Uso di RGMP: Nozioni di base e case study

Sommario

Introduzione

Il protocollo RGMP (Router-Port Group Management Protocol) viene utilizzato con lo snooping IGMP per vincolare il traffico multicast ai livelli in cui è realmente necessario. Lo snooping IGMP invia il traffico multicast a tutte le porte del router. Con RGMP, il traffico multicast viene inviato solo alle porte che devono riceverlo. Il protocollo RGMP è progettato per essere eseguito sulla backbone della rete multicast; per la comprensione di questo documento è utile avere una conoscenza di base del multicast (IGMP, PIM, multicast routing).

Èstata introdotta una nuova funzionalità che sostituisce il protocollo RGMP e offre una maggiore scalabilità. Questa funzione è denominata snooping PIM (Protocol Independent Multicast) ed esegue lo stesso obiettivo di RGMP. Lo snooping PIM non rientra nell'ambito di questo documento.

Per ulteriori informazioni, consultare il documento sulla configurazione dello snooping PIM.

Prerequisiti

Requisiti

I lettori di questo documento devono essere consapevoli delle seguenti limitazioni di protocollo:

- Ènecessario eseguire il protocollo RGMP sia sui router che sugli switch.
- Ènecessario abilitare lo snooping IGMP sugli switch.
- RGMP funziona solo per i gruppi configurati con la modalità sparse PIM.
- Le origini che inviano traffico multicast connesso direttamente a uno switch RGMP non sono supportate.
- La connessione di più router alla stessa porta dello switch non è supportata (ad esempio, due router sullo stesso hub).
- La connessione di più router allo stesso switch non RGMP non è supportata.
- Il protocollo RGMP consente solo di limitare il traffico verso un router connesso direttamente o verso un router connesso tramite uno switch non compatibile con RGMP. RGMP non è in grado di limitare il traffico a un router multicast connesso dietro un altro switch compatibile con RGMP.

Il mancato rispetto di queste restrizioni può causare interruzioni nella connettività multicast.

Componenti usati

RGMP è un protocollo in esecuzione tra gli switch Catalyst e i router, entrambi devono supportare RGMP per permettere il funzionamento della funzione. I seguenti switch supportano RGMP:

- Catalyst 6000: a partire dalla versione 5.4 del software
- Catalyst 6000 con software di sistema Cisco IOS®: dal software 12.1(3a)E3
- Catalyst 5000: a partire dalla versione 5.4 del software

Il protocollo RGMP è supportato nelle seguenti versioni del software del router Cisco IOS:

- 12.3 Mainline
- 12,3T
- 12.2 Mainline
- 12.2.S
- 12,2 T
- 12,1E
- 12.1T (a partire dalla versione 12.1(5)T1)
- 12.0S (a partire dalla versione 12.0(10)S)
- 12.0ST (a partire dalla versione 12.0(11)ST)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

