排除ASA組播常見問題

目錄

簡介

本文檔介紹自適應安全裝置(ASA)上的組播路由和常見問題。

功能資訊

注意：有關自適應安全裝置(ASA)、Firepower威脅防禦(FTD)或安全防火牆威脅防禦(FTD)上組播路由的更新內容，請參閱以下文章：
Firepower威脅防禦IGMP和組播基礎知識故障排除
排除Firepower威脅防禦和ASA組播PIM故障

縮寫/縮寫

縮寫說明	說明
FHR	第一跳路由器 — 直接連線到組播流量源的一跳。
LHR	最後一跳路由器 — 直接連線到組播流量接收者的跳數。
RP	交匯點
DR	指定路由器
SPT	最短路徑樹
RPT	集結點(RP)樹，共用樹
RPF	反向路徑轉送
石油	傳出介面清單
MRIB	多點傳送路由資訊庫
MFIB	組播轉發資訊庫
ASM	任意來源多點傳送
BSR	啟動路由器

SSM	來源特定多點傳送
FP	快速路徑
SP	慢速路徑
CP	控制點
PPS	每秒資料包速率

ASA上的組播可以配置為以下兩種模式之一：

- PIM稀疏模式(協定無關組播:RFC 4601)
- IGMP Stub-mode(Internet組管理協定：RFC 2236)

因為ASA通過真正的組播路由協定(PIM)與鄰居通訊，所以PIM稀疏模式是首選模式。在ASA 7.0版本發佈之前，IGMP存根模式是唯一一個組播配置選項，其操作方法只是將客戶端收到的IGMP報告轉發到上游路由器。

