使用IP定向廣播功能配置SD-Access靜默主機

目錄

簡介

本文檔介紹如何在SD-Access中管理無聲主機，使用L2泛洪和IP定向廣播解決連線難題。

說明

大多數終端及其網路介面會定期傳輸流量，尤其是與控制相關的消息，如ARP或DHCP。但是，某些終端僅在出現提示時響應，而不是定期傳送資料包。這些裝置僅按需傳送控制資料包。在網路中，此類終端通常稱為靜默主機。在SD-Access上下文中，靜默主機必須停止所有流量或通過阻止控制平面資料包來限制其通訊。

在SDA交換矩陣中，廣播會在每個邊緣節點被抑制，或使用L2泛洪轉發到所有邊緣 — 此過程通常僅限於Edge節點和L2邊界。將廣播轉發到VLAN上的每個埠會模仿傳統第2層網路的行為，從而顯著幫助靜默主機保持活動狀態。但是，管理交換矩陣環境中的靜默主機帶來了挑戰，因為缺乏常規

通訊可能會中斷身份驗證機制、控制平面註冊和轉發。

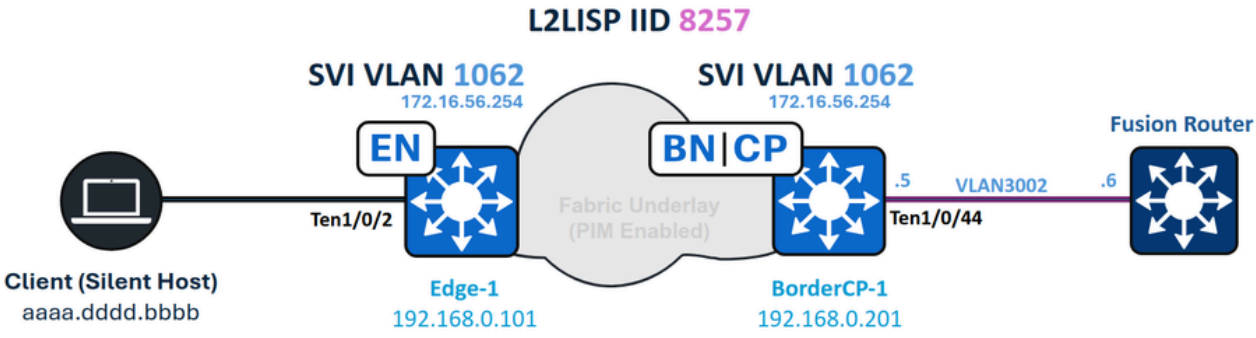
啟用L2泛洪只能解決部分問題。靜默主機只有在另一台裝置生成廣播資料包時，才能從交換矩陣內的同一VLAN或從交換矩陣邊界接收廣播資料包。IP定向廣播是指目標地址設定為子網廣播地址的IP資料包，源於該子網外部的主機。此功能需要在底層提供組播支援。在交換矩陣中啟用IP定向廣播時，所有子網廣播資料包都會到達該子網內的每台主機。此功能還可以使用標準單播資料包喚醒裝置，從而有效地模擬傳統網路中的「未知單播」行為。

拓撲

硬體和軟體

- Catalyst 9000 系列交換器
- Catalyst中心版本2.3.7.9
- Cisco IOS® XE 17.15.03及更高版本(Border/CP & Edge)

拓撲：



網路圖表

需求

思科建議您瞭解以下主題：

- 網際網路通訊協定(IP)轉送
- Locator/ID Separation Protocol(LISP)

- 通訊協定無關多點傳送(PIM)
- SD-Access中的第2層泛洪

需求

- 此功能需要Cisco Catalyst Center 1.3或更高版本
- Cisco IOS XE 17.3和Cisco DNA Advantage許可證*
- 對於ASR和ISR邊界，需要Cisco IOS XE 17.3.1或更高版本
- 不支援Catalyst 3000、4000、6000系列交換機或Nexus 7000

