Risoluzione dei problemi ACI Intra-Fabric Forwarding - MultiPod Forwarding

Sommario

Introduzione
Premesse
Panoramica dell'inoltro di più dispositivi
Componenti Multi-Pod
Topologia per esempi di multi-pod
Flusso di lavoro generale per la risoluzione dei problemi di inoltro di più dispositivi
Flusso di lavoro di risoluzione dei problemi Unicast Multi-Pod
1. Confermare che la foglia in entrata riceva il pacchetto. Usare lo strumento ELAM CLI mostrato nella sezione "Strumenti" insieme all'output del report disponibile nella versione 4.2. Viene usata anche l'applicazione ELAM Assistant.
2. La foglia in entrata sta imparando la destinazione come punto finale nel VRF in entrata? Se no, c'è un percorso?
Configurazione ELAM Assistant
Verifica decisioni di inoltro
3. Confermare sul dorso che l'IP di destinazione è presente in COOP in modo che la richiesta proxy funzioni.
4. Decisione per l'inoltro di proxy Multi-Pod Spine
5. Verificare l'EVPN BGP sul dorso
6. Verificare il COOP sugli aculei nel POD di destinazione.
7. Verificare che la foglia di uscita abbia le informazioni locali.
Utilizzo di fTriage per verificare il flusso end-to-end
Richieste proxy in cui il PE non è in COOP
Verifica ARP Glean
Scenario n. 1 per la risoluzione dei problemi relativi ai multipod (Unicast)
Risoluzione dei problemi relativi alla topologia
Causa: Endpoint mancante in COOP
Altre possibili cause
Cenni preliminari sull'inoltro multicast, unicast sconosciuto e broadcast multi-Pod
BD GIPo in GUI
Piano di controllo multicast IPN
Piano dati multicast IPN
Configurazione RP fantasma
Flusso di lavoro per la risoluzione dei problemi relativi a broadcast, unicast sconosciuto e multicast (BUM) di più dispositivi
1. Verificare innanzitutto che il flusso venga effettivamente trattato come destinazione multipla dal fabric.
2. Identificare il GIPo di BD.
3. Verificare le tabelle di routing multicast nell'IPN per tale GIPo.
Scenario n. 2 per la risoluzione dei problemi relativi a più dispositivi (BUM Flow)

[Possibile causa 1: Più router sono proprietari dell'indirizzo RP PIM](#)
[Possibile causa 2: I router IPN non stanno imparando le route per l'indirizzo RP](#)
[Possibile causa 3: I router IPN non stanno installando il routing GIPo o il router RPF punta ad ACI](#)
[Altri riferimenti](#)

Introduzione

In questo documento vengono illustrati i passaggi per comprendere e risolvere i problemi relativi a uno scenario di inoltro di Multi-Pod ACI.

Premesse

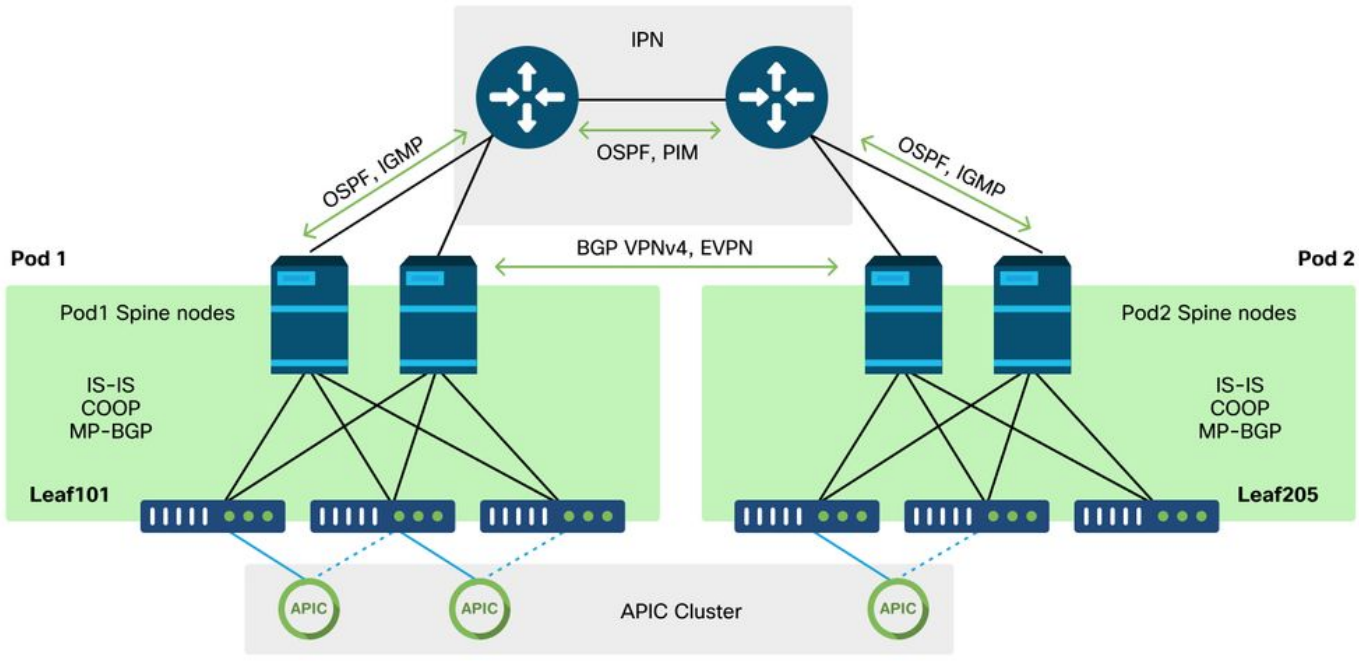
Il materiale tratto da questo documento è stato Risoluzione dei problemi di Cisco Application Centric Infrastructure, Second Edition libro, in particolare **Inoltro intra-fabric - Multi-Pod Forwarding** capitolo.

Panoramica dell'inoltro di più dispositivi

In questo capitolo verrà descritto come risolvere i problemi di connettività non corretta tra i dispositivi di pod in un ambiente a più dispositivi

Prima di esaminare esempi specifici di risoluzione dei problemi, è importante soffermarsi un attimo su come comprendere i componenti Multi-Pod ad alto livello.

Componenti Multi-Pod



Analogamente a un fabric ACI tradizionale, un fabric Multi-Pod è ancora considerato un singolo fabric ACI e si basa su un singolo cluster APIC per la gestione.

All'interno di ogni singolo Pod, ACI utilizza gli stessi protocolli nella sovrapposizione di un fabric tradizionale. Questo include IS-IS per lo scambio di informazioni TEP, oltre alla selezione OIF (Multicast Outgoing Interface), COOP per un repository di endpoint globale e BGP VPNv4 per la distribuzione di router esterni attraverso la struttura.

