思科ACI中L3out上的重叠子网

目录

简介

思科以应用为中心的基础设施(ACI)通过L3out（第3层外）促进内部租户和外部路由网络之间的通信。 此类L3outs也可配置为具有一个或多个终端组(EPG)。 为使ACI知道如何将传入流量分类，作为L3out的EPG，需要在启用特定标志的情况下定义显式子网。本文旨在从基于合同的策略应用的角度，对L3out EPG的硬件实现进行一些说明。我们将具体探讨标记“外部EPG的外部子网”，以及在单独的EPG上将重叠前缀声明为“外部”的意外后果。

概念

经验法则是：部署L3outs时，同一虚拟路由和转发(VRF)实例中的单独EPG不应具有标记为“外部EPG的外部子网”的重叠子网。这也意味着来自特定子网的流量不应通过不同EPG进入。这可能导致根据针对不相关EPG声明的子网的最长前缀匹配对流量进行意外分类。让我们看几个场景，详细了解一下

先决条件

对ACI的基本了解：L3outs、合同和策略实施。以下对一些有用术语进行了简要说明，有关这些术语的更详细信息不在本文档的范围内：

pcTag:ACI将流量分类到pcTag，这些是EPG的内部表示形式。默认情况下，这些值具有VRF范围 — 即，它们在VRF中是唯一的，但可在VRF之间重复使用。但是，如果一个EPG与位于不同VRF/租户中的另一个EPG有合同，则pcTag值具有全局范围 — 即，您在ACI中找不到具有相同pcTag的任何其他EPG。

拉丁美洲:嵌入式逻辑分析仪模块。此工具用于根据过滤器在ASIC上捕获一个数据包，并检查数据包上设置的报头/标志。此工具还有助于了解基于硬件的查找/逻辑

类/dclass:当流量进入枝叶时，枝叶将根据策略实施方向和本地可用前缀知识将源和目标流量标记到EPG中 — 在ELAM捕获中，这将分别被视为sclass和dclass

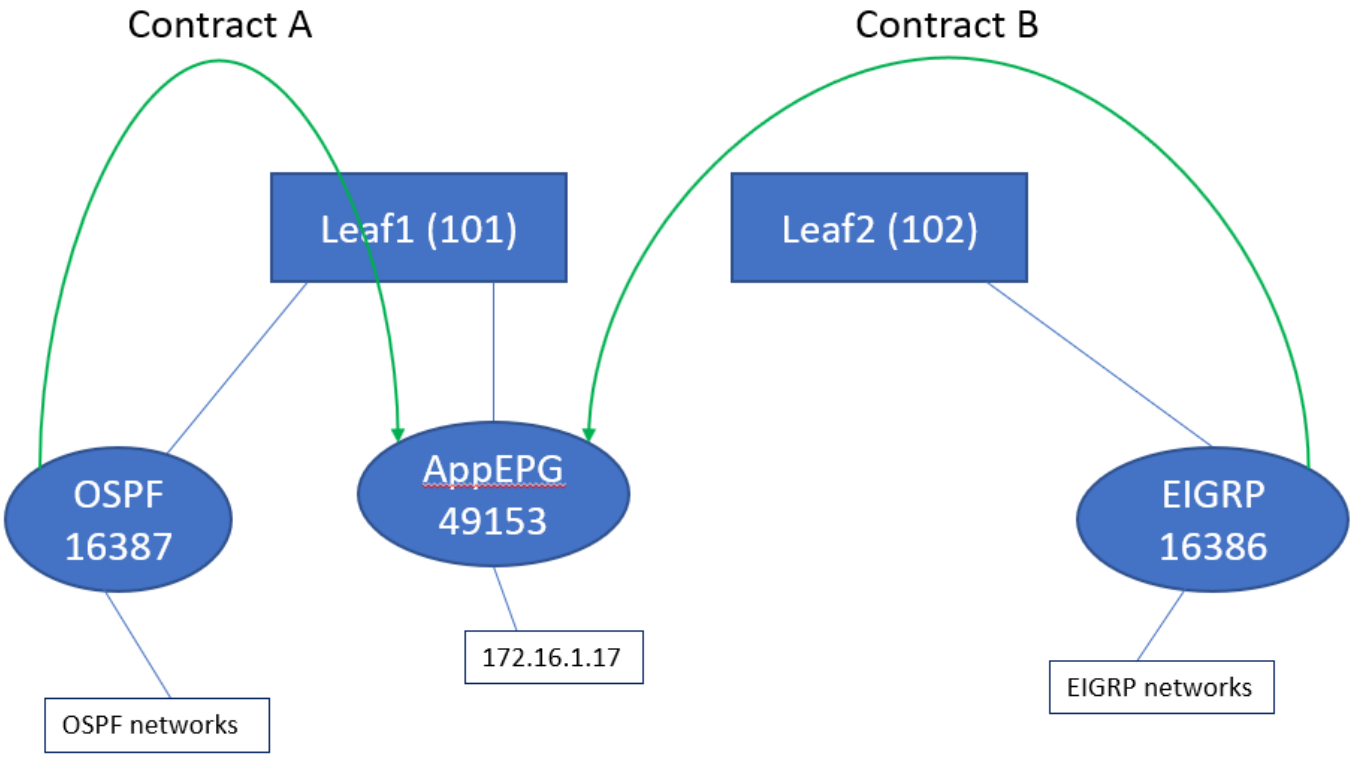
zoning-rule：这些是合同的内部表示形式，类似于ACL的行。SrcEpg和DstEpg值应与sclass/dclass匹配，以便流量达到给定规则并被允许。默认情况下，在强制vrf中，隐式拒绝作为最

