Configurare l'host invisibile all'utente con accesso SD con la funzionalità di trasmissione diretta IP

Sommario

Introduzione

In questo documento viene descritta la gestione degli host inattivi in SD-Access, risolvendo i problemi di connettività mediante il flooding L2 e il broadcast diretto da IP.

Descrizione

La maggior parte degli endpoint e le relative interfacce di rete trasmettono il traffico periodicamente, in particolare i messaggi relativi al controllo, ad esempio ARP o DHCP. Tuttavia, alcuni endpoint rispondono solo quando richiesto, anziché inviare pacchetti a intervalli regolari.

Questi dispositivi inviano pacchetti di controllo solo su richiesta. Nelle reti, tali endpoint sono comunemente noti come host silenziosi. Nell'ambito di SD-Access, gli host silenziosi devono interrompere tutto il traffico o limitare la loro comunicazione trattenendo i pacchetti del control plane.

Nel fabric SDA, le trasmissioni vengono soppresse in ciascun nodo Edge o inoltrate a tutti gli spigoli utilizzando il flooding L2, un processo in genere limitato ai nodi Edge e ai bordi L2. L'inoltro dei broadcast a tutte le porte di una VLAN imita il comportamento di una rete tradizionale di layer 2, che aiuta in modo significativo gli host silenziosi a rimanere attivi. Tuttavia, la gestione degli host silenziosi in un ambiente fabric presenta delle difficoltà, in quanto la mancanza di una comunicazione regolare può interrompere i meccanismi di autenticazione, le registrazioni del control plane e l'inoltro.

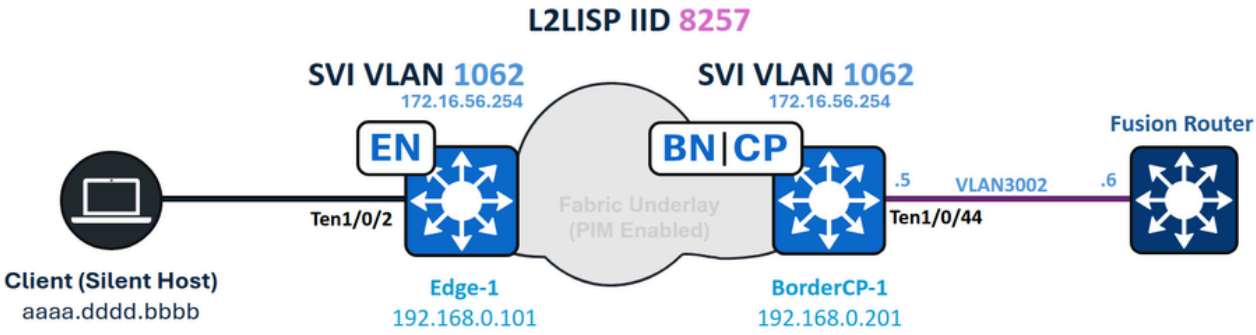
L'attivazione del flooding L2 consente di risolvere solo una parte del problema. Gli host silenziosi possono ricevere pacchetti di broadcast solo quando vengono generati da un altro dispositivo, o dalla stessa VLAN all'interno della struttura o dal bordo di un'infrastruttura. Una trasmissione diretta IP si riferisce a un pacchetto IP con un indirizzo di destinazione impostato sull'indirizzo di trasmissione di una subnet, proveniente da un host esterno a tale subnet. Questa funzionalità richiede il supporto multicast nella struttura sottostante. Quando la trasmissione diretta tramite IP è abilitata nella struttura, tutti i pacchetti di trasmissione della subnet raggiungono tutti gli host all'interno della subnet. Questa funzionalità consente inoltre di riattivare i dispositivi utilizzando pacchetti unicast standard, simulando in modo efficace il comportamento "unicast sconosciuto" delle reti tradizionali.

Topologia

Hardware e software

- Switch Catalyst serie 9000
- Catalyst Center versione 2.3.7.9
- Cisco IOS® XE 17.15.03 e versioni successive (Border/CP & Edge)

Topologia:



Esempio di rete

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Inoltro IP (Internet Protocol)
- Locator/ID Separation Protocol (LISP)
- PIM (Protocol Independent Multicast)
- Inondazione di livello 2 in SD-Access

Requisiti

- Questa funzionalità richiede Cisco Catalyst Center 1.3 o versione successiva
- Licenze Cisco IOS XE 17.3 e Cisco DNA Advantage*
- Per i bordi ASR e ISR, è richiesto Cisco IOS XE 17.3.1 o versione successiva
- gli switch Catalyst serie 3000, 4000 e 6000 o Nexus 7000 non sono supportati

---

⚠ Attenzione: L'attivazione della funzione di trasmissione diretta IP attiva automaticamente L2 Flooding. Prima di abilitare questa funzione, verificare che la funzionalità multicast nella base funzioni correttamente.

È possibile attivare o disattivare Trasmissione diretta IP dopo aver creato il pool IP, in modo analogo alla gestione dei pool wireless o delle impostazioni di L2 Flooding.

