

瞭解機會無線加密流程

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[說明](#)

[步驟](#)

[Lab Repro詳細資訊](#)

[OWE FLOW](#)

[原始信標幀](#)

[隱藏的SSID信標](#)

[從客戶端傳送到OWE轉換SSID的探測請求](#)

[從AP傳送到客戶端的探測響應](#)

[開放式身份驗證](#)

[從客戶端到AP的關聯請求](#)

[從AP傳送到客戶端的關聯響應](#)

[金鑰交換](#)

[L2身份驗證成功](#)

[IP學習狀態](#)

[客戶端處於運行狀態](#)

[不支援OWE加密的客戶端](#)

[快速過渡資訊](#)

[PSK/dot1x不支援OWE](#)

[疑難排解](#)

[RA跟蹤和EPC \(嵌入式資料包捕獲 \)](#)

[AIR PCAP](#)

[漫遊](#)

簡介

本檔案介紹OWE轉換流程及其在Catalyst 9800無線LAN控制器(WLC)上的運作方式。

必要條件

需求

思科建議您瞭解以下主題：

- 如何設定9800 WLC(存取點(AP))以達成基本操作
- 如何配置WLAN和策略配置檔案。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- C9800-80、Cisco IOS® XE 17.12.4，還在Cisco IOS® XE 17.9.6中進行了測試
- AP型號：C9136I，已檢查本地和靈活連線模式。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

說明

- OWE（機會無線加密）是對IEEE 802.11的擴展，為無線介質提供加密。基於OWE的身份驗證的目的是避免AP和客戶端之間的開放式非安全無線連線。
- OWE使用基於Diffie-Hellman演算法的加密來設定無線加密。
- 使用OWE時，客戶端和AP在訪問過程中執行Diffie-Hellman金鑰交換，並將生成的配對金鑰與4次握手一起使用。
- 使用 OWE 可提升部署開放式或共用 PSK 型網路時的無線網路安全性。

步驟

1. 配置一個OPEN WLAN而不使用任何加密/安全並啟用廣播。
2. 使用OWE安全設定配置另一個SSID，並在過渡模式 — wlan-id中對映開放式WLAN ID號。禁用此OWE過渡SSID中的廣播SSID選項。
3. 在OPEN WLAN「transition-mode-wlan-id」欄位中對映OWE轉換WLAN ID號。

Lab Repro詳細資訊

- 開放式SSID名稱：未結欠款
- OWE轉換SSID名稱：OWE-Transition
- OPEN-OWE的BSSID:40:ce:24:dd:2e:87
- OWE-Transition的BSSID:40:ce:24:dd:2e:8f

OWE FLOW

1. 可以廣播開放式SSID的信標。您可以在AIR PCAP中通過其SSID名稱看到它。
2. 我們還可以在AIR PCAP中看到名為「Wildcard」（萬用字元）而不是其自身SSID名稱的已啟用隱藏安全SSID。
3. 一旦客戶端收到開放SSID的信標幀（如果它有或支援OWE），就可以開始向OWE轉換SSID（即已啟用安全的SSID而不是開放SSID）傳送探測請求。
4. OWE支援的客戶端可以從轉換SSID獲取探測響應。

5. 客戶端和AP之間可以進行OPEN身份驗證。
6. 客戶端可以向AP傳送包含DH金鑰交換詳細資訊的關聯請求，並將生成的配對金鑰用於4次握手。
7. AP可以傳送關聯響應。
8. AP和客戶端裝置之間可能會發生四次握手。
9. 金鑰管理成功後，L2 PSK可以成功。
10. 客戶端可以從DHCP、ARP等獲取IP。
11. 客戶端可以進入RUN狀態。
12. 如果不支援OWE的客戶端裝置，則它可以向OPEN SSID本身傳送探測請求，並且它可以直接獲取IP，而不是進入RUN狀態。

