

# Televisión IP

Notas del curso Tecnología de Servicios Audiovisuales

Pablo Flores Guridi

4 de noviembre de 2019

## Índice

<b>1. Introducción</b>	<b>2</b>
<b>2. IP Multicasting</b>	<b>3</b>
2.1. Niveles de conformidad . . . . .	3
2.2. Rangos IP para el envío de multicasts . . . . .	3
2.3. Capa 2 al enviar IP multicasts . . . . .	3
<b>3. Internet Group Management Protocol (IGMP)</b>	<b>5</b>
3.1. Formato de un mensaje IGMPv2 . . . . .	5
3.2. Descripción de IGMPv2 . . . . .	6
3.2.1. Diagrama de estados de un <i>host</i> . . . . .	6
3.2.2. Diagramas de estados de un router . . . . .	8
<b>4. IGMP Snooping</b>	<b>11</b>
4.1. Switch como IGMP <i>Querier</i> . . . . .	11
4.2. Reenvío de datos . . . . .	11
4.3. Reenvío de mensajes IGMP . . . . .	11
<b>Referencias</b>	<b>12</b>

## 1. Introducción

La Televisión IP, o IPTV como es comúnmente denominada, es una tecnología utilizada para distribuir señales de televisión hacia un conjunto de usuarios. Cumple el mismo propósito que la televisión terrestre, por cable o satelital: distribuir una grilla de servicios (lo más amplia posible) que pueda ser vista en un televisor, en general a través de un decodificador digital (STB, del inglés *Set Top Box*). Si bien se emplea el protocolo IP, no se utiliza la Internet pública, sino que una red IP privada [1].

A diferencia de la IPTV, el OTT (del inglés *Over The Top*), se trata de la distribución de contenido multimedia sobre la Internet pública. Puede tratarse de contenido a demanda (VoD, del inglés *Video on Demand*) o lineal. El primer caso refiere a contenido que puede ser accedido por el usuario en el momento que lo desee, como por ejemplo las series de Netflix [2] o los videos de Youtube [3]. El contenido lineal, en cambio, es televisión en tiempo real, contenido que se está emitiendo en este preciso momento, como por ejemplo una radio por Internet reproducida desde TuneIn [4].

Para distribuir IPTV en general se envía el MPEG TS [5] sobre UDP o RTP+UDP. Estos paquetes serán a su vez encapsulados en IP. Se recomienda que los paquetes IP no sean fragmentados por la red porque esto puede aumentar las pérdidas, por lo que el tamaño máximo de un paquete IP será limitado por el MTU, que muy a menudo tiene un tamaño de 1500 bytes. Esta es la razón por la cual se acostumbra encapsular siete paquetes TS en un paquete IP.

Para hacer llegar estos datagramas a los usuarios finales se emplea el uso de multicasts. Esto hace a la IPTV una tecnología escalable porque la cabecera de televisión envía una única vez cada una de las señales a la red y son los usuarios los que deciden recibir uno u otro tráfico. No se establece una conexión independiente por cada contenido reproducido, como sí sucede en OTT. Conceptos importantes para la implementación de IPTV son entonces el *IP multicasting* y las maneras que tienen los equipos de red de controlar el tráfico: el *Internet Group Management Protocol (IGMP)*, mediante el cual un STB pide a los equipos de red el tráfico correspondiente a una señal de televisión, e *IGMP Snooping*, un mecanismo que tienen algunos switches para optimizar el uso del ancho de banda. Todos estos temas serán abordados más adelante.

Quedan fuera del alcance de este documento los mecanismos de señalización y envío de metadata. Esto es: descubrimiento de servicios, envío de la guía de programación y datos necesarios para la descrición de las señales, entre otros. Existen distintas maneras de hacerlo, algunas abiertas y otras propietarias, definidas por algún proveedor de tecnología en particular. Para el caso de DVB existe un estándar que puede ser fácilmente accedido [6].

La estructura de este documento es como sigue. En la sección 2 se presenta el uso de multicasts sobre IP. La sección 3 aborda IGMP y finalmente, en la sección 4 se introduce IGMP Snooping.

## 2. IP Multicasting

El *IP multicasting* fue especificado en 1989 en [7] y se trata de la transmisión de datagramas IP a un conjunto (o grupo) de *hosts* en simultáneo, denominado *host group*. Mediante el uso de *IP multicasts* (o simplemente “multicasts”) es posible identificar cero, uno o incluso múltiples *hosts* con una única dirección IP de destino.

