ACIのL3Outサブネット分類のトラブルシューティング

内容

はじめに

略語

外部EPG分類

- 外部EPGサブネットフラグ

検証とトラブルシューティングに関するコマンド

- ルーティング
- 分類
- 契約
- 中継ルーティング

サブネット外部EPG分類の一般的な問題

- pcTag 15
- 重複するサブネット

ルート制御のデフォルト動作の変更のインポート

はじめに

このドキュメントでは、Cisco ACIのL3Out EPG内の外部サブネットの分類について説明します。

略語

- BD：ブリッジドメイン
- EPG：エンドポイントグループ
- ExEPG：外部エンドポイントグループ
- RIB：ルーティング情報ベース
- VRF:Virtual Routing and Forwarding(VRF)
- クラスID:EPGを識別するタグ

外部EPG分類

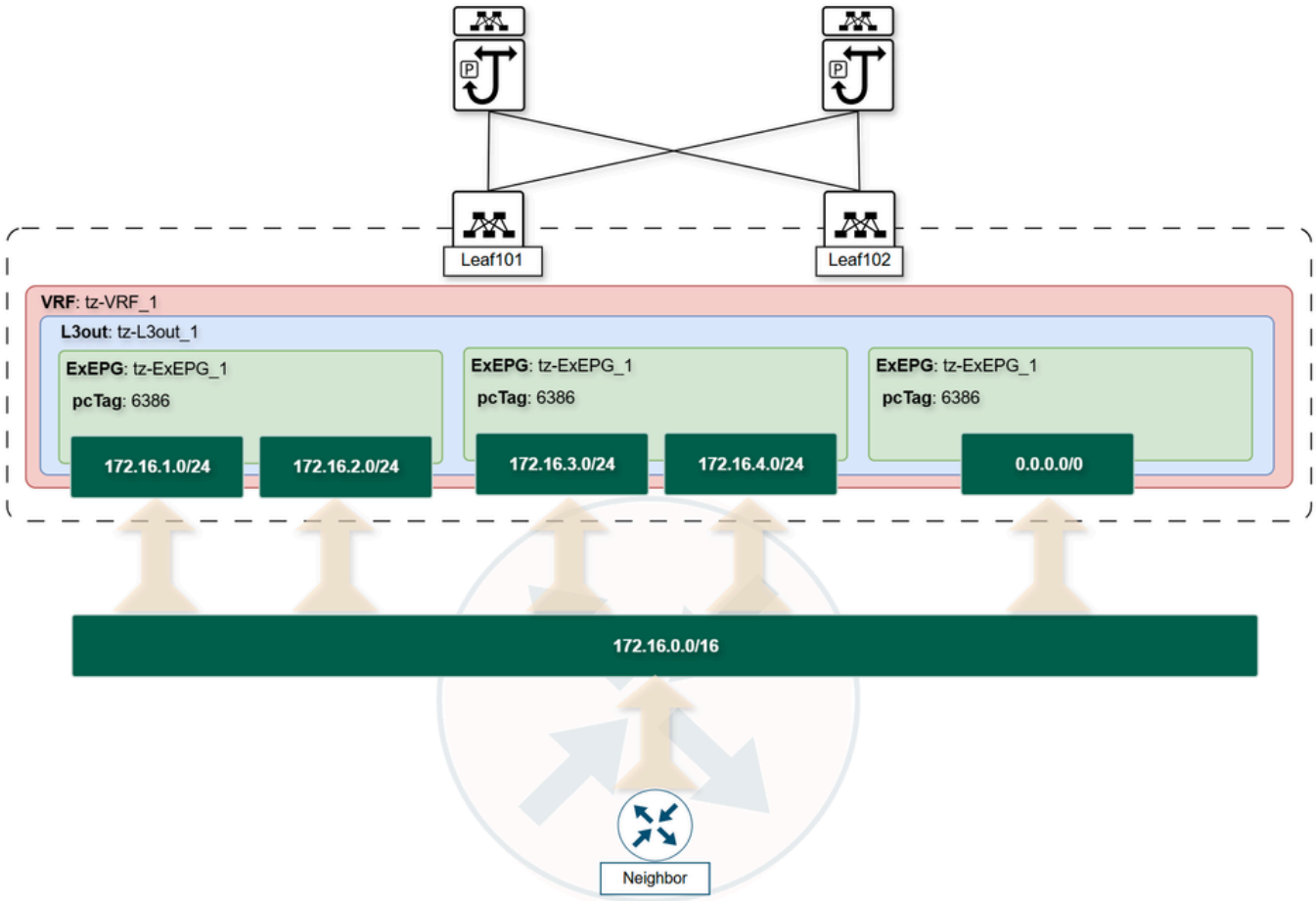
Cisco ACIの外部EPGは、L3Out経由で接続された外部ルーテッドネットワークを表します。通常のEPGがエンドポイントを分類する方法と同様に、外部EPGはVRFごとに外部サブネットを分類します。つまり、各サブネットはVRFコンテキスト内で一意である必要があります。

一般的に、外部EPGサブネットにはダイナミックルーティングプロトコルで受け入れられるプレフィックスだけが含まれていると誤解されています。ただし、L3Outが作成されると、着信アドバタイズメントをフィルタリングするデフォルトルートマップがあります。そのため、ダイナミックルーティングプロトコルによってアドバタイズされたすべてのプレフィックスはデフォルト

で受け入れられます。ExEPGでサブネットを定義する主な目的は、契約の適用とポリシーの適用のために、ExEPGに含まれるサブネットに一意のpcTagを割り当てることだけです。

