Fehlerbehebung: ACI Intra-Fabric Forwarding - MultiPod Forwarding

Inhalt

Einleitung

In diesem Dokument werden die Schritte zum Verständnis und zur Fehlerbehebung in einem ACI-Szenario mit Multi-Pod-Weiterleitung beschrieben.

Hintergrundinformationen

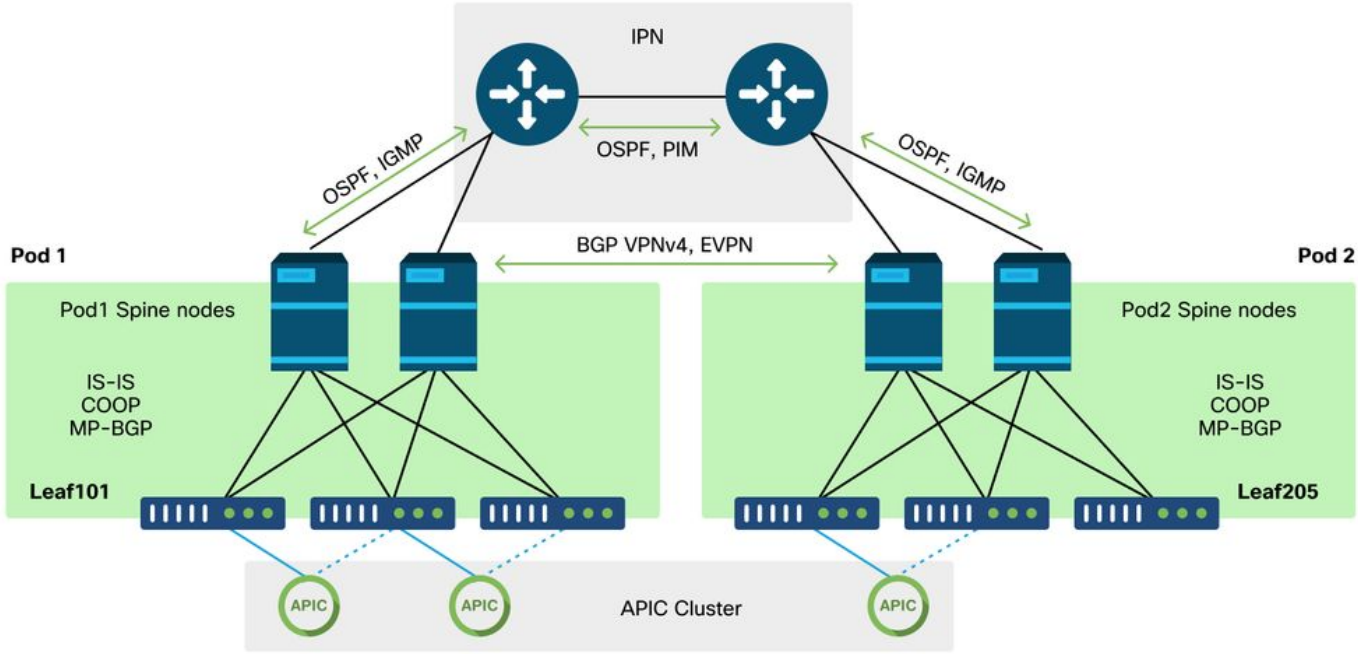
Das Material aus diesem Dokument wurde aus dem Fehlerbehebung: Cisco Application Centric Infrastructure, Second Edition Buch, insbesondere das **Fabric-interne Weiterleitung - Multi-Pod-Weiterleitung** Kapitel.

Multi-Pod Forwarding - Überblick

In diesem Kapitel wird die Fehlerbehebung in Szenarien beschrieben, in denen die Verbindung zwischen PODs in einer Multi-Pod-Umgebung nicht richtig funktioniert.

Bevor Sie sich einige Beispiele zur Fehlerbehebung ansehen, sollten Sie sich einen Moment Zeit nehmen, um die Multi-Pod-Komponenten umfassend zu verstehen.

Multi-Pod-Komponenten



Ähnlich wie bei einer traditionellen ACI-Fabric gilt eine Multi-Pod-Fabric immer noch als eine einzige ACI-Fabric und ist für das Management auf einen einzigen APIC-Cluster angewiesen.

Innerhalb jedes einzelnen POD nutzt die ACI im Overlay dieselben Protokolle wie eine

herkömmliche Fabric. Dazu gehören IS-IS für den Austausch von TEP-Informationen sowie die Auswahl von Multicast Outgoing Interface (OIF), COOP für ein globales Endpunkt-Repository und BGP VPNv4 für die Verteilung externer Router über die Fabric.

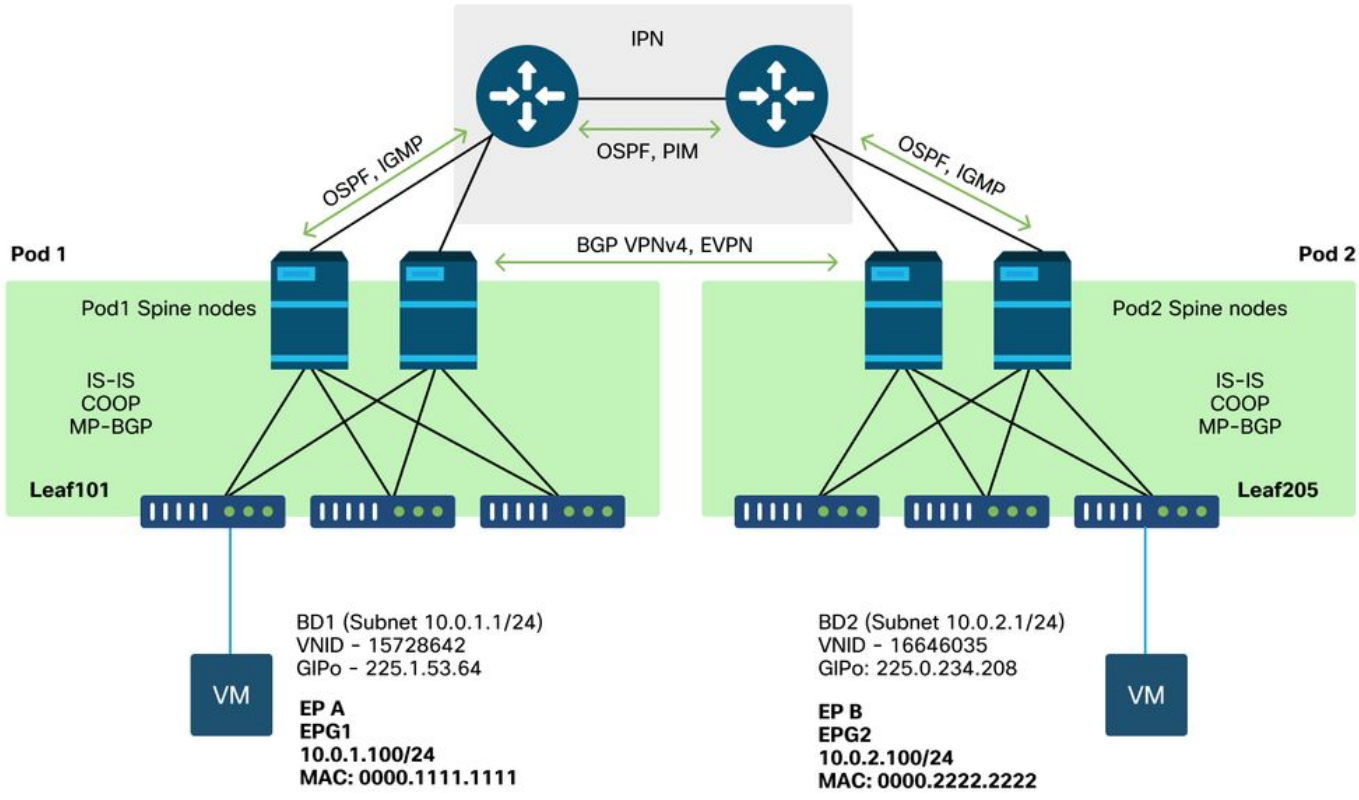
Multi-Pod baut auf diesen Komponenten auf, da es jeden Pod miteinander verbinden muss.

- Zum Austausch von Routing-Informationen über TEPs im Remote-Pod wird der zusammenfassende TEP-Pool über das IPN mit OSPF angekündigt.
- Zum Austausch externer Routen, die von einem Pod an einen anderen übertragen wurden, wird die BGP VPNv4-Adressfamilie auf die Spine-Knoten erweitert. Jeder Pod wird zu einem separaten Routen-Reflektor-Cluster.
- Zur Synchronisierung von Endpunkten und anderen in COOP über PODs gespeicherten Informationen wird die BGP EVPN-Adressfamilie auf die Spine-Knoten erweitert.
- Um die Überflutung von Broadcast-, Unknown-Unicast- und Multicast (BUM)-Datenverkehr zwischen PODs zu bewältigen, fungieren die Spine-Knoten in jedem Pod als IGMP-Hosts, und die IPN-Router tauschen Multicast-Routing-Informationen über bidirektionales PIM aus.

Ein Großteil der Szenarien und Workflows zur Multi-Pod-Fehlerbehebung ähnelt den Single-Pod-ACI-Fabrics. Dieser Abschnitt zu Multi-Pod befasst sich hauptsächlich mit den Unterschieden zwischen Single-Pod- und Multi-Pod-Weiterleitung.

Topologie für Multi-Pod - Beispiele

Wie bei allen Szenarien ist es auch bei der Fehlerbehebung wichtig, den erwarteten Status zu kennen. Verweisen Sie auf diese Topologie für die Beispiele in diesem Kapitel.



