# SD-Access 무선 초기 설정 문제 해결 및 확인

## 목차



## 소개

이 문서에서는 SD-Access 무선 설정의 기본 연결 문제를 식별하는 기본 문제 해결 단계를 설명합니다. 이 표에서는 무선 관련 솔루션의 문제를 격리하기 위해 확인하는 항목과 명령에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

SD-Access 솔루션에 대한 지식

에서 이미 SD 액세스 토폴로지를 설정했습니다.

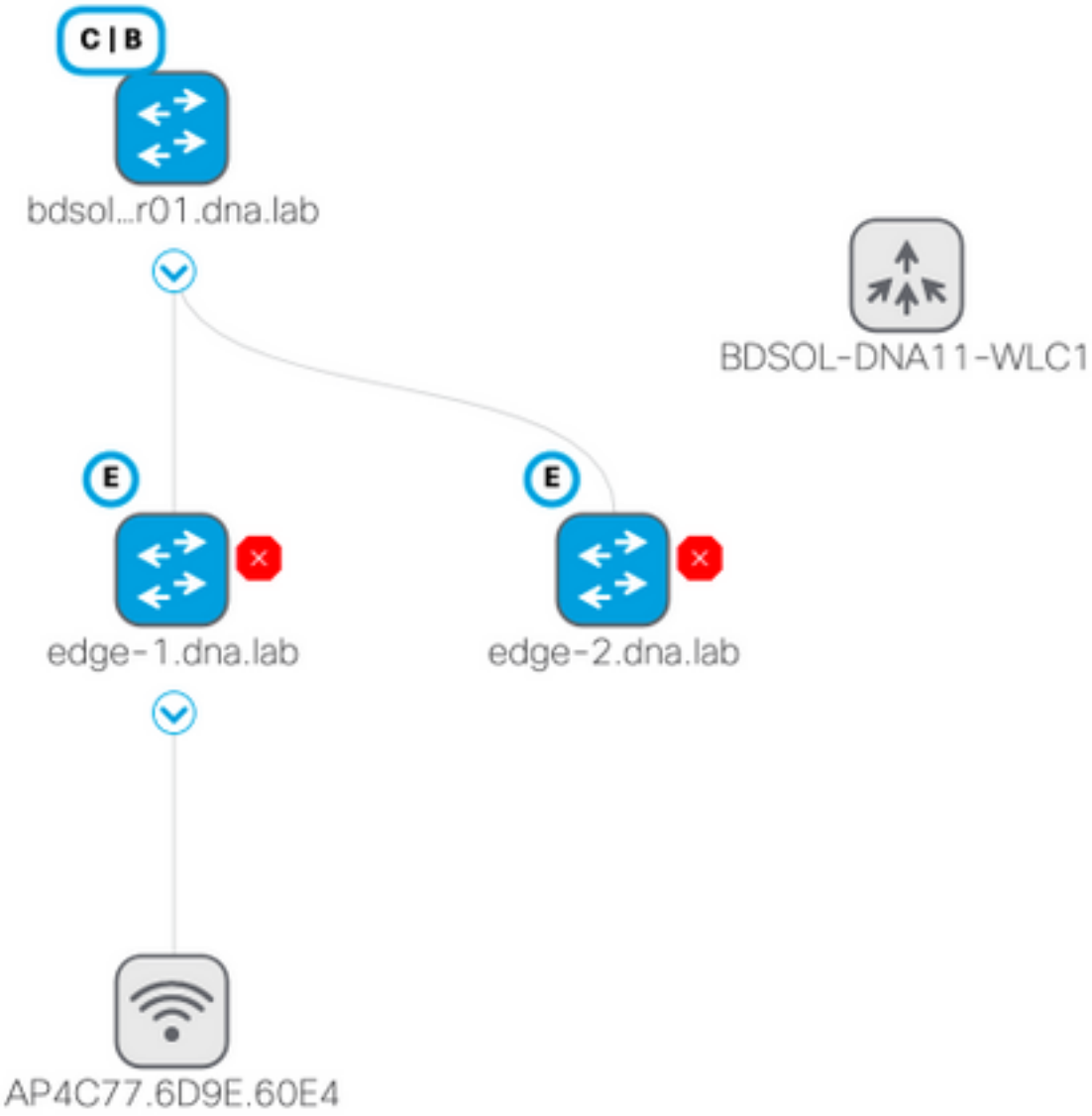
### 사용되는 구성 요소

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다. SD 액세스 무선에 대해 지원되는 다른 유형의 장치가 있지만 이 문서에서는 이 섹션에 설명된 장치를 중점적으로 다룹니다. 명령은 플랫폼 및 소프트웨어 버전에 따라 달라질 수 있습니다.

