SD-Access에서 액세스 터널 생성 이해

목차

소개

이 문서에서는 SD-Access에 있는 액세스 터널의 내용, 목적 및 액세스 터널의 형성을 분류하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- LISP(Locator ID Separation Protocol)
- 무선

사용되는 구성 요소

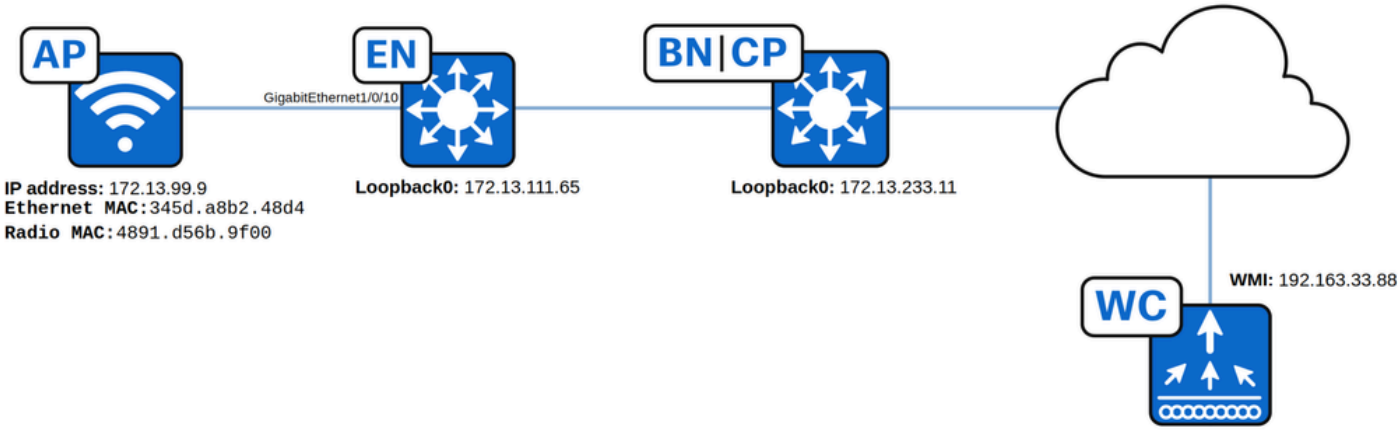
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco WLC(Wireless LAN Controller) - C9800-CL, Cisco IOS® XE 17.12.04
- SDA 에지 노드 - C9300-48P, Cisco IOS® XE 17.12.05
- SDA 보더 노드/컨트롤 플레인 - C9500-48P, Cisco IOS® XE 17.12.05
- Cisco Access Point - C9130AXI-A, 버전 17.9.5.47

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

토폴로지



이 문서에서 사용된 토폴로지

개요

Cisco SD-Access의 액세스 터널은 패브릭 에지 노드와 AP(Access Point) 사이에 설정된 VXLAN(Virtual Extensible LAN) 터널입니다. 이 터널은 VXLAN에서 클라이언트 트래픽을 캡슐화하여 SD-Access 패브릭 내에서 원활한 통신을 지원합니다. 액세스 터널은 액세스 포인트에 연결된 무선 클라이언트에서 패브릭 엣지로 트래픽을 전달하는 데이터 플레인 오버레이의 역할을 하며, 네트워크 전체에서 일관된 정책 시행 및 세그멘테이션을 보장합니다.

