

# DNA를 사용하여 무선에 대한 소프트웨어 정의 액세스 구현

## 목차

---

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[SD-Access](#)

[SD-Access 무선 아키텍처](#)

[개요](#)

[SDA 역할 및 용어](#)

[언더레이 및 오버레이 네트워크](#)

[기본 워크플로](#)

[AP 조인](#)

[클라이언트 온보드](#)

[클라이언트 로밍](#)

[구성](#)

[네트워크 디아이어그램](#)

[Cisco DNA에서 WLC 검색 및 프로비저닝](#)

[WLC 추가](#)

[액세스 포인트 추가](#)

[SSID 생성](#)

[WLC 프로비저닝](#)

[액세스 포인트 프로비저닝](#)

[패브릭 사이트 만들기](#)

[패브릭에 WLC 추가](#)

[AP 조인](#)

[클라이언트 온보드](#)

[다음을 확인합니다.](#)

[WLC 및 Cisco DNA에서 패브릭 컨피그레이션 확인](#)

[문제 해결](#)

[클라이언트가 IP 주소를 가져오지 않음](#)

[SSID가 브로드캐스트되지 않음](#)

[관련 정보](#)

---

## 소개

이 문서에서는 패브릭 지원 WLC 및 Cisco DNA의 액세스 LAP와 관련된 무선 기술용 SDA를 구현하는 방법에 대해 설명합니다.

# 사전 요구 사항

## 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 9800 WLC(Wireless LAN Controller) 컨피그레이션
- LAP(Lightweight Access Point)
- Cisco DNA

## 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 9800-CL WLC Cisco IOS® XE, 버전 17.9.3
- Cisco 액세스 포인트: 9130AX, 3802E, 1832I
- Cisco DNA 버전 2.3.3.7

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-Access

Software-Defined Access는 동적 규칙 및 자동화된 세그멘테이션을 통해 네트워크 전반에 보안 정책을 설정하고 자동으로 시행하며, 최종 사용자가 네트워크에 연결하는 방법을 제어 및 구성할 수 있도록 합니다. SD-Access는 연결된 각 엔드포인트와 초기 신뢰 수준을 설정하고 이를 지속적으로 모니터링하여 신뢰 수준을 다시 확인합니다. 엔드포인트가 정상적으로 동작하지 않거나 치료가 탐지된 경우, 최종 사용자는 침해가 발생하기 전에 엔드포인트를 즉시 억제하고 조치를 취할 수 있으며, 비즈니스 위험을 줄이고 리소스를 보호할 수 있습니다. 완전히 통합된 솔루션이며 신규 및 구축된 네트워크 모두에 쉽게 구축하고 구성할 수 있습니다.

SD-Access는 SDN(Software-Defined Networking) 구성 요소를 사용하여 IBN(Intent-Based Networking) 및 중앙 정책 제어를 제공하는 기존 캠퍼스 네트워크의 진화 과정인 Cisco 기술입니다.

SD-Access의 세 가지 네트워크 중심 핵심 요소:

1. 네트워크 패브릭: 프로그래밍 가능한 오버레이 및 가상화를 지원하는 네트워크 자체를 추상화 한 것입니다. 네트워크 패브릭은 유선 및 무선 액세스를 모두 지원하며, 이를 통해 서로 분할되고 비즈니스 의도에 따라 정의되는 여러 개의 논리적 네트워크를 호스팅할 수 있습니다.
2. 오케스트레이션: Cisco DNA는 SDA의 오케스트레이터 엔진입니다. Cisco DNA는 SDN 컨트롤러처럼 작동합니다. 패브릭에서 정책 및 컨피그레이션 변경을 구현합니다. 또한 네트워크 설계를 지원하고 DNA Assurance를 통해 실시간 네트워크 텔레메트리 운영 및 성능 분석을 지원하는 툴도 통합됩니다. Cisco DNA의 역할은 보안, QoS(Quality of Service), 마이크로세그멘테이션을 위한 정책 변경 및 네트워크 의도를 제공하도록 네트워크 패브릭을 오케스트레

이션하는 것입니다.

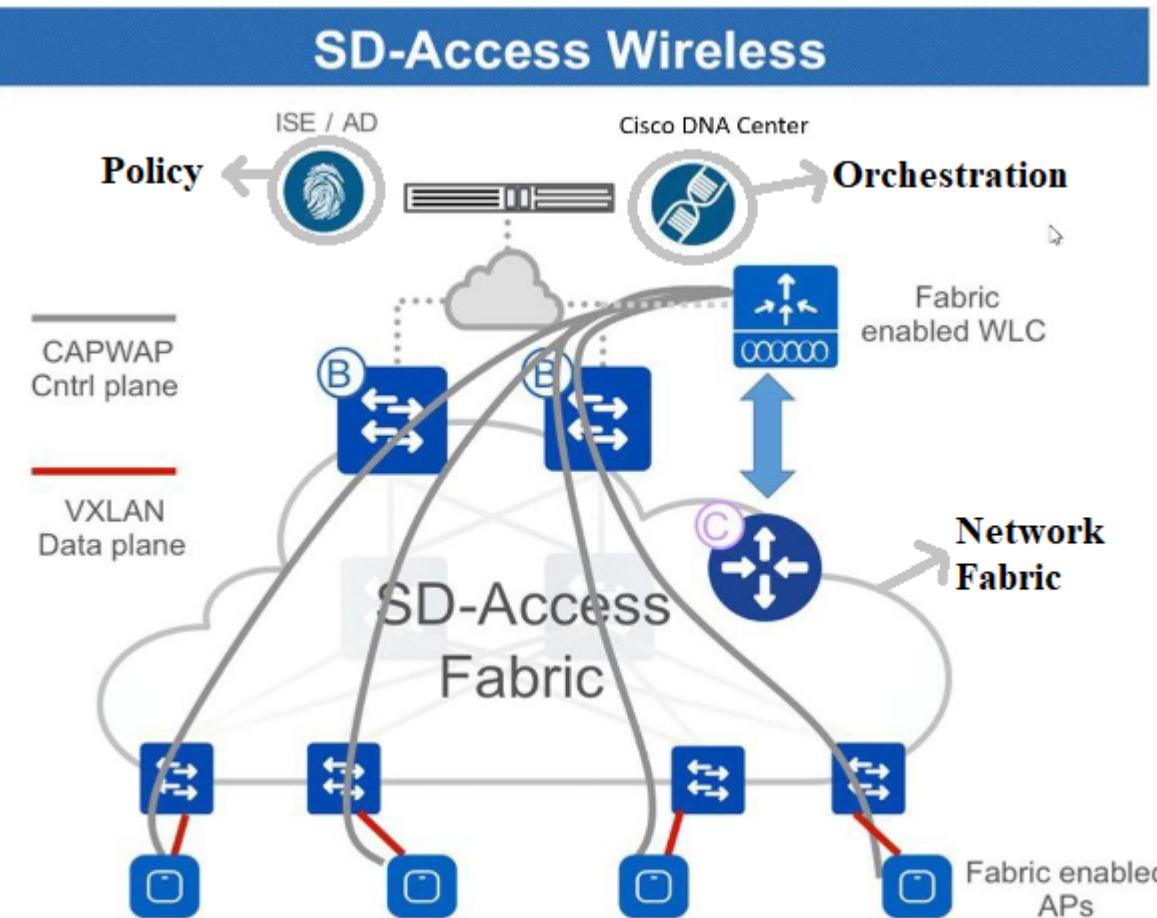
3. 정책: ISE(Identity Services Engine)는 네트워크 정책을 정의하는 툴입니다. ISE는 디바이스와 노드가 가상 네트워크로 분할되는 방식을 구성합니다. ISE는 또한 액세스 디바이스에서 패브릭으로 들어갈 때 사용자 트래픽을 분할하는 데 사용되는 SGT(Scalable Group Tag)를 정의합니다. SGR은 ISE에서 정의한 마이크로세그먼테이션 정책을 시행해야 합니다.