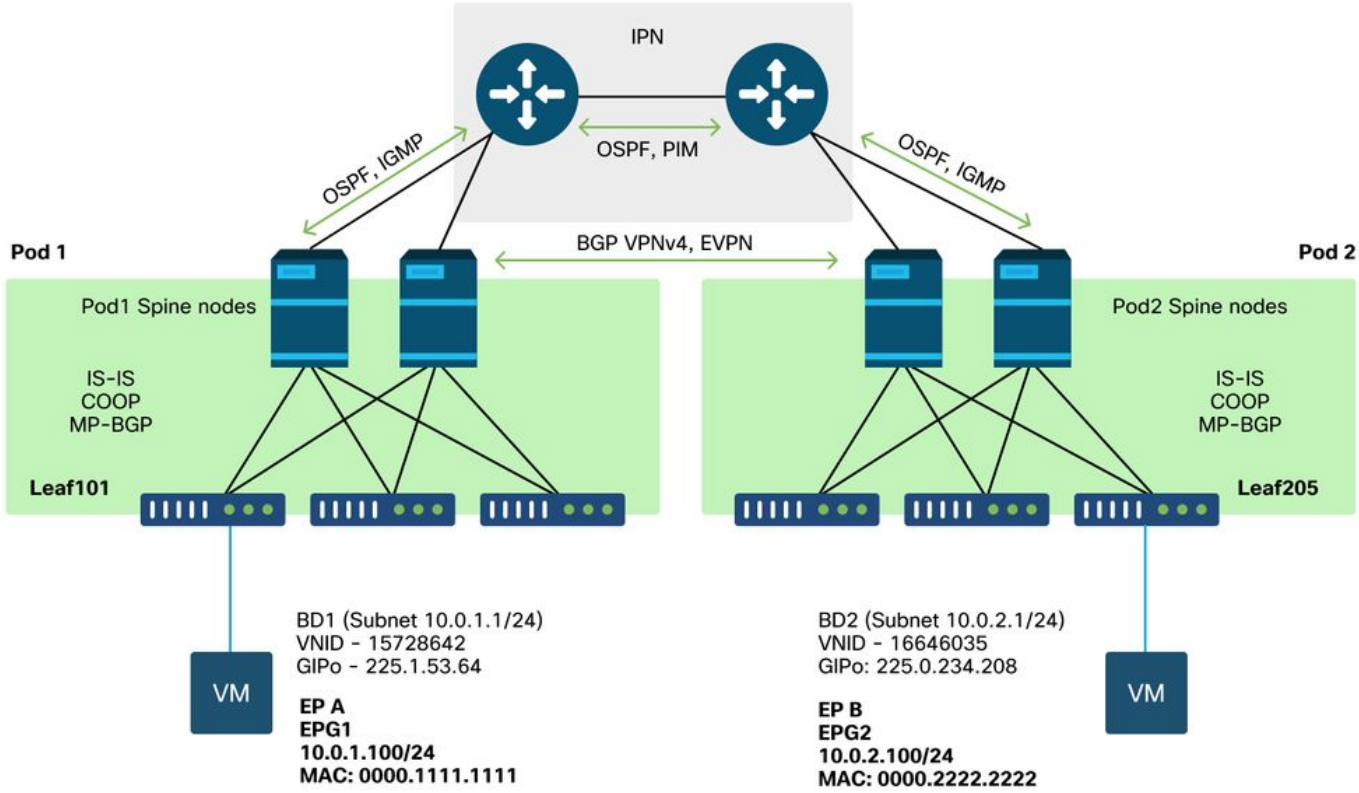
Multi-Pod si basa su questi componenti in quanto deve collegare ciascun Pod insieme.

- Per scambiare informazioni di routing relative ai TEP nel POD remoto, OSPF viene utilizzato per pubblicizzare il pool TEP di riepilogo tramite l'IPN.
- Per scambiare le route esterne apprese da un POD all'altro, la famiglia di indirizzi VPNv4 BGP viene estesa tra nodi spine. Ogni Pod diventa un gruppo di riflessione di percorso separato.
- Per sincronizzare gli endpoint e altre informazioni archiviate in COOP tra i pod, la famiglia di indirizzi EVPN BGP viene estesa tra i nodi spine.
- Infine, per gestire il sovraccarico del traffico broadcast, unicast sconosciuto e multicast (BUM) attraverso i pod, i nodi spine di ciascun pod agiscono come host IGMP e i router IPN scambiano informazioni di routing multicast tramite PIM bidirezionale.

Gran parte degli scenari e dei flussi di lavoro per la risoluzione dei problemi di Multi-Pod sono simili ai fabric Single Pod ACI. Questa sezione Multi-Pod si concentrerà principalmente sulle differenze tra Single Pod e Multi-Pod forwarding.

Topologia per esempi di multi-pod

Come per la risoluzione dei problemi in qualsiasi scenario, è importante iniziare con la comprensione dello stato previsto. Fare riferimento a questa topologia per gli esempi di questo capitolo.



Flusso di lavoro generale per la risoluzione dei problemi di inoltro di più dispositivi

Ad alto livello, quando si esegue il debug di un problema di inoltro a più pod, è possibile valutare i seguenti passaggi:

1. Il flusso è unicast o multidestinazione? Tenere presente che anche se si prevede che il flusso sia unicast nello stato attivo, se ARP non viene risolto si tratta di un flusso a più destinazioni.
2. Il flusso è instradato o bloccato? In genere, un flusso instradato dalla prospettiva ACI è un flusso qualsiasi in cui l'indirizzo MAC di destinazione è l'indirizzo MAC del router di proprietà di un gateway configurato su ACI. Inoltre, se l'inondazione ARP è disabilitata, la foglia in entrata viene indirizzata in base all'indirizzo IP del destinatario. Se l'indirizzo MAC di destinazione non è di proprietà di ACI, lo switch eseguirà l'inoltro in base all'indirizzo MAC o seguirà il comportamento "unicast sconosciuto" configurato sul dominio bridge.
3. La foglia in entrata sta perdendo il flusso? fTriage e ELAM sono gli strumenti migliori per confermare questo.

Se il flusso è unicast di livello 3:

1. La foglia in entrata dispone di un endpoint che rileva per l'IP di destinazione nello stesso VRF dell'EPG di origine? In tal caso, avrà sempre la precedenza su qualsiasi percorso appreso. La foglia inoltrerà direttamente all'indirizzo del tunnel o all'interfaccia di uscita dove viene appreso l'endpoint.
2. Se non viene rilevato alcun endpoint, la foglia in entrata dispone di un percorso per la destinazione con il flag 'Pervasive' impostato? Ciò indica che la subnet di destinazione è configurata come subnet del dominio del bridge e che l'hop successivo deve essere il proxy della spine nel Pod locale.
3. Se non esiste un percorso pervasivo, l'ultima risorsa potrebbe essere qualsiasi percorso appreso tramite L3Out. Questa parte è identica all'inoltro Single Pod L3Out.

Se il flusso è unicast di livello 2:

1. La foglia in entrata dispone di un endpoint con informazioni sull'indirizzo MAC di destinazione nello stesso dominio bridge dell'EPG di origine? In questo caso, la foglia inoltrerà all'IP del tunnel remoto o all'interfaccia locale da cui viene appreso l'endpoint.
2. Se non si conosce l'indirizzo MAC di destinazione nel dominio bridge di origine, la foglia verrà inoltrata in base al comportamento "unicast sconosciuto" su cui è impostato BD. Se è impostata su 'Flood', la foglia verrà inondata fino al gruppo multicast GIPo allocato per il dominio bridge. I pod locali e remoti dovrebbero averne una copia allagata. Se è impostato su 'Proxy hardware', il fotogramma viene inviato al dorso per una ricerca proxy e inoltrato in base alla voce COOP del dorso.