⚠ 注意：啟用IP定向廣播功能會自動啟用L2泛洪。啟用此功能之前，請確保襯底中的組播功能正常運行。

可以在建立IP池後啟用或禁用IP定向廣播，類似於管理無線池或L2泛洪設定。

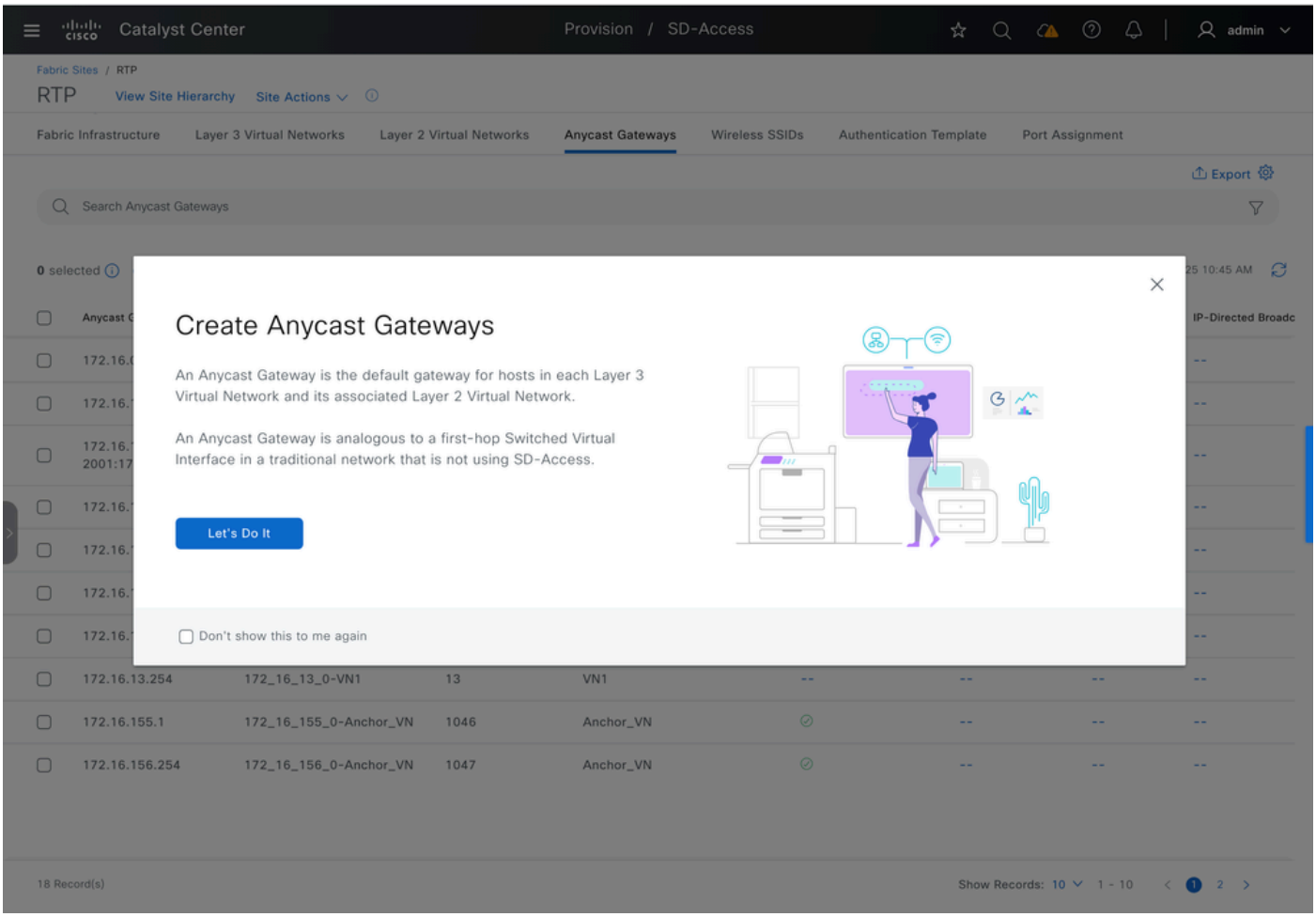
Catalyst Center配置

啟用IP定向廣播後，Catalyst Center會啟動交換矩陣範圍的調配任務。所有邊緣節點、L2邊界和具有L3切換的邊界都包含在此調配流程中。

在UI中觸發IP定向廣播工作流程：

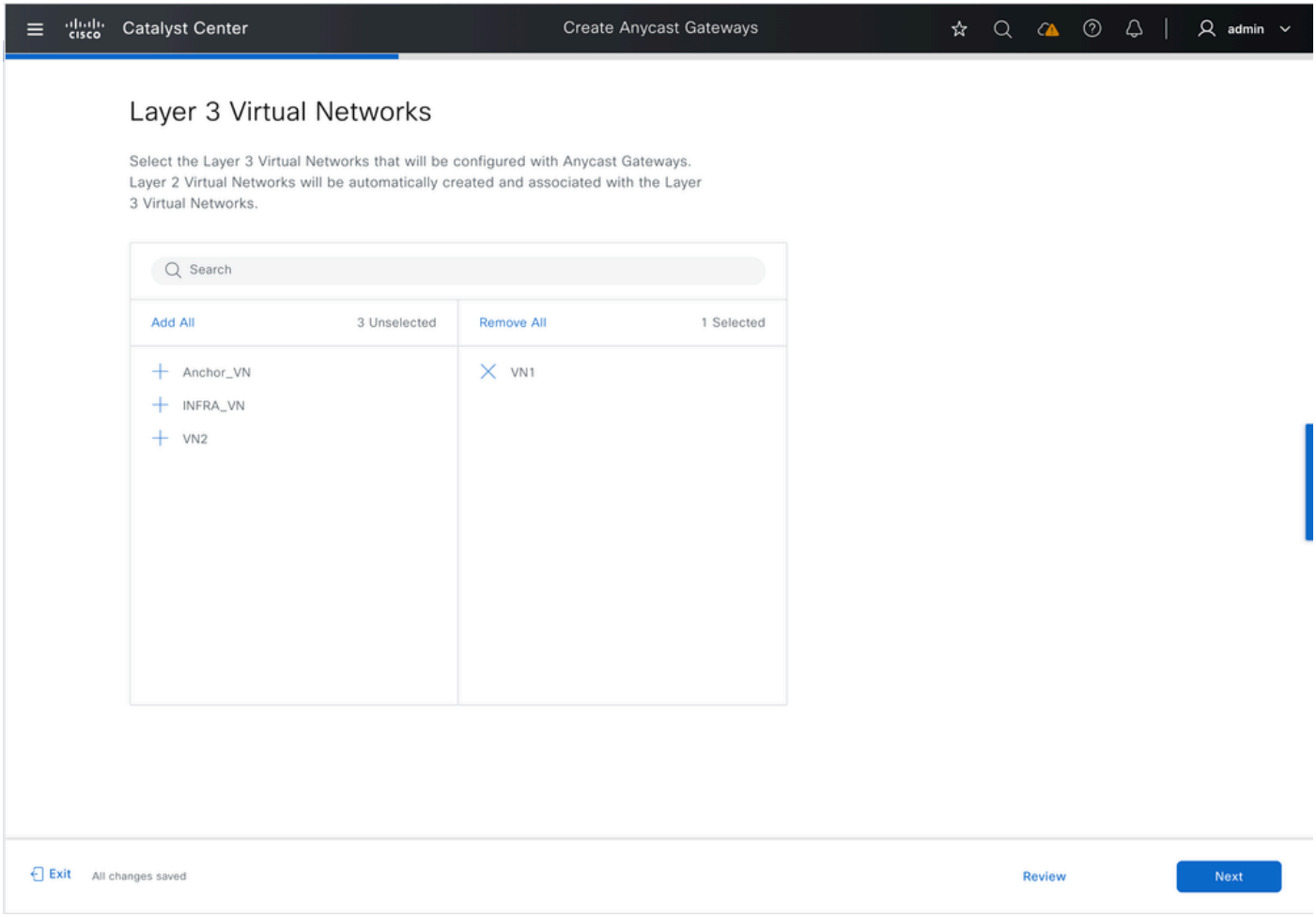
1. 轉到Provision。
2. 選擇交換矩陣站點。
3. 選擇所需站點。
4. 導航到任播網關。