SDA는 중앙 집중식 오피스트레이션을 기반으로 합니다. 프로그래밍 가능한 오피스트레이션 엔진인 Cisco DNA, 정책 엔진인 ISE, 새로운 세대의 프로그래밍 가능한 스위치를 조합하면 이전보다 훨씬 유연하고 관리 가능한 패브릭 시스템이 됩니다.



참고: 이 문서에서는 특히 SD-Access Wireless에 대해 설명합니다.

네트워크 패브릭은 다음 요소로 구성됩니다.

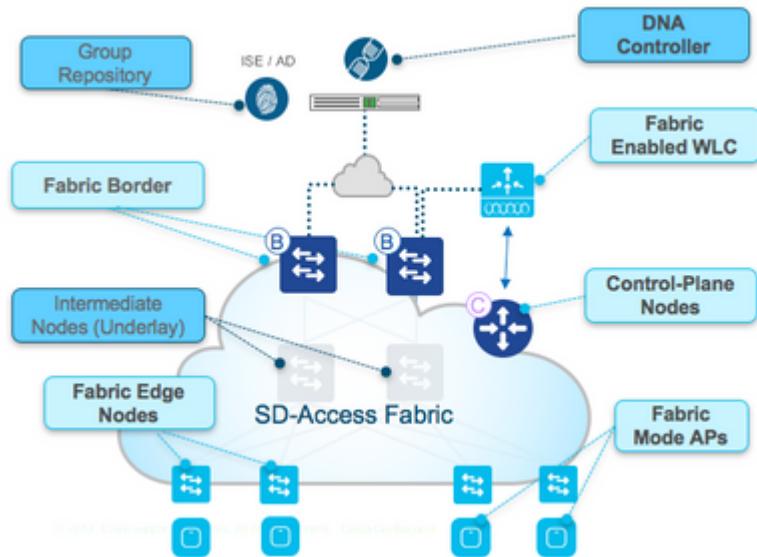


네트워크 패브릭의 요소

패브릭에 대한 무선 통합으로 인해 무선 네트워크에 다음과 같은 여러 가지 이점이 있습니다. 간소화, 물리적 위치에 걸쳐 확장된 서브넷을 통한 모빌리티, 중앙 집중식 정책을 통해 유선 및 무선 도메인 모두에서 일관되게 세분화할 수 있습니다. 또한 컨트롤러가 무선 네트워크에 대한 중앙 집중식 서비스 및 컨트롤 플레이인으로 계속 기능하면서 데이터 플레인을 해제하여 임무를 전달할 수 있게 합니다. 따라서 FlexConnect 모델과 마찬가지로 데이터 플레인 트래픽을 더 이상 처리할 필요가 없으므로 무선 컨트롤러 확장성이 실제로 향상됩니다.

# SD-Access 무선 아키텍처

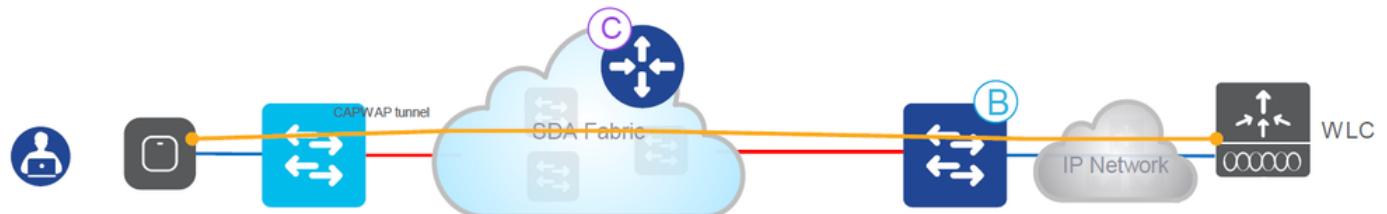
## 개요



## SDA 개요

지원되는 기본 SDA 무선 구축 모델은 두 가지입니다.

