전환 모드로 Enhanced Open SSID 구성 - OWE

목차

소개

이 문서에서는 Catalyst 9800 Wireless LAN Controller(9800 WLC)에서 Enhanced Open with Transition Mode를 구성하고 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco WLC(Wireless Lan Controller) 9800.
- Wi-Fi 6E를 지원하는 Cisco AP(액세스 포인트)
- IEEE 표준 802.11ax.
- 와이어샤크

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- IOS® XE 17.9.3이 포함된 WLC 9800-CL
- AP C9130, C9136, CW9162, CW9164 및 CW9166.
- Wi-Fi 6 클라이언트
  - iPhone SE3rd gen on IOS 16

    - Mac OS 12의 MacBook.
- Wi-Fi 6E 클라이언트
    - Lenovo X1 Carbon Gen11(Intel AX211 Wi-Fi 6 및 6E 어댑터, 드라이버 버전 22.200.2(1).
    - Netgear A8000 Wi-Fi 6 및 6E Adapter with driver v1(0.0.108);
    - Android 13이 있는 휴대폰 픽셀 6a;
    - 휴대 전화 삼성 S23 안드로이드 13.

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.

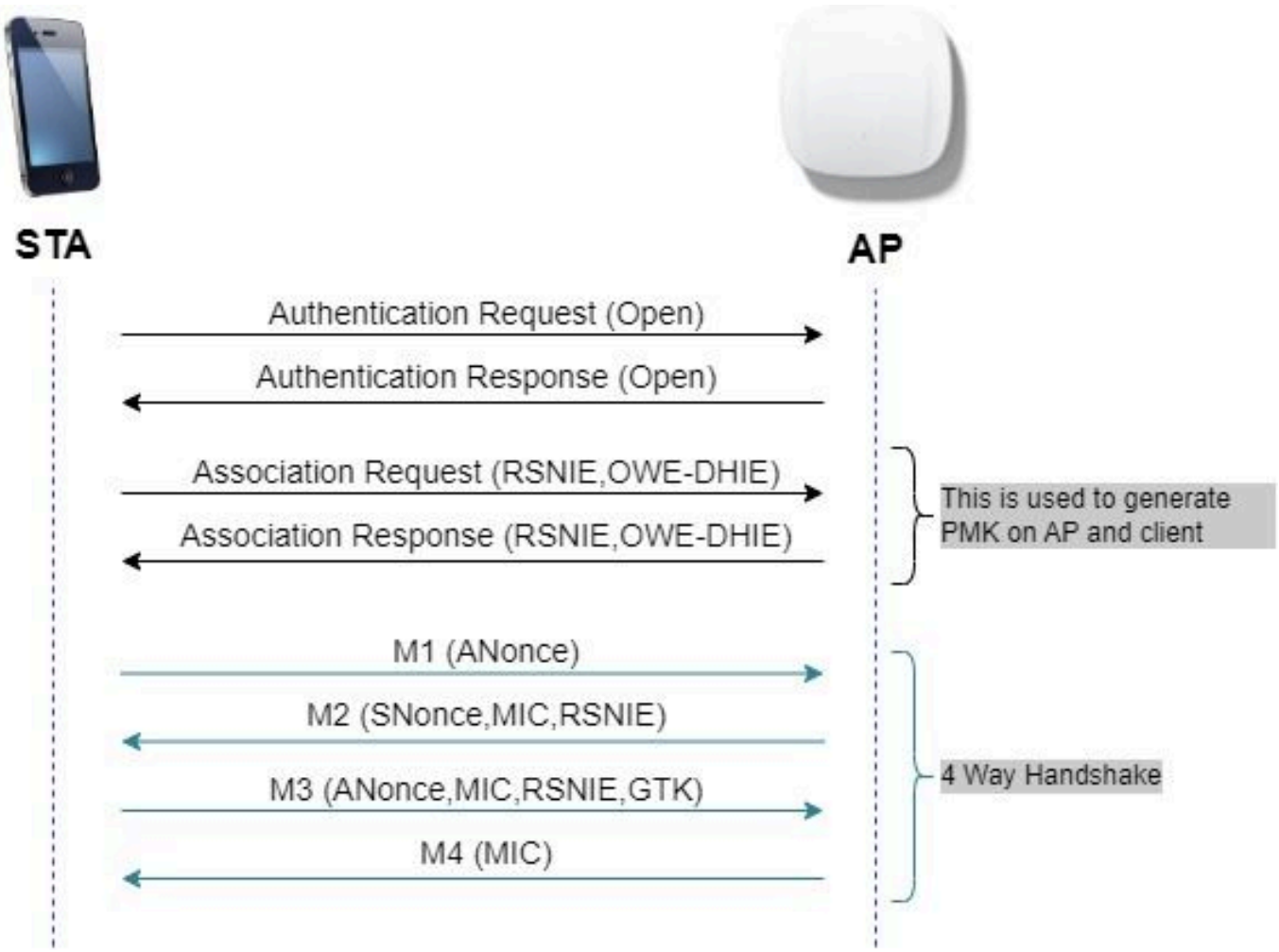
배경 정보

Enhanced Open은 WiFi Alliance에서 WPA3 무선 보안 표준의 일부로 제공하는 인증입니다. 공개(인증되지 않음) 네트워크에서 OWE(Opportunistic Wireless Encryption)를 사용하여 공용 PSK 무선 네트워크에 비해 수동 스니핑을 방지하고 단순한 공격을 방지합니다.

Enhanced Open을 사용하면 클라이언트와 WLC(중앙 인증의 경우) 또는 AP(FlexConnect 로컬 인증의 경우)가 연결 프로세스 중에 Diffie-Hellman 키 교환을 수행하고 4방향 핸드셰이크로 PMK(pairwise master key secret)를 사용합니다.

빌린 돈

OWE(Opportunistic Wireless Encryption)는 IEEE 802.11의 확장으로서 무선 매체(IETF RFC 8110). OWE 기반 인증의 목적은 AP와 클라이언트 간의 개방적이고 안전하지 않은 무선 연결을 피하는 것입니다. OWE는 Cryptography 기반의 Diffie-Hellman 알고리즘을 사용하여 무선 암호화를 설정합니다. OWE를 사용하면 클라이언트와 AP는 액세스 절차 중에 Diffie-Hellman 키 교환을 수행하고 4-way 핸드셰이크로 결과 PMK(pairwise master key) 암호를 사용합니다. OWE를 사용하면 개방형 또는 공유 PSK 기반 네트워크가 구축된 구축에서 무선 네트워크 보안이 향상됩니다.



OWE 프레임 교환

전환 모드

일반적으로 엔터프라이즈 네트워크에는 암호화되지 않은 게스트 SSID가 하나만 있으며, 향상된 개방형 클라이언트를 지원하지 않는 이전 클라이언트와 향상된 개방형 클라이언트가 공존하는 최신 클라이언트가 모두 있는 것을 선호합니다. 전환 모드는 이 시나리오에 맞게 특별히 도입되었습니다 .

이를 위해서는 2개의 SSID(WISE를 지원하는 숨겨진 SSID 1개 및 Open이며 브로드캐스트되는 두 번째 SSID)를 구성해야 합니다.

OWY(Opportunistic Wireless Encryption) 전환 모드에서는 OWY 및 비 OWY STA가 동일한 SSID에 동시에 연결할 수 있습니다. 모든 OWE STA가 OWE 전환 모드에서 SSID를 볼 경우 OWE에 연결됩니다.