La membresía de un *host* a un grupo de multicast es dinámica. Esto quiere decir que un *host* puede unirse o abandonar un grupo en cualquier momento. No existen restricciones respecto al número de miembros de un *host group*, y un *host* puede ser miembro de múltiples grupos a la vez. Además, no es necesario que un *host* sea miembro de un grupo en particular para que le envíe multicasts.

Los equipos encargados de enrutar a las multicasts entre distintas redes son denominados “routers de multicast”. Un *host* siempre envía una multicast a su red local. Esta multicast llegará a todos sus *hosts* vecinos, pero si el *time-to-live* del datagrama es mayor a 1, los distintos routers de multicast se encargarán de reenviarlas hacia otras redes en las cuales haya miembros.

El protocolo mediante el cual un *host* se une o abandona un grupo de multicast, y reporta su membresía a un router de multicast, es denominado *Internet Group Management Protocolo (IGMP)* y se describe en la sección 3.

### 2.1. Niveles de conformidad

La especificación [7] define tres niveles de conformidad:

- **Nivel 0:** sin soporte para el uso de multicasts.

Puede haber *hosts* que no soporten trabajar con multicasts y no serán afectados en caso que haya otros *hosts* en la red que sí lo hagan. Las direcciones IP de los grupos de multicast están bien definidas por lo que son fácilmente reconocibles.

- **Nivel 1:** soporte para el envío de multicasts pero no para su recepción.

Este nivel de conformidad permite a los *hosts* participar de algunos grupos de multicast definidos para ciertos servicios, pero no podrán unirse a un grupo de multicast cualquiera. Sí serán capaces de enviar datagramas a cualquier grupo de multicast. No requiere la implementación del protocolo IGMP.

- **Nivel 2:** soporte total para el uso de multicasts.

Este nivel de conformidad permite a un *host* tanto el envío como la recepción de multicasts. Sí requiere la implementación del protocolo IGMP.

### 2.2. Rangos IP para el envío de multicasts

El rango de direcciones IP definido para los grupos de multicast es:

$$[224.0.0.0 - 239.255.255.255],$$

y este conjunto de direcciones IP es denominado *Clase D*. Las direcciones *Clase D* son todas aquellas con sus bits más significativos en 1110.

En particular, la dirección 224.0.0.0 no debe ser asignada a ningún grupo de multicast, en tanto que todos los *hosts* con nivel 2 de conformidad deben ser miembros del grupo 224.0.0.1, siempre. A estos grupos de multicast predefinidos se los denomina grupos permanentes (en rigor su nombre es en inglés, *permanent groups*). Puede haber otros, pero no los trataremos en este documento.

La dirección IP de origen de un datagrama enviado a un grupo de multicast debe ser la del *host* que hizo el envío. Una dirección de multicast nunca debe ser puesta como dirección de origen.

### 2.3. Capa 2 al enviar IP multicasts

La manera de definir la dirección MAC de destino al enviar un datagrama hacia una dirección IP perteneciente a un grupo de multicast es mediante un mapeo entre ambos campos.

El rango de direcciones MAC asignado para el envío de multicasts es:

[01 : 00 : 5E : 00 : 00 : 00 – 01 : 00 : 5E : 7F : FF : FF],

donde los 23 bits menos significativos deben coincidir con los 23 bits menos significativos del *host group*. Según lo visto en la sección 2.2, un *host group* es definido por los 28 bits menos significativos de una dirección IP Clase D, por lo que más de un grupo de multicast contará con la misma dirección MAC de destino.

**Ejemplo 2.1.** Para el grupo de multicast 235.150.0.63, la dirección MAC de destino debe ser 01-00-5E-16-00-3F (00000001-00000000-01011110-000**10110**-00000000-00**111111**, donde los números en negrita son los obtenidos a partir del *host group*). Es posible ver que el grupo de multicast 235.22.0.63 contará con la misma dirección MAC de destino.

