ACI 패브릭 내 포워딩 문제 해결 - MultiPod 포워딩

목차

소개

이 문서에서는 ACI 멀티 포드 포워딩 시나리오를 이해하고 문제를 해결하는 단계에 대해 설명합니다.

배경 정보

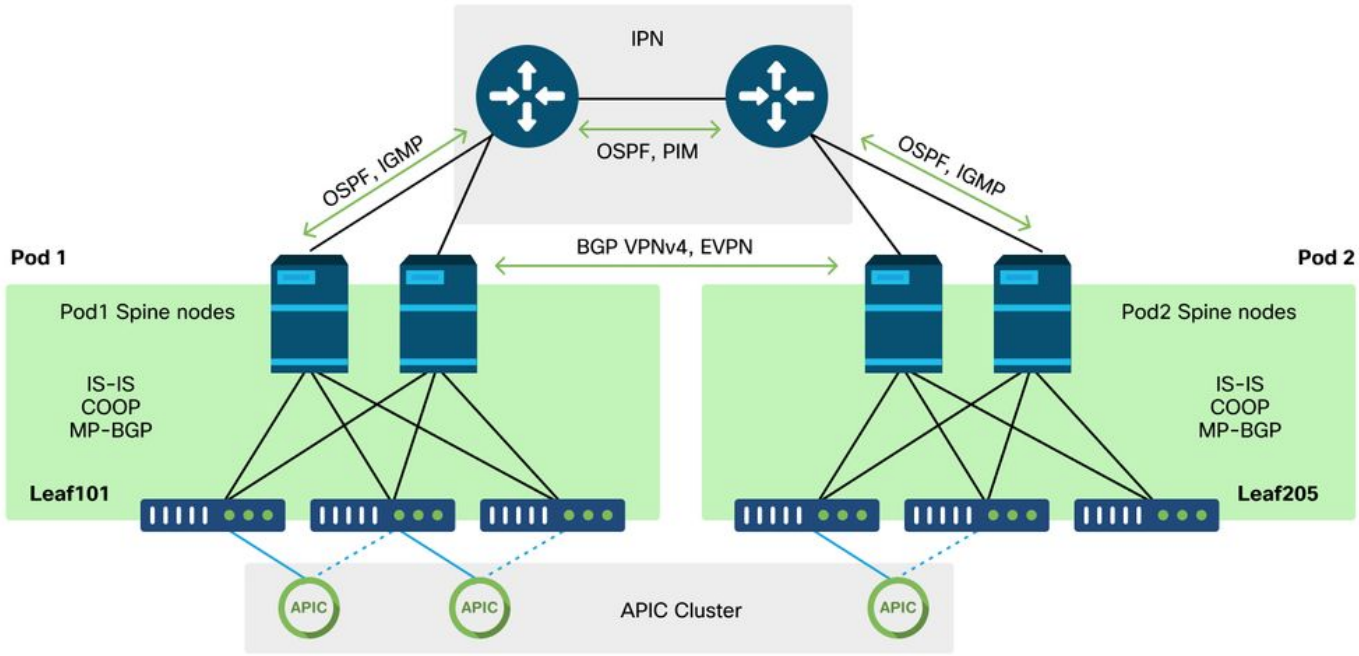
이 문서의 자료는 Cisco Application Centric Infrastructure, Second Edition 트러블슈팅 특히 **패브릭 내 포워딩 - 멀티 포드 포워딩** 장.

멀티 포드 포워딩 개요

이 장에서는 다중 포드 환경에서 포드 간에 연결이 올바르게 작동하지 않는 시나리오를 해결하는 방법을 설명합니다

구체적인 트러블슈팅 예를 보기 전에 잠시 시간을 내어 Multi-Pod 구성 요소를 대략적으로 이해하는 것이 중요합니다.

멀티 포드 구성 요소



기존 ACI 패브릭과 마찬가지로, 다중 포드 패브릭은 여전히 단일 ACI 패브릭으로 간주되며 관리를 위해 단일 APIC 클러스터에 의존합니다.

각 개별 Pod 내에서 ACI는 오버레이에서 기존 패브릭과 동일한 프로토콜을 활용합니다. 여기에는 TEP 정보 교환과 OIF(Multicast Outgoing Interface) 선택을 위한 IS-IS, 글로벌 엔드포인트 리포지토리를 위한 COOP, 패브릭을 통한 외부 라우터 배포를 위한 BGP VPNv4가 포함됩니다.

멀티 포드는 각 포드를 연결해야 하므로 이러한 구성 요소를 기반으로 구축됩니다.

- 원격 포드의 TEP와 관련된 라우팅 정보를 교환하기 위해 OSPF를 사용하여 IPN을 통해 요약

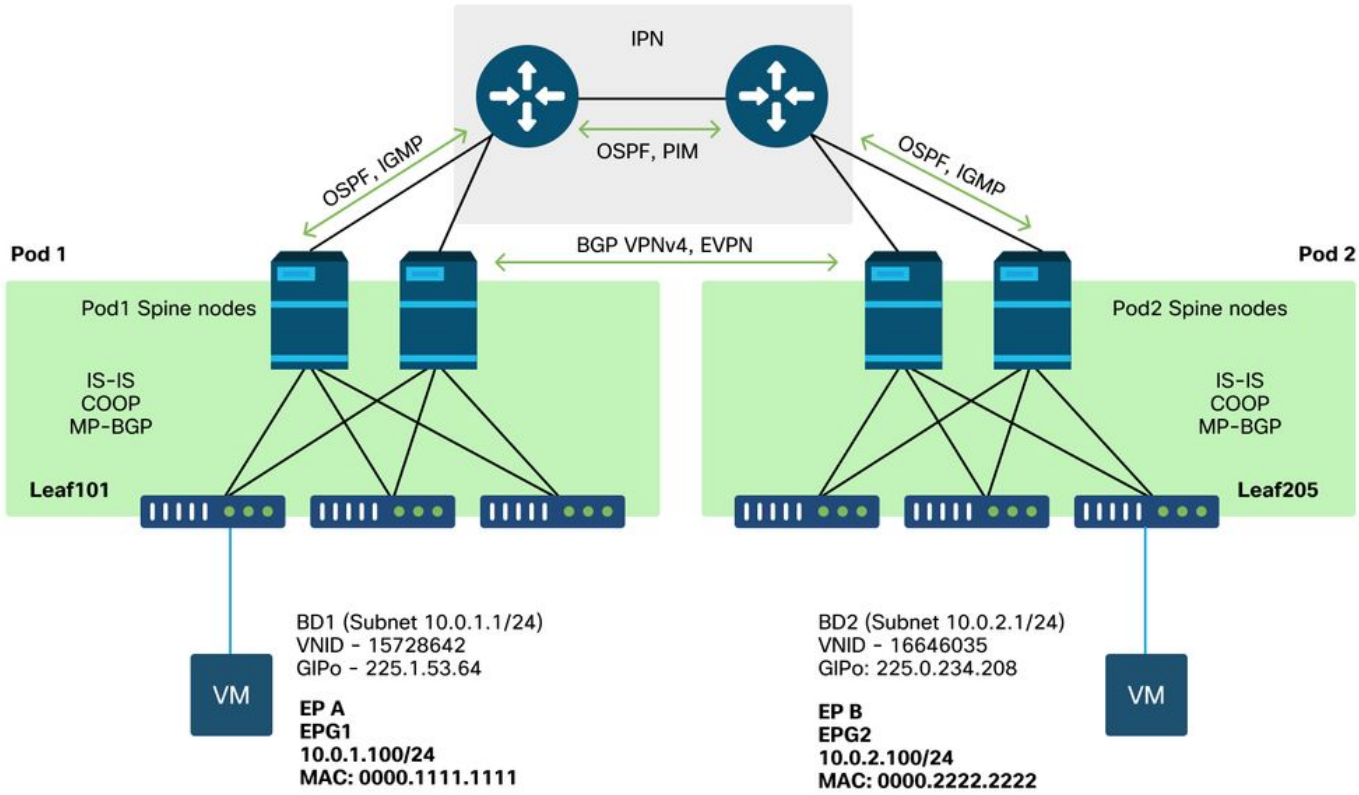
TEP 풀을 광고합니다.

