

Wi-Fi 6E WLAN Layer 2 보안 구성 및 확인

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[Wi-Fi 6E 보안](#)

[WPA3](#)

[레벨 세트: WPA3 모드](#)

[Cisco Catalyst Wi-Fi 6E AP](#)

[클라이언트 지원 보안 설정](#)

[구성](#)

[네트워크 다이어그램](#)

[설정](#)

[기본 컨피그레이션](#)

[다음을 확인합니다.](#)

[보안 확인](#)

[WPA3 - AES\(CCMP128\) + 부채](#)

[WPA3 - AES\(CCMP128\) + 전환 모드로 인한 부담](#)

[WPA3-개인 - AES\(CCMP128\) + SAE](#)

[WPA3-개인 - AES\(CCMP128\) + SAE + FT](#)

[WPA3-엔터프라이즈 + AES\(CCMP128\) + 802.1x-SHA256 + FT](#)

[WPA3-엔터프라이즈 + GCMP128 암호 + SUITEB-1X](#)

[WPA3-엔터프라이즈 + GCMP256 암호 + SUITEB192-1X](#)

[보안 결론](#)

[문제 해결](#)

[관련 정보](#)

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/WPA3 Encryption

AES(CCMP128) <input checked="" type="checkbox"/>	CCMP256 <input type="checkbox"/>
GCMP128 <input type="checkbox"/>	GCMP256 <input type="checkbox"/>

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.

Protected Management Frame

PMF

Required



Association Comeback Timer*

1

SA Query Time*

200

PMF 옵션

인증 키 관리

다음은 17.9.x 버전에서 사용할 수 있는 AKM 옵션입니다.

Auth Key Mgmt

SAE FT + SAE

OWE FT + 802.1x

802.1x-
SHA256

Anti Clogging Threshold*

Max Retries*

Retransmit Timeout*

PSK Format

PSK Type

Pre-Shared Key*

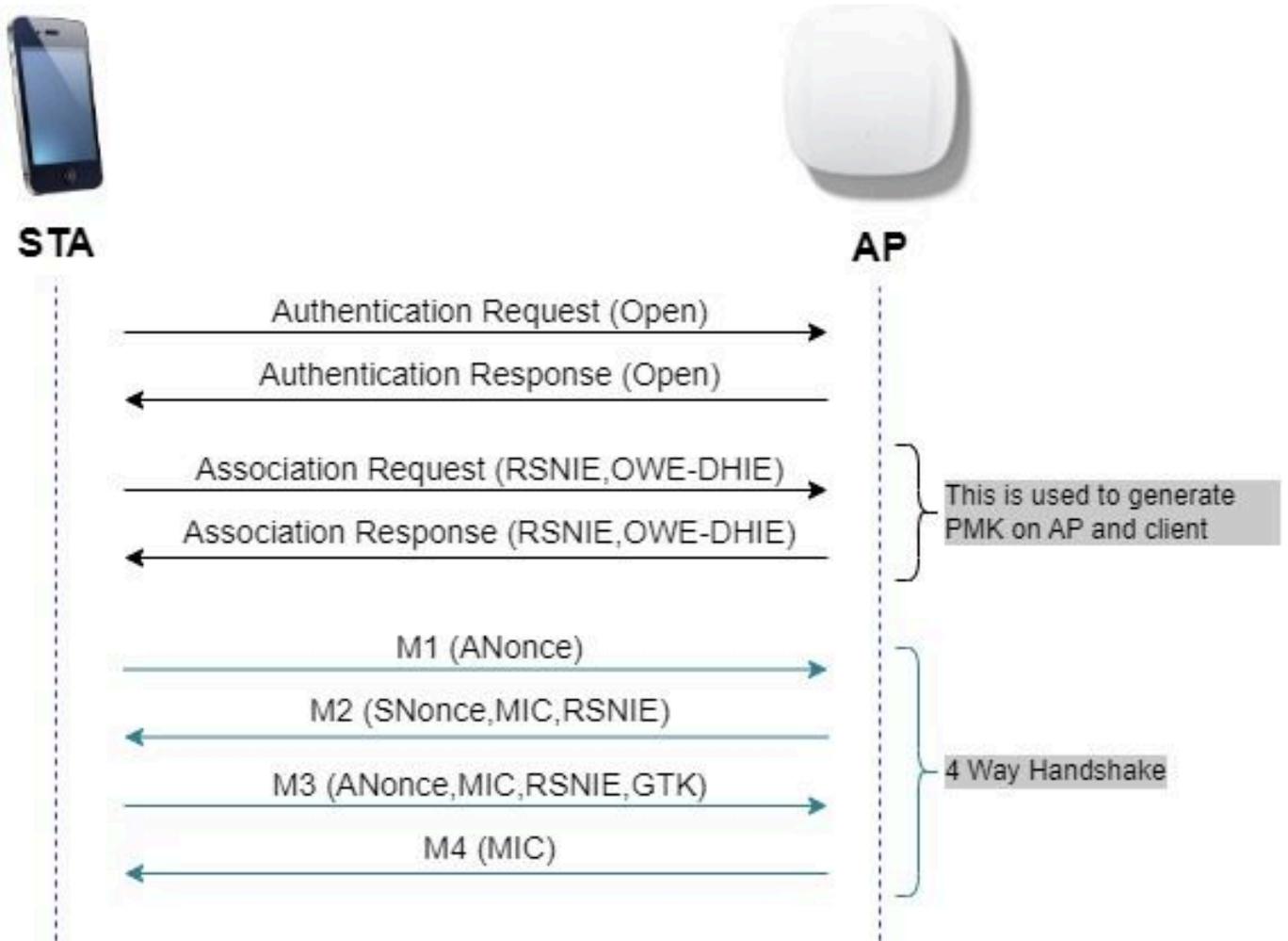
SAE Password Element ⓘ

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.

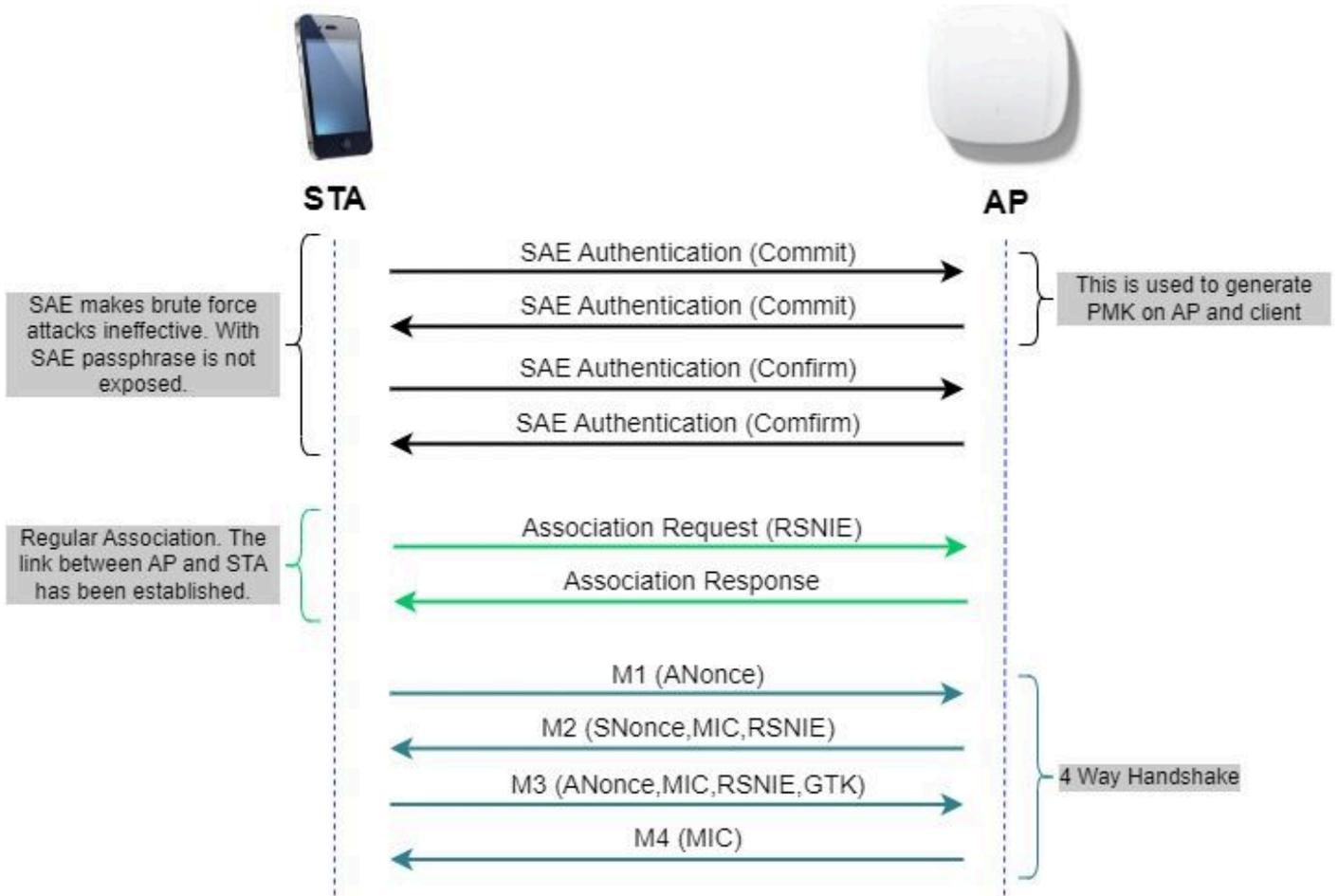
WPA3 및 Wi-Fi 6E에서는 H2E를 사용하는 SAE가 필수입니다.

