

# Cisco DNA Center 릴리스 1.1 및 1.2의 무선 FAQ 및 문제 해결 소프트웨어 정의 액세스

## 목차

[Cisco.com에 게시된 참조 문서](#)

[제어 노드, 에지 노드, WLC\(무선 LAN 컨트롤러\) 및 액세스 포인트\(AP\)의 패브릭에 대한 커트 시트 프로비저닝 후 Cisco DNA Center에서 AireOS WLC Config 푸시\(참고:3504 WLC로 참조 사용\)](#)

[WLC 프로비저닝 후 radius 요약 표시](#)

[WLAN Config Push from\(WLAN 컨피그레이션 푸시\)는 "show wlan summary\(WLAN 요약 표시\)" 아래에 표시됩니다.](#)

[WLC를 패브릭에 추가한 후 Cisco DNA Center에서 WLC Config 푸시](#)

[맵 서버에 연결할 수 있는지 확인하는 방법](#)

[패브릭 맵-서버 연결 디버깅](#)

[패브릭이 활성화되었는지 여부를 확인하는 방법 및 예상되는 결과는 무엇입니까?](#)

[Cisco DNA Center의 WLAN Config Push는 Provision\(프로비저닝\) > Fabric\(패브릭\) > Host Onboarding\(호스트 온보딩\)에서 WLC를 패브릭에 추가하고 WLAN\(Fabric Wireless LAN\)에 클라이언트 IP 풀을 할당한 후 "show fabric wlan summary\(패브릭 wlan 요약 표시\)"에서 확인할 수 있습니다.](#)

[Cisco DNA Center를 통해 고가용성\(HA\)을 구성하는 동안 WLC 교체 프로세스](#)

[무선 문제 디버깅](#)

[AP Join 디버깅/액세스 터널 형성 디버깅](#)

[클라이언트 디버깅](#)

[AP 온보딩](#)

[기존 방법/단계:\(AP Vlan Scope에는 WLC를 가리키는 옵션 43 또는 옵션 60이 있음\)](#)

[플러그 앤 플레이/제로 터치 AP 프로비저닝\(AP VLAN 범위 고려 시 Cisco DNA 센터를 가리키는 옵션 43이 있음\)](#)

**Cisco.com**

- [각 릴리스의 무선 구성 설명서](#)

- [SD 무선 구축 설명서](#)

- [무선 모범 사례 가이드](#)

- [무선용 기술 참조 문서](#)

- [SDA 호환성 매트릭스](#)

- [릴리스별 Cisco DNA Center 사용 설명서](#)

, , WLC( LAN ) (AP)

- `show lisp instance-id <L2 ap instance id> ethernet server MAC to Endpoint Identification (EID) Mapping`

- `show lisp instance-id <L3 ap instance id> ipv4 IP EID`

- `show lisp instance-id 8188 ethernet server address-resolution MAC to IP Mapping for a specific instance ID`

-

- show lisp instance-id <L2 ap instance id> ethernet database wlc
  - show lisp instance-id <L2 client instance id> ethernet database wlc
  - show access-tunnel summary
- WLC
- ap
  - 
  - show fabric map-server summary
- show ip tunnel fabric

## 프로비저닝 후 Cisco DNA Center에서 AireOS WLC Config 푸시(참고:3504 WLC로 참조 사용)

### WLC 프로비저닝 후 radius 요약 표시

(sdawlc3504) >show radius summary

```
Vendor Id Backward Compatibility..... Disabled
Call Station Id Case..... lower
Accounting Call Station Id Type..... Mac Address
Auth Call Station Id Type..... AP's Radio MAC Address:SSID
Extended Source Ports Support..... Enabled
Aggressive Failover..... Disabled
Keywrap..... Disabled
Fallback Test:
  Test Mode..... Passive
  Probe User Name..... cisco-probe
  Interval (in seconds)..... 300
MAC Delimiter for Authentication Messages..... hyphen
MAC Delimiter for Accounting Messages..... hyphen
RADIUS Authentication Framed-MTU..... 1300 Bytes
```

#### Authentication Servers

Idx	Type	Server Address	Port	State	Tout	MgmtTout	RFC3576	IPSec - state/Profile
1	* NM	192.168.2.193	1812	Enabled	2	5	Enabled	Disabled - /none
2	M	172.27.121.193	1812	Enabled	2	5	Enabled	Disabled - /none

