Solución de problemas de clasificación de subred L3Out en ACI

Contenido

Introducción

Este documento describe la clasificación de las subredes externas dentro de los EPG L3Out de Cisco ACI.

Abreviaturas

- BD: Dominio de Bridge
- EPG: Grupo de terminales
- ExEPG: Grupo de terminales externos
- COSTILLA: Base de información de routing
- VRF: Routing y reenvío virtual
- ID de clase: Etiqueta que identifica un EPG

Clasificación de EPG externo

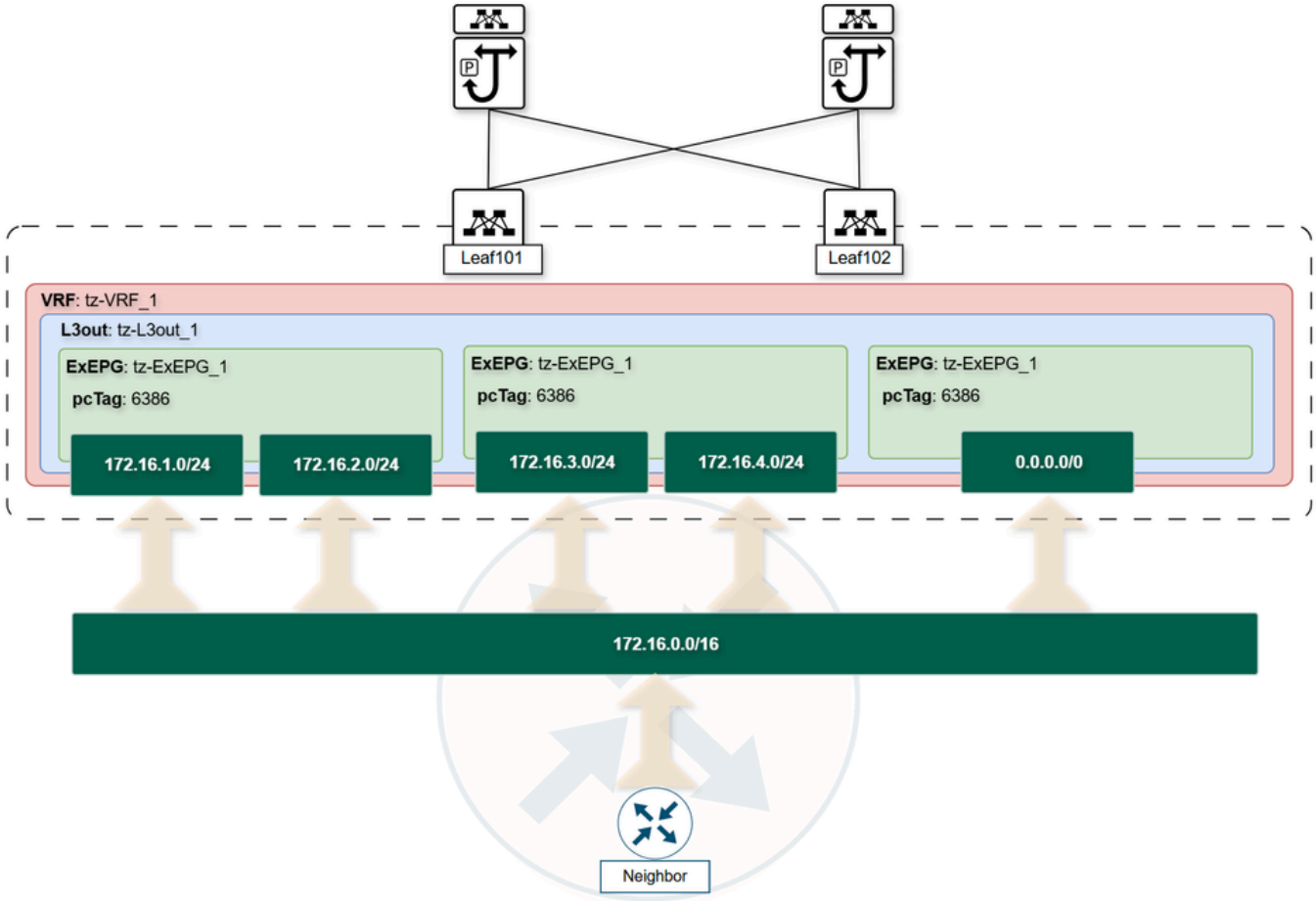
Un EPG externo en Cisco ACI representa las redes enrutadas externas conectadas a través de L3Outs. De manera similar a cómo un EPG regular clasifica los extremos, un EPG externo clasifica las subredes externas por VRF, lo que significa que cada subred debe ser única dentro de su contexto VRF.

Un error común es que una subred EPG externa sólo incluye prefijos aceptados a través del protocolo de ruteo dinámico. Sin embargo, cuando se crea una salida L3, hay un route-map

predeterminado que filtra los anuncios entrantes; por lo tanto, todos los prefijos anunciados por el protocolo de ruteo dinámico son aceptados de forma predeterminada. El objetivo principal de definir subredes en un ExEPG es la clasificación solo para asignar una pcTag única a las subredes incluidas en el ExEPG para la aplicación de políticas y la aplicación de contratos.

