Risoluzione dei problemi relativi alla classificazione della subnet L3Out in ACI

Sommario

Introduzione

Abbreviazioni

Classificazione EPG esterna

- Flag subnet EPG esterne

Comandi per la verifica e la risoluzione dei problemi

- Routing
- Classificazione
- Contratti
- Routing transit

Problemi comuni nella classificazione EPG esterna della subnet

- tag PC 15
- Subnet sovrapposte

Importa modifica comportamento predefinito controllo ciclo di lavorazione

Introduzione

Questo documento descrive la classificazione delle subnet esterne negli EPG L3Out di Cisco ACI,

Abbreviazioni

- BD: Dominio bridge
- EPG: Gruppo endpoint
- ExEPG: Gruppo endpoint esterno
- NERVATURA: Base informazioni di routing
- VRF: Routing e inoltro virtuale
- ID classe: Tag che identifica un EPG

Classificazione EPG esterna

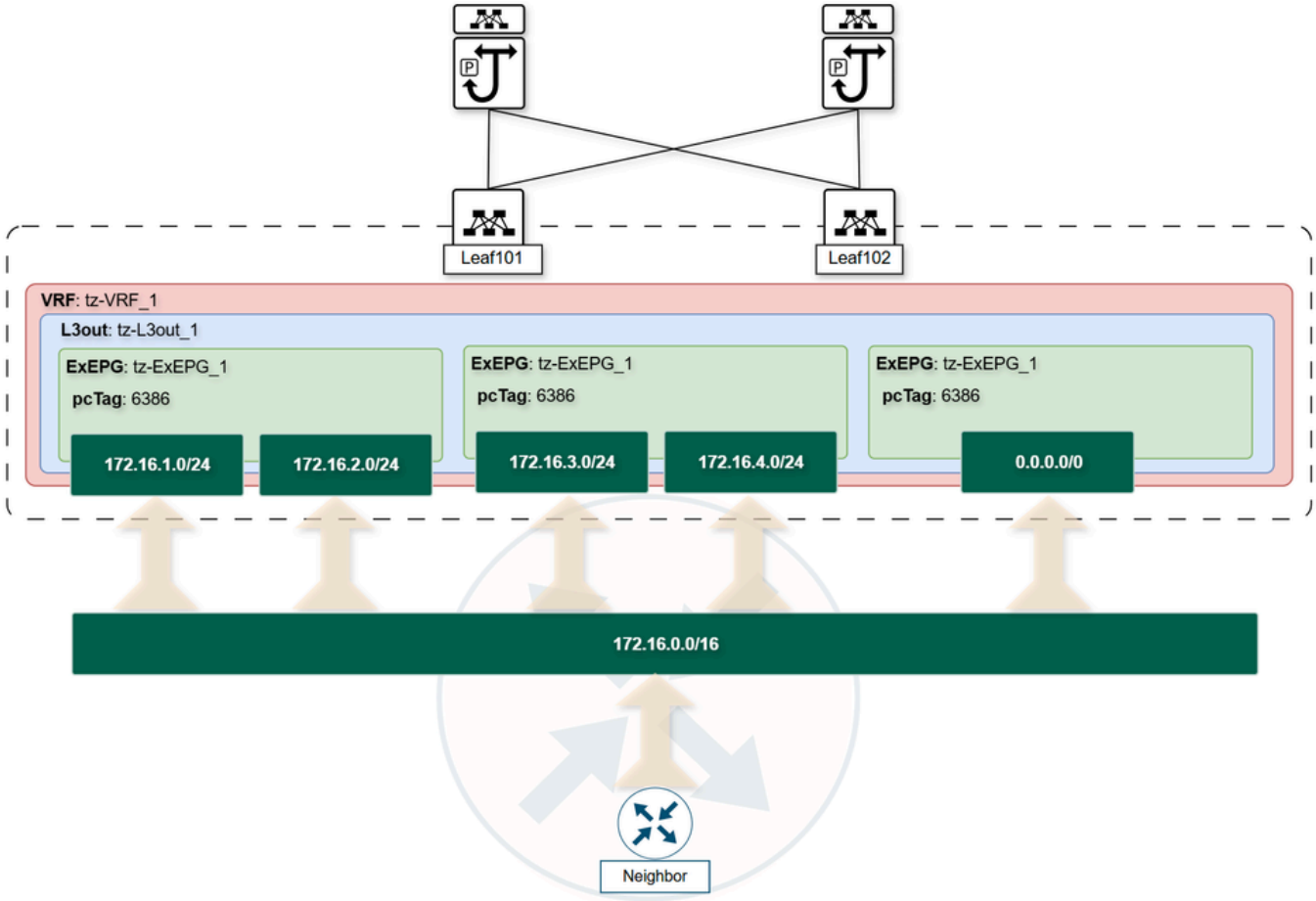
Un EPG esterno in Cisco ACI rappresenta le reti di routing esterne connesse tramite L3Outs. Analogamente alla classificazione degli endpoint da parte di un EPG standard, un EPG esterno classifica le subnet esterne in base al VRF, ovvero ogni subnet deve essere univoca all'interno del relativo contesto VRF.

Un errore comune è rappresentato dal fatto che una subnet EPG esterna include solo prefissi accettati tramite il protocollo di routing dinamico. Tuttavia, quando viene creato un L3Out, è disponibile un filtro predefinito per le route-map negli annunci in ingresso; pertanto, tutti i prefissi

annunciati dal protocollo di routing dinamico sono accettati per impostazione predefinita. Lo scopo principale della definizione di subnet in un ExEPG è la classificazione solo per assegnare un PcTag univoco alle subnet racchiuse nell'ExEPG per l'applicazione del contratto e delle policy.

