

기회주의적 무선 암호화 흐름 이해

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[설명](#)

[단계](#)

[Lab Repro 세부 정보](#)

[OWE 플로우](#)

[원래 비컨 프레임](#)

[숨겨진 SSID 비콘](#)

[클라이언트에서 WISE 전환 SSID로 전송된 프로브 요청](#)

[AP에서 클라이언트로 전송된 프로브 응답](#)

[OPEN 인증](#)

[클라이언트에서 AP로의 연결 요청](#)

[AP에서 클라이언트로 보낸 연결 응답](#)

[키 교환](#)

[L2 인증 성공](#)

[IP 학습 상태](#)

[클라이언트 실행 상태](#)

[WISE 암호화가 지원되지 않는 클라이언트](#)

[빠른 전환 정보](#)

[WISE는 PSK/dot1x에서 지원되지 않습니다.](#)

[문제 해결](#)

[RA 추적 및 EPC\(임베디드 패킷 캡처\)](#)

[항공 모함](#)

[로밍](#)

소개

이 문서에서는 OWE 전환 흐름과 Catalyst 9800 WLC(Wireless LAN Controller)에서 작동하는 방식에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 기본 작동을 위해 9800 WLC, 액세스 포인트(AP)를 구성하는 방법
- WLAN 및 정책 프로파일 구성 방법

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- C9800-80, Cisco IOS® XE 17.12.4 및 Cisco IOS® XE 17.9.6에서 테스트됨
- AP 모델: C9136I, 로컬 및 플렉스 연결 모드에서 모두 확인됨.

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.

설명

- OWE(Opportunistic Wireless Encryption)는 무선 매체를 위한 암호화를 제공하는 IEEE 802.11의 확장입니다. OWE 기반 인증의 목적은 AP와 클라이언트 간의 안전하지 않은 개방형 무선 연결을 방지하는 것입니다.
- OWE는 무선 암호화를 설정하기 위해 Diffie-Hellman 알고리즘 기반 암호화를 사용합니다.
- OWE를 사용하면 클라이언트와 AP는 액세스 절차 중에 Diffie-Hellman 키 교환을 수행하고 그 결과로 생성되는 페어와이즈 암호를 4방향 핸드셰이크로 사용합니다.
- OWE를 사용하면 개방형 또는 공유 PSK 기반 네트워크가 구축된 구축에서 무선 네트워크 보안이 향상됩니다.

단계

1. 암호화/보안 없이 하나의 OPEN WLAN을 구성하고 브로드캐스트를 활성화합니다.
2. OWE 보안 설정으로 다른 SSID를 구성하고 변환 모드 wlan-id에서 OPEN WLAN ID 번호를 매핑합니다. 이 OWE 변환 SSID에서 브로드캐스트 SSID 옵션을 비활성화합니다.
3. OPEN WLAN "transition-mode-wlan-id" 필드에 OWE 전환 WLAN ID 번호를 매핑합니다.

Lab Repro 세부 정보

- 개방형 SSID 이름: 채무액 공개
- OWE 전환 SSID 이름: 채무 이행
- OPEN-WISE의 BSSID: 40:ce:24:dd:2e:87
- BSSID OF OWE-Transition(WISE-Transition의 BSSID): 40:ce:24:dd:2e:8f

OWE 플로우

1. 신호는 OPEN SSID에 대해 브로드캐스트될 수 있습니다. AIR PCAP에서 해당 SSID 이름으로 신호를 볼 수 있습니다.

2. 또한 AIR PCAP에서 자체 SSID 이름 대신 "Wildcard"라는 이름의 숨겨진 보안 지원 SSID를 볼 수 있습니다.
3. 클라이언트가 OPEN SSID에 대한 비콘 프레임을 수신하면 WISE가 있거나 이를 지원하는 경우 WISE 전환 SSID(OPEN SSID 대신 보안이 활성화된 SSID)로 프로브 요청 전송을 시작할 수 있습니다.
4. WISE 지원 클라이언트는 전환 SSID에서 프로브 응답을 가져올 수 있습니다.
5. 클라이언트와 AP 간에 OPEN 인증이 발생할 수 있습니다.
6. 클라이언트는 DH 키 교환 세부사항이 포함된 연결 요청을 AP에 전송하고 그 결과로 생성되는 쌍방향 암호를 4-way 핸드셰이크에 사용할 수 있습니다.
7. AP에서 연결 응답을 보낼 수 있습니다.
8. AP와 클라이언트 장치 간에 4방향 핸드셰이크가 발생할 수 있습니다.
9. 성공적인 키 관리 후에는 L2 PSK가 성공할 수 있습니다.
10. 클라이언트는 DHCP, ARP 등에서 IP를 가져올 수 있습니다.
11. 클라이언트는 RUN 상태로 전환할 수 있습니다.
12. WISE를 지원하지 않는 클라이언트 디바이스인 경우 OPEN SSID 자체에 프로브 요청을 보낼 수 있으며 RUN 상태로 갈 수 있는 것보다 직접 IP를 가져올 수 있습니다.

원래 비콘 프레임

- 여기서 AIR PCAP는 SSID "OPEN-WISE" 브로드캐스트(비콘 프레임)를 보여줍니다. 전환 SSID 세부사항이 포함되어 있으며 "OWE-Transition"이라고 합니다.

