SDアクセスでのアクセストンネル作成について

内容

はじめに

このドキュメントでは、SD-Accessのアクセストンネルの概要、その目的、およびアクセストンネルの形成をトリアージする方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ロケータID分離プロトコル(LISP)
- ワイヤレス

使用するコンポーネント

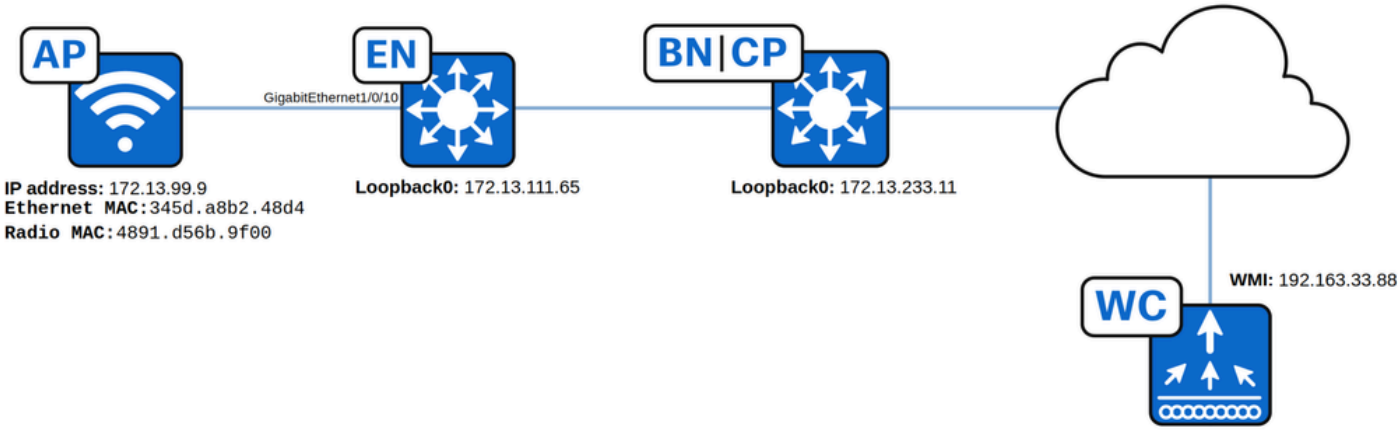
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- シスコワイヤレスLANコントローラ(WLC):C9800-CL、Cisco IOS® XE 17.12.04
- SDAエッジノード：C9300-48P、Cisco IOS® XE 17.12.05
- SDAボーダーノード/コントロールプレーン：C9500-48P、Cisco IOS® XE 17.12.05
- Ciscoアクセスポイント – C9130AXI-A、バージョン17.9.5.47

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

トポロジ



この記事で使用されるトポロジ

概要

Cisco SDアクセスのアクセストンネルは、ファブリックエッジノードとアクセスポイント(AP)の間に確立された仮想拡張LAN(VXLAN)トンネルです。 このトンネルはクライアントトラフィックをVXLANにカプセル化し、SDアクセスファブリック内でのシームレスな通信を可能にします。アクセストンネルは、アクセスポイントに接続されたワイヤレスクライアントからのトラフィックをファブリックエッジに伝送するデータプレーンオーバーレイとして機能し、ネットワーク全体で一貫したポリシーの適用とセグメント化を実現します。

アクセストンネル形成プロセス

1. APが接続され、Power over Ethernet(PoE)経由で電源が投入されている。
2. APはオーバーレイでDHCP経由でIPアドレスを取得します。このプロセス中に、APはワイヤレスLANコントローラのDHCPサーバからオプション43も受信します。
3. ファブリックエッジは、APのIPアドレスとイーサネットMACを登録し、LISPコントロールプレーンを更新します。
4. WLCはLISP CPに問い合せて、APがファブリックデバイス(FDA)に接続されているかどうかを確認します。
5. LISPコントロールプレーンは、APが接続されているファブリックデバイスのロケータ(Loopback 0 IP)を使用してWLCに応答します。応答がある場合は、APがファブリックに接続され、ファブリック対応としてマークされていることを意味します。
6. WLCは、LISPコントロールプレーンで、WLCからFEへのメタデータ情報とともに、AP無線MACのL2 LISP登録を実行します。
7. LISPコントロールプレーンはファブリックエッジに通知し、WLCから受信したメタデータを送信します。このメタデータには、APであることを示すフラグとAPのIPアドレスが含まれています。