개방형 WLAN과 OWE WLAN 전송 비콘 프레임 모두 WISE WLAN의 비콘 및 프로브 응답 프레임에는 개방형 WLAN의 BSSID 및 SSID를 캡슐화하기 위한 Wi-Fi Alliance 벤더 IE가 포함되며, 마찬가지로 개방형 WLAN에도 WISE WLAN을 포함합니다.

Owe STA는 OWE 전환 모드에서 동작하는 OWE AP의 오픈 BSS의 SSID를 가용 네트워크의 리스트에서 사용자에게 표시해야 하며, 그 OWE AP의 OWE BSS SSID의 표시를 억제해야 한다.

지침 및 제한:

- 개방 수준을 높이려면 WPA3 전용 정책이 필요합니다. WPA3은 Cisco Wave 1(Cisco IOS® 기반) AP에서 지원되지 않습니다.
- PMF(Protected Management Frame)를 Required(필수)로 설정해야 합니다. 이 설정은 기본적으로 WPA3 전용 레이어 2 보안으로 설정됩니다.
- Enhanced Open은 Enhanced Open을 지원하는 최신 버전을 실행하는 최종 클라이언트에서만 작동합니다.

구성

관리자가 Enhanced Open을 구성하려 하지만 이전 클라이언트가 게스트 SSID에 연결할 수 있도록 허용하는 일반적인 활용 사례입니다.

네트워크 다이어그램

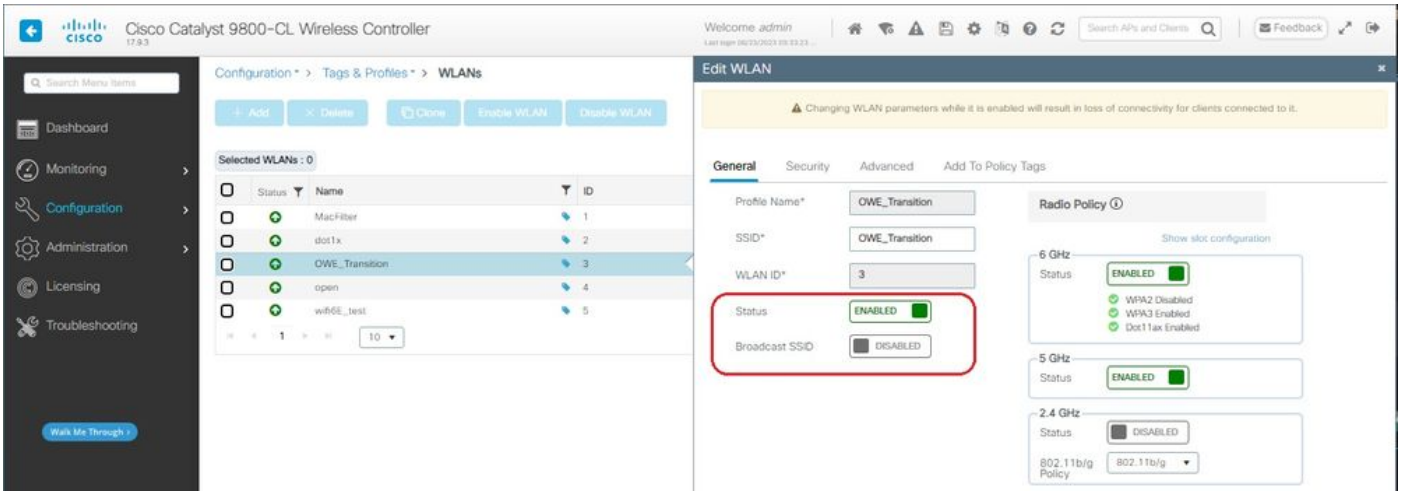
네트워크 토폴로지

GUI 구성 단계:

첫 번째 SSID를 생성합니다. 이를 "OWE_Transition"이라고 합니다. 이 예에서는 WLAN ID 3을 입력하고 "Broadcast SSID"(브로드캐스트 SSID) 옵션이 비활성화된 상태로 숨겨져 있는지 확인합니다.

1단계 Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > WLANs(WLAN)를 선택하여 WLANs 페이지를 엽니다.

2단계 Add(추가)를 클릭하여 새 WLAN을 추가하고 > WLAN 이름 "WISE_Transition"을 추가하고 > Status(상태)를 Enable(활성화)로 변경하고 > Broadcast SSID(브로드캐스트 SSID)가 Disabled(비활성화됨)로 설정되었는지 확인합니다.



OWE Transition 확장 개방형 SSID 숨김

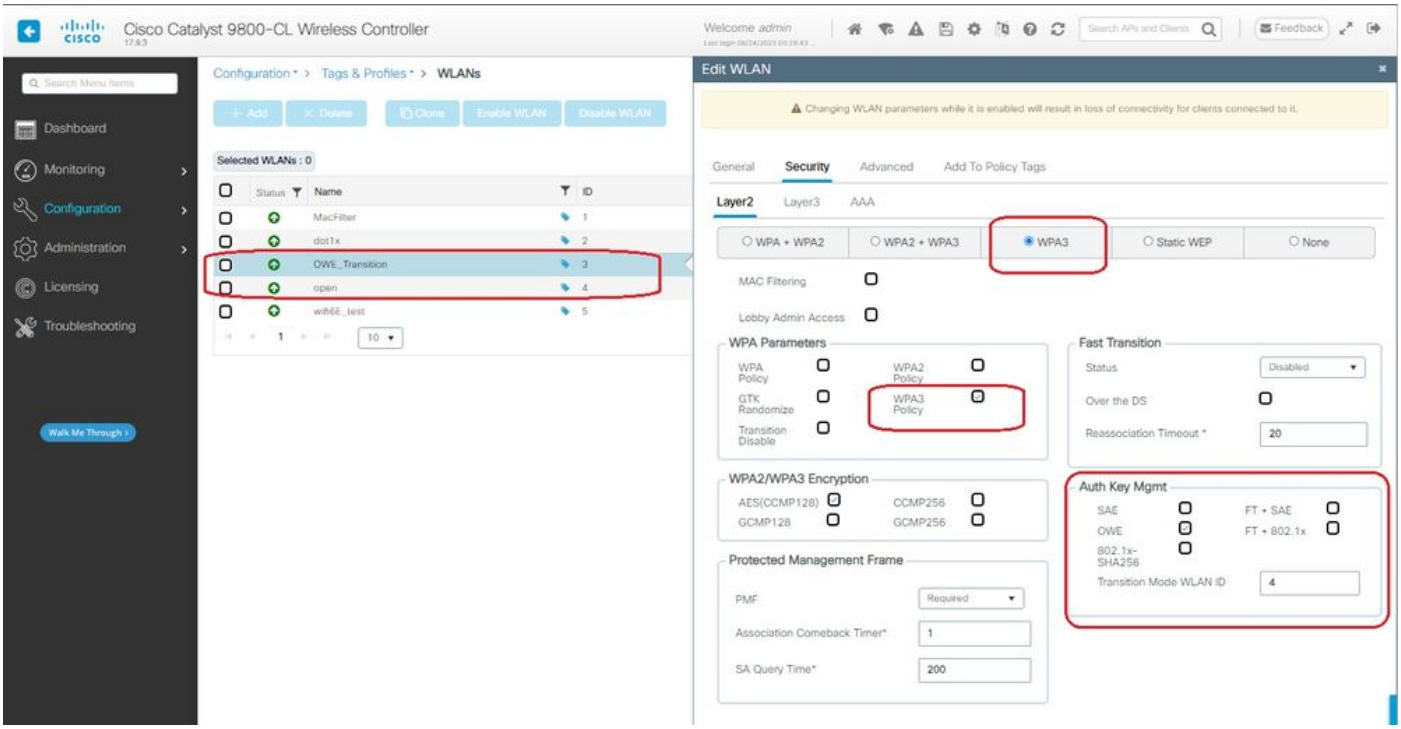
3단계 Security(보안) > Layer 2(레이어 2) 탭 > Select WPA3(WPA3 선택)를 선택합니다.