**WLAN Config Push from(WLAN 컨피그레이션 푸시)는 "show wlan summary(WLAN 요약 표시)" 아래에 표시됩니다.**

(sdawlc3504) >show wlan summary

Number of WLANs..... 7

WLAN ID	WLAN Profile Name / SSID	Status
1	Test / Test	Enabled
17	dnac_guest_F_global_5dfbd_17 / dnac_guest_206	Disabled
18	dnac_psk_2_F_global_5dfbd_18 / dnac_psk_206	Disabled

```

19      dnac_wpa2__F_global_5dfbd_19 / dnac_wpa2_206      Enabled
management      none
20      dnac_open__F_global_5dfbd_20 / dnac_open_206      Enabled
management      none
21      Test!23_F_global_5dfbd_21 / Test!23      Disabled
management      none

```

## WLC를 패브릭에 추가한 후 Cisco DNA Center에서 WLC Config 푸시

### 맵 서버에 연결할 수 있는지 확인하는 방법

### 패브릭에 WLC를 추가한 후 패브릭 맵 서버 요약 표시

```
(sdawlc3504) >show fabric map-server summary
```

```
MS-IP      Connection status
```

```
-----
```

```
192.168.4.45      UP
```

```
192.168.4.66      UP
```

### 패브릭 맵-서버 연결 디버깅

다양한 이유로 인해 컨트롤 플레인(CP) 연결이 중단되거나 다운될 수 있습니다.

1. CP가 중단된 경우(이 경우에는 아님)
2. WLC를 CP에 연결하는 중간 노드(예: fusion router)
3. 링크 다운으로 WLC에 대한 CP 연결이 중단된 경우 이는 WLC를 통해 즉시 네이버에 연결하거나 CP를 WLC로 바로 연결할 수 있습니다.

패브릭 맵 서버 세부 정보 표시

```
show fabric TCP creation-history <Map-Server IP>
```

추가 정보를 제공할 수 있는 디버깅

```
debug fabric lisp map-server tcp enable
```

패브릭이 활성화되었는지 여부를 확인하는 방법 및 예상되는 결과는 무엇입니까?

### 패브릭에 WLC를 추가한 후 패브릭 요약 표시

```
(sdawlc3504) >show fabric summary
```

```
Fabric Support..... enabled
```

```
Enterprise Control Plane MS config
```

```
-----
```

```
Primary Active MAP Server
```

```
IP Address..... 192.168.4.45
```

Secondary Active MAP Server  
IP Address..... 192.168.4.66

Guest Control Plane MS config  
-----

Fabric TCP keep alive config  
-----

Fabric MS TCP retry count configured ..... 3  
Fabric MS TCP timeout configured ..... 10  
Fabric MS TCP keep alive interval configured .... 10  
Fabric Interface name configured ..... management

Fabric Clients registered ..... 0

Fabric wlans enabled ..... 3

Fabric APs total Registration sent ..... 30

Fabric APs total DeRegistration sent ..... 9

Fabric AP RLOC requested ..... 15

Fabric AP RLOC response received ..... 30

Fabric AP RLOC send to standby ..... 0

Fabric APs registered by WLC ..... 6

VNID Mappings configured: 4

Name	L2-Vnid	L3-Vnid	IP Address/Subnet
182_10_50_0-INFRA_VN	8188	4097	182.10.50.0 / 255.255.255.128
10_10_10_0-Guest_Area	8190	0	0.0.0.0 / 0.0.0.0
182_10_100_0-DEFAULT_VN	8191	0	0.0.0.0 / 0.0.0.0
182_11_0_0-DEFAULT_VN	8189	0	0.0.0.0 / 0.0.0.0

Fabric Flex-Acl-tables	Status
DNAC_FABRIC_FLEX_ACL_TEMPLATE	Applied

Fabric Enabled Wlan summary

WLAN ID	SSID	Type	L2 Vnid	SGT	RLOC IP	Clients
19	dnac_wpa2_206	WLAN	8189	0	0.0.0.0	0
20	dnac_open_206	WLAN	8189	0	0.0.0.0	0

Cisco DNA Center의 WLAN Config Push는 Provision(프로비저닝) > Fabric(패브릭) > Host Onboarding(호스트 온보딩)에서 WLC를 패브릭에 추가하고 WLAN(Fabric Wireless LAN)에 클라이언트 IP 풀을 할당한 후 "show fabric wlan summary(패브릭 wlan 요약 표시)"에서 확인할 수 있습니다.

