Uso de RGMP: Fundamentos y Casos Prácticos

Contenido

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.

Tenga en cuenta que ahora existe una nueva función que reemplaza a RGMP y es más escalable. Esta función se denomina snooping de multidifusión independiente del protocolo (PIM) y realiza el mismo objetivo que RGMP. La indagación PIM está fuera del alcance de este documento.

Para obtener más información, refiérase a Configuración de Snooping PIM.

Prerequisites

Requirements

Los lectores de este documento deben ser conscientes de estas limitaciones de protocolo:

- Debe ejecutar RGMP en los routers y los switches.
- Debe activar la indagación IGMP en los switches.
- RGMP sólo funcionará para 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.
- RGMP sólo le permite restringir el tráfico hacia un router conectado directamente o hacia un router conectado que no sea un switch compatible con RGMP. RGMP no es capaz de restringir el tráfico a un router multicast conectado detrás de otro switch compatible con RGMP.

Si no se siguen estas restricciones, puede producirse una interrupción de la conectividad multidifusión.

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

RGMP se soporta en las siguientes versiones del software del router Cisco IOS:

- Línea principal 12.3
- 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)
- 12.0ST (a partir de la versión 12.0(11)ST)

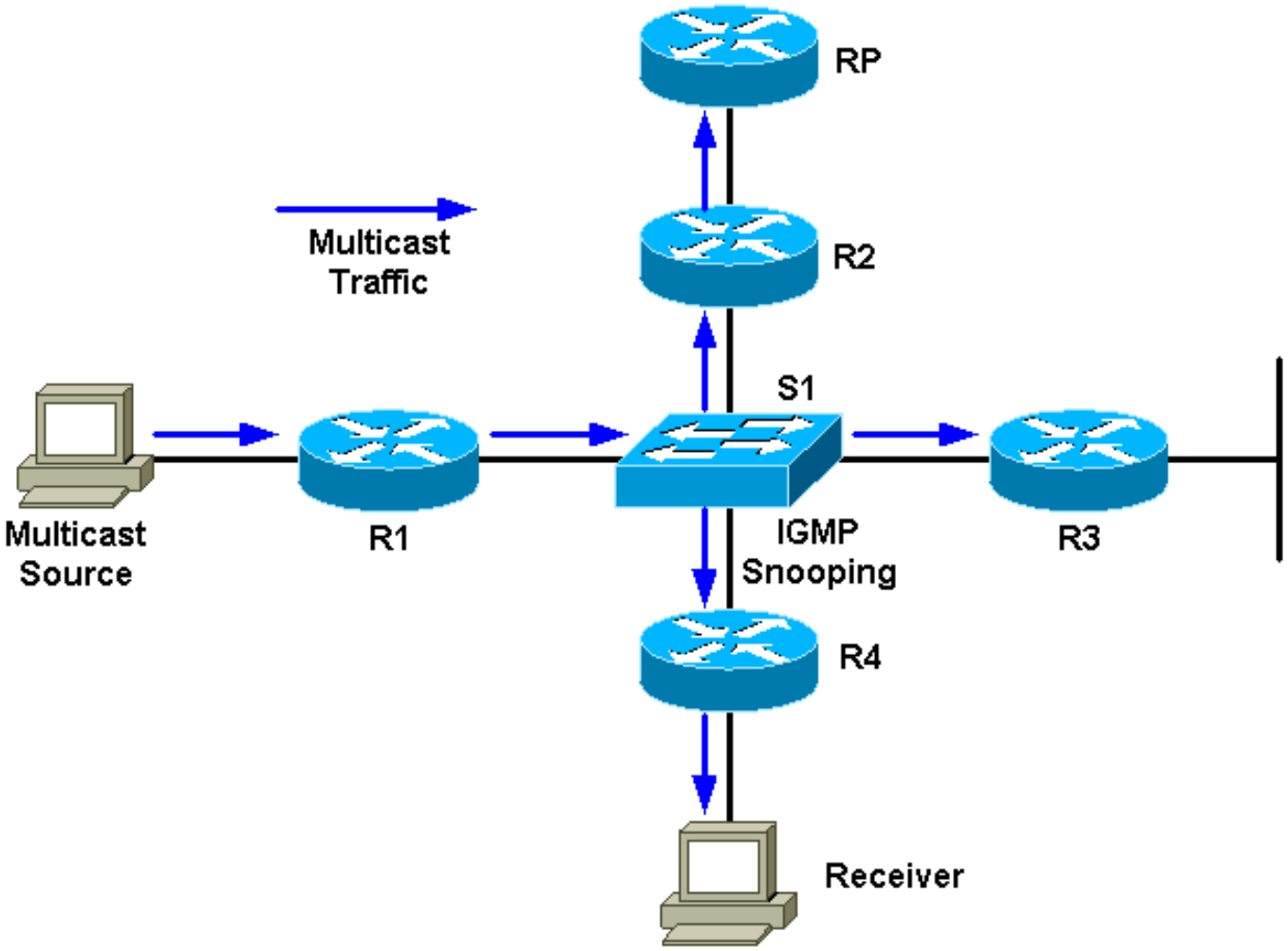
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

