Konfigurieren der Funktion für direkten SD-Access-Host mit IP-Directed Broadcast

Inhalt

Einleitung

In diesem Dokument wird die Verwaltung von Silent Hosts in SD-Access sowie die Bewältigung von Verbindungsproblemen mithilfe von L2-Flooding und IP-basiertem Broadcast beschrieben.

Beschreibung

Die meisten Endpunkte und ihre Netzwerkschnittstellen übertragen regelmäßig Datenverkehr, insbesondere steuerungsrelevante Nachrichten wie ARP oder DHCP. Bestimmte Endpunkte reagieren jedoch nur, wenn sie dazu aufgefordert werden, anstatt Pakete in regelmäßigen Abständen zu senden. Diese Geräte senden Kontrollpakete nur auf Anforderung. In Netzwerken werden solche Endgeräte häufig als Silent Hosts bezeichnet. Im Kontext von SD-Access müssen

Silent Hosts den gesamten Datenverkehr unterbinden oder ihre Kommunikation einschränken, indem sie Control-Plane-Pakete zurückhalten.

In der SDA-Fabric werden Broadcasts entweder an jedem Edge-Knoten unterdrückt oder mithilfe von L2-Flooding an alle Edges weitergeleitet - ein Prozess, der in der Regel auf Edge-Knoten und L2-Grenzen beschränkt ist. Die Weiterleitung von Broadcasts an jeden Port in einem VLAN ähnelt dem Verhalten eines herkömmlichen Layer-2-Netzwerks, wodurch Silent Hosts deutlich aktiver bleiben. Die Verwaltung von stillen Hosts in einer Fabric-Umgebung ist jedoch mit Herausforderungen verbunden, da die fehlende regelmäßige Kommunikation die Authentifizierungsmechanismen, die Registrierung der Kontrollebene und die Weiterleitung unterbrechen kann.

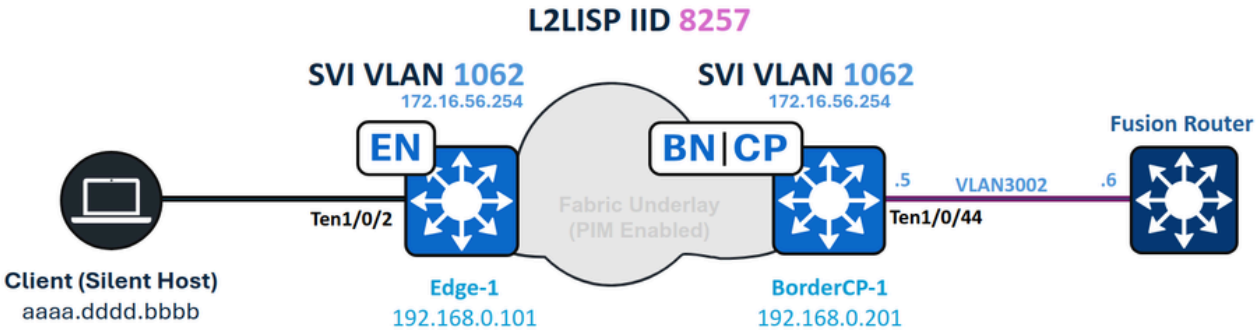
Durch die Aktivierung von L2-Flooding wird nur ein Teil des Problems behoben. Unbeaufsichtigte Hosts können Broadcast-Pakete nur dann empfangen, wenn diese von einem anderen Gerät generiert werden - entweder aus demselben VLAN innerhalb der Fabric oder von einer Fabric Border. Ein IP-gerichteter Broadcast bezieht sich auf ein IP-Paket, dessen Zieladresse auf die Broadcast-Adresse eines Subnetzes festgelegt ist, das von einem Host außerhalb dieses Subnetzes stammt. Für diese Funktion ist Multicast-Unterstützung im Underlay erforderlich. Wenn IP Directed Broadcast in der Fabric aktiviert ist, erreichen alle Subnetz-Broadcast-Pakete jeden Host in diesem Subnetz. Diese Funktion ermöglicht auch das Aktivieren von Geräten mithilfe von Standard-Unicast-Paketen und simuliert so effektiv das "unbekannte Unicast"-Verhalten, das in herkömmlichen Netzwerken zu finden ist.

Topologie

Hardware und Software

- Catalyst Switches der Serie 9000
- Catalyst Center Version 2.3.7.9
- Cisco IOS® XE 17.15.03 und höher (Border/CP & Edge)

Topologie:



Netzwerkdiagramm

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Internet Protocol (IP)-Weiterleitung
- Locator/ID Separation Protocol (LISP)
- Protocol Independent Multicast (PIM)
- Layer-2-Flooding in SD-Access

Anforderungen

- Diese Funktion erfordert Cisco Catalyst Center 1.3 oder höher
- Cisco IOS XE 17.3- und Cisco DNA Advantage-Lizenzen*
- Für ASR- und ISR-Grenzen ist Cisco IOS XE 17.3.1 oder höher erforderlich.
- Catalyst Switches der Serien 3000, 4000, 6000 oder Nexus 7000 werden nicht unterstützt

---

⚠ Vorsicht: Durch Aktivieren der Funktion "IP-Directed Broadcast" wird L2-Flooding automatisch aktiviert. Stellen Sie sicher, dass die Multicast-Funktion im Underlay korrekt funktioniert, bevor Sie diese Funktion aktivieren.

Sie können IP-Directed Broadcast nach dem Erstellen des IP-Pools aktivieren oder deaktivieren, ähnlich wie bei der Verwaltung von Wireless-Pools oder L2-Flooding-Einstellungen.