액세스 터널 형성 프로세스

1. AP가 연결되어 있고 PoE(Power over Ethernet)를 통해 전원이 켜집니다.
2. AP는 오버레이에서 DHCP를 통해 IP 주소를 가져옵니다. 이 과정에서 AP는 DHCP 서버에서 Wireless LAN Controller에 대한 옵션 43도 받습니다.
3. 패브릭 엣지는 AP의 IP 주소 및 이더넷 MAC를 등록하고 LISP 컨트롤 플레인을 업데이트합니다.
4. WLC는 LISP CP에 쿼리하여 AP가 패브릭 디바이스에 연결되었는지 확인합니다.
5. LISP 컨트롤 플레인은 AP가 연결된 패브릭 디바이스의 로케이터(루프백 0 IP)를 사용하여 WLC에 응답합니다. 답변이 있으면 AP가 패브릭에 연결되어 있고 패브릭 활성화로 표시됨을 의미합니다.
6. WLC는 LISP 제어 평면에서 AP 무선 MAC에 대해 WLC에서 FE로의 메타데이터 정보와 함께 L2 LISP 등록을 수행합니다.
7. LISP 컨트롤 플레인에서 패브릭 에지에 알리고 WLC에서 받은 메타데이터를 전송합니다. 이 메타데이터에는 AP 및 AP IP 주소임을 나타내는 플래그가 포함되어 있습니다.
8. 패브릭 에지에서 정보를 처리합니다. AP임을 인식하고 AP와 패브릭 에지 사이에 액세스 터널이라고도 하는 VXLAN 터널을 생성합니다.

SD-Access 내에서 AP 온보딩을 위한 액세스 터널 형성이 성공적으로 이루어지도록 하려면 다음

단계를 읽어 보십시오. 이러한 확인에 실패하면 터널 생성을 방지할 수 있습니다. 한 단계에서 예상한 결과가 나오지 않으면 해당 단계와 관련된 구성 요소에 문제 해결 작업을 집중합니다.

프로세스 확인

AP가 IP 주소를 획득하는지 확인

AP가 IP 주소를 수신하는지 확인하려면 에지 노드에서 다음 명령을 실행합니다.

<#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)

이전 출력에서 인터페이스 GigabitEthernet 1/0/10에 연결된 AP가 VLAN 99의 IP 주소 172.13.99.9이며 이더넷 MAC 주소 345d.a8b2.48d4임을 확인할 수 있습니다.
출력이 비어 있으면 AP가 IP 주소를 가져오지 못했거나 PoE(Power over Ethernet)가 작동하지 않습니다. PoE가 작동하는지 확인하려면 다음 명령을 실행하여 액세스 포인트의 MAC 주소가 MAC 주소 테이블에 표시되는지 확인합니다.

<#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

PoE의 인라인 전원이 작동하는지 확인하려면 다음 명령을 실행합니다.