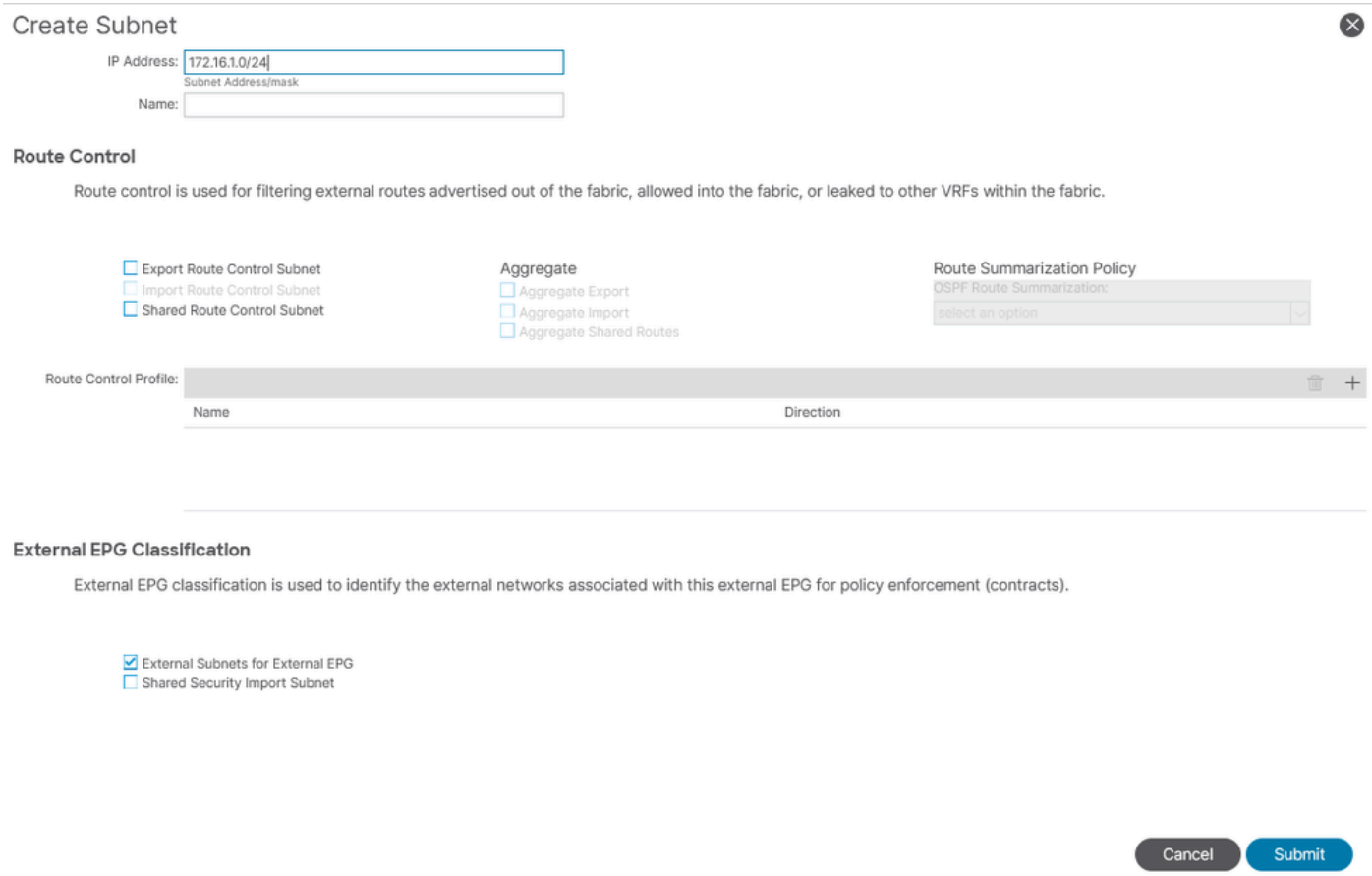
Questa classificazione consente il controllo granulare dei criteri. Ad esempio, un singolo router adiacente esterno può annunciare una supernet all'ACI, che può quindi essere segmentata in più ExEPG. Ciò consente di applicare diverse azioni contrattuali a subnet distinte, ad esempio consentendo a specifici EPG interni di comunicare solo con subnet esterne designate o reindirizzando il traffico destinato a determinati prefissi verso un nodo PBR prima di raggiungere la destinazione finale.

Il diagramma mostra come Cisco ACI classifica le subnet esterne in base agli EPG esterni, consentendo una segmentazione precisa del traffico e l'applicazione dei contratti.



Flag subnet EPG esterne

Per classificare e gestire i prefissi esterni all'interno di un ExEPG in ACI, vengono configurati flag di subnet specifici durante la creazione di un prefisso di subnet in un ExEPG. In questa sezione vengono illustrati in dettaglio i contrassegni e l'utilizzo previsto:



- Subnet esterna per EPG esterno:
  Questo flag indica che la subnet risiede all'esterno dell'infrastruttura ACI e non è configurata in alcun dominio Bridge o EPG. Deve essere utilizzato solo quando il prefisso viene annunciato da un router adiacente o inserito in modo statico nel RIB. Questo flag è attivato per impostazione predefinita.

- Esporta subnet di controllo route:
  Questo flag indica che la subnet viene annunciata dall'ACI al router adiacente di routing tramite il protocollo di routing dinamico. Non deve essere abilitato contemporaneamente al flag Subnet esterna per EPG esterno, in quanto ciò può causare loop di routing di layer 3. Poiché ACI classifica la subnet come esterna e la annuncia nuovamente, possono verificarsi incoerenze di routing nonostante i meccanismi di prevenzione dei loop nei protocolli di routing.

- Subnet di controllo route condivisa:
  Questo flag viene impostato quando il prefisso della subnet deve essere condiviso tra più VRF, consentendo la perdita di route tra i contesti.

- Subnet importazione protezione condivisa:
  Utilizzato in combinazione con il flag Shared Route Control Subnet, consente la condivisione dei pcTag di protezione per subnet esterne su VRF diverse, facilitando l'applicazione coerente delle policy.