8.5.151 무선 컨트롤러

에지 노드로서의 16.9.3 9300 스위치

### 토폴로지




## 문제 해결 및 격리

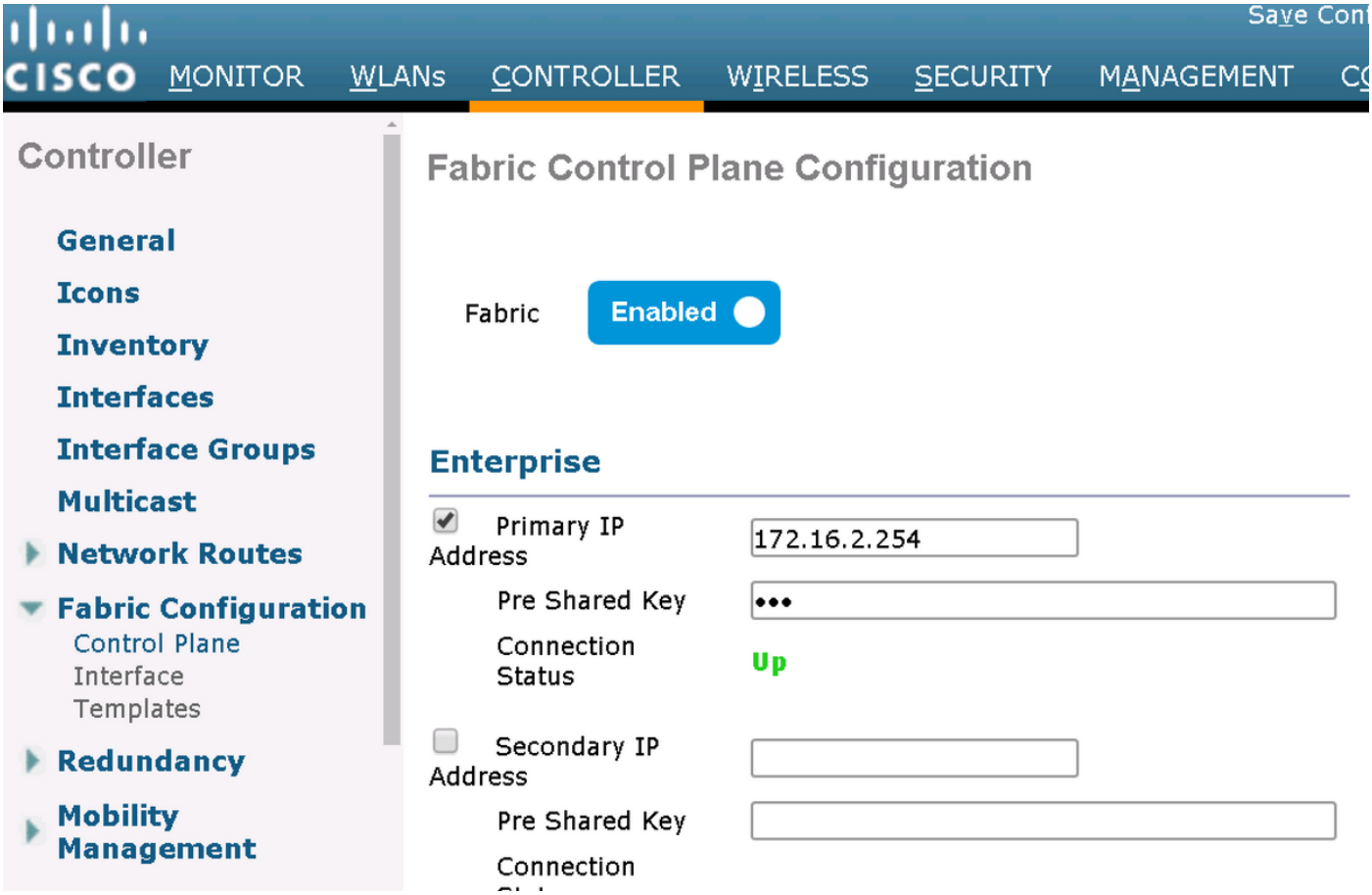
### 빠른 확인

SD 액세스 시나리오에는 종종 실수의 원인이 되는 일련의 요구 사항이 있으므로 이러한 요구 사항이 충족되었는지 먼저 확인하십시오.

- LISP 제어 평면 노드의 WLC를 가리키는 특정 경로(기본 경로를 사용하지 않음)가 있는지 확인합니다
- 글로벌 라우팅 테이블을 사용하여 AP가 Infra VN에 있는지 확인합니다
- AP 자체에서 WLC를 ping하여 AP가 WLC에 연결되어 있는지 확인합니다
- WLC에서 제어 평면의 패브릭 상태가 가동 상태인지 확인합니다
- AP가 패브릭 지원 상태인지 확인합니다

## 시나리오 1. LISP/MAP 서버 컨트롤 플레인에 WLC 등록 확인

WLC를 DNA Center의 패브릭에 추가하면 DNA-C에서 컨트롤 플레인으로 정의된 노드에 대한 연결을 설정하기 위해 명령이 컨트롤러에 푸시됩니다. 첫 번째 단계는 이러한 등록이 성공적으로 이루어지도록 하는 것입니다. 컨트롤 플레인의 LISP 컨피그레이션이 어떤 식으로든 손상되면 이 등록이 실패할 수 있습니다.




이 상태가 down으로 표시되면 WLC와 제어 평면 간에 디버그 또는 패킷 캡처를 실행하는 것이 유용할 수 있습니다. 등록에는 4342의 TCP와 UDP가 모두 포함됩니다. 제어 평면이 적절한 컨피그레이션을 얻지 못한 경우 WLC에서 보낸 TCP SYN에 TCP RST로 응답할 수 있습니다.

명령줄에서 show fabric map-**server summary를 사용하여 동일한** 상태를 확인할 수 있습니다. 이 프로세스는 WLC CLI에서 **debug fabric lisp map-server all**로 디버깅됩니다. 재연결 시도를 유발하려면 DNA Center로 이동하여 패브릭에서 WLC를 제거한 후 다시 추가하도록 선택할 수 있습니다.

