Configuration de l'hôte silencieux SD-Access avec la fonctionnalité de diffusion dirigée IP

Table des matières

Introduction

Ce document décrit la gestion des hôtes silencieux dans SD-Access, en répondant aux défis de connectivité à l'aide de l'inondation L2 et de la diffusion dirigée IP.

Description

La plupart des terminaux et leurs interfaces réseau transmettent régulièrement du trafic, en particulier les messages liés au contrôle tels que ARP ou DHCP. Cependant, certains points d'extrémité répondent uniquement lorsqu'ils y sont invités, plutôt que d'envoyer des paquets à intervalles réguliers. Ces périphériques envoient des paquets de contrôle uniquement à la demande. Dans le domaine des réseaux, ces terminaux sont généralement appelés « hôtes

silencieux ». Dans le contexte de SD-Access, les hôtes silencieux doivent arrêter tout trafic ou restreindre leur communication en retenant les paquets du plan de contrôle.

Dans le fabric SDA, les diffusions sont soit supprimées au niveau de chaque noeud Edge, soit transmises à tous les noeuds Edge à l'aide d'une inondation L2, processus généralement limité aux noeuds Edge et aux frontières L2. Le transfert des diffusions vers chaque port d'un VLAN imite le comportement d'un réseau de couche 2 traditionnel, ce qui permet aux hôtes silencieux de rester actifs. Cependant, la gestion d'hôtes silencieux dans un environnement de fabric présente des difficultés, car leur absence de communication régulière peut perturber les mécanismes d'authentification, les enregistrements du plan de contrôle et le transfert.

L'activation de l'inondation de couche 2 ne résout qu'une partie du problème. Les hôtes silencieux peuvent recevoir des paquets de diffusion uniquement lorsqu'un autre périphérique les génère, soit à partir du même VLAN à l'intérieur du fabric, soit à partir d'une frontière de fabric. Une diffusion dirigée par IP fait référence à un paquet IP dont l’adresse de destination est définie sur l’adresse de diffusion d’un sous-réseau, provenant d’un hôte situé en dehors de ce sous-réseau. Cette fonctionnalité nécessite la prise en charge de la multidiffusion dans le sous-réseau. Lorsque la diffusion dirigée IP est activée dans le fabric, tous les paquets de diffusion de sous-réseau atteignent chaque hôte de ce sous-réseau. Cette fonctionnalité peut également réveiller les périphériques à l'aide de paquets de monodiffusion standard, simulant ainsi le comportement de monodiffusion inconnue des réseaux traditionnels.

Topologie

Matériel et logiciels

- Commutateurs Catalyst 9000
- Catalyst Center Version 2.3.7.9
- Cisco IOS® XE 17.15.03 et versions ultérieures (Border/CP et Edge)

Topologie:

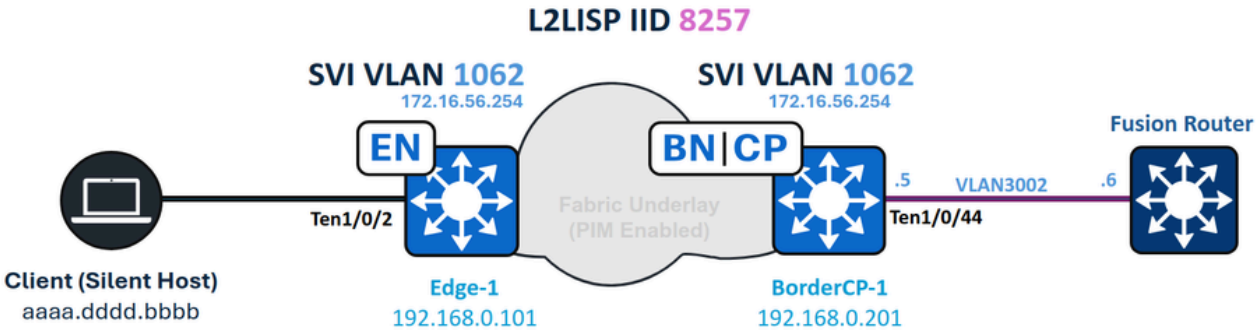


Diagramme du réseau

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Transmission IP (Internet Protocol)
- Protocole LISP (Locator/ID Separation Protocol)
- Protocole PIM (Protocol Independent Multicast)
- Inondation de couche 2 dans SD-Access

Exigences

- Cette fonctionnalité nécessite Cisco Catalyst Center 1.3 ou version ultérieure
- Licences Cisco IOS XE 17.3 et Cisco DNA Advantage*
- Pour les frontières ASR et ISR, Cisco IOS XE 17.3.1 ou supérieur est requis
- Les commutateurs Catalyst 3000, 4000, 6000 ou Nexus 7000 ne sont pas pris en charge

---

⚠ Mise en garde : L'activation de la fonction de diffusion dirigée IP active automatiquement l'inondation de couche 2. Assurez-vous que la fonctionnalité de multidiffusion dans le sous-réseau fonctionne correctement avant d'activer cette fonctionnalité.

Vous pouvez activer ou désactiver la diffusion dirigée IP après avoir créé le pool d'adresses IP, comme pour la gestion des pools sans fil ou les paramètres d'inondation de couche 2.