Poiché gli output della risoluzione dei problemi sono notevolmente diversi per il formato unicast rispetto al BUM, gli output di lavoro e gli scenari per il formato unicast verranno presi in considerazione prima di passare al BUM.

Flusso di lavoro di risoluzione dei problemi Unicast Multi-Pod

Seguendo la topologia, scorrere il flusso da 10.0.2.100 su foglia205 a 10.0.1.100 su foglia101.

Prima di procedere, è importante verificare se l'origine ha risolto ARP per il gateway (per un flusso instradato) o per l'indirizzo MAC di destinazione (per un flusso con bridging)

1. Confermare che la foglia in entrata riceva il pacchetto. Usare lo strumento ELAM CLI mostrato nella sezione "Strumenti" insieme all'output del report disponibile nella versione 4.2. Viene usata anche l'applicazione ELAM Assistant.

```
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
```

Notare che è stato attivato il comando ELAM, che conferma la ricezione del pacchetto sullo switch in entrata. Osservare ora un paio di campi nel rapporto poiché l'output è molto esteso.

```
================================================================================================
===========
                                                        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
```

Il report contiene molte più informazioni sulla destinazione del pacchetto, ma l'app ELAM Assistant è al momento più utile per interpretare questi dati. L'output di ELAM Assistant per questo flusso verrà illustrato più avanti in questo capitolo.

2. La foglia in entrata sta imparando la destinazione come punto finale nel VRF in entrata? Se no, c'è un percorso?

```
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
+------------------------------------+--------------+----------------+-------------+----------
---+----------------------------+
```

L'assenza dell'output del comando precedente indica che l'IP di destinazione non viene appreso. Quindi controllare la tabella di routing.

```
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
```

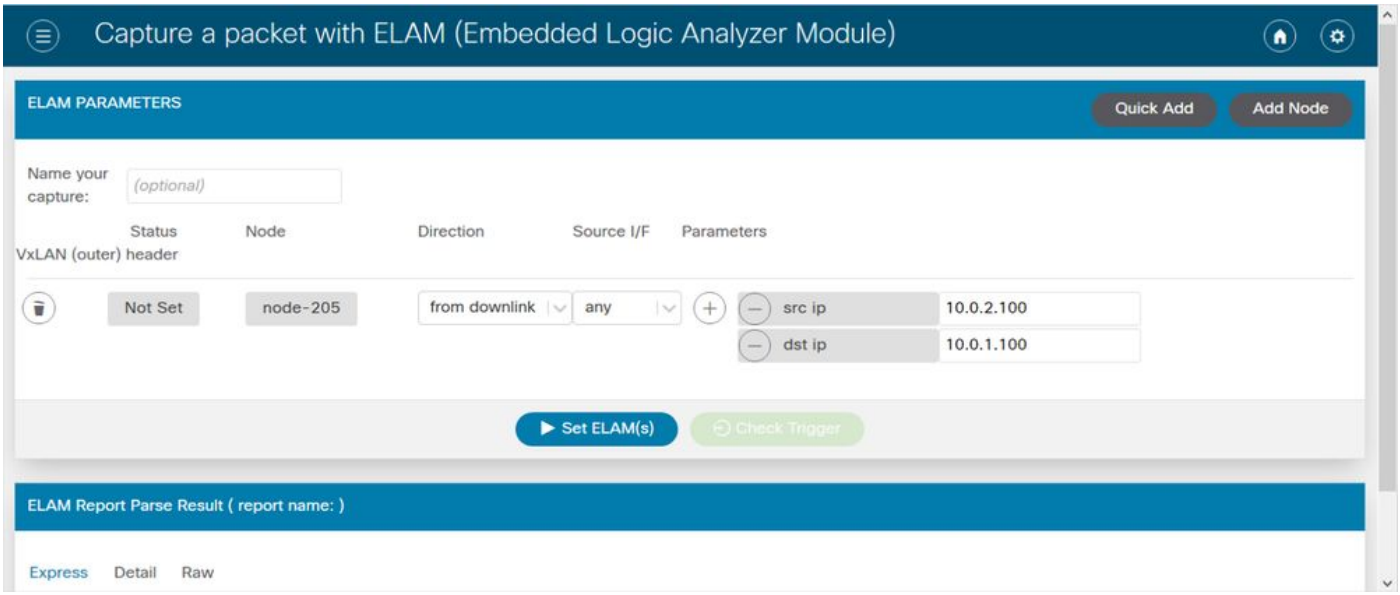
Nell'output precedente, viene visualizzato il flag pervasivo che indica che si tratta di una route subnet del dominio del bridge. L'hop successivo deve essere un indirizzo proxy anycast sugli spine.

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

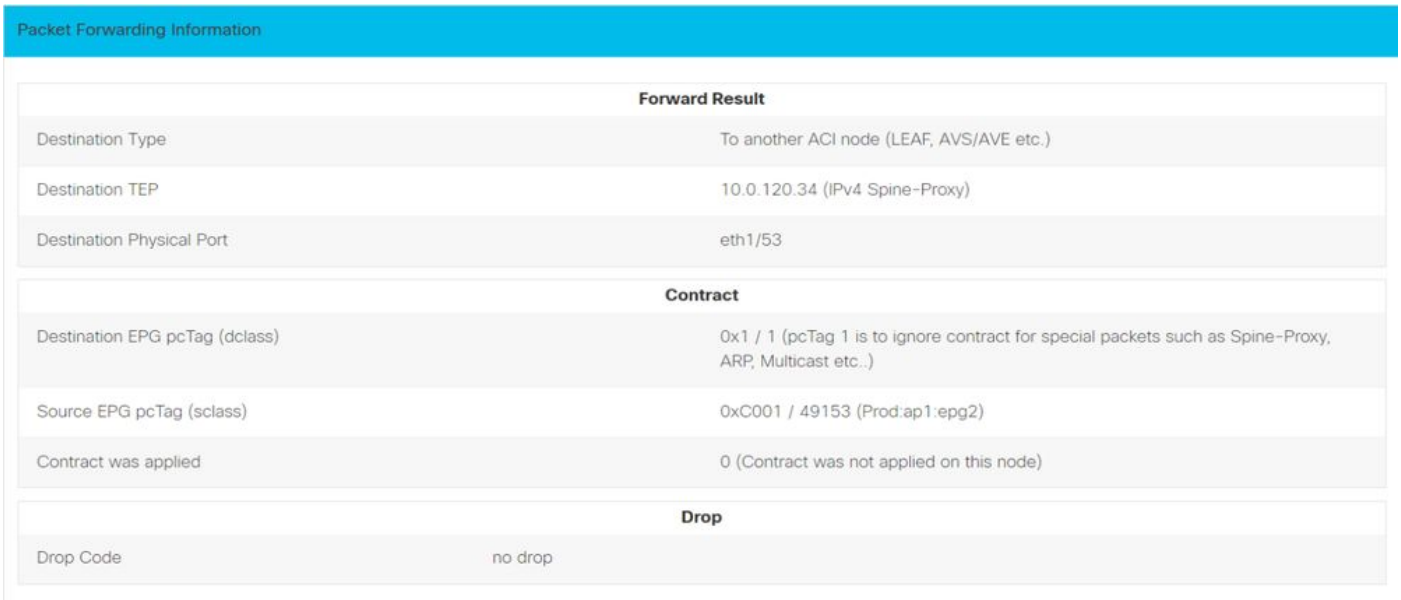
Notare che se l'endpoint viene acquisito su un tunnel o su un'interfaccia fisica, questa operazione avrà la precedenza, in modo che il pacchetto venga inoltrato direttamente qui. Per ulteriori informazioni, consultare il capitolo "Inoltro esterno" di questo manuale.

