

Uso de RGMP: Fundamentos y Casos Prácticos

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[RGMP reduce la carga en la red](#)

[RGMP en detalle](#)

[Causas que hacen que el router envíe paquetes RGMP](#)

[Qué sucede cuando un switch recibe paquetes RGMP](#)

[Configuración y verificación de RGMP](#)

[RGMP en el software del sistema corriente del Cisco IOS del Catalyst 6000](#)

[Caso Práctico](#)

[Habilitación de RGMP en el Switch](#)

[Activación de RGMP en los routers](#)

[Funcionamiento de RGMP en la VLAN 2](#)

[RGMP se incorpora a la operación en VLAN 3](#)

[Operación de abandono de RGMP](#)

[Operación RGMP Bye](#)

[Información Relacionada](#)

Introducción

El Protocolo de administración de grupo de puertos y routers (RGMP) se utiliza con indagaciones IGMP para restringir el tráfico de multidifusión a las capas en las que realmente se necesita. El sondeo IGMP envía el tráfico multicast a todos los puertos del router. Con RGMP, el tráfico Multicast sólo se envía a los puertos que necesitan recibirlo. El RGMP se diseñó para que se ejecutara en la estructura básica de la red multicast; conocimiento básico de la multidifusión (IGMP, PIM, ruteo de multidifusión) es útil para comprender este documento.

Observe que ahora existe una nueva función que substituye el RGMP y es más scalable. Esta característica se llama snooping de la multidifusión independiente de protocolo (PIM) y realiza la misma meta que el RGMP. El snooping PIM está fuera del ámbito de este documento.

Para más información, refiera a [configurar el snooping PIM](#).

prerrequisitos

Requisitos

Los Quien lea este documento deben ser conscientes de estas limitaciones del protocolo:

- Debe ejecutar RGMP en los routers y los switches.
- Usted necesita habilitar el IGMP Snooping en el Switches.
- El RGMP trabajará solamente para los grupos configurados con el modo disperso de PIM.
- No se admiten las fuentes que envían tráfico Multicast que está conectado directamente a un switch RGMP.
- No se admite la conexión de varios routers en el mismo puerto del switch (por ejemplo, dos routers en el mismo eje de conexión).
- No se admite la conexión de routers múltiples al mismo switch no RGMP.
- El RGMP permite solamente que usted restrinja el tráfico hacia directamente un router conectado o hacia un router conectado siendo un Switch capaz NON-RGMP. El RGMP no es capaz de restringir el tráfico a un router de multidifusión conectado detrás de otro Switch capaz RGMP.

El error seguir estas restricciones puede dar lugar a las roturas en la Conectividad del Multicast.

Componentes Utilizados

RGMP es un protocolo que funciona entre los switches y routers Catalyst, los cuales deben ser compatibles con RGMP a fin de que la característica funcione. El siguiente switch soporta RGMP:

- Catalyst 6000: desde la versión de software 5.4
- Software del sistema de Cisco IOS® del Catalyst que se ejecuta 6000: desde el software 12.1(3a)E3
- Catalyst 5000: desde la versión de software 5.4

El RGMP se soporta en las versiones siguientes del Cisco IOS Router Software:

- 12.3 Mainline
- 12.3T
- Línea principal 12.2
- 12.2.S
- 12.2T
- 12.1E
- 12.1T (comenzando con la versión 12.1(5)T1)
- 12.0S (a partir de la versión 12.0(10)S)
- 12.0O (empezando por la versión 12.0(11)ST)

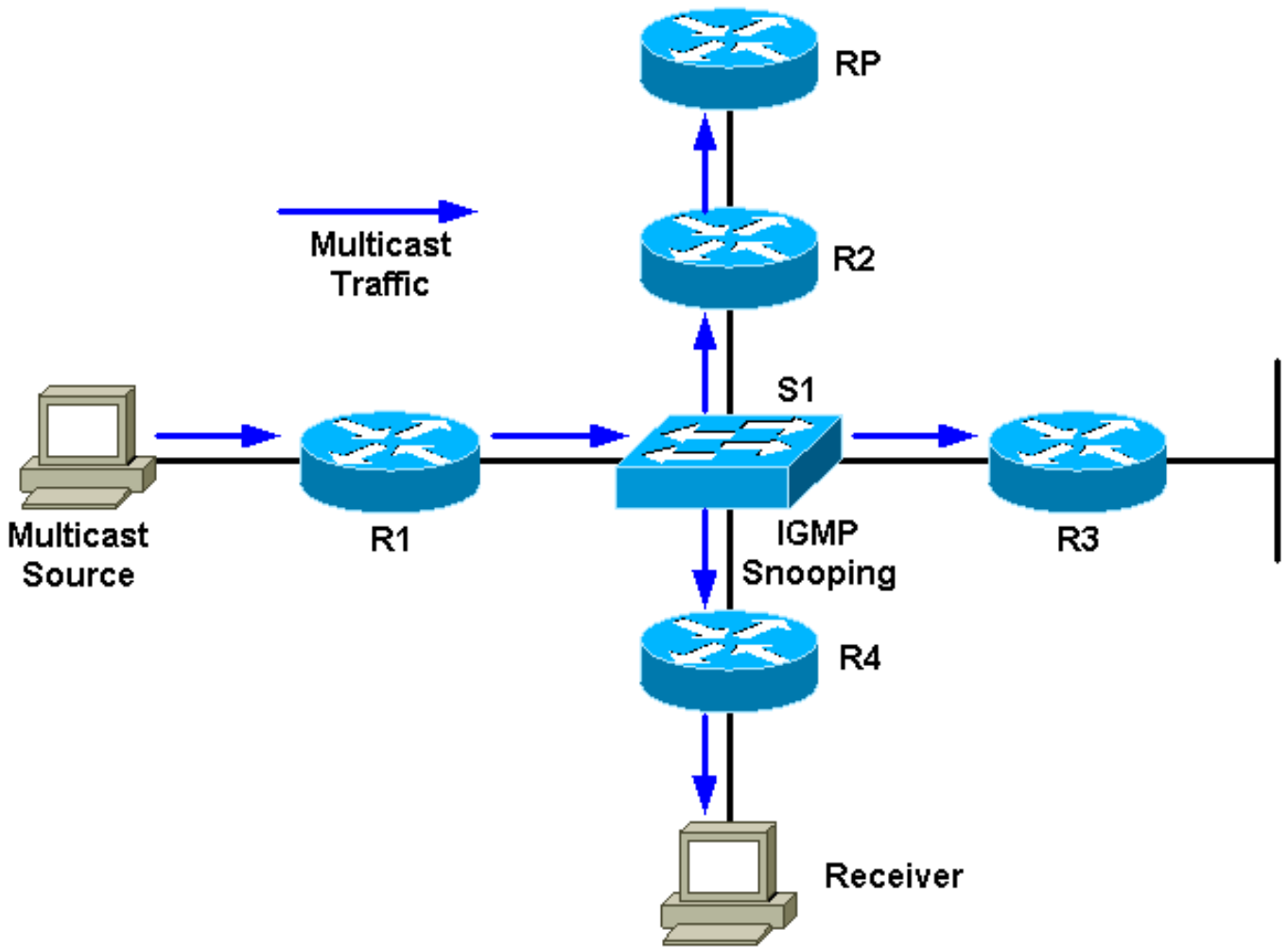
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte las [Convenciones de Consejos Técnicos de Cisco](#).