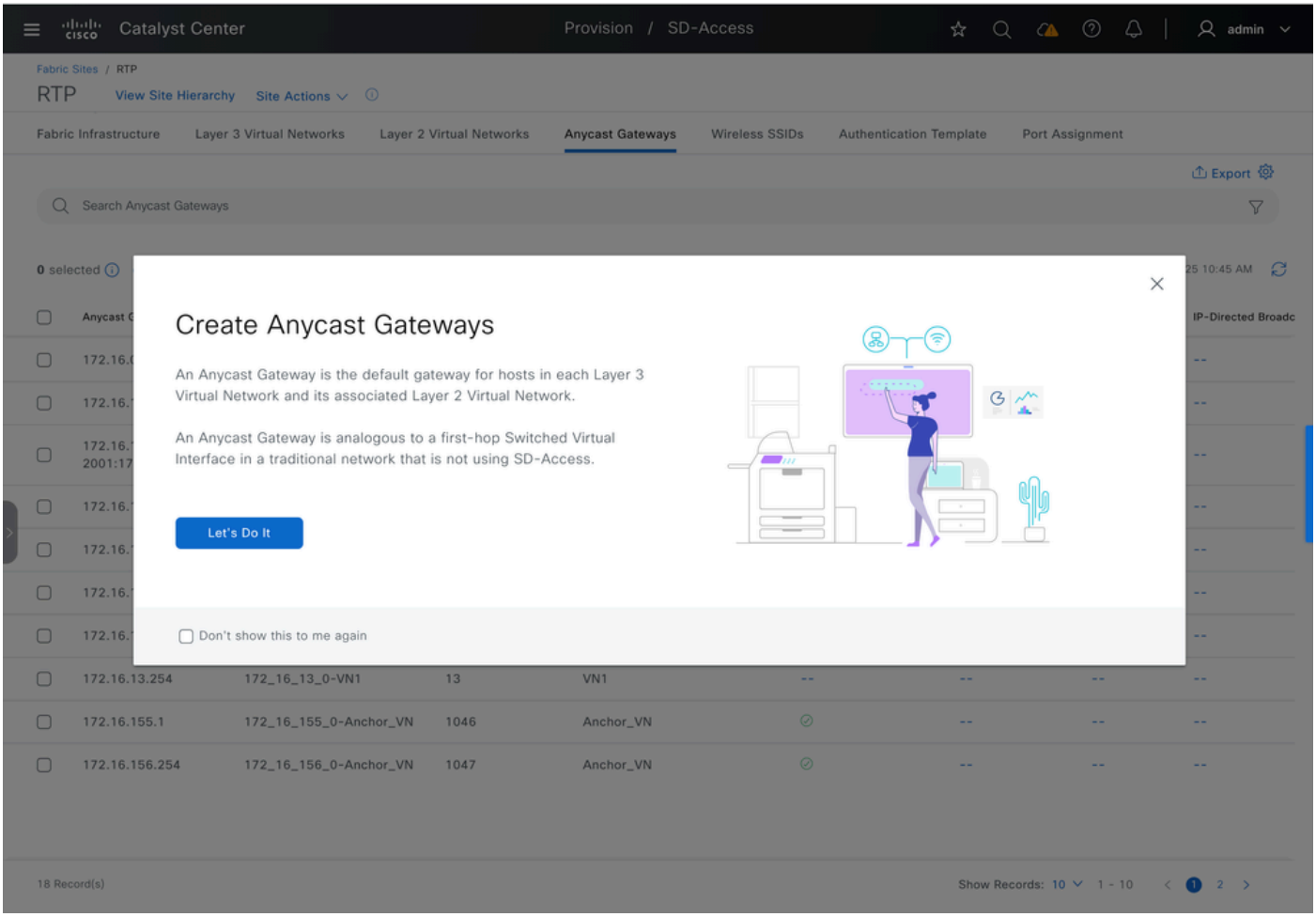
Configurazione di Catalyst Center

Quando la trasmissione diretta tramite IP è abilitata, Catalyst Center avvia un'attività di provisioning a livello di struttura. Tutti i nodi Edge, i bordi L2 e i bordi con handoff L3 sono inclusi in questo processo di provisioning.

Per attivare il flusso di lavoro Trasmissione diretta IP nell'interfaccia utente:

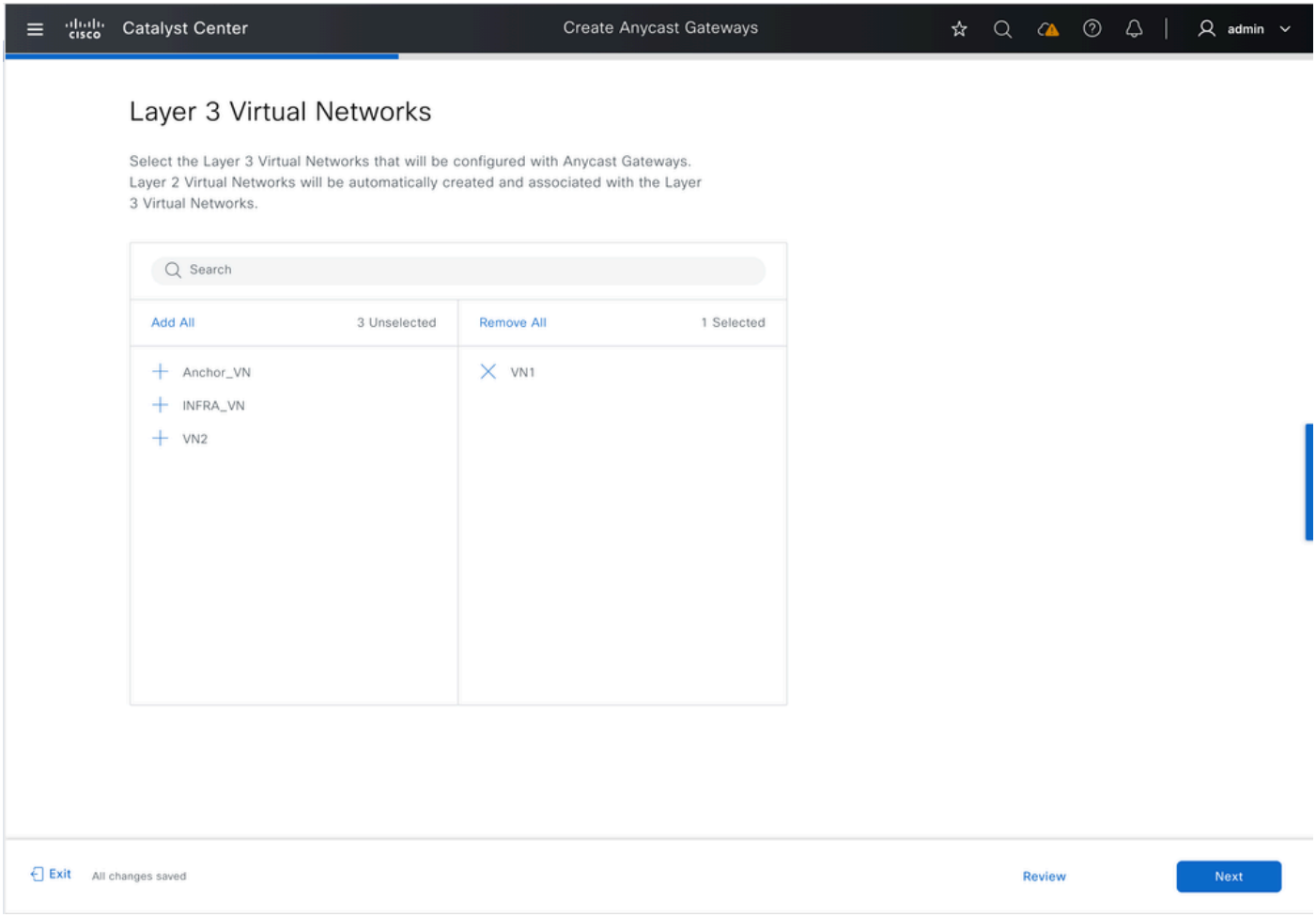
1. Passare al provisioning.
2. Selezionare Siti fabric.
3. Scegliere il sito desiderato.
4. Passare a Anycast Gateway.

Da qui è possibile configurare le impostazioni necessarie per la trasmissione diretta IP.



