOIN(S,G). En este estado, el router está

transmitiendo el canal (S,G) por dicha interfaz de red, porque hay un una serie de routers que lo han solicitado (los routers de la lista {IP}).

La Tabla 6 describe ocho procesos, numerados del 1 al 8 y separados entre sí por líneas discontinuas. Estos ocho procesos constituyen la máquina de estados "Downstream" (S,G) del router de la presente invención.

El proceso 1 se ejecuta cuando el router está en estado NI y recibe un mensaje JOIN(S,G) de un router cuya IP es IP1. El router cambia al estado JOIN (IP1) e inicializa el timer T(IP1) asociado la dirección IP1 y el timer Expiry_Timer o ET con el valor del parámetro "Holdtime" contenido en el mensaje JOIN(S,G) recibido. El router empieza a transmitir el canal multicast (S,G) por la interfaz de red por la cual ha recibido dicho mensaje JOIN(S,G).

El parámetro "Holdtime" de los mensajes PIM-SM, está descrito en el apartado "4.9.5 Join/Prune Message Format", de las RFC 4601, e indica el tiempo en segundos durante el cual el router que recibe el mensaje debe mantener el estado "Joined" o "Pruned".

En el proceso 2, el router ya está transmitiendo el canal (S,G) y recibe un nuevo mensaje JOIN(S,G) de un router cuya IP, indicada como IP2, no está en su lista de direcciones IP del registro asociado al canal (S,G). En este caso, el router añade la dirección IP2 a su lista e inicia el valor del timer T(IP2) con el valor del parámetro "Holdtime" del mensaje recibido. Si el valor del timer ET es mayor que el parámetro "Holdtime" contenido en el mensaje JOIN(S,G) recibido, el timer ET no se modifica. En caso contrario, es decir cuando el timer ET tiene un valor menor que "Holdtime", se pone este valor "Holdtime" en el timer ET. Este funcionamiento se ha indicado en la tabla 6 mediante la expresión "ET -> HT". En este segundo proceso, el router continúa transmitiendo el canal (S,G).

En el proceso 3 el router recibe un mensaje JOIN(S,G) de un router cuya IP, que en este caso es IP1, ya está en su lista. En este caso simplemente actualiza los timers T(IP1) y ET tal como se ha explicado en el proceso 2, y continúa trasmitiendo el canal (S,G)

En el proceso 4, el router recibe un mensaje PRUNE(S,G) de un router cuya dirección IP, que en este caso es IP2, está en su lista, pero IP2 no es el único elemento de su lista. El router elimina IP2 de su lista y continúa transmitiendo el canal (S,G).

En el proceso 5, el router recibe un mensaje PRUNE(S,G) de un router cuya dirección IP, que en este caso es IP1, es la última dirección que queda en el registro asociado al canal (S,G). En este caso el router elimina la dirección IP1 de la lista, deja de transmitir el canal (S,G) y cambia al estado NI.

En el proceso 6, el timer T(IP1) asociado a IP1, que es el único elemento que hay en la lista IP, llega al valor cero. En este caso, el router elimina IP1 de la lista, deja de transmitir el canal (S,G) y cambia al estado NI.

En el proceso 7, el timer T(IP2) asociado a una IP2, que no es el único elemento de la lista, llega al valor cero. En este caso, el router debe tener en cuenta si el router que envía los mensajes PIM-SM desde la dirección IP2 es un router que ha cancelado la supresión de mensajes o no. En el primer caso, el router elimina la dirección IP2 de la lista y en el segundo caso mantiene la dirección IP2 aunque el timer T(IP2) sea cero. Más adelante se describe cómo un router que implementa la presente invención sabe si los otros routers han cancelado la supresión de mensajes.

El proceso 8 muestra lo que sucede cuando el timer ET llega a cero. En este caso, el router elimina todas las IP de la lista, cambia al estado NI y deja de transmitir el canal (S,G).

Los routers que implementan la presente invención pueden configurarse para cancelar siempre la supresión de mensajes periódicos, aunque existan routers en la red que no hayan anunciado su capacidad de cancelar la supresión de mensajes.

Además, los routers que implementan la presente invención disponen de un mecanismo para saber si los otros routers de una red implementan la presente invención o no. Esto es conveniente por dos motivos.

En primer lugar, un router “downstream” que implementa la presente invención necesita saber si un router “upstream“ al cual envía mensajes PIM-SM implementa o no la presente invención. Por ejemplo, si un router R1 que implementa la presenta invención envía mensajes JOIN a un router R2, el router R1 necesita saber si el router R2 implementa la presente invención pues si el router R2 es del estado de la técnica anterior y otro router R3

envía un mensaje PRUNE al router R2 referido a un tráfico multicast que el router R1 desea seguir recibiendo, el router R1 debe enviar inmediatamente un mensaje JOIN para anular el efecto del mensaje PRUNE del router R3. En cambio, si el router R2 implementa la presente invención, el router R1 no tiene que preocuparse de los mensajes que envíen los demás routers, ya que el router R2 hace un seguimiento individual de las peticiones de cada router.

En segundo lugar, un router "upstream" que implementa la presente invención necesita saber si un router "downstream" que le envía mensajes PIM-SM implementa o no la presente invención y si el router "downstream" ha cancelado la supresión de mensajes aunque no todos los routers se hayan puesto de acuerdo para cancelar la supresión de mensajes.

En el mecanismo por defecto del estado de la técnica anterior, tal como se describe en las RFC 4601, los routers no anuncian si han cancelado o no la supresión de mensajes, lo que anuncian es si tienen la capacidad de anular la supresión de mensajes. Sólo cuando todos los routers de una red han anunciado que tienen la capacidad de anular la supresión de mensajes proceden todos los routers de forma común a cancelar la supresión de mensajes.

