Identificar e solucionar problemas de classificação de sub-rede L3Out na ACI

Contents

Introdução

Este documento descreve a classificação de sub-redes externas dentro dos EPGs L3Out da Cisco ACI,

Abreviaturas

- BD: Domínio de bridge
- EPG: Grupo de endpoints
- ExEPG: Grupo de Ponto de Extremidade Externo
- COSTELAS: Base de Informações de Roteamento
- VRF: Roteamento e encaminhamento virtual
- ID da classe: Marca que identifica um EPG

Classificação de EPG Externo

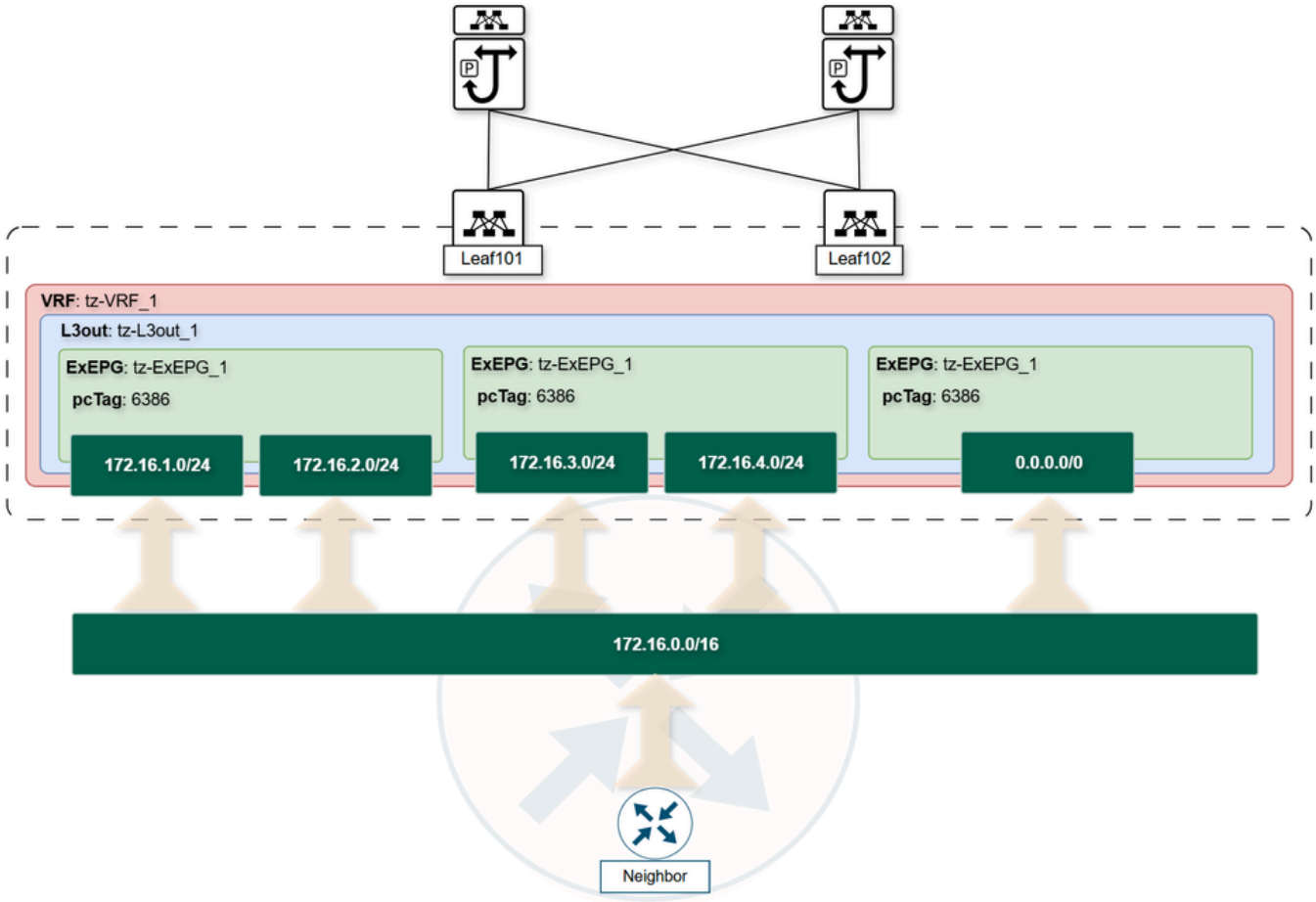
Um EPG externo na Cisco ACI representa redes roteadas externas conectadas através de L3Outs. Semelhante à maneira como um EPG regular classifica terminais, um EPG externo classifica sub-redes externas em uma base por VRF, o que significa que cada sub-rede deve ser exclusiva dentro de seu contexto de VRF.

Uma concepção equivocada comum é que uma sub-rede de EPG externa inclui apenas prefixos aceitos por meio do protocolo de roteamento dinâmico. No entanto, quando um L3Out é criado,

há um mapa de rota padrão filtrando anúncios recebidos; assim, todos os prefixos anunciados pelo protocolo de roteamento dinâmico são aceitos por padrão. A finalidade principal de definir sub-redes em um ExEPG é a classificação somente para atribuir um pcTag exclusivo às sub-redes incluídas no ExEPG para aplicação de contrato e política.