Allgemeiner Workflow zur Fehlerbehebung bei der Multi-Pod-Weiterleitung

Auf hoher Ebene können beim Debuggen eines Problems mit Multi-Pod-Weiterleitung die folgenden Schritte evaluiert werden:

1. Handelt es sich bei dem Fluss um Unicast oder ein Multi-Destination-Paket? Denken Sie daran, dass selbst wenn erwartet wird, dass der Datenfluss im funktionierenden Zustand als Unicast vorliegt, es sich bei dem nicht aufgelösten ARP um einen Multidestination-Datenfluss handelt.
2. Wird der Fluss geroutet oder überbrückt? Aus ACI-Sicht ist ein gerouteter Datenfluss in der Regel jeder Datenfluss, bei dem die Ziel-MAC-Adresse die Router-MAC-Adresse ist, die einem auf der ACI konfigurierten Gateway gehört. Wenn ARP-Flooding deaktiviert ist, wird das Eingangs-Leaf außerdem auf Basis der Ziel-IP-Adresse geroutet. Wenn die Ziel-MAC-Adresse nicht der ACI gehört, leitet der Switch die Daten entweder basierend auf der MAC-Adresse weiter oder verwendet das in der Bridge-Domäne konfigurierte Unicast-Verhalten.
3. Lässt das Eingangsblatt den Fluss fallen? fTriage und ELAM sind die besten Tools, um dies zu bestätigen.

Wenn es sich um Layer-3-Unicast handelt:

1. Verfügt das Eingangs-Leaf über einen Endpunkt, der für die Ziel-IP-Adresse in derselben VRF-Instanz wie die Quell-EPG lernt? In diesem Fall hat dies stets Vorrang vor allen erlernten Routen. Das Leaf leitet den Datenverkehr direkt an die Tunneladresse oder die Ausgangsschnittstelle weiter, von der der Endpunkt erfasst wird.
2. Wenn es keine Endgeräteerfassung gibt, verfügt der Eingangs-Leaf über eine Route für das Ziel, für das die Markierung "Pervasive" festgelegt wurde? Dies weist darauf hin, dass das Ziel-Subnetz als Bridge-Domain-Subnetz konfiguriert ist und dass der Next-Hop der Spine-Proxy im lokalen Pod sein sollte.
3. Wenn es keine Pervasive Route gibt, dann wäre das letzte Mittel jede Route, die durch ein L3Out gelernt wird. Dieser Abschnitt ist identisch mit der L3Out-Weiterleitung über einen einzelnen Pod.

Wenn es sich um Layer-2-Unicast handelt:

1. Verfügt das Eingangs-Leaf über einen Endpunkt, der in derselben Bridge-Domäne wie die Quell-EPG nach der Ziel-MAC-Adresse sucht? Wenn dies der Fall ist, leitet der Leaf die Daten an die Remote-Tunnel-IP oder die lokale Schnittstelle weiter, von der der Endpunkt empfangen wird.
2. Wenn in der Quell-Bridge-Domäne keine Informationen für die Ziel-MAC-Adresse vorhanden sind, leitet das Leaf basierend auf dem BD-Verhalten "unknown-unicast" weiter. Wenn sie auf "Flood" (Überschwemmung) festgelegt ist, wird das Leaf an die GIPo-Multicast-Gruppe überflutet, die der Bridge-Domäne zugewiesen ist. Lokale und entfernte PODs sollten eine geflutete Kopie erhalten. Wenn sie auf 'Hardware Proxy' gesetzt ist, wird der Frame zur Proxy-Suche an den Spine gesendet und basierend auf dem COOP-Eintrag des Spines weitergeleitet.

Da sich die Fehlerbehebungsausgaben für Unicast erheblich von denen für BUM unterscheiden, werden Arbeitsausgaben und Szenarien für Unicast vor dem Umstieg auf BUM berücksichtigt.

Multi-Pod Unicast-Fehlerbehebungs-Workflow

Befolgen Sie die Topologie, und gehen Sie durch den Fluss von 10.0.2.100 auf leaf205 zu 10.0.1.100 auf leaf101.

Bevor Sie an dieser Stelle fortfahren, müssen Sie überprüfen, ob für die Quelle ARP für das Gateway (für einen gerouteten Fluss) oder die MAC-Zieladresse (für einen überbrückten Fluss) aufgelöst ist.

1. Bestätigen Sie, dass der Eingangs-Leaf das Paket empfängt. Verwenden Sie das im Abschnitt "Tools" gezeigte ELAM CLI-Tool zusammen mit der in 4.2 verfügbaren Berichtsausgabe. Die ELAM Assistant-App wird ebenfalls verwendet.

```
module-1# debug platform internal tah elam asic 0
module-1(DBG-elam)# trigger reset
module-1(DBG-elam)# trigger init in-select 6 out-select 1
module-1(DBG-elam-insel6)# set outer ipv4 src_ip 10.0.2.100 dst_ip 10.0.1.100
module-1(DBG-elam-insel6)# start
module-1(DBG-elam-insel6)# status
ELAM STATUS
===========
Asic 0 Slice 0 Status Armed
Asic 0 Slice 1 Status Triggered
```

Beachten Sie, dass das ELAM ausgelöst wird und bestätigt, dass das Paket am Eingangs-Switch empfangen wurde. Sehen Sie sich nun einige Felder im Bericht an, da die Ausgabe umfangreich ist.

```
================================================================================================
===========
                                                        Captured Packet

================================================================================================
===========

------------------------------------------------------------------------------------------------
-----------
Outer Packet Attributes
------------------------------------------------------------------------------------------------
-----------
Outer Packet Attributes       : l2uc ipv4 ip ipuc ipv4uc
Opcode                        : OPCODE_UC

------------------------------------------------------------------------------------------------
-----------
Outer L2 Header
------------------------------------------------------------------------------------------------
-----------
Destination MAC               : 0022.BDF8.19FF
Source MAC                    : 0000.2222.2222
802.1Q tag is valid           : yes( 0x1 )
CoS                           : 0( 0x0 )
Access Encap VLAN             : 1021( 0x3FD )

------------------------------------------------------------------------------------------------
------------
Outer L3 Header
```

```
-------------------------------------------------------------------------------------------
------------
L3 Type                      : IPv4
IP Version                   : 4
DSCP                         : 0
IP Packet Length             : 84 ( = IP header(28 bytes) + IP payload )
Don't Fragment Bit           : not set
TTL                          : 255
IP Protocol Number           : ICMP
IP CheckSum                  : 10988( 0x2AEC )
Destination IP               : 10.0.1.100
Source IP                    : 10.0.2.100
```

Der Bericht enthält weitere Informationen zum Speicherort des Pakets. Die ELAM Assistant-App ist jedoch derzeit für die Interpretation dieser Daten nützlicher. Die ELAM Assistant-Ausgabe für diesen Fluss wird später in diesem Kapitel gezeigt.

2. Lernt der Eingangs-Leaf das Ziel als Endpunkt in der Eingangs-VRF-Instanz? Wenn nicht, gibt es eine Route?

```
a-leaf205# show endpoint ip 10.0.1.100 detail
Legend:
s - arp              H - vtep             V - vpc-attached     p - peer-aged
R - peer-attached-rl B - bounce           S - static           M - span
D - bounce-to-proxy  O - peer-attached    a - local-aged       m - svc-mgr
L - local            E - shared-service
+-----------------------------------+---------------+-----------------+--------------+----------
---+----------------------------+
    VLAN/                           Encap           MAC Address       MAC Info/
Interface     Endpoint Group
    Domain                          VLAN            IP Address        IP Info
                  Info
+-----------------------------------+---------------+-----------------+--------------+----------
---+----------------------------+
```

Keine Ausgabe im obigen Befehl bedeutet, dass die Ziel-IP-Adresse nicht erfasst wird. Überprüfen Sie anschließend die Routing-Tabelle.

```
a-leaf205# show ip route 10.0.1.100 vrf Prod:Vrf1
IP Route Table for VRF "Prod:Vrf1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

10.0.1.0/24, ubest/mbest: 1/0, attached, direct, pervasive
  *via 10.0.120.34%overlay-1, [1/0], 01:55:37, static, tag 4294967294
       recursive next hop: 10.0.120.34/32%overlay-1
```

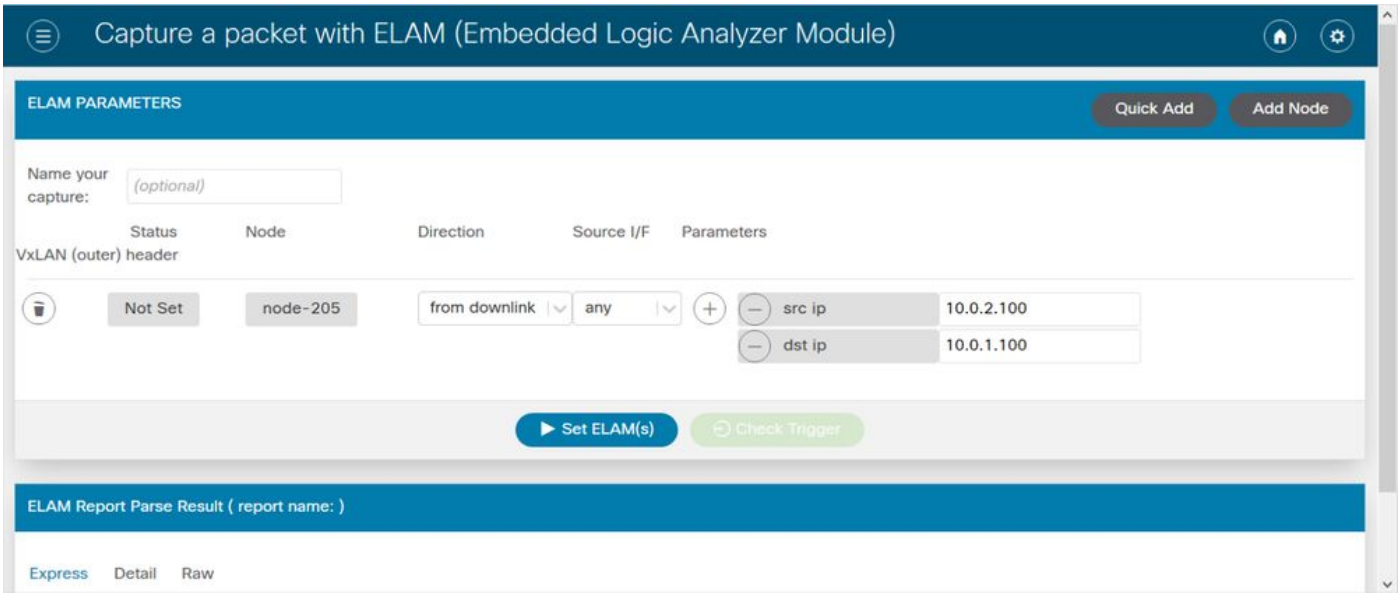
In der obigen Ausgabe wird das Kennzeichen angezeigt, das anzeigt, dass es sich um eine Bridge-Domain-Subnetzroute handelt. Next-Hop sollte eine Anycast-Proxy-Adresse auf den Spines sein.

```
a-leaf205# show isis dtep vrf overlay-1 | grep 10.0.120.34
10.0.120.34        SPINE   N/A             PHYSICAL,PROXY-ACAST-V4
```

