ASA组播故障排除和常见问题

目录

简介

本文解释可以遇到，当曾经功能时可适应安全工具(ASA)的组播功能，以及潜在问题。

先决条件

要求

Cisco 建议您了解以下主题：

- ASA组播

使用的组件

本文档不限于特定的软件和硬件版本。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

功能信息

ASA Line configuration命令指南概述路由功能和如何配置它：

http://www.cisco.com/en/US/docs/security/asa/asa90/configuration/guide/route_multicast.html

在ASA的组播可以在两个模式之一中配置：

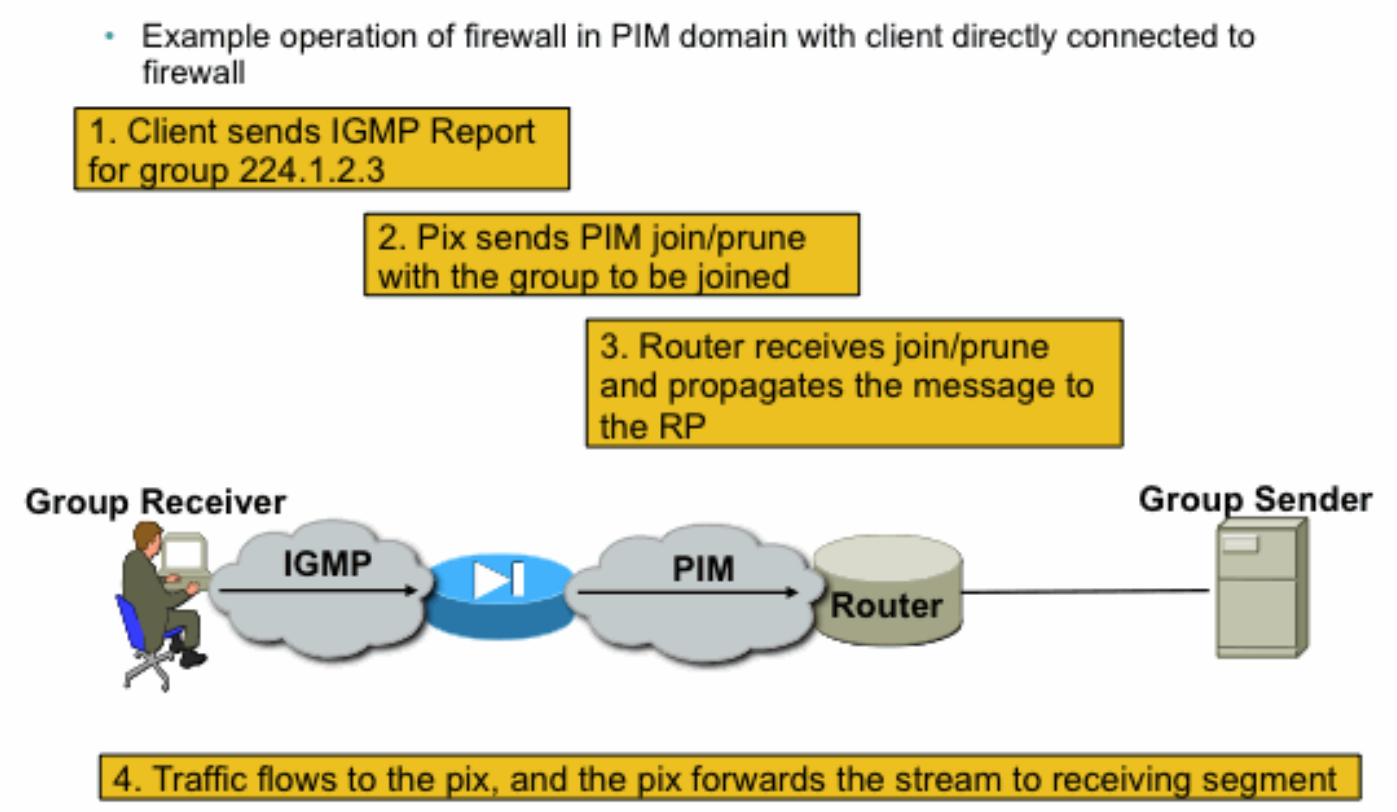
- PIM稀疏模式(首选)
- IGMP Stub模式(互联网组管理协议， RFC 2236 IGMPv2)