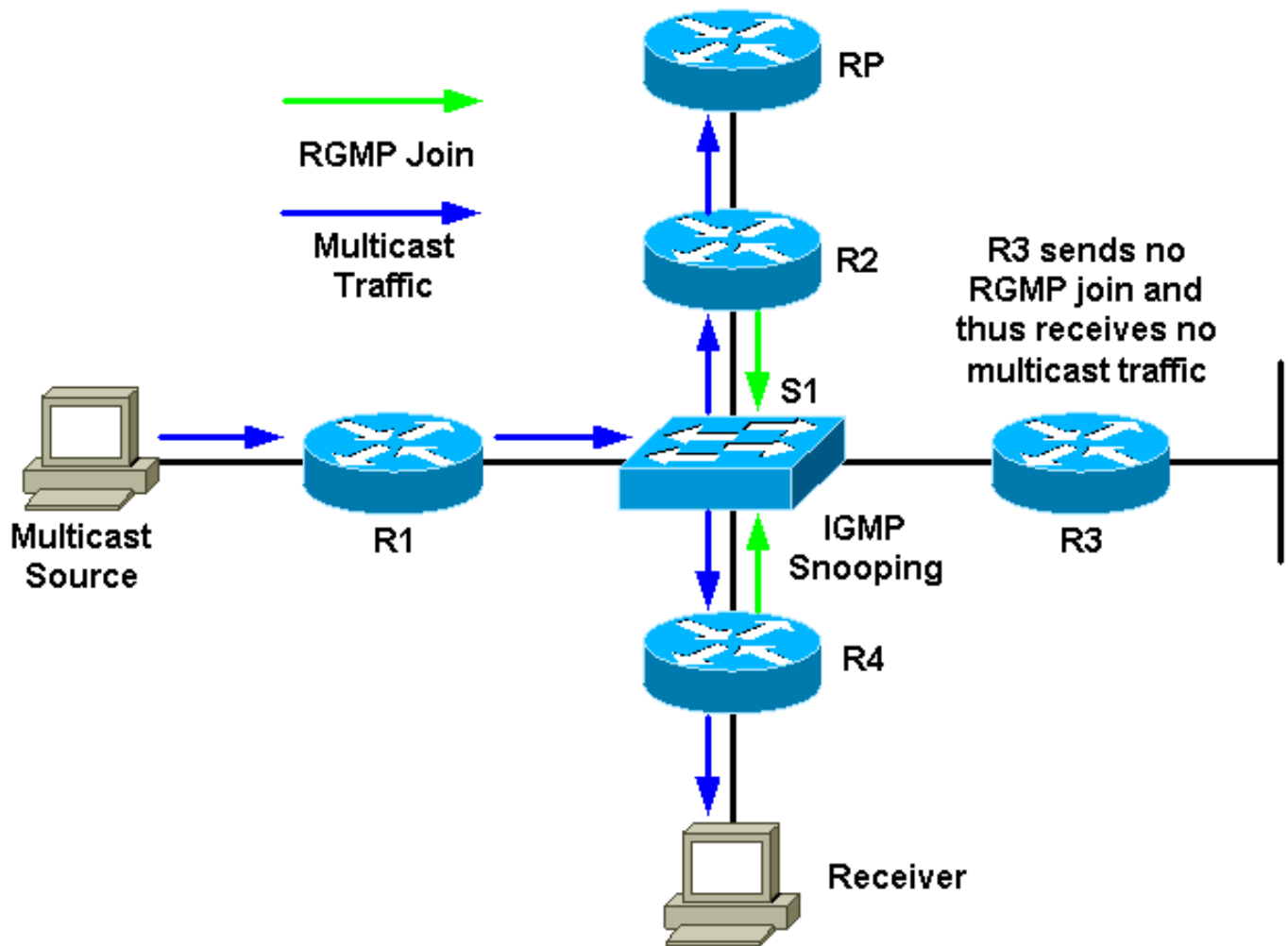
RGMP reduce la carga en la red

El propósito del RGMP es eliminar el tráfico multidifusión innecesario. Este diagrama muestra una red hipotética sin el RGMP habilitado:



Hay un origen de multidifusión conectado con el r1 y un receptor conectados con el R4. El RP para el grupo está detrás del R2. El tráfico es reenviado por R1 al switch (por PIM y por tabla mruta, ya que hay un receptor detrás de la interfaz del switch). El Switch detectará este red de origen solamente con el IGMP Snooping y creará una entrada estática de memoria direccionable por contenido (CAM) que señala a todo el Routers: R1, r2, R3, y R4. El tráfico de multidifusión será enviado a todos los routers, incluso a R3, que no necesita el tráfico. Si el tráfico de multidifusión es de gran volumen, puede crearle una carga innecesaria al router R3. Se creó RGMP para solucionar este problema.