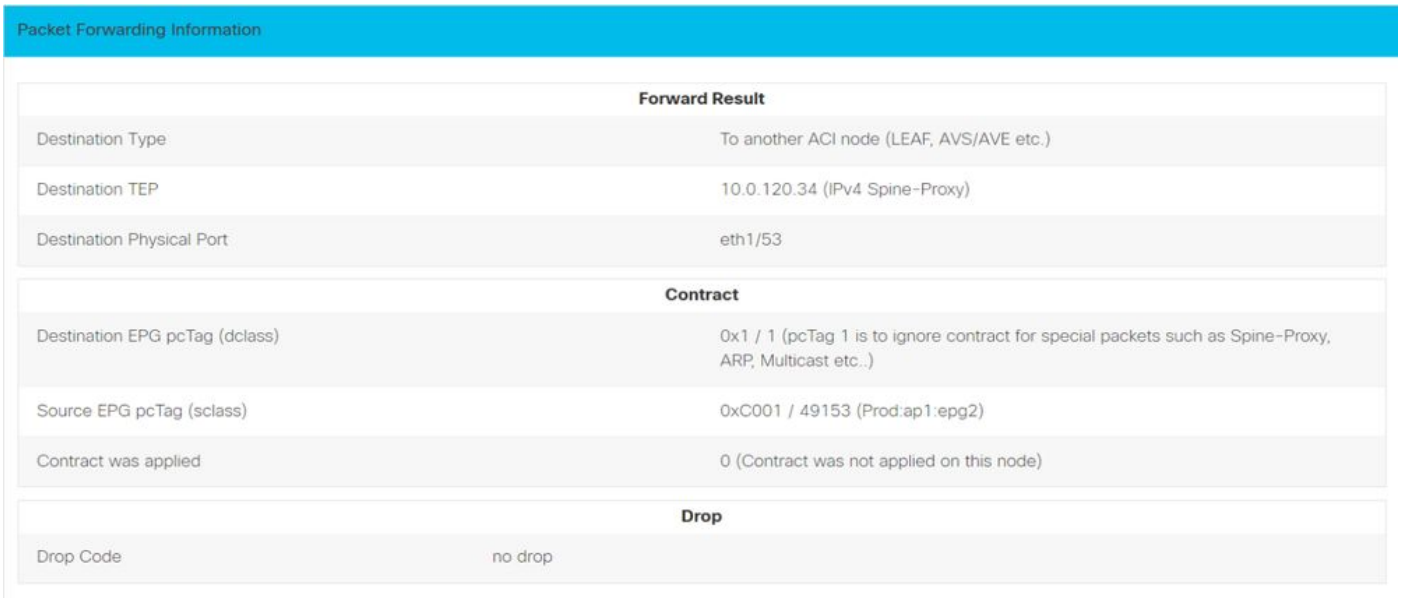
Beachten Sie, dass die Erkennung des Endpunkts über einen Tunnel oder eine physische Schnittstelle Vorrang hat, sodass das Paket direkt dorthin weitergeleitet wird. Weitere Informationen finden Sie im Kapitel "Externe Weiterleitung" dieses Buchs.

Verwenden Sie den ELAM-Assistenten, um die Weiterleitungsentscheidungen in den oben genannten Ausgaben zu bestätigen.

Konfiguration des ELAM-Assistenten



Weiterleitungsentscheidungen überprüfen



Die Ausgabe oben zeigt, dass der Eingangs-Leaf das Paket an die IPv4-Spine-Proxyadresse weiterleitet. Das wird erwartet.

3. Vergewissern Sie sich auf dem Spine, dass die Ziel-IP in COOP vorhanden ist, sodass die Proxy-Anforderung funktioniert.

Es gibt mehrere Möglichkeiten, die COOP-Ausgabe auf dem Spine zu erhalten, zum Beispiel sehen Sie es mit einem 'show coop internal info ip-db' Befehl:

```
a-spine4# show coop internal info ip-db | grep -B 2 -A 15 "10.0.1.100"
```

```
------------------------------
IP address : 10.0.1.100
Vrf : 2392068 <-- This vnid should correspond to vrf where the IP is learned. Check operational
tab of the tenant vrfs
Flags : 0x2
EP bd vnid : 15728642
EP mac :  00:00:11:11:11:11
Publisher Id : 192.168.1.254
Record timestamp : 12 31 1969 19:00:00 0
Publish timestamp : 12 31 1969 19:00:00 0
Seq No: 0
Remote publish timestamp: 09 30 2019 20:29:07 9900483
URIB Tunnel Info
Num tunnels : 1
      Tunnel address : 10.0.0.34 <-- When learned from a remote pod this will be an External
Proxy TEP. We'll cover this more
      Tunnel ref count : 1

------------------------------
```

Weitere Befehle, die auf dem Spine ausgeführt werden:

COOP für L2-Eintrag abfragen:

```
moquery -c coopEpRec -f 'coop.EpRec.mac=="00:00:11:11:22:22"
```

COOP für L3-Eintrag abfragen und übergeordneten L2-Eintrag abrufen:

```
moquery -c coopEpRec -x rsp-subtree=children 'rsp-subtree-
filter=eq(coopIpv4Rec.addr,"192.168.1.1")' rsp-subtree-include=required
```

COOP nur für L3-Eintrag abfragen:

```
moquery -c coopIpv4Rec -f 'coop.Ipv4Rec.addr=="192.168.1.1"'
```

Das Nützliche an der Multiple-Moquery ist, dass sie auch direkt auf einem APIC ausgeführt werden können und der Benutzer jeden Spine sehen kann, der den Datensatz in coop hat.

4. Weiterleitungsentscheidung für Multi-Pod Spine-Proxy

Wenn der COOP-Eintrag des Spine auf einen Tunnel im lokalen Pod verweist, basiert die Weiterleitung auf dem traditionellen ACI-Verhalten.

Beachten Sie, dass der Besitzer einer TEP im Fabric überprüft werden kann, indem er von einem APIC ausgeführt wird: **moquery -c ipv4Addr -f 'ipv4.Addr.addr=="<Tunneladresse>"**

Im Proxyszenario lautet der nächste Tunnelhop 10.0.0.34. Wer ist der Besitzer dieser IP-Adresse?:

```
a-apic1# moquery -c ipv4Addr -f 'ipv4.Addr.addr=="10.0.0.34"' | grep dn
dn               : topology/pod-1/node-1002/sys/ipv4/inst/dom-overlay-1/if-[lo9]/addr-
[10.0.0.34/32]
dn               : topology/pod-1/node-1001/sys/ipv4/inst/dom-overlay-1/if-[lo2]/addr-
[10.0.0.34/32]
```

Diese IP gehört beiden Spine-Knoten in Pod 1. Dies ist eine spezifische IP, die als externe Proxy-Adresse bezeichnet wird. Ebenso wie die ACI über Proxy-Adressen verfügt, die den Spine-Knoten innerhalb eines Pod gehören (siehe Schritt 2 dieses Abschnitts), sind auch dem Pod selbst Proxy-

Adressen zugewiesen. Dieser Schnittstellentyp kann wie folgt überprüft werden:

```
a-apic1# moquery -c ipv4If -x rsp-subtree=children 'rsp-subtree-
filter=eq(ipv4Addr.addr,"10.0.0.34")' rsp-subtree-include=required

...
# ipv4.If
mode         : anycast-v4,external

# ipv4.Addr
 addr             : 10.0.0.34/32
 dn               : topology/pod-1/node-1002/sys/ipv4/inst/dom-overlay-1/if-[lo9]/addr-
[10.0.0.34/32]
```

Das Flag "extern" zeigt an, dass es sich um einen externen Proxy-TEP handelt.

5. Überprüfen Sie das BGP EVPN auf dem Spine.

Der Datensatz des COOP-Endpunkts muss aus BGP EVPN auf dem Spine importiert werden. Der folgende Befehl kann verwendet werden, um zu überprüfen, ob es sich in EVPN befindet (wenn es sich jedoch bereits in COOP mit einem Next-Hop des externen Remote-Pod-Proxys TEP befindet, kann davon ausgegangen werden, dass es von EVPN stammt):

```
a-spine4# show bgp l2vpn evpn 10.0.1.100 vrf overlay-1
Route Distinguisher: 1:16777199
BGP routing table entry for [2]:[0]:[15728642]:[48]:[0000.1111.1111]:[32]:[10.0.1.100]/272,
version 689242 dest ptr 0xaf42a4ca
Paths: (2 available, best #2)
Flags: (0x000202 00000000) on xmit-list, is not in rib/evpn, is not in HW, is locked
Multipath: eBGP iBGP

 Path type: internal 0x40000018 0x2040 ref 0 adv path ref 0, path is valid, not best reason:
Router Id, remote nh not installed
 AS-Path: NONE, path sourced internal to AS
  192.168.1.254 (metric 7) from 192.168.1.102 (192.168.1.102)
    Origin IGP, MED not set, localpref 100, weight 0
    Received label 15728642 2392068
    Received path-id 1
    Extcommunity:
        RT:5:16
        SOO:1:1
        ENCAP:8
        Router MAC:0200.0000.0000

          Advertised path-id 1
 Path type: internal 0x40000018 0x2040 ref 1 adv path ref 1, path is valid, is best path, remote
nh not installed
 AS-Path: NONE, path sourced internal to AS
  192.168.1.254 (metric 7) from 192.168.1.101 (192.168.1.101)
    Origin IGP, MED not set, localpref 100, weight 0
    Received label 15728642 2392068
    Received path-id 1
    Extcommunity:
        RT:5:16
        SOO:1:1
        ENCAP:8
        Router MAC:0200.0000.0000

          Path-id 1 not advertised to any peer
```

Beachten Sie, dass der obige Befehl auch für eine MAC-Adresse ausgeführt werden kann.

