Configuración del Host Silencioso de Acceso SD con la Función IP Directed Broadcast

Contenido

Introducción

Este documento describe la administración de hosts silenciosos en SD-Access, abordando los desafíos de conectividad mediante la inundación de L2 y la difusión dirigida por IP.

Descripción

La mayoría de los terminales y sus interfaces de red transmiten el tráfico periódicamente, especialmente los mensajes relacionados con el control, como ARP o DHCP. Sin embargo, ciertos extremos responden sólo cuando se les solicita, en lugar de enviar paquetes a intervalos regulares. Estos dispositivos envían paquetes de control únicamente a demanda. En las redes, estos terminales se conocen comúnmente como hosts silenciosos. En el contexto de SD-Access,

los hosts silenciosos deben detener todo el tráfico o restringir su comunicación reteniendo los paquetes del plano de control.

En el fabric SDA, las difusiones se suprimen en cada nodo de borde o se reenvían a todos los bordes mediante la inundación de capa 2, un proceso que normalmente se limita a los nodos de borde y los bordes de capa 2. El reenvío de difusiones a cada puerto de una VLAN imita el comportamiento de una red de Capa 2 tradicional, lo que ayuda significativamente a que los hosts silenciosos permanezcan activos. Sin embargo, la gestión de hosts silenciosos en un entorno de fabric presenta desafíos, ya que la falta de comunicación regular puede interrumpir los mecanismos de autenticación, los registros del plano de control y el reenvío.

La habilitación de la inundación de L2 solo aborda parte del problema. Los hosts silenciosos pueden recibir paquetes de broadcast solamente cuando otro dispositivo los genera, ya sea desde dentro de la misma VLAN dentro del entramado o desde un borde del entramado. Una difusión dirigida IP hace referencia a un paquete IP con una dirección de destino establecida en la dirección de difusión de una subred, que se origina en un host fuera de esa subred. Esta función requiere compatibilidad con multidifusión en la capa subyacente. Cuando se habilita la difusión dirigida IP en el fabric, todos los paquetes de difusión de subred llegan a cada host dentro de esa subred. Esta función también puede activar dispositivos mediante paquetes de unidifusión estándar, simulando de forma eficaz el comportamiento de "unidifusión desconocida" que se encuentra en las redes tradicionales.

Topología

Hardware y software

- Catalyst 9000 Series Switch
- Catalyst Center Versión 2.3.7.9
- Cisco IOS® XE 17.15.03 y versiones posteriores (frontera/CP y extremo)

Topología:

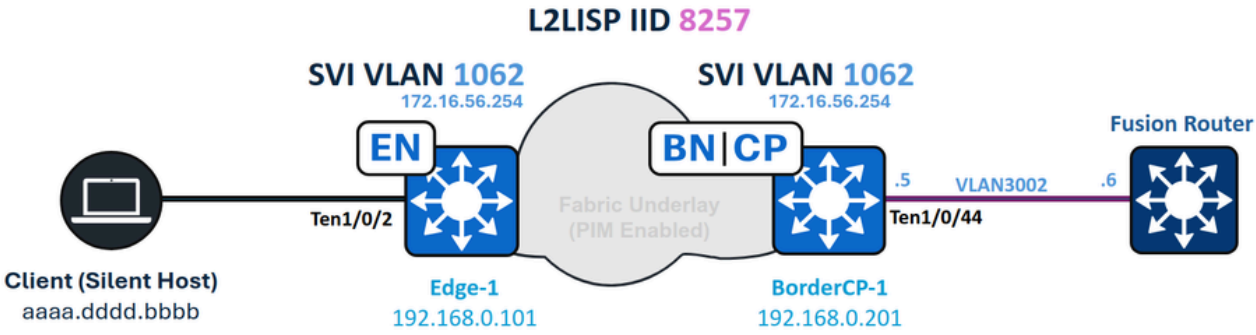


Diagrama de la red

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Reenvío de protocolo de Internet (IP)
- Protocolo de separación Localizador/ID (LISP)
- Multidifusión independiente de protocolo (PIM)
- Inundación de capa 2 en SD-Access

Requirements

- Esta función requiere Cisco Catalyst Center 1.3 o superior
- Licencias Cisco IOS XE 17.3 y Cisco DNA Advantage*
- Para ASR e ISR Borders, se requiere Cisco IOS XE 17.3.1 o superior
- Los switches Catalyst series 3000, 4000, 6000 o Nexus 7000 no son compatibles

---

⚠ Precaución: La activación de la función Difusión dirigida IP activa automáticamente la Inundación de capa 2. Asegúrese de que la funcionalidad de multidifusión de la capa subyacente funciona correctamente antes de activar esta función.

Puede activar o desactivar la difusión dirigida IP después de crear el grupo IP, de forma similar a la gestión de grupos inalámbricos o a la configuración de saturación de nivel 2.