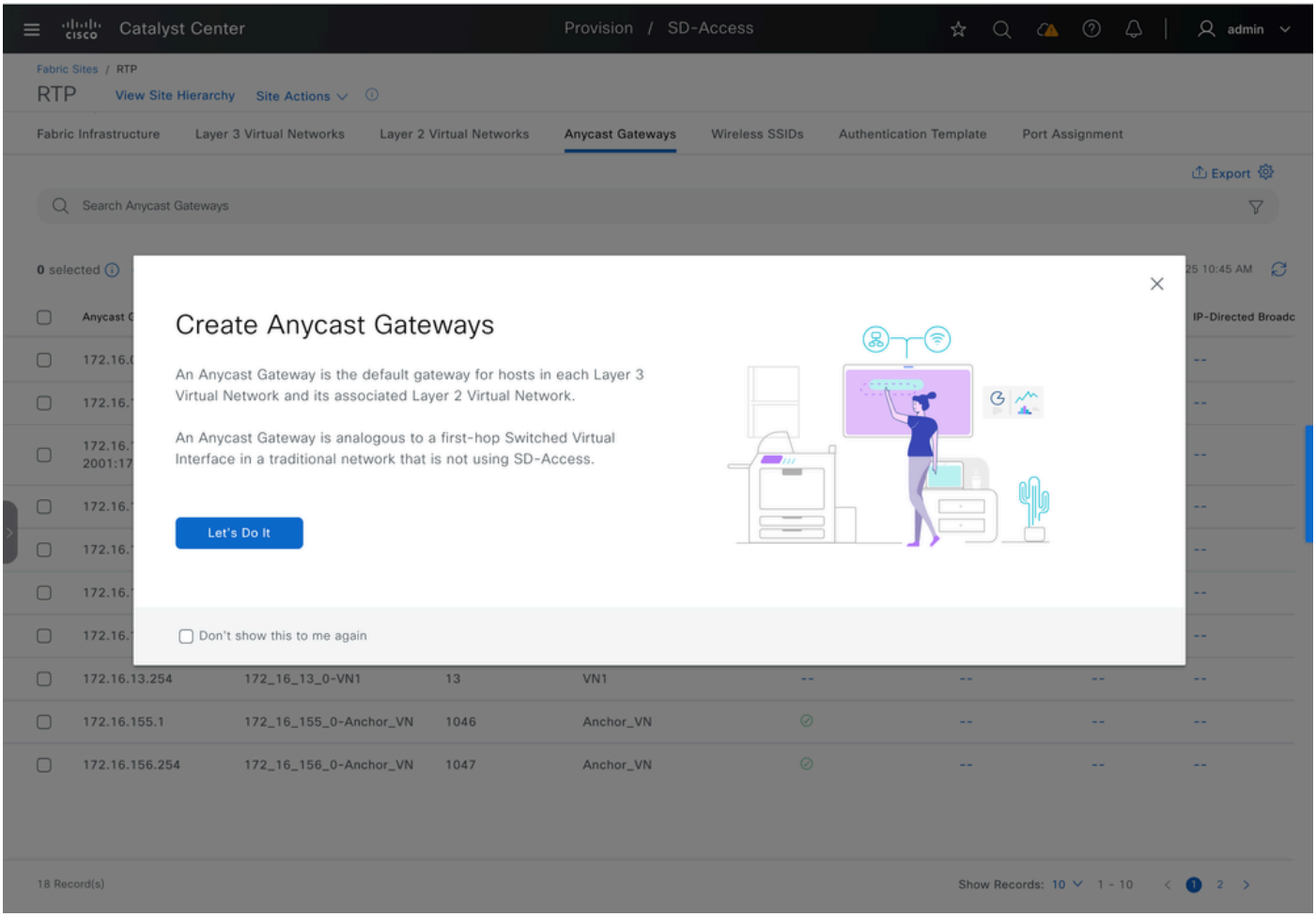
Catalyst Center-Konfiguration

Wenn "IP Directed Broadcast" aktiviert ist, leitet Catalyst Center eine Fabric-weite Bereitstellungsaufgabe ein. Alle Edge-Knoten, L2-Ränder und Ränder mit L3-Übergabe sind in diesem Bereitstellungsprozess enthalten.

So lösen Sie den IP-gesteuerten Broadcast-Workflow in der Benutzeroberfläche aus:

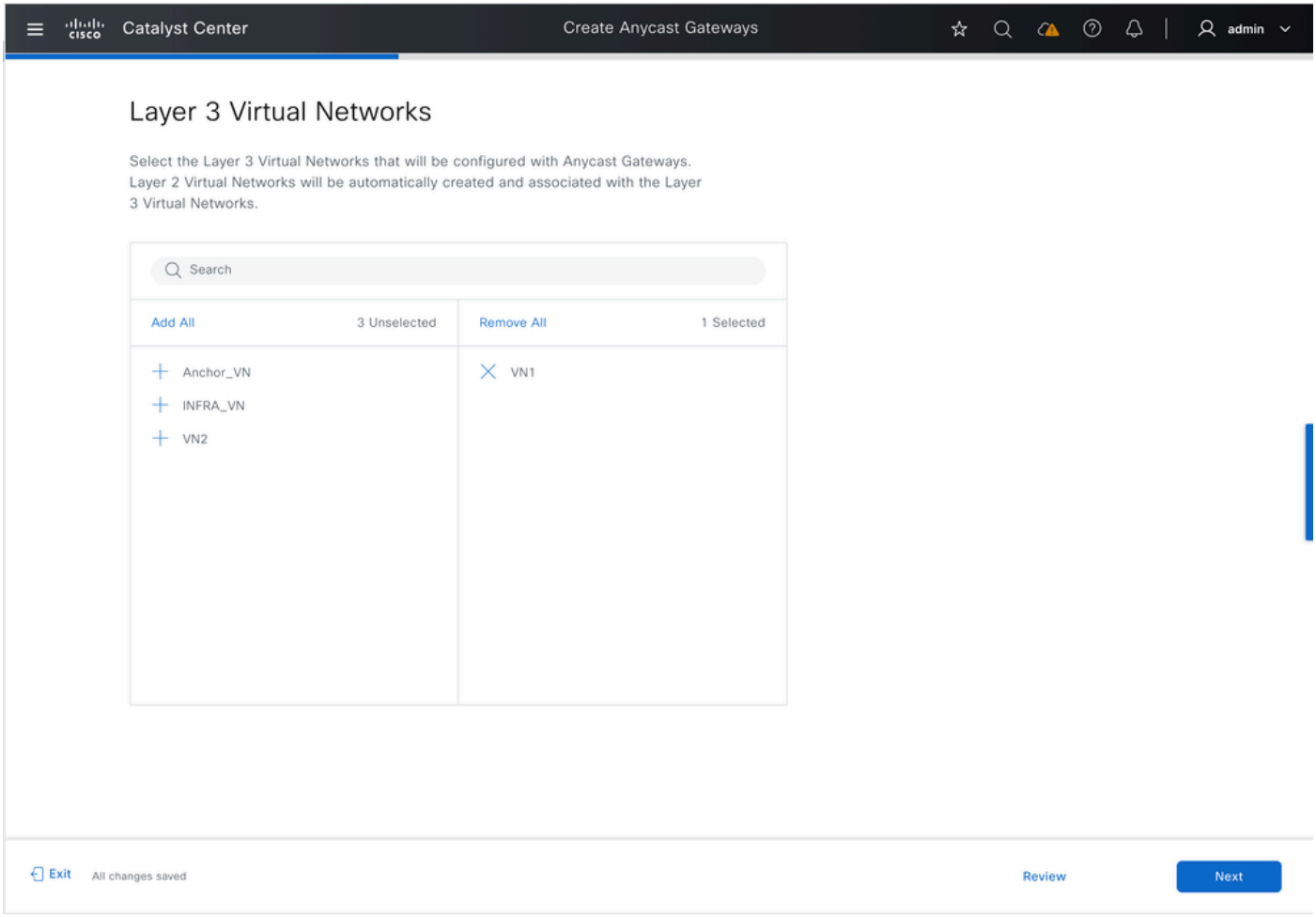
1. Gehen Sie zu Bereitstellung.
2. Wählen Sie Fabric-Standorte aus.
3. Wählen Sie den gewünschten Standort aus.
4. Navigieren Sie zu Anycast Gateways.

Von dort aus können Sie die erforderlichen Einstellungen für IP-Directed Broadcast konfigurieren.



