Configurar host silencioso de acesso SD com recurso de transmissão direcionada por IP

Contents

Introdução

Este documento descreve o gerenciamento de hosts silenciosos no acesso SD, abordando desafios de conectividade usando inundação de L2 e broadcast direcionado por IP.

Descrição

A maioria dos endpoints e suas interfaces de rede transmitem tráfego periodicamente, especialmente mensagens relacionadas ao controle, como ARP ou DHCP. No entanto, alguns endpoints respondem apenas quando solicitados, em vez de enviar pacotes em intervalos regulares. Esses dispositivos enviam pacotes de controle somente sob demanda. Na rede, esses endpoints são comumente conhecidos como Hosts Silenciosos. Dentro do contexto de SD-

Access, os hosts silenciosos devem interromper todo o tráfego ou restringir sua comunicação retendo pacotes de plano de controle.

Na estrutura SDA, os broadcasts são suprimidos em cada nó de borda ou encaminhados para todas as bordas usando a inundação de L2, um processo normalmente limitado aos nós de borda e às bordas de L2. O encaminhamento de broadcasts para cada porta em uma VLAN imita o comportamento de uma rede tradicional de Camada 2, o que ajuda significativamente os Hosts Silenciosos a permanecerem ativos. No entanto, gerenciar hosts silenciosos em um ambiente de malha apresenta desafios, pois sua falta de comunicação regular pode interromper os mecanismos de autenticação, registros do plano de controle e encaminhamento.

Habilitar a inundação de L2 endereça apenas parte do problema. Os hosts silenciosos podem receber pacotes de broadcast somente quando outro dispositivo os gera, seja de dentro da mesma VLAN dentro da estrutura ou de uma borda de estrutura. Um broadcast direcionado por IP refere-se a um pacote IP com um endereço de destino definido para o endereço de broadcast de uma sub-rede, originado de um host fora dessa sub-rede. Este recurso requer suporte a multicast na subjacência. Quando o broadcast direcionado por IP é ativado na estrutura, todos os pacotes de broadcast de sub-rede atingem cada host dentro dessa sub-rede. Esse recurso também pode despertar dispositivos usando pacotes unicast padrão, simulando efetivamente o comportamento "unicast desconhecido" encontrado nas redes tradicionais.

Topologia

Hardware e software

- Catalyst 9000 Series Switches
- Catalyst Center Versão 2.3.7.9
- Cisco IOS® XE 17.15.03 e posterior (Borda/CP e Borda)

Topologia:

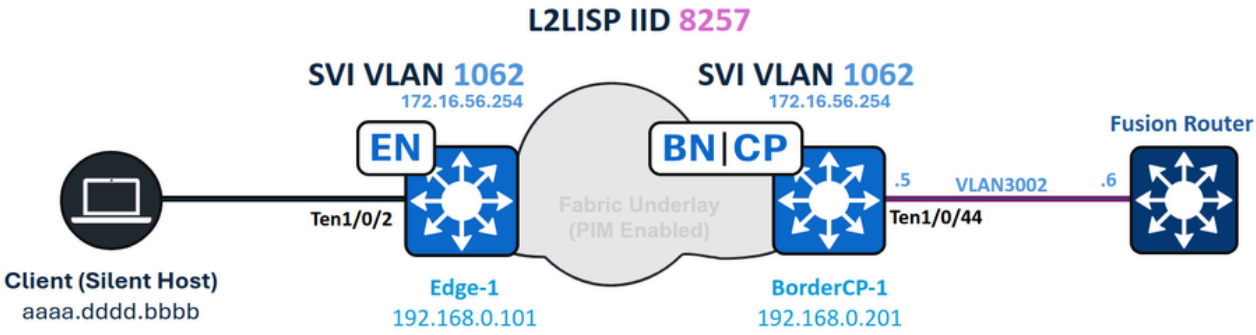


Diagrama de Rede

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Encaminhamento de Internet Protocol (IP)
- Protocolo de separação de localizador/ID (LISP)
- Multicast independente de protocolo (PIM)
- Inundação da camada 2 no acesso SD

Requisitos

- Este recurso requer o Cisco Catalyst Center 1.3 ou superior
- Cisco IOS XE 17.3 e licenças Cisco DNA Advantage*
- Para fronteiras ASR e ISR, é necessário o Cisco IOS XE 17.3.1 ou superior
- Switches das séries Catalyst 3000, 4000, 6000 ou Nexus 7000 não são suportados

---

⚠ Caution: Habilitar o recurso IP Directed Broadcast ativa automaticamente a inundação de L2. Certifique-se de que a funcionalidade de multicast na subjacência funcione corretamente antes de ativar esse recurso.

Você pode habilitar ou desabilitar a Difusão Direcionada por IP após criar o Pool de IPs, como gerenciar pools sem fio ou configurações de Inundação de L2.

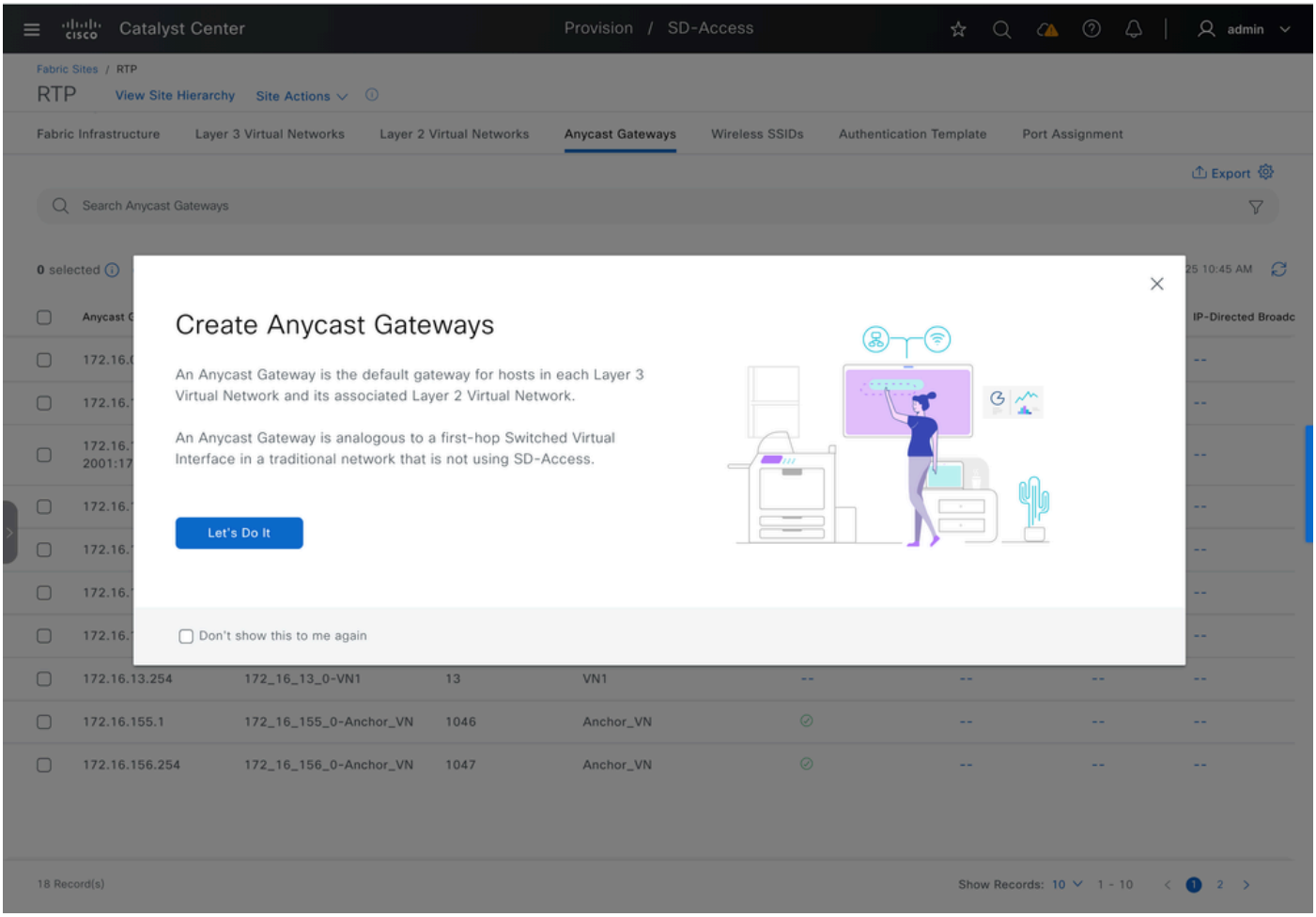
Configuração do Catalyst Center

Quando o IP Directed Broadcast está habilitado, o Catalyst Center inicia uma tarefa de provisionamento em toda a estrutura. Todos os nós de borda, bordas L2 e bordas com handoff L3 estão incluídos neste processo de provisionamento.

