瞭解機會無線加密流程

目錄

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」。

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」。

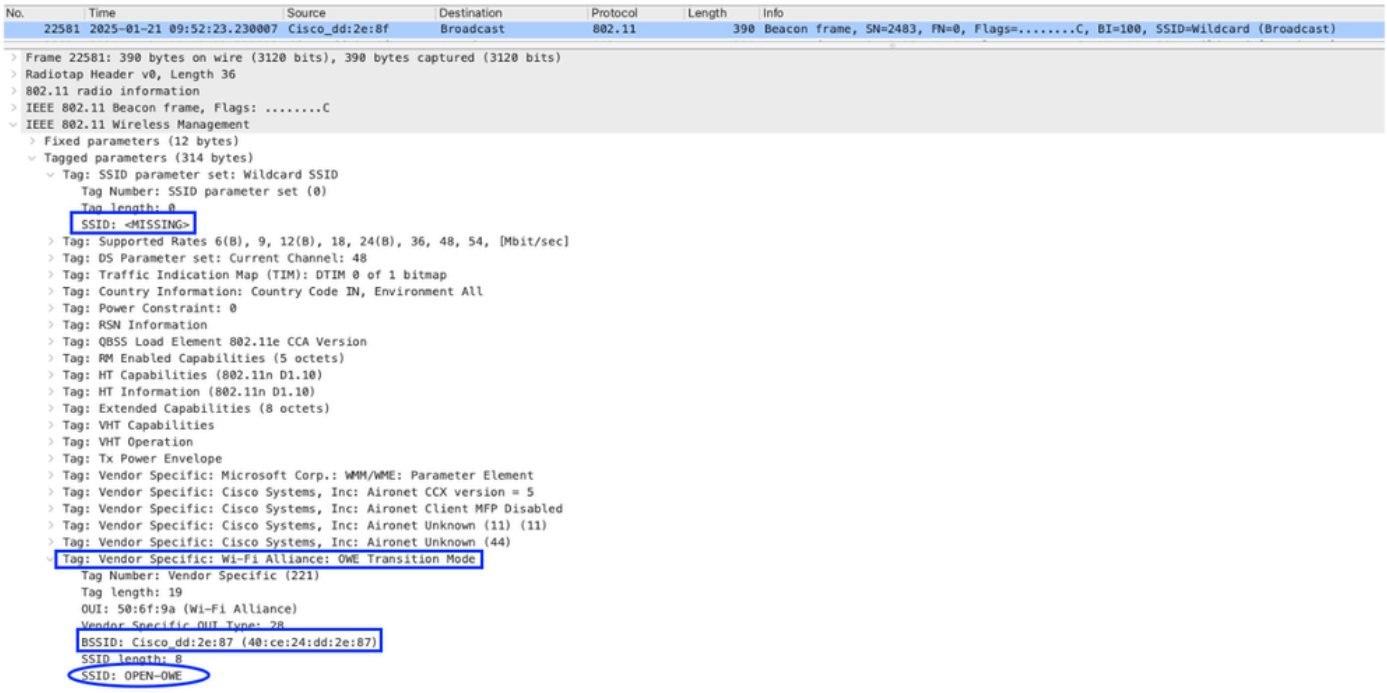

圖2:隱藏SSID - OWE轉換

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。

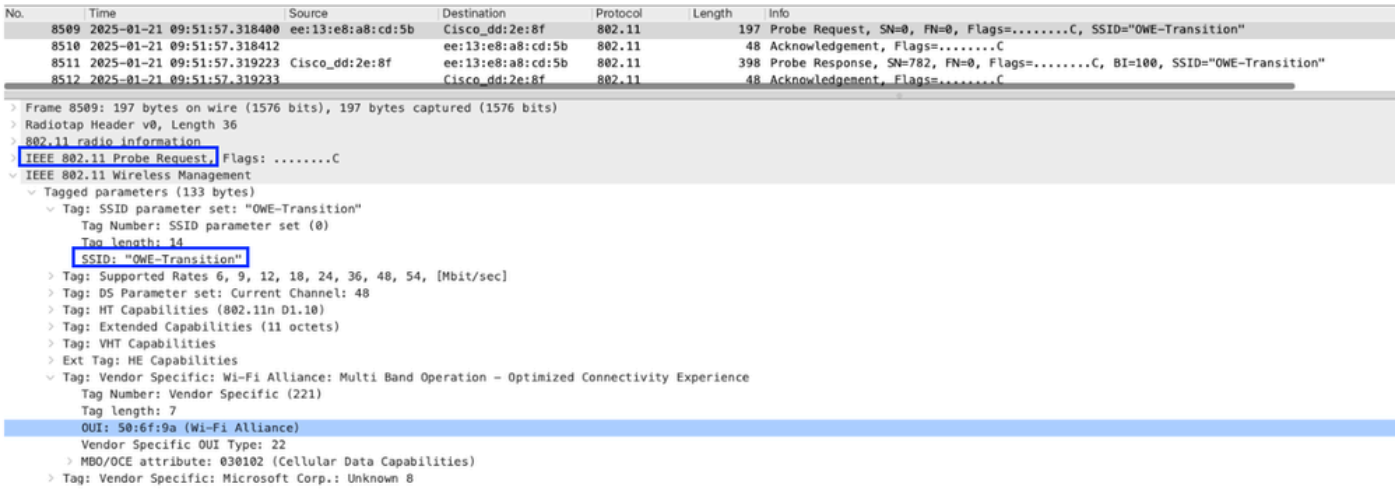

圖3:探測請求

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」。

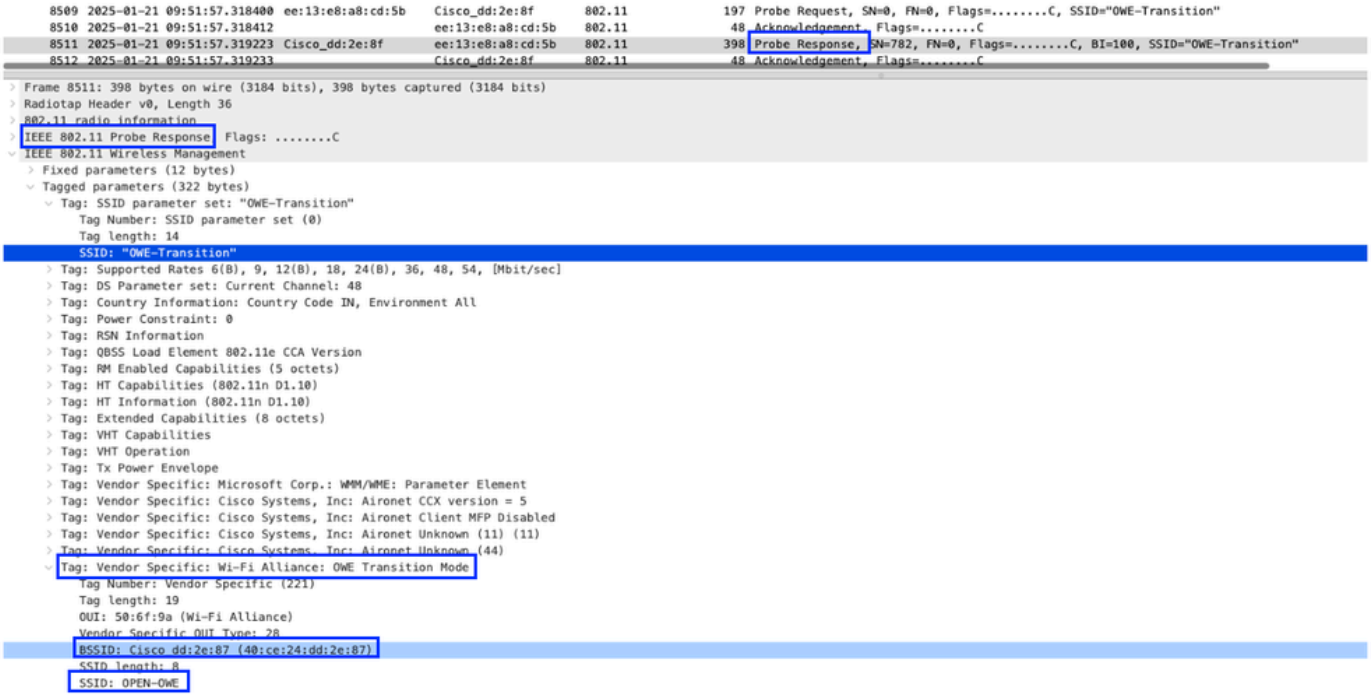

圖4:探測響應

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。

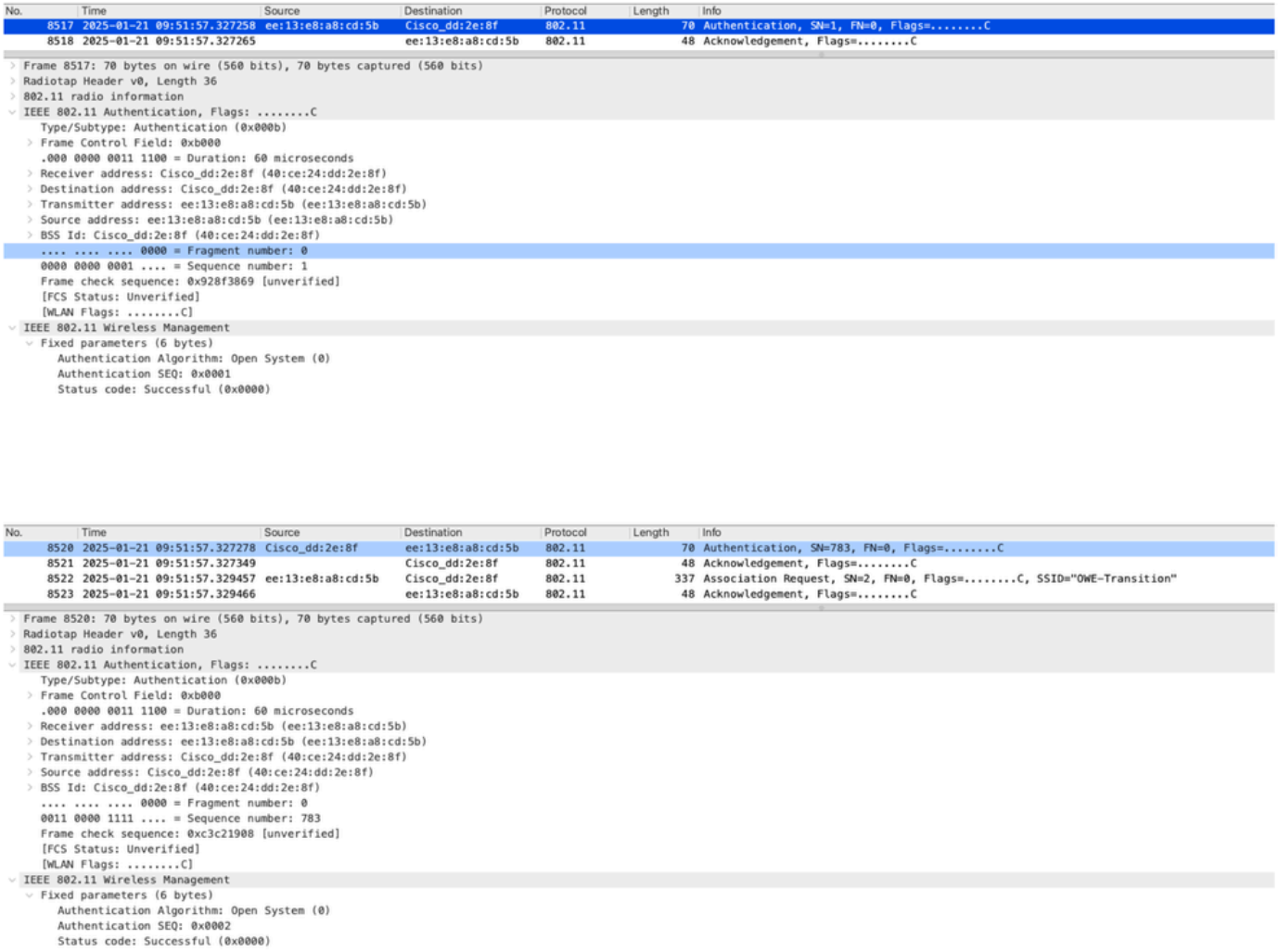