您可以在此處配置IP定向廣播所需的設定。



建立任播網關

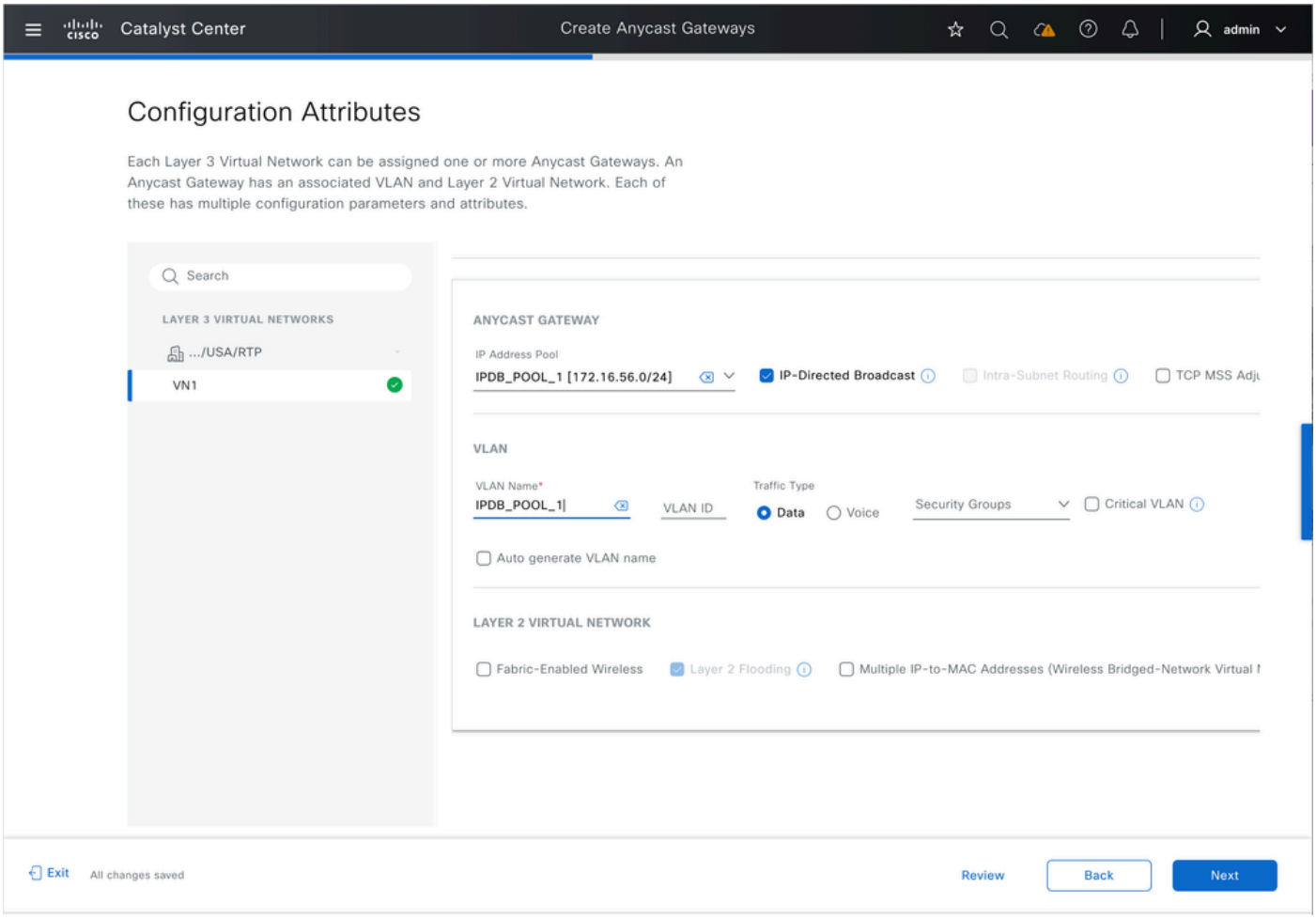
選擇所需的L3虛擬網路，然後按一下下一步繼續。



選擇L3虛擬網路

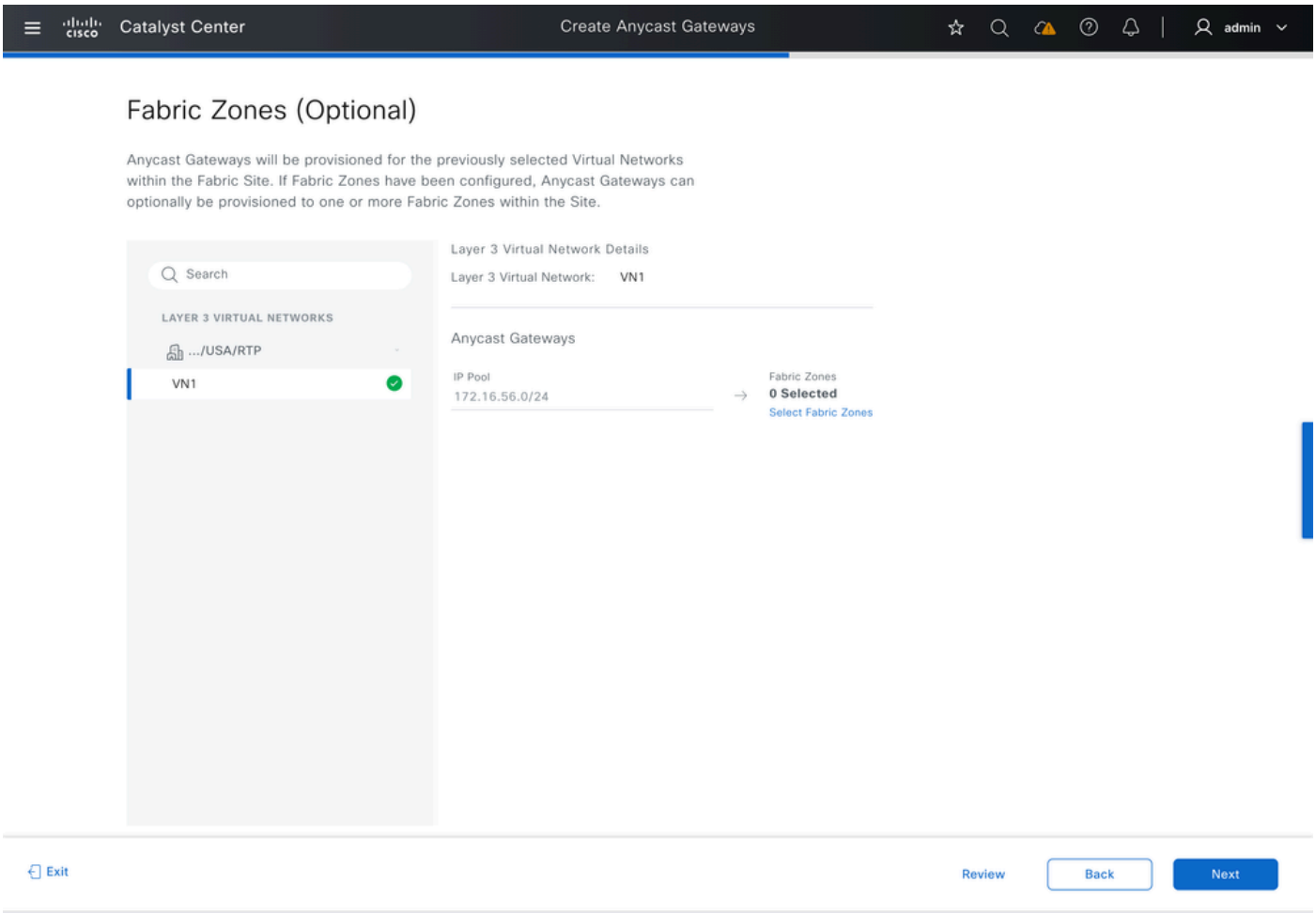
選擇IP池，啟用IP定向廣播，然後輸入VLAN名稱。

提示：啟用IP定向廣播會自動啟用L2泛洪。



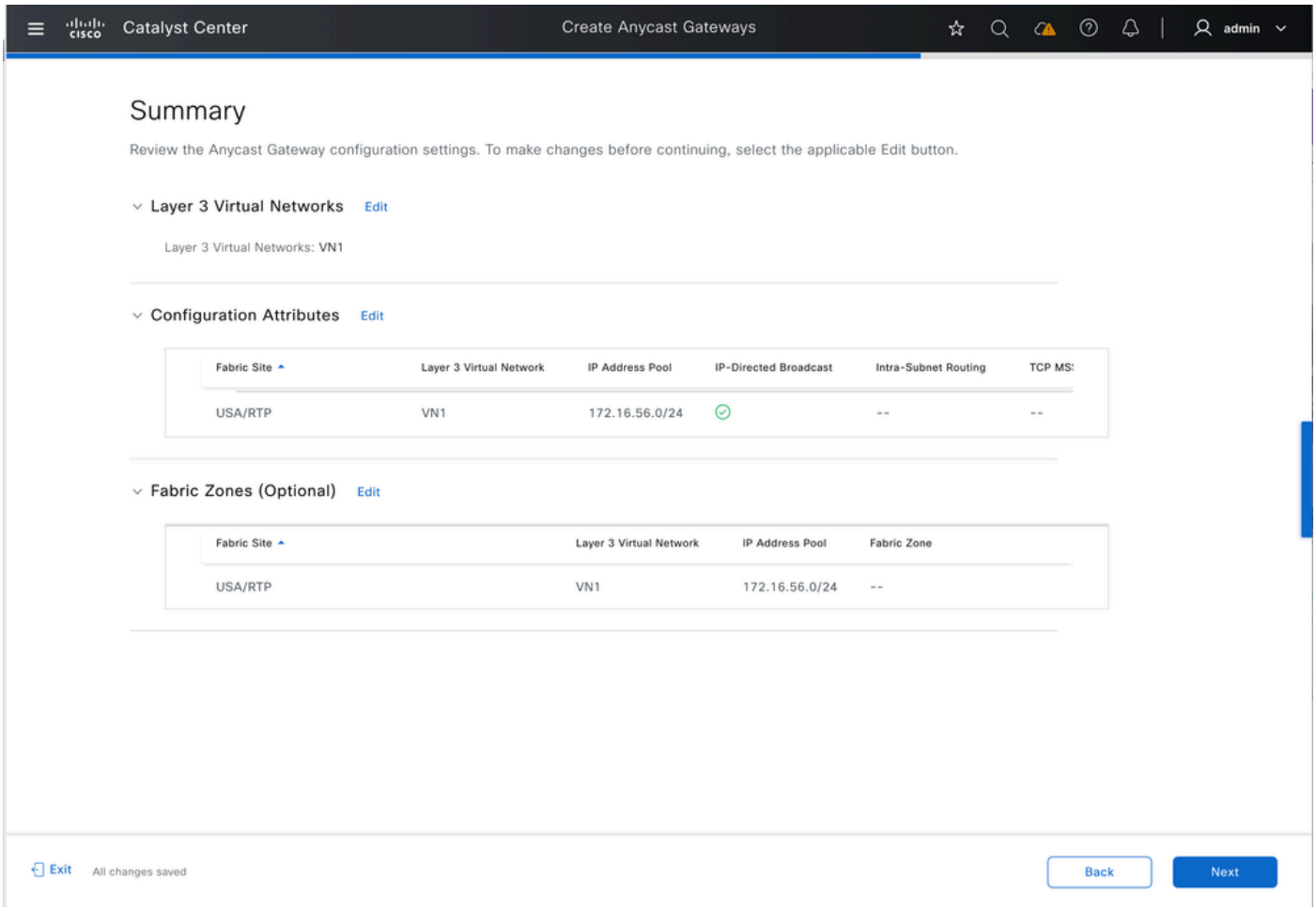
啟用IP定向廣播

如果Fabric Zones存在，則可以選擇將Anycast Gateways調配到站點內的一個或多個交換矩陣區域。



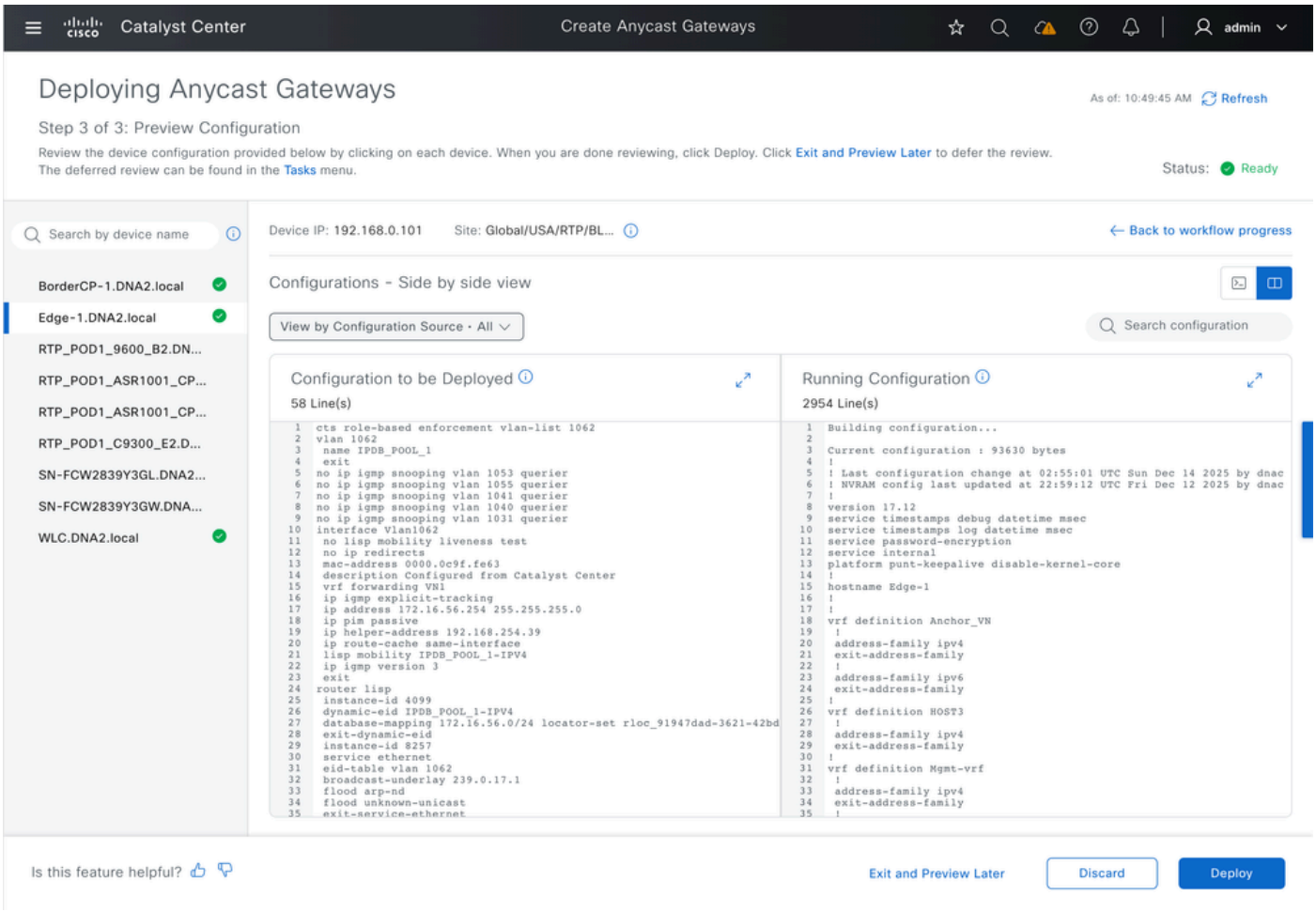
選擇交換矩陣區域

在繼續部署之前，請檢視已配置設定的摘要以確認準確性。



摘要

預覽生成的配置。按一下Deploy將配置應用到交換矩陣。



配置預覽

網路裝置配置

邊界配置 — IP傳輸

配置了IP傳輸的交換矩陣邊界將其BGP對等介面設定為「ip network-broadcast」，以允許轉發IP子網廣播。交換矩陣池（終端VLAN）的任播網關IP從環回介面更改為已啟用「ip directed-broadcast」的SVI。Fabric Border需要這兩種配置才能將IP子網廣播資料包轉換為完整廣播，從而允許該過程按預期運行。

IP網路廣播和IP網路廣播配置：

<#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
```

配置的第二部分使IP定向廣播功能能夠使用ARP請求（廣播）喚醒靜默主機，這與傳統網路在處理未知單播流量時的行為相似。使用此設定，交換矩陣外部的源可以使用標準單播流量喚醒終端，而不依賴於子網廣播或LAN喚醒（「魔術資料包」）機制。