-192.168.1.254 ist die TEP des Datenflugzeugs, die während der Multi-Pod-Einrichtung konfiguriert wurde. Beachten Sie jedoch, dass der Next-Hop der externe Proxy-TEP ist, obwohl er im BGP als NH angekündigt wird.

-192.168.1.101 und .102 sind die Pod 1 Spine-Knoten, die diesen Pfad ankündigen.

6. Überprüfen Sie COOP auf den Spines im Ziel-Pod.

Der gleiche Befehl wie zuvor kann verwendet werden:

```
a-spine2# show coop internal info ip-db | grep -B 2 -A 15 "10.0.1.100"

------------------------------
IP address : 10.0.1.100
Vrf : 2392068
Flags : 0
EP bd vnid : 15728642
EP mac :  00:50:56:81:3E:E6
Publisher Id : 10.0.72.67
Record timestamp : 10 01 2019 15:46:24 502206158
Publish timestamp : 10 01 2019 15:46:24 524378376
Seq No: 0
Remote publish timestamp: 12 31 1969 19:00:00 0
URIB Tunnel Info
Num tunnels : 1
      Tunnel address : 10.0.72.67
      Tunnel ref count : 1

------------------------------
```

Überprüfen Sie mithilfe des folgenden Befehls auf einem APIC, wer die Tunneladresse besitzt:

```
a-apic1# moquery -c ipv4Addr -f 'ipv4.Addr.addr=="10.0.72.67"'
Total Objects shown: 1

# ipv4.Addr
addr             : 10.0.72.67/32
childAction      :
ctrl             :
dn               : topology/pod-1/node-101/sys/ipv4/inst/dom-overlay-1/if-[lo0]/addr-
[10.0.72.67/32]
ipv4CfgFailedBmp :
ipv4CfgFailedTs  : 00:00:00:00.000
ipv4CfgState     : 0
lcOwn            : local
modTs            : 2019-09-30T18:42:43.262-04:00
monPolDn         : uni/fabric/monfab-default
operSt           : up
operStQual       : up
pref             : 0
rn               : addr-[10.0.72.67/32]
status           :
tag              : 0
type             : primary
vpcPeer          : 0.0.0.0
```

Der obige Befehl zeigt, dass der Tunnel von COOP auf leaf101 verweist. Dies bedeutet, dass

leaf101 den lokalen Lernprozess für den Zielendpunkt haben sollte.

7. Überprüfen Sie, ob der Ausgangs-Leaf über den lokalen Lernpfad verfügt.

Dies kann über den Befehl "show endpoint" erfolgen:

```
a-leaf101# show endpoint ip 10.0.1.100 detail
Legend:
s - arp              H - vtep             V - vpc-attached     p - peer-aged
R - peer-attached-rl B - bounce           S - static           M - span
D - bounce-to-proxy  O - peer-attached    a - local-aged       m - svc-mgr
L - local            E - shared-service
+------------------------------------+--------------+-----------------+-------------+----------
---+----------------------------+
    VLAN/                           Encap           MAC Address       MAC Info/
Interface     Endpoint Group
    Domain                          VLAN            IP Address        IP
Info                        Info
+------------------------------------+--------------+-----------------+-------------+----------
---+----------------------------+
341                                     vlan-1075    0000.1111.1111 LV
po5                 Prod:ap1:epg1
Prod:Vrf1                               vlan-1075        10.0.1.100 LV
po5
```

Beachten Sie, dass der Endpunkt gelernt ist. Das Paket muss basierend auf Port-Channel 5 mit eingestelltem VLAN-Tag 1075 weitergeleitet werden.

Verwenden von fTriage zum Überprüfen des End-to-End-Datenflusses

Wie im Abschnitt "Tools" dieses Kapitels beschrieben, kann fTriage verwendet werden, um einen vorhandenen Flow-to-End abzubilden und zu verstehen, was jeder Switch im Pfad mit dem Paket macht. Dies ist besonders bei größeren und komplexeren Bereitstellungen wie Multi-Pod nützlich.

Beachten Sie, dass fTriage einige Zeit in Anspruch nehmen wird, um vollständig ausgeführt zu werden (potenziell 15 Minuten).

Wenn fTriage für den Beispielablauf ausgeführt wird:

```
a-apic1# ftriage route -ii LEAF:205 -dip 10.0.1.100 -sip 10.0.2.100
fTriage Status: {"dbgFtriage": {"attributes": {"operState": "InProgress", "pid": "7297",
"apicId": "1", "id": "0"}}}
Starting ftriage
Log file name for the current run is: ftlog_2019-10-01-16-04-15-438.txt
2019-10-01 16:04:15,442 INFO     /controller/bin/ftriage route -ii LEAF:205 -dip 10.0.1.100 -sip
10.0.2.100
2019-10-01 16:04:38,883 INFO     ftriage:     main:1165 Invoking ftriage with default password
and default username: apic#fallback\\admin
2019-10-01 16:04:54,678 INFO     ftriage:     main:839  L3 packet Seen on a-leaf205 Ingress:
Eth1/31  Egress: Eth1/53 Vnid: 2392068
2019-10-01 16:04:54,896 INFO     ftriage:     main:242  ingress encap string vlan-1021
2019-10-01 16:04:54,899 INFO     ftriage:     main:271  Building ingress BD(s), Ctx
2019-10-01 16:04:56,778 INFO     ftriage:     main:294  Ingress BD(s) Prod:Bd2
2019-10-01 16:04:56,778 INFO     ftriage:     main:301  Ingress Ctx: Prod:Vrf1
2019-10-01 16:04:56,887 INFO     ftriage:   pktrec:490  a-leaf205: Collecting transient losses
snapshot for LC module: 1
2019-10-01 16:05:22,458 INFO     ftriage:     main:933  SIP 10.0.2.100 DIP 10.0.1.100
```

```
2019-10-01 16:05:22,459 INFO     ftriage:  unicast:973  a-leaf205: <- is ingress node
2019-10-01 16:05:25,206 INFO     ftriage:  unicast:1215 a-leaf205: Dst EP is remote
2019-10-01 16:05:26,758 INFO     ftriage:     misc:657  a-leaf205: DMAC(00:22:BD:F8:19:FF) same
as RMAC(00:22:BD:F8:19:FF)
2019-10-01 16:05:26,758 INFO     ftriage:     misc:659  a-leaf205: L3 packet getting
routed/bounced in SUG
2019-10-01 16:05:27,030 INFO     ftriage:     misc:657  a-leaf205: Dst IP is present in SUG L3
tbl
2019-10-01 16:05:27,473 INFO     ftriage:     misc:657  a-leaf205: RwDMAC DIPo(10.0.72.67) is
one of dst TEPs ['10.0.72.67']
2019-10-01 16:06:25,200 INFO     ftriage:     main:622  Found peer-node a-spine3 and IF: Eth1/31
in candidate list
2019-10-01 16:06:30,802 INFO     ftriage:     node:643  a-spine3: Extracted Internal-port GPD
Info for lc: 1
2019-10-01 16:06:30,803 INFO     ftriage:     fcls:4414 a-spine3: LC trigger ELAM with IFS:
Eth1/31 Asic :3 Slice: 1 Srcid: 24
2019-10-01 16:07:05,717 INFO     ftriage:     main:839  L3 packet Seen on a-spine3 Ingress:
Eth1/31 Egress: LC-1/3 FC-24/0 Port-1 Vnid: 2392068
2019-10-01 16:07:05,718 INFO     ftriage:   pktrec:490  a-spine3: Collecting transient losses
snapshot for LC module: 1
2019-10-01 16:07:28,043 INFO     ftriage:      fib:332  a-spine3: Transit in spine
2019-10-01 16:07:35,902 INFO     ftriage:  unicast:1252 a-spine3: Enter dbg_sub_nexthop with
Transit inst: ig infra: False glbs.dipo: 10.0.72.67
2019-10-01 16:07:36,018 INFO     ftriage:  unicast:1417 a-spine3: EP is known in COOP (DIPo =
10.0.72.67)
2019-10-01 16:07:40,422 INFO     ftriage:  unicast:1458 a-spine3: Infra route 10.0.72.67 present
in RIB
2019-10-01 16:07:40,423 INFO     ftriage:     node:1331 a-spine3: Mapped LC interface: LC-1/3
FC-24/0 Port-1 to FC interface: FC-24/0 LC-1/3 Port-1
2019-10-01 16:07:46,059 INFO     ftriage:     node:460  a-spine3: Extracted GPD Info for fc: 24
2019-10-01 16:07:46,060 INFO     ftriage:     fcls:5748 a-spine3: FC trigger ELAM with IFS: FC-
24/0 LC-1/3 Port-1 Asic :0 Slice: 1 Srcid: 40
2019-10-01 16:08:06,735 INFO     ftriage:  unicast:1774 L3 packet Seen on FC of node: a-spine3
with Ingress: FC-24/0 LC-1/3 Port-1  Egress: FC-24/0 LC-1/3 Port-1 Vnid: 2392068
2019-10-01 16:08:06,735 INFO     ftriage:   pktrec:487  a-spine3: Collecting transient losses
snapshot for FC module: 24
2019-10-01 16:08:09,123 INFO     ftriage:     node:1339 a-spine3: Mapped FC interface: FC-24/0
LC-1/3 Port-1 to LC interface: LC-1/3 FC-24/0 Port-1
2019-10-01 16:08:09,124 INFO     ftriage:  unicast:1474 a-spine3: Capturing Spine  Transit pkt-
type L3 packet on egress LC on Node: a-spine3 IFS: LC-1/3 FC-24/0 Port-1
2019-10-01 16:08:09,594 INFO     ftriage:     fcls:4414 a-spine3: LC trigger ELAM with IFS: LC-
1/3 FC-24/0 Port-1 Asic :3 Slice: 1 Srcid: 48
2019-10-01 16:08:44,447 INFO     ftriage:  unicast:1510 a-spine3: L3 packet Spine egress
Transit pkt Seen on a-spine3 Ingress: LC-1/3 FC-24/0 Port-1 Egress: Eth1/29 Vnid: 2392068
2019-10-01 16:08:44,448 INFO     ftriage:   pktrec:490  a-spine3: Collecting transient losses
snapshot for LC module: 1
2019-10-01 16:08:46,691 INFO     ftriage:  unicast:1681 a-spine3: Packet is exiting the fabric
through {a-spine3: ['Eth1/29']} Dipo 10.0.72.67 and filter SIP 10.0.2.100 DIP 10.0.1.100
2019-10-01 16:10:19,947 INFO     ftriage:     main:716  Capturing L3 packet Fex: False on node:
a-spine1 IF: Eth2/25
2019-10-01 16:10:25,752 INFO     ftriage:     node:643  a-spine1: Extracted Internal-port GPD
Info for lc: 2
2019-10-01 16:10:25,754 INFO     ftriage:     fcls:4414 a-spine1: LC trigger ELAM with IFS:
Eth2/25 Asic :3 Slice: 0 Srcid: 24
2019-10-01 16:10:51,164 INFO     ftriage:     main:716  Capturing L3 packet Fex: False on node:
a-spine2 IF: Eth1/31
2019-10-01 16:11:09,690 INFO     ftriage:     main:839  L3 packet Seen on a-spine2 Ingress:
Eth1/31 Egress: Eth1/25 Vnid: 2392068
2019-10-01 16:11:09,690 INFO     ftriage:   pktrec:490  a-spine2: Collecting transient losses
snapshot for LC module: 1
2019-10-01 16:11:24,882 INFO     ftriage:      fib:332  a-spine2: Transit in spine
2019-10-01 16:11:32,598 INFO     ftriage:  unicast:1252 a-spine2: Enter dbg_sub_nexthop with
Transit inst: ig infra: False glbs.dipo: 10.0.72.67
2019-10-01 16:11:32,714 INFO     ftriage:  unicast:1417 a-spine2: EP is known in COOP (DIPo =
```

```
10.0.72.67)
2019-10-01 16:11:36,901 INFO     ftriage:  unicast:1458 a-spine2: Infra route 10.0.72.67 present
in RIB
2019-10-01 16:11:47,106 INFO     ftriage:     main:622  Found peer-node a-leaf101 and IF:
Eth1/54 in candidate list
2019-10-01 16:12:09,836 INFO     ftriage:     main:839  L3 packet Seen on a-leaf101 Ingress:
Eth1/54 Egress: Eth1/30 (Po5) Vnid: 11470
2019-10-01 16:12:09,952 INFO     ftriage:   pktrec:490  a-leaf101: Collecting transient losses
snapshot for LC module: 1
2019-10-01 16:12:30,991 INFO     ftriage:     nxos:1404 a-leaf101: nxos matching rule id:4659
scope:84 filter:65534
2019-10-01 16:12:32,327 INFO     ftriage:     main:522  Computed egress encap string vlan-1075
2019-10-01 16:12:32,333 INFO     ftriage:     main:313  Building egress BD(s), Ctx
2019-10-01 16:12:34,559 INFO     ftriage:     main:331  Egress Ctx Prod:Vrf1
2019-10-01 16:12:34,560 INFO     ftriage:     main:332  Egress BD(s): Prod:Bd1
2019-10-01 16:12:37,704 INFO     ftriage:  unicast:1252 a-leaf101: Enter dbg_sub_nexthop with
Local inst: eg infra: False glbs.dipo: 10.0.72.67
2019-10-01 16:12:37,705 INFO     ftriage:  unicast:1257 a-leaf101: dbg_sub_nexthop invokes
dbg_sub_eg for ptep
2019-10-01 16:12:37,705 INFO     ftriage:  unicast:1784 a-leaf101: <- is egress node
2019-10-01 16:12:37,911 INFO     ftriage:  unicast:1833 a-leaf101: Dst EP is local
2019-10-01 16:12:37,912 INFO     ftriage:     misc:657  a-leaf101: EP if(Po5) same as egr
if(Po5)
2019-10-01 16:12:38,172 INFO     ftriage:     misc:657  a-leaf101: Dst IP is present in SUG L3
tbl
2019-10-01 16:12:38,564 INFO     ftriage:     misc:657  a-leaf101: RW seg_id:11470 in SUG same
as EP segid:11470
fTriage Status: {"dbgFtriage": {"attributes": {"operState": "Idle", "pid": "0", "apicId": "0",
"id": "0"}}}
fTriage Status: {"dbgFtriage": {"attributes": {"operState": "Idle", "pid": "0", "apicId": "0",
"id": "0"}}}
```