### 3. Internet Group Management Protocol (IGMP)

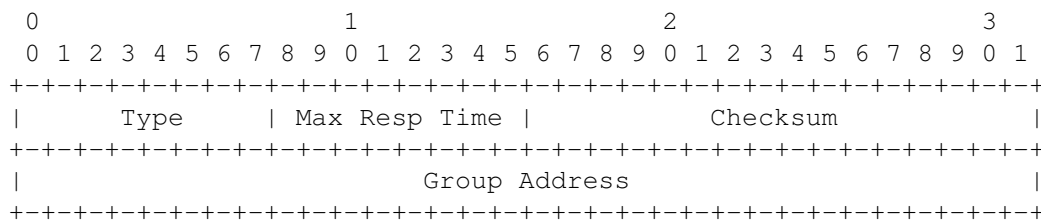
El *Internet Group Management Protocol* (IGMP) debe ser implementado por todo *host* que quiera recibir multicasts en una red IP, ya que mediante este protocolo es que se reporta a los routers de multicast vecinos su pertenencia a un cierto grupo. A partir de este momento y durante toda esta sección, siempre que se refiera a un router, en rigor se estará haciendo referencia a un router de multicast.

La versión original del protocolo data de 1989 (IGMPv1) y es especificada en [7]. Esta versión fue actualizada en 1997 por la versión 2 (IGMPv2) especificada en [8], que a su vez fue actualizada en 2002 por la versión 3 (IGMPv3) especificada en [9].

Si bien todas las versiones son compatibles hacia atrás, en esta sección nos centraremos únicamente en IGMPv2. Queda fuera del alcance de este documento la compatibilidad entre versiones.

#### 3.1. Formato de un mensaje IGMPv2

Los mensajes IGMPv2 son encapsulados en datagramas IP y tienen un tamaño de ocho bytes según el siguiente formato:



en donde

- **Type** especifica el tipo de mensaje, y puede tomar tres valores posibles:
  - **Membership Query** (0x11): son mensajes enviados por los routers con dos posibles subtipos:
    - **General Query**: utilizados para aprender qué grupos tienen miembros en una interfaz de red específica. Son enviados a la dirección *all-system multicast group* (224.0.0.1).
    - **Group-Specific Query**: utilizados para aprender si un determinado grupo tiene algún miembro en una interfaz de red específica. Son enviados a la multicast del grupo correspondiente.
  - **Version 2 Membership Report** (0x16): son enviados por un *host* a la dirección de multicast correspondiente para avisar al router que el *host* es miembro del grupo.
  - **Leave Group** (0x17): son enviados por un *host* a la dirección *all-routers multicast group* (224.0.0.2) cuando desea abandonar un grupo específico.
- **Max Response Time**: este campo sólo tiene valor en mensajes de tipo *Membership Query* enviados por un router. Especifica el tiempo máximo, en unidades de 1/10 segundos, permitido antes de que el *host* responda con un *Membership Report*. En todos los demás mensajes debe valer cero.
- **Checksum**: es el complemento a uno de la suma (también complemento a uno) de todo el mensaje IGMP (toda la carga útil del paquete IP). Para computar la suma, este campo debe ser puesto con sus 16 bits en cero. Luego, el complemento a uno de la suma es agregado en el cambio antes de enviar el mensaje.
- **Group Address**: este campo tomará los siguientes valores según el tipo de mensaje:
  - cero para un *General Query*;
  - la dirección de multicast del grupo consultado para un *Group-Specific Query*;
  - la dirección de multicast del grupo reportado para un *Membership Report*; y
  - la dirección de multicast del grupo abandonado para un *Leave Group*.

## 3.2. Descripción de IGMPv2

Toda red de multicast debe tener un router encargado de enviar periódicamente mensajes del tipo *Membership Query* de manera de saber qué *hosts* son miembros de qué grupos de multicast. Este router es denominado *Querier* y en general será único en la red. Puede haber otros routers, pero deberán funcionar en modo *Non-Querier*. Esto quiere decir que no enviarán mensajes preguntando membresía. El *Querier* debe recibir todas las multicasts de la red en sus interfaces y las reenviará hacia donde haya *hosts* miembros.

Cuando un router inicia, lo debe hacer como *Querier* en cada una de sus interfaces. Sin embargo, si escucha un *Membership Query* de otro router con dirección IP menor a la suya, debe cambiar su rol a *Non-Querier*. Sólo volverá a su rol de *Querier* en caso que transcurra cierto tiempo sin escuchar un *Membership Query* por parte del otro router. Ese tiempo es conocido como *Other Querier Present Interval*.

