

IPTV: Streaming Multicast

Edición 2024



Agenda

Clase 1: Teórico

- Introducción
- IP Multicasting
- IGMP v2
- IGMP v3
- IGMP Snooping

Clase 2: Práctico

- Repaso de teórico
- Demo de IGMP
- Análisis de paquetes



Introducción

¿Qué es IPTV?

Tecnología utilizada para **distribuir señales de televisión hacia un conjunto de usuarios**, para que una grilla de servicios pueda ser vista por un televisor

En general, se utiliza un **decodificador digital** para recibir la señal (**Set Top Box** o STB)

Si bien usa el protocolo IP, no se usa la internet pública, sino una **red privada**



Introducción

IPTV vs. OTT

OTT (**Over The Top**) implica la distribución de contenido multimedia **sobre la internet pública**

Si bien puede utilizar una CDN para mejorar la distribución, los servicios OTT no se meten con la gestión end-to-end de la red, sino que dependen de las condiciones de la red

Ejemplos: contenido a demanda de servicios como Netflix, Youtube, o Hulu, entre otros.

IPTV, en cambio, suele ser un servicio gestionado por quien opera la propia red, que tiene recursos dedicados a esta distribución de contenido



Introducción

¿Cómo se implementa?

Típicamente, se envía el MPEG **Transport Stream sobre UDP** o sobre RTP sobre UDP

Se recomienda que los paquetes IP no sean fragmentados por la red porque puede aumentar las pérdidas

El tamaño máximo es limitado por MTU, que suele ser 1500 bytes

Entonces, lo más común es encontrar **7 paquetes TS encapsulados en un paquete IP**



Introducción

¿Cómo se implementa?

Se usan las multicasts, que forman parte del protocolo IP. De esta manera, **la cabecera de televisión envía una única vez cada señal a la red** y los usuarios deciden recibir o no el tráfico

En OTT, por el otro lado, se establece una conexión independiente por cada contenido reproducido. Esto es más difícil de escalar.

Para comprender cómo se transmite IPTV en la red, hay que profundizar en las dos tecnologías involucradas: **IP multicasting** e **IGMP** (Internet Group Management Protocol)

Es con ellos que una STB recibe las señales y los dispositivos de red optimizan la distribución



IP Multicast

IP multicasting especifica la **transmisión de paquetes IP a un conjunto de hosts en simultáneo**, que se denomina host group

Se usan direcciones IP multicast (o solo “multicasts”) para identificar cero, uno o varios hosts con una única dirección IP de destino

La membresía de un host a un grupo multicast es dinámica, ya que puede unirse o abandonar el grupo en cualquier momento

No existen restricciones respecto al número de miembros de un host group, y un host puede ser miembro de varios grupos a la vez



IP Multicast

Los equipos encargados de enrutar a las multicasts entre distintas redes se denominan routers de multicast

Un host manda una multicast a su red local que llegará a todos sus vecinos. Pero si el time to live del paquete es mayor a 1, los routers multicast se encargarán de reenviarlo hacia otras redes en las que haya miembros

El protocolo mediante el cual un host se une o abandona un grupo de multicast y reporta su membresía se llama IGMP y se verá más adelante



IP Multicast

Niveles de Conformidad

En el RFC 1112 de 1989 se definen tres niveles de conformidad en dispositivos:

Nivel 0: hosts sin soporte para el uso de multicasts, que no serán afectados por otros que sí lo hagan ya que las direcciones IP de los grupos multicast están bien definidas.

Nivel 1: hosts que soportan el envío de multicasts pero no recepción, por lo que pueden participar de algunos grupos multicast pero no podrán unirse a cualquiera.

Nivel 2: hosts con soporte total de multicast, tanto envío como recepción. Este nivel de hosts requiere la implementación del protocolo IGMP.



IP Multicast

Rangos IP

El rango IP definido para los grupos de multicast es [224.0.0.0 - 239.255.255.255] (clase D), de donde se definen los grupos predefinidos llamados “permanentes”. Algunos de ellos son:

- 224.0.0.0, dirección a la que no debe ser asignada a ningún grupo
- 224.0.0.1, de la cual todos los hosts con nivel de conformidad 2 deben ser miembros

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.



IP Multicast

¿Y qué pasa en capa 2?

