

# IPダイレクトブロードキャスト機能を使用したSDアクセスサイレントホストの設定

## 内容

---

[はじめに](#)

[説明](#)

[トポロジ](#)

[ハードウェアとソフトウェア](#)

[要件](#)

[要件](#)

[Catalyst Centerの設定](#)

[ネットワークデバイスの設定](#)

[IPダイレクトブロードキャストフォワーディング](#)

[境界 – 入力CPUパントおよびサブネットブロードキャスト変換](#)

[Edge : 入力ブロードキャスト](#)

[不明なユニキャスト転送](#)

[認証テンプレートでのWake-on-LANの有効化](#)

[認証前のホストの手動VLAN割り当て](#)

[アクセス制御方向](#)

[代替シナリオ](#)

[エッジノードと同一VLAN – レイヤ2フラッディング](#)

[エッジノードと異なるVLAN – 不明なユニキャスト](#)

[SDアクセス中継 – 不明なユニキャスト](#)

[SDアクセス中継 – IPダイレクトブロードキャスト](#)

## はじめに

このドキュメントでは、SD-Accessでのサイレントホストの管理と、L2フラッディングおよびIPダイレクトブロードキャストを使用した接続の課題への対処について説明します。

## 説明

ほとんどのエンドポイントとそのネットワークインターフェイスは、特にARPやDHCPなどの制御関連のメッセージを定期的にトラフィックを送信します。ただし、特定のエンドポイントは、定期的にパケットを送信するのではなく、プロンプトが表示されたときにのみ応答します。これらのデバイスは、オンデマンドベースでのみ制御パケットを送信します。ネットワークでは、このようなエンドポイントは一般にサイレントホストと呼ばれます。SDアクセスのコンテキスト

トにおいて、サイレントホストは、コントロールプレーンパケットを保留することにより、すべてのトラフィックを停止するか、通信を制限する必要があります。

SDAファブリックでは、ブロードキャストは各エッジノードで抑制されるか、L2フラッディングを使用してすべてのエッジに転送されます。このプロセスは通常、エッジノードとL2ボーダーに限定されます。VLAN上のすべてのポートにブロードキャストを転送することは、従来のレイヤ2ネットワークの動作を模倣しており、サイレントホストがアクティブな状態を維持するのに大きく役立ちます。ただし、ファブリック環境でのサイレントホストの管理には課題があります。これは、サイレントホストの定期的な通信の欠如が、認証メカニズム、コントロールプレーンの登録、および転送を中断させる可能性があるためです。

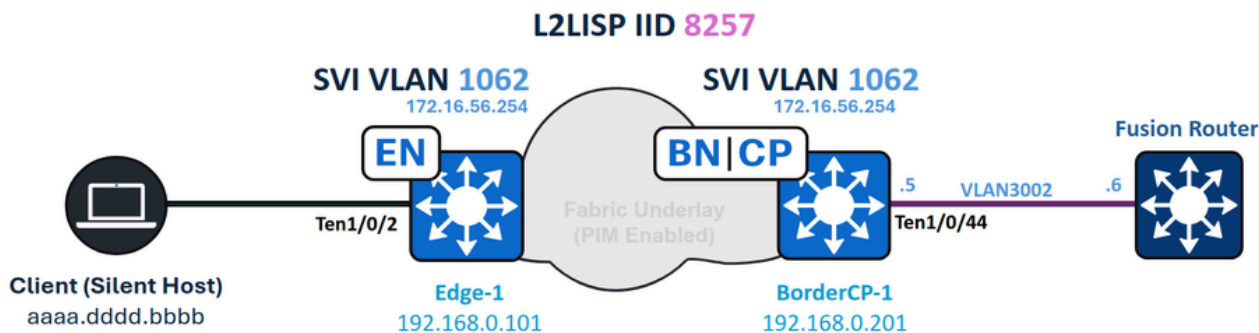
L2フラッディングを有効にすると、問題の一部にしか対処できません。サイレントホストがブロードキャストパケットを受信できるのは、ファブリック内の同じVLAN内またはファブリックボーダーから別のデバイスがブロードキャストパケットを生成した場合だけです。IPダイレクトブロードキャストとは、サブネットのブロードキャストアドレスに設定された宛先アドレスを持つIPパケットのことで、そのサブネットの外部にあるホストから発信されます。この機能には、アンダーレイでのマルチキャストサポートが必要です。IPダイレクトブロードキャストがファブリックで有効になっている場合、すべてのサブネットブロードキャストパケットはそのサブネット内のすべてのホストに到達します。この機能は、標準のユニキャストパケットを使用してデバイスをウェイクアップさせることもでき、従来のネットワークで見られる「未知のユニキャスト」動作を効果的にシミュレートします。

## トポロジ

### ハードウェアとソフトウェア

- Catalyst 9000 シリーズ スイッチ
- Catalyst Centerバージョン2.3.7.9
- Cisco IOS® XE 17.15.03以降 ( Border/CPおよびEdge )

トポロジ :



ネットワーク図

## 要件

次の項目に関する知識があることが推奨されます。

- インターネットプロトコル(IP)転送
- ローター/ID分離プロトコル(LISP)
- Protocol Independent Multicast ( PIM )
- SDアクセスでのレイヤ2フラッディング

## 要件

- この機能を使用するには、Cisco Catalyst Center 1.3以降が必要です
- Cisco IOS XE 17.3およびCisco DNA Advantageライセンス\*
- ASRとISRの境界には、Cisco IOS XE 17.3.1以降が必要です
- Catalyst 3000、4000、6000シリーズスイッチまたはNexus 7000はサポートされません



注意:IPダイレクトブロードキャスト機能を有効にすると、L2フラッディングが自動的にアクティブになります。この機能を有効にする前に、アンダーレイのマルチキャスト機能が正しく動作していることを確認してください。