多點傳送的元件

通常，組播基礎結構由以下元件組成：

傳送方=>發起組播流的主機或網路裝置。例如，傳送影片和/或音訊流的伺服器以及運行路由協定（如EIGRP或OSPF）的網路裝置。

接收者=>接收組播流的主機或裝置。此術語通常用於主動關注流量並使用IGMP加入或離開有問題的組播組的主機。

路由器/ASA =>負責處理組播流/流量並將其轉發到網路其他網段的網路裝置（需要時），從源到客戶端。

組播路由協定=>負責轉發組播資料包的協定。最常見的是PIM（協定無關組播），但也有其他如MOSPF的組播。

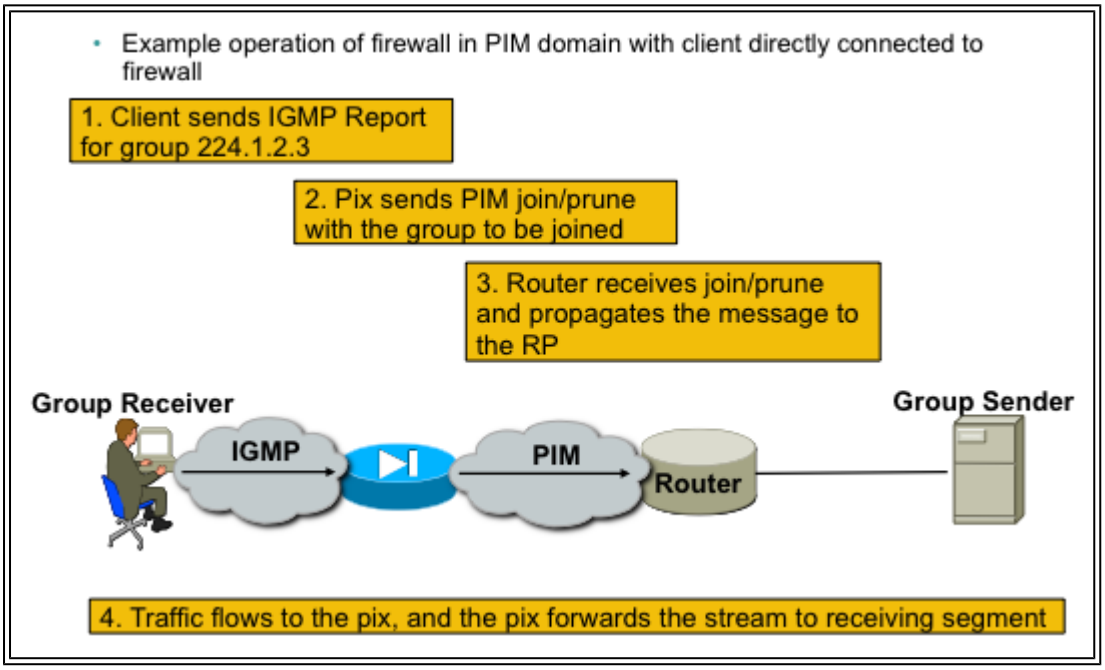
Internet組管理協定(IGMP)=>客戶端用來從特定組接收組播流的過程。

PIM稀疏模式操作

- ASA支援PIM稀疏模式和PIM雙向模式。
- 不能同時配置PIM sparse-mode和IGMP stub-mode命令。

- 使用PIM稀疏模式時，所有組播流量最初流向集結點(RP)，然後轉發到接收器。一段時間後，組播流直接從源傳輸到接收器（並繞過RP）。

此圖說明了一個常見的部署，其中ASA在一個介面上擁有組播客戶端，在另一個介面上擁有PIM鄰居：



PIM稀疏模式示例配置

1.啟用組播路由（全域性配置模式）。

<#root>

ASA(config)#

multicast-routing

2.定義PIM集結點地址。

<#root>

ASA(config)#

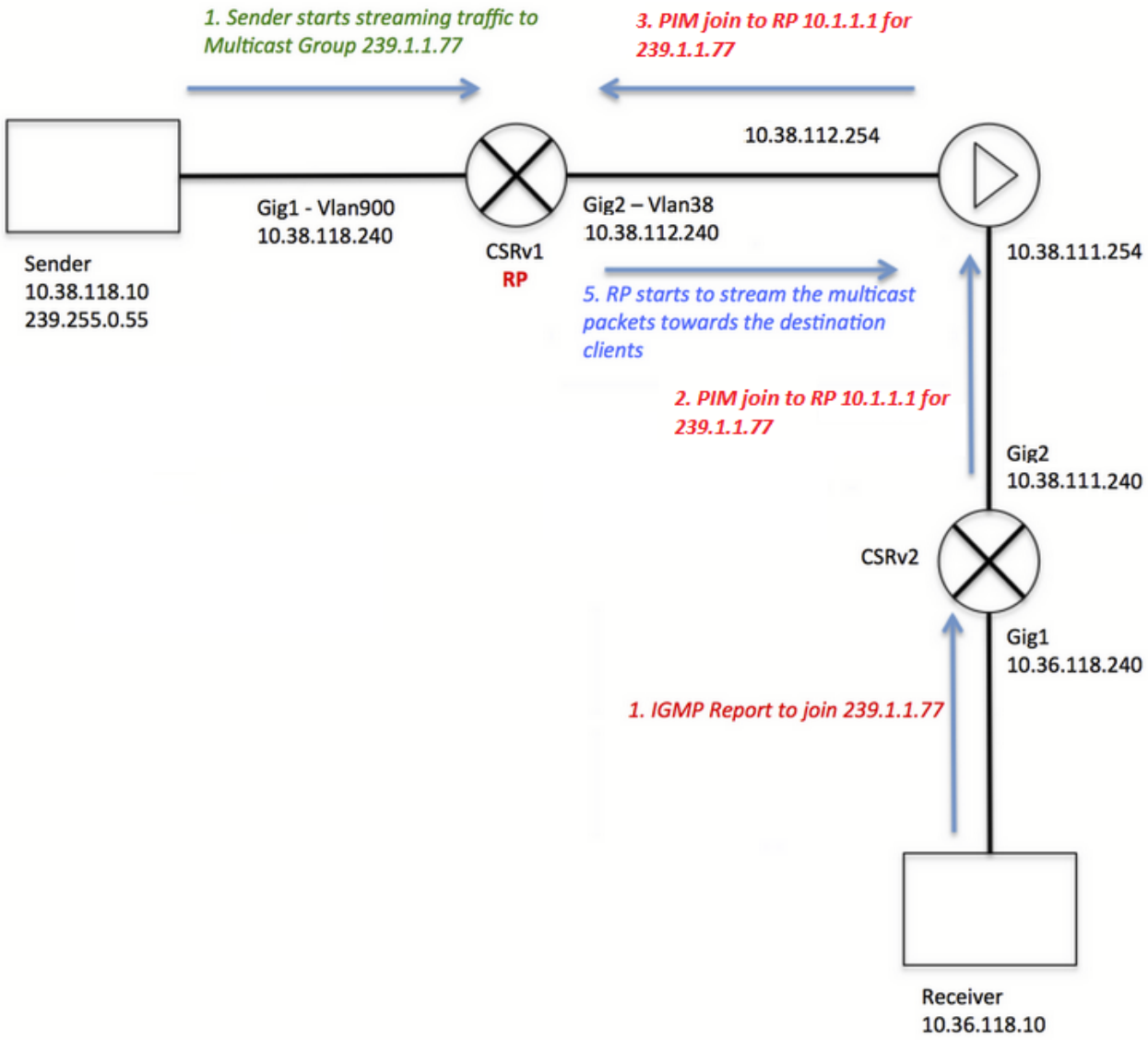
pim rp-address 172.18.123.3

3.允許組播資料包在適當的介面上進入（僅當ASA的安全策略阻止入站組播資料包時才需要）。

<#root>

```
access-list 105 extended permit ip any host 224.1.2.3
access-group 105 in interface outside
```

PIM稀疏模式示例：



請注意，客戶端IGMP註冊（紅色步驟）和伺服器接收的流（綠色步驟）的顏色不同，因此採用這種方式來證明這兩個過程可以獨立進行。

客戶端註冊步驟（紅色步驟）：

1.客戶端傳送組239.1.1.77的IGMP報告

2.路由器向為組239.1.1.77配置的靜態RP(10.1.1.1)傳送PIM加入消息。

3. ASA向RP傳送組239.1.1.77的PIM加入消息。

ASA在show mroute命令輸出中顯示PIM *、G條目：

<#root>

```
ciscoasa#
```

show mroute 239.1.1.77

```
Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State

(*, 239.1.1.77), 00:03:43/00:02:41, RP 10.1.1.1, flags: S
  Incoming interface: outside
  RPF nbr: 10.38.111.240
  Immediate Outgoing interface list:
    inside, Forward, 00:03:43/00:02:41
```

但是，由於源伺服器尚未啟動任何流，因此ASA上的「show mfib」輸出不會顯示任何收到的資料包：

<#root>

```
ciscoasa#
```

show mfib 239.1.1.77

```
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, K - Keepalive
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count

(*,239.1.1.77) Flags: C K
   Forwarding: 0/0/0/0, Other: 0/0/0
   outside Flags: A
   inside Flags: F NS
     Pkts: 0/0
```

在伺服器開始向組播組傳送任何流量之前，RP只顯示一個「*.G」條目，清單中沒有傳入介面，例如：

<#root>

```
CRSv#
```

show ip mroute 239.1.1.77

```
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, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       G - Received BGP C-Mroute, g - Sent BGP C-Mroute,
       N - Received BGP Shared-Tree Prune, n - BGP C-Mroute suppressed,
       Q - Received BGP S-A Route, q - Sent BGP S-A Route,
       V - RD & Vector, v - Vector, p - PIM Joins on route,
       x - VxLAN group
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 239.1.1.77), 00:00:02/00:03:27, RP 10.1.1.1, flags: S
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    GigabitEthernet2, Forward/Sparse-Dense, 00:00:02/00:03:27
```

一旦伺服器開始流到組播組，RP會建立「S，G」條目，並將面向傳送方的介面放在傳入介面清單中，並開始將流量下發到ASA:

<#root>

```
CRSv#
```

show ip mroute 239.1.1.77

```
...

(*, 239.1.1.77), 00:03:29/stopped, RP 10.1.1.1, flags: SF
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    GigabitEthernet2, Forward/Sparse-Dense, 00:03:29/00:02:58

(10.38.118.10, 239.1.1.77), 00:00:07/00:02:52, flags: FT
  Incoming interface: GigabitEthernet1, RPF nbr 0.0.0.0
  Outgoing interface list:
    GigabitEthernet2, Forward/Sparse-Dense, 00:00:07/00:03:22
```

使用以下命令進行驗證：

- show mroute命令顯示「S，G」條目

- show mfib命令顯示轉發資料包計數器

- show conn 命令顯示與組播組ip相關的連線

<#root>

ciscoasa#

show mroute 239.1.1.77

```
Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State

(*, 239.1.1.77), 00:06:22/00:02:50, RP 10.1.1.1, flags: S
  Incoming interface: outside
  RPF nbr: 10.38.111.240
  Immediate Outgoing interface list:
    inside, Forward, 00:06:22/00:02:50

(10.38.118.10, 239.1.1.77), 00:03:00/00:03:28, flags: ST
  Incoming interface: outside
  RPF nbr: 10.38.111.240
  Immediate Outgoing interface list:
    inside, Forward, 00:03:00/00:03:26
```

ciscoasa#

show mfib 239.1.1.77

```
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, K - Keepalive
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count

(*,239.1.1.77) Flags: C K
   Forwarding: 15/0/1271/0, Other: 0/0/0
   outside Flags: A
   inside Flags: F NS
     Pkts: 0/15
(10.38.118.10,239.1.1.77) Flags: K
   Forwarding: 7159/34/1349/360, Other: 0/0/0
   outside Flags: A
   inside Flags: F NS
     Pkts: 7159/5
```

ciscoasa#

show conn all | i 239.1.1.77

```
UDP outside  10.38.118.10:58944 inside  239.1.1.77:5004, idle 0:00:00, bytes 10732896, flags -
UDP outside  10.38.118.10:58945 inside  239.1.1.77:5005, idle 0:00:01, bytes 2752, flags -
UDP outside  10.38.118.10:58944 NP Identity Ifc  239.1.1.77:5004, idle 0:00:00, bytes 0, flags -
UDP outside  10.38.118.10:58945 NP Identity Ifc  239.1.1.77:5005, idle 0:00:01, bytes 0, flags -
```