Este diagrama muestra la misma red con el RGMP habilitado (si se asume que el Routers y el Switch son RGMP capaces):



R2 y R4 enviarán una unión RGMP para ese grupo multidifusión hacia el switch. R3 no enviará una incorporación RGMP. Como resultado, el switch sólo reenviará el tráfico de multidifusión recibido de R1 para ese grupo a R2 y R4 y no a R3. Esto reduce el tráfico en la red.

RGMP en detalle

El RGMP es, como el CGMP, un protocolo que se ejecuta entre un router y un Switch. Los routers envían paquetes RGMP y los switches escuchan los paquetes RGMP. Los switches nunca envían paquetes RGMP, y los routers ignoran todos los paquetes RGMP que reciben. Los paquetes RGMP son paquetes IP de tipo IGMP y se envían a la dirección de grupo reservada 224.0.0.25 (dirección MAC 01-00-5e-00-00-19). Como paquetes IGMP, se envían con un Time to Live (TTL) de 1. El direccionamiento 224.0.0.25 es una dirección reservada correspondiente a todas las direcciones Multicast del Switch. Un paquete RGMP contiene básicamente un campo Tipo, un campo de grupo de direcciones y una suma de comprobación.

Esta tabla muestra los diversos campos del tipo disponibles para los paquetes RGMP:

Descripción	Acción
Hello	Cuando RGMP está activado en el router, no se envía tráfico de datos multidifusión hacia el router por medio del switch salvo que se envíe una unión RGMP específicamente al grupo.
Adiós	Cuando se desactiva RGMP en el router, el

	switch le envía todo el tráfico de datos multidifusión.
Incorporarse	El tráfico de datos de multidifusión para una dirección MAC de multidifusión desde la dirección de grupo G de Capa 3 se envía al router. Estos paquetes tienen el grupo G en el campo de dirección de grupo del paquete RGMP.
Salir	El tráfico de datos multidifusión para el grupo G no es enviado al router. Estos paquetes tienen el grupo G en el campo de dirección de grupo del paquete RGMP.

Los paquetes de saludo (hello y bye) utilizan 0.0.0.0 como la dirección de grupo en el paquete RGMP. Los paquetes Join (Unirse) y Leave (Irse) utilizan la dirección del grupo que le interesa al router (para unirse o irse).

Los paquetes RGMP usan los siguientes tipos de direcciones:

Tipo de dirección	Dirección utilizada
Dirección MAC de destino de todos los paquetes RGMP	01-00-5e-00-00-19
IP Address de destino de todos los paquetes RGMP	224.0.0.25
Grupo de dirección usado en los Hello (saludo) RGMP y el adiós	0.0.0.0
Grupo de direcciones usadas en RGMP Join y Leave	El grupo multidifusión para el que se envía la incorporación o la salida

[Causas que hacen que el router envíe paquetes RGMP](#)

Hello (saludo) RGMP

Siempre que el RGMP se habilite en el router, el router envía un mensaje de los Hello (saludo) RGMP al Switch que indica que el Switch no debe remitir el tráfico de datos de multidifusión a este router a menos que un RGMP Join se envíe específicamente para un grupo. Observe también que el PIM esté configurado en el router para que funcione esta característica. Controle la Herramienta Localizador MIB para asegurarse de que CISCO-BULK-FILE-MIB está soportado por su dispositivo. Los mensajes de saludo de RGMP siempre preceden los mensajes de saludo de PIM.

Adiós RGMP

Siempre que el RGMP se inhabilite en el router, envía un Mensaje de despedida de RGMP para indicar al Switch que el router está haciendo no más el RGMP y que todo el tráfico Multicast se debe remitir otra vez a este router.

El RGMP se une a

Siempre que un router envíe un PIM se una a, también construye un RGMP se una a y lo envía hacia fuera en la misma interfaz en la cual el PIM Join debe ser enviado. Usando los diagramas anteriores como un ejemplo, el R4 envía un mensaje de incorporación PIM al RP cuando recibe un informe IGMP del receptor para el grupo G. También envía una unión RGMP en la misma interfaz, que es capturada por el switch S1. El s1 procesa el paquete y agrega ese puerto de router a la entrada estática de la capa 2 (entrada de CAM estática) para el grupo G. Esto permite reenviar tráfico al grupo G de este puerto.

Para resumir:

- Se envía un RGMP Join cada vez que un router crea una entrada (*,G) y se envía en la misma interfaz en que envía un mensaje PIM Join.
- El mensaje de incorporación RGMP se envía siempre que un router crea una entrada (S,G). El router enviará un mensaje de incorporación PIM en la interfaz hacia S y por lo tanto Incorporación RGMP también se envía en la misma interfaz hacia S.
- El mensaje de incorporación RGMP se envía cada vez que se envía un mensaje de incorporación PIM, pero no cuando este último se recibe.
- Si existen varias fuentes que transmiten hacia el grupo G y una entrada (*,G), sólo se emitirá un RGMP Join.

Ausencia de rgmp

Siempre que un router envíe un mensaje de separación de PIM para a (*, G) o (S, G), también marca para ver si hay por lo menos otra entrada mroute para este grupo para la interfaz en la cual la pasa PIM fue enviada. Si no hay otra entrada, ausencia de rgmp se envía en la misma interfaz.