가능한 원인은 컨트롤 플레인에 컨피그레이션 라인이 없습니다. 작동 컨피그레이션의 예는 다음과 같습니다(가장 중요한 부분만 해당).

```
rtr-cp-mer-172_16_200_4#show run | s WLC
 locator-set WLC
  10.241.0.41
  exit-locator-set
 map-server session passive-open WLC
```

WLC ip가 없거나(10.241.0.41) passive-open 명령이 없으면 CP는 WLC 연결을 거부합니다.

실행할 디버깅은 다음과 같습니다.

- **'debug capwap events enable'**

- **'debug capwap errors enable'**
- **'debug fabric ap-join events enable( ap-join )'**
- **'debug fabric ap-join detail enable'**
- **'debug fabric lisp map-server all enable'**

WLC

```
*msfMsgQueueTask: May 07 14:08:10.080: Sent map-request to MS 10.32.47.128 for AP 10.32.58.36
VNID 4097
*msfMsgQueueTask: May 07 14:08:10.080: No messages are present in the Client list for Local UDP
socket
*msfMsgQueueTask: May 07 14:08:10.080: msfSendLocalUDPSocketMessage:637 Message get for UDP file
socket list with path /tmp/msif_local_udp_socket_file failed
*osapiBsnTimer: May 07 14:08:15.179: Map-reply timer for MS IP 10.32.47.128 expired for AP IP
10.32.58.36 and VNID 4097
*msfMsgQueueTask: May 07 14:08:15.179: msfQueue: recieved LISP_MAP_SERVER_TIMEOUT_QUEUE_MSG
*msfMsgQueueTask: May 07 14:08:15.179: Found entry AP 10.32.58.36 vnid 4097
*msfMsgQueueTask: May 07 14:08:15.179: Added AP 10.32.58.36 VNID 4097 for long retry map-request
*msfMsgQueueTask: May 07 14:08:15.179: Found entry AP 10.32.58.36 vnid 4097
*msfMsgQueueTask: May 07 14:08:15.179: No messages are present in the Client list for Local UDP
socket
*msfMsgQueueTask: May 07 14:08:15.179: msfSendLocalUDPSocketMessage:637 Message get for UDP file
socket list with path /tmp/msif_local_udp_socket_file failed
*spamApTask0: May 07 14:08:16.084: 00:fc:ba:15:95:00 WTP Event Request from 10.32.58.36:5248
epoch 1525694896
*spamApTask0: May 07 14:08:16.084: 00:fc:ba:15:95:00 WTP Event Response sent to 10.32.58.36:5248
*osapiBsnTimer: May 07 14:08:17.839: NAK Timer expiry callback
*msfMsgQueueTask: May 07 14:08:17.839: msfQueue: recieved LISP_MAP_SERVER_NAK_TIMEOUT_QUEUE_MSG
*msfMsgQueueTask: May 07 14:08:17.839: Started periodic NAK processing timer
*msfMsgQueueTask: May 07 14:08:17.839: Process list of AP (1) for which RLOC is not received
```

패브릭 제어 평면에 WLC에 대한 특정 경로가 없기 때문에 패브릭 비활성화 상태에서 AP에 조인하는 WLC 디버깅의 예입니다

```
(POD3-WLC1) >*emWeb: Oct 16 08:54:21.593: Fabric is supported for apType 54

*emWeb: Oct 16 08:54:21.593: Fabric is supported for apType 54

*emWeb: Oct 16 08:55:26.295: ip c0a82700,subnet ffffff00,l2vnid 8191,l3vnid 1001
*emWeb: Oct 16 08:55:26.295: Vnid Mapping added at index 2 with entries 192_168_39_0-
INFRA_VN,8191,4097,c0a82700,ffffff00.Count 3

*emWeb: Oct 16 08:55:26.295:
                            Log to TACACS server(if online): fabric vnid create name
192_168_39_0-INFRA_VN l2-vnid 8191 ip 192.168.39.0 subnet 255.255.255.0 l3-vnid 4097

*spamReceiveTask: Oct 16 08:55:26.295: Fabric is supported for AP f4:db:e6:61:24:a0 (Pod3-
AP4800). apType 54

*spamReceiveTask: Oct 16 08:55:26.295: spamProcessFabricVnidMappingAddRequest: Fabric Adding
vnid mapping for AP Pod3-AP4800 f4:db:e6:61:24:a0,lradIp 192.168.39.100,AP l2_vnid 0, AP l3_vnid
0
*spamReceiveTask: Oct 16 08:55:26.295: Vnid Mapping return from index 2 with entries name
192_168_39_0-INFRA_VN,l2vnid 8191,l3vnid 4097,ip c0a82700,mask ffffff00.Count 3

*spamReceiveTask: Oct 16 08:55:26.295: spamSendFabricMapServerRequest: MS request from AP Pod3-
AP4800 f4:db:e6:61:24:a0,l3vnid 4097,PMS 192.168.30.55,SMS 0.0.0.0,mwarIp 192.168.31.59,lradIp
192.168.39.100
*emWeb: Oct 16 08:55:29.944:
                            Log to TACACS server(if online): save
```

```
(POD3-WLC1) >*spamApTask6: Oct 16 08:56:49.243: Fabric is supported for AP f4:db:e6:64:02:a0
(Pod3-AP3800). apType 52,apModel AIR-AP3802I-B-K9.

*spamApTask6: Oct 16 08:56:51.949: Fabric is supported for AP f4:db:e6:64:02:a0 (Pod3-AP3800).
apType 52,apModel AIR-AP3802I-B-K9.

*spamApTask6: Oct 16 08:56:51.953: Fabric is supported for AP f4:db:e6:64:02:a0 (Pod3-AP3800).
apType 52,apModel AIR-AP3802I-B-K9.

*spamApTask6: Oct 16 08:56:51.953: Fabric is supported for AP f4:db:e6:64:02:a0 (Pod3-AP3800).
apType 52,apModel AIR-AP3802I-B-K9.

*spamApTask6: Oct 16 08:56:51.953: spamSendFabricMapServerRequest: MS request from AP Pod3-
AP3800 f4:db:e6:64:02:a0 can not be sent ,AP vnid mapping does not exist
```