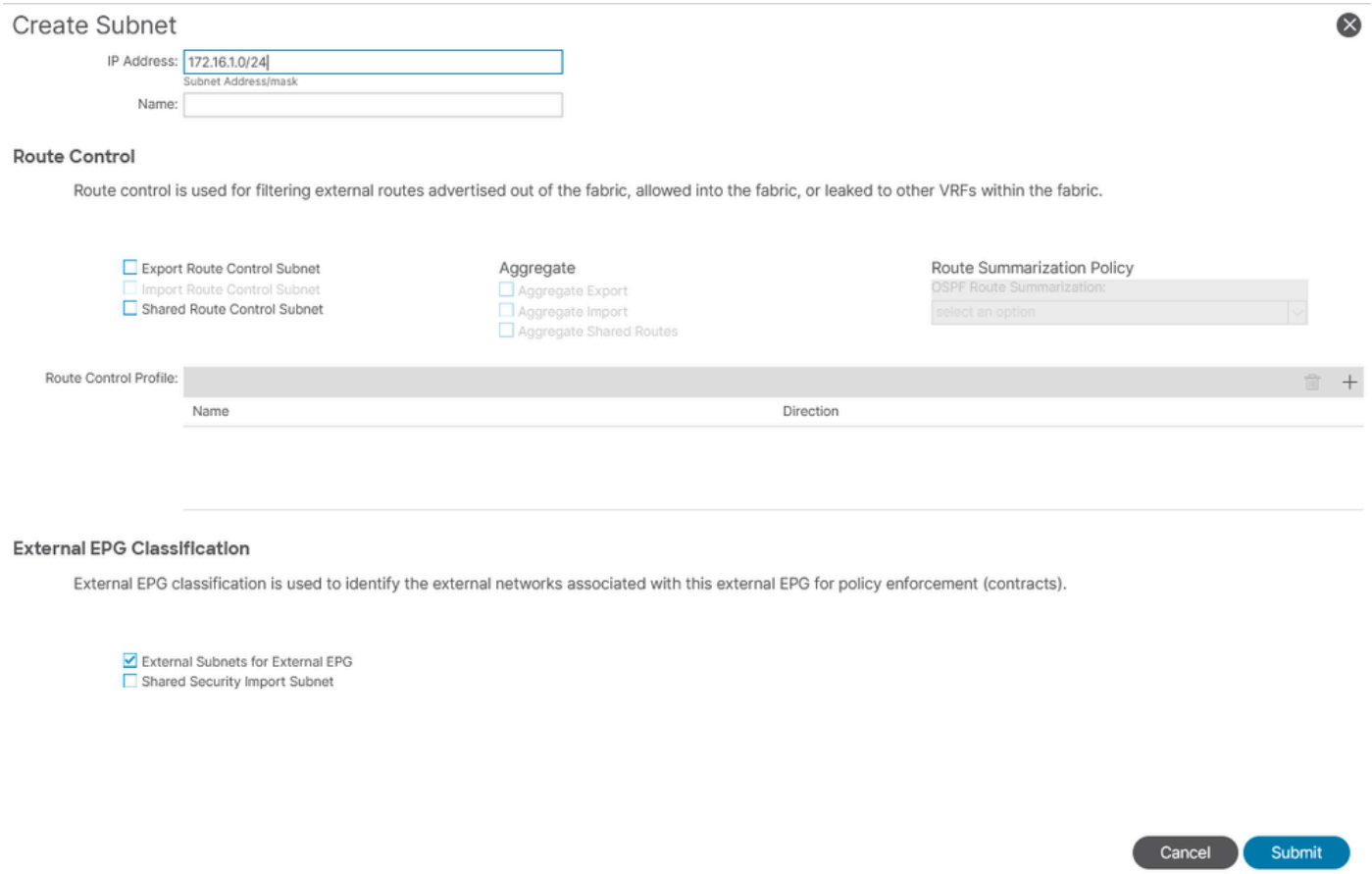
Esta clasificación permite un control granular de las políticas. Por ejemplo, un solo vecino externo puede anunciar una superred a ACI, que se puede segmentar en varios ExEPG. Esto permite que diferentes acciones de contrato se apliquen a diferentes subredes, como permitir que EPG internos específicos se comuniquen solamente con subredes externas designadas o redireccionar el tráfico destinado a ciertos prefijos a un nodo PBR antes de alcanzar su destino final.

Este diagrama ilustra cómo Cisco ACI clasifica las subredes externas en función de los EPG externos, lo que permite una segmentación del tráfico y una aplicación de contratos precisos.



Indicadores de subredes EPG externas

Para clasificar y gestionar prefijos externos en un ExEPG en ACI, se configuran indicadores de subred específicos al crear un prefijo de subred en un ExEPG. En esta sección se detalla cada indicador y su uso esperado:



- Subred externa para EPG externo:
  Este indicador indica que la subred reside fuera del fabric de ACI y no está configurada en ningún dominio de puente ni EPG. Sólo se debe utilizar cuando el prefijo es anunciado por un vecino de ruteo o inyectado estáticamente en el RIB. Este indicador está activado de forma predeterminada.

- Exportar subred de control de ruta:
  Este indicador designa que la subred se anuncia desde ACI al vecino de ruteo a través del protocolo de ruteo dinámico. No debe activarse simultáneamente con el indicador de subred externa para EPG externo, ya que esto puede provocar loops de ruteo de Capa 3. Dado que ACI clasifica la subred como externa y también la anuncia de vuelta, esto puede conducir a inconsistencias de ruteo a pesar de los mecanismos de evasión de loop en los protocolos de ruteo.

- Subred de control de ruta compartida:
  Este indicador se establece cuando el prefijo de subred está pensado para compartirse a través de varios VRF, lo que permite la fuga de rutas entre los contextos.

- Subred de importación de seguridad compartida:
  Utilizado junto con el indicador Shared Route Control Subnet, esto permite compartir etiquetas de pc de seguridad para subredes externas a través de diferentes VRF, facilitando la aplicación de políticas consistentes.

- Importar subred de control de ruta:
  Este indicador permite un control granular sobre los prefijos recibidos de los vecinos de

ruteo. De forma predeterminada, ACI acepta todos los anuncios de rutas entrantes; para habilitar este indicador, es necesario activar la aplicación de control de rutas para filtrar los prefijos entrantes.

- Sección Agregada:
  Aplicable únicamente a la subred quad-0 (0.0.0.0/0), esta sección resume todos los prefijos de la RIB para la exportación o importación agregada. Cuando las subredes se filtran a otros VRF, se resumen como rutas compartidas agregadas para optimizar las tablas de ruteo.

Comandos de verificación y resolución de problemas

Ruteo

Para comenzar, la ruta debe estar presente en la tabla de ruteo del VRF en los switches de hoja de borde. Por ejemplo, este comando muestra una ruta BGP en el VRF tz:tz-VRF_1:

<#root>

```
Leaf101#
show ip route bgp vrf tz:tz-VRF_1


IP Route Table for VRF "tz:tz-VRF_1"


'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>


172.16.1.0/24
, ubest/mbest: 1/0
*via 10.10.1.2
%tz:tz-VRF_1, [20/0], 00:00:04, bgp-65002, external, tag 65003
Leaf101#
```

Esto confirma que la ruta está instalada en la tabla de ruteo VRF y está disponible para decisiones de reenvío.

Clasificación

Después de que la ruta esté presente en la tabla de ruteo, la clasificación determina cómo se maneja el tráfico según la política. En ACI, la clasificación está vinculada al ExEPG y sus subredes asociadas.