Anycast-Gateways erstellen

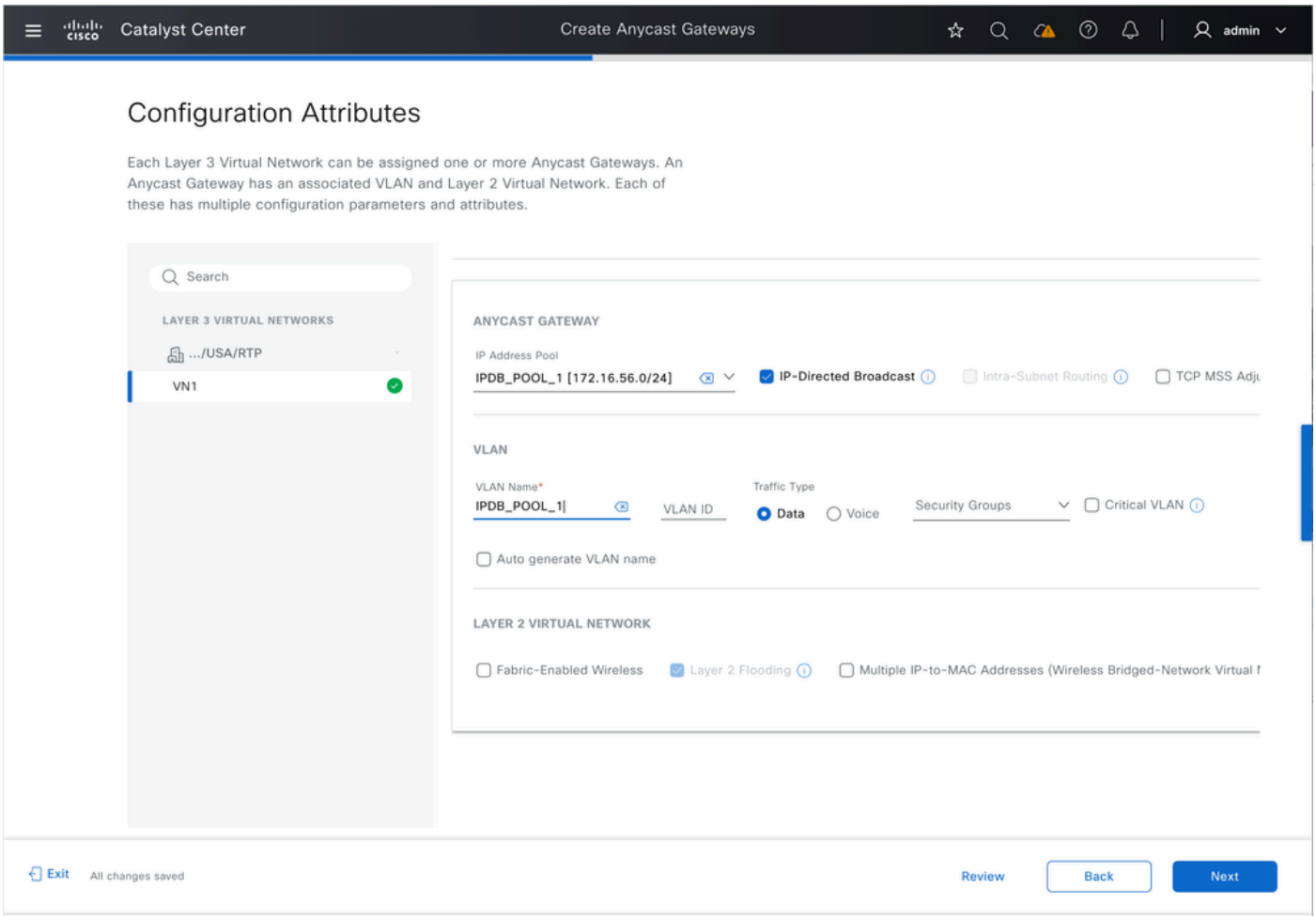
Wählen Sie das gewünschte virtuelle L3-Netzwerk aus, und klicken Sie dann auf Weiter, um fortzufahren.



Virtuelle L3-Netzwerke auswählen

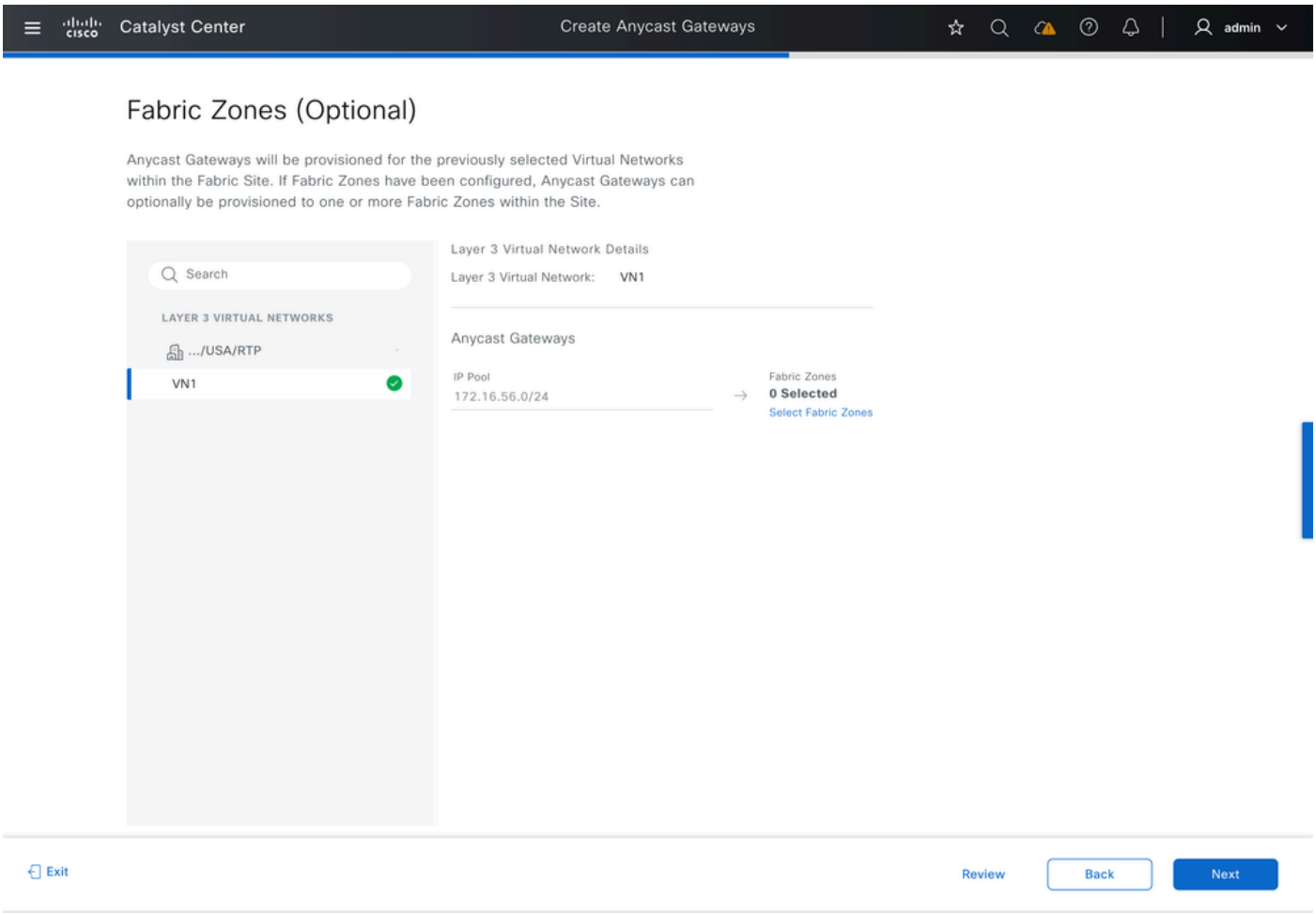
Wählen Sie den IP-Pool aus, aktivieren Sie IP-Directed Broadcast, und geben Sie den VLAN-Namen ein.

Tipp: Durch die Aktivierung von IP-Directed Broadcast wird L2-Flooding automatisch aktiviert.