Cuando un *host* recibe un *General Query* inicia un temporizador independiente para cada uno de los grupos de multicast a los que pertenece. Cada temporizador toma un valor aleatorio y uniforme en el rango  $(0, \text{Max Response Time}]$ , con *Max Response Time* el valor recibido en el *General Query* enviado por el router. Cuando un *host* recibe un *Group-Specific Query*, hace lo mismo, pero únicamente para el grupo específico del mensaje. Si en alguno de los dos casos anteriores el *host* ya cuenta con un temporizador corriendo, debe volver a configurarlo siempre y cuando *Max Response Time* sea menor al valor actual del temporizador. Cuando el temporizador de alguno de los grupos expira, el *host* debe enviar un *Membership Report* al grupo correspondiente para indicar al router que cuenta con miembros en esa interfaz. Si el *host* recibe un *Membership Report* de otro *host* en la red antes de que su temporizador expire, lo debe detener sin enviar ningún reporte para no generar duplicados.

Cuando un router recibe un *Membership Report* agrega el grupo reportado a su lista de grupos de multicast con miembros en la interfaz específica. Luego, inicia un temporizador con cierto valor denominado *Group Membership Interval*. Si no se recibe un reporte de algún *host* miembro del grupo antes que el temporizador expire, el router asume que el grupo ya no cuenta con miembros en la interfaz específica y por lo tanto deja de reenviar la multicast por esa interfaz.

Cuando un *host* se une a un grupo de multicast por vez primera, debe enviar un *Membership Report* “no solicitado” para que el router se entere que en la red hay un nuevo miembro (quizás sea el único). Por otra parte, cuando un *host* abandona un grupo de multicast debe enviar un *Leave Group*. Esto es necesario siempre y cuando haya sido el último en enviar un *Membership Report* al router. Si no fuera el caso, puede decidir no enviar ningún mensaje, ya que debe haber otro miembro en la red.

Cuando un router recibe un *Leave Group* para un grupo que tiene miembros en una interfaz en particular, envía cierta cantidad de *Group-Specific Queries* cada cierto tiempo para ver si existen otros miembros activos en la red. La cantidad de *Group-Specific Queries* enviada se conoce como *Last Member Query Count* y el tiempo entre mensajes es denominado *Last Member Query Interval*. Si luego de expirado el tiempo de respuesta a estos mensajes el router no recibe reportes por parte de algún *host*, asume que el grupo ya no tiene miembros en la red correspondiente y deja de reenviar la multicast por esa interfaz.

### 3.2.1. Diagrama de estados de un *host*

El comportamiento de un *host* puede ser comprendido mejor basándose en el diagrama de estados de la figura 3.1. Los estados en los que puede estar un *host*, los eventos que lo llevan a pasar de un estado al otro y las acciones llevadas adelante al hacerlo son comentadas en esta sección.

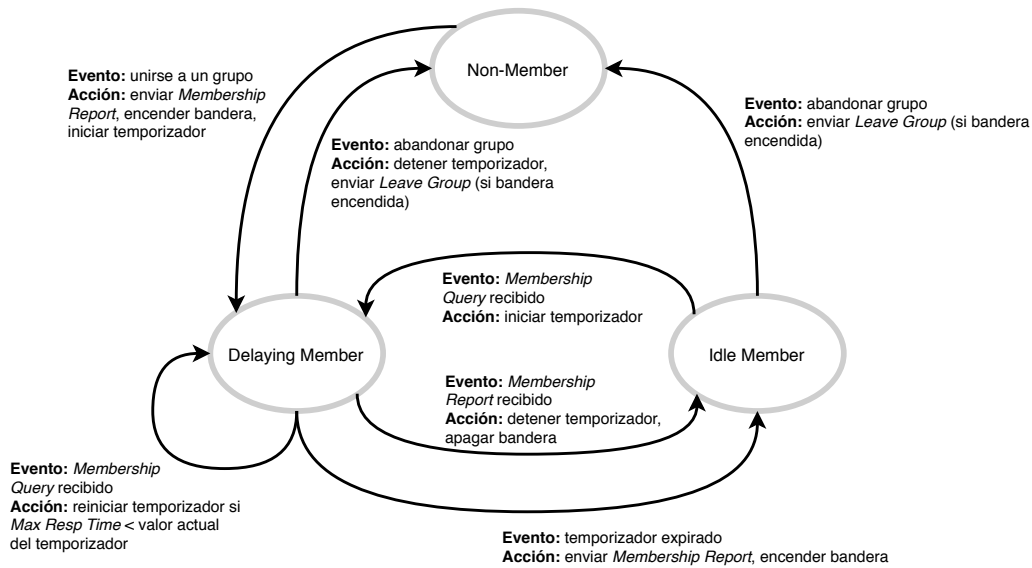


Figura 3.1: Diagrama de estados de un *host* en IGMPv2.

