Multicast en una red de oficinas centrales: Indagación CGMP y IGMP

Contenido

Introducción

La función de indagación de Cisco Group Management Protocol (CGMP) y de Internet Group Management Protocol (IGMP) es limitar el tráfico multicast en una red conmutada. De forma

predeterminada, un switch de LAN satura el tráfico multicast dentro del dominio de difusión, lo que puede consumir mucho ancho de banda si varios servidores multicast envían secuencias al segmento.

Antes de comenzar

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

Prerequisites

No hay requisitos previos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Antecedentes

El tráfico multicast se satura porque normalmente un switch reconoce direcciones MAC al examinar el campo de direcciones de origen de todas las tramas que recibe. Una dirección MAC multidifusión nunca se utiliza como dirección de origen para un paquete. Estas direcciones no aparecen en la tabla de direcciones MAC, y el switch no cuenta con un método para reconocerlas.

La primera solución para este problema es configurar las direcciones MAC estáticas para cada grupo y cada cliente. Esta solución funciona bien, sin embargo, no es ni escalable ni dinámica. Use esta solución en un switch Catalyst 4000, 5000, o 6000 al emitir uno de los siguientes comandos:

- **set cam static**
- **set cam permanent**

Estos dos comandos tienen el mismo efecto, excepto que las entradas estáticas desaparecen al reiniciar, y las entradas permanentes no lo hacen.

La segunda solución consiste en utilizar CGMP, un protocolo de propiedad de Cisco que se ejecuta entre el router multicast y el switch. CGMP permite que el router multicast de Cisco comprenda los mensajes IGMP enviados por los hosts y le informa al switch acerca de los datos contenidos en el paquete IGMP.

La última solución (y la más eficaz) es utilizar la indagación de IGMP. Con la indagación de IGMP, el switch intercepta los mensajes IGMP del host mismo y actualiza su tabla MAC según corresponda. Se necesita hardware avanzado para admitir la simulación de IGMP.

Las configuraciones CGMP detalladas en este documento se utilizan para los switches Catalyst 4000 y 5000 que ejecutan CatOS (no se admite CGMP en los switches Catalyst 6000). Por otra parte, las configuraciones IGMP de indagación se utilizan para los switches Catalyst 5000 y 6000 que ejecutan CatOS.

La siguiente sección describe brevemente una dirección multicast, explica las funciones del IGMP, y proporciona detalles adicionales sobre CGMP e IGMP snooping.

Dirección Multicast

1. Las direcciones IP multicast son direcciones IP de clase D. Por lo tanto, todas las direcciones IP desde 224.0.0.0 hasta 239.255.255.255 son direcciones IP multicast. También se las conoce como Direcciones de grupo de destino (GDA).
2. Para cada GDA, existe una dirección MAC asociada. Esta dirección MAC se forma por 01-00-5e, seguido de los últimos 23 bits de las GDA traducidas a hexadecimales, como se muestra a continuación.239.20.20.20 corresponde a MAC 01-00-5e-14-14-14.239.10.10.10 corresponde a MAC 01-00-5e-0a-0a-0a.Por consiguiente, esto no es un mapping uno a uno, sino un mapping uno a varios. De estas dos direcciones, puede observar que el primer octeto (239) no se usa en la dirección MAC. Las direcciones multicast con los mismos últimos tres octetos pero con el primer octeto diferente tienen direcciones MAC que se superponen.
3. Algunas direcciones IP multicast se reservan para uso especial, como se muestra a continuación.224.0.0.1 - Todos los hosts con función multicast.224.0.0.2 – Todos los routers con función multicast.224.0.0.5 y 224.0.0.6 son utilizadas por Abrir primero el trayecto más corto (OSPF).

En general, las direcciones desde 224.0.0.1 a 224.0.0.255 se reservan y son utilizadas por numerosos protocolos (estándar o prioritarios, como Hot Standby Router Protocol (HSRP)). Cisco recomienda que no utilice estos para GDA en una red multidifusión. Las indagaciones CGMP e IGMP no trabajan con este rango de dirección reservada.

Internet Group Management Protocol

IGMP es un estándar definido en RFC1112 para IGMPv1, en RFC2236 para IGMPv2 y en RFC3376 para IGMPv3. IGMP especifica de qué manera un host puede registrarse con un router para recibir tráfico multicast específico. En la siguiente sesión se presenta una breve descripción general de IGMP.

IGMPv1

Los mensajes IGMP versión 1 (IGMPv1) se transmiten en datagramas IP y contienen los siguientes campos:

- Versión: 1
- Tipo: Existen dos tipos de mensajes IGMP, Consulta sobre Afiliación e Informe de Afiliación.
- Checksum
- GDA

Los informes de afiliación son emitidos por hosts que desean recibir un grupo multicast específico (GDA). Los routers emiten las consultas de afiliación en intervalos regulares para verificar si todavía existe un host interesado en la GDA en ese segmento.

Los informes de afiliación del host se ejecutan de forma no solicitada (cuando el host desea recibir primero el tráfico GDA) o para responder a una solicitud de afiliación. Son enviados junto con los siguientes campos:

L2 Information

- MAC de origen: Dirección MAC del Host
- MAC de destino: MAC de destino para GDA

Información de nivel 3

- IP de origen: Dirección IP del host
- IP de destino: GDA

Paquete IGMP

- Los datos IGMP contienen, además, el GDA y algunos otros campos.

Las consultas de afiliación del host son enviadas por el router a la dirección multicast: 224.0.0.1. Estas consultas usan 0.0.0.0 en el campo IGMP GDA. Unhost para cada grupo debe responder a dicha consulta, o el router deja de reenviar el tráfico para ese GDA a dicho segmento (después de tres intentos). El router mantiene una entrada de ruteo multidifusión para cada fuente y la enlaza a una lista de interfaces de salida (interfaz desde donde viene el informe de IGMP). Después de tres intentos de consultas sobre IGMP sin respuesta, esta interfaz se borra de la lista de interfaz de salida para todas las entradas conectadas a ese GDA.

> **Nota:** El IGMPv1 no tiene ningún mecanismo de abandono. Si un host ya no desea recibir el tráfico, simplemente sale. Si éste es el último host de la subred, el router no recibe respuesta alguna a su consulta y borra la GDA para esa subred.

IGMPv2

En IGMP Versión 2 (IGMPv2), el campo versión fue quitado y el campo tipo ahora puede aceptar valores diferentes. Los tipos se muestran a continuación.

- Consulta sobre afiliación
- Informe de afiliación de IGMPv1
- Versión 2 informe de afiliación
- Abandonar el grupo

A continuación, aparecen descripciones de las funciones nuevas más importantes agregadas en IGMPv2.

- Mensaje de Abandono de IGMP: cuando un host desea abandonar un grupo, debe enviar un mensaje Leave Group IGMP al destino 224.0.0.2 (en lugar de retirarse en forma silenciosa como en IGMPv1).
- Ahora, un router puede enviar una consulta específica de grupo al enviar una consulta de afiliación al grupo GDA en vez de enviarla a 0.0.0.0.

IGMPv3

En el IGMP Versión 3 (ICMPv3), hay un campo de tipo que puede tener los siguientes valores:

- Consulta sobre afiliación
- Informe de afiliación versión 3

Una implementación de IGMPv3 también *debe soportar los siguientes tres tipos de mensajes para interoperar con las versiones anteriores del IGMP:*

- Informe de afiliación [RFC1112] de la versión 1
- Informe de afiliación de la Versión 2 (RFC2236)
- Grupo de Abandono de la Versión 2 [RFC2236]

El IGMPv3 agrega compatibilidad para el filtro de origen, es decir, la capacidad que tiene un sistema para informar el interés en la recepción de los paquetes de las direcciones de origen específicas, o de todas las direcciones excepto las **direcciones de origen específicas enviadas a una dirección multicast específica.** Esta característica también se denomina Source Specific Multicast (SSM).

Para que una computadora soporte el SSM, debe soportar el IGMPv3. Sin embargo, relativamente pocos OS soportan IGMPv3. Windows XP es compatible con IGMPv3. Además, hay parches de soporte disponibles de IGMPv3 para FreeBSD y Linux.

