

Fehlerbehebung bei häufigen ASA-Multicast-Problemen

Inhalt

[Einleitung](#)

[Informationen zu Funktionen](#)

[Abkürzungen/Akronyme](#)

[Komponenten von Multicast](#)

[PIM Sparse Mode-Betrieb](#)

[PIM Sparse-Mode-Beispielkonfiguration](#)

[Beispiel für PIM Sparse Mode:](#)

[IGMP-Stub-Modus](#)

[IGMP-Stub-Modus-Konfiguration](#)

[Bidir PIM](#)

[Bidir PIM-Konfiguration](#)

[Methodik der Fehlerbehebung](#)

[Informationen, die bei der Fehlerbehebung von Multicast-Problemen gesammelt werden müssen](#)

[Hilfreiche Befehlsausgabe anzeigen](#)

[Paketerfassung](#)

[Beispiel für eine ASA PIM Sparse-Mode-Multicast-Bereitstellung](#)

[Datenanalyse](#)

[Häufige Probleme](#)

[Die ASA sendet aufgrund von HSRP keine PIM-Nachrichten an Upstream-Router](#)

[Die ASA ignoriert IGMP-Berichte, da es sich nicht um den festgelegten Router im LAN-Segment handelt.](#)

[IGMP-Berichte werden von der Firewall abgelehnt, wenn der IGMP-Schnittstellengrenzwert überschritten wird](#)

[Die ASA leitet Multicast-Datenverkehr nicht im Bereich 232.x.x.x/8 weiter.](#)

[Die ASA verwirft Multicast-Pakete aufgrund einer Überprüfung der Umkehrpfad-Weiterleitung](#)

[Die ASA generiert beim PIM-Switchover zum Source-Tree keine PIM-Join-Nachricht](#)

[Die ASA verwirft Multicast-Pakete aufgrund von TTL-Überschreitungen \(Time To Live\).](#)

[Hohe CPU-Auslastung und Paketverluste der ASA aufgrund einer bestimmten Multicast-Topologie](#)

[Die ASA verwirft die ersten Pakete, wenn ein Multicast-Stream gestartet wird](#)

[Ein trennender Multicast-Empfänger unterbricht den Empfang der Multicast-Gruppe an anderen Schnittstellen.](#)

[Die ASA verwirft Multicast-Pakete aufgrund der Sicherheitsrichtlinie für ausgehende Zugriffslisten.](#)

[Die ASA verwirft fortlaufend einige Pakete \(aber nicht alle\) in einen Multicast-Stream, da die Durchsatzrate für die Kontrollpunkte begrenzt wird.](#)

[Der Multicast-Stream wird aufgrund einer PIM ASSERT-Nachricht angehalten.](#)

[ASA sendet PIM-Join, wird aber aufgrund einer Paketgröße größer als MTU nicht vom Nachbarn verarbeitet](#)

Einleitung

In diesem Dokument werden das Multicast-Routing auf der Adaptive Security Appliance (ASA) und häufige Probleme beschrieben.

Informationen zu Funktionen

Hinweis: Aktualisierte Informationen zum Multicast-Routing auf der Adaptive Security Appliance (ASA),

Firepower Threat Defense (FTD) oder Secure Firewall Threat Defense (FTD) finden Sie in den folgenden Artikeln:

[Fehlerbehebung: Firepower Threat Defense - IGMP- und Multicast-Grundlagen](#)

[Fehlerbehebung bei Firepower Threat Defense und ASA Multicast PIM](#)

Abkürzungen/Akronyme

| Abkürzungen | Erläuterung |
|-------------|--|
| FHR | First-Hop-Router - ein Hop, der direkt mit der Quelle des Multicast-Verkehrs verbunden ist. |
| LHR | Last-Hop-Router - ein Hop, der direkt mit den Empfängern des Multicast-Verkehrs verbunden ist. |
| RP | Rendezvous-Point |
| DR | Designierter Router |
| SPT | Baum mit dem kürzesten Pfad |
| RPT | Rendezvous-Point (RP)-Struktur, Shared-Tree |
| RP | Umgekehrte Pfadweiterleitung |
| ÖL | Liste der ausgehenden Schnittstellen |
| MRIB | Multicast Routing Information Base |
| MFIB | Multicast Forwarding Information Base |
| ASM | Quellenunabhängiges Multicast |
| BSR | Bootstrap-Router |
| SSM | Source-Specific Multicast |
| FP | Schneller Pfad |

| | |
|-----|-----------------------|
| SP | Langsamer Pfad |
| CP | Kontrollpunkt |
| PPS | Paketrate pro Sekunde |

Multicast kann auf dem ASA-Gerät in einem von zwei Modi konfiguriert werden:

- PIM Sparse-Mode (Protocol Independent Multicast: [RFC 4601](#))
- IGMP-Stub-Modus (Internet Group Management Protocol: [RFC 2236](#))

Der PIM Sparse-Mode wird bevorzugt, da die ASA über ein echtes Multicast-Routing-Protokoll (PIM) mit Nachbarn kommuniziert. Der IGMP-Stub-Modus war die einzige Multicast-Konfigurationsoption vor der Veröffentlichung von ASA Version 7.0 und wurde durch die einfache Weiterleitung von IGMP-Berichten von Clients an Upstream-Router betrieben.

Komponenten von Multicast

Im Allgemeinen besteht eine Multicast-Infrastruktur aus folgenden Komponenten:

Absender => Host- oder Netzwerkgerät, das den Multicast-Stream generiert. Beispiele hierfür sind Server, der Video- und/oder Audio-Streams sendet, und Netzwerkgeräte, auf denen ein Routing-Protokoll wie EIGRP oder OSPF ausgeführt wird.

Receiver => Host oder Gerät, das den Multicast-Stream empfängt. Dieser Begriff wird häufiger für Hosts verwendet, die aktiv am Datenverkehr interessiert sind und IGMP verwenden, um der betreffenden Multicast-Gruppe beizutreten oder diese zu verlassen.

Router/ASA => Netzwerkgeräte, die für die Verarbeitung und Weiterleitung des Multicast-Streams/Datenverkehrs an andere Segmente des Netzwerks verantwortlich sind, wenn diese von der Quelle an den Client bzw. die Clients benötigt werden.

Multicast Routing Protocol => Verantwortliches Protokoll für die Weiterleitung der Multicast-Pakete Die gängigste Methode ist PIM (Protocol Independent Multicast), aber es gibt noch andere, z. B. MOSPF.

Internet Group Management Protocol (IGMP) => Prozess, mit dem Clients einen Multicast-Stream von einer bestimmten Gruppe empfangen.

PIM Sparse Mode-Betrieb

- Die ASA unterstützt den bidirektionalen PIM Sparse-Mode- und PIM-Modus.
- PIM Sparse-Mode- und IGMP Stub-Mode-Befehle dürfen nicht gleichzeitig konfiguriert werden.
- Beim PIM Sparse-Mode fließt der gesamte Multicast-Verkehr zunächst zum Rendezvous Point (RP) und wird dann an die Empfänger weitergeleitet. Nach einiger Zeit geht der Multicast-Fluss direkt von der Quelle zu den Empfängern (und umgeht den RP).