No.	Time	Source	Destination	Protocol	Length	Info
47285	2025-01-21 09:53:18.259879	Cisco_dd:2e:87	Broadcast	802.11	376	Beacon frame, SN=1157, FN=0, Flags=.....C, BI=100, SSID="OPEN-OWE"
> Frame 47285: 376 bytes on wire (3008 bits), 376 bytes captured (3008 bits) on interface 0 > Radiotap Header v0, Length 36 > 802.11 radio information > IEEE 802.11 Beacon frame, Flags:C > IEEE 802.11 Wireless Management > Fixed parameters (12 bytes) > Tagged parameters (300 bytes) > Tag: SSID parameter set: "OPEN-OWE" > Tag Number: SSID parameter set (0) > Tag length: 8 > SSID: "OPEN-OWE" > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec] > Tag: DS Parameter set: Current Channel: 48 > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap > Tag: Country Information: Country Code IN, Environment All > Tag: Power Constraint: 0 > Tag: QBSS Load Element 802.11e CCA Version > Tag: RM Enabled Capabilities (5 octets) > Tag: HT Capabilities (802.11n D1.10) > Tag: HT Information (802.11n D1.10) > Tag: Extended Capabilities (8 octets) > Tag: VHT Capabilities > Tag: VHT Operation > Tag: Tx Power Envelope > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element > Tag: Vendor Specific: Cisco Systems, Inc: Aironet CCX version = 5 > Tag: Vendor Specific: Cisco Systems, Inc: Aironet Client MFP Disabled > Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (11) (11) > Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (44) > Tag: Vendor Specific: Wi-Fi Alliance: OWE Transition Mode > Tag Number: Vendor Specific (221) > Tag length: 25 > OUI: 50:6f:9a (Wi-Fi Alliance) > Vendor Specific OUI Type: 28 > BSSID: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f) > SSID length: 14 > SSID: OWE-Transition						

이미지-1: 개방형 SSID의 비콘 프레임

숨겨진 SSID 비콘

- WLAN 컨피그레이션에 따라 이 "OWE-Transition" SSID에 대해 "broadcasting"이 비활성화되지만 AIR PCAP에서 SSID 이름 "Wildcard"가 포함된 숨겨진 SSID 신호를 볼 수 있습니다. 그러나 해당 패킷을 선택하면 WISE-Transition 세부 정보가 포함됩니다.
- 이 패킷을 사용하여 숨겨진 SSID의 BSSID를 가져옵니다(예: "40:ce:24:dd:2e:8f"). 패킷

캡처에서 검색합니다.

- 이 패킷에서는 SSID가 "Missing"이고 전환 SSID가 "OPEN-WISE"로, BSSID가 "40:ce:24:dd:2e:87"로 표시됨을 보여 줍니다.

No.	Time	Source	Destination	Protocol	Length	Info
22581	2025-01-21 09:52:23.230007	Cisco_dd:2e:8f	Broadcast	802.11	390	Beacon frame, SN=2483, FN=0, Flags=.....C, BI=100, SSID=wildcard (Broadcast)
> Frame 22581: 390 bytes on wire (3120 bits), 390 bytes captured (3120 bits)						
> Radiotap Header v0, Length 36						
> 802.11 radio information						
> IEEE 802.11 Beacon frame, Flags:C						
IEEE 802.11 Wireless Management						
Fixed parameters (12 bytes)						
Tagged parameters (314 bytes)						
Tag: SSID parameter set: Wildcard SSID						
Tag Number: SSID parameter set (0)						
Tag length: 0						
SSID: <MISSING>						
Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]						
Tag: DS Parameter set: Current Channel: 48						
Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap						
Tag: Country Information: Country Code IN, Environment All						
Tag: Power Constraint: 0						
Tag: RSN Information						
Tag: QoS Load Element 802.11e CCA Version						
Tag: RM Enabled Capabilities (5 octets)						
Tag: HT Capabilities (802.11n D1.0)						
Tag: HT Information (802.11n D1.0)						
Tag: Extended Capabilities (8 octets)						
Tag: VHT Capabilities						
Tag: VHT Operation						
Tag: Tx Power Envelope						
Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element						
Tag: Vendor Specific: Cisco Systems, Inc: Aironet CCX version = 5						
Tag: Vendor Specific: Cisco Systems, Inc: Aironet Client MFP Disabled						
Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (11) (11)						
Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (44)						
Tag: Vendor Specific: Wi-Fi Alliance: OWE Transition Mode						
Tag Number: Vendor Specific (221)						
Tag length: 19						
OUI: 50:6f:9a (Wi-Fi Alliance)						
Vendor Specific OUI Type: 28						
BSSID: Cisco_dd:2e:8f (40:ce:24:dd:2e:87)						
SSID length: 8						
SSID: OPEN-OWE						

이미지-2: 숨겨진 SSID - OWE 전환

클라이언트에서 WISE 전환 SSID로 전송된 프로브 요청

- 비콘 프레임 "OPEN-WISE" SSID를 기반으로 클라이언트는 연결해야 하는 다른 SSID 세부사항을 알게 됩니다. 이 시나리오에서 "WISE-Transition"입니다. 클라이언트가 WISE 암호화를 지원할 수 있는 경우 프로브 요청을 "WISE-Transition" SSID로 전송하고 응답을 받을 수 있습니다.
- 프로브 요청이 WISE-Transition BSSID "40:ce:24:dd:2e:8f"로 전송되었으며 응답을 받았습니다. 이 프로브 응답 패킷 내에서도 OPEN-WISE SSID 세부사항을 볼 수 있습니다

No.	Time	Source	Destination	Protocol	Length	Info
8509	2025-01-21 09:51:57.318400	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	802.11	197	Probe Request, SN=0, FN=0, Flags=.....C, SSID="OWE-Transition"
8510	2025-01-21 09:51:57.318412		ee:13:e8:a8:cd:5b	802.11	48	Acknowledgement, Flags=.....C
8511	2025-01-21 09:51:57.319223	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	802.11	398	Probe Response, SN=782, FN=0, Flags=.....C, BI=100, SSID="OWE-Transition"
8512	2025-01-21 09:51:57.319233		Cisco_dd:2e:8f	802.11	48	Acknowledgement, Flags=.....C
> Frame 8509: 197 bytes on wire (1576 bits), 197 bytes captured (1576 bits)						
> Radiotap Header v0, Length 36						
> 802.11 radio information						
> IEEE 802.11 Probe Request, Flags:C						
IEEE 802.11 Wireless Management						
Tagged parameters (133 bytes)						
Tag: SSID parameter set: "OWE-Transition"						
Tag Number: SSID parameter set (0)						
Tag length: 14						
SSID: "OWE-Transition"						
Tag: Supported Rates 6, 9, 12, 18, 24, 36, 48, 54, [Mbit/sec]						
Tag: DS Parameter set: Current Channel: 48						
Tag: HT Capabilities (802.11n D1.0)						
Tag: Extended Capabilities (11 octets)						
Tag: VHT Capabilities						
Ext Tag: HE Capabilities						
Tag: Vendor Specific: Wi-Fi Alliance: Multi Band Operation - Optimized Connectivity Experience						
Tag Number: Vendor Specific (221)						
Tag length: 7						
OUI: 50:6f:9a (Wi-Fi Alliance)						
Vendor Specific OUI Type: 22						
MBO/OCE attribute: 030102 (Cellular Data Capabilities)						
Tag: Vendor Specific: Microsoft Corp.: Unknown 8						