- 한 포드에서 다른 포드로 학습된 외부 경로를 교환하기 위해 BGP VPNv4 주소군이 스파인 노드 간에 확장됩니다. 각 Pod는 별도의 경로 리플렉터 클러스터가 됩니다.
- COOP에 저장된 엔드포인트 및 기타 정보를 Pod 간에 동기화하기 위해 BGP EVPN 주소군이 스파인 노드 간에 확장됩니다.
- 마지막으로, Pod에서 브로드캐스트, 알 수 없는 유니캐스트 및 멀티캐스트(BUM) 트래픽의 플러딩을 처리하기 위해 각 Pod의 스파인 노드는 IGMP 호스트의 역할을 하며 IPN 라우터는 양방향 PIM을 통해 멀티캐스트 라우팅 정보를 교환합니다.

다중 포드 문제 해결 시나리오 및 워크플로의 상당 부분은 단일 포드 ACI 패브릭과 유사합니다. 이 Multi-Pod 섹션에서는 주로 Single Pod와 Multi-Pod 포워딩 간의 차이점을 중점적으로 살펴봅니다.

멀티 포드 예를 위한 토폴로지

모든 시나리오의 트러블슈팅과 마찬가지로, 예상되는 상태가 무엇인지 이해하는 것부터 시작해야 합니다. 이 장의 예는 이 토폴로지를 참조하십시오.



멀티 포드 포워딩 문제 해결을 위한 일반 워크플로

상위 레벨에서 멀티 포드 포워딩 문제를 디버깅할 때 다음 단계를 평가할 수 있습니다.

1. 플로우가 유니캐스트 또는 다중 목적지입니까? 플로가 작업 상태에서 유니캐스트될 것으로 예상되더라도 ARP가 확인되지 않으면 다중 대상 플로우입니다.
2. 흐름이 라우팅됩니까 브리지됩니까? 일반적으로 ACI 관점의 라우팅된 흐름은 목적지 MAC 주소가 ACI에 구성된 게이트웨이가 소유한 라우터 MAC 주소인 모든 흐름입니다. 또한 ARP 플러딩을 비활성화할 경우 인그레스 리프는 대상 IP 주소를 기반으로 라우팅됩니다. 목적지

MAC 주소가 ACI에서 소유하지 않은 경우 스위치는 MAC 주소를 기반으로 전달되거나 브리지 도메인에 구성된 '알 수 없는 유니캐스트' 동작을 따릅니다.
3. 인그레스 리프가 흐름을 중단합니까? Triage와 ELAM은 이를 확인하는 가장 좋은 툴입니다.

플로우가 레이어 3 유니캐스트인 경우

1. 인그레스 leaf에는 소스 EPG와 동일한 VRF에 있는 목적지 IP에 대한 엔드포인트 learn이 있습니까? 이 경우 학습한 모든 경로보다 항상 우선합니다. Leaf는 엔드포인트가 학습되는 터널 주소 또는 이그레스 인터페이스로 직접 전달됩니다.
2. 엔드포인트가 학습되지 않은 경우 인그레스 리프에 '퍼베이시브' 플래그가 설정된 대상에 대한 경로가 있습니까? 이는 대상 서브넷이 브리지 도메인 서브넷으로 구성되어 있고 다음 홉이 로컬 포드의 스파인 프록시여야 함을 나타냅니다.
3. 퍼베이시브 경로가 없는 경우 마지막 방법은 L3Out을 통해 학습되는 모든 경로입니다. 이 부분은 단일 포드 L3Out 포워딩과 동일합니다.

플로우가 레이어 2 유니캐스트인 경우

1. 인그레스 리프에 소스 EPG와 동일한 브리지 도메인의 대상 MAC 주소에 대한 엔드포인트 학습이 있습니까? 이 경우 leaf는 원격 터널 IP로 전달되거나 엔드포인트가 학습되는 로컬 인터페이스 밖으로 전달됩니다.
2. 소스 브리지 도메인에서 대상 MAC 주소에 대한 학습이 없는 경우 리프는 BD가 설정된 'unknown-unicast' 동작을 기반으로 전달됩니다. 'Flood'로 설정하면 Leaf가 브리지 도메인에 할당된 GIPo 멀티캐스트 그룹으로 플러딩됩니다. 로컬 및 원격 Pod는 플러딩 복사본을 받아야 합니다. '하드웨어 프록시'로 설정된 경우 프록시 조회를 위해 프레임이 스파인으로 전송되고 스파인의 COOP 항목에 따라 전달됩니다.

트러블슈팅 출력이 BUM과 비교하여 유니캐스트에 대해 상당히 다르므로, 유니캐스트에 대한 작업 출력 및 시나리오는 BUM으로 이동하기 전에 고려됩니다.

멀티 포드 유니캐스트 문제 해결 워크플로

토폴로지에 따라 leaf205의 10.0.2.100에서 leaf101의 10.0.1.100으로 이어지는 흐름을 살펴봅니다.

참고, 여기서 진행하기 전에 소스가 게이트웨이(라우팅된 흐름의 경우)에 대해 ARP를 해결했는지 또는 목적지 MAC 주소(브리지된 흐름의 경우)를 해결했는지 확인해야 합니다

1. 인그레스 리프가 패킷을 수신하는지 확인합니다. 4.2에서 제공되는 보고서 출력과 함께 "Tools" 섹션에 표시된 ELAM CLI 툴을 사용합니다. ELAM Assistant App도 사용됩니다.

```
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
```

패킷이 인그레스 스위치에서 수신되었음을 확인하는 ELAM이 트리거되었습니다. 이제 결과가 방대하기 때문에 보고서에서 몇 개의 필드를 보십시오.

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

패킷의 위치에 대한 더 많은 정보가 보고서에 있지만 ELAM Assistant 앱이 현재 이 데이터를 해석하는 데 더 유용합니다. 이 흐름에 대한 ELAM Assistant 출력은 이 장의 뒷부분에 표시됩니다.