[Qué sucede cuando un switch recibe paquetes RGMP](#)

Con RGMP deshabilitado y la indagación IGMP habilitada en el switch, cada entrada de reenvío de grupo multidifusión tiene una lista de puertos de salida que incluye todos los puertos de router multidifusión además de todos los puertos en los que se incorporan hosts interesados al grupo multidifusión. Cuando RGMP está habilitado, cambia lo siguiente:

- El Switches no envía a cualquier grupo de multidifusión a un router habilitado para RGMP a menos que el router lo pida específicamente (a excepción del grupo reservado en el rango 224.0.0.x y para 224.0.1.[39-40]).
- Los switches aún envían tráfico de multidifusión desde todos los grupos a los routers no compatibles con RGMP.

Hello (saludo) RGMP

Cuando un paquete de los Hello (saludo) RGMP se recibe de un puerto de router, el Switch marca este puerto de router como RGMP capaz, y el tráfico de la multidifusión general se envía no más a ese puerto de router de multidifusión.

Nota: Los paquetes de los Hello (saludo) RGMP no se remiten generalmente el chasis de los. Los paquetes de los Hello (saludo) RGMP se remiten solamente hacia fuera una vez que el primer

Hello (saludo) RGMP se recibe en un puerto que el puerto entonces se marca como puerto RGMP y el paquete de saludo se remite encendido a otro puerto de router de multidifusión RGMP capaz.

Adiós RGMP

En el recibo del adiós RGMP, el unmark el puerto de router como puerto del router RGMP y agrega este puerto en todo el grupo existente en ese VLA N.

El RGMP se une a

Al recibirse un paquete RGMP Join para un grupo determinado, el switch agrega el puerto del router desde el cual se recibió el RGMP Join en la lista de puertos de destino para ese grupo. Las uniones RGMP también se reenvían a todos los puertos del router compatibles con RGMP.

Ausencia de rgmp

Cuando un paquete RGMP Leave es recibido para un grupo específico, el switch elimina el puerto del router desde el grupo de puertos interesado en recibir ese grupo.

Configuración y verificación de RGMP

Para habilitar el RGMP en un Switch:

```
#set igmp enable
!--- If this has not been done previously. #set rgmp enable
```

Usted puede verificar la configuración tecleando:

```
#sh rgmp group
#sh multi router
#sh rgmp stat
#sh multi group
```

Para configurar RGMP en un router:

```
#ip rgmp
!--- In interface mode.
```

y, si no hecho previamente:

```
#ip multicast-routing
!--- In global configuration mode. #ip pim sparse-mode
!--- In interface mode.
```

RGMP en el software del sistema corriente del Cisco IOS del Catalyst 6000

El RGMP en el software del sistema corriente del Cisco IOS del Catalyst 6000 tiene estas características:

- Habilitado por abandono en todo el puerto L2 (switchport) y no puede ser inhabilitado
- Las necesidades de ser permisos en cualquier Multicast L3 viran hacia el lado de babor si la interfaz del Multicast L3 es necesaria actuar como el router RGMP; esto es hecha publicando

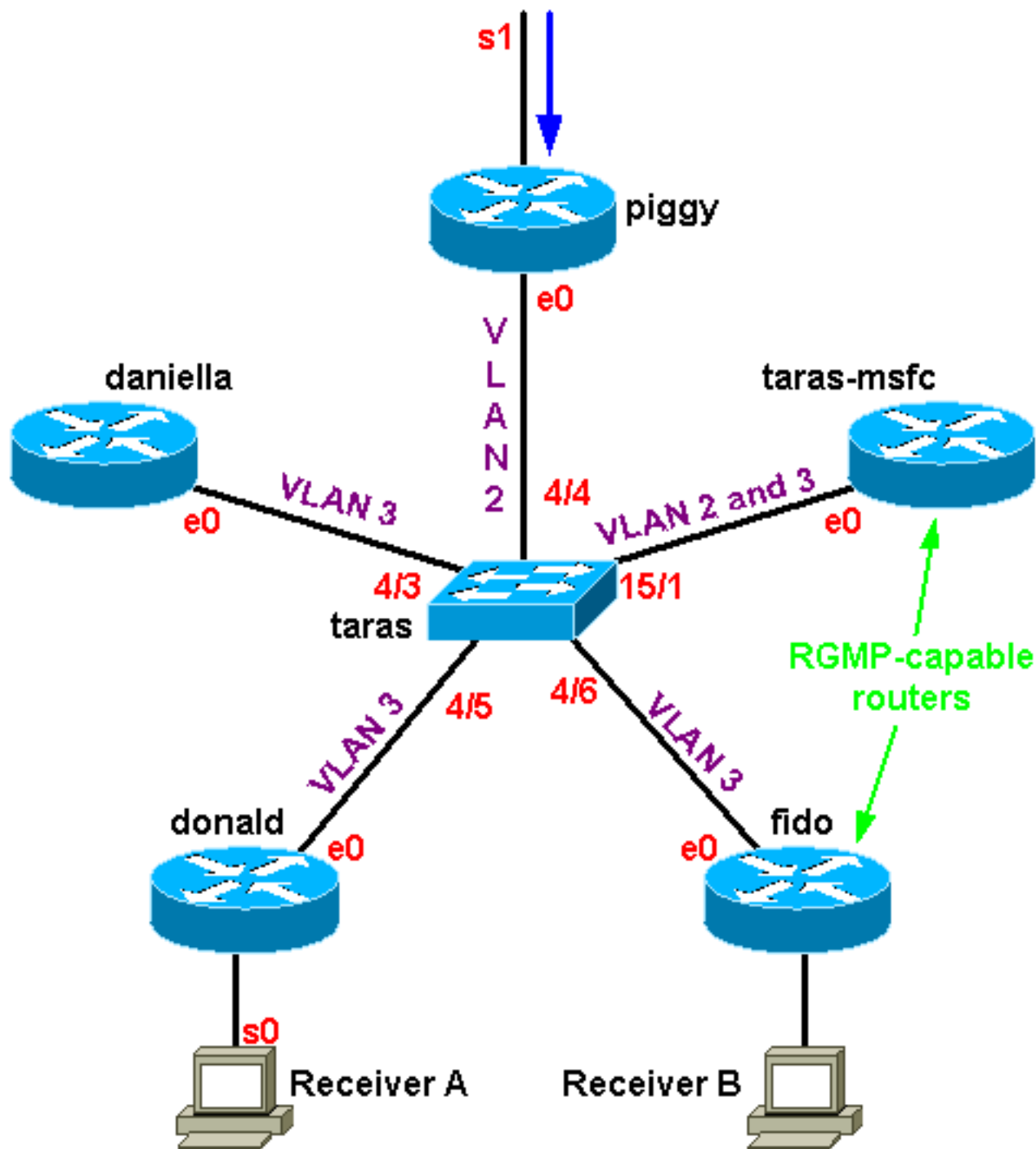
el **comando ip rgmp** en el modo de la interfaz (como en el Routers regular del Cisco IOS). Las interfaces que ejecutan el RGMP y cualquier otro router RGMP detectado por el IGMP Snooping pueden ser verificados publicando el siguiente comando:

```
Boris#show ip igmp snooping mrouter
vlan          ports
-----+-----
   1   Po3,Router
  10   Gi3/8,Router
  11   Gi3/8,Router
 100   Router
 101   Router
 198   Po3,Router
 199   Po3,Router+
 222   Router
'+'- RGMP capable router port
Boris#
```