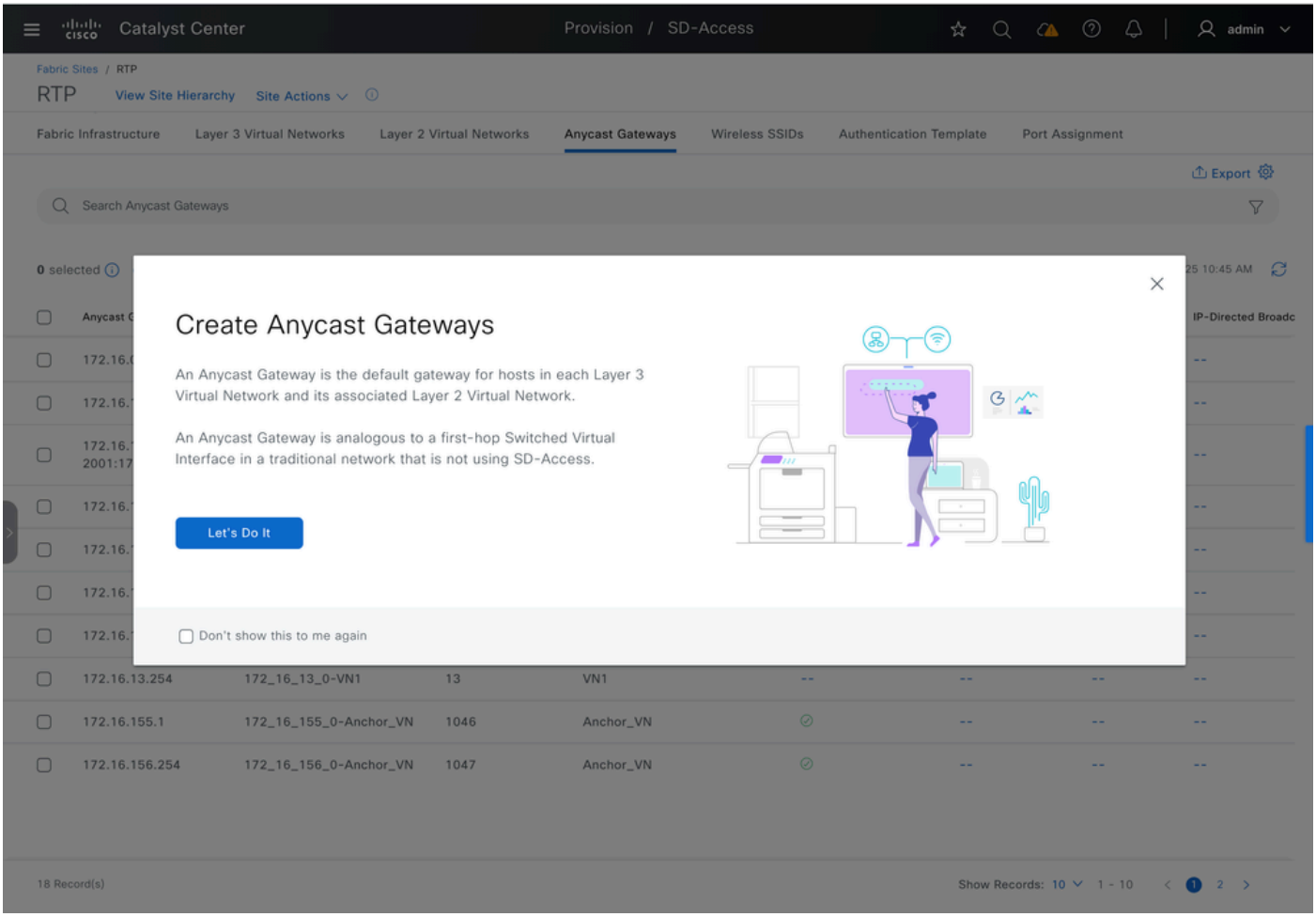
Configuration de Catalyst Center

Lorsque la diffusion dirigée IP est activée, Catalyst Center lance une tâche de mise en service à l'échelle du fabric. Tous les noeuds de périphérie, les frontières L2 et les frontières avec transfert L3 sont inclus dans ce processus d'approvisionnement.

Pour déclencher le flux de travail de diffusion dirigée IP dans l'interface utilisateur :

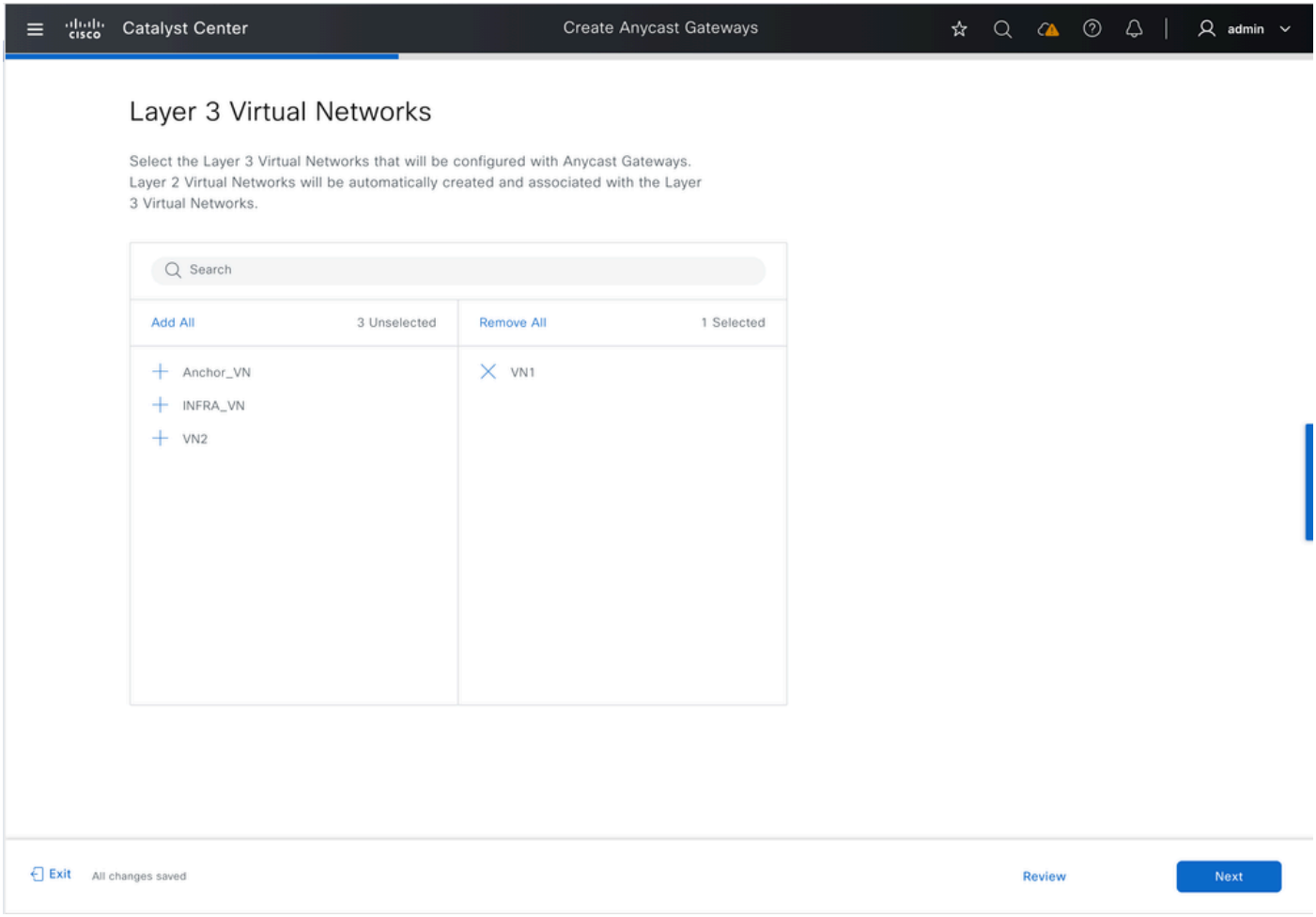
1. Accédez à Provisionner.
2. Sélectionnez Fabric Sites.
3. Sélectionnez le site souhaité.
4. Accédez à Passerelles Anycast.

À partir de là, vous pouvez configurer les paramètres requis pour la diffusion dirigée IP.