2. 인그레스 리프가 인그레스 VRF에서 목적지를 엔드포인트로 학습합니까? 그렇지 않다면 길이 있나요?

```
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
```

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

위 명령의 출력이 없으면 대상 IP가 학습되지 않습니다. 다음으로 라우팅 테이블을 확인합니다.

```
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
```

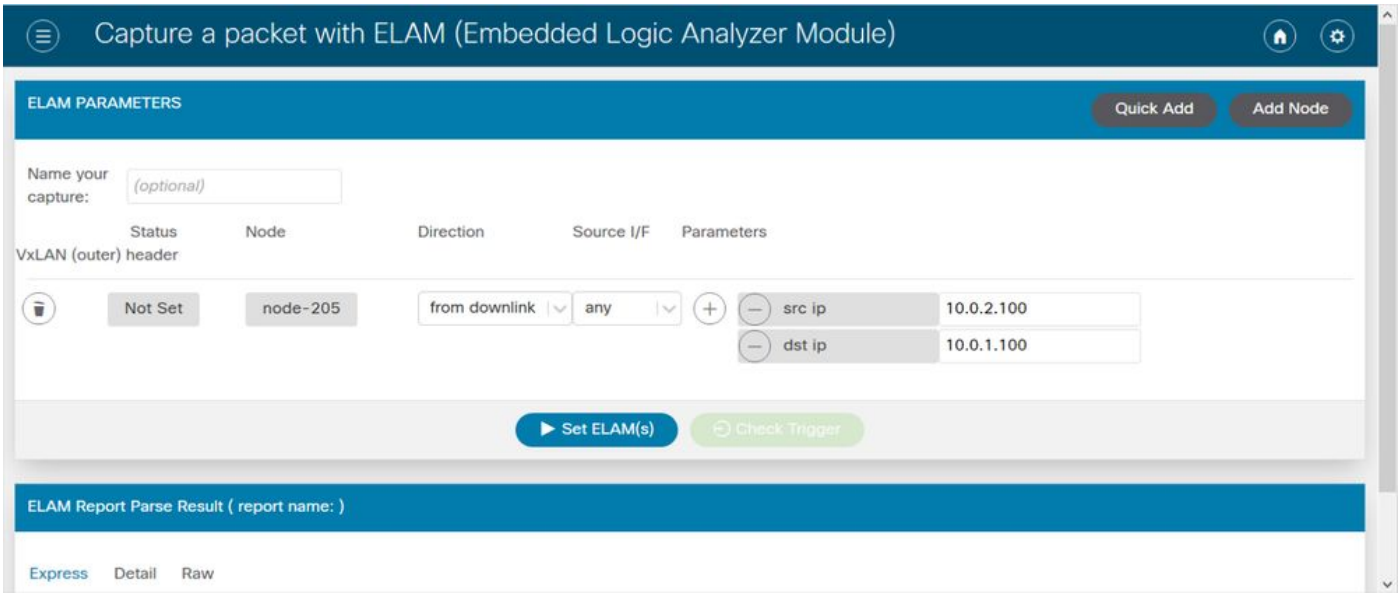
위 출력에서 퍼베이시브 플래그가 표시되며, 이는 브리지 도메인 서브넷 경로임을 나타냅니다. next-hop은 스핀의 애니캐스트 프록시 주소여야 합니다.

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

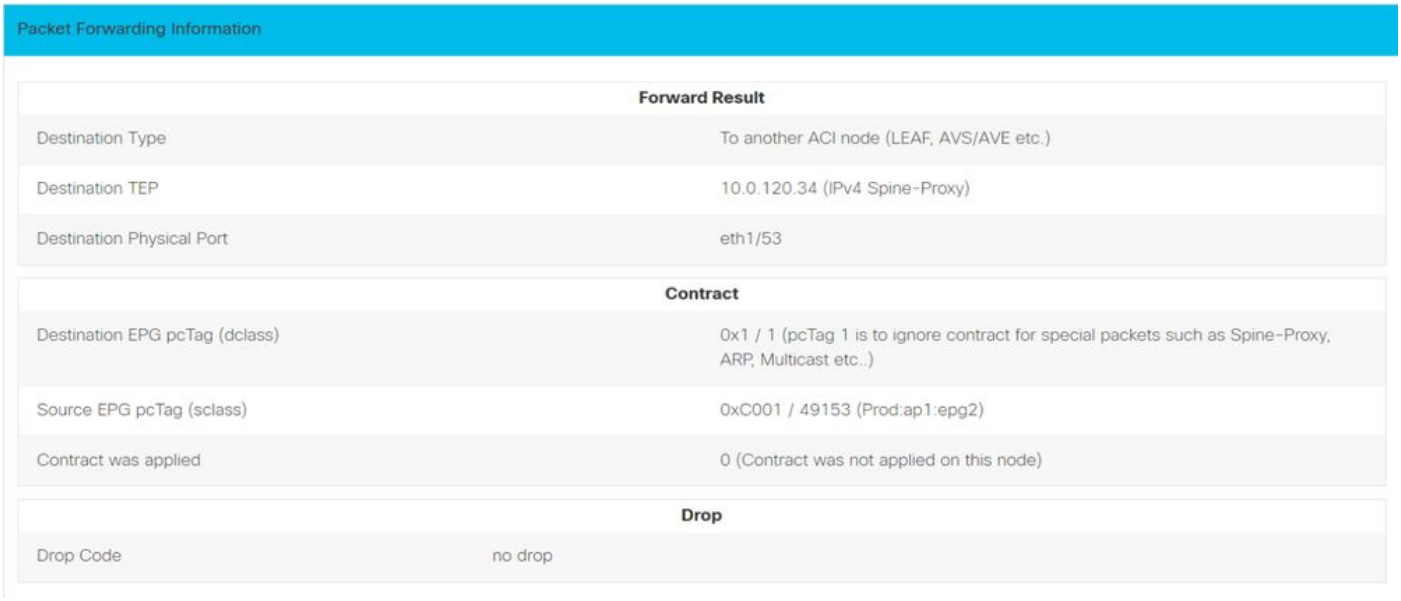
엔드포인트가 터널이나 물리적 인터페이스에서 학습되는 경우, 이 점이 우선하므로 패킷이 직접 해당 곳으로 전달됩니다. 자세한 내용은 이 책의 "외부 전달" 장을 참조하십시오.

ELAM Assistant를 사용하여 위 출력에 표시된 전달 결정을 확인합니다.

ELAM Assistant 컨피그레이션



전달 결정 확인



Packet Forwarding Information

Forward Result	
Destination Type	To another ACI node (LEAF, AVS/AVE etc.)
Destination TEP	10.0.120.34 (IPv4 Spine-Proxy)
Destination Physical Port	eth1/53

Contract	
Destination EPG pcTag (dclass)	0x1 / 1 (pcTag 1 is to ignore contract for special packets such as Spine-Proxy, ARP, Multicast etc..)
Source EPG pcTag (sclass)	0xC001 / 49153 (Prod:ap1:epg2)
Contract was applied	0 (Contract was not applied on this node)

Drop	
Drop Code	no drop

위 출력은 인그레스 리프가 패킷을 IPv4 스파인 프록시 주소로 포워딩하고 있음을 보여줍니다. 이것이 일어날 것으로 예상되는 일입니다.

3. 스파인에서 프록시 요청이 작동하도록 대상 IP가 COOP에 있는지 확인합니다.