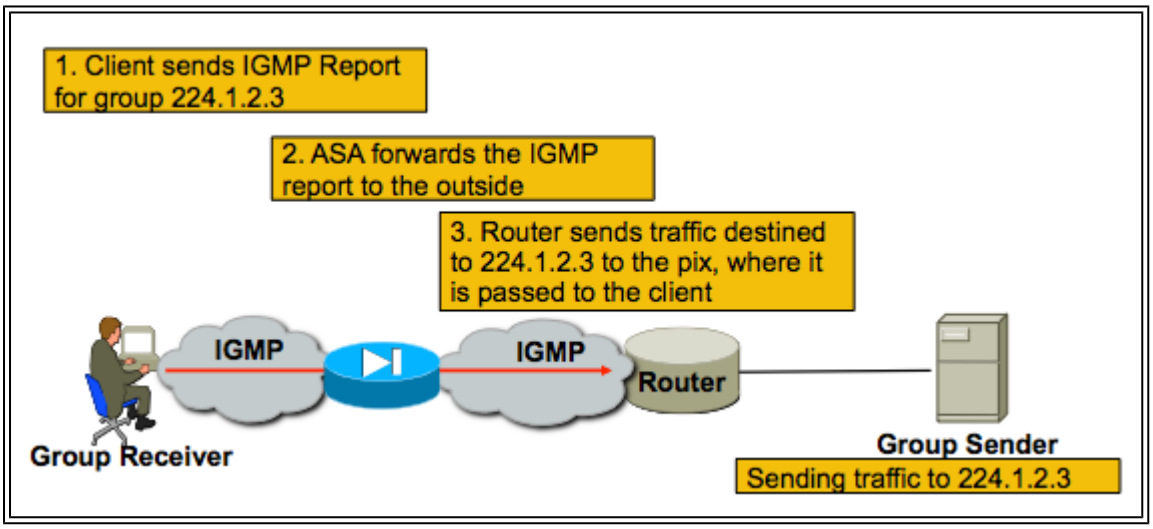
注意：一旦客戶端關閉組播客戶端應用程式，主機將傳送IGMP查詢消息。

如果這是路由器知道的唯一一台主機，因為客戶端想要接收該流，則路由器會向RP傳送IGMP修整消息。

IGMP Stub模式操作

- 在IGMP Stub模式下，ASA充當組播客戶端，生成或向相鄰路由器轉發IGMP報告（也稱為IGMP「加入」），以觸發組播流量的接收
- 路由器定期向主機傳送查詢，檢視網路上的任何節點是否希望繼續接收組播流量。
- 不建議使用IGMP末節模式，因為PIM稀疏模式比末節模式有許多優點（具有更高效的組播流量流、參與PIM的能力等）。

此圖說明為IGMP Stub模式配置的ASA的基本操作：



IGMP Stub模式配置

1.啟用組播路由（全域性配置模式）。

<#root>

```
ASA(config)#
```

multicast-routing

2.在防火牆接收igmp報告的介面上，配置igmp forward-interface命令。將資料包從介面轉發到流源。在此示例中，組播接收器直接連線到內部介面，並且組播源位於外部介面之外。

<#root>

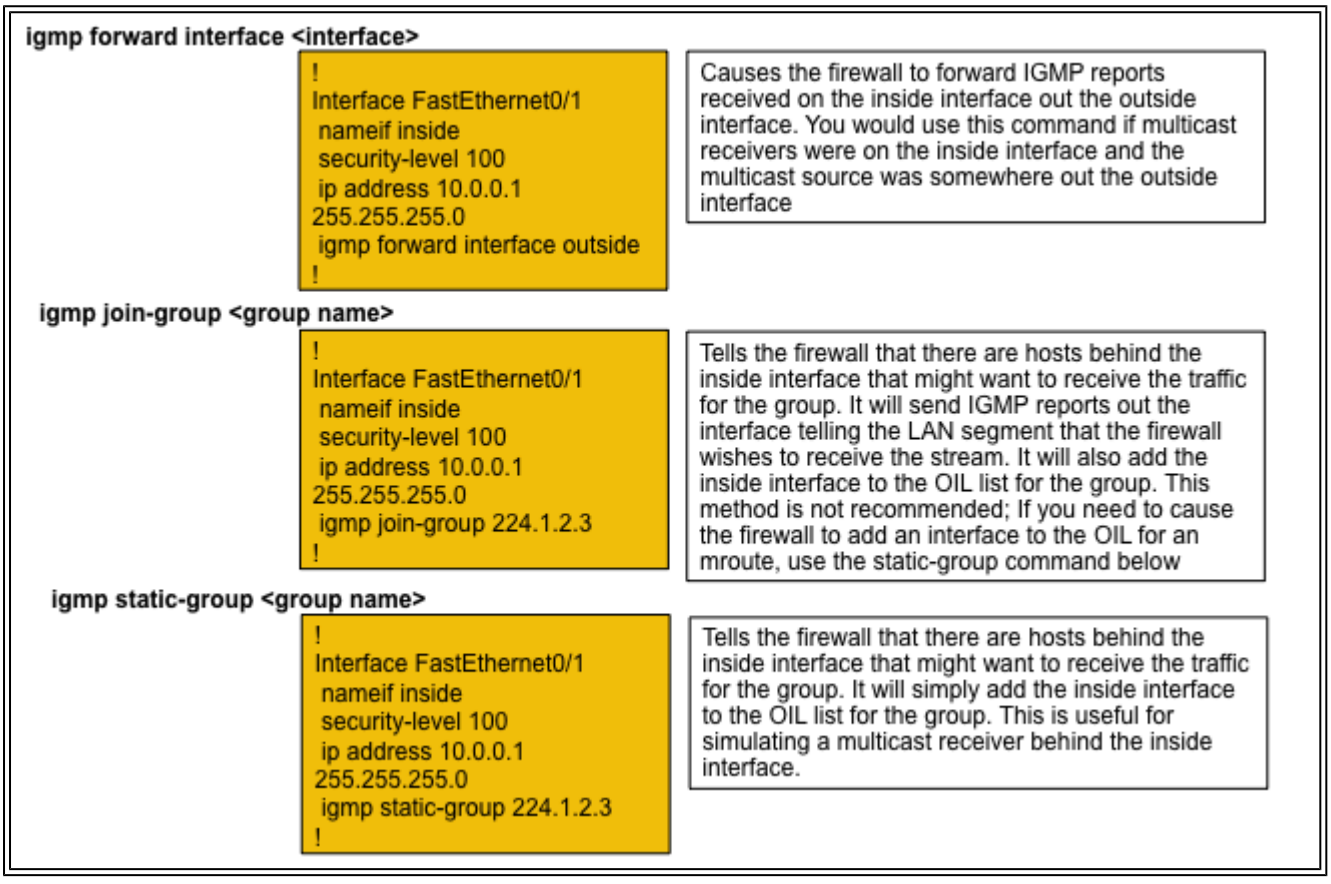
```
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
```

```
 no pim
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.0.0.1 255.255.255.0
 no pim


igmp forward interface outside

!
```

3.允許組播資料包在適當的介面上進入（僅當ASA的安全策略拒絕入站組播流量時需要這樣做）。

```
<#root>

ASA(config)#

access-list 105 extended permit ip any host 224.1.2.3

ASA(config)#

access-group 105 in interface outside
```

通常會有關於不同igmp介面子模式命令的混淆，此圖描述了何時使用每個命令：



Bidir PIM

在雙向PIM中，沒有共用樹(SPT)。這意味著三件事：

1.第一跳路由器（連線到傳送方）不將PIM註冊資料包傳送到RP。

2. RP不傳送PIM JOIN消息以加入源樹。

3.通向接收方的路徑中的路由器向RP傳送PIM加入消息以加入RPT。

這意味著ASA不會生成(S，G)，因為裝置沒有加入SPT。所有多點傳播流量都會通過RP。只要存在(*,G),ASA就會轉發所有組播流量。如果沒有(*,G)，則表示ASA從未收到PIM加入資料包。如果是這種情況，ASA不得轉發組播資料包。

