

# Solução de problemas de encaminhamento externo da ACI

## Contents

[Introduction](#)

[Informações de Apoio](#)

[Overview](#)

[Componentes L3Out](#)

[Componentes principais de uma L3Out](#)

[Roteamento externo](#)

[Fluxo de roteamento externo de alto nível](#)

[Opções de configuração de EPG de L3Out](#)

[Uma sub-rede L3Out sendo definida incluindo a definição do 'escopo'](#)

[Topologia L3Out usada nesta seção](#)

[Topologia L3Out](#)

[Adjacências](#)

[BGP](#)

[Perfil de conectividade de mesmo nível — Local-AS](#)

[Perfil de conectividade de mesmo nível — AS remoto](#)

[L3Out — Perfil de conectividade de peer BGP](#)

[Perfil de nó lógico — Associação de nó](#)

[Verificação BGP CLI \(eBGP com exemplo de loopback\)](#)

[OSPF](#)

[L3Out — Perfil de Interface OSPF — ID e Tipo de Área](#)

[Perfil de interface lógica — SVI](#)

[Perfil de interface OSPF](#)

[Perfil de interface OSPF — temporizador Hello / Dead e tipo de rede](#)

[Detalhes da política de interface OSPF](#)

[verificação CLI do OSPF](#)

[EIGRP](#)

[Perfil de Interface EIGRP](#)

[Verificação CLI do EIGRP](#)

[Anúncio de rota](#)

[Fluxo de trabalho de anúncio de rota de domínio de ponte](#)

[Antes de aplicar o contrato entre a L3Out e o EPG interno](#)

[Depois de aplicar o contrato entre a L3Out e o EPG interno](#)

[Após selecionar 'Anunciar Externamente' na Sub-rede BD](#)

[Após associar L3Out ao BD](#)

[anúncio de rota BGP](#)

[anúncio de rota EIGRP](#)

[Configuração da L3 do Domínio de Bridge](#)

[Cenário de solução de problemas de anúncio de rota de domínio de ponte](#)

[Perfil de rota de negação de exportação padrão](#)

[Fluxo de trabalho de importação de roteiro externo](#)

[A rota está instalada na tabela de roteamento BL](#)

[Verificar rota em folha interna](#)

[Cenário de solução de problemas de rota externa](#)

[Fluxo de trabalho de anúncio de roteiro de trânsito](#)

[Topologia de roteamento de trânsito](#)

[Política de marcação de rota](#)

[Controle de rota de exportação](#)

[Roteamento de trânsito ao receber e anunciar BL são os mesmos](#)

[Cenários de solução de problemas de roteamento de trânsito #1: Rota de trânsito não anunciada](#)

[Cenários de solução de problemas de roteamento de trânsito #2: Rota de trânsito não recebida](#)

[Roteador externo com VRF único — Rota de trânsito não recebida](#)

[Cenários de identificação e solução de problemas de roteamento de trânsito #3 — Rotas de trânsito anunciadas inesperadamente](#)

[Contrato e L3Out](#)

[EPG baseado em prefixo em L3Out](#)

[Localização do pcTag para uma L3Out](#)

[Exemplo 1: Saída L3 única com prefixo específico](#)

[Sub-rede com escopo 'Sub-redes Externas para o EPG Externo'](#)

[Exemplo 2: Única L3Out com vários prefixos](#)

[Exemplo 3a: Vários EPGs L3Out em um VRF](#)

[Verificação do pcTag L3Out](#)

[Exemplo 3b: vários EPGs L3Out com contratos diferentes](#)

[Validação do caminho de dados usando Triagem — fluxo permitido pela política](#)

[Validação do caminho de dados usando Triagem — fluxo não permitido pela política](#)

[Exemplo 4: várias L3Outs com vários prefixos](#)

[Validação do caminho de dados usando Triagem — fluxo permitido pela política](#)

[Validação do caminho de dados usando Triagem — fluxo não permitido pela política](#)

[Validação do caminho de dados — regras de zoneamento](#)

[Verificação do pcTag do VRF](#)

[Confirmando o pcTag usado pelo pacote usando o aplicativo ELAM Assistant](#)

[Saída do aplicativo ELAM Assistant para src 32771 para dst 49153](#)

[Conclusão](#)

[L3Out Compartilhado](#)

[Overview](#)

[Topologia L3Out compartilhada](#)

[Fluxo de trabalho L3Out compartilhado — aprendizado de rotas externas](#)

[Rota externa como vista na folha de borda](#)

[Verificações de BGP na folha de borda](#)

[Verificações no servidor leaf](#)

[Fluxo de trabalho L3Out compartilhado — anunciando rotas internas](#)

[Verificar a rota estática BD no BL](#)

[Cenário de solução de problemas L3Out compartilhado — vazamento de rota inesperado](#)

[Uso de 'Agregar Compartilhado'](#)

## Introduction

Este documento descreve as etapas para entender e solucionar problemas de um L3out na ACI

## Informações de Apoio

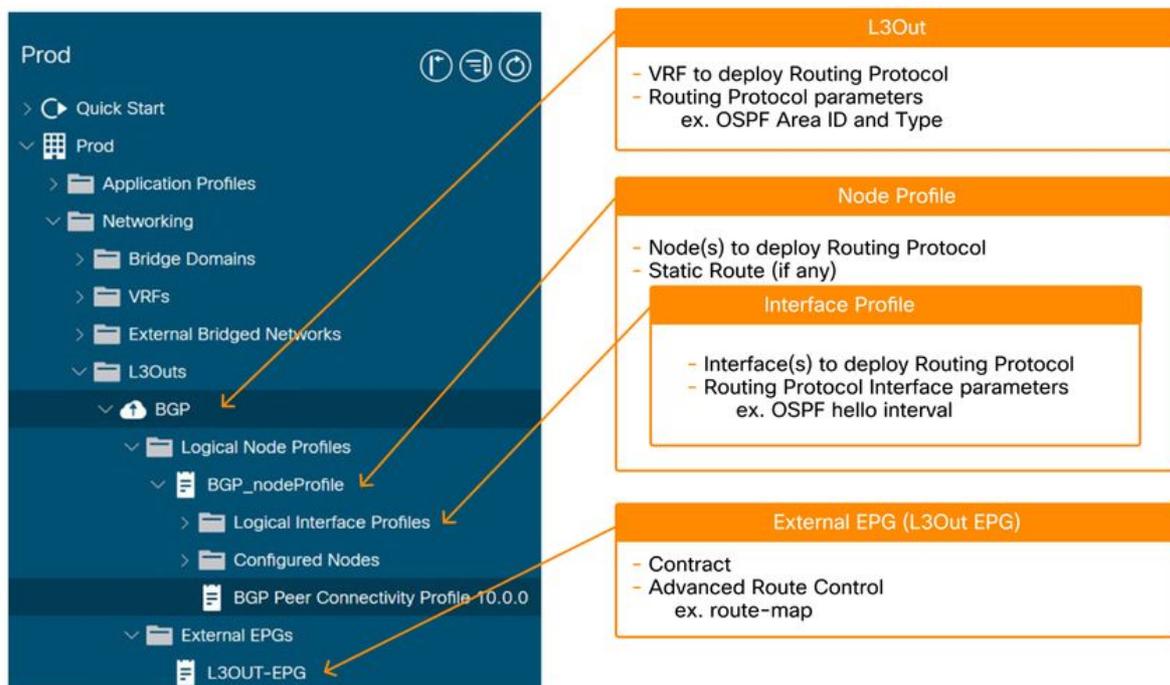
O material deste documento foi extraído do livro [Troubleshooting Cisco Application Centric Infrastructure, Second Edition](#) especificamente dos capítulos **External Forwarding - Overview**, **External Forwarding - Adjacencies**, **External Forwarding - Route Advertiy**, **External Forwarding - Contract and L3out** e **External Forwarding - Share L3out**.

## Overview

### Componentes L3Out

A figura a seguir ilustra os principais componentes necessários para configurar um L3 externo (L3Saída).

### Componentes principais de uma L3Out



1. Raiz de L3Out: Selecione um protocolo de roteamento para implantar (como OSPF, BGP).Selecione um VRF para implantar o protocolo de roteamento.Selecione um Domínio L3Out para definir interfaces leaf e VLAN disponíveis para a L3Out.
2. Perfil do nó: Selecione switches leaf para implantar o protocolo de roteamento. Estes são normalmente conhecidos como "Border Leaf Switches" (BL).Configure Router-ID (RID) para o protocolo de roteamento em cada folha de borda. Diferentemente de um roteador normal,

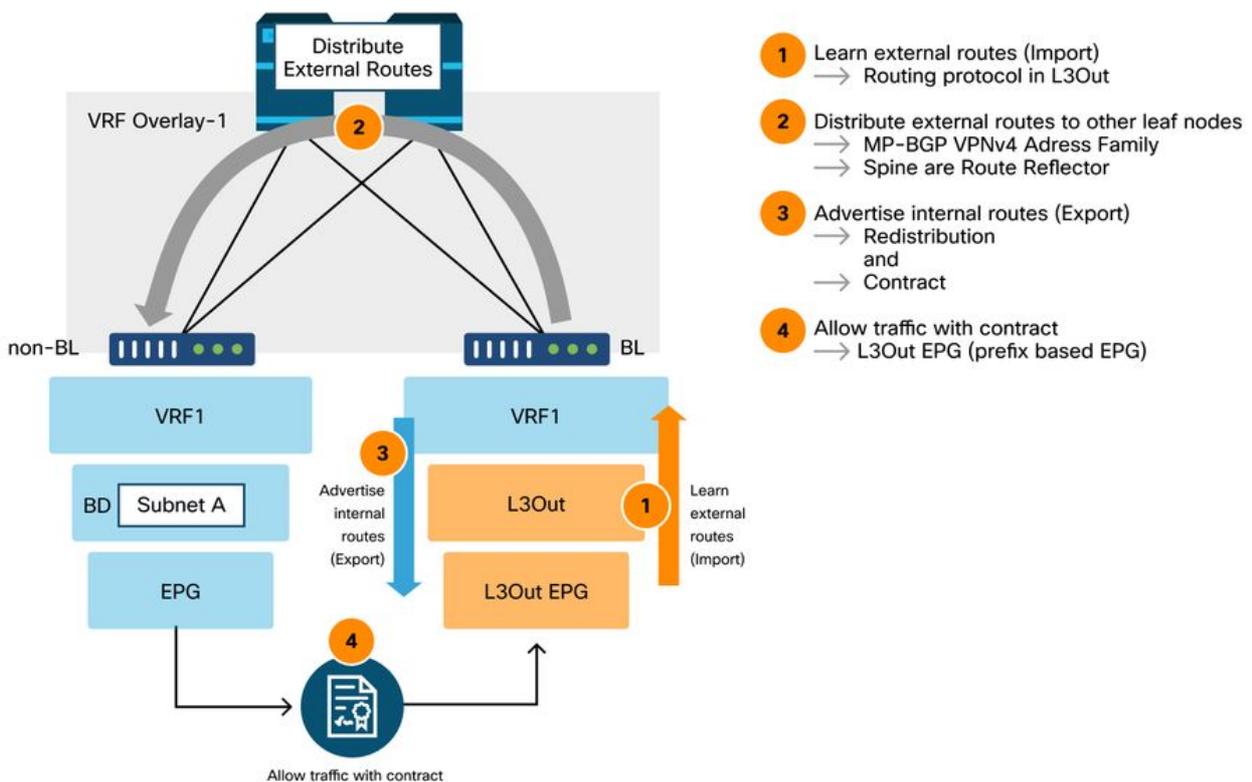
a ACI não atribui automaticamente Router-ID com base em um endereço IP no switch. Configure uma rota estática.

3. Perfil de interface: Configurar interfaces leaf para executar o protocolo de roteamento. Por exemplo, tipo de interface (SVI, porta roteada, subinterface), ID da interface e endereços IP, etc. Selecione uma política para os parâmetros do protocolo de roteamento no nível da interface (como intervalo de Hello).
4. EPG externo (EPG de saída L3P): Um 'EPG externo' é um requisito difícil para implantar toda a política vinculada à L3Out, como endereços IP ou SVIs para estabelecer vizinhos. Detalhes sobre como usar EPGs externos serão abordados posteriormente.

## Roteamento externo

O diagrama a seguir mostra a operação de alto nível envolvida no roteamento externo.

### Fluxo de roteamento externo de alto nível



1. As BL(s) estabelecerão adjacências de protocolos de roteamento com roteadores externos.
2. Os prefixos de rotas são recebidos de roteadores externos e injetados no MP-BGP como o caminho da família de endereços VPNv4. No mínimo, dois nós spine devem ser configurados como refletos de rota BGP para refletir rotas externas para todos os nós leaf.
3. Prefixos internos (sub-redes BD) e/ou prefixos recebidos de outras L3Out devem ser explicitamente redistribuídos no protocolo de roteamento para serem anunciados ao roteador externo.
4. Aplicação de segurança: Uma L3Out contém pelo menos um EPG L3Out. Um contrato deve ser consumido ou fornecido no EPG L3Out (também chamado de l3extInstP do nome da classe) para permitir o tráfego de entrada/saída do L3Out.

## Opções de configuração de EPG de L3Out

Na seção L3Out EPG, as sub-redes podem ser definidas com uma série de opções de 'Escopo' e 'Agregar', conforme ilustrado abaixo:

### Uma sub-rede L3Out sendo definida incluindo a definição do 'escopo'

The screenshot shows the 'Create Subnet' configuration page. The IP Address field is set to 192.168.1.0/24. The Name field is empty. The 'scope' section has five options: 'Export Route Control Subnet', 'Import Route Control Subnet', 'External Subnets for the External EPG' (checked), 'Shared Route Control Subnet', and 'Shared Security Import Subnet'. Below the scope section are fields for BGP Route Summarization Policy, aggregate options, and a Route Control Profile table.

Name	Direction
------	-----------

Opções de 'Escopo':

- **Sub-rede de Controle de Rotas de Exportação:** este escopo tem o objetivo de anunciar (exportar) uma sub-rede da ACI para fora por meio da L3Out. Embora isso seja principalmente para o Roteamento de trânsito, também pode ser usado para anunciar uma sub-rede BD conforme descrito na seção "Anúncio de sub-rede BD ACI".
- **Importar sub-rede de controle de rota:** este escopo trata da aprendizagem (importação) de uma sub-rede externa da L3Out. Por padrão, esse escopo está desabilitado, por isso está esmaecido, e uma folha de borda (BL) aprende todas as rotas de um protocolo de roteamento. Esse escopo pode ser habilitado quando precisa limitar as rotas externas aprendidas via OSPF e BGP. Isso não é suportado para EIGRP. Para usar este escopo, 'Imposição de Controle de Rota de Importação' precisa ser habilitada primeiro em um determinado L3Out.
- **Sub-redes Externas para o EPG Externo (segurança de importação):** este escopo é usado para permitir pacotes com a sub-rede configurada de ou para a L3Out com um contrato. Ele classifica um pacote no EPG L3Out configurado com base na sub-rede, de modo que um contrato no EPG L3Out possa ser aplicado ao pacote. Este escopo é uma Correspondência de Prefixo Mais Longa em vez de uma correspondência exata como outros escopos para a tabela de roteamento. Se 10.0.0.0/16 estiver configurado com 'Sub-redes Externas para o EPG Externo' em L3Out EPG A, todos os pacotes com IP nessa sub-rede, como 10.0.1.1, serão classificados em L3Out EPG A para usar um contrato nela. Isso não significa que o

escopo 'Sub-redes Externas para o EPG Externo' instale uma rota 10.0.0.0/16 em uma tabela de roteamento. Ele criará uma tabela interna diferente para mapear uma sub-rede para um EPG (pcTag) somente para um contrato. Ele não tem nenhum efeito nos comportamentos do protocolo de roteamento. Esse escopo deve ser configurado em uma L3Out que está aprendendo a sub-rede.

- **Sub-rede de controle de rota compartilhada:** este escopo é para vazar uma sub-rede externa para outro VRF. A ACI usa o MP-BGP e o Route Target para vazar uma rota externa de um VRF para outro. Esse escopo cria uma lista de prefixos com a sub-rede, que é usada como um filtro para exportar/importar rotas com destino de rota em MP-BGP. Esse escopo deve ser configurado em uma L3Out que está aprendendo a sub-rede no VRF original.
- **Sub-rede de Importação de Segurança Compartilhada:** este escopo é usado para permitir pacotes com a sub-rede configurada quando os pacotes estão se movendo através de VRFs com uma L3Out. Uma rota em uma tabela de roteamento vaza para outro VRF com a "Sub-rede de controle de rota compartilhada", conforme mencionado acima. No entanto, outro VRF ainda não sabe a qual EPG a rota vazada deve pertencer. A 'Subrede de Importação de Segurança Compartilhada' informa outro VRF do EPG L3Out ao qual a rota vazada pertence. Portanto, esse escopo pode ser usado somente quando "Sub-redes externas para o EPG externo" também é usado, caso contrário, o VRF original não sabe a qual L3Out EPG a sub-rede pertence. Este escopo também é a Correspondência de Prefixo Mais Longa.

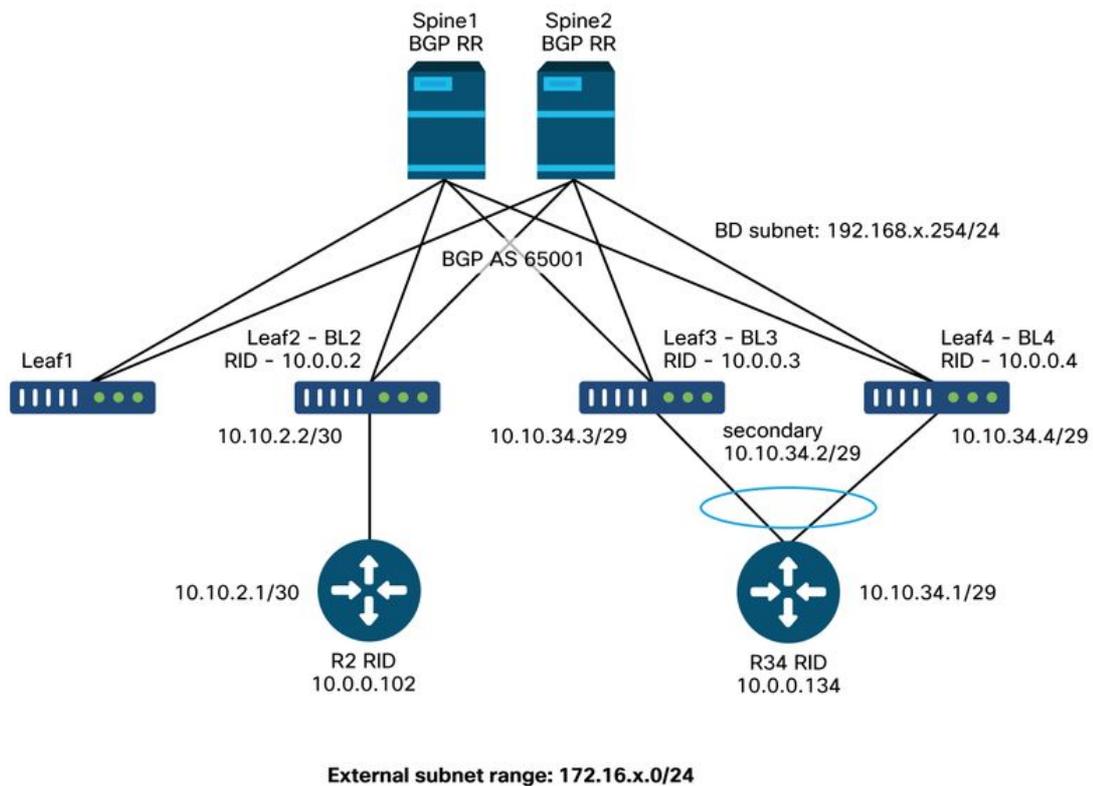
Opções de 'Agregar':

- **Exportação Agregada:** esta opção pode ser usada somente para 0.0.0.0/0 com 'Sub-rede de Controle de Rota de Exportação'. Quando a 'Sub-rede de Controle de Rota de Exportação' e a 'Exportação Agregada' estão habilitadas para 0.0.0.0/0; ele cria uma lista de prefixos com '0.0.0.0/0 le 32' que corresponde a qualquer sub-rede. Portanto, esta opção pode ser usada quando uma L3Out precisa anunciar (exportar) quaisquer rotas para o exterior. Quando uma agregação mais granular é necessária, o Mapa de Rota/Perfil com uma lista de prefixos explícita pode ser usado.
- **Importação Agregada:** esta opção pode ser usada somente para 0.0.0.0/0 com 'Sub-rede de Controle de Rota de Importação'. Quando 'Import Route Control Subnet' e 'Aggregate Import' estão habilitados para 0.0.0.0/0, ele cria uma lista de prefixos com '0.0.0.0/0 le 32' que corresponde a qualquer sub-rede. Portanto, esta opção pode ser usada quando uma L3Out precisa aprender (importar) quaisquer rotas de fora. No entanto, a mesma coisa pode ser realizada desabilitando 'Imposição de controle de rota de importação', que é o padrão. Quando uma agregação mais granular é necessária, o Mapa de Rota/Perfil com uma lista de prefixos explícita pode ser usado.
- **Rotas compartilhadas agregadas:** esta opção pode ser usada para qualquer sub-rede com 'Sub-rede de controle de rota compartilhada'. Quando 'Sub-rede de controle de rota compartilhada' e 'Rotas compartilhadas agregadas' estão ativadas para 10.0.0.0/8 como exemplo, ele cria uma lista de prefixos com '10.0.0.0/8 le 32' que corresponde a 10.0.0.0/8, 10.1.0.0/16 e assim por diante.

