Superposición de subredes en L3outs en Cisco ACI

Contenido

Introducción

Cisco Application Centric Infrastructure (ACI) facilita la comunicación entre arrendatarios internos y redes enrutadas externas mediante L3outs (capa 3 saliente). Estos L3outs también se pueden configurar para tener uno o más grupos de punto final (EPG). Para que ACI sepa cómo clasificar el tráfico entrante, como EPG de L3out, es necesario definir subredes explícitas con ciertos indicadores habilitados. Este artículo pretende arrojar luz sobre la implementación de hardware de los EPG L3out en el contexto de la aplicación de políticas basadas en contratos. Exploraremos específicamente el indicador 'subredes externas para EPG externos' y las consecuencias inesperadas de declarar prefijos superpuestos como 'externos' en EPG separados.

Concepto

La regla general es: al implementar L3outs, los EPG separados en la misma instancia de Virtual Routing and Forwarding (VRF) no deben tener subredes superpuestas marcadas como 'subred externa para EPG externos'. Esto también significa que el tráfico originado en una subred específica no debe entrar a través de diferentes EPG. Esto puede provocar una clasificación inesperada del tráfico basada en la coincidencia de prefijos más largos frente a las subredes declaradas frente a EPG no relacionados. Veamos algunos escenarios para entender esto en detalle

Prerequisites

Comprensión básica de ACI: L3outs, contratos y aplicación de políticas. A continuación se explican brevemente algunos términos útiles, y la información más detallada al respecto está por debajo del alcance de este documento:

pcTag: ACI clasifica el tráfico en etiquetas de pc y éstas son representaciones internas de los EPG. Estos valores, de forma predeterminada, tienen un alcance de VRF; es decir, son únicos dentro de un VRF, pero se pueden reutilizar entre los VRF. Sin embargo, si un EPG tiene un contrato con otro EPG en un VRF/Arrendatario diferente , el valor pcTag tiene un alcance global;

es decir, no encontrará ningún otro EPG en ACI con la misma pcTag.

ELAM: Módulo de análisis lógico integrado. Esta herramienta se utiliza para capturar un paquete en ASIC basado en filtros y para verificar los encabezados/indicadores configurados en el paquete. Esta herramienta también ayuda a comprender las búsquedas y la lógica realizadas por hardware