Para disparar o fluxo de trabalho de Difusão Direcionada por IP na interface do usuário:

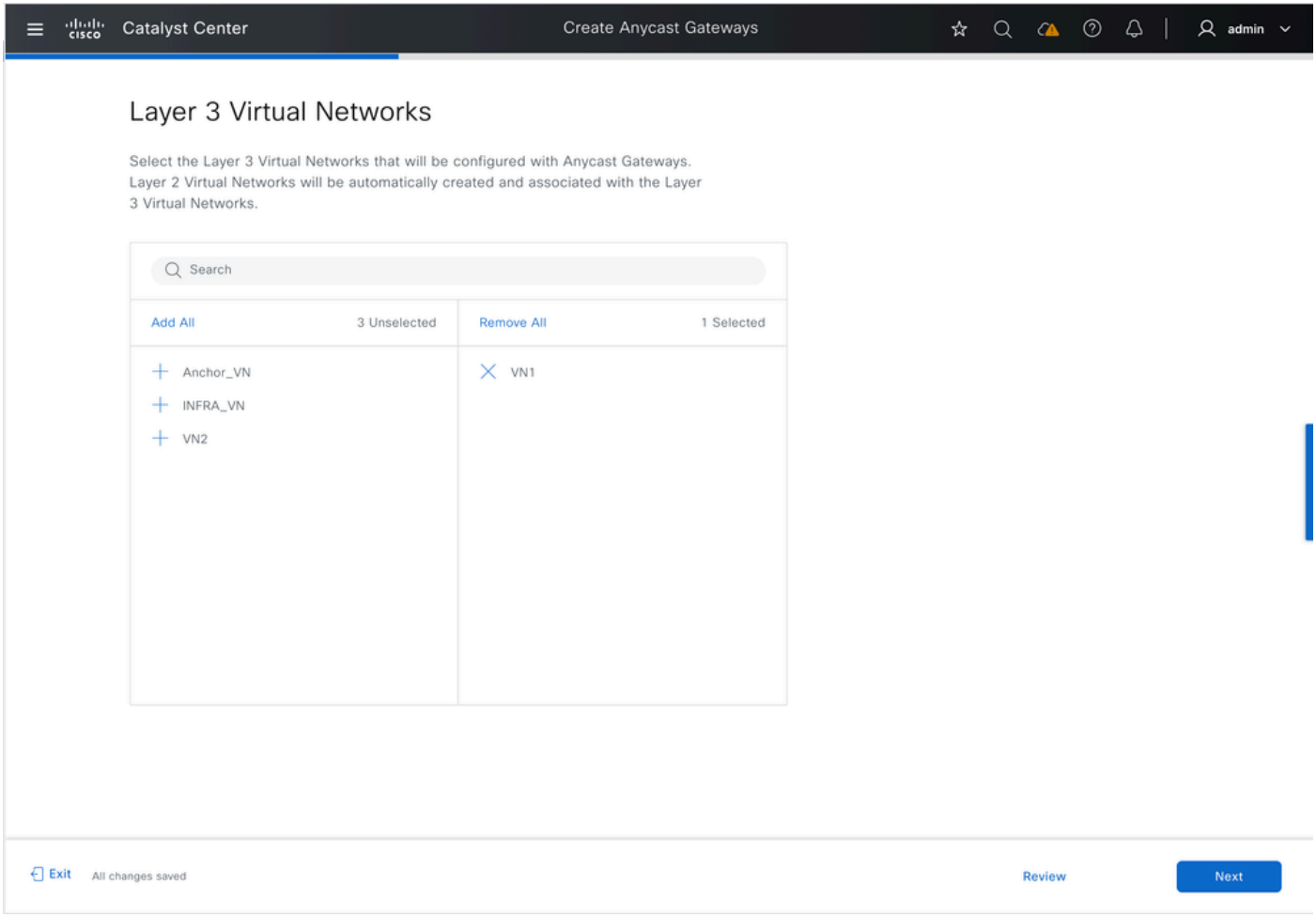
1. Vá para Provisionar.
2. Selecione Fabric Sites.
3. Escolha o site desejado.
4. Navegue até Anycast Gateways.

A partir daí, você pode definir as configurações necessárias para Difusão Direcionada por IP.



Criar Gateways Anycast

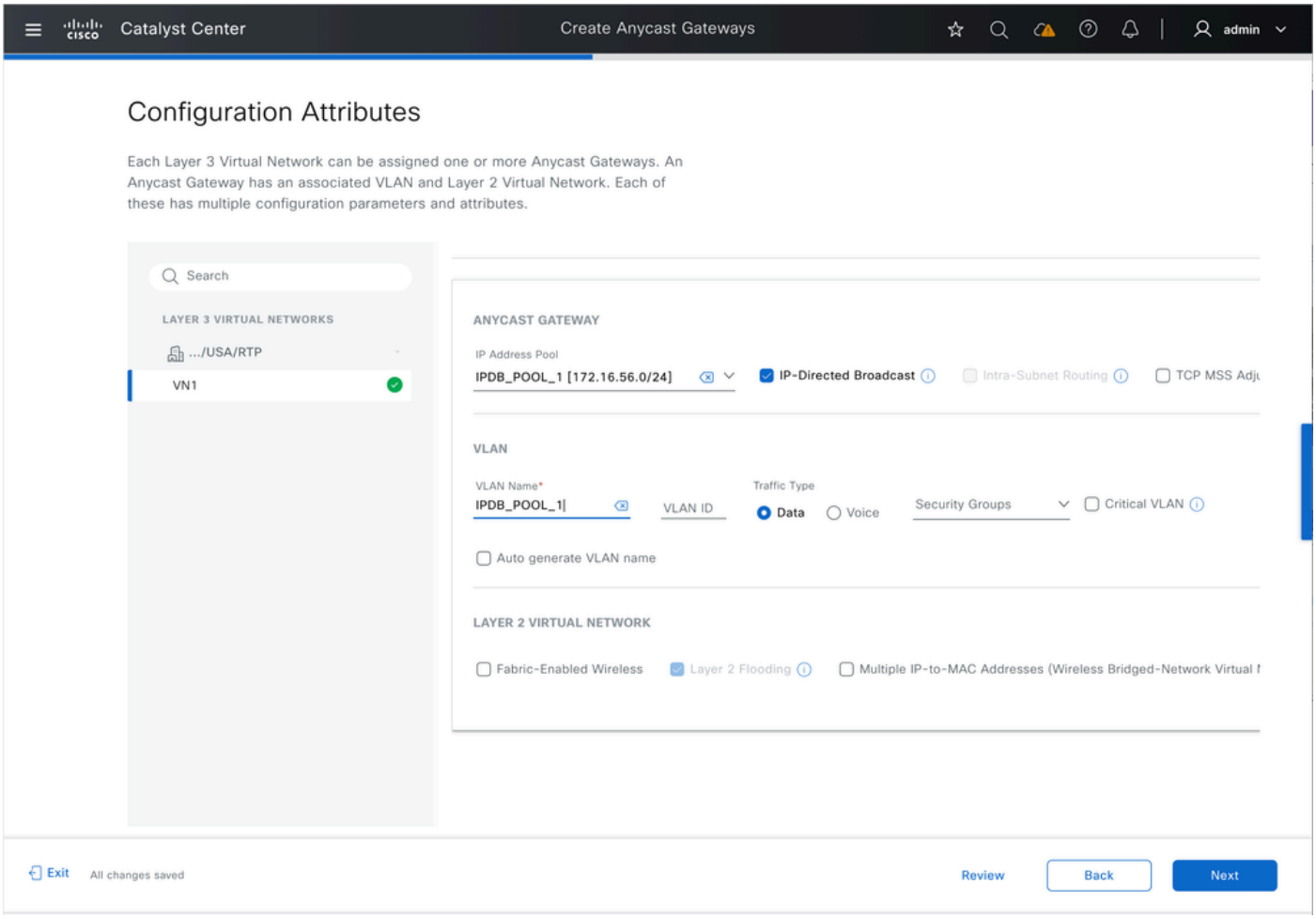
Selecione a Rede virtual L3 desejada e clique em Avançar para continuar.