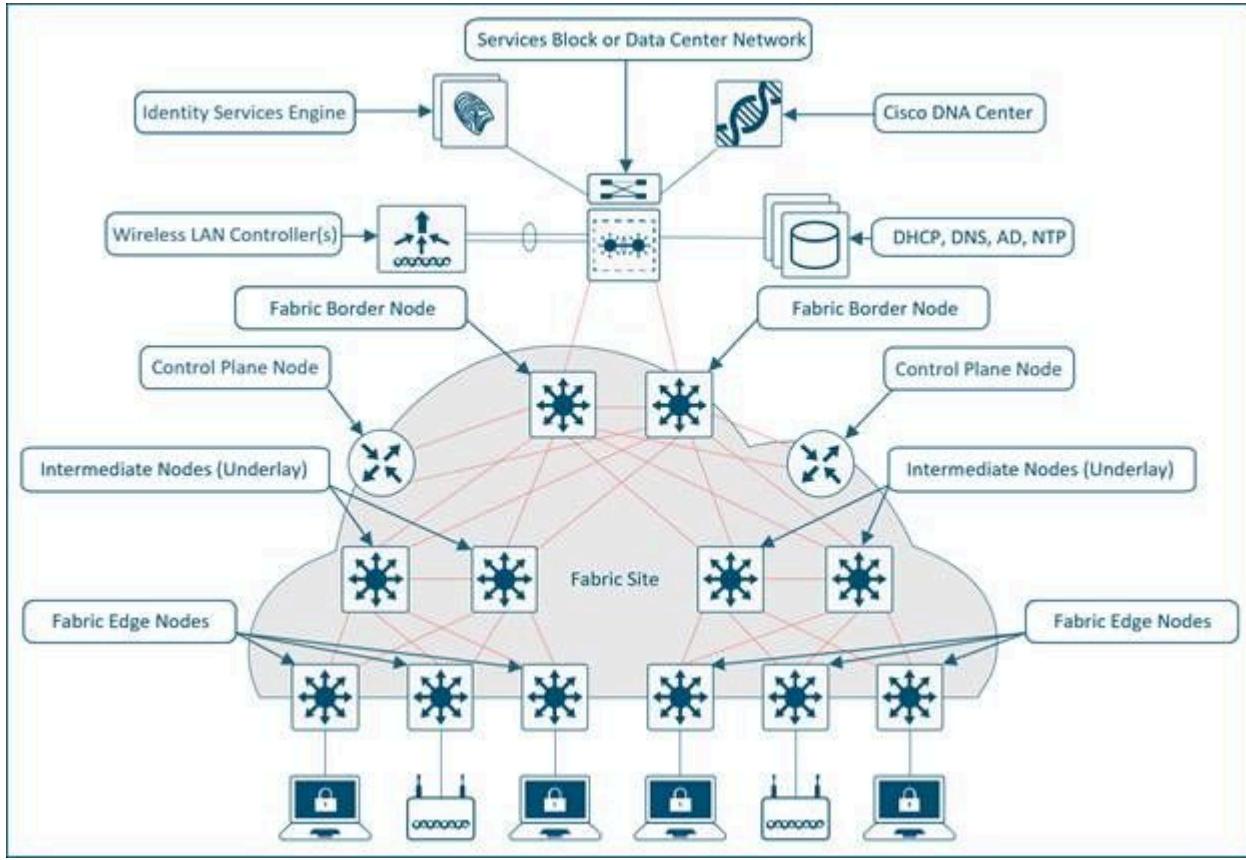
그 중 하나는 OTT(over-the-top) 방식으로서 패브릭 유선 네트워크에 연결된 기존 CAPWAP 구축입니다. SDA 패브릭은 CAPWAP 제어 및 데이터 플레인 트래픽을 무선 컨트롤러로 전송합니다.



## Over-The-Top 방법

이 구축 모델에서 SDA 패브릭은 무선 트래픽을 위한 전송 네트워크입니다(마이그레이션에 종종 구축되는 모델). AP는 클래식 로컬 모드와 매우 유사하게 작동합니다. CAPWAP 제어 평면과 데이터 평면 모두 컨트롤러에서 종료되므로 컨트롤러가 패브릭에 직접 참여하지 않습니다. 이 모델은 유선 스위치가 먼저 SDA 패브릭으로 마이그레이션되지만 무선 네트워크가 아직 완전한 패브릭 오버레이 통합을 위한 준비가 되지 않은 경우에 자주 사용됩니다.

다른 구축 모델은 완전히 통합된 SDA 모델입니다. 무선 네트워크는 패브릭에 완전히 통합되고 오버레이에 참여하므로 서로 다른 WLAN이 서로 다른 가상 네트워크(VN)에 속할 수 있습니다. 무선 컨트롤러는 AP를 관리하기 위해 CAPWAP 컨트롤 플레인만 관리하며, CAPWAP 데이터 플레인은 컨트롤러에 오지 않습니다.



완전 통합형 SDA 모델

무선 데이터 플레인은 유선 스위치와 유사하게 처리됩니다. 각 AP는 VXLAN에 데이터를 캡슐화하여 패브릭 에지 노드로 전송하며, 이 경우 패브릭 전반에서 다른 에지 노드로 전송됩니다. 무선 컨트롤러는 패브릭 컨트롤러로 구성되어야 하며, 이는 정상적인 작동을 수정한 것입니다.

패브릭 지원 컨트롤러는 패브릭 제어 평면과 통신하며, 레이어 2 클라이언트 MAC 주소 및 레이어 2 VNI(Virtual Network Identifier) 정보를 등록합니다. AP는 무선 엔드포인트와의 통신을 담당하며, 트래픽의 캡슐화 및 캡슐화 해제를 통해 VXLAN 데이터 플레인을 지원합니다.

## SDA 역할 및 용어

네트워크 패브릭은 다음 요소로 구성됩니다.