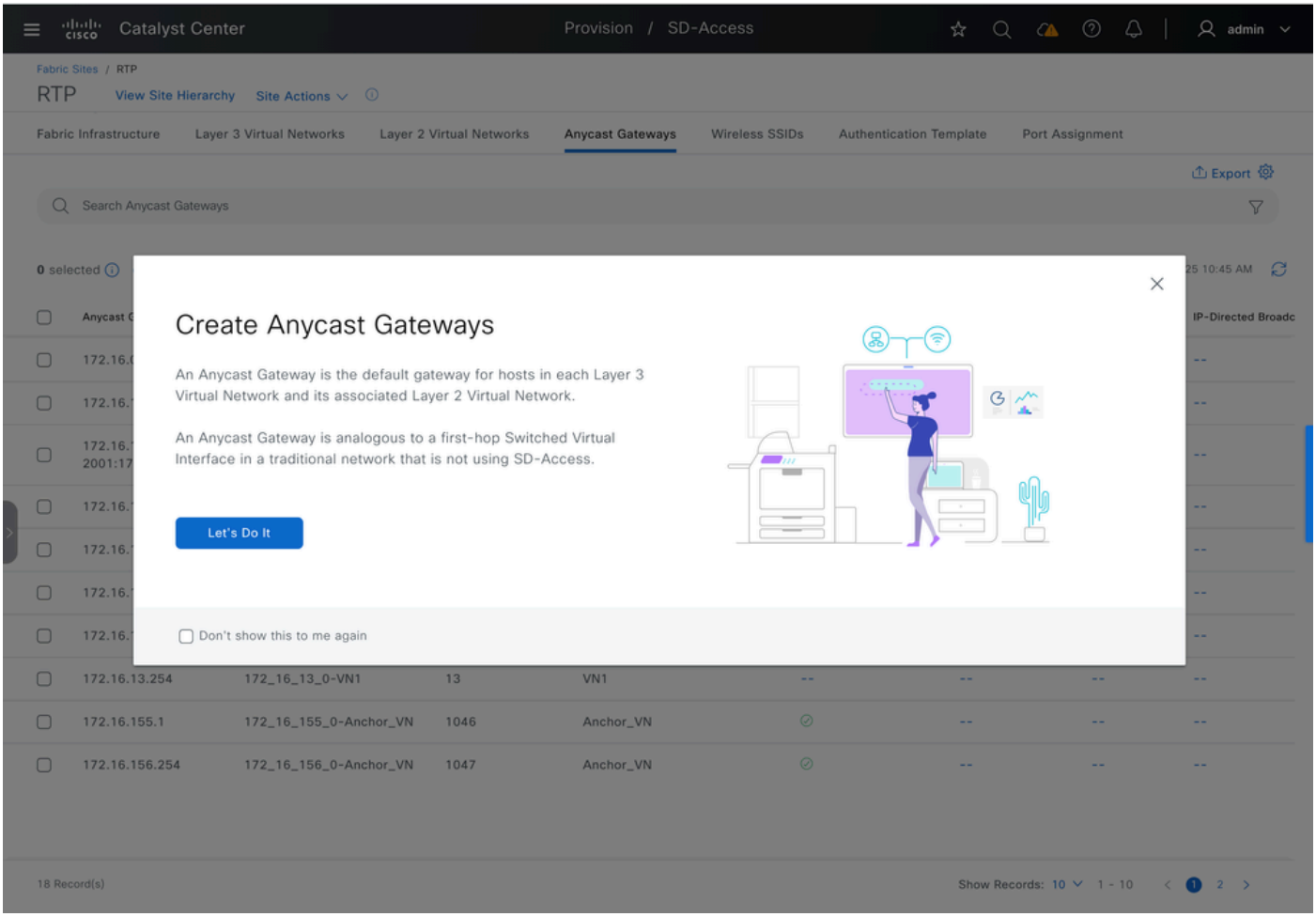
Configuración de Catalyst Center

Cuando la difusión dirigida IP está activada, Catalyst Center inicia una tarea de aprovisionamiento de todo el fabric. En este proceso de aprovisionamiento se incluyen todos los nodos perimetrales, los bordes de capa 2 y los bordes con transferencia de capa 3.

Para activar el flujo de trabajo de Difusión dirigida IP en la interfaz de usuario:

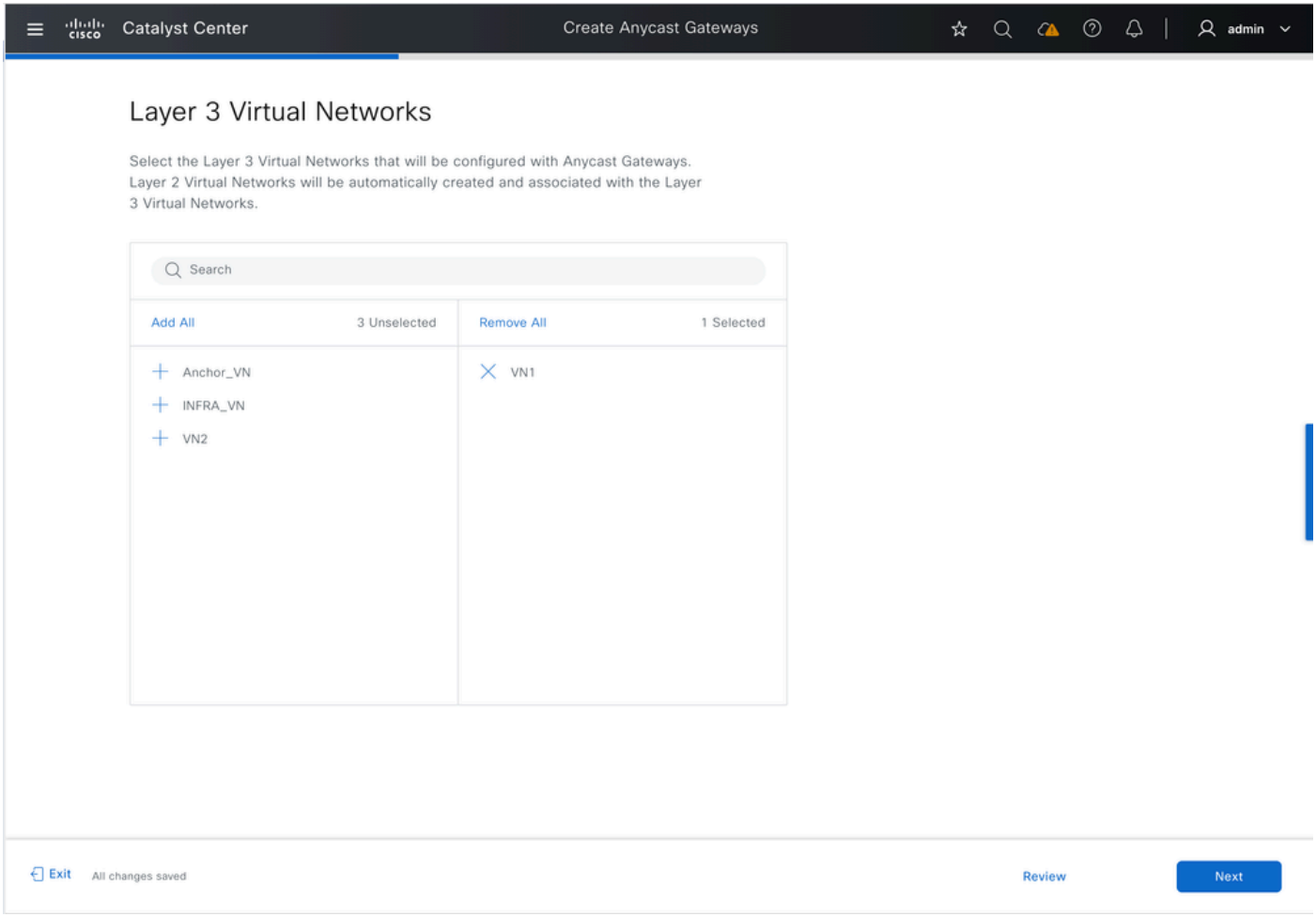
1. Vaya a Aprovisionamiento.
2. Seleccione Fabric Sites.
3. Seleccione el sitio deseado.
4. Vaya a Anycast Gateways.

A partir de ahí, puede configurar los parámetros necesarios para Difusión dirigida IP.