스파인에서 COOP 출력을 가져오는 방법에는 여러 가지가 있습니다. 예를 들어 'show coop internal info ip-db' 명령을 사용하여 COOP 출력을 확인합니다.

```
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

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

스파인에서 실행할 기타 명령:

l2 항목에 대한 COOP 쿼리:

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

COOP에서 l3 항목을 쿼리하고 부모 l2 항목을 가져옵니다.

```
moquery -c coopEpRec -x rsp-subtree=children 'rsp-subtree-
```

```
filter=eq(coopIpv4Rec.addr,"192.168.1.1")' rsp-subtree-include=required
```

l3 항목에 대해서만 COOP 쿼리:

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

다중 moquery의 유용한 점은 APIC에서 직접 실행할 수 있으며, 사용자는 레코드가 coop에 있는 모든 spine을 볼 수 있다는 점입니다.

4. 멀티 포드 스파인 프록시 전달 결정

스파인의 COOP 항목이 로컬 Pod의 터널을 가리키는 경우 포워딩은 기존 ACI 동작을 기반으로 합니다.

TEP의 소유자는 APIC에서 실행하여 패브릭에서 확인할 수 있습니다. moquery **-c ipv4Addr -f 'ipv4.Addr.addr=="<tunnel address>"'**

프록시 시나리오에서 터널 next-hop은 10.0.0.34입니다. 이 IP 주소의 소유자는 누구입니까?:

```
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]
```

이 IP는 Pod 1의 두 스파인 노드에서 모두 소유합니다. 외부 프록시 주소라고 하는 특정 IP입니다. ACI가 Pod 내의 스파인 노드가 소유한 프록시 주소를 갖는 것과 같은 방식으로(이 섹션의 2단계 참조) Pod 자체에 할당된 프록시 주소도 있습니다. 이 인터페이스 유형은 다음을 실행하여 확인할 수 있습니다.

```
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]
```

'external' 플래그는 외부 프록시 TEP임을 나타냅니다.

5. 스파인에서 BGP EVPN 확인

Spine의 BGP EVPN에서 CoOp 엔드포인트 레코드를 가져와야 합니다. 다음 명령을 사용하여 EVPN에 있는지 확인할 수 있습니다(원격 Pod 외부 프록시 TEP의 다음 홉과 이미 COOP에 있는 경우 EVPN에서 온 것으로 간주할 수 있음).

```
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
```

위 명령은 MAC 주소에서도 실행할 수 있습니다.

-192.168.1.254는 다중 포드 설정 중에 구성되는 데이터 플레인 TEP입니다. 그러나 BGP에서 NH로 광고되더라도 실제 next-hop은 외부 프록시 TEP가 됩니다.

-192.168.1.101 및 .102는 이 경로를 광고하는 Pod 1 스파인 노드입니다.

6. 대상 포드의 스파인에서 COOP를 확인합니다.

이전과 동일한 명령을 사용할 수 있습니다.

```
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

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

APIC에서 다음 명령을 실행하여 터널 주소를 소유한 사용자를 확인합니다.

```
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
```

위 명령은 COOP에서 leaf101로의 터널이 있음을 나타냅니다. 즉 leaf101은 대상 끝점에 대한 로컬 학습을 가져야 합니다.

7. 이그레스 리프에 로컬 학습이 있는지 확인합니다.

이는 'show endpoint' 명령을 통해 수행할 수 있습니다.

```
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
```

엔드포인트가 학습됩니다. 패킷은 VLAN 태그 1075가 설정된 포트 채널 5를 기반으로 전달되어야 합니다.

분류를 사용하여 엔드 투 엔드 흐름 확인

이 장의 "툴" 섹션에서 설명한 것처럼, Triage를 사용하여 기존 플로우를 엔드 투 엔드로 매핑하고 경로의 모든 스위치가 패킷과 어떤 작업을 수행하는지 파악할 수 있습니다. 이 기능은 멀티포드와

같이 규모가 크고 복잡한 구축에서 특히 유용합니다.

Triage를 완전히 실행하는 데 약간의 시간이 걸립니다(잠재적으로 15분).

예시 흐름에서 분류를 실행할 경우

```
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"}}}
```

트리지에 많은 양의 데이터가 있습니다. 가장 중요한 필드 중 일부가 강조 표시됩니다. 패킷의 경로는 'leaf205 (Pod 2) > spine3 (Pod 2) > spine2 (Pod 1) > leaf101 (Pod 1)'입니다. 이 과정에서 이루어진 모든 전달 결정 및 계약 조회도 표시됩니다.

레이어 2 플로우인 경우, Triage의 구문을 다음과 같이 설정해야 합니다.

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

EP가 COOP에 없는 프록시 처리된 요청

구체적인 장애 시나리오를 고려하기 전에 Multi-Pod를 통한 유니캐스트 전달과 관련된 한 가지 사항을 추가로 논의해야 합니다. 대상 엔드포인트를 알 수 없고 요청이 프록시되며 엔드포인트가 COOP에 없는 경우 어떻게 됩니까?

이 시나리오에서는 패킷/프레임이 스파인으로 전송되고 희박한 요청이 생성됩니다.

스파인이 간결한 요청을 생성하면 원래 패킷은 요청에 계속 보존되지만 패킷은 이더 타입 0xfff2를 수신합니다. 이더 타입은 간헐적으로 예약된 사용자 지정 이더 타입입니다. 따라서 Wireshark와 같은 패킷 캡처 툴에서는 이러한 메시지를 해석하기가 쉽지 않습니다.

외부 레이어 3 대상도 239.255.255.240으로 설정됩니다. 이 그룹은 글린 메시지에 대해 특별히 예약된 멀티캐스트 그룹입니다. 이는 패브릭 전체에 걸쳐 플러딩되어야 하며, Glean 요청의 대상 서브넷이 구축된 이그레스 리프 스위치는 대상을 확인하기 위해 ARP 요청을 생성합니다. 이러한 ARP는 구성된 BD 서브넷 IP 주소에서 전송됩니다. 따라서 브리지 도메인에서 유니캐스트 라우팅이 비활성화된 경우 프록시 요청으로 무음/알 수 없는 엔드포인트의 위치를 확인할 수 없습니다.

이그레스 리프 및 이후에 생성된 ARP 및 수신된 ARP 응답에서 일반 메시지가 수신되는 것을 다음 명령을 통해 확인할 수 있습니다.