## Topologia L3Out usada nesta seção

A seguinte topologia será usada nesta seção:

## Topologia L3Out



## Adjacências

Esta seção explica como solucionar problemas e verificar adjacências de protocolos de roteamento em interfaces L3Out.

Abaixo estão alguns parâmetros para verificar se serão aplicáveis a todos os protocolos de roteamento externo da ACI:

- **ID do roteador:** na ACI, cada L3Out precisa usar o mesmo ID do roteador no mesmo VRF na mesma folha, mesmo que os protocolos de roteamento sejam diferentes. Além disso, apenas um desses L3Outs na mesma folha pode criar um loopback com o ID do roteador, que geralmente é BGP.
- **MTU:** Embora o requisito rígido de MTU seja apenas para a adjacência OSPF, é recomendável corresponder o MTU para qualquer protocolo de roteamento para garantir que qualquer pacote jumbo usado para troca/atualizações de rota possa ser transmitido sem fragmentação, pois a maioria dos quadros de plano de controle será enviada com o conjunto de bits DF (não fragmentar), que descartará o quadro se seu tamanho exceder o MTU máximo da interface.
- **Refletor de roteador MP-BGP:** sem isso, o processo BGP não será iniciado em nós folha. Embora isso não seja necessário para o OSPF ou EIGRP apenas para estabelecer um vizinho, ainda é necessário para BLs distribuir rotas externas para outros nós de folha.
- **Falhas:** sempre verifique as falhas durante e após a conclusão da configuração.

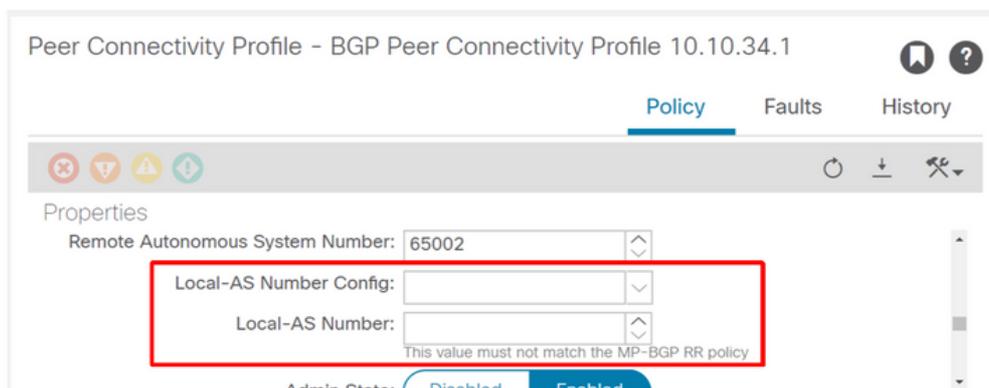
## BGP

Esta seção usa um exemplo de um peering eBGP entre o loopback em BL3, BL4 e R34 da topologia na seção Visão geral. O BGP AS em R34 é 65002.

Verifique os seguintes critérios ao estabelecer uma adjacência BGP.

- Número AS do BGP local (lado BL da ACI).

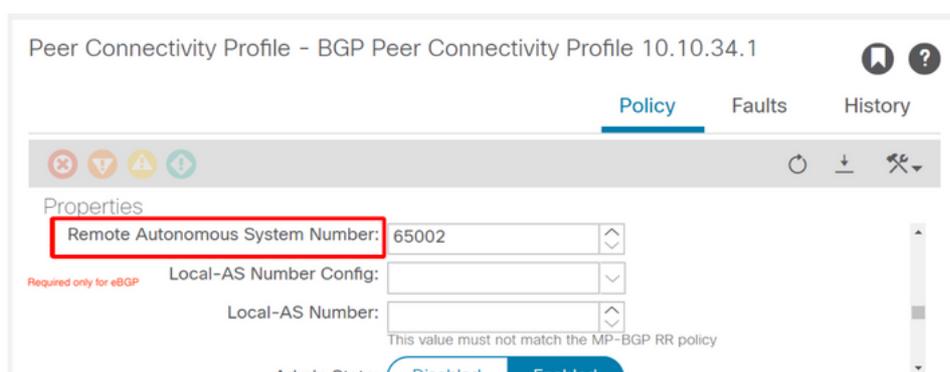
## Perfil de conectividade de mesmo nível — Local-AS



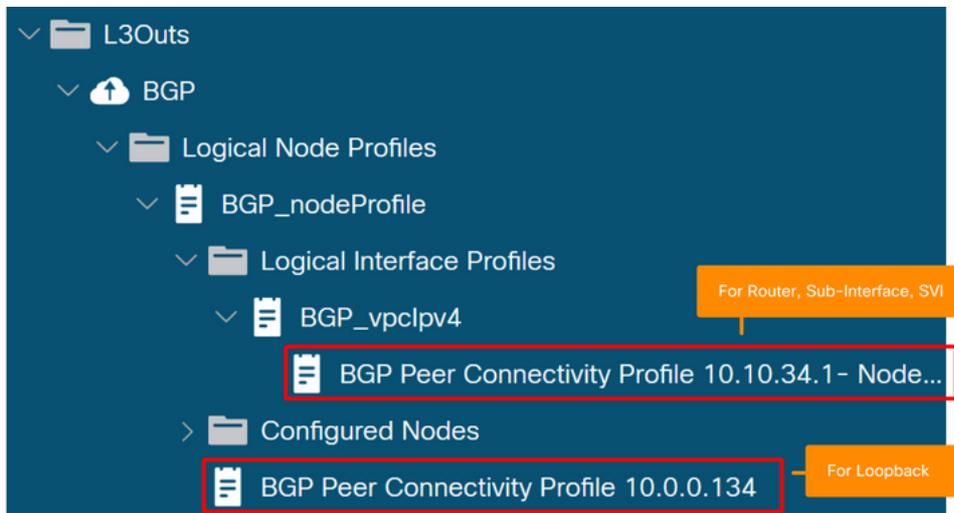
O número AS de BGP de um usuário L3Out será automaticamente o mesmo que o AS de BGP para o infra-MP-BGP que é configurado na política do Refletor de Rota BGP. A configuração 'Local AS' no Perfil de Conectividade de Par BGP não é necessária, a menos que seja necessário disfarçar o AS BGP da ACI para o mundo externo. Isso significa que os roteadores externos devem apontar para o AS do BGP configurado no Refletor de Rota do BGP.

**OBSERVAÇÃO** — O cenário em que a configuração de AS local é necessária é o mesmo do comando autônomo 'local-as' do NX-OS.

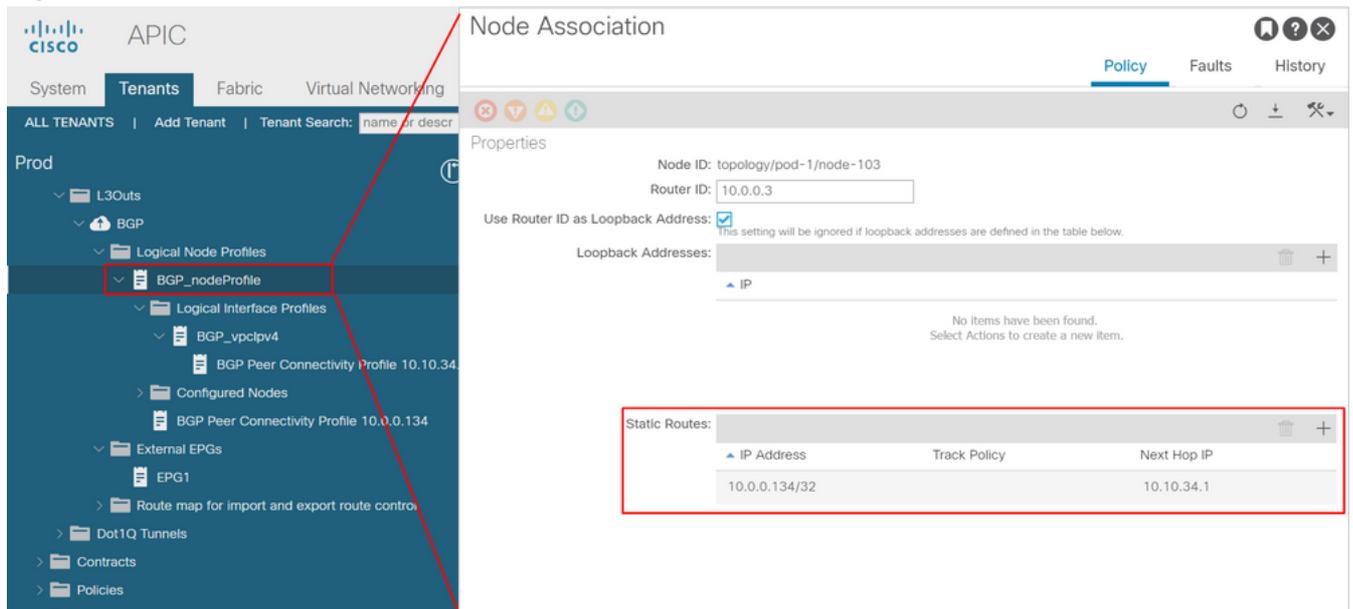
- Número AS do BGP remoto (lado externo) **Perfil de conectividade de mesmo nível — AS remoto**



O número AS do BGP remoto é necessário apenas para o eBGP onde o AS do BGP do vizinho é diferente do AS do BGP da ACI. IP de origem para sessão de peer BGP. **L3Out — Perfil de conectividade de peer BGP**



A ACI suporta a obtenção de uma sessão BGP da interface de loopback sobre um tipo de interface ACI L3Out (roteada, subinterface, SVI). Quando uma sessão BGP precisa ser originada de um loopback, configure o Perfil de Conectividade de Par BGP no Perfil de Nó Lógico. Quando a sessão BGP precisa ser originada de uma interface/sub-interface/SVI roteada, configure o Perfil de Conectividade de Par BGP no Perfil de Interface Lógica. Alcançabilidade IP de peer BGP. **Perfil de nó lógico — Associação de nó**



Quando os IPs de peer do BGP forem loopbacks, certifique-se de que o BL e o roteador externo tenham alcance para o endereço IP do peer. As rotas estáticas ou OSPF podem ser usadas para obter acessibilidade aos IPs pares. **Verificação BGP CLI (eBGP com exemplo de loopback)** As saídas CLI para as etapas a seguir são coletadas do BL3 na topologia da seção Visão geral. **1. Verifique se a sessão BGP está estabelecida** 'State/PfxRcd' na seguinte saída CLI significa que a sessão BGP está estabelecida.

```
f2-leaf3# show bgp ipv4 unicast summary vrf Prod:VRF1
BGP summary information for VRF Prod:VRF1, address family IPv4 Unicast
BGP router identifier 10.0.0.3, local AS number 65001
```

```
Neighbor          V    AS MsgRcvd MsgSent  TblVer  InQ  OutQ Up/Down  State/PfxRcd
```

```
10.0.0.134      4 65002      10      10      10      0      0 00:06:39 0
```

Se o 'State/PfxRcd' mostrar Idle ou Ative, os pacotes BGP ainda não estão sendo trocados com o peer. Nesse cenário, verifique o seguinte e passe para a próxima etapa.

- Verifique se o roteador externo está apontando para o AS do BGP da ACI corretamente (número AS local 65001).
- Certifique-se de que o Perfil de Conectividade de Par BGP da ACI esteja especificando o IP vizinho correto do qual o roteador externo está originando a sessão BGP (10.0.0.134).
- Certifique-se de que o Perfil de Conectividade de Par BGP da ACI esteja especificando o AS vizinho correto do roteador externo (Remote Autonomous System Number na GUI que aparece na CLI como AS 65002).

## 2. Verificar detalhes de Vizinhos BGP (Perfil de Conectividade de Pares BGP)

O comando a seguir mostra os parâmetros que são chave para o estabelecimento de vizinhos BGP.

- IP do vizinho: 10.0.0.134.
- BGP AS vizinho: 65002 AS remoto.
- IP de origem: Usando loopback3 como origem da atualização.
- eBGP multi-hop: O peer de BGP externo pode estar a até 2 saltos de distância.

```
f2-leaf3# show bgp ipv4 unicast neighbors vrf Prod:VRF1
BGP neighbor is 10.0.0.134, remote AS 65002, ebgp link, Peer index 1
BGP version 4, remote router ID 10.0.0.134
BGP state = Established, up for 00:11:18
Using loopback3 as update source for this peer
External BGP peer might be upto 2 hops away

...

For address family: IPv4 Unicast
...
Inbound route-map configured is permit-all, handle obtained
Outbound route-map configured is exp-13out-BGP-peer-3047424, handle obtained
Last End-of-RIB received 00:00:01 after session start
Local host: 10.0.0.3, Local port: 34873
Foreign host: 10.0.0.134, Foreign port: 179
fd = 64
```

Quando o peer do BGP é estabelecido corretamente, o 'host local' e o 'host externo' aparecem na parte inferior da saída.

## 3. Verifique a alcançabilidade de IP para o peer de BGP

```
f2-leaf3# show ip route vrf Prod:VRF1
10.0.0.3/32, ubest/mbest: 2/0, attached, direct
  *via 10.0.0.3, lo3, [0/0], 02:41:46, local, local
  *via 10.0.0.3, lo3, [0/0], 02:41:46, direct
10.0.0.134/32, ubest/mbest: 1/0
  *via 10.10.34.1, vlan27, [1/0], 02:41:46, static <--- neighbor IP reachability via static
route
10.10.34.0/29, ubest/mbest: 2/0, attached, direct
  *via 10.10.34.3, vlan27, [0/0], 02:41:46, direct
```

```
*via 10.10.34.2, vlan27, [0/0], 02:41:46, direct
10.10.34.2/32, ubest/mbest: 1/0, attached
*via 10.10.34.2, vlan27, [0/0], 02:41:46, local, local
10.10.34.3/32, ubest/mbest: 1/0, attached
*via 10.10.34.3, vlan27, [0/0], 02:41:46, local, local
```

Certifique-se de que o ping para o IP vizinho funcione a partir do IP de origem do BGP da ACI.

```
f2-leaf3# iping 10.0.0.134 -v Prod:VRF1 -S 10.0.0.3
PING 10.0.0.134 (10.0.0.134) from 10.0.0.3: 56 data bytes
64 bytes from 10.0.0.134: icmp_seq=0 ttl=255 time=0.571 ms
64 bytes from 10.0.0.134: icmp_seq=1 ttl=255 time=0.662 ms
```

#### 4. Verifique a mesma coisa no roteador externo

Veja a seguir um exemplo de configuração no roteador externo (NX-OS independente).

```
router bgp 65002
vrf f2-bgp
  router-id 10.0.0.134
  neighbor 10.0.0.3
    remote-as 65001
    update-source loopback134
    ebgp-multihop 2
    address-family ipv4 unicast
  neighbor 10.0.0.4
    remote-as 65001
    update-source loopback134
    ebgp-multihop 2
    address-family ipv4 unicast

interface loopback134
vrf member f2-bgp
ip address 10.0.0.134/32

interface Vlan2501
no shutdown
vrf member f2-bgp
ip address 10.10.34.1/29

vrf context f2-bgp
ip route 10.0.0.0/29 10.10.34.2
```

#### 5. Etapa adicional — tcpdump

Nos nós leaf da ACI, a ferramenta tcpdump pode farejar a interface da CPU 'kpm\_inb' para confirmar se os pacotes de protocolo chegaram à CPU leaf. Use a porta L4 179 (BGP) como um filtro.

```
f2-leaf3# tcpdump -ni kpm_inb port 179
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on kpm_inb, link-type EN10MB (Ethernet), capture size 65535 bytes
20:36:58.292903 IP 10.0.0.134.179 > 10.0.0.3.34873: Flags [P.], seq 3775831990:3775832009, ack
807595300, win 3650, length 19: BGP, length: 19
20:36:58.292962 IP 10.0.0.3.34873 > 10.0.0.134.179: Flags [.), ack 19, win 6945, length 0
20:36:58.430418 IP 10.0.0.3.34873 > 10.0.0.134.179: Flags [P.], seq 1:20, ack 19, win 6945,
```

length 19: BGP, length: 19

20:36:58.430534 IP 10.0.0.134.179 > 10.0.0.3.34873: Flags [.], ack 20, win 3650, length 0

## OSPF

Esta seção usa um exemplo de vizinhança OSPF entre BL3, BL4 e R34 da topologia na seção Visão geral com AreaID 1 (NSSA) do OSPF.

A seguir estão os critérios comuns para verificar o estabelecimento de adjacências OSPF.

- ID e tipo de área OSPF

### L3Out — Perfil de Interface OSPF — ID e Tipo de Área



Assim como qualquer dispositivo de roteamento, o ID e o tipo da área OSPF precisam corresponder em ambos os vizinhos. Algumas limitações específicas da ACI nas configurações de ID de área do OSPF incluem:

- Uma L3Out pode ter apenas um ID de área OSPF.
- Duas L3Outs podem usar o mesmo ID de área OSPF no mesmo VRF somente quando estão em dois nós de folha diferentes.

Embora o ID do OSPF não precise ser o backbone 0, no caso do Roteamento de trânsito ele é necessário entre dois L3Outs OSPF na mesma folha; um deles deve usar a área 0 do OSPF porque qualquer troca de rota entre áreas OSPF deve passar pela área 0 do OSPF.

- MTU

### Perfil de interface lógica — SVI

Logical Interface Profile - OSPF\_vpclpv4

Policy Faults History

General Routed Sub-Interfaces Routed Interfaces **SVI** Floating SVI

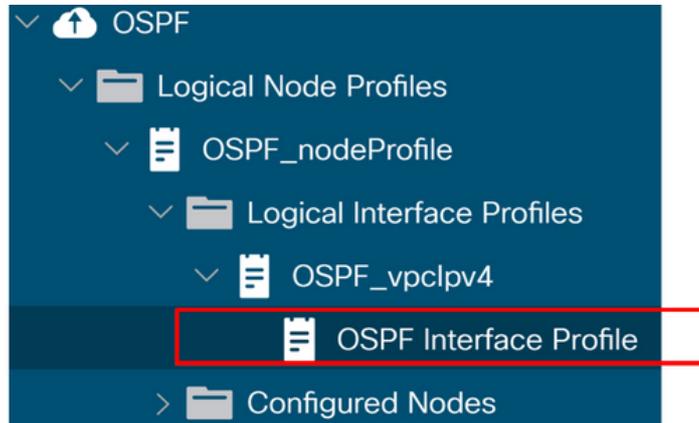
Path	Side A IP	Side B IP	Secondary IP Address	IP Address	MAC Address	MTU (bytes)	Encap	Encap Scope
Pod-1/Node-103-104/N9K_VPC_3-4_13	10.10.34.3/29	10.10.34.4/29	10.10.34.2/29	0.0.0.0	00:22:BD:F8:19:FF	9000	vlan-2502	Local

O MTU padrão na ACI é de 9000 bytes, em vez de 1500 bytes, que é geralmente o padrão usado em dispositivos de roteamento tradicionais. Verifique se a MTU corresponde ao dispositivo

externo. Quando o estabelecimento do vizinho OSPF falha devido à MTU, ele fica preso em EXCHANGE/DROTHER.

- Máscara de sub-rede IP. O OSPF requer que o IP vizinho use a mesma máscara de sub-rede.
- OSPF Interface Profile (Perfil da interface OSPF).

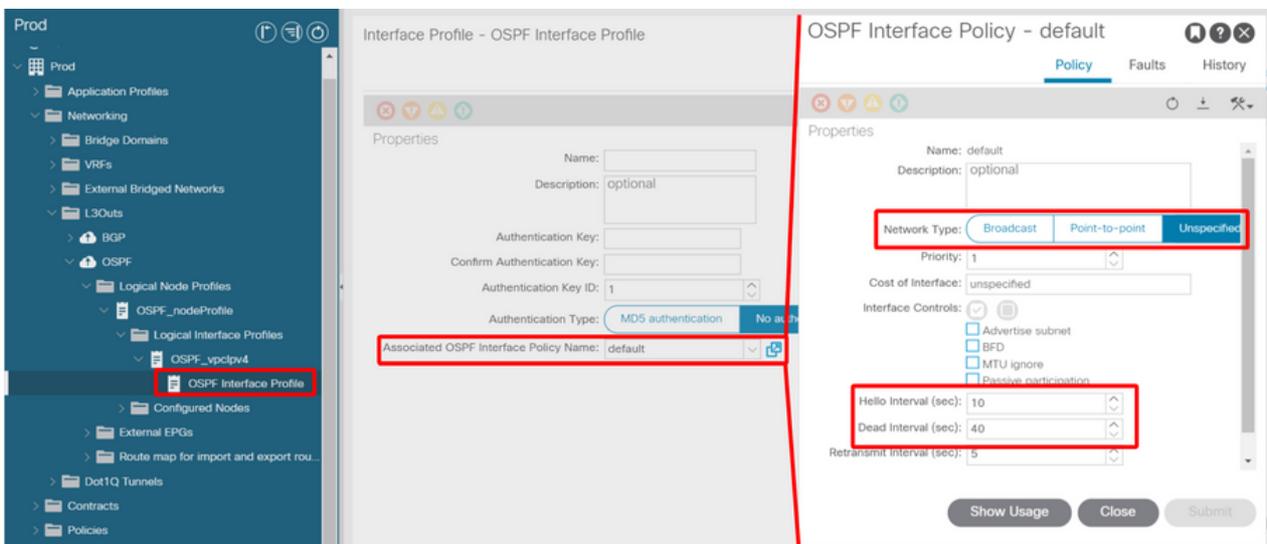
## Perfil de interface OSPF



Isso equivale a 'ip router ospf <tag> area <area id>' em uma configuração NX-OS autônoma para ativar o OSPF na interface. Sem isso, as interfaces leaf não se unirão ao OSPF.