Creación de gateways Anycast

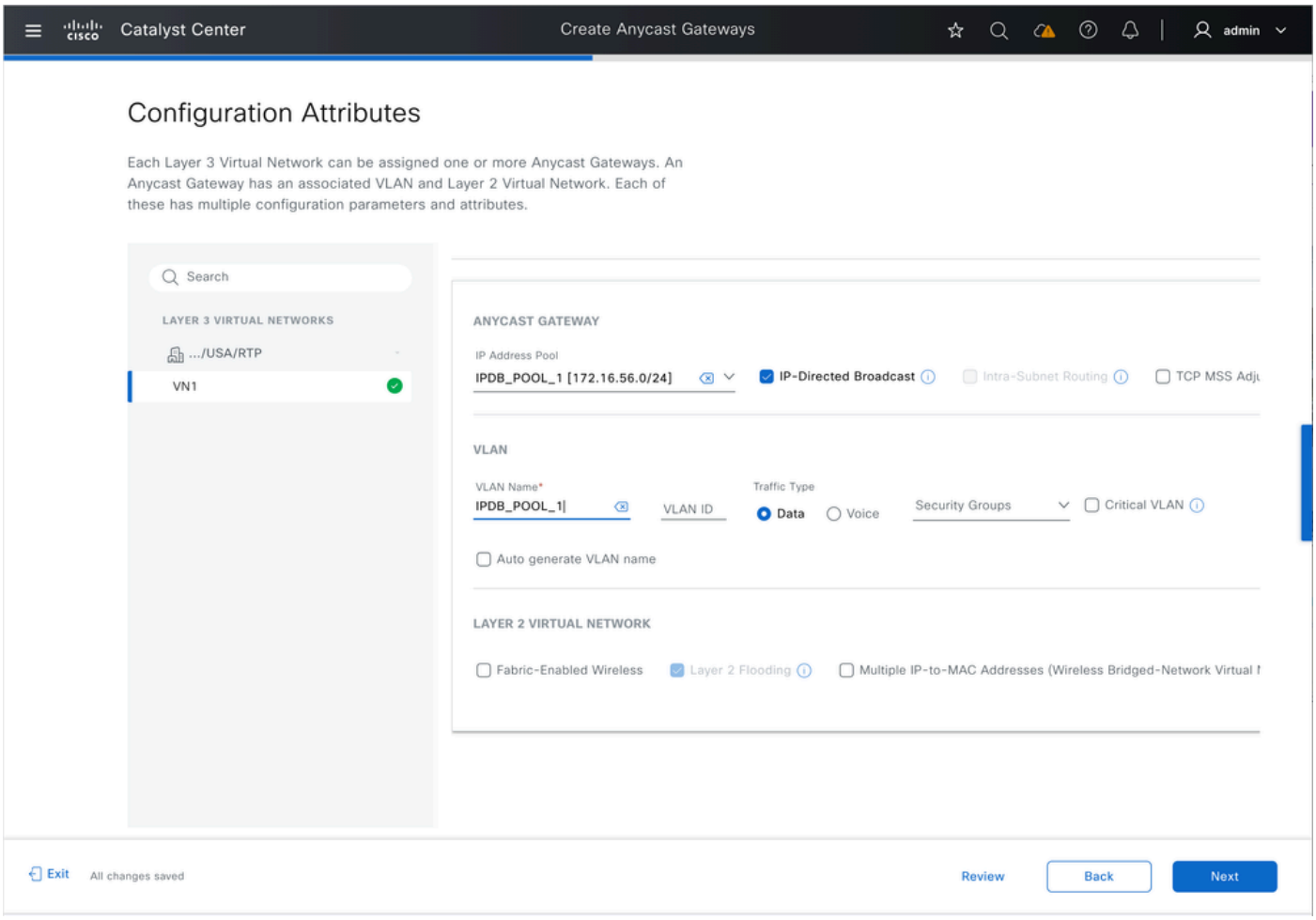
Seleccione la red virtual de capa 3 que desee y, a continuación, haga clic en Siguiente para continuar.



Seleccionar redes virtuales L3

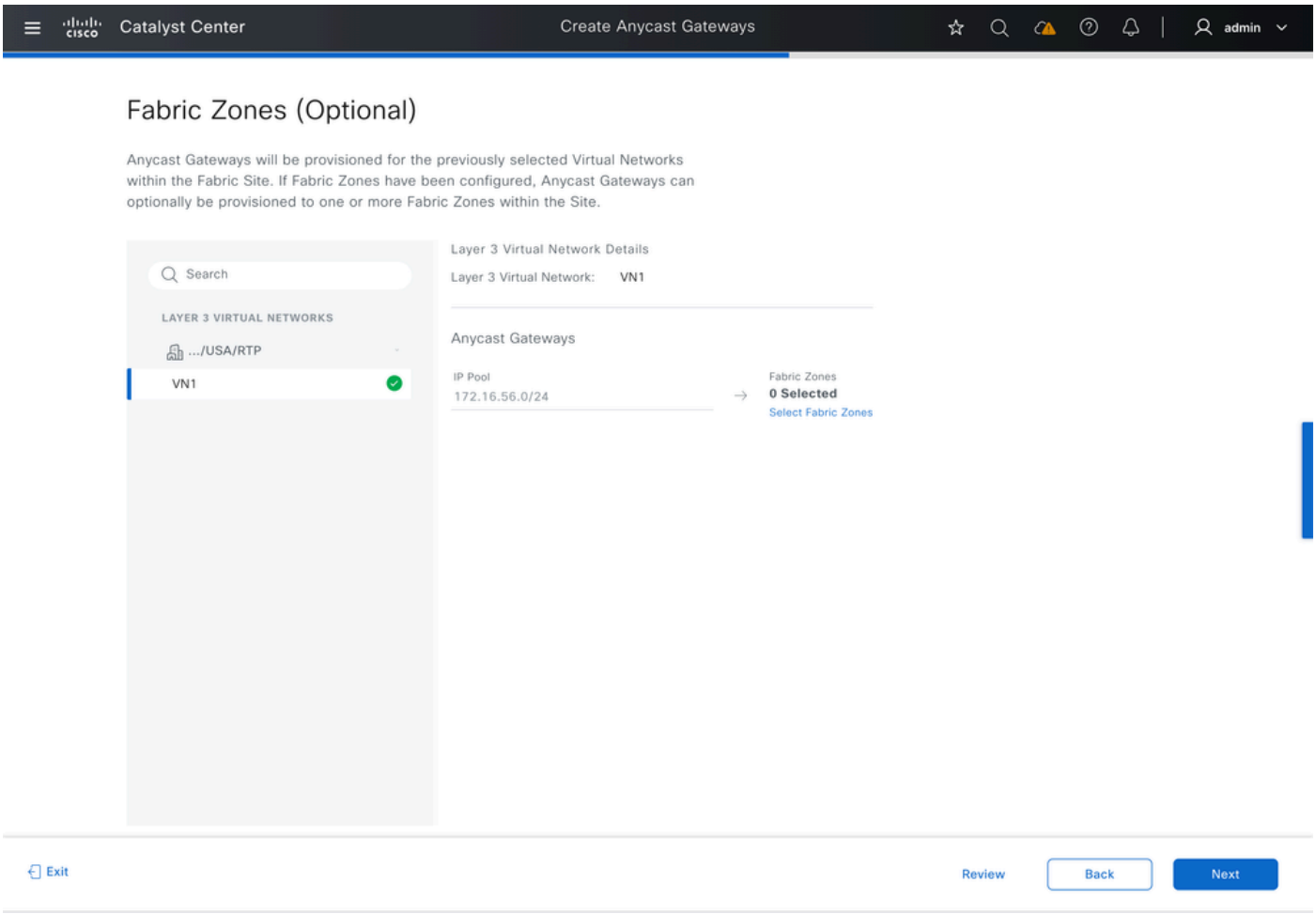
Seleccione el pool IP, habilite IP Directed Broadcast e ingrese el nombre de la VLAN.

Consejo: La activación de la difusión dirigida IP activa automáticamente la inundación de L2.