En el proceso 7 de la Tabla 6, el router "upstream" sabe que el router "downstream" ha cancelado la supresión de mensajes si se da cualquiera de las dos circunstancias siguientes:

a) el router "downstream" ha comunicado que es un router que implementa la presente invención y si cancela o no los mensajes periódicos.

b) todos los routers de la red han anunciado su capacidad de cancelar la supresión de mensajes.

Para comunicar que implementan la presente invención y si suprimen o no los mensajes periódicos, los routers de la presente invención pueden anunciarlo en sus mensajes "Hello" que envían de forma periódica por todas sus interfaces de red donde ejecutan el protocolo PIM-SM.

Una primera forma de anunciarlo consiste en definir un nuevo bloque de datos de los denominados “Option” con un nuevo valor de OptionType en el mensaje “Hello”. Los diferentes valores del parámetro OptionType de los mensajes “Hello” se explican en el apartado 4.9.2 de las RFC 4601 y actualmente varían de 1 a 20. Se puede utilizar un valor fuera de este rango, por ejemplo OptionType = 30, para anunciar que un router implementa la presente invención y utilizar uno de los campos o parámetros del nuevo mensaje para indicar si el router ha cancelado la supresión de mensajes periódicos.

Una segunda forma de anunciarlo consiste en utilizar el bloque de datos “LAN_PRUNE_Delay” y poner un valor especial en el parámetro Override_Interval, por ejemplo los valores 0 y 1 que tienen poco sentido como valor de espera en milisegundos. De esta forma, por ejemplo, cuando los routers de la presente invención reciben un mensaje “Hello” cuyo valor Override_Interval es 0 saben que lo envía un router que implementa la presente invención y que ha cancelado la supresión de mensajes. Si reciben el valor 1 interpretan que el router que ha enviado el mensaje implementa la presente invención pero no ha cancelado la supresión de mensajes.

Volviendo al ejemplo de la Fig.4, supongamos que los routers 410, 420, 430, 440 y 450 son routers que implementan la presente invención. Cuando el host 460 envía un mensaje IGMPv3 o MLDv2 al router 450 para indicar que desea dejar de recibir el tráfico del canal (S,G), el router 450 envía un mensaje PRUNE(S,G) al router 440. Según la invención, el router 440 mantiene un registro del tráfico (S,G) solicitado en su interfaz de red 442 por cada uno de los routers de la línea de red multiacceso 445 que han solicitado tráfico enviando mensajes PIM-SM a dicho router 440. Gracias a ello, el router 440 sabe si hay algún router que todavía desea recibir el canal (S;G). Si no es el caso, cuando el router 440 recibe el mensaje PRUNE (S,G) enviado por el router 450, realiza inmediatamente las acciones siguientes: deja de transmitir tráfico multicast por su interfaz de red “downstream” 442 y envía al router 430 un mensaje PRUNE (S,G). El mismo proceso se produce sucesivamente en los routers 430, y 420: cuando cada uno de ellos recibe el mensaje PRUNE (S,G) del router “downstream”, si su registro para el tráfico (S,G) solicitado en su interfaz de red “downstream”, respectivamente 432 y 422, indica que no queda ningún router interesado en recibir el canal (S,G), de forma inmediata dicho router 430, 420 deja de enviar tráfico por su dicha interfaz de red “downstream” y envía un mensaje PRUNE (S,G) al router “upstream” siguiente. Cuando el router 410 recibe el mensaje PRUNE (S,G)

del router 420, realiza el mismo proceso que los routers 440, 430 y 420, con la diferencia de que no envía un mensaje PRUNE (S,G), ya que está conectado directamente a la fuente 400. Por lo tanto, a partir del momento en que el router 450 envía el primer mensaje PRUNE(S,G), si en las líneas de red multiacceso 445, 435, 425 y 415 no queda ningún otro router interesado en recibir el canal (S,G), el router 410 deja de transmitir el canal (S,G) de forma prácticamente inmediata. En efecto, el único retraso que se produce, además del inherente a la transmisión de los mensajes PRUNE a través de la red, que se realiza en un tiempo muy corto y de todas formas es inevitable, es el que corresponde al tiempo necesario para que cada router actualice y compruebe sus registros del tráfico multicast solicitado, según la invención. Pero éstas son operaciones que un router puede realizar en tiempos extremadamente cortos, como bien sabe un experto en la materia.

El seguimiento individual de las peticiones de cada router PIM-SM que se realiza gracias al router según la invención, además de las ventajas ya explicadas, tiene otras aplicaciones importantes. Por ejemplo, permite contabilizar o autorizar el tráfico multicast, lo que generalmente se denomina AAA (“Authentication, Autorization and Acounting”). Esto puede realizarse ventajosamente, por ejemplo, asociando información relativa a la AAA a cada elemento (IP_Router, IP_Timer) de la lista {(IP_Router, IP_Timer)} del registro de tráfico multicast de cada router. De esta forma, un router mejorado según la invención puede aplicar unas condiciones específicas relativas a la contabilización y/o a la autorización de transmisión de un tipo de tráfico multicast a un router determinado, identificado por la dirección IP_Router y para el cual dicho router mejorado tiene almacenada una información relativa a la AAA.

