

# 了解SD-Access中的接入隧道创建

## 目录

---

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[拓扑](#)

[概述](#)

[接入隧道形成过程](#)

[检验流程](#)

[验证AP是否获取IP地址](#)

[在LISP控制平面上验证AP的IP和以太网MAC注册](#)

[验证WLC是否将设备标记为支持矩阵](#)

[检验LISP控制平面上的无线电MAC注册](#)

[验证访问隧道创建](#)

[调试和跟踪](#)

[摘要](#)

---

## 简介

本文档介绍SD-Access中的接入隧道是什么、其用途以及如何对接入隧道的形成进行分类。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- 定位器ID分离协议(LISP)
- 无线

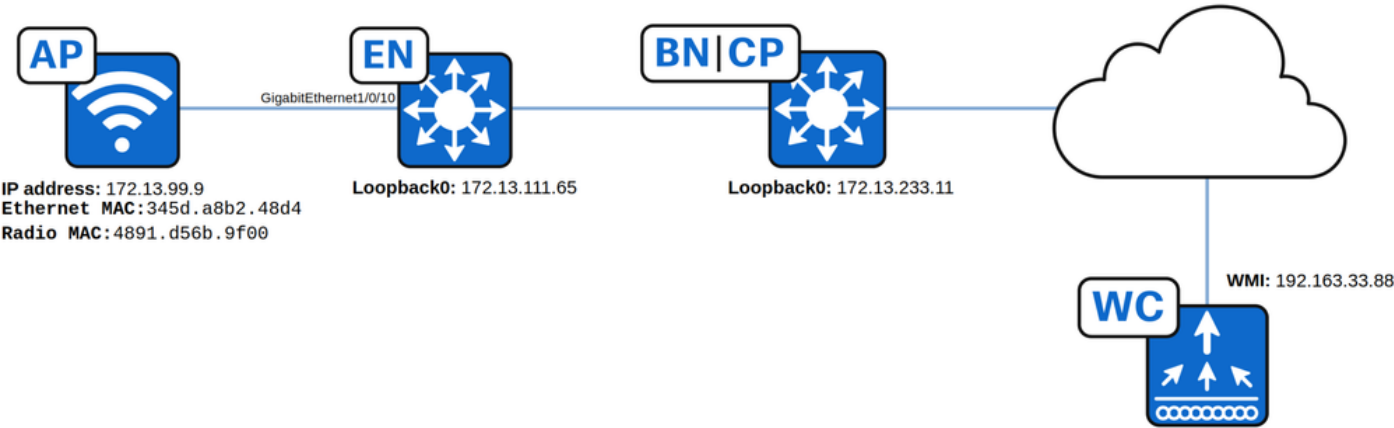
### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科无线局域网控制器(WLC)- C9800-CL、Cisco IOS® XE 17.12.04
- SDA边缘节点 — C9300-48P,Cisco IOS® XE 17.12.05
- SDA边界节点/控制平面 — C9500-48P,Cisco IOS® XE 17.12.05
- 思科接入点 — C9130AXI-A，版本17.9.5.47

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

# 拓扑



本文中使用的拓扑

## 概述

Cisco SD-Access中的接入隧道是在交换矩阵边缘节点和接入点(AP)之间建立的虚拟可扩展局域网(VXLAN)隧道。此隧道在VXLAN中封装客户端流量，从而在SD-Access交换矩阵内实现无缝通信。接入隧道用作数据平面重叠，将流量从连接到接入点的无线客户端传输到交换矩阵边缘，从而确保在整个网络中实现一致的策略实施和分段。

## 接入隧道形成过程

1. AP已插入并通过以太网供电(PoE)通电。
2. AP通过重叠中的DHCP获取IP地址。在此过程中，AP还会从DHCP服务器接收无线LAN控制器的选项43。
3. 交换矩阵边缘注册AP的IP地址和以太网MAC并更新LISP控制平面。
4. WLC查询LISP CP以了解AP是否连接到交换矩阵设备。
5. LISP控制平面使用连接AP的交换矩阵设备的定位器(Loopback 0 IP)对WLC做出应答。如果有答案，则表示AP已连接到交换矩阵并标记为启用交换矩阵。
6. WLC在LISP控制平面中对AP无线电MAC执行L2 LISP注册，同时执行从WLC到FE的元数据信息。
7. LISP控制平面通知交换矩阵边缘并发送从WLC接收的元数据。此元数据包含一个标志，表示它是AP和AP IP地址。
8. 交换矩阵边缘处理信息。它获知它是AP并在该AP和交换矩阵边缘之间创建一个VXLAN隧道，也称为接入隧道。