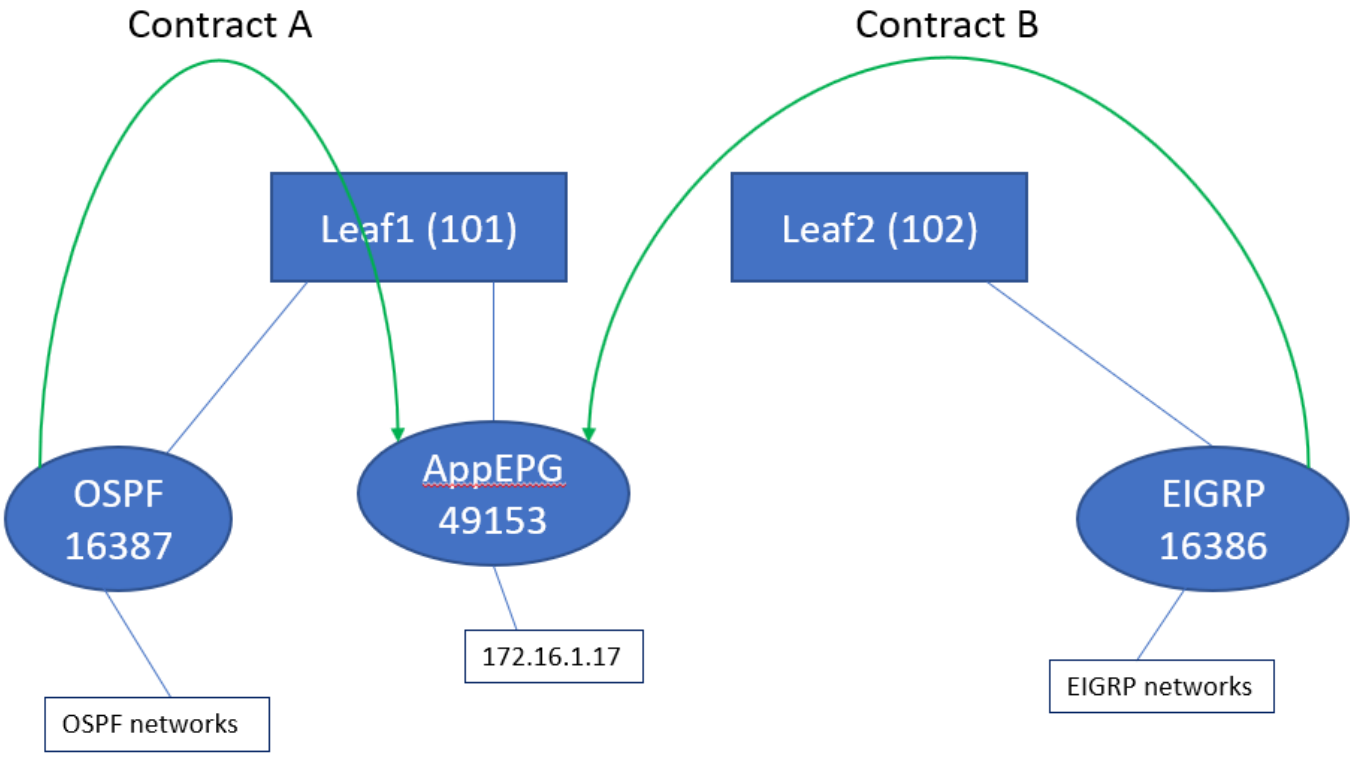
sclass/dclass: cuando el tráfico llega a una hoja, en función de la dirección de la aplicación de políticas y el conocimiento de prefijo disponible localmente, la hoja marcará el tráfico de origen y de destino en los EPG; en las capturas de ELAM esto se verá como clase y clase respectivamente

zoning-rule: Éstas son representaciones internas de contratos y son similares a líneas de una ACL. Los valores SrcEpg y DstEpg deben coincidir con sclass/dclass para que el tráfico llegue a una regla determinada y se permita. De forma predeterminada, en un vrf forzado hay una negación implícita como la última línea , por lo que cualquier tráfico que no coincida con una regla determinada llegará a la negación implícita y se descartará.

Configuración y topología

Dos hojas - 101 y 102 , modelo: N9K-C93180YC-EX

- Versión 3.2(4e)
- Un VRF utilizado: Preferencia de aplicación de políticas: AplicadoDirección de aplicación de políticas: Acceso.VRF VNID(Identificador de red VxLAN): 2752513 ; pcTag: 32770
- L3out en hoja1 (101) - Protocolo: Abrir primero la ruta más corta (OSPF)Usuario de interfaz L3 para la vecindad: eth1/22 (10.27.48.1/24)PcTag EPG externo: 16387
- EPG de la aplicación en Leaf101 Troncal - eth1/24 pcTag: 49153Punto final IP: 172.16.1.17 Gateway: 172.16.1.254/24 - implementado en Bridge Domain (BD) BD tiene pcTag 32771
- L3out en hoja 2 (2002) - Protocolo: Protocolo de routing de gateway interior mejorado (EIGRP)SVI utilizado para la vecindad con Path 1/16 - vlan 2747 (10.27.47.1/24)PcTag EPG externo: 163869



Escenarios

Tráfico originado por subredes superpuestas

En este escenario, analizamos la clasificación errónea potencial cuando el tráfico se origina a partir de subredes superpuestas (desde la perspectiva de ACI)

OSPF anuncia:

10.9.9.6/32

EIGRP anuncia:

10.9.9.1/32

Comenzamos con la topología del Diagrama 1, pero sin contratos. Para EPG en OSPF, definimos la subred 0.0.0.0/0 como 'subred externa para EPG externos' y 10.9.9.0/24 con el mismo indicador para EPG de EIGRP. Así son las mesas de Leaf1 y 2:

Hoja1:

```
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
```

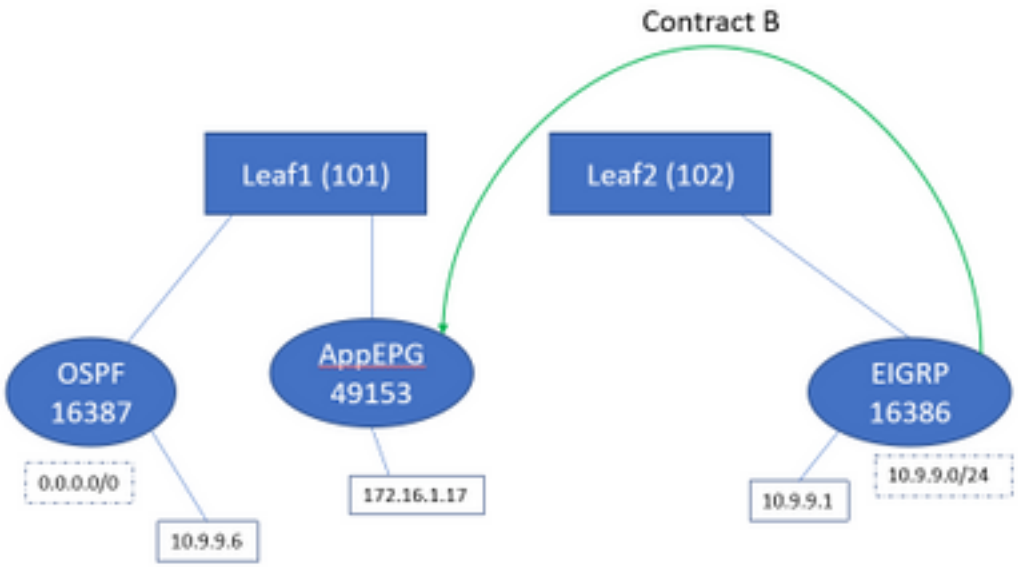
```
      Domain                            VLAN            IP Address        IP Info
+-----------------------------------+--------------+-----------------+--------------+----------
---+
48                                      vlan-2743    dcce.c15b.1e47 L
eth1/24
shparanj:eigrp-test                     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
```

Hoja2:

```
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
```

Vamos a agregar el contrato B (contrato en arrendatario , ámbito vrf - filtro: común:predeterminado)



Tan pronto como agregamos el contrato B - vemos el prefijo EPG eigrp agregado en la hoja1:

```
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
```

Veamos otras políticas:

Contratos de la hoja 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)
4604 49153 16386 default enabled 2752513 permit src_dst_any(9) 4605 16386 49153 default enabled
2752513 permit src_dst_any(9)
```

Contratos de la hoja 2 (no se han modificado):

```
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)
```

En este escenario, el tráfico que llega de ospf l3out , con el que esperamos ser etiquetados 16387 se etiqueta con 16386 en su lugar. Esto se debe a que el tráfico llega a la nueva entrada de prefijo en Leaf1.

Ping desde 10.9.9.6 al punto final 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
```

Ping funciona incluso sin un contrato entre ospf epg y app-epg. Esto se debe a que se opone a la política para eigrp-epg y se permite.

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
```

En esta situación, el tráfico termina funcionando debido a la clasificación en una pcTag que tiene un contrato con el destino previsto. Sin embargo, si, por ejemplo, la hoja de cálculo era una tercera hoja separada, entonces nuestro tráfico fallaría - ya que la entrada para el contrato sólo existiría en la tercera hoja (política de ingreso) o en la hoja102 (política de egreso).

Fabric con subredes superpuestas declaradas como externas en EPG externos independientes

En este escenario, analizamos el conflicto de políticas y la potencial mala clasificación debido a la superposición o a las mismas subredes declaradas como externas en diferentes EPG externos.

OSPF anuncia la red:

10.9.1.0/24

EIGRP anuncia la red:

10.9.2.0/24

Comenzamos con la topología del Diagrama 1, pero sin contratos. Definimos la subred 10.9.0.0/16 as 'subred externa para EPG externos' para EPG en ambos L3outs.

Así son las mesas de Leaf1 y 2:

Hoja 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
```

Hoja2:

```
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
```

En este estado, sin ningún contrato, no vemos fallas en ninguno de los EPG. ¡Todavía no se ha detectado superposición en los prefijos!