이미지-3: 프로브 요청

AP에서 클라이언트로 전송된 프로브 응답

- 클라이언트는 SSID "OWE-Transition"에 대한 프로브 응답을 받았지만 WiFi Alliance에 원래 SSID 세부사항 "OPEN-OWE"가 있습니다.

```
8509 2025-01-21 09:51:57.318400 ee:13:e8:a8:cd:5b Cisco_dd:2e:8f 802.11 197 Probe Request, SN=0, FN=0, Flags=.....C, SSID="OWE-Transition"
8510 2025-01-21 09:51:57.318412 ee:13:e8:a8:cd:5b 802.11 48 Acknowledgement, Flags=.....C
8511 2025-01-21 09:51:57.319223 Cisco_dd:2e:8f ee:13:e8:a8:cd:5b 802.11 398 Probe Response, SN=782, FN=0, Flags=.....C, BI=100, SSID="OWE-Transition"
8512 2025-01-21 09:51:57.319233 Cisco_dd:2e:8f 802.11 48 Acknowledgement, Flags=.....C

> Frame 8511: 398 bytes on wire (3184 bits), 398 bytes captured (3184 bits)
> Radiotap Header v0, Length 36
> 802.11 radio information
  IEEE 802.11 Probe Response Flags: .....C
  IEEE 802.11 Wireless Management
    Fixed parameters (12 bytes)
    Tagged parameters (322 bytes)
      Tag: SSID parameter set: "OWE-Transition"
        Tag Number: SSID parameter set (0)
        Tag length: 14
        SSID: "OWE-Transition"
      Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
      Tag: DS Parameter set: Current Channel: 48
      Tag: Country Information: Country Code IN, Environment All
      Tag: Power Constraint: 0
      Tag: RSN Information
      Tag: QSSS Load Element 802.11e CCA Version
      Tag: RM Enabled Capabilities (5 octets)
      Tag: HT Capabilities (802.11n D1.10)
      Tag: HT Information (802.11n D1.10)
      Tag: Extended Capabilities (8 octets)
      Tag: VHT Capabilities
      Tag: VHT Operation
      Tag: Tx Power Envelope
      Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
      Tag: Vendor Specific: Cisco Systems, Inc: Aironet CCX version = 5
      Tag: Vendor Specific: Cisco Systems, Inc: Aironet Client MFP Disabled
      Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (11) (11)
      Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (44)
      Tag: Vendor Specific: Wi-Fi Alliance: OWE Transition Mode
        Tag Number: Vendor Specific (221)
        Tag length: 19
        OUI: 50:6f:9a (Wi-Fi Alliance)
        Vendor Specific OUI Type: 28
        BSSID: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f)
        SSID length: 8
        SSID: OPEN-OWE
```

이미지-4: 프로브 응답

OPEN 인증

- 프로브 응답을 받은 후 연결 전에 클라이언트와 AP 간에 OPEN 인증을 수행하여 클라이언트 wifi 세부사항/기능을 확인할 수 있습니다.

No.	Time	Source	Destination	Protocol	Length	Info
8517	2025-01-21 09:51:57.327250	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	802.11	70	Authentication, SN=1, FN=0, Flags=.....C
8518	2025-01-21 09:51:57.327265		ee:13:e8:a8:cd:5b	802.11	48	Acknowledgement, Flags=.....C
> Frame 8517: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) > Radiotap Header v0, Length 36 > 802.11 radio information > IEEE 802.11 Authentication, Flags:C Type/Subtype: Authentication (0x000b) > Frame Control Field: 0xb000 .000 0000 0011 1100 = Duration: 60 microseconds > Receiver address: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f) > Destination address: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f) > Transmitter address: ee:13:e8:a8:cd:5b (ee:13:e8:a8:cd:5b) > Source address: ee:13:e8:a8:cd:5b (ee:13:e8:a8:cd:5b) > BSS Id: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f) 0000 = Fragment number: 0 0000 0000 0001 = Sequence number: 1 Frame check sequence: 0x928f3869 [unverified] [FCS Status: Unverified] [WLAN Flags:C]						
> IEEE 802.11 Wireless Management > Fixed parameters (6 bytes) Authentication Algorithm: Open System (0) Authentication SEQ: 0x0001 Status code: Successful (0x0000)						

No.	Time	Source	Destination	Protocol	Length	Info
8520	2025-01-21 09:51:57.327278	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	802.11	70	Authentication, SN=783, FN=0, Flags=.....C
8521	2025-01-21 09:51:57.327349		Cisco_dd:2e:8f	802.11	48	Acknowledgement, Flags=.....C
8522	2025-01-21 09:51:57.329457	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	802.11	337	Association Request, SN=2, FN=0, Flags=.....C, SSID="OWE-Transition"
8523	2025-01-21 09:51:57.329466		ee:13:e8:a8:cd:5b	802.11	48	Acknowledgement, Flags=.....C
> Frame 8520: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) > Radiotap Header v0, Length 36 > 802.11 radio information > IEEE 802.11 Authentication, Flags:C Type/Subtype: Authentication (0x000b) > Frame Control Field: 0xb000 .000 0000 0011 1100 = Duration: 60 microseconds > Receiver address: ee:13:e8:a8:cd:5b (ee:13:e8:a8:cd:5b) > Destination address: ee:13:e8:a8:cd:5b (ee:13:e8:a8:cd:5b) > Transmitter address: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f) > Source address: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f) > BSS Id: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f) 0000 = Fragment number: 0 0011 0000 1111 = Sequence number: 783 Frame check sequence: 0xc3c21908 [unverified] [FCS Status: Unverified] [WLAN Flags:C]						
> IEEE 802.11 Wireless Management > Fixed parameters (6 bytes) Authentication Algorithm: Open System (0) Authentication SEQ: 0x0002 Status code: Successful (0x0000)						