Los administradores deben distinguir entre el soporte de IGMPv3 en el router e IGMPv3 snooping en el switch. Son dos características diferentes.

Soporte de IGMPv3 en switches Catalyst (L2)

- El Catalyst 6000 que ejecuta el software en modo híbrido (CatOS en Supervisor y Cisco IOS® Software en MSFC) soporta oficialmente IGMPv3 snooping a partir de la versión 7.5(1).
- En las versiones anteriores a la 7.5(1), el switch Catalyst 6000 no tenía soporte oficial para el IGMPv3, pero debía administrar normalmente paquetes de IGMPv3.
- El Catalyst 6000 que ejecuta Integrated IOS Software soporta IGMPv3 en el router (interfaz L3) a partir de la versión 12.1(8a)E.
- El Catalyst 4000 admite únicamente IGMPv3 en el router del Supervisor III y IV. No soporta IGMPv3 snooping.

Soporte de IGMPv3 en routers Cisco (L3)

El IGMPv3 es admitido en todas las plataformas que ejecutan Cisco IOS® software Release 12.1(5)T y versiones posteriores.

Advertencias

Cuando un switch ejecuta la indagación IGMP, intercepta los paquetes IGMP y llena la Capa 2 (L2) estática, reenviando la tabla en función del contenido de los paquetes interceptados. Cuando hay hosts IGMPv1 o v2 en la red, el switch lee las Incorporaciones y los Abandonos de IGMP para determinar qué host desea recibir la secuencia multicast, o dejar de recibir de la secuencia multicast.

El IGMPv3 es más complicado, porque utiliza no sólo el grupo de dirección (dirección multicast), sino también las fuentes de las que se espera tráfico. Aparte del switch Catalyst 6000 que ejecuta CatOS 7.5 o una versión posterior y Native IOS Version 12.1(8a)E o una posterior, actualmente no se dispone de otros switches para indagar de forma eficaz los paquetes y crear una tabla de

reenvío en función de esta información. Por lo tanto, cuando hay un host IGMPv3 en el switch se debe desactivar la función de indagación IGMP. Cuando se desactiva IGMP snooping, el switch no puede construir dinámicamente una tabla de reenvío L2 para las secuencias multicast. Es decir, el switch satura las secuencias multicast.

Cuando la simulación de IGMP está desactivada, una de las soluciones es configurar manualmente las entradas dinámicas de la Memoria direccionable por contenido (CAM) multicast para evitar la inundación de la subred con tráfico multicast. Sin embargo, ésta es una carga administrativa y no una solución dinámica. Cuando un cliente ya no desea recibir el tráfico, la entrada CAM no se quita del switch (salvo mediante una intervención manual), de manera que el tráfico de la red se continúa dirigiendo al host.

También, al usar el IGMPv3 en la red, los switches que usan CGMP funcionan normalmente aunque la CGMP Fastleave no funcione. Si CGMP Fastleave es necesaria, lo mejor es volver al IGMPv2.

Las advertencias extraordinarias específicas de la plataforma pueden encontrarse en las notas de la versión de los switches correspondientes.

Interoperabilidad entre IGMPv1 e IGMPv2

Con IGMPv1 y IGMPv2, sólo un router por subred IP envía consultas. Este router se denomina router de consulta. En IGMPv1, se elige el router de consulta con la ayuda del protocolo de ruteo multidifusión. En IGMPv2, se elige según la dirección IP menor entre los routers. A continuación, se muestran varias posibilidades:

Escenario 1: Router IGMPv1 con una combinación de Hosts IGMPv1 e IGMPv2

El router no interpreta el informe IGMPv2 y, en consecuencia, todos los hosts deben usar solamente el informe IGMPv1.

Escenario 2: Router IGMPv2 con una combinación de Hosts IGMPv2 e IGMPv3

Los hostsIGMPv1 no entienden la consulta de IGMPv2 o la consulta de afiliación al grupo IGMPv2. El router debe utilizar solamente el IGMPv1, y suspender la operación de abandono.

Escenario 3: El router IGMPv1 y el IGMPv2 ubicados en el mismo segmento

El router IGMPv1 no tiene modo alguno para detectar el router IGMPv2. Por lo tanto, el router IGMPv2 debe ser configurado por el administrador como un router IGMPv1. En todo caso, es posible que no coincidan con el router de consulta.

Interoperabilidad entre IGMPv1/IGMPv2 y IGMPv3

Con todas las versiones de IGMP, sólo un router por subred IP envía consultas. Este router se denomina router de consulta. En el IGMPv1, el router de consulta se selecciona con la ayuda del multicast routing protocol. En IGMPv2 e IGMPv3, se selecciona según la dirección IP más pequeña entre los routers. A continuación, se mencionan varias opciones de interoperabilidad.

Escenario 1: Router IGMPv1/IGMPv2 con una combinación de Hosts IGMPv1/IGMPv2 e IGMPv3

Debido a que el router no entiende los informes de IGMPv3, todos los hosts utilizan informes de IGMPv1/IGMPv2.

Escenario 2: Router IGMPv3 con una combinación de Hosts IGMPv1/IGMPv2 e IGMPv3

Los hosts IGMPv1/IGMPv2 no entienden la consulta de IGMPv3 o la consulta de membresía de IGMPv3. El router sólo debe usar la versión de IGMP que corresponda con la versión de cliente de IGMP menor presente. Si hay clientes IGMPv3 e IGMPv2, el router utiliza el IGMPv2. Si hay clientes IGMPv1, IGMPv2, e IGMPv3, el router utiliza el IGMPv1.

Escenario 3: Diversas versiones de Routers en el mismo Segmento

Cuando los routers de diferentes versiones están presentes en el mismo segmento, los routers de versiones inferiores no tienen forma de detectar los routers de versiones superiores. Por lo tanto, los distintos routers deben ser configurados por el administrador como la misma versión. Esta versión debe coincidir con la versión inferior en cualquier router de consulta presente.

IGMP en un router

Si, de forma predeterminada, no hay ningún usuario registrado en un grupo específico de una subred, el router no reenvía el tráfico multicast para ese grupo en esa subred. Eso significa que un router necesita recibir un informe IGMP para una GDA a fin de agregarla a la tabla de ruteo de multidifusión y comenzar a reenviar tráfico para ese grupo.

En un router, debe realizar las siguientes acciones:

1. Active el ruteo multicast en el modo global, como se muestra a continuación.

   ```
   ip multicast-routing
   ```

2. Configure un protocolo de ruteo multicast en la interfaz involucrada, tal como se muestra a continuación.

   ```
   ip pim dense-mode
   ```

3. Controle IGMP como se muestra a continuación.

   ```
   show ip igmp interface
   show ip igmp group
   show ip mroute
   ```

4. Configure un router para enviar el informe IGMP (en la interfaz), como se muestra a continuación.

   ```
   ip igmp join-group [GDA_ip_address]
   ip igmp version [1 | 2 | 3]
   ```

Ejemplo práctico en un router

Un router se configura para rutear entre dos subinterfaces, Fast-Ethernet 0.2 y Fast-Ethernet 0.3. Ambas interfaces están también configuradas para ejecutar IGMP. En la siguiente salida, puede

ver la versión de IGMP, el grupo unido, etc.