<#root>

Edge#show power inline gigabitEthernet 1/0/10

```
Interface  Admin
```

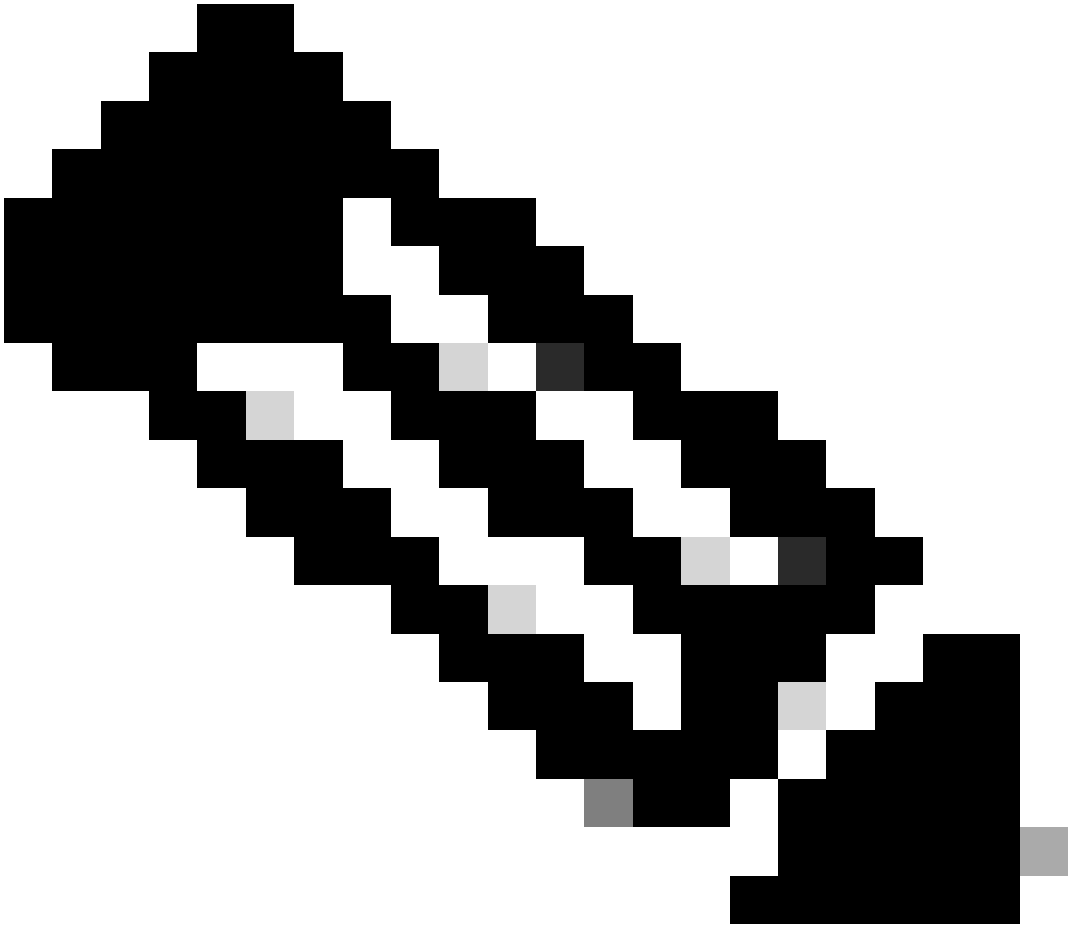
Oper

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

on

```
     30.0   C9130AXI-A   4    30.0
```

PoE는 작동 중이며 30.0와트로 작동합니다.



참고: 액세스 포인트는 IP 주소를 얻은 후 기존 네트워킹과 마찬가지로 WLC(Wireless LAN

Controller)에 연결하려고 시도합니다. show ap summary 명령을 실행할 때 AP가 나열되지 않으면 AP 조인의 문제를 해결합니다.

LISP 컨트롤 플레인에서 AP의 IP 및 이더넷 MAC 등록 확인

패브릭 에지에 대한 제어 평면(맵 서버라고도 함)을 식별하려면 다음 명령을 실행합니다.

<#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
```

컨트롤 플레인은 172.13.233.11이며, 이는 해당 디바이스의 루프백0이 됩니다.

패브릭 사이트의 컨트롤 플레인을 식별하는 또 다른 방법은 이 명령을 실행하는 것입니다.

<#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
```

WLC에서 컨트롤 플레인의 LISP 세션이 UP 상태임을 확인할 수도 있습니다.