	ESTADO 1	MENSAJE	ESTADO 2	ACCIONES
1.	INCLUDE (A)	IS_IN (B)	INCLUDE (A+B)	T(B)=GMI
2.	INCLUDE (A)	IS_EX (B)	EXCLUDE (A*B,B-A)	T(B-A)=0 DEL(A-B) GT=GMI
3.	EXCLUDE (X,Y)	IS_IN (A)	EXCLUDE (X+A,Y-A)	T(A)=GMI
4.	EXCLUDE (X,Y)	IS_EX (A)	EXCLUDE (A-Y,Y*A)	T(A-X-Y)=GMI DEL (X-A) DEL (Y-A) GT=GMI
5.	INCLUDE (A)	ALLOW (B)	INCLUDE (A+B)	T(B)=GMI
6.	INCLUDE (A)	BLOCK (B)	INCLUDE (A)	SEND Q(G,A*B
7.	INCLUDE (A)	TO_EX (B)	EXCLUDE (A*B,B-A)	T(B-A)=0 DEL (A-B) SEND Q(G,A*B GT=GMI
8.	INCLUDE (A)	TO_IN (B)	INCLUDE (A+B)	T(B)=GMI SEND Q(G,A-B
9.	EXCLUDE (X,Y)	ALLOW (A)	EXCLUDE (X+A,Y-A)	T(A)=GMI
10.	EXCLUDE (X,Y)	BLOCK (A)	EXCLUDE (X+(A-Y),Y)	T(A-X-Y)=GT SEND Q(G,A-Y
11.	EXCLUDE (X,Y)	TO_EX (A)	EXCLUDE (A-Y,Y*A)	T(A-X-Y)=GT DEL (X-A) DEL (Y-A) SEND Q(G,A-Y GT=GMI
12.	EXCLUDE (X,Y)	TO_IN (A)	EXCLUDE (X+A,Y-A)	T(A)=GMI SEND Q(G,X-A SEND Q(G)

Tabla 2 (ESTADO DE LA TÉCNICA): ejemplo de funcionamiento de un router IGMP del estado de la técnica que aplica el protocolo IGMPv3.

MENSAJE ENVIADO POR EL HOST	FUENTES CUYO TRÁFICO TRANSMITE EL ROUTER	ACCIONES QUE REALIZA EL ROUTER
INCLUDE(S1)	S1	T(S1)=GMI
ALLOW(S2)	S1, S2	T(S1)=GMI
BLOCK(S1)	S1, S2	T(S1)=LMQT ; SEND Q(G, S1)
ALLOW(S3)	S1, S2, S3	T(S3)=GMI
BLOCK(S2)	S1, S2, S3	T(S2)=LMQT ; SEND Q(G, S2)

Tabla 3 (ESTADO DE LA TÉCNICA): ejemplo de funcionamiento de un router IGMP del estado de la técnica que aplica el protocolo IGMPv3, cuando un host cambia de canal sucesivamente.

	ESTADO 1	MENSAJE	ESTADO 2	ACCIONES
1.	INCLUDE (A)	IS_IN (B)	INCLUDE (B)	T(B)=GMI DEL(A-B)
2.	INCLUDE (A)	IS_EX (B)	EXCLUDE ({},B)	T(B)=0 DEL(A-B) GT=GMI
3.	EXCLUDE (X,Y)	IS_IN (A)	INCLUDE (A)	T(A)=GMI DEL(X+Y)-A
4.	EXCLUDE (X,Y)	IS_EX (A)	EXCLUDE ({},A)	T(A)=0 DEL(X+Y)-A GT=GMI
5.	INCLUDE (A)	ALLOW (B)	INCLUDE (A+B)	T(B)=GMI
6.	INCLUDE (A)	BLOCK (B)	INCLUDE (A-B)	DEL(B)
7.	INCLUDE (A)	TO_EX (B)	EXCLUDE ({},B)	T(B)=0 DEL (A-B) GT=GMI
8.	INCLUDE (A)	TO_IN (B)	INCLUDE (B)	T(B)=GMI DEL(A-B)
9.	EXCLUDE (X,Y)	ALLOW (A)	EXCLUDE (X+A,Y-A)	T(A)=GMI
10.	EXCLUDE (X,Y)	BLOCK (A)	EXCLUDE (X-A,Y+A)	T(A)=0
11.	EXCLUDE (X,Y)	TO_EX (A)	EXCLUDE ({},A)	T(A)=0 DEL (X+Y)-A GT=GMI
12.	EXCLUDE (X,Y)	TO_IN (A)	INCLUDE (A)	T(A)=GMI DEL (X+Y)-A

Tabla 4 : ejemplo de funcionamiento de un router IGMP mejorado según una primera forma de realización de la invención.

	ESTADO 1	MENSAJE	ESTADO 2	ACCIONES
1.	INCLUDE (A) EXCLUDE (Y)	IS_IN (B)	INCLUDE (B) EXCLUDE (Y)	T(B)=GMI DEL(A-B)
2.	INCLUDE (A) EXCLUDE (Y)	IS_EX (B)	INCLUDE (A) EXCLUDE (B)	DEL(Y-B) GT = GMI
3.	INCLUDE (A) EXCLUDE (Y)	ALLOWIN (B)	INCLUDE (A+B) EXCLUDE (Y)	T(B)=GMI
4.	INCLUDE (A) EXCLUDE (Y)	BLOCKIN (B)	INCLUDE (A-B) EXCLUDE (Y)	DEL(B)
5.	INCLUDE (A) EXCLUDE (Y)	ALLOWEX (B)	INCLUDE (A) EXCLUDE (Y-B)	DEL(B)
6.	INCLUDE (A) EXCLUDE (Y)	BLOCKEX (B)	INCLUDE (A) EXCLUDE (Y+B)	

Tabla 5: ejemplo de funcionamiento de un router IGMP mejorado según una segunda forma de realización de la invención.