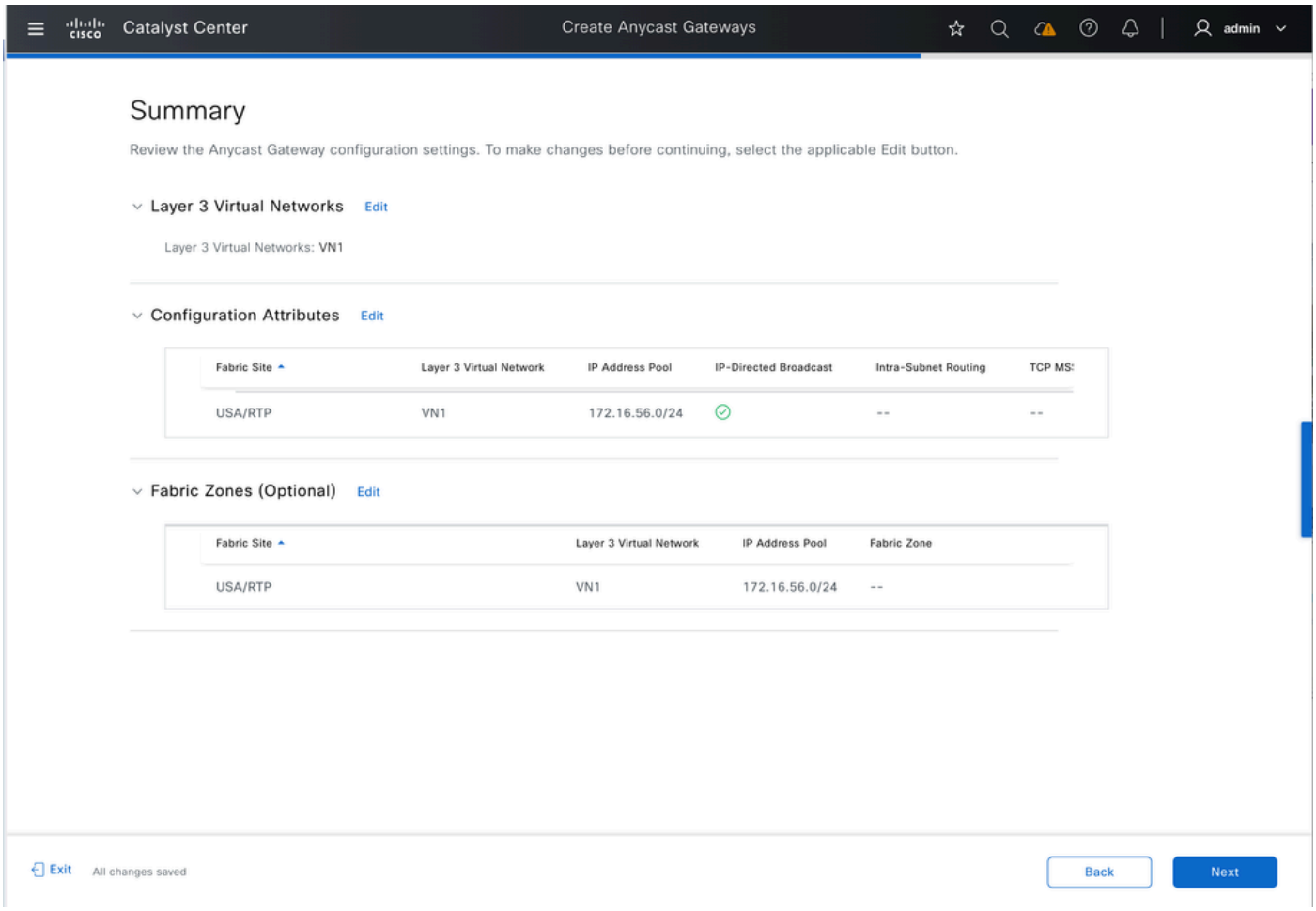
IP-Directed Broadcast aktivieren

Wenn Fabric-Zonen vorhanden sind, können Sie optional Anycast Gateways für eine oder mehrere Fabric-Zonen am Standort bereitstellen.



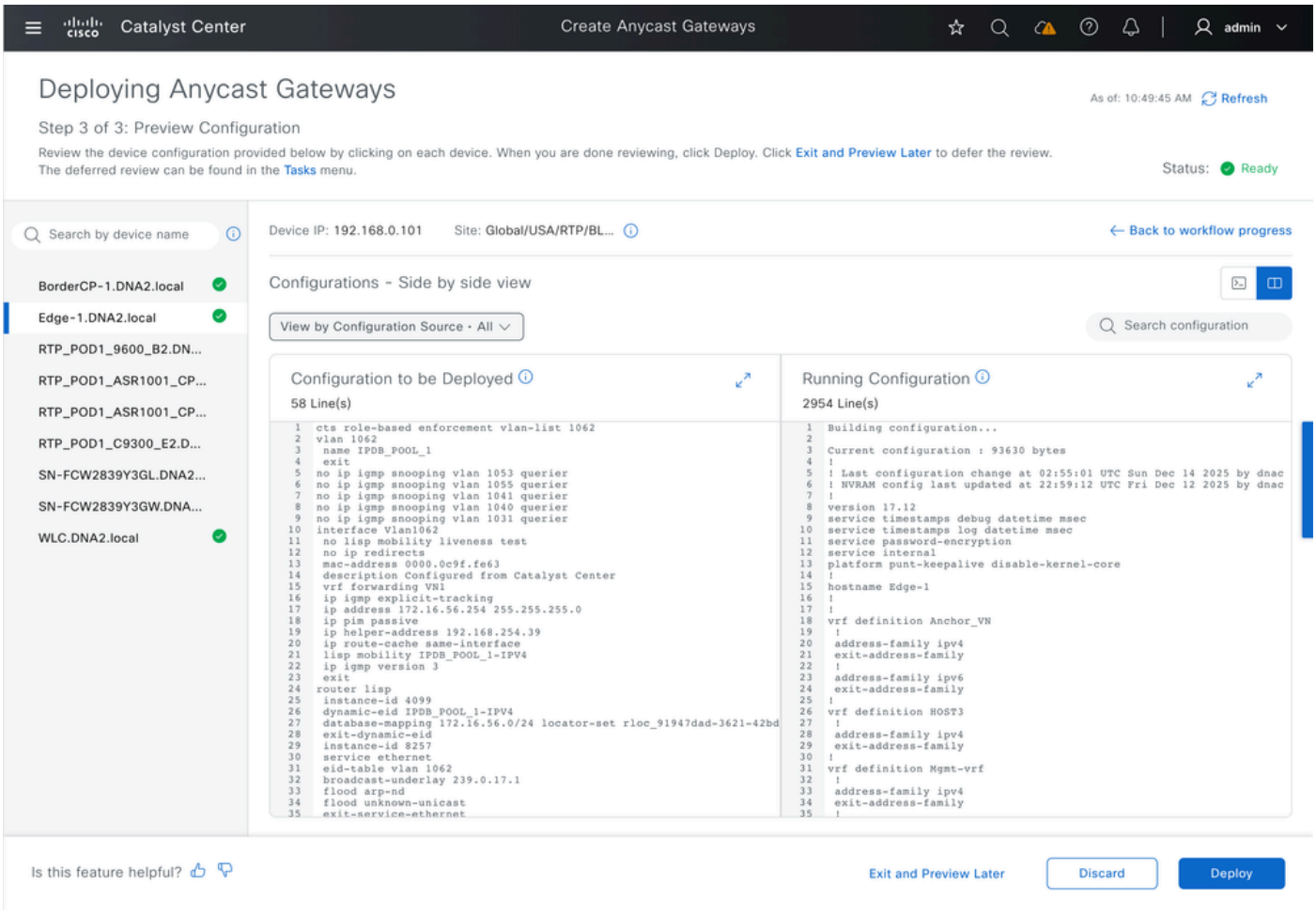
Fabric-Zonen auswählen

Überprüfen Sie die Zusammenfassung der konfigurierten Einstellungen auf Richtigkeit, bevor Sie mit der Bereitstellung fortfahren.



Zusammenfassung

Vorschau der generierten Konfigurationen anzeigen. Klicken Sie auf Deploy (Bereitstellen), um die Konfiguration auf die Fabric anzuwenden.



Konfigurationsvorschau

Konfiguration von Netzwerkgeräten

Grenzkonfiguration - IP-Transit

Bei konfigurierten Fabric-Grenzen mit IP-Transit sind die BGP-Peering-Schnittstellen mit "ip network-broadcast" konfiguriert, um die Weiterleitung von IP-Subnetz-Broadcasts zu ermöglichen. Die Anycast Gateway-IP für den Fabric-Pool (Endpunkt-VLAN) wechselt von einer Loopback-Schnittstelle zu einer SVI, für die "ip directed-broadcast" aktiviert ist. Beide Konfigurationen sind erforderlich, damit Fabric Border IP-Subnetz-Broadcast-Pakete in Full-Broadcast umwandelt und der Prozess wie vorgesehen funktioniert.