<#root>

WLC#show wireless fabric summary

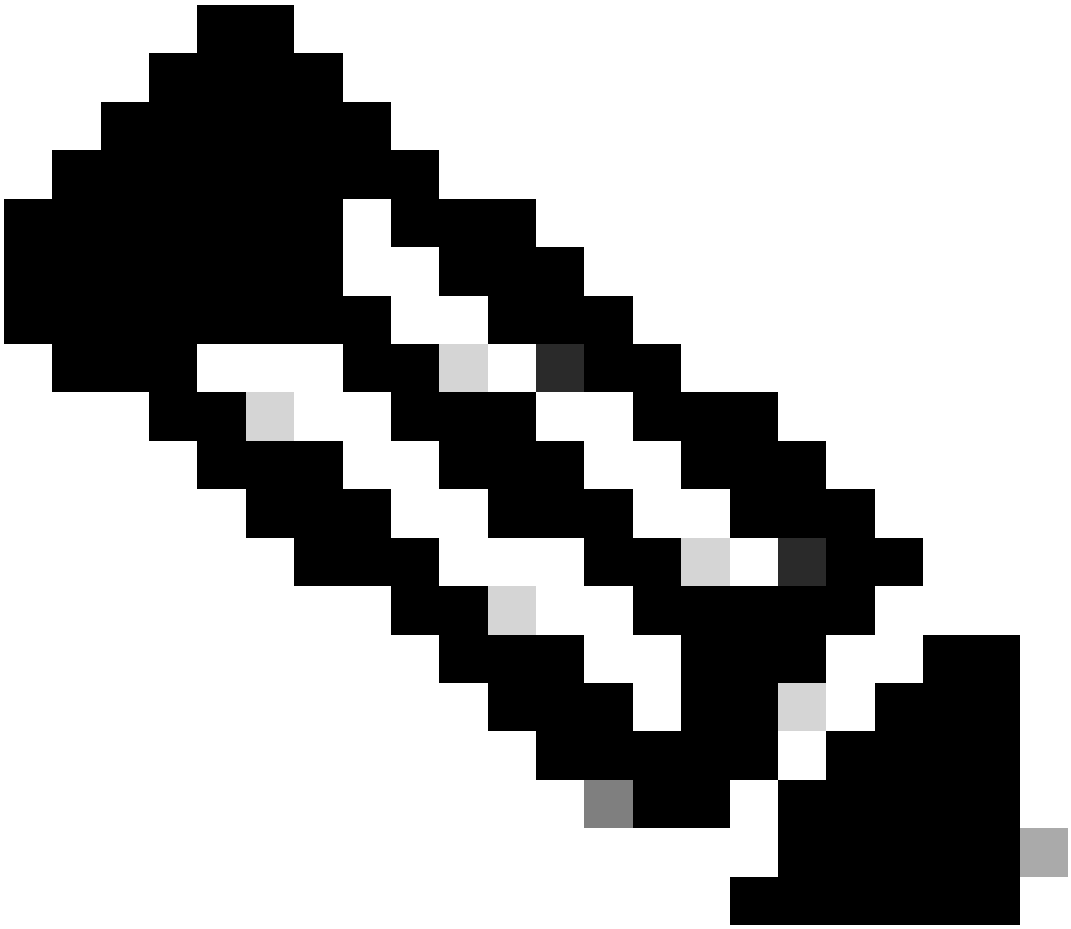
```
Fabric Status :

Enabled



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

172.13.233.11

    ddc2df8446e2479d

Up
```

이 명령을 사용하여 제어 평면에 등록된 AP의 IP를 찾을 수 있습니다.

<#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
```



참고: AP는 항상 레이어 3에 INFRA_VN을 사용하며, 이 INFRA_VN은 항상 인스턴스 ID 4097에 매핑됩니다.

IP 주소가 172.13.99.9인 AP에 대한 등록이 완료되었습니다. 인증 실패가 없으며 에지 노드 172.13.111.65(로케이터)에 연결됩니다.

MAC 주소가 제어 평면에 등록되어 있는지 확인하려면 먼저 AP가 연결된 VLAN의 레이어 2 인스턴스 ID를 식별합니다. 다음 명령을 사용합니다.

<#root>

Edge#show vlan id 99

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

```
99

 AP_VLAN active

L2LI0:8188

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

VLAN 99는 인스턴스 ID 8188에 매핑됩니다. 이 인스턴스 ID를 사용하여 이 명령을 실행하여 이더넷 MAC 주소가 제어 평면에 등록되었는지 확인합니다.