Configuración

```
ip multicast-routing


interface FastEthernet0
 no ip address
 no ip directed-broadcast
!
interface FastEthernet0.2
 encapsulation isl 2
 ip address 10.2.2.1 255.255.255.0
 no ip redirects
 no ip directed-broadcast
 ip pim dense-mode
!
interface FastEthernet0.3
 encapsulation isl 3
 ip address 10.3.3.1 255.255.255.0
 no ip redirects
 no ip directed-broadcast
 ip pim dense-mode
!
```

show ip igmp interface

```
 Fa0.2 is up, line protocol is up
 Internet address is 10.2.2.1/24
 IGMP is enabled on interface
 Current IGMP version is 2
 CGMP is disabled on interface
 IGMP query interval is 60 seconds
 IGMP querier timeout is 120 seconds
 IGMP max query response time is 10 seconds
 Inbound IGMP access group is not set
 IGMP activity: 3 joins, 2 leaves
 Multicast routing is enabled on interface
 Multicast TTL threshold is 0
 Multicast designated router (DR) is 10.2.2.1 (this system)
 IGMP querying router is 10.2.2.1 (this system)
 Multicast groups joined: 224.0.1.40

 Fa0.3 is up, line protocol is up
 Internet address is 10.3.3.1/24
 IGMP is enabled on interface
 Current IGMP version is 2
 CGMP is disabled on interface
 IGMP query interval is 60 seconds
 IGMP querier timeout is 120 seconds
 IGMP max query response time is 10 seconds
 Inbound IGMP access group is not set
 IGMP activity: 1 joins, 1 leaves
 Multicast routing is enabled on interface
 Multicast TTL threshold is 0
 Multicast designated router (DR) is 10.3.3.1 (this system)
 IGMP querying router is 10.3.3.1 (this system)
```

```
No multicast groups joined
```

show ip mroute and show ip igmp group

```
Router_A#show ip mroute
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned
       R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode


(*, 239.10.10.10), 00:01:15/00:02:59, RP 0.0.0.0, flags: DJC
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    FastEthernet0.3, Forward/Dense, 00:01:16/00:00:00

(10.2.2.2, 239.10.10.10), 00:00:39/00:02:20, flags: CT
  Incoming interface: FastEthernet0.2, RPF nbr 0.0.0.0
  Outgoing interface list:
    FastEthernet0.3, Forward/Dense, 00:00:39/00:00:00

Router_A#show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface            Uptime    Expires   Last Reporter
239.10.10.10     Fa0.3                00:02:48  00:02:04  10.3.3.2
Router_A#
```

Protocolo de administración de grupo de Cisco

Para el soporte CGMP en los switches de Catalyst, consulte la Matriz de Soporte de los Switches de Catalyst Multicast.

Tramas CGMP y tipos de mensajes

Cisco implementó por primera vez CGMP para restringir el tráfico multicast en una red L2. Dado que un switch, por esencia, no es capaz de considerar paquetes L3, no puede distinguir un paquete IGMP. Con CGMP, el router proporciona la interfaz entre los hosts. Los routers utilizan el lenguaje de IGMP, y los switches utilizan el lenguaje de CGMP.

Las tramas CGMP son tramas Ethernet con la dirección MAC de destino 01-00-0c-dd-dd-dd y con un encabezado de Protocolo de acceso de subred (SNAP) con un valor de 0x2001. Las tramas CGMP contienen los siguientes campos:

- Versión: 1 ó 2.
- Tipo de mensaje: Agregar o Eliminar.
- Cuenta: El número de pares de direcciones multidifusión/ unidifusión en el mensaje.
- GDA: La dirección MAC de 48 bits del grupo multicast.
- Dirección de Origen Unicast (USA): La dirección MAC de unidifusión de 48 bits de los dispositivos que pretenden unirse al GDA.

Nota: El valor del campo de recuento determina cuántas veces se muestran los dos últimos campos.

De forma predeterminada, los procesadores de un switch (denominados NMP en Catalyst) sólo escuchan las direcciones multicast cuando **show cam system** se ejecuta. Cuando habilita CGMP en un switch, la dirección 01-00-0c-dd-dd-dd se agrega a la **show cam system** resultado del comando.

La siguiente tabla incluye todos los posibles mensajes de CGMP.

GDA	USA	Agregar/Eliminar	Significado
Mcast MAC	MAC de cliente	Incorporarse	Agregue el puerto al grupo.
Mcast MAC	MAC de cliente	Salir	Borrar el puerto del grupo.
00-00-00-00-00-00	MAC de router	Incorporarse	Asigne el puerto del router.
00-00-00-00-00-00	MAC de router	Salir	Desasigne el puerto del router.
Mcast MAC	00-00-00-00-00-00	Salir	Elimine el grupo.
00-00-00-00-00-00	00-00-00-00-00-00	Salir	Elimine todos los grupos.

Aprendizaje de los puertos de router

El switch necesita conocer todos los puertos del router para que se agreguen de manera automática a toda entrada multicast creada recientemente. El switch toma conocimiento de los puertos cuando recibe una incorporación CGMP a GDA 00-00-00-00-00-00 con un router MAC USA (tercer tipo de mensaje en la tabla). Estos mensajes son generados por el router en todas las interfaces configuradas para ejecutar el CGMP. Sin embargo, también existe un método estático para configurar los puertos del router en el switch.

Cómo unirse a un grupo con CGMP

- Un nuevo cliente solicita recibir tráfico para una GDA, por lo que el cliente envía un mensaje de pertenencia IGMP.
- El router recibe el informe de IGMP, lo procesa y envía un mensaje CGMP al switch. El router copia la dirección MAC de destino en el campo GDA de la Conexión CGMP, y copia la dirección MAC de origen en la USA de la conexión CGMP. Luego la envía de vuelta al switch.
- Un switch con el CGMP habilitado debe escuchar las direcciones CGMP 01-00-0c-dd-dd-dd. El procesador del switch mira en la tabla CAM para Estados Unidos. Una vez que se detecta

la USA en la tabla CAM, el switch sabe en qué puerto está ubicada la USA, y lleva a cabo una de las siguientes opciones:Crea una nueva entrada estática para el GDA y conecta el puerto USA a ésta unto con todos los puertos del router.Agrega el puerto USA a la lista de puertos para esta GDA (si la entrada estática ya existe).

Salida de un grupo con CGMP

Las entradas estáticas aprendidas con CGMP son permanentes, a menos que se produzca un cambio de tipología de spanning tree en la VLAN o que el router envíe uno de los últimos mensajes de ausencia de CGMP en la tabla anterior.

Cuando IGMPv1 es el host, no envíe mensajes de Abandono de IGMP. El router envía solamente los mensajes de Abandono si no recibe una respuesta a tres consultas consecutivas sobre IGMP. Esto significa que no se elimina ningún puerto de un grupo si aún hay usuarios interesados en ese grupo.

Con la introducción de IGMPv2 y la presencia de IGMP Leave, Cisco se agrega a la especificación CGMP original (CGMPv2). Esta adición se llama CGMP Fast-Leave.

El procesamiento CGMP Fast-Leave permite al switch detectar mensajes Leave IGMPv2 enviados a la dirección multicast de todos los routers (224.0.0.2) por hosts en cualquiera de los puertos del módulo de motor supervisor. Cuando el módulo del motor supervisor recibe un mensaje de Salida, activa un temporizador de respuesta de consulta y envía un mensaje al puerto en el que esa salida fue recibida para determinar si todavía hay un host dispuesto a recibir a este grupo multicast en ese puerto. Si este temporizador caduca antes de recibirse un mensaje de incorporación CGMP, debe separarse el puerto del árbol multicast para el grupo multicast especificado en el mensaje de ausencia original. Si se trata del último puerto de un grupo multicast, este reenvía el mensaje de ausencia de IGMP a todos los puertos del router. El router activa luego el proceso de borrado normal enviando una consulta específica de grupo. Dado que no se recibe respuesta alguna, el router elimina este grupo de la tabla de ruteo multicast para esa interfaz. También envía un mensaje CGMP Leave (Ausencia de CGMP) al switch que borra al grupo de la tabla estática. El procesamiento Fast-Leave asegura una administración del ancho de banda óptima para todos los hosts en una red conmutada, incluso cuando se utilizan grupos multicast múltiples simultáneamente.

Cuando CGMP Leave está habilitado, se agregan dos entradas a la **show cam system** resultado del comando, como se muestra a continuación.

```
01-00-5e-00-00-01
01-00-5e-00-00-02
```

IGMP Leave utiliza 224.0.0.2 e IGMP Query utiliza 224.0.0.1.

Utilice los siguientes pasos para solucionar los problemas de CGMP.