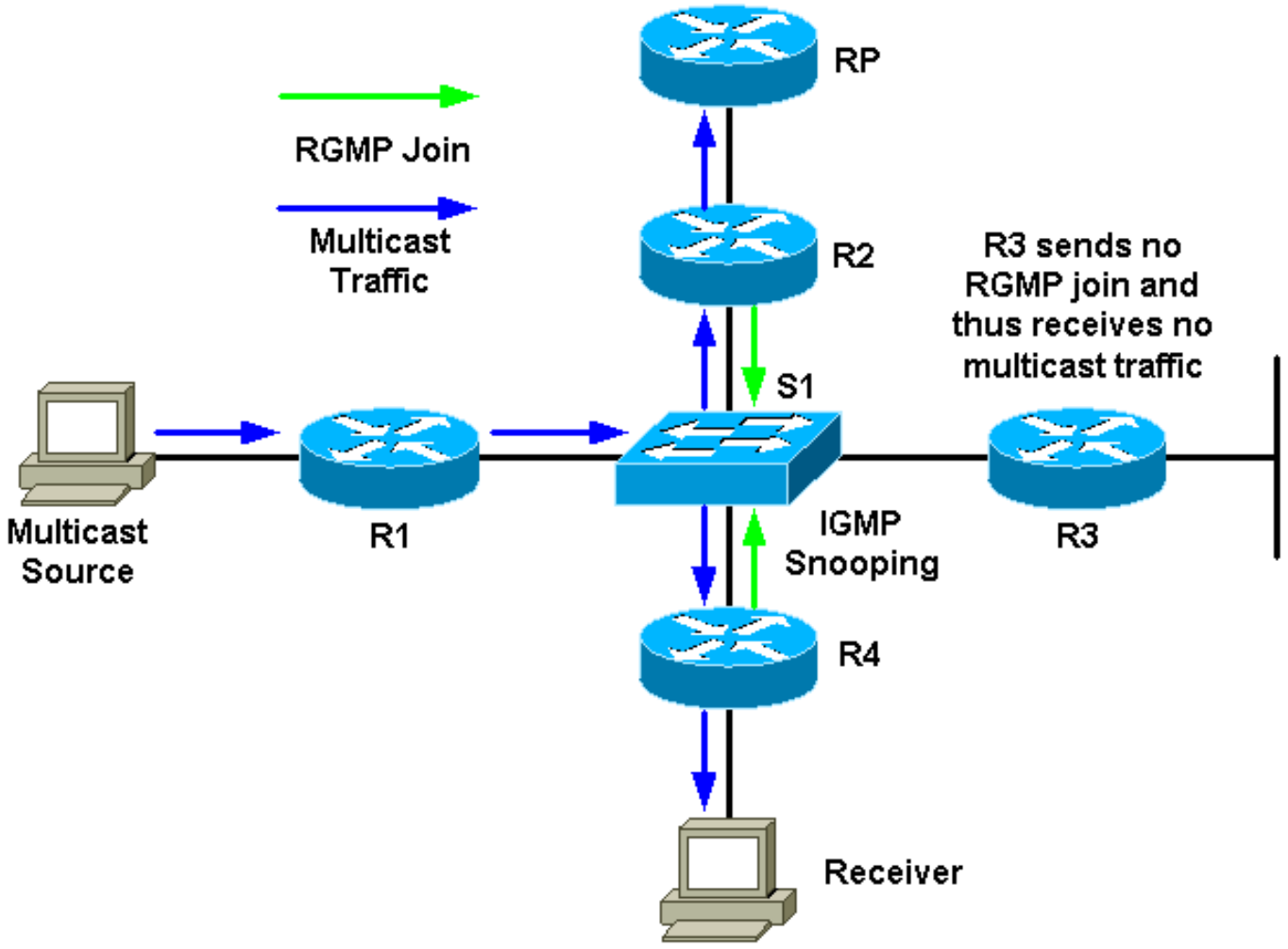
RGMP reduce la carga en la red

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



Hay una fuente multicast conectada a R1 y un receptor conectado a 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 esta red sólo de origen con indagación IGMP y creará una entrada estática de Memoria direccionable por contenido (CAM) que apuntará a todos los 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 RGMP habilitado (suponiendo que los routers y el switch son compatibles con RGMP):