패브릭 프로비저닝 후 패브릭 wlan 요약 표시

```
(sdawlc3504) >show fabric wlan summary
```

WLAN ID VNID Name	SSID	Type	L2 Vnid	SGT	RLOC IP	Clients
19 182_11_0_0-DEFAULT_VN	dnac_wpa2_206	WLAN	8189	0	0.0.0.0	0
20 182_11_0_0-DEFAULT_VN	dnac_open_206	WLAN	8189	0	0.0.0.0	0

## Cisco DNA Center를 통해 고가용성(HA)을 구성하는 동안 WLC 교체 프로세스

유지 관리 창에서 작업을 수행하십시오. Cisco DNA Center를 통해 HA 쌍에서 새 WLC를 다시 구성하는 작업은 패브릭에서 기본 WLC를 제거하지 않으면 오늘 불가능합니다.

1. 교체해야 하는 WLC가 대기 모드인지 확인합니다. 그렇지 않은 경우 수동 전환을 수행하고 대기 상태로 만드십시오.
2. 프로비저닝 페이지에서 Cisco DNA Center에서 HA 비활성화
3. HA가 비활성화되면 WLC가 인벤토리에서 자동으로 제거됩니다.
4. WLC를 물리적으로 교체하고 새 WLC에 기본 전제 조건을 수동으로 구성
5. Cisco DNA Center에서 새로운 WLC 발견
6. 이미 Cisco DNA Center에 있던 패브릭에서 기본 WLC를 제거합니다. (이 단계를 수행하지 않으면 새 WLC로 HA를 구성하면 오류가 발생하고 Cisco DNA Center를 통해 실패합니다.)
7. 새로운 WLC 및 이중화 관리 IP를 사용하여 HA를 다시 구성합니다. [두 WLC가 다시 로드됩니다.]
8. Primary WLC의 Inventory(인벤토리)에서 수동 재동기화를 수행하거나 다음 재동기화 주기가 Cisco DNA Center에서 정보를 업데이트할 때까지 기다립니다. 완료되면 새로 추가된 WLC가 인벤토리에서 사라지고 고가용성 아래에 대기 상태로 표시됩니다.
9. 패브릭에 WLC 다시 추가

### 주의 사항

**CSCvn24661** Cisco DNA 센터: WLC 중 하나가 이미 패브릭에 포함되어 있으면 WLC HA를 페어링할 수 없습니다.

### 해결 방법:

1. CLI를 통해 WLC HA를 수동으로 구성합니다. 성능에 영향을 미치지 않습니다. [참고: 더 이상 Cisco DNA Center를 통해 HA를 구성하거나 비활성화할 수 없습니다.]
2. 위의 절차 단계에서 설명한 대로 Cisco DNA Center를 통해 패브릭을 비활성화합니다. [참고: 이렇게 하면 다운타임이 두 배 증가하게 됩니다. 패브릭을 비활성화하는 동안 한 번, HA를 생성하는 동안 두 번째로 발생합니다.]

## AP Join 디버깅/액세스 터널 형성 디버깅

1. AP에 IP 주소가 있는지 확인

패브릭 에지에서 ip dhcp snooping 바인딩 → 표시

연결된 AP 인터페이스에 대한 IP가 표시되지 않으면 스위치에서 아래 디버깅을 활성화하

고 AP가 IP를 수신하는지 확인하십시오.

디버그 ip dhcp snooping 패킷

디버그 ip dhcp snooping 이벤트

아래에 첨부된 샘플 로그 파일 →

예:

*Floor\_Edge-6#sh ip dhcp snooping 바인딩*

*MacAddress IpAddress Lease(sec) Type VLAN Interface*

—————

*0C:75:BD:0D:46:60 182.10.50.7 670544 dhcp-snooping 1021 기가비트 이더넷1/0/7 AP 인  
터페이스에 IP가 있어야 합니다.*

2. AP가 WLC에 가입하는지 확인합니다.

WLC에 ap 요약 → 표시

WLC에서 ap join stat 요약 → 표시

AP가 WLC에 가입하지 않은 경우 WLC에서 아래 디버그를 활성화합니다.