Utilizzare l'Assistente ELAM per confermare le decisioni di inoltro viste negli output di cui sopra.

Configurazione ELAM Assistant



Verifica decisioni di inoltro



L'output mostrato sopra mostra che la foglia in entrata sta inoltrando il pacchetto all'indirizzo proxy della spine IPv4. Questo è ciò che ci si aspetta.

3. Confermare sul dorso che l'IP di destinazione è presente in COOP in modo che la richiesta proxy funzioni.

Èpossibile ottenere l'output COOP sul dorso in diversi modi, ad esempio guardandolo con un comando 'show coop internal info ip-db':

```
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

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

Altri comandi da eseguire sul dorso:

Query COOP per voce l2:

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

Query COOP per voce l3 e recupero voce l2 padre:

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

Query COOP solo per voce l3:

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

L'aspetto utile della query multipla è che può anche essere eseguita direttamente su un APIC e l'utente può vedere ogni direttrice che ha il record in coop.

4. Decisione per l'inoltro di proxy Multi-Pod Spine

Se l'ingresso COOP della spine punta a un tunnel nel Pod locale, l'inoltro si basa sul comportamento tradizionale dell'ACI.

Si noti che il proprietario di un TEP può essere verificato nell'infrastruttura eseguendo da un APIC: **moquery -c ipv4Addr -f 'ipv4.Addr.addr="<indirizzo tunnel>"'**

Nello scenario proxy, l'hop successivo del tunnel è 10.0.0.34. Chi è il proprietario di questo indirizzo IP?:

```
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]
```

Questo IP è di proprietà di entrambi i nodi di spine nel Pod 1. Si tratta di un IP specifico chiamato indirizzo proxy esterno. Allo stesso modo in cui ACI ha indirizzi proxy di proprietà dei nodi spine all'interno di un Pod (vedere il punto 2 di questa sezione), ci sono anche indirizzi proxy assegnati al Pod stesso. È possibile verificare questo tipo di interfaccia eseguendo:

```
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]
```

Il flag 'external' indica che si tratta di un TEP di un proxy esterno.

5. Verificare l'EVPN BGP sul dorso

Il record dell'endpoint di copia deve essere importato da BGP EVPN sul dorso. Il seguente comando può essere utilizzato per verificare che sia in EVPN (anche se se è già in COOP con un hop successivo del POD remoto esterno TEP si può supporre che provenga da EVPN):

```
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
```

Il comando precedente può essere eseguito anche per un indirizzo MAC.

-192.168.1.254 è il piano dati TEP configurato durante la configurazione di più dispositivi. Tuttavia, anche se viene pubblicizzato in BGP come NH, l'hop successivo effettivo sarà il proxy esterno TEP.

-192.168.1.101 e .102 sono i nodi di spine del Pod 1 che pubblicizzano questo percorso.

6. Verificare il COOP sugli aculei nel POD di destinazione.

Èpossibile utilizzare lo stesso comando utilizzato in precedenza:

```
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

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

Verificare il proprietario dell'indirizzo del tunnel eseguendo il comando seguente su un controller APIC:

```
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
```

Il comando precedente mostra che il tunnel tra i punti COOP e leaf101. Ciò significa che leaf101 deve avere informazioni locali per l'endpoint di destinazione.

7. Verificare che la foglia di uscita abbia le informazioni locali.

A tale scopo, è possibile usare il comando "show endpoint":

```
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
```

Il punto finale viene appreso. Il pacchetto deve essere inoltrato sulla base del canale della porta 5 con il tag VLAN 1075 impostato.

Utilizzo di fTriage per verificare il flusso end-to-end

Come descritto nella sezione "Strumenti" di questo capitolo, fTriage può essere usato per mappare un flusso end-to-end esistente e capire cosa sta facendo ogni switch del percorso con il pacchetto. Ciò è particolarmente utile in installazioni più grandi e complesse, come ad esempio i Multi-Pod.

Si noti che l'esecuzione completa di fTriage richiederà un certo tempo (potenzialmente 15 minuti).

Quando si esegue fTriage nel flusso di esempio:

```
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"}}}
```

La fTriage contiene una grande quantità di dati. Vengono evidenziati alcuni dei campi più importanti. Notare che il percorso del pacchetto era 'leaf205 (Pod 2) > spine3 (Pod 2) > spine2 (Pod 1) > leaf101 (Pod 1)'. Tutte le decisioni di inoltro e le ricerche di contratto effettuate lungo il percorso sono visibili.

Se si tratta di un flusso di livello 2, è necessario impostare la sintassi della fTriage sul tipo:

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

Richieste proxy in cui il PE non è in COOP

Prima di prendere in considerazione scenari di errore specifici, c'è un altro pezzo da discutere in relazione all'inoltro unicast su Multi-Pod. Cosa succede se l'endpoint di destinazione è sconosciuto, la richiesta è inoltrata tramite proxy e l'endpoint non è in COOP?

In questo scenario, il pacchetto/frame viene inviato alla direttrice e viene generata una richiesta di guadagno.

Quando il dorso genera una richiesta di glean, il pacchetto originale viene comunque mantenuto nella richiesta. Tuttavia, il pacchetto riceve ethertype 0xfff2, un Ethertype personalizzato riservato alle glean. Per questo motivo, non sarà facile interpretare questi messaggi in strumenti di acquisizione dei pacchetti come Wireshark.

Anche la destinazione del layer 3 esterno è impostata su 239.255.255.240, che è un gruppo multicast riservato appositamente per i messaggi in chiaro. Questi devono essere trasmessi in tutta la struttura e gli switch foglia in uscita con subnet di destinazione della richiesta di glean distribuita genereranno una richiesta ARP per risolvere la destinazione. Questi ARP vengono inviati dall'indirizzo IP della subnet BD configurato. Pertanto, le richieste proxy non possono risolvere la posizione degli endpoint invisibili all'utente/sconosciuti se il routing unicast è disabilitato in un dominio bridge.