Créer des passerelles Anycast

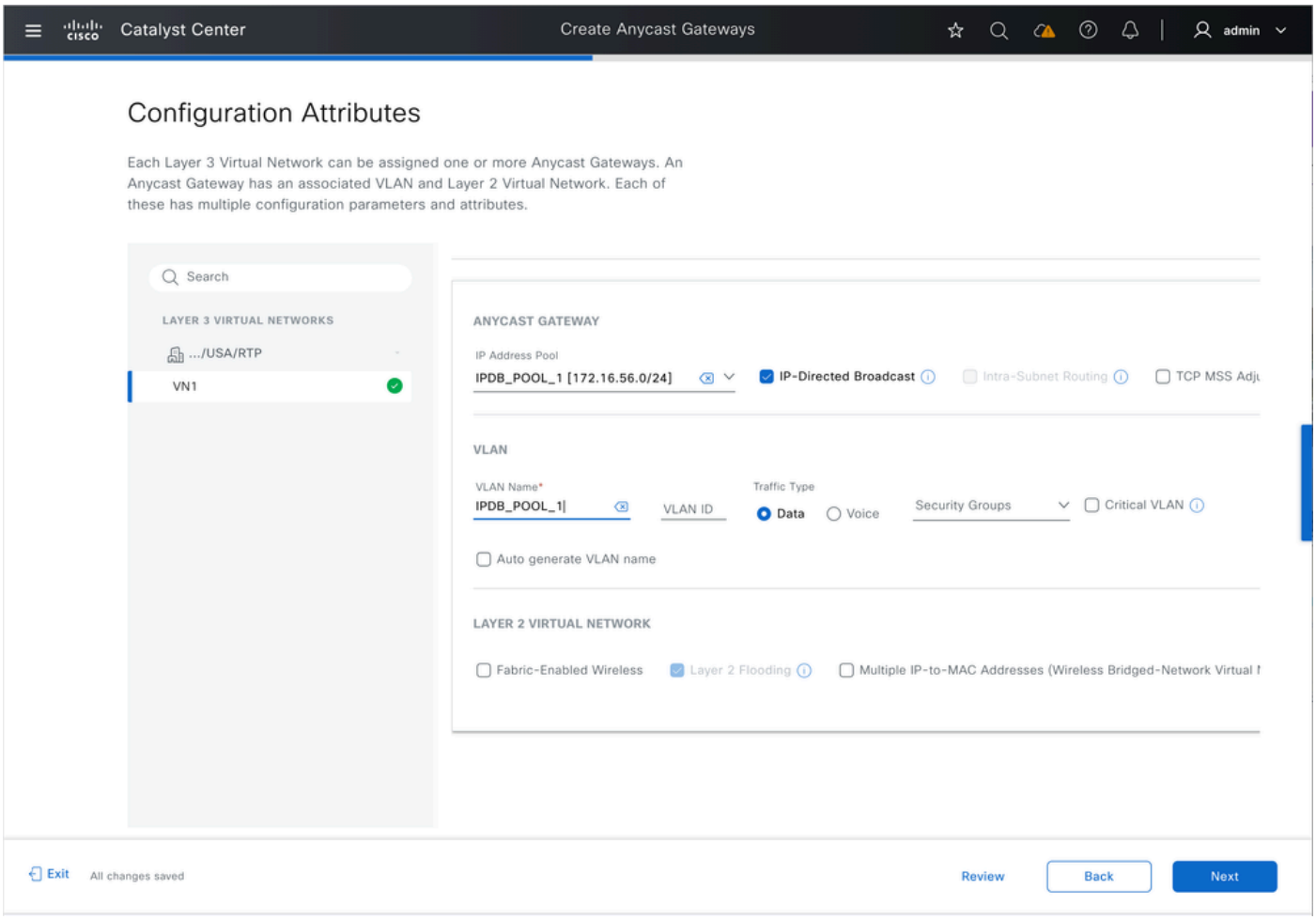
Sélectionnez le réseau virtuel L3 souhaité, puis cliquez sur Next pour continuer.



Sélectionner des réseaux virtuels de couche 3

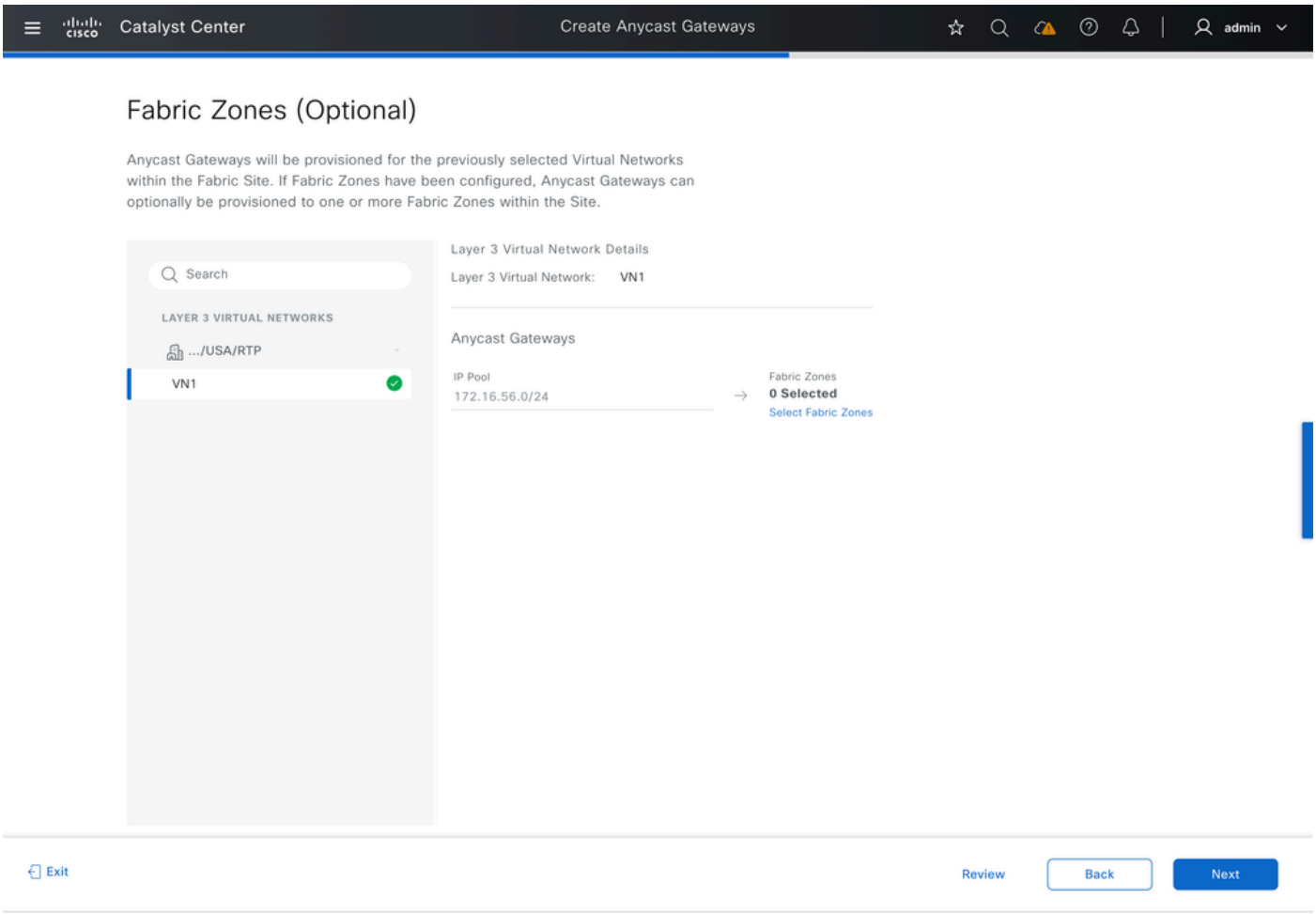
Sélectionnez le pool d'adresses IP, activez IP Directed Broadcast et entrez le nom du VLAN.

Conseil : L'activation de la diffusion dirigée IP active automatiquement l'inondation de couche 2.