Un *host* puede estar en cualquiera de los tres estados especificados a continuación, para cada grupo de multicast y en cada interfaz física:

- **“Non-Member”**: un *host* está en este estado cuando no pertenece al grupo de multicast. Es el estado inicial de cualquier *host*.
- **“Delaying Member”**: un *host* está en este estado cuando pertenece al grupo de multicast y tiene un temporizador corriendo para ese grupo.
- **“Idle Member”**: un *host* está en este estado cuando pertenece al grupo de multicast pero no tiene un temporizador corriendo para este grupo.

Existen cinco posibles eventos que pueden generar un cambio de estado en un *host*:

- **“Unirse a un grupo”**: es el evento mediante el cual un *host* se une al grupo de multicast. Sólo puede ocurrir en el estado *Non-Member*.
- **“Abandonar un grupo”**: es el evento mediante el cual un *host* abandona el grupo de multicast. Sólo puede ocurrir cuando el *host* es miembro del grupo, o sea en los estados *Delaying member* y *Idle Member*.
- **“Membership Query recibido”**: ocurre cuando un *host* recibe un *General Query* o un *Group-Specific Query*. Un *General Query* aplica a todos los grupos de multicast a los que el *host* es miembro, en tanto que un *Group-Specific Query* aplica únicamente al grupo de multicast específico. Los *hosts* en estado *Non-Member* deben ignorar estos eventos.
- **“Membership Report recibido”**: ocurre cuando un *host* recibe un *Membership Report* para el grupo de multicast en cuestión, enviado por otro *host*. Estos mensajes son ignorados cuando el *host* está en los estados *Non-Member* y *Idle Member*.
- **“Temporizador expirado”**: ocurre cuando el temporizador correspondiente al grupo de multicast en cuestión expira. Sólo ocurre cuando el *host* está en el estado *Delaying Member*.

Existen finalmente siete posibles acciones a tomar por un *host* en respuesta a los eventos anteriores:

- **“Enviar Membership Report”**: el *host* envía un *Membership Report* al router para informar su pertenencia al grupo de multicast. Es enviado a la multicast del grupo.

- **“Enviar *Leave Group*”**: el *host* envía un *Leave Group* al router para informar que abandona el grupo de multicast. Este mensaje puede no ser enviado si la bandera indicando haber sido el último *host* en enviar un *Membership Report* está apagada.
- **“Encender bandera”**: esta bandera es encendida cuando el *host* es el último en enviar un *Membership Report* para el grupo de multicast.
- **“Apagar bandera”**: la misma bandera se apaga cuando otro *host* envía un *Membership Report* para el grupo de multicast.
- **“Iniciar temporizador”**: el *host* inicia un temporizador para el grupo de multicast. Se hace con un valor aleatorio y uniforme en el rango  $(0, Max Response Time]$ , con *Max Response Time* el valor recibido en el *Membership Query* enviado por el router. Si se trata de un *Membership Report* “no solicitado”, el *Max Response Time* se reemplaza por un valor previamente definido denominado *Unsolicited Report Interval*.
- **“Reiniciar temporizador”**: acción realizada cuando el *host* ya tiene un temporizador corriendo para el grupo de multicast y recibe un *Membership Query* con *Max Response Time* menor al tiempo actual del temporizador. En ese caso se procede como en *Iniciar temporizador*.
- **“Detener temporizador”**: se detiene el temporizador para el grupo de multicast correspondiente.

El grupo de multicast *all-system multicast group* (224.0.0.1) se maneja de una manera especial. Para este grupo todos los *hosts* comienzan en el estado *Idle Member*, nunca se desplazan hacia otro estado, y tampoco envían *Membership Reports* para este grupo.

### 3.2.2. Diagramas de estados de un router

A continuación se describe el comportamiento de un router de multicast. Primero, en la figura 3.2 se presentan los estados *Querier* y *Non-Querier*, y cómo son las transiciones de uno hacia el otro. Luego, en la figura 3.3 se muestra cómo un router en estado de *Querier* lleva registro de los *hosts* miembros de los distintos grupos de multicast.