- 컨트롤 플레인 노드: LISP(Location Separator Protocol) 컨트롤 플레인에 속해 있으며 위치 관계(또는 디바이스 관계)에 대한 EID(엔드포인트 ID)를 관리하는 위치 매핑 시스템(호스트 디이터베이스)입니다. 컨트롤 플레인은 컨트롤 플레인 기능을 제공하는 전용 라우터가 될 수도 있고 다른 패브릭 네트워크 요소와 공존할 수도 있습니다.
- 패브릭 보더 노드: 일반적으로 외부 네트워크와 SDA 패브릭 간의 경계에서 작동하는 라우터로, 패브릭의 가상 네트워크에 라우팅 서비스를 제공합니다. 외부 레이어 3 네트워크를 SDA 패브릭에 연결합니다.
- 패브릭 에지 노드: 스위치, AP 및 라우터와 같은 비패브릭 디바이스를 SDA 패브릭에 연결하는 패브릭 내 디바이스입니다. 이 노드는 가상 오버레이 터널 및 VPN을 VXLAN(Virtual eXtensible LAN)으로 생성하고 패브릭 바인딩 트래픽에 SGT를 부여하는 노드입니다. 패브릭 에지 양쪽의 네트워크는 SDA 네트워크 내부에 있습니다. 유선 엔드포인트를 SD-Access 패브

릭에 연결합니다.

- 중간 노드: 이러한 노드는 SDA 패브릭의 코어 내부에 있으며 에지 또는 경계 노드에 연결됩니다. 중간 노드는 SDA 트래픽을 IP 패킷으로 전달하기만 합니다. 여러 가상 네트워크가 관련되어 있음을 인식하지 못합니다.
- 패브릭 WLC: 패브릭이 활성화되어 있고 SDA 제어 평면에 참여하지만 CAPWAP 데이터 평면을 처리하지 않는 무선 컨트롤러입니다.
- 패브릭 모드 AP: 패브릭이 활성화된 액세스 포인트. 무선 트래픽은 AP에서 VXLAN으로 캡슐화되므로 에지 노드를 통해 패브릭으로 전송할 수 있습니다.
- Cisco DNA(DNAC): SDA(Software Defined Access) 패브릭 오버레이 네트워크용 엔터프라이즈 SDN 컨트롤러이며, 자동화 및 보증 작업을 모두 담당합니다. 또한 언더레이를 구성하는 네트워크 디바이스(SDA와 관련되지 않음)에 대한 일부 자동화 및 관련 작업에도 활용할 수 있습니다.
- ISE: ISE(Identity Services Engine)는 AAA(Authentication, Authorization and Accounting) 서버의 역할 및 기능 중 적어도 하나가 아니라 다양한 역할과 기능을 수행할 수 있는 향상된 정책 플랫폼입니다. ISE는 일반적으로 AD(Active Directory)와 상호 작용하지만, 사용자는 소규모 구축을 위해 ISE 자체에서도 로컬로 구성할 수 있습니다.



참고: 컨트롤 플레인은 SDA 아키텍처의 중요한 인프라 요소이므로 탄력적으로 구축하는 것이 좋습니다.

## 언더레이 및 오버레이 네트워크

SDA 아키텍처는 물리적 네트워크(언더레이 네트워크)에서 실행되는 프로그래밍 가능한 가상 네트워크(오버레이 네트워크)를 지원하는 패브릭 기술을 활용합니다.

패브릭은 오버레이입니다.

오버레이 네트워크는 디바이스를 가상으로 연결하는 데 사용되는 논리적 토플로지이며, 임의의 물리적 언더레이 토플로지를 기반으로 구축됩니다. 대체 전달 특성을 사용하여 언더레이에서 제공하지 않는 추가 서비스를 제공합니다. 하나 이상의 가상화되고 세그먼트화된 네트워크를 생성하기 위해 언더레이 상단에 생성됩니다. 오버레이의 소프트웨어 정의 특성으로 인해 물리적 연결의 제약 없이 매우 유연한 방식으로 연결할 수 있습니다. 오버레이는 단일 물리적 출구 지점(패브릭 경계 노드)을 갖도록 프로그래밍할 수 있고 하나의 방화벽을 사용하여 뒤에 있는 네트워크를 보호할 수 있으므로(위치 여부에 관계 없이) 보안 정책을 적용하는 쉬운 방법입니다. 오버레이는 VXLAN을 사용하여 트래픽을 캡슐화합니다. VXLAN은 VNI(VXLAN 네트워크 식별자)로 식별되는 각 오버레이 네트워크를 사용하여 언더레이를 통한 전송을 위해 완전한 레이어 2 프레임을 캡슐화합니다. 오버레이 패브릭은 복잡한 경향이 있으며, 배포된 새로운 가상 네트워크에 상당한 관리자 오버헤드가 필요하거나 보안 정책을 구현해야 합니다.