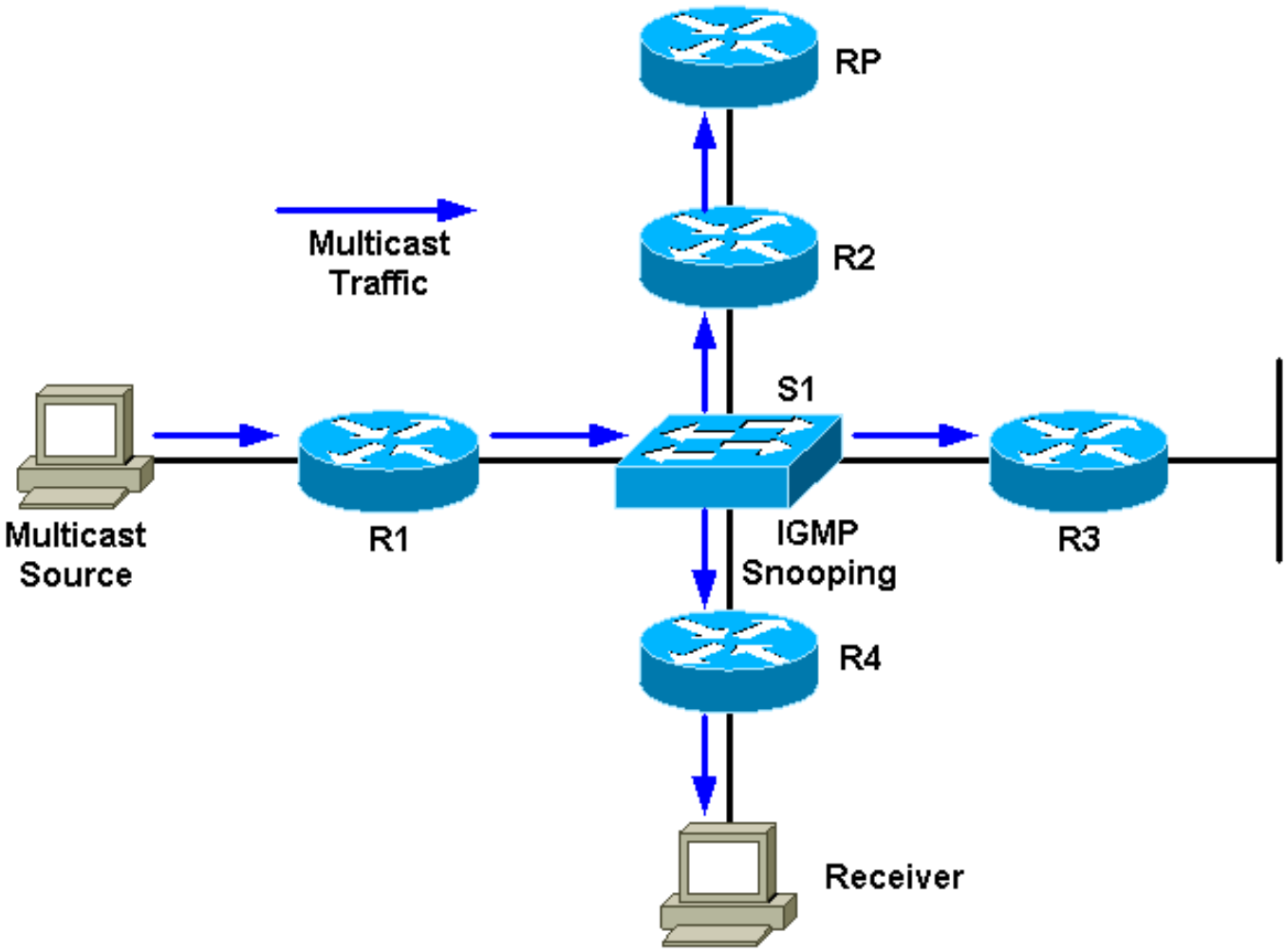
Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