<#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
```

AP의 이더넷 MAC 345d.a8b2.48d4 등록이 인증 실패 없이 완료되었으며 에지 노드 172.13.111.65(Locator)에 연결됩니다.

WLC에서 디바이스를 패브릭 활성화로 표시하는지 확인합니다.

<#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

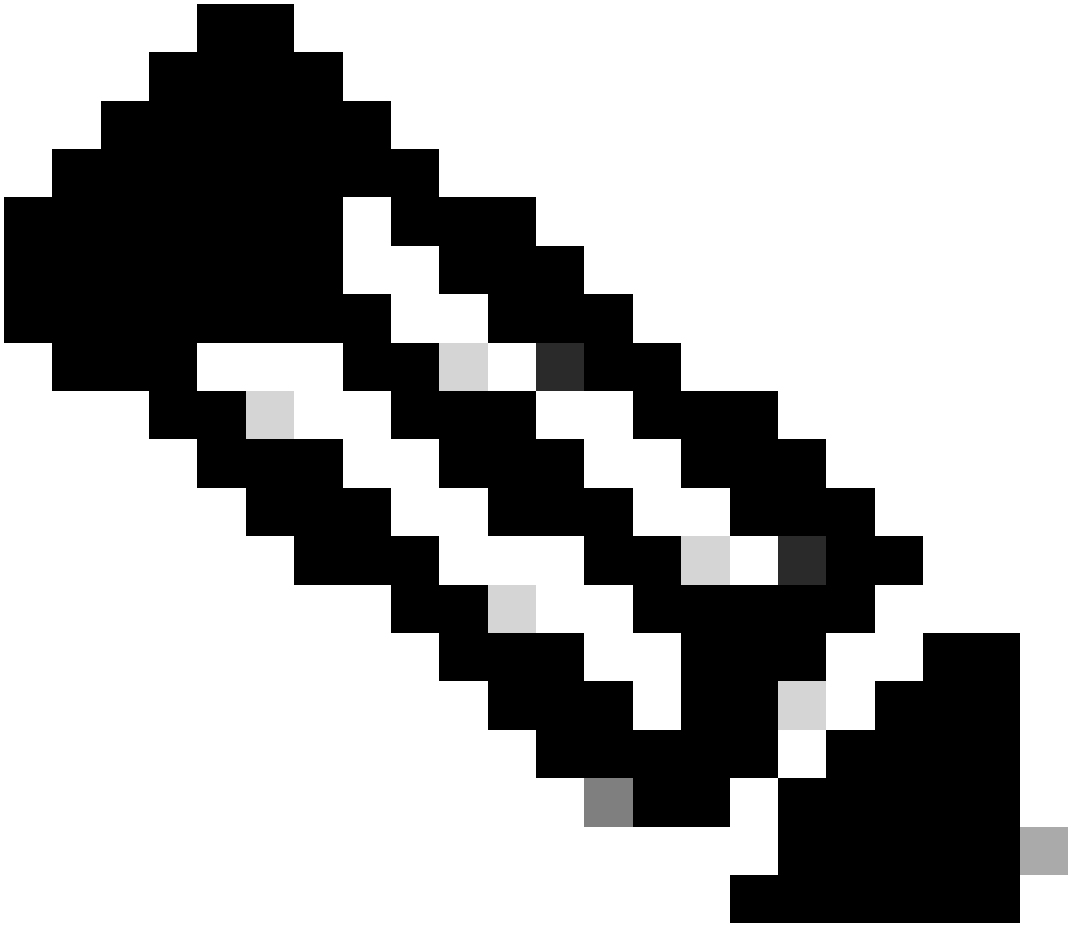
4891.d56b.9f00

default location MX

172.13.99.9

Registered

IP 주소가 172.13.99.9인 AP가 패브릭 AP로 올바르게 표시됩니다. AP가 나열되지 않으면 WLC가 LISP 제어 플레인에서 응답을 받지 못했음을 나타냅니다. 이 출력에서 AP의 무선 MAC 주소는 4891.d56b.9f00입니다.



참고: AP가 제어 평면에 등록되었지만 Fabric-enabled로 표시되지 않은 경우, 방화벽이 UDP 포트 4342의 LISP 트래픽을 차단하지 않는지 확인합니다.

LISP 컨트롤 플레인에서 Radio MAC 등록 확인

이더넷 MAC 주소의 등록을 확인하는 데 사용된 것과 동일한 명령을 사용하되 이더넷 MAC 주소를 무선 MAC 주소로 교체합니다.

<#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
```