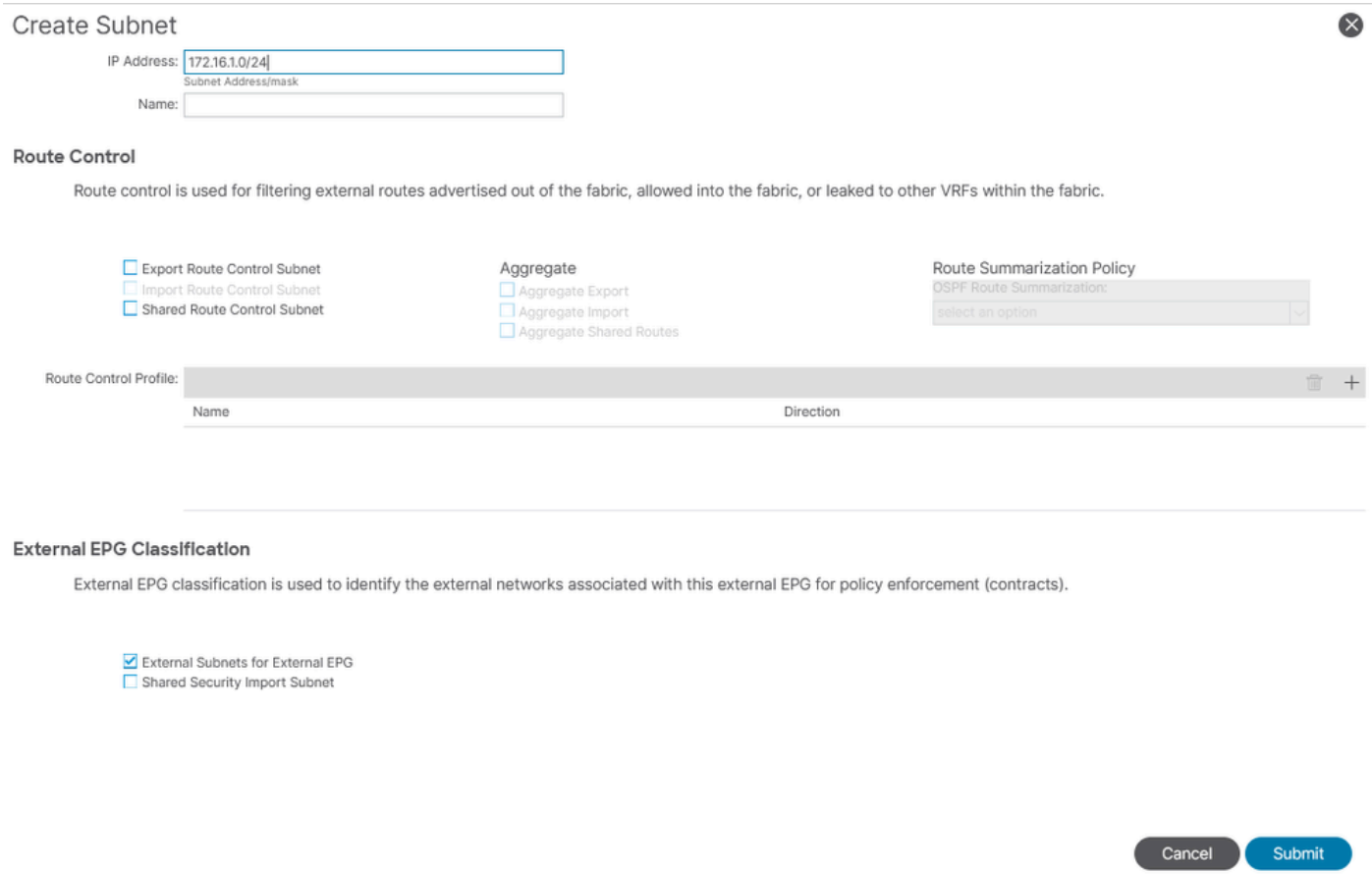
この分類により、きめ細かなポリシー制御が可能になります。たとえば、1つの外部ネイバーがACIにスーパーネットをアドバタイズし、その後ACIを複数のExEPGにセグメント化できます。これにより、特定の内部EPGが指定された外部サブネットとだけ通信することを許可したり、最終宛先に到達する前に特定のプレフィックス宛てのトラフィックをPBRノードにリダイレクトしたりするなど、異なる契約アクションを異なるサブネットに適用できます。

この図は、Cisco ACIが外部EPGに基づいて外部サブネットを分類し、トラフィックを正確にセグメント化して契約を適用する方法を示しています。



外部EPGサブネットフラグ

ACIでExEPG内の外部プレフィックスを分類および管理するには、ExEPGでサブネットプレフィックスを作成するときに特定のサブネットフラグを設定します。このセクションでは、各フラグとその使用目的について詳しく説明します。



- 外部EPGの外部サブネット：
  このフラグは、サブネットがACIファブリックの外部にあり、ブリッジドメインまたはEPG内で設定されていないことを示します。プレフィックスがルーティングネイバーによってアドバタイズされるか、RIBに静的に挿入される場合にのみ使用する必要があります。このフラグはデフォルトで有効になっています。

- ルート制御サブネットのエクスポート：
  このフラグは、ダイナミックルーティングプロトコルを介して、サブネットがACIからルーティングネイバーにアドバタイズされることを示します。レイヤ3ルーティングループを引き起こす可能性があるため、外部EPG用の外部サブネットのフラグと同時に有効にしないでください。ACIはサブネットを外部として分類し、またアドバタイズして戻すため、ルーティングプロトコルのループ回避メカニズムにもかかわらず、ルーティングの不整合が発生する可能性があります。

- 共有ルート制御サブネット：
  このフラグは、サブネットプレフィックスを複数のVRFで共有し、コンテキスト間でのルートの漏洩を可能にする場合に設定します。

- 共有セキュリティインポートサブネット：
  共有ルート制御サブネットフラグと組み合わせて使用することで、異なるVRF間で外部サブネットのセキュリティpcTagを共有し、一貫性のあるポリシー適用を促進します。

- ルート制御サブネットのインポート：
  このフラグにより、ルーティングネイバーから受信するプレフィックスをきめ細かく制御できます。デフォルトでは、ACIはすべての着信ルートアドバタイズメントを受け入れます。