- Importa subnet di controllo route:
  Questo flag consente il controllo granulare sui prefissi ricevuti dai router adiacenti. Per

impostazione predefinita, ACI accetta tutti gli annunci delle route in ingresso; per abilitare questo flag è necessario attivare l'imposizione del controllo route per filtrare i prefissi in ingresso.

- Sezione aggregata:
  Applicabile solo alla subnet quad-0 (0.0.0.0/0), questa sezione riepiloga tutti i prefissi nel RIB per l'esportazione o l'importazione aggregata. Quando le subnet vengono inviate ad altri VRF, vengono riepilogate come route condivise aggregate per ottimizzare le tabelle di routing.

Comandi per la verifica e la risoluzione dei problemi

Routing

Per iniziare, il percorso deve essere presente nella tabella di routing del VRF sugli switch Border Leaf. Ad esempio, questo comando mostra una route BGP nel 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#
```

Ciò conferma che il percorso è installato nella tabella di routing VRF e che è disponibile per le decisioni di inoltro.

Classificazione

Dopo la presenza della route nella tabella di routing, la classificazione determina la modalità di gestione del traffico in base ai criteri. In ACI, la classificazione è legata all'ExEPG e alle relative subnet associate.

Per convalidare la classificazione della subnet in un'istanza ExEPG, è possibile eseguire una query sull'APIC per la classe l3extInstP, che rappresenta l'istanza External EPG. La relativa classe figlio l3extSubnet elenca le subnet configurate in tale ExEPG. Ad esempio:

<#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 non viene restituito alcun output per la classe l3extSubnet, significa che non sono configurate subnet in External EPG. Senza le subnet configurate, ACI non può associare un pcTag alla subnet del traffico in ingresso. Il traffico verrà quindi interrotto nonostante il percorso sia presente nella tabella di routing.

Un altro aspetto importante da notare è l'ambito della subnet, che rappresenta i flag impostati per la subnet in questione:

- Import-security

La subnet è stata contrassegnata con External Subnet for External EPG.

- export-rtctrl

La subnet è stata contrassegnata con Export Route Control.

- import-rtctrl

La subnet è stata contrassegnata con Import Route Control.

- protezione condivisa

La subnet è stata contrassegnata con Subnet importazione protezione condivisa.

- shared-rtctrl

La subnet è stata contrassegnata con il controllo del percorso condiviso.

I protocolli di instradamento e i processi del control plane aggiornano le tabelle di instradamento alla ricezione di un prefisso da un vicino menzionato, che vengono quindi programmati nelle tabelle di inoltro HAL L3. I percorsi HAL L3 rappresentano i percorsi effettivi di layer 3 programmati nelle tabelle di inoltro hardware (ASIC) sugli switch foglia. Queste route derivano dai calcoli dei protocolli di routing e delle tabelle di routing e vengono utilizzate per le decisioni di inoltro.

<#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#
```

Successivamente, quando una subnet viene configurata con il flag Subnet esterna per EPG esterno in un ExEPG, un processo interno chiamato Policy Manager (policy-mgr) aggiorna la tabella di mapping prefisso-a-pcTag con questa voce subnet e il pcTag associato. Policy Manager funge da motore di orchestrazione delle regole centralizzato dell'infrastruttura, traducendo le definizioni delle regole di alto livello in configurazioni utilizzabili per l'azione nell'infrastruttura ACI. Ciò garantisce una connettività delle applicazioni e un comportamento di rete coerenti e sicuri applicando i tag pc corretti per la classificazione del traffico e le decisioni di inoltro in base alle subnet esterne configurate.

<#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#
```

Ciò conferma che il prefisso 172.16.1.0/24 viene annunciato dal vicino allo switch a foglia di bordo ACI, e l'ACI ha classificato il prefisso sotto pcTag 32771

Contratti

Una regola di zoning è il processo sottostante che applica le politiche contrattuali tra EPG (inclusi gli ExEPG) all'interno del fabric. Il VRF VNID (ambito) e il pcTag dell'EPG esterno possono essere utilizzati per definire e convalidare le regole di comunicazione applicate tra gli EPG di origine e di destinazione. Essenzialmente, le regole di zoning convertono le relazioni contrattuali di alto livello in regole specifiche e applicabili programmate sugli switch foglia.

Un aspetto importante da considerare è la posizione in cui il contratto viene installato nel fabric. Per impostazione predefinita, il VRF è configurato con la Direzione di applicazione del controllo dei criteri impostata su In entrata. Questa impostazione determina che la regola di suddivisione in zone per un determinato contratto viene installata sullo switch foglia in cui risiede l'endpoint di origine.

Per questo esercizio, il traffico proviene da un'uscita L3Out, la regola di suddivisione in zone viene installata sulla foglia di confine che si connette a tale uscita L3Out, in quanto questa foglia funge da foglia di origine per il traffico che entra nell'infrastruttura.

<#root>