Bidir PIM配置

1.啟用組播路由（全域性配置模式）。

```
<#root>

ASA(config)#

 multicast-routing
```

2.定義PIM集結點地址。

```
<#root>

ASA(config)#

pim rp-address 172.18.123.3 bidir
```

3.允許組播資料包在適當的介面上進入（僅當ASA的安全策略阻止入站組播資料包時才需要）。

```
<#root>

access-list 105 extended permit ip any host 224.1.2.3
access-group 105 in interface outside
```

故障排除方法

排除多播問題故障時要收集的資訊

為了完全瞭解和診斷ASA上的組播轉發問題，需要以下部分或全部資訊：

·網路拓撲描述、組播傳送方、接收方和交匯點的位置。
·特定的組IP地址，以及使用的埠和協定。
·組播流出現故障時ASA生成的系統日誌。
· ASA命令列介面的特定show命令輸出：

<#root>

```
show mroute
show mfib
show pim neighbor
show route
show tech-support
```

·資料包捕獲，顯示組播資料是否到達ASA，以及資料包是否通過ASA轉發(注意資料包的IP生存時間(TTL)。這可以通過命令「show capture x detail」看到)
·IGMP和/或PIM資料包的資料包捕獲。範例：

<#root>

```
capture cap1 interface outside match ip any host 239.1.1.77

  >>> This captures the multicast traffic itself

capture cappim1 interface inside match pim any any

         >>> This captures PIM Join/Prune messages

capture capigmp interface inside match igmp any any

          >>> This captures IGMP Report/Query messages
```

·來自相鄰組播裝置（路由器）的資訊，如「show mroute」和「show mfib」。
·資料包捕獲和/或show命令，以確定ASA是否丟棄組播資料包。「show asp drop」命令可用於確定ASA是否丟棄資料包。此外，型別為「asp-drop」的資料包捕獲可用於捕獲ASA丟棄的所有資料包，然後檢查丟棄捕獲中是否存在組播資料包。

有用的顯示命令輸出

show mroute命令輸出會顯示不同的組和轉發資訊，非常類似於IOS show mroute 命令。show mfib命令會顯示各種多點傳播組的轉送狀態。觀察轉送封包計數器和其他（表示捨棄）尤其重要：

<#root>

```
ciscoasa#

show mfib

Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, K - Keepalive
```

```
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.1.2.3) Flags: S K
   Forwarding: 0/0/0/0, Other: 0/0/0
   inside Flags: F
     Pkts: 0/0
(192.168.1.100,224.1.2.3) Flags: K
   Forwarding: 6749/18/1300/182, Other: 690/0/690
   outside Flags: A
   inside Flags: F
     Pkts: 6619/8
(*,232.0.0.0/8) Flags: K
   Forwarding: 0/0/0/0, Other: 0/0/0
ciscoasa#
```

clear mfib counters 命令可用於清除計數器，這在測試期間非常有用：

```
<#root>

ciscoasa#

clear mfib counters
```

封包擷取

板載資料包捕獲實用程式對於解決組播問題非常有用。在本範例中，擷取DMZ介面上所有目的地為239.17.17.17的輸入封包：

```
<#root>

ciscoasa#

capture dmzcap interface dmz


ciscoasa#

capture dmzcap match ip any host 239.17.17.17

ciscoasa#

show cap dmzcap


324 packets captured

   1: 17:13:30.976618       802.1Q vlan#301 P0 10.1.123.129.2000 > 239.17.17.17.16384:  udp 172
   2: 17:13:30.976679       802.1Q vlan#301 P0 10.1.123.129.2000 > 239.17.17.17.16384:  udp 172
   3: 17:13:30.996606       802.1Q vlan#301 P0 10.1.123.129.2000 > 239.17.17.17.16384:  udp 172
```

```
   4: 17:13:30.996652       802.1Q vlan#301 P0 10.1.123.129.2000 > 239.17.17.17.16384:  udp 172
   5: 17:13:31.016676       802.1Q vlan#301 P0 10.1.123.129.2000 > 239.17.17.17.16384:  udp 172
   6: 17:13:31.016722       802.1Q vlan#301 P0 10.1.123.129.2000 > 239.17.17.17.16384:  udp 172
....
```

show capture x detail 命令的輸出顯示了資料包的TTL，這非常有用。在此輸出中，封包的TTL為1（且ASA會傳遞此封包，因為它不會預設降低IP封包的TTL），但下游路由器會捨棄封包：

<#root>

ASA#

show cap capout detail

```
453 packets captured
...
   1: 14:40:39.427147 c062.6baf.8dc3 0100.5e7f.02c3 0x8100 Length: 1362
      802.1Q vlan#1007 P0 10.4.2.95.1806 > 239.255.2.195.5000:  [udp sum ok] udp 1316 (DF) [ttl 1] (id
```

資料包捕獲對於捕獲PIM和IGMP流量也很有用。此擷取顯示內部介面已收到來源為10.0.0.2的IGMP封包（IP通訊協定2）：

<#root>

ciscoasa#

capture capin interface inside

ciscoasa#

capture capin match igmp any any

ciscoasa#

show cap capin

```
1 packets captured
1: 10:47:53.540346 802.1Q vlan#15 P0 10.0.0.2 > 224.1.2.3:  ip-proto-2, length 8
ciscoasa#
```

請注意，使用「show capture x detail」命令可看到封包的TTL。

在此我們可以看到已獲取的ASP丟棄捕獲，其中顯示丟棄的多播資料包以及丟棄的原因(punt-rate-limit):

<#root>

ASA#

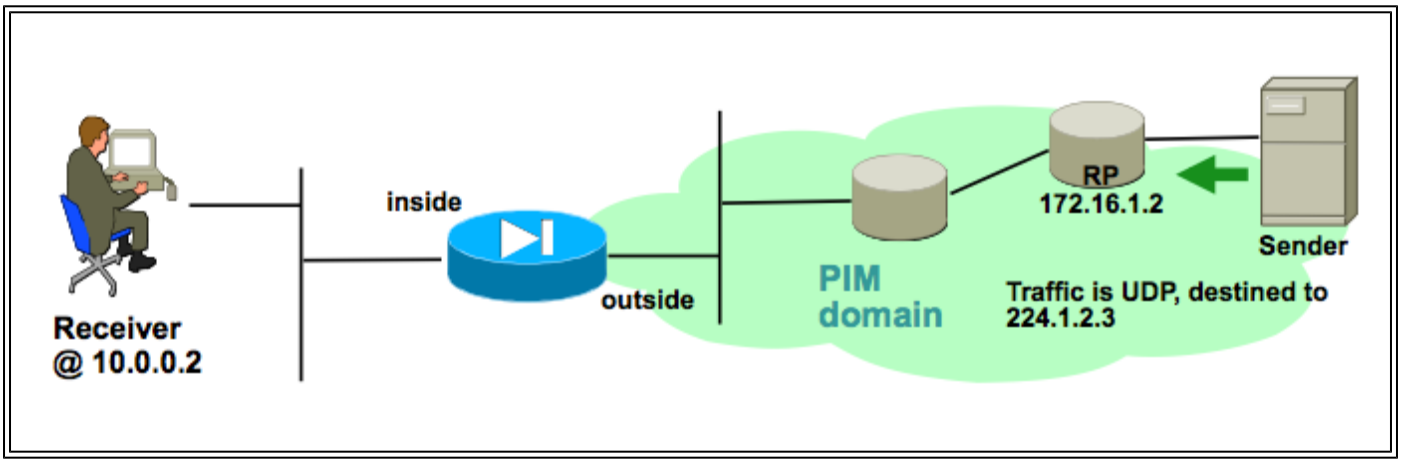
```
show cap capasp det

 12: 14:37:26.538332 c062.6baf.8dc3 0100.5e7f.02c3 0x8100 Length: 1362
      802.1Q vlan#1007 P0 10.76.4.95.1806 > 239.255.2.195.5000:  [udp sum ok] udp 1316 (DF) [ttl 1] (id
  13: 14:37:26.538439 c062.6baf.8dc3 0100.5e7f.02c3 0x8100 Length: 1362
      802.1Q vlan#1007 P0 10.76.4.95.1806 > 239.255.2.195.5000:  [udp sum ok] udp 1316 (DF) [ttl 1] (id
```