1. Debido a un conflicto con el HSRP, el procesamiento CGMP Leave se inhabilita de forma predeterminada. El HSRP utiliza la dirección MAC 01-00-5e-00-00-02, que es igual a IGMP Leave con IGMP Versión 2. Con CGMP Fast-Leave, todos los paquetes de HSRP se dirigen a la CPU del switch. Debido a que un mensaje HSRP no es un paquete IGMP, el switch regenera dichos mensajes y los envía a los puertos del router. Los routers que reciben hsrp hello o hsrp peers pierden la conectividad. Por lo tanto, al ejecutar un debug en problemas

de HSRP, intente desactivar CGMP Fast-Leave.Para habilitar el procesamiento de ausencia de CGMP, ejecute el comando **set cgmp leave enable** comando.
2. Cuando se habilita el procesamiento de ausencia de CGMP, el switch de la familia Catalyst 5000 reconoce los puertos del router a través de PIM-v1, HSRP, y de los mensajes de incorporación automática de CGMP. Cuando el procesamiento de ausencia CGMP está desactivado, el switch de la familia Catalyst 5000 aprende los puertos del router a través de los mensajes de incorporación automática CGMP únicamente.
3. El CGMP no recorta el tráfico multicast para ninguna dirección IP de multidifusión que mapee en el rango de direcciones MAC de 01-00-5E-00-00-00 a 01-00-5E-00-00-FF. Las direcciones multicast IP reservadas en el rango 224.0.0.0 a 224.0.0.255, se usan para reenviar tráfico multidifusión IP local en un salto de L3 simple.

CGMP y Red de Origen Solamente

Una red sólo de origen es un segmento que sólo cuenta con una multidifusión de origen y ningún cliente real. Por lo tanto, hay una posibilidad de que no se generen reportes IGMP en ese segmento. Sin embargo, CGMP todavía debe restringir la inundación de esta fuente (sólo para el uso del router). Si un router detecta tráfico multicast en una interfaz sin el informe IGMP, se identifica como red de origen solamente multidifusión. El router genera un mensaje de incorporación CGMP para sí mismo y el switch simplemente agrega este grupo (sólo con el puerto del router).

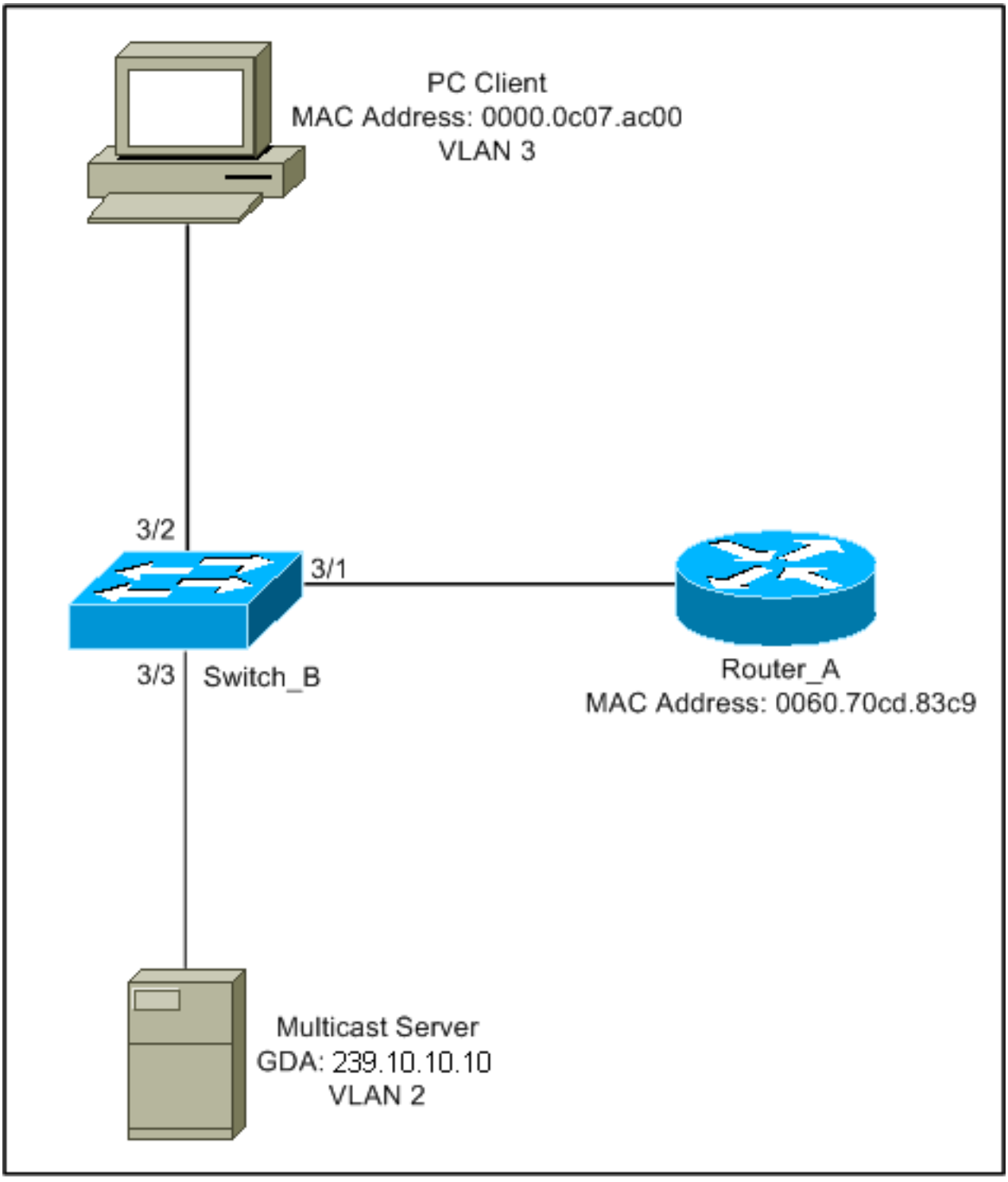
Configuración de Cisco Routers y Switches para Habilitar CGMP

Los siguientes comandos solamente son válidos para las Catalyst 4000 y 5000 Series (más 2901, 2902, 2926, 2948G, y 4912).

- Router MulticastEnable IP multicasting (comando global):**ip multicast-routing**Habilite cada interfaz que ejecuta CGMP (modo de interfaz) con los siguientes comandos:**ip pimip igmpip cgmp**Depure el problema multicast de L2 con los siguientes comandos:**debug ip igmpdebug ip cgmp**
- Catalyst 4000 ó 5000Active/desactive CGMP con los siguientes comandos:**set cgmp**Habilite/inhabilite CGMP Fast-Leave con los siguientes comandos:**set cgmp leave**Configure el router multidifusión (estático) con los siguientes comandos:**set multicast router**Borre el router multicast con los siguientes comandos:**clear multicast router**A continuación se detallan varios comandos para verificar el funcionamiento de CGMP.**show cam staticshow cgmp statisticshow cgmp leaveshow multicast routershow multicast groupshow multicast group cgmpshow multicast group count**

Ejemplo Práctico del Comando Debug, Resultado y Uso de CGMP

El siguiente es un ejemplo práctico de configuración para un router Cisco y para switches de Catalyst.



Esta configuración muestra las operaciones involucradas cuando un host se une a un grupo. Esta configuración también muestra las operaciones que tienen lugar cuando un host deja un grupo con Fast-Leave habilitado. También se proporcionan los rastros de sabueso y la configuración del switch y el router.

Cómo unirse a un grupo con CGMP

Consulte estos pasos al unirse a un grupo con CGMP.