RGMP riduce il carico sulla rete

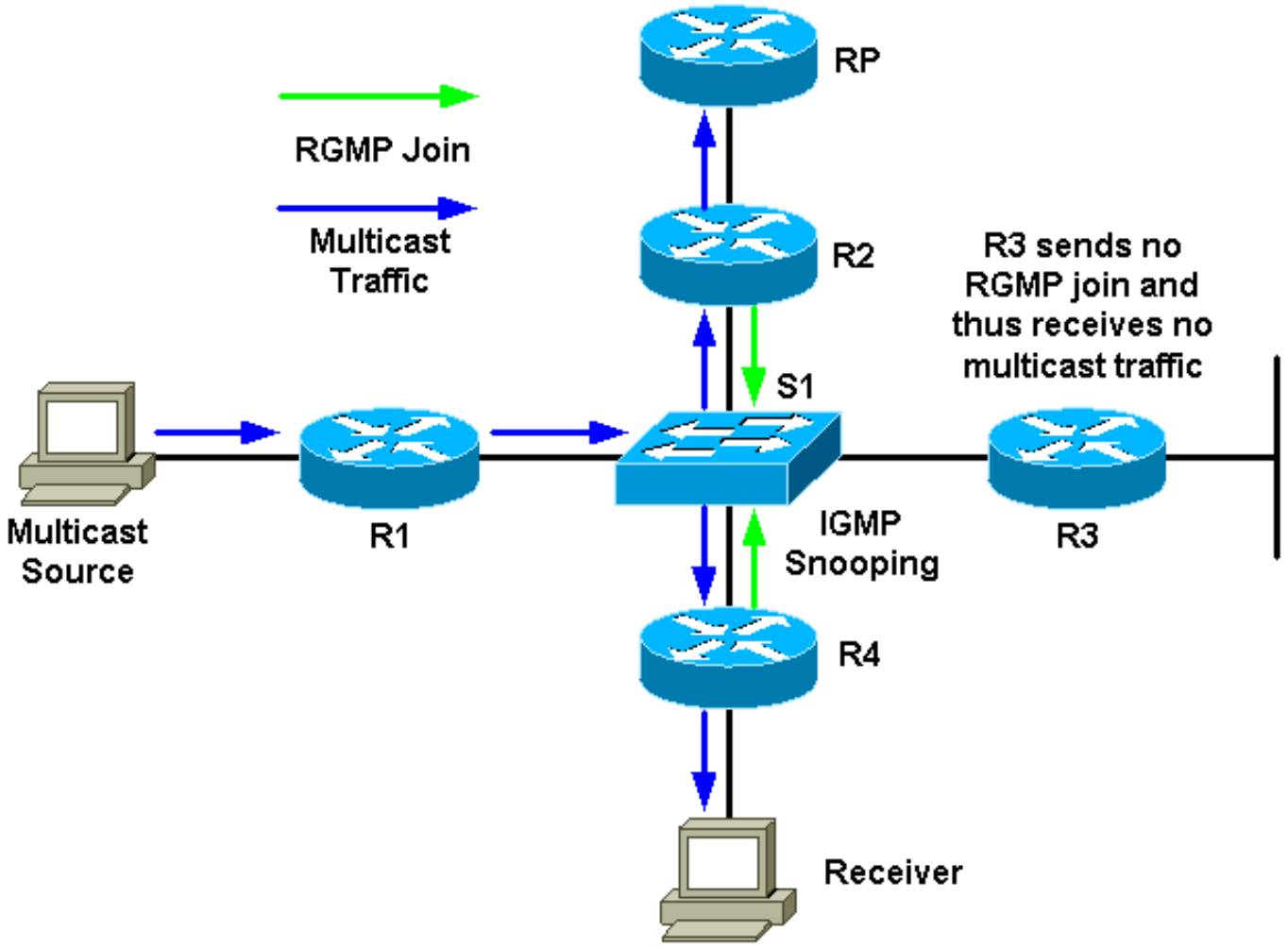
Lo scopo di RGMP è eliminare il traffico multicast non necessario. Il diagramma mostra una rete

ipotetica senza RGMP abilitato:



A R1 è collegata un'origine multicast e a R4 un ricevitore. L'RP per il gruppo si trova dietro R2. Il traffico viene inoltrato da R1 allo switch (per PIM e tabella mroute, poiché c'è un ricevitore dietro l'interfaccia dello switch). Lo switch rileva la rete solo sorgente con snooping IGMP e crea una voce statica CAM (Content-Addressable Memory) che punta a tutti i router: R1, R2, R3 e R4. Il traffico multicast verrà inviato a tutti i router, incluso R3, che non necessita del traffico. Se il volume del traffico multicast è elevato, è possibile che venga creato un carico non necessario sul router R3. Per risolvere il problema, è stato creato il protocollo RGMP.

Il diagramma mostra la stessa rete con RGMP abilitato (presupponendo che i router e lo switch siano compatibili con RGMP):



R2 e R4 invieranno allo switch un join RGMP per quel gruppo multicast. R3 non invierà un join RGMP. Di conseguenza, lo switch inoltrerà solo il traffico multicast ricevuto da R1 per quel gruppo a R2 e R4 e non a R3. Ciò riduce il traffico sulla rete.

RGMP in dettaglio

Come il protocollo CGMP, il protocollo RGMP è un protocollo in esecuzione tra un router e uno switch. I router inviano pacchetti RGMP e gli switch restano in ascolto dei pacchetti RGMP. Gli switch non inviano mai pacchetti RGMP e i router ignorano i pacchetti RGMP che potrebbero ricevere. I pacchetti RGMP sono pacchetti IP di tipo IGMP e vengono inviati all'indirizzo riservato del gruppo 224.0.0.25 (indirizzo MAC 01-00-5e-00-00-19). I pacchetti IGMP vengono inviati con un valore TTL (Time To Live) pari a 1. L'indirizzo 224.0.0.25 è un indirizzo riservato corrispondente a tutti gli indirizzi multicast dello switch. Un pacchetto RGMP contiene fondamentalmente un campo Type, un campo indirizzo di gruppo e un checksum.

