

# Configurar e solucionar problemas do vPC Fabric Peering de VXLAN para NXOS

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Diagrama de Rede](#)

[Configuração](#)

[Configuração de TCAM](#)

[TCAM Carving](#)

[Configuração para vPC](#)

[Domínio VPC](#)

[Keep-alive](#)

[Interface de Camada 3 para o Link Ponto Virtual](#)

[VPC Peer-Link](#)

[Enlaces ascendentes](#)

[Configuração SPINES](#)

[Tráfego de broadcast, unicast desconhecido e multicast com encapsulamento de replicação de entrada](#)

[Tráfego de broadcast, unicast desconhecido e multicast com encapsulamento de replicação de entrada](#)

[Tráfego de broadcast, unicast desconhecido e multicast com encapsulamento multicast](#)

[Tráfego de broadcast, unicast desconhecido e multicast com desencapsulamento multicast](#)

[Verificar](#)

[Informações Relacionadas](#)

---

## Introdução

Este documento descreve como configurar, verificar o emparelhamento de estrutura vPC para o fluxo de tráfego NXOS e BUM.

## Pré-requisitos

### Requisitos

A Cisco recomenda o conhecimento destes tópicos:

- vPC (canal de porta virtual)
- LAN extensível virtual (VXLAN)

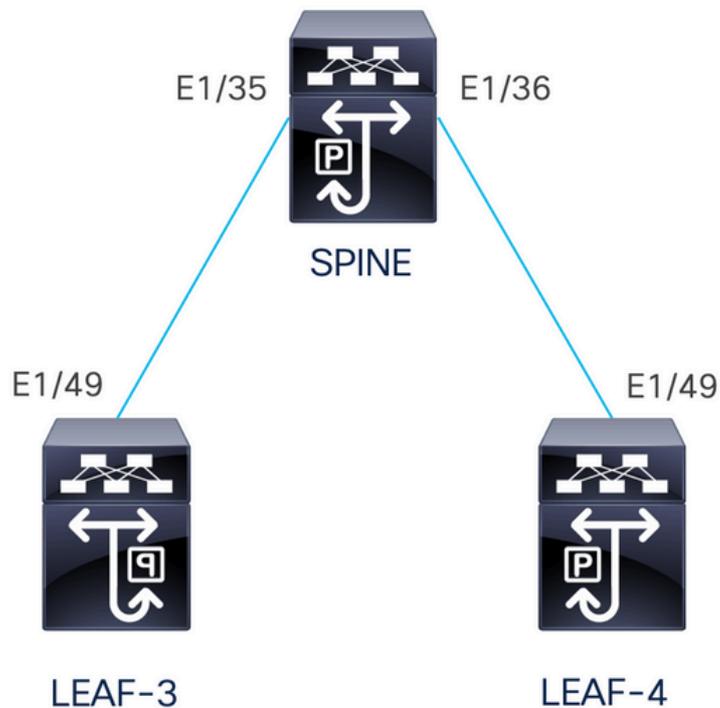
## Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- N9K-C93240YC-FX2 para switches leaf Versão: 10.3(3)
- N9K-C9336C-FX2 para switch Spine Versão: 10.3(3)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Diagrama de Rede



O vPC Fabric Peering fornece uma solução avançada de acesso dual-homing sem sobrecarga de portas físicas desperdiçadas para o vPC Peer Link. Esse recurso preserva todas as características de um vPC tradicional.

Nesta implantação, temos Leaf-3 e Leaf-4 configurados como vPC com peering de estrutura.

## Configuração

### Configuração de TCAM

Antes da configuração, há uma verificação na memória TCAM:

```

LEAF-4(config-if)# sh hardware access-list tcam region
      NAT ACL[nat] size = 0
      Ingress PACL [ing-ifac1] size = 0
      VACL [vac1] size = 0
      Ingress RAcl [ing-racl] size = 2304
      Ingress L2 QOS [ing-l2-qos] size = 256
      Ingress L3/VLAN QOS [ing-l3-vlan-qos] size = 512
      Ingress SUP [ing-sup] size = 512
      Ingress L2 SPAN filter [ing-l2-span-filter] size = 256
      Ingress L3 SPAN filter [ing-l3-span-filter] size = 256
      Ingress FSTAT [ing-fstat] size = 0
      span [span] size = 512
      Egress RAcl [egr-racl] size = 1792
      Egress SUP [egr-sup] size = 256
      Ingress Redirect [ing-redirect] size = 0
      Egress L2 QOS [egr-l2-qos] size = 0
      Egress L3/VLAN QOS [egr-l3-vlan-qos] size = 0
      Ingress Netflow/Analytics [ing-netflow] size = 512
      Ingress NBM [ing-nbm] size = 0
      TCP NAT ACL[tcp-nat] size = 0
      Egress sup control plane[egr-copp] size = 0
      Ingress Flow Redirect [ing-flow-redirect] size = 0 <<<<<<<<
      Ingress PAcl IPv4 Lite [ing-ifac1-ipv4-lite] size = 0
      Ingress PAcl IPv6 Lite [ing-ifac1-ipv6-lite] size = 0
      Ingress CNTACL [ing-cntacl] size = 0
      Egress CNTACL [egr-cntacl] size = 0
      MCAST NAT ACL[mcast-nat] size = 0
      Ingress DAcl [ing-dacl] size = 0
      Ingress PAcl Super Bridge [ing-pacl-sb] size = 0
      Ingress Storm Control [ing-storm-control] size = 0
      Ingress VACL redirect [ing-vacl-nh] size = 0
      Egress PAcl [egr-ifac1] size = 0
      Egress Netflow [egr-netflow] size = 0

```

O vPC Fabric Peering requer a aplicação da gravação TCAM de região ing-flow-redirect. A gravação TCAM exige salvar a configuração e recarregar o switch antes de usar o recurso.

Esse espaço no TCAM tem largura dupla, portanto, o mínimo que podemos atribuir é 512.