4단계 PMF(Protected Management Frame)를 Required(필수)로 설정합니다.

5단계 WPA Parameters(WPA 매개변수) > WPA3 Policy(WPA3 정책)를 선택합니다. AES(CCMP128) Encryption and OWE Auth Key Management를 선택합니다.

6단계 Add WLAN ID 4 (open WLAN) to "Transition Mode WLAN ID(WLAN 열기)"(WLAN ID 4(WLAN ID)를 추가합니다.

7단계 Apply to Device(디바이스에 적용)를 클릭합니다.

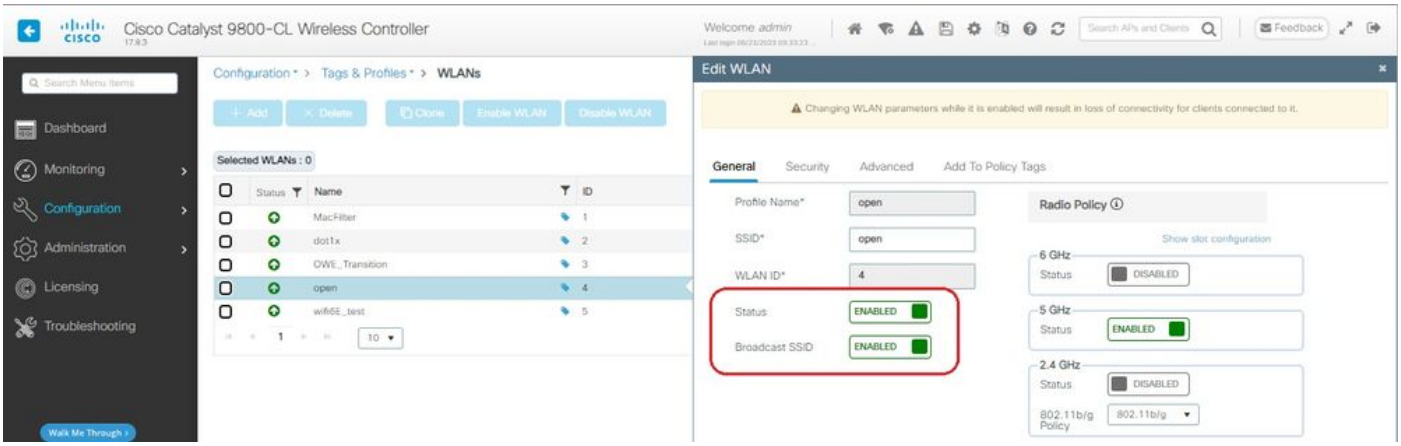


OWE 전환 모드 - OWE SSID

두 번째 SSID를 생성하고 이 예에서는 WLAN ID 4에서 "open"이라고 부르며 "Broadcast SSID"를 활성화해야 합니다.

1단계 Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > WLANs(WLAN)를 선택하여 WLANs 페이지를 엽니다.

2단계 Add(추가)를 클릭하여 새 WLAN을 추가하고 > WLAN 이름 "open(열기)"을 추가하고 > Status(상태)를 Enable(활성화)로 변경하고 > Broadcast SSID(브로드캐스트 SSID)가 Enabled(활성화됨)인지 확인합니다.

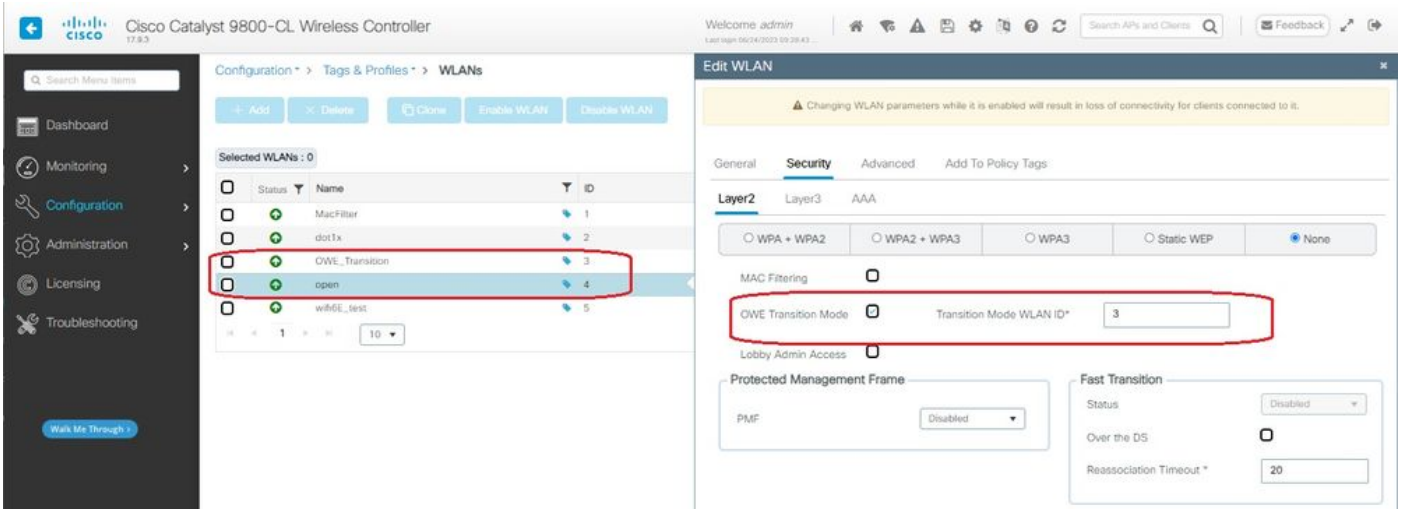


OWE 전환 오픈 SSID

3단계 Security(보안) > Layer 2(레이어 2) 탭 > Choose None(없음)을 선택합니다.

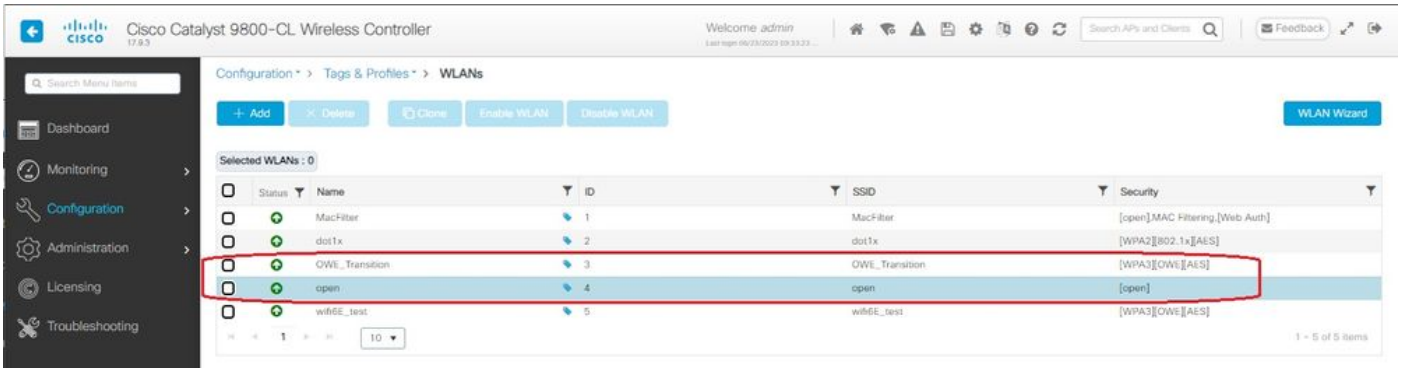
4단계 "Transition Mode WLAN ID(전환 모드 WLAN ID)" 상자에 WLAN ID 4(OWE_Transition)를 추가합니다.