1. Habilite el CGMP en el switch, como se muestra a continuación.

```
Switch_B (enable) set cgmp en
MCAST-CGMP: Set CGMP Sys Entrie
MCAST-CGMP: Set CGMP Sys Entrie
```

```
MCAST-CGMP: Set CGMP Sys Entrie
CGMP support for IP multicast enabled.
Switch_B (enable)
```

Como puede ver a continuación, la entrada 01-00-0c-dd-dd-dd se incluye para todas las VLAN en la **show cam system** resultado del comando. Asimismo, a medida que la red ejecuta CGMP Fast-Leave, pueden verse las entradas para 01-00-5e-00-00-01 y 01-00-5e-00-00-02.

```
Switch_B (enable) show cgmp leave

CGMP:       enabled
CGMP leave: enabled
Switch_B (enable) show cam system
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------ -----  -------------------------------------------
1     00-10-2f-00-14-00  #          7/1
1     00-e0-fe-4b-f3-ff  #          1/9
1     01-00-0c-cc-cc-cc  #          1/9
1     01-00-0c-cc-cc-cd  #          1/9
1     01-00-0c-dd-dd-dd  #          1/9
1     01-00-0c-ee-ee-ee  #          1/9
1     01-80-c2-00-00-00  #          1/9
1     01-80-c2-00-00-01  #          1/9
2     00-10-2f-00-14-00  #          7/1
2     01-00-0c-cc-cc-cc  #          1/9
2     01-00-0c-cc-cc-cd  #          1/9
2     01-00-0c-dd-dd-dd  #          1/9
2     01-80-c2-00-00-00  #          1/9
2     01-80-c2-00-00-01  #          1/9
3     01-00-0c-cc-cc-cc  #          1/9
3     01-00-0c-cc-cc-cd  #          1/9
3     01-00-0c-dd-dd-dd  #          1/9
3     01-80-c2-00-00-00  #          1/9
3     01-80-c2-00-00-01  #          1/9
Total Matching CAM Entries Displayed = 19
```

2. El router envía un mensaje de incorporación CGMP a GDA 00-00-00-00-00-00 con el puerto USA MAC del router. Por lo tanto, el puerto del router se agrega a la lista de puertos del router (consulte el primer ejemplo a continuación).**En el router**

```
6d01h: CGMP: Sending self Join on Fa0.3
6d01h:       GDA 0000.0000.0000, USA 0060.70cd.83c9
```

En el switch

```
MCAST-CGMP-JOIN: recvd CGMP JOIN msg on port 3/1 vlanNo 2
MCAST-CGMP-JOIN: join GDA 00-00-00-00-00-00 MCAST-CGMP-JOIN:USA
                 00-60-70-cd-83-c9
MCAST-ROUTER: Adding QUERIER port 3/1, vlanNo 2
MCAST-ROUTER: Creating RouterPortTimer for  port 3/1, vlanNo 2

Switch_B (enable) show multi router
CGMP enabled
IGMP disabled

Port       Vlan
---------  ----------------
 3/1       2-3

Total Number of Entries = 1
'*' - Configured
```

3. La PC en 3/1 envía un informe IGMP que contiene la GDA: 239.10.10.10 (consulte la trama 2 a continuación). A continuación se muestra el **show ip igmp group** resultado del comando en el router Router_A.Esto muestra que el router ahora reenvía tráfico de 224.10.10.10 a fa0.3. Esto es consecuencia de la recepción del informe IGMP a partir del 10.3.3.2, que es la PC del cliente.

```
Router_A#show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface            Uptime    Expires   Last Reporter
239.10.10.10     Fa0.3                00:02:48  00:02:04  10.3.3.2
Router_A#
```

4. El router recibe el informe y envía un mensaje de incorporación CGMP junto con la siguiente información:MAC de origen: Dirección MAC del routerDest MAC: 01-00-cc-dd-dd-ddContenidos: Dirección MAC del cliente PC (Estados Unidos): 00-00-0c-07-ac-00 dirección MAC del grupo multicast: 01-00-5e-0a-0a-0a (véase la trama 3 a continuación)**En el router**

```
6d01h: IGMP: Received v2 Report from 10.3.3.2 (Fa0.3) for 239.10.10.10
6d01h: CGMP: Received IGMP Report on Fa0.3
6d01h:       from 10.3.3.2 for 239.10.10.10
6d01h: CGMP: Sending Join on Fa0.3
```

5. El switch con 01-00-cc-dd-dd-dd en el **show cam system** el resultado del comando tiene CGMP habilitado. El switch puede procesar el paquete.El switch efectúa una búsqueda en la tabla dinámica CAM para determinar en qué puerto se ubica la dirección de MAC de la PC del cliente. La dirección se localiza en puerto 3/2 y el switch realiza una entrada estática en la tabla CAM 01-00-5e-0a-0a-0a determinada para puerto 3/2 El switch también agrega el puerto del router 3/1 a la entrada estática para ese GDA.**En el switch**

```
MCAST-CGMP-JOIN: recvd CGMP JOIN msg on port 3/1 vlanNo 3
MCAST-CGMP-JOIN: join GDA 01-00-5e-0a-0a-0a MCAST-CGMP-JOIN:USA 00-60-5c-f4-bd-e2
MCAST-CGMP-JOIN: 3/2/3: index 81
MCAST-CGMP-JOIN: recvd CGMP JOIN msg on port 3/1 vlanNo 2
MCAST-CGMP-JOIN: join GDA 01-00-5e-00-01-28 MCAST-CGMP-JOIN:USA 00-60-70-cd-83-c9
MCAST-CGMP-JOIN: 3/1/2: index 80
```

6. Todo el tráfico posterior para el grupo multicast 239.10.10.10 se reenvía solamente a este puerto en este VLAN. A continuación se muestra la entrada estática en el switch Catalyst donde el 3/1 es el puerto del router y 3/2 es el puerto del cliente.

```
Switch_B (enable) show cam static
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------    -----  ------------------------------------------
3     01-00-5e-0a-0a-0a             3/1-2
Total Matching CAM Entries Displayed = 3
Switch_B (enable)
```

Salida de un grupo con CGMP que tenga activado Fast-Leave

El ejemplo que aparece a continuación requiere que el cliente sea un cliente versión 2 de IGMP y que Fast-Leave esté habilitado en el switch.

1. El siguiente procedimiento habilita el CGMP Fast-Leave. Observe el **show cgmp leave** para determinar si está habilitado. Además, observe el **show cam system** salida de comando para determinar si el switch escucha 01-00-5e-00-00-01 y 01-00-5e-00-00-02 (direcciones utilizadas para la salida).

```
Switch_B (enable) show cgmp leave

CGMP:       enabled
CGMP leave: enabled
Switch_B (enable) show cam sys
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------    -----  -------------------------------------------
1     00-10-2f-00-14-00  #          7/1
1     00-e0-fe-4b-f3-ff  #          1/9
1     01-00-0c-cc-cc-cc  #          1/9
1     01-00-0c-cc-cc-cd  #          1/9
1     01-00-0c-dd-dd-dd  #          1/9
1     01-00-0c-ee-ee-ee  #          1/9
1     01-80-c2-00-00-00  #          1/9
1     01-80-c2-00-00-01  #          1/9
2     00-10-2f-00-14-00  #          7/1
2     01-00-0c-cc-cc-cc  #          1/9
2     01-00-0c-cc-cc-cd  #          1/9
2     01-00-0c-dd-dd-dd  #          1/9
2     01-00-5e-00-00-01  #          1/9
2     01-00-5e-00-00-02  #          1/9
2     01-80-c2-00-00-00  #          1/9
2     01-80-c2-00-00-01  #          1/9
3     01-00-0c-cc-cc-cc  #          1/9
3     01-00-0c-cc-cc-cd  #          1/9
3     01-00-0c-dd-dd-dd  #          1/9
3     01-00-5e-00-00-01  #          1/9
3     01-00-5e-00-00-02  #          1/9
3     01-80-c2-00-00-00  #          1/9
Do you wish to continue y/n [n]?  y
Total Matching CAM Entries Displayed = 22
```

2. El cliente envía un mensaje de ausencia IMPG a 224.0.0.2. El switch lo intercepta y envía una Consulta IGMP en el puerto en el que recibe la ausencia. A continuación se muestra **debug** resultado en el switch:

```
MCAST-IGMP-LEAVE:Recvd leave on port 3/2 vlanNo 3
MCAST-IGMP-LEAVE:router_port_tbl[vlanNo].QueryTime = 0
MCAST-IGMP-LEAVE:deletion_timer = 1
MCAST-SEND:Transmitting IGMP Mac Based GS Query msg on port 3/2 vlanNo 3
MCAST-SEND:  Transmit Succeeded for IGMP Group Specific Query msg on port 3/2 vlanNo 3
```

