思科ACI中L3outs上的重疊子網

目錄

簡介

思科以應用為中心的基礎設施(ACI)通過L3outs（第3層出站）促進內部租戶和外部路由網路之間的通訊。 也可以將這樣的L3outs配置為具有一個或多個終端組(EPG)。 為了讓ACI知道如何對傳入流量進行分類，作為L3out的EPG，需要定義顯式子網，同時啟用某些標誌。本文旨在對基於合約策略應用中L3out EPG的硬體實現進行一些說明。我們將專門探討「外部EPG的外部子網」的標籤，以及在單獨的EPG上宣佈重疊字首為「外部」的意外後果。

概念

經驗法則是：部署L3outs時，同一虛擬路由和轉發(VRF)例項中的不同EPG不應具有標籤為「外部EPG的外部子網」的重疊子網。這也意味著源自特定子網的流量不應通過不同的EPG進入。這可能會造成流量根據針對不相關的EPG宣告的子網的最長字首匹配進行意外分類。讓我們看幾個場景來詳細瞭解這一點

必要條件

對ACI的基本瞭解：L3outs、合約和策略實施。下面簡要介紹一些有用的術語，有關這些術語的更多詳細資訊不在本檔案的範圍之內：

pcTag:ACI將流量分類為pcTags，這些是EPG的內部表示形式。預設情況下，這些值具有VRF範圍 — 即，它們在VRF中是唯一的，但可以在VRF中重複使用。但是，如果一個EPG與不同VRF/租戶中的另一個EPG存在合約，則pcTag值具有全域性範圍 — 即，您將找不到具有相同pcTag的ACI中的任何其他EPG。

ELAM:嵌入式邏輯分析器模組。此工具用於根據過濾器在ASIC上捕獲一個資料包，並檢查資料包上設定的報頭/標誌。此工具還有助於理解基於硬體的查詢/邏輯

sclass/dclass:當流量進入枝葉時，根據策略實施方向和本地可用的字首知識，枝葉會將源流量和目標流量標籤到EPG中 — 在ELAM捕獲中，將分別視為sclass和dclass

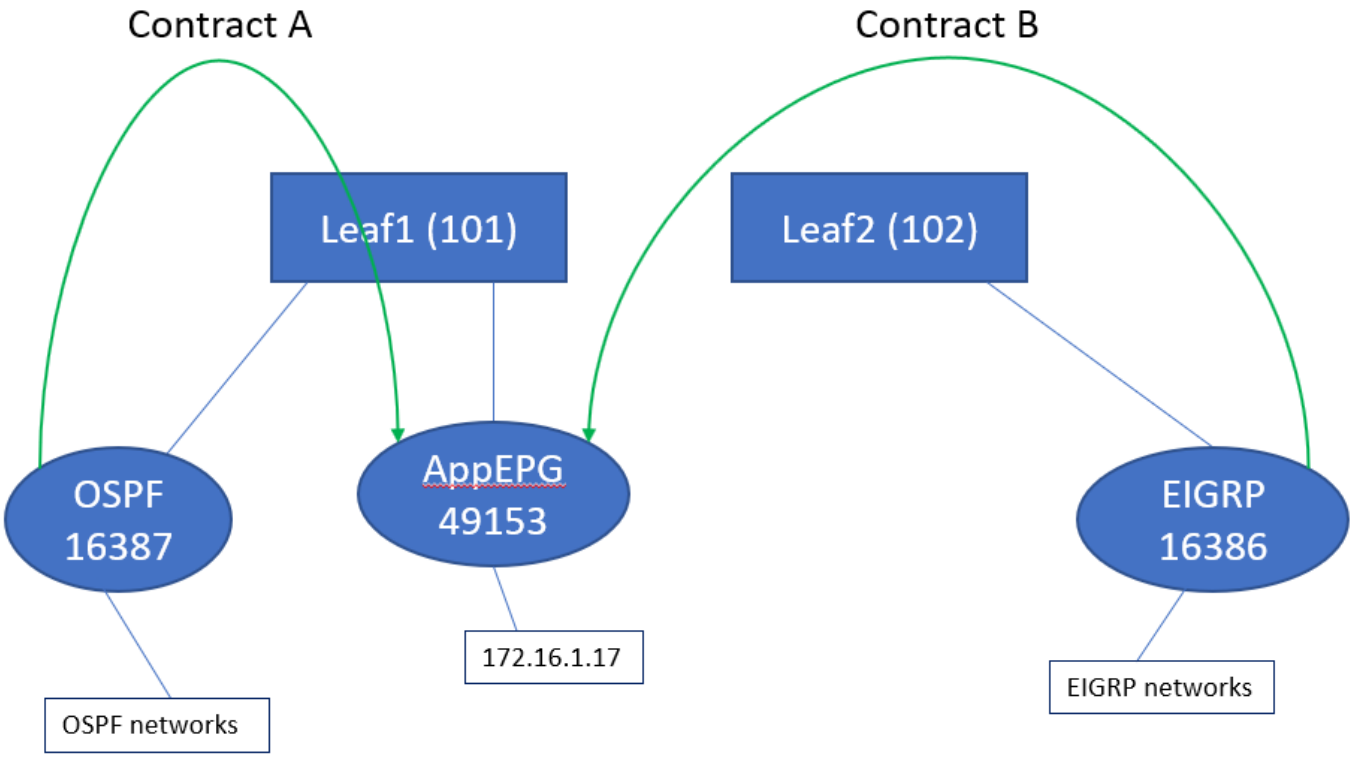
zoning-rule：這些是合約的內部表示形式，類似於ACL的行。SrcEpg和DstEpg值應與sclass/dclass匹配，以便流量達到給定規則並被允許。預設情況下，在強制的vrf中，最後一行有一