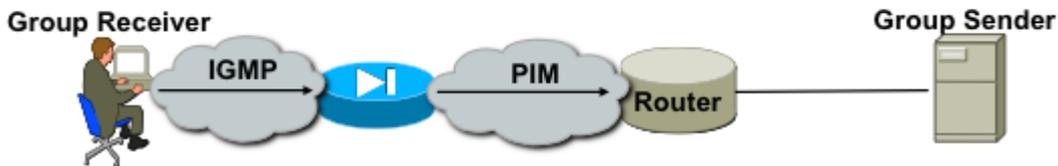
Dieses Bild zeigt eine allgemeine Bereitstellung, bei der die ASA über Multicast-Clients auf einer Schnittstelle und PIM-Nachbarn auf einer anderen verfügt:

- Example operation of firewall in PIM domain with client directly connected to firewall

1. Client sends IGMP Report for group 224.1.2.3

2. Pix sends PIM join/prune with the group to be joined

3. Router receives join/prune and propagates the message to the RP



4. Traffic flows to the pix, and the pix forwards the stream to receiving segment

PIM Sparse-Mode-Beispielkonfiguration

1. Multicast-Routing aktivieren (globaler Konfigurationsmodus)

```
<#root>
```

```
ASA(config)#
```

```
multicast-routing
```

2. Definieren der PIM-Rendezvous-Point-Adresse

```
<#root>
```

```
ASA(config)#
```

```
pim rp-address 172.18.123.3
```

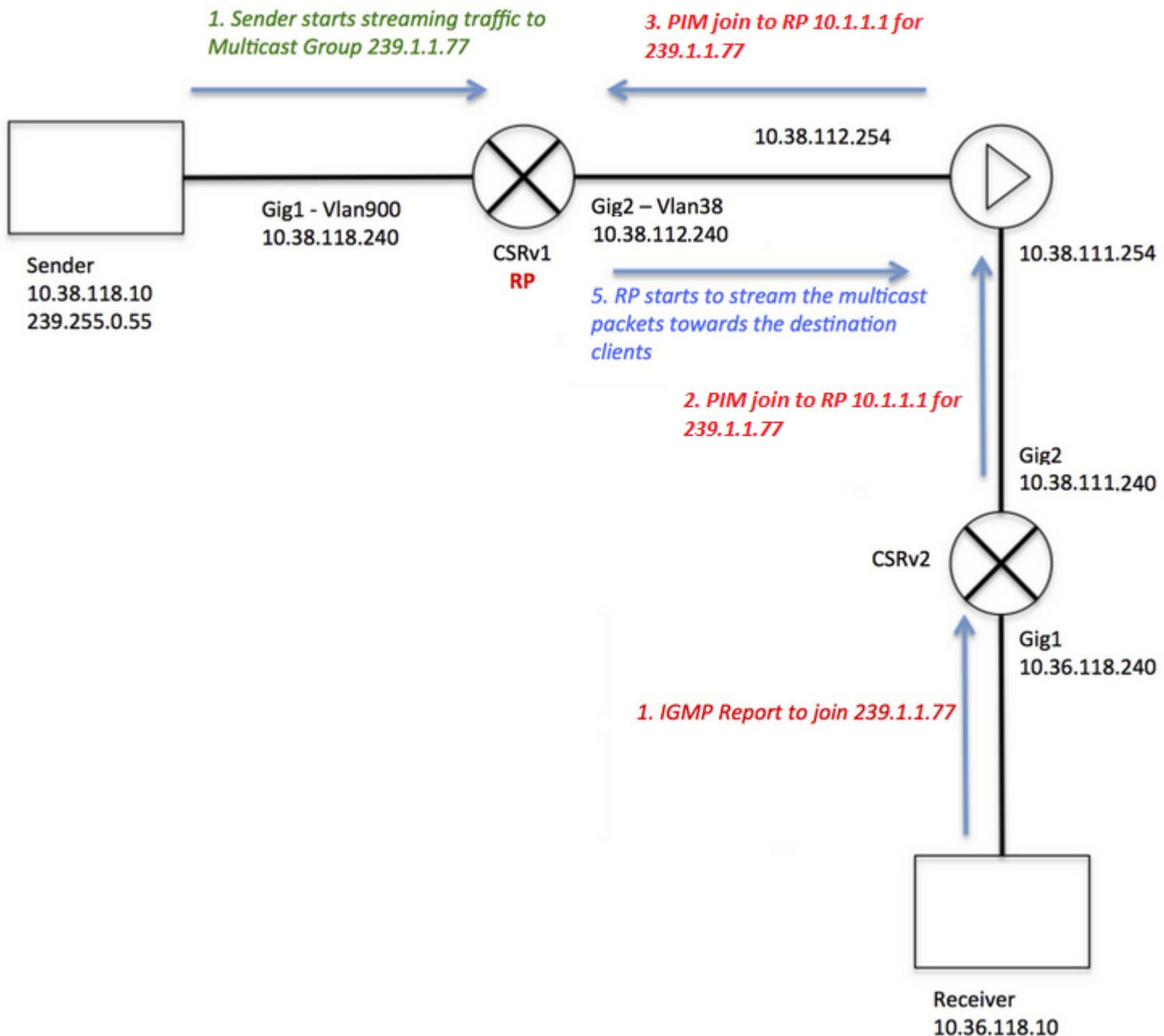
3. Lassen Sie die Multicast-Pakete an der entsprechenden Schnittstelle zu (nur erforderlich, wenn die Sicherheitsrichtlinien der ASA die eingehenden Multicast-Pakete blockieren).

```
<#root>
```

```
access-list 105 extended permit ip any host 224.1.2.3
```

```
access-group 105 in interface outside
```

Beispiel für PIM Sparse Mode:



Beachten Sie, dass die Client-IGMP-Registrierung (Schritte in Rot) und der Stream vom Server empfangen werden (Schritte in Grün) unterschiedlich gefärbt wurden. Auf diese Weise konnte nachgewiesen werden, dass beide Prozesse unabhängig voneinander stattfinden können.

Schritte zur Client-Registrierung (rote Schritte):

1. Client sendet IGMP-Bericht für Gruppe 239.1.1.77
2. Der Router sendet eine PIM-Join-Nachricht an den statischen RP, der für die Gruppe 239.1.1.77 konfiguriert wurde (10.1.1.1).
3. ASA sendet an RP eine PIM Join-Nachricht für die Gruppe 239.1.1.77.

ASA zeigt den PIM *,G-Eintrag in der Ausgabe des Befehls **show mroute** an:

<#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

Da der Quellserver jedoch keinen Stream gestartet hat, zeigt die Ausgabe von "show mfib" auf der ASA keine empfangenen Pakete an:

<#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

Bevor der Server Datenverkehr an die Multicast-Gruppe sendet, zeigt der RP nur einen "*.G"-Eintrag ohne eingehende Schnittstelle in der Liste an, wie z. B.:

<#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

Sobald der Server mit dem Streaming zur Multicast-Gruppe beginnt, erstellt der RP einen "S,G"-Eintrag und platziert die Schnittstelle, die dem Absender gegenübersteht, in der Liste der eingehenden Schnittstellen und beginnt, den Datenverkehr flussabwärts an die ASA zu senden:

```

<#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
  
```

Verwenden Sie diese Befehle für die Verifizierung:

- **show mroute** zeigt einen "S,G"-Eintrag an
- **show mfib**: Zeigt Zähler für weitergeleitete Pakete an
- Befehl **show conn** zeigt die Verbindung an, die mit der Multicast-Gruppen-IP in Zusammenhang steht.

```

<#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 -
```