3. Como no se recibió una respuesta, el Catalyst envía el mensaje de salida de IGMP al router, como se muestra a continuación.

```
MCAST-TIMER:IGMPLeaveTimer expired on port 3/2 vlanNo 3 GDA 01-00-5e-0a-0a-0a
MCAST-TIMER:IGMPLeaveTimer expiry: Transmit IGMP Leave on port 3/1 vlanNo 3
MCAST-SEND:Transmitting IGMP Leave msg on port 3/1 vlanNo 3
MCAST-SEND: Inband Transmit Succeeded for IGMP Leave Message on port 3/1 vlanNo 3
```

4. El router recibe un mensaje IGMP Leave (Ausencia de IGMP), por eso envía un mensaje de

Ausencia de IGMP al switch y también elimina el grupo de la lista de grupos de IGMP. A continuación se muestra el **debug** salida del comando en el router.**En el router**

```
IGMP: Received Leave from 10.200.8.108 (Fa0.3) for 239.10.10.10
IGMP: Send v2 Query on Fa0.3 to 239.10.10.10
IGMP: Send v2 Query on Fa0.3 to 239.10.10.10
CGMP: Sending Leave on Fa0.3
      GDA 0100.5e0a.0a0a, USA 0000.0000.0000
IGMP: Deleting 239.10.10.10 on Fa0.3
```

Seguimientosy Configuración de CGMP

Trama 1

La trama 1 es una trama de Incorporación CGMP a GDA 00-00-00-00-00-00. Se utiliza para agregar el puerto del router a la lista de puertos del router.

```
ISL: ----- ISL Protocol Packet -----
     ISL:
     ISL: Destination Address               = 01000C0000
     ISL: Type                              = 0 (Ethernet)
     ISL: User                              = 0 (Normal)
     ISL: Source Address                    = 8C958B7B1000
     ISL: Length                            = 76
     ISL: Constant value                    = 0xAAAA03
     ISL: Vendor ID                         = 0x8C958B
     ISL: Virtual LAN ID (VLAN)             = 2
     ISL: Bridge Protocol Data Unit (BPDU)  = 0
     ISL: Port Index                        = 193
     ISL: Reserved
     ISL:
ETHER: ----- Ethernet Header -----
     ETHER:
     ETHER: Destination = Multicast 01000CDDDDDD
!--- Send to the CGMP !--- macaddress present in show cam sys !--- command output.

     ETHER: Source      = Station Cisco11411E1
     ETHER: 802.3 length = 24
     ETHER:
LLC:  ----- LLC Header -----
     LLC:
     LLC:  DSAP Address = AA, DSAP IG Bit = 00 (Individual Address)
     LLC:  SSAP Address = AA, SSAP CR Bit = 00 (Command)
     LLC:  Unnumbered frame: UI
     LLC:
SNAP: ----- SNAP Header -----
     SNAP:
     SNAP: Vendor ID = Cisco1
     SNAP: Type = 2001 (CGMP)
     SNAP:
CGMP: ----- CGMP -----
     CGMP:
     CGMP: Version   = 16
     CGMP: Type      = 0 (Join)
     CGMP: Reserved
     CGMP: Count     = 1
     CGMP:
     CGMP: Group Destination Address and Unicast Source Address
```

```
     CGMP:
     CGMP:    GDA    =0000.0000.0000
     CGMP:    USA    =0000.0C14.11E1
!--- MAC address of the router. CGMP:
```

El resultado de la trama 1 está en el switch y el puerto conectado al router es 3/1:

Trama 2

La trama 2 es un informe de afiliación IGMP enviado por el host para solicitar (o confirmar) si los usuarios desean recibir el tráfico para el grupo 239.10.10.10.

```
ISL: ----- ISL Protocol Packet -----
     ISL:
     ISL: Destination Address               = 01000C0000
     ISL: Type                              = 0 (Ethernet)
     ISL: User                              = 0 (Normal)
     ISL: Source Address                    = 8C958B7B1000
     ISL: Length                            = 76
     ISL: Constant value                    = 0xAAAA03
     ISL: Vendor ID                         = 0x8C958B
     ISL: Virtual LAN ID (VLAN)             = 2
     ISL: Bridge Protocol Data Unit (BPDU)  = 0
     ISL: Port Index                        = 195
     ISL: Reserved
     ISL:
ETHER: ----- Ethernet Header -----
     ETHER:
     ETHER: Destination = Multicast 01005E0A0A0A
!--- Destination is the GDA MAC. ETHER: Source = Station Cisco176DCCA !--- Sourced by the PC
connected in 3/1. ETHER: Ethertype = 0800 (IP) ETHER: IP: ----- IP Header ----- IP: IP: Version
= 4, header length = 20 bytes IP: Type of service = C0 IP: 110. .... = internetwork control IP:
...0 .... = normal delay IP: .... 0... = normal throughput IP: .... .0.. = normal reliability
IP: Total length = 28 bytes IP: Identification = 0 IP: Flags = 0X IP: .0.. .... = may fragment
IP: ..0. .... = last fragment IP: Fragment offset = 0 bytes IP: Time to live = 1 seconds/hops
IP: Protocol = 2 (IGMP) IP: Header checksum = CC09 (correct) IP: Source address = [10.1.1.2] IP:
Destination address = [224.10.10.10] IP: No options IP: IGMP: ----- IGMP header ----- IGMP:
IGMP: Version = 1 IGMP: Type = 6 (Ver2 Membership Report) IGMP: Unused = 0x00 IGMP: Checksum =
FFEA (correct) IGMP: Group Address = [224.10.10.10] IGMP:
```

Trama 3

La trama 3 es la trama CGMP enviada por el router al switch para informarle al switch que debe agregar una entrada estática para 01-00-5e-0a-0a-0a.

```
ISL: ----- ISL Protocol Packet -----
     ISL:
     ISL: Destination Address               = 01000C0000
     ISL: Type                              = 0 (Ethernet)
     ISL: User                              = 0 (Normal)
     ISL: Source Address                    = 8C958B7B1000
     ISL: Length                            = 76
     ISL: Constant value                    = 0xAAAA03
     ISL: Vendor ID                         = 0x8C958B
     ISL: Virtual LAN ID (VLAN)             = 2
     ISL: Bridge Protocol Data Unit (BPDU)  = 0
     ISL: Port Index                        = 193
     ISL: Reserved
     ISL:
ETHER: ----- Ethernet Header -----
     ETHER:
```

```
     ETHER: Destination = Multicast 01000CDDDDDD
     ETHER: Source      = Station Cisco11411E1
     ETHER: 802.3 length = 24
     ETHER:
LLC:  ----- LLC Header -----
     LLC:
     LLC:  DSAP Address = AA, DSAP IG Bit = 00 (Individual Address)
     LLC:  SSAP Address = AA, SSAP CR Bit = 00 (Command)
     LLC:  Unnumbered frame: UI
     LLC:
SNAP: ----- SNAP Header -----
     SNAP:
     SNAP: Vendor ID = Cisco1
     SNAP: Type = 2001 (CGMP)
     SNAP:
CGMP: ----- CGMP -----
     CGMP:
     CGMP: Version   = 16
     CGMP: Type      = 0 (Join)
     CGMP: Reserved
     CGMP: Count     = 1
     CGMP:
     CGMP: Group Destination Address and Unicast Source Address
     CGMP:
     CGMP:    GDA    =0100.5E0A.0A0A
!--- GDA MAC added in show cam static !--- command output.

     CGMP:    USA    =0000.0C76.DCCA
!--- MAC of the PC in 3/1. CGMP:
```

A continuación aparece la configuración del router y del switch.

```
 Router_A (router) Configuration:

 Router_A#write terminal
 Building configuration...

 Current configuration:
 !
 version 12.0
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname Router_A
 !
 !
 ip subnet-zero
 ip multicast-routing
 ip dvmrp route-limit 20000


 interface FastEthernet0
  no ip address
  no ip directed-broadcast
 !
 interface FastEthernet0.1
  encapsulation isl 1
  ip address 10.1.1.1 255.255.255.0
  no ip redirects
  no ip directed-broadcast
 !
 interface FastEthernet0.2
```

```
 encapsulation isl 2
 ip address 10.2.2.1 255.255.255.0
 no ip redirects
 no ip directed-broadcast
 ip pim dense-mode
 ip cgmp
!
interface FastEthernet0.3
 encapsulation isl 3
 ip address 10.3.3.1 255.255.255.0
 no ip redirects
 no ip directed-broadcast
 ip pim dense-mode
 ip cgmp
!
```

```
Switch_B configuration for CGMP:

#cgmp
set cgmp enable
set cgmp leave enable
!

CGMP statistics for VLAN 3:

Switch_B (enable) show cgmp sta 3
CGMP enabled

CGMP statistics for vlan 3:
valid rx pkts received           109
invalid rx pkts received         0
valid cgmp joins received        108
valid cgmp leaves received       1
valid igmp leaves received       1
valid igmp queries received      63
igmp gs queries transmitted      1
igmp leaves transmitted          1
failures to add GDA to EARL      0
topology notifications received  0
Switch_B (enable)
```

IGMP Snooping

IGMP Snooping es otra función que le permite capturar directamente las tramas IGMP. Para obtener soporte de indagación IGMP en switches Catalyst, consulte la Matriz de soporte de switch Catalyst multidifusión.