## TCAM Carving

Neste cenário, o ing-racl tem espaço suficiente para o 512 e atribuir esse 512 ao ing-flow-redirect.

```

LEAF-4(config-if)# hardware access-list tcam region ing-racl 1792
Please save config and reload the system for the configuration to take effect

```

```

LEAF-4(config)# hardware access-list tcam region ing-flow-redirect 512
Please save config and reload the system for the configuration to take effect

```

---

Observação: ao configurar o emparelhamento de estrutura do vPC por meio do DCNM, a gravação do TCAM será realizada, mas será necessário recarregar para que tenha efeito

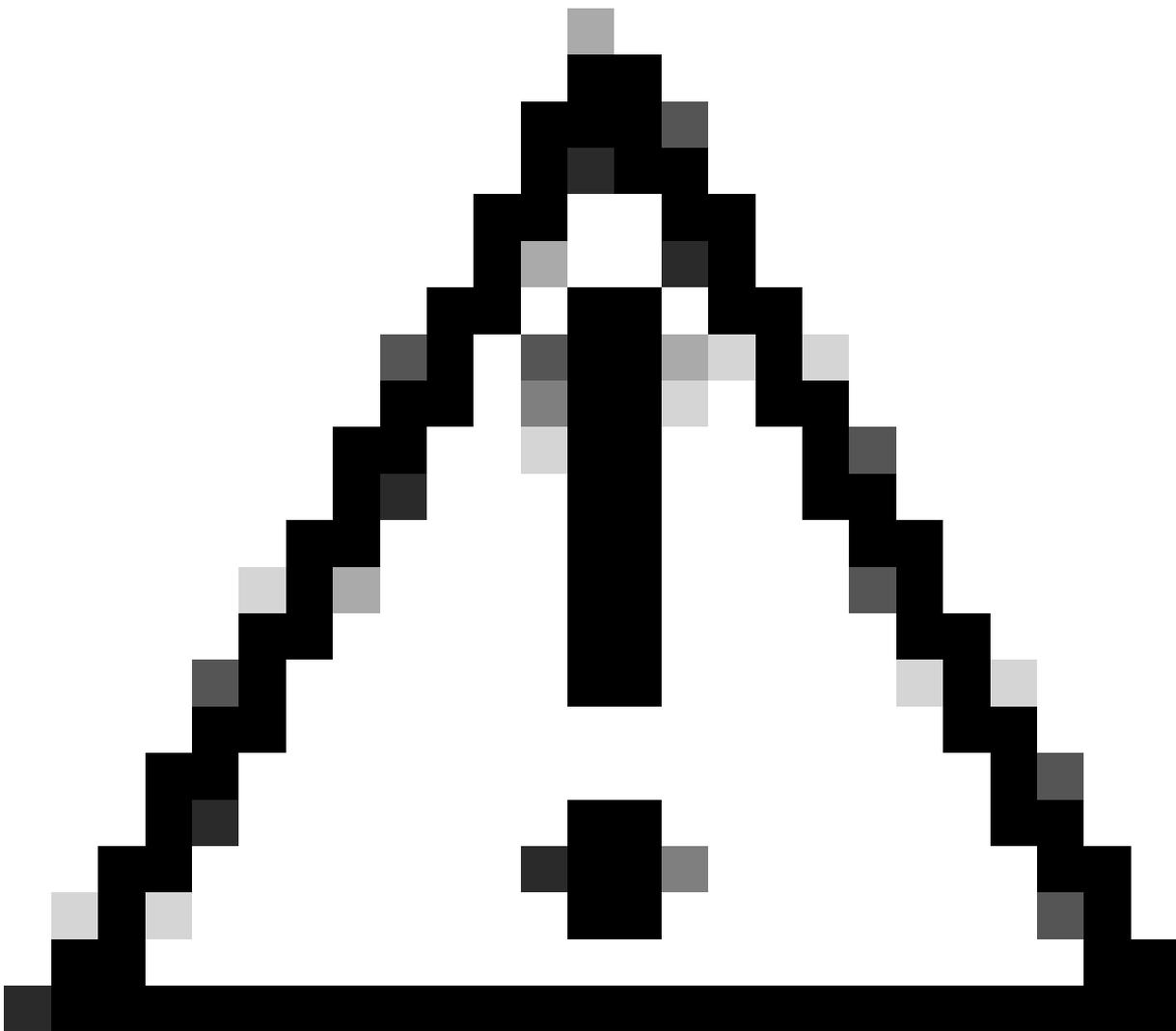
---

Uma vez feita a alteração, ela será refletida no comando:

```
513E-B-11-N9K-C93240YC-FX2-4# sh hardware access-list tcam region
    NAT ACL[nat] size = 0
    Ingress PACL [ing-ifacl] size = 0
    VACL [vacl] size = 0
    Ingress RAACL [ing-racl] size = 2304
    Ingress L2 QOS [ing-l2-qos] size = 256
    Ingress L3/VLAN QOS [ing-l3-vlan-qos] size = 512
    Ingress SUP [ing-sup] size = 512
    Ingress L2 SPAN filter [ing-l2-span-filter] size = 256
    Ingress L3 SPAN filter [ing-l3-span-filter] size = 256
    Ingress FSTAT [ing-fstat] size = 0
    span [span] size = 512
    Egress RAACL [egr-racl] size = 1792
    Egress SUP [egr-sup] size = 256
```

```
Ingress Redirect [ing-redirect] size = 0
  Egress L2 QOS [egr-l2-qos] size = 0
  Egress L3/VLAN QOS [egr-l3-vlan-qos] size = 0
  Ingress Netflow/Analytics [ing-netflow] size = 512 <<<<<
    Ingress NBM [ing-nbm] size = 0
    TCP NAT ACL[tcp-nat] size = 0
  Egress sup control plane[egr-copp] size = 0
  Ingress Flow Redirect [ing-flow-redirect] size = 0
  Ingress PACL IPv4 Lite [ing-ifacl-ipv4-lite] size = 0
  Ingress PACL IPv6 Lite [ing-ifacl-ipv6-lite] size = 0
    Ingress CNTACL [ing-cntacl] size = 0
    Egress CNTACL [egr-cntacl] size = 0
    MCAST NAT ACL[mcast-nat] size = 0
    Ingress DAACL [ing-dacl] size = 0
  Ingress PACL Super Bridge [ing-pacl-sb] size = 0
  Ingress Storm Control [ing-storm-control] size = 0
    Ingress VACL redirect [ing-vacl-nh] size = 0
    Egress PACL [egr-ifacl] size = 0
```

---



Cuidado: certifique-se de que o dispositivo seja recarregado após as alterações no TCAM, caso contrário o VPC não será ativado devido a alterações não aplicadas no

---

---

TCAM.