패브릭 네트워크에 컨트롤 플레인이 2개 있는 경우 WLC는 항상 등록 또는 쿼리를 위해 양쪽에 연결합니다. 두 컨트롤 플레인 모두 등록에 긍정적인 응답을 줄 것으로 예상되므로 두 컨트롤 플레인 중 하나가 어떤 이유로든 AP를 거부하면 WLC가 패브릭에서 AP를 등록하지 못합니다. 그러나 응답하지 않는 컨트롤 플레인은 허용되며 나머지 컨트롤 플레인이 사용됩니다.

AP가 전역 라우팅 테이블을 통해 WLC에 연결되지만 LISP는 WLC를 확인하는 데 계속 사용됩니다. AP가 WLC로 전송하는 트래픽은 순수한 CAPWAP 제어(vxlan과 관련 없음)이지만, WLC가 AP로 전송하는 반환 트래픽은 오버레이의 Vxlan을 통해 전달됩니다. 에지의 AP 게이트웨이 SVI에서 WLC로의 연결을 테스트할 수 없습니다. Anycast 게이트웨이이기 때문에 같은 IP가 보더 노드에도 있기 때문입니다. 연결을 테스트하려면 AP 자체에서 ping하는 것이 가장 좋습니다.

## 시나리오 2. 액세스 포인트가 IP 주소를 가져오지 않습니다.

액세스 포인트는 DNA Center에 정의된 Infra VNI의 AP Poo에서 ip 주소를 받아야 합니다. 이렇게 되지 않으면 일반적으로 AP가 연결된 스위치 포트가 올바른 vlan으로 이동하지 않은 것입니다. CDP를 통해 연결 중인 액세스 포인트를 탐지하는 경우 스위치는 AP 풀에 대해 DNA-C에 의해 정의된 vlan에 스위치 포트를 설정하는 스위치 포트 매크로를 적용합니다. 문제가 되는 스위치 포트가 실제로 매크로로 구성되지 않은 경우, 구성을 수동으로 설정하거나(AP가 IP를 얻고 WLC에 조인하고 코드를 업그레이드하고 CDP 버그를 해결하도록) CDP 연결 프로세스를 해결할 수 있습니다. 올바른 컨피그레이션으로 프로비저닝되도록 AP를 호스팅할 DNA-Center의 포트를 정적으로 정의하도록 호스트 온보딩을 구성할 수도 있습니다.

Smartport 매크로가 자동으로 시작되지 않습니다. 스위치가 적어도 하나의 AP로 프로비저닝되지 않은 경우 AP 매크로가 기본 VLAN 1이 아닌 올바른 VLAN으로 프로비저닝되었는지 확인할 수 있습니다

```
Pod3-Edge1#show macro auto device
Device:lightweight-ap
Default Macro:CISCO_LWAP_AUTO_SMARTPORT
Current Macro:CISCO_LWAP_AUTO_SMARTPORT
Configurable Parameters:ACCESS_VLAN
Defaults Parameters:ACCESS_VLAN=1
Current Parameters:ACCESS_VLAN=2045
```

Cisco DNA-C에서 이를 설정하기 위해 푸시하는 명령은 다음과 같습니다

```
macro auto execute CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT builtin CISCO_LWAP_AUTO_SMARTPORT
ACCESS_VLAN=2045
macro auto global processing
```

## 시나리오 3. 액세스 포인트에는 패브릭 에지 노드에 구축된 vxlan 터널이 없습니다.

AP가 WLC에 조인하면 WLC(AP가 패브릭을 지원하는 경우)가 제어 평면에 AP를 특수 유형의 클라이언트로 등록합니다. 그런 다음 제어 평면은 AP가 연결된 패브릭 에지 노드에 AP를 향하는 vxlan 터널을 구축하도록 요청합니다.

AP는 vxlan 캡슐화를 사용하여 클라이언트 트래픽을 전송하므로(그리고 RUN 상태의 클라이언트에만 해당), 패브릭 클라이언트가 연결될 때까지 AP에 대한 vxlan 정보를 보지 않는 것이 정상입니다.

AP에서 명령 show **ip tunnel fabric은** 클라이언트가 연결되면 vxlan 터널 정보를 표시합니다.

```
AP4001.7A03.5736#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    172.16.2.253 00:00:0C:9F:F4:5E           Forward      VXLAN     39731  4209554
16345   2087073
AP4001.7A03.5736#
```

Fabric Edge 노드에서 show access-**tunnel summary 명령은** 액세스 포인트를 향해 구축된 vxlan 터널을 표시합니다. AP가 연결되면 컨트롤 플레인의 생성 명령이 실행되자마자 터널이 표시됩니다.