このフラグを有効にするには、ルート制御適用をアクティブにして着信プレフィックスをフィルタリングする必要があります。

- 集約セクション：
  このセクションでは、集約の工クスポートまたはインポート用にRIB内のすべてのプレフィックスの概要を示します。これは、quad-0(0.0.0.0/0)サブネットにのみ適用されます。サブネットが他のVRFにリークされると、集約された共有ルートとして集約され、ルーティングテーブルが最適化されます。

検証とトラブルシューティングに関するコマンド

ルーティング

まず、境界リーフスイッチのVRFのルーティングテーブルにルートが存在する必要があります。たとえば、次のコマンドはVRF tz:tz-VRF_1内のBGPルートを示します。

```
<#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#
```

これにより、ルートがVRFルーティングテーブルにインストールされ、転送の決定に使用できることを確認できます。

分類

ルートがルーティングテーブルに存在すると、分類によってポリシーに基づいてトラフィックの処理方法が決定されます。ACIでは、分類はExEPGとそれに関連付けられたサブネットに関連付けられています。

ExEPGでサブネット分類を検証するには、外部EPGインスタンスを表すl3extInstPクラスについ

てAPICに照会できます。その子クラスl3extSubnetは、そのExEPGの下で設定されているサブネットをリストします。例：

<#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#
```

l3extSubnetクラスに対して出力が返されない場合は、外部EPGにサブネットが設定されていないことを示しています。サブネットが設定されていないと、ACIはpcTagを着信トラフィックサブネットに関連付けることができず、ルーティングテーブルにルートが存在するにもかかわらず、トラフィックがドロップされます。

もう1つ注意すべき重要な点は、サブネットのスコープです。これは、対象のサブネットに設定されているフラグを表します。

- インポートセキュリティ

このサブネットには、外部EPG用の外部サブネットというフラグが付いています。

- エクスポートrtctrl

このサブネットにはエクスポートルート制御のフラグが付いています。

- インポートRTCTRL

このサブネットにはインポートルート制御のフラグが付いています。

- 共有セキュリティ

このサブネットには、Shared Security Import Subnetというフラグが付いています。

- 共有RTCTRL

サブネットには共有ルート制御のフラグが付いています。

ルーティングプロトコルとコントロールプレーンプロセスは、指定されたネイバーからプレフィクスを受信するとルーティングテーブルを更新し、そのプレフィクスはHAL L3転送テーブルにプログラムされます。HAL L3ルートは、リーフスイッチのハードウェア転送テーブル(ASIC)にプログラムされた実際のレイヤ3ルートを表します。これらのルートは、ルーティングプロトコルとルーティングテーブルの計算から取得され、転送の決定に使用されます。

```
<#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#
```

その後、サブネットがExEPGの「外部EPG用の外部サブネット」フラグを使用して設定されると、ポリシーマネージャ(policy-mgr)と呼ばれる内部プロセスは、このサブネットエントリと関連するpcTagを使用して、プレフィクスとpcTagのマッピングテーブルを更新します。Policy Managerは、ファブリックの中央集中型ポリシーオーケストレーションエンジンとして機能し、高レベルのポリシー定義をACIファブリック全体で実用的な構成に変換します。これにより、設定された外部サブネットに基づいてトラフィックの分類と転送の決定に対して正しいpcTagが適用されるため、アプリケーションの接続とネットワーク動作の一貫性と安全性が確保されます。