個隱式deny，因此與特定規則不匹配的任何流量都會遇到隱式deny並被丟棄。

設定和拓撲

兩個枝葉 — 101和102，型號：N9K-C93180YC-EX

- 版本3.2(4e)
- 使用了一個VRF - 策略實施首選項：已實施策略實施方向：Ingress。VRF VNID（VxLAN網路識別符號）：2752513;pcTag: 32770
- Leaf1中的L3out(101)- 通訊協定:開放最短路徑優先(OSPF)適用於鄰居的L3介面使用者 — eth1/22(10.27.48.1/24)外部EPG pcTag:16387
- EPG在Leaf101上的應用 中繼 — eth1/24 pcTag:49153IP端點：172.16.1.17 網關：172.16.1.254/24 — 部署在Bridge Domain(BD)上 BD有pcTag標32771
- Leaf2上的L3out(202)- 通訊協定:增強型內部閘道路由通訊協定(EIGRP)SVI用於路徑1/16的鄰居關係 — vlan 2747(10.27.47.1/24)外部EPG pcTag:163869



案例

來自重疊子網的流量

在此場景中，我們將研究當流量源自重疊子網時（從ACI的角度來看）可能出現的錯誤分類

OSPF通告：

10.9.9.6/32

EIGRP通告：

10.9.9.1/32

我們從圖1中的拓撲開始，但沒有合約。對於OSPF上的EPG，我們將子網0.0.0.0/0定義為「外部EPG的外部子網」，並使用相同的EIGRP標誌將子網10.9.9.0/24定義為「外部EPG的外部子網」。Leaf1和2上的表如下所示：

Leaf1:

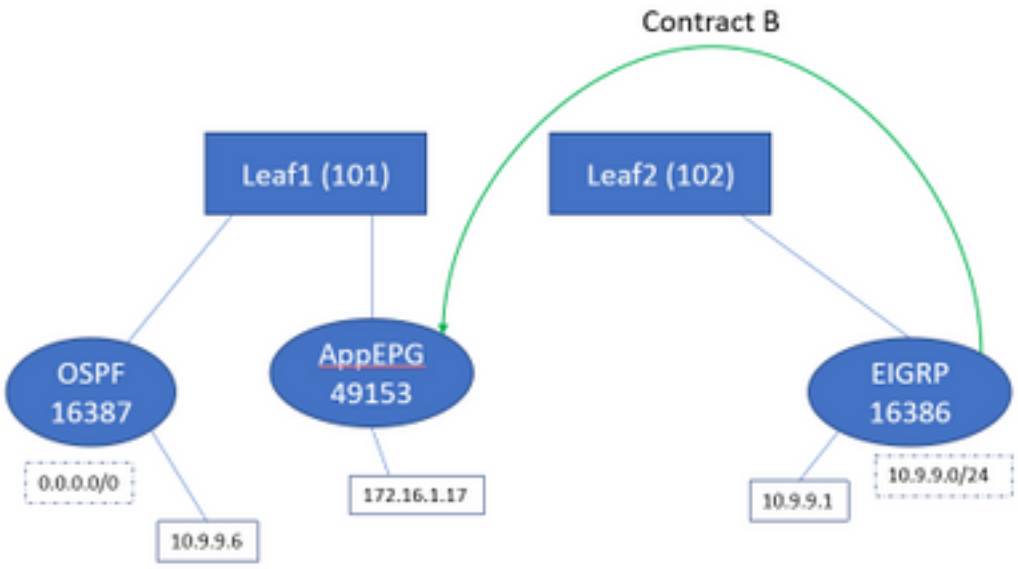
```
leaf101# show end int eth1/24
Legend:
 s - arp              H - vtep             V - vpc-attached     p - peer-aged
 R - peer-attached-rl B - bounce           S - static           M - span
 D - bounce-to-proxy  O - peer-attached    a - local-aged       L - local
+------------------------------------+--------------+-----------------+--------------+----------
---+
      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
```