IPプールの作成後は、ワイヤレスプールの管理やL2フラッディング設定と同様に、IPダイレクトブロードキャストを有効または無効にすることができます。

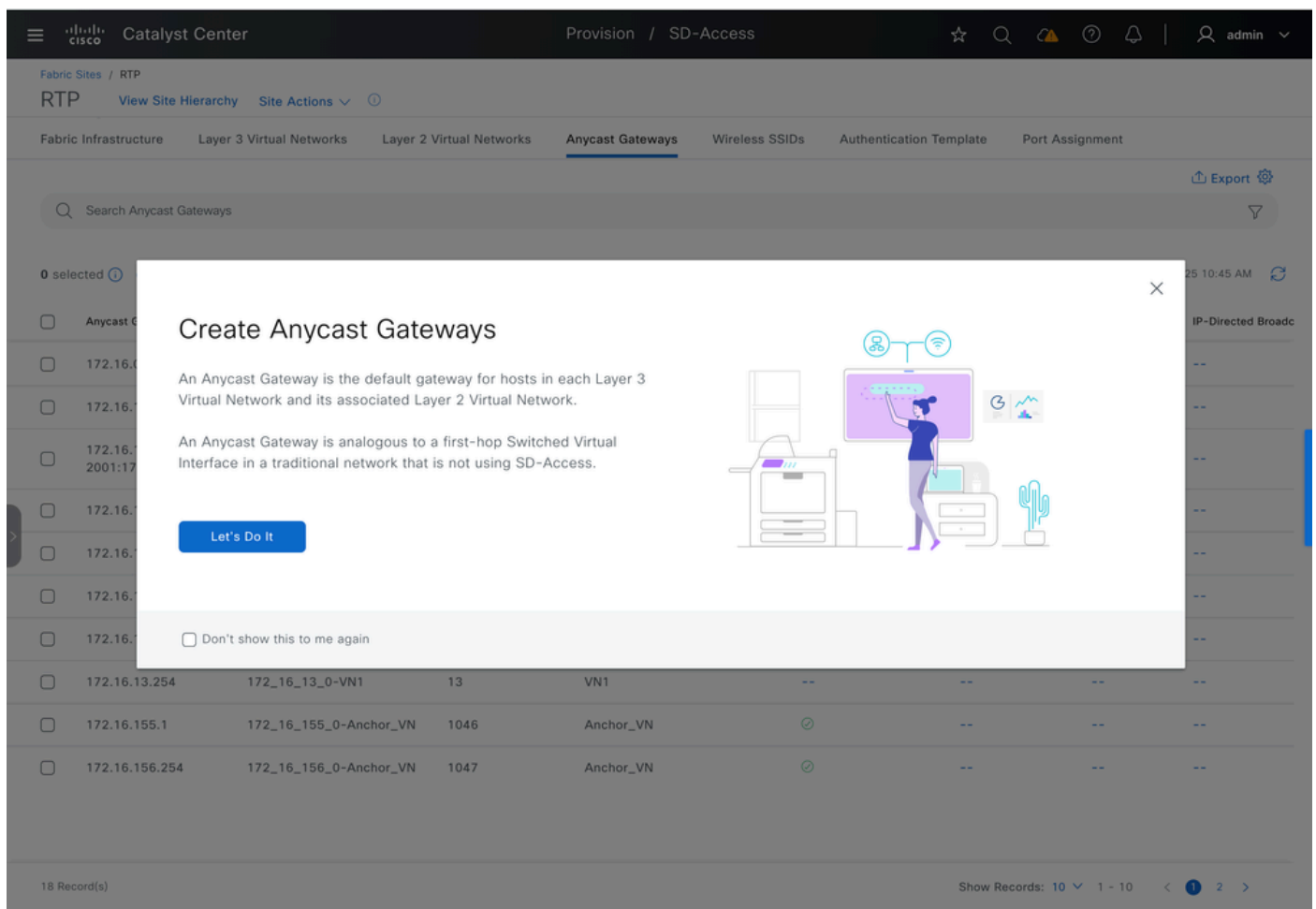
## Catalyst Centerの設定

IPダイレクトブロードキャストをイネーブルにすると、Catalyst Centerではファブリック全体のプロビジョニングタスクが開始されます。このプロビジョニングプロセスには、すべてのエッジノード、L2境界、およびL3ハンドオフ付きの境界が含まれます。

UIでIPダイレクトブロードキャストワークフローをトリガーするには、次の手順を実行します。

1. Provisionに移動します。
2. Fabric Sitesを選択します。
3. 目的のサイトを選択します。
4. Anycast Gatewaysに移動します。

そこから、IPダイレクトブロードキャストに必要な設定を行うことができます。



The screenshot shows the Cisco Catalyst Center interface with a modal dialog titled "Create Anycast Gateways". The dialog contains the following text:

**Create Anycast Gateways**

An Anycast Gateway is the default gateway for hosts in each Layer 3 Virtual Network and its associated Layer 2 Virtual Network.

An Anycast Gateway is analogous to a first-hop Switched Virtual Interface in a traditional network that is not using SD-Access.

[Let's Do It](#)

Don't show this to me again

The background shows a table of Anycast Gateways with columns for IP address, Name, ID, and other details. The table has 18 records.

エニーキャストゲートウェイの作成

目的のL3仮想ネットワークを選択し、Nextをクリックして続行します。

## Layer 3 Virtual Networks

Select the Layer 3 Virtual Networks that will be configured with Anycast Gateways. Layer 2 Virtual Networks will be automatically created and associated with the Layer 3 Virtual Networks.

Search	
<a href="#">Add All</a>	3 Unselected
<a href="#">Remove All</a>	1 Selected
<a href="#">+</a> Anchor_VN	<a href="#">×</a> VN1
<a href="#">+</a> INFRA_VN	
<a href="#">+</a> VN2	

[Exit](#) All changes saved

[Review](#)

[Next](#)

L3仮想ネットワークの選択

IPプールを選択し、IPダイレクトブロードキャストを有効にして、VLAN名を入力します。



ヒント:IPダイレクトブロードキャストを有効にすると、L2フラッディングが自動的にアクティブになります。

Catalyst Center Create Anycast Gateways admin

### Configuration Attributes

Each Layer 3 Virtual Network can be assigned one or more Anycast Gateways. An Anycast Gateway has an associated VLAN and Layer 2 Virtual Network. Each of these has multiple configuration parameters and attributes.