8. ファブリックエッジは情報を処理します。APであることを学習し、APとファブリックエッジ間にアクセストンネルとも呼ばれるVXLANトンネルを作成します。

SDアクセス内のAPオンボーディングで正常なアクセストンネル形成を確実にするには、次の手順を実行します。これらのチェックに失敗すると、トンネルの作成を妨げる可能性があります。手順で期待どおりの結果が得られない場合は、その手順に関連するコンポーネントのトラブルシューティングに焦点を当てます。

プロセスの確認

APがIPアドレスを取得するかどうかの確認

APがIPアドレスを受信していることを確認するには、エッジノードで次のコマンドを実行します。

<#root>

Edge#show device-tracking database interface gigabitEthernet 1/0/10

```
...
     Network Layer Address   Link Layer Address  Interface  vlan prlvl age state     Time left
DH4
```

172.13.99.9

345d.a8b2.48d4

Gi1/0/10

99

0024 15s REACHABLE 237 s try 0(47302 s)

上記の出力から、インターフェイスGigabitEthernet 1/0/10に接続されたAPのIPアドレスはVLAN 99上で172.13.99.9であり、イーサネットMACアドレスは345d.a8b2.48d4であることがわかります。
出力が空の場合は、APがIPアドレスの取得に失敗したか、Power over Ethernet(PoE)が機能していません。PoEが動作していることを確認するには、次のコマンドを実行して、アクセスポイントのMACアドレスがMACアドレステーブルに表示されていることを確認します。

<#root>

Edge#show mac address-table interface gigabitEthernet 1/0/10

```
Mac Address Table
-------------------------------------------
Vlan Mac Address Type Ports
---- ----------- -------- -----
```

