排除ASA组播常见问题

目录

简介

本文档介绍自适应安全设备(ASA)上的组播路由和常见问题。

功能信息

注意：有关自适应安全设备(ASA)、Firepower威胁防御(FTD)或安全防火墙威胁防御(FTD)上组播路由的更新内容，请参阅以下文章：
Firepower威胁防御IGMP和组播基础故障排除
排除Firepower威胁防御和ASA组播PIM故障

缩写/缩写

缩写词	说明
FHR	第一跳路由器 — 直接连接到组播流量源的一跳。
LHR	最后一跳路由器 — 直接连接到组播流量接收器的跳。
RP	交汇点
DR	指定路由器
SPT	最短路径树
RPT	交汇点(RP)树、共享树
RPF	反向路径转发
石油	传出接口列表
MRIB	组播路由信息库
MFIB	组播转发信息库
ASM	任意源组播
BSR	Bootstrap路由器

SSM	源特定组播
FP	快速路径
服务提供商	慢速路径
CP	控制点
PPS	每秒数据包速率

ASA上的组播可以配置为以下两种模式之一：

- PIM稀疏模式(协议无关组播:RFC 4601)
- IGMP末节模式(互联网组管理协议:RFC 2236)

因为ASA通过真正的组播路由协议(PIM)与邻居通信，所以PIM稀疏模式是首选模式。在ASA 7.0版本发布之前，IGMP末节模式是唯一的组播配置选项，其操作方法只是将从客户端收到的IGMP报告转发到上游路由器。

组播组件

通常，组播基础设施由以下组件组成：

发送方=>发起组播流的主机或网络设备。例如，发送视频和/或音频流的服务器以及运行路由协议（如EIGRP或OSPF）的网络设备。

Receiver =>接收组播流的主机或设备。此术语通常用于那些对流量有积极兴趣并使用IGMP加入或离开有问题的组播组的主机。

路由器/ASA =>负责处理组播流/流量并在需要时从源到客户端转发到网络其他网段的网络设备。

组播路由协议=>负责转发组播数据包的协议。最常见的是PIM（协议无关组播），但也有其它类似于MOSPF的组播。

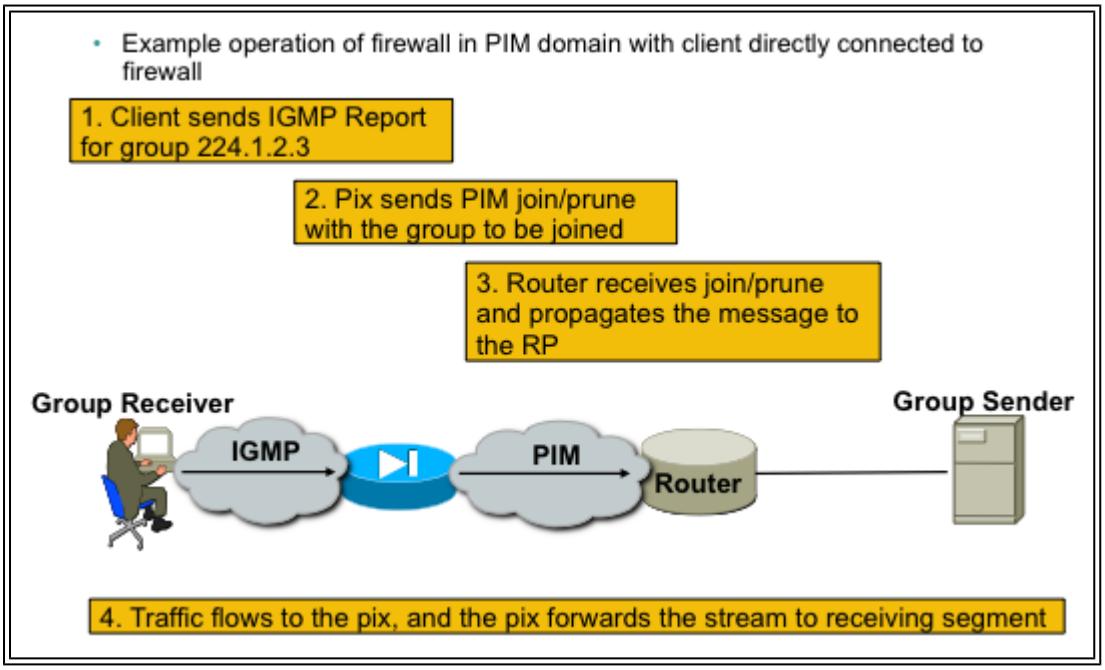
Internet组管理协议(IGMP)=>客户端用于接收来自特定组的组播流的过程。

PIM稀疏模式操作

- ASA支持PIM稀疏模式和PIM双向模式。
- 不能同时配置PIM sparse-mode和IGMP stub-mode命令。
- 使用PIM稀疏模式时，所有组播流量最初流向交汇点(RP)，然后转发到接收器。一段时间后