ARP 확인 간소화

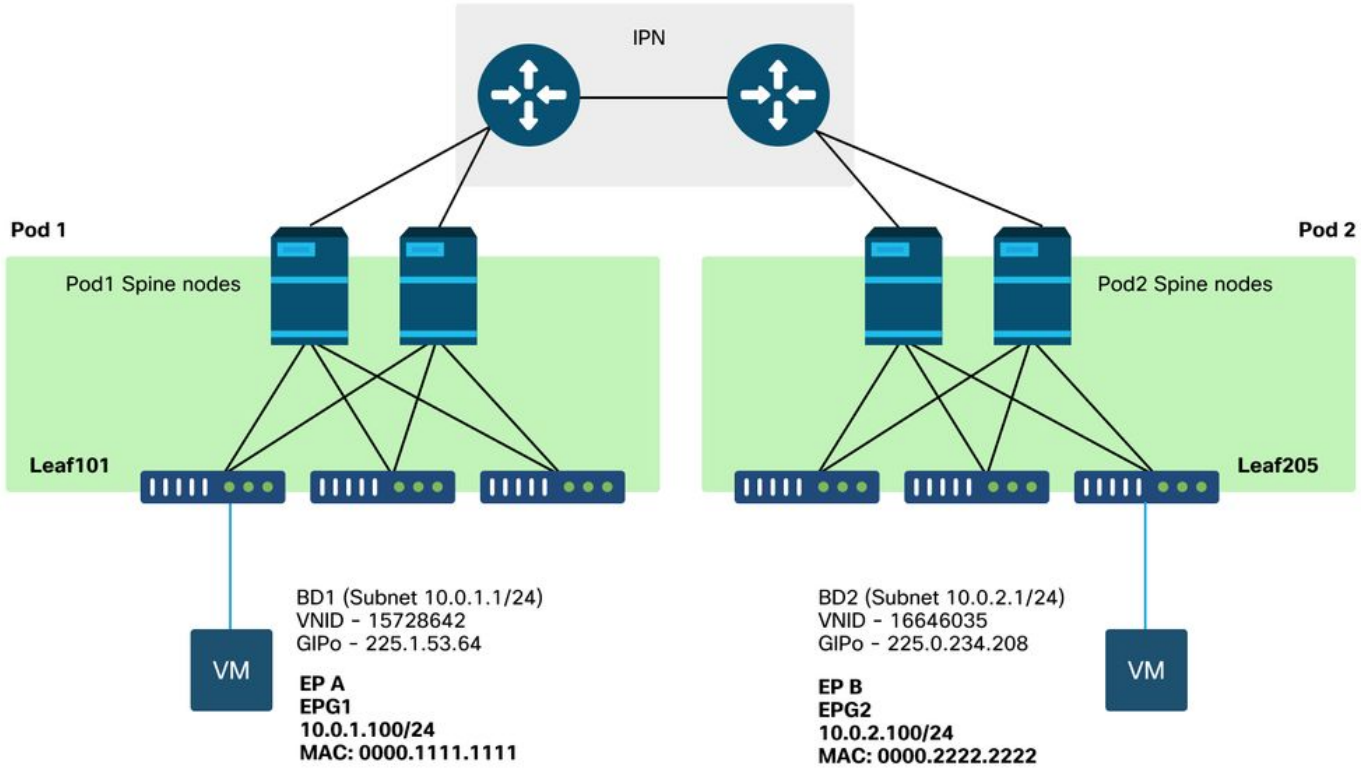
```
a-leaf205# show ip arp internal event-history event | grep -F -B 1 192.168.21.11
...
73) Event:E_DEBUG_DSF, length:127, at 316928 usecs after Wed May  1 08:31:53 2019
Updating epm ifidx: 1a01e000 vlan: 105 ip: 192.168.21.11, ifMode: 128 mac: 8c60.4f02.88fc   <<<
Endpoint is learned
75) Event:E_DEBUG_DSF,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

참고로, 239.255.255.240으로 전송되는 일반 메시지는 이 그룹을 IPN의 양방향 PIM 그룹 범위에 포함해야 하는 이유입니다.

Multi-Pod 트러블슈팅 시나리오 #1(유니캐스트)

다음 토폴로지에서 EP B는 EP A와 통신할 수 없습니다.

토폴로지 문제 해결



Multi-Pod 전달에 대해 나타나는 많은 문제는 단일 Pod에 나타나는 문제와 동일합니다. 이 때문에 멀티팟에 특화된 문제들이 집중되고 있다.

앞에서 설명한 유니캐스트 트러블슈팅 워크플로를 따르는 동안 요청이 프록시되지만 Pod 2의 스파인 노드에는 COOP의 대상 IP가 없습니다.

원인: COOP에 엔드포인트가 없습니다.

앞서 설명한 것처럼 원격 포드 엔드포인트의 COOP 항목은 BGP EVPN 정보로부터 채워집니다. 그 결과 다음을 확인하는 것이 중요합니다.

a.) 소스 포드(포드 2) 스파인에 EVPN이 있습니까?

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

b.) 원격 포드(포드 1) 스파인이 EVPN에 포함되어 있습니까?

```
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:
```

Pod 1 spine에 Spine이 있고 next-hop IP는 0.0.0.0입니다. 이는 COOP에서 로컬로 내보내기되었음을 의미합니다. 그러나 '피어에 알림' 섹션에는 Pod 2 스파인 노드가 포함되어 있지 않습니다.

c.) BGP EVPN이 Pod 간에 연결됩니까?