---

## Configuração para vPC

### Domínio VPC

No LEAF-3 e no LEAF-4 no domínio VPC, a configuração é para especificar os endereços IP para o link de peer keep-alive e virtual

```
vpc domain 1
  peer-keepalive destination 192.168.1.1 source 192.168.1.2 vrf management
  virtual peer-link destination 10.10.10.2 source 10.10.10.1 dscp 56

interface port-channel1
  vpc peer-link
```

### Keep-alive

Qualquer enlace direto de Camada 3 entre pares vPC deve ser usado somente para peer-keep alive. Ele deve estar em um VRF separado, dedicado apenas à manutenção de atividade. Neste cenário, estamos usando o gerenciamento de interface do switch.

```
LEAF-3
interface mgmt0
  vrf member management
  ip address 192.168.1.1/24
```

```
LEAF-4
interface mgmt0
  vrf member management
  ip address 192.168.1.2/24
```

### Interface de Camada 3 para o Link Ponto Virtual

A interface de Camada 3 usada para o link peer virtual não deve ser a mesma usada para o keep-alive, você pode usar o mesmo loopback usado para a subjacência ou pode ser um loopback dedicado no Nexus

Aqui, o loopback0 é para a subjacência e o loopback2 é um loopback dedicado para o link de peer virtual, enquanto o loopback1 é a interface associada à nossa interface NVE.

LEAF-3

```
interface loopback0
  ip address 10.1.1.1/32
  ip router ospf 1 area 0.0.0.0
  ip pim sparse-mode

interface loopback1
  ip address 172.16.1.2/32
  ip address 172.16.1.1/32 secondary
  ip router ospf 1 area 0.0.0.0
  ip pim sparse-mode

interface loopback2
  ip address 10.10.10.2/32
  ip router ospf 1 area 0.0.0.0
```

#### LEAF-4

```
interface loopback0
  ip address 10.1.1.2/32
  ip router ospf 1 area 0.0.0.0
  ip pim sparse-mode

interface loopback1
  ip address 172.16.1.3/32
  ip address 172.16.1.1/32 secondary
  ip router ospf 1 area 0.0.0.0
  ip pim sparse-mode

interface loopback2
  ip address 10.10.10.1/32
  ip router ospf 1 area 0.0.0.0
```

## VPC Peer-Link

O link de peer precisa ter um canal de porta atribuído, mesmo que não atribuamos uma interface física ao canal de porta.

```
LEAF-3(config-if)# sh run interface port-channel 1 membership
```

```
interface port-channel1
  switchport
  switchport mode trunk
  spanning-tree port type network
  vpc peer-link
```