	ESTADO 1	MENSAJE / EVENTO	ESTADO 2	ACCIONES
1.	NI	JOIN(S,G) FROM(IP1)	JOIN(IP1)	T(IP1) = HT ET = HT
2.	J(IP1)	JOIN(S,G) FROM(IP2)	JOIN(IP1,IP2)	T(IP2) = HT ET -> HT
3.	J(IP1)	JOIN(S,G) FROM(IP1)	JOIN(IP1)	T(IP1) = HT ET -> HT
4.	J(IP1,IP2)	PRUNE(S,G) FROM(IP2)	JOIN(IP1)	DEL (IP2)
5.	J(IP1)	PRUNE(S,G) FROM (IP1)	NI	DEL (IP1)
6.	J(IP1)	T(IP1) = 0	NI	DEL (IP1)
7.	J(IP1,IP2)	T(IP2) = 0	JOIN(IP) JOIN(IP1,IP2)	IF [NSP(IP2)] DEL (IP2)
8.	J(...)	ET = 0	NI	DEL ALL IP

Tabla 6 : Máquina de estados “dowstream” (S,G) de un router PIM-SM según la invención

El significado de las abreviaciones en la Tabla 6 es el siguiente:

NI	:	estado “No_Info”
J	:	estado “JOIN” referido a las direcciones IP indicadas
T	:	timer asociado a la dirección IP indicada
ET	:	timer “Expiry_Timer”
HT	:	valor del parámetro “Holdtime” en el mensaje JOIN recibido
FROM	:	mensaje enviado desde la dirección IP indicada
DEL	:	borrar del registro la dirección IP indicada
DELL ALL IP	:	borrar del registro todas las direcciones IP
NSP	:	el router de la dirección IP indicada no suprime mensajes
IF	:	la acción se realiza si se cumple la condición indicada

REIVINDICACIONES

1. Procedimiento para monitorizar o gestionar equipos (110, 120, 130) conectados a una red de datos (150) caracterizado porque:

- dicha red de datos (150) dispone de una estación de control (100) que monitoriza o gestiona dichos equipos (110, 120,130), y;
- cada uno de dichos equipos puede estar en uno o en varios estados diferentes, y;
- dichos equipos (110,120,130) envían mensajes en un protocolo de ruteo multicast para solicitar recibir tráfico multicast, y;
- dicho tráfico multicast solicitado consiste en grupos multicast y canales multicast que se corresponden con los estados de cada equipo, y;
- dicha estación de control (100) conoce el estado o los estados de cada equipo a partir de los grupos multicast y canales multicast solicitados por cada equipo.

2. Procedimiento según la reivindicación 1 caracterizado porque

- en dicha red de datos hay como mínimo un router multicast (220, 230) conectado a dichos equipos (240, 250, 260, 270, 280), y;
- dichos equipos envían dichos mensajes en un protocolo de ruteo multicast a un dicho router multicast (220, 230), y;
- un router multicast (210, 220, 230) transmite dicha información de grupos multicast y canales multicast solicitados por cada equipo a dicha estación de control (200)

3. Procedimiento según cualquiera de las reivindicaciones 1 y 2 caracterizado porque

- dicha estación de control (100, 200) envía como mínimo a uno de dichos equipos una información para configurar o modificar el estado de dicho equipo.

4. Procedimiento según cualquiera de las reivindicaciones 2 y 3, cuando dicho router multicast es un router IGMP (220, 230) conectado dichos equipos.

5. Procedimiento según cualquiera de las reivindicaciones 2 y 3 cuando dicho router multicast que transmite la información a dicha estación de control es un router PIM-SM (210).

6. Procedimiento según cualquiera de las reivindicaciones 2, 3, 4 y 5 cuando dicho router multicast (310,320,330) que transmite dicha información a dicha estación de control (300) incluye un agente SNMP (316, 326, 336) y dicha información se almacena en una base de datos MIB (317, 327, 337) y se transmite a la estación de control mediante el protocolo SNMP.

7. Procedimiento según cualquiera de las reivindicaciones 2, 3, 4 y 6 cuando dicho router IGMP (220, 230) almacena en unos registros asociados con el protocolo IGMP la información de los grupos y canales multicast solicitados por cada equipo asociando dichos grupos y canales multicast solicitados por cada equipo con un identificador de cada equipo.

8. Procedimiento según la reivindicación 7 cuando dicho router IGMP (320, 330) almacena dicha información de grupos y canales multicast solicitados por cada equipo en una base de datos MIB (327, 337)

9. Procedimiento según la reivindicación 8 cuando dicho router IGMP (320, 330) transmite dicha información almacenada en dicha base de datos MIB (327, 337) a la estación de control (300).

10. Procedimiento según la reivindicación 9 cuando dicho router IGMP (320, 330) transmite dicha información almacenada en dicha base de datos MIB (327, 337) utilizado el protocolo SNMP.

11. Procedimiento según cualquiera de las reivindicaciones 2, 3, 5 y 6 cuando dicho router PIM-SM (210) almacena en unos registros asociados con el protocolo PIM-SM la información de los grupos y canales multicast solicitados por cada router multicast asociando dichos grupos y canales multicast con un identificador de cada router que solicita dichos grupos y canales multicast.

12. Procedimiento según la reivindicación 11 cuando dicho router PIM-SM (310) almacena dicha información de grupos y canales multicast solicitados por cada router multicast en una base de datos MIB (317)

13. Procedimiento según la reivindicaciones 12 cuando dicho router PIM-SM (310) transmite dicha información almacenada en dicha base de datos MIB (317) a la estación de control (300).

14. Procedimiento según la reivindicación 13 cuando dicho router PIM-SM (310) transmite dicha información utilizado el protocolo SNMP.