后一行，因此任何与特定规则不匹配的流量都将达到隐式拒绝并被丢弃。

设置和拓扑

两个枝叶 — 101和102，型号：N9K-C93180YC-EX

- 版本3.2(4e)
- 使用一个VRF - 策略实施首选项：强制策略实施方向：入口.VRF VNID（VxLAN网络标识符）：2752513;pcTag:32770
- 枝叶1中的L3out(101)- 协议： 开放最短路径优先(OSPF)邻居关系的L3接口用户 — eth1/22(10.27.48.1/24)外部EPG pcTag:16387
- 枝叶101上的应用EPG 中继 — eth1/24 pcTag:49153IP终端：172.16.1.17 网关：172.16.1.254/24 — 部署在网桥域(BD)上 BD有pcTag 32771
- Leaf2上的L3out(202)- 协议：增强型内部网关路由协议 (EIGRP)用于与路径1/16邻居关系的SVI - vlan 2747(10.27.47.1/24)外部EPG pcTag:163869



场景

来自重叠子网的流量

在此场景中，我们观察流量来自重叠子网时（从ACI的角度）可能的错误分类

OSPF通告：

10.9.9.6/32

EIGRP通告：

10.9.9.1/32

我们从图1中的拓扑开始，但没有任何合同。对于OSPF上的EPG，我们将子网0.0.0.0/0定义为“外部EPG的外部子网”，将10.9.9.0/24定义为与EIGRP的EPG具有相同标志的子网。以下是Leaf1和2上的表：

枝叶1:

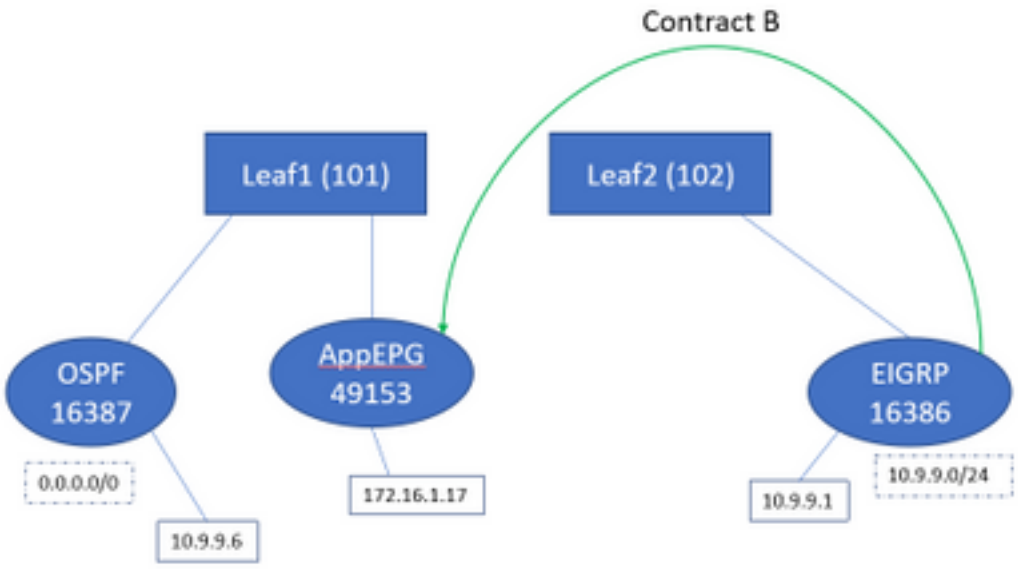
```
leaf101# show end int eth1/24
Legend:
 s - arp              H - vtep             V - vpc-attached     p - peer-aged
 R - peer-attached-rl B - bounce           S - static           M - span
 D - bounce-to-proxy  O - peer-attached    a - local-aged       L - local
+------------------------------------+--------------+-----------------+--------------+----------
---+
      VLAN/                            Encap           MAC Address       MAC Info/
Interface
      Domain                           VLAN            IP Address        IP Info
+------------------------------------+--------------+-----------------+--------------+----------
---+
48                                        vlan-2743    dcce.c15b.1e47 L
eth1/24
shparanj:eigrp-test                       vlan-2743       172.16.1.17 L
eth1/24

leaf101# show ip route vrf shparanj:eigrp-test
IP Route Table for VRF "shparanj:eigrp-test"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

10.9.9.1/32, ubest/mbest: 1/0
    *via 10.0.248.0%overlay-1, [200/128576], 05:31:49, bgp-65003, internal, tag 65003
10.9.9.6/32, ubest/mbest: 1/0
    *via 10.27.48.2, eth1/22, [110/5], 05:09:51, ospf-default, intra
10.27.47.0/24, ubest/mbest: 1/0
    *via 10.0.248.0%overlay-1, [200/0], 05:31:49, bgp-65003, internal, tag 65003
10.27.48.0/24, ubest/mbest: 1/0, attached, direct
    *via 10.27.48.1, eth1/22, [1/0], 05:31:46, direct
10.27.48.1/32, ubest/mbest: 1/0, attached
    *via 10.27.48.1, eth1/22, [1/0], 05:31:46, local, local
172.16.1.0/24, ubest/mbest: 1/0, attached, direct, pervasive
    *via 10.0.240.34%overlay-1, [1/0], 05:27:43, static
172.16.1.254/32, ubest/mbest: 1/0, attached, pervasive
    *via 172.16.1.254, vlan47, [1/0], 05:31:52, local, local



leaf101# show zoning-rule scope 2752513
Rule ID         SrcEPG          DstEPG          FilterID        operSt          Scope
Action                              Priority
=======         ======          ======          ========        ======          =====
======                              ========
4173            0               0               implicit        enabled         2752513
deny,log                            any_any_any(21)
4174            0               0               implarp         enabled         2752513
permit                              any_any_filter(17)
4175            0               15              implicit        enabled         2752513
deny,log                            any_vrf_any_deny(22)
4207            0               32771           implicit        enabled         2752513
```

```
permit                                  any_dest_any(16)


<<vsh>>  (to go into vsh propmt , type: #vsh )

leaf101# show system internal policy-mgr prefix | grep shparanj:eigrp-test
2752513 26     0x1a          Up     shparanj:eigrp-test
0.0.0.0/0   15      False  True   False
2752513 26     0x8000001a    Up     shparanj:eigrp-test
::/0   15      False  True   False
```