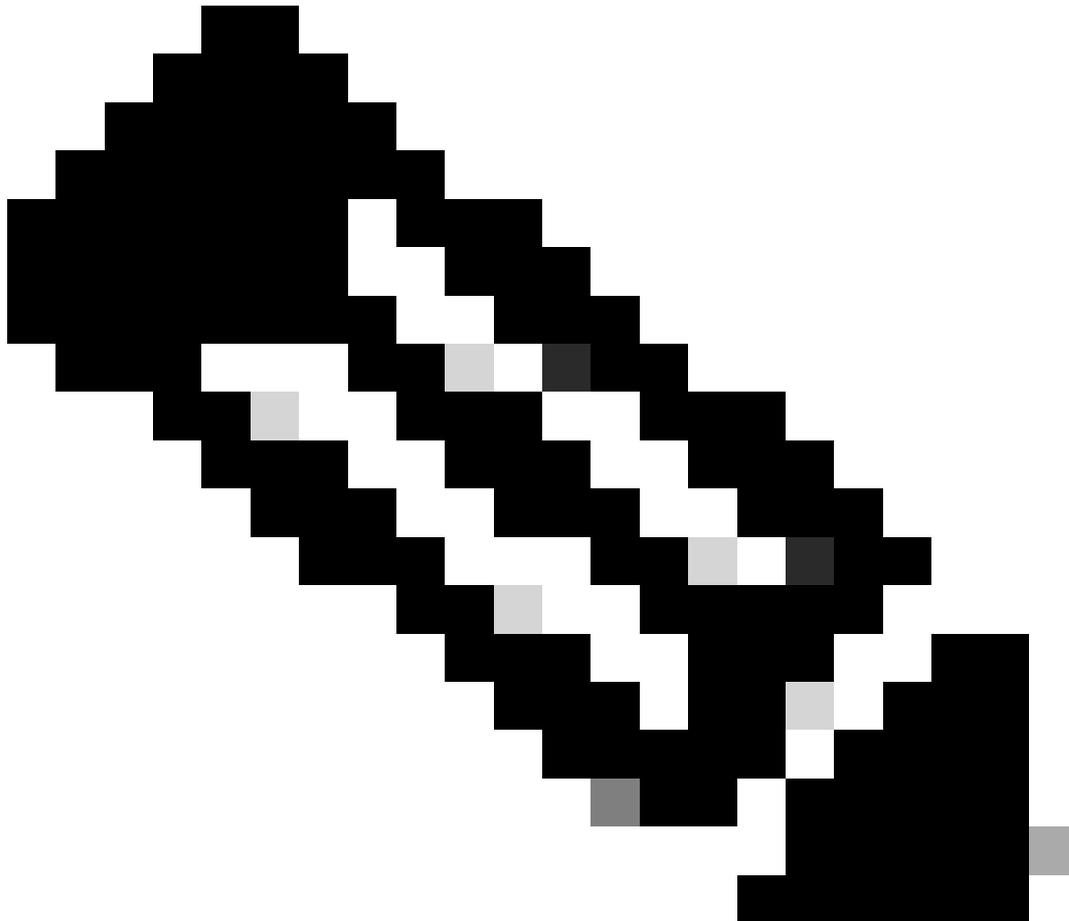
## Enlaces ascendentes

A última parte da configuração é configurar os links em ambos os leafs em direção ao SPINE com o comando port-type fabric.

```
interface Ethernet1/49
```

```
port-type fabric <<<<<<<<
medium p2p
ip unnumbered loopback0
ip router ospf 1 area 0.0.0.0
ip pim sparse-mode
no shutdown
```

---



Observação: se você não configurar a estrutura de tipo de porta, não poderá ver o keep-alive sendo gerado pelo Nexus

---

## Configuração SPINES

Nos spines, é recomendável definir QoS para corresponder ao valor de DSCP configurado no domínio VPC, já que o link par do vPC Fabric Peering é estabelecido na rede de transporte.

As mensagens CFS de informações de plano de controle usadas para sincronizar informações de estado da porta, informações de VLAN, mapeamento VLAN-para-VNI, endereços MAC do host e

grupos de rastreamento IGMP são transmitidas pela malha. As mensagens CFS são marcadas com o valor de DSCP apropriado, que deve ser protegido na rede de transporte.

```
class-map type qos match-all CFS
  match dscp 56
```

```
policy-map type qos CFS
  class CFS
    Set qos-group 7 <<< Depending on the platform it can be 4
```

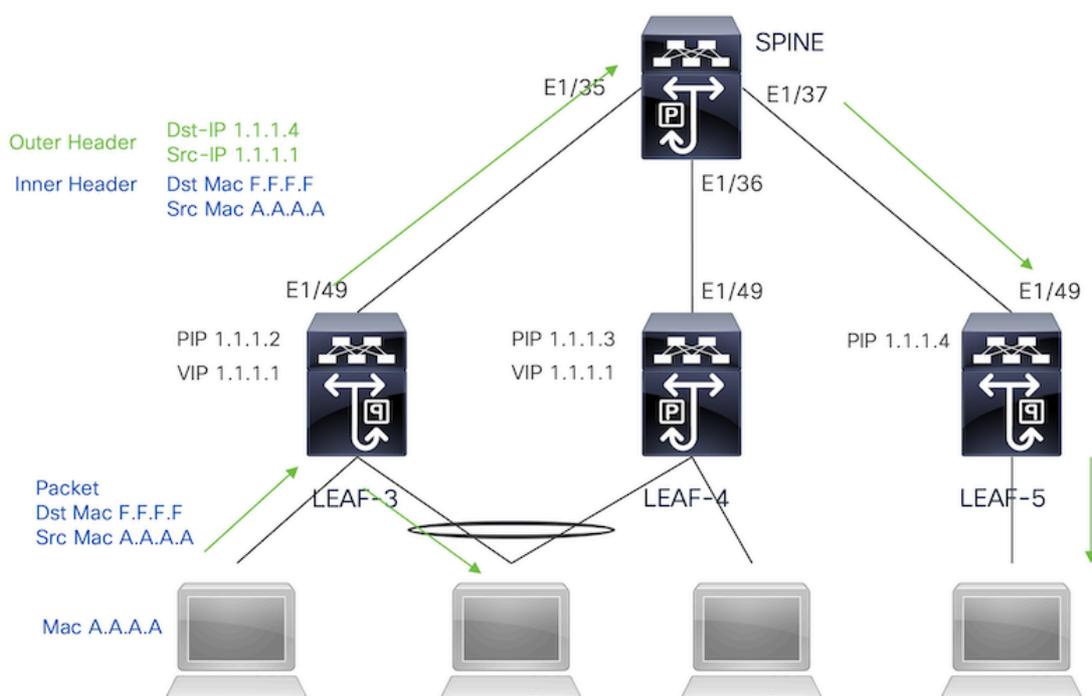
```
interface Ethernet 1/35-36
  service-policy type qos input CFS
```

## Tráfego de broadcast, unicast desconhecido e multicast com encapsulamento de replicação de entrada

Quando o nexus recebe um pacote que precisa ser transmitido, ele gera 2 cópias do pacote.

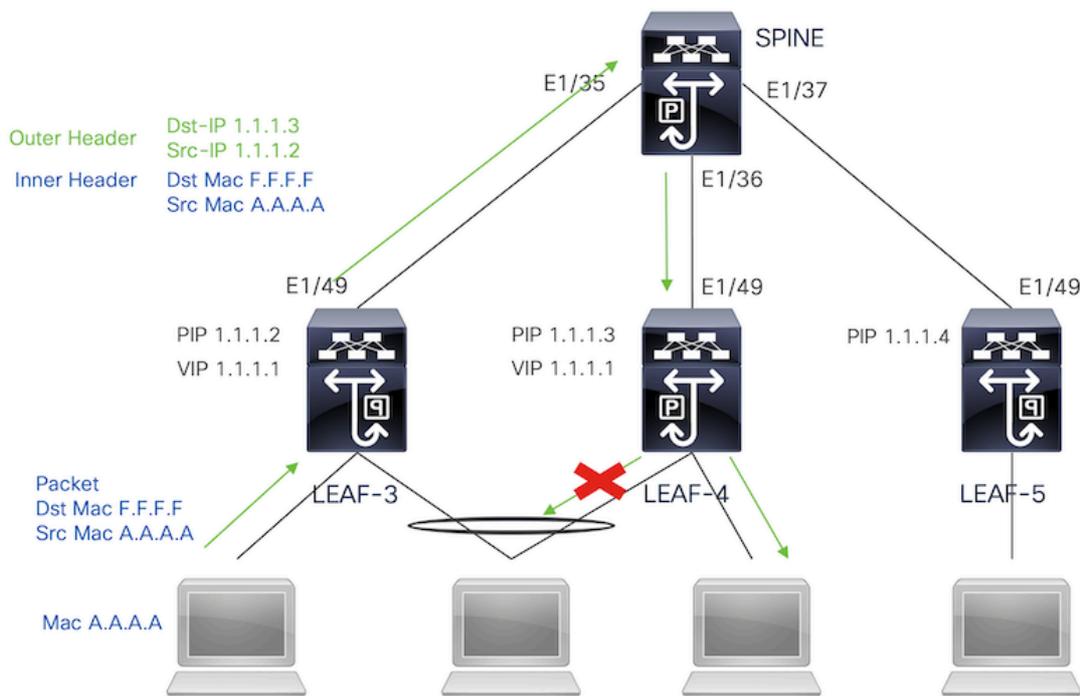
1. Para todos os VTEPS remotos na lista de inundação para o VNI, incluindo as portas de acesso local
2. Para o peer VPC remoto