原始信標幀

- 此處，AIR PCAP顯示SSID「OPEN-OWE」廣播（信標幀）。包含轉換SSID詳細資訊，稱為「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
  
```

圖1：開放式SSID的信標幀

隱藏的SSID信標

- 根據WLAN配置，此「OWE-Transition」SSID禁用「廣播」，但是您可以看到AIR PCAP中包含SSID名稱「Wildcard」的隱藏SSID信標。但是，如果檢查該資料包，它包含OWE-Transition詳細資訊。
- 使用此資料包（如「40:ce:24:dd:2e:8f」）獲取隱藏SSID的BSSID，並在資料包捕獲中搜尋它。
- 在此資料包中，它顯示SSID「Missing」，並包含其轉換SSID為「OPEN-OWE」和BSSID「40:ce:24:dd:2e:87」。

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						

圖2:隱藏SSID - OWE轉換

從客戶端傳送到OWE轉換SSID的探測請求

- 根據信標幀「OPEN-OWE」SSID，客戶端會知道需要連線的其他SSID詳細資訊，在此場景中為「OWE-Transition」。如果客戶端能夠支援OWE加密，則它可以將探測請求傳送到「OWE-Transition」SSID並獲得響應。
- 探測請求傳送到OWE-Transition BSSID "40:ce:24:dd:2e:8f"，並獲得響應。在此探測響應資料包中，您還可以看到OPEN-OWE SSID詳細資訊。

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	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	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						

圖3:探測請求

從AP傳送到客戶端的探測響應

- 客戶端收到SSID「OWE-Transition」的探測響應，但是在WiFi Alliance中，其原始SSID詳細資訊為「OPEN-OWE」。

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	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	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:
>	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: PM 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

圖4:探測響應

開放式身份驗證

- 收到探測響應後，客戶端和AP之間可能會進行OPEN身份驗證，以在關聯之前檢查客戶端wifi詳細資訊/功能。

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)						

圖5:探測成功後進行OPEN身份驗證

從客戶端到AP的關聯請求

- 請注意，在此資料包中，客戶端可以附加用於加密的Diffie-Hellman引數值。

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(0), 9, 12(0), 18, 24(0), 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.: WMN/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: 7c2782ba4c77a98c7076d1fa2e3493347ec16d4c64345dccf8b9bb68b212ff31						

圖6:關聯請求

- 在RA跟蹤中，您可以開始檢視關聯階段的客戶端日誌，

```
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
```

從AP傳送到客戶端的關聯響應

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: .....C
  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: .....C]
> 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
```

圖7:關聯響應

```
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
```

金鑰交換

AP和客戶端裝置之間可能會發生4次握手。

AP傳送Key-1

Key-2 send by client

AP傳送的金鑰3

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:87	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:86	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: 00000000000000000000000000000000
 WPA Key ID: 00000000000000000000000000000000
 WPA Key MIC: 00000000000000000000000000000000
 WPA Key Data Length: 22
 > WPA Key Data: dd14000fac0421b550dab0a335c355e7f4daa4a633af

圖8:4次握手

```

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身份驗證成功

```

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學習狀態

```
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
```

客戶端處於運行狀態

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

不支援OWE加密的客戶端

- 通過檢查信標幀本身，客戶端可以知道他們是否能夠支援此加密方法。如果不受支援，則它只需向開啟SSID「OPEN-OWE」傳送探測請求即可執行正常的開放身份驗證、獲取IP地址，然後可以進入RUN狀態。

```
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
```

快速過渡資訊

- 我們只能在OPEN驗證或Webauth(CWA/LWA/EWA)中設定OWE。
- OWE轉換不支援FT。
- 如果啟用FT，則會收到此錯誤消息，

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

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

圖9:在OWE轉換SSID中啟用FT時的錯誤消息

PSK/dot1x不支援OWE

我們無法在這些組合中啟用OWE，

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

如果您嘗試啟用其中任一方法，可能會收到錯誤訊息，

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

圖10:在OWE SSID中啟用其他身份驗證方法時收到錯誤消息

⚠ 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

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

圖11:啟用AKM時的錯誤消息

- 在Cisco IOS® XE 17.9.6 IOS版本中，選擇「WPA2+WPA3」時，您可以在AKM下看到「OWE」選項，但是您會收到錯誤消息，您不能將OWE用於此組合。

⚠ 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

圖12:選擇WPA2+WPA3時出現錯誤消息

- 在Cisco IOS® XE 17.12.4版本中，當您選擇「WPA2+WPA3」時，無法在AKM中獲得「

OWE」選項，

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

圖13:錯誤消息 — 未獲得AKM中的OWE選項

疑難排解

1. 檢查WLAN、OPEN SSID和OWE轉換SSID中的配置必須對映轉換WLAN ID。
2. 廣播選項必須在OWE轉換SSID中禁用，它只能在OPEN SSID中啟用。
3. 檢查本文所述的支援的身份驗證/加密/FT方法。
4. 如果從WLC端開始配置正常，請收集所需的日誌和輸出以縮小問題範圍，