Selecionar Redes Virtuais L3

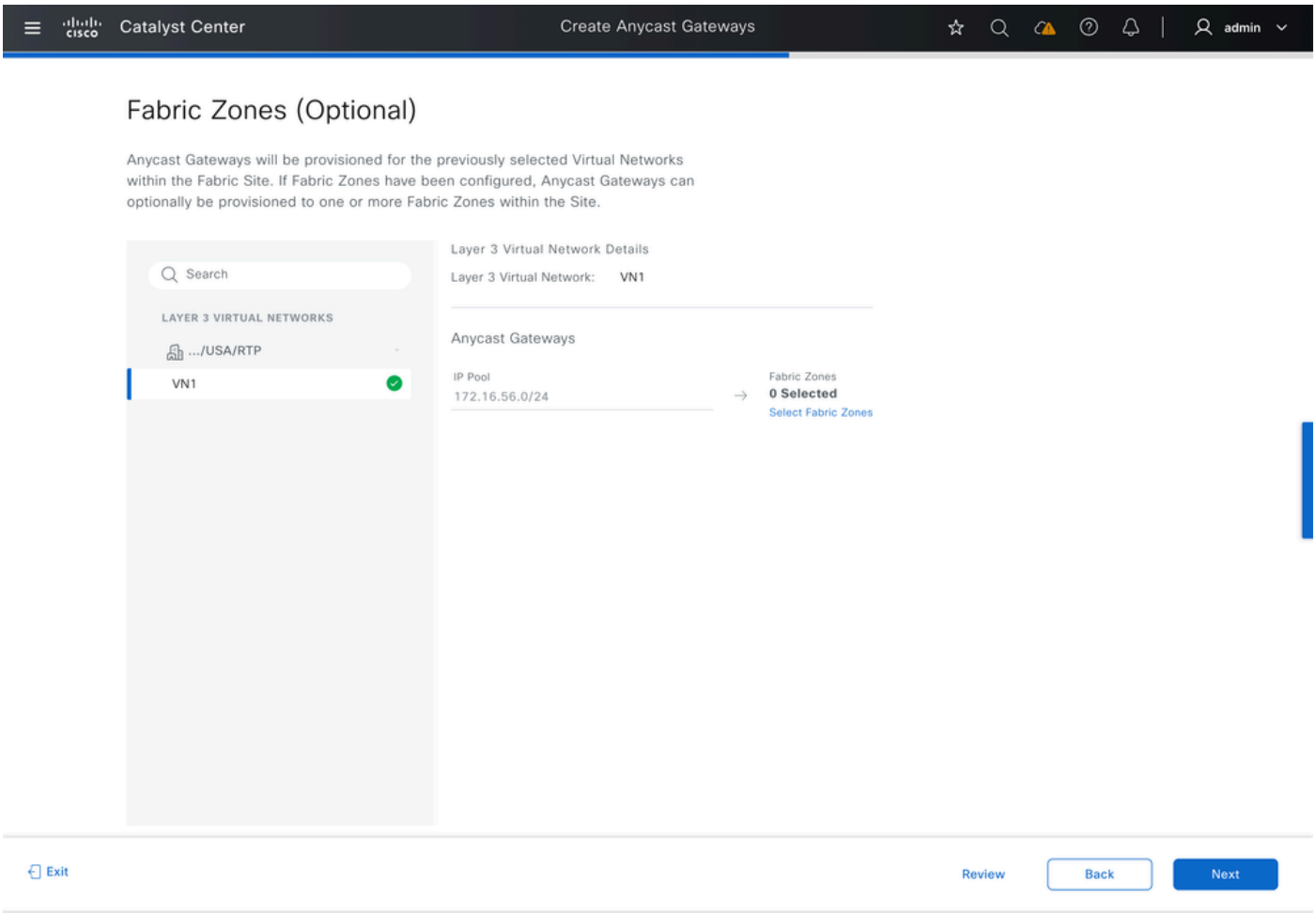
Selecione o IP Pool, ative a transmissão direcionada por IP e insira o nome da VLAN.

Tip: Habilitar a transmissão direcionada por IP ativa automaticamente a inundação de L2.



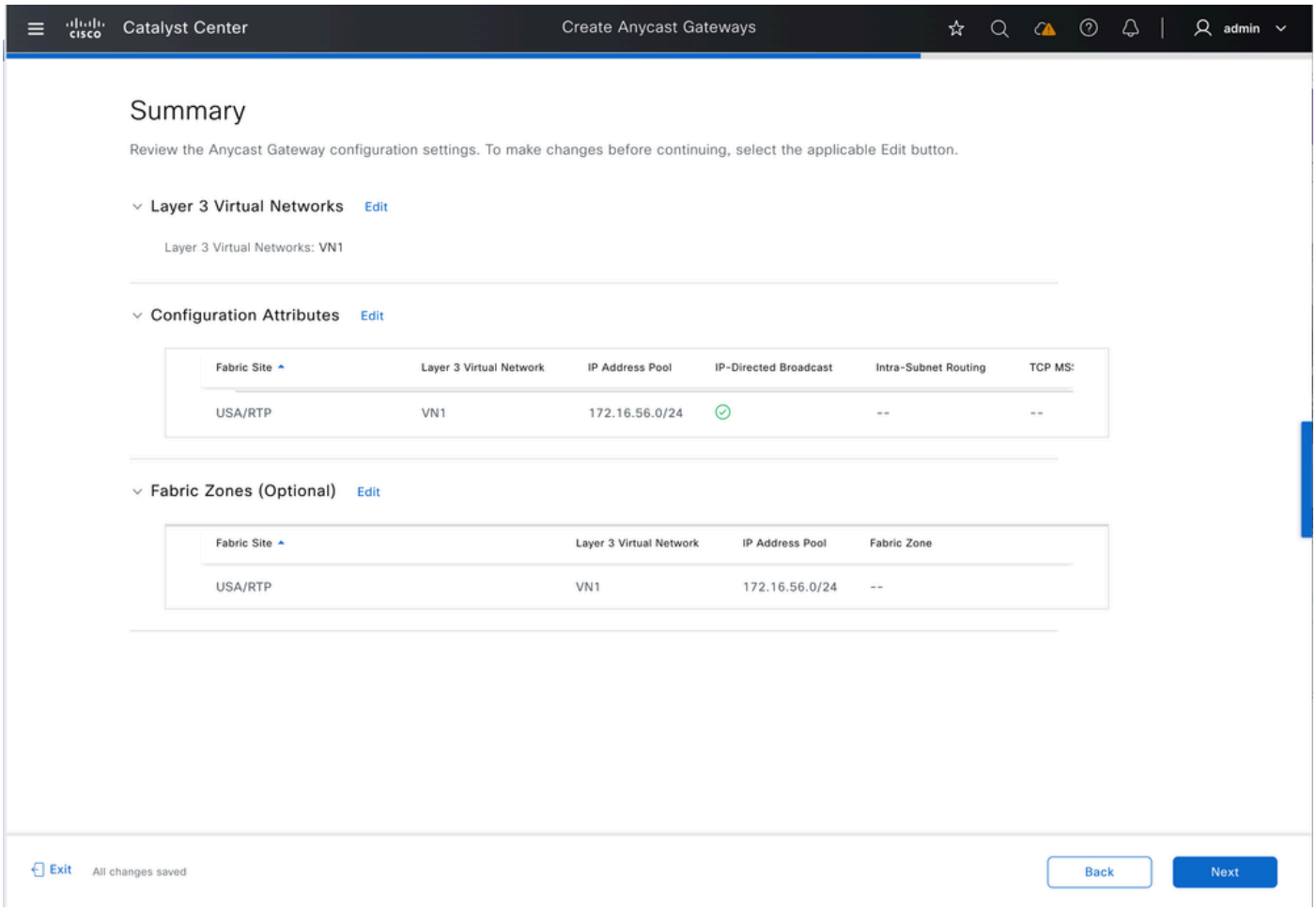
Habilitar transmissão direcionada por IP

Se houver Zonas de malha, você poderá provisionar, opcionalmente, Gateways Anycast para uma ou mais Zonas de malha dentro do site.