Para definir la dirección MAC de destino al enviar un datagrama hacia una dirección IP perteneciente a un grupo de multicast, se usa un mapeo entre los campos

El rango de MAC asignado para multicasts es [01 : 00 : 5E : 00 : 00 : 00 - 01 : 00 : 5E : 7F : FF : FF]

De ese rango, los 23 bits menos significativos deben coincidir con los 23 bits menos significativos del host group

Dado que el host group es definido por los 28 bits menos significativos de una dirección clase D, más de un grupo multicast contará con la misma dirección MAC de destino



IP Multicast

Ejemplo de dirección MAC

Se tiene el grupo de multicast 235.150.0.63, que en binario sería:

235	150	0	63
11101011	10010110	00000000	00111111

Usando los 23 bits menos significativos (en amarillo) con los bits predefinidos de la MAC multicast, se obtiene la dirección 01:00:5E:16:00:3F, que se arma como:

01	00	5E	16	00	3F
00000001	00000000	01011110	00010110	00000000	00111111



IP Multicast

Ejemplo de dirección MAC

Sin embargo, si considero el grupo multicast 235.22.0.63, obtengo en binario:

235	22	0	63
11101011	00010110	00000000	00111111

Como solo se modificó el noveno bit, no entra en los 23 menos significativos por lo que no cambia la MAC del grupo multicast y queda repetida con respecto al otro grupo:

01	00	5E	16	00	3F
00000001	00000000	01011110	00010110	00000000	00111111



IGMP

Introducción

Internet Group Management Protocol (IGMP) debe ser implementado por todo host que quiera recibir multicasts en una red IP, porque debe reportar su pertenencia a grupos.

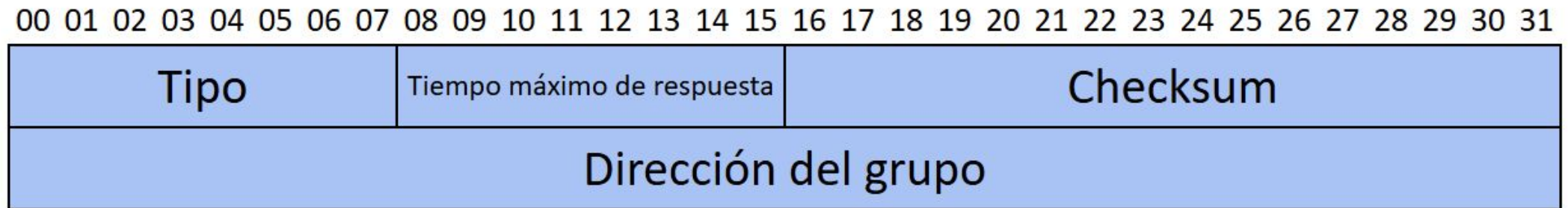
Se han definido hasta ahora tres versiones del protocolo: IGMPv1 (1989), IGMPv2 (1997) e IGMPv3 (2002). Todas ellas son compatibles hacia atrás.

El foco estará en IGMPv2 por su amplia adopción, aunque también veremos conceptos de la versión 3.



IGMP v2

Formato del mensaje



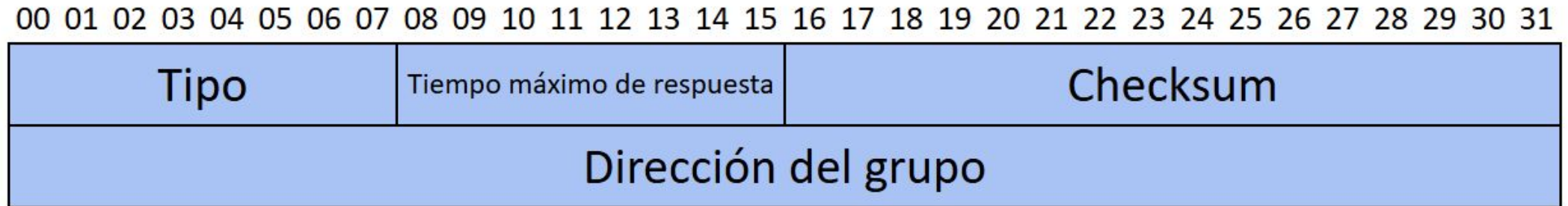
Tipo: tiene tres valores posibles en v2:

1. **Membership query** (0x11): enviados por los routers con dos posibles subtipos
 - General query: usado para aprender qué grupos tienen miembros en una interfaz de red, se envía a la *all-system* multicast group (224.0.0.1)
 - Group Specific Query: usado para aprender si un determinado grupo tiene algún miembro en una interfaz de red, se envía a la multicast del grupo



IGMP v2

Formato del mensaje



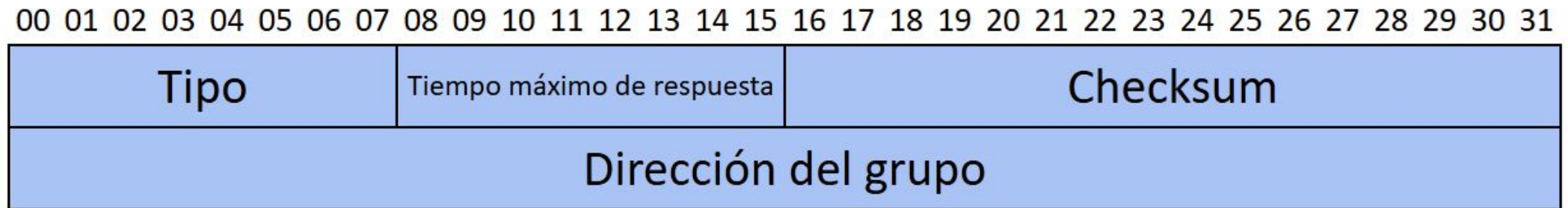
Tipo: tiene tres valores posibles en v2:

2. **Version 2 Membership Report (0x16):** enviados por un host a la dirección de multicast correspondiente para avisar al router que es miembro del grupo
3. **Leave Group (0x17):** enviados por un host a la dirección *all-routers* multicast group (224.0.0.2) cuando desea abandonar un grupo específico



IGMP v2

Formato del mensaje



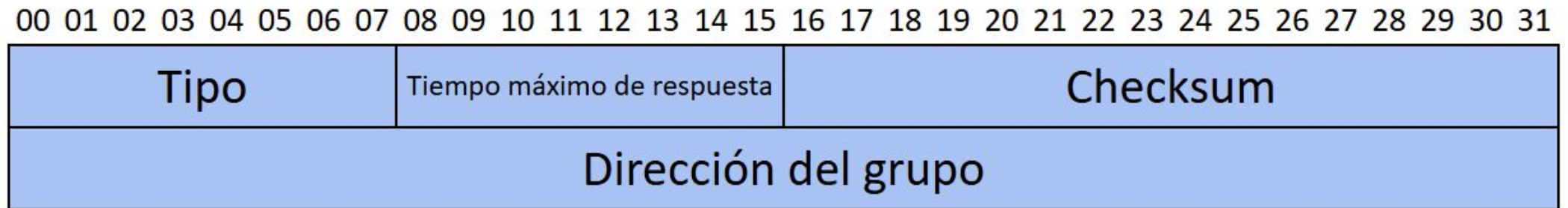
Tiempo máximo de respuesta: solo corresponde en el Membership Query del router. Establece el tiempo permitido antes que el host responda con un Membership Report.

Checksum: complemento a uno de la suma de todo el mensaje IGMP (carga útil del paquete IP)



IGMP v2

Formato del mensaje



Dirección de grupo: según el tipo de mensaje toma diferentes valores:

- 0 para un General Query
- Toma la multicast del grupo consultado en caso de ser Group-Specific Query
- Toma la multicast del grupo reportado en caso de ser Membership Report
- Toma la multicast del grupo abandonado en caso de ser Leave Group



IGMP v2

Descripción

Debe tener un **router encargado de enviar periódicamente mensajes Membership Query** para saber qué hosts son miembros de qué grupos de multicast. Ese router es el **Querier** y es único

Puede haber **otros routers** pero **serán Non-Querier** y no enviarán mensajes de consulta

Todo router se inicializa en modo Querier en todas las interfaces y manda Membership Query a todas ellas. Sin embargo, **si escucha un Membership Query de otro router con dirección IP menor a la suya, debe cambiar su rol a Non-Querier**