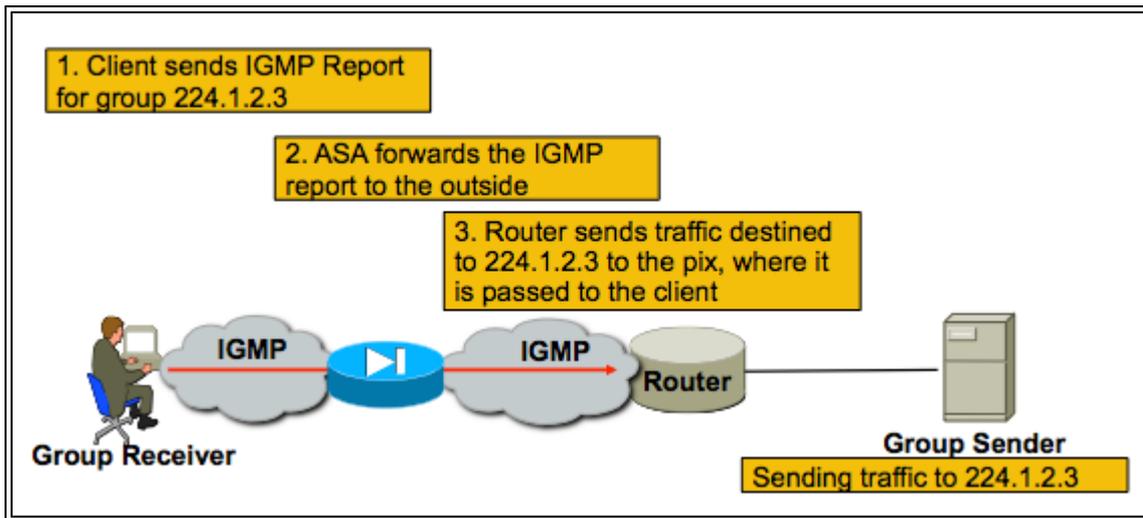
Hinweis: Sobald der Client die Multicast Client-Anwendung schließt, sendet der Host eine IGMP-Abfragemeldung.

Falls dies der einzige Host ist, der vom Router als Client bekannt ist und den Stream empfangen möchte, sendet der Router eine IGMP Prune-Nachricht an den RP.

IGMP-Stub-Modus

- Im IGMP-Stub-Modus agiert die ASA als Multicast-Client und generiert oder leitet IGMP-Berichte (auch als IGMP-Joins bezeichnet) an benachbarte Router weiter, um den Empfang von Multicast-Datenverkehr auszulösen.
- Router senden regelmäßig Anfragen an die Hosts, um festzustellen, ob ein Knoten im Netzwerk weiterhin Multicast-Datenverkehr empfangen möchte.
- Der IGMP-Stub-Modus wird nicht empfohlen, da der PIM Sparse-Mode gegenüber dem Stub-Modus mit zahlreichen Vorteilen verbunden ist (effizienterer Multicast-Datenverkehr, Möglichkeit zur Teilnahme am PIM usw.).

Dieses Bild zeigt die grundlegende Funktionsweise eines ASA, das für den IGMP-Stub-Modus konfiguriert wurde:



IGMP-Stub-Modus-Konfiguration

1. Multicast-Routing aktivieren (globaler Konfigurationsmodus)

```
<#root>
```

```
ASA(config)#
```

```
multicast-routing
```

2. Konfigurieren Sie auf der Schnittstelle, von der die Firewall die igmp-Berichte empfängt, den Befehl `igmp forward-interface`. Leitet die Pakete von der Schnittstelle an die Quelle des Streams weiter. In diesem Beispiel sind die Multicast-Empfänger direkt mit der internen Schnittstelle verbunden, und die Multicast-Quelle befindet sich außerhalb der externen Schnittstelle.

```
<#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. Lassen Sie die Multicast-Pakete an der entsprechenden Schnittstelle zu (nur erforderlich, wenn die Sicherheitsrichtlinie der ASA den eingehenden Multicast-Datenverkehr ablehnt).