枝叶2:

```
leaf102# show ip route vrf shparanj:eigrp-test
IP Route Table for VRF "shparanj:eigrp-test"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

10.9.9.1/32, ubest/mbest: 1/0
    *via 10.27.47.10, vlan78, [90/128576], 06:13:41, eigrp-default, internal
10.9.9.6/32, ubest/mbest: 1/0
    *via 10.0.0.64%overlay-1, [200/5], 05:20:27, bgp-65003, internal, tag 65003
10.27.47.0/24, ubest/mbest: 1/0, attached, direct
    *via 10.27.47.2, vlan78, [1/0], 3d21h, direct
10.27.47.2/32, ubest/mbest: 1/0, attached
    *via 10.27.47.2, vlan78, [1/0], 3d21h, local, local
10.27.48.0/24, ubest/mbest: 1/0
    *via 10.0.0.64%overlay-1, [200/0], 05:35:06, bgp-65003, internal, tag 65003

leaf102# show zoning-rule scope 2752513 Rule ID SrcEPG DstEPG FilterID operSt Scope Action
Priority ======= ====== ====== ======== ====== ===== ====== ======== 4472 0 0 implicit enabled
2752513 deny,log any_any_any(21) 4471 0 0 implarp enabled 2752513 permit any_any_filter(17) 4470
0 15 implicit enabled 2752513 deny,log any_vrf_any_deny(22) <<vsh>> leaf102# show system
internal policy-mgr prefix | grep shparanj:eigrp-test 2752513 37 0x80000025 Up shparanj:eigrp-
test ::/0 15 False True False 2752513 37 0x25 Up shparanj:eigrp-test 0.0.0.0/0 15 False True
False 2752513 37 0x25 Up shparanj:eigrp-test 10.9.9.0/24 16386 False True False
```

让我们添加合同B（租户中的合同，范围vrf — 文件管理器：common:default）



添加合同B后，我们会看到在枝叶1上添加的eigrp EPG前缀：

```
leaf101# show system internal policy-mgr prefix | grep shparanj:eigrp-test
2752513 26 0x1a Up shparanj:eigrp-test 10.9.9.0/24 16386 False True False 2752513 26 0x1a Up
shparanj:eigrp-test 0.0.0.0/0 15 False True False 2752513 26 0x8000001a Up shparanj:eigrp-test
::/0 15 False True False
```

我们来看看其他策略：

枝叶1合同：

```
leaf101# show zoning-rule scope 2752513
Rule ID         SrcEPG          DstEPG          FilterID        operSt          Scope
Action                              Priority
=======         ======          ======          ========        ======          =====
======                              ========
4173            0               0               implicit        enabled         2752513
deny,log                            any_any_any(21)
4174            0               0               implarp         enabled         2752513
permit                              any_any_filter(17)
4175            0               15              implicit        enabled         2752513
deny,log                            any_vrf_any_deny(22)
4207            0               32771           implicit        enabled         2752513
permit                              any_dest_any(16)
4604 49153 16386 default enabled 2752513 permit src_dst_any(9) 4605 16386 49153 default enabled
2752513 permit src_dst_any(9)
```

枝叶2合同（保持不变）：

```
leaf102# show zoning-rule scope 2752513
Rule ID         SrcEPG          DstEPG          FilterID        operSt          Scope
Action                              Priority
=======         ======          ======          ========        ======          =====
======                              ========
4472            0               0               implicit        enabled         2752513
deny,log                            any_any_any(21)
4471            0               0               implarp         enabled         2752513
permit                              any_any_filter(17)
4470            0               15              implicit        enabled         2752513
deny,log                            any_vrf_any_deny(22)
```

在此场景中，从ospf l3out传入的流量，我们期望使用 16387改为使用16386标记。这是因为流量到达Leaf1上的新前缀条目。

从10.9.9.6 ping终端172.16.1.17:

```
# ping 172.16.1.17 vrf shp-ospf source 10.9.9.6 count 1000 interval 1
PING 172.16.1.17 (172.16.1.17) from 10.9.9.6: 56 data bytes
64 bytes from 172.16.1.17: icmp_seq=0 ttl=253 time=2.207 ms
64 bytes from 172.16.1.17: icmp_seq=1 ttl=253 time=1.443 ms
64 bytes from 172.16.1.17: icmp_seq=2 ttl=253 time=1.312 ms
```

即使没有ospf epg和app-epg之间的合同，Ping也能正常工作。这是因为它与eigrp-epg的策略相冲

突，并且获得允许。

拉丁美洲：

```
module-1(DBG-elam)# trigger init in-select 6 out-select 0
module-1(DBG-elam-insel6)# set outer ipv4 src_ip 10.9.9.6
module-1(DBG-elam-insel6)# start
module-1(DBG-elam-insel6)# stat
ELAM STATUS
===========
Asic 0 Slice 0 Status Armed
Asic 0 Slice 1 Status Triggered
module-1(DBG-elam-insel6)# report | grep sclass
      sug_lurw_vec.info.nsh_special.sclass: 0x4002
      sug_lurw_vec.info.ifabric_spine.sclass: 0x4002
      sug_lurw_vec.info.ifabric_leaf.sclass: 0x4002
#dec 0x4002
16386
```