ASA PIM稀疏模式組播部署示例

此圖說明ASA如何在PIM稀疏模式下與鄰居裝置互動。

瞭解網路拓撲

準確確定特定組播流的傳送者和接收者的位置。此外，還要確定組播組的IP地址以及交匯點的位置。



在這種情況下，可以在ASA的外部介面接收資料，然後轉發到內部介面上的組播接收器。由於接收方與ASA的內部介面位於同一個IP子網中，因此當客戶端請求接收資料流時，預計會在內部介面收到IGMP報告。傳送方的IP地址為192.168.1.50。

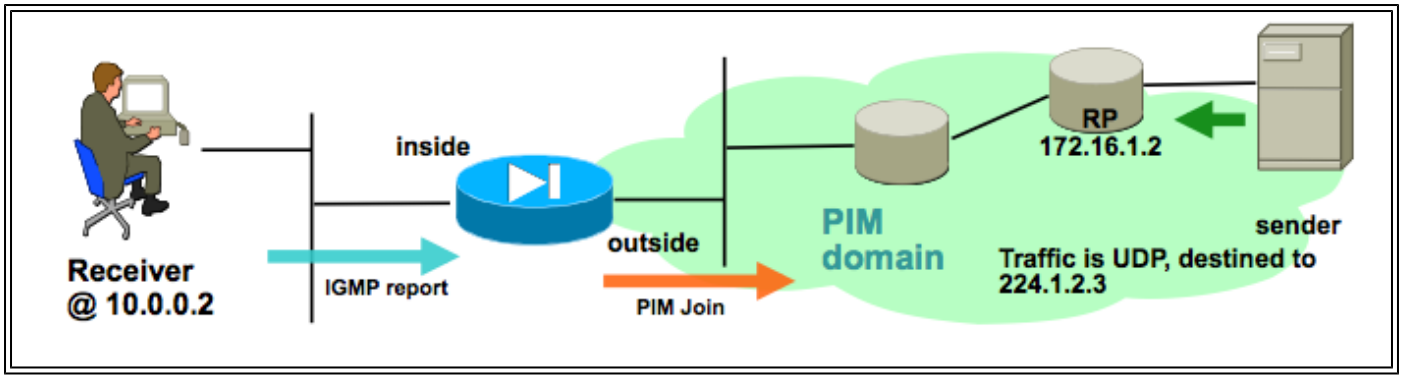
驗證ASA是否從接收方收到IGMP報告

在本示例中，IGMP報告由接收方生成並由ASA處理。

資料包捕獲和debug igmp的輸出可用於驗證ASA是否收到並成功處理了IGMP消息。

驗證ASA是否向交匯點傳送PIM加入消息

ASA解釋IGMP報告並生成PIM加入消息，然後將其從介面傳送到RP。

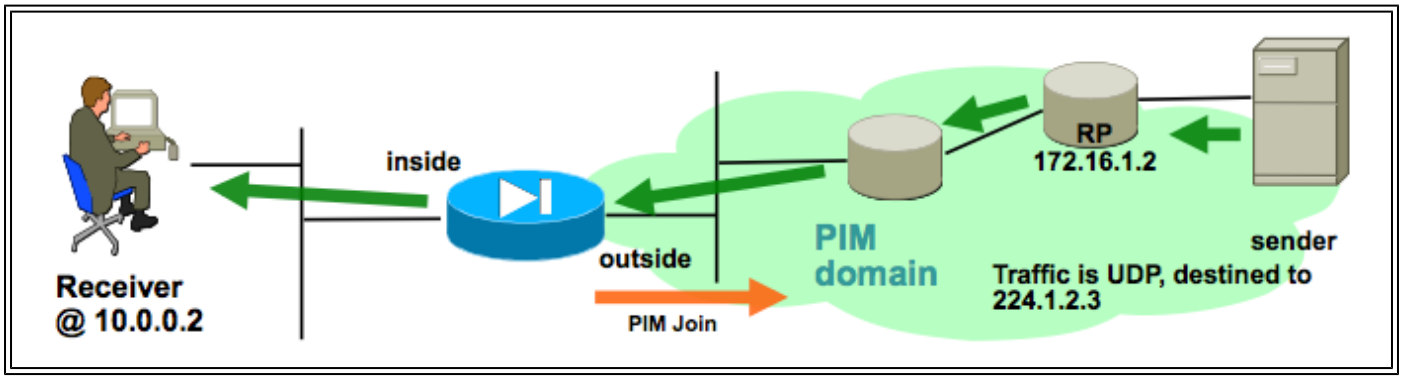


此輸出來自debug pim group 224.1.2.3並顯示ASA成功傳送PIM加入消息。組播流的傳送方是192.168.1.50。

```
IPv4 PIM: (*,224.1.2.3) J/P processing
IPv4 PIM: (*,224.1.2.3) Periodic J/P scheduled in 50 secs
IPv4 PIM: (*,224.1.2.3) J/P adding Join on outside
IPv4 PIM: (*,224.1.2.3) inside Processing timers
IPv4 PIM: Sending J/P message for neighbor 10.2.3.2 on outside for 1 groups
IPv4 PIM: [0] (192.168.1.50,224.1.2.3/32) MRIB update (a=0,f=0,t=1)
IPv4 PIM: [0] (192.168.1.50,224.1.2.3/32) outside MRIB update (f=20,c=20)
IPv4 PIM: [0] (192.168.1.50,224.1.2.3) Signal present on outside
IPv4 PIM: (192.168.1.50,224.1.2.3) Create entry
IPv4 PIM: [0] (192.168.1.50,224.1.2.3/32) outside MRIB modify NS
IPv4 PIM: Adding monitor for 192.168.1.50
```

驗證ASA接收並轉發組播流

ASA開始接收外部介面上的組播流量（以綠色箭頭所示），並將其轉發到內部接收方。



show mroute和show mfib命令以及資料包捕獲可用於驗證ASA接收和轉發組播資料包。

連線表內建立了連線來表示組播流：

```
<#root>

ciscoasa#

show conn

59 in use, 29089 most used
...
```

```
UDP outside:192.168.1.50/52075 inside:224.1.2.3/1234 flags -
...
```