Solo volverá a ser Querier si pasa un cierto tiempo sin recibir Membership Query de ningún otro router con IP menor. Ese tiempo es el Other Querier Present Interval



IGMP v2

Descripción

Cuando un host recibe un General Query inicia un **temporizador** para cada uno de sus grupos multicast. Cada temporizador tiene un **valor aleatorio entre 0 y el valor Max Response Time** que recibe en el General Query

Cuando un host recibe un Group-Specific Query, hace lo mismo pero **solo para un grupo**

En ambos casos, si recibe un Query mientras ya tiene un temporizador corriendo, se fija si el Max Response Time es menor al valor actual de su temporizador y, en caso afirmativo, lo reinicia

Cuando un temporizador expira, el host debe enviar un Membership Report al grupo para indicar al router que sigue habiendo miembros en esa interfaz



IGMP v2

Descripción

Cuando un router recibe un Membership Report agrega el grupo reportado a su lista de multicast e inicia un temporizador con el valor llamado Group Membership Interval

Si no se recibe un reporte de algún host, el router asume que ese grupo ya no tiene miembros y deja de reenviar multicast por esa interfaz

Cuando un host se une a un grupo de multicast por primera vez, envía un Membership Report “no solicitado” para que el router se entere que en la red hay un nuevo miembro

Cuando un host abandona un grupo envía un Leave Group, en caso de haber sido el último en enviar un Membership Report. Si no fue el último, puede no avisar que abandona el grupo



IGMP v2

Descripción

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

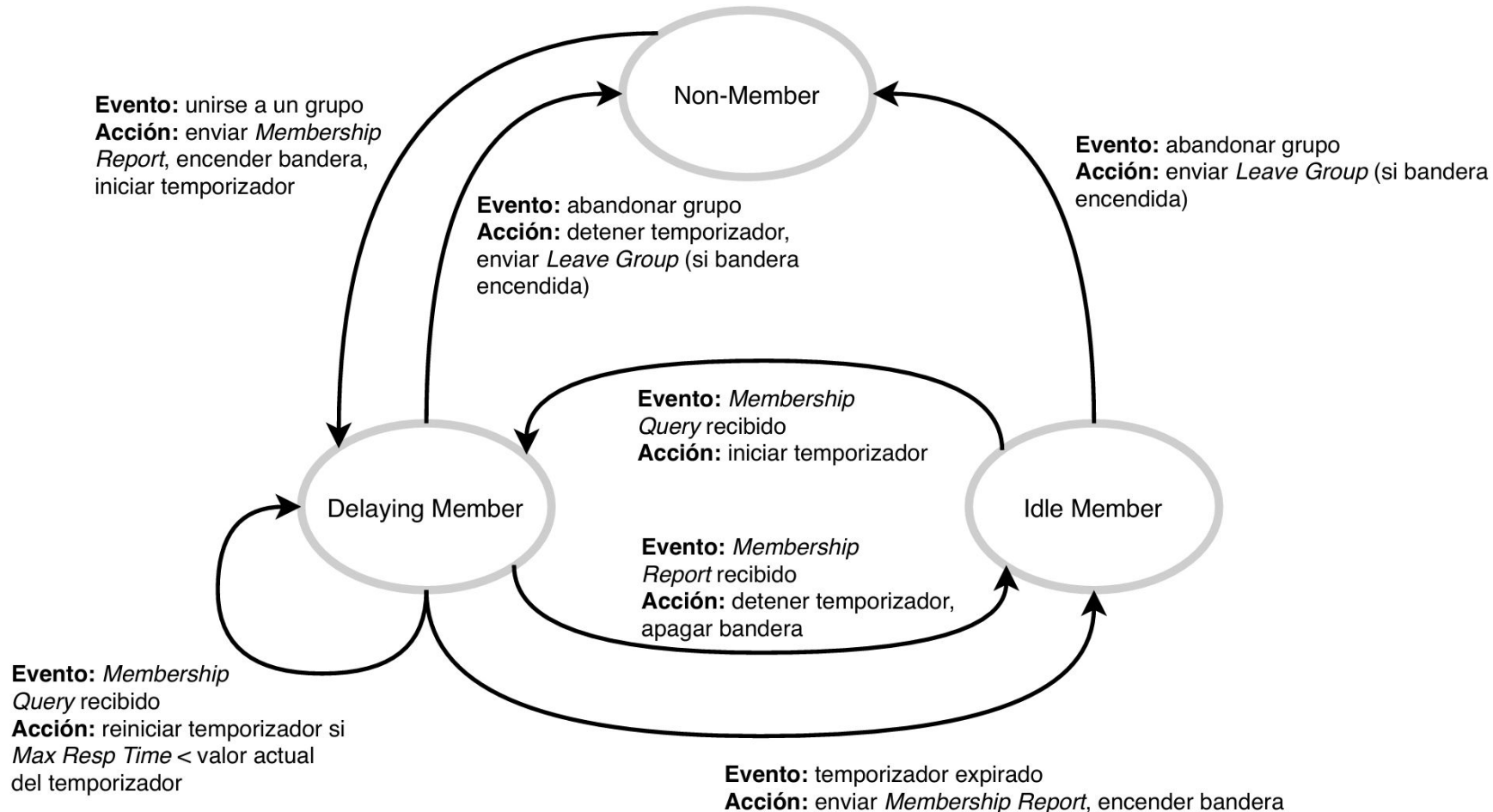
La cantidad de Group-Specific Queries enviada se conoce como Last Member Query Count y el tiempo entre mensajes es denominado Last Member Query Interval