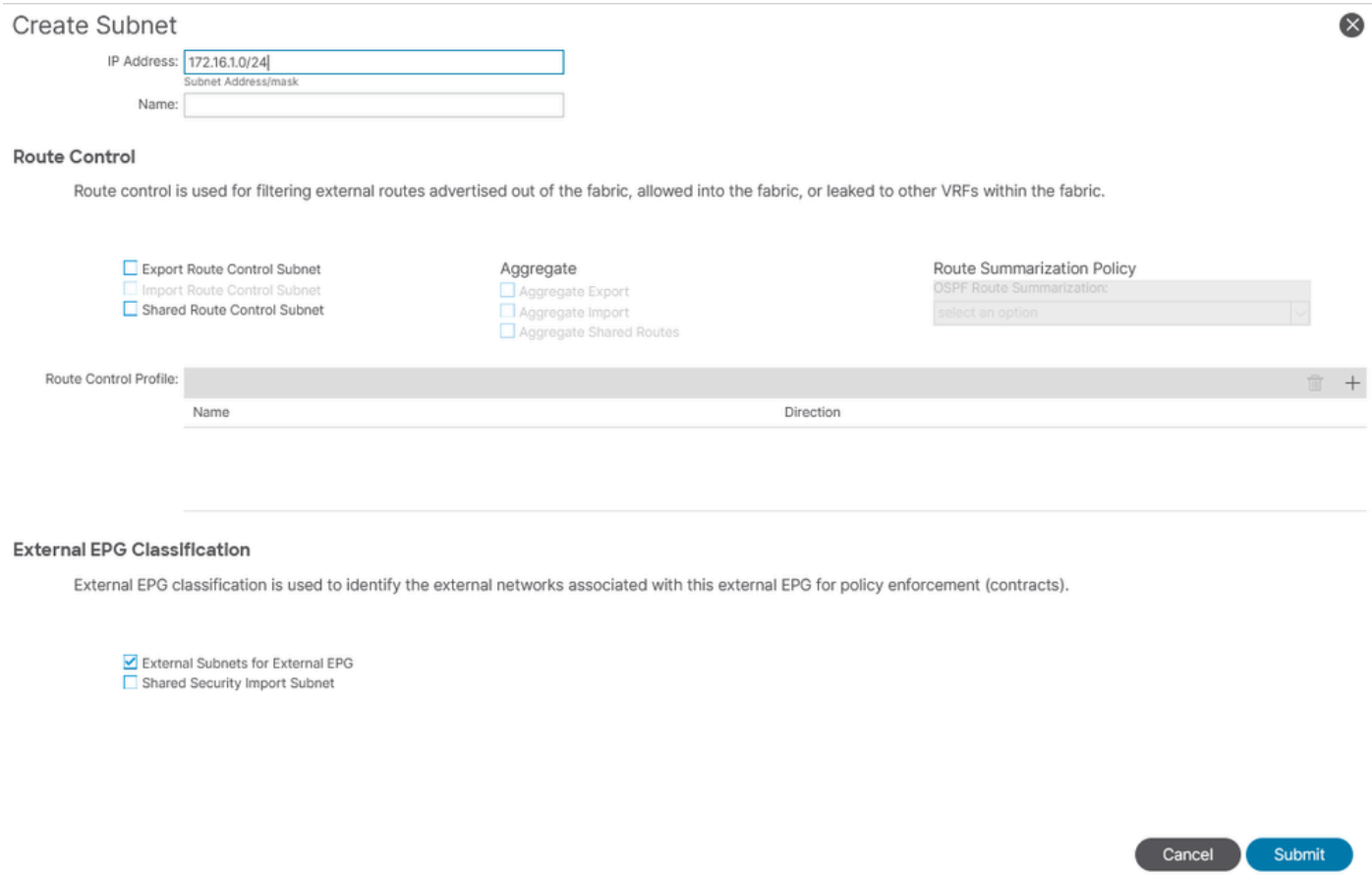
Essa classificação permite o controle de política granular. Por exemplo, um único vizinho externo pode anunciar uma super-rede à ACI, que pode ser segmentada em vários ExEPGs. Isso permite que diferentes ações de contrato sejam aplicadas a sub-redes distintas, como permitir que EPGs internos específicos se comuniquem somente com sub-redes externas designadas ou redirecionar o tráfego destinado a determinados prefixos para um nó PBR antes de atingir seu destino final.

Este diagrama ilustra como a Cisco ACI classifica sub-redes externas com base em EPGs externos, permitindo a segmentação precisa do tráfego e a aplicação de contratos.



Sinalizadores de Sub-redes EPG Externas

Para classificar e gerenciar prefixos externos em um ExEPG na ACI, sinalizadores de sub-rede específicos são configurados ao criar um prefixo de sub-rede em um ExEPG. Esta seção detalha cada flag e seu uso pretendido:



- Sub-rede externa para EPG externo:
  Essa flag indica que a sub-rede reside fora da estrutura da ACI e não está configurada em nenhum domínio de bridge ou EPG. Ele deve ser usado somente quando o prefixo for anunciado por um vizinho de roteamento ou injetado estaticamente no RIB. Esse sinalizador é ativado por padrão.

- Sub-rede de Controle de Rotas de Exportação:
  Essa flag designa que a sub-rede seja anunciada da ACI ao vizinho de roteamento por meio do protocolo de roteamento dinâmico. Ele não deve ser ativado simultaneamente com a Sub-rede Externa para flag de EPG Externo, pois isso pode causar loops de roteamento de Camada 3. Como a ACI classifica a sub-rede como externa e também a anuncia de volta, isso pode levar a inconsistências de roteamento, apesar dos mecanismos de prevenção de loop nos protocolos de roteamento.

- Sub-rede de Controle de Rota Compartilhada:
  Esse sinalizador é definido quando o prefixo de sub-rede deve ser compartilhado em vários VRFs, permitindo o vazamento de rota entre os contextos.

- Sub-rede de Importação de Segurança Compartilhada:
  Usado em conjunto com o flag de sub-rede de controle de rota compartilhada, permite o compartilhamento de pcTags de segurança para sub-redes externas em diferentes VRFs, facilitando a aplicação consistente de políticas.

- Sub-rede de Controle de Rotas de Importação:
  Esse flag permite o controle granular sobre os prefixos recebidos dos vizinhos de

roteamento. Por padrão, a ACI aceita todos os anúncios de rotas de entrada; a habilitação desse sinalizador requer a ativação da aplicação de controle de rota para filtrar prefixos de entrada.