Resumen de la Función Indagación IGMP

La función IGMP snooping, como el nombre lo indica, es una función que le permite al switch “escuchar” la conversación IGMP entre los hosts y los routers. Cuando un switch escucha un informe IGMP de un host para un grupo multicast dado, el switch agrega el número del puerto del host a la lista GDA para ese grupo. Y, cuando el switch escucha una IGMP Leave, quita el puerto del host de la entrada de tabla CAM.

Aprendizaje del Puerto del Router

El switch escucha los siguientes mensajes para detectar los puertos del router con la función IGMP snooping:

- Consulta sobre afiliación IGMP enviar a 01-00-5e-00-00-01
- PIMv1 hello send to 01-00-5e-00-00-02
- PIMv2 hello send to 01-00-5e-00-00-0d
- Sondas DVMRP enviar a 01-00-5e-00-04
- Mensaje MOSPF enviado a 01-00-5e-00-05 ó 06

Al habilitar la indagación IGMP en un switch, todas las entradas MAC anteriores se agregan al **show cam system** salida del comando del switch de snooping. Una vez que se detecta un puerto del router, se agrega a la lista de puertos de todos los GDA en ese VLAN.

Asociación de un grupo a IGMP Snooping

Éstos son dos escenarios de unión:

Escenario A: El host A es el primer host en unirse a un grupo del segmento.

1. El host A envía un informe de afiliación de IGMP no solicitado.
2. El switch intercepta el informe de membresía IGMP enviado por el host que deseaba unirse al grupo.
3. El switch crea una entrada multicast para ese grupo y la conecta al puerto del cual ha recibido el informe y a todos los puertos de los routers.
4. El switch reenvía el informe IGMP a todos los puertos del router. De esta manera, el router también reciba el informe IGMP, y actualice su tabla de ruteo multidifusión en consecuencia.

Situación B: Ahora el host B es el segundo host en unirse al mismo grupo.

1. El host B envía un informe de afiliación de IGMP no solicitado.
2. El switch intercepta el informe de afiliación IGMP enviado por el host que desea unirse al grupo.
3. El switch no reenvía necesariamente el informe IGMP a todos los puertos del router. De hecho, el switch reenvía los informes IGMP a los puertos del router con el informe proxy, y solamente reenvía informe por grupo dentro de los 10 segundos.

   Nota: Para mantener la afiliación del grupo, el router multicast envía una consulta IGMP cada 60 segundos. El switch intercepta esta consulta y la envía a todos sus puertos. Todos los hosts que son miembros de la respuesta del grupo que consulta. Pero, dado que el switch también intercepta el informe de respuesta, el otro host no ve cada uno de los otros informes y, por lo tanto, todos los hosts envían un informe (en lugar de uno por grupo). Entonces, el switch también utiliza un Informe Proxy para reenviar sólo un informe por grupo de todas las respuestas recibidas.

Suponga que el host A desea salir del grupo, pero el host B todavía desea recibir el grupo.

- Este switch captura el mensaje de ausencia de IGMP del host A.
- El switch emite una consulta IGMP específica de grupo para el grupo de ese puerto (exclusiva para ese puerto).
- SI el switch no recibe un informe, descarta este puerto desde la entrada. Si recibe una respuesta de ese puerto, no hace nada y descarta el abandono.

- El host B todavía está interesado por ese grupo en ese switch. Esto no sería el último puerto que no es de router en la entrada. Por lo tanto, el switch no reenvía el mensaje de ausencia.

Ahora, suponga que el Host B quiere salir del grupo y que es el último usuario interesado para este grupo en este segmento.

- Este switch captura el mensaje de ausencia de IGMP del host A.
- El switch emite una consulta de IGMP específica para ese grupo en ese puerto.
- Si el switch no recibe un informe, desecha este puerto de la entrada.
- Este es el último puerto que no es de router para esa GDA. El switch reenvía el mensaje de ausencia de IGMP a todos los puertos del router y quita la entrada de su tabla.

Interacción entre IGMP y CGMP

En algunas redes, debido a las limitaciones del hardware, posiblemente no pueda ejecutar IGMP Snooping en todos los switches. En este caso, es probable que necesite ejecutar CGMP en algunos switches en la misma red.

Tenga en cuenta que éste es un caso especial. El switch que ejecuta la indagación de IGMP detecta mensajes CGMP y que algunos switches en la red están ejecutando CGMP. Por lo tanto, se traslada a un modo IGMP-CGMP especial y desactiva la generación de informes de proxy. Esto es absolutamente necesario para la operación correcta del CGMP, porque los routers utilizan la dirección MAC de origen del informe IGMP para crear una Incorporación CGMP. Los routers que ejecutan CGMP necesitan ver todos los informes de IGMP Cualquier informe que se envíe al router debe ser totalmente necesario para la indagación de IGMP.

Red de Origen Solamente Multicast

Si el segmento contiene sólo un servidor multicast (fuente multicast) y no posee ningún cliente, podría darse una situación en la que no tenga paquetes IGMP en ese segmento, pero sí tenga mucho tráfico multicast. En este caso, el switch simplemente reenvía el tráfico de ese grupo a todos en el segmento. Afortunadamente, un switch que está ejecutando una indagación IGMP puede detectar estas secuencias de multidifusión y agrega un ingreso de multidifusión a ese grupo simplemente con el puerto del router. Estas entradas están marcadas internamente como mcast_source_only y caducan cada 5 minutos o bien cuando el puerto del router desaparece. Observe que hasta después de esta desactualización, la dirección es aprendida nuevamente en pocos segundos si el tráfico continúa. Durante el período de reaprendizaje, puede producirse una inundación momentánea en la VLAN. Para evitar esto y conservar las entradas, utilice el **set igmp flooding enable | disable** comando. Después de que se inhabilita la inundación, el switch no cierra las entradas de origen solamente.

Limitaciones

Al igual que CGMP, las GDA que mapean a una MAC fuera del rango 01-00-5e-00-00-xx nunca son separadas por indagación de IGMP.

Configuración de Indagación de IGMP en Cisco Switches

Para habilitar/inhabilitar la indagación de IGMP, ejecute el siguiente comando:

- **set igmp**

Para configurar el router multicast (estático) emita el siguiente comando:

- **set multicast router**
- **clear multicast router *port* | *all>***

Para supervisar y verificar las estadísticas de IGMP, ejecute los siguientes comandos:

- **show igmp statistics**
- **show multicast router**

Ejemplo Práctico de Indagación de IGMP

La configuración para este ejemplo es similar a la prueba CGMP que se utilizó antes en este documento. La única diferencia es que los puertos 3/2 y 3/3 están conectados a la misma VLAN y que ambos están configurados como clientes para unirse al grupo 224.10.10.10.