- Temporizador Hello / Dead do OSPF, tipo de rede

## Perfil de interface OSPF — temporizador Hello / Dead e tipo de rede



## Detalhes da política de interface OSPF

# Create OSPF Interface Policy



Name: OSPFIntPolicy

Description: optional

Network Type:  Broadcast  Point-to-point  Unspecified

Priority: 1

Cost of Interface: unspecified

Interface Controls:

- Advertise subnet
- BFD
- MTU ignore
- Passive participation

Hello Interval (sec): 10

Dead Interval (sec): 40

Retransmit Interval (sec): 5

Transmit Delay (sec): 1

O OSPF requer que os temporizadores Hello e Dead correspondam em cada dispositivo vizinho. Eles são configurados no OSPF Interface Profile.

Certifique-se de que o tipo de rede da interface OSPF corresponda ao dispositivo externo. Quando o dispositivo externo usa o tipo Ponto a Ponto, o lado da ACI também precisa configurar explicitamente Ponto a Ponto. Eles também são configurados no OSPF Interface Profile.

## verificação CLI do OSPF

As saídas CLI nas etapas a seguir são coletadas do BL3 na topologia da seção "Visão geral".

### 1. Verifique o status do vizinho OSPF

Se 'State' for 'FULL' na seguinte CLI, o vizinho OSPF está estabelecido corretamente. Caso contrário, vá para a próxima etapa para verificar os parâmetros.

```
f2-leaf3# show ip ospf neighbors vrf Prod:VRF2
OSPF Process ID default VRF Prod:VRF2
Total number of neighbors: 2
Neighbor ID      Pri State                Up Time  Address        Interface
10.0.0.4         1 FULL/DR              00:47:30 10.10.34.4     Vlan28        <--- neighbor with BL4
10.0.0.134       1 FULL/DROTHER        00:00:21 10.10.34.1     Vlan28        <--- neighbor with R34
```

Na ACI, os BLs formarão vizinhanças OSPF entre si sobre roteadores externos ao usar o mesmo ID de VLAN com um SVI. Isso ocorre porque a ACI tem um domínio de inundação interno chamado L3Out BD (ou BD externo) para cada ID de VLAN nas SVIs L3Out. Observe que a

VLAN ID 28 é uma VLAN interna chamada PI-VLAN (Platform-Independent VLAN) em vez da VLAN real (Access Encap VLAN) usada no fio. Use o comando a seguir para verificar a VLAN do access encap ('vlan-2502').

```
f2-leaf3# show vlan id 28 extended
```

VLAN Name	Encap	Ports
28	vxlan-14942176, vlan-2502	Eth1/13, Po1

Pode-se obter a mesma saída também através do ID da VLAN do encapsulamento de acesso.

```
f2-leaf3# show vlan encap-id 2502 extended
```

VLAN Name	Encap	Ports
28	vxlan-14942176, vlan-2502	Eth1/13, Po1

## 2. Verificar a área do OSPF

Certifique-se de que o ID e o Tipo da área OSPF sejam idênticos aos vizinhos. Se o perfil da interface OSPF estiver ausente, a interface não se juntará ao OSPF e não aparecerá na saída CLI do OSPF.

```
f2-leaf3# show ip ospf interface brief vrf Prod:VRF2
```

```
OSPF Process ID default VRF Prod:VRF2
Total number of interface: 1
Interface          ID      Area          Cost   State   Neighbors Status
Vlan28             94     0.0.0.1       4      BDR    2         up
```

```
f2-leaf3# show ip ospf vrf Prod:VRF2
```

```
Routing Process default with ID 10.0.0.3 VRF Prod:VRF2
```

```
...
Area (0.0.0.1)
Area has existed for 00:59:14
Interfaces in this area: 1 Active interfaces: 1
Passive interfaces: 0 Loopback interfaces: 0
This area is a NSSA area
Perform type-7/type-5 LSA translation
SPF calculation has run 10 times
Last SPF ran for 0.001175s
Area ranges are
Area-filter in 'exp-ctx-proto-3112960'
Area-filter out 'permit-all'
Number of LSAs: 4, checksum sum 0x0
```

## 3. Verifique os detalhes da interface OSPF

Certifique-se de que os parâmetros de nível de interface atendam aos requisitos para o estabelecimento de vizinhos OSPF, como sub-rede IP, tipo de rede, temporizador Hello/Dead. Observe a ID da VLAN para especificar que o SVI é PI-VLAN (vlan28)

```
f2-leaf3# show ip ospf interface vrf Prod:VRF2
```

```
Vlan28 is up, line protocol is up
IP address 10.10.34.3/29, Process ID default VRF Prod:VRF2, area 0.0.0.1
```

```
Enabled by interface configuration
State BDR, Network type BROADCAST, cost 4
Index 94, Transmit delay 1 sec, Router Priority 1
Designated Router ID: 10.0.0.4, address: 10.10.34.4
Backup Designated Router ID: 10.0.0.3, address: 10.10.34.3
2 Neighbors, flooding to 2, adjacent with 2
Timer intervals: Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello timer due in 0.000000
No authentication
Number of opaque link LSAs: 0, checksum sum 0
```

```
f2-leaf3# show interface vlan28
Vlan28 is up, line protocol is up, autostate disabled
Hardware EtherSVI, address is 0022.bdf8.19ff
Internet Address is 10.10.34.3/29
MTU 9000 bytes, BW 10000000 Kbit, DLY 1 usec
```

#### 4. Verifique a acessibilidade do IP ao vizinho

Embora os pacotes Hello do OSPF sejam pacotes de Multicast local de link, os pacotes DBD do OSPF necessários para a primeira troca LSDB do OSPF são unicast. Portanto, a acessibilidade unicast também precisa ser verificada para o estabelecimento de vizinhança OSPF.

```
f2-leaf3# iping 10.10.34.1 -v Prod:VRF2
PING 10.10.34.1 (10.10.34.1) from 10.10.34.3: 56 data bytes
64 bytes from 10.10.34.1: icmp_seq=0 ttl=255 time=0.66 ms
64 bytes from 10.10.34.1: icmp_seq=1 ttl=255 time=0.653 ms
```

#### 5. Verifique o mesmo no roteador externo

A seguir estão exemplos de configurações no roteador externo (NX-OS independente)

```
router ospf 1
  vrf f2-ospf
  router-id 10.0.0.134
  area 0.0.0.1 nssa

interface Vlan2502
  no shutdown
  mtu 9000
  vrf member f2-ospf
  ip address 10.10.34.1/29
  ip router ospf 1 area 0.0.0.1
```

Certifique-se de verificar a MTU também na interface física.

#### 6. Etapa adicional — tcpdump

Nos nós leaf da ACI, o usuário pode executar tcpdump na interface da CPU 'kpm\_inb' para verificar se os pacotes de protocolo chegaram à CPU leaf. Embora haja vários filtros para o OSPF, o número de protocolo IP é o filtro mais abrangente.

- Número do protocolo IP: proto 89 (IPv4) ou ip6 proto 0x59 (IPv6)
- Endereço IP do vizinho: host <ip>
- IP Mcast Local de Link OSPF: host 224.0.0.5 ou host 224.0.0.6

```
f2-leaf3# tcpdump -ni kpm_inb proto 89
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on kpm_inb, link-type EN10MB (Ethernet), capture size 65535 bytes
22:28:38.231356 IP 10.10.34.4 > 224.0.0.5: OSPFv2, Hello, length 52
22:28:42.673810 IP 10.10.34.3 > 224.0.0.5: OSPFv2, Hello, length 52
22:28:44.767616 IP 10.10.34.1 > 224.0.0.5: OSPFv2, Hello, length 52
22:28:44.769092 IP 10.10.34.3 > 10.10.34.1: OSPFv2, Database Description, length 32
22:28:44.769803 IP 10.10.34.1 > 10.10.34.3: OSPFv2, Database Description, length 32
22:28:44.775376 IP 10.10.34.3 > 10.10.34.1: OSPFv2, Database Description, length 112
22:28:44.780959 IP 10.10.34.1 > 10.10.34.3: OSPFv2, LS-Request, length 36
22:28:44.781376 IP 10.10.34.3 > 10.10.34.1: OSPFv2, LS-Update, length 64
22:28:44.790931 IP 10.10.34.1 > 224.0.0.6: OSPFv2, LS-Update, length 64
```

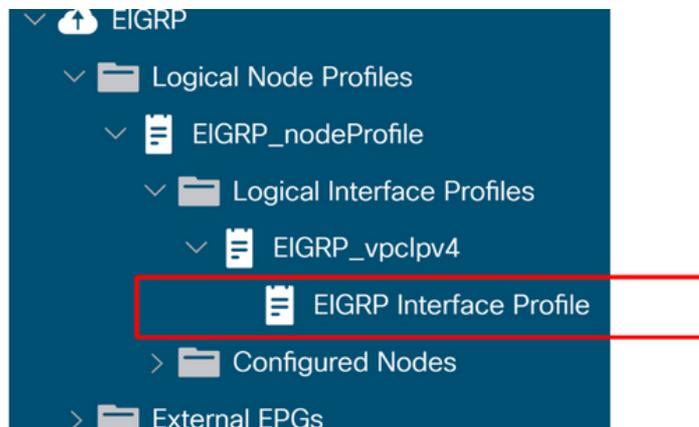
## EIGRP

Esta seção usa um exemplo de vizinhança EIGRP entre BL3, BL4 e R34 da topologia na seção "Visão Geral" com EIGRP AS 10.

A seguir estão os critérios comuns para o estabelecimento de adjacências EIGRP.

- EIGRP AS: Um AS EIGRP é atribuído a um L3Out. Isso precisa corresponder ao dispositivo externo.
- Perfil de Interface EIGRP.

### Perfil de Interface EIGRP



Isso é equivalente à configuração 'ip router eigrp <as>' em um dispositivo NX-OS autônomo. Sem isso, as interfaces leaf não se unirão ao EIGRP.

- MTU

Embora isso não tenha que coincidir para simplesmente estabelecer a vizinhança EIGRP, os pacotes de troca de topologia EIGRP podem se tornar maiores do que a MTU máxima permitida nas interfaces entre os peers e, como esses pacotes não podem ser fragmentados, eles são descartados e, como resultado, a vizinhança EIGRP sofrerá flap.

### Verificação CLI do EIGRP

As saídas CLI nas etapas a seguir são coletadas do BL3 na topologia da seção "Visão geral".

#### 1. Verifique o status do vizinho EIGRP

```
f2-leaf3# show ip eigrp neighbors vrf Prod:VRF3
```

```
EIGRP neighbors for process 10 VRF Prod:VRF3
```

H	Address	Interface	Hold (sec)	Uptime	SRTT (ms)	RTO	Q Cnt	Seq Num	
0	10.10.34.4	vlan29	14	00:12:58	1	50	0	6	<--- neighbor with BL4
1	10.10.34.1	vlan29	13	00:08:44	2	50	0	4	<--- neighbor with R34

Na ACI, os BLs formarão uma vizinhança EIGRP entre si sobre os roteadores externos quando usarem o mesmo ID de VLAN com SVI. Isso ocorre porque uma ACI tem um domínio de inundação interno chamado L3Out BD (ou BD externo) para cada ID de VLAN em L3Out SVIs.

Observe que a VLAN ID 29 é uma VLAN interna chamada PI-VLAN (Platform-Independent VLAN) em vez da VLAN real (Access Encap VLAN) usada no fio. Use o comando a seguir para verificar a VLAN do access encap (vlan-2503).

```
f2-leaf3# show vlan id 29 extended
```

VLAN Name	Encap	Ports
29 Prod:VRF3:l3out-EIGRP:vlan-2503	vxlan-15237052, vlan-2503	Eth1/13, Po1

Pode-se obter a mesma saída também através do ID da VLAN do encapsulamento de acesso.

```
f2-leaf3# show vlan encap-id 2503 extended
```

VLAN Name	Encap	Ports
29 Prod:VRF3:l3out-EIGRP:vlan-2503	vxlan-15237052, vlan-2503	Eth1/13, Po1

## 2. Verifique os detalhes da interface do EIGRP

Certifique-se de que o EIGRP esteja sendo executado na interface esperada. Caso contrário, marque Perfil de Interface Lógico e Perfil de Interface EIGRP.

```
f2-leaf3# show ip eigrp interfaces vrf Prod:VRF3
```

```
EIGRP interfaces for process 10 VRF Prod:VRF3
```

Interface	Peers	Xmit Queue Un/Reliable	Mean SRTT	Pacing Time Un/Reliable	Multicast Flow Timer	Pending Routes
vlan29	2	0/0	1	0/0	50	0

Hello interval is 5 sec  
Holdtime interval is 15 sec  
Next xmit serial: 0  
Un/reliable mcasts: 0/2 Un/reliable ucasts: 5/10  
Mcast exceptions: 0 CR packets: 0 ACKs suppressed: 2  
Retransmissions sent: 2 Out-of-sequence rcvd: 0  
Classic/wide metric peers: 2/0

```
f2-leaf3# show int vlan 29
```

```
Vlan29 is up, line protocol is up, autostate disabled  
Hardware EtherSVI, address is 0022.bdf8.19ff  
Internet Address is 10.10.34.3/29
```

MTU 9000 bytes, BW 10000000 Kbit, DLY 1 usec

### 3. Verifique o mesmo no roteador externo

Veja a seguir o exemplo de configuração no roteador externo (NX-OS independente).

```
router eigrp 10
vrf f2-eigrp

interface Vlan2503
no shutdown
vrf member f2-eigrp
ip address 10.10.34.1/29
ip router eigrp 10
```

### 4. Etapa adicional — tcpdump

Nos nós de folha da ACI, o usuário pode executar tcpdump na interface da CPU 'kpm\_inb' para confirmar se os pacotes de protocolo chegaram à CPU da folha. Use o número de protocolo IP 88 (EIGRP) como um filtro.

```
f2-leaf3# tcpdump -ni kpm_inb proto 88
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on kpm_inb, link-type EN10MB (Ethernet), capture size 65535 bytes
23:29:43.725676 IP 10.10.34.3 > 224.0.0.10: EIGRP Hello, length: 40
23:29:43.726271 IP 10.10.34.4 > 224.0.0.10: EIGRP Hello, length: 40
23:29:43.728178 IP 10.10.34.1 > 224.0.0.10: EIGRP Hello, length: 40
23:29:45.729114 IP 10.10.34.1 > 10.10.34.3: EIGRP Update, length: 20
23:29:48.316895 IP 10.10.34.3 > 224.0.0.10: EIGRP Hello, length: 40
```

## Anúncio de rota

Esta seção se concentra na verificação e na solução de problemas de anúncio de rota na ACI. Especificamente, ele analisa exemplos que envolvem:

- Anúncio de sub-rede de domínios de bridge.
- Anúncio de rota de trânsito.
- Controle de rota de importação e exportação.

Esta seção discute o vazamento de rota como se refere a L3Outs compartilhados em seções posteriores.

### Fluxo de trabalho de anúncio de rota de domínio de ponte

Antes de examinar a solução de problemas comum, o usuário deve se familiarizar com como o anúncio do domínio de ponte deve funcionar.

O anúncio de BD, quando o BD e L3Out estão no mesmo VRF, envolve:

- Ter um relacionamento de contrato entre a L3Out e o EPG interno.
- Associando o L3Out ao Domínio de Bridge.
- Selecionando 'Anunciar Externamente' na sub-rede BD.

Além disso, também é possível controlar o anúncio do domínio de ponte usando perfis de rota de exportação que impedem a necessidade de associar o L3Out. No entanto, 'Anunciar externamente' ainda deve ser selecionado. Este é um caso de uso menos comum, portanto ele não será discutido aqui.

O relacionamento de contrato entre L3Out e o EPG é necessário para fazer com que a rota estática pervasiva BD seja enviada para o BL. O anúncio de rota real é tratado através da redistribuição da rota estática no protocolo externo. Por fim, os mapas de rota de redistribuição só serão instalados nas L3Outs associadas ao BD. Dessa forma, a rota não é anunciada por todos os L3Outs.

Nesse caso, a sub-rede BD é 192.168.1.0/24 e deve ser anunciada via OSPF L3Out.

### Antes de aplicar o contrato entre a L3Out e o EPG interno

```
leaf103# show ip route 192.168.1.0/24 vrf Prod:Vrf1
IP Route Table for VRF "Prod:Vrf1"
'*' denotes best ucast next-hop
***' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%' in via output denotes VRF
Route not found
```

Observe que a rota BD ainda não está presente no BL.

### Depois de aplicar o contrato entre a L3Out e o EPG interno

Neste ponto, nenhuma outra configuração foi feita. O L3Out ainda não está associado ao BD e o sinalizador 'Anunciar Externamente' não está definido.

```
leaf103# show ip route 10.0.1.0/24 vrf Prod:Vrf1
IP Route Table for VRF "Prod:Vrf1"
'*' denotes best ucast next-hop
***' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%' in via output denotes VRF
192.168.1.0/24, ubest/mbest: 1/0, attached, direct, pervasive
  *via 10.0.120.34%overlay-1, [1/0], 00:00:08, static, tag 4294967294
    recursive next hop: 10.0.120.34/32%overlay-1
```

Observe que a rota de sub-rede de BD (indicada pelo flag pervasivo) agora está implantada no BL. Observe, no entanto, que a rota está marcada. Este valor de tag é um valor implícito atribuído a rotas BD antes de ser configurado com 'Anunciar Externamente'. Todos os protocolos externos impedem que essa marca seja redistribuída.

### Após selecionar 'Anunciar Externamente' na Sub-rede BD

O L3Out ainda não foi associado ao BD. Entretanto, observe que a marca foi apagada.

```
leaf103# show ip route 192.168.1.0/24 vrf Prod:Vrf1
IP Route Table for VRF "Prod:Vrf1"
```

'\*' denotes best ucast next-hop  
'\*\*' denotes best mcast next-hop  
'[x/y]' denotes [preference/metric]  
'%' in via output denotes VRF  
192.168.1.0/24, ubest/mbest: 1/0, attached, direct, pervasive \*via 10.0.120.34%overlay-1, [1/0],  
00:00:06, static recursive next hop: 10.0.120.34/32%overlay-1

Neste ponto, a rota ainda não está sendo anunciada externamente porque não há um mapa de rota e uma lista de prefixos que correspondam a esse prefixo para redistribuição no protocolo externo. Isso pode ser verificado com os seguintes comandos:

```
leaf103# show ip ospf vrf Prod:Vrf1
Routing Process default with ID 10.0.0.3 VRF Prod:Vrf1
Stateful High Availability enabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
Table-map using route-map exp-ctx-2392068-deny-external-tag
Redistributing External Routes from
  static route-map exp-ctx-st-2392068
  direct route-map exp-ctx-st-2392068
  bgp route-map exp-ctx-PROTO-2392068
  eigrp route-map exp-ctx-PROTO-2392068
  coop route-map exp-ctx-st-2392068
```

A rota de BD é programada como uma rota estática, portanto, verifique o mapa de rota de redistribuição estática executando 'show route-map <route-map name>' e, em seguida, 'show ip prefix-list <name>' em qualquer lista de prefixo presente no mapa de rota. Faça isso na próxima etapa.

## Após associar L3Out ao BD

Como mencionado anteriormente, essa etapa resulta na lista de prefixos que corresponde à sub-rede BD sendo instalada no mapa de rota de redistribuição de protocolo estático para externo.

```
leaf103# show route-map exp-ctx-st-2392068
route-map exp-ctx-st-2392068, deny, sequence 1
  Match clauses:
    tag: 4294967294
  Set clauses:

...
route-map exp-ctx-st-2392068, permit, sequence 15803
  Match clauses:
    ip address prefix-lists: IPv4-st16390-2392068-exc-int-inferred-export-dst
    ipv6 address prefix-lists: IPv6-deny-all
  Set clauses:
    tag 0
```

Verifique a lista de prefixos:

```
leaf103# show ip prefix-list IPv4-st16390-2392068-exc-int-inferred-export-dst
ip prefix-list IPv4-st16390-2392068-exc-int-inferred-export-dst: 1 entries
  seq 1 permit 192.168.1.1/24
```

A sub-rede BD está sendo combinada para redistribuir no OSPF.

Neste ponto, o fluxo de trabalho de configuração e verificação está concluído para o anúncio da sub-rede BD fora da L3Out. Depois desse ponto, a verificação seria específica do protocolo. Por

exemplo:

- Para EIGRP, verifique se a rota está sendo instalada na tabela de topologia com 'show ip eigrp topology vrf <name>'
- Para OSPF, verifique se a rota está sendo instalada na tabela do banco de dados como um LSA externo com 'show ip ospf database vrf <name>'
- Para BGP, verifique se a rota está no RIB BGP com 'show bgp ipv4 unicast vrf <name>'

## anúncio de rota BGP

Para o BGP, todas as rotas estáticas são permitidas implicitamente para redistribuição. O mapa de rota que corresponde à sub-rede BD é aplicado no nível de vizinho BGP.

```
leaf103# show bgp ipv4 unicast neighbor 10.0.0.134 vrf Prod:Vrf1 | grep Outbound
Outbound route-map configured is exp-l3out-BGP-peer-2392068, handle obtained
```

No exemplo acima, 10.0.0.134 é o vizinho BGP configurado dentro da L3Out.

