Wi-Fi 6E WLAN Layer 2 보안 구성 및 확인

목차

소개

이 문서에서는 Wi-Fi 6E WLAN Layer 2 보안을 구성하는 방법 및 여러 클라이언트에서 예상되는 사항에 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.
- 도구: Wireshark v4.0.6

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- IOS® XE 17.9.3이 포함된 WLC 9800-CL
- AP C9136, CW9162, CW9164 및 CW9166.
- 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

Wi-Fi 6E는 완전히 새로운 표준이 아니라 확장형이라는 것을 알아야 합니다. Wi-Fi 6E는 기본적으로 Wi-Fi 6(802.11ax) 무선 표준을 6GHz 무선 주파수 대역으로 확장한 것입니다.

Wi-Fi 6E는 최신 Wi-Fi 표준인 Wi-Fi 6를 기반으로 구축되지만, Wi-Fi 6E 장치 및 애플리케이션만 6GHz 대역에서 작동할 수 있습니다.

Wi-Fi 6E 보안

Wi-Fi 6E는 Wi-Fi Protected Access 3(WPA3) 및 Opportunistic Wireless Encryption(WISE)으로 보안을 제공하며 개방형 및 WPA2 보안과 역호환성이 없습니다.

이제 Wi-Fi 6E 인증에 WPA3 및 향상된 개방 보안이 필수이며 Wi-Fi 6E에도 AP 및 클라이언트에서 PMF(Protected Management Frame)가 필요합니다.

6GHz SSID를 구성할 때 다음과 같은 특정 보안 요구 사항을 충족해야 합니다.

- WISE, SAE 또는 802.1x-SHA256을 사용하는 WPA3 L2 보안
- 보호된 관리 프레임 사용;
- 다른 L2 보안 방법은 허용되지 않습니다. 즉 혼합 모드가 가능하지 않습니다.

WPA3

WPA3은 WPA2보다 우수한 인증을 활성화하여 Wi-Fi 보안을 개선하고 암호화 강도를 높이며 중요 네트워크의 복원력을 향상시킵니다.

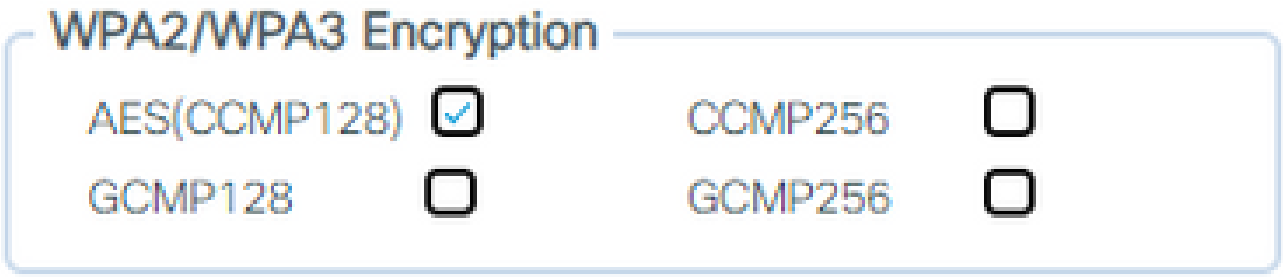
WPA3의 주요 기능은 다음과 같습니다.

- PMF(Protected Management Frame)는 유니캐스트 및 브로드캐스트 관리 프레임을 보호하고 유니캐스트 관리 프레임을 암호화합니다. 즉, 무선 침입 탐지 및 무선 침입 방지 시스템 snow는 클라이언트 정책을 적용하는 무차별 대입(brute-force) 방식이 적습니다.
- SAE(Simultaneous Authentication of Equals)는 비밀번호 기반 인증 및 키 합의 메커니즘을 활성화합니다. 이는 무차별 대입 공격으로부터 보호합니다.
- 전환 모드는 WPA2를 사용하여 WPA3을 지원하지 않는 클라이언트를 연결하는 혼합 모드입니다.

WPA3은 지속적인 보안 개발 및 적합성과 상호 운용성에 관한 것입니다.
WPA3(WPA2와 동일)을 지정하는 정보 요소가 없습니다. WPA3은 AKM/암호 그룹/PMF 조합으로 정의됩니다.

9800 WLAN 컨피그레이션에서는 4개의 서로 다른 WPA3 암호화 알고리즘을 사용할 수 있습니다.

이는 GCMP(Galois/Counter Mode Protocol) 및 CCMP(Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)를 기반으로 합니다. AES(CCMP128), CCMP256, GCMP128 및 GCMP256:

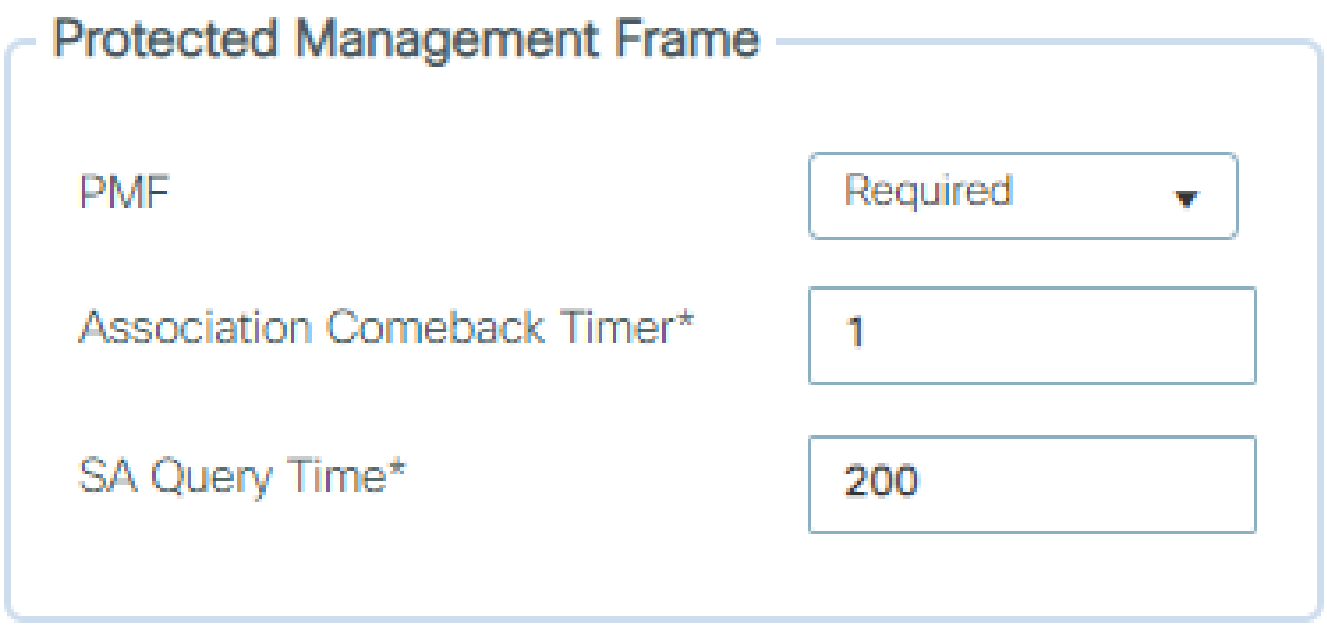


WPA2/3 암호화 옵션

PMF

PMF를 활성화하면 WLAN에서 PMF가 활성화됩니다.

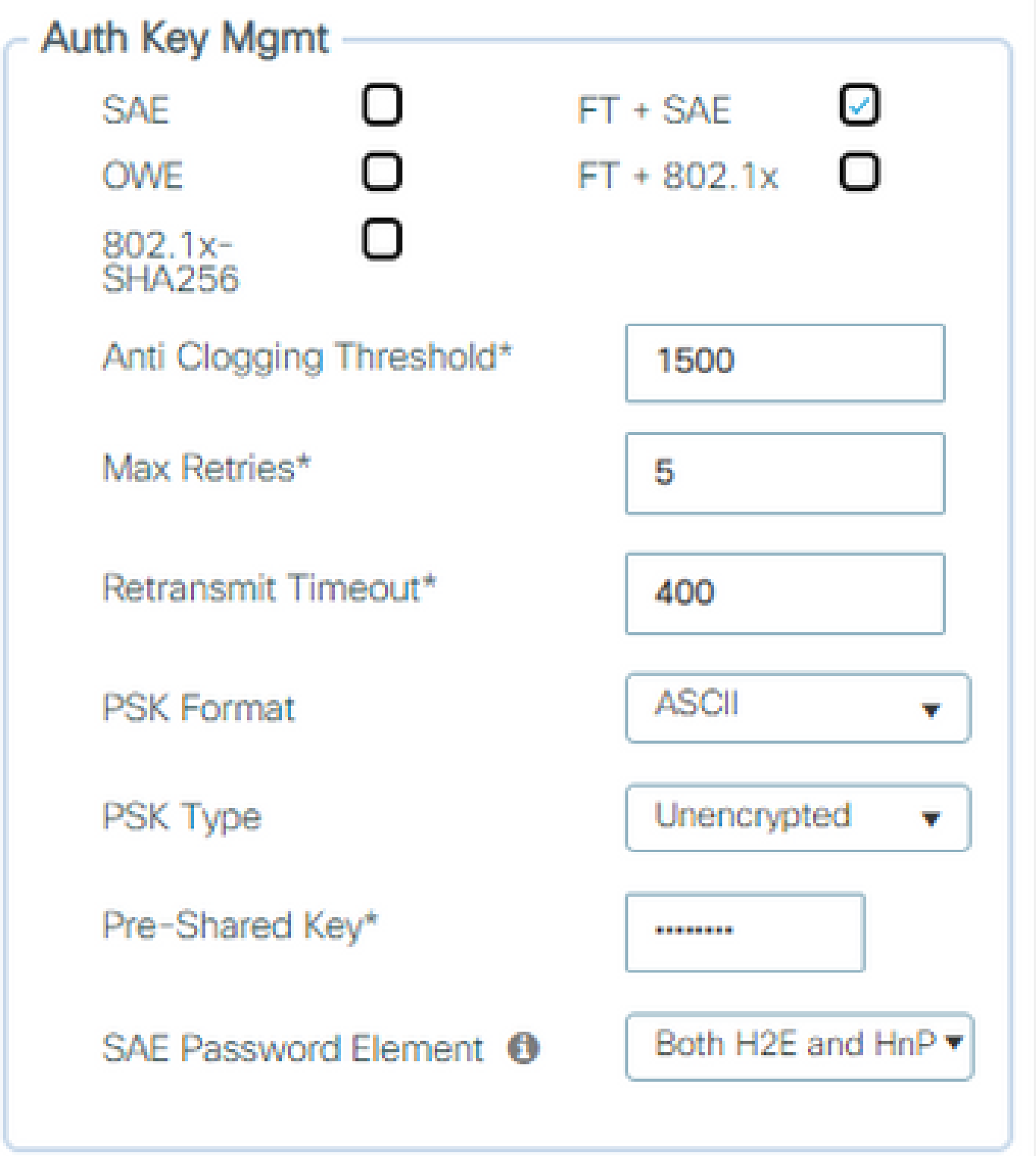
기본적으로 802.11 관리 프레임은 인증되지 않으므로 스푸핑으로부터 보호되지 않습니다. MFP(Infrastructure Management Protection Frame) 및 802.11w PMF(Protected Management Frame)는 이러한 공격을 차단합니다.



PMF 옵션

인증 키 관리

다음은 17.9.x 버전에서 사용할 수 있는 AKM 옵션입니다.

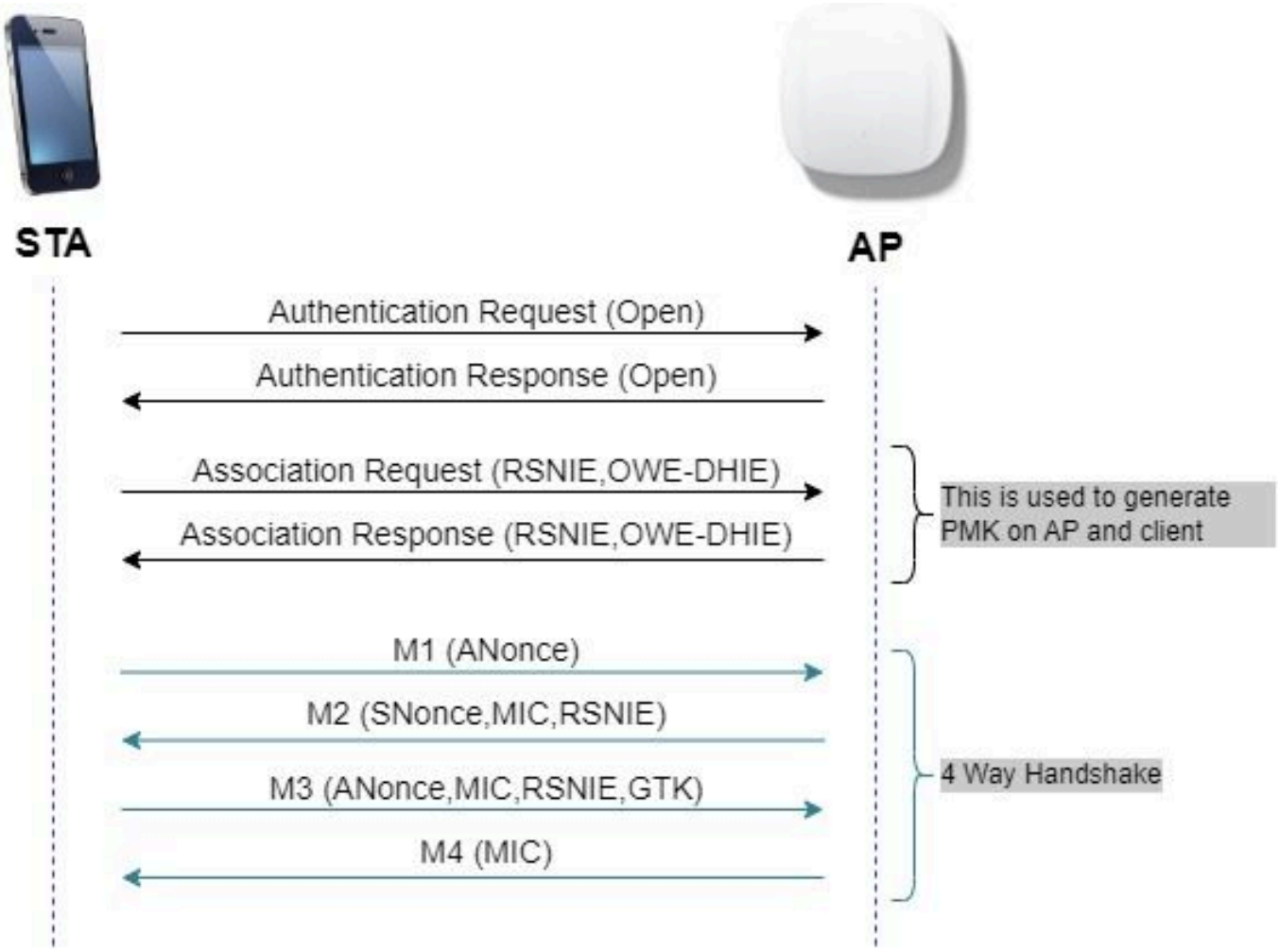


AKM 옵션

빌린 돈

OWE(Opportunistic Wireless Encryption)는 무선 미디어(IETF RFC 8110)의 암호화를 제공하는 IEEE 802.11의 확장입니다. 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 보안

이 향상됩니다.



OWE 프레임 교환

새우

WPA3은 Simultaneous Authentication of Equals라는 새로운 인증 및 키 관리 메커니즘을 사용합니다. 이 메커니즘은 SAE H2E(Hash-to-Element)를 사용하여 더욱 향상됩니다.