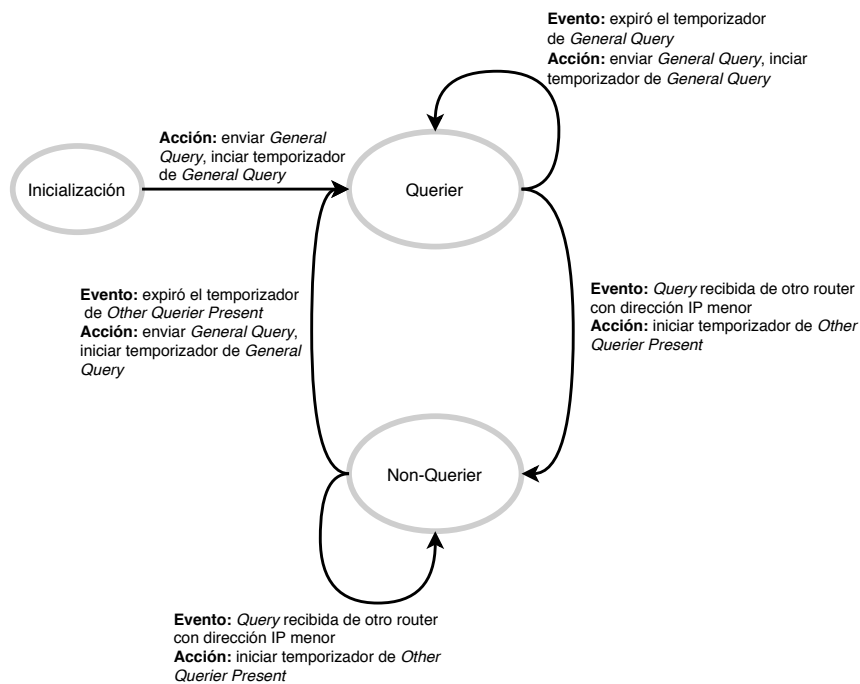


Figura 3.2: Estados de *Querier* y *Non-Querier*, y sus transiciones en IGMPv2.

Tal y como se muestra en la figura 3.2, un router puede estar en alguno de los siguientes dos estados:



- **“Querier”**: cuando un router es designado para transmitir consultas de membresía (*Queries*) en IGMP.
- **“Non-Querier”**: cuando en la red hay otro router designado para transmitir consultas de membresía (*Queries*) en IGMP.

Los siguientes tres eventos pueden hacer a un router cambiar de estado:

- **“Expiró el temporizador de *General Query*”**: ocurre cuando el temporizador para la transmisión de mensajes *General Query* expira.
- **“*Query* recibida de otro router con dirección IP menor”**: ocurre cuando un *Membership Query* es recibido desde otro router en la red con dirección IP menor.
- **“Expiró el temporizador de *Other Querier Present*”**: ocurre cuando el temporizador configurado para esperar un *Membership Query* de otro router en la red con menor dirección IP expira.

Hay tres acciones que un router puede tomar en respuesta a los eventos anteriores:

- **“Iniciar temporizador de *General Query*”**: el router inicia el temporizador de *General Query* en un valor denominado *Query Interval*.
- **“Iniciar temporizador de *Other Querier Present*”**: el router inicia el temporizador de *Other Querier Present* en un valor denominado *Other Querier Present Interval*.
- **“Enviar *General Query*”**: el mensaje *General Query* es enviado al *all-system multicast group* (224.0.0.1).

Un router en estado de *Querier* lleva el seguimiento de la membresía de los *hosts* a los grupos de multicast existentes según el diagrama de estados de la figura 3.3.