Nella tabella vengono mostrati i diversi campi Type disponibili per i pacchetti RGMP:

Descrizione	Azione
Salve	Quando sul router è abilitato RGMP, lo switch non invia alcun traffico di dati multicast al router, a meno che non venga inviato specificamente un join RGMP per un gruppo.

Ciao	Quando il protocollo RGMP è disabilitato sul router, lo switch invia tutto il traffico di dati multicast al router.
Partecipa	Il traffico di dati multicast per un indirizzo MAC multicast proveniente dall'indirizzo di gruppo di layer 3 G viene inviato al router. Il gruppo G di questi pacchetti è nel campo Group Address (Indirizzo gruppo) del pacchetto RGMP.
Esci	Il traffico dati multicast per il gruppo G non viene inviato al router. I pacchetti hanno il gruppo G nel campo group address (indirizzo gruppo) del pacchetto RGMP.

I pacchetti Hello e Bye utilizzano 0.0.0.0 come indirizzo di gruppo nel pacchetto RGMP. Partecipa e lascia utilizzare l'indirizzo del gruppo che interessa il router (per unirsi o uscire).

I pacchetti RGMP utilizzano i seguenti tipi di indirizzi:

Tipo di indirizzo	Indirizzo utilizzato
Indirizzo MAC di destinazione di tutti i pacchetti RGMP	01-00-5e-00-00-19
Indirizzo IP di destinazione di tutti i pacchetti RGMP	224.0.0.25
Indirizzo di gruppo utilizzato in RGMP Hello e Bye	0.0.0.0
Indirizzo del gruppo utilizzato in RGMP Join and Leave	Gruppo multicast per cui viene inviato l'accesso o l'uscita

Cause dell'invio di pacchetti RGMP da parte del router

RGMP Hello

Quando sul router è abilitato RGMP, il router invia un messaggio RGMP Hello allo switch per comunicargli che lo switch non deve inoltrare il traffico di dati multicast a questo router, a meno che non venga inviato specificamente un RGMP Join per un gruppo. Inoltre, per il corretto funzionamento di questa funzionalità, è necessario configurare il protocollo PIM sul router. I messaggi RGMP Hello vengono inviati agli stessi intervalli di ritrasmissione dei messaggi PIM Hello (l'impostazione predefinita è 30 secondi). I messaggi RGMP Hello precedono sempre i messaggi PIM Hello.

Bye RGMP

Ogni volta che il protocollo RGMP è disabilitato sul router, invia un messaggio RGMP Bye per segnalare allo switch che il router non sta più eseguendo il protocollo RGMP e che tutto il traffico multicast deve essere inoltrato nuovamente al router.

Join RGMP

Ogni volta che un router invia un join PIM, crea anche un join RGMP e lo invia sulla stessa interfaccia su cui deve essere inviato un join PIM. Utilizzando i diagrammi precedenti come esempio, R4 invia un messaggio di join PIM all'RP quando riceve un report IGMP dal ricevitore per il gruppo G. Inoltre, invia un join RGMP sulla stessa interfaccia, che viene quindi acquisito dallo switch S1. S1 elabora il pacchetto e aggiunge la porta del router alla voce statica di layer 2 (voce statica CAM) per il gruppo G. Ciò consente l'inoltro del traffico per il gruppo G su questa porta.

Per riepilogare:

- Il join RGMP viene inviato ogni volta che un router crea una voce (*,G) e viene inviato sulla stessa interfaccia su cui invia un messaggio di join PIM.
- Il join RGMP viene inviato ogni volta che un router crea una voce (S,G). Il router invierà un messaggio di join PIM sull'interfaccia verso S, quindi anche il messaggio di join RGMP verrà inviato sulla stessa interfaccia verso S.
- Il join RGMP viene inviato ogni volta che si invia il join PIM, ma non quando si riceve il join PIM.
- Se esistono più origini che inviano al gruppo G ed è presente una voce (*,G), verrà inviato un solo join RGMP.

Uscita RGMP

Ogni volta che un router invia un messaggio PIM Prune per un (*,G) o (S,G), verifica anche se esiste almeno un'altra voce di route per questo gruppo per l'interfaccia su cui è stata inviata la PIM Prune. Se non sono presenti altre voci, viene inviato un congedo RGMP sulla stessa interfaccia.