，组播流直接从源传输到接收器（并绕过RP）。

此图片说明了一个常见部署，其中ASA在一个接口上拥有组播客户端，而在另一个接口上拥有PIM邻居：



PIM稀疏模式示例配置

1.启用组播路由（全局配置模式）。

<#root>

ASA(config)#

multicast-routing

2.定义PIM交汇点地址。

<#root>

ASA(config)#

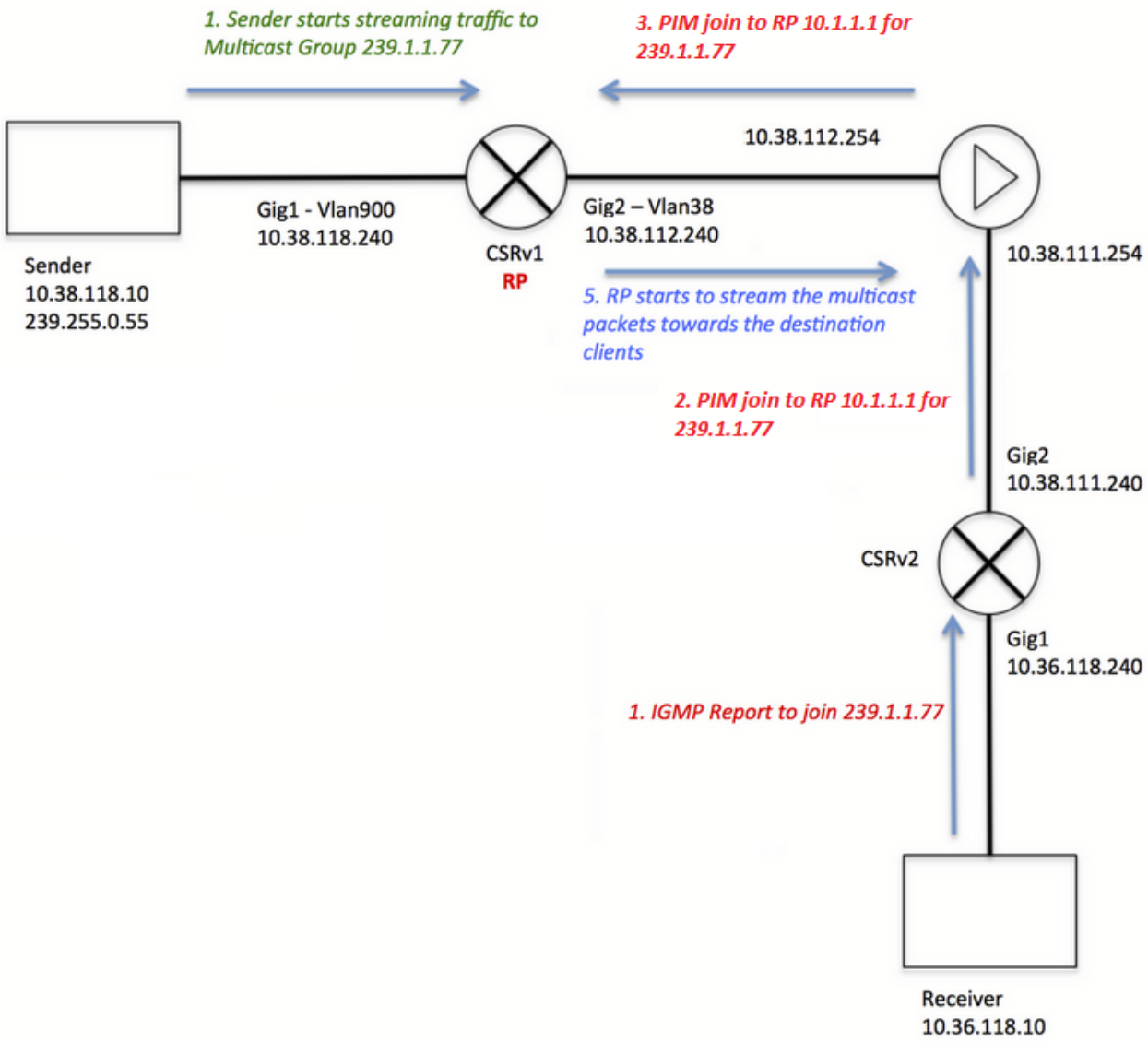
pim rp-address 172.18.123.3

3.在适当的接口上允许组播数据包进入（仅在ASA的安全策略阻止入站组播数据包时才需要）。

<#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：



请注意，客户端IGMP注册（以红色显示）和服务器接收的流（以绿色显示）的颜色不同，因此采用这种方式来证明两个过程可以独立进行。

客户端注册步骤（红色步骤）：

1.客户端发送组239.1.1.77的IGMP报告

2.路由器将PIM加入消息发送到为组239.1.1.77配置的静态RP(10.1.1.1)。

3. ASA向RP发送组239.1.1.77的PIM加入消息。

ASA在show mroute命令输出上显示PIM *,G条目：

<#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，由于源服务器尚未启动任何数据流，因此ASA上的“show mfib”输出不会显示任何收到的数据包：

<#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
```

在服务器开始向组播组发送任何流量之前，RP仅显示“*.G”条目，列表中没有传入接口，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
```

一旦服务器开始向组播组传输数据流，RP就会创建一个“S，G”条目，并将面向发送方的接口放在传入接口列表中，并开始将流量下游发送到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
```

使用以下命令进行验证：

- show mroute命令显示“S，G”条目

- show mfib命令显示转发数据包计数器

- show conn命令显示与组播组ip相关的连接

<#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 -
```