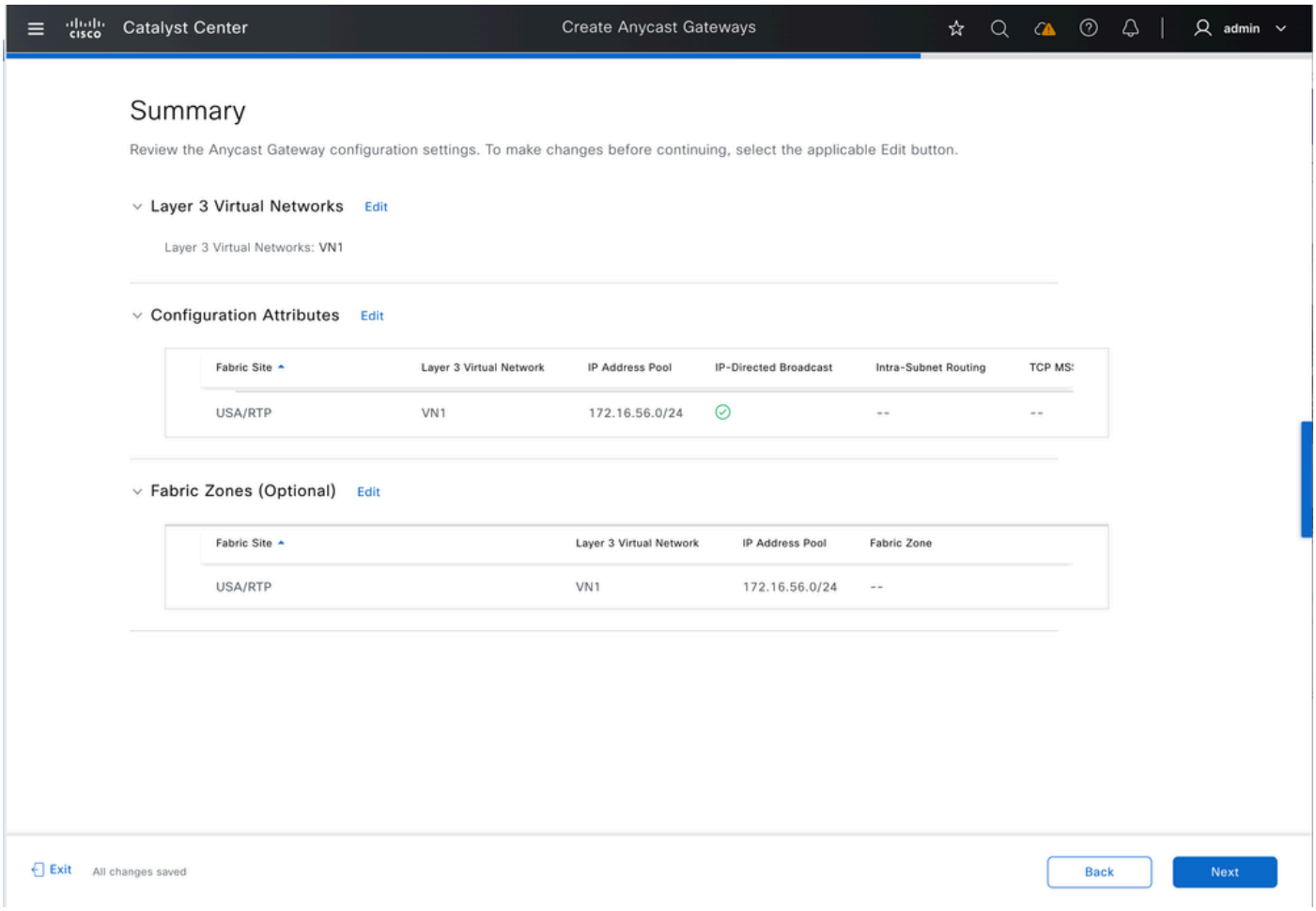
Activar difusión dirigida IP

Si existen zonas de fabric, puede proporcionar de forma opcional gateways de difusión ilimitada a una o varias zonas de fabric del sitio.



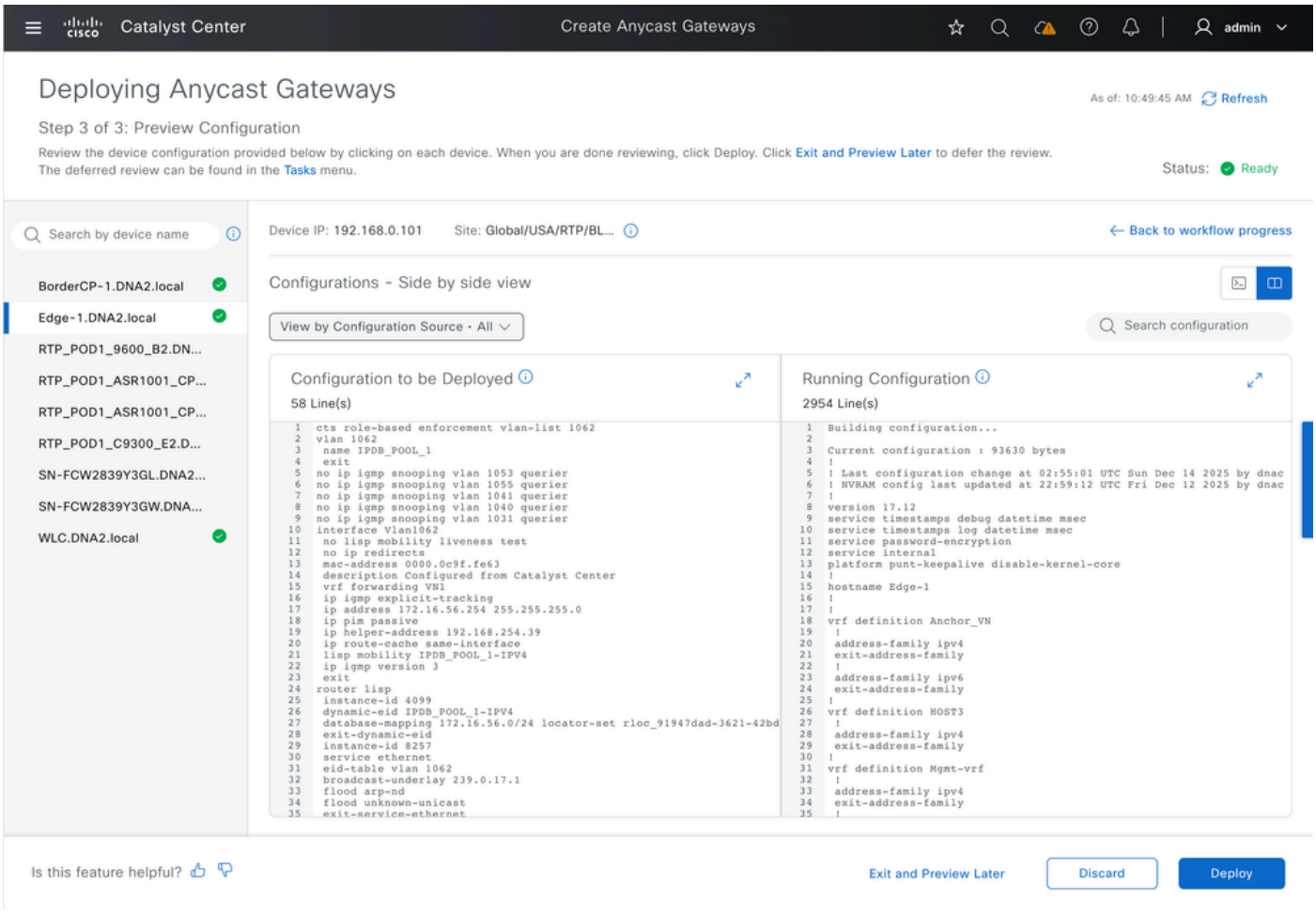
Seleccionar zonas de fabric

Revise el resumen de los parámetros configurados para confirmar la precisión antes de continuar con la implementación.



Summary

Vista previa de las configuraciones generadas. Haga clic en Deploy para aplicar la configuración al fabric.



Vista previa de configuración

Configuración de dispositivos de red

Configuración de borde - Tránsito IP

Los límites de fabric con IP Transit configurado tienen sus interfaces de peering BGP configuradas con "ip network-broadcast" para permitir el reenvío de difusiones de subred IP. La IP de gateway de difusión ilimitada para el grupo de fabric (VLAN de terminal) cambia de una interfaz de bucle invertido a una SVI, que tiene activada la difusión dirigida por IP. Ambas configuraciones son necesarias para que el borde del fabric convierta los paquetes de difusión de subred IP en difusiones completas, lo que permite que el proceso funcione según lo previsto.