무선 MAC 주소는 인증 실패 없이 완전히 등록되며 에지 노드 172.13.111.65(Locator)에 연결됩니다. 출력에는 WLC AP 비트도 표시됩니다. LISP 컨트롤 플레인에서 이 등록이 RLOC 172.13.111.65의 AP에 속한다는 것을 에지 노드에 나타내기 위해 사용하는 플래그입니다.

액세스 터널 생성 확인 합니다

마지막 단계는 패브릭 에지에 액세스 터널이 생성되었는지 확인하는 것입니다. 앞에서 설명한 것처럼, 이는 SD-Access에서 AP 온보딩의 궁극적인 목표입니다. 액세스 터널의 생성을 확인하려면 다음 명령을 실행합니다.

<#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

액세스 터널 0은 AP 172.13.99.9를 에지 노드 로케이터 172.13.111.65에 연결하며 51초 동안 가동되었습니다. 모든 재설정 후 타이머가 0으로 설정됩니다.

또한 터널이 FED(Forwarding Engine Driver) 추상화 레이어에서 프로그래밍되었는지 확인할 수 있습니다. 이 추상화 레이어는 스위치 하드웨어와 직접 인터페이스합니다.

<#root>

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

Interface IF_ID State

Ac0

0x00000058

READY

IF_ID를 사용하여 이 터널에 대한 자세한 정보를 찾을 수 있습니다.

<#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

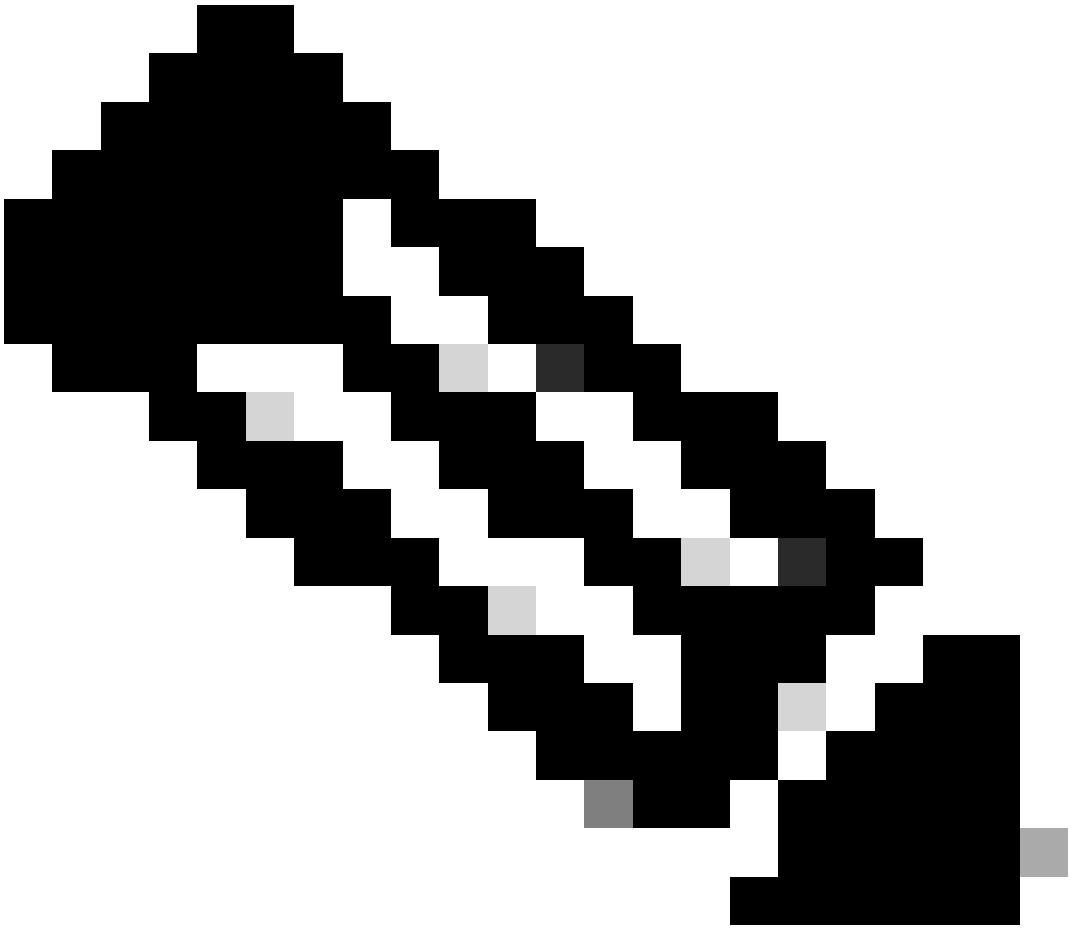
...