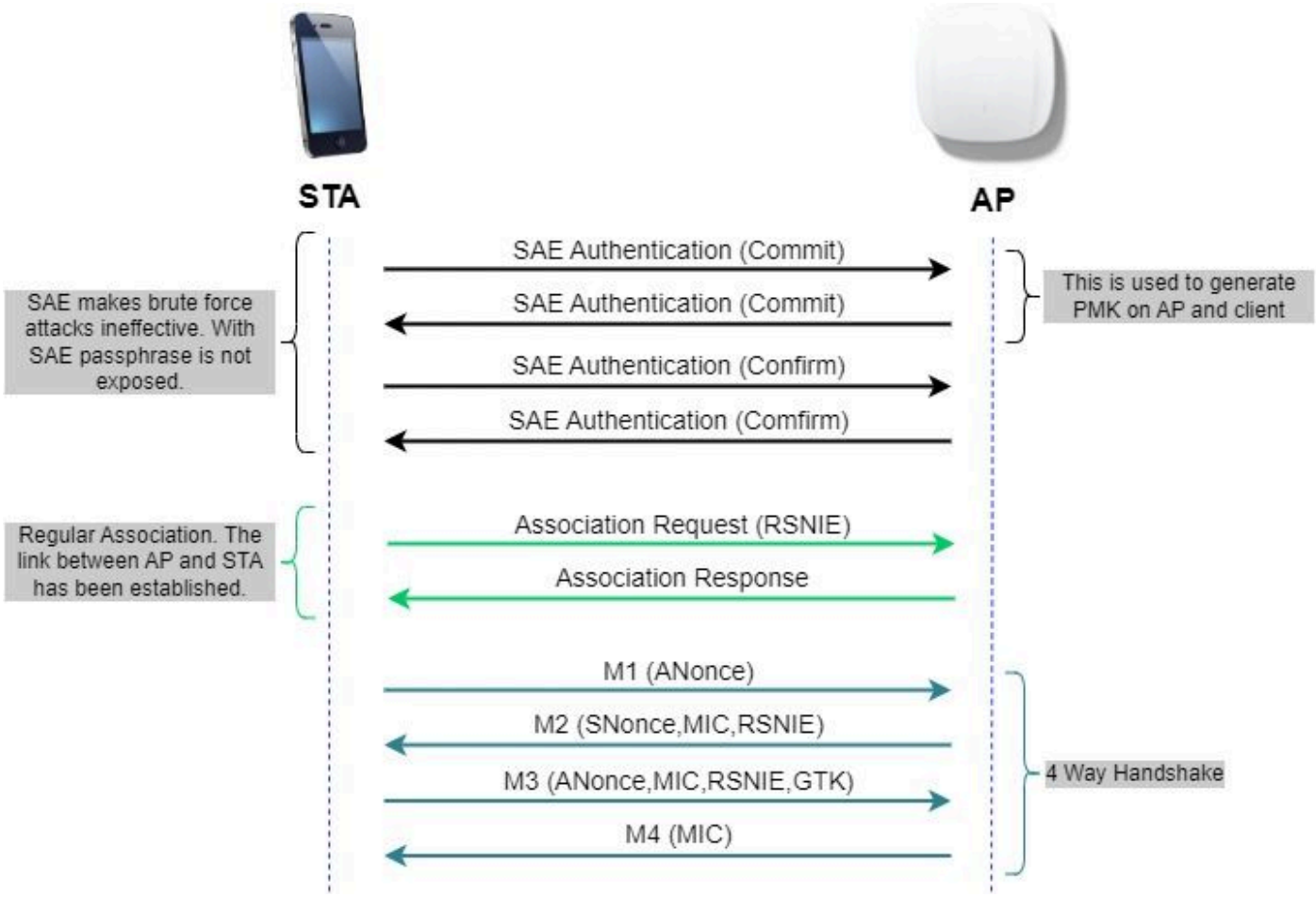
WPA3 및 Wi-Fi 6E에서는 H2E를 사용하는 SAE가 필수입니다.

SAE는 이산 로그 암호화를 사용하여 오프라인 사전 공격에 강할 수 있는 비밀번호를 사용하여 상호 인증을 수행하는 방식으로 효율적인 교환을 수행합니다.

오프라인 사전 공격은 공격자가 추가 네트워크 상호작용 없이 가능한 비밀번호를 시도하여 네트워크 비밀번호를 확인하려고 시도하는 것입니다.

클라이언트가 액세스 포인트에 연결할 때 SAE 교환을 수행합니다. 성공하면 세션 키가 파생되는 암호화 방식의 강력한 키가 각각 생성됩니다. 기본적으로 클라이언트와 액세스 포인트는 커밋(commit) 및 확인 단계로 진행됩니다.

일단 약속이 있으면 클라이언트와 액세스 포인트는 생성할 세션 키가 있을 때마다 확인 상태로 이동할 수 있습니다. 이 방법은 순방향 비밀성을 사용합니다. 즉 침입자가 하나의 키를 해독할 수 있지만 다른 모든 키를 해독할 수는 없습니다.



SAE 프레임 교환

Hash-to-Element(H2E)

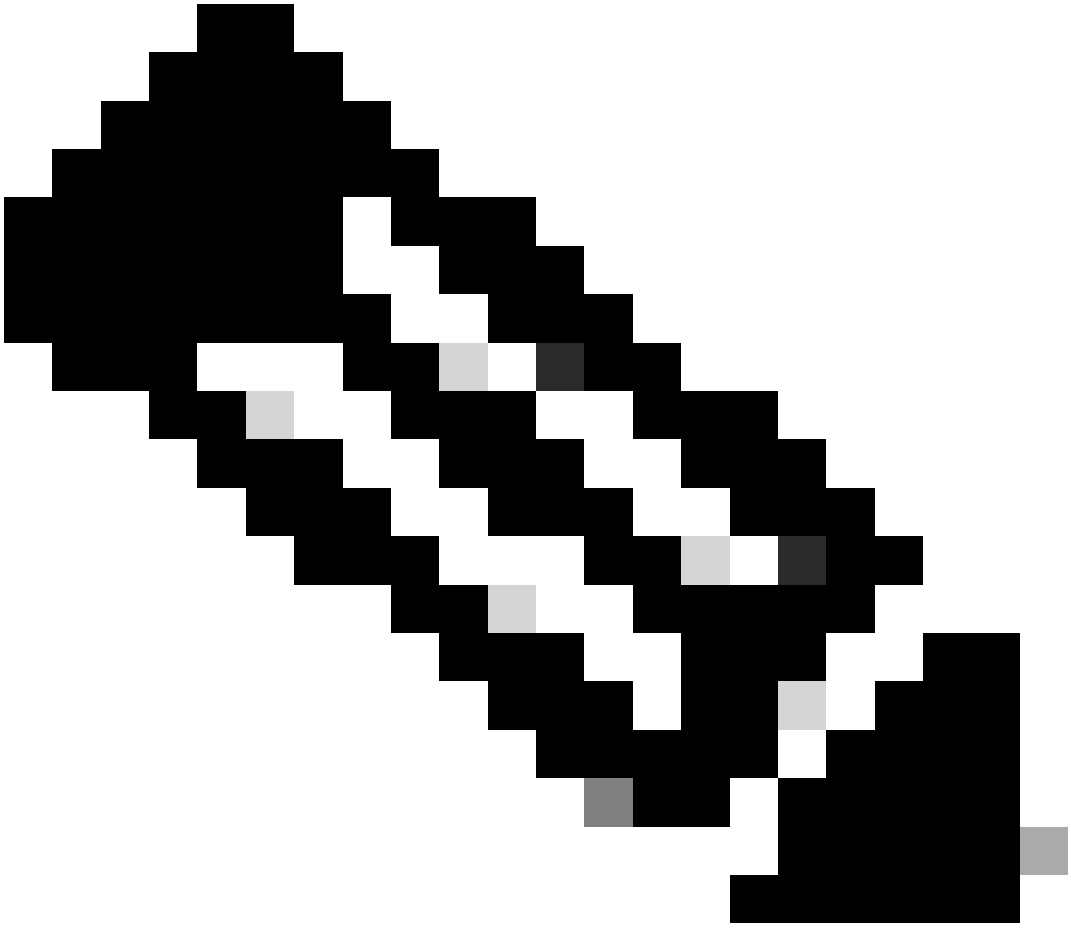
H2E(Hash-to-Element)는 새로운 PWE(SAE Password Element) 메서드입니다. 이 방법에서, SAE 프로토콜에서 사용되는 비밀 PWE는 비밀번호로부터 생성된다.

H2E를 지원하는 스테이션(STA)이 AP와 SAE를 시작할 때 AP가 H2E를 지원하는지 확인한다. 대답이 "예"인 경우 AP는 H2E를 사용하여 SAE Commit 메시지에 새로 정의된 상태 코드 값을 사용하여 PWE를 파생시킵니다.

STA가 HnP(Hunting-and-Pecking)를 사용하면 전체 SAE exchange는 변경되지 않습니다.

H2E를 사용하는 동안 PWE 파생은 다음 구성 요소로 나뉩니다.

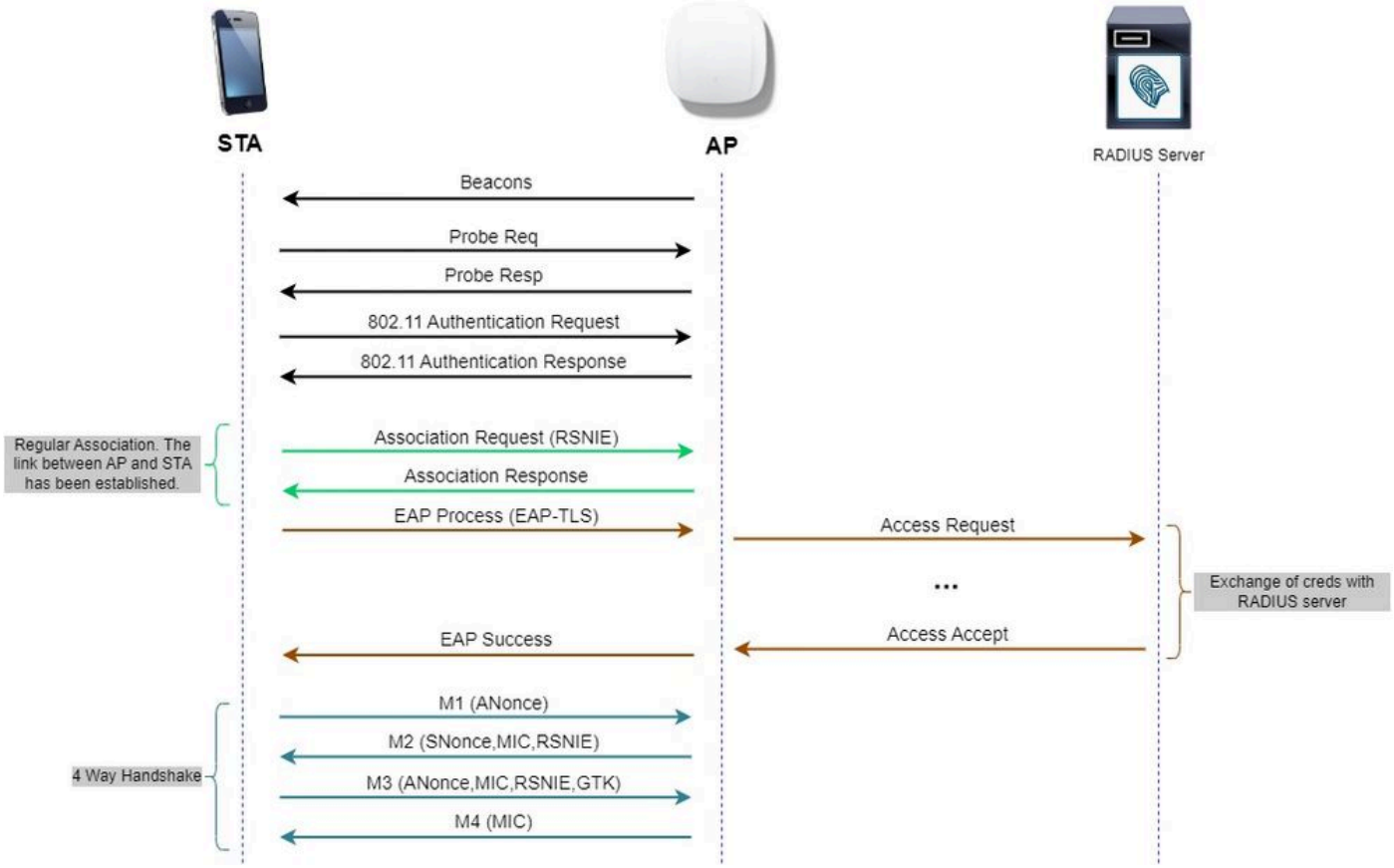
- 비밀번호에서 PT(Secret Intermediate Element) 파생입니다. 이 작업은 지원되는 각 그룹에 대해 디바이스에서 비밀번호가 처음 구성된 경우 오프라인으로 수행할 수 있습니다.
- 저장된 PT에서 PWE 유도. 이는 협상된 그룹 및 피어의 MAC 주소에 따라 다릅니다. 이 작업은 SAE 교환 중에 실시간으로 수행됩니다.



참고: 6GHz는 Hash-to-Element SAE PWE 메서드만 지원합니다.

802.1x라고도 하는 WPA-엔터프라이즈

WPA3-Enterprise는 가장 안전한 WPA3 버전으로, RADIUS 서버와의 사용자 인증을 위해 사용자 이름과 비밀번호를 802.1X와 함께 사용합니다. 기본적으로 WPA3은 128비트 암호화를 사용하지만 선택적으로 구성할 수 있는 192비트 암호화 강도 암호화를 도입하여 민감한 데이터를 전송하는 모든 네트워크를 추가로 보호합니다.



WPA3 엔터프라이즈 다이어그램 흐름

레벨 세트: WPA3 모드

- WPA3-개인
  - WPA3-개인 전용 모드
    - PMF 필요
  - WPA3-개인 전환 모드
    - 구성 규칙: AP에서 WPA2-Personal이 활성화될 때마다 WPA2-Personal 전용 모드에서 작동하도록 관리자가 명시적으로 재지정하지 않는 한 WPA3-Personal 전환 모드도 기본적으로 활성화되어야 합니다

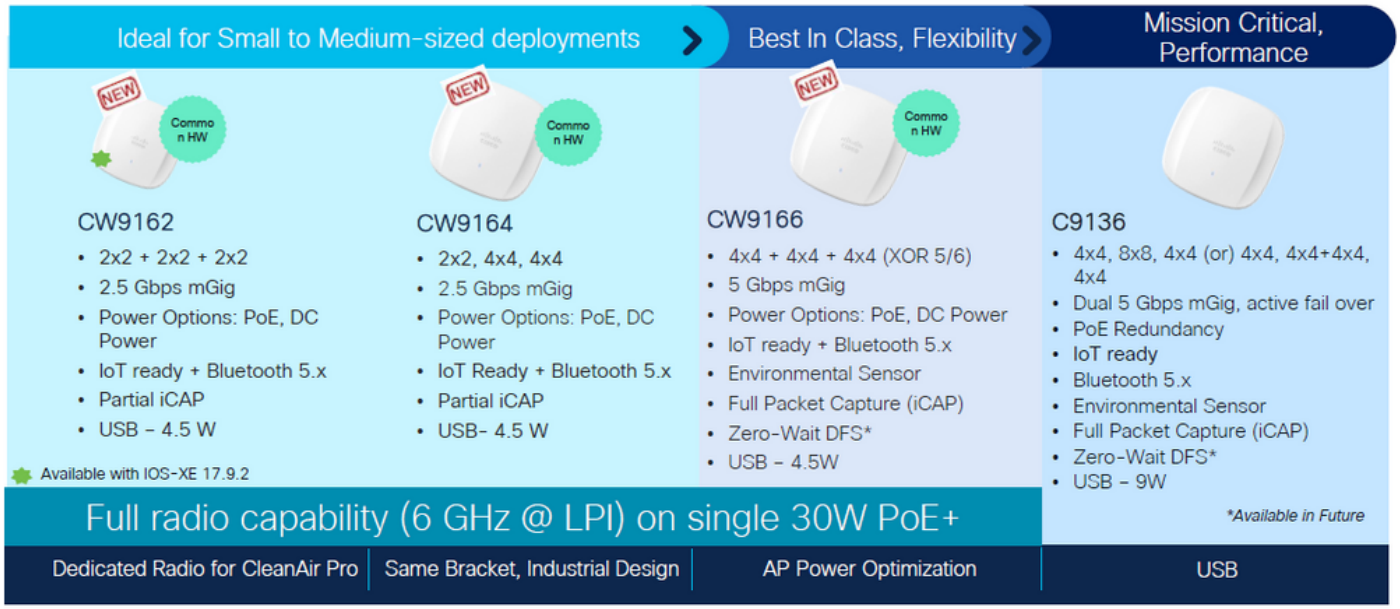
- WPA3-엔터프라이즈
  - WPA3-엔터프라이즈 전용 모드
    - 모든 WPA3 연결에 대해 PMF를 협상합니다.
  - WPA3-엔터프라이즈 전환 모드
    - PMF는 WPA3 연결을 위해 협상됩니다.
    - WPA2 연결용 PMF(선택 사항)
  - WPA3-Enterprise suite-B "192비트" 모드 - CNSA(Commercial National Security Algorithm)
    - 연방 정부에만 국한되지 않고
    - 컨피그레이션 오류를 방지하기 위한 일관된 암호화 암호 그룹
    - 암호화 및 더 나은 해시 기능을 위해 GCMP 및 ECCP 추가(SHA384)
    - PMF 필요

- WPA3 192비트 보안은 EAP-TLS에 배타적이어야 합니다. EAP-TLS에서는 신청자 및 RADIUS 서버 모두에 인증서가 필요합니다.
- WPA3 192비트 엔터프라이즈를 사용하려면 RADIUS 서버가 다음 중 하나의 허용된 EAP 암호를 사용해야 합니다.

  TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

클라이언트 보안 호환성 매트릭스를 포함하여 Cisco WLAN의 WPA3 구현에 대한 자세한 내용은 [WPA3 구축 가이드](#)를 [참조하십시오](#).

Cisco Catalyst Wi-Fi 6E AP



Wi-Fi 6E 액세스 포인트

클라이언트 지원 보안 설정

WiFi Alliance 웹 페이지 제품 찾기를 사용하여 WPA3-Enterprise를 지원하는 제품을 찾[을](#) 수 [있습니다](#).

Windows 디바이스에서는 "netsh wlan show drivers" 명령을 사용하여 어댑터에서 지원하는 보안 설정이 무엇인지 확인할 수 있습니다.

다음은 인텔 AX211의 출력입니다.

```
C:\Users\tantunes>netsh wlan show drivers

Interface name: Wi-Fi

    Driver                    : Intel(R) Wi-Fi 6E AX211 160MHz
    Vendor                    : Intel Corporation
    Provider                  : Intel
    Date                      : 3/9/2023
    Version                   : 22.200.2.1
    INF file                  : oem151.inf
    Type                      : Native Wi-Fi Driver
    Radio types supported     : 802.11b 802.11g 802.11n 802.11a 802.11ac 802.11ax
    FIPS 140-2 mode supported : Yes
    802.11w Management Frame Protection supported : Yes
    Hosted network supported  : No
    Authentication and cipher supported in infrastructure mode:
                                Open            None
                                Open            WEP-40bit
                                Open            WEP-104bit
                                Open            WEP
                                WPA-Enterprise  TKIP
                                WPA-Enterprise  CCMP
                                WPA-Personal    TKIP
                                WPA-Personal    CCMP
                                WPA2-Enterprise TKIP
                                WPA2-Enterprise CCMP
                                WPA2-Personal   TKIP
                                WPA2-Personal   CCMP
                                Open            Vendor defined
                                WPA3-Personal   CCMP
                                Vendor defined  Vendor defined
                                WPA3-Enterprise 192 Bits GCMP-256
                                OWE             CCMP
                                WPA3-Enterprise CCMP
                                WPA3-Enterprise TKIP
    Number of supported bands : 3
                                2.4 GHz [ 0 MHz - 0 MHz]
                                5 GHz   [ 0 MHz - 0 MHz]
                                6 GHz   [ 0 MHz - 0 MHz]
    IHV service present       : Yes
    IHV adapter OUI           : [00 00 00], type: [00]
    IHV extensibility DLL path: C:\WINDOWS\System32\DriverStore\FileRepository\netwtw6e.inf_amd64_eda979fbdedea064\IntelIHVRouter12.dll
```

클라이언트 AX211용 _netsh wlan show driver_의 Windows 출력

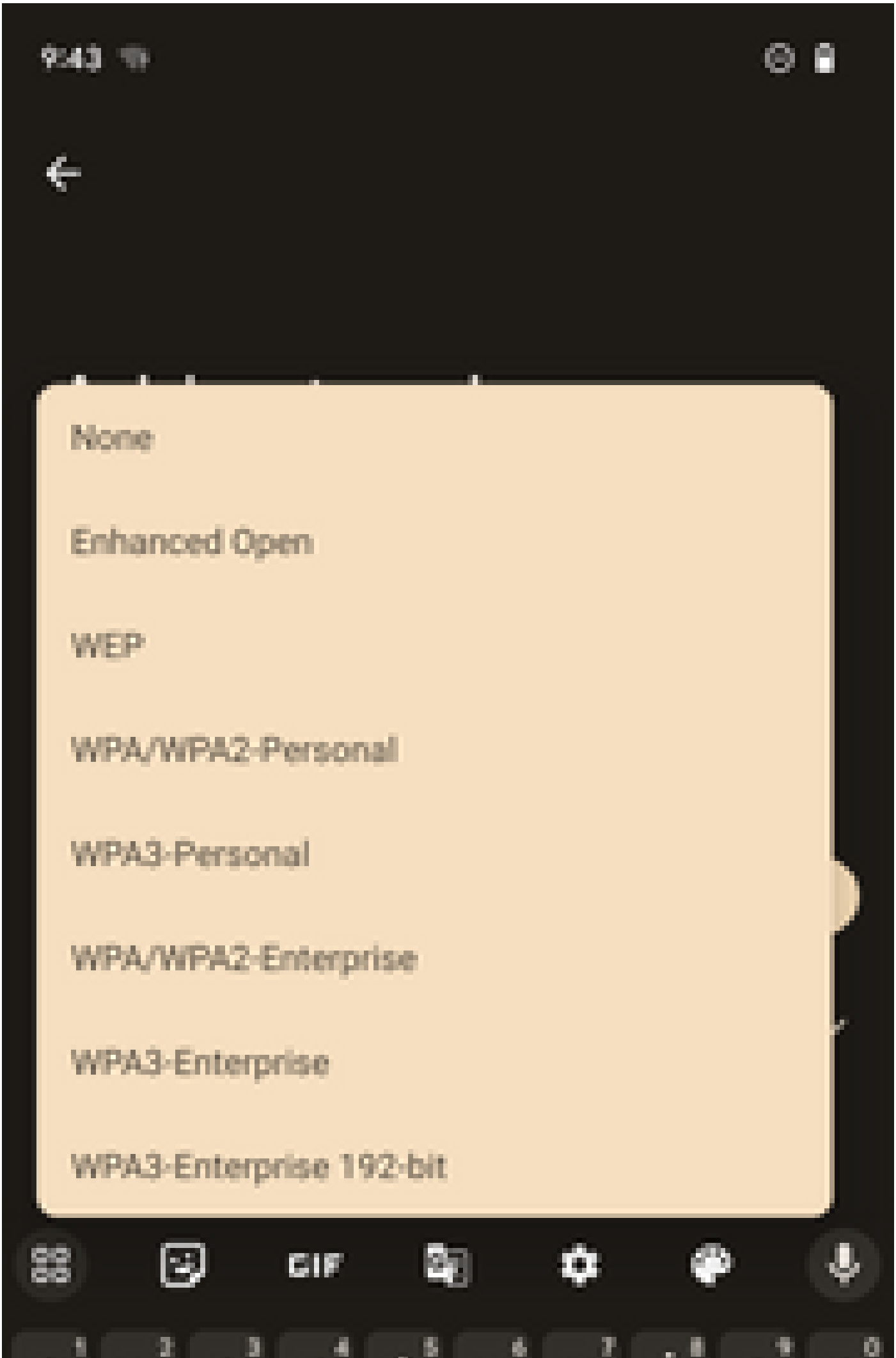
넷기어 A8000:

```
Interface name: A8000_NETGEAR

    Driver                     : NETGEAR A8000 WiFi 6 & 6E Adapter
    Vendor                     : NETGEAR Inc.
    Provider                   : MediaTek, Inc.
    Date                       : 11/25/2022
    Version                    : 1.0.0.108
    INF file                   : oem9.inf
    Type                       : Native Wi-Fi Driver
    Radio types supported      : 802.11b 802.11a 802.11g 802.11n 802.11ac 802.11ax
    FIPS 140-2 mode supported : Yes
    802.11w Management Frame Protection supported : Yes
    Hosted network supported  : No
    Authentication and cipher supported in infrastructure mode:
                                Open             None
                                Open             WEP-40bit
                                Open             WEP-104bit
                                Open             WEP
                                WPA-Enterprise   TKIP
                                WPA-Enterprise   CCMP
                                WPA3-Personal    CCMP
                                OWE              CCMP
                                WPA-Personal     TKIP
                                WPA-Personal     CCMP
                                WPA2-Enterprise  TKIP
                                WPA2-Enterprise  CCMP
                                WPA2-Personal    TKIP
                                WPA2-Personal    CCMP
    Number of supported bands : 3
                                2.4 GHz [ 0 MHz - 0 MHz]
                                5 GHz   [ 0 MHz - 0 MHz]
                                6 GHz   [ 0 MHz - 0 MHz]
    IHV service present        : Yes
    IHV adapter OUI            : [00 00 00], type: [00]
    IHV extensibility DLL path: C:\WINDOWS\system32\mtkihvux.dll
    IHV UI extensibility ClSID: {00000000-0000-0000-0000-000000000000}
    IHV diagnostics CLSID      : {00000000-0000-0000-0000-000000000000}
    Wireless Display Supported: Yes (Graphics Driver: Yes, Wi-Fi Driver: Yes)
```

클라이언트 Netgear A8000s용 _netsh wlan show driver_의 Windows 출력

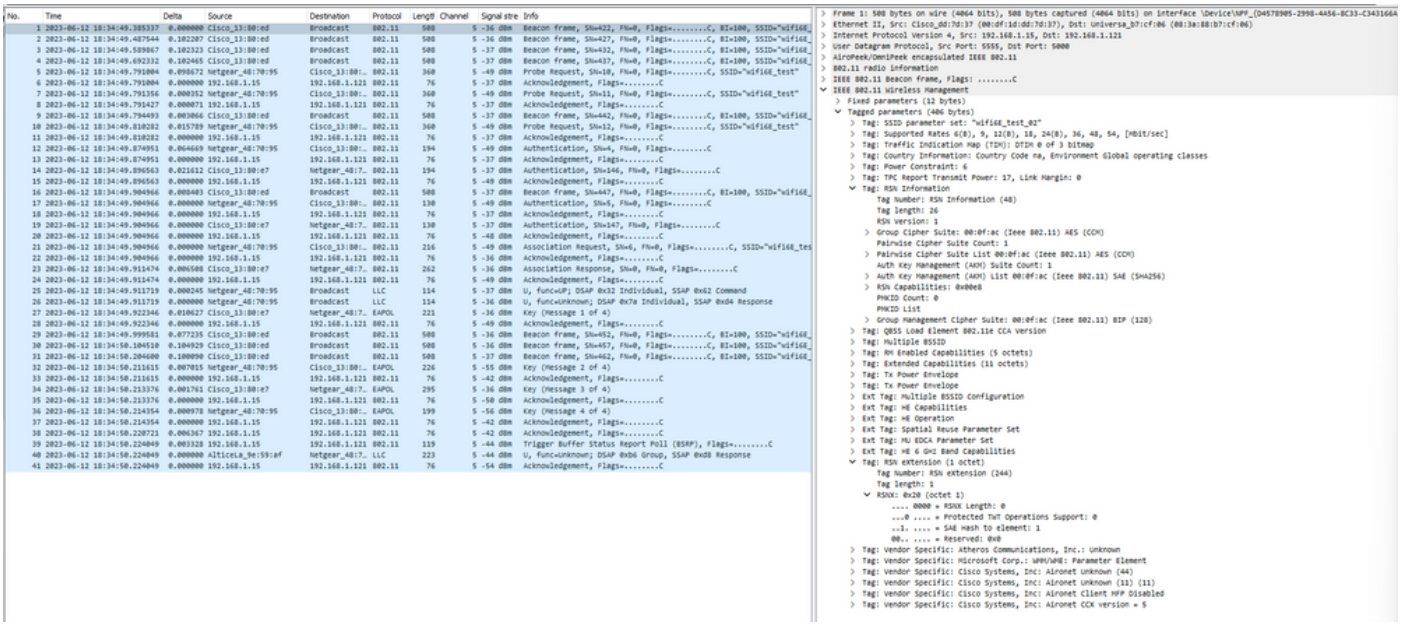
Android 픽셀 6a:


9:43
None
Enhanced Open
WEP
WPA/WPA2-Personal
WPA3-Personal
WPA/WPA2-Enterprise
WPA3-Enterprise
WPA3-Enterprise 192-bit
GIF

를 선택할 수 있지만 클라이언트가 연결할 수 없는 것으로 관찰되었습니다. 빠른 전환과 함께 SAE를 사용하려는 경우 항상 SAE 및 FT+SAE 확인란을 모두 활성화합니다.

WLAN Security(WLAN 보안) 설정의 WLC GUI에서 보기:

비콘 OTA 확인:

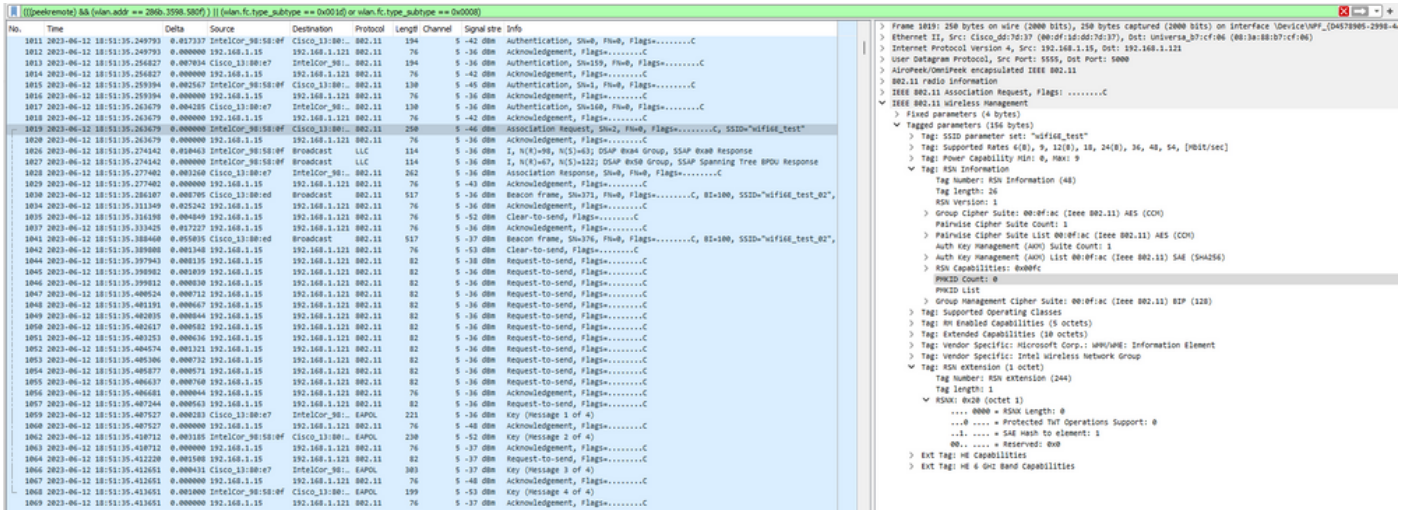


WPA3 SAE + FT 비컨

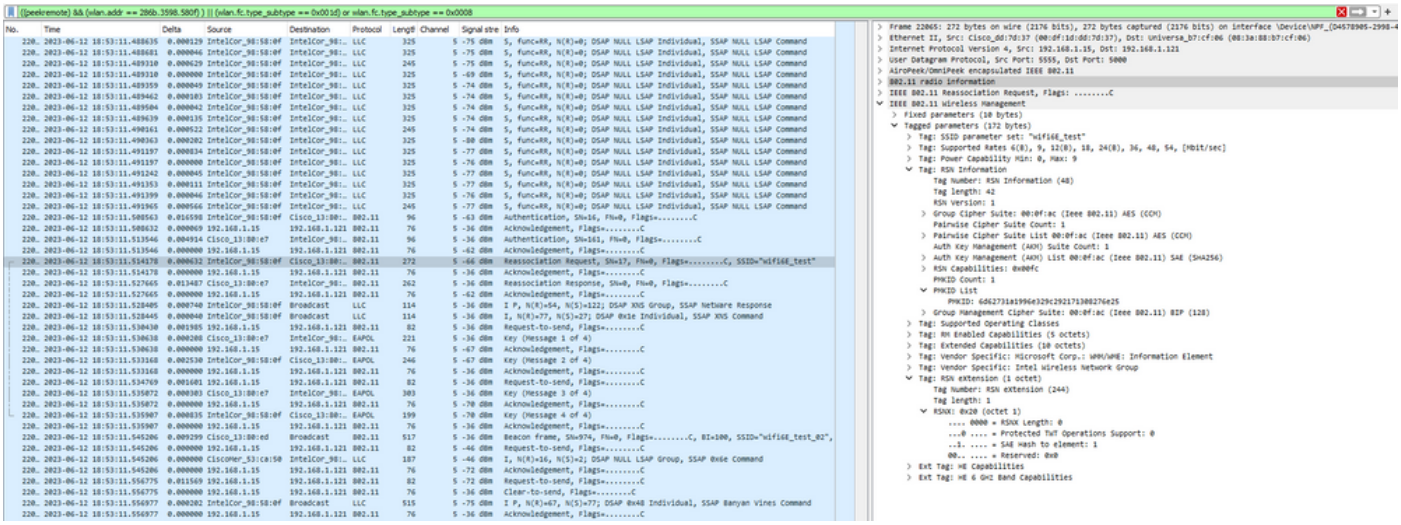
여기서는 Wi-Fi 6E 클라이언트가 다음과 연결된 것을 관찰할 수 있습니다.