La ricezione del messaggio di luminanza sulla foglia di uscita e l'ARP generato successivamente e la risposta ARP ricevuta possono essere verificate mediante il seguente comando:

Verifica ARP Glean

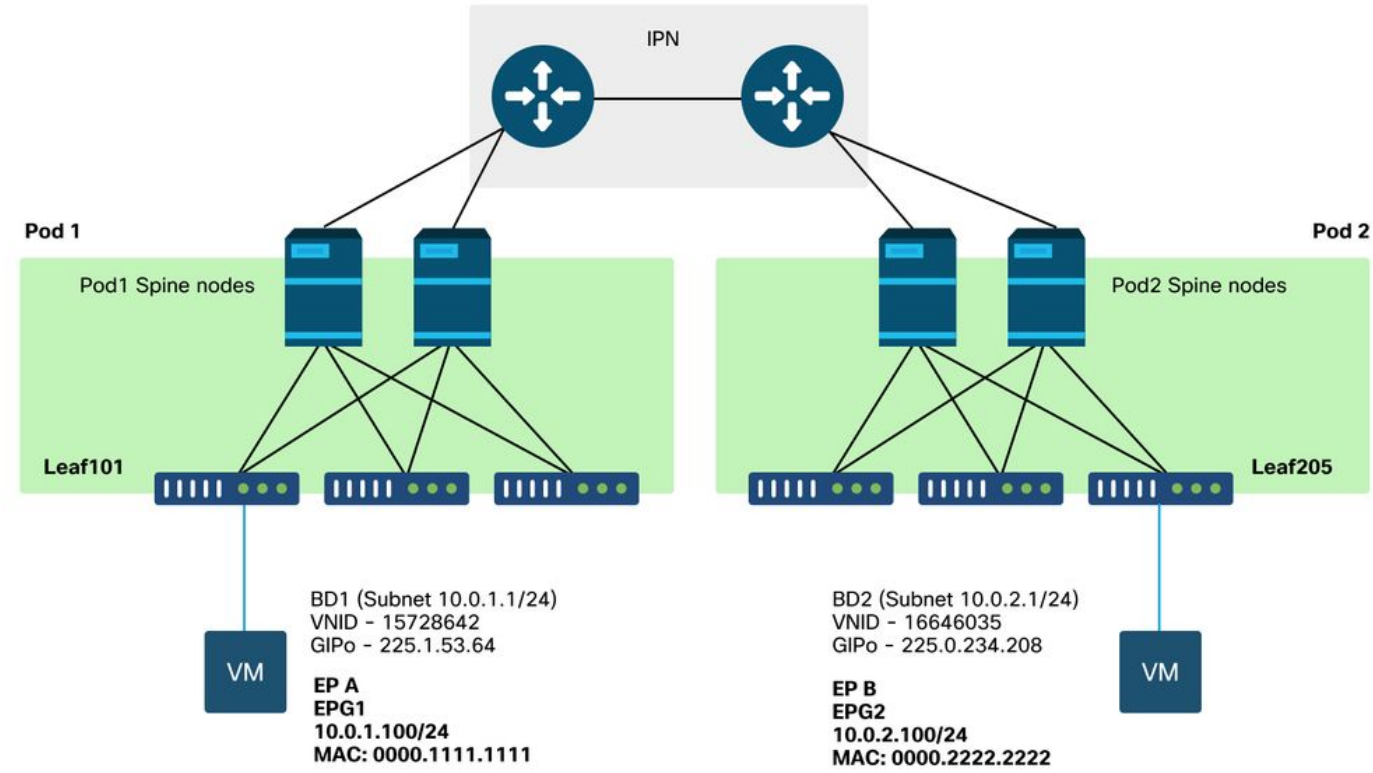
```
a-leaf205# show ip arp internal event-history event | grep -F -B 1 192.168.21.11
...
73) Event:E_DEBUG_DSF, length:127, at 316928 usecs after Wed May  1 08:31:53 2019
Updating epm ifidx: 1a01e000 vlan: 105 ip: 192.168.21.11, ifMode: 128 mac: 8c60.4f02.88fc   <<<
Endpoint is learned
75) Event:E_DEBUG_DSF, 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
```

Per riferimento, i messaggi in grigio inviati a 239.255.255.240 è il motivo per cui questo gruppo deve essere incluso nell'intervallo di gruppi PIM bidirezionali sull'IPN.

Scenario n. 1 per la risoluzione dei problemi relativi ai multipod (Unicast)

Nella topologia seguente, EP B non è in grado di comunicare con EP A.

Risoluzione dei problemi relativi alla topologia



Notare che molti dei problemi riscontrati per l'inoltro di più dispositivi sono identici ai problemi riscontrati in un unico dispositivo. Per questo motivo, i problemi specifici del Multi-Pod sono concentrati su.

Mentre si segue il flusso di lavoro di risoluzione dei problemi unicast descritto in precedenza, notare che la richiesta è inoltrata ma i nodi di spine nel Pod 2 non hanno l'IP di destinazione in COOP.

Causa: Endpoint mancante in COOP

Come già accennato, le voci COOP per gli endpoint dei POD remoti vengono popolate dalle informazioni EVPN BGP. Di conseguenza, è importante determinare:

a) Il POD di origine (Pod 2) spine lo ha in EVPN?

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

b.) Il pod remoto (Pod 1) spine lo ha in EVPN?

```
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:
```

Il Pod 1 ha la spine e l'IP dell'hop successivo è 0.0.0.0; questo significa che è stato esportato localmente da COOP. Si noti, tuttavia, che la sezione 'Pubblicizzato ai peer' non include i nodi di spine Pod 2.

c.) BGP EVPN è disponibile tra i dispositivi POD?

```
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
```

Nell'output precedente si noti che i peer BGP EVPN sono disattivati tra i dispositivi POD. Qualsiasi valore diverso da un valore numerico nella colonna State/PfxRcd indica che l'adiacenza non è attiva. Gli EP del Pod 1 non vengono appresi tramite EVPN e non vengono importati in COOP.

Se il problema si verifica, verificare quanto segue:

1. L'OSPF è attivo tra i nodi della spine e gli IPN connessi?
2. I nodi spine hanno percorsi appresi tramite OSPF per gli IP spine remoti?
3. Il percorso completo sull'IPN supporta l'MTU jumbo?
4. Tutte le adiacenze di protocollo sono stabili?

Altre possibili cause

Se l'endpoint non si trova nel database COOP di un POD e il dispositivo di destinazione è un host silenzioso (non viene appreso su uno switch foglia nella struttura), verificare che il processo di sgranatura della struttura funzioni correttamente. Perché questo funzioni:

- Ènecessario abilitare il routing unicast in BD.
- La destinazione deve trovarsi in una subnet BD.
- L'IPN deve fornire il servizio di routing multicast per il gruppo 239.255.255.240.

La sezione successiva tratta in modo più approfondito la questione del multicast.