이미지-5: Probe 성공 후 OPEN 인증

클라이언트에서 AP로의 연결 요청

- 이 패킷에서는 클라이언트가 암호화를 위해 Diffie-Hellman 매개변수 값을 연결할 수 있습니다

No.	Time	Source	Destination	Protocol	Length	Info
8522	2025-01-21 09:51:57.329457	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	802.11	337	Association Request, SN=2, FN=0, Flags=.....C, SSID="OWE-Transition"
8523	2025-01-21 09:51:57.329466		ee:13:e8:a8:cd:5b	802.11	48	Acknowledgement, Flags=.....C
> Frame 8522: 337 bytes on wire (2696 bits), 337 bytes captured (2696 bits) > Radiotap Header v0, Length 36 > 802.11 radio information > IEEE 802.11 Association Request, Flags:C > IEEE 802.11 Wireless Management > Fixed parameters (4 bytes) > Tagged parameters (269 bytes) Tag: SSID parameter set: "OWE-Transition" Tag Number: SSID parameter set (0) Tag length: 14 SSID: "OWE-Transition" > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec] > Tag: Power Capability Min: -20, Max: 14 > Tag: Supported Channels > Tag: HT Capabilities (802.11n D1.10) > Tag: RSN Information > Tag: RM Enabled Capabilities (5 octets) > Tag: Supported Operating Classes > Tag: Extended Capabilities (11 octets) > Tag: VHT Capabilities > Tag: Vendor Specific: Samsung Electronics Co.,Ltd > Tag: Vendor Specific: Samsung Electronics Co.,Ltd > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Information Element Ext Tag: OWE Diffie-Hellman Parameter Ext Tag length: 34 (Tag len: 35) Ext Tag Number: OWE Diffie-Hellman Parameter (32) Group: 256-bit random ECP group (19) Public Key: 7c2782ba4c77a98c7076d1fa2e3493347ec16d4c64345dccc8b9b68b212ff31						

이미지-6: 연결 요청

- RA 추적에서는 Association(연결) 단계에서 클라이언트 로그를 볼 수 있습니다.

2025/01/21 15:21:57.391071821 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (note): MAC: ee13.e8a8.cd5b
 2025/01/21 15:21:57.391117645 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (debug): MAC: ee13.e8a8.cd5b

AP에서 클라이언트로 보낸 연결 응답

No.	Time	Source	Destination	Protocol	Length	Info
8527	2025-01-21 09:51:57.333153	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	802.11	245	Association Response, SN=784, FN=0, Flags=.....C
8528	2025-01-21 09:51:57.333161	Cisco_dd:2e:8f	Cisco_dd:2e:8f	802.11	48	Acknowledgement, Flags=.....C

> Frame 8527: 245 bytes on wire (1960 bits), 245 bytes captured (1960 bits)

> Radiotap Header v0, Length 36

> 802.11 radio information

> IEEE 802.11 Association Response, Flags:

 Type/Subtype: Association Response (0x0001)

 > Frame Control Field: 0x1000

 .000 0000 0011 1100 = Duration: 60 microseconds

 > Receiver address: ee:13:e8:a8:cd:5b (ee:13:e8:a8:cd:5b)

 > Destination address: ee:13:e8:a8:cd:5b (ee:13:e8:a8:cd:5b)

 > Transmitter address: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f)

 > Source address: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f)

 > BSS Id: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f)

 0000 = Fragment number: 0

 0011 0001 0000 = Sequence number: 784

 Frame check sequence: 0x7fbed111 [unverified]

 [FCS Status: Unverified]

 [WLAN Flags:

> IEEE 802.11 Wireless Management

 > Fixed parameters (6 bytes)

 > Capabilities Information: 0x1111

 Status code: Successful (0x0000)

 ..00 0000 0000 0001 = Association ID: 0x0001

 > Tagged parameters (175 bytes)

 > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]

 > Tag: RSN Information

 > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element

 > Tag: HT Capabilities (802.11n D1.10)

 > Tag: HT Information (802.11n D1.10)

 > Tag: Extended Capabilities (8 octets)

 > Tag: VHT Capabilities

 > Tag: VHT Operation

 > Tag: RM Enabled Capabilities (5 octets)

 > Tag: BSS Max Idle Period

이미지-7: 연결 응답

2025/01/21 15:21:57.391334260 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5b
 2025/01/21 15:21:57.392296819 {wncd_x_R0-0}{1}: [dot11] [21675]: (note): MAC: ee13.e8a8.cd5b Association

키 교환

AP와 클라이언트 장치 간에 4-way 핸드셰이크가 발생할 수 있습니다.

Key-1 send by AP(AP에 의한 키-1 전송)

Key-2 클라이언트에서 전송

Key-3 send by AP(AP에 의한 키-3 전송)

Key-4 클라이언트에서 전송

No.	Time	Source	Destination	Protocol	Length	Info
8540	2025-01-21 09:51:57.360919	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	EAPOL	193	Key (Message 1 of 4)
8541	2025-01-21 09:51:57.360930	Cisco_dd:2e:8f	Cisco_dd:2e:8f	802.11	48	Acknowledgement, Flags=.....C
8542	2025-01-21 09:51:57.363375	Cisco_dd:2e:8f	Broadcast	802.11	376	Beacon frame, SN=3335, FN=0, Flags=.....C, BI=100, SSID="OPEN-OWE"
8543	2025-01-21 09:51:57.365594	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	EAPOL	215	Key (Message 2 of 4)
8544	2025-01-21 09:51:57.365603	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	802.11	48	Acknowledgement, Flags=.....C
8545	2025-01-21 09:51:57.366921	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	EAPOL	267	Key (Message 3 of 4)
8546	2025-01-21 09:51:57.366929	Cisco_dd:2e:8f	Cisco_dd:2e:8f	802.11	48	Acknowledgement, Flags=.....C
8547	2025-01-21 09:51:57.368482	Cisco_dd:2e:8f	Broadcast	802.11	376	Beacon frame, SN=3336, FN=0, Flags=.....C, BI=100, SSID="newssid"
8548	2025-01-21 09:51:57.373313	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	EAPOL	171	Key (Message 4 of 4)
8549	2025-01-21 09:51:57.373334	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	802.11	48	Acknowledgement, Flags=.....C