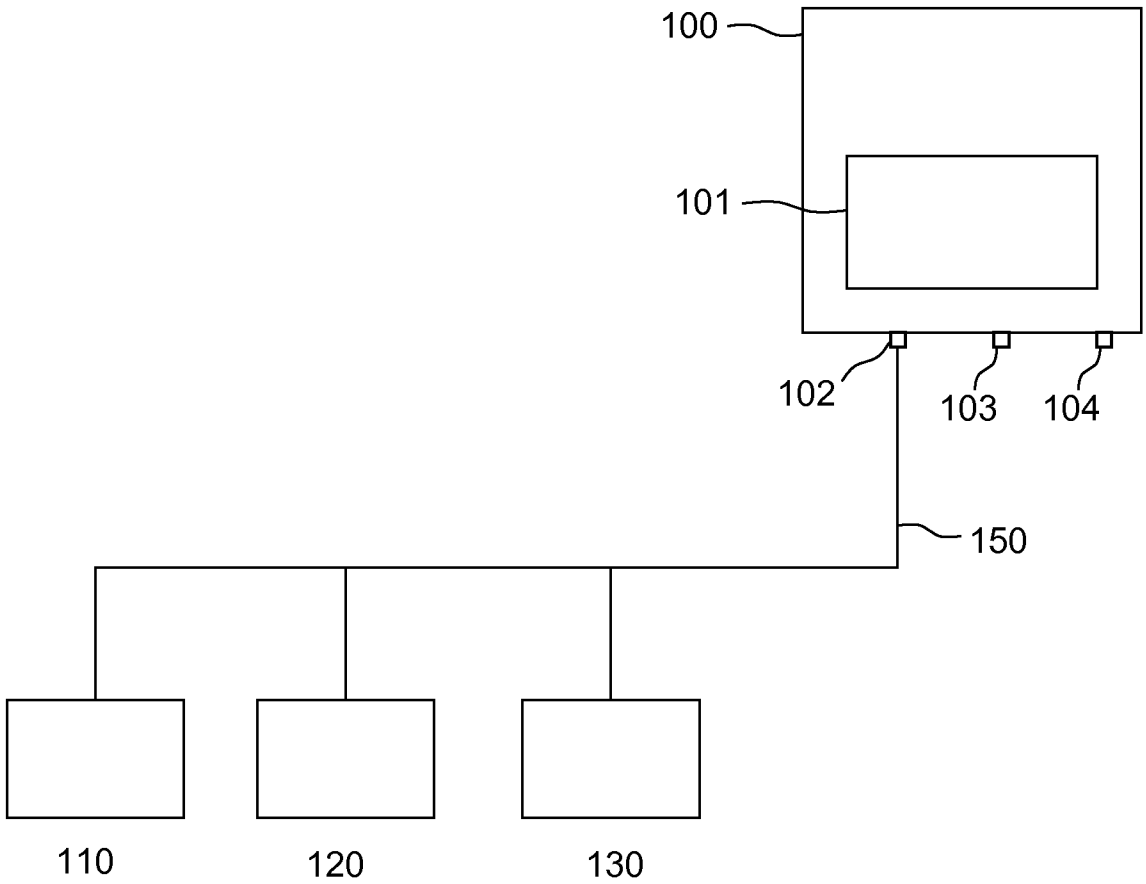


FIG. 1

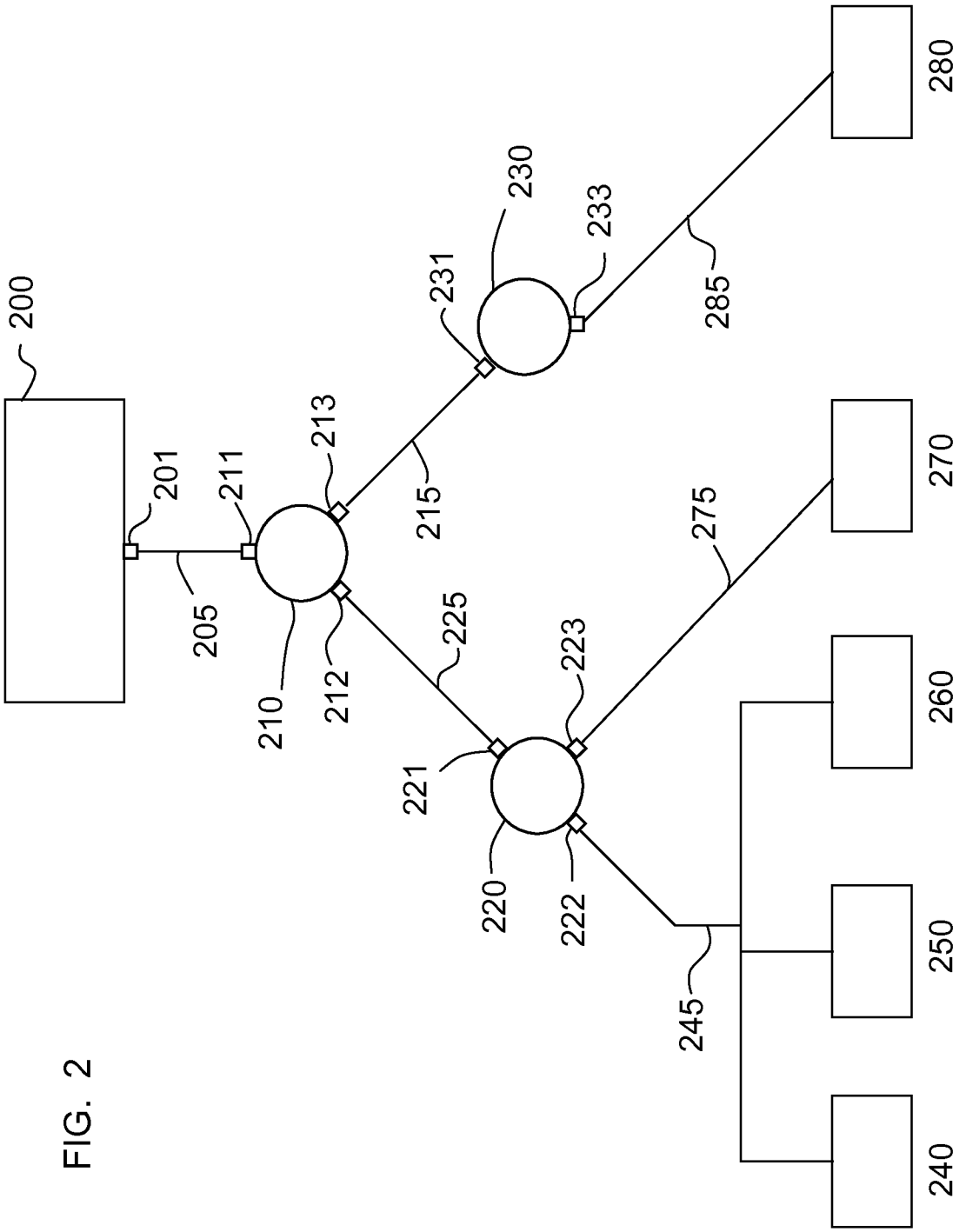

200
201
205
210
211
212
213
215
220
221
222
223
225
230
231
233
240
245
250
260
270
275
280
285

FIG. 2