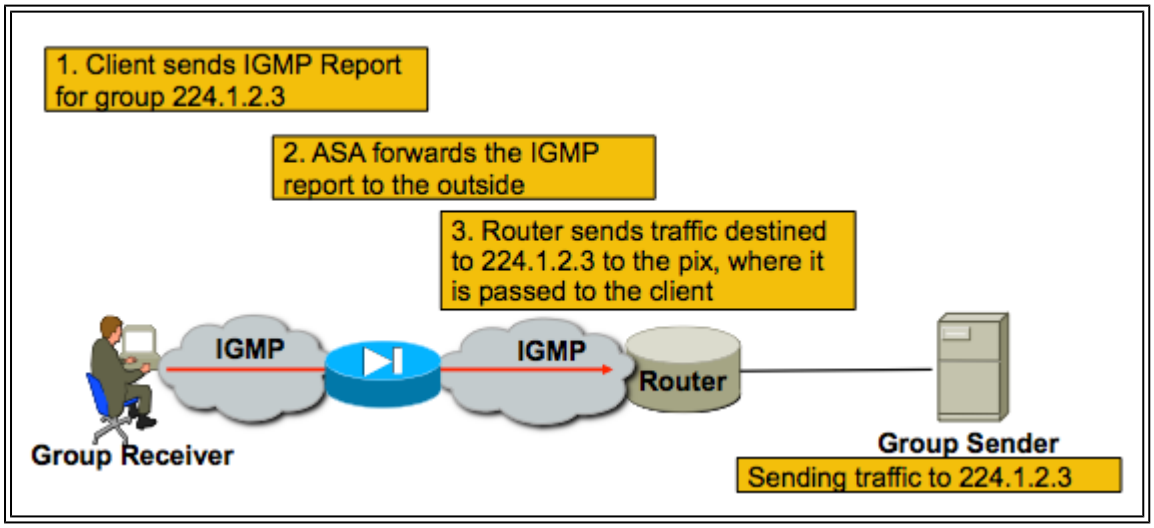
注意：一旦客户端关闭组播客户端应用，主机将发送IGMP查询消息。

如果这是路由器知道的唯一主机，因为客户端想要接收数据流，则路由器会向RP发送IGMP修剪消息。

IGMP末节模式操作

- 在IGMP末节模式下，ASA充当组播客户端，生成或向相邻路由器转发IGMP报告（也称为IGMP“加入”），以触发组播流量的接收
- 路由器会定期向主机发送查询，以查看网络上的任何节点是否希望继续接收组播流量。
- 不推荐IGMP末节模式，因为PIM稀疏模式比末节模式具有许多优点（更高效的组播流量传输、参与PIM的能力等）。

此图片说明为IGMP末节模式配置的ASA的基本操作：



IGMP末节模式配置

1.启用组播路由（全局配置模式）。

<#root>

ASA(config)#

multicast-routing

2.在防火墙接收igmp报告的接口上，配置igmp forward-interface命令。将数据包从接口转发到流源。在本示例中，组播接收器直接连接到内部接口，而组播源不在外部接口上。

<#root>

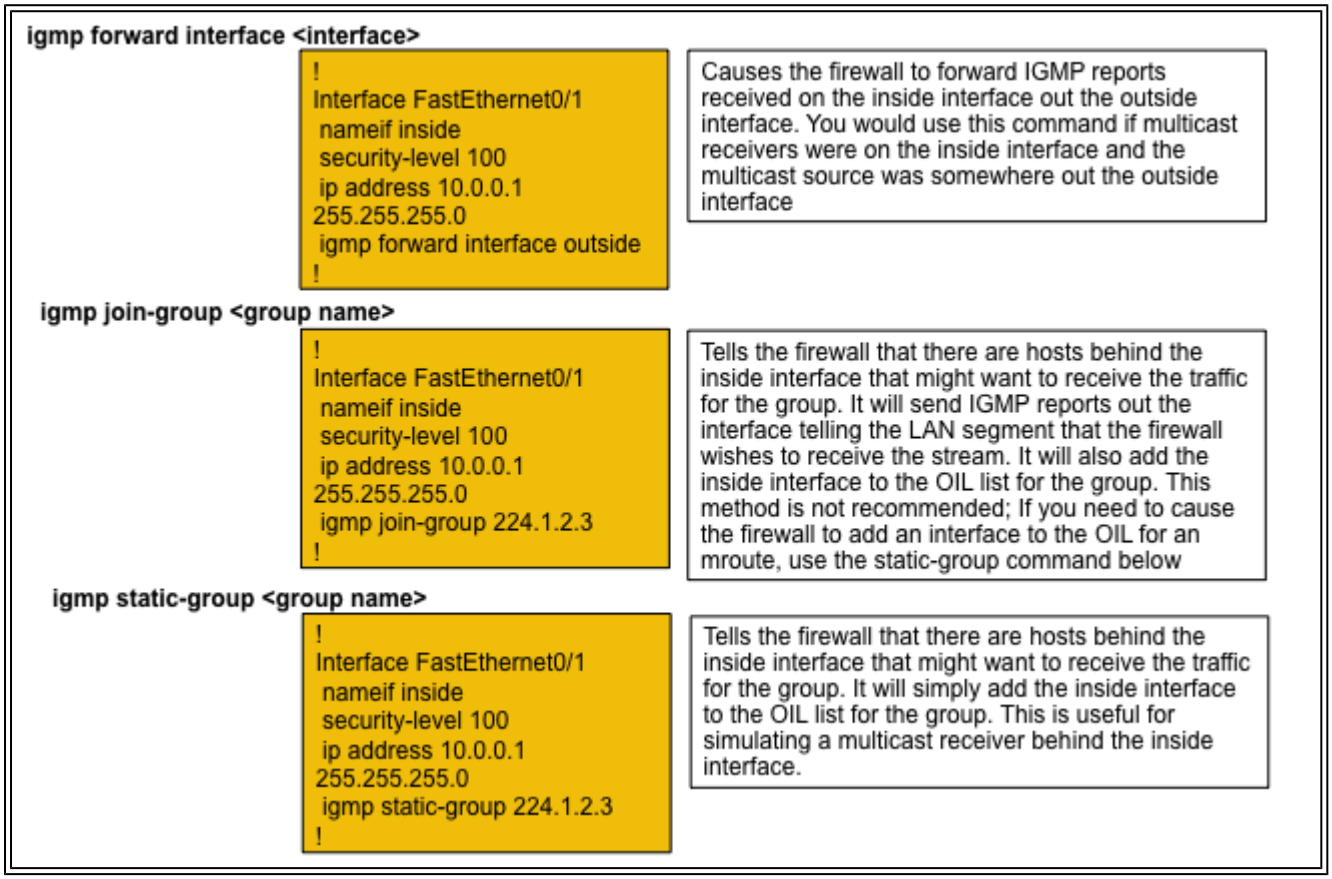
```
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
 no pim
!
```

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


igmp forward interface outside

!
```

3.在适当的接口上允许组播数据包进入（仅当ASA的安全策略拒绝入站组播流量时才需要）。

```
<#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，不同igmp接口子模式命令存在混淆，下图描述了何时使用每个命令：



Bidir PIM

双向PIM中没有共享树(SPT)。这意味着三件事：

1.第一跳路由器（连接到发送方）不向RP发送PIM注册数据包。

2. RP不发送PIM JOIN消息以加入源树。

3.接收方路径中的路由器向RP发送PIM加入消息以加入RPT。

这意味着ASA不会生成(S，G)，因为设备不会加入SPT。所有组播流量都通过RP。只要(*,G)存在，ASA就会转发所有组播流量。如果没有(*,G)，则表示ASA从未收到PIM加入数据包。如果是这种情况，ASA不得转发组播数据包。