Configuración de broadcast de red IP y broadcast de red 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
```

Esta segunda parte de la configuración habilita la función IP Directed-Broadcast para reactivar hosts silenciosos mediante una solicitud ARP (broadcast), similar al comportamiento de las redes tradicionales al gestionar tráfico unicast desconocido. Con esta configuración, las fuentes externas al fabric pueden activar los terminales mediante tráfico unidifusión estándar, sin depender de las difusiones de subred ni de los mecanismos Wake-on-LAN ("paquete mágico").

<#root>

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

instance-id 4099



dynamic-eid IPDB_POOL_1-IPV4



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


instance-id 8257


   service ethernet
     eid-table vlan 1062

     broadcast-underlay 239.0.17.1

-- Enables Layer 2 Flooding to use BUM group 239.0.17.1


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


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

Configuración perimetral

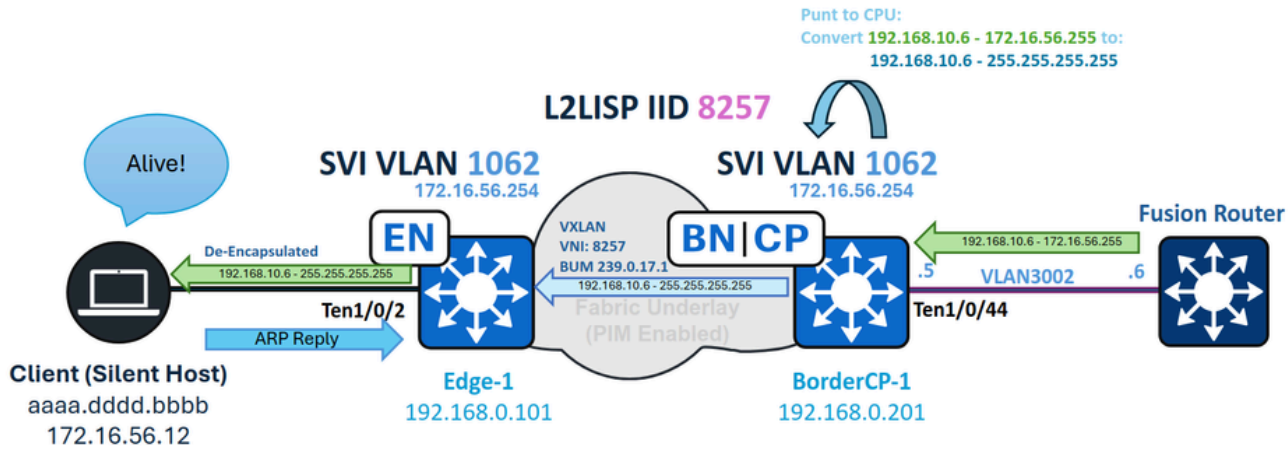
La configuración del nodo de borde de fabric coincide con la de un conjunto con cables estándar con la función Inundación de capa 2 habilitada. El comando CLI "ip directed-broadcast" no aparece en los nodos perimetrales.

<#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 Directed Broadcast Forwarding



Reenvío IPDB

Conversión de frontera - CPU de entrada y difusión de subred

En este ejemplo, un broadcast de subred IP con una IP de destino de 172.16.56.255 (la dirección de broadcast para el conjunto 172.16.56.0/24) se rutea desde la red externa y llega primero al borde del entramado. La interfaz de capa 3 de entrada es IP Transit SVI (VLAN 3002). Debido a que "ip network-broadcast" está habilitado en esta interfaz, el paquete se acepta para la conversión de difusión completa; sin esta configuración, el paquete se descartaría.

El paquete llega al SVI 3002 y, como paquete de difusión, se envía a la CPU del switch. Con la difusión de red IP configurada, el paquete se permite y se convierte en una difusión 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 el procesamiento de la CPU, la VLAN 1062, la interfaz de destino, convierte el paquete en una transmisión completa, ya que está configurado con "ip directed-broadcast".

<#root>

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

```
 Directed broadcast forwarding is enabled
```

Puede resolver este evento mediante el comando debug ip packet. Para evitar un resultado excesivo y un uso elevado de los recursos, aplique siempre una lista de acceso como filtro al ejecutar esta depuración.

<#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

El borde de ingreso actúa como el origen de multidifusión (S) y el grupo (G) para la encapsulación BUM, usando su Loopback 0 como la dirección de origen y el grupo BUM configurado como el destino.

En el plano de control PIM, asegúrese de que aparezca un enlace descendente hacia los bordes del entramado en la Lista de interfaces salientes para la ruta de multidifusión. Para el plano de datos, utilice el comando show ip mfib count para verificar que los contadores de reenvío de hardware están aumentando para la entrada S,G en el borde.

<#root>

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

(

192.168.0.201

,

239.0.17.1

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

Incoming interface: Null0

, RPF nbr 0.0.0.0
 Outgoing interface list:

TenGigabitEthernet1/0/42

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

-- Downlink to Fabric Edge or Intermediate Node

BorderCP-1#show ip mfib 239.0.17.1 192.168.0.201 count

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

Group: 239.0.17.1

Source: 192.168.0.201,

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

 HW Forwarding: 2124804

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

Este documento no proporciona una explicación detallada de la formación del árbol multicast subyacente o la inundación de la Capa 2. En el caso de estados S,G faltantes, incompletos o incorrectos, la porción de multidifusión subyacente del gusano de red requiere una resolución de problemas independiente.

Edge - Broadcast de entrada

En los extremos del fabric, la difusión entrante encapsulada en VXLAN en multidifusión se desencapsula y se reenvía a la VLAN asociada con VNI (8257), alcanzando todos los puertos en un estado de reenvío en el árbol de extensión.

Primero, verifique que la entrada S,G del borde (con el loopback de borde como origen) para el grupo BUM esté presente y reenviando tráfico. Utilice los mismos comandos mroute y mfib para verificar esto, asegúrese de que la subinterfaz L2LISP correspondiente a la VLAN (1062)

aparezca como interfaz de salida.

<#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
```

Después de la desencapsulación, el paquete se reenvía en la VLAN 1062 a todos los puertos asignados a esa 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

Una vez que el terminal recibe el paquete de difusión, debe reconocer el paquete como relevante y responder. Como resultado, el terminal podría enviar un paquete ARP, que actualiza la tabla de seguimiento de dispositivos en el 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

Después de volver a registrar el terminal en el seguimiento de dispositivos, se importa a la base de datos LISP del nodo de borde y, a continuación, se registra con el plano de control.

Para implementaciones Pub-Sub de LISP, el plano de control publica la información de terminal recién registrada en los bordes, creando instantáneamente una entrada de caché de mapa de LISP para reenviar el tráfico al nodo de borde apropiado.