5단계 Apply to Device(디바이스에 적용)를 클릭합니다.



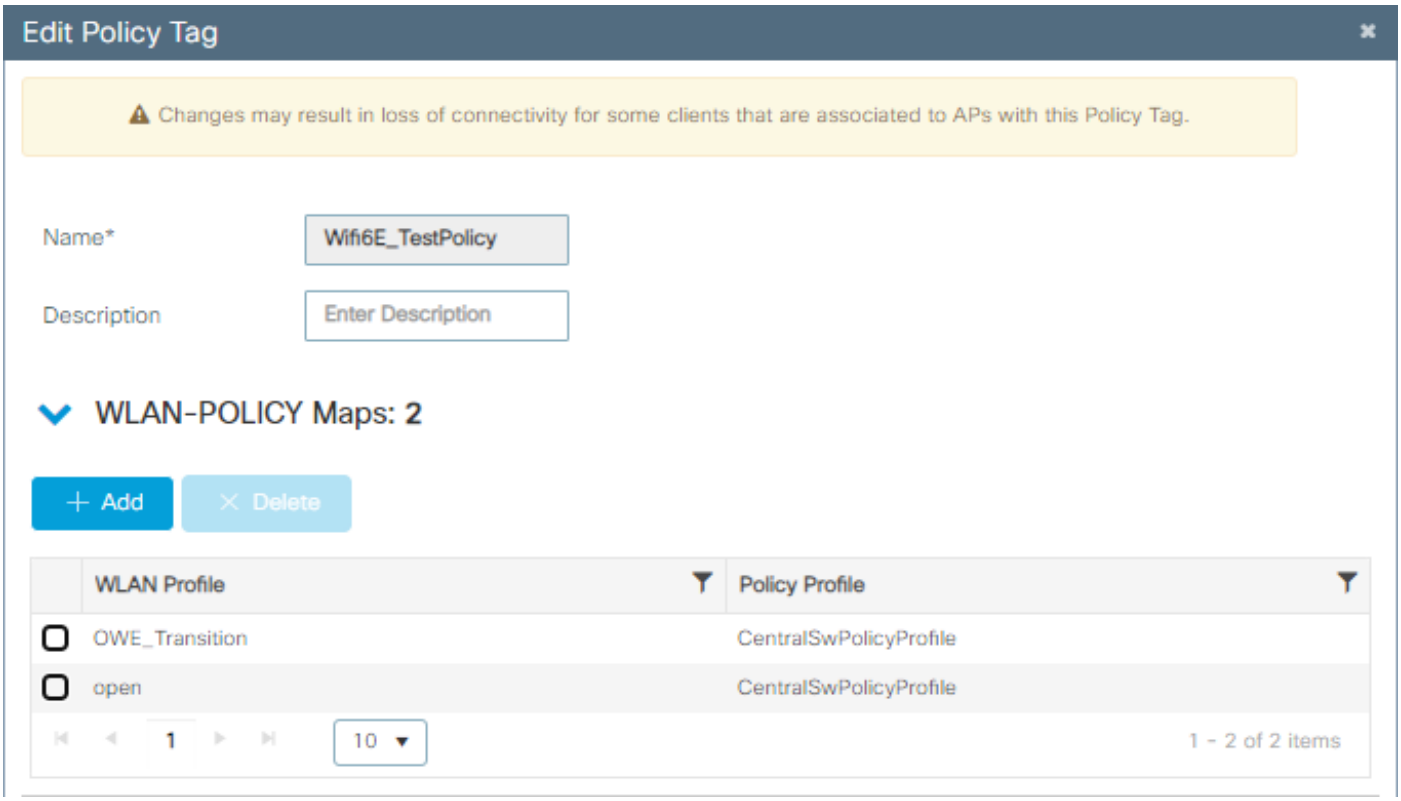
OWE 전환 모드 개방형 *WLAN* 보안

이 스크린샷은 최종 결과를 보여줍니다. 한 WLAN은 "OWE_Transition"이라는 이름의 WPA3+OWE+WPA3에 대해 보안 및 구성되어 있고 다른 하나는 "open"이라는 이름의 완전 개방형 SSID입니다. "open"이라는 완전 개방형 SSID만 비콘에서 SSID를 브로드캐스트하지만 "OWE_Transition"은 숨겨집니다.



OWE 전환 모드 WLAN

6단계 생성한 WLAN을 원하는 정책 프로파일에 매핑하여 AP에 적용합니다.



정책 태그

CLI에 대해 구성:

향상된 개방형 SSID:

```
Device# conf t
Device(config)# wlan OWE_Transition 3 OWE_Transition
Device(config)# no broadcast-ssid
Device(config)# no security ft adaptive
Device(config)# no security wpa wpa2
Device(config)# no security wpa akm dot1x
Device(config)# security wpa akm owe
Device(config)# security wpa transition-mode-wlan-id 4
Device(config)# security wpa wpa3
Device(config)# security pmf mandatory
Device(config)# no shutdown
```

개방형 SSID:

```
Device# conf t
Device(config)# wlan open 4 open
Device(config)# no security ft adaptive
Device(config)# no security wpa
Device(config)# no security wpa wpa2
Device(config)# no security wpa wpa2 ciphers aes
Device(config)# no security wpa akm dot1x
Device(config)# security wpa transition-mode-wlan-id 3
Device(config)# no shutdown
```

정책 프로필:

```
Device(config)# wireless tag policy Wifi6E_TestPolicy
Device(config-policy-tag)# wlan open policy CentralSwPolicyProfile
Device(config-policy-tag)# wlan OWE_Transition policy CentralSwPolicyProfile
```

다음을 확인합니다.

이것은 검증 섹션입니다.

CLI에서 WLAN 컨피그레이션을 확인합니다.