99

345d.a8b2.48d4

DYNAMIC

Gi1/0/10

PoEのインライン電源が動作していることを確認するには、次のコマンドを実行します。

<#root>

Edge#show power inline gigabitEthernet 1/0/10

Interface Admin

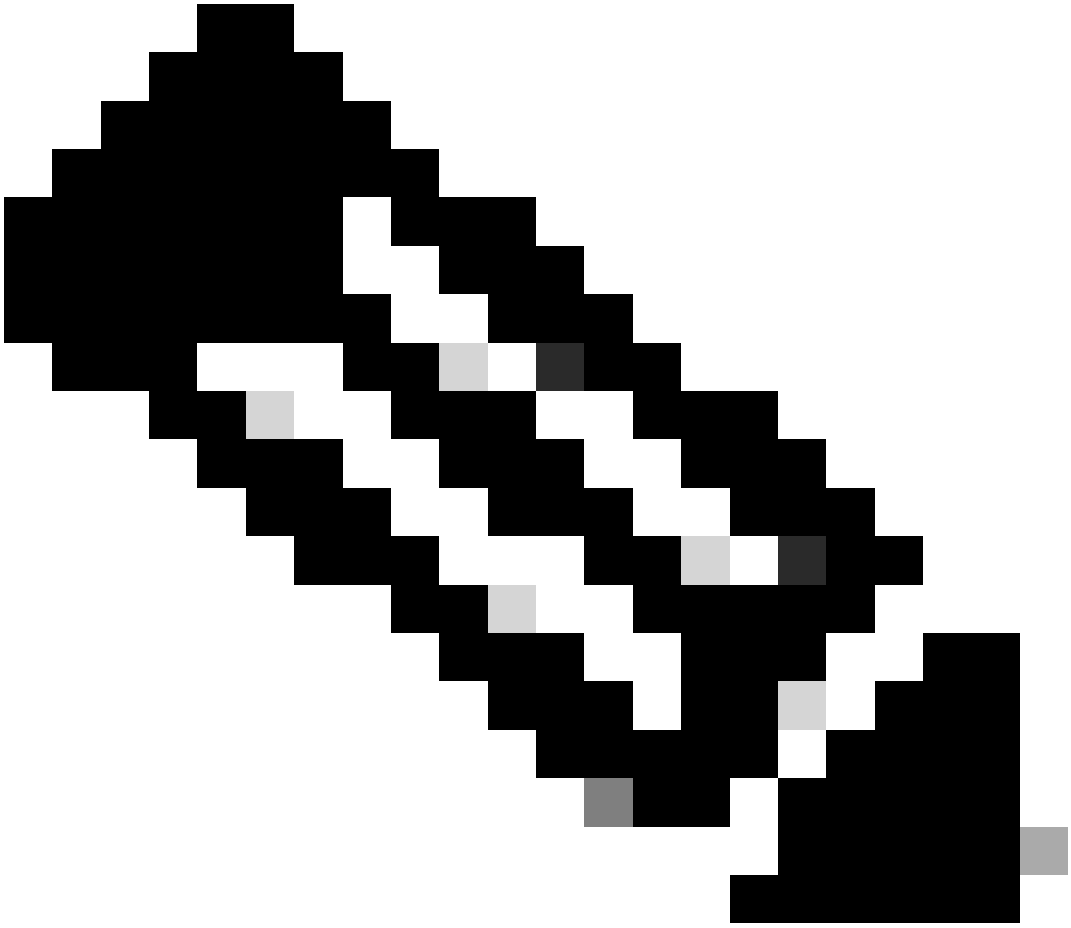
Oper

Power Device Class Max
(Watts)
--- --- --- --- --- --- --- ---
Gi1/0/10 auto

on

30.0 C9130AXI-A 4 30.0

PoEは30.0ワットで動作し、動作しています。



注:IPアドレスを取得すると、アクセスポイントは従来のネットワーキングと同様にワイヤレスLANコントローラ(WLC)への参加を試みます。show ap summaryコマンドの実行時にAPがリストされない場合、AP joinのトラブルシューティングを行います。

LISPコントロールプレーンでのAPのIPおよびイーサネットMAC登録の確認

ファブリックエッジのコントロールプレーン（マップサーバとも呼ばれる）を特定するには、次のコマンドを実行します。

<#root>

Edge#show lisp session

```
Sessions for VRF default, total: 1, established: 1
Peer State Up/Down In/Out Users
```

172.13.233.11

:4342 Up 1d02h 326/324 12

コントロールプレーンは172.13.233.11で、このデバイスのloopback0になります。

ファブリックサイトのコントロールプレーンを識別するもう1つの方法は、次のコマンドを実行することです。

<#root>

```
Edge#show running-config | section map-server


etr map-server

172.13.233.11

 key 7 050F020C734848514D514117595853732F
etr map-server

172.13.233.11

 proxy-reply
etr map-server

172.13.233.11

 key 7 050F020C734848514D514117595853732F
etr map-server

172.13.233.11

 proxy-reply
```

WLCでは、コントロールプレーンとのLISPセッションがUP状態であることも確認できます。

<#root>

```
WLC#show wireless fabric summary


Fabric Status :

Enabled



Control-plane:
Name                    IP-address       Key                Status
------------------------------------------------------------------------------------------
default-control-plane

172.13.233.11

    ddc2df8446e2479d

Up
```

コントロールプレーンに登録されているAPのIPを見つけるには、次のコマンドを使用します。

<#root>

Border#show lisp instance-id 4097 ipv4 server 172.13.99.9

LISP Site Registration Information
...

EID-prefix: 172.13.99.9/32 instance-id 4097

First registered: 22:14:34
Last registered: 22:14:34
Routing table tag: 0
Origin: Dynamic, more specific of 172.13.99.0/24
...
TTL: 1d00h

State: complete

Extranet IID: Unspecified
Registration errors:

Authentication failures: 0

Allowed locators mismatch: 0

ETR 172.13.111.65:21839, last registered 22:14:34, proxy-reply, map-notify <-- Last registration