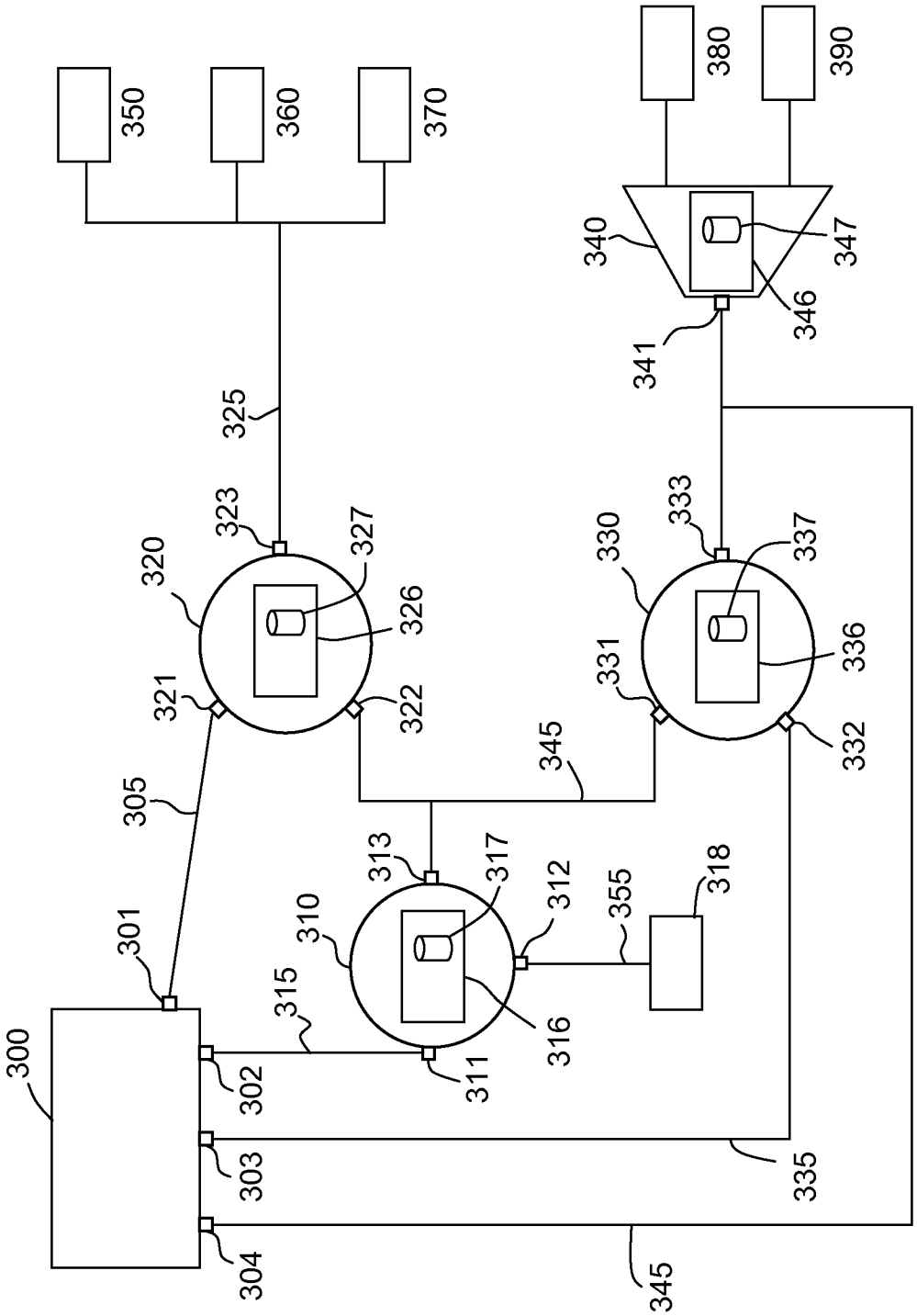

350
360
370
380
390
340
347
346
341
325
323
327
320
326
321
322
330
333
337
331
336
332
345
305
313
317
312
355
318
310
301
315
316
311
300
302
303
304
335
345