Cenni preliminari sull'inoltro multicast, unicast sconosciuto e broadcast multi-Pod

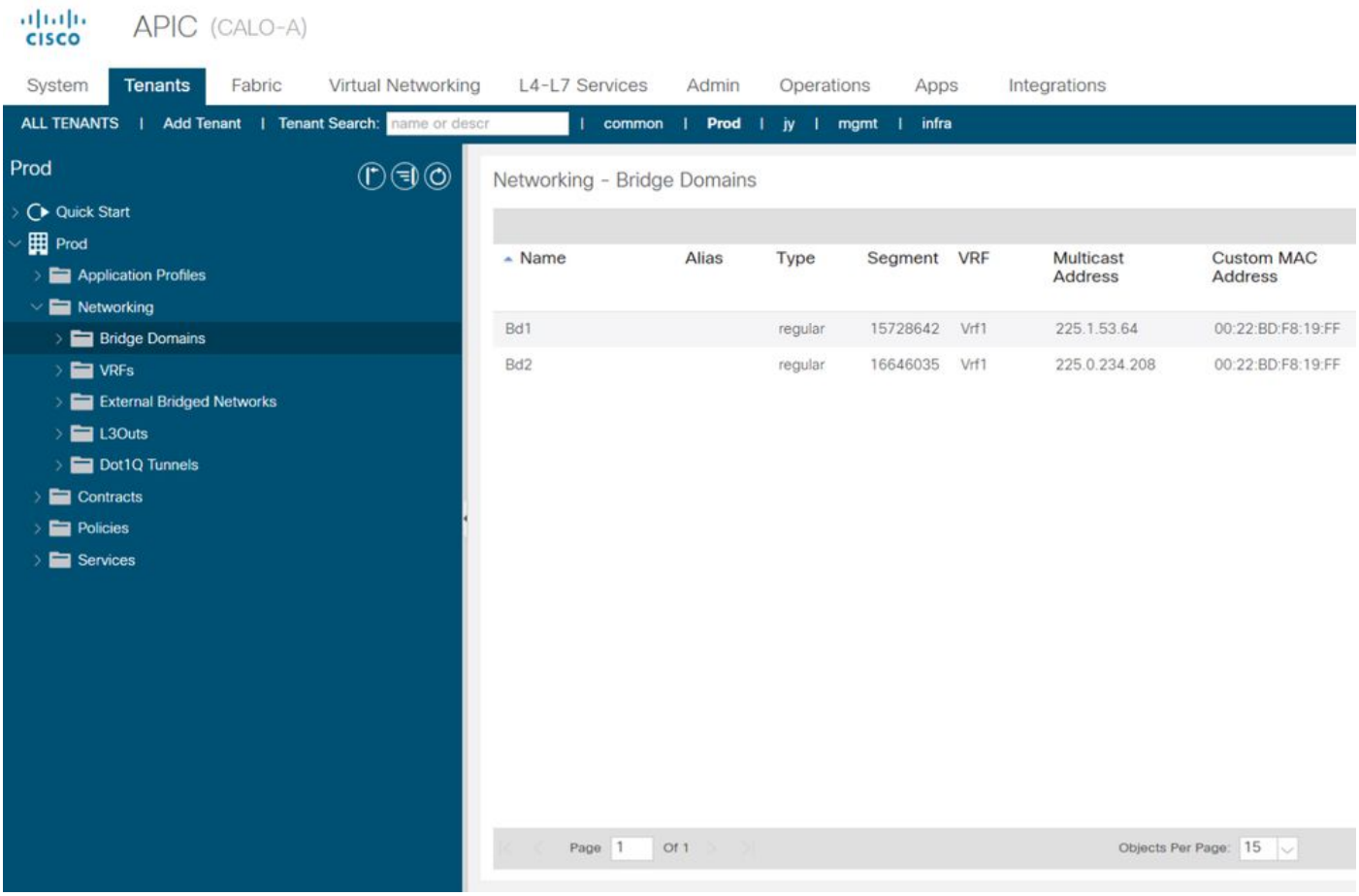
In ACI, il traffico viene inondato attraverso gruppi multicast sovrapposti in molti scenari diversi. Ad esempio, l'inondazione si verifica per:

- Multicast e traffico broadcast.
- unicast sconosciuto da inondare.
- Messaggi di ricezione ARP fabric.
- Messaggi di annuncio del PE.

Molte caratteristiche e funzionalità si basano sull'inoltro BUM.

In ACI, a tutti i domini bridge viene assegnato un indirizzo multicast noto come indirizzo GIPo (Group IP Outer). Tutto il traffico che deve essere inondato all'interno di un dominio bridge viene inondato in questo GIPo.

BD GIPo in GUI



L'oggetto può essere interrogato direttamente su uno degli APIC.