La salida precedente muestra un Cisco IOS Software corriente del Catalyst 6000 con el **comando ip rgmp** configurado en la interfaz del VLA N 199. En el VLA N 199, marcan al router como RGMP capaz. El router en la significa del Cisco IOS Software el 6500 Router sí mismo en el VLA N 199.

Caso Práctico

Este diagrama representa una red real usando el RGMP:



En este caso, solamente el fido y el (MSFC) de la Multilayer Switch Feature Card en los taras son routers habilitados para RGMP; el donald, el daniella, y guarros son routers sin capacidad para RGMP. Existe un origen de multidifusión 4.4.4.1 que transmite hacia 224.1.1.1 ubicado en el serie detrás del piggy. Las msfc de los taras están haciendo el Routing entre VLAN entre el VLAN2 y el VLAN3. No hay receptor en el VLAN2 sino dos receptores en el VLAN3: uno detrás de fido y uno detrás de donald.

Nota: En la siguiente sección, la salida no precedida por un comando específico se asume para ser de `debug ip rgmp` en el Routers y de `set trace mcast 5` en el Switch.

Habilitación de RGMP en el Switch

Primero, permiso RGMP en los taras (un Catalyst 6000 Switch), si se asume que no se configura ninguno del Routers para el RGMP todavía. Tan pronto como se habilite el RGMP, el Switch agrega el Multicast MAC Address 01-00-5e-00-00-19 a la tabla del CAM del sistema, así que

significa que comienza a escuchar todos los paquetes enviados a esa dirección MAC. Éste es el direccionamiento que corresponde a 224.0.0.25, que es utilizada por el RGMP:

```
taras (enable) set rgmp enable
RGMP enabled.
```

```
taras (enable) show cam sys
```

```
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry $ = Dot1x Security Entry
VLAN  Dest MAC/Route Des      [CoS]  Destination Ports or VCs / [Protocol Type]
-----
1      00-d0-00-3f-8b-fc R#          15/1
1      00-d0-00-3f-8b-ff #           1/3
1      01-00-0c-cc-cc-cc #           1/3
1      01-00-0c-cc-cc-cd #           1/3
1      01-00-0c-dd-dd-dd #           1/3
1      01-00-5e-00-00-19 #          1/3
1      01-80-c2-00-00-00 #          1/3
1      01-80-c2-00-00-01 #          1/3
2      00-d0-00-3f-8b-fc R#          15/1
2      01-00-0c-cc-cc-cc #           1/3
2      01-00-0c-cc-cc-cd #           1/3
2      01-00-0c-dd-dd-dd #           1/3
2      01-00-5e-00-00-19 #          1/3
2      01-80-c2-00-00-00 #          1/3
2      01-80-c2-00-00-01 #          1/3
3      00-d0-00-3f-8b-fc R#          15/1
3      01-00-0c-cc-cc-cc #           1/3
3      01-00-0c-cc-cc-cd #           1/3
3      01-00-0c-dd-dd-dd #           1/3
3      01-00-5e-00-00-19 #          1/3
3      01-80-c2-00-00-00 #          1/3
3      01-80-c2-00-00-01 #          1/3
```

Activación de RGMP en los routers

Ahora permiso RGMP en las msfc de los taras y el fido. Configuran al router en el modo de la interfaz, y como el **debug ip rgmp** se está ejecutando usted puede ver que el router comienza a enviar los paquetes de los Hello (saludo) RGMP en eso la interfaz cada 30 segundos.

```
taras(config-if)#ip rgmp
00:10:24: RGMP: Sending a Hello packet on Ethernet0
00:10:54: RGMP: Sending a Hello packet on Ethernet0
00:11:24: RGMP: Sending a Hello packet on Ethernet0
00:11:54: RGMP: Sending a Hello packet on Ethernet0
```

