

Understand Opportunistic Wireless Encryption Flow

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Description](#)

[Steps](#)

[Details of Lab Repro](#)

[OWE FLOW](#)

[Original Beacon frame](#)

[Hidden SSID Beacons](#)

[Probe Request sent from client to OWE Transition SSID](#)

[Probe Response sent from AP to Client](#)

[OPEN authentication](#)

[Association Request from client to AP](#)

[Association Response sent from AP to Client](#)

[Key Exchange](#)

[L2 Authentication Successful](#)

[IP Learning State](#)

[Client in RUN state](#)

[Clients which are not supported for OWE encryption](#)

[Fast Transition Information](#)

[OWE is not supported with PSK/dot1x](#)

[Troubleshooting](#)

[RA Trace and EPC\(Embedded Packet Capture\)](#)

[AIR PCAP](#)

[Roaming](#)

Introduction

This document describes OWE transition flow and how it works on the Catalyst 9800 Wireless LAN Controller (WLC).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- How to configure the 9800 WLC, the Access Point (AP) for basic operation
- How to configure WLAN and Policy Profiles.

Components Used

The information in this document is based on these software and hardware versions:

- C9800-80, Cisco IOS® XE 17.12.4 and also tested in Cisco IOS® XE 17.9.6
- AP model : C9136I, checked in both local and flex connect mode.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Description

- OWE (Opportunistic Wireless Encryption) is an extension to IEEE 802.11 which provides encryption for the wireless medium. The purpose of OWE based authentication is to avoid open unsecured wireless connectivity between the AP's and clients.
- The OWE uses the Diffie-Hellman algorithms-based Cryptography to setup the wireless encryption.
- With OWE, the client and AP perform a Diffie-Hellman key exchange during the access procedure and use the resulting pairwise secret with the 4-way handshake.
- The use of OWE enhances wireless network security for deployments where Open or shared PSK based networks are deployed.

Steps

1. Configure one OPEN WLAN without any encryption/security and enable broadcasting.
2. Configure another SSID with OWE security settings and map the OPEN WLAN ID number in transition-mode-wlan-id. Disable broadcast SSID option in this OWE transition SSID.
3. Map the OWE transition WLAN ID number in OPEN WLAN "transition-mode-wlan-id" field.

Details of Lab Repro

- Open SSID Name: OPEN-OWE
- OWE Transition SSID Name: OWE-Transition
- BSSID of OPEN-OWE: 40:ce:24:dd:2e:87
- BSSID of OWE-Transition: 40:ce:24:dd:2e:8f

OWE FLOW

1. Beacons can be broadcast for OPEN SSID. You can see it by its SSID name in AIR PCAP.
2. We can also see the hidden security enabled SSID with the name "Wildcard" instead of its own SSID name in AIR PCAP.
3. Once the clients receive the beacon frame for OPEN SSID, if it has or supports OWE, then it can start sending probe request to OWE transition SSID (which is that security enabled SSID instead of OPEN SSID).

4. OWE supported clients can get probe response from transition SSID.
5. OPEN authentication can happen between client and AP.
6. Client can send association request to the AP with DH key exchange details and use the resulting pairwise secret for 4-way handshake.
7. AP can send association response.
8. Four-Way handshake can happen between AP and client device.
9. After successful key management, L2 PSK can be successful.
10. Client can get IP from DHCP, ARP etc.,
11. Client can go to RUN state.
12. If client devices which are not supporting OWE, then it can send probe request to OPEN SSID itself and it can directly get IP than it can go to RUN state.

Original Beacon frame

- Here, AIR PCAP shows that, the SSID "OPEN-OWE" broadcasting (Beacon Frame). Which contains transition SSID details and it called "OWE-Transition".

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) > 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						

Image-1 : Beacon Frame of OPEN SSID

Hidden SSID Beacons

- As per WLAN configuration, "broadcasting" is disabled for this "OWE-Transition" SSID, however, you can see hidden SSID beacons in AIR PCAP which contain the SSID Name "Wildcard". However, if you check that packet, it contains OWE-Transition details.
- Get the BSSID of hidden SSID by using the this packet, such as "40:ce:24:dd:2e:8f" and search it in packet capture.
- In this packet, it shows that, SSID "Missing" and it contains its transition SSID as "OPEN-OWE" and its BSSID "40:ce:24:dd:2e:8f".