- Seção Agregada:
  Aplicável somente à sub-rede quad-0 (0.0.0.0/0), esta seção resume todos os prefixos no RIB para exportação ou importação agregada. Quando as sub-redes vazam para outros VRFs, elas são resumidas como rotas compartilhadas agregadas para otimizar as tabelas de roteamento.

Comandos de Verificação e Troubleshooting

Roteamento

Para começar, a rota deve estar presente na tabela de roteamento do VRF nos switches Border Leaf. Por exemplo, este comando mostra uma rota BGP no 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#
```

Isso confirma que a rota está instalada na tabela de roteamento VRF e está disponível para decisões de encaminhamento.

Classificação

Depois que a rota está presente na tabela de roteamento, a classificação determina como o tráfego é tratado com base na política. Na ACI, a classificação está vinculada ao ExEPG e suas sub-redes associadas.

Para validar a classificação de sub-rede em um ExEPG, o APIC pode ser consultado para a classe l3extInstP, que representa a ocorrência de EPG externo. Sua classe filha l3extSubnet lista as sub-redes configuradas nesse ExEPG. Por exemplo:

<#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#
```

Se nenhuma saída for retornada para a classe l3extSubnet, isso indica que nenhuma sub-rede está configurada no EPG externo. Sem as sub-redes configuradas, a ACI não pode associar um pcTag à sub-rede de tráfego de entrada, resultando no descarte do tráfego, apesar da rota existente na tabela de roteamento.

Outro aspecto importante a ser observado, é o escopo da sub-rede, que representa os flags definidos para a sub-rede em questão:

- Segurança de importação

A sub-rede foi sinalizada com Sub-rede Externa para EPG Externo.

- export-rtctrl

A sub-rede foi sinalizada com Controle de Rota de Exportação.

- import-rtctrl

A sub-rede foi sinalizada com Controle de Rota de Importação.

- segurança compartilhada

A sub-rede foi sinalizada com a Sub-rede de Importação de Segurança Compartilhada.

- shared-rtctrl

A sub-rede foi sinalizada com Controle de Rota Compartilhada.

Os protocolos de roteamento e os processos do plano de controle atualizam as tabelas de roteamento ao receberem um prefixo de um vizinho mencionado, que são então programados nas tabelas de encaminhamento de HAL L3. As rotas HAL L3 representam as rotas reais da camada 3 programadas nas tabelas de encaminhamento de hardware (ASICs) nos switches leaf. Essas rotas são derivadas dos protocolos de roteamento e dos cálculos da tabela de roteamento e são usadas para decisões de encaminhamento.

<#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#
```

Subsequentemente, quando uma sub-rede é configurada com o sinalizador Sub-rede Externa para EPG Externo em um ExEPG, um processo interno chamado Gerenciador de Políticas (policy-mgr) atualiza sua tabela de mapeamento de prefixo para pcTag com essa entrada de sub-rede e o pcTag associado. O Policy Manager funciona como o mecanismo de orquestração de política centralizada em malha, convertendo definições de política de alto nível em configurações acionáveis em toda a malha da ACI. Isso garante conectividade de aplicativos e comportamento de rede consistentes e seguros, aplicando os pcTags corretos para classificação de tráfego e decisões de encaminhamento com base nas sub-redes 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#
```

Isso confirma que o prefixo 172.16.1.0/24 está sendo anunciado pelo vizinho para o switch leaf de borda da ACI e a ACI classificou o prefixo abaixo de pcTag 32771

Contratos

Uma regra de zoneamento é o processo subjacente que aplica políticas de contrato entre EPGs (incluindo ExEPGs) na estrutura. O VNID (escopo) do VRF e o pcTag do EPG externo podem ser usados para definir e validar as regras de comunicação aplicadas entre os EPGs de origem e destino. Essencialmente, as regras de zoneamento traduzem relacionamentos de contrato de alto nível em regras específicas e aplicáveis programadas nos switches leaf.

Um aspecto importante a ser considerado é onde o contrato é instalado na malha. Por padrão, o VRF é configurado com a Direção de aplicação de controle de política definida como entrada. Essa configuração determina que a regra de zoneamento para um determinado contrato seja instalada no switch folha onde o ponto de extremidade de origem reside.

Para este exercício, o tráfego é recebido de uma L3Out, a regra de zoneamento é instalada na folha de borda que se conecta a essa L3Out, pois essa folha atua como a folha de origem para o tráfego que entra na malha.

<#root>

```
Leaf101#
```

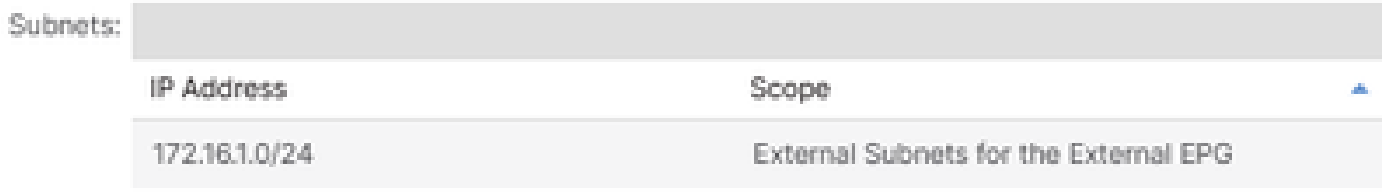
show zoning-rule scope 3047430 | egrep "Rule|---|32771"

```
+---------+--------+--------+----------+----------------+---------+---------+--------------------+------
| 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#
```