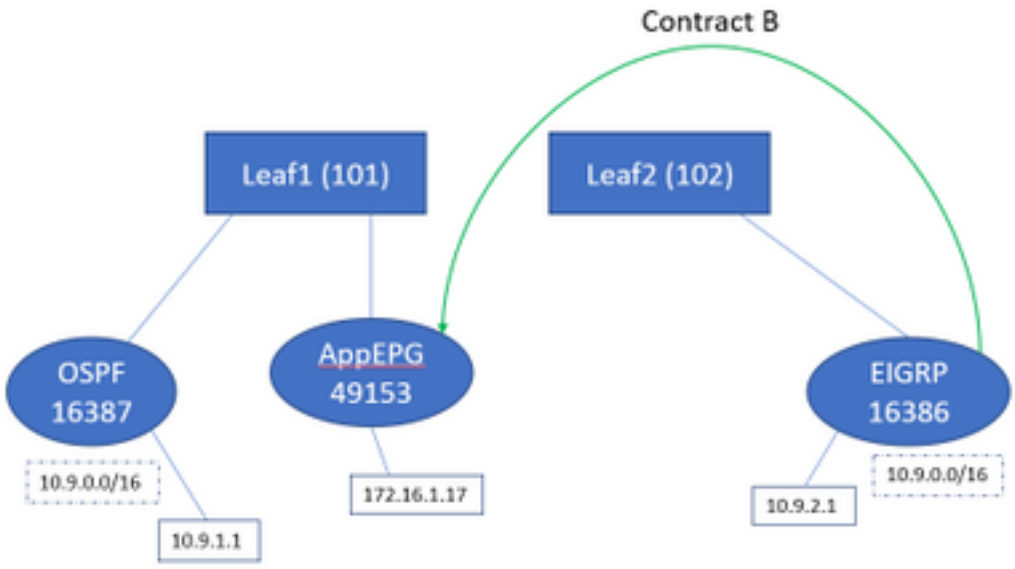
Si agregamos el Contrato B, vemos un error en la aplicación EPG (que consume el Contrato B).

Fault Properties

General | Troubleshooting

Fault Code:	F0467
Severity:	minor
Last Transition:	2019-02-19T18:38:25.436+05:30
Lifecycle:	Raised
Affected Object:	topology/pod-1/node-101/local/svc-policyelem-id-0/cdef-[uni/tn-shparanj/brc-interEPG]/epgCont-[uni/tn-shparanj/ap-cisco-it-eigrp/epg-secure]/fr-[uni/tn-shparanj/brc-interEPG/dirass/cons-[uni/tn-shparanj/ap-cisco-it-eigrp/epg-secure]-any-no]/to-[uni/tn-shparanj/brc-interEPG/dirass/prov-[uni/tn-shparanj/out-eigrp-test/instP-ext-epg]-any-no]/nwissues
Description:	Fault delegate: Configuration failed for uni/tn-shparanj/ap-cisco-it-eigrp/epg-secure due to Prefix Entry Already Used in Another EPG, debug message:
Type:	Config
Cause:	configuration-failed
Change Set:	configQual:prefix-entry-already-in-use, configSt:failed-to-apply, temporaryError:no
Created:	2019-02-19T18:35:59.015+05:30
Code:	F0467
Number of Occurrences:	1
Original Severity:	minor

Topología:



Veamos el cambio en las tablas:

```
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
```

La hoja 2 permanece inalterada.

Esto nos muestra que se ha instalado la regla de zonificación correspondiente al Contrato B. Sin embargo, el prefijo no se puede agregar, ya que ya existe - marcado contra OSPF EPG!

Y eso es exactamente lo que la falla nos advierte, "entrada de prefijo ya usada en otro EPG" - la falla se provoca solamente cuando hay un conflicto en una hoja determinada entre la política (reglas de zonificación) y su aplicación. La falla se provoca en el EPG del consumidor.