GIPo BD 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
```

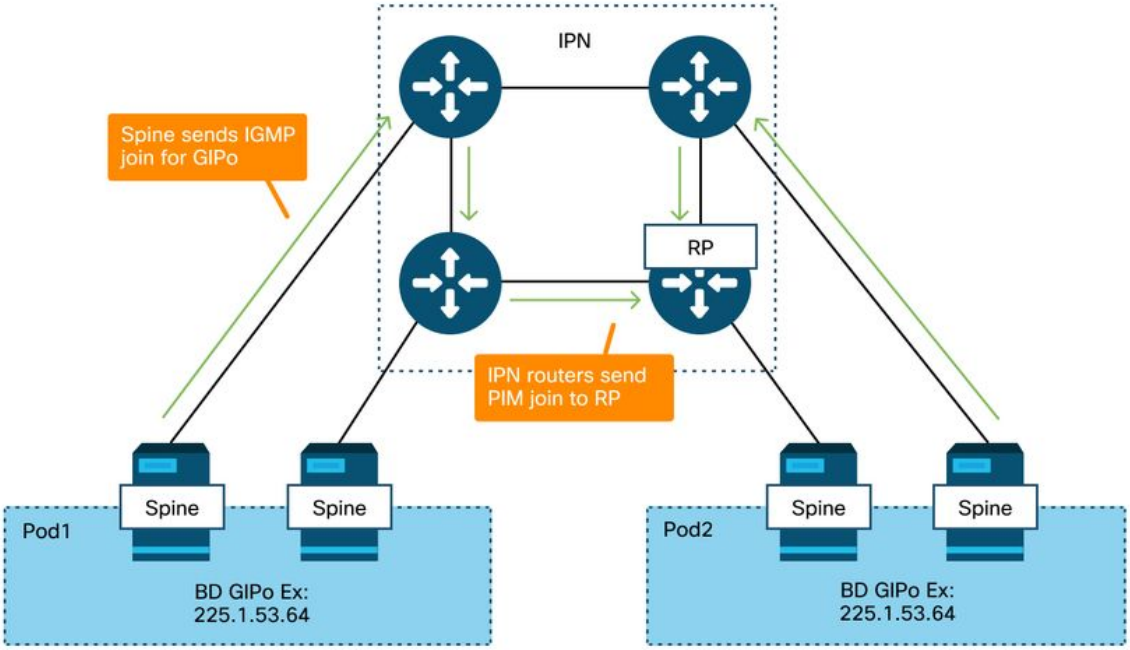
```
mtu                     : inherit
multiDstPktAct          : bd-flood
nameAlias               :
ownerKey                :
ownerTag                :
pcTag                   : 16387
rn                      : BD-Bd1
scope                   : 2392068
seg                     : 15728642
status                  :
type                    : regular
uid                     : 16011
unicastRoute            : yes
unkMacUcastAct          : proxy
unkMcastAct             : flood
v6unkMcastAct           : flood
vmac                    : not-applicable
```

Le informazioni di cui sopra sul flusso GIPo sono vere indipendentemente dal fatto che si utilizzi o meno Multi-Pod. La parte aggiuntiva di questa funzionalità che riguarda i dispositivi multi-pod è il routing multicast sull'IPN.

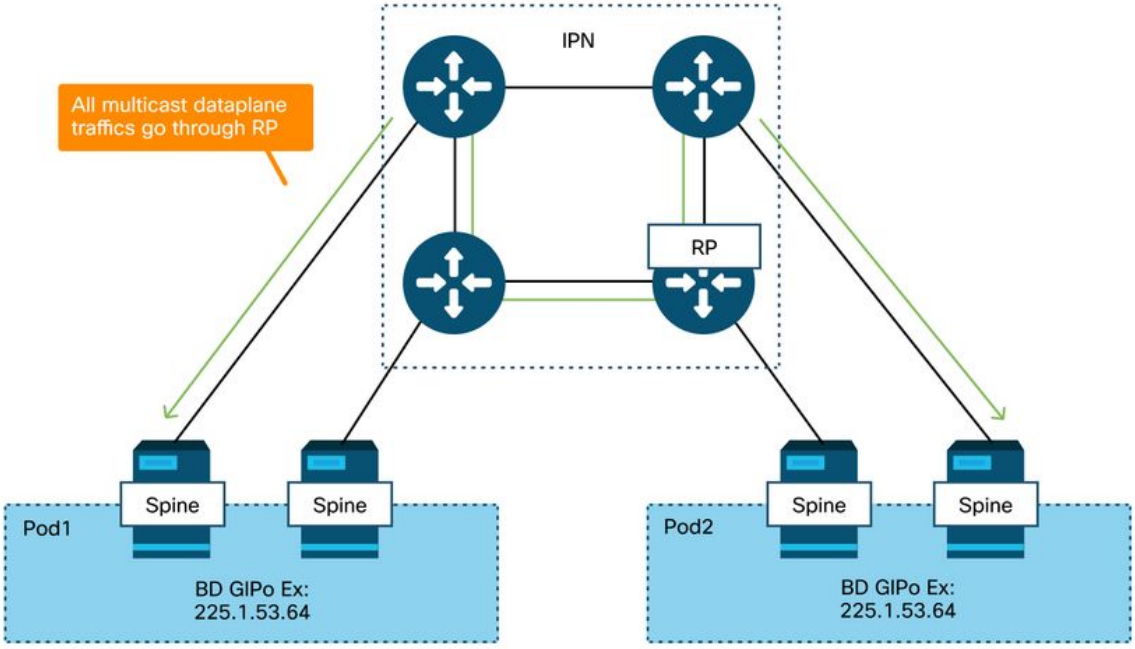
Il routing multicast IPN prevede quanto segue:

- I nodi dorsali fungono da host multicast (solo IGMP). Non eseguono PIM.
- Se un BD viene distribuito in un Pod, una spine da quel pod invierà un join IGMP su una delle sue interfacce con IPN. Questa funzionalità viene distribuita su tutti i nodi della spine e sull'interfaccia con interfaccia IPN su molti gruppi.
- Gli IPN ricevono tali join e inviano i join PIM verso il PIM RP bidirezionale.
- Poiché viene utilizzato PIM Bidir, non esistono alberi (S,G). In PIM Bidir vengono utilizzati solo alberi (*,G).
- Tutto il traffico del dataplane inviato al GIPo passa attraverso il RP.

Piano di controllo multicast IPN



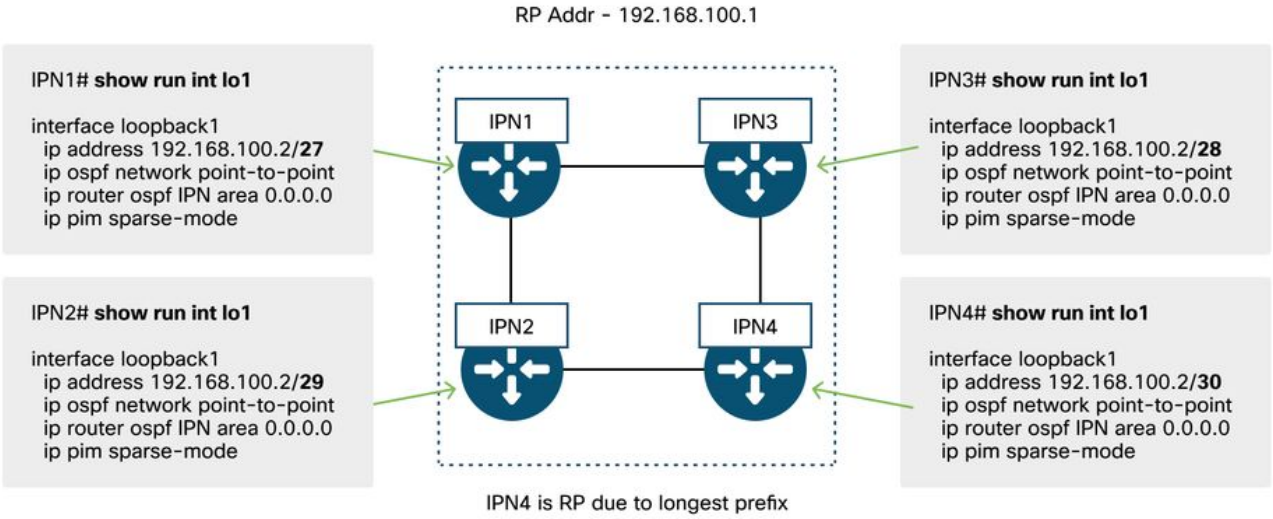
Piano dati multicast IPN



L'unico modo per ottenere la ridondanza RP con PIM Bidir è utilizzare Phantom. Questo è trattato in dettaglio nella sezione Multi-Pod Discovery di questo libro. Come breve riepilogo, notare che con RP fantasma:

- Tutti gli IPN devono essere configurati con lo stesso indirizzo RP.
- L'indirizzo RP esatto non deve esistere su alcun dispositivo.
- Più dispositivi annunciano la raggiungibilità alla subnet che contiene l'indirizzo IP RP fantasma. Le subnet pubblicizzate devono avere lunghezze diverse, in modo che tutti i router concordino su chi sta pubblicizzando il miglior percorso per l'RP. Se questo percorso viene perso, la convergenza dipende dall'IGP.

Configurazione RP fantasma



Flusso di lavoro per la risoluzione dei problemi relativi a broadcast, unicast sconosciuto e multicast (BUM) di più dispositivi

1. Verificare innanzitutto che il flusso venga effettivamente trattato come destinazione multipla dal fabric.

Il flusso verrà inondato in BD nei seguenti esempi comuni:

- Il frame è una trasmissione ARP e l'inondazione ARP è attivata in BD.
- Il frame è destinato a un gruppo multicast. Notare che anche se lo snooping IGMP è abilitato, il traffico viene sempre inondato nel fabric sul GIPo.
- Il traffico è destinato a un gruppo multicast per il quale ACI fornisce servizi di routing multicast.
- Il flusso è un layer 2 (flusso con bridging) e l'indirizzo MAC di destinazione è sconosciuto e il comportamento unicast sconosciuto in BD è impostato su 'Flood'.

Il modo più semplice per determinare quale decisione di inoltro verrà presa è con un ELAM.

2. Identificare il GIPo di BD.

Fare riferimento alla sezione precedente di questo capitolo che parla di questo argomento. Gli ELAM del dorso possono anche essere eseguiti tramite l'applicazione ELAM Assistant per verificare che il traffico venga ricevuto.

3. Verificare le tabelle di routing multicast nell'IPN per tale GIPo.