Creazione di gateway Anycast

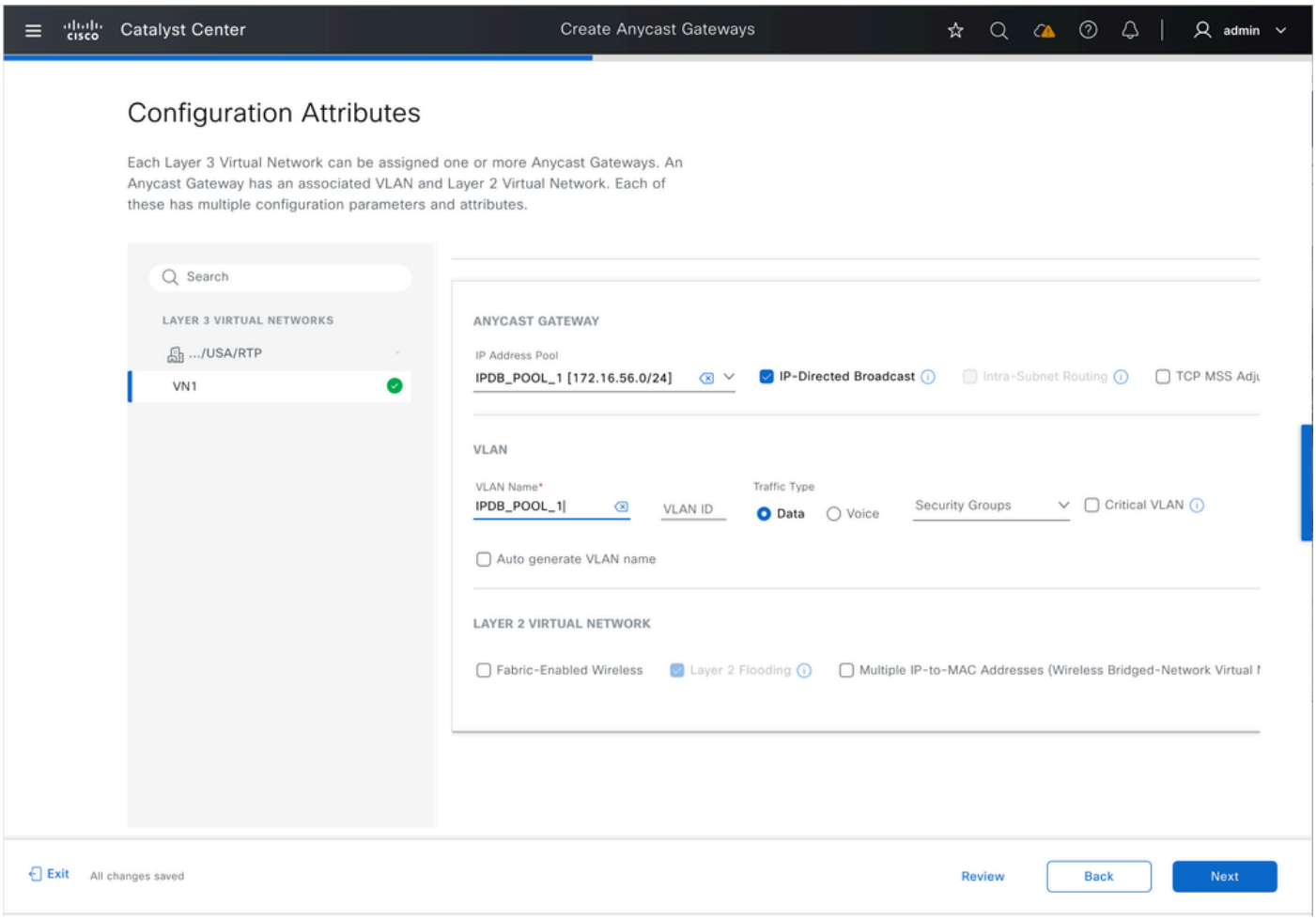
Selezionare la rete virtuale L3 desiderata, quindi fare clic su Avanti per continuare.



Seleziona reti virtuali L3

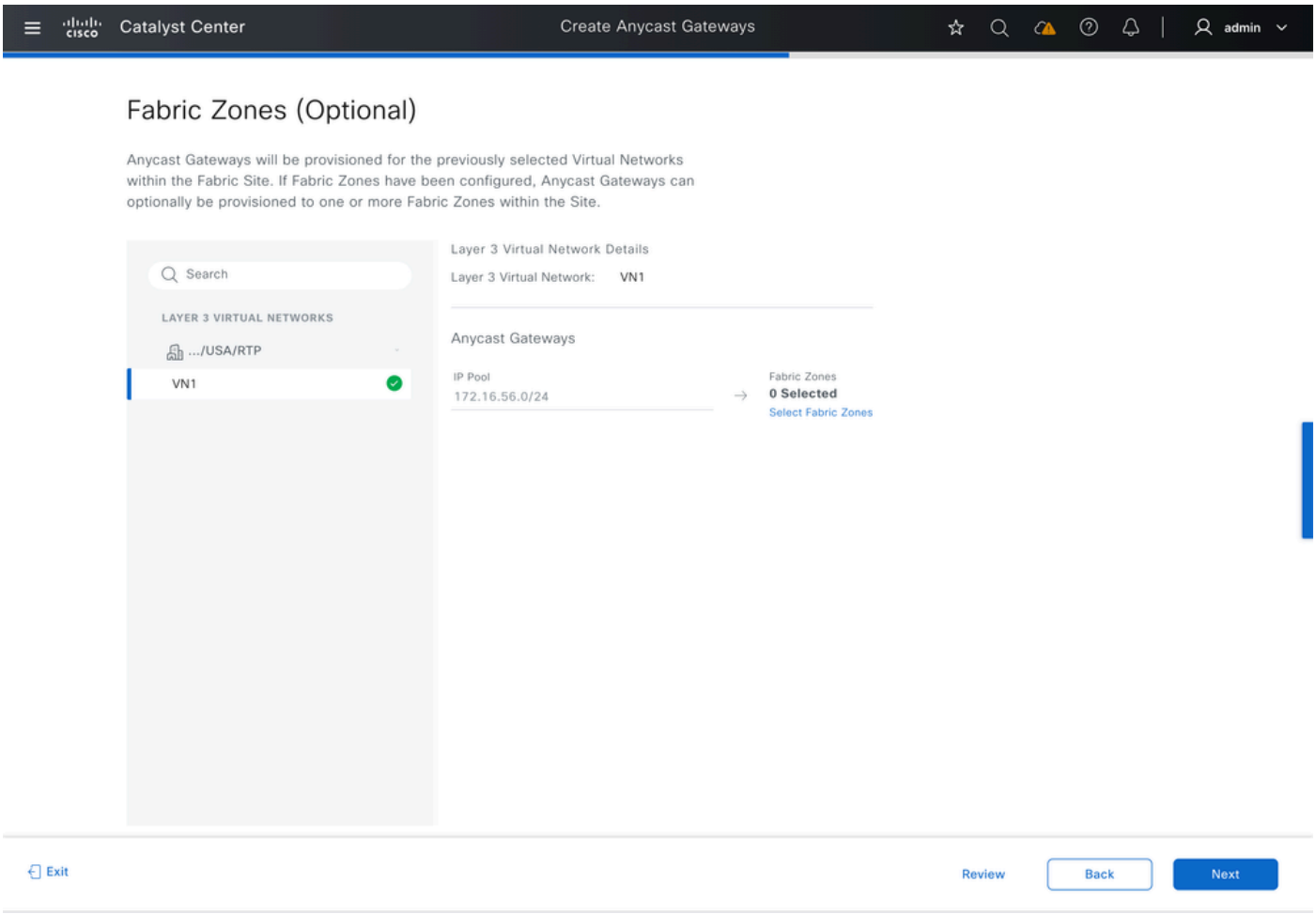
Selezionare il pool IP, abilitare la trasmissione diretta IP e immettere il nome della VLAN.

Suggerimento: L'attivazione della trasmissione diretta IP attiva automaticamente il flooding L2.