<#root>

```
Device#show wlan id 3
WLAN Profile Name : OWE_Transition
==================================================

Identifier : 3

Description :

Network Name (SSID) : OWE_Transition

Status : Enabled

Broadcast SSID : Disabled

[...]
Security

802.11 Authentication : Open System

Static WEP Keys : Disabled

Wi-Fi Protected Access (WPA/WPA2/WPA3) : Enabled

WPA (SSN IE) : Disabled
WPA2 (RSN IE) : Disabled

WPA3 (WPA3 IE) : Enabled

AES Cipher : Enabled

CCMP256 Cipher : Disabled
GCMP128 Cipher : Disabled
GCMP256 Cipher : Disabled
Auth Key Management
802.1x : Disabled
PSK : Disabled
```

```
CCKM : Disabled
FT dot1x : Disabled
FT PSK : Disabled
FT SAE : Disabled
Dot1x-SHA256 : Disabled
PSK-SHA256 : Disabled
SAE : Disabled
```

OWE : Enabled

```
SUITEB-1X : Disabled
SUITEB192-1X : Disabled
SAE PWE Method : Hash to Element, Hunting and Pecking(H2E-HNP)
```

Transition Disable : Disabled

```
CCKM TSF Tolerance (msecs) : 1000
```

OWE Transition Mode : Enabled

OWE Transition Mode WLAN ID : 4

```
OSEN : Disabled
FT Support : Disabled
FT Reassociation Timeout (secs) : 20
FT Over-The-DS mode : Disabled
```

PMF Support : Required

```
PMF Association Comeback Timeout (secs): 1
PMF SA Query Time (msecs) : 200
[...]
#show wlan id 4
WLAN Profile Name : open
==================================================
```

Identifier : 4

```
Description :
```

Network Name (SSID) : open

Status : Enabled

Broadcast SSID : Enabled

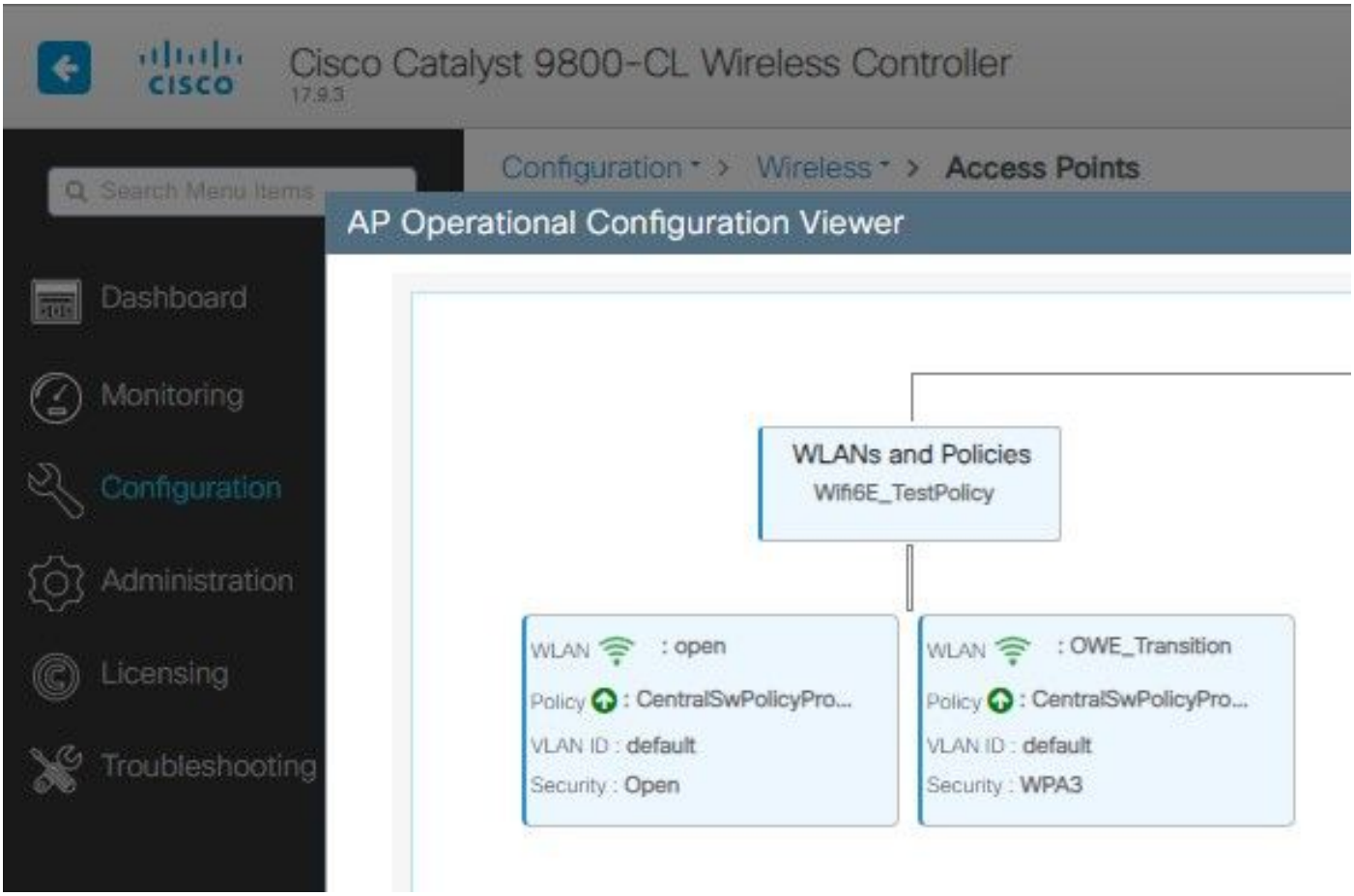
```
[...]
Security
802.11 Authentication : Open System
Static WEP Keys : Disabled
```

Wi-Fi Protected Access (WPA/WPA2/WPA3) : Disabled

OWE Transition Mode : Enabled

```
OWE Transition Mode WLAN ID : 3


OSEN : Disabled
FT Support : Disabled
FT Reassociation Timeout (secs) : 20
FT Over-The-DS mode : Disabled

PMF Support : Disabled


PMF Association Comeback Timeout (secs): 1
PMF SA Query Time (msecs) : 200
[...]
```

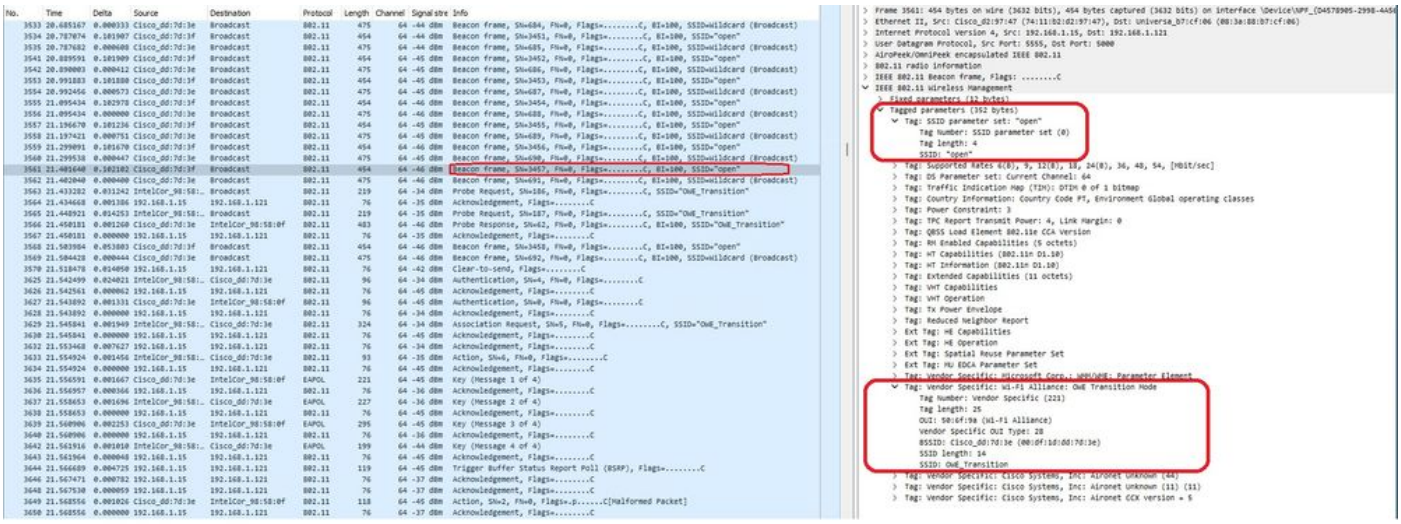
WLC에서 AP 컨피그레이션으로 이동하여 두 WLAN이 모두 AP에서 활성 상태인지 확인할 수 있습니다.