在此场景中，由于流量被分类为与目标有合同的pcTag，因此流量最终工作正常。但是，例如，如果计算枝叶是单独的第3个枝叶，则我们的流量将失败 — 因为合同条目仅存在于第3个枝叶（入口策略）或枝叶102（出口策略）上。

具有重叠子网的交换矩阵在单独的外部EPG上声明为外部

在此场景中，我们将考虑由于不同外部EPG上声明为外部的重叠或相同子网而导致的策略冲突和可能的错误分类。

OSPF通告网络：

10.9.1.0/24

EIGRP通告网络：

10.9.2.0/24

我们从图1中的拓扑开始，但没有任何合同。我们将子网10.9.0.0/16定义为两个L3outs上EPG的“外部EPG的外部子网”。

以下是Leaf1和2上的表：

枝叶1:

```
leaf101# show ip route vrf shparanj:eigrp-test
IP Route Table for VRF "shparanj:eigrp-test"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

10.9.1.0/24, ubest/mbest: 1/0
    *via 10.27.48.2, eth1/22, [110/5], 00:01:50, ospf-default, intra
10.9.2.0/24, ubest/mbest: 1/0
    *via 10.0.248.0%overlay-1, [200/128576], 00:00:32, bgp-65003, internal, tag 65003
10.27.47.0/24, ubest/mbest: 1/0
    *via 10.0.248.0%overlay-1, [200/0], 01:54:45, bgp-65003, internal, tag 65003
```

```
10.27.48.0/24, ubest/mbest: 1/0, attached, direct
    *via 10.27.48.1, eth1/22, [1/0], 1d09h, direct
10.27.48.1/32, ubest/mbest: 1/0, attached
    *via 10.27.48.1, eth1/22, [1/0], 1d09h, local, local
172.16.1.0/24, ubest/mbest: 1/0, attached, direct, pervasive
    *via 10.0.240.34%overlay-1, [1/0], 1d09h, static
172.16.1.254/32, ubest/mbest: 1/0, attached, pervasive
    *via 172.16.1.254, vlan47, [1/0], 1d09h, local, local


leaf101# show zoning-rule scope 2752513
Rule ID         SrcEPG          DstEPG          FilterID        operSt          Scope
Action                              Priority
=======         ======          ======          ========        ======          =====
======                              ========
4173            0               0               implicit        enabled         2752513
deny,log                            any_any_any(21)
4174            0               0               implarp         enabled         2752513
permit                              any_any_filter(17)
4175            0               15              implicit        enabled         2752513
deny,log                            any_vrf_any_deny(22)
4207            0               32771           implicit        enabled         2752513
permit                              any_dest_any(16)

<<vsh>>

leaf101#  show system internal policy-mgr prefix | grep shparanj:eigrp-test
2752513 26     0x1a          Up     shparanj:eigrp-test
10.9.0.0/16  16387   False  True   False
2752513 26     0x1a          Up     shparanj:eigrp-test
0.0.0.0/0   15      False  True   False
2752513 26     0x8000001a    Up     shparanj:eigrp-test
::/0   15      False  True   False
```