通读这些步骤，确保在SD-Access中成功形成AP自注册访问隧道。这些检查的任何失败都可能阻止隧道创建。如果某个步骤未能产生预期结果，则应将故障排除工作重点放在与该步骤相关的组件上。

## 检验流程

## 验证AP是否获取IP地址

要验证AP是否收到IP地址，请在边缘节点上运行以下命令：

```
<#root>
```

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

```
...
Network Layer Address   Link Layer Address   Interface   vlan prlv1 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)
```

从之前的输出中可以确认，连接到接口GigabitEthernet 1/0/10的AP在VLAN 99上具有IP地址172.13.99.9，以太网MAC地址为345d.a8b2.48d4。

如果输出为空，则AP无法获取IP地址或以太网供电(PoE)不起作用。要确认PoE运行正常，请运行以下命令，验证接入点的MAC地址显示在MAC地址表中：

```
<#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
```

要确认PoE的内联电源工作正常，请运行以下命令：

```
<#root>
```

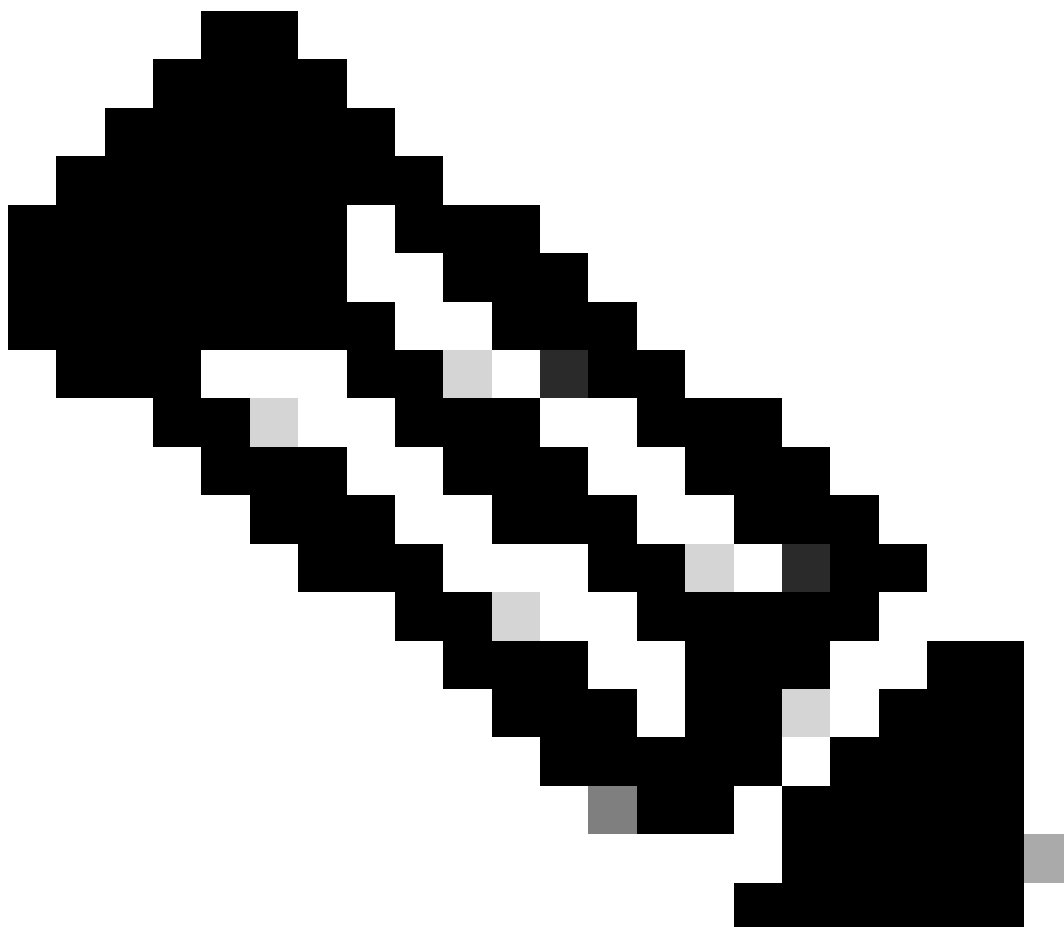
```
Edge#show power inline gigabitEthernet 1/0/10
```

```
Interface Admin
Oper
```

| Power    | Device     | Class | Max  |
|----------|------------|-------|------|
| (Watts)  |            |       |      |
| -----    |            |       |      |
| Gi1/0/10 | auto       |       |      |
| on       |            |       |      |
| 30.0     | C9130AXI-A | 4     | 30.0 |