<#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

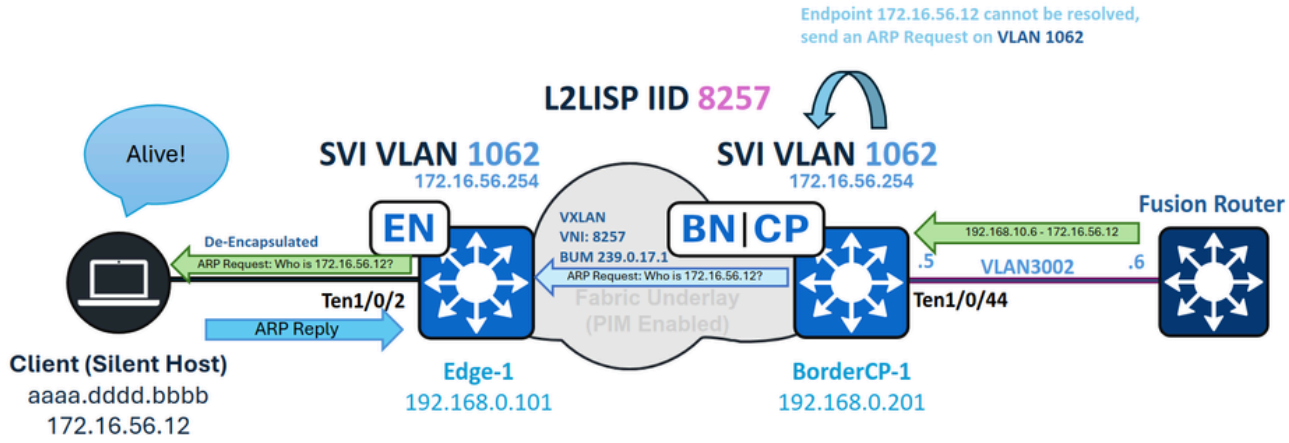
up

    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)

En el caso de implementaciones LISP/BGP (SDA 1.0), si la implementación está distribuida (sin ubicación compartida), la actualización de la caché de mapas de LISP para un terminal desconocido puede tardar hasta un minuto, ya que las respuestas de mapas negativos (NMR) deben caducar en primer lugar.

Un host silencioso debe ignorar los paquetes como las difusiones de subred si no está programado para responder a ellos. Algunos terminales requieren un "paquete mágico" (como un eco UDP), mientras que otros solo responden a un ARP de difusión. El host silencioso en sí determina qué tipo de paquete lo activa para activarse. Entre las opciones más comunes, se prefiere una solicitud ARP, como se explica en la sección Desconocido Unicast Forwarding.

Reenvío unidifusión desconocido



Reenvío unidifusión desconocido

Cuando un grupo está habilitado para la difusión dirigida IP, no solo permite la gestión de difusiones de subred, sino que también permite que los límites del fabric actúen como puertas de enlace para el reenvío de tráfico de unidifusión desconocido. En este contexto, el tráfico de unidifusión desconocido se refiere a paquetes destinados a terminales que no están registrados actualmente en el plano de control.

De manera similar a un gateway de red tradicional que envía una solicitud ARP cuando encuentra una entrada ARP incompleta, el borde genera una solicitud ARP y la inunda a todos los nodos de fabric. Esto garantiza que el host silencioso reciba la solicitud, se despierte y envíe una respuesta ARP, volviéndose a registrar en el plano de control.

Esta funcionalidad es posible porque la VLAN de terminal (1062) se configura como una SVI y como una instancia de L2LISP en el borde del entramado. Con "flood arp-nd" habilitado en el ID de capa 2, el borde puede inundar las solicitudes ARP generadas por la SVI siempre que haya tráfico dirigido a un EID de LISP desconocido, lo que garantiza que los hosts silenciosos reciban la solicitud ARP y tengan la oportunidad de responder y actualizar su registro en el plano de control.

<#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
```

Cuando el borde del entramado recibe un paquete destinado a 172.16.56.12 en SVI 3002, que forma parte del terminal VN/VRF, intenta la resolución de LISP, ya que la salida de CEF se establece en "glean" (lo que significa que el dispositivo intenta resolver la adyacencia de destino mediante el protocolo de capa descendente). Este proceso activa simultáneamente una petición de mapa LISP y una resolución ARP para el host no registrado (silencioso).

<#root>

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


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


172.16.56.0/24,
 uptime: 00:00:30, expires: never, via dynamic-EID, send-map-request, local-to-site
Sources: NONE
State:
```

send-map-request

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

send-map-request   -- LISP Resolution attempted

<#root>

BorderCP-1#show ip cef vrf VN1 172.16.56.12

172.16.56.0/24

attached to LISP0.4099

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

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

glean for LISP0.4099

Se crea una entrada ARP incompleta, lo que hace que el borde envíe una solicitud ARP al punto final desconocido 172.16.56.12. Esta solicitud ARP, como paquete de difusión, se reenvía en sentido descendente mediante Inundación de capa 2 y la función Inundación ARP-ND.

Para verificar que la inundación de la Capa 2 esté operativa, monitoree los contadores MFIB para el S,G local del borde.

<#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

El paquete ARP inundado alcanza el host silencioso, activándolo y solicitando una respuesta ARP. Esta respuesta actualiza la tabla de seguimiento de dispositivos (SISF) en el Fabric Edge y crea una entrada de base de datos LISP. Como resultado, el borde del fabric inicia un registro en el plano de control.

<#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

Después de volver a registrar el terminal en el seguimiento de dispositivos, se importa a la base de datos LISP del nodo de borde y, a continuación, se registra con el plano de control.

Para implementaciones Pub-Sub de LISP, el plano de control publica la información de terminal recién registrada en los bordes, creando instantáneamente una entrada de caché de mapa de LISP para reenviar el tráfico al nodo de borde apropiado.

<#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)

En el caso de implementaciones LISP/BGP (SDA 1.0), si la implementación está distribuida (sin

ubicación compartida), la actualización de la caché de mapas de LISP para un terminal desconocido puede tardar hasta un minuto, ya que las respuestas de mapas negativos (NMR) deben caducar en primer lugar.

Consejo: La frontera nunca resuelve ARP para el host silencioso; solo se requiere el registro del terminal. Cuando el host silencioso responde, el paquete ARP se envía como unidifusión de Capa 2, por lo que no se inunda hacia el borde. Como resultado, no espere ver una entrada ARP o una entrada de rastreo de dispositivos en el borde.

Habilitación de Wake-on-LAN en Plantillas de Autenticación

Cuando los usuarios de fabric tienen habilitada la opción Sin autenticación, los paquetes inundados del borde llegan a hosts silenciosos mientras el puerto sea parte de la VLAN donde está habilitada la inundación; sin embargo, con la autenticación cerrada (en particular), dos factores principales se vuelven importantes.

Asignación Manual de VLAN para el Host Antes de la Autenticación

Si no se asigna ninguna VLAN, el puerto no recibe paquetes inundados de su VLAN designada. Cuando se espera que RADIUS asigne una VLAN, esto crea un "¿Pollo o Huevo?" dilema: el paquete inundado no se puede reenviar a una VLAN diferente (comúnmente conocida como salto de VLAN) para activar la autenticación de usuario y obtener una asignación de VLAN de RADIUS.

Al configurar el puerto en Host-Onboarding, si el dispositivo se identifica como "silencioso", asigne manualmente la VLAN mediante el menú desplegable para los grupos de DATOS.

El problema de los hosts silenciosos que no pueden autenticarse antes de la asignación de VLAN no es exclusivo de SD-Access; se trata de un reto de diseño común en cualquier red segura tradicional.