## anúncio de rota EIGRP

Como o OSPF, um mapa de rotas é usado para controlar a redistribuição de Estático para EIGRP. Dessa forma, somente as sub-redes associadas à L3Out e definidas como 'Anunciar Externamente' devem ser redistribuídas. Isso pode ser verificado com este comando:

```
leaf103# show ip eigrp vrf Prod:Vrf1
IP-EIGRP AS 100 ID 10.0.0.3 VRF Prod:Vrf1
Process-tag: default
Instance Number: 1
Status: running
Authentication mode: none
Authentication key-chain: none
Metric weights: K1=1 K2=0 K3=1 K4=0 K5=0
metric version: 32bit
IP proto: 88 Multicast group: 224.0.0.10
Int distance: 90 Ext distance: 170
Max paths: 8
Active Interval: 3 minute(s)
Number of EIGRP interfaces: 1 (0 loopbacks)
Number of EIGRP passive interfaces: 0
Number of EIGRP peers: 2
Redistributing:
  static route-map exp-ctx-st-2392068
  ospf-default route-map exp-ctx-PROTO-2392068
  direct route-map exp-ctx-st-2392068
  coop route-map exp-ctx-st-2392068
  bgp-65001 route-map exp-ctx-PROTO-2392068
```

A configuração final de BD em funcionamento é mostrada abaixo.

## Configuração da L3 do Domínio de Bridge

The screenshot displays the Cisco APIC interface for configuring a Bridge Domain (BD1). The left sidebar shows the navigation tree with 'Networking' and 'Bridge Domains' expanded, and 'BD1' selected. The main content area shows the 'Policy' tab, 'L3 Configurations' sub-tab, and a table of subnets. The subnet 192.168.1.1/24 is highlighted, showing it is advertised externally. The 'Associated L3 Outs' section shows 'L3 Out' with 'OSPF' selected. The status bar at the top shows '100' and various icons.

## Cenário de solução de problemas de anúncio de rota de domínio de ponte

Nesse caso, o sintoma típico seria normalmente que uma sub-rede BD configurada não está sendo anunciada fora de uma L3Out. Siga o fluxo de trabalho anterior para entender qual componente foi desfeito.

Comece com a configuração antes de obter um nível muito baixo verificando o seguinte:

- Há um contrato entre o EPG e a L3Out?
- A L3Out está associada ao BD?
- A sub-rede BD está definida para anunciar externamente?
- A adjacência de protocolo externo está ativa?

### Possível causa: BD não implantado

Esse caso seria aplicável em alguns cenários diferentes, como:

- O EPG interno está usando a integração do VMM com a opção Sob demanda e nenhum ponto de extremidade da VM foi anexado ao grupo de portas do EPG.
- O EPG interno foi criado, mas nenhuma associação de caminho estático foi configurada ou a interface na qual o caminho estático está configurado está inoperante.

Em ambos os casos, o BD não seria implantado e, como resultado, a rota estática do BD não seria enviada para o BL. A solução aqui é implantar alguns recursos ativos em um EPG que está vinculado a este BD para que a sub-rede seja implantada.

### Possível causa: OSPF L3Out está configurado como 'Stub' ou 'NSSA' sem redistribuição

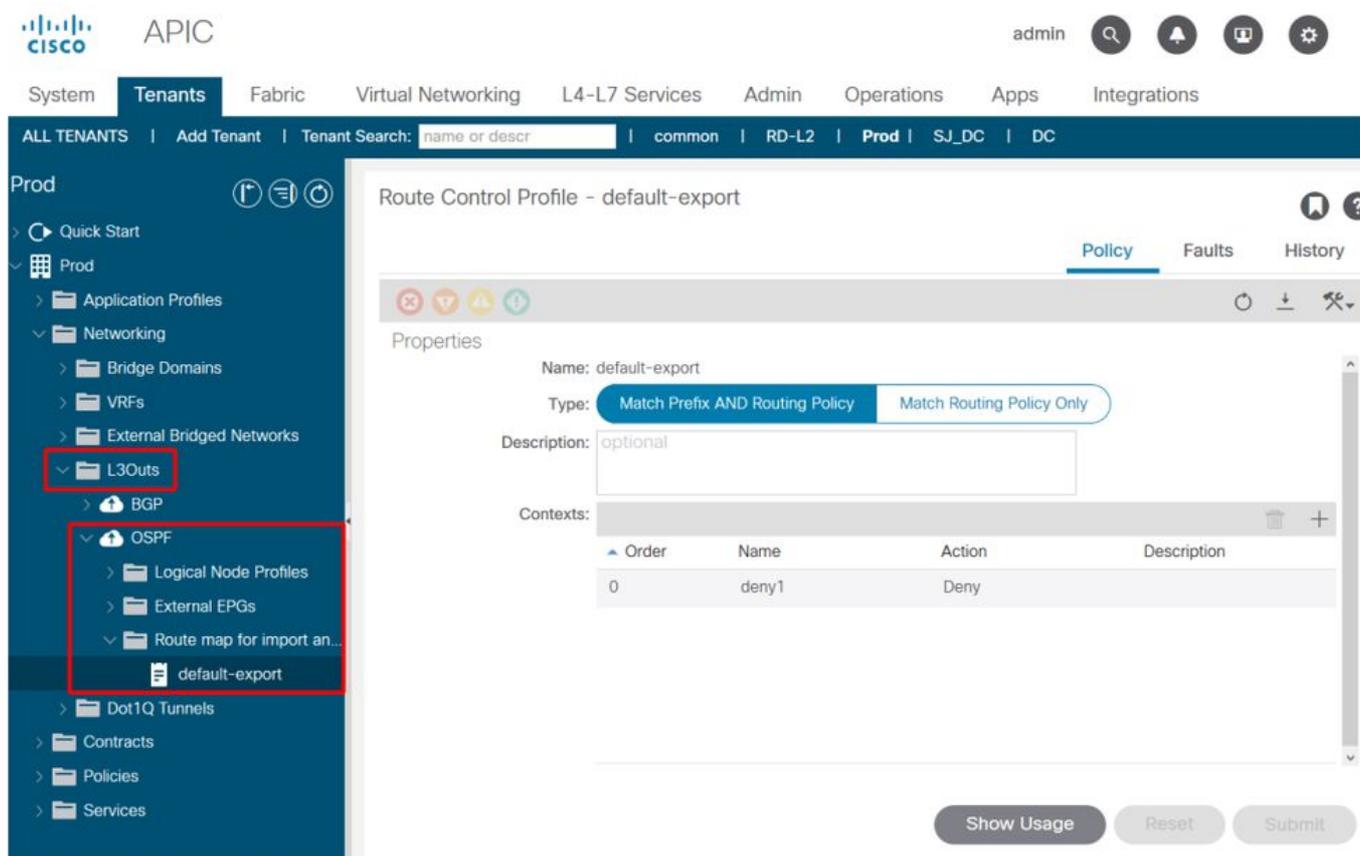
Quando o OSPF é usado como o protocolo L3Out, as regras básicas do OSPF ainda devem ser

seguidas. As áreas stub não permitem LSAs redistribuídos, mas podem anunciar uma rota padrão. As áreas NSSA permitem caminhos redistribuídos, mas 'Enviar LSAs redistribuídos para a área NSSA' deve ser selecionado em L3Out. Ou o NSSA também pode anunciar uma rota padrão, desabilitando 'LSA de resumo de origem', que é um cenário típico em que 'Enviar LSAs redistribuídos na área NSSA' seria desabilitado.

### Possível causa: Perfil de Rota 'Default-Export' com uma Ação 'Deny' configurada na L3Out

Quando os perfis de rota são configurados em uma L3Out com os nomes 'default-export' ou 'default-import', eles são implicitamente aplicados à L3Out. Além disso, se o perfil de rota de exportação padrão for definido para uma ação de negação e configurado como 'Match Prefix and Routing Policy', as sub-redes BD deverão ser anunciadas fora desta L3Out e serão implicitamente negadas:

### Perfil de rota de negação de exportação padrão



As correspondências de prefixo dentro do perfil de rota de exportação padrão não incluirão implicitamente sub-redes BD se a opção 'Corresponder somente à política de roteamento' estiver selecionada.

### Fluxo de trabalho de importação de roteiro externo

Esta seção discute como a ACI aprende rotas externas através de uma L3Out e distribui isso para nós de leaf internos. Ele também abrange casos de uso de vazamento de trânsito e rota em seções posteriores

Como na seção anterior, o usuário deve estar ciente do que acontece em um nível superior.

Por padrão, todas as rotas aprendidas através do protocolo externo são redistribuídas no processo BGP de estrutura interna. Isso é verdadeiro independentemente de quais sub-redes estão configuradas no EPG externo e quais sinalizadores estão selecionados. Há dois exemplos em que isso não é verdade.

- Se a opção 'Aplicação de controle de rota' na política L3Out de nível superior estiver definida como 'Importar'. Nesse caso, o modelo de importação de rota passaria de um modelo de lista de bloqueio (especifique apenas o que não deve ser permitido) para um modelo de lista de permissão (tudo é implicitamente negado, a menos que configurado de outra forma).
- Se o protocolo externo for EIGRP ou OSPF e um Interleak Route-Profile usado não corresponder às rotas externas.

Para que uma rota externa seja distribuída para uma folha interna, o seguinte deve acontecer:

- A rota deve ser aprendida no BL a partir do roteador externo. Para ser um candidato a redistribuir no processo MP-BGP da estrutura, a rota deve ser instalada na tabela de roteamento, e não apenas no protocolo RIB.
- A rota deve ter permissão para ser redistribuída ou anunciada no processo BGP interno. Isso deve sempre acontecer, a menos que seja usada a imposição de controle de rota de importação ou um Interleak Route-Profile.
- Uma Política de Refletor de Rota BGP deve ser configurada e aplicada a um Grupo de Política de Pod que seja aplicado ao Perfil de Pod. Se isso não for aplicado, o processo BGP não será inicializado nos switches.

Se o EPG/BD interno estiver no mesmo VRF que o L3Out, as três etapas acima serão todas necessárias para que o EPG/BD interno use rotas externas.

## A rota está instalada na tabela de roteamento BL

Nesse caso, a rota externa que deve ser aprendida nos BLs 103 e 104 é 172.16.20.1/32.

```
leaf103# show ip route 172.16.20.1 vrf Prod:Vrf1
IP Route Table for VRF "Prod:Vrf1"
'*' denotes best ucast next-hop
***' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'% ' in via output denotes VRF

172.16.20.1/32, ubest/mbest: 1/0
   *via 10.10.34.3, vlan347, [110/20], 00:06:29, ospf-default, type-2
```

É evidente que ele está instalado na tabela de roteamento como sendo aprendido através do OSPF. Se não foi visto aqui, verifique o protocolo individual e assegure que as adjacências estejam ativas. A rota é redistribuída no BGP. O mapa de rota de redistribuição pode ser verificado, depois de verificar que nem a aplicação 'Import' ou Interleak Route-Profiles são usados, olhando o mapa de rota usado para o protocolo externo para redistribuição BGP. Consulte o seguinte comando:

```
leaf103# show bgp process vrf Prod:Vrf1

Information regarding configured VRFs:

BGP Information for VRF Prod:Vrf1
```

```
VRF Type : System
VRF Id : 85
VRF state : UP
VRF configured : yes
VRF refcount : 1
VRF VNID : 2392068
Router-ID : 10.0.0.3
Configured Router-ID : 10.0.0.3
Confed-ID : 0
Cluster-ID : 0.0.0.0
MSITE Cluster-ID : 0.0.0.0
No. of configured peers : 1
No. of pending config peers : 0
No. of established peers : 1
VRF RD : 101:2392068
VRF EVPN RD : 101:2392068
```

...

```
Redistribution
  direct, route-map permit-all
  static, route-map imp-ctx-bgp-st-interleak-2392068
  ospf, route-map permit-all
  coop, route-map exp-ctx-st-2392068
  eigrp, route-map permit-all
```

Aqui é evidente que o mapa de rota 'permit-all' é usado para redistribuição de OSPF para BGP. Esse é o padrão. A partir daqui, o BL pode ser verificado e a rota local originária do BGP verificada:

```
a-leaf101# show bgp ipv4 unicast 172.16.20.1/32 vrf Prod:Vrf1
BGP routing table information for VRF Prod:Vrf1, address family IPv4 Unicast
BGP routing table entry for 172.16.20.1/32, version 25 dest ptr 0xa6f25ad0
Paths: (2 available, best #2)
Flags: (0x80c0002 00000000) on xmit-list, is not in urib, exported
  vpn: version 16316, (0x100002) on xmit-list
Multipath: eBGP iBGP
```

```
Advertised path-id 1, VPN AF advertised path-id 1
Path type: redistrib 0x408 0x1 ref 0 adv path ref 2, path is valid, is best path
AS-Path: NONE, path locally originated
  0.0.0.0 (metric 0) from 0.0.0.0 (10.0.0.3)
  Origin incomplete, MED 20, localpref 100, weight 32768
  Extcommunity:
    RT:65001:2392068
    VNID:2392068
    COST:pre-bestpath:162:110
```

```
VRF advertise information:
Path-id 1 not advertised to any peer
```

```
VPN AF advertise information:
Path-id 1 advertised to peers:
  10.0.64.64          10.0.72.66
Path-id 2 not advertised to any peer
```

Na saída acima, 0.0.0.0/0 indica que ela foi originada localmente. A lista de pares anunciados são os nós spine na estrutura que atuam como refletos de rota.

## Verificar rota em folha interna

O BL deve anunciá-lo aos nós spine por meio da família de endereços BGP VPNv4. Os nós spine devem anunciá-lo a todos os nós de folha com o VRF implantado (verdadeiro no exemplo sem vazamento de rota). Em qualquer um desses nós folha, execute 'show bgp vpnv4 unicast <route> vrf overlay-1' para verificar se ele está em VPNv4

Use o comando abaixo para verificar a rota no leaf interno.

```
leaf101# show ip route 172.16.20.1 vrf Prod:Vrf1
IP Route Table for VRF "Prod:Vrf1"
 '*' denotes best ucast next-hop
 '**' denotes best mcast next-hop
 '[x/y]' denotes [preference/metric]
 '%' in via output denotes VRF

172.16.20.1/32, ubest/mbest: 2/0
  *via 10.0.72.64%overlay-1, [200/20], 00:21:24, bgp-65001, internal, tag 65001
    recursive next hop: 10.0.72.64/32%overlay-1
  *via 10.0.72.67%overlay-1, [200/20], 00:21:24, bgp-65001, internal, tag 65001
    recursive next hop: 10.0.72.67/32%overlay-1
```

Na saída acima, a rota está sendo aprendida por BGP e os próximos saltos devem ser os TEPs físicos (PTEP) dos BLs.

```
leaf101# acidiag fmvread
      ID  Pod ID          Name      Serial Number      IP Address      Role      State
LastUpdMsgId
-----
      103     1      a-leaf101  FDO20160TPS      10.0.72.67/32   leaf
active    0
      104     1      a-leaf103  FDO20160TQ0      10.0.72.64/32   leaf
active    0
```

## Cenário de solução de problemas de rota externa

Neste cenário, a folha interna (101) não está recebendo uma ou mais rotas externas.

Como sempre, primeiro verifique o básico. Verifique se:

- As adjacências do protocolo de roteamento estão ativas nos BLs.
- Uma Política de Refletor de Rota BGP é aplicada ao Grupo de Políticas do Pod e ao Perfil do Pod.

Se os critérios acima estiverem corretos, abaixo estão alguns exemplos mais avançados do que pode estar causando o problema.

### Possível causa: VRF não implantado no leaf interno

Nesse caso, o problema seria que não há EPGs com recursos implantados na folha interna onde a rota externa é esperada. Isso pode ser causado por ligações de caminho estático configuradas apenas em interfaces inativas ou ter apenas EPGs integrados do VMM no modo sob demanda presentes sem anexos dinâmicos detectados.

Como o L3Out VRF não é implantado na folha interna (verifique com 'show vrf' na folha interna), a folha interna não importará a rota BGP do VPNv4.

Para resolver esse problema, o usuário deve implantar recursos no L3Out VRF no leaf interno.

### Possível causa: A Imposição de Rota de Importação está sendo usada

Como mencionado anteriormente, quando a imposição de controle de rota de importação está habilitada, o L3Out aceita apenas rotas externas explicitamente permitidas. Normalmente, o recurso é implementado como um mapa de tabela. Um mapa de tabela fica entre o protocolo RIB e a tabela de roteamento real de modo que ele afete apenas o que está na tabela de roteamento.

Na saída abaixo, o controle de rota de importação está ativado, mas não há nenhuma rota explicitamente permitida. Observe que o LSA está no banco de dados OSPF, mas não na tabela de roteamento no BL:

```
leaf103# vsh -c "show ip ospf database external 172.16.20.1 vrf Prod:Vrf1"
      OSPF Router with ID (10.0.0.3) (Process ID default VRF Prod:Vrf1)
```

#### Type-5 AS External Link States

Link ID	ADV Router	Age	Seq#	Checksum	Tag
172.16.20.1	10.0.0.134	455	0x80000003	0xb9a0	0

```
leaf103# show ip route 172.16.20.1 vrf Prod:Vrf1
```

```
IP Route Table for VRF "Prod:Vrf1"
'*' denotes best ucast next-hop
***' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'% ' in via output denotes VRF
```

```
Route not found
```

Aqui está o mapa de tabela que está instalado causando este comportamento:

```
leaf103# show ip ospf vrf Prod:Vrf1
```

```
Routing Process default with ID 10.0.0.3 VRF Prod:Vrf1
Stateful High Availability enabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
Table-map using route-map exp-ctx-2392068-deny-external-tag
Redistributing External Routes from..
```

```
leaf103# show route-map exp-ctx-2392068-deny-external-tag
```

```
route-map exp-ctx-2392068-deny-external-tag, deny, sequence 1
```

```
Match clauses:
```

```
tag: 4294967295
```

```
Set clauses:
```

```
route-map exp-ctx-2392068-deny-external-tag, deny, sequence 19999
```

```
Match clauses:
```

```
ospf-area: 0.0.0.100
```

```
Set clauses:
```

Qualquer aprendizado na área 100, que é a área configurada nesta L3Out, é implicitamente

negado por este mapa de tabela para que não seja instalado na tabela de roteamento.

Para resolver esse problema, o usuário deve definir a sub-rede no EPG externo com o sinalizador 'Import Route Control Subnet' ou criar um perfil de rota de importação que corresponda aos prefixos a serem instalados.

- Observe que a imposição de importação não é suportada para EIGRP.
- Observe também que para o BGP, a aplicação de importação é implementada como um mapa de rota de entrada aplicado ao vizinho BGP. Verifique a subseção "Anúncio de rota BGP" para obter detalhes sobre como verificar isso.

### Possível causa: um Interleak Profile está sendo usado

Os Interleak Route-Profiles são usados para L3Outs do EIGRP e do OSPF e destinados a permitir o controle sobre o que é redistribuído do IGP para o BGP, bem como permite a aplicação de políticas como a configuração de atributos do BGP.

Sem um perfil de rota de interleak, todas as rotas são implicitamente importadas para o BGP.

Sem um perfil de rota de intervazamento:

```
leaf103# show bgp process vrf Prod:Vrf1
```

Information regarding configured VRFs:

BGP Information for VRF Prod:Vrf1

```
VRF Type           : System
VRF Id             : 85
VRF state          : UP
VRF configured     : yes
VRF refcount       : 1
VRF VNID           : 2392068
Router-ID          : 10.0.0.3
Configured Router-ID : 10.0.0.3
Confed-ID          : 0
Cluster-ID         : 0.0.0.0
MSITE Cluster-ID   : 0.0.0.0
No. of configured peers : 1
No. of pending config peers : 0
No. of established peers : 1
VRF RD             : 101:2392068
VRF EVPN RD        : 101:2392068
```

...