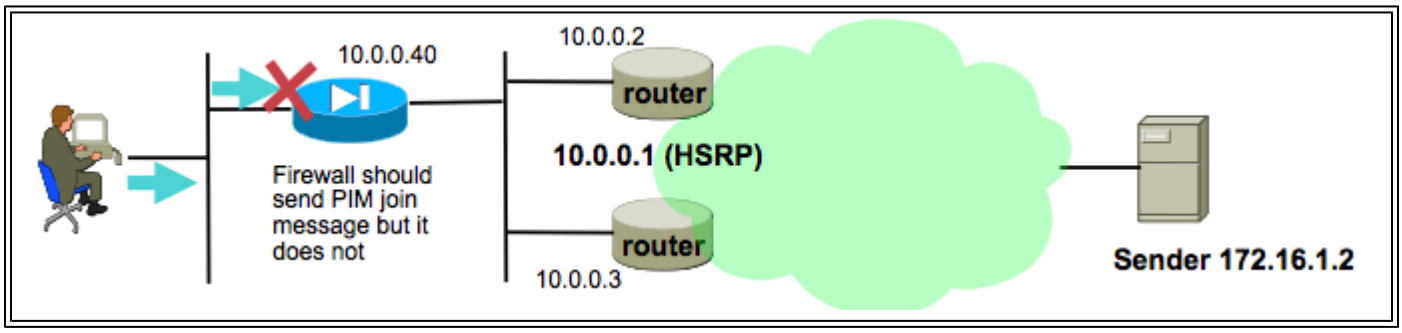
資料分析

常見問題

本節提供了一系列與實際ASA組播相關的問題

由於HSRP，ASA無法向上游路由器傳送PIM消息

遇到此問題時，ASA無法通過介面傳送任何PIM消息。此圖顯示ASA無法向傳送方傳送PIM消息，但是當ASA需要向RP傳送PIM消息時，會出現相同的問題。



debug pim 命令的輸出顯示ASA無法將PIM消息傳送到上游下一跳路由器：

```
IPv4 PIM: Sending J/P to an invalid neighbor: outside 10.0.0.1
```

此問題並非特定於ASA，而且還會影響路由器。此問題是由路由表配置和PIM鄰居使用的HSRP配置的組合觸發的。

路由表指向HSRP IP 10.0.0.1作為下一跳裝置：

```
<#root>

ciscoasa#

show run route

route outside 0.0.0.0 0.0.0.0 10.0.0.1 1
```

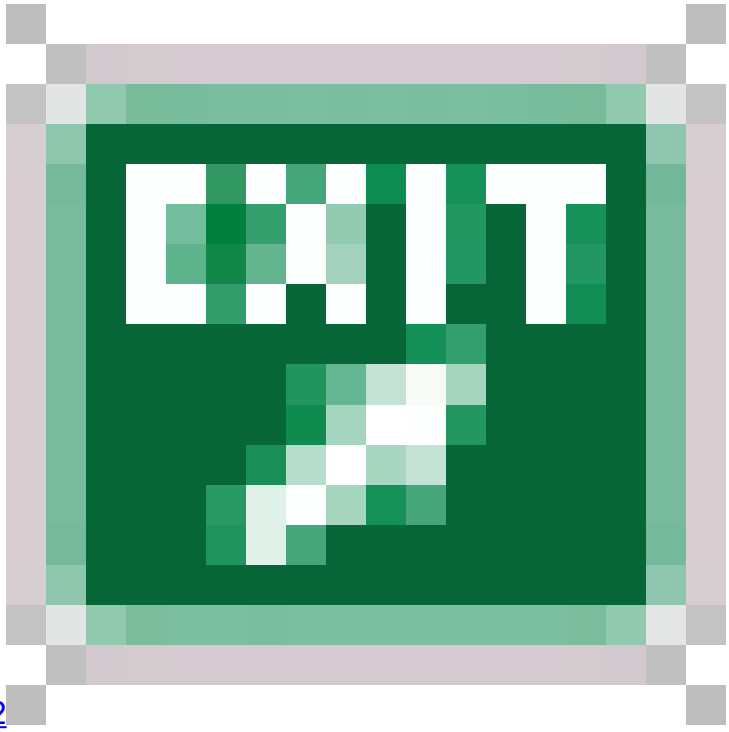
但是，在路由器的物理介面IP地址之間形成PIM鄰居關係，而不是HSRP IP:

```
<#root>
```

```
ciscoasa#
show pim neighbor
Neighbor Address  Interface          Uptime    Expires DR pri Bidir
10.0.0.2          outside            01:18:27  00:01:25 1
10.0.0.3          outside            01:18:03  00:01:29 1 (DR)
```

有關詳細資訊，請參閱PIM稀疏模式為什麼不能與到HSRP地址的靜態路由配合使用？。

檔案節錄：



為什麼路由器不傳送加入/修剪消息？ RFC 2362
「路由器定期向與每個(S，G)、(*,G)和(*,*,RP)條目關聯的每個不同RPF鄰居傳送加入/修剪消息。只有當RPF鄰居是PIM鄰居時，才會傳送加入/修整消息。

為了緩解問題，請在ASA上為相關流量新增一個靜態mroute條目。確保它指向兩個路由器介面IP地址（10.0.0.2或10.0.0.3）之一。在本例中，此命令允許ASA傳送指向組播傳送方172.16.1.2的PIM消息：

<#root>

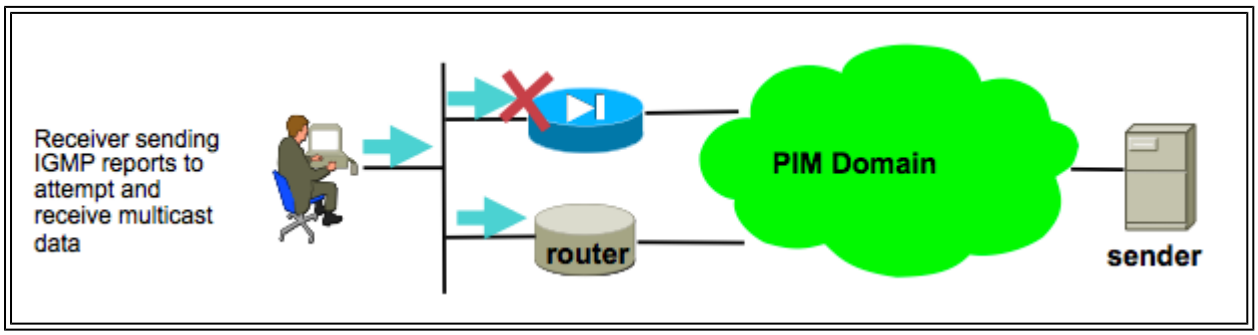
```
ciscoasa(config)#
mroute 172.16.1.2 255.255.255.255 10.0.0.3
```

完成此操作後，組播路由表將覆蓋ASA的單播路由表，ASA將PIM消息直接傳送到10.0.0.3鄰居。

ASA忽略IGMP報告，因為它不是LAN網段上的指定路由器

對於此問題，ASA從直接連線的組播接收方收到IGMP報告，但忽略該報告。不生成調試輸出，資料

包被簡單地丟棄，資料流接收失敗。



對於此問題，ASA會忽略該資料包，因為它不是客戶端所在的LAN網段上選擇的指定路由器。

此ASA CLI輸出顯示不同的裝置是內部介面網路上的指定路由器（以「DR」表示）：

<#root>

ciscoasa#

show pim neighbor

```
 Neighbor Address  Interface          Uptime    Expires DR pri Bidir
 192.168.1.2       outside             01:18:27  00:01:25 N/A>
 10.0.0.2          inside              01:18:03  00:01:29 1
```

(DR)