<#root>

```
interface TenGigabitEthernet1/0/2
```

```
 switchport access vlan 1062
```

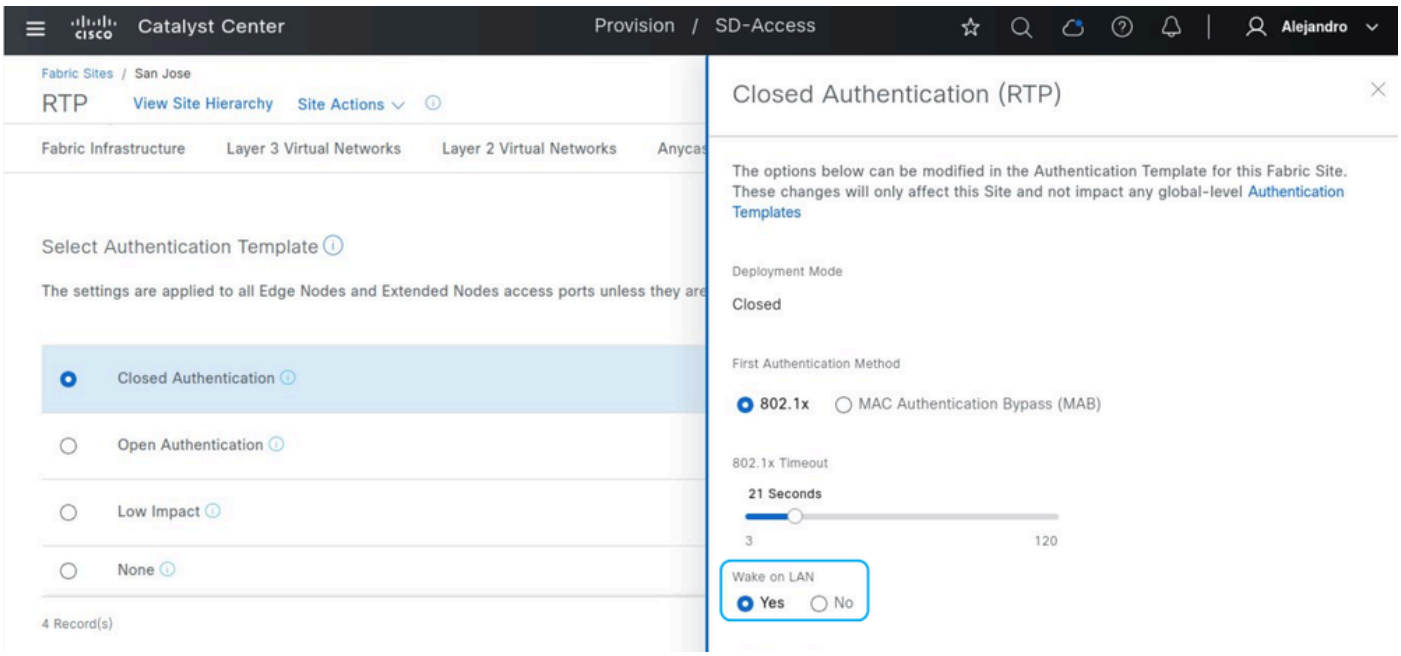
```
 switchport mode access
 device-tracking attach-policy IPDT_POLICY
 dot1x timeout tx-period 7
 dot1x max-reauth-req 3
```

```
source template DefaultWiredDot1xClosedAuth
```

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

Dirección de control de acceso

De forma predeterminada, si Wake-on-LAN no está habilitado en la configuración de la plantilla de autenticación dentro de Host-Onboarding, las plantillas de autenticación utilizan "access-session control-direction both". Esta configuración hace que el puerto descarte tanto los paquetes entrantes como los paquetes que se reenviarían fuera del puerto. Cuando Wake-on-LAN está habilitado, la configuración cambia a "access-session control-direction in", restringiendo solamente el tráfico de ingreso. Este ajuste permite que los paquetes alcancen y reactiven el host silencioso, lo que le permite iniciar la autenticación MAB.



Wake on LAN

Sin Wake-on-LAN:

<#root>

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


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

 control-direction both


 access-session

closed


access-session port-control auto



Edge-1#show authentication session interface Te1/0/2 detail | i Oper

Oper host mode: multi-auth


Oper control dir: both

Oper host mode: multi-auth


Oper control dir: both
```

Antes de que el terminal se autentique, la interfaz asignada a él no aparece como inundación habilitada en los estados del árbol de expansión.

<#root>

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


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

Con Wake-on-LAN activado:

<#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
```

Incluso antes de la autenticación, el puerto está habilitado para el tráfico de salida, lo que permite que los paquetes alcancen y reactiven el host silencioso.

<#root>

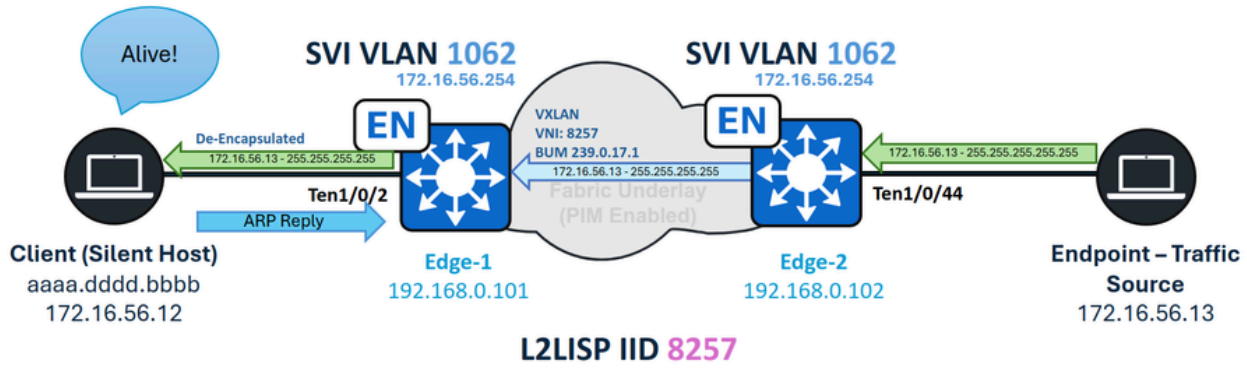
```
Edge-1#show spanning-tree interface TenGigabitEthernet 1/0/2

Vlan                Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------

VLAN1062

             Desg

FWD

 19        128.2    P2p Edge
```

Escenarios alternativos

Nodos periféricos y misma VLAN: inundación de capa 2

Si el objetivo es reactivar un host silencioso desde un dispositivo dentro del fabric en la misma VLAN que el host, no se requiere la función Difusión dirigida IP. En su lugar, la activación de la