```
<#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#
```

これにより、プレフィックス172.16.1.0/24がネイバーによってACI境界リーフスイッチにアドバタイズされ、ACIがそのプレフィックスをpcTag 32771に分類したことが確認できます

契約

ゾーニング・ルールは、ファブリック内のEPG（ExEPGを含む）間で契約ポリシーを適用するための基盤となるプロセスです。外部EPGのVRF VNID（スコープ）とpcTagを使用して、送信元EPGと宛先EPGの間に適用される通信ルールを定義および検証できます。基本的に、ゾーン分割ルールは、ハイレベルな契約関係を、リーフスイッチ上にプログラムされた特定の強制可能なルールに変換します。

考慮すべき重要な点は、契約がファブリックのどこにインストールされているかということです。デフォルトでは、VRFはPolicy Control Enforcement Direction(PCP)をingressに設定して設定されます。この設定により、特定のコントラクトのゾーン分割ルールが、ソースエンドポイントが存在するリーフスイッチにインストールされることが決定されます。

この例では、トラフィックはL3Outから着信します。このリーフはファブリックに入るトラフィックのソースリーフとして機能するため、ゾーン分割ルールはそのL3Outに接続するボーダーリーフにインストールされます。

<#root>

Leaf101#

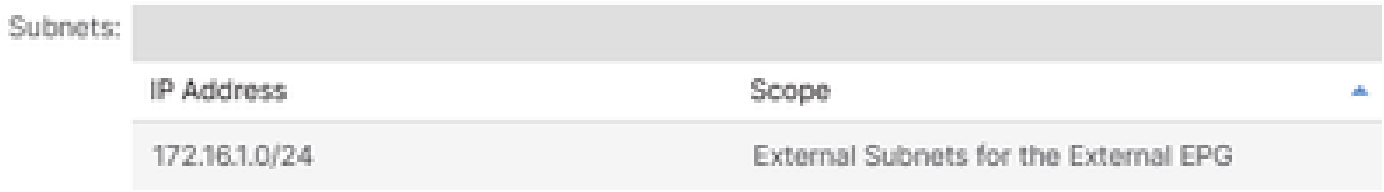
show zoning-rule scope 3047430 | egrep "Rule|---|32771"

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

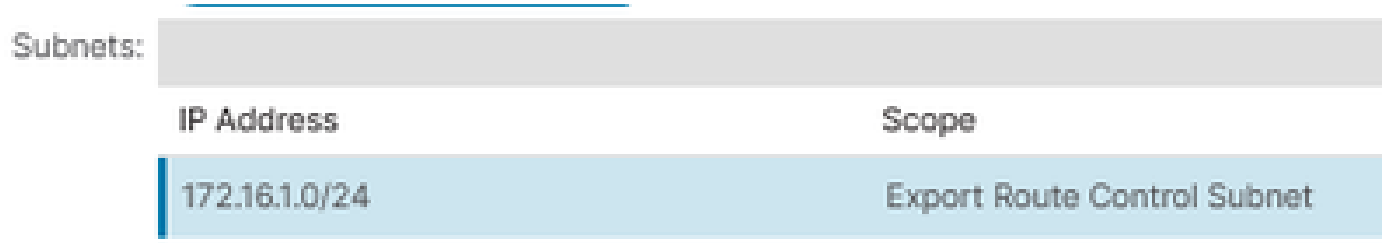
中継ルーティング