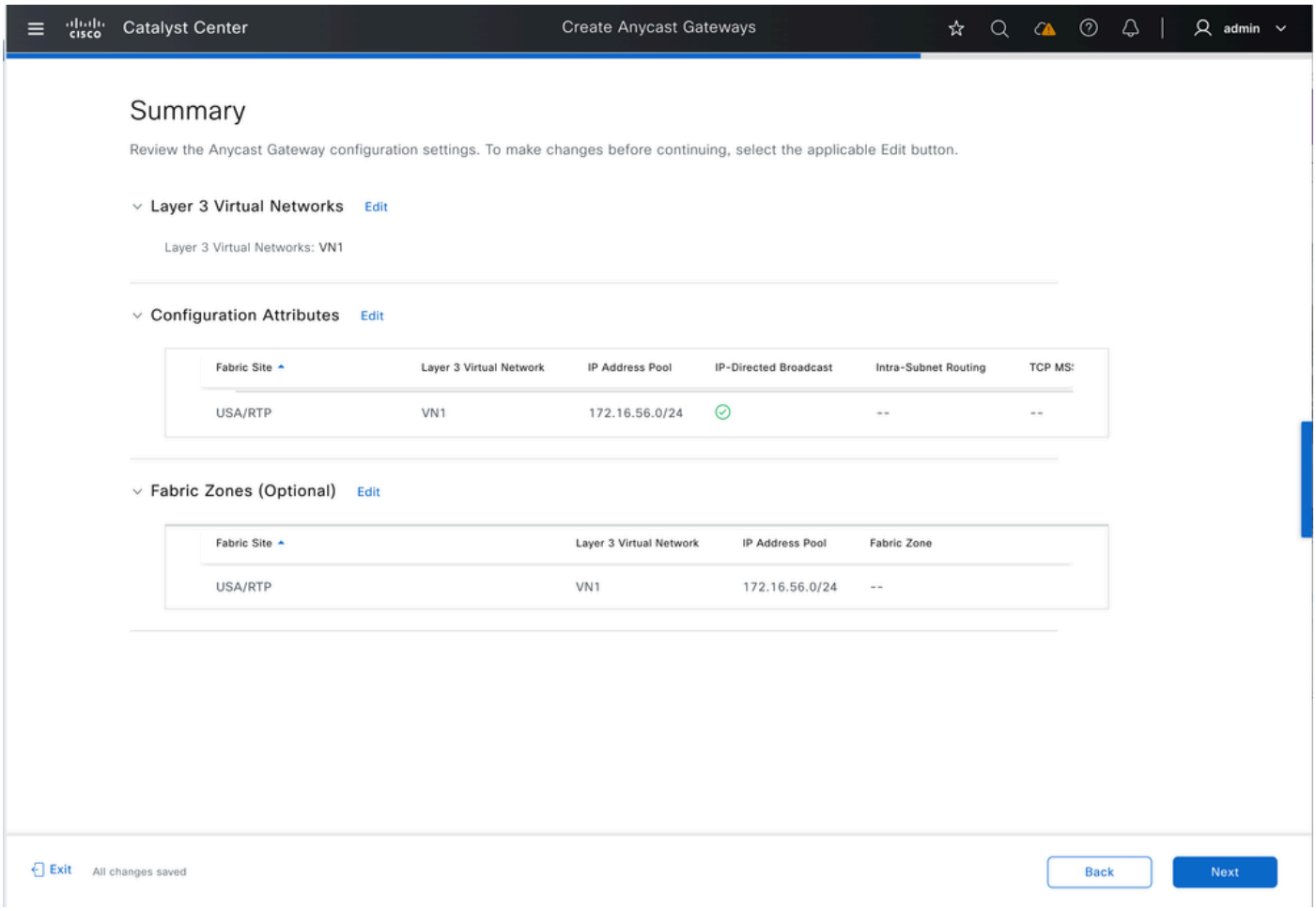
Activer la diffusion dirigée IP

Si des zones de fabric existent, vous pouvez éventuellement provisionner des passerelles Anycast sur une ou plusieurs zones de fabric du site.



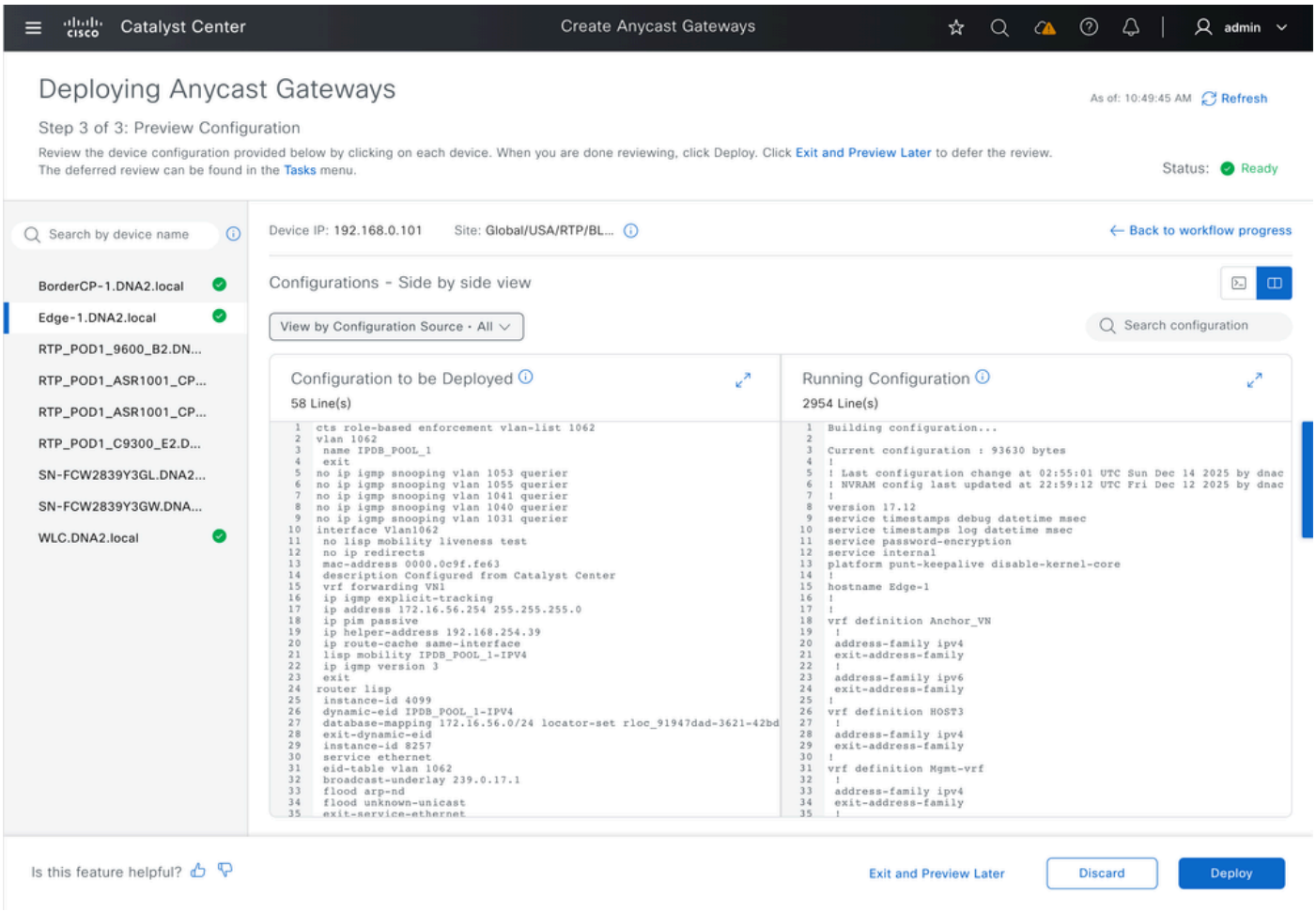
Sélectionner des zones de fabric

Vérifiez le résumé des paramètres configurés pour confirmer leur exactitude avant de poursuivre le déploiement.