PIM稀疏模式是首选，因为ASA与使用一个真的组播路由协议(PIM)的邻居联络。IGMP Stub模式是唯一的组播配置选项，在ASA版本7.0通过转发从往上游路由器的客户端接收的IGMP报告发布，并且操作前。

PIM稀疏模式操作

- ASA支持PIM稀疏模式和PIM双向模式。
- 不能同時配置PIM稀疏模式和IGMP模式命令。
- 使用所有组播数据流最初流到聚合点(RP)的PIM稀疏模式，然后转发往接收方。在一些时间组播流直接地从来源将去接收方后(绕过RP)。

下面的图片说明ASA有一个接口的组播客户端的一普通的部署和别的PIM邻居：



PIM稀疏模式配置示例

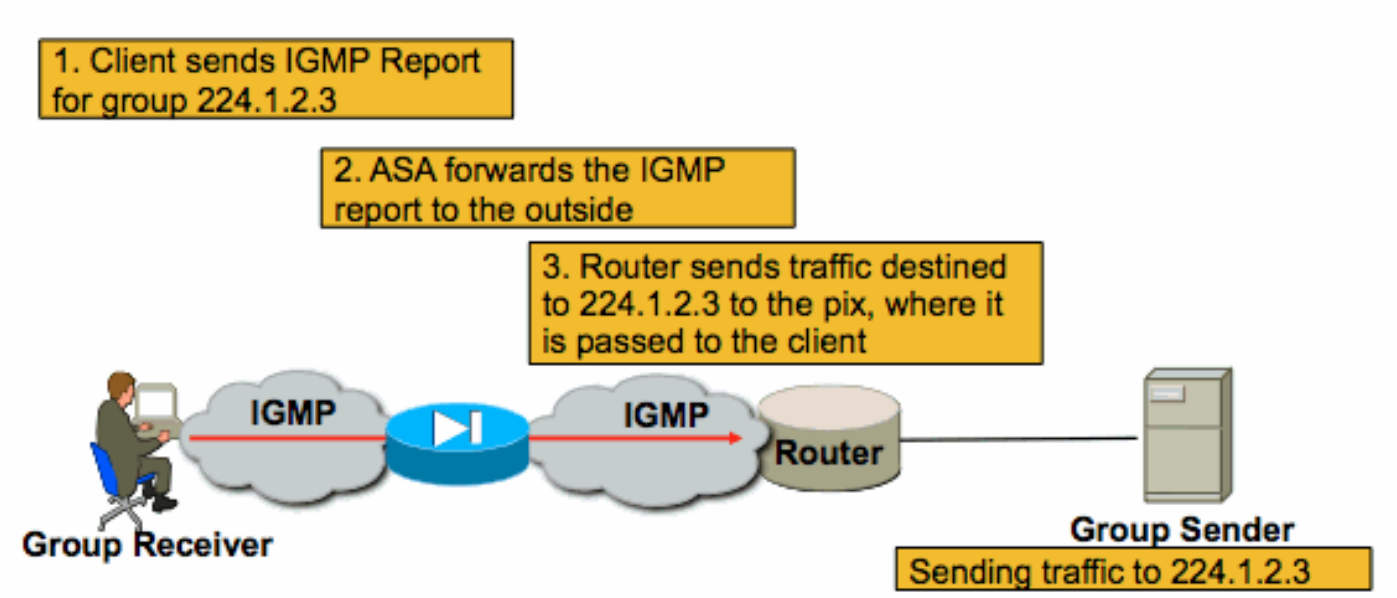
完成这些步骤：

1. 启用组播路由(全局配置模式)。`ASA(config)# multicast-routing`
2. 定义PIM集合点地址。`ASA(config)# pim rp-address 172.18.123.3`
3. 允许组播信息包在适当的接口(必要，只有当ASA的安全策略阻塞入站组播信息包)。`access-list 105 extended permit ip any host 224.1.2.3`
   `access-group 105 in interface outside`