인텔 AX211

클라이언트의 RSN 정보에 중점을 둔 연결 OTA:

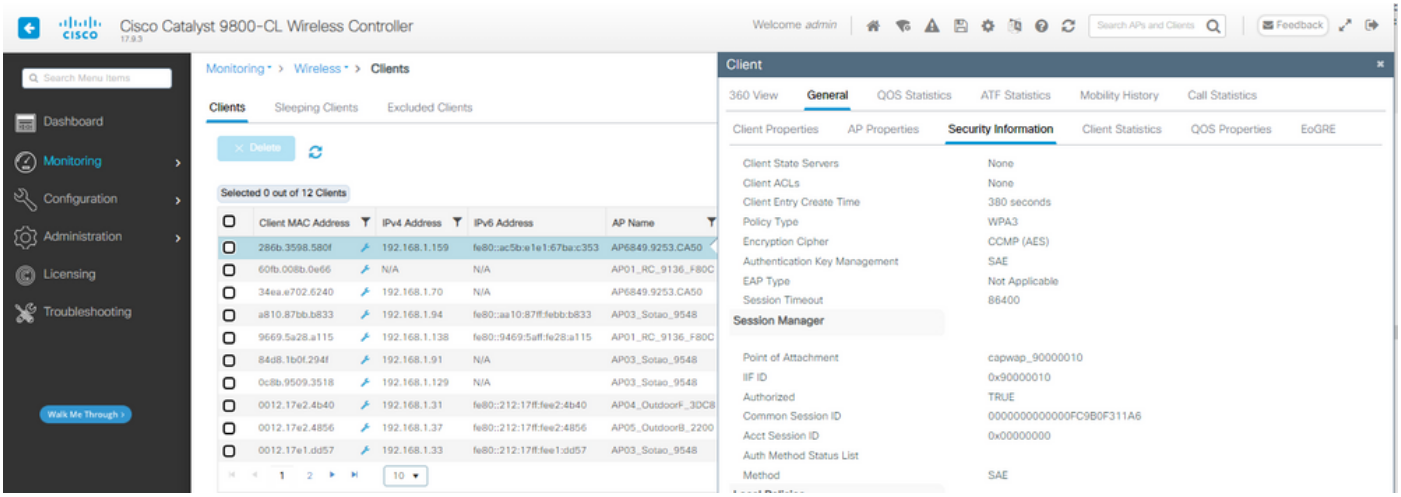


PMKID를 볼 수 있는 로밍 이벤트:



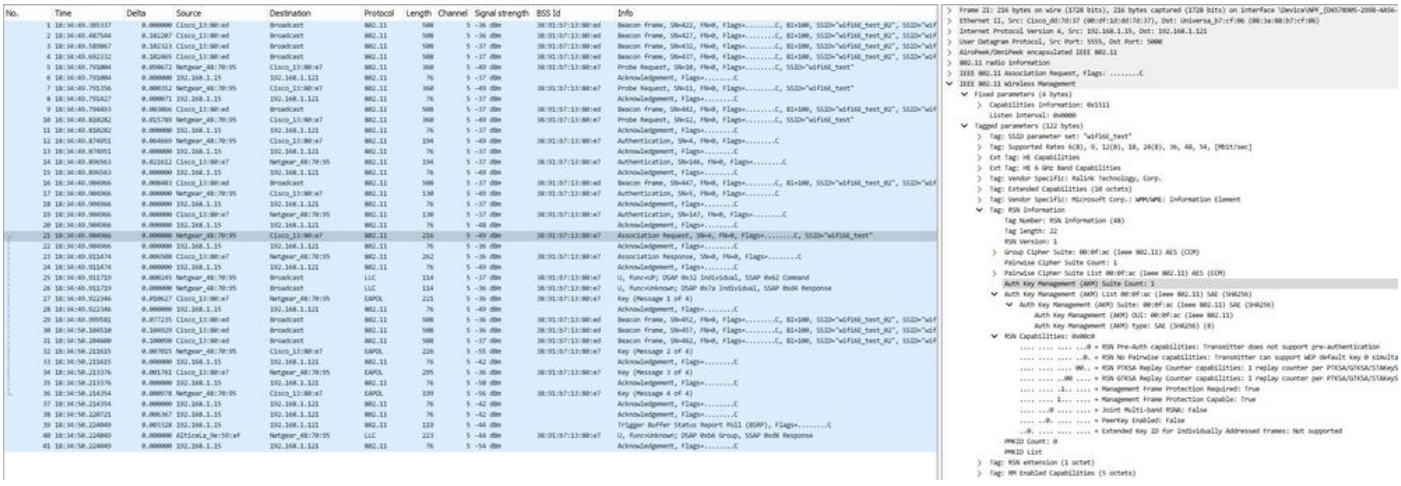
WPA3 SAE + FT 재연결 요청

WLC의 클라이언트 세부사항:



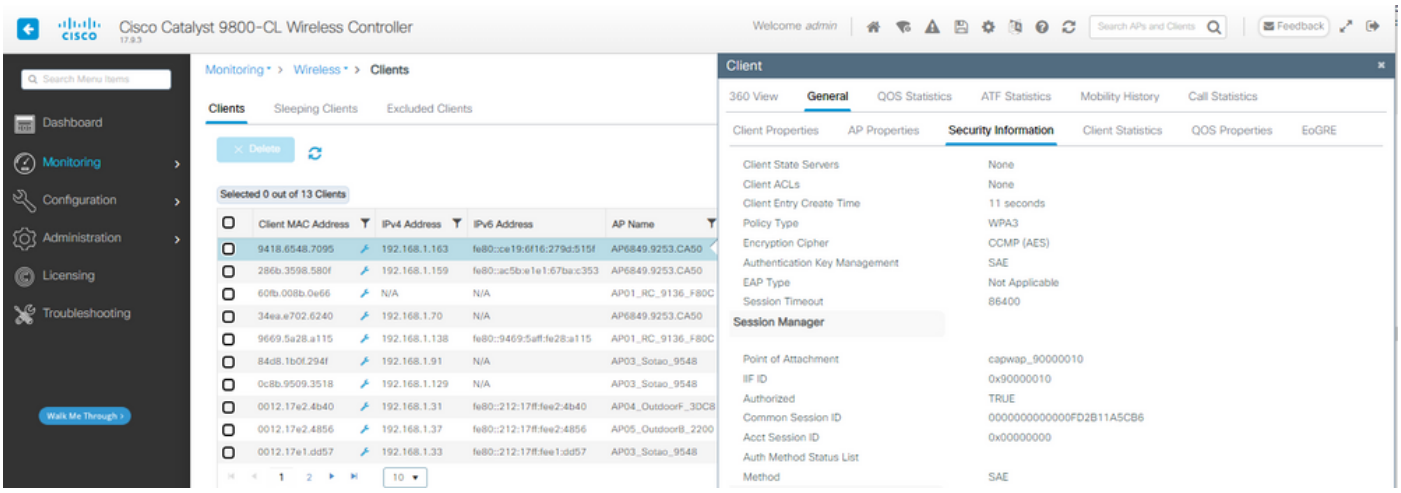
넷기어 A8000

클라이언트의 RSN 정보에 초점을 맞추어 OTA를 연결합니다. 초기 연결:



ssss

WLC의 클라이언트 세부사항:



픽셀 6a

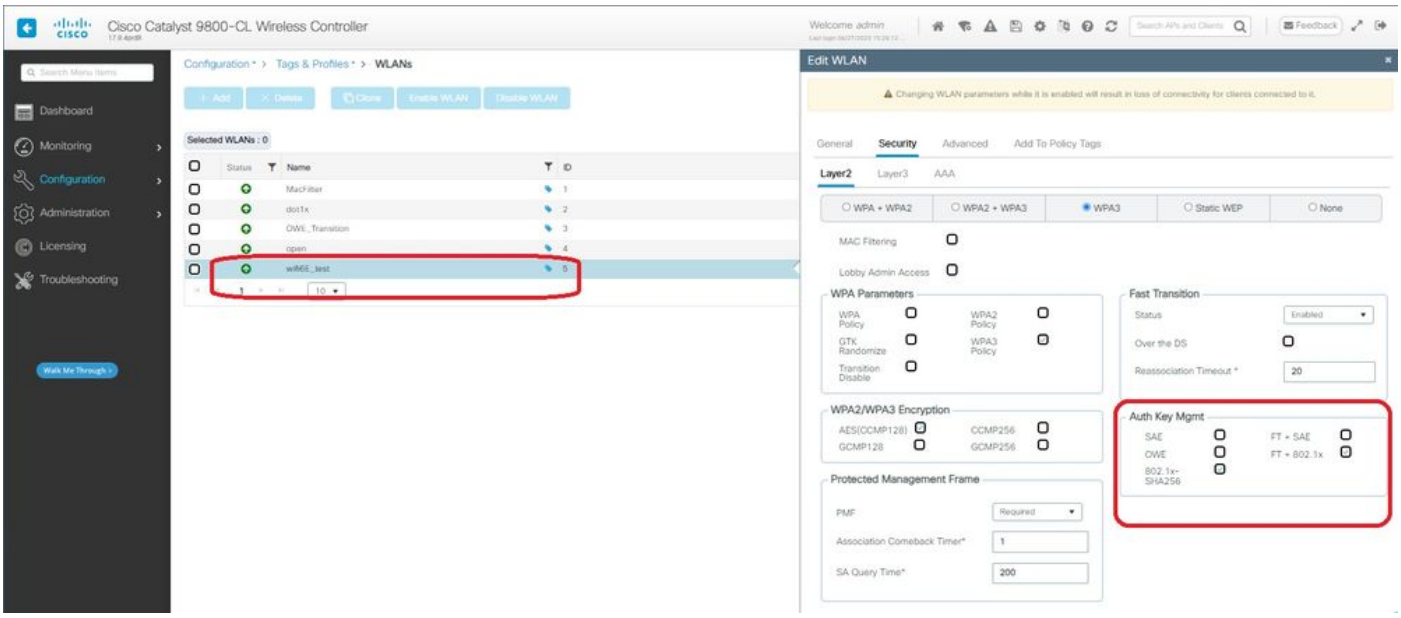
FT가 사용하도록 설정된 경우 디바이스에서 로밍할 수 없습니다.

삼성 S23

FT가 사용하도록 설정된 경우 디바이스에서 로밍할 수 없습니다.

WPA3-엔터프라이즈 + AES(CCMP128) + 802.1x-SHA256 + FT

WLAN 보안 구성:



WPA3 Enterprise 802.1x-SHA256 + FTWLAN 보안 구성

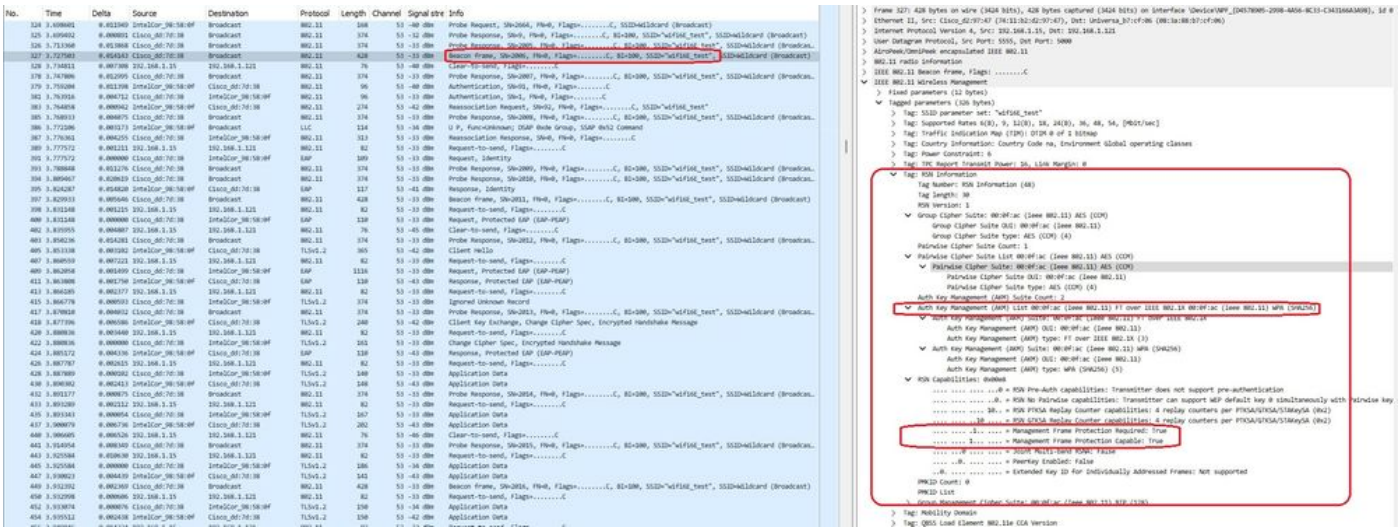
WLAN Security(WLAN 보안) 설정의 WLC GUI에서 보기:

여기서는 각 디바이스에서 오는 인증을 보여주는 ISE 라이브 로그를 확인할 수 있습니다.

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint Profile	Authenticat...	Authorizati...	Authorizati...	IP Address	Network Device
				Identity	Endpoint ID	Endpoint Profile	Authentication	Authorization	Authorization	IP Address	Network Device
Jun 27, 2023 01:52:38.130 PM			0	tantunes	04:29:2E:C9:E3:71		WirelessDot...	WirelessDot...	PermitAccess		
Jun 27, 2023 01:52:38.130 PM				tantunes	04:29:2E:C9:E3:71		WirelessDot...	WirelessDot...	PermitAccess		eWLC-9800-01
Jun 27, 2023 01:51:53.850 PM			0	tantunes	24:95:2F:72:8A:66	Unknown	WirelessDot...	WirelessDot...	PermitAccess		
Jun 27, 2023 01:51:53.850 PM				tantunes	24:95:2F:72:8A:66	Unknown	WirelessDot...	WirelessDot...	PermitAccess		eWLC-9800-01
Jun 27, 2023 01:50:58.679 PM			0	tantunes	94:18:65:48:70:95	Netgear-Device	WirelessDot...	WirelessDot...	PermitAccess		
Jun 27, 2023 01:50:58.679 PM				tantunes	94:18:65:48:70:95	Netgear-Device	WirelessDot...	WirelessDot...	PermitAccess		eWLC-9800-01
Jun 27, 2023 01:50:43.883 PM				tantunes	94:18:65:48:70:95	Netgear-Device	WirelessDot...	WirelessDot...	PermitAccess		eWLC-9800-01
Jun 27, 2023 01:50:42.877 PM			0	tantunes	28:6B:35:98:58:0F	Intel-Device	WirelessDot...	WirelessDot...	PermitAccess		
Jun 27, 2023 01:50:42.877 PM				tantunes	28:6B:35:98:58:0F	Intel-Device	WirelessDot...	WirelessDot...	PermitAccess		eWLC-9800-01

ISE 라이브 로그

Beacon OTA는 다음과 같습니다.