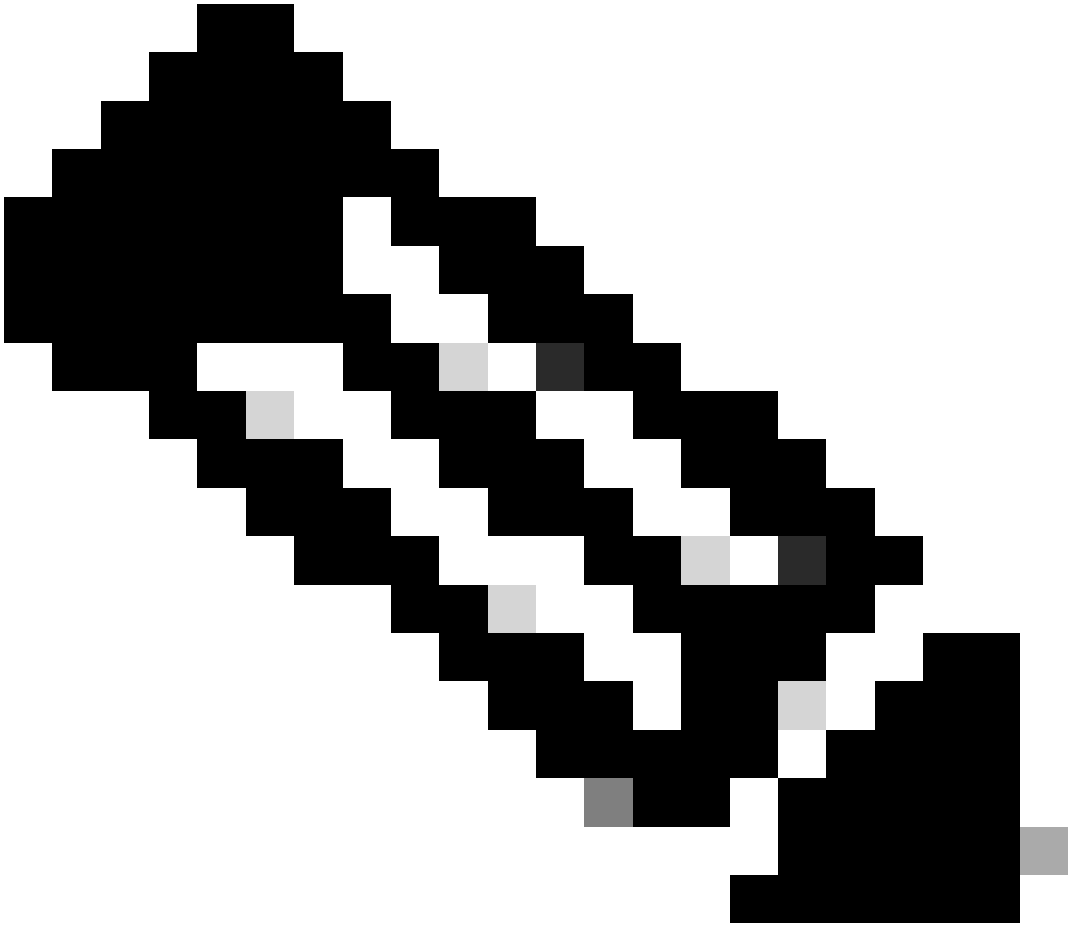
TTL 1d00h, no merge, hash-function sha1
state complete, no security-capability
...
Domain-ID 1559520338
Multihoming-ID unspecified
sourced by reliable transport

Locator

Local State Pri/Wgt Scope

172.13.111.65

yes up 10/10 IPv4 none



注:APはレイヤ3に対して常にINFRA_VNを使用し、このINFRA_VNは常にインスタンスID 4097にマッピングされます。

IPアドレス172.13.99.9のAPの登録が完了します。認証の失敗はなく、エッジノード 172.13.111.65 (ロケータ) に接続されています。

MACアドレスがコントロールプレーンに登録されているかどうかを確認するには、まず、APが接続されているVLANのレイヤ2インスタンスID(RID)を特定します。次のコマンドを使用します。

<#root>

Edge#show vlan id 99

```
VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
```

99

```
 AP_VLAN active
```

```
L2LI0:8188

, Gi1/0/10, Ac0
...
```

VLAN 99はインスタンスID 8188にマッピングされます。このインスタンスIDを使用して、イーサネットMACアドレスがコントロールプレーンに登録されているかどうかを確認するには、次のコマンドを実行します。

<#root>

```
Border#show lisp instance-id 8188 ethernet server 345d.a8b2.48d4


LISP Site Registration Information
...

EID-prefix: 345d.a8b2.48d4/48 instance-id 8188


First registered: 22:57:39
Last registered: 22:57:39
Routing table tag: 0
Origin: Dynamic, more specific of any-mac
...

State: complete


Extranet IID: Unspecified
Registration errors:

Authentication failures: 0


Allowed locators mismatch: 0

ETR 172.13.111.65:21839, last registered 22:57:39, proxy-reply, map-notify


   TTL 1d00h, no merge, hash-function sha1
   state complete, no security-capability
   ...
   Domain-ID 1559520338
   Multihoming-ID unspecified
   sourced by reliable transport

Locator

      Local State Pri/Wgt Scope

172.13.111.65

 yes   up    10/10   IPv4 none
```