Bidir PIM配置

1.启用组播路由（全局配置模式）。

```
<#root>

ASA(config)#

 multicast-routing
```

2.定义PIM交汇点地址。

```
<#root>

ASA(config)#

pim rp-address 172.18.123.3 bidir
```

3.在适当的接口上允许组播数据包进入（仅在ASA的安全策略阻止入站组播数据包时才需要）。

```
<#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

排除多播问题故障时要收集的信息

为了完全了解和诊断ASA上的组播转发问题，需要以下部分或全部信息：

·网络拓扑描述、组播发送方、接收方和交汇点的位置。
·特定组IP地址，以及使用的端口和协议。

·组播流出现故障时ASA生成的系统日志。
· ASA命令行界面的特定show命令输出：

<#root>

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

·数据包捕获，显示组播数据是否到达ASA，以及数据包是否通过ASA转 发(注意数据包的IP生存时间(TTL))。这可以通过命令show capture x detail看到)
·为IGMP和/或PIM数据包捕获数据包。示例：

<#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
```

·来自相邻组播设备（路由器）的信息，例如“show mroute”和“show mfib”。
·数据包捕获和/或show命令确定ASA是否丢弃组播数据包。“show asp drop”命令可用于确定ASA是否丢弃数据包。此外，“asp-drop”类型的数据包捕获可用于捕获ASA丢弃的所有数据包，然后检查丢弃捕获中是否存在组播数据包。

有用的show命令输出

show mroute命令输出显示各种组和转发信息，与IOS show mroute 命令非常相似。show mfib命令显示各种组播组的转发状态。观察转发数据包计数器和其他（表示丢弃）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命令可用于清除计数器，这在测试期间非常有用：

```
<#root>

ciscoasa#

clear mfib counters
```

数据包捕获

板载数据包捕获实用程序对于解决组播问题非常有用。在本示例中，捕获在DMZ接口发往239.17.17.17的所有入口数据包：

```
<#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 命令的输出显示了数据包的TTL，这非常有用。在此输出中，数据包的TTL为1（并且ASA传递此数据包，因为默认情况下它不会递减IP数据包的TTL），但下游路由器会丢弃数据包：

```
<#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
```

数据包捕获对于捕获PIM和IGMP流量也非常有用。此捕获显示内部接口已收到来自10.0.0.2的IGMP数据包（IP协议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#
```

请注意，可以使用“show capture x detail”命令查看数据包的TTL。

在这里我们可以看到已捕获的ASP丢包捕获，其中显示已丢弃的组播数据包以及丢弃的原因(punt-rate-limit):