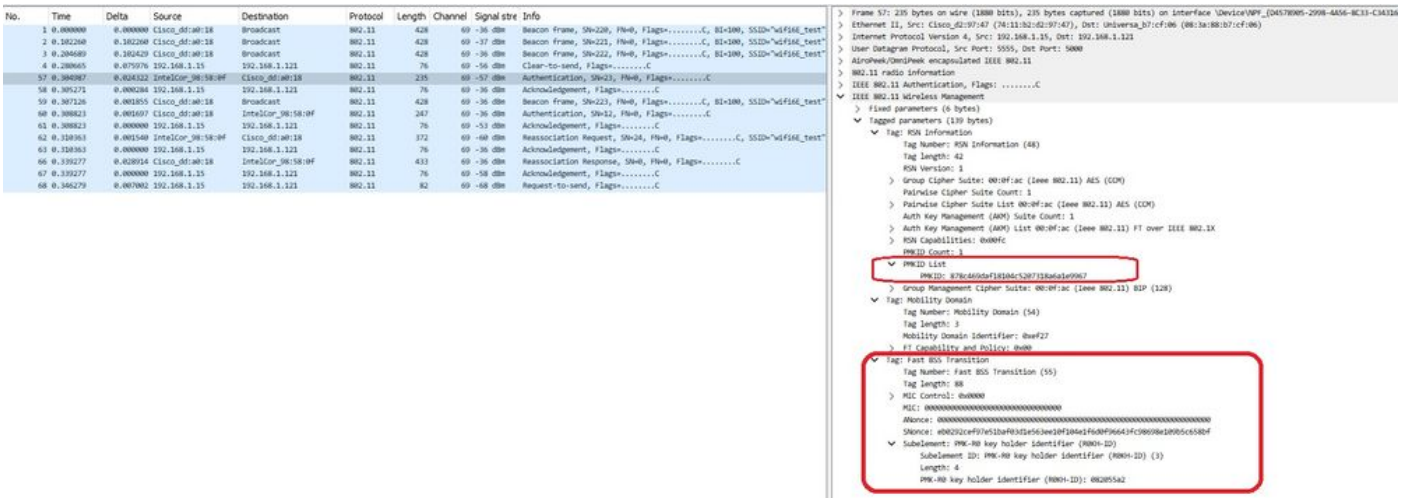


WPA3 Enterprise 802.1x +FT 비컨

여기서는 Wi-Fi 6E 클라이언트가 다음과 연결된 것을 관찰할 수 있습니다.

인텔 AX211

로밍 이벤트에 대한 클라이언트의 RSN 정보에 중점을 둔 연결 OTA:

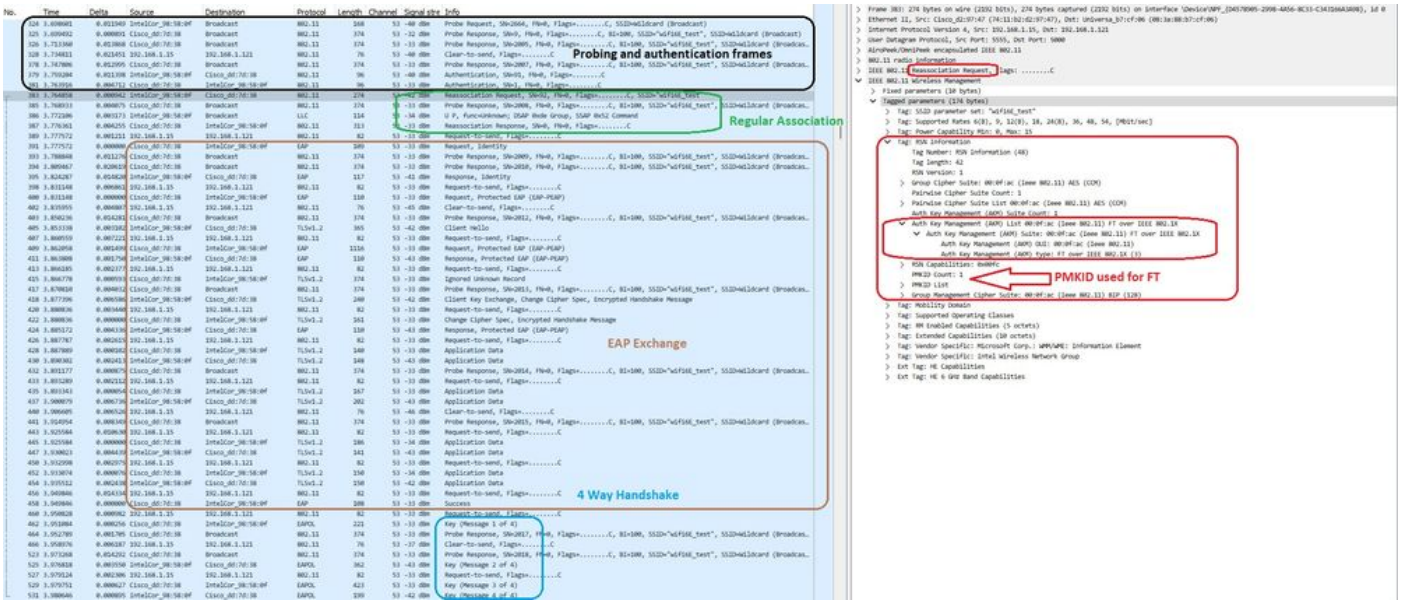


WPA3 Enterprise 802.1x + FT 로밍 이벤트

WLAN에서(예: WLC GUI에서) 클라이언트를 수동으로 삭제하면 흥미로운 동작이 발생합니다. 클

라이언트는 연결 해제 프레임을 수신하지만 동일한 AP에 다시 연결하려고 시도하며 재연결 프레임을 사용하고 클라이언트 세부사항이 AP/WLC에서 삭제되었기 때문에 완전한 EAP 교환이 이루어집니다.

이는 기본적으로 새로운 Association(연결) 프로세스와 동일한 프레임 교환입니다. 여기에서 프레임 교환을 볼 수 있습니다.



WPA3 Enterprise 802.1x + FT Ax211 연결 흐름

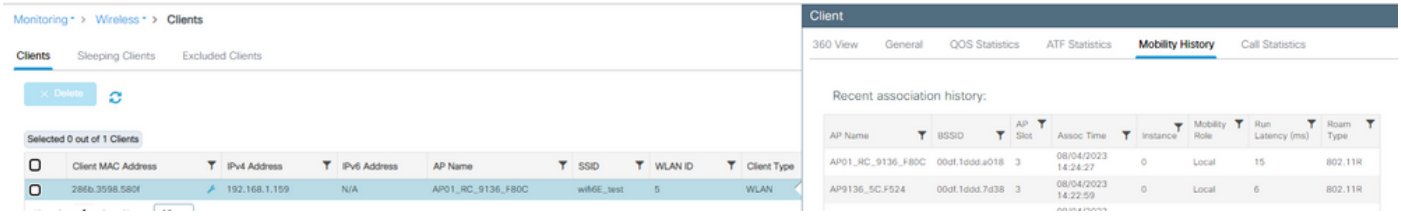
WLC의 클라이언트 세부사항:

WPA3 Enterprise 802.1x + FT 클라이언트 세부사항

이 클라이언트는 DS를 통해 FT를 사용하여 테스트되었으며 802.11r을 사용하여 로밍할 수 있었습니다.

AX211 로밍(FT over DS)

FT 로밍 이벤트도 볼 수 있습니다.



WPA3 Enterprise(FT 포함)

그리고 wlc의 클라이언트 ra 추적:

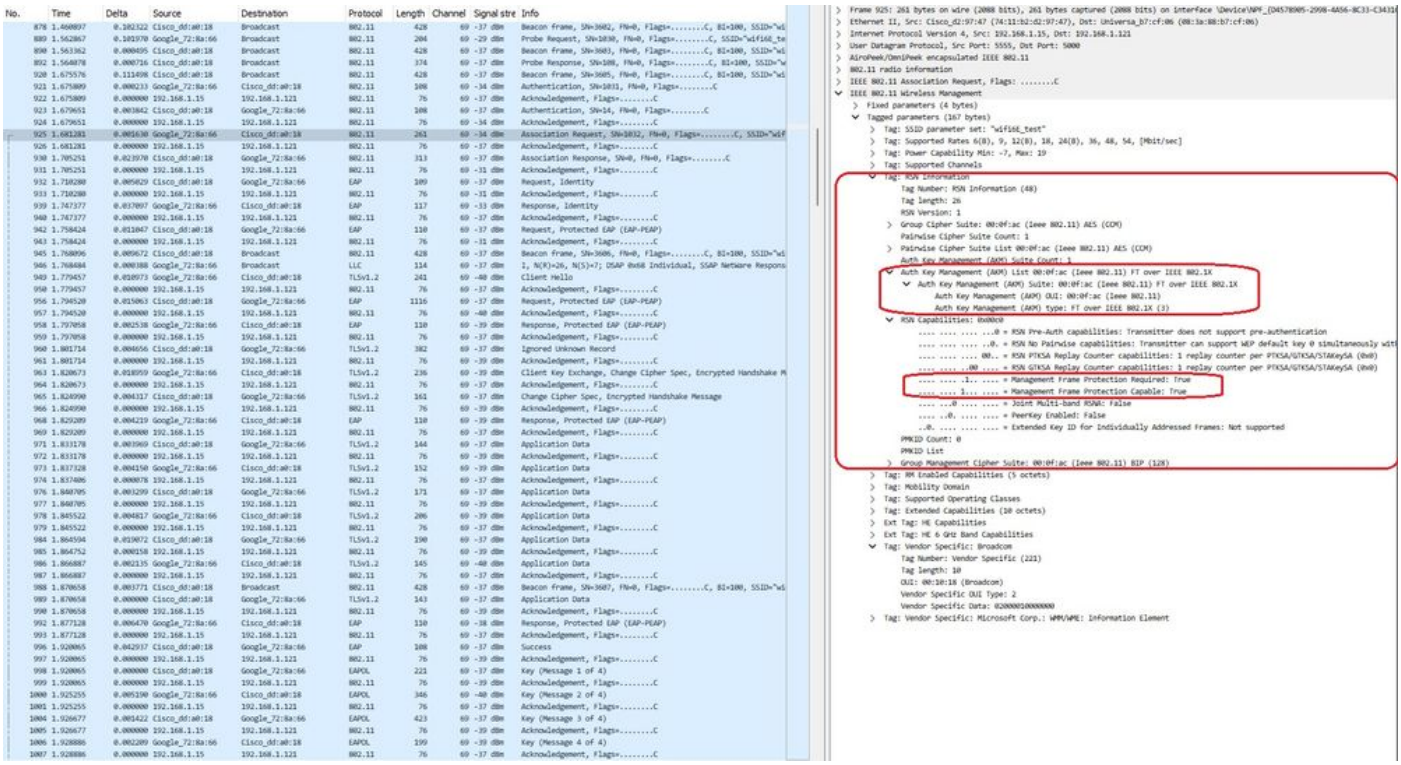
```
Logging display requested on 2023/08/04 14:27:55 (GMT) for Hostname: [eWLC-9800-01], Model: [C9800-CL-K9], Version: [17.09.03], SN: [9RY35HS10G9], MD_SN: [9RY35HS10G9]
2023/08/04 14:22:59.315300237 {vmcd_x_R0-0}{1}: [client-orch-sm] [15210]: (note): MAC: 286b.3598.580f Re-Association received. BSSID 00df.1ddd.7d38, WLAN wifi6E_test, Slot 3 AP 00df.1ddd.7d30, AP9136_5C.F524, old BSSID 00df.1ddd.a018
2023/08/04 14:22:59.315044120 {vmcd_x_R0-0}{1}: [dot11] [15210]: (note): MAC: 286b.3598.580f Association success. AID 33, Roaming = True, WGB = False, 11r = True, 11w = True Fast roam = True
2023/08/04 14:22:59.316408412 {vmcd_x_R0-0}{1}: [client-orch-sm] [15210]: (note): MAC: 286b.3598.580f Delete mobile payload sent for BSSID: 00df.1ddd.a010 WTP mac: 00df.1ddd.a010 slot id: 3
2023/08/04 14:22:59.316652383 {vmcd_x_R0-0}{1}: [client-orch-state] [15210]: (note): MAC: 286b.3598.580f Client state transition: S_CO_RUN -> S_CO_L2_AUTH_IN_PROGRESS
2023/08/04 14:22:59.317328574 {vmcd_x_R0-0}{1}: [client-auth] [15210]: (note): MAC: 286b.3598.580f ADD MOBILE sent. Client state flags: 0x71 BSSID: MAC: 00df.1ddd.7d38 capwap IFID: 0x9000000d, Add mobiles sent: 1
2023/08/04 14:22:59.321041947 {vmcd_x_R0-0}{1}: [client-orch-sm] [15210]: (note): MAC: 286b.3598.580f Mobility discovery triggered. Client mode: Local
2023/08/04 14:22:59.321044391 {vmcd_x_R0-0}{1}: [client-orch-state] [15210]: (note): MAC: 286b.3598.580f Client state transition: S_CO_L2_AUTH_IN_PROGRESS -> S_CO_MOBILITY_DISCOVERY_IN_PROGRESS
2023/08/04 14:22:59.321064980 {vmcd_x_R0-0}{1}: [mm-client] [15210]: (note): MAC: 286b.3598.580f Mobility Successful. Roam Type None, Sub Roam Type MM_SUB_ROAM_TYPE_INTRA_INSTANCE, Previous BSSID MAC: 00df.1ddd.a010  Client IFID: 0xa0000003, Client Role:
Local PoA: 0x9000000d PoP: 0x0
2023/08/04 14:22:59.321213902 {vmcd_x_R0-0}{1}: [client-auth] [15210]: (note): MAC: 286b.3598.580f ADD MOBILE sent. Client state flags: 0x76 BSSID: MAC: 00df.1ddd.7d38 capwap IFID: 0x9000000d, Add mobiles sent: 1
2023/08/04 14:22:59.321254052 {vmcd_x_R0-0}{1}: [client-orch-state] [15210]: (note): MAC: 286b.3598.580f Client state transition: S_CO_MOBILITY_DISCOVERY_IN_PROGRESS -> S_CO_DPATH_PLUMB_IN_PROGRESS
2023/08/04 14:22:59.321463455 {vmcd_x_R0-0}{1}: [client-orch-state] [15210]: (note): MAC: 286b.3598.580f Client state transition: S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS
2023/08/04 14:22:59.321666600 {vmcd_x_R0-0}{1}: [client-orch-state] [15210]: (note): MAC: 286b.3598.580f Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_RUN
2023/08/04 14:24:27.918055521 {vmcd_x_R0-0}{1}: [client-orch-sm] [15210]: (note): MAC: 286b.3598.580f Re-Association received. BSSID 00df.1ddd.a018, WLAN wifi6E_test, Slot 3 AP 00df.1ddd.a010, AP01_RC_9136_F80C, old BSSID 00df.1ddd.7d38
2023/08/04 14:24:27.919097444 {vmcd_x_R0-0}{1}: [dot11] [15210]: (note): MAC: 286b.3598.580f Association success. AID 33, Roaming = True, WGB = False, 11r = True, 11w = True Fast roam = True
2023/08/04 14:24:27.921992623 {vmcd_x_R0-0}{1}: [client-orch-sm] [15210]: (note): MAC: 286b.3598.580f Delete mobile payload sent for BSSID: 00df.1ddd.7d38 WTP mac: 00df.1ddd.7d30 slot id: 3
2023/08/04 14:24:27.922776547 {vmcd_x_R0-0}{1}: [client-orch-state] [15210]: (note): MAC: 286b.3598.580f Client state transition: S_CO_RUN -> S_CO_L2_AUTH_IN_PROGRESS
2023/08/04 14:24:27.925409164 {vmcd_x_R0-0}{1}: [client-auth] [15210]: (note): MAC: 286b.3598.580f ADD MOBILE sent. Client state flags: 0x71 BSSID: MAC: 00df.1ddd.a018 capwap IFID: 0x9000000e, Add mobiles sent: 1
2023/08/04 14:24:27.931505071 {vmcd_x_R0-0}{1}: [client-orch-sm] [15210]: (note): MAC: 286b.3598.580f Mobility discovery triggered. Client mode: Local
2023/08/04 14:24:27.931511962 {vmcd_x_R0-0}{1}: [client-orch-state] [15210]: (note): MAC: 286b.3598.580f Client state transition: S_CO_L2_AUTH_IN_PROGRESS -> S_CO_MOBILITY_DISCOVERY_IN_PROGRESS
2023/08/04 14:24:27.931569962 {vmcd_x_R0-0}{1}: [mm-client] [15210]: (note): MAC: 286b.3598.580f Mobility Successful. Roam Type None, Sub Roam Type MM_SUB_ROAM_TYPE_INTRA_INSTANCE, Previous BSSID MAC: 00df.1ddd.7d38  Client IFID: 0xa0000003, Client Role:
Local PoA: 0x9000000e PoP: 0x0
2023/08/04 14:24:27.931861935 {vmcd_x_R0-0}{1}: [client-auth] [15210]: (note): MAC: 286b.3598.580f ADD MOBILE sent. Client state flags: 0x76 BSSID: MAC: 00df.1ddd.a018 capwap IFID: 0x9000000e, Add mobiles sent: 1
2023/08/04 14:24:27.931913122 {vmcd_x_R0-0}{1}: [client-orch-state] [15210]: (note): MAC: 286b.3598.580f Client state transition: S_CO_MOBILITY_DISCOVERY_IN_PROGRESS -> S_CO_DPATH_PLUMB_IN_PROGRESS
2023/08/04 14:24:27.933010101 {vmcd_x_R0-0}{1}: [client-orch-state] [15210]: (note): MAC: 286b.3598.580f Client state transition: S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS
2023/08/04 14:24:27.933501101 {vmcd_x_R0-0}{1}: [client-orch-state] [15210]: (note): MAC: 286b.3598.580f Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_RUN
```

넷기어 A8000

이 클라이언트에서는 WPA3-Enterprise가 지원되지 않습니다.