Search

LAYER 3 VIRTUAL NETWORKS

- .../USA/RTP
- VN1** ✓

#### ANYCAST GATEWAY

IP Address Pool  
**IPDB\_POOL\_1 [172.16.56.0/24]**  IP-Directed Broadcast  Intra-Subnet Routing  TCP MSS Adj

---

#### VLAN

VLAN Name\* **IPDB\_POOL\_1** VLAN ID Traffic Type **Data** Voice Security Groups  Critical VLAN

Auto generate VLAN name

---

#### LAYER 2 VIRTUAL NETWORK

Fabric-Enabled Wireless  Layer 2 Flooding  Multiple IP-to-MAC Addresses (Wireless Bridged-Network Virtual I

Exit All changes saved Review Back Next

IPダイレクトブロードキャストの有効化

ファブリックゾーンが存在する場合、任意でエニーキャストゲートウェイをサイト内の1つ以上のファブリックゾーンにプロビジョニングできます。

## Fabric Zones (Optional)

Anycast Gateways will be provisioned for the previously selected Virtual Networks within the Fabric Site. If Fabric Zones have been configured, Anycast Gateways can optionally be provisioned to one or more Fabric Zones within the Site.

The screenshot displays the configuration page for an Anycast Gateway. On the left, a sidebar shows a search bar and a list of Layer 3 Virtual Networks under the path "/USA/RTP". The network "VN1" is selected and highlighted. The main content area is titled "Layer 3 Virtual Network Details" and shows "Layer 3 Virtual Network: VN1". Below this, the "Anycast Gateways" section displays the "IP Pool" as "172.16.56.0/24". To the right of the IP Pool, it indicates "Fabric Zones: 0 Selected" and provides a link to "Select Fabric Zones".

[Exit](#)[Review](#)[Back](#)[Next](#)

ファブリックゾーンの選択

展開を続行する前に、構成された設定の概要を確認して正確であることを確認してください。

## Summary

Review the Anycast Gateway configuration settings. To make changes before continuing, select the applicable Edit button.

### Layer 3 Virtual Networks [Edit](#)

Layer 3 Virtual Networks: VN1

### Configuration Attributes [Edit](#)

Fabric Site	Layer 3 Virtual Network	IP Address Pool	IP-Directed Broadcast	Intra-Subnet Routing	TCP MS
USA/RTP	VN1	172.16.56.0/24	🟢	--	--

### Fabric Zones (Optional) [Edit](#)

Fabric Site	Layer 3 Virtual Network	IP Address Pool	Fabric Zone
USA/RTP	VN1	172.16.56.0/24	--

[Exit](#) All changes saved

[Back](#)

[Next](#)

要約

生成された構成をプレビューします。Deployをクリックして、設定をファブリックに適用します

。

Catalyst Center Create Anycast Gateways

## Deploying Anycast Gateways

Step 3 of 3: Preview Configuration

Review the device configuration provided below by clicking on each device. When you are done reviewing, click Deploy. Click [Exit and Preview Later](#) to defer the review. The deferred review can be found in the [Tasks](#) menu. Status: ● Ready

Device IP: 192.168.0.101 Site: Global/USA/RTP/BL... [← Back to workflow progress](#)

Configurations - Side by side view

View by Configuration Source - All

Search configuration

Configuration to be Deployed	Running Configuration
58 Line(s)	2954 Line(s)
<pre> 1 cts role-based enforcement vlan-list 1062 2 vlan 1062 3 name IPDB_POOL_1 4 exit 5 no ip igmp snooping vlan 1053 querier 6 no ip igmp snooping vlan 1055 querier 7 no ip igmp snooping vlan 1041 querier 8 no ip igmp snooping vlan 1040 querier 9 no ip igmp snooping vlan 1031 querier 10 interface Vlan1062 11 no lisp mobility liveness test 12 no ip redirects 13 mac-address 0000.0c9f.fe63 14 description Configured from Catalyst Center 15 vrf forwarding VN1 16 ip igmp explicit-tracking 17 ip address 172.16.56.254 255.255.255.0 18 ip pim passive 19 ip helper-address 192.168.254.39 20 ip route-cache same-interface 21 lisp mobility IPDB_POOL_1-IPV4 22 ip igmp version 3 23 exit 24 router lisp 25 instance-id 4099 26 dynamic-eid IPDB_POOL_1-IPV4 27 database-mapping 172.16.56.0/24 locator-set rloc_91947dad-3621-42bd 28 exit-dynamic-eid 29 instance-id 8257 30 service ethernet 31 eid-table vlan 1062 32 broadcast-underlay 239.0.17.1 33 flood arp-nd 34 flood unknown-unicast 35 exit-service-ethernet </pre>	<pre> 1 Building configuration... 2 3 Current configuration : 93630 bytes 4 ! 5 ! Last configuration change at 02:55:01 UTC Sun Dec 14 2025 by dnac 6 ! NVRAM config last updated at 22:59:12 UTC Fri Dec 12 2025 by dnac 7 ! 8 version 17.12 9 service timestamps debug datetime msec 10 service timestamps log datetime msec 11 service password-encryption 12 service internal 13 platform punt-keepalive disable-kernel-core 14 ! 15 hostname Edge-1 16 ! 17 ! 18 vrf definition Anchor_VN 19 ! 20 address-family ipv4 21 exit-address-family 22 ! 23 address-family ipv6 24 exit-address-family 25 ! 26 vrf definition HOST3 27 ! 28 address-family ipv4 29 exit-address-family 30 ! 31 vrf definition Mgmt-vrf 32 ! 33 address-family ipv4 34 exit-address-family 35 ! </pre>

Is this feature helpful? [👍](#) [👎](#) [Exit and Preview Later](#) [Discard](#) [Deploy](#)

構成のプレビュー

## ネットワークデバイスの設定

### ボーダー設定 – IP中継

IP Transitが設定されたファブリック境界では、BGPピアリングインターフェイスに「ip network-broadcast」が設定され、IPサブネットブロードキャストの転送が許可されます。ファブリックプール（エンドポイントVLAN）のエニーキャストゲートウェイIPは、ループバックインターフェイスから、「ip directed-broadcast」が有効なSVIに変更されます。どちらの設定も、ファブリックボーダーがIPサブネットブロードキャストパケットを完全なブロードキャストに変換して、プロセスを意図したとおりに機能させるために必要です。

IPネットワークブロードキャストおよびIPネットワークブロードキャストの設定：

```
<#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
```