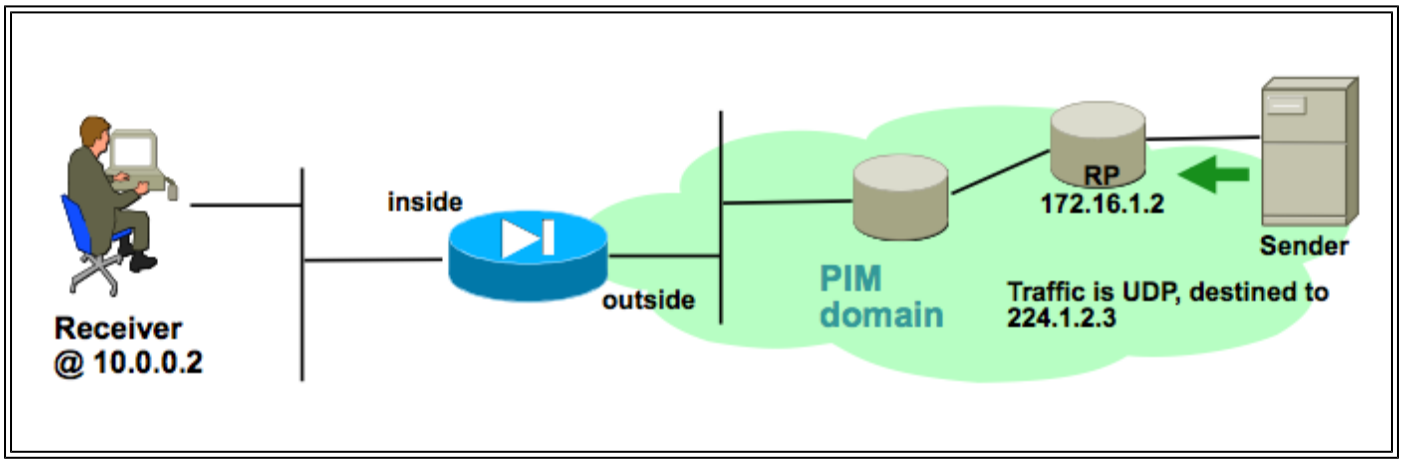
```
<#root>

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稀疏模式组播部署示例

下图说明了ASA如何在PIM稀疏模式下与邻居设备交互。

了解网络拓扑

准确确定特定组播流的发送器和接收器的位置。此外，确定组播组IP地址以及交汇点的位置。



在这种情况下，可以在ASA的外部接口接收数据，然后将其转发到内部接口上的组播接收器。由于接收方与ASA的内部接口位于同一个IP子网中，因此当客户端请求接收数据流时，预计会在内部接口处收到IGMP报告。发送方的IP地址是192.168.1.50。

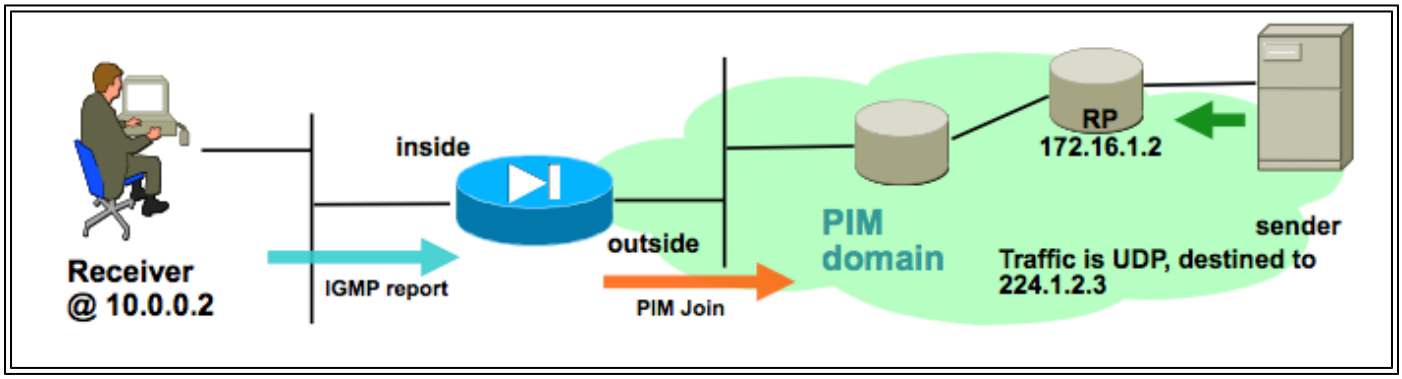
验证ASA是否从接收方收到IGMP报告

在本示例中，IGMP报告由接收方生成并由ASA处理。

数据包捕获和debug igmp的输出可用于验证ASA是否接收并成功处理IGMP消息。

验证ASA向交汇点发送PIM加入消息

ASA解释IGMP报告并生成PIM加入消息，然后将其从接口发送到RP。

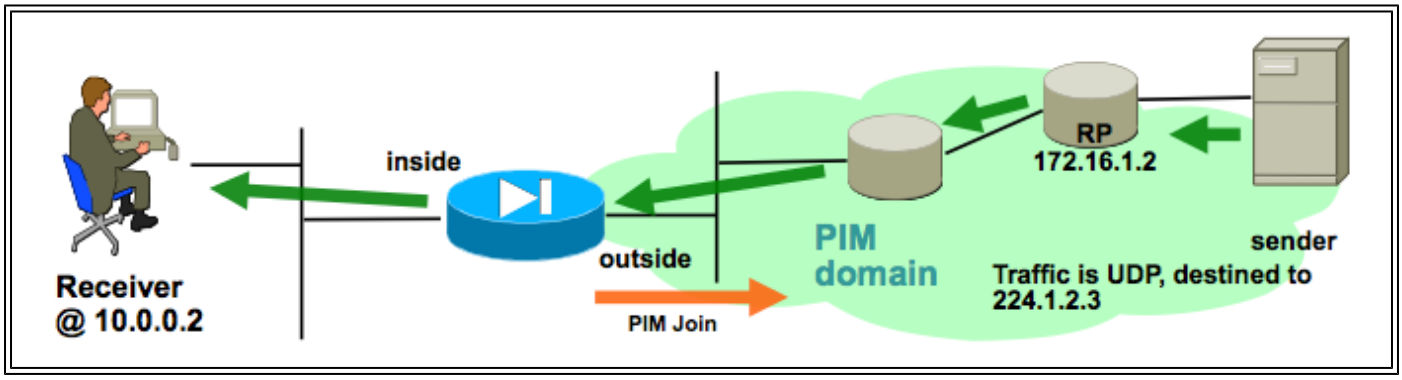


此输出来自debug pim group 224.1.2.3并显示ASA成功发送PIM加入消息。组播流的发送方是192.168.1.50。

```
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
```

验证ASA接收并转发组播流

ASA开始在外部接口上接收组播流量（以绿色箭头表示），然后将其转发到内部接收器。



show mroute和show mfib命令以及数据包捕获可用于验证ASA接收和转发组播数据包。

连接表中会构建一个连接来表示组播流：

<#root>

```
ciscoasa#
```

show conn

```
59 in use, 29089 most used
...
UDP outside:192.168.1.50/52075 inside:224.1.2.3/1234 flags -
...
```

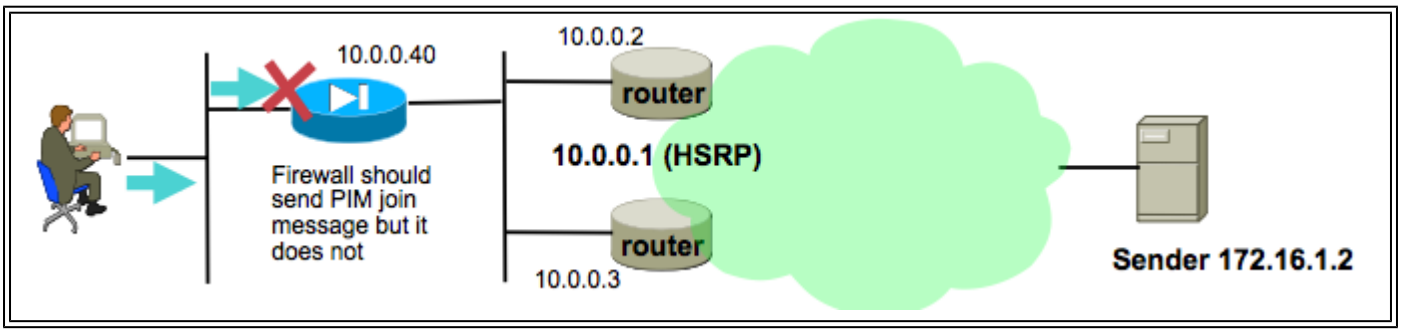
数据分析

常见问题

本部分提供了一系列与实际ASA组播相关的问题

由于HSRP，ASA无法向上游路由器发送PIM消息

遇到此问题时，ASA无法从接口发送任何PIM消息。此图显示ASA无法向发送方发送PIM消息，但是当ASA需要向RP发送PIM消息时，也会出现相同的问题。



debug pim命令的输出显示ASA无法将PIM消息发送到上游下一跳路由器：

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

此问题并不特定于ASA，也会影响路由器。问题是由路由表配置和PIM邻居使用的HSRP配置的组合触发的。

路由表指向HSRP IP 10.0.0.1作为下一跳设备：