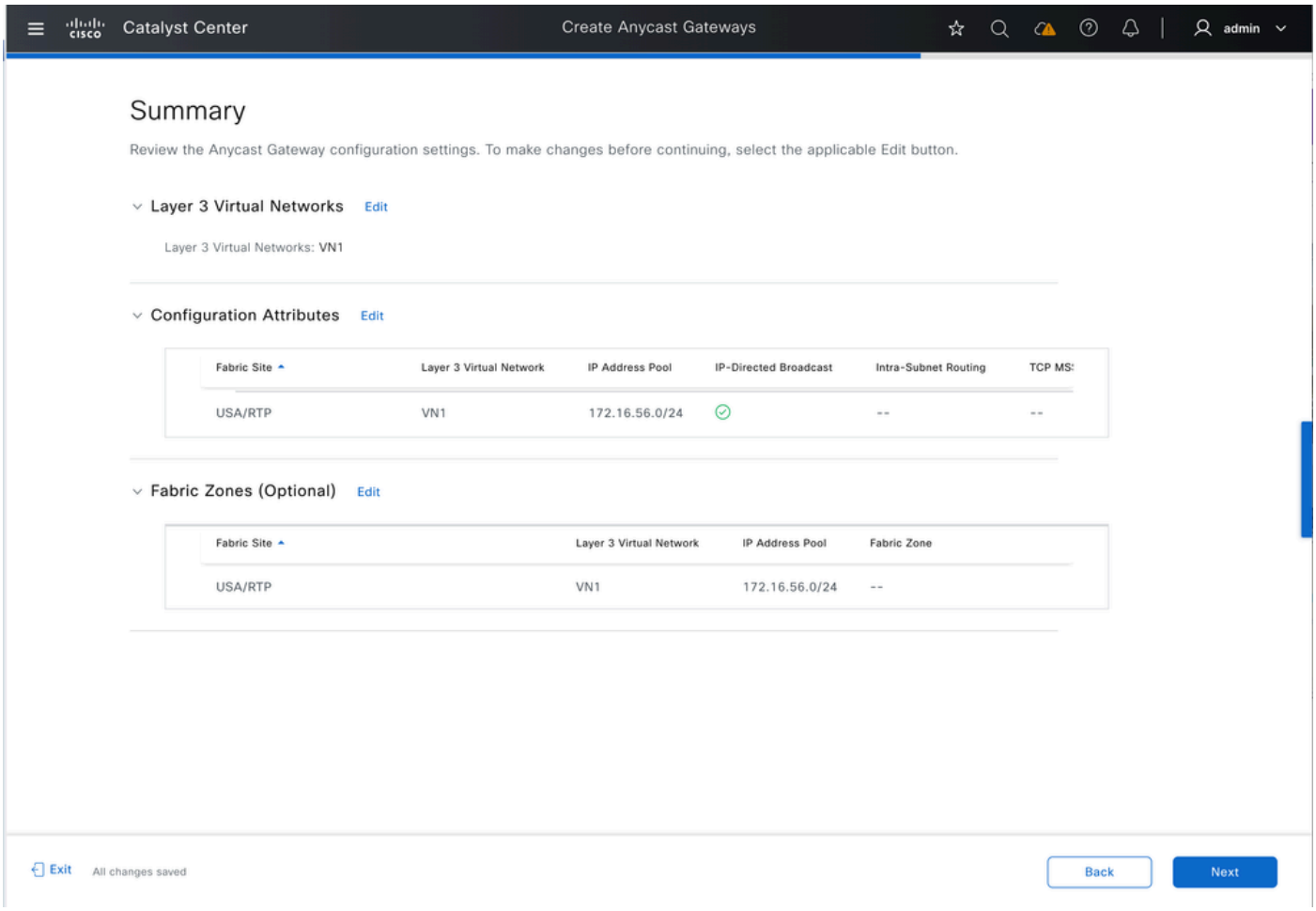
Abilita trasmissione diretta IP

Se sono presenti zone fabric, è possibile effettuare il provisioning dei gateway Anycast su una o più zone fabric all'interno del sito.



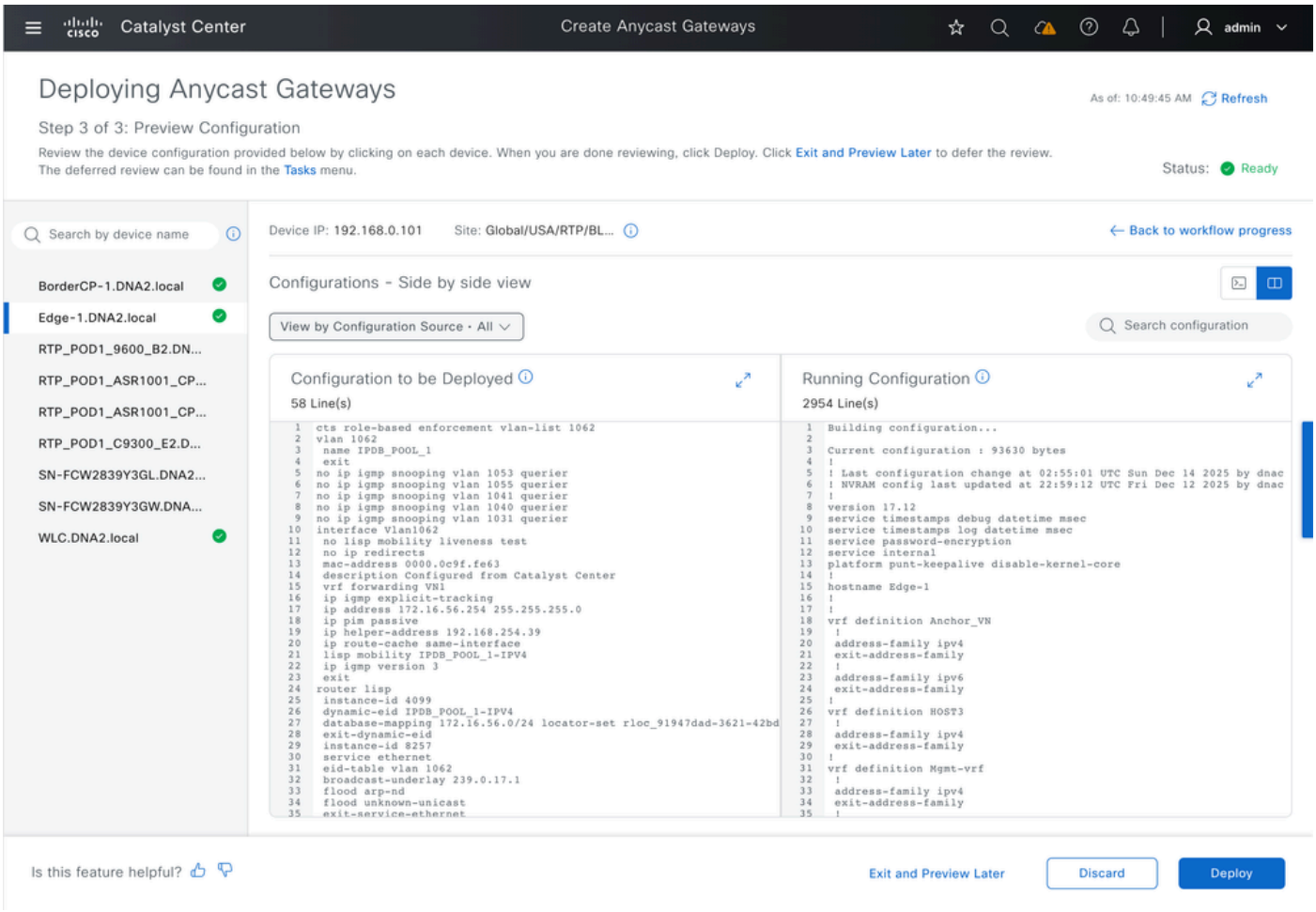
Seleziona zone fabric

Esaminare il riepilogo delle impostazioni configurate per verificare l'accuratezza prima di procedere con la distribuzione.



Riepilogo

Visualizzate in anteprima le configurazioni generate. Fare clic su Distribuisci per applicare la configurazione all'infrastruttura.