圖5:探測成功後進行OPEN身份驗證

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。

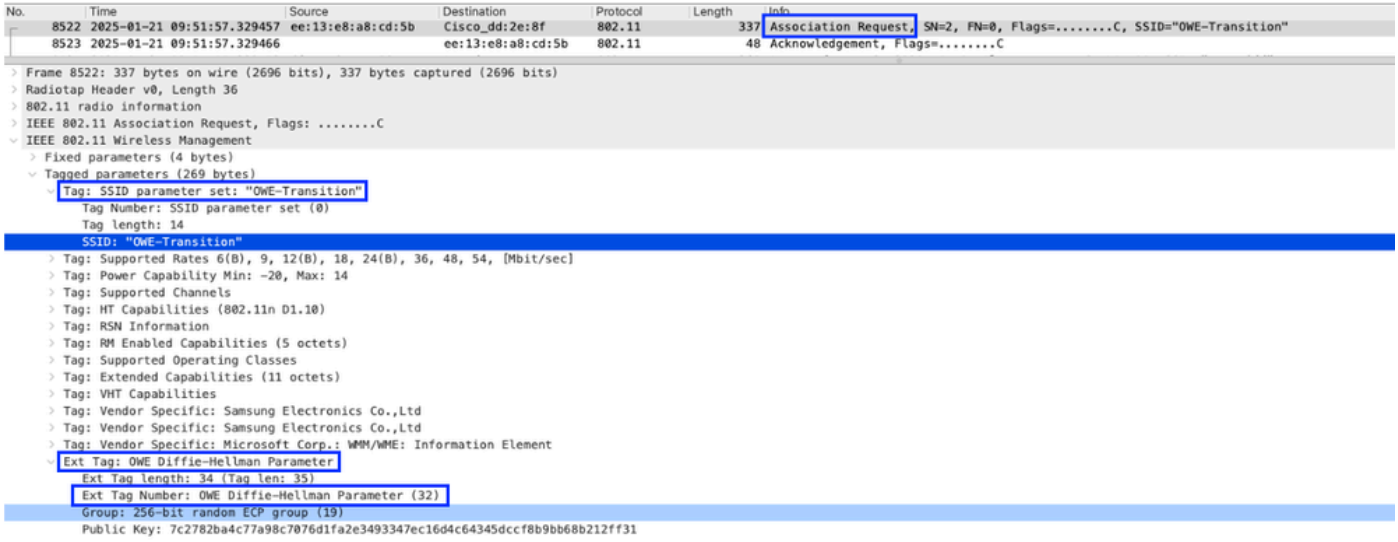

圖6:關聯請求

- 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  A
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

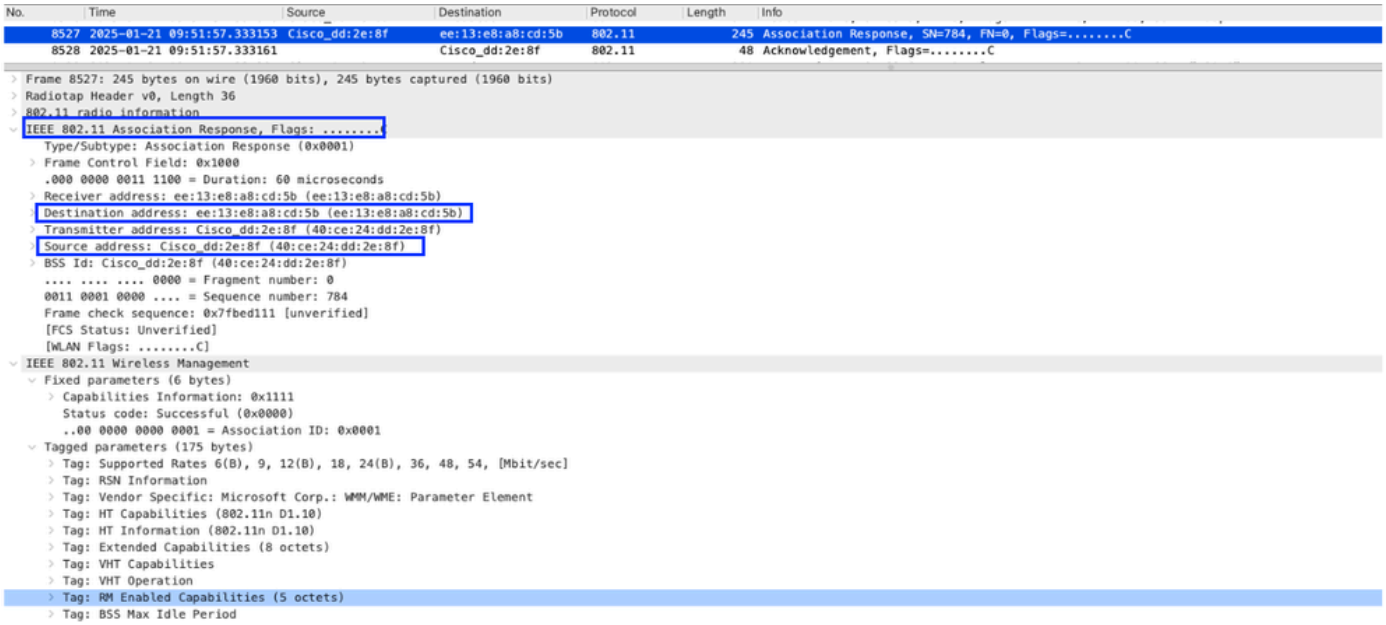

圖7:關聯響應

```
2025/01/21 15:21:57.391334260 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5
2025/01/21 15:21:57.392296819 {wncd_x_R0-0}{1}: [dot11] [21675]: (note): MAC: ee13.e8a8.cd5b  Associati
```