```
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
```

위 출력에서 BGP EVPN 피어링이 Pod 간에 다운되었음을 확인합니다. State/PfxRcd 열의 숫자 값 이외의 값은 인접성이 작동되지 않음을 나타냅니다. Pod 1 EP는 EVPN을 통해 학습되지 않으며 COOP로 가져오지 않습니다.

이 문제가 표시되면 다음을 확인합니다.

1. 스파인 노드와 연결된 IPN 간에 OSPF가 활성화되어 있습니까?
2. 스파인 노드에 원격 스파인 IP에 대해 OSPF를 통해 학습된 경로가 있습니까?
3. IPN의 전체 경로가 점보 MTU를 지원합니까?
4. 모든 프로토콜 인접성이 안정적입니까?

기타 가능한 원인

엔드포인트가 Pod의 COOP 데이터베이스에 없고 대상 디바이스가 무음 호스트인 경우(패브릭의 leaf 스위치에서 학습되지 않음) 패브릭 Glean 프로세스가 올바르게 작동하는지 확인합니다. 이를 위해

- BD에서 유니캐스트 라우팅을 활성화해야 합니다.
- 대상은 BD 서브넷에 있어야 합니다.
- IPN은 239.255.255.240 그룹에 대한 멀티캐스트 라우팅 서비스를 제공해야 합니다.

멀티캐스트 부분에 대해서는 다음 섹션에서 자세히 설명합니다.

Multi-Pod broadcast, unknown unicast, and multicast (BUM) forwarding 개요

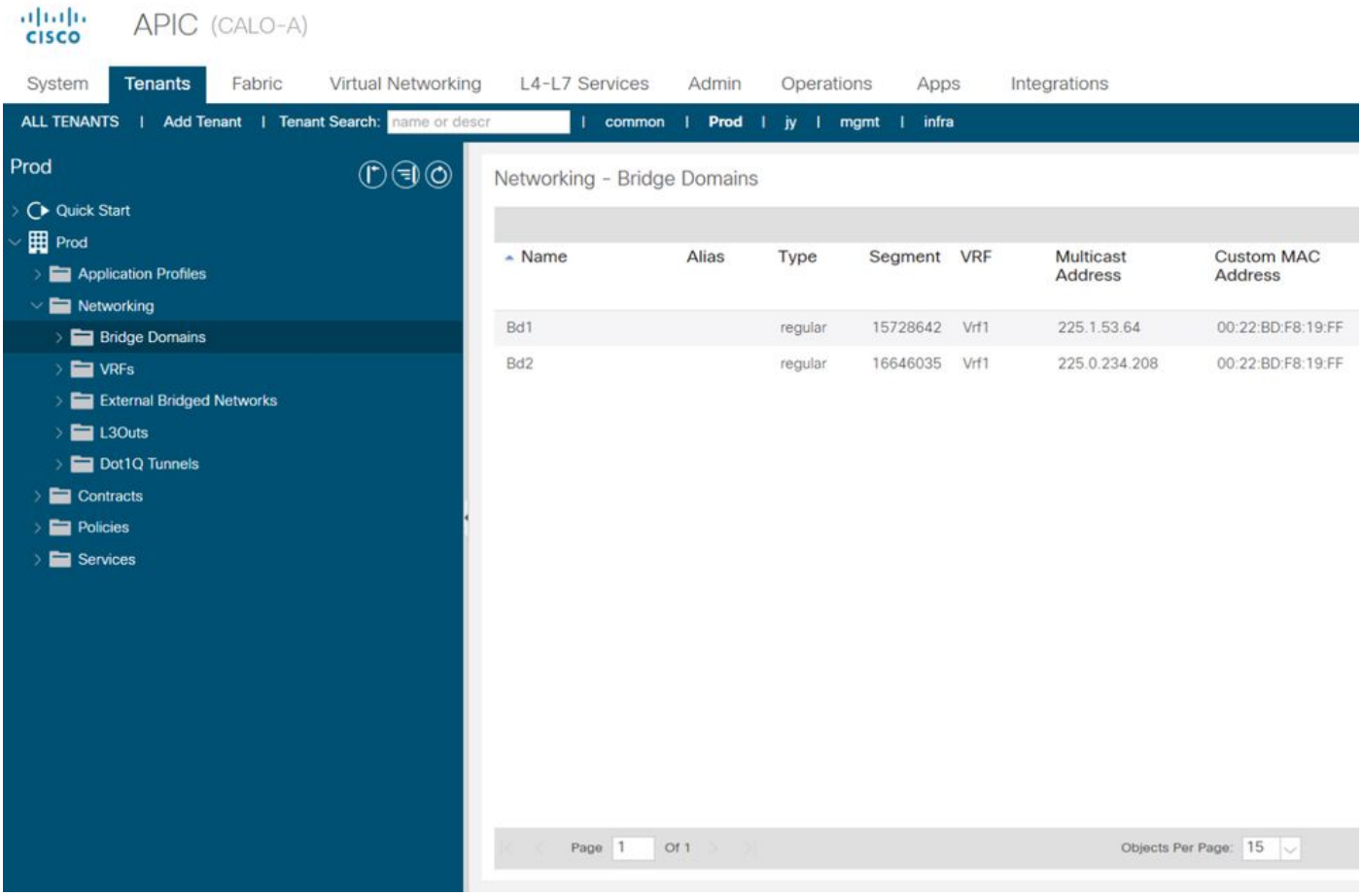
ACI에서는 여러 가지 시나리오에서 오버레이 멀티캐스트 그룹을 통해 트래픽이 플러딩됩니다. 예를 들어, 플러딩은 다음에 대해 발생합니다.

- 멀티캐스트 및 브로드캐스트 트래픽.
- 플러딩되어야 하는 알 수 없는 유니캐스트.
- Fabric ARP는 메시지를 간소화합니다.
- EP가 메시지를 알립니다.

많은 기능과 기능이 BUM 포워딩을 사용합니다.

ACI 내에서 모든 브리지 도메인은 GIPo(Group IP Outer) 주소라고 하는 멀티캐스트 주소에 할당됩니다. 브리지 도메인 내에서 플러딩해야 하는 모든 트래픽이 이 GIPo에서 플러딩됩니다.

GUI의 BD GIPo



APIC 중 하나에서 객체를 직접 쿼리할 수 있습니다.

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
```

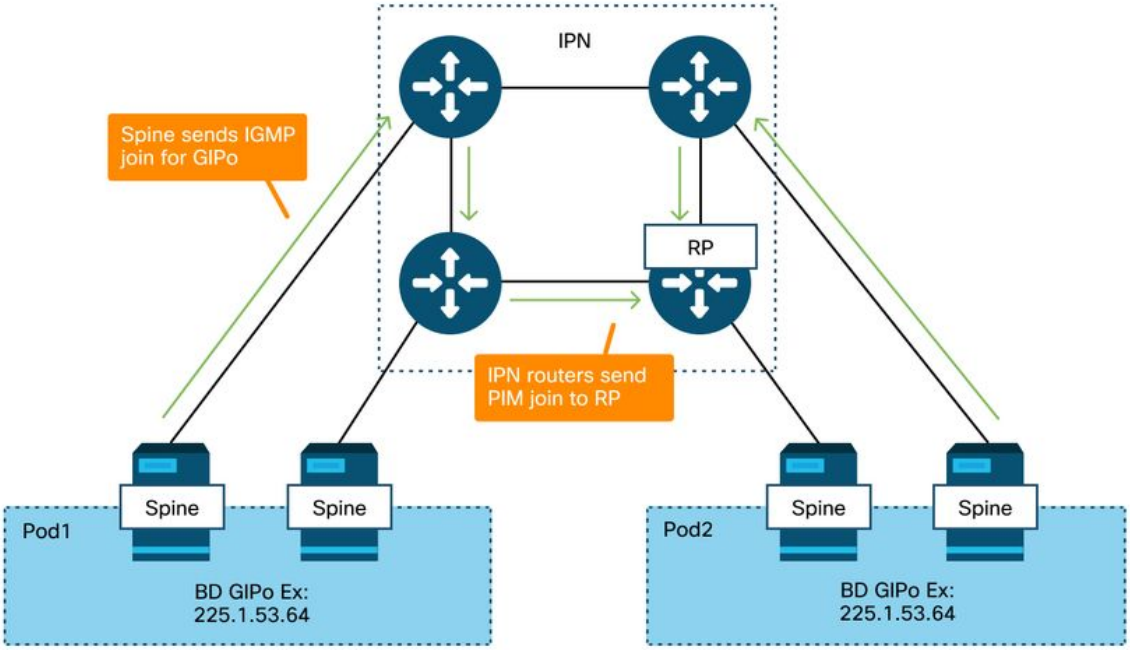
```
lcOwn                   : local
limitIpLearnToSubnets   : yes
llAddr                  : ::
mac                     : 00:22:BD:F8:19:FF
mcastAllow              : no
modTs                   : 2019-09-30T20:12:01.339-04:00
monPolDn                : uni/tn-common/monepg-default
mtu                     : 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
```

위와 같은 GIPo flooding에 대한 정보는 Multi-Pod의 사용 여부와 관계없이 사실이다. 이 중 멀티포드와 관련된 부분은 IPN의 멀티캐스트 라우팅입니다.