```
<#root>
```

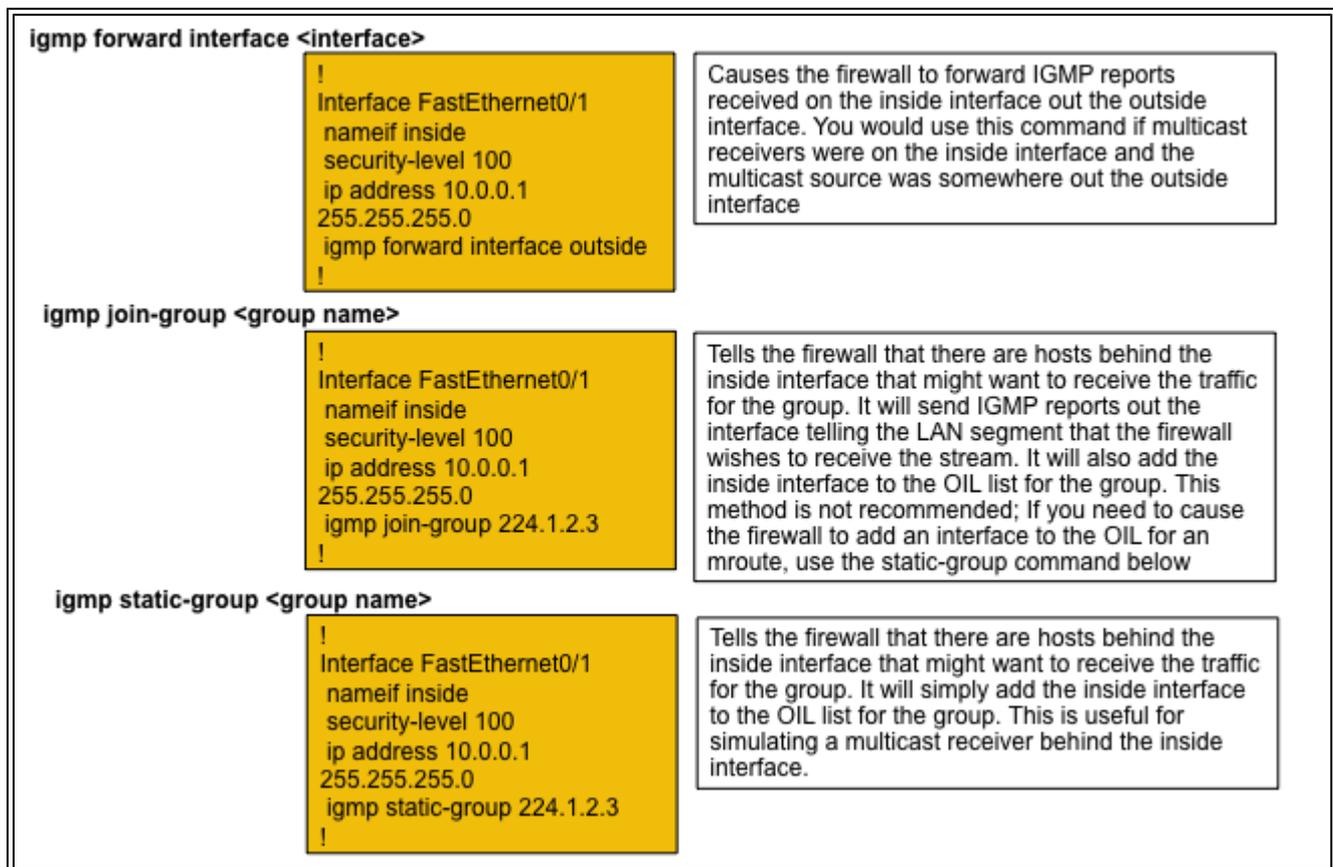
```
ASA(config)#
```

```
access-list 105 extended permit ip any host 224.1.2.3
```

```
ASA(config)#
```

```
access-group 105 in interface outside
```

Häufig bestehen Unklarheiten hinsichtlich der verschiedenen Untermodusbefehle der igmp-Schnittstelle. In diesem Diagramm wird beschrieben, wann die einzelnen Befehle verwendet werden sollten:



Bidir PIM

Im bidirektionalen PIM gibt es keinen Shared Tree (SPT). Das bedeutet drei Dinge:

1. Der erste Hop-Router (mit dem Sender verbunden) sendet keine PIM-Registrierungspakete an den RP.
2. Der RP sendet keine PIM-JOIN-Nachrichten, um dem Quellbaum beizutreten.
3. Router im Pfad zum Empfänger senden PIM-Join-Nachrichten an den RP, um dem RPT beizutreten.

Das bedeutet, dass die ASA kein (S,G) generiert, da Geräte nicht Teil des SPT werden. Der gesamte Multicast-Datenverkehr läuft über den RP. Die ASA leitet den gesamten Multicast-Datenverkehr weiter, solange ein (*,G) vorliegt. Wenn kein (*,G) vorhanden ist, bedeutet dies, dass die ASA niemals ein PIM-Join-Paket empfangen hat. In diesem Fall darf die ASA keine Multicast-Pakete weiterleiten.

Bidir PIM-Konfiguration

1. Multicast-Routing aktivieren (globaler Konfigurationsmodus)

```
<#root>
ASA(config)#
  multicast-routing
```

2. Definieren der PIM-Rendezvous-Point-Adresse

```
<#root>
ASA(config)#
pim rp-address 172.18.123.3 bidir
```

3. Lassen Sie die Multicast-Pakete an der entsprechenden Schnittstelle zu (nur erforderlich, wenn die Sicherheitsrichtlinien der ASA die eingehenden Multicast-Pakete blockieren).

```
<#root>
access-list 105 extended permit ip any host 224.1.2.3
access-group 105 in interface outside
```

Methodik der Fehlerbehebung

Informationen, die bei der Fehlerbehebung von Multicast-Problemen gesammelt werden müssen

Um ein Multicast-Weiterleitungsproblem auf der ASA vollständig zu verstehen und zu diagnostizieren, sind einige oder alle dieser Informationen erforderlich:

âf» Eine Beschreibung der Netzwerktopologie, des Standorts der Multicast-Sender und -Empfänger sowie

des Rendezvous-Points.

ãf» Die spezifische IP-Adresse der Gruppe sowie die verwendeten Ports und Protokolle.

ãf» Syslogs, die von der ASA generiert werden, wenn der Multicast-Stream Probleme aufweist.

ãf» Spezifische Ausgabe des Befehls show von der ASA-Befehlszeilenschnittstelle:

```
<#root>
```

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

ãf» Paketerfassung, um anzuzeigen, ob die Multicast-Daten bei der ASA ankommen und ob die Pakete über die ASA weitergeleitet werden (**notieren Sie sich die IP Time to Live (TTL) des Pakets**. Dies wird durch den Befehl "show capture x detail" angezeigt.)

ãf» Paketerfassung für IGMP- und/oder PIM-Pakete Beispiel:

```
<#root>
```

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

```
>>> This captures the multicast traffic itself
```

```
capture cappiml 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
```

ãf» Informationen von benachbarten Multicast-Geräten (Routern) wie "show mroute" und "show mfib".

ãf» Paketerfassung und/oder Befehle zum Anzeigen, um festzustellen, ob die ASA die Multicast-Pakete verwirft. Mit dem Befehl "show asp drop" kann bestimmt werden, ob die ASA die Pakete verwirft. Darüber hinaus können Paketerfassungen vom Typ "asp-drop" verwendet werden, um alle Pakete zu erfassen, die von der ASA verworfen werden. Anschließend kann überprüft werden, ob die Multicast-Pakete bei der Verwerfenerfassung vorhanden sind.

Hilfreiche Befehlsausgabe anzeigen

Die Ausgabe des Befehls *show mroute* zeigt die verschiedenen Gruppen und Weiterleitungsinformationen und ähnelt stark dem IOS-Befehl *show mroute*. Der Befehl *show mfib* zeigt den Weiterleitungsstatus der verschiedenen Multicast-Gruppen an. Es ist besonders wichtig, den *Weiterleitungspaketzähler* sowie den *Andere* (der Verwerfen anzeigt) zu beobachten:

```
<#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#

```

Mit dem Befehl **clear mfib counters** können die Zähler gelöscht werden. Dieser Befehl ist während des Tests sehr nützlich:

```

<#root>
ciscoasa#
clear mfib counters

```

Paketerfassung

Das integrierte Dienstprogramm zur Paketerfassung ist sehr nützlich, um Probleme mit Multicast zu beheben. In diesem Beispiel werden alle Eingangspakete an der DMZ-Schnittstelle, die an 239.17.17.17 gerichtet sind, erfasst:

```

<#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
....
```

Die Ausgabe des Befehls **show capture x detail** zeigt die TTL der Pakete an, was sehr nützlich ist. In dieser Ausgabe ist die TTL des Pakets 1 (und die ASA übergibt dieses Paket, da es die TTL von IP-Paketen standardmäßig nicht herabsetzt). Ein Downstream-Router würde die Pakete jedoch verwerfen:

```
<#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 0
```

Paketerfassungen sind auch nützlich, um PIM- und IGMP-Datenverkehr zu erfassen. Diese Erfassung zeigt, dass die interne Schnittstelle ein IGMP-Paket (IP-Protokoll 2) empfangen hat, das von 10.0.0.2 stammt:

```
<#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#
```

Beachten Sie, dass die TTL der Pakete mit dem Befehl "show capture x detail" angezeigt werden kann.

Hier sehen wir die durchgeführten ASP-Drop-Captures, die die verworfenen Multicast-Pakete und den Grund für die Verwerfungen zeigen (Punkt-Rate-Limit):