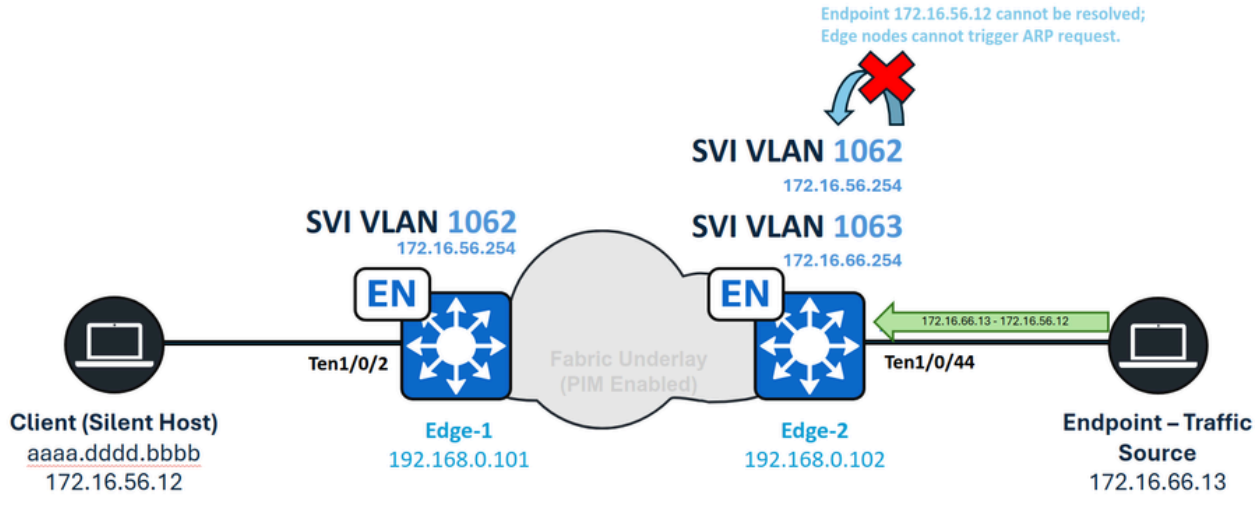
Inundación de Capa 2 (en un conjunto no inalámbrico) es suficiente para permitir el intercambio de paquetes de difusión, difusiones de subred o solicitudes ARP. Para la autenticación cerrada, se mantienen los requisitos de Wake-on-LAN.



Misma VLAN: gestión de host silenciosa

Nodos periféricos y VLAN diferente: unidifusión desconocida

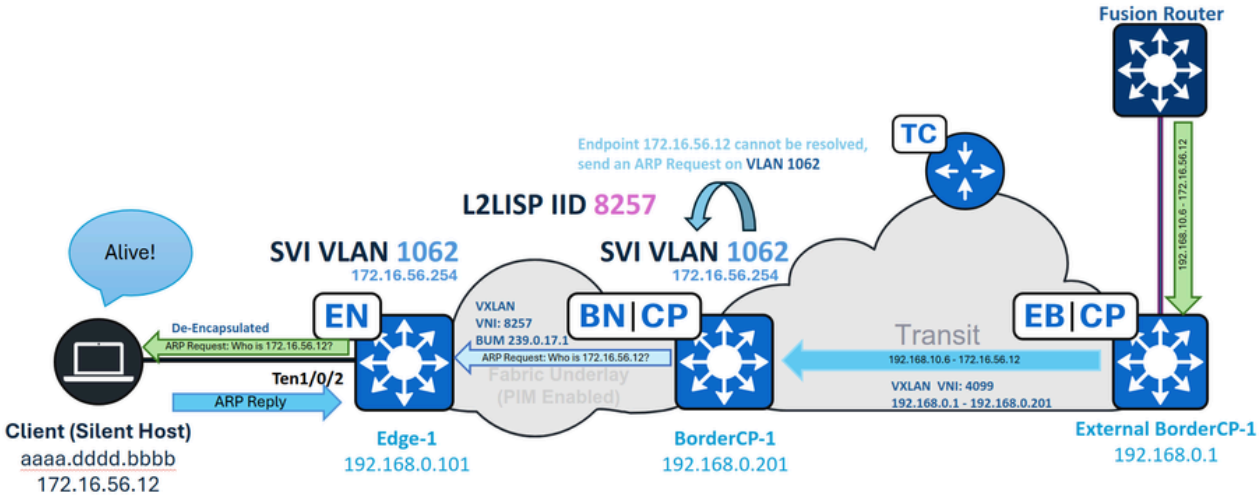
Cuando un terminal dentro del fabric envía tráfico de unidifusión a un host silencioso conectado a un nodo de fabric periférico, la ruta de reenvío de unidifusión desconocida no está disponible. A diferencia de los bordes del fabric, los nodos de borde del fabric tienen bordes definidos como LISP Proxy-ETR, que habilitan automáticamente una función de reenvío denominada "Señal y reenvío" cuando se detecta un terminal desconocido. El Fabric Edge debe activar la solicitud ARP requerida en el primer intento de resolver la dirección. Sin embargo, una vez que LISP identifica el punto final como un EID desconocido, los paquetes subsiguientes no activan solicitudes ARP adicionales. Este escenario se considera no compatible.



Unicast Inter-VLAN desconocido

Tránsito de acceso SD: unidifusión desconocida

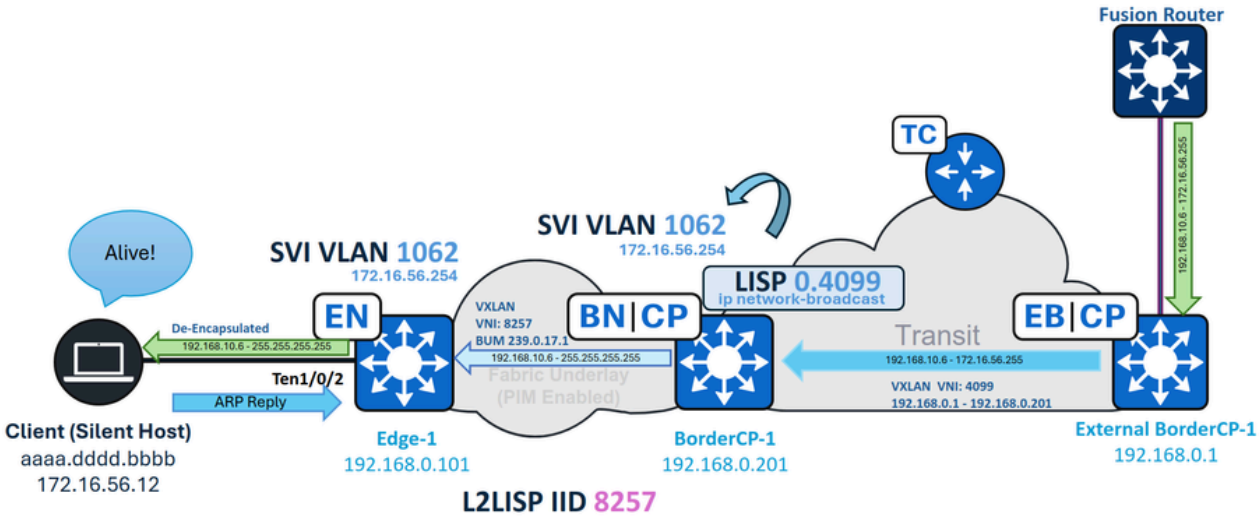
En el caso de SD-Access Transit, el tráfico unicast desconocido se soporta de forma nativa sin ningún requisito especial. El tráfico que se origina desde un borde remoto se rutea a través de la red de tránsito de acceso SD, con las difusiones de subred tratadas como tráfico ruteado regular. Cuando el tráfico alcanza el borde del sitio local, se realizan las operaciones estándar, incluidas la limpieza del tráfico, la inundación de solicitudes ARP y la resolución LISP.



SD-Access Transit Unknown Unicast

SD-Access Transit - Broadcast dirigido por IP

Cuando el tránsito de acceso SD está en uso, el borde del sitio local recibe la difusión dirigida IP en la subinterfaz LISP para la VPN (por ejemplo, la interfaz 4099), en lugar de en una SVI. Para asegurarse de que la función Difusión dirigida IP acepte y convierta la difusión en una difusión de subred, debe configurar manualmente el parámetro "ip network-broadcast" en la subinterfaz LISP.



IPDB de tránsito de acceso SD

En BorderCP-1 (límite de sitio local):

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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).