디버그 capwap 이벤트 활성화

디버그 capwap 오류 사용

3. AP가 CAPWAP를 형성하지만 AP와 스위치 간에 액세스 터널이 형성되지 않은 경우 아래 검사를 수행하십시오.

1단계:WLC의 AP에 RLOC IP가 있습니까? 그렇지 않은 경우 a점을 선택하십시오.)

a) 패브릭 컨트롤 플레인 프로토콜의 복원력을 높이려면 각 패브릭 노드의 전역 라우팅 테이블에 WLC에 대한 특정 경로가 있어야 합니다.WLC의 IP 주소에 대한 경로는 Border의 언더레이 IGP 프로토콜로 재배포하거나 각 노드에서 정적으로 구성해야 합니다.즉, 기본 경로를 통해 WLC에 연결할 수 없습니다.

2단계:WLC의 AP에 올바른 RLOC가 표시되고 "show fabric summary" 아래에 RLOC가 정상적으로 수신되고 요청된 RLOC가 표시되는 경우 아래 단계를 확인하십시오.

b) 컨트롤 플레인 노드, "show lisp instance-id <L2 ap instance id> ethernet server" → AP용 기본 라디오 MAC를 포함해야 합니다.

패브릭 에지 노드, "show lisp instance-id <L2 ap instance id> ethernet database wlc" → AP의 이더넷 MAC이 아니라 AP용 기본 라디오 MAC을 포함해야 합니다.

위의 2개 명령이 AP의 Base Radio MAC를 표시하지 않고 액세스 터널이 형성되지 않는 경우.컨트롤 플레인에서 "debug lisp control-plane all"을 활성화하고 로깅에서 기본 라디오 MAC을 검색합니다.[참고:컨트롤 플레인의 "debug lisp control-plane all"은 매우 채팅 상태가 됩니다. 디버그를 켜기 전에 콘솔 로깅을 비활성화하십시오.]

아래와 같은 인증 실패가 표시되면 WLC와 CP 노드 간의 인증 키를 확인하십시오.

12월 7일 17:42:01.655:LISP-0:MS Site EID IID 8188 prefix any-mac  
SVC\_VLAN\_IAF\_MAC site\_uci, Registration 실패, 더 구체적인 2c0b.e9c6.ec80/48 인증

12월 7일 17:42:01.659:LISP-0:IID 8188 EID 2c0b.e9c6.ec80/48에 대해 신뢰할 수 있는 등  
록 메시지 등록 거부 빌드, 거부 코드:인증 실패/2.

WLC와 CP 간의 패브릭 컨피그레이션에서 인증 키를 확인하는 방법

WLC에서 컨트롤러 → 패브릭 구성 → 컨트롤 플레인 →(사전 공유 키) 아래의 GUI를 확인하  
십시오.

CP에서 sh running-config를 사용하여 스위치를 확인하십시오. | b map-server 세션

CP#sh running-config | b map-server 세션

map-server session passive-open WLC

사이트 사이트\_uci

apic-em에서 구성된 설명 맵 서버

**authentication-key uci(WLC의 사전 공유 키가 CP의 이 인증 키와 일치해야 함) [참고:일반  
적으로 Cisco DNA Center는 이 키를 푸시하므로, 필요한 경우 변경하지 말고 CP/WLC에  
구성된 내용을 알아야 합니다.]**

#### 4. 액세스 터널에 대한 일반 검사 및 표시 명령

##### a) show access-tunnel summary

```
Floor_Edge-6#sh access-tunnel summary
```

```
Access Tunnels General Statistics:
```

```
Number of AccessTunnel Data Tunnels = 5
```

```
Name SrcIP SrcPort DestIP DstPort VrfId
```

```
-----  
Ac4 192.168.4.68 N/A 182.10.50.6 4789 0  
Ac24 192.168.4.68 N/A 182.10.50.5 4789 0  
Ac19 192.168.4.68 N/A 182.10.50.8 4789 0  
Ac15 192.168.4.68 N/A 182.10.50.7 4789 0  
Ac14 192.168.4.68 N/A 182.10.50.2 4789 0
```

```
Name IfId Uptime
```

```
-----  
Ac4 0x00000037 2 days, 20:35:29  
Ac24 0x0000004C 1 days, 21:23:16  
Ac19 0x00000047 1 days, 21:20:08  
Ac15 0x00000043 1 days, 21:09:53  
Ac14 0x00000042 1 days, 21:03:20
```

##### b) show platform software fed switch active ifm interfaces access tunnel

```
Floor_Edge-6#show platform software fed switch active ifm interfaces access-tunnel
```

```
Interface IF_ID State  
-----  
Ac4 0x00000037 READY  
Ac14 0x00000042 READY
```