Si iniciamos el tráfico desde 10.9.2.1 , se descarta en Leaf101 debido a la negación de la política:

```
# 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
```

Vemos que se suprimen las respuestas del PE 172.16.1.17 a 10.9.2.1. Esto se debe a que:

- Las solicitudes de 10.9.2.1 procedentes del fabric ya se han clasificado con la clase 16386. Éstas llegan al ID de regla 4604 y se permiten
- Las respuestas de 172.16.1.17 se marcan con dclass 16387 - esto se recoge en base a las reglas de prefijo policy-mgr. No hay ninguna regla correspondiente a 16387 y se deniegan.

En esta situación, la clasificación errónea hace que el tráfico se descarte aunque parecemos tener la configuración correcta (si se ignora la falla).

Fabric con prefijo 0.0.0.0/0 declarado como externo en varios EPG externos

En esta situación, analizamos la clasificación errónea potencial y las violaciones de seguridad inesperadas debido a la aplicación de la subred 0.0.0.0/0 como externa en diferentes EPG externos.

OSPF anuncia la red:

10.7.7.0/24

EIGRP anuncia la red:

10.8.8.0/24

Comenzamos con la topología del Diagrama 1, pero sin contratos. Definimos la subred 0.0.0.0/0 como 'subred externa para EPG externos' para EPG en ambos L3outs.

Así son las mesas de Leaf1 y 2:

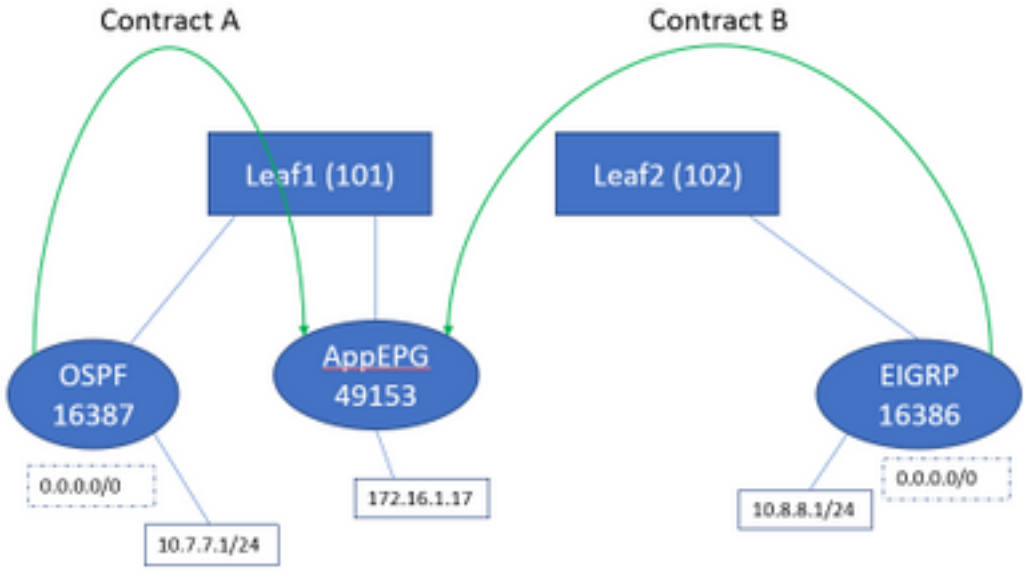
Hoja1:

```
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
```