Peers	Active-peers	Routes	Paths	Networks	Aggregates
1	1	7	11	0	0

Redistribution

```
direct, route-map permit-all
static, route-map imp-ctx-bgp-st-interleak-2392068
ospf, route-map permit-all
coop, route-map exp-ctx-st-2392068
eigrp, route-map permit-all
```

Com um perfil de rota de interfuga:

```
a-leaf103# show bgp process vrf Prod:Vrf1
```

Information regarding configured VRFs:

```
BGP Information for VRF Prod:Vrf1
VRF Type           : System
VRF Id             : 85
VRF state          : UP
VRF configured     : yes
VRF refcount       : 1
VRF VNID           : 2392068
Router-ID          : 10.0.0.3
Configured Router-ID : 10.0.0.3
Confed-ID          : 0
Cluster-ID         : 0.0.0.0
MSITE Cluster-ID   : 0.0.0.0
No. of configured peers : 1
No. of pending config peers : 0
No. of established peers : 1
VRF RD             : 101:2392068
VRF EVPN RD        : 101:2392068
```

...

```
Redistribution
  direct, route-map permit-all
  static, route-map imp-ctx-bgp-st-interleak-2392068
  ospf, route-map imp-ctx-proto-interleak-2392068
  coop, route-map exp-ctx-st-2392068
  eigrp, route-map permit-all
```

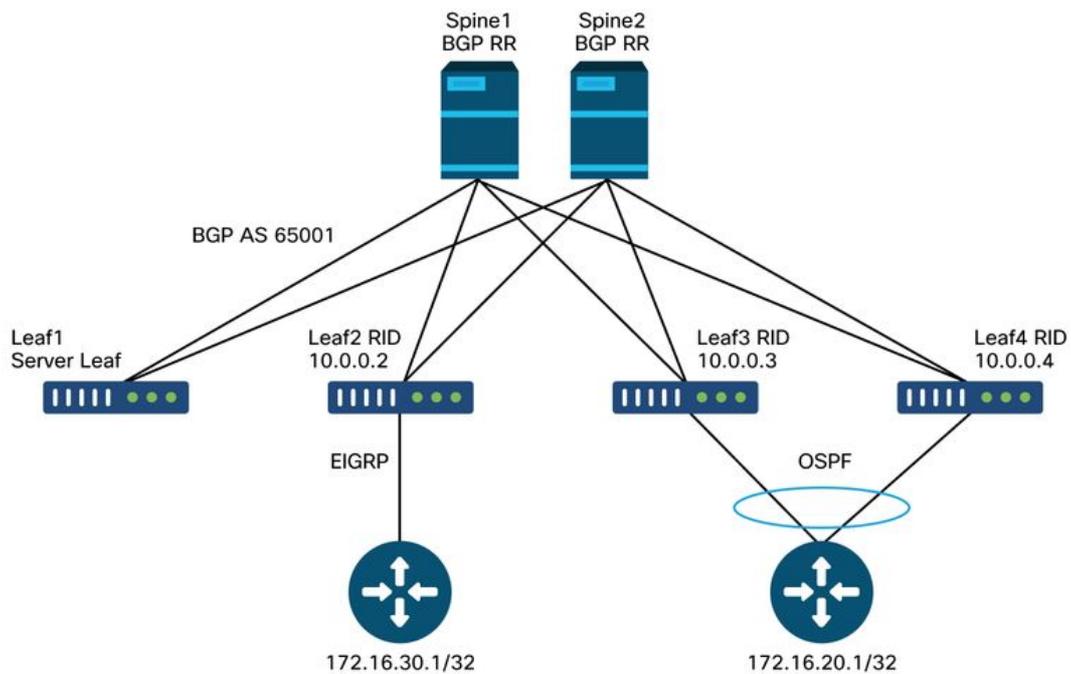
O mapa de rota destacado acima permitiria apenas o que é explicitamente correspondido no Interleak Profile configurado. Se a rota externa não corresponder, ela não será redistribuída no BGP.

## Fluxo de trabalho de anúncio de roteiro de trânsito

Esta seção discute como as rotas de uma L3Out são anunciadas por outra L3Out. Isso também cobriria o cenário em que as rotas estáticas configuradas diretamente em um L3Out precisam ser anunciadas. Ele não abordará cada consideração de protocolo específica, mas como isso é implementado na ACI. Não entrará no roteamento de trânsito entre VRF neste momento.

Este cenário usará a seguinte topologia:

## Topologia de roteamento de trânsito



O fluxo de alto nível de como 172.16.20.1 seria aprendido do OSPF e depois anunciado no EIGRP, e verificações de todo o processo e cenários de Troubleshooting, são discutidos abaixo.

Para que a rota 172.16.20.1 seja anunciada no EIGRP, uma das seguintes opções deve ser configurada:

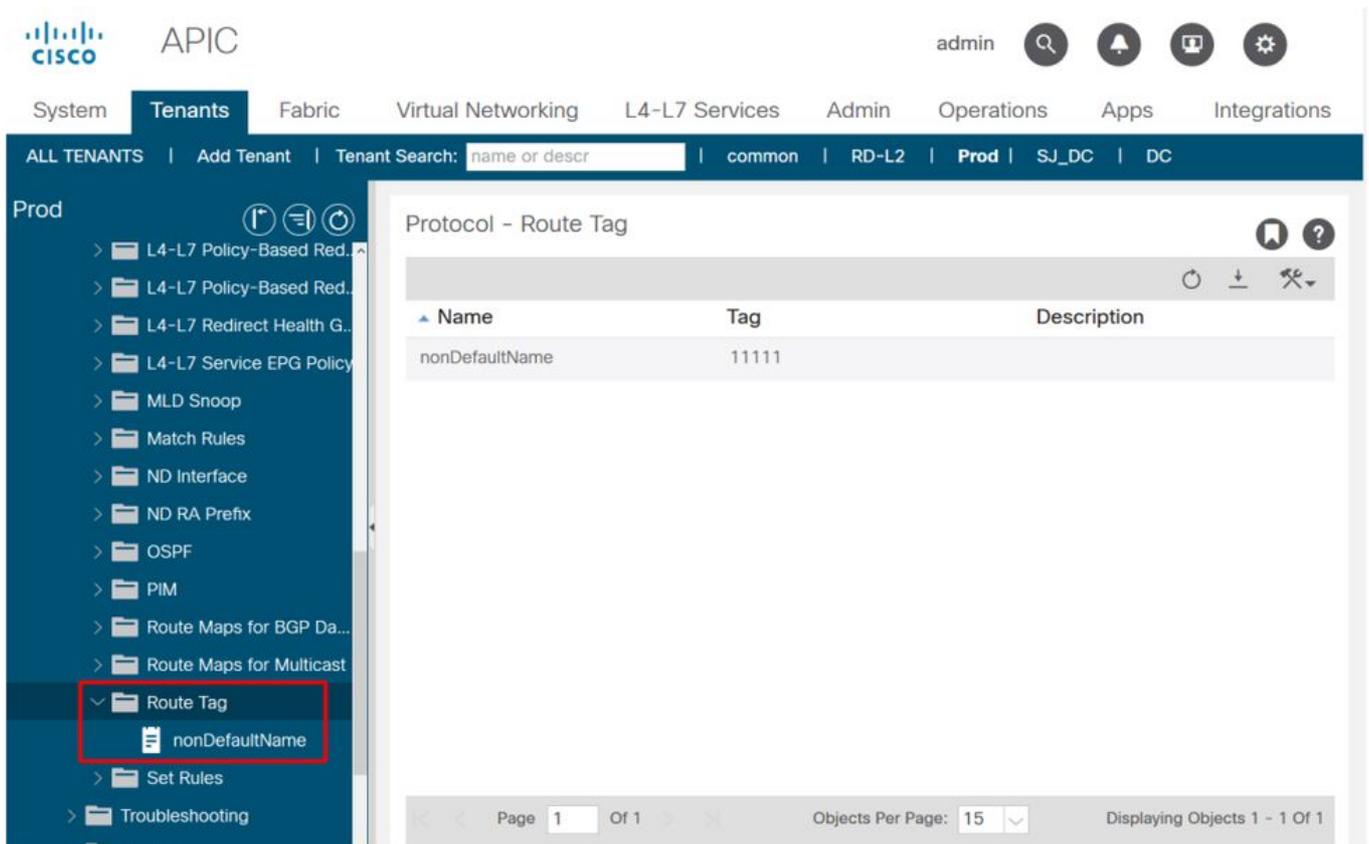
- A sub-rede a ser anunciada poderia ser definida na L3Out do EIGRP com o flag 'Export Route-Control Subnet'. Como mencionado na seção Visão geral, esse flag é usado principalmente para roteamento de trânsito e define as sub-redes que devem ser anunciadas fora desse L3Out.
- Configure 0.0.0.0/0 e selecione 'Aggregate Export' e 'Export Route Control Subnet'. Isso cria um mapa de rota para redistribuição no protocolo externo que corresponde a 0.0.0.0/0 e todos os prefixos que são mais específicos (que é uma correspondência efetiva qualquer). Observe que quando 0.0.0.0/0 é usado com 'Aggregate Export', as rotas estáticas não serão correspondidas para redistribuição. Isso evita anunciar inadvertidamente rotas BD que não devem ser anunciadas.
- Por fim, é possível criar um perfil de rota de exportação que corresponda aos prefixos a serem anunciados. O uso desse método poderia configurar a opção 'Aggregate' com prefixos além de 0.0.0.0/0.

As configurações acima resultariam no anúncio da rota de trânsito, mas ainda assim ela precisa ter uma política de segurança em vigor para permitir o fluxo do tráfego do dataplane. Como ocorre com qualquer comunicação de EPG para EPG, um contrato deve ser estabelecido antes que o tráfego seja permitido.

Observe que sub-redes externas duplicadas com a "Sub-rede externa para EPG externo" não podem ser configuradas no mesmo VRF. Quando configuradas, as sub-redes precisam ser mais específicas que 0.0.0.0. É importante configurar a 'Sub-rede externa para EPG externo' apenas para a L3Out onde a rota está sendo recebida. Não configure isso na L3Out que deveria estar anunciando essa rota.

Também é importante entender que todas as rotas de trânsito são marcadas com uma tag VRF específica. Por padrão, esta marca é 4294967295. A política de Marca de Rota é configurada em 'Locatário > Rede > Protocolos > Marca de Rota:

## Política de marcação de rota



The screenshot shows the Cisco APIC interface. The top navigation bar includes 'System', 'Tenants', 'Fabric', 'Virtual Networking', 'L4-L7 Services', 'Admin', 'Operations', 'Apps', and 'Integrations'. The 'Tenants' tab is active, and the 'Prod' tenant is selected. The left sidebar shows a tree view of configurations, with 'Route Tag' and its sub-item 'nonDefaultName' highlighted with a red box. The main content area displays the 'Protocol - Route Tag' configuration page, which includes a table with the following data:

Name	Tag	Description
nonDefaultName	11111	

At the bottom of the page, there is a pagination bar showing 'Page 1 Of 1', 'Objects Per Page: 15', and 'Displaying Objects 1 - 1 Of 1'.

Essa política de marcação de rota é então aplicada ao VRF. A finalidade dessa tag é essencialmente evitar loops. Essa marca de rota é aplicada quando a rota de trânsito é anunciada de volta em uma L3Out. Se essas rotas forem recebidas de volta com a mesma marca de rota, a rota será descartada.

### Verifique se a rota está presente no BL receptor via OSPF

Como na última seção, verifique primeiro se o BL que deve receber inicialmente a rota correta.

```
leaf103# show ip route 172.16.20.1 vrf Prod:Vrf1
IP Route Table for VRF "Prod:Vrf1"
'*' denotes best ucast next-hop
***' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
%' in via output denotes VRF

172.16.20.1/32, ubest/mbest: 1/0
  *via 10.10.34.3, vlan347, [110/20], 01:25:30, ospf-default, type-2
```

Por enquanto, suponha que o anúncio L3Out esteja em um BL diferente (como na topologia) (cenários posteriores discutirão onde ele está no mesmo BL).

### Verifique se a rota está presente no BGP no OSPF BL receptor

Para que a rota OSPF seja anunciada ao roteador EIGRP externo, a rota precisa ser anunciada

no BGP no OSPF BL receptor.

```
leaf103# show bgp ipv4 unicast 172.16.20.1/32 vrf Prod:Vrf1
BGP routing table information for VRF Prod:Vrf1, address family IPv4 Unicast
BGP routing table entry for 172.16.20.1/32, version 30 dest ptr 0xa6f25ad0
Paths: (2 available, best #1)
Flags: (0x80c0002 00000000) on xmit-list, is not in urib, exported
  vpn: version 17206, (0x100002) on xmit-list
Multipath: eBGP iBGP

  Advertised path-id 1, VPN AF advertised path-id 1
  Path type: redistrib 0x408 0x1 ref 0 adv path ref 2, path is valid, is best path
  AS-Path: NONE, path locally originated
    0.0.0.0 (metric 0) from 0.0.0.0 (10.0.0.3)
      Origin incomplete, MED 20, localpref 100, weight 32768
      Extcommunity:
        RT:65001:2392068
        VNID:2392068
        COST:pre-bestpath:162:110

VRF advertise information:

Path-id 1 not advertised to any peer

VPN AF advertise information:
Path-id 1 advertised to peers:
  10.0.64.64          10.0.72.66
Path-id 2 not advertised to any peer
```

A rota está no BGP.

Verifique no EIGRP BL que deve anunciar a rota que está instalada

```
leaf102# show ip route 172.16.20.1 vrf Prod:Vrf1
IP Route Table for VRF "Prod:Vrf1"
'*' denotes best ucast next-hop
'***' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%' in via output denotes VRF

172.16.20.1/32, ubest/mbest: 2/0
  *via 10.0.72.67%overlay-1, [200/20], 00:56:46, bgp-65001, internal, tag 65001
    recursive next hop: 10.0.72.67/32%overlay-1
  *via 10.0.72.64%overlay-1, [200/20], 00:56:46, bgp-65001, internal, tag 65001
    recursive next hop: 10.0.72.64/32%overlay-1
```

Ele é instalado na tabela de roteamento com próximos saltos de sobreposição que apontam para os nós de folha de borda de origem.

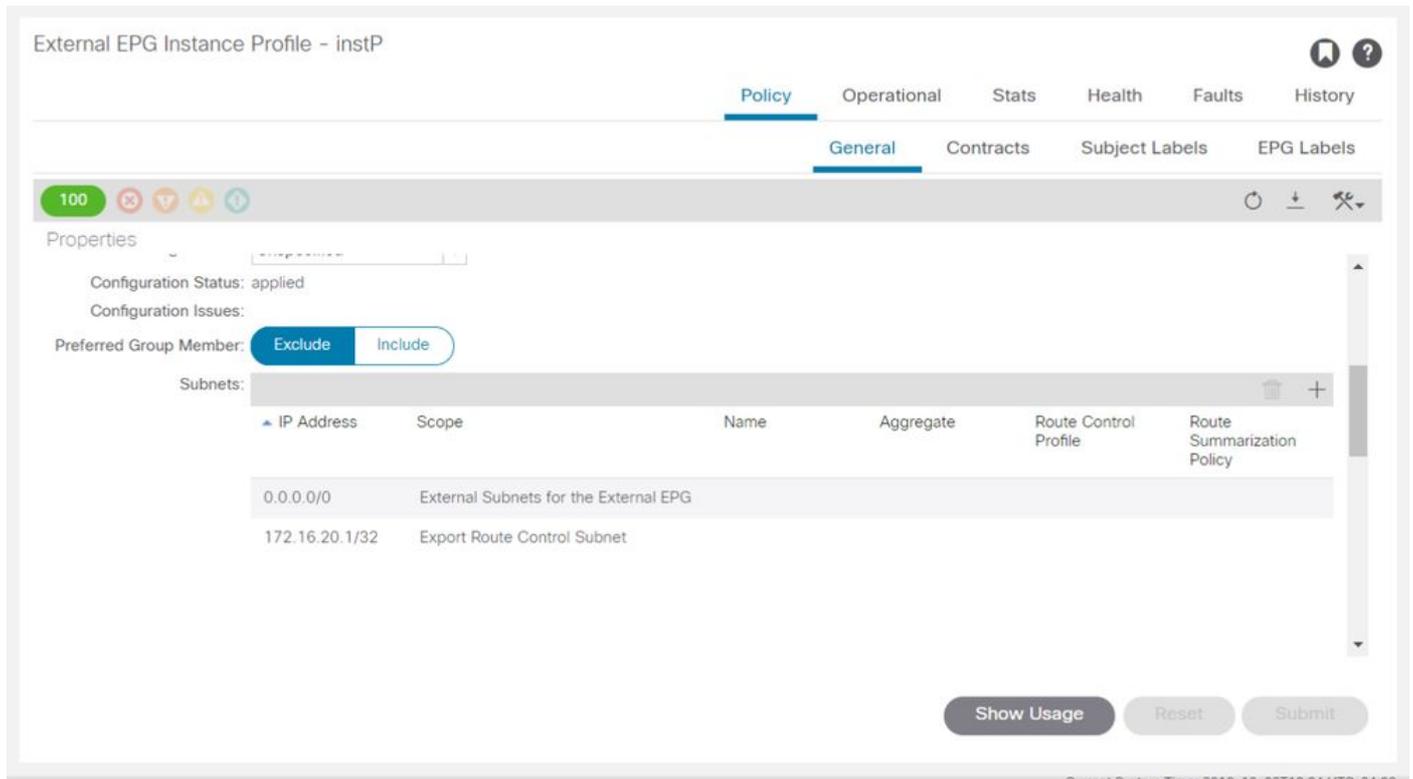
```
leaf102# acidiag fnvread

  ID   Pod ID           Name           Serial Number      IP Address          Role           State
LastUpdMsgId
-----
  103   1             a-leaf101      FDO20160TPS       10.0.72.67/32      leaf
active  0
```

## Verifique se a rota é anunciada no BL

A rota será anunciada pelo BL 102 como resultado da definição do sinalizador 'Sub-rede de controle de rota de exportação' na sub-rede configurada:

## Controle de rota de exportação



Use o comando a seguir para exibir o mapa de rotas criado como resultado do sinalizador 'Controle de rota de exportação':

```
leaf102# show ip eigrp vrf Prod:Vrf1
IP-EIGRP AS 101 ID 10.0.0.2 VRF Prod:Vrf1
  Process-tag: default
  Instance Number: 1
  Status: running
  Authentication mode: none
  Authentication key-chain: none
  Metric weights: K1=1 K2=0 K3=1 K4=0 K5=0
  metric version: 32bit
  IP proto: 88 Multicast group: 224.0.0.10
  Int distance: 90 Ext distance: 170
  Max paths: 8
  Active Interval: 3 minute(s)
  Number of EIGRP interfaces: 1 (0 loopbacks)
  Number of EIGRP passive interfaces: 0
  Number of EIGRP peers: 1
  Redistributing:
    static route-map exp-ctx-st-2392068
    ospf-default route-map exp-ctx-proto-2392068
    direct route-map exp-ctx-st-2392068
    coop route-map exp-ctx-st-2392068
```

Para procurar a 'redistribuição BGP > EIGRP', examine o mapa de rotas. Mas o mapa de rota em si deve ser o mesmo, independentemente de o protocolo de origem ser OSPF, EIGRP ou BGP. As rotas estáticas serão controladas com um mapa de rota diferente.

```
leaf102# show route-map exp-ctx-proto-2392068
route-map exp-ctx-proto-2392068, permit, sequence 15801
  Match clauses:
    ip address prefix-lists: IPv4-proto32771-2392068-exc-ext-inferred-export-dst
    ipv6 address prefix-lists: IPv6-deny-all
  Set clauses:
    tag 4294967295

a-leaf102# show ip prefix-list IPv4-proto32771-2392068-exc-ext-inferred-export-dst
ip prefix-list IPv4-proto32771-2392068-exc-ext-inferred-export-dst: 1 entries
seq 1 permit 172.16.20.1/32
```

Na saída acima, a marca VRF é definida nesse prefixo para prevenção de loop e a sub-rede configurada com "Controle de rota de exportação" é correspondida explicitamente.

## Roteamento de trânsito ao receber e anunciar BL são os mesmos

Conforme discutido anteriormente, quando os BLs de recebimento e anúncio são diferentes, a rota deve ser anunciada através da estrutura usando BGP. Quando os BLs são os mesmos, a redistribuição ou o anúncio pode ser feito diretamente entre os protocolos na folha.

Veja a seguir breves descrições de como isso é implementado:

- **Roteamento de trânsito entre duas L3Outs OSPF na mesma folha:** o anúncio de rota é controlado por meio de um 'filtro de área' aplicado ao nível do processo OSPF. Uma L3Out na área 0 deve ser implantada na folha, já que as rotas são anunciadas entre áreas, ao contrário de serem anunciadas por meio de redistribuição. Use 'show ip ospf vrf <name>' para exibir a lista de filtros. Exiba o conteúdo do filtro usando 'show route-map <filter name>'.
- **Roteamento de trânsito entre OSPF e EIGRP L3Outs na mesma folha:** o anúncio de rota é controlado através de mapas de rota de redistribuição que podem ser vistos com 'show ip ospf' e 'show ip eigrp'. Observe que se houver vários L3Outs OSPF no mesmo BL, a única maneira de redistribuir em apenas um desses L3Outs OSPF é se o outro for um Stub ou NSSA com '**Send redistributed LSAs into NSSA area**' desabilitado para que não permita nenhum LSA externo.
- **Roteamento de trânsito entre OSPF ou EIGRP e BGP na mesma folha:** O anúncio de rota no IGP é controlado através de mapas de rota de redistribuição. O anúncio de rota no BGP é controlado por meio de um mapa de rota de saída aplicado diretamente ao vizinho BGP ao qual a rota deve ser enviada. Isso pode ser verificado com 'show bgp ipv4 unicast neighbor <neighbor address> vrf <name> | grep Outbound'.
- **Roteamento de trânsito entre dois BGP I3Outs na mesma folha:** Todo o anúncio é controlado através de mapas de rota aplicados diretamente ao vizinho BGP para o qual a rota deve ser enviada. Isso pode ser verificado com 'show bgp ipv4 unicast neighbor <neighbor address> vrf <name> | grep Outbound'.

**Cenários de solução de problemas de roteamento de trânsito #1: Rota de trânsito não anunciada**

Este cenário de Troubleshooting envolve rotas que devem ser aprendidas através de um L3Out não sendo enviadas para fora do outro L3Out.

Como sempre, verifique os conceitos básicos antes de analisar qualquer coisa específica da ACI.