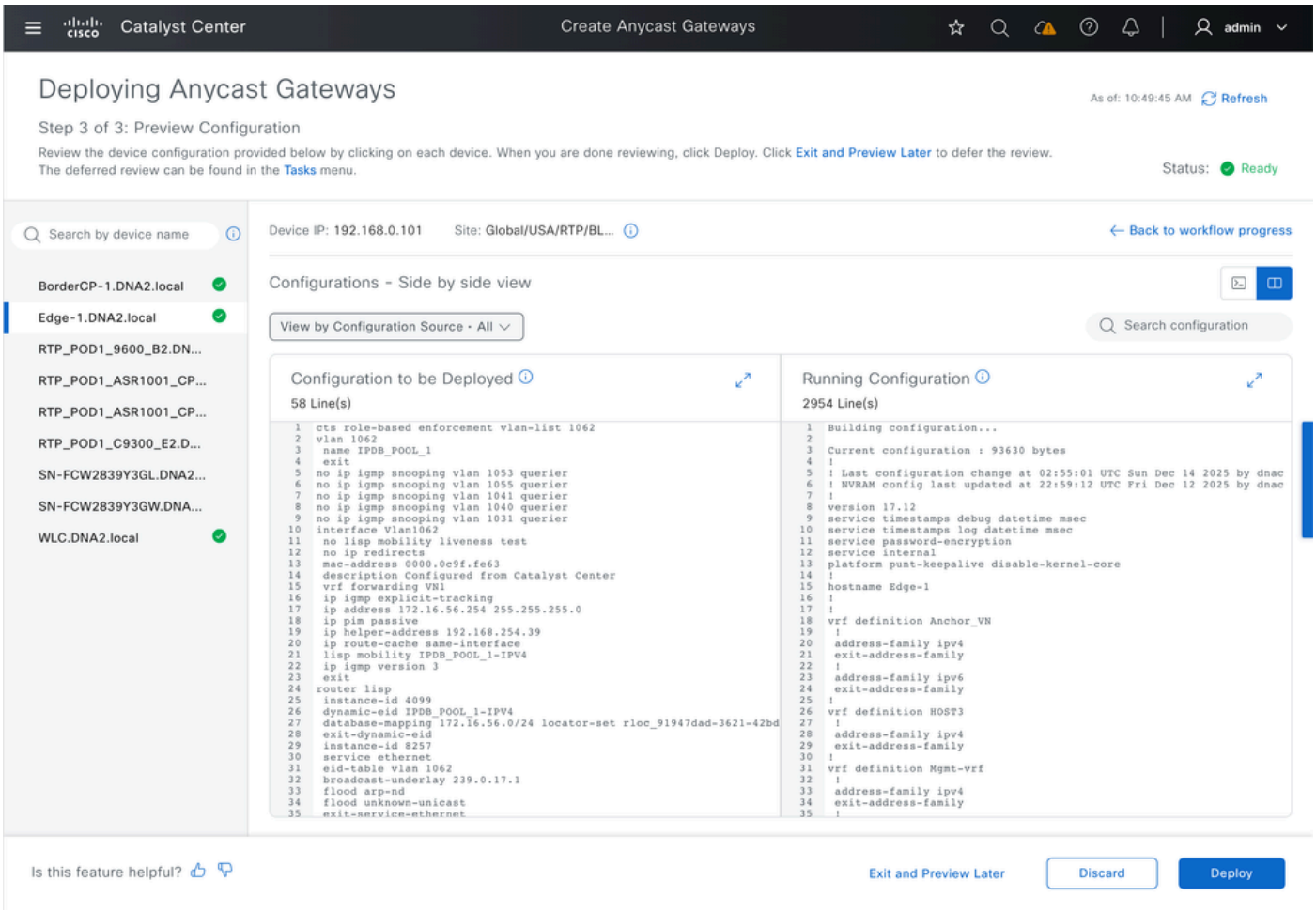
Selecionar zonas de malha

Revise o resumo das configurações definidas para confirmar a precisão antes de continuar com a implantação.



Summary

Visualize as configurações geradas. Clique em Implantar para aplicar a configuração à estrutura.



Visualização da configuração

Configuração do dispositivo de rede

Configuração de borda - Trânsito IP

As Bordas de Estrutura com Trânsito IP configurado têm suas interfaces de peering BGP definidas com "ip network-broadcast" para permitir o encaminhamento de broadcasts de sub-rede IP. O IP do gateway anycast para o pool de estrutura (VLAN de endpoint) muda de uma interface de loopback para uma SVI, que tem o "ip directed-broadcast" habilitado. Ambas as configurações são necessárias para que a Borda da estrutura converta pacotes de broadcast de sub-rede IP em broadcasts completos, permitindo que o processo funcione conforme pretendido.

Configuração de transmissão de rede IP e transmissão de rede IP:

<#root>

vlan 1062

 name

IPDB_POOL_1

interface TenGigabitEthernet1/0/44 -- L3 Handoff Interface

switchport mode trunk

switchport trunk allowed vlan all

interface Vlan1062 -- Anycast Gateway interface, now converted to an SVI

no lisp mobility liveness test
no ip redirects
mac-address 0000.0c9f.fe63
description Configured from Catalyst Center

vrf forwarding VN1

ip address 172.16.56.254 255.255.255.0

ip helper-address 192.168.254.39
ip route-cache same-interface
lisp mobility IPDB_POOL_1-IPV4

ip directed-broadcast

-- Subnet broadcasts can be translated into full broadcasts

no autostate

--

Required to keep the SVI in up/up in absence of ports assigned to the VLAN

interface Vlan3002 -- BGP Peering interface, from IP Transit configuration

description vrf interface to External router
vrf forwarding VN1

ip address 192.168.10.5 255.255.255.252

no ip redirects

ip network-broadcast

--

```
Enabled on all L3 handoff SVIs on the VRF where the target VLAN belongs to


 ip pim sparse-mode
 ip route-cache same-interface
```

Essa segunda parte da configuração permite que o recurso de Difusão Direcionada de IP ative hosts silenciosos usando uma Solicitação ARP (broadcast), semelhante ao comportamento de redes tradicionais ao lidar com tráfego unicast desconhecido. Com essa configuração, as fontes fora da estrutura podem despertar endpoints usando o tráfego unicast padrão, sem depender de broadcasts de sub-rede ou mecanismos Wake-on-LAN ("pacote mágico").

<#root>

```
router lisp
 prefix-list SITE_LOCAL_EIDS_V4
 172.16.56.0/24

instance-id 4099



dynamic-eid IPDB_POOL_1-IPV4



database-mapping 172.16.56.0/24 locator-set rloc_0f43c5d8-f48d-48a5-a5a8-094b87f3a5f7


instance-id 8257


   service ethernet
     eid-table vlan 1062

     broadcast-underlay 239.0.17.1

-- Enables Layer 2 Flooding to use BUM group 239.0.17.1


 flood arp-nd                  -- Enables the flooding of ARP requests with Layer 2 Flooding


 flood unknown-unicast
     database-mapping mac locator-set rloc_0f43c5d8-f48d-48a5-a5a8-094b87f3a5f7
ip dhcp snooping vlan 1062
```

Configuração de borda

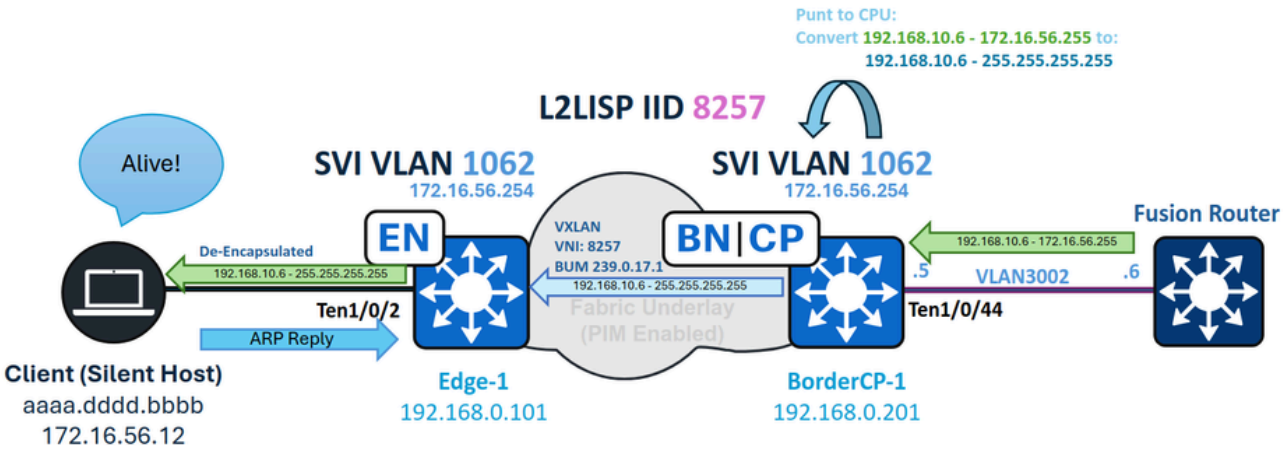
A configuração do nó de borda de estrutura corresponde à de um pool com fio padrão com a Inundação de Camada 2 habilitada. O comando CLI "ip directed-broadcast" não aparece em nós de borda.

<#root>

```
cts role-based enforcement vlan-list 1062


vlan 1062


 name

IPDB_POOL_1



interface Vlan1062


 no lisp mobility liveness test
 no ip redirects
 mac-address 0000.0c9f.fe63
 description Configured from Catalyst Center
 vrf forwarding VN1
 ip igmp explicit-tracking

ip address 172.16.56.254 255.255.255.0


 ip pim passive
 ip helper-address 192.168.254.39
 ip route-cache same-interface
 lisp mobility IPDB_POOL_1-IPV4
 ip igmp version 3

router lisp
 instance-id 4099
   dynamic-eid IPDB_POOL_1-IPV4
     database-mapping 172.16.56.0/24 locator-set rloc_91947dad-3621-42bd-ab6b-379ecebb5a2b

 instance-id 8257


   service ethernet


 eid-table vlan 1062



  broadcast-underlay 239.0.17.1


     flood arp-nd
     flood unknown-unicast
   remote-rloc-probe on-route-change
 instance-id-range 8240 , 8245 , 8249 , 8254 , 8256 -

8257

 override
  remote-rloc-probe on-route-change
  service ethernet


eid-table vlan
```

```
 1041 , 1048 , 1053 , 1059 , 1061 -
1062

    database-mapping mac locator-set rloc_91947dad-3621-42bd-ab6b-379ecebb5a2b
 ip dhcp snooping vlan 1062
```

Encaminhamento de broadcast direcionado por IP



Encaminhamento IPDB

Borda - Conversão de ingresso de punt de CPU e broadcast de sub-rede

Neste exemplo, um broadcast de sub-rede IP com um IP de destino 172.16.56.255 (o endereço de broadcast para o pool 172.16.56.0/24) é roteado a partir da rede externa e chega primeiro à Borda da Estrutura. A interface de Camada 3 de entrada é a SVI de Trânsito IP (VLAN 3002). Como o "ip network-broadcast" está ativado nessa interface, o pacote é aceito para conversão de broadcast completa; sem essa configuração, o pacote seria descartado.