<#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
```

邊緣配置

交換矩陣邊緣節點配置與已啟用第2層泛洪的標準有線池配置匹配。「ip directed-broadcast」CLI命令不會顯示在邊緣節點上。

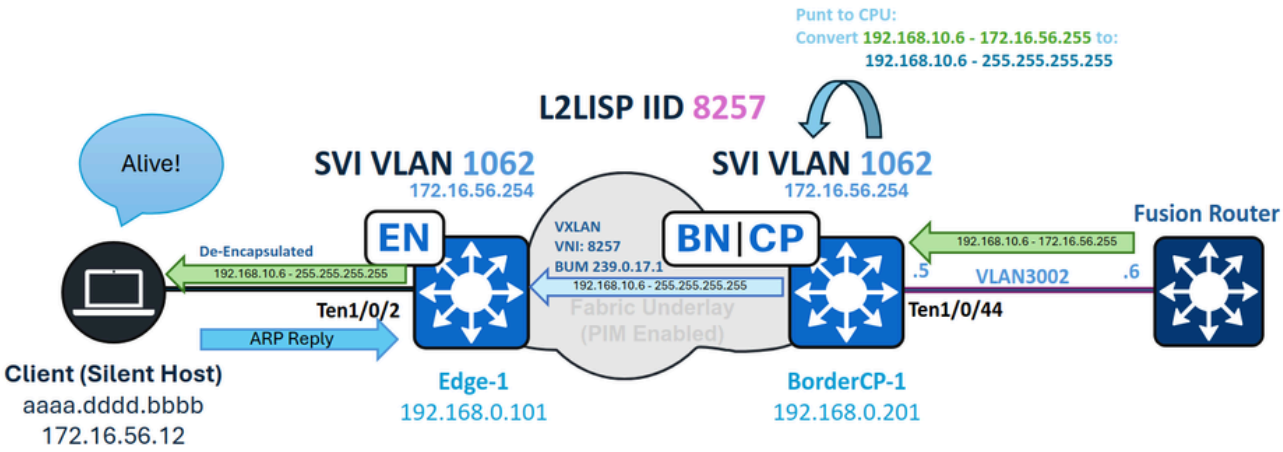
<#root>

```
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
```

IP導向廣播轉送



IPDB轉發

邊框 — 輸入CPU分支和子網廣播轉換

在本示例中，目的IP為172.16.56.255(池172.16.56.0/24的廣播地址)的IP子網廣播從外部網路路由，首先到達交換矩陣邊界。輸入第3層介面是IP傳輸SVI(VLAN 3002)。 由於在此介面上啟用了「ip network-broadcast」，因此完全廣播轉換會接受封包；如果沒有此組態，封包將會遭捨棄。

資料包到達SVI 3002，作為廣播資料包被傳送到交換機CPU。如果配置了IP網路廣播，資料包將被允許並轉換為完整廣播。

<#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
```

在CPU處理期間，VLAN 1062（目標介面）將資料包轉換為完整廣播，因為它配置了「ip directed-broadcast」。

<#root>

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

Directed broadcast forwarding is enabled

您可以使用debug ip packet指令對此事件進行疑難排解。為避免輸出過多和資源使用率高，請在運行此調試時始終應用訪問清單作為過濾器。