Si usted ahora mira el Switch, usted puede ver que los puertos 4/6 y 15/1 están marcados como puertos de router habilitado para RGMP. Note que el Switch recibe siempre un Hello (saludo) RGMP momentos antes de un saludo de PIM:

```
MCAST-IGMPQ:recvd an RGMP Hello on the port 15/1 vlanNo 3 GDA 0.0.0.0
MCAST-RGMP: Received RGMP Hello in vlanNo 3 on port 15/1
MCAST-IGMPQ:recvd a PIM V2 packet of type HELLO on the port 15/1 vlanNo 3
```

```
taras (debug-eng) show multi ro
```

```
Port      Vlan
-----
4/3       3
4/4       2
4/5       3
4/6       + 3
15/1      + 2-3
```

Total Number of Entries = 5

'*' - Configured

'+' - RGMP-capable

Funcionamiento de RGMP en la VLAN 2

Puesto que hay receptor activo detrás del donald (no hay todavía un receptor detrás del fido), el tráfico Multicast en el VLAN2 necesita ser remitido sobre el VLAN3. Tan el MSFC en las necesidades de los taras de conseguir el tráfico en el VLAN2. Sin embargo, puesto que se habilita el RGMP, el Switch no más adelante el tráfico Multicast al MSFC. La MSFC debe enviar al switch un RGMP Join en la VLAN 2 como una petición para recibir ese grupo.

El router envía:

```
MCAST-IGMPQ:recvd an RGMP Hello on the port 15/1 vlanNo 3 GDA 0.0.0.0
```

```
MCAST-RGMP: Received RGMP Hello in vlanNo 3 on port 15/1
```

```
MCAST-IGMPQ:recvd a PIM V2 packet of type HELLO on the port 15/1 vlanNo 3
```

```
taras (debug-eng) show multi ro
```

Port	Vlan
4/3	3
4/4	2
4/5	3
4/6	+ 3
15/1	+ 2-3

Total Number of Entries = 5

'*' - Configured

'+' - RGMP-capable

El supervisor en el switch lo recibe:

```
MCAST-IGMPQ:recvd an RGMP Hello on the port 15/1 vlanNo 3 GDA 0.0.0.0
```

```
MCAST-RGMP: Received RGMP Hello in vlanNo 3 on port 15/1
```

```
MCAST-IGMPQ:recvd a PIM V2 packet of type HELLO on the port 15/1 vlanNo 3
```

```
taras (debug-eng) show multi ro
```

Port	Vlan
4/3	3
4/4	2
4/5	3
4/6	+ 3
15/1	+ 2-3

Total Number of Entries = 5

'*' - Configured

'+' - RGMP-capable

Usando el grupo del **rgmp de la demostración**, usted puede ver que el puerto 15/1 se ha unido al grupo 01-00-5e-01-01-01 en el VLAN2. Note que en el VLAN3, la entrada de CAM estática está presente, pero el único puerto de router incluido en la lista de puertos es el del router sin capacidad para RGMP (es decir, 15/1 y 4/6 no está en la lista de puertos para la entrada en el VLAN3 porque eso Routers es RGMP capaz y no envió un RGMP se une a en el VLAN 3). Note también en la tabla de CAM estática a que los grupos 01-00-5e-00-01-[27,28], correspondiente a 224.0.1.[39,40] usado por el auto-RP, no son afectados por la operación de RGMP. Todo el tráfico para estos grupos aún se dirige a todos los routers de multidifusión, sin importar si aceptan RGMP:

```
taras (enable) show cam sta
```

```
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.  
X = Port Security Entry $ = Dot1x Security Entry
```

VLAN	Dest MAC/Route Des	[CoS]	Destination Ports or VCs / [Protocol Type]
2	01-00-5e-01-01-01		4/4,15/1
2	01-00-5e-00-01-27		4/4,15/1
2	01-00-5e-00-01-28		4/4,15/1
3	01-00-5e-01-01-01		4/5,4/3
3	01-00-5e-00-01-27		4/3,4/5-6,15/1
3	01-00-5e-00-01-28		4/3,4/5-6,15/1

```
taras (enable) show rgmp group 01-00-5e-01-01-01
```

```
RGMP enabled
```

VLAN	Dest MAC/Route Des	[CoS]	RGMP Joined Router Ports
2	01-00-5e-01-01-01		15/1

```
Total Number of Entries = 1
```

Ahora mire las estadísticas de RGMP para el VLAN2. El Switch está recibiendo regularmente los Hello (saludo) RGMP y el RGMP se une a los paquetes. Consigue a un Hello (saludo) RGMP cada 30 segundos de las msfc de los taras, y las msfc de los taras envían un RGMP se unen a para 224.1.1.1 cada vez que envía un PIM se une a para ese grupo:

```
taras (enable) show rgmp stat 2
```

```
RGMP enabled
```

```
RGMP statistics for vlan 2:
```

```
Receive :
```

Valid pkts:	67
Hellos:	40
Joins:	27
Leaves:	0
Join Alls:	0
Leave Alls:	0
Byes:	0
Discarded:	0

```
Transmit :
```

Total pkts:	0
Failures:	0
Hellos:	0
Joins:	0
Leaves:	0
Join Alls:	0
Leave Alls:	0
Byes:	0

Hasta ahora, taras-msfc y fido sólo han enviado paquetes de saludo en VLAN 3:

```
taras (enable) show rgmp stat 3
```

```
RGMP enabled
```

```
RGMP statistics for vlan 3:
```

```
Receive :
```

Valid pkts:	468
Hellos:	468
Joins:	0
Leaves:	0
Join Alls:	0
Leave Alls:	0
Byes:	0

```

Discarded:          0
Transmit :
  Total pkts:      0
  Failures:        0
  Hellos:          0
  Joins:           0
  Leaves:          0
  Join Alls:       0
  Leave Alls:      0
  Byes:

```

RGMP se incorpora a la operación en VLAN 3

Si usted ahora comienza el receptor B detrás del fido, el router habilitado para RGMP enviará un RGMP se une a al Switch para el grupo 224.1.1.1. El Switch lo recibirá y agregará el puerto 4/6 (fido) a la lista de receptores interesados para ese grupo en el VLAN3.