O pacote chega no SVI 3002 e, como um pacote de broadcast, é enviado para a CPU do switch. Com o broadcast de rede IP configurado, o pacote é permitido e convertido em um broadcast completo.

<#root>

```
BorderCP-1#show run interfave Vlan3002
```

```
interface Vlan3002
  vrf forwarding VN1
  ip address 192.168.10.5 255.255.255.252
  ip network-broadcast

BorderCP-1#show ip cef vrf VN1 172.16.56.255
172.16.56.255/32
   receive for Vlan1062       --- The routing result is "receive", indicating that the packet undergoes
```

Durante o processamento da CPU, a VLAN 1062—a interface de destino—converte o pacote em um broadcast completo, já que está configurada com "ip directed-broadcast".

<#root>

```
BorderCP-1#show ip interface vlan 1062 | i Directed
```

```
 Directed broadcast forwarding is enabled
```

Você pode solucionar esse evento usando o comando debug ip packet. Para evitar saída excessiva e uso alto de recursos, sempre aplique uma lista de acesso como um filtro ao executar essa depuração.

<#root>

```
ip access-list standard 10
```

```
10  permit
```

```
192.168.10.6     --- Directed Broadcast source IP
```

```
BorderCP-1#debug ip packet detail 10
```

```
IP:
```

```
s=192.168.10.6 (Vlan3002)
```

,

d=172.16.56.255

(nil), len 100,

input feature

ICMP type=8, code=0, MCI Check(110), rtype 0, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
IP: s=192.168.10.6 (Vlan3002), d=172.16.56.255 (nil), len 100, input feature
ICMP type=8, code=0, Role-based Proxy(116), rtype 0, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE

FIBipv4-packet-proc: route packet from Vlan3002 src 192.168.10.6 dst 172.16.56.255

FIBfwd-proc: VN1:172.16.56.255/32 receive entry

FIBipv4-packet-proc: packet routing failed

IP: tableid=3, s=192.168.10.6 (Vlan3002), d=172.16.56.255 (Vlan1062) nexthop=172.16.56.255, routed via F

IP: s=192.168.10.6 (Vlan3002), d=172.16.56.255 (Vlan1062), len 100, output feature
ICMP type=8, code=0, feature skipped, Role-based Access List(53), rtype 1, forus FALSE, sendself FALSE,

IP: s=192.168.10.6 (Vlan3002), d=172.16.56.255 (Vlan1062), g=255.255.255.255, len 100, forward directed

A borda de entrada atua como a origem multicast (S) e o grupo (G) para encapsulamento de BUM, usando seu Loopback 0 como o endereço de origem e o grupo BUM configurado como o destino.

No plano de controle PIM, certifique-se de que um downlink em direção às bordas da estrutura apareça na lista de interface de saída para a rota multicast. Para o plano de dados, use o comando show ip mfib count para verificar se os contadores de encaminhamento de hardware estão aumentando para a entrada S,G na borda.

<#root>

BorderCP-1#show ip mroute 239.0.17.1 192.168.0.201 | be \(

(

192.168.0.201

```
,
239.0.17.1
), 5w0d/00:02:33, flags: FTA

Incoming interface: Null0
, RPF nbr 0.0.0.0
 Outgoing interface list:

TenGigabitEthernet1/0/42
, Forward/Sparse, 2d09h/00:03:23, flags:
-- Downlink to Fabric Edge or Intermediate Node

BorderCP-1#show ip mfib 239.0.17.1 192.168.0.201 count

Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Default
  16 routes, 6 (*,G)s, 3 (*,G/m)s

Group: 239.0.17.1


Source: 192.168.0.201,

    SW Forwarding: 1/0/130/0, Other: 0/0/0

 HW Forwarding: 2124804
/0/116/0, Other: 0/0/0
 Totals - Source count: 1, Packet count: 2124805
Groups: 1, 1.00 average sources per group
```

Este documento não fornece uma explicação detalhada da formação de árvore multicast subjacente ou inundação de Camada 2. No caso de estados S,G ausentes, incompletos ou errados, a parte multicast subjacente do worm requer uma solução de problemas independente.

Borda - Transmissão de entrada

Em Fabric Edges, o broadcast de entrada encapsulado em VXLAN em multicast é desencapsulado e encaminhado para a VLAN associada ao VNI (8257), alcançando todas as portas em um estado de encaminhamento em Spanning-Tree.

Primeiro, verifique se a entrada S,G da borda (com o loopback de borda como origem) para o

grupo BUM está presente e encaminhando o tráfego. Use os mesmos comandos mroute e mfib para verificar isso, certifique-se de que a sub-interface L2LISP correspondente à VLAN (1062) esteja listada como interface de saída.

<#root>

Edge-1#show ip mroute 239.0.17.1 192.168.0.201 | be \(
(192.168.0.201, 239.0.17.1),

2d09h/00:01:10, flags: JT

Incoming interface: TenGigabitEthernet1/1/2,

RPF nbr 192.168.98.2

Outgoing interface list:

L2LISP0.8257

, Forward/Sparse-Dense, 2d09h/00:02:21, flags:

Edge-1#show ip mfib 239.0.17.1 192.168.0.201 verbose | be Forwarding

Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
I/O Item Counts: HW Pkt Count/FS Pkt Count/PS Pkt Count Egress Rate in pps
Default

(192.168.0.201,239.0.17.1)

Flags: K HW DDE
  0x12C OIF-IC count: 0, OIF-A count: 1
  SW Forwarding: 2/0/402/0, Other: 0/0/0

HW Forwarding: 145023

/0/128/0, Other: 0/0/0
  TenGigabitEthernet1/1/2 Flags: RA A MA

L2LISP0.8257

,

L2LISP Decap Flags: RF F NS

CEF: OCE (lisp decap)
Pkts: 0/0/2 Rate: 0 pps

Após o desencapsulamento, o pacote é encaminhado na VLAN 1062 para todas as portas atribuídas a essa VLAN.

<#root>

Edge-1#show spanning-tree vlan 1062

VLAN1062

```
  Spanning tree enabled protocol rstp
  Root ID      Priority 33830
               Address 00b1.e331.d580
               This bridge is the root
               Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

   Bridge ID   Priority 33830 (priority 32768 sys-id-ext 1062)
               Address 00b1.e331.d580
               Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
               Aging Time 300 sec

Interface           Role Sts Cost      Prio.Nbr  Type
------------------- ---- --- --------- -------- --------------------------------
```

Te1/0/2 Desg FWD 20000 128.3 P2p Edge

Po1 Desg FWD 20000 128.3049 P2p

Depois que o ponto final recebe o pacote de broadcast, ele deve reconhecer o pacote como relevante e responder. Como resultado, o endpoint pode enviar um pacote ARP, que atualiza a tabela de rastreamento de dispositivo no switch.

<#root>

Edge-1#show device-tracking database interface Te1/0/2 | be Network

```
    Network Layer Address Link Layer Address Interface vlan prlvl age state     Time left
```

ARP 172.16.56.12 aaaa.dddd.bbbb Te1/0/2 1062 0005 0s REACHABLE 241 s

Depois que o ponto final é registrado novamente no rastreamento de dispositivo, ele é importado para o banco de dados LISP do nó de borda e, em seguida, registrado com o plano de controle.

Para implantações PUB-Sub de LISP, o Plano de controle publica as informações de endpoint recém-registradas nas Bordas, criando instantaneamente uma entrada de cache de mapa LISP para encaminhar o tráfego para o nó de borda apropriado.