APのイーサネットMAC 345d.a8b2.48d4の登録は、認証障害なしで完了し、エッジノード172.13.111.65（ロケータ）に接続されています。

WLCでデバイスがファブリック対応としてマーキングされていることの確認

<#root>

WLC#show fabric ap summary

Number of Fabric AP : 1

AP Name Slots AP Model

Ethernet MAC

Radio MAC

Location Country

IP Address

State

AP345D.A8B2.48D4 3 C9130AXI-A

345d.a8b2.48d4

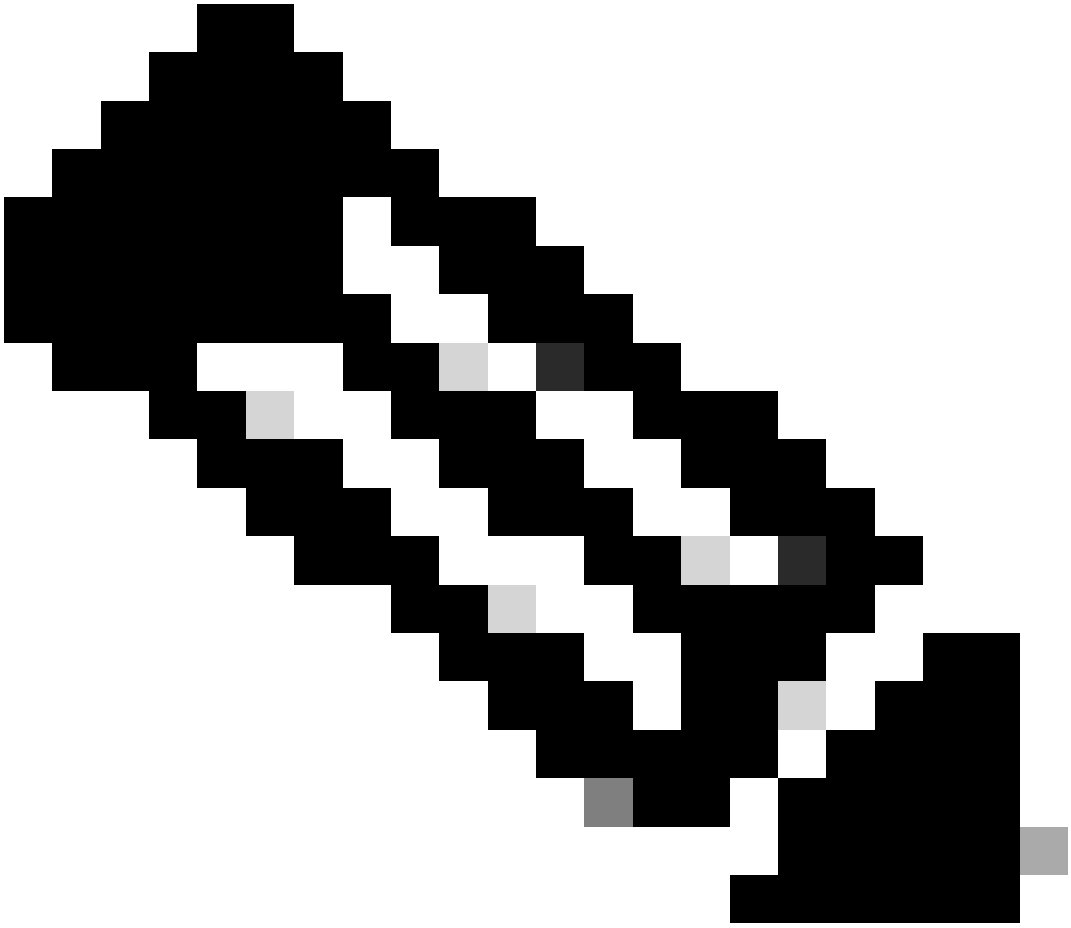
4891.d56b.9f00

default location MX

172.13.99.9

Registered

IPアドレス172.13.99.9のAPは、ファブリックAPとして正しくマーキングされています。APがリストされていない場合は、WLCがLISPコントロールプレーンからの応答を受信できなかったことを示します。この出力では、APの無線MACアドレスは4891.d56b.9f00です。



注：APがコントロールプレーンに登録されているが、ファブリック対応としてマークされていない場合は、ファイアウォールがUDPポート4342でLISPトラフィックをブロックしていないことを確認してください。

LISPコントロールプレーンでの無線MAC登録の確認

イーサネットMACアドレスの登録の確認に使用したのと同じコマンドを使用しますが、イーサネットMACアドレスを無線MACアドレスで置き換えます。

<#root>

Border#show lisp instance-id 8188 ethernet server 4891.d56b.9f00

LISP Site Registration Information
...