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

RGMP es, al igual que 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 tiempo de vida (TTL) de 1. La dirección 224.0.0.25 es una dirección reservada que corresponde 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 diferentes campos de 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
Dirección IP de destino de todos los paquetes RGMP	224.0.0.25
Dirección de grupo usada en RGMP Hello y Bye	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

RGMP Hello

Siempre que se habilita RGMP en el router, el router envía un mensaje de saludo RGMP al switch indicando que el switch no debe reenviar el tráfico de datos multicast a este router a menos que se envíe específicamente una incorporación RGMP 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 se inhabilita RGMP en el router, envía un mensaje de despedida RGMP para indicar al switch que el router ya no está haciendo RGMP y que todo el tráfico multicast debe reenviarse nuevamente a este router.

Unión de RGMP

Siempre que un router envía una unión PIM, también construye una unión RGMP y la envía en la misma interfaz en la que se enviará la unión PIM. Utilizando los diagramas anteriores como ejemplo, R4 envía un mensaje de unión 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. S1 procesa el paquete y agrega el puerto del router a la entrada estática de capa 2 (entrada 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.

RGMP Leave

Siempre que un router envía un mensaje de PIM Prune para un (*,G) o (S,G), también verifica si hay al menos otra entrada de ruta multicast para este grupo para la interfaz en la que se envió la PIM Prune. Si no hay otra entrada, se envía un RGMP Leave 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:

- Los switches no envían ningún grupo multicast a un router con capacidad RGMP a menos que el router lo solicite específicamente (excepto para el 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.

RGMP Hello

Cuando se recibe un paquete RGMP Hello de un puerto del router, el switch marca este puerto del router como habilitado para RGMP y el tráfico multicast general ya no se envía a ese puerto del router multicast.

Nota: Los paquetes Hello de RGMP generalmente no se reenvían fuera del chasis. Los paquetes de RGMP Hello se reenvían solamente una vez que se recibe el primer RGMP Hello en un puerto El puerto se marca luego como un puerto RGMP y el paquete Hello se reenvía a otro puerto de

router multicast habilitado para RGMP.

Adiós RGMP

Al recibir RGMP Bye, desmarque el puerto del router como puerto del router RGMP y agregue este puerto a todo el grupo existente en esa VLAN.

Unión de RGMP

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.

RGMP Leave

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 RGMP en un switch:

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

Puede verificar la configuración escribiendo:

```
#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 lo ha hecho anteriormente:

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

RGMP en Catalyst 6000 que ejecuta Cisco IOS System Software

RGMP en el Catalyst 6000 que ejecuta Cisco IOS System Software tiene estas características:

- Habilitado de forma predeterminada en todos los puertos L2 (switchport) y no se puede inhabilitar

- Necesita estar habilitado en cualquier puerto multicast L3 si la interfaz multicast L3 es necesaria para actuar como router RGMP; esto se hace ejecutando el comando **ip rgmp** en el modo de interfaz (como en los routers Cisco IOS normales).

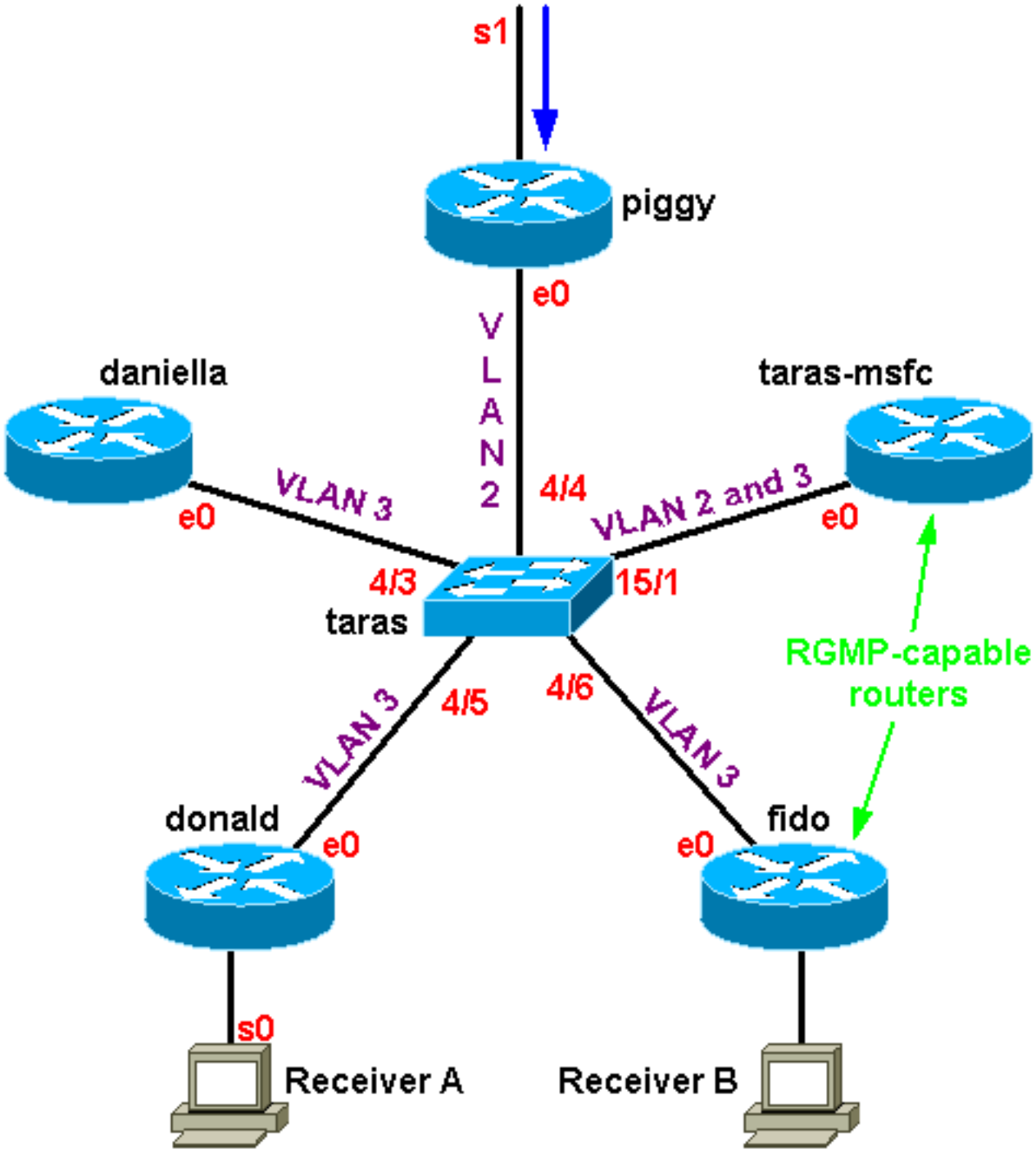
Las interfaces que ejecutan RGMP y cualquier otro router RGMP detectado por la indagación IGMP pueden verificarse mediante la ejecución del siguiente comando:

```
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#
```

El resultado anterior muestra un Catalyst 6000 que ejecuta Cisco IOS Software con el comando **ip rgmp** configurado en la interfaz VLAN 199. En la VLAN 199, el router se marca como habilitado para RGMP. El router en Cisco IOS Software representa el router 6500 en la VLAN 199.

Caso Práctico

Este diagrama representa una red real usando RGMP:



En este caso, sólo fido y la Tarjeta de función de switch multicapa (MSFC) en taras son routers con capacidad RGMP; donald, daniella y piggy son routers no aptos 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. Taras-msfc está haciendo el ruteo entre VLAN 2 y VLAN 3. No hay ningún receptor en la VLAN 2, sino dos receptores en la VLAN 3: uno detrás de fido y uno detrás de donald.

Nota: En la siguiente sección, se asume que la salida no precedida por un comando específico es de **debug ip rgmp** en los routers y establezca trace mcast 5 en el switch.

Habilitación de RGMP en el Switch

Primero, active RGMP en taras (un switch Catalyst 6000), suponiendo que ninguno de los routers esté configurado para RGMP todavía. Tan pronto como se habilita RGMP, el switch agrega la dirección MAC multicast 01-00-5e-00-00-19 a la tabla CAM del sistema, lo que significa que comienza a escuchar todos los paquetes enviados a esa dirección MAC. Esta es la dirección que

corresponde a 224.0.0.25, que es utilizada por 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 habilite RGMP en taras-msfc y fido. El router se configura en el modo de interfaz, y a medida que **debug ip rgmp** se ejecuta, puede ver que el router comienza a enviar paquetes Hello RGMP en esa 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 ahora mira el switch, puede ver que los puertos 4/6 y 15/1 están marcados como puertos de router compatibles con RGMP. Observe que el switch siempre recibe un saludo RGMP justo antes de un saludo 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

Dado que hay un receptor activo detrás de donald (todavía no hay un receptor detrás de fido), el tráfico multicast en VLAN 2 debe reenviarse a VLAN 3. Por lo tanto, la MSFC en las taras necesita obtener el tráfico en la VLAN 2. Sin embargo, dado que RGMP está habilitado, el switch ya no reenvía el tráfico multicast a la MSFC. La MSFC debe enviar al switch un RGMP Join en la VLAN 2 como una petición para recibir ese grupo.

El router envía:

```
16:10:28: RGMP: Sending a Join packet on Vlan2 for group 224.1.1.1
16:10:29: RGMP: Sending a Join packet on Vlan2 for group 224.1.1.1
```

El supervisor en el switch lo recibe:

```
MCAST-RGMP: Received RGMP Join for 224.1.1.1 in vlanNo 2 on port 15/1
```

Con el **grupo show rgmp**, puede ver que el puerto 15/1 se ha unido al grupo 01-00-5e-01-01-01 en la VLAN 2. Observe que en la VLAN 3, la entrada CAM estática está presente, pero el único puerto de router incluido en la lista de puertos es el del router no habilitado para RGMP (es decir, 15/1 y 4/6 no están en la lista de puertos para la entrada en la VLAN 3 porque esos routers son aptos para RGMP y no enviaron una unión RGMP en la VLAN 3). Observe también en la tabla CAM estática que los grupos 01-00-5e-00-01-[27,28], correspondientes a 224.0.1.[39,40] utilizados por auto-rp, no se ven afectados por el funcionamiento 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 observe las estadísticas de RGMP para VLAN 2. El switch recibe regularmente paquetes RGMP Hello y RGMP Join. Obtiene un RGMP Hello cada 30 segundos de taras-msfc, y taras-msfc envía una RGMP Join para 224.1.1.1 cada vez que envía una PIM Join 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 ahora inicia el receptor B detrás de fido, el router con capacidad RGMP enviará una incorporación RGMP al switch para el grupo 224.1.1.1. El switch lo recibirá y añadirá el puerto 4/6 (fido) a la lista de receptores interesados para ese grupo en la VLAN 3.

En el router, verá:

```
01:07:49: RGMP: Sending a Join packet on Ethernet0 for group 224.1.1.1
01:07:49: RGMP: Sending a Join packet on Ethernet0 for group 224.1.1.1
01:07:49: RGMP: Sending a Join packet on Ethernet0 for group 224.1.1.1
01:07:51: RGMP: Sending a Join packet on Ethernet0 for group 224.1.1.1
```

El switch recibe la unión RGMP y agrega el puerto 4/6 del router a la entrada estática. Puede ver el resultado en varios 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

Suponga que el Receptor B ya no está interesado, por lo que fido ya no necesita el tráfico multicast para ese grupo y enviará una PIM Prune para el grupo en la interfaz. El router también envía una licencia RGMP para que el grupo haga saber al switch que ya no está interesado en ese grupo.

Cuando el Receptor B aún está activo, **show ip mroute** muestra la entrada (S,G) con un indicador C, indicando que hay 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 ya no está interesado, PIM enviará un mensaje de recorte, pero la entrada (S,G) no se elimina 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:

```
01:18:50: RGMP: Sending a Leave packet on Ethernet0 for group 224.1.1.1
01:18:58: RGMP: Sending a Hello packet on Ethernet0
```

Después de que el switch recibe la ausencia de RGMP, puede ver en el grupo RGMP que ya no hay entradas para la VLAN 3:

```
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 inhabilita el RGMP en fido, enviará una despedida RGMP y el switch cambiará 4/6 de un puerto de router RGMP a un puerto de router normal:

En fido:

```
01:24:45: RGMP: Sending a Bye packet on Ethernet0
```

En el switch:

```
MCAST-IGMPQ:recvd 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