Cosa succede quando uno switch riceve pacchetti RGMP

Con RGMP disabilitato e lo snooping IGMP abilitato sullo switch, ogni voce di inoltro del gruppo multicast nello switch ha un elenco di porte di output che include tutte le porte del router multicast e tutte le porte su cui gli host interessati sono uniti al gruppo multicast. Quando RGMP è abilitato, vengono modificati i seguenti elementi:

- Gli switch non inviano gruppi multicast a un router compatibile con RGMP a meno che il router non ne faccia specifica richiesta (ad eccezione del gruppo riservato nell'intervallo 24.0.0.x e 224.0.1.[39-40]).
- Gli switch continuano a inviare traffico multicast da tutti i gruppi a router non compatibili con RGMP.

RGMP Hello

Quando si riceve un pacchetto RGMP Hello da una porta del router, lo switch contrassegna questa porta del router come compatibile con RGMP e il traffico multicast generale non viene più inviato a quella porta del router multicast.

Nota: i pacchetti RGMP Hello generalmente non vengono inoltrati fuori dallo chassis. I pacchetti RGMP Hello vengono inoltrati solo dopo la ricezione del primo pacchetto RGMP Hello su una porta. La porta viene quindi contrassegnata come porta RGMP e il pacchetto Hello viene inoltrato

su un'altra porta di router multicast che supporta RGMP.

Bye RGMP

Alla ricezione di RGMP Bye, deselezionare la porta del router come porta del router RGMP e aggiungere questa porta su tutti i gruppi esistenti nella VLAN.

Join RGMP

Quando si riceve un pacchetto RGMP Join per un gruppo specifico, lo switch aggiunge la porta del router da cui è stato ricevuto il pacchetto RGMP all'elenco delle porte di destinazione per quel gruppo. I join RGMP vengono inoltrati anche a tutte le porte dei router compatibili con RGMP.

Uscita RGMP

Quando si riceve un pacchetto RGMP Leave per un gruppo specifico, lo switch rimuove la porta del router dal gruppo di porte interessate a ricevere quel gruppo.

Configurazione e verifica di RGMP

Per abilitare RGMP su uno switch:

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

Per verificare l'impostazione, digitare:

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

Per configurare RGMP su un router:

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

e, se non precedentemente:

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

RGMP su Catalyst 6000 con software di sistema Cisco IOS

Il protocollo RGMP su Catalyst 6000 con software di sistema Cisco IOS ha le seguenti caratteristiche:

- Abilitata per impostazione predefinita su tutte le porte L2 (switchport) e non può essere

disabilitata
- Deve essere abilitata su qualsiasi porta multicast L3 se l'interfaccia multicast L3 è necessaria per fungere da router RGMP; a tal fine, usare il comando **ip rgmp** nella modalità interfaccia (come sui router Cisco IOS standard).