設定のこの2番目の部分では、IPダイレクトブロードキャスト機能を使用して、未知のユニキャストトラフィックを処理する際の従来のネットワークの動作と同様に、ARP要求（ブロードキャスト）を使用してサイレントホストをウェイクアップできます。この設定により、ファブリック外部のソースは、サブネットブロードキャストやWake-on-LAN（「マジックパケット」）メカニズムに依存することなく、標準のユニキャストトラフィックを使用してエンドポイントをウェイクアップできます。

<#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
```

## エッジ設定

ファブリックエッジノードの設定は、レイヤ2フラッディングが有効な標準の有線プールの設定と一致します。「ip directed-broadcast」CLIコマンドはエッジノードでは使用できません。

<#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

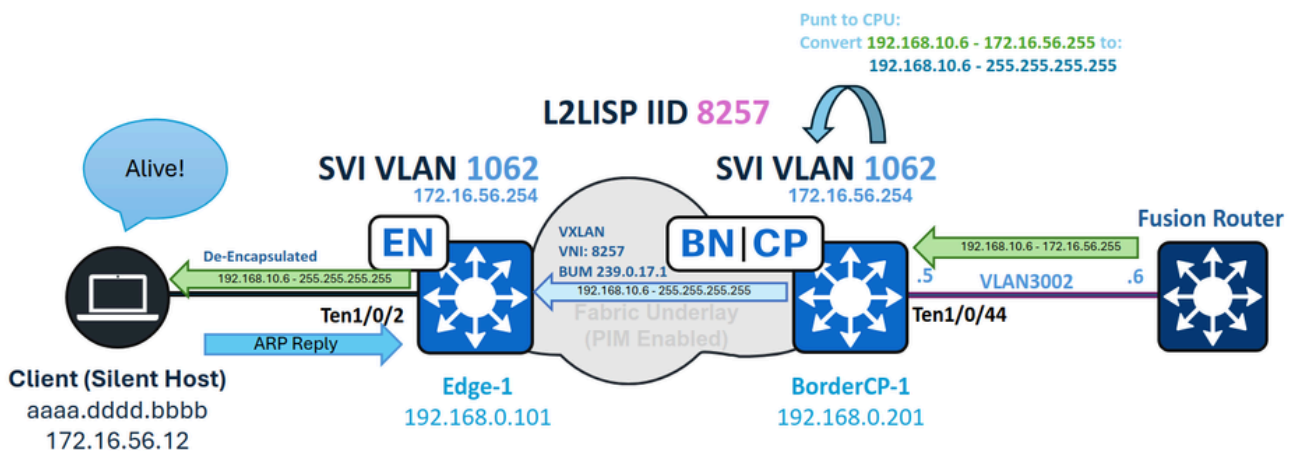
1041 , 1048 , 1053 , 1059 , 1061 -

1062

```
database-mapping mac locator-set rloc_91947dad-3621-42bd-ab6b-379ecebb5a2b
```

```
ip dhcp snooping vlan 1062
```

## IPダイレクトブロードキャストフォワーディング



IPDB転送

## 境界 – 入力CPUパントおよびサブネットブロードキャスト変換

この例では、宛先IPが172.16.56.255(プール172.16.56.0/24のブロードキャストアドレス)であるIPサブネットブロードキャストが、外部ネットワークからルーティングされ、最初にファブリックボーダーに到達します。入力レイヤ3インターフェイスは、IPトランジットSVI(VLAN 3002)です。このインターフェイスでは「ip network-broadcast」が有効になっているため、パケットはフルブロードキャスト変換に受け入れられます。この設定を行わないと、パケットは廃棄されます。

パケットはSVI 3002に到達し、ブロードキャストパケットとしてスイッチのCPUにパントされます。IP network-broadcastが設定されている場合、パケットは許可され、フルブロードキャストに変換されます。

<#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
```

CPUの処理中、VLAN 1062 (宛先インターフェイス) は、パケットをフルブロードキャストに変換します。これは、「ip directed-broadcast」が設定されているためです。

<#root>

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

```
Directed broadcast forwarding is enabled
```

このイベントは、debug ip packetコマンドを使用してトラブルシューティングできます。過度の出力と高いリソース使用率を避けるために、このデバッグの実行時には常にフィルタとしてアクセスリストを適用してください。

<#root>

```
ip access-list standard 10
```

```
10 permit
```

```
192.168.10.6      --- Directed Broadcast source IP
```

```
BorderCP-1#debug ip packet detail 10
```

```
IP:
```

```
s=192.168.10.6 (Vlan3002)
```

```
,
d=172.16.56.255

(nil), len 100,

input feature

ICMP type=8, code=0, MCI Check(110), rtype 0, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
IP: s=192.168.10.6 (Vlan3002), d=172.16.56.255 (nil), len 100, input feature
ICMP type=8, code=0, Role-based Proxy(116), rtype 0, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE

FIBipv4-packet-proc: route packet from Vlan3002 src 192.168.10.6 dst 172.16.56.255

FIBfwd-proc: VN1:172.16.56.255/32 receive entry

FIBipv4-packet-proc: packet routing failed

IP: tableid=3, s=192.168.10.6 (Vlan3002), d=172.16.56.255 (Vlan1062) nexthop=172.16.56.255, routed via F

IP: s=192.168.10.6 (Vlan3002), d=172.16.56.255 (Vlan1062), len 100, output feature
ICMP type=8, code=0, feature skipped, Role-based Access List(53), rtype 1, forus FALSE, sendself FALSE,

IP: s=192.168.10.6 (Vlan3002), d=172.16.56.255 (Vlan1062), g=255.255.255.255, len 100, forward directed
```

入力ポーターは、BUMカプセル化のマルチキャスト送信元(S)およびグループ(G)として機能します。ループバック0を送信元アドレスとして使用し、設定済みのBUMグループを宛先として使用します。

PIMコントロールプレーンで、ファブリックエッジへのダウンリンクがマルチキャストルートの発信インターフェイスリスト(OIL)に表示されることを確認します。データプレーンの場合は、show ip mfib countコマンドを使用して、Border上のS,Gエントリに対してハードウェア転送カウンタが増加していることを確認します。