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)

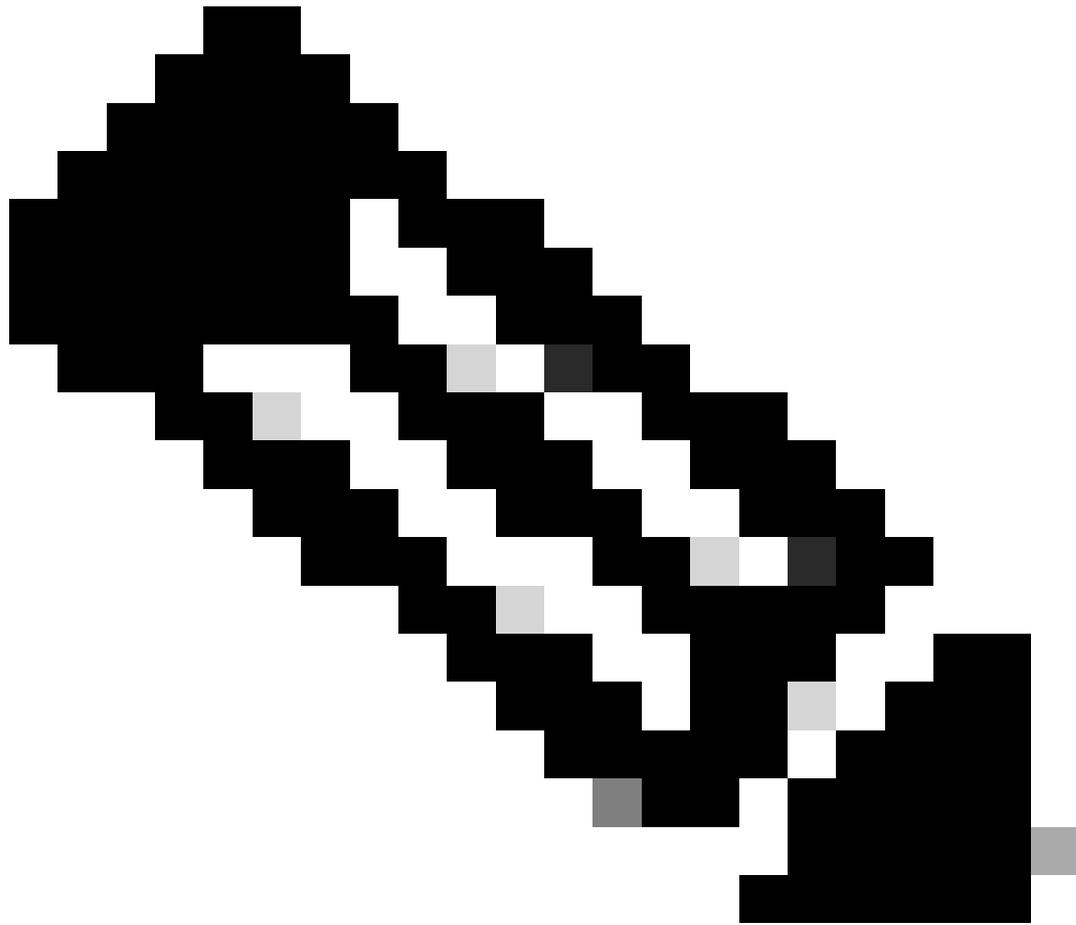
H2E(Hash-to-Element)는 새로운 PWE(SAE Password Element) 메서드입니다. 이 방법에서, SAE 프로토콜에서 사용되는 비밀 PWE는 비밀번호로부터 생성된다.

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.

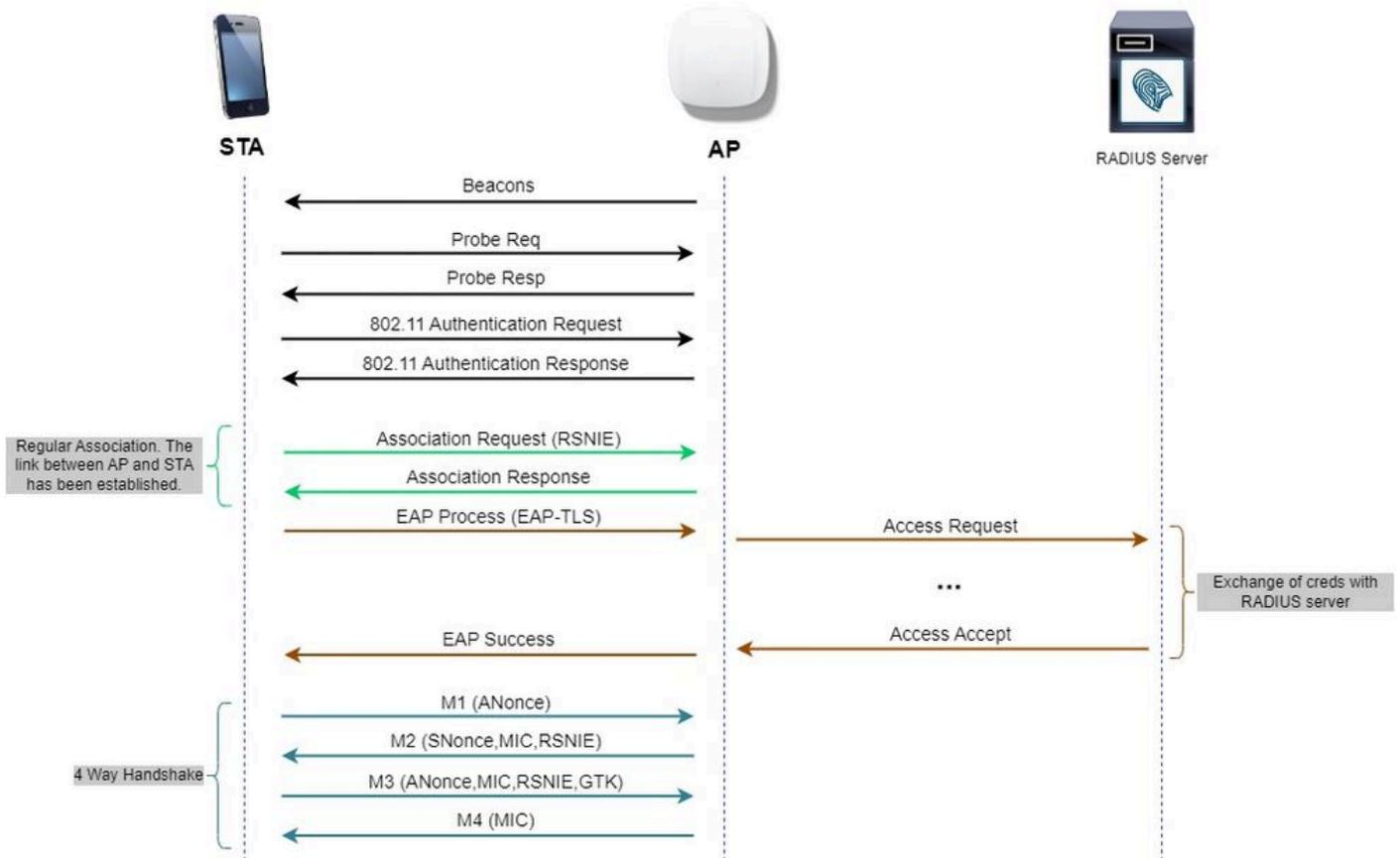
- 비밀번호에서 PT(Secret Intermediate Element) 파생입니다. 이 작업은 지원되는 각 그룹에 대해 디바이스에서 비밀번호가 처음 구성된 경우 오프라인으로 수행할 수 있습니다.
- 저장된 PT에서 PWE 유도. 이는 협상된 그룹 및 피어의 MAC 주소에 따라 다릅니다. 이 작업은 SAE 교환 중에 실시간으로 수행됩니다.



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 가이드를 참조하십시오.](#)

Cisco Catalyst Wi-Fi 6E AP

Ideal for Small to Medium-sized deployments	Best In Class, Flexibility		Mission Critical, Performance
 <p>CW9162</p> <ul style="list-style-type: none"> • 2x2 + 2x2 + 2x2 • 2.5 Gbps mGig • Power Options: PoE, DC Power • IoT ready + Bluetooth 5.x • Partial iCAP • USB - 4.5 W <p><small>Available with IOS-XE 17.9.2</small></p>	 <p>CW9164</p> <ul style="list-style-type: none"> • 2x2, 4x4, 4x4 • 2.5 Gbps mGig • Power Options: PoE, DC Power • IoT Ready + Bluetooth 5.x • Partial iCAP • USB- 4.5 W 	 <p>CW9166</p> <ul style="list-style-type: none"> • 4x4 + 4x4 + 4x4 (XOR 5/6) • 5 Gbps mGig • Power Options: PoE, DC Power • IoT ready + Bluetooth 5.x • Environmental Sensor • Full Packet Capture (iCAP) • Zero-Wait DFS* • USB - 4.5W 	 <p>C9136</p> <ul style="list-style-type: none"> • 4x4, 8x8, 4x4 (or) 4x4, 4x4+4x4, 4x4 • Dual 5 Gbps mGig, active fail over • PoE Redundancy • IoT ready • Bluetooth 5.x • Environmental Sensor • Full Packet Capture (iCAP) • Zero-Wait DFS* • USB - 9W <p><small>*Available in Future</small></p>
Full radio capability (6 GHz @ LPI) on single 30W PoE+			
Dedicated Radio for CleanAir Pro	Same Bracket, Industrial Design	AP Power Optimization	USB

Wi-Fi 6E 액세스 포인트

클라이언트 지원 보안 설정

WiFi Alliance 웹 페이지 제품 찾기를 사용하여 WPA3-Enterprise를 지원하는 제품을 찾을 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_eda979fbdede064\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\mtknhvux.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:



None

Enhanced Open

WEP

WPA/WPA2-Personal

WPA3-Personal

WPA/WPA2-Enterprise

WPA3-Enterprise

WPA3-Enterprise 192-bit



CIF



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:

The screenshot displays a Wireshark capture of a WLAN security handshake. The packet list on the left shows a series of 802.11 frames. The packet details pane on the right provides a detailed view of the Authentication and Association Request frames, including fields like SSID, capabilities, and cipher suite information.

WPA3 SAE + FT 비전

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

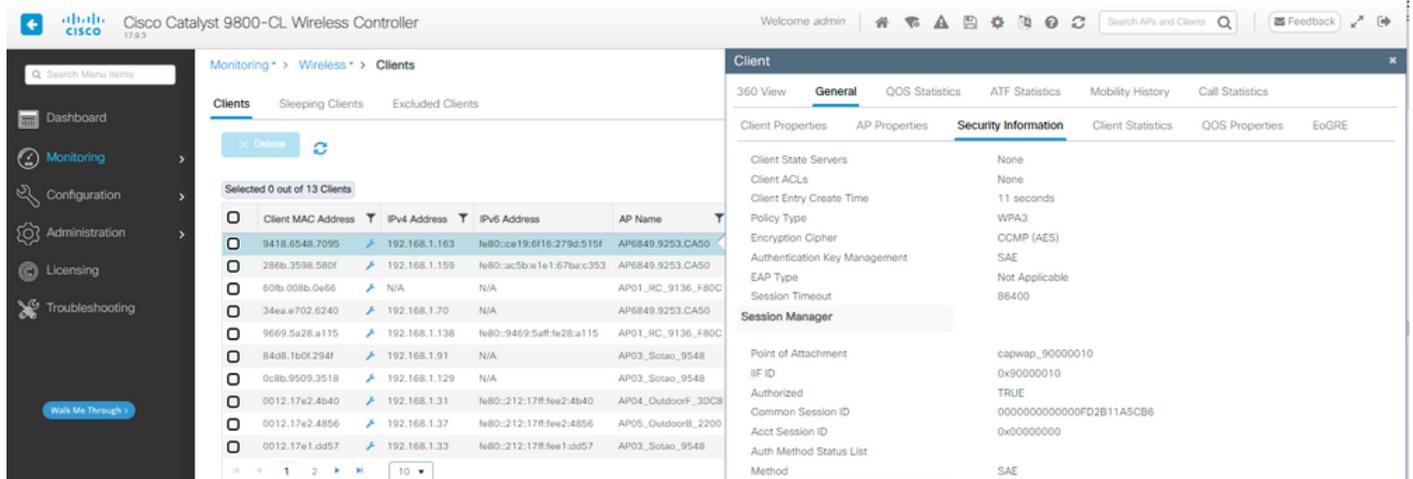
인텔 AX211

클라이언트의 RSN 정보에 중점을 둔 연결 OTA:

The screenshot displays a Wireshark capture of a WLAN security handshake. The packet list on the left shows a series of 802.11 frames. The packet details pane on the right provides a detailed view of the Authentication and Association Request frames, including fields like SSID, capabilities, and cipher suite information.