Para a primeira cópia, o Nexus encapsulou o tráfego usando o IP de origem do endereço IP secundário e o IP de destino do VTEP remoto e também para as portas de acesso local.



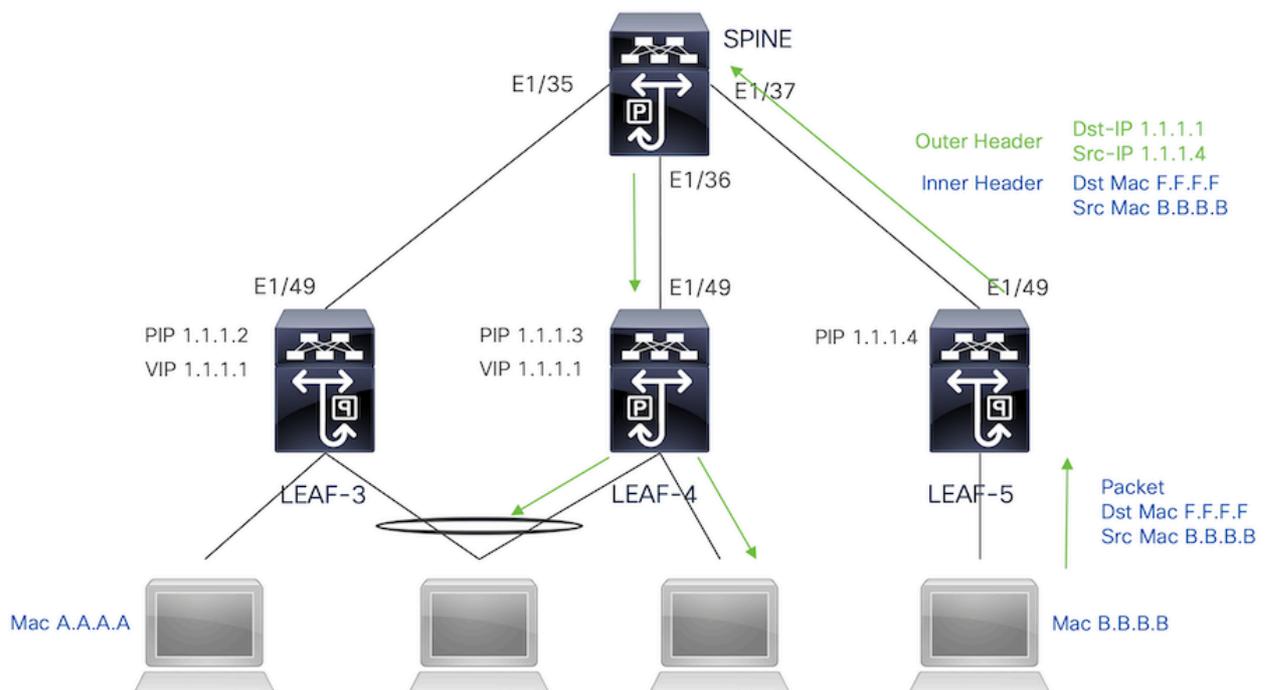
Para a segunda cópia, ela será enviada ao peer do VPC remoto, o IP de origem será o principal do loopback e o IP de destino será o PIP do peer do VPC remoto.

Uma vez recebido o pacote da coluna, o VTEP remoto encaminhará o pacote somente às portas órfãs.