<#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
```

このドキュメントでは、アンダーレイのマルチキャストツリーの形成やレイヤ2フラッディングについては詳しく説明していません。S、Gの状態が欠落しているか、不完全であるか、または間違っている場合は、NetWormのアンダーレイマルチキャスト部分を個別にトラブルシューティングする必要があります。

## Edge : 入カブロードキャスト

ファブリックエッジでは、マルチキャストのVXLANでカプセル化された着信ブロードキャストは、カプセル化が解除され、VNI(8257)に関連付けられたVLANに転送され、スパニングツリーのフォワーディングステータスのすべてのポートに到達します。

まず、BUMグループの境界からのS,Gエントリ（送信元としてBorderループバックを使用）が存在し、トラフィックを転送していることを確認します。これを確認するには、同じmrouteコマンドとmfibコマンドを使用します。VLAN(1062)に対応するL2LISPサブインターフェイスが発信インターフェイスとしてリストされていることを確認してください。

<#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
```

カプセル化解除後、パケットはVLAN 1062上で、そのVLANに割り当てられたすべてのポートに転送されます。

<#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

エンドポイントは、ブロードキャストパケットを受信した後、そのパケットを該当するものとして認識し、応答する必要があります。その結果、エンドポイントはARPパケットを送信し、スイッチ上のデバイスラッキングテーブルが更新されます。

<#root>

Edge-1#show device-tracking database interface Te1/0/2 | be Network

Network Layer Address	Link Layer Address	Interface	vlan	prlv1	age	state	Time left
ARP 172.16.56.12	aaaa.dddd.bbbb	Te1/0/2	1062	0005	0s	REACHABLE	241 s

エンドポイントがデバイストラッキングに再登録されると、エッジノードのLISPデータベースにインポートされ、コントロールプレーンに登録されます。

LISP Pub-Subの展開では、コントロールプレーンが新しく登録されたエンドポイント情報を境界にパブリッシュし、トラフィックを適切なエッジノードに転送するためのLISPマップキャッシュエントリを即座に作成します。

<#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:
```

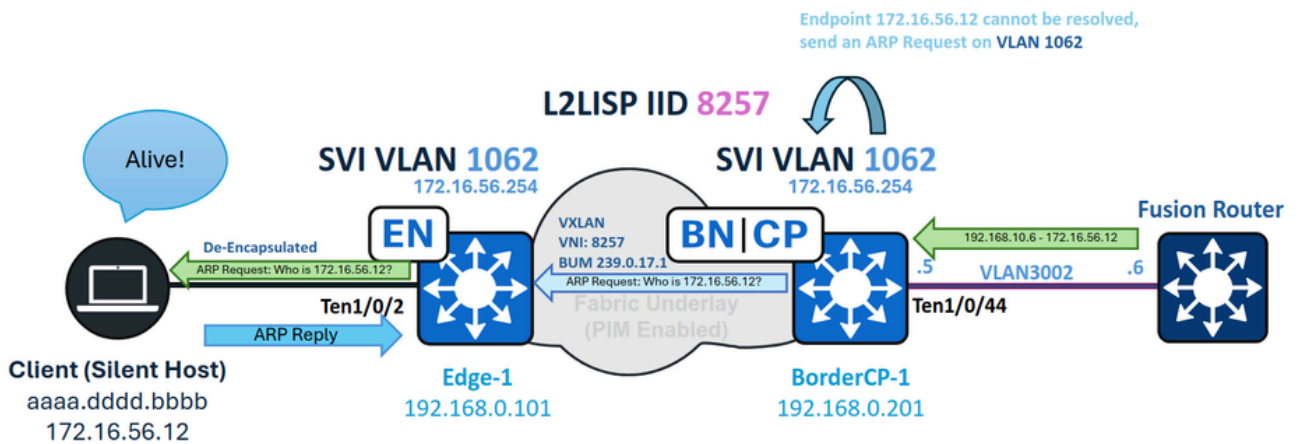
```
Last RLOC-probe sent: 00:22:19 (rtt 4ms)
```

LISP/BGP(SDA 1.0)の導入では、導入が分散 (非同期) されると、最初に否定応答 (NMR)が期限切れになるため、不明なエンドポイントのLISPマップキャッシュの更新に最大1分

かかる場合があります。

サイレントホストは、サブネットブロードキャストなどのパケットに応答するようにプログラムされていない場合、それらのパケットを無視する必要があります。「マジックパケット」(UDPエコーなど)を必要とするエンドポイントもあれば、ブロードキャストARPにのみ応答するエンドポイントもあります。サイレントホスト自体は、スリープ解除をトリガーするパケットのタイプを決定します。「不明なユニキャスト転送」セクションで説明されているように、最も一般的なオプションの中で、通常はARP要求が優先されます。

## 不明なユニキャスト転送



不明なユニキャスト転送

プールがIP Directed Broadcastに対して有効になっていると、サブネットブロードキャストの処理が許可されるだけでなく、ファブリックポーターが未知のユニキャストトラフィックを転送するためのゲートウェイとして機能できるようになります。このコンテキストでは、不明なユニキャストトラフィックとは、現在コントロールプレーンに登録されていないエンドポイント宛てのパケットを指します。

不完全なARPエントリが検出されたときにARP要求を送信する従来のネットワークゲートウェイと同様に、ポーターはARP要求を生成し、すべてのファブリックノードにフラッディングします。これにより、サイレントホストが要求を受信し、起動してARP応答を送信し、それによって自身がコントロールプレーンに再登録されます。

この機能が可能なのは、エンドポイントVLAN(1062)がFabric Border上でSVIとL2LISPインスタンスの両方として設定されているためです。L2 IIDで「flood arp-nd」を有効にすると、不明なLISP EIDに宛てられたトラフィックがあるたびに、SVIによって生成されたARP要求を境界でフラッディングできるため、サイレントホストがARP要求を受信し、応答してコントロールプレーンでの登録を更新する機会を得ることができます。

<#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
```