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

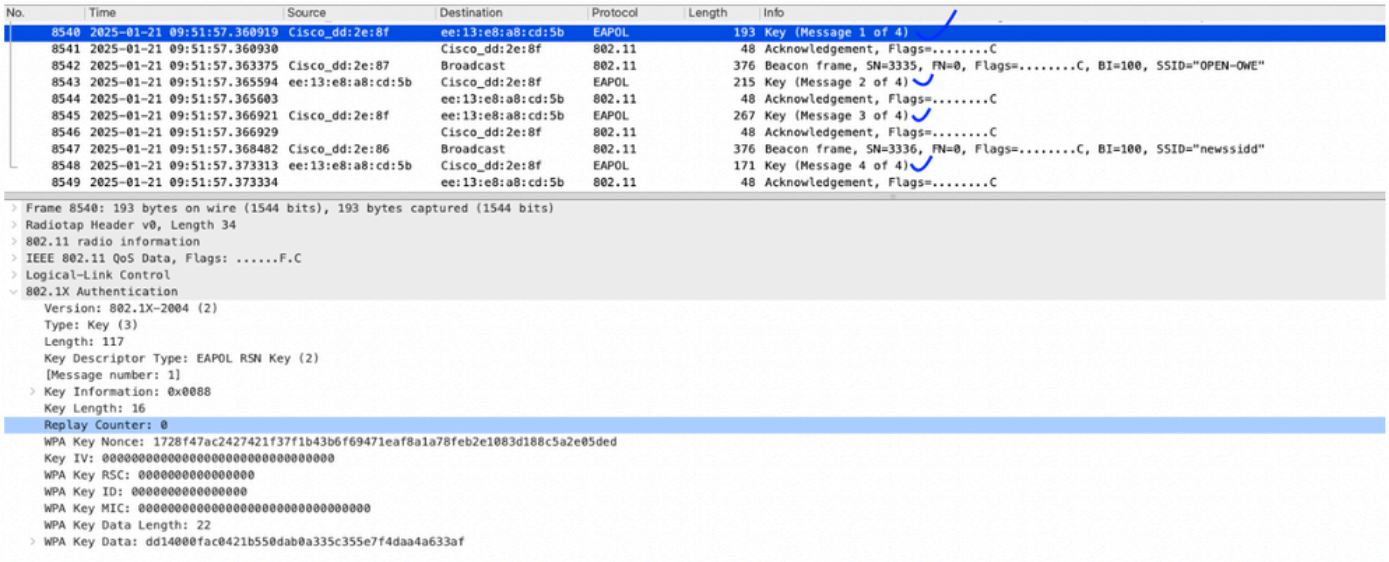

圖8:4次握手

```
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.cd5
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.cd5
2025/01/21 15:21:57.437239513 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5
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 interfac
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 interfac
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.cd5
```