枝葉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
```

讓我們新增合約B（租戶中的合約，範圍vrf — 檔案管理器：common:default）



新增合約B — 我們看到在leaf1上新增了eigrp EPG字首：

```
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
```

讓我們看看其他策略：

枝葉1合約：

```
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)
```

枝葉2合約（保持不變）：

```
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)
```

在此場景中，來自ospf l3out的流量進入，我們希望標籤該流量 16387改為使用16386標籤。這是因為流量會命中Leaf1上的新首碼專案。

從10.9.9.6對端點172.16.1.17執行ping:

```
# 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
```

即使沒有ospf epg和app-epg之間的合約，Ping也會工作。這是因為 Ping會與eigrp-epg的策略相衝

突並被允許。

ELAM:

```
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
```

在此案例中，由於分類到與目標目的地具有合約的pcTag中，流量最終會正常工作。但是，例如，如果計算枝葉是獨立的第三枝葉，則我們的流量將失敗，因為合約條目將只存在於第三枝葉（入口策略）或枝葉102（出口策略）上。

在獨立的外部EPG上宣告為外部的子網重疊的交換矩陣

在此場景中，我們將檢視策略衝突和由於不同外部EPG上被宣告為外部的子網重疊或相同而導致的錯誤分類。

OSPF通告網路：

10.9.1.0/24

EIGRP通告網路：

10.9.2.0/24

我們從圖1中的拓撲開始，但沒有合約。我們為兩個L3outs上的EPG定義子網10.9.0.0/16 as 「外部EPG的外部子網」。

Leaf1和2上的表如下所示：

枝葉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
```