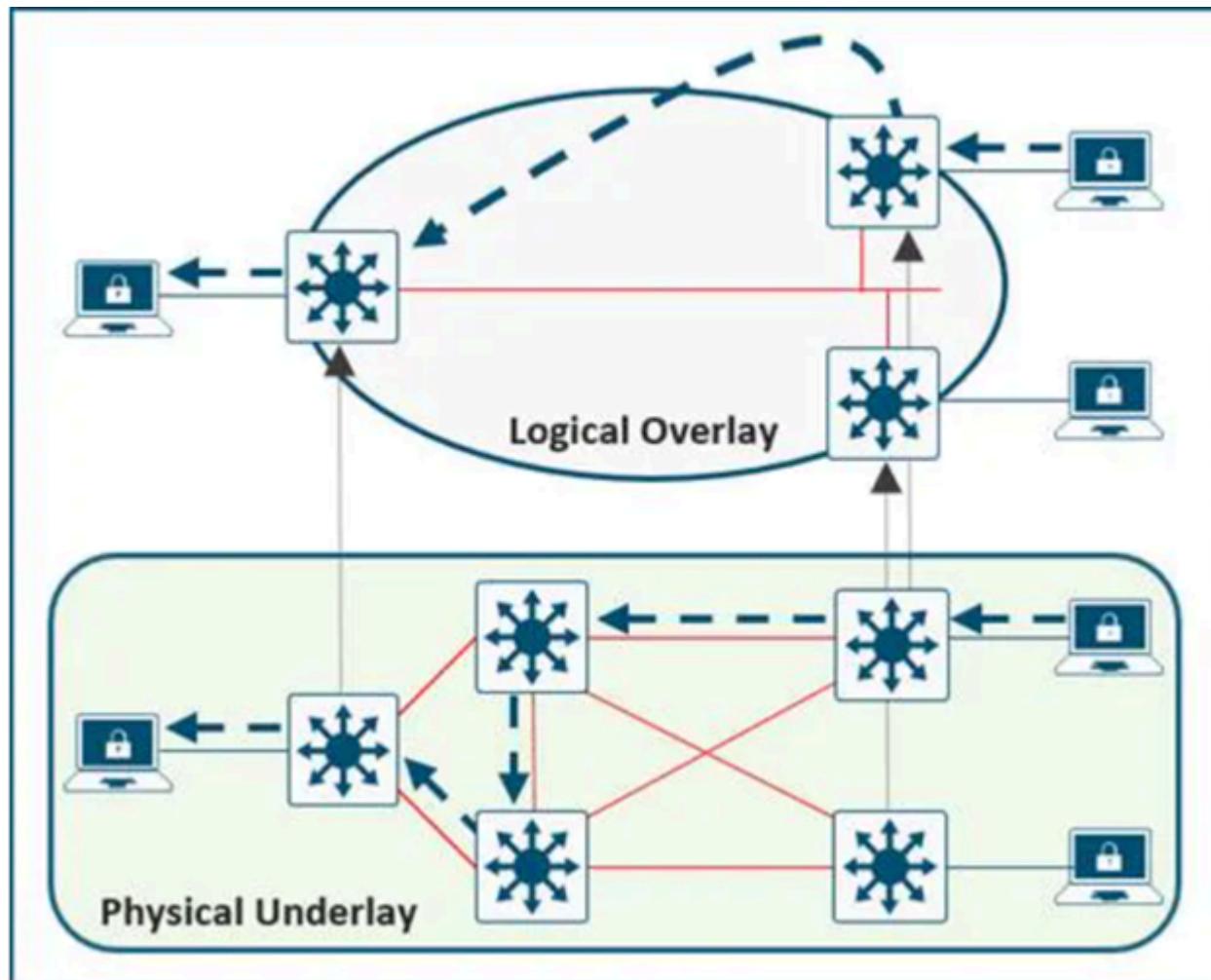
네트워크 오버레이의 예:

- GRE, mGRE
- MPLS, VPLS
- IPSec, DMVPN
- CAPWAP
- 리스프
- OTV
- DFA
- ACI

언더레이이 네트워크는 SDA 네트워크를 구축하는 데 사용되는 스위치, 라우터, 무선 AP와 같은 물리적 노드에 의해 정의됩니다. 언더레이의 모든 네트워크 요소는 라우팅 프로토콜을 사용하여 IP 연결을 설정해야 합니다. 언더레이 네트워크는 기존의 액세스, 배포, 코어 모델을 사용하지 않을 것으로 보이지만 강력한 성능, 확장성 및 고가용성을 제공하는 잘 설계된 레이어 3 기반을 사용해야 합니다.



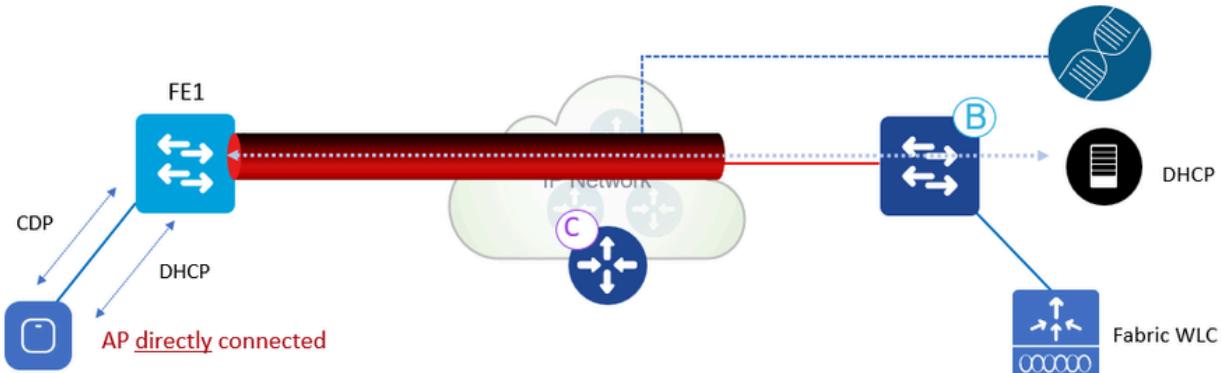
참고: SDA는 언더레이 네트워크에서 IPv4를 지원하고 오버레이 네트워크에서 IPv4 및/또는 IPv6를 지원합니다.



언더레이 및 오버레이 네트워크

## 기본 워크플로

AP 조인



AP 조인 워크플로

## AP 조인 워크플로:

1. 관리자가 INFRA\_VN의 DNAC에서 AP 풀을 구성합니다. Cisco DNA는 모든 패브릭 에지 노드의 컨피그레이션을 사전 프로비저닝하여 AP를 자동으로 온보딩합니다.
  2. AP가 연결되어 있고 전원이 켜집니다. Fabric Edge는 CDP를 통해 AP를 검색하고 매크로를 적용하여 스위치 포트를 올바른 VLAN에 할당합니다(또는 인터페이스 템플릿).
  3. AP가 오버레이에서 DHCP를 통해 IP 주소를 가져옵니다.
  4. Fabric Edge는 AP IP 주소 및 MAC(EID)를 등록하고 CP(Control Plane)를 업데이트합니다.
  5. AP가 기존 방법으로 WLCs IP를 학습합니다. 패브릭 AP가 로컬 모드 AP로 조인됩니다.
  6. WLC는 패브릭을 지원하는지 확인합니다(Wave 2 또는 Wave 1 AP).
  7. AP가 패브릭에서 지원되는 경우 WLC는 CP에 쿼리하여 AP가 패브릭에 연결되어 있는지 확인합니다.
  8. RLOC를 사용하여 CP(Control Plane)가 WLC에 회신합니다. 즉, AP가 패브릭에 연결되어 있으며 "패브릭 사용"으로 표시됩니다.
  9. WLC는 CP의 AP에 대해 L2 LISP 등록을 수행합니다(즉, AP "특수" 보안 클라이언트 등록). 이는 WLC에서 패브릭 엣지로 중요한 메타데이터 정보를 전달하는 데 사용됩니다.
  10. 이 프록시 등록에 대한 응답으로 CP(Control Plane)는 Fabric Edge에 알림을 보내고 WLC에서 받은 메타데이터(AP 및 AP IP 주소임을 나타내는 플래그)를 전달합니다.
  11. Fabric Edge는 정보를 처리하고 AP임을 인식하여 지정된 IP에 대한 VXLAN 터널 인터페이스를 생성합니다(최적화: 스위치측은 클라이언트가 참가할 준비가 되었습니다.)