Para validar la clasificación de subred en un ExEPG, se puede consultar el APIC para la clase

l3extInstP, que representa la instancia de EPG externo. Su clase secundaria l3extSubnet enumera las subredes configuradas bajo ese ExEPG. Por ejemplo:

<#root>

```
moquery -c l3extInstP -f 'l3ext.InstP.dn*"[ tenant name ].*[ l3out name ]"' -x rsp-subtree=children rsp-
```

<#root>

```
APIC#

moquery -c l3extInstP -f 'l3ext.InstP.dn*"tz.*l3out"' -x rsp-subtree=children rsp-subtree-class=l3extSub


Total Objects shown: 1

# l3ext.InstP

name : tz-ExEPG_1


!-- cut for brevity --!
configSt : applied
descr :
dn : uni/tn-tz/out-l3out/instP-tz-ExEPG_1
!-- cut for brevity --!
floodOnEncap : disabled
isSharedSrvMsiteEPg : no
lcOwn : local
matchT : AtleastOne
mcast : no
modTs : 2025-09-10T00:36:49.239+00:00
monPolDn : uni/tn-common/monepg-default
nameAlias :
pcEnfPref : unenforced

pcTag : 32771


pcTagAllocSrc : idmanager
prefGrMemb : exclude
prio : unspecified
rn : instP-tz-ExEPG_1
scope : 3047430
status : modified
targetDscp : unspecified
triggerSt : triggerable
txId : 1152921504612318828
uid : 15374
userdom : :all:

# l3ext.Subnet

ip : 172.16.1.0/24


!-- cut for brevity --!
dn : uni/tn-tz/out-l3out/instP-tz-ExEPG_1/extsubnet-[172.16.1.0/24]
extMngdBy :
```

```
lcOwn : local
modTs : 2025-09-10T01:05:13.249+00:00
monPolDn : uni/tn-common/monepg-default
!-- cut for brevity --!
rn : extsubnet-[172.16.1.0/24]
```

scope : import-security

```
status :
uid : 15374
userdom : :all:

APIC#
```

Si no se devuelve ningún resultado para la clase l3extSubnet, indica que no hay subredes configuradas bajo el EPG externo. Sin subredes configuradas, ACI no puede asociar una pcTag a la subred de tráfico entrante, lo que hace que el tráfico se descarte a pesar de la ruta existente en la tabla de routing.

Otro aspecto importante a tener en cuenta es el alcance de la subred, que representa los indicadores establecidos para la subred en cuestión:

- Seguridad de importación

La subred se ha marcado con Subred externa para EPG externo.

- export-rtctrl

La subred se ha marcado con Control de ruta de exportación.

- import-rtctrl

La subred se ha marcado con Control de ruta de importación.

- seguridad compartida

La subred se ha marcado con Subred de importación de seguridad compartida.

- shared-rtctrl

La subred se ha marcado con el control de ruta compartida.

Los protocolos de ruteo y los procesos del plano de control actualizan las tablas de ruteo al recibir un prefijo de un vecino mencionado, que luego se programan en las tablas de reenvío HAL L3. Las rutas HAL L3 representan las rutas reales de Capa 3 programadas en las tablas de reenvío de hardware (ASIC) en los switches de hoja. Estas rutas se derivan de los cálculos de los protocolos de ruteo y la tabla de ruteo y se utilizan para decisiones de reenvío.

<#root>

```
<-- When the prefix is not configured under the External EPG, a classification of 0xf is seen -->
```

```
Leaf101#
vsh_lc -c 'show platform internal hal l3 routes vrf tz:tz-VRF_1' | egrep "Prefix/Len|172.16.1.0" | cut -
VRF |   Prefix/Len  | RT|CLSS| Flags
4675| 172.16.1.0/ 24| UC| f|spi,dpi
Leaf101#
<-- When the prefix is configured under the External EPG, a classification of the pcTag in hexadecimal
Leaf101#
vsh_lc -c 'show platform internal hal l3 routes vrf tz:tz-VRF_1' | egrep "Prefix/Len|172.16.1.0" | cut -
VRF |   Prefix/Len  | RT|CLSS| Flags
4675| 172.16.1.0/ 24| UC|8003|spi,dpi
Leaf101#
Leaf101#
vsh_lc -c '
dec 0x8003'
32771
Leaf101#
```

Posteriormente, cuando una subred se configura con el indicador Subred externa para EPG externo en un ExEPG, un proceso interno denominado Administrador de políticas (policy-mgr) actualiza su tabla de asignación de prefijo a etiqueta de pc con esta entrada de subred y la etiqueta de pc asociada. El administrador de políticas actúa como el motor de orquestación de políticas centralizadas del fabric, que traduce las definiciones de políticas de alto nivel en configuraciones procesables en el fabric de ACI. Esto garantiza una conectividad de aplicaciones y un comportamiento de red coherentes y seguros mediante la aplicación de las etiquetas de pc correctas para la clasificación del tráfico y las decisiones de reenvío basadas en las subredes externas configuradas.

<#root>

```
Leaf101#
vsh -c 'show system internal policy-mgr prefix' | egrep "tz:tz-VRF_1"
3047430 36 0x80000024 Up tz:tz-VRF_1 ::/0 15 True True False False
3047430 36 0x24 Up tz:tz-VRF_1 0.0.0.0/0 15 True True False False
3047430 36 0x24 Up tz:tz-VRF_1 172.16.1.0/24 32771 True True False False
Leaf101#
```

Esto confirma que el prefijo 172.16.1.0/24 está siendo anunciado por el vecino al switch de hoja de borde ACI, y ACI ha clasificado el prefijo debajo de pcTag 32771

Contratos

Una regla de división en zonas es el proceso subyacente que aplica las políticas de contrato entre los EPG (incluidos los ExEPG) dentro del fabric. El VRF VNID (alcance) y la pcTag del EPG externo se pueden utilizar para definir y validar las reglas de comunicación aplicadas entre los EPG de origen y de destino. Básicamente, las reglas de zonificación traducen las relaciones contractuales de alto nivel en reglas específicas y aplicables programadas en los switches de hoja.

Un aspecto importante que debe tenerse en cuenta es el lugar donde se instala el contrato en el fabric. De forma predeterminada, el VRF se configura con la dirección de aplicación de control de políticas establecida en ingreso. Esta configuración determina que la regla de zonificación para un contrato determinado está instalada en el switch de hoja donde reside el punto final de origen.

Para este ejercicio, el tráfico es entrante desde una L3Out, la regla de zonificación se instala en la hoja de borde que se conecta a esa L3Out, ya que esta hoja actúa como la hoja de origen para el tráfico que ingresa al entramado.