IGMP Stub模式操作

- 在IGMP Stub模式ASA作为组播客户端通过生成或转发IGMP报道(亦称IGMP “加入”)往邻接路由器，触发组播数据流的接收
- 路由器周期地将发送查询到主机发现在网络的任何节点是否要继续收到组播数据流。
- 没有推荐IGMP Stub模式，因为PIM稀疏模式提供在Stub模式的许多好处(包括更有效的组播数据流运输流量、能力参加PIM等等)。

下面的图片说明为IGMP Stub模式配置的ASA的基本操作。



IGMP模式配置

完成这些步骤：

1. 启用组播路由(全局配置模式)。`ASA(config)# multicast-routing`
2. 在您将收到igmp报告的接口，请配置igmp转发接口命令。转发数据包往数据流的来源的接口。在下面的示例中的，组播接收器直接地连接对内部接口，并且组播源是在外部接口之外。`!`

```
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. 允许组播信息包在适当的接口(仅必要ASA的安全策略是否否决入站组播数据流)。`access-list 105 extended permit ip any host 224.1.2.3`

   `access-group 105 in interface outside`经常有混乱在不同的**igmp接口从属方式**命令附近，并且下图所示什么时候尝试描述使用其中每一

   ：

igmp forward interface <interface>

```
!
Interface FastEthernet0/1
 nameif inside
 security-level 100
 ip address 10.0.0.1
255.255.255.0
 igmp forward interface outside
!
```

Causes the firewall to forward IGMP reports received on the inside interface out the outside interface. You would use this command if multicast receivers were on the inside interface and the multicast source was somewhere out the outside interface

igmp join-group <group name>

```
!
Interface FastEthernet0/1
 nameif inside
 security-level 100
 ip address 10.0.0.1
255.255.255.0
 igmp join-group 224.1.2.3
!
```

Tells the firewall that there are hosts behind the inside interface that might want to receive the traffic for the group. It will send IGMP reports out the interface telling the LAN segment that the firewall wishes to receive the stream. It will also add the inside interface to the OIL list for the group. This method is not recommended; If you need to cause the firewall to add an interface to the OIL for an mroute, use the static-group command below

igmp static-group <group name>

```
!
Interface FastEthernet0/1
 nameif inside
 security-level 100
 ip address 10.0.0.1
255.255.255.0
 igmp static-group 224.1.2.3
!
```

Tells the firewall that there are hosts behind the inside interface that might want to receive the traffic for the group. It will simply add the inside interface to the OIL list for the group. This is useful for simulating a multicast receiver behind the inside interface.

故障排除方法

应收集的信息，当排除故障组播问题时

为了完全了解和诊断在ASA的一组播转发问题，一些或所有此信息也许是需要的：

- 网络拓扑，包括位置fo组播发送方，接收方和集合点的说明。
- 流量使用的特定组IP地址，以及被使用的端口和协议。
- ASA生成的Syslog，在组播流有麻烦时候。
- 从ASA命令行界面的特定show命令输出，包括：`show mroute`
  `show mfib`
  `show pim neighbor`
  `show route`
  `show tech-support`
- 显示的数据包捕获，如果组播数据到达在ASA，并且，如果数据包通过ASA转发。
- 显示IGMP和PIM数据包的数据包捕获。
- 从相邻组播设备(路由器)的信息例如“显示mroute’，并且“请显示mfib’。
- 数据包捕获并且/或者显示命令确定ASA是否丢弃组播信息包。‘请显示asp丢弃’命令能使用确定ASA是否丢弃数据包。另外，类型‘asp丢弃的’数据包捕获可以使用获取ASA丢弃的所有信息包，然后被检查发现组播信息包是否是存在丢弃捕获。

有用的show命令输出

显示mroute命令输出显示多种组和转发信息，并且非常类似于IOS**显示mroute**命令。**显示mfib**命令显示多种组播组的转发状况。(是特别指示丢包)的重要观察*转发数据包*计数器，以及*其他*：