```
<#root>

ciscoasa#

show run route

route outside 0.0.0.0 0.0.0.0 10.0.0.1 1
```

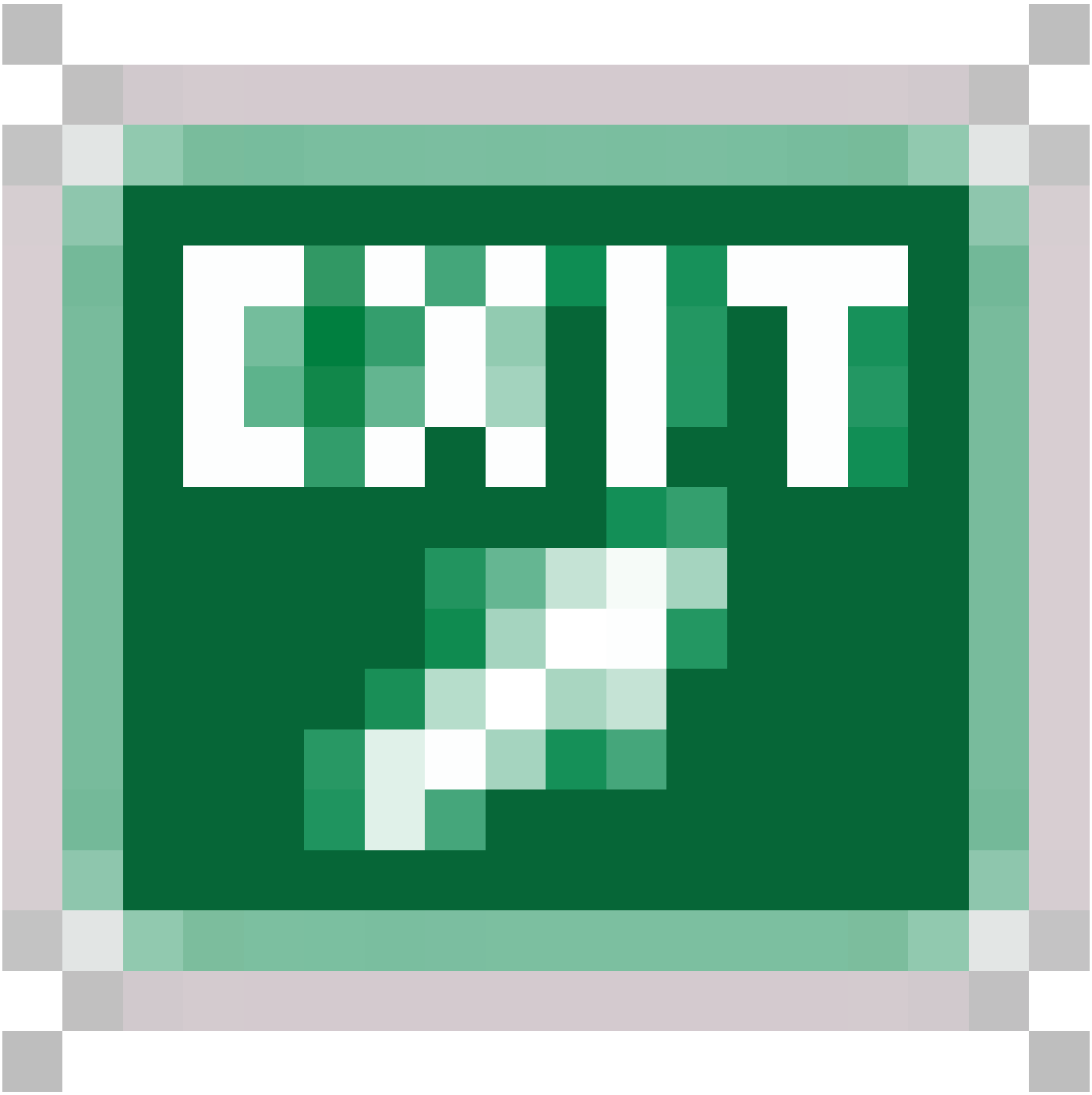
但是，PIM邻居关系在路由器的物理接口IP地址之间形成，而不是HSRP IP:

```
<#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)
```

有关详细信息，请参阅"为什么PIM稀疏模式不能与到HSRP地址的静态路由配合使用？"。

本文档摘录：

为什么路由器不发送加入/修剪消息？ RFC 2362指



“路由器定期向每个(S，G)、(*,G)和(*,*,RP)条目关联的每个不同RPF邻居发送加入/修剪消息。只有当RPF邻居是PIM邻居时，才会发送加入/修剪消息。"

为了缓解问题，请在ASA上为相关流量添加一个静态mroute条目。确保它指向两个路由器接口的IP地址（10.0.0.2或10.0.0.3）之一。在本例中，此命令允许ASA向地址为172.16.1.2的组播发送方发送PIM消息：

<#root>

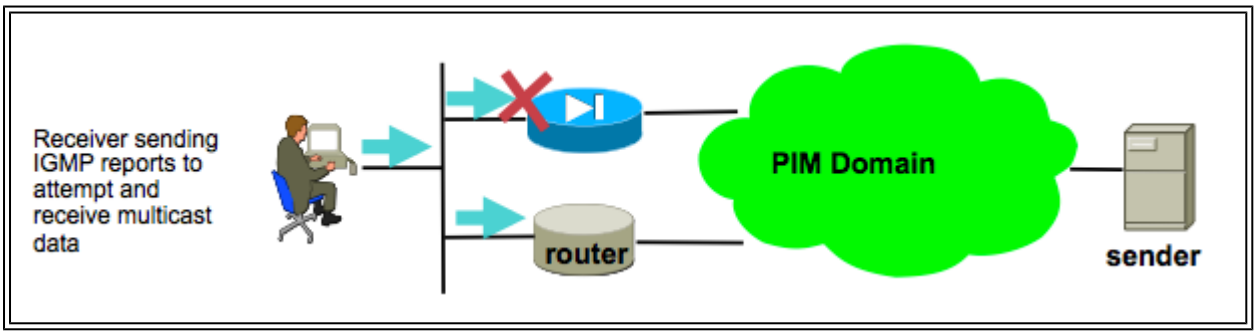
```
ciscoasa(config)#
```

mroute 172.16.1.2 255.255.255.255 10.0.0.3

完成此操作后，组播路由表将覆盖ASA的单播路由表，ASA将PIM消息直接发送到10.0.0.3邻居。

ASA会忽略IGMP报告，因为它不是LAN网段上的指定路由器

对于此问题，ASA从直接连接的组播接收器接收IGMP报告，但它忽略了该报告。不生成调试输出，数据包被丢弃，数据流接收失败。



对于此问题，ASA会忽略数据包，因为它不是客户端所在的LAN网段上选举出的指定路由器。

此ASA CLI输出显示不同的设备是内部接口网络上的指定路由器（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)

默认情况下，将multicast-routing命令添加到配置中时，所有ASA接口上都启用PIM。如果ASA的内部接口（客户端所在的位置）上有其他PIM邻居（其他路由器或ASA），并且由于该网段的DR而选择了其中一个邻居，则其他非DR路由器会丢弃IGMP报告。解决方案是在接口上禁用PIM(在涉及的接口上使用no pim命令)，或通过pim dr-priority接口命令将ASA设置为网段的DR。

当超过IGMP接口限制时，防火墙会拒绝IGMP报告

默认情况下，ASA允许在接口上跟踪500个当前活动联接（报告）。这是可配置的最大值。如果接口外的客户端请求大量组播流，最多可以遇到500个活动加入，并且ASA可以忽略来自组播接收器的其他传入IGMP报告。

要确认这是否是导致组播故障的原因，请发出命令“show igmp interface interfacename”并查找该接口的“IGMP limit”信息。

<#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无法转发232.x.x.x/8范围内的组播流量

此地址范围用于源特定组播(SSM),ASA当前不支持该组播。

debug igmp命令的输出显示以下错误：

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

由于反向路径转发检查，ASA会丢弃组播数据包

在这种情况下，ASA在接口上接收组播流量，但不会将其转发到接收方。ASA会丢弃数据包，因为它们未通过反向路径转发(RPF)安全检查。RPF在所有接口上为组播流量启用，且无法禁用(对于单播数据包，默认情况下检查未启用，并使用ip verify reverse-path interface命令启用)。

由于RPF检查，当在接口上收到组播流量时，ASA会检查是否有路由返回该接口上的组播流量源（它检查单播和组播路由表）。如果它没有通往发送方的路由，则会丢弃数据包。这些丢包在show asp drop的输出中可视为计数器：

<#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
```

一个选项是为流量发送方添加路由。在本示例中，mroute命令用于满足对源自外部接口上收到的172.16.1.2的组播流量的RPF检查：

<#root>

```
ciscoasa(config)#
```

mroute 172.16.1.2 255.255.255.255 outside

ASA在PIM切换到源树时不生成PIM加入

最初，PIM稀疏模式组播数据包从组播发送方流到RP，然后通过共享组播树从RP流到接收方。但是，一旦聚合比特率达到特定阈值，最接近组播接收方的路由器会尝试沿源特定树接收流量。此路由器为组生成新的PIM加入并将其发送到组播流的发送方（而不是像以前一样发送到RP）。

组播流量的发送方可以驻留在与RP不同的ASA接口上。当ASA收到要切换到源特定树的PIM加入时，ASA必须具有到发送方IP地址的路由。如果未找到此路由，则会丢弃PIM加入数据包，并在debug pim的输出中看到此消息

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

此问题的解决方案是为流的发送方添加一个静态mroute条目，指出发送方所在的ASA接口。

ASA由于超过生存时间(TTL)而丢弃组播数据包

在这种情况下，由于数据包的TTL太低，组播流量会失败。这会导致ASA或网络中的其他设备丢弃它们。

通常，组播数据包的IP TTL值由发送它们的应用程序设置得非常低。有时，默认情况下这样做是为了帮助确保组播流量不会在网络中传输得太远。例如，默认情况下， 局域网 客户端应用（常用的组播发射器和测试工具）将IP数据包中的TTL默认设置为1。

由于特定组播拓扑，ASA的CPU使用率较高，并且数据包被丢弃

如果关于组播拓扑的所有这些条件都成立，则ASA可能会遇到高CPU使用率，而组播流可能会遇到丢包情况：

1. ASA充当RP。
2. ASA是组播流的第一跳接收方。这意味着组播发送方与ASA接口位于同一IP子网中。

3. ASA是组播流的最后一跳路由器。这意味着组播接收器与ASA接口位于同一IP子网中。

如果遇到上述所有症状，则 由于设计限制，ASA被迫处理切换组播流量。这会导致高数据速率组播流遇到丢包情况。当丢弃这些数据包时，show asp drop计数器会增加，该计数器是punt-rate-limit。

要确定ASA是否存在此问题，请完成以下步骤：

第1步：检查ASA是否为RP:

<#root>

show run pim
show pim tunnel

第2步：检查ASA是否为最后一跳路由器：

<#root>

show igmp group

<mcast_group_IP>

第3步：检查ASA是否是第一跳路由器：

<#root>

show mroute

<mcast_group_IP>

可以采取以下步骤来缓解此问题：

— 修改拓扑，使ASA不是RP。或者，使发送方或接收方未直接连接到ASA

— 使用IGMP末节模式代替PIM进行组播转发。

首次启动组播流时，ASA会丢弃前几个数据包

当组播流的第一个数据包到达ASA时，ASA必须构建该特定组播连接和关联的mroute条目来转发数据包。当条目正在创建过程中，一些组播数据包可能会被丢弃，直到路由和连接已建立（通常这只需不到一秒钟）。组播流设置完成后，数据包不再受速率限制。