<#root>

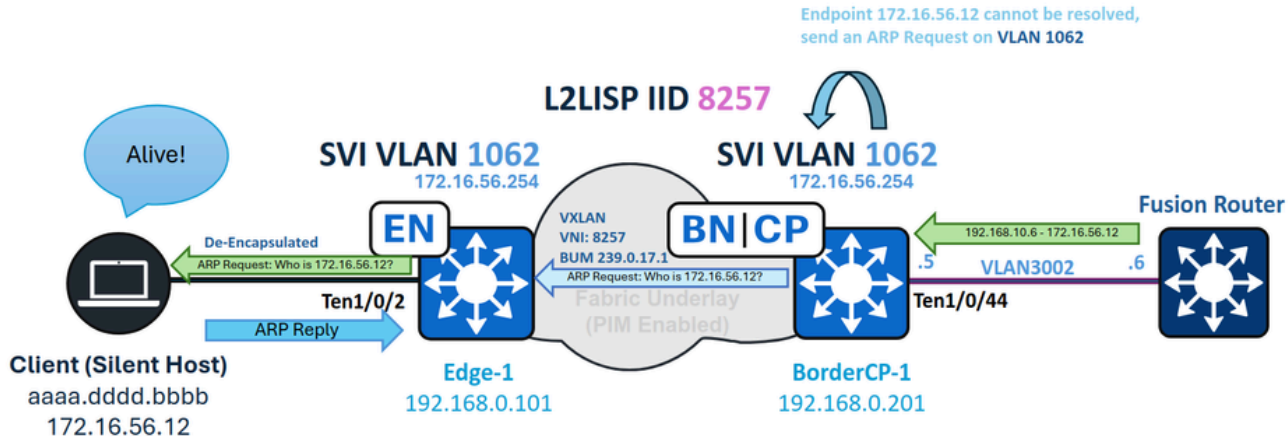
```
BorderCP-1#show lisp instance-id 4099 ipv4 map 172.16.56.12/32

LISP IPv4 Mapping Cache for LISP 0 EID-table vrf VN1 (IID 4099), 1 entries

172.16.56.12/32
, uptime: 5w0d, expires: never,
via pub-sub
,
complete
, local-to-site
 SGT: 2
 Sources: pub-sub

 State: complete, last modified: 5w0d, map-source: local
 Exempt, Packets out: 6(2432 bytes), counters are not accurate (~ 5w0d ago)
 Configured as EID address space

Locator
       Uptime
State
 Pri/Wgt Encap-IID

192.168.0.101
 5w0d
up
    10/10    -
  Last up-down state change: 5w0d, state change count: 1
  Last route reachability change: 5w0d, state change count: 1
  Last priority / weight change: never/never
  RLOC-probing loc-status algorithm:
    Last RLOC-probe sent: 00:22:19 (rtt 4ms)
```

Para implantações LISP/BGP (SDA 1.0), se a implantação for distribuída (não colocalizada), a atualização do cache de mapas LISP para um ponto de extremidade desconhecido pode levar até

um minuto, pois as Respostas de Mapa Negativo (NMRs) devem expirar primeiro.

Um host silencioso deve ignorar pacotes como broadcasts de sub-rede se não estiver programado para responder a eles. Alguns endpoints exigem um "pacote mágico" (como um eco UDP), enquanto outros respondem apenas a um ARP de broadcast. O próprio host silencioso determina que tipo de pacote o aciona para despertar. Entre as opções mais comuns, uma solicitação ARP é normalmente preferida, conforme explicado na seção Encaminhamento unicast desconhecido.

Encaminhamento Unicast Desconhecido



Encaminhamento unicast desconhecido

Quando um pool é habilitado para o IP Directed Broadcast, ele não só permite o tratamento de broadcasts de sub-rede, mas também permite que as Fabric Borders atuem como gateways para o encaminhamento de tráfego unicast desconhecido. Neste contexto, o tráfego unicast desconhecido refere-se a pacotes destinados a endpoints que não estão atualmente registrados no plano de controle.

Semelhante a um gateway de rede tradicional que envia uma solicitação ARP quando encontra uma entrada ARP incompleta, a borda gera uma solicitação ARP e a inunda para todos os nós de estrutura. Isso garante que o host silencioso receba a solicitação, desperte e envie uma resposta ARP, registrando-se novamente no Plano de Controle.

Essa funcionalidade é possível porque a VLAN de ponto de extremidade (1062) está configurada como uma SVI e como uma instância L2LISP na Borda da Estrutura. Com o "flood arp-nd" ativado no L2 IID, a borda pode inundar solicitações ARP geradas pelo SVI sempre que houver tráfego direcionado para um EID LISP desconhecido, garantindo que os hosts silenciosos recebam a solicitação ARP e tenham a oportunidade de responder e atualizar seu registro no plano de controle.

<#root>

```
BorderCP-1#show vlan id 1062

VLAN Name        Status Ports
---- ----------------------------------------
1062


IPDB_POOL_1

 active
L2LI0:8257

,
Te1/0/44
BorderCP-1#show run | se 8257


instance-id 8257


 remote-rloc-probe on-route-change
  service ethernet


eid-table vlan 1062



 broadcast-underlay 239.0.17.1


  flood arp-nd


  flood unknown-unicast
  database-mapping mac locator-set rloc_0f43c5d8-f48d-48a5-a5a8-094b87f3a5f7
```

Quando a borda da estrutura recebe um pacote destinado a 172.16.56.12 no SVI 3002, que faz parte do endpoint VN/VRF, ele tenta a resolução do LISP, já que a saída do CEF está definida como "glean" (o que significa que o dispositivo tenta resolver a adjacência de destino usando o protocolo de camada de downstream). Esse processo dispara simultaneamente uma solicitação de mapa LISP e uma resolução ARP para o host não registrado (silencioso).

<#root>

```
BorderCP-1#show lisp instance-id 4099 ipv4 map-cache 172.16.56.12

LISP IPv4 Mapping Cache for LISP 0 EID-table vrf VN1 (IID 4099), 1 entries

172.16.56.0/24,
```

```
 uptime: 00:00:30, expires: never, via dynamic-EID, send-map-request, local-to-site
Sources: NONE
State:
```

send-map-request

```
, last modified: 00:00:30, map-source: local
Exempt, Packets out: 2(1152 bytes), counters are not accurate (~ 2d15h ago)
Configured as EID address space
Configured as dynamic-EID address space
Encapsulating dynamic-EID traffic
Negative cache entry, action:
```

send-map-request   -- LISP Resolution attempted

<#root>

BorderCP-1#show ip cef vrf VN1 172.16.56.12

172.16.56.0/24

attached to LISP0.4099

BorderCP-1#show ip cef vrf VN1 172.16.56.12 internal | se output chain:

```
output chain:
PushCounter(LISP:172.16.56.0/24) 766CBD050CF0
```

glean for LISP0.4099

Uma entrada ARP incompleta é criada, solicitando que a Borda envie uma solicitação ARP ao ponto final desconhecido 172.16.56.12. Essa solicitação ARP, como um pacote de broadcast, é encaminhada downstream usando a Inundação da Camada 2 e o recurso Inundação ARP-ND.

Para verificar se a inundação de Camada 2 está operacional, monitore os contadores MFIB para o S,G local da borda.

<#root>

BorderCP-1#show ip mroute 239.0.17.1 192.168.0.201 | be \(

(

192.168.0.201

,

239.0.17.1

), 5w0d/00:02:33, flags: FTA

Incoming interface: Null0

, RPF nbr 0.0.0.0
 Outgoing interface list:

TenGigabitEthernet1/0/42

, Forward/Sparse, 2d09h/00:03:23, flags:

-- Downlink to Fabric Edge or Intermediate Node

BorderCP-1#show ip mfib 239.0.17.1 192.168.0.201 count

Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Default
  16 routes, 6 (*,G)s, 3 (*,G/m)s

Group: 239.0.17.1

Source: 192.168.0.201,

    SW Forwarding: 1/0/130/0, Other: 0/0/0

 HW Forwarding: 2124804

/0/116/0, Other: 0/0/0
 Totals - Source count: 1, Packet count: 2124805
Groups: 1, 1.00 average sources per group

O pacote ARP inundado chega ao host silencioso, despertando-o e solicitando uma resposta ARP. Essa resposta atualiza a tabela de rastreamento de dispositivo (SISF) na Borda da malha e cria uma entrada de banco de dados LISP. Como resultado, a Borda da estrutura inicia um registro no Plano de controle.

<#root>

Edge-1#show device-tracking database interface Te1/0/2 | be Network

    Network Layer Address Link Layer Address Interface vlan prlvl age state   Time left

```
ARP 172.16.56.12           aaaa.dddd.bbbb     Te1/0/2   1062 0005   0s REACHABLE 241 s
```

Depois que o ponto final é registrado novamente no rastreamento de dispositivo, ele é importado para o banco de dados LISP do nó de borda e, em seguida, registrado com o plano de controle.

Para implantações PUB-Sub de LISP, o Plano de controle publica as informações de endpoint recém-registradas nas Bordas, criando instantaneamente uma entrada de cache de mapa LISP para encaminhar o tráfego para o nó de borda apropriado.

<#root>

```
BorderCP-1#show lisp instance-id 4099 ipv4 map 172.16.56.12/32

LISP IPv4 Mapping Cache for LISP 0 EID-table vrf VN1 (IID 4099), 1 entries

172.16.56.12/32
, uptime: 5w0d, expires: never,
via pub-sub
,
complete
, local-to-site
 SGT: 2
 Sources: pub-sub

 State: complete, last modified: 5w0d, map-source: local
 Exempt, Packets out: 6(2432 bytes), counters are not accurate (~ 5w0d ago)
 Configured as EID address space

Locator
       Uptime
State
 Pri/Wgt Encap-IID

192.168.0.101
 5w0d
up
    10/10    -
  Last up-down state change: 5w0d, state change count: 1
  Last route reachability change: 5w0d, state change count: 1
  Last priority / weight change: never/never
  RLOC-probing loc-status algorithm:
    Last RLOC-probe sent: 00:22:19 (rtt 4ms)
```

Para implantações LISP/BGP (SDA 1.0), se a implantação for distribuída (não colocalizada), a atualização do cache de mapas LISP para um ponto de extremidade desconhecido pode levar até um minuto, pois as Respostas de Mapa Negativo (NMRs) devem expirar primeiro.