PoE工作正常，工作功率为30.0瓦。

---



注意：获取IP地址后，接入点会尝试加入无线LAN控制器(WLC)，类似于传统网络。如果在运行show ap summary命令时未列出AP，请排除AP加入故障。

---

在LISP控制平面上验证AP的IP和以太网MAC注册

要标识交换矩阵边缘的控制平面（也称为映射服务器），请运行命令：

<#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
```

控制平面是172.13.233.11，该平面是该设备的环回接口0。

确定交换矩阵站点的控制平面的另一种方法是运行以下命令：

```
<#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
```

在WLC上，您还可以验证与控制平面的LISP会话处于UP状态：

```
<#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

使用此命令查找在控制平面上注册的AP的IP:

<#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



注意：AP始终使用第3层的INFRA\_VN，并且此INFRA\_VN始终映射到实例ID 4097。

IP地址为172.13.99.9的AP已完成注册。没有身份验证失败，它已连接到边缘节点172.13.111.65（定位器）。

要验证MAC地址是否在控制平面上注册，首先要确定AP所连接的VLAN的第2层实例ID。使用下列命令：

```
<#root>
```

```
Edge#show vlan id 99
```

```
VLAN Name Status Ports
```

```
-----
```

```
99
```

```
AP_VLAN active
```

```
L2L10:8188
```

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

VLAN 99映射到实例ID 8188。使用此实例ID，运行以下命令以确认是否在控制平面上注册了以太网MAC地址：

```
<#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的以太网MAC 345d.a8b2.48d4的注册已完成，没有任何身份验证失败，并且已连接到边缘节点172.13.111.65（定位器）。

验证WLC是否将设备标记为支持矩阵

```
<#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地址为172.13.99.9的AP已正确标记为交换矩阵AP。如果AP未列出，则表明WLC无法从LISP控制平面收到响应。在此输出中，AP的无线电MAC地址为4891.d56b.9f00。