Ac15	0x00000043	READY
Ac19	0x00000047	READY
Ac24	0x0000004c	READY

Floor\_Edge-6#

b 명령 아래의 액세스 터널이 a)보다 높으면 문제가 됩니다.여기서 Fed 엔트리는 Fabric Edge에서 올바르게 지워지지 않았으므로 IOS에 비해 Fed에 여러 액세스 터널 엔트리가 있습니다.c 명령을 실행한 후 대상 IP 비교. 여러 액세스 터널이 동일한 대상 IP를 공유하는 경우 프로그래밍 문제가 발생합니다.

c) show platform software fed switch active ifm if-id <각 AP IF-ID> [참고:이전 명령에서 각 IF-ID를 가져올 수 있습니다.]

Floor\_Edge-6#show platform software fed switch active ifm if-id 0x00000037

```
Interface IF_ID      : 0x00000000000000037
Interface Name      : Ac4
Interface Block Pointer : 0xffc0b04c58
Interface State     : READY
Interface Status    : ADD
Interface Ref-Cnt   : 2
Interface Type      : ACCESS_TUNNEL
  Tunnel Type      : L2Lisp
  Encap Type       : VxLan
  IF_ID            : 0x37
```

Port Information

```
Handle ..... [0x2e000094]
Type ..... [Access-tunnel]
Identifier ..... [0x37]
Unit ..... [55]
```

Access tunnel Port Logical Subblock

```
Access Tunnel id   : 0x37
Switch Num        : 1
Asic Num          : 0
PORT LE handle    : 0xffc0b03c58
L3IF LE handle    : 0xffc0e24608
DI handle         : 0xffc02cdf48
RCP service id    : 0x0
HTM handle decap  : 0xffc0e26428
RI handle decap   : 0xffc0afb1f8
SI handle decap   : 0xffc0e26aa8
RCP opq info      : 0x1
L2 Brdcast RI handle : 0xffc0e26808
GPN               : 3201
Encap type        : VXLAN
L3 protocol       : 17
Src IP            : 192.168.4.68
Dest IP           : 182.10.50.6
Dest Port         : 4789
Underlay VRF      : 0
XID cpp handle    : 0xffc03038f8
```

Port L2 Subblock

```
Enabled ..... [No]
Allow dot1q ..... [No]
Allow native ..... [No]
Default VLAN ..... [0]
Allow priority tag ... [No]
Allow unknown unicast [No]
Allow unknown multicast[No]
Allow unknown broadcast[No]
Allow unknown multicast[Enabled]
```



```

Allow unknown unicast [Enabled]
IPv4 ARP snoop ..... [No]
IPv6 ARP snoop ..... [No]
Jumbo MTU ..... [0]
Learning Mode ..... [0]
Port QoS Subblock
Trust Type ..... [0x7]
Default Value ..... [0]
Ingress Table Map ..... [0x0]
Egress Table Map ..... [0x0]
Queue Map ..... [0x0]
Port Netflow Subblock
Port CTS Subblock
Disable SGACL ..... [0x0]
Trust ..... [0x0]
Propagate ..... [0x1]
%Port SGT ..... [-180754391]
Ref Count : 2 (feature Ref Counts + 1)
IFM Feature Ref Counts
FID : 91, Ref Count : 1
No Sub Blocks Present

```

**d) show platform software access-tunnel switch active R0**

```

Floor_Edge-6#show platform software access-tunnel switch active R0
Name      SrcIp          DstIp          DstPort  VrfId  Iif_id
-----
Ac4       192.168.4.68   182.10.50.6    0x12b5   0x0000 0x000037
Ac14      192.168.4.68   182.10.50.2    0x12b5   0x0000 0x000042
Ac15      192.168.4.68   182.10.50.7    0x12b5   0x0000 0x000043
Ac19      192.168.4.68   182.10.50.8    0x12b5   0x0000 0x000047
Ac24      192.168.4.68   182.10.50.5    0x12b5   0x0000 0x00004c

```

**show platform software access-tunnel switch active R0 statistics**

```

Floor_Edge-6#show platform software access-tunnel switch active R0 statistics
Access Tunnel Counters (Success/Failure)
-----
Create                6/0
Create Obj Download   6/0
Delete                3/0
Delete Obj Download   3/0
NACK                  0/0