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



IGMP v2

Estados del host



El estado de un host puede ser:

Non-member: estado inicial, no pertenece al grupo multicast

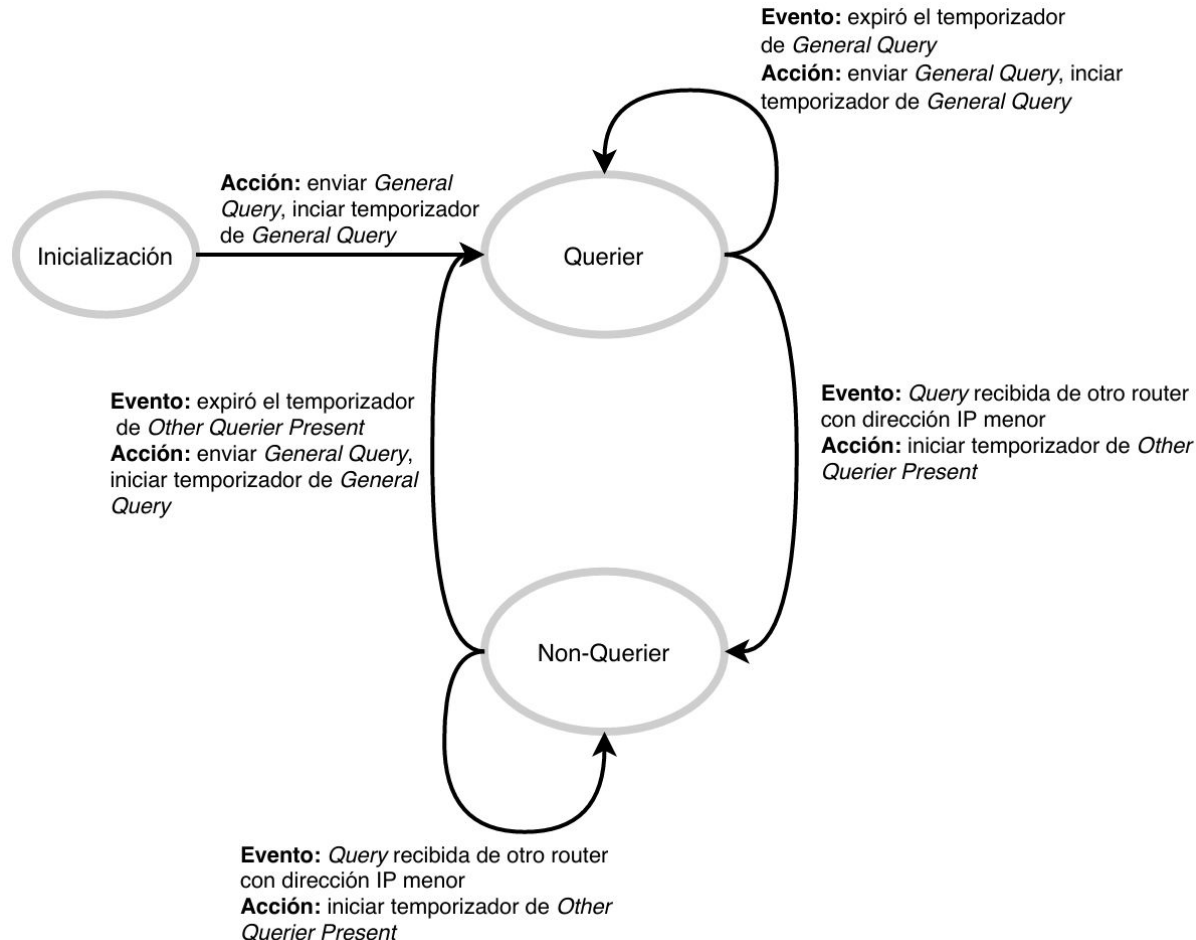
Delaying member: pertenece al grupo multicast y tiene un temporizador corriendo