<#root>

```
Leaf101#
```

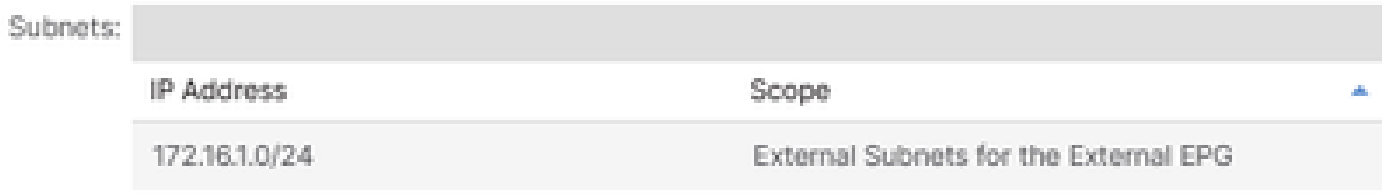
show zoning-rule scope 3047430 | egrep "Rule|---|32771"

```
+---------+--------+--------+----------+----------------+---------+---------+------------------+------
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       | operSt  |  Scope  |        Name      |
+---------+--------+--------+----------+----------------+---------+---------+------------------+------
|  4441   | 49153  | 32771  |     5    |     bi-dir     | enabled | 3047430 |     tz:Contract  |
|  4500   | 32771  | 49153  |     5    | uni-dir-ignore | enabled | 3047430 |     tz:Contract  |
+---------+--------+--------+----------+----------------+---------+---------+------------------+------
Leaf101#
```

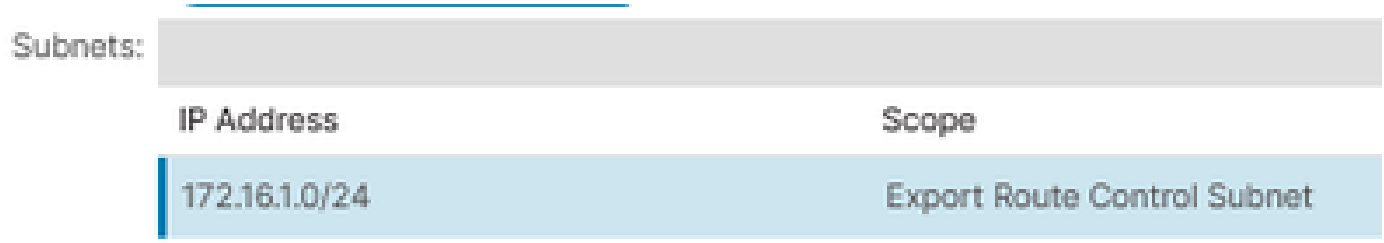
Routing de tránsito

El routing de tránsito permite que el fabric actúe como una red de tránsito anunciando las rutas

externas aprendidas de un L3Out a otro. Para configurar correctamente el ruteo de tránsito, la subred entrante debe marcarse con el indicador Subred externa para EPG externo.



Simultáneamente, el L3Out que anuncia esta subred a otros peers externos debe tener el indicador Export Route Control Subnet habilitado en la subred correspondiente. Este indicador permite que la subred se redistribuya y anuncie fuera del fabric a través del protocolo de ruteo configurado en ese L3Out.



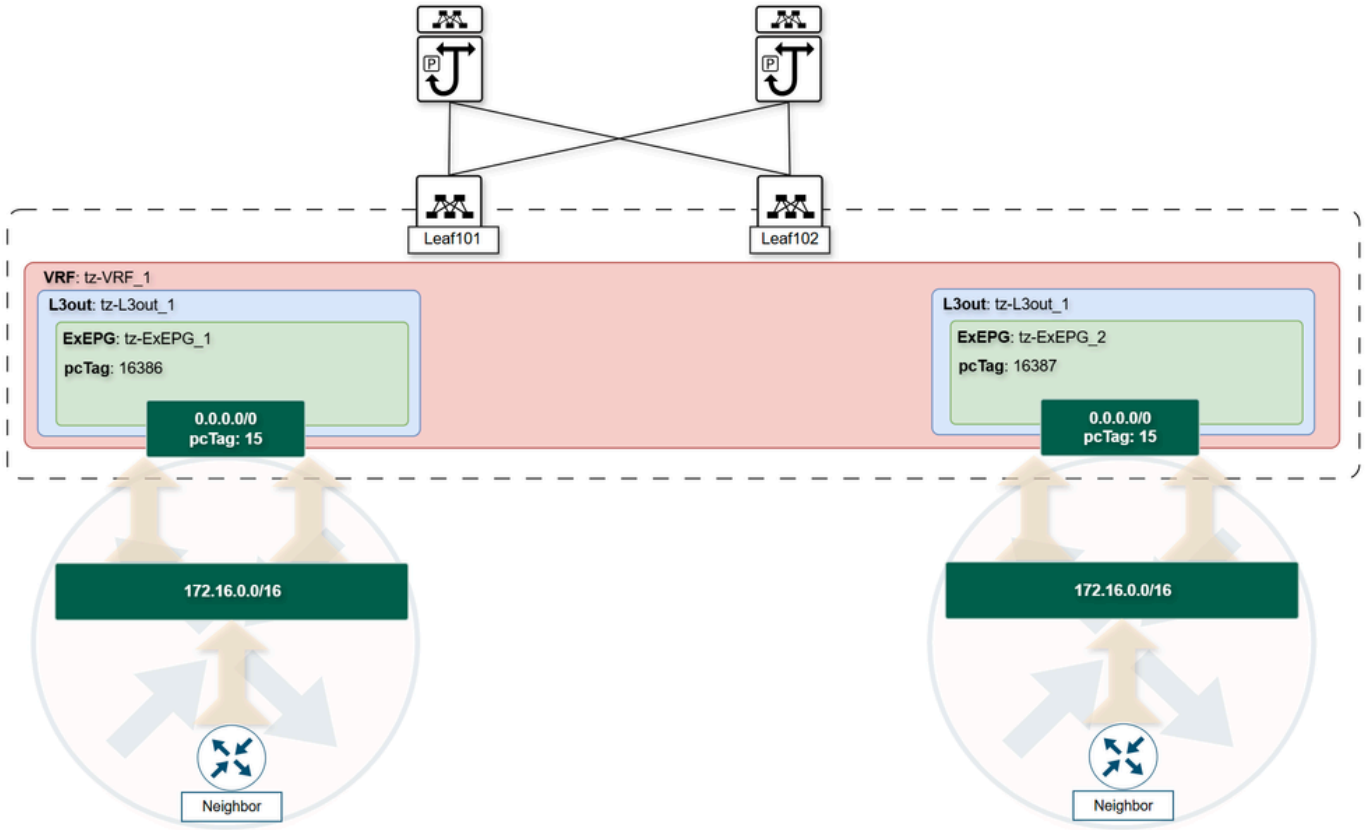
Por último, se debe configurar un contrato entre el L3out recibido y el L3out exportador para completar el proceso de distribución de la ruta.