OWE 전환 모드 AP 작동 구성 뷰어

활성화된 경우 AP는 Open SSID를 가진 비컨만 수행하지만 WISE IE(Transition Mode Information Element)를 전달합니다. Enhanced Open을 지원하는 클라이언트가 이 SSID에 연결되면 WISE를 자동으로 사용하여 모든 트래픽 포스트 연결을 암호화합니다.

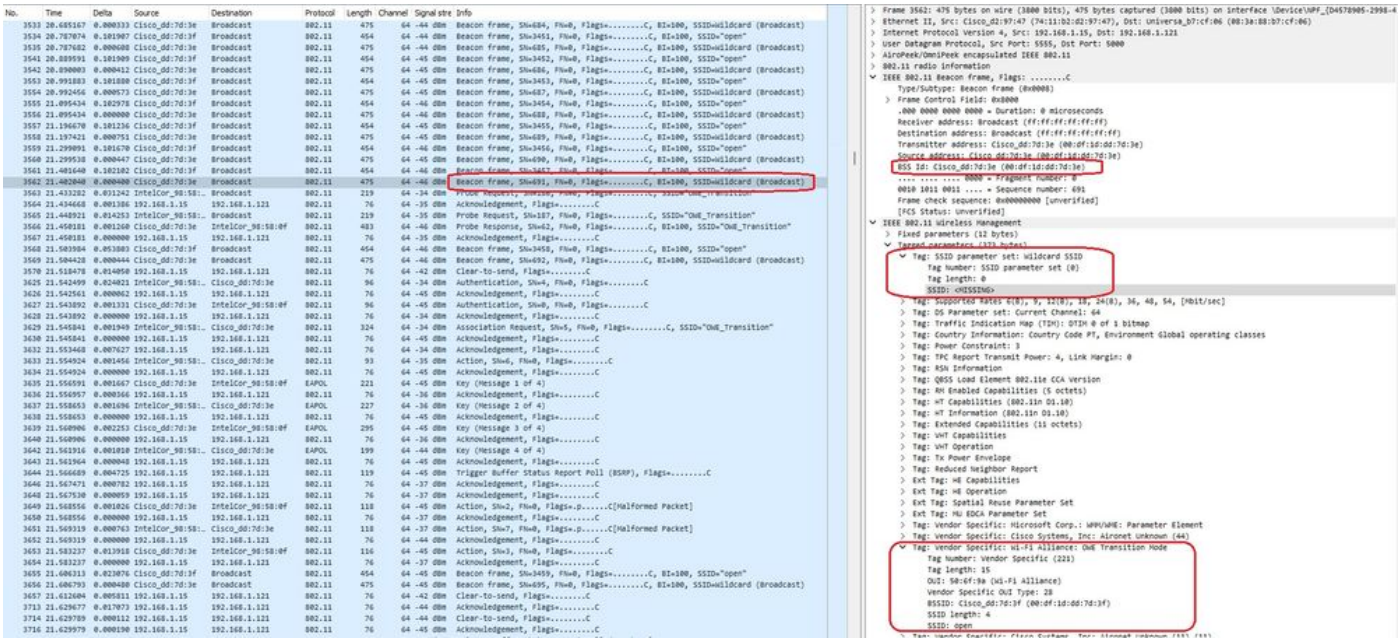
OTA(Over the Air)를 통해 관찰할 수 있는 내용은 다음과 같습니다.



OWE Transition Open SSID 비컨

SSID가 "open"인 비콘 전송에는 BSSID 및 SSID 이름 "WISE_Transition"과 같은 고급 개방형 SSID 세부사항이 포함된 WISE 전환 모드 IE가 포함됩니다.

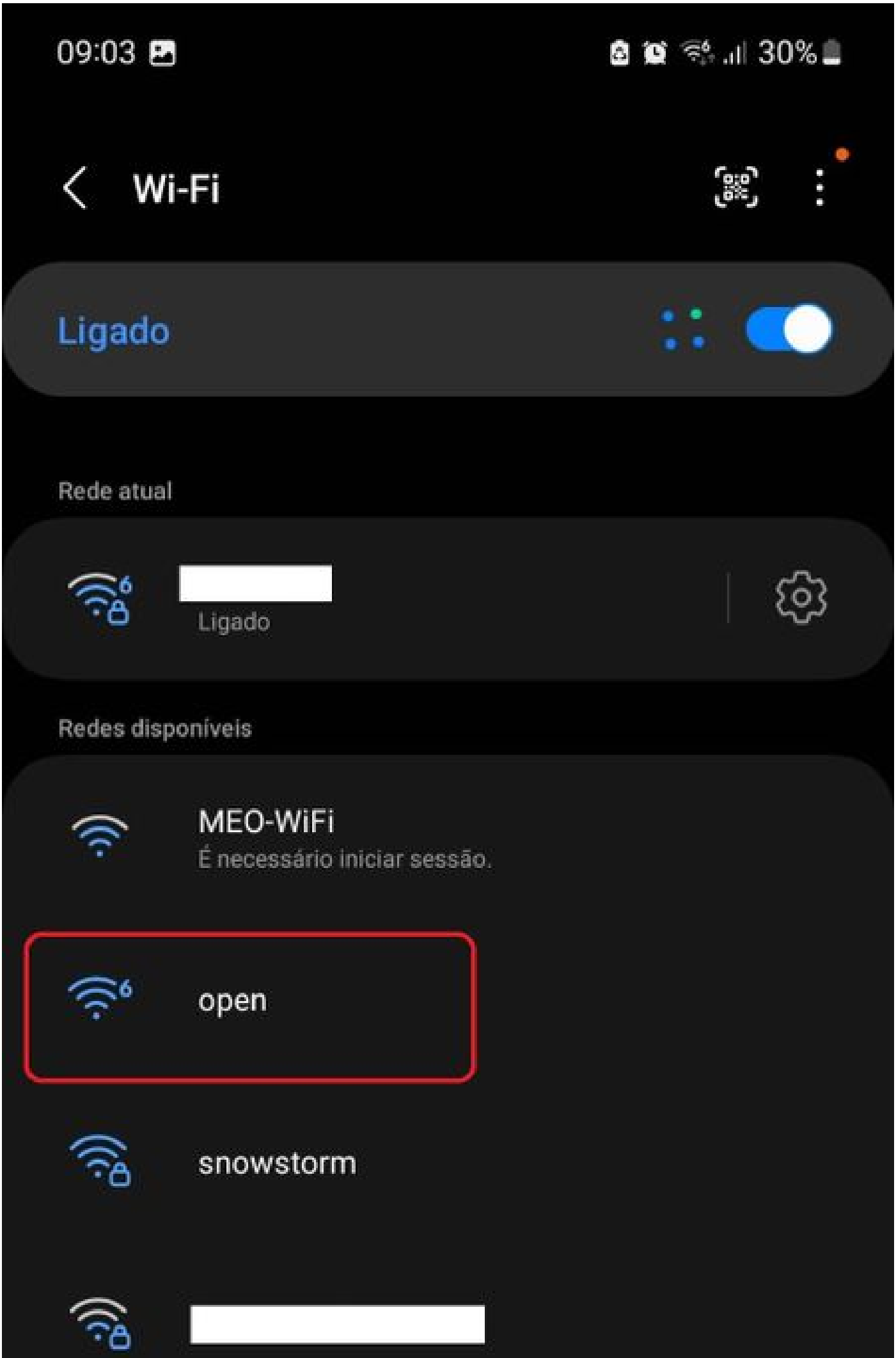
또한 SSID가 숨겨진 비콘 OTA가 있으며 bssid로 필터링하면 프레임이 BSSID 00:df:1d:dd:7d:3e로 전송됩니다. 이는 WISE 전환 모드 IE 내의 BSSID입니다.