預設情況下，將multicast-routing命令新增到配置中時，在所有ASA介面上啟用PIM。如果ASA的內部介面（客戶端所在的位置）上有其他PIM鄰居（其他路由器或ASA），並且這些鄰居之一因該段的DR而被選中，則其他非DR路由器丟棄IGMP報告。解決方案是在介面上禁用PIM(在涉及的介面上使用 no pim命令)，或通過pim dr-priority介面命令將ASA設定為網段的DR。

超過IGMP介面限制時，防火牆會拒絕IGMP報告

預設情況下，ASA允許在介面上跟蹤500個當前活動聯接（報告）。這是可配置的最大值。如果某個介面的客戶端請求大量組播流，最多可以達到500個活動加入，並且ASA可以忽略來自組播接收器的其他入站IGMP報告。

要確認這是否是組播故障的原因，請發出命令「show igmp interface interfacename」並查詢該介面的「IGMP limit」資訊。

<#root>

ASA#

show igmp interface inside

```
Hosting-DMZ is up, line protocol is up
  Internet address is 10.11.27.13/24
  IGMP is enabled on interface
```

```
  Current IGMP version is 2
  IGMP query interval is 125 seconds
  IGMP querier timeout is 255 seconds
  IGMP max query response time is 10 seconds
  Last member query response interval is 1 seconds
  Inbound IGMP access group is:
```

IGMP limit is 500, currently active joins: 500

```
  Cumulative IGMP activity: 7018 joins, 6219 leaves
  IGMP querying router is 10.11.27.13 (this system)
```

```
DEBUG - IGMP: Group x.x.x.x limit denied on outside
```

ASA無法轉發232.x.x.x/8範圍內的組播流量

此地址範圍用於ASA當前不支援的源特定組播(SSM)。

debug igmp命令的輸出顯示以下錯誤：

```
IGMP: Exclude report on inside ignored for SSM group 232.179.89.253
```

由於反向路徑轉發檢查，ASA丟棄組播資料包

在這種情況下，ASA在介面上接收組播流量，但不會將其轉發到接收方。ASA丟棄資料包，因為它們未通過反向路徑轉發(RPF)安全檢查。RPF在所有介面上為組播流量啟用，且無法禁用(對於單播資料包，預設情況下檢查未啟用，並使用ip verify reverse-path interface命令啟用)。

由於RPF檢查，當在介面上收到組播流量時，ASA會檢查是否有路由返回到該介面上的組播流量源（它檢查單播和組播路由表）。如果它沒有通往傳送方的路由，則會丟棄資料包。在show asp drop的輸出中可將這些丟棄視為計數器：

<#root>

```
ciscoasa(config)#
```

show asp drop

```
Frame drop:
  Invalid UDP Length                                       2
  No valid adjacency                                      36
  No route to host                                      4469
  Reverse-path verify failed                          121012
```

一個選項是為流量的傳送者新增mroute。在本示例中，mroute命令用於滿足對外部介面上接收的源自172.16.1.2的組播流量的RPF檢查：

```
<#root>

ciscoasa(config)#

mroute 172.16.1.2 255.255.255.255 outside
```

ASA在PIM切換到源樹時不會生成PIM加入

最初，PIM稀疏模式組播資料包從組播傳送方流到RP，然後通過共用組播樹從RP流到接收方。但是，一旦聚合位元率達到特定閾值，最接近組播接收方的路由器會嘗試沿源特定樹接收流量。此路由器為組生成新的PIM加入，並將其傳送到組播流的傳送方（而不是像以前那樣傳送到RP）。

組播流量的傳送方可以駐留在RP以外的其他ASA介面上。當ASA收到PIM加入以切換到源特定樹時，ASA必須具有到達傳送方IP地址的路由。如果沒有找到此路由，則會丟棄PIM加入資料包，並在debug pim的輸出中看到此消息

```
NO RPF Neighbor to send J/P
```

此問題的解決方案是為流的傳送方新增靜態路由條目，指出傳送方所在的ASA介面。

由於超過生存時間(TTL),ASA丟棄組播資料包

在這種情況下，由於封包的TTL太低，多點傳播流量會失敗。這會導致ASA或網路中的其他裝置丟棄它們。

組播資料包的IP TTL值通常由傳送它們的應用程式設定。有時，預設情況下這樣做是為了幫助確保組播流量不會在網路中傳輸過遠。例如，預設情況下， LAN 客戶端應用（常用的組播發射器和測試工具）將IP資料包中的TTL預設設定為1。

由於特定組播拓撲，ASA的CPU使用率較高，並且丟包

如果關於組播拓撲的所有這些條件都成立，則ASA可能會遇到高CPU使用率，而組播流可能會遇到丟包情況：

1. ASA充當RP。
2. ASA是組播流的第一跳接收方。這表示多點傳送傳送傳送者與ASA介面位於同一個IP子網路中。
3. ASA是組播流的最後一個跳路由器。這意味著組播接收器與ASA介面位於同一個IP子網中。

如果遇到所有上述症狀，則 由於設計限制，ASA被迫處理切換組播流量。這會導致資料速率較高的組播流經歷丟包。當丟棄這些資料包時，show asp drop計數器會遞增，該計數器是punt-rate-

limit。

要確定ASA是否存在此問題，請完成以下步驟：

第1步：檢查ASA是否為RP:

<#root>

```
show run pim
show pim tunnel
```

第2步：檢查ASA是否為最後一跳路由器：

<#root>

```
show igmp group
```

<mcast_group_IP>

第3步：檢查ASA是否為第一跳路由器：

<#root>

```
show mroute
```

<mcast_group_IP>

可以採取以下步驟來緩解此問題：

— 修改拓撲，使ASA不是RP。或者，使傳送方或接收方未直接連線到ASA

— 使用IGMP stub-mode而不是PIM進行組播轉發。

首次啟動組播流時，ASA丟棄前幾個資料包

當組播流的第一個資料包到達ASA時，ASA必須構建該特定組播連線和相關的mroute條目以轉發資料包。當條目處於建立過程中時，一些組播資料包可能會被丟棄，直到路由和連線建立完畢（通常這只需不到一秒鐘）。組播流設定完成後，資料包不再受速率限制。

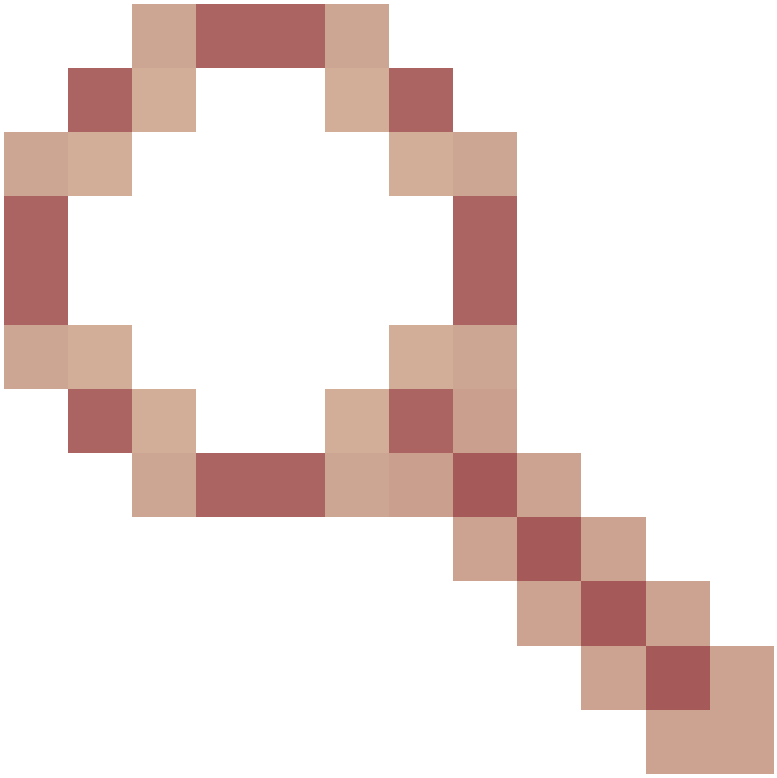
因此丟棄的資料包的ASP丟棄原因為「(punt-rate-limit)Punt rate limit exceeded」。這是「show capture asp」的輸出（其中asp是在ASA上配置的ASP丟棄捕獲，用於捕獲丟棄的資料包），您可以看到由於以下原因而丟棄的多播資料包：