> Frame 8540: 193 bytes on wire (1544 bits), 193 bytes captured (1544 bits)
 > Radiotap Header v0, Length 34
 > 802.11 radio information
 > IEEE 802.11 QoS Data, Flags:F.C
 > Logical-Link Control
 > 802.1X Authentication
 Version: 802.1X-2004 (2)
 Type: Key (3)
 Length: 117
 Key Descriptor Type: EAPOL RSN Key (2)
 [Message number: 1]
 > Key Information: 0x0088
 Key Length: 16
 Replay Counter: 0
 WPA Key Nonce: 1728f47ac2427421f37f1b43b6f69471eaf8a1a78feb2e1083d188c5a2e05ded
 Key IV: 00000000000000000000000000000000
 WPA Key RSC: 00000000000000000000000000000000
 WPA Key ID: 00000000000000000000000000000000
 WPA Key MIC: 00000000000000000000000000000000
 WPA Key Data Length: 22
 > WPA Key Data: dd14000fac0421b550dab0a335c355e7f4daa4a633af

이미지-8: 4-Way 핸드셰이킹

```

2025/01/21 15:21:57.392538716 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.392557538 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.392640494 {wncd_x_R0-0}{1}: [client-auth] [21675]: (note): MAC: ee13.e8a8.cd5b L2
2025/01/21 15:21:57.394830551 {wncd_x_R0-0}{1}: [client-auth] [21675]: (info): MAC: ee13.e8a8.cd5b Cli
2025/01/21 15:21:57.395171903 {wncd_x_R0-0}{1}: [client-auth] [21675]: (info): MAC: ee13.e8a8.cd5b Cli
2025/01/21 15:21:57.420590731 {wncd_x_R0-0}{1}: [client-auth] [21675]: (info): MAC: ee13.e8a8.cd5b Cli

2025/01/21 15:21:57.420706435 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.420775720 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.426548998 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.426725965 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.426727805 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.434078994 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.434099154 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (note): MAC: ee13.e8a8.cd5b
  
```

L2 인증 성공

```

2025/01/21 15:21:57.434111288 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.434250308 {wncd_x_R0-0}{1}: [client-auth] [21675]: (note): MAC: ee13.e8a8.cd5b L2
2025/01/21 15:21:57.434286035 {wncd_x_R0-0}{1}: [client-auth] [21675]: (info): MAC: ee13.e8a8.cd5b Cli
2025/01/21 15:21:57.434308953 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (debug): MAC: ee13.e8a8.cd5b
  
```

IP 학습 상태

```
2025/01/21 15:21:57.434789679 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (note): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.436611026 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.437239513 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.437508189 {wncd_x_R0-0}{1}: [client-iplearn] [21675]: (info): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.534166453 {wncd_x_R0-0}{1}: [sisf-packet] [21675]: (info): TX: DHCPv4 from interface
2025/01/21 15:21:57.535325325 {wncd_x_R0-0}{1}: [client-iplearn] [21675]: (note): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.535874658 {wncd_x_R0-0}{1}: [sisf-packet] [21675]: (info): TX: DHCPv4 from interface
2025/01/21 15:21:57.536500021 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (debug): MAC: ee13.e8a8.cd5b
```

클라이언트 실행 상태

```
2025/01/21 15:21:57.537017277 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5b
```

WISE 암호화가 지원되지 않는 클라이언트

- 비콘 프레임 자체를 검토하면 클라이언트는 이 암호화 방법을 지원할 수 있는지 여부를 알게 됩니다. 지원되지 않는 경우, SSID "OPEN-WISE"를 열기 위해 프로브 요청을 보내고 일반적인 개방형 인증을 수행하여 IP 주소를 가져온 다음 RUN 상태로 전환할 수 있습니다.

```
2025/01/16 15:36:06.178370757 {wncd_x_R0-2}{1}: [client-orch-sm] [17332]: (note): MAC: d037.4587.8f35
2025/01/16 15:36:06.209288788 {wncd_x_R0-2}{1}: [dot11] [17332]: (note): MAC: d037.4587.8f35 Associati
2025/01/16 15:36:06.248651191 {wncd_x_R0-2}{1}: [client-auth] [17332]: (note): MAC: d037.4587.8f35 Ope
2025/01/16 15:36:06.248751507 {wncd_x_R0-2}{1}: [client-orch-state] [17332]: (note): MAC: d037.4587.8f3
2025/01/16 15:36:06.281808554 {wncd_x_R0-2}{1}: [client-orch-state] [17332]: (note): MAC: d037.4587.8f3
2025/01/16 15:36:06.303307756 {wncd_x_R0-2}{1}: [client-orch-state] [17332]: (note): MAC: d037.4587.8f3
2025/01/16 15:36:10.305041414 {wncd_x_R0-2}{1}: [client-iplearn] [17332]: (note): MAC: d037.4587.8f35
2025/01/16 15:36:10.305777492 {wncd_x_R0-2}{1}: [client-orch-state] [17332]: (note): MAC: d037.4587.8f3
```

빠른 전환 정보

- OPEN 인증 또는 Webauth(CWA/LWA/EWA)에서만 OWE를 구성할 수 있습니다.
- FT는 OWE 변환에서 지원되지 않습니다.
- FT를 활성화하면 다음과 같은 오류 메시지가 표시됩니다.

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
☐
WPA2 Policy
☐

GTK Randomize
☐
WPA3 Policy
☒

Transition Disable
☐

Fast Transition

Status
Enabled

Over the DS
☐

Reassociation Timeout *
20

WPA2/WPA3 Encryption

AES(CCMP128)
☒
CCMP256
☐

GCMP128
☐
GCMP256
☐

Protected Management Frame

PMF
Required

Association Comeback Timer*
1

SA Query Time*
200

Auth Key Mgmt

Fast Transition needs to be disabled

SAE
☐
FT + SAE
☐

OWE
☒
FT + 802.1X
☐

802.1X-SHA256
☐

Transition Mode WLAN ID
9

Cancel
Update & Apply to Device

이미지-9: Ownne Transition SSID에서 FT를 활성화하는 경우 오류 메시지

WISE는 PSK/dot1x에서 지원되지 않습니다.