En el router, usted ve:

```

taras (enable) show rgmp stat 3
RGMP enabled
RGMP statistics for vlan 3:

```

```

Receive :
  Valid pkts:      468
  Hellos:          468
  Joins:           0
  Leaves:          0
  Join Alls:       0
  Leave Alls:      0
  Byes:            0
  Discarded:       0
Transmit :
  Total pkts:      0
  Failures:        0
  Hellos:          0
  Joins:           0
  Leaves:          0
  Join Alls:       0
  Leave Alls:      0
  Byes:

```

El switch recibe la unión RGMP y agrega el puerto 4/6 del router a la entrada estática. Usted puede ver el resultado en los diversos **comandos show**:

```

MCAST-IGMPQ:recvd an RGMP Join on the port 4/6 vlanNo 3 GDA 224.1.1.1
MCAST-RGMP: Received RGMP Join for 224.1.1.1 in vlanNo 3 on port 4/6
EARL-MCAST: SetRGMPPortInGDA: RGMP port 4/6 in vlanNo 3 joining for the first time
for this group 224.1.1.1

```

```

MCAST-RELAY:Relaying packet on port 15/1 vlanNo 3
MCAST-SEND: Inband Transmit Succeeded for IGMP RELAY msg on port 15/1 vlanNo 3

```

```

taras (enable) show rgmp group
RGMP enabled

```

VLAN	Dest MAC/Route Des	[CoS]	RGMP Joined Router Ports
2	01-00-5e-01-01-01		15/1
3	01-00-5e-01-01-01		4/6

Total Number of Entries = 2

```
taras (enable) show cam sta 01-00-5e-01-01-01
```

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

```
X = Port Security Entry $ = Dot1x Security Entry
```

VLAN	Dest MAC/Route Des	[CoS]	Destination Ports or VCs / [Protocol Type]
2	01-00-5e-01-01-01		4/4,15/1
3	01-00-5e-01-01-01		4/3,4/5-6

```
taras (enable) show rgmp stat 3
```

```
RGMP enabled
```

```
RGMP statistics for vlan 3:
```

```
Receive :
```

Valid pkts:	542
Hellos:	532
Joins:	10
Leaves:	0
Join Alls:	0
Leave Alls:	0
Byes:	0
Discarded:	0

```
Transmit :
```

Total pkts:	0
Failures:	0
Hellos:	0
Joins:	0
Leaves:	0
Join Alls:	0
Leave Alls:	0
Byes:	0

Operación de abandono de RGMP

Asuma que el receptor B no está interesado más, así que fido necesita no más el tráfico Multicast para ese grupo y enviará una pasa PIM para el grupo en la interfaz. El router también envía ausencia de rgmp para que el grupo deje el Switch saber que no está interesado en ese grupo más.

Cuando el receptor B es todavía activo, la **ruta multicast del IP de la demostración** muestra (S, G) entrada con el indicador A.C., diciéndole allí es un receptor conectado interesado:

```
fido#show ip mroute 224.1.1.1
```

```
IP Multicast Routing Table
```

```
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,  
L - Local, P - Pruned, R - RP-bit set, F - Register flag,  
T - SPT-bit set, J - Join SPT, M - MSDP created entry,  
X - Proxy Join Timer Running, A - Advertised via MSDP, U - URD,  
I - Received Source Specific Host Report
```

```
Outgoing interface flags: H - Hardware switched
```

```
Timers: Uptime/Expires
```

```
Interface state: Interface, Next-Hop or VCD, State/Mode
```

```
(* , 224.1.1.1), 00:01:18/00:00:00, RP 10.10.10.1, flags: SJCL
```

```
Incoming interface: Ethernet0, RPF nbr 33.3.3.1
```

```
Outgoing interface list:
```

```
Serial0, Forward/Sparse-Dense, 00:01:18/00:01:41
```

```
(4.4.4.1, 224.1.1.1), 00:01:16/00:02:59, flags: CLJT
```

```
Incoming interface: Ethernet0, RPF nbr 33.3.3.1
```

```
Outgoing interface list:
```

```
Serial0, Forward/Sparse-Dense, 00:01:16/00:01:43
```

Cuando el receptor B está interesado no más, el PIM enviará un mensaje de la pasa, pero (S, G)

entrada no se quita inmediatamente. El temporizador (resaltado en rojo) se retrocede hasta el tiempo muerto de entrada. Observe que en este punto la entrada continúa allí pero con el indicador P informándonos que está separada y finalizará el tiempo de espera.

```
01:15:25: PIM: Send v2 Prune on Ethernet0 to 33.3.3.1 for (10.10.10.1/32, 224.1.1.1), WC-bit, RPT-bit, S-bit
01:15:25: PIM: Received v2 Join/Prune on Ethernet0 from 33.3.3.4, not to us
01:15:28: RGMP: Sending a Hello packet on Ethernet0
01:15:29: PIM: Received v2 Join/Prune on Ethernet0 from 33.3.3.3, not to us
01:15:29: PIM: Join-list: (*, 224.1.1.1) RP 10.10.10.1, RPT-bit set, WC-bit set, S-bit set
01:15:29: PIM: Join-list: (4.4.4.1/32, 224.1.1.1), S-bit set
```

IP Multicast Routing Table

```
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Advertised via MSDP, U - URD,
       I - Received Source Specific Host Report
```

Outgoing interface flags: H - Hardware switched

Timers: Uptime/Expires

Interface state: Interface, Next-Hop or VCD, State/Mode

```
(*, 224.1.1.1), 00:08:31/00:02:39, RP 10.10.10.1, flags: SJP
  Incoming interface: Ethernet0, RPF nbr 33.3.3.1
  Outgoing interface list: Null
```

```
(4.4.4.1, 224.1.1.1), 00:08:29/00:02:29, flags: PJT
  Incoming interface: Ethernet0, RPF nbr 33.3.3.1
  Outgoing interface list: Null
```