Die fTriage enthält eine große Datenmenge. Einige der wichtigsten Felder sind hervorgehoben. Beachten Sie, dass der Pfad des Pakets "leaf205 (Pod 2) > spine3 (Pod 2) > spine2 (Pod 1) > leaf101 (Pod 1)" lautete. Alle Entscheidungen über die Weiterleitung und die unterwegs getroffenen Vertragsabfragen werden ebenfalls angezeigt.

Wenn es sich um einen Layer-2-Fluss handelt, muss die Syntax von fTriage wie folgt festgelegt werden:

```
ftriage bridge -ii LEAF:205 -dmac 00:00:11:11:22:22
```

Proxyanforderungen, bei denen das EP nicht im COOP enthalten ist

Bevor Sie bestimmte Fehlerszenarien in Betracht ziehen, sollten Sie noch einen weiteren Aspekt im Zusammenhang mit der Unicast-Weiterleitung über Multi-Pod erörtern. Was passiert, wenn der Zielendpunkt unbekannt ist, die Anforderung an einen Proxy gesendet wird und der Endpunkt sich nicht in der COOP befindet?

In diesem Szenario wird das Paket/der Frame an den Spine gesendet, und eine Glean-Anforderung wird generiert.

Wenn die Spine eine Glean-Anforderung generiert, wird das ursprüngliche Paket in der Anforderung beibehalten. Das Paket erhält jedoch den Ethertype 0xfff2, einen benutzerdefinierten Ethertype, der für Gleans reserviert ist. Aus diesem Grund wird es nicht einfach sein, diese Nachrichten in Paketerfassungstools wie Wireshark zu interpretieren.

Für das äußere Layer-3-Ziel ist ebenfalls 239.255.255.240 festgelegt, was eine reservierte Multicast-Gruppe speziell für gelangende Nachrichten ist. Diese sollten über die Fabric geleitet

werden, und alle Egress-Leaf-Switches, auf denen das Ziel-Subnetz der bereitgestellten Glean-Anforderung ausgeführt wird, generieren eine ARP-Anforderung zur Auflösung des Ziels. Diese ARPs werden von der konfigurierten BD-Subnetz-IP-Adresse gesendet (daher können Proxyanforderungen den Standort von Silent-/Unknown-Endpunkten nicht auflösen, wenn Unicast-Routing in einer Bridge-Domäne deaktiviert ist).

Der Empfang der "Glean"-Nachricht auf dem Egress-Leaf und die anschließend generierte ARP- und empfangene ARP-Antwort kann mithilfe des folgenden Befehls überprüft werden:

Glean ARP-Verifizierung

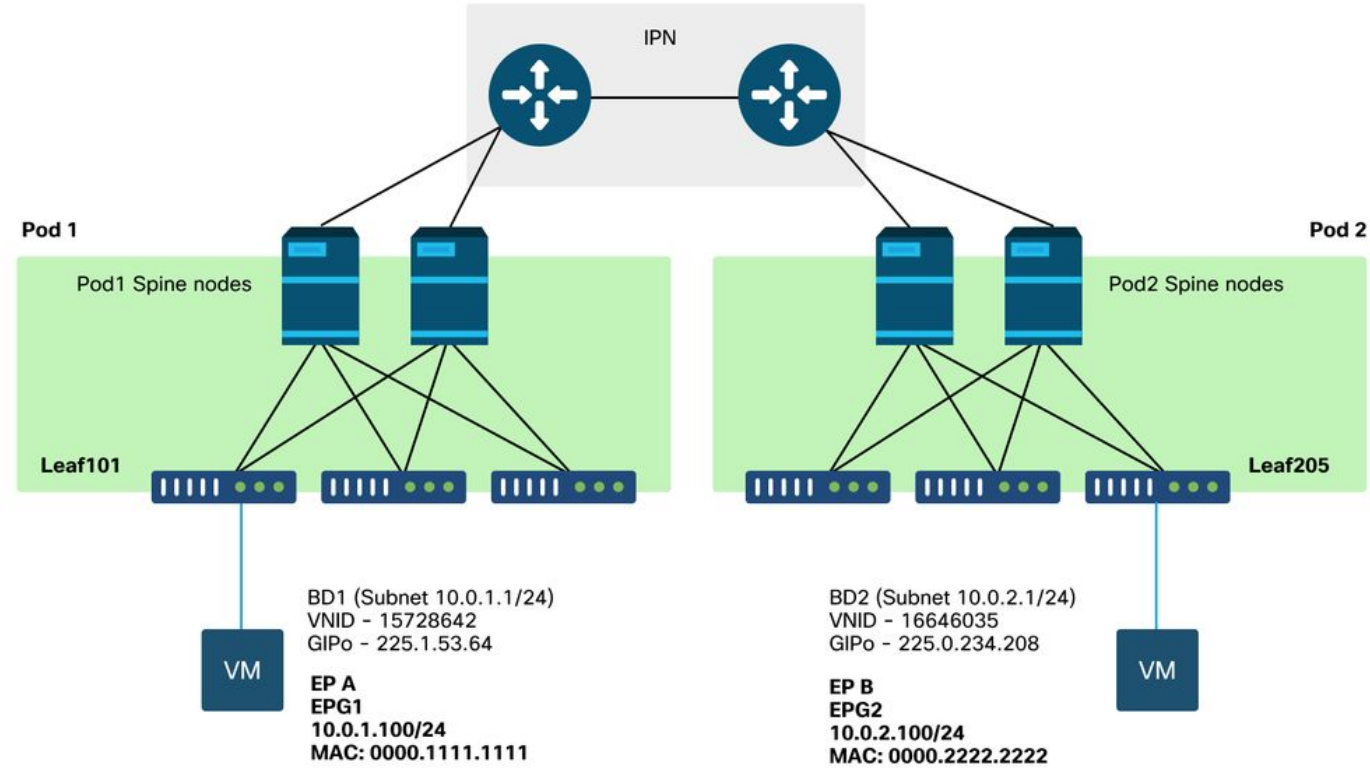
```
a-leaf205# show ip arp internal event-history event | grep -F -B 1 192.168.21.11
...
73) Event:E_DEBUG_DSF, length:127, at 316928 usecs after Wed May  1 08:31:53 2019
Updating epm ifidx: 1a01e000 vlan: 105 ip: 192.168.21.11, ifMode: 128 mac: 8c60.4f02.88fc   <<<
Endpoint is learned
75) Event:E_DEBUG_DSF, length:152, at 316420 usecs after Wed May  1 08:31:53 2019
log_collect_arp_pkt; sip = 192.168.21.11; dip = 192.168.21.254; interface = Vlan104;info = Garp
Check adj:(nil)  <<< Response received
77) Event:E_DEBUG_DSF, length:142, at 131918 usecs after Wed May  1 08:28:36 2019
log_collect_arp_pkt; dip = 192.168.21.11; interface = Vlan104;iod = 138; Info = Internal Request
Done   <<< ARP request is generated by leaf
78) Event:E_DEBUG_DSF, length:136, at 131757 usecs after Wed May  1 08:28:36 2019   <<< Glean
received, Dst IP is in BD subnet
log_collect_arp_glean;dip = 192.168.21.11;interface = Vlan104;info = Received pkt Fabric-Glean:
1
79) Event:E_DEBUG_DSF, length:174, at 131748 usecs after Wed May  1 08:28:36 2019
log_collect_arp_glean; dip = 192.168.21.11; interface = Vlan104; vrf = CiscoLive2019:vrf1; info
= Address in PSVI subnet or special VIP   <<< Glean Received, Dst IP is in BD subnet
```