Anteprima configurazione

Configurazione dispositivo di rete

Configurazione bordo - Transito IP

Per i bordi dei fabric con transito IP configurato, le interfacce peer BGP sono impostate su "ip network-broadcast" per consentire l'inoltro di broadcast su subnet IP. L'IP del gateway Anycast per il pool di infrastrutture (VLAN endpoint) passa da un'interfaccia di loopback a una SVI, con la funzione "ip direct-broadcast" abilitata. Entrambe le configurazioni sono necessarie per il Fabric Border per convertire i pacchetti broadcast IP subnet in broadcast completi, consentendo al processo di funzionare come previsto.

Configurazione di IP Network Broadcast & IP Network Broadcast:

<#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
```

Questa seconda parte della configurazione consente alla funzionalità di trasmissione diretta IP di riattivare gli host in background utilizzando una richiesta ARP (broadcast), simile al comportamento delle reti tradizionali nella gestione del traffico unicast sconosciuto. Con questa configurazione, le origini esterne alla struttura possono riattivare gli endpoint utilizzando il traffico unicast standard, senza dipendere dai broadcast della subnet o dai meccanismi Wake-on-LAN ("pacchetto magico").

<#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
```

Configurazione Edge

La configurazione del nodo perimetrale dell'infrastruttura corrisponde a quella di un pool cablato standard con Flooding di layer 2 abilitato. il comando CLI "ip direct-broadcast" non viene

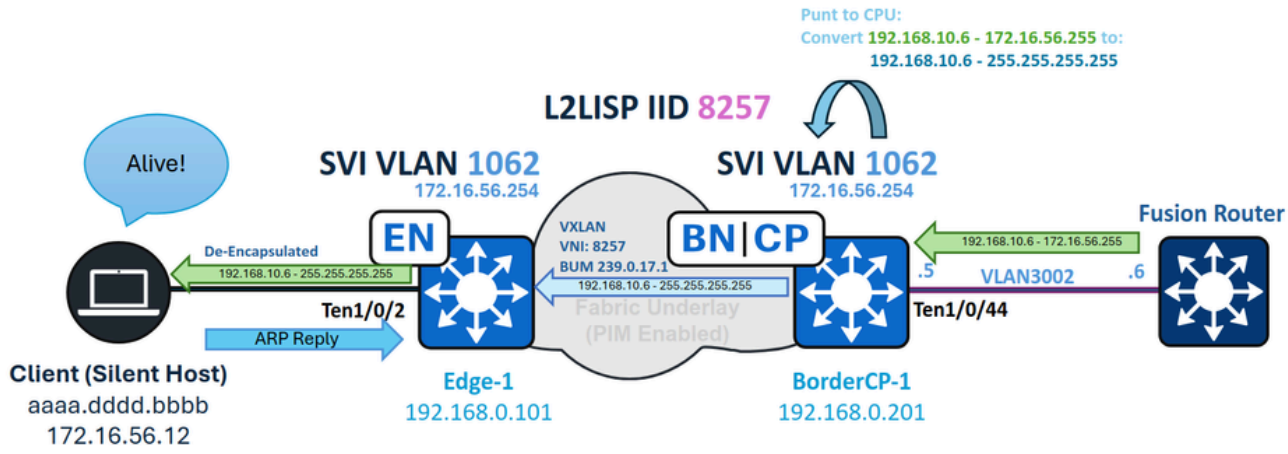
visualizzato sui nodi Edge.

<#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
```

Inoltro broadcast diretto IP



Inoltro IPDB

Bordo - Conversione trasmissioni punt CPU e subnet in ingresso

Nell'esempio, una subnet IP trasmessa con un indirizzo IP di destinazione pari a 172.16.56.255 (l'indirizzo di broadcast per il pool 172.16.56.0/24) viene instradata dalla rete esterna e arriva prima al bordo dell'infrastruttura. L'interfaccia in entrata di layer 3 è l'IP Transit SVI (VLAN 3002). Poiché "ip network-broadcast" è abilitato su questa interfaccia, il pacchetto viene accettato per la conversione full-broadcast; senza questa configurazione, il pacchetto verrebbe scartato.

Il pacchetto arriva sulla SVI 3002 e, come pacchetto broadcast, viene indirizzato alla CPU dello switch. Con la trasmissione di rete IP configurata, il pacchetto viene autorizzato e convertito in trasmissione completa.

<#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 l'elaborazione della CPU, la VLAN 1062 (interfaccia di destinazione) converte il pacchetto in un broadcast completo, in quanto è configurata con "ip direct-broadcast".

<#root>

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