```
<#root>
ASA#
show cap capasp det
12: 14:37:26.538332 c062.6baf.8dc3 0100.5e7f.02c3 0x8100 Length: 1362
```

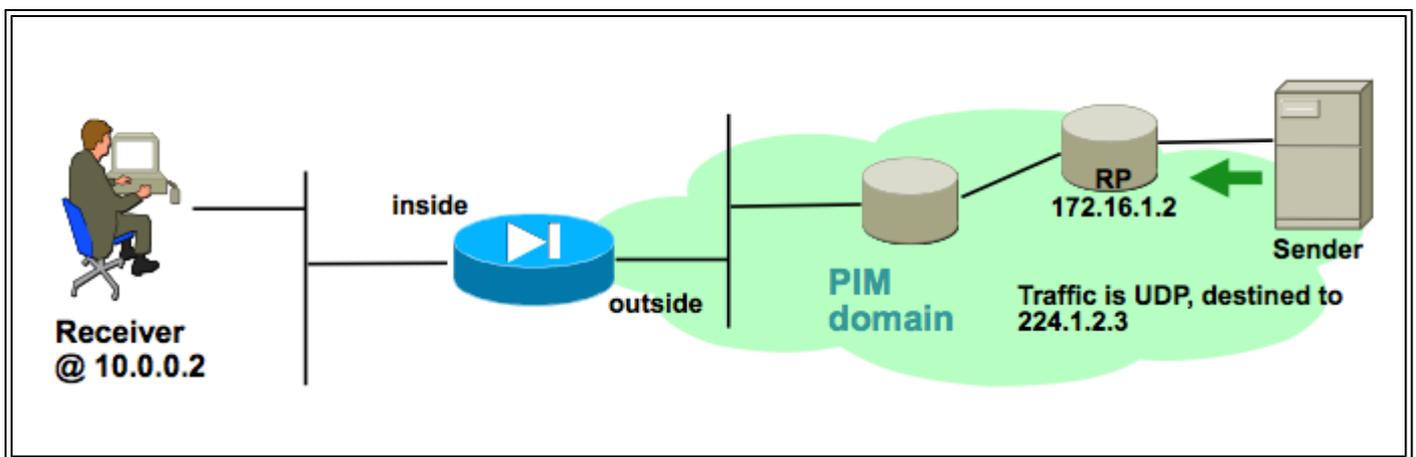
```
802.1Q vlan#1007 P0 10.76.4.95.1806 > 239.255.2.195.5000: [udp sum ok] udp 1316 (DF) [ttl 1] (id
13: 14:37:26.538439 c062.6baf.8dc3 0100.5e7f.02c3 0x8100 Length: 1362
802.1Q vlan#1007 P0 10.76.4.95.1806 > 239.255.2.195.5000: [udp sum ok] udp 1316 (DF) [ttl 1] (id
```

Beispiel für eine ASA PIM Sparse-Mode-Multicast-Bereitstellung

Dieses Diagramm veranschaulicht die Interaktion zwischen ASA und benachbarten Geräten im PIM Sparse-Mode.

Kenntnis der Netzwerktopologie

Bestimmen Sie genau den Standort der Sender und Empfänger des jeweiligen Multicast-Streams. Bestimmen Sie außerdem die IP-Adresse der Multicast-Gruppe und den Ort des Treffpunkts.



In diesem Fall können die Daten an der externen Schnittstelle der ASA empfangen und an den Multicast-Empfänger an der internen Schnittstelle weitergeleitet werden. Da sich der Empfänger im gleichen IP-Subnetz befindet wie die interne Schnittstelle der ASA, wird erwartet, dass ein IGMP-Bericht an der internen Schnittstelle empfangen wird, wenn der Client den Empfang des Streams anfordert. Die IP-Adresse des Absenders lautet 192.168.1.50.

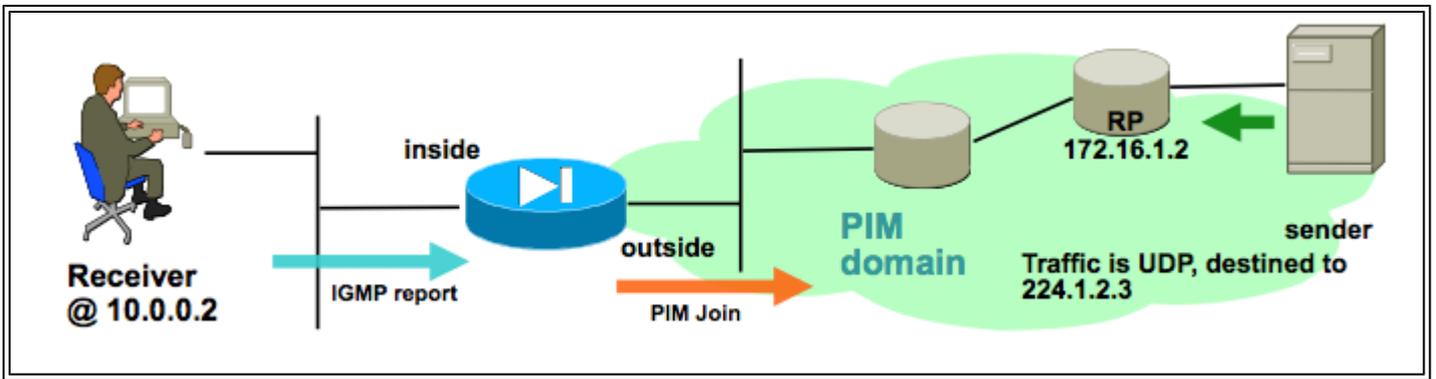
Überprüfen Sie, ob die ASA den IGMP-Bericht vom Empfänger empfängt.

In diesem Beispiel wird der IGMP-Bericht vom Empfänger generiert und von der ASA verarbeitet.

Mithilfe der Paketerfassung und der Ausgabe von *debug igmp* kann überprüft werden, ob die ASA die IGMP-Meldung empfangen und erfolgreich verarbeitet hat.

Vergewissern Sie sich, dass die ASA eine PIM-Join-Nachricht an den Rendezvous Point sendet.

Die ASA interpretiert den IGMP-Bericht und generiert eine PIM-Join-Nachricht. Diese wird dann über die Schnittstelle an den RP gesendet.



Diese Ausgabe stammt aus der debug-PIM-Gruppe 224.1.2.3 und zeigt, dass die ASA die PIM-Join-Nachricht erfolgreich sendet. Der Absender des Multicast-Streams ist 192.168.1.50.

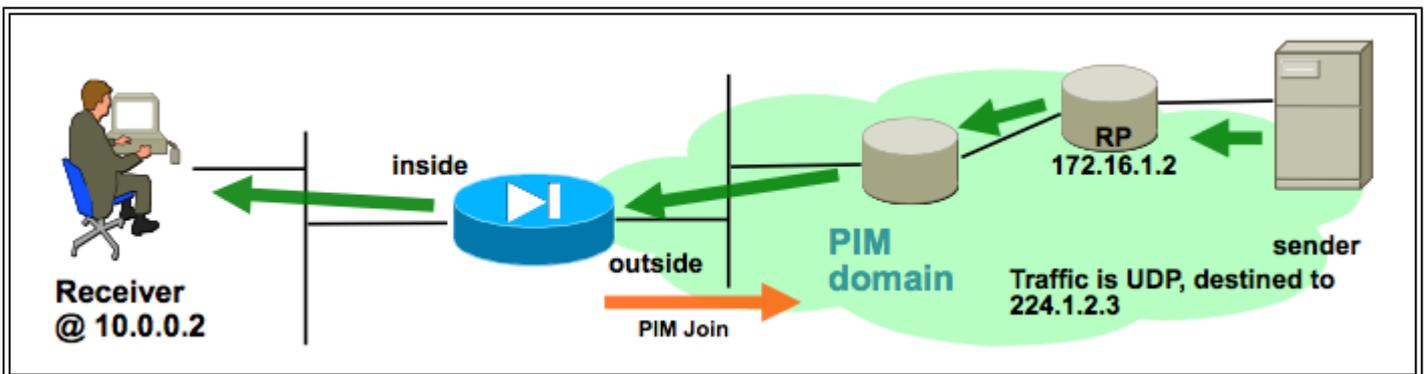
```

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

```

Überprüfen, ob die ASA den Multicast-Stream empfängt und weiterleitet

Die ASA beginnt mit dem Empfang von Multicast-Datenverkehr an der externen Schnittstelle (dargestellt durch die grünen Pfeile) und leitet diesen an die Empfänger im Inneren weiter.



Mit den Befehlen **show mroute** und **show mfib** sowie mit der Paketerfassung kann überprüft werden, ob die ASA die Multicast-Pakete empfängt und weiterleitet.

Eine Verbindung wird in der Verbindungstabelle erstellt, um den Multicast-Stream darzustellen:

```

<#root>
ciscoasa#
show conn
59 in use, 29089 most used

```

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

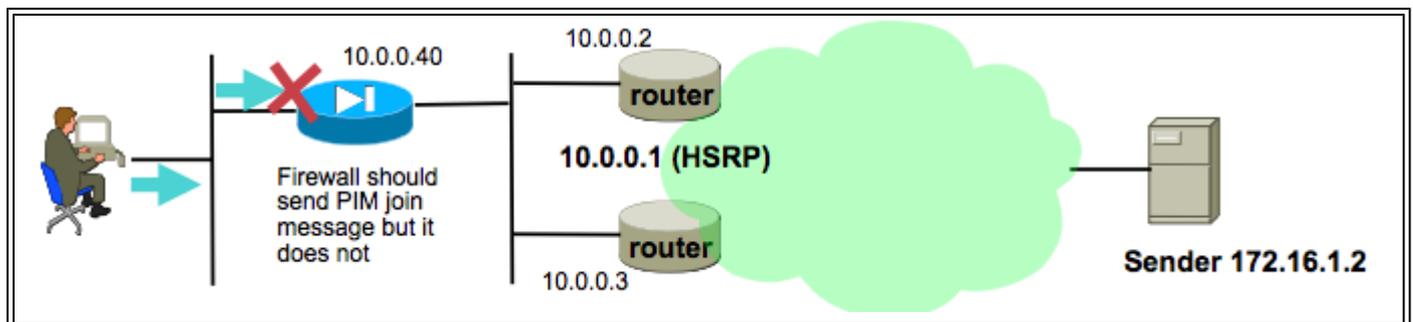
Datenanalyse

Häufige Probleme

In diesem Abschnitt werden eine Reihe von Problemen im Zusammenhang mit ASA-Multicast in der Praxis beschrieben.

Die ASA sendet aufgrund von HSRP keine PIM-Nachrichten an Upstream-Router

Wenn dieses Problem auftritt, kann die ASA keine PIM-Nachrichten von einer Schnittstelle senden. Dieses Diagramm zeigt, dass die ASA keine PIM-Nachrichten an den Absender senden kann. Das gleiche Problem tritt jedoch auf, wenn die ASA eine PIM-Nachricht an den RP senden muss.



Die Ausgabe des Befehls **debug pim** zeigt an, dass die ASA die PIM-Nachricht nicht an den Upstream-Next-Hop-Router senden kann:

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

Dieses Problem betrifft nicht nur die ASA, sondern auch Router. Das Problem wird durch die Kombination der Konfiguration der Routing-Tabelle und der von den PIM-Nachbarn verwendeten HSRP-Konfiguration ausgelöst.

Die Routing-Tabelle verweist auf die HSRP IP 10.0.0.1 als Next-Hop-Gerät:

```
<#root>  
ciscoasa#  
show run route  
route outside 0.0.0.0 0.0.0.0 10.0.0.1 1
```

Die PIM-Nachbarbeziehung wird jedoch zwischen den IP-Adressen der physischen Schnittstellen der Router und nicht der HSRP-IP gebildet:

```

<#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)

```

Weitere Informationen finden Sie unter ["Why does nicht PIM Sparse Mode Work with a Static Route to an HSRP Address?" \(Warum funktioniert der PIM Sparse Mode nicht mit einer statischen Route zu einer HSRP-Adresse?\)](#).

Ein Auszug aus dem Dokument:

Warum sendet der Router keine Join/Prune-Nachricht? RFC 2362 gibt an, dass "ein Router eine periodische Join/Prune-Nachricht an jeden RPF-Nachbarn sendet, der jedem (S,G)-, (,G)- und (*,*,RP)-Eintrag zugeordnet ist. Join/Prune-Nachrichten werden nur gesendet, wenn der RPF-Nachbar ein PIM-Nachbar ist."*

Um das Problem zu beheben, fügen Sie auf der ASA einen statischen Routeneintrag für den betreffenden Datenverkehr hinzu. Vergewissern Sie sich, dass der Verweis auf eine der beiden IP-Adressen für die Router-Schnittstelle (10.0.0.2 oder 10.0.0.3) verweist. In diesem Fall ermöglicht dieser Befehl der ASA das Senden von PIM-Nachrichten, die an den Multicast-Absender 172.16.1.2 gerichtet sind:

```

<#root>

ciscoasa(config)#

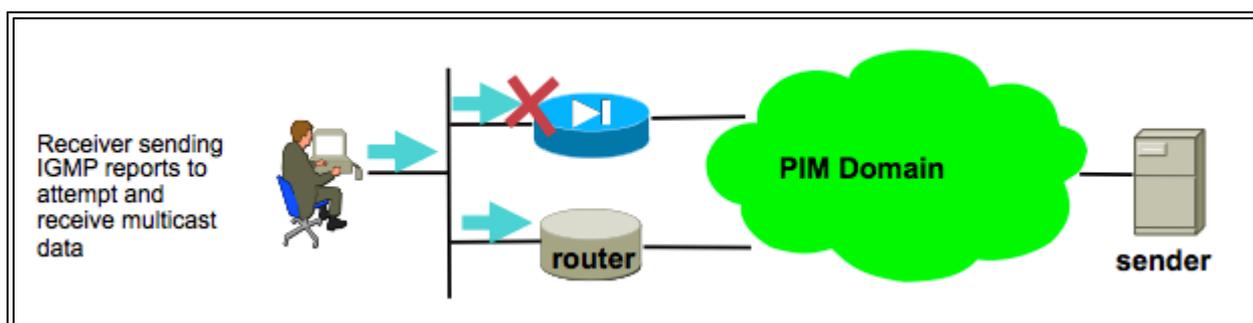
mroute 172.16.1.2 255.255.255.255 10.0.0.3

```

Anschließend überschreibt die Multicast-Routing-Tabelle die Unicast-Routing-Tabelle der ASA, und die ASA sendet die PIM-Nachrichten direkt an den Nachbarn 10.0.0.3.

Die ASA ignoriert IGMP-Berichte, da es sich nicht um den festgelegten Router im LAN-Segment handelt.

Für dieses Problem empfängt die ASA einen IGMP-Bericht von einem direkt verbundenen Multicast-Empfänger, ignoriert diesen jedoch. Es wird keine Debug-Ausgabe generiert, und das Paket wird einfach verworfen, und der Stream-Empfang schlägt fehl.



Bei diesem Problem ignoriert die ASA das Paket, da es sich nicht um den vom PIM ausgewählten

designierten Router im LAN-Segment handelt, in dem sich die Clients befinden.

Diese Ausgabe der ASA CLI zeigt, dass ein anderes Gerät der designierte Router (als "DR" bezeichnet) im internen Schnittstellennetzwerk ist:

```
<#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)
```

PIM ist standardmäßig an allen ASA-Schnittstellen aktiviert, wenn der *Multicast-Routing*-Befehl zur Konfiguration hinzugefügt wird. Wenn sich an der internen Schnittstelle der ASA (in der sich die Clients befinden) weitere PIM-Nachbarn (andere Router oder ASAs) befinden und einer dieser Nachbarn ausgewählt wurde, weil der DR für dieses Segment ausgewählt wurde, dann werden IGMP-Berichte von anderen Nicht-DR-Routern verworfen. Die Lösung besteht darin, PIM auf der Schnittstelle zu deaktivieren (mit dem Befehl *no pim* auf der betroffenen Schnittstelle) oder die ASA als DR für das Segment über den Schnittstellenbefehl **pim dr-priority** festzulegen.

IGMP-Berichte werden von der Firewall abgelehnt, wenn der IGMP-Schnittstellengrenzwert überschritten wird

Standardmäßig lässt die ASA 500 aktuell aktive Joins (Berichte) zu, die über eine Schnittstelle nachverfolgt werden. Dies ist der maximale Wert, der konfiguriert werden kann. Wenn eine große Anzahl von Multicast-Streams von Clients außerhalb einer Schnittstelle angefordert wird, können maximal 500 aktive Joins festgestellt werden, und die ASA könnte zusätzliche eingehende IGMP-Berichte von den Multicast-Empfängern ignorieren.

Um zu überprüfen, ob dies die Ursache eines Multicast-Fehlers ist, geben Sie den Befehl "show igmp interface *interfacename*" ein, und suchen Sie nach den IGMP-Limit-Informationen für die Schnittstelle.