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，

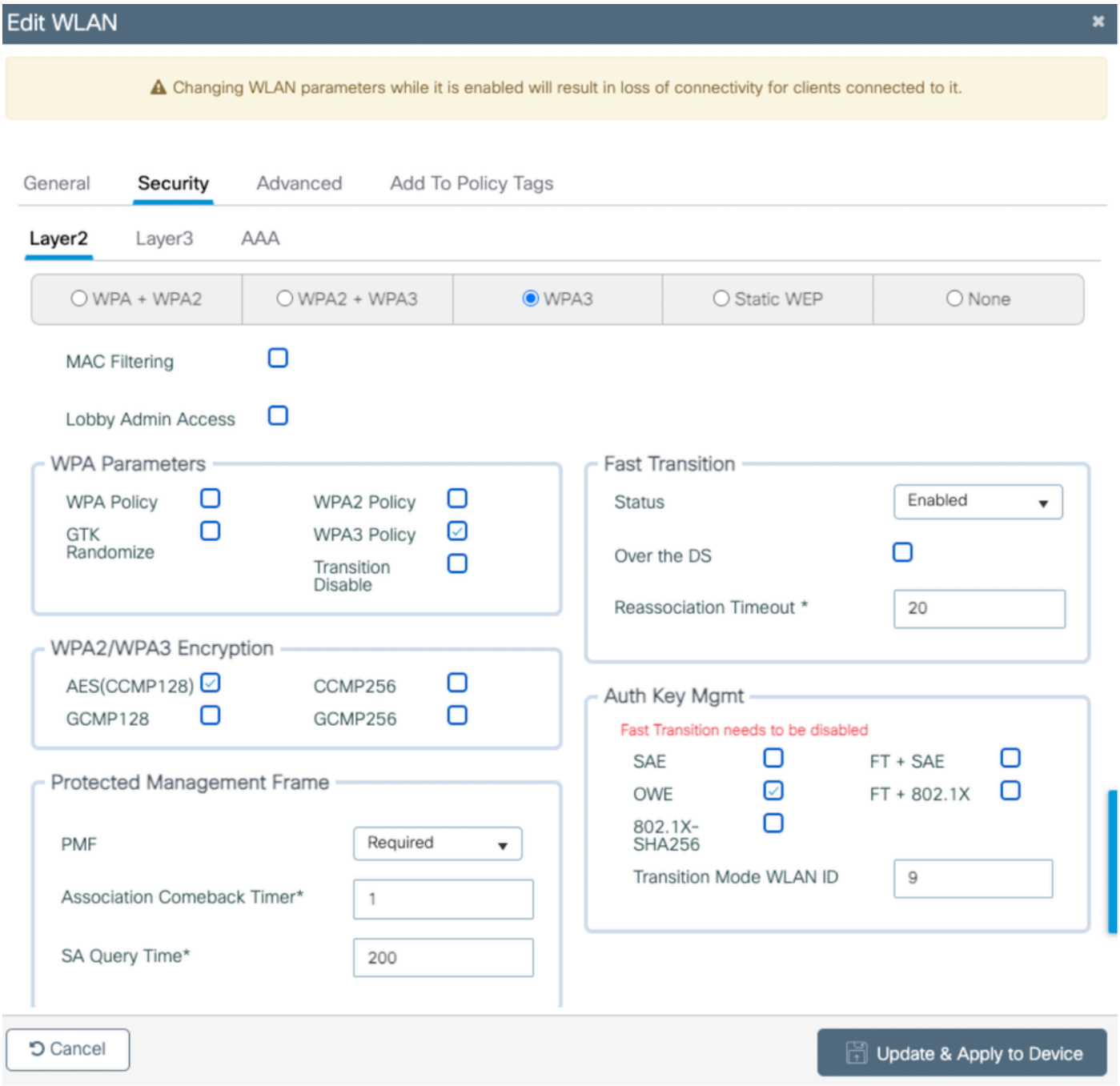

圖9:在OWE轉換SSID中啟用FT時的錯誤消息

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，

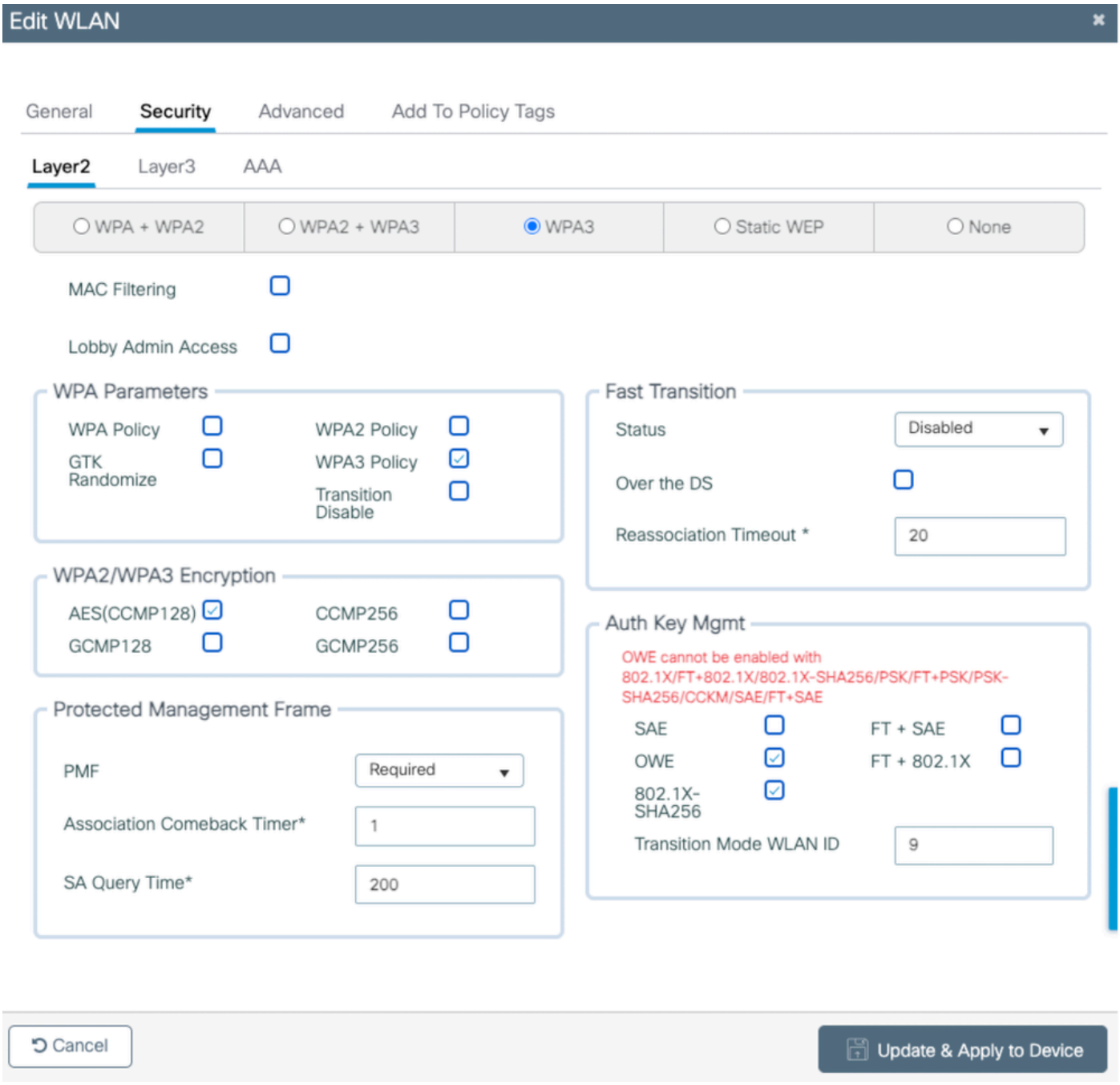