Konfiguration für IP-Netzwerk-Broadcast und IP-Netzwerk-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
```

Mit diesem zweiten Teil der Konfiguration kann die Funktion "IP Directed-Broadcast" automatische Hosts mithilfe einer ARP-Anforderung (Broadcast) aktivieren, ähnlich dem Verhalten traditioneller Netzwerke bei der Verarbeitung von unbekanntem Unicast-Datenverkehr. Bei dieser Konfiguration können Quellen außerhalb der Fabric Endpunkte mithilfe von Standard-Unicast-Datenverkehr aktivieren, ohne auf Subnetz-Broadcasts oder Wake-on-LAN ("Magic Packet") angewiesen zu sein.

<#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
```

Edge-Konfiguration

Die Konfiguration des Fabric-Edge-Knotens entspricht der eines kabelgebundenen Standardpools mit aktiviertem Layer-2-Flooding. Der CLI-Befehl "ip directed-broadcast" wird auf den Edge-

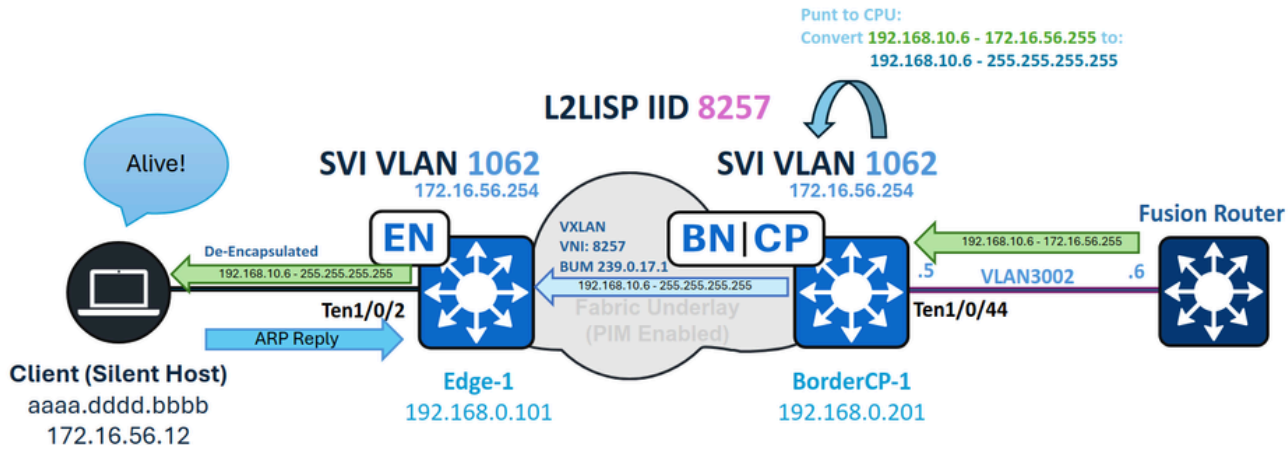
Knoten nicht angezeigt.

<#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



IPDB-Weiterleitung

Grenze - Umwandlung von Eingangs-CPU-Punt und Subnetz-Broadcast

In diesem Beispiel wird ein IP-Subnetz mit der Ziel-IP-Adresse 172.16.56.255 (die Broadcast-Adresse für den Pool 172.16.56.0/24) vom externen Netzwerk geroutet und erreicht zuerst die Fabric Border. Die Eingangs-Layer-3-Schnittstelle ist die IP Transit SVI (VLAN 3002). Da "ip network-broadcast" auf dieser Schnittstelle aktiviert ist, wird das Paket für die vollständige Broadcast-Umwandlung akzeptiert. ohne diese Konfiguration würde das Paket verworfen.

Das Paket erreicht die SVI 3002 und wird als Broadcast-Paket an die Switch-CPU gesendet. Bei konfigurierter IP-Netzwerk-Broadcast-Funktion wird das Paket zugelassen und in eine vollständige Broadcast-Funktion umgewandelt.

<#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
```

Während der CPU-Verarbeitung wandelt VLAN 1062 - die Zielschnittstelle - das Paket in eine vollständige Broadcast-Übertragung um, da sie mit "ip directed-broadcast" konfiguriert ist.

<#root>

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



 Directed broadcast forwarding is enabled
```

Sie können dieses Ereignis mit dem Befehl debug ip packet beheben. Um eine übermäßige Ausgabe und eine hohe Ressourcennutzung zu vermeiden, sollten Sie beim Ausführen dieses Debuggens immer eine Zugriffsliste als Filter anwenden.

<#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
```

Die Eingangsgrenze fungiert als Multicast-Quelle (S) und -Gruppe (G) für die BUM-Kapselung. Loopback 0 dient dabei als Quelladresse und die konfigurierte BUM-Gruppe als Ziel.

Stellen Sie auf der PIM-Kontrollebene sicher, dass in der Liste der ausgehenden Schnittstellen für die Multicast-Route ein Downlink zu den Fabric-Kanten angezeigt wird. Verwenden Sie für die Datenebene den Befehl show ip mfib count (Anzahl der mfib angezeigten Daten), um zu überprüfen, ob die Anzahl der Hardware-Weiterleitungszähler für den S,G-Eintrag im Rahmen steigt.

<#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
```

In diesem Dokument werden die Bildung von Multicast-Strukturen auf der Basis oder Layer-2-Flooding nicht im Detail erläutert. Bei fehlenden, unvollständigen oder falschen S,G-Zuständen muss der zugrunde liegende Multicast-Teil des Netzwerks unabhängig behoben werden.

Edge - Eingangs-Broadcast

An Fabric-Edges wird der in VXLAN auf Multicast gekapselte eingehende Broadcast entkapselt und an das mit dem VNI verknüpfte VLAN weitergeleitet (8257), wobei alle Ports im Weiterleitungsstatus im Spanning-Tree erreicht werden.

Überprüfen Sie zunächst, ob der S,G-Eintrag an der Grenze (mit dem Border-Loopback als Quelle) für die BUM-Gruppe vorhanden ist, und leiten Sie den Datenverkehr weiter. Verwenden Sie die gleichen mroute- und mfib-Befehle, um dies zu überprüfen. Stellen Sie sicher, dass die L2LISP-Subschnittstelle, die dem VLAN (1062) entspricht, als ausgehende Schnittstelle aufgeführt ist.

<#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
```

Nach der Entkapselung wird das Paket über VLAN 1062 an alle diesem VLAN zugewiesenen Ports weitergeleitet.

<#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
```

Nachdem der Endpunkt das Broadcast-Paket empfangen hat, muss er es als relevant erkennen und antworten. Das Ergebnis ist, dass der Endpunkt ein ARP-Paket senden kann, das die Geräteverfolgungstabelle auf dem Switch aktualisiert.