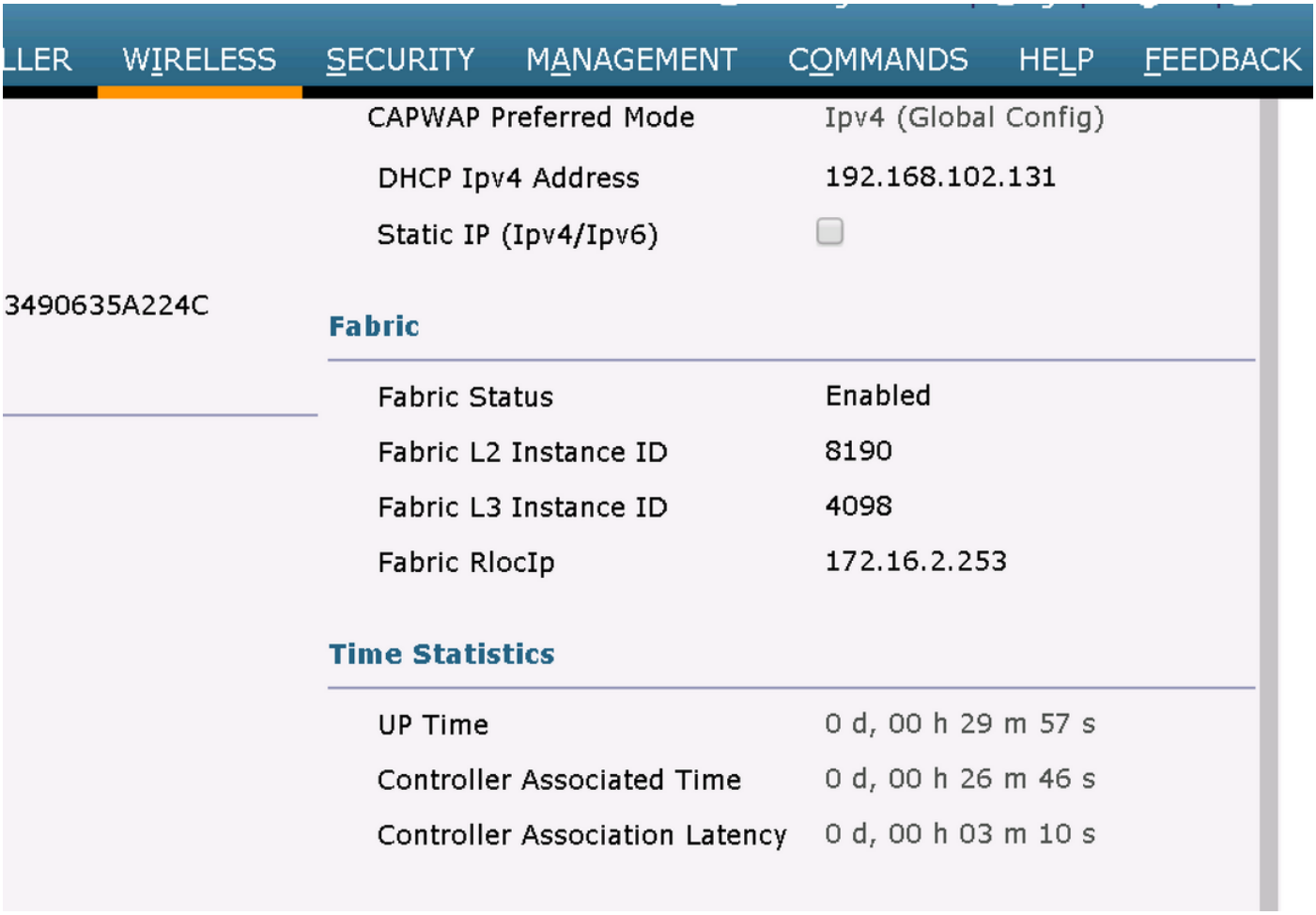
```
edge01#show access-tunnel summ

Access Tunnels General Statistics:
  Number of AccessTunnel Data Tunnels       = 2


Name   SrcIP           SrcPort DestIP          DstPort VrfId
------ --------------- ------- --------------- ------- ----
Ac1    172.16.2.253    N/A     192.168.102.130 4789    2
Ac0    172.16.2.253    N/A     192.168.102.131 4789    2


Name   IfId            Uptime
------ ---------- --------------------
Ac1    0x0000003B 1 days, 22:53:48
Ac0    0x0000003A 0 days, 22:47:06
```

액세스 포인트 페이지의 WLC에서 해당 AP에 해당하는 L2 LISP 인스턴스 ID를 확인한 다음 연결된 패브릭 에지에서 해당 인스턴스의 통계를 확인할 수 있습니다.




```
SDA-D-6880-1#show lisp instance-id 8188 ethernet statistics
LISP EID Statistics for instance ID 8188 - last cleared: never
Control Packets:
  Map-Requests in/out:                      0/0
    Encapsulated Map-Requests in/out:       0/0
    RLOC-probe Map-Requests in/out:         0/0
    SMR-based Map-Requests in/out:          0/0
    Map-Requests expired on-queue/no-reply  0/0
    Map-Resolver Map-Requests forwarded:    0
    Map-Server Map-Requests forwarded:      0
  Map-Reply records in/out:                 0/0
    Authoritative records in/out:           0/0
    Non-authoritative records in/out:       0/0
    Negative records in/out:                0/0
    RLOC-probe records in/out:              0/0
    Map-Server Proxy-Reply records out:     0
  Map-Register records in/out:              24/0
    Map-Server AF disabled:                 0
    Authentication failures:                0
  Map-Notify records in/out:                0/0
    Authentication failures:                0
  Deferred packet transmission:             0/0
    DDT referral deferred/dropped:          0/0
    DDT request deferred/dropped:           0/0
```

## 시나리오 4. 잠시 후 누락된 액세스 터널 항목

WLC가 Cisco DNA-C를 통해 프로비저닝되고 패브릭에 추가될 때 처음으로 액세스 터널이 성공적으로 생성될 수 있지만, 무선 컨피그레이션(예: WLAN 컨피그레이션)을 다시 프로비저닝할 때 AP에 대한 액세스 터널 항목이 누락되어 무선 클라이언트가 IP를 성공적으로 가져올 수 없는 것으로 관찰

됩니다.