```
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 counter命令可以用于清除计数器，在测试期间是非常有用的：

```
ciscoasa# clear mfib counters
ciscoasa#
```

使用捕获的数据包捕获组播数据流

ASA的内置数据包捕获工具为排除故障组播问题是非常有用的。在下面的示例中，所有到达数据包在ASA的DMZ接口，被注定对239.17.17.17将捕获：

```
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
....
```

数据包捕获为捕获PIM和IGMP流量也是有用的。下面的捕获显示内部接口接收IGMP信息包(从10.0.0.2 2)来源的IP协议：

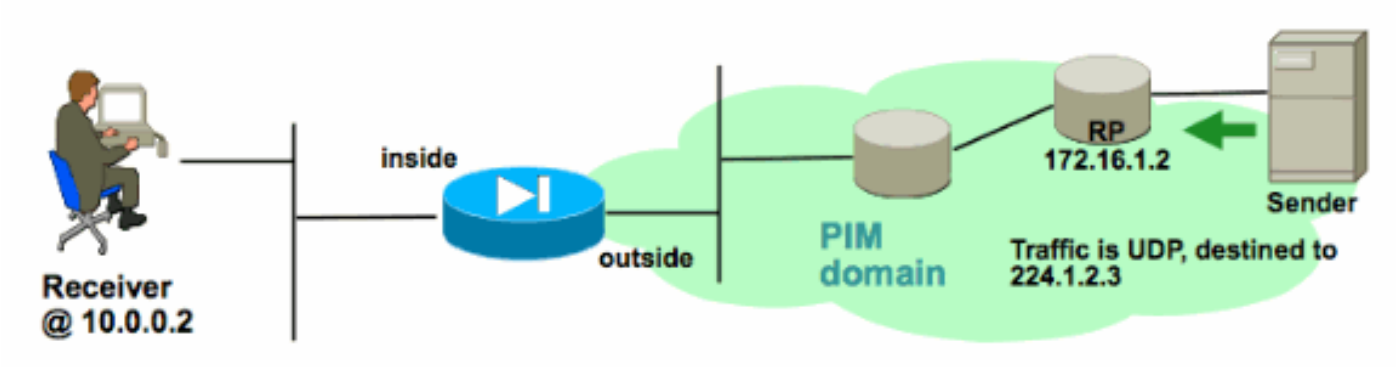
```
ciscoasa# capture capin interface inside
ciscoasa# capture capin match igmp any any
ciscoasa# show cap capin
1 packets captured
1: 10:47:53.540346 802.1Q vlan#15 P0 10.0.0.2 > 224.1.2.3:
  ip-proto-2, length 8
ciscoasa#
```

示例ASA PIM稀疏模式组播部署

下图所示说明ASA如何与邻接设备呼应获得流同PIM稀疏模式的组播数据流。在此特定示例中，ASA接收。

了解网络拓扑

正确地确定特定组播流的发送方和接收方您哪里测试驻留。并且，请确定组播组IP地址使用的，以及集合点的位置。



在这种情况下，数据应该至多是ASA的接收的接口和转发对在内部接口的组播接收器。由于接收方是在IP子网和ASA的内部接口一样，请期望发现IGMP报告接收在ASA的内部接口，当客户端的要求接收数据流。发送方的IP地址是192.168.1.50。