```

**e) show platform software access-tunnel switch active F0**

```

Floor_Edge-6#show platform software access-tunnel switch active F0
Name      SrcIp          DstIp          DstPort  VrfId  Iif_id  Obj_id  Status
-----
Ac4       192.168.4.68   182.10.50.6    0x12b5   0x0000 0x000037 0x00d270 Done
Ac14      192.168.4.68   182.10.50.2    0x12b5   0x0000 0x000042 0x03cbca Done
Ac15      192.168.4.68   182.10.50.7    0x12b5   0x0000 0x000043 0x03cb9b Done
Ac19      192.168.4.68   182.10.50.8    0x12b5   0x0000 0x000047 0x03cb6b Done
Ac24      192.168.4.68   182.10.50.5    0x12b5   0x0000 0x00004c 0x03caf4 Done

```

**show platform software access-tunnel switch active F0 statistics**

```

Floor_Edge-6#show platform software access-tunnel switch active F0 statistics

```

```

Access Tunnel Counters      (Success/Failure)
-----
Create                      0/0
Delete                      3/0
HW Create                   6/0
HW Delete                   3/0
Create Ack                  6/0
Delete Ack                  3/0
NACK Notify                 0/0

```

**f) show platform software object-manager switch active f0 statistics**

```

Floor_Edge-6#show platform software object-manager switch active f0 statistics
Forwarding Manager Asynchronous Object Manager Statistics

```

```

Object update: Pending-issue: 0, Pending-acknowledgement: 0
Batch begin:   Pending-issue: 0, Pending-acknowledgement: 0
Batch end:    Pending-issue: 0, Pending-acknowledgement: 0
Command:      Pending-acknowledgement: 0
Total-objects: 987
Stale-objects: 0
Resolve-objects: 3
Error-objects: 1
Paused-types: 0

```

**g) show platform software object-manager switch active f0 pending-issue-update**

**show platform software object-manager switch active f0 pending-ack-update**

**show platform software object-manager switch active f0 error object**

**5. 수집이 필요한 추적 및 디버깅**

**a) 추적/디버깅을 활성화하기 전에 아카이브 로그 수집**

**요청 플랫폼 소프트웨어 추적 아카이브 대상 플래시:<파일 이름>**

```

Floor_Edge-6#request platform software trace archive target flash:Floor_Edge-6_12_14_18
Waiting for trace files to get rotated.
Creating archive file [flash:Floor_Edge-6_12_14_18.tar.gz]
Done with creation of the archive file: [flash:Floor_Edge-6_12_14_18.tar.gz]

```

**b) 로깅 버퍼 증가 및 콘솔 비활성화**

```

Floor_Edge-6(config)#logging buffered 214748364
Floor_Edge-6(config)#no logging console

```

**c) 추적 설정**

**set platform software trace forwarding switch active R0 access-tunnel verbose**  
**set platform software trace forwarding switch active F0 access-tunnel verbose**  
**플랫폼 소프트웨어 추적 fed 스위치 활성화 ifm\_main 디버그**  
**set platform software trace fed switch active access\_tunnel verbose**

**set platform software trace forwarding-manager switch active F0 aom verbose**

**d) 디버깅 사용**

디버그 l2lisp 모두  
디버그 lisp 컨트롤 플레인 모두

e) AP가 연결된 종료 인터페이스 포트 없음

f) 아카이브 로그를 1단계와 동일) 다른 파일 이름으로 수집

g) 로깅 파일을 플래시에 리디렉션

Floor\_Edge-6#로깅 표시 | 플래시 리디렉션:<파일 이름>

```
Floor_Edge-6#show logging | redirect flash:console_logs_Floor_Edge-6_12_14_18
```

## 클라이언트 디버깅

SDA FEW에서 무선 클라이언트 디버깅 문제가 복잡해질 수 있습니다.

한 번에 하나의 디바이스를 제거하려면 아래 워크플로를 따르십시오.

1. WLC
2. 패브릭 에지
3. 액세스 포인트(패브릭 에지에서 디버깅이 AP를 가리키는 경우)
4. 중간/경계 노드(데이터 경로에 문제가 있는 경우)
5. 컨트롤 플레인 노드.(제어 경로 문제가 발생한 경우)

## WLC 디버깅

클라이언트 연결 문제의 경우 show 명령 및 디버깅이 포함된 WLC에 대한 정보를 수집하여 디버깅을 시작하십시오.