Résumé

Affichez un aperçu des configurations générées. Cliquez sur Deploy pour appliquer la configuration au fabric.



Aperçu de la configuration

Configuration des périphériques réseau

Configuration de la frontière - Transit IP

Les interfaces d'appairage BGP des frontières de fabric configurées avec IP Transit sont définies avec « ip network-broadcast » pour permettre le transfert des diffusions de sous-réseau IP. L'adresse IP de la passerelle Anycast pour le pool de fabric (VLAN de point de terminaison) passe d'une interface de bouclage à une interface SVI, pour laquelle la fonction « ip directed-broadcast » est activée. Ces deux configurations sont nécessaires pour que la périphérie du fabric convertisse les paquets de diffusion de sous-réseau IP en diffusions complètes, permettant ainsi au processus de fonctionner comme prévu.

Diffusion réseau IP et configuration de diffusion réseau 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
```

Cette deuxième partie de la configuration permet à la fonctionnalité IP Directed-Broadcast de réveiller les hôtes silencieux à l'aide d'une requête ARP (diffusion), comme le font les réseaux traditionnels lorsqu'ils traitent du trafic de monodiffusion inconnu. Avec cette configuration, les sources externes au fabric peuvent réveiller les terminaux à l'aide du trafic de monodiffusion standard, sans dépendre des diffusions de sous-réseau ou des mécanismes Wake-on-LAN (« paquet magique »).

<#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
```

Configuration de périphérie

La configuration du noeud de périphérie du fabric correspond à celle d'un pool câblé standard

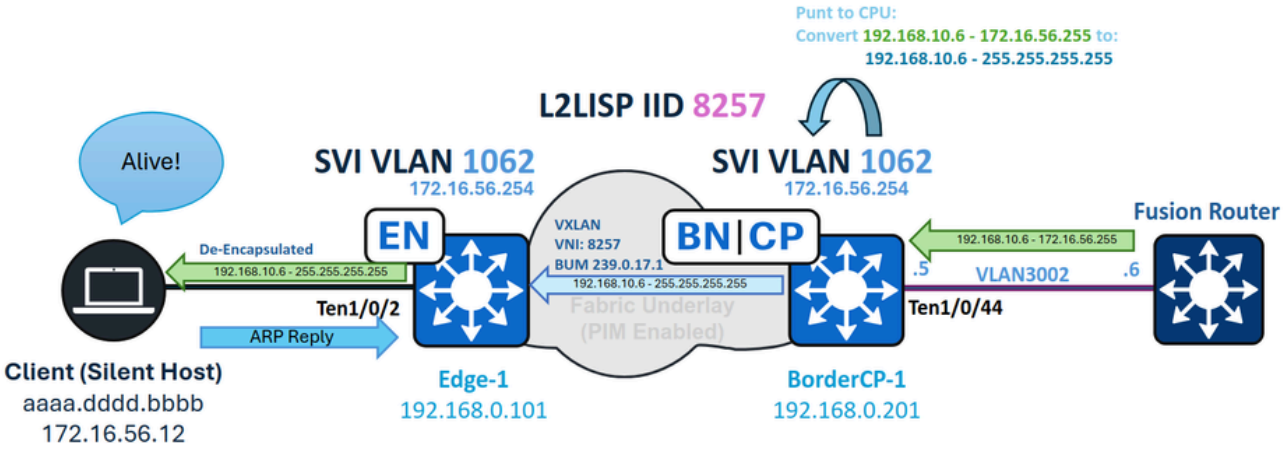
avec l'option Inondation de couche 2 activée. La commande CLI « ip directed-broadcast » n'apparaît pas sur les noeuds Edge.

<#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
```

Transfert de diffusion dirigé IP



Transfert IPDB

Périphérie - Conversion de débit processeur entrant et de diffusion de sous-réseau

Dans cet exemple, une diffusion de sous-réseau IP avec l'adresse IP de destination 172.16.56.255 (l'adresse de diffusion pour le pool 172.16.56.0/24) est routée à partir du réseau externe et arrive d'abord à la périphérie du fabric. L'interface de couche 3 d'entrée est l'interface SVI de transit IP (VLAN 3002). Étant donné que « ip network-broadcast » est activé sur cette interface, le paquet est accepté pour une conversion de diffusion complète ; sans cette configuration, le paquet serait abandonné.

Le paquet arrive sur l'interface SVI 3002 et, en tant que paquet de diffusion, est envoyé au processeur du commutateur. Une fois la diffusion réseau IP configurée, le paquet est autorisé et converti en diffusion complète.

<#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
```

Pendant le traitement du processeur, le VLAN 1062 (l'interface de destination) convertit le paquet en diffusion complète, car il est configuré avec « ip directed-broadcast ».

<#root>

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

```
 Directed broadcast forwarding is enabled
```

Vous pouvez dépanner cet événement en utilisant la commande debug ip packet. Pour éviter une sortie excessive et une utilisation élevée des ressources, appliquez toujours une liste de contrôle d'accès comme filtre lors de l'exécution de ce débogage.

<#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
```

La bordure d'entrée agit comme source de multidiffusion (S) et groupe (G) pour l'encapsulation BUM, en utilisant son bouclage 0 comme adresse source et le groupe BUM configuré comme destination.

Sur le plan de contrôle PIM, assurez-vous qu'une liaison descendante vers les bords du fabric apparaît dans la liste des interfaces sortantes pour la route de multidiffusion. Pour le plan de données, utilisez la commande show ip mfib count pour vérifier que les compteurs de transfert matériel augmentent pour l'entrée S, G sur la frontière.

<#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
```

Ce document ne fournit pas d'explication détaillée de la formation d'arborescence multicast sous-jacente ou de l'inondation de couche 2. En cas d’états S, G manquants, incomplets ou incorrects, la partie de multidiffusion sous-jacente du réseau nécessite un dépannage indépendant.

Périphérie - Diffusion entrante

Sur les périphéries de fabric, la diffusion entrante encapsulée dans le VXLAN sur la multidiffusion est désencapsulée et transférée au VLAN associé au VNI (8257), atteignant tous les ports dans un état de transmission dans le Spanning Tree.

Vérifiez d'abord que l'entrée S, G de la frontière (avec le bouclage Border comme source) pour le groupe BUM est présente et transfère le trafic. Utilisez les mêmes commandes mroute et mfib pour vérifier ceci, assurez-vous que la sous-interface L2LISP correspondant au VLAN (1062) est listée comme interface sortante.

<#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
```

Après la désencapsulation, le paquet est transféré sur le VLAN 1062 vers tous les ports affectés à ce 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

Une fois que le point d'extrémité reçoit le paquet de diffusion, il doit le reconnaître comme pertinent et y répondre. Par conséquent, le terminal peut envoyer un paquet ARP, qui met à jour la table de suivi des périphériques sur le commutateur.

<#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
```

Une fois le point d'extrémité réenregistré dans le suivi des périphériques, il est importé dans la base de données LISP du noeud Périphérie, puis enregistré dans le plan de contrôle.

Pour les déploiements LISP Pub-Sub, le plan de contrôle publie les informations de point de terminaison nouvellement enregistrées sur Borders, créant instantanément une entrée de cache de mappage LISP pour transférer le trafic vers le noeud de périphérie approprié.