ファブリックボーダーは、エンドポイントVN/VRFの一部であるSVI 3002上で172.16.56.12宛ての packets を受信すると、CEF出力が「グリーンング」(デバイスがダウンストリームレイヤプロトコルを使用して宛先の隣接関係を解決しようとすることを意味する)に設定されているため、LISP解決を試みます。このプロセスは、未登録(サイレント)ホストに対するLISPマップ要求とARP解決の両方を同時にトリガーします。

```
<#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

不完全なARPエントリが作成され、不明なエンドポイント172.16.56.12にARP要求を送信するようBorderに要求する。このARP要求は、ブロードキャストパケットとして、レイヤ2フラッディングおよびフラッディングARP-ND機能を使用してダウンストリームに転送されます。

レイヤ2フラッディングが動作していることを確認するには、境界のローカルS,GのMFIBカウンタを監視します。

<#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
```

フラッディングされたARPパケットはサイレントホストに到達し、スリープ状態を解除してARP応答を要求します。この応答により、ファブリックエッジ上のデバイストラッキング(SISF)テーブルが更新され、LISPデータベースエントリが作成されます。その結果、ファブリックエッジはコントロールプレーンへの登録を開始します。

```
<#root>
```

```
Edge-1#show device-tracking database interface Te1/0/2 | be Network
```

```
Network Layer Address Link Layer Address Interface vlan prlv1 age state Time left
```

ARP 172.16.56.12

aaaa.dddd.bbbb

Te1/0/2

1062 0005

0s REACHABLE 241 s

エンドポイントがデバイストラッキングに再登録されると、エッジノードのLISPデータベースにインポートされ、コントロールプレーンに登録されます。

LISP Pub-Subの展開では、コントロールプレーンが新しく登録されたエンドポイント情報を境界にパブリッシュし、トラフィックを適切なエッジノードに転送するためのLISPマップキャッシュエントリを即座に作成します。

<#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)
```

LISP/BGP(SDA 1.0)の導入では、導入が分散 (非コロケーション) されると、最初に否定応答 (NMR)が期限切れになるため、不明なエンドポイントのLISPマップキャッシュの更新に最大1分かかる場合があります。



ヒント：サイレントホストのARPは境界で解決されません。エンドポイントの登録だけが必要です。サイレントホストが応答すると、ARPパケットはレイヤ2ユニキャストとして送信されるため、境界に向けてフラッディングされません。その結果、ARPエントリやデバイストラッキングエントリがBorder上に表示されることは想定されていません。

## 認証テンプレートでのWake-on-LANの有効化

ファブリックユーザが認証をイネーブルにしていない場合、ポートがフラッディングがイネーブルになっているVLANの一部である限り、境界からのフラッディングされたパケットはサイレントホストに到達します。ただし、(特に) Closed Authenticationでは、2つの主要な要因が重要になります。

## 認証前のホストの手動VLAN割り当て

VLANが割り当てられていない場合、ポートは指定VLANからフラッディングされたパケットを受信しません。VLANがRADIUSによって割り当てられると予想される場合、「鶏か卵か？」というジレンマが生じます。ユーザ認証をトリガーし、RADIUSからVLAN割り当てを取得するために、フラッディングされたパケットを別のVLANに転送 (一般にVLANホッピングと呼ばれる) することはできません。

Host-Onboardingでポートを設定する際に、デバイスが「silent」と識別される場合は、DATAブールのドロップダウンメニューを使用してVLANを手動で割り当てます。

サイレントホストがVLAN割り当ての前に認証できないという問題は、SD-Access固有のものではありません。これは、従来のセキュアなネットワークで見られる一般的な設計上の課題です。

<#root>

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

```
switchport access vlan 1062
```

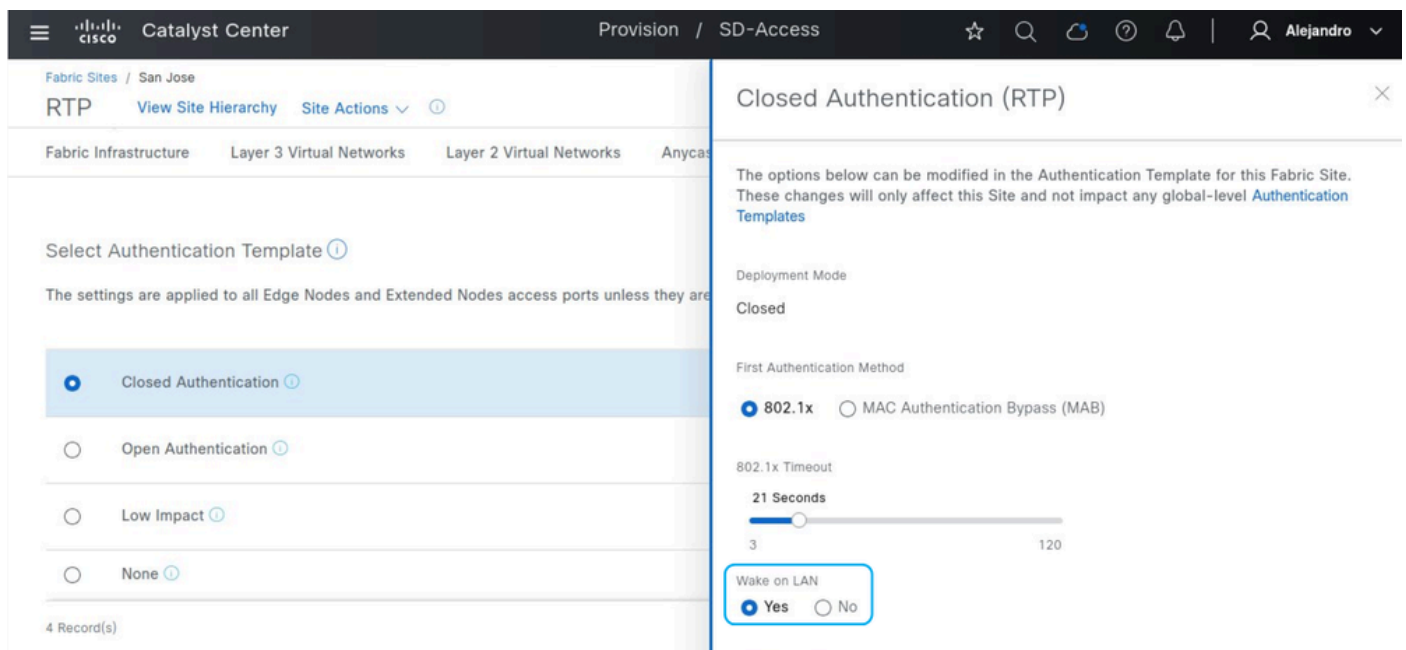
```
switchport mode access
device-tracking attach-policy IPDT_POLICY
dot1x timeout tx-period 7
dot1x max-reauth-req 3
```