EID-prefix: 4891.d56b.9f00/48 instance-id 8188

```
First registered: 22:49:43
Last registered: 22:49:43
Routing table tag: 0
Origin: Dynamic, more specific of any-mac
...
State: complete
Extranet IID: Unspecified
Registration errors:
```

Authentication failures: 0

```
Allowed locators mismatch: 0
ETR 192.163.33.88:59019, last registered 22:49:43, no proxy-reply, no map-notify
   TTL 1d00h, no merge, hash-function sha2
   state complete, no security-capability
   ...
   sourced by reliable transport
   Affinity-id: 0 , 0
```

WLC AP bit: Set

Locator

```
       Local State Pri/Wgt Scope
```

172.13.111.65

```
 yes   up    0/0     IPv4 none
```

無線MACアドレスは、認証障害なしで完全に登録され、エッジノード172.13.111.65 (ロケータ) に接続されます。 この出力には、WLC AP bit: Setも示されます。これは、この登録がRLOC 172.13.111.65上のAPに属していることをエッジノードに示すためにLISPコントロールプレーンによって使用されるフラグです。

アクセストンネルの作成の確認

最後のステップは、ファブリックエッジでのアクセストンネルの作成を確認することです。前述したように、これがSDアクセスでのAPオンボーディングの最終的な目標です。アクセストンネルの作成を確認するには、次のコマンドを実行します。

<#root>

Edge#show access-tunnel summary

```
Access Tunnels General Statistics:
Number of AccessTunnel Data Tunnels = 1
Name   RLOC IP(Source)   AP IP(Destination) VRF ID Source Port Destination Port
------ --------------- ------------------ ------ ----------- ----------------
```

Ac0

172.13.111.65

172.13.99.9

0 N/A 4789

Name IfId Uptime
------ ---------- --------------------

Ac0 0x00000058 0 day, 00:00:51

アクセストンネル0は、AP 172.13.99.9をエッジノードロケータ172.13.111.65に接続し、51秒間起動しています。タイマーは、リセットのたびに0に設定されます。

また、トンネルがフォワーディングエンジンドライバ(FED)抽象化レイヤでプログラムされており、スイッチハードウェアと直接インターフェイスすることも確認できます。

<#root>

Edge#show platform software fed switch active ifm interfaces access-tunnel

Interface IF_ID State

Ac0

0x00000058

READY

IF_IDを使用して、このトンネルの詳細を確認できます。

<#root>

Edge#show platform software fed switch active ifm if-id 0x00000058

Interface IF_ID : 0x0000000000000058
Interface Name : Ac0
Interface Block Pointer : 0x73d6c83dc6f8