トランジットルーティングでは、あるL3Outから学習した外部ルートを別のL3Outにアドバタイズすることにより、ファブリックをトランジットネットワークとして機能させることができます。トランジットルーティングを適切に設定するには、着信サブネットを外部EPG用の外部サブネッ

トのフラグでマークする必要があります。



同時に、このサブネットを他の外部ピアにアドバタイズするL3Outでは、対応するサブネットでExport Route Control Subnetフラグを有効にする必要があります。このフラグを使用すると、そのL3Outで設定されたルーティングプロトコルを介して、サブネットをファブリックから再配布し、アドバタイズすることができます。



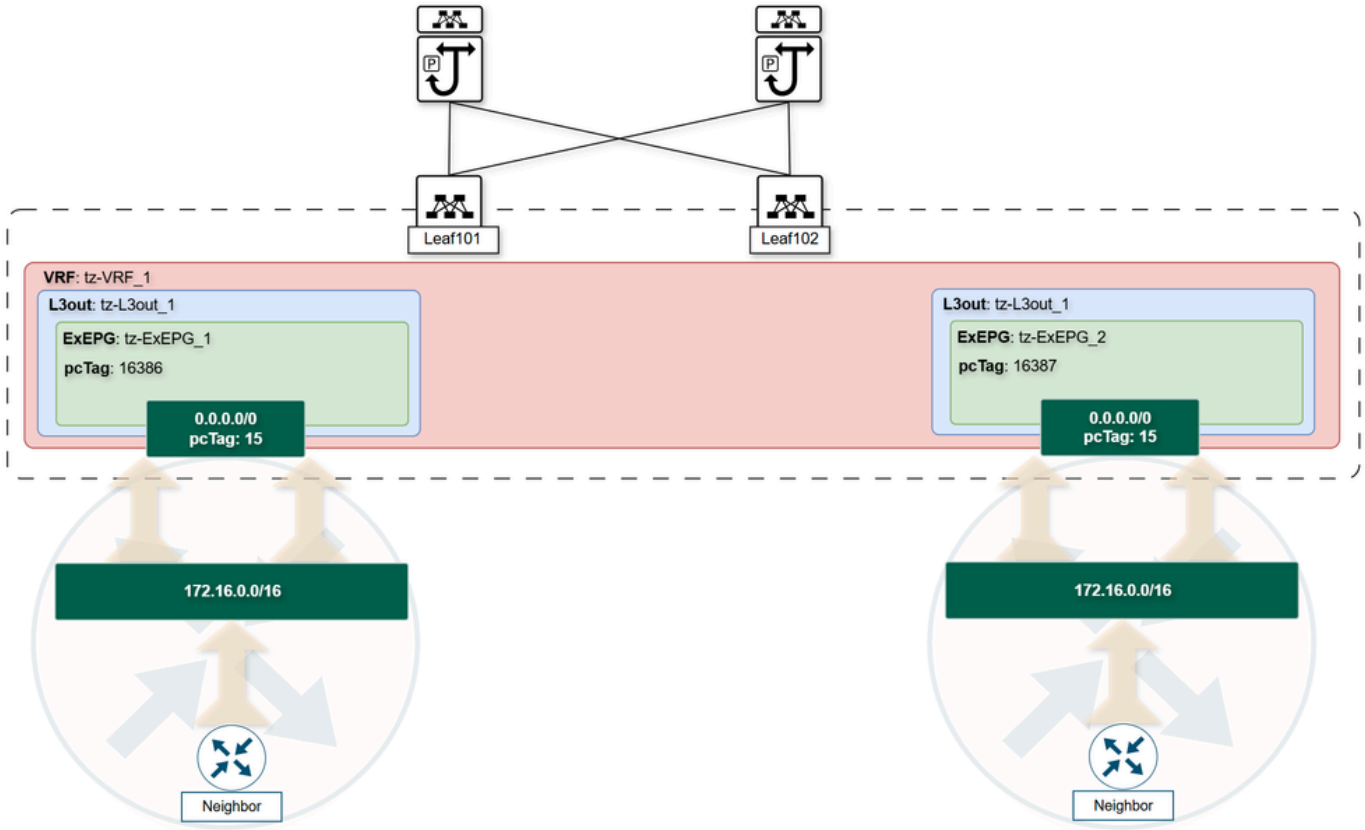
最後に、ルートを分散させるプロセスを完了するために、受信L3outとエクスポートL3outの間のコントラクトを設定する必要があります。

サブネット外部EPG分類の一般的な問題

pcTag 15

以前は、このドキュメントで、ExEPGサブネットは、ポリシー適用上の理由から、正しいpcTagでサブネットを分類するのに役立つと述べられていました。 この分類の重要な例外は、External Subnet for External EPGフラグを設定した場合のquad-0 subnet(0.0.0.0/0)です。このサブネットには常に予約済みのpcTag 15が割り当てられ、VRF内のすべての外部トラフィックに対してワイルドカードとして効果的に機能します。

次の図は、同じVRF内の複数のExEPGで外部EPG用の外部サブネットを使用してquad-0を設定する際に発生する問題を示しています。



- quad-0サブネットは、デフォルトルートと間違われることがよくあります。ダイナミックルーティングネイバーがACI L3Outへのデフォルトルートだけをアドバタイズする場合など、これが当てはまる場合もありますが、ACIにおけるクワッド0サブネットの役割は、あらゆるものに対応できる分類として広い方が考えられます。