### AireOS WLC show 명령

show run-config

기술

wlan 요약 표시

show wlan <id> → 모든 SSID에 대해 이 출력을 수집합니다(작업 중 및 비작동 시 최소 1개).

패브릭 요약 표시

fabric map-server 요약 표시

클라이언트 요약 표시

show client detail <mac\_id>

### AireOS WLC 디버그 명령

디버그 클라이언트 <mac1> → 클라이언트 연결, 로밍, 디버깅

debug fabric client detail enable → 이렇게 하면 정보 패브릭 등록 메시지가 표시됩니다.

## 패브릭 에지 디버깅

WLC에서 디버깅한 후 클라이언트에 대한 컨트롤 플레인 경로 관련 문제가 없음을 확인했습니다. 클라이언트가 Assoc, Authentication(인증)에서 올바른 SGT 태깅 또는 AAA 파라미터로 실행 상태로 이동하고 이 단계로 이동하여 문제를 추가로 격리합니다.

위 AP 디버깅 섹션에 설명된 대로 액세스 터널 프로그래밍이 정확하다는 것도 확인해야 합니다.

### 확인할 명령 표시

에서 L2 lisp 인스턴스 ID 찾기(위의 show client detail <mac\_id>)

`show lisp instance-id <L2_LISP> ethernet database wlc` → 특정 L2 lisp 인스턴스 ID에 대한 모든 WLC 관련 클라이언트가 나열됩니다. 소스 수는 네트워크의 컨트롤 플레인 노드 수와 일치해야 합니다.

`show lisp instance-id <L2_LISP> ethernet database wlc <client mac in h.h.h>` → 특정 클라이언트에 대한 세부 정보가 표시됩니다.

장치 추적 데이터베이스 표시 | i v | → 클라이언트가 연결되어 있고 있어야 하는 특정 SVI를 찾습니다.

장치 추적 데이터베이스 표시 | i <mac> → 클라이언트 항목을 찾습니다. 올바른 VLAN, 인터페이스, 상태 및 기간을 기준으로 합니다.

`show mac address-table dynamic vlan <VLAN-ID>` → mac에 대한 항목이 디바이스 추적 데이터베이스와 일치해야 합니다. 일치하는 경우 FED에서 mac 주소 항목을 확인하십시오.

`show ip dhcp snooping binding vlan <vlan_where_client_is_connected>`

`show ip arp vrf <VN>`

`show mac address-table vlan <vlan_where_client_is_connected>`

`show platform software fed switch active matm macTable vlan <vlan_where_client_is_connected>` → 올바른 경우 로컬 스위치에서 무선 클라이언트에 대한 프로그래밍이 올바르게 수행됩니다.

`show platform software matm switch active F0 mac <mac_id>`

### 패브릭 에지의 디버그 명령

Fabric Edge에서 클라이언트 항목 프로그래밍에 문제가 있는 경우 Fed 추적을 수집해야 합니다. 아래 디버그를 활성화한 후에는 두 가지 방법으로 동일한 작업을 수행할 수 있습니다.

메서드에 관계없이 활성화해야 하는 명령을 디버깅하고 설정합니다.

```
set platform software trace fed switch active all modules emergency
플랫폼 소프트웨어 추적 fed 스위치 활성화 l2_fib_entry verbose 설정
플랫폼 소프트웨어 추적 fed 스위치 활성화 l2_fib_adj verbose 설정
플랫폼 소프트웨어 추적 fed 스위치 active inject verbose
set platform software trace fed switch active matbose
```

debug(콘솔 로그를 비활성화하고 로그 버퍼를 늘리는지 확인)

디버그 디바이스 추적

디버그 lisp 컨트롤 플레인 모두

디버그 플랫폼 모두

모두 디버그 matt

**방법 1: 디버그를 활성화한 후 특정 클라이언트에 대한 무선 활성 추적 로그 수집 [DHCP 문제가 발생한 경우 이 방법을 사용하지 마십시오.]**

문제가 재생성될 때까지 기다립니다.

```
디버그 플랫폼 조건 mac <mac-id> 컨트롤 플레인
디버그 플랫폼 조건 시작
디버그 플랫폼 조건 중지
소프트 추적 필터 이전 무선 컨텍스트 mac <mac-id> 요청
```

문제가 재생성된 후 콘솔 로그를 플래시로 리디렉션합니다.

**방법 2: 디버깅 활성화 후 아카이브 추적 로그 수집**

문제가 재생성될 때까지 기다립니다.