<#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
```

Nachdem der Endpunkt bei der Geräteverfolgung erneut registriert wurde, wird er in die LISP-Datenbank des Edge-Knotens importiert und anschließend auf der Kontrollebene registriert.

Bei LISP-Pub-Sub-Bereitstellungen veröffentlicht die Kontrollebene die neu registrierten Endpunktinformationen an den Grenzen und erstellt sofort einen LISP-Map-Cache-Eintrag, um den Datenverkehr an den entsprechenden Edge-Knoten weiterzuleiten.

<#root>

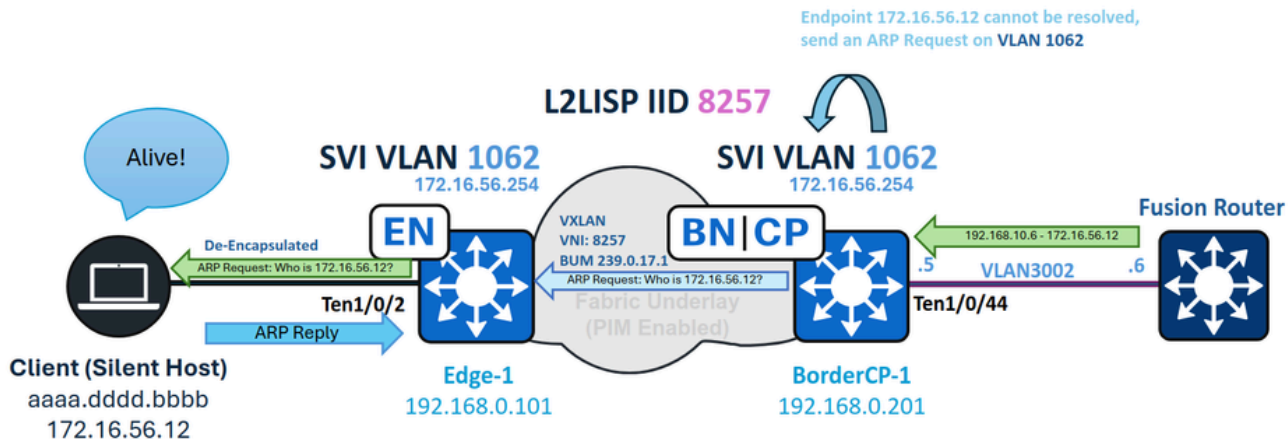
```
BorderCP-1#show lisp instance-id 4099 ipv4 map 172.16.56.12/32

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)
```

Bei LISP/BGP (SDA 1.0)-Bereitstellungen kann die Aktualisierung des LISP-Zuordnungscaches für einen unbekannten Endpunkt bis zu einer Minute dauern, wenn die Bereitstellung verteilt (nicht angeordnet) ist, da die Negative Map Replies (NMRs) zuerst ablaufen müssen.

Ein stummer Host muss Pakete wie Subnetz-Broadcasts ignorieren, wenn er nicht dafür programmiert ist, darauf zu reagieren. Einige Endgeräte benötigen ein "Magic Packet" (z. B. ein UDP-Echo), während andere nur auf ein Broadcast-ARP reagieren. Der unbeaufsichtigte Host selbst bestimmt, welche Paketart ihn zum Aufwachen veranlasst. Eine der am häufigsten verwendeten Optionen ist eine ARP-Anforderung, die im Abschnitt Unicast Forwarding (Unbekannte Unicast-Weiterleitung) beschrieben wird.

Unbekannte Unicast-Weiterleitung



Unbekannte Unicast-Weiterleitung

Wenn ein Pool für IP-Directed-Broadcast aktiviert ist, ermöglicht er nicht nur die Verarbeitung von Subnetz-Broadcasts, sondern auch die Funktion von Fabric Borders als Gateways für die Weiterleitung von unbekanntem Unicast-Datenverkehr. In diesem Zusammenhang bezieht sich unbekannter Unicast-Datenverkehr auf Pakete, die für Endpunkte bestimmt sind, die derzeit nicht auf der Kontrollebene registriert sind.

Ähnlich wie ein herkömmliches Netzwerk-Gateway, das eine ARP-Anfrage sendet, wenn ein unvollständiger ARP-Eintrag auftritt, generiert der Border eine ARP-Anfrage und überflutet sie an alle Fabric-Knoten. Dadurch wird sichergestellt, dass der unbeaufsichtigte Host die Anforderung erhält, sie aktiviert und eine ARP-Antwort sendet, sodass er sich erneut auf der Kontrollebene registriert.

Diese Funktionalität ist möglich, da das Endpunkt-VLAN (1062) sowohl als SVI als auch als L2LISP-Instanz an der Fabric Border konfiguriert ist. Wenn "flood arp-nd" in der L2-ID aktiviert ist,

kann die Border ARP-Anforderungen überfluten, die von der SVI generiert werden, wenn Datenverkehr an eine unbekannte LISP-EID weitergeleitet wird. So wird sichergestellt, dass stille Hosts die ARP-Anforderung empfangen und die Möglichkeit haben, ihre Registrierung auf der Kontrollebene zu beantworten und zu aktualisieren.

<#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
```

Wenn die Fabric Border ein Paket empfängt, das für 172.16.56.12 auf SVI 3002 - das Teil des Endpunkts VN/VRF ist - bestimmt ist, versucht sie die LISP-Auflösung, da die CEF-Ausgabe auf "Glean" gesetzt ist (d. h. das Gerät versucht, die Ziel-Adjacency mithilfe des Downstream-Layer-Protokolls aufzulösen). Dieser Prozess löst gleichzeitig eine LISP-Map-Request und eine ARP-Auflösung für den nicht registrierten Host aus.

<#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

Es wird ein unvollständiger ARP-Eintrag erstellt, der Border dazu auffordert, eine ARP-Anforderung an den unbekannten Endpunkt 172.16.56.12 zu senden. Diese ARP-Anforderung wird als Broadcast-Paket mithilfe von Layer-2-Flooding und der Flood-ARP-ND-Funktion nach unten weitergeleitet.

Überwachen Sie die MFIB-Zähler für das lokale S,G der Grenze, um sicherzustellen, dass Layer-2-Flooding funktioniert.

<#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

Das geflutete ARP-Paket erreicht den automatischen Host, aktiviert es und fordert eine ARP-Antwort an. Diese Antwort aktualisiert die SISF-Tabelle (Device Tracking) am Fabric Edge und

erstellt einen LISP-Datenbankeintrag. Daher initiiert der Fabric-Edge eine Registrierung auf der Kontrollebene.

<#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
```

Nachdem der Endpunkt bei der Geräteverfolgung erneut registriert wurde, wird er in die LISP-Datenbank des Edge-Knotens importiert und anschließend auf der Kontrollebene registriert.

Bei LISP-Pub-Sub-Bereitstellungen veröffentlicht die Kontrollebene die neu registrierten Endpunktinformationen an den Grenzen und erstellt sofort einen LISP-Map-Cache-Eintrag, um den Datenverkehr an den entsprechenden Edge-Knoten weiterzuleiten.

<#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)
```

Bei LISP/BGP (SDA 1.0)-Bereitstellungen kann die Aktualisierung des LISP-Zuordnungscaches für einen unbekannten Endpunkt bis zu einer Minute dauern, wenn die Bereitstellung verteilt (nicht angeordnet) ist, da die Negative Map Replies (NMRs) zuerst ablaufen müssen.

Tipp: Die Grenze löst ARP für den unbeaufsichtigten Host nie auf. nur die Endpunktregistrierung erforderlich ist. Wenn der stumme Host antwortet, wird das ARP-Paket als Layer-2-Unicast gesendet, sodass es nicht an die Grenze geleitet wird. Erwarten Sie daher keinen ARP- oder Device-Tracking-Eintrag an der Grenze.

Aktivieren von Wake-on-LAN in Authentifizierungsvorlagen

Wenn für Fabric-Benutzer "Keine Authentifizierung" aktiviert ist, erreichen geflutete Pakete von der Grenze stille Hosts, solange der Port Teil des VLAN ist, in dem Flooding aktiviert ist. Mit Closed Authentication (insbesondere Closed Authentication) werden jedoch zwei Hauptfaktoren von Bedeutung.

Manuelle VLAN-Zuweisung für den Host vor der Authentifizierung

Wenn kein VLAN zugewiesen ist, empfängt der Port keine gefluteten Pakete von seinem designierten VLAN. Wird erwartet, dass ein VLAN über RADIUS zugewiesen wird, entsteht ein "Chicken or the Egg?" Dilemma: Das geflutete Paket kann nicht an ein anderes VLAN (auch als VLAN-Hopping bezeichnet) weitergeleitet werden, um die Benutzerauthentifizierung auszulösen und eine VLAN-Zuweisung von RADIUS abzurufen.