PMKID를 볼 수 있는 로깅 이벤트:

WLC의 클라이언트 세부사항:



픽셀 6a

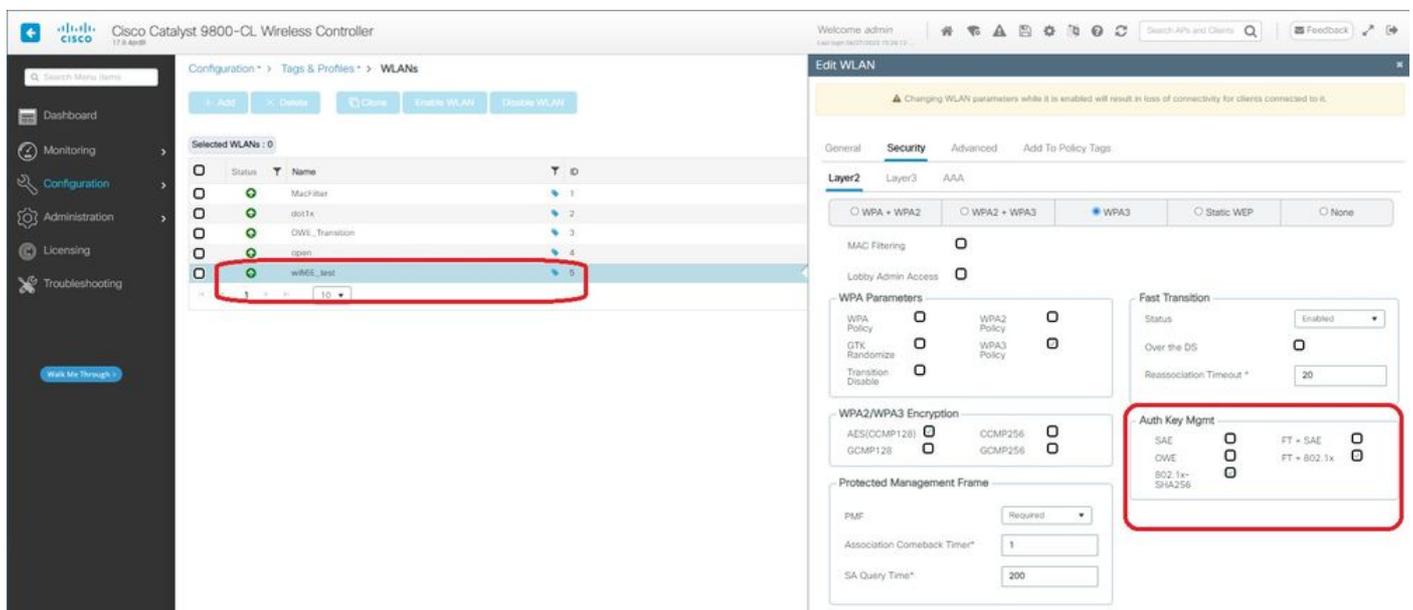
FT가 사용하도록 설정된 경우 디바이스에서 로밍할 수 없습니다.

삼성 S23

FT가 사용하도록 설정된 경우 디바이스에서 로밍할 수 없습니다.

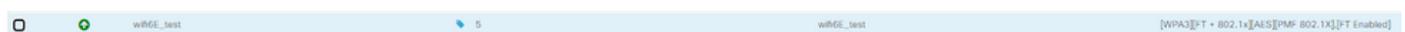
WPA3-엔터프라이즈 + AES(CCMP128) + 802.1x-SHA256 + FT

WLAN 보안 구성:



WPA3 Enterprise 802.1x-SHA256 + FT WLAN 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
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			0	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			0	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			0	tantunes	94:18:65:48:70:95	Netgear-Device	WirelessDot...	WirelessDot...	PermitAccess		eWLC-9800-01
Jun 27, 2023 01:50:43.883 PM			0	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			0	tantunes	28:6B:35:98:58:0F	Intel-Device	WirelessDot...	WirelessDot...	PermitAccess		eWLC-9800-01

ISE 라이브 로그

Beacon OTA는 다음과 같습니다.