토폴로지는 9500(CP) —> 9300(Edge) —> AP —> Wireless Client입니다.

에지 노드의 **show access-tunnel summary**에서 **항목**이 올바르게 관찰됩니다.

```
edge_2#show access-tunnel summary

Access Tunnels General Statistics:
Number of AccessTunnel Data Tunnels = 1


Name SrcIP SrcPort DestIP DstPort VrfId
------ --------------- ------- --------------- ------- ----
Ac0 172.16.3.98 N/A 172.16.3.131 4789 0


Name IfId Uptime
------ ---------- --------------------
Ac0 0x0000003C 5 days, 18:19:37
```

그러나 **show platform software fed switch active ifm interfaces access-tunnel을** 선택하면 이 예에서 AP에 대한 항목이 없거나 하드웨어에서 프로그래밍하지 못했습니다.

```
edge_2#show platform software fed switch active ifm interfaces access-tunnel
Interface IF_ID State
----------------------------------------------------------------
Ac0 0x0000003c FAILED
```

추가 출력:

```
edge_2#sh platform software access-tunnel switch active F0
Name SrcIp DstIp DstPort VrfId Iif_id Obj_id Status
-------------------------------------------------------------------------------------------------
Ac0 98.3.16.172 131.3.16.172 0x12b5 0x000 0x00003c 0x00585f Done


edge_2#sh platform software access-tunnel switch active R0
Name SrcIp DstIp DstPort VrfId Iif_id
-----------------------------------------------------------------------
Ac0 172.16.3.98 172.16.3.131 0x12b5 0x0000 0x00003c
```

서로 다른 출력을 비교해야 하며 **show access-tunnel summary**에 표시된 모든 **터널이** 각 출력에 있어야 합니다.

## 시나리오 5. 무선 클라이언트가 IP 주소를 가져올 수 없음

vxlan 터널이 있고 모든 터널이 정상으로 보이지만 무선 클라이언트가 체계적으로 IP 주소를 가져올 수 없는 경우 옵션 82 문제가 발생할 수 있습니다. 클라이언트의 DHCP DISCOVER는 에지 노드의 Anycast 게이트웨이에 의해 전달되므로, DHCP 서버 OFFER가 돌아오는 길에 테두리를 통해 오른쪽 에지 노드로 전송되는 데 문제가 있습니다. DHCP DISCOVER를 전달하는 패브릭 에지가 다른 정보와 함께 인코딩된 에지 노드의 실제 패브릭 RLOC(루프백 IP)를 포함하는 옵션 82 필드를

DHCP DISCOVER에 추가하는 이유입니다. 따라서 DHCP 서버가 옵션 82를 지원해야 합니다.

DHCP 프로세스의 문제를 해결하려면 패브릭 노드(특히 클라이언트 에지 노드)에서 캡처를 수행하여 패브릭 에지가 옵션 82 필드를 추가하는지 확인합니다.

### 시나리오 6. 게스트 패브릭/웹 인증이 작동하지 않음/클라이언트 리디렉션 안 함

게스트 패브릭 시나리오는 Flexconnect 액세스 포인트의 CWA(Central Web Authentication)와 매우 유사하며 패브릭 AP가 flexconnect 모드가 아닌 경우에도 동일한 방식으로 작동합니다.

리디렉션 ACL 및 URL은 첫 번째 mac 인증 결과에서 ISE에 의해 반환되어야 합니다. ISE 로그와 WLC의 클라이언트 세부사항 페이지에서 이를 확인합니다.

리디렉션 ACL은 WLC의 Flex ACL로 존재해야 하며, 포트 8443(최소)의 ISE IP 주소에 대한 "permit" 문을 포함해야 합니다.

클라이언트는 WLC의 클라이언트 세부사항 페이지에서 "CENTRAL_WEBAUTH_REQ" 상태여야 합니다. 클라이언트는 기본 게이트웨이를 ping할 수 없으며 이는 예상된 결과입니다. 리디렉션되지 않은 경우 클라이언트 웹 브라우저에서 IP 주소를 수동으로 입력할 수 있습니다(DNS를 배제하려면 ISE 호스트 이름을 확인해야 함). 클라이언트 브라우저의 포트 8443에서 ISE IP를 입력하고 포털 페이지를 볼 수 있어야 합니다. 이 흐름은 리디렉션되지 않습니다. 이러한 상황이 발생하지 않으면 ACL 문제 또는 라우팅 문제가 발생할 수 있습니다. HTTP 패킷이 중지된 위치를 확인하기 위해 패킷 캡처를 수집합니다.