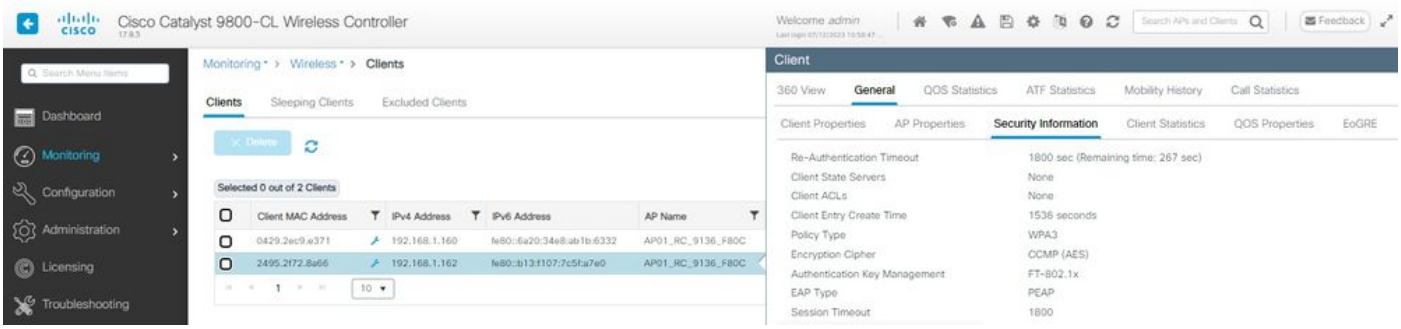
픽셀 6a

클라이언트의 RSN 정보에 중점을 둔 연결 OTA:



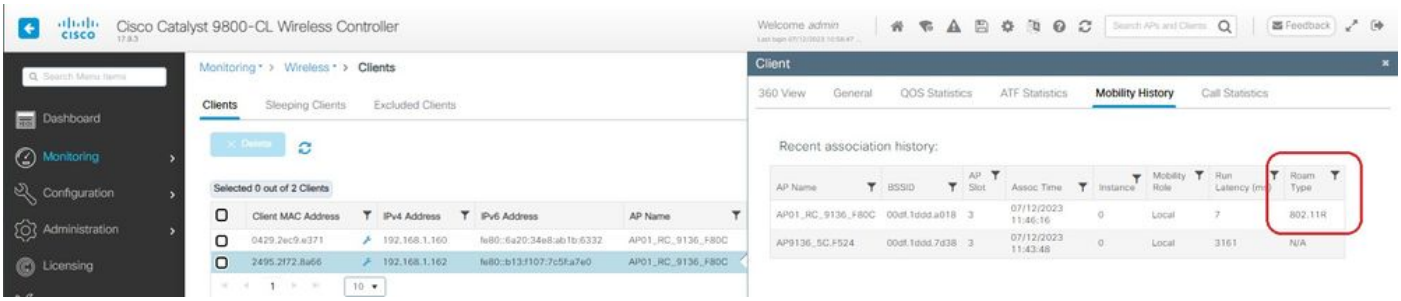
WPA3 Enterprise 802.1x + FT Pixel6a 연결

WLC의 클라이언트 세부사항:



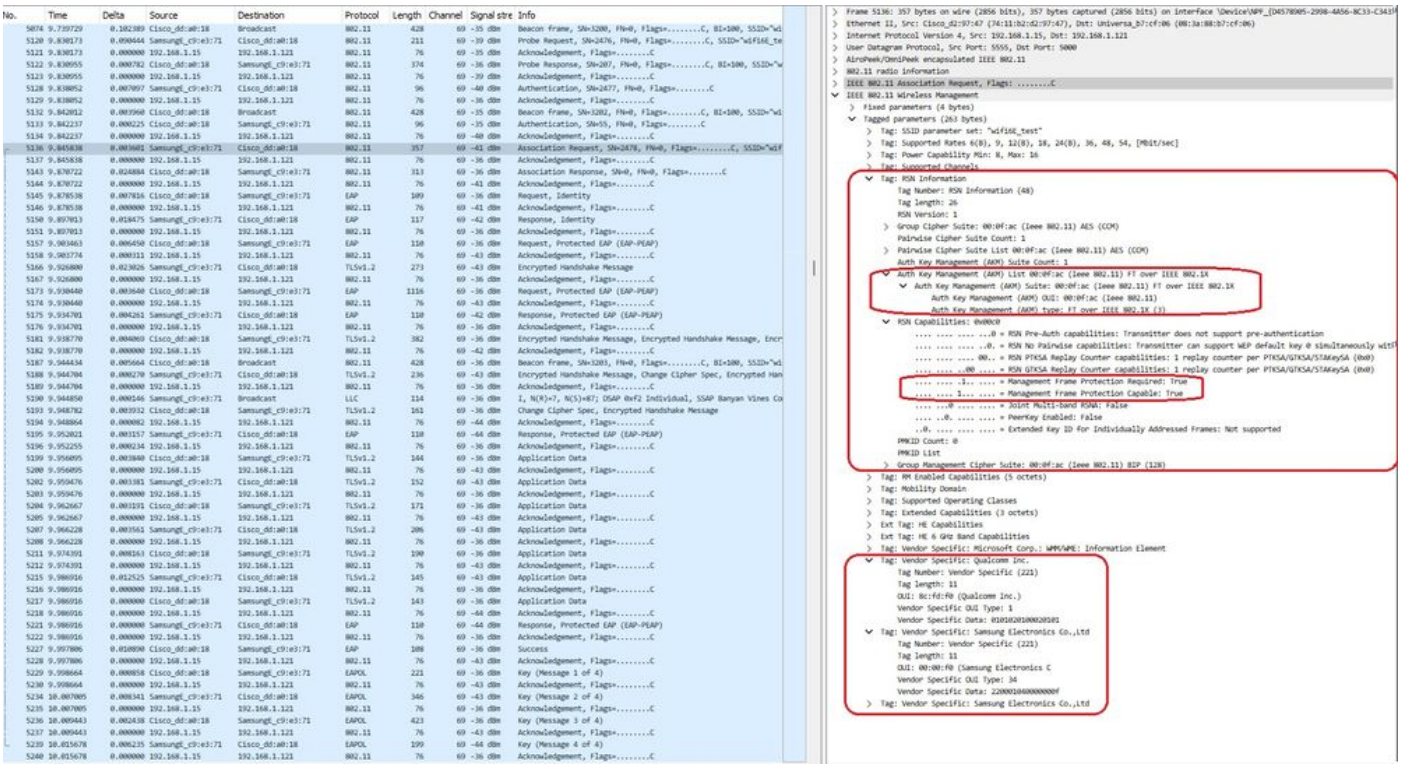
WPA3 Enterprise 802.1x + FT Pixel6a Client 상세 정보

roam type 802.11R을 확인할 수 있는 Over the Air에 roam 유형을 집중 조명합니다.



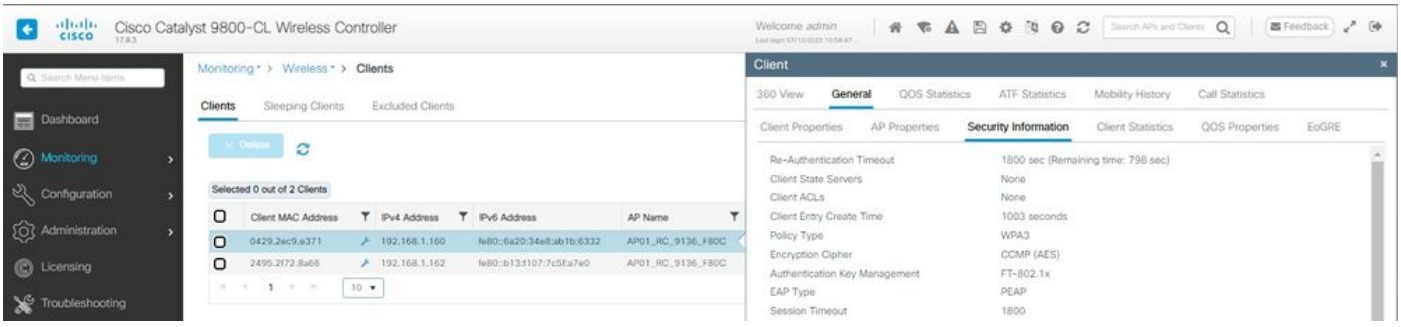
삼성 S23

클라이언트의 RSN 정보에 중점을 둔 연결 OTA:



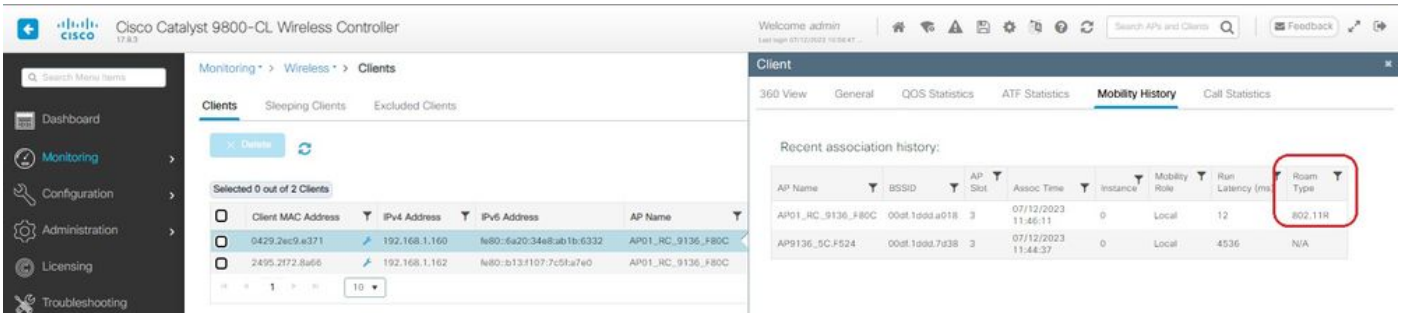
S23 FToTA 로밍 이벤트

WLC의 클라이언트 세부사항:



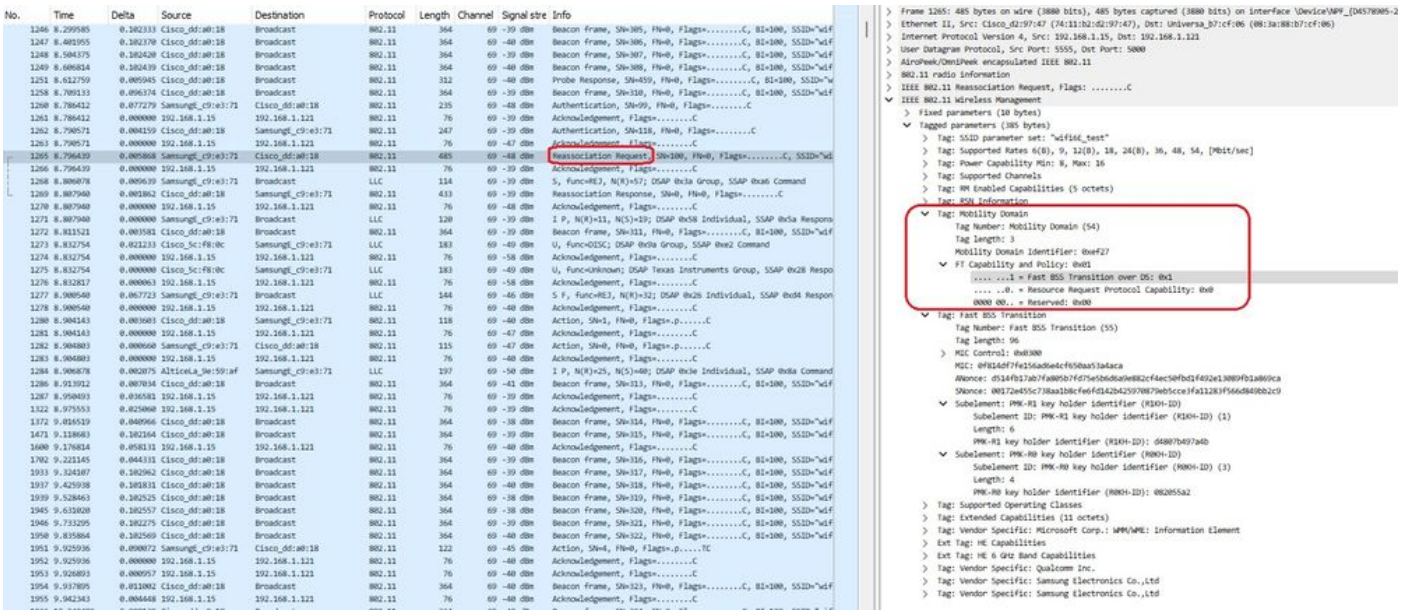
S23 클라이언트 속성

roam type 802.11R을 확인할 수 있는 Over the Air에 roam 유형을 집중 조명합니다.