```
 Directed broadcast forwarding is enabled
```

Per risolvere questo evento, usare il comando debug ip packet. Per evitare un output eccessivo e un utilizzo elevato delle risorse, applicare sempre un elenco degli accessi come filtro quando si esegue il debug.

<#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

Il bordo in entrata funge da origine multicast (S) e da gruppo (G) per l'incapsulamento BUM, utilizzando il relativo loopback 0 come indirizzo di origine e il gruppo BUM configurato come destinazione.

Sul piano di controllo PIM, assicuratevi che nell'elenco Interfaccia in uscita (Outgoing Interface List) per la route multicast venga visualizzato un collegamento verso il basso verso gli spigoli della struttura. Per il data plane, usare il comando show ip mfib count per verificare che i contatori di inoltro hardware siano in aumento per la voce S,G sul bordo.

<#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

Questo documento non fornisce una spiegazione dettagliata della formazione di alberi multicast sottostanti o dell'inondazione di layer 2. In caso di stati S,G mancanti, incompleti o errati, la porzione di substrato multicast della rete richiede una risoluzione dei problemi indipendente.

Edge - Trasmissione in ingresso

Sui bordi della struttura, la trasmissione in arrivo incapsulata nella VXLAN sul multicast viene decapsulata e inoltrata alla VLAN associata alla VNI (8257), raggiungendo tutte le porte in stato di inoltro nello Spanning-Tree.

Verificare innanzitutto che la voce S,G del bordo (con loopback del bordo come origine) per il gruppo BUM sia presente e inoltrare il traffico. Per verificare questa condizione, usare gli stessi comandi mroute e mfib; verificare che l'interfaccia secondaria L2LISP corrispondente alla VLAN (1062) sia elencata come interfaccia in uscita.

<#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

Dopo il decapsulamento, il pacchetto viene inoltrato sulla VLAN 1062 a tutte le porte assegnate a tale 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

Dopo aver ricevuto il pacchetto di trasmissione, l'endpoint deve riconoscere il pacchetto come rilevante e rispondere. Di conseguenza, l'endpoint può inviare un pacchetto ARP, che aggiorna la tabella di tracciamento dei dispositivi sullo 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

Dopo la nuova registrazione dell'endpoint nella traccia delle periferiche, l'endpoint viene importato nel database LISP del nodo Edge e quindi registrato con il Control Plane.

Per le distribuzioni LISP Pub-Sub, il Control Plane pubblica le informazioni sull'endpoint appena registrate sui Bordi, creando istantaneamente una voce della mappa-cache LISP per inoltrare il traffico al nodo perimetrale appropriato.

<#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

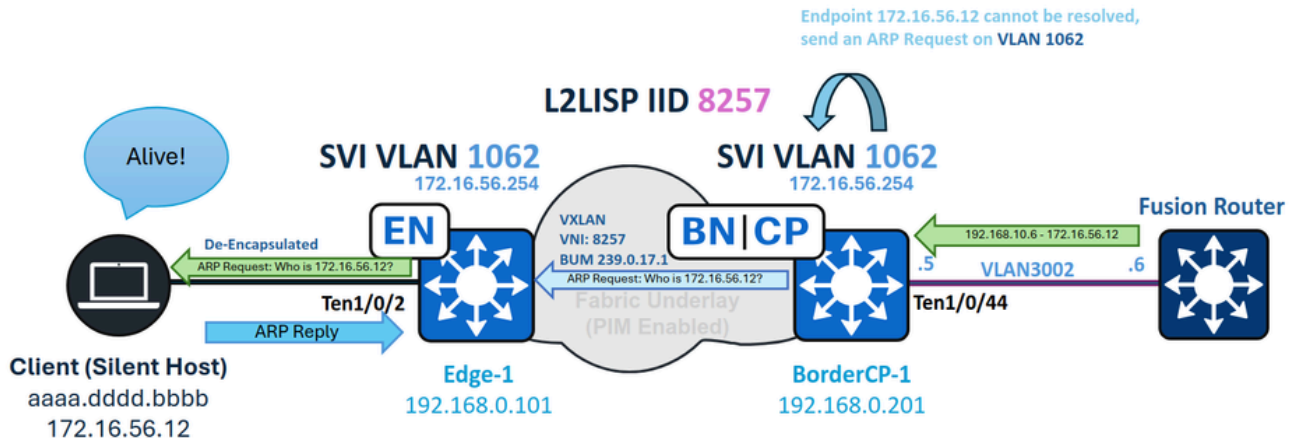
    10/10   -
  Last up-down state change: 5w0d, state change count: 1
  Last route reachability change: 5w0d, state change count: 1
  Last priority / weight change: never/never
  RLOC-probing loc-status algorithm:
    Last RLOC-probe sent: 00:22:19 (rtt 4ms)

Per le distribuzioni LISP/BGP (SDA 1.0), se la distribuzione è distribuita (non collocata), l'aggiornamento della cache delle mappe LISP per un endpoint sconosciuto può richiedere fino a

un minuto, poiché le risposte Mapping negative (NMR) devono prima scadere.

Se non è programmato, un host silenzioso deve ignorare i pacchetti, ad esempio le trasmissioni subnet, per rispondere. alcuni endpoint richiedono un "pacchetto magico" (ad esempio un Eco UDP), mentre altri rispondono solo a un ARP di trasmissione. L'host invisibile all'utente determina il tipo di pacchetto che lo attiva. Tra le opzioni più comuni, è in genere preferibile una richiesta ARP, come illustrato nella sezione Inoltro unicast sconosciuto.

Inoltro unicast sconosciuto



Inoltro unicast sconosciuto

Quando un pool è abilitato per la trasmissione diretta IP, non solo consente la gestione delle trasmissioni subnet, ma consente anche ai fabric Borders di fungere da gateway per l'inoltro del traffico unicast sconosciuto. In questo contesto, il traffico unicast sconosciuto si riferisce ai pacchetti destinati agli endpoint che non sono attualmente registrati nel Control Plane.

Analogamente a un gateway di rete tradizionale che invia una richiesta ARP quando rileva una voce ARP incompleta, il bordo genera una richiesta ARP e la invia a tutti i nodi Fabric. In questo modo l'host silenzioso riceve la richiesta, si sveglia e invia una risposta ARP, registrandosi nuovamente sul Control Plane.

Questa funzionalità è possibile perché la VLAN dell'endpoint (1062) è configurata sia come SVI sia come istanza L2LISP sul bordo dell'infrastruttura. Con l'opzione "flood arp-end" abilitata nell'ID L2, il Border può inondare le richieste ARP generate dalla SVI ogni volta che il traffico viene indirizzato a un EID LISP sconosciuto, garantendo che gli host silenziosi ricevano la richiesta ARP e abbiano la possibilità di rispondere e aggiornare la loro registrazione nel Control Plane.

<#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 il bordo dell'infrastruttura riceve un pacchetto destinato alla versione 172.16.56.12 sulla SVI 3002 (che fa parte dell'endpoint VN/VRF), tenta la risoluzione LISP, poiché l'output CEF è impostato su "glean" (il dispositivo cerca di risolvere l'adiacenza di destinazione utilizzando il protocollo del livello a valle). Questo processo attiva contemporaneamente una richiesta di mappa LISP e una risoluzione ARP per l'host non registrato (invisibile all'utente).

<#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

Viene creata una voce ARP incompleta, che richiede al Border di inviare una richiesta ARP all'endpoint sconosciuto 172.16.56.12. Questa richiesta ARP, come pacchetto broadcast, viene inoltrata a valle utilizzando il Layer 2 Flooding e la funzione Flood ARP-ND.

Per verificare che l'allagamento di layer 2 sia operativo, monitorare i contatori MFIB per la S,G locale del bordo.

<#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

Il pacchetto ARP allagato raggiunge l'host silenzioso, riattivandolo e richiedendo una risposta ARP. Questa risposta aggiorna la tabella SISF (Device-Tracking) sul perimetro della struttura e crea una voce del database LISP. Di conseguenza, il Fabric Edge avvia la registrazione al Control Plane.

<#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

Dopo la nuova registrazione dell'endpoint nella traccia delle periferiche, l'endpoint viene importato nel database LISP del nodo Edge e quindi registrato con il Control Plane.

Per le distribuzioni LISP Pub-Sub, il Control Plane pubblica le informazioni sull'endpoint appena registrate sui Bordi, creando istantaneamente una voce della mappa-cache LISP per inoltrare il traffico al nodo perimetrale appropriato.

<#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)
```

Per le distribuzioni LISP/BGP (SDA 1.0), se la distribuzione è distribuita (non collocata),

l'aggiornamento della cache delle mappe LISP per un endpoint sconosciuto può richiedere fino a un minuto, poiché le risposte Mapping negative (NMR) devono prima scadere.

Suggerimento: Il confine non risolve mai l'ARP per l'host silenzioso; è necessaria solo la registrazione dell'endpoint. Quando l'host silenzioso risponde, il pacchetto ARP viene inviato come unicast di layer 2, in modo da non essere inondato verso il bordo. Di conseguenza, non si prevede di visualizzare una voce ARP o una voce di tracciamento del dispositivo sul bordo.

Abilitazione della riattivazione LAN nei modelli di autenticazione

quando gli utenti della struttura non hanno l'opzione No Authentication (Nessuna autenticazione), i pacchetti flooded provenienti dal bordo raggiungono gli host silenti finché la porta fa parte della VLAN in cui è abilitata la funzione flooding; tuttavia, con l'autenticazione chiusa (in particolare), due fattori principali diventano importanti.

Assegnazione manuale della VLAN per l'host prima dell'autenticazione

Se non è stata assegnata alcuna VLAN, la porta non riceve pacchetti collegati dalla VLAN designata. Quando si prevede che una VLAN venga assegnata da RADIUS, viene creato un "pollo o l'uovo?" dilemma: il pacchetto propagato non può essere inoltrato a una VLAN diversa (chiamata comunemente VLAN hopping) per attivare l'autenticazione dell'utente e ottenere un'assegnazione VLAN da RADIUS.

Quando si configura la porta in Host-Onboarding, se il dispositivo è identificato come "invisibile all'utente", assegnare manualmente la VLAN utilizzando il menu a discesa per i pool DI DATI.