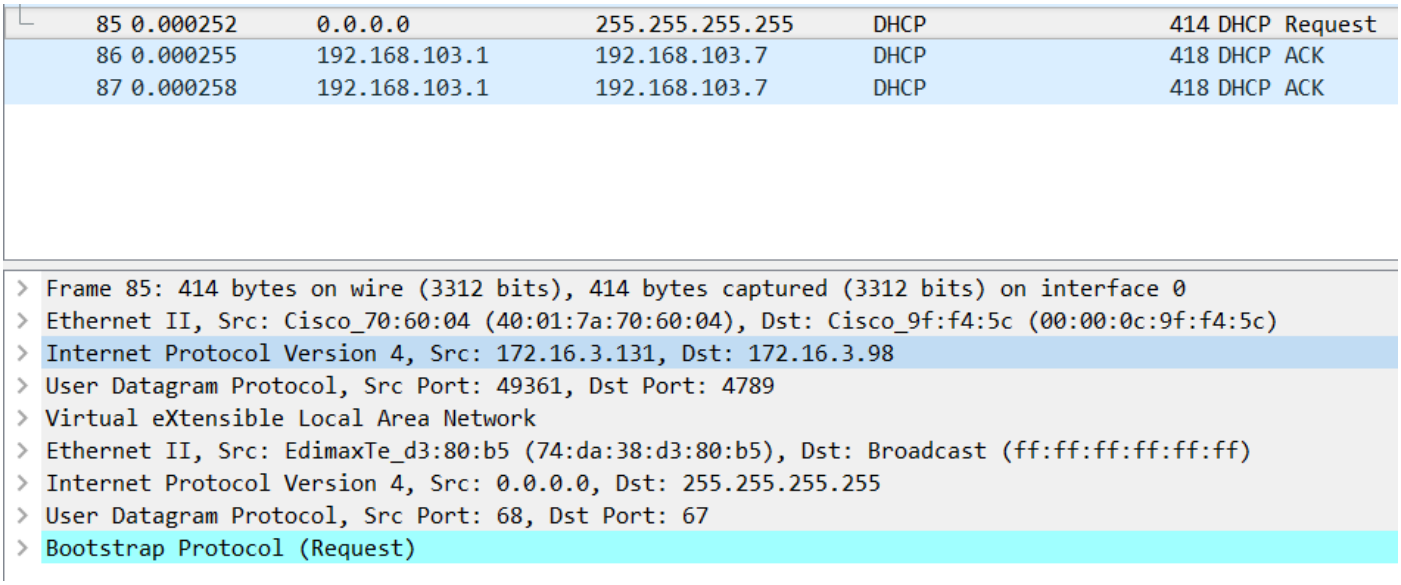
## 이해

### 패브릭 아키텍처에서 무선 클라이언트가 IP 주소를 얻는 방법

| | | | | | | |
|---|---|---|---|---|---|---|
| 65 | 0.000191 | 0.0.0.0 | 255.255.255.255 | DHCP | 392 | DHCP Discover - Transaction ID 0x5fd8da22 |
| 66 | 0.000194 | 0.0.0.0 | 255.255.255.255 | DHCP | 418 | DHCP Discover - Transaction ID 0x5fd8da22 |
| 80 | 0.000234 | 0.0.0.0 | 255.255.255.255 | DHCP | 392 | DHCP Discover - Transaction ID 0x5fd8da22 |
| 81 | 0.000238 | 0.0.0.0 | 255.255.255.255 | DHCP | 418 | DHCP Discover - Transaction ID 0x5fd8da22 |
| 82 | 0.000241 | 192.168.103.1 | 192.168.103.7 | DHCP | 418 | DHCP Offer - Transaction ID 0x5fd8da22 |
| 83 | 0.000245 | 192.168.103.1 | 192.168.103.7 | DHCP | 418 | DHCP Offer - Transaction ID 0x5fd8da22 |
| 84 | 0.000248 | 0.0.0.0 | 255.255.255.255 | DHCP | 440 | DHCP Request - Transaction ID 0x5fd8da22 |
| 85 | 0.000252 | 0.0.0.0 | 255.255.255.255 | DHCP | 414 | DHCP Request - Transaction ID 0x5fd8da22 |
| 86 | 0.000255 | 192.168.103.1 | 192.168.103.7 | DHCP | 418 | DHCP ACK - Transaction ID 0x5fd8da22 |
| 87 | 0.000258 | 192.168.103.1 | 192.168.103.7 | DHCP | 418 | DHCP ACK - Transaction ID 0x5fd8da22 |

패킷 캡처는 패브릭 AP와 패브릭 에지 사이에서 이루어집니다. 두 개의 DHCP Discover 패킷이 전송되었기 때문에 패킷이 중복됩니다. 트래픽은 패브릭 에지에서만 인그레스(ingress)였으며 캡처되었습니다.

DHCP 패킷은 항상 2개입니다. CAPWAP에서 컨트롤러에 직접 전송하여 업데이트를 유지합니다. VXLAN에서 제어 노드로 보낸 다른 노드. AP가 예를 들어 DHCP 서버에서 VXLAN을 통한 DHCP 제공을 받으면 CAPWAP를 사용하여 컨트롤러에 복사본을 보냅니다.




패킷이 전송된 위치를 확인하려면 Wireshark에서 클릭해야 합니다. 여기서 소스가 AP 172.16.3.131이고 패킷이 패브릭 에지 172.16.3.98로 전송되었음을 알 수 있습니다. 패브릭 엣지가 이를 제어 노드에 전달했습니다.

## 패브릭 시나리오의 웹 리디렉션 흐름 이해

WLC의 리디렉션 ACL은 일치하는 거부 명령문에서 리디렉션/가로채기되는 트래픽을 정의합니다(끝에 암시적 거부가 있음). 리디렉션할 트래픽은 WLC가 리디렉션하도록 CAPWAP 캡슐화 내에서 WLC로 전송됩니다. permit 문을 매칭할 때, 트래픽은 리디렉션되지 않고 패브릭에서 통과되어 전달됩니다(ISE로 향하는 트래픽은 이 카테고리로 진입).