Problemas comunes en la clasificación de EPG externo de subred

pcTag 15

Anteriormente, en este documento, se afirmaba que la subred ExEPG le ayuda a clasificar las subredes en la pcTag correcta por motivos de aplicación de políticas. Una excepción importante a esta clasificación es la subred quad-0 (0.0.0.0/0) cuando se configura con el indicador Subred externa para EPG externo. A esta subred siempre se le asigna la pcTag 15 reservada, que actúa eficazmente como comodín para todo el tráfico externo dentro de un VRF.

Este diagrama representa el problema que enfrenta la configuración de quad-0 con Subred Externa para EPG Externo en múltiples ExEPG dentro del mismo VRF:



- La subred quad-0 se confunde a menudo con la ruta predeterminada. Aunque esto es cierto a veces, como cuando un vecino de routing dinámico anuncia solo la ruta predeterminada a la salida L3 de ACI, el papel de la subred quad-0 en ACI es más amplio como clasificación general.
- Es una práctica común configurar varios ExEPG con la subred quad-0 para aceptar todos los prefijos anunciados por un vecino. Aunque esto logra el objetivo de una amplia aceptación, puede conducir a un ruteo asimétrico inesperado cuando se configuran múltiples ExEPG con quad-0 dentro del mismo VRF. Cuando se configuran múltiples ExEPG dentro del mismo VRF con quad-0 como subred externa, ACI no puede seleccionar determinantemente qué L3Out utilizar para una subred de destino específica. En su lugar, selecciona una L3Out arbitrariamente.
- Este comportamiento puede causar ruteo asimétrico, tráfico intermitente o incluso caídas de tráfico si el L3Out seleccionado aleatoriamente no tiene los contratos necesarios para permitir la comunicación.

Subredes superpuestas

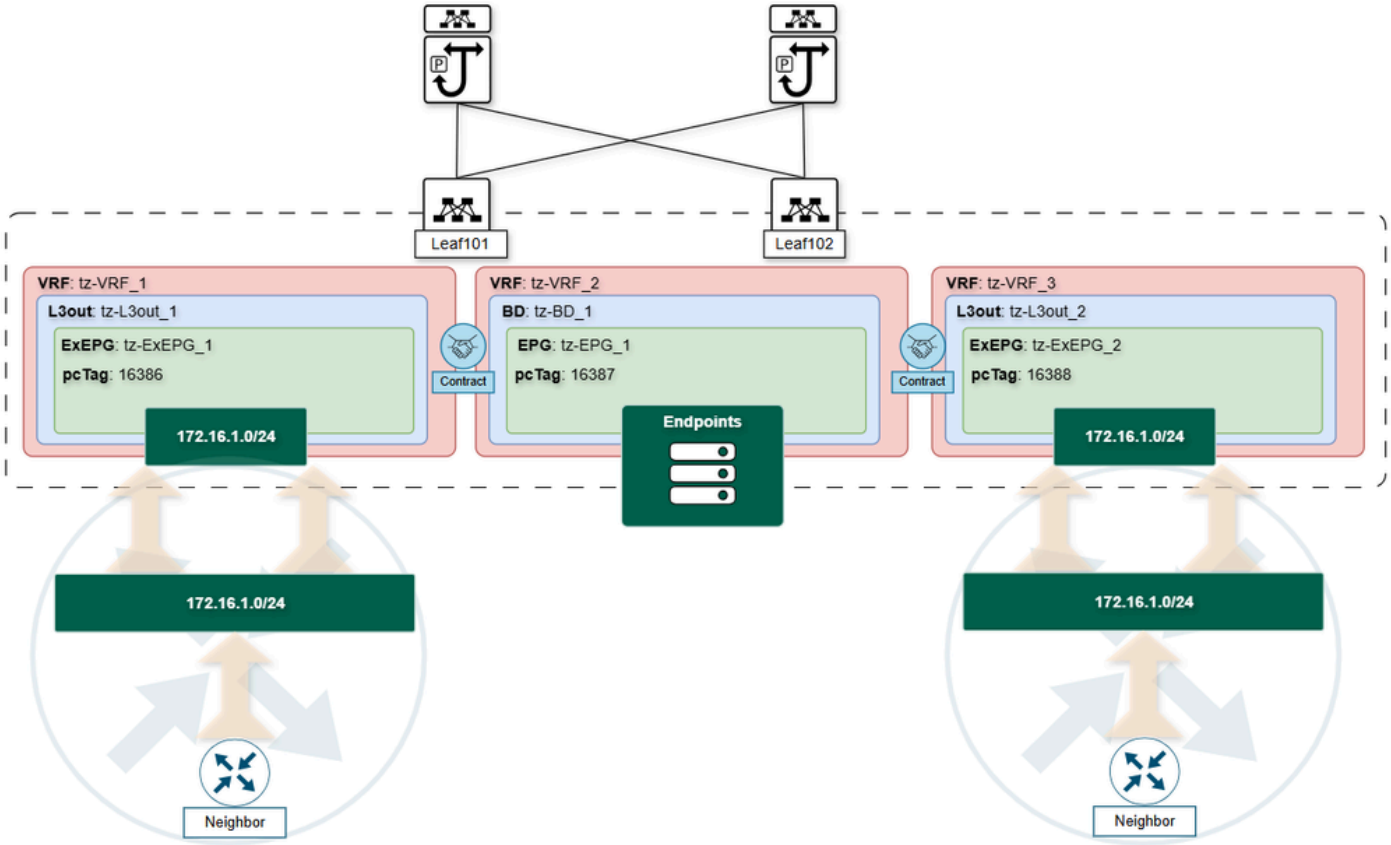
No se permite la configuración de subredes idénticas en diferentes ExEPG. Si intenta hacerlo, se produce el error "F0467: "Entrada de Prefijo Ya Utilizada en Otro EPG", evitando la duplicación de subred dentro de un VRF.