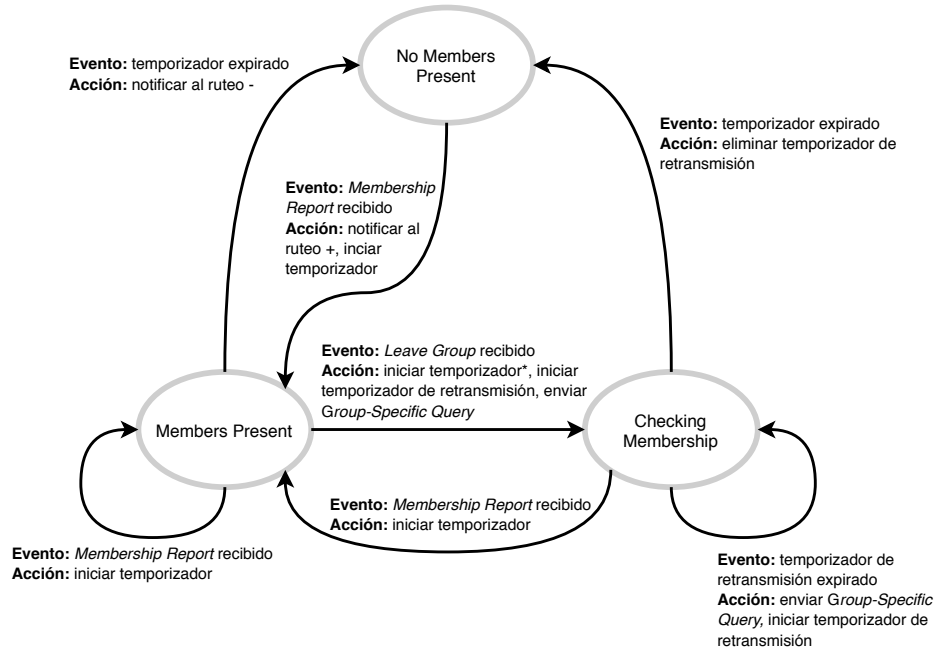


Figura 3.3: Un router funcionando como *Querier* en IGMPv2.

Para cada grupo de multicast, un router puede estar en cualquiera de los siguientes tres estados:

- **“No Members Present”**: cuando no hay *hosts* en la red que hayan enviado *Membership Reports* para el grupo de multicast. Este es el estado inicial para un router respecto a cualquier grupo de multicast.

- **“Members Present”**: cuando hay un *host* en la red que haya enviado un *Membership Report* para el grupo de multicast.
- **“Checking Membership”**: cuando el router recibió un *Leave Group* pero todavía no recibió un *Membership Report* para el grupo de multicast.

Cualquiera de los siguientes cuatro eventos pueden hacer a un router cambiar de estado:

- **“Membership Report recibido”**: ocurre cuando el router recibe un *Membership Report* para el grupo de multicast.
- **“Leave Group recibido”**: ocurre cuando el router recibe un *Leave Group* para el grupo de multicast.
- **“Temporizador expirado”**: ocurre cuando el temporizador configurado para esperar *Membership Reports* para el grupo de multicast expira.
- **“Temporizador de retransmisión expirado”**: ocurre cuando el temporizador configurado para retransmitir *Group-Specific Queries* expira.

Finalmente, hay seis posibles acciones que pueden ser tomadas en respuesta a los eventos anteriores:

- **“Iniciar temporizador”**: se realiza para el grupo de multicast correspondiente. También puede reiniciarse el temporizador en caso de ya estar corriendo. El valor que toma el temporizador es denominado *Group Membership Interval*.
- **“Iniciar temporizador\*”**: esta acción es igual a la anterior, salvo que en este caso el temporizador es configurado a un valor distinto:  $[Last Member Query Interval \times Last Member Query Count]$ , con *Last Member Query Interval* el *Max Response Time* en los *Group-Specific Query* enviados en el estado *Checking Membership*, y *Last Member Query Count* la cantidad de retransmisiones de *Group-Specific Queries* antes de asumir que el grupo ya no tiene más miembros.
- **“Iniciar temporizador de retransmisión”**: se inicia un temporizador para los reenvíos de *Group-Specific Queries*. El valor que toma este temporizador es denominado *Last Member Query Interval*.
- **“Enviar Group-Specific Query”**: estos mensajes son enviados para el grupo de multicast que se recibió el *Leave Group*. Deben tener el valor *Max Response Time* configurado como *Last Member Query Interval*.
- **“Notificar al ruteo +”**: se notifica al protocolo de ruteo que hay miembros de este grupo en la red.
- **“Notificar al ruteo -”**: se notifica al protocolo de ruteo que ya no hay miembros de este grupo en la red.

## 4. IGMP Snooping

El comportamiento por defecto de un switch es reenviar todo el tráfico de multicast por todas sus interfaces independientemente de tener *hosts* miembros conectados o no. Este comportamiento puede cargar la red de manera innecesaria.