debug/show 명령을 사용하여 AP 조인 워크플로를 확인하고 검증할 수 있습니다.

컨트롤 플레인

lisp 컨트롤 플레인 모두 디버그

show lisp instance-id <L3 instance id> ipv4 server(AP가 연결된 에지 스위치에서 등록한 AP IP 주소를 표시해야 함)

show lisp instance-id <L2 instance id> 이더넷 서버(AP 라디오와 이더넷 mac-address, WLC에 의해 등록된 AP 라디오 및 AP가 연결된 에지 스위치에 의한 이더넷 mac을 표시해야 함)

에지 스위치

모두 디버그 액세스 터널

lisp 컨트롤 플레인 모두 디버그

show access-tunnel 요약

show lisp instance < L2 instance id> ethernet database wlc access-points(AP 무선 mac을 여기에 표시해야 함)

WLC

show fabric ap summary

WLC LISP 디버깅

플랫폼 소프트웨어 추적 설정 wcd 새시 활성 r0 lisp-agent-api 디버그

플랫폼 소프트웨어 추적 wwncd 새시 활성 r0 lisp-agent-db 디버그 설정

플랫폼 소프트웨어 추적 wcd 새시 활성 r0 lisp-agent-fsm 디버그 설정

플랫폼 소프트웨어 추적 설정 wcd 새시 활성 r0 lisp-agent-internal debug

플랫폼 소프트웨어 추적 설정 wcd 새시 활성 r0 lisp-agent-lib 디버그

플랫폼 소프트웨어 추적 설정 wnnd 새시 활성 r0 lisp-agent-lispmsg 디버그

플랫폼 소프트웨어 추적 설정 wcd 새시 활성 r0 lisp-agent-shim 디버그

플랫폼 소프트웨어 추적 설정 wcd 새시 활성 r0 lisp-agent-transport 디버그

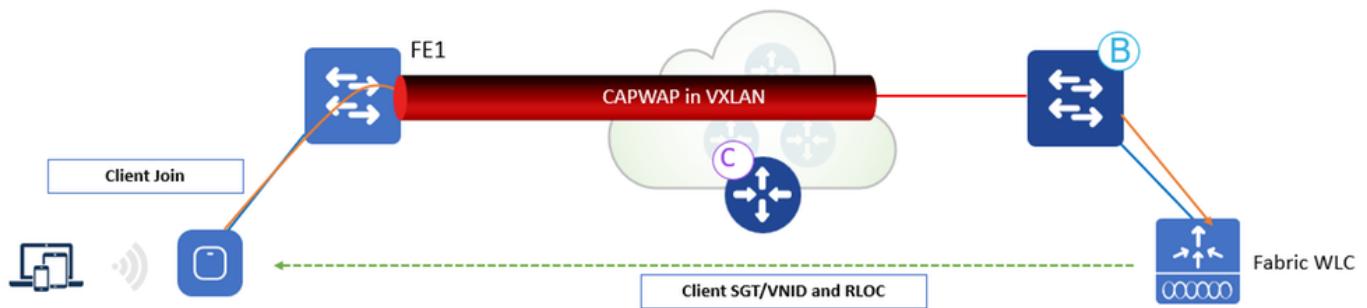
플랫폼 소프트웨어 추적 설정 wcd 새시 활성 r0 lisp-agent-ha 디버그

플랫폼 소프트웨어 추적 설정 wnnd 새시 활성 r0 ewlc-infra-evq 디버그

액세스 포인트

show ip tunnel fabric

클라이언트 온보드



클라이언트 온보드 워크플로

클라이언트 온보드 워크플로:

1. 클라이언트가 패브릭 지원 WLAN에 대해 인증합니다. WLC는 ISE에서 SGT를 가져오고 RLOC IP와 함께 클라이언트 L2VNID 및 SGT로 AP를 업데이트합니다. WLC는 내부 데이터베이스의 AP RLOC를 알고 있습니다.
2. WLC 프록시가 CP에 클라이언트 L2 정보 등록 클라이언트 SGT와 같은 추가 정보를 전달하기 위해 LISP 수정된 메시지입니다.
3. 패브릭 엣지는 CP에 의해 알림을 받고 L2의 클라이언트 MAC를 전달 테이블에 추가하고 클라이언트 SGT를 기반으로 ISE에서 정책을 가져옵니다.
4. 클라이언트가 DHCP 요청을 시작합니다.
5. AP는 L2 VNI 정보를 사용하여 VXLAN에서 캡슐화합니다.
6. 패브릭 엣지는 L2 VNID를 VLAN 인터페이스에 매핑하고 오버레이에서 DHCP를 전달합니다(유선 패브릭 클라이언트와 동일).
7. 클라이언트가 DHCP로부터 IP 주소를 수신합니다.
8. DHCP 스누핑(및/또는 고정용 ARP)은 패브릭 엣지가 CP에 클라이언트 EID 등록을 트리거합니다.

debug/show 명령을 사용하여 클라이언트 온보드 워크플로를 확인하고 검증할 수 있습니다.