S23 로밍 유형 802.11R

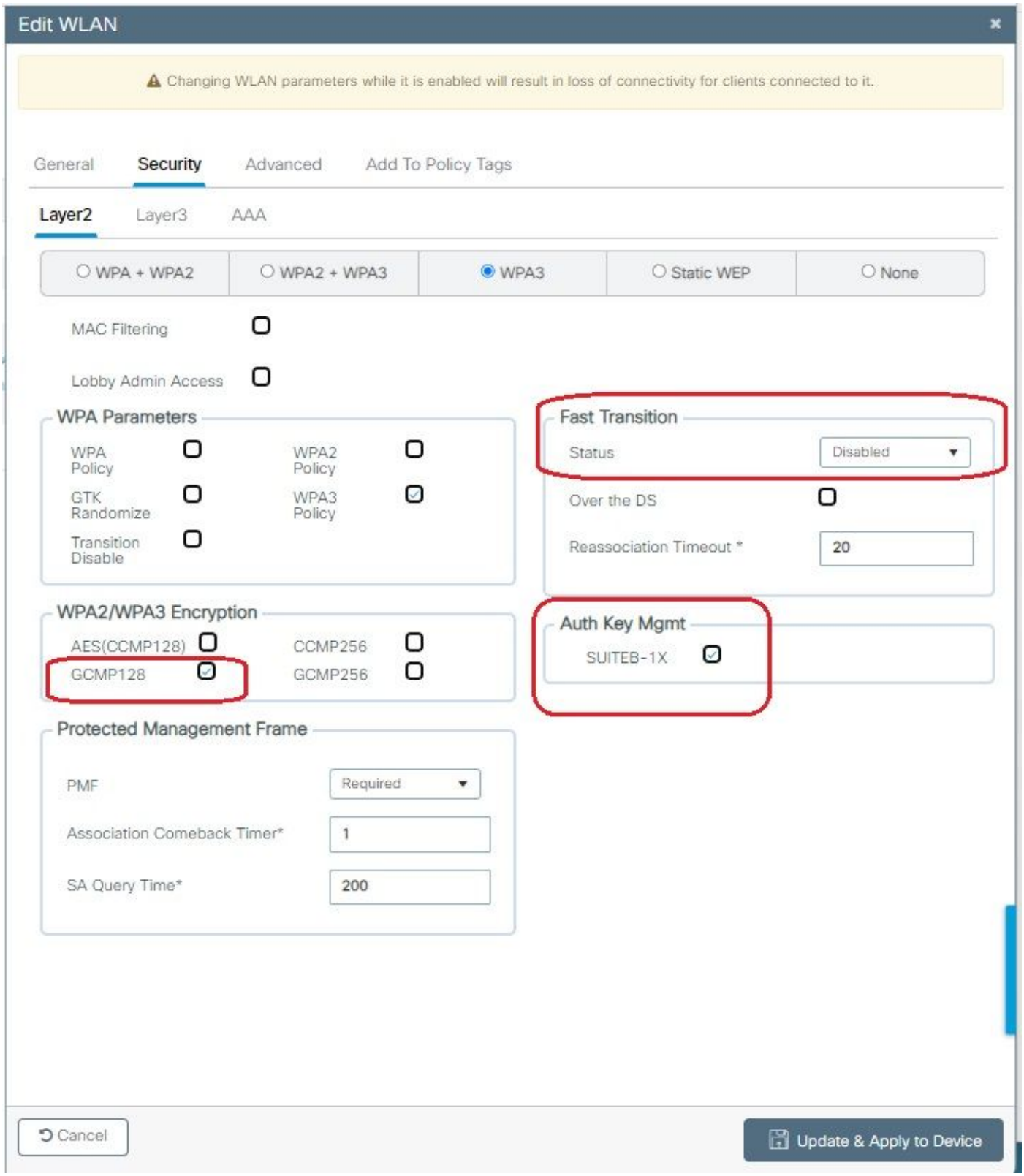
이 클라이언트는 DS를 통해 FT를 사용하여 테스트되었으며 802.11r을 사용하여 로밍할 수 있었습니다.



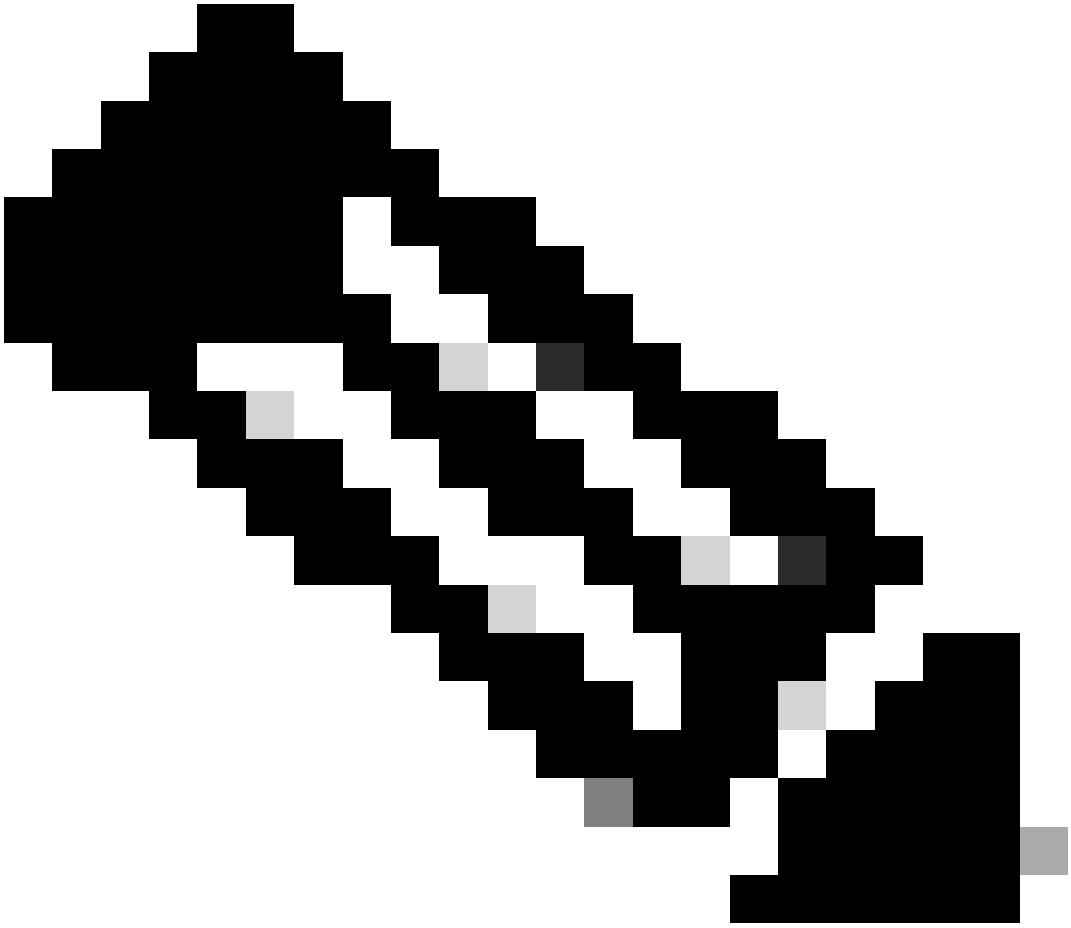
S23 로밍 FToDS 패킷

WPA3-엔터프라이즈 + GCMP128 암호 + SUITEB-1X

WLAN 보안 구성:



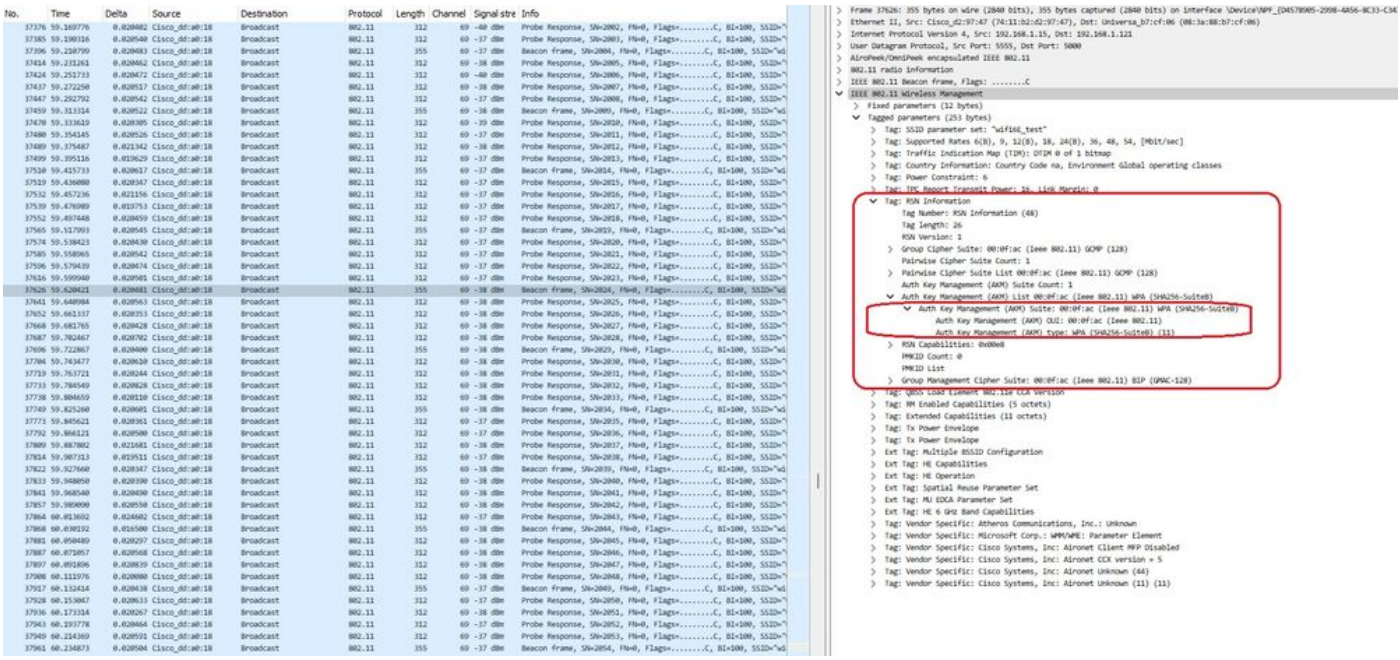
WPA3 Enterprise SuiteB-1X 보안 구성



참고: FT는 SUITEB-1X에서 지원되지 않습니다.

WLAN Security(WLAN 보안) 설정의 WLC GUI에서 보기:

비콘 OTA 확인:

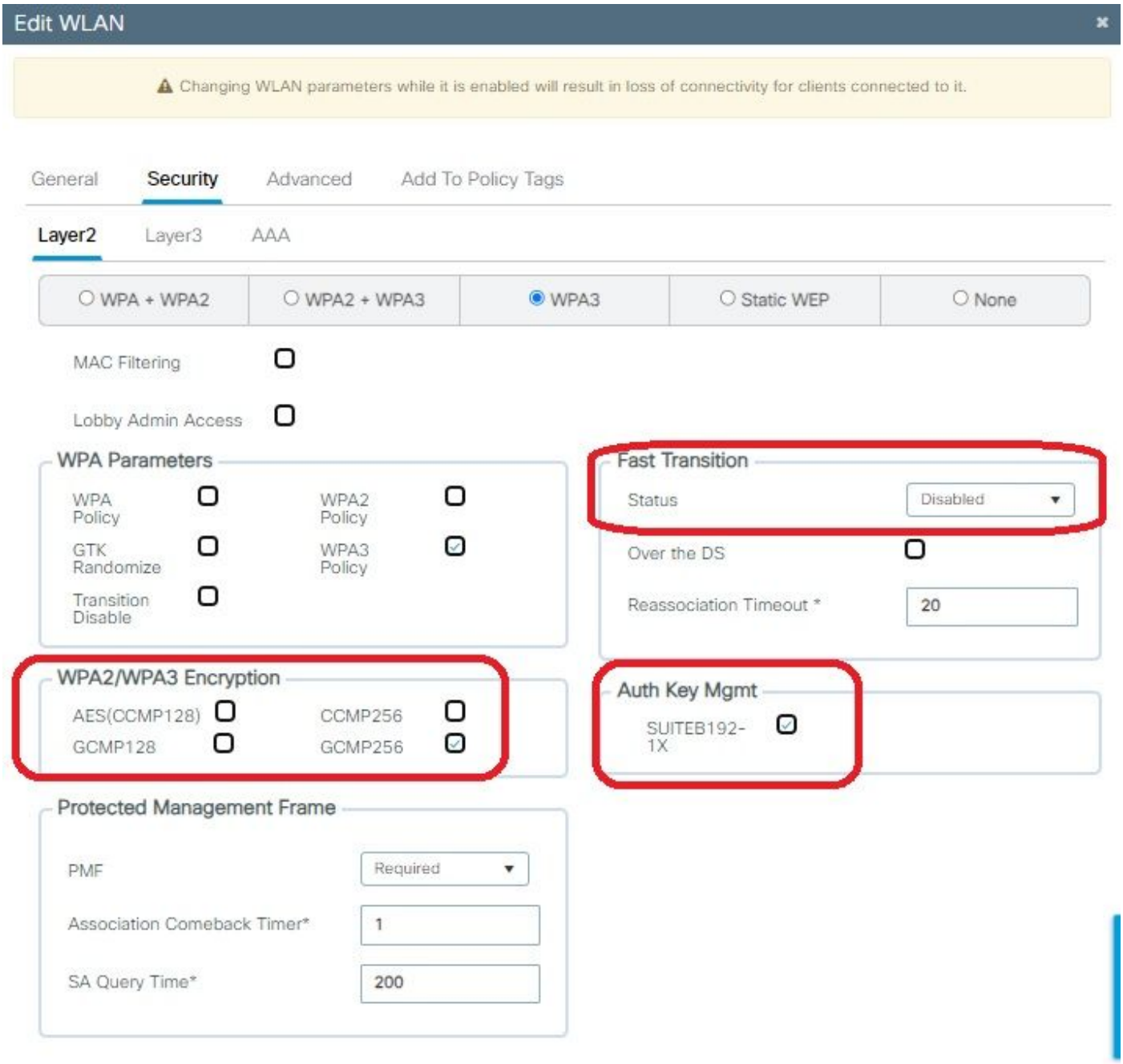


WPA3 Enterprise SuiteB-1X 비컨

테스트한 클라이언트 중 SuiteB-1X를 사용하여 WLAN에 연결할 수 있는 클라이언트가 없었으므로 이 보안 방법을 지원하는 클라이언트가 없었습니다.

WPA3-엔터프라이즈 + GCMP256 암호 + SUITEB192-1X

WLAN 보안 구성:



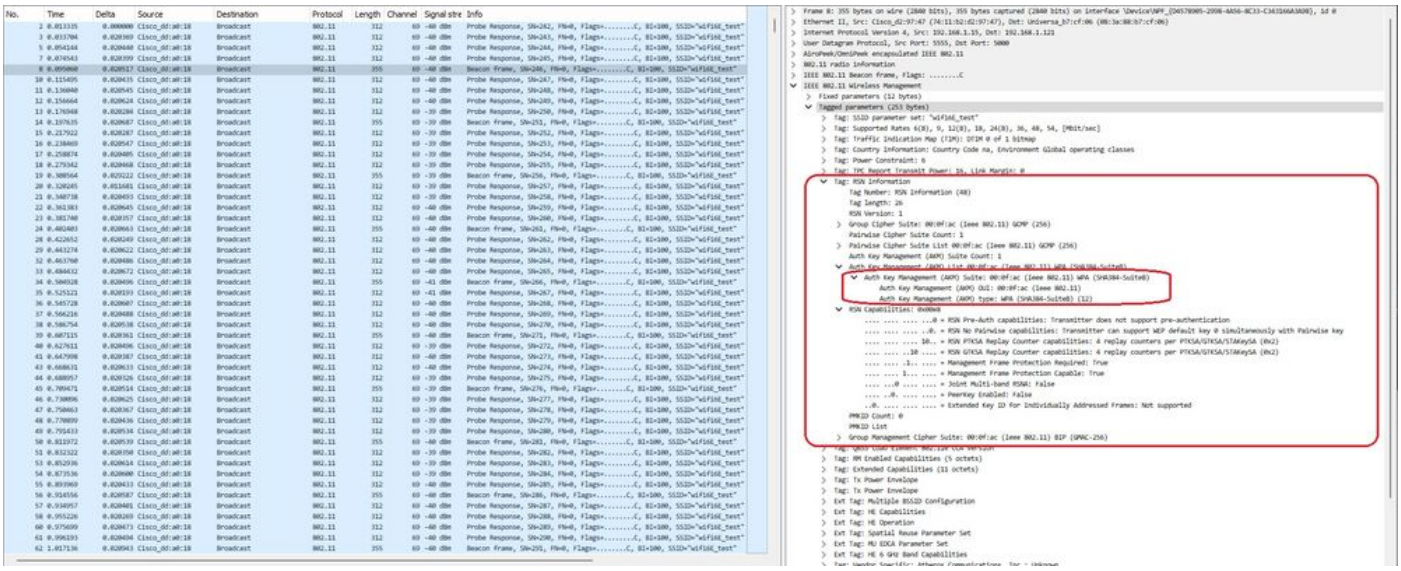
WPA3 Enterprise SUITE192-1x 보안 설정

참고: FT는 GCMP256+SUITEB192-1X에서 지원되지 않습니다.