```
Leaf101#
```

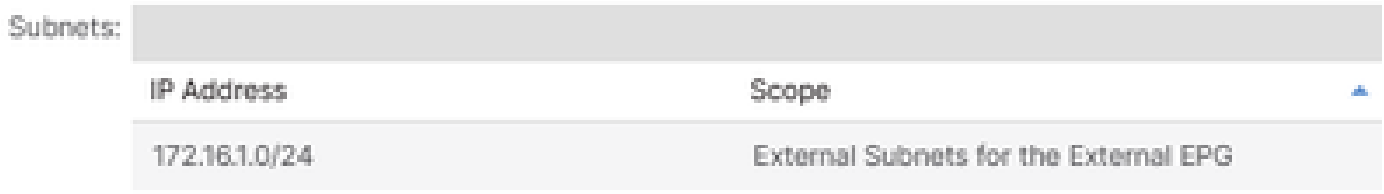
show zoning-rule scope 3047430 | egrep "Rule|---|32771"

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

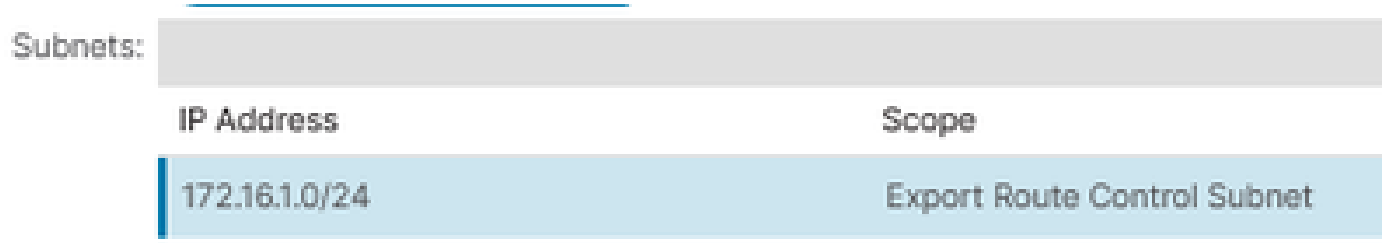
Routing transit

Il routing di transito consente al fabric di fungere da rete di transito pubblicizzando percorsi esterni

appresi da un L3Out all'altro. Per configurare correttamente il routing di transito, la subnet in ingresso deve essere contrassegnata con il flag External Subnet for External EPG.



Contemporaneamente, per l'uscita L3 che annuncia la subnet ad altri peer esterni è necessario che il flag Esporta subnet di controllo route sia abilitato nella subnet corrispondente. Questo flag consente di ridistribuire la subnet e pubblicizzarla all'esterno dell'infrastruttura tramite il protocollo di routing configurato su tale L3Out.



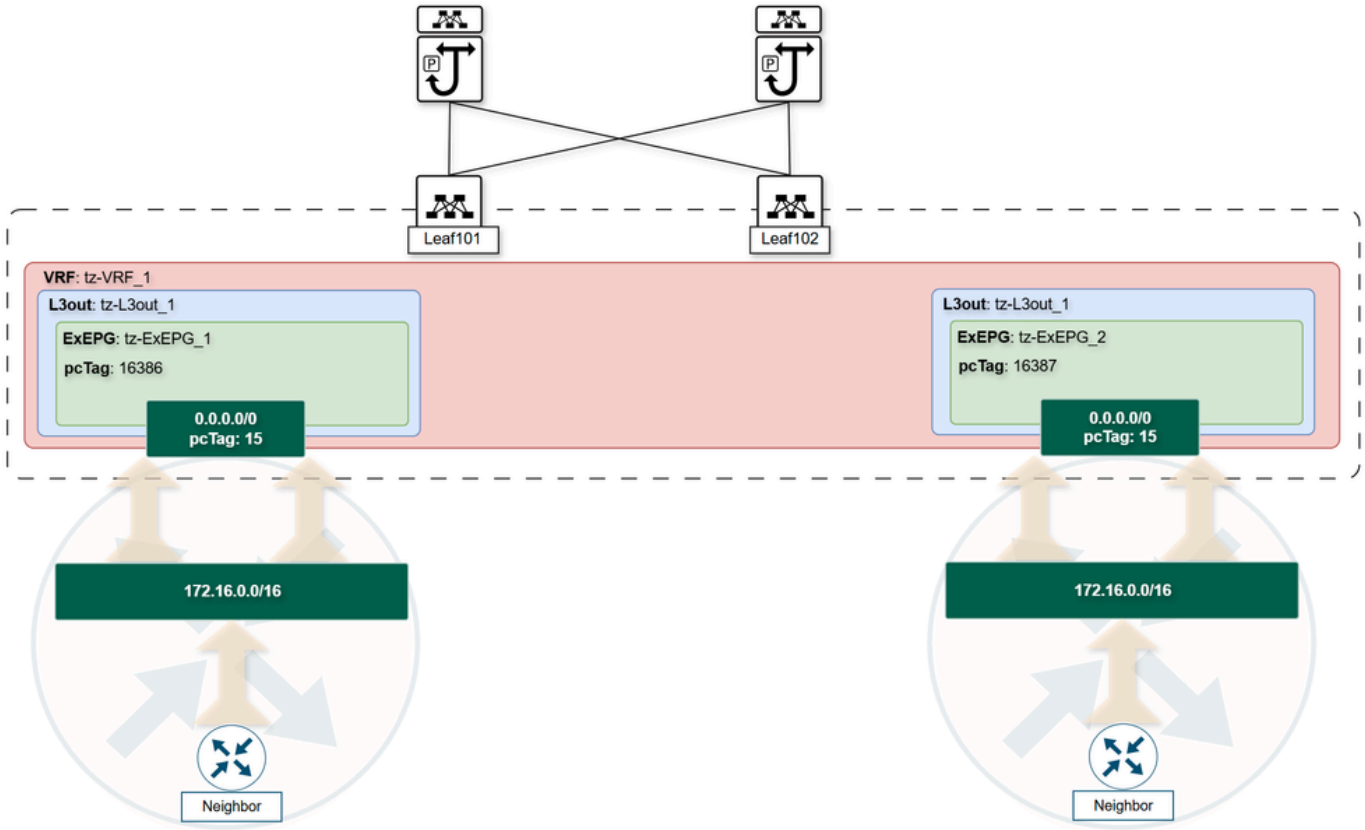
Infine, per completare il processo di distribuzione del percorso, è necessario configurare un contratto tra il router L3out ricevuto e il router L3out esportatore.

Problemi comuni nella classificazione EPG esterna della subnet

tag PC 15