<#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
```

入口邊界用其環回0作為源地址，配置的BUM組作為目的地，用作BUM封裝的組播源(S)和組(G)。

在PIM控制平面上，確保組播路由的傳出介面清單中顯示一條通向交換矩陣邊緣的下行鏈路。對於資料平面，請使用show ip mfib count命令驗證邊界上的S、G條目的硬體轉發計數器是否增加。

<#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

本檔案沒有深入說明底層多點傳送樹狀目錄或第2層泛濫。在缺失、S、G狀態不完整或錯誤的情況下，網路蠕蟲的底層組播部分需要獨立的故障排除。

邊緣 — 入口廣播

在交換矩陣邊緣上，將組播上封裝在VXLAN中的傳入廣播解封裝並轉發到與VNI關聯的VLAN(8257)，在生成樹中到達處於轉發狀態的所有埠。

首先，驗證來自BUM組的邊界（以邊界環回作為源）的S、G條目是否存在，並轉發流量。使用相同的mroute和mfib命令檢查此情況，確保對應於VLAN(1062)的L2LISP子介面列為傳出介面。

<#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

解除封裝後，資料包在VLAN 1062上轉發到分配給該VLAN的所有埠。

<#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
```

端點收到廣播封包後，必須識別封包為相關並回應。因此，端點可以傳送ARP資料包，用於更新交換機上的裝置跟蹤表。

<#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
```