Il problema degli host invisibili all'utente che non sono in grado di eseguire l'autenticazione prima dell'assegnazione della VLAN non è specifico di SD-Access; si tratta di una sfida di progettazione comune che si riscontra in qualsiasi rete tradizionale protetta.

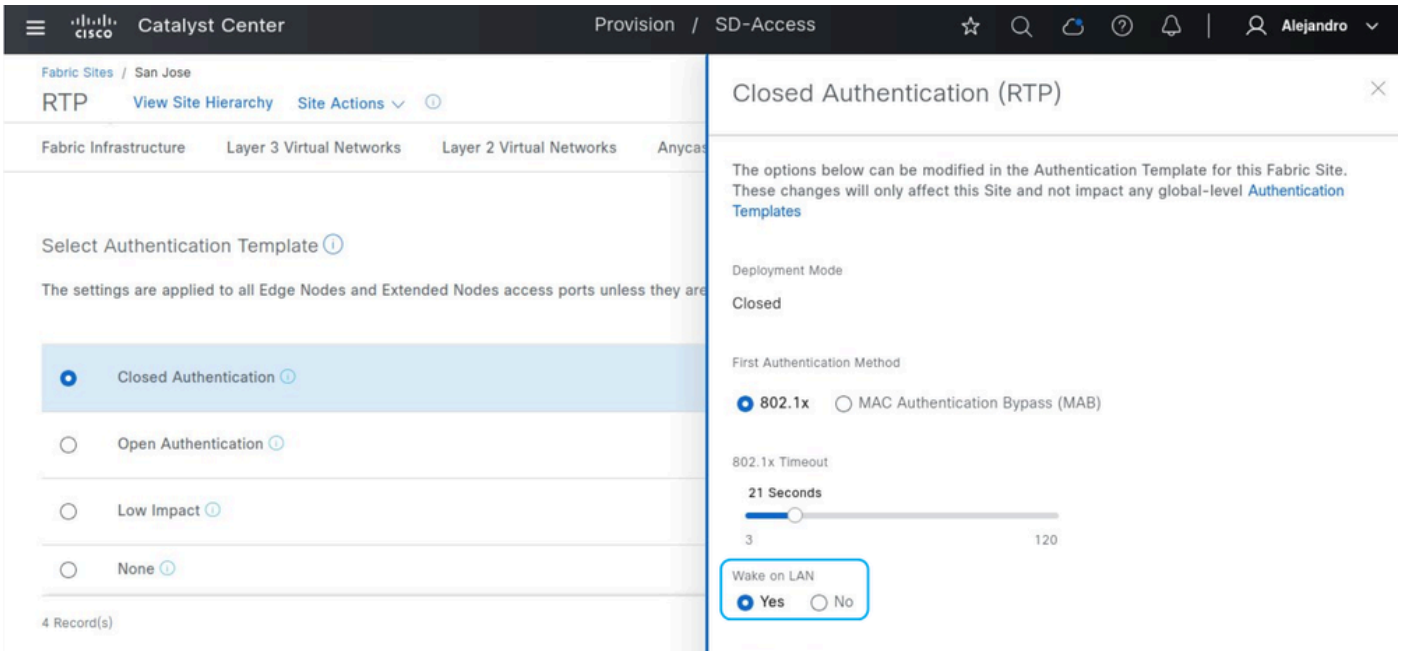
<#root>

```
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
```

Direzione controllo accesso

Per impostazione predefinita, se la riattivazione LAN non è attivata nelle impostazioni del modello di autenticazione in Host-Onboarding, i modelli di autenticazione utilizzano "access-session-control-direction both". In base a questa configurazione, la porta rifiuta sia i pacchetti in arrivo sia i pacchetti che verrebbero inoltrati fuori dalla porta. Quando la funzione Wake-on-LAN è attivata, l'impostazione cambia in "access-session control-direction in", limitando solo il traffico in entrata. Questa regolazione consente ai pacchetti di raggiungere e riattivare l'host invisibile all'utente, consentendo di avviare l'autenticazione MAB.



Riattivazione su LAN

Senza 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
```

Prima dell'autenticazione dell'endpoint, l'interfaccia assegnata non è elencata come abilitata al flooding negli stati dello Spanning Tree.

<#root>

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


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

Con riattivazione LAN abilitata:

<#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
```

Anche prima dell'autenticazione, la porta è abilitata per il traffico in uscita, consentendo ai pacchetti di raggiungere e riattivare l'host invisibile all'utente.

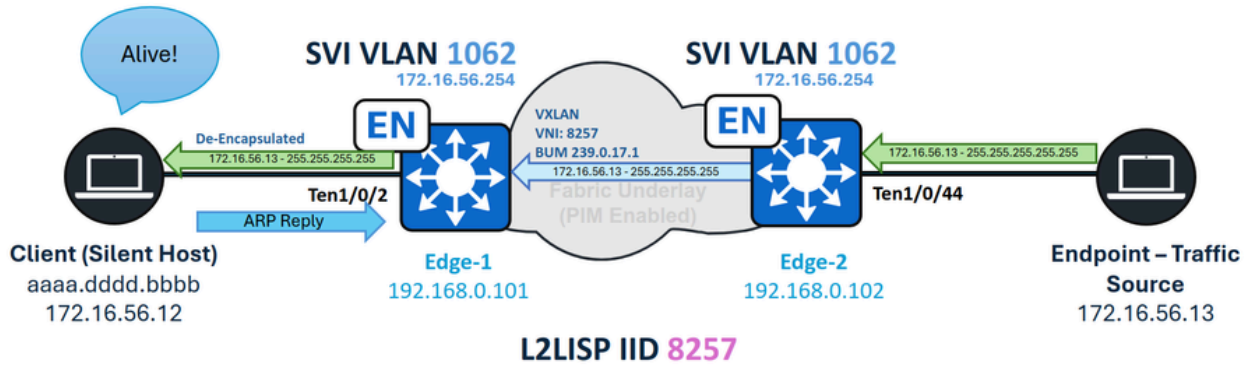
<#root>

```
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
```

Scenari alternativi

Nodi perimetrali e stessa VLAN - Flooding di layer 2

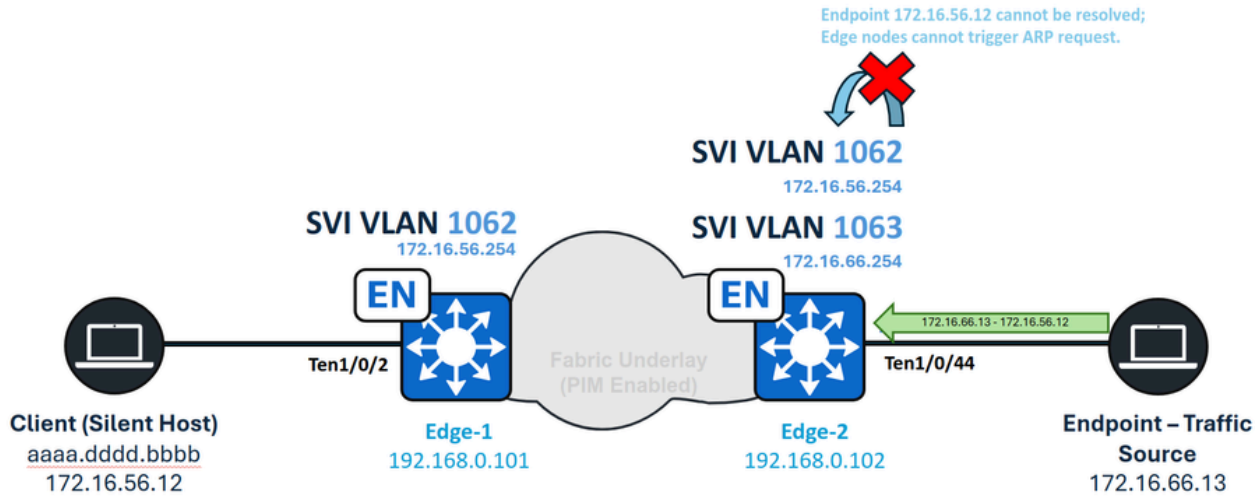
Se l'obiettivo è riattivare un host invisibile all'utente da un dispositivo all'interno della struttura sulla stessa VLAN dell'host, non è necessaria la funzione di trasmissione diretta IP. Al contrario, abilitare il layer 2 Flooding (in un pool non wireless) è sufficiente per consentire lo scambio di pacchetti broadcast, broadcast di subnet o richieste ARP. Per l'autenticazione chiusa, i requisiti di riattivazione LAN vengono mantenuti.