圖10:在OWE SSID中啟用其他身份驗證方法時收到錯誤消息

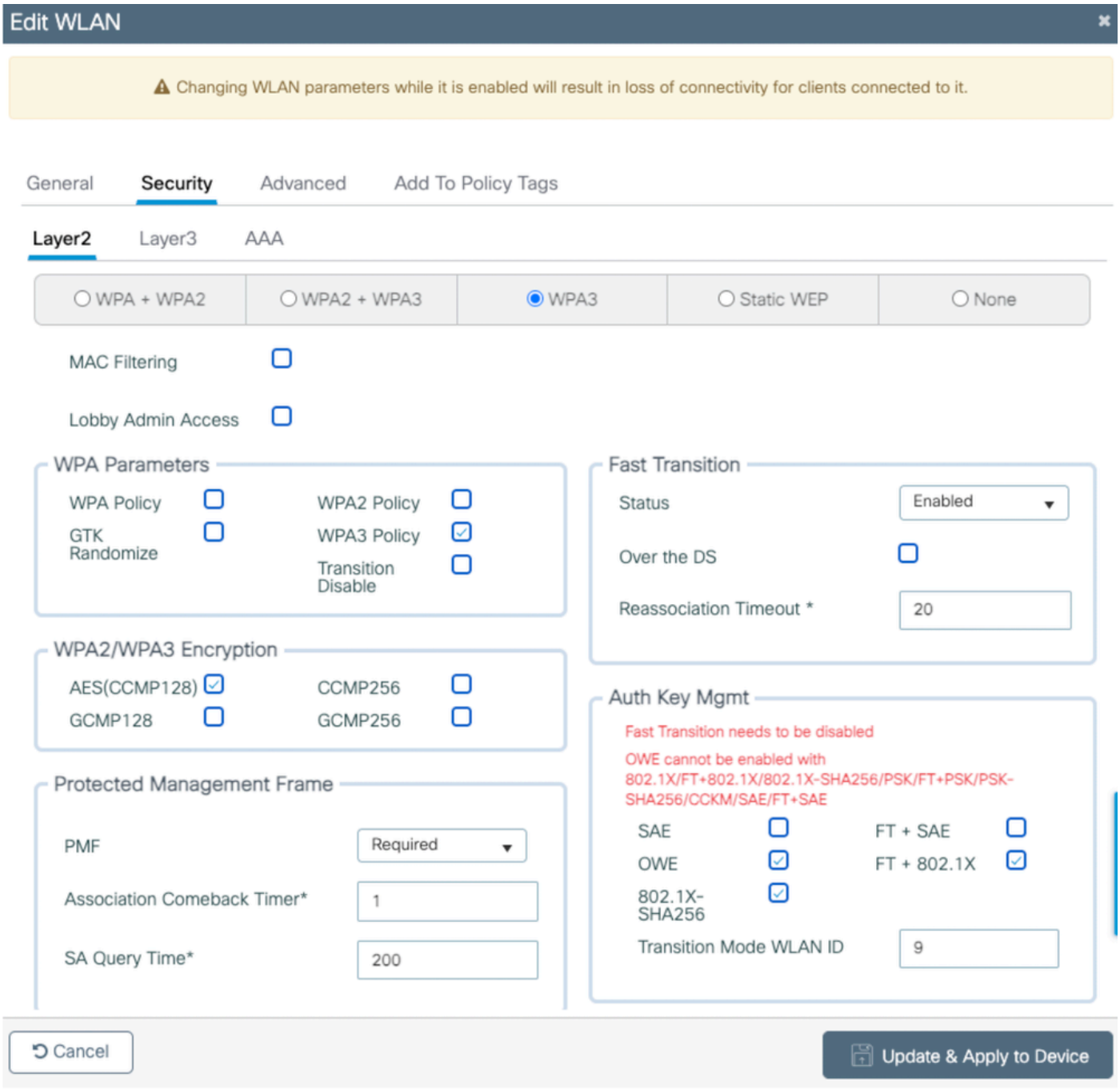

圖11:啟用AKM時的錯誤消息

- 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。

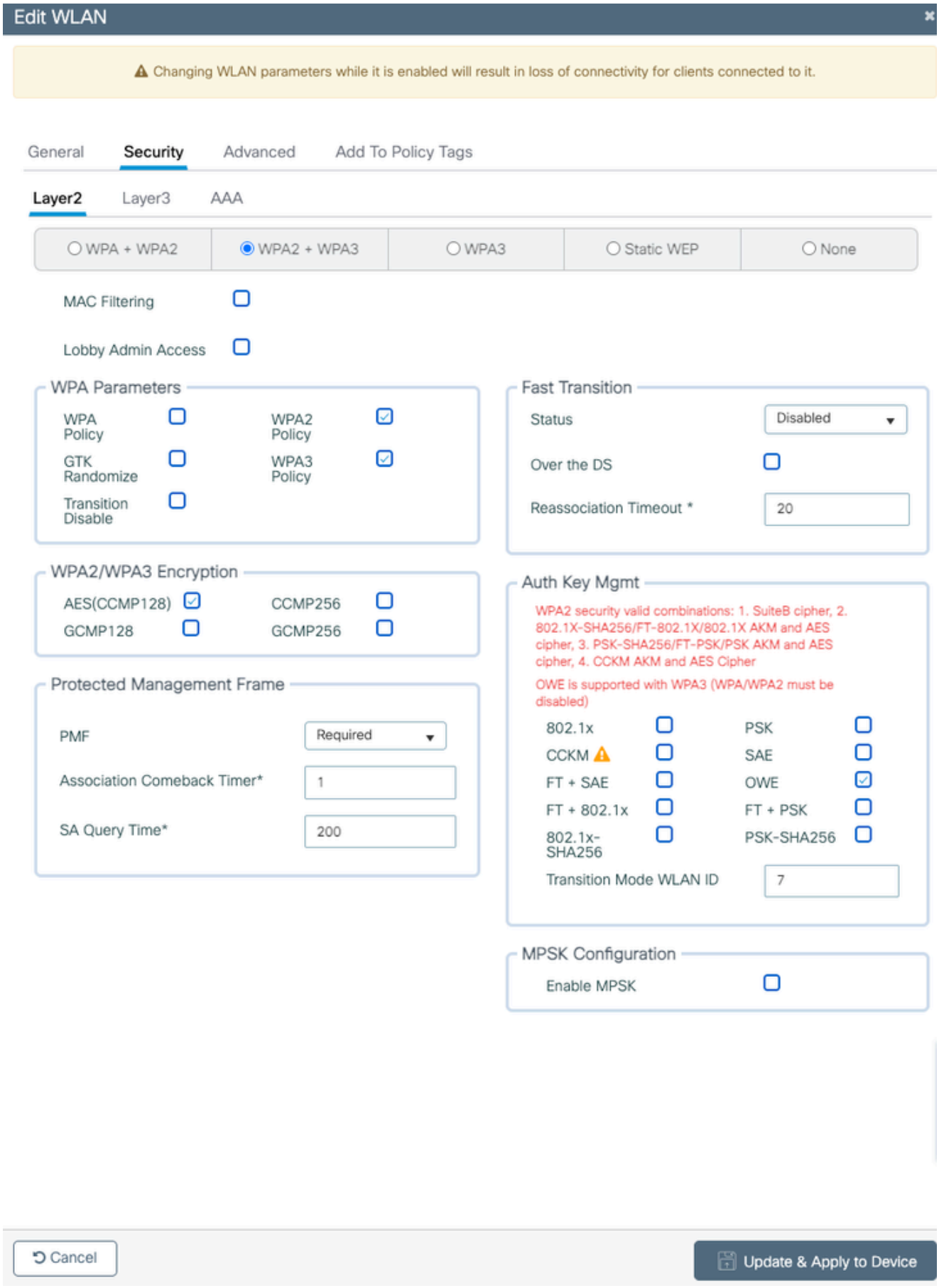

圖12:選擇WPA2+WPA3時出現錯誤消息