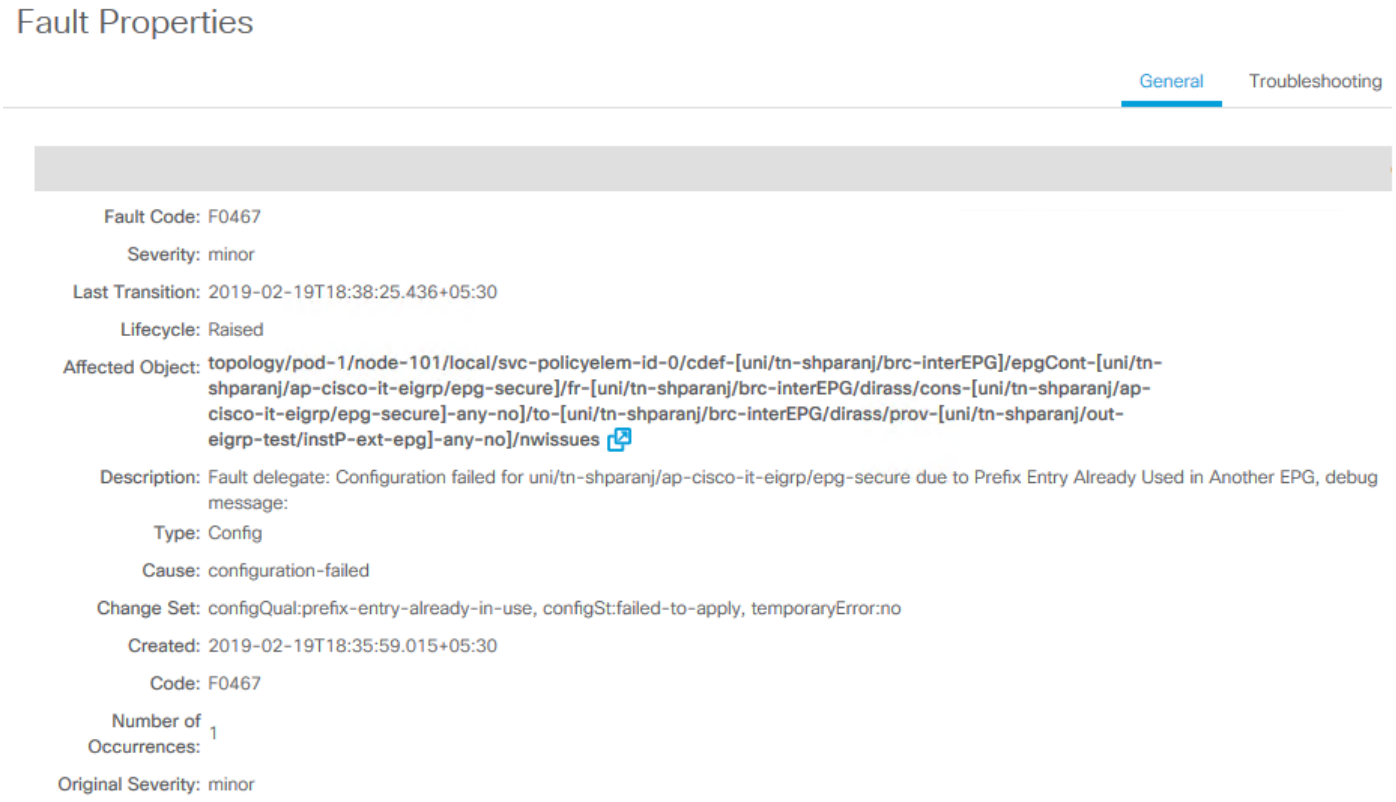
枝叶2:

```
leaf102# show ip route vrf shparanj:eigrp-test
IP Route Table for VRF "shparanj:eigrp-test"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

10.9.1.0/24, ubest/mbest: 1/0
    *via 10.0.0.64%overlay-1, [200/5], 00:05:29, bgp-65003, internal, tag 65003
10.9.2.0/24, ubest/mbest: 1/0
    *via 10.27.47.10, vlan80, [90/128576], 00:04:10, eigrp-default, internal
10.27.47.0/24, ubest/mbest: 1/0, attached, direct
    *via 10.27.47.2, vlan80, [1/0], 01:58:24, direct
10.27.47.2/32, ubest/mbest: 1/0, attached
    *via 10.27.47.2, vlan80, [1/0], 01:58:24, local, local
10.27.48.0/24, ubest/mbest: 1/0
    *via 10.0.0.64%overlay-1, [200/0], 1d09h, bgp-65003, internal, tag 65003

leaf102# show zoning-rule scope 2752513
Rule ID         SrcEPG          DstEPG          FilterID        operSt          Scope
Action                              Priority
=======         ======          ======          ========        ======          =====
======                              ========
4472            0               0               implicit        enabled         2752513
deny,log                            any_any_any(21)
4471            0               0               implarp         enabled         2752513
```

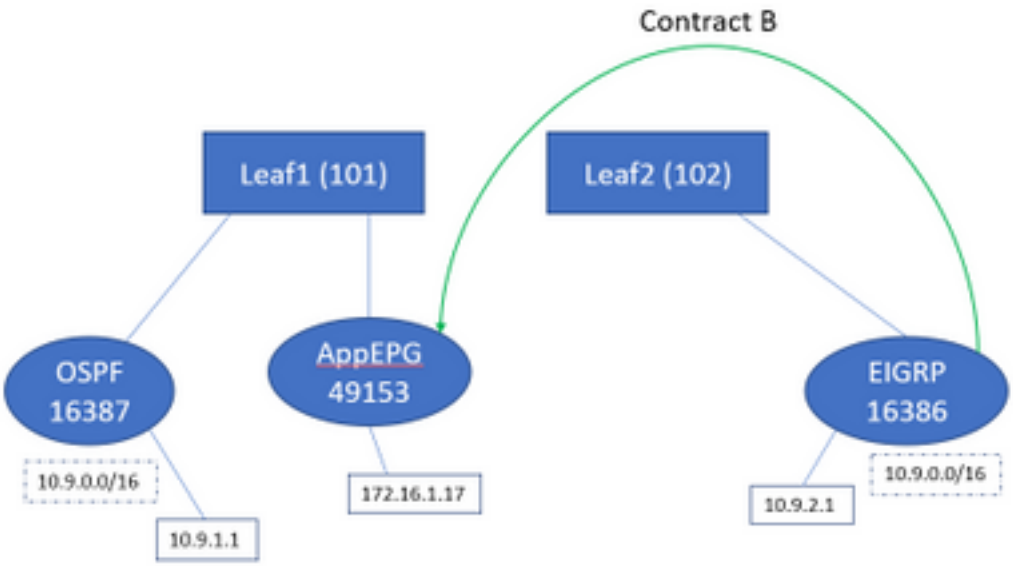
```
permit                                  any_any_filter(17)
4470            0               15              implicit        enabled         2752513
deny,log                                any_vrf_any_deny(22)

<<vsh>>

leaf102# show system internal policy-mgr prefix | grep shparanj:eigrp-test
2752513 37      0x80000025      Up      shparanj:eigrp-test
::/0    15      False   True    False
2752513 37      0x25            Up      shparanj:eigrp-test
0.0.0.0/0    15       False   True    False
2752513 37      0x25            Up      shparanj:eigrp-test
10.9.0.0/16   16386    False   True    False
```

在此状态下，如果没有任何合同，我们将看到两个EPG上都没有故障。尚未检测到前缀重叠！

如果添加合同B，我们会在应用EPG中看到故障（会消耗合同B）。



拓扑：



让我们看看表中的变化：

```
leaf101# show zoning-rule scope 2752513
Rule ID         SrcEPG          DstEPG          FilterID        operSt          Scope
Action                              Priority
=======         ======          ======          ========        ======          =====
======                              ========
4173            0               0               implicit        enabled         2752513
deny,log                            any_any_any(21)
4174            0               0               implarp         enabled         2752513
permit                              any_any_filter(17)
4175            0               15              implicit        enabled         2752513
deny,log                            any_vrf_any_deny(22)
4207            0               32771           implicit        enabled         2752513
permit                              any_dest_any(16)
4605 49153 16386 default enabled 2752513 permit src_dst_any(9) 4604 16386 49153 default enabled
2752513 permit src_dst_any(9) <<vsh>> leaf101# show system internal policy-mgr prefix | grep
shparanj:eigrp-test 2752513 26 0x1a Up shparanj:eigrp-test 10.9.0.0/16 16387 False True False
2752513 26 0x1a Up shparanj:eigrp-test 0.0.0.0/0 15 False True False 2752513 26 0x8000001a Up
shparanj:eigrp-test ::/0 15 False True False
```