在裝置跟蹤中重新註冊端點後，將其匯入到邊緣節點的LISP資料庫中，然後向控制平面註冊。

對於LISP Pub-Sub部署，控制平面將新註冊的終端資訊發佈到邊界，即時建立LISP對映快取條目以將流量轉發到適當的邊緣節點。

<#root>

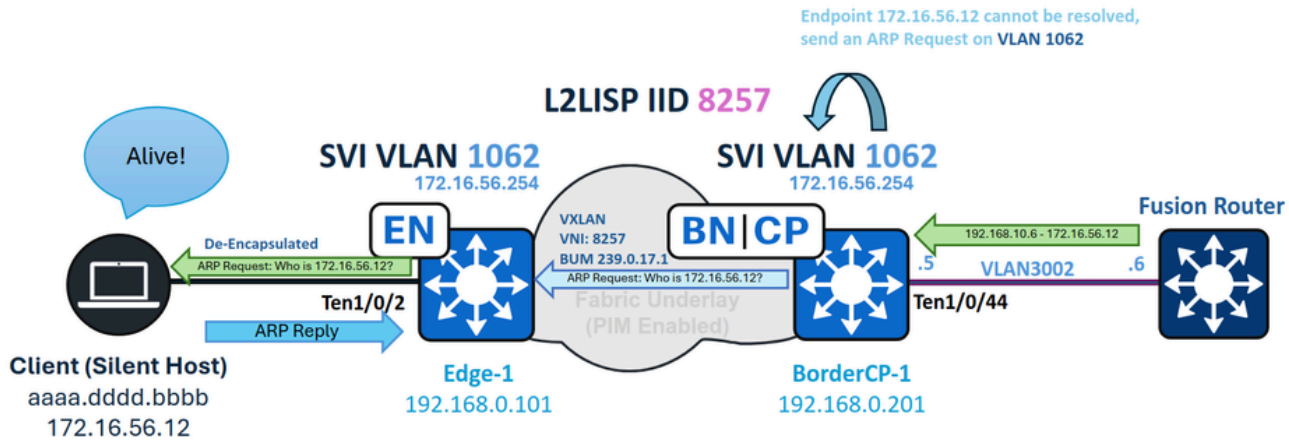
```
BorderCP-1#show lisp instance-id 4099 ipv4 map 172.16.56.12/32

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)
```

對於LISP/BGP(SDA 1.0)部署，如果部署是分散式（非配位），更新未知終端的LISP對映快取最多可能需要一分鐘，因為負對映應答(NMR)必須首先過期。

如果無聲主機沒有設定響應資料包的程式，則必須忽略這些資料包（如子網廣播）。某些端點需要「魔術資料包」（例如UDP回應），而其他端點僅對廣播ARP作出響應。靜默主機本身決定哪種型別的資料包會觸發它喚醒。在最常見的選項中，通常優先使用ARP請求，如未知單播轉發一節所述。

未知的單點傳播轉發



未知的單點傳播轉發

當為IP定向廣播啟用池時，它不僅允許處理子網廣播，還允許交換矩陣邊界充當轉發未知單播流量的網關。在此上下文中，未知的單點傳播流量是指目的地為當前未在控制平面中註冊的終端的資料包。

類似於傳統網路網關在遇到不完整的ARP條目時傳送ARP請求，邊界會生成一個ARP請求並將其泛洪到所有交換矩陣節點。這可以確保靜默主機收到請求、喚醒並傳送ARP應答，從而在控制平面中重新註冊自己。

此功能之所以可行，是因為端點VLAN(1062)在交換矩陣邊界上同時配置為SVI和L2LISP例項。在L2 IID中啟用了「flood arp-nd」後，邊界可以在有流向未知LISP EID的流量時泛洪SVI生成的ARP請求，確保無聲主機收到ARP請求並有機會響應並在控制平面中更新其註冊。

<#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
```

當交換矩陣邊界收到發往SVI 3002上172.16.56.12的資料包（屬於終端VN/VRF的一部分）時，它將嘗試LISP解析，因為CEF輸出設定為「聚集」（表示裝置嘗試使用下游層協定解析目標鄰接關係）。 此過程同時觸發未註冊（靜默）主機的LISP對映請求和ARP解析。

<#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

建立了一個不完整的ARP條目，提示邊界向未知端點172.16.56.12傳送ARP請求。此ARP請求作為廣播資料包使用第2層泛洪和泛洪ARP-ND功能向下游轉發。

要驗證第2層泛洪是否正常運行，請監控邊界本地S、G的MFIB計數器。

<#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

泛洪的ARP資料包到達靜默主機，將其喚醒並提示ARP應答。此響應更新交換矩陣邊緣上的裝置跟蹤(SISF)表並建立LISP資料庫條目。因此，交換矩陣邊緣將啟動對控制平面的註冊。

<#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

在裝置跟蹤中重新註冊端點後，將其匯入到邊緣節點的LISP資料庫中，然後向控制平面註冊。

對於LISP Pub-Sub部署，控制平面將新註冊的終端資訊發佈到邊界，即時建立LISP對映快取條目以將流量轉發到適當的邊緣節點。

<#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)
```

對於LISP/BGP(SDA 1.0)部署，如果部署是分散式（非配位），更新未知終端的LISP對映快取最多可能需要一分鐘，因為負對映應答(NMR)必須首先過期。

提示：邊界從不解析靜默主機的ARP;僅需要終端註冊。無提示主機應答時，ARP資料包作為第2層單播傳送，因此不會向邊界泛洪。因此，不要期望在邊界上看到ARP條目或裝置跟蹤條目。

在身份驗證模板中啟用LAN喚醒

當交換矩陣使用者啟用無身份驗證時，只要埠是啟用泛洪的VLAN的一部分，來自邊界處的泛洪資料包就會到達靜默主機；但是，對於封閉式身份驗證（尤其是封閉式身份驗證），兩個主要因素變得很重要。

身份驗證前為主機手動分配VLAN

如果沒有指定VLAN，則埠不會從其指定的VLAN接收泛洪資料包。當VLAN應該由RADIUS分配時，會建立「Chicken or the Egg？」 困境：無法將泛洪資料包轉發到其他VLAN（通常稱為VLAN跳躍），以觸發使用者身份驗證並從RADIUS獲取VLAN分配。