Tip: A Borda nunca resolve o ARP para o host silencioso; somente o registro de ponto de extremidade é necessário. Quando o host silencioso responde, o pacote ARP é enviado como um unicast de Camada 2, de modo que não é despejado em direção à Borda. Como resultado, não espere ver uma entrada ARP ou uma entrada de rastreamento de dispositivo na borda.

Ativação do Wake-on-LAN em modelos de autenticação

Quando os usuários da estrutura não têm nenhuma autenticação ativada, os pacotes inundados da fronteira alcançam hosts silenciosos, desde que a porta faça parte da VLAN onde a inundação está ativada; no entanto, com a autenticação fechada (em particular), dois fatores principais se tornam importantes.

Atribuição manual de VLAN para o host antes da autenticação

Se nenhuma VLAN for atribuída, a porta não receberá pacotes inundados de sua VLAN designada. Quando se espera que uma VLAN seja atribuída pelo RADIUS, isso cria um "Frango ou o Ovo?" dilema: o pacote inundado não pode ser encaminhado para uma VLAN diferente (comumente chamada de salto de VLAN) para disparar a autenticação de usuário e obter uma atribuição de VLAN do RADIUS.

Ao configurar a porta na Integração de host, se o dispositivo for identificado como "silencioso", atribua manualmente a VLAN usando o menu suspenso para os pools de DADOS.

A questão de hosts silenciosos serem incapazes de se autenticar antes da atribuição de VLAN não é exclusiva do SD-Access; é um desafio de design comum encontrado em qualquer rede protegida tradicional.

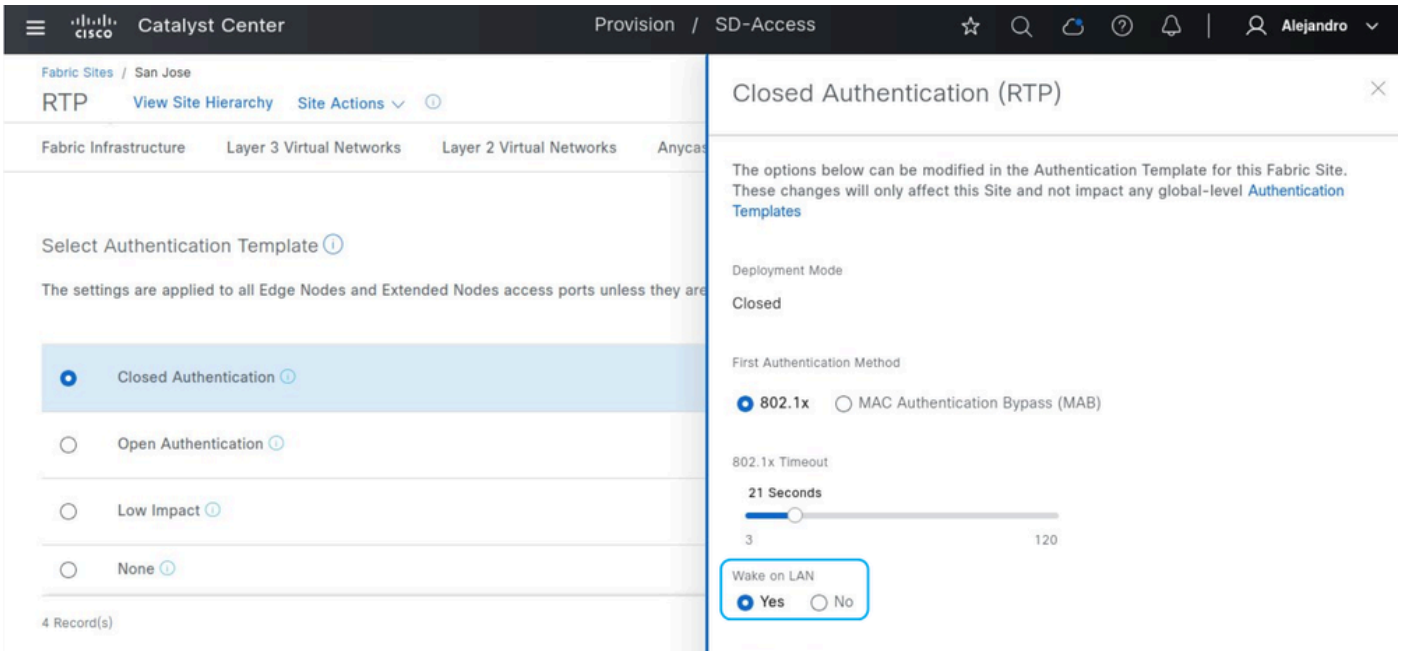
<#root>

interface TenGigabitEthernet1/0/2

```
 switchport access vlan 1062


 switchport mode access
 device-tracking attach-policy IPDT_POLICY
 dot1x timeout tx-period 7
 dot1x max-reauth-req 3


source template DefaultWiredDot1xClosedAuth


 spanning-tree portfast
 spanning-tree bpduguard enable
```

Direção do controle de acesso

Por padrão, se o Wake-on-LAN não estiver habilitado nas configurações do modelo de autenticação dentro do Host-onboarding, os modelos de autenticação usarão "access-session control-direction both". Essa configuração faz com que a porta descarte os pacotes de entrada e os pacotes que seriam encaminhados para fora da porta. Quando o Wake-on-LAN está habilitado, a configuração é alterada para "access-session control-direction in", restringindo apenas o tráfego de entrada. Esse ajuste permite que os pacotes alcancem e despertem o host silencioso, permitindo que ele inicie a autenticação MAB.



Wake-on-LAN

Sem Wake-on-LAN:

<#root>

```
Edge-1#show run all | se template DefaultWiredDot1xClosedAuth
template DefaultWiredDot1xClosedAuth


 dot1x pae authenticator
 dot1x timeout supp-timeout 7
 dot1x max-req 3
 switchport mode access
 switchport voice vlan 2046
 mab radius
 access-session host-mode multi-auth
 access-session
 control-direction both


 access-session
closed


access-session port-control auto



Edge-1#show authentication session interface Te1/0/2 detail | i Oper
Oper host mode: multi-auth

Oper control dir: both
Oper host mode: multi-auth

Oper control dir: both
```

Antes que o ponto final seja autenticado, a interface atribuída a ele não é listada como habilitada para inundação nos estados Spanning Tree.

<#root>

```
Edge-1#show spanning-tree interface Te1/0/2


no spanning tree info available for TenGigabitEthernet1/0/2
```

Com Wake-on-LAN habilitado:

<#root>

```
Edge-1#show run | se template DefaultWiredDot1xClosedAuth
```

```
template DefaultWiredDot1xClosedAuth


 dot1x pae authenticator
 dot1x timeout supp-timeout 7
 dot1x max-req 3
 switchport mode access
 switchport voice vlan 2046
 mab
 access-session control-direction in


 access-session closed


 access-session port-control auto
```

```
Edge-1#show authen session interface Te1/0/2 de | i Oper

Oper host mode: multi-auth
Oper control dir: in

Oper host mode: multi-auth
Oper control dir: in
```

Mesmo antes da autenticação, a porta é habilitada para tráfego de saída, permitindo que os pacotes alcancem e despertem o host silencioso.

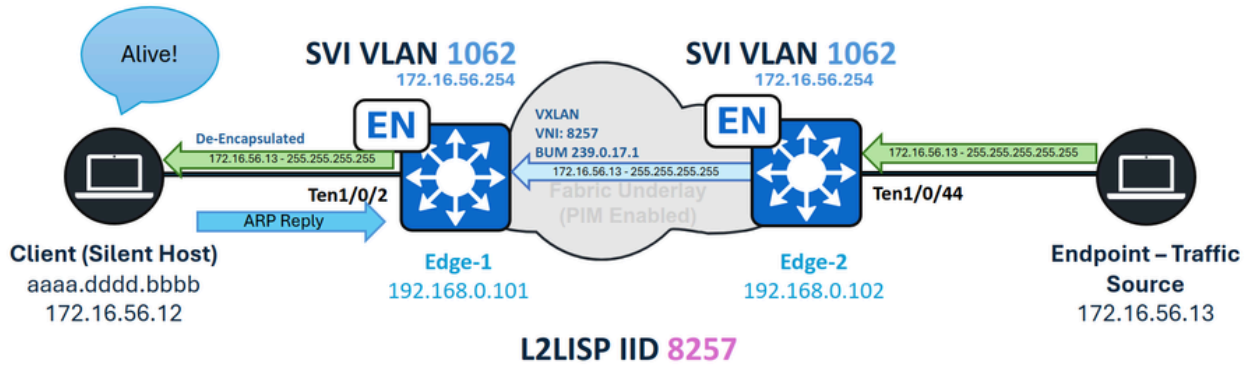
<#root>

```
Edge-1#show spanning-tree interface TenGigabitEthernet 1/0/2

Vlan                Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
VLAN1062
            Desg
FWD
 19        128.2    P2p Edge
```