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 D1.10) > 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						

Image-2 : Hidden SSID - OWE Transition

Probe Request sent from client to OWE Transition SSID

- Based on the beacon frame "OPEN-OWE" SSID, the client comes to know the other SSID details which it needs to connect, in this scenario, it is "OWE-Transition". If client is able to support OWE encryption, then it can send the probe request to "OWE-Transition" SSID and get a response.
- Probe request sent to OWE-Transition BSSID "40:ce:24:dd:2e:8f" and got a response. Inside this probe response packet also, you can see OPEN-OWE SSID details.

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	Cisco_dd:2e:8f	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	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 D1.10) > 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						

Image-3 : Probe Request

Probe Response sent from AP to Client

- Client received probe response for the SSID "OWE-Transition" however it has its original SSID details "OPEN-OWE" in WiFi Alliance.

```

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: QoS 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

```

Image-4 : Probe Response

OPEN authentication

- After getting probe response, OPEN authentication can happen between Client and AP to check the clients wifi details/capabilities, before association.

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)						

Image-5 : OPEN Authentication after successful Probe

Association Request from client to AP

- In this packet, notice the client can be attaching Diffie-Hellman parameter value for encryption.

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: 7c2782ba4c77a98c7076d1fa2e3493347ec16d4c64345dccc78b9bb68b212ff31						

Image-6 : Association Request

- In RA trace, you can start seeing the client logs from Association phase,

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

Association Response sent from AP to Client

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		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

Image-7 : Association Response

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 Response sent from AP to Client

Key Exchange

4-way handshake can happen between AP and client device.

Key-1 send by AP

Key-2 send by client

Key-3 send by AP

Key-4 send by client

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	Broadcast	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	Broadcast	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	ee:13:e8:a8:cd:5b	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: 0000000000000000
 WPA Key ID: 0000000000000000
 WPA Key MIC: 00000000000000000000000000000000
 WPA Key Data Length: 22
 > WPA Key Data: dd1400fac0421b550dab0a335c355e7f4daa4a633af

Image-8 : 4-Way Handshake

```

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 C1i
2025/01/21 15:21:57.395171903 {wncd_x_R0-0}{1}: [client-auth] [21675]: (info): MAC: ee13.e8a8.cd5b C1i
2025/01/21 15:21:57.420590731 {wncd_x_R0-0}{1}: [client-auth] [21675]: (info): MAC: ee13.e8a8.cd5b C1i

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 Authentication Successful

```

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 C1i
2025/01/21 15:21:57.434308953 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (debug): MAC: ee13.e8a8.cd5b

```

IP Learning State


```

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

```

Client in RUN state

```

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

```

Clients which are not supported for OWE encryption

- By reviewing a beacon frame itself, the clients come to know, whether they are able to support this encryption method or not. If it is not supported, then it can just send a probe request to open SSID “OPEN-OWE” and can do a normal open authentication, get IP address, then it can go the RUN state.