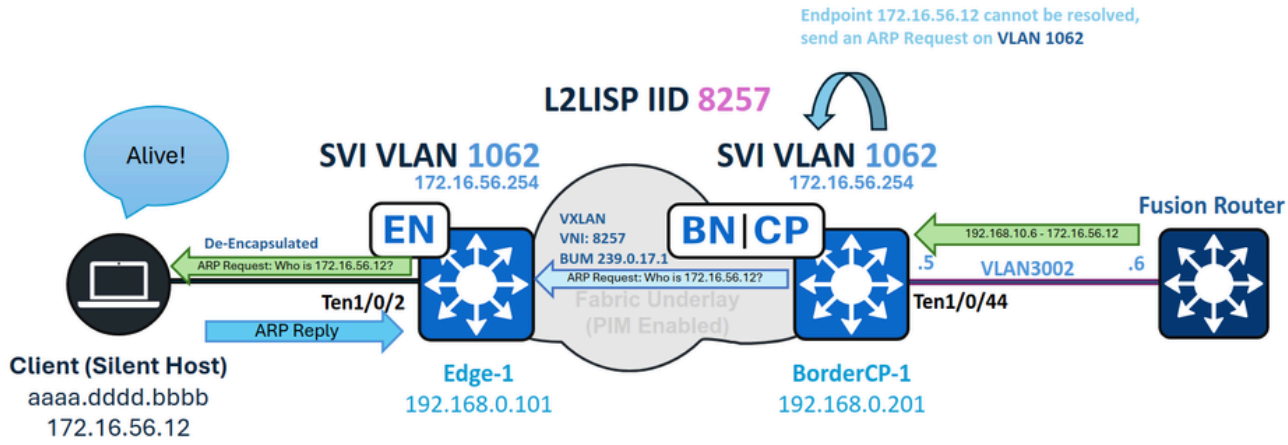
<#root>

```
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)
```

Pour les déploiements LISP/BGP (SDA 1.0), si le déploiement est distribué (non colocalisé), la mise à jour du cache de mappage LISP pour un point de terminaison inconnu peut prendre jusqu'à une minute, car les réponses de mappage négatives (NMR) doivent d'abord expirer.

Un hôte silencieux doit ignorer les paquets tels que les diffusions de sous-réseau s'il n'est pas programmé pour y répondre. Certains terminaux nécessitent un « paquet magique » (tel qu'un écho UDP), tandis que d'autres ne répondent qu'à un ARP de diffusion. L'hôte silencieux détermine lui-même le type de paquet qui déclenche son réveil. Parmi les options les plus courantes, une requête ARP est généralement préférée, comme expliqué dans la section Unknown Unicast Forwarding.

Transfert de monodiffusion inconnu



Transfert de monodiffusion inconnu

Lorsqu'un pool est activé pour la diffusion dirigée IP, il permet non seulement la gestion des diffusions de sous-réseau, mais également aux frontières de fabric de servir de passerelles pour le transfert du trafic de monodiffusion inconnu. Dans ce contexte, le trafic de monodiffusion inconnu fait référence à des paquets destinés à des terminaux qui ne sont pas actuellement enregistrés dans le plan de contrôle.

De la même manière qu'une passerelle réseau traditionnelle envoie une requête ARP lorsqu'elle rencontre une entrée ARP incomplète, la périphérie génère une requête ARP et l'inonde dans tous les noeuds de fabric. Cela garantit que l'hôte silencieux reçoit la requête, se réveille et envoie une réponse ARP, se réenregistrant ainsi dans le plan de contrôle.

Cette fonctionnalité est possible, car le VLAN de point d'extrémité (1062) est configuré à la fois en tant qu'interface SVI et en tant qu'instance L2LISP sur la périphérie du fabric. Lorsque l'option « flood arp-nd » est activée dans l'ID de couche 2, le périphérique peut inonder les requêtes ARP générées par l'interface SVI chaque fois qu'un trafic est dirigé vers un EID LISP inconnu, ce qui garantit que les hôtes silencieux reçoivent la requête ARP et ont la possibilité de répondre et de mettre à jour leur inscription dans le plan de contrôle.

<#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
```

Lorsque la frontière de fabric reçoit un paquet destiné à 172.16.56.12 sur SVI 3002, qui fait partie du terminal VN/VRF, elle tente une résolution LISP, puisque la sortie CEF est définie sur « glean » (ce qui signifie que le périphérique tente de résoudre la contiguïté de destination à l'aide du protocole de couche aval). Ce processus déclenche simultanément une requête de mappage LISP et une résolution ARP pour l'hôte non enregistré (silencieux).

<#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

Une entrée ARP incomplète est créée, invitant la périphérie à envoyer une requête ARP au point d'extrémité inconnu 172.16.56.12. Cette requête ARP, en tant que paquet de diffusion, est transmise en aval à l'aide de l'inondation de couche 2 et de la fonctionnalité d'inondation ARP-ND.

Pour vérifier que l'inondation de couche 2 est opérationnelle, surveillez les compteurs MFIB pour le S, G local de la frontière.

<#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

Le paquet ARP diffusé atteint l'hôte silencieux, le réveille et demande une réponse ARP. Cette réponse met à jour la table de suivi des périphériques (SISF) sur la périphérie du fabric et crée une entrée de base de données LISP. Par conséquent, Fabric Edge lance un enregistrement sur le plan de contrôle.

<#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
```

Une fois le point d'extrémité réenregistré dans le suivi des périphériques, il est importé dans la base de données LISP du noeud Périphérie, puis enregistré dans le plan de contrôle.

Pour les déploiements LISP Pub-Sub, le plan de contrôle publie les informations de point de terminaison nouvellement enregistrées sur Borders, créant instantanément une entrée de cache de mappage LISP pour transférer le trafic vers le noeud de périphérie approprié.