Sin embargo, las subredes superpuestas pueden existir entre diferentes VRF porque cada VRF mantiene un contexto de tabla de ruteo independiente. Esta separación permite configurar la misma subred en los ExEPG que pertenecen a VRF diferentes. A pesar de esto, la precaución es crítica cuando se realiza una fuga de ruta VRF que involucra estas subredes superpuestas, ya que puede llevar a decisiones de reenvío asimétricas debido a conflictos en la clasificación de

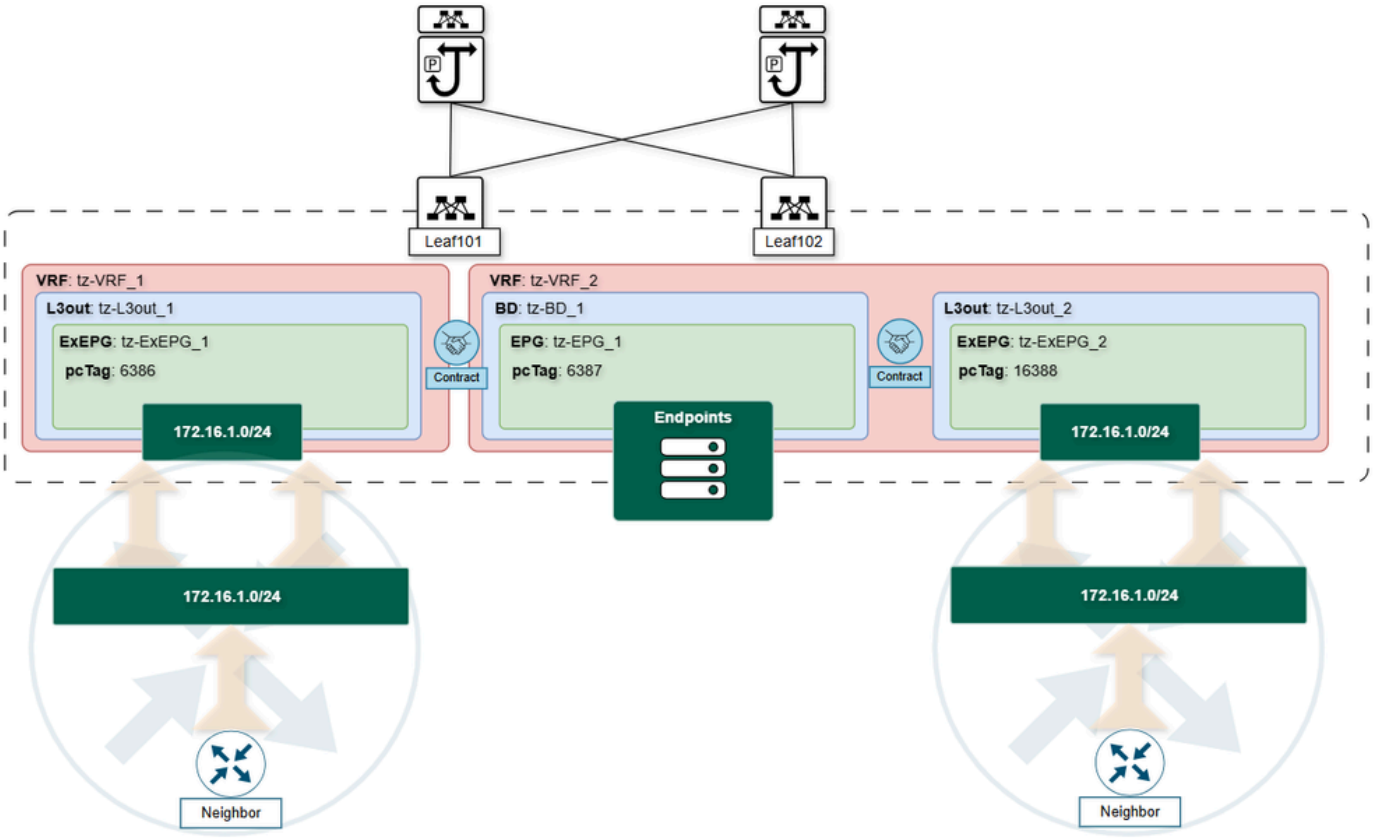
subred (pcTag) versus la información de ruteo (RIB).

Los escenarios clave incluyen:

- Fuga de Ruta de Dos VRF a un Tercer VRF:
  Cuando dos VRF filtran la misma subred en un tercer VRF, el VRF receptor instala la primera subred que recibe en función de la política compartida del APIC. Si el switch de hoja que maneja este VRF se reinicia o la elección de ruteo cambia, la tabla de ruteo podría actualizarse a un L3Out diferente, causando un comportamiento de reenvío inconsistente.



- L3Out ExEPG de Local a VRF que se Solapa con Subredes Filtradas:
  En diseños donde se utiliza la fuga de rutas, si un ExEPG L3Out local se configura con la misma subred que una subred filtrada, la entrada de ruteo local siempre tiene prioridad sobre las rutas filtradas.



Estas situaciones resaltan que los problemas de reenvío asimétrico surgen de la capa de decisión de clasificación y reenvío, no de la tabla de ruteo en sí. Mientras que la clasificación de subred asocia una subred con un L3Out y un ExEPG específicos para la aplicación de políticas, la tabla de ruteo puede apuntar a un destino L3Out diferente. Esta discordancia puede hacer que el tráfico se reenvíe de forma incoherente, lo que puede provocar posibles problemas de conectividad o lagunas en la aplicación de políticas.

Importar cambio de comportamiento predeterminado de control de ruta

De forma predeterminada, ACI acepta todos los anuncios de rutas entrantes de los vecinos. Para controlar qué prefijos se aceptan, debe habilitar la aplicación de control de ruta: entrante en el objeto raíz L3Out:

Vaya a Arrendatarios > [nombre de arrendatario] > Redes > L3outs > [nombre de L3out].

Esta acción crea un route-map bajo el protocolo de ruteo seleccionado.