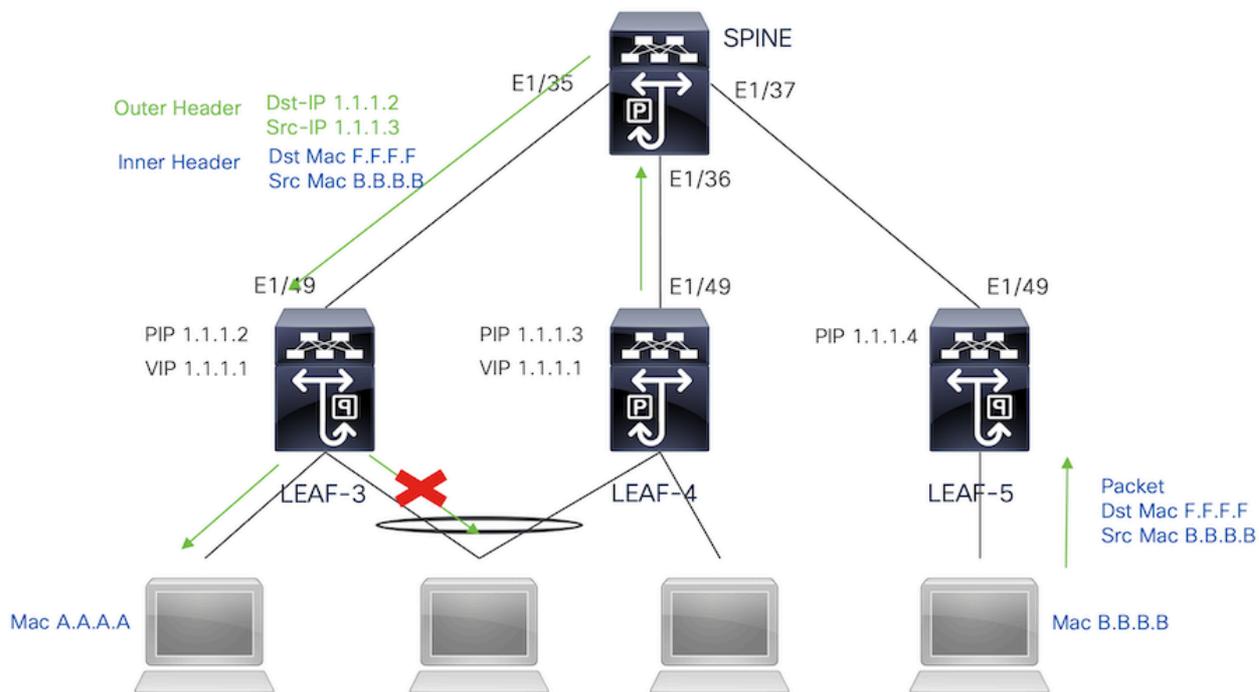
## Tráfego de broadcast, unicast desconhecido e multicast com encapsulamento de replicação de entrada

Como o IP de destino para o tráfego de BUM recebido de outro VTEP é o VIP que o tráfego mistura para um dos dispositivos VPC, ele desencapsula o pacote e o envia para as portas de acesso.



Para fazer com que o tráfego alcance as portas órfãs conectadas no peer do VPC remoto, o nexus gera uma cópia do pacote e vai enviá-lo somente ao VPC remoto usando o endereço IP primário como IP de origem/destino.

Uma vez recebido no peer vpc remoto, o nexus desencapsula o tráfego e o encaminha somente para portas órfãs.

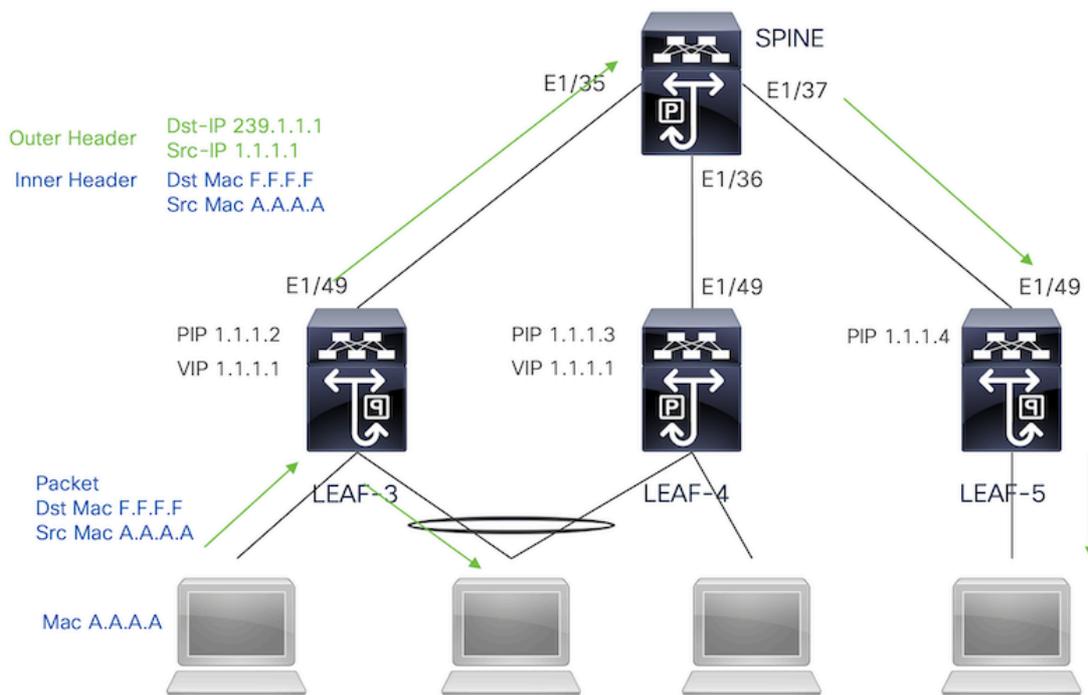


## Tráfego de broadcast, unicast desconhecido e multicast com encapsulamento multicast

Quando o nexus recebe um pacote que precisa ser transmitido, ele gera 2 cópias do pacote.