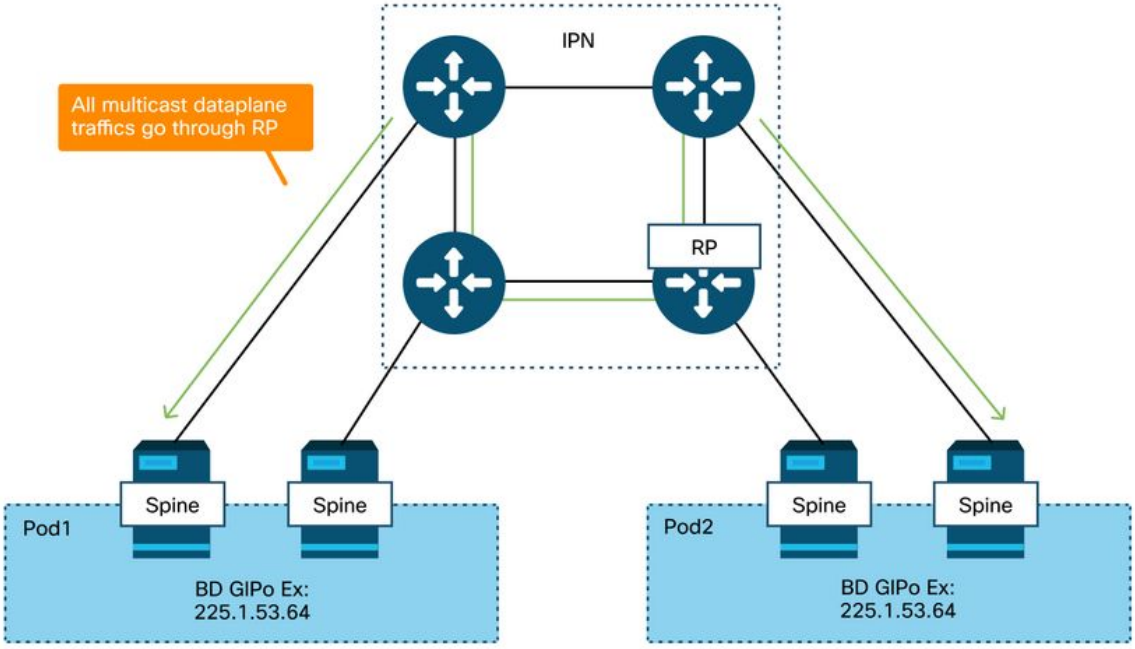
IPN 멀티캐스트 라우팅에는 다음이 포함됩니다.

- 스파인 노드는 멀티캐스트 호스트로 작동합니다(IGMP만 해당). PIM을 실행하지 않습니다.
- BD가 Pod에 구축된 경우 해당 Pod의 스파인 하나가 IPN 연결 인터페이스 중 하나에서 IGMP 조인을 전송합니다. 이 기능은 모든 스파인 노드 및 IPN 연결 인터페이스에서 여러 그룹에 걸쳐 스트라이핑됩니다.
- IPN은 이러한 조인을 수신하고 양방향 PIM RP를 향해 PIM 조인을 전송합니다.
- PIM Bidir이 사용되므로 (S,G) 트리가 없습니다. (*,G) 트리만 PIM Bidir에서 사용됩니다.
- GIPo로 전송된 모든 데이터 플레인 트래픽은 RP를 통과합니다.

IPN 멀티캐스트 컨트롤 플레인



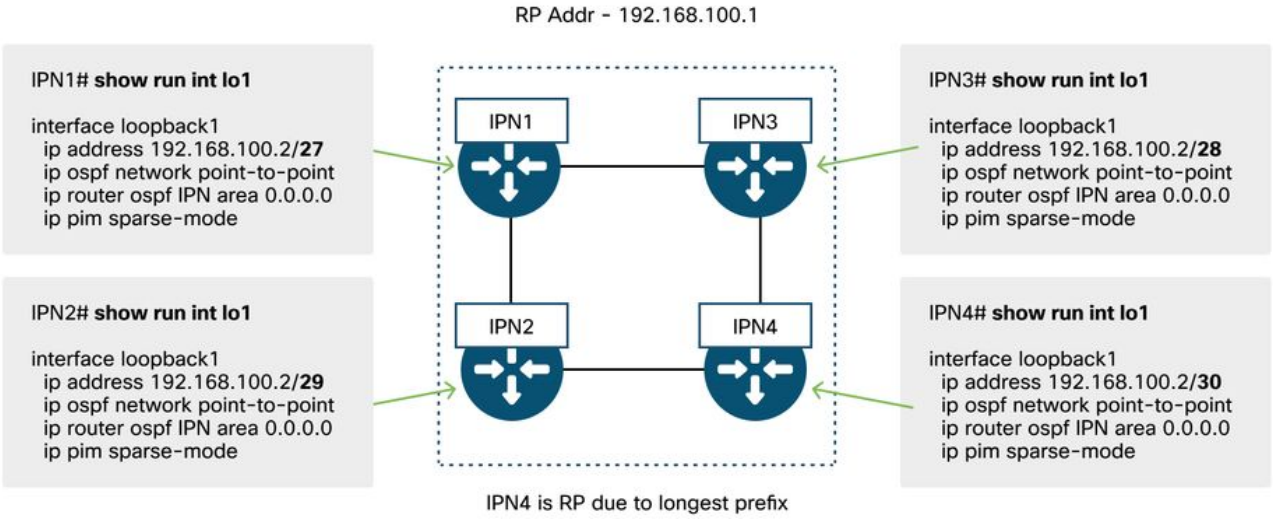
IPN 멀티캐스트 데이터 플레인



PIM Bidir을 사용한 RP 이중화 방법은 Phantom을 사용하는 것입니다. 이 내용은 이 책의 Multi-Pod Discovery 부분에서 자세히 다룹니다. 빠른 요약으로, Phantom RP를 사용하면 다음을 수행할 수 있습니다.

- 모든 IPN은 동일한 RP 주소로 구성해야 합니다.
- 정확한 RP 주소는 어떤 디바이스에도 없어야 합니다.
- 여러 디바이스는 Phantom RP IP 주소를 포함하는 서브넷에 대한 연결성을 알립니다. 모든 라우터가 누가 RP를 위한 최상의 경로를 광고하는지 합의할 수 있도록 광고되는 서브넷은 서브넷 길이가 달라야 합니다. 이 경로가 손실되면 컨버전스는 IGP에 따라 달라집니다.

Phantom RP 컨피그레이션



멀티 포드 브로드캐스트, 알 수 없는 유니캐스트 및 멀티캐스트 (BUM) 문제 해결 워크플로

1. 먼저 패브릭에서 플로우를 다중 대상으로 취급하는지 확인합니다.

흐름은 다음과 같은 일반적인 예에서 BD에 플러딩됩니다.

- 프레임은 ARP 브로드캐스트이며 BD에서 ARP 플러딩이 활성화됩니다.
- 프레임은 멀티캐스트 그룹으로 전달됩니다. IGMP-snooping이 활성화된 경우에도 트래픽은 항상 GIPo의 패브릭으로 플러딩됩니다.
- 트래픽은 ACI가 멀티캐스트 라우팅 서비스를 제공하는 멀티캐스트 그룹으로 전달됩니다.
- 흐름은 레이어 2(브리지 흐름)이고 대상 MAC 주소는 알 수 없으며 BD의 알 수 없는 유니캐스트 동작이 '플러드'로 설정됩니다.

어떤 전달 결정을 내릴지 가장 쉽게 결정하는 방법은 ELAM을 사용하는 것입니다.

2. BD GIPo를 확인합니다.

이에 대해 설명하는 이 장의 앞부분에 나오는 부분을 참조하라. Spine ELAM은 ELAM Assistant App을 통해 실행하여 플러딩된 트래픽이 수신되는지 확인할 수도 있습니다.