Interface Type : ACCESS_TUNNEL

...
Tunnel Type : L2Lisp

```
Encap Type : VxLan
...
```

이는 VXLAN 캡슐화를 사용하는 L2 lisp 터널이며 인터페이스 유형은 access-tunnel입니다.



참고: show access-tunnel summary 명령 및 FED 명령의 출력에서 일치하는 액세스 터널 수가 중요합니다. 불일치는 잘못된 프로그래밍을 나타낼 수 있습니다.

AP에서 다음 명령을 사용하여 액세스 터널의 생성을 확인할 수 있습니다.

<#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

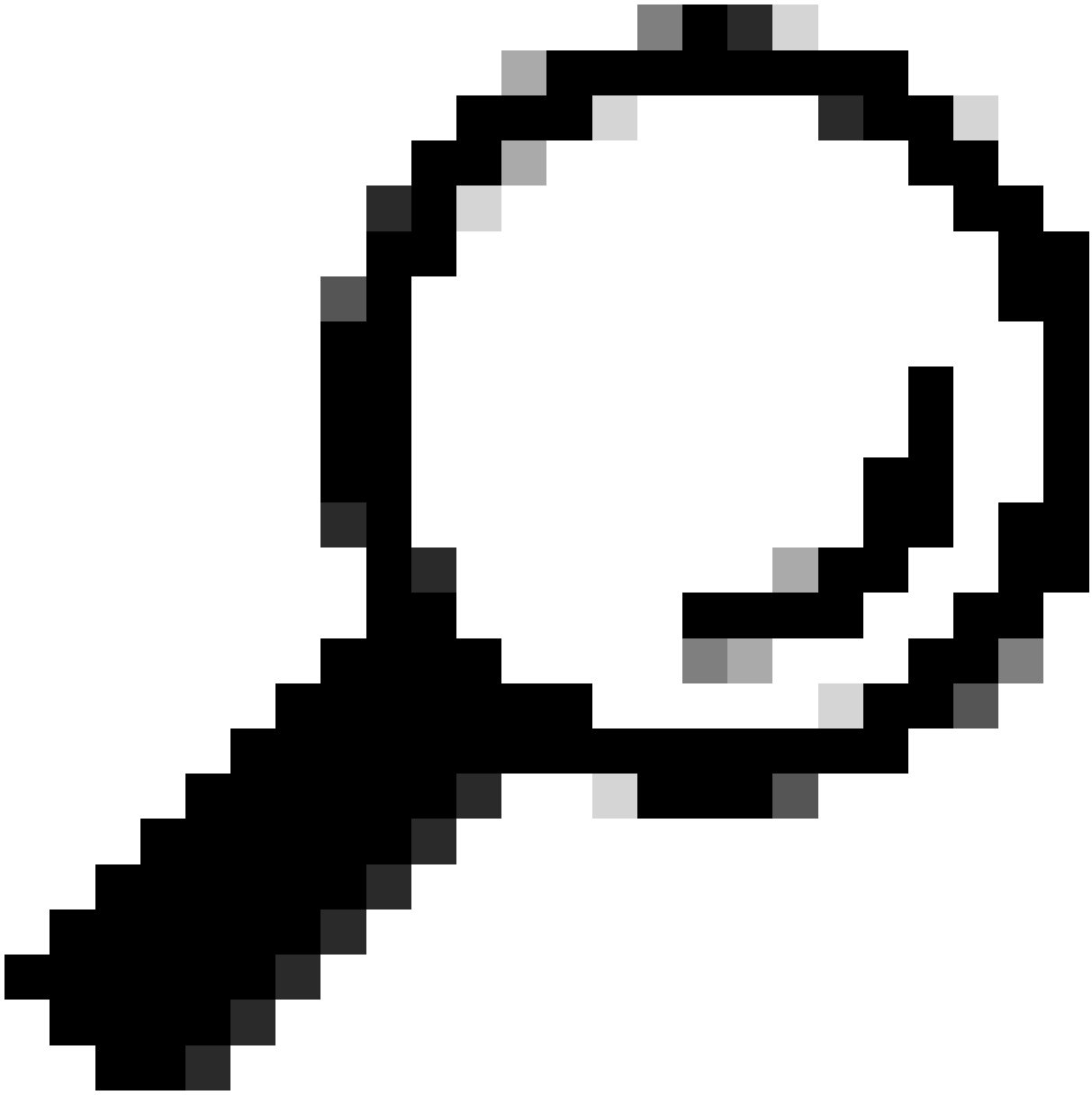
00:00:0C:9F:F2:80

Forward

VXLAN

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

AP에는 에지 노드의 로케이터 172.13.111.65를 가리키는 액세스 터널이 있습니다. MAC 주소 00:00:0C:9F:F2:80은 AP가 연결된 VLAN인 SVI(Switch Virtual Interface) 99에 속합니다. 캡슐화 유형은 VXLAN입니다.



팁: 활성 클라이언트가 연결된 경우에만 AP에 터널이 표시됩니다. 그렇지 않으면 빈 출력이 반환됩니다.

디버그 및 추적

액세스 터널 생성을 보다 상세하게 디버깅하려면 패브릭 에지에서 다음 추적을 활성화합니다.

```
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
```