이러한 조합에서는 OWE를 활성화할 수 없습니다.

1. 802.1x 또는 FT+802.1x
2. PSK 또는 FT+PSK 또는 PSK-SHA256
3. SAE 또는 FT+SAE
4. 802.1x-SHA256 또는 FT+802.1x-SHA256

이러한 방법 중 하나를 활성화하려고 하면

General **Security** Advanced Add To Policy Tags**Layer2** Layer3 AAA☐ WPA + WPA2☐ WPA2 + WPA3☒ WPA3☐ Static WEP☐ NoneMAC Filtering ☐Lobby Admin Access ☐

WPA Parameters

WPA Policy ☐GTK Randomize ☐WPA2 Policy ☐WPA3 Policy ☒Transition Disable ☐

WPA2/WPA3 Encryption

AES(CCMP128) ☒GCMP128 ☐CCMP256 ☐GCMP256 ☐

Protected Management Frame

PMF Required ▾

Association Comeback Timer* 1

SA Query Time* 200

Fast Transition

Status Disabled ▾

Over the DS ☐

Reassociation Timeout * 20

Auth Key Mgmt

OWE cannot be enabled with
802.1X/FT+802.1X/802.1X-SHA256/PSK/FT+PSK/PSK-
SHA256/CCKM/SAE/FT+SAE

SAE ☐FT + SAE ☐OWE ☒FT + 802.1X ☐802.1X-SHA256 ☒

Transition Mode WLAN ID 9

Cancel

Update & Apply to Device

이미지-10: WISE SSID에서 다른 인증 방법을 활성화하는 동안 오류 메시지를 받습니다.

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

☐

WPA2 Policy

☐

GTK Randomize

☐

WPA3 Policy

☒

Transition Disable

☐

WPA2/WPA3 Encryption

AES(CCMP128)

☒

CCMP256

☐

GCMP128

☐

GCMP256

☐

Protected Management Frame

PMF

Required

Association Comeback Timer*

1

SA Query Time*

200

Fast Transition

Status

Enabled

Over the DS

☐

Reassociation Timeout *

20

Auth Key Mgmt

Fast Transition needs to be disabled

OWE cannot be enabled with
802.1X/FT+802.1X/802.1X-SHA256/PSK/FT+PSK/PSK-SHA256/CCKM/SAE/FT+SAE

SAE

☐

FT + SAE

☐

OWE

☒

FT + 802.1X

☒

802.1X-SHA256

☒

Transition Mode WLAN ID

9

Cancel

Update & Apply to Device

이미지-11: AKM을 활성화하는 동안 오류 메시지 표시

- Cisco IOS® XE 17.9.6 IOS 버전에서는 "WPA2+WPA3"을 선택하면 AKM에서 "OWE" 옵션을 볼 수 있지만 이 조합에서는 OWE를 사용할 수 없다는 오류 메시지가 표시됩니다.

⚠ 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 Disabled ▾
 Over the DS ☐
 Reassociation Timeout * 20

WPA2/WPA3 Encryption

AES(CCMP128) ☒ CCMP256 ☐
 GCMP128 ☐ GCMP256 ☐

Protected Management Frame

PMF Required ▾
 Association Comeback Timer* 1
 SA Query Time* 200

Auth Key Mgmt

WPA2 security valid combinations: 1. SuiteB cipher, 2. 802.1X-SHA256/FT-802.1X/802.1X AKM and AES cipher, 3. PSK-SHA256/FT-PSK/PSK AKM and AES cipher, 4. CCKM AKM and AES Cipher

OWE is supported with WPA3 (WPA/WPA2 must be disabled)

802.1x ☐ PSK ☐
 CCKM ⚠ ☐ SAE ☐
 FT + SAE ☐ OWE ☒
 FT + 802.1x ☐ FT + PSK ☐
 802.1x-SHA256 ☐ PSK-SHA256 ☐
 Transition Mode WLAN ID 7

MPSK Configuration

Enable MPSK ☐

↶ Cancel

🔄 Update & Apply to Device

이미지-12: WPA2+WPA3을 선택할 때 오류 메시지 표시

- Cisco IOS® XE 17.12.4 버전에서는 "WPA2+WPA3"을 선택하면 AKM에서 "OWE" 옵션을 사

용할 수 없습니다.

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☐

GTK Randomize☐

WPA2 Policy☒

WPA3 Policy☒

Transition Disable☐

WPA2/WPA3 Encryption

AES(CCMP128)☒

GCMP128☐

CCMP256☐

GCMP256☐

Protected Management Frame

PMF

Required

Association Comeback Timer*

1

SA Query Time*

200

Fast Transition

Status

Enabled

Over the DS

☐

Reassociation Timeout *

20

Auth Key Mgmt

WPA2 security valid combinations: 1. SuiteB cipher, 2. 802.1X-SHA256/FT-802.1X/802.1X AKM and AES cipher, 3. PSK-SHA256/FT-PSK/PSK AKM and AES cipher, 4. CCKM AKM and AES Cipher

WPA3 security valid combinations: 1. SuiteB cipher, 2. 802.1X-SHA256/FT-802.1X AKM and AES cipher, 3. SAE/FT-SAE/OWE AKM and AES cipher.

802.1X☐

PSK☐

CCKM ⚠☐

SAE☐

FT + SAE☐

FT + 802.1X☐

FT + PSK☐

802.1X-SHA256☐

PSK-SHA256☐

MPSK Configuration

Enable MPSK

☐

↶ Cancel

📄 Update & Apply to Device

이미지-13: 오류 메시지 - AKM에서 WISE 옵션을 가져오지 않음

문제 해결

1. WLAN, OPEN SSID 및 OWE Transition SSID 모두에서 컨피그레이션을 확인하려면 전환 WLAN ID가 매핑되어야 합니다.
2. Broadcasting 옵션은 WISE 전환 SSID에서 비활성화해야 하며 OPEN SSID에서만 활성화해야 합니다.
3. 이 문서에 설명된 지원되는 인증/암호화/FT 방법을 확인하십시오.
4. WLC 쪽에서 컨피그레이션이 괜찮은 경우, 에서는 필요한 로그와 출력을 수집하여 문제를 좁혀 주십시오.