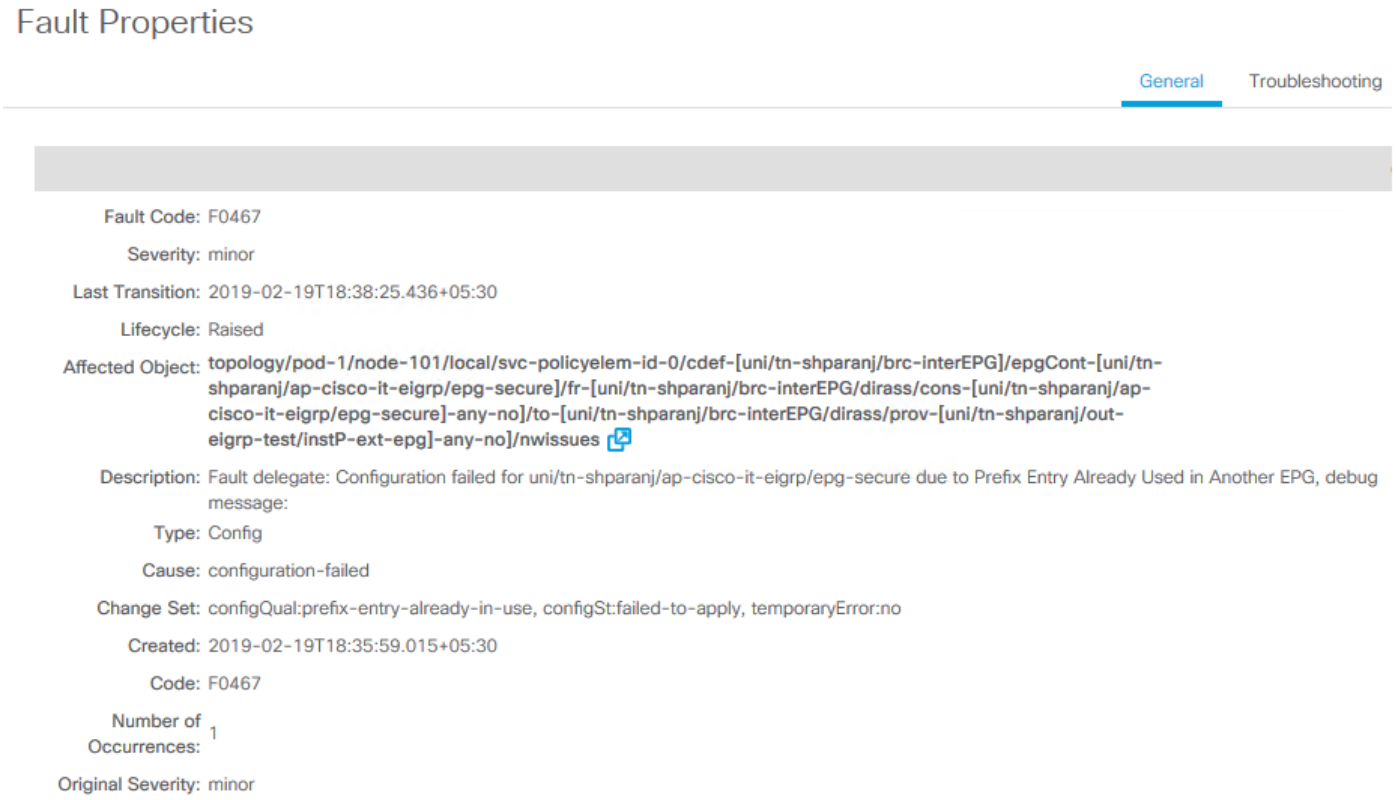
枝葉2:

```
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
```

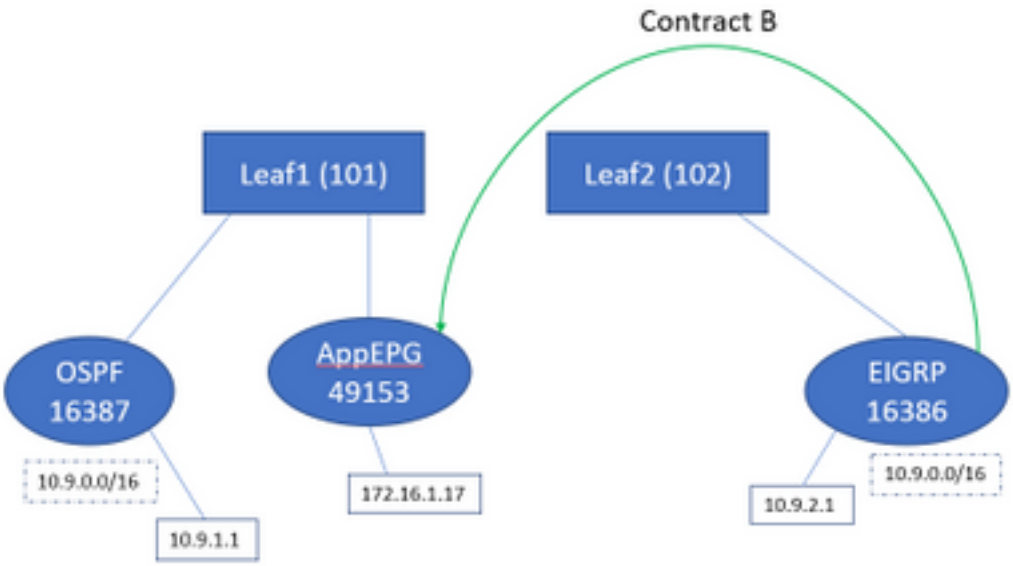
```
permit                                  any_any_filter(17)
4470            0               15              implicit        enabled         2752513
deny,log                                any_vrf_any_deny(22)

<<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
```