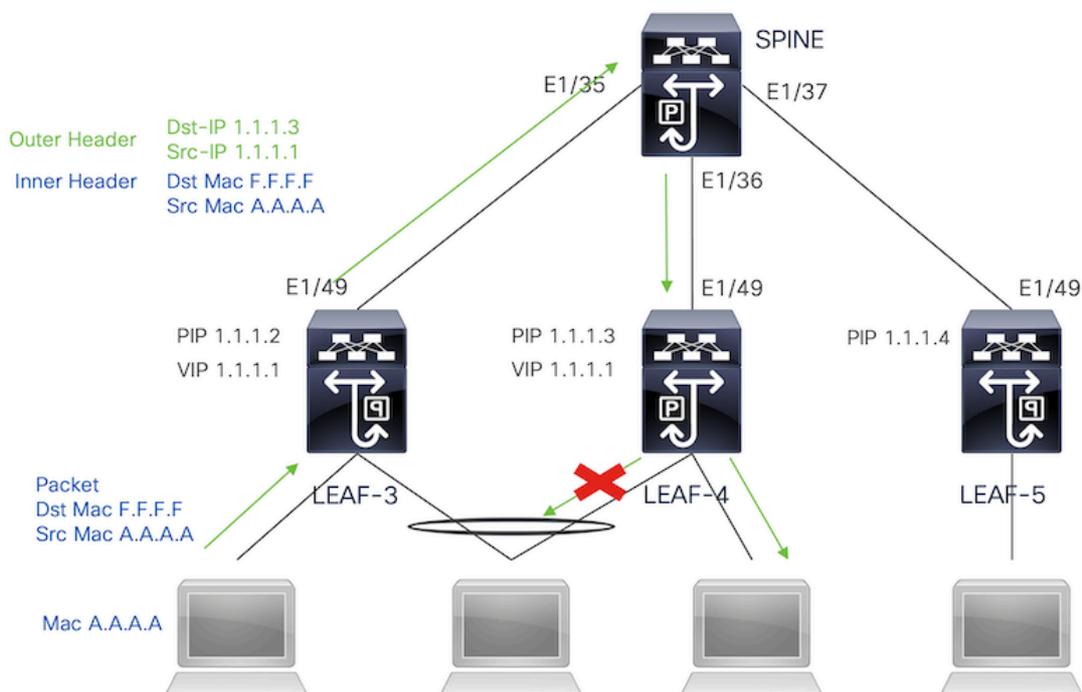
1. O pacote será enviado a todos os OIFs na entrada S,G multicast incluindo as portas de acesso local
2. Para o peer VPC remoto

Para a primeira cópia, o Nexus encapsulou o tráfego usando o IP de origem do endereço IP secundário e o IP de destino do grupo multicast configurado.



Para a segunda cópia, ela será enviada ao peer do VPC remoto, o IP de origem será o secundário do loopback e o IP de destino será o PIP do peer do VPC remoto.

Uma vez recebido o pacote da coluna, o VTEP remoto encaminha o pacote somente para as portas órfãs.



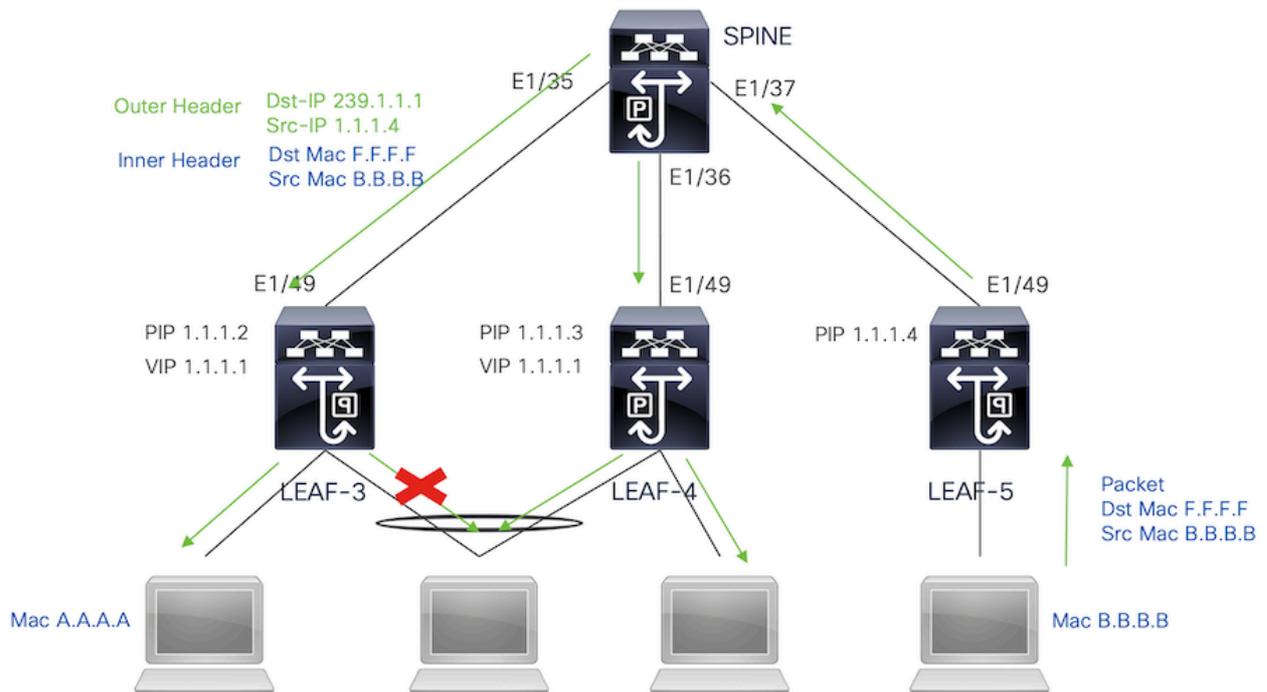
## Tráfego de broadcast, unicast desconhecido e multicast com desencapsulamento multicast

Para o processo de desencapsulamento, o pacote chegará a ambos os peers VPC. Somente um

dispositivo VPC encaminhará o tráfego através dos canais de porta VPC. Isso será decidido pelo Encaminhador exibido no comando.

```
module-1# show forwarding internal vpc-df-hash
```

VPC DF: FORWARDER



## Verificar

Para garantir que o VPC esteja ativo, execute os próximos comandos:

Verifique a acessibilidade dos endereços IP usados para o link de peer virtual.

```
LEAF-3# sh ip route 10.10.10.1
IP Route Table for VRF "default"
'*' denotes best ucast next-hop
'***' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

10.10.10.1/32, ubest/mbest: 1/0
   *via 192.168.120.1, Eth1/49, [110/3], 01:15:01, ospf-1, intra
```

```
LEAF-3# ping 10.10.10.1
PING 10.10.10.1 (10.10.10.1): 56 data bytes
64 bytes from 10.10.10.1: icmp_seq=0 ttl=253 time=0.898 ms
64 bytes from 10.10.10.1: icmp_seq=1 ttl=253 time=0.505 ms
64 bytes from 10.10.10.1: icmp_seq=2 ttl=253 time=0.433 ms
64 bytes from 10.10.10.1: icmp_seq=3 ttl=253 time=0.465 ms
```