Stessa VLAN - Gestione host invisibile all'utente

Nodi perimetrali e VLAN diversa - Unicast sconosciuto

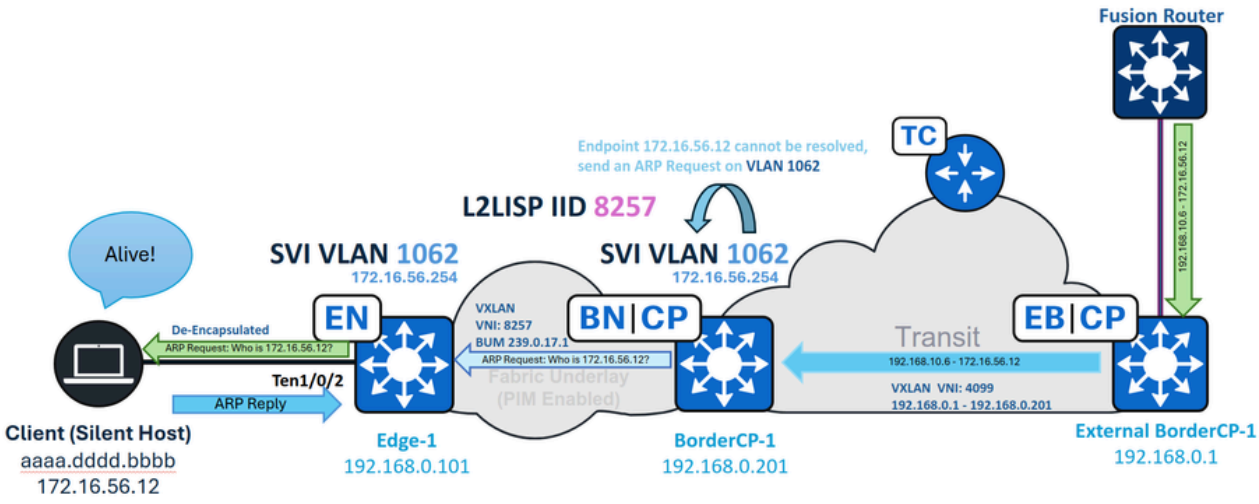
Quando un endpoint all'interno del fabric invia traffico unicast a un host invisibile all'utente connesso a un nodo Fabric Edge, il percorso di inoltro Unicast sconosciuto non è disponibile. A differenza dei bordi dell'infrastruttura, i nodi Fabric Edge dispongono di bordi definiti come LISP Proxy-ETR, che abilitano automaticamente una funzionalità di inoltro chiamata "Segnale e inoltro" quando viene rilevato un endpoint sconosciuto. Fabric Edge deve attivare la richiesta ARP richiesta al primo tentativo di risolvere l'indirizzo. Tuttavia, quando il protocollo LISP identifica l'endpoint come EID sconosciuto, i pacchetti successivi non attivano richieste ARP aggiuntive. Questo scenario è considerato non supportato.



Unicast Inter-VLAN sconosciuto

SD-Access Transit - Unicast sconosciuto

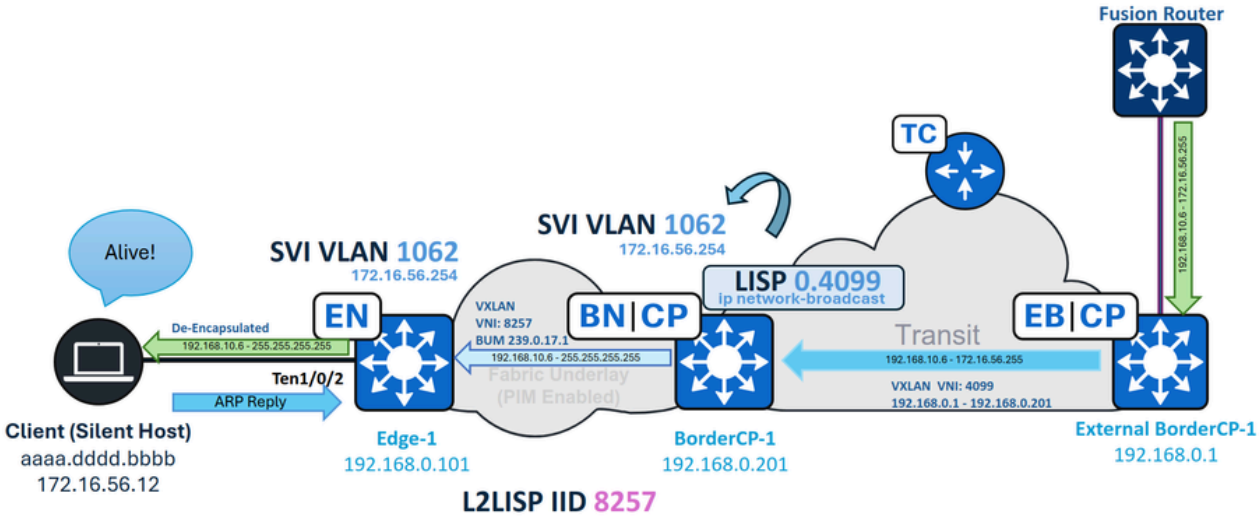
Nel caso di SD-Access Transit, il traffico unicast sconosciuto è supportato in modo nativo senza alcun requisito speciale. Il traffico proveniente da un confine remoto viene instradato attraverso la rete SD-Access Transit, in cui i broadcast della subnet vengono considerati come normali flussi di traffico. Quando il traffico raggiunge il confine del sito locale, vengono eseguite operazioni standard, tra cui Traffic Glean, ARP Request flooding e la risoluzione LISP.



SD-Access Transit Unicast sconosciuto

Transito SD - Trasmissione diretta IP

Quando si utilizza SD-Access Transit, il Border del sito locale riceve il broadcast indirizzato IP sull'interfaccia secondaria LISP per la VPN (ad esempio, l'interfaccia 4099), piuttosto che su una SVI. Per assicurarsi che la trasmissione venga accettata e convertita in una subnet broadcast dalla funzione di trasmissione diretta IP, è necessario configurare manualmente il parametro "ip network-broadcast" sull'interfaccia secondaria LISP.



SD-Access Transit IPDB

Su BorderCP-1 (Bordo sito locale):

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).