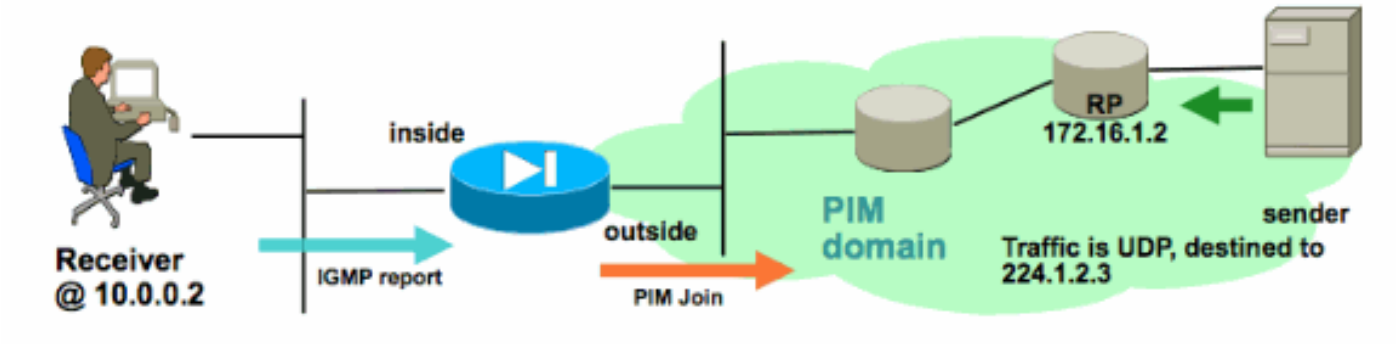
正在验证ASA收到从接收方的IGMP报告

在本例中， IGMP报告由接收方生成并且由ASA处理。

数据包捕获和调试igmp输出可以用于验证接收和顺利地处理IGMP信息的ASA。

正在验证ASA传送往集合点的一PIM Join消息

ASA解释IGMP报道并且生成PIM Join消息，然后传送它往RP的接口。



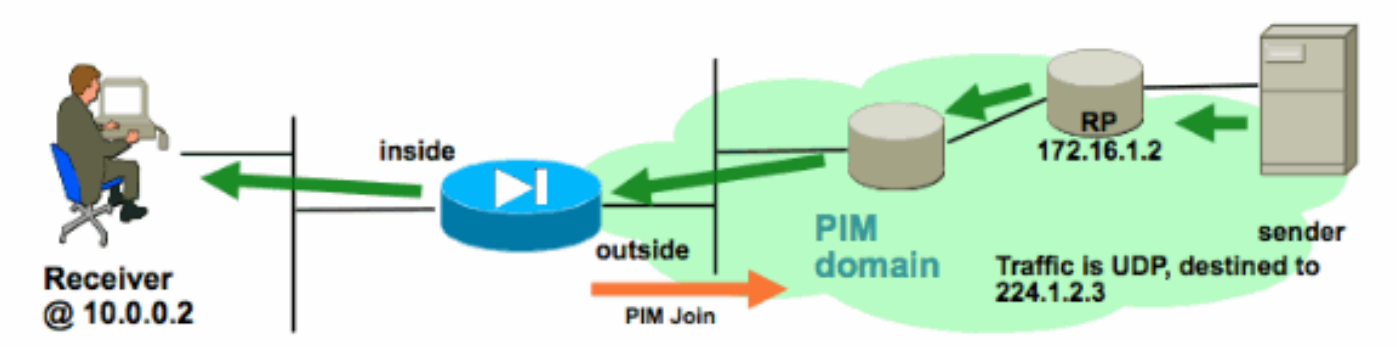
下面的输出是从调试pim组224.1.2.3并且显示顺利地发送PIM Join消息的ASA。组播流的发送方是192.168.1.50

```
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 192.168.1.5
```