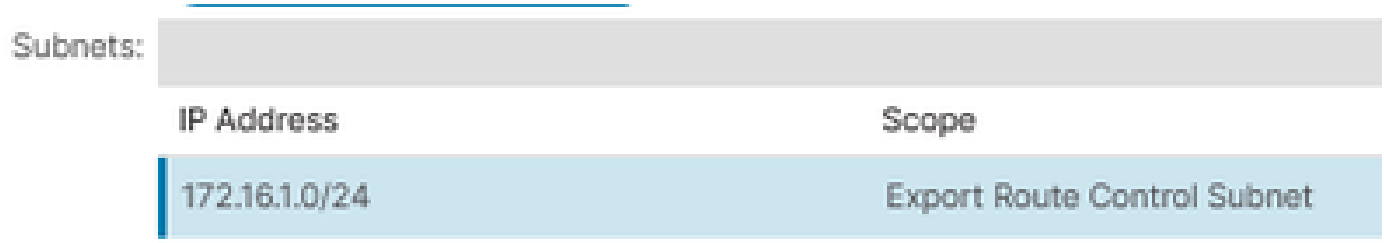
Roteamento de trânsito

O roteamento de trânsito permite que a estrutura atue como uma rede de trânsito anunciando rotas externas aprendidas de um L3Out para outro. Para configurar corretamente o roteamento de

trânsito, a sub-rede de entrada deve ser marcada com a sub-rede externa para o flag EPG externo.



Simultaneamente, a L3Out que anuncia esta sub-rede a outros peers externos deve ter o indicador Export Route Control Subnet ativado na sub-rede correspondente. Esse flag permite que a sub-rede seja redistribuída e anunciada fora da estrutura por meio do protocolo de roteamento configurado nessa L3Out.



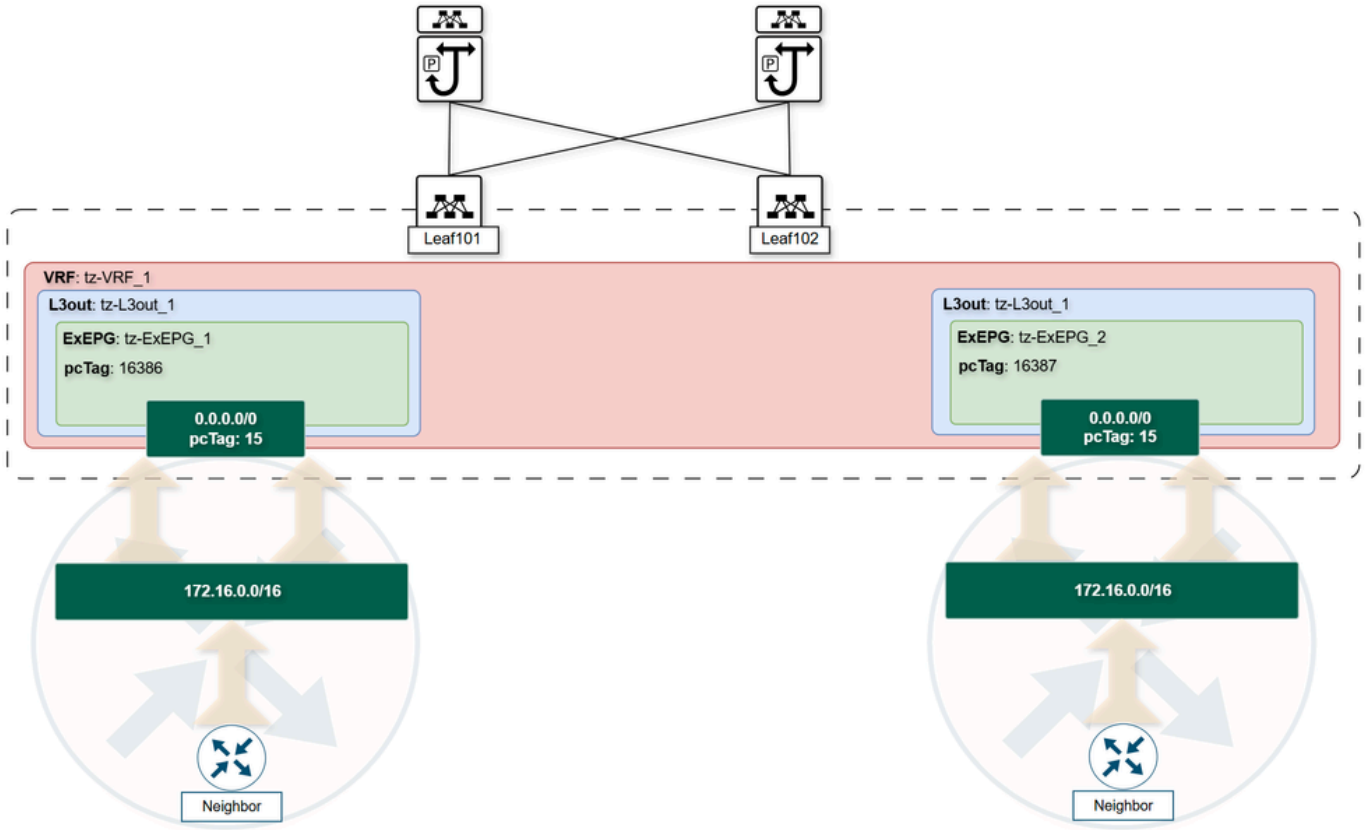
Por fim, um contrato entre o L3out recebido e o L3out de exportação precisa ser configurado para concluir o processo de distribuição da rota.

Problemas comuns na classificação de EPG externo de sub-rede

pcTag 15

Anteriormente, neste documento, foi declarado que a sub-rede do ExEPG o ajuda a classificar as sub-redes no pcTag correto por motivos de aplicação da política. Uma exceção importante para essa classificação é a sub-rede quad-0 (0.0.0.0/0) quando configurada com o sinalizador Sub-rede Externa para EPG Externo. Essa sub-rede recebe sempre o pcTag 15 reservado, atuando efetivamente como um curinga para todo o tráfego externo em um VRF.