因此丢弃的数据包的ASP丢弃原因为“(punt-rate-limit)Punt rate limit exceeded”。这是“show capture asp”的输出（其中asp是在ASA上配置的ASP丢弃捕获，用于捕获丢弃的数据包），您可以看到由于

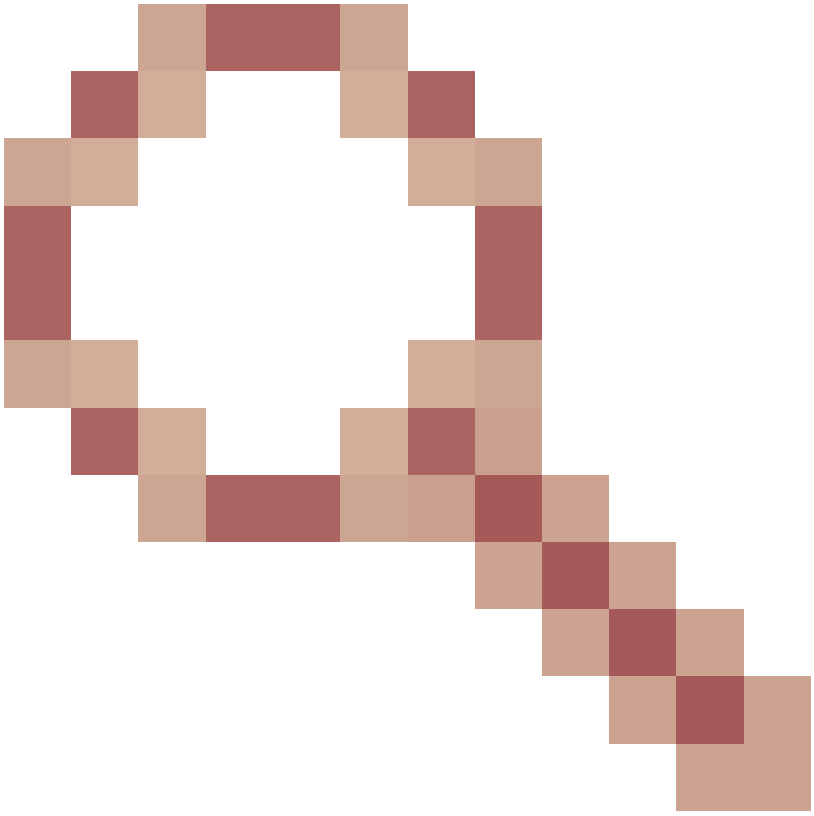
以下原因丢弃的多播数据包：

<#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
```

断开组播接收器会中断其它接口上的组播组接收

只有在IGMP末节模式下运行的ASA才会遇到此问题。参与PIM组播路由的ASA不会受到影响。



问题通过Cisco Bug ID CSCeg确定48235
一个接口上的IGMP离开会中断其他接口上的组播流量。

这是漏洞的版本说明，它解释了问题：

```
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
```

由于出站访问列表的安全策略，ASA丢弃组播数据包

对于此特定问题，ASA会丢弃组播数据包（根据配置的安全策略）。但是，网络管理员很难确定丢包的原因。在这种情况下，由于为接口配置的出站访问列表，ASA会丢弃数据包。解决方法是允许出站访问列表中的组播流。

发生这种情况时，组播数据包将使用ASP丢弃计数器“FP no mcast output intrf(no-mcast-intrf)”丢弃。

由于控制点速率限制，ASA会持续丢弃组播流中的某些数据包（但不是全部）

流量极有可能受到控制点的速率限制，这是由于punt-rate-limit所致。查看asp丢弃输出和捕获以确认：

<#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条目显示所有流量都进行了进程交换：

<#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
```

组播路由表显示(*,G)，但没有(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
```

此处的问题是，到达ASA的数据包组播数据包的TTL为1。ASA将这些数据包转发到下游设备（因为它不会减少TTL），但路由器下游会丢弃这些数据包。因此，下游路由器不会向ASA向发送方发送PIM(S，G)加入（源特定加入）。ASA在收到此PIM加入之前不会生成(S，G)条目。由于未构建(S，G)，因此所有组播流量都会进行进程交换，从而导致速率限制。

此问题的解决方法是确保数据包的TTL不是1，这允许下游设备向发送方发送源特定联接；这会导致ASA在表中安装源特定路由，然后所有数据包都进行快速交换（而不是处理交换），流量必须流经ASA，而不会出现问题。

组播流因PIM ASSERT消息而暂停

如果两个网络设备将相同的组播数据包转发到同一子网，则理想情况下，其中一个网络设备必须停止转发数据包（因为复制数据流是浪费的）。如果运行PIM的路由器检测到它们接收了相同的数据包，则它们会在该LAN上生成ASSERT消息，以选择哪个网络设备停止转发该流。

有关此消息的更多信息，请参阅与ASSERT过程相关的RFC 4601部分。

调试显示，ASA收到组239.1.1.227的IGMP报告，但是由于它从相邻路由器收到的断言消息，它忽略了该报告：

```
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)
```

在生产网络中观察到此问题，其中两个站点在第2层意外桥接，因此组播接收器所在的LAN有两个设备向它们转发组播流量。由于另一个网络问题，ASA和另一个设备无法通过PIM Hello检测到对方，因此它们都承担了LAN的指定路由器角色。这导致组播流量工作一段时间，然后在设备发送ASSERT消息时失败。为了解决该问题，在第2层桥接设备的不正确连接被禁用，然后问题得到解决。

ASA发送PIM加入，但由于数据包大小大于MTU，邻居不会处理该加入

在1997年观察到这629575899点。ASA是为巨型帧配置的，而4900没有。当客户端请求超过73个组播流时，某些组播流将不起作用。73个SG将创建大小为1494的PIM加入消息，该消息仍在MTU内。74SG将创建大于1500的PIM加入消息，这导致4900M丢弃入站数据包。

此问题的解决方法是：

1.确保在4900M上全局启用巨帧

2.使用MTU 9216配置物理接口和SVI

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。