正在验证ASA接收并且转发组播流

ASA开始接收在外部接口的组播数据流(说明由绿色箭头)和转发它对在里面的接收方。



显示mroute和**显示mfib**命令，以及数据包捕获，可以使用验证ASA接收并且转发组播信息包。

连接在ASA的连接表里将被建立代表组播流：

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

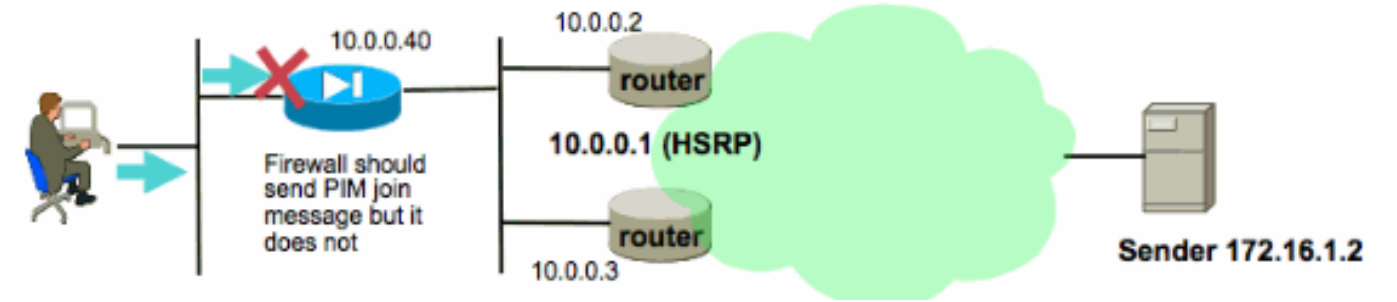
数据分析

常见问题

此部分提供网络管理员以前遇到了的一系列的真实世界的ASA组播相关问题。

ASA不能传送PIM信息往上游路由器由于HSRP

当此问题遇到时， ASA不能传送任何PIM信息接口。下图所示显示ASA不能传送往发送方的PIM信息，但是同一问题能被看到，当ASA需要传送往RP时的PIM信息。



调试pim输出显示ASA不能传送PIM信息到上行下一跳路由器：

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

此问题不是特定对ASA，并且影响路由器。问题由PIM邻居和HSRP配置的触发使用的组合ASA的路由表配置。

ASA的路由表指向HSRP IP 10.0.0.1作为下一跳设备：

```
ciscoasa# sh run route
route outside 0.0.0.0 0.0.0.0 10.0.0.1 1
```
然而， PIM邻接关系形成在路由器的物理接口IP地址，而不是HSRP IP:之间

```
ciscoasa# sh 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)
```
参考PIM稀疏模式为什么不与静态路由一起使用对HSRP地址？。

摘自本文的一个部分：

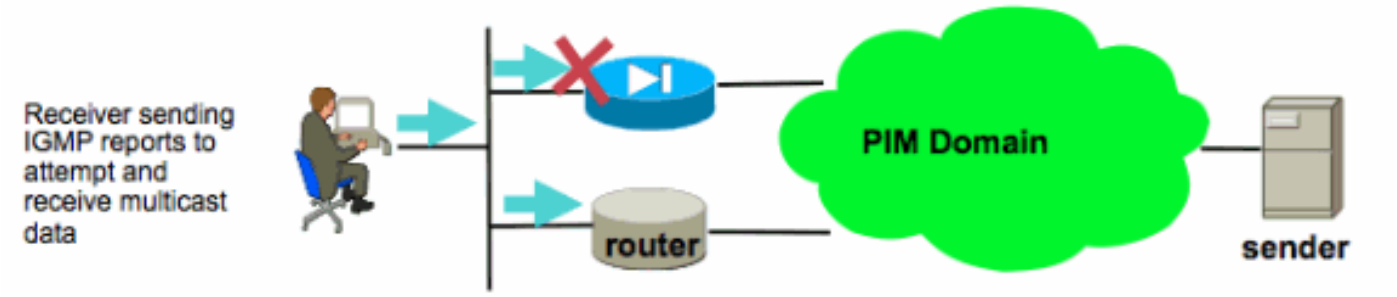
"路由器为什么不发送汇合/消减消息？RFC 2362阐明，"路由器传送一个定期汇合/消减消息给每个明显的RPF邻居关联与每(S， G)，(， G)和(*， *， RP)条目。汇合/消减消息传送，只有当RPF邻居是PIM邻居"。*