- 一般的には、クワッド0サブネットを持つ複数のExEPGを設定して、ネイバーからアドバタイズされたすべてのプレフィックスを受け入れます。これにより幅広く受け入れられるという目標は達成されますが、同じVRF内でquad-0を使用する複数のExEPGが設定されている場合は、予期しない非対称ルーティングが発生する可能性があります。 同じVRF内の複数のExEPGが外部サブネットとしてquad-0で設定されている場合、ACIは特定の宛先サブネットに使用するL3Outを決定論的に選択できません。代わりに、1つのL3Outを任意に選択します。
- この動作により、ランダムに選択されたL3Outに通信を許可するために必要な契約がない場合は、非対称ルーティングが発生したり、トラフィックが断続的になったり、トラフィックが廃棄される可能性があります。

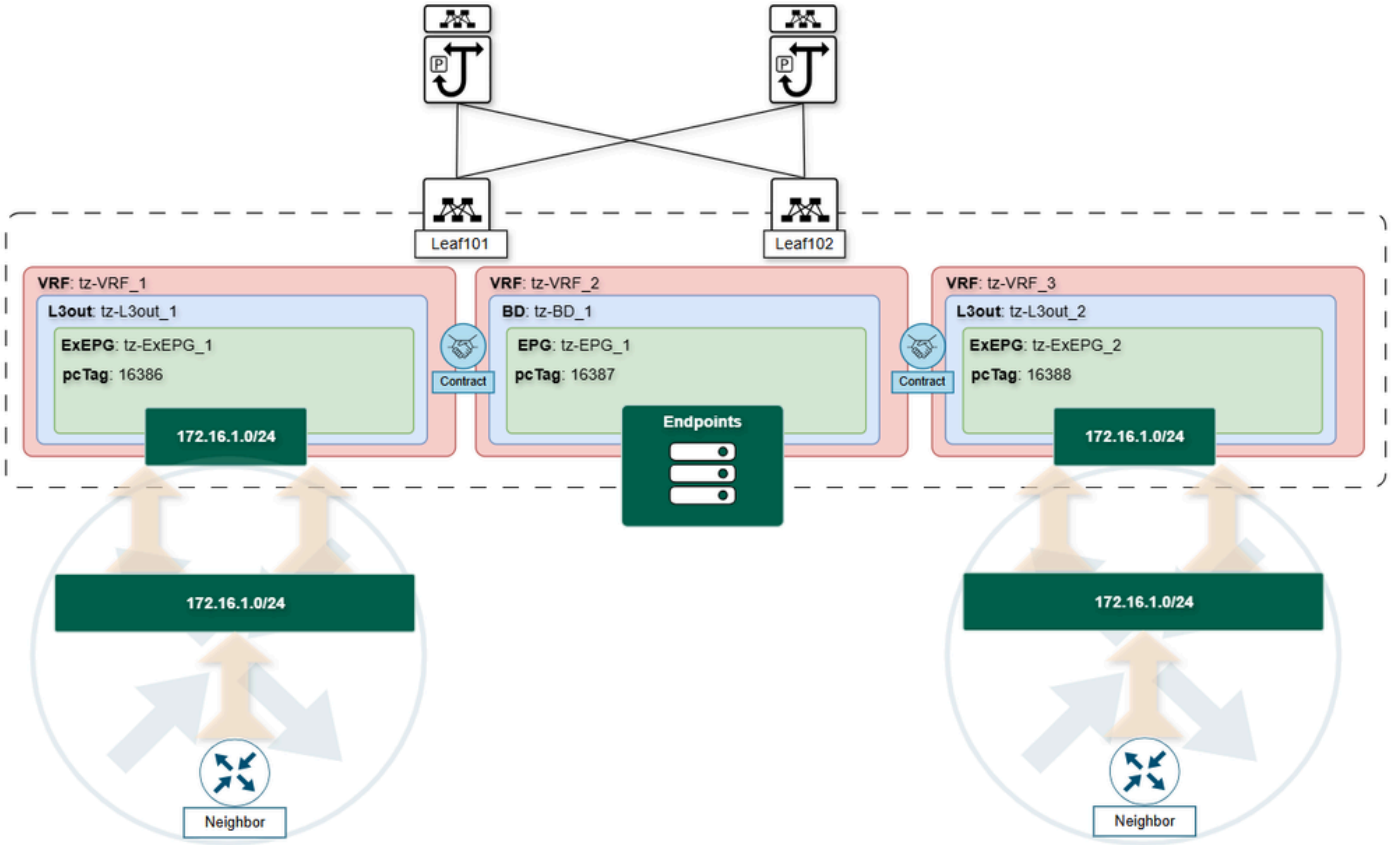
重複するサブネット

異なるExEPG間で同一のサブネットを設定することはできません。これを試みると、障害「F0467: Prefix Entry Already Used in Another EPG」がトリガーされ、VRF内でのサブネットの重複が防止されます。

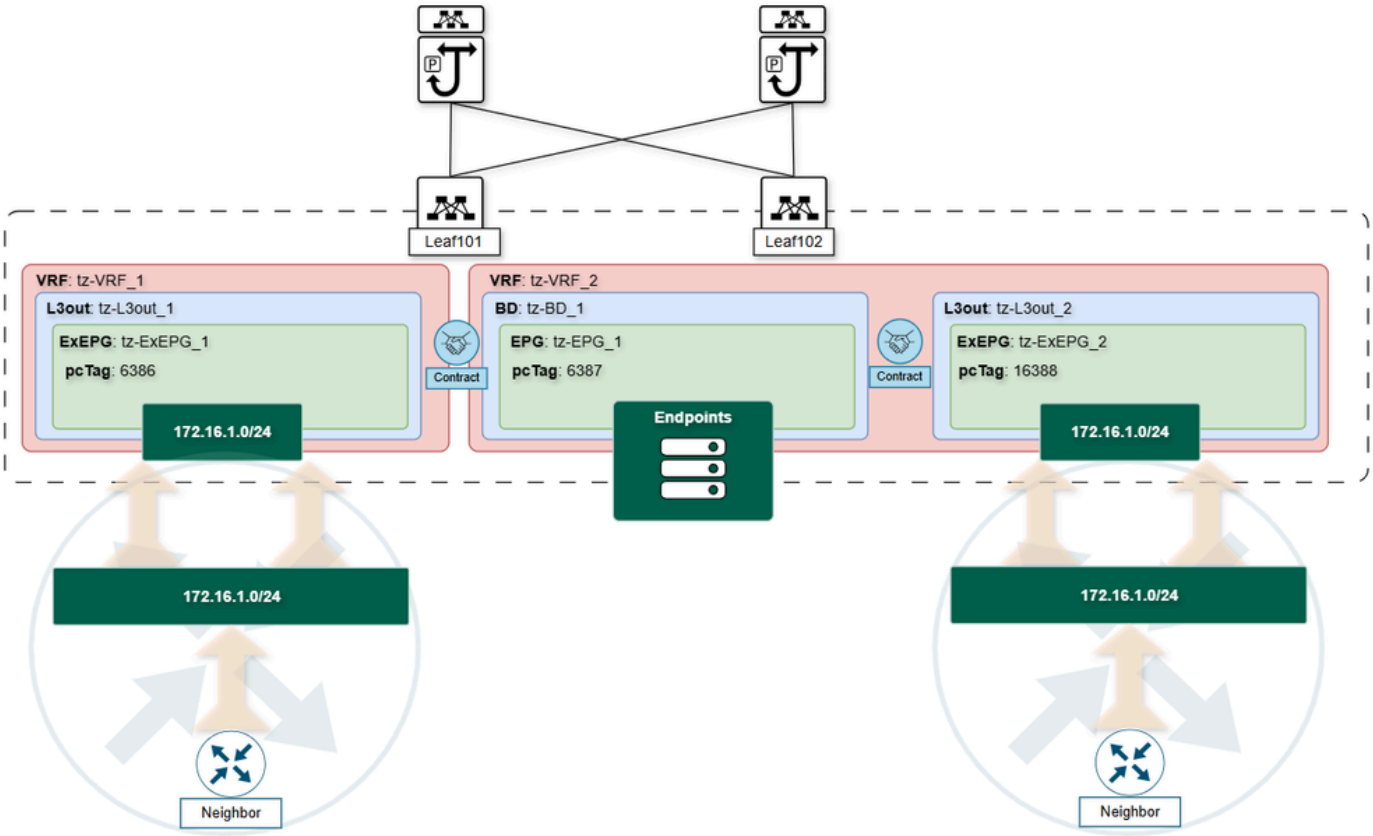
ただし、各VRFが独立したルーティングテーブルコンテキストを維持するため、異なるVRF間でサブネットが重複する可能性があります。この分離により、異なるVRFに属するExEPGで同じサブネットを設定できます。ただし、これらの重複サブネットに関係するVRFルート漏出を実行する場合は、サブネット分類(pcTag)とルーティング情報(RIB)の競合が原因で非対称フォワーディングの決定が発生する可能性があるため、注意が必要です。

主なシナリオは次のとおりです。