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
324	3.099802	0.000000	0.000000 Cisco_05:00:18	Broadcast	802.11	428	59	-36	Probe Request, SMO=04, PWR=, Flags=....., R1=000, SSID="wif6a_test", SSID+M1=card (Broadcast)
325	3.099802	0.000000	0.000000 Cisco_05:00:18	Broadcast	802.11	428	59	-36	Probe Response, SMO=04, PWR=, Flags=....., R1=000, SSID="wif6a_test", SSID+M1=card (Broadcast)
326	3.131568	0.000000	0.000000 Cisco_05:00:18	Broadcast	802.11	374	59	-36	Clear-to-send, Flags=....., R1=000, SSID="wif6a_test", SSID+M1=card (Broadcast)
327	3.132783	0.000000	0.000000 Cisco_05:00:18	Broadcast	802.11	428	59	-36	Beacon Frame, SMO=04, PWR=, Flags=....., R1=000, SSID="wif6a_test", SSID+M1=card (Broadcast)

```

> Frame 327: 428 bytes on wire (344 bits), 428 bytes captured (344 bits) on interface DeviceVAP_04578900-2998-4636-8C13-CA1314
> Ethernet II, Src: Cisco_02:17:74:74:74:74 (08:00:0c:2c:17:74:74:74), Dst: Unknown_07:cf:06 (08:00:0c:07:cf:06)
> Internet Protocol Version 4, Src: 192.168.1.15, Dst: 192.168.1.121
> User Datagram Protocol, Src Port: 5555, Dst Port: 59000
> AlohaPcap/OnPcap encapsulated IEEE 802.11
> IEEE 802.11 wireless management
> IEEE 802.11 radio information
> Fixed parameters (12 bytes)
> Tagged parameters (120 bytes)
  > Tag: SSID parameter Set: "wif6a_test"
    > Tag: Supported Rates (8), 1, 2, 5.5, 11, 24, 36, 48, 54, 60, 66, 84, 96, 108, 120, 132, 144, 162, 180, 200, 216, 240, 270, 300, 360, 420, 480, 540, 600, 660, 720, 780, 840, 900, 960, 1080, 1200, 1320, 1440, 1560, 1680, 1800, 1920, 2040, 2160, 2280, 2400, 2520, 2640, 2760, 2880, 3000, 3120, 3240, 3360, 3480, 3600, 3720, 3840, 3960, 4080, 4200, 4320, 4440, 4560, 4680, 4800, 4920, 5040, 5160, 5280, 5400, 5520, 5640, 5760, 5880, 6000, 6120, 6240, 6360, 6480, 6600, 6720, 6840, 6960, 7080, 7200, 7320, 7440, 7560, 7680, 7800, 7920, 8040, 8160, 8280, 8400, 8520, 8640, 8760, 8880, 9000, 9120, 9240, 9360, 9480, 9600, 9720, 9840, 9960, 10080, 10200, 10320, 10440, 10560, 10680, 10800, 10920, 11040, 11160, 11280, 11400, 11520, 11640, 11760, 11880, 12000, 12120, 12240, 12360, 12480, 12600, 12720, 12840, 12960, 13080, 13200, 13320, 13440, 13560, 13680, 13800, 13920, 14040, 14160, 14280, 14400, 14520, 14640, 14760, 14880, 15000, 15120, 15240, 15360, 15480, 15600, 15720, 15840, 15960, 16080, 16200, 16320, 16440, 16560, 16680, 16800, 16920, 17040, 17160, 17280, 17400, 17520, 17640, 17760, 17880, 18000, 18120, 18240, 18360, 18480, 18600, 18720, 18840, 18960, 19080, 19200, 19320, 19440, 19560, 19680, 19800, 19920, 20040, 20160, 20280, 20400, 20520, 20640, 20760, 20880, 21000, 21120, 21240, 21360, 21480, 21600, 21720, 21840, 21960, 22080, 22200, 22320, 22440, 22560, 22680, 22800, 22920, 23040, 23160, 23280, 23400, 23520, 23640, 23760, 23880, 24000, 24120, 24240, 24360, 24480, 24600, 24720, 24840, 24960, 25080, 25200, 25320, 25440, 25560, 25680, 25800, 25920, 26040, 26160, 26280, 26400, 26520, 26640, 26760, 26880, 27000, 27120, 27240, 27360, 27480, 27600, 27720, 27840, 27960, 28080, 28200, 28320, 28440, 28560, 28680, 28800, 28920, 29040, 29160, 29280, 29400, 29520, 29640, 29760, 29880, 30000, 30120, 30240, 30360, 30480, 30600, 30720, 30840, 30960, 31080, 31200, 31320, 31440, 31560, 31680, 31800, 31920, 32040, 32160, 32280, 32400, 32520, 32640, 32760, 32880, 33000, 33120, 33240, 33360, 33480, 33600, 33720, 33840, 33960, 34080, 34200, 34320, 34440, 34560, 34680, 34800, 34920, 35040, 35160, 35280, 35400, 35520, 35640, 35760, 35880, 36000, 36120, 36240, 36360, 36480, 36600, 36720, 36840, 36960, 37080, 37200, 37320, 37440, 37560, 37680, 37800, 37920, 38040, 38160, 38280, 38400, 38520, 38640, 38760, 38880, 39000, 39120, 39240, 39360, 39480, 39600, 39720, 39840, 39960, 40080, 40200, 40320, 40440, 40560, 40680, 40800, 40920, 41040, 41160, 41280, 41400, 41520, 41640, 41760, 41880, 42000, 42120, 42240, 42360, 42480, 42600, 42720, 42840, 42960, 43080, 43200, 43320, 43440, 43560, 43680, 43800, 43920, 44040, 44160, 44280, 44400, 44520, 44640, 44760, 44880, 45000, 45120, 45240, 45360, 45480, 45600, 45720, 45840, 45960, 46080, 46200, 46320, 46440, 46560, 46680, 46800, 46920, 47040, 47160, 47280, 47400, 47520, 47640, 47760, 47880, 48000, 48120, 48240, 48360, 48480, 48600, 48720, 48840, 48960, 49080, 49200, 49320, 49440, 49560, 49680, 49800, 49920, 50040, 50160, 50280, 50400, 50520, 50640, 50760, 50880, 51000, 51120, 51240, 51360, 51480, 51600, 51720, 51840, 51960, 52080, 52200, 52320, 52440, 52560, 52680, 52800, 52920, 53040, 53160, 53280, 53400, 53520, 53640, 53760, 53880, 54000, 54120, 54240, 54360, 54480, 54600, 54720, 54840, 54960, 55080, 55200, 55320, 55440, 55560, 55680, 55800, 55920, 56040, 56160, 56280, 56400, 56520, 56640, 56760, 56880, 57000, 57120, 57240, 57360, 57480, 57600, 57720, 57840, 57960, 58080, 58200, 58320, 58440, 58560, 58680, 58800, 58920, 59040, 59160, 59280, 59400, 59520, 59640, 59760, 59880, 60000, 60120, 60240, 60360, 60480, 60600, 60720, 60840, 60960, 61080, 61200, 61320, 61440, 61560, 61680, 61800, 61920, 62040, 62160, 62280, 62400, 62520, 62640, 62760, 62880, 63000, 63120, 63240, 63360, 63480, 63600, 63720, 63840, 63960, 64080, 64200, 64320, 64440, 64560, 64680, 64800, 64920, 65040, 65160, 65280, 65400, 65520, 65640, 65760, 65880, 66000, 66120, 66240, 66360, 66480, 66600, 66720, 66840, 66960, 67080, 67200, 67320, 67440, 67560, 67680, 67800, 67920, 68040, 68160, 68280, 68400, 68520, 68640, 68760, 68880, 69000, 69120, 69240, 69360, 69480, 69600, 69720, 69840, 69960, 70080, 70200, 70320, 70440, 70560, 70680, 70800, 70920, 71040, 71160, 71280, 71400, 71520, 71640, 71760, 71880, 72000, 72120, 72240, 72360, 72480, 72600, 72720, 72840, 72960, 73080, 73200, 73320, 73440, 73560, 73680, 73800, 73920, 74040, 74160, 74280, 74400, 74520, 74640, 74760, 74880, 75000, 75120, 75240, 75360, 75480, 75600, 75720, 75840, 75960, 76080, 76200, 76320, 76440, 76560, 76680, 76800, 76920, 77040, 77160, 77280, 77400, 77520, 77640, 77760, 77880, 78000, 78120, 78240, 78360, 78480, 78600, 78720, 78840, 78960, 79080, 79200, 79320, 79440, 79560, 79680, 79800, 79920, 80040, 80160, 80280, 80400, 80520, 80640, 80760, 80880, 81000, 81120, 81240, 81360, 81480, 81600, 81720, 81840, 81960, 82080, 82200, 82320, 82440, 82560, 82680, 82800, 82920, 83040, 83160, 83280, 83400, 83520, 83640, 83760, 83880, 84000, 84120, 84240, 84360, 84480, 84600, 84720, 84840, 84960, 85080, 85200, 85320, 85440, 85560, 85680, 85800, 85920, 86040, 86160, 86280, 86400, 86520, 86640, 86760, 86880, 87000, 87120, 87240, 87360, 87480, 87600, 87720, 87840, 87960, 88080, 88200, 88320, 88440, 88560, 88680, 88800, 88920, 89040, 89160, 89280, 89400, 89520, 89640, 89760, 89880, 90000, 90120, 90240, 90360, 90480, 90600, 90720, 90840, 90960, 91080, 91200, 91320, 91440, 91560, 91680, 91800, 91920, 92040, 92160, 92280, 92400, 92520, 92640, 92760, 92880, 93000, 93120, 93240, 93360, 93480, 93600, 93720, 93840, 93960, 94080, 94200, 94320, 94440, 94560, 94680, 94800, 94920, 95040, 95160, 95280, 95400, 95520, 95640, 95760, 95880, 96000, 96120, 96240, 96360, 96480, 96600, 96720, 96840, 96960, 97080, 97200, 97320, 97440, 97560, 97680, 97800, 97920, 98040, 98160, 98280, 98400, 98520, 98640, 98760, 98880, 99000, 99120, 99240, 99360, 99480, 99600, 99720, 99840, 99960, 100080, 100200, 100320, 100440, 100560, 100680, 100800, 100920, 101040, 101160, 101280, 101400, 101520, 101640, 101760, 101880, 102000, 102120, 102240, 102360, 102480, 102600, 102720, 102840, 102960, 103080, 103200, 103320, 103440, 103560, 103680, 103800, 103920, 104040, 104160, 104280, 104400, 104520, 104640, 104760, 104880, 105000, 105120, 105240, 105360, 105480, 105600, 105720, 105840, 105960, 106080, 106200, 106320, 106440, 106560, 106680, 106800, 106920, 107040, 107160, 107280, 107400, 107520, 107640, 107760, 107880, 108000, 108120, 108240, 108360, 108480, 108600, 108720, 108840, 108960, 109080, 109200, 109320, 109440, 109560, 109680, 109800, 109920, 110040, 110160, 110280, 110400, 110520, 110640, 110760, 110880, 111000, 111120, 111240, 111360, 111480, 111600, 111720, 111840, 111960, 112080, 112200, 112320, 112440, 112560, 112680, 112800, 112920, 113040, 113160, 113280, 113400, 113520, 113640, 113760, 113880, 114000, 114120, 114240, 114360, 114480, 114600, 114720, 114840, 114960, 115080, 115200, 115320, 115440, 115560, 115680, 115800, 115920, 116040, 116160, 116280, 116400, 116520, 116640, 116760, 116880, 117000, 117120, 117240, 117360, 117480, 117600, 117720, 117840, 117960, 118080, 118200, 118320, 118440, 118560, 118680, 118800, 118920, 119040, 119160, 119280, 119400, 119520, 119640, 119760, 119880, 120000, 120120, 120240, 120360, 120480, 120600, 120720, 120840, 120960, 121080, 121200, 121320, 121440, 121560, 121680, 121800, 121920, 122040, 122160, 122280, 122400, 122520, 122640, 122760, 122880, 123000, 123120, 123240, 123360, 123480, 123600, 123720, 123840, 123960, 124080, 124200, 124320, 124440, 124560, 124680, 124800, 124920, 125040, 125160, 125280, 125400, 125520, 125640, 125760, 125880, 126000, 126120, 126240, 126360, 126480, 126600, 126720, 126840, 126960, 127080, 127200, 127320, 127440, 127560, 127680, 127800, 127920, 128040, 128160, 128280, 128400, 128520, 128640, 128760, 128880, 129000, 129120, 129240, 129360, 129480, 129600, 129720, 129840, 129960, 130080, 130200, 130320, 130440, 130560, 130680, 130800, 130920, 131040, 131160, 131280, 131400, 131520, 131640, 131760, 131880, 132000, 132120, 132240, 132360, 132480, 132600, 132720, 132840, 132960, 133080, 133200, 133320, 133440, 133560, 133680, 133800, 133920, 134040, 134160, 134280, 134400, 134520, 134640, 134760, 134880, 135000, 135120, 135240, 135360, 135480, 135600, 135720, 135840, 135960, 136080, 136200, 136320, 136440, 136560, 136680, 136800, 136920, 137040, 137160, 137280, 137400, 137520, 137640, 137760, 137880, 138000, 138120, 138240, 138360, 138480, 138600, 138720, 138840, 138960, 139080, 139200, 139320, 139440, 139560, 139680, 139800, 139920, 140040, 140160, 140280, 140400, 140520, 140640, 140760, 140880, 141000, 141120, 141240, 141360, 141480, 141600, 141720, 141840, 141960, 142080, 142200, 142320, 142440, 142560, 142680, 142800, 142920, 143040, 143160, 143280, 143400, 143520, 143640, 143760, 143880, 144000, 144120, 144240, 144360, 144480, 144600, 144720, 144840, 144960, 145080, 145200, 145320, 145440, 145560, 145680, 145800, 145920, 146040, 146160, 146280, 146400, 146520, 146640, 146760, 146880, 147000, 147120, 147240, 147360, 147480, 147600, 147720, 147840, 147960, 148080, 148200, 148320, 148440, 148560, 148680, 148800, 148920, 149040, 149160, 149280, 149400, 149520, 149640, 149760, 149880, 150000, 150120, 150240, 150360, 150480, 150600, 150720, 150840, 150960, 151080, 151200, 151320, 151440, 151560, 151680, 151800, 151920, 152040, 152160, 152280, 152400, 152520, 152640, 152760, 152880, 153000, 153120, 153240, 153360, 153480, 153600, 153720, 153840, 153960, 154080, 154200, 154320, 154440, 154560, 154680, 154800, 154920, 155040, 155160, 155280, 155400, 155520, 155640, 155760, 155880, 156000, 156120, 156240, 156360, 156480, 156600, 156720, 156840, 156960, 157080, 157200, 157320, 157440, 157560, 157680, 157800, 157920, 158040, 1
```

라이언트는 연결 해제 프레임 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.

The image shows a Wireshark packet capture analysis of a client's connection attempt. The main pane displays a list of frames with annotations:

- Probing and authentication frames:** Frames 104-110, including Probe Request, Probe Response, Clear-to-send, Authentication, and Authentication Success.
- Regular Association:** Frames 111-118, including Request, Identity, Probe Response, Request, Protected EAP, and Request-to-send.
- EAP Exchange:** Frames 119-124, including Request, Protected EAP, Change Cipher Spec, and Response, Protected EAP.
- 4 Way Handshake:** Frames 125-130, including Key Message 1, 2, 3, and 4.

A detailed view of the EAP Exchange (frames 119-124) is shown on the right, highlighting the PMKID used for FT (Fast Transition) in the Group Management (GM) list.

WPA3 Enterprise 802.1x + FT Ax211 연결 흐름

WLC의 클라이언트 세부사항:

The screenshot shows the Cisco WLC Client Configuration page for a client with MAC address 286b.3598.5801. The 'Security Information' tab is selected, displaying the following configuration:

- Re-authentication Timeout: 1800 sec (Remaining time: 462 sec)
- Client State Servers: None
- Client ACLs: None
- Client Entry Create Time: 1338 seconds
- Policy Type: WPA3
- Encryption Cipher: CCMP (AES)
- Authentication Key Management: FT-802.1x
- EAP Type: PEAP
- Session Timeout: 1800

WPA3 Enterprise 802.1x + FT 클라이언트 세부사항

이 클라이언트는 DS를 통해 FT를 사용하여 테스트되었으며 802.11r를 사용하여 로밍할 수 있습니다.