패브릭 에지에서 액세스 터널 프로그래밍을 검증하는 Catalyst 9000 access-tunnel platform-dependent 명령:

```
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>
```

WLC에서 액세스 터널에 대한 프로세스를 디버깅하려면 다음 명령을 활성화합니다.

```
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
```

등록 프로세스를 위한 디버깅. 이러한 명령은 에지 노드에서 실행하여 AP의 IP 주소 및 이더넷 MAC 등록을 시도하는지 확인하고, 제어 평면에서 등록에 성공했는지 확인할 수 있습니다.

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

요약

- SD-Access의 액세스 터널은 VXLAN에 캡슐화된 패브릭 내에서 클라이언트 트래픽을 전달하는 액세스 포인트와 패브릭 에지 노드 간의 VXLAN 터널입니다.
- SGT(Security Group Tag)가 무선 엔드포인트의 액세스 포인트 레벨에서 태깅되기 때문에 통합된 무선 데이터 플레인과 일관된 정책 시행이 가능합니다.
- 확인 및 분류 작업에는 패브릭 제어 평면의 등록을 확인하고, 패브릭 에지 노드의 생성을 확인하고, 특정 show 명령을 사용하여 WLC에서 AP의 패브릭 상태를 확인하는 작업이 포함됩니다.
- 트러블슈팅은 터널이 올바르게 생성되고 컨피그레이션 변경 후에도 안정적으로 유지되도록 하는 데 중점을 둡니다.
- 액세스 터널은 SD-Access에 새 AP를 온보딩할 때 최종 목표입니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.