Interface Block State : READY

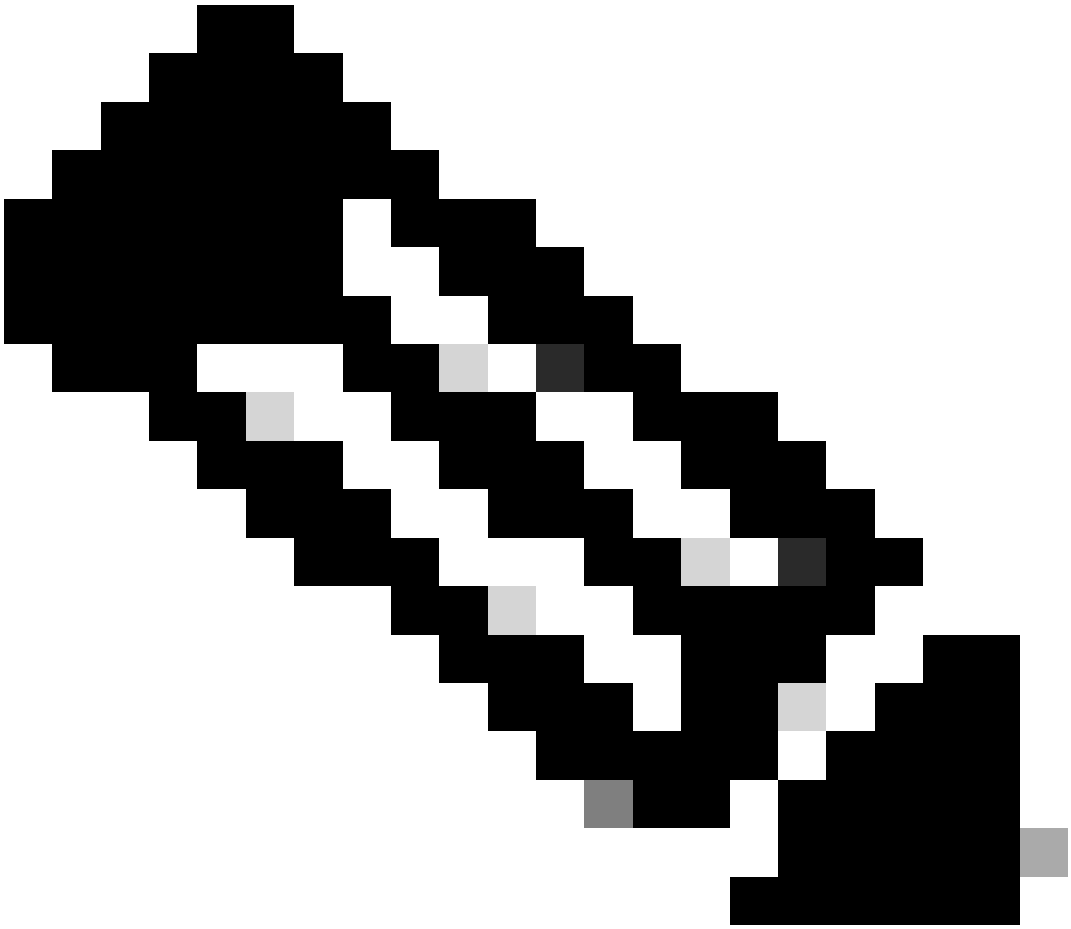
Interface State : Enabled

...

Interface Type : ACCESS_TUNNEL

```
...
Tunnel Type : L2Lisp
Encap Type : VxLan
...
```

これはVXLANカプセル化を使用するL2 lispトンネルで、インターフェイスタイプはaccess-tunnelです。



注:show access-tunnel summaryコマンドとFEDコマンドの両方の出力に一致するアクセストンネルの数が重要です。不一致は、プログラミングの誤りを示している可能性があります。

APで、次のコマンドを使用してアクセストンネルの作成を確認できます。

<#root>

AP#show ip tunnel fabric

```
Fabric GWs Information:
Tunnel-Id GW-IP         GW-MAC            Adj-Status Encap-Type Packet-In
  Bytes-In Packet-Out Bytes-out
        1
```