컨트롤 플레인

lisp 컨트롤 플레인 모두 디버그

에지 스위치

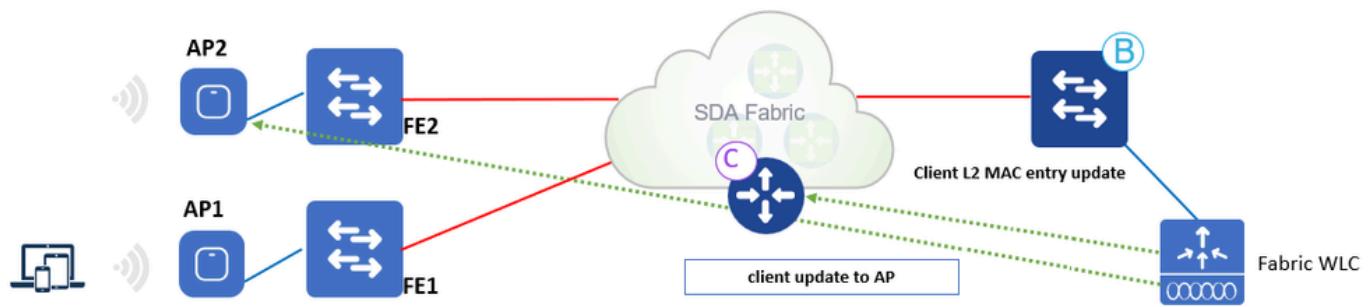
lisp 컨트롤 플레인 모두 디버그

debug ip dhcp snooping 패킷/이벤트

WLC

LISP 통신의 경우 AP 조인과 동일한 디버그가 수행됩니다.

## 클라이언트 로밍



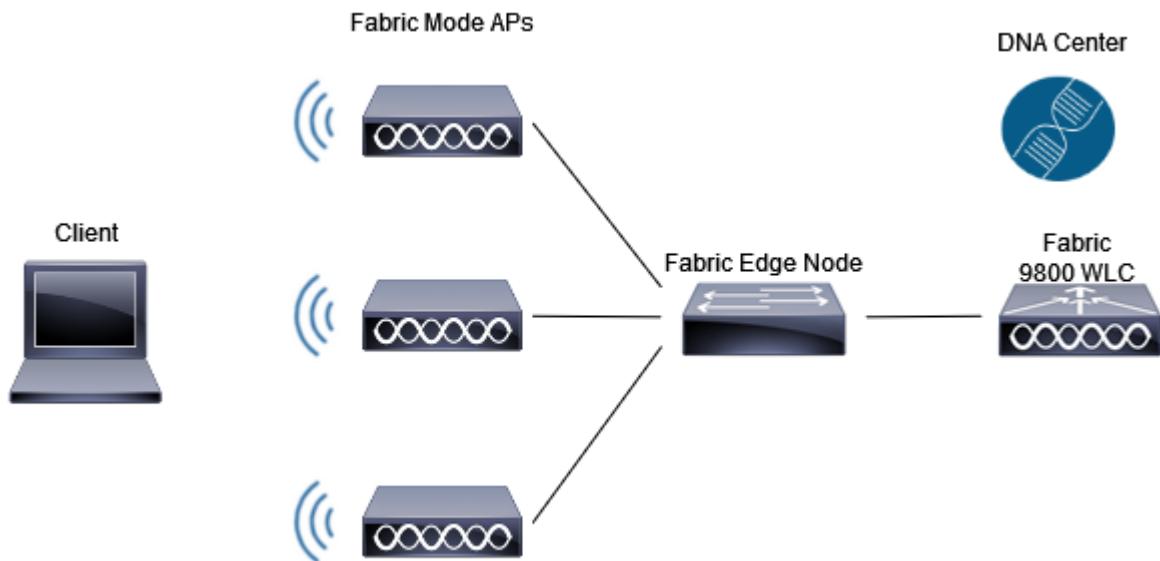
클라이언트 로밍 워크플로

클라이언트 로밍 워크플로:

1. 클라이언트가 FE2의 AP2로 로밍(스위치 간 로밍). WLC는 AP에 의해 알림을 받습니다.
2. WLC는 클라이언트 정보(SGT, RLOC)를 사용하여 AP의 전달 테이블을 업데이트합니다.
3. WLC가 새로운 RLOC 패브릭 에지 2를 사용하여 CP의 L2 MAC 항목을 업데이트합니다.
4. CP는 다음 사항을 알립니다.
  - VXLAN 터널을 가리키는 포워드 테이블에 클라이언트 MAC을 추가하기 위한 패브릭 에지 FE2(roam-to switch).
  - 무선 클라이언트를 위해 정리할 Fabric Edge FE1(roam-from 스위치).
5. 패브릭 에지는 트래픽을 수신하면 CP 데이터에 있는 L3 항목(IP)을 업데이트합니다.
6. 패브릭 에지 2의 VLAN 인터페이스(Anycast GW)가 동일하므로 Roam은 레이어 2입니다.

## 구성

네트워크 디자인



네트워크 다이어그램

## Cisco DNA에서 WLC 검색 및 프로비저닝

### WLC 추가

1단계. WLC를 추가할 위치로 이동합니다. 새 건물/층을 추가할 수 있습니다.

Design(설계) > Network Hierarchy(네트워크 계층)로 이동하여 건물/층을 입력하거나 이미지에 표시된 대로 새 층을 생성할 수 있습니다.

 Cisco DNA Center

The screenshot shows the Ekahau Site Survey application. On the left, there is a search bar labeled "Search Hierarchy" and a "Search Help" button. The main left panel displays a hierarchical tree view under "Global" and "Lisbon". Under "Lisbon", there is a folder named "Lisbon" containing "Floor 1" and "MyFloor", along with other building icons. A context menu is open over a building icon in the map area, listing options: "Edit Building", "Delete Building", "Add Floor" (which is highlighted with a red box), "Import Ekahau Project", "Import Ekahau Survey", "Sync: DNA Spaces/CMX", "Export Maps", "View Devices", and "View Settings".