```
source template DefaultWiredDot1xClosedAuth
```

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

## アクセス制御方向

デフォルトでは、Host-Onboarding内の認証テンプレート設定でWake-on-LANが有効になっていない場合、認証テンプレートは「access-session control-direction both」を使用します。この設定により、ポートは着信パケットと、ポートから転送されるパケットの両方をドロップします。Wake-on-LANを有効にすると、設定が「access-session control-direction in」に変わり、入カトラフィックのみが制限されます。この調整により、パケットがサイレントホストに到達してウェイクアップし、MAB認証を開始できるようになります。



The screenshot shows the Cisco Catalyst Center interface for configuring authentication templates. The main panel displays a list of authentication templates: Closed Authentication (selected), Open Authentication, Low Impact, and None. The right-hand panel, titled 'Closed Authentication (RTP)', shows the following settings:

- Deployment Mode: Closed
- First Authentication Method: 802.1x (selected), MAC Authentication Bypass (MAB)
- 802.1x Timeout: 21 Seconds (slider range from 3 to 120)
- Wake on LAN: Yes (selected), No

Wake on LAN ( ウェイクオンLAN )

Wake-on-LANなし :

<#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
```

エンドポイントが認証される前は、そのエンドポイントに割り当てられたインターフェイスは、スパンニングツリーステートでフラッディング対応としてリストされません。

```
<#root>
```

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

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

Wake-on-LANを有効にした場合：

```
<#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
```

認証前でも、ポートは出力トラフィックに対して有効になっており、パケットがサイレントホストに到達してウェイクアップできます。

```
<#root>
```

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

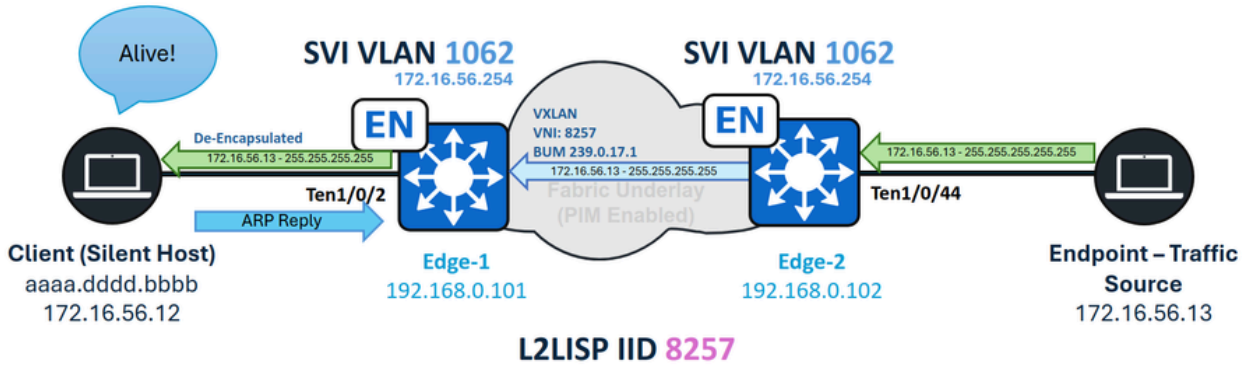
Vlan	Role	Sts	Cost	Prio.Nbr	Type
-----					
VLAN1062					
	Desg				
FWD					
19	128.2	P2p	Edge		

## 代替シナリオ

### エッジノードと同一VLAN - レイヤ2フラッディング

ホストと同じVLAN上にあるファブリック内のデバイスからサイレントホストをウェイクアップさせる場合は、IPダイレクトブロードキャスト機能は必要ありません。その代わりに、(非ワイヤレスプールで)レイヤ2フラッディングを有効にすれば、ブロードキャストパケット、サブネット

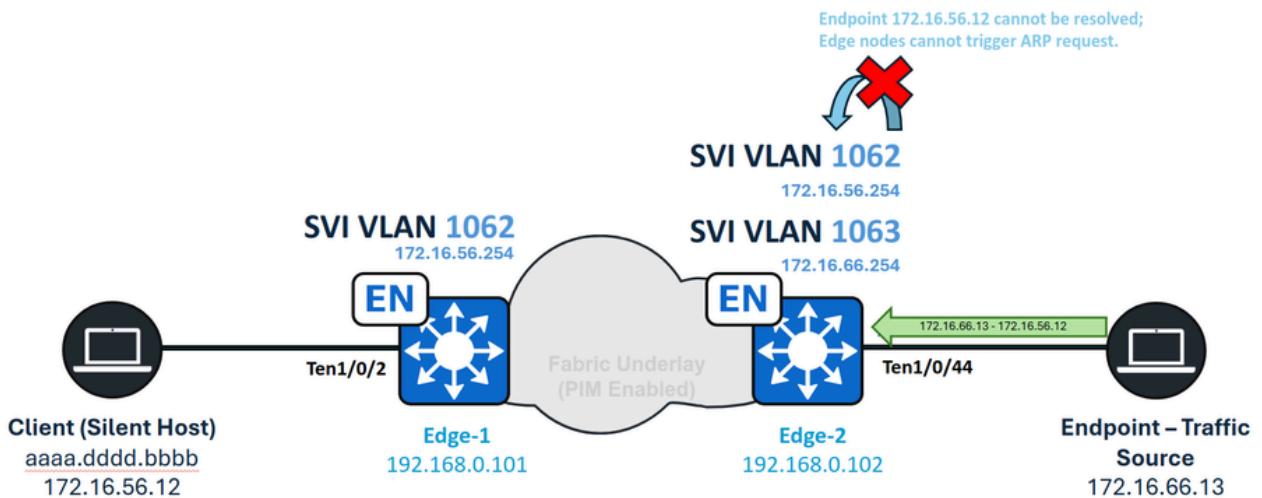
ブロードキャスト、またはARP要求の交換が可能になります。閉じた認証では、Wake-on-LANの要件が維持されます。