플랫폼 소프트웨어 추적 아카이브 요청

파일을 수집하여 로그를 디코딩하고 클라이언트 mac에 대한 fed, ios, fman 로그를 분석합니다.

문제가 재생성된 후 콘솔 로그를 플래시로 리디렉션합니다.

## 엑세스 포인트 디버깅

### 2800/3800/1562 AP 모델의 디버깅

AP 측 문제의 경우 AP 측 로그를 수집하고 SR에 연결하기 전에 모든 WLC show 명령 및 로그를 수집해야 합니다.

클라이언트 측에서 데이터 관련 문제를 디버깅하려면 다음 단계를 수행하십시오.

#### 1. AP show 명령을 수집합니다.(2-3회, 테스트 전/후)

시계 표시

기간 길이 0

기간

기술

로깅 표시

컨트롤러 nss 상태 표시 컨트롤러 nss 상태

IP 터널 패브릭 표시

CWA 문제가 발생한 경우, 상위 명령 외에도 아래 로그도 수집하십시오.아래 명령은 테스트를 완료하기 전후에 한 번 수집해야 합니다.

```
show client access-lists pre-auth all <client mac>
```

```
show client access-lists post-auth all <client mac>
```

```
show ip access lists(IP 액세스 목록 표시)
```

```
show controller d [0/1] 클라이언트
```

```
show capwap cli detailcb
```

기술 지원

#### 2. AP 디버그(MAC 주소당 필터)

클라이언트 데이터 경로 문제:

```
debug dot11 client datapath eapol addr <mac>
```

```
debug dot11 client datapath dhcp addr <mac>
```

```
debug dot11 client datapath arp addr <mac>
```

클라이언트 AP 추적:

```
config ap client-trace address add <mac>  
config ap client-trace 출력 콘솔 로그 활성화
```

```
config ap client-trace filter all enable
```

```
config ap client-trace filter probe disable
```

```
config ap client-trace start
```

기간

```
exec-timeout 0 0
```

CWA 문제:

```
debug capwap client avc all
```

디버그 capwap 클라이언트 acl

디버그 클라이언트 <client mac>

```
debug dot11 client level info address <mac>
```

```
debug dot11 클라이언트 수준 이벤트 주소 <mac>
```

디버그 flexconnect pmk

클라이언트 DHCP 디버깅 문제

아래 디버그를 사용하여 디버깅할 수 있는 문제

1. 스위치에 DHCP 검색 메시지가 표시되지 않음
2. 무선 클라이언트가 DHCP 제안을 받지 않습니다. DHCP 검색은 "debug ip dhcp snooping packet" 로그에서 관찰됨
3. AP에 연결된 포트, 업링크 포트 및 퓨전 측의 DHCP 서버에 연결된 포트에서 패킷 캡처를 수집합니다.

디버깅/표시 명령

1. SSID가 IP 풀에 할당된 경우 Cisco DNA Center를 확인합니다.
2. WLC에서 WLAN이 활성화되었는지 확인
3. 무선이 활성화되고 802.11a 및 802.11b 네트워크가 모두 활성화되었는지 확인합니다.

## AP 온보딩

기존 방법/단계:(AP Vlan Scope에는 WLC를 가리키는 옵션 43 또는 옵션 60이 있음)

1. 인증을 "인증 없음"으로 선택합니다.
2. AP IP 풀을 사용하여 Infra\_VN을 구성하고 무선 클라이언트 IP 풀을 사용하여 Default\_VN을 구성합니다.
3. AP가 Infra\_VN과 연결된 에지 인터페이스 포트 구성
4. AP가 IP를 가져오고 WLC에 가입하면 디바이스 인벤토리에서 검색됩니다.
5. AP를 선택하고 특정 지점에 지정하고 AP를 프로비저닝합니다.
6. 프로비저닝되면 패브릭에 WLC를 추가하는 동안 생성된 AP 그룹에 AP가 할당됩니다.

플러그 앤 플레이/제로 터치 AP 프로비저닝(AP VLAN 범위 고려 시 Cisco DNA 센터를 가리키는 옵션 43이 있음)

### AP 디버그

#### DHCP 디버깅

패브릭 에지 측면:

사용할 디버그:

디버그 ip dhcp snooping 패킷

디버그 ip dhcp snooping 이벤트

아래에 첨부된 샘플 로그 파일입니다.