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
878	1.408897	0.263322	Cisco_08:a0:18	Broadcast	802.11	428	69-17	dbm	Beacon frame, SN=3685, PWR=, Flags=.....C, BI=100, SSID=W
879	1.409037	0.143270	Cisco_72:8a:56	Broadcast	802.11	204	69-17	dbm	Probe Request, SN=3685, PWR=, Flags=.....C, SSID=Wifi6a, S
880	1.563162	0.000405	Cisco_08:a0:18	Broadcast	802.11	428	69-17	dbm	Beacon frame, SN=3685, PWR=, Flags=.....C, BI=100, SSID=W
882	1.564878	0.000716	Cisco_08:a0:18	Broadcast	802.11	374	69-17	dbm	Probe Response, SN=3685, PWR=, Flags=.....C, BI=100, SSID=W
928	1.675576	0.114498	Cisco_08:a0:18	Broadcast	802.11	428	69-17	dbm	Beacon frame, SN=3685, PWR=, Flags=.....C, BI=100, SSID=W
932	1.675989	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-17	dbm	Authentication, SN=0111, PWR=, Flags=.....C
933	1.675989	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-17	dbm	Acknowledgment, Flags=.....C
923	1.679651	0.003842	Cisco_08:a0:18	Broadcast	802.11	108	69-17	dbm	Authentication, SN=14, PWR=, Flags=.....C
924	1.679651	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-17	dbm	Acknowledgment, Flags=.....C
925	1.682828	0.000000	192.168.1.15	192.168.1.122	802.11	284	69-17	dbm	Association Request, SN=0002, PWR=, Flags=.....C, SSID=Wifi6a
926	1.682181	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-17	dbm	Acknowledgment, Flags=.....C
930	1.782511	0.023970	Cisco_08:a0:18	Google_72:8a:56	802.11	313	69-17	dbm	Association Request, SN=0, PWR=, Flags=.....C
931	1.782511	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-13	dbm	Acknowledgment, Flags=.....C
932	1.782629	0.000620	Google_72:8a:56	Google_72:8a:56	EAP	309	69-17	dbm	Request, Identity
933	1.782629	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-11	dbm	Acknowledgment, Flags=.....C
939	1.747377	0.017007	Google_72:8a:56	Cisco_08:a0:18	EAP	137	69-13	dbm	Response, Identity
940	1.747377	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-17	dbm	Acknowledgment, Flags=.....C
942	1.784244	0.012047	Cisco_08:a0:18	Google_72:8a:56	EAP	110	69-17	dbm	Request, Protected EAP (EAP-PEAP)
943	1.784244	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-11	dbm	Acknowledgment, Flags=.....C
945	1.788956	0.005672	Cisco_08:a0:18	Broadcast	802.11	428	69-17	dbm	Beacon frame, SN=3685, PWR=, Flags=.....C, BI=100, SSID=W
946	1.788956	0.000180	Google_72:8a:56	Google_72:8a:56	LIC	124	69-17	dbm	1, N(1)=0, N(5)=; SOAP Error Individual, SOAP NameSpace
949	1.794517	0.018971	Google_72:8a:56	Cisco_08:a0:18	802.11	241	69-17	dbm	Client Hello
950	1.794517	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-17	dbm	Acknowledgment, Flags=.....C
956	1.794529	0.015081	Cisco_08:a0:18	Google_72:8a:56	EAP	1116	69-17	dbm	Request, Protected EAP (EAP-PEAP)
957	1.794529	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-10	dbm	Acknowledgment, Flags=.....C
958	1.797058	0.002510	Google_72:8a:56	Cisco_08:a0:18	EAP	110	69-19	dbm	Response, Protected EAP (EAP-PEAP)
959	1.797058	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-17	dbm	Acknowledgment, Flags=.....C
960	1.801724	0.004656	Cisco_08:a0:18	Google_72:8a:56	802.11	382	69-17	dbm	Ignored Unknown Record
961	1.801724	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-19	dbm	Acknowledgment, Flags=.....C
963	1.820673	0.018709	Google_72:8a:56	Cisco_08:a0:18	802.11	236	69-17	dbm	Client key exchange, Change Cipher Spec, Encrypted Handshake M
964	1.820673	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-17	dbm	Acknowledgment, Flags=.....C
965	1.820990	0.003327	Cisco_08:a0:18	Google_72:8a:56	802.11	161	69-17	dbm	Change Cipher Spec, Encrypted Handshake Message
966	1.820990	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-19	dbm	Acknowledgment, Flags=.....C
968	1.820990	0.004229	Google_72:8a:56	Cisco_08:a0:18	EAP	110	69-19	dbm	Response, Protected EAP (EAP-PEAP)
969	1.820990	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-17	dbm	Acknowledgment, Flags=.....C
971	1.811178	0.003900	Cisco_08:a0:18	Google_72:8a:56	802.11	144	69-17	dbm	Application data
972	1.811178	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-19	dbm	Acknowledgment, Flags=.....C
973	1.817128	0.004150	Google_72:8a:56	Cisco_08:a0:18	802.11	132	69-19	dbm	Application data
974	1.817128	0.000078	192.168.1.15	192.168.1.122	802.11	76	69-17	dbm	Acknowledgment, Flags=.....C
976	1.840795	0.003200	Cisco_08:a0:18	Google_72:8a:56	802.11	171	69-17	dbm	Application data
977	1.840795	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-19	dbm	Acknowledgment, Flags=.....C
978	1.845522	0.004817	Google_72:8a:56	Cisco_08:a0:18	802.11	206	69-19	dbm	Application data
979	1.845522	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-17	dbm	Acknowledgment, Flags=.....C
984	1.848494	0.018072	Cisco_08:a0:18	Google_72:8a:56	802.11	190	69-17	dbm	Application data
985	1.848494	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-19	dbm	Acknowledgment, Flags=.....C
986	1.866887	0.002135	Google_72:8a:56	Cisco_08:a0:18	802.11	145	69-19	dbm	Application data
987	1.866887	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-17	dbm	Acknowledgment, Flags=.....C
988	1.870858	0.003771	Cisco_08:a0:18	Broadcast	802.11	428	69-17	dbm	Beacon frame, SN=3687, PWR=, Flags=.....C, BI=100, SSID=W
989	1.870858	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-17	dbm	Acknowledgment, Flags=.....C
990	1.870858	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-19	dbm	Acknowledgment, Flags=.....C
992	1.877128	0.006470	Google_72:8a:56	Cisco_08:a0:18	EAP	110	69-18	dbm	Response, Protected EAP (EAP-PEAP)
993	1.877128	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-17	dbm	Acknowledgment, Flags=.....C
996	1.920065	0.002917	Cisco_08:a0:18	Google_72:8a:56	802.11	108	69-17	dbm	Success
997	1.920065	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-19	dbm	Acknowledgment, Flags=.....C
998	1.920065	0.000000	Cisco_08:a0:18	Google_72:8a:56	EAPOL	223	69-17	dbm	Key (Message 1 of 4)
999	1.920065	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-19	dbm	Acknowledgment, Flags=.....C
1000	1.920255	0.000000	Cisco_08:a0:18	Google_72:8a:56	EAPOL	346	69-18	dbm	Key (Message 2 of 4)
1001	1.920255	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-17	dbm	Acknowledgment, Flags=.....C
1004	1.920677	0.003422	Cisco_08:a0:18	Google_72:8a:56	EAPOL	423	69-17	dbm	Key (Message 3 of 4)
1005	1.920677	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-19	dbm	Acknowledgment, Flags=.....C
1006	1.920886	0.000209	Google_72:8a:56	Cisco_08:a0:18	EAPOL	199	69-19	dbm	Key (Message 4 of 4)
1007	1.920886	0.000000	192.168.1.15	192.168.1.122	802.11	76	69-17	dbm	Acknowledgment, Flags=.....C

```

Frame 925: 284 bytes on wire (2288 bits), 263 bytes captured (2088 bits) on Interface Wpa_04578005-2998-4006-8C31-C3A13
Ethernet II, Src: Cisco_08:07:047 (14:11:16:02:07:047), Dst: Anderson_07:1c:96 (08:1c:3b:07:1c:96)
Internet Protocol Version 4, Src: 192.168.1.15, Dst: 192.168.1.122
User Datagram Protocol, Src Port: 5555, Dst Port: 5000
AiroPcap/OSintPcap encapsulated IEEE 802.11
IEEE 802.11 radio information
IEEE 802.11 Association Request, Flags: .....C
Tagged parameters (167 bytes)
  Tag: SSID parameter set: "Wifi6a_test"
  Tag: Supported Rates (6R): 9, 12(0), 18, 24(0), 36, 48, 54, [Mbit/sec]
  Tag: Power Capability Mtr: 7, Max: 29
  Tag: Supported Channels
  Tag: RSN Information
    Tag Number: RSN Information (48)
    Tag Length: 28
    RSN Version: 1
    Group Cipher Suite: 00:0f:ac (See IEEE 802.11) AES (CCM)
    Pairwise Cipher Suite Count: 1
    Pairwise Cipher Suite List: 00:0f:ac (See IEEE 802.11) AES (CCM)
    Auth Key Management (AKM) Suite Count: 1
    Auth Key Management (AKM) List: 00:0f:ac (See IEEE 802.11) FT over IEEE 802.1X
    Auth Key Management (AKM) OUI: 00:0f:ac (See IEEE 802.11)
    Auth Key Management (AKM) type: FT over IEEE 802.1X (1)
  RSN Capabilities: 00:00
    .....0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
    .....0 = RSN No Pairwise capabilities: Transmitter can support MP default key @ simultaneously wdt
    .....0 = RSN PTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/TKkey5A (0x0)
    .....00 = RSN GTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/TKkey5A (0x0)
    .....1 = Management frame Protection Required: True
    .....1 = Management frame Protection Capable: True
    .....0 = 32bit MIC11-band RSN: false
    .....0 = Perkey Enabled: false
    .....0 = Extended key ID for Individually Addressed Frames: Not supported
  PMSKID Count: 0
  PMSKID List:
  Group Management Cipher Suite: 00:0f:ac (See IEEE 802.11) BIP (128)
  Tag: W Enabled Capabilities (5 octets)
  Tag: Mobility domain
  Tag: Supported Operating Classes
  Tag: Extended Capabilities (20 octets)
  Ext Tag: HE Capabilities
  Ext Tag: HE 4-0-0 Band Capabilities
  Tag: Vendor Specific: Broadcom
    Tag Number: Vendor Specific (221)
    Tag Length: 10
    OUI: 00:13:00 (Broadcom)
    Vendor Specific OUI Type: 2
    Vendor Specific Data: 0000000000000000
  Tag: Vendor Specific: Microsoft Corp.: WPAVUE: Information Element
  
```

WPA3 Enterprise 802.1x + FT Pixel6a 연결

WLC의 클라이언트 세부사항:

WPA3 Enterprise 802.1x + FT Pixel6a Client 상세 정보

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

삼성 S23

클라이언트의 RSN 정보에 중점을 둔 연결 OTA:

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
1246	8.295985	0.102133	Cisco_d5:80:18	Broadcast	802.11	364	69	-39 dBm	Beacon frame, SW=805, Fw=0, Flags=.....C, B1=100, SSID="wif
1247	8.401935	0.102170	Cisco_d5:80:18	Broadcast	802.11	364	69	-40 dBm	Beacon frame, SW=806, Fw=0, Flags=.....C, B1=100, SSID="wif
1248	8.504375	0.102420	Cisco_d5:80:18	Broadcast	802.11	364	69	-39 dBm	Beacon frame, SW=807, Fw=0, Flags=.....C, B1=100, SSID="wif
1249	8.606824	0.102419	Cisco_d5:80:18	Broadcast	802.11	364	69	-40 dBm	Beacon frame, SW=808, Fw=0, Flags=.....C, B1=100, SSID="wif
1251	8.612759	0.005945	Cisco_d5:80:18	Broadcast	802.11	312	69	-40 dBm	Probe Response, SW=859, Fw=0, Flags=.....C, B1=100, SSID="w
1258	8.701133	0.096374	Cisco_d5:80:18	Broadcast	802.11	364	69	-39 dBm	Beacon frame, SW=110, Fw=0, Flags=.....C, B1=100, SSID="wif
1260	8.786422	0.077279	Samsung_c9:e3:71	Cisco_d5:80:18	802.11	235	69	-48 dBm	Authentication, SW=99, Fw=0, Flags=.....C
1261	8.786422	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-39 dBm	Acknowledgment, Flags=.....C
1262	8.790571	0.004159	Cisco_d5:80:18	Samsung_c9:e3:71	802.11	247	69	-39 dBm	Authentication, SW=118, Fw=0, Flags=.....C
1263	8.790571	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-47 dBm	Acknowledgment, Flags=.....C
1265	8.796439	0.005968	Samsung_c9:e3:71	Cisco_d5:80:18	802.11	485	69	-48 dBm	Association Request, SW=100, Fw=0, Flags=.....C, SSID="wif
1266	8.796439	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-39 dBm	Acknowledgment, Flags=.....C
1268	8.800740	0.005639	Samsung_c9:e3:71	Broadcast	LLC	114	69	-39 dBm	S, Func=03, N(5)=19; DSAP 0x0a Group, SSAP 0x0a Command
1269	8.807940	0.001362	Cisco_d5:80:18	Samsung_c9:e3:71	802.11	413	69	-39 dBm	Association Response, SW=0, Fw=0, Flags=.....C
1270	8.807940	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-48 dBm	Acknowledgment, Flags=.....C
1271	8.807940	0.000000	Samsung_c9:e3:71	Broadcast	LLC	120	69	-39 dBm	I P, N(5)=19; DSAP 0x08 Individual, SSAP 0x0a Respons
1272	8.813121	0.001581	Cisco_d5:80:18	Broadcast	802.11	364	69	-39 dBm	Beacon frame, SW=111, Fw=0, Flags=.....C, B1=100, SSID="wif
1273	8.832754	0.012133	Cisco_Sc:F8:0c	Samsung_c9:e3:71	LLC	183	69	-40 dBm	U, Func=01C; DSAP 0x0a Group, SSAP 0x02 Command
1274	8.832754	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-58 dBm	Acknowledgment, Flags=.....C
1275	8.832754	0.000000	Cisco_Sc:F8:0c	Samsung_c9:e3:71	LLC	183	69	-49 dBm	U, Func=Unknown; DSAP Texas Instruments Group, SSAP 0x28 Respo
1276	8.832817	0.000063	192.168.1.15	192.168.1.121	802.11	76	69	-58 dBm	Acknowledgment, Flags=.....C
1277	8.800540	0.007723	Samsung_c9:e3:71	Broadcast	LLC	144	69	-46 dBm	S P, Func=02, N(5)=12; DSAP 0x0a Individual, SSAP 0x0a Respon
1278	8.800540	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-40 dBm	Acknowledgment, Flags=.....C
1280	8.804143	0.003063	Cisco_d5:80:18	Samsung_c9:e3:71	802.11	118	69	-47 dBm	Action, SW=1, Fw=0, Flags=p.....C
1281	8.804143	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-47 dBm	Acknowledgment, Flags=.....C
1282	8.804803	0.000660	Samsung_c9:e3:71	Cisco_d5:80:18	802.11	115	69	-47 dBm	Action, SW=0, Fw=0, Flags=p.....C
1283	8.804803	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-40 dBm	Acknowledgment, Flags=.....C
1284	8.806878	0.002075	Altiocel_a3e:59:af	Samsung_c9:e3:71	LLC	197	69	-50 dBm	I P, N(5)=25, N(5)=40; DSAP 0x0a Individual, SSAP 0x0a Command
1286	8.913192	0.007034	Cisco_d5:80:18	Broadcast	802.11	364	69	-41 dBm	Beacon frame, SW=113, Fw=0, Flags=.....C, B1=100, SSID="wif
1287	8.950493	0.036381	Cisco_d5:80:18	Broadcast	802.11	364	69	-39 dBm	Acknowledgment, Flags=.....C
1322	8.975553	0.029908	192.168.1.15	192.168.1.121	802.11	76	69	-39 dBm	Acknowledgment, Flags=.....C
1372	9.051619	0.040566	Cisco_d5:80:18	Broadcast	802.11	364	69	-38 dBm	Beacon frame, SW=114, Fw=0, Flags=.....C, B1=100, SSID="wif
1471	9.118083	0.102164	Cisco_d5:80:18	Broadcast	802.11	364	69	-39 dBm	Beacon frame, SW=115, Fw=0, Flags=.....C, B1=100, SSID="wif
1600	9.176814	0.058111	192.168.1.15	192.168.1.121	802.11	76	69	-40 dBm	Acknowledgment, Flags=.....C
1702	9.221145	0.044111	Cisco_d5:80:18	Broadcast	802.11	364	69	-39 dBm	Beacon frame, SW=116, Fw=0, Flags=.....C, B1=100, SSID="wif
1913	9.124197	0.102062	Cisco_d5:80:18	Broadcast	802.11	364	69	-39 dBm	Beacon frame, SW=117, Fw=0, Flags=.....C, B1=100, SSID="wif
1917	9.425938	0.103151	Cisco_d5:80:18	Broadcast	802.11	364	69	-40 dBm	Beacon frame, SW=118, Fw=0, Flags=.....C, B1=100, SSID="wif
1919	9.528463	0.102525	Cisco_d5:80:18	Broadcast	802.11	364	69	-38 dBm	Beacon frame, SW=119, Fw=0, Flags=.....C, B1=100, SSID="wif
1945	9.613020	0.102557	Cisco_d5:80:18	Broadcast	802.11	364	69	-38 dBm	Beacon frame, SW=120, Fw=0, Flags=.....C, B1=100, SSID="wif
1946	9.731295	0.102275	Cisco_d5:80:18	Broadcast	802.11	364	69	-39 dBm	Beacon frame, SW=121, Fw=0, Flags=.....C, B1=100, SSID="wif
1948	9.835864	0.102569	Cisco_d5:80:18	Broadcast	802.11	364	69	-40 dBm	Beacon frame, SW=122, Fw=0, Flags=.....C, B1=100, SSID="wif
1951	9.925936	0.000072	Samsung_c9:e3:71	Cisco_d5:80:18	802.11	122	69	-45 dBm	Action, SW=4, Fw=0, Flags=p.....C
1952	9.925936	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-40 dBm	Acknowledgment, Flags=.....C
1953	9.926093	0.000057	192.168.1.15	192.168.1.121	802.11	76	69	-40 dBm	Acknowledgment, Flags=.....C
1954	9.917895	0.011002	Cisco_d5:80:18	Broadcast	802.11	364	69	-40 dBm	Beacon frame, SW=123, Fw=0, Flags=.....C, B1=100, SSID="wif
1955	9.942143	0.006448	192.168.1.15	192.168.1.121	802.11	76	69	-40 dBm	Acknowledgment, Flags=.....C

```

> Frame 1265: 485 bytes on wire (3880 bits), 485 bytes captured (3880 bits) on interface Device\MPF_04578095-2
> Ethernet II, Src: Cisco_02:09:74:47:74:11:02:02:97:47, Dst: Universa_07:cf:06:48:3a:80:10:7c:f0:06
> Internet Protocol Version 4, Src: 192.168.1.15, Dst: 192.168.1.121
> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
> AiroPcap/OnixPcap encapsulated IEEE 802.11
> IEEE 802.11 radio information
> IEEE 802.11 Reassociation Request, Flags: .....C
> IEEE 802.11 Key Management
> Fixed parameters (18 bytes)
> Tagged parameters (185 bytes)
> Tag: SSID parameter set: "wif166_test"
> Tag: Supported Rates A(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
> Tag: Power Capability M(n), 8, Max: 16
> Tag: Supported Channels
> Tag: RM Enabled Capabilities (5 octets)
> Tag: DSM Information
> Tag: Mobility Domain
  > Tag Number: Mobility Domain (54)
  Tag Length: 3
  Mobility Domain Identifier: 0xe2f2
  > FT Capability and Policy: 0x01
  .....0 = Fast BSS Transition over DS: 0x1
  .....0 = Resource Request Protocol Capability: 0x0
  0x00 0x00 = Reserved: 0x00
> Tag: Fast BSS Transition
  Tag Number: Fast BSS Transition (55)
  Tag Length: 96
  MDC Control: 0x0000
  MDC: @#124d7f4e16ad0ecf650a5a1a4ca
  Address: d514f817ab7fa005b76f75e10b0a0822cfa0c50fb3f492e1080f01a809ca
  Owner: 00122a55578aa18c4ef4124242597007905c0e9fa12283f566d00b2c3
  > Subelement: PMK-R1 key holder Identifier (R104-ID) (1)
  Length: 6
  PMK-R1 key holder Identifier (R104-ID): d68070d97ad0
  > Subelement: PMK-R0 key holder Identifier (R004-ID) (3)
  Length: 4
  PMK-R0 key holder Identifier (R004-ID): 002055a2
> Tag: Supported Operating Classes
> Tag: Extended Capabilities (13 octets)
> Ext Tag: Vendor-Specific: Microsoft Corp.: WPA/WPA2 Information Element
> Ext Tag: HE Capabilities
> Ext Tag: HE 6 GHz Band Capabilities
> Tag: Vendor-Specific: Qualcomm Inc.
> Tag: Vendor-Specific: Samsung Electronics Co., Ltd
> Tag: Vendor-Specific: Samsung Electronics Co., Ltd

```

S23 로밍 FToDS 패킷

WPA3-엔터프라이즈 + GCMP128 암호 + SUITEB-1X

WLAN 보안 구성:

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General **Security** Advanced Add To Policy Tags

Layer2 Layer3 AAA

WPA + WPA2
 WPA2 + WPA3
 WPA3
 Static WEP
 None

MAC Filtering

Lobby Admin Access

WPA Parameters

WPA Policy	<input type="checkbox"/>	WPA2 Policy	<input type="checkbox"/>
GTK Randomize	<input type="checkbox"/>	WPA3 Policy	<input checked="" type="checkbox"/>
Transition Disable	<input type="checkbox"/>		

WPA2/WPA3 Encryption

AES(CCMP128)	<input type="checkbox"/>	CCMP256	<input type="checkbox"/>
GCMP128	<input checked="" type="checkbox"/>	GCMP256	<input type="checkbox"/>