## 패브릭 활성화 상태에서 WLC에 조인하는 AP의 로그

액세스 포인트가 WLC에 등록되는 즉시 컨트롤러는 SDA 제어 노드(LISP 맵 서버)에 IP 및 MAC 주소를 등록합니다.

AP는 WLC가 LISP RLOC 패킷을 수신하는 경우에만 패브릭 활성화 모드에서 WLC에 조인합니다. 이 패킷은 AP가 패브릭 에지에 연결되어 있는지 확인하기 위해 전송됩니다.

이 예에서 WLC에 사용되는 디버그는 다음과 같습니다.

- **'debug capwap events enable'**
- **'debug capwap errors enable'**
- **'debug fabric ap-join events enable( ap-join )'**
- **'debug fabric ap-join detail enable'**
- **'debug fabric lisp map-server all enable'**

테스트의 경우 AP가 재부팅됩니다.

```
*spamApTask0: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for Aggregated
Payload 3 sent to 172.16.3.131:5256
*msfMsgQueueTask: May 07 13:00:18.804: NAK list count becoming 0
*msfMsgQueueTask: May 07 13:00:18.804: NAK list count becoming 0
*msfMsgQueueTask: May 07 13:00:18.804: Cleaned up AP RLOC NAK entry for AP 172.16.3.131 vnid
4097 for BOTH MS
*msfMsgQueueTask: May 07 13:00:18.804: Inserted entry for AP IP 172.16.3.131 and VNID 4097, db
idx 12
*msfMsgQueueTask: May 07 13:00:18.804: Map-reply timer started for AP IP 172.16.3.131 and VNiD
```

4097
*msfMsgQueueTask: May 07 13:00:18.804: Creating new timer for AP IP 172.16.3.131 and VNID 4097
*msfMsgQueueTask: May 07 13:00:18.804: Map-reply Timer Started Successfully for AP IP 172.16.3.131 and VNID 4097
*msfMsgQueueTask: May 07 13:00:18.804: Not able to find nonce 0x3cd13556-0x81864b7b avl entry
*msfMsgQueueTask: May 07 13:00:18.804: FAIL: not able to find avl entry
*msfMsgQueueTask: May 07 13:00:18.804: Nonce 0x3cd13556-0x81864b7b inserted into nonce aVL tree for AP IP 172.16.3.131 VNID 4097 for MS 172.16.3.254
*msfMsgQueueTask: May 07 13:00:18.804: Set nonce 0x3cd13556-0x81864b7b for AP 172.16.3.131 and VNID 4097
*msfMsgQueueTask: May 07 13:00:18.804: Nonce 0x3cd13556-0x81864b7b is updated for AP IP 172.16.3.131, VNID 4097 and MS IP 172.16.3.254, db idx 12
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for PHY payload sent to 172:16:3:131
*msfMsgQueueTask: May 07 13:00:18.804: Build and send map-request for AP IP 172.16.3.131 and VNID 4097 to MS IP 172.16.3.254
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for RrmInterferenceCtrl payload sent to 172:16:3:131
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for RrmInterferenceCtrl payload sent to 172:16:3:131
*msfMsgQueueTask: May 07 13:00:18.804: nonce = 3cd13556-81864b7b lisp_map_request_build allocating nonce
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for RrmNeighbourCtrl payload sent to 172.16.3.131
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for CcxRmMeas payload sent to 172.16.3.131
***msfMsgQueueTask: May 07 13:00:18.804: Sending map-request for AP 172.16.3.131 VNID 4097 to MS 172.16.3.254**
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update request for AP ext-logging AP ext-logging message sent to 172.16.3.131:5256
*spamReceiveTask: May 07 13:00:18.804: 70:70:8b:20:29:00 Configuration update for Delba sent to 172.16.3.131:5256
***msfMsgQueueTask: May 07 13:00:18.804: Map-request for AP IP 172.16.3.131 VNID 4097 to MS 172.16.3.254 is sent**
***msfMsgQueueTask: May 07 13:00:18.804: Sent map-request to MS 172.16.3.254 for AP 172.16.3.131 VNID 4097**
*msfMsgQueueTask: May 07 13:00:18.804: Invalid secondary MS IP 0.0.0.0 for map-request for AP IP 172.16.3.131
*msfMsgQueueTask: May 07 13:00:18.804: No messages are present in the Client list for Local UDP socket
*msfTcpTask: May 07 13:00:18.807: Sending the UDP control packet to queue task
*msfMsgQueueTask: May 07 13:00:18.807: msfQueue: recieved LISP_MAP_SERVER_UDP_PACKET_QUEUE_MSG
*msfMsgQueueTask: May 07 13:00:18.807: Mapping Record has locators and actions
*msfMsgQueueTask: May 07 13:00:18.807: Mapping record address 172.16.3.98 EID address 172.16.3.98
*msfMsgQueueTask: May 07 13:00:18.807: Got AVL entry for nonce 0x3cd13556-0x81864b7b in map-reply for AP IP 172.16.3.131
***msfMsgQueueTask: May 07 13:00:18.807: Sent received RLOC IP 172.16.3.98 for AP 172.16.3.131 and VNID 4097 in map-reply to spam task**
***msfMsgQueueTask: May 07 13:00:18.807: Added RLOC 172.16.3.98 for AP IP 172.16.3.131**
***spamReceiveTask: May 07 13:00:18.807: Recieved Fabric rloc response from msip 172.16.3.254 with apvnid 4097,fabricRLoc 172.16.3.98 apip 172.16.3.131 apRadMac 70:70:8b:20:29:00**

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.