웨인 비콘

또한 WISE 숨겨진 비콘에는 개방형 ssid BSSID 및 SSID 이름 "open"을 사용하는 WISE 전환 모드 IE가 포함되어 있습니다.

이러한 스크린샷은 Enhanced Open을 지원하는 Android 전화기를 보여줍니다. 잠금 아이콘이 없는 열린 SSID만 표시하지만(잠금 아이콘은 사용자가 암호를 사용하여 연결해야 한다고 믿게 함), 일단 연결되면 보안이 Enhanced Open 보안이 사용됨을 보여줍니다.


09:03
30%
Wi-Fi
Ligado
Rede atual
Ligado
Redes disponíveis
MEO-WiFi
É necessário iniciar sessão.
open
snowstorm

```
Client MAC Address : 286b.3598.580f
[...]
AP Name: AP9136_5C.F524
AP slot : 1
Client State : Associated
Policy Profile : CentralSwPolicyProfile
Flex Profile : N/A
Wireless LAN Id: 3
```

WLAN Profile Name: OWE_Transition

Wireless LAN Network Name (SSID): OWE_Transition

```
BSSID : 00df.1ddd.7d3e
Connected For : 682 seconds
Protocol : 802.11ax - 5 GHz
Channel : 64
Client IIF-ID : 0xa0000003
Association Id : 2
```

Authentication Algorithm : Open System

```
Idle state timeout : N/A
[...]
```

Policy Type : WPA3

Encryption Cipher : CCMP (AES)

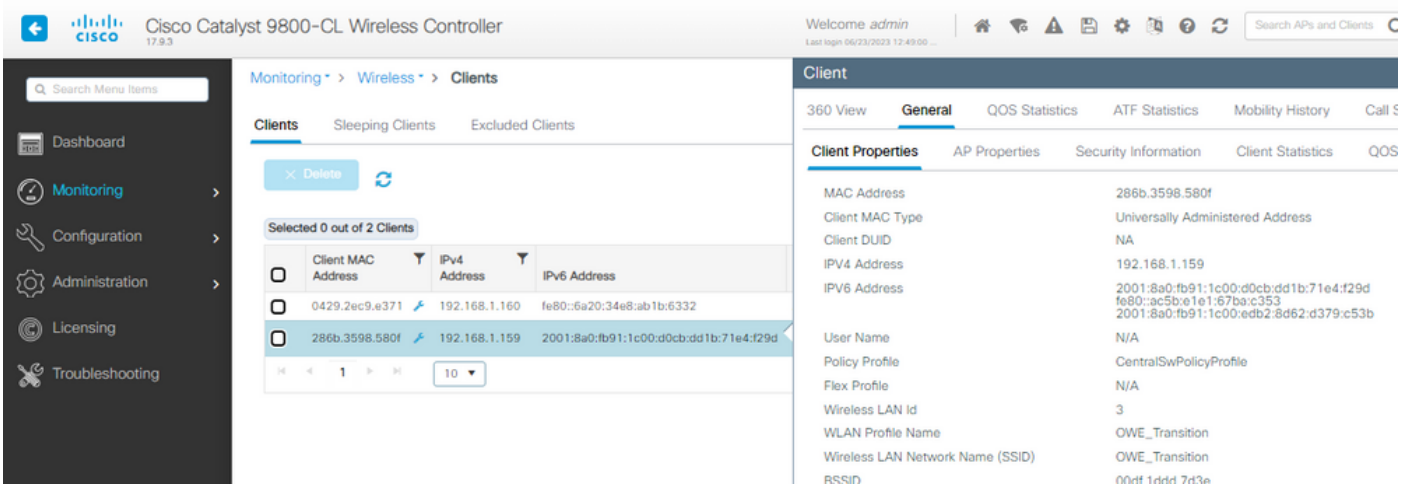
Authentication Key Management : OWE

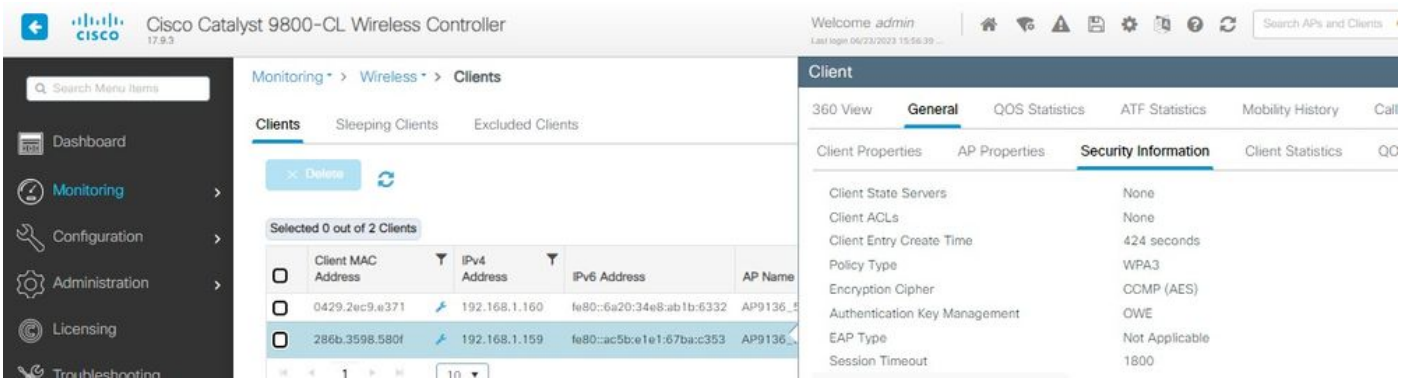
```
Transition Disable Bitmap : None
User Defined (Private) Network : Disabled
User Defined (Private) Network Drop Unicast : Disabled
Encrypted Traffic Analytics : No
```

Protected Management Frame - 802.11w : Yes

```
EAP Type : Not Applicable
```

또한 WLC GUI에서도 동일한 내용을 관찰할 수 있습니다.





Enhanced Open을 지원하지 않는 클라이언트의 경우 암호화 없이 열린 SSID만 보고 연결합니다.

여기에 나와 있는 것처럼, 이러한 클라이언트는 Enhanced Open(각각 IOS 15의 iPhone 및 Mac OS 12의 MacBook)을 지원하지 않으며 개방형 게스트 SSID만 표시하고 암호화를 사용하지 않는 클라이언트입니다.