<#root>

Border Leaf#

show ip bgp neighbors vrf tz:tz-VRF1 | egrep route-map

Outbound route-map configured is exp-l3out-ExEPG-peer-2981888, handle obtained

Inbound route-map configured is imp-l3out-ExEPG-peer-2981888, handle obtained

Border Leaf#

show route-map imp-l3out-ExEPG-peer-2981888

route-map imp-l3out-ExEPG-peer-2981888,

permit

, sequence 15801
Match clauses:

ip address prefix-lists: IPv4-peer49155-2981888-exc-ext-inferred-import-dst

ipv6 address prefix-lists: IPv6-deny-all
Set clauses:

Border Leaf#

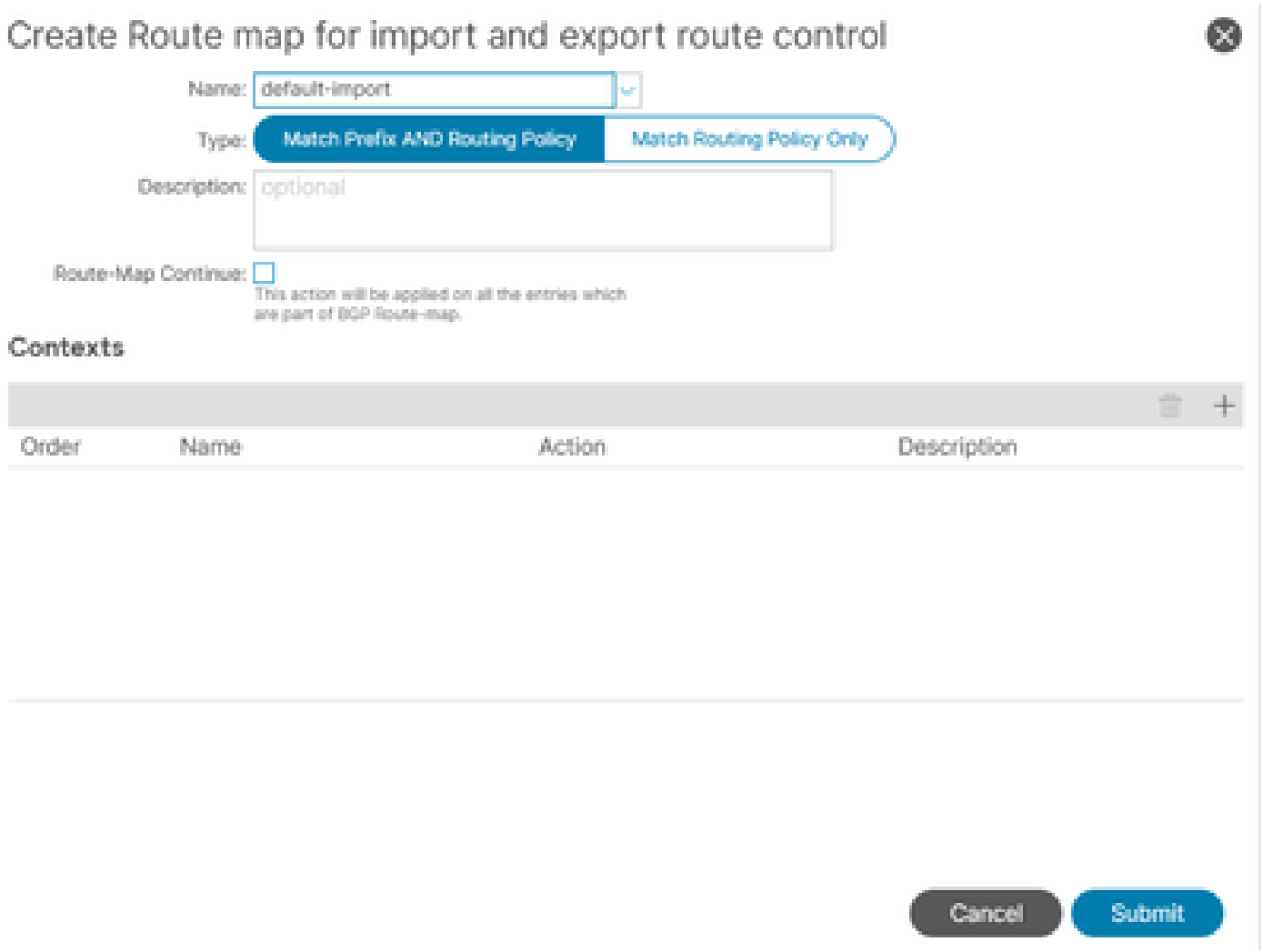
show ip prefix-list IPv4-peer49155-2981888-exc-ext-inferred-import-dst

ip prefix-list IPv4-peer49155-2981888-exc-ext-inferred-import-dst: 1 entries
seq 1 permit 172.16.1.0/24
Border Leaf#

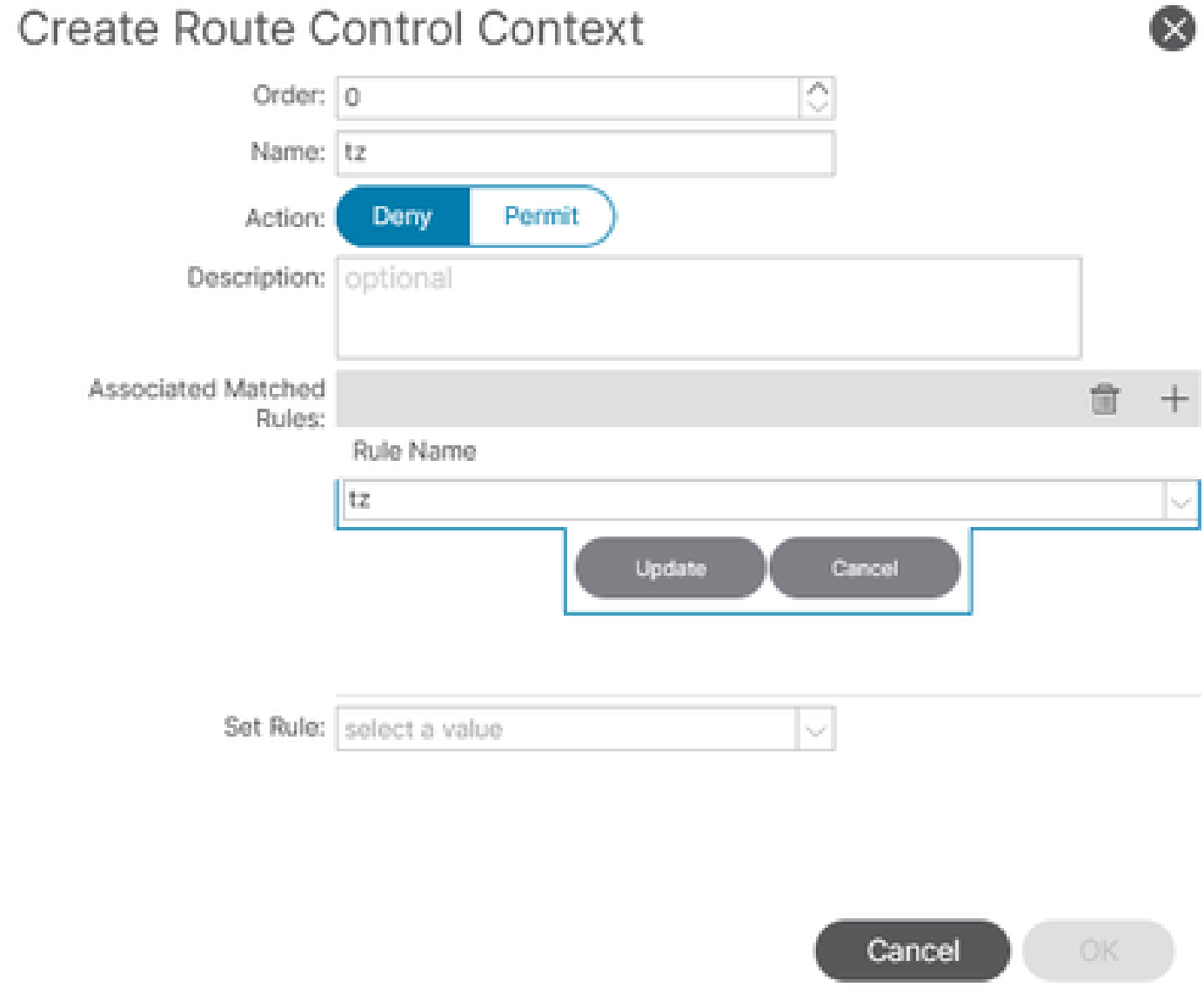
De forma predeterminada, este route-map de importación permite todos los prefijos entrantes. Para modificar este comportamiento:

Vaya a Arrendatarios > [nombre de arrendatario] > Redes > L3outs > [nombre de L3out] > Mapa de ruta para el control de ruta de importación y exportación

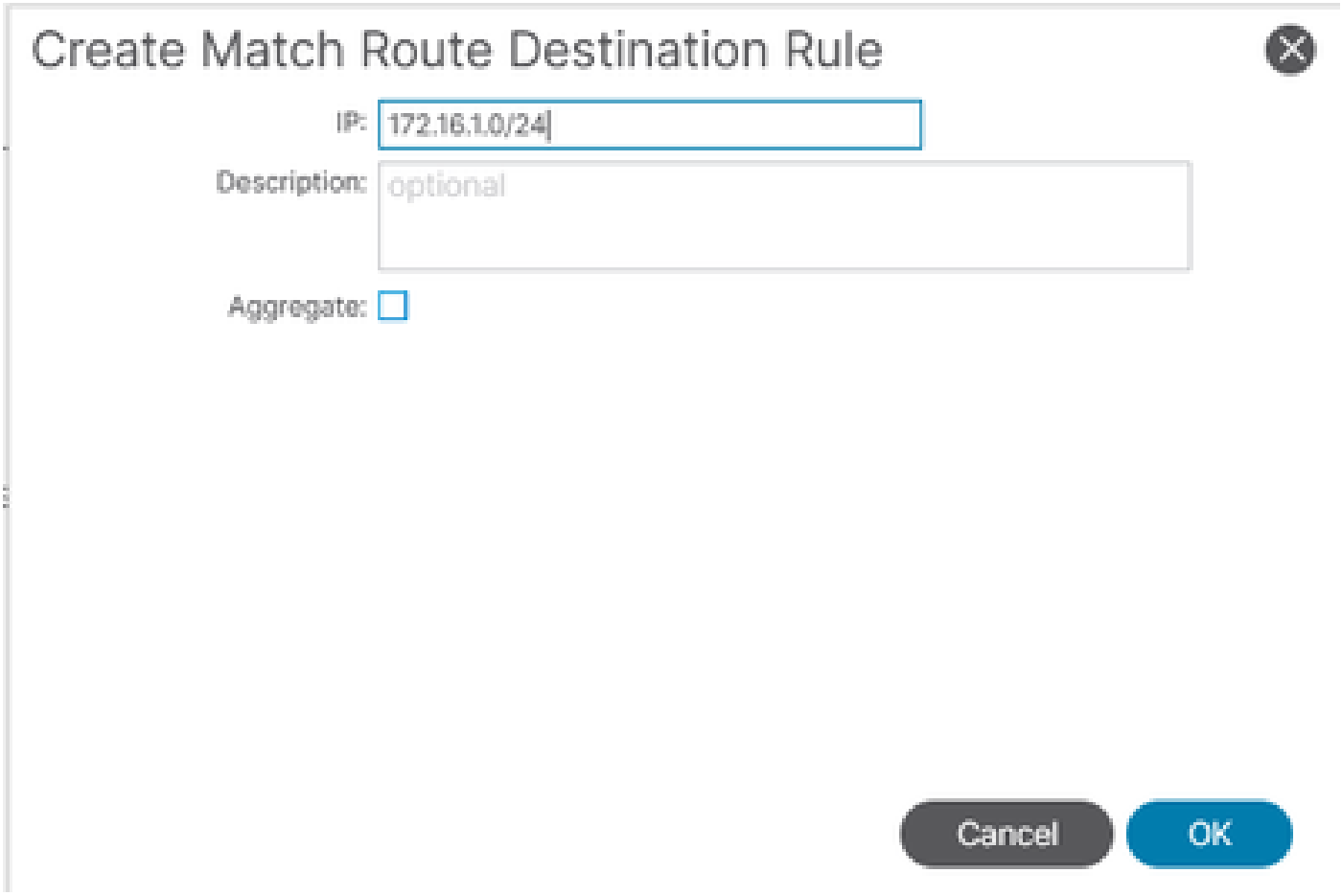
Seleccione el route-map de importación predeterminado o cree uno nuevo mediante el icono de engranaje situado en la parte superior derecha.



En la sección Contexto, cree una nueva regla asociada coincidente.



En la sección Reglas de coincidencia, desplácese hasta Prefijo de coincidencia y agregue las subredes específicas que desea controlar.



Después de enviar las directivas, la acción de importación route-map cambia en consecuencia, imponiendo el filtrado de prefijos deseado.

<#root>

```
Border Leaf#

show route-map imp-l3out-ExEPG-peer-2981888


route-map imp-l3out-ExEPG-peer-2981888,

deny

, sequence 8001
Match clauses:
ip address prefix-lists: IPv4-peer49155-2981888-exc-ext-in-default-import2tzOtz-dst
ipv6 address prefix-lists: IPv6-deny-all
Set clauses:

Border Leaf#
```

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).