在主機自註冊中配置埠時，如果裝置標識為「靜默」，則使用資料池的下拉選單手動分配VLAN。

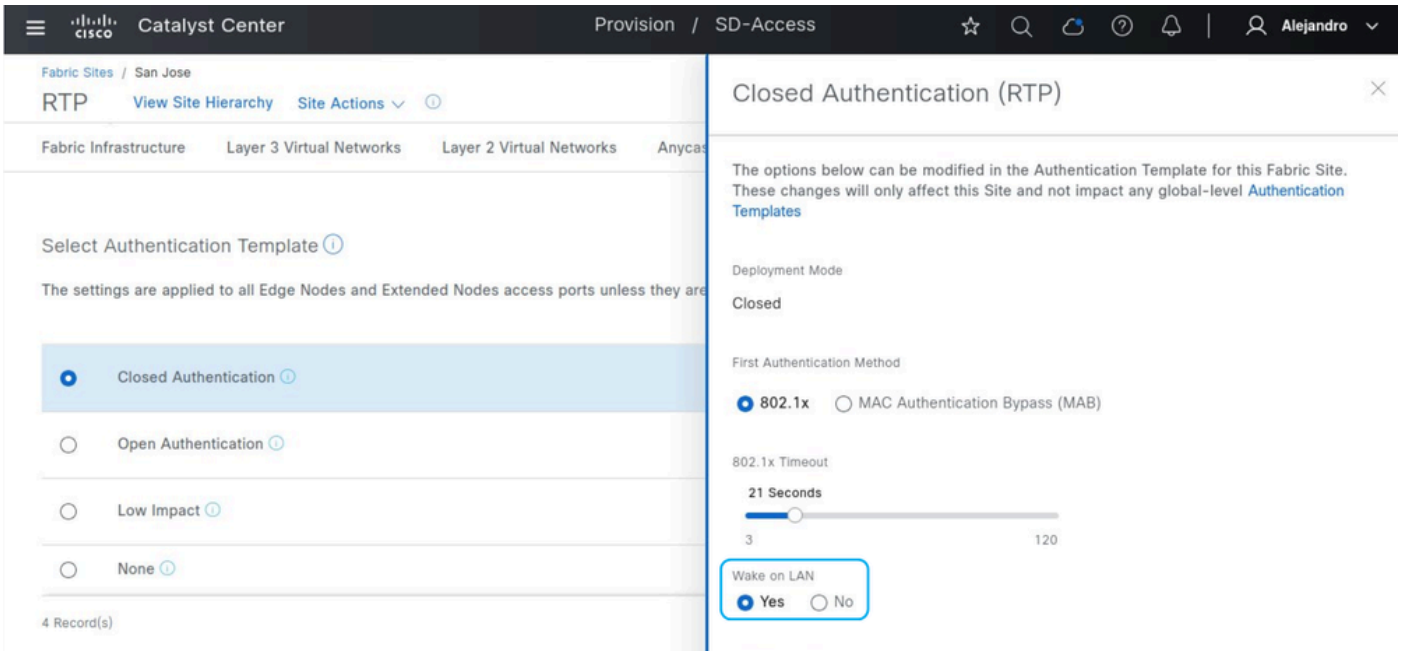
在VLAN分配之前，靜默主機無法進行身份驗證的問題不是SD-Access獨有的；這是任何傳統安全網路中都存在的常見設計挑戰。

<#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
```

存取控制方向

預設情況下，如果在主機自註冊中的身份驗證模板設定中未啟用LAN喚醒，則身份驗證模板將使用「access-session control-direction both」。 此組態會促使連線埠捨棄傳入封包和將轉送出連線埠的封包。啟用LAN喚醒後，設定將更改為「access-session control-direction in」，僅限制輸入流量。此調整允許資料包到達並喚醒靜默主機，使其能夠啟動MAB身份驗證。



LAN喚醒

不使用LAN喚醒：

<#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
```

在終端進行身份驗證之前，分配給它的介面在生成樹狀態中未列為已啟用泛洪。

<#root>

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


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

啟用LAN喚醒後：

<#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
```

甚至在驗證之前，連線埠就會啟用輸出流量，允許封包到達和喚醒沈默主機。

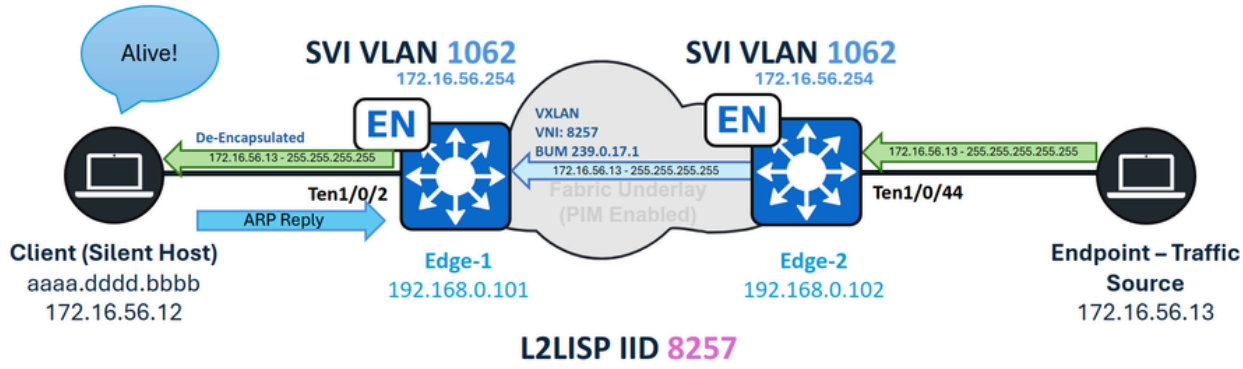
<#root>