Zum Vergleich: Wenn "Glean Messages" an den 239.255.255.240 gesendet werden, muss diese Gruppe in den bidirektionalen PIM-Gruppenbereich auf dem IPN aufgenommen werden.

Multi-Pod Fehlerbehebung #1 (Unicast)

In der folgenden Topologie kann EP B nicht mit EP A kommunizieren.

Fehlerbehebung Topologie



Beachten Sie, dass viele der bei der Multi-Pod-Weiterleitung festgestellten Probleme identisch mit den Problemen bei einem einzelnen Pod sind. Aus diesem Grund werden spezifische Probleme bei Multi-Pod angesprochen.

Beachten Sie beim Befolgen des zuvor beschriebenen Unicast-Fehlerbehebungs-Workflows, dass die Anforderung zwar ein Proxy ist, die Spine-Knoten in Pod 2 jedoch nicht die Ziel-IP in COOP haben.

Ursache: Endpunkt fehlt in COOP

Wie bereits erwähnt, werden die COOP-Einträge für Remote-Pod-Endpunkte aus den BGP-EVPN-Informationen übernommen. Daher ist es wichtig, Folgendes zu bestimmen:

a) Ist sie beim Spine des Quell-Pod (Pod 2) im EVPN vorhanden?

```
a-spine4# show bgp l2vpn evpn 10.0.1.100 vrf overlay-1
<no output>
```

b.) Ist dies beim Remote-Pod-Spine (Pod 1) im EVPN der Fall?

```
a-spine1# show bgp l2vpn evpn 10.0.1.100 vrf overlay-1
Route Distinguisher: 1:16777199    (L2VNI 1)
BGP routing table entry for [2]:[0]:[15728642]:[48]:[0050.5681.3ee6]:[32]:[10.0.1.100]/272,
version 11751 dest ptr 0xafbf8192
Paths: (1 available, best #1)
Flags: (0x00010a 00000000) on xmit-list, is not in rib/evpn
Multipath: eBGP iBGP

 Advertised path-id 1
```

```
 Path type: local 0x4000008c 0x0 ref 0 adv path ref 1, path is valid, is best path
 AS-Path: NONE, path locally originated
  0.0.0.0 (metric 0) from 0.0.0.0 (192.168.1.101)
    Origin IGP, MED not set, localpref 100, weight 32768
    Received label 15728642 2392068
    Extcommunity:
        RT:5:16

          Path-id 1 advertised to peers:
```

Der Pod 1 Spine hat es und die Next-Hop IP ist 0.0.0.0; d. h. sie wurde lokal aus COOP exportiert. Beachten Sie jedoch, dass der Abschnitt "Für Peers beworben" keine Pod 2 Spine-Knoten enthält.

c.) Steht BGP-EVPN zwischen den PODs?

```
a-spine4# show bgp l2vpn evpn summ vrf overlay-1

Neighbor            V      AS   MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.1.101   4 65000       57380    66362            0     0      0  00:00:21  Active
192.168.1.102   4 65000       57568    66357            0     0      0  00:00:22  Active
```

Beachten Sie in der obigen Ausgabe, dass die BGP-EVPN-Peerings zwischen den PODs ausgefallen sind. Alles außer einem numerischen Wert in der Spalte State/PfxRcd weist darauf hin, dass die Adjacency nicht aktiv ist. Pod 1 EPs werden nicht über EVPN gelernt und nicht in COOP importiert.

Wenn dieses Problem auftritt, überprüfen Sie Folgendes:

1. Steht OSPF zwischen den Spine-Knoten und den verbundenen IPNs?
2. Verfügen die Spine-Knoten über Routen, die über OSPF für die Remote-Spine-IPs abgefragt wurden?
3. Unterstützt der vollständige Pfad über das IPN Jumbo-MTU?
4. Sind alle Protokoll-Adjacencies stabil?

Andere mögliche Ursachen

Wenn sich der Endpunkt nicht in der COOP-Datenbank eines Pod befindet und das Zielgerät ein unbeaufsichtigter Host ist (der auf keinem Leaf-Switch in der Fabric erfasst wird), stellen Sie sicher, dass der Fabric Glean-Prozess ordnungsgemäß funktioniert. Damit dies funktioniert:

- Unicast-Routing muss auf dem BD aktiviert sein.
- Das Ziel muss sich in einem BD-Subnetz befinden.
- Das IPN muss einen Multicast-Routing-Service für die Gruppe 239.255.255.240 bereitstellen.

Der Multicast-Bereich wird im nächsten Abschnitt genauer beschrieben.

Multi-Pod Broadcast, Unicast und Multicast (BUM) Forwarding Overview

In der ACI wird der Datenverkehr in vielen verschiedenen Szenarien über Overlay-Multicast-Gruppen geleitet. Hochwasser tritt beispielsweise auf für:

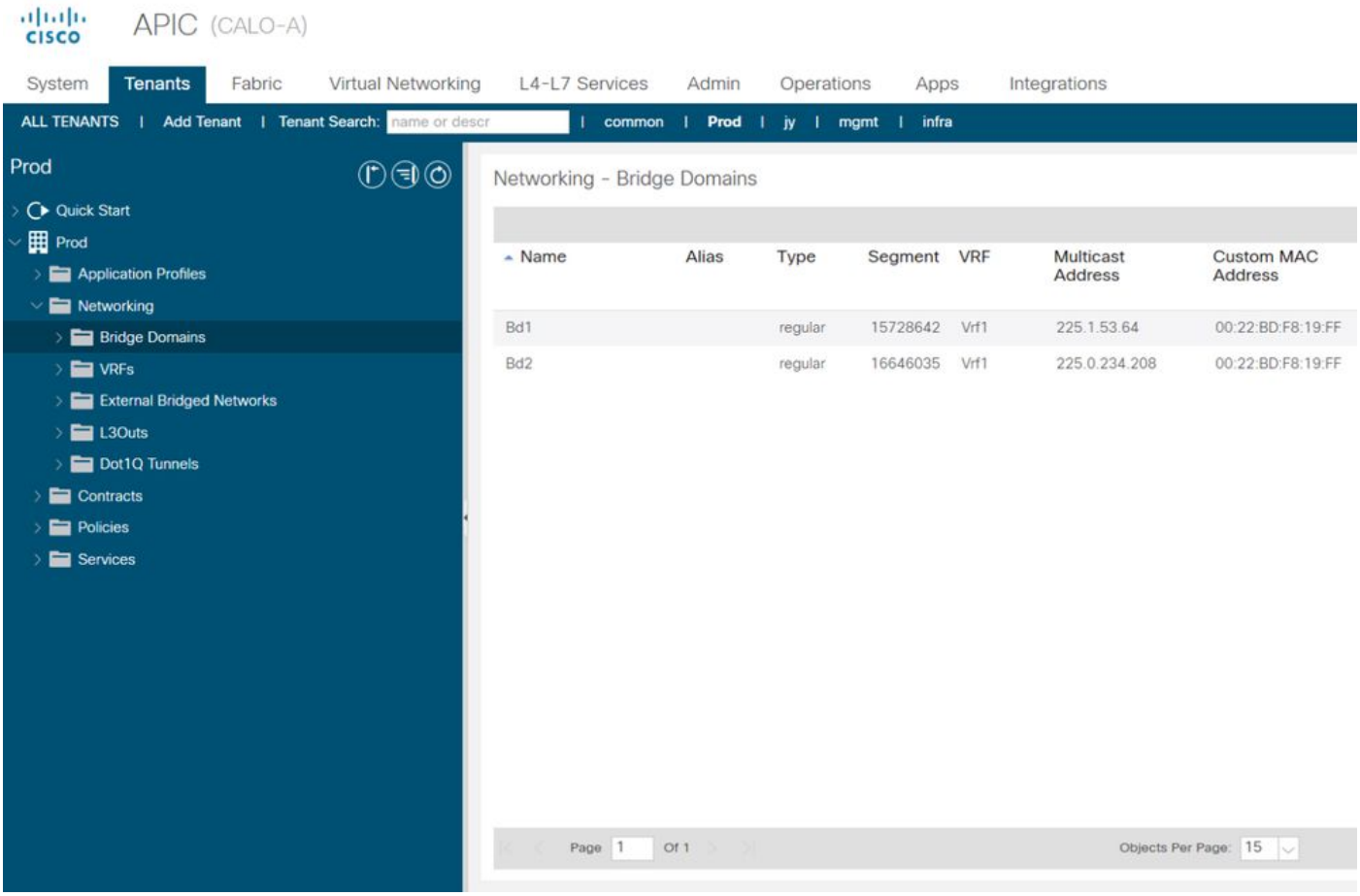
- Multicast- und Broadcast-Datenverkehr
- Unbekannter Unicast, der geflutet werden muss.