In precedenza, in questo documento, si affermava che la subnet ExEPG consente di classificare le subnet nel pcTag corretto per motivi di applicazione dei criteri. Un'importante eccezione a questa classificazione è la subnet quad-0 (0.0.0.0/0) quando configurata con il flag Subnet esterna per EPG esterno. A questa subnet viene sempre assegnato il pcTag 15 riservato, che funge da carattere jolly per tutto il traffico esterno all'interno di un VRF.

Il diagramma mostra il problema di configurazione del quad-0 con subnet esterna per EPG esterno su più ExEPG all'interno dello stesso VRF:



- La subnet quad-0 viene spesso scambiata per la route predefinita. Anche se a volte questo è vero, ad esempio quando un router adiacente dinamico annuncia solo la route predefinita all'ACI L3Out, il ruolo della subnet quad-0 in ACI è più ampio, come una classificazione catch-all.
- È pratica comune configurare più ExEPG con la subnet quad-0 in modo da accettare tutti i prefissi annunciati da un router adiacente. Anche se questo raggiunge l'obiettivo di un'ampia accettazione, può portare a un routing asimmetrico imprevisto quando più ExEPG con quadruplo 0 sono configurati all'interno dello stesso VRF. Quando più ExEPG all'interno dello stesso VRF sono configurati con quadruplo 0 come subnet esterna, ACI non può selezionare in modo deterministico quale L3Out utilizzare per una subnet di destinazione specifica. Al contrario, seleziona arbitrariamente una L3Out.