64 bytes from 10.10.10.1: icmp\_seq=4 ttl=253 time=0.558 ms

LEAF-3(config-if)# show vpc brief

Legend:

(\*) - local vPC is down, forwarding via vPC peer-link

```
vPC domain id           : 1
Peer status             : peer adjacency formed ok <<<<
vPC keep-alive status   : peer is alive <<<<
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 consistency status : success
vPC role                : secondary
Number of vPCs configured : 0
Peer Gateway            : Disabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status    : Disabled
Delay-restore status    : Timer is off.(timeout = 30s)
Delay-restore SVI status : Timer is off.(timeout = 10s)
Delay-restore Orphan-port status : Timer is off.(timeout = 0s)
Operational Layer3 Peer-router : Disabled
Virtual-peerlink mode   : Enabled <<<<<<<<
```

vPC Peer-link status

```
-----
id  Port  Status  Active vlans
--  ---  -
1   Po1   up      1,10,50,600-604,608,610-611,614-618,638-639,
        662-663,701-704
```

Para verificar as funções do VPC, execute o comando:

LEAF-3(config-if)# sh vpc role

vPC Role status

```
-----
vPC role                : secondary <<<<
Dual Active Detection Status : 0
vPC system-mac          : 00:23:04:ee:be:01
vPC system-priority     : 32667
vPC local system-mac    : d0:e0:42:e2:09:6f
vPC local role-priority : 32667
vPC local config role-priority : 32667
vPC peer system-mac     : 2c:4f:52:3f:46:df
vPC peer role-priority  : 32667
vPC peer config role-priority : 32667
```

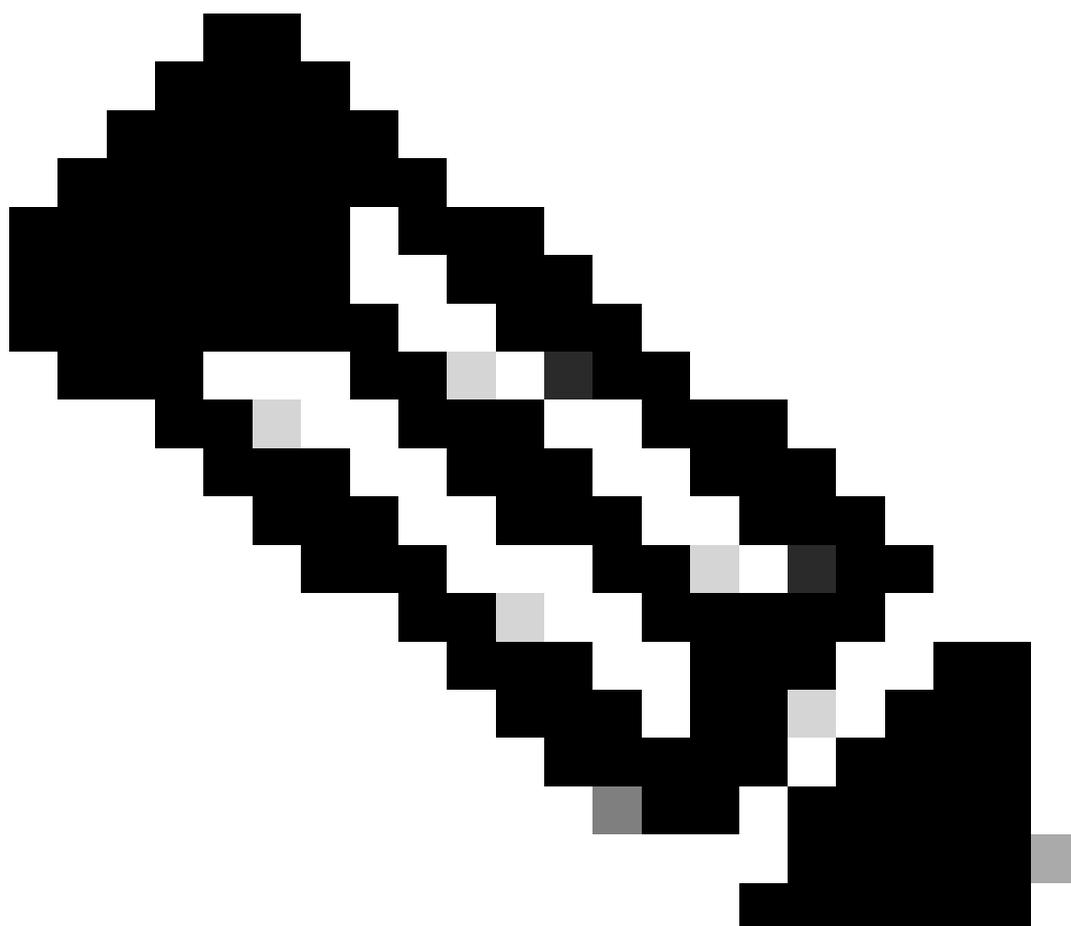
Todas as vlans permitidas no canal de porta do link par devem ser mapeadas para um VNI, caso não estejam, elas serão exibidas como inconsistentes

```
LEAF-3(config-if)# show vpc virtual-peerlink vlan consistency
Following vlans are inconsistent
1 608 610 611 614 615 616 617 618 638 639 701 702 703 704
```

Para confirmar se a configuração nos links ascendentes está programada corretamente, execute o comando:

```
LEAF-3(config-if)# show vpc fabric-ports
Number of Fabric port : 1
Number of Fabric port active : 1
```

Fabric	Ports	State
-----		
Ethernet	1/49	UP



Observação: o NVE e a interface de loopback associada a ele serão exibidos a menos

---

que o VPC esteja ativo.

---

## Informações Relacionadas

- [Suporte técnico e downloads da Cisco](#)

## 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.