枝叶2保持不变。

这显示已安装与合同B对应的分区规则。但是，前缀无法添加，因为它已存在 — 根据OSPF EPG标记！

而这正是故障警告我们的“已在另一个EPG中使用的前缀条目” — 只有当策略（分区规则）和其应用之间的特定枝叶发生冲突时，才会出现故障。在消费者EPG上发生故障。

如果我们从10.9.2.1开始流量，则由于策略拒绝，它在枝叶101上被丢弃：

```
# show logging ip access-list internal packet-log deny

[ Tue Feb 19 19:31:33 2019 234270 usecs]: CName: shparanj:eigrp-test(VXLAN: 2752513), VlanType:
FD_VLAN, Vlan-Id: 48, SMac: 0xdccec15b1e47, DMac:0x0022bdf819ff, SIP: 172.16.1.17, DIP:
10.9.2.1, SPort: 0, DPort: 0, Src Intf: Ethernet1/24, Proto: 1, PktLen: 98 [ Tue Feb 19 19:31:31
2019 234310 usecs]: CName: shparanj:eigrp-test(VXLAN: 2752513), VlanType: FD_VLAN, Vlan-Id: 48,
SMac: 0xdccec15b1e47, DMac:0x0022bdf819ff, SIP: 172.16.1.17, DIP: 10.9.2.1, SPort: 0, DPort: 0,
```

```
Src Intf: Ethernet1/24, Proto: 1, PktLen: 98
```

我们看到EP 172.16.1.17到10.9.2.1的应答被丢弃。这是因为：

- 来自10.9.2.1的从交换矩阵传入的请求已分类为16386类 — 这些请求符合规则ID 4604，允许通过
- 来自172.16.1.17的应答标记为dclass 16387 — 这根据policy-mgr前缀规则进行选择。没有与16387对应的规则，这些规则将被拒绝。

在这种情况下，分类错误会导致流量被丢弃，即使我们似乎有正确的配置（如果忽略故障）。

具有0.0.0.0/0前缀的交换矩阵在多个外部EPG上声明为外部

在此场景中，我们将0.0.0.0/0子网作为外部EPG应用于不同外部EPG，因此可能会出现分类错误和意外安全违规。

OSPF通告网络：

10.7.7.0/24

EIGRP通告网络：

10.8.8.0/24

我们从图1中的拓扑开始，但没有任何合同。我们将子网0.0.0.0/0定义为两个L3outs上EPG的“外部EPG的外部子网”。

以下是Leaf1和2上的表：

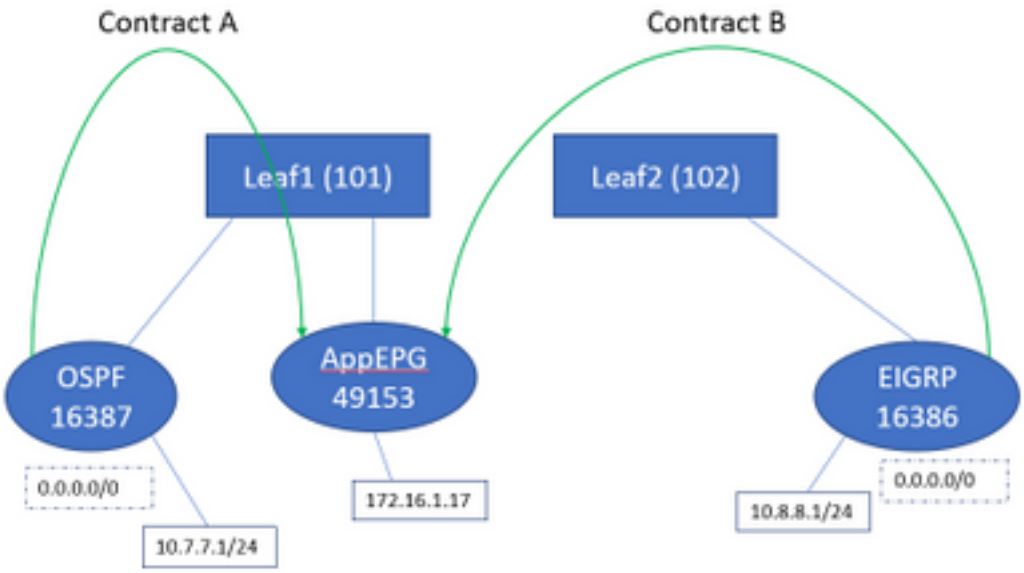
枝叶1:

```
leaf101# show zoning-rule scope 2752513
Rule ID         SrcEPG          DstEPG          FilterID        operSt          Scope
Action                              Priority
=======         ======          ======          ========        ======          =====
======                              ========
4173            0               0               implicit        enabled         2752513
deny,log                            any_any_any(21)
4174            0               0               implarp         enabled         2752513
permit                              any_any_filter(17)
4175            0               15              implicit        enabled         2752513
deny,log                            any_vrf_any_deny(22)
4207            0               32771           implicit        enabled         2752513
permit                              any_dest_any(16)

leaf101# show ip route vrf shparanj:eigrp-test
IP Route Table for VRF "shparanj:eigrp-test"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

10.7.7.0/24, ubest/mbest: 1/0
    *via 10.27.48.2, eth1/22, [110/5], 00:23:29, ospf-default, intra
10.8.8.0/24, ubest/mbest: 1/0
    *via 10.0.248.0%overlay-1, [200/128576], 00:02:30, bgp-65003, internal, tag 65003
10.27.47.0/24, ubest/mbest: 1/0
```