RA 추적 및 EPC(임베디드 패킷 캡처)

WLC GUI에 로그인 -> 문제 해결 -> Radioactive Trace(방사능 추적) -> Add client wifi MAC address(클라이언트 wifi MAC 주소 추가) -> Click that clients(해당 클라이언트) 확인란 -> Start(시작)

WLC GUI에 로그인 -> 문제 해결 -> 패킷 캡처 -> 새 파일 이름 추가 -> 업링크 인터페이스 및 WMI VLAN/Interface -> Start(시작)를 선택합니다.

클라이언트 컴퓨터에서: 가능하면 wireshark 애플리케이션을 설치하고 WiFi 인터페이스를 선택하여 패킷 캡처를 수집할 수 있습니다.

<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213949-wireless-debugging-and-log-collection-on.html#anc12>

항공 모함

MAC 랩톱을 사용하거나 AP 중 하나를 스니퍼 모드로 구성하여 수집할 수 있습니다. 이 링크를 참조하십시오.

MAC 노트북 컴퓨터에서:

<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-mobility/217042-collect-packet-captures-over-the-air-on.html>

스니퍼 AP에서:

<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/217057-configure-access-point-in-sniffer-mode-o.html>

한 랩톱(wireshark 서버)을 스위치 포트에 연결하고 wireshark 애플리케이션이 설치되어 있어야 하며 이 wireshark 서버는 WLC WMI 인터페이스에 연결할 수 있어야 합니다. WLC와 wireshark 서버 사이에 프로토콜이 있는 경우 방화벽에서 "5555 또는 5000 또는 5556"을 허용해야 합니다.

wireshark가 설치된 PC에 "gscaler"가 설치되어 있는지 확인하고, "꺼주십시오", Windows Defender와 같은 방화벽이나 그 안에 있는 것이 있으면 비활성화하고 PCAP를 수집해 보십시오.

로밍

클라이언트가 한 AP에서 다른 AP로 로밍할 때 다음 단계를 수행해야 합니다.

- 다시 연결/연결을 전송해야 함 - 클라이언트 요청에 따라 다릅니다.
- 연결 요청에서 DH(Diffie-Helman) 세부 정보를 전송해야 합니다.
- 클라이언트는 이 PMK가 클라이언트와 AP 모두에서 생성됨을 기반으로 AP로부터 연결 응답에서 DH 세부사항을 가져올 수 있습니다.
- AP와 클라이언트 간에 4-Way 핸드셰이크가 발생할 수 있습니다.
- OWE에서는 FT를 활성화할 수 없으므로 802.11r을 사용할 수 없습니다.
- 클라이언트가 로밍할 때마다 DH 교환 후 4방향 핸드셰이크를 해야 합니다.
- 자체 PMKID를 사용하는 클라이언트와 AP는 각 AP 및 클라이언트마다 고유합니다.
- 클라이언트가 동일한 AP에 연결하는 경우 동일한 PMKID를 사용할 수 없습니다. 어떤 시나리오에서는 클라이언트가 AP보다 삭제되어 새 PMKID를 생성할 수 있지만 클라이언트는 4방향 핸드셰이크에 동일한 PMKID를 사용합니다.

예:

클라이언트가 동일한 AP에 연결된 경우 Association-Request 및 Association-Response 모두에서 동일한 PMKID를 볼 수 있습니다. 연결 응답에서 동일한 PMKID를 사용하는 경우 DH 세부사항을 볼 수 없습니다.

```
8522 2025-01-21 09:51:57.329457 ee:13:e8:a8:cd:5b Cisco_dd:2e:8f 802.11 337 21 b5 50 da b0 a3 35 c3 55 e7 f4 da a4 a6 33 af Association Request, SN=2, FN=0, Flags=.....C, SSID="OWE-Tr
44117 2025-01-21 09:53:12.847592 ee:13:e8:a8:cd:5b Cisco_dd:2e:8f 802.11 337 21 b5 50 da b0 a3 35 c3 55 e7 f4 da a4 a6 33 af Association Request, SN=2, FN=0, Flags=.....C, SSID="OWE-Tr

> Frame 8522: 337 bytes on wire (2696 bits), 337 bytes captured (2696 bits)
> Radiotap Header v0, Length 36
> 802.11 radio information
> IEEE 802.11 Association Request, Flags: .....C
> IEEE 802.11 Wireless Management
  > Fixed parameters (4 bytes)
  > Tagged parameters (269 bytes)
    > Tag: SSID parameter set: "OWE-Transition"
    > Tag: Supported Rates 6(B), 9, 12(B), 10, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: Power Capability Min: -20, Max: 14
    > Tag: Supported Channels
    > Tag: HT Capabilities (802.11n D1.10)
    > Tag: RSN Information
      Tag Number: RSN Information (48)
      Tag length: 42
      RSN Version: 1
      > Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
      Pairwise Cipher Suite Count: 1
      > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
      Auth Key Management (AKM) Suite Count: 1
      > Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) Opportunistic Wireless Encryption
      RSN Capabilities: 0x00c0
      PMKID Count: 1
      > PMKID List
        PMKID: 21 b5 50 da b0 a3 35 c3 55 e7 f4 da a4 a6 33 af
      > Group Management Cipher Suite: 00:0f:ac (Ieee 802.11) BIP (128)
    > Tag: RM Enabled Capabilities (5 octets)
    > Tag: Supported Operating Classes
    > Tag: Extended Capabilities (11 octets)
    > Tag: VHT Capabilities
    > Tag: Vendor Specific: Samsung Electronics Co.,Ltd
    > Tag: Vendor Specific: Samsung Electronics Co.,Ltd
    > Tag: Vendor Specific: Microsoft Corp.: MRM/OME: Information Element
  > Ext Tag: OWE Diffie-Hellman Parameter
    Ext Tag Length: 34 (Tag len: 35)
    Ext Tag Number: OWE Diffie-Hellman Parameter (32)
    Group: 256-bit random ECP group (19)
    Public Key: 7c 27 82 ba 4c 77 a9 8c 70 76 d1 fa 2e 34 93 34 7e c1 6d 4c 64 34 5d cc f8 b9 bb 68 b2 ff 31
```

이미지-14: 동일한 PMKID 사용

이미지-17: AP는 DH 값을 사용하여 새 PMKID를 생성합니다.