- Questo comportamento può causare un routing asimmetrico, intermittenza del traffico o addirittura perdite di traffico se l'uscita L3T selezionata casualmente non dispone dei contratti necessari per consentire la comunicazione.

Subnet sovrapposte

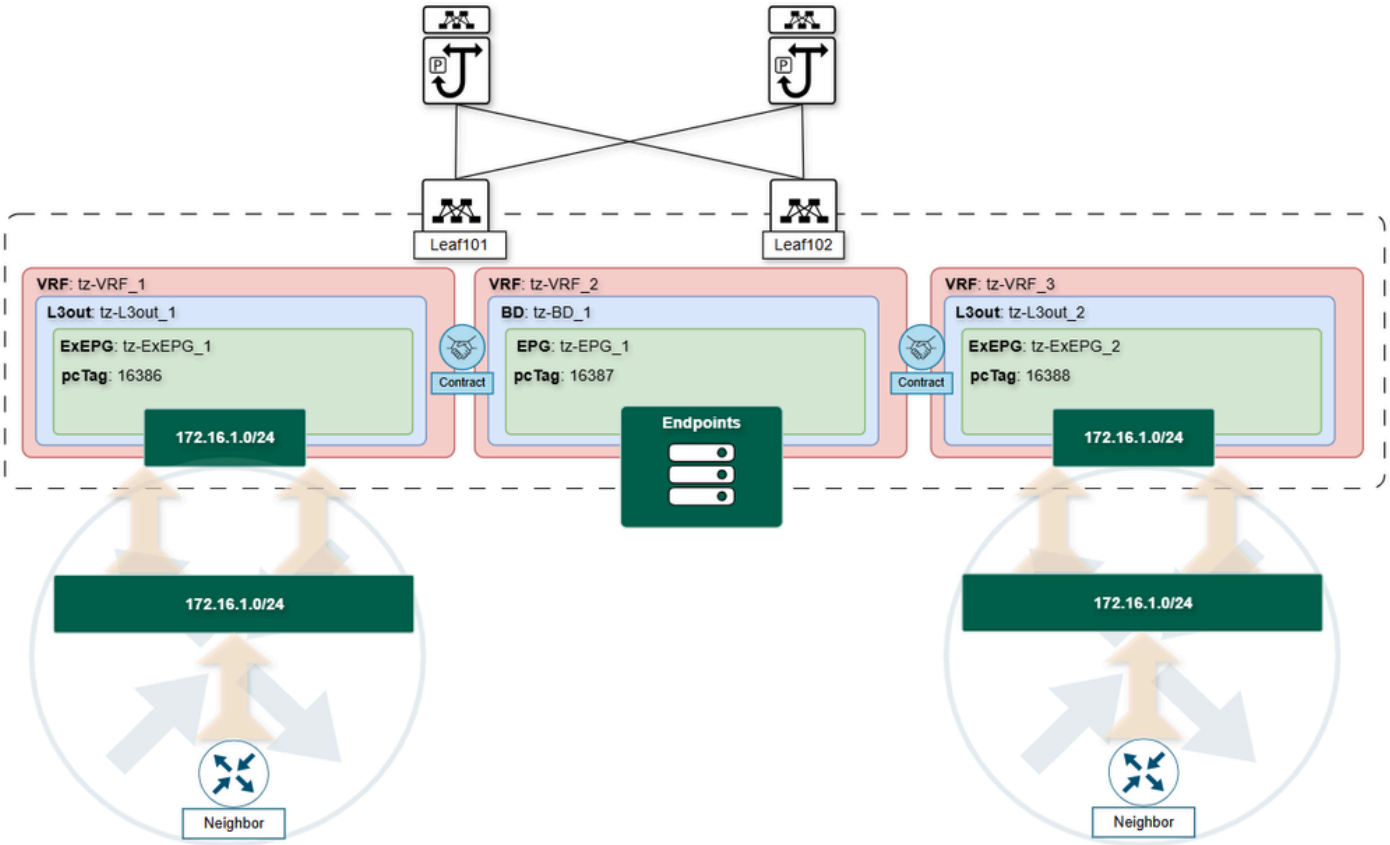
Non è consentita la configurazione di subnet identiche su ExEPG diversi. Il tentativo di eseguire questa operazione attiva l'errore "F0467: Voce di prefisso già utilizzata in un altro EPG", che impedisce la duplicazione della subnet all'interno di un VRF.

Tuttavia, è possibile che subnet sovrapposte siano presenti in VRF diverse, in quanto ogni VRF gestisce un contesto di tabella di routing indipendente. Questa separazione consente di configurare la stessa subnet in ExEPG che appartengono a VRF diversi. Nonostante ciò, è fondamentale essere cauti quando si eseguono perdite di route VRF che coinvolgono queste subnet sovrapposte, in quanto ciò può causare decisioni di inoltro asimmetriche a causa di conflitti

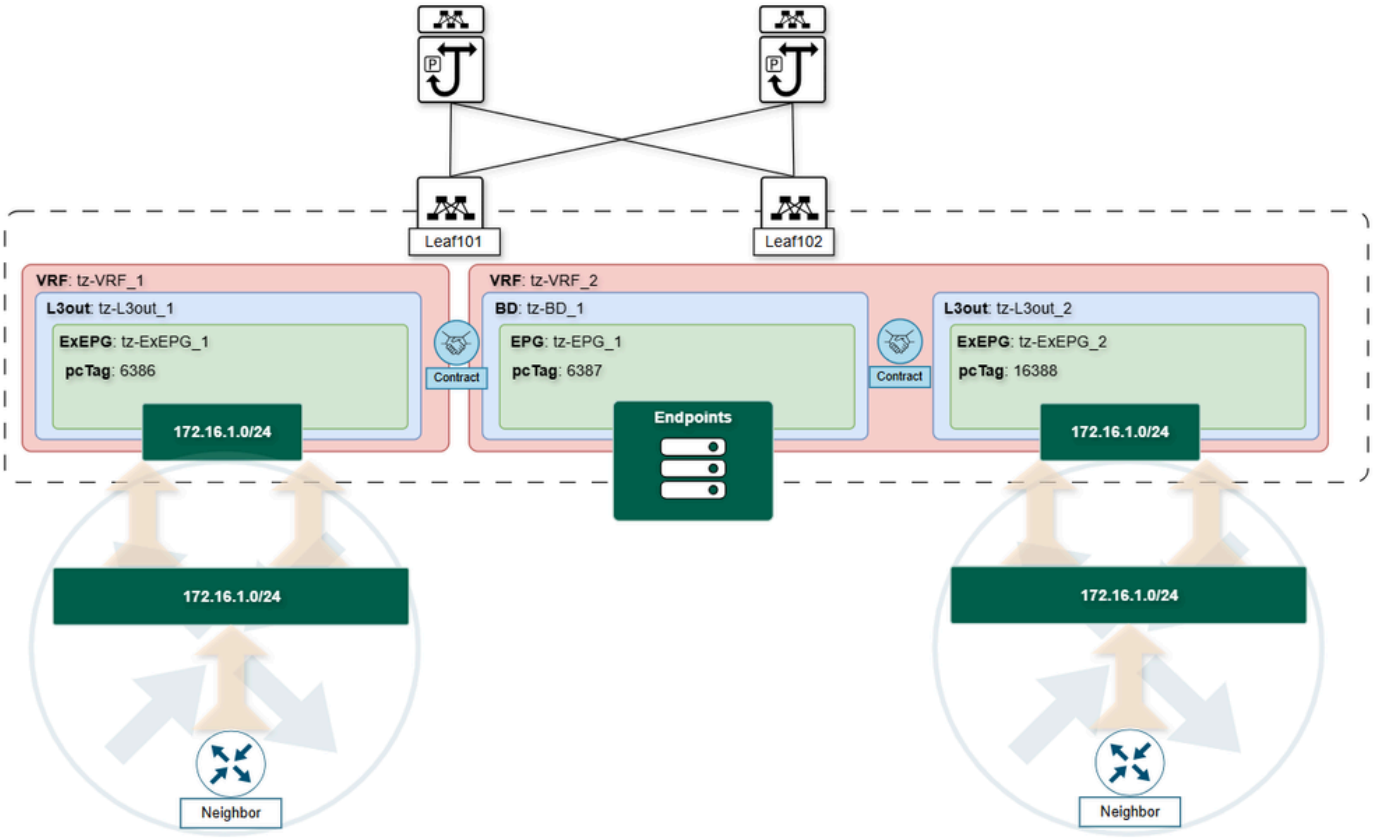
nella classificazione delle subnet (pcTag) rispetto alle informazioni di routing (RIB).

Gli scenari principali includono:

- Indirizzare le perdite da due VRF a un terzo VRF:
  Quando due VRF filtrano la stessa subnet in un terzo VRF, il VRF ricevente installa la prima subnet che riceve in base ai criteri condivisi dall'APIC. Se lo switch foglia che gestisce questo VRF viene riavviato o la selezione del routing viene modificata, la tabella di routing potrebbe essere aggiornata a un'uscita L3 diversa, causando un comportamento di inoltro incoerente.



- Local-to-VRF L3Out ExEPG che si sovrappone alle subnet perse:
  Nelle progettazioni in cui viene utilizzata la perdita di route, se una L3Out locale ExEPG è configurata con la stessa subnet come subnet perduta, la voce di routing locale ha sempre la precedenza sulle route perdute.



Queste situazioni evidenziano che i problemi di inoltro asimmetrico derivano dal livello di decisione di classificazione e inoltro, non dalla tabella di routing stessa. Mentre la classificazione della subnet associa una subnet a uno specifico L3Out ed ExEPG per l'applicazione dei criteri, la tabella di routing può puntare a una destinazione L3Out diversa. Questa mancata corrispondenza può causare l'inoltro incoerente del traffico, con potenziali problemi di connettività o gap di applicazione delle policy.

Importa modifica comportamento predefinito controllo ciclo di lavorazione

Per impostazione predefinita, ACI accetta tutti gli annunci route in ingresso dai vicini. Per controllare quali prefissi vengono accettati, è necessario abilitare l'applicazione del controllo route: in ingresso nell'oggetto radice L3Out:

Passare a Tenant > [nome tenant] > Rete > L3outs > [nome L3out] .

Questa azione consente di creare una route-map nel protocollo di routing selezionato.

<#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#

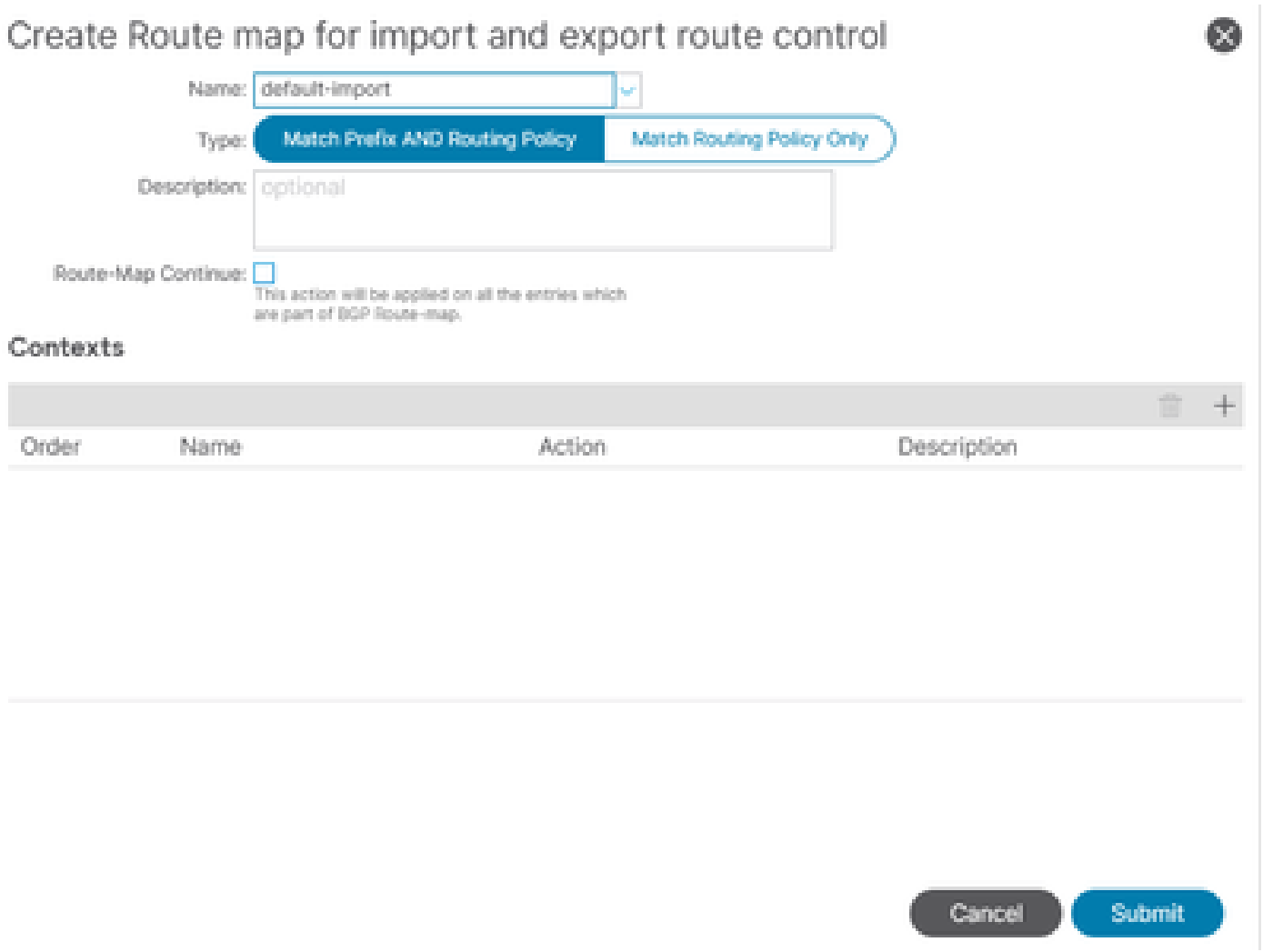
show ip prefix-list IPv4-peer49155-2981888-exc-ext-inferred-import-dst

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

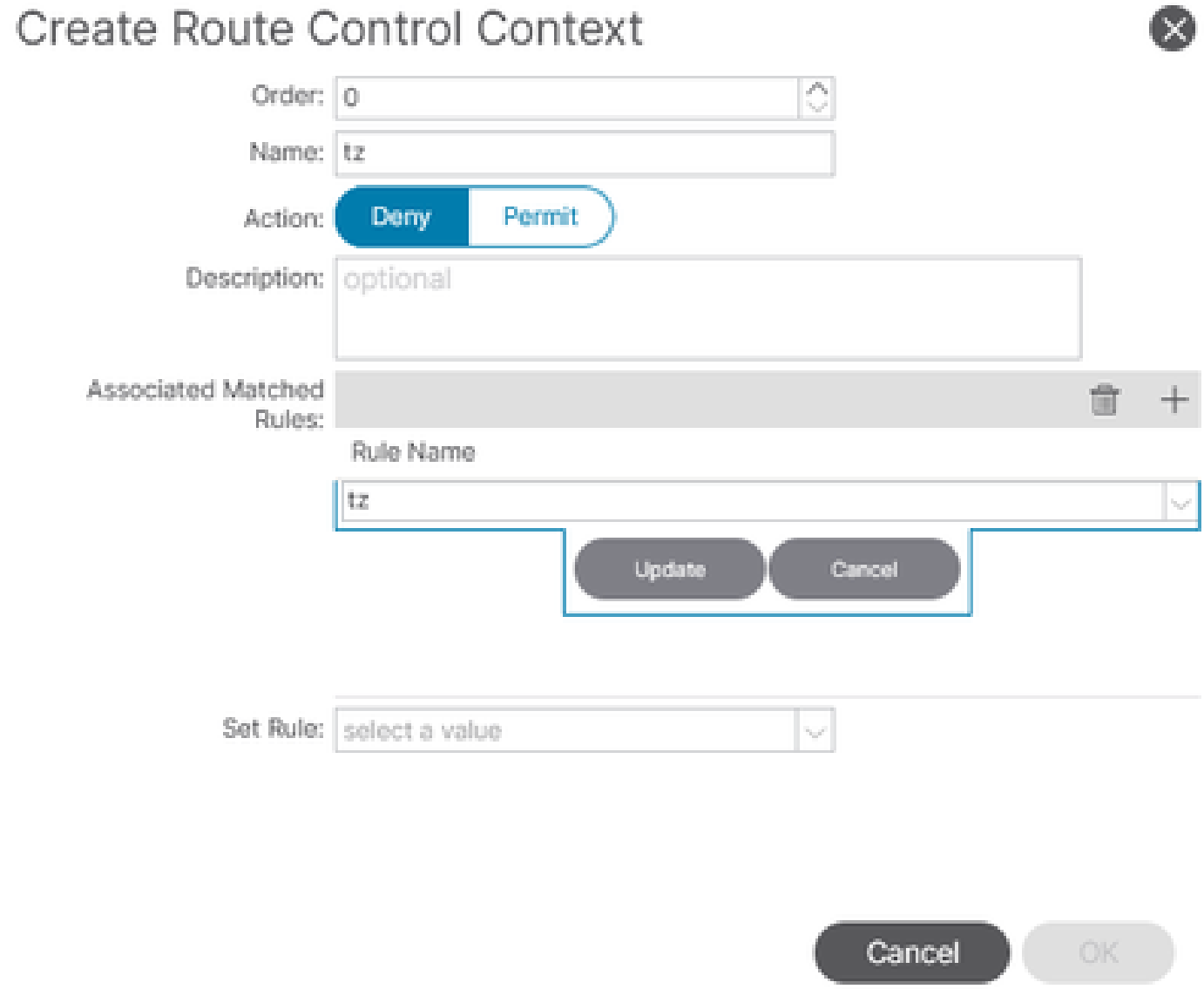
Per impostazione predefinita, questa route-map di importazione consente tutti i prefissi in ingresso. Per modificare questo comportamento:

Passare a Tenant > [nome tenant] > Rete > L3outs > [Nome L3out] > Mappa percorso per il controllo dei percorsi di importazione ed esportazione

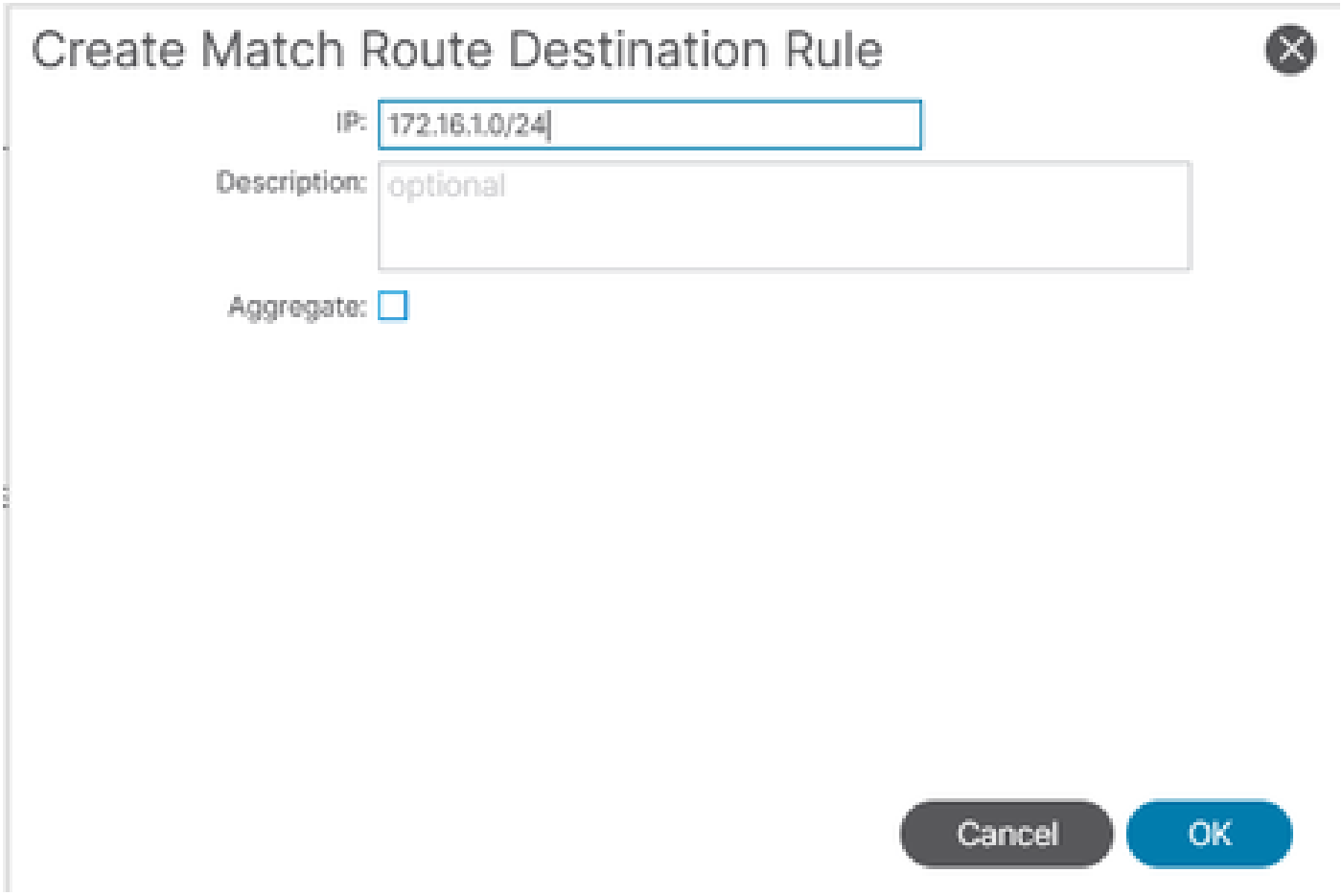
Selezionate la mappa del percorso di importazione di default o createne una nuova utilizzando l'icona dell'ingranaggio in alto a destra.



Nella sezione Contesto creare una nuova regola di corrispondenza associata.



Nella sezione Regole corrispondenza scorrere fino a Prefisso corrispondenza e aggiungere le subnet specifiche che si desidera controllare.



Dopo l'invio dei criteri, l'azione di importazione route-map cambia di conseguenza, applicando il filtro prefissi desiderato.

<#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#
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).