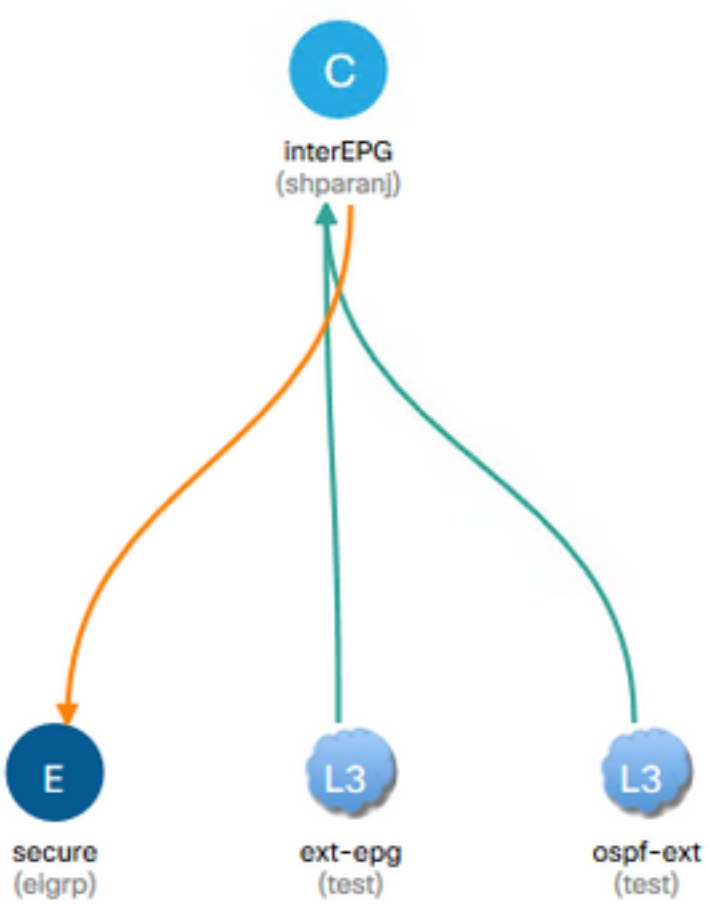
```
    *via 10.0.248.0%overlay-1, [200/0], 00:02:33, bgp-65003, internal, tag 65003
10.27.48.0/24, ubest/mbest: 1/0, attached, direct
    *via 10.27.48.1, eth1/22, [1/0], 1d07h, direct
10.27.48.1/32, ubest/mbest: 1/0, attached
    *via 10.27.48.1, eth1/22, [1/0], 1d07h, local, local
172.16.1.0/24, ubest/mbest: 1/0, attached, direct, pervasive
    *via 10.0.240.34%overlay-1, [1/0], 1d07h, static
172.16.1.254/32, ubest/mbest: 1/0, attached, pervasive
    *via 172.16.1.254, vlan47, [1/0], 1d07h, local, local


<<vsh>>

leaf101# show system internal policy-mgr prefix | grep shparanj:eigrp-test
2752513 26     0x1a          Up     shparanj:eigrp-test
0.0.0.0/0   15      False  True   False
2752513 26     0x8000001a    Up     shparanj:eigrp-test
::/0   15      False  True   False
```

枝叶2:

```
leaf102# show ip route vrf shparanj:eigrp-test
IP Route Table for VRF "shparanj:eigrp-test"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

10.7.7.0/24, ubest/mbest: 1/0
    *via 10.0.0.64%overlay-1, [200/5], 00:26:07, bgp-65003, internal, tag 65003
10.8.8.0/24, ubest/mbest: 1/0
    *via 10.27.47.10, vlan80, [90/128576], 00:05:08, eigrp-default, internal
10.27.47.0/24, ubest/mbest: 1/0, attached, direct
    *via 10.27.47.2, vlan80, [1/0], 00:05:11, direct
10.27.47.2/32, ubest/mbest: 1/0, attached
    *via 10.27.47.2, vlan80, [1/0], 00:05:11, local, local
10.27.48.0/24, ubest/mbest: 1/0
    *via 10.0.0.64%overlay-1, [200/0], 1d07h, bgp-65003, internal, tag 65003


leaf102#  show zoning-rule scope 2752513
Rule ID         SrcEPG          DstEPG          FilterID        operSt          Scope
Action                              Priority
=======         ======          ======          ========        ======          =====
======                              ========
4472            0               0               implicit        enabled         2752513
deny,log                            any_any_any(21)
4471            0               0               implarp         enabled         2752513
permit                              any_any_filter(17)
4470            0               15              implicit        enabled         2752513
deny,log                            any_vrf_any_deny(22)

<<vsh>>

leaf102# show system internal policy-mgr prefix | grep shparanj:eigrp-test
2752513 37     0x80000025    Up     shparanj:eigrp-test
::/0   15      False  True   False
2752513 37     0x25          Up     shparanj:eigrp-test
0.0.0.0/0   15      False  True   False
```