Idle member: pertenece al grupo multicast y no tiene un temporizador corriendo



IGMP v2

Estados del router



Un router puede ser:

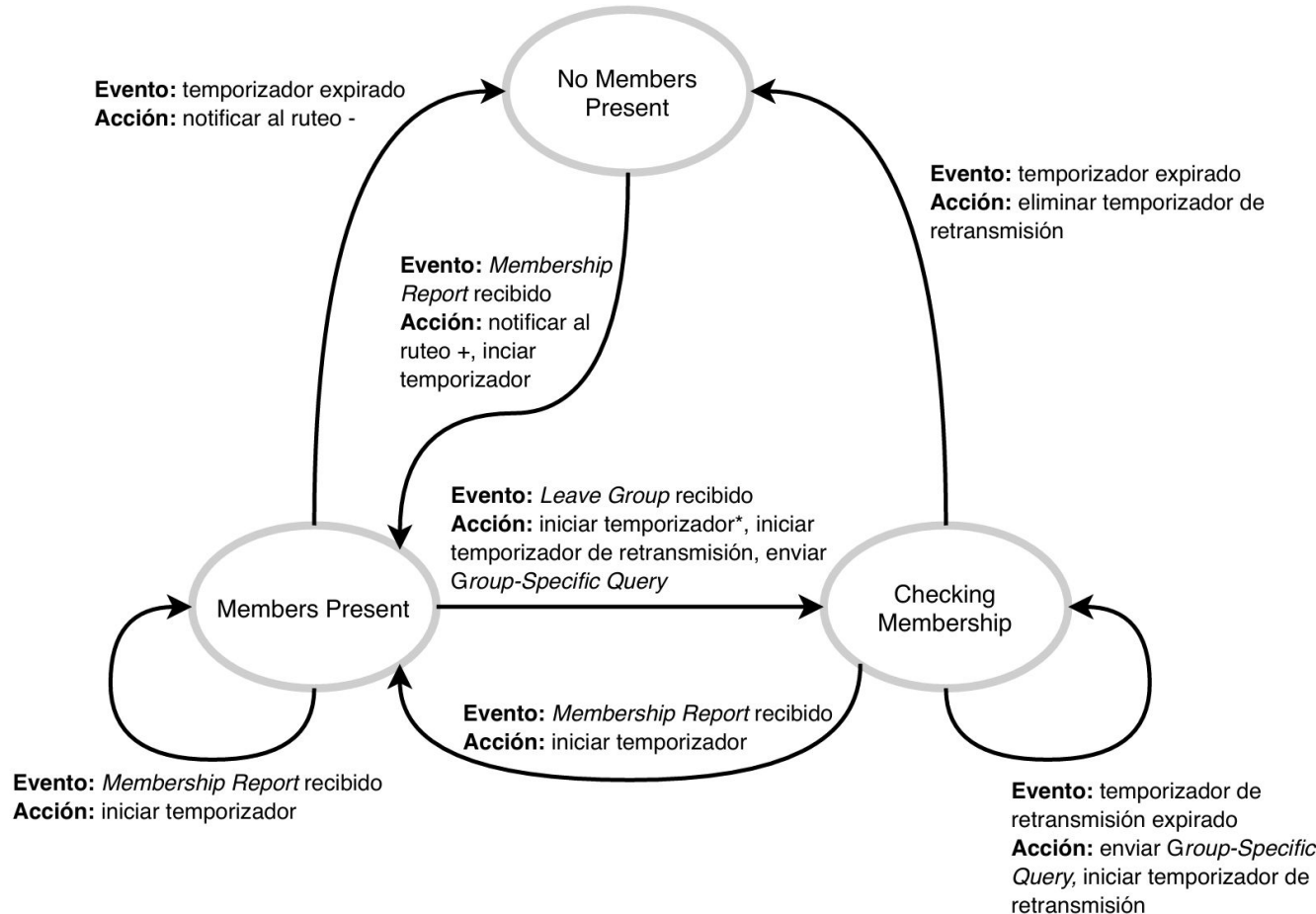
Querier: estado inicial de todos los routers, designado para transmitir consultas de membresía IGMP. Es el router con menor dirección IP