在這種狀態下，沒有任何合約，我們看不出任何一個EPG存在缺陷。尚未檢測到字首中的重疊！

如果新增合約B，則會在app-EPG（它使用合約B）中看到錯誤。



拓撲：



讓我們看一下表中的變化：

```
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
```

Leaf2保持不變。

這顯示已安裝與合約B對應的分割槽規則。但是不能新增字首，因為它已經存在 — 根據OSPF EPG進行標籤！

而這正是該故障警告我們的「已在另一個EPG中使用的字首條目」 — 僅當策略（分割槽規則）及其應用之間的特定枝葉上存在衝突時才引發該故障。消費者EPG上發生故障。

如果我們從10.9.2.1啟動流量，由於策略拒絕，該流量在Leaf101上被丟棄：

```
# 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
```
我們看到從EP 172.16.1.17到10.9.2.1的回覆被丟棄。這是因為：

- 來自交換矩陣的10.9.2.1請求已分類為16386類 — 這些請求到達規則ID 4604並允許通過
- 來自172.16.1.17的回覆標有dclass 16387 — 這是根據policy-mgr字首規則選取的。沒有對應於16387的規則，這些被拒絕。

在這種情況下，誤分類會導致流量被丟棄，即使我們似乎有正確的配置（如果忽略故障）。

在多個外部EPG上將字首為0.0.0.0/0的交換矩陣宣告為外部

在此場景中，我們將檢視由於將0.0.0.0/0子網作為外部子網應用於不同的外部EPG而可能出現的錯誤分類和意外安全違規。

OSPF通告網路：

10.7.7.0/24

EIGRP通告網路：

10.8.8.0/24

我們從圖1中的拓撲開始，但沒有合約。我們將子網0.0.0.0/0定義為「外部EPG的外部子網」，用於L3出站上的EPG。

Leaf1和2上的表如下所示：

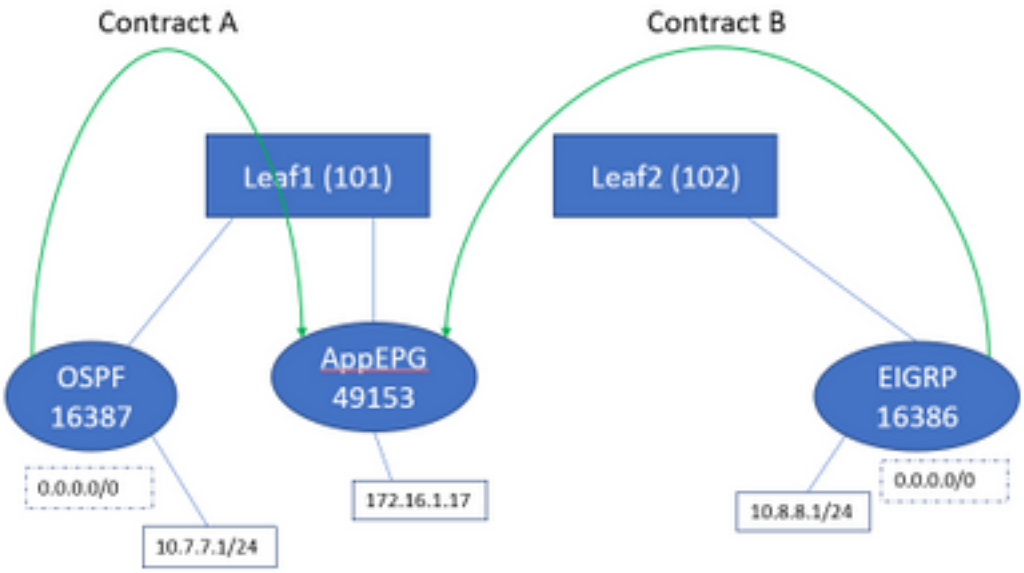
Leaf1:

```
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
```