为了减轻问题，请添加在ASA的一个静态mroute条目有问题的流量的。确保它指向两个路由器接口IP地址之一(10.0.0.2或10.0.0.3在以上示例)。在这种情况下，以下命令允许ASA传送PIM信息将组播发送方指向在172.16.1.2 ：

```
ciscoasa(config)# mroute 172.16.1.2 255.255.255.255 10.0.0.3
```
一旦这执行组播路由表将改写ASA的单播路由表，并且ASA将传送PIM信息直接地给10.0.0.3邻居。

ASA忽略IGMP报告，由于它不是LAN分段的指定路由器

对于此问题， ASA收到从一台直接地连接的组播接收器的一IGMP报道，忽略它。debug输出不会生成，并且数据包丢弃，并且数据流接收发生故障。



对于此问题， ASA丢弃数据包，因为它不是客户端驻留的LAN分段的PIM选择的指定路由器。

下面ASA CLI的输出显示一个不同的设备是指定路由器(表示由"DR")内部接口网络的：

```
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，当**组播路由**命令被添加到ASA的配置时， PIM在所有ASA接口启用。如果有其他PIM邻居(其他路由器或ASA) ASA的内部接口的(其中客户端驻留)，并且那些邻居之一选择，因为该分段，则其他的DR，非DR路由器将丢弃IGMP报道。解决方案将禁用在ASA的接口的PIM (用**没有pim命令**在介入的接口)，或者使ASA分段的DR使用**pim dr优先级interface命令**。

ASA不能转发在232.x.x.x/8范围的组播数据流

此地址范围发挥作用与ASA当前不支持的源特定组播(SSM)的。

调试igmp输出将显示此错误：

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

ASA丢包组播信息包由于反向路径转发检查

在这种情况下，在接口的ASA接收组播数据流，然而它没有转发到接收方。数据包由ASA丢弃，因为他们失败反向路径转发(RPF)安全性检查。RPF在组播数据流的所有接口启用，并且不可能禁用默认情况下(对于单播信息包检查不打开和启用与**ip验证interface命令的reverse-path**)。

由于RPF检查，当组播数据流接收在接口时， ASA检查发现有一个路由回到组播数据流流量(的来源检查单播和组播路由表)在该接口。如果它没有一个路由到发送方，丢弃数据包。这些丢包能被看到作为计数器在输出中**显示asp丢弃**：

```
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
```

此问题可以通过添加特定组播路由条目减轻到流量的发送方的ASA。在下面的示例中的， mroute命令在外部接口用于满足从172.16.1.2发出的组播数据流的RPF检查接收：

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

ASA不生成PIM加入在对来源树的PIM切换

最初， PIM稀疏模式组播信息包从组播发送方将流到RP，然后从RP到接收方通过一共享组播树。然而，聚集比特率一次达到一特定的阈值，路由器最接近组播接收器将尝试收到沿来源特定的树的流量。此路由器将生成组的新的PIM加入并且发送它往组播流的发送方(和不往RP，作为以前)。

根据网络拓扑，组播数据流的发送方在一个不同的ASA接口比RP也许驻留。当ASA接收PIM加入换成来源特定树时， ASA必须有路由到发送方的IP地址。如果没找到此路由， PIM加入数据包将丢弃，并且下列信息在**调试pim中**输出将被看到：

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

此问题的解决方案是添加每数据流的发送方的静态mroute条目，指出ASA接口哪些发送方驻留。

ASA丢包组播信息包由于超出的存活时间(TTL)

在这种情况下，因为数据包的TTL太低，组播数据流失败。这的网络促成ASA，或者一些其它设备，丢弃他们。

通常组播信息包有IP TTL值设置的非常低由发送他们的应用程序。默认情况下有时这执行帮助保证组播数据流太虽则不移动网络。默认情况下例如，视频LAN客户端应用(一个普遍的组播发射器和测试工具)默认情况下设置在IP数据包的TTL到1。

ASA体验高CPU使用情况和丢弃的数据包由于特定组播拓扑

ASA也许体验高CPU，并且组播流也许经受丢包，如果所有以下是真的关于组播拓扑：

1. ASA作为RP。
2. ASA是组播流的第一个跳接收方。这意味着组播发送方是在同样IP子网ASA接口。
3. ASA是组播流的最后一跳路由器。这意味着组播接收器是在IP子网和ASA接口一样。

如果所有在上面是真的，则到期执行ASA将被迫处理交换机组播数据流的设计限制。这导致高数据传输比组播流经受丢包。增加的显示asp丢弃计数器，当这些数据包丢弃时是PUNT速率限制。

为了确定ASA是否遇到此问题，请完成这些步骤：

步骤 1：检查ASA通过使用两命令，是否是RP ：

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

步骤 2：检查ASA通过使用此命令，是否是最后一跳路由器：