```
<#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
```

Die ASA leitet Multicast-Datenverkehr nicht im Bereich 232.x.x.x/8 weiter.

Dieser Adressbereich ist für Source Specific Multicast (SSM) vorgesehen, das von der ASA derzeit nicht unterstützt wird.

In der Ausgabe des Befehls **debug igmp** wird folgender Fehler angezeigt:

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

Die ASA verwirft Multicast-Pakete aufgrund einer Überprüfung der Umkehrpfad-Weiterleitung

In diesem Fall empfängt die ASA Multicast-Datenverkehr über eine Schnittstelle, wird jedoch nicht an den Empfänger weitergeleitet. Pakete werden von der ASA verworfen, da sie die Sicherheitsüberprüfung von Reverse Path Forwarding (RPF) nicht bestehen. RPF ist auf allen Schnittstellen für Multicast-Datenverkehr aktiviert und kann nicht deaktiviert werden (bei Unicast-Paketen ist die Prüfung standardmäßig nicht aktiviert und wird mit dem Befehl *ip verify reverse path* aktiviert).

Aufgrund der RPF-Prüfung überprüft die ASA beim Empfang von Multicast-Datenverkehr an einer Schnittstelle, ob eine Route zurück zur Quelle des Multicast-Datenverkehrs vorhanden ist (sie prüft die Unicast- und Multicast-Routing-Tabelle) an dieser Schnittstelle. Verfügt er nicht über eine Route zum Absender, verwirft er das Paket. Diese Drops können als Zähler in der Ausgabe von *show asp drop* angezeigt werden:

```
<#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
```

Eine Option besteht darin, eine Route für den Absender des Datenverkehrs hinzuzufügen. In diesem Beispiel wird der Befehl *mroute* verwendet, um die RPF-Prüfung auf Multicast-Datenverkehr von 172.16.1.2 abzudecken, der von der externen Schnittstelle empfangen wurde:

```
<#root>
```

```
ciscoasa(config)#
```

```
mroute 172.16.1.2 255.255.255.255 outside
```

Die ASA generiert beim PIM-Switchover zum Source-Tree keine PIM-Join-Nachricht

Zunächst werden PIM Sparse-Mode-Multicast-Pakete vom Multicast-Sender zum RP und dann vom RP über einen Shared Multicast Tree zum Empfänger übertragen. Wenn die aggregierte Bitrate jedoch einen bestimmten Grenzwert erreicht, versucht der Router, der dem Multicast-Empfänger am nächsten ist, Datenverkehr entlang des quellspezifischen Trees zu empfangen. Dieser Router generiert einen neuen PIM-Join für die Gruppe und sendet diesen an den Absender des Multicast-Streams (und nicht wie zuvor an den RP).

Der Absender des Multicast-Verkehrs kann sich auf einer anderen ASA-Schnittstelle als der RP befinden. Wenn die ASA den PIM-Join erhält, um zum quellspezifischen Tree zu wechseln, muss die ASA über eine Route zur IP-Adresse des Absenders verfügen. Wenn diese Route nicht gefunden wird, werden die PIM-Join-Pakete verworfen, und diese Meldung wird in der Ausgabe von *debug pim* angezeigt.

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

Die Lösung für dieses Problem besteht darin, einen statischen mroute-Eintrag für den Absender des Streams hinzuzufügen, der auf die ASA-Schnittstelle verweist, auf der sich der Absender befindet.

Die ASA verwirft Multicast-Pakete aufgrund von TTL-Überschreitungen (Time To Live).

In diesem Fall schlägt der Multicast-Datenverkehr fehl, da die TTL der Pakete zu niedrig ist. Dies führt dazu, dass die ASA oder ein anderes Gerät im Netzwerk sie verwirft.

Bei Multicast-Paketen wird der IP-TTL-Wert oft sehr niedrig angesetzt, je nachdem, von welcher Anwendung die Pakete gesendet wurden. Manchmal wird dies standardmäßig durchgeführt, um sicherzustellen, dass der Multicast-Verkehr nicht zu weit durch das Netzwerk fließt. Beispielsweise wird standardmäßig das Video-LAN Die Client-Anwendung (ein beliebiger Multicast-Transmitter und ein gängiges Test-Tool) setzt die TTL im IP-Paket standardmäßig auf 1.

Hohe CPU-Auslastung und Paketverluste der ASA aufgrund einer bestimmten Multicast-Topologie

Die CPU der ASA kann sehr hoch sein, und beim Multicast-Stream können Paketverluste auftreten, wenn alle diese Bedingungen für die Multicast-Topologie zutreffen:

1. Die ASA fungiert als RP.
2. Die ASA ist der erste Hop-Empfänger des Multicast-Streams. Das bedeutet, dass sich der Multicast-Absender im gleichen IP-Subnetz wie eine ASA-Schnittstelle befindet.
3. Die ASA ist der Last Hop Router des Multicast-Streams. Das bedeutet, dass sich ein Multicast-Empfänger im gleichen IP-Subnetz wie eine ASA-Schnittstelle befindet.

Wenn alle genannten Symptome auftreten, Aufgrund einer Designeinschränkung ist die ASA gezwungen, den Multicast-Verkehr zu verarbeiten. Dies führt zu Multicast-Streams mit hoher Datenrate, bei denen

Paketverluste auftreten. Der Zähler für das Anzeigen von asp drop, der beim Verwerfen dieser Pakete inkrementiert, ist eine Beschränkung der Punktrate.

Führen Sie die folgenden Schritte aus, um festzustellen, ob ein ASA-Gerät mit diesem Problem konfrontiert ist:

Schritt 1: Überprüfen Sie, ob es sich bei der ASA um den RP handelt:

```
<#root>  
  
show run pim  
show pim tunnel
```

Schritt 2: Überprüfen Sie, ob die ASA der letzte Hop-Router ist:

```
<#root>  
  
show igmp group  
  
<mcast_group_IP>
```

Schritt 3: Überprüfen Sie, ob es sich bei der ASA um den ersten Hop-Router handelt:

```
<#root>  
  
show mroute  
  
<mcast_group_IP>
```

Folgende Schritte können unternommen werden, um dieses Problem zu beheben:

- Ändern Sie die Topologie so, dass ASA nicht der RP ist. Oder stellen Sie sicher, dass der Absender oder Empfänger nicht direkt mit der ASA verbunden ist.
- Verwenden Sie anstelle von PIM den IGMP-Stub-Modus für die Multicast-Weiterleitung.

Die ASA verwirft die ersten Pakete, wenn ein Multicast-Stream gestartet wird

Wenn die ersten Pakete eines Multicast-Streams bei der ASA eingehen, muss die ASA diese spezielle Multicast-Verbindung und den zugehörigen Routing-Eintrag erstellen, um die Pakete weiterzuleiten. Während der Eintrag erstellt wird, können einige Multicast-Pakete verworfen werden, bis die mroute und die Verbindungen hergestellt sind (dies dauert in der Regel weniger als eine Sekunde). Nach Abschluss der Einrichtung des Multicast-Streams sind die Pakete nicht mehr auf die Übertragungsrates beschränkt.

Bei Paketen, die aus diesem Grund verworfen wurden, wurde der ASP-Verwerfungsgrund "(punt-rate-limit) Punt rate limit beyond" (Grenzwert für die Punt-Rate) überschritten. Dies ist die Ausgabe von "show capture asp" (wobei "asp" eine ASP-Ablagerungserfassung ist, die auf dem ASA-Gerät konfiguriert wurde, um verworfene Pakete zu erfassen), und Sie können die Multicast-Pakete sehen, die aus diesem Grund verworfen wurden:

<#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 1

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

2 packets shown

Ein trennender Multicast-Empfänger unterbricht den Empfang der Multicast-Gruppe an anderen Schnittstellen.

Dieses Problem tritt nur bei ASAs auf, die im IGMP-Stub-Modus arbeiten. ASAs, die am PIM-Multicast-Routing teilnehmen, sind nicht betroffen.

Das Problem wird anhand der Cisco Bug-ID [CSCeg48235](#) identifiziert. IGMP Leave auf einer Schnittstelle unterbricht den Multicast-Verkehr auf anderen Schnittstellen.

Dies ist der Release-Hinweis des Bugs, der das Problem erklärt:

Symptom:

When a PIX or ASA firewall is configured for IGMP stub mode multicast reception and traffic from a multi

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

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 IGMP

Die ASA verwirft Multicast-Pakete aufgrund der Sicherheitsrichtlinie für ausgehende Zugriffslisten.

Bei diesem spezifischen Problem verwirft die ASA Multicast-Pakete (gemäß der konfigurierten Sicherheitsrichtlinie). Für den Netzwerkadministrator ist es jedoch schwierig, den Grund für das Verwerfen von Paketen zu ermitteln. In diesem Fall verwirft die ASA Pakete aufgrund der für eine Schnittstelle konfigurierten Liste ausgehender Zugriffe. Die Problemumgehung besteht darin, den Multicast-Stream in der ausgehenden Zugriffsliste zuzulassen.

In diesem Fall werden Multicast-Pakete mit dem ASP-Drop-Zähler "FP no mcast output intrf (no-mcast-intrf)" verworfen.

Die ASA verwirft fortlaufend einige Pakete (aber nicht alle) in einen Multicast-Stream, da die Durchsatzrate für die Kontrollpunkte begrenzt wird.

Der Datenverkehr wird wahrscheinlich aufgrund der Durchsatzratenbegrenzung durch den Kontrollpunkt begrenzt. Sehen Sie sich die asp-Drop-Ausgabe an, und erfassen Sie zur Bestätigung:

<#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

Der Eintrag mfib zeigt an, dass der gesamte Datenverkehr prozessgesteuert ist:

<#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

Die Multicast-Routing-Tabelle zeigt ein (*,G), aber kein (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

Das Problem hierbei ist, dass die TTL der an der ASA eingehenden Multicast-Datenpakete 1 ist. Die ASA leitet diese Pakete an das Downstream-Gerät weiter (da sie die TTL nicht herabsetzt), aber der Router verwirft die Pakete Downstream. Daher sendet der Downstream-Router keine PIM-Verbindung (S,G-Verbindung) (eine quellspezifische Verbindung) an die ASA an den Absender. Die ASA erstellt erst dann einen (S,G)-Eintrag, wenn sie diesen PIM-Join erhält. Da (S,G) nicht erstellt wird, wird der gesamte Multicast-Verkehr per Prozess-Switching weitergeleitet, wodurch eine Durchsatzbegrenzung erreicht wird.

Die Lösung für dieses Problem besteht darin, sicherzustellen, dass der TTL-Wert der Pakete nicht 1 ist, sodass das Downstream-Gerät die quellspezifische Verbindung an den Absender senden kann. Dadurch installiert die ASA eine quellspezifische Route in der Tabelle, und dann werden alle Pakete schnell vermittelt (anstatt verarbeitet zu werden), und der Datenverkehr muss problemlos durch die ASA fließen.

Der Multicast-Stream wird aufgrund einer PIM ASSERT-Nachricht angehalten.

Wenn zwei Netzwerkgeräte die gleichen Multicast-Pakete an dasselbe Subnetz weiterleiten, muss idealerweise eines davon die Weiterleitung der Pakete beenden (da es Verschwendung ist, den Stream zu duplizieren). Wenn PIM-Router erkennen, dass sie die gleichen Pakete erhalten, die sie auch an derselben Schnittstelle erzeugen, generieren sie ASSERT-Nachrichten in diesem LAN, um auszuwählen, welches Netzwerkgerät den Stream nicht mehr weiterleitet.

Weitere Informationen zu dieser Meldung finden Sie in einem [Abschnitt von RFC 4601 zum ASSERT-Prozess](#).

Die Fehlerbehebungen zeigen, dass die ASA einen IGMP-Bericht für die Gruppe 239.1.1.227 empfängt, diesen jedoch aufgrund der Bestätigungsmeldung ignoriert, die sie von einem benachbarten Router empfängt:

```
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)
```

Dieses Problem wurde in einem Produktionsnetzwerk beobachtet, in dem zwei Standorte versehentlich auf Layer 2 überbrückt wurden. Das LAN, in dem sich die Multicast-Empfänger befanden, verfügte also über zwei Geräte, die Multicast-Datenverkehr an sie weiterleiteten. Aufgrund eines weiteren Netzwerkproblems konnten sich die ASA und ein anderes Gerät nicht über PIM-Hellos gegenseitig erkennen. Aus diesem Grund übernahmen beide die Rolle des designierten Routers für das LAN. Dies führte dazu, dass der Multicast-Datenverkehr eine Weile funktionierte und dann fehlschlug, als die ASSERT-Nachrichten von den Geräten gesendet wurden. Um das Problem zu beheben, wurde die falsche Verbindung, die die Geräte auf Layer 2 überbrückte, deaktiviert und das Problem dann behoben.

ASA sendet PIM-Join, wird aber aufgrund einer Paketgröße größer als MTU nicht

vom Nachbarn verarbeitet

Dies wurde bei 629575899 beobachtet. Die ASA wurde für Jumbo-Frames konfiguriert, der 4900 nicht. Wenn der Client mehr als 73 Multicast-Streams angefordert hat, funktionieren bestimmte Multicast-Streams nicht. 73 SGs erstellen eine PIM-Join-Nachricht der Größe 1494, die noch MTU-Werte erreicht. 74 SGs erstellen eine PIM-Join-Nachricht, die größer als 1500 ist, wodurch die 4900M das eingehende Paket verwerfen.

Das Problem wurde wie folgt behoben:

1. Stellen Sie sicher, dass Jumbo Frames auf dem 4900M global aktiviert sind.
2. Konfigurieren Sie die physische Schnittstelle und die SVI mit einer MTU von 9216.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.