새 축 만들기

2단계 출은 출기합니다. 비단의 신을 이미지드 업로드할 수 있습니다.

가 있는 패브릭 프로파일이 선택한 풀에 추가되고 정책 프로파일이 패브릭 프로파일에 매핑되면 패브릭에 대해 활성화됩니다.

WLC GUI 쪽에서 Configuration(컨피그레이션) > Wireless(무선) > Fabric(패브릭) > Profiles(프로파일)로 이동합니다.

Configuration > Wireless > Fabric > Profiles

Edit Fabric Profile

Profile Name\* s2-demo\_Global\_F\_d3r

Description s2-demo\_Global\_F\_d3r

L2 VNID 8189

SGT Tag 2-65519

⚠️ Modifying the profile may result in loss of connectivity

#### 패브릭 프로파일

6단계. Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > Policy(정책)로 이동합니다. 정책 프로필에 매핑된 패브릭 프로필을 확인합니다.

Configuration > Tags & Profiles > Policy

Edit Policy Profile

⚠️ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General Access Policies QoS and AVC Mobility Advanced

WLAN Timeout

Fabric Profile  s2-demo\_Global\_F\_d3r

Session Timeout (sec) 1800

Idle Timeout (sec) 300

Idle Threshold (bytes) 0

Link-Local Bridging

mDNS Service Policy default-mdns-ser ...

Hotspot Server Search or Select

#### 정책에 구성된 패브릭 프로파일

다음을 확인합니다.

WLC 및 Cisco DNA에서 패브릭 컨피그레이션 확인

WLC CLI에서:

WLC1# show tech

WLC1# show tech wireless

컨트롤 플레인 구성:

라우터 lisp

로케이터 테이블 기본값

로케이터 집합 WLC

172.16.201.202

로케이터 집합 종료

!

맵-서버 세션 패시브-오픈 WLC

사이트 사이트\_uci

설명 맵 - Cisco DNA-Center에서 구성된 서버

authentication-key 7 <키>

CB1-S1#sh lisp 세션

VRF에 대한 세션 기본값, 합계: 9, 설정: 5

피어 상태 Up/Down In/Out

172.16.201.202:4342 Up 3d07h 14/14

WLC 구성:

무선 패브릭

무선 패브릭 제어 평면 기본 제어 평면

ip 주소 172.16.2.2 키 0 47aa5a

WLC1# show fabric map-server summary

MS-IP 연결 상태

---

172.16.1.2 UP

WLC1# show wireless fabric 요약

패브릭 상태: 활성화됨

컨트롤 플레인:

이름 IP 주소 키 상태

---

default-control-plane 172.16.2.2 47aa5a Up

WLC GUI에서 Configuration(컨피그레이션) > Wireless(무선) > Fabric(패브릭)으로 이동하고 패브릭 상태가 Enabled(활성화됨)인지 확인합니다.

Configuration(컨피그레이션) > Wireless(무선) > Access Points(액세스 포인트)로 이동합니다. 목록에서 하나의 AP를 선택합니다. 패브릭 상태가 활성화되었는지 확인합니다.

Cisco DNA에서 Provision(프로비저닝) > Fabric Sites(패브릭 사이트)로 이동하여 패브릭 사이트가 있는지 확인합니다. 해당 패브릭 사이트에서 Fabric Infrastructure(패브릭 인프라) > Fabric(패브릭)으로 이동하여 WLC가 패브릭으로 활성화되어 있는지 확인합니다.

## 문제 해결

### 클라이언트가 IP 주소를 가져오지 않음

1단계. SSID가 패브릭인지 확인합니다. WLC GUI에서 Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > Policy(정책)로 이동합니다. 정책을 선택하고 Advanced(고급)로 이동합니다. 패브릭 프로파일이 활성화되어 있는지 확인합니다.

2단계. 클라이언트가 IP learn 상태에 머물러 있는지 확인합니다. WLC GUI에서 Monitoring(모니터링) > Wireless(무선) > Clients(클라이언트)로 이동합니다. 클라이언트 상태를 확인합니다.

3단계. 정책이 DHCP가 필요한지 확인합니다.

4단계. 트래픽이 AP - 에지 노드 간에 로컬로 전환되는 경우, 클라이언트 연결을 위해 AP 로그(client-trace)를 수집합니다. DHCP 검색이 전달되었는지 확인합니다. DHCP 제안이 도착하지 않으면 에지 노드에 문제가 발생합니다. DHCP가 전달되지 않으면 AP에 문제가 있는 것입니다.

5단계. 에지 노드 포트에서 EPC를 수집하여 DHCP 검색 패킷을 확인할 수 있습니다. DHCP 검색 패킷이 표시되지 않으면 AP에 문제가 있는 것입니다.

### SSID가 브로드캐스트되지 않음

1단계. AP 무선 장치가 다운되었는지 확인합니다.

2단계. WLAN이 켜져 있고 브로드캐스트 SSID가 활성화되었는지 확인합니다.

3단계. AP가 패브릭을 사용하는 경우 AP 컨피그레이션을 확인합니다. Configuration(컨피그레이션) > Wireless(무선) > Access Points(액세스 포인트)로 이동하고 한 AP를 선택하고 General(일반) 탭에서 Fabric Status Enabled(패브릭 상태 활성화) 및 RLOC 정보를 볼 수 있습니다.

4단계. Configuration(컨피그레이션) > Wireless(무선) > Fabric(패브릭) > Control Plane(컨트롤 플레인)으로 이동합니다. 컨트롤 플레인이 IP 주소로 구성되어 있는지 확인합니다.

5단계. Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > Policy(정책)로 이동합니다. 정책을 선택하고 Advanced(고급)로 이동합니다. 패브릭 프로파일이 활성화되어 있는지 확인합니다.

6단계. Cisco DNA로 이동하여 Create SSID(SSID 생성) 및 Provision WLC(WLC 프로비저닝)의 [단계를 다시 수행합니다](#). Cisco DNA는 WLC에 SSID를 다시 푸시해야 합니다.

## 관련 정보

- [Cisco 기술 지원 및 다운로드](#)

## 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.