- As adjacências de protocolo estão ativas?
- A rota, que a ACI deve anunciar, foi aprendida com um protocolo externo?
- Para o BGP, o caminho está sendo descartado devido a algum atributo de BGP? (as-path, etc.).
- O L3Out receptor o tem no banco de dados OSPF, na tabela de topologia EIGRP ou na tabela BGP?
- Uma Política de Refletor de Rota BGP é aplicada ao Grupo de Política de Pod que é aplicado ao Perfil de Pod?

Se todas as verificações de protocolo básicas estiverem configuradas corretamente, abaixo estão algumas outras causas comuns para uma rota de trânsito que não está sendo anunciada.

#### **Possível causa: Sem área 0 do OSPF**

Se a topologia afetada envolve dois OSP L3Outs na mesma folha de borda, então deve haver uma Área 0 para que as rotas sejam anunciadas de uma área para outra. Examine o marcador "Roteamento de trânsito entre dois L3Outs OSPF na mesma folha" acima para obter mais detalhes.

#### **Possível causa: A área OSPF é stub ou NSSA**

Isso seria visto se o OSPF L3Out fosse configurado com uma área Stub ou NSSA que não estivesse configurada para anunciar LSAs externos. Com o OSPF, os LSAs externos nunca são anunciados em áreas de stub. Eles serão anunciados em áreas NSSA se a opção 'Enviar LSAs redistribuídos para a área NSSA' estiver selecionada.

#### **Cenários de solução de problemas de roteamento de trânsito #2: Rota de trânsito não recebida**

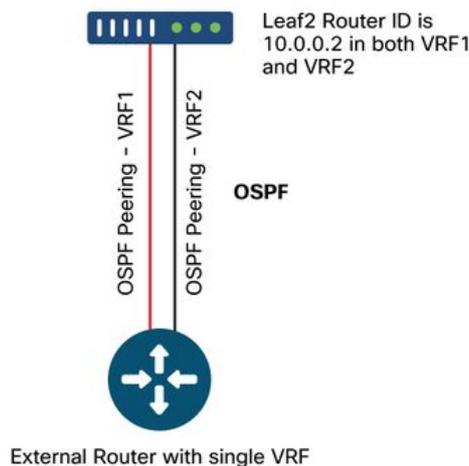
Neste cenário, o problema é que algumas rotas anunciadas por uma ACI L3Out não estão sendo recebidas de volta em outra L3Out. Esse cenário pode ser aplicável se os L3Outs estiverem em duas estruturas separadas e forem conectados por roteadores externos ou se os L3Outs estiverem em VRFs diferentes e as rotas estiverem sendo passadas entre os VRFs por um roteador externo.

#### **Possível causa: O BL está configurado com o mesmo ID de roteador em vários VRFs**

De uma perspectiva de configuração, um router-id não pode ser duplicado dentro do mesmo VRF. No entanto, geralmente é bom usar o mesmo router-id em VRFs diferentes, desde que os dois VRFs não estejam conectados aos mesmos domínios de protocolo de roteamento.

Considere a seguinte topologia:

#### **Roteador externo com VRF único — Rota de trânsito não recebida**



O problema aqui seria que a folha da ACI vê LSAs com seu próprio Router-ID sendo recebido, fazendo com que eles não sejam instalados no banco de dados OSPF.

Além disso, se a mesma configuração fosse vista com pares VPC, os LSAs seriam continuamente adicionados e excluídos em alguns roteadores. Por exemplo, o roteador veria LSAs vindos de seu peer VPC com VRF e LSAs vindos do mesmo nó (com o mesmo Router-ID) que foram originados no outro VRF.

Para resolver esse problema, o usuário deve certificar-se de que um nó terá um router-id diferente e exclusivo em cada VRF no qual ele tem um L3Out.

**Possível causa: rotas de uma L3Out em uma malha da ACI recebidas em outra malha com a mesma marca VRF**

A marcação de rota padrão na ACI é sempre a mesma, a menos que seja alterada. Se as rotas forem anunciadas de uma L3Out em uma estrutura de VRF ou ACI para outra L3Out em outra estrutura de VRF ou ACI sem alterar as marcas de VRF padrão, as rotas serão descartadas pelos BLs receptores.

A solução para esse cenário é simplesmente usar uma política exclusiva de marcação de rota para cada VRF na ACI.

**Cenários de identificação e solução de problemas de roteamento de trânsito #3 — Rotas de trânsito anunciadas inesperadamente**

Esse cenário seria visto quando as rotas de trânsito são anunciadas em uma L3Out onde não se pretende que sejam anunciadas.

**Possível causa: uso de 0.0.0.0/0 com 'Exportação Agregada'**

Quando uma sub-rede externa é configurada como 0.0.0.0/0 com 'Sub-rede de controle de rota de exportação' e 'Exportação agregada', o resultado é que uma correspondência de todos os mapas de rota de redistribuição é instalada. Nesse caso, todas as rotas no BL que foram aprendidas por OSPF, EIGRP ou BGP são anunciadas na L3Out onde isso é configurado.

Abaixo está o mapa de rota implantado no leaf como resultado da Exportação Agregada:

```

leaf102# show ip eigrp vrf Prod:Vrf1
IP-EIGRP AS 101 ID 10.0.0.2 VRF Prod:Vrf1
  Process-tag: default
  Instance Number: 1
  Status: running
  Authentication mode: none
  Authentication key-chain: none
  Metric weights: K1=1 K2=0 K3=1 K4=0 K5=0
  metric version: 32bit
  IP proto: 88 Multicast group: 224.0.0.10
  Int distance: 90 Ext distance: 170
  Max paths: 8
  Active Interval: 3 minute(s)
  Number of EIGRP interfaces: 1 (0 loopbacks)
  Number of EIGRP passive interfaces: 0
  Number of EIGRP peers: 1
  Redistributing:
    static route-map exp-ctx-st-2392068
    ospf-default route-map exp-ctx-PROTO-2392068
    direct route-map exp-ctx-st-2392068
    coop route-map exp-ctx-st-2392068
    bgp-65001 route-map exp-ctx-PROTO-2392068
  Tablemap: route-map exp-ctx-2392068-deny-external-tag , filter-configured
  Graceful-Restart: Enabled
  Stub-Routing: Disabled
  NSF converge time limit/expiries: 120/0
  NSF route-hold time limit/expiries: 240/0
  NSF signal time limit/expiries: 20/0
  Redistributed max-prefix: Disabled
  selfAdvRtTag: 4294967295
leaf102# show route-map exp-ctx-PROTO-2392068
route-map exp-ctx-PROTO-2392068, permit, sequence 19801
Match clauses:
  ip address prefix-lists: IPv4-PROTO32771-2392068-agg-ext-inferred-export-dst
  ipv6 address prefix-lists: IPv6-deny-all
Set clauses:
  tag 4294967295

```

```

leaf102# show ip prefix-list IPv4-PROTO32771-2392068-agg-ext-inferred-export-dst
  ip prefix-list IPv4-PROTO32771-2392068-agg-ext-inferred-export-dst: 1 entries
seq 1 permit 0.0.0.0/0 le 32

```

Essa é a principal causa dos loops de roteamento que envolvem um ambiente ACI.

## Contrato e L3Out

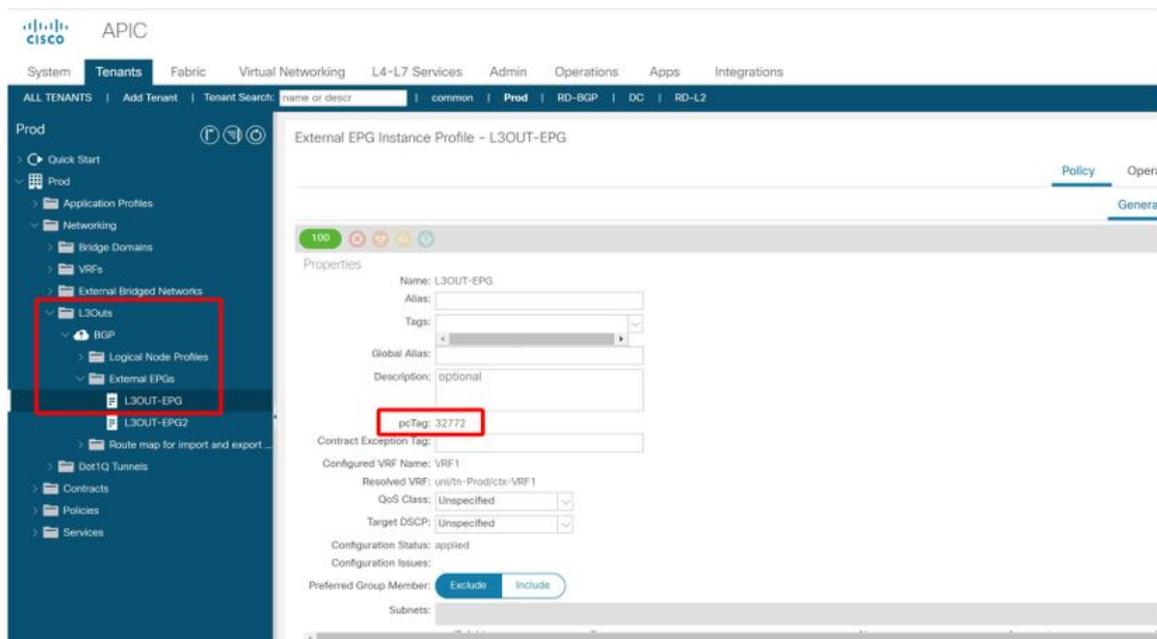
### EPG baseado em prefixo em L3Out

Em um EPG interno (que não seja L3Out), os contratos são aplicados após derivar o pcTag da origem e o pcTag do EPG de destino. A VLAN/VXLAN de encapsulamento do pacote recebido na porta de downlink é usada para conduzir esse pcTag classificando o pacote no EPG. Sempre que você aprende um endereço MAC ou um endereço IP, ele é aprendido junto com seu encapsulamento de acesso e o EPG pcTag associado. Para obter mais detalhes sobre a aplicação de pcTag e contratos, consulte o capítulo "Políticas de segurança".

L3Outs também dirigem um pcTag usando seu L3Out EPG (EPG externo) localizado em 'Locatário > Rede > L3OUT > Redes > L3OUT-EPG'. No entanto, L3Outs não dependem de VLANs e interfaces para classificar pacotes como tal. Em vez disso, a classificação é baseada no prefixo/sub-rede de origem em uma forma de 'Correspondência de Prefixo Mais Longa'. Portanto, um EPG L3Out pode ser chamado de **EPG baseado em prefixo**. Depois que um pacote é classificado em uma L3Out com base em uma sub-rede, ele segue um padrão de aplicação de política semelhante ao de um EPG regular.

O diagrama a seguir descreve onde o pcTag de um determinado EPG L3Out pode ser encontrado na GUI.

## Localização do pcTag para uma L3Out



O usuário é responsável por definir a tabela EPG baseada em prefixo. Isso é feito usando o escopo de sub-rede 'Sub-rede externa para EPG externo'. Cada conjunto de sub-redes com esse escopo adicionará uma entrada em uma tabela estática de LPM (Correspondência de Prefixo Mais Longo). Essa sub-rede apontará para o valor de pcTag que será usado para qualquer endereço IP que se enquadre nesse prefixo.

A tabela LPM de sub-redes EPG baseadas em prefixo pode ser verificada em switches leaf usando o seguinte comando:

```
vsh -c 'show system internal policy-mgr prefix'
```

Lembrete:

- As entradas da tabela LPM têm o escopo definido para VNID VRF. A pesquisa é feita por vrf\_vnid/src pcTag/dst pcTag.
- Cada entrada aponta para um único pcTag. Como consequência, dois EPGs L3Out não podem usar a mesma sub-rede com o mesmo comprimento de máscara dentro do mesmo VRF.
- A sub-rede 0.0.0.0/0 sempre usa pcTag 15 especial. Dessa forma, ela pode ser duplicada, mas só deve ser feita com um entendimento completo das implicações de aplicação da política.

- Esta tabela é usada em ambas as direções. De L3Out para Leaf Local Endpoint, o pcTag de origem é derivado usando essa tabela. Do Ponto de Extremidade Local de Folha para L3Out, o pcTag de destino é derivado usando esta tabela.
- Se o VRF tiver a configuração de imposição 'Ingress' para 'Policy Control Enforcement Direction', a tabela de prefixo LPM estará presente nos L3Out BLs, bem como em qualquer switch leaf no VRF que tenha um contrato com o L3Out.

## Exemplo 1: Saída L3 única com prefixo específico

**Cenário:** Um único BGP L3Out em vrf Prod:VRF1 com um L3Out EPG. O prefixo 172.16.1.0/24 está sendo recebido de uma fonte externa, portanto, deve ser classificado no EPG L3Out.

```
bdsol-aci32-leaf3# show ip route 172.16.1.0 vrf Prod:VRF1
IP Route Table for VRF "Prod:VRF1"
'*' denotes best ucast next-hop
 '**' denotes best mcast next-hop
 '[x/y]' denotes [preference/metric]
 '%' in via output denotes VRF

172.16.1.0/24, ubest/mbest: 1/0
  *via 10.0.0.134%Prod:VRF1, [20/0], 00:56:14, bgp-132, external, tag 65002
    recursive next hop: 10.0.0.134/32%Prod:VRF1
```

Primeiro, adicione a sub-rede à tabela de prefixos.

## Sub-rede com escopo 'Sub-redes Externas para o EPG Externo'

## Create Subnet

IP Address:   
address/mask

Name:

scope:  Export Route Control Subnet  
 Import Route Control Subnet  
 External Subnets for the External EPG  
 Shared Route Control Subnet  
 Shared Security Import Subnet

BGP Route Summarization Policy:

aggregate:  Aggregate Export  
 Aggregate Import  
 Aggregate Shared Routes

Route Control Profile:

Name	Direction

Verifique a programação da lista de prefixos nos switches leaf que têm o VRF da L3Out:

```
bdsol-aci32-leaf3# vsh -c ' show system internal policy-mgr prefix ' | egrep "Prod|==|Addr"
Vrf-Vni VRF-Id Table-Id Table-State VRF-Name Addr
Class Shared Remote Complete
=====
2097154 35 0x23 Up Prod:VRF1
0.0.0.0/0 15 True True False
2097154 35 0x23 Up Prod:VRF1
172.16.1.0/24 32772 True True False
```

O pcTag do EPG L3Out é 32772 no 2097154 de escopo vrf.

## Exemplo 2: Única L3Out com vários prefixos

Expandindo o exemplo anterior, neste cenário L3Out está recebendo vários prefixos. Ao inserir cada prefixo é funcionalmente sólido, uma opção alternativa (dependendo do projeto pretendido) é aceitar todos os prefixos recebidos no L3Out.

Isso pode ser feito com o prefixo '0.0.0.0/0'.

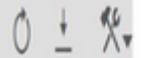
# Subnet - 0.0.0.0/0



Policy

Faults

History



## Properties

IP Address: 0.0.0.0/0  
address/mask

- Scope:
- Export Route Control Subnet
  - Import Route Control Subnet
  - External Subnets for the External EPG
  - Shared Route Control Subnet
  - Shared Security Import Subnet

- Aggregate:
- Aggregate Export
  - Aggregate Import
  - Aggregate Shared Routes

BGP Route Summarization Policy:

Route Control Profile:

Name ▲ Direction

No items have been found.  
Select Actions to create a new item.

Isso resulta na seguinte entrada da tabela de prefixos do policy-mgr:

```
bdsol-aci32-leaf3# vsh -c ' show system internal policy-mgr prefix ' | egrep "Prod|==|Addr"
Vrf-Vni VRF-Id Table-Id Table-State VRF-Name Addr
Class Shared Remote Complete
=====
2097154 35 0x23 Up Prod:VRF1
0.0.0.0/0 15 True True False
2097154 35 0x23 Up Prod:VRF1
172.16.1.0/24 32772 True True False
```

Observe que o pcTag atribuído a 0.0.0.0/0 usa o valor 15, não 32772. O pcTag 15 é um pcTag de sistema reservado que é usado apenas com 0.0.0.0/0, que age como caractere curinga para corresponder a todos os prefixos em um L3Out.

Se o VRF tiver uma única L3Out com um único EPG L3Out usando o 0.0.0.0/0, o prefixo de política permanecerá exclusivo e será a abordagem mais fácil para capturar tudo.

### Exemplo 3a: Vários EPGs L3Out em um VRF

Neste cenário, há vários EPGs L3Out no mesmo VRF.

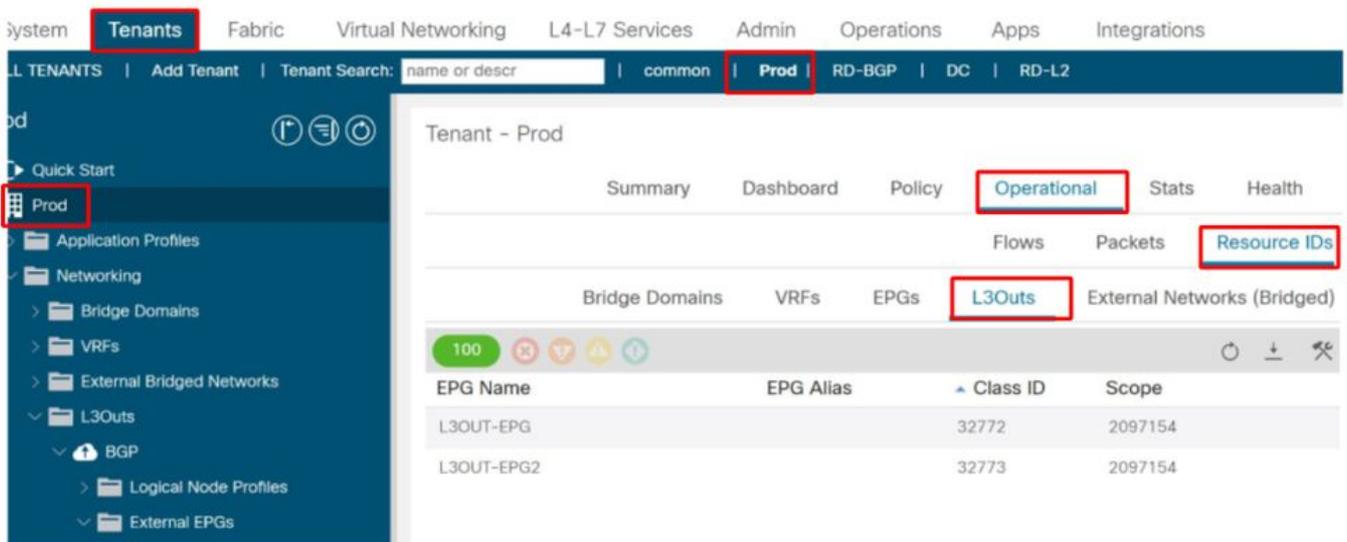
Note: De uma perspectiva do EPG baseado em prefixo, as duas configurações a seguir resultarão em entradas equivalentes na tabela de prefixos do gerenciador de políticas do LPM:

1. Duas L3Outs com uma L3Out EPG cada.
2. Uma L3Out com dois L3Out EPGs

Em ambos os cenários, o número total de EPGs L3Out é 2. Isso significa que cada um terá seu próprio pcTag e sub-redes associadas.

Todas as pcTags de um determinado EPG L3Out podem ser visualizadas na GUI em 'Locatário > Operacional > ID do recurso > L3Outs'

### Verificação do pcTag L3Out



Neste cenário, a estrutura da ACI está recebendo vários prefixos dos roteadores externos e a definição de L3Out EPG é a seguinte:

- 172.16.1.0/24 atribuído a L3OUT-EPG.
- 172.16.2.0/24 atribuído a L3OUT-EPG2.
- 172.16.0.0/16 atribuído a L3OUT-EPG (para capturar o prefixo 172.16.3.0/24).

Para corresponder a isso, a configuração será definida da seguinte maneira:

- L3OUT-EPG tem as sub-redes 172.16.1.0/24 e 172.16.0.0/16 com o escopo 'Sub-rede Externa para o EPG Externo'.
- L3OUT-EPG2 tem a sub-rede 172.16.2.0/24 com o escopo 'Sub-rede externa para o EPG externo'.

As entradas resultantes da tabela de prefixos serão:

```
bdsol-aci32-leaf3# vsh -c 'show system internal policy-mgr prefix' | egrep "Prod|==|Addr"
Vrf-Vni VRF-Id Table-Id Table-State VRF-Name Addr
Class Shared Remote Complete
=====
2097154 35 0x23 Up Prod:VRF1
0.0.0.0/0 15 True True False
2097154 35 0x23 Up Prod:VRF1
172.16.1.0/24 32772 True True False
2097154 35 0x23 Up Prod:VRF1
172.16.0.0/16 32772 True True False
2097154 35 0x23 Up Prod:VRF1
172.16.2.0/24 32773 True True False
```

172.16.2.0/24 é atribuído ao pcTag 32773 (L3OUT-EPG2) e 172.16.0.0/16 é atribuído ao 32772 (L3OUT-EPG).

Neste cenário, a entrada para 172.16.1.0/24 é redundante, pois a super-rede /16 é atribuída ao mesmo EPG.

Vários EPGs L3Out são úteis quando o objetivo é aplicar diferentes contratos a grupos de prefixos dentro de um único L3Out. O próximo exemplo ilustrará como os contratos entram em vigor com vários EPGs L3Out.