172.13.111.65

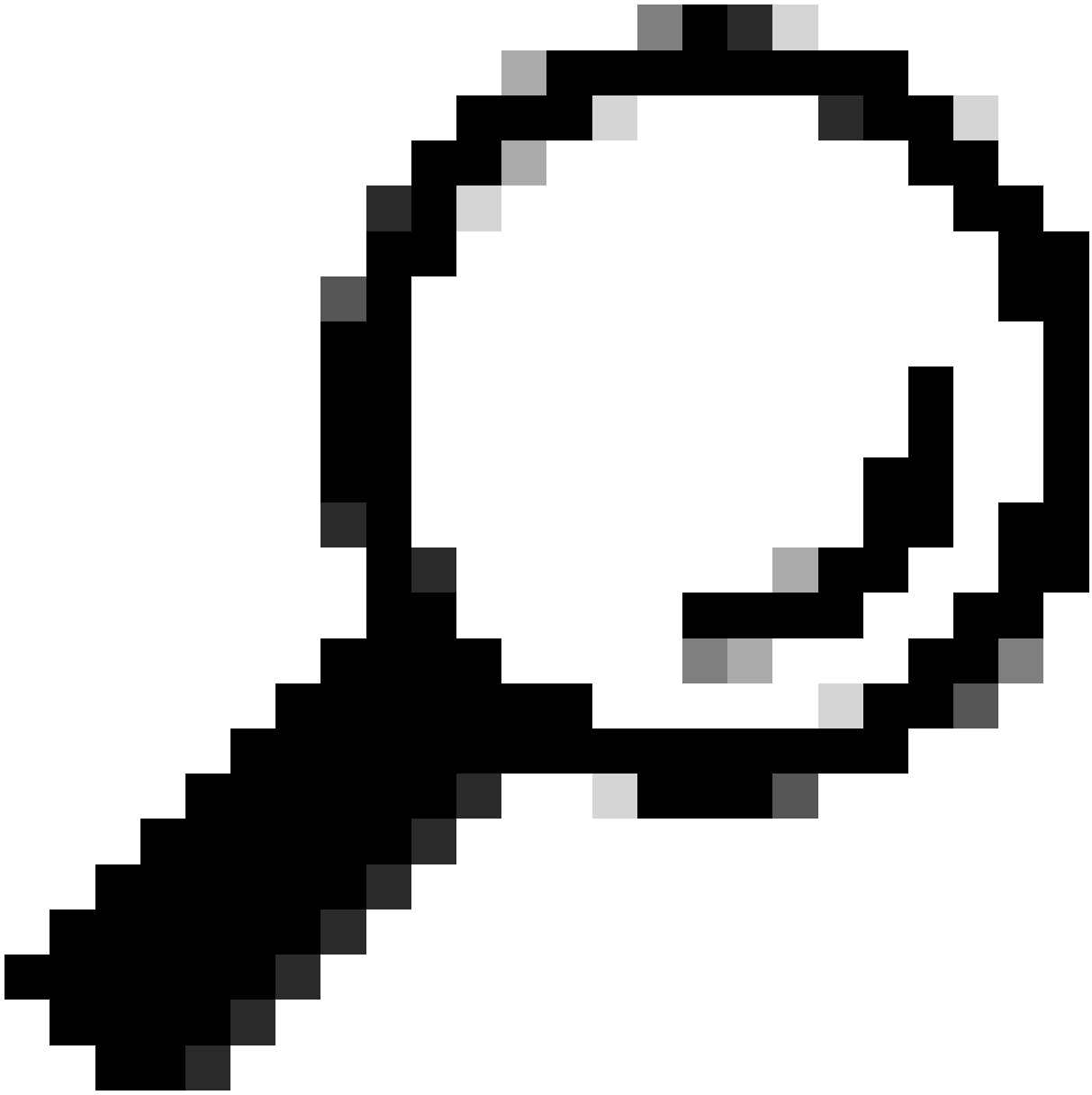
00:00:0C:9F:F2:80

Forward

VXLAN

```
      121
   17096    239       35041
AP APP Fabric Information:
GW_ADDR ENCAP_TYPE VNID SGT FEATURE_FLAG GW_SRC_MAC GW_DST_MAC
```

APには、エッジノードのロケータ172.13.111.65をポイントするアクセストンネルがあります。MACアドレス00:00:0C:9F:F2:80は、スイッチ仮想インターフェイス(SVI)99に属しています。これは、APが接続されているVLANです。カプセル化タイプはVXLANです。



ヒント：トンネルは、アクティブなクライアントが接続されている場合にのみAPに表示されます。それ以外の場合、コマンドは空の出力を返します。

デバッグとトレース

アクセストンネル作成の高度なデバッグを行うには、ファブリックエッジで次のトレースを有効にします。

```
set platformsoftware trace forwarding-manager switch active R0 access-tunnel debug
set platform software trace forwarding-manager switch active F0 access-tunnel debug
set platform software trace forwarding-manager switch active access-tunnel noise
request plat sof trace rotate all
show pla sof trace message forwarding-manager switch active R0 reverse
show pla sof trace message forwarding-manager switch active F0 reverse
```

```
show pla sof trace message fed sw active reverse
```

Catalyst 9000のaccess-tunnel platform-dependentコマンドを使用して、ファブリックエッジ上のアクセストンネルプログラミングを確認します。

```
show platform software fed switch active ifm interfaces access-tunnel
show platform software access-tunnel switch active R0
show platform software access-tunnel switch active R0 statistics
show platform software access-tunnel switch active F0
show platform software access-tunnel switch active F0 statistics
show platform software fed switch active ifm if-id <if-id>
```

WLCでアクセストンネルのプロセスをデバッグするには、次のコマンドを有効にします。

```
set platform software trace wncd chassis active r0 lisp-agent-api
set platform software trace wncd chassis active r0 lisp-agent-db
set platform software trace wncd chassis active r0 lisp-agent-fsm
set platform software trace wncd chassis active r0 lisp-agent-ha
set platform software trace wncd chassis active r0 lisp-agent-internal g
set platform software trace wncd chassis active r0 lisp-agent-lib
set platform software trace wncd chassis active r0 lisp-agent-lispmsg
set platform software trace wncd chassis active r0 lisp-agent-shim
set platform software trace wncd chassis active r0 lisp-agent-transport
```

登録プロセスのデバッグ。これらのコマンドをエッジノードで実行すると、APのIPアドレスとイーサネットMACを登録しようとしているかどうかを確認できます。また、コントロールプレーンで実行すると、登録が正常に行われているかどうかを確認できます。

```
debug lisp filter eid <mac-or-ip>
debug lisp control-plane all
```

要約

- SDアクセスのアクセストンネルは、ファブリックエッジノードと、VXLANでカプセル化されたファブリック内でクライアントトラフィックを伝送するアクセスポイントとの間のVXLANトンネルです。
- セキュリティグループタグ(SGT)はワイヤレスエンドポイントのアクセスポイントレベルでタグ付けされるため、統合ワイヤレスデータプレーンと一貫したポリシー適用が可能になります。
- 検証とトリアージには、ファブリックコントロールプレーンでの登録のチェック、ファブリックエッジノードでの作成の確認、および特定のshowコマンドを使用したWLC上のAPのファブリックステータスの確認が含まれます。
- トラブルシューティングでは、トンネルが正しく作成され、設定の変更後も安定していることを確認することに重点が置かれます。
- 新しいAPをSD-Accessにオンボーディングする際の最終目標は、アクセストンネルです。

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。