<#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)
```

Pour les déploiements LISP/BGP (SDA 1.0), si le déploiement est distribué (non colocalisé), la mise à jour du cache de mappage LISP pour un point de terminaison inconnu peut prendre jusqu'à une minute, car les réponses de mappage négatives (NMR) doivent d'abord expirer.

Conseil : La frontière ne résout jamais le protocole ARP pour l'hôte silencieux ; seul l'enregistrement du terminal est requis. Lorsque l'hôte silencieux répond, le paquet ARP est envoyé en monodiffusion de couche 2, de sorte qu'il n'est pas diffusé vers la périphérie. Par conséquent, ne vous attendez pas à voir une entrée ARP ou une entrée de suivi de périphérique sur la frontière.

Activation de Wake-on-LAN dans les modèles d'authentification

Lorsque l'option Aucune authentification est activée pour les utilisateurs du fabric, les paquets inondés provenant des hôtes silencieux d'accès en limite sont inondés tant que le port fait partie du VLAN où l'inondation est activée ; cependant, avec l'authentification fermée (en particulier), deux facteurs principaux deviennent importants.

Attribution manuelle de VLAN pour l'hôte avant authentification

Si aucun VLAN n'est attribué, le port ne reçoit pas les paquets diffusés depuis son VLAN désigné. Lorsqu'un VLAN est censé être attribué par RADIUS, cela crée un « poulet ou l'oeuf ? » dilemme : le paquet diffusé ne peut pas être transféré à un autre VLAN (communément appelé « saut de VLAN ») pour déclencher l'authentification de l'utilisateur et obtenir une affectation de VLAN de RADIUS.

Lors de la configuration du port dans Host-Onboarding, si le périphérique est identifié comme « silencieux », attribuez manuellement le VLAN à l'aide du menu déroulant pour les pools de DONNÉES.

Le problème des hôtes silencieux qui ne peuvent pas s'authentifier avant l'attribution de VLAN n'est pas unique à SD-Access ; il s'agit d'un défi de conception courant que l'on retrouve dans tout réseau sécurisé traditionnel.

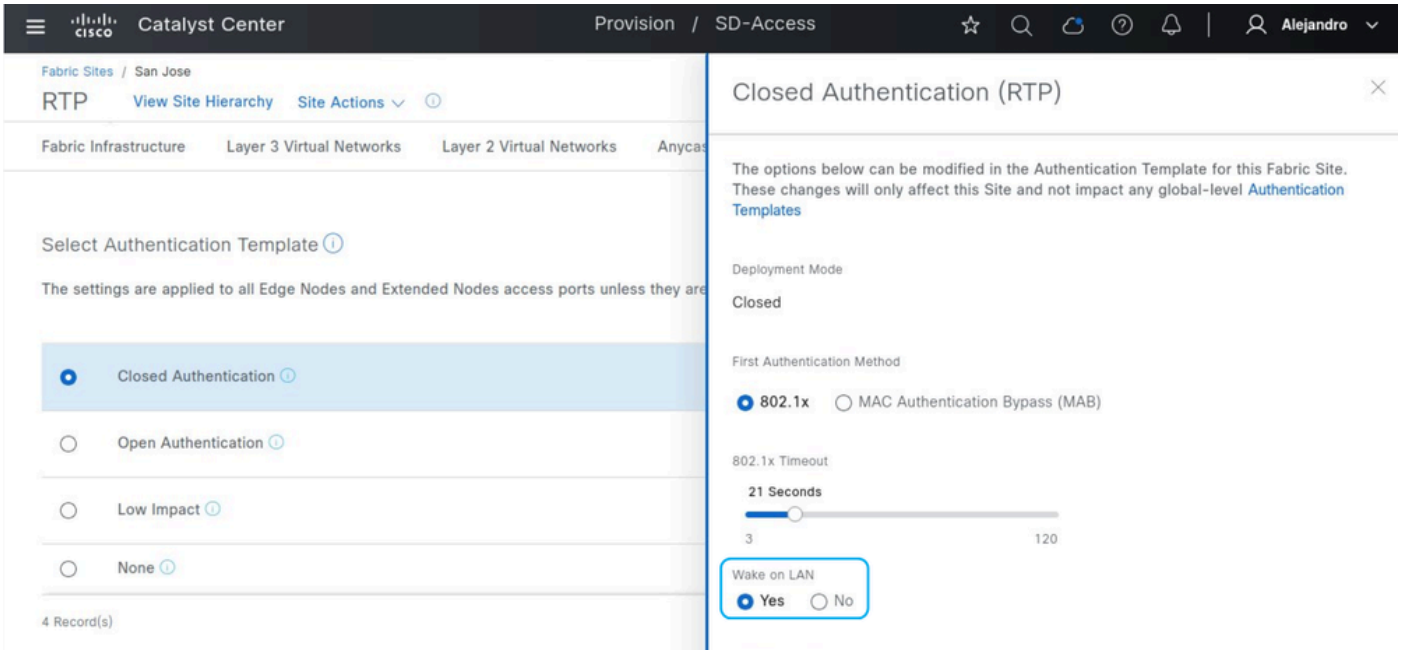
<#root>

```
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
```

Direction De Contrôle D'Accès

Par défaut, si Wake-on-LAN n'est pas activé dans les paramètres du modèle d'authentification dans Host-Onboarding, les modèles d'authentification utilisent « access-session control-direction both ». Cette configuration entraîne l'abandon par le port des paquets entrants et des paquets qui seraient transférés hors du port. Lorsque Wake-on-LAN est activé, le paramètre devient « access-session control-direction in », ce qui limite uniquement le trafic entrant. Cet ajustement permet aux paquets d'atteindre et de réveiller l'hôte silencieux, ce qui lui permet de lancer l'authentification MAB.



Wake on LAN

Sans 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
```

Avant l'authentification du point d'extrémité, l'interface qui lui est attribuée n'est pas répertoriée comme étant activée pour la propagation dans les états Spanning Tree.

<#root>

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



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

Avec Wake-on-LAN activé :

<#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
```

Même avant l'authentification, le port est activé pour le trafic de sortie, ce qui permet aux paquets d'atteindre et de réveiller l'hôte silencieux.

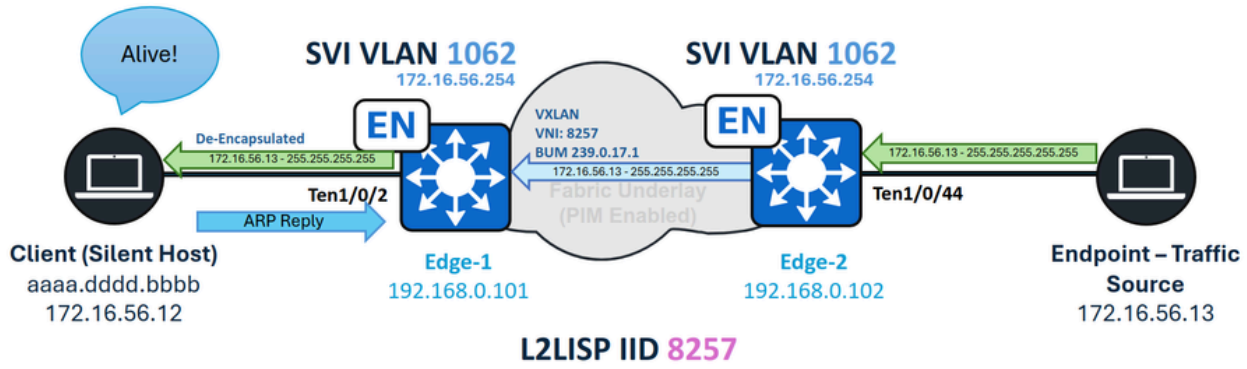
<#root>