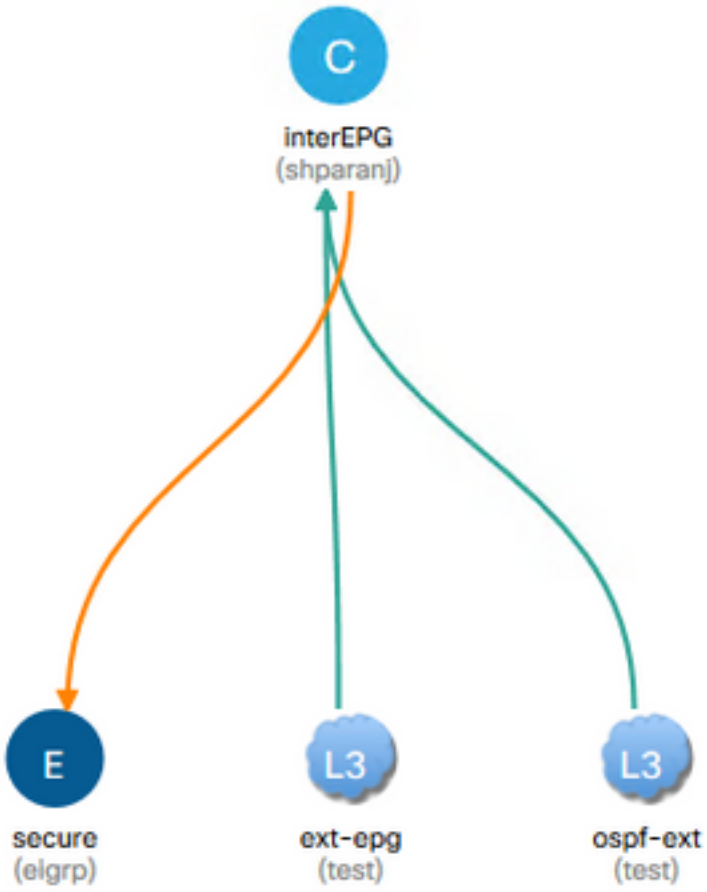
```
    *via 10.27.48.1, eth1/22, [1/0], 1d07h, direct
10.27.48.1/32, ubest/mbest: 1/0, attached
    *via 10.27.48.1, eth1/22, [1/0], 1d07h, local, local
172.16.1.0/24, ubest/mbest: 1/0, attached, direct, pervasive
    *via 10.0.240.34%overlay-1, [1/0], 1d07h, static
172.16.1.254/32, ubest/mbest: 1/0, 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
```

枝葉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
```



如果同時新增合約A和B，我們仍然看不到任何錯誤。



讓我們看看傳單上的桌子：

Leaf1:

```
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上的表保持不變。

我們沒有發現任何缺陷，因為從每個枝葉的角度來看，實際上不存在政策衝突。**將0.0.0.0/0用作外部EPG時新增的規則ID是特殊的。**

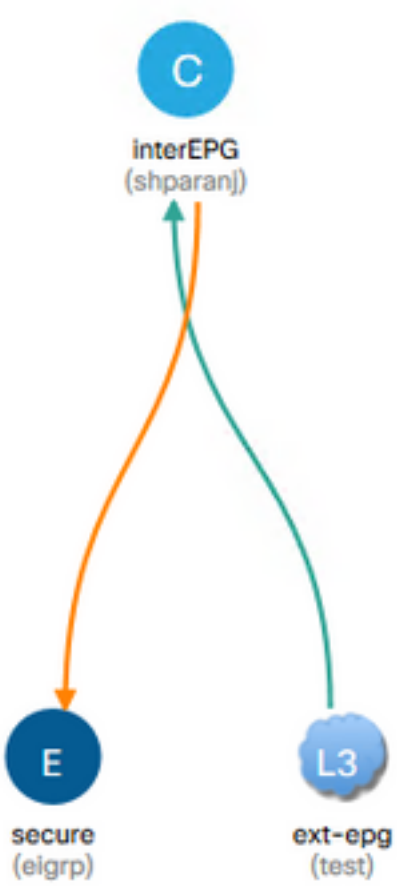
- **從各自的EPG進入任一邊界枝葉的流量標有32770類 — 這是VRF的pcTag。**
- 此流量上的dclass為49153 - app-EPG的pcTag。
- **來自app-EPG的返回流量類別為15**

Leaf1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
```

即使刪除合約A，10.7.7.1仍可以繼續與172.16.1.17通訊。



這是因為刪除合約A不會導致Leaf1上的分割槽規則發生任何更改。

```
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，進入OSPF外部EPG的流量繼續使用VRF pcTag進行標籤，因為EPG仍將0.0.0.0/0標籤為外部子網。

這會導致違反安全策略，即兩個EPG在強制VRF中無需合約即可通訊。

進一步閱讀

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