Este diagrama representa o problema de configuração do quad-0 com sub-rede externa para EPG externo em vários ExEPGs dentro do mesmo VRF:



- A sub-rede quad-0 é frequentemente confundida com a rota padrão. Embora isso seja algumas vezes verdade, como quando um vizinho de roteamento dinâmico anuncia apenas a rota padrão para a ACI L3Out, a função da sub-rede quad-0 na ACI é mais ampla como uma classificação catch-all.
- É uma prática comum configurar vários ExEPGs com a sub-rede quad-0 para aceitar todos os prefixos anunciados por um vizinho. Embora isso atinja o objetivo de ampla aceitação, pode levar a um roteamento assimétrico inesperado quando vários ExEPGs com quad-0 são configurados dentro do mesmo VRF. Quando vários ExEPGs dentro do mesmo VRF são configurados com quad-0 como uma sub-rede externa, a ACI não pode selecionar deterministicamente qual L3Out usar para uma sub-rede de destino específica. Em vez disso, ele seleciona um L3Out arbitrariamente.
- Esse comportamento pode causar roteamento assimétrico, tráfego intermitente ou até mesmo quedas de tráfego se a L3Out selecionada aleatoriamente não tiver os contratos necessários para permitir a comunicação.

Sub-redes Sobrepostas

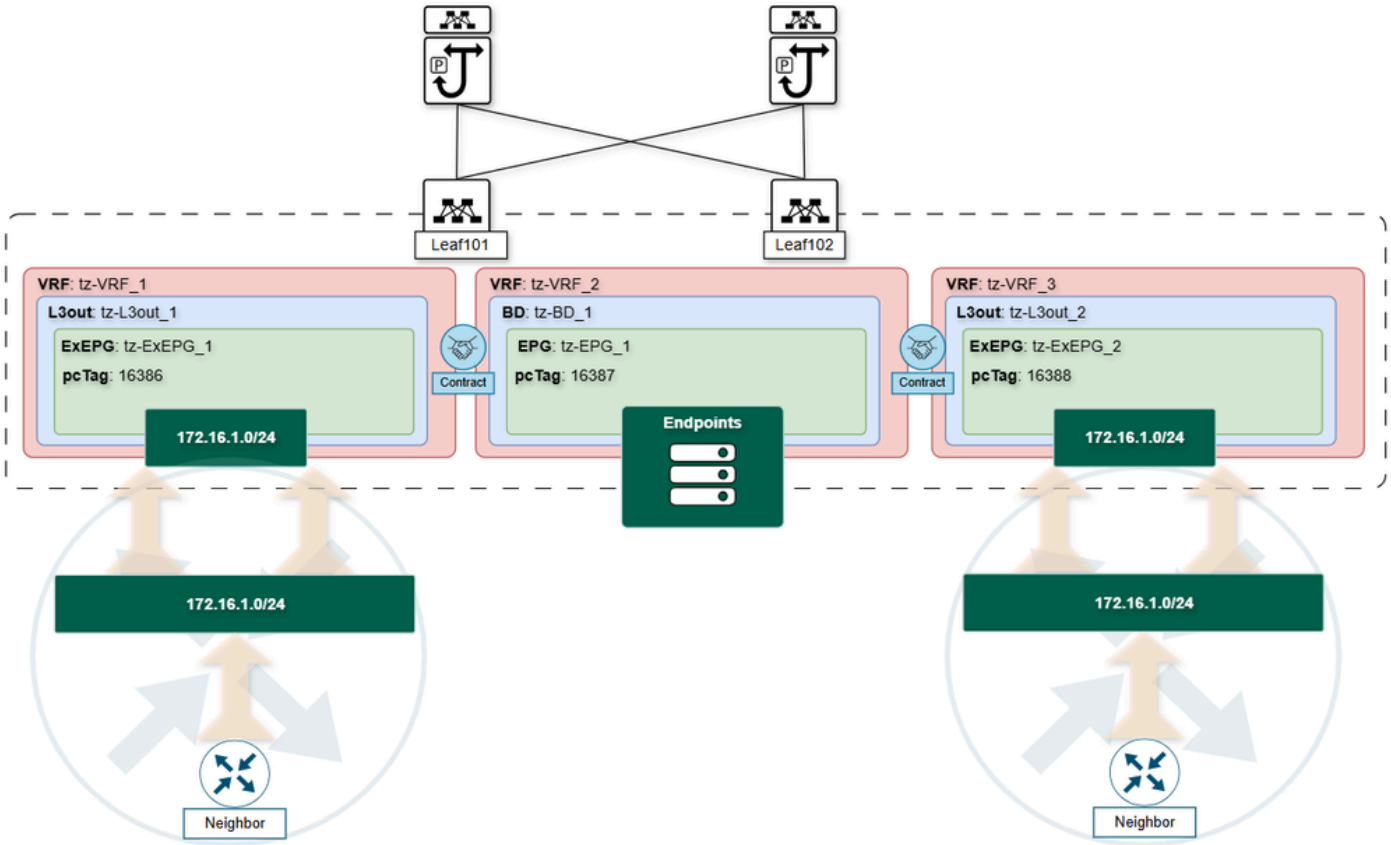
A configuração de sub-redes idênticas em diferentes ExEPGs não é permitida. A tentativa de fazer isso aciona a falha "F0467: Entrada de prefixo já usada em outro EPG", evitando a duplicação de sub-rede em um VRF.