```
show igmp group <mcast_group_IP>
```

步骤 3：检查ASA通过使用此命令，是否是第一跳跃路由器：

```
show mroute <mcast_group_IP>
```

断开的组播接收器中断其他接口的组播组接收

操作在IGMP Stub模式的仅ASA遇到此问题。参加PIM组播路由的ASA不受影响。

问题由bug CSCeg48235识别- IGMP ：正在停止的组rcvr中断分组其他接口的接收

这是从bug的版本注释，解释问题：

```
Symptom:
When a PIX or ASA firewall is configured for IGMP stub mode multicast reception and
traffic from a multicast group is forwarded to more than one interface, if a host
behind a receiving interface sends an IGMP Leave message for the group, it could
temporarily interrupt the reception for that group on other interfaces of the firewall.

The problem is triggered when the firewall forwards the IGMP leave for the group
towards the upstream device; that device then sends a IGMP query to determine if any
other receivers exist out that interface towards the firewall, but the firewall does
not report that it still has valid receivers.

Conditions:
The PIX or ASA must be configured for IGMP stub mode multicast. IGMP stub mode is a
legacy multicast forwarding technique, whereby IGMP packets from receivers are forwarded
through the firewall towards the source of the stream. It is recommended to use PIM
multicast routing instead of stub igmp forwarding.

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,
causing their IGMP reports to be forwarded towards the sender more frequently, thus
restarting the stream quicker.
```

ASA丢包组播信息包由于出局访问安全策略列出

使用此特定请发出ASA正确地丢弃组播信息包(每个已配置的安全策略)。然而，识别丢包的原因网络管理员是很难的。在这种情况下， ASA丢弃数据包由于为接口配置的出局访问列表。应急方案是允许在出局访问列表的组播流。

当这发生，组播信息包将丢弃，并且ASP丢弃计数器将是“FP没有mcast输出intrf (NO-

mcastintrf)”。

当组播流首先开始时， ASA丢弃最初的少数数据包

当组播流的第一数据包到达在ASA时， ASA必须构件特殊请组播连接和相关的mroute条目转发数据包。当条目创建时一些组播信息包也许丢弃直到mroute，并且连接被建立了(这少于一秒钟通常采取)。一旦组播流设置完成，数据包不再将是被限制的速率。

被丢弃的数据包为此将有“(PUNT速率限制)超过的平底船速率限制” ASP丢弃原因。下面输出**显示捕获asp** (其中asp是在ASA配置的ASP丢弃捕获获取丢弃的数据包)，并且您能看到为此被丢弃的组播信息包：

```
ASA # sh 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 rate limit exceeded
   2: 16:14:49.919172 10.23.2.2.810 > 239.255.123.123.890:  udp 32 Drop-reason:
 (punt-rate-limit) Punt rate limit exceeded
2 packets shown
```

相关信息

- 技术支持和文档 - Cisco Systems