Le uscite variano a seconda della piattaforma IPN in uso, ma ad alto livello:

- Tutti i router IPN devono concordare l'RP e l'RPF per questo GIPo deve puntare a questo albero.
- Un router IPN collegato a ciascun Pod dovrebbe ottenere un join IGMP per il gruppo.

Scenario n. 2 per la risoluzione dei problemi relativi a più dispositivi (BUM Flow)

In questo scenario vengono illustrati tutti gli scenari che prevedono la mancata risoluzione di ARP in scenari Multi-Pod o BUM (unicast sconosciuto, ecc.).

Le cause possibili sono diverse.

Possibile causa 1: Più router sono proprietari dell'indirizzo RP PIM

Con questo scenario, la foglia in entrata inonda il traffico (verificare con ELAM), il POD di origine riceve e inonda il traffico, ma il POD remoto non lo ottiene. Per alcuni BD, l'allagamento funziona, per altri no.

Sull'IP, eseguire 'show ip route <indirizzo IP>' per GIPo per verificare che l'albero RPF punti a più router diversi.

In questo caso, verificare quanto segue:

- Verificare che l'indirizzo RP PIM effettivo non sia configurato in nessuna posizione. Tutti i dispositivi che possiedono l'indirizzo RP effettivo vedranno una route locale /32 per esso.
- Verificare che più router IPN non stiano pubblicizzando la stessa lunghezza di prefisso per l'RP nello scenario RP fantasma.

Possibile causa 2: I router IPN non stanno imparando le route per l'indirizzo RP

Allo stesso modo della prima causa possibile, qui il traffico inondato non riesce a lasciare l'IPN. L'output del comando "show ip route <indirizzo IP>" su ciascun router IPN visualizza solo la lunghezza del prefisso configurato localmente anziché l'annuncio degli altri router.

Di conseguenza, ogni dispositivo considera l'RP come tale anche se l'indirizzo IP reale dell'RP non è configurato da nessuna parte.

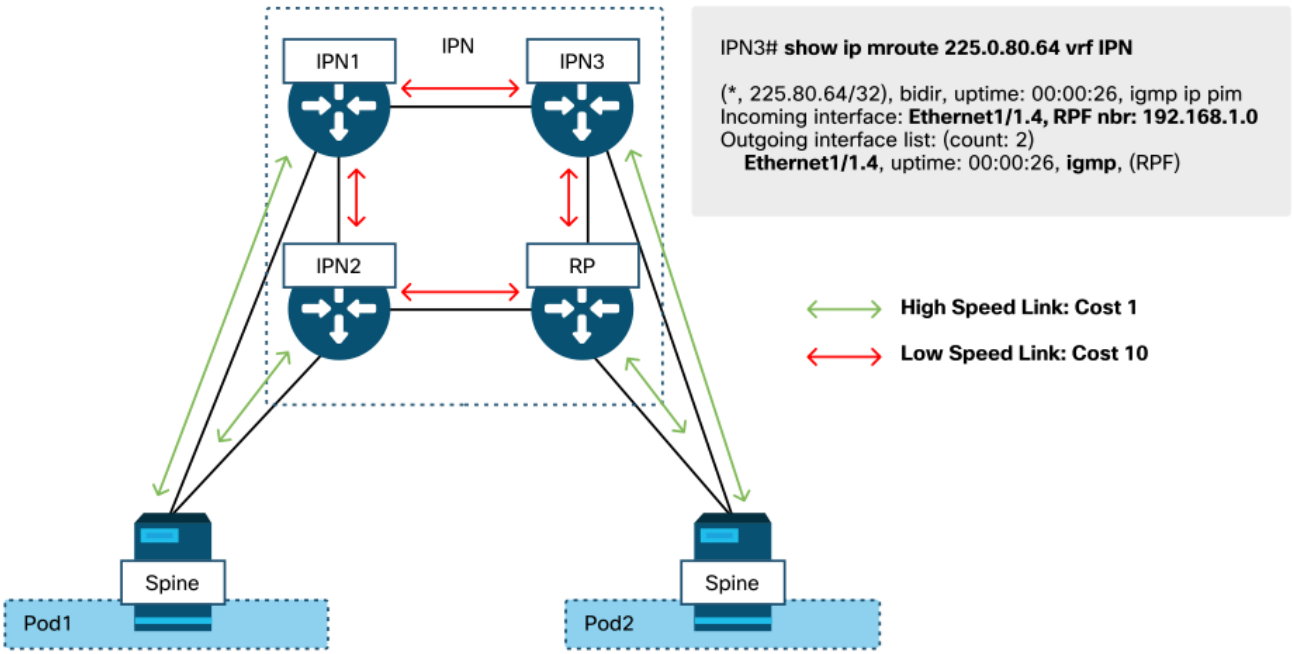
Se è così. verificare quanto segue:

- Verificare che le adiacenze di routing siano attive tra router IPN. Verificare che la route si trovi nel database del protocollo effettivo, ad esempio nel database OSPF.
- Verificare che tutti i loopback che dovrebbero essere RP candidati siano configurati come tipi di rete OSPF point-to-point. Se questo tipo di rete non è configurato, ogni router annuncerà sempre la lunghezza del prefisso /32, a prescindere dalla configurazione effettiva.

Possibile causa 3: I router IPN non stanno installando il routing GIPo o il router RPF punta ad ACI

Come accennato in precedenza, ACI non esegue PIM sui collegamenti con IPN. Ciò significa che il miglior percorso dell'IPN verso l'RP non deve mai puntare ad ACI. In questo caso, è possibile connettere più router IPN alla stessa spine e visualizzare una metrica OSPF migliore attraverso la spine rispetto a quella visualizzata direttamente tra i router IPN.

Interfaccia RPF per ACI



Per risolvere il problema:

- Verificare che le adiacenze del protocollo di routing tra i router IPN siano attive.
- Aumentare le metriche dei costi OSPF per i collegamenti con interfaccia IPN sui nodi della spine a un valore che rende tale metrica meno preferibile rispetto ai collegamenti da IPN a IPN.

Altri riferimenti

Prima del software ACI 4.0, erano state riscontrate alcune problematiche relative all'utilizzo di COS 6 da parte di dispositivi esterni. La maggior parte di questi problemi sono stati risolti con i miglioramenti apportati alla versione 4.0, ma per ulteriori informazioni, fare riferimento alla sessione di CiscoLive "BRKACI-2934 - Troubleshooting Multi-Pod" e alla sezione "Quality of Service".

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).