IGMP Snooping es el proceso mediante el cual los switches (dispositivos de capa 2) son capaces de escuchar el tráfico IGMP (de capa 3) entre routers y *hosts* de manera de mantener un mapeo de qué grupos de multicast tienen miembros en qué interfaces. De esta manera es posible reenviar el tráfico de multicast únicamente por las interfaces que tengan miembros. Se trata de una optimización de capa 2 para IGMP, aunque es claro que en rigor no se está respetando completamente el modelo OSI.

IGMP Snooping no es un estándar, sino que es una funcionalidad que fue siendo incorporada por la industria. Fue entonces que en 2006 se creó la recomendación [10] que sólo tiene carácter informativo y presenta algunos lineamientos respecto a cómo implementarlo. En esta sección se aborda el tema únicamente de manera conceptual y por lo tanto, a quien interesara en detalle, se recomienda consultar la cita anterior.

### 4.1. Switch como IGMP *Querier*

Tal y como se presentó en la sección 3, para que funcione IGMP (y por lo tanto IGMP Snooping) debe haber al menos un router de multicast que reciba todo el tráfico correspondiente a todos los grupos de multicast en sus interfaces. Este router además debe generar *Membership Queries* y recibir los mensajes *Membership Report* y *Leave Group* por parte de los *hosts*.

En general, los switches que implementan IGMP Snooping incorporan funcionalidades de capa 3 y permiten ser configurados como *Queriers*. Lo que se acostumbra a hacer entonces en una red local es configurar un único switch en modo *Querier*, encargado de implementar IGMP para dialogar con los *hosts*. Los demás switches simplemente escucharán el tráfico IGMP y reenviarán los datagramas según los grupos de multicast cuenten con miembros o no en cada una de sus interfaces.

### 4.2. Reenvío de datos

Un switch funcionando como *Querier* debe recibir el tráfico correspondiente a todos los grupos multicast de la red en sus interfaces. Para eso es necesario que cualquier switch que implemente IGMP Snooping reenvíe el tráfico de multicast, no sólo por las interfaces conectadas a *hosts* miembros, sino también por las conectadas al *Querier*. También mediante IGMP Snooping es que un switch aprende si una interfaz está conectada al *Querier* o a un *host*.

Un switch que implemente IGMP Snooping deberá mantener tablas para el reenvío de grupos de multicast que pueden estar basadas en direcciones MAC o direcciones IP. Los hay de los dos, pero es preferible que se basen en direcciones IP por la ambigüedad de las direcciones MAC comentada en la sección 2.

### 4.3. Reenvío de mensajes IGMP

Un switch que implemente IGMP Snooping también deberá tratar con cuidado los mensajes IGMP. Por ejemplo, los *Membership Queries* enviados por el *Querier* deben ser reenviados a todos los *hosts*, sin embargo, los mensajes *Membership Report* deben ser filtrados y enviados únicamente al *Querier* con cierta periodicidad. Si no fuera de esta manera, un *host* que recibe un *Membership Report* por parte de otro *host* pasaría a estado *Idle Member* y dejaría de enviar mensajes de membresía. En tal caso el switch dejaría de saber si por la interfaz conectada a ese *host* es necesario seguir enviando el tráfico correspondiente a ese grupo de multicast o no.

## Referencias

- [1] Wes Simpson. *Video Over IP (Second Edition)*. Focal Press Media Technology Professional Series. Focal Press, second edition, 2008.
- [2] Netflix. <https://www.netflix.com>. [Accedido: 4 de noviembre de 2019].
- [3] Youtube. <https://www.youtube.com>. [Accedido: 4 de noviembre de 2019].
- [4] TuneIn. <https://tunein.com>. [Accedido: 4 de noviembre de 2019].
- [5] Generic Coding of Moving Pictures and Associated Audio: Systems. Standard, International Organization for Standardization, Geneva, CH, December 2000.
- [6] Digital Video Broadcasting (DVB); Transport of MPEG-2 TS Based DVB Services over IP Based Networks. Standard, Digital Video Broadcasting, April 2016.
- [7] S. Deering. Host extensions for IP multicasting. RFC 1112, August 1989.
- [8] W. Fenner. Internet Group Management Protocol, Version 2. RFC 2236, November 1997.
- [9] B. Cain, S. Deering, I. Kouvelas, B. Fenner, and A. Thyagarajan. Internet Group Management Protocol, Version 3. RFC 3376, October 2002.
- [10] M. Christensen, Thrane & Thrane, K. Kimball, Hewlett-Packard, F. Solensky, and Calix. Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches. RFC 4541, May 2006.