如果同时添加A和B合同，我们仍未发现任何故障。



让我们看看枝叶上的表格：

枝叶1:

```
leaf101# show zoning-rule scope 2752513
Rule ID         SrcEPG          DstEPG          FilterID        operSt          Scope
Action                              Priority
=======         ======          ======          ========        ======          =====
======                              ========
4173            0               0               implicit        enabled         2752513
deny,log                            any_any_any(21)
4174            0               0               implarp         enabled         2752513
permit                              any_any_filter(17)
4175            0               15              implicit        enabled         2752513
deny,log                            any_vrf_any_deny(22)
4207            0               32771           implicit        enabled         2752513
permit                              any_dest_any(16)
4616            49153           15              default         enabled         2752513
permit                              src_dst_any(9)
4617            32770           49153           default         enabled         2752513
permit                              src_dst_any(9)

<<vsh>>
leaf101# show system internal policy-mgr prefix | grep shparanj:eigrp-test 2752513 26 0x1a Up
shparanj:eigrp-test 0.0.0.0/0 15 False True False 2752513 26 0x8000001a Up shparanj:eigrp-test
::/0 15 False True False
```

Leaf2上的表保持不变。

我们看不到任何故障，因为实际上从每个枝叶的角度来看，没有策略冲突。将0.0.0.0/0用作外部EPG时添加的规则ID是特殊的。

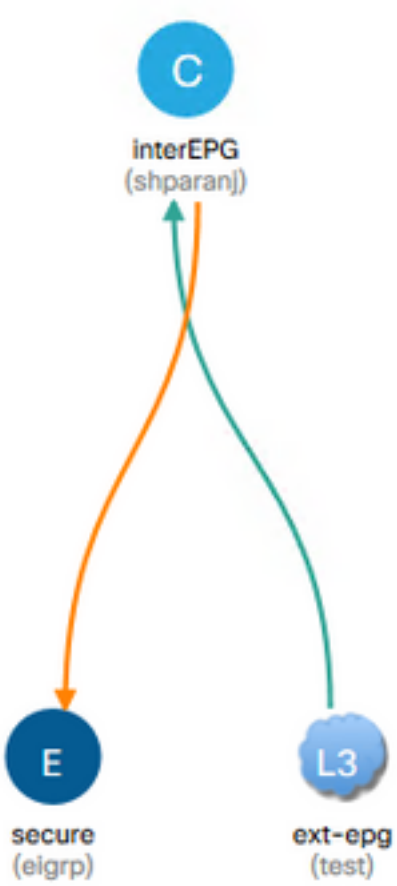
- **从各自的EPG进入任一边界枝叶的流量标有sclass 32770 — 这是VRF的pcTag。**
- 此流量上的dclass为49153 — 应用EPG的pcTag。
- **来自应用EPG的返回流量的类为15**

枝叶1上的ELAM:

```
module-1(DBG-elam)# trigger init in-select 6 out-select 0
module-1(DBG-elam-insel6)# set outer ipv4 src_ip 10.7.7.1
module-1(DBG-elam-insel6)# start
module-1(DBG-elam-insel6)# stat
ELAM STATUS
===========
Asic 0 Slice 0 Status Armed
Asic 0 Slice 1 Status Triggered

module-1(DBG-elam-insel6)# report | grep sclass
      sug_lurw_vec.info.nsh_special.sclass: 0x8002
      sug_lurw_vec.info.ifabric_spine.sclass: 0x8002
      sug_lurw_vec.info.ifabric_leaf.sclass: 0x8002
module-1(DBG-elam-insel6)# dec 0x8002
32770

module-1(DBG-elam-insel6)# reset
module-1(DBG-elam-insel6)# set outer ipv4 dst_ip 10.7.7.1
module-1(DBG-elam-insel6)# start
module-1(DBG-elam-insel6)# stat
ELAM STATUS
===========
Asic 0 Slice 0 Status Armed
Asic 0 Slice 1 Status Armed

module-1(DBG-elam-insel6)# stat
ELAM STATUS
```

```
===========
Asic 0 Slice 0 Status Armed
Asic 0 Slice 1 Status Triggered

module-1(DBG-elam-insel6)# report | grep dclass
      sug_lurw_vec.info.nsh_special.dclass: 0xF
      sug_lurw_vec.info.ifabric_leaf.dclass: 0xF
```

即使我们删除合同A，10.7.7.1也可以继续与172.16.1.17通信。



这是因为删除合同A不会导致对Leaf1上的分区规则进行任何更改。

```
leaf101# show system internal policy-mgr prefix | grep shparanj:eigrp-test
2752513 26     0x1a          Up     shparanj:eigrp-test
0.0.0.0/0   15      False  True   False
2752513 26     0x8000001a    Up     shparanj:eigrp-test
::/0   15      False  True   False
leaf101# exit
leaf101# show zoning-rule scope 2752513
Rule ID         SrcEPG          DstEPG          FilterID        operSt          Scope
Action                              Priority
=======         ======          ======          ========        ======          =====
======                              ========
4173            0               0               implicit        enabled         2752513
deny,log                            any_any_any(21)
4174            0               0               implarp         enabled         2752513
permit                              any_any_filter(17)
4175            0               15              implicit        enabled         2752513
```

```
deny,log                        any_vrf_any_deny(22)
4207            0               32771           implicit        enabled         2752513
permit                          any_dest_any(16)
4616            49153           15              default         enabled         2752513
permit                          src_dst_any(9)
4617            32770           49153           default         enabled         2752513
permit                          src_dst_any(9)
```

此外，OSPF外部EPG上传入的流量继续使用VRF pcTag进行标记，因为EPG仍将0.0.0.0/0标记为外部子网。

这会导致违反安全策略，即两个EPG能够在强制VRF中无合同地通信。

进一步阅读

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/ACI_Best_Practices/b_ACI_Best_Practices/b_ACI_Best_Practices_chapter_010010.html