No entanto, sub-redes sobrepostas podem existir em diferentes VRFs porque cada VRF mantém um contexto de tabela de roteamento independente. Essa separação permite que a mesma sub-rede seja configurada em ExEPGs pertencentes a VRFs diferentes. Apesar disso, é essencial ter cuidado ao executar vazamento de rota VRF envolvendo essas sub-redes sobrepostas, pois isso pode levar a decisões de encaminhamento assimétrico devido a conflitos na classificação de sub-

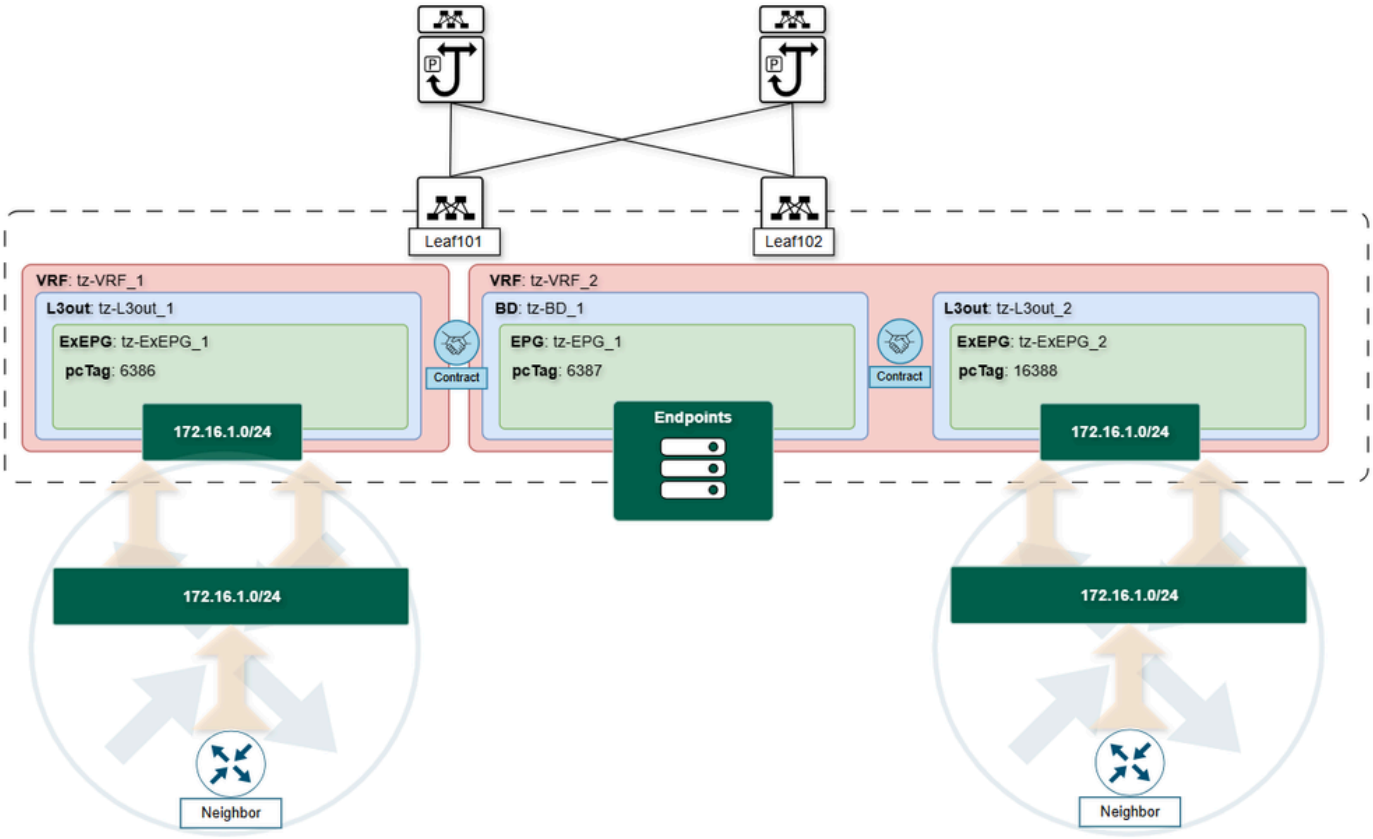
rede (pcTag) versus informações de roteamento (RIB).

Os principais cenários incluem:

- Vazamento de rota de dois VRFs em um terceiro VRF:
  Quando dois VRFs vazam a mesma sub-rede em um terceiro VRF, o VRF receptor instala a primeira sub-rede que recebe com base na política compartilhada do APIC. Se o switch de folha que lida com esse VRF for reinicializado ou a eleição de roteamento for alterada, a tabela de roteamento poderá ser atualizada para uma L3Out diferente, causando um comportamento de encaminhamento inconsistente.



- ExEPG de Saída Local para VRF L3Sobreposição com Sub-redes Vazadas:
  Em designs nos quais o vazamento de rota é usado, se um ExEPG L3Out local for configurado com a mesma sub-rede de uma sub-rede vazada, a entrada de roteamento local sempre terá precedência sobre as rotas vazadas.



Essas situações destacam que os problemas de encaminhamento assimétrico surgem da camada de decisão de classificação e encaminhamento, não da própria tabela de roteamento. Enquanto a classificação de sub-rede associa uma sub-rede a um L3Out e ExEPG específico para aplicação de política, a tabela de roteamento pode apontar para um destino L3Out diferente. Essa incompatibilidade pode fazer com que o tráfego seja encaminhado de forma inconsistente, levando a possíveis problemas de conectividade ou lacunas de aplicação de política.

Alteração de Comportamento Padrão do Controle de Rotas de Importação

Por padrão, a ACI aceita todos os anúncios de rota de entrada dos vizinhos. Para controlar quais prefixos são aceitos, você deve habilitar a Imposição de Controle de Rota: entrada no objeto raiz L3Out:

Navegue para Locatários > [nome do locatário] > Rede > L3outs > [nome do L3out].

Esta ação cria um mapa de rota sob o protocolo de roteamento selecionado.