El siguiente ejemplo explica varias manipulaciones, analiza lo que hace el switch y examina la salida resultante. En el siguiente ejemplo, *Switch_B es un Catalyst 5500 que ejecuta IGMP Snooping, y Router_A es el router multicast conectado con el puerto 3/1.*

1. Habilite la indagación IGMP en el switch y vea el resultado mediante la ejecución del **debug** comando. Observe que cada conjunto de entradas se ha agregado al **show cam sys** salida del comando, que permite la detección del puerto del router a través de PIM, MOSPF, etc.

```
Switch_B (enable)  set igmp en

MCAST-IGMP: Set Sys Entries
MCAST-SYS-ENTRIES: Add system Entries in vlan 1
MCAST-IGMP: Set Sys Entries
MCAST-SYS-ENTRIES: Add system Entries in vlan 2
MCAST-IGMP: Set Sys Entries
MCAST-SYS-ENTRIES: Add system Entries in vlan 3

IGMP feature for IP multicast enabled

Switch_B (enable) show cam sys
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------ -----  -------------------------------------------
1     00-10-2f-00-14-00  #          7/1
1     00-e0-fe-4b-f3-ff  #          1/9
1     01-00-0c-cc-cc-cc  #          1/9
1     01-00-0c-cc-cc-cd  #          1/9
1     01-00-0c-dd-dd-dd  #          1/9
1     01-00-0c-ee-ee-ee  #          1/9
1     01-00-5e-00-00-01  #          1/9
1     01-00-5e-00-00-04  #          1/9
1     01-00-5e-00-00-05  #          1/9
1     01-00-5e-00-00-06  #          1/9
1     01-00-5e-00-00-0d  #          1/9
1     01-80-c2-00-00-00  #          1/9
1     01-80-c2-00-00-01  #          1/9
2     00-10-2f-00-14-00  #          7/1
2     01-00-0c-cc-cc-cc  #          1/9
2     01-00-0c-cc-cc-cd  #          1/9
2     01-00-0c-dd-dd-dd  #          1/9
2     01-00-5e-00-00-01  #          1/9
2     01-00-5e-00-00-04  #          1/9
2     01-00-5e-00-00-05  #          1/9
```

```
2     01-00-5e-00-00-06  #          1/9
2     01-00-5e-00-00-0d  #          1/9
```

2. El switch recibe un paquete de PIMv2 del router Router_A y agrega el puerto del router.

```
MCAST-IGMPQ:recvd a PIM V2 packet of type HELLO on the port 3/1 vlanNo 2
MCAST-ROUTER: Adding port 3/1, vlanNo 2
MCAST-ROUTER: Creating RouterPortTimer for  port 3/1, vlanNo 2
MCAST-IGMPQ:recvd a PIM V2 packet of type HELLO on the port 3/1 vlanNo 3
MCAST-ROUTER: Adding port 3/1, vlanNo 3
MCAST-ROUTER: Creating RouterPortTimer for  port 3/1, vlanNo 3

Switch_B (enable) show multi router
CGMP disabled
IGMP enabled

Port       Vlan
---------  ----------------
 3/1       2-3

Total Number of Entries = 1
'*' - Configured
Switch_B (enable)
```

3. Conecte un nuevo host en el grupo 224.10.10.10 (en el puerto 3/2). Este host envía un informe de afiliación IGMP. Se recibe el informe, buscado por el switch, se agrega la entrada y se reenvía el informe IGMP al router.**En Switch_B**

```
MCAST-IGMPQ:recvd an IGMP V2 Report on the port 3/2 vlanNo 3
      GDA 224.10.10.10
MCAST-RELAY:Relaying packet on port 3/1 vlanNo 3
MCAST-SEND: Inband Transmit Succeeded for IGMP RELAY msg on port 3/1
      vlanNo 3

Switch_B (enable) show cam static
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN  Dest MAC/Route Des [CoS] Destination Ports or VCs / [Protocol Type]
----  ------------------ ----- -------------------------------------------
3     01-00-5e-0a-0a-0a         3/1-2
```

4. Agregue un usuario más en VLAN 3 en el puerto 3/3, tal como se muestra a continuación.

```
Switch_B (enable) show cam static

  * = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.

  X = Port Security Entry

  VLAN Dest MAC/Route Des [CoS] Destination Ports or VCs / [Protocol Type]
  ---- ------------------ ----- -------------------------------------------
  3    01-00-5e-0a-0a-0a         3/1-3
```

5. Quite el puerto 3/2. El puerto 3/2 envía un mensaje de ausencia de IGMP; el switch devuelve una consulta específica de grupo IGMP en el puerto 3/2 e inicia el temporizador. Cuando caduca el temporizador sin recibir respuesta, borra el puerto del grupo.

```
MCAST-IGMPQ:recvd an IGMP Leave on the port 3/2 vlanNo 3 GDA 224.10.10.10
MCAST-IGMPQ-LEAVE:router_port_tbl[vlanNo].QueryTime = 0
```

```
MCAST-DEL-TIMER: Deletion Timer Value set to Random Value  1
MCAST-SEND:Transmitting IGMP Mac Based GS Query msg on port 3/2 vlanNo 3
MCAST-SEND:  Transmit Succeeded for IGMP Group Specific Query msg on port 3/2 vlanNo 3
MCAST-TIMER:IGMPLeaveTimer expired on port 3/2 vlanNo 3 GDA 01-00-5e-0a-0a-0a
MCAST-TIMER:IGMPLeaveTimer:delete leave timer


Switch_B (enable) show cam static
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry

VLAN Dest MAC/Route Des [CoS] Destination Ports or VCs / [Protocol Type]
---- ------------------ ----- -------------------------------------------
3    01-00-5e-0a-0a-0a         3/1,3/3
```

6. El host en puerto 3/3 sale del grupo y envía un mensaje de Ausencia de IGMP. La única diferencia con el punto anterior es que el mensaje de ausencia de IGMP finalmente se reenvía al puerto del router.

```
MCAST-IGMPQ:recvd an IGMP Leave on the port 3/3 vlanNo 3 GDA 224.10.10.10
MCAST-SEND:Transmitting IGMP Mac Based GS Query msg on port 3/3 vlanNo 3
MCAST-SEND:  Transmit Succeeded for IGMP Group Specific Query msg on
             port 3/3 vlanNo 3
MCAST-TIMER:IGMPLeaveTimer expired on port 3/3 vlanNo 3 GDA
             01-00-5e-0a-0a-0a
MCAST-TIMER:IGMPLeaveTimer expiry: Transmit IGMP Leave on port 3/1
             vlanNo 3
MCAST-SEND:Transmitting IGMP Leave msg on port 3/1 vlanNo 3
MCAST-SEND: Inband Transmit Succeeded for IGMP Leave Message on port 3/1
             vlanNo 3
MCAST-TIMER:IGMPLeaveTimer:delete leave timer
```

La configuración de subred volvió al principio, su estado se encuentra en el Paso 1. La entrada de multidifusión ha desaparecido de la **show cam static** resultado del comando.

Para finalizar, vea un ejemplo de **show igmp static** resultado del comando, como se muestra a continuación.

```
Switch_B (enable) show igmp stat 2
IGMP enabled

IGMP statistics for vlan 2:
Total valid pkts rcvd:           329
Total invalid pkts recvd         0
General Queries recvd            82
Group Specific Queries recvd     0
MAC-Based General Queries recvd  0
Leaves recvd                     0
Reports recvd                    82
Queries  Xmitted                 0
GS Queries Xmitted               0
Reports Xmitted                  0
Leaves Xmitted                   0
Failures to add GDA to EARL      0
Topology Notifications rcvd      0

Switch_B (enable) show igmp stat 3
IGMP enabled
```

```
IGMP statistics for vlan 3:
Total valid pkts rcvd:           360
Total invalid pkts recvd         0
General Queries recvd            93
Group Specific Queries recvd     6
MAC-Based General Queries recvd  0
Leaves recvd                     11
Reports recvd                    64
Queries  Xmitted                 0
GS Queries Xmitted               14
Reports Xmitted                  0
Leaves Xmitted                   10
Failures to add GDA to EARL      0
Topology Notifications rcvd      1
Switch_B (enable)
```

Información Relacionada

- Matriz de Soporte de Switches de Catalyst Multicast
- Página de soporte de multidifusión IP
- Soporte de tecnología de Cisco
- Soporte de producto de Cisco
- Soporte Técnico y Documentación - Cisco Systems