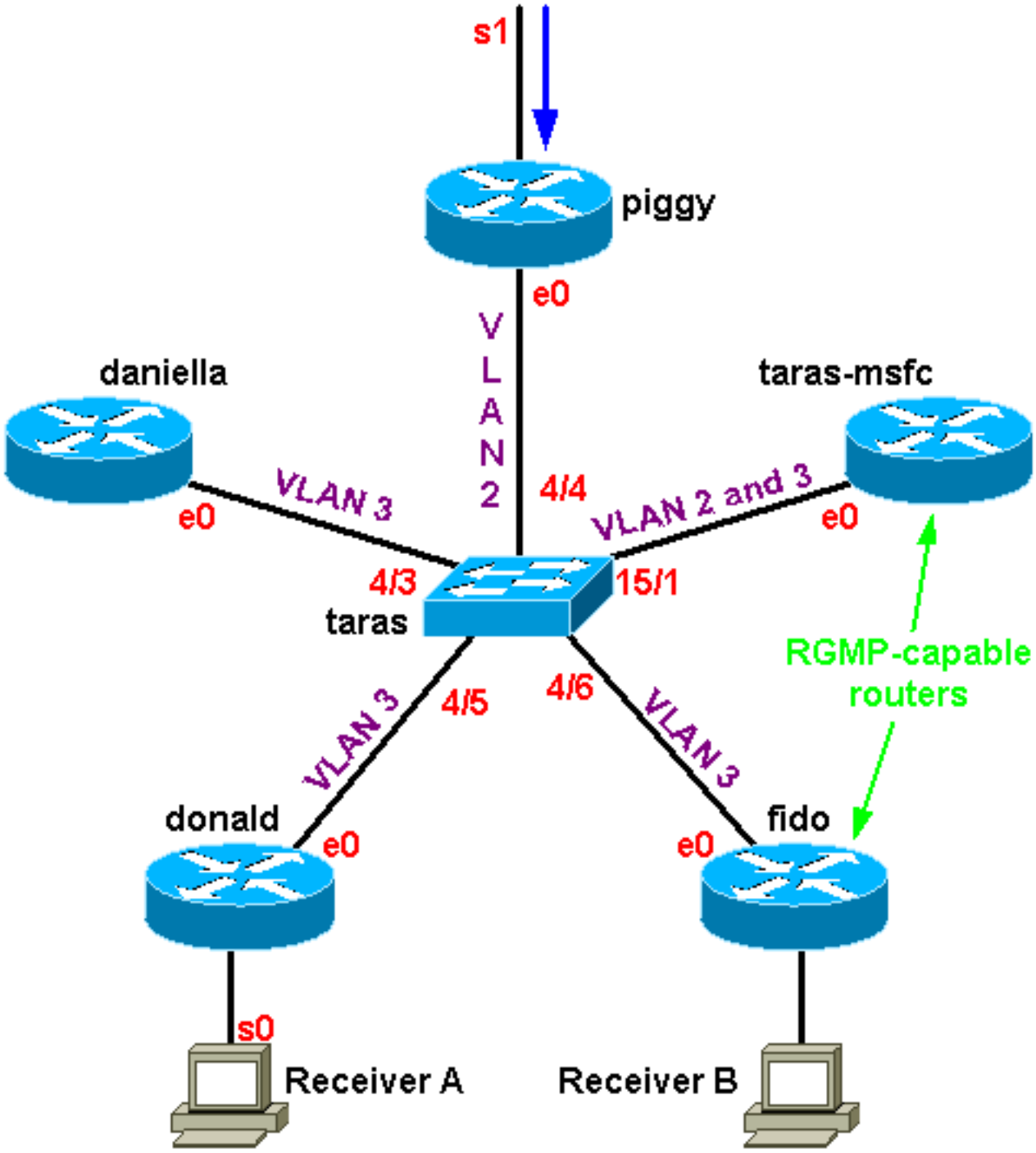
Le interfacce che eseguono RGMP e qualsiasi altro router RGMP rilevato dallo snooping IGMP possono essere verificate usando il seguente comando:

```
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#
```

Nell'output precedente viene mostrato un Catalyst 6000 con software Cisco IOS con il comando **ip rgmp** configurato sull'interfaccia VLAN 199. Sulla VLAN 199, il router è contrassegnato come compatibile con RGMP. Nel software Cisco IOS, il router è lo stesso 6500 della VLAN 199.

Case study

Il diagramma seguente rappresenta una rete reale che utilizza RGMP:



In questo caso, solo fido e l'MSFC (Multilayer Switch Feature Card) nei sistemi tara sono router compatibili con RGMP; donald, daniella e piggy sono router non compatibili con RGMP. Una sorgente multicast 4.4.4.1 sta inviando a 224.1.1.1 che si trova sul lato seriale dietro il porcile. Taras-msfc sta eseguendo il routing tra VLAN tra la VLAN 2 e la VLAN 3. La VLAN 2 non include alcun ricevitore, ma solo due ricevitori: uno dietro fido e uno dietro donald.

Nota: nella sezione successiva, si presume che l'output non preceduto da un comando specifico provenga da **debug ip rgmp** sui router e impostare trace mcast 5 sullo switch.

Abilitazione di RGMP sullo switch

In primo luogo, abilitare RGMP su taras (uno switch Catalyst 6000), presupponendo che nessuno dei router sia ancora configurato per RGMP. Non appena il protocollo RGMP è abilitato, lo switch aggiunge l'indirizzo MAC multicast 01-00-5e-00-00-19 alla tabella CAM del sistema, ossia inizia ad ascoltare tutti i pacchetti inviati a quell'indirizzo MAC. Questo è l'indirizzo che corrisponde a

224.0.0.25, utilizzato da 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
```

Abilitazione di RGMP sui router

Abilitare ora RGMP su taras-msfc e fido. Il router è configurato in modalità interfaccia e, quando il comando **debug ip rgmp** è in esecuzione, il router inizia a inviare i pacchetti RGMP Hello sull'interfaccia ogni 30 secondi.