- 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，

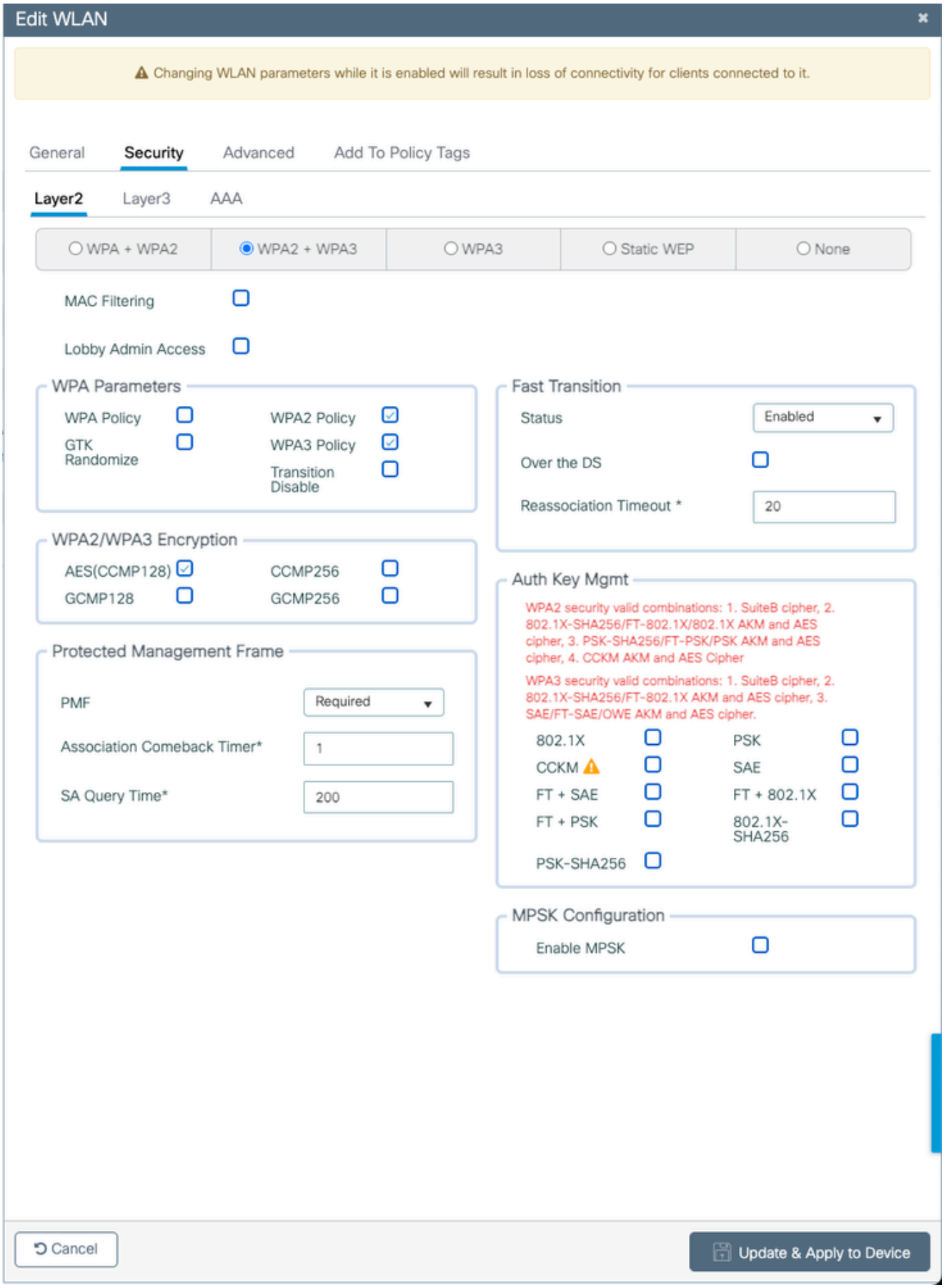

圖13:錯誤消息 — 未獲得AKM中的OWE選項

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覈取方塊 — > 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。