同じVLAN - サイレントホスト処理

### エッジノードと異なるVLAN - 不明なユニキャスト

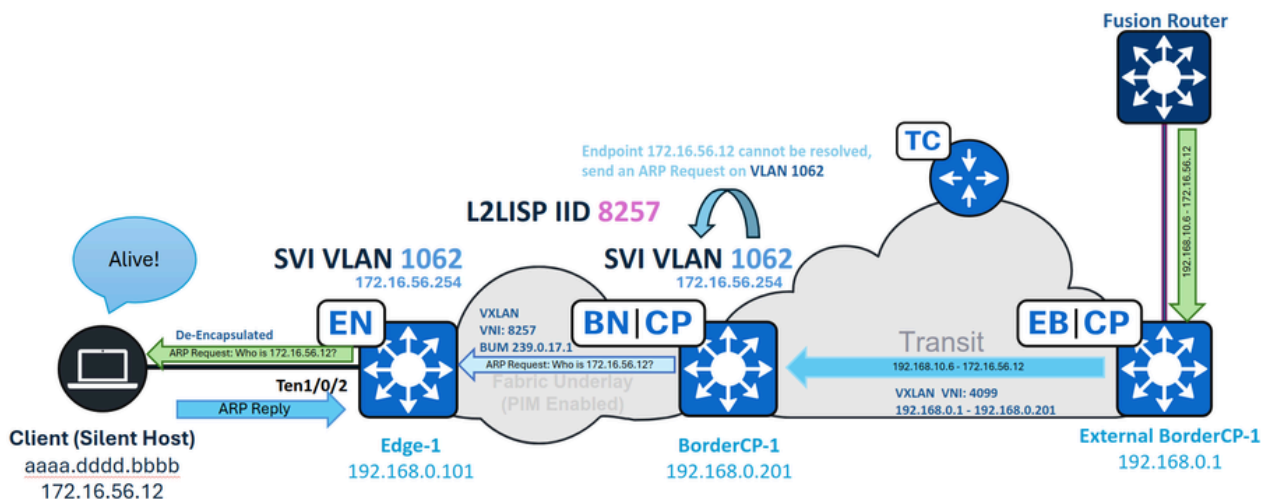
ファブリック内のエンドポイントがファブリックエッジノードに接続されたサイレントホストにユニキャストトラフィックを送信する場合、不明なユニキャスト転送パスは使用できません。ファブリックボーダーとは異なり、ファブリックエッジノードにはLISPプロキシETRとして定義されたボーダーがあり、不明なエンドポイントが検出されると、「Signal & Forward」と呼ばれる転送機能が自動的に有効になります。ファブリックエッジは、アドレスの解決を最初に試みたときに、必要なARP要求をトリガーする必要があります。ただし、LISPがエンドポイントを不明なEIDとして識別すると、後続のパケットは追加のARP要求をトリガーしません。このシナリオはサポート対象外と見なされます。



不明なユニキャストVLAN間

## SDアクセス中継 – 不明なユニキャスト

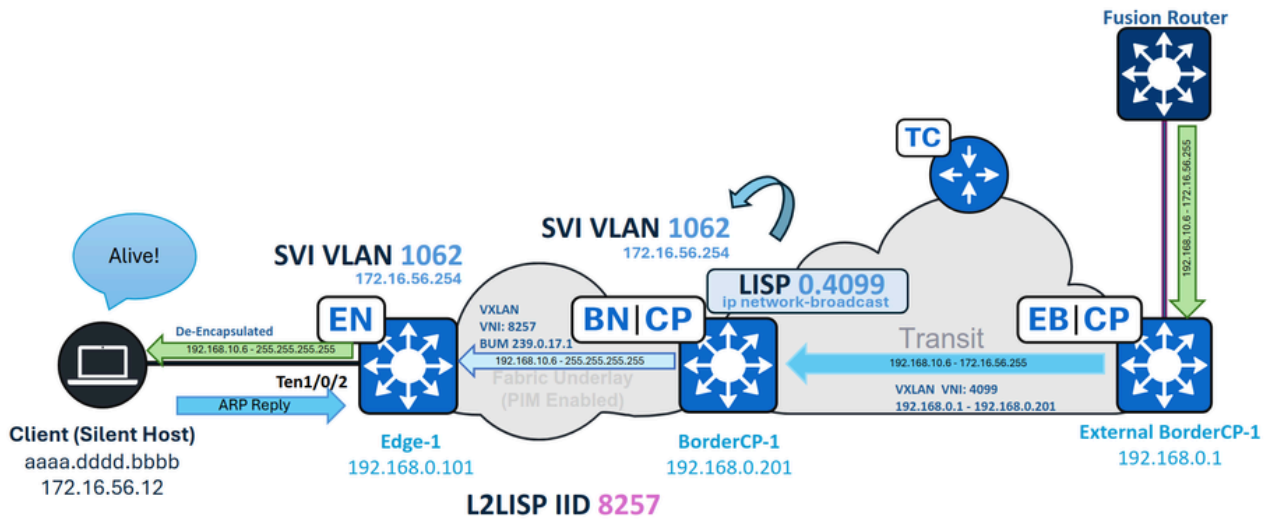
SDアクセス中継の場合、不明なユニキャストトラフィックは特別な要件なしにネイティブでサポートされます。リモートポーターから発信されたトラフィックは、SDアクセス中継ネットワークを介してルーティングされます。サブネットブロードキャストは、通常のルーテッドトラフィックとして扱われます。トラフィックがローカルサイトの境界に到達すると、トラフィック収集、ARP要求フラッディング、LISP解決などの標準的な操作が実行されます。



SDアクセストランジット不明ユニキャスト

## SDアクセス中継 – IPダイレクトブロードキャスト

SDアクセス中継が使用されている場合、ローカルサイトの境界では、SVIではなく、VNに対するLISPサブインターフェイス (インターフェイス4099など) でIPダイレクトブロードキャストを受信します。ブロードキャストが受け入れられ、IPダイレクトブロードキャスト機能によってサブネットブロードキャストに変換されるようにするには、LISPサブインターフェイスで「ip network-broadcast」パラメータを手動で設定する必要があります。



SDアクセス中継IPDB

BorderCP-1 (ローカルサイト境界):

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

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。