注意：如果AP已在控制平面上注册，但未标记为启用交换矩阵，请确保没有防火墙阻止UDP端口4342上的LISP流量。

## 检验LISP控制平面上的无线电MAC注册

使用与验证以太网MAC地址注册相同的命令，但用无线电MAC地址替换以太网MAC地址：

```
<#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

无线电MAC地址已完全注册，没有任何身份验证失败，并连接到边缘节点172.13.111.65 ( 定位器 )。 输出还显示WLC AP位：设置，LISP控制平面使用的标志，用于向边缘节点指示此注册属于其RLOC 172.13.111.65上的AP。

## 验证访问隧道创建

最后一步是检验交换矩阵边缘上访问隧道的创建。如前所述，这是SD-Access中AP自注册的最终目标。要验证访问隧道的创建，请运行以下命令：

<#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 0x000000058 0 day, 00:00:51

接入隧道0将AP 172.13.99.9连接到边缘节点定位器172.13.111.65，并且已运行51秒。每次重置后，计时器都设置为0。

您还可以确认隧道在转发引擎驱动程序(FED)抽象层编程，该抽象层直接与交换机硬件连接：

<#root>

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

Interface IF\_ID State

-----  
Ac0  
0x000000058  
READY

使用IF\_ID，您可以找到有关此隧道的更多信息：

<#root>

Edge#show platform software fed switch active ifm if-id 0x000000058

Interface IF\_ID : 0x00000000000000058  
Interface Name : Ac0  
Interface Block Pointer : 0x73d6c83dc6f8

Interface Block State : READY

Interface State : Enabled

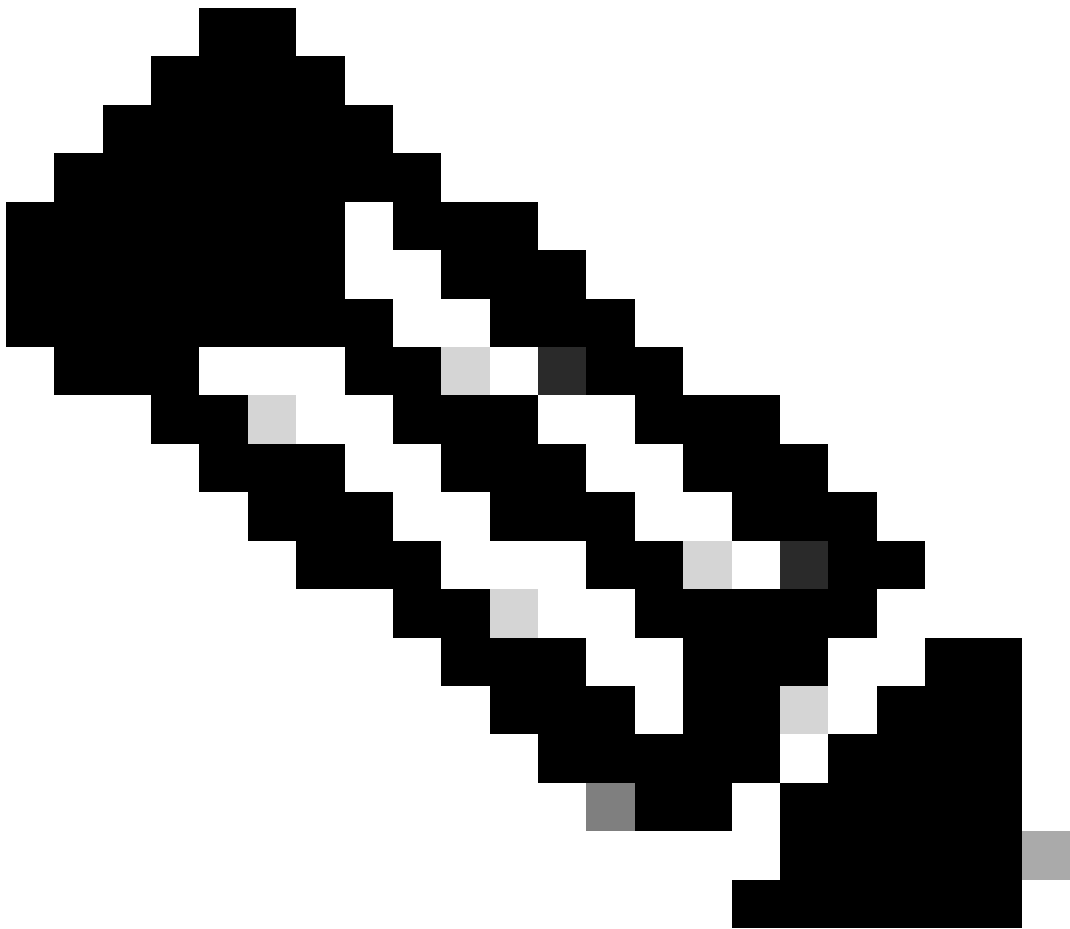
...

Interface Type : ACCESS\_TUNNEL

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

这是使用VXLAN封装的L2 lisp隧道，接口类型为access-tunnel。

---



注意：在show access-tunnel summary命令和FED命令的输出中，访问隧道的数量必须匹配。不匹配可能表示编程错误。