Proximus
17:04
Settings
Wi-Fi
Wi-Fi
open
Unsecured Network
MY NETWORKS
[redacted]
OTHER NETWORKS
apr0v0
[redacted]
Other...
Ask to Join Networks
Notify

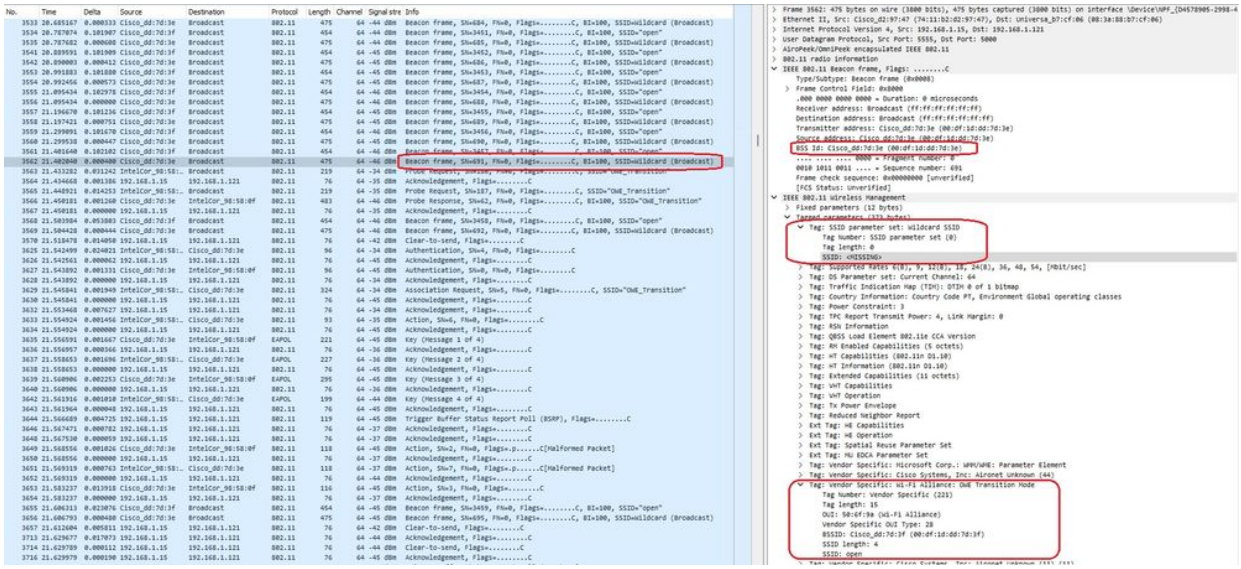
```
Client MAC Address : b44b.d623.a199
[...]
AP Name: AP9136_5C.F524
AP slot : 1
Client State : Associated
Policy Profile : CentralSwPolicyProfile
Flex Profile : N/A

Wireless LAN Id: 4


WLAN Profile Name: open


Wireless LAN Network Name (SSID): open


BSSID : 00df.1ddd.7d3f
[...]

Authentication Algorithm : Open System


[...]

Protected Management Frame - 802.11w : No


EAP Type : Not Applicable
```

문제 해결

1. 모든 클라이언트가 지원하는 것은 아니지만 클라이언트가 WISE를 지원하는지 확인합니다. 클라이언트 공급업체 문서를 확인하십시오. 예를 들어, Apple은 여기서 해당 장치에 대한 지원을 문서화했습니다.
2. 일부 이전 클라이언트는 WISE 전환 모드 IE가 있고 범위에 있는 네트워크에 SSID가 없기 때문에 Open ssid 비컨을 수락하지 않을 수도 있습니다. 클라이언트에서 Open SSID를 볼 수 없는 경우 WLAN 컨피그레이션에서 Transition VLAN(0으로 설정)을 제거하고 WLAN이 표시되는지 확인합니다.
3. 클라이언트에서 개방형 SSID, 지원 OWE를 확인하지만 여전히 WPA3 없이 연결하는 경우 전환 VLAN ID가 올바르고 두 WLAN의 신호에서 브로드캐스트되고 있는지 확인합니다. 스니퍼 모드에서 AP를 사용하여 OTA 트래픽을 캡처할 수 있습니다. 스니퍼 모드의 AP를 구성하려면 다음 단계를 실행하십시오. 스니퍼 모드의 APs Catalyst 91xx.
    - SSID "open"을 사용하여 비컨이 전송되며, BSSID 및 SSID 이름 "WISE_Transition"과 같은 고급 개방형 SSID 세부사항이 포함된 WISE 전환 모드 IE가 포함됩니다. 

      OWE Transition Open SSID 비컨

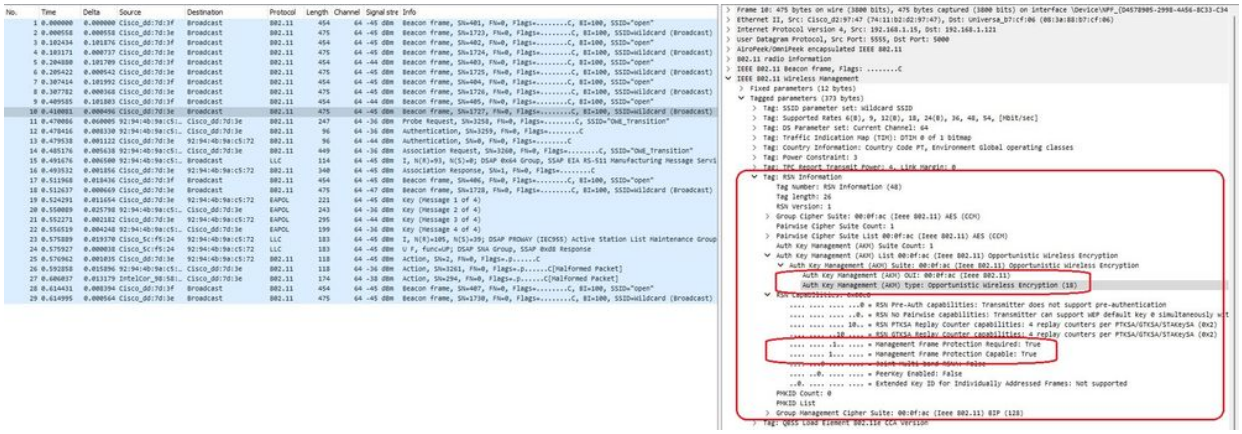
    - 또한 SSID가 숨겨진 비콘 OTA가 있으며 bssid로 필터링하면 프레임이 BSSID 00:df:1d:dd:7d:3e로 전송됩니다. 이는 WISE 전환 모드 IE 내의 BSSID입니다.



웨인 비콘

또한 WISE 숨겨진 비콘에는 개방형 ssid BSSID 및 SSID 이름 "open"을 사용하는 WISE 전환 모드 IE가 포함되어 있습니다.

- AKM 정보를 확인하고 MFP가 Required and Capable로 광고되는지 확인할 수도 있습니다.



웨인 비콘 AKM

4. 클라이언트 mac 주소 및 y를 기반으로 RadioActive 추적 수집다음과 유사한 로그가 표시됩니다.

2023/06/23 15:08:58.567933 {wncd_x_R0-0}{1}: [client-keymgmt] [14854]: (note): MAC: xxxx.xxxx.xxxx EAP Key management successful. AKM:OWE Cipher:CCMP WPA Version: WPA3

2023/06/23 15:10:06.971651 {wncd_x_R0-0}{1}: [client-orch-state] [14854]: (note): MAC: xxxx.xxxx.xxxx Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_RUN

참조

Wi-Fi 6E란?

Wi-Fi 6과 Wi-Fi 6E의 비교

Wi-Fi 6E 한눈에 보기

Wi-Fi 6E: Wi-Fi 백서의 다음 장

Cisco Catalyst 9800 Series Wireless Controller 소프트웨어 컨피그레이션 가이드 17.9.x

WPA3 구축 가이드

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.