### Exemplo 3b: vários EPGs L3Out com contratos diferentes

Este cenário contém a seguinte configuração:

- Contrato ICMP permitindo somente ICMP.
- Contrato HTTP permitindo somente a porta 80 de destino tcp.
- O EPG1 (pcTag 32770) fornece o contrato HTTP consumido pelo L3OUT-EPG (pcTag 32772).
- O EPG2 (pcTag 32771) fornece o contrato ICMP consumido pelo L3OUT-EPG2 (pcTag 32773).

Os mesmos prefixos policymgr do exemplo anterior serão usados:

- 172.16.1.0/24 em L3OUT-EPG deve permitir HTTP para EPG1

- 172.16.2.0/24 em L3OUT-EPG2 deve permitir ICMP para EPG2
- policy-mgr prefix e zoning-rules:

```
bdsol-aci32-leaf3# vsh -c ' show system internal policy-mgr prefix ' | egrep "Prod|==|Addr"
Vrf-Vni VRF-Id Table-Id Table-State VRF-Name Addr
Class Shared Remote Complete
=====
=====
2097154 35 0x23 Up Prod:VRF1
0.0.0.0/0 15 True True False
2097154 35 0x23 Up Prod:VRF1
172.16.1.0/24 32772 True True False
2097154 35 0x23 Up Prod:VRF1
172.16.0.0/16 32772 True True False
2097154 35 0x23 Up Prod:VRF1
172.16.2.0/24 32773 True True False
```

```
bdsol-aci32-leaf3# show zoning-rule scope 2097154
```

```
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+
| Rule ID | SrcEPG | DstEPG | FilterID | Dir | operSt | Scope | Name | Action |
Priority |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+
| 4326 | 0 | 0 | implicit | uni-dir | enabled | 2097154 | | deny,log |
any_any_any(21) |
| 4335 | 0 | 16387 | implicit | uni-dir | enabled | 2097154 | | permit |
any_dest_any(16) |
| 4334 | 0 | 0 | implarp | uni-dir | enabled | 2097154 | | permit |
any_any_filter(17) |
| 4333 | 0 | 15 | implicit | uni-dir | enabled | 2097154 | | deny,log |
any_vrf_any_deny(22) |
| 4332 | 0 | 16386 | implicit | uni-dir | enabled | 2097154 | | permit |
any_dest_any(16) |
| 4342 | 32771 | 32773 | 5 | uni-dir-ignore | enabled | 2097154 | ICMP | permit |
fully_qual(7) |
| 4343 | 32773 | 32771 | 5 | bi-dir | enabled | 2097154 | ICMP | permit |
fully_qual(7) |
| 4340 | 32770 | 32772 | 38 | uni-dir | enabled | 2097154 | HTTP | permit |
fully_qual(7) |
| 4338 | 32772 | 32770 | 37 | uni-dir | enabled | 2097154 | HTTP | permit |
fully_qual(7) |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+
```

## Validação do caminho de dados usando Triagem — fluxo permitido pela política

Com um fluxo ICMP entre 172.16.2.1 na rede externa e 192.168.3.1 no EPG2, a Triagem pode ser usada para capturar e analisar o fluxo. Nesse caso, inicie a Triagem nos switches leaf 103 e 104, pois o tráfego pode entrar em qualquer um deles:

```
admin@apic1:~> ftriage route -ii LEAF:103,104 -sip 172.16.2.1 -dip 192.168.3.1
fTriage Status: {"dbgFtriage": {"attributes": {"operState": "InProgress", "pid": "14454",
"apicId": "1", "id": "0"}}}
Starting ftriage
Log file name for the current run is: ftlog_2019-10-02-22-30-41-871.txt
2019-10-02 22:30:41,874 INFO /controller/bin/ftriage route -ii LEAF:103,104 -sip 172.16.2.1
```

```

-dip 192.168.3.1
2019-10-02 22:31:28,868 INFO      ftriage:      main:1165 Invoking ftriage with default password
and default username: apic#fallback\admin
2019-10-02 22:32:15,076 INFO      ftriage:      main:839  L3 packet Seen on bdsol-aci32-leaf3
Ingress: Eth1/12 (Po1) Egress: Eth1/12 (Po1) Vnid: 11365
2019-10-02 22:32:15,295 INFO      ftriage:      main:242  ingress encap string vlan-2551
2019-10-02 22:32:17,839 INFO      ftriage:      main:271  Building ingress BD(s), Ctx
2019-10-02 22:32:20,583 INFO      ftriage:      main:294  Ingress BD(s) Prod:VRF1:l3out-BGP:vlan-
2551
2019-10-02 22:32:20,584 INFO      ftriage:      main:301  Ingress Ctx: Prod:VRF1
2019-10-02 22:32:20,693 INFO      ftriage:      pktrec:490 bdsol-aci32-leaf3: Collecting transient
losses snapshot for LC module: 1
2019-10-02 22:32:38,933 INFO      ftriage:      nxos:1404 bdsol-aci32-leaf3: nxos matching rule
id:4343 scope:34 filter:5
2019-10-02 22:32:39,931 INFO      ftriage:      main:522  Computed egress encap string vlan-2502
2019-10-02 22:32:39,933 INFO      ftriage:      main:313  Building egress BD(s), Ctx
2019-10-02 22:32:41,796 INFO      ftriage:      main:331  Egress Ctx Prod:VRF1
2019-10-02 22:32:41,796 INFO      ftriage:      main:332  Egress BD(s): Prod:BD2
2019-10-02 22:32:48,636 INFO      ftriage:      main:933  SIP 172.16.2.1 DIP 192.168.3.1
2019-10-02 22:32:48,637 INFO      ftriage:      unicast:973 bdsol-aci32-leaf3: <- is ingress node
2019-10-02 22:32:51,257 INFO      ftriage:      unicast:1202 bdsol-aci32-leaf3: Dst EP is local
2019-10-02 22:32:54,129 INFO      ftriage:      misc:657  bdsol-aci32-leaf3: EP if(Po1) same as
egr if(Po1)
2019-10-02 22:32:55,348 INFO      ftriage:      misc:657  bdsol-aci32-leaf3:
DMAC(00:22:BD:F8:19:FF) same as RMAC(00:22:BD:F8:19:FF)
2019-10-02 22:32:55,349 INFO      ftriage:      misc:659  bdsol-aci32-leaf3: L3 packet getting
routed/bounced in SUG
2019-10-02 22:32:55,596 INFO      ftriage:      misc:657  bdsol-aci32-leaf3: Dst IP is present in
SUG L3 tbl
2019-10-02 22:32:55,896 INFO      ftriage:      misc:657  bdsol-aci32-leaf3: RW seg_id:11365 in
SUG same as EP segid:11365
2019-10-02 22:33:02,150 INFO      ftriage:      main:961  Packet is Exiting fabric with peer-
device: bdsol-aci32-n3k-3 and peer-port: Ethernet1/16

```

**A triagem confirma o acerto da regra de zoneamento contra a regra ICMP de L3OUT\_EPG2 para EPG:**

```

2019-10-02 22:32:38,933 INFO      ftriage:      nxos:1404 bdsol-aci32-leaf3: nxos matching rule
id:4343 scope:34 filter:5

```

## **Validação do caminho de dados usando Triagem — fluxo não permitido pela política**

Com o tráfego ICMP originado de 172.16.1.1 (L3OUT-EPG) em direção a 192.168.3.1 (EPG2), espere uma queda de política.

```

admin@apic1:~> ftriage route -ii LEAF:103,104 -sip 172.16.1.1 -dip 192.168.3.1
fTriage Status: {"dbgFtriage": {"attributes": {"operState": "InProgress", "pid": "15139",
"apicId": "1", "id": "0"}}}
Starting ftriage
Log file name for the current run is: ftlog_2019-10-02-22-39-15-050.txt
2019-10-02 22:39:15,056 INFO      /controller/bin/ftriage route -ii LEAF:103,104 -sip 172.16.1.1
-dip 192.168.3.1
2019-10-02 22:40:03,523 INFO      ftriage:      main:1165 Invoking ftriage with default password
and default username: apic#fallback\admin
2019-10-02 22:40:43,338 ERROR      ftriage:      unicast:234 bdsol-aci32-leaf3: L3 packet getting fwd
dropped, checking drop reason
2019-10-02 22:40:43,339 ERROR      ftriage:      unicast:234 bdsol-aci32-leaf3: L3 packet getting fwd
dropped, checking drop reason
SECURITY_GROUP_DENY            condition setcast:236 bdsol-aci32-leaf3: Drop reason -

```

```

SECURITY_GROUP_DENY          condition set
2019-10-02 22:40:43,340 INFO   ftriage: unicast:252 bdsol-aci32-leaf3: policy drop flow
sclass:32772 dclass:32771 sg_label:34 proto:1
2019-10-02 22:40:43,340 INFO   ftriage:      main:681 : Ftriage Completed with hunch: None
fTriage Status: {"dbgFtriage": {"attributes": {"operState": "Idle", "pid": "0", "apicId": "0",
"id": "0"}}}

```

A triagem confirma que o pacote é descartado com o motivo SECURITY\_GROUP\_DENY (queda de política) e que o pcTag de origem derivado é 32772 e o pcTag de destino é 32771. Verificando isso com as regras de zoneamento, não há claramente entradas entre esses EPGs.

```

bdsol-aci32-leaf3# show zoning-rule scope 2097154 src-epg 32772 dst-epg 32771
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Rule ID | SrcEPG | DstEPG | FilterID | Dir | operSt | Scope | Name | Action | Priority |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+

```

## Exemplo 4: várias L3Outs com vários prefixos

O cenário é configurado de forma semelhante ao exemplo 3 (definições de EPG L3Out e L3Out), mas a rede definida em ambos os EPGs L3Out é 0.0.0.0/0.

A configuração do contrato é a seguinte:

- Contrato ICMP1 permitindo ICMP.
- Contrato ICMP2 permitindo ICMP.
- O EPG1 (pcTag 32770) fornece um contrato ICMP1 consumido pelo L3OUT-EPG (pcTag 32772).
- O EPG2 (pcTag 32771) fornece um contrato ICMP2 consumido por L3OUT-EPG2 (pcTag 32773).

Essa configuração pode parecer ideal no caso em que a rede externa está anunciando muitos prefixos, mas há pelo menos dois blocos de prefixos que seguem padrões de fluxo permitidos diferentes. Neste exemplo, um prefixo deve permitir apenas ICMP1 e o outro deve permitir apenas ICMP2.

Apesar de usar '0.0.0.0/0' duas vezes no mesmo VRF, apenas um prefixo é programado na tabela de prefixos do policy-mgr:

```

bdsol-aci32-leaf3# vsh -c ' show system internal policy-mgr prefix ' | egrep "Prod|==|Addr"
Vrf-Vni VRF-Id Table-Id Table-State VRF-Name Addr
Class Shared Remote Complete
=====
=====
2097154 35 0x23 Up Prod:VRF1

```

Dois fluxos reexaminados a seguir. Com base na configuração do contrato acima, espera-se o seguinte:

1. 172.16.2.1 (L3OUT-EPG2) a 192.168.3.1 (EPG2) **devem** ser permitidos pelo ICMP2
2. 172.16.2.1 (L3OUT-EPG2) para 192.168.1.1 (EPG1) **não** deve ser permitido, pois não há contrato entre EPG1 e L3OUT-EPG2

## Validação do caminho de dados usando Triagem — fluxo permitido pela política

Execute a triagem com um fluxo ICMP de 172.16.2.1 (L3OUT-EPG2) para 192.168.3.1 (EPG2 — pcTag 32771).

```
Starting ftriage
Log file name for the current run is: ftlog_2019-10-02-23-11-14-298.txt
2019-10-02 23:11:14,302 INFO      /controller/bin/ftriage route -ii LEAF:103,104 -sip 172.16.2.1
-dip 192.168.3.1
2019-10-02 23:12:00,887 INFO      ftriage:      main:1165 Invoking ftriage with default password
and default username: apic#fallback\admin
2019-10-02 23:12:44,565 INFO      ftriage:      main:839 L3 packet Seen on bdsol-aci32-leaf3
Ingress: Eth1/12 (Po1) Egress: Eth1/12 (Po1) Vnid: 11365
2019-10-02 23:12:44,782 INFO      ftriage:      main:242 ingress encap string vlan-2551
2019-10-02 23:12:47,260 INFO      ftriage:      main:271 Building ingress BD(s), Ctx
2019-10-02 23:12:50,041 INFO      ftriage:      main:294 Ingress BD(s) Prod:VRF1:l3out-BGP:vlan-
2551
2019-10-02 23:12:50,042 INFO      ftriage:      main:301 Ingress Ctx: Prod:VRF1
2019-10-02 23:12:50,151 INFO      ftriage:      pktrec:490 bdsol-aci32-leaf3: Collecting transient
losses snapshot for LC module: 1
2019-10-02 23:13:08,595 INFO      ftriage:      nxos:1404 bdsol-aci32-leaf3: nxos matching rule
id:4336 scope:34 filter:5
2019-10-02 23:13:09,608 INFO      ftriage:      main:522 Computed egress encap string vlan-2502
2019-10-02 23:13:09,609 INFO      ftriage:      main:313 Building egress BD(s), Ctx
2019-10-02 23:13:11,449 INFO      ftriage:      main:331 Egress Ctx Prod:VRF1
2019-10-02 23:13:11,449 INFO      ftriage:      main:332 Egress BD(s): Prod:BD2
2019-10-02 23:13:18,383 INFO      ftriage:      main:933 SIP 172.16.2.1 DIP 192.168.3.1
2019-10-02 23:13:18,384 INFO      ftriage:      unicast:973 bdsol-aci32-leaf3: <- is ingress node
2019-10-02 23:13:21,078 INFO      ftriage:      unicast:1202 bdsol-aci32-leaf3: Dst EP is local
2019-10-02 23:13:23,926 INFO      ftriage:      misc:657 bdsol-aci32-leaf3: EP if(Po1) same as
egr if(Po1)
2019-10-02 23:13:25,216 INFO      ftriage:      misc:657 bdsol-aci32-leaf3:
DMAC(00:22:BD:F8:19:FF) same as RMAC(00:22:BD:F8:19:FF)
2019-10-02 23:13:25,217 INFO      ftriage:      misc:659 bdsol-aci32-leaf3: L3 packet getting
routed/bounced in SUG
2019-10-02 23:13:25,465 INFO      ftriage:      misc:657 bdsol-aci32-leaf3: Dst IP is present in
SUG L3 tbl
2019-10-02 23:13:25,757 INFO      ftriage:      misc:657 bdsol-aci32-leaf3: RW seg_id:11365 in
SUG same as EP segid:11365
2019-10-02 23:13:32,235 INFO      ftriage:      main:961 Packet is Exiting fabric with peer-
device: bdsol-aci32-n3k-3 and peer-port: Ethernet1/16
```

Esse fluxo é permitido (como esperado) pela regra de zoneamento 4336.

## Validação do caminho de dados usando Triagem — fluxo não permitido pela política

Execute a triagem com um fluxo ICMP de 172.16.2.1 (L3OUT-EPG2) para 192.168.1.1 (EPG1 — pcTag 32770):

```
admin@apic1:~> ftriage route -ii LEAF:103,104 -sip 172.16.2.1 -dip 192.168.1.1
fTriage Status: {"dbgFtriage": {"attributes": {"operState": "InProgress", "pid": "31500",
"apicId": "1", "id": "0"}}}
Starting ftriage
Log file name for the current run is: ftlog_2019-10-02-23-53-03-478.txt
2019-10-02 23:53:03,482 INFO      /controller/bin/ftriage route -ii LEAF:103,104 -sip 172.16.2.1
-dip 192.168.1.1
2019-10-02 23:53:50,014 INFO      ftriage:      main:1165 Invoking ftriage with default password
```

```

and default username: apic#fallback\admin
2019-10-02 23:54:39,199 INFO      ftriage:      main:839  L3 packet Seen on bdsol-aci32-leaf3
Ingress: Eth1/12 (Po1) Egress: Eth1/12 (Po1) Vnid: 11364
2019-10-02 23:54:39,417 INFO      ftriage:      main:242  ingress encap string vlan-2551
2019-10-02 23:54:41,962 INFO      ftriage:      main:271  Building ingress BD(s), Ctx
2019-10-02 23:54:44,765 INFO      ftriage:      main:294  Ingress BD(s) Prod:VRF1:l3out-BGP:vlan-
2551
2019-10-02 23:54:44,766 INFO      ftriage:      main:301  Ingress Ctx: Prod:VRF1
2019-10-02 23:54:44,875 INFO      ftriage:      pktrec:490 bdsol-aci32-leaf3: Collecting transient
losses snapshot for LC module: 1
2019-10-02 23:55:02,905 INFO      ftriage:      nxos:1404 bdsol-aci32-leaf3: nxos matching rule
id:4341 scope:34 filter:5
2019-10-02 23:55:04,525 INFO      ftriage:      main:522  Computed egress encap string vlan-2501
2019-10-02 23:55:04,526 INFO      ftriage:      main:313  Building egress BD(s), Ctx
2019-10-02 23:55:06,390 INFO      ftriage:      main:331  Egress Ctx Prod:VRF1
2019-10-02 23:55:06,390 INFO      ftriage:      main:332  Egress BD(s): Prod:BD1
2019-10-02 23:55:13,571 INFO      ftriage:      main:933  SIP 172.16.2.1 DIP 192.168.1.1
2019-10-02 23:55:13,572 INFO      ftriage:      unicast:973 bdsol-aci32-leaf3: <- is ingress node
2019-10-02 23:55:16,159 INFO      ftriage:      unicast:1202 bdsol-aci32-leaf3: Dst EP is local
2019-10-02 23:55:18,949 INFO      ftriage:      misc:657  bdsol-aci32-leaf3: EP if(Po1) same as
egr if(Po1)
2019-10-02 23:55:20,126 INFO      ftriage:      misc:657  bdsol-aci32-leaf3:
DMAC(00:22:BD:F8:19:FF) same as RMAC(00:22:BD:F8:19:FF)
2019-10-02 23:55:20,126 INFO      ftriage:      misc:659  bdsol-aci32-leaf3: L3 packet getting
routed/bounced in SUG
2019-10-02 23:55:20,395 INFO      ftriage:      misc:657  bdsol-aci32-leaf3: Dst IP is present in
SUG L3 tbl
2019-10-02 23:55:20,687 INFO      ftriage:      misc:657  bdsol-aci32-leaf3: RW seg_id:11364 in
SUG same as EP segid:11364
2019-10-02 23:55:26,982 INFO      ftriage:      main:961  Packet is Exiting fabric with peer-
device: bdsol-aci32-n3k-3 and peer-port: Ethernet1/16

```

Esse fluxo é permitido (inesperado) pela regra de zoneamento 4341. As regras de zoneamento devem agora ser analisadas para compreender porquê.

## Validação do caminho de dados — regras de zoneamento

As regras de zoneamento correspondentes aos dois últimos testes são as seguintes:

- Esperado — fluxo atinge a linha 4336 da regra de zoneamento (contrato ICMP2).
- Inesperado — fluxo atinge a linha 4341 da regra de zoneamento (contrato ICMP1).

```

+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+
| Rule ID | SrcEPG | DstEPG | FilterID | Dir | operSt | Scope | Name | Action |
Priority |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+
| 4326 | 0 | 0 | implicit | uni-dir | enabled | 2097154 | | deny,log |
any_any_any(21) |
| 4335 | 0 | 16387 | implicit | uni-dir | enabled | 2097154 | | permit |
any_dest_any(16) |
| 4334 | 0 | 0 | implarp | uni-dir | enabled | 2097154 | | permit |
any_any_filter(17) |
| 4333 | 0 | 15 | implicit | uni-dir | enabled | 2097154 | | deny,log |
any_vrf_any_deny(22) |
| 4332 | 0 | 16386 | implicit | uni-dir | enabled | 2097154 | | permit |
any_dest_any(16) |
| 4339 | 32770 | 15 | 5 | uni-dir | enabled | 2097154 | ICMP2 | permit |

```

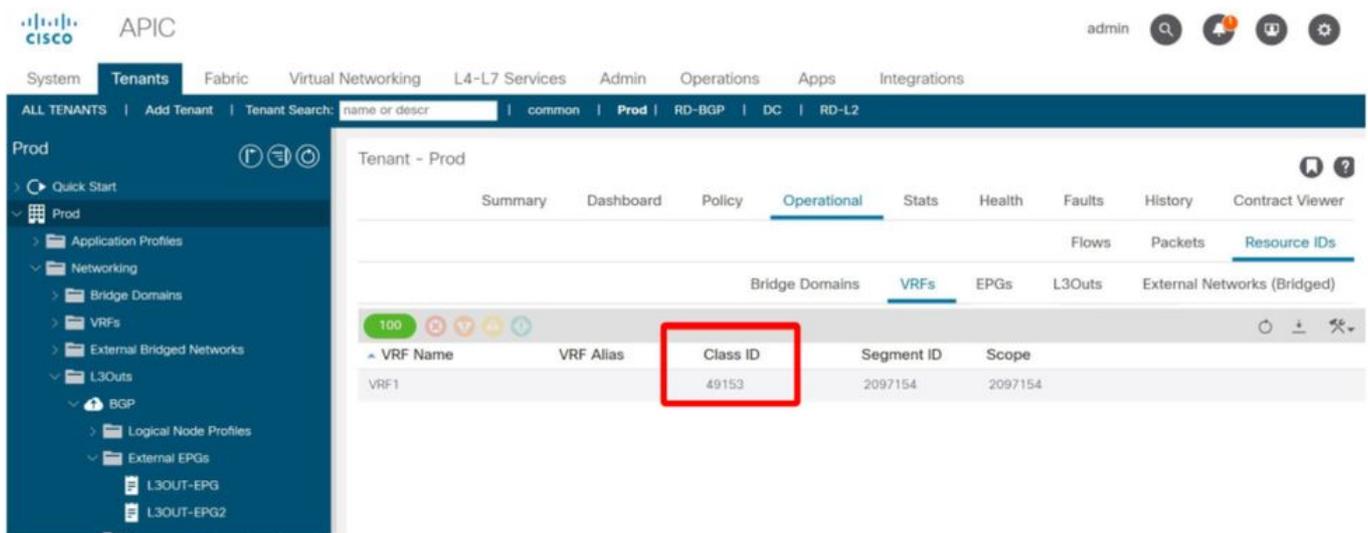
```

fully_qual(7) |
| 4341 | 49153 | 32770 | 5 | uni-dir | enabled | 2097154 | ICMP2 | permit |
fully_qual(7) |
| 4337 | 32771 | 15 | 5 | uni-dir | enabled | 2097154 | ICMP1 | permit |
fully_qual(7) |
| 4336 | 49153 | 32771 | 5 | uni-dir | enabled | 2097154 | ICMP1 | permit |
fully_qual(7) |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
-----+

```

Ambos os fluxos derivam o src pcTag de 49153. Este é o pcTag do VRF. Isso pode ser verificado na interface do usuário:

## Verificação do pcTag do VRF



O seguinte acontece quando o prefixo 0.0.0.0/0 está em uso com uma L3Out:

- O tráfego de um EPG interno para um EPG de L3Out com 0.0.0.0/0 derivará um pcTag de destino de 15.
- O tráfego de um EPG L3Out com 0.0.0.0/0 para um EPG interno da ACI derivará um pcTag de origem do VRF (49153).