Protected Management Frame

PMF

Association Comeback Timer*

SA Query Time*

Fast Transition

Status

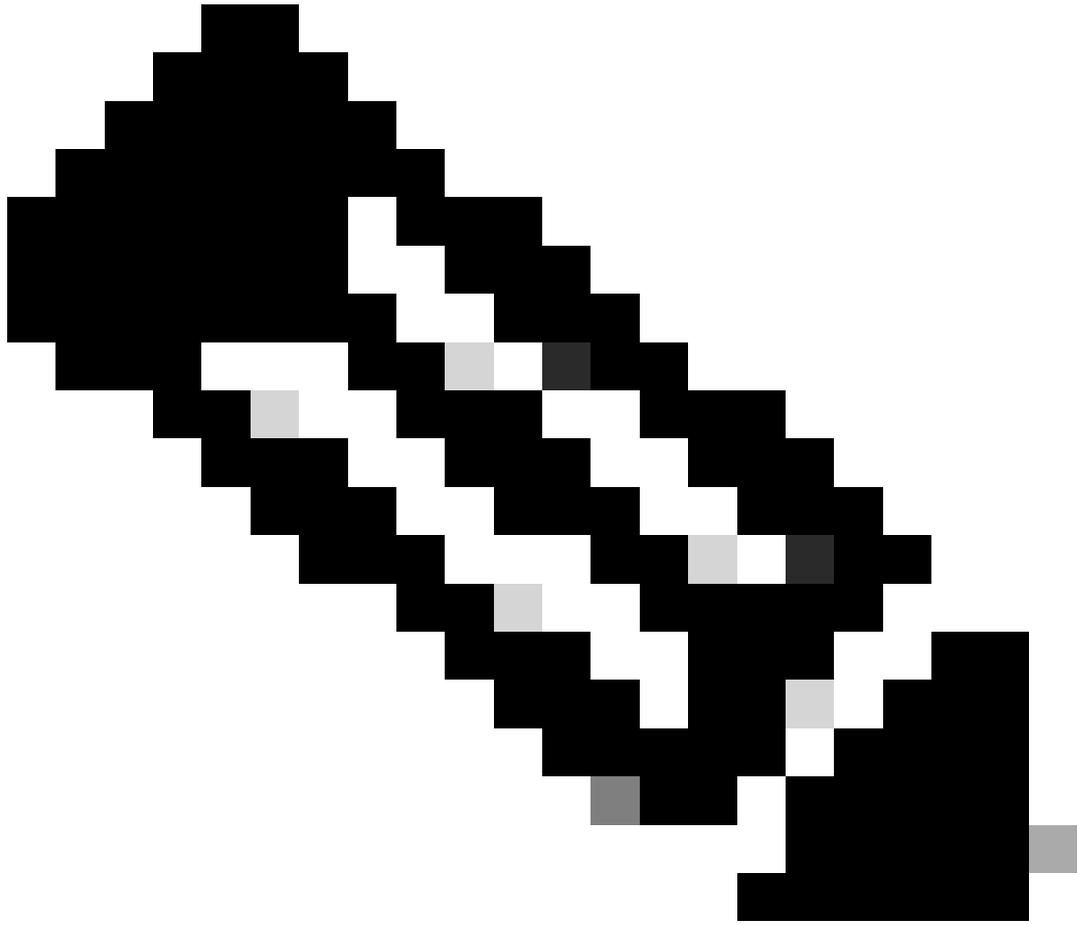
Over the DS

Reassociation Timeout *

Auth Key Mgmt

SUITEB-1X

WPA3 Enterprise SuiteB-1X 보안 구성



참고: FT는 SUITEB-1X에서 지원되지 않습니다.

WLAN Security(WLAN 보안) 설정의 WLC GUI에서 보기:

○  wlan_test

 5

wlan_test

[WPA3][SUITEB-1X][GCMP128]

비콘 OTA 확인:

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	str	Info
37376	59.189776	0.820482	Cisco_05:00:18	Broadcast	802.11	312	69	-48	dbm	Probe Response, SW=2062, Fw=0, Flags=.....C, B=100, SSID=N
37385	59.190516	0.820488	Cisco_05:00:18	Broadcast	802.11	312	69	-17	dbm	Probe Response, SW=2063, Fw=0, Flags=.....C, B=100, SSID=N
37396	59.191709	0.820481	Cisco_05:00:18	Broadcast	802.11	355	69	-17	dbm	Beacon frame, SW=2064, Fw=0, Flags=.....C, B=100, SSID=N
37414	59.192161	0.820462	Cisco_05:00:18	Broadcast	802.11	312	69	-38	dbm	Probe Response, SW=2065, Fw=0, Flags=.....C, B=100, SSID=N
37424	59.192373	0.820472	Cisco_05:00:18	Broadcast	802.11	312	69	-48	dbm	Probe Response, SW=2066, Fw=0, Flags=.....C, B=100, SSID=N
37437	59.192258	0.820457	Cisco_05:00:18	Broadcast	802.11	312	69	-38	dbm	Probe Response, SW=2067, Fw=0, Flags=.....C, B=100, SSID=N
37447	59.1925726	0.820442	Cisco_05:00:18	Broadcast	802.11	312	69	-17	dbm	Probe Response, SW=2068, Fw=0, Flags=.....C, B=100, SSID=N
37459	59.193154	0.820522	Cisco_05:00:18	Broadcast	802.11	355	69	-38	dbm	Beacon frame, SW=2069, Fw=0, Flags=.....C, B=100, SSID=N
37470	59.193629	0.820399	Cisco_05:00:18	Broadcast	802.11	312	69	-39	dbm	Probe Response, SW=2070, Fw=0, Flags=.....C, B=100, SSID=N
37480	59.194345	0.820561	Cisco_05:00:18	Broadcast	802.11	355	69	-17	dbm	Beacon frame, SW=2071, Fw=0, Flags=.....C, B=100, SSID=N
37489	59.194567	0.821342	Cisco_05:00:18	Broadcast	802.11	312	69	-38	dbm	Probe Response, SW=2072, Fw=0, Flags=.....C, B=100, SSID=N
37499	59.195116	0.821929	Cisco_05:00:18	Broadcast	802.11	312	69	-17	dbm	Probe Response, SW=2073, Fw=0, Flags=.....C, B=100, SSID=N
37520	59.195713	0.820817	Cisco_05:00:18	Broadcast	802.11	355	69	-17	dbm	Beacon frame, SW=2074, Fw=0, Flags=.....C, B=100, SSID=N
37529	59.195888	0.820835	Cisco_05:00:18	Broadcast	802.11	312	69	-17	dbm	Probe Response, SW=2075, Fw=0, Flags=.....C, B=100, SSID=N
37532	59.1957236	0.821156	Cisco_05:00:18	Broadcast	802.11	312	69	-17	dbm	Probe Response, SW=2076, Fw=0, Flags=.....C, B=100, SSID=N
37539	59.197089	0.821751	Cisco_05:00:18	Broadcast	802.11	312	69	-17	dbm	Probe Response, SW=2077, Fw=0, Flags=.....C, B=100, SSID=N
37552	59.197468	0.820499	Cisco_05:00:18	Broadcast	802.11	312	69	-17	dbm	Probe Response, SW=2078, Fw=0, Flags=.....C, B=100, SSID=N
37565	59.197993	0.820561	Cisco_05:00:18	Broadcast	802.11	355	69	-17	dbm	Beacon frame, SW=2079, Fw=0, Flags=.....C, B=100, SSID=N
37574	59.198423	0.820438	Cisco_05:00:18	Broadcast	802.11	312	69	-17	dbm	Probe Response, SW=2080, Fw=0, Flags=.....C, B=100, SSID=N
37585	59.198865	0.820542	Cisco_05:00:18	Broadcast	802.11	312	69	-17	dbm	Probe Response, SW=2081, Fw=0, Flags=.....C, B=100, SSID=N
37596	59.199429	0.820476	Cisco_05:00:18	Broadcast	802.11	312	69	-17	dbm	Probe Response, SW=2082, Fw=0, Flags=.....C, B=100, SSID=N
37616	59.199949	0.820995	Cisco_05:00:18	Broadcast	802.11	312	69	-17	dbm	Probe Response, SW=2083, Fw=0, Flags=.....C, B=100, SSID=N
37628	59.200621	0.820881	Cisco_05:00:18	Broadcast	802.11	355	69	-38	dbm	Beacon frame, SW=2084, Fw=0, Flags=.....C, B=100, SSID=N
37641	59.200964	0.820961	Cisco_05:00:18	Broadcast	802.11	312	69	-38	dbm	Probe Response, SW=2085, Fw=0, Flags=.....C, B=100, SSID=N
37652	59.201317	0.820351	Cisco_05:00:18	Broadcast	802.11	312	69	-38	dbm	Probe Response, SW=2086, Fw=0, Flags=.....C, B=100, SSID=N
37668	59.202765	0.820428	Cisco_05:00:18	Broadcast	802.11	312	69	-38	dbm	Probe Response, SW=2087, Fw=0, Flags=.....C, B=100, SSID=N
37687	59.203467	0.820792	Cisco_05:00:18	Broadcast	802.11	312	69	-38	dbm	Probe Response, SW=2088, Fw=0, Flags=.....C, B=100, SSID=N
37696	59.202867	0.820480	Cisco_05:00:18	Broadcast	802.11	355	69	-38	dbm	Beacon frame, SW=2089, Fw=0, Flags=.....C, B=100, SSID=N
37704	59.203477	0.820430	Cisco_05:00:18	Broadcast	802.11	312	69	-38	dbm	Probe Response, SW=2090, Fw=0, Flags=.....C, B=100, SSID=N
37719	59.203721	0.820240	Cisco_05:00:18	Broadcast	802.11	312	69	-38	dbm	Probe Response, SW=2091, Fw=0, Flags=.....C, B=100, SSID=N
37731	59.204549	0.820628	Cisco_05:00:18	Broadcast	802.11	312	69	-38	dbm	Probe Response, SW=2092, Fw=0, Flags=.....C, B=100, SSID=N
37738	59.204659	0.820180	Cisco_05:00:18	Broadcast	802.11	312	69	-38	dbm	Probe Response, SW=2093, Fw=0, Flags=.....C, B=100, SSID=N
37749	59.205208	0.820495	Cisco_05:00:18	Broadcast	802.11	355	69	-38	dbm	Beacon frame, SW=2094, Fw=0, Flags=.....C, B=100, SSID=N
37775	59.205621	0.820921	Cisco_05:00:18	Broadcast	802.11	312	69	-17	dbm	Probe Response, SW=2095, Fw=0, Flags=.....C, B=100, SSID=N
37792	59.206121	0.820908	Cisco_05:00:18	Broadcast	802.11	312	69	-17	dbm	Probe Response, SW=2096, Fw=0, Flags=.....C, B=100, SSID=N
37809	59.207002	0.821581	Cisco_05:00:18	Broadcast	802.11	312	69	-38	dbm	Probe Response, SW=2097, Fw=0, Flags=.....C, B=100, SSID=N
37814	59.207213	0.821521	Cisco_05:00:18	Broadcast	802.11	312	69	-17	dbm	Probe Response, SW=2098, Fw=0, Flags=.....C, B=100, SSID=N
37822	59.207660	0.820847	Cisco_05:00:18	Broadcast	802.11	312	69	-38	dbm	Beacon frame, SW=2099, Fw=0, Flags=.....C, B=100, SSID=N
37833	59.208050	0.820398	Cisco_05:00:18	Broadcast	802.11	312	69	-38	dbm	Probe Response, SW=2100, Fw=0, Flags=.....C, B=100, SSID=N
37841	59.208540	0.820490	Cisco_05:00:18	Broadcast	802.11	312	69	-38	dbm	Probe Response, SW=2101, Fw=0, Flags=.....C, B=100, SSID=N
37857	59.209090	0.820550	Cisco_05:00:18	Broadcast	802.11	312	69	-38	dbm	Probe Response, SW=2102, Fw=0, Flags=.....C, B=100, SSID=N
37864	00.013062	0.820462	Cisco_05:00:18	Broadcast	802.11	312	69	-17	dbm	Probe Response, SW=2103, Fw=0, Flags=.....C, B=100, SSID=N
37868	00.013192	0.820508	Cisco_05:00:18	Broadcast	802.11	355	69	-38	dbm	Beacon frame, SW=2104, Fw=0, Flags=.....C, B=100, SSID=N
37881	00.013049	0.820297	Cisco_05:00:18	Broadcast	802.11	312	69	-38	dbm	Probe Response, SW=2105, Fw=0, Flags=.....C, B=100, SSID=N
37887	00.013167	0.820468	Cisco_05:00:18	Broadcast	802.11	312	69	-38	dbm	Probe Response, SW=2106, Fw=0, Flags=.....C, B=100, SSID=N
37897	00.013096	0.820839	Cisco_05:00:18	Broadcast	802.11	312	69	-38	dbm	Probe Response, SW=2107, Fw=0, Flags=.....C, B=100, SSID=N
37908	00.011976	0.820888	Cisco_05:00:18	Broadcast	802.11	312	69	-38	dbm	Probe Response, SW=2108, Fw=0, Flags=.....C, B=100, SSID=N
37917	00.112414	0.820438	Cisco_05:00:18	Broadcast	802.11	355	69	-17	dbm	Beacon frame, SW=2109, Fw=0, Flags=.....C, B=100, SSID=N
37928	00.113067	0.820611	Cisco_05:00:18	Broadcast	802.11	312	69	-17	dbm	Probe Response, SW=2100, Fw=0, Flags=.....C, B=100, SSID=N
37936	00.173114	0.820267	Cisco_05:00:18	Broadcast	802.11	312	69	-38	dbm	Probe Response, SW=2101, Fw=0, Flags=.....C, B=100, SSID=N
37943	00.193778	0.820664	Cisco_05:00:18	Broadcast	802.11	312	69	-17	dbm	Probe Response, SW=2102, Fw=0, Flags=.....C, B=100, SSID=N
37949	00.114369	0.820993	Cisco_05:00:18	Broadcast	802.11	312	69	-17	dbm	Probe Response, SW=2103, Fw=0, Flags=.....C, B=100, SSID=N
37961	00.114873	0.820998	Cisco_05:00:18	Broadcast	802.11	355	69	-17	dbm	Beacon frame, SW=2104, Fw=0, Flags=.....C, B=100, SSID=N

```

> frame 37626: 355 bytes on wire (2840 bits), 355 bytes captured (2840 bits) on interface \Device\NPF_{04576965-2998-4456-8C13-C4}
> Ethernet II, Src: Cisco_02:00:07:40:74:11(02:00:07:40:74:11), Dst: Unknown_02:00:07:40:74:11(02:00:07:40:74:11)
> Internet Protocol Version 4, Src: 192.168.1.15, Dst: 192.168.1.111
> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
> AlohaPdu/OnStream encapsulated IEEE 802.11
> IEEE 802.11 radio information
> IEEE 802.11 beacon frame, Flags: .....C
> IEEE 802.11 Wireless Management
> Fixed parameters (12 bytes)
> Tagged parameters (213 bytes)
  > Tag: SSID parameter set: "wifi_test"
  > Tag: Supported Rates (6(B), 9, 12(6), 18, 24(6), 36, 48, 54, [Mbit/sec])
  > Tag: Traffic Indication Map (TIM): OFDM # of 1 bitmap
  > Tag: Country Information: Country Code not set, Environment Global operating classes
  > Tag: Power Constraint: 6
  > Tag: TX Report Transmit Power: 36, L1tx Operat: 0
  > Tag: RSN Information
    > Tag Number: RSN Information (64)
    > Tag Length: 36
    > RSN Version: 1
    > Group Cipher Suite: 00000000: IEEE 802.11 GOWP (128)
    > Pairwise Cipher Suite Count: 1
    > Pairwise Cipher Suite List 00000000: IEEE 802.11 GOWP (128)
    > Auth Key Management (AKM) Suite Count: 1
    > Auth Key Management (AKM) List 00000000: IEEE 802.11 WPA (SHA256-SuiteB)
    > Auth Key Management (AKM) SUIT: 00000000: IEEE 802.11 WPA (SHA256-SuiteB)
    > Auth Key Management (AKM) Type: WPA (SHA256-SuiteB) (11)
    > RSN Capabilities: 000000
    > PMKID Count: 0
    > PMKID List
    > Group Management Cipher Suite: 00000000: IEEE 802.11 GOWP (128)
  > Tag: QoS User Element: IEEE 802.11 QoS version
  > Tag: WPA Enabled Capabilities (5 octets)
  > Tag: Extended Capabilities (1 octets)
  > Tag: Tx Power Envelope
  > Tag: Tx Power Envelope
  > Ext Tag: Multiple BSSID Configuration
  > Ext Tag: HE Capabilities
  > Ext Tag: HE Operation
  > Ext Tag: Spatial Reuse Parameter Set
  > Ext Tag: HE SCA Parameter Set
  > Ext Tag: HE 4 GHz Band Capabilities
  > Tag: Vendor Specific: Atheros Communications, Inc.: Unknown
  > Tag: Vendor Specific: Microsoft Corp.: WPAHE: Parameter Element
  > Tag: Vendor Specific: Cisco Systems, Inc.: Airont Client MFP Disabled
  > Tag: Vendor Specific: Cisco Systems, Inc.: Airont CCK version = 5
  > Tag: Vendor Specific: Cisco Systems, Inc.: Airont Unknown (64)
  > Tag: Vendor Specific: Cisco Systems, Inc.: Airont Unknown (11) (11)