```

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

```

Fast Transition Information

- We are able to configure OWE only in OPEN authentication or in Webauth (CWA/LWA/EWA).
- FT is not supported in OWE transition.
- If you enable FT, you get this error message,

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
☐

Fast Transition

Status
Enabled

Over the DS
☐

Reassociation Timeout *
20

WPA2/WPA3 Encryption

AES(CCMP128)
☒

GCMP128
☐

CCMP256
☐

GCMP256
☐

Protected Management Frame

PMF
Required

Association Comeback Timer*
1

SA Query Time*
200

Auth Key Mgmt

Fast Transition needs to be disabled

SAE
☐

OWE
☒

802.1X-SHA256
☐

FT + SAE
☐

FT + 802.1X
☐

Transition Mode WLAN ID
9

Cancel
Update & Apply to Device

Image-9 : Error Message when we enable FT in OWE Transition SSID

OWE is not supported with PSK/dot1x

We are not able to enable OWE in these combinations,

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

If you try to enable any one of the these methods, you can get the error message,

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 Association Comeback Timer* SA Query Time*

Fast Transition

Status Over the DS ☐Reassociation Timeout *

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

Cancel

Update & Apply to Device

Image-10: Error Message getting while enabling other authentication methods in OWE SSID

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

Image-11: Error Message while enabling AKM

- In Cisco IOS® XE 17.9.6 IOS version, you can see "OWE" option under AKM when you select "WPA2+WPA3" however you can get the error message, you are not able to use OWE with this combination.

⚠ 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

Image-12: Error message when we choose WPA2+WPA3

- In Cisco IOS® XE 17.12.4 version, when you choose "WPA2+WPA3", you cannot get the option "OWE" in AKM,

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
☐
CCKM
☐
FT + SAE
☐
FT + PSK
☐
PSK-SHA256
☐

PSK
☐
SAE
☐
FT + 802.1X
☐
802.1X-SHA256
☐

MPSK Configuration

Enable MPSK
☐

Cancel
Update & Apply to Device

Image-13 : Error Message - Not getting OWE option in AKM

Troubleshooting

1. Check the configurations in both the WLANs, in OPEN SSID and in OWE transition SSID must have transition WLAN ID mapped.
2. Broadcasting option must be disabled in OWE transition SSID, it must be enabled only in OPEN SSID.
3. Check the supported authentication/encryption/FT methods described in this article.
4. If the configurations are fine from WLC end, then please collect the required logs and outputs to narrow down the issue,

RA Trace and EPC (Embedded Packet Capture)

Login to WLC GUI -> Troubleshooting -> Radioactive Trace -> Add client wifi MAC address -> Click that clients checkbox -> Start

Login to WLC GUI -> Troubleshooting -> Packet Capture -> Add new file name -> Choose the uplink interface and WMI VLAN/Interface -> Start.

From Client Machine: If possible, you can install wireshark application and collect the packet capture by choosing WiFi interface.

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

AIR PCAP

You can collect it by using MAC laptop or configuring one of the AP in to sniffer mode, please refer these links,

From MAC laptop:

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

From Sniffer AP:

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

Connect one laptop (wireshark server) to the switch port and it must have wireshark application installed in it, this wireshark server must have reachability to WLC WMI interface. Need to allow the protocol "5555 or 5000 or 5556" in firewall if it presents in between your WLC and wireshark server.

Check is there any "gscaler" installed in that PC where wireshark installed, if it is than please "turn off" and try, if it is any firewall like windows defender or anything present in it, please disable those and try to collect PCAP.

Roaming

When client roams from one AP to another, it needs to do these steps,

- Need to send re-association/association - Depends on the client request.
- Need to send DH (Diffie-Helman) details in association request.
- Client can get DH details in association response from AP, based on this PMK gets generated in both client and AP.
- 4-Way handshake can happen between AP and client.

- In OWE, you are unable to enable FT, so 802.11r is not possible.
- Each time, when client roams, it needs to do 4-way handshake after DH exchange in association.
- Client and AP using its own PMKID, it is unique for each APs and clients.
- If client connects to the same AP, than it can use the same PMKID. In some scenario, if the client got deleted than AP can generate a new PMKID however the client uses the same PMKID for 4-way handshake.

Example:

If client connects to the same AP, then you can see same PMKID in both Association-Request and Association-Response. In Association response, you cannot see DH details if it uses the same PMKID.

8522	2025-01-21 09:51:57.329457	ee:13:e8:a8:cd:5b	Cisco_ddi2e: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_ddi2e: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), 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 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) GIP (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.: 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: 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 12 ff 31
  
```

Image-14: Using Same PMKID

No.	Time	Source	Destination	Protocol	Length	Sequence Number (BE)	PMKID	Info
8527	2025-01-21 09:51:57.333153	Cisco_ddi2e:8f	ee:13:e8:a8:cd:5b	802.11	245		21 b5 50 da b0 a3 35 c3 55 e7 f4 da a4 a6 33 af	Association Response, SN=784, FN=0, 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: .....C
> IEEE 802.11 Wireless Management
  > Fixed parameters (6 bytes)
  > Tagged parameters (175 bytes)
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > 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) GIP (128)
    > 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
  
```

Image-15: Association Response with same PMKID

For testing, deleted this client manually from WLC and it got associated again to the same AP, at this time, the client sends a same PMKID however AP sends DH details in association response.

Image-16: After deleting, Client sent same PMKID with DH details

Image-17: AP uses DH values to generate its new PMKID

In this example: Both AP and client uses the same PMKID while doing 4-Way handshake, check in "M1 and in M2" messages.

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

Image- 18: AP and Client using the same PMKID

In this example: Client using the same PMKID but AP using different PMKID which it generated after client got deleted, check "M1 and M2" messages.

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

Image-19: AP and Client using different PMKID

From Internal RA Trace:

In this example: Client sent DH parameters in association-request and AP processed then generated the PMK.

```
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
```

After this, the same client connecting to the same AP, at this time, AP did not generated new PMKID,

```
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
```