RA跟蹤和EPC (嵌入式資料包捕獲)

登入到WLC GUI -> Troubleshooting -> Radiative Trace -> Add client wifi MAC address -> Click that clients 擷取方塊 —> Start

登入到WLC GUI -> 故障排除 —> 資料包捕獲 —> 新增新檔名 —> 選擇上行鏈路介面和WMI VLAN/介面 —> 啟動。

從客戶端電腦：如果可能，您可以通過選擇WiFi介面安裝Wireshark應用並收集資料包捕獲。

<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

您可以通過使用MAC筆記型電腦或將其中一個AP配置為監聽器模式來收集它，請參閱以下連結：

在MAC筆記型電腦上：

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

從監聽器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>

將一台膝上型電腦 (wireshark伺服器) 連線到交換機埠，並且必須安裝wireshark應用程式，此wireshark伺服器必須能夠訪問WLC WMI介面。如果在WLC和Wireshark伺服器之間出現協定，則需要允許防火牆中的「5555、5000或5556」協定。

檢查安裝了wireshark的PC中是否安裝了任何「gscaler」，如果是「關閉」並嘗試，如果是windows defender之類的防火牆或其中存在的任何內容，請禁用它們，然後嘗試收集PCAP。

漫遊

當客戶端從一個AP漫遊到另一個AP時，它需要執行這些步驟，

- 需要傳送重新關聯/關聯 — 取決於客戶端請求。
- 需要在關聯請求中傳送DH(Diffie-Helman)詳細資訊。

- 客戶端可以從AP獲取關聯響應中的DH詳細資訊，基於此PMK在客戶端和AP中生成。
- AP和客戶端之間可以進行4次握手。
- 在OWE中，您無法啟用FT，因此不可能使用802.11r。
- 每次客戶端漫遊時，需要在DH交換後進行關聯的四次握手。
- 客戶端和AP使用自己的PMKID，對於每個AP和客戶端來說都是唯一的。
- 如果使用者端連線到同一個AP，則它可以使用同一個PMKID。在某些情況下，如果客戶端被刪除而非AP，可以生成新的PMKID，但是客戶端使用相同的PMKID進行4次握手。

範例：

如果客戶端連線到同一個AP，則在Association-Request和Association-Response中都可以看到相同的PMKID。在關聯響應中，如果使用PMKID，則無法檢視DH詳細資訊。

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) on interface 0 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) 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.: 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 bb 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							

圖14:使用同一PMKID

No.	Time	Source	Destination	Protocol	Length	Sequence Number (BE)	PMKID	Info
8527	2025-01-21 09:51:57.333153	Cisco_dd:2e: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) on interface 0 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: 0x00e8 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: 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								

圖15:使用同一PMKID的關聯回應

為了進行測試，已手動從WLC刪除此客戶端，並且它再次與同一個AP關聯，此時，客戶端傳送同一個PMKID，但AP在關聯響應中傳送DH詳細資訊。

No.	Time	Source	Destination	Protocol	Length	Sequence Number (BE)	PMKID	Info
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 44117: 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 D1.0) > 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: 0x0000 > 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.: 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: ba ba f5 2b f0 a5 4c 02 2f 16 f1 0b ad 95 a0 4f cf 95 79 58 3d dc 77 96 bb b3 59 52 42 25 cf 6f								

圖16:刪除後，使用者端傳送了包含詳細資訊的PMKID

No.	Time	Source	Destination	Protocol	Length	Sequence Number (BE)	PMKID	Info
44121	2025-01-21 09:53:12.851872	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	802.11	266			Association Response, SN=1229, FN=0, Flags=.....C
> Frame 44121: 266 bytes on wire (2128 bits), 266 bytes captured (2128 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 (196 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: 26 > 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: 0x0000 > PMKID Count: 0 > PMKID List > Group Management Cipher Suite: 00:0f:ac (Ieee 802.11) BIP (128) > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element > 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: RM Enabled Capabilities (5 octets) > Tag: BSS Max Idle Period > 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: e4 44 ea 00 6f f3 69 35 33 93 59 3f 7d b7 2e ab d4 04 26 7e 62 da d9 2a 88 c9 4e f5 e2 69 a1 c5								

圖17:AP使用DH值生成其新的PMKID

在此範例中：AP和客戶端在進行4次握手時使用同一個PMKID，請簽入「M1和M2」消息。

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								

圖 — 18:使用相同PMKID的AP和客戶端

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。