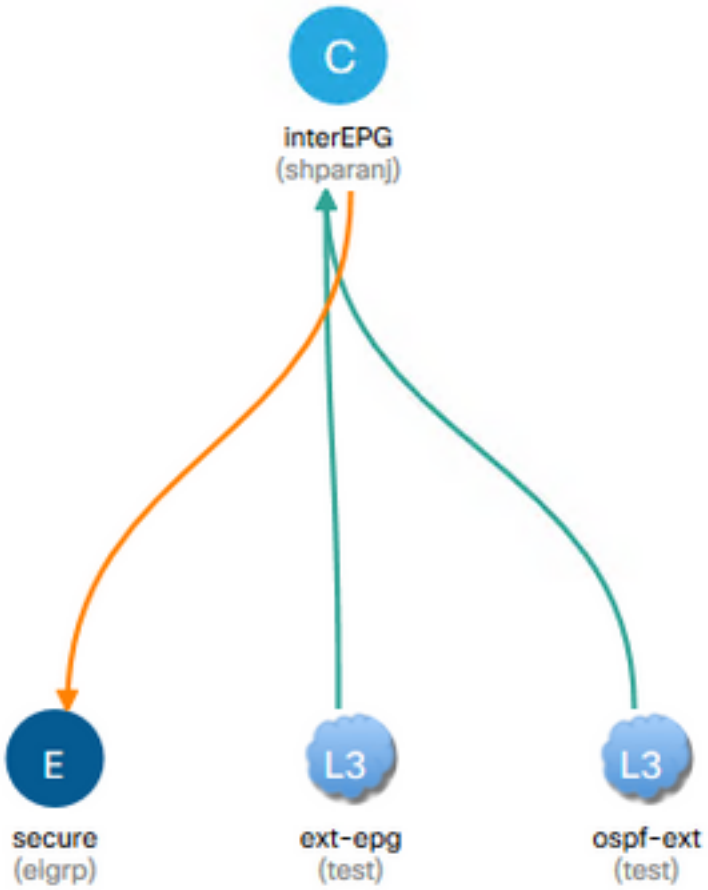
Hoja2:

```
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
```



Si agregamos ambos contratos A y B, todavía no vemos ningún fallo.



Veamos las mesas de Leafs:

Hoja1:

```
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
```

Las tablas de la hoja 2 permanecen inalteradas.

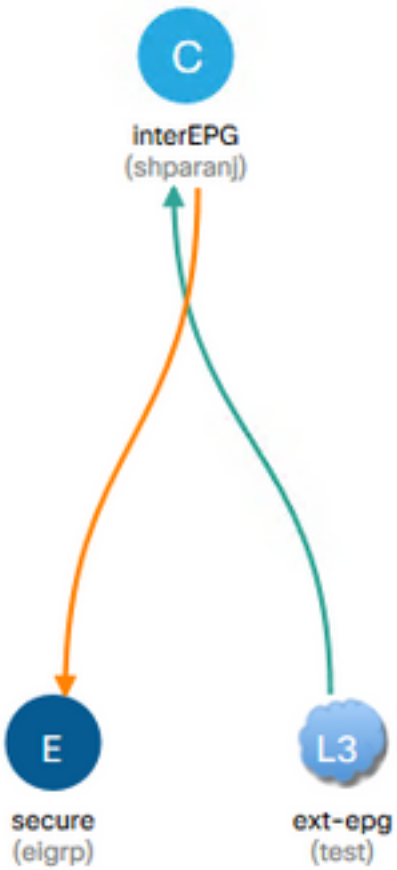
No vemos fallas, ya que en realidad no hay conflicto político desde la perspectiva de cada hoja.
Los ID de regla agregados cuando se utiliza 0.0.0.0/0 como EPG externo son especiales.

- **El tráfico que llega a cualquiera de las hojas de borde desde sus respectivos EPG se marca con la clase 32770 - esta es la pcTag del VRF.**
- dclass en este tráfico es 49153 - pcTag de la aplicación-EPG.
- **El tráfico de retorno de la aplicación-EPG tiene una clase de 15**

ELAM en hoja1:

```
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
```

Incluso si eliminamos el Contrato A, 10.7.7.1 puede continuar la comunicación con 172.16.1.17.



Esto se debe a que la eliminación del Contrato A no da lugar a ningún cambio en las reglas de zonificación en Leaf1.

```
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)
```

Además, el tráfico entrante en OSPF EPG externo sigue etiquetándose con VRF pcTag, ya que EPG aún tiene 0.0.0.0/0 marcado como subred externa.

Esto conlleva una violación de la política de seguridad, es decir, dos EPG capaces de comunicarse sin un contrato en un VRF forzado.

Lectura adicional

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