---

在AP上，您可以使用以下命令验证访问隧道的创建：

<#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

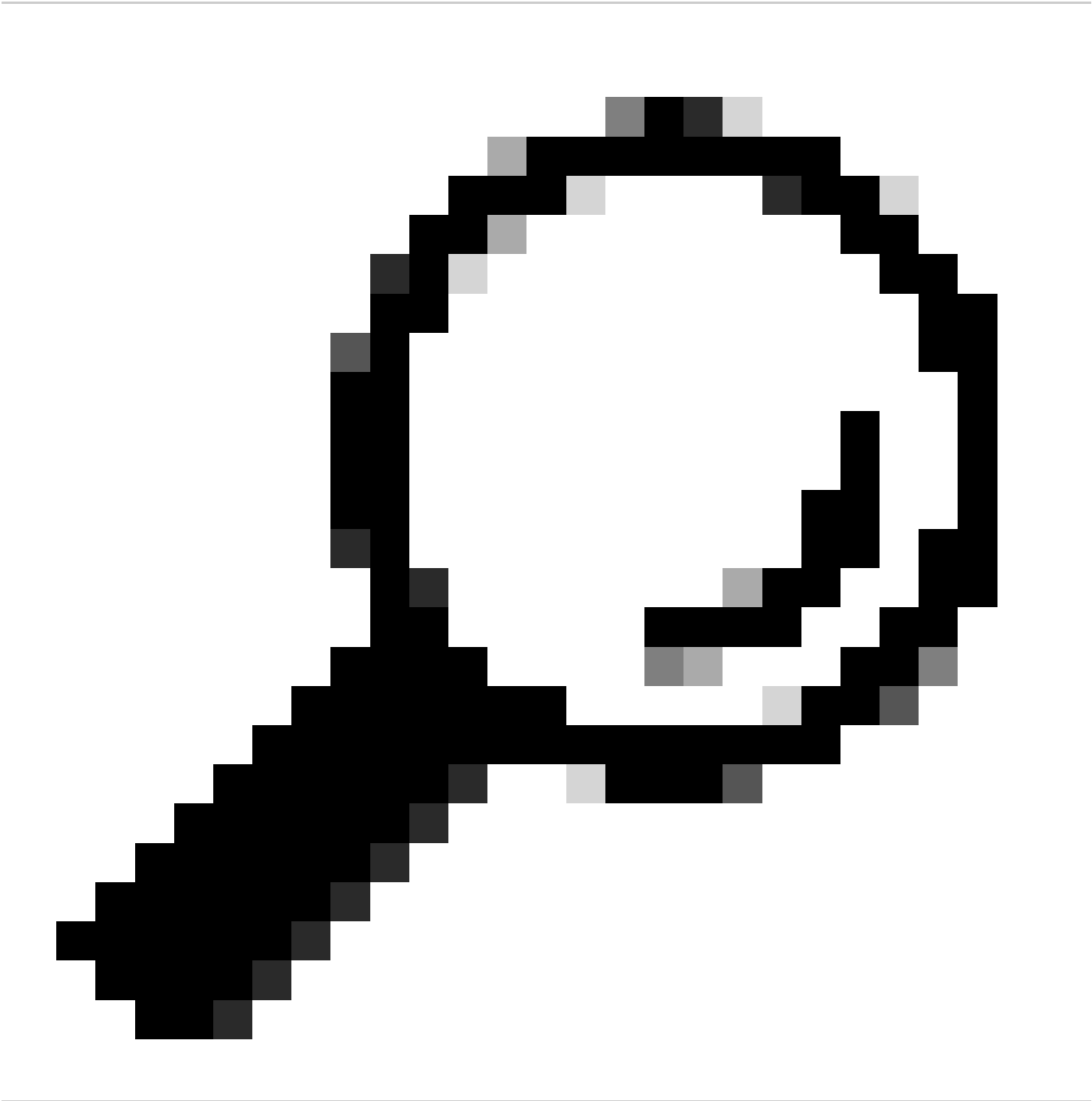
00:00:0C:9F:F2:80

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具有指向边缘节点定位器172.13.111.65的访问隧道。MAC地址00:00:0C:9F:F2:80属于交换机虚拟接口(SVI)99，即AP所连接的VLAN。封装类型是VXLAN。



---

提示：仅当连接活动客户端时，隧道才会显示在AP上。否则，该命令将返回空输出。

---

## 调试和跟踪

要更高级地调试访问隧道创建，请在交换矩阵边缘启用以下跟踪：

```
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 access-tunnel platform-dependent命令，用于验证交换矩阵边缘上的访问隧道编程：

```
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>
```

要调试WLC上访问隧道的进程，请启用以下命令：

```
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-lispmmsg
set platform software trace wncd chassis active r0 lisp-agent-shim
set platform software trace wncd chassis active r0 lisp-agent-transport
```

注册过程的调试。这些命令可以在边缘节点上运行以验证它是否正在尝试注册AP的IP地址和以太网MAC，也可以在控制平面上运行以确认注册是否成功进行。

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

## 摘要

- SD-Access中的接入隧道是交换矩阵边缘节点和接入点之间的VXLAN隧道，在VXLAN中封装的交换矩阵内传输客户端流量。

- 它们支持统一无线数据平面和一致的策略实施，因为安全组标记(SGT)在无线终端的接入点级别进行标记。
- 验证和分类涉及检查交换矩阵控制平面上的注册，确认在交换矩阵边缘节点上创建，以及使用特定的show命令验证WLC上AP的交换矩阵状态。
- 故障排除的重点是确保正确创建隧道并在配置更改后保持稳定。
- 将新的AP注册到SD-Access时，接入隧道是最终目标。

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。