- 2つのVRFから3番目のVRFへのルートの漏洩：
  2つのVRFが同じサブネットを3つ目のVRFにリークすると、受信側VRFはAPICからの共有ポリシーに基づいて、受信した最初のサブネットをインストールします。このVRFを処理するリーフスイッチがリブートするか、またはルーティング選択が変更されると、ルーティングテーブルが異なるL3Outに更新され、一貫性のない転送動作が発生する可能性があります。



- リークされたサブネットとオーバーラップするローカルからVRFへのL3Out ExEPG:
  ルート漏出を使用する設計では、ローカルL3Out ExEPGが漏出サブネットと同じサブネットで設定されている場合、ローカルルーティングエントリは常に漏出ルートよりも優先されます。



これらの状況は、非対称フォワーディングの問題が、ルーティングテーブル自体ではなく、分類およびフォワーディングの意思決定レイヤから発生していることを示しています。サブネット分類では、ポリシーを適用するためにサブネットを特定のL3OutおよびExEPGに関連付けますが、ルーティングテーブルは別のL3Out宛先を指すことができます。このミスマッチにより、トラフィックの転送に一貫性が失われ、接続の問題やポリシー適用のギャップが生じる可能性があります。

ルート制御のデフォルト動作の変更のインポート

デフォルトでは、ACIはネイバーからの着信ルートアドバタイズメントをすべて受け入れます。受け入れるプレフィックスを制御するには、L3OutルートオブジェクトでRoute Control Enforcement: inboundを有効にする必要があります。

Tenants > [tenant name] > Networking > L3outs > [L3out name]の順に移動します。

この操作により、選択したルーティングプロトコルの下にルートマップが作成されます。

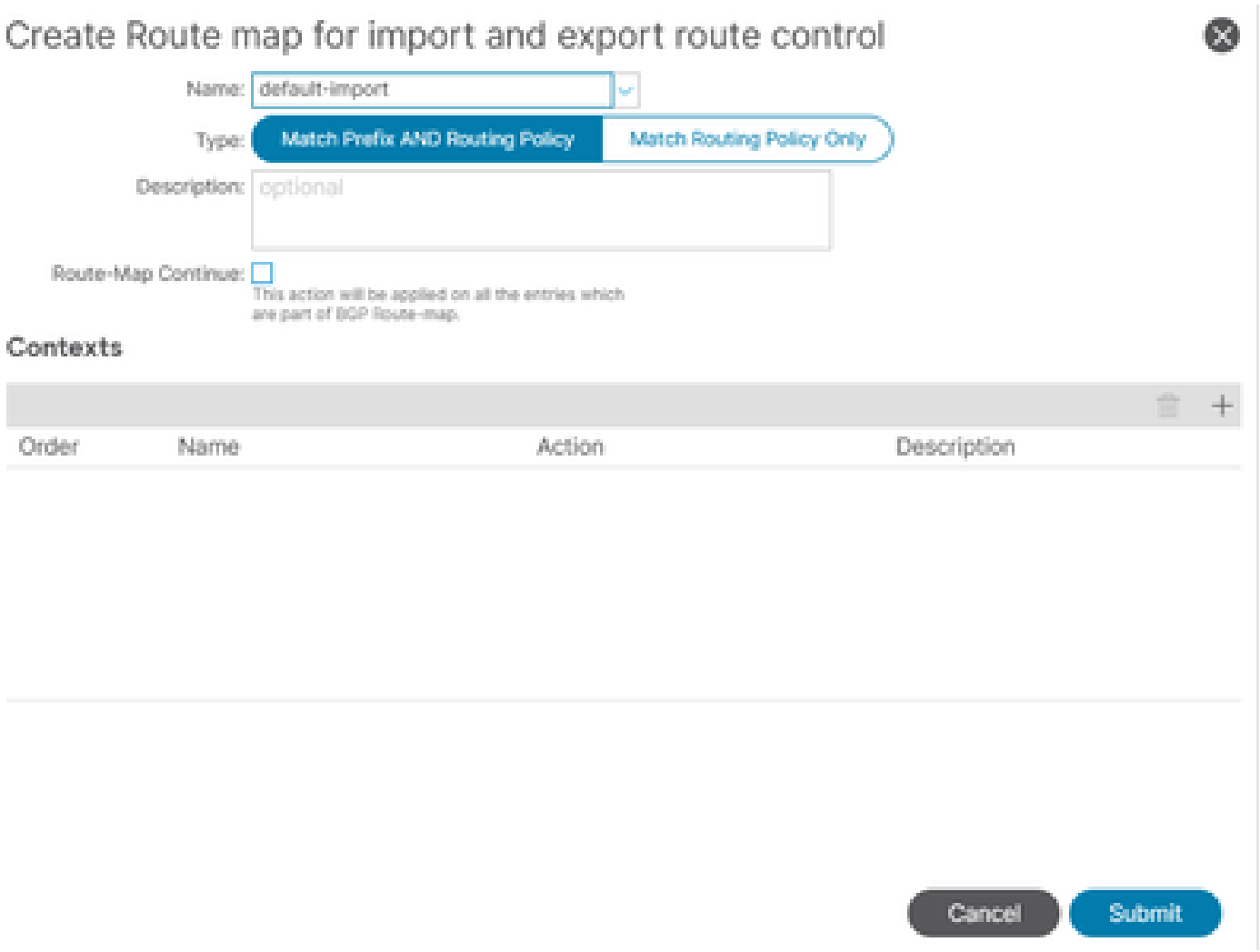
<#root>