```

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:

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General **Security** Advanced Add To Policy Tags

Layer2 Layer3 AAA

WPA + WPA2 WPA2 + WPA3 WPA3 Static WEP None

MAC Filtering

Lobby Admin Access

WPA Parameters

WPA Policy WPA2 Policy
GTK Randomize WPA3 Policy
Transition Disable

Fast Transition

Status
Over the DS
Reassociation Timeout *

WPA2/WPA3 Encryption

AES(CCMP128) CCMP256
GCMP128 GCMP256

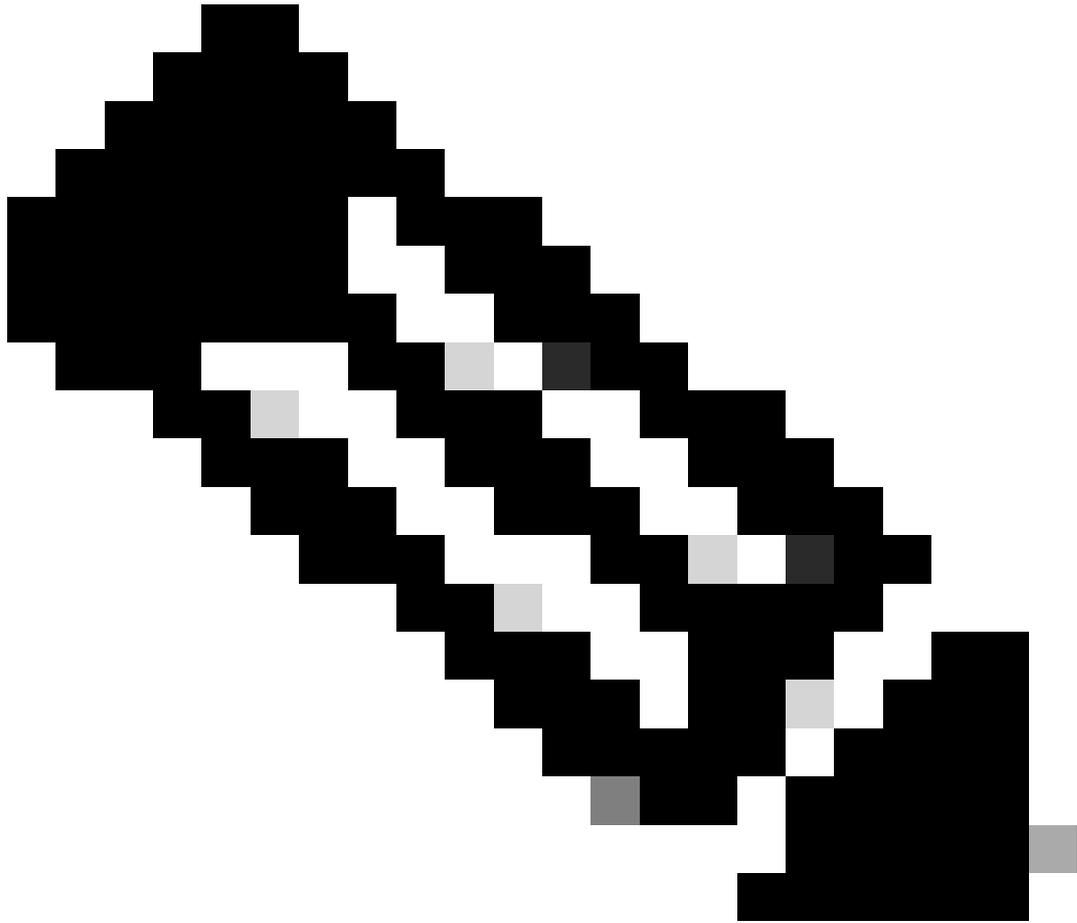
Auth Key Mgmt

SUITEB192-1X

Protected Management Frame

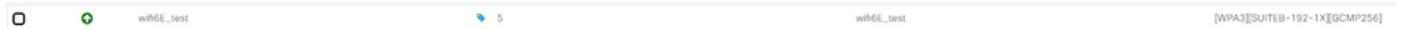
PMF
Association Comeback Timer*
SA Query Time*

WPA3 Enterprise SUITE192-1x 보안 설정



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

WLC GUI WLAN 목록의 WLAN:



테스트에 사용되는 WLAN

비콘 OTA 확인:

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
빌린 돈	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 명령](#)에 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.