- Fabric-ARP-Fehlermeldungen.
- EP kündigt Nachrichten an.

Viele Funktionen hängen von der BUM-Weiterleitung ab.

Innerhalb der ACI wird allen Bridge-Domänen eine Multicast-Adresse zugewiesen, die als Group IP Outer (oder GIPo)-Adresse bezeichnet wird. Sämtlicher Datenverkehr, der innerhalb einer Bridge-Domäne geflutet werden muss, wird auf diesem GIPo geflutet.

BD GIPo in GUI



Das Objekt kann direkt auf einem der APICs abgefragt werden.

BD GIPo in Moquery

```
a-apic1# moquery -c fvBD -f 'fv.BD.name=="Bd1"'
Total Objects shown: 1

# fv.BD
name                       : Bd1
OptimizeWanBandwidth       : no
annotation                 :
arpFlood                   : yes
bcastP                     : 225.1.53.64
childAction                :
configIssues               :
descr                      :
dn                         : uni/tn-Prod/BD-Bd1
epClear                    : no
epMoveDetectMode           :
```

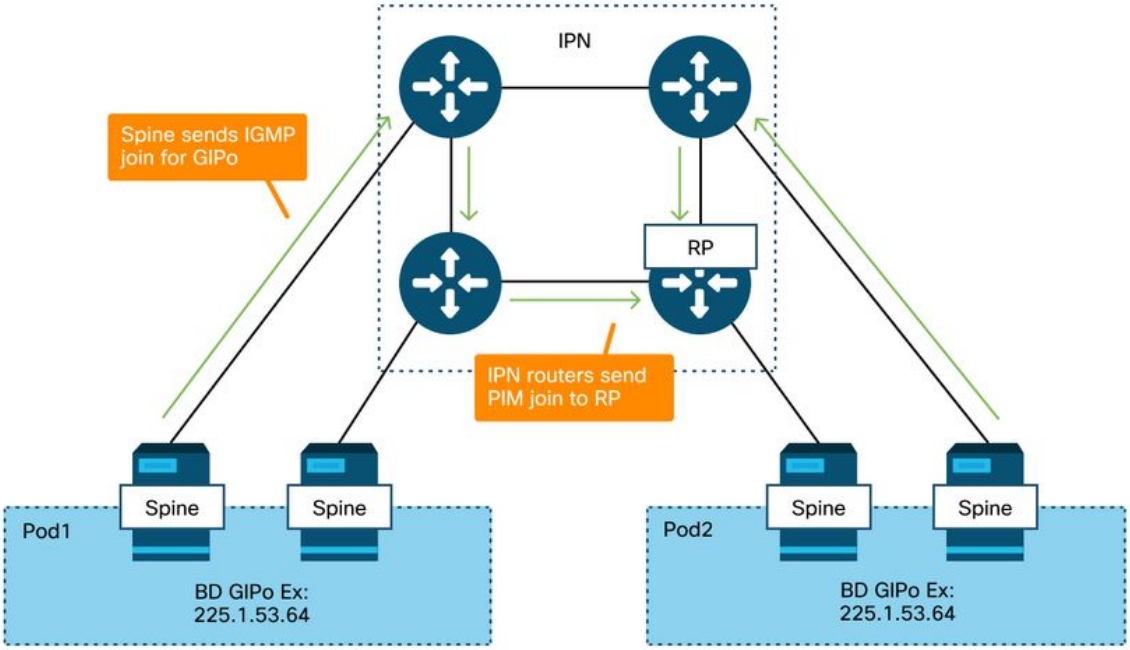
```
extMngdBy                :
hostBasedRouting         : no
intersiteBumTrafficAllow : no
intersiteL2Stretch       : no
ipLearning               : yes
ipv6McastAllow           : no
lcOwn                    : local
limitIpLearnToSubnets    : yes
llAddr                   : ::
mac                      : 00:22:BD:F8:19:FF
mcastAllow               : no
modTs                    : 2019-09-30T20:12:01.339-04:00
monPolDn                 : uni/tn-common/monepg-default
mtu                      : inherit
multiDstPktAct           : bd-flood
nameAlias                :
ownerKey                 :
ownerTag                 :
pcTag                    : 16387
rn                       : BD-Bd1
scope                    : 2392068
seg                      : 15728642
status                   :
type                     : regular
uid                      : 16011
unicastRoute             : yes
unkMacUcastAct           : proxy
unkMcastAct              : flood
v6unkMcastAct            : flood
vmac                     : not-applicable
```

Die obigen Informationen über GIPo Flooding gelten unabhängig davon, ob Multi-Pod verwendet wird oder nicht. Ein weiterer Aspekt bei Multi-Pod ist das Multicast-Routing auf dem IPN.

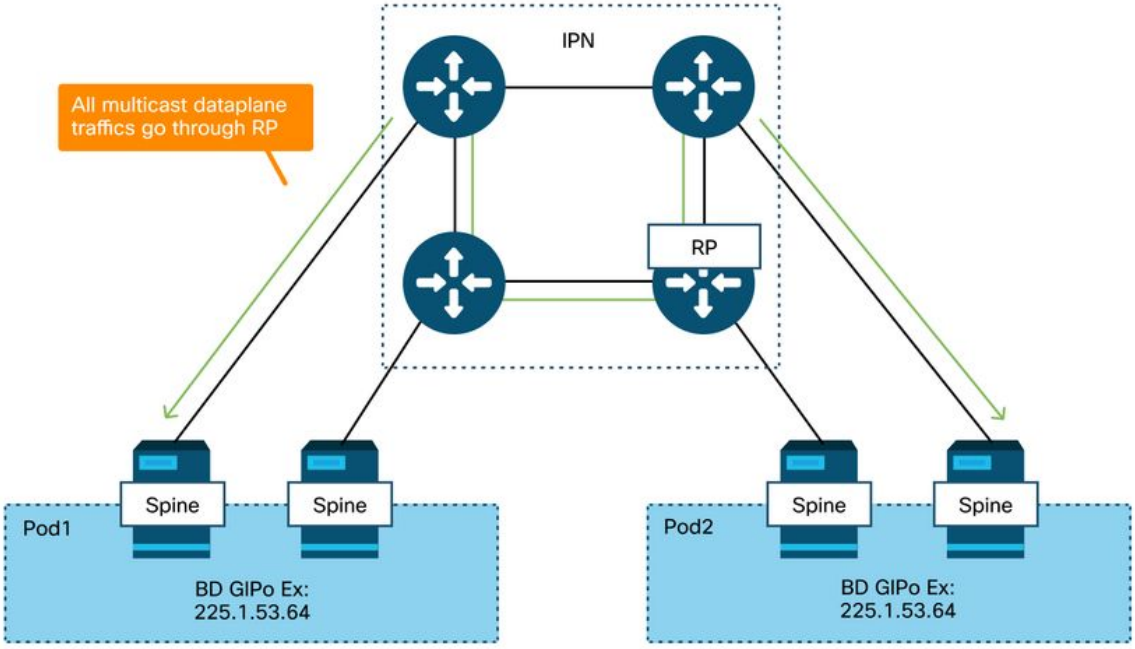
IPN-Multicast-Routing umfasst folgende Schritte:

- Spine-Knoten fungieren als Multicast-Hosts (nur IGMP). PIM wird nicht ausgeführt.
- Wenn ein BD in einem Pod bereitgestellt wird, sendet ein Spine dieses Pod einen IGMP-Join an eine der IPN-zugewandten Schnittstellen. Diese Funktionalität erstreckt sich über alle Spine-Knoten und die IPN-seitige Schnittstelle über viele Gruppen.
- Die IPNs empfangen diese Joins und senden PIM-Joins an den bidirektionalen PIM-RP.
- Da PIM Bidir verwendet wird, gibt es keine (S,G)-Bäume. In PIM Bidir werden nur (*,G)-Trees verwendet.
- Der gesamte Datenverkehr über Datenflugzeuge, der an das GIPo gesendet wird, durchläuft den RP.

IPN-Multicast-Kontrollebene



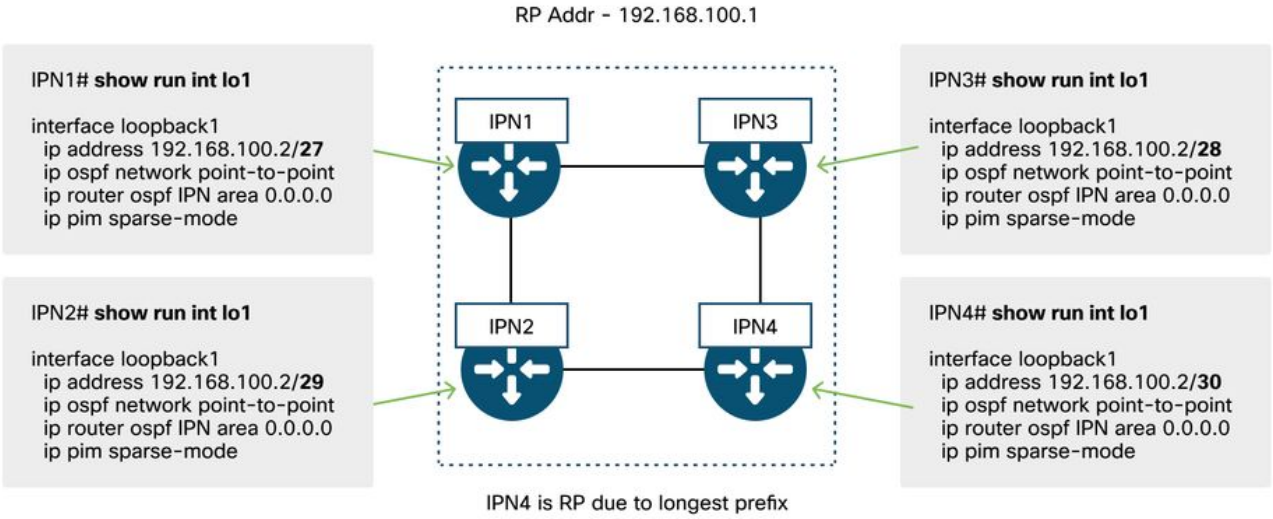
IPN-Multicast-Datenflugzeug



Die einzige Möglichkeit zur RP-Redundanz mit PIM Bidir ist die Verwendung von Phantom. Dies wird im Abschnitt zum Multi-Pod Discovery dieses Buchs ausführlich behandelt. Beachten Sie kurz, dass Phantom RP:

- Alle IPNs müssen mit derselben RP-Adresse konfiguriert werden.
- Die genaue RP-Adresse darf auf keinem Gerät vorhanden sein.
- Mehrere Geräte melden die Erreichbarkeit an das Subnetz, das die IP-Adresse des Phantom-RP enthält. Die angegebenen Subnetze sollten in der Subnetzlänge variieren, damit sich alle Router darauf einigen können, wer den besten Pfad für den RP angibt. Wenn dieser Pfad verloren geht, ist die Konvergenz vom IGP abhängig.