```
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#
```

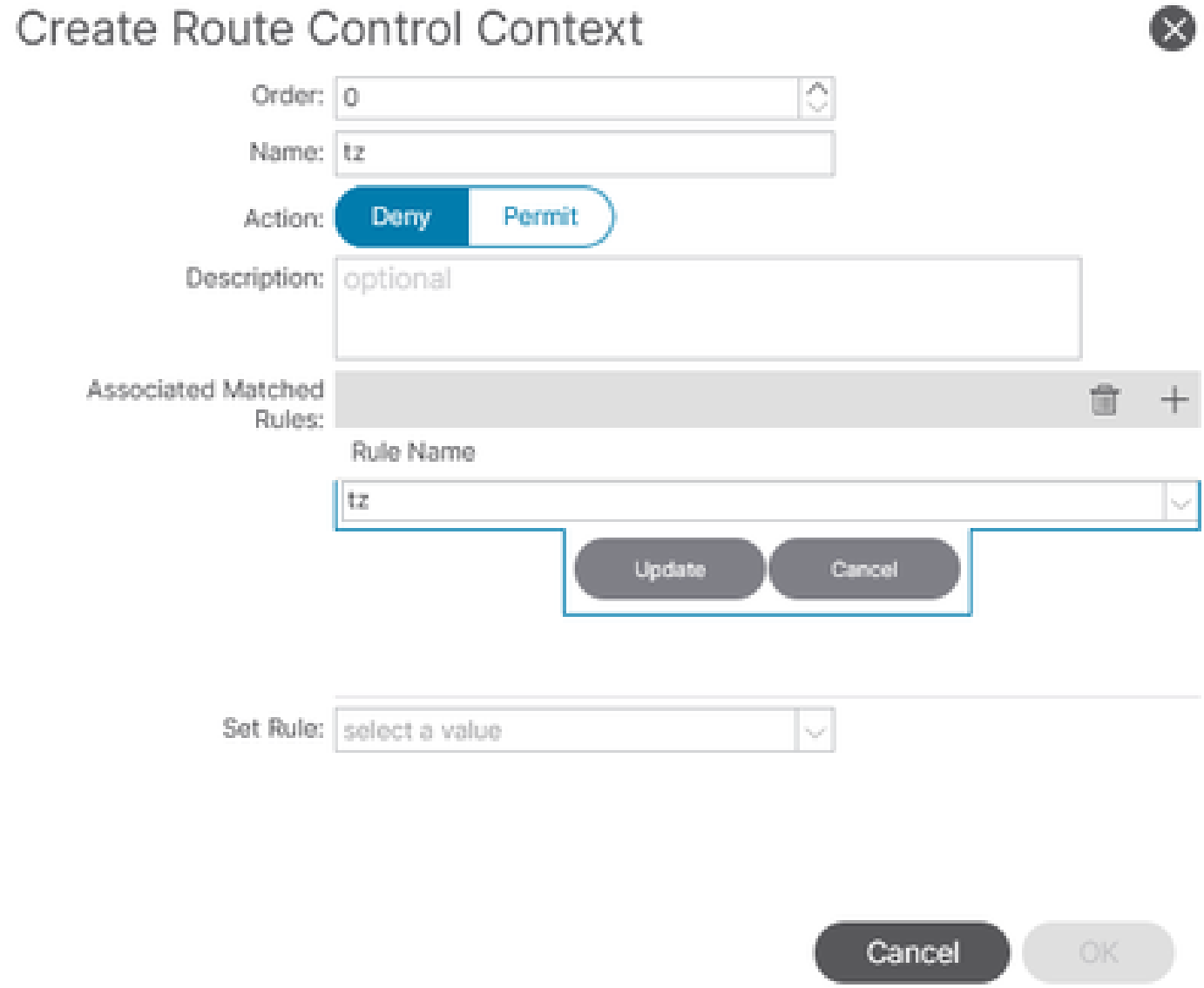
デフォルトでは、このインポートルートマップはすべての着信プレフィックスを許可します。この動作を変更するには：

Tenants > [tenant name] > Networking > L3outs > [L3out name] > Route map for import and export route controlの順に移動します。

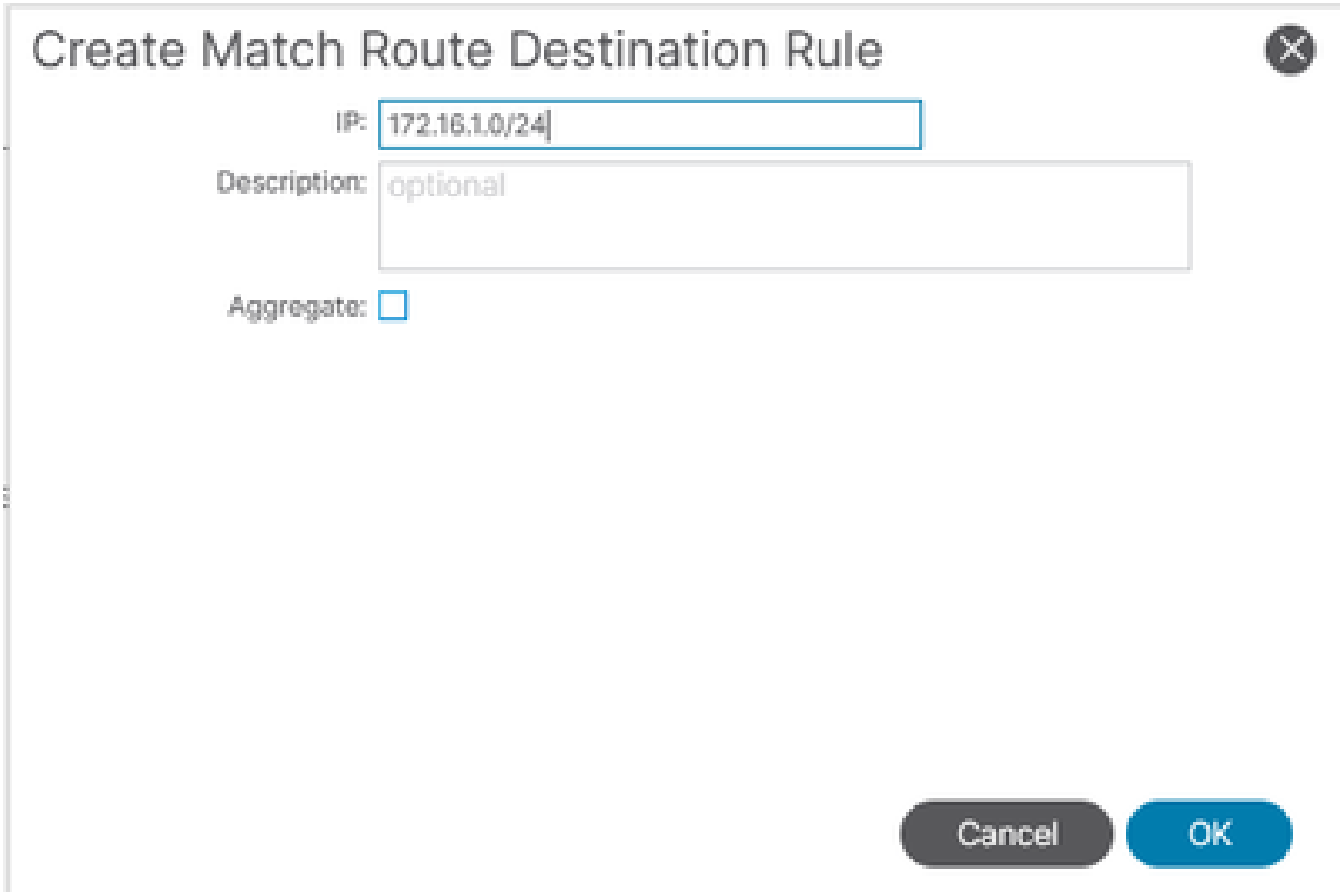
デフォルトのインポートルートマップを選択するか、右上の歯車アイコンを使用して新しいルートマップを作成します。



Contextセクションで、新しい関連付けられた一致ルールを作成します。



Match RulesセクションでMatch Prefixまでスクロールし、制御する特定のサブネットを追加します。



ポリシーを送信すると、それに応じてインポートルートマップアクションが変更され、目的のプレフィックスフィルタリングが適用されます。

```
<#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#
```

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。