```
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
```

Scénarios de remplacement

Noeuds de périphérie et même VLAN - Inondation de couche 2

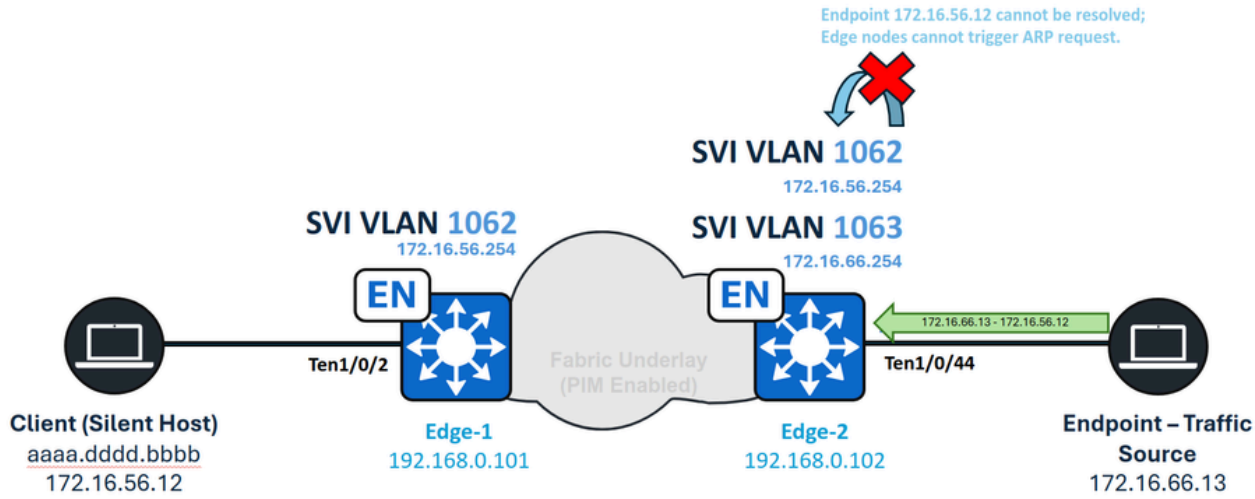
Si l'objectif est de réveiller un hôte silencieux à partir d'un périphérique au sein du fabric sur le même VLAN que l'hôte, la fonctionnalité IP Directed Broadcast n'est pas requise. À la place, l'activation de l'inondation de couche 2 (dans un pool non sans fil) est suffisante pour permettre l'échange de paquets de diffusion, de diffusions de sous-réseau ou de requêtes ARP. Pour l'authentification fermée, les exigences Wake-on-LAN sont maintenues.



Même VLAN - Gestion des hôtes silencieux

Noeuds de périphérie et VLAN différent - Monodiffusion inconnue

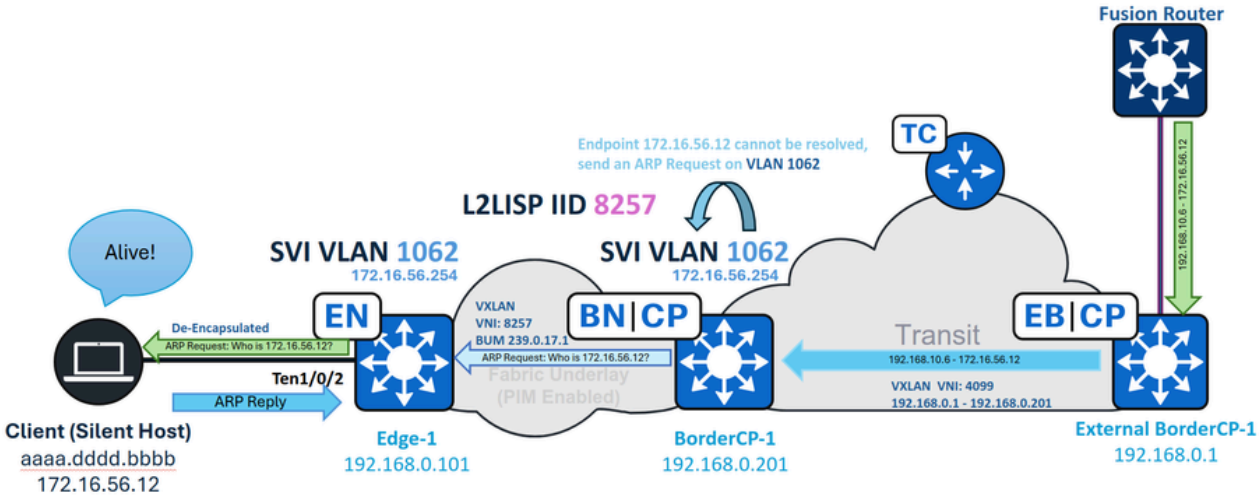
Lorsqu'un point de terminaison à l'intérieur du fabric envoie du trafic de monodiffusion à un hôte silencieux connecté à un noeud Périphérie du fabric, le chemin de transfert de monodiffusion inconnu n'est pas disponible. Contrairement aux frontières de fabric, les noeuds de périphérie de fabric ont des frontières définies en tant que proxy LISP-ETR, qui activent automatiquement une fonction de transfert appelée « Signal & Forward » lorsqu'un point d'extrémité inconnu est détecté. La périphérie du fabric doit déclencher la requête ARP requise lors de la première tentative de résolution de l'adresse. Cependant, une fois que LISP identifie le point d'extrémité comme un EID inconnu, les paquets suivants ne déclenchent pas de requêtes ARP supplémentaires. Ce scénario est considéré comme non pris en charge.



Unknown Unicast Inter-VLAN

SD-Access Transit - Monodiffusion inconnue

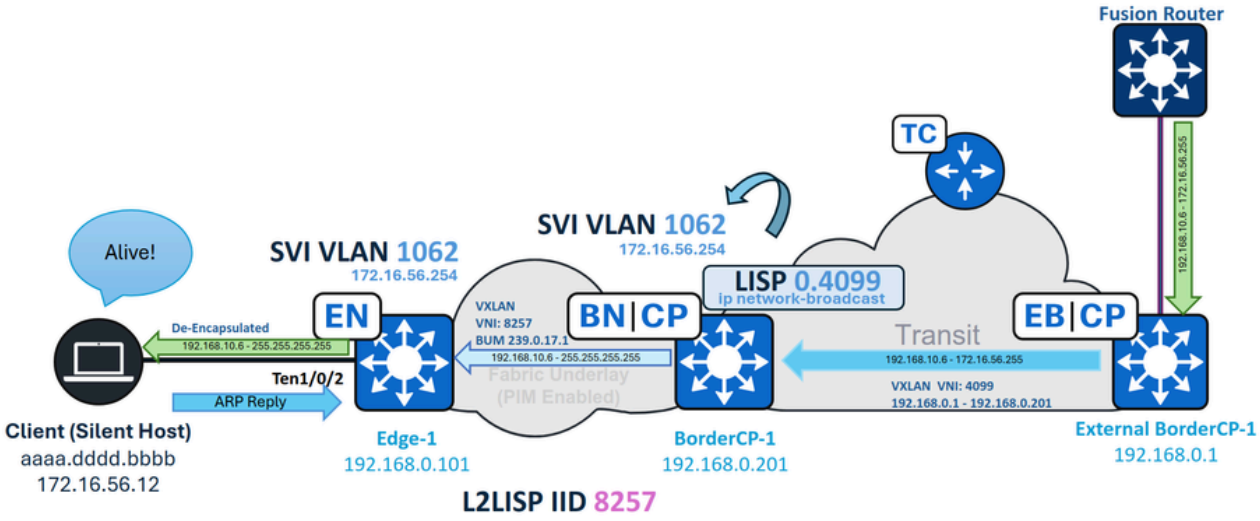
Dans le cas de SD-Access Transit, le trafic de monodiffusion inconnu est pris en charge de manière native sans aucune exigence particulière. Le trafic provenant d'une frontière distante est acheminé via le réseau de transit SD-Access, les diffusions de sous-réseau étant traitées comme du trafic routé normal. Lorsque le trafic atteint la frontière du site local, des opérations standard sont effectuées, y compris le glanage du trafic, l'inondation des requêtes ARP et la résolution LISP.



SD-Access Transit Unknown Unicast

SD-Access Transit - Diffusion dirigée IP

Lorsque SD-Access Transit est utilisé, la périphérie du site local reçoit la diffusion dirigée IP sur la sous-interface LISP du VLAN (par exemple, l'interface 4099), plutôt que sur une interface SVI. Pour vous assurer que la diffusion est acceptée et convertie en diffusion de sous-réseau par la fonctionnalité IP Directed Broadcast, vous devez configurer manuellement le paramètre « ip network-broadcast » sur la sous-interface LISP.



SD-Access Transit IPDB

À la frontièreCP-1 (frontière du site local) :

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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.