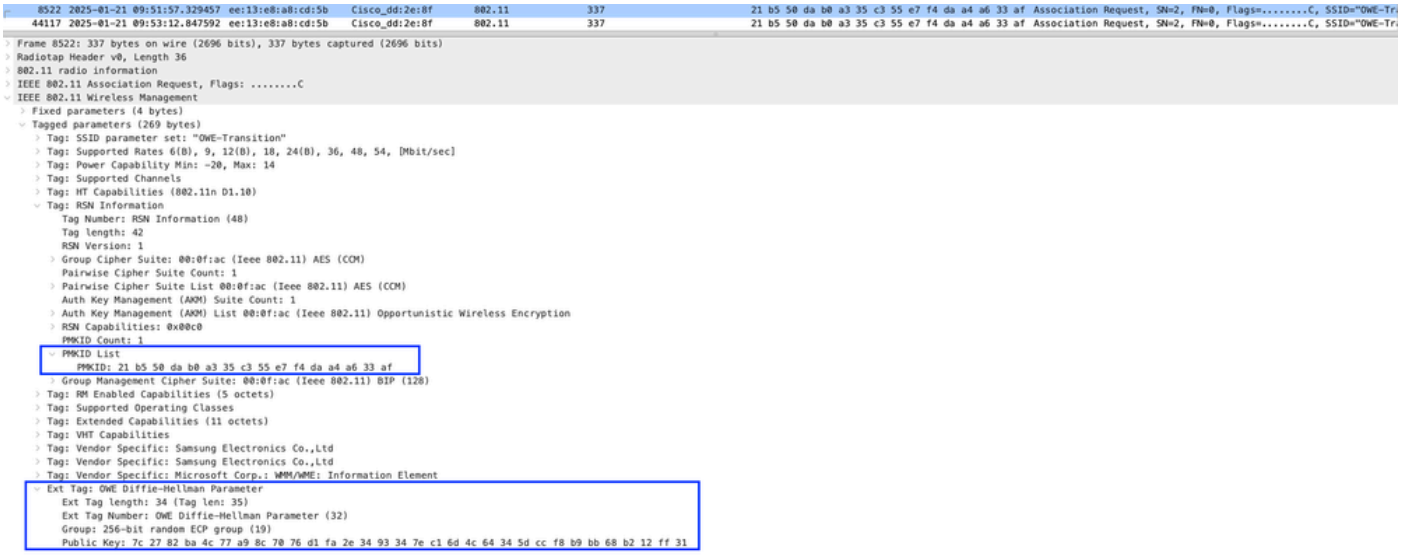

圖14:使用同一PMKID

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。

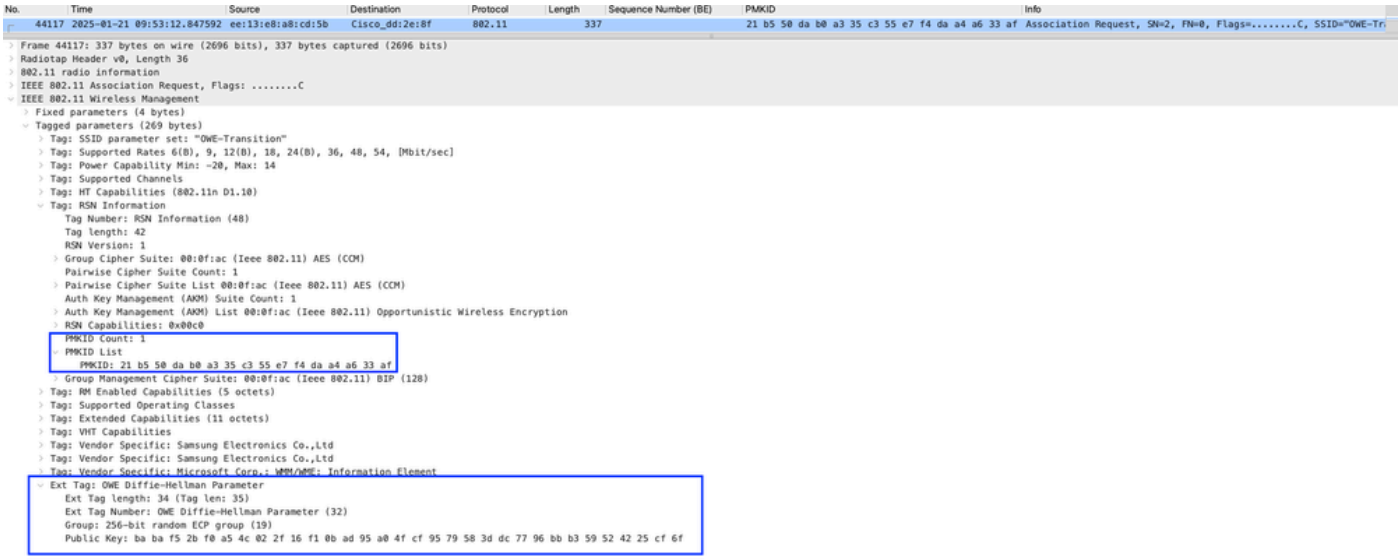

圖16:刪除後，使用者端傳送了包含詳細資訊的PMKID

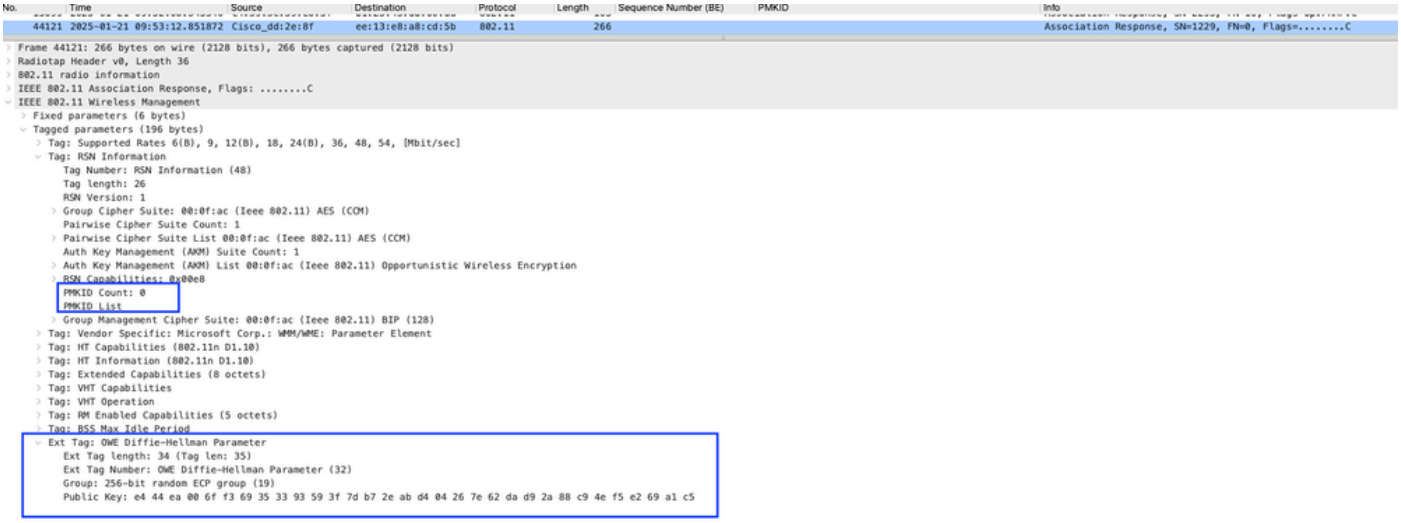

圖17:AP使用DH值生成其新的PMKID

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。

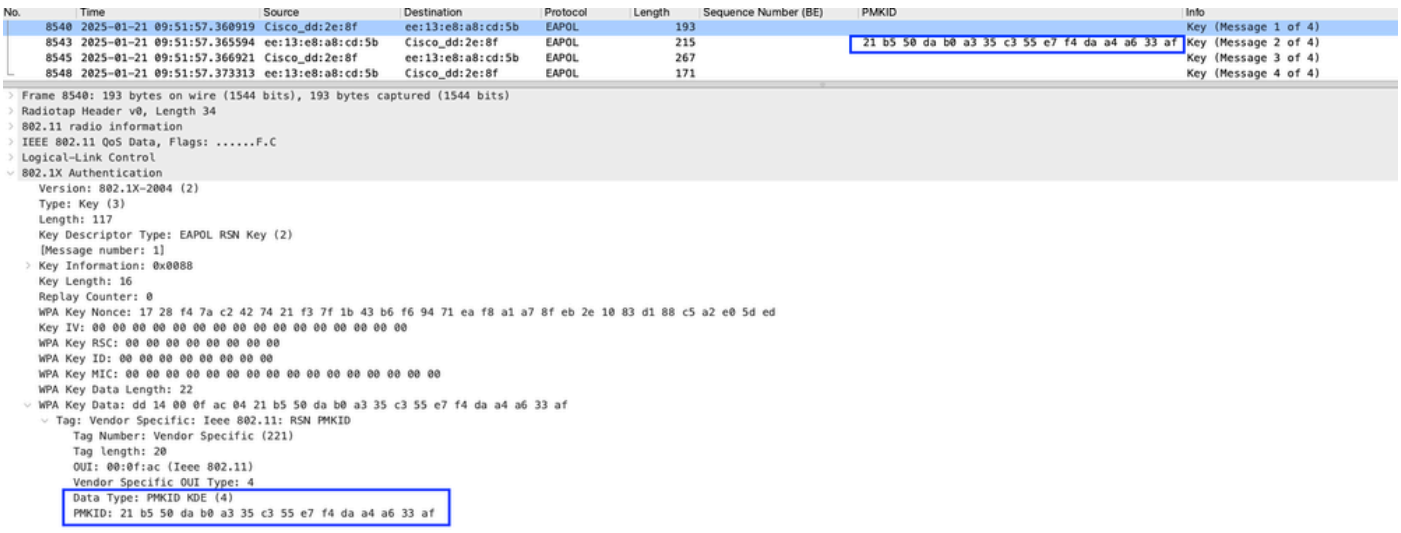

圖 — 18:使用相同PMKID的AP和客戶端