<#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#

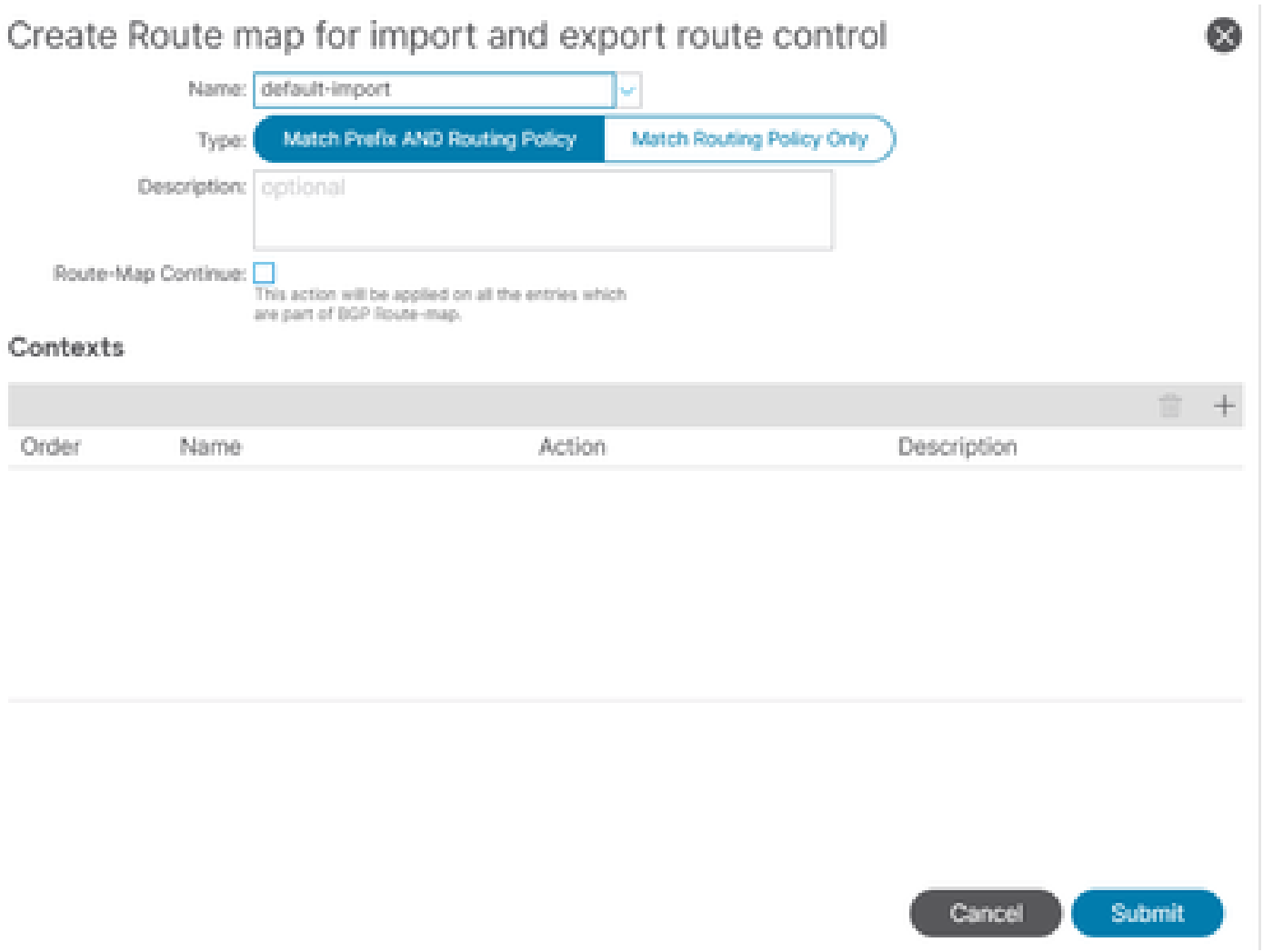
show ip prefix-list IPv4-peer49155-2981888-exc-ext-inferred-import-dst

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

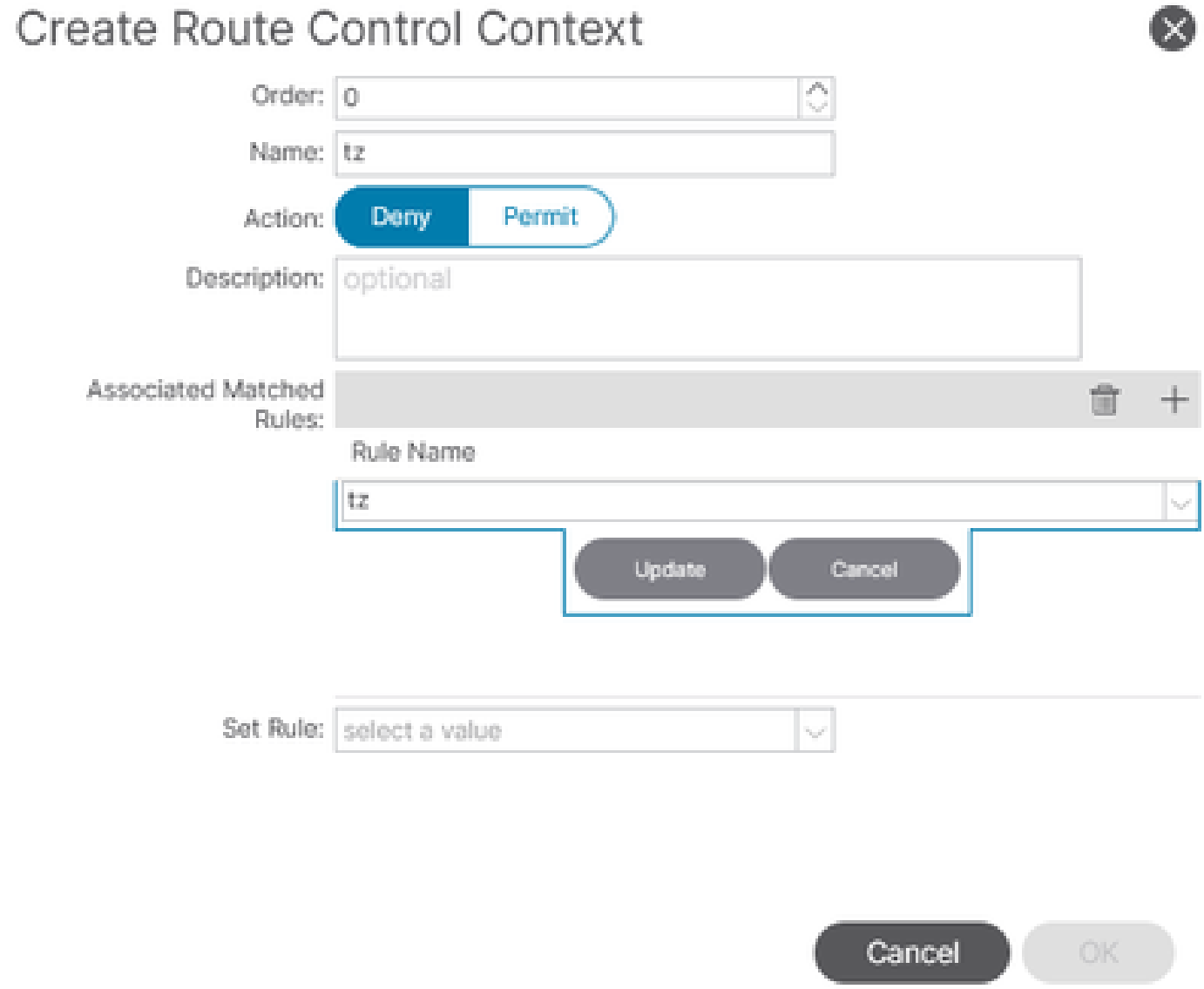
Por padrão, esse mapa de rota de importação permite todos os prefixos de entrada. Para modificar esse comportamento:

Navegue até Locatários > [nome do locatário] > Rede > L3outs > [nome do L3out] > Mapa de rotas para controle de rotas de importação e exportação

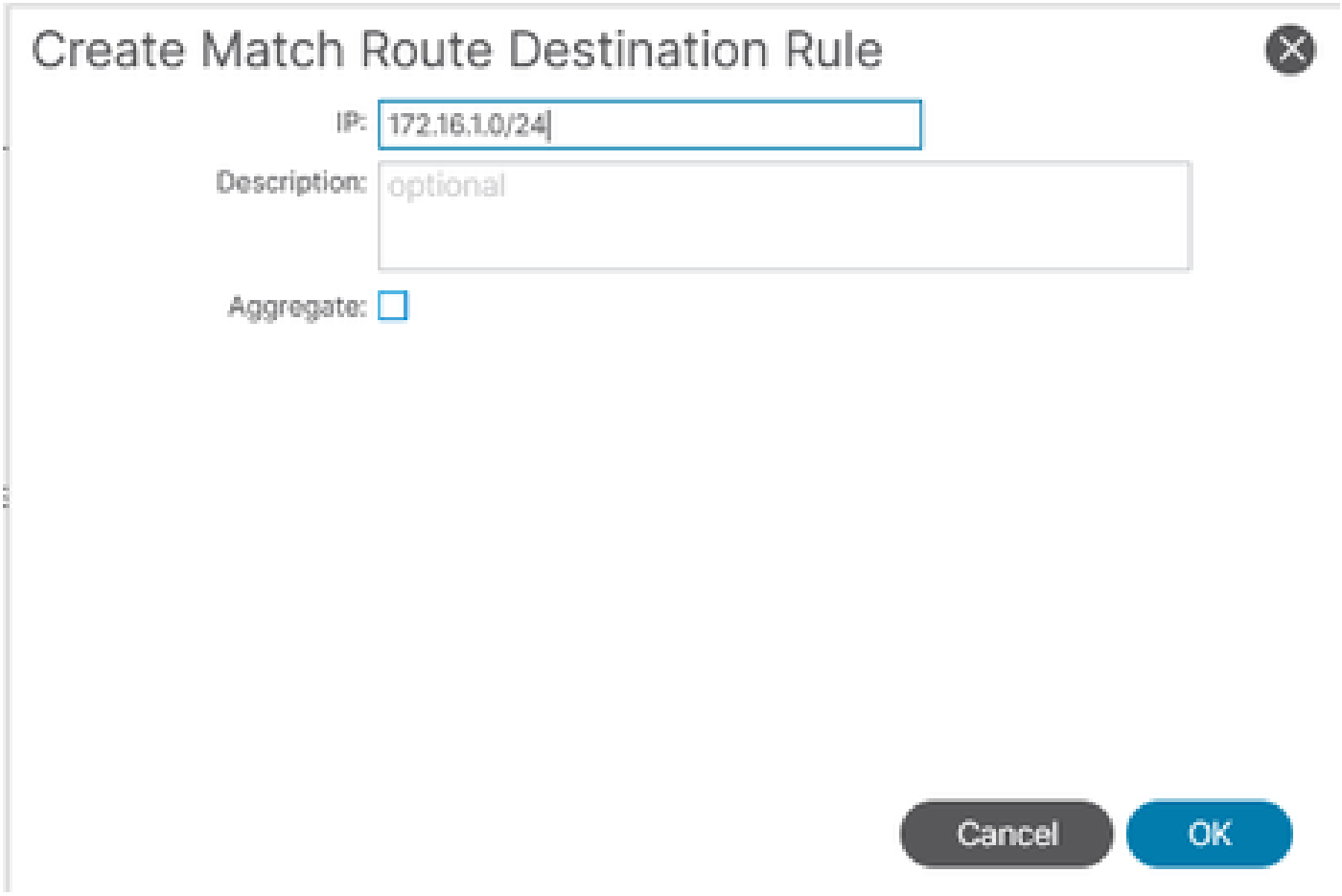
Selecione o mapa de rota de importação padrão ou crie um novo usando o ícone gear na parte superior direita.



Na seção Contexto, crie uma nova Regra Associada Correspondente.



Na seção Regras de Correspondência, role até Prefixo de Correspondência e adicione as sub-redes específicas que você deseja controlar.



Depois de enviar as políticas, a ação importar mapa de rota é alterada de acordo, reforçando a filtragem de prefixo desejada.

<#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#
```

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.