Phantom-RP-Konfiguration



Workflow zur Fehlerbehebung für Multi-Pod Broadcast, Unicast und Multicast (BUM)

1. Stellen Sie zunächst sicher, dass der Datenfluss vom Fabric tatsächlich als Multi-Destination behandelt wird.

Der Fluss wird im BD geflutet, wie in den folgenden Beispielen gezeigt:

- Der Frame ist ein ARP-Broadcast, und ARP Flooding ist auf dem BD aktiviert.
- Der Frame ist für eine Multicast-Gruppe bestimmt. Beachten Sie, dass selbst bei aktiviertem IGMP-Snooping der Datenverkehr immer noch in die Fabric des GIPo geleitet wird.
- Der Datenverkehr ist für eine Multicast-Gruppe bestimmt, für die die ACI Multicast-Routing-Services bereitstellt.
- Der Datenfluss ist ein Layer-2-Datenfluss (Bridge-Datenfluss), und die MAC-Zieladresse ist unbekannt, und das unbekannte Unicast-Verhalten auf dem BD ist auf "Flood" (Überschwemmung) festgelegt.

Die einfachste Methode, um zu bestimmen, welche Weiterleitungsentscheidung getroffen wird, ist mit einem ELAM.

2. Identifizieren Sie den BD-GIPo.

Lesen Sie dazu den Abschnitt weiter oben in diesem Kapitel. Spine-ELAMs können auch über die ELAM Assistant-App ausgeführt werden, um zu überprüfen, ob der geflutete Datenverkehr empfangen wird.

3. Überprüfen Sie die Multicast-Routing-Tabellen auf dem IPN für diesen GIPoS.

Die Ausgaben hierfür variieren je nach verwendeter IPN-Plattform, allerdings auf hoher Ebene:

- Alle IPN-Router müssen den RP vereinbaren, und der RPF für diesen GIPo muss auf diesen Tree verweisen.
- Ein mit jedem Pod verbundener IPN-Router sollte eine IGMP-Mitgliedschaft für die Gruppe erhalten.

Multi-Pod Fehlerbehebung #2 (BUM-Fluss)

Dieses Szenario deckt alle Szenarien ab, bei denen ARP nicht in Multi-Pod- oder BUM-Szenarien aufgelöst wird (unbekannter Unicast usw.).

Hier gibt es mehrere häufige mögliche Ursachen.

Mögliche Ursache 1: Die PIM RP-Adresse ist Eigentum mehrerer Router.

Bei diesem Szenario flutet der Eingangs-Leaf den Datenverkehr (Überprüfung mit ELAM), der Quell-Pod empfängt und flutet den Datenverkehr, der Remote-Pod hingegen nicht. Bei manchen BDs funktioniert Hochwasser, bei anderen nicht.

Führen Sie auf dem IPN den Befehl "show ip mroute <GIPo-Adresse>" für GIPo aus, um zu sehen, dass der RPF-Tree auf mehrere verschiedene Router verweist.

Wenn dies der Fall ist, prüfen Sie Folgendes:

- Vergewissern Sie sich, dass die tatsächliche PIM RP-Adresse nirgends konfiguriert ist. Für jedes Gerät, das Eigentümer dieser RP-Adresse ist, wird eine lokale /32-Route angezeigt.
- Vergewissern Sie sich, dass mehrere IPN-Router im Szenario mit Phantom-RP nicht dieselbe Präfixlänge für den RP angeben.

Mögliche Ursache 2: IPN-Router lernen keine Routen für die RP-Adresse

Genau wie die erste mögliche Ursache kann auch hier der überschwemmte Datenverkehr das IPN nicht verlassen. Die Ausgabe von "show ip route <rp address>" auf jedem IPN-Router zeigt nur die lokal konfigurierte Präfixlänge an und nicht die von den anderen Routern angekündigten Präfixe.

Dies führt dazu, dass jedes Gerät denkt, es sei der RP, obwohl die tatsächliche RP-IP-Adresse nirgendwo konfiguriert ist.

Wenn dies der Fall ist. Folgendes überprüfen:

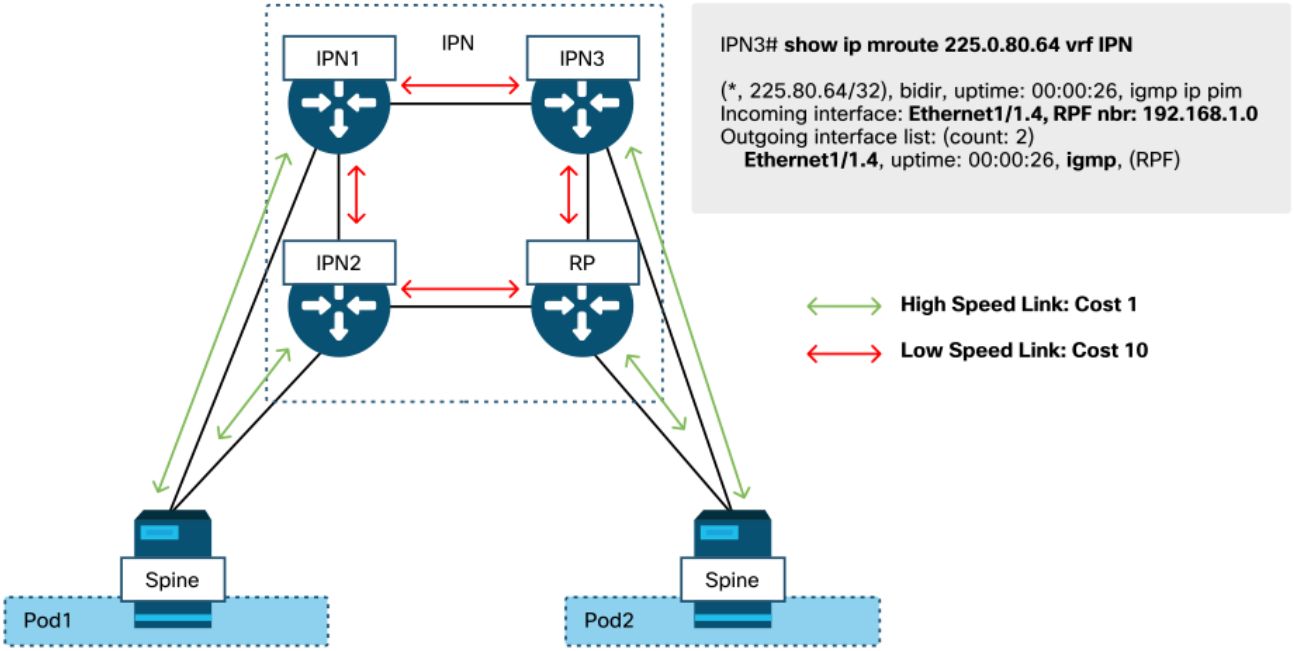
- Überprüfen Sie, ob die Routing-Nachbarschaften zwischen den IPN-Routern aktiv sind. Überprüfen Sie, ob die Route in der tatsächlichen Protokolldatenbank (z. B. in der OSPF-Datenbank) vorhanden ist.
- Überprüfen Sie, ob alle Loopbacks, die als mögliche RPs verwendet werden sollen, als OSPF-Point-to-Point-Netzwerktypen konfiguriert sind. Wenn dieser Netzwerktyp nicht

konfiguriert ist, kündigt jeder Router eine /32-Präfixlänge an, unabhängig davon, was tatsächlich konfiguriert ist.

Mögliche Ursache 3: IPN-Router installieren keine GIPo-Route oder RPF verweist auf die ACI

Wie bereits erwähnt, führt die ACI PIM nicht auf ihren IPN-Verbindungen aus. Das bedeutet, dass der beste IPN-Pfad zum RP niemals auf die ACI verweisen sollte. In diesem Szenario wären mehrere IPN-Router mit demselben Spine verbunden, und es würde sich eine bessere OSPF-Metrik durch den Spine ergeben als direkt zwischen IPN-Routern.

RPF-Schnittstelle zur ACI



So beheben Sie dieses Problem:

- Stellen Sie sicher, dass Routing-Protokoll-Nachbarschaften zwischen IPN-Routern aktiv sind.
- Erhöhen Sie die OSPF-Kostenmetriken für die IPN-zugewandten Verbindungen an den Spine-Knoten auf einen Wert, der diese Metrik weniger bevorzugt als die IPN-to-IPN-Verbindungen.

Andere Verweise

Vor der ACI-Software 4.0 gab es einige Probleme bei der Verwendung von COS 6 durch externe Geräte. Die meisten dieser Probleme wurden durch 4.0-Erweiterungen behoben. Weitere Informationen finden Sie in der CiscoLive-Sitzung "BRKACI-2934 - Troubleshooting Multi-Pod" und im Abschnitt "Quality of Service".

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.