```
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
```

替代方案

邊緣節點和相同VLAN — 第2層泛洪

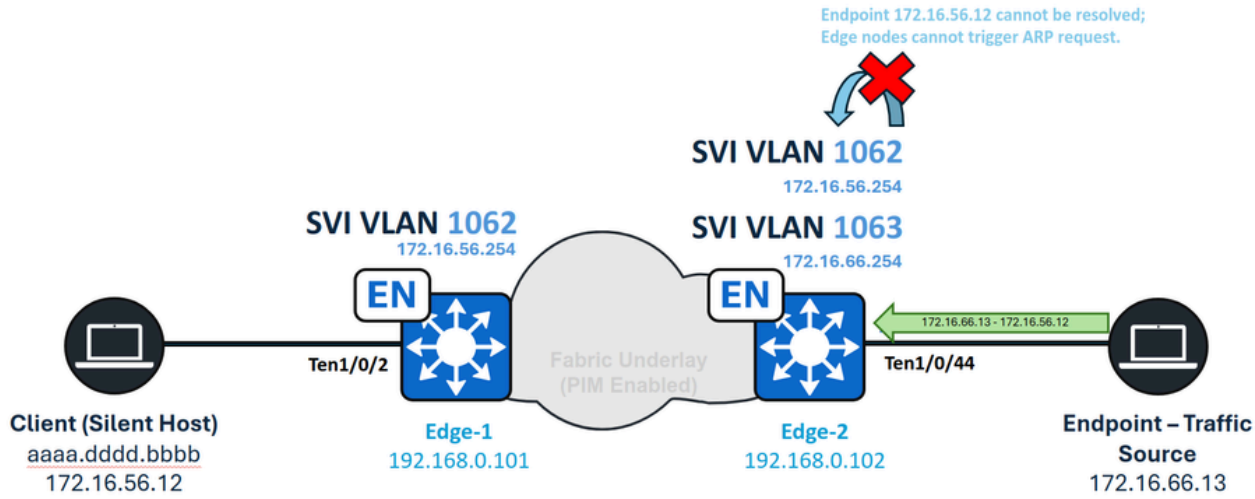
如果目標是從與主機位於同一VLAN上的交換矩陣內的裝置喚醒靜默主機，則不需要IP定向廣播功能。相反，啟用第2層泛洪（在非無線池中）足以允許交換廣播資料包、子網廣播或ARP請求。對於封閉式身份驗證，LAN喚醒要求保持不變。



相同VLAN — 無提示主機處理

邊緣節點和不同VLAN — 未知單播

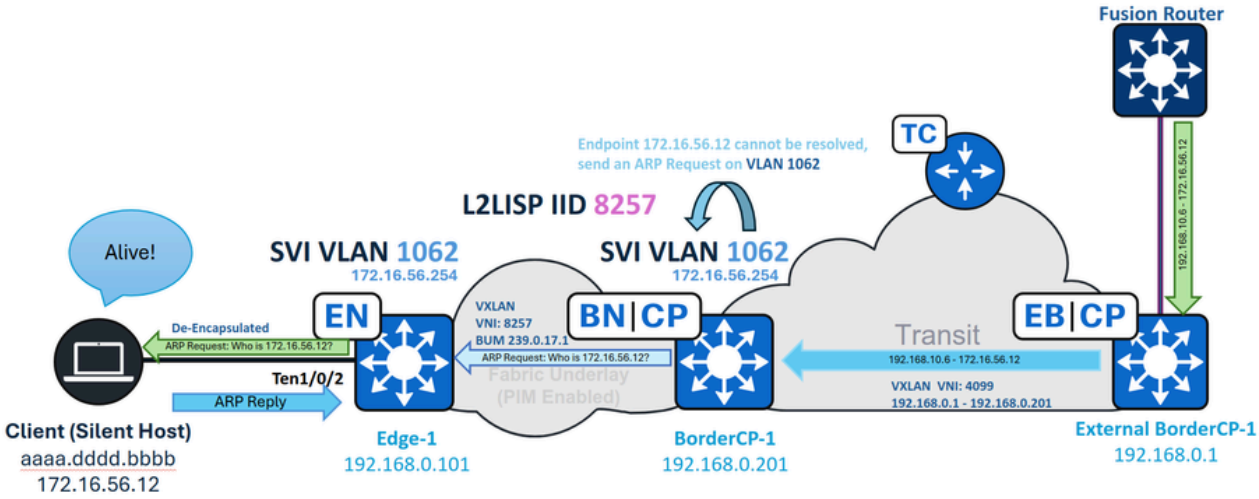
當交換矩陣內的終端將單播流量傳送到連線到交換矩陣邊緣節點的靜默主機時，未知單播轉發路徑不可用。與交換矩陣邊界不同的是，交換矩陣邊緣節點具有定義為LISP代理ETR的邊界，當檢測到未知端點時，該邊界會自動啟用稱為「訊號與轉發」的轉發功能。在第一次嘗試解析地址時，交換矩陣邊緣必須觸發所需的ARP請求。但是，一旦LISP將端點識別為未知EID，後續資料包就不會觸發其他ARP請求。此情況被視為不受支援。



未知的單點傳播VLAN間

SD-Access傳輸 — 未知的單播

在SD-Access Transit中，未知的單點傳播流量會原生受支援，沒有任何特殊要求。來自遠端邊界的流量通過SD-Access Transit網路進行路由，而子網廣播被視為常規路由流量。當流量到達本地站點邊界時，將執行標準操作，包括流量收集、ARP請求泛洪和LISP解析。

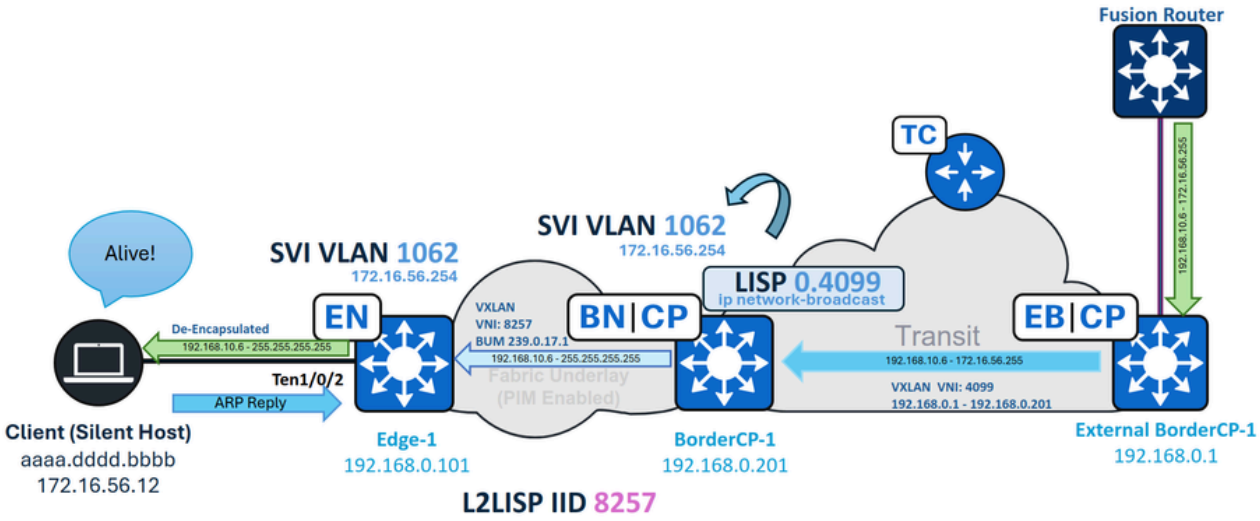


SD-Access傳輸未知單播

SD存取傳輸 — IP導向廣播

當使用SD-Access Transit時，本地站點邊界在VN的LISP子介面（例如，介面4099）上而不是SVI上接收IP定向廣播。要確保廣播被接受並通過IP定向廣播功能轉換為子網廣播，您必須在

LISP子介面上手動配置「ip network-broadcast」引數。



SD存取傳輸IPDB

在BorderCP-1（本地站點邊界）：

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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。