FIG. 3

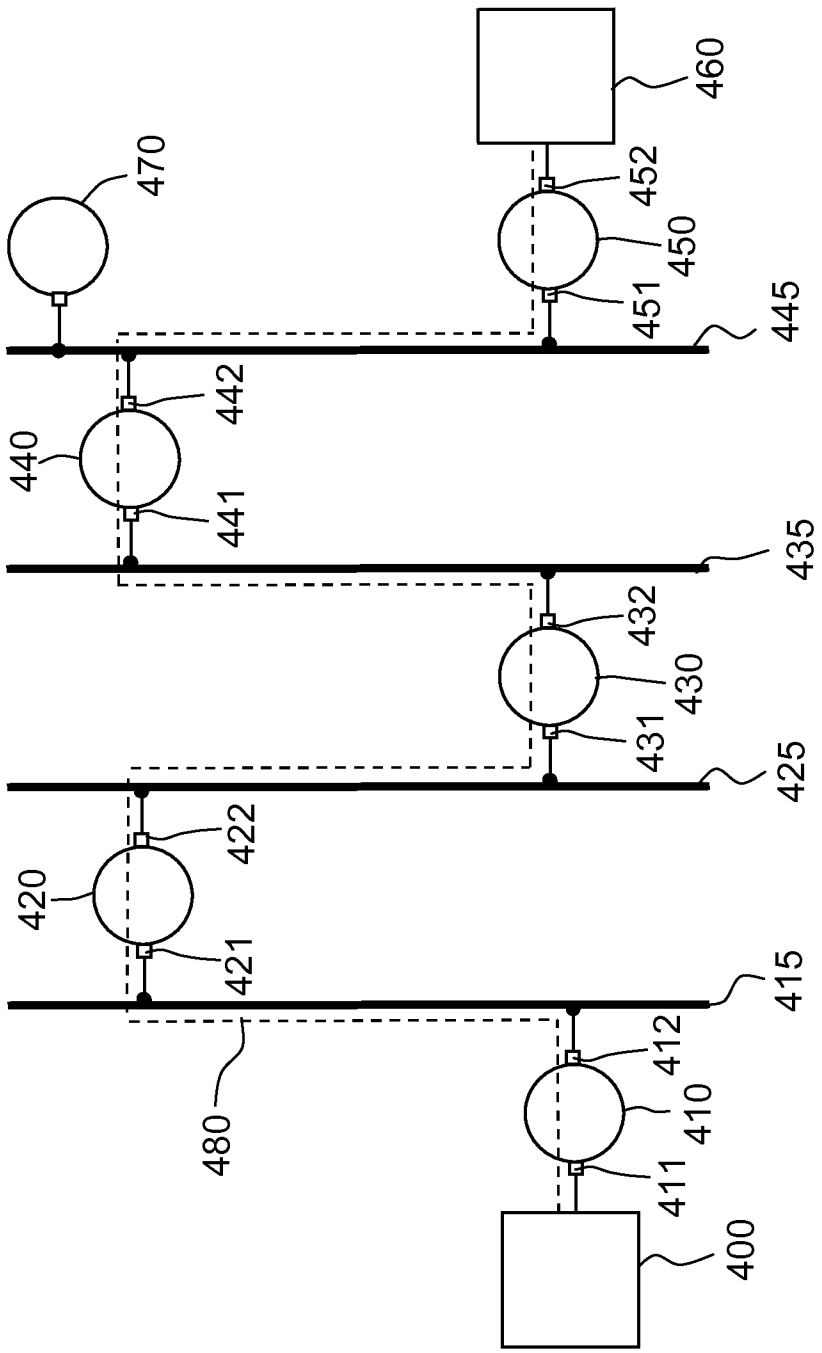

460
452
450
451
445
470
442
440
441
435
432
430
431
425
422
420
421
415
412
410
411
400
480

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/ ES 2009/070047

A. CLASSIFICATION OF SUBJECT MATTER

see extra sheet
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L, G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

INVENES,EPODOC, WPI, Inspec

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2004177124 A1 (HANSEN) 09.09.2004, abstract; paragraphs [0004-0013];	1
A	EP 1370025 B1 (RICOH COMPANY) 10.12.2003, paragraphs [0012-0014];	1
A	US 2004015619 A1 (BROWN et al.) 22.01.2004, abstract; paragraph [0022]; paragraphs [0035-0038];	1
A	US 2006031543 A1 (MOTOYAMA et al.) 09.02.2006, paragraphs [0042-0054];	1

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance.
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure use, exhibition, or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other documents , such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
09.June.2009 (09.06.2009)	**(01/07/2009)**
Name and mailing address of the ISA/ O.E.P.M. Paseo de la Castellana, 75 28071 Madrid, España. Facsimile No. 34 91 3495304	Authorized officer M. Alvarez Moreno Telephone No. +34 91 349 54 95

Form PCT/ISA/210 (second sheet) (July 2008)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/ ES 2009/070047

Patent document cited in the search report	Publication date	Patent family member(s)	Publication date
US 2004177124 A	09.09.2004	WO 0210919 A	07.02.2002
		AU 7803801 A	13.02.2002
		EP 1305712 AB	02.05.2003
		EP 20010955993	27.07.2001
		JP 2004505373 T	19.02.2004
		US 6757714 B	29.06.2004
		US 7117239 B	03.10.2006
		AT 339725 T	15.10.2006
		US 2007011295 A	11.01.2007
		DE 60123076 T	29.03.2007
EP 1370025 AB	10.12.2003	EP 20030011122	22.05.2003
		JP 2004013901 A	15.01.2004
		HK 1059693 A	23.02.2007
		DE 60308755 T	16.08.2007
		US 7506048 B	17.03.2009
US 2004015619 A	22.01.2004	NONE	----------
US 2006031543 A	09.02.2006	JP 2005216307 A	11.08.2005
		US 7296079 B	13.11.2007
		US 2008028091 A	31.01.2008
		US 7447790 B	04.11.2008

INTERNATIONAL SEARCH REPORT

International application No.