<#root>

```
ASA #

show capture asp

2 packets captured
   1: 16:14:49.419091 10.23.2.2.810 > 239.255.123.123.890:  udp 32 Drop-reason: (punt-rate-limit) Punt
   2: 16:14:49.919172 10.23.2.2.810 > 239.255.123.123.890:  udp 32 Drop-reason: (punt-rate-limit) Punt
2 packets shown
```

斷開多播接收器會中斷其它介面上的多播組接收

只有在IGMP Stub模式下運行的ASA才會遇到此問題。參與PIM組播路由的ASA不受影響。



此問題是由思科錯誤ID CSCeg48235識別的
一個介面上的IGMP保留會中斷其他介面上的組播流量。

以下是錯誤的版本說明，其中說明問題：

```
Symptom:
When a PIX or ASA firewall is configured for IGMP stub mode multicast reception and traffic from a mult

The problem is triggered when the firewall forwards the IGMP leave for the group towards the upstream d

Conditions:
The PIX or ASA must be configured for IGMP stub mode multicast. IGMP stub mode is a legacy multicast fo

Workarounds:
1) Use PIM multicast routing instead of IGMP stub mode.
2) Decrease multicast IGMP query timers so that the receivers are queried more frequently, so their IGM
```

由於出站訪問清單的安全策略，ASA丟棄組播資料包

對於此特定問題，ASA丟棄組播資料包（根據配置的安全策略）。但是，網路管理員很難確定丟包的原因。在這種情況下，由於為介面配置的出站訪問清單，ASA將丟棄資料包。因應措施是允許傳出存取清單中的多點傳送流。

發生這種情況時，組播資料包將使用ASP丟棄計數器「FP no mcast output intrf(no-mcast-intrf)」丟棄。

由於控制點速率限制，ASA連續丟棄組播流中的某些資料包（但不是全部）

流量最有可能受到控制點的速率限制，這是由於punt-rate-limit。檢視asp drop輸出和捕獲以確認：

<#root>

ASA#

show asp drop

```
Frame drop:
  Punt rate limit exceeded (punt-rate-limit)                                  1492520
```

```
ASA#  show cap capasp det
 12: 14:37:26.538332 c062.6baf.8dc3 0100.5e7f.02c3 0x8100 Length: 1362
      802.1Q vlan#1007 P0 10.76.4.95.1806 > 239.255.2.195.5000:  [udp sum ok] udp 1316 (DF) [ttl 1] (id
```

mfib條目顯示所有流量都進行進程交換：

<#root>

ASA(config)#

show mfib 239.255.2.1195

```
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, K - Keepalive
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count

(*,239.255.2.195) Flags: C K
   Forwarding: 4278/50/1341/521, Other: 0/0/0
   Outside-1007 Flags: A
   RDEQ-to-Corporate Flags: F NS
     Pkts: 0/4278                                <---- HERE
```

組播路由表顯示(*,G)，但沒有(S，G)。

```
<#root>

ASA(config)#

show mroute  239.255.2.1195

Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State

(*, 239.255.2.195), 00:44:03/00:02:44, RP 10.1.135.10, flags: S
  Incoming interface: Outside-1007
  RPF nbr: 10.100.254.18
  Immediate Outgoing interface list:
    RDEQ-to-Corporate, Forward, 00:44:03/00:02:44
```

這裡的問題是，到達ASA的資料包組播資料包的TTL是1。ASA正在將這些資料包轉發到下游裝置（因為它不會減少TTL），但路由器下游將丟棄這些資料包。因此，下游路由器不會將PIM(S，G)聯接（特定於源的聯接）傳送到ASA到傳送方。ASA在收到此PIM加入之前不會生成(S，G)條目。由於(S，G)未構建，因此所有組播流量都會進行進程交換，從而產生速率限制。

此問題的解決方法是確保資料包的TTL不是1，這允許下游裝置向傳送方傳送源特定的連線；這會導致ASA在表中安裝源特定的路由，然後所有資料包都進行快速交換（而不是處理交換），並且流量必須順利通過ASA。

組播流因PIM ASSERT消息而停止

如果兩個網路裝置將相同的組播資料包轉發到同一子網，則理想情況下，其中一個網路裝置必須停止轉發這些資料包（因為複製資料流是浪費）。如果運行PIM的路由器檢測到它們接收到與它們也在同一介面上生成的相同資料包，則它們會在該LAN上生成ASSERT消息以選擇哪個網路裝置停止轉發該流。

有關此消息的更多資訊，請參閱與ASSERT過程相關的RFC 4601一節。

調試顯示，ASA收到組239.1.1.227的IGMP報告，但由於它收到來自相鄰路由器的斷言消息，它忽略了該報告：

```
IPv4 PIM: (*,239.1.1.227) Periodic J/P scheduled in 50 secs
IPv4 PIM: (*,239.1.1.227) J/P adding Join on outside
IPv4 PIM: (10.99.41.205,239.1.1.227)RPT J/P adding Prune on outside
IPv4 PIM: (10.99.41.253,239.1.1.227)RPT J/P adding Prune on outside
IGMP: Received v2 Report on inside from 10.20.213.204 for 239.1.1.227
IGMP: Updating EXCLUDE group timer for 239.1.1.227
IPv4 PIM: (10.99.41.253,239.1.1.227) Received [15/110] Assert from 10.20.13.2 on inside
IPv4 PIM: (10.99.41.253,239.1.1.227) Assert processing message wins
IPv4 PIM: (10.99.41.253,239.1.1.227) inside Update assert timer (winner 10.20.13.2)
```

在生產網路中觀察到此問題，其中兩個站點在第2層意外橋接，因此組播接收器所在的LAN有兩個裝置向它們轉發組播流量。由於另一個網路問題，ASA和其他裝置無法通過PIM hello檢測到對方，因此它們都承擔了LAN的指定路由器角色。這導致組播流量工作一段時間，然後在裝置傳送ASSERT消息時失敗。為了解決此問題，在第2層橋接裝置的錯誤連線被禁用，然後問題得以解決。

ASA傳送PIM加入，但由於資料包大小大於MTU，因此鄰居不處理該加入

在1996年觀察到這629575899情況。ASA配置為巨型幀，而4900未配置。當客戶端請求超過73個多播流時，某些多播流無法工作。73個SG會建立大小為1494的PIM加入消息，該消息仍在MTU內。74SG會建立大於1500的PIM加入消息，這導致4900M丟棄入站資料包。

此問題的解決方法為：

1.確保在4900M上全域性啟用巨型幀

2.使用MTU 9216配置物理介面和SVI

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。