WLC GUI WLAN 목록의 WLAN:

테스트에 사용되는 WLAN

비콘 OTA 확인:

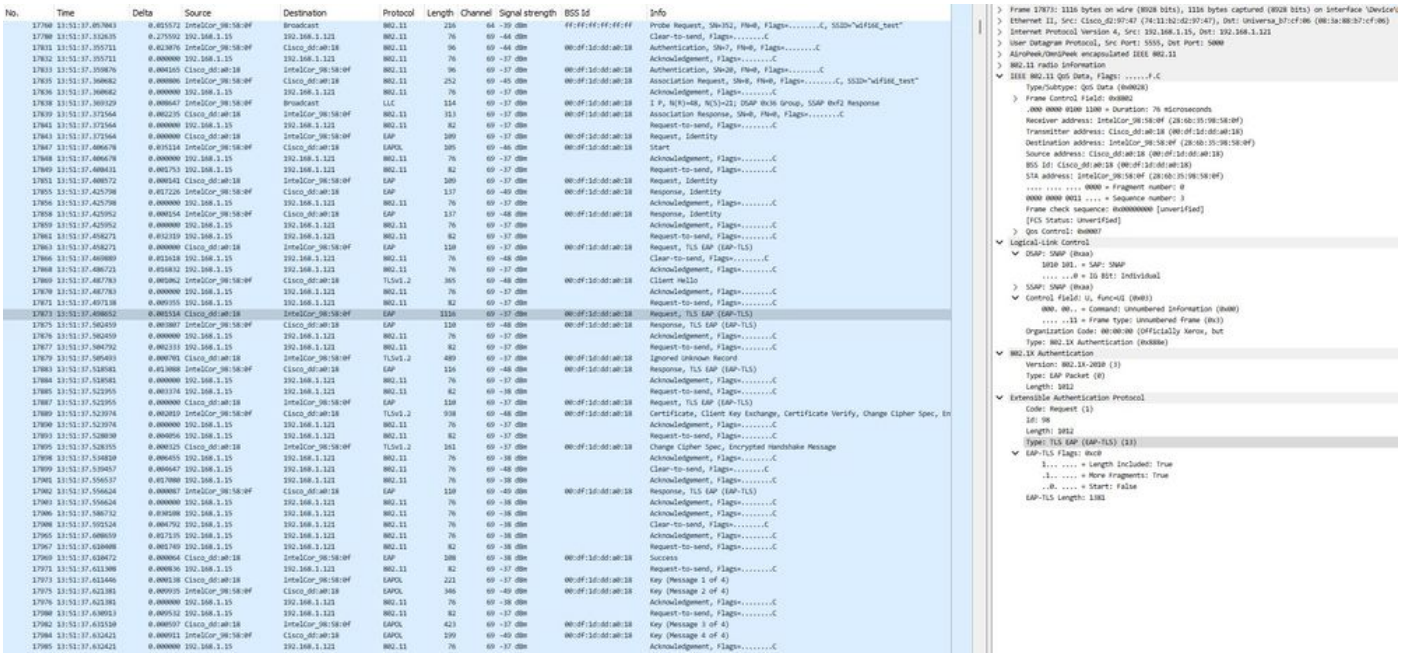


WPA3 Enterprise SUITE192-1x 비컨

여기서는 Wi-Fi 6E 클라이언트가 다음과 연결된 것을 관찰할 수 있습니다.

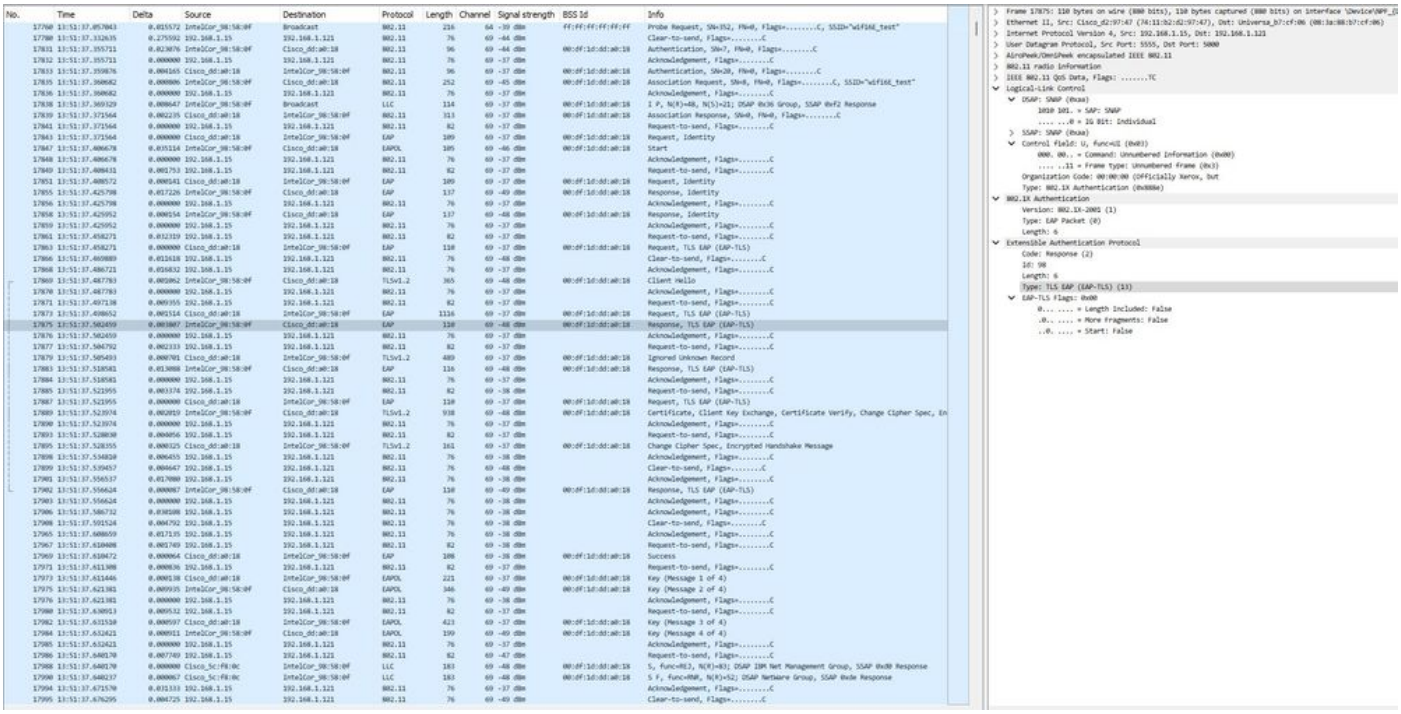
인텔 AX211

클라이언트의 RSN 정보에 중점을 둔 연결 OTA:



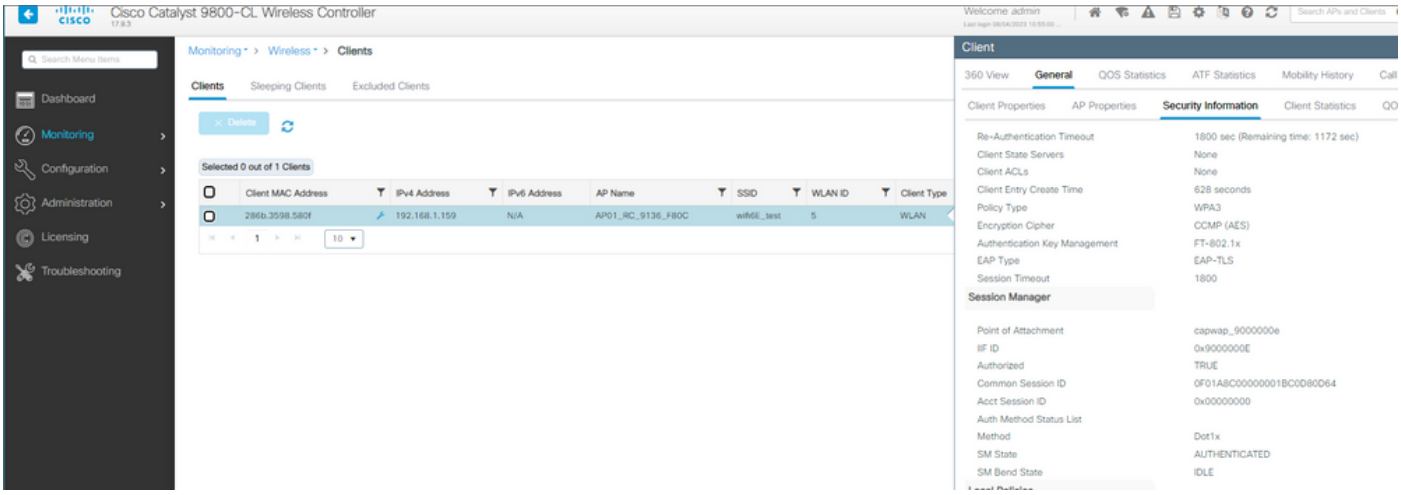
인텔 AX211 클라이언트 및 RSN 정보와 EAP-TLS가 연결된 WPA3 엔터프라이즈

EAP-TLS 교환:



인텔 AX211 클라이언트 및 EAP-TLS 주안점과 EAP-TLS가 연결된 WPA3 엔터프라이즈

WLC의 클라이언트 세부사항:



EAP-TLS 클라이언트 세부 정보가 있는 WPA3 Enterprise

넷기어 A8000

이 클라이언트에서는 WPA3-Enterprise가 지원되지 않습니다.

픽셀 6a

이 문서를 작성한 날짜에는 이 클라이언트가 EAP-TLS를 사용하여 WPA3 Enterprise에 연결할 수 없습니다.

이 문제는 현재 작업 중인 고객 측 문제였으며, 해결되는 대로 이 문서를 업데이트해야 합니다.

삼성 S23

이 문서를 작성한 날짜에는 이 클라이언트가 EAP-TLS를 사용하여 WPA3 Enterprise에 연결할 수 없습니다.

이 문제는 현재 작업 중인 고객 측 문제였으며, 해결되는 대로 이 문서를 업데이트해야 합니다.

보안 결론

이전의 모든 테스트 결과, 다음과 같은 결론이 도출되었습니다.

프로토콜	암호화	AKM	AKM 암호	EAP 방법	FT-오버타	FT-OverDS	인텔 AX211	삼성/구글 안드로이드	넷기어 A8000
빌린돈	AES-CCMP128	빌린 돈	나.	나.	해당 없음	해당 없음	지원됨	지원됨	지원됨
새우	AES-CCMP128	SAE(H2E만 해당)	SHA256	나.	지원됨	지원됨	지원됨: H2E 전용 및 FT-oTA	지원됨: H2E 전용. FT 실패. FT-oDS에 실패했습니다.	지원되는 항목: H2E 전용 및 FT-oTA FT-oDS에 실패했습니다.
엔터프라이즈	AES-CCMP128	802.1x-SHA256	SHA256	PEAP/FAST/TLS	지원됨	지원됨	지원됨: SHA256 및 FT-oTA/oDS 지원되지 않음: EAP-FAST	지원됨: SHA256 및 FT-oTA, FT-oDS(S23) 지원되지 않음: EAP-FAST, FT-oDS(Pixel6a)	지원됨: SHA256 및 FT-oTA 지원되지 않음: EAP-FAST, FT-oDS.
엔터	GCMP128	제품군B-1x	SHA256-SuiteB	PEAP/FAST/TLS	지원	지원되지 않음	지원되지 않음	지원되지 않음	지원되지 않음

프라이즈					되지 않음				
엔터프라이즈	GCMP256	스위트B-192	SHA384-SuiteB	TLS	지원되지 않음	지원되지 않음	해당 없음/미정	해당 없음/미정	지원되지 않음

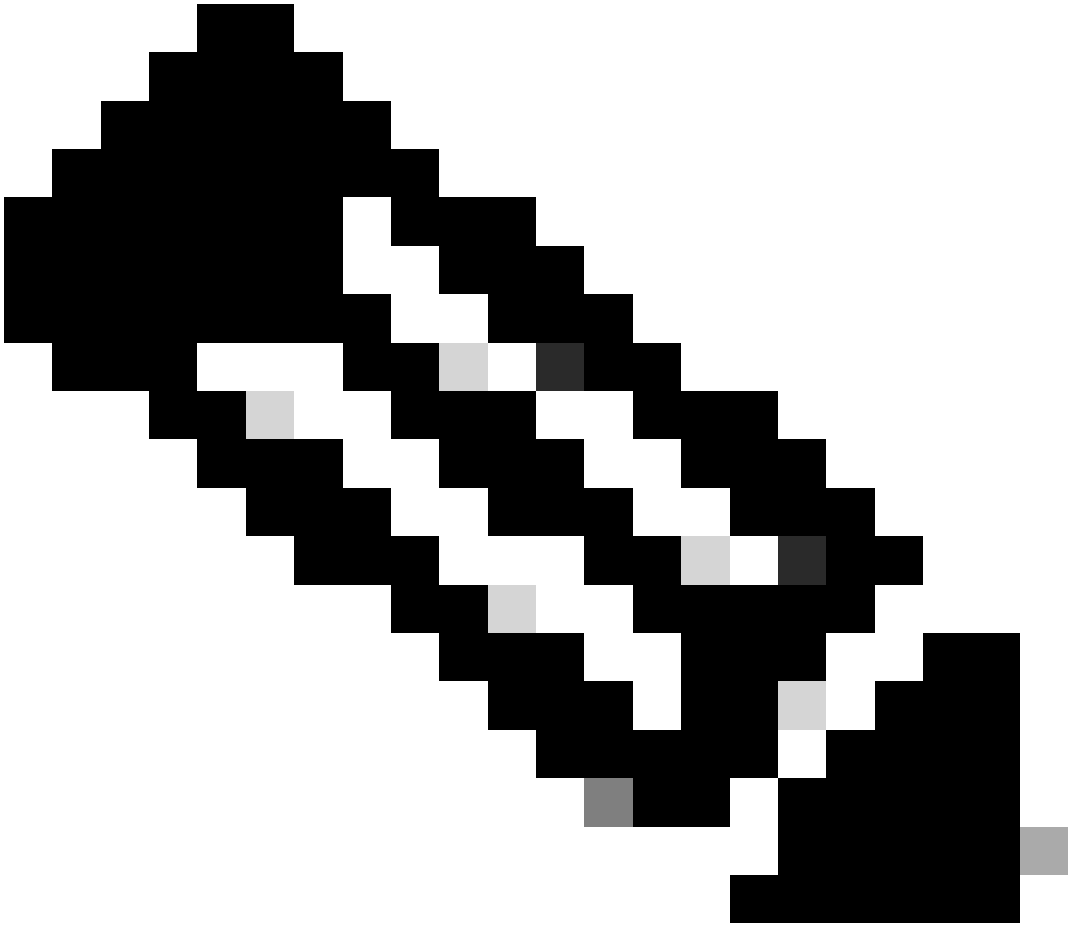
문제 해결

이 문서에서 사용된 문제 해결은 온라인 문서를 기반으로 합니다.

[COS AP 문제 해결]

트러블슈팅에 대한 일반적인 지침은 클라이언트가 임의 MAC 주소가 아닌 장치 MAC을 사용하여 연결하는지 확인하기 위해 클라이언트 MAC 주소를 사용하여 WLC에서 디버그 모드에서 RA 추적을 수집하는 것입니다.

무선 문제 해결의 경우 클라이언트 서비스 AP의 채널에서 트래픽을 캡처하는 스니퍼 모드에서 AP를 사용하는 것이 좋습니다.



참고: debug 명령을 사용하기 전에 Debug 명령에 대한 중요 정보를 참조하십시오.

관련 정보

Wi-Fi 6E란?

Wi-Fi 6과 Wi-Fi 6E의 비교

Wi-Fi 6E 한눈에 보기

Wi-Fi 6E: Wi-Fi 백서의 다음 장

Cisco Live - Catalyst Wi-Fi 6E 액세스 포인트를 사용한 차세대 무선 네트워크 아키텍처

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.