Non-Querier: estado de un router que recibe un query de un router con IP menor. Con el temporizador activo, no se envían queries IGMP a la red



IGMP v2

Estados del querier



El estado de un router querier puede ser:

No members present: estado inicial respecto a todos los grupos. Estado sin hosts en la red

Members present: cuando hay al menos un host enviando Membership Reports

Checking membership: cuando se recibió un Leave Group y ningún Membership Report



IGMP v3

Formato del Membership Report

00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31		
Tipo	Reservado	Checksum
Reservado	Número de registros de grupo	
Registro de grupo [1]		
Registro de grupo [2]		
...		
Registro de grupo [N]		



IGMP v3

Diferencias con IGMPv2

Introduce la capacidad de **especificar una lista de fuentes permitidas** o bloqueadas para recibir tráfico multicast (Source-Specific Multicast, SSM)

Mejora la eficiencia del tráfico multicast al permitir a los hosts seleccionar fuentes específicas

Mantiene **compatibilidad** con IGMPv2, pero agrega funcionalidad más granular para controlar el tráfico

Mensajes más complejos como **Membership Report v3** incluyen detalles de la fuente



IGMP Snooping

Los switches reenvían todo el tráfico multicast por todas las interfaces, sin importar si hay hosts miembros. Este comportamiento puede sobrecargar la red innecesariamente

IGMP Snooping es el proceso donde **los switches escuchan el tráfico IGMP entre routers y hosts**

Permite mantener un mapeo de qué grupos multicast tienen miembros en qué interfaces

El tráfico multicast se reenvía solo por las interfaces con hosts miembros

Es una optimización de capa 2 para IGMP, pero no respeta completamente el modelo OSI

No es un estándar, sino una funcionalidad adoptada por la industria



IGMP Snooping

Switch como Querier

Para que funcione IGMP e IGMP Snooping, debe haber al menos un router de multicast en la red

El router genera Membership Queries y recibe Membership Reports y Leave Group

Switches con IGMP Snooping suelen tener **funcionalidades de capa 3** y pueden actuar como Querier

En redes locales, se configura un único switch como Querier

Los demás switches solo escuchan el tráfico IGMP y reenvían datagramas según la membresía de cada interfaz



IGMP Snooping

Reenvío de datos

Un switch Querier recibe tráfico de todos los grupos multicast en la red

Cualquier switch con IGMP Snooping debe reenviar tráfico multicast no solo a hosts miembros, sino también al Querier

Los **switches aprenden qué interfaces están conectadas al Querier o a un host** mediante IGMP Snooping

Los switches deben **mantener tablas para el reenvío** de grupos multicast, basadas en direcciones MAC o IP

Se prefieren direcciones IP por la ambigüedad de las direcciones MAC



IGMP Snooping

Reenvío de mensajes IGMP

Los switches que implementan IGMP Snooping deben gestionar mensajes IGMP:

Membership **Queries** del Querier **se reenvían a todos los hosts**

Membership **Reports** se filtran y **se envían solo al Querier** periódicamente

Si un host recibe un Membership Report de otro host, pasaría a Idle Member y dejaría de enviar mensajes

El switch podría **dejar de enviar tráfico multicast si no detecta membresía activa** en una interfaz conectada a ese host