3. 해당 GIPo의 IPN에서 멀티캐스트 라우팅 테이블을 확인합니다.

이 작업을 수행하는 출력은 사용 중인 IPN 플랫폼에 따라 다르지만 상위 레벨에서는 다음과 같습니다.

- 모든 IPN 라우터는 RP에 동의해야 하며 이 GIPo의 RPF는 이 트리를 가리켜야 합니다.
- 각 Pod에 연결된 하나의 IPN 라우터가 그룹의 IGMP 가입을 받아야 합니다.

Multi-Pod 트러블슈팅 시나리오 #2(BUM 플로우)

이 시나리오에서는 Multi-Pod 또는 BUM 시나리오(알 수 없는 유니캐스트 등)에서 ARP가 확인되지 않는 시나리오를 다룹니다.

여기에는 몇 가지 일반적인 원인이 있습니다.

가능한 원인 1: 여러 라우터가 PIM RP 주소 소유

이 시나리오에서는 인그레스 리프가 트래픽을 플러딩하고(ELAM으로 확인), 소스 Pod가 트래픽을 수신하고 플러딩하지만 원격 Pod는 이를 수신하지 않습니다. BD의 경우, 홍수가 효과가 있지만, 다른 BD의 경우 그렇지 않습니다.

IPN에서 GIPo에 대해 'show ip mroute <GIPo address>'를 실행하여 RPF 트리가 여러 다른 라우터를 가리키는지 확인합니다.

이 경우 다음을 확인하십시오.

- 실제 PIM RP 주소가 아무 곳에도 구성되지 않았는지 확인합니다. 해당 실제 RP 주소를 소유한 디바이스에는 로컬 /32 경로가 표시됩니다.
- 여러 IPN 라우터가 Phantom RP 시나리오에서 RP에 대해 동일한 접두사 길이를 광고하지 않는지 확인합니다.

가능한 원인 2: IPN 라우터가 RP 주소에 대한 경로를 학습하지 않음

첫 번째 가능한 원인과 같은 방식으로, 여기서 홍수 트래픽은 IPN을 떠나지 못하고 있습니다. 각 IPN 라우터의 'show ip route <rp address>' 출력은 다른 라우터가 광고하는 접두사 길이가 아니라 로컬로 구성된 접두사 길이만 표시합니다.

따라서 실제 RP IP 주소가 아무 곳에도 구성되지 않았음에도 각 디바이스는 RP로 간주합니다.

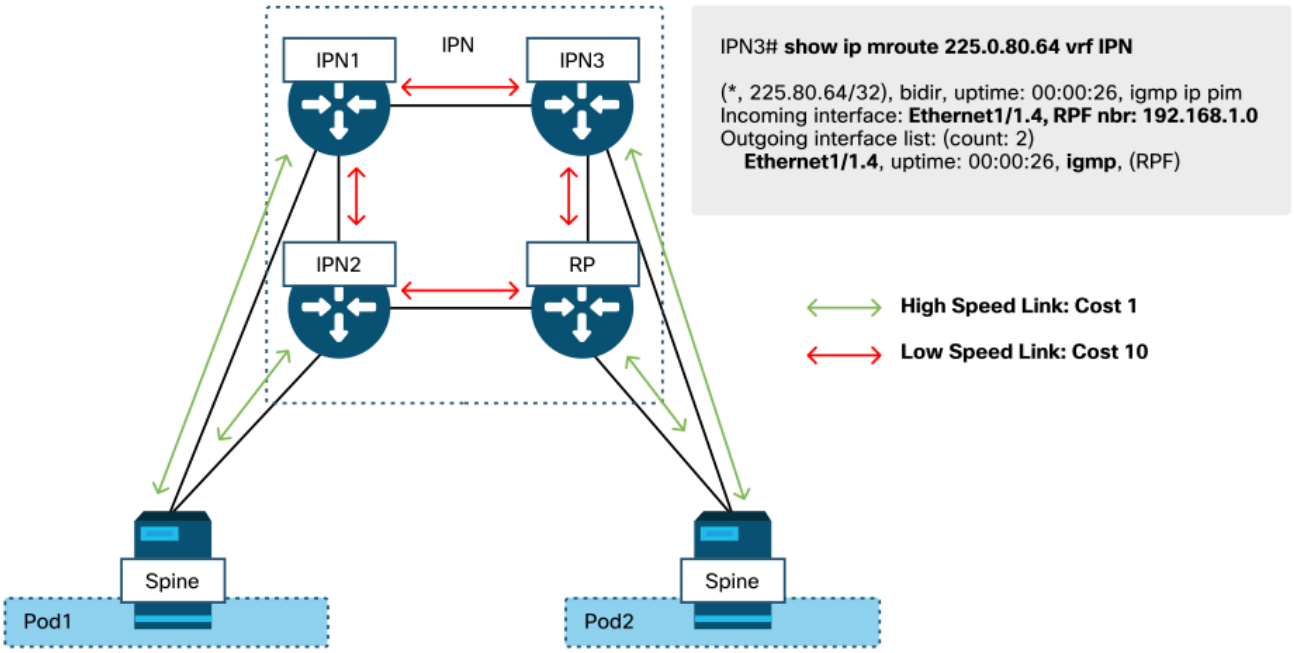
그렇다면 다음을 확인합니다.

- IPN 라우터 간에 라우팅 인접성이 설정되어 있는지 확인합니다. 경로가 실제 프로토콜 데이터베이스(예: OSPF 데이터베이스)에 있는지 확인합니다.
- 후보 RP가 되어야 하는 모든 루프백이 OSPF 포인트-투-포인트 네트워크 유형으로 구성되었는지 확인합니다. 이 네트워크 유형이 구성되지 않은 경우 각 라우터는 실제로 구성된 것과 상관없이 항상 /32 접두사 길이를 알립니다.

가능한 원인 3: IPN 라우터가 GIPo 라우트 또는 RPF가 ACI를 가리키도록 설치하지 않음

앞에서 언급한 것처럼 ACI는 IPN 연결 링크에서 PIM을 실행하지 않습니다. 이는 RP를 향한 IPN의 최상의 경로가 ACI를 가리키면 안 된다는 것을 의미합니다. 이러한 상황이 발생할 수 있는 시나리오는 여러 IPN 라우터가 동일한 스파인에 연결되어 있고 IPN 라우터 간보다 스파인을 통해 더 나은 OSPF 메트릭이 표시되는 경우입니다.

ACI로의 RPF 인터페이스



이 문제를 해결하려면

- IPN 라우터 간의 라우팅 프로토콜 인접성이 작동되는지 확인합니다.
- 스파인 노드의 IPN 연결 링크에 대한 OSPF 비용 메트릭을 IPN-to-IPN 링크보다 해당 메트릭을 덜 선호하게 하는 값으로 늘립니다.

기타 참조

ACI 소프트웨어 4.0 이전에는 외부 디바이스에서 COS 6을 사용하는 데 몇 가지 문제가 있었습니다. 이러한 문제의 대부분은 4.0 개선 사항을 통해 해결되었지만 자세한 내용은 CiscoLive 세션 "BRKACI-2934 - Troubleshooting Multi-Pod" 및 "Quality of Service" 섹션을 참조하십시오.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.