```
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
```

Se si controlla lo switch, si osserverà che le porte 4/6 e 15/1 sono contrassegnate come porte router compatibili con RGMP. Si noti che lo switch riceve sempre un RGMP Hello subito prima di un PIM Hello:

```
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
```

Funzionamento di RGMP sulla VLAN 2

Poiché è presente un ricevitore attivo dietro Donald (non è ancora presente un ricevitore dietro Fido), il traffico multicast nella VLAN 2 deve essere inoltrato sulla VLAN 3. Quindi, l'MSFC in Tara deve ricevere il traffico sulla VLAN 2. Tuttavia, poiché RGMP è abilitato, lo switch non inoltra più il traffico multicast all'MSFC. L'MSFC deve inviare un join RGMP sulla VLAN 2 allo switch come richiesta per ricevere il gruppo.

Il router invia:

```
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
```

Il supervisore dello switch riceve le seguenti informazioni:

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

Utilizzando il gruppo **show rgmp**, è possibile verificare che la porta 15/1 è stata aggiunta al gruppo 01-00-5e-01-01-01 nella VLAN 2. Si noti che nella VLAN 3 è presente la voce CAM statica, ma l'unica porta del router inclusa nell'elenco delle porte è quella del router non compatibile con RGMP (ossia, 15/1 e 4/6 non sono nell'elenco delle porte per la voce nella VLAN 3 perché questi router sono compatibili con RGMP e non hanno inviato un join RGMP nella VLAN 3). Si noti inoltre nella tabella statica CAM che i gruppi 01-00-5e-00-01-[27,28], corrispondenti a 224.0.1.[39,40] utilizzati da auto-rp, non sono interessati dal funzionamento RGMP. Tutto il traffico per questi gruppi continua ad andare a tutti i router multicast, indipendentemente dal fatto che siano compatibili con 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
```

Osservare ora le statistiche RGMP sulla VLAN 2. Lo switch riceve regolarmente pacchetti RGMP Hello e RGMP Join. Riceve un Hello RGMP ogni 30 secondi da taras-msfc e taras-msfc invia un Join RGMP per 24.1.1.1 ogni volta che invia un Join PIM per quel gruppo:

```
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
```

Fino a questo punto, taras-msfc e fido hanno inviato solo pacchetti Hello sulla 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:
```

Operazione di unione RGMP sulla VLAN 3

Se si avvia il ricevitore B dietro il fido, il router compatibile con RGMP invierà un join RGMP allo switch per il gruppo 24.1.1.1. Lo switch lo riceverà e aggiungerà la porta 4/6 (fido) all'elenco dei

ricevitori interessati per quel gruppo nella VLAN 3.

Sul router vengono visualizzati:

```
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
```

Lo switch riceve il join RGMP e aggiunge la porta router 4/6 alla voce statica. Il risultato può essere visualizzato in diversi comandi **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
```

Operazione di uscita RGMP

Si supponga che il ricevitore B non sia più interessato, quindi fido non necessita più del traffico multicast per quel gruppo e invierà una copia PIM per il gruppo nell'interfaccia. Il router invia anche un'autorizzazione RGMP al gruppo per comunicare allo switch che non è più interessato a quel gruppo.

Quando il ricevitore B è ancora attivo, il comando **show ip route** visualizza la voce (S,G) con un flag C, per segnalare che il ricevitore è collegato e si è interessati:

```
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
```

Quando il ricevitore B non è più interessato, PIM invia un messaggio di eliminazione, ma la voce (S,G) non viene rimossa immediatamente. Il timer (evidenziato in rosso) sta effettuando il conto alla rovescia fino al timeout dell'immissione. Si noti che a questo punto, la voce è ancora presente ma con il flag P che ci dice che è potato e timeout.

```
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
```

Una volta scaduto il valore (S,G), fido invia un'autorizzazione RGMP allo switch per il gruppo 24.1.1.1:

```
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
```

Dopo che lo switch ha ricevuto il congedo RGMP, è possibile verificare nel gruppo RGMP che non sono più presenti voci per 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
```

Operazione Bye RGMP

Se si disabilita il protocollo RGMP sul router, il router invierà un byte RGMP e lo switch passerà da una porta router RGMP a una porta router normale:

Su fido:

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

Sullo 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
```

Informazioni correlate

- Supporto dei prodotti LAN
- Supporto della tecnologia di switching LAN
- Documentazione e supporto tecnico – Cisco Systems