Wenn das Gerät bei der Konfiguration des Ports beim Host-Onboarding als "stumm" erkannt wird, weisen Sie das VLAN manuell über das Dropdown-Menü für die DATA-Pools zu.

Das Problem, dass sich unbeaufsichtigte Hosts vor der VLAN-Zuweisung nicht authentifizieren können, ist nicht ausschließlich auf SD-Access beschränkt. Es handelt sich hierbei um eine

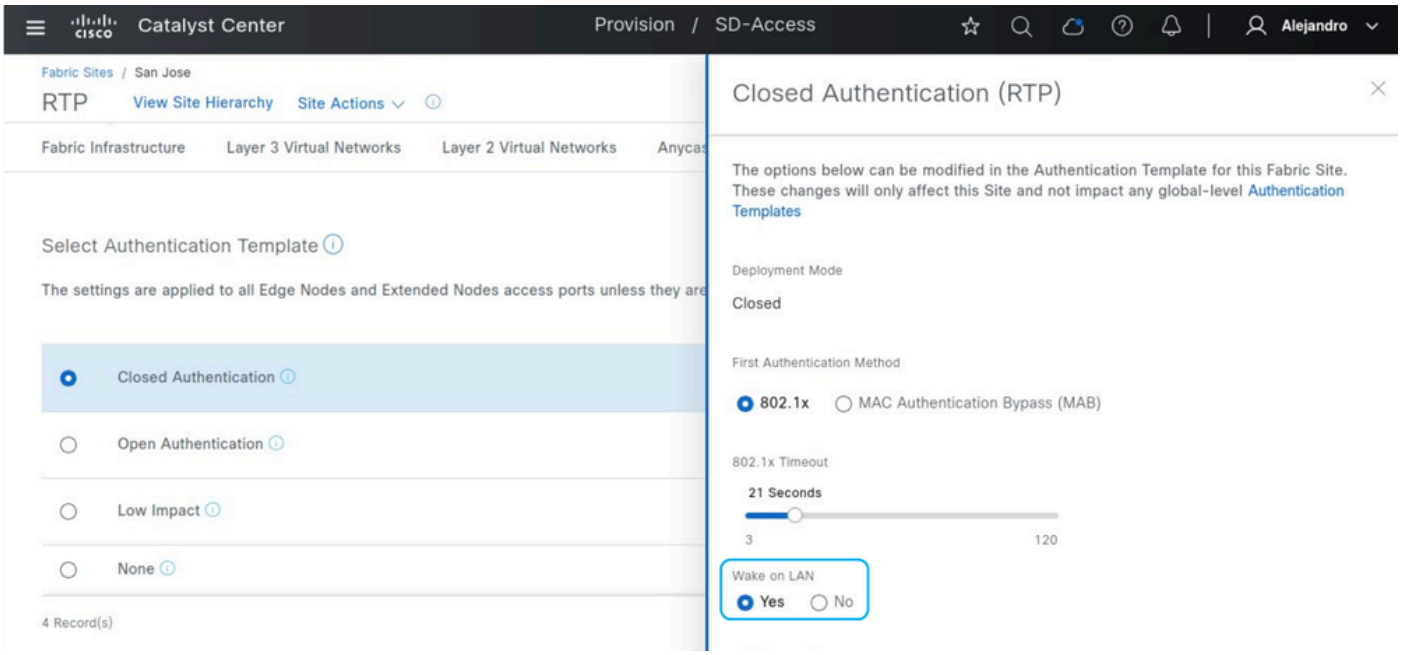
häufige Designherausforderung, die in einem herkömmlichen sicheren Netzwerk anzutreffen ist.

<#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
```

Zugriffskontrollrichtung

Wenn Wake-on-LAN in den Authentifizierungsvorlageneinstellungen innerhalb von Host-Onboarding nicht aktiviert ist, verwenden Authentifizierungsvorlagen standardmäßig sowohl die Zugriffssitzungssteuerungsrichtung als auch die Zugriffssteuerungsrichtung. Bei dieser Konfiguration verwirft der Port sowohl eingehende Pakete als auch Pakete, die vom Port weitergeleitet werden. Wenn Wake-on-LAN aktiviert ist, ändert sich die Einstellung in "access-session control-direction in", wodurch nur der eingehende Datenverkehr eingeschränkt wird. Durch diese Anpassung können Pakete den unbeaufsichtigten Host erreichen und aktivieren, sodass dieser die MAB-Authentifizierung initiieren kann.



Wake on LAN

Ohne 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
```

Vor der Authentifizierung des Endpunkts wird die ihm zugewiesene Schnittstelle in den Spanning Tree-Status nicht als Flooding-aktiviert aufgeführt.

<#root>

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


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

Bei Aktivierung von Wake on LAN:

<#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
```

Bereits vor der Authentifizierung wird der Port für den ausgehenden Datenverkehr aktiviert, sodass Pakete den automatischen Host erreichen und aktivieren können.

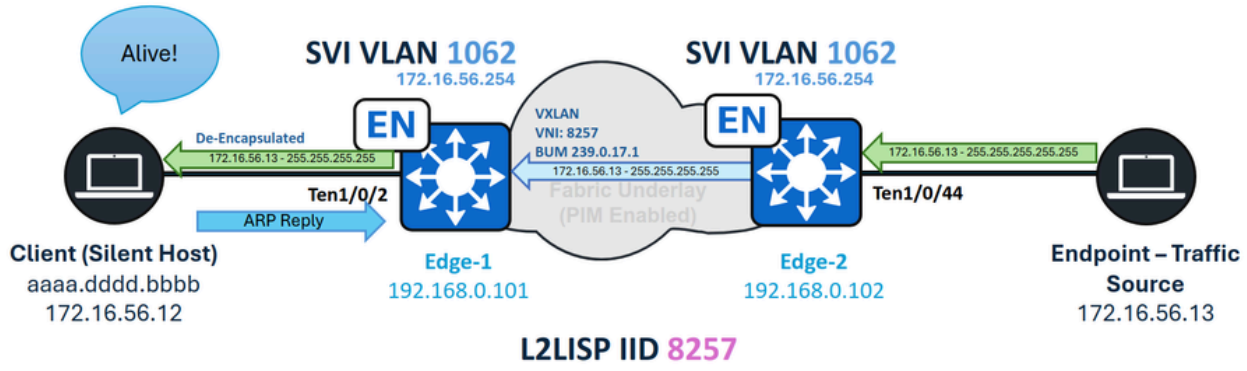
<#root>