在此範例中：使用者端使用相同的PMKID但AP使用不同的PMKID（在使用者端被刪除後生成），請檢查「M1和M2」訊息。

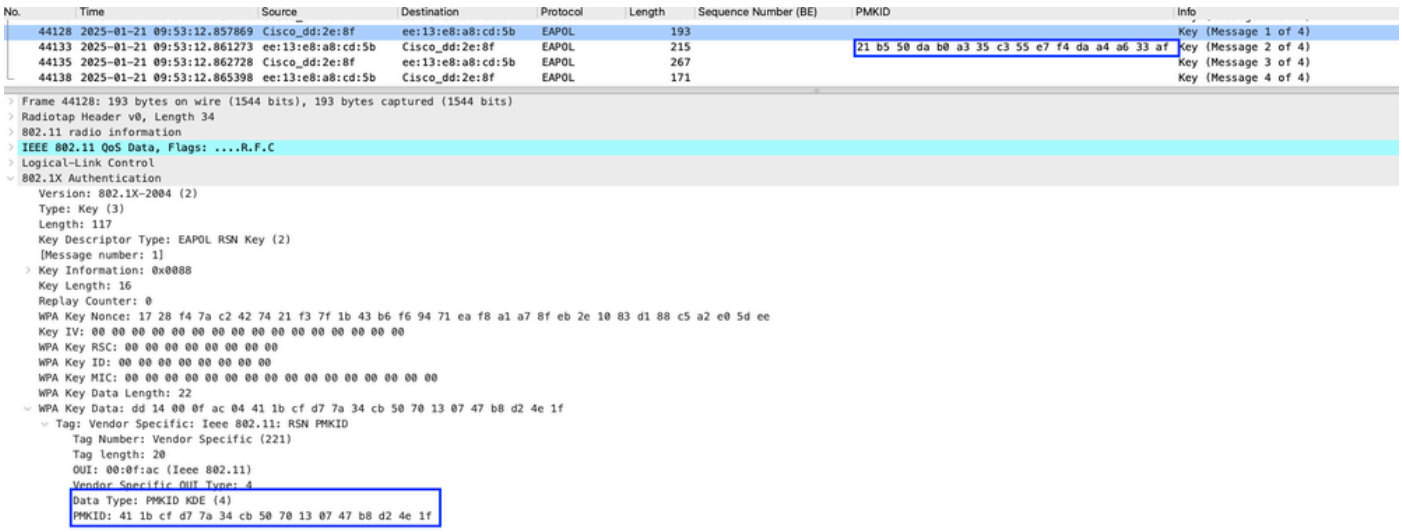

圖19:使用不同PMKID的AP和客戶端

在內部RA跟蹤中：

在此範例中：客戶端傳送了association-request中的DH引數，且AP已處理而不是生成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
```

之後，同一個使用者端連線到同一個AP，這時AP沒有產生新的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
```

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）。