PCT/ ES 2009/070047

CLASSIFICATION OF SUBJECT MATTER

H04L 12/24 (2006.01)
H04L 12/26 (2006.01)

INFORME DE BÚSQUEDA INTERNACIONAL

Solicitud internacional Nº

PCT/ ES 2009/070047

A. CLASIFICACIÓN DEL OBJETO DE LA SOLICITUD

Ver hoja adicional

De acuerdo con la Clasificación Internacional de Patentes (CIP) o según la clasificación nacional y CIP.

B. SECTORES COMPRENDIDOS POR LA BÚSQUEDA

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

H04L, G06F

Otra documentación consultada, además de la documentación mínima, en la medida en que tales documentos formen parte de los sectores comprendidos por la búsqueda

Bases de datos electrónicas consultadas durante la búsqueda internacional (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

INVENES,EPODOC, WPI, Inspec

C. DOCUMENTOS CONSIDERADOS RELEVANTES

Categoría*	Documentos citados, con indicación, si procede, de las partes relevantes	Relevante para las reivindicaciones Nº
A	US 2004177124 A1 (HANSEN) 09.09.2004, resumen; párrafos [0004-0013];	1
A	EP 1370025 B1 (RICOH COMPANY) 10.12.2003, párrafos [0012-0014];	1
A	US 2004015619 A1 (BROWN et al.) 22.01.2004, resumen; párrafo [0022]; párrafos [0035-0038];	1
A	US 2006031543 A1 (MOTOYAMA et al.) 09.02.2006, párrafos [0042-0054];	1

☐ En la continuación del Recuadro C se relacionan otros documentos ☒ Los documentos de familias de patentes se indican en el Anexo

* Categorías especiales de documentos citados:

"A" documento que define el estado general de la técnica no considerado como particularmente relevante.

"E" solicitud de patente o patente anterior pero publicada en la fecha de presentación internacional o en fecha posterior.

"L" documento que puede plantear dudas sobre una reivindicación de prioridad o que se cita para determinar la fecha de publicación de otra cita o por una razón especial (como la indicada).

"O" documento que se refiere a una divulgación oral, a una utilización, a una exposición o a cualquier otro medio.

"P" documento publicado antes de la fecha de presentación internacional pero con posterioridad a la fecha de prioridad reivindicada.

"T" documento ulterior publicado con posterioridad a la fecha de presentación internacional o de prioridad que no pertenece al estado de la técnica pertinente pero que se cita por permitir la comprensión del principio o teoría que constituye la base de la invención.

"X" documento particularmente relevante; la invención reivindicada no puede considerarse nueva o que implique una actividad inventiva por referencia al documento aisladamente considerado.

"Y" documento particularmente relevante; la invención reivindicada no puede considerarse que implique una actividad inventiva cuando el documento se asocia a otro u otros documentos de la misma naturaleza, cuya combinación resulta evidente para un experto en la materia.

"&" documento que forma parte de la misma familia de patentes.

Fecha en que se ha concluido efectivamente la búsqueda internacional.	Fecha de expedición del informe de búsqueda internacional
09.Junio.2009 (09.06.2009)	**01 de Julio de 2009 (01/07/2009)**
Nombre y dirección postal de la Administración encargada de la búsqueda internacional O.E.P.M. Paseo de la Castellana, 75 28071 Madrid, España. Nº de fax 34 91 3495304	Funcionario autorizado M. Alvarez Moreno Nº de teléfono +34 91 349 54 95

INFORME DE BÚSQUEDA INTERNACIONAL

Información relativa a miembros de familias de patentes

Solicitud internacional Nº

PCT/ES 2009/070047

Documento de patente citado en el informe de búsqueda	Fecha de Publicación	Miembro(s) de la familia de patentes	Fecha de Publicación
US 2004177124 A	09.09.2004	WO 0210919 A	07.02.2002
		AU 7803801 A	13.02.2002
		EP 1305712 AB	02.05.2003
		EP 20010955993	27.07.2001
		JP 2004505373 T	19.02.2004
		US 6757714 B	29.06.2004
		US 7117239 B	03.10.2006
		AT 339725 T	15.10.2006
		US 2007011295 A	11.01.2007
		DE 60123076 T	29.03.2007
EP 1370025 AB	10.12.2003	EP 20030011122	22.05.2003
		JP 2004013901 A	15.01.2004
		HK 1059693 A	23.02.2007
		DE 60308755 T	16.08.2007
		US 7506048 B	17.03.2009
US 2004015619 A	22.01.2004	NINGUNO	----------
US 2006031543 A	09.02.2006	JP 2005216307 A	11.08.2005
		US 7296079 B	13.11.2007
		US 2008028091 A	31.01.2008
		US 7447790 B	04.11.2008

INFORME DE BÚSQUEDA INTERNACIONAL

Solicitud internacional Nº

PCT/ ES 2009/070047

CLASIFICACIÓN DEL OBJETO DE LA SOLICITUD

H04L 12/24 (2006.01)
H04L 12/26 (2006.01)