```
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
```

Alternative Szenarien

Edge-Knoten und dasselbe VLAN - Layer-2-Flooding

Wenn das Ziel darin besteht, einen unbeaufsichtigten Host von einem Gerät innerhalb der Fabric auf demselben VLAN wie den Host zu aktivieren, ist die Funktion "IP Directed Broadcast" nicht erforderlich. Stattdessen reicht die Aktivierung von Layer-2-Flooding (in einem nicht drahtlosen Pool) aus, um den Austausch von Broadcast-Paketen, Subnetz-Broadcasts oder ARP-Anfragen zu ermöglichen. Für die geschlossene Authentifizierung gelten die Wake-on-LAN-Anforderungen.

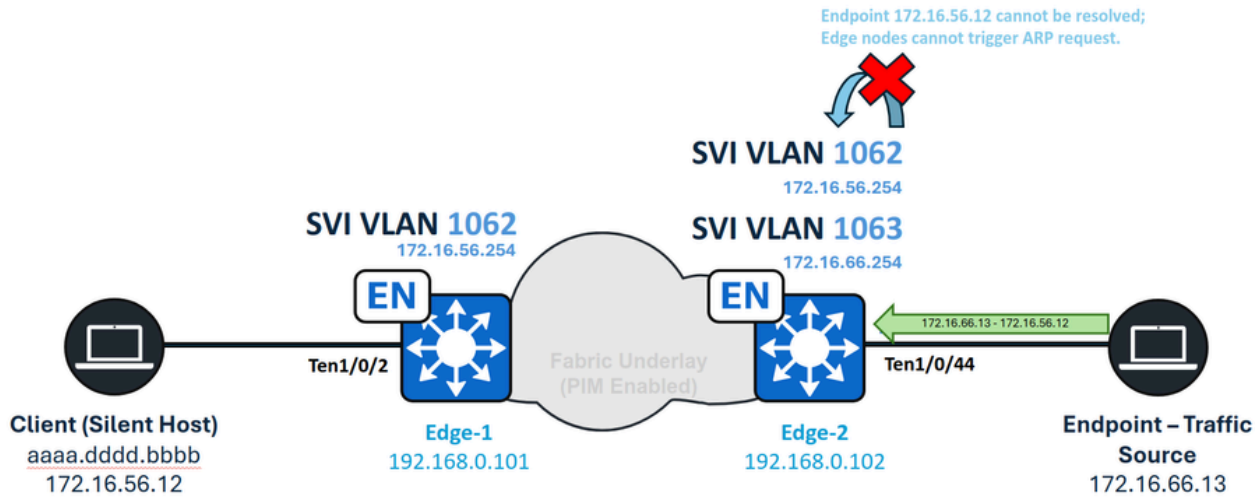


Gleiches VLAN - Silent Host-Verarbeitung

Edge-Knoten und anderes VLAN - Unbekanntes Unicast

Wenn ein Endpunkt innerhalb der Fabric Unicast-Datenverkehr an einen unbeaufsichtigten Host sendet, der mit einem Fabric Edge-Knoten verbunden ist, ist der Unicast-Weiterleitungspfad nicht verfügbar. Im Gegensatz zu Fabric Borders verfügen Fabric Edge-Knoten über Borders, die als

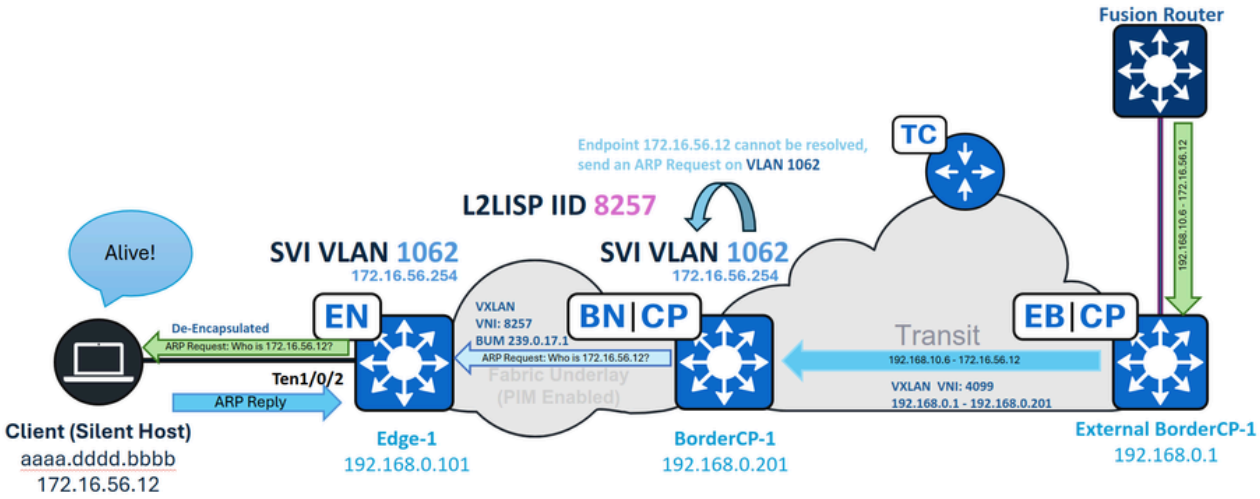
LISP-Proxy-ETRs definiert sind. Diese aktivieren automatisch eine Weiterleitungsfunktion mit der Bezeichnung "Signal & Forward", wenn ein unbekannter Endpunkt erkannt wird. Der Fabric-Edge muss beim ersten Versuch, die Adresse aufzulösen, die erforderliche ARP-Anforderung auslösen. Sobald LISP den Endpunkt jedoch als unbekannte EID identifiziert hat, lösen nachfolgende Pakete keine weiteren ARP-Anforderungen aus. Dieses Szenario wird als nicht unterstützt betrachtet.



Unbekanntes Unicast-Inter-VLAN

SD-Access-Transit - Unbekannt Unicast

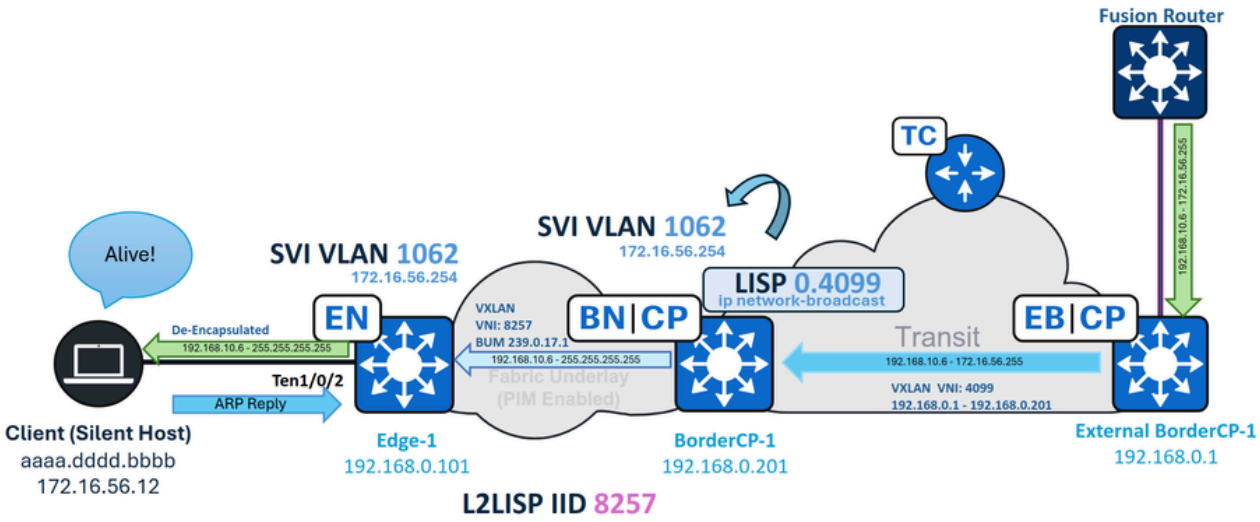
Bei einem SD-Access-Transit wird unbekannter Unicast-Datenverkehr nativ und ohne besondere Anforderungen unterstützt. Datenverkehr, der von einer Remote-Grenze ausgeht, wird über das SD-Access Transit-Netzwerk geleitet, wobei Subnetz-Broadcasts als regulärer gerouteter Datenverkehr behandelt werden. Wenn der Datenverkehr die lokale Standortgrenze erreicht, werden Standardvorgänge ausgeführt, darunter Traffic Glean, ARP Request Flooding und LISP Resolution.



SD-Zugriffstransit unbekannt Unicast

SD-Access-Transit - IP-Directed Broadcast

Wenn ein SD-Access-Transit verwendet wird, empfängt der lokale Border den IP-Directed Broadcast über die LISP-Subschnittstelle für das VPN (z. B. Schnittstelle 4099) und nicht über eine SVI. Um sicherzustellen, dass der Broadcast akzeptiert und von der Funktion "IP Directed Broadcast" in ein Subnetz konvertiert wird, müssen Sie den Parameter "ip network-broadcast" auf der LISP-Subschnittstelle manuell konfigurieren.



SD-Zugangs-Transit-IPDB

An BorderCP-1 (lokale Standortgrenze):

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.