Cenários alternativos

Nós de borda e mesma VLAN - inundação de camada 2

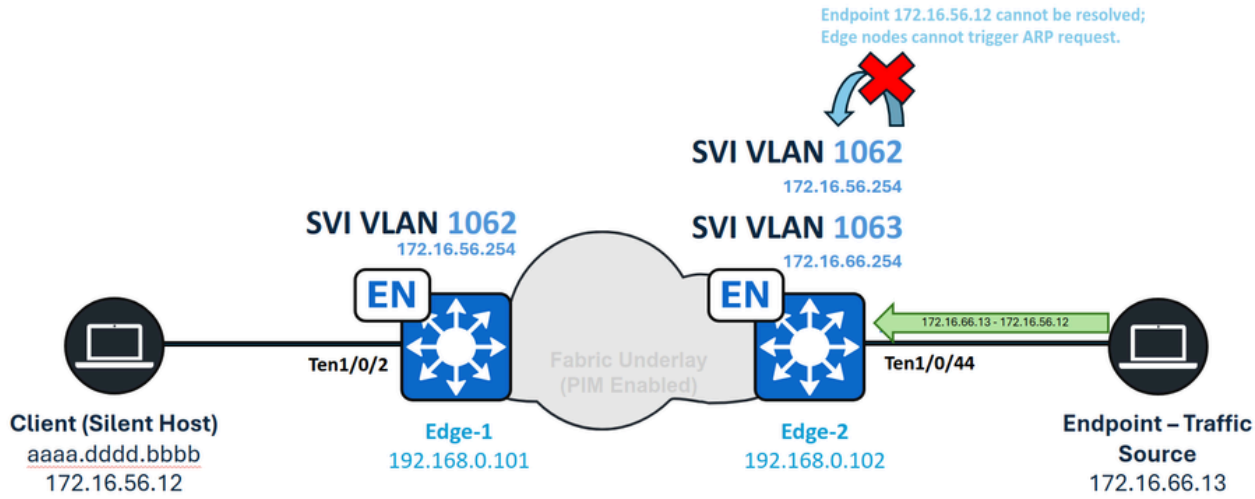
Se o objetivo é despertar um host silencioso de um dispositivo dentro da estrutura na mesma VLAN que o host, o recurso de transmissão direcionada por IP não é necessário. Em vez disso, habilitar a inundação de Camada 2 (em um pool sem fio) é suficiente para permitir a troca de pacotes de broadcast, broadcasts de sub-rede ou solicitações ARP. Para a autenticação fechada, os requisitos Wake-on-LAN são mantidos.



Mesma VLAN - Manipulação silenciosa de host

Nós de borda e VLAN diferente - unicast desconhecido

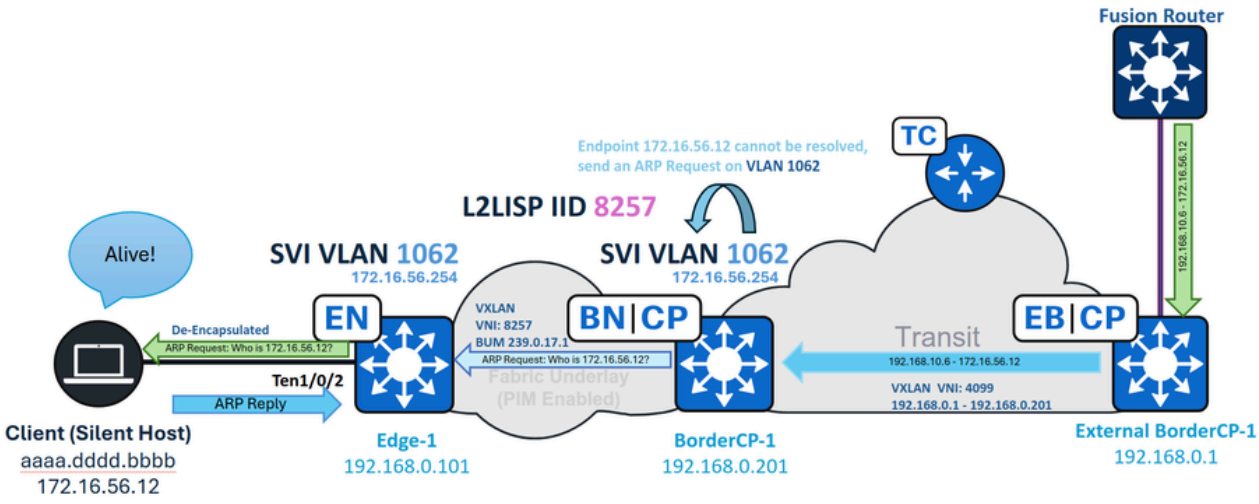
Quando um endpoint dentro da malha envia tráfego unicast a um host silencioso conectado a um nó de borda de malha, o caminho de encaminhamento unicast desconhecido não está disponível. Diferentemente das Bordas de Malha, os nós de Borda de Malha têm Bordas definidas como Proxy-ETRs LISP, que habilitam automaticamente um recurso de encaminhamento chamado "Sinal e Encaminhamento" quando um endpoint desconhecido é detectado. A Borda de malha deve disparar a solicitação ARP necessária na primeira tentativa de resolver o endereço. No entanto, uma vez que LISP identifica o ponto final como um EID desconhecido, os pacotes subsequentes não disparam solicitações ARP adicionais. Este cenário é considerado sem suporte.



Unicast Inter-VLAN desconhecido

SD-Access Transit - Unknown Unicast

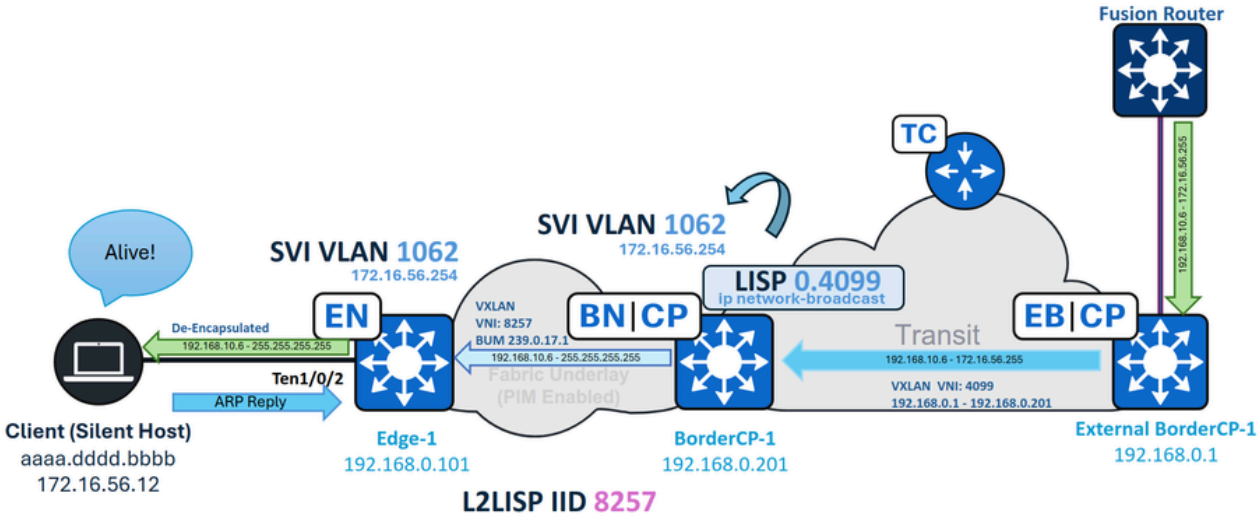
No caso de SD-Access Transit, o tráfego unicast desconhecido é suportado nativamente sem nenhum requisito especial. O tráfego originário de uma borda remota é roteado através da rede de trânsito de acesso SD, com broadcasts de sub-rede tratados como tráfego roteado regular. Quando o tráfego atinge a fronteira do site local, as operações padrão são executadas, incluindo Glean de tráfego, inundação de solicitação ARP e resolução LISP.



Unicast desconhecido do trânsito de acesso SD

SD-Access Transit - IP Directed Broadcast (Trânsito de Acesso SD - Transmissão Direcionada por IP)

Quando o tráfego de acesso SD está em uso, a borda da instalação local recebe o broadcast direcionado IP na subinterface LISP para o VN (por exemplo, a interface 4099), em vez de em um SVI. Para garantir que o broadcast seja aceito e convertido em um broadcast de sub-rede pelo recurso IP Directed Broadcast, você deve configurar manualmente o parâmetro "ip network-broadcast" na sub-interface LISP.



SD-Access Transit IPDB (IPDB de trânsito de acesso SD)

Em BorderCP-1 (fronteira de local):

```
interface LISP0.4099
  ip network-broadcast
```

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.