Luego de que finalmente se agote el tiempo de espera de la entrada (S,G), fido envía un mensaje de ausencia de RGMP al switch para el grupo 224.1.1.1:

```
01:15:25: PIM: Send v2 Prune on Ethernet0 to 33.3.3.1 for (10.10.10.1/32, 224.1.1.1), WC-bit, RPT-bit, S-bit
01:15:25: PIM: Received v2 Join/Prune on Ethernet0 from 33.3.3.4, not to us
01:15:28: RGMP: Sending a Hello packet on Ethernet0
01:15:29: PIM: Received v2 Join/Prune on Ethernet0 from 33.3.3.3, not to us
01:15:29: PIM: Join-list: (*, 224.1.1.1) RP 10.10.10.1, RPT-bit set, WC-bit set, S-bit set
01:15:29: PIM: Join-list: (4.4.4.1/32, 224.1.1.1), S-bit set
```

IP Multicast Routing Table

```
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Advertised via MSDP, U - URD,
       I - Received Source Specific Host Report
```

Outgoing interface flags: H - Hardware switched

Timers: Uptime/Expires

Interface state: Interface, Next-Hop or VCD, State/Mode

```
(*, 224.1.1.1), 00:08:31/00:02:39, RP 10.10.10.1, flags: SJP
  Incoming interface: Ethernet0, RPF nbr 33.3.3.1
  Outgoing interface list: Null
```

```
(4.4.4.1, 224.1.1.1), 00:08:29/00:02:29, flags: PJT
  Incoming interface: Ethernet0, RPF nbr 33.3.3.1
  Outgoing interface list: Null
```

Después de que el Switch reciba ausencia de rgmp, usted puede ver en el grupo RGMP que hay no más cualquier entrada para el VLAN3:

```
MCAST-IGMPQ:recvd an RGMP Leave on the port 4/6 vlanNo 3 GDA 224.1.1.1
```

```
MCAST-RGMP: Received RGMP Leave for 224.1.1.1 in vlanNo 3 on port 4/6
EARL-MCAST: ClearRGMPPortInGDA last RGMP port going away for all groups - delete rgmp_info
too for GDA 01-00-5e-01-01-01 vlanNo 3
MCAST-RELAY:Relaying packet on port 15/1 vlanNo 3
MCAST-SEND: Inband Transmit Succeeded for IGMP RELAY msg on port 15/1 vlanNo 3
```

```
taras (debug-eng) show rgmp group
RGMP enabled
```

VLAN	Dest MAC/Route Des	[CoS]	RGMP Joined Router Ports
2	01-00-5e-01-01-01		15/1

```
taras (debug-eng) show rgmp stat 3
RGMP enabled
RGMP statistics for vlan 3:
```

```
Receive :
Valid pkts:          588
Hellos:              574
Joins:               11
Leaves:              3
Join Alls:           0
Leave Alls:           0
Byes:                0
Discarded:           0
```

Operación RGMP Bye

Si usted inhabilita el RGMP en el fido, enviará un adiós RGMP, y el Switch cambiará 4/6 de un puerto del router RGMP a un puerto del router normal:

En el fido:

```
MCAST-IGMPQ:recvd an RGMP Leave on the port 4/6 vlanNo 3 GDA 224.1.1.1
MCAST-RGMP: Received RGMP Leave for 224.1.1.1 in vlanNo 3 on port 4/6
EARL-MCAST: ClearRGMPPortInGDA last RGMP port going away for all groups - delete rgmp_info
too for GDA 01-00-5e-01-01-01 vlanNo 3
MCAST-RELAY:Relaying packet on port 15/1 vlanNo 3
MCAST-SEND: Inband Transmit Succeeded for IGMP RELAY msg on port 15/1 vlanNo 3
```

```
taras (debug-eng) show rgmp group
RGMP enabled
```

VLAN	Dest MAC/Route Des	[CoS]	RGMP Joined Router Ports
2	01-00-5e-01-01-01		15/1

```
taras (debug-eng) show rgmp stat 3
RGMP enabled
RGMP statistics for vlan 3:
```

```
Receive :
Valid pkts:          588
Hellos:              574
Joins:               11
Leaves:              3
Join Alls:           0
Leave Alls:           0
Byes:                0
Discarded:           0
```

En el switch:


```
MCAST-IGMPQ:rcvcd an RGMP Bye  on the port 4/6 vlanNo 3 GDA 0.0.0.0
MCAST-RGMP: Received RGMP Bye in vlanNo 3 on port 4/6
MCAST-RELAY:Relaying packet on port 15/1 vlanNo 3
MCAST-SEND: Inband Transmit Succeeded for IGMP RELAY msg on port 15/1 vlanNo 3
```

```
taras (debug-eng) show rgmp stat 3
```

```
RGMP enabled
```

```
RGMP statistics for vlan 3:
```

```
Receive :
```

```
Valid pkts:          603
Hellos:              588
Joins:               11
Leaves:              3
Join Alls:           0
Leave Alls:           0
Byes:                1
Discarded:           0
```

```
Transmit :
```

```
Total pkts:         0
Failures:            0
Hellos:              0
Joins:               0
Leaves:              0
Join Alls:           0
Leave Alls:           0
Byes:                0
```

```
taras (enable) show multi router
```

```
Port      Vlan
```

```
-----
```

```
4/3       3
4/4       2
4/5       3
4/6       3
4/48      1
15/1      + 2-3
```

[Información Relacionada](#)

- [Soporte de Producto de LAN](#)
- [Soporte de Tecnología de LAN Switching](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)