이 예에서는 다음을 수행합니다. AP와 클라이언트 모두 4-Way 핸드셰이크를 수행하는 동안 동일한 PMKID를 사용하며 "M1 및 M2" 메시지를 체크인합니다.

No.	Time	Source	Destination	Protocol	Length	Sequence Number (BE)	PMKID	Info
8540	2025-01-21 09:51:57.360919	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	EAPOL	193			Key (Message 1 of 4)
8543	2025-01-21 09:51:57.365594	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	EAPOL	215		21 b5 50 da b0 a3 35 c3 55 e7 f4 da a4 a6 33 af	Key (Message 2 of 4)
8545	2025-01-21 09:51:57.366921	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	EAPOL	267			Key (Message 3 of 4)
8548	2025-01-21 09:51:57.373313	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	EAPOL	171			Key (Message 4 of 4)

> Frame 8540: 193 bytes on wire (1544 bits), 193 bytes captured (1544 bits)

> Radiotap Header v0, Length 34

> 802.11 radio information

> IEEE 802.11 QoS Data, Flags:F.C

> Logical-Link Control

> 802.1X Authentication

Version: 802.1X-2004 (2)

Type: Key (3)

Length: 117

Key Descriptor Type: EAPOL RSN Key (2)

[Message number: 1]

> Key Information: 0x0088

Key Length: 16

Replay Counter: 0

WPA Key Nonce: 17 28 f4 7a c2 42 74 21 f3 7f 1b 43 b6 f6 94 71 ea f8 a1 a7 8f eb 2e 10 83 d1 88 c5 a2 e0 5d ed

Key IV: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

WPA Key RSC: 00 00 00 00 00 00 00 00

WPA Key ID: 00 00 00 00 00 00 00 00

WPA Key MIC: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

WPA Key Data Length: 22

> WPA Key Data: dd 14 00 0f ac 04 21 b5 50 da b0 a3 35 c3 55 e7 f4 da a4 a6 33 af

> Tag: Vendor Specific: IEEE 802.11: RSN PMKID

Tag Number: Vendor Specific (221)

Tag Length: 20

OUI: 00:0f:ac (IEEE 802.11)

Vendor Specific OUI Type: 4

Data Type: PMKID KDE (4)

PMKID: 21 b5 50 da b0 a3 35 c3 55 e7 f4 da a4 a6 33 af

이미지- 18: 동일한 PMKID를 사용하는 AP 및 클라이언트

이 예에서는 다음을 수행합니다. 동일한 PMKID를 사용하지만 클라이언트가 삭제된 후 생성된 다른 PMKID를 사용하는 AP를 사용하는 클라이언트는 "M1 및 M2" 메시지를 확인합니다.

No.	Time	Source	Destination	Protocol	Length	Sequence Number (BE)	PMKID	Info
44128	2025-01-21 09:53:12.857869	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	EAPOL	193			Key (Message 1 of 4)
44133	2025-01-21 09:53:12.861273	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	EAPOL	215		21 b5 50 da b0 a3 35 c3 55 e7 f4 da a4 a6 33 af	Key (Message 2 of 4)
44135	2025-01-21 09:53:12.862728	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	EAPOL	267			Key (Message 3 of 4)
44138	2025-01-21 09:53:12.865398	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	EAPOL	171			Key (Message 4 of 4)

> Frame 44128: 193 bytes on wire (1544 bits), 193 bytes captured (1544 bits)

> Radiotap Header v0, Length 34

> 802.11 radio information

> IEEE 802.11 QoS Data, Flags:R.F.C

> Logical-Link Control

> 802.1X Authentication

Version: 802.1X-2004 (2)

Type: Key (3)

Length: 117

Key Descriptor Type: EAPOL RSN Key (2)

[Message number: 1]

> Key Information: 0x0088

Key Length: 16

Replay Counter: 0

WPA Key Nonce: 17 28 f4 7a c2 42 74 21 f3 7f 1b 43 b6 f6 94 71 ea f8 a1 a7 8f eb 2e 10 83 d1 88 c5 a2 e0 5d ee

Key IV: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

WPA Key RSC: 00 00 00 00 00 00 00 00

WPA Key ID: 00 00 00 00 00 00 00 00

WPA Key MIC: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

WPA Key Data Length: 22

> WPA Key Data: dd 14 00 0f ac 04 41 1b cf d7 7a 34 cb 50 70 13 07 47 b8 d2 4e 1f

> Tag: Vendor Specific: IEEE 802.11: RSN PMKID

Tag Number: Vendor Specific (221)

Tag Length: 20

OUI: 00:0f:ac (IEEE 802.11)

Vendor Specific OUI Type: 4

Data Type: PMKID KDE (4)

PMKID: 41 1b cf d7 7a 34 cb 50 70 13 07 47 b8 d2 4e 1f

이미지-19: 다른 PMKID를 사용하는 AP 및 클라이언트

내부 RA 추적에서:

이 예에서는 다음을 수행합니다. 클라이언트가 연결 요청에서 DH 매개변수를 보냈고 AP가 PMK를 생성한 것보다 처리했습니다.

2025/01/21 15:18:50.157081690 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157082294 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157523328 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b

```
2025/01/21 15:18:50.157531792 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157532236 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157532538 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157841380 {wncd_x_R0-0}{1}: [dot11-frame] [21675]: (debug): MAC: ee13.e8a8.cd5b OW
```

그 후 동일한 클라이언트가 동일한 AP에 연결되었지만 AP에서 새 PMKID를 생성하지 않았습니다.

```
2025/01/21 15:21:57.391898613 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.391903915 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.391906073 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.391906329 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
```

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.