O script `contract_parser` fornece uma visão holística das regras de zoneamento:

```

bdsol-aci32-leaf3# contract_parser.py --vrf Prod:VRF1
Key:
[prio:RuleId] [vrf:{str}] action protocol src-epg [src-l4] dst-epg [dst-l4]
[flags][contract:{str}] [hit=count]
[7:4339] [vrf:Prod:VRF1] permit ip icmp tn-Prod/ap-App/epg-EPG1(32770) pfx-0.0.0.0/0(15)
[contract:uni/tn-Prod/brc-ICMP2] [hit=0]
[7:4337] [vrf:Prod:VRF1] permit ip icmp tn-Prod/ap-App/epg-EPG2(32771) pfx-0.0.0.0/0(15)
[contract:uni/tn-Prod/brc-ICMP] [hit=0]
[7:4341] [vrf:Prod:VRF1] permit ip icmp tn-Prod/vrf-VRF1(49153) tn-Prod/ap-App/epg-EPG1(32770)
[contract:uni/tn-Prod/brc-ICMP2] [hit=270]
[7:4336] [vrf:Prod:VRF1] permit ip icmp tn-Prod/vrf-VRF1(49153) tn-Prod/ap-App/epg-EPG2(32771)
[contract:uni/tn-Prod/brc-ICMP] [hit=0]

```

## Confirmando o pcTag usado pelo pacote usando o aplicativo ELAM Assistant

O ELAM Assistant App oferece outro método para confirmar o pcTag de origem e destino dos

fluxos de tráfego ao vivo.

A captura de tela abaixo mostra o resultado do ELAM para o tráfego de 32771 pcTag para 49153 pcTag.

## Saída do aplicativo ELAM Assistant para src 32771 para dst 49153

Packet Forwarding Information	
<b>Forward Result</b>	
Destination Type	To a local port
Destination Logical Port	Po1
Destination Physical Port	eth1/12
Sent to SUP/CPU instead	no
SUP Redirect Reason (SUP code)	NONE
<b>Contract</b>	
Destination EPG pcTag (dclass)	32771 (Prod:App:EPG2)
Source EPG pcTag (sclass)	49153 (Prod:VRF1:13out-BGP:vlan-2551)

## Conclusão

O uso de 0.0.0.0/0 deve ser acompanhado cuidadosamente dentro de um VRF, pois cada L3Out usando essa sub-rede herdarão os contratos aplicados a todos os outros L3Out usando-a. Isso provavelmente levará a fluxos de licença não planejados.

# L3Out Compartilhado

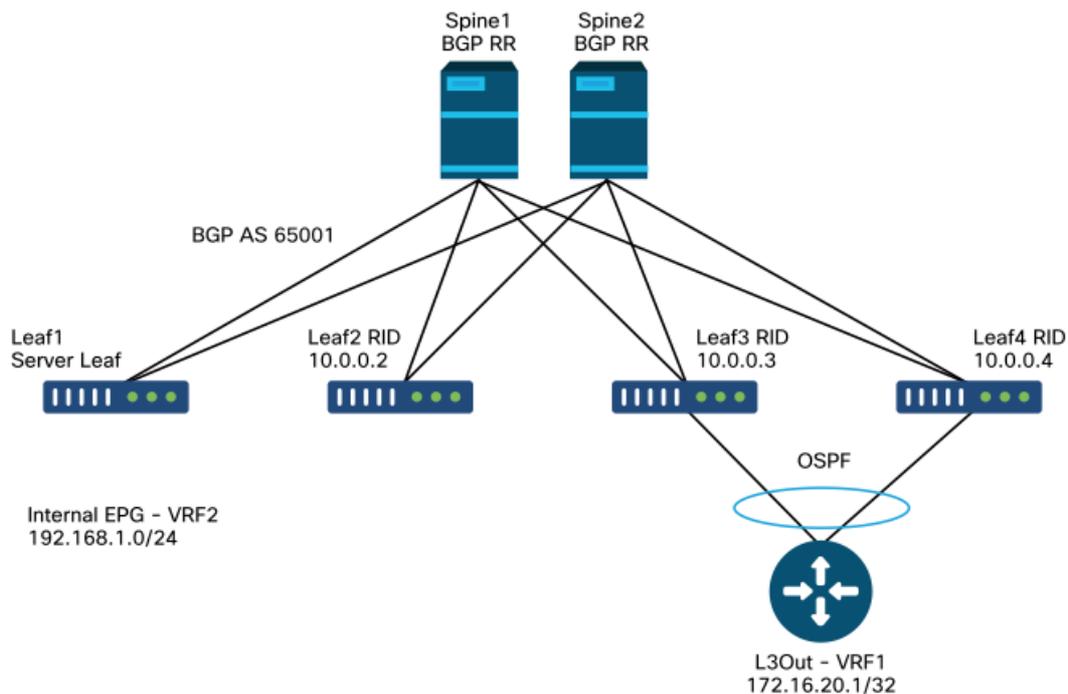
## Overview

Esta seção discutirá como solucionar problemas de anúncio de rota em configurações L3Out compartilhadas. O termo 'L3Out Compartilhado' se refere ao cenário em que um L3Out está em um VRF, mas um EPG interno com um contrato com o L3Out está em outro VRF. Com L3Outs compartilhados, o vazamento de rota está sendo feito internamente na estrutura da ACI.

Esta seção não entrará em detalhes detalhados sobre a solução de problemas de política de segurança. Para isso, consulte o capítulo "Políticas de segurança" deste manual. Esta seção também não falará em detalhes sobre a classificação de Prefixo de Política Externa para fins de segurança. Consulte a seção "Contrato e L3Out" no capítulo "encaminhamento externo".

Esta seção usa a seguinte topologia para nossos exemplos.

## Topologia L3Out compartilhada



Em um alto nível, as seguintes configurações devem estar em vigor para que uma L3Out Compartilhada funcione:

- Uma sub-rede L3Out deve ser configurada com o escopo 'Sub-rede de Controle de Rota Compartilhada' para vaziar rotas externas para VRFs internos. A opção 'Agregar compartilhado' também pode ser selecionada para vaziar todas as rotas que são mais específicas do que a sub-rede configurada.
- Uma sub-rede L3Out deve ser configurada com o escopo 'Sub-rede de Importação de Segurança Compartilhada' para programar as políticas de segurança necessárias para permitir a comunicação através dessa L3Out.
- A sub-rede BD interna deve ser definida como 'Compartilhada entre VRFs' e 'Anunciar Externamente' para programar a sub-rede BD no VRF externo e anunciá-la.
- Um contrato de escopo 'locatário' ou 'global' deve ser configurado entre o EPG interno e o EPG externo do L3Out compartilhado.

A próxima seção entrará em detalhes sobre como as rotas vazadas são anunciadas e aprendidas na ACI.

## Fluxo de trabalho L3Out compartilhado — aprendizado de rotas externas

Esta seção vai delinear o caminho de uma rota externa aprendida conforme ela é anunciada na estrutura.

### Rota externa como vista na folha de borda

Este comando mostrará a rota externa aprendida do OSPF:

```
leaf103# show ip route 172.16.20.1/32 vrf Prod:Vrf1
IP Route Table for VRF "Prod:Vrf1"
'*' denotes best ucast next-hop
'***' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%' in via output denotes VRF

172.16.20.1/32, ubest/mbest: 1/0
    *via 10.10.34.3, vlan347, [110/20], 03:59:59, ospf-default, type-2
```

Em seguida, a rota deve ser importada para o BGP. Por padrão, todas as rotas externas devem ser importadas para o BGP.

## Verificações de BGP na folha de borda

A rota deve estar na família de endereços BGP VPNv4 com um destino de rota a ser distribuído em toda a estrutura. O destino de rota é uma comunidade estendida de BGP exportada pelo VRF externo e importada por qualquer VRF interno que precise receber o caminho.

Em seguida, verifique o destino de rota que está sendo exportado pelo VRF externo no BL.

```
leaf103# show bgp process vrf Prod:Vrf1
```

Information regarding configured VRFs:

```
BGP Information for VRF Prod:Vrf1
VRF Type                : System
VRF Id                  : 85
VRF state                : UP
VRF configured          : yes
VRF refcount            : 1
VRF VNID                : 2392068
Router-ID               : 10.0.0.3
Configured Router-ID   : 10.0.0.3
Confed-ID               : 0
Cluster-ID              : 0.0.0.0
MSITE Cluster-ID       : 0.0.0.0
No. of configured peers : 1
No. of pending config peers : 0
No. of established peers : 0
VRF RD                  : 101:2392068
VRF EVPN RD             : 101:2392068
```

...

```
Wait for IGP convergence is not configured
Export RT list:
    65001:2392068
Import RT list:
    65001:2392068
Label mode: per-prefix
```

A saída acima mostra que qualquer caminho anunciado do VRF externo para o VPNv4 deve receber um destino de rota de 65001:2392068.

Em seguida, verifique o caminho bgp:

```

leaf103# show bgp ipv4 unicast 172.16.20.1/32 vrf Prod:Vrf1
BGP routing table information for VRF Prod:Vrf1, address family IPv4 Unicast
BGP routing table entry for 172.16.20.1/32, version 30 dest ptr 0xa6f25ad0
Paths: (2 available, best #1)
Flags: (0x80c0002 00000000) on xmit-list, is not in urib, exported
      vpn: version 17206, (0x100002) on xmit-list
Multipath: eBGP iBGP

Advertised path-id 1, VPN AF advertised path-id 1
Path type: redist 0x408 0x1 ref 0 adv path ref 2, path is valid, is best path
AS-Path: NONE, path locally originated
  0.0.0.0 (metric 0) from 0.0.0.0 (10.0.0.3)
    Origin incomplete, MED 20, localpref 100, weight 32768
    Extcommunity:
      RT:65001:2392068
      VNID:2392068
      COST:pre-bestpath:162:110

VRF advertise information:
Path-id 1 not advertised to any peer

VPN AF advertise information:
Path-id 1 advertised to peers:
  10.0.64.64          10.0.72.66
Path-id 2 not advertised to any peer

```

A saída acima mostra que o caminho tem o destino de rota correto. O caminho VPNv4 também pode ser verificado usando o comando 'show bgp vpnv4 unicast 172.16.20.1 vrf overlay-1'.

## Verificações no servidor leaf

Para que o leaf EPG interno instale a rota anunciada pelo BL, ele deve importar o destino da rota (mencionado acima) para o VRF interno. O processo BGP do VRF interno pode ser verificado para validar isso:

```

leaf101# show bgp process vrf Prod:Vrf2

Information regarding configured VRFs:

BGP Information for VRF Prod:Vrf2
VRF Type           : System
VRF Id             : 54
VRF state          : UP
VRF configured     : yes
VRF refcount       : 0
VRF VNID           : 2916352
Router-ID          : 192.168.1.1
Configured Router-ID : 0.0.0.0
Confed-ID          : 0
Cluster-ID         : 0.0.0.0
MSITE Cluster-ID   : 0.0.0.0
No. of configured peers : 0
No. of pending config peers : 0
No. of established peers : 0
VRF RD             : 102:2916352
VRF EVPN RD        : 102:2916352
...
Wait for IGP convergence is not configured

```

```
Import route-map 2916352-shared-svc-leak
Export RT list:
    65001:2916352
Import RT list:
    65001:2392068
    65001:2916352
```

A saída acima mostra o VRF interno importando o destino da rota que é exportado pelo VRF externo. Além disso, há um "Mapa de rota de importação" que é referenciado. O mapa de rota de importação inclui os prefixos específicos definidos na L3Out compartilhada com o sinalizador 'Sub-rede de Controle de Rota Compartilhada'.

O conteúdo do mapa de rotas pode ser verificado para garantir que ele inclui o prefixo externo:

```
leaf101# show route-map 2916352-shared-svc-leak
route-map 2916352-shared-svc-leak, deny, sequence 1
Match clauses:
    pervasive: 2
Set clauses:
route-map 2916352-shared-svc-leak, permit, sequence 2
Match clauses:
    extcommunity (extcommunity-list filter): 2916352-shared-svc-leak
Set clauses:
route-map 2916352-shared-svc-leak, permit, sequence 1000
Match clauses:
    ip address prefix-lists: IPv4-2392068-16387-5511-2916352-shared-svc-leak
    ipv6 address prefix-lists: IPv6-deny-all
Set clauses:
a-leaf101# show ip prefix-list IPv4-2392068-16387-5511-2916352-shared-svc-leak
ip prefix-list IPv4-2392068-16387-5511-2916352-shared-svc-leak: 1 entries
    seq 1 permit 172.16.20.1/32
```

A saída acima mostra o mapa de rota de importação que inclui a sub-rede a ser importada.

As verificações finais incluem verificar se a rota está na tabela BGP e se está instalada na tabela de roteamento.

Tabela BGP no servidor folha:

```
leaf101# show bgp ipv4 unicast 172.16.20.1/32 vrf Prod:Vrf2
BGP routing table information for VRF Prod:Vrf2, address family IPv4 Unicast
BGP routing table entry for 172.16.20.1/32, version 3 dest ptr 0xa763add0
Paths: (2 available, best #1)
Flags: (0x08001a 00000000) on xmit-list, is in urib, is best urib route, is in HW
    vpn: version 10987, (0x100002) on xmit-list
Multipath: eBGP iBGP

Advertised path-id 1, VPN AF advertised path-id 1
Path type: internal 0xc0000018 0x40 ref 56506 adv path ref 2, path is valid, is best path
    Imported from 10.0.72.64:5:172.16.20.1/32
AS-Path: NONE, path sourced internal to AS
    10.0.72.64 (metric 3) from 10.0.64.64 (192.168.1.102)
    Origin incomplete, MED 20, localpref 100, weight 0
    Received label 0
    Received path-id 1
    Extcommunity:
        RT:65001:2392068
        VNID:2392068
```

```
COST:pre-bestpath:162:110
Originator: 10.0.72.64 Cluster list: 192.168.1.102
```

A rota é importada para a tabela interna de BGP de VRF e tem o destino de rota esperado.

As rotas instaladas podem ser verificadas:

```
leaf101# vsh -c "show ip route 172.16.20.1/32 detail vrf Prod:Vrf2"
IP Route Table for VRF "Prod:Vrf2"
 '*' denotes best ucast next-hop
 *** denotes best mcast next-hop
 '[x/y]' denotes [preference/metric]
 '%' in via output denotes VRF
172.16.20.1/32, ubest/mbest: 2/0
  *via 10.0.72.64%overlay-1, [200/20], 01:00:51, bgp-65001, internal, tag 65001 (mpls-vpn)
    MPLS[0]: Label=0 E=0 TTL=0 S=0 (VPN)
    client-specific data: 548
    recursive next hop: 10.0.72.64/32%overlay-1
    extended route information: BGP origin AS 65001 BGP peer AS 65001 rw-vnid: 0x248004
table-id: 0x36 rw-mac: 0
  *via 10.0.72.67%overlay-1, [200/20], 01:00:51, bgp-65001, internal, tag 65001 (mpls-vpn)
    MPLS[0]: Label=0 E=0 TTL=0 S=0 (VPN)
    client-specific data: 54a
    recursive next hop: 10.0.72.67/32%overlay-1
    extended route information: BGP origin AS 65001 BGP peer AS 65001 rw-vnid: 0x248004
table-id: 0x36 rw-mac: 0
```

A saída acima usa um comando 'vsh -c' específico para obter a saída 'detail'. O sinalizador 'detail' inclui a regravação de VXLAN VNID. Este é o VNID VXLAN do VRF externo. Quando o BL recebe tráfego de dataplane com esse VNID, ele sabe que deve tomar a decisão de encaminhamento no VRF externo.

O valor rw-vnid está em hexadecimal, portanto, converter em decimal obterá o VNID de VRF de 2392068. Procure o VRF correspondente usando 'show system internal epm vrf all | grep 2392068' na folha. Uma pesquisa global pode ser realizada em um APIC usando o comando 'moquery -c fvCtx -f 'fv.Ctx.seg=="2392068"'.

O IP do próximo salto também deve apontar para os PTEPs BL e o '%overlay-1' indica que a pesquisa de rota para o próximo salto está no VRF de sobreposição.

## Fluxo de trabalho L3Out compartilhado — anunciando rotas internas

Como nas seções anteriores, anunciar sub-redes BD internas fora de um L3Out compartilhado é tratado pelo seguinte:

- A sub-rede BD (VRF interno) é instalada no BL (VRF externo) como uma rota estática. Essa implantação de rota estática é um resultado do relacionamento de contrato entre o EPG interno e a L3Out.
- A rota estática é redistribuída no protocolo externo quando o escopo 'Anunciado Externamente' é definido na sub-rede BD.

Verificar a rota estática BD no BL

```
leaf103# vsh -c "show ip route 192.168.1.0 detail vrf Prod:Vrf1"
IP Route Table for VRF "Prod:Vrf1"
'*' denotes best ucast next-hop
'***' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%' in via output denotes VRF

192.168.1.0/24, ubest/mbest: 1/0, attached, direct, pervasive
  *via 10.0.120.34%overlay-1, [1/0], 00:55:27, static, tag 4294967292
    recursive next hop: 10.0.120.34/32%overlay-1
    vrf crossing information:  VNID:0x2c8000 ClassId:0 Flush#:0
```

Observe que na saída acima o VNID do VRF interno está definido para a regravação. O próximo salto também é definido para o endereço proxy-v4-anycast.

A rota acima é anunciada externamente através dos mesmos mapas de rota que são demonstrados na seção "Anúncio de rota".

Se uma sub-rede BD for definida como 'Anunciar Externamente', ela será redistribuída em **cada protocolo externo do L3Out** com o qual o EPG interno tem um relacionamento de contrato.

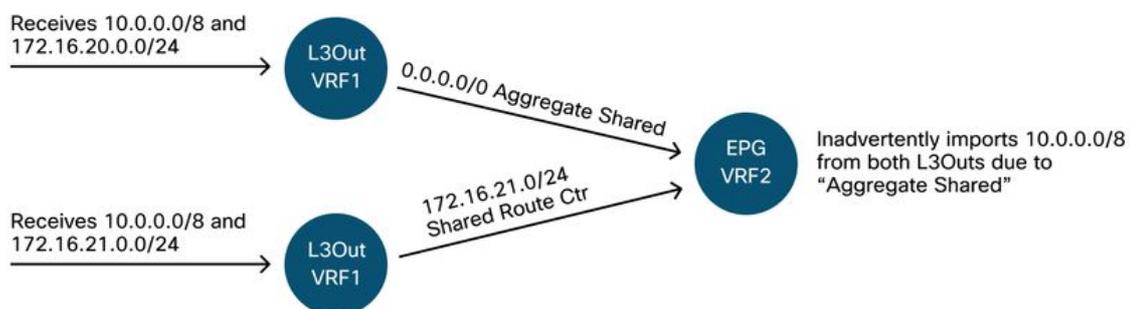
## Cenário de solução de problemas L3Out compartilhado — vazamento de rota inesperado

Esse cenário tem várias L3Outs no VRF externo e um EPG interno está recebendo uma rota de uma L3Out onde a rede **não está** definida com as opções de escopo 'compartilhado'.

### Uso de 'Agregar Compartilhado'

Considere a seguinte figura:

### Vazamento de rota inesperado



O mapa de importação do BGP com a lista de prefixos programada a partir dos flags '**Shared Route Control Subnet**' é aplicado no nível do VRF. Se uma L3Out no VRF1 tiver uma sub-rede com 'Sub-rede de Controle de Rota Compartilhada', todas as rotas recebidas em L3Outs no VRF1 que corresponderem a essa Sub-rede de Controle de Rota Compartilhada serão importadas para o VRF2.

O design acima pode resultar em fluxos de tráfego inesperados. Se não houver contratos entre o